FOREWORD

I am a firm believer that Information and Communication Technologies are making an essential contribution to economic growth and to jobs in Europe. Such technologies can open new avenues for exploration, and circumvent existing roadblocks in the marketplace. By addressing and ultimately validating the feasibility of revolutionary new ideas, upstream 'visionary-driven' research should prepare the way for more 'industrially-driven' research on a wider, and more commercial scale.

Quantum Information Processing and Communication (QIPC) is a new scientific field which opens unconventional perspectives for information processing. Quantum physics has revolutionised science in the 20th century. The exploitation of quantum effects is set to revolutionise information processing in the 21st century. There is a major world-wide effort to advance research in QIPC, which has led to a deeper and broader understanding of information theory, of computer science and of the fundamental laws of the quantum world. It has the potential to lead to new technologies and to devices capable of performing tasks which could not be accomplished before. These may radically change the way we communicate and compute.

Europe has been at the forefront of QIPC research since the beginning, both within IST and national research programmes. The articles presented in this brochure give a broad and balanced overview of the current developments on QIPC, which we hope will help decision makers and strategists to further understand and continue to support investment in this important new field. We also need to attract more young scientists to work in long-term research. Giving them an insight into the exiting world of QIPC may just help. This publication is a useful source of information for scientists from adjacent research fields, and also for the wider, scientifically minded public.

I would like to thank all the scientists who have contributed, and to wish them every success in their endeavours to advance our knowledge in this strategically important field.

Viviane Reding
European Commissioner for
Information and Society and Media

Introduction

Thierry Van der Pyl
Thierry Van der Pyl is Head of Unit "Future and Emerging Technologies" in DG INFSO, European Commission. He holds the degree *Docteur d'Etat es Sciences Mathématiques* from Université Pierre et Marie Curie Paris VI in France.

Antonella Karlson
Antonella Karlson is scientific officer in Unit "Future and Emerging Technologies" in DG INFSO, European Commission and the coordinator of the FET Proactive Initiative in QIPC. She has a Ph.D. in theoretical physics from The City College of The City University of New York. Her research experience is in the area of quantum field theory, laser-atom interactions and QIPC.

Quantum Information Processing and Communication (QIPC) is a new scientific field with origins in the late 80's and early 90's. It is multidisciplinary by nature, with scientists coming from diverse areas in both theoretical and experimental physics (atomic physics, quantum optics and laser physics, high energy and mathematical physics, condensed matter, etc.) and from other disciplines such as computer science, mathematics, material science and engineering. The main goal is to understand the quantum nature of information and to learn how to formulate, manipulate, and process it using physical systems that operate on quantum mechanical principles, more precisely on the control and manipulation of individual quantum degrees of freedom. There is something specific that is unusual and sets QIPC apart from most other fields of science and technology - something that makes it so desirable and so interesting, but at the same time so challenging and so evasive. It is the way QIPC connects the most fundamental theory with fundamental experimentation, whilst offering novel, practical and useful applications at the same time. Research in QIPC has led to a deeper and broader understanding of quantum mechanics and of the fundamental laws of the quantum world, the causality principle, the nature of information, information theory and computer science. It has led to the conception of machines and devices able to perform tasks which could not be accomplished before and have the potential to radically change the way we communicate and compute.

Aim of this publication

The aim of this publication is to report on and to promote Quantum Information Processing and Communication (QIPC) research in Europe. It consists of a collection of short articles written by the most prominent European experts. The intention is to present, in an accessible way, the colorful mosaic of different aspects of QIPC research. The goal of each article is to cover first the basic concepts and ideas of a particular sub-area and then to give examples, possible applications and technological realisations. The stress is on results obtained within the context of European Commission or nationally-funded projects. We believe that the set of articles gives a broad and balanced overview of current QIPC research in Europe: main topics, achievements, challenges, visions, as well as the research groups, projects and collaborations, at a level appropriate for non-specialists.

We hope that this publication will give a structured and up-to-date overview of European research in QIPC and will help decision makers, both at pan-European and national level (research policy, academia and industry), further support this field. We also believe that this publication will attract young scientists to the field and help them gain a new insight in QIPC. This publication can be a useful source of information for scientists from adjacent research fields, as well as for the wider scientifically curious public. We hope that everybody will be fascinated by the multitude of daring ideas and the richness of exchange between excellent researchers.

We hope that this publication will contribute *to building a European identity and to expressing a unified image of QIPC research in Europe*.

Structure of this publication

The publication is a collective effort to give a status report of European QIPC research at this point in time (March 2005). It covers most of the research areas of QIPC. It starts with an excellent overview written by David Deutsch and Artur Ekert, which gives in a nutshell the main visions and challenges of the whole field. Afterwards Anton Zeilinger presents the basic ideas of quantum information and the reasons why it is so different, so challenging and so fascinating at the same time. This is followed by four articles on quantum entanglement, which is one of the main physical phenomena that constitute the basis of QIPC. The first two articles cover theoretical aspects, the last two – experimental ones. Next is an article on quantum teleportation explaining one of the most amazing phenomena in QIPC. Quantum communication, one of the two main aspects of QIPC, is introduced by the experts in the field - Nicolas Gisin and John Rarity. In 2004 the FET-funded project QuComm won the Descartes prize (consortium members: A. Karlsson – coordinator, Th. Debuisschert, A. Ekert, N. Gisin, R. Hughes, G. Rarity, H. Weinfurter, A. Zeilinger). We are happy that six of the eight QuComm partners have contributed to this publication. Next follow four articles which present the experimental challenges related to quantum communication, entanglement of photons, optical approaches to QIPC, etc. Afterwards is an overview article on quantum cryptography written by Artur Ekert, one of the fathers of this field. Follow two articles on fundamental mathematical aspects of quantum communication with important repercussions on practical realizations. The next article presents new ideas on the relation between quantum information and statistical mechanics. Quantum computation is the second main aspect of QIPC. It is introduced by an extensive and comprehensive article on quantum algorithms. The

reader can understand the advantages of quantum computing with respect to classical computing and the basic concepts of quantum computer science. This is followed by an article on quantum simulations, which explains how this approach can obtain results circumventing some of the difficulties of universal quantum computation. The article on decoherence presents a fundamental physical issue in QIPC and is one of its critical challenges. Next is a group of nine articles: each presenting a possible specific realization of a quantum information processor (QIP) based on a different physical system. To our knowledge, there exist two realisations of a QIP that are not presented here: one is based on nuclear magnetic resonance and the other one – on quantum dots. To date, no one specific realisation has proved to be the winning one. At present, some of them demonstrate more advantages than others or are at a more advanced stage of development. Only further research can show how a future QIP will look like. The final two articles present concrete spin-off applications of the basic principles of QIPC.

QIPC in the European Research Programmes: More than 15 years of research

QIPC has a high-risk nature and long-term outlook with visions within the scope of information and communication technologies. The potential of QIPC was quickly recognised by FET – the Future and Emerging Technologies programme of the Information Society Technologies priority of the Research Programme of the European Commission. The pathfinder role of FET played a crucial role for the development of QIPC in Europe.

In the late 80's and early 90's quantum phenomena were studied by projects funded by the EC in the field of optoelectronics and electronics with the aim to overcome the limitations to the respective state-of-the-art devices. In the Fourth Framework Programme (FP4, 1995 – 1998) this research gradually evolved towards the objective of "quantum information processing". The focus was on the demonstration of quantum effects with photons, which was technologically more mature. In the mid 90's, important results were achieved by several groups in Europe and shortly after they became the driving force behind a number of FET projects.

During 1998 the QCEPP working group (the so-called Pathfinder project) laid the basis for the research field of Quantum Information Processing and Communications at the European level and was the first endeavour explicitly to addres this area of research. This working group produced an extensive report with a roadmap, a map of European research teams with relevant competencies and set the research agenda for several years ahead. It played a crucial role by organising the research community, stimulating it to reach critical mass within a short time period and building the support for the launch of QIPC as a Proactive Initiative.

In FP5 (1999 – 2002) FET launched QIPC as a Proactive Initiative (PI). It was implemented via 'calls for proposals' directly targeted to QIPC. There were two calls for proposals and 25 projects were launched with an EU funding of 31 M€. The contracts of the last group of FP5 projects finish at the end of 2005. Coordinating the work of these projects is a main priority of FET. Each year, since the beginning of the proactive initiative, two major events are organised. The first one is a 'cluster review' and conference. Its goals are to evaluate the work of each project and how its objectives fit within the cluster, to revise priorities if necessary and to evaluate the progress of the cluster as a whole. The second event is the annual

European QIPC workshop where projects present their work. Both fora give the opportunity for interactions between the members of the projects and for cross-fertilisation.

In FP6 (2003 - 2006) QIPC continues as a FET Proactive Initiative. There was one call for Integrated Projects (IP) with deadline 22 September 2004. There are three Integrated Projects which succeeded in the evaluations and negotiations are in progress. Projects are to start in September 2005 with a contract for four years. The total EU funding is 25 M€. These IPs are:

- SCALA: Scalable Quantum Computing with Light and Atoms
- QAP: Qubit Applications
- EuroSQIP: European Superconducting Quantum Information Processor

All projects deal with central topics of quantum computing and one of them (QAP) addresses in addition central topics of quantum communication and quantum information. All three consortia involve leading European scientists in their respective fields. In all projects the European dimension is a clear added value. In two of them (SCALA and QAP) the accent on integration across different disciplines and approaches is very strong and it is considered crucial for the further advancement of QIPC research in Europe.

QIPC is also funded via the *FET-Open* continuous submission scheme, which supports long-term, risky and visionary research. In this case the research area is not specified in advance and QIPC projects are competing with all other areas sponsored by FET. In FP5 ten QIPC projects with total cost of 7 M€ and EU funding of 5.6 M€ were launched. The QUIPROCONE Thematic Network successfully coordinated all QIPC projects in FP5, integrating the projects arising from the Open scheme with those supported through the proactive initiative. In FP6 four projects are already funded via FET Open and others are expected to follow. The role of FET Open is essential as it supports new topics that had not been addressed in the proactive initiative and prevents the time gaps that would otherwise occur by relying solely on dedicated QIPC calls.

In 2004 there was a call for proposals for coordinated actions related to structuring the ERA (European Research Area). The project "Structuring the ERA with quantum information science and technology" or *ERA-Pilot QIST* was successful and started work on February 1, 2005. It has many challenging objectives with the goal to promote QIPC research in Europe and to give recommendations to European and national authorities on policy, structuring, coordination and funding. The deliverables include: regular updates of the QIPC roadmap document; elaboration of a map of European research teams and expertise; information on national initiatives and programs; information on international initiatives and programs; proposal for coordination and synergies between national and EC initiatives; proposal for benchmarking; organisation of conferences, etc.

Within QIPC – FET specific efforts were dedicated to quantum cryptography. In FP4 seed work was done by the EQCSPOT project. It led to a wider field of investigation in a number of projects of the QIPC Proactive Initiative in FP5, where they reached maturity. In FP6 this area of research was transferred to more applied parts of the IST programme. Quantum cryptography is now part of the strategic objective "Towards a global dependability and security framework", where a large Integrated Project SECOQC is funded. The consortium consists of about 40 partners, including several large companies. The EC funding is of 11.35 M€. The project includes all prominent groups in Europe active in this field. They were all initially funded through FET.

QIPC and National Initiatives

Apart from the EU program, QIPC is also coordinated and funded on national level. An extensive list of such initiatives is not available at the moment and it is one of the goals of the project ERA-Pilot QIST. Initiatives exist in the United Kingdom, Denmark, Sweden, Austria, France, Germany, Italy, Slovakia and Poland.

Coordination between national and EC programs will have decisive influence on the progress of QIPC research in Europe. Strong and visionary leadership of high quality is also important. Only by stronger coordination between national efforts among each other and with the EC program, can the required critical mass in various sub-fields can be reached and maintaind. Experience and knowledge should be shared and neither efforts nor funding should be duplicated. Funding will ultimately have to concentrate mainly on centers of excellence specialised in a certain domain in order to achieve the highest possible impact.

Outlook

The field of QIPC has matured in the last ten years. There is critical mass in Europe in the main sub-fields. It is clear that QIPC research has gained an important European dimension which is crucial for its further development. It is, however, necessary to expand and strengthen activities at the European level.

We are working towards common goals and a common European strategy. It is crucial to support and maintain research in the main areas of QIPC: quantum communication, computation and information theory. At this stage it is also important to keep a diversity of experimental realizations and approaches, and yet actively to look for synergies and integration between them in order to reach concrete objectives. Some areas of QIPC seem closer to achieving a number of landmark results and have the potential to make possible concrete applications within a medium-term future. We need to ensure timely and appropriate concentration of efforts and coordination of activities in these areas.

Breakthroughs of the type needed to make QIPC a reality cannot be expected to follow a precise timetable. It is however imperative that at each point in time we have a clear understanding of the results obtained, an assessment of the strengths and weaknesses in present research, as well as a clear definition of the challenges and the objectives. The collective effort of the scientific community has resulted in a stable version of “QIPC: strategic report on current status, visions and goals for research in Europe”. This roadmap-type document and the current publication complement each other and represent important milestones on the way toward a common European strategy in QIPC.

For more information on FET activities in QIPC, please see:
http://www.cordis.lu/ist/fet/qipc.htm

Overview

David Deutsch
Since 1999 David Deutsch has been a Visiting Professor of Physics at the University of Oxford, where he is a founder member of the Centre for Quantum Computation at the Clarendon Laboratory. In 2002 he received the Fourth International Award on Quantum Communication for "theoretical work on Quantum Computer Science". In 1998 he was awarded the Institute of Physics' Paul Dirac Prize and Medal, for "pioneering work in quantum computation leading to the concept of a quantum computer and for contributing to the understanding of how such devices might be constructed from quantum logic gates in quantum networks". He is a Distinguished Fellow of the British Computer Society, and author of the highly acclaimed popular book "The Fabric of Reality".

Artur Ekert
Artur Ekert is the Leigh Trapnell Professor of Quantum Physics at the Department of Applied Mathematics and Theoretical Physics, University of Cambridge, UK. He has worked with and advised several companies and government agencies and has made a number of contributions to quantum information science, in particular to quantum cryptography, which he co-invented. He was also a member of the EU-funded IST project QuComm that received the 2004 Descartes prize.

The theory of classical computation was laid down in the 1930s, was implemented within a decade, became commercial within another decade, and dominated the world's economy half a century later. However, the classical theory of computation is fundamentally inadequate. It cannot describe information processing in quantum systems such as atoms or molecules. Yet logic gates and wires are becoming smaller and soon they will be made out of only a handful of atoms. If this process is to continue in the future, new, quantum technology must replace or supplement what we have now.

In addition, quantum information technology can support entirely new modes of information processing based on quantum principles. Its eventual impact may be as great or even greater than that of its classical predecessor.

While conventional computers perform calculations on fundamental pieces of information called bits, which can take the values 0 or 1, quantum computers use objects called quantum bits, or qubits, which can represent both 0 and 1 at the same time. This phenomenon is called quantum superposition. Such inherently quantum states can be prepared using, for example, electronic states of an atom, polarized states of a single photon, spin states of an atomic nucleus, electrodynamical states of a superconducting circuit, and many other physical systems. Similarly, registers made out of several qubits can simultaneously represent many numbers in quantum superpositions. Quantum processors can then evolve initial superpositions of encoded numbers into different superpositions. During such an evolution, each number in the superposition is affected and the result is a massive parallel computation performed in a single component of quantum hardware. The laws of quantum mechanics then allow this information to be recombined in certain ways. For instance, quantum algorithms can turn a certain class of hard mathematical problems into easy ones -- the factoring of large numbers being the most striking example so far. Another potential use is code-breaking, which has generated a great deal of interest among cryptologists and the data security industry.

In order to accomplish any of the above tasks, any classical computer has to repeat the same computation that many times or use that many discrete processors working in parallel. This has a decisive impact on the execution time and memory requirement. Thus quantum computer technology will be able to perform tasks utterly intractable on any conceivable non-quantum hardware.

Qubits can also become entangled. Quantum entanglement is a subtle non-local correlation between the parts of a quantum system. It has no classical analogue. An entangled state shared by two separated parties is a valuable resource for novel quantum communication protocols, including quantum cryptography, quantum teleportation and quantum dense coding. Quantum cryptography offers new methods of secure communication that are not threatened even by the power of quantum computers. Unlike all classical cryptography it relies on the laws of physics rather than on ensuring that successful eavesdropping would require excessive computational effort. Moreover, it is practical with current quantum technology - pilot applications are already commercially available.

Experimental and theoretical research in quantum information science is attracting increasing attention from both academic researchers and industry worldwide. The knowledge that nature can be coherently controlled and manipulated at the quantum level is both a powerful stimulus and one of the greatest challenges facing experimental physics. Going to the moon is straightforward by comparison -- though fortunately the exploration of quantum technology has many staging posts along the way, each of which will yield scientifically and technologically useful results.

In principle we know how to build a quantum computer: we start with simple quantum logic gates and connect them up into quantum networks. A quantum logic gate, like classical gates such as AND and OR, is a very simple computing device that performs one elementary quantum operation, usually on one or two qubits, in a given time. However, the more interacting qubits are involved, the harder it tends to be to engineer the interaction that would display the quantum behaviour. The more components there are, the more likely it is that quantum information will spread outside the quantum computer and be lost into the environment, thus spoiling the computation. This process is called decoherence. Thus the task

is to engineer sub-microscopic systems in which qubits affect each other but not the environment. The good news is that it has been proved that if decoherence-induced errors are small (and satisfy certain other achievable conditions), they can be corrected faster than they occur, even if the error correction machinery itself is error-prone. The requirements for the physical implementation of quantum fault tolerance are, however, very stringent. We can either try to meet them directly by improving technology or go beyond the network model of computation and design new, inherently fault-tolerant, architectures for quantum computation. Both approaches are being pursued.

There are many useful tasks, such as quantum communication or cryptography, which involve only a few consecutive quantum computational steps. In such cases, the unwelcome effects of decoherence can be adequately diminished by improving technology and communication protocols. Here the research focus is on new photon sources, quantum repeaters and new detectors, which will allow long-distance entanglement manipulation and communication at high bit rates, both in optical fibres and free space.

Within a decade, it will be possible to place sources of entangled photons on satellites, which will allow global quantum communication, teleportation and perfectly secure cryptography. Quantum cryptography relies on quantum communication technology but its progress and future impact on secure communication will depend on new protocols such as, for example, quantum--cryptographic authentication and quantum digital signatures.

The next thing on the horizon is a quantum simulator. This is a quantum system in which the interactions between the particles could be engineered to simulate another complex system in an efficient way – a task that is inherently intractable on classical, but not quantum, technology.

Building quantum simulators would allow, for example, the development of new materials, accurate description of chemical compounds and reactions, or a deeper understanding of high temperature superconductivity. The goal is to push the existing quantum technologies, such as optical lattices, to their limits and build quantum simulators within a decade or so.

Last but not least, the search for scalable quantum information technologies goes on. This astonishing field appears to involve practically the whole of physics, and stretches the theoretical and experimental resources of every branch of physics, from quantum optics and atomic physics to solid state devices. It is likely that there will not be a single winner in this search: a number of different technologies will complement each other. Some of them will be more suitable for quantum memories, some of them for quantum processing, some for quantum communication and so on. Therefore, in addition to developing individual technologies, we also need interfaces between these technologies, so that we can transfer a qubit, for example, from a polarized photon to an electron in a quantum dot. The hybrid technologies and architectures for quantum computation, including interfaces between them, are the long-term goals for years to come.

Quantum information technology is a fundamentally new way of harnessing nature and it has potential for truly revolutionary innovation. There is almost daily progress in developing promising technologies for realising quantum information processing with various advantages over its classical counterparts. After all, the best way to predict the future is to create it. From the perspective of the future, it may well be that the real computer age has not yet even begun.

Quantum Information

Anton Zeilinger
Anton Zeilinger is Professor of Physics at the Institute of Experimental Physics of the University of Vienna and at the IQOQI - Institute of Quantum Optics and Quantum Information of the Austrian Academy of Sciences in Vienna. Anton Zeilinger's research focus lies in the fields of quantum communication, which exploits the fundamental insights of quantum physics for new technologies such as quantum teleportation, quantum cryptography and quantum computation, and quantum experiments of macromolecules. His group's most important recent research achievements include the world's first quantum teleportation, the first transmission of real information using entangled-state quantum cryptography and the observation of quantum interference for clusters of seventy carbon atoms. *(The photo is copyright (c) Volker Steger.)*

Quantum physics is a child of the 20th century. In 1900, in "an act of desperation" Max Planck had to invent the idea that light is emitted or absorbed by a glowing body in energy packets. But light itself was still considered to be a continuous wave. In 1905, Albert Einstein created the "revolutionary" idea, as he himself called it, that light itself consists of particles, later called photons. For him, photons were as realistic as particles can be. While Albert Einstein received his Nobel Prize in 1922 for that idea, it took until 1925/26 for the full mathematical quantum theory to be developed by Werner Heisenberg and Erwin Schrödinger. Today, quantum physics is the basis of huge industries. Without quantum physics, we would not be able to understand modern solid state computers and computer chips, which are basically everywhere. For example, a simple mobile phone contains an immensely better computer than those used by scientists thirty years ago. Another application of quantum physics is the laser, where the fundamental theoretical concepts had been invented by Einstein in 1917. Furthermore, all of chemistry can be understood on the basis of Schrödinger's work, and that way quantum physics plays an important role in biological processes.

While over the years, more and more applications of quantum physics emerged, the basic philosophical questions remained. The conceptual challenges had already been pointed out by Albert Einstein at many occasions. At least as early as 1909, Albert Einstein had already pointed out that randomness or chance plays a completely novel role in the quantum world. His famous saying that God does not play dice implies exactly that. Another criticism by Einstein focused on was the question where this randomness of individual quantum events comes from. He believed that a deeper explanation is possible.

The problem is most easily seen in the case of the decay of radioactive atoms. If we consider a large sample of many atoms, we know that half of them will decay within their half-life. But it is completely random at which time which specific atom decays. We are only left with probabilities. That is, we can only predict the probability that a certain atom decays within a

given period of time, but no more. The individual process is completely random. It is fascinating that this way, science has discovered a fundamental limit to the quest of finding a cause for every event. In the case of quantum physics, such a detailed cause cannot be given for the individual event, like the decay of specific radioactive atoms. Many physicists are not happy with this, and would like some deeper explanation. The late Irish physicist John Bell formulated it in the way that physics must some day explain "why events happen".

Another counter-intuitive feature of quantum physics arises when one considers two particles which once interacted. It was first observed by Einstein, Podolsky and Rosen in 1935 that two quantum systems, say, two particles, which interacted at some time in their past and which have become separated later stay connected in a very strange way. Measurement on one of the two particles influences the quantum state of the other one, no matter how far it is away! Erwin Schrödinger called this phenomenon "entanglement" and to him, it was not one but *the* essential characteristic of quantum physics. Theory at that time already predicted that this influence should be instant, that is, with infinite velocity, and thus surpassing Einstein's velocity of light limit. The phenomenon may be explained with a very simple example (**Figure 1**). We consider pairs of quantum dice which are entangled with each other. The phenomenon itself can only be seen in the laboratory with elementary particles or, at most, atoms. But considering dice, one can show the essential features in a most clear way.

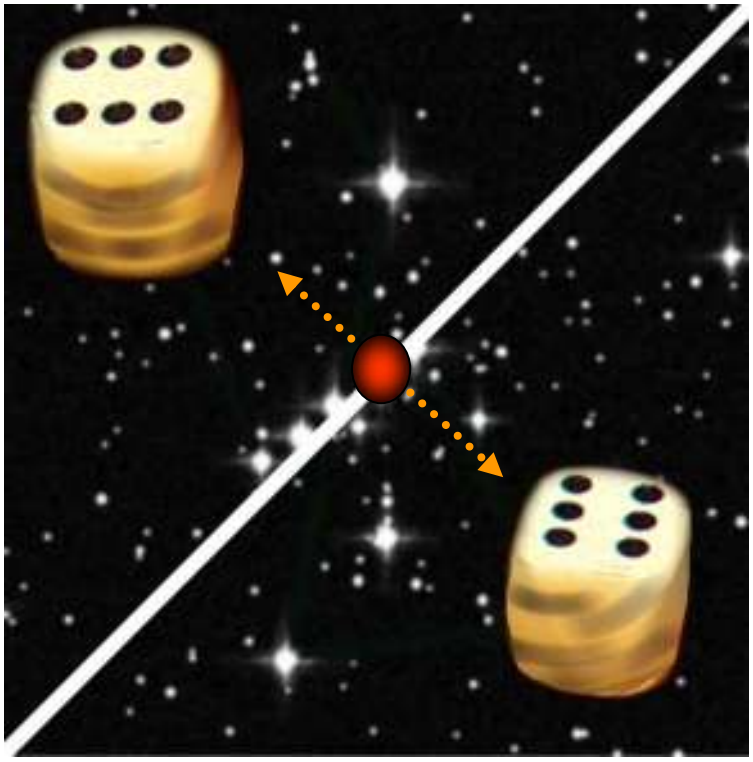


Figure 1

Figure 1: Illustration of quantum entanglement. Two pairs of futuristic quantum dice. They are generated in a common source and, if one die is thrown and shows, as in the figure, say, "6", the other one will also definitely show "6". The next pair thrown will show another number, maybe "3", but always, both pairs are the same.

Such quantum dice are connected in a very interesting way. If you throw one dice, it will show randomly one of the six faces, but then you know definitely that the other one, no matter how far away, will show the same number! One might ask whether such a phenomenon can

be explained in any "natural" way. One possibility would be that the dice are born with some hidden properties in a sense that they are both loaded the same way. The other possibility would be that there is some hidden communication from one dice to the other one. Physicists have very good reasons to believe that neither of the two explanations is possible today anymore, after an increasing body of experimental evidence fully confirms quantum physics. The conceptually interesting situation of quantum entanglement may be summarized as follows: We have (at least) two different experimental stations where we have done measurements on two systems which are entangled with each other. Then, perfect correlations exist between the measurement results on both sides, even as each individual measurement result is completely random. So the conceptual challenge is to explain how two completely random events can be perfectly correlated! Needless to say that quantum theory fully predicts the experimental observations.

The founding fathers of quantum physics, including Niels Bohr, Albert Einstein, Werner Heisenberg and Erwin Schrödinger, were involved in very deep discussions about these conceptual issues already very early in the 1920s and 1930s. But at that time, one had to work with gedanken experiments (thought experiments), since the limited technical abilities did not allow to actually check whether Nature is really as strange as predicted by quantum physics in every detail for individual systems. Yet, it should be remarked that for statistical ensembles, quantum mechanics was very well confirmed. Only technological developments, particularly the development of lasers, made it possible to confirm the predictions of quantum physics also for individual systems like individual particles. Such experiments started in the 1970s, and step by step confirmed more and more of the strange predictions of quantum physics for individual particles. Thus, a series of beautiful experiments was performed, mainly on photons, the particles of light, but also on neutrons and atoms, which really showed us that Nature is indeed as strange as predicted by quantum physics. In essence, we have to live with objective randomness, with entanglement and with the fact that the features of the system observed can in general not be considered to exist before the observation is performed. Yet, most interestingly and surprisingly to essentially all people in the field, these experiments laid the foundations for a new information technology where individual quantum systems are the carriers of information.

In general, information is expressed in bits which may have the value "0" or "1". In computers, bits are represented as the physical states of a certain physical system. For example, they could be pits on a CD. It is obvious that a physical bit can only be either "0" or "1", as long as it is represented by a classical system. Yet, with the possibility of handling individual quantum particles in very great detail, the question arises which new phenomena can occur when we use such quantum systems to represent information and when their propagation and processing is determined by the laws of quantum physics. The first rather interesting situation arises when we consider the qubit or quantum bit. As opposed to a classical bit, a qubit need not be just in the states "0" or "1", but it can also be in what is called a superposition of "0" and "1". What this means is that the value of the bit is not well-defined. If one measures it, one gets randomly the answer "0" or "1", and which specific results one obtains for a specific qubit is objectively random in the way explained above. While one therefore apparently looses certainty when using qubits, the big advantage of a qubit is that superposition can exist in many different ways, and therefore the qubit has the potential to represent more information than a classical bit.

Furthermore, if one has two or more qubits, they can be entangled with each other. Then observation of one qubit influences the quantum states of the others. The correlations between the measurement results on the qubits entangled with each other can be perfectly correlated.

Thus, while the value of an individual qubit might be completely random, measurement on one qubit defines the bit-value of the other one just as in the example with the dice above.

The research in quantum information is a hot topic world-wide today, with many groups exploring different topics of this newly emerging field. The most interesting areas explored are quantum communication, quantum cryptography, quantum teleportation and quantum computation.

Technically most advanced today is quantum cryptography. Cryptography itself is a very wide field with many diverse areas. The general idea is to protect information from being exploited by an unauthorized user. For example, one may have two parties, Alice and Bob, who would like to exchange some secret message and who want to make sure that no eavesdropper is able to tap that information. One possibility to achieve this is that Alice uses a secret key with which she locks the information and Bob, having the same key, unlocks it. Evidently, transporting the key is a potential security hazard. Here, quantum cryptography comes to the rescue, as it allows the exchange of a secret key in such a way that any eavesdropper would immediately be detected. In the case of entangled-state quantum cryptography, Alice and Bob share many pairs of entangled photons on which they perform measurements. The measurement results on each side are completely random, but if the same quantity is measured, they are identical. Thus, Alice and Bob arrive at the same long sequence of random numbers, which they then can utilize to encode a secret message (**Figure 2**). The present status of quantum cryptography is such that first prototypes exist on the market and a large European collaboration, SECOQC, has been started in 2004 with the goal of developing turn-key quantum cryptography systems within a few years.

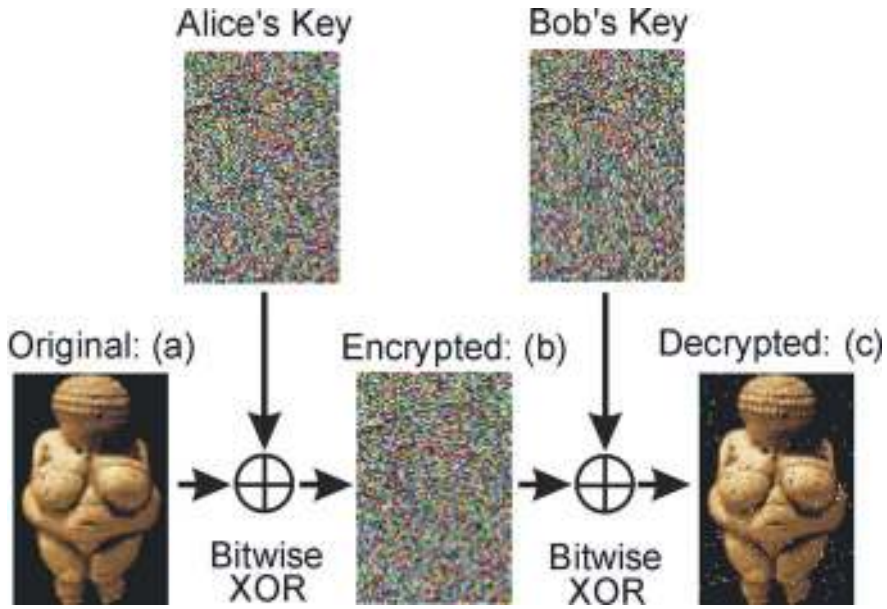


Figure 2

Figure 2: Experimental realization of quantum cryptography. The image of "Venus von Willendorf" is sent from Alice to Bob as the encoded message. Alice's key and Bob's key have been generated using entangled pairs of photons. They each are completely random, but identical. The message is encrypted by a bit-wise combination of the information in the image and the key. Bob can easily decode the information.

Quantum teleportation is *the* application of the fundamental concepts discussed above which triggers most of the fantasy. The basic idea there is to transfer the quantum state of one system over to another, distant one in such a way that the new system becomes identical with the original. Without going into too much detail here, the way it works is a double application of entanglement. If, say, Alice has an original particle whose state she wants to teleport over to Bob, they agree to share an additional pair of entangled particles. Alice gets one from the pair and Bob gets one. Alice then performs a joint measurement on the particle to be teleported and her member of the entangled pair, a very specific measurement which forces the two particles to become entangled. This procedure immediately projects Bob's distant particle into a state which is uniquely related to Alice's original. One might think that this procedure violates Einstein's speed of light limit. Closer inspection shows a very subtle point. Alice's entanglement procedure results in four different possible entangled states, with each of the four states resulting in Bob's particle being in a slightly different state. Alice cannot influence which of the four kinds of entanglement she obtains, the specific result being objectively random just in the way as discussed above. She must tell Bob which result she obtained for him to be able to read out properly the information already carried by his particle. Thus, the objective randomness of the individual quantum event, so much disliked by Einstein, prohibits quantum physics from violating Einstein's own theory of relativity. It would be fascinating to learn what he would have to say about this peculiar conceptual situation. The procedure is called quantum teleportation rather than quantum faxing because by necessity, the original particle looses its own state; it looses its own identity because it becomes entangled. Thus, at Alice's place, a particle disappears with certain features and Bob obtains a particle with identically the same features. Today, teleportation has been demonstrated not only with photons, but also for states of atoms. Yet, its future application will certainly not be an alternative to space travel, this still being just science fiction. Rather, one might very well consider quantum teleportation to be a means of communication between future quantum computers.

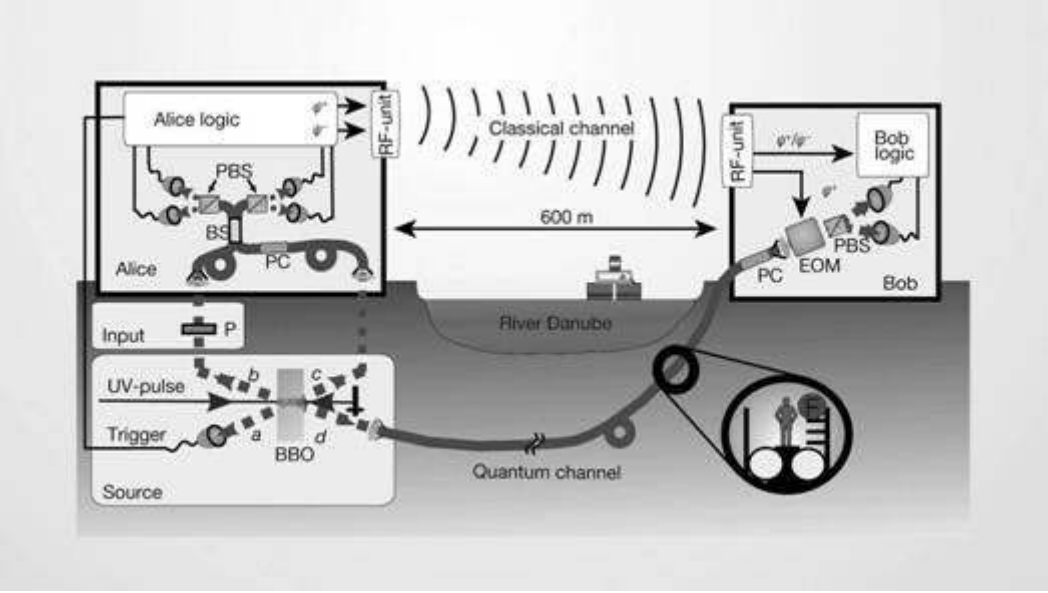


Figure 3

Figure 3: Long-distance quantum teleportation across the River Danube. The quantum channel (fiber *F*) rests in a sewage-pipe tunnel below the river in Vienna, while the classical microwave channel passes above it. A pulsed laser (wavelength, 394 nm; rate, 76 MHz) is

used to pump a β-barium borate (*BBO*) crystal that generates the entangled photon pair *c* and *d* and photons *a* and *b* (wavelength, 788 nm) by spontaneous parametric down-conversion. The state of photon *b* after passage through polarizer *P* is the teleportation input photon; *a* serves as the trigger. Photons *b* and *c* are guided into a single-mode optical-fiber beam splitter (*BS*) connected to polarizing beam splitters (*PBS*) for Bell-state measurement. Polarization rotation in the fibers is corrected by polarization controllers (*PC*) before each run of measurements. The logic electronics identify the Bell state and convey the result through the microwave channel (*RF* unit) to Bob's electro-optic modulator (*EOM*) to transform photon *d* into the original state of input photon *b*.

In a quantum computer, information is represented by many qubits, each of them in some kind of superposition. The resulting state is in general very highly entangled and extremely rich in information. The basic point is that a quantum computer, because of the possibility of superposition of different information inputs, can solve some problems with immensely higher speeds than any existing classical computer. Remarkable among those is factoring of large numbers into their prime factors. This problem is in a different complexity class for quantum computers than for classical computers. For classical computers, the problem is of exponential complexity, meaning that the resources needed, for example the time to factor a specific number, grow exponentially with the size of the input. Therefore, it is easily possible to invent a large enough number whose factoring takes more time than the age of the Universe on any conceivable classical computer. On the other hand, for a quantum computer the problem is of polynomial complexity only. The impossibility of factoring is at the heart of the RSA encryption algorithm widely used today. A quantum computer would immediately break such codes, yet, it may be seen as an irony that quantum physics delivers its own cryptographic method which is safe against such attacks. It actually appears that in the war between code-makers and code-breakers, the code-makers have finally won.

It should be noted that a quantum computer concept is the first one which is fundamentally different from existing computers, because from a conceptual point of view, all classical computers are equivalent. Following Rolf Landauer's dictum "information is physical", representing information in quantum systems resulted in completely new computational procedures.

The experimental realization of a quantum computer requires very detailed control over complex quantum systems consisting of many qubits. These qubits may either be atoms or ions in a trap, some specific quantum states in a semiconductor, the current in a superconductor or even individual photons. All these possibilities are being exploited at present in many different places.

A completely different concept of computation is the one-way quantum computer. There, one starts the quantum computer in a highly complex initial entangled state, a so-called cluster state. Then, the computation does not proceed by operating on the input, but rather by performing measurements one by one on the qubits of the cluster state. The sequence of these measurements defines the specific calculation to be performed. Because of entanglement, measurement on one qubit changes the state of all the others and, if it is done right, a final set of remaining qubits contains the answer to the calculation. This very recent concept is something with no parallel in existing computers. Its best analogy may be seen as the Infinite Library of the Argentinean writer Jorge Luis Borges. That library contains all books ever printed and all books that will ever be published. The cluster state in a quantum computer contains all possible results in a very tricky, highly entangled state. The computation then drives the state towards the desired result of a specific calculation. Actually, the situation is

philosophically even more interesting, as the initial cluster state does not really contain the final answer but just the possibility for it, and the sequence of measurement creates the result. There are many other interesting concepts which have been proposed or tested in the field of quantum information. These include ideas where two parties not trusting each other can make sure that the other one is not cheating, quantum cryptography between more than two parties and many other concepts. Some of these aspects will be addressed in the other articles presented here. The situation today is probably best summarized by the observation that we really witness the emergence of new information technologies, and it is impossible to day exactly what the final technology will look like. Many different concepts are being explored, and some of the steps done in the laboratory are like the first steps of a baby who does not know in which direction to walk, but who is happy to be able to walk at all.

References:

[1] Anton Zeilinger, "Quantum Teleportation", updated version of the 2001 contribution in Scientific American, Scientific American Collection "The Edge of Physics" (2003).

[2] A. Zeilinger, R. A. Bertlmann (Eds.), *Quantum [Un]speakables, From Bell to Quantum Information.* Springer (2002).

[3] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, Hugo Zbinden, "Quantum cryptography", Rev. Mod. Phys. **74**, 145 (2002).

[4] C. Macchiavello, G.M. Palma, A. Zeilinger (Eds.), *Quantum Computation and Quantum Information Theory. Reprint Volume with Introductory Notes for ISI TMR Network School.* World Scientific Publishing (2001).

[5] Dik Bouwmeester, Artur Ekert, Anton Zeilinger, *The Physics of Quantum Information. Quantum Cryptography, Quantum Teleportation, Quantum Computation.* Springer (2000).

Projects funded by the European Commission and related to the work in this article:

QuComm
Long Distance Photonic Quantum Communication
Start date: 01/01/2000
End date: 30/04/2004
Project web site http://www.imit.kth.se/QEO/qucomm/
Contact Person: Prof. A. Karlsson, KTH, Sweden
IST-1999-10033, Fifth Framework Programme

RAMBOQ
pRobabilistic gAtes Making Binary Optical Quanta
Start date: 01/01/2003
End date: 31/12/2005
Project web site http://www.ramboq.net
Contact Person: Prof. J.G. Rarity, U. Bristol
IST-2001-38864, Fifth Framework Programme

ERA-Pilot QIST
CA Co-ordination Action-Network „Structuring the European Research Area within Quantum Information Science and Technology "
Sixth Framework Programme

QAP: FP6 Integrated Project in the process of negotiations
Qubit Applications
Contact person: Dr. Jason Twamley, NUI Maynooth, Ireland, Jason.Twamley@may.ie

QUACS
IHP-Network "Quantum Complex Systems: Entanglement and Decoherence from Nano- to Macro-Scales", Project Reference HPRN-CT-2002-00309
Fifth Framework Programme

Cold Quantum Gases
IHP-Network „Preparations and Applications of Quantum-Degenerate Cold Atomic / Molecular Gases“,Project Reference HPRN-2000-00125
Fifth Framework Programme

QUIPROCONE
IST-Network „ Quantum Information Processing and Communications Network of Excellence“,Project Reference IST-1999-29064
Fifth Framework Programme

TMR-Network “Perfect Crystal Neutron Optics”, Project Reference FMRX960057
Fourth Framework Programme

Marie-Curie-Fellowship “Multi-dimensional entangled states based on the orbital angular momentum of light”, Dr. Gabriel Molina-Terriza, Project Reference HPMF-CT-2002-02087
Fifth Framework Programme

Marie-Curie-Fellowship “Quantum interference and structure formation with large molecules”, Dr. Björn Brezger, Project Reference HPMF-CT-2000-00797
Fifth Framework Programme

TMR-Network “FUNDAMENTALS AND APPLICATIONS of COHERENT MATTER WAVE SOURCES USING LASER COOLED ATOMS”, Project Reference FMRX960002
Fourth Framework Programme

TMR-Network “The Physics of Quantum Information”, Project Reference FMRX960087
Fourth Framework Programme (Coordinator)

Contact information of the authors of this article:

Anton Zeilinger
Institut für Experimentalphysik
Universität Wien
Boltzmanngasse 5
1090 Wien
Austria
Phone: +43 1 4277 51201
Fax: +43 1 4277 9512
e-mail: zeilinger-office@exp.univie.ac.at
http://www.quantum.univie.ac.at/zeilinger/

Quantum entanglement

Maciej Lewenstein
Maciej Lewenstein has obtained his degree in Physics from Warsaw University. From 1980 he worked at the Center for Theoretical Physics of the Polish Academy of Sciences. He received his doctoral degree in 1983 at the University of Essen and habilitation in 1986 in Warsaw. He became a full Professor in Poland in 1993. In 1995 he joined “Service de Photones, Atomes et Molecules” of CEA in Saclay. In 1998 he became a full professor and a head of the quantum optics theory group at the University of Hannover. In 2005 he started a new theory group at the “Insitut de Ciencias Fotoniques” in Barcelona. His research interests include: quantum optics, quantum information and statistical physics.

Chiara Macchiavello
Chiara Macchiavello finished her degree in Physics in 1991 and her PhD in 1995 at the University of Pavia. She held a post-doctoral for two years at the University of Oxford. Since 1998 she has been an Assistant Professor at the University of Pavia. Her research interests include quantum information processing and quantum optics.

Dagmar Bruss
Since 2003 Dagmar Bruss is a professor at the Institute of Theoretical Physics at the University of Duesseldorf, Germany. Her research interests include the foundations of quantum information theory, classification of entanglement and quantum optical implementations of quantum computation.

Abstract

Entanglement is a fundamental resource in quantum information theory. It allows performing new kinds of communication, such as quantum teleportation and quantum dense coding. It is an essential ingredient in some quantum cryptographic protocols and in quantum algorithms. We give a brief overview of the concept of entanglement in quantum mechanics, and discuss the major results and open problems related to the recent scientific progress in this field.

Introduction

Entanglement is a property of the states of quantum systems that are composed of many parties, nowadays frequently called Alice, Bob, Charles etc. Entanglement **expresses particularly strong correlations between these parties,** persistent even in the case of large separations among the parties, and going beyond simple intuition.

Historically, the concept of entanglement goes back to the famous **Einstein-Podolski-Rosen (EPR) "paradox"**. Einstein, who discovered relativity theory and the modern meaning of causality, was never really happy with quantum mechanics. In his opinion every reasonable physical theory should exhibit a so called local realism.

Suppose that we consider two particles, one of which is sent to Alice and one to Bob, and we perform independent local measurements of "reasonable" physical observables on these particles. Of course, the results might be correlated, because the particles come from the same source. But Einstein wanted really to restrict the correlations for "reasonable" physical observables to the ones that result from statistical distributions of some hidden (i.e. unknown to us and not controlled by us) variables that characterize the source of the particles. Since quantum mechanics did not seem to produce correlations consistent with a local hidden variable (LHV) model, Einstein concluded that quantum mechanics is not a complete theory. Erwin Schrödinger, in answer to Einstein's doubts, introduced in 1935 the term "Verschränkung" (in English "entanglement") in order to describe these particularly strong quantum mechanical correlations.

Entanglement was since then a subject of intense discussions among experts in the foundations of quantum mechanics and philosophers of science (and not only science). It took, however, nearly 30 years until John Bell was able to set the framework for experimental investigations on the question of local realism. Bell formulated his famous inequalities, which have to be fulfilled in any multiparty system described by a LHV model. Alain Aspect and coworkers in Paris have demonstrated in their seminal experiment in 1981 that **quantum mechanical states violate these inequalities**. Recent very precise experiments of Anton Zeilinger's group in Vienna confirmed fully Aspect's demonstrations. **All these experiments indicate the correctness of quantum mechanics**, and despite various loopholes, they exclude the possibility of LHV models describing properly the physics of the considered systems.

Entanglement has become again the subject of cover pages news in the 90's, when quantum information was born. It was very quickly realized that **entanglement is one of the most important resources for quantum information processing**. Entanglement is a necessary ingredient for quantum cryptography, quantum teleportation, quantum dense

coding, and if not necessary, then at least a much desired ingredient for quantum computing.

At the same time the theory of entanglement is related to some of the open questions of mathematics, or more precisely linear algebra and functional analysis. A solution of the entanglement problem could help to characterize the so called positive linear maps, i.e. linear transformations of positive definite operators (or physically speaking quantum mechanical density matrices, see below) into positive definite operators.

Entanglement of pure states

In quantum mechanics (QM) a state of a quantum system corresponds to a vector |Psi> in some vector space, called **Hilbert space**. Such states are called **pure states**. One of the most important properties of QM is that **linear superpositions** of state-vectors are also legitimate state-vectors. **This superposition principle lies at the heart of the matter-wave dualism and of quantum interference phenomena.**

Entanglement is also a result of superposition, but in the composite space of the involved parties. Let us for the moment focus on two parties, Alice and Bob. It is then easy to define states which are not entangled. Such states are product states of the form **$|\Phi\rangle = |a\rangle|b\rangle$,** i.e. Alice has at her disposal |a>, while Bob has |b>. Product states obviously carry no correlations between Alice and Bob. **Entangled pure states may be now defined as those which are superpositions of at least two product states, such as**

$|\Phi\rangle = \alpha_1|a_1\rangle|b_1\rangle + \alpha_2|a_2\rangle|b_2\rangle$ + etc.

but cannot be written as a single product state in any other basis. All entangled pure states contain strong quantum mechanical correlations, and do not admit LHV models.

Entanglement of mixed states and the separability problem

Verify whether a given state-vector is a product state or not is a relatively easy task. In practice, however, we often either do not have full information about the system, or are not able to prepare a desired state perfectly. In effect in everyday situations we deal practically always with statistical mixtures of pure states. There exists a very convenient way to represent such mixtures as so called density operators, or matrices. A density matrix rho corresponding to a pure state-vector |Φ> is a projector onto this state. More general density matrices can be represented as sums of projectors onto pure state-vectors weighted by the corresponding probabilities.

The definition of entangled mixed states for composite systems has been formulated by Reinhard Werner from Braunschweig in 1989. In fact, this definition determines which states are not entangled. Non-entangled states, called separable states, are mixtures of pure product states, i.e. convex sums of projectors onto product vectors:

$$\rho = \Sigma_i \, \mathbf{p_i|a_i\rangle|b_i\rangle\langle a_i|\langle b_i|}, \qquad (*)$$

where $0 \leq p_i \leq 1$ are probabilities, i.e. $\Sigma_i\ p_i = 1$. The physical interpretation of this definition is simple: a separable state can be prepared by Alice and Bob by using local operations and classical communication. Checking whether a given state is separable or not is a notoriously difficult task, since one has to check whether the decomposition (*) exists or not. This difficult problem is known under the name of "separability or entanglement problem", and has been a subject of intensive studies in the recent years.

Simple entanglement criteria

The difficulty of the separability problem comes from the fact that rho admits in general an infinite number of decompositions into a mixture of some states, and one has to check whether among them there exists at least one of the form (*). One of the most powerful necessary conditions for separability has been found by one of the fathers of quantum information, the late Asher Peres. Peres (Technion, Haifa) observed that since Alice and Bob may prepare separable states using local operations, Alice may safely reverse the time arrow in her system, which will change the state, but will not produce something unphysical. In general, such a partial time reversal is not a physical operation, and can transform a density operator (which is positive definite) into an operator that is no more positive definite. In fact this is what happens with all pure entangled states. Mathematically speaking partial time reversal corresponds to partial transposition of the density matrix (only on Alice's side). We arrive in this way at the Peres criterion: ***If a state*** ρ ***is separable then its partial transposition has to be positive definite.*** This criterion is usually called positive partial transpose condition, or shortly PPT condition. Amazingly, the PPT condition is not only necessary for separability, but it is also a sufficient condition for low dimensional systems such as two qubits (dimension 2x2)and a system composed of one qubit and one qutrit (dimension 2x3). In higher dimensions, starting from 2x4 and 3x3, this is no longer true: there exist entangled states with positive partial transpose, which are called PPT entangled states.

There exist several other necessary or sufficient separability criteria which have been established and frequently discussed in recent years. For example, states that are close to the completely chaotic state (whose density operator is equal to the normalized identity) are necessarily separable. There exist also other criteria that employ entropic inequalities, uncertainty relations, or an appropriate reordering of the density matrix (so called realignment criterion) etc. There exists, however, no general simple operational criterion of separability that would work in systems of arbitrary dimension.

Entanglement witnesses

The set of all states P is obviously compact and convex. If ρ_1 and ρ_2 are legitimate states, so is their convex mixture. The set of separable states S is also compact and convex (see **Figure 1**). From the theory of convex sets and Hahn-Banach theorem we conclude that for any entangled state there exists a hyperplane in the space of operators separating rho from S. Such a hyperplane defines uniquely a Hermitian operator W (observable) which has the following properties: The expectation value of W on all separable states, $\langle W \rangle \geq 0$, whereas its expectation value on ρ is negative, i.e. $\langle W \rangle_\rho < 0$.

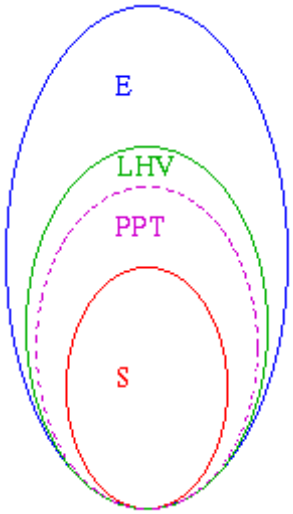


Figure 1

Such an observable is for obvious reasons called entanglement witness, since it "detects" the entanglement of ρ. Every entangled state has its witnesses; the problem obviously is to find appropriate witnesses for a given state. To find out whether a given state is separable one should check whether its expectation value is non-negative for all witnesses. Obviously this is a necessary and sufficient separability criterion, but unfortunately it is not operational, in the sense that there is no simple procedure to test for all witnesses.

Nevertheless, witnesses provide a very useful tool to study entanglement, especially if one has some knowledge about the state in question. They provide a sufficient entanglement condition, and may be obviously optimized (see **Figure 2**) by shifting the hyperplane in a parallel way towards S.

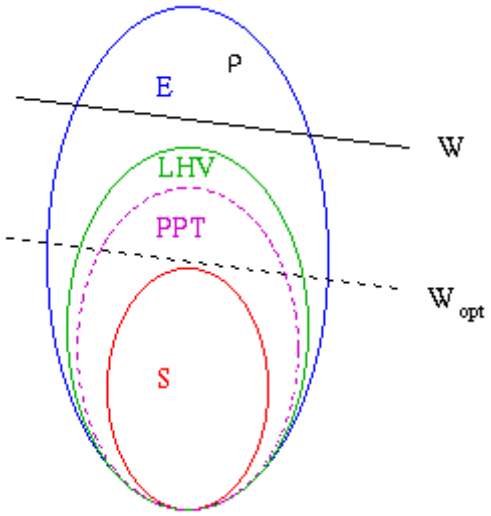


Figure 2

Bell inequalities

After introducing the concept of separability and entanglement for mixed states, it is legitimate to ask what is the relation of mixed state entanglement and the existence of a LHV model, which requires that the state cannot violate any of the Bell-like inequalities. Let us discuss an example of such inequalities, the so called Clauser-Horne-Shimony-Holt inequality for two qubits. Let us assume that Alice and Bob measure two binary observables each, namely A_1, A_2, and B_1, B_2. The observables are random variables taking the values +1 or – 1, correlated possibly through some dependence on local hidden variables. It is easy to see that in the classical world, if $B_1 + B_2$ is zero, then $B_1 - B_2$ is either +2 or –2, and vice versa. Therefore if we define $s = A_1(B_1 + B_2) + A_2(B_1 - B_2)$, we obtain that $2 \geq s \geq -2$. This inequality holds also after averaging over various realizations. On the other hand, it can be shown that by taking suitable sets of observables for Alice and Bob we can find pure and even mixed quantum states that violate this inequality.

Are Bell-like inequalities similar in this respect to witnesses, i.e. for a given entangled state can one always find a Bell-like inequality that "detects" it? The answer to this question is no, and has been already given by R. Werner in 1989. Even for two qubits there exist entangled states that admit an LHV model, i.e. cannot violate any Bell-like inequality.

This observation indicates already that there is more structure in the "eggs" of **Figure 1** and **Figure 2**. Separable states are evidently inside the PPT egg, according to the Peres condition. They admit an LHV model, i.e. they are also inside the LHV egg. But what about PPT entangled states? Do they violate some Bell-like inequality? Peres has formulated a conjecture that this not the case, and there is a lot of evidence that this conjecture is correct, although a rigorous proof is still missing.

The distillability problem and bound entanglement

Above we have classified quantum states according to the property of being either separable or entangled. An alternative classification approach is based on the possibility of distilling the entanglement of a given state. In a distillation protocol the entanglement of a given state is increased by performing local operations and classical communication on a set of identically prepared copies. In this way one obtains fewer, but "more entangled", copies. This kind of technique was originally proposed in 1996 by Bennett and coworkers in the context of quantum teleportation, in order to achieve faithful transmission of quantum states over noisy channels. It also has applications in quantum cryptography as a method for quantum privacy amplification in entanglement based protocols in the presence of noise, as pointed out by David Deutsch and coworkers from Oxford.

The distillability problem poses the question whether a given quantum state can be distilled or not. A separable state can never be distilled because the average entanglement of a set of states cannot be increased by local operations. Furthermore, the positivity of the partial transpose ensures that no distillation is possible. Thus, a given PPT entangled state is not distillable, and is therefore called bound entangled. There may

even exist undistillable entangled states which do not have the PPT property. However, this conjecture is not proved at the moment.

The first example of a PPT entangled state has been found by Pawel Horodecki from Gdansk in 1997. These states are so called edge states, which means that they cannot be written as a mixture of a separable state and a PPT entangled state. Particularly simple families of states have been suggested by Charles Bennett and coworkers at IBM, New York. They have found the so called unextendible product bases (UPB), i.e. sets of orthogonal product state-vectors, with the property that the space orthogonal to this set does not contain any product vector. It turns out that the projector onto this space is a PPT state, which obviously has to be entangled since it does not contain any product vector in its range (note that all state-vectors in the decomposition of a separable state ρ into a mixture of product states belong automatically to the range of ρ).

The existence of bound entanglement is a mysterious invention of Nature. It is an interesting question to ask whether bound entanglement is a useful resource to perform quantum information processing tasks. It was shown so far that this is not the case for communication protocols such as quantum teleportation and quantum dense coding (i.e. a protocol that allows to enhance the transmission of classical information, using entanglement). However, surprisingly, it is possible to distill a secret key in quantum cryptography, starting from certain bound entangled states.

Entanglement detection

As discussed above, entanglement is a precious resource in quantum information processing. Typically in a real world experiment noise is always present and it leads to a decrease of entanglement in general. Thus, it is of fundamental interest for experimental applications to be able to test the entanglement properties of the generated states. A traditional method to this aim is represented by the Bell inequalities, a violation of which indicates the presence of entanglement. However, as mentioned above, not every entangled state violates a Bell inequality. So, not all entangled states can be detected by using this method. Another possibility is to perform complete state tomography, which allows determining all the elements of the density matrix. This is a useful method to get a complete knowledge of the density operator of a quantum system, but to detect entanglement it is an expensive process as it requires an unnecessary large number of measurements. If one has certain knowledge about the state the most appropriate technique is the measurement of the witness observable, which can be achieved by few local measurements. A negative expectation value clearly indicates the presence of entanglement.

All these methods have been successfully implemented in various experiments. Recently another method for the detection of entanglement was suggested based on the physical approximation of the partial transpose. It remains a challenge to implement this idea in the laboratory because it requires the implementation of non local measurements.

Entanglement measures

When classifying a quantum state as being entangled, a natural question is to **quantify the amount of entanglement** it contains. For pure quantum states there exists a well defined entanglement measure, namely the von Neumann entropy of the density operator of a subsystem of the composite state. For mixed states the situation is more complicated. There are several different possibilities to define an entanglement measure. The so called entanglement cost describes the amount of entanglement one needs in order to generate a given state. An alternative measure is the entanglement of formation, which is a more abstract definition. A further possibility to quantify entanglement is given by the minimum distance to separable states. Finally, motivated by physical applications, one can introduce the distillable entanglement which quantifies the extractable amount of entanglement.

Unfortunately all of these quantities are very difficult to compute in general. For example, in order to determine the entanglement of formation one has to find the decomposition of the state that leads to the minimum average von Neumann entropy of a subsystem and this is a very challenging task. So far a complete analytical formula for the entanglement of formation only exists for composite systems of two qubits.

Entanglement in multipartite systems

So far, we have restricted ourselves to the case of composite systems with two subsystems, so called bipartite systems. When considering more than two parties, i.e multipartite systems, the situation becomes much more complex. For example, for the most simple tripartite case of three qubits, a pure state can be either completely separable, or biseparable (i.e. one of the three parties is not entangled with the other two), or genuinely entangled among all three parties. The latter class again consists of inequivalent subclasses, the so called GHZ and W states. This concept can be generalized to mixed states. For more than three parties it is easy to imagine that the number of subclasses grows fast.

In recent years there has been much progress in the creation of multipartite entangled states in the laboratory. The existence of genuine multipartite entanglement has also been demonstrated experimentally by using the concept of witness operators.

Even if the full classification of multipartite entanglement is a formidable task, certain classes of states, the so called graph states, have been completely characterized and shown to be useful both for quantum computational and quantum error correction protocols. Moreover, a deeper understanding of entanglement has proved to be very fruitful in connection with statistical properties of physical systems. All of these problems are discussed in more details in other sections of this publication.

References

[1] Einstein, P. Podolsky and N. Rosen, Phys. Rev. **47**, 777 (1935)
[2] J.S. Bell, Physics **1**, 195 (1964)
[3] P. Horodecki, Phys. Lett. A **232**, 333 (1997)
[4] M. Lewenstein et al., J. Mod. Opt. **47**, 2481 (2000)
[5] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996)

[6] E. Schrödinger, Naturwissenschaften **23**, 807 (1935)
[7] R.F. Werner, Phys. Rev. A **40**, 4277 (1989)

Contact information of the author of this article

Maciej Lewenstein
Institut de Ciènces Fotòniques (ICFO)
C/Jordi Girona 29, Nexus 29
08034 Barcelona
Spain
Email: maciej.lewenstein@icfo.es

Chiara Macchiavello
Istituto Nazionale di Fisicadella Materia, Unita' di Pavia
Dipartimento di Fisica "A. Volta"
via Bassi 6
I-27100 Pavia
Italy
Email: chiara@unipv.it

Prof. Dr. Dagmar Bruss
Inst. fuer Theoretische Physik III
Heinrich-Heine-Universitaet Duesseldorf
Universitaetsstr. 1, Geb. 25.32
D-40225 Duesseldorf,
Germany
Email: bruss@thphy.uni-duesseldorf.de

Various faces of quantum entanglement

Ryszard Horodecki
Ryszard Horodecki is a full professor of theoretical physics at the Institute of Theoretical Physics and Astrophysics of the University of Gdansk in Poland. He is a Member of the Council of the Polish Laboratory of Physics for Information Processing and the editor of the journal "Open Systems and Information Dynamics". Since 1999 he is leading the quantum information activities at Gdańsk University and participating in a number of European funded IST projects (EQUIP, QPRODIS, RESQ), as well as numerous national (KBN) projects. In 2004 his group received the Wojciech Rubinowicz Prize by the Polish Physical Society for their achievements in quantum information theory. This includes pioneering research on quantum entanglement, in particular identifying the so called "bound entanglement phenomenon".

Abstract
We present one of the greatest intellectual adventures: the discovery and investigation of **a new resource of Nature**. It is responsible for its subtle organization on fundamental level. The resource called quantum entanglement is extraordinarily sensitive to environmental perturbations. It is the "fuel" for many fascinating effects including quantum teleportation and quantum cryptography and is **a key element of quantum computer theory**. We outline, in rather popular form, the methods of detection of entanglement and various faces of its intrinsic structure, which still offers new phenomena not only on the quantum but sometimes also on the classical level of physical reality.

Introduction
The fact that Nature can be described, and even more, that the description allows to predict results of experiments is highly nontrivial. Nature might have been malicious, and it might not exhibit any regularity while being asked questions in laboratories. Fortunately it is not the case. Subsequent theories have been experimentally verified to cover more and more phenomena.

The best description of the micro world that we currently have at our disposal is Quantum Mechanics. It was discovered at the beginning of the previous century and turned out to be encoded in a highly nontrivial way, by means of a rather abstract, complex mathematical model called the **Hilbert space**. In this context one can ask why and for what reason Nature requires an abstract description in terms of a Hilbert space. The first, and at the same time, crucial step to

resolve this problem was done as early as in 1935 **by Einstein, Podolsky and Rosen (EPR)** on one hand and by **Schroedinger** on the other hand. They revealed two different faces – a correlation one and an information one - of the peculiar organization of composite quantum systems, which was called by Schroedinger "entanglement". The latter phenomenon is strictly connected to the fundamental notion of the quantum description of nature: **quantum state**. What is a quantum state? The simplest answer is the following**: it is the available (to us) information about a given quantum system.** When we have maximal information, the system is said to be in a pure state ψ. In reality, even if at some point we have maximal information about a system, as a result of uncontrolled interaction of the system with the environment, we lose part of this information. The system is then said to have passed into a mixed state ρ.

By investigating states of quantum composite systems, Schroedinger discovered that such a system can be in a pure state, even if its subsystems are not in any definite pure state. Physically such states emerge from the interaction between the subsystems, which brings the initial product state, describing independent systems into a joint state exhibiting quantum correlation. An entangled state can arise as a result of the decay of an unstable system into subsystems e.g., it can be the decay of a pion π_0 into an electron and a positron. The formal origin of entangled states lies in the fact that the quantum formalism uses a tensor description of composite systems, and in the superposition principle.

Description of entanglement: formal definition

To illustrate the above mathematical "recipe" for entangled state, consider a simple, but paradigmatic example of a composite system of two spin-particles, such as the above mentioned positron and electron pair emerging from pion decay. The tensor product allows us to think about two cases: the positron has spin up and the electron spin down, which we denote by |↑>p |↓>e and the inverse, |↑>e |↓>p, meaning that the electron has spin up, while the positron - spin down. Now, the superposition principle tells us that if we superpose those two cases, i.e. to create a quantum alternative, we also obtain a legitimate state, called singlet state in this particular case:

|Ψp e> = 1/√2 (|↑>p |↓>e - |↑>e |↓>p) ≠ |Ψp> |Ψe>.

It is crucial here, that the state cannot be represented as a product of states |Ψp> and |Ψe> describing individual systems. In general, it is said that **a state is entangled, whenever it cannot be represented in a product form, i.e. |ΨAB> ≠ |ΨA> |ΨB>.**

In the laboratory, as a result of uncontrolled disturbance, we deal with mixed states rather than with pure ones. Up to the late 80's it was not clear to what extent and in what sense a mixed state can be entangled. Therefore the definition of separable (i.e. not entangled) state proposed by Werner (1989) as a generalization of the above definition for pure states, was an important step. To understand quantum entanglement more deeply, let us consider in more detail its correlation aspects discovered by Einstein, Podolsky and Rosen.

The "correlation" face of quantum entanglement: local realism and entanglement.

EPR noted that quantum formalism predicts very strong correlation between distant particles, which interacted in the past with one another. Strictly speaking they analyzed correlations between such properties of the particles as position and momentum. EPR assumed locality, tried to exploit weird correlations of singlet state to prove that the properties must be "elements of reality", in other words, that they "sit" on the system, and therefore quantum mechanics is incomplete, since it does not predict the properties, offering only probability distribution over the properties. At that time, physicists did not have enough reasons to believe that **the quantum description of Nature is "almost" universal, i.e. it describes correctly all phenomena excluding gravity.** Thus entanglement was treated as a metaphysical phenomenon which will never go into the laboratory. Fortunately in 1964 John Bell formalized the concept of local realism by using the old idea of hidden variables. Soon after the discovery of quantum mechanics, appearing to be a radically different description of Nature form the classical one, people, including EPR, believed that quantum probabilities emerging from quantum states are the result of our incomplete knowledge of the microworld. They hoped that the laws of physics are deterministic on a deeper level and can be described by some deterministic variables, at present unknown to us, called therefore **"hidden variables".** The basic problem was to confront such a deterministic (i.e. classical in spirit) description and the quantum description with experiments in the case of subsystems (particles) emerging from the decay of a joint system (e.g. the mentioned pion decay). How can one do it? Let us imagine, a source that sends in opposite directions two particles and two observers, who sit in distant labs, and measure some dychotomic observables i.e. the ones, that have only two values +1 or -1 (an example is the spin or photon polarization). Each observer measures two such observables (Alice chooses a and a', Bob b and b'). Having a list of the outcomes, one can easily calculate the correlation between the outcome of the observables. For a given pair of observables, they are simply the averages of the products of the outcomes i.e. $\langle a,b\rangle$, $\langle a,b'\rangle$, $\langle a',b\rangle$, $\langle a',b'\rangle$. Let us note that out of these averages, we can build an average of a new observable called Bell observable B=ab+ab'+a'b-a'b'. If we assume that for every particle, the observables have well defined value, we can easily verify, that the absolute value of the Bell observable cannot exceed 2 (e.g. for a=1, a'=1, b=1, b'=1, B=2) which we write as follows:

$$\mathbf{|\langle ab+a'b+ab'-a'b'\rangle| \equiv |\langle B\rangle| \leq 2 \quad \text{or equivalently} \quad |\langle 2 - B\rangle| \geq 0}$$

where the symbol $\langle\rangle$ means average taken over distributions of hidden variables, that determine values of the observables for particular particles. The inequality must be valid even though we do not know anything about the probability distribution or about the variables. In this way we have derived a particular Bell-type inequality found by Clauser, Horne, Shimony and Holt (CHSH). The remarkable feature of Bell's result is that the mean value of observable can be (i) verified in laboratory independently of any theory and (ii) computed in any theory.

It turns out that if we compute mean value of Bell observable according to quantum rules, so that Bell observable becomes an operator B shows mean value is evaluated in some quantum state, then CHSH inequality can be violated for some choices of observables a,b,a',b', i.e. surprisingly we can have $\langle B\rangle_\rho > 2$. In 1982 A. Aspect J. Dalibard and P.Grangier performed convincing experiment that confirmed violation of Bell's inequalities. Since that time, many new Bell's

inequalities have been derived and tested, and all of them confirmed validity of quantum predictions. Thus, putting aside notorious problem of "loopholes" (e.g. not all particles are detected) experimental violation of Bell's inequalities means that assumptions of local realism contradicts experiment. Thus one of basic manifestations of entanglement are so strong correlations that cannot be described by any local realistic theory.

Detection of entanglement - entanglement witnesses

Is this the only implication of Bell's inequality? At the beginning of 90-ties many new questions arose connected with violation of Bell's inequalities. Bell's observable looks quite mysterious, and it is reasonable to ask about its physical sense. Furthermore, one can ask about its deeper connection with entanglement. The top of the iceberg was uncovered by Werner (1989) and Popescu (1995). Werner not only gave accurate definition of separable mixed states (these mixed states that are not entangled) but also noted that there exist entangled states that similarly as separable states admit hidden variable model, hence do not violate Bell's inequalities. Popescu showed that having system in such a state, by means of local operations one can get a new state whose entanglement can be detected by Bell's "witness"! This was the advent of entanglement manipulation era.

At that time physicists wondered not only what entanglement is, but also what is it useful for. First explicit application entanglement was cryptographic protocol by Ekert 1991 based on entangled states and Bell inequalities. Soon after several peculiar effects was discovered, being ferment for a new domain - quantum information theory as a specific fusion of quantum mechanics, Shannon information theory and computer science. The effects are: quantum dense coding, quantum teleportation, entanglement swapping, and reducing communication complexity. Essentially all the effects were based on entanglement and have been verified in beautiful experiments. It turned out that entanglement is new, much more subtle resource than energy, extremely fragile with respect to disturbance caused by environment. As a result pure entangled states undergo fast degradation, i.e. become mixed state with weaker entanglement. Therefore from the point of view of practical applications, a significant step was the discovery of so called distillation protocol (Bennett et al. 1996) allowing reversing, in a sense, degradation process. Namely, out of n weakly entangled pairs, by use of local operations and classical communication (LOCC) one can obtain a smaller amount of m pairs, $m<n$ of nearly maximally entangled pairs - two qubit singlet states being units of entanglement. When the protocol is optimal, the rate $m/n=D$ is simply measure of entanglement contained in noisy state ρ and is called distillable entanglement.

In this situation, there appeared important questions: i) How to check theoretically that a given state is entangled? ii) Is it possible to detect entanglement directly in lab? The answer to these questions has been provided in 1996. It turned out that two-component system ρAB is entangled if and only if there exists observable quantity W that mean value of this observable in the state is negative i.e. $\langle W \rangle \rho < 0$, while for all separable states, the mean value is always nonnegative $\langle W \rangle \rho sep \geq 0$. Terhal first analyzed in detail the above criterion in the context of Bell inequalities and called W entanglement witness. There are two important implications. First, if we got from somebody the state written on piece of paper, then to check if it is entangled or not, we have to decide, if there exists witness that violates the above inequality. It is not always easy,

though physicists found various methods to deal with this problem. Second, expecting some state in lab, we can find a witness for it, and check if the state we have actually produced is entangled or not. Recently, the concept was improved by introducing so called nonlinear entanglement witnesses, which can detect very weak entanglement. In 2003 De Martini group in Rome has performed first detection of entanglement witness. Quite recently in cooperation with Hannover group entanglement witnesses have been constructed and measured for multiparticle states in Max Planck Institute, in München.

The concept of entanglement witness may prove useful for information processing in quantum systems, where permanent control of quality of entanglement is required. In the context of entanglement witness it is also natural is there something in common between violation of the latter inequality on <W> and violation of CHSH inequality by entangled states. Comparing the inequalities we find that the observable 2-B in CHSH inequality is nothing more than a particular entanglement witness. It turns out that Bell, constructing his inequality has built first entanglement witness! In some way however Bell's witness is different from some "regular" entanglement witnesses. It detects not only entanglement, but also violation of local realism. In this context there was a significant result (Brükner et al. 2004) showing that each Bell witness detects states which can be used as a resource for reducing communication complexity of certain distributed computation task. Therefore both from practical as well as conceptual point of view, characterizing of all Bell witnesses is more than desired.

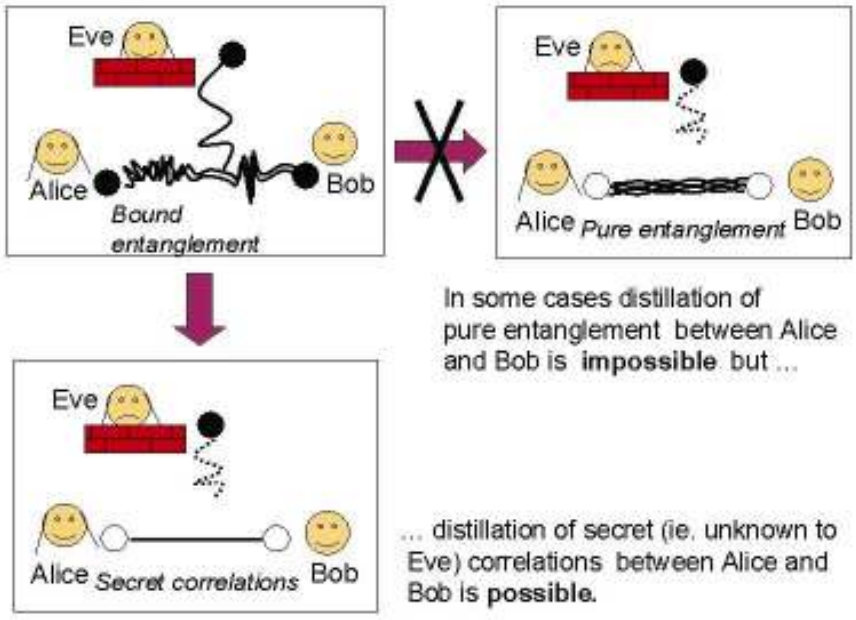


Figure 1

Positive maps as entanglement detectors: bound entanglement

It turns out that all known Bell type observables are weak witnesses in the sense that they do not detect many entangled states. Even the entanglement witnesses, though needed for experiment, theoretically are not the best tools to detect entanglement. However, to any witness there corresponds some "positive" map on states. It turns out that positive maps are much stronger detectors of entanglement. Example of such map is transpose of one of the subsystems A or B of compound system AB in state ρ_{AB} (partial transpose). Such operation can be interpreted as time inversion on a subsystem. Often it happens that such map destroys state in the sense that it looses positivity, hence also its probabilistic interpretation (probabilities must be positive!). However if the state was separable, then after such map it is still a legitimate state. Thus, the map can be used to "detect" entanglement of a given state on paper. Partial transpose is very strong entanglement test discovered by Asher Peres (1996). Though there exist some states which cannot be detected by Peres test. Existence of such states was at the beginning just an interesting mathematical news, without physical significance. The situation changed dramatically, when the question was asked whether all states containing noisy entanglement are distillable i.e. whether by means of local operations and classical communication Alice and Bob in their distant labs can draw pure entanglement, e.g. singlets which, as we have mentioned, are resource for newly discovered quantum protocols.

It was quite surprising, when it turned out that entangled states undetectable by Peres criterion are non-distillable. Pure entanglement used to build the state by LOCC is totally lost, i.e. it would never be regained. From physical point of view, it means that there is a sort of irreversibility, different from that in thermodynamics, where we have reversible Carnot cycle. In this context very interesting research is being carried out towards two directions (i) "thermodynamics of entanglement" being a (not direct) formal analogue of statistical thermodynamics (ii) the implications for the latter following from entanglement via famous Landauer principle.

As one can see, structure of "noisy" entanglement is not homogenous. We have at least two types of entanglement: bound (non-distillable) and free (distillable) one. For two-component systems bound entanglement is very passive, and it is not easy to make it to be useful, as compared with multipartite bound entangled states. Yet, in 1999 an effect of activation was discovered, where entanglement was "pumped" from bound entangled state to a system containing small amount of free entanglement. For some time, it was thought that one couldn't use bound entanglement as a resource for drawing secret cryptographic key. It was quite surprising, when it turned out that there are bound entangled states from which one can obtain cryptographic key (see **Figure 1**). So there is a hope that this weak kind of entanglement can become of practical importance.

When bound entanglement was discovered, nobody imagined that it might have a connection with classical cryptography. However, in 2000 Gisin and Wolf conjectured existence of "bound information" in classical cryptography, basing on connections between entanglement theory and classical cryptography. In 2003 such "bound information" has been discovered by Acin, Masannes and Cirac. Its existence puts interesting fundamental constraints for classical cryptography. It seems to be one of first case, where quantum physics allowed predicting some phenomena in classical information theory.

The "information" face of entanglement

As mentioned in the Introduction, Schrödinger discovered another face of entanglement, which discloses a deep difference in quantum and classical description of the relation between a part and wholeness of the compound system. What struck Schrödinger was the contradiction between classical relation concerning total information H(A,B) about compound system and information content of its subsystems H(A), H(B) and the corresponding relation implied by quantum description. Schrödinger's first observation can be formalised in terms of classical information theory, leading to the following entropic inequalities: $H(A,B) > H(A)$ or $H(A,B) - H(A) > 0$. Similar inequalities hold for subsystem B. They say that the maximal Shannon information about subsystems give us total knowledge about system. The above inequalities can be viewed as an analogy to the Bell inequalities having nothing common with local realism except for that they need the classical probability theory. But do states which satisfy the above inequalities exist? It turns out, that like as Bell inequalities the entropic ones are satisfied by all separable states. Then we have entropic inequalities:

$$\mathbf{S(\rho A,B) \geq S(\rho A) \text{ or } S(\rho A,B) - S(\rho A) \geq 0}$$

where $S(\rho A,B)$, $S(\rho A)$ are some quantum entropies of the system and subsystem respectively. In general, entropic inequalities can be violated by entangled states. Two important conclusions follow from that: firstly the inequalities are detectors of entanglement and for bipartite states they are sometimes stronger than Bell witnesses. The second observation express what Schrödinger noticed, that is a quantum relation between the order in the system and the order in the subsystems: total information about compound quantum system do not provides total information about its subsystems! In this context direct experimental violation of the entropic inequalities will be not only a great technological challenge but also experimental confirmation highly no intuitive relation order – disorder in quantum world. Recently another connection between the entropic uncertainty relations and entanglement which provide separability criteria has been founded.

But is this all what we can read from information face of entanglement? It is remarkable, that the later says about something very important in the context fundamental differences between classical and quantum information. Indeed, what determines about violation or not entropic inequalities are differences $I = S(\rho A,B) - S(\rho A)$ and $I' = S(\rho A,B) - S(\rho B)$ between the total entropy of the system and entropies of its subsystems. Dependently on whether a state violates the entropic inequalities or not, the differences I (I') can be negative or positive and zero. Then, the negative value of I(I') is a manifestation of non-classical features of information being a consequence of entanglement contained in the state. Indeed, it has been first shown for some two-qubit systems (1996) and recently generalised to arbitrary ones the states having negative value of I (I') can be used to quantum teleportation and that from such states a pure entanglement (i.e. singlets) can be distilled. The quantity $Ic = - I$ was introduced (1996) in the different context and called coherent information. The research continued from 1998 succeed in 2004 showed that coherent information constitutes a central quantity in quantum communication. Namely the most important operational quantity in this domain - capacity of the channel defined as a amount faithfully sent qubits (per one use channel) can be expressed by coherent information.

Conclusions

The nature of quantum entanglement is highly non intuitive. For instance the Theory of Special Relativity does not admit the existence of superluminal signals. However quantum entanglement gets through it very well. Though it "generates" instant correlations between events in distant labs, at the same time it makes it impossible to control them. Hence they cannot be used for superluminal communication. Another peculiar feature of quantum entanglement is its "monogamy". It means that if we have two systems A and B, which are maximally entangled, then neither of them can be entangled with any other system C. It can be shown that entanglement monogamy reflects the principle that quantum states cannot be cloned. But the most important issue is that entanglement constitutes a real resource, which allows to perform tasks that cannot be performed with standard resources like classical information or energy. As we mentioned before, this resource is extraordinarily sensitive to destruction by the influence of the environment. **It is one of the greatest challenges of quantum technology to obtain optimal ways of distillation of entanglement, which is the basic "fuel" for a quantum computer.** Finally one can state, that quantum entanglement is not only a useful resource, but also its existence is one of the most fascinating features of Nature. It can not be excluded that entanglement will provide us with other surprises in future.

List of terms and acronyms

Qubit: unit of quantum information being a counterpart of bit form classical information. It can be represented physically as two-level system for example spin-1/2 particle.

Quantum computer: computing machine (Feynman, 1982; Deutsh 1985) based directly on laws of quantum physics, which would use quantum information processing to solve efficiently problems difficult for classical computers.

Classical (quantum) entropy: measure of information contained in a given classical (quantum) object.

References

[1] G. Alber, T. Beth, M. Horodecki, P. Horodecki, R. Horodecki, H. Weinfurter, R. Werner and A. Zeilinger, *Quantum Information,* Springer-Verlag, 2001
[2] A. Peres, *Phys. Rev. Lett.* **77**, 1413 (1996)
[3] R .Horodecki, M. Horodecki, *Phys. Rev. A*, **54,** 1838 (1996)
[4] B. Schumacher, M.A. Nielsen, *Phys. Rev. A*, **54**, 2629 (1966)
[5] D. Bruss, J. Math. Phys. **43,** 4237 (2002)
[6] K. Audenaert, M. B. Plenio, and J. Eisert, *Phys. Rev. Lett.* **90**, 027901 (2003)
[7] B. M. Terhal, M. M. Wolf and A.C. Doherty, *Phys. Today*, **56**, 46 (2003)
[8] O. Guehne, M. Lewenstein, *Phys. Rev. A*, **70**, 022316 (2004)

Project funded by the European Commission and relation to the work in his article:
EQUIP
Entanglement in Quantum Information Processing and Communication
Start date: 01/01/2000
End date: 31/12/2002
Project web site: http://www.equip.qipc.org/

Contact Person: Martin Wilkens, U Potsdam, martin.wilkens@physik.uni-potsdam.de

RESQ
Resources for Quantum Information
Start date: 01/01/2003
End date: 31/12/2005
Project web site: http://www.ulb.ac.be/project/RESQ/
Contact Person: Serge Massar, Université Libre de Bruxelles, smassar@ulb.ac.be

QUPRODIS
Quantum Properties of Distributed Systems
Start date: 01/01/2003
End date: 31/12/2005
Project web site: http://www.quprodis.org/
Contact Person: Wilkens, U Potsdam, martin.wilkens@physik.uni-potsdam.de

Contact information of the author of this article
Ryszard Horodecki
Faculty of Mathematics Physics and Computer Science
Institute of Theoretical Physics and Astrophysics
ul. Wita Stwosza 57
80-952 Gdańsk
Poland
Email: fizrh@univ.gda.pl

Quantum entanglement – multi-photon sources

Gerd Leuchs
Gerd Leuchs is a professor at the Max Planck Research Group, Institute of Optics, Information and Photonics, University of Erlangen-Nürnberg in Germany. His research interest include classical and quantum optics and quantum information. He is a member of EPS, DPG, DGaO, OSA, IoP, AAAS. He is in the consortium of the following EU-funded IST projects: ACQUIRE, QUICOV (coordination), SECOQC and COVAQIAL and in several national projects: Quantum Cryptography, DFG-SPP Quantum Information Processing (coordination). He is also Nanomach AG (director) Heisenberg-Fellow of DFG, Fellow of OSA and IoP, JILA Visiting Fellow.

Harald Weinfurter
Herald Weinfurter is a professor at the Physics Department of the University of Munich and at the Max-Planck-Institute for Quantum Optics in Garching. His research is in experimental physics, namely on the foundations of quantum mechanics and quantum information. He is a member of EPS, ÖPG, OSA. He is in the consortium of the following EU-funded IST projects: EQCSPOT, QuComm, RAMBOQ, SECOQC and in several national projects: Quantum Cryptography, DFG-SPP Quantum Information Processing, DFG-SFB Solid State Quantum Information Processing. He has received the following professional awards: START-prize (Austria), Philip-Morris-award, Descartes-Prize (EU).

Abstract
Entanglement lies in the heart of almost all methods of quantum communication and computation. Efficient and economical generation of entangled states of light are of crucial importance for the success of future quantum communication applications. This article introduces the experimental methods to produce entangled light modes both in the discrete and continuous variable regime.

Introduction
Optical quantum technologies are beginning to enter domains having been dominated by classical optics. There are two different scenarios. In the first one a classical technology is pushed until one reaches a point where the operation is limited by quantum effects. Long distance optical communication is in such a situation with state of the art optical amplifiers working essentially at a quantum limited performance. Here technologies borrowed from quantum optics such as all optical signal regeneration are beginning to help [1]. In this context optical fiber solitons play a special role [2]**. In the**

second scenario a quantum effect allows for novel technological applications such as quantum communication and there most prominently quantum cryptography. Data security on optical transmission lines are an example for a subject of fast growing relevance. **The basis for these innovations is the ability to control and manipulate quantum states of light.**

In quantum optics there are two different domains. One domain deals essentially with single or few photons or photon pairs. In the other domain the light field is highly excited and one deals typically with millions of photons at a time. The first section discusses multi-photon entanglement where the excitation per mode is a few photons and detectors can still discriminate between different photon numbers. For single photon sources which likewise belong to the first domain see the relevant article in this publication. Applications of photon-pair entanglement are entanglement based quantum cryptography and quantum teleportation. More recently, multi-photon entanglement and linear optics quantum logic were used in first experiments on entanglement purification and decoherence free communication and in novel multiparty quantum communication protocols. Section 2 addresses the generation of soliton light pulses which belong to the second domain. The special stability of solitons is discussed below and is the reason why solitons are well described by one phase and one amplitude value. Amplitude and phase are quantum variables which can vary continuously over a wide range. Advances in quantum soliton technologies have relevance for both of the scenarios mentioned above [1,3]. The generation of quantum states of solitons will be discussed in this chapter and is important for applications in the continuous variable domain dealing with intense light pulses. Quantum solitons have been used to implement quantum communication protocols such as teleportation, entanglement swapping, optimal cloning of Gaussian states, and quantum erasing and solitons are relevant for quantum key distribution with intense light beams.

Multi-photon Entanglement (few photons)

At the few photon level entanglement between photons cannot yet be generated by coupling them via some interaction. However, there are several emission processes, in particular parametric down conversion, where, due to the conservation of energy and of linear or angular momentum, the properties of two emitted photons become entangled. Introducing a linear coupling between modes of two or more such sources of entangled photons leads to multi-photon entanglement. For the required linear coupling one may use a beam splitter such as in **Figure 1b**. An alternative is to use multiple emission events, where in the scheme shown in **Figure 1a**, a single pump pulse produces two pairs of entangled photons [4].

Historically, entanglement between spatially separated quanta was first observed in measurements of the polarization correlation between γ-quanta emitted from electron-positron annihilation. Later on a series of experiments was performed mostly with polarization entangled photons from a 2-photon cascade emission from Calcium atoms. Both methods suffer from low yield in spite of the significant technical requirements. Now, cascade emissions from quantum dots are investigated for their potential to efficiently generate entangled photon pairs. So far, these experiments did not succeed most likely due to asymmetries in the shape of the dots. But this might change soon. Currently the best method to efficiently generate entangled pairs of photons is offered by parametric down-conversion (PDC).

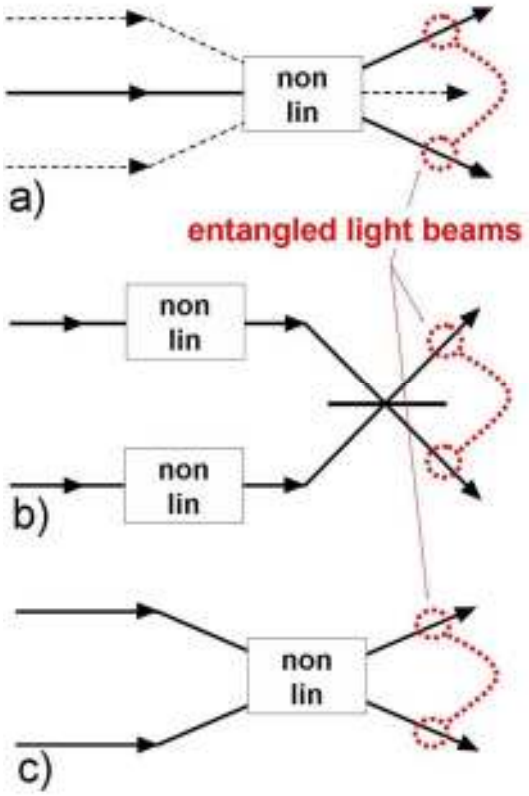


Figure 1: Figure 1b shows the work horse for creating continuous variable quantum entanglement. The two single mode nonlinear interactions both create squeezed light which is made to interfere at a beam splitter such that both outputs carry equal mean intensity. The resulting entanglement has been classified using for example criteria based on Einstein, Podolsky and Rosen and it has been used in a number of continuous variable quantum protocols.

When light propagates through an optically nonlinear medium with second-order non-linearity $\chi^{(2)}$, the conversion of a light quantum from the incident pump field into a pair of photons in the "idler" and "signal" modes can occur (see the scheme in **Figure 1a**). In principle this can be seen as the inverse of the frequency doubling process in nonlinear optics. Energy- and momentum-conservation can give rise to entanglement in various degrees of freedom, like position-momentum- and time-energy-entanglement. The relative orientations of pump-beam direction and polarization, and the optical axis of the crystal determine the actual direction of the emission of a certain wave length. We distinguish two possible alignment types as shown in **Figure 2**: For type-I down-conversion, the pump is, for example, extraordinarily polarized and idler and signal beams have the same (ordinary) polarization. The different colours are emitted into cones centred on the pump beam. In type-II down-conversion the pump is extraordinarily polarized and in order to fulfil the momentum conservation inside the crystal (phase-matching) the two down-converted photons have orthogonal polarization, offering the possibility to generate polarization entangled photon pairs.

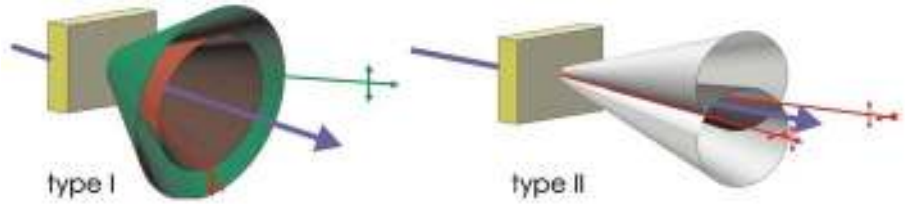


Figure 2

One can distinguish two ways to observe entanglement: in the first one, by selecting detection events, one can chose a sub-ensemble of possible outcomes, which exhibits the non-classical features of entangled states. Particularly for observing entanglement between more than two photons this is the method of choice. As a second way, true entangled photon pairs can be generated directly for various degrees of freedom. Several methods to obtain momentum-entangled pairs have been experimentally demonstrated, but are extremely difficult to handle experimentally due to the huge requirements on the stability of the whole setup. Any phase change, i.e. a change in the path lengths by as little as 10nm is devastating for the experiment. The source of time-energy entangled photon pairs partially shares these problems and, to avoid detection selection, would require fast optical switches. As it delivers the state which is most robust when transporting it over large distances through optical fibers, it is the best choice for long-range quantum communication. To obtain this type of entanglement it suffices to employ single frequency pump lasers or coherent pump pulses, and consequently to use unbalanced Mach-Zehnder interferometers for state preparation and analysis [5].

Any stability requirements are significantly relaxed when using polarization entanglement communicated via free-space quantum channels. In type-II down-conversion the down-converted photons are emitted into two cones, one ordinary polarized, the other extraordinary polarized. For proper alignment of the optical axis of the nonlinear crystal, the two cones intersect along two lines (see **Figure 2**). Along the two directions ("1" and "2"), where the cones overlap, one obtains the entangled state. Using two extra birefringent elements, one can easily produce any of the four orthogonal Bell-states.

A typical experiment uses a pump beam from a single-mode argon ion laser. With the advent of blue laser diodes the system will become much more economical and ideally suited for quantum communication applications. **Figure 3** shows the picture of a diode pumped source. Optics focuses the pump beam into a 2 mm BBO-crystal (beta-Barium-Borate). After compensating birefringence the entangled photons are collected with single mode fibers which enable transport of the quantum state over moderate distances. For quantum channels of more than 100 m length, free-space telescope links are advisable. At the end of the channels, the entanglement is analyzed using polarization analyzers consisting of two-channel polarizers (polarizing beam splitters) preceded by a rotatable half wave plate. The detectors are cooled silicon avalanche photo-diodes operated in the Geiger mode. Coincidence rates are recorded as a function of the polarizer settings at the two observers. One now obtains routinely a coincidence fringe visibility of more than 97% with 100 observed coincidences per miliwatt pump power and per milimeter crystal length.

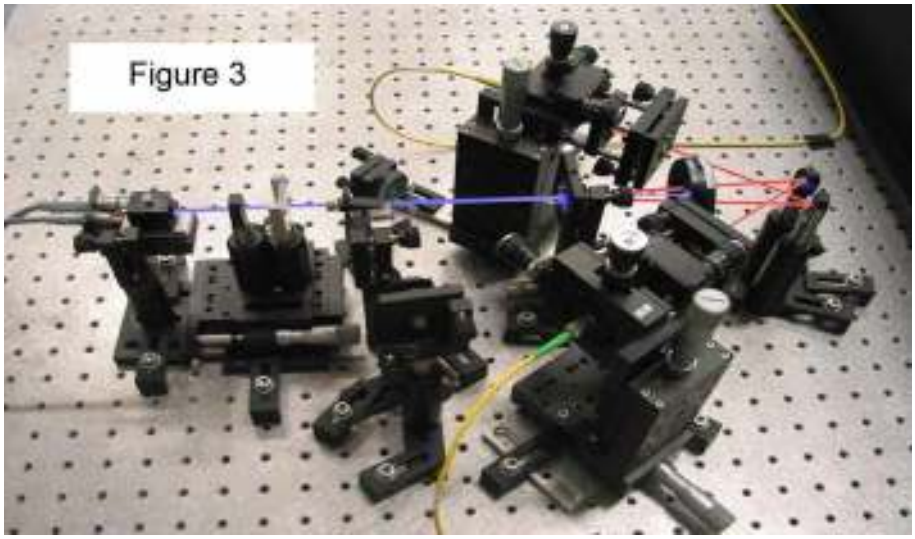


Figure 3

A highly efficient multi-mode source becomes possible when using sandwiched type I crystals, though only for thin crystals. Significant improvement will be possible with periodically poled crystals, as they exhibit significantly higher optical nonlinearity. Together with waveguide structures first demonstrations proved the advantages. In particular for time-bin entanglement these crystals will enable a step forward to efficient quantum communication applications.

For the observation of entanglement between more than two photons pulsed lasers have to be used. The higher peak power and the short pulse duration relative to the coherence length of the observed photons enable the interferometric combination of several pairs of photons to obtain the desired multi-photon entanglement. Currently, various states with three and four photons are under investigation and already employed in first quantum communication protocols like secret sharing and quantum telecloning. Various ideas are tested to increase the number of communication partners to an even higher number.

Entanglement of intense light beams (many photons)

The generation of intense quantum entangled light fields requires a nonlinear interaction between light and matter which is not yet available for individual photons. The alternative, a laser source of correlated photons is also possible. There are two different approaches towards entangled field modes (see **Figure 1 b and c**). One uses an inter-mode interaction between two different modes of the light field mediated by a nonlinear optical medium. The other one uses an intra-mode nonlinear interaction within this mode which changes the quantum uncertainty of the continuous variables describing this mode. With optical fiber solitons both venues are possible. In both diagrams **Figure 1b** and c different field modes may be injected into the input ports on the left hand side. If one for example considers the lower diagram with one input port carrying an intense laser beam and the other one a vacuum field i.e. no excitation then the entanglement generation scheme is very close to parametric down conversion used in the discrete variable case.

Classical Solitons

Before discussing the quantum properties of optical solitons in more detail, the behaviour of classical solitons are reviewed. Optical solitons are light pulses with special behaviour requiring a nonlinear interaction with the material in which they propagate [3]. Without any

nonlinear interaction optical pulses disperse that is they broaden when travelling along in an optical fiber as indicated by the broken black line shape at the fiber output in **Figure 4**. The line shapes in the Figure refer to the variation of the intensity with time. Depending on the sign of the dispersion of glass at the wavelength under study, either the long or the short wavelength components will be faster than the others leading to a frequency chirp of the pulse at the fiber output. Now any material has some optical nonlinearity although often fairly small. If for a given pulse energy the pulse intensity is kept high by spatial confinement the effective nonlinearity can be sufficiently high. In the case of glass the nonlinearity is the optical Kerr effect which in a simple picture leads to a contribution to the refractive index which is proportional to the light intensity. If the intensity varies such as in an optical pulse there will be a resulting nonlinear phase shift varying proportional to the intensity. The phase varying in time over the pulse duration is equivalent to a local frequency change. The bottom line is that the Kerr effect producing new frequency components will also lead to a frequency chirp of the pulse. If the two effects, i.e. dispersion and Kerr effect, lead to chirps of different sign but same magnitude then both effects cancel each other and the pulse will propagate without change: this is what is called soliton. The remarkable stability of soliton pulses in a medium where different wavelengths travel with different speeds can be visualised following the sketch in **Figure 5** which goes back to Lin Mollenauer. He was the first to observe optical fiber solitons. The upper sketch in the Figure shows dispersion, slow wavelength fall behind the fast ones. If, however, the propagation condition of the pulse depends on the intensity of the pulse dispersion may be compensated as indicated in the lower sketch in **Figure 5**. Running on a soft mat the high performance runners have to run up hill which slows them down, whereas the slower ones have the advantage of running down hill. If the system is well balanced the group members stay together. In standard optical fibers this condition can be met at wavelengths larger than 1.3 micrometers. The soliton keeps the pulse together and thus helps to maintain spatial confinement of the pulse energy also in the direction of propagation. This helps to maintain an effective nonlinear coefficient large enough for the observation of quantum effects. In the experimental studies it helps that solitons are dynamically stable solutions of the nonlinear differential equation describing propagation.

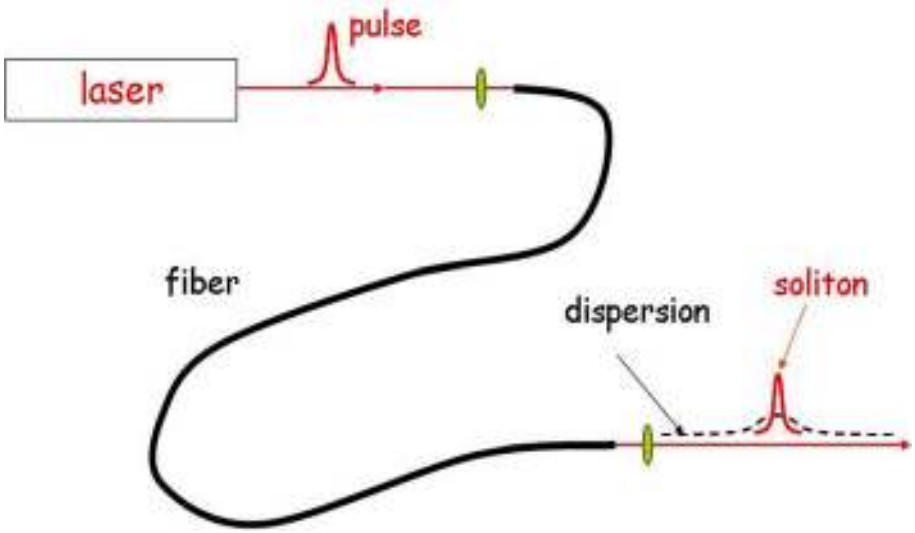


Figure 4

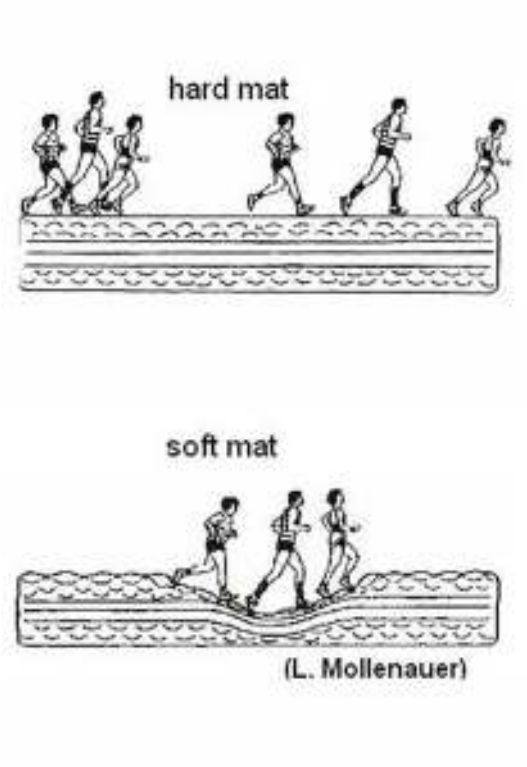


Figure 5

Optical quantum solitons

Solitons with an amplitude and a phase, both as well defined simultaneously as allowed for by Heisenberg's uncertainty relation, still have a corresponding uncertainty. In the phase space coordinate system in **Figure 6** a classical electric field is represented by a point, the arrow from the origin to this point representing the amplitude and its angle with respect to the X-axis representing the phase. With equal uncertainties in all directions a coherent soliton is described by a circular contour line in phase space. The fact that the coherent quantum soliton has an uncertainty in the amplitude variable leads to a dynamical evolution of the soliton. The different amplitudes experience a different nonlinear phase shift due to the Kerr effect as indicated in **Figure 6** [3]. This results in a squeezed contour line in phase space. Various techniques are available to rotate this squeezed region of uncertainty such that eventually one will have reached a reduced quantum uncertainty of the amplitude. The experimentally achieved reduction of the amplitude variance below shot noise is typically 0.3.

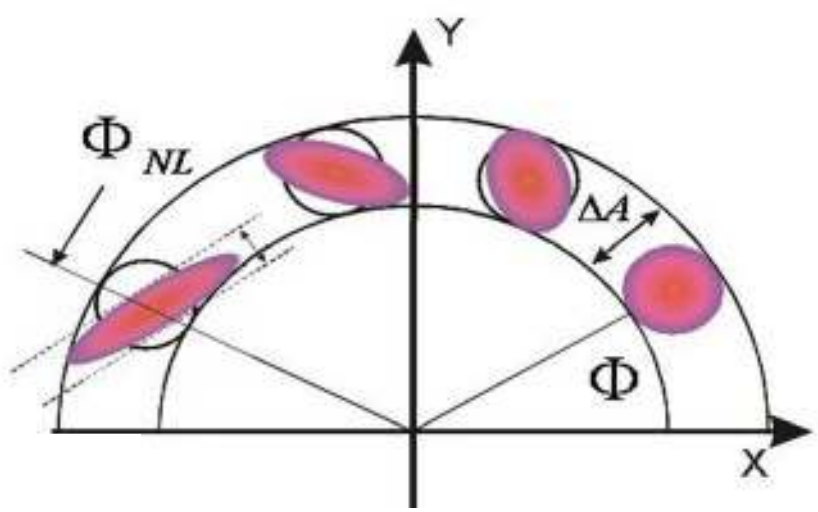


Figure 6

There is a worthwhile alternative to the continuous quantum variables amplitude and phase. These are the Stokes parameters which can be most efficiently represented using Poincaré's sphere (see **Figure 7**) [6]. The coordinate S_1, e.g., represents the difference of the number of photons in the two basis modes describing the polarization. The similarity to the Bloch sphere of discrete variables namely of qubits is apparent. In the case of continuous variables discussed here the excitation i.e. the number of quanta per mode is much higher and as a result the state occupies a much smaller volume than in the discrete, dichotomic case. The small sphere in the figure shows a coherent polarization mode and the elongated cigar a squeezed polarization mode. Experimentally, polarization variables offer the great advantage that they can be detected by amplitude measuring detectors only, and their use in the continuous quantum variable regime is growing. Squeezed quantum variables are the resource one needs when generating entanglement according to the scheme in **Figure 1b**.

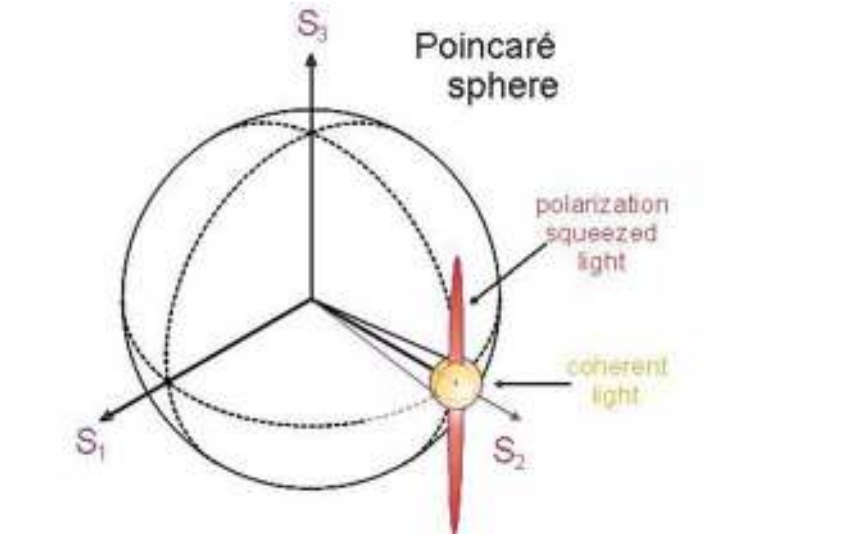


Figure 7

Generation of multi-photon entanglement with solitons

Entanglement is the basic building block for many quantum information experiments with continuous variables [3, 7]. One way two generate entanglement in standard optical

communication fibers is to launch two pulses, having different propagation speed inside the fiber, into the fiber and to let them interact inside the fiber (see **Figure 1c**). It is of course advantageous if both pulses are solitons. Again one may think of runners to visualize the interaction such as for the one-dimensional case displayed in **Figure 5**. Now there are two groups of runners running on a soft mat heading towards a collision with each other. Often there is a flaw in such simple pictures, and this also holds in the picture used here. Unlike runners, photons may run through each other with-out devastating collisions. Through the dents in the mat the two pulses interact. It is a unique property of solitons that they emerge from the interaction without having changed their shape, but their position and phase is shifted by the "collision" and they experience a transient spectral shift during the collision as shown in **Figure 8**. (The Figure shows the temporal variation of the spectrum of the two pulses – from let to right: frequency; from front to back: time). If the middle of the collision is placed at the end of the fiber the spectral shifts are frozen and the emerging pulses are entangled also in energy and spectral shift.

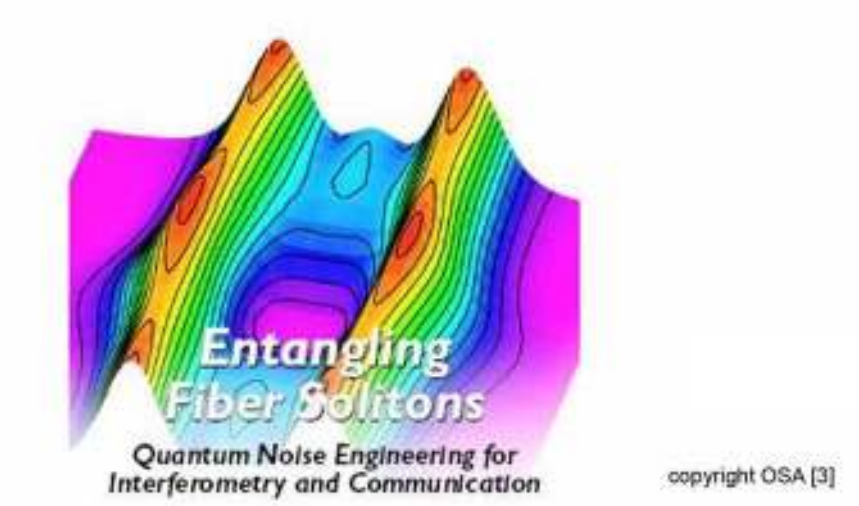


Figure 8

Conclusions

One of the startling features of quantum theory is the quantum uncertainty inherent to quantum systems allowing in general only for probabilistic predictions. Based on the concept of quantum entanglement, on the other hand, one can make conditional predictions which are definite. In the case of two entangled modes of a light field the measurement of one variable, discrete or continuous, of one of the modes may well have a large uncertainty but based on this first measurement one can predict with precision the outcome of a second measurement on the entangled variable on the other light mode. **Entangled systems are thus the basis for quantum information** and in this article we discussed the generation of entangled light modes both in the discrete and continuous variable regime. **Quantum entanglement of light fields plays a central role in almost every quantum communication protocol. It is, therefore, a basic ingredient to quantum engineering applications.** Nonlinear phenomena like parametric down-conversion and solitons are the ideal tools to generate various types of multi-photon entangled states and entanglement between bright light beams.

List of terms and acronyms

PDC: parametric down conversion
BBO: beta Barium Borate crystal
Soliton: pulse with dynamically stable shape in a dispersive environment

References

[1] I.P. Kaminow and T. Li (eds.), "**Optical Fiber Telecommunications IV-A: Components** (Optics and Photonics)", Academic Press (2002); and I.P. Kaminow and T. Li (eds.), "**Optical Fiber Telecommunications IV-B: Systems and Impairments** (Optics and Photonics), Academic Press (2002)

[2] G.P. Agrawal, "**Nonlinear Fiber Optics**", Academic Press, San Diego, 2001Qu

[3] G. Leuchs and N. Korolkova, "**Quantum Noise Engineering for Interferometry and Communication**", Optics and Photonics News, February 2002, p. 64

[4] M. Bourennane, M. Eibl, S. Gaertner, N. Kiesel, Ch. Kurtsiefer, M. Zukowski, and H. Weinfurter, "**Multiphoton entanglement**", in 'Quantum Information Processing', G. Leuchs and T. Beth (eds.), VCH-Wiley, p. 292-299 (2002)

[5] W. Tittel and G. Weihs, "**Photonic Entanglement for Fundamental Tests and Quantum Communication**", *Quant. Inf. Comput.* **1,** 3-56 (2001)

[6] N. Korolkova, "**Quantum polarization for continuous variable information processing**", in "Quantum Information Processing", Th. Beth and G.Leuchs (eds.), 2nd edition, Wiley-VCH, Weinheim, 2005

[7] S.L. Braunstein and A.K. Pati (eds.), "**Quantum Information with Continuous Variables**", Kluwer Academic Publishers, Dordrecht, 2003

Projects funded by the European Commission and related to the work in this article:

ACQUIRE
Advanced quantum information research
Start date: 01/01/1996
End date: 30/06/1999
Project web site: http://www.acquire.uni-hd.de/
Contact person: Elisabeth Giacobino, ENS Laboratoire Kastler-Brossel, Paris

QUICOV
Quantum information with continuous variables
Start date: 01-Jan-2000
End date: 30-Jun-2003
Project web site: http://kerr.physik.uni-erlangen.de/quicov/
Contact Person: Gerd Leuchs

COVAQIAL
Continuous variable quantum information with atoms and light
Start date: 01/09/2004
End date: 31/08/2007
Project web site: http://www.ulb.ac.be/project/covaqial/
Contact Person: Prof. Nicolas Cerf, Ecole Polytechnique, Université Libre de Bruxelles, ncerf@ulb.ac.be

EQCSPOT
European Quantum Cryptography and Single Photon Optical Technologies
Start date: 01/11/1998
End date: 31/10/2000
Project web site http://www.cordis.lu/esprit/src/28139.htm
Contact Person: Prof. J.G. Rarity, U. Bristol, john.rarity@bristol.ac.uk

QuComm
Long Distance Photonic Quantum Communication
Start date: 01/01/2000
End date: 30/04/2004
Project web site http://www.imit.kth.se/QEO/qucomm/
Contact Person: Prof. A. Karlsson, KTH, Sweden, Andkar@imit.kth.se

RAMBOQ
pRobabilistic gAtes Making Binary Optical Quanta
Start date: 01/01/2003
End date: 31/12/2005
Project web site http://www.ramboq.net
Contact Person: Prof. J.G. Rarity, U. Bristol, john.rarity@bristol.ac.uk

SECOQC
Development of a Global Network for Secure Communication based on Quantum Cryptography
Start date: 01/05/2004
End date: 30/04/2008
Project web site http://www.secoqc.net/
Contact Person: Christian Monyk, ARC Seibersdorf, Austria, christian.monyk@arcs.ac.at

Projects funded by National initiatives or organizations and related to the work in this article:

QIV
Quanten-Informationsverarbeitung
Start date: 01/04/1999
End date: 31/03/2005
Project web site: www.quiv.de
Contact Person: G. Leuchs

Contact information of the authors of this article:

Gerd Leuchs
Institute of Optics, Information and Photonics
University of Erlangen-Nürnberg
Günther-Scharowsky.Strasse 1
D91058 Erlangen
Germany
Email: Leuchs@physik.uni-erlangen.de
Web page: http://kerr.physik.uni-erlangen.de

Harald Weinfurter
Department of Physics
Universtity of Munich
Schellingstr. 4
D80799 Munich
Germany
Email: Harald.weinfurter@physik.uni-muenchen.de
Web page: http://xqp.physik.uni-muenchen.de

New perspectives in multiphoton entanglement and hyper-entanglement manipulations

Francesco De Martini
Francesco De Martini is a professor of Quantum Optics and Quantum Information at the Physics Department of Università “La Sapienza”, Roma, Italy. He is the author of several books and of more than 200 scientific articles related to various modern aspects of nonlinear-optics and nonlinear spectroscopy, free-electron lasers, quantum optics, optical microcavity and microlasers. In the last years his most important scientific contributions concern the fields of fundamental processes and quantum information: quantum entanglement, quantum state teleportation, quantum nonlocality, quantum cloning and Schroedinger-cat states. He was the chairman of the 5th European QIPC Workshop (Rome, 2004). He is the coordinator of the EU-funded IST project ATESIT and of other nationally funded research projects in the field of quantum information. On 2004 he was awarded the Luigi Tartufari Prize from Accademia Nazionale dei Lincei.

Paolo Mataloni
Paolo Mataloni is a professor at the Laboratory of Optics and Nonlinear Optics of the Physics Department of Università “La Sapienza”, Roma, Italy. His fields of research are nonlinear optics, ultrafast optical phenomena, optical microcavities and microlasers, quantum interferometry and quantum information with photons: generation, detection and characterization of entangled photon states, generation of hyper-entangled states and mixed states, quantum nonlocality, etc. He was a member of the organizing committee of the 5th European QIPC Workshop (Rome, 2004). He is also a member of the EPS QEOD board.

Fabio Sciarrino
Fabio Sciarrino is a post-doctoral fellowship within the EU-funded IST project ATESIT at the Istituto Nazionale per la Fisica della Materia, Roma, Italy. His fields of research are quantum optics and quantum information, generation of twin beams by an OPO source, optical implementation of quantum teleportation, quantum cloning, universal NOT gate, optical parametric amplification of quantum states. He was a member of the organizing committee of the 5th European QIPC Workshop (Rome, 2004).

Abstract
The realization of quantum information systems of increasing complexity requires the development of novel linear and non linear quantum optical techniques. In this paper we present different approaches which can be undertaken to increase the available Hilbert space. Hyper-entangled states have been prepared by entangling in polarization and momentum two photons generated by a type I nonlinear crystal. Multiparticle quantum superposition of pure photon states has been generated from a multiple universal cloning of a single photon qubit by a high gain, quantum-injected parametric amplifier. Finally, a different approach is given by adopting the symmetrization technique over the symmetric subspace of two polarization qubits.

Introduction
The key resource for modern quantum information (QI) is represented by the entanglement of quantum states. It combines three basic structural elements of quantum theory (a) the superposition principle, (b) the quantum non-separability property and (c) the exponential scaling of the state space with the number of partitions. This unique resource, associated with peculiar nonclassical correlations among separated quantum systems, can be used to perform computational and cryptographic tasks that are impossible for classical systems.

Quantum optics has represented an excellent experimental test bench for various novel concepts introduced within the framework of the QI theory. Entangled photonic qubit pairs can be generated by the spontaneous parametric down conversion (SPDC) process in a nonlinear (NL) crystal where, under suitable phase-matching conditions, a pump photon of frequency ν_p is annihilated and two photons of frequencies ν_1 and ν_2, with $\nu_p = \nu_1 + \nu_2$, are created. Several kinds of reliable SPDC sources allow to generate either entangled pure or (controllable) mixed states and photon qubits can be encoded in polarization, or energy or momentum directions. As far as polarization entanglement is concerned, the bipartite Hilbert space $H_1 \otimes H_2$, with $\dim(H_1) = \dim(H_2) = 2$ is spanned by the four Bell-state entangled basis, $|\Psi^{\pm}\rangle = (2)^{-1/2}[|H_1,V_2\rangle \pm |V_1,H_2\rangle]$, $|\Phi^{\pm}\rangle = (2)^{-1/2}[|H_1,H_2\rangle \pm |V_1,V_2\rangle]$, where H and V correspond to the horizontal and vertical linear field's polarizations. On the practical side, single photons or photon pairs, are ideal carriers of information for quantum communication since they can be distributed over long distances in free-space and in low-loss optical fibers.

Photon states can be easily and accurately manipulated using linear and non-linear optical devices and can be efficiently measured by means of single-photon detectors.

An intrinsic limit of SPDC is given by the fact that no more than one photon pair is created time by time within each microscopic annihilation-creation process. Since the two photons are generally entangled in a single degree of freedom all possible qubits are limited to a 2x2 Hilbert space, while for some fundamental processes and QI applications [1] it is important to operate with multi-partite entanglement in a larger dimension Hilbert space. This can be obtained in different ways, for example by entangling two photons in more than one degree of freedom and creating in this way a so-called hyper-entangled state, or by entangling more and more photons at the same time (multiparticle entanglement). Other proposals aimed to increase the availble Hilbert space concern the generation of N-level quantum systems (quNits) [2]. In the following sections we describe the results of some recent experiments performed in the laborary of Rome which contribute to enlarge the boundaries of applications of optical techniques to QI.

Hyper-entangled states

Hyper-entangled states are prepared in order to entangle two photons at the same time in two degrees of freedom, in our case polarization and momentum. One of their peculiar properties is that they allow discriminating with 100% efficiency the four orthogonal Bell states, a result which is impossible to achieve with standard linear optics. The idea of encoding the information in the degrees of freedom of polarization and momentum of the same photon was experimentally demonstrated in the first quantum state teleportation (QST) experiment performed in Rome [3].

Hyper-entangled states have been generated by using a SPDC source of entanglement recently realized [4], with peculiar characteristics of flexibility in terms of state generation. Let's refer to **Figure 1**: the source is based on a single arm interferometer which accomplishes the generation of the polarization entangled states $|\Psi^{\pm}\rangle$ and $|\Phi^{\pm}\rangle$ by the superposition of the parametric emission cones, on the left and on the right side, of a type-I NL crystal, excited in two opposite directions by a retro-reflected UV laser beam. The transverse circular section of the parametric emission identifies the so-called "entanglement-ring" (e-ring). Besides polarization entanglement, momentum entanglement is realized by selecting two pairs of correlated directions with a four hole screen intercepting the e-ring (namely a_1, b_2 and a_2, b_1 in **Figure 1**). The "phase-preserving" character of the parametric process allows the two corresponding modal emissions to occur with the same phase. In the present experiment this can be setted by suitable tilting of thin glass plates. As a consequence, in either one of the two SPDC cones, the momentum entangled Bell state $|\psi^{\pm}\rangle = (2)^{-1/2}[|a_1, b_2\rangle \pm |a_2, b_1\rangle]$ is created and hyper-entanglement arises from the product of the polarization and momentum entangled states, i.e. $|\Psi^{\pm}\rangle\otimes|\psi^{\pm}\rangle$ or $|\Phi^{\pm}\rangle\otimes|\psi^{\pm}\rangle$ [5]. Let's consider for example the states $|\Psi^{\pm}\rangle\otimes|\psi^{\pm}\rangle$: the two photons can belong to either one of the correlated modes, a_1-b_2 or a_2-b_1, with orthogonal polarizations, H_1-V_2 or V_1-H_2. This corresponds to have a four qubit state by using only two photons.

The nonlocal character of hyper-entangled states has been verified by a double Bell's inequalities test, performed either with the polarization or the momentum degree of freedom. In both cases a violation of more than 100 standard deviations with respect to the limit value implied by local realistic theories has been obtained by integrating the experimental data over 180s.

We have also characterized the hyper-entangled states $|\Psi^{\pm}\rangle\otimes|\psi^{\pm}\rangle$ by a Hong-Ou-Mandel (HOM) interferometer. In this case the two photons are brought together within a semi-transparent beam splitter (BS), in such a way that the modes a_1-a_2 and b_1-b_2 mix together to generate the output modes a'_1-a'_2 and b'_1-b'_2, respectively (**see Figure 2a**). At the BS output four single-photon detectors register the radiation belonging to the modes a'_1, a'_2, b'_1 and b'_2. Two photon coincidences are registered in either one of the following combinations: a'_1-b'_1, a'_1-b'_2, a'_2,-b'_2 and a'_2-b'_1, while no coincidence is measured for a'_1-a'_2, and b'_1-b'_2.
Let's consider for example the combination a'_1-b'_1: when the photons reach simultaneously the BS, i.e. with zero delay, we can observe a dip or a peak in the two photon coincidence rate depending on the symmetry of the hyper-entangled state which is modified by a proper setting of the polarization and momentum entanglement phases (see the curves of **Figure 2b**). Similar results are obtained for the other mode combinations, a'_1-b'_2, a'_2,-b'_2 and a'_2-b'_1, by changing either one of the momentum and the polarization phases.

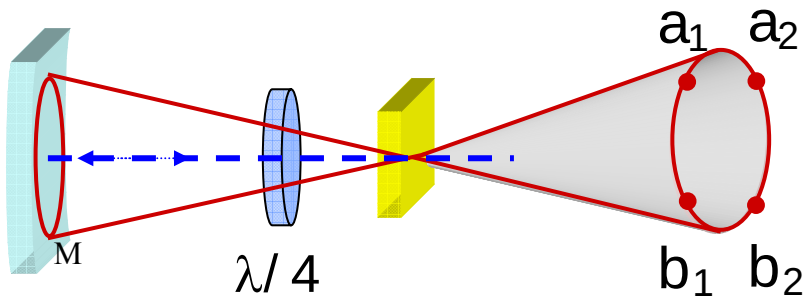
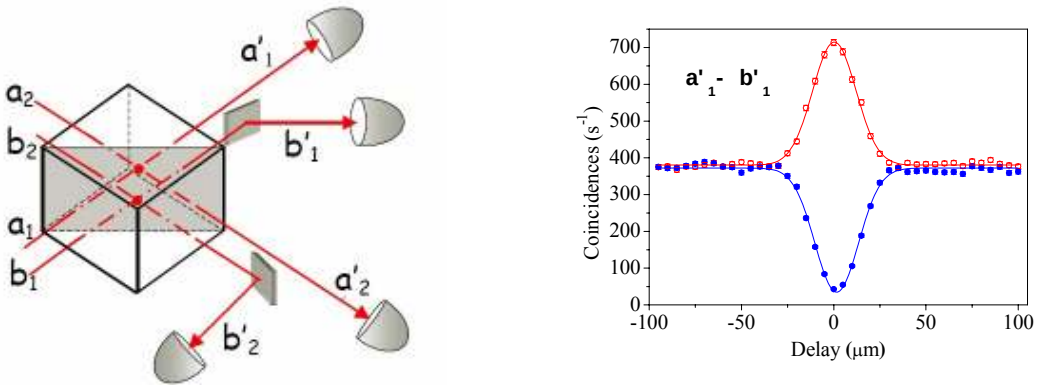


Figure 1: Layout of the parametric source of polarization-momentum hyper-entangled 2-photon states. Mirror M reflects either the pump beam or the radiation generated by the NL crystal, allowing the space-time superposition of the emission cones. The polarization entangled state is generated by double passage of the SPDC radiation through a quarter-wave plate (□/4). Phase transition $|\square\rangle \rightarrow |\square\rangle$, or $|\square\rangle \rightarrow |\square\rangle$, is performed by micrometric traslation displacement of the NL crystal along the pump beam direction. Momentum entanglement is created by selecting two pairs of correlated modes, a_1-b_2 and a_2-b_1, within the e-ring.



a) b)

Figure 2 a): Spatial coupling of the input modes a_1, a_2, b_1, b_2 on the BS. The BS output modes a'_1, a'_2, b'_1, b'_2, are shown. b): a'_1-b'_1 coincidence rates measured for different values of photon delay. Maximum of interference occurs at zero time delay. A polarization filter placed in front of each detector is setted at either +45° or –45°. Lower curve: symmetric state $|\square\rangle\otimes|\square\rangle$; upper curve: antisymmetric state $\square\rangle\otimes|\square\rangle$.

Optical Parametric Amplification

In the last years highly sophisticated methods of "nonlinear optics" (NLO) have started to be applied in QI. The SPDC process (**Figure 3a**) provides the more reliable source of entangled states, as said. It arises as the interaction between the pump field of mode k_P and the vacuum electromagnetic fields of the modes k_1 and k_2. In addition to SPDC, the nonlinear Quantum Injected – Optical Parametric Amplifier (QI-OPA) scheme has proven to represent a unique NL Optics application for QI manipulations. In the present case a single photon is injected over the mode k_1 and overlaps with the pump field inside the NL crystal (**Figure 3b**) stimulating the emission of pairs of photons over the modes k_1 and k_2. Such process is at the basis of important realizations of the quantum analogues of two fundamental processes of classical information: the NOT gate and the cloning (copying) machine. A "high gain" version of that machine consists of a multi-particle, all-optical "Schroedinger Cat" structure. There, in virtue of the basic information-preserving character of the OPA amplification process, the quantum superposition character of a single photon qubit is transferred, in the condition of high intensity pump, onto a multiparticle quantum superposition, thus realizing a "multi-particle qubit" (M-qubit).

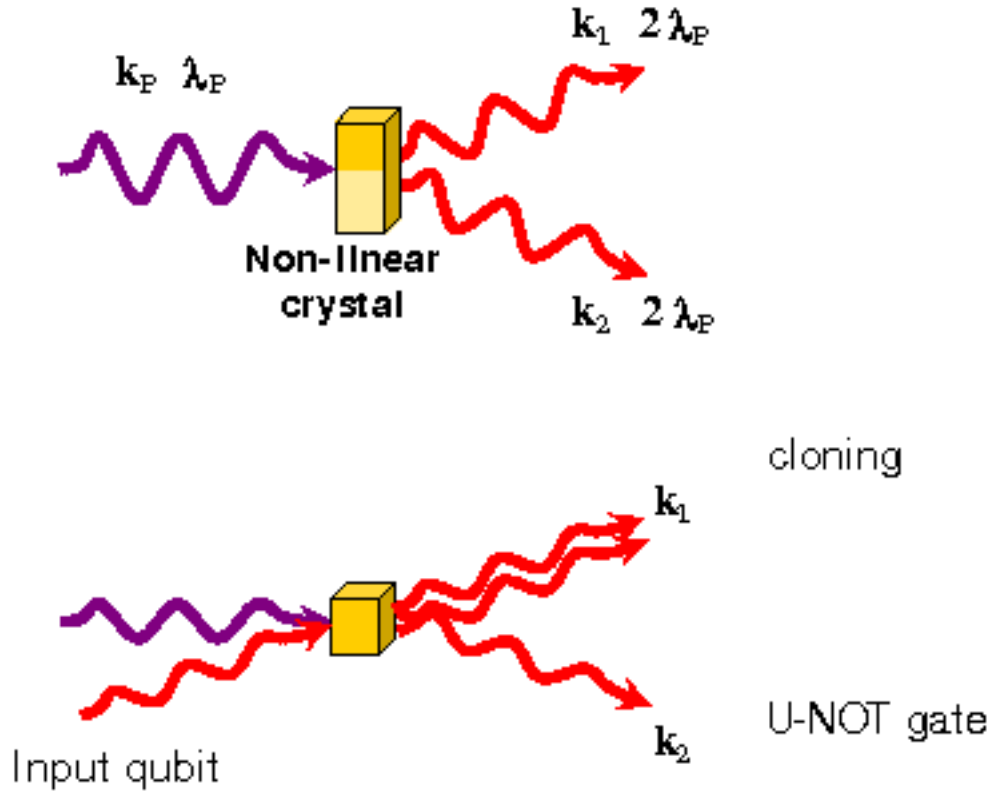


Figure 3: Schematic diagrams of the different non-linear interactions described in the present paper: (a) spontaneous parametric down-conversion, (b) quantum-injected optical parametric amplification.

Cloning and flipping processes in quantum information

Let us first address the optimal realization of the cloning and flipping processes. Quantum information is represented by qubits which can exist in a state $|\phi\rangle$, that is, a superposition of two orthogonal basis states $\{|0\rangle,|1\rangle\}$, i.e. $|\phi\rangle=\alpha|0\rangle+\beta|1\rangle$. Information encoded in quantum

system has to obey rules of quantum physics which impose strict bounds on possible manipulations with quantum information. The common denominator of these bounds is that all quantum-mechanical transformations have to be represented by completely positive (CP) maps which in turn impose a constraint on the fidelity of quantum-mechanical measurements. That is, an unknown state of a qubit cannot be precisely determined (or reconstructed) from a measurement performed over a finite ensemble of identically prepared qubits. In particular, the mean fidelity of the best possible (optimal) state estimation strategy based on the measurement of N identically prepared qubits is F=(N+1)/(N+2). One of the obvious consequences of this bound on the estimation fidelity is that unknown states of quantum systems cannot be cloned, viz. copied perfectly, namely the perfect cloning map of the form $|\phi\rangle \rightarrow |\phi\rangle|\phi\rangle$ is not permitted by the rules of quantum mechanics. Certainly if this would be possible, then one would be able to violate the bound on the fidelity of estimation. Moreover, this possibility would trigger more dramatic changes in the present picture of the physical world, e.g. it would be possible to use quantum nonlocality for superluminal signaling. Another map which cannot be performed perfectly on an unknown state of a qubit is the spin-flip or the universal-NOT, i.e. the operation $|\phi\rangle \rightarrow |\phi^{\perp}\rangle$, where the state $|\phi^{\perp}\rangle$ is orthogonal to the original $|\phi\rangle$; spin-flipping is indeed an *anti-unitary* transformation.

In spite of the fact that some quantum-mechanical transformations on unknown states of qubits cannot be performed perfectly one still may ask what the best possible approximations of these maps are within the given structure of quantum theory. Investigation of these universal optimal transformations, that is, the best approximations of forbidden quantum processes, is important since it reveals bounds on manipulations of information with quantum systems.

In the domain of quantum optics it is possible to realize experimentally universal quantum machines by associating a cloning transformation with a photon amplification process, e.g. involving inverted atoms in a laser amplifier or a nonlinear (NL) medium in a quantum-injected optical parametric amplifier. This can be done in virtue of the existing isomorphism between any logic state of a qubit and the polarization state of the photon qubit. For the non degenerate mode QIOPA, N photons, prepared identically in an arbitrary quantum state (qubit) $|\phi\rangle$ of polarization are injected into the amplifier on the input mode k_1. The amplifier then generates on the same output "cloning mode" (k_1) M>N copies, or "clones" of the input qubit $|\phi\rangle$. Correspondingly, the OPA amplifier generates on the output "anticloning mode" (k_2), M-N states $|\phi^{\perp}\rangle$, thus realizing a quantum universal NOT gate [6]. The nonlinear QIOPA apparatus is found to realize the most general cloning transformation, i.e. involving any value of N and M. A fundamental property of the OPA device is its universality, implying equal quantum efficiencies of the amplification process for any input state. This feature leads to the spontaneous emission of photons with arbitrary polarization states, which represents the unavoidable noise of the cloning process.

Generation of a multiparticle superposition state

The method of Multiple High-Gain (HG) N→M Cloning can be exploited to generate a multi-photon superposition entangled state. This technique reproduces a (noisy) copy of the quantum superposition properties of a single, N=1 pure injected input qubit into the analogous properties of a multi-photon M>>1, pure output state: indeed a "massive qubit" (M-qubit) [7]. Conceptually, the adopted method consists of transferring the well accessible and easily achievable quantum superposition condition affecting any input single-particle qubit to a "macroscopic", i.e. multi-particle amplified quantum-state. In virtue of the general

information-preserving (i.e. coherence-preserving) property of the parametric amplification (OPA) the generated macroscopic state keeps the same quantum superposition character and the interfering capabilities of the input optical-polarization π-encoded qubit, thus realizing a genuine multiphoton quantum superposition state. Such device allows to investigate the topic of the distribution of the information carried by N qubits into several quantum channels starting from a detailed study of the more general cloning process, which represents the optimal way to encode information originally stored in a 2^N dimensional quantum system into a larger one.

Let us now consider the experimental realization (**Figure 4**) [7]. The first step is the generation of the single photon to be amplified, this is achieved by a SPDC process induced by the UV pump beam propagating toward the left direction. By an appropriate manipulation of the UV polarization the non-linear interaction is made inefficient in order to generate no more than one pair per time. The detection of a photon generated over the mode $-k_2$ ensures the presence of a twin photon over the mode $-k_1$ and represents the conditional trigger for the overall process. The photon emitted over the mode $-k_1$ is re-injected inside the NL crystal and overlaps with the reflected UV beam. In this second passage the polarization of the pump beam is rotated to achieve a high gain non-linear effect. The M-qubit state generated by parametric amplification now freely propagates over the cloning (k_1) and anticloning (k_2) modes. The output state can be analyzed over the mode k_2: there any interference effect is a demonstration of the information preserving amplification process.

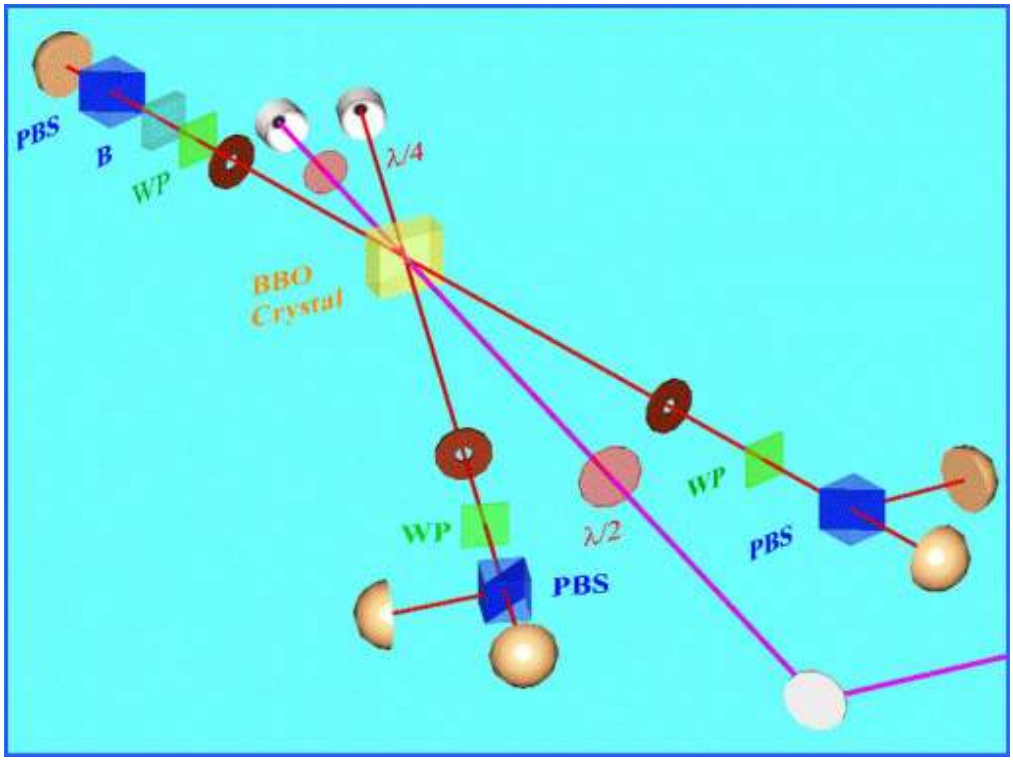


Figure 4: Setup for the realization of a M-qubit optical state.

Methods of symmetrization by linear optics

A different approach which can be undertaken to increase the available Hilbert space and to manipulate QI is the combination of photonic states generated by different source by exploiting basic linear optics components: beam splitter, polarizer beam splitter and single photon detectors.

In this framework, Knill, Laflamme, and Milburn (Nature (London) **409**, 46 (2001)) showed that scalable universal quantum computing can be realized with single photon sources, linear optics and single-photon detectors. This work revealed the full power of "linear optics" and stimulated a great amount of experimental and theoretical investigations where various quantum processes with photonic qubits were demonstrated leading to the first all-optical implementations of the C-NOT gate.

In the last years linear optics methods have been successfully applied to implement projection over the symmetric subspace (SSP) of two polarization encoded qubits. The SSP operation can be accomplished exploiting the bosonic behaviour of the photons by stimulating a coalescence between the two photon qubits to be projected by means of a Hong-Ou-Mandel interferometer.

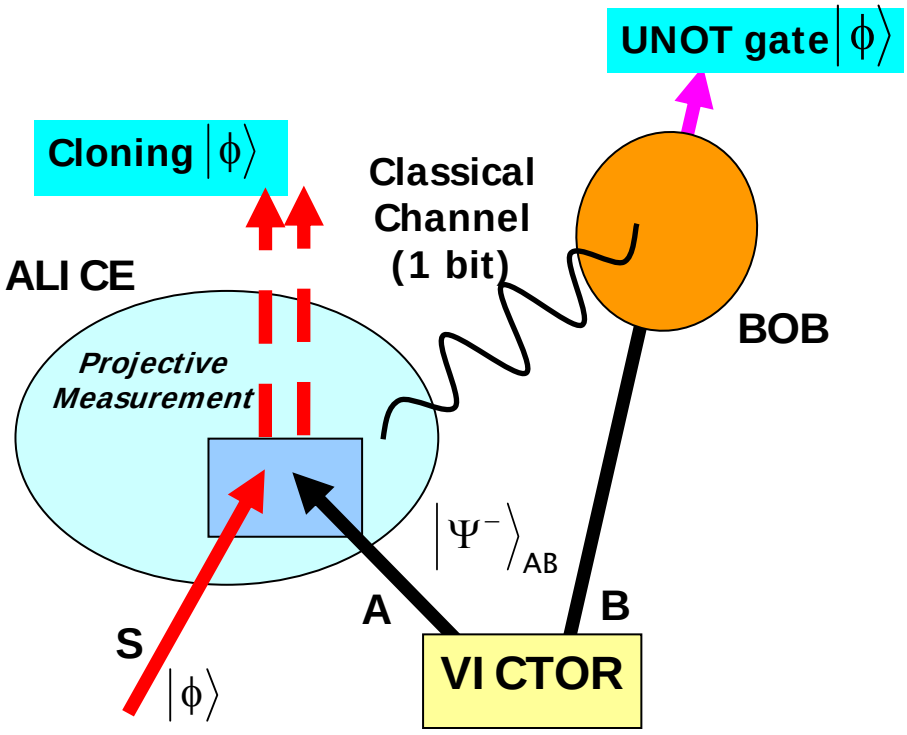


Figure 5: General scheme for the simultaneous realization of the Teleportation of the UNOT gate and the Universal Quantum Cloning Machine.

By adopting the symmetrization technique, different information tasks can be carried out. Among the most significative ones, a slightly modified teleportation protocol has been realized which allows to contextually implement the optimal quantum cloning and the universal NOT gate [8]. In particular, the latter transformation is teleported in a different location and hence called Tele-UNOT gate. The scheme of such protocol is reported in **Figure 5**: as in QST protocol, Alice and Bob share an entangled state of the qubits *A* and *B*.

The input qubit *S* in the state $|\phi\rangle$ reaches Alice's station. She projects the qubit *S* and *A* over the symmetric subspace and communicates the result to Bob by sending one classical bit. If the projection is successful, the qubits S and A are transformed into the optimal clones of $|\phi\rangle$ while the qubit B ends up into the optimal flipped state.

A similar scheme allows performing a purification protocol which, as an alternative strategy to quantum error correction techniques, allows overcoming computation and communication noise by purifying the quantum states that have been corrupted. An optimal purification method for single qubits mixed states, based on SSP techniques, has been successfully implemented for two qubits [8]. This purification acts on a collection of identical systems, and probabilistically filters out purely noisy part of the overall signal.

Conclusions and perspectives

In this paper we have presented some new optical schemes which allow operating in a large dimension Hilbert space. In particular, hyper-entangled states, prepared by entangling two photons in polarization and momentum, allow creating four qubits with only two photons. By these states the complete analysis of the four orthogonal Bell states can be performed. A "high gain" cloning machine consisting of a multi-particle, all-optical "Schroedinger Cat" structure has been realized by the Quantum Injected – Optical Parametric Amplification method. By this state the practical implementation of the universal 2-qubit logic gates may be performed. Within the framework of linear optics, it has been shown how the quantum symmetrization method allows to teleport the UNOT gate and to perform a quantum purification protocol which represents an alternative strategy to standard quantum error correction.

List of terms and acronyms

QIOPA: quantum injected optical parametric amplification
QST: quantum state teleportation
SPDC: spontaneous parametric down conversion
SSP: symmetric subspace projection
UNOT: Universal NOT gate
UOQCM: Universal Optimal Quantum Cloning Machine

References

[1] S.B. Chen, J.W. Pan, Y. Zhang, C. Bruckner, A. Zeilinger, Phys. Rev. Lett. **90**, 160408-1 (2003)

[2] H. Bechmann-Pasquinucci, A. Peres, Phys. Rev. Lett. **85**, 3313 (2000); R. T. Thew, A. Acin, H. Zbinden, and N. Gisin, Quantum Information and Computation **4**, 93 (2004)

[3] D. Boschi, S. Branca, F. De Martini, L. Hardy and S. Popescu, Phys. Rev. Lett. **80**, 1121 (1998)

[4] C. Cinelli, G. Di Nepi, M. Barbieri, F. De Martini and P. Mataloni, Phys. Rev. A, **70**, 022321 (2004)

[5] C. Cinelli, M. Barbieri, F. De Martini, and P. Mataloni, quant-ph/0406148 and Laser Phys. **15**, 124 (2005)

[6] F. De Martini, V. Bužek, F. Sciarrino, and C. Sias, Nature (London) **419**, 815 (2002); A. Lamas Linares, C. Simon, J. C. Howell, and D. Bouwmeester, Science **296**, 712 (2002); F. De Martini, D. Pelliccia, and F. Sciarrino, Phys. Rev. Lett. **92**, 067901 (2004)

[7] F. De Martini, Phys. Rev. Lett. **81**, 2842 (1998); F. De Martini and F. Sciarrino, e-print quant-ph/0410225 (2004)

[8] M. Ricci, F. Sciarrino, C. Sias, and F. De Martini, Phys. Rev. Lett. **92**, 047901 (2004); M. Ricci, *et al*., Phys. Rev. Lett. **93**, 170501 (2004)

Projects funded by the European Commission and related to the work in this article:

IST-2000-29681 ATESIT
Active Teleportation and Entangled State Technology
Start date: 01/08/2001
End date: 31/07/2005
http://atesit.phys.uniroma1.it/
Contact Person: Francesco De Martini, Università "La Sapienza", francesco.demartini@uniroma1.it

Projects funded by National initiatives or organizations and related to the work in this article:

PRA INFM 2002 CLON
Quantum teleportation and quantum cloning by the optical parametric squeezing process
Start date: 01/01/2003
End date: 31/12/2005
http://quantumoptics.phys.uniroma1.it/
Contact Person: Francesco De Martini, Università "La Sapienza", francesco.demartini@uniroma1.it

M.I.U.R. – FIRB 2001
Realization of Quantum Teleportation and Quantum Cloning by the Optical Parametric Squeezing Process
Start date: 01/01/2004
End date: 31/12/2006
http://quantumoptics.phys.uniroma1.it/
Contact Person: Francesco De Martini, Università "La Sapienza", francesco.demartini@uniroma1.it

Contact information of the authors of this article:
Francesco De Martini
Dipartimento di Fisica
Universita' di Roma "La Sapienza"
P.le Aldo Moro 2, Roma 00185
Italy
Email: francesco.demartini@uniroma1.it
Web page: http://quantumoptics.phys.uniroma1.it/

Paolo Mataloni
Dipartimento di Fisica
Universita' di Roma "La Sapienza"
P.le Aldo Moro 2, Roma 00185
Italy
Email: paolo.mataloni@uniroma1.it
Web page: http://quantumoptics.phys.uniroma1.it/:

Fabio Sciarrino
Istituto Nazionale per la Fisica della Materia, Dipartimento di Fisica
Universita' di Roma "La Sapienza"
P.le Aldo Moro 2, Roma 00185
Italy
Email: fabio.sciarrino@uniroma1.it
Web page: http://quantumoptics.phys.uniroma1.it/

Quantum teleportation in Europe

Samuel L. Braunstein
Samuel L. Braunstein is working at the Computer Science Department at the University of York in the UK. He joined the University of York in 2003 and is heading a group on non-standard computation. He is the editor of three books "Quantum Computing," "Scalable Quantum Computing" and "Quantum Information with Continuous Variables" and serves on the editorial board of the journal *Fortschritte der Physik*. He is a founding managing editor of the journal *Quantum Information and Computation*. Braunstein invented one of the early teleportation schemes and participated in its experimental realization. He participated in the EU-funded IST FET project QUICOV. He received the following professional awards: Lord Kelvin Lecturer 2001, Royal Society – Wolfson Research Merit Award 2003.

Pieter Kok
Pieter Kok is working in Hewlett Packard Laboratories, Filton Road Stoke Gifford in Bristol, UK. He received his PhD in physics from the University of Wales, Bangor. After a two-year Postdoctoral Research Associateship at the Jet Propulsion Laboratory in Pasadena, he is now Research Fellow at Hewlett-Packard Laboratories in Bristol. His research activities include linear optical quantum computing and relativistic quantum information theory. He participated in the EU-funded IST FET projects RAMBOQ and NanomagiQ. Professional awards: Institute of Physics QEP PhD Award 2001.

In memory of **Asher Peres**. One of the co-inventors of teleportation. A scholar, a man of science and integrity, a friend.

For some years now, teleportation has been a center of attention. And indeed, **it has become a reality: Researchers have teleported photons, light beams and atoms over distances of up to a few meters and in some cases much further.** How far can this promise be extended? What role has Europe played?

For those familiar with Star Trek, we might expect teleportation to be defined as some kind of instantaneous `disembodied' transport. However, Einstein's theory of relativity tells us that the fastest speed is the speed of light. We must therefore modify our science-fiction based definition to: teleportation is some kind of "disembodied" transport.

This definition is better, but what can the term "disembodied" mean? After all, examples of disembodied transport abound, including the telephone, the fax, the world wide web, etc. Should these processes count as teleportation? In fact, these are all copying processes. They measure the sound, image, or what-have-you, leaving it behind and sending the information gleaned from these measurements across space in some disembodied way. A machine at the receiving end recreates a copy of the original.

However, these straightforward measure-and-copy-at-a-distance schemes would all suffer severe limitations as we try scaling them down to atomic scales. Indeed, if we wanted to "copy" something like the state of an electron, everything we have talked about so far changes: the amount of information we have to transport is actually rather small, but suddenly we have to worry about the quantum mechanical Heisenberg uncertainty principle. For example, we cannot determine the orientation of an electron's spinning axis with arbitrarily high precision, or even whether the electron is spinning clockwise or counter-clockwise. This information would characterize the *spin state* of the electron, **but the intrinsic lack of precision rules out any measure-and-copy-at-a-distance scheme of teleportation of an atomic-scale system.** Let us reiterate this argument: **Quantum mechanics prohibits us from learning everything about an unknown system.** It is this prohibition of learning the complete identity of a system that also eliminates the possibility to make perfect copies of it. This more sophisticated way of looking at Heisenberg's principle is called **the *no-cloning* theorem.**

While "copying" or "cloning" is prohibited by quantum mechanics, the invention of *quantum teleportation* in 1993 suggested another way to achieve disembodied transport. Teleportation (for short) was invented by a team of scientists working in North America, Europe and Israel [1]. It allows even atomic-scale systems to be perfectly transported in a disembodied manner without the limitations due measurement in quantum theory.

To see how one can get around no-cloning, let us outline the steps in a **teleportation protocol**: First let us introduce the actors: Alice, the sender; and Bob, the receiver. Alice is given a quantum system, say an electron in a spin state that is unknown to her. After manipulating that electron in some way to obtain some information about its state, she communicates with Bob, the receiver, using only a conventional communication channel – something conveying only disembodied information – such as radio, the telephone, email, or even a letter in a bottle. Upon receipt of the message, Bob should then be capable of somehow reconstructing the spin state of the original electron on an electron in his own laboratory. He doesn't need to recreate the matter itself, just the information content. The same set of steps would apply whether Alice and Bob were teleporting an electron, a photon, an atom, or the state of any other type of quantum system.

So far we have said nothing special about Bob here. Why couldn't anybody tap the communication channel that Alice and Bob are using, and simply apply the same recreation protocol that Bob is using? They too could create a perfect copy of the state in their own lab. But as we have already argued, if more than one copy of the quantum state were to exist, this would violate the no-cloning theorem. For quantum teleportation to work there would have to be something singling out Bob as the unique receiver. That special something is shared between himself and Alice and it is called *quantum entanglement*. (By the way, this also

means that as Bob recreates the quantum state in his lab, Alice's original version of that state must be destroyed – a fundamental deviation from any conventional copying process.)

Entanglement is a property of two or more quantum particles, such as electrons. However, the simplest form of entanglement exists between pairs of systems. For example, an entangled pair of electrons may be constrained to have perfectly anti-parallel spins. Under such circumstances, whenever the spin state of one electron in any given direction is clockwise, its partner *must* be spinning counter-clockwise in the same direction. If this were true for all possible axes, we would say that the two electrons are maximally entangled. In fact, there are many kinds of entanglement, but this is the type we are interested in for our purposes.

Let us now return to Alice and Bob and see how they use entanglement to teleport the state of an electron. In fact, Alice and Bob will need three electrons: The first is the electron whose spin we want to teleport. The other two electrons are an entangled pair, with one of the entangled electrons in Alice's lab and its partner electron in Bob's lab. This shared resource in effect establishes a private untappable channel of communication between Alice and Bob. In principle, there is no limit to how far apart these two entangled electrons may be. In Switzerland, quantum teleportation of the state of polarization of a photon has been carried out over a separation of 55 meters with the entanglement shared through more than 2 km of optical fiber [2, 3].

Now, what is the curious manipulation that Alice performs on her electron? We somehow have to connect the initial electron to be teleported with the entangled electron pair. Alice accomplishes this by creating new entanglement between the two electrons at her site, forcing them to have correlated (or anti-correlated) spin states. How can she create entanglement? It turns out this can rather straightforwardly be achieved by a measurement that involves both electrons. In the simplest case this measurement would create anti-parallel entangled spins. However, since one of these electrons is already anti-parallel to the electron in Bob's laboratory, Bob's electron instantaneously *collapses* into the spin state of the initial electron that Alice was handed. If a different type of correlation is created by Alice's measurement, she must inform Bob what kind of correlation she found. She does this by sending this information through the conventional communication channel connecting them. With this information Bob can adjust his electron so that its final state is the one Alice was initially given.

Our discussion above was in terms of the teleportation of an electron's spin. In fact, most of the experiments that have been performed confirming teleportation have been with light – either single photons, or beams of laser light. A recent exception was the teleportation of the atomic state of Calcium ions in an ion trap in Austria [4], in the same issue of the journal a closely related experiment was published by a United States group using Beryllium ions.

The Austrian experiment used three ions sitting in a row, trapped by electric fields, and separated by 5 □m. The quantum state to be teleported corresponds to the electronic level structure of the ions. The distance between the ions is small enough to allow the ions to interact via electrical Coulomb repulsion forces. And yet, the distance is sufficiently large to allow the ions to be addressed and manipulated individually with focused laser pulses. The interactions between adjacent ions can create entanglement between their electronic structures. Sequences of laser pulses change the state of the ions (as well as the entanglement) in a very controllable way.

Like any experiment, teleportation is not perfect. However, **the quality of every teleportation experiment can, in principle, be measured by its *fidelity*.** The fidelity

describes how closely Bob's recreated quantum state matches the original. The fidelity can be compared to a reference value that can be achieved 'classically' (without shared entanglement between Alice and Bob). In the Austrian ion-trap experiment, this figure of merit was about 75%, as compared to a 66% fidelity value that could be achieved without entanglement.

As mentioned above, the vast majority of teleportation experiments have been with light. Indeed, the very first experimental demonstrations of quantum teleportation were announced independently by two groups in 1997. As we see below, each of the many possible implementations of teleportation involves its own set of technical subtleties and hurdles. From the initial breakthroughs of 1997 to date, much progress has been made and today, a number of groups can confidently claim the achievement of successful and *bona fide* teleportation.

One of these first teleportation experiments [5] was carried out in Italy. Rather than using three particles, this experiment encoded the information corresponding to a quantum state directly onto one of the entangled photons. This greatly simplified their experiment and allowed any type of entanglement measurement to be carried out. Their experiment chose to encode the polarization of a photon and yielded fidelity of about 85%, as compared to a baseline of 75% without entanglement. This important achievement, however, does not lend itself to building more general protocols. By comparison, the second experiment, in Austria, used a freely propagating photon as the incoming state to be teleported [6], in addition to an entangled pair of photons. The Austrian experiment used a simple beam-splitter to allow Alice to measure the necessary entanglement. The difficulty with this latter scheme is that not every type of entanglement can be resolved in this way. Nonetheless, because an actual system is teleported, the scheme can be scaled up to more sophisticated protocols.

A variation of teleportation involves the teleportation of an entangled state, so-called *entanglement swapping*. One key feature of entanglement swapping is that because the state being teleported is entangled itself, it is truly an unknown quantum state. Using a setup very similar to their original scheme, the Austrian group experimentally demonstrated entanglement swapping [7]. They later carried out a much higher fidelity entanglement swapping experiment yielding a fidelity of 89% [8].

One subtlety in some of the above single-photon teleportation experiments [6, 7, 8] is that they require an additional step of *post-selecting* the state at Bob's end. In other words, all the photons involved in a particular run go through a detector and only a subset are selected as having been teleported. This limitation was overcome by modifying the balance of probabilities between the source of the unknown state and the source of the entangled pairs. An experiment implementing such a variation then became the first to demonstrate the teleportation of freely propagating single-photon states without post-selection [9].

So far, we have considered teleportation from one fixed location to another. However, one of the surprising features of quantum teleportation is that in principle, Bob's location need not be known by Alice. In this situation Alice would simply send the results of her measurement to all possible locations that Bob might be (say via some broadcast). When Bob receives the message containing Alice's results, he may complete his actions on his half of the entangled pair to reproduce the original state Alice was given. Naively, allowing Bob to move around with his setup would involve the storage and then movement of one-half of an entangled pair – a potentially very difficult task.

Recently, an experiment involving collaborators from China, Austria and Germany was carried out that demonstrated this feature of open-destination teleportation, though without the need for state storage. The experiment essentially involved the creation of a 4-photon

entangled state (a so-called Greenberger-Horne-Zeilinger or GHZ state) as the entanglement resource instead of the usual two-photon (or Bell-state) entanglement [10]. These multi-particle GHZ states have the interesting property that by making suitable measurements on a subset of all but two of the particles, the unmeasured pair collapses into ordinary two-particle entangled states. If the four photons are directed to four different locations, then depending on which of the particles were measured, the remaining entangled pair will then be found at their corresponding locations. This entangled pair could then be used to perform teleportation in the usual manner, but now with the extra freedom on Bob's part to choose the destination (and potentially also for Alice to choose the point of departure).

Among the above experiments, the ion-trap scheme was unique in allowing for teleportation *on demand*. In other words, the teleportation could be performed precisely when needed on the system given to Alice. In all of the other experiments, which involved the teleportation of light (in fact, of single photons of light) only weak sources of light were available, both for the state to be teleported and the entangled pair shared between Alice and Bob. Thus, all of these single-photon experiments were operated in a conditional manner, relying on the rare occurrences of the states required. This limitation stems from our reliance on lasers as sources of coherent light. Lasers typically produce strong coherent beams. To achieve single-photon teleportation, the laser can be very much attenuated in order to obtain occasional randomly appearing photons. Obtaining single photons or even pairs on demand from such a source is currently beyond our capabilities. Despite this difficulty in 1998 one of the earliest teleportation experiments, involving a team of scientists from the US, Japan, the UK and Denmark, managed to perform on-demand teleportation of whole coherent beams of light, in an unconditional manner [11]. Indeed, rather than attenuating the beams to obtain weak (and randomly occurring) single-photon states or entangled pairs, they used multi-photon entangled states, called two-mode squeezed states, to teleport coherent beams of light. Rather than polarization, the teleported state encoded the coherent amplitude and phase of the laser beam. A fidelity of about 58% was achieved using this source of entanglement, above the best fidelity of 50% which might be achieved without entanglement.

Conclusions

Quantum teleportation is almost certainly going to be an important component of any future quantum information infrastructure. European scientists have been at the forefront of teleportation research since its inception when the idea looked very much like a pipe dream. Indeed, European groups have led the way and are still at the cutting edge of teleportation theory and experiment, inventing teleportation schemes, developing and refining a variety of implementations, and achieving a variety of impressive experiments.

References

[1] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres and W.K. Wootters, *Physical Review Letters* **70**, 1895 (1993)

[2] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden and N. Gisin, *Nature* **421**, 509 (2003)

[3] H. de Riedmatten, I. Marcikic, W. Tittel, H. Zbinden, D. Collins and N. Gisin, *Physical Review Letters* **92**, 047904 (2004)

[4] M. Riebe, H. Häffner, C.F. Roos, W. Hänsel, J. Benhelm, G.P.T. Lancaster, T.W. Körber, C. Becher, F. Schmidt-Kaler, D.F.V. James and R. Blatt, *Nature* **429**, 734 (2004)

[5] D. Boschi, S. Branca, F. De Martini, L. Hardy and S. Popescu, *Physical Review Letters* **80**, 1121 (1998)

[6] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter and A. Zeilinger, *Nature* **390**, 575 (1997)

[7] J.-W. Pan, D. Bouwmeester, H. Weinfurter and A. Zeilinger, *Physical Review Letters* **80**, 3891 (1998)

[8] J.-W. Pan, M. Daniell, S. Gasparoni, G. Weihs and A. Zeilinger, *Physical Review Letters* **86**, 4435 (2001)

[9] J.-W. Pan, S. Gasparoni, M. Aspelmeyer, T. Jennewein and A. Zeilinger, *Nature* **421**, 721 (2003)

[10] Z. Zhao, Y.-A. Chen, A.-N. Zhang, T. Yang, H.J. Briegel and J.-W. Pan, *Nature* **430**, 54 (2004)

[11] A. Furusawa, J.L. Sørensen, S.L. Braunstein, C.A. Fuchs, H.J. Kimble and E.S. Polzik, *Science* **282,** 706 (1998)

Contact information of the authors of this article:

Samuel L. Braunstein
Computer Science Department
University of York
York YO10 5DD
United Kingdom
Email: schmuel@cs.york.ac.uk
Web page: http://www.cs.york.ac.uk/~schmuel/home.html

Pieter Kok
Quantum Information Processing Group
Hewlett-Packard Laboratories
Filton Road, Stoke Gifford
Bristol
United Kingdom
Email: pieter.kok@hp.com
Web page: http://www.pieterkok.com

Quantum Communication

Nicolas Gisin
Nicolas Gisin is a professor in the Group of Applied Physics, University of Geneva, Switzerland. After a post-doc at the University of Rochester, NY, and four years in industry, he returned to academia in 1988. His research work ranges from optical fibers and instrumentation for telecommunication to quantum communication and theoretical physics. In February 2003, his work on quantum cryptography was recognised by the MIT Technology Review as one of the 10 technologies that should "change the world".

John G. Rarity
John rarity is a professor of Optical Communications at the E&EE Department of the University of Bristol, Bristol, UK. Prof Rarity has been developing Quantum cryptography since its discovery some 15 years ago and is presently involved in projects developing linear optics quantum logic and low cost free space quantum cryptography. He is the coordinator of the EU-funded IST project RAMBOQ and a member of the SECOQC integrated project on Quantum Cryptography.

Both authors were part of the IST-QuCom project that received the 2004 Descartes prize.

Abstract

Optical communication changed our society. Ever denser trains of light pulses cover our planet. Technology has been so successful that the underlying physics becomes crucial for near- and mid-future developments. The physics of light pulses with few light quanta – called photons – is quantum physics. Accordingly, the technology of future communication is quantum communication.

Introduction

Quantum communication is the art of transferring quantum states from one place to another. The general idea is that quantum states encode quantum information, thus quantum

communication also implies communication of quantum information. A nice feature of quantum communication is that it covers aspects of practical relevance as well as basic physics. The prominent application is quantum cryptography, which, together with quantum random number generators, is the most advanced realization of devices operating at the individual quanta level (see next chapter in this volume).

The basic physics aspect is evident when we exploit quantum entanglement in quantum communications. This allows one to investigate the nonlocal characteristics of quantum physics that appear, among others, in teleportation, dense coding and tests of Bell inequalities. The weirdness of quantum entanglement is manifest when one realises that it provides a channel through which useful correlations can be established, like those necessary for quantum cryptography and teleportation, but these kinds of channels do not follow any path in ordinary space. Moreover, the time order of the measurements doesn't matter. Even the direction in which the particles fly to establish the entanglement doesn't matter: a particle may fly from Bob to Alice, entangling Alice and Bob, but the teleportation process, for instance, could well go from Alice to Bob. Actually, in theory, Bob may even have moved in-between the creation and the use of entanglement to another location without even Alice noticing it; still the entanglement, i.e. the quantum channel, links Alice to Bob.

A priori, quantum communication could be realized with any quantum systems. However, the most natural carrier of "flying quantum information" are photons, that is "light particles". Indeed, these fly naturally and are rather easy to isolate during their propagation. At present, the development of optical systems is largely driven by the classical communication industry. However, the continuous bit rate increase will inevitably lead us into the quantum domain. Indeed, the number of photons per bit has to get lower if the mean power remains constant. This situation is similar to that prevailing in the semiconductor industry, according to the well known exponential law formulated by Moore. Inevitably, the 21st century's technology will be dominated by quantum mechanics. As noted by Michael Berry [1], the 19th century saw the discovery and formalization of electromagnetism which radically changed the 20^{th} century technology and similarly the 20th century saw the discovery of quantum mechanics which will play a central role in the technology of this century.

For students, quantum communication is an excellent subject, teaching them about basic quantum physics from a modern perspective. Moreover, they learn it in the fascinating, and thus motivating, context of quantum teleportation and similar counter-intuitive phenomena. Simultaneously the students learn about optical sources, detectors and components (optical fibers, isolators, switches, etc) that are the basic tools of the modern optical engineers.

Quantum cryptography, quantum teleportation and experiments on entanglement are the subjects of 3 other articles in this series. Hence, we shall not address them in details here, but encourage the reader to examine them. Here we shall concentrate first on the choice of the medium for quantum communication, optical fibers versus free space in section 2, next on the challenge of extending quantum communication to longer distances, section 3, finally on multiparty quantum communication in section 4.

The quantum communication channel: Optical fibers versus free space

The choice of communication channel is intricately linked with the wavelength of light. Long distance fibre optic communications exploit the low loss of silica fibres in the 1.3 μm and 1.55 μm wavelength bands. However the initial development of quantum communications

came through the development of efficient, low noise photon counting detectors based on Silicon APD's sensitive to visible and near infra-red light (400nm-1 μm wavelength).

As a result groups originating from the quantum optics community have exploited the convenient silicon detectors to perform key initial experiments. These experiments have been primarily either free space or short range fibre optic demonstrations.

The development (and commercialisation) of convenient long wavelength (1.3-1.6 μm) photon counting detectors have allowed groups originating from telecommunications to develop fiber experiments for long range quantum communication demonstrations and applications. These experiments are able to use standard fibres installed for classical communications to take quantum communications out of the laboratory [2].

In the longer term the move to long wavelength fibre experiments is more likely to lead to practical applications. However the shorter wavelength free space systems could still see applications outside the earth's atmosphere where diffraction rather than scattering loss is the range limiting factor. In fact in space we may see experiments over ranges measured in thousands of kilometres, truly testing the non-locality of quantum mechanics! [3]

Towards longer distances

At present, quantum communication is limited to some tens of km, maybe even up to 100 km. Actually there is not a strict limit, but, because of the losses, the probability that a photon makes it through the channel decreases exponentially with the distance. The other limiting factor is the photon detector noise. Indeed, all single-photon detectors have a small but non-negligible probability to fire by accident, i.e. to deliver an electronic signal even in the absence of any photon. Such fake signals are called dark-counts; they are of course independent of the channel's length. When the distance between the sender and the receiver is so large that the probability of a dark-count is similar to the probability for a photon sent by the transmitter to be detected by the receiver, then it is intuitively clear that no communication is possible any longer.

The naive way around this problem would be to try to amplify the signal, that is to amplify the photon. But, according to the basic rules of quantum physics, this is impossible: it is impossible to clone quantum states. Note that if it were possible, then the adversary Eve could do so and keep a clone for her self: this would be the end of quantum cryptography. Note furthermore that it would also contradict the Heisenberg uncertainty relation (one could first clone the state, next perform incompatible measurement on each of the two clones). Finally, it would also allow one to use entanglement to signal at arbitrary high speed, in particular faster than light, contradicting thus relativity. This no-cloning theorem is thus absolutely central in today's physics. Accordingly, one may fear that quantum communications are condemned to rather short distances. But this is not quite so: the magic of quantum entanglement allows one to concatenate quantum channels, hence to extend their lengths to arbitrary long distances.

Consider the case where A-B and B-C both share an entangled state. In this case B holds two quantum systems, one entangled with A, the other entangled with C. If B measures any one of his systems, he destroys the entanglement. But quantum physics allows B to perform a joint measurement on his two systems. Formally such a joint measurement is represented by a self-adjoint operator whose eigenstates are entangled. In simpler words, a joint measurement does not provide any information about any of the two individual systems, but provides information only about the relationship between them. This is the basis of entanglement

swapping, see chapter 6 (?). By performing such a joint measurement, B can concatenate the two entanglements A-B and B-C into a longer one connecting A-C. This is the basic idea of a quantum repeater. But it is not yet complete, as discussed below. Such a partial quantum repeater is called a quantum relay [4]. Note that interestingly entanglement plays two roles here. First, as a non-local channel delivering correlations to distant partners. Next, as a means to measure relative properties without acquiring any information about the individual systems. Both aspects of entanglement are necessary.

The probability that two photons send out by B both make it, one to A, the other to C is actually the same as the probability that a single photon makes it directly from A to C. Hence, entanglement swapping as described above doesn't increase the probability of a successful photon transmission, or equivalently doesn't increase the probability of successfully establishing entanglement between A and C. However, it does help in decreasing the probability of a dark-count. Indeed, a dark-count can only happen when a detector is opened in the absence of a photon. By dividing the total length into smaller sections, the probability of losing a photon is reduced; hence the dark-count probability is reduced. Consequently, quantum relays increase the maximal distance over which quantum communication can be realized, but only to a limited extent which depends on the channel loss and detector characteristics. Typically, with today's technology it could extend the distance to a few hundreds of km, but at the cost of ultra low bit rates.

In order to really fight against the exponential bit rate decrease, one has first to divide the channel into smaller sections, as above, next to establish entanglement in each section in parallel. Once entanglement is established in a section, one should be able to keep it until a nearby section also holds entanglement. This requires quantum memories, i.e. the possibility to store quantum information while keeping all its coherence, including possible entanglement with other systems. This is an active, but very challenging, field of research. Only the successful development of quantum memories compatible with existing quantum channels will allow the realization of quantum repeaters [5], thus the extension of quantum communication to a world wide quantum web.

Multi-party quantum communication

Quantum entanglement offers correlations with some promise. For example, two maximally entangled qubits offer perfect correlation with the promise that no third party has any correlation, in other words the promise is that the 2 perfectly correlated bits are secret. In general it is not known what to do with the quantum correlation! This is not surprising, since the field is still in its infancy and it is only during the last few years that computer scientists and physicists have collaborated on this within European projects. A recent example is the demonstration of bit-string tossing [6], a nice result made possible only thanks to quantum communication, but whose utility is still unclear.

Another example, worth to mention, is the 3-party Byzantine agreement protocol. In this scenario the 3 parties are only connected by one-to-one communication channels. Their goal is to communicate openly, i.e. there is no secrecy requirement. To the contrary, the parties like to make sure that every one receives the same information. Furthermore, there is no outside adversary, but one (and not more) out of the 3 parties might be cheating. In such a case, the two honest parties like to be certain to receive the same information. It is pretty easy to convince oneself that without any further resources, this Byzantine problem is impossible.

Indeed, if the sender (one of the 3 players) sends a bit to his two colleagues using the two channels that connect him to each of them, then the two colleagues should check whether they receive the same bit. For this they send to each other the bit they received. If each of the two receiver receives twice the same bit, it's all fine. But what if one of them receives two different bit values? In such a case there is no way for this receiver to find out whether it is the sender that sent out confusing information, or whether it is his colleague who cheats. Notice that such a scenario is very common in distributed databases: whenever the database has to be updated, it is crucial that all parts of the database update simultaneously and coherently. Indeed, think of a database containing the price of some goods. If some malevolent person manages to have the price erroneously cheap here and expensive there, then this intruder could easily profit from such a confused situation. Interestingly, progress on this classical problem has been made recently by assuming that the 3 players share correlations arising from a "natural" quantum state [7]. By this we mean a 3-party quantum state with high symmetry: a 3 spin-1 state of zero total angular momentum. This example supports the conjecture that quantum correlation are the natural building blocks of many cryptographic tasks.

Conclusions

Quantum communication is a fascinating field for basic physics and for students. It combines concepts and technique from basic quantum physics to optical engineering, from information theory to communication complexity. Simultaneously, it is the most advanced field within Quantum Information Sciences. First commercial quantum cryptography systems are already finding their ways to niche markets. Still, serious challenges have still to be faced in order to increase the bit rates and the distances.

This is still a very young field. New concepts, new applications and new techniques are expected to emerge from the ongoing research. These may well affect our society as much as classical communication did change our world.

References

[1] Introduction to Q computation and information, eds Lo, Spiller and Popescu, World Scientific 1998

[2] P.D. Townsend et al., Electron. Lett. 29,634,1993; D. Stucki et al., New J.Phys. 4,41,2002; R.J. Hughes et al., J.Mod.Opt. 47,533,2000; T. Kimura et al., Single-photon interference over 150-km transmission using silica-based integrated-optic interferometers for quantum cryptography, quant-ph/???

[3] W.T. Buttler et al., J. Mod.Opt. 47,549,2000 ; Ch. Kurtsiefer et al., Nature 419, 450, 2002 ; M. Aspelmeyer et al., Long-Distance Free-Space Distribution of Quantum Entanglement, quant-ph/; Mo Xiao-fan et al., Intrinsic-Stabilization Uni-Directional Quantum Key Distribution Between Beijing and Tianjin, quant-ph/0412XXX.

[4] E. Waks et al., Phys.Rev. A 65,052310,2002 ; B.C. Jacobs et al., Phys.Rev. A 66,052307,2002; D. Colins et al., quant-ph/0311

[5] H. Briegel et al., Phys. Rev. Lett. 81,5932, 1998

[6] S. Massar et al., quant-ph/0408120 & 040812

[7] M. Fitzi, N. Gisin and U. Maurer, Phys. Rev. Lett. 87,217901,2001

[8] S. Tanzilli et al., in preparation

Figure 1: Dr S. Tanzilli aligning a "quantum transfer" experiment in which the state of an entangled photon at 1300nm is swapped onto a photon at 710 nm. The experiment confirmed that the initially independent 710 nm photon is then entangled by performing a test of Bell inequality [8].

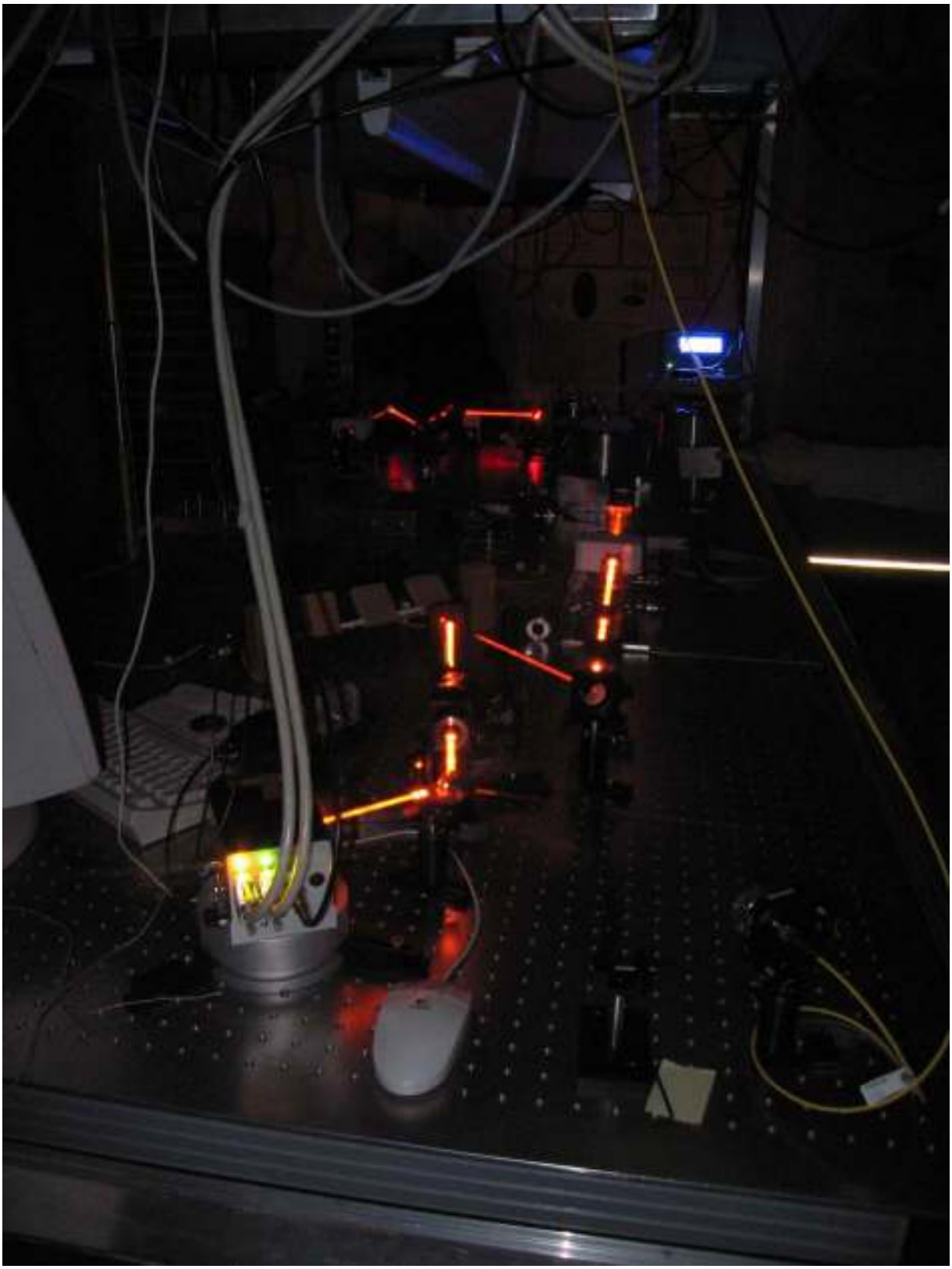


Figure 2: A "quantum transfer" experiment in which the state of an entangled photon at 1300nm is swapped onto a photon at 710 nm. The experiment confirmed that the initially independent 710 nm photon is then entangled by performing a test of Bell inequality [8].

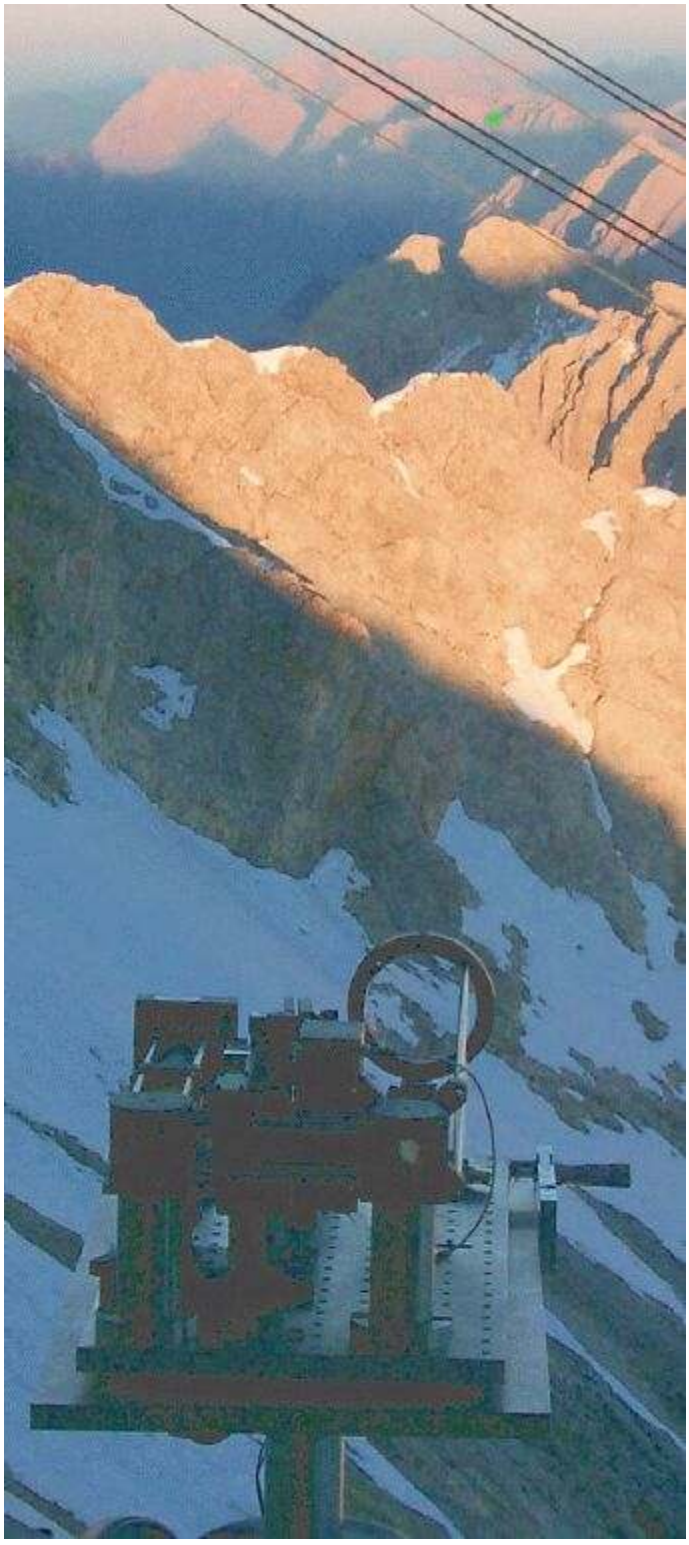


Figure 3: Source of the free-space quantum cryptography demonstration in south Germany.

Figure 4: Aerial picture of the first world database archiving system secure by quantum cryptography. Commercial systems by id Quantique are installed at the two ends of the fiber-quantum-channel.

Figure 5: Commercial single-photon detector compatible with telecom optical fibers.

Projects funded by the European Commission and related to the work in this article:

QuComm
Long Distance Photonic Quantum Communication
Start date: 01/01/2000
End date: 30/04/2004
Project web site http://www.imit.kth.se/QEO/qucomm/
Contact Person: Prof. A. Karlsson, KTH, Sweden, Andkar@imit.kth.se

EQCSPOT
European Quantum Cryptography and Single Photon Optical Technologies
Start date: 01/11/1998
End date: 31/10/2000
Project web site http://www.cordis.lu/esprit/src/28139.htm
Contact Person: Prof. J.G. Rarity, U. Bristol

EQUIP
Entanglement in Quantum Information Processing and Communication
Start date: 01/01/2000
End date: 31/12/2002
Project web site: http://www.equip.qipc.org/
Contact Person: Martin Wilkens, U Potsdam
e-mail: Martin.Wilkens@physik.uni-potsdam.de

RESQ
Resources for Quantum Information
Start date: 01/01/2003
End date: 31/12/2005
Project web site: http://www.ulb.ac.be/project/RESQ/
Contact Person: Serge Massar, Université Libre de Bruxelles, smassar@ulb.ac.be

RamboQ
pRobabilistic gAtes Making Binary Optical Quanta
Start date: 01/01/2003
End date: 31/12/2005
Project web site http://www.ramboq.net
Contact Person: Prof. J.G. Rarity, U. Bristol

SECOQC
Development of a Global Network for Secure Communication based on Quantum Cryptography
Start date: 01/05/2004
End date: 30/04/2008
Project web site http://www.secoqc.net/
Contact Person: Christian Monyk, ARC Seibersdorf, Austria, christian.monyk@arcs.ac.at

TMR network on the physics of entanglement

QAP: FP6 Integrated Project in the process of negotiations
Qubit Applications
Contact person: Dr. Jason Twamley, NUI Maynooth, Jason.Twamley@may.ie

ESF: program on “QUANTUM INFORMATION THEORY AND QUANTUM COMPUTATION”
Start date: 1999
End date: June 2004
Project web site: http://www.esf.org/esf_article.php?activity=1&article=26&domain=1
Contact person: Neil Williams

Projects funded by National initiatives or organizations and related to the work in this article:
NCCR (National Center of Competence and Research): project on Q communication, first phase July 2001-June 2005, funding 1.900.000CHF, second phase: July 2005 – June 2009, funding about 2.000.000CHF

Contact information of the authors of this article:

Prof. Nicolas Gisin
Group of Applied Physics
University of Geneva
20, rue de l'Ecole de Medecine
CH-1211 Geneva 4
Switzerland
Tel:+41-22-379.6597 Fax: +41-22-379.3980

Prof. John Rarity
Department of Electrical and Electronic Engineering
University of Bristol
Woodland Road
Bristol BS8 1UB
Tel: +44 (0) 117 954 5174 Fax: +44 (0)117 954 5206
Email: john.rarity@bristol.ac.uk

Twin-photon sources for quantum information applications

Anders Karlsson
Anders Karlsson (M.Sc. Engineering Physics, Ph.D. Electrical Engineering KTH) is Professor of Quantum Photonics at the School of Information and Communication Technology, Royal Institute of Technology (KTH), Stockholm, Sweden. He has been a visiting researcher at NTT Basic Research Laboratory, Stanford University, and lecturer at École Polytechnique, Palaiseau. His research interests are quantum information, quantum optics and wavelength-scale photonics. He is also the director of the KTH M.Sc. program in Microelectronics. He is a member of the EU-funded IST project SECOQC (FP6), and he was the coordinator of the EU-funded IST project QuComm that received the 2004 Descartes price.

Daniel Ljunggren
Daniel Ljunggren (M.Sc. Electrical Engineering, KTH) is a Ph.D.-student at the School of Information and Communication Technology, Royal Institute of Technology (KTH), Stockholm, Sweden. His current research interest is quantum information theory and experiments, in particular quantum cryptography and entangled state sources in quasi-phase matched materials.

Maria Tengner
Maria Tengner (M.Sc. Engineering Physics, KTH) is a Ph.D.-student at the School of Information and Communication Technology, Royal Institute of Technology (KTH), Stockholm, Sweden. Her current research interest is quantum information theory and experiments, in particular entangled state quantum cryptography and entangled state sources in quasi-phase matched materials.

Abstract
Entangled states are a key physical resource in many quantum information applications. In quantum communications and tests of linear optical quantum logic the work-horse today for the generation of entangled states is based upon twin-photon generation in so called non-linear optics parametric down-conversion. In this chapter we discuss some of the physics and engineering issues involved in improving the technology for such twin-photon sources.

Introduction
Optical entanglement has become a fundamental resource in quantum communication applications such as quantum cryptography, quantum teleportation, the quantum repeater, and linear optics quantum computing [1]. In addition, entangled photon pairs are essential for recently proposed methods in quantum metrology and for many investigations of basic quantum effects. Most applications require very bright, efficient, and well-controlled sources of entanglement, which in terms of optics means that they should be is efficiently coupled into optical fibers or be well adapted to free space optics. In the chapter of Gisin and Rarity the general scenario for quantum communication has been described, and a description of light sources and detectors for quantum communication has been given in the chapters by Weinfurter and Leuchs, the chapter by Shields and Abram, and in the chapter by Walmsley and Banaszek. In the present chapter we discuss in a bit more details some of the technology aspects of entangled state sources, and ask ourselves what is to be expected in terms of development in the near future.

Photonic quantum bits
Before embarking on describing various sources of photonic entangled states, let us step back a bit and describe first how to encode quantum information on light pulses as this relates to what types of entangled state we are interested in producing. Basically, all types of encoding formats that can be used in classical optical communication one can think of using also for quantum communication. However, most commonly used is to encode on the polarization of light for free space communication, and for optical fibers, especially for the long-haul telecommunication wavelength of 1550 nm, to encode on the phase or on time slots (time bins) of light pulses. A particularly illustrative example is the concept of “time-bin qubits” explored by the group of N. Gisin in Geneva (proposed in 1999 [2]), where the bit encoding is done on well defined time slots, see **Figure. 1**. A data bit “0” or “1” is then represented by a photon, which is either in the first time-bin – a “0”, or the second – a “1”, or in a quantum mechanical superposition of the two slots.

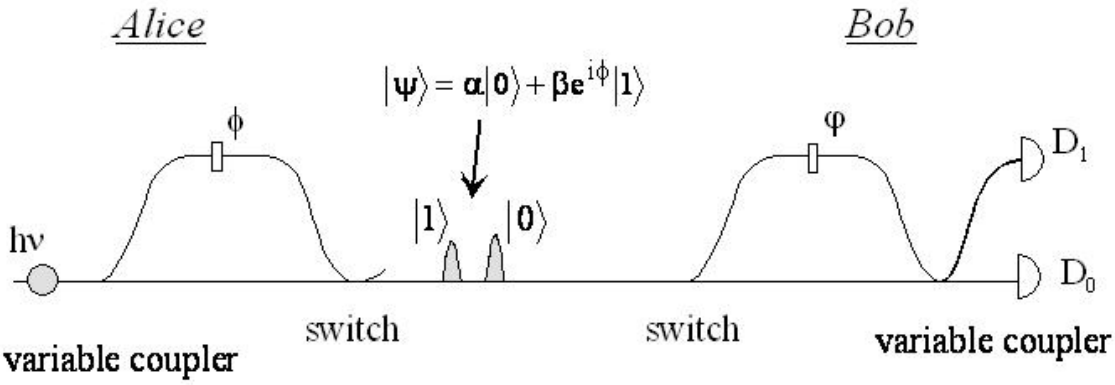


Figure 1: Creation and analysis of a time-qubits. A photon is put into a superposition of taking either a short or long path length creating a time bin superposition. On the receiving side a similar device can decode the encoded bit.

Such a time-bin setup is actually rather similar to systems used for faint laser-pulse based quantum cryptography by among others British Telecom, University of Geneva, IBM, Los Alamos National Laboratory, KTH and many others. The good performance of these systems underlines the robustness of time-bin qubits with respect to decoherence effects as encountered while traveling down an optical fiber.

Parametric down-conversion: an overview

As described in the chapter of Weinfurter and Leuchs and the chapter of Walmsley and Banaszek, the most common way at present to efficiently generate entangled pairs of photons is offered by parametric down-conversion (PDC) using non-linear optics. Parametric down-conversion can be seen as the inverse of so called non-linear optics frequency doubling. What then is frequency doubling you may wonder? Actually, a simple example of frequency doubling is found in the pen-like green laser pointers commonly used these days.

The human eye is most sensitive for green color, hence a green laser pointer is nice to have! However, laser diodes emitting in the green are difficult to do, so in the green laser pointer, a laser diode emitting in the infrared first pumps, i.e. injects energy to a solid state Nd:Yag lasers crystal which emits laser light at 1064nm. This light in turn hits an optical crystal where it is doubled in frequency (meaning that the wavelength is half the original value) to the characteristic green light at 532nm, which we then use as our high tech pointer. All these elements, a diode laser, an Nd:Yag laser crystal, a non-linear optical crystal, plus the electronics and the battery to drive the laser, all fits within size of a ball-point pen.

The physics of the frequency conversion is that when strong pump light propagates through an optically nonlinear medium, the response of the medium- the crystal, to the light is not linear with the pump field. This is a bit similar to the distortions, the clippings and overtones in an audio amplifier when one crank up the volume too much when listening to one's favorite rock album. Back to the crystal again, the non-linear response leads to the generation of new optical fields –overtones- at other well-defined frequencies than the pump field. In the case of PDC this process is used to take an energy-rich pump-photon to be converted into two less energy-rich twin-photons. In the conversion process, physics requires that the energy and momentum is conserved. This conservation creates the quantum correlations- entanglement

between the photons- hence the name “photon twins”, which physicist and engineers now eagerly are exploring in quantum information applications.

At this moment, it may be worthwhile to pause and think of the relevant time frames for science and technology development. Non-linear optics was enabled in the 1960s by the development of lasers allowing sufficiently strong optical fields to be created in a controlled manner. The thirty to forty year delay in harvesting this technology in terms of applications outside science, such as in optical communications, in medicine, or in pen-size laser pointers may indeed seem very long. Today the time-to-market from “science to product” is typically much shorter, but for most technologies both a near term and long term perspective must be taken in order to correctly assess the innovation potential.

For quantum technologies, the time perspective likely is a mixed one, with some technologies, such as quantum cryptography, having matured very fast. For the case of the entangled state sources, many of the sources and systems under development and use today, may still appear to be bulky or semi-compact. Nevertheless taking the pen-like green laser pointer as a nice example, it can be anticipated that in a near term perspective these sources will be made even more compact and easy to use.

Entangled state sources - an overview, and where to next?

Let us focus on some of the development in PDC that has taken place over the last few years, notably within the European context of the IST-QuComm project. For many quantum communication experiments, requiring femto-second pulses (such as three, four or five-photon entanglement) the sources still require a solid state laser pumping of a so called Ti:Sapphire laser capable of delivering very short pulses. Such a system is a rather costly and bulky, still extremely useful! However, in many applications where the very short pulse-length is of secondary importance, the drive has been to develop more compact, cheap and easy-to-operate sources of entangled photons. To give some of the desired characteristics, one would like to be able to generate photon pairs at 800, 1300 or 1550nm, or a suitable combination of these. The pulse repetition rate and duty cycle should be large, typically above 1 MHz with more than a 100 000 photon pairs/second. The photons should also preferably be generated in a narrow wavelength band, which for optical fibre systems allows them to propagate longer distances without two different pulses being blurred. The source should have small footprint (one to a few square decimetres), allow for efficient optical fibre coupling, be cheap, and have a minimum number of adjustments needed, i.e. be a “plug-and-PLAY” source, and not a “plug-and-PRAY” one. In the last few years, significant progress was made in this direction, which in turn allowed for many of the new exciting physics and technology experiments described elsewhere in this publication.

How do we get entanglement optically? In terms of entanglement generation for photon polarization (the oscillation direction of the electric field), let us first remind ourselves what polarization entangled twin-photons are. The characteristic properties of polarization entangled photons are such that for the individual photon the polarization is completely random before it is measured. What is only known about the two photons is that whatever the polarization of the first photon turns out to be, the polarization of its twin-photon will be orthogonal. The randomness of the individual photon, but the complete correlation to its twin partner, it what makes entangled twin-photons useful for cryptography and computing, i.e. as a mean to generate identical random numbers at two locations, or as a perfect carrier of the strongest possible statistical correlations physics permits throughout a computation.

As described in the article by Weinfurter and Leuchs, to obtain polarisation entangled states one can fulfill the energy and momentum conservation using various schemes. Perhaps the best-known scheme is one where two orthogonally polarized photons are emitted into two intersecting cones in so called type II phase matching [3]. In one of these cones horizontally polarized light is emitted, in the second vertically. Looking then at the intersection of the cones, one cannot tell which polarization is emitted, one can only tell that the photons at the two intersecting cones will be orthogonal – they have twin properties. An alternative, and more efficient way to generate an entangle state, however is the two crystal source using type I phase matching [4] and two thin crystals. Here the two crystals are placed perpendicular to each other, one creating vertically polarized photons, the other horizontally polarized ones. If pump light then hits both of them creating down-converted photons either being both horizontally polarized, or both vertically. Then, if one cannot by any means distinguish in which of the crystals the down-conversion took place, one will obtain an entangled state. As Weinfurter and Leuchs points out, with the advent of blue laser diodes (with wavelengths around 400 nm) of sufficient power, polarization entanglement around 800 nm can be generated in an efficient manner, and it can be expected that in the next years to come such sources will be amply deployed in down-conversion experiments, both in science, education and in engineering applications.

The other interesting wavelengths for quantum communication systems are given by the telecom windows of optical fibers around 1300 nm and 1550nm optical wavelengths. For these wavelengths laser diode pumped down-conversion sources have been developed, taking advantage of bulk crystals as well as on periodically poled waveguides [5,6,7]. For optical fiber applications, however, polarization entanglement is less interesting because typically the polarization is scrambled as photons travels along an optical fiber. For these wavelengths, perhaps the most interesting entanglement then is that of time-bin entanglement, which has proven to be highly fruitful for experiments. Taking the time-bin quantum bit as a starting point, to create entangled time-bin photon twins, these can be created by pumping a non-linear crystal with two subsequent (classical) light pulses, see **Figure. 2**. In this arrangement each pump photon is split into being a super-position of taking a short or a long path, which when the pump photon is converted into twin-photons, the twin-photon inherits the superposition of short or long path, thus becoming entangled. This source, proposed in 1999 by the University of Geneva [2], has subsequently been successfully used by the Geneva group in quantum key-distribution, quantum secret sharing, quantum teleportation and quantum relay experiments, many of these experiments realized within the IST-QuComm project.

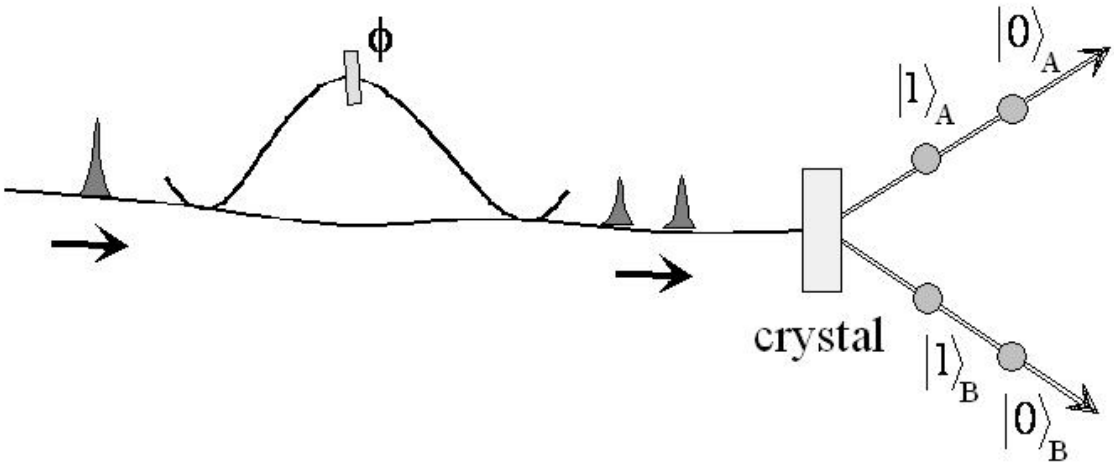


Figure 2: Creation of an entangled time-bin qubits. A classical light-pulse is split into two subsequent pulses by means of an interferometer with large path-length-difference. Pumping a non-linear crystal, a photon pair is created either by pulse 1 (in time-bin 1) or by pulse 2 (in time-bin 2). The uncertainty (superposition) of the path taken by each pump photon is translated into a superposition of the twin-photons thus creating a time-bin entangled state.

Lately, in the search for more efficient sources, PDC in quasi-phase matched (QPM) materials has attracted attention [5-10], see also the article by Wamsley and Banaszek. In these nano-structured materials the optical nonlinearity is periodically changed on the length-scale of the optical wavelength. This simplifies the momentum conservation condition and gives a freedom to choose the wavelengths of the down converted light and the directions of emission by simply varying the period. Intuitively, the periodic changes in the material assist the conversion process by giving an extra momentum kick to the light. One can loosely compare it to the inverse process in down-hill skiing on moguls, where unless one is skiing well in phase with the periodicity of the bumps one may get an undesired momentum kick. In QPM materials, the momentum kicks are used positively. An advantage with the QPM materials is that it is possible to work with emission along the propagation direction of the pump light and therefore use longer crystals resulting in high photon rates. High rates also means that one can get many photons in a narrow wavelength band, which is good if the light should propagate long distances in an optical fiber. At KTH we have combined the two crystal idea mentioned earlier with the quasi-phase matching technique in potassium titanyl phosphate (KTP), giving a very bright source suitable for applications in quantum communication [5]. In **figure 3,** to illustrate entanglement is shown the density matrix (i.e. the quantum mechanical state) of the entangled state generated by this source. The choice of non-degenerate wavelengths at 810 nm and 1550 nm is, with the 1550 nm arm time-bin encoded, could make such a source useful for quantum communication schemes taking advantage of both the low attenuation in fibers at infrared and the good detector performance at the near visible region of 810 nm. Related work at Massachusetts Institute of Technology (MIT) in the group of Wong and Shapiro [6] also seeks to explore this mixed wavelength entanglement with interesting work towards coupling the 800 nm photon to Rubidium atoms to be used as quantum memories with a potential long term application in quantum repeaters.

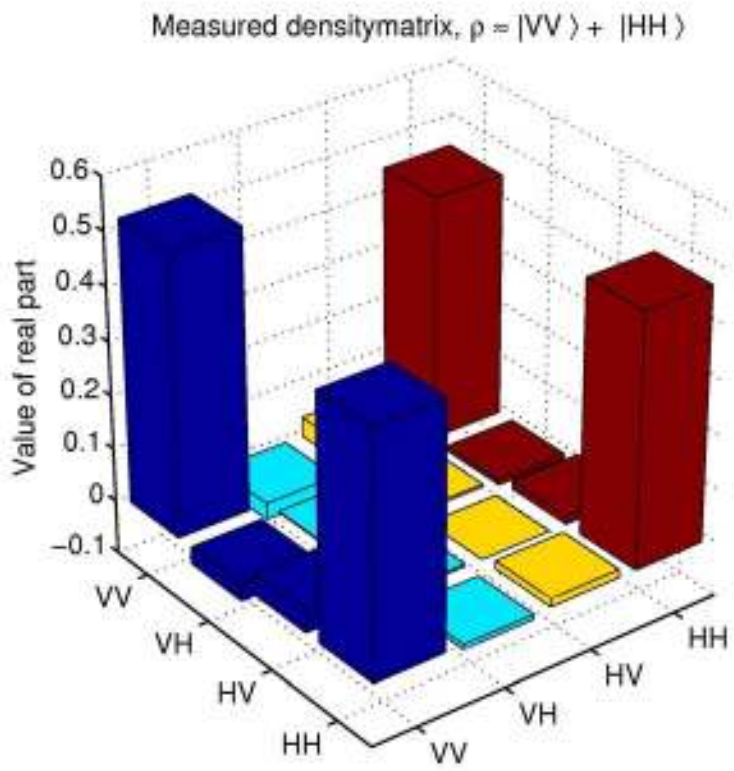


Figure 3: Experimental density matrix of wavelength non-degenerate (800/1500 nm) polarization entangled state generated by parametric down-conversion in KTP and measured by a tomographic procedure (picture D. Ljunggren, M. Tengner, KTH). If all four columns in the corners are large, this means that the quantum state is entangled and hence carries the quantum correlations making it useful for quantum information experiments.

Quasi-phase matching (QPM) has also been successfully used in time-bin entanglement in a collaboration between the University of Nice and the University of Geneva [7]. In these experiments a periodically poled lithium niobate crystal having also waveguiding structure was used. The combination of quasi-phase matching with waveguiding to confine the pump and the photon-twins together in a small region in this case allowed for an increase of the photon pair creation rate by about four orders of magnitude, and in many ways this combination would seem to be the way to go. Related work by Sanaka et al. [8] also has also shown very good results for with periodically poled lithium niobate waveguides. Overall, we believe the time is becoming ripe for more advanced entanglement engineering using tailored sources. Very interesting work on this has been done by Banaszek and Wamsley [9,10]. A nice very recent example of entanglement engineering may also be the MIT work on frequency-entangled states of potential use in timing measurement beyond the resolution limit set by conventional classical light [11].

Finally, let us mention also the interesting work in progress at THALES and Université Paris 7 – Denis Diderot in France carried out within Esprit OFCORSE II, IST:QuComm, and IST:RAMBOQ towards making an extremely compact source of twin-photons based on intra-cavity parametric down-conversion inside a laser diode [12,]. This structure works as laser for the pump light, and then simultaneously performs nonlinear conversion to generate photon twins. Fabrication tolerances, however, are very strict, but if successful it would be an interesting alternative for some applications to the non-linear crystal sources mentioned above.

Conclusion

Quantum information and Communication has come a long way indeed with commercial first-generation quantum cryptography systems now hitting the market, and a number of excellent field experiments using entangled state systems has also being demonstrated. One of the next steps forward assisting in the engineering and applications of quantum technologies will be on improving the practicality and performance of entangled state sources, as well as providing optimized sources for application-tailored entangled states.

Acknowledgements

The work presented in this overview was mainly carried out within the EU FP5 QIPC project IST-QuComm as well as carried on within the EU FP5 QIPC project RAMBOQ, and to some extent within the EU FP6 SECOQC project. The authors would also like to acknowledge S. Ducci and V. Berger of Univ. Paris 7 for providing the latest info on diode laser twin-photon sources, and finally the national funding agencies for their support of this work.

List of terms and acronyms

PDC: Parametric Down-Conversion, the non-linear optical process creating photon twins.
QPM: Quasi-phase matching, a nano-structuring of the non-linear material to gives increased flexibility for the choice of wavelengths in non-linear optical frequency conversion.
Nd:Yag: Neodynium doped Yttrium Aluminium Garnet, a common material for solid state lasers.
KTP: potassium titanyl phosphate, a common crystal used for non-linear optics.

References

[1] W. Tittel and G. Weihs, , Quant. Inf. Comput. 1, 3-56 (2001)

[2] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden, Phys. Rev. Lett. 82, 2594 (1999)

[3] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, Phys. Rev. Lett. 75, 4337 (1995)

[4] P. G. Kwiat, E. Waks, A. G. White, I. Appelbaum, and P. H. Eberhard, Phys. Rev. A 60, R773 (1999); D. V. Strekalov, Y.-H. Kim, and Y. Shih, Phys. Rev. A 60, 2685 (1999)

[5] M. Pelton, P. Marsden, D. Ljunggren, M. Tengner, A. Karlsson, A. Fragemann, C. Canalias, and F. Laurell, Optics Express 12, 3573 (2004)

[6] M. Fiorentino, G. Messin, C. E. Kuklewicz, F. N. C. Wong, and J. H. Shapiro, Phys. Rev. A 69, 041801(R) (2004)

[7] S. Tanzilli, H. De Riedmatten, W. Tittel, H. Zbinden, P. Baldi, M. De Micheli, D. B. Ostrowsky, and N. Gisin, Electron. Lett. 37, 26 (2001)

[8] Kaoru Sanaka, Karin Kawahara, and Takahiro Kuga, Phys. Rev. Lett. 11, 5620 (2001)

[9] K. Banaszek, A.B. U'Ren and I.A. Walmsley, Opt. Lett. 26, 1367 (2001)

[10] A.B. U'Ren, K. Banaszek, I.A. Walmsley, Quantum Information and Computation 3, 480 (2003)

[11] O. Kuzucu, M. Fiorentino, M. A. Albota, F. N. C. Wong, F. X. Kaertner, Phys. Rev. Lett., vol.94 p.083601 (2005)

[12] A. De Rossi, V. Ortiz, M. Calligaro, B. Vinter, J. Nagle, S. Ducci, and V. Berger, Semicond. Sci. Technol. 19, L99 (2004)

Projects funded by the European Commission and related to the work in this article:
QuComm
Long Distance Photonic Quantum Communication
Start date: 01/01/2000
End date: 30/04/2004
Project web site http://www.imit.kth.se/QEO/qucomm/
Contact Person: Prof. A. Karlsson, KTH, Sweden

Descartes prize

Descartes prize ceremony, members of the QuComm project winning team from left to right: V. Berger, N. Gisin, A. Karlsson, M. Aspelmeyer, A. Zeilinger, and T. Jennewein.

Copyright: Institut fuer Experimentalphysik, Universitaet Wien, Photo: Robin Riegler
Descartes prize ceremony, members of the QuComm project winning team from left to right: N. Gisin, A. Karlsson, M. Aspelmeyer and A. Zeilinger.

RAMBOQ
pRobabilistic gAtes Making Binary Optical Quanta
Start date: 01/01/2003
End date: 31/12/2005
Project web site http://www.ramboq.net
Contact Person: Prof. J.G. Rarity, U. Bristol

SECOQC
Development of a Global Network for Secure Communication based on Quantum Cryptography
Start date: 01/05/2004
End date: 30/04/2008
Project web site http://www.secoqc.net/
Contact Person: Christian Monyk, ARC Seibersdorf, Austria, christian.monyk@arcs.ac.at

QAP: FP6 Integrated Project in the process of negotiations
Qubit Applications
Contact person: Dr. Jason Twamley, NUI Maynooth, Ireland, Jason.Twamley@may.ie

Projects funded by National initiatives or organizations and related to the work in this article:
SSF – INGVAR
Swedish Foundation for Strategic Research
Individual Grant for Advances of Research Leaders
SSF – Strategic Research Center in Photonics
Swedish Foundation for Strategic Research
Strategic Research Center in Photonics, project Quantum Communication
VR- Quantum Information Technologies
VR- Special Researcher Position
Swedish Science Research Council (VR)
Contact information of the authors of this article:
Anders Karlsson, Professor Quantum Photonics
School of Information and Communication Technology
Laboratory of Optics, Photonics and Quantum Electronics
Royal Institute of Technology (KTH)
Electrum 229
S-164 40 Kista, Sweden
Tel: +46-8-790 40 81, Fax: +46-8-790 4090
email: andkar@imit.kth.se ,
Internet: www.quantum.se

Quantum interface between light and matter

Eugene S. Polzik
Eugene Polzik is a professor at the Niels Bohr Institute of the Copenhagen University in Denmark. He is also the Director of the Danish National Research Foundation Center for Quantum Optics. His research is concentrated in the areas of quantum optics and experimental quantum information science. He is the fellow of the Institute of Physics and won the Danish Physical Society Award (NKT Prize) in 1999. He is a member of the following EU-funded IST projects – CAUAC, QUICOV, COVAQIAL, FQA. Prof. Polzik's research was named among the 10 top achievements in science in 1998 by AAAS. He is also honorary professor at the University of Aarhus and a Distinguished Invited Professor at the Institute for Photonic Sciences in Barcelona.

Abstract
Quantum information systems require an **interface between information processors - atoms, and long-distance information carriers - light pulses**. In classical communication the role of such interface is played, e.g., by photo-detectors and amplifiers which detect, measure, and amplify light pulses transmitting, for example internet communications, and convert them into electrical current pulses which then go into our computers. Such an interface is inapplicable in QI where communication and computing is performed with quantum states which are simply ruined by the measurement. **This article describes the principles of quantum interfaces capable of a faithful transfer of quantum states between light and matter.**

Introduction
Distributed quantum networks capable of long-distance quantum communication will inevitably involve some kind of light-atoms quantum interface. Such an interface should be capable of a faithful conversion of a quantum state of a light pulse into corresponding quantum state of an atomic memory or an atomic quantum processor, and vice versa. It is known from the basics of quantum mechanics that an unknown quantum state cannot be faithfully determined by measurements. Therefore a simple classical strategy of detecting a pulse of light and converting it into a classical pulse of electric current will introduce so many errors into the quantum network that all advantages of QI will be wiped off. Similarly, an atomic node of a quantum communication network or a quantum computer which exists in an entangled quantum state cannot be simply converted into an electrical signal which will then drive a laser producing a light pulse for communication.

A quantum light-atoms interface must use fundamentally new principles which provide a faithful quantum state transfer from one medium to another. Very recently first experimental

advances along those lines have been made by European and US teams. A quantum state of a weak pulse of light has been faithfully mapped and stored in an atomic ensemble. Distant atomic samples have been entangled via interaction with light paving the road towards long distance teleportation of atoms. An entangled state of a single photon and a single ion has been also generated. These developments are the first steps towards long distance quantum networks and communication.

This article is mostly about the quantum interface based on multi-atom ensembles. An alternative approach using single atoms trapped inside high-Q optical cavities is discussed in another article in this publication.

Long-distance entanglement between atomic objects

One of the most ambitious quantum communications schemes, "quantum teleportation", requires an entangled state to be shared by the sender and the receiver. Teleportation of a quantum state between distant nodes of a quantum network requires quantum entanglement to be first created between the distant nodes (see the articles on entanglement and the one on the basics of teleportation). For teleportation of atomic states, one has to create long-lived entangled states of two distant atomic objects. Short distance entanglement and teleportation of a single material particle, an ion, has been recently demonstrated by a European and a US teams using short-range entanglement generated via charge-to-charge interaction over a distance around 0.01mm. There is, however, little doubt that a long distance entanglement between atoms has to be mediated by light, the only practical long distance carrier.

Quantum entanglement is an attribute that links two or more quantum systems as one, allowing particles with two distinct quantum states to have a much closer relationship than classical physics permits. It is clear from this "definition" that entanglement is all about how a system is divided into two. A simple example is two electrons in a helium atom. A quantum state of the electrons cannot be viewed as a product of the individual electronic states. Such mutual interconnection is particularly spectacular if two entangled objects are not tied together as in the helium atom, but are far apart -- for example, two photons separated by many kilometres. However, material objects like atoms do not fly apart as easily as photons and are therefore much more difficult to entangle at a distance.

The first demonstration of an entangled state of two distant material objects has been done by a European team [1]. In this work the collective spins (magnetization) of the first and the second ensemble have been entangled. A pictorial view of the entangled state of this kind is presented in the **Figure 1**. A collective spin of an atomic ensemble cannot, according to the, so called, uncertainty principle, have a well defined direction. The principle developed by one of the founding fathers of quantum physics, Werner Heisenberg in 1927, states that certain "complementary" properties of light and matter cannot be determined simultaneously without an uncertainty. This "quantum uncertainty" is shown in the **Figure 1** as a pink circle around the end of the spin vector. One can, in principle, carry out a measurement of the direction of the spin in, say X-Y plane (the Y projection), which will most likely produce a result somewhere inside the uncertainty area. However, as a result of this knowledge, the direction of the spin in the X-Z plane becomes totally undetermined. If one attempts to obtain the best possible knowledge about *both* Y and Z projections, then the pink circle is the best accuracy that can be achieved. However, for two **entangled** atomic samples the two vectors of magnetization become parallel, despite the fact that each of them still has an undefined direction. This is an example of the non-local quantum superposition, or distant entanglement.

The measurement on the spin direction of one of the two entangled samples immediately reveals the direction of the other spin, which can be very far away from the first one.

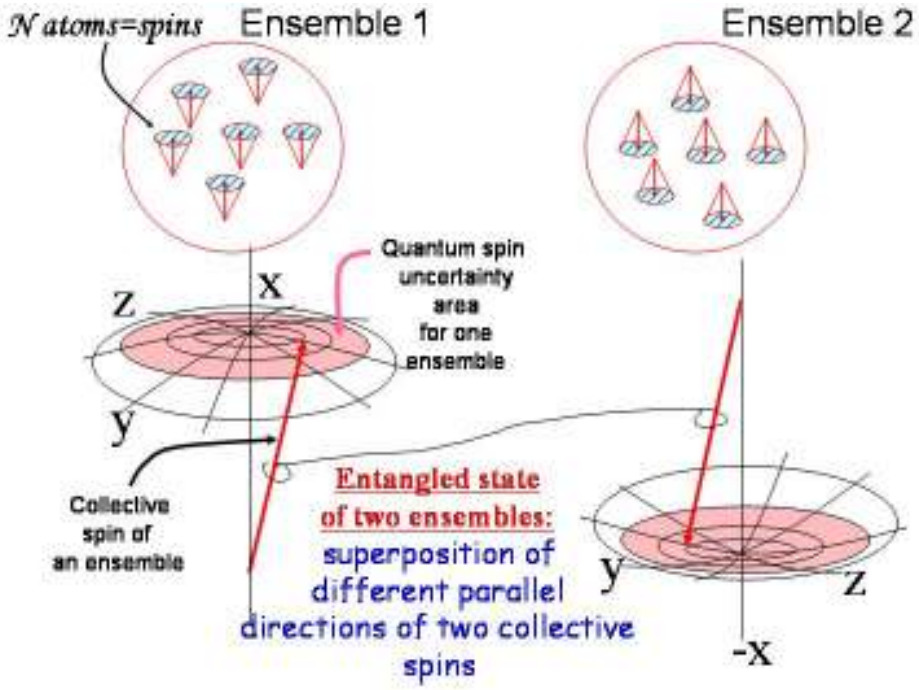


Figure 1

In the experiment [1] entanglement has been generated by a quantum measurement on a pulse of light transmitted through the two atomic samples. The longest distance to-date at which the entanglement of material objects has been generated is 0.4 m. However, much longer distances are feasible since the limit on the distance is set only by losses which light experiences propagating between the two samples. Such entanglement can serve as the basis for the long distance quantum teleportation of states of atomic objects.

Quantum limits for classical communication networks

Pulses of light are the prime carriers of today's internet and phone communications. As the speed and capacity of internet doubles every 18 months, the tendency is to use weaker and weaker pulses, because optical communication lines cannot otherwise stand the ever-growing amount of light. At the same time light of different colours is used to send parallel streams of information via the same fibre, the process called frequency multiplexing.

But there is a fundamental limit to this growth. It can be illustrated by the "complementarity" or uncertainty principle already mentioned above. Translated in modern language it states that the amplitude and the colour of a weak pulse of light are "complementary", that is they cannot be determined simultaneously with high accuracy. This property is a manifestation of the fragility of quantum states used in QIP. The weaker are pulses of light the lower their rate must be in order to separate the colours of different communication channels. Therefore different colour channels of tomorrow's communications will mix up and produce errors in communication if this information is recorded into the classical memory via standard detection. **In order to overcome this quantum limit, communication of the future can use a quantum memory instead of a classical memory used today.**

However, quantum physics not only puts limits but also opens up novel possibilities in communication and computing (see article 13 for the general discussion of the quantum channel information capacity). Within the field of quantum information, quantum complementarity of light can be used to encode information and link quantum computers in quantum networks. Quantum memory is required to transfer the complementary quantum variables between light and atoms.

Quantum memory for light based on atomic ensembles

In the paper published in November 25, 2004 issue of *Nature* [2] three European groups collaborating under the EU project COVAQIAL have for the first time demonstrated recording of illusive "complementary" quantum properties of light in atomic memory.

In the experiment [2] performed at the Niels Bohr Institute in Copenhagen an extremely weak pulse of light containing just a few photons has been stored in a ensemble of Caesium atoms contained in special cells. The experiment utilized relatively simple technology (gas of atoms at room temperature) and hence can, in principle, be scalable into a multi-channel device.

Quantum memory which can be used for storage of an incoming pulse of light has to meet the following criteria:

- Memory must work for light prepared by a third party is a quantum state unknown to the memory holder
- Memory must provide storage of the quantum state of light with fidelity surpassing that of the best classical memory possible
- Memory must allow for a retrieval of the stored quantum state

The fidelity criterion is very important because no realistic device can provide 100% fidelity, however, the "benchmark" classical fidelity must be surpassed. Every class of quantum states is characterized by its benchmark classical fidelity. For some classes this fidelity is known. For example, for a class of coherent states of light the benchmark classical fidelity for memory performance is 50%. The importance of coherent states of light in communication is due to their wide use in classical communication, as well as in quantum cryptography (see article 10 for description of quantum cryptography with coherent states). **The experiment [2] demonstrated the light quantum storage fidelity of up to 70%, significantly higher than the classical benchmark.**

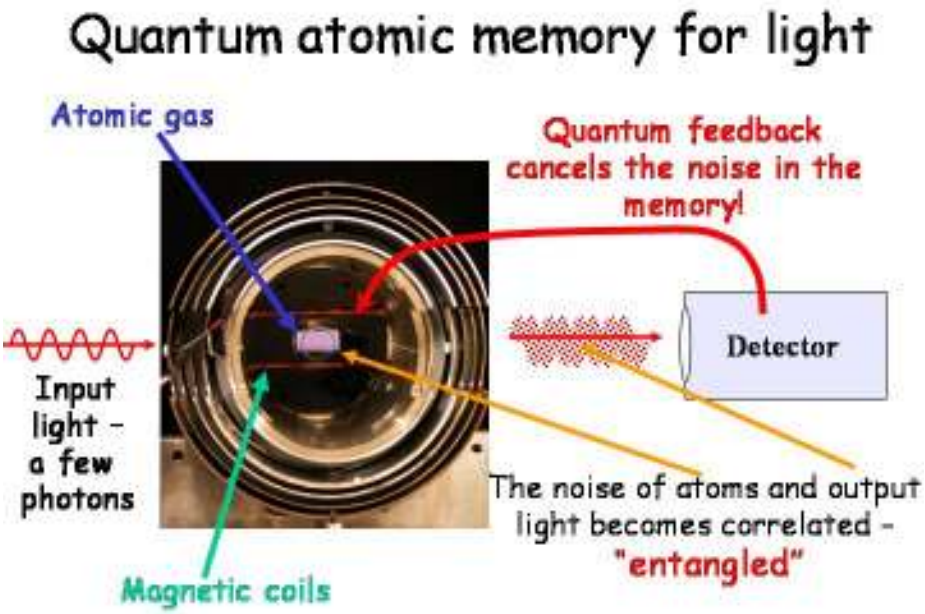


Figure 2

Quantum memory protocol utilizes entanglement of light and atoms and is an alternative to the quantum teleportation protocol. The principle steps of the quantum memory protocol are shown in the **Figure 2**. An atomic memory is first initialized, i.e., oriented along X direction, as shown in **Figure 1**, by sending a pulse of circularly polarized light along X axis. Next a linearly polarized quantum pulse of light which is to be stored is combined with a strong, orthogonally polarized entangling pulse and sent through the atomic sample in the Z direction. In the process of interaction of this combined pulse with atoms the amplitude of the quantum pulse is mapped onto the Y-projection, of the collective atomic magnetization and stored there. The transmitted pulse which becomes entangled with the atoms is detected by ultra-sensitive detectors and its phase is measured. This phase signal contains information about the initial quantum phase of light mixed with the unavoidable quantum noise of the Z-projection of atomic magnetization. The measured signal is converted into an electric current pulse. This electric current is then applied to coils generating magnetic field which rotates the Z-projection of the atomic magnetization such that the atomic quantum noise is cancelled and the phase of the initial pulse of light is mapped onto this projection of atomic magnetization. **This quantum noise cancellation provided by entanglement and quantum feedback is in the heart of the quantum memory protocol.**

After several milliseconds of storage time, a long time by quantum information standards, the atomic memory state is checked by a read out pulse of light to verify the fidelity of the stored state.
Future directions of this research involve

- development of the quantum memory read out – a faithful transfer of the stored state (or of another state which can be a result of quantum processing of the stored state) back onto another pulse of light for further use in a quantum network
- demonstration of the capability of this memory protocol to store other quantum states of light, such as a single photon state, or its superpositions, a qubit state.

Irrespectively of applications the demonstrated transfer of complementary "immeasurable" properties between light and matter is of principal interest in quantum physics.

An alternative and promising approach to the quantum memory for light based on the so-called electromagnetically induced transparency (EIT) leading to the "stopped light" has been proposed by a European-US collaboration [3]. Researchers in the US successfully demonstrated *classical* memory for light using EIT, and the extension to the quantum domain is much awaited.

Towards a quantum repeater

A powerful approach towards long-distance quantum entanglement and communication called a quantum repeater has been proposed by a European team in 1998 [4]. The idea there is to split a quantum communication line into sections – repeaters - connecting intermediate stations. Entanglement is first generated between pairs of neighboring stations by detecting a photon emitted by each pair of stations **(see Figure 3).** This process is launched at all pairs of neighboring stations simultaneously and can be probabilistic, i.e., can have low probability of success due to losses of photons in communication lines. The loss of light in communication channels is the central problem of long distance quantum communication. Quantum repeaters tackle the problem of signal loss by temporarily storing the state of a photon emitted at each repeater. This allows new photons with the same state to be generated at each repeater, meaning a long travel distance is achieved by a number of short steps. Because of the parallel nature of this process, the total length of the communication link can still be very long. Generation of such entanglement apparently requires a long lived entanglement resource, because one has to wait until all pairs of stations are entangled. After this has been achieved, teleportation of entanglement (entanglement swapping) between stations can be used to extend the entanglement over the entire communication link length.

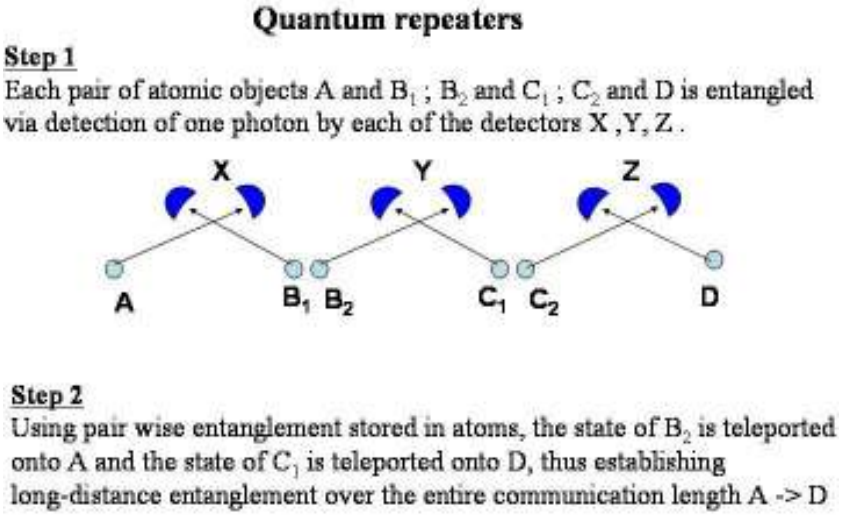


Figure 3

One of the possible realizations of the repeater is based on a single trapped ion (see article 15 for an overview of QIP with trapped ions). A first step towards this goal has been demonstrated by a team from Ann Arbor, University of Michigan, USA [5] (see **Figure 4**). Following the laser excitation, a single ion emits a photon. The photon is detected by one of the two detectors, one responding to the vertical polarization, V, and the other to the horizontal polarization, H, of the photon, as shown in the upper part of the figure. The resulting state of the spin polarization of the ion is then analyzed by optical-microwave analysis. It has been demonstrated that the state of the ion is entangled with the photon state,

showing for the first time a qubit-type entanglement of a photon and a long lived state of an ion.

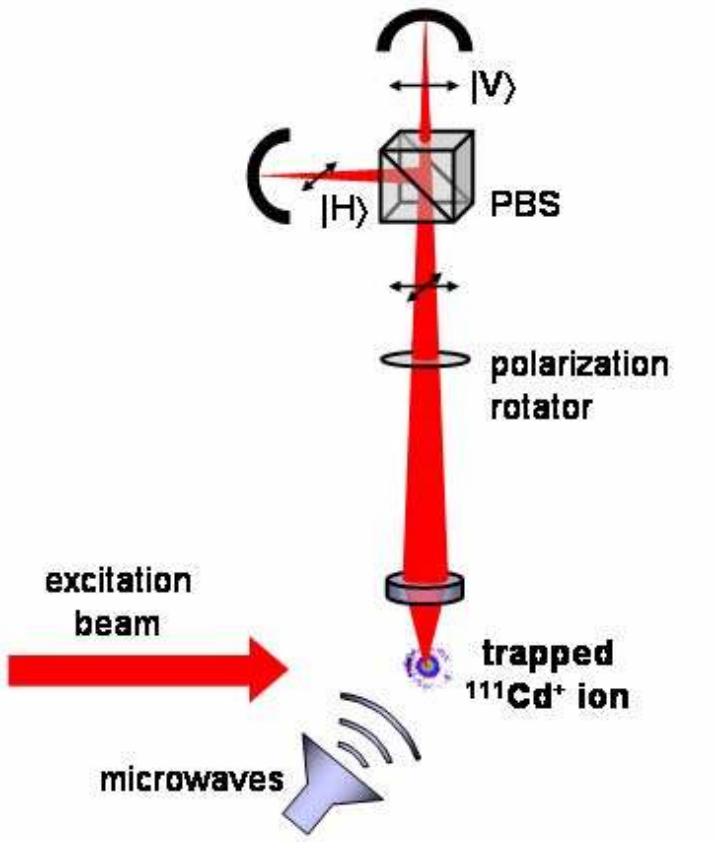


Figure 4

The entanglement described in [5] is generated probabilistically since most of the photons emitted by the ion do not hit detectors at all. However, this is not necessarily an obstacle for using this approach for a quantum repeater. One just has to wait a bit longer before all repeater stages work. The role played by a single ion in [5] can be played by an ensemble of atoms, which can be easier to implement. First experiments along those lines have been performed in the US [6].

The deterministic quantum memory for light described in the third section of the article may be capable of further improving the performance of a quantum repeater by increasing the probability of the photon teleportation at each stage of the repeater.

Conclusions

Classical information is transmitted by light and received and processed by material devices, such as detectors and computers. Likewise, *quantum* information is transmitted with light and processed in atom-based quantum processors. Transfer of fragile quantum states between light and atoms requires a special kind of interface with entanglement as a key ingredient. Light-atoms quantum interface capable of transferring quantum information from light to atoms has been under active development worldwide in the past few years. European researchers have contributed to some of the most important proposals and experimental demonstrations in this area of research. Future progress will allow building prototype long distance quantum networks. Quantum memory for light will also be necessary for certain types of quantum

computers. Ideas developed for **quantum** light-atoms interface may lead to reduced error rates and increased speed in **classical** fiber communication.

List of terms and acronyms

Spin: in this article is a magnetic momentum of an atom
Collective spin of an ensemble of atoms: a sum of all individual atomic spins
Quantum state: a mathematical construction which provides the most complete description of light or atoms

References

[1] Experimental long-lived entanglement of two macroscopic objects. B. Julsgaard, A. Kozhekin, and E. S. Polzik, *Nature*, **413**, 400 (2001)

[2] Quantum memory for photons: dark-state polaritons. Fleischhauer M., Lukin M. D. *Phys. Rev. A*, **65**, 022314 (2002)

[3] Experimental demonstration of quantum memory for light. B. Julsgaard, J. Sherson, J. Fiurášek, J.I. Cirac, and E.S. Polzik, *Nature*, **432**, 482 (2004)

[4] Quantum repeaters: The role of imperfect local operations in quantum communication. H.J. Briegel, W. Dur, J.I. Cirac, and P. Zoller, *Physical Review Letters*, **81**, 5932-5935 (1998)

[5] Observation of entanglement between a single trapped atom and a single photon. B.B.Blinov, D.L. Moehring, L.M. Duan and C. Monroe. *Nature,* **428**, 153-157 (2004)

[6] Generation of nonclassical photon pairs for scalable quantum communication with atomic ensembles, Kuzmich A., Bowen W.P., Boozer A.D., Boca A., Chou C.W., Duan L.M., and Kimble H.J., *Nature* **423**, 731-734 (2003); Shaping quantum pulses of light via coherent atomic memory, M.D. Eisaman, L. Childress, A. Andre, F. Massou, A.S. Zibrov, M.D. Lukin. Physical Review Letters **93**, 233602 (2004)

Projects funded by the European Commission and related to the work in this article:

CAUAC
Cold Atoms and Ultra-precise Atomic Clocks
Start date: 01/05/2000
End date: 30/04/2004
Project web site: http://volt.dfm.dtu.dk/cauac/
Contact Person: Dr. Jes Henningsen, Danish Institute for Fundamental Metrology, JH@dfm.dtu.dk

QUICOV
Quantum Information with Continuous Variables
Start date: 01/01/2000
End date: 30/06/2003
Project web site: http://kerr.physik.uni-erlangen.de/quicov/
Contact Person: Prof. Gerd Leuchs, Institute of Optics, Information und Photonics, University of Erlangen-Nuremberg, leuchs@physik.uni-erlangen.de

COVAQIAL
Continuous **Va**riable **Q**uantum **I**nformation with **A**toms and **L**ight
Start date: 01/09/2004
End date: 31/08/2007
Project web site: http://www.ulb.ac.be/project/covaqial/
Contact Person: Prof. Nicolas Cerf, Ecole Polytechnique, Université Libre de Bruxelles, ncerf@ulb.ac.be

Projects funded by National initiatives or organizations and related to the work in this article:
QUANTOP
Danish National Research Foundation Center for Quantum Optics
Start date: 01/09/2001
End date: 31/07/2006
Project web site: http://quantop.nbi.dk/
Contact person: Eugene S. Polzik, Niels Bohr Institute, Copenhagen University, polzik@nbi.dk

Contact information of the authors of this article:
Eugene S. Polzik
Niels Bohr Institute
Copenhagen University
Blegdamsvej 17
Copenhagen, 2100
Denmark
Email: polzik@nbi.dk
Web page: http://quantop.nbi.dk/qoptlab.html

Photonic engineering for quantum information processing

Ian Walmsley
Ian Walmsley **is** Professor of Experimental Physics and Head of Atomic and Laser Physics.Department of Physics at the University of Oxford, Clarendon Laboratory in Oxford, UK. His research is in the area of quantum and nonlinear optics. He is a Fellow of the Institute of Physics, UK, the American Physical Society and the Optical Society of America. He is also former US National Science Foundation Presidential Young Investigator. Ian Walmsley is a member of the Management Team of the UK QIP IRC, and former Director of the MURI Center for Quantum Information, a multidisciplinary research collaboration in the USA. He is former Professor of Optics and Director of the Institute of Optics, University of Rochester, Rochester, NY, USA.

Konrad Banaszek
Konrad Banaszek works at the Institute of Physics, Nicolaus Copernicus University, Toruń, Poland. Joined the faculty of the Institute after holding a Junior Research Fellowship at St. John's College, Oxford. He is doing research in the areas of quantum optics and quantum information science. In 2001 he won the European Physical Society Fresnel Prize in fundamental aspects. He is a member of the National Laboratory for Atomic, Molecular, and Optical Physics in Toruń, Poland.

Abstract

Photons offer one potentially important platform for encoding and manipulating information using the rules of quantum physics. In order to realise this potential, they must interact with each other – something that they are not normally inclined to do. However, it is possible using a combination of standard optical elements and detectors to synthesize an effective interaction provided the photons have the right character. An important component of current research is the drive to develop sources of photons that exhibit the right properties.

Introduction

The photon plays a central role in emerging quantum technologies, from imaging and precision measurement to communications and computing. The ability to generate individual photons of the appropriate character is therefore of paramount importance. Photonic technologies exploit both the wave and particle-like properties of these quantum entities. In cryptography, for instance, the indivisible nature of the photon ensures the security of the transmission. In quantum communications, however, the wavelike properties of superposition are important also.

Because both aspects are important, care must be taken to engineer these properly otherwise the basic physical phenomena that are at the heart of these applications will not function as required, leading to the failure of the technology itself. Therefore at present attention is being paid to how photons can be engineered, and to what kind of sources are most appropriate for the several different applications.

The issues are that the light generated by these sources must be exactly one photon, without any possibility that it could be zero or two. Moreover, these individual photons must be very tightly controlled – they must, for example, have the same color, arrival time, duration, bandwidth, polarization, etc.

The reason for this is that the photons must be capable of interfering with each other. The phenomenon of quantum interference relies both on the wavelike properties of the photons and their particle-like properties, and is at the heart of all of the quantum information processing schemes based on optics. In order for such schemes to work properly, the individual photons used in the computer must all be exactly alike, not distinguishable in any way, even in principle.

Wave interference

In broad terms, quantum information processing exploits the subtle interplay between wave- and particle-like properties of quantum systems. Optical radiation is a good example of this quantum mechanical wave-particle duality. Young's experiment, in which light diffracted from a pair of narrow slits generates a beautiful pattern of interference fringes, leaves little doubt that light should be described in terms of waves. On the other hand, the photoelectric effect, in which light illuminating a metal electrode ejects a discrete number of electrons with a characteristic energy distribution hints towards the particle nature of light, a feature that can be unambiguously confirmed in more elaborate experiments. Quantum mechanics reconciles both points of view using an advanced mathematical apparatus that enables to integrate the wave and the particle aspects of microscopic objects into one consistent physical theory.

When preparing quantum systems for quantum information processing applications, we need to consider simultaneously of their wave and particle characteristics. We illustrate this point by discussing first the wave behaviour of light in a simple experiment shown schematically in **Figure 1(a)**. In this experiment, we take a glass plate covered on one side with a thin layer of silver which transmits half of the incident light and reflects the remaining half. Suppose now that we illuminate both sides of the plate with identical light beams. Each beam, represented in **Figure 1(a)** as a wave, will generate a smaller outgoing wave on each side of the plate. A careful calculation shows that one of the four outgoing partial waves will have its maxima and minima flipped with respect to the incident wave that generated it. If we now want to find out the amount of light that will leave through each side of the plate, we need to superpose both

the partial waves that are generated on this side. We see that on one side the two waves will add up generating a stronger wave, whereas on the other side the two waves will cancel each other because one of them is flipped upside down. These are respectively the effects of constructive and destructive interference.

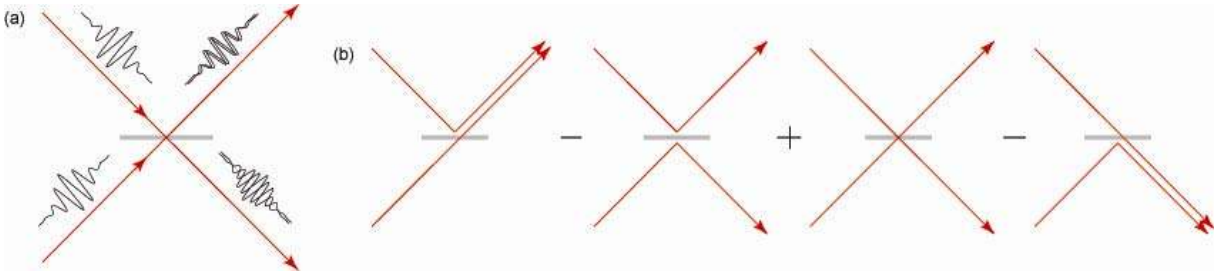


Figure 1
(a) Interference of two classical waves at a beam splitter. **(b)** The four possible paths for combining two photons at a beam splitter.

A necessary condition for the interference between the incident waves is that they must generate completely indistinguishable outgoing partial waves; that is, we cannot tell where the wave came from just by looking at its shape after the plate. Therefore the incident waves must be prepared in such a way that after the transmission or reflection from the plate they occupy exactly the same region in space, they begin and end at the same time, and oscillate with the same frequency. If any of these conditions is not satisfied, the amplitudes of the outgoing partial waves cannot be added or subtracted coherently, and the quality of interference deteriorates. The easiest way to ensure that both the incident beams share the same characteristics is to derive them from the same source. This can be done with another half-silvered plate which splits a single beam into two waves that are then directed onto the glass plate discussed above.

Quantum cryptography

So far, we have been able to understand the operation of the experimental setup depicted in **Figure 1(a)** using only notions of the wave theory. However, as we said at the beginning, we now have compelling experimental evidence that light is composed of discrete portions of energy, called photons. The number of photons contained in a light beam can be in principle measured by sending it into a metal electrode and counting the number of electrons it ejects. Such a process, although very difficult to implement in practice, underlies the operation principle of single-photon detectors, reviewed in article 5. When we perform photon counting with a typical light source such as a laser or a light bulb, we find that the number of photons varies greatly from one experimental realization to another. This means that the photon number is not a well-defined quantity and that is has to be described by a statistical distribution.

Imagine however that we have a light source that produces a beam containing exactly one photon, and that we send it to one beam splitter and then interfere the outputs using the setup shown in **Figure 1(a)**. A single photon, being an elementary portion of optical radiation, cannot be split by the first plate into smaller bits. (As we discuss later, a splitting process can be realized in non-linear optics, but it dramatically changes properties of the input photon.) Therefore there will be a chance for the photon to go through either the upper or the lower path in the interferometer, and if we performed a photon number measurement in each path we would find that the photon has taken one of the paths, but of course never both of them at

once. However, the state of the photon after the first half-silvered plate will not be just a mixture of these two possibilities. Quantum mechanics tells us that the state of the photon is described by a set of probability amplitudes. Furthermore, in the present case these probability amplitudes are given by the partial waves introduced in the previous section. The probability that the photon will be detected in a given path of the setup is proportional to the intensity of the corresponding partial wave. Following this rule, the photon will leave through the definite output port of the interferometer as in the classical case discussed previously.

The interference of wave-like probability amplitudes for a single photon forms the basis of operation for quantum cryptography. The sender prepares a superposition of a single photon between two paths distinguished by a certain degree, such as time delay, polarization, or spatial localisation as in our example. The quantum mechanical state of the photon can be modulated by introducing a small delay between these two paths. The receiving party can then try to identify the state of the photon by bringing these two paths together and making them interfere. Unambiguous identification is possible if perfectly destructive interference takes place on one of the output ports and consequently the behaviour of the photon at the exit of the interferometer can be predicted with certainty. This simple reasoning illustrates requirements for light sources used in quantum cryptography [1]. On the one hand, they should emit pulses containing exactly single photons. On the other hand, we need to take care of the wave properties of these pulses (or in quantum-mechanical terms, of the spatio-temporal probability amplitudes describing the photons) to ensure good interference on the output.

Linear-optics quantum computing

The requirements for interference become more stringent when we start with a number of single photons beams and bring them to interfere with one another using half-silvered plates. Such an experimental procedure is needed to build a linear-optics quantum computer, as it implements multiparticle interference which underlies the power of quantum computing [2]. The most elementary version of multiparticle interference is when two single photons fall onto two sides of a half-silvered plate. The photons, being quantum particles, then "stick together", always leaving via the same port of the beam splitter. This effect can be explained with the help of **Figure 1(b)** depicting four possible two-photon paths: both the photons leaving through the upper port, both the photons leaving through the lower port, both the photons are transmitted and leave through separate ports, finally both the photons are reflected and also leave through distinct ports. Each one of these possibilities is described by a certain probability amplitude. It turns out that if the last two cases (both photons transmitted or both photons reflected) are indistinguishable on the output, their probability amplitudes will cancel each other. This is a form of quantum-mechanical destructive interference, but between two-photon events [3].

This type of interference is more difficult to implement experimentally, as in the most general case we would like to interfere photons that have no common history between them. In the case of single-photon interference we brought to overlap "two halves" of the same photon. Consequently, if our photon varied in some of their properties from one run to another, this did not affect the interference as in every single realization the two components were identical. In multiparticle interference, every photon used in the experiment must be engineered to be exactly the same that is described by identical spatio-temporal probability amplitudes, in order to be able to interfere with other photons.

Engineering the shape of the photon

There are two general approaches to generating single photons with well-defined spatio-temporal probability amplitudes. The first is to take a single atom whose electron is in an excited state. When the electron decays to the ground state, it emits a single photon. The important ingredients in this approach are obtaining a lone, isolated atom, and making sure that the photon it emits does not go all over the place, but is concentrated in the direction that is needed for the application. This is the method of cavity quantum electrodynamics (or cavity QED), and can in principle provide single photons "on demand".

The second method uses one photon, the ancilla, to announce, or "herald", the presence of a second photon. The key ingredient of this method is a source of photons that are siblings, in the sense that they are always generated together. Such a source is made up of a large number of atoms, each of which is very weakly excited, in contrast to the case of the single atom source. By weakly excited, we mean that only a few of the many atoms will be in an excited state, and it will be impossible to know which of them are. Nonetheless, when one of these atoms decays back to the ground state, it emits two photons, rather than one. One of these is used as the herald photon, whose registration on a detector signals the availability of the other.

A single atom can be obtained in several ways. One way is to cool a cloud of atoms using laser scattering, and drop them carefully into a "trap" made of light. If the atoms slowly dribble out of the cloud into the trap, then it is often possible to select one of them by looking at the scattering it produces from a probe laser beam. Another way is to use the excitations in a solid to mimic the single atom. For example, in a semiconductor microstructure, electrons may be confined to a very small region of space. In this case the state the occupy take on the discrete character of atomic spectra rather than the continuous nature of normal semiconductor absorption. The states are most atom-like when the electrons are confined in all three dimensions, in so-called quantum dots [4]. Other atom-like excitations in solids can also be used, for example, a defect in a crystal that has been damaged by injection of dopant atoms, such as the nitrogen-vacancy center (NV) in diamond [5].

The direction of photon emission is engineered by enclosing the atom or quantum dot in an optical cavity consisting of two mirrors. An atom in free space normally radiates into almost 4π steradians, and so the photon spreads out into all space, like a wave from a stone thrown into a pond. This means that a small detector some distance from the atom will not receive much of the radiated power – effectively the probability that it will register a photon is very small. This situation can be improved by surrounding the atom by spherical mirror – in which case all the power radiated by the atom will be reflected back toward it. If, however, there is a small hole in the sphere, then eventually all the light will leak out of this hole, so a small detector placed there will register a single photon emitted by the atom with near certainty. Although it is impractical to surround an atom be a spherical mirror, the same effect can be achieved by surrounding it with two sections of a sphere – two mirrors – that look to the atom to be very large. If this is done carefully, then the photon emitted by the atom will have a high probability of being emitted through one of the mirrors in a nice collimated beam. At the same time the temporal shape of the photon will be set by how many times it bounces back and forth between the two mirrors before escaping [6]. This constriction of the way in which the photon may be emitted can be called "vacuum engineering", since it consists of structuring the possible modes that the photon sees.

The second approach uses a process of nonlinear optics, specifically parametric down-conversion, in which a so-called pump beam (with, say, a wavelength of 400 nm) splits into

two daughter photons (with wavelengths near 800 nm), in a crystal made from favorable atoms. The reason that a herald is needed is because the generation of the photon pairs is inherently random. Most times that the pump beam is applied nothing happens, and sometimes a pair of photons is generated, though it is not possible to say beforehand which application of the pump beam will yield the photons. This process yields photons with spatio-temporal amplitudes favourable for detection even without a cavity [7]. This is because many atoms take part in the process, all radiating in phase as shown in **Figure 2**. As it is inherently impossible to tell which atom will generate the photons, their probability amplitudes interfere constructively and combine to form a single beam propagating in well-defined direction.

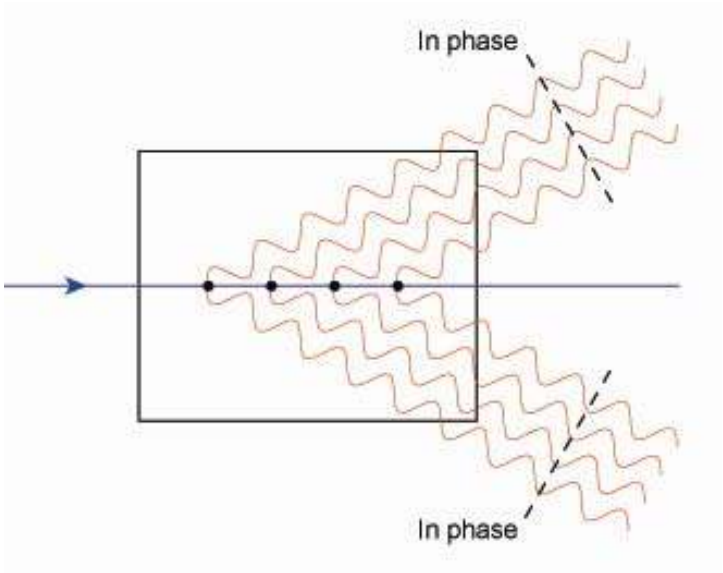


Figure 2
Production of photon pairs in a nonlinear crystal. Multiple generation paths from many atoms lead to well-defined beams.

There is a need for vacuum engineering here, too, though. The reason is that the photons are not only correlated in the sense that one photon indicates the presence of a second, but also because the wavelength (or color) of one photon indicates the wavelength of the second. This can easily be understood by energy conservation – if the pump beam has a very well defined frequency, ω, then each of its photons has a well-defined energy $\hbar\omega$. The sum of the energies of the daughter photons must be exactly that of a pump photon. Typically, however, the frequency of the individual daughter photons is not well defined, only the sum is.

This correlation is a liability for single photon preparation, because it is actually a quantum correlation, or entanglement, between the two photons. This means that the photons do not individually have a well-defined state, as discussed in article 2. Thus when one of them is measured, and its frequency is learned, this "collapses" the state of the other onto a specific frequency. The measurement of the herald will, however, yield a different frequency on each run of the experiment, so that the frequency of the heralded photon will also vary randomly from run to run. Therefore two such identical sources run in parallel to generate two heralded photons will usually generate two very different photons – they will have random, and most likely quite different, frequencies. This means that they will not interfere, and will be useless for quantum information processing [8]. At present the most common method of avoiding the problem is simple – throw away all of the herald photons that do not have a pre-selected

frequency. This ensures that the signal photons are all the same, and are suitable for QIP, at the expense of a large number of wasted photon pairs.

Although we have concentrated on frequency here, similar arguments hold for the other properties of the photons; their spatial extent and their polarization. Therefore great care is needed in designing sources of this kind for applications in QIP. Fortunately a number of strategies for source engineering are possible, and it is possible to circumvent this problem. In the future this aspect of heralding will need to be explored more thoroughly experimentally.

Conclusions

Photonic quantum information processing requires sources of precisely characterized photons. These will be single photon wavepackets, with prescribed spectra, spatial shapes and polarizations. Since the promise of the applications in quantum cryptography, quantum communications and quantum computing is so large, and the pay-offs attractive, a good deal of research effort is now being invested in designing and building such sources. Within the next decade, we expect that these will be available as standard laboratory items.

List of terms and acronyms

QIP: quantum information processing
HOM: Hong-Ou-Mandel

References

[1] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden Rev. Mod. Phys., **74**, 145 (2002)
[2] E. Knill, R. LaFlamme and G. Milburn, Nature, **409**, 46 (2001)
[3] C. K. Hong, Z. Y. Ou and L. Mandel, Phys. Rev. Lett., **59**, 2044 (1987)
[4] A. J. Shields, R. M. Stevenson, R. M. Thompson, et al. Phys. Status Solidi B **238**, 353 (2000); C. Santori, D. Fattal, J. Vukovic, G. S. Solomon amd Y. Yamamoto, Nature, **419**, 594 (2002)
[5] C. Kurtsiefer, S. Mayer, P. Zarda, H. Weinfurter, Phys. Rev. Lett., **85**, 290 (2000)
[6] A. Kuhn, M. Hennrich, G. Rempe, Phys. Rev. Lett., **89**, 067901 (2002); J. McKeever, A. Boca, A. D. Boozer, *et al.* Science **303**, 1992 (2004)
[7] A.B. U'Ren, C. Silberhorn, K. Banaszek and I. A. Walmsley , Phys. Rev. Lett. **93**, 093601 (2004)
[8] A. B. U'Ren, K. Banaszek and I. A. Walmsley, Quant. Info. Comput., **3**, 480 (2003)

Projects funded by National initiatives or organizations and related to the work in this article:
QIP IRC
Quantum Information Processing Interdisciplinary Research Collaboration
Start date: 01/04/2004
End date: 31/03/2009
Project web site www.qipirc.org
Contact Person: Andrew Briggs, University of Oxford, andrew.briggs@materials.oxford.ac.uk
Contact information of the authors of this article:
Ian A. Walmsley
Department of Physics

University of Oxford
Clarendon Laboratory
Parks Rd.
Oxford
UK
Email: walmsley@physics.ox.ac.uk
Web page: http://www.ultrafast.physics.ox.ac.uk

Konrad Banaszek
Institute of Physics
Nicolaus Copernicus University
Ul. Grudziądzka 5
PL-87-100 Toruń
Poland
E-mail: kbanasz@phys.uni.torun.pl
Web page: http://www.phys.uni.torun.pl

Semiconductor sources of single photons and photon pairs

Andrew Shields
Andrew Shields is the leader of the Quantum Information Group at Toshiba Research Europe Ltd in Cambridge, UK. His research interests are in optoelectronics, quantum optics and the applications of quantum information technology. He is a member of the following EU-funded IST projects: RAMBOQ, SAWPhoton and SECOQC. He is also the coordinator of the UK DTI funded Q-LED Project. Andrew Shields is industrial collaborator of IRC in QIP and a member of EPSRC Materials Strategic Advice Team.

Izo Abram
Izo Abram is the Head of Photonics and Quantum Electronics Group in the Laboratory for Photonics and Nanostructures - CNRS, Marcoussis, France. He is working on quantum and nonlinear optics, and on semiconductor nanostructures. He is the coordinator of the EU-funded IST project S4P (FP5) and of FP6 ERA-Net coordination action NanoSci-ERA. He is a member of the following national projects on semiconductor quantum optics: NanoQUB, POLQUA and BISQUE.

Abstract

For quantum optics to have an impact outside the laboratory it is essential to develop practical sources of non-classical light. Integration of nanometer-scale quantum dots inside a conventional semiconductor light emitting diode (LED) allows the realization of an LED for single photons. Semiconductor processing technologies can also be used to embed the quantum dot in a high quality optical cavity to strongly enhance the radiative decay rate and produce pairs of indistinguishable photons. The applications for these novel quantum light sources include single photon quantum cryptography, photonic quantum logic, quantum imaging and optical metrology.

Introduction

Photons are tiny amounts of electromagnetic energy that cannot be broken down to smaller fractions. In other words, they are the "quanta" or "particles" that make up light. They are created whenever energetic electrons (called "excited" electrons, in physics) in atoms, molecules or solids "fall" to lower-energy states. The energy thus released from each electron is carried away as a photon.

In an ordinary macroscopic source of light, billions and billions of electrons lose energy, at any one time, to produce billions and billions of photons. Even in a faint 1 Watt light bulb, some 10^{15} (a million billion) visible photons are emitted every second.

While for most practical uses we need to shine huge numbers of photons on an object to see it, in recent years a lot of research has gone into developing the ultimate faint light source, a device that emits only one photon every time it is turned on. But what good is such a faint source in which we can barely "see" the light? The answer is that it lets us see all the strange quantum properties of light, such as "uncertainty", "complementarity", "superposition" or "entanglement", and thus opens up perspectives in the emerging field of Quantum Information that relies on these quantum features for coding, transmitting or processing information. This field is inaccessible to traditional, macroscopic light sources because the statistics associated with the very large number of photons washes out the individual quantum behaviour. In macroscopic sources, all we can see is an averaged-out classical result and we cannot access the attributes of each individual photon.

Optically pumped single photon sources

In order to make a single-photon source, we have to put at the heart of the device a very small emitter, in which only one electron can "fall" to a lower-energy state. Initially, setups delivering single photons were built around a single atom or a single molecule, either isolated in space or embedded in a crystal as an "impurity". One of the most successful devices was

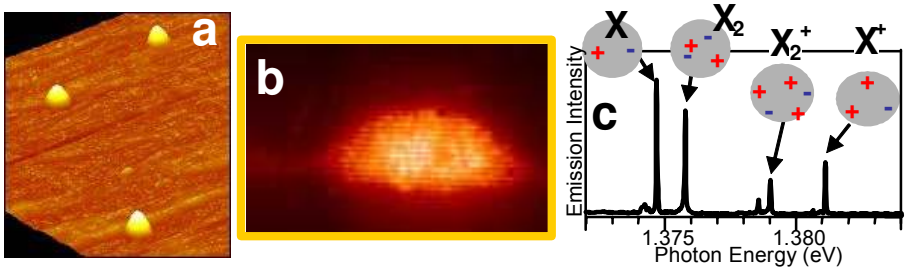


Figure 1 : (a) image of quantum dots on growth surface recorded in atomic force microscope; (b) STM cross-sectional image of dot embedded in semiconductor (courtesy of P.Koenraad, Eindhoven) and c) typical emission spectrum of dot showing sharp exciton emission lines

based on a single nitrogen "impurity" atom located next to a vacant site (that is, next to a missing carbon atom) in a diamond crystal. A more sophisticated source of single photons, that permits to tailor the properties of the emitted photons to the particular needs of an application, can be built out of semiconductors, by exploiting the mature technology that has been developed for microelectronics, and pushing it even further, well beyond the most advanced specifications needed for microelectronics. Many of these devices were developed through the sponsorship of the EC, which funded two of the earliest research programmes in this area in the FP5 projects S4P and SAWPHOTON.

Semiconductor single-photon sources are build around a single "quantum dot", like those imaged in **Figures1a and 1b**, which is a small island of one semiconductor (usually Indium Arsenide, InAs) having dimensions of the order of 20 nm (i.e. some 100 atoms) across and height 2 or 3 nm (corresponding to some 10 to 15 atoms), embedded in a sea of another semiconductor, usually GaAs. Thanks to its small size, a quantum dot has few electrons that can become energetic. At this point we shall introduce some semiconductor jargon – and physics – by saying that when an electron receives energy it passes into an "excited state" leaving behind it a positively-charged "hole". The electron-hole pair is often considered as a new particle called an "exciton". When the electron recombines with the hole and returns to its state of origin, the energy of the exciton is converted into a photon which leaves the quantum dot. Because of the strong attraction and repulsion of the electrons and holes, each combination of particles that can be trapped in the dot corresponds to a different value of the energy so that each photon that is emitted corresponds to a distinct wavelength (see **Figure.1c**).

The physics of the excitons in a quantum dot thus points to a simple scheme for the realization of a single-photon source: First, the semiconductor sample containing the quantum dot is exposed to a flash of light (for example, a laser pulse) and billions of photons from that flash are absorbed into the semiconductor creating billions of electron-hole pairs. A few of these pairs get trapped in the quantum dot where they can recombine and emit light. We can then collect only the light that is emitted at the one-exciton wavelength and we can be sure that it will consist of only one photon, since it will be the result of the recombination of only one (indeed, the last) exciton. Clearly, from the point of view of energy efficiency, a single-photon source is very bad. However, this energy expense is the price to pay to allow our macroscopic instruments to access the nanoworld and the quantum physics that governs it.

In order to prove that there is only one photon, there is a simple experiment that we can do: We can direct the emerging light pulse onto a half-silvered mirror (called "beam- splitter" by physicists) and use a single photon detector to monitor the light which is transmitted and another to detect that reflected (**Figure 2a**). If the light pulse contains only one photon it will either be transmitted or reflected by the beamsplitter, but cannot be split in two to activate both detectors at once. Thus the absence of any double clicks in **Figure 2b** for zero time delay between the two detectors is a direct proof that a single quantum dot emits only one photon every time it is excited, and is thus a good candidate for a single photon source.

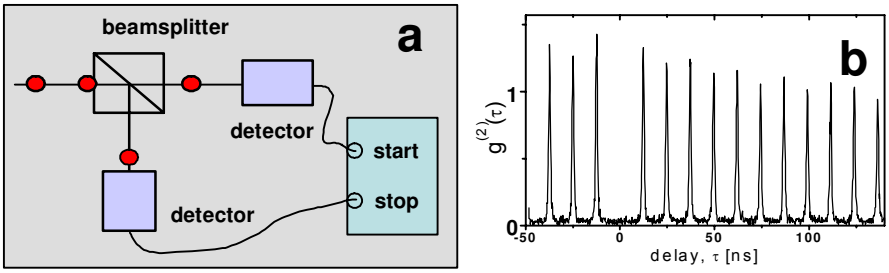


Figure 2 : (a) arrangement to test for single photon emission. The experiment records the number of photon pairs as a function of the time delay between the photons. (b) experimental proof of single photon emission from dot. The fact that the detectors never fire simultaneously proves they are emitted one at a time.

It should be noted that while the photon was postulated to exist by Max Planck and Einstein a century ago, it was this simple experiment, performed for the first time with atoms in 1976, that was the first direct experimental proof for the existence of the photon, as it was the first

electromagnetic phenomenon that could not be described in any way by the classical theory of electromagnetism.

Single Photon LEDs

A major advantage of using quantum dots as the photon generating centres is that they can easily be inserted during the growth of a semiconductor device. This allows us to place a quantum dot inside an ordinary semiconductor light emitter to create an LED for single photons, which can be driven by an applied voltage pulse rather than a pico-second laser. The attraction of an electrically-powered emitter is that it avoids the use of a pump laser, as well as its intricate alignment with the quantum dot. As a result, a compact and robust photon source can be designed suitable for use outside the laboratory. Such an LED for single photons could bring quantum light generation to the non-specialist, allowing a much wider uptake of the ideas of quantum optics and photonic quantum information.

In the single photon LED shown schematically in **Figure 3(a) and (b)**, the quantum dot is embedded between two electrical contact regions. The layer below the dots is doped with Silicon atoms which provide excess energetic electrons, while the region above is doped with Beryllium which removes electrons, leaving some "holes" in the lower energy band. Applying a voltage pulse between the two contacts attracts an electron from the lower contact and a hole from the upper contact into the quantum dot (**Figure 3c**). Trapped within the dot, the electron relaxes into the hole in the lower energy band, releasing its excess energy as an emitted single photon.

In order to direct the emitted photons in a useful direction (into an optical fibre, for example), a trick commonly used with conventional LEDs is employed of embedding the quantum dot within an optical cavity. The lower mirror of this cavity, grown inside the device, consists of a stack of alternating layers of GaAs and AlAs that reflects light at the dot emission wavelength, while the upper reflector is formed by the semiconductor/air interface. The cavity radically alters the angular emission profile from the device, producing a ten-fold increase in the photon collection efficiency, to values which are already useful for many applications.

Tailoring the structure of the quantum dot allows a wide range of single photon emission wavelengths to be designed. Most work so far has been done for small InGaAs quantum dot emitting around 900nm. Recently, however, researchers at TREL, Cambridge, funded by the FP6 project SECOQC, have developed a technique to grow large single quantum dots emitting around 1300nm, an important wavelength for fibre optical communications. This presents the prospect that single photons could be transmitted over

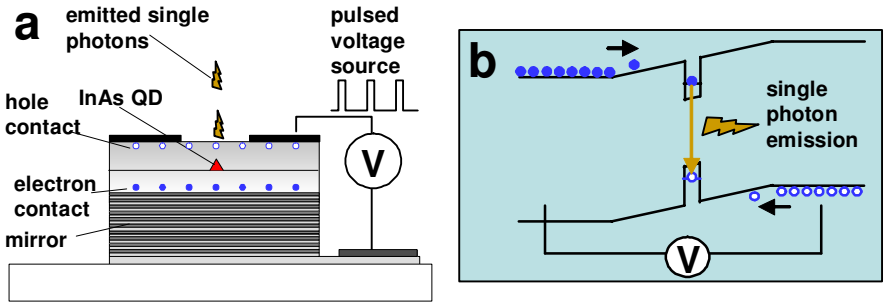


Figure 3 : (a) Schematic of a single photon LED and (b) application of a voltage pulse drives an electron and hole into dot causing a single photon to be emitted

long distances through optical fibres. Single photon generation has also been pushed to shorter wavelengths, using a CdSe (Bremen), InP (Berlin) or InGaN (Stanford/Tokyo) dot.

The first application for single photon LEDs is in quantum cryptography, a technique for securing communications on optical networks using single photons. This application is a means for distributing a digital cryptographic key with security guaranteed by the laws of quantum mechanics. This security, however, may be compromised if true single-photon pulses are not used. For example, key distribution systems that use faint laser pulses containing on average one photon, are vulnerable because the laser unavoidably sometimes emits two or more photons in a pulse. A true single photon source is therefore required to ensure security and achieve the highest possible bit rates and reach. Development of single photon LEDs for fibre based quantum cryptography is supported by the FP6 Integrated Project SECOQC, as well as a UK national project (Q-LED) supported by the UK Department of Trade and Industry.

Cavity effects

As well as directing more of the emission in a useful direction, cavities can speed up the emission of the photons. This is best seen in cavities where the photons are squeezed in all three spatial directions. In **Figure 4** the cavity consists of a semiconductor (GaAs) cylinder of diameter 400 nm (about one optical wavelength in GaAs) and of similar height. In order to improve the quality (or sharpness) of its resonances, both the top and bottom of the cylinder are bounded each by a high-reflectivity "Bragg mirror", consisting of an alternation of thin layers of two semiconductors GaAs/AlAs. When a quantum dot is embedded in a cavity with dimensions of the order of the wavelength, such as the GaAs cylinder described above, its emission will be affected by the resonance conditions in the cavity. In particular, the photon is emitted in a shorter time. This is particularly important in applications based upon quantum interference effects that require a good "coherence" (that is, a regularity of the electromagnetic oscillations that constitute the photon).

A frequent problem is that while the photon is being emitted by the quantum dot, the random thermal motion of the atoms in the semiconductor causes rapid and random fluctuations in the photon wavelength destroying the coherence of emitted photon. However, in a cavity of small enough volume and sharp enough resonances photon emission can happen faster than the random wavelength fluctuations due to the thermal motion of the semiconductor atoms, implying that the coherence of the emission is preserved, and the photons emerging from the cavity can undergo quantum interference effects, as we shall see below.

Even more startling effects are predicted to happen when the photon is squeezed into a sufficiently small volume to ensure a strong interaction with the dot. If the quality of the cavity is sufficiently high to ensure that the photon stays there for a long time before leaking

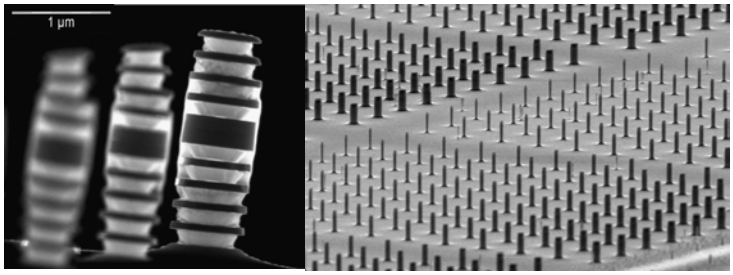


Figure 4 : (a) Micropillar cavities consisting of a central GaAs cylinder, bounded above and below by a multilayer mirror structure. Such cavities enhance the emission of quantum dots embedded in them. (b) Sample of micropillars of different dimensions.

out through one of the mirrors or the side, the emitted photon can be reabsorbed by the quantum dot, leading to a periodic oscillation where the energy is transferred back and forth between the excited electron and the photon. Evidence for this strong interaction between the dot and photon has recently been inferred from the wavelength of the emitted photon by teams in Wuerzburg, CIT, Pasadena and LPN, Marcoussis. Strong coupling between the photon and dot could allow the realisation of non-linear single photon devices, which would simplify photonic quantum logic circuits.

Quantum Logic with Photons

The FP5 FET Project RamboQ is developing the technology for scalable quantum logic based on photons. Photons have several advantages for quantum information processing. For example, they travel fast, do not lose their coherence when they travel, and thanks to the fibre optic communication industry, there are many components available for guiding and manipulating photons. The approach in linear optics quantum computing (LOQC) is to build logic gates from optical circuits consisting of ordinary optical components such as beamsplitters and polarization rotators. Although such a gate only sometimes gives the correct result, we can determine when it has been successful by a certain firing pattern in a number of extra single photon detectors. By stringing together successful gates in an ingenious way, it is possible to process quantum information encoded on the photons. Sources capable of delivering a regular stream of single photons are essential for scaling this technology beyond the single gate level. The first application is likely to be in future quantum communication networks using photons.

LOQC is an example of an application that requires quantum interference of two or more indistinguishable photons. In this quantum phenomenon, when two identical photons are incident simultaneously on the opposite input ports of a 50/50 beamsplitter, (see **Figure 5a**) they exit both together via the same output port. This occurs because the final state in which one photon exits through each output port of the beamsplitter is subject to "destructive interference" and can never happen. There are two ways in which this final state could be obtained: either both incident photons could be transmitted by the beamsplitter (Case iii in **Figure 5a**), or both photons could be reflected (Case iv). However, because the electromagnetic waves that constitute the photon are inverted when they are reflected by the beamsplitter, the amplitude of case (iii) exactly cancels with that of case (iv), killing the final state in which the two photons are separate.

Figure 5b depicts a fibre-optic version of the two-photon interference experiment using a quantum dot single photon source developed by the RamboQ Project. Notice in Fig. 5c that there is a reduction in the rate of co-incident counts in the two detectors when the two photons are injected into the arms of the 2x2 coupler at the same time, attesting to the possibility of the

two photons exiting together through the same output port. Notice also that the dip does not extend to zero, which means that photons are sometimes distinguishable and may leave the beamsplitter separately. This occurs because the thermal motion of the semiconductor atoms

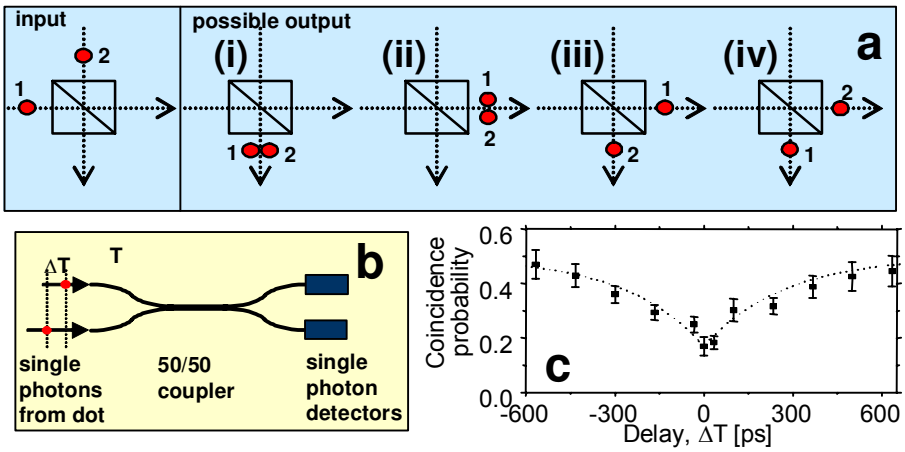


Figure 5 : (a) possible outcomes after inserting two photons into opposite ports of a beamsplitter. Outcomes (iii) and (iv) cancel, ensuring the two photons always leave in the same arm; (b) fibre version and c) experimental verification of 2-photon interference

degrades the coherence of the emitted photons and introduces a jitter in their time of emission rendering the two photons distinguishable. These effects can be overcome by further enhancing the cavity effects described in the previous section. Two-photon interference has also been observed using free space optics by the groups at Stanford and LPN, Marcoussis.

Conclusions

Ultimately this research seeks to create practical devices for generating single photons and photon pairs that can be used by non-experts outside of laboratory conditions. The impact of a generic technology for quantum light generation with a cost comparable to the light emitting diodes ubiquitous in today's imaging, information technology and communication systems would be immense. It would certainly stimulate and accelerate the use of quantum optics in a wide range of scientific disciplines. The famous experiments of quantum optics might become commonplace in undergraduate laboratories. It may even trigger a quantum optics industry in Europe with applications as diverse as secure communications, medical imaging and ultra-dense microchip fabrication. Just as it would have been impossible to predict the full impact of the diode laser, we may expect that many of the eventual applications of semiconductor quantum photonic devices are yet to be discovered.

List of terms and acronyms

LED: light emitting diode
InAs: Indium Arsenide, the semiconductor material used to fabricate quantum dots
GaAs: Gallium Arsenide, the material used to grow most of the surrounding device layers
LOQC: linear optics quantum computing

References

[1] P. Michler, in *Single Quantum Dots Fundamentals, Applications and New Concepts* (Springer, Berlin, 2003).

[2] A. J. Shields *et al.*, *Nano-Physics and Bio-Electronics*, (Elsevier, Amsterdam, 2002).
[3] Proceedings of SPIE Mini-symposium on Photonics with Single Quantum Dot Devices (Photonics West 2005).
[4] Ph. Grangier and I. Abram, "*Single photons on demand",* Physics World, Feb. 2003.

Acknowledgements

We thank colleagues at TREL, LPN and University of Cambridge for providing the figures and the EC & National bodies for funding.

Projects funded by the European Commission and related to the work in this article:

S4P
Solid State Sources for Single Photons
Start date: 01/01/2000
End date: 31/12/2003
Project web site: http://www.iota.u-psud.fr/~S4P/
Contact Person: Izo Abram, CNRS/LPN, izo.abram@lpn.cnrs.fr

SAWPHOTON
Single Electron Source Generating Individual Photons for Secure Optical Communications
Start date: 01/05/2000
End date: 30/04/2003
Project web site http://ntserv.fys.ku.dk/sawphoton1/
Contact Person: Andrew Shields, TREL, andrew.shields@crl.toshiba.co.uk

RAMBOQ
pRobabilistic gAtes Making Binary Optical Quanta
Start date: 01/01/2002
End date: 31/12/2005
Project web site http://www.ramboq.net
Contact Person: Andrew Shields, TREL, andrew.shields@crl.toshiba.co.uk

SECOQC
Development of a Global Network for Secure Communication based on Quantum Cryptography
Start date: 01/04/2003
End date: 31/03/2007
Project web site http://www.secoqc.net
Contact Person: Andrew Shields, TREL, andrew.shields@crl.toshiba.co.uk

Projects funded by National initiatives or organizations and related to the work in this article:

Q-LED
Quantum Light Emitting Diode for Secure Communications
Start date: 01/04/2002
End date: 31/03/2005
Project web site http://www.osda.org.uk/projects/qled.html
Contact Person: Andrew Shields, TREL, andrew.shields@crl.toshiba.co.uk

POLQUA
POrtes Logiques QUAntiques utilisant des sources de photons uniques monomodes à base de semiconducteurs
Start date: 01/10/2002
End date: 30/09/2005
Contact Person: Izo Abram, CNRS/LPN, izo.abram@lpn.cnrs.fr

BISQUE
Boîtes quantIques Semi-conductrices et information QUantiquE
Start date: 01/10/2002
End date: 30/09/2004
Contact Person: Izo Abram, CNRS/LPN, izo.abram@lpn.cnrs.fr

Contact information of the authors of this article:
Andrew Shields
Quantum Information Group
Toshiba Research Europe Ltd
260 Cambridge Science Park
Milton Road
Cambridge
UK
Email: Andrew.shields@crl.toshiba.co.uk
Web page: www.quantum.toshiba.co.uk

Izo Abram
Laboratory for Photonics and Nanostructures
Centre National de la Recherche Scientifique
route de Nozay
Marcoussis 91460
France
Email : izo.abram@lpn.cnrs.fr
Web page : www.lpn.cnrs.fr

Quantum cryptography

Artur Ekert
Artur Ekert is the Leigh Trapnell Professor of Quantum Physics at the Department of Applied Mathematics and Theoretical Physics, University of Cambridge, UK. He has worked with and advised several companies and government agencies and has made a number of contributions to quantum information science, in particular to quantum cryptography, which he co-invented.

He was also a member of the EU-funded IST project QuComm that received the 2004 Descartes prize.

Abstract

Quantum cryptography offers new methods of secure communication. Unlike traditional classical cryptography, which employs various mathematical techniques to restrict eavesdroppers from learning the contents of encrypted messages, quantum cryptography is focused on the physics of information. The process of sending and storing information is always carried out by physical means, for example photons in optical fibres or electrons in electric current. Eavesdropping can be viewed as measurements on a physical object - in this case the carrier of the information. What the eavesdropper can measure, and how, depends exclusively on the laws of physics. Using quantum phenomena we can design and implement a communication system which can always detect eavesdropping. This is because measurements on the quantum carrier of information disturb it and so leave traces.

Introduction

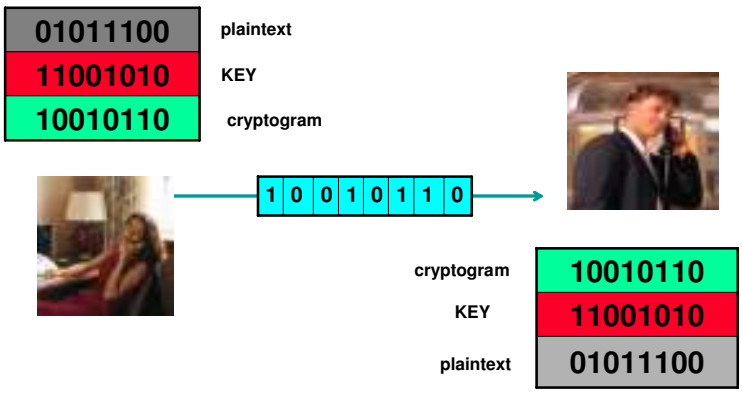
Quantum cryptography was discovered independently in the US and Europe. The first one to propose it was Stephen Wiesner (shown in the picture on the left), then at Columbia University in New York, who, in the early 1970's, introduced the concept of quantum conjugate coding. He showed how to store or transmit two messages by encoding them in two "conjugate observables", such as linear and circular polarization of light, so that either, but not both, of which may be received and decoded. He illustrated his idea with a design of unforgeable bank notes. A decade later, building upon this work, Charles H. Bennett, of the IBM T.J. Watson Research Center, and Gilles Brassard, of the Université de Montréal, proposed a method for secure communication based on Wiesner's "conjugate observables". In 1990, independently and initially unaware of the earlier work, Artur Ekert, then a Ph.D. student at the University of Oxford, discovered and developed a different approach to quantum cryptography based on peculiar quantum correlations known as quantum entanglement. Since then quantum cryptography has evolved into a thriving experimental area

and is quickly becoming a commercial proposition (see, for example, www.idQuantique.com, www.MagiQtech.com, or www.elsag.it).

This popular account of quantum cryptography covers the basic principles behind quantum key distributions.

Cryptographic keys and their distribution

Despite a long and colourful history, cryptography became part of mathematics and information theory only in the late 1940s, mainly as a result of the work of Claude Shannon (1916-2001) of Bell Laboratories in New Jersey. Shannon showed that truly unbreakable ciphers do exist and, in fact, they had been known for over 30 years. They were devised in about 1918 by an American Telephone and Telegraph engineer Gilbert Vernam and Major Joseph Mauborgne of the US Army Signal Corps, and are called either "one-time pads" or Vernam ciphers. Both the original design and the modern version one time pads are based on the binary alphabet.



The message, also known as a plaintext, is converted to a sequence of 0's and 1's, using some publicly known rule. (For example, Vernam used the five bit code designed by the Frenchman Emile Baudot). The key is another sequence of 0's and 1's of the same length. Each bit of the message, or the plaintext, is then combined with the respective bit of the key, according to the addition in base 2: 0+0=0, 0+1=1+0=1, 1+1=0. The key is a random sequence of 0's and 1's hence the resulting cryptogram - the plaintext plus the key - is also random and therefore completely scrambled unless one knows the key. The plaintext can be recovered by the addition (in base 2 again) of the cryptogram and the key.

In the example above the sender, traditionally called Alice, ads each bit of the plaintext 01011100… to the corresponding bit of the key 11001010… obtaining the cryptogram 10010110…, which is then transmitted to the receiver, traditionally called Bob. Both Alice and Bob must have two exact copies of the key beforehand; Alice needs the key to encrypt the plaintext, Bob needs the exact copy of the key to recover the plaintext from the cryptogram. An eavesdropper, called Eve, who has intercepted the cryptogram and knows the general method of encryption but not the key will not be able to infer anything useful about the original message. Indeed, Shannon proved that if the key is secret, the same length as the message, truly random, and never reused, then the one-time pad is unbreakable. Thus we do have unbreakable ciphers!

There is a snag, however. All one-time pads suffer from a serious practical drawback, known as the key distribution problem. Potential users have to agree secretly and in advance on the key - a long, random sequence of 0's and 1's. Once they have done this, they can use the key for enciphering and deciphering and the resulting cryptograms can be transmitted publicly, for example, broadcasted by radio, posted on Internet or printed in a newspaper, without compromising the security of messages. But the key itself must be established between the sender and the receiver by means of a very secure channel - for example, a very secure telephone line, a private meeting or hand-delivery by a trusted courier. Such a secure channel is usually available only at certain times and under certain circumstances. So users far apart, in order to guarantee perfect security of subsequent crypto-communication, have to carry around with them an enormous amount of secret and meaningless as such information (cryptographic keys), equal in volume to all the messages they might later wish to send. This is not very convenient.

Furthermore, even if a "secure" channel is available its security can never be really guaranteed. A fundamental problem remains because, in principle, any classical private channel can be monitored passively, without the sender or receiver knowing that the eavesdropping has taken place. This is because classical physics - the theory of macroscopic bodies and phenomena such as paper documents, magnetic tapes and radio signals - allows all physical properties of an object to be measured without disturbing those properties. Since all information, including a cryptographic key, is encoded in measurable physical properties of some object or signal, classical theory leaves open the possibility of passive eavesdropping, because it allows the eavesdropper in principle to measure physical properties without disturbing them. This is not the case in quantum theory, which forms the basis for quantum cryptography.

Before we discuss quantum methods for distribution of cryptographic keys let us mention a beautiful mathematical approach to the problem.

Public keys

Cryptologists and mathematicians tried very hard to eliminate the key distribution problem. In the 1970's, with the miniaturization of radio equipment, progress in computer technology, and a rapid growth of cryptographic communication the key distribution was turning into an expensive and logistical nightmare. It looked like the only way to send a key securely was to deliver it in person or via a courier. Banks employed special dispatchers, who would race across the country with padlocked briefcases, personally distributing keys to everyone that the bank would communicate with over the next few days. The cryptographic community accepted that the key-distribution problem might be unavoidable. However, this all changed in 1976 when Whitfield Diffie and Martin Hellman published their groundbreaking ideas about secure key exchange. The paper, which also referenced a related work by Ralph Merkle, was shortly followed by another elegant algorithm, today known as the RSA encryption, named after the three inventors, Ron Rivest, Adi Shamir, and Leonard Adleman. In December 1997, the British government revealed that these techniques were in fact discovered somewhat earlier by James Ellis and his colleagues Clifford Cocks and Malcolm Williamson working for the British Government Communication Headquarters (GCHQ). The basic idea behind a mathematical solution to the key distribution, know as public key encryption, is deceptively simple.

Public-key cryptosystems work on the principle of a safebox with two keys, one "public key" to lock it, and another "private key" to open it. Think about encryption in terms of locking a message inside a safebox and consider a scenario in which Bob designed the safebox with the two keys. Bob can produce many such safeboxes and make them easily available to anyone who may want to send secret messages to him. Bob's safeboxes come open with the locking (public) key attached to them. Alice can just pick up one of them, put her message in the box and lock it with the attached public key. Once the safebox is locked Bob is the only person who can open it because he has the unlocking (private) key. This key never leaves Bob, and so the key-distribution problem no longer exists

The mathematical safebox is based on the idea of a trapdoor function, i.e. a function that is very easy to compute one-way but its reverse is very hard. The public and the private key are two numbers that are related to each other, however, in order to derive the private key from the public key one needs to perform lengthy calculation which is tantamount to finding prime factors of large integers. Alice and Bob avoid the key distribution problem but unfortunately their security depends on unproved mathematical assumptions, such as the difficulty of factoring large integers.

Mathematicians believe (firmly, though they have not actually proved it) that in order to factorise a number with L decimal digits, any classical computer needs a number of steps that grows exponentially with L, that is to say, adding one extra digit to the number to be factorised generally multiplies the time required by a fixed factor. Thus, as we increase the number of digits, the task rapidly becomes intractable. The largest number that has been factorised as a mathematical challenge, i.e. a number whose factors were secretly chosen by mathematicians in order to present a challenge to other mathematicians, had 174 digits (as of January 2005). No one can even conceive of how one might factor, say, thousand-digit numbers by classical means; the computation would take many times as long the estimated age of the universe. However, all this applies only to classical computers. In the 1980s physicists asked what would happen if you could build a computer out of individual atoms and molecules. The world of atoms and molecules is governed by quantum mechanics and some quantum phenomena, such as quantum superpositions and quantum entanglement (we will return to quantum entanglement very soon), can support qualitatively new types of computation. Moreover, there are problems which are intractable to all classical computers but which can be efficiently solved on a quantum computer. In 1994 Peter Shor showed that factoring large integers is one of them! Thus once a quantum factorisation engine (a special-purpose quantum computer for factorising large numbers) is built public key systems will become insecure. Indeed, in one sense they are already insecure: any RSA-encrypted message that is recorded today will become readable moments after the first quantum factorisation engine is switched on, and therefore RSA cannot be used for securely transmitting any information that will still need to be secret on that happy day.

Admittedly, that day is probably decades away, but can anyone prove, or give any reliable assurance, that it is? Confidence in the slowness of technological progress is all that the security of the RSA system now rests on!

Polarized photons

We shall now leave mathematics and enter the world of quantum physics. Physicists view key distribution as a physical process associated with sending information from one place to

another. From this perspective eavesdropping is a set of measurements performed on carriers of information, in our particular case on polarized photons.

Light can be described in terms of both particles (photons) and oscillating electric fields. The direction of the oscillation is known as a photon's polarization and although photons can be prepared in infinite number of polarization states, only two directions of polarization, perpendicular to each other, can be distinguished in a single measurement. But how do we measure polarization?

If a polarized photon impinges on a birefringent crystal (such as calcite) it behaves in one of two ways depending on its polarization in relation to the crystal. The photon may pass straight through the crystal and emerge polarized perpendicular to the crystal's optic axis (we denote this polarization as ↔), or it may be shifted and emerge polarized along that axis (which we denote as ↕). If the photon entering the crystal is already polarized in one of these two rectilinear directions (↔ or ↕), it will undergo no change of polarization but will be deterministically routed into the straight or shifted path, respectively.

If a photon polarized at some intermediate direction enters the crystal, however, it will have some probability of going into each beam and will be repolarized according to which beam it goes into, forgetting its original polarization. The most random behaviour occurs when the photon is polarized halfway between ↔ and ↕, that is, at 45 (which we denote as ∴) or 135 degrees (denoted as_). Such photons are equally likely to go into either beam, revealing nothing about their original polarization and losing all memory of it.

Suppose you are told in advance that a given photon is polarized in one of the two "rectilinear" directions, vertical (↕ or horizontal (↔) without being informed of the specific polarization. Then you can reliably tell which direction by sending the photon into an apparatus consisting of a vertically oriented calcite crystal and two photo-detectors that can record single photons. The calcite crystal directs the incoming photon to the upper detector if it was horizontally polarized and to the lower detector if it was vertically polarized. Such an apparatus is useless for distinguishing diagonal (∴or _ photons, but these can be reliably distinguished by a similar crystal that has been rotated by 45 degrees from the original orientation. The rotated crystal, in turn, is useless for distinguishing vertical from horizontal photons. In general, by rotating the crystal by α degree one can reliably distinguish between photons polarized at α and 180-α degrees. However, different types of polarization are incompatible physical properties, i.e. a sharp value of rectilinear polarization (↕ or ↔) precludes any sharp value of diagonal polarization (∴or_) and vice versa.

It follows from this description that each type of polarization allows to encode one bit of information, with a simple denotation, e.g. horizontal polarization = 0, vertical polarization = 1, or polarization at 45 degrees = 0, polarization at 135 degrees = 1, or polarization at α degrees = 0, polarization at 180- α degrees = 1. Measuring polarization of a single photon always gives a binary outcome, either 0 or 1, however, for this encoding to be meaningful the receiver must know in advance which type of polarization was used to encode the bit. If I tell you that I am sending you one photon which carries one bit of information encoded either in rectilinear or diagonal polarization then the best you can do is to choose one of the two polarization measurements and record the outcome. I may tell you afterwards which type of polarization I used to encode the bit. If you measured this particular polarization you know the bit value, if not, the bit value is irretrievably lost.

Quantum entanglement

Quantum key distribution can be illustrated in terms of a peculiar coin tossing. If Alice and Bob are at the same location they can generate a random secret key by tossing an unbiased coin many times and recording the outcomes. If they are far apart they can achieve the same goal but with the help of magic quantum coins. Magic quantum coins come in pairs and if tossed they are always anti-correlated; when one lands head up the other lands tail up and vice versa. We never observe two head or two tails. This anti-correlation persists even if the two coins from the same pair are taken far apart and tossed at their respective distant locations. Such "non-local" correlations appear between two or more quantum particles, e.g. photons or atoms, when they are prepared in the so-called entangled state. For example, in a process called parametric down conversion (PDC) a photon from a laser beam enters a beta-borium-borate crystal and gets absorbed while it excites an atom in the crystal. The atom subsequently decays emitting two entangled photons whose polarizations are always opposite. Alice and Bob may receive one photon each and "tossing a quantum coin" amounts to testing photon's polarization.

Each photon in the entangled pair is in the state of undefined polarization but when the polarizations of the photons are measured they have opposite values, provided that the measurements are of the same type. For example, if Alice and Bob both measure rectilinear polarizations, they are each equally likely to record either a 0 (↔, horizontal polarization) or a 1 (↕, vertical), but if Alice obtains a 0, Bob will certainly obtain a 1, and vice versa.

But perhaps our source produces pairs of photons with polarizations chosen randomly between ↕↔ and ↔↕? It turns out that if Alice and Bob both measure diagonal polarizations their results are also opposite; they are each equally likely to record either a 0 (∴, 45 degrees diagonal) or a 1 (_, 135 degrees diagonal) but each time Alice obtains a 0, Bob obtains a 1, and vice versa. However, following our description of the polarization measurements above, we can see that if we prepare two photons with polarizations ↕↔ or ↔↕ then Alice and Bob will observe all possible outcomes, __, ∴∴, ∴_, and _∴ with the equal frequency. It is impossible to explain entanglement induced anti-correlations, observed for any two prescribed perpendicular polarizations at α and 180-α degrees, by assuming that any of the two photons has a specific polarization prior to the measurements. If they do we loose perfect anti-correlations. It is quite amazing that individual photons do not carry any bit values because their polarization is undefined, or, if you wish, completely randomized, but when measurements of the same type are performed on the photons they reveal two bit values that always differ; we obtain either 01 or 10.

Quantum key distribution

We can now describe the simple scheme for quantum key distribution based of distribution of entangled photons. The purpose of the scheme is for Alice and Bob to exchange a secret random key that they can subsequently use, as in the one-time pad, to send meaningful secret messages when the need arises. The scheme uses a quantum channel, through which Alice and Bob receive entangled photons from an external source, which may be controlled by an eavesdropper, in conjunction with a classical public channel, through which they exchange ordinary messages. An eavesdropper, Eve, is free to try to temper with the source. This is probably the most counter-intuitive key distribution protocol because it accommodates scenarios in which Eve herself distributes entangled quantum particles to Alice and Bob! Furthermore, she learns the entire contents of messages sent through the public channel but we assume that she could not disturb or alter these messages even if she wanted to.

Entangled photons fly apart from a source towards the two legitimate users, Alice and Bob, who, for each incoming photon, decide randomly and independently from each other whether to test rectilinear or diagonal polarization. A single run of the experiment may look like this

Alice	_	↕	↕	∴	↕	_	↕	∴	↕	↔	↔	↔	↔	∴	↕	∴	↔	↕	_	_
Bob	∴	∴	↔	_	↔	∴	↔	_	↔	_	↕	↕	∴	_	_	↕	↕	_	↕	∴

For the first pair both Alice and Bob decided to test diagonal polarization and their results are opposite. For the second pair Alice measured rectilinear polarization whilst Bob measured diagonal. In this case their results are not correlated at all. In the third instant they both measured rectilinear polarization and obtained opposite results, etc.

After completing all the measurements, Alice and Bob discuss their data in public so that anybody can listen including their adversary, Eve, but nobody can alter or suppress such public messages. Alice and Bob tell each other which type of polarization they measured for each incoming photon but they do not disclose the actual outcomes of the measurements. For example, for the first pair Alice may say "I measured diagonal polarization" and Bob may confirm "So did I". At this point they know that the results in the first measurement are opposite. Alice knows that Bob registered ∴ because she registered_, and vice versa. However, although Eve learns that the results are opposite she does not know whether it is ∴ for Alice and _ for Bob, or _ for Alice and ∴ for Bob. The two outcomes are equally likely, so the actual values of bits associated with different results are still secret.

Alice and Bob then test for entanglement. Polarization of entangled photons is always opposite if they both measured rectilinear or diagonal polarization and is random otherwise. They reveal the outcomes in all instances in which they made measurement of different types (shaded columns in the table below). These outcomes, which are subsequently discarded, should be uncorrelated.

Alice	_	↕	↕	∴	↕	_	↕	∴	↕	↔	↔	↔	↔	∴	↕	∴	↔	↕	_	_
Bob	∴	∴	↔	_	↔	∴	↔	_	↔	_	↕	↕	∴	_	_	↕	↕	_	↕	∴

They end up with shorter strings which should now contain perfectly anti-correlated entries. They check whether the two strings are indeed anti-correlated by comparing, in public, randomly selected entries (shaded columns in the table below).

Alice	_	↕	∴	↕	_	↕	∴	↕	↔	↔	∴	↔	_
Bob	∴	↔	_	↔	∴	↔	_	↔	↕	↕	_	↕	∴

Perfect anti-correlations indicates entanglement. The publicly revealed entries are discarded and the remaining results are translated into a binary string, following the agreed upon encoding e.g. as in the table below.

Alice	_	↕	↕	↕	∴	↕	↔	_
Bob	∴	↔	↔	↔	_	↔	↕	∴
KEY	1	0	0	0	0	0	1	1

Why is the key secure?

We have already mentioned that if any two photons are entangled then the individual photons have undefined polarization. If you wish, you may think about this situation as the individual photons having randomly chosen polarization. Hence there is no bit value encoded in the polarization prior to the measurement, which means there is nothing to eavesdrop on!

Let us be more specific and adopt the scenario that is most favourable for eavesdropping, namely we will allow Eve to prepare all the photons and send them to Alice and Bob! Eve's objective is to prepare the pairs in such a way that she can predict Alice's and Bob's results and that the pairs pass the anti-correlation test. This is impossible. Suppose Eve prepares a pair of photons choosing randomly one of the four states: ↕↔, ↔↕, ∴_ or _∴. Suppose it is ↕↔. She then sends one photon to Alice and one to Bob. Let us concentrate only on instances in which Alice and Bob measured the same type of polarization as only those instances contribute to the final key. If both Alice and Bob choose to measure rectilinear polarization on their respective photons then they obtain opposite results and Eve knows the outcomes; if they choose to measure diagonal polarization then, although the outcomes are random, they can still obtain opposite results with probability 50%. Although Eve knows, on average, every second bit of the key she will be discovered because this will result in 25% of errors when Alice and Bob check anti-correlations in their test for entanglement More technical eavesdropping analysis shows that all, however sophisticated, eavesdropping strategies are doomed to fail, even if Eve has access to superior technology, including quantum computers. The more information Eve has about the key, the more disturbance she creates.

The key distribution procedure described above is somewhat idealised. The problem is that there is, in principle, no way of distinguishing errors due to eavesdropping from errors due to spurious interaction with the environment, which is presumably always present. This implies that all quantum key distribution protocols which do not address this problem are, strictly speaking, inoperable in the presence of noise, since they require the transmission of messages to be suspended whenever an eavesdropper (or, therefore, noise) is detected. Conversely, if we want a protocol that is secure in the presence of noise, we must find one that allows secure transmission to continue even in the presence of eavesdroppers. Several such protocols were designed. They are based on two approaches, namely on purification of quantum entanglement, proposed in this context by Deutsch, Ekert, Jozsa, Macchiavello, Popescu, and Sanpera, and on classical error correction, pioneered by Dominic Mayers. Subsequently the two approaches have been unified and simplified by Peter Shor and John Preskill.

Conclusions

There is much more to say (and write) about the subject and the reader should be warned that this brief overview has only scratched the surface of the many activities that are presently being pursued under the heading of quantum cryptography. Experimental quantum cryptography has rapidly evolved from early demonstrations at the IBM T.J. Watson Research Laboratory in Yorktown Heights in the U.S. and the Defence Research Agency in Malvern, in the U.K. to several beautiful experiments that demonstrated full fledged quantum key distribution both in optical fibres and free space. Quantum cryptography today is a commercial alternative to more conventional, classical cryptography. However, let me stop here hoping that even the simplest outline of quantum key distribution has enough interesting science to keep you entertained for a while.

Projects funded by the European Commission and related to the work in this article:

TMR network on the physics of entanglement

EQCSPOT
European Quantum Cryptography and Single Photon Optical Technologies
Start date: 01/11/1998
End date: 31/10/2000
Project web site http://www.cordis.lu/esprit/src/28139.htm
Contact Person: Prof. J.G. Rarity, U. Bristol, john.rarity@bristol.ac.uk

EQUIP
Entanglement in Quantum Information Processing and Communication
Start date: 01/01/2000
End date: 31/12/2002
Project web site: http://www.equip.qipc.org/
Contact Person: Martin Wilkens, U Potsdam, martin.wilkens@physik.uni-potsdam.de

QuComm
Long Distance Photonic Quantum Communication
Start date: 01/01/2000
End date: 30/04/2004
Project web site http://www.imit.kth.se/QEO/qucomm/
Contact Person: Prof. A. Karlsson, KTH, Sweden, Andkar@imit.kth.se

QAIP
Quantum Algorithms and Information Processing
Start date: 04/01/2000
End date: 03/01/2003
Project web site: http://www.cwi.nl/projects/QAIP/
Contact person: Harry Buhrman, Stichting Matematisch Centrum, harry.buhrman@cwi.nl

RESQ
Resources for Quantum Information
Start date: 01/01/2003
End date: 31/12/2005
Project web site: http://www.ulb.ac.be/project/RESQ/
Contact Person: Serge Massar, Université Libre de Bruxelles, smassar@ulb.ac.be

TOPQIP
Topological Quantum Information Processing
Start date: 01/01/2003
End date: 31/12/2005
Project web site: http://isiosf.isi.it/research/project/Topqip/topqiplogo.htm
Contact Person: Paolo Zanardi, ISI Foundation, zanardi@isiosf.isi.it

ESF: program on "QUANTUM INFORMATION THEORY AND QUANTUM COMPUTATION"
Start date: 1999
End date: June 2004
Project web site: http://www.esf.org/esf_article.php?activity=1&article=26&domain=1
Contact person: Neil Williams

Projects funded by National initiatives or organizations and related to the work in this article:

EPSRC QIP Interdisciplinary Research Collaboration (2004-)
EPSRC Joint Infrastructure Fund Award, (2001-2004)
EPSRC research grant "Multiphoton Entanglement and Quantum Information" (1999-2002).

Royal Society, personal research grant (1993-2001).

Contact information of the authors of this article:
Artur Ekert
Leigh Trapnell Professor of Quantum Physics
DAMTP, University of Cambridge
Wilberforce Road, Cambridge CB3 0WA,
United Kingdom
Web page: http://cam.qubit.org/users/artur/
Tel: +44 1223 760394

Quantum cloning and key distribution with continuous variables

Nicolas Cerf
Nicolas Cerf is Associate Professor at ULB, where he heads the Centre for Quantum Information and Communication (QUIC). After having earned a Ph.D. in Physics at ULB in 1993, he was awarded a Marie Curie fellowship from the EC, and worked for two years as a post-doctoral research associate at the Division of Theoretical Physics in Orsay, France. His research then mainly concerned quantum many-body systems and quantum Monte Carlo methods. In 1995, he joined the California Institute of Technology, USA, to work on quantum computation and information theory, which then became his main research interest. In 1998, he was appointed as an Associate Professor at ULB, where he now teaches information and communication theory. He earned the Caltech President's Fund 1997 award, the Alcatel-Bell 1999 prize awarded by the Belgian National Fund for Scientific Research (FNRS), and a Fulbright award in 1999. He was member of the steering committee of the 5-year quantum information theory programme funded by the European Science Foundation, and is (or has been) involved in several QIPC projects under the EU-funded IST programme (EQUIP, QUIPROCONE, RESQ, SECOQC, COVAQIAL).

Philippe Grangier
Philippe Grangier is Directeur de Recherche at CNRS, and he is leading the Quantum Optics group in Institut d'Optique, Orsay. He got a Thèse de 3e Cycle in 1982 on Experimental Tests of Bell's Inequalities (under the supervision of Alain Aspect), and a Thèse d'Etat in 1986 on Experimental Studies on Non-Classical Properties of the Light, such as the production of single-photon states. After a post-doc in Bell Laboratories on squeezed states interferometry in 1987, he conducted many researches in quantum optics, and then in quantum information. He has been awarded prizes by Académie des Sciences (1987), French Physical Society (1988), Ernst-Abbe foundation (Carl Zeiss Award, 1990), and CNRS (Médaille d'Argent, 2002). Since the beginning of the 90's he has been involved in many European RTD projects, in the ESPRIT and then in the IST programs, as well as in Human Potential networks. He was the coordinator of two Research Training Networks, "Non-Classical Light" (1993-1996) and "QUEST" (2000-2004), and now he is in charge of the EU-funded IST FP6 Integrated Project "SCALA" (Scalable Quantum Computing with Light and Atoms). His research activities presently include various aspects of quantum cryptography, and the manipulation of single trapped atoms for quantum information processing.

Abstract

Quantum information with continuous variables is a paradigm which has attracted a growing interest lately, as a consequence of the prospect for high-rate quantum communication systems that may result from the use of standard telecommunication components. After introducing the concept of quantum continuous variables in optics, we turn to the fundamental impossibility of cloning continuous-variable light states, a result which is at the heart of quantum key distribution. We then present state-of-the-art quantum key distribution systems relying on continuous variables, with a special emphasis on the experimental demonstration of protocols using coherent light states. Finally, we briefly review the recent security proofs of these cryptographic protocols.

Introduction

Over the last years, there has been a lot of interest about the possibility to realize quantum informational and computational tasks with so-called **continuous variables**. In short, the idea is to use, as quantum information carriers, physical quantities that have a continuous spectrum (such as the quadrature amplitudes of the quantized light field) instead of binary quantities (such as the polarization state of a single photon). This research direction was triggered by the theoretical proposal for continuous-variable quantum teleportation, which was quickly followed by its experimental demonstration [1].

As is well known, the central concepts of quantum information theory such as quantum teleportation, quantum cryptography, or quantum algorithms have been initially developed for binary quantum carriers (quantum bits). This is indeed the most natural way to go in order to build the quantum counterpart to classical informational processes. However, the use of continuous-variable quantum systems, which may involve many photons in a light field, has some potential advantages over single-particle quantum systems. Such advantages lie in the prospect for higher optical data rates and simpler processing tools, based upon standard telecommunication techniques. Another significant strength of this paradigm is that the light-atoms quantum interface can be designed for continuous variables, so that distant atomic continuous-variable systems can be entangled.

The European Union has been at the forefront of the dramatic development of the field of **continuous-variable quantum information processing and communications** (CV-QIPC). A great deal of the main achievements in this direction, both theoretical and experimental, is due to European teams. To mention just a few, on the experimental side the group of Eugene Polzik (Niels Bohr Institute, Copenhagen, Denmark) was the first to entangle two atomic ensembles, and to realize a quantum memory for light [2]. The group of Gerd Leuchs (University of Erlangen, Germany) realized continuous-variable quantum cryptography, quantum erasing, and quantum cloning [3], and the group of one of the authors (PG) was the first to demonstrate continuous-variable coherent-state quantum cryptography [4], as well as de-gaussification operations. On the theoretical side, many groups have been involved in these developments, for example the group of Ignacio Cirac (Max-Planck Institute, Garching, Germany) who contributed to the characterization of continuous-variable entanglement, the group of Martin Plenio (Imperial College, London, UK) who investigated continuous-variable entanglement purification with non-Gaussian operations, the group of Reinhard Werner (Technical University of Braunschweig, Germany) who initiated the study of bound entanglement with Gaussian states, or the group of one of the authors (NC) who initiated the study of continuous-variable quantum cloning [5] as well as quantum cryptography.

This illustrates with no doubt that Europe has been a leading actor in CV-QIPC. **Two European projects are (or have been) entirely devoted to exploring this research direction, namely**

QUICOV (IST-1999-13071) and COVAQIAL (FP6-511004). This research effort is, to our knowledge, unmatched worldwide. In addition, an annual series of European workshops solely focused on this topic, funded by the European Science Foundation, has been organized since 2002.

Optical quantum continuous variables

Let us consider the continuous variables that naturally appear when describing a light field. In classical electromagnetism, a light field can be written as an oscillatory function $x\cos(\omega t) + p\sin(\omega t)$, where ω is the angular frequency while x and p are the **quadrature components** of the field. If $\cos(\omega t)$ is viewed as a reference field, generally called the Local Oscillator (LO), then x is the amplitude of the component of the field that is in phase with the LO, while p is the amplitude of the component that is in quadrature with the LO. Clearly, x and p make a pair of **continuous variables** that completely characterize the optical field.

When the quantum properties of light become of interest, such a classical description is not valid any more and we have to quantize the light field, that is, we have to turn to quantum optics. Then, the "granularity" of the light field becomes important and gives rise to photon counting processes, while the quadrature components x and p become non-commuting (but still continuous) observables. As a result of the Heisenberg uncertainty principle, x and p cannot be known together, in contrast to the situation in classical optics: any measurement of x deletes the information on p, and conversely. In some sense, the two quadrature components of light behave exactly as the usual position-momentum pair in quantum mechanics, hence the notation. This suggests that we can build a whole set of quantum informational processes where the quadrature pair (x, p) carries the information. This departs from the standard QIPC paradigm where a binary variable (a bit) is encoded into a dichotomic degree of freedom of a single photon (a quantum bit), e.g., its polarization.

Although dealing with continuous-variable quantum information is conceptually less natural, it comes with several advantages: (i) the measurement technique, called **homodyne detection**, works at a very high rate; (ii) it is sufficient to process simple non-classical states of the light, known as single-mode squeezed states, into linear optics circuits in order to perform a large variety of multipartite informational processes over continuous variables; (iii) the Bell measurement, a corner stone of QIPC, can be realized deterministically with a balanced beam splitter followed by homodyne measurement. By comparison, quantum-bit based QIPC processes suffer the following problems: (i) the measurement technique is based on comparatively slower avalanche photodiodes; (ii) multipartite quantum circuits typically require two-body interaction between quantum bits; (iii) the Bell measurement achieved with a beam splitter is fundamentally restricted to a probabilistic measurement (it succeeds with a probability of 50% at most).

Continuous-variable quantum cloning

Consider for a moment the case of quantum bits. As is well known, the duality between the computational basis $\{|0\rangle, |1\rangle\}$ and the dual basis $\{|0\rangle + |1\rangle, |0\rangle - |1\rangle\}$ prohibits the simultaneous determination of the "value" of a state in both bases. This duality is at the heart of the **quantum no-cloning theorem**: it is impossible to duplicate perfectly the state of a quantum bit. Coming back to case of continuous variables, one notes that the canonical variables (x, p) are linked by a Fourier transform, just as the Hadamard transform maps the computational to the dual basis for qubits. The quantum no-cloning theorem then implies that it is not possible to clone position states (x-states) and momentum states (p-states) by a same process. By measuring x and preparing clones as x-localized states, one would make a perfect x-states cloner; but this cloner would then fail at cloning

p-localized states. Obviously, the converse holds too, so that we must turn to **approximate** optimal cloning machines, which achieve the best possible imperfect copying of the state that is compatible with quantum mechanics.

A very natural candidate for continuous-variable cloning is a transformation that adds the same noise on both quadrature components. By exploiting the connection between measurement and cloning theory, a tight bound on this cloner can be obtained by exploiting the well-known fact that the best joint measurement of x and p for a coherent state suffers from an extra noise whose variance is equal to twice the shot-noise unit. Clearly, cloning the state and then measuring x on one clone and p on the other clone cannot beat this optimal measurement, so that the cloning process comes itself with a "price" of one shot-noise unit, the other unit simply coming from the measurement process. As was shown by the group of one of the authors (NC), one can build a Gaussian cloning machine that exactly saturates this bound [5]. The quantum circuit of this cloner (see **Figure 1a**) consists of four continuous-variable controlled-NOT gates preceded by a preparation stage. The two auxiliary input modes need to be initially prepared in the vacuum state, and they contribute each for half a shot-noise unit to the cloning noise. As a result, this cloner adds a Gaussian-distributed noise on both quadrature components x and p with a variance of one shot-noise unit, which implies that the cloning fidelity is equal to 2/3 for all coherent states. It may be realized using a phase-insensitive amplifier of gain 2 followed by a balanced beam splitter (see **Figure 1b**). A variant of this setup has been experimentally implemented very recently by the group of Gerd Leuchs [3]. Interestingly, the physical origin of the cloning noise becomes much more evident in the case of continuous variables than with quantum bits: it is indeed clear from **Figure 1** that the noise affecting the clones can be traced back to the vacuum fluctuations that unavoidably enter via the two auxiliary modes of the cloner.

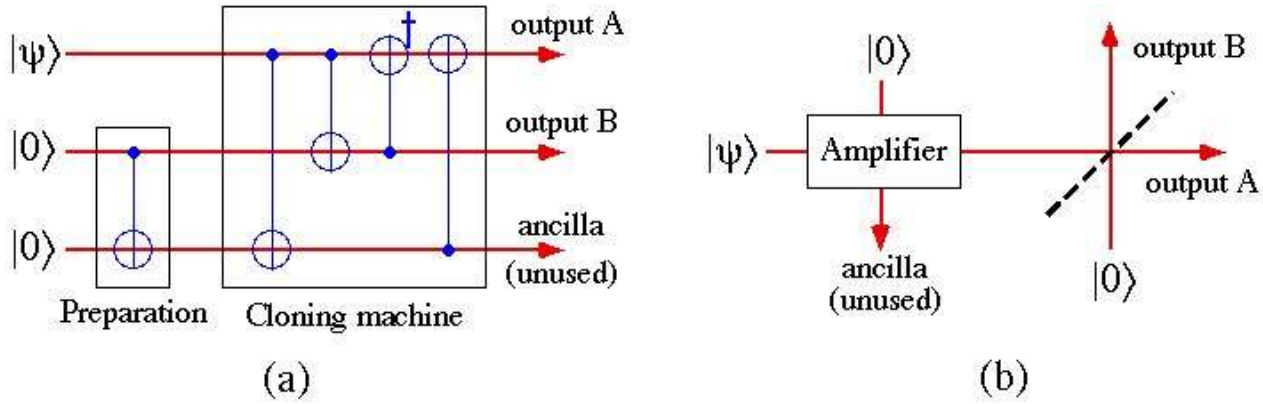


Figure 1

Continuous-variable quantum key distribution

The investigation of quantum cloning is of a particular significance given the strong connection between quantum cloning and quantum cryptography: it is indeed the impossibility to make a perfect cloning that makes it possible to detect a potential eavesdropper in a quantum cryptographic scheme. More specifically, the use of an optimal quantum cloner generally makes it possible to derive a tight upper bound on the information acquired by the potential eavesdropper. This connection provides a strong incentive to devising quantum cryptographic schemes specifically designed for continuous variable.

More precisely, the idea is to exploit this impossibility to perfectly clone the x- and p-states by turning it into a problem for the eavesdropper (Eve). The first proposal for CV-QKD relying on a

continuous modulation of key carriers was made by the team of one of the authors (NC), and independently by Gottesman and Preskill. This protocol, which can be viewed as the direct continuous analogue of BB84, requires squeezed states of light. The sender (Alice) chooses to encode a Gaussian value into the x-displacement of an x-squeezed state, or similarly for the quadrature p. Then, the receiver (Bob) measures one of the two quadratures by homodyne detection, and publicly discloses whether x or p was measured. If the encoded and measured quadratures coincide, then Alice and Bob know that they share correlated Gaussian data, from which they can distill a secret key by using appropriate techniques (otherwise they simply discard their data). This protocol, however, has never been implemented in the laboratory because the need for squeezed states makes it impractical.

An important progress was then made by the group of one of the authors (PG), who proposed a **coherent-state** CV-QKD protocol building upon these previous squeezed-state proposals [6]. The breakthrough was to explicitly establish a secure protocol using Gaussian-modulated coherent states of light, which can be easily generated with a laser. In this protocol, Alice modulates both x and p quadratures of a coherent state. Bob again measures one of them, and publicly discloses which one, so the corresponding quadrature is kept by Alice to make a correlated pair. The security of the protocol against individual Gaussian attacks was proven by using the concept of "equivalent noise" referred to the input, which is common in electronics and has been used previously in the context of quantum non-demolition measurements in optics (see [4]). The security criterion is then very simple: the equivalent noise variance N of the transmission line, evaluated at the line input, cannot exceed one shot-noise unit: $N < 1$. This condition is actually equivalent to limit on CV quantum cloning, that is, the best attack would be the optimal Gaussian cloning machine that is depicted in **Figure 1**.

An important observation is that the equivalent noise variance includes two contributions, namely the "vacuum noise" $(1–T)/T$, which is due to the losses in a line of transmission T, and the "excess noise" $\varepsilon = N – (1–T)/T$, which may be due for instance to spontaneous emission from an in-line amplifier. The security criterion $N \leq 1$ can then be equivalently written as $\varepsilon < 2 – 1/T$. In the ideal case of a lossy but noiseless line, the security thus requires that $T > 1/2$ (i.e., more than half the intensity has to reach the receiver). This limit, known as the **3dB-loss limit,** was first thought to be generic to CV-QKD. It was quickly realized, however, that it is protocol-dependent and can be beaten just like in photon-counting QKD (where no loss limit applies because only the photons that are received by Bob are taken into account). A similar technique, known as **reverse reconciliation**, was shown to be applicable to continuous variables, so that the key distribution remains secure for any value of the line transmission [4]. To achieve this, the secret key must be made out of the (noisy) data received by Bob instead of the data sent by Alice. Since it is harder for Eve to infer Bob's errors than to guess Alice's data, this reverse protocol provides a definite advantage to Alice and Bob. A related technique to beat the 3-dB loss limit is to carry out a post-selection by putting a threshold on Bob's data. However, the security of such post-selection protocols is not well established yet, since the best eavesdropping strategy has not been studied so far.

Experimental demonstration

A table-top experimental demonstration of this coherent-state continuous-variable protocol with reverse reconciliation was reported in [4] (see **Figure 2**). The setup uses a laser diode at 780 nm to generate pulses at a repetition rate of 800 kHz. These coherent light pulses are modulated in amplitude and phase by Alice, and then measured by Bob with an homodyne detection. An essential ingredient to make this protocol practical lies in the ability to efficiently extract secret bits from correlated strings of continuous data, and simultaneously to correct errors without revealing

too much information to Eve. A method for achieving this goal, named **sliced reconciliation,** was proposed by the group of one of the authors (NC). By alternating bit-extraction and error-correction steps over successive "bit slices" it is possible to extract a number of common bits that reaches typically 80 to 90% of Shannon's limit. This method was applied to the experimental data obtained with a variance ranging between 25 and 40 shot-noise units. The obtained net secret key bit rate was 1.7 Mbit/s for a lossless line and 75 kbit/s for a line with a 3.1dB loss. These rates are quite significant when compared to photon-counting QKD, and they open very interesting perspectives for coherent states CV-QKD. The table-top experiment shown in **Figure 2** may straightforwardly be transposed to telecom wavelength (1550 nm) by using only standard telecom components. A significant advantage is that the setup does not need sophisticated devices such as single-photon sources or counters.

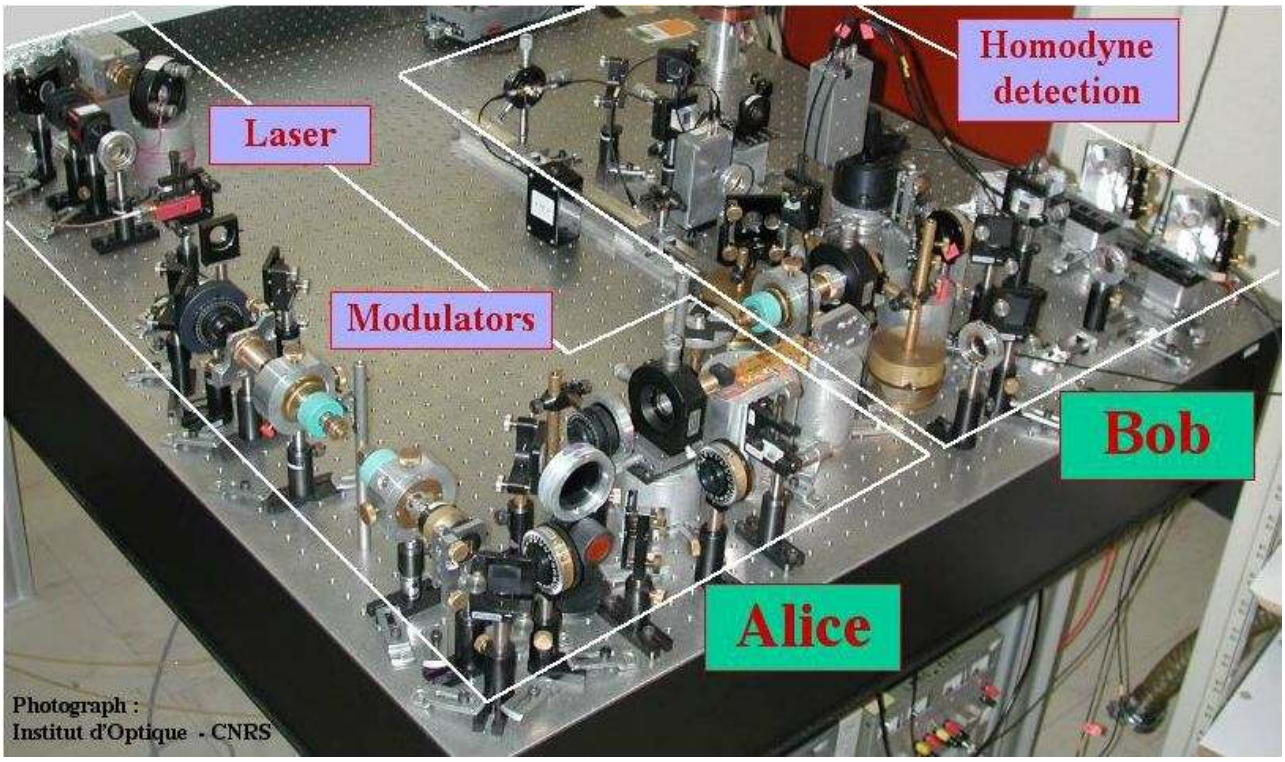


Figure 2

Security proofs

The first security proof on direct [6] and reverse [4] reconciliation protocols only considered individual Gaussian attacks. This certainly does not mean easy attacks, because such attacks already imply that Eve must have a long-lived quantum memory for storing light states, and also must produce pairs of light beams with arbitrary entanglement. Nevertheless, such attacks are not the most general ones, and, more recently, several new security proofs of coherent-state CV-QKD have appeared. An important first step is to realize that these protocols are actually equivalent to entangled-based protocols, where Alice measures simultaneously both quadratures on her entangled beam so to prepare a Gaussian-modulated coherent state at Bob's side. This **virtual entanglement**, also known for photon-counting QKD, is very useful for establishing security proofs. In particular, it implies that there is an **entanglement-breaking limit** in continuous-variable protocols, corresponding to an intercept-and-resend attack, which gives $\varepsilon < 2$. This means that when the excess noise exceeds two shot-noise units, no secure communication is possible

More restrictive security limits can actually be established. For an entanglement-based protocol using reverse reconciliation, the security bound becomes $\varepsilon < 1$. For a coherent-state protocol, the bound is $\varepsilon < 2 - 1/T$ for direct reconciliation, and $\varepsilon < 1/2 - 1/T + (1/T^2 + 1/4)^{1/2}$ for reverse reconciliation, provided that the variance of Alice's modulation is large enough. The relation between the excess noise ε and the maximum distance for secure QKD is shown in **Figure 3**, assuming fiber losses of 0.2 dB/km. Curve (a) is the entanglement-breaking attack ($\varepsilon = 2$), curve (b) is obtained with the entangled-beam reverse-reconciled protocol ($\varepsilon=1$), while the last two curves correspond to coherent-state protocols using either direct (c) or reverse (d) reconciliation.

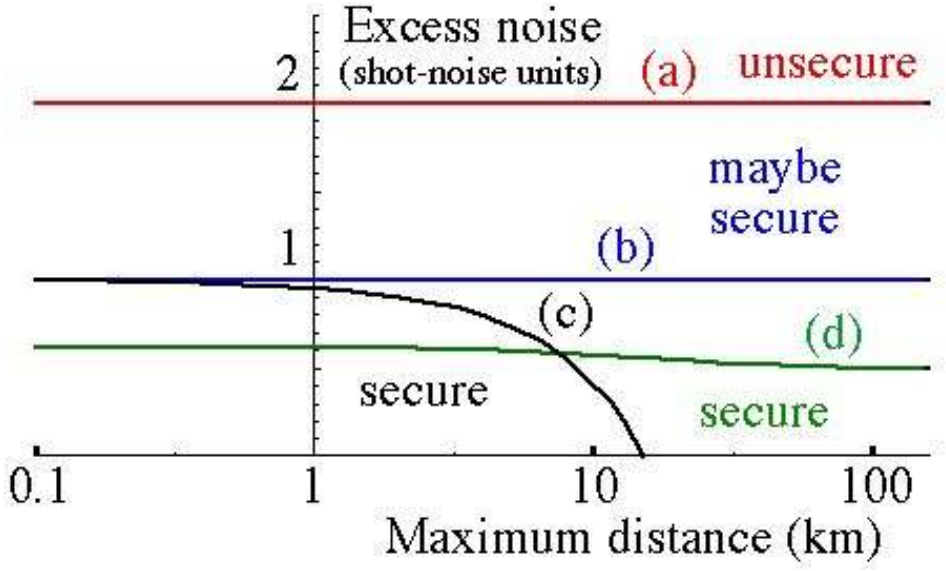


Figure 3

Interestingly, it can be shown by using entropic Heisenberg relations that the individual Gaussian attacks are actually the best possible attacks against reverse-reconciled protocols [7]. This proof covers all non-Gaussian attacks and even collective attacks, provided that their size remains smaller than the key size and provided that Eve does not delay her measurement until after the key distillation procedure. It means that the above limits that were derived for individual Gaussian attacks are actually valid in a much more general framework. It is worth emphasizing that according to this proof, Alice and Bob must use a Gaussian modulation for exchanging data because this modulation maximizes the entropy for a given variance. In that respect, using any kind of discrete modulation of the signal will be less efficient, a fact which further justifies the Gaussian encoding scheme.

Progresses have also been made in the direction of **unconditional security**, first by extending the well-known unconditional security proof of Gottesman and Preskill. In short, the idea is to show that squeezing, which is required in the Gottesman-Preskill proof, is used only to evaluate the channel's error rate, and can actually be replaced by a channel tomography procedure using only coherent states [8]. This approach shows that unconditional security of coherent-state QKD is achievable, although it guarantees a much lower secret bit rate than in [4] because the used encoding scheme is far less efficient than a Gaussian modulation. Other security proofs, based upon general information-theoretic arguments, have also been published very recently.

Conclusions

As a conclusion, let us emphasize again that, in principle, secure CV-QKD can be achieved for arbitrarily high channel losses. The theoretical long-distance secret key bit rate of the reverse-reconciled coherent-state protocols is roughly equal to that of an ideal BB84, with a perfect single-photon source and detector. A basic lesson we can draw from reverse reconciliation is that the errors due to line losses can be eliminated, in principle, to the same extent as the line losses do not compromise the security of photon-counting protocols. In some sense, the role of errors in photon-counting QKD is played by the excess noise for reverse-reconciled CV-QKD, and they both lead to a fundamental decrease in the secret bit rate. As illustrated in **Figure 3**, the maximum tolerable excess noise for coherent-states CV-QKD decreases with the distance, which is what eventually puts a limit on the achievable security on long distances.

The experiments realized so far are table-top proof-of-principle experiments. Nevertheless, it must be pointed out that coherent-state CV-QKD can be implemented by using only standard optical telecommunications equipment, without the need for dedicated photon sources or single photon counters. Several experiments are presently under way to characterize such systems in the telecom domain. Like with photon-counting QKD, several options are available: the pulses can be sent one way in an optical fiber, or may be retro-reflected using Faraday mirrors, or may be sent in free space by using a polarization variant of the basic scheme. These various possibilities are presently investigated in several European laboratories (namely Orsay, Geneva, and Erlangen) in the framework of the **Integrated Project SECOQC**.

Ultimately, losses will be a limitation for CV-QKD protocols for practical reasons, just like they are for photon-counting protocols. One may then consider building "quantum repeaters", based on CV entanglement distillation procedures. A first step in that direction is to learn how to manipulate CV non-Gaussian states, which are a required ingredient for CV entanglement distillation. This was recently achieved by the group of one of the authors (PG) [9]. All these recent developments, both on the theoretical and experimental side, clearly indicate that quantum continuous variables are a promising tool for the future of Quantum Information Processing and Communications.

List of terms and acronyms

CV: continuous variable
QIPC: quantum information processing and communication
CV-QIPC: continuous-variable quantum information processing and communication
QKD: quantum key distribution
CV-QKD: continuous-variable quantum key distribution
LO: local oscillator
BB84: quantum key distribution protocol due to Bennett and Brassard in1984

References

[1] A. Furusawa, J.L. Sorensen, S.L. Braunstein, C.A. Fuchs, H.J. Kimble, and E.S. Polzik, Science 282, 706 (1998).
[2] B. Julsgaard, J. Sherson, J.I. Cirac, J. Fiurasek, and E.S. Polzik, Nature 432, 482 (2004).
[3] U.L. Andersen, V. Josse, and G. Leuchs, http://arxiv.org/abs/quant-ph/0501005
[4] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N.J. Cerf, and P. Grangier, Nature 421, 238 (2003).
[5] N.J. Cerf, A. Ipe, and X. Rottenberg, Phys. Rev. Lett. 85, 1754 (2000).
[6] F. Grosshans and P. Grangier, Phys. Rev. Lett. 88, 057902 (2002).
[7] F. Grosshans and N.J. Cerf, Phys. Rev. Lett. 92, 047905 (2004).
[8] S. Iblisdir, G. Van Assche, and N.J. Cerf, Phys. Rev. Lett. 93, 170502 (2004).

[9] J. Wenger, R. Brouri, and P. Grangier, Phys. Rev. Lett. 92, 153601 (2004).

Projects funded by the European Commission and related to the work in this article:

QUICOV
Quantum Information with Continuous Variables
Start date: 01/01/2000
End date: 31/06/2003
Project web site: http://kerr.physik.uni-erlangen.de/quicov/
Contact Person: Gerd Leuchs, Universität Erlangen-Nurnberg, leuchs@physik.uni-erlangen.de

COVAQIAL
Continuous Variable Quantum Information with Atoms and Light
Start date: 01/09/2004
End date: 31/08/2007
Project web site: http://www.ulb.ac.be/project/covaqial/
Contact Person: Nicolas Cerf, Université Libre de Bruxelles, nicolas.cerf@ulb.ac.be

SECOQC
Development of a Global Network for Secure Communication based on Quantum Cryptography
Start date: 01/04/2004
End date: 31/03/2008
Project web site: http://www.secoqc.net/
Contact Person: Christian Monyk, ARC Seibersdorf research GmbH, christian.monyk@arcs.ac.at

Contact information of the authors of this article:
Nicolas Cerf
Ecole Polytechnique
Université Libre de Bruxelles
50 avenue F. D. Roosevelt, CP 165
1050 Bruxelles
Belgium
Email: nicolas.cerf@ulb.ac.be
Web page: http://quic.ulb.ac.be

Philippe Grangier
Quantum Optics Group
Laboratoire Charles Fabry de l'Institut d'Optique
Bâtiment 503, Centre Universitaire
91403 Orsay
France
Email: philippe.grangier@iota.u-psud.fr
Web page: http://www.iota.u-psud.fr/~grangier/Optique_quantique.html

Quantum communication – Quantum channel capacities

Reinhard F. Werner
Reinhard Werner is a full professor at the Institute for Mathematical Physics of the Technical University of Braunschweig in Germany. He is specialized in the conceptual and mathematical foundations of quantum mechanics, especially quantum information theory. He is a partner in the EU-funded IST FP5 projects EQUIP and QUPRODIS. He is also a member of Schwerpunkt "Quanten-informationsver-arbeitung", DFG, Germany.

Andreas Winter
Andreas Winter is a lecturer at the Department of Mathematics of the University of Bristol, United Kingdom. He is interested in quantum and classical information theory and discrete mathematics. is a partner in the EU-funded IST projects RESQ and ECRYPT. He is also a member of the Interdisciplinary Research Collaboration "Quantum Information Processing", EPSRC, U.K.

Abstract
Capacities measure the amount of information that can be stored in a quantum memory or transmitted through a quantum communication channel, assuming optimal error correction, and in the asymptotic limit of many uses of the device. Different capacities are defined for tasks such as the transmission of classical information, or of quantum information, or the transmission with guaranteed security against eavesdropping. The theory of such capacities requires efficient methods for converting different quantum resources. We describe recent breakthroughs obtained in the last two years, and point out the currently "hot" questions.

Introduction

One of the key realizations from the beginning of quantum information theory was that entanglement, hitherto considered merely as a paradoxical trait of quantum mechanics, attained a quantitative status. In the quantum teleportation process, the role of entanglement was that of a necessary resource, of which one bit was used up for every teleportation step, much like a fuel. Likewise the gain of a teleportation process, namely the error-free transfer of the state of one qubit system, came to be looked at in a quantitative way, as the transmission of one bit of quantum information.

This quantitative, task-oriented turn is a characteristic feature of quantum information theory. The basic quantum resources "entanglement" and "quantum transmission" are combined with many other resources, which can be described classically, such as the transmission of classical information, the generation of secret key (shared randomness) and the transmission of classical information in a provably secure way.

How much information?

Information is one of the key notions of modern society. Yet the use of this term is strangely fuzzy, and its meaning in everyday language is rather different from its technical meaning in the theory of information as founded by Claude Shannon [1] in 1948. Since quantum information theory shares many features with Shannon's theory, it may be helpful to dwell a little bit on this difference. In everyday language, information is often used for the sort of thing one obtains from an "information desk", were one hopes to find a well-informed person. Information in this sense is *about* something. In a message it would refer to the content, or meaning. In contrast the technical term information would refer to its *size*, and to the possibility of efficiently transmitting or storing it. For example, it is no concern for information theory whether a television satellite is spreading misinformation, but it has a lot to say about the technical quality of the image. Or think of the yes/no question asked at a wedding, which certainly carries a lot of meaning and a commitment for life. Information theory would look at this from the point of view of the clerk who has to record and file the answers. He quickly discovers that the most efficient way is to store only the records of the "no" answers. This saves him almost all the work and ink, which means, in the language of information theory, that the information content of those answers is very close to zero.

The restraint of information theory with regard to content may seem regrettable. However, it was a necessary step for arriving at a quantitative theory, and a key for the huge success of the theory. So how does information theory measure the size of a message? For a book one might just count the number of characters. But how can one compare then a book written in Latin characters with a book written in Chinese? The main idea is to first compress the message to as short a bit string as possible. This is done by compression programs as they are commonly used on PCs and which are based, in fact, on information theoretical techniques. Similar algorithms exist for the Chinese language, so one can easily compare the size of texts on the basis of the universal unit "bit".

The coding idea is also fundamental for judging the size of a storage or transmission device. Usually there will be errors in such a device, and a "noisy channel" introducing random bit errors is clearly losing some information. However, by a suitable encoding of the input data and corresponding decoding of the output from the channel one can reduce errors, possibly at the expense of the size of the message that can be sent. The best rate of transmissions that can be achieved in this way is called the **capacity** of the device. These ideas apply to transmission or storage alike, since storage is just a transmission to a future time.

Figure 1 shows the basic scheme for channel encoding. The arrows each indicate a message of one bit. For sending one has available a noisy channel N. In the scheme shown it is used four times, although the net transmission is only of two bits. If encoding and decoding succeed to eliminate (or "correct") the errors, we would say that the channel has at least the capacity ½. Usually, however, the errors can not be eliminated completely. But for larger and larger messages they can be reduced better and better. The mathematical definition of capacity always involves this kind of limit, requiring the errors to become as small as desired for large messages. If this works with just twice as many channel uses as bits sent, the capacity of N will be ½.

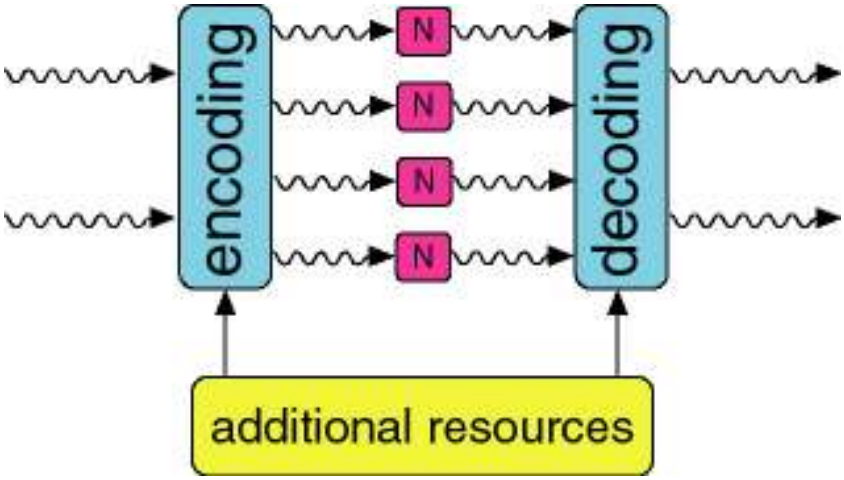


Figure 1 shows the possibility to bring additional resources to the encoding and decoding processes. This will be discussed later on.

A crucial problem in the theory of capacities is that their definition requires finding the best encoding/decoding scheme for large messages. Especially for large systems it is out of the question to determine the best schemes numerically. However, one can often construct good families of error correcting codes, and sometimes even show that such codes are asymptotically not far from the optimum. The gain of such investigations is twofold: on the one hand the good codes may also be practically a good choice, and one achieves the computation of capacities without having to solve explicitly the high dimensional optimization problems. The prototype of a result of the last kind is Shannon's noisy channel coding theorem, which gives a simple formula for channel capacities of classical channels. And theoretical as this problem may seem, its solution has been central for recent communication technology; for example, the now ubiquitous low-intensity (and hence error-prone) wireless communication networks operate near the Shannon limit.

Quantum information

In all this, the precise physical nature of the information carrying systems plays no role. Information theory does not care, whether information is written on paper stored on a magnetic disc, or communicated by waving flags. When we speak of quantum information, and thereby refer to quantum mechanics and the type of physical systems it describes, we apparently make an exception to this rule. There are, however, close analogies between the information theoretical setup and the way quantum mechanics describes physical systems. In fact, even before the current surge of interest in this point of view, an axiomatic approach to quantum mechanics was based on the view that quantum systems should always be thought of

as carriers of an interaction between macroscopic devices. The typical scheme is displayed in **Figure 2**.

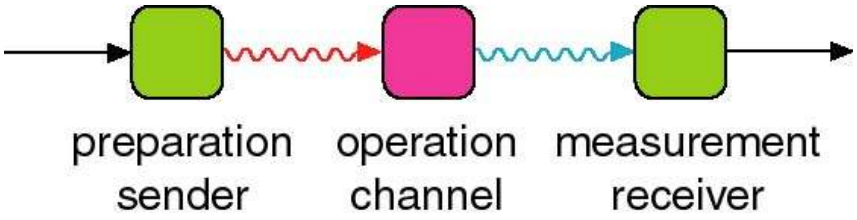


Figure 2

Any experiment in the scope of quantum mechanics begins with a preparation, by which some quantum systems are created in a controlled way. The final stage is always a measurement, which typically destroys the quantum system, and yields as output some classical data. In between further things may happen to the system, for example it may be left to its own spontaneous dynamics, maybe subject to noise from the environment, or to actions by the experimenter. All the predictions of quantum mechanics are statistical, i.e., there is no prediction for single runs of such experiment, but only for the probabilities of events, when the same experiment is run many times. The overall experiment can be described completely in classical terms, and we can just as well consider this as a transmission experiment, in which the preparation acts as the sender, the measurement as the receiver, and further operations may either correspond to noise acting on the system or to actions of the experimenter. These information theoretical interpretations of these parts are given on **Figure 2** in the second line.

One may wonder why a new kind of "quantum" information is seen at work here, in spite of the fact that everything can be described classically. The reason is that we focus on the possible operations between preparation and measurement, and try to build devices which work on arbitrary, unknown input states, and with arbitrary control measurements. For example, an ideal channel for quantum information is by definition one whose outputs perform in all statistical experiments in the same way as the inputs. This includes quantum mechanical interference experiments, and one could say that transmitting quantum information is the same task as sending quantum systems in such a way that none of the many possible interference experiments is spoiled by the transmission.

On the other hand, if we restrict a priori to a subclass of possible preparations and measurements, we effectively lower our demands on the "quality" of transmission – for example, when there is only one, fixed, measurement, the above definition captures a classical ideal channel, which preserves the measurement results of this one observable.

A fairly recent and still inspiring overview of quantum information theory is contained in [2].

Sending classical information on quantum channels

The first uses foreseen for quantum channels were quite traditional: encode classical, that is, ordinary, information. Since quantum channels, just like classical channels, introduce noise, the challenge, formulated circa from the sixties, was to find the analogue of Shannon's capacity formula. This question was essentially resolved in 1996 by Holevo and Schumacher/Westmoreland, who proved the general coding theorem (i.e., a prescription how to construct asymptotically capacity achieving codes, for arbitrary channels), which includes Shannon's classic (and classical) result as a special case.

More recent work has shown that providing further resources in the spirit of **Figure 1** need not increase the capacity: prior shared randomness (that is, shared access to the outcomes of fair coin tosses), though helpful in coordinating the actions of encoder and decoder, does not increase the capacity. However, this is not so for shared entanglement between encoder and decoder: it generically increases the capacity, and Bennett et al. have found a beautiful formula for the "entanglement-assisted capacity" of a channel, generalizing Shannon's expression. Finally, feedback (unlimited noiseless classical communication from decoder to encoder) can increase the classical capacity of a quantum channel as well (in contrast to a famous result by Shannon for classical channels), as exotic examples constructed by Bennett et al. show.

Sending quantum information on quantum channels

An obviously more ambitious task, and a more "quantum" one, would be to transmit quantum information on the channel N. This problem arose only in the last decade, with the identification of quantum information as a new kind of information. It is a practical problem in quantum networks, where quantum computers will need to exchange parts of their quantum states. Since "quantum wires", are prone to errors to a much higher degree than classical communication links, it is essential to understand the (quantum) error correction possibilities, and to at least estimate the capacity of a given quantum channel [3].

Surprisingly, quantum channel coding, while somehow extending classical (Shannon type) techniques, has many unprecedented subtleties, which prevented finding the determination of capacity except for a few special channels. And even though early on Schumacher proposed a conjectured capacity formula, a general method for constructing good codes was lacking altogether. Only recently Shor publicized a sketch of a general proof (which still awaits publication), and soon after, Devetak developed a technique that reduces the question to **private classical communication**. Namely, it is well known that an ideal quantum channel provides perfect security against any quantum mechanical eavesdropper; Devetak showed a way how to turn this around and "upgrade" coding schemes for private communication to quantum channel codes. The difficulty is to pass from the transmission of classical messages, represented by quantum states sent into the channel, to the transmission of coherent superpositions of these states, and the crucial insight is that the privacy is enough to guarantee protection of these superpositions. This technique subsequently led to a proof of the long-conjectured so-called "hashing inequality" [4], which was long known to be the pivotal result on which a host of other quantum capacities hinges.

The balance of resources

As we have seen, a quantum channel is good for many things, and its quality at a given task depends additionally on further resources available to encoder and decoder. This state of affairs, even with the new insights obtained recently, leads to a rather confusing array of different capacities: one for each combination of task and assisting resources. One may wonder why such a bewildering variety does not arise in Shannon's information theory – one reason is of course that there we do not have so many incomparable tasks. But more fundamentally, classical channel capacity is much less affected by additional resources, as discussed above: shared randomness and feedback do not affect it.

Nevertheless, quantum information theory has found its integrating power in systematizing the available basic resources, which are in one-to-one relation with basic tasks: sending a classical bit (**cbit**), sending a unit of quantum information (**qubit**), sharing the outcome of a perfect and fair coin toss, i.e., one random bit (**rbit**), or sharing a unit of entanglement (**ebit**) are the most important ones. Since entanglement gives rise to private shared classical information (this is the basis of quantum cryptography), we are also motivated to consider sending a cbit privately (**pbit**), and of sharing one bit of secret random key (**kbit**). **Figure 3** illustrates the relations between these resources in the form of a "map": whenever there is a path from a resource to another, one can perform a conversion by encoding and decoding. All conversion paths are annotated with their capacity, that is, the optimal conversion rate of unit of destination per unit of origin. Some paths require the presence of an additional resource, as in **Figure 1**. These conversion paths (teleportation, superdense coding, and classical one-time pad encryption) are drawn in green.

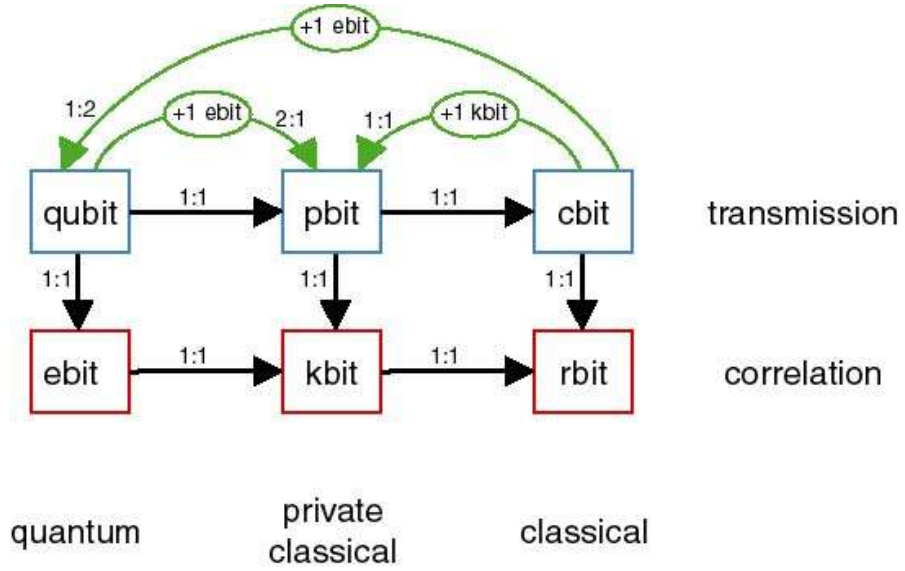


Figure 3

For ideal resources, these conversion paths are now fully understood. However, for noisy resources the diagram still holds many challenges, which are also vital for the practical sides of quantum operation engineering. For example, given a noisy quantum channel, how many qubits can it transmit, how many ebits can it distribute, and how much does a given capacity increase when unlimited entanglement or feedback become available? The recent insights mentioned above provide (partial) answers to these questions. Quite expectedly, but in stark contrast to the purely classical scenario, all the charted resources become incomparable for quantum channels, so for example there exist channels which have zero qubit capacity, but positive pbit capacity, as shown by Horodecki et al. [5]. This has interesting implications for quantum cryptography: the optimal way to use a given quantum channel for sending private information may not be to perform quantum error correction first, and use the resulting nearly ideal channel as a private one, but rather a direct method, correcting only some of the quantum errors.

Conclusions

Quantum communication theory leads us to consider a multitude of informational tasks and associated resources. We work with abstractions such as qubits, ebits, rbits, pbits and kbits, transcending the bits of Shannon's information theory, which continue to exist in the new theory as cbits. All of these resources are not equivalent, even though some can be converted into others, albeit usually irreversibly. Capacities quantify the optimal efficiency of such conversions, especially of noisy resources. Recent progress has clarified the relationship between several capacities of noisy channels, such as the classical, private and quantum capacities of a channel, as well as these same capacities if other resources like free entanglement, feedback (communication from the decoder to the encoder) or bidirectional classical side communication, are available. The driving direction of capacity theory is to build a rigorous quantitative understanding of "quantum information" and its associated tasks.

Great challenges remain, even for simple looking systems. For example, even for highly symmetric depolarizing quantum channels, we have only upper and lower estimates on the qubit capacity, but no way to compute its value. This means that there is still a gap in our understanding of quantum information and error correction. Closing this gap will certainly produce new pathways for quantum information engineering. In this sense the resource oriented theory of capacities has always been and will continue to be close to the practical concerns of the field.

List of terms and acronyms

capacity: the (usually: asymptotic) optimal conversion rate of one resource into another.
resource: any channel, state, or other help available in a communication setup; very important are the unit resources, qubit, ebit, cbit.
qubit: here: the resource of being able to transmit perfectly the state of a two-level "qubit" system.
ebit: a unit of pure entanglement: the entanglement of a singlet state of two spin-1/2 systems.
cbit: a classical bit.

References

[1] C. E. Shannon. A Mathematical Theory of Communication. *Bell System Technical Journal,* vol. 27, pp. 379-423 and 623-656, July and October, 1948

[2] C. H. Bennett and P. W. Shor. Quantum information theory. *IEEE Trans. Info. Theory,* vol. 44, pp. 2724-2742, 1998

[3] D. Kretschmann and R. F. Werner. Tema con variazioni: quantum channel capacity. *New J. Phys.*, vol. 6, art. no. 26, 2004

[4] I. Devetak and A. Winter. Relating Quantum Privacy and Quantum Coherence: An Operational Approach. *Phys. Rev. Lett.,* vol. 93, art. no. 080501, 2004

[5] K. Horodecki, M. Horodecki, P. Horodecki and J. Oppenheim. Secure key from bound entanglement. *Phys. Rev. Lett.,* to appear, 2005 (eprint quant-ph/0309110)

Projects funded by the European Commission and related to the work in this article:
EQUIP
Entanglement in Quantum Information Processing and Communication
Start date: 01/01/2000

End date: 31/12/2002
Project web site: http://www.equip.qipc.org/
Contact Person: Martin Wilkens, U Potsdam, Martin.Wilkens@physik.uni-potsdam.de

QUPRODIS
Quantum Properties of Distributed Systems
Start date: 01/01/2003
End date: 31/12/2005
Project web site: http://www.quprodis.org/
Contact Person: Wilkens, U Potsdam, Martin.Wilkens@physik.uni-potsdam.de
RESQ
Resources for Quantum Information
Start date: 01/01/2003
End date: 31/12/2005
Project web site: http://www.ulb.ac.be/project/RESQ/
Contact Person: Serge Massar, Université Libre de Bruxelles, smassar@ulb.ac.be

ECRYPT
Network of Excellence in Cryptology
Start date: 01/02/2004
End date: 31/01/2008
Project web site: http://www.ecrypt.eu.org/
Contact Person: Bart Preneel, Katholieke Universiteit Leuven, ecrypt-contact@ecrypt.eu.org

Projects funded by National initiatives or organizations and related to this article:

DFG Schwerpunktprogramm "Quanteninformationsverarbeitung" (Germany)
Start date: 01/04/1999
End date: 31/03/2005
Project web site: http://kerr.physik.uni-erlangen.de/qiv/
Contact Person: Gerd Leuchs, University of Erlangen, leuchs@physik.uni-erlangen.de

EPSRC IRC "QIP" (U.K.)
Interdisciplinary Research Collaboration "Quantum Information Processing"
Start date: 01/04/2004
End date: 31/03/2009
Project web site: http://www.qipirc.org/
Contact Person: Andrew Briggs, Oxford University, andrew.briggs@materials.ox.ac.uk

Contact information of the authors of this article:
Reinhard F. Werner
Institute for Mathematical Physics
Technical University of Braunschweig
Mendelssohnstrasse 3
D-38106 Braunschweig
Germany
Email: r.werner@tu-bs.de
Web page: http://www.imaph.tu-bs.de/home/werner/

Andreas Winter
Department of Mathematics
University of Bristol
University Walk
Bristol BS8 1TW
United Kingdom
Email: a.j.winter@bris.ac.uk
Web page: http://www.maths.bris.ac.uk/~csajw/

Quantum information meets statistical mechanics

José Ignacio Latorre
José Ignacio Latorre is an associate professor at the University of Barcelona, Spain. His research has focused on quantum field theory, renormalization group, phenomenology of high energy physics and quantum information. He has participated in several EU-funded IST projects (ESPRIT, EURIDICE, EQUIP, QUIPROCONE). He has participated in different national commisions to shape the future research in physics in Spain. He was awarded the Distinció de Recerca Avançada from the Generalitat de Catalunya for the next 6 years. He has published around 70 papers and is directing its 8 PhD. He founded the Benasque Center for Science.

Martin Bodo Plenio
Martin Bodo Plenio is a Professor of Quantum Physics at the Department of Physics, Imperial College London, London, UK working on Quantum Information Science and Theoretical Quantum Optics. He has participated in EU-funded IST projects EQUIP and QUPRODIS and QUIPROCONE and has been founder and chair of the 5 year ESF programme 'Quantum Information Theory and Quantum Computing. Recently he was co-author of the successful proposal for a national Interdisciplinary Research Collaboration on Quantum Information Processing funded by EPSRC and serves on its management committee. He has published more than 80 refereed papers and has been awarded the Maxwell Medal and Prize for 2005 of the Institute of Physics, UK.

Abstract

Entanglement is one of the key resources in quantum information science and the investigation of its properties is therefore on of the main areas of quantum information research. Over the last few years many new results have been obtained and many helpful techniques have been developed for the description of entanglement. Now we are entering a stage where these insights are being applied to other areas of physics. Of particular importance are emerging connections between entanglement and statistical physics and thermodynamics.

Introduction

One of the main innovations of quantum information theory is its new viewpoint of entanglement, ie quantum correlations, as a resource. This resource permits us to overcome constraints such as that of locality and therefore permits the implementation of information processing tasks such as quantum teleportation that are impossible otherwise. The properties of quantum correlations in many-particle systems are also thought to hold the key to understanding the efficiency of quantum computation. As a consequence the study of entanglement as a resource is an objective of quantum information theory research worldwide.

Some of this research has been described in Section 2, and so the aim of the present chapter is to concentrate in particular on the fascinating connections that are emerging between entanglement theory and statistical mechanics and thermodynamics. The two main routes by which this connection is emerging are described in the sections below.

Entanglement and the Foundations of Thermodynamics

The first approach is due to the realization that constraints and resources are intimately related in physics. If we impose a constraint on a physical setting then certain tasks become impossible. A resource must be made available to overcome the restrictions imposed by the constraints. Such a resource may be manipulated and transformed under the constrained set of operations but under the fundamental law that the resource cannot be created employing only the constrained set of operations. Placing this intuition on a more solid basis leads to the realization that both entanglement theory and a mathematical formulation of thermodynamics take forms that are formally analogous [1]. However, the structure of entanglement is more complex as it does not generally appear to satisfy a particular condition that would lead to a unique concept of entanglement entropy, unlike in thermodynamics. Various approaches are being taken to either consider entanglement under more general operations to ensure that this condition is satisfied [2] or to consider the resources of entanglement theory in more detail [3]. Establishing such a formal connection between entanglement theory and statistic mechanics would lead to a far deeper understanding of entanglement with the concomitant potential for new insights into the nature of quantum computation and other entanglement based quantum information applications.

Entanglement and Quantum-Many Body Physics

The second route is based upon the achievements in understanding the entanglement for few spin systems in abstract entanglement theory (see above and Section 2). The aim is to employ and extend these tools to the study of quantum correlations in many body problems, usually associated to Condensed Matter Physics and, more specifically, to Quantum Statistical Mechanics. The overlap of both fields of expertise has produced a remarkable set of new ideas that are developing in new powerful techniques to solve long-standing problems. This chapter is devoted to review some of the results obtained on this field during the last few years.

Quantum Information places enormous focus on quantum states and the correlations they carry rather than on their dynamics. If our goal is to perform a task such as teleportation, it is more relevant to understand a quantum state *per se* than the Hamiltonian that generated it. From this new point of view we may wonder what are the entanglement properties of ground

states associated with physically motivated Hamiltonians. Since correlation functions are a way to characterize entanglement, we do expect entanglement to play a relevant role in the presence of critical phenomena.

Initial approaches were concerned with the calculation of the entanglement properties of the ground state of specific interacting quantum systems. This has led to a preliminary understanding of some of the properties of entanglement in such systems. In this context it is of course important which type of quantity, or figure of merit, is being considered. One approach, extensively analyzed in the statistical mechanics context, is the study of the decay behaviour of correlations with distance that is observed when two separate spins are measured (see lhs of **Figure 1**). As the ground state is a pure quantum state any such correlations are related to entanglement of the system as a whole. At the quantum critical point these correlation tend to decay like a power law while away from the quantum critical point they decay exponentially. The disadvantage of this approach is the lack of a transparent connection between these correlations obtained in the measurement of these two spins and the entanglement properties of the state as a whole. A more detailed approach, that was motivated by ideas that had been developed originally in work on the abstract theory of entanglement, considers the entanglement that can be realized in two separated spins of a chain when one first individually measures all other spins in the chain (see rhs of **Figure 1**). The additional information gained about the state in this way then *activates* entanglement in the two remaining spins taking into account the entanglement structure of the state as a whole. This quantity exhibits intriguing behaviour [4,5] and is an example of a novel point of view by which one can consider statistical mechanics systems from a quantum information perspective.

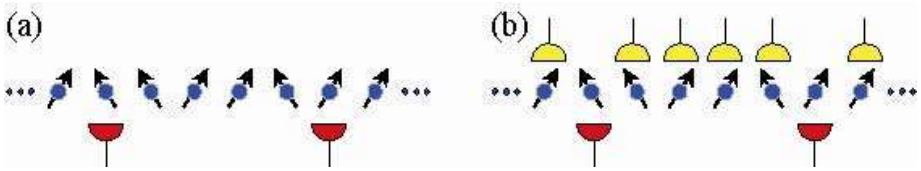


Figure 1

Another figure of merit able to capture long distance correlations is the von Neumann entropy of the reduced density matrix for a subset of L spins of a total of N (N could be infinite) in a spin chain. This entropy quantifies the entanglement between this group of spins and the remainder of the chain (see Section 2). In **Figure 2** it is illustrated that away from the critical point, this entropy saturates while it is seen to scale logarithmically with L at the quantum phase transition [6, 7].

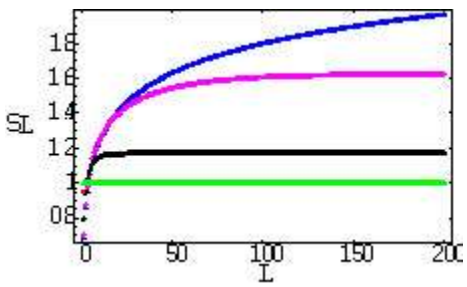


Figure 2

More precisely, the entropy scales with a coefficient that corresponds to the central charge of the conformal field theory describing the critical point. This study, originating from a desire

to understand the behaviour of interacting quantum systems near quantum phase transitions, ie the condensed matter domain, has been clarified by tools from quantum information, and rigorously proven employing novel mathematical methods from random matrix theory [7], highlighting yet again the interdisciplinary approach of quantum information science.

Results on entanglement scaling have also been extended to systems in higher spatial dimensions. Systems in two, three or more spatial dimensions, with both spins and harmonic oscillators (ie discretized field theories), have been considered. They can be proven to obey, in many situations, an ``area law'' behaviour [8], ie the entanglement between a region and its environment scales proportionally to their common surface and not the volume. This behaviour can hold true even for some systems with diverging correlation length. As a consequence it provides yet another angle under which to consider the properties of quantum many body systems. Recently provided proofs of this property have depended heavily on the machinery developed in quantum information science and entanglement theory over the last few years.

Beyond the interest in itself, the scaling of entanglement at quantum phase transitions explains qualitatively and quantitatively the reason for the success and failure of a very powerful method for numerical study of Hamiltonians, namely the density matrix renormalization group technique. The less entanglement a state carries, the fewer terms are required in the superposition to describe the quantum state of the system. For low entanglement it becomes more efficient and more accurate to approximate the state and its quantum correlations in clever truncations of the state space. The difficulty in handling large entanglement is the main obstruction to achieve good simulations of quantum systems. The deeper understanding of these issues that has been obtained in the work on the problems described above has then paved the way for very interesting development.

Indeed, it has been known for some time that the density matrix renormalization group approach may be formulated in terms of so-called matrix product states. However, insights from entanglement theory and quantum information permit a novel understanding of these states and, crucially, pave the way for their extension to higher dimensional states in higher spatial dimensions known as Projective Entangled Pairs States (PEPS). This extension has proven extremely powerful for attacking long standing problems. New classical algorithms have been developed that handle entanglement rather than the coefficients of a quantum state in its natural (computational) basis. In particular, the extension of PEPS has opened a remarkable new approach that overcomes the shortcomings of the density matrix renormalization group in two or more spatial dimensions [9]. This particular breakthrough is promising and will need a lot of further work to be consolidated.

A number of avenues to further investigate entanglement in many-body systems have been followed and we concentrate only on some of them: the use of PEPS, the loss of entanglement along renormalization trajectories and the study of entanglement in non-local Hamiltonian dynamics.

Entanglement, measured by the reduced density matrix entropy of a subset of the system, has also been shown to decrease monotonically along known renormalization group flows. This analytical result connects with the discussion of the irreversibility of renormalization group flows [10]. The latest development in this field is the construction of a renormalization group transformation on states rather than on Hamiltonians [11]. The long-distance discussion

behaviour of any quantum state is obtainable through renormalization group transformations and its fixed points can be identified.

Finally, it is worth discussing the scaling of entanglement in systems controlled by non-local Hamiltonians. Two general facts dictate the amount of entanglement in the system. On one hand, the more non-local the interactions are, the more entangled the states become under evolution. On the other hand, the more symmetry the system maintains, the lower the entanglement that is preserved. Both features, namely highly non-local interactions and little or no symmetry, are present in the Hamiltonians that describe quantum algorithms designed to solve NP-complete problems. Indeed, it has been numerically shown that entanglement scales maximally in such systems [12]. This is important, it can be shown that systems with little entanglement can be efficiently simulated on a classical computer. The proposed quantum algorithms use as much entanglement as possible and are thus hard to simulate classically.

Conclusions

Following the development of many new tools for the description of entanglement in quantum information science we are now beginning to reap the benefits of this work. These new tools are of particular importance in new insights that are being gained into the connection between entanglement and statistical mechanics. Beautiful results have been obtained and the cross-fertilization between Quantum Information and Statistical Mechanics is likely to continue for the next years and provide many new insights beneficial for both fields of research.

References

[1] V. Vedral and E. Kashefi, "Uniqueness of Entanglement Measure and Thermodynamics", Phys. Rev. Lett. **89**, 037903 (2002)

[2] K. Audenaert, M. B. Plenio, and J. Eisert, "Entanglement Cost under Positive-Partial-Transpose-Preserving Operations" Phys. Rev. Lett. **90**, 027901 (2003)

[3] M. Horodecki, P. Horodecki, R. Horodecki, J. Oppenheim, A. Sen De, U. Sen, B. Synak, "Local versus non-local information in quantum information theory: formalism and phenomena", e-print quant-ph/0410090

[4] F. Verstraete, M.A. Martin-Delgado and J.I. Cirac, "Diverging Entanglement Length in Gapped Quantum Spin Systems", Phys. Rev. Lett. **92**, 087201 (2004)

[5] J.K. Pachos and M.B. Plenio, "Three-spin interactions in optical lattices and criticality in cluster Hamiltonians", Phys. Rev. Lett. **93**, 056402 (2004)

[6] G. Vidal, J. I. Latorre, E. Rico, A. Kitaev, "Entanglement in quantum critical phenomena", Phys. Rev. Lett. **90** 227902 (2003)

[7] J.P. Keating and F. Mezzadri, "Random Matrix Theory and Entanglement in Quantum Spin Chains", e-print arxiv quant-ph/0407047

[8] M.B. Plenio, J. Eisert, J. Dreissig and M. Cramer, "Entropy, entanglement, and area: analytical results for harmonic lattice systems", e-print arxiv quant-ph/0405142

[9] F. Verstraete, D. Porras, J. I. Cirac, "DMRG and periodic boundary conditions: a quantum information perspective", Phys. Rev. Lett. **93**, 227205 (2004)

[10] J.I. Latorre, C.A. Lutken, E. Rico, G. Vidal, "Fine-grained entanglement loss along renormalization group flows", e-print arxiv quant-ph/0404120

[11] F. Verstraete, J.I. Cirac, J.I. Latorre, E. Rico, M.M. Wolf, "Renormalization group transformations on quantum states", e-print arxiv quant-ph/0410227

[12] R. Orus, J.I. Latorre, "Universality of Entanglement and Quantum Computation Complexity", Phys. Rev. A **69**, 052308 (2004)

Projects funded by the European Commission and related to the work in this article:

EQUIP
Entanglement in Quantum Information Processing and Communication
Start date: 01/01/2000
End date: 31/12/2002
http://www.equip.qipc.org/description.html
Contact Person: Martin Wilkens, Martin.Wilkens@quantum.physik.uni-potsdam.de Universität Potsdam, Am Neuen Palais 10, 14469 Potsdam

QUPRODIS
Quantum Properties of Distributed Quantum Systems
Start date: 01/01/2003
End date: 31/12/2005
http://www.quprodis.org/
Contact Person: Martin Wilkens, Martin.Wilkens@quantum.physik.uni-potsdam.de
Universität Potsdam, Am Neuen Palais 10, 14469 Potsdam

Projects funded by National initiatives or organizations and related to the work in this article:

QIP IRC
Quantum Information Processing Interdisciplinary Research Collaboration
Start date: 01/04/2004
End date: 31/03/2009
http://www.qipirc.org/
Contact Person: Andrew Briggs, Department of Materials, University of Oxford, andrew.briggs@materials.ox.ac.uk

Contact information of the authors of this article:
José I Latorre
Departament d'Estructura i Constituents de la Matèria
Universitat de Barcelona
Diagonal 647
08028 Barcelona
Spain
Email: latorre@ecm.ub.es
Web page: http://sophia.ecm.ub.es/latorre/

Martin B Plenio
Quantum Optics and Laser Science Group, Blackett Laboratory
Imperial College
Prince Consort Road
London SW7 2BW
UK
Email: m.plenio@imperial.ac.uk
Web page: http://www.lsr.ph.ic.ac.uk/~plenio/

Quantum algorithms

Harry Buhrman
Harry Buhrman is working at the CWI, Amsterdam, The Netherlands. He obtained his Ph.D. at the University of Amsterdam in 1993. In 1997 he joined the Dutch national research institute for computer science and mathematics (CWI) and in 2000 was appointed full Professor at the University of Amsterdam. He heads the quantum computing group at the CWI. His research area includes quantum computing and computational complexity theory. He was coordinator of the EU-funded IST FP5 project QAIP.

Richard Jozsa
Richard Jozsa is Professor of Computer Science at the University of Bristol UK. He obtained his DPhil in Mathematics from Oxford in 1981. His research area is quantum information science and his achievements include co-invention of quantum teleportation and (with Deutsch) the first demonstration of the power of quantum over classical computation. From 1998 to 2003 he was an EPSRC Senior Research Fellow and in 2004 he was awarded the LMS Naylor prize for his work in quantum computation and information.

Miklos Santha
Miklos Santha is working at CNRS, LRI, Orsay, France. He received a Ph.D. in Mathematics from Paris in 1981, and a Doctorat d'Etat in Computer Science from Orsay in 1988. In 1988 he joined the CNRS where he is a senior researcher in the Laboratoire de Recherche en Informatique at Orsay and

where he heads the team “Algorithms and Complexity”. His research interests include quantum computing, randomized algorithms and complexity theory. In the last decade he was the coordinator for LRI of several EU projects on randomized and quantum algorithms.

Abstract

The study of quantum algorithms is one of the most tantalising and imaginatively captivating areas in all scientific research today. It is based on the realisation that novel non-classical features of quantum physics can be ingeniously exploited to provide immense benefits for computation and communication. In this article we will convey the significance of quantum theory from the point of view of computer science and then go on to describe some of the most significant known applications to computational tasks. European scientists have made many groundbreaking contributions, firmly establishing Europe as a world leader in this subject.

Introduction

Many central areas of development in the modern world are being increasingly dominated by information technology**.** We are witnessing an insatiable drive for ever increasing computing power in the storage, processing and communication of information, as computers become increasingly miniaturised and faster in terms of microprocessor clock speed.

In the mid 1980s the UK physicist D. Deutsch emphasised that there is a profound relationship between physics and computer technology [1] which may be simply stated as follows: computers are necessarily *physical* objects and computations are always *physical* processes. This statement, which may appear innocuous at first sight, has remarkable and far reaching consequences. It implies that the possibilities and limitations of computation (and further cognate issues such as data security, computational complexity etc.) are not purely abstract mathematical issues but instead these questions must rest on the laws of physics.

With the current state of miniaturisation in computer fabrication technology, logic gates will soon reach an atomic scale where matter obeys the laws of quantum (rather than the more familiar classical) physics. Hence a new quantum technology must replace or supplement what we have now. This leads to a startling realisation: quantum technology can offer far more than just an increased level of miniaturisation and higher clock speeds – it can support entirely new kinds of computation based on quantum principles offering qualitatively new (“non-classical”) algorithms and new modes of communication with remarkable features. The subject of quantum algorithms focuses on the study and exploitation of such intrinsically new quantum modes of computation and communication. We will see that it leads to an immensely enhanced level of computational power and many of its most significant applications have been developed by European scientists.

Bits and qubits – encoding information

Information may always be encoded in a standard form as a sequence of 0’s and 1’s, the two possible values of a *bit*. For example any text using the 26 letters of the alphabet may be unambiguously encoded using a choice of some 26 of the 32 5-bit strings and any text is then written as a sequence of bits. In physical terms the bit values 0 and 1 always refer to two distinguishable physical states of some physical system. For example in a digital electronic computer, two levels of voltage are used. One bit of information may also be encoded in two

different polarisations of a photon or in two different electronic states of an atom. In the latter cases the physical system is governed by the laws of quantum physics and is not well described by the laws of classical physics.

Consider a bit encoded in a quantum system such as the polarisation of a photon where the values 0 and 1 chosen to correspond to the basic states of horizontal and vertical polarisation. According to the laws of quantum mechanics the system may also be in a coherent *superposition* of the two basic states. In such a state the system is interpreted intuitively as being "simultaneously in both state 0 and 1" (to varying degrees that depend on coefficients that determine the exact form of the superposition). Any such physical system that may encode the basic bit values as well as any possible superposition is called a *qubit*.

An especially important feature of the quantum behaviour of qubits arises when we consider a string of several bits or qubits in a row. This is the phenomenon of *quantum entanglement*, discussed at length in other sections of this volume, and which is fundamentally important for quantum algorithms. The basic idea from our perspective is the following. Consider two bits in a row. There are four possible states 00,01,10,11. If these are encoded in a quantum system of two qubits then in addition, we can have any superpositions of the four possibilities. More generally for n bits there 2^n possibilities but any single state of n bits may be written simply as a bit string of length n. In contrast n qubits may be in a superposition of all 2^n possibilities and the state of the system now has an exponentially large description. In this sense multi-qubit systems have an "exponentially enhanced richness" for embodying information compared to classical multi-bit systems of the same physical size. This feature has profound consequences for information processing and communication as described below.

So far we have discussed how information may be *encoded* in the state of a physical system. An important dual aspect is how information may be *accessed* or *read out*. Again we find a dramatic difference between classical and quantum physics. Information in classical physics may in principle always be read out completely and perfectly. In stark contrast, the laws of quantum physics dictate that any attempt to read the information encoded in a multi-qubit quantum state will irretrievably disturb the state. In fact only a very small amount of the vast information content may be read out while the rest must remain inaccessible! The full "unknowable" information embodied in the identity of a quantum state is called *quantum information*.

Information processing – quantum computation

When a physical system evolves in time, the identity of its state changes. Thus quantum physical evolution may be naturally viewed as the processing of quantum information. The laws of physics allow us to predict and *calculate* the changing identity of the state. Feynman in 1982 made a remarkable and profound observation: if we calculate or "simulate" the quantum evolution on any standard (classical) computer then the amount of computational effort involved generally grows enormously as time passes. Soon the space and time resources needed to continue the simulation will exceed all that is available while the physical system itself continues to evolve steadily in time without any increasing overheads in resources. Thus we arrive at a bizarre picture of the quantum world: in ordinary time evolution nature processes quantum information at an astonishing rate that cannot be matched by any conventional computer simulation, yet when the processing is finished, most of the information is kept hidden and inaccessible to being read!

A quantum computer is any physical device that exploits the greatly enhanced information-processing power of quantum evolution for computational purposes. The first formal model for such a device was proposed in the UK by Deutsch [1]. The very restricted accessibility of the resulting processed quantum information imposes a severe limitation on our ability to exploit the enhanced computing power but it does not annul it!

As a basic illustrative example suppose we have a quantum computer programmed to compute a function f(x). The computer evolves the labelled input state encoding x to a labelled output state which encodes the value of f(x). Now we may prepare the input state to be an equal superposition of *all* possible input values x. Running the computer *once* then produces an output state whose quantum information content encodes *all* the values of the function in superposition. This process, introduced by Deutsch [1], is called computation by quantum parallelism. Because of the inherent inaccessibility of quantum information we are unable to read out all the function values from the output state. Nevertheless small amounts of "global" information – information about the set of all function values – may be read out, and this information, although small, may still require a vast (exponential) amount of computing effort to obtain on a conventional classical computer. Below we will describe important basic examples.

The Deutsch-Jozsa quantum algorithm and computational complexity

The first quantum algorithm to explicitly exhibit the benefit of quantum over classical computation was given by Deutsch and Jozsa (UK) in 1992 [2]. It was a starting point that inspired several of the most important subsequent developments in the subject. Our computational task is the following. We are given a black box that computes a function f. The inputs x are n-bit strings and the function values are single bits i.e. f(x) is 0 or 1 for any n-bit string x. It is promised that f is either a constant function (i.e. all values are 0 or all are 1) or else f is "balanced" in the sense that exactly half of its 2^n values are 0 and half are 1. Our task is to decide with certainty whether f is balanced or constant using the least number of queries to the box.

In the classical case it can be argued that exponentially many queries are needed (in fact a number exceeding $2^{(n-1)}$) whereas in the quantum context the problem may be solved with only a *single* query! We can get an intuitive idea of the algorithm as follows. Suppose we represent value 0 by a black bar and value 1 by a white bar. Then a constant function is represented by a pattern that's uniformly all black or all white whereas a balanced function is represented by a varying pattern of black and white bars in equal number. We want to distinguish these two types of pattern and we are allowed only to examine bars individually. Classically we need to examine many individual bars before we can be certain whether the pattern is uniformly coloured or not. But in the quantum case we can examine all bars in *one* look-up by examining them all individually simultaneously in superposition. The pattern effect that we wish to discern is a very small amount of "global" information about all the bars together, which can then be obtained from this single superposition state. It is significant to note that the quantum method involves an *exponential* reduction in the number of queries - a huge benefit over any classical method.

To obtain a systematic measure of the benefits of quantum computation relative to classical computation generally we assess the difficulty or *computational complexity* of any computational task in terms of the resources of time (number of steps) and space (amount of memory) needed to solve it. Evidently these resources will generally increase with the size of the input for the task and we ask how *rapidly* these resources grow as a function of input size.

For example in the Deutsch-Jozsa algorithm above we take the input size to be n, the number of bits that form the input to the black box. Then for any classical algorithm the time resource will grow exponentially with input size (as exponentially many queries are needed) whereas the quantum algorithm requires only linear growth of time resources; (in addition to the single query, about 3n further steps are needed [2] to extract the desired pattern information) i.e. the quantum algorithm is *exponentially faster* than any classical algorithm.

Shor's quantum factoring algorithm and the quantum Fourier transform

As another example of computational complexity consider the computational task of multiplication: the input is a pair of n digit numbers and the output is their product. The simple multiplication technique taught in primary schools is an algorithm that uses roughly n^2 steps to compute the product. We say that this is a *polynomial time* or *efficient* algorithm since the number of steps is bounded by a constant power (i.e. a polynomial function) of the input size. This is in contrast to an exponential growth which eventually outstrips any given polynomial. Algorithms running in polynomial time are regarded as "feasible in practice" in terms of their resource consumption. Algorithms requiring more than polynomial time are viewed as intractable - not really executable in practice as they consume resources at an unacceptably high rate.

The reverse task, factorisation, is to take an n digit number A (assumed here to not be a prime) and output a smaller number (not 1) that divides A exactly. The fastest known classical algorithm requires a number of steps that exceeds 10 to the power of the square root of n i.e. no efficient (classical) algorithm is known for factorisation. As n grows relatively modestly, the time required for factoring grows astronomically. The task quickly becomes intractable whereas multiplication (for a similar range of n values) can be performed in a fraction of a second.

In 1994 Peter Shor (then at Bell Labs, USA) announced a landmark result: he gave an efficient quantum algorithm for factorisation. In contrast to the intractable classical algorithms Shor's quantum algorithm runs in a number of steps less than n^3 where n is the number of digits of the number being factored.

The details of how this algorithm works may be seen in the review article [3] by Ekert and Jozsa (one of the earliest and most widely read accounts, prepared with support from the **EU TMR network ERP-4061PL95-1412**). Here we will give only a brief intuitive overview. We begin by applying some pure mathematics (developed by the great French mathematician Legendre in the early 1800s) that converts the task of factorisation of A into the task of determining the *period* of a suitably constructed function f. In fact f may be taken to be the exponential function $f(x) = 2^x \bmod A$ where x ranges over whole numbers. The sequence of values f(1), f(2), f(3),... eventually repeats and cycles through the same set of numbers. We want to determine the length of this cycle. This periodicity is a pattern feature of the graph of f and we saw above that quantum computers have a special advantage over classical computers in extracting just such pattern features or global properties. Classically we need to evaluate f many times (in fact intractably many times) before we can discern the periodicity with confidence. However a quantum process can evaluate many values of f all in superposition, in only a single execution of f and extract the periodicity information from a small number of such runs.

A fundamental ingredient in the quantum factoring algorithm is the so-called *quantum Fourier transform* [3, 4]. The Fourier transform is a classical mathematical construction that has been known for over a hundred years to be useful in problems involving periodicities (such as discerning periodic influences from tables of ocean tide heights). In a quantum context this powerful tool has a far greater efficacy as the particular mathematical form of the Fourier transform serendipitously aligns with the mathematical formalism of quantum physics! In more technical terms, it is a *unitary* transform and furthermore as a consequence of properties of entanglement, it can be efficiently applied to a very large data set when the latter is presented in superposition [3, 4]. In fact this property is the essential key to the efficiency of the quantum factoring algorithm.

In pure mathematics the concept of the Fourier transform may be generalised and extended into a beautiful and elegant theory - the so-called theory of Fourier transforms on general groups - providing an associated generalised notion of periodicity. Using these generalised notions other important computational tasks may be viewed as periodicity problems and hence solved efficiently on a quantum computer. An example (given by Shor) is the so-called evaluation of discrete logarithms [4] a problem which has fundamental importance in public key cryptography. The problem of periodicity determination in the generalised (group theoretic) setting is known as "the hidden subgroup problem". An account of this fundamental theory is given in [4] (produced with support from the EU network QAIP). In the next section we will describe this seminal problem and outline the quantum algorithm which efficiently solves it.

The hidden subgroup problem

A growing trend in recent years in quantum computing has been to cast quantum algorithms in a group theoretical setting. Group theory provides a unifying framework for several quantum algorithms, clarifies their key ingredients, and therefore contributes to a better understanding of why they can in some contexts be more efficient than the best known classical algorithms. The most important unifying problem of group theory for the purpose of quantum algorithms turned out to be the so-called hidden subgroup problem (HSP) which can be cast in the following broad terms. Let G be a finite group and let H be a subgroup of G. We are given an efficiently computable function f mapping G into a finite set which "hides" the subgroup H in the following sense: f is constant on the left cosets of H and it takes distinct values on different cosets. The computational task is to determine the unknown subgroup H, while being allowed to query values of the function f.

Every known classical algorithm which solves the HSP takes polynomial time in the size of the group G. Quantum computing enables us to solve the problem in polynomial time in the *logarithm* of the size of the group whenever G is abelian (which means that the group multiplication is commutative), and also in some cases when G is non abelian. This represents an exponential speedup over classical algorithms. We present now an outline of the quantum algorithm for the abelian case, which is based on the quantum Fourier transform.

To appreciate better the power of the quantum Fourier transform, some familiarity is needed with characters of abelian groups. By definition, a character is a complex valued function on the group which "respects" the group multiplication in the following sense: the value of the function at the product of two group elements is the complex product of the values taken at the individual elements. If n is the size of the group then there are always n different characters, and the value of a character at any group element is always an n^{th} root of the unity.

The characters over G also form group which is isomorphic to G, so we can label the characters by the group elements themselves. As an example suppose that G is the cyclic group of integers modulo d. Then the value of the y^{th} character at the group element x is the $(xy)^{th}$ power of some fixed principal d^{th} root of the unity. From this rule we can deduce the character values over any general abelian group as any such group is always direct products of cyclic groups. With the help of the characters we can define for any subgroup H its so-called orthogonal subgroup: it consists of the group elements y for which the y^{th} character maps every element of H into unity. To recover H it is sufficient to know its orthogonal subgroup, since there is an efficient classical algorithm which determines H from it. In fact the quantum procedure for solving the HSP will just sample randomly from the orthogonal group of H.

The characters of G form a basis of the n-dimensional vector space of complex valued functions over G. Another useful basis of this vector space is the computational basis. In that basis the function associated with the group element y simply takes the value 1 at the point y, and 0 everywhere else. In these terms the Fourier transform over G can be defined as the basis transformation which maps the computational basis to the character basis. Whereas implementing the Fourier transform *classically* takes polynomial time in n, there is a quantum procedure which achieves this in time polynomial in the *logarithm* of n i.e. an exponentially shorter time. Currently every quantum algorithm with exponential speedup over classical computations uses this efficient quantum Fourier transform. Mathematically, the following property of the quantum Fourier transform is used in the algorithms for HSP. Let us suppose that we have a uniform superposition of the group element labels ranging over a coset of the hidden subgroup H, and we apply the quantum Fourier transform to it. Then, independently of which coset was the support of the superposition, we will end up in a uniform superposition over the orthogonal subgroup of H, where only the *phase* of the superposition coefficients will depend on the particular coset that we started with. Stated more intuitively: if we consider the coset as a kind of "perturbation" of the hidden subgroup, then the Fourier transform will smoothen it by transforming the perturbation into innocuous phases.

Let us now outline the quantum algorithm itself for HSP. We begin by setting up a quantum state that represents a uniform superposition of all the elements of the group G. (This can be readily achieved using the Fourier transform applied to a standard starting state). Next, using this state as input to the evaluation of f, we obtain a uniform superposition of all pairs (x, f(x)). A quantum measurement of the value of f in the second register will yield a randomly chosen value $f(x_0)$ and collapse the first register to the superposition of only those x's with the same value $f(x)=f(x_0)$ i.e. the coset x_0+H of G. If we now perform a Fourier transform on this state, then as we said previously, we will end up with the uniform superposition over the orthogonal subgroup of H, where the information of x_0 appears only in the phases of the superposition coefficients. If we now measure this state, we will receive a random element of the orthogonal subgroup of H, independently of x_0. When this process is repeated about log n times, we will have enough information to (classically) determine H efficiently.

What can be said about the HSP when the group G is not abelian? First of all, it contains as special cases several famous and important problems. A primal example is the problem kmown as graph isomorphism. For this problem the input is two graphs with the same number of vertices, and it has to be decided if they are isomorphic. To be isomorphic there has to be a matching between the vertex sets of the two graphs which also exactly matches up all the edges. It can be shown that the graph isomorphism problem is equivalent to an instance of the HSP in the case that G is the (non-abelian) full permutation group.

The other important remark about the non abelian case is that it is much harder than the abelian one. Let us point out here two possible difficulties which can arise if we try to copy the Fourier sampling based algorithm which worked well for the abelian case. Firstly, there might not be efficient implementations for the quantum Fourier transform. And secondly, even if there is one (which is for example true for the permutation group), there might not be an efficient analogue of the classical procedure which reconstructs the subgroup H from the outputs of the Fourier sampling.

Still, there are some important positive results about HSP in the non abelian case, and many have been contributed by European researchers. Using the Fourier sampling approach, Roetteler and Beth [5] could solve it in the case of some special wreath product groups, and Friedl, Ivanyos, Magniez, Santha and Sen [6] could handle the case of solvable groups with constant exponent and of constant length derived series. In a different approach without using the Fourier transform Ivanyos, Magniez and Santha [7] constructed an efficient quantum algorithm for solvable groups when the hidden subgroup is normal. Let us close this section by mentioning the very intriguing case of the dihedral group (the group of symmetries of a regular polygon). Ettinger and Hoyer [8] could show that a small number of Fourier samplings give already enough information to recover the hidden subgroup. Nevertheless it is still unknown whether there exists an efficient (classical or quantum) algorithm which implements the recovery process. The general HSP continues to provide a fascinating and important research challenge today!

Quantum search and quantum walks

We have seen that quantum computers can be very effective in problems involving a lot of structure, which was represented as a pattern in a large volume of data. Quantum computers can also help in problems with less structure too, providing benefits over classical computing that are very significant. In his celebrated result, Grover has shown that a marked item in a set of n elements can be found quadratically faster using a quantum algorithm than by any classical, deterministic or randomized process. Let us emphasize that the elements in the set where the search is performed don't have any particular structure, the only information we can receive about them is by querying (in one computational step) if an item is marked or not. This type of computational model is often referred to as oracle computation, and the complexity of the process is measured by the number of queries.

Classically search problems are often solved by random walks in graphs. Therefore it was natural to look for quantum analogues of random walks, and indeed this subject is currently a a flourishing research area, with surprising applications to algorithmic problems. For example Grover's algorithm can be reinterpreted as the quantum analogue of the random walk in the complete graph on n elements.

A classical random walk is performed on the vertices of a finite undirected graph. It starts from some specific vertex of a graph, or more generally from some initial distribution on the vertices. At every time step, if the walk is at some vertex u of degree d (i.e. d is the number of edges emanating from u), then one of the neighbouring vertices is selected with uniform probability 1/d.

The above random walk can be described in an alternative way using edges rather than vertices as the basic sites. To be more precise, we can direct the edges in both directions, and take the state space for the walk to be the set of all directed edges. In this picture a step of the

walk comprises two elementary transformations. If the state of the walk is the edge (u,v), then first a "coin flip" is performed i.e. we make a probabilistic replacement of (u,v) by (u,w) where w ranges over all neighbours of u and each is selected with probability 1/d. Next a shift transformation takes place which simply maps (deterministically) the edge (u,w) to (w,u). It can be shown that resulting distribution on the source vertices of the edges will then be the same as the distribution as obtained in the original walk over the vertices. Why do we bother mentioning this alternative description of the walk? The reason is that this way of looking at classical walks is much more amenable to quantization.

The state space of the quantum walk will also be the set of directed edges (u,v), and a basic step will be the product of two unitary transformations similar to the above: a coin flip and a shift. The coin flip can be any unitary transformation which is, for every vertex u, locally unitary over the set (u,v), where v is a neighbour of u. A natural choice for this local unitary transformation turns out to be the so-called diffusion operator which is at the heart of Grover's algorithm. (Geometrically this is the reflection in the uniform superposition over all states (u,v), where again v is a neighbour of u). The shift operation is the same as in the classical case.

Quantum walks may be applied to search problems, leading to some beautiful algorithmic solutions. As an example we mention the element distinctness problem. In this problem we are given a set of n numbers which have indices from 1 to n, and one has to decide if there are two identical numbers among them. Classically this problem can not be decided with less than n queries, but Ambainis [10] has shown that in a quantum context, $n^{2/3}$ queries are sufficient. The algorithm uses a quantum walk on a graph whose vertices are the subsets of size $n^{2/3}$ of the indices. There is an edge between two sets if they differ exactly in two elements. Graph theorists call this graph the Johnson graph. We say that a vertex A is marked if it contains two indices that label the same number and then the walk will find a marked set, if there is any. The behaviour of this walk may be elegantly analysed using a recent result of Szegedy [9] showing that the running time is of order $n^{2/3}$.

Let us close this section by mentioning a few further applications of this new theory, again mostly due to European scientists. Magniez, Santha and Szegedy [11] designed a quantum algorithm which decides if there is a triangle in an n vertex graph with $n^{13/10}$ queries. The obvious application of Grover search would yield an algorithm with $n^{3/2}$ queries since there are potentially n^3 triangles in a graph. The beauty of this algorithm is that it calls a quantum walk inside another one as its checking procedure. Buhrman and Spalek [12] applied quantum walks to the following problem: given three n x n matrices A,B and C, decide if the product of A and B is equal to C. Here an interesting feature is that their result applies not only for query complexity, but also for the number of scalar multiplications. Classically the best randomized algorithm takes time n^2 whereas the quantum algorithm requires time $n^{5/3}$. Finally Ambainis, Kempe and Rivosh showed that for the marked item search problem we can get essentially the same speed up benefits in a rectangular grid graph as in the complete graph (which has every pair of vertices connected by an edge).

Distributed computation - communication complexity

The success story of quantum algorithms is tremendous and one might wonder whether qubits and quantum information processing may also be more efficient for the transfer of information over quantum *communication networks*. Indeed a single qubit has a general state that is labelled by continuous parameters and one might ask: can we use a single qubit to

encode a message that consists of *many* classical bits? Unfortunately this is not the case. A single qubit can contain at most a single bit of information as was demonstrated early on by Holevo [14]. Qubits are not more powerful for the transmission of information than classical bits. Suppose Alice (in Paris) wants to send a message to Bob (in Amsterdam) that is a 1000 bits long, then she needs to send also 1000 qubits to Bob and there is no way of doing this with fewer qubits.

But the story is dramatically different when we change the setup slightly! Suppose that Alice does not want to send a message to Bob but instead she wants to make an appointment with him to spend a day together. Since both Alice and Bob have a hectic lifestyle and busy schedules they have to compare their diaries to find a timeslot in which they both are available. Classically the following conversation might occur: Alice: Hello Bob, how are you doing? Shall we make an appointment to spend some time together? Bob: darling that is a great idea I am really worn out and I could use some time off. How about this coming Monday? Alice: well let's see, hmm, this Monday I have an appointment with my dentist and in the afternoon I have my Yoga lesson. Did I tell you how relaxing they are? How about Wednesday? Bob: oh no not on Wednesday, then I have to go to court to settle a case with my neighbour. Friday is good for me, how about that? Alice: no not Friday, I am seeing my mother. Etc… This conversation can take a long time, and will result in a high telephone bill until Alice and Bob finally find out that they are too busy to see each other in the near future.

It can be shown that the best possible classical protocol for this problem is for Alice to send the data of her *whole* diary to Bob, who then can decide whether they have a free slot available and when. Suppose that the diary of Alice is 10000 Kbits in size. Then she has to send that many bits to Bob, and that is the best they can do.

Surprisingly in a quantum world they can actually do much better as Buhrman, Cleve, and Wigderson showed [15]. If Alice and Bob were to use a quantum communication channel then they would only need to send about 100 Kqubits (this being the square root of the classical requirement above). This saving in communication is quite surprising since it seems to contradict the earlier mentioned result of Holevo. The difference is that we are not dealing with a message that needs to be transmitted but a distributed function, in this case the appointment scheduling problem. The actual information that Alice and Bob want to learn is the time and day that they both are available (if at all). This is very little compared to the whole diary that needs to be sent in the classical scenario.

The quantum communication protocol for the appointment scheduling problem uses the ideas of the fast search and quantum random walk algorithm discussed above. The quantum protocol is magically able to zoom in on a free slot without explicitly distributing the diary data between Alice and Bob. In a similar way, using a distributed version of the Deutsch-Jozsa problem and algorithm, even *exponential* savings in communication cost can be achieved if Alice and Bob use a quantum channel.

Using a quantum scheme called *quantum fingerprinting*, Buhrman, Cleve, Watrous, and de Wolf [16] demonstrated another distributed scenario where quantum communication establishes and exponential superiority. The quantum fingerprinting scheme has the property that it already on just a *few* qubits outperforms any classical protocol and thus is an ideal candidate for prospective near term physical implementation. The scheme has the additional bonus that it can be used in cryptographic protocols, like quantum digital signatures and quantum string commitment schemes (not discussed in this article). Thus quantum

fingerprinting and variants may in the short term lead to a variety of few-qubit implementations and this protocol has the potential to become a commercial product.

The study of quantum distributed computing has also sheds new light on the famous nonlocality "paradox" of Einstein, Podolsky, and Rosen, introduced long ago in 1935. The paradox is a thought experiment that was intended by its authors to show that quantum mechanics in its current form was incomplete. The paradox involves two entangled quantum particles, nowadays called EPR-pairs. Quantum mechanics predicts that, as a consequence of entanglement, the two particles will behave as a single global entity even if they are widely separated in space. For example a measurement on one particle can instantaneously change the state of the other, contradicting the postulate that influences cannot travel faster than the speed of light. Modern experiments indeed have shown that this entangled behaviour is reality and this feature constitutes one of the essential quantum novelties that makes quantum computation so successful and interesting. Buhrman, Hoyer, Massar, and Roehrig [17] demonstrated that the tools, techniques and protocols developed for (distributed) quantum computing, such as the algorithms discussed in the previous sections, can be used to construct new experiments that put beyond all doubt the entangled behaviour of EPR-pairs. This line of research demonstrates a valuable and significant interplay between the disciplines of physics and computer science.

Outlook

In current research development, quantum computing continues to take fascinating and unexpected turns. A significant recent development is the surprising application of quantum computing techniques to establish *classical* results in computer science and mathematics. De Wolf and Kerenidis [18] have shown that a quantum algorithmic technique, combined with quantum information theory leads to a result in classical coding theory. This result is seen as a breakthrough in classical coding theory and opens up a whole new avenue of quantum computing research. It is important to note that these results do not require a working quantum computer! A current trend in quantum computing is that more of these applications to classical computer science and mathematics are emerging. The section on distributed quantum computing shows that such an application is also possible to physics and we expect to see more of these in the near future.

Another important programme for further research is the understanding of the origins of quantum computational speed-up and also their limitations, characterising the particular quantum physical features that underlie computational benefits. A significant step in this programme was taken by Jozsa and Linden [19] in the EU RESQ network, demonstrating an explicit relationship between quantum computational speed-up and the presence of entanglement in the quantum states produced during the algorithm. Another important step was made by Raussendorf and Briegel [20] in Germany in 2000 developing a model for quantum computation in which information processing is carried out entirely by quantum measurements. This remarkable concept is intrinsically quantum, having no counterpart in the conventional (classical) theory of computation. This general programme is especially exciting as it may shed light on the nature and origins of physical laws themselves, perhaps even leading to an understanding of the highly enigmatic structure of quantum theory in terms of concepts from computation and complexity.

We have seen the fundamental significance of the quantum Fourier transform in the development of many quantum algorithms and a continuing important programme for future

research is the recognition of further such tools and the invention of corresponding new quantum algorithms.

Conclusions

The study of quantum algorithms is one of the most tantalising and imaginatively captivating areas in all scientific research today. It draws together in a very explicit way, fundamental inputs from theoretical computer science and quantum physics, offering remarkable insights for both. Indeed the subject of quantum information processing has developed to become one of the most active and high profile areas in current scientific research. However the Computer Science component has traditionally been under-represented and a growing awareness of this fact in the US and Canada has lead to some very large scale investment in those countries (e.g. the Perimeter Institute, Waterloo, Canada). If Europe is to enjoy a healthy continuation of its excellent track record of internationally leading research in this field, substantial funding initiatives and support from the EU will be required to retain Europe's most talented and brilliant young researchers within Europe.

References

[1] Deutsch, D. 1985 Proc. R. Soc. Lond. A400, 97.
[2] Deutsch, D. and Jozsa, R. 1992 Proc. R. Soc. Lond. A439, 553.
[3] Ekert, A. and Jozsa, R. 1996 Rev. Mod. Phys. 68, 733.
[4] Jozsa, R. 2001 Comp. Sci. Eng. March/April issue, 34.
[5] Roetteler, M. and Beth, T. 1998 http://xxx.lanl.gov/abs/quant-ph/9812070.
[6] Ivanyos, G. Magniez, F. and Santha M. 2003 Int. Journ. Found. Comp. Sci. 14(5), 723-740.
[7] Friedl, K. Ivanyos, G. Magniez, F. Santha M. and Sen, P. 2003 Proc. 35th ACM STOC. 1-9.
[8] Ettinger. M. and Hoyer, P. 2000 Adv. in Appl. Math. 25(3), 239-251.
[9] Szegedy, M. 2004 Proc. 45th IEEE FOCS, 32-41.
[10] Ambainis, A. 2004 Proc. 45th IEEE FOCS, 22-31.
[11] Magniez, F. Santha, M. and Szegedy, M. 2005 Proc. 17th ACM-SIAM SODA.
[12] Buhrman, H. and Spalek, R. 2003 http://xxx.lanl.gov/abs/quant-ph/0409035
[13] Ambainis, A. Kempe, J. and Rivosh A. 2005 Proc. 17th ACM-SIAM SODA.
[14] Holevo, A.S. 1973 Problems of Information Transmission 9, 177-183.
[15] Buhrman, H. Cleve, R. Wigderson, A. 1998 Proc. 30th ACM STOC. 63-68.
[16] Buhrman, H. Cleve, R. Watrous, J. de Wolf, R. 2001 Phys. Rev. Lett. 87(16), 167902
[17] Buhrman, H. Hoyer, P. Massar, M. Roehrig, H. 2003 Phys. Rev. Lett. 91, 047903
[18] Kerenidis, J de Wolf, R. 2004 *Journal of Computer and System Sciences*, 69(3):395-420
[19] Jozsa, R. and Linden, N. 2003 Proc. R. Soc. Lond. A459, 2011.
[20] Raussendorf, R. and Briegel, H. 2001 Phys. Rev. Lett. 86, 5188.

Projects funded by the European Commission and related to the work in this article:

QI (TMR network)
The physics of quantum information
http://info.uibk.ac.at/c/c7/c704/qinet/

QAIP
Quantum Algorithms and Information Processing
Start date: 04/01/2000
End date: 03/01/2003
Project web site: http://www.cwi.nl/projects/QAIP/
Contact person: Harry Buhrman, harry.buhrman@cwi.nl

RESQ
Resources for Quantum Information
Start date: 01/01/2003
End date: 31/12/2005
Project web site: http://www.ulb.ac.be/project/RESQ/
Contact Person: Serge Massar, Université Libre de Bruxelles, smassar@ulb.ac.be

EQUIP
Entanglement in Quantum Information Processing and Communication
Start date: 01/01/2000
End date: 31/12/2002
Project web site: http://www.equip.qipc.org/
Contact Person: Martin Wilkens, U Potsdam, Martin.Wilkens@physik.uni-potsdam.de

Projects funded by National initiatives or organizations and related to the work in this article:

ESF-QIT
Quantum information processing and quantum computing
http://www.esf.org/esf_article.php?activity=1&article=26&domain=1

Contact information of the authors of this article:
Harry Buhrman
Department INS4
CWI
Kruislaan 413, P.O. Box 94079
1090 GB Amsterdam
The Netherlands
Email: Harry.Buhrman@cwi.nl
http://db.cwi.nl/personen/publiek/zoek_show.php4?persnr=552

Richard Jozsa
Department of Computer Science
University of Bristol
Merchant Venturers Building
Woodland Road
Bristol BS8 1UB
United Kingdom
Email: R.Jozsa@bristol.ac.uk
Web page : http://www.cs.bris.ac.uk/People/personal.jsp?person=115954

Miklos Santha
Laboratoire de Recherche en Informatique
Universite Paris Sud
Bat. 490
91405 Orsay
France
Email: santha@lri.fr
Web page : http://www.lri.fr/~santha/

Quantum simulations

Vladimír Bužek
Vladimír Bužek is professor and head of the Research Center for Quantum Information of the Slovak Academy of Sciences. He has graduated at the Moscow State University where he has also received his PhD (1985) in theoretical physics. He has been a visiting professor at the Imperial College in London, and the National University in Maynooth, Ireland. Presently his research interests are focused on various aspects of quantum information processing.

*"**On Exactitude in Science** . . . In that Empire, the Art of Cartography attained such Perfection that the map of a single Province occupied the entirety of a City, and the map of the Empire, the entirety of a Province. In time, those Unconscionable Maps no longer satisfied, and the Cartographers Guilds struck a Map of the Empire whose size was that of the Empire, and which coincided point for point with it. The following Generations, who were not so fond of the Study of Cartography as their Forebears had been, saw that that vast Map was Useless, and not without some Pitilessness was it, that they delivered it up to the Inclemencies of Sun and Winters. In the Deserts of the West, still today, there are Tattered Ruins of that Map, inhabited by Animals and Beggars; in all the Land there is no other Relic of the Disciplines of Geography."*

Suarez Miranda,Viajes de varones prudentes (Libro IV,Cap. XLV, Lerida, 1658)
By Jorge Luis Borges, Collected Fictions (translated by Andrew Hurley, Penguin 1999).

The power of the scientific understanding of the nature of the physical universe is in its potential to predict results of experiments.

Understanding the physical universe

We comprehend a physical situation via models constructed in a framework of a specific paradigm (physical theory). This is the way how we picture and understand the world. We create models of reality to describe the world in a same way as cartographers prepare maps to picture landscape of a country. The ability to model the world is probably the most distinctive feature of human cognitive aptitudes. In order to model a physical situation (be it a photon or the whole universe) we use mathematics. The complexity of mathematical language allows us to express physical theories and models in a simple form.

What does it mean to model a physical system?

There are two aspects of modelling a physical situation. Firstly, we have to specify kinematics of a physical system, that is, we have to determine how to properly characterize and parameterize states and properties of the system. Secondly, we have to determine dynamics that reflects a time evolution of an initial state of the given system under specific conditions. Dynamics is usually determined on the basis of dynamical equations that are based on a very general formulation of the model, it might be either Lagrange or a Hamilton formalism that is used to obtain dynamical equations of the physical system.

Solving dynamical equations

In relatively simple cases equations describing evolution of physical systems can be solved. These might be either analytical or numerical solutions. Based on them prediction of results of experiments given specific initial conditions can be obtained. When we refer to numerical solutions we usually have in mind computers that are presently available. These can be classified as classical. This classification follows the observation of Rolf William Landauer according to which the information is physical. Given the fact that presently information on computers is processed based on rules of classical physics we can call these computers as classical.

Intrinsic quantum models

Unfortunately in many cases analytical solutions of physical models do not exist and numerical calculations cannot be performed on classical computers due to the complexity of the problem in hand. Richard Feynman has argued that intrinsic quantum models cannot be in general efficiently solved on classical computers. Kinematics of quantum system is very complex due to the principle of quantum superposition. States of quantum systems are described as vectors in Hilbert spaces with dimensions that exponentially increase with number of constituent particles in systems. Therefore classical computers fail to solve general quantum problems. Classical maps of the quantum world are not good enough – they are too big to be accommodated in a classical world and are to imperfect to describe quantum reality. So “cartographers” are forced to use quantum tools to describe quantum world.

Quantum computers

The paradigm of quantum information processing helps us to address most difficult models of the quantum world. Quantum computers are devices operating on the same principles as the world to be described. At least we are sure that the “map” will not be larger than the world itself. Classical computers are digital devices that represent a state or an operation in terms of binary strings. Quantum computers due to quantum superposition principle are more like analogue computers. Moreover, the nature of quantum world (the concept of infinite ensembles representing states of quantum systems and the concept of quantum measurements) directly forces us think in terms of a reduced set of relevant physical parameters of interest (specification of relevant observables) rather than a complete description of a quantum system. Consequently, one can consider quantum computers as (approximate) simulators of other quantum systems.

Quantum simulations

The isomorphism (or at least a reasonable approximation) between models of physical systems which is due to the universality of mathematical language provide us with a possibility to study efficiently one system via investigation of another system that might be under an efficient control. Therefore, a quantum system that can be relatively easy controlled (i.e. its initial states can be prepared with high fidelity and its dynamics is well controlled) can serve as a simulator of another quantum system. Here the task is not to obtain the precise "solution" but rather a realistic estimate of measurable consequences.

Stability of quantum simulators

One of the most important aspects of simulators is their stability. It has to be required that simulators are stable with respect to small uncertainties in the control of their dynamics. Any analogue simulator has to exhibit non-chaotic behaviour.

Efficiency of quantum simulators

The simulator has to be efficient enough to allow us to mimic the most complex dynamics of physical systems. Therefore we require that the resources required for simulation rise polynomially with the size of the modeled system.

On exactitude in quantum simulations

One of the greatest achievements in physics over past ten-fifteen years is a development of experimental techniques that allow us to control states and dynamics of individual quantum systems and to control there mutual interaction. We can expect that in a foreseeable future scalable quantum simulators will be available. Physics is a science of reasonable (justified) approximations. The power of quantum simulations is in their capacity to reasonably and efficiently mimic real world. Therefore they will be the most useful tool for studying the physical universe.

Projects funded by the European Commission and related to the work in this article:

EQUIP
Entanglement in Quantum Information Processing and Communication
Start date: 01/01/2000
End date: 31/12/2002
Project web site: http://www.equip.qipc.org/
Contact Person: Martin Wilkens, U Potsdam, martin.wilkens@physik.uni-potsdam.de

QUBITS
Quantum Based Information Processing and Transfer with Single Atoms and Photons
Start date: 01/01/2000
End date: 31/12/2002
Project web site: http://www.imperial.ac.uk/physics/qubits/
Contact Person: Peter Knight, Imperial College, London, UK, p.knight@ic.ac.uk

QUEST
Quantum entangled states of trapped particles
Start date: 01/05/2000
End date: 31/04/2004
Project web site: http://www.iota.u-psud.fr/~quest/index.html

Contact Person: Philippe Grangier, IOTA, Orsay, France, philippe.grangier@iota.u-psud.fr

QUPRODIS
Quantum Properties of Distributed Systems
Start date: 01/01/2003
End date: 31/12/2005
Project web site: http://www.quprodis.org/
Contact Person: Wilkens, U Potsdam, martin.wilkens@physik.uni-potsdam.de

QGATES
Quantum Gates and Elementary Scalable Processors Using Deterministically Addressed Atoms
Start date: 1/1/2003
End date: 31/12/2005
Project web site: http://www.imperial.ac.uk/physics/qgates/
Contact Person: Dr D M Segal, Imperial College London, d.segal@ic.ac.uk

CONQUEST
Controlled quantum coherence and entanglement in sets of trapped particles
Start date: 01/03/2004
End date: 28/02/2008
Project web site: http://www.quniverse.sk/conquest/
Contact Person: Vladimir Buzek, Bratislava, Slovakia, buzek@savba.sk

ERA-Pilot QIST

Contact information of the authors of this article:
Vladimír Bužek
Research Center for Quantum Information
Slovak Academy of Sciences
Bratislava, Slovakia
buzek@savba.sk
www.quniverse.sk/buzek

Hiding from the Environment: Decoherence-Free Subspaces in Quantum Information Processing

Peter L. Knight
Peter L. Knight is professor at Imperial College London, United Kingdom. He is also acting Principal of the Physical Sciences Faculty and Head of the Physics Department at Imperial College in London and Chief Scientific Advisor to the National Physical Laboratory. He is doing research in Theoretical Quantum Optics and Quantum Information Processing. Prof. Knight is a Fellow of the Royal Society and immediate Past-President of the Optical Society of America. Participation in several European (currently QGATES, CONQUEST, and soon to be SCALA) and national projects (QIP IRC of the EPSRC in the UK), Fellow of the Royal Society and Editor of Journal of Modern Optics and Contemporary Physics.

Almut Beige
Dr Almut Beige is University Research Fellow of the Royal Society at Imperial College London with previous positions at the Department of Applied Mathematics and Theoretical Physics in Cambridge and the Max-Planck-Institute for Quantum Optics in Garching. Research interests in Theoretical Quantum Optics and Quantum Information Processing, participation in several European Networks (currently QGATES and soon to be SCALA) and in the QIP IRC of the EPSRC in the UK.

William J. Munro
Dr William J. Munro is a Senior Research Scientist within Hewlett Packard Laboratories, Bristol, United Kingdom. He is working in the Quantum Information Processing group located in Bristol with previous positions within the Centre for Quantum Computation at the University of Queensland in Brisbane Australia and the Physics Department at the University of Waikato in New Zealand. His research interests have focused around the practical implementation for optical and solid state quantum hardware, the generation of optical nonlinearities and the characterization of quantum states and processes. He currently participates in the EU projects RAMBOQ and SECOQC.

Abstract
The efficiency of quantum computing relies on the fact that the behavior of quantum mechanical systems follows a different logic than the behavior of classical systems. However, it is in general difficult to find physical systems well decoupled from the environment, which might destroy their quantumness. An important task in quantum information science is therefore the engineering of systems with states hidden from the environment, which are known as decoherence-free states. Another task is finding efficient ways to manipulate them.

Introduction
A quantum computer is extraordinarily sensitive to the random disturbances it experiences from its surrounding environment. This presents major challenges to any proposed realization. One might imagine working incredibly hard to isolate the qubits that make up the quantum register from the environment. But even such an isolated register would need to be opened up to the influences of the external world, if only because the qubit manipulation and read out is done from outside. For a quantum computer to execute a quantum algorithm efficiently, it needs to evolve by unitary quantum dynamics, uninterrupted by the randomizing influences of the environment. One of the requirements for quantum computing to work efficiently is that the achievable gate operation times are much longer than the decoherence times in the system. Since it seems impossible to isolate a quantum system completely from the environment without losing the ability to manipulate its state, decoherence and the corresponding loss of information seemed unavoidable.

In this article, we describe recent developments in the area of engineering quantum computing architectures with decoherence-free subspaces, in which one hides the qubits from the environment. A crucial step in potentially overcoming the deleterious effects of the environment was the realization that quantum mechanical systems containing many components can possess large subspaces of decoherence-free states [1]. These are states, which do not couple to the environment [2]. A trivial example is the great number of ground states of a system (for example one made up of many identical atoms), which are well protected against spontaneous decay. But such DF states can even involve excited states: they

can arise from the *symmetry* of the system-environment coupling. To minimise decoherence, the quantum bits (qubits) should always remain encoded in decoherence-free states. Here we briefly review several mechanisms which allow us to manipulate a system without it ever leaving its decoherence-free subspace (DFS). Examples are given for recent implementations of decoherence-free states in quantum optical systems. We also point out future directions.

Decoherence-free states

There are many types of decoherence that can occur in a quantum mechanical system. Dissipation, for example, is the spontaneous loss of energy into the environment and occurs mainly in quantum optical systems in form of photon emissions. In other physical setups, the interaction of the system with its environment results in the accumulation of random phase factors or in random and therefore unknown flips of states encoding the information "0" into states encoding the information "1" and vice versa. Decoherence is, in general, unavoidably connected with the partial or complete loss of information previously stored in the qubits.

Error correction (described elsewhere in this collection of articles) is possible in quantum computation of course by employing ancilla to detect and repair error syndromes. But again, for resilient quantum computation, robust against errors, the gate infidelity (the margin of error or inaccuracy in the execution of a supposedly unitary gate operation) needs to be less than a part in a thousand or better. Otherwise the array of qubits making up the error correcting system actually create even more errors, in a cascade of unpredictable disturbances, making it impossible to realize fault tolerant computation. Our task is therefore to find ways of improving the resilience of systems used in Quantum Information Processing (QIP) to decoherence. One way to overcome this problem is to encode the logical information in decoherence-free states. These are states for which the probability for a decoherence event to take place is zero. Decoherence-free states are those states that effectively do not couple to the environment. Moreover, the system's time evolution should not result in the population of states which can yield decoherence at a later time. This will in general put limits on the speed of any qubit manipulation if we are to avoid shocking the system into populating unwanted and unstable states that will destroy the coherent evolution. Detailed analysis of the quantum mechanical formalism shows that the decoherence-free states always span a whole subspace of states, which makes it possible for us to use them to generate protected physical qubits (and additional ancilla states for error correction).

A trivial example of a decoherence-free state, one which is robust against spontaneous emission, is formed from those states involving only ground atomic states, as mentioned above. Another more sensible and useful example is an antisymmetric state of two atoms, one of which is excited, which couples symmetrically to the environment. In such a case, both atoms have a finite probability amplitude to emit a photon but their efforts interfere destructively and as a result, the system will remain for a long time in its initial state. In general, we have found that the more components a system is made of, the larger is its available subspace of decoherence-free states.

Another decoherence-free subspace, which allows to encode one qubit, such that it is protected against random flips of $|0\rangle$ into $|1\rangle$ and $|1\rangle$ into $|0\rangle$, respectively, is formed by the states $|00+11\rangle$ and $|10+01\rangle$. Whenever a random flip occurs, the information stored in the system does not change, since the quantum state of the system remains the same. One only has to assure that both qubits see the same environment and therefore undergo the same decoherence processes.

Depending on the effect of the environment, i.e. whether there is an exchange of energy between system and environment taking place, the decoherence-free states are sometimes called noiseless states. In certain cases, it is useful to consider decoherence-free subsystems instead of looking for decoherence-free subspaces. The subsystem idea is a genuine generalization, which includes the subspace as a special case, in the essence the difference being that information in a sub-system can be protected even though the full state of the system is not noiseless.

How to manipulate a hidden population

Initially, it was believed that decoherence-free states are so well hidden from the environment that it is practically impossible to process the information encoded in them. It was felt that as soon as an external perturbation was applied, the system would open up to decoherence and the benefits of DFS are lost. However, it has been shown that the opposite can even be true. Several schemes have been developed that allow for the implementation of quantum gate operations inside a decoherence-free subspace. Here, we give a few examples (see eg Ref 3). The easiest approach would be to engineer interactions that keep the system always inside a decoherence-free state (**Figure 1**). In this way, the system would be constantly protected against decoherence. But of course we then need to find ways to address the qubits during gate operations without unduly opening up a channel for the environment to decohere the system. Such interactions are in general difficult, but not impossible to find [3].

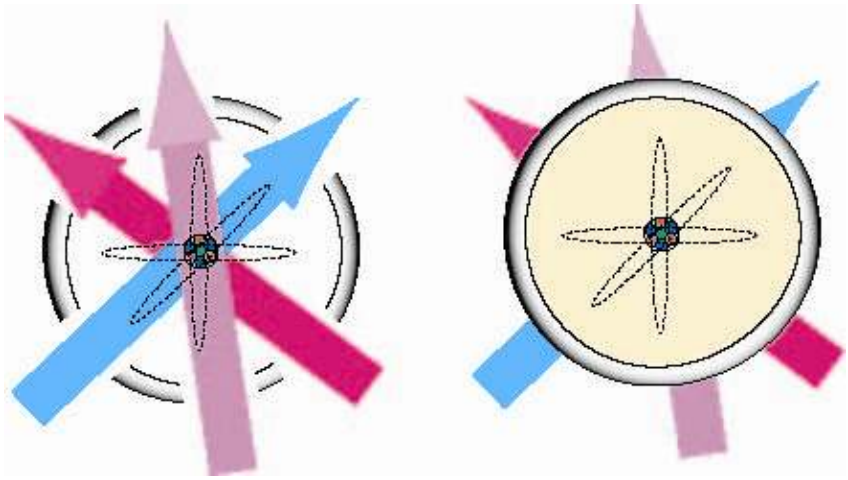


Figure 1: Cartoon indicting a qubit (schematically indicated by the orbiting Bohr atom) on the left hand side being manipulated externally (eg by laser beams) and this opening up the qubit to decoherence from the outer environment; on the right hand side we sketch a qubit entirely isolated from the environment.

Quantum computing using dissipation

High decoherence rates can actually decouple the qubits from unwanted states, such that easy-to-implement single-qubit interactions can result in quantum gate operations. They specifically employ those features which distinguish the decoherence-free states from the non-decoherence free states of a system. It has been shown (for example by Beige et al in ref[3] and in later work by several other groups) that dissipation can be used to realize quantum computing schemes that are robust, relatively fast and resourceful. Effectively, the time evolution is restricted to remain within the DFS, whatever the applied interaction. Let us give

a simple early example that was found of such a process. Cavity QED, in which trapped atoms or ions can be entangled via a mutually experienced light field offers great potential in QIP. However, the limitations of spontaneous emission and cavity field decay need to be overcome for this to be a serious method to realize a quantum register. We have proposed [3] the use of a decoherence-free subspace to almost entirely remove the errors due to cavity decay during the performance of a conditional logic CNOT gate. A DFS, as we have stressed, consists of a subspace of states each of which gain the same phase due to environmental interactions and hence remain coherent relative to each other. Using three-level transitions in what is called a Lambda configuration (essentially a Raman system) one can obtain a DFS and generate a maximally entangled state of the atoms. This entangled state may be used as a bus to perform a CNOT gate without exciting the cavity mode, provided the system is monitored for decays. The fidelity of the gate can be very close to unity to first order if all cavity decays are detected. The probability of success still depends strongly on the spontaneous emission rate of the excited levels. The well-known technique of adiabatic population transfer may be also used to enable universal quantum computing, and recent work has shown how dissipation can be used to improve the gate performance using such ideas. Readout in such a system is provided by standard electron shelving methods pioneered for ion trap experiments and known to be highly efficient.

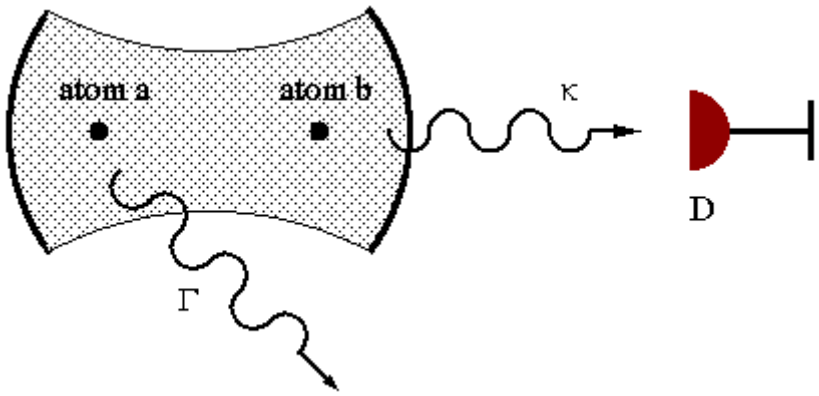


Figure 2: Schematic outline of two trapped atoms or ions labeled a and b within an optical cavity, whose state is monitored by a photodetector D: the spontaneous decay rate Gamma can be made irrelevant by the use of appropriate level and transition schemes and the DFS survives (in this scheme probabilistically) the effects of the cavity decay rate Kappa [3].

Dynamical decoupling

Another way of preventing any applied interaction from moving the system out of the decoherence-free subspace is to apply a very strong interaction that causes a very fast time evolution of all states outside the DFS [4]. Any subsequent applied additional weak interaction cannot move the system out of the DFS. This dynamically decouples the subspace.

What has been achieved so far

Several experiments demonstrating the presence of decoherence-free states and their usefulness for the coherent control of open quantum systems have already been performed. The first of them was a photon experiment by Paul Kwiat and his co-workers [5] which used

parametric down conversion to generate symmetric and antisymmetric two-photon states, which were then tested for their relative sensitivity to dephasing. The DFS state generated was shown to be substantially resistant to such sources of decoherence. This showed that at least flying qubits can be protected against dephasing. But what of the stationary qubits used in the most-commonly proposed quantum registers? Ions trapped in linear ion traps (see fig 3) have already shown remarkable prospects for QIP as discussed elsewhere in this collection of articles, and have been used to demonstrate simple quantum algorithms, error correction and atomic teleportation. In the same year as the Kwiat experiment, it was shown by Wineland's group in Boulder [6] that interference of system-environment interactions can also be used to substantially enhance the lifetime of certain excited atomic states used in ion trap experiments. In these experiments, superpositions of ions were generated with varying symmetry, and their resistance to externally imposed noise studied: again the DFS superposition was shown to be remarkably stable.

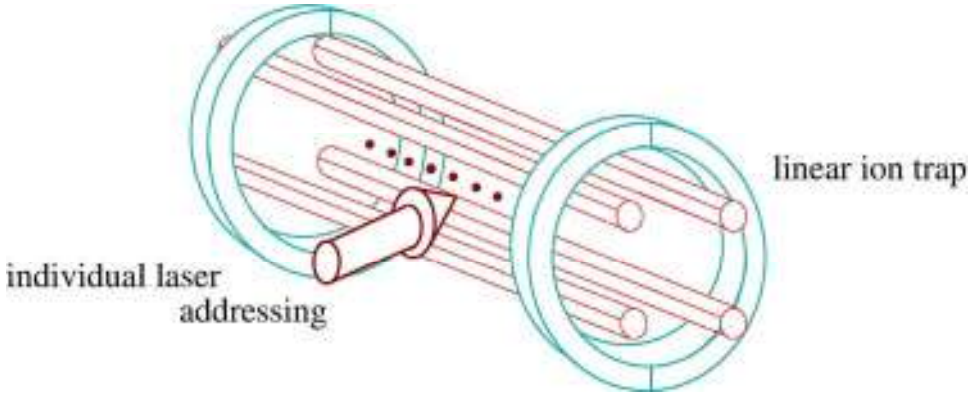


Figure 3: Cartoon sketch of a linear ion trap which single qubit laser addressing; such traps have been used to demonstrate the formation of DFS and their resilience to externally imposed noise by Kielpinski et al [6].

Since then there has been progress in other realizations of DFS, including in NMR quantum computing [7]

Future prospects

Apart from the ion-trap and photon experiments described above, there are many other possibilities to exploit decoherence-free states for quantum computing. An example that has been widely discussed in the literature is the atom-cavity system. Only very recently it has became possible to store atoms for a long time between two mirrors, such that they can interact with a standing light field. Compared to ion-traps, this has many advantages. A challenge for the future is to investigate whether DFS can be combined with quntum error correction with an accuracy that would permit fault tolerant networks to be constructed.

Conclusions

A major problem in quantum information processing is the need to retain quantum coherence while algorithms are executed. This requires exquisite precision, as many gate operations are needed to be completed before coherence is lost. Error correction is possible and coherence restored, but only if this precision is achieved. It is likely that fault tolerant computing will require the use of decoherence-free subspaces in order to make a scalable, robust quantum register.

List of terms and acronyms

DFS – decoherence-free subspace
DF – decoherence-free
NMR - Nuclear Magnetic Resonance
QED - Quantum Electrodynamics

References

[1] P Zanardi and M Rasetti, Phys Rev Lett 79, 3306 (1997)
[2] I Chuang, D Lidar, B Whaley and many others have pioneered the use of engineered states and transition dynamics to ameliorate the effects of decoherence
[3] A Beige, D Braun, B Tregenna and P L Knight, Phys Rev Lett 85, 1762 (2000)
[4] L. Viola, E. Knill, and S. Lloyd, Dynamical decoupling of open quantum systems, Phys. Rev. Lett. 82, 2417 (1999)
[5] P. G. Kwiat, A. J. Berglund, J. B. Altepeter, and A. G. White, Experimental verification of decoherence-free subspaces, Science 290, 498 (2000).
[6] C. J. Myatt, B. E. King, Q. A. Turchette, C. A. Sackett, D. Kielpinski, W. M. Itano, C. Monroe, and D. J. Wineland, Decoherence of quantum superpositions through coupling to engineered reservoirs, Nature 403, 269 (2000)
[7] L Viola et al, "Experimental Realization of Noiseless Subspaces for Quantum Information Processing", Science 293, 2059 (2001)

Projects funded by the European Commission and related to the work in this article:

QUGATES
Quantum Gates and Elementary Scalable Processors Using Deterministically Addressed Atoms
Start date: 1/1/2003
End date: 31/12/2005
Project web site: http://www.imperial.ac.uk/physics/qgates/
Contact Person: Dr D M Segal, Imperial College London, d.segal@ic.ac.uk

Projects funded by National initiatives or organizations and related to the work in this article:

UK EPSRC QIP IRC
UK Quantum Information Processing Interdisciplinary Research Collaboration
Start date: 1/4/2004
End date: 30/4/2010
Project web site: http://www.qipirc.org/
Contact Person: Prof Andrew Briggs, Department of Materials Science, University of Oxford; andrew.briggs@materials.ox.ac.uk

Contact information of the authors of this article:

Prof Peter L. Knight FRS
Blackett Laboratory
Imperial College London
Prince Consort Road
London SW7 2BW
United Kingdom
Email: p.knight@ic.ac.uk
Web page: http://www.lsr.ph.ic.ac.uk/~plk/

Dr Almut Beige
Blackett Laboratory
Imperial College London

Prince Consort Road
London SW7 2BW
United Kingdom
Email: a.beige@ic.ac.uk

Dr William J. Munro
Quantum Information Processing Group,
Hewlett-Packard Laboratories,
Filton Road,
Stoke Gifford,
Bristol, BS34 8QZ
United Kingdom
Email: bill,munro@hp.com
Web page: http://www.hpl.hp.com/research/qip/people/Bill_Munro/

Quantum information processing with atoms and ions

J. Ignacio Cirac
Ignacio Cirac is Director of the Theory Division at the Max-Planck Institute for Quantum Optics in Garching, Germany. He is also Honorary Professor in the Theoretical Quantum Optics and Quantum Information department of the Technical University of Munich. He is a member of the Spanish and Austrian Academies of Science and Fellow of the American Physical Society. He is a member of the following EU-funded IST projects: RESQ, QUPRODIS, TOPQIP, COVAQUIAL and CONQUEST. He is participating in several projects of the DFG and of Bayer (Germany). He has been awarded the Felix Kuschnitz Preiss of the Austrian Academy of Sciences and the Medal of the Spanish Royal Physical Society.

Peter Zoller
Peter Zoller is a professor at the Institute for Theoretical Physics of University of Innsbruck in Austria and Scientific Director of the Institute for Quantum Optics and Quantum Information at the Austrian Academy of Sciences. His research work is mainly in the areas of theoretical quantum optics and quantum information. He has been given the following prizes: Born Award of the Optical Society of America, Wittgenstein Award of the Austrian Science Fund, Schrödinger Award of the Austrian Academy of Sciences, Max Planck Medal of the German Physical Society. He is also a member of the Austrian Academy of Sciences. Previous positions held: Professor of Physics and JILA Fellow, JILA, University of Colorado, Boulder (US) (1990-1994). He is participating in five EU-funded projects in quantum optics and quantum information.

Abstract

We review some of the ideas that have been proposed to build quantum computers and quantum simulators using atoms interacting with laser light. We concentrate on two particular systems, namely neutral atoms loaded in optical lattices and trapped ions. We show some of the experimental achievements that have been realized so far, in particular in performing

small-scale quantum computations using trapped ions and building quantum simulators with atoms in optical lattices.

Introduction

During the last years we have witnessed an enormous progress in the control and manipulation of atomic systems. It is now possible to isolate one, two, or some few atoms in some region of space, and to keep them there for very long times. One can also manipulate the internal (electronic and spin) quantum state of the atoms using lasers, and perform individual measurements which thus reflect some of the intriguing properties of Quantum Mechanics. Furthermore, in recent years experimentalists have managed to control the interaction between several atoms, which has led to the preparation of so-called entangled states. These states are the essential ingredients of both fundamental (and even philosophical) concepts of Quantum Theory and applications related to the efficient and secure transfer and processing of information. In fact, atomic systems seem to be ideally suited for several applications in the field of Quantum Information Processing, and in particular to build quantum computers and simulators.

This article is an adaptation of [1], where we will review some of the most important concepts and experimental highlights in two particular set-ups which involve atoms. The first one deals with neutral atoms in optical lattice which are manipulated using lasers. We will show how it is possible to create entangled states and to perform quantum simulations by changing the laser parameters. This system is thus ideal to create massive atomic entanglement and to investigate problems in several fields of Science which cannot be treated even with the most powerful (classical) computers that will be developed in the foreseeable future. The second set-up deals with trapped ions (i.e. charged atoms) that are also manipulated using lasers. We will show how it is possible, at least in principle, to build an scalable quantum computer using this system, and we will also report on the first experiments in this direction. We will also discuss the experimental perspectives in both systems.

There are other quantum optical systems that have experienced a very remarkable progress during the last years, and which may be equally important in the context of quantum information. Just to mention some examples, in the context of cavity QED groups at Caltech, Georgia Tech (US), Innsbruck (Austria), and Munich (Germany) have trapped single atoms and ions inside cavities, and let them interact with the cavity field, which can be used as single (or entangled) photon(s) generators as well as to build quantum repeaters for quantum communication. Atoms have been trapped in several kinds of optical and magnetic traps, and they have been moved very precisely to different locations in space by groups in Bonn, Hannover, Heidelberg, Munich, etc. Distant ensembles of atoms have been entangled using laser fields, and the quantum state of light has been recorded in the ensembles and read out in Copenhagen.

Cold atoms in optical lattices

Optical lattices are generated by counterpropagating laser beams in 1, 2 or 3 dimensions which create a sinusoidal spatial pattern of laser intensity. The frequency of laser light is chosen such that atoms are attracted toward regions where the light intensity is large, so that the atoms feel a periodic potential. At very low temperatures, the atoms remain trapped at the bottom of those potentials and they may be transferred from one potential well to the neighbor

by a quantum mechanical effect called tunneling (they disappear from a well and suddenly appear in the other).

In order to load an optical lattice with atoms at very low temperature, one uses Bose-Einstein condensates. Those are sets of atoms which practically do not move (i.e. are at temperatures of the order of 1 nano Kelvin) , and that are also trapped by magnetic forces. By switching off the magnetic fields and, at the same time, switching on the optical lattices, the atoms go from one potential to the other adiabatically. Once they are there, they find their way in the potential wells until the laser light is kept constant and they occupy an equilibrium positions.

The physics of these atoms in the optical lattices can be understood in terms of the so-called Hubbard model. The distinguishing feature of this system is the time dependent control of the hopping matrix elements J (tunneling between neighboring sites) and onsite interaction U (potential energy) by the intensity of the lattice laser. Increasing the intensity deepens the lattice potential, and suppresses the hopping while at the same time increasing the atomic density at each lattice site and thus the onsite interaction. Increasing the intensity will, therefore, decrease the ratio the ratio of kinetic to potential energy, J/U, and the system becomes strongly interacting. In the case of bosonic atoms, the system will undergo a quantum phase transition from the superfluid state (the condensate in the optical lattice) to a Mott insulator state. In this Mott insulator regime we achieve a situation where exactly one atom is loaded per lattice site, thus providing a very large number of identifiable atoms whose internal hyperfine or spin states can serve as qubits. This Mott insulator quantum phase transition was proposed in 1998 and first realized in a remarkable experimental in Munich (Germany) in 2001. Since then, there are several groups that have observed this behavior in Mainz (Germany), NIST (US), Texas (US), and Zurich (Switzerland).

Entanglement of these atomic qubits is obtained by combing the collisional interactions with a spin-dependent optical lattice, where by an appropriate choice of atomic states and laser configurations the qubit in state |0> sees a different laser lattice potential than the atom in state |1>. This allows us to move atoms conditional to the state of the qubit. In particular, we can collide two atoms by hand, as illustrated in **Figure 1**, so that the component of the wave function with the first atom in |1> and the second atom in |0> will pick up a collisional phase which entangles the atoms. For atoms prepared in an equal superposition of the two internal states, we have again a phase gate between adjacent atoms. A Ramsey type experiment to generate and detect a Bell state via these collisional interactions has been realized recently in a seminal experiment in the Munich group.

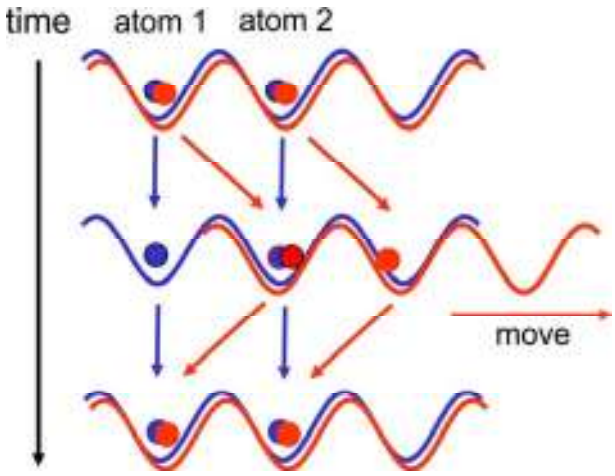


Figure 1

In a lattice loaded with many atoms a single movement will entangle in parallel all qubits. For three atoms this produces a maximally entangled GHZ-state, and for 2-dimensional lattices this allows the generation of a cluster state, which is the basic resource for universal quantum computing in Briegel and Raussendorf's one way quantum computer.

The parallelism inherent in the lattice movements makes atoms in optical lattices ideal candidates for a Feynman-type quantum simulator for bosonic, fermionic and spin many body systems, allowing simulation of various types and strengths of particle interactions, and 1,2 or 3-dimensional lattice configurations in a regime of many atoms, clearly inaccessible to any classical computer. By a stroboscopic switching of laser pulses and lattice movements combined with collisional interactions one can implement sequences of 1 and 2-qubit operations to simulate the time evolution operator of a many body system. For translationally invariant systems, there is no need to address individual lattice sites, which makes the requirements quite realistic in the light of the present experimental developments. On the other hand, as noted above, Hubbard Hamiltonians with interactions controlled by lasers can also be realized directly with cold bosonic or fermionic atoms in optical lattices. This analogue quantum simulation provides a direct way of studying properties of strongly correlated systems in cold atom labs, which in the future may develop into a novel tool of condensed matter physics.

While most of the above discussion has focused on optical lattices, new designs of arrays of microtraps e.g. based on nano-optics or magnetic microtraps will be one way to allow individual addressing of atomic qubits and entanglement operations. The ideas reviewed above about how to implement quantum gates with atoms in optical lattices can be easily extended to these systems, and we expect that in the near future will be implemented experimentally. The main advantage of these systems is that once they operate correctly, they can be relatively easily scaled-up.

For the near future, we expect that atoms in optical lattices will be used to simulate a variety of other physical systems like, for example, interacting Fermions in 2 Dimensions using different lattice geometries. We also expect an important progress towards loading single (neutral) atoms in different types of potentials (optical, magnetic, etc), and the performance of quantum gates with few of these systems. This would allow creating few atom entangled states which may be used to observe violations of Bell inequalities, or to observe interesting phenomena like teleportation or error correction. As opposed to the trapped ions, at the moment it is hard to predict if scalable quantum computation will be possible with neutral atoms in optical lattices with the present experimental set--ups. In any case, due to the high parallelism of these systems, we can clearly foresee that they will allow us to obtain a deep insight into condensed matter physics via quantum simulations.

Cold trapped ions

Right after the discovery of Shor's factoring algorithm in 1994, trapped ions interacting with laser light were identified as one of the most promising candidates to build a small-scale quantum computer. The reason is that, for many years, the technology to control and manipulate single (or few) ions had been very strongly developed in the fields of ultrahigh precision spectroscopy and atomic clocks. In particular, ions can be trapped and cooled such that they remain practically frozen in a specific region of space; their internal states can be precisely manipulated using lasers, and one can perform measurements with practically 100%

efficiency; they also interact with each other very strongly due to the Coulomb repulsion, and they can, at the same time, be decoupled from the environment very efficiently.

The ions stored and laser cooled in an electromagnetic trap can be described in terms of a set of external and internal degrees of freedom. The first ones are closely related to the center of mass motion of each ion, whereas the second ones are related to the motion of electrons within each atom, as well as to the presence of electronic and nuclear spins, and are responsible for the existence of a discrete energy level structure in each ion. Each qubit can be stored in two of those internal levels, which we will denote by |0> and |1>. These levels have to be very long-lived, such that they are not disturbed during the computation. This can be achieved, for example, by choosing them as ground hyperfine or metastable Zeeman levels, where spontaneous emission is either not present or inhibited.

To start the computation, one can prepare all the qubits in state |0> by using optical pumping techniques, in which whenever the ion is in a state different to |0> it absorbs a photon and decays into another state until it finally reaches the desired state. After the computation, one can read out the state of the ions by performing measurements based on the quantum jumps technique. The idea is to illuminate the ions with a laser light with the appropriate frequency and polarization so that if an ion is in the state |0> it does not absorb photons, whereas if it is in |1> it absorbs and emits photons. Whenever fluorescence is detected or not, this indicates that the atom has been measured in state |1> and |0>, respectively.

The computation itself requires the implementation of single- and a particular two-qubit gates. The first ones can be carried out on each atom independently by coupling their internal states |0> and |1> with a laser (or two, in Raman configuration). By adjusting the frequency and intensity of the laser, one can carry out general single-qubit gates. For the two-qubit gates, controlled interactions are always required. In the case of the trapped ions, the interaction is provided by the Coulomb repulsion. This force, however, does not depend on the internal states, and thus it is not sufficient to produce the gate by its own. The main idea introduced by us in 1995 is to use a laser to couple the internal state of the ions to the external ones, which are in turn affected by the Coulomb force, and in this way one produces the desired effect in the internal levels of the ions. Another way of interpreting the way in which this gate proceeds is by noting that the motional states are somehow shared by all the atoms (i.e., if we move an atom then the others will move as well). Thus, the laser couples the internal state of each of the ions to the common motional state and then another laser interaction couples the modes back. The fact that the laser couples the internal and external degrees of freedom of the ions is a simple consequence of the fact that each time an ion absorbs or emits a photon, not only the internal but also the motional state is changed due to the photon recoil.

The specific way in which the two--qubit gate was implemented in the original proposal required that the ions be at zero temperature and that they can be singly addressed by the laser beam without affecting the rest. In recent years, various ingenious ways of simplifying these requirements have been proposed by various groups, in particular also Mølmer and Sørensen, Milburn, and Plenio and collaborators.

The experimental verification of these ideas started in the US in 1995 with a proof of principle experiment in which a two-qubit quantum gate was realized. Since then on, several milestones have been achieved, especially in the laboratories led by David Wineland at NIST (US) and Rainer Blatt in Innsbruck (Austria). Several versions of two-qubit gates have been carried out leading to very high efficiencies, the so-called Deutsch-Jozsa algorithm with a

single ion has been implemented in Innsbruck, and even three and four particle entangled state have been prepared by performing small quantum computations in these labs. Other quantum information experiments with trapped ions have taken place in Aarhus (Denmark), Michigan (US), and Munich (Germany).

The main obstacle to scale-up the current set-ups is based on the fact that as the number of ions in the trap is increased, it becomes harder to only affect the desired ions with the laser without affecting the rest, something which spoils the computation. About three years ago, new proposals to overcome this obstacle emerged. The idea proposed by Wineland and col. is to separate the region where the ions are stored from the one in which the gates take place (see **Figure 2**). In order to perform a gate, the ion (or ions) are moved from the storage region to the gate region, something which does not disturb their internal state (since, as mentioned above, the Coulomb interaction is independent of that unless we couple them with a laser). There, they are driven by lasers to perform the gate, and then they are moved back to the storage region. The additional heating of the ions motion due to this transfer can be removed by cooling an ion of a different species which, on the one hand cools the other sympathetically and, on the other, does not disturb their internal states. Preliminary experiments demonstrating all the basic elements of this proposal have been successfully carried out at NIST. In view of these experiments, we see at present no fundamental obstacle to achieve scalable quantum computation in these systems.

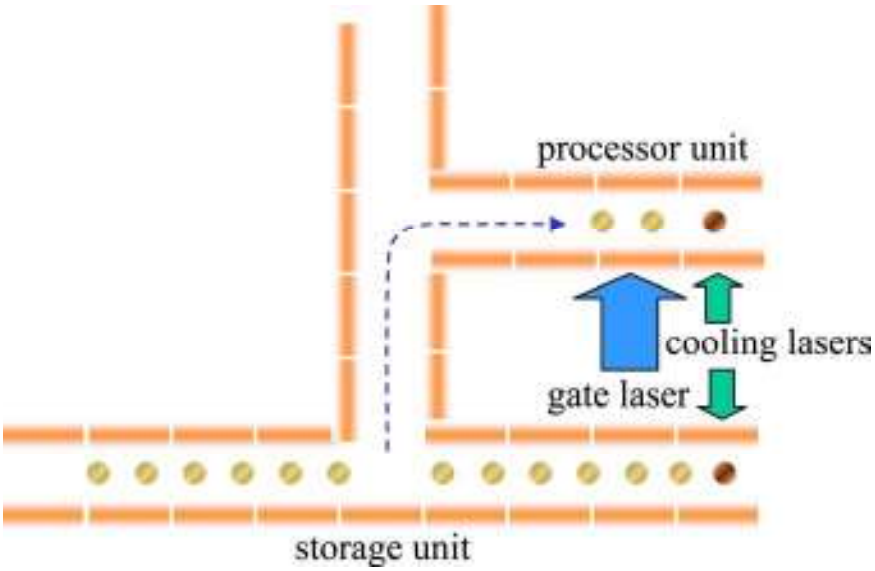


Figure 2

For the near future, we expect a very crucial experimental progress with trapped ions. Very likely, proof of principle experiments demonstrating teleportation, quantum error correction, and other intriguing properties of Quantum Mechanics will take place with 3 to 6 ions. When the technology allows reaching 30 ions (e.g. using the scalable proposals) a new avenue of experiments will open up. In that case, one could start performing computations which would compete with the most powerful classical computers that we have nowadays. Whether it will be possible to scale-up the present setups up to several hundred thousands of ions or not, something which is required to factor 200 digit numbers using Shor's algorithm and which requires fault--tolerant error correction, is still an open question. What we know by now is that there is no fundamental obstacle to achieve this goal, but it does only depend on the capability to develop the appropriate technologies. We would like to emphasize that trapped ions are the only system where this strong statement can be made nowadays.

Conclusions

During the last few years scientist have found ways of implementing quantum computations and simulations using atomic systems. Very recently there has been a great experimental progress which has allowed experimentalist to take the first steps towards building a quantum computer and quantum simulators. In this article we have illustrated this statement with two different set-ups: trapped ions and neutral atoms in optical lattices.

The physics of trapped ions is very well understood. In fact, with the recent experimental results we can foresee no fundamental obstacle to build a scalable quantum computer with this system. Of course, technical development may impose severe restrictions to the time scale in which this is achieved. On the other hand, neutral atoms in optical lattices seem to be ideal candidates to study a variety of physical phenomena by using them to simulate other physical systems. This quantum simulation may turn out to be the first real application of quantum information processing.

References

[1] J. I. Cirac and P. Zoller, Phys. Today **57**, 38 (2004)
[2] J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995)
[3] D. Kielpinksi, C. Monroe, and D. J. Wineland, Nature **417**, 709 (2002)
[4] D. Leibfried, B. DeMarco, V. Meyer, D. Lucas, M. Barrett, J. Britton, W. M. Itano, B. Jelenkovi, C. Langer, T. Rosenband, D. J. Wineland, Nature **422**, 412 (2003)
[5] F. Schmidt-Kaler, H. Häffner, M. Riebe, S. Gulde, G.P.T. Lancaster, T. Deuschle, C. Becher, C.F. Roos, J. Eschner, R. Blatt, Nature **422**, 408 (2003)
[6] D. Jaksch, C. Bruder, J.I. Cirac, C. Gardiner and P. Zoller, Phys. Rev. Lett. **81**, 3108 (1998)
[7] M. Greiner, O. Mandel, T. Esslinger, T.W. Hänsch, I. Bloch, Nature **415**, 39 (2002)
[8] D. Jaksch, H.-J. Briegel, J.I. Cirac, C. W. Gardiner, and P. Zoller, Phys. Rev. Lett. **82**, 1975 (1999)
[9] O. Mandel, M. Greiner, A. Widera, T. Rom, T.W. Hänsch, and I. Bloch, Nature **425**, 937(2003)

Projects funded by the European Commission and related to the work in this article:
RESQ
Resources for quantum information
Start date: 01/01/2003
End date: 31/12/2005
Project web site: www.ulb.ac.be/project/RESQ
Contact Person: Serge Massar, Universite Liber de Bruxelles, Belgium, smassar@ulb.ac.be

Contact information of the authors of this article:
J. Ignacio Cirac
Theory Division
Max-Planck Institute for Quantum Optics
Hans-Kopfermann Str. 1,
Garching
Germany
Email: Ignacio.Cirac@mpq.mpg.de
Web page: http://www.mpq.mpg.de/Theory.htlm

Peter Zoller
Institute for Theoretical Physics and Institute for Quantum Optics and Information
University of Innsbruck and Austrian Academy of Science
Technikerstr. 25
Innsbruck
Austria
Email: Peter.Zoller@uibk.ac.at
Web page: http://th-physik.uibk.ac.at/qo/

Quantum information processing with trapped ions

Rainer Blatt
Rainer Blatt is Professor of Physics at the Institut für Experimentalphysik, Universität Innsbruck in Austria, and Institute Director of the Institut für Quantenoptik und Quanteninformation, Österreichische Akademie der Wissenschaften, Innsbruck, Austria; His main fields of research activity are: Quantum Optics and Quantum Information, Precision Spectroscopy, especially with laser cooled trapped ions. Participation in EU projects: QUEST, CONQUEST, QGATES, SCALA, National Projects: FWF program "Control and measurement of coherent quantum systems".

Andrew Steane
Andrew Steane is Professor of Physics at the Center for Quantum Computation, Atomic and Laser Physics, University of Oxford, England and Tutorial Fellow of Exeter College. His main fields of research activity are: experimental quantum optics, especially laser cooling and trapped ions, theoretical quantum information, especially quantum error correction. Participation in EC projects: QUBITS, QUEST, CONQUEST, QGATES, SCALA; national projects: QIPIRC. Andrew Steane received the Maxwell Medal of the Institute of Physics (2000).

Abstract

Strings of atomic ions confined in an electromagnetic field configuration, so-called ion traps, serve as carriers of quantum information. With the use of lasers and optical control techniques, quantum information processing with trapped ions was demonstrated during the

last few years. The technology is inherently scalable to larger devices and appears very promising for an implementation of quantum processors.

Introduction

The use of strings of trapped ions in electromagnetic traps, so-called Paul traps, provides a very promising route towards scalable quantum information processing. There are ongoing investigations in several laboratories whose direction is towards implementing a quantum computer based on this technique. In the following, the methods will be briefly described and the state-of-the-art will be highlighted with some of the latest experimental results.

Ion trapping

Trapping configurations for ions using ac voltages are known since 1958 and are named after their inventor, Wolfgang Paul (University of Bonn, Nobel prize 1989). Paul traps are frequently used in mass spectrometry. However, only since the early 80s has it become possible to store and optically detect individual ions in Paul traps. This is due to the fact that the confined ions usually move quickly inside the trap, so that they exhibit a large Doppler effect which broadens the emitted spectrum and makes them difficult to detect spectroscopically. With the advent of the optical cooling techniques, originally proposed by Hänsch and Schawlow for free atoms and by Wineland and Dehmelt for trapped particles, then first realized by Neuhauser, Toschek and Dehmelt (Univ. Heidelberg) and Wineland (NBS Boulder, Co) with a single trapped ion, the motion of ions could be reduced such that they move only within a region smaller than the wavelength of the incident radiation. In this regime the Doppler effect essentially disappears, making precise control and detection of the ions possible. A single trapped ion can scatter light sufficiently strongly that it can even be observed with the naked eye. These experiments laid the foundation of experimenting with single atoms and their manipulation using laser light.

One of the unique features of experiments with single trapped ions is that each ion is available over and over again for repeated measurements. In the middle of the 80s single ions in Paul traps allowed the observation for the first time of the long-postulated phenomenon of *quantum jumps*. In such an experiment, one exploits the fact that during the scattering of fluorescent photons the ion must jump back and forth between a pair of its electronic states. If during this process the ion gets excited to a different (third) electronic state it is no longer available to generate fluorescence and thus it ceases to radiate. Thus as the ion moves to and from the third state, sometimes called a ‘shelf’ state, the relatively strong fluorescence disappears and reappears again. These characteristic jumps in the observed fluorescence indicate the fundamental quantum process of a single quantum system, here the ion, being forced by observation to choose between possible states. Furthermore, the quantum state it chooses is indicated by the detected fluorescence with close to 100% reliability. This technique, known as the *electron shelving* or the *quantum jump* method results from experimenting with a single particle and provides an important asset for the realization of a quantum information processor. It provides a fast and very reliable way to measure the quantum bits: this is both crucial for reading out the final result of a computation, and also very useful for correcting errors as the computation proceeds.

Quantum information processing

Qubits are implemented using two energy levels of a single trapped ion. Quantum registers need rows of such ions which are interacting in a controlled way. This can be realized using so-called linear Paul traps (see **Figure 1**). Such a trap device is derived from the Paul mass filter which employs four hyperbolic electrodes and rf-voltages to transmit an ion beam in a mass selective way. For a trap, the basic structure is an arrangement of four rods (rf-voltages) and two ring electrodes (dc-voltages) for axial confinement, but many variations on this structure are possible, including for example flat electrodes constructed on the surface of a substrate by microfabrication techniques. Ions are confined along the longitudinal axis in the centre of the four rods. Under the action of laser cooling, the ions form a string as shown in **Figure 2**. The distance between neighbouring ions slightly varies along the string because the ions all lie in a parabolic well and also repel one another. The result is that the repulsive forces from the outer ions squeeze the inner ones closer together. Such an ion string provides a register with the quantum information stored in the electronic states of the individual ions.

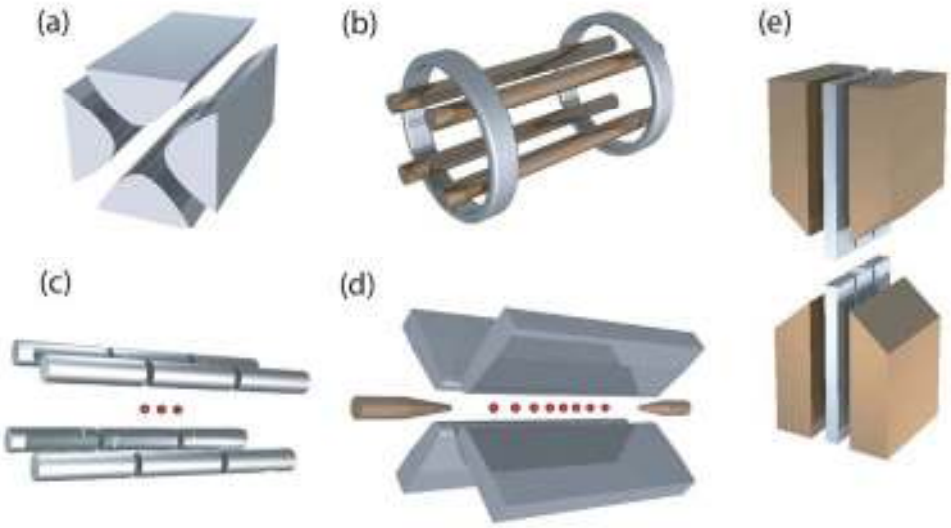


Figure 1

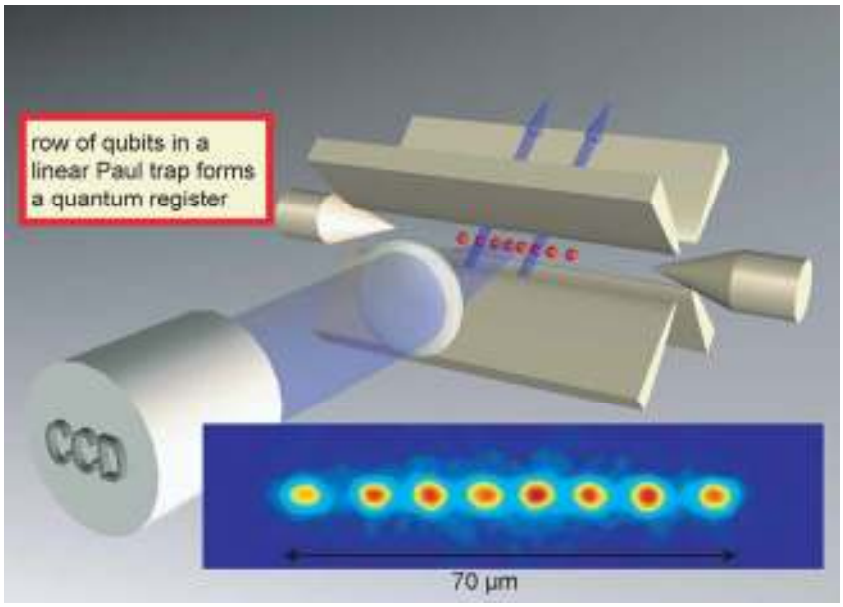


Figure 2

The distance between neighbouring ions can be adjusted by means of the dc voltages. Each ion can be manipulated individually with a focussed laser beam, i.e. single-qubit operations are possible. In addition to single qubit operations, CNOT-gate operations between any two qubits are necessary to build a universal quantum computer. Ignacio Cirac and Peter Zoller (Univ. Innsbruck) proposed a procedure for this in 1995. The important idea was that the ion *motion* provides an additional degree of freedom which can be used to carry and convey information. It is significant that the strong repulsive Coulomb forces imply that the ions are interacting, and indeed they tend to move as a single body. Using methods first developed for laser cooling, Cirac and Zoller showed how to link the internal electronic state of any given ion, i.e. any qubit in the register, to the quantum state of motion of the whole string of ions. The Cirac-Zoller proposal is, in short, to use a sequence of such links to achieve a state change of a target qubit conditional to the state of a controlling qubit.

For this purpose, they suggest that one starts with the quantum register at complete rest, i.e. initially the motion of the string of ions needs to be completely frozen, or in quantum mechanical terms, it is considered to be in the ground state of the corresponding harmonic oscillator. With a laser pulse directed to the controlling qubit, the internal excited state information of that particular qubit (which could be any ion of the quantum register, depending on the algorithm in question) is then mapped onto the centre-of-mass motion, i.e. in case there was a (non-zero) excited state amplitude, that is now written into an excited state amplitude of the motion, whereas the controlling ion's internal state is put in its ground state. Due to the Coulomb interaction this quantum of centre-of-mass motion describes the movement of the entire ion string and is, of course, shared by all ions. Thus, the new quantum state of the register is an entangled state of the internal (electronic) and the external (vibronic or motional) states. With a laser directed subsequently to any other ion (serving as the target ion, depending on the algorithm) it is then possible to manipulate the internal state of that target ion if and only if there is motion in the ion string. Finally, taking the motion out of the string by undoing the first step to the controlling ion, and thus restoring the controlling qubit, makes it possible to realize the truth table of the CNOT-gate operation completely and coherently.

This 1995 proposal launched the interest in ion trap quantum computing, because all the essential ingredients of a computer were shown to be available using experimental techniques which were already either realised or very close to realisation in the laboratory. We will discuss below the subsequent experimental implementations of this and related ideas.

As a carrier for the quantum information, long-lived atomic states are required. Since 1995 a variety of ions has been investigated as candidates for quantum information processing. The qubits can be encoded either by using narrow optical transitions (so-called ‘forbidden’ transitions), or by using radio-frequency transitions between levels split by an applied magnetic field (Zeeman effect) or by the internal hyperfine interaction of the ion. The latter is most promising because it is highly stable, it is used for example in atomic clocks. While the actual technical implementation varies strongly depending on the ions used, the Cirac-Zoller concept can be realized in any type of configuration. Three teams have up till now realised a controlled quantum gate such as CNOT between trapped ions: the Boulder group (D. Wineland et al. at NIST, Boulder, Co., USA), the Innsbruck group (R. Blatt et al. at Univ. Innsbruck, Austria) and the Oxford group (A. Steane and D. Lucas et al. at University of Oxford, England). The Michigan group (C. Monroe et al at University of Michigan, USA) have demonstrated entanglement of an ion and an emitted photon.

During the last few years, in particular the experiments of the Boulder and Innsbruck groups have proved the feasibility of quantum information processing using different approaches. While the Innsbruck experiments follow closely the original Cirac-Zoller proposal and use optical transitions with individual addressing in Ca^+ ions, the Boulder experiments use Be^+ ions where the qubits are encoded in hyperfine states and coherent manipulation is achieved by using further gate proposals implemented by Raman-transitions. In the Boulder experiments individual addressing is achieved by separating off ions from the string using control voltages. Although quite different experimentally, both experiments have implemented quantum information processing quite successfully and very similar conceptually. Below, we will present some examples based on the Innsbruck Ca^+ experiment, however, the Boulder results are very similar and at this time it is by no means obvious which element will actually be best suited for a scaled implementation using trapped ions. **Figure 2** shows the Ca^+ setup schematically and a string of ions representing a quantum register.

Fundamental 2-ion logic gate

A universal quantum information processor requires the implementation of a CNOT-gate operation, i.e. a conditional operation between any two qubits of a quantum register. Following closely the proposal by Cirac and Zoller, two ions were loaded where the first one serves as the control qubit and the second one represents the target qubit. With a laser pulse directed towards ion 1, its excited state amplitude was written to the motion using a sideband pulse, i.e. a laser pulse exciting the internal and the external degrees of freedom of the controlling qubit. Then a series of pulses was applied to the target ion in such a way that the amplitude of the wave function is changed if and only if there was any motion in the two-ion string. Finally, a laser pulse applied to the controlling ion again remaps the motional state to the excited state of the first ion and the string is at rest as it was before the entire operation started. **Figure 3** shows the schematically the sequence of laser pulses and the realized truthtable of the operation.

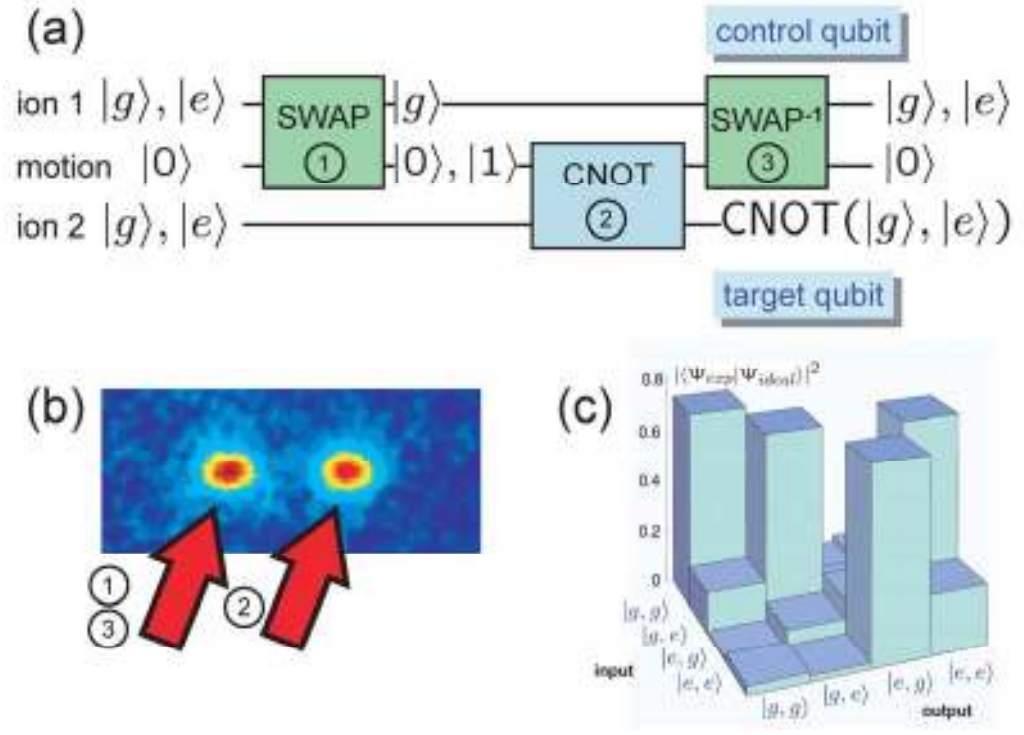


Figure 3

In the experiments in Boulder, a laser pulse illuminated two ions together, in such a way that they experienced an oscillating force which depended on their internal qubit states. The ions experienced a driven oscillation which returned them to their initial motional state after an integer number of periods, while causing the joint qubit state to undergo a net rotation which is equivalent to the CNOT gate.

Algorithms with trapped ions

The simplest quantum algorithms can be demonstrated using just two qubits.

Consider the following, quite classical, problem: Throwing coins usually is a fair game since on the average the outcome has a 50% probability showing either side. On the other hand, if someone tries to cheat and uses a (fake) coin with two equal sides, such bets become extremely unfair. Therefore, prior to betting a measurement is in order to ensure fair play. However, answering the question whether a coin is fair (head on one side, tail on the other) or fake (heads or tails on both sides) requires two examinations, i.e. a look on each side. In a quantum world this is not the case due to the fact that superpositions are completely acceptable. Therefore, if a coin were represented in a quantum way (say a "quantum coin"), the information concerning whether both sides are equal or different is clearly available in the quantum description. Accordingly, an appropriately taken quantum measurement on such a quantum coin would certainly be able to tell the difference since it could check for the superposition in question. Therefore, using a quantum processor and an appropriately written algorithm allows one to obtain the required information (fair or fake) in a *single* step. The associated quantum program is known as the Deutsch-Josza algorithm and it requires for a coin a two-valued function. A quantum advantage is truly present here, because one may imagine a case where evaluating the function is a long and complicated process: the quantum computer only needs to run the evaluating logic once, not twice as would be required by traditional computing methods. For a minimal demonstration, two qubits are needed. Clearly, an implementation of such a rudimentary example does not solve an advanced problem. However, it is able to demonstrate quantum information processing and its advantages compared to classical computing.

The two quantum bits can be provided with a single ion. This is because even with a single ion the internal electronic state can be used to carry one qubit and the external (centre-of-mass) motion is able to carry another qubit.

This quantum algorithm was demonstrated by the Innsbruck group using the internal and external (motional) excitations as qubits. The entire procedure requires several manipulations which are realized with a sequence of laser pulses. The outcome of the procedure is either "0" (encoded in the excited state population of the ion) if the "quantum coin" was false (i.e. two equal sides) or it is "1" if the quantum coin was fair (i.e. two different sides of the coin). The procedure was completely general and proves that quantum information processing is faster, i.e. it requires less steps, than classical computing. The reason for this is of course, that in quantum mechanics a superposition is available whereas classically only two discrete states are available.

Quantum state computation

While the use of superposition states already demonstrates some of the computational power of quantum information processing, for example with the Deutsch-Jozsa algorithm, the

ultimate potential of quantum state manipulation becomes visible only by including non-local operations. Superpositions of quantum systems at different positions are outside the realm of classical experience and therefore such 'entangled' states really demonstrate the quantum nature of information processing systems. Non-local operations can be realized in a computational way by making use of the Cirac-Zoller CNOT-gate operation. Consider for example the result of such a computation step if the controlling ion carries a superposition as an input, clearly an operation which cannot be done classically. Producing such states makes it impossible to describe the state in terms of individual independent particles at different locations. In fact, from a mathematical viewpoint it becomes impossible to consider the particles as independent: they are 'inextricably interwoven' and the quantum state of the system is highly non-local, in that it cannot be described as a sum or product of its parts.

Such states are also called EPR states (after Einstein, Podolski and Rosen, who first envisioned such nonlocal quantum states in 1935) and are nowadays usually called Bell states (after John Bell who used them to distinguish between the quantum and classical world). Such states are of a peculiar nature and they cannot be produced by any classical means: they require non-local quantum operations. With an ion trap quantum information processor, however, such Bell states can simply be created at the push of a button. Moreover, these states are then available as a resource for further quantum information processing, unlike the correlated pairs of photons or decaying particles, where such states are only probabilistically available and are usually destroyed when detected.

Adding another ion to the quantum register allows us to process quantum information with three qubits. Aside from the larger computational space this makes it possible for the first time to investigate entanglement for three particles at the push of a button. Tri-partite entangled states have become important for experiments exploring the fundamentals of quantum mechanics, for quantum communication purposes and they provide the first step towards studying multi-particle entanglement.

The maximally entangled state $|\Psi\rangle=1/\sqrt{2}(|ggg\rangle+|eee\rangle$ (i.e. in a measurement one observes either all ions in state $|g\rangle$ or in state $|e\rangle$ and no other combinations) is known as the Greenberger-Horne-Zeilinger (GHZ) state. Its importance is due to the fact that entangling more than two particles leads to a conflict with local realism for non-statistical predictions of quantum mechanics. This is in contrast to experiments with two entangled particles testing Bell's inequalities, which observe conflicts only with statistical predictions. With the three-qubit quantum processor it is now possible for the first time to actually “quantum compute” these states at the push of a button and to investigate, for example, their decoherence and their dynamical behaviour under the influence of a measurement.

Teleportation

In addition to “computing states”, with the availability of even a small quantum information processor, a variety of quantum protocols can now be run and tested. One of the most important and most striking way to convey quantum information is the teleportation protocol by Bennett et al.. Teleportation is concerned with the complete transfer of information from one particle to another.

Specifying a quantum state completely generally requires an infinite amount of information, even for qubits. Moreover, measuring a system would immediately alter its state, therefore transferring quantum information is hard. However, as shown by Bennett et al., entanglement

can be used together with classical communication to achieve the complete transfer of quantum information, a process coined teleportation. Teleportation using pairs of photons has been demonstrated, however, the techniques employed are probabilistic and they require post-selection of measured photons. That is, the success of the protocol is rare, perhaps once in 10000 attempts, and these good events are only identified after the fact. In contrast, a fully controlled process such as is possible in trapped ions can succeed on most attempts.

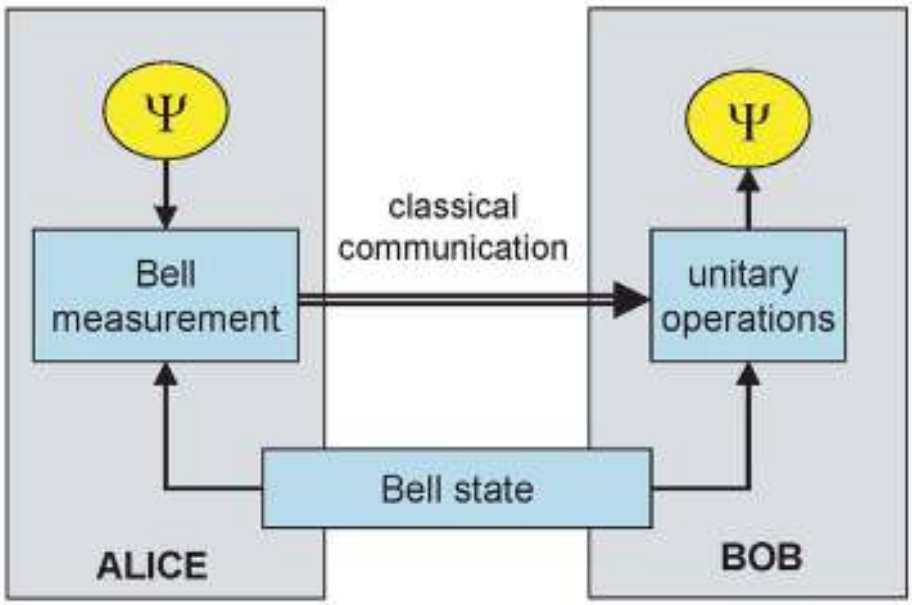


Figure 4

The teleportation protocol works as follows (see **Figure 4**): In order to transfer the quantum information Alice and Bob establish two channels, a classical channel and a quantum channel. On the latter they share a Bell state as a resource required for the protocol. Sender Alice manipulates the unknown input two-qubit state $|\Psi\rangle$ coherently by a CNOT-gate operation and a single qubit rotation. Then Alice measures the respective states of the ions and gets as a result the information on which Bell state she now has. Clearly, during this measurement the quantum information at Alice's location (and thus the original state $|\Psi\rangle$) is destroyed. The outcome of Alice's measurement is then classically communicated to Bob who subsequently manipulates (using laser pulses) his part of the originally shared Bell state depending on the measured result. In this way, Bob exactly retrieves the initially given state $|\Psi\rangle$ and teleportation is achieved.

Such fully controlled or deterministic teleportation was achieved for the first time in 2004 by the teams at Innsbruck and, independently, Boulder.

Teleportation is highly significant, not only as a communication protocol, but also because it is a central ingredient of fault-tolerant methods. These are required to implement operations and corrections within the registers of a quantum computer, when the computer is stabilised by quantum error correction.

Scalability and error correction

One of the major advantages of the ion trap quantum computer is its scalability. This is achieved, for example, by simply adding another ion to the string confined in the trap. Loading an additional ion to the register does not change the basic frequency of the vibrating string, the lowest frequency of its common motion is always the same. Thus, by adding ions to the register the Cirac-Zoller approach works in exactly the same way as with fewer ions. The drawback, however, is that by adding ions the entire register becomes "heavier", and therefore influencing the ion motion becomes slower, and of course, putting everything into the ground state to begin with becomes more and more difficult. But, more importantly, all entangling excitations become slower since they include the excitation or de-excitation of a vibrational quantum. Eventually, with very many ions such a system becomes sluggish and hard to handle. It will become technically very difficult to operate. Therefore, this may actually limit direct scaling to tens of ions in a single string.

Consequently, it would be much better to keep single or few ions stored in individual sites and then try to interconnect between them. In this way the ions are well confined, isolated from each other and can be individually controlled and accessed. Quantum information processing then requires a quantum channel to convey the quantum information between the different sites. One way to achieve this, is to write the static information contained in the atomic qubits to a photon which then could be transmitted via an optical fibre and finally coupled again to another ion. For this, a full transmission protocol (photonic channel) was proposed by Cirac, Zoller, Kimble and Mabuchi and a corresponding experiment is currently under way in Innsbruck. For this, the single ions are trapped inside an arrangement of two opposing mirrors called an optical cavity which forces the atom to emit or absorb into the cavity axis. With appropriate reflection and transmission properties of the mirrors and an optimized timing, quantum information can be reliably transferred. Although the linking protocol and the physics of the interface provide a beautiful method, the cavity technology requires advanced hardware and thus poses severe experimental problems.

For this reason and in order to build up a larger-scale quantum processor, the Boulder group proposed a "quantum-charged-coupled-device" (QCCD or "ion-chip") which consists of many interconnected segmented ion traps. The idea is to shuttle ions between different locations to carry the quantum information. This would allow communication between sets of ions. In such a structure one could distinguish between a loading area, a cooling and logic region. It is conceivable that shuttling the ions back and forth between different areas of such a segmented trap structure would allow one to interconnect different groups of ions serving as memory and the auxiliary ions which would be required to implement error corrections.. Currently, several groups are pursuing this approach with the goal to build and operate a small ion chip. With this technique, in fact, scaling the ion-trap quantum information processor seems feasible after all.

A major ingredient for further scaling of any quantum information processor is the implementation of error correction. Whereas in classical information processing error correction is very well known and implemented, it was not clear for some time whether error correction would actually work with quantum processes. The reason for this is simply that quantum information cannot be copied like classical information and therefore, classical error correction protocols which usually rely on redundant encoding do not work Fortunately and surprisingly, it is known now for several years that with the use of entangling operations, quantum error correction protocols can actually work and first experiments towards their

implementation have already been carried with NMR-based systems and very recently even with trapped ions by the Boulder group.

For a reliable operation of extended quantum information processing it will be indispensable to implement error correction protocols routinely. It appears that the information of a single two-level system needs to be encoded into five or even seven physical qubits and a certain number of quantum gate operations and measurements will be necessary to keep that information stored and "alive" as a logical qubit. Scaling a quantum information processor will then require the coupling of logical qubits and subsequently gate operations between them.

Conclusions

While quantum information processors with trapped ions seems bulky and often balky at present, they offer a viable route towards larger devices. An outline of a design for an ion chip computer allowing a billion operations on 300 logical qubits has been set out by one of us. This is not feasible yet but such a document acts as a guide to the next stage of development. In the nearer term, ion traps will provide us with the playground on which we can try out and invent more algorithms, better quantum processing and even do new physics. Using quantum coherences and their possibly uninterrupted, protected or corrected, dynamical evolution will lead to new schemes for precision measurements and offer new ways of bringing the quantum world to a larger scale.

References

[1] J. I. Cirac and P. Zoller. *Quantum computations with cold trapped ions.* Phys. Rev. Lett. **74**, 4091 (1995)

[2] A. Steane, *The ion trap quantum information processor*. Appl. Phys. **B 64**, 623 (1997)

[3] D. Leibfried, R. Blatt, C. Monroe, D. Wineland, *Quantum dynamics of single trapped ions*. Rev. Mod. Phys. **75**, 281 (2003)

[4] F. Schmidt-Kaler, H. Häffner, M. Riebe, S. Gulde, G.P.T. Lancaster, T. Deuschle, C. Becher, C.F. Roos, J. Eschner, R. Blatt, *Realization of the Cirac-Zoller controlled-NOT quantum gate*. Nature **422**, 408 (2003)

[5] D. Leibfried, B. Demarco, V. Meyer, D. Lucas, M. Barrett, J. Britton, W. M. Itano, B. Jelenkovic, C. Langer, T. Rosenband, and D. J. Wineland, *Experimental demonstration of a robust, high-fidelity geometric two ion-qubit phase gate*. Nature 422, 412 (2003)

[6] M. Riebe, H. Häffner, C. F. roos, W. Hänsel, J. Benhelm, G.P.T. Lancaster, T. W. Körber, C. Becher, F. Schmidt-Kaler, D.F.V. James, and R. Blatt, *Deterministic quantum teleportation with atoms.* Nature **429**, 734 (2004)

[7] M. D. Barrett, J. Chiaverini, T. Schaetz, J. Britton, W. M. Itano, J. D. Jost, E. Knill, C. Langer, D. Leibfried, R. Ozeri, and D.J. Wineland, *Deterministic quantum teleportation of atomic qubits*. Nature **429**, 737 (2004)

[8] A. Steane, *How to build a 300 bit, 1 Gop quantum computer.* arXiv:quant-ph/0412165

Projects funded by the European Commission and related to the work in this article:

QUEST
Quantum entangled states of trapped particles
Start date: 01/05/2000
End date: 31/04/2004

Project web site: http://www.iota.u-psud.fr/~quest/index.html
Contact Person: Philippe Grangier, IOTA, Orsay, France, philippe.grangier@iota.u-psud.fr

CONQUEST
Controlled quantum coherence and entanglement in sets of trapped particles
Start date: 01/03/2004
End date: 28/02/2008
Project web site: http://www.quniverse.sk/conquest/
Contact Person: Vladimir Buzek, Bratislava, Slovakia, buzek@savba.sk

QGATES
Quantum Gates and Elementary Scalable Processors Using Deterministically Addressed Atoms
Start date: 01/01/2003
End date: 31/12/2005
Project web site: http://www.ph.imperial.ac.uk/qgates/
Contact person: Peter Knight, Imperial College of Science, technology and Medecine, p.knight@ic.ac.uk

QUBITS
Quantum Based Information Processing and Transfer with Single Atoms and Photons
Start date: 01/01/2000
End date: 31/12/2002
Project web site: http://www.imperial.ac.uk/physics/qubits/
Contact Person: Peter Knight, Imperial College, London, UK, p.knight@ic.ac.uk

SCALA : FP6 project under negotiation
Scalable Quantum computing with Light and Atoms
Contact person: Philippe Grangier, CNRS, philippe.grangier@iota.u.psud.fr

Projects funded by National initiatives or organizations and related to the work in this article:

Austria: FWF program “Control and measurement of coherent quantum systems”
UK: QIPIRC

Contact information of the authors of this article:
Rainer Blatt
Institut für Experimentalphysik, Universität Innsbruck, Technikerstrasse 25, and
Institut für Quantenoptik und Quanteninformation, Österreichische Akademie der Wissenschaften (Austrian Academy of Sciences),
Otto-Hittmair Platz 1
A-6020 Innsbruck
Austria
Email: Rainer.Blatt@uibk.ac.at
Web page: http://heart-c704@uibk.ac.at

Andrew Steane
Center for Quantum Computation, Atomic and Laser Physics,
University of Oxford
Clarendon Laboratory
Parks Road
Oxford OX1 3PU
England
Email: a.steane1@physics.ox.ac.uk
Web page: http://eve.physics.ox.ac.uk/Personal/steane/AMS.html

Cavity quantum electrodynamics

Jean-Michel Raimond
Jean-Michel Raimond is professor of physics at Université Pierre et Marie Curie and member of Laboratoire Kastler Brossel, Département de Physique de l'Ecole Normale Supérieure in Paris, France. He is also senior member of Institut Universitaire de France, Chaire d'Optique Quantique. His research is in the area of experimental Quantum Optics, including Cavity Quantum Electrodynamics, Quantum Information Processing and Cold Trapped Atoms. He is a member of the following EU-funded IST projects: QUBITS, QGATES, QUEST, CONQUEST

Gerhard Rempe
Gerhard Rempe is working at the Max-Planck Institute for Quantum Optics in Garching, Germany. He is also Scientific Member and Director of the Max-Planck Society and professor at the University of Technology in Munich. He is doing research in experimental Quantum Optics including Atom Optics, Bose-Einstein Condensation, Cavity Quantum Electrodynamics, Quantum Information Processing, and Slow Molecules. He is a member of the following EU-funded IST projects: QUBITS, QGATES, QUEST, CONQUEST.

Abstract

The simplest model in quantum optics deals with a single two-level atom interacting with a single mode of the radiation field. This ideal situation is implemented in Cavity Quantum Electrodynamics experiments, using high quality microwave or optical cavities as photon boxes. It provides a test bench for fundamental quantum processes and a promising ground for quantum information processing.

Introduction

Most experiments dealing with matter-light interaction involve a large number of atoms interacting with laser fields made up of a large number of photons. The simplest situation,

however, involves a single atom interacting with one or a few photons. Achieving this situation is the aim of Cavity Quantum Electrodynamics (CQED) [1, 2].

The history of CQED started, more than 50 years ago, with a seminal remark by Purcell. The radiation properties of an atom can be changed by controlling the boundary conditions of the electromagnetic field with mirrors or cavities. CQED experiments initially measured modifications of spontaneous emission rates or spatial patterns in low-quality cavities. They evolved to higher and higher atom-cavity couplings and photon storage times. Most of them are now in the so-called regime of 'strong coupling', in which the coherent interaction of a single atom with one photon stored in a very-high-quality cavity, a modern equivalent of Einstein's photon box, overwhelms the incoherent dissipative processes.

CQED experiments implement a situation so simple that their results can be cast in terms of the fundamental postulates of quantum theory. They are thus appropriate for tests of basic quantum properties: quantum superposition, complementarity or entanglement. In the context of quantum information processing, the atom and the cavity are long-lived qubits, and their mutual interaction provides a controllable entanglement mechanism – an essential requirement for quantum computing or teleportation applications. CQED is therefore a fertile ground for quantum information processing. In addition, the ability to manipulate mesoscopic fields, containing a few to a few tens of photons, made it possible to explore the fuzzy boundary between the quantum and the classical worlds, unveiling the decoherence mechanisms that confine the quantum weirdness at a microscopic scale.

CQED comes in two flavours: microwave and optical. Both situations achieve the strong-coupling regime, with different and complementary features. In the microwave domain, very excited 'Rydberg' states interact with superconducting millimetre-wave cavities. Dissipation is very low, and the pace of the atom-field entanglement process is slow. An exquisite degree of control is reached, making it possible to tailor complex multi-qubit entangled states. In Europe, this line of research is mainly pursued by H. Walther in Munich, and S. Haroche with one of us (JMR) in Paris. In the optical domain, low-lying atomic levels interact with room-temperature optical cavities. The interaction is much faster, as is the dissipation. This, however, turns out to be an asset: optical photons can be efficiently coupled in or out of the cavity. Optical CQED thus provides a natural and essential interface between flying photonic qubits for the transmission of quantum information and stationary atomic qubits for the storage of quantum information. In Europe, this regime of CQED is studied by one of us (GR), while other groups are setting up new experiments.

This paper gives a short introduction into CQED. It highlights some recent achievements and discusses perspectives for quantum information processing opened up by the first experiments. More details and references can be found in [2 - 4].

Microwave Cavity Quantum Electrodynamics

In order to reach the strong coupling regime, a CQED experiment must combine large atom-field couplings with long atomic and field lifetimes. The longest photon storage times, in the 1 ms to 1 s range, are obtained in the millimetre-wave domain (few tens of GHz), with photon boxes made up of superconducting materials cooled down to cryogenic temperatures. They have sizes comparable to the wavelength and provide a high field confinement, essential to increase the atom-field coupling. Rydberg atoms, in which an alkali's valence electron is promoted to a level with a large principal quantum number N, are strongly coupled to

microwaves. In particular, circular levels, realizing Bohr's orbit, have an extremely long lifetime (30 ms for $N = 50$). They can be detected in a selective and sensitive way by field ionization. They are ideal tools for cavity field manipulations.

Figure 1 presents the scheme of a CQED experiment with circular Rydberg atoms [5]. Laser and microwave excitation of an atomic beam, effusing from oven *O,* prepares in box *B* one of the states *e* or *g* (*N*=51 or *N*=50). Before entering *B*, the atoms are velocity-selected by laser techniques. The state preparation being pulsed and performed at a precise location, the position of an atom at any time during its transit through the apparatus is well determined. This is essential to ensure single qubit addressing. The atoms, very sensitive to microwave fields, are in a cryogenic environment, cooled below 1 K and shielded from the room temperature blackbody background. They interact with the superconducting cavity *C*, nearly resonant with the transition between *e* and *g* at 51 GHz. A static electric field applied across the cavity mirrors tunes the atomic transition in or out of resonance with *C*, via Stark effect. The atoms are finally detected in the field-ionization counter *D*, whose efficiency reaches 90%, providing a nearly ideal qubit read-out.

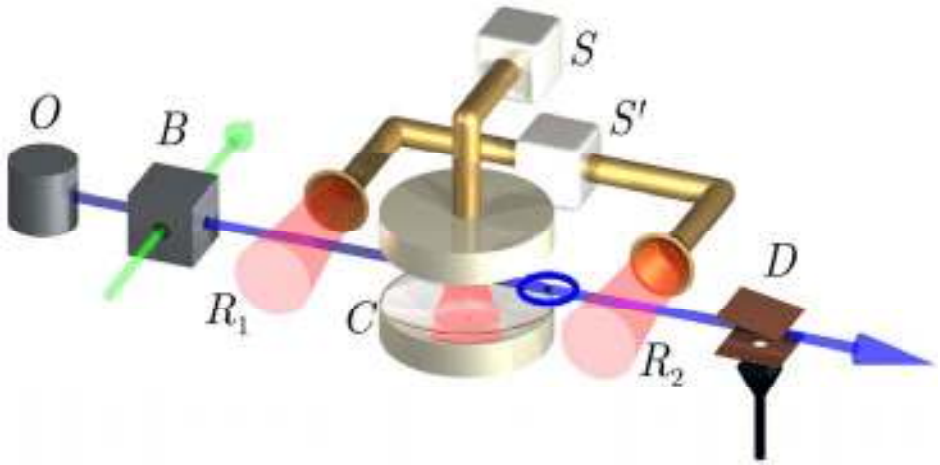


Figure 1 A classical source *S*, coupled to *C*, can be used to fill the cavity with a mesoscopic quasi-classical field. Another source *S'* feeds two interaction zones R_1 and R_2 sandwiching *C*. The resonant interaction of the atom with the classical field in these zones realizes single-qubit gates. The atom can thus be prepared in any state before entering *C*. The gate realized in R_2 before the final detection in the {*e*, *g*} basis by *D*, makes it possible to analyse completely the final atomic state.

Most quantum entanglement manipulations realized so far rely on the resonant atom-cavity interaction. The simplest situation is an atom entering the empty resonant cavity in the upper state, *e*. The initial quantum state *e*,0 is degenerate with *g*,1 representing an atom in the lower state with one photon in the cavity. The atom-field dipole interaction couples these states and the atom-cavity system thus oscillates between them in a `vacuum Rabi oscillation'. Note that no evolution takes place when the initial state is *g*,0 (atom in the ground state and empty cavity) since there is no excitation to exchange.

Figure 2 presents an experimental vacuum Rabi oscillation. The probability P_e for detecting the atom in *e* is plotted as a function of the atom-cavity interaction time, t_i. The observation of four 20 μs periods shows that the coherent atom-cavity interaction dominates dissipative processes, fulfilling the strong coupling condition. This oscillation is a reversible spontaneous emission process. The atom in *e* emits a photon. When the emission occurs in free space, the photon escapes at light velocity and is lost. Ordinary spontaneous emission is irreversible.

Here, the emitted photon remains trapped in *C*, ready to be absorbed again by the atom. In the strong coupling regime, spontaneous emission is a reversible process!

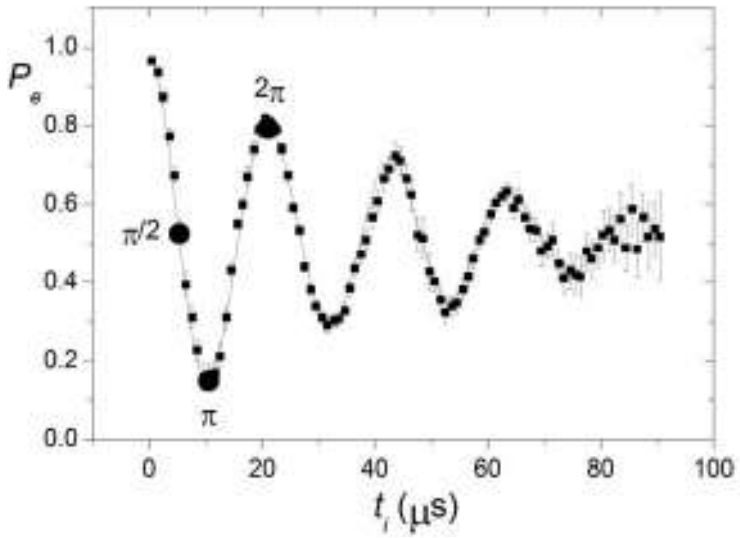


Figure 2

Oscillatory spontaneous emission is at the heart of an interesting quantum device, studied in the Munich group: the micromaser (see the Chapter by Raithel *et al.* in [1]). A stream of Rydberg atom crosses the cavity. Cumulative emissions build up a mesoscopic field. The cavity damping time is so long that the maser action is sustained even though the average time interval between atoms is much greater than their transit time through *C*. The micromaser operates with much less than a single excited atom at a time, a remarkable regime in which quantum effects are of paramount importance.

The vacuum Rabi oscillation provides elementary stitches to knit complex entangled states. Three atom-cavity interaction times are particularly interesting. They are depicted by black circles in **Figure 2**. At a quarter of a period, atom and cavity are in a coherent superposition of *e*,0 and *g*,1 with equal weights. This is an entangled state, similar to the one of the spin pair used to discuss the EPR (Einstein-Podolski-Rosen) situation, illustrating quantum non-locality. The atom-cavity entanglement lives as long as the photon in the cavity, about a millisecond. This time is much longer than the mere 5 μs required for its creation, allowing for complex sequences.

Half a period corresponds to an atom-cavity state exchange. An atom entering the empty cavity in a superposition of its energy states always ends up in *g*, leaving in *C* a coherent superposition of the zero- and one-photon states. In quantum information terms, the qubit carried by the atom is copied onto the cavity. The process is reversible. An atom entering C in the lower level *g* for a half-period interaction takes away the cavity state. This operation does not create entanglement, but is essential since the cavity field is not directly accessible here, in contrast with optical CQED situations.

Finally, a full Rabi oscillation period drives the atom-cavity system back to its initial state, albeit with a state sign change. The same phase shift occurs when the initial state is *g*,1, the atom transiently absorbing the photon and releasing it. Note again that *g*,0 remains invariant. The state sign change is thus conditioned to the state of the atom and of the cavity. It is a conditional coherent quantum dynamics, i.e. a quantum gate.

Combining these transformations, the ENS group has realized complex quantum information processing sequences [5]. In a quantum memory experiment, the state of a first atom is copied onto *C*, stored for a while, and later taken away by a second atom. An EPR atomic pair is created by entangling a first atom with *C* (quarter of a period interaction). The cavity state and, hence, its entanglement with the first atom is then copied onto a second atom. Quantum correlations between the atomic states assess the coherence of the process.

The most complex sequence realized so far is the creation of a three-qubit entangled state. The cavity is entangled with a first atom, as above. A second atom then comes in and realizes a quantum gate operation based on the full Rabi period. It gets entangled with *C* and, hence, with the first atom, completing the three-qubit entanglement. Quantum correlations between these qubits are then measured. A third atom is involved to read out the field state. Altogether, the production and analysis of this entanglement involves four qubits, three one-qubit gates and three two-qubit ones. It is among the most complex sequences realized with individually addressed qubits.

The entanglement fidelity is, above, mainly limited by cavity damping. Another type of quantum gate gets rid of this limitation. Two atoms, one in *e* and one in *g*, interact simultaneously with the non-resonant cavity. The first virtually emits a photon in *C*, immediately absorbed by the other. This cavity-induced coherent collision creates entanglement and provides gate dynamics. Since the photon is only virtually present, the process is not affected by cavity losses. It is very promising for quantum information processing with moderate quality cavities.

Another remarkable feature of these experiments is the ability to manipulate in *C* mesoscopic fields, made up of a few to a few tens of photons. Their interaction with a single atom is strong enough to put them in a mesoscopic quantum states superposition, for instance a superposition of two fields with different classical phases. These non-classical states bear a strong analogy with the famous Schrödinger cat, suspended between life and death in quantum limbs. The slow relaxation of the cavity makes it possible to study in 'real time' the decoherence mechanism [5] transforming the quantum superposition into a probabilistic alternative, the transition being faster and faster when the cat's size increases. These decoherence studies are important for fundamental quantum mechanics issues but also because decoherence is a serious obstacle on the road towards practical quantum computation.

Optical Cavity Quantum Electrodynamics

All CQED experiments can be described by three physically distinct time scales. One is the period of the oscillatory exchange of a single energy quantum between the atom and the cavity, the Rabi time, see **Figure 2**. A second time is the transit time of the atom through the cavity. The third time comes from the coupling of the combined atom-cavity system to the environment and is determined by the photon lifetime inside the cavity and the atomic lifetime due to spontaneous emission into directions not supported by the cavity.

In principle, these three times scales can be arbitrary, making the description of an experiment rather tedious. CQED, however, achieves the ideal situation in which these time scales can differ by orders of magnitude. The distinct hierarchy is the key ingredient for coherently controlling the system at the level of single atomic and photonic quanta. In the microwave domain, it ensures that different atoms passing the cavity one after the other interact with

essentially the same cavity field. In the optical domain, the time scales follow a different hierarchy. While in the regime of strong coupling the single-photon Rabi period is still shorter than the lifetimes of both the cavity and the atom, the transit time can now be many orders of magnitude longer. It follows that a single atom can interact with literally thousands and millions of photons one after the other. This provides an excellent opportunity to make real-time measurements on a single atom by observing the photons emitted from the cavity. In fact, the rate of information one can achieve from a single intra-cavity atom can significantly exceed the corresponding rate of a free-space atom, for two reasons: one is the nearly 'one-dimensional' radiation environment, the other is the fast time scale provided by the short Rabi period in the regime of strong coupling. The loss of photons is therefore a highly useful ingredient of optical CQED experiments [6].

It follows, that atoms and photons play opposite roles in microwave and optical CQED. This can also be understood when comparing the kind of excitation that is typically employed to drive the atom-cavity system in the two domains. In most microwave experiments, energy is provided by atoms entering the cavity in the excited state, quickly depositing a photon into the cavity. In the optical domain, atoms tend to be in their ground state, and excitation of the system is provided by an external laser. Two configurations are possible: Firstly, the laser drives the atom which then emits a photon into the cavity, again by virtue of the short Rabi time in the strong coupling regime. Secondly, the laser excites the cavity whose transmission is modified by the presence of the atom. In both configurations, accurate knowledge about the atom can be obtained by observing with unprecedented time resolution the photons that escape the cavity through one (or both) of its mirrors.

Let us now look at a typical experiment as displayed in **Figure 3** [2]. Here, the cavity is of the Fabry-Perot type and consists of two concave dielectric mirrors facing each other at a distance of the order of a few 100 μm. In addition to a small cavity waist, the small distance between the mirrors is an essential requirement for achieving strong coupling. This can easily be explained by noting that the huge electric field (typically a few 100 V/m) of a photon confined to a small volume in space makes the interaction between the atom and the photon very large. The small mirror spacing, however, has a pronounced disadvantage: the photon lifetime is small, too. To compensate the decrease of the cavity lifetime, the reflectivity of the mirrors must be as high as possible. The best commercially available mirrors feature transmission, absorption and scattering losses down to about 1 : 1 000 000 each, a value several 10 000 times smaller than that of metallic mirrors. This makes it possible to realize cavities with a finesse of a few 100 000, meaning that single photons are reflected to and fro several 100 000 times.

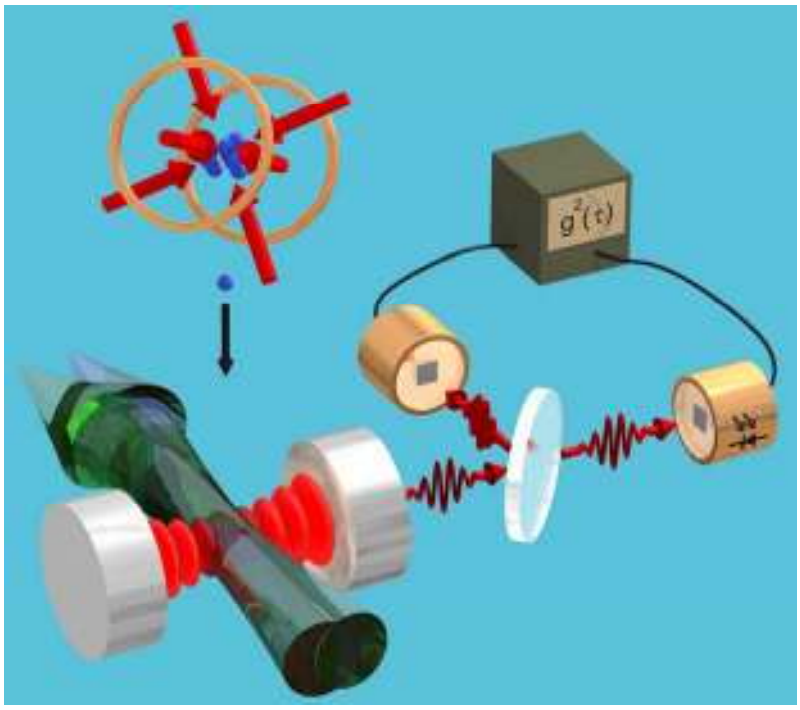


Figure 3

Single atoms are now sent between the two mirrors, either dropped from above or injected from below in fountain geometry. The velocity of the atoms is reduced to a value close to zero by standard laser cooling and trapping techniques. In the simplest situation, these atoms just pass the cavity in free fall, in which case transit times of the order of a few 10 μs are achieved. The atoms can also be trapped inside the cavity by means of an auxiliary laser field (not shown in **Figure 3**). In the latter case, single atoms have been observed to stay inside the cavity for many seconds, limited either by collisions with atoms of the background gas in a non-perfect vacuum or, ultimately, by the cavity-enhanced vacuum fluctuations of the trapping laser. The extended cavity dwell time, however, comes at the expense of a dramatically more complex protocol of capturing, trapping and cooling the intra-cavity atom. The precise control of the atomic motion between closely spaced, highly reflecting mirrors is subject of intense investigations in several laboratories worldwide.

Many spectacular CQED experiments have been performed in the optical domain during the last few years. These include the observation of single atoms in real-time, the vacuum-stimulated scattering of photons, the feedback on the atomic motion based on a velocity measurement, the cooling of atomic motion by means of a novel technique avoiding spontaneous emission, the realization of a continuously operated single-atom light source, the optical transport of single atoms through a high-finesse cavity, and the spectroscopic investigation of the energy-level structure of the strongly coupled system. But arguably most interesting from the point of view of quantum information processing is the demonstration of a novel light source emitting single photons on demand, as described now in more detail.

A novel feature of this new light source is that it generates photons without spontaneous emission. In particular, the emitting atom is at no time promoted to an excited state. Instead, the atom is always in a so-called dark state: By slowly varying the parameters of the system, the atom is adiabatically transferred from one ground state to another ground state (of another hyperfine or Zeeman level) while depositing a photon into the initially empty cavity. The process is intrinsically reversible and thus ideal to inter-convert flying and stationary qubits,

i.e. photons and atoms, respectively. It also allows one to shape the time-dependent amplitude and phase of the emitted photon. Experimentally, the passage is achieved by slowly increasing the intensity of the laser driving the atom (see **Figure 3**) and simultaneously decreasing the strength of the atom-cavity coupling, e.g., by removing the atom from the cavity. The decrease of the atom-cavity coupling can alternatively be realized by employing cavity decay, i.e., by removing the photon from the system. In the latter case, the atom can be pumped back to the initial state and the whole process can be repeated as long as the atom resides in the cavity. In this way, a bit stream of single-photon pulses is generated.

Figure 4 shows data from the very first experiment [2] already performed in 2002 with atoms falling through the cavity at such a low rate that the probability of having two or more atoms in the cavity is negligible. The figure displays the intensity autocorrelation function of the emitted photon stream as measured with the Hanbury-Brown and Twiss setup of **Figure 3**. The pronounced peaks reflect the pulsed nature of the light source and occur at times determined by the repetition rate of the pump laser, about 200 kHz. The missing peak at zero delay time proofs that single photons are emitted, because single photons cannot hit simultaneously the two photon detectors behind the beam splitter. The decay of the peak height for increasing delay time comes from the finite atom-cavity transit time in this first experiment. The decay was largely suppressed in similar experiments performed recently with a trapped atom or ion. Exciting results were also obtained in an experiment in which two photons generated successively were appropriately delayed and superimposed on a beam splitter. A novel interference effect was observed that occurs only for quantum light fields. It proves that a CQED single-photon light source is ideal for quantum communications and quantum computing in a distributed network of atom-cavity systems, as proposed by several theory groups worldwide.

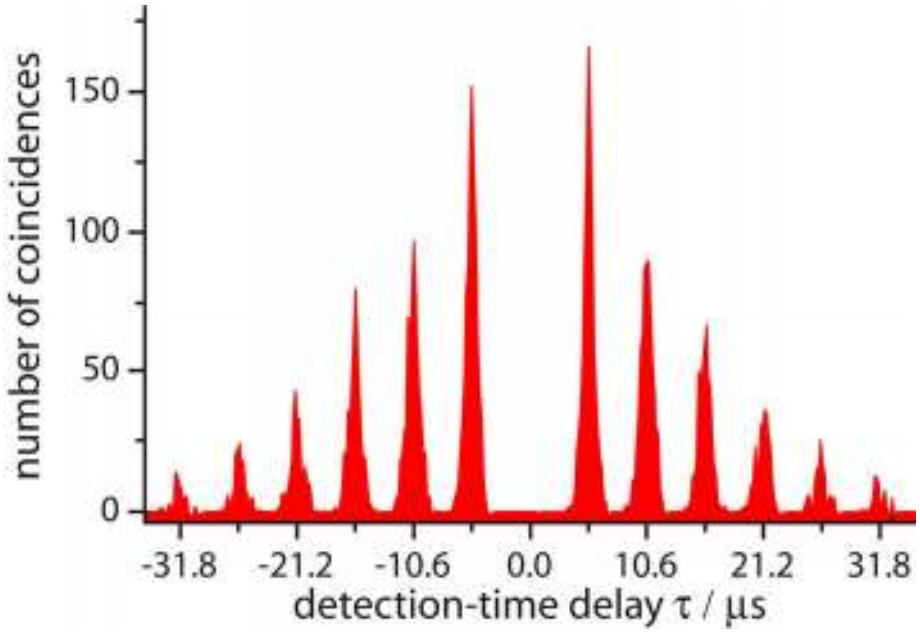


Figure 4

The experimental techniques required to control both the internal and external degrees of freedom of single strongly coupled atoms are quite demanding, making the experiments a true challenge. However, experimental progress has been impressive in the relatively young research field of optical CQED. From the theoretical side, the dissipative coupling to the environment makes the description of optical experiments very difficult. A big challenge is to

take into account the atomic motion and the effect of the light force. This force arises from the recoil kicks the atom experiences when scattering a photon. The inclusion of the light force leads to a complex interplay between the motion of the atom, its internal dynamics and the dynamics of the cavity field. No general solutions of the problem of a driven, open system are known even for one intra-cavity atom.

Conclusions

Both in the microwave and the optical domains, more experiments in the same league as those mentioned above are now in progress or planned. For example, it will be possible to repeatedly move trapped atoms in and out of the strong-coupling region in the near future, enabling one to address individual or pairs of qubits of an atomic quantum register with a high-finesse cavity. Hence, deterministic entanglement of one stationary atom (out of many) and a flying photon is within sight. In another line of experiments, setups with two separated cavities are presently under construction. They will offer a much greater flexibility and new possibilities for quantum information processing. For example, atomic state teleportation at a macroscopic distance (several meters) seems to be in reach. Finally, non-local Schrödinger cat states could be created and studied. Such states are a completely new species of quantum monsters, putting our understanding of decoherence and non-locality under close scrutiny.

It is even possible to envision experiments blending atom chip and CQED concepts. On-chip conveyor belts can be used to transport atoms and move them into on-chip transmission-line cavities. Such integrated experiments provide a scalable architecture for quantum information processing. Coherence preserving traps can be tailored for Rydberg atoms, holding them over superconducting chips, which block their only decay, spontaneous emission. In addition, the on-chip atoms could be coupled with superconducting qubits also integrated on-chip, opening a wealth of new possibilities. Last but not least, the recent advances in nanotechnology will allow one to design novel wavelength-sized optical cavities, e.g., with photonic band gap materials. Such small cavities could dramatically boost the speed of quantum gates or the rate of single photons delivered on demand. A first step into this direction has already been done with the achievement of strong coupling in systems with artificial atoms, i.e. quantum dots. All these exciting possibilities give CQED a bright future!

List of terms and acronyms

CQED: Cavity Quantum Electrodynamics

References

[1] P. R. Berman (Ed.), *Cavity Quantum Electrodynamics*, in *Advances in Atomic, Molecular and Optical Physics, supplement 2*, Academic Press, New York, 1994
[2] F. De Martini and C. Monroe (Eds.), *Experimental Quantum Computation and Information*, in *Proceedings of the International School of Physics "Enrico Fermi"*, IOS Press, Amsterdam, 2002.
[3] H. Mabuchi and A. C. Doherty, Science **298**, 1372 (2002)
[4] K. J. Vahala, Nature (London) **424**, 839 (2003)
[5] J.-M. Raimond, M. Brune and S. Haroche, Rev. Mod. Phys. **73**, 565 (2001)
[6] G. Rempe, Physics World **13** (12), 37 (2000)

Projects funded by the European Commission and related to the work in this article:

QUBITS
Quantum Based Information Processing and Transfer with Single Atoms and Photons
Start date: 01/01/2000
End date: 31/12/2002
Project web site: http://www.imperial.ac.uk/physics/qubits/
Contact Person: Peter Knight, Imperial College, London, UK, p.knight@ic.ac.uk

QUEST
Quantum entangled states of trapped particles
Start date: 01/05/2000
End date: 31/04/2004
Project web site: http://www.iota.u-psud.fr/~quest/index.html
Contact Person: Philippe Grangier, IOTA, Orsay, France, philippe.grangier@iota.u-psud.fr

QUIPROCONE
Quantum Information Processing & Communications Network of Excellence
Start date: 01/08/2000
End date: 31/07/2003
Project web site: http://www.quiprocone.org/quipmain.htm
Contact Person: Tim Spiller, Hewlett Packard, Bristol, UK, ts@hplb.hpl.hp.com

QGATES
Quantum Gates and Elementary Scalable Processors Using Deterministically Addressed Atoms
Start date: 01/01/2003
End date: 31/12/2005
Project web site: http://www.imperial.ac.uk/physics/qgates/
Contact Person: Danny Segal, Imperial College, London, UK, d.segal@ic.ac.uk

CONQUEST
Controlled quantum coherence and entanglement in sets of trapped particles
Start date: 01/03/2004
End date: 28/02/2008
Project web site: http://www.quniverse.sk/conquest/
Contact Person: Vladimir Buzek, Bratislava, Slovakia, buzek@savba.sk

Projects funded by National initiatives or organizations and related to the work in this article:

QIV
Quanteninformationsverarbeitung
Start date: 01/04/1999
End date: 31/03/2005
Project web site: http://kerr.physik.uni-erlangen.de/qiv/
Contact Person: Gerd Leuchs, Erlangen, Germany, leuchs@physik.uni-erlangen.de

Contact information of the authors of this article:
Jean-Michel Raimond
Laboratoire Kastler Brossel, Département de Physique
Ecole Normale Supérieure
24 rue Lhomond
75005 Paris
France
Email: jmr@lkb.ens.fr
Web page: http://www.lkb.ens.fr/recherche/qedcav/english/englishframes.html

Gerhard Rempe
Max-Planck Institute for Quantum Optics
Hans-Kopfermann-Str. 1
D-85748 Garching

Germany
Email: gerhard.rempe@mpq.mpg.de
Web page: http://www.mpq.mpg.de/qdynamics/

QIP with trapped electrons in vacuum

Paolo Tombesi
Paolo Tombesi is professor and Head of the Physics Department at the University of Camerino in Camerino, Italy. His research activities include: quantum optics and quantum information. Member of: OSA, SIF, EPS, APS, and AAAS. Italian projects funded by MIUR: PRIN 1997, 2001, 2002, 2003; FIRB 2001; funded by INFM: PRA 1998; PAIS-A 1999, 2001. EU projects: ERBCHRXCT930114, ERBFMRXCT960066, HPRN-CT-2000-00121, FET IST-2001-33167, MRTN-CT-2003-505089, FP6-STREP-003772. Consultant of MIUR 1986-1989.

Irene Marzoli
Irene Marzoli is researcher at the Physics Department at the University of Camerino in Camerino, Italy. Her research interests include theoretical quantum optics and quantum computing. She is a member of the Optical Society of America (OSA). She is a member of the following EU-funded IST projects: FET IST-2001-33167 and FP6-STREP-003772.

Abstract
By means of static electric and magnetic fields one can construct scalable traps able to confine many single electrons in vacuum. The ground state and the first excited state of the trapped electron's axial motion together with its spin states store the quantum bits. Selected radio wave or microwave pulses permit to perform any desired logic gate and to implement a fault-tolerant quantum computer.

Introduction
In the search for the implementation of quantum computing a number of experimental approaches, from a variety of scientific disciplines, are pursuing different paths to meet the quantum mechanical challenges involved [1]. However, we are still at the proof-of-principle stage, where operations are limited to a small number of qubits. In the long run towards a

winning technology for quantum computation it is, hence, worthy to investigate new systems. Encouraged by the impressive results obtained in the experiments with a single electron in a Penning trap and by the recent advancements in three-dimensional micro-trap fabrication, we showed the theoretical possibility of realizing a scalable quantum computer with trapped electrons in vacuum [2]. This system is the object of the project QUELE, FP6-STREP-003772, funded by the European Union under the 6th Framework Programme. The final task of the QUELE project will be to experimentally realize this quantum processor.

The Penning trap

Penning traps are able to confine charged particles by means of a combination of a static quadrupole potential with a homogeneous magnetic field. See **Figure 1** By using electrons in vacuum we combine the low de-coherence environment and experimental accuracy typical of ion traps with the high clock speed, compactness, and scalability of solid-state devices. Furthermore, an array of planar Penning traps, holding single electrons, can realize an artificial molecule suitable for NMR-like quantum information processing. In our approach, thus, we bring together the better of two avenues to quantum information processing: nuclear magnetic resonance and ion trapping.

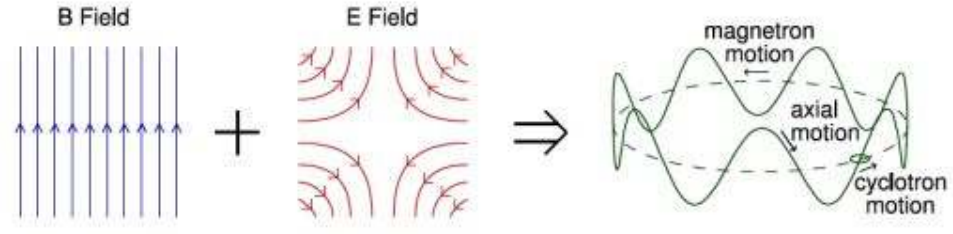


Figure 1

Both approaches, indeed, have provided the first experimental demonstrations of fundamental logic quantum gates and quantum algorithms, though still limited to few qubits. An obvious advantage of trapping electrons instead of ions is, because of the smaller mass, the higher trapping frequency of the quantized external degrees of freedom, which are known as magnetron, axial and cyclotron motion. Indeed, the typical resonance frequencies of the resulting electron motion lie in the radiofrequency and microwave domain, making it possible to employ the same technological resources and methods developed for NMR experiments. Moreover, differently from a Paul trap, a Penning trap does not rely on radio frequency fields to trap charged particles, a benefit in terms of stability of the trapping potential. In turns, this translates into less de-coherence affecting the trapped particles. Typical experimental values for a trapped electron are reported in the Table 1. See **Figure 2.**

Transition:	Frequency:	$h\nu/k_b$:	Damping:
Magnetron	$\nu_m = 11.85$ kHz	$\frac{h\nu_m}{k_b} = 0.57\ \mu$K	$\frac{\gamma_m}{2\pi} \approx 10^{-15}$ Hz
Axial	$\nu_z = 64.42$ MHz	$\frac{h\nu_z}{k_b} = 3.1$ mK	$\frac{\gamma_z}{2\pi} \approx 5$ Hz
Cyclotron	$\nu_c = 146.5$ GHz	$\frac{h\nu_c}{k_b} = 7.0$ K	$\frac{\gamma_c}{2\pi} \approx 0.02$ Hz
Spin	$\nu_s = 146.7$ GHz	$\frac{h\nu_c}{k_b} = 7.0$ K	$\frac{\gamma_s}{2\pi} \approx 10^{-12}$ Hz

Figure 2

Therefore, electrons trapped in vacuum seem to be a promising candidate for quantum information processing. Experiments with a single-electron have achieved an astonishing precision in determining the value of fundamental constants, such as the electron giromagnetic factor *g*. Moreover, the experimental control has reached the quantum level for the cyclotron motion of the electron, which has been prepared and maintained in the lowest Fock states [3].

The new scalable trap

Our system consists of a set of electrons confined in vacuum within an innovative trapping arrangement. Our scheme reproduces a linear array, or a planar disposal, of Penning traps with inter-particle distances *d* that could range from a few micrometers up to one millimetre or more. See **Figure 3**.

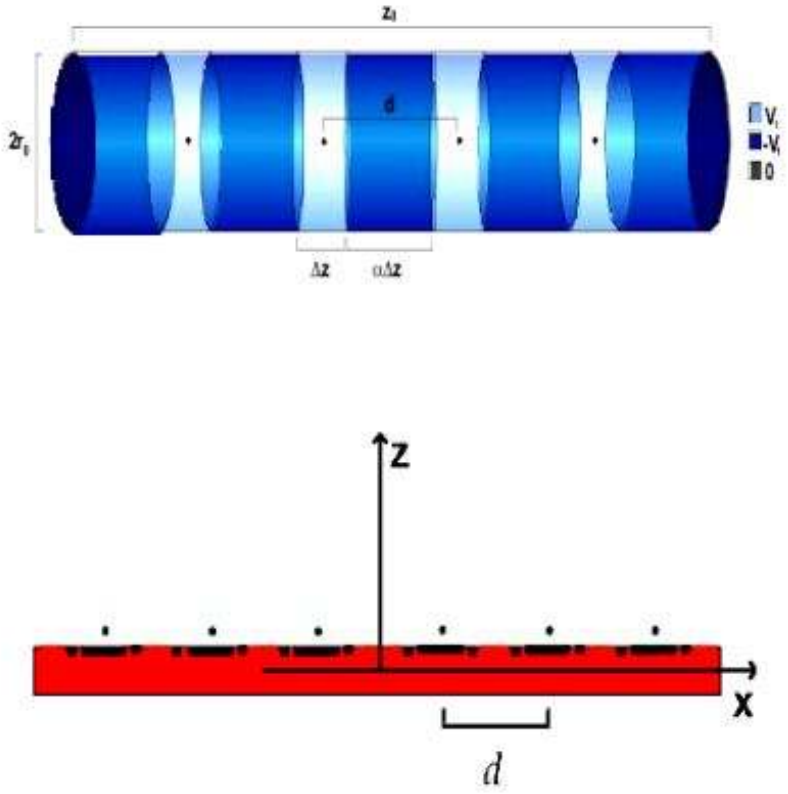


Figure 3

Quantum information is encoded in the different quantized degrees of freedom of the electron motion as well as in the two states of the spin. Although the magnetron motion, which is metastable, possesses a very small damping rate it is, however, too slow for quantum information purposes. It remains in its state for years. The cyclotron motion has a damping time of 0.1 s due to synchrotron radiation, which could be reduced by cavity effects. However, because of its high frequency, at the cryogenic temperature of 100 mK the system will work, it will remain in its ground state. The axial motion, when not in contact with the measurement apparatus, has a damping time of the order of 10^6 s, because it is weakly damped by synchrotron radiation. The fast decay time of the cyclotron motion will permit the cooling of the axial motion down to the ground state transfering the axial energy to the cyclotron by means of a suitable coupling. The spin will spontaneously flip in years. Thus, as logical states for the quantum processor it will be considered the ground and first excited levels of the axial oscillator, respectively $|0\rangle_z$ and $|1\rangle_z$, and the two spin states $|\downarrow\rangle$ and $|\uparrow\rangle$ for the logical states $|0\rangle$ and $|1\rangle$.

The gates

The gate operations on single particles are performed by means of appropriate electromagnetic pulses at the radio wave or microwave frequencies. When combined with specific static inhomogeneous fields, they permit one to achieve universal computation on the qubits of each single electron and the conditional dynamics. See **Figure 4**.

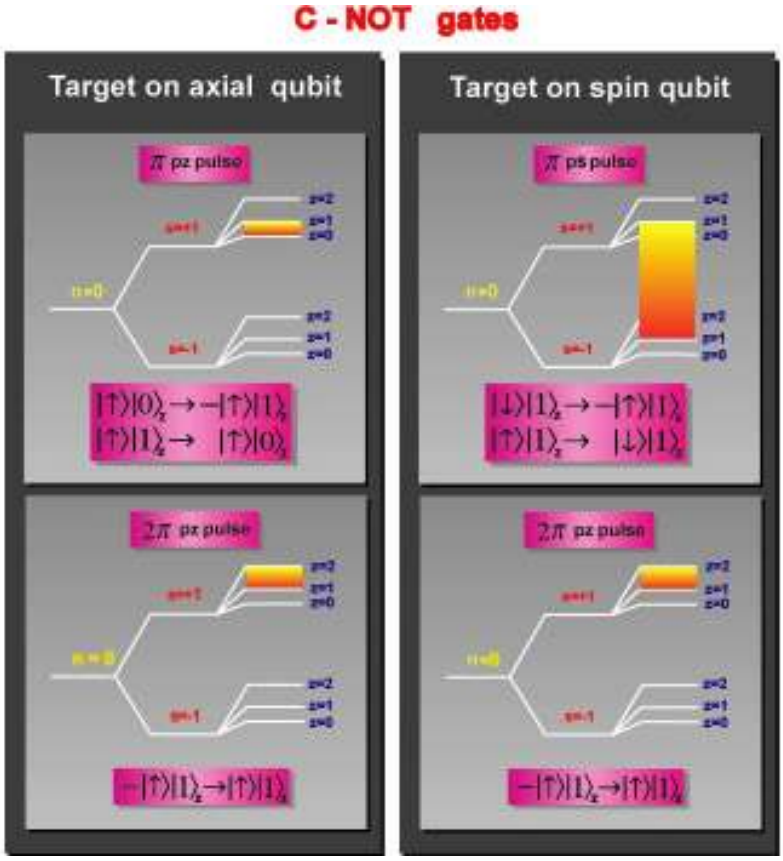


Figure 4

In order to realize universal gates between qubits of different electrons, and to have the complete scalability of the system, we exploit the Coulomb interaction in the following way. Each trap confines a single electron, which oscillates with its own axial frequency. See

Figure 5. When two neighbouring particles are put into resonance, they may exchange a quantum of excitation.

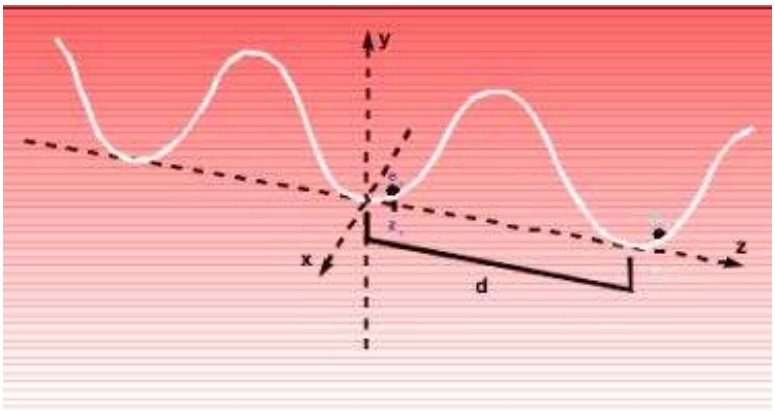


Figure 5

If we are dealing with the lowest Fock states of the axial motion, i.e. $|0\rangle_z$ and $|1\rangle_z$, this operation amounts to a swapping gate. See **Figure 6**.

$$
\begin{aligned}
|0\rangle_{1z}|0\rangle_{2z} &\rightarrow |0\rangle_{1z}|0\rangle_{2z} \\
|0\rangle_{1z}|1\rangle_{2z} &\rightarrow i|1\rangle_{1z}|0\rangle_{2z} \\
|1\rangle_{1z}|0\rangle_{2z} &\rightarrow i|0\rangle_{1z}|1\rangle_{2z} \\
|1\rangle_{1z}|1\rangle_{2z} &\rightarrow -|1\rangle_{1z}|1\rangle_{2z}
\end{aligned}
$$

Figure 6

This ability, combined with the universal set of quantum gates on every single electron, allows us to implement conditional dynamics between different particles.

Fault-tolerance

Our final goal is to have a scalable fault-tolerant quantum computer [4], then it is important that the system maintains its coherence as long as possible, in order to perform all logical operations needed before loosing the coherence. We distinguish two main de-coherence sources: thermal noise in the electrode surfaces and voltage fluctuations induced by the electronic apparatus controlling the gate dynamics. Thermal noise in the electrode surfaces is a fundamental phenomenon, in principle not eliminable and depending, for a given electrodes arrangement, only on the temperature of the trapping device. Differently, the noise fed into the system by the electronic apparatus depends on the properties of its electronic components, their temperature, and the characteristics of any noise reduction device. Therefore, this noise source can be, in principle, reduced, though it is difficult to estimate the ultimate technological limit.

Thermal noise in the electrode surfaces, due to the induced image charges, produces fluctuating electric and magnetic fields at the position of the trapped electrons. These fluctuating fields, in turn, induce de-coherence and heating in the energy eigenstates of the

axial and spin electron motions. These effects can be estimated using the theoretical models available in the literature [5]. One can show that they depend on the spectral functions of the fluctuating electric and magnetic fields. In our device, the de-coherence effects due to thermal noise in the electrode surface affect much more quickly the axial qubit than the spin qubit. When, in our quantum processor, thermal noise in the electrode surfaces is the main source of de-coherence, we can perform roughly 10^6–10^8 coherent operations. However, the effects of the additional noise produced by the electronic apparatus controlling the gate switching can be more important. Generally, noise in the electrode voltage induces fluctuations at the electron position, both in the electric field and in the electric field gradient. Heating and de-coherence of the electron axial states, due to the noisy electronic apparatus, will depend on the spectral density of the electric field noise. Good low-temperature electronics could have noise as small as 10^{-11}V/√Hz [6], corresponding to a capability for our system of 10^4 - 10^6 coherent operations.
This corresponds to an error probability per gate below the threshold for fault-tolerant computation.

Conclusions

We have shown that a system consisting of trapped electrons in vacuum is a valid candidate for a scalable quantum computer. This approach presents three major advantages: high clock speed, low de-coherence, and scalability.

The qubit readout can be achieved by axial frequency measurements as in traditional Penning traps or by capacitance and charge measurements as in semiconductor quantum dots. A fundamental requirement of our scheme is the ground state cooling of the axial motion. Though not yet experimentally demonstrated, this task should be, by applying specific techniques, within the reach of present technology.
A possible scheme, able to avoid the cooling of the axial motion, exploits the effect of the static magnetic field gradient we have to introduce in order to make each electron's spin singularly addressable. Indeed, in this case one can show that the Coulomb interaction among the trapped electrons results in an effective spin-spin coupling, as in the molecules used for NMR quantum computing.

Qubits are encoded in the two-level system provided by the electron spin, similarly to what happens for NMR spin one-half nuclei. In this case we loose one qubit per site (the axial qubit) but we gain in the feasibility of the device, without having to cool the axial motion down to its ground state. The resulting system may be regarded as an artificial molecule suitable for NMR quantum computation. Actually, we can even envisage applications to simulate other quantum systems, like the Ising model or a spin glass. In addition, the spin-spin coupling strength depends on external parameters, like the intensity of the magnetic field gradient, the trapping frequencies, and the inter-particle separation, that can be adjusted to obtain the optimal performance of the quantum processor.

List of terms and acronyms

Qubit: quantum bit
Fock state: the eigenstate of the harmonic oscillator
NMR: Nuclear Magnetic Resonance
.

References

[1] M.A. Nielsen and I.L. Chuang, *Quantum computation and quantum information* Cambridge University Press 2000
[2] G. Ciaramicoli, I. Marzoli, and P. Tombesi, Phys. Rev. Lett. **91**, 017901 (2003)
[3] S. Peil and G. Gabrielse, Phys. Rev. Lett. **83**, 1287 (1999)
[4] A.M. Steane, Nature **399**, 124 (1999); D.P. DiVincenzo, Forstchr. Phys. **48**, 771 (2000)
[5] C. Henkel, S. Pötting, and M. Wilkens, Appl. Phys. B: Laser Opt. **69**, 379 (1999)
[6] B.E. Kane, Nature **393**, 133 (1998)

Projects funded by the European Commission and related to the work in this article:

QUELE
Quantum Computing with Trapped Electrons
Start date: 01/09/2004
End date: 31/08/2007
Project web site: http://fisica.unicam.it/quele
Contact Person: Paolo Tombesi, University of Camerino, Italy, paolo.tombesi@unicam.it

CONQUEST
Controlled Quantum Coherence and Entanglement in Sets of Trapped Particles
Start date: 01/03/2004
End date: 28/02/2008
Project web site: http://www.quniverse.sk/conquest/
Contact Person: Vladimir Buzek, Research Center for Quantum Information, Bratislava, Slovakia, buzek@savba.sk

Projects funded by National initiatives or organizations and related to the work in this article:

MEPTRAP
Multi-electron Penning Trap
Start date: 01/10/2001
End date: 30/09/2003
Project web site: none
Contact Person: Paolo Tombesi, University of Camerino, Italy, paolo.tombesi@unicam.it

Contact information of the authors of this article:
Paolo Tombesi
Department of Physics
University of Camerino
Via Madonna delle Carceri
62032 Camerino, Italy.
Email: paolo.tombesi@unicam.it

Irene Marzoli
Department of Physics
University of Camerino
Via Madonna delle Carceri
62032 Camerino, Italy
Email: irene.marzoli@unicam.it

Atom chips

Jörg Schmiedmayer
Jörg Schmiedmayer is professor of physics at the Physikalisches Institut of the Universität Heidelberg in Heidelberg, Germany. His research interests include**:** atomic physics, quantum optics and quantum information. He is a member of the following professional societies: American Physical Society and EPS. He is the coordinator of the following EU-funded IST projects: ACQUIRE and ACQP. He is also a member of the EU-funded IST projects: FASTnet, AtomChips and SCALA. Positions held in the past: Universität Innsbruck (1994-2000).

Edward Hinds FRS
Edward Hinds is professor of physics at Imperial College London, England. His research interests include: atomic and molecular physics, quantum optics and quantum information. He is a member of the following professional societies: Fellow of the Royal Society, Fellow of the Institute of Physics, Fellow of the Optical Society of America, Fellow of the American Physical Society. He is a member of the following EU-funded IST projects: FASTNET, ColdMolecules, QGATES, AtomChips, SCALA. He has received the following professional awards: Royal Society Visiting Professor, Oxford University 1992/3, Royal Society Leverhulme Trust Senior Research Fellow 1998/9, Alexander von Humboldt Prize 1998-2003, EPSRC Senior Research Fellow 1999-2004. Positions held in past: Full Professor Yale University, USA (1988-95) and Professor of Physics Sussex University (1995-2002).

Abstract

Atom Chips are microfabricated, integrated devices in which electric, magnetic and optical fields can confine, control and manipulate cold atoms. Through miniaturization, atom chips offer a versatile new technology for implementing modern ideas in quantum optics, quantum measurement and quantum information processing. Over the last five years, there has been spectacular progress in preparing and manipulating the quantum states of atom clouds on chips. The next big challenge is manipulating single atoms, allowing them to have controlled collisions and coupling them to single photons in optical microcavities. This emerging technology will lead to new quantum devices and ultimately to quantum information processing on a chip.

Introduction

Scientific and technological progress in the last decades has shown that miniaturization and integration can lead to robust applications of fundamental physics, be it electronics and semiconductor physics in integrated circuits and data processing, or optics in micro-optical devices, sensors and communication. Atom Chips are starting to realize a similar practical advance for quantum optical systems based on neutral atoms and photons.

In micro electronics, electrons move *through* micro fabricated wires, switches, transistors, etc. in electronic integrated circuits, chips, to perform elaborate tasks. In ***Atom Chips***, atoms are trapped *above* a surface, and forces under our control manipulate their motion and internal states. These forces are due to electric, magnetic and optical fields which originate in microscopic structures built on the surface of the chip. The forces produced in this way can confine atoms to micrometer-sized regions, where the characteristic quantum energy $h^2/2Ma^2$ (h is Planck's constant, M is the mass of the atom and a is the 1 μm size of the trap) corresponds to a temperature of a few hundred nanoKelvins. Since the atoms can be much colder than this, quantum effects can be completely dominant, opening the possibility of new quantum devices based on the control of neutral atoms. This quantum confinement idea is precisely the one used to harness the electrons in mesoscopic quantum electronic devices. However, the atoms here are very well isolated from the warm solid state environment, allowing their quantum states to remain undisturbed for tens or hundreds of seconds. The combination of this long decoherence time together with the capability of precise microscopic control makes the atom chip an exceedingly attractive candidate for robust implementation of new quantum devices.

Breadth of applicability

Research over the last five years has already established the atom chip as an immensely versatile new technology able to perform an astonishing range of functions. Already we know how to collect atoms, cool them to nK temperatures and load them into tiny traps a few microns above the surface of the chip. Several groups now have Bose Einstein condensates (BEC) on a chip, in which some 10,000 atoms all have precisely the same wavefunction. This is a pure quantum state, similar to that of the light in a laser beam and it provides a crucial starting point for many quantum devices, including a quantum information processor, because it is a state of essentially no entropy. After several years of intense development, techniques have emerged for making electric, magnetic and optical fields drive coherent manipulations of this quantum state. Much of this development has focussed on understanding and controlling the decoherence processes due to fluctuations of the fields and the fundamentals now seem to be understood.

Thus we now have some key ingredients of a powerful and versatile new technology capable of preparing and manipulating complex quantum states of atomic ensembles on a chip. With this toolbox in hand, the research community is well placed to realise many of the beautiful new ideas of quantum control and quantum information that have emerged over the last decade. For example, experiments on atoms in large optical lattices and cavities have shown how to prepare strings of single atoms and how to transfer quantum information coherently between atoms and photons. This could now be implemented on a chip, using the atom string as a quantum information register, and the atom-cavity coupling as a simple quantum interconnect providing optical readout. Suitable time-dependent fields should be able to manipulate the qubits to make them perform quantum logic operations. Although atom chips have only just begun to work, we can see now how all this might be integrated into a single

device. This is a daunting task, but it is also an exciting one with spectacular promise for future technology.

Micro Traps

Magnetic fields produced on the chip can manipulate a neutral atom by exerting forces on its magnetic dipole moment. For example, if a wire on the surface of the chip carries a current I this makes a magnetic field that loops around the wire, as illustrated in **Figure 1**. If a uniform field B is added to this, a line of zero net magnetic field forms parallel to the wire, as shown by the dashed line. The energy of a magnetic atom – one with electron spin, such as lithium or rubidium - is proportional to the strength of the field. Thus the atom moves on a potential surface, indicated by the mesh in the figure, which traps atoms along the dashed line at a distance R from the wire. This distance can be controlled by adjusting the current I or the field B. The force that pushes atoms to the centre of the trap is proportional to R^{-2}, which means that miniature traps with a small value of R can hold atoms very tightly, reaching nanometer scales of confinement with very low levels of power dissipation.

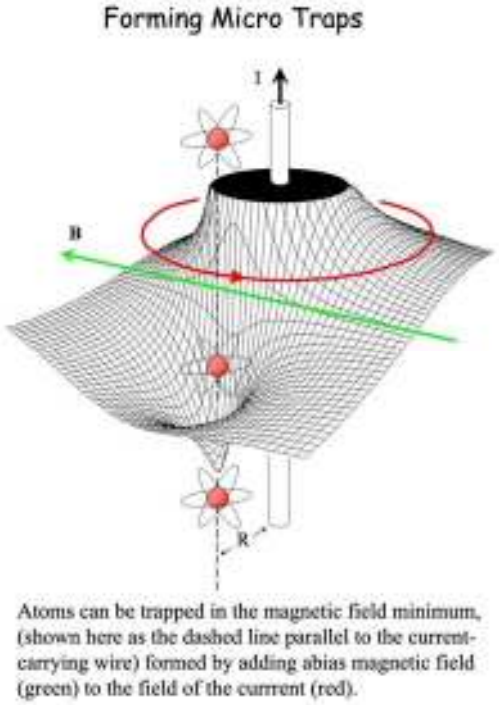


Figure 1

Electric fields can also be used to control the atoms through the electric dipole interaction. Atoms are attracted to static fields and to low-frequency light fields. If the frequency of the light is increased to lie above an atomic resonance, the atom can be pushed away from the light. Using a standing wave it is particularly simple to make a closely-spaced array of traps, since the atoms are attracted to each of the antinodes or nodes. Oscillating fields (optical, microwave or radiofrequency) also make it possible to manipulate the internal states of an atom, where quantum information is most securely stored. For example, quantum oscillations in the hyperfine sublevels of a Cs atom are the basis of the atomic clock, which is so stable it provides the international definition of the second. Atomic clocks on a chip are already a reality.

The full potential of atom chips for quantum applications is only accessible if the structures can be miniaturized to a scale of order 1 µm or below. This will allow atoms and photons to be coupled in a coherent way by placing atoms in a specific part of a light field. It will also allow tunneling between separated traps to make controlled atom-atom interactions. Researchers are working intensively on developing smaller electric and magnetic structures and on integrating new components such as micro-optics and micro-cavities into atom chips.

Fabrication of Atom Chips

Structures for magnetic and electric micro manipulation of neutral atoms benefit from being fabricated on a surface. They can be made much smaller and more robust than free-standing structures. Heat is dissipated easily through the substrate, allowing significantly higher currents to be sent through thin wires, and this results in tighter confinement and more precise control of the atoms. Micro-fabrication on a surface also permits precise positioning, as required in complex circuits with several different electric, magnetic or optical components. Combining, adapting and developing diverse fabrication technologies is therefore a central research activity.

A very promising technique for fabricating high quality wires on an atom chip has been developed within the framework of ACQUIRE and ACQP collaborations. The best results so far have come from Au layers on Si single crystal substrates. State-of-the-art multi-layer structures, with feature sizes less than 500nm and with very smooth wires, allow large current densities (up to 10^8 A/cm^2 for sub-µm wires at room temperature) and electric fields (up to 500V of potential difference over a ~10µm gap). The wires structures that are now being made have the capability of confining neutral atoms at trap frequencies up to 1 MHz, corresponding to a confinement length of ~10nm. A typical atom chip set-up ready to be mounted into the UHV chamber of the experiment and an electron microscope picture of a detailed structure on an ACQP chip are shown in **Figure 2**.

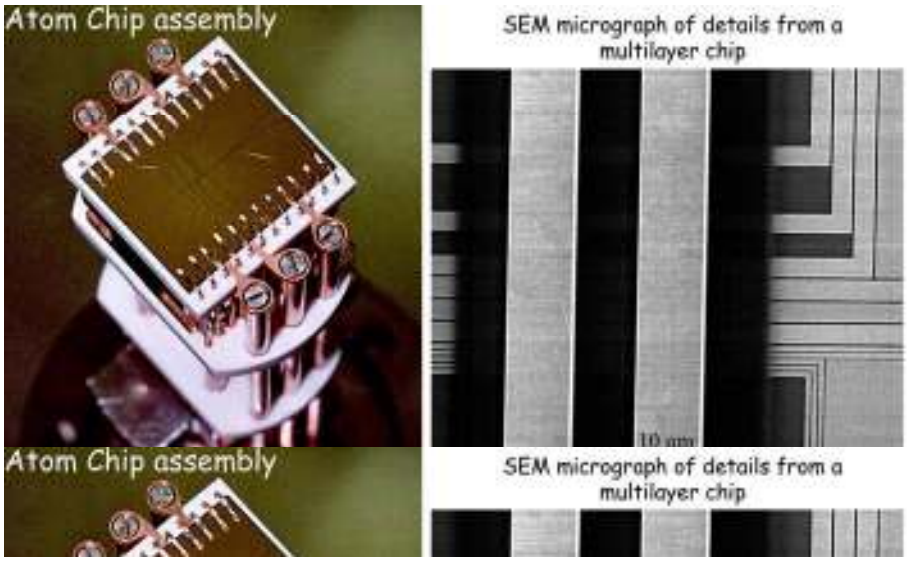


Figure 2

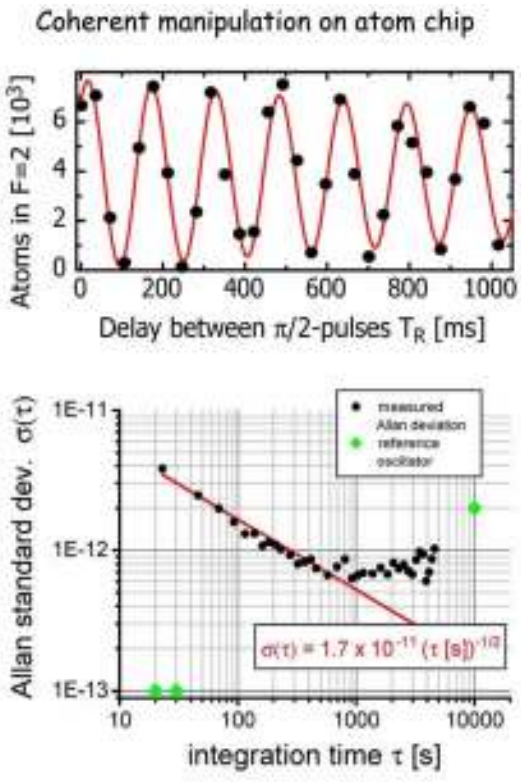
Magnetic atom chips are also being made using permanent magnetic microstructures. The first experiments used commercial magnetic storage media, such as floppy disks, video tape and hard disks. Bose-Einstein condensates have been loaded in such chips and versatile manipulations have been demonstrated with the help of adjustable bias fields. Now, custom-

built Pt/Co multilayer thin films are being developed within the QGates and FASTnet projects. As no real current flows in these films, they can make atom traps with very low technical and thermal noise. Super conducting structures at low temperature also offer low noise. In addition, the low temperature environment should be suitable for manipulating Rydberg atoms and may allow the coupling of neutral atoms to solid state quantum devices.

Quantum-Coherent Manipulation of Atoms

It is remarkable that atoms at temperatures in the nanoKelvin range can be placed a few micrometers from a room temperature surface and retain their quantum coherence for many seconds. The influence of the nearby surface on quantum manipulation can be divided into two categories. [1] The surface of the chip has electromagnetic modes that are thermally excited. The resulting field noise above the chip can induce motion of the atoms and can flip their spins, leading to decoherence of the quantum state. [2] The materials of the chip and the method of fabrication leave imperfections of the structure that in turn cause imperfections in the atom-trapping potentials. From experiments conducted over the last five years within the ACQUIRE, ACQP, FASTnet and QGates collaborations we now know how to design and fabricate chips that keep all these effects under control.

A beautiful experiment done in Munich shows the quantum coherence that can be achieved using atoms on a chip. Here ^{87}Rb atoms were magnetically trapped in a superposition of the two hyperfine ground states $|F=1, m_F=-1\rangle$ and $|F=2, m_F=1\rangle$. These states differ in energy by 6.8GHz, causing the phase of the superposition to oscillate at that frequency. **Figure 3** shows a Rubidium atomic clock on a chip. The beat between the atomic oscillation and a stable reference clock, demonstrates the long coherence time (>2.8 s) The long term stability of the clock was not limited by decoherence, but by the local reference oscillator. This shows that atom chips are suitable for practical quantum instruments. In terms of quantum information processing, the clock is an example of quantum-coherent single qubit manipulations. The next big challenge is to manipulate the interactions between atoms to produce controlled entanglement.



top: Ramsey fringes show the coherence of atoms held 8 µm from the chip surface with a coherence lifetime of 2.8 s. *bottom:* Stability analysis of the atom chip Rb clock. The long time stability is determined by the reference oscillator

Figure 3

Integrating atoms and photons

Integration of optical elements into the atom chip will be important, both as an atom-light interconnect and to facilitate the manipulation of atoms on the chip.

A light beam can be strongly altered by as few as 10 atoms provided it is well focused and the atoms are at its waist. The light becomes even more sensitive if it passes several times back and forth in an optical cavity. For the purpose of detecting one atom it is not necessary to have particularly high finesse provided the waist size is small: a few hundred is sufficient (mirror reflectivity ~99%) with a waist size of a few µm. The arrival of one atom between two such fibres significantly alters the light reflected and transmitted by the gap.

If the finesse of the micro-cavity is increased to $>10^4$, the atom-photon coupling can exceed the cavity damping rate and an excitation can oscillate coherently between the atom and the cavity. In this regime, two atoms sharing the same cavity can be entangled in a controlled way to perform quantum logic operations.

Several European laboratories working within the QGATES, ACQP and FASTnet collaborations now have atom chips with small optical structures on board capable of detecting a single atom in the cavity. Two approaches are shown **Figure 4**. On the left a pair of optical fibres with its, end coated with a dielectric mirror forms a microscopic cavity with finesse >2000. On the right we present an SEM image showing part of an array of 2000 curved mirrors etched into silicon. After coating these with dielectric films, and combined

with a plane mirror on a fiber as illustrated, these form 100 µm-long optical cavities with finesse exceeding 6000.

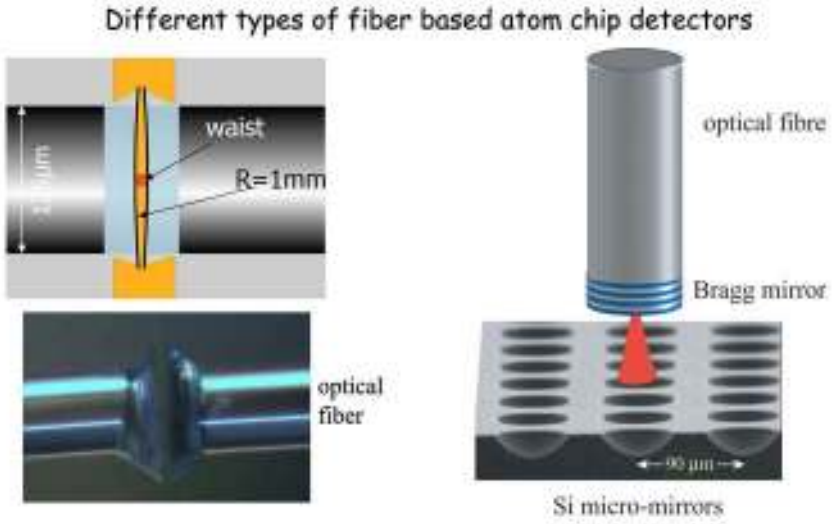


Figure 4

Conclusions

The Atom Chip offers a newly emerging technology for atomic devices based on quantum mechanics. Applications are already demonstrated involving both quantum coherence within atoms, such as microscopic atomic clocks, and between atoms, such as BEC on a chip. With recent advances on the fabrication and materials, it is now possible to achieve decoherence times of many seconds. Techniques for more complex atom manipulations using electric, magnetic and optical fields are making rapid progress and control on the micrometer length scale is now possible. The problems of single atom detection and preparation are now also solved. Putting all these capabilities together in a single chip remains a challenging project, but it is a realistic project and one with immense scientific and technological payoff. Our vision is that atom chips will deliver a variety of important quantum applications ranging from metrology to sensing to quantum information storage and processing. Many such applications are described in the other articles in this issue. We hope that this brief article provides some insight into the promise of atom chips to realise these exciting new ideas.

References

[1] *Microscopic Atom Optics: From Wires to an Atom Chip:* R. Folman, P. Krüger, J. Schmiedmayer, J. Denschlag, C. Henkel in Advances of Atomic and Molecular and Optical Physics Ed. P. Berman, H. Walter Vol. **48**, 263 (2002)

[2] *Atom Chips: Fabrication and Thermal Properties*: S. Groth, P. Krüger, S. Wildermuth, R. Folman, T. Fernholz, J. Schmiedmayer, D. Mahalu, I. Bar-Jospeh, Appl. Phys. Lett. 85, 2980 (2004)

[3] *Coherence in Microchip Traps:* P. Treutlein, P. Hommelhoff, T. Steinmetz, T. W. Hänsch, J. Reichel, , Phys. Rev. Lett. 92, 203005 (2004)

[4] *Towards integrated optical non-destructive single atom detectors:* P. Horak, B.G. Klappauf, A. Haase, R. Folman, J. Schmiedmayer P. Domokos, E.A. Hinds, Phys. Rev. A. **67**, 043806 (2003)

[5] *Special Issue on Atom Chips* Editors: C Henkel, Ch Westbrook, J. Schmiedmayer, EPJ D (May 2005)

[6] M. P. A. Jones, C. J. Vale, D. Sahagun, B. V. Hall, and E. A. Hinds, "Spin Coupling between Cold Atoms and the Thermal Fluctuations of a Metal Surface", Phys. Rev. Lett. 91, 080401 (2003)

[7] M. P. A. Jones, C. J. Vale, D. Sahagun, B. V. Hall, C. C. Eberlein, B. E. Sauer, K. Furusawa, D. Richardson, and E. A. Hinds, “Cold atoms probe the magnetic field near a wire”, J. Phys B 37, L15 (2004)

[8] P.K. Rekdal, S. Scheel, P.L. Knight and E.A. Hinds, “Thermal spin-flips in atom chips”, Phys Rev A 70 013811 (2004)

[9] S. Eriksson, F. Ramirez-Martinez, E.A. Curtis, B.E. Sauer, P.W. Nutter, E.W. Hill and E.A. Hinds, “Micron-sized atom traps made from magneto-optical thin films” Appl Phys B 79, 811 (2004)

[10] Moktadir, Z., Kukharenka, A., Kraft, M., Bagnall, D. M., Jones, M., Powell, H. and Hinds, E. A. “Etching techniques for the realization of optical micro-cavities on silicon for atom traps”. J. Micromech. Microeng. 14, 1 (2004)

Projects funded by the European Commission and related to the work in this article:

ACQUIRE
ACQUIRE
Atom Chips for Qauntum InformationReserach
Start date: 01/01/2000End date: 31/12/2002
Project web site: http://www.acquire.uni-hd.de/
Contact person: Jörg Schmiedmayer, Physikalisches Institut, Universität Heidelberg, Germany
joerg.schmiedmayer@physi.uni-heidelberg.de

ACQP
Atom Chip Quantum Processor
Start date: 01/01/2003
End date: 31/12/2005
Project web site: http://acqp.physi.uni-heidelberg.de/
Contact person: Jörg Schmiedmayer, Physikalisches Institut, Universität Heidelberg, Germany
joerg.schmiedmayer@physi.uni-heidelberg.de

FASTNET

ColdMolecules
Project web site: http://www.lac.u-psud.fr/coldmolecules/network/index.html

QGATES
Quantum Gates and Elementary Scalable Processors Using Deterministically Addressed Atoms
Start date: 01/01/2003
End date: 31/12/2005
Project web site: http://www.ph.imperial.ac.uk/qgates/
Contact person: Peter Knight, Imperial College of Science, technology and Medecine, p.knight@ic.ac.uk

AtomChips
Project web site: http://www.iota.u-psud.fr/~atomchip/

SCALA: FP6 Integrated Project in the process of negotiations.
Scalable Quantum computing with Light and Atoms
Contact person: Philippe Grangier, CNRS, philippe.grangier@iota.u.psud.fr

Projects funded by National initiatives or organizations and related to the work in this article:

DFG Forschungsschwepunkte: Quanteninformation, Wechselwirkung in entarteten Quantengasen, Kompetenznetzwerk Quantninformation (Baaden Wuertemberg)

EPSRC Cold Atoms in Microtraps Programme, UK Quantum Information IRC, UK Cold Atoms Network, UK Quantum Devices Network, Australian Centre for Quantum Atom Optics.

Contact information of the authors of this article:
Prof. Dr. Joerg Schmiedmayer
Universitaet Heidelberg
Physikalisches Institut
Philosophenweg 12
69120 Heidelberg
Germany
Tel: 49 6221 549 325 Fax: 49 6221 47 57 33
Email: joerg.schmiedmayer@physik.uni-heidelberg.de

Prof. Edward Hinds
Imperial College of Science, Technology and Medecine
Quantum Optics & Laser Science Group
Department of Physics
Blackett Laboratory
South Kensington Campus
London SW7 2AZ
Tel+ 44 (0)20 7594 7901
Email: ed.hinds@imperial.ac.uk

Atomic q-bits and optical lattices

Ennio Arimondo
Ennio Arimondo is professor of Structure of Matter since 1984 at the Universitá di Pisa, Dipartimento di Fisica in Pisa, Italy. His research activities are in the area of laser spectroscopy, laser cooling, atom deposition on surfaces, atom optics and quantum information. He is the coordinator of the following EU-funded IST projects: Cold Quantum Gases, NANOCOLD, OLAQUI.

Immanuel Bloch
Immanuel Bloch is professor of physics at the Johannes Gutenberg-University, Institut für Physik in Mainz, Germany. His research activity is in the area of quantum optics, ultracold quantum gases and quantum information. He is a member of the following EU-funded ISTprojects: OLAQUI, MC-EXT. He participates in the national focus research program of the German Science Foundation. He is the winner of the following awards: Gottfried-Wilhelm-Leibniz prize 2005, Rudolf-Kaiser prize 2003, Otto-Hahn medal 2002, Philip-Morris research prize 2000.

Dieter Meschede
Dieter Meschede is professor of physics since 1990 at the Universität Bonn, Institut für Angewandte Physik in Bonn, Germany. His research activities are in the area of quantum optics and quantum information. He is a member of the following EU-funded IST projects: QGates, NANOCOLD, FASTNet.

He participates in the Quantum Information Processing Priority Program of the Deutsche Forschungsgemeinschaft.

Abstract
Neutral atoms can be stored in the periodic intensity pattern of interfering laser light fields. Such arrays of trapping potentials – so called optical lattices – can be loaded with ultracold atoms forming a natural quantum register. Recently it has become possible to address and transport single atoms in these potentials, as well as to realize quantum gate arrays between trapped neutral atoms. We review the state of the art in these experiments and provide an outlook on the fascinating prospects for quantum information and simulation with ultracold atoms in optical lattices.

Introduction
Neutral atoms are one of the most promising candidates for realizing quantum information processing devices. Sophisticated methods, widely applied in atomic clocks, have been developed over many decades to coherently manipulate the internal quantum states of an atom. Their charge neutrality protects them well from external perturbations, leading to a reduced decoherence of the quantum dynamics. Neutral atoms in optical lattice are unique for quantum information purposes, as they are so far the only physical system, in which both an outstanding degree of single particle control exists, while simultaneously large scale qubit systems can be realized.

Very recently, a series of spectacular advances in the control over the motional degree of freedom of neutral atoms has opened fascinating prospects for quantum information processing. Single atoms can now be trapped one by one in a string of microscopic trapping potentials formed by laser light – a so called one dimensional (1D) optical lattice potential. At the same time, a large 2D and 3D array of these light traps can now be filled with a Bose-Einstein condensate and converted into a huge atomic quantum register of up to 100000 qubits, with a single atom at each lattice site.

The quantum state of individual atomic qubits can now be manipulated with sufficient precision that single atoms can be addressed in individual optical lattice potentials. Conveyor belts allow us to move atoms around at will and simultaneously retain full control over their internal and external degrees of freedom. State dependent quantum conveyer belts have enabled the creation of a massive array of quantum gates acting between atoms, which is promising for the creation of large scale entanglement—a vital resource for quantum information applications.

In this article we give an introduction to the state of art of controlling neutral atoms in optical lattices and outline the path for future challenges in this field.

Trapping atoms in optical lattices
Optical lattices are formed by the interference of several laser beams to form a perfectly periodic intensity pattern of light in space. The simplest (1D-) optical lattice can in fact be created by just superposing two counterpropagating laser beams, such that an optical standing wave is created. The optical standing wave consists of dark and bright stripes with a period of half an optical wavelength.

The interfering light pattern, the standing wave, is completely defect free and forms a perfectly periodic spatial structure. So how can atoms be trapped in these interference patterns? Typically the wavelength of the light fields used to form the optical lattice are very far detuned (usually about 50 nm) from an atomic resonance transition but the oscillating electric field of the laser light nevertheless induces an oscillating atomic dipole moment within the atom which is in-phase for red detuning and 180° out-of-phase for blue detuning of trapping laser field and atomic resonance frequency. This oscillating electric dipole then interacts with the external oscillating electric field of the laser which causes the internal energy of the atom to decrease for red and increase for blue detuning. In inhomogeneous, patterned light fields, the internal energy shift results in an effective potential from which the so called dipole force arises. For example, when the frequency of the laser light is below an atomic transition frequency, atoms are pulled into the intensity maxima of the laser field, whereas they are repelled from it in the opposite case: Since this force is very feeble only extremely slow "cold" atoms can be influenced by this force. The advent of efficient laser cooling methods was thus necessary before such experiments could start.

The optical standing wave pattern forms a perfectly periodic potential in which atoms can be trapped. Atomic motion in such a periodic potential has many similarities with e. g. electronic motion in crystalline metal. Higher dimensional (2D, 3D) optical lattice structures can be created by interfering more laser beams, e.g. by overlapping three orthogonal standing waves on top of each other, resulting in a simple-cubic lattice structure. Such an optical lattice can be viewed as a regular array of hundreds of thousands of small optical tweezers in which particles can be stored. By interfering the laser beams in different geometries it also possible to create more complex interference patterns and thereby exercise a great degree of control over the shape of the optical potential. Even more so, the potential depth of such an artificial crystal of light can be changed easily by simply controlling the intensity of the laser beams. So just by turning the laser power up or down, one can enhance or diminish the lattice depth.

Storing, observing, and transporting single atoms in optical lattices

The simplest method to store cold, i. e. slow atoms is provided by the so called magneto-optical trap. The MOT is loaded by slowing atoms from residual gas atoms and subjecting them to radiation pressure forces at the center of a magnetic quadrupole. With sensitive photon counters atomic fluorescence is monitored at the single atom level, which contributes less than 1 picowatt. From the steplike intensity distribution the precise number of atoms is inferred before the atoms are transferred to the 1D optical lattice (Schrader et al., 2004). Careful superposition of the MOT and the trapping laser beams warrant 100% efficient transfer of atoms into the optical lattice. Storage of the atoms is terminated by collisions with residual gas atom at large velocities within typically one minute. This time is sufficient to carry out numerous processes involving one or many atoms, it is thus not a limit for the realization of quantum information processes.

In the 1D lattice the atoms can be continuously observed if the laser light causing atomic fluorescence provides at the same time cooling forces – otherwise they would rapidly be heated out of the micropotentials. At λ=1 µm wavelength, the micropotentials of the 1D optical lattice are spaced by $\lambda/2$=0.5 µm, only. As shown in **Figure 1**, this separation is too small to individually detect two atoms stored in adjacent micropotentials with a typical long distance microscope resolution of 1-2 µm. However, if the atomic separation is larger than 3 or 4 micropotential periods, their separation can be measured with less than 0.1 µm accuracy – enough to exactly determine the number of micropotentials separating two atoms.

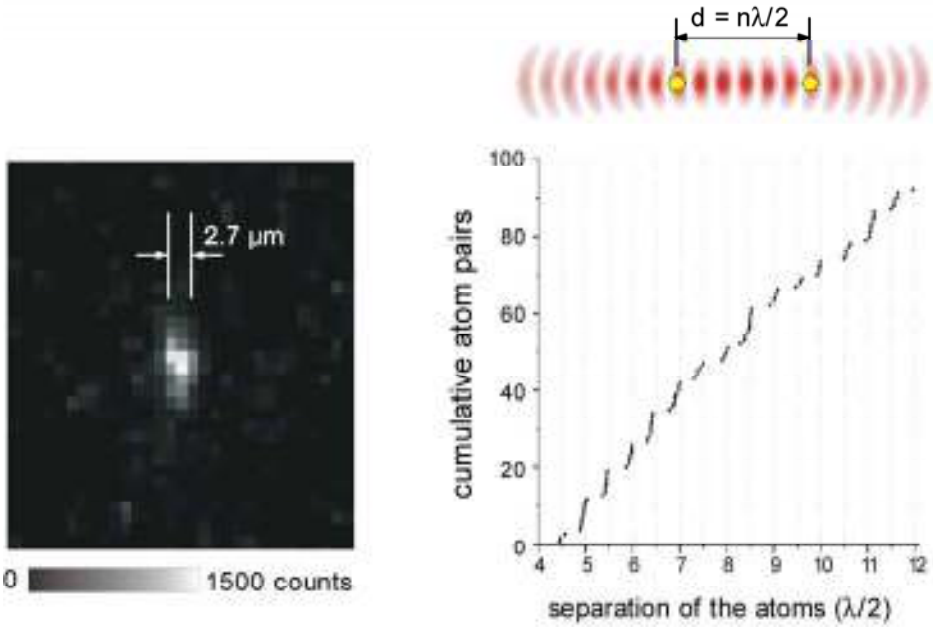


Figure 1: Storing single atoms in a 1D optical lattice **Left:** Image of a single fluorescing atom trapped in a1D optical potential. In the horizontal direction, the micropotentials are separated by 0.5 µm while the microscope resolution is about 2.7 µm. **Right:** The separation of two atoms can precisely be measured for atoms, i.e. the exact number of separating micropotentials can be given.

If the frequency of one of the two counterpropagating laser beams is slightly lowered or increased the interference pattern walks upward or downward in **Figure 2**, respectively, allowing transport of the atoms over macroscopic distances (cm). A photon counting camera allows to record small movies showing such controlled motion of a group of atoms when the optical lattice is operated as the optical conveyor belt. The "optical conveyor belt" opens the potential to bring atoms in a controlled way from one functional site to another one. For applications the quantum state of atoms can for example be prepared at one point and then transported into the electromagnetic field of a Fabry-Perot type optical microcavity where interactions with single photons can take place.

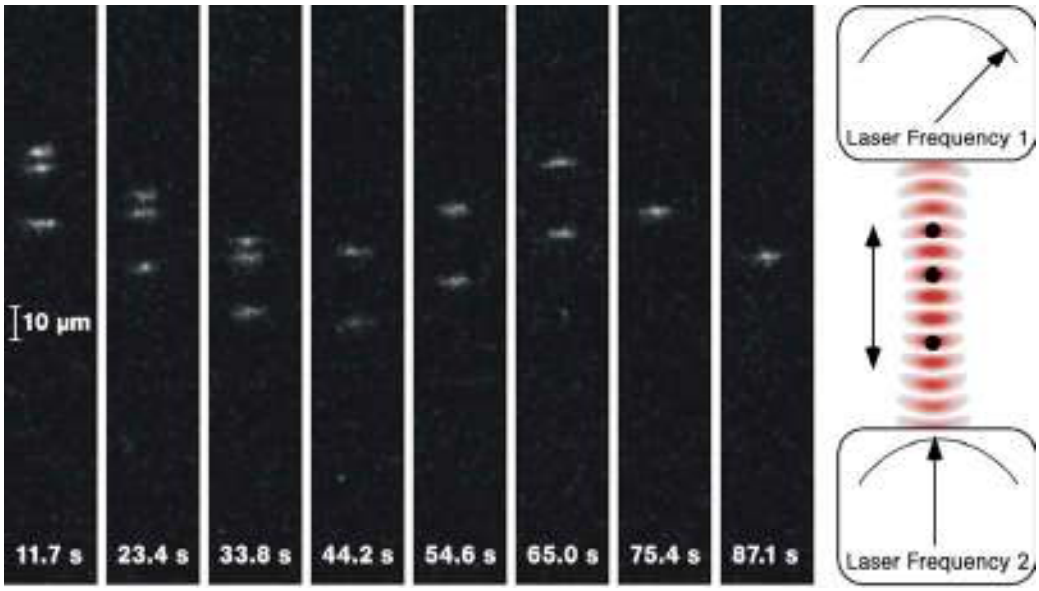


Figure 2: Optical Conveyor Belt. Snapshots of a group of 3 atoms transported with an optical conveyor belt. The laser frequencies are controlled by a computer. Departure of atoms from the conveyor belt is caused by collisions with hot residual gas atoms.

Controlling individual atom qubits in optical lattices: a neutral atom quantum register

With neutral atoms, qubits can in principle be realized with any two levels of their quantum structure, external states of atomic motion as well as internal states of the atomic electron and spin. For this article we concentrate on magnetic sublevels of the internal atomic quantum state which allow convenient manipulation by external radiofrequency fields.

In an experiment, two specific magnetic sublevels of the electronic atomic ground state are selected for the representation of the qubit. The qubit may be modelled by a sphere where the north- and southpole correspond to the logocal “0” and “1”-state, respectively. The state of the qubit can be indicated by an arrow locating the state on the surface of the sphere. Application of a resonant microwave pulse causes rotation of the arrow, and the rotation angle depends on the duration of the pulse. For instance, a so called ‚π-pulse’ rotates the angle from the north- to the south-pole and vice versa, thus it is equivalent to a logical inversion operation. A quantum register is obviously a combination of several qubits, which can be manipulated one by one, in our case atom by atom.

Operation of a register, whether of classical and quantum nature, requires realization of several functional steps: In the first step, the register must be physically prepared and initialised. In the second step, information must be written into the individual bits or qubits. In the final step, the full information must be retrieved bit by bit or qubit by qubit. For a quantum register one must demonstrate in addition to the case of a classical register that coherent superposition states of the two qubit states can be generated and is maintained for extended periods of time.

The first step is a straightforward once a string of neutral atom is prepared as described in the previous section, see **Figure 3**: Identical spin states (more precisely pseudo spin states) of all atomic qubits are prepared by “optical pumping” which by a series of absorption-emission cycles prepares all atoms to the same quantum state, for example the state corresponding to the logical ‚0’.

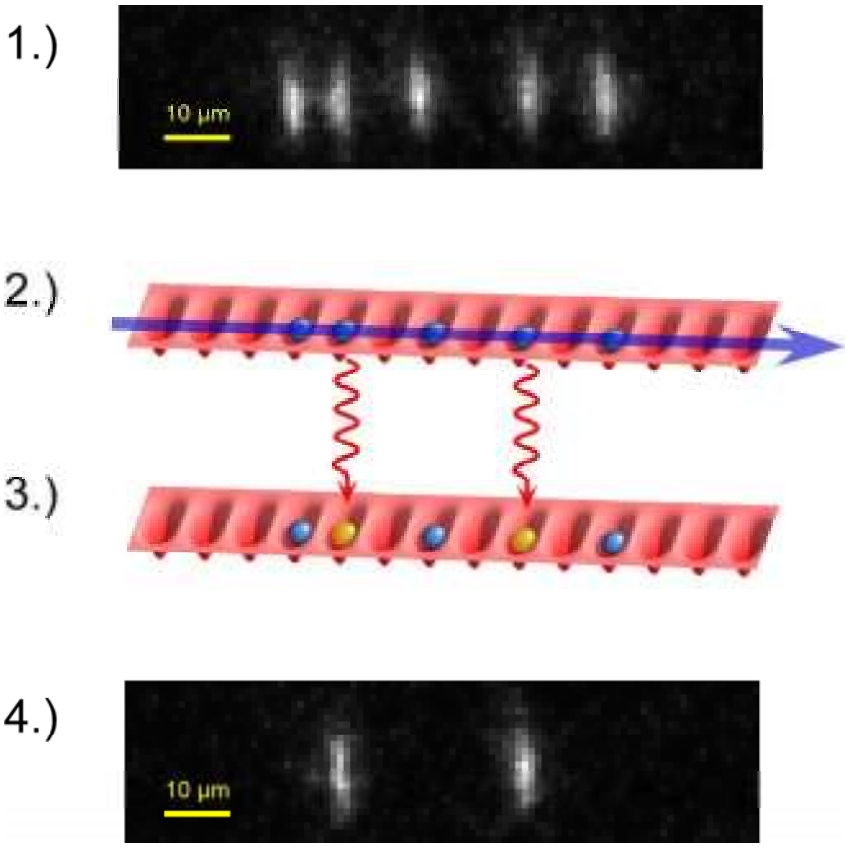


Figure 3: Operational steps of a quantum register.1.) Five atomic qubits are stored in a 1D lattice. 2.) By optical pumping all atoms are prepared in the same initial quantum state (‚blue', dark atoms). 3.) Two sequential microwave pulses invert the quantum state of the second and forth qubit (‚yellow', bright atoms). 4.) The register ist read out showing the two bright atoms only.

To achieve selectivity in the second step, an inhomogeneous magnetic field is applied which renders the magnetic resonance condition for the microwave pulse rotating the qubit state valid for a single qubit site only. Thus application of the microwave field causes rotation at this site only, even though the microwave field fills all space. At a measured spatial resolution of 2.5 µm this method could formally allow operation of a 400 qubit register in a 1mm standing wave light field. Note that a closely related method is used to obtain spatial resolution in magnetic resonance imaging procedures (MRI).

For information retrieval the quantum state of the atomic qubit is unanimously detected by .methods of laser spectroscopy which can discriminate between two atomic levels with excellent contrast. With this method for example the time evolution of the coherent superposition of the two qubit states can be observed as a function of the microwave pulse duration. The sinusoidal oscillation of the qubit state between the "0" and the "1"-state is called "Rabi-oscillation", it proves the coherent nature of the superposition and thus the quantum property of the neutral atom quantum register.

Initialising a Large Quantum Register of Neutral Atoms

A completely different approach of preparing a very large quantum register of neutral atoms has been realized with Bose-Einstein condensates in optical lattices. With the first experimental realization of such atomic Bose-Einstein condensates, perfect control over the

motional state of a matter sample had been reached. A large number of particles – all in the ground state of the trapping potential -- can now routinely be created within physics laboratories around the world. Typically Bose-Einstein condensates are formed in magnetic traps, but they can be easily transferred into an optical lattice by slowly increasing the lattice potential depth. In this way the atoms of a Bose-Einstein condensate remain in the ground state of the combined magnetic and optical trapping potential. In the state of a Bose-Einstein condensate, each atom is however delocalized over the lattice and a matter wave interference pattern can be observed as these waves are diffracted off the optical potential upon release (see **Figure 4a**)! Due to the delocalized nature of the individual atoms in a BEC, it can not be very well used for quantum information purposes. In one of the most influential publications in the field of ultracold atoms, however, Peter Zoller and his group in Innsbruck suggested already in 1998 (Jaksch et al., 1998) that one should be able to convert the weakly interacting Bose gas into the strongly interacting quantum state of a Mott insulator by increasing the optical lattice depth, such that the interactions between atoms on a single lattice site dominate over the kinetic energy. In such a Mott insulator, the atoms are however localized to single lattice sites, with exactly one atom per lattice site (see **Figure 4b**)! Such a state forms a perfectly initialized quantum register: all atoms are not only in identical internal states but also in the vibrational ground state of each lattice site. Thus an array of quantum bits all in a well defined initial logical state "0" is formed.

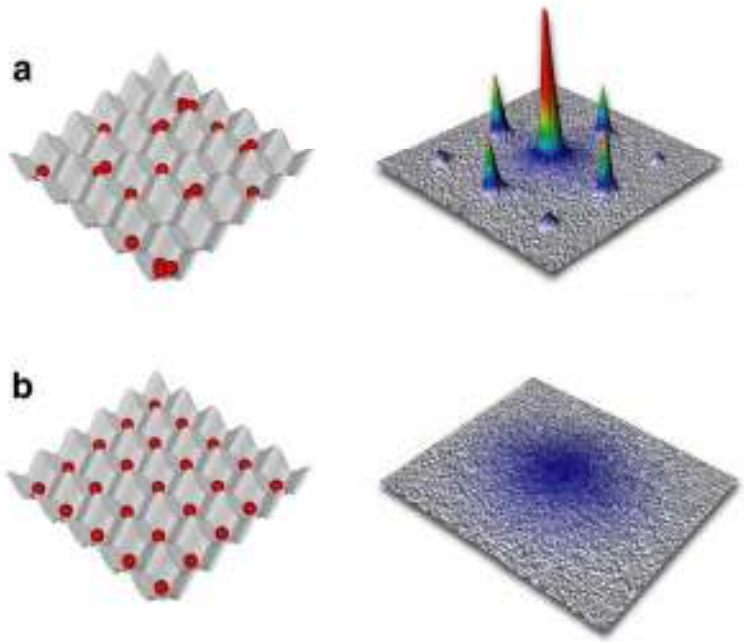


Figure 4(a): In the superfluid state of a Bose-Einstein condensate, the underlying atoms can be described as a giant macroscopic matter wave. When such a condensate is released from the periodic potential a multiple matter wave interference pattern is formed owing to the phase coherence between the atomic wavefunctions on different lattice sites. In this case the phase of the macroscopic matter wave is well defined. However, the atom number on each lattice site fluctuates. **Figure 4(b)**: In the other limit of a Mott insulating state of matter each lattice site is filled with a fixed number of atoms but the phase of the matter wave field remains uncertain. No matter wave interference can be seen in this case when the quantum gases are released from the lattice potential.

By exploiting the Mott transition it has now become experimentally possible to initialize a large set of up to 100000 qubits in a single experimental step (Greiner et al., 2002). But how can we realize quantum gates between atoms trapped on different lattice sites? Here Dieter Jaksch, Ignacio Cirac, and Peter Zoller, then at the University of Innsbruck had an ingenious idea: they proposed to use state dependent optical potentials in order to bring neighbouring atoms together on a single lattice site. Both atoms would undergo a collisional interaction which would result in a precisely defined phase shift of the two particle state. By setting this collisional phase shift to π, a quantum phase gate would then have been realized (Jaksch et al., 1999). One might think that using collisions for the delicate quantum control of two particles is not such a good idea, as collisions usually destroy the fragile coherence properties of quantum objects. However, in the ultracold temperature regime collisions are fully coherent processes and can indeed be used without destroying interference properties of the underlying quantum systems.

The idea on how to juggle atoms in a controlled way to their neighbours is based on state dependent lattice potentials. Here one again exploits the fact that atoms have internal magnetic substructure corresponding to a "red" ("0") and a "blue" ("1") state in **Figure 5**. By carefully controlling the polarization of the lattice laser fields one can arrange that both internal states experience different lattice potentials such that they can be moved relative to each other. Let us imagine that some atoms in the lattice, initially in the red state, are converted into blue atoms. These blue atoms can now be moved relative to the red atoms and brought into contact with other red atoms in the lattice by moving the blue lattice potentials relative to the red lattice potential (see **Figure 6**). By perfectly controlling such lattice displacements it is possible to move the atoms over a precisely defined separation and to distant neighbour atoms.

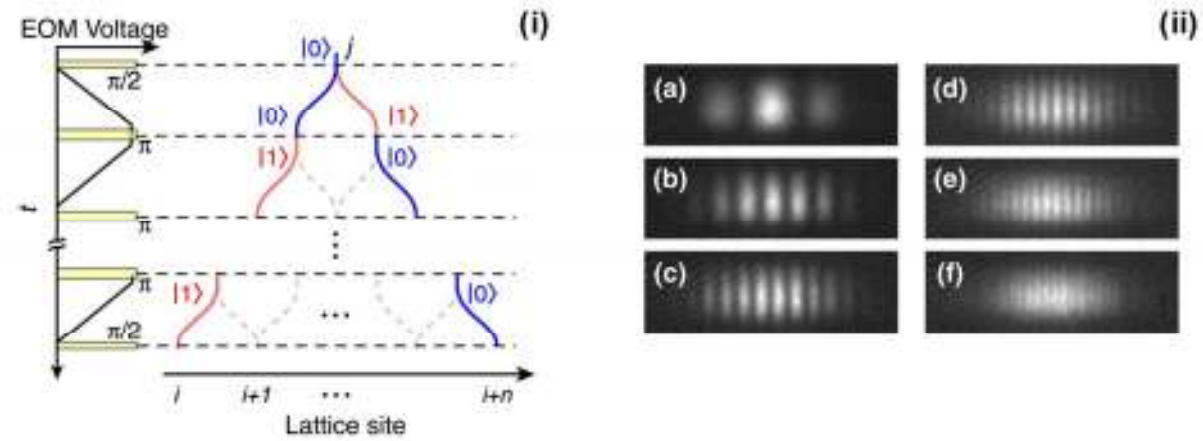


Figure 5(i): Schematic sequence used for the quantum conveyer belt. A single atom on lattice site j can be transported over an arbitrary number of lattice sites depending on its spin state (marked as blue and red curves). **Figure 5(ii)**: This has allowed us to split the wave function of the atom in a coherent way, such that a single atom simultaneously moves to the left and to the right. The coherence of the split wave-packets has been demonstrated in an interference experiment. For larger distances between the split wave-functions, the period of the interference pattern decreases.

These controlled interactions have allowed a novel degree of control over the atoms in the system. For the first time one can completely control the interaction between two atoms that would otherwise have never interacted (Mandel et al., 2003). The periodic structure of the potential that the atoms experience in an optical lattice furthermore has a powerful parallelism built into it. With just a single lattice displacement operation one can bring each atom into

contact with its neighboring atom, thereby realizing a powerful quantum gate array (see **Figure 6**). Such quantum gate arrays are very useful for generating highly entangled many body states. In a modern view such highly entangled multi-particle states can be seen as a resource for quantum information processing and are therefore not only of fundamental but also of practical interest.

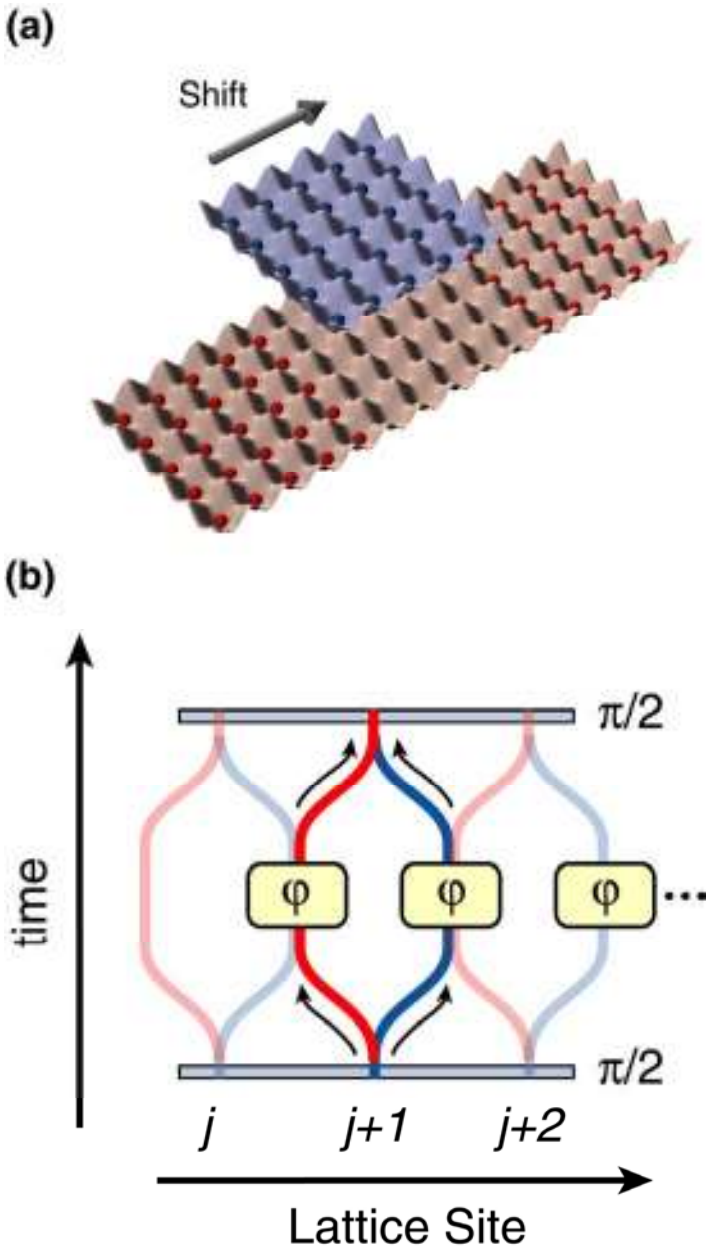


Figure 6(a): Controlled interactions between atoms on different lattice sites can be realized with the help of spin-dependent lattice potentials. In such spin dependent potentials, atoms in a, let us say, blue internal state experience a different lattice potential than atoms in a red internal state. These lattices can be moved relative to each other such that two initially separated atoms can be brought into controlled contact with each other. **Figure 6(b):** This can be extended to form a massively parallel quantum gate array. Consider a string of atoms on different lattice sites. First the atoms are placed in a coherent superposition of the two internal states (red and blue). Then spin dependent potentials are used to split each atom such that it simultaneously moves to the right and to the left and is brought into contact with the neighbouring atoms. There both atoms interact and a controlled phase shift φ is introduced. After such a controlled collision the atoms are again moved back to their original lattice sites.

One great challenge in using ultracold atoms in optical lattices for quantum information remains how to address single atoms on different lattice sites. Recently Dieter Meschede and his group in Bonn have shown that by using magnetic field gradients it is possible to select single atoms separated by a few lattice sites and it remains to be seen whether such an advanced level of control can be extended to the quantum register of a Mott insulator. Other possibilities to address single atoms are currently pursued by the group of William D. Phillips at NIST (USA). In one of their experiments his group has been able to achieve a patterned loading of an optical lattice in which only every third lattice site is filled with atoms. The increased distance between the atoms should then allow one to optically focus a laser beam to a single filled lattice site in order to manipulate the atoms therein. A second approach currently pursued by his group consists in dynamically changing the spacing of the lattice by controlling the angle under which the laser beams interfere. In such an "accordion lattice" one can quickly change from a small lattice spacing to a large lattice spacing configuration to address the atoms in the lattice. A different approach is based on the continuous use of a lattice with a larger spacing, in the 3-5 ∝m range, as produced by laser beams interfering at an angle. The large lattice spacing allows optical excitation of individual lattice sites, and also ionization of the atoms and detection with high efficiency of the ions to probe the quantum computation output.

Outlook

Neutral atom quantum computing schemes, introduced theoretically not long ago, are now implemented in experiments on optical lattices. Further schemes have been suggested, including excitation of Rydberg interactions to implement fast two-bit quantum gates, and a regime of "dipole blockade" to drive the atomic system into single excited collective atomic states (Jaksch et al., 2000).

In a lattice the nearest neighbor interactions can be efficiently controlled. Thus neutral atom lattice systems are ideally suited to generate so called quantum simulators in order to physically realize and analyze theoretical models of many particle physics over a wide range of parameters which cannot be investigated with current mathematical tools and classical computational resources.

The possibility to create a quantum register with fermionic atoms in an optical lattice has recently received some attention both theoretically and experimentally, and the number of experiments with fermions in optical lattices is rapidly increasing. Fermion particles obeying the Pauli exclusion principle cannot be located at the same position in space and with the same energy, Because when loaded into an optical lattices they are ‚naturally' spread owing to different lattice sites, fermions represent an alternative route to the creation of atomic qu-bits within an optical lattice.

Conclusions

The process of taming and engineering the quantum world has been highly successful at the level of single auntum objects or simple pair systems. The great promise for quantum coherent manipulation lies in systems composed fo several or even many subsystems. The scalability of the physical systems is now becoming a central issue.

In order to achieve scalability systems must satisfy to partly conflicting conditions: They must be composed of many subsystems which can be manipulated individually. Simultaneously quantum coherence must be maintained throughout the whole system.

Systems composed of neutral atoms are highly promising candidates to approach such goals: We can already control medium scale 1D lattices of atoms at the individual particle level, while at large scales massive entanglement generation has been demonstrated for 2D and 3D neutral atom lattices. Bringing these worlds together promises to open the route towards testing concepts for large scale entanglement and gaining insight into the question how growing complexity affects quantum correlations of the multi-particle system. If we succeed we have come significantly closer to Richard Feynman's vision of simple quantum simulators.

References

[1] GREINER, M., MANDEL, O., ESSLINGER, T., HÄNSCH, T. W. & BLOCH, I. (2002) Quantum phase transition from a superfluid to a Mott insulator in a gas of ultracold atoms. *Nature,* 415**,** 39-44

[2] JAKSCH, D., BRIEGEL, H. J., CIRAC, J. I., GARDINER, C. W. & ZOLLER, P. (1999) Entanglement of atoms via cold controlled collisions. *Phys. Rev. Lett.,* 82**,** 1975-1978

[3] JAKSCH, D., BRUDER, C., CIRAC, J. I., GARDINER, C. W. & ZOLLER, P. (1998) Cold Bosonic Atoms in Optical Lattices. *Phys. Rev. Lett.,* 81**,** 3108-3111

[4] JAKSCH, D., CIRAC, J. I., ZOLLER, P., ROLSTON, S. L., COTE, R. & LUKIN, M. D. (2000) Fast quantum gates for neutral atoms. *Phys. Rev. Lett.,* 85**,** 2208-2211

[5] MANDEL, O., GREINER, M., WIDERA, A., ROM, T., HÄNSCH, T. W. & BLOCH, I. (2003) Controlled Collisions for Multiparticle Entanglement of Optically Trapped Atoms. *Nature,* 425**,** 937

[6] SCHRADER, D., DOTSENKO, I., KHUDAVERDYAN, M., MIROSHNYCHENKO, Y., RAUSCHENBEUTEL, A. & MESCHEDE, D. (2004) Neutral Atom Quantum Register. *Phys. Rev. Lett.,* 93**,** 150501

Projects funded by the European Commission and related to the work in this article:

QGates
Quantum Gates and Elementary Scalable Processors Using Deterministically Addressed Atoms
Start date:01/01/2003
End date: 31/12/2005
Project web site: http://www.imperial.ac.uk/physics/qgates/
Contact person: Peter Knight, p.knight@ic.ac.uk

QUASICOMBS
Quantum Simulator for Strongly Correlated Many Body Systems
Start date: 1/4/2004
End date: 31/3/2008
Project web site: www.physik.uni-mainz.de/quantum
Contact Person: Immanuel Bloch

NANOCOLD
Nanodeposition of active ordered structures by cold atom technologies
Start date: 1/1/2001
End date: 31/12/2004
Project web site: nanocold.df.unipi.it
Contact Person: Ennio Arimondo

OLAQUI
Optical LAttices and Quantum Information
Start date: 1/2/2005
End date: 31/1/2008
Project web site http://olaqui.df.unipi.it
Contact Person: Ennio Arimondo

Projects funded by National initiatives or organizations and related to the work in this article:
QIV
Quanteninformationsverarbeitung
Start date: 1/4/1999
End date: 31/3/2005
Project web site http://kerr.physik.uni-erlangen.de/qiv/
Contact Person: Gerd Leuchs

Contact information of the authors of this article:

Ennio Arimondo
Dipartimento di Fisica E. Fermi
Universitá di Pisa
Largo Pontecorvo n. 3
Pisa
Italy
Email: arimondo@df.unipi.it
Web page: www.df.unipi.it/gruppi/struttura/index.htm

Immanuel Bloch
Institut für Physik
Johannes Gutenberg-University
Staudingerweg 7
55128 Mainz
Germany
Email: bloch@uni-mainz.de
Web page: http://www.physik.uni-mainz.de/quantum/bec/index.html

Dieter Meschede
Institut für Angewandte Physik
Universität Bonn
Wegelerstrasse 8
53115 Bonn
Germany
Email: meschede@iap.uni-bonn.de
Web page: www.iap.uni-bonn.de/ag_meschede/english/index_eng.html

Superconducting qubits: quantum mechanics by fabrication

Hans Mooij
Hans Mooij is professor at the Kavli Institute of Nanoscience, Delft University of Technology, The Netherlands. He is also the director of the Kavli Institute. His research interests include: mesoscopic effects in nanofabricated structures and quantum properties of superconducting circuits. He is a member of the following EU-funded IST projects: SQUBIT and SQUBIT2. He received the Agilent Technologies Europhysics Prize 2004 with Nakamura (Japan), and SQUBIT partners Devoret and Esteve.

Abstract
Superconducting qubits are quantum two level systems that are fabricated with the tools of semiconductor chip technology. Because they are made of superconducting material their coherence is high. At this time single qubits of different types have been fabricated and studied, as well as two coupled qubits. They behave as true quantum bits over times as long as 4 microseconds, while the basic operations can be performed in less than a thousandth of a microsecond. The contribution to superconducting qubit research is relatively very high from Europe.

Introduction
To build the large quantum computer of the future, it seems obvious to start with particles that have long-proven quantum properties, such as atoms. They are by nature well-isolated units with properties that are almost not influenced by the outside world. However, this also means that their mutual interaction is weak and completely new techniques are required to control many thousands of them. The ordinary computers that we all use contain billions of solid state devices. If one could fabricate qubits with the same technology, integration to large numbers would be relatively easy. Ten years ago, it was hard to imagine that such fabricated quantum particles could exist. Now, superconducting circuits as pictured (**Figure 1**) can be driven in the same way as the spins in an MRI-scan. Research groups in Europe, supported by the European Union in the Future and Emerging Technology program (projects SQUBIT and SQUBIT2), have been instrumental in this development.

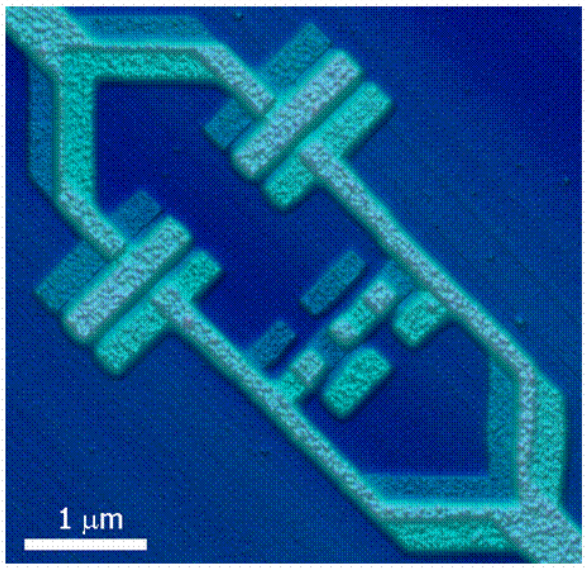


Figure 1

We all take for granted that quantum mechanics must be used to describe quarks, electrons, atoms and molecules. Why does it stop there? Why not use the Schrödinger wave equations to describe a virus or an elephant? All matter is subjected to the rules of quantum mechanics, but in large objects the wave description of the multitude of constituent particles loses relevance. There is a close analogy with light. When a second light bulb is switched on in a room, the average amplitude of the light waves is not doubled, only the power. The light waves from the hot wires are not coherent, they do not have exactly the same frequency and phase. With two laser beams one can double the amplitude, because laser light is coherent. Something similar is possible with quantum mechanics of large objects. In recent years we have discovered that individual micrometer-sized objects, which have been fabricated with the tools for semiconductor chip technology, do behave as coherent quantum particles. These artificial quantum objects are very promising as quantum bits for a quantum computer, because their properties can be designed and tooled. They can be fabricated in very large numbers on a chip. To obtain the essential coherence, the objects are fabricated from superconducting material. Superconductivity is the state that occurs in many metals when they are cooled down to very low temperatures.

Superconductivity

In a superconductor, the electrons are condensed into one single collective fluid. In ordinary metals or semiconductors all electrons occupy their own quantum state, of which there are millions in a small transistor. Quantum mechanics is needed to understand the average electrical and thermal properties, but the detailed control of each state that is necessary for quantum computing can only be realized when a few electrons are isolated from the others and addressed individually. In superconductors, all electrons are described with one single quantum state. A significant amount of energy is needed for an electron to escape from this collective fluid, so the single state is quite robust. The consequence is that an electrical current can flow through the metal without friction, no energy or information is transferred to the crystal lattice. This is the ideal starting point for a solid state quantum bit. To explain these superconducting qubits, a

short discussion of some elements of the theoretical description of superconductivity is needed.

In superconductors, the electrons form pairs which are called Cooper pairs and which have double the charge of single electrons. The pairs are described with a quantum wave function. An ordinary wave has an amplitude (the maximum height of the wave) and a phase (where is the wave at what time). The amplitude of the superconducting wave function determines the number of pairs, the way the phase changes in space determines the current. As the pairs have an electrical charge, the phase is also intimately connected with the magnetic field. The quantum nature of superconductors leads to the fact that it is impossible to determine both the number of Cooper pairs and the phase accurately at the same time, in analogy with the better known Heisenberg relation for a quantum mechanical particle that says that a very accurate measurement of the velocity leads to uncertainty in its position and vice versa.

Integrated semiconductor circuits have transistors, for superconducting electronics one uses devices that are called Josephson junctions. A Josephson junction consists of two parallel metal thin films that are separated by a very thin insulator. In superconducting qubits the junctions are usually made of aluminium, with aluminium oxide as the insulator. The oxide is so thin that electrons and Cooper pairs can cross through it, in a process that is itself quantum mechanical and is called tunnelling. The Josephson tunnel junction provides a weak coupling between the two superconducting films. The engineer of superconducting electronics chooses the overlapping area of the two films and the oxide thickness to obtain the needed coupling strength. This strength is expressed as energy, the Josephson energy. The maximum current that can pass through the junction without voltage is proportional to the Josephson energy. For quantum circuits, another energy is equally important. This is the energy of the electric field in the junction when one Cooper pair is moved across the insulator from one metal electrode to the other, called the charging energy. It can be ignored in large junctions. However, in junctions that are smaller than one ten-thousandth of a millimetre a significant voltage has to be applied across the junction to provide the energy for a Cooper pair to cross the insulator. The different types of superconducting qubit are best distinguished with the relevant strength of the two energy terms.

Superconducting qubits

A good recent review of superconducting qubits is provided by reference 1. The charge qubit uses the charging energy to define its two states, while the smaller Josephson energy provides the transfer between them. The charge qubit consists of a small superconducting volume called the Cooper pair box that is connected to the circuit by a Josephson junction. First studies of Cooper pair boxes were performed by the Quantronics group at the CEA in Saclay, with support from the European Union [2]. A voltage applied to a nearby gate influences the energy of the charges on the box (**Figure 2**). For zero gate voltage, the lowest energy is found with no electrical charge. For a specific value of the gate voltage, typically a millivolt, the box has its lowest energy when it is charged with one Cooper pair. In between, there is a value where the energy values with zero and with one pair are equal. The qubit is used in the regime near this symmetry point. Because the Josephson tunnelling provides a connection between the two charge states, two new superposition states are formed. Each superposition is a well-defined combination of the charge states. At the symmetry value of the gate

voltage, the energy values of the superposition states are different by twice the Josephson energy. The qubit in equilibrium occupies the superposition state with the lowest energy, the ground state. It can be excited to the higher energy state by the application of an AC microwave voltage to the gate, with a frequency that exactly corresponds to the energy difference. It is also possible to create superpositions of the qubit states, in the same way as with spins in nuclear magnetic resonance (NMR). In particular when a measurement is performed, one must remember that the qubit states themselves are well-known superpositions of the charge states. Measurement can be performed by measuring the electrical charge on the Cooper pair with a small on-chip measuring instrument. Such an electrometer has been developed at Chalmers University in Sweden [3]. Other measurement techniques are possible. The first time that coherent dynamics were observed in a charge qubit was at NEC in Japan.

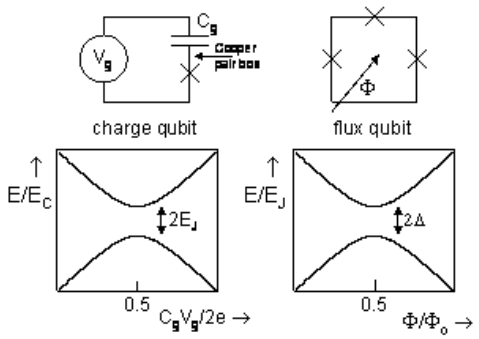


Figure 2

The flux qubit uses the opposite regime where the Josephson energy is significantly larger than the charging energy. The phase of the superconducting wave function is now more important than the charge. When the phase varies along the loop, a superconducting current is present. When the whole loop is traversed, the phase has to come back to its original value, or may be different by an integer number times 2π. In a superconducting loop, a different value of the total phase change is connected with a different circulating current. For zero magnetic flux (the magnetic field times the area) through the loop, the lowest energy is obtained for a phase change zero and with zero current. When the flux through the loop is equal to the superconducting flux quantum (Planck's constant divided by the Cooper pair charge 2e), the lowest energy is found when the phase change is 2π. There is a close analogy with the charging energy, the magnetic flux taking the role of the gate voltage. A unit 2π of phase change is called a fluxoid. At a value of the flux equal to half a flux quantum, the states with and without a fluxoid have equal energies. The flux qubit is operated in this neighbourhood. To obtain quantum tunnelling between the fluxoid states, the Josephson energy should be not too large and the charging energy not too small. The two fluxoid states have opposite circulating current through the loop [4]. The previous discussion shows that there is a large simularity between charge and flux qubits, they are in fact each other's dual.

A very inventive extension to the charge qubit was developed by the group in Saclay [5]. The principle is indicated in **Figure 3**. The Cooper pair box has two parallel junctions and it can be calculated that the states with and without one Cooper pair have currents flowing through these two junctions with opposite direction. It is easier to detect this current than to measure the charge directly. Fine-tuning is possible by variation of the magnetic flux through the small loop. For practical reasons that have to

do with material properties, it seems unlikely that the pure charge qubit can be used for large circuits. Scaling up to large numbers of qubits is possible with the quantronium.

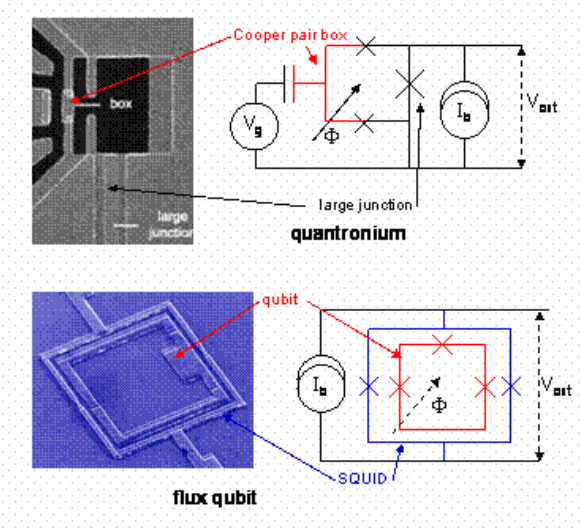


Figure 3

Another type of superconducting qubit, called the phase qubit, was developed by a number of groups in the United States, the group at NIST having the most developed results. This qubit employs a single Josephson junction with a large value of the Josephson energy, but the effective strength is reduced by a strong bias current close to the maximum value. With the junction acting as an inductor, an oscillation occurs which provides the qubit states. No significant work on this type of qubit is performed in Europe.

Present status

In the last few years progress has been fast in superconducting qubits, with essential contributions from a large number of European groups. In fact, more than half of the total work in the world comes from Europe. An example of coherent oscillations between qubit states is shown in **Figure 4**. Charge qubits are studied experimentally in Sweden (Chalmers University) and Germany (PTB Braunschweig). The quantronium continues to be developed at Saclay with beautiful and very promising results. Coherence times of more than 500 nanoseconds are obtained. Detailed control of one qubit has been demonstrated, using well-known sequences of microwave pulses as developed over many years for nuclear magnetic resonance [6]. An example is shown in **Figure 5**. The next step will be the study of two qubits.

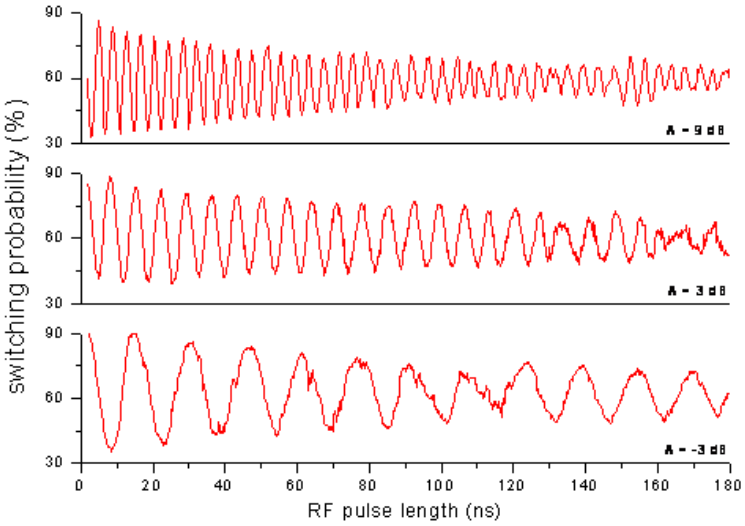


Figure 4

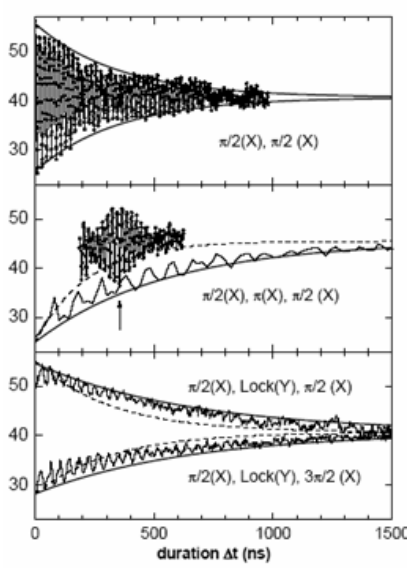


Figure 5

For flux qubits, the major contributions on the world scale have come from Europe, although clear activity is also present in the United States and Japan. Single qubits are now well-controlled and attention is moving towards multi-qubit systems. In Jena University in Germany, a spectroscopic technique was used to observe the behaviour of two interacting flux qubits [7]. At Delft University, The Netherlands, coherent dynamics of single and double flux qubits has been obtained. Coherence times are of the order of 400 nanoseconds, but with special compensation techniques have been increased to 4 microseconds. Qubit operations can be performed in a fraction of a nanosecond. The combination of a single flux qubit with a quantum oscillator was also brought to coherent time-evolution [8]. A picture of a 2-qubit sample is shown in **Figure 6**.

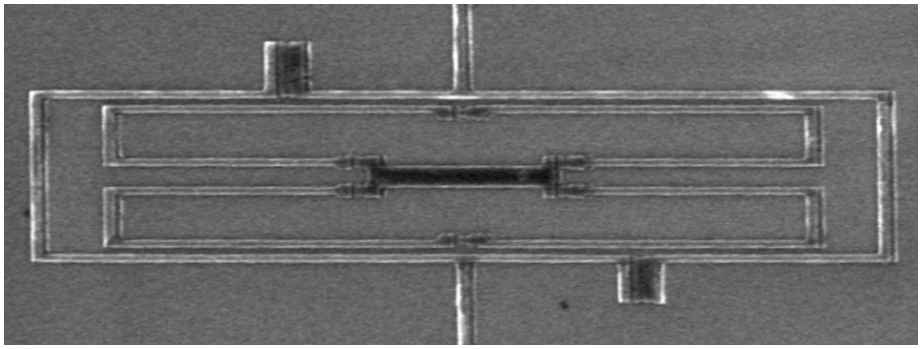


Figure 6

Five years ago, it was supposed by many that decoherence would be too strong in superconducting qubits for them to become practical. It remains a significant factor, but steady progress is made. Decoherence means that quantum information leaks out to uncontrolled degrees of freedom. The measurement circuit is one definite source of decoherence, but thanks to strong contributions from theoretical groups this problem is well understood. The connecting circuits can be designed in such a way that the relaxation and dephasing rates are long enough to allow 100000 operations. Theory groups in Europe have been leading the world in this area. Theory groups in Germany (Karlsruhe, Munich, and Regensburg) and Italy (Catania, Pisa) are to be mentioned specially. Unfortunately, there are other processes that induce decoherence. They are connected with microscopic materials defects in the insulating barriers of the tunnel junctions, that are unstable in time. Materials research is needed to improve the quality of fabrication. It is possible to fabricate superconducting films with perfect crystal structure and very homogeneous oxide, but it is still difficult to make the small junctions in this way. More work is needed.

Apart from the mentioned groups, in a number of places in Europe general technology for superconducting quantum electronics is developed and new effects are studied. In this context, groups in Finland (Jyvaskyla and Helsinki) are important. In Grenoble, France, a special quantum system with an integrated oscillator is studied, that may well lead to a new type of qubit. All groups collaborate and exchange information on a very regular basis through the European projects SQUBIT and SQUBIT2, in the 5th and 6th Framework respectively.

Prospects

Superconducting qubits are catching up with such established quantum physics fields as nuclear magnetic resonance and atom physics. The promise of scalability to large numbers of qubits is fully present for the superconducting technology, using semiconductor fabrication techniques. Among the solid state quantum systems, superconductors are clearly ahead in achieving coherent quantum dynamics. No insurmountable barrier for further progress is in sight.

Conclusions

Superconducting qubits have been developed that perform the basic operations for a quantum computer. More work is needed, but the present results indicate that the

understanding of the systems is sound and that there is no principal problem to build a large quantum computer based on this type of qubit.

The operation times of superconducting qubits is of order 1 nanosecond, the coherence times are at this time around several microseconds. Coherence is still limited by materials defects and optimization of junction fabrication needs to be performed.

References

[1] M.H. Devoret, A. Walraff, J.M. Martinis, to be published ; arXiv :cond-mat/0411174
[2] V. Bouchiat, D. Vion, P. Joyez,, D. Esteve, M.H. Devoret, Physica Scripta T**76**, 165 (1998)
[3] T. Duty, D. Gunnarsson, K. Bladh, P. Delsing, Phys.Rev. B**69**, 140503 (2004)
[4] J.E. Mooij, T.P. Orlando, L.Levitov, Lin Tian, C.H. van der Wal, S. Lloyd, Science **285**, 1036 (1999)
[5] D. Vion, A. Aassime, A. Cottet, P. Joyez, H. Pothier, C. Urbina, D. Esteve, M.H. Devoret, Science **296**, 286 (2002)
[6] E. Collin, G. Ithier, A. aassime, P. Joyez, D. Vion, D. Esteve, to be published in Phys.Rev.Letters, arXiv :cond-mat/0404503
[7] A. Izmalkov et al., Phys.Rev.Letters **93**, 037003 (2004)
[8] I. Chiorescu, Y. Nakamura, C.J.P.M. Harmans, J.E. Mooij, Science **299**, 1869 (2004)

Projects funded by the European Commission and related to the work in this article:

SQUBIT2
Superconducting Qubits: Quantum Computing with Josephson Junctions
Start date: 01/01/2004
End date: 01/01/2007
Contact Person: Goran Wendin, Chalmers University Sweden, goran.wendin@mc2.chalmers.se

Projects funded by National initiatives or organizations and related to the work in this article:

FOM Concentration Group Quantum Information Processing
Start date: 01/06/2004
End date: 01/06/2012
Contact Person: Leo Kouwenhoven, Leo@qt.tn.tudelft.nl

NanoNed Flagship Quantum Computing
Start date: 01/01/2005
End date: 01/01/2010
Web site: http://www.stw.nl/nanoned/
Contact person: Hans Mooij, Mooij@qt.tn.tudelft.nl

Contact information of the author of this article:
Hans Mooij
Kavli Institute of Nanoscience
Delft University of Technology
Lorentzweg 1
2628 CJ
Delft
The Netherlands
Email: j.e.mooij@tnw.tudelft.nl

Quantum information processing in carbon

Jason Twamley
Jason Twamley is Senior Lecturer in the Department of Mathematical Physics at the National University of Ireland in Maynooth, Ireland (www.nuim.ie). His research interests include: decoherence, quantum control, physical implementations of quantum processors. He is the coordinator of the following EU-funded IST projects: QIPDDF, IST-1999-11617 and QIPDDF-ROSES IST-2001-37150. He is the recipient of the Science Foundation Ireland Research Award with Prof. C. Wunderlich for quantum information processing using trapped ion spin–molecules (~3MEuros). For the past three years, Dr. Twamley has been acting as the Dean of Research and Graduate Studies for the National University of Ireland, Maynooth.

Jörg Wrachtrup
Jörg Wrachtrup is a professor at the Institute of Physics, University of Stuttgart, Germany. His primary research interest lies in the field of optical investigation of single quantum systems in solids and biophysics. Since the start of 2000 he is full professor at the Universität Stuttgart where he is the director of the "3. Physikalisches Institut". His research work has been rewarded with several prizes, including the Ernst-Reuter-Preis (1995, FU Berlin, Dissertationspreis), the Gustav-Hertz-Preis (1996, Deutschen Physikalischen Gesellschaf).

Abstract
We outline the recent advances in carbon-based quantum computer technology. This includes nanotube based, fullerene based and Diamond based quantum computer technologies.

Introduction

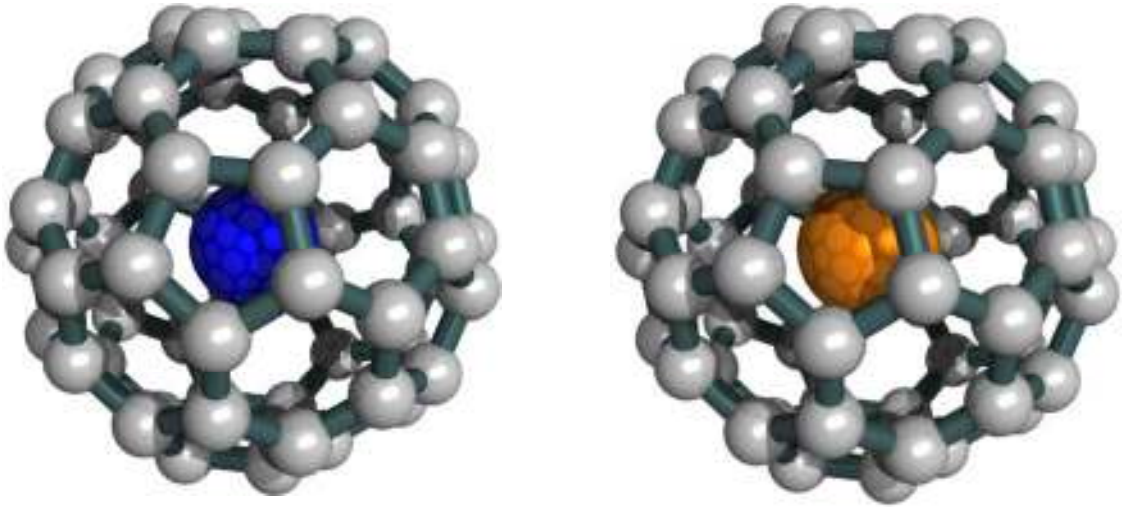
A room-temperature solid-state technology represents the "holy grail", in the search for a viable, scalable technology for quantum information processing (QIP). Until recently, achieving such a goal might have seemed "science fiction", but the recent achievements of a number of researchers (some FET funded and some non-FET funded), in the area of carbon-based QIP have prompted a serious rethink and indications are that this fledgling niche area of QIP research (carbon-based technologies), has the potential to exceed many expectations.

Solid-state QIP technologies are mostly based on existing technologies: superconducting circuits, quantum dots, semiconductor heterostructures, doped Silicon devices, etc. Of course, to achieve the technological advances required to perform QIP, such existent technologies need major developments and these are underway. These developments are aided by the (sometimes), enormous banks of knowledge that already exists with respect to these technologies and materials. One avenue of QIP research which does not benefit from such a preexistence of expertise but despite this, is making very rapid progress, i.e. the black-sheep of QIP technologies, are those technologies based on carbon. These carbon-based QIP proto-technologies include: nanotube materials where quantum spin-dots/qubit are located in the nanotube wall itself, nanotubes which enclose electron spin/qubit carrying molecules, individual fullerene (or Buckyball) molecules which are altered to encapsulate electron spin/qubits and finally bulk carbon (in the form of Diamond), which is engineered to contain electron spin/qubits within special defects of the Diamond lattice known as Nitrogen-Vacancy defects. In this article we will focus primarily on the last two of the above, the Buckyball molecules (C60), which have been altered to encapsulate a single Nitrogen or Phosphorous atom and the Nitrogen-Vacancy (NV), defect in Diamond.

Buckyball Qubits

Buckyballs are the common name given to a very special type of carbon molecule discovered in 1985 by Robert Curl, Harold Kroto and Richard Smalley Harry Kroto, who were awarded the Nobel Prize in chemistry for their work in 1996. The molecule contains sixty carbon atoms all connected together like a round soccer ball (**Figure 1/ Subfigures Figure 1a and Figure 1b**). In 1997, researchers at Berlin's Hahn-Meitner-Institute (HMI), accidentally discovered that Buckyballs could be formed around atomic Nitrogen and later on, around atomic Phosphorous [2] (shorthand N@C60 or P@C60). This interesting molecule was reported in the literature and preliminary investigations by Alois Weidinger and his colleagues at HMI into its structure indicated that it possessed unpaired electrons and that (most unusually), the Electron-Spin-Resonance signal indicated that the trapped Nitrogen atom was not interacting chemically with the sixty carbon atoms of the Buckyball cage. It appeared that this molecule was acting as a nanoscopic (diameter of 1nanometer), neutral atom trap for the Nitrogen atom! In 1999-2000, the European Future and Emerging Technologies programme launched it's proactive call for research into Quantum Information Processing and Communication and J. Twamley put forward the plan of examining these types of Buckyballs as potential elements in a quantum information processor. The research plan was ideally suited to the FET proactive programme, as although the basis for the ideas were sound enough, the research was high-risk, long-term and the research team was spread over many nations within the EC. This latter aspect was necessary as the expertise to tackle the question just did not exist in a single country. The research was funded by the FET and the two-year project [QIPDDF], produced valuable milestones such as the proposed use of the magnetic dipole interaction to coupled neighboring molecules [3], a quantum computer design using the material with individually addressed qubits [4], and a design without using individually addressed qubits [5]. The research also told us much more about this unusual

material which we will summarise below. Another vital element of performing research via European Union programmes is the ability to meet new colleagues and to form new and long-lasting research collaborations and the FET QIPC Conference meeting in 2001 in Torino, Itlay brought together many of the partners which make up a more recent FET project focused on developing a readout technique to determine the electronic spin state of a single N@C60 molecule. This project, QIPDDF-ROSES, has also produced a number of milestone discoveries such as the execution of a two-qubit gate in Diamond [5], improved synthesis techniques to yield 100% pure Buckyball materials, evidence that the NV-Diamond system can coupled to the Buckyballs via magnetic dipole interactions and the performance of detailed quantum control of the NV-Diamond system via the execution of Quantum Process Tomography. ***Without the FET programme, the "black sheep" concept of utilizing the trapped spin system within a Buckyball would not have been examined.*** The potential use of this system as evidenced by the results of the original FET project QIPDDF, has expanded and now this material is being studied by a number of other research consortia all over the world for use in quantum information processing and otherwise.



(a) (b)

Figure1: Schematic diagram of doped Buckyballs, (a) Nitrogen in C60 or N@C60 and, (b) Phosphorus in C60 or P@C60.

As a means of categorizing the current status of development of Buckyball mediated QIP let us follow roughly the first five DiVincenzo criteria for a physical implementation of QIP technology [6]. These are that one must: (DiV 1) have a well defined extendible qubit array, (DiV 2) be able to initialize the qubit array into a known state, e.g. the "00000…" state, (DiV 3) the quantum information must survive in this array for a long time compared to the duration needed to execute a quantum gate, i.e. long decoherence times ($>10^4$ gate operation times), (DiV4) be able to have enough control over the qubit array to execute the basic universal set of quantum computer operations, and finally (DiV 5), be able to read out the state of the qubit array at the end of the computation.

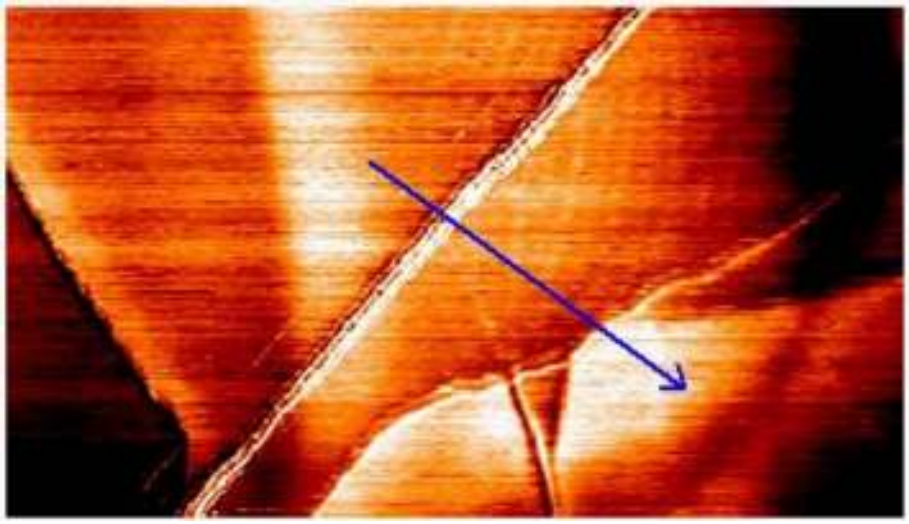


Figure 2: Scanning Tunneling Microscope (STM) image of rigid self-assembled Buckyball wire. Wire is several Buckyballs thick but can be rigidly pushed across the substrate in the arrow direction by the STM tip.

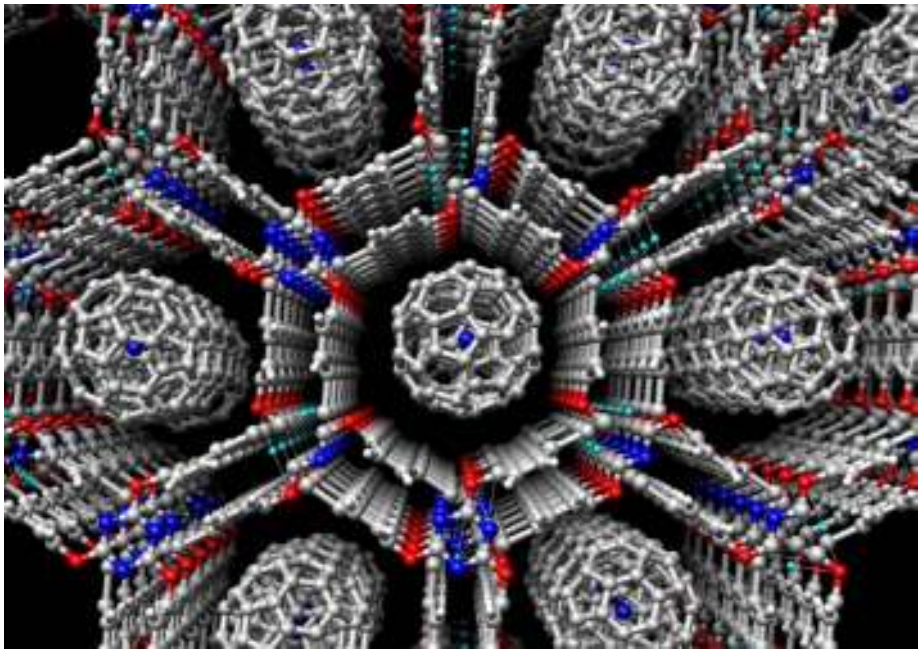


Figure 3: Schematic of experimentally self-assembled molecular tubes of doped Buckyballs.

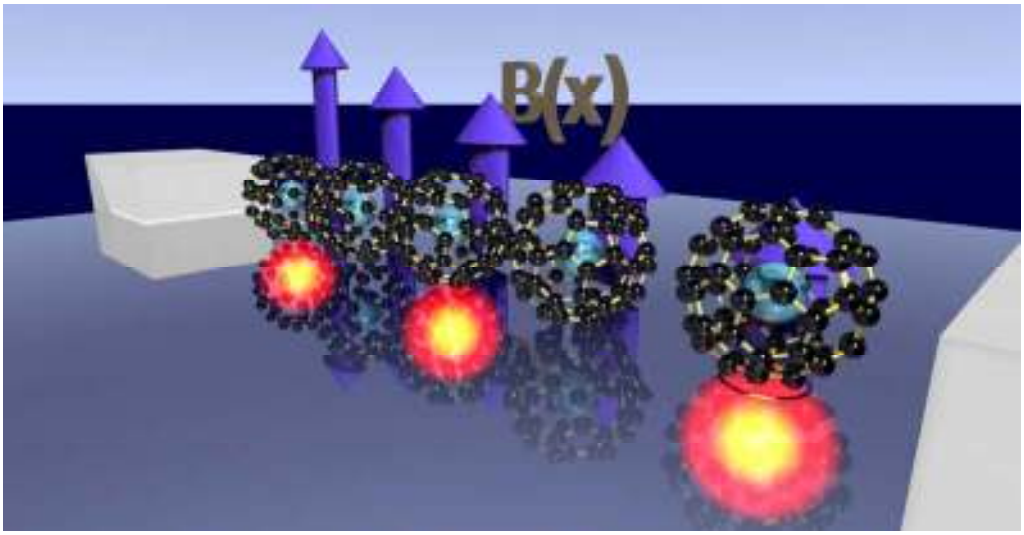


Figure 4: Schematic of theoretical Buckyball processor device consisting of a linear array of Buckyballs on Diamond between two current carrying wires with Nitrogen-Vacancy defects in the Diamond registered below specific Buckyballs in the array. The current though the wires creates a magnetic field gradient (B(x)), along the molecular array. The NV defects act as the optical inputs & outputs to the processor.

DiV 1 (*qubit array*): it is now possible to produce 100% pure Nitrogen or Phosphorous Buckyball material. We now know that each of these molecules contains a very well defined spin system and thus can contain a qubit. Thus the hard work of mechanically isolating an individual qubit has been done already via "chemical" means, one molecule = one qubit. We understand well that engineering via a top-down approach on nanoscale dimensions is incredibly tough but the use of carbon-based qubit materials allows fantastic bottom-up self-assembly chemical techniques to be used. This allows individual Buckyball wires to be fashioned (**Figure 2**), while huge numbers of parallel identical Buckyball wires can be fashioned quickly via self-assembly (**Figure 3**). One possible quantum processor design is shown in (**Figure 4**), and this will require the fabrication of a linear array of molecules, then registered with a few metal wires and buried NV readout systems.

DiV 2: (*initialize the qubit array):* Initializing these molecules to a known state will be possible once a readout system has been developed.

DiV 3: (*long decoherence time):* The trapped electron spin decoherence properties are, undisputedly, the single most astonishing property of these Buckyball materials. The dephasing time (or T_2), for the trapped Buckyball electrons has been measured to be at least 250microseconds, though this is at low temperature. This feature was already hinted at in the original Electron-Spin-Resonance experiments of [1], and this time may prove to actually be much longer as our measurements grow more sensitive. Theoretically, however, with such an enormously long lifetime for the trapped quantum information, we should be able to perform $\sim 10^4$ quantum gate operations, matching trapped ion quantum information processor designs. It is quite possible that these Buckyball materials possess the longest lived electron coherence times outside a crystal defect structure and although we have some insights as to why this is, the complete story regarding their long-lived electron states have yet to be fully understood.

DiV 4: (*execute quantum computer operations):* Two separate designs for a quantum processor have been developed. The first one [3], uses currents flowing thru small wires to

generate a large magnetic field gradient which will cause each of the spin systems in the molecules to possess different resonant frequencies. One can then apply microwave radiation pulses to the entire processor at the appropriate frequency to address a single specific molecule. Each molecule is separated from its neighbor by <10 nanometers and they interact via magnetic dipole coupling. The second design [4], uses an alternating array of P@C60-N@C60-P@C60… with no magnetic field gradient to perform quantum cellular automata quantum information processing. Here one addresses many molecules at once but by having two molecule types in the linear array one has enough flexibility to perform full blown quantum computation.

DiV 5: (*qubit readout*): This is the most challenging obstacle towards using these molecules as components in a solid-state quantum information processing device. No technology to-date can determine the spin-state of the electrons trapped within an individual Buckyball. Developing such a technology has been the sole focus of the recent FET QIPC project QIPDDF-ROSES. Among various possible candidates, buried Nitrogen-Vacancy defects in Diamond coupled magnetically to the Buckyballs have shown to be very possible. The NV-defect system will allow a fast ***optical readout and reset*** of quantum information stored in the Buckyball array. The quantum information will then be manipulated via microwave pulses. Towards this end we have studied the NV-defects themselves as we will have to be able to manipulate the readout systems with great precision. By making use of techniques from single molecule spectroscopy and optically detected magnetic resonance we have been able to find NV-defects with nearby ^{13}C atoms. We have then been able to execute a two-spin quantum gate coupling the electron spins of the NV-defect to the nuclear spin of the ^{13}C (see more below). Over the past year, though international collaborations, we have been developing NV-defect Diamond synthesis techniques that have produced ultra-pure samples. Such samples, like the Buckyballs, have extremely long decoherence times (>300 microseconds), but amazingly, at **room temperature.** Top-down techniques to implant NV-defects with nanometer resolution are under intense development but, as visualized in **Figure 4**, the spacing of NV-readout systems might not need to be so small and a combination of top-down fabrication of the NV-readouts coupled with bottom-up fabrication of the Buckyball linear array might do the trick. Most recently, we have achieved another milestone, only previously achieved by NMR QIP, all-optical QIP and trapped ion QIP where have been able to interrogate the quantum coherence properties of the NV-systems themselves using a procedure known as Quantum Process Tomography (Figure5_21).

In summary, through the opportunities made available for pro-active collaborations on a European level by the Future and Emerging Technologies Unit, Buckyball quantum processing technology has emerged from being a theoretical concept to being a worldwide research area which it rapidly achieving goals undreamed about previously.

Defects in Diamond: A Potential Hardware for Quantum Information Processing

Diamond is one of the most fascinating materials. As a gemstone, hard coating and future electronic material it is of economical relevance. Pure diamond is colorless and optically transparent. The most valuable gemstones are made from such material. Often however, diamond is coloured. In fact 80% of all stones found in nature are classified as colored diamond. A large number of impurities in diamond are so called color centers, which determine the color of the crystal. Famous examples are blue diamonds, where the color comes from trace amounts of boron. Most color centers are known in detail and are used

commercially to enhance the color of certain gemstones making them more valuable. Usually their chemically composition is simple, like a single impurity atom as in the case of the boron defect. Due to a substantial progress in material production nowadays diamond, which is practically free of impurities, can be synthesised. These developments together with the controlled generation and implantation of color centers have fostered the application of diamond in other areas of future information technology, namely QIP.

Recently different research groups in Europe have shown the potential usefulness of color centers in diamond as single photon sources for secure data transfer in quantum communication. Such single photon sources are novel type of light sources, which emit single photons on demands being a key element in quantum cryptography. Currently the most promising experimental approach uses single quantum systems as photon emitters. In this technology a single quantum system is excited by an external photon source or pumped electrically, the concomitant emission of a single photon is used to encode quantum information. A couple of quantum systems like ions, quantum dots, molecules or colour centers have been investigated. Figures of merit in the field are room temperature operation and high photostability of the system. Also, the photon emission rate should be high enough and the emission wavelength should be compatible with telecommunication requirements. Color centers in diamond meet most of these requirements. As an example, the nitrogen vacany defect center in diamond has been shown to be a stable room temperature single photon emitter. The advantage as compared to other sources is the unsurpassed photostability and ability to position single NV centers with high spatial accuracy. Narrow room temperature emission lines are found in Ni related defect centers in diamond. Production of synthetic diamond containing NV color centers has been shown. The defect is bright, emits at a wavelength where telecommunication fibers have low absorption and has a narrow room temperature emission wavelength. In the next couple of years it can be expected that an easy-to-use and robust single photon modules can be developed from single defect centers in diamond. The aim will be to develope a fiber-based compact module which will contain all necessary elements in a single piece of optical fiber. Such fiber modules might allow for transform limited single photon emission when operated at low temperature and hence might be an enabling technology for all optical quantum computing.

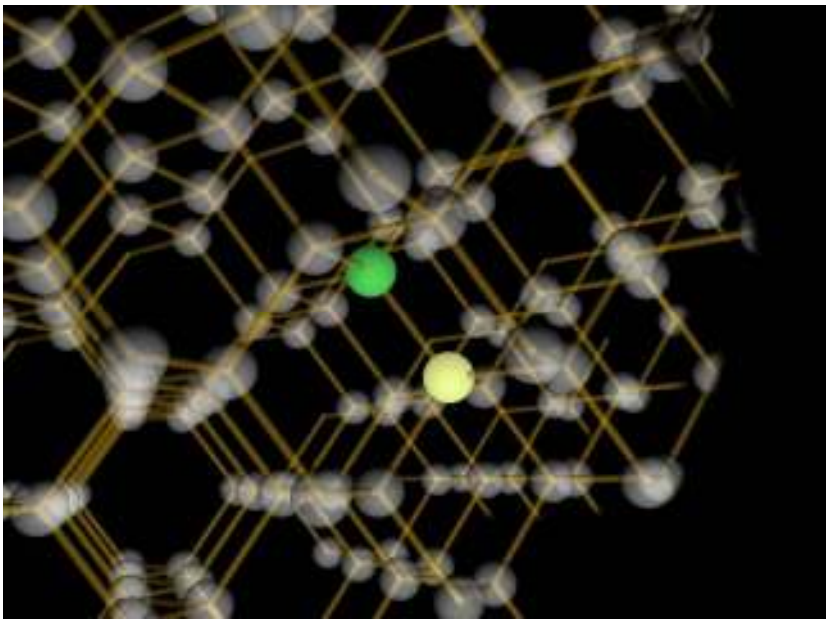


Figure 5: The nitrogen (green) and vacancy (yellow) forms nitrogen-vacancy defect in the diamond lattice.

A couple of defect centers in diamond are of potential use as quantum bits (qubits) for quantum computing as well. A prominent example is the nitrogen vacancy defect center (see **Figure 5**). In this defect the electron spin can be used as a quantum bit. It has been shown that the state of a single qubit can be read out at low temperature. Moreover, single and two-qubits manipulation is feasible even at room temperature [5, 7] (see **Figure 6)**. An important figure of merit is the dephasing time which is up to 0.35 ms under ambient conditions for this system. Qubit manipulations occurs on a timescale of some ten nanoseconds. Hence more than 10^4 qubit operations can be carried out before dephasing occurs. Nuclear spins are expected to show even longer dephasing times and hence are particularly interesting candidates as qubits or quantum memory. In the NV center nuclear spins are coupled to electron spins and hence are accessible as qubits as well. In this way quantum logic operation with a single electron and nuclear spin at a nitrogen vacancy defect center under ambient conditions have been demonstrated. In this scheme only nuclear spins which are sufficiently close (few 10^{-10}m) to the electron spin can be used. Hence this scheme cannot be scaled to larger number of qubits by adding nuclear spins. A scalable scheme requires the mutual coupling of defect centers. For this nitrogen atoms need to be implanted in diamond with high spatial accuracy. The precision needed is subject to the interaction chosen. For magnetic dipolar coupled centers, distances should not be larger than 5 nm, while for optical transition dipole coupling the distance can be as large as 10nm. Recently it was shown how to generate coupled defect center pairs by implantation of nitrogen molecules. In future devices advanced nano implantation techniques like the deposition of nitrogen atoms through moveable nano apertures need to be used. In these techniques low energy nitrogen ions (kinetic energy smaller 7keV) are implanted into a diamond substrate through a small (diameter 5nm) hole in the tip of a cantilever of an atomic force microscope. To allow for the addressing of single quantum bits, magnetic or electric field gradients need to be applied via gate electrodes. Owing to the close proximity of the defects, the requirements on the nanofabrication of the device are quite stringent though not beyond the capability of current technology.

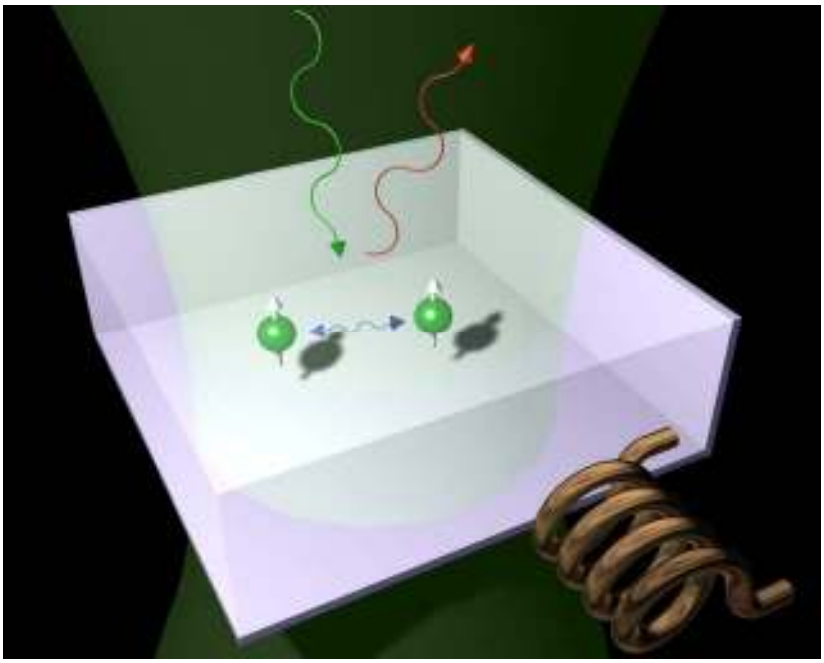


Figure 6: The interacting spins associated with single defects can be read out optically. Scattered laser photons (green, red arrows) provide information about spin states. Spin manipulation is realized using radio frequency pulses provided by microwave coil.

In summary, defects in diamond are promising systems for future quantum information technology. On short terms single photon devices based on certain colour centers have the potential to provide widely applicable devices. Quantum memories or processors certainly require advanced nanotechnologies. From the European perspective it is important to note that the world leading commercial supplier of diamond materials with unsurpassed knowledge in material production and structuring is based in Europe. In addition the perspective for room temperature device operation certainly is attractive and should be a key driving element for future research.

Conclusions

Although in its infancy, carbon based quantum processing technologies already have achieved much. The results obtained to date, and the promise of room temperature operations, set goals for other solid-state implementations. As the ITRS roadmap advances, the greater use of carbon/diamond in spintronics and other technologies will greatly aid in the push for developing carbon-based QIP.

List of terms and acronyms

Buckyball: Buckmeisterfullerene or C60, is a molecule with 60 Carbon atoms arranged in the shape of a round soccer ball.
NV: nitrogen-vacancy defect in diamond
ESR: Electron Spin Resonance, a technique to probe the local electronic environment within a molecule by irradiating a (usually) large ensemble of molecules (~10^{12}), with microwave radiation and observing the emitted re-radiation.
STM: Scanning Tunneling Microscope, a device used to image objects on atomic length scales.
ITRS: International Technology Roadmap for Semiconductors.

References

[1] B. Pietzak, *et al.*, *Buckminsterfullerene C60: A Chemical Faraday Cage for Atomic Nitrogen*, Chem. Phys. Lett. 279 (1997) 259

[2] W. Harneit, *Fullerene-based electron-based quantum computer,* Phys. Rev. A **65**, 032322 (2002)

[3] D. Suter and K. Lim, *Scalable architecture for spin-based quantum computers with a single type of gate,* Phys. Rev. A **65**, 052309 (2003)

[4] J. Twamley, *Quantum-cellular-automata quantum computing with endohedral fullerenes*, Phys. Rev. A **67**, 052318 (2003)

[5] F. Jelezko. *et al. Observation of coherent oscillation of a single nuclear spin and realization of a two-qubit conditional quantum gate*, Phys. Rev. Lett. **93**, 130501 (2004)

[6] D. P. DiVincenzo, in Mesoscopic Electron Transport, eds. Sohn, Kowenhoven, Schoen (Kluwer 1997), p. 657, cond-mat/9612126; "The Physical Implementation of Quantum Computation," Fort. der Physik 48, 771 (2000), quant-ph/0002077

[7] F. Jelezko, T. Gaebel., I. Popa, A. Gruber & J. Wrachtrup, *Observation of coherent oscillations in a single electron spin*, Phys. Rev. Lett. **92**, 076401 (2004)

Projects funded by the European Commission and related to the work in this article:

QIPDDF
A study for the construction of a Quantum Information Processing Device using Doped Fullerenes
Start date: 01/01/2000
End date: 31/12/2002
Project web site: http://www.thphys.may.ie/EC/QIPDDF/QIPDDF.htm
Contact Person: (first and last name, affiliation, email): Jason Twamley, National University of Ireland, Maynooth, Maynooth, Co. Kildare, Ireland, Jason.Twamley@nuim.ie

QIPDDF-ROSES
A study for the construction of a Quantum Information Processing Device using Doped Fullerenes and with the ReadOut of Single Electron Spin
Start date: 01/01/2003
End date: 31/12/2004
Project web site: http://www.thphys.may.ie/EC/ROSES/roeses_project.htm
Contact Person: (first and last name, affiliation, email): Jason Twamley, National University of Ireland, Maynooth, Maynooth, Co. Kildare, Ireland, Jason.Twamley@nuim.ie

Projects funded by National initiatives or organizations and related to the work in this article:

QIV
Quanteninformations-Verarbeitung
Start date: 1999
End date: 2005
Project web site http://kerr.physik.uni-erlangen.de/qiv/
Contact Person: Prof. Dr. Gerd Leuchs, Institut für Optik, Information und Photonik Staudtstr.7 D-91058 Erlangen, mail: leuchs@physik.uni-erlangen.de

Contact information of the authors of this article:
Jason Twamley
Department of Mathematical Physics
National University of Ireland, Maynooth
Maynooth, Co. Kildare
Ireland
Email: Jason.Twamley@nuim.ie
Web page: www.thphys.nuim.ie

Jörg Wrachtrup
3. Physikalisches Institut
Universität Stuttgart
Pfaffenwaldring 57
D-70550 Stuttgart
Germany
Email: wrachtrup@physik.uni-stuttgart.de
Web page: http://www.physik.uni-stuttgart.de/institute/pi/3/

Quantum computing with rare-earth-ion doped crystals

Stefan Kröll
Stefan Kröll is professor of atomic physics at the Department of Physics, Lund Institute of Technology (LTH) in Lund, Sweden. He is also the Director of Graduate Studies LTH. In the past he held the Research Position in Optical Physics at the Swedish Natural Science Research Council. His past and present research interests include: non-linear laser spectroscopy, coherent processes and quantum information applications in rare-earth-ion doped crystals. He is the coordinator for the EU-funded IST projects: REQC, hardware and ESQUIRE.

Klaus Mølmer
Klaus Mølmer is professor of Atomic Physics and Quantum Optics at the Department of Physics and Astronomy, University of Aarhus in Aarhus, Denmark. He is also Honorary Professor at the University of Copenhagen. He is a member of the EU-funded IST project ESQUIRE. He is also a member of the Danish National Research Foundation Center for Quantum Optics. Recipient of the Aarhus University Biennial Research Award 2004 and the Biennial Award of the Danish Physical Society 1999. Member of The Royal Danish Academy of Sciences and Letters.

Mattias Nilsson
Mattias Nilsson is a Ph.D. in atomic physics at the Department of Physics, Lund Institute of Technology (LTH) in Lund, Sweden. His research activities include: optical storage and processing of information using coherent transients, and coherent interactions in rare-earth-ion-doped crystals for applications in quantum information science. Previously member of the Swedish teams in the Young Physicist Tournament and the Physics Olympiad.

Abstract

Solid state lasers, like for example a common laser pointer, emit light from ions sitting within a crystal host. Our rare-earth quantum computer is implemented in such doped crystals, using rare-earth ions like neodymium, europium and thulium, which are randomly distributed throughout the crystal. The random distribution of ions is structured into quantum hardware using optical pulses. The ions have ground states in which bit values can be stored for long times, and their excited states have different energies so that different ions can be selectively addressed by laser light with different frequencies. The selective excitation permits high accuracy operations on groups of single ions (qubits) and the interaction between neighboring ions in the host permit implementation of quantum gates.

Introduction

The picture in **Figure 1** shows an yttrium silicate crystal, doped with praseodymium. The crystal looks transparent, but if it is irradiated with a wavelength that has been adjusted with a precision of one in a million to exactly the position in the orange region where praseodymium ions absorb, the light will be absorbed. All praseodymium ions, however, do not absorb at exactly the same frequency. In fact, if the wavelength is narrowed down another million times, to a frequency precision of 1 part in 10^{12}, and a weakly doped crystal is irradiated, it is possible to select and interact with individual ions in the crystal. Although the individual praseodymium ions are intrinsically equivalent, their actual absorption frequency when embedded in the crystal is determined by the local electric and magnetic fields. A pure single crystal has a very regular structure so one would believe that praseodymium ions substituting for the yttrium ions in the crystal in **Figure 1** might still be equivalent. However, the slight difference between the size of the dopant ion and the host ion for which it substitutes induces strain in the crystal. The local field and the absorption frequency at a given site are therefore determined by the occupancy of dopant ions in the immediate vicinity, and observing the absorption frequency we get information about local conditions at the ion site. Since the absorption lines of the ions are so narrow, we can see absorption frequency (or energy level) changes of one part in 10^{12}. With such a resolution it is actually possible to use a single ion as a local probe, keeping track of what is happening in its vicinity. In particular, the charge distribution and thereby also the electric field of a neighboring ion, depends on its internal quantum state. This means that the quantum state of one ion influences the field acting on its neighbors and hence their absorption frequencies.

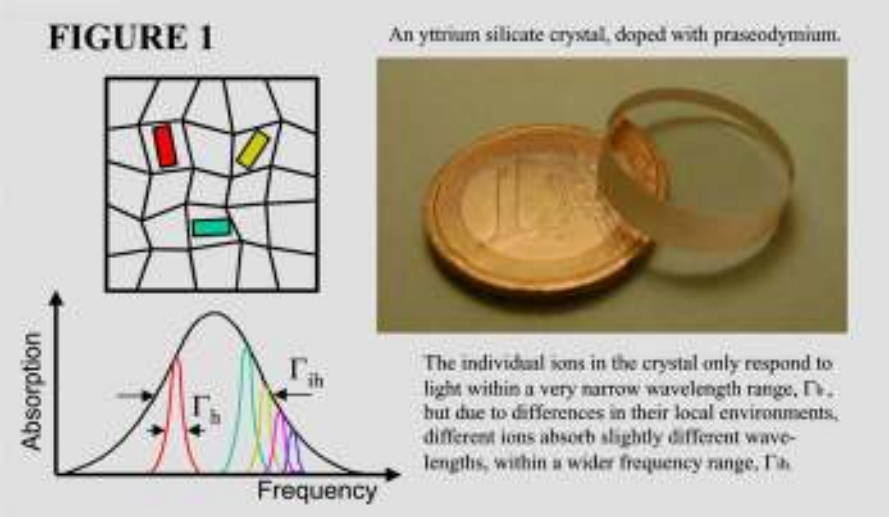


Figure 1

Ideally, one could imagine a crystal growth process, in which the dopant ions enter the material in a structured manner, allowing us to keep track of the position of every single ion. This, however, is not the situation with crystal growth techniques of today, and we are left with essentially no control of the positions of the ions and no control of how the crystal influences their individual absorption frequencies. In view of the extreme demands on precision control of the quantum systems in a quantum computer, the randomness in ion position and frequency at first seems to make quantum computing in these systems a hopeless task. It turns out, however, that capitalizing on the large value of Avogadro's number, even the tiniest crystal contains an immense number of ions. Hence we can choose a random set of excitation frequencies and be sure that many ions at random positions within the crystal will respond exactly at these frequencies, and we can detect their presence by the absorption properties of the crystal at the selected frequencies.

In this text, we describe how we can initialize the crystal material to perform as a quantum computer, by organizing the ions in frequency space, effectively creating order out of disorder. We describe how to perform one- and two-bit gates under ideal assumptions, and we show how we can perform operations which are robust to various error sources.

Quantum computing on "needles in a hay stack"

Today there is a clear consensus on what properties are important for a good qubit:

1. Each qubit must be individually addressable and it must be possible to prepare it in a selected fiducial quantum state

A simplified atomic level scheme of a rare earth ion is shown in **Figure 2**. It has long-lived (seconds) ground states $|0\rangle$, $|1\rangle$ and $|aux\rangle$, and an excited state $|e\rangle$. We can transfer the ions between states, say from $|0\rangle$ to $|1\rangle$ by using first a laser pulse exciting the ion from $|0\rangle \rightarrow |e\rangle$ and then another pulse on the $|e\rangle \rightarrow |1\rangle$ transition. As discussed in the introduction, the frequency for the ground-to-excited-state transition differ for different ions and in this scheme a qubit is initially identified as all the ions in the crystal for which the optical $|0\rangle \rightarrow |e\rangle$ transition has a certain absorption frequency, thus the frequency of our laser pulses determines which qubit we are interacting with.

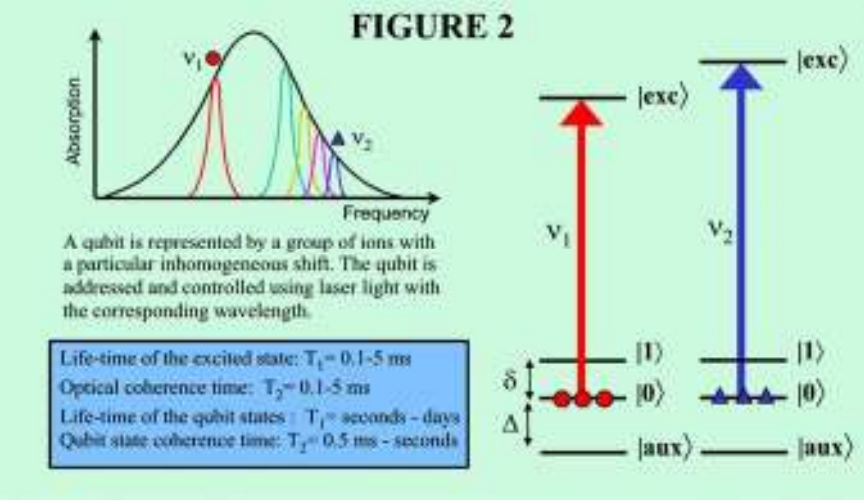


Figure 2

The discrete absorption lines of the individual ions in **Figure 2** are like needles in a large inhomogeneously broadened hay stack of absorption lines. We find and isolate this needle in the following way: If we send a light beam tuned to the ν_0 frequency through the crystal, ions with the specific $|0\rangle \rightarrow |e\rangle$ transition absorption frequency ν_0 will absorb the laser light and be promoted to the $|e\rangle$ state. From here they spontaneously decay back to one of the ground states. Those that decay to the $|0\rangle$ state will repeatedly be promoted to the $|e\rangle$ state until they decay to the $|1\rangle$ or $|aux\rangle$ states and, eventually, there will be a hole in the absorption profile. If the laser is tuned in frequency around ν_0 we can dig out a pit in the absorption profile. If the region across which the laser is tuned includes both frequencies ν_0 and $\nu_0+\delta$, where δ is the energy difference between the $|0\rangle$ and $|1\rangle$ states (**Figure 2**), all ions with their $|0\rangle \rightarrow |e\rangle$ transition absorption frequency around ν_0 will now be in their $|aux\rangle$ ground state. Finally, tuning the laser to a narrow range around $\nu_0+\Delta$, where Δ is the energy difference between the $|0\rangle$ and $|aux\rangle$ state, the ions are transferred from the $|aux\rangle$ state back into the $|0\rangle$ state. These ions absorb radiation at the desired well-defined frequency ν_0.

For the quantum computation it is important to have full control over all the excitations in the material as the excitation creates (random) energy shifts of the neighboring ions in the material. Due to the hole burning of a broad pit around ν_0, the qubit is located in a frequency region where there are no absorbing ions at nearby frequencies (**Figure 3**), and hence there is no excess excitation of spectator ions.

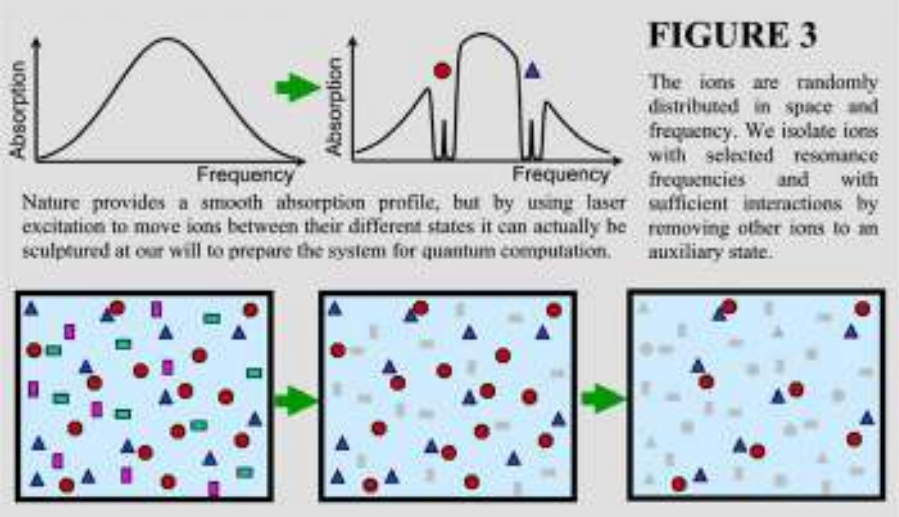


Figure 3

2. The qubit must preserve quantum information over a time period at least four or five orders of magnitude longer than the time for performing an operation on the qubits

If a frequency range $>\delta$ is emptied of ions, pulses on the $|0\rangle \rightarrow |e\rangle$ and $|e\rangle \rightarrow |1\rangle$ transitions of microsecond duration can be resonantly applied to the qubits without exciting ions outside the emptied frequency range. The ions can remain in a superposition of quantum states $|0\rangle$ and $|1\rangle$ for times ranging between milliseconds and seconds, and hence 10^3-10^6 operations can be carried out before the qubit decoheres and looses its quantum properties.

3. The qubits must interact such that they can become entangled

For a two-qubit gate there is often a control bit which determines whether an operation on a target qubit takes place or not. An excited ion can shift nearby ions in and out of resonance

with the laser field and turn their absorption on and off. To use this interaction as a precisely controllable quantum gate, it must be ensured for all qubits that all ions in each qubit are in the same state. This can be achieved provided each ion in the target qubit is close to an ion in the control qubit. A qubit initially consist of all ions absorbing at an arbitrarily selected frequency, but as the ions sit randomly in the crystal most target qubit ions will have no nearby control qubit ion. Such target ions cannot be used for quantum computing operations and must be removed from the target qubit (**Figure 3**). This is then done by transferring them to the auxiliary ground state hyperfine level. This assures that only interacting ions are left in the qubit.

4. It must be possible to read out the state of the qubits in an efficient way

The qubits are defined by the absorption frequencies of the participating ions, and a large number of ions, ion-pairs, or groups of ions all are driven in unison by the laser fields. The quantum computer described is an ensemble computer, but unlike ensemble computing with Nuclear Magnetic Resonance techniques, the rare earth system can be initialized in a pure quantum state prior to the calculation, and the ensemble only plays a role for read-out: The state of the ions can be read out by the macroscopic absorption or fluorescence properties of the crystal on the $|0\rangle \rightarrow |e\rangle$ and $|1\rangle \rightarrow |e\rangle$ transitions of the different qubits.

One and two-bit gates

Under ideal circumstances, the ions behave like perfect two-level atoms, when irradiated on any of the resonant transitions, and arbitrary qubit operations can be performed on the system. Quantum dynamics of a two-level system can be represented by the motion of a point on a spherical surface. The ground and excited states correspond to the south and north poles of this sphere. A pulse driving an atom from its ground state to its excited state is then equivalent to a 180 degree rotation on the sphere. Such a pulse is called a π-pulse. A logical NOT-operation on a rare earth qubit, for example is accomplished by application of three laser π-pulses on the $|0\rangle$-$|e\rangle$ and $|1\rangle$-$|e\rangle$ transitions, see **Figure 4(a)**, which precisely transfer all population between states $|0\rangle$ and $|1\rangle$ via the excited state $|e\rangle$. The operation only acts on the desired qubit, because it involves the frequency-selective resonant transition to the excited state.

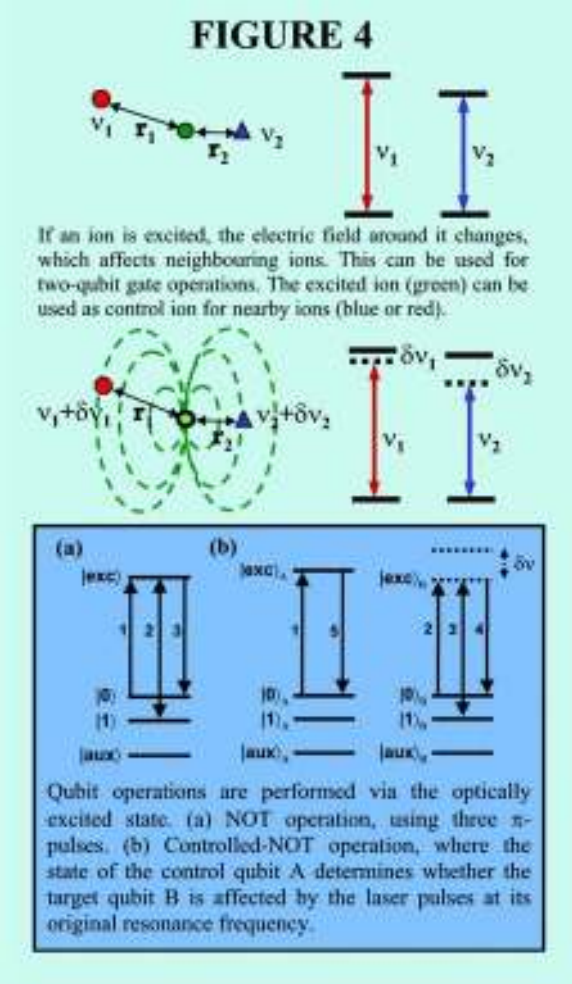


Figure 4

Using the interaction described above, one ion can control the dynamics of another ion in the following way (**Figure 4**): the excitation of the $|0\rangle \rightarrow |e\rangle$ transition of one ion leads to an energy shift of the $|e\rangle$-state of the neighboring ions, conditioned on the control ion originally being in state $|0\rangle$. If we then apply a sequence of laser pulses on the target ion, achieving a NOT-operation, the pulses will be resonant if the control ion is in the $|1\rangle$-state, but they will be off-resonant if the control ion initially was in the $|0\rangle$-state, and then they will never affect the target ion. The net result is what is called a C-NOT operation, see **Figure 4(b)**, yielding a flip of the target bit if the control bit is in state $|1\rangle$. The C-NOT gate and the one-bit gates together constitute a universal set of gates, and any quantum computation operation can be expressed in terms of these. We note that the addressing of both the control and the target ion gate is qubit specific due to the inhomogeneous shifts of their excited states, and we also note that the interaction only has to cause a large enough detuning to prevent the target ion transition to the excited state, the precise value is not important.

The crystal is prepared for the quantum computation by a hole burning procedure which creates frequency intervals with no ions except in narrow central frequency windows (**Figure 3**). Light resonant with these central frequencies interact effectively with the qubit ions but not with the other ions in the crystal. The number of ions in the designated qubit frequency windows will be small if the windows are made too narrow. The resonant excitation, however, will be subject to errors if the frequency windows are too broad, since we then want to excite by one and the same laser pulse a number of ions with slightly different excitation

frequencies. This problem is familiar in liquid and solid state Nuclear Magnetic Resonance studies, where a number of clever excitation schemes have been found, which are tolerant to uncertainties about the precise value of parameters in the system Hamiltonian as long as they stay constant throughout the interaction. As previously stated, a pulse that will drive an atom from its ground to its excited state is equivalent to a 180 degree rotation from the south to the north pole around a horizontal axis. Having an unknown laser field strength or unknown laser detuning is equivalent to not knowing the rotation angle on the sphere or not knowing precisely around which axis the rotation takes place. However, by an intelligent choice of sequence of rotations we may still get all ions very close to north pole even if they experience slightly different fields. We start by a ~90 degree rotation around the, say, x-axis, putting our initial south pole state on the equator, we then rotate the sphere ~180 degree around the y-axis; and finally we apply again the ~90 degree rotation about the x-axis. In case of perfect operation, the middle rotation has no effect, but as shown on the left sphere in **Figure 5,** a too small rotation does not reach the equator, but the 180 degree rotation then puts our states above the equator by the same amount, so that the final rotation, assuming it still is too slow, hits very close to the desired final state. **Figure 5** also shows the accomplishments of a more advanced pulse, a hyperbolic secant pulse which can carry out a uniform operation on ions with a broad range of different detunings. Pulses with even better error compensation exist, and with numerical search routines laser pulses with smoothly varying amplitudes and phases with the best possible performance has been identified. A 3-4 microsecond long pulse can indeed excite with nearly 100 % probability all ions in a nearly MHz wide frequency window, while ions more than 5 MHz away from resonance are excited far below the per cent level. Experiments with hyperbolic secant pulses have demonstrated multiple reliable transfers of atoms between qubit states.

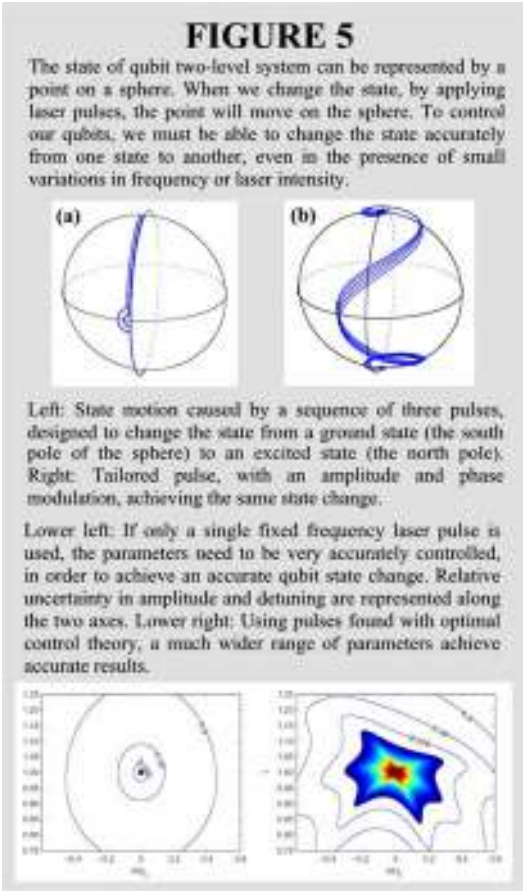


Figure 5

Conclusions

The rare-earth-ion doped crystals are serious candidates for quantum computing. Spectral hole-burning gives the means to take a large number of ions, embedded in a crystal with no particular ordering in neither space nor frequency domain, and from this select a sub-set of ions with the properties we want, e.g., clusters of interacting ions that will work as quantum processors. In some materials, such quantum hardware can be durable, in the sense that the spectral holes are very long-lived, and the crystals may even be shipped between production and research facilities after hole-burning. We have already observed reliable one-bit processes, where we use laser light to control the state of the ions, and we have documented the interactions needed for two-bit gates.

The qubit requirements in the "Quantum computing on needles in a hay stack" section are not sufficient to build a quantum computer. There is an additional criterion: it must be possible to scale the system from a few-qubit system to a system with a large number, say hundreds or thousands, of qubits. Materials research as well as research into scalable architectures involving for example different dopants taking care of qubit storage, mediation of interactions and read-out may pave the way for progress in this field.

List of terms and acronyms

Rare earth elements: a name given to the chemical elements with atomic numbers between 58 and 71. They are neither rare nor earths, but many rare earths elements were first found in minerals. Due to their electronic and nuclear properties some of the rare earth elements have suitable optical properties when they are doped into transparent crystals.

Hyperfine structure: the splitting of atomic energy levels into hyperfine states, with a small difference in energy, e.g. due to different orientations of the nuclear spin relative to the electronic cloud. These states are often relatively stable and here we let one hyperfine state signify a logical bit value of 0 and let another hyperfine state signify a logical 1.

Inhomogeneous broadening: when individual atoms absorb light at slightly different wavelengths. The total absorption line will be given by the sum of the absorption of all atoms and may be much wider than the line-widths of the individual absorbers (the homogeneous line-width).

Hole-burning: by exciting atoms absorbing within a small part of an inhomogeneously broadened absorption line, using a narrow-band light source, the absorption at that particular wavelength is reduced, creating a spectral hole in the absorption profile. If the atoms are permanently removed to a new state, the hole will be persistent.

References

[1] N. Ohlsson, R.K. Mohan and S. Kröll, *Quantum computer hardware based on rare-earth-ion-doped inorganic crystals*, Opt. Comm. 201, 71 (2002)

[2] I. Roos and K. Mølmer, *Quantum computing with an inhomogeneously broadened ensemble of ions: Suppression of errors from detuning variations by especially adapted pulses and coherent population trapping*, Phys. Rev. A 69, 022321 (2004)

[3] J. J. Longdell, M.J.Sellars and N.B.Manson, *Demonstration of conditional quantum phase shift between ions in a solid*, Phys. Rev. Lett. 93, 130503 (2004)

[4] M. Nilsson, L. Rippe, R. Klieber, D. Suter and S. Kröll, *Hole-burning techniques for isolation and study of individual hyperfine transitions in inhomogeneously broadened solids, demonstrated in Pr3+:Y2SiO5*, Phys. Rev. B 70, 214116 (2004)

[5] O. Guillot-Noël, Ph. Goldner, E. Antic-Fidancev, and J. L. Le Gouët, *Analysis of magnetic interactions in rare-earth-doped crystals for quantum manipulation*, to be published in Phys. Rev. B, accepted Dec. 2004

Projects funded by the European Commission and related to the work in this article:

REQC
Development of quantum computer hardware based on rare-earth-ion-doped inorganic crystals
Start date: 1/10/2001
End date: 30/9/2002
Contact Person: Stefan Kröll, Department of Atomic Physics, Lund Institute of Technology, stefan.kroll@fysik.LTH.se

ESQUIRE
Experimental realization of quantum gates and development of scalable quantum computer schemes in rare-earth-ion-doped inorganic crystals
Start date: 1/1/2003
End date: 31/12/2005
Project web site: http://www-atom.fysik.lth.se/photonEcho/Esquire/
Contact Person: Stefan Kröll, Department of Atomic Physics, Lund Institute of Technology, stefan.kroll@fysik.LTH.se

Projects funded by National initiatives or organizations and related to the work in this article:

The work described in this paper has also been supported by the Swedish Research Council and the Knut and Alice Wallenberg Foundation, the Danish National Research Foundation and CNRS, France.
Contact Person: (Stefan Kröll, Department of Atomic Physics, Lund Institute of Technology, stefan.kroll@fysik.LTH.se)

Contact information of the authors of this article:
Stefan Kröll
Department of Atomic Physics
Lund Institute of Technology
P.O. Box 118
SE-221 00
Lund
Sweden
Email: stefan.kroll@fysik.LTH.se
Web page: http://www-atom.fysik.lth.se/afdocs/staff/staff.asp

Klaus Mølmer
Department of Physics and Astronomy
University of Aarhus
Ny Munkegade, Building 520
DK-8000
Aarhus
Denmark
Email: moelmer@phys.au.dk
Web page: http://www.phys.au.dk/quantop/theory.shtm

Mattias Nilsson
Department of Atomic Physics
Lund Institute of Technology
P.O. Box 118
SE-221 00
Lund
Sweden
Email: mattias.nilsson@fysik.LTH.se
Web page: http://www-atom.fysik.lth.se/afdocs/staff/staff.asp

Quantum imaging

Claude Fabre
Claude Fabre is a professor at the Laboratoire Kastler Brossel, University P.M. Curie and Ecole Normale Supérieure, Paris, France. His research interests include: specific quantum properties of light, generation, study and use of non-classical states of light (quantum correlations and entanglement, squeezing, quantum correlations and fluctuations in optical images). He is a member of SFP, EPS, fellow of the OSA and the coordinator of EU-funded IST project "QUANTIM" (Quantum Imaging).

Abstract
Optical images are a privileged way to convey a great quantity of information in a parallel way. Due to the quantum nature of light, this information is inevitably affected by uncontrolled fluctuations, the "quantum noise" or shot noise, which limits the reliability of the information extraction from the image. Quantum optics allows us to **tailor the spatial distribution of quantum fluctuations** so as to reduce the quantum noise in the information channels that one wants to read out. In a related way, it offers the possibility of generating **spatial quantum entanglement** between different parts of an optical image. This unique feature, which can be implemented either in the photon counting regime or in the regime of intense beams with continuously varying local intensities, can be used to make up new ways of recording images, such as "two-photon imaging", or to improve the quality of information extraction from the image. It may lead in the future to new microscopy techniques to record features in images which are much smaller than the wavelength of the light or to improve the optical storage capacity beyond the wavelength limit. In a more remote future, it may lead to novel massively parallel architectures in quantum computing.

Introduction
For more than two decades now, techniques have been developed, first at the theoretical then experimental level, which were able to get rid of, or at least to reduce, quantum fluctuations in measurements performed on the **total intensity** of macroscopic light beams. This domain has recently been successfully developed in the direction of quantum information processing.

In a parallel way, a new domain has emerged, which deals with measurements of the **spatial distribution of light,** performed on "pixellised" detectors (like CCD cameras), either in the photon counting regime or with macroscopic intensities [1]. It was discovered that one could tailor at will the spatial quantum fluctuations of light (of course within the constraint imposed by Heisenberg inequalities), and also that it was possible to produce **spatial quantum**

entanglement and therefore to create strong correlations in the measurements performed at different points of the optical image.

As images are often used to record, process and store information, these ideas can in turn be applied to the problem of **quantum processing of information in** images: quantum techniques have the potentiality to improve the sensitivity of measurements performed in images and to increase the optical resolution beyond the wavelength limit, not only at the single photon counting level, but also with macroscopic beams of light. These new techniques could then be of interest in many domains where light is used as a tool to convey information in very delicate physical measurements, such as ultra-weak absorption spectroscopy or Atomic Force Microscopy. Detecting details in images smaller than the wavelength has obvious applications in the fields of microscopy and pattern recognition in images, and also in optical data storage, where it is now envisioned to store bits on areas much smaller than the square of the wavelength. Furthermore, spatial entanglement leads to completely novel and fascinating effects, such as **two-photon, or "ghost", imaging**, in which the camera is illuminated by light which did not interact with the object to image, or "quantum microlithography", where the quantum entanglement is able to act upon matter at a scale smaller than the wavelength.

This kind of study is a rather new subject of quantum optics. The investigations made so far concern mainly the ways of producing and characterizing spatially entangled non-classical light and also first simple implementations of applications, which showed that it is possible using such concepts to improve information extraction from images. To illustrate these somewhat abstract considerations, we will give in the following a short description of several achievements obtained in the domain, and conclude by mentioning some perspectives and open problems which seem promising and deserve therefore more investigations in the future.

The "quantum laser pointer"

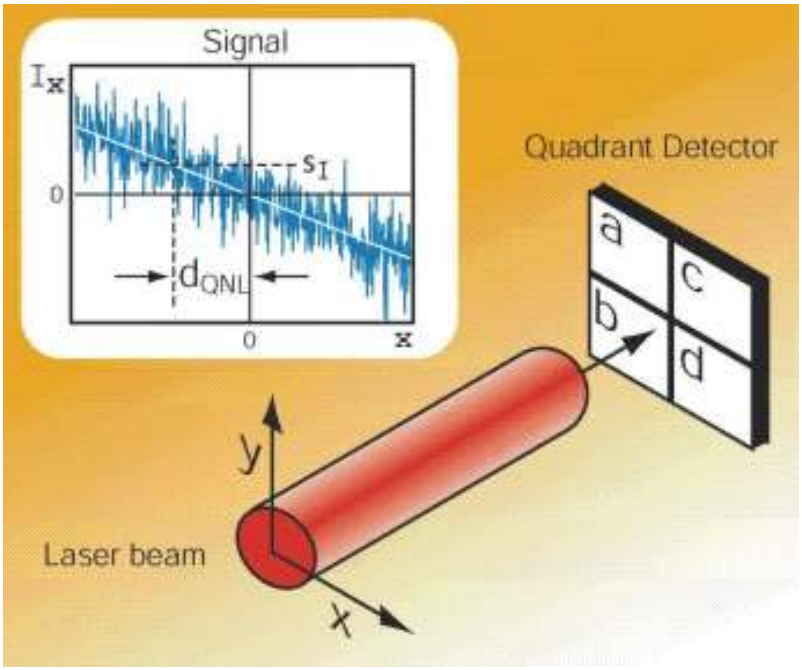


Figure 1: Experimental set-up for measuring the transverse displacement of a laser beam. Top left: signal obtained by making the pixel combination (a+b)-(c+d)

It has been known for a long time, and experimentally demonstrated, that the sensitivity of optical measurements performed on the global intensity, or on the global phase, of a light beam can be improved by using **single mode non-classical states of light**, such as sub-Poissonian or squeezed states. This is no longer true for measurements performed in optical images, in which one monitors a variation of the transverse distribution of the light. The simplest of these measurements is that of the **position of the centre of a beam**, which is obtained using a quadrant detector: if the four partial intensities are equal, the beam is exactly centred on the detector, and any imbalance gives information about the transverse displacement of the beam. The sensitivity of such a measurement, at the nanometer scale, is limited by the standard quantum noise, or shot noise, present on the four measurements. It was first shown theoretically that the pointing sensitivity can be improved beyond such a standard quantum limit (SQL) by using **multi-mode non-classical light**, namely a mixing of a coherent beam with squeezed vacuum states in transverse modes of specific shape. This mixing actually creates a perfect quantum correlation between the intensities measured on the different pixels of the detector.

This effect has been recently experimentally demonstrated: the first experiment was able to improve the measurement of the displacement of a 0.5 mm diameter beam in a given direction of the transverse plane below the SQL, at the angstrom level, using a split detector and a two-mode non-classical light. In a second experiment [2], using a quadrant detector and a three-mode non-classical light, it was possible to measure simultaneously the two transverse coordinates of the beam centre below the SQL.

The theoretical understanding of such measurements in images has also advanced, and the transverse mode responsible for the noise in a measurement of any quantity derived from the combination of the intensities measured on different pixels has been identified. This opens the possibility of improving many image processing and analysis functions, such as pattern recognition, image segmentation, or wavefront analysis. Techniques have been theoretically proposed for producing **spatially entangled beams**, which are perfectly correlated in transverse position, and having at the same time perfectly anticorrelated angular deviations with respect to the optical axis (displacement and tilt are quantum-conjugate quantities, associated to non-commuting operators).

Observation of pure spatial quantum correlations in parametric down conversion

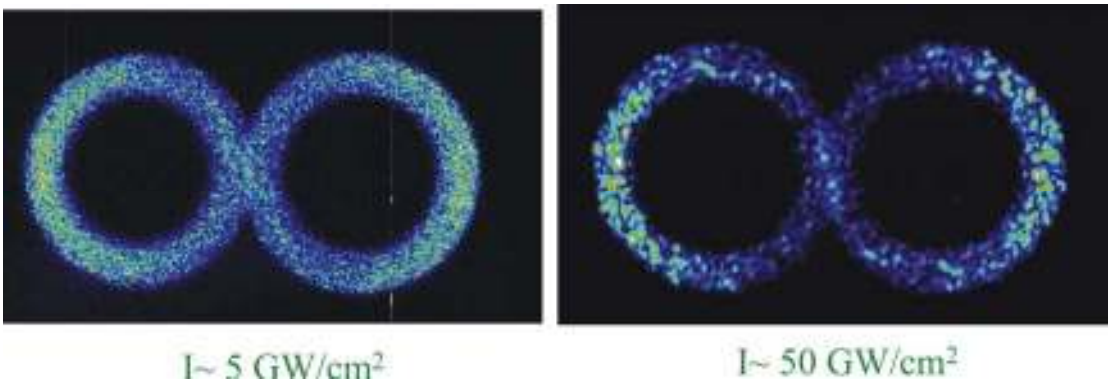


Figure 2: Images obtained by spontaneous down conversion in the high gain regime. The points in the signal and idler circles which are symmetrical with respect to the image center are quantum correlated.

The experiments described in the previous section dealt with the tailoring of **the transverse distribution of temporal quantum fluctuations in light**. There is another possible kind of quantum noise study on images, which concerns **pure spatial quantum fluctuations**, i.e. the pixel-to-pixel fluctuations of the light intensity when it is integrated over the total duration of a single light pulse**.** It concerns only **spatial averages and no longer time averages**. Measuring at the quantum level pixel-to pixel fluctuations is a new experimental challenge, and novel and delicate experimental techniques had to be developed in order to reach the SQL for spatial fluctuations, then to observe the two specific spatial quantum effect described in this paragraph and in the following.

It is well-known that parametric down conversion produces twin photons which are spatially perfectly correlated at the quantum level. This effect has been extensively used in beautiful experiments at the photon counting level. When the pump intensity is raised by a large factor, many twin photons are produced which can no longer be counted individually. One obtains on the signal and idler beams *quantum correlated images*, each having large pixel to pixel fluctuations, but (almost) identical intensity values on symmetrical pixels. In the high parametric gain regime where roughly 10 to 100 photons were recorded on average on each pixel, such a pixel to pixel quantum correlation in a single shot spatial statistics was recently demonstrated [3]. The best spatial noise reduction observed was about 50% below the standard quantum limit. This important achievement can now be used to information processing in images, for example to improve the sensitivity in the detection of faint images.
Parametric down converters, when inserted in resonant optical cavities produce highly correlated single mode coherent beams. The same kind of device has been theoretically shown to produce also spatially correlated light provided that one uses specific optical cavities, such as confocal cavities. The experimental implementation of these effects turns out to be very delicate, and only small amounts of spatial correlations have been so far measured in such devices.

Noiseless image parametric amplification

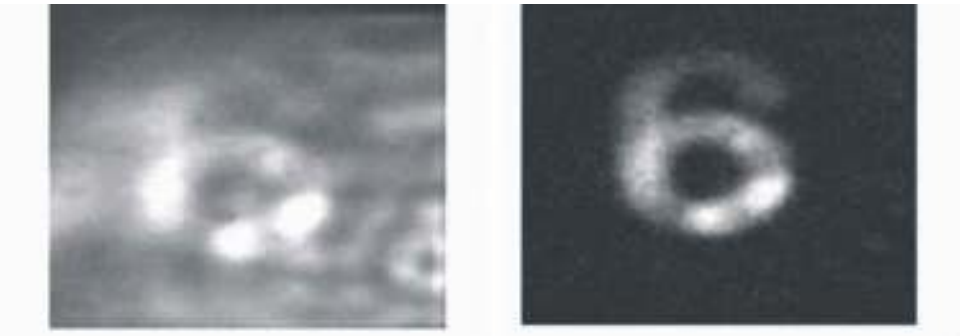


Figure 3: Left: amplified image of a very week signal noised by the parametric spontaneous down conversion. Right: amplified image when the background noise is subtracted.

Optical amplification is one of the key techniques in the handling of optical information. Quantum theory shows that the amplification process induces inevitably a degradation of the signal to noise ratio by at least a factor 2 when oscillating signals are amplified in a way independent of the phase of the oscillation. In contrast the amplification can be noiseless in the phase-sensitive configuration. In particular parametric amplification can operate in such a phase sensitive configuration and amplify an optical signal without degrading it. This was experimentally shown a few years ago for the temporal fluctuations measured at the different points of an image. It was recently demonstrated that this is also the case for the pixel to pixel spatial fluctuations recorded on a single-shot image amplified by a pulsed optical parametric amplifier [4]. In a very delicate experiment the spatial noise figures were determined in the phase-sensitive and phase insensitive schemes, and it was shown that in the low gain regime the phase sensitive amplifier does not add noise, while the phase insensitive amplifier leads to the degradation of the signal to noise ratio by a factor 2. Amplification of faint images without degradation of their quality is obviously a domain which may have important applications.

Classical and quantum features in "two-photon imaging"

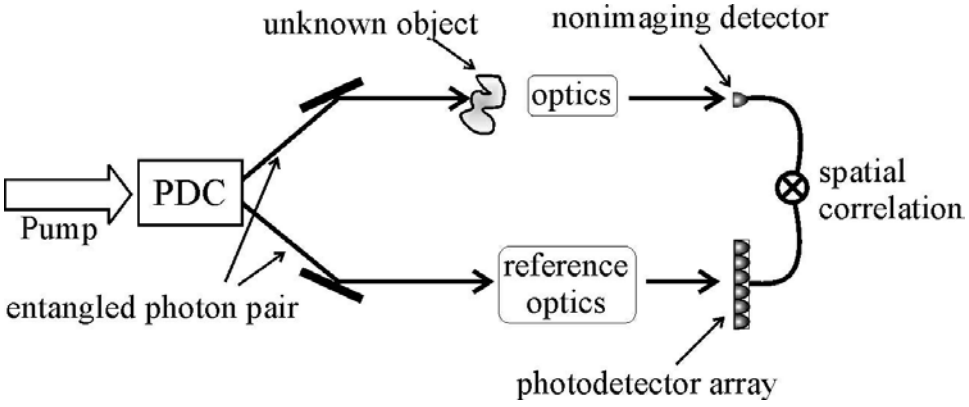


Figure 4: Experimental set-up for two-photon imaging

Entangled two-photon imaging ("ghost imaging") is based on the spatial correlations existing between the signal and idler twin photons produced by spontaneous parametric down-conversion. Its principle is the following (see **Figure 4**): one inserts in the signal arm an object that one intends to observe. The image of this object is obtained in a rather paradoxical way, without using a pixellised detector, but instead a single, non imaging, detector on the

signal beam. On the other hand, one inserts a pixellised detector (i.e. a camera) in the idler arm where there is no object. The entangled imaging technique carries out the observation of the object by detecting the coincidences between the measured photons on the signal and idler beams. This technique was implemented at the photon counting level in a number of beautiful experiments in the mid nineties, and was generally considered as the perfect example of use of spatial quantum correlations. The theory was then extended to the case where macroscopic intensities were detected. It was also predicted that both the near field and the far field images could be imaged in the same experimental set-up. But very recently experiments were also able to obtain a near field image by the same technique using beams produced by a regular beam-splitter, and not twin photons. A lively worldwide discussion started on the precise assignment of classical and quantum features in "two-photon imaging": it was in particular discovered, and experimentally demonstrated [5], that the same imaging technique could be made, both in the near field and in the far field, by using classical correlated beams, such as a thermal beam divided in two parts on a beam-splitter, instead of quantum correlated beams. Only some quantitative features, such as the contrast of the image are improved when one uses quantum correlated beams instead of classical correlations.

From the point of view of applications, the fact that ghost imaging may be realized using a simple beam-splitter instead of twin beams produced by a complex set-up is positive in terms of cost and simplicity: this shows that there is some practical interest in precisely assigning what is classical and what is quantum in a given phenomenon, a discussion which is generally considered as purely academic.

Other results in Quantum Imaging

Among the numerous problems that are currently studied under the general name of quantum imaging, the investigations concerning the quantum limits on optical resolution have a special importance, as they may lead to new concepts in microscopy and optical data storage. Such so-called **super-resolution techniques**, studied for a long time at the classical level in the perspective of beating the Rayleigh limit of resolution, were recently revisited at the quantum level [6]. It was shown that it was possible to improve the performance of super-resolution techniques by injecting non-classical light in very specific transverse modes, namely the eigenmodes of the propagation through the imaging system. The precise generation scheme of such a multi-mode non-classical light was recently obtained. The simplicity of the scheme brings confidence that quantum-enhanced super-resolution technique can effectively be implemented in an actual experiment.

Transverse solitons are potential candidates for the role of spatial q-bits, and soliton arrays for the role of q-registers. The theoretical study of their quantum features has been recently undertaken in different configurations: free propagating solitons through planar Kerr media, and cavity solitons appearing in degenerate parametric oscillators. The existence of local noise reduction and spatial correlations has been predicted in such devices.

Non linear media have been used for a long time to process images. For example, up-conversion of optical images from the infrared to the visible has been proposed and realized in order to take advantage of the higher quality of CCD detectors in the visible. This domain was also recently investigated at the quantum level in second harmonic generation: it has been shown that there existed configurations where the up-conversion of any image to the second harmonic field was possible without adding quantum noise to the initial image.

It is also interesting to investigate how the now "classical" protocols of quantum information on global variables, such as teleportation or cryptography, could be extended into the domain of images, and in which respect the intrinsic parallelism peculiar to imaging could be used in these protocols. The quantum teleportation of images was particularly studied in detail [7]. The proposed scheme has indeed a lot of similarities with the usual holographic technique, with the advantage that, in the quantum teleportation scheme, no quantum noise is added by the image reproduction device. A similar analysis is currently made for the problem of dense coding.

Conclusions and Perspectives

The domain of quantum imaging has been pioneered by teams in Russia (Saint Petersburg, Moscow), in Europe (Como, Paris, Lille) and in the US (Boston, Evanston). European funding of various projects (QSTRUCT, QUANTIM) has produced a strong community in Europe on this subject (Paris, Como, Palma, Glasgow, Lille, Besançon) with collaborative research links with Russia, USA and Australia. The subject is now studied by a growing number of teams throughout the world. In particular the US administration has realized the potentialities of the domain and included Quantum Imaging in a list of priority subjects.

Microscopy, wavefront correction, image processing, optical data storage and optical measurements in general constitute a very important domain of our present day technologies. They can benefit in various ways from the researches on quantum imaging. They can directly use the improvements brought by quantum effects and demonstrated by laboratory experiments, but their present complexity is an obstacle to such applications. At a less ambitious level, but perhaps more realistic, many optical technologies could be significantly improved by using the highly sophisticated methods developed in quantum optics labs to reach, and go beyond, the level of quantum noise in images.

A lot of research work remains indeed to be done, on the experimental side, to improve the light sources and the detectors in order to obtain high levels of quantum spatial entanglement and, but also on the theoretical side, to find more practical applications of spatial entanglement to information technologies. A promising direction of research is certainly the use of orbital angular momentum of light to convey and process quantum information. So far, the spatial quantum effects are somewhat on the edges of quantum computing, as they have been essentially used in the domain of metrology and information storage. No proposition has been made up to now to use the parallelism of optical imaging in quantum computing algorithms. This subject is obviously a very difficult one, but undoubtedly interesting. It requires collaborative work between the quantum computing and quantum imaging communities.

List of terms and acronyms

SQL (Standard Quantum Limit): level of noise obtained in measurements using ordinary light sources such as thermal sources or usual lasers. It is also often named as "shot noise".

References

[1] For a review, see for example: M. Kolobov *Rev. Mod. Phys.* **71** 1539 (1999), and M. Kolobov L.A. Lugiato, A. Gatti and E. Brambilla *Quantum imaging*, J. Opt. B: Quantum Semiclass. Opt. **4**, S183 (2002)

[2] N. Treps, N. Grosse, C. Fabre, H. Bachor, P.K. Lam, “The "Quantum Laser Pointer", Science **301,** 940 (2003)

[3] O. Jedrkiewicz , Y.K. Jiang, E. Brambilla, A. Gatti, M. Bache, L. Lugiato, P. Di Trapani “detection of sub-shot noise spatial fluctuations in high parametric gain down conversion” Phys. Rev. Letters **93** 243601 (2004)

[4] A. Mosset, F. Devaux, E. Lantz, "Experimental demonstration of noiseless amplification of images", preprint

[5] A. Gatti, E. Brambilla, M.Bache and L.A. Lugiato , *Ghost Imaging with thermal light: Comparing entanglement and classical correlation* Phys. Rev. Lett, **93** 093602 (2004)

[6] M. Kolobov, C. Fabre, "Quantum limits on optical resolution”, Phys. Rev. Letters **85** 3789 (2000)

[7] I.V.Sokolov, M.I.Kolobov, A.Gatti, L.A.Lugiato, *Quantum holographic teleportation*, Optics Communications, 193, 175 (2001)

Projects funded by the European Commission and related to the work in this article:

QUANTIM
Quantum Imaging
Start date: 01/01/2001
End date: 30/06/2004
Project web site: http://quantim.dipscfm.uninsubria.it/main2.html
Contact Person: C. Fabre, Ecole Normale Supérieure (fabre@spectro.jussieu.fr)

Contact information of the authors of this article:

Claude Fabre
Laboratoire Kastler Brossel
Ecole Normale Supérieure et Université Pierre et Marie Curie
Campus Jussieu case 74
75252 Paris cedex 05 France
Email: fabre@spectro.jussieu.fr
Web page: http://quantim.dipscfm.uninsubria.it/main2.html

Quantum measurement with entangled-photon states

Alexander Sergienko
Alexander Sergienko is a Resident Consultant in ELSAG spa, Genoa, Italy and a Professor of Electrical & Computer Engineering and Professor of Physics at Boston University, USA. His research interests include quantum state engineering, entanglement manipulation and processing, ultra-precise optical measurement in science and technology (quantum metrology), quantum information processing, quantum cryptography and communication. He is a Fellow of OSA and a member of APS and IEEE/LEOS.

Abstract
Two photons in a pair generated in the nonlinear process of spontaneous parametric down conversion (SPDC) are, in general, strongly entangled. Accordingly, they contain extremely strong energy, time, polarization, and momentum quantum correlations. This entanglement involving more than one pair of quantum variable has served as a powerful tool in fundamental studies of quantum theory. It is now playing a significant role in the development of novel information processing techniques and new optical measurement technologies.

Introduction
Entangled-photon states produced by the non-linear optical process of spontaneous parametric down-conversion are composed of photons that are created with strongly correlated properties that remain so even after the photons have propagated to widely separated locations in space. These strong quantum correlations, naturally present between down-conversion photons, allow for uniquely quantum mechanical and often superior forms of measurement to be performed. These quantum states are also capable of encoding information, providing robust coherence properties associated with entanglement that allow this information to be transported and transformed in unique ways. Their resistance to the decoherence phenomena that have hampered other approaches to quantum information processing has put entangled-photon optics in a position of importance in the area of quantum communication. Quantum information research has served as an excellent vehicle for developing fundamental principles of quantum mechanics creating a scientific basis for the rapid development of quantum technologies in the 21st century. The rapid development of quantum cryptography

originally initiated in academic research labs has been recently pursued by several industrial centers. The overall success in quantum science and engineering has stimulated development of multiple tools operating exclusively according to the rules of quantum mechanics. They have clear advantages over existing techniques in many areas of research and technological measurement.

Traditionally, in optical metrology absolute measurement always requires *a priori* knowledge of basic parameters of light before its interaction with a physical system. Although most physics measurements are carried out with independent particles, it is the collective nature of entangled particles that reveals the most fascinating and unexpected aspects of the quantum world. One curious aspect of the behavior of a pair of particles in an entangled state is that, though each individual particle exhibits an inherent uncertainty in behavior, the joint entity of an entangled pair can exhibit no such uncertainty. As an example, while the time of arrival of an individual particle may be totally random, an entangled pair must always arrive simultaneously. This unique aspect of entanglement leads to a self-referencing capability in timing. Similar non-classical entanglement of two photons could be demonstrated in their polarizations (spin), energies (frequency) and direction of propagation (wave vector). Such a property offers a unique tool for carrying out absolute measurements without relying on an *a priori* calibrated optical standard by making use of entangled photons. We outline the implications and significance of entanglement exploitation for the development of a new type of optical measurement - quantum optical metrology.

Entangled photons first became of great interest in probing the foundations of quantum mechanics. Debates surrounding the foundations of quantum mechanics have been ongoing since the introduction of the theory, particularly since the 1930's, with entangled-photon states often playing a central role in providing essential empirical information. Entangled states of increasingly better quality have continually been sought in order to better and better differentiate quantum behavior from classical phenomena. Entangled quantum systems are composed of at least two component subsystems and are described by states that cannot be written as a product of independent subsystem states. The nonlinear optical process known as spontaneous parametric down-conversion (SPDC) has become the most widely accepted method for creating entangled quantum states in optics. New, high-intensity sources of SPDC have been developed over the last two decades. Spontaneous parametric down-conversion of a laser photon into a pair of photons is said to be of one of two types based on the satisfaction of phase-matching conditions, as either type I or of type II, corresponding to whether the two photons of the down-conversion pair are produced with the same polarization or orthogonal polarizations, respectively. The two photons of a pair, often called signal (s) and idler (i) for historical reasons, can also leave the down-converting medium either in the same direction or in different directions, known as the collinear and non-collinear cases, respectively. (See **Figure 1**)

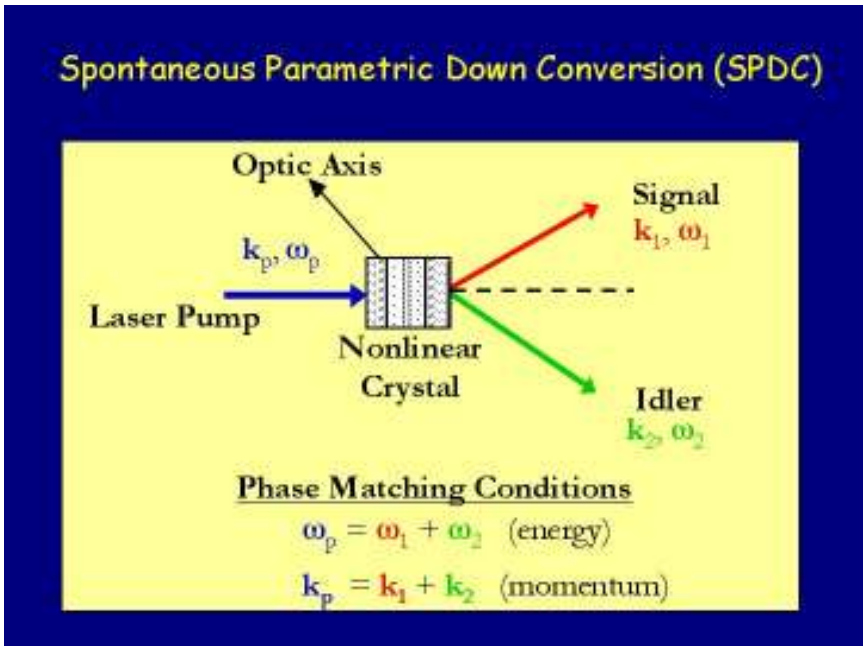


Figure 1

Spontaneous parametric down conversion (SPDC)

The medium where down-conversion takes place is usually some sort of birefringent crystal, for example, potassium dihydrogen phosphate (KDP), possessing an optical nonlinearity. Upon entrance to a nonlinear crystal, there is a small probability (on the order of 10^{-7}) that a given photon from the incident pump beam will be down-converted into a photon pair (see **Figure 1**). If down-conversion occurs, these conserved quantities are carried into the resulting photon pair under the constraints of their respective conservation laws, with the result that the phases of the corresponding wave-functions match, which are referred to as the phase-matching conditions. Down-conversion photons are thus produced in two spectral cones, one for each photon, within which two-photons appear each as a pair of photons on opposite sides of the pump-beam direction (See **Figure 1**). Entanglement between two particles involving one particular quantum variable, such as spin, was discussed by David Bohm in his famous 1954 Quantum Mechanics book [1]. In the mid-1980s, Hong, Ou and Mandel [2] created noncollinear, type-I phase-matched SPDC photon pairs in KDP crystal using an ultraviolet continuous-wave (cw) laser pump in a seminal experiment empirically demonstrating the strong temporal correlation of the two down-conversion photons. The main step in the development of practical quantum correlation and quantum entanglement tools was the development of ultra-bright sources of correlated photons and development of novel principles of entangled states engineering. This also includes entangled states of higher dimensionality and entangled quantum states demonstrating simultaneous entanglement in several pairs of quantum variables (hyper-entanglement). The successful development of such features has opened a way for quantum optical designers to the construction of optical measurement approaches that achieve higher accuracy and grater amount of information about the system under investigation in comparison with their classical counterparts.

Quantum photometry

Historically, the idea of calibrating single-photon detectors without any need for using traditional blackbody radiation sources was the first example of practical utilization of non-classical correlations between two photons produced in the nonlinear process of spontaneous parametric down conversion. (See **Figure 2**) This technique has paved the way for several other quantum measurement approaches that exploit non-classical correlation and later benefited from the full power of quantum entanglement utilization. The unique possibility of non-local self-referencing present in the optical system that is distributed in space-time is the main advantage of quantum correlation and entanglement [4].

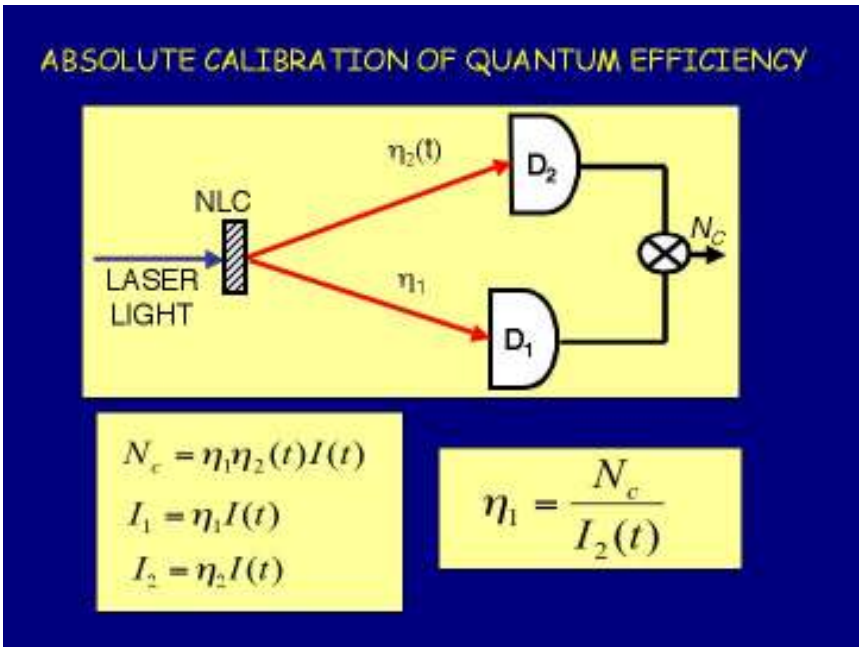


Figure 2

Using non-classical timing correlation between two photons for calibrating quantum efficiency of photodetectors

Another uniquely quantum feature lies in the spontaneous nature of the SPDC process. The probability of spontaneous photon pair creation is governed by the principles of quantum mechanics and can serve as a universal and independent reference for calibrating the optical radiation intensity and brightness (radiance) [3, 4]. The accuracy of such universal quantum referencing is limited only by the accuracy to which we know the values of major universal quantum constants. The additional significant convenience that is provided by the parametric nonlinear process consists in the possibility of accurately measuring the infrared signal brightness by detecting visible idler radiation without the need of using infrared detectors, which are usually very noisy and have low sensitivity [4]. These two approaches established foundations of new area in optical metrology – quantum photometry.

Quantum Ellipsometry

A question that arises frequently in the metrology of surfaces is the following: How does one measure reliably the reflection or transmission coefficient of an unknown sample? The outcome of such a measurement depends on the reliability of both the source and the detector used to carry out the measurements. If they both are absolutely calibrated, such measurements would be trivial. Since such ideal conditions are never met in practice, and since high precision measurements are often required, a myriad of experimental techniques have been developed over last century to circumvent the imperfections of the devices involved in these measurements. One optical measurement setting in which high-precision measurements is a necessity is ellipsometry, in which the polarization of light modification by the surface is used to study parameters of substrates, a technique established more than a hundred years ago. Ellipsometers have proven to be an important metrological tool in many arenas, ranging from the semiconductor industry to biomedical applications. They are particularly useful when the reflective properties of the material depend on its topological, geometrical, and chemical properties. Folded and unfolded protein detection in the drug discovery process and polarization scatterometry for critical dimensions evaluation in semiconductor lithography are just two examples where ellipsometry can be extremely useful these days.

Classical and quantum ellipsometry

To carry out *ideal* ellipsometry, one needs a perfectly calibrated source and detector. Various approaches, such as null (See **Figure 3** - left) and interferometric techniques, have been commonly used in ellipsometers to approach this ideal. A novel technique has recently been proposed for obtaining reliable ellipsometric measurements based on the use of twin photons produced by the process of spontaneous optical parametric downconversion (SPDC). (See **Figure 3** – right) The technique makes direct use of polarization-entangled photon pairs emitted through SPDC. This approach effectively comprises an interferometric ellipsometer, although none of the optical elements usually associated with constructing an interferometer are utilized, thanks to the power of nonlocal quantum correlations. Instead, polarization entanglement itself is harnessed to perform interferometry and to achieve ideal ellipsometry.

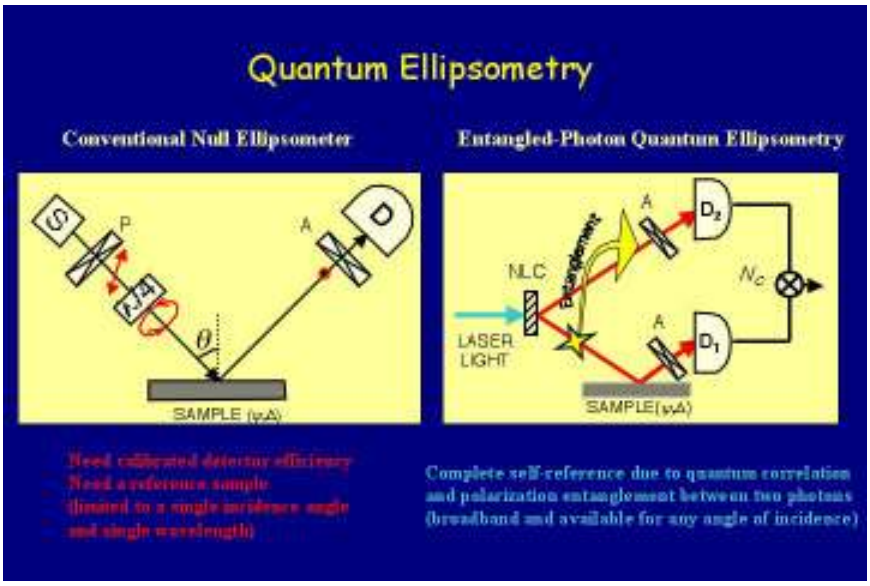


Figure 3

The theoretical foundations of single-frequency quantum ellipsometry for biophysics and nanophotonics applications have recently been developed. The first experimental implementations of correlated-photon and entangled-photon ellipsometry have indicated the potential of quantum polarization measurement [5]. Both the amplitude and phase modulation of polarized light due to surface structures are captured by the real and imaginary parts of measured polarization density matrix. Any classical approach would require performing two independent experiments to recover a similar quantity of information.

Quantum optical coherence tomography (QOCT)

Optical coherence tomography (OCT) has become a versatile and useful biological imaging technique, particularly in ophthalmology, cardiology, and dermatology. It is an interferometric scheme that makes use of a light source of short coherence time (broad spectrum) to carry out axial sectioning of a biological specimen. (See **Figure 4** – left). The axial resolution is enhanced by increasing the spectral bandwidth of the source (submicrometer resolution has recently been achieved by using a light source with a bandwidth of 325 nm). However, as the bandwidth is increased, the effects of group-velocity dispersion become increasingly deleterious for testing inner layers of tissue. Various techniques have been used in attempts to counteract the effects of dispersion, but these usually require *a priori* knowledge of the dispersion intrinsic to the specimen.

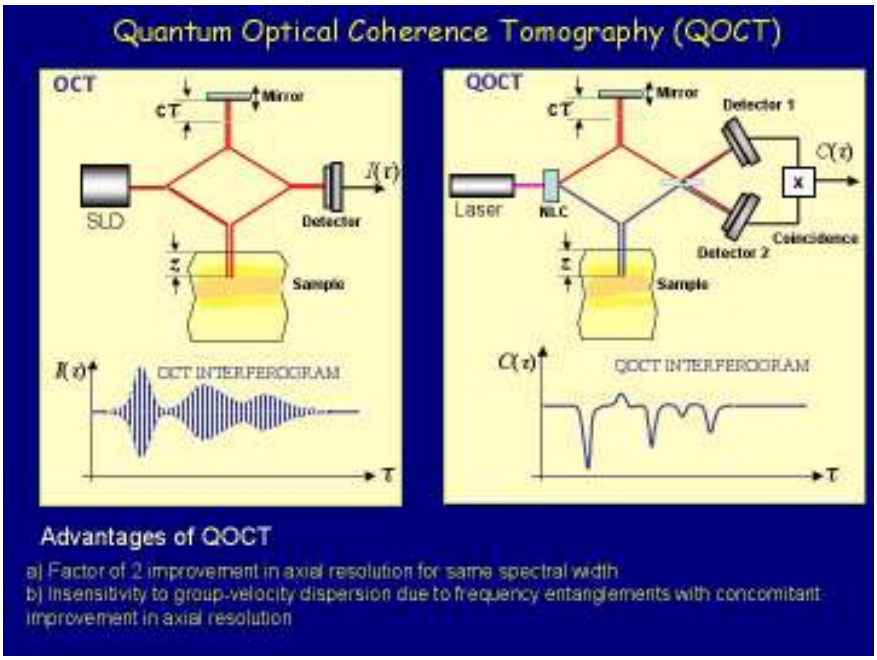


Figure 4

Conventional OCT and quantum optical coherence tomography (QOCT)

A quantum version of OCT makes use of an entangled twin-photon light source. (See **Figure 4** – right). One particular merit of quantum-optical coherence tomography (QOCT) is that it is inherently immune to dispersion by virtue of the frequency entanglement associated with the twin-photon pairs. The non-classical effect of dispersion cancellation is at the heart of QOCT approach, promising higher spatial resolution and more precise tissue modification diagnostics at the sub-micron level. Moreover, for sources of the same spectral bandwidth, the entangled nature of the twin photons provides a factor of 2 enhancement in axial resolution relative to conventional OCT. A correlated though non-entangled twin-photon light source (which is also nonclassical) is characterized by a factorizable state. Such a source would provide an intermediate enhancement in resolution of a factor of square root of 2 when the spectrum is Gaussian. However, the benefit of dispersion-cancellation does not accrue in this case. The basic physical principles of quantum version of optical coherence tomography for sub-micron biomedical imaging have recently been developed and demonstrated in a model environment [6].

Engineered entangled-photon sources

The development of integrated periodically-poled nonlinear structures has recently opened the road to the practical implementation of flexible and compact sources of entangled states. The intelligent engineering of the SPDC spectrum has enabled researchers to produce novel entangled states that have not been available from nature directly. Sources of high intensity entangled-photon flux have already revolutionized the

area of quantum cryptography, bringing it into the real world outside research labs. Because of interferometric nature of optical coherence tomography OCT, it achieves high axial resolution mainly by using the short temporal coherence length of the light source, thus allowing it to be enhanced by the use of broadband sources such as superluminescent light-emitting diodes and ultrashort pulsed lasers. For QOCT, this means that in order to become compatible and even superior in resolution for biomedical coherence imaging applications totally new entangled-photon sources with ultra high spectral bandwidth must be developed.

It has been shown that quasi-phase matching (QPM) can be used to substantially enhance the spectral width of the entangled two-photon state produced in the down conversion process, while simultaneously maintaining its specific frequency anticorrelation [7]. QPM provides a feasible alternative to conventional phase matching and QPM engineering opens up new possibilities for intelligent design of specialty entangled-photon states. The longitudinal variation of QPM period (chirping) strongly affects the spatiotemporal properties of entangled photon pairs. The merit of a longitudinally chirped QPM is that it permits many different signal and idler photon wavelengths to be phase matched at different positions inside the nonlinear crystal, broadening the spectral content of the two-photon state. Chirped QPM down conversion offers a very broadband source for dispersion-canceled QOCT, providing the sub-micron level of lateral resolution that is not degraded with penetration depth inside the tissue.

Future challenges and perspectives

The telecommunication industry is coming back from the recent downturn and has revised its plans for deployment of 40 Gb and even faster networks in the near future. This has put rather heavy pressure on optical engineers to develop high-resolution techniques for evaluating chromatic and polarization mode dispersion (PMD) with an adequate resolution. It has been shown that without identifying and carefulyl accounting for such detrimental features and without their active compensation, all future optical communication standards cannot actually function, due to dispersive spread of telecommunication signals. The use of quantum correlations has enabled the design of new, a more accurate technique for characterizing chromatic dispersion in fibers [8]. The addition of intrinsically quantum interplay between polarization and frequency entanglement in SPDC (hyper-entanglement) has given rise to a polarization mode dispersion measurement technique that utilizes the power of quantum polarization interferometry and provides an order of magnitude enhancement in the resolution of PMD measurement in comparison with the best existing devices available today [8].

The need for ultra-high resolution optical measurement is one of the novel challenges in biotechnology and semiconductor research and in industry. In several modern areas of science and technology, a clear crisis in ***non-invasive*** measurement technologies has appeared, as modern biophotonics and nanotechnology move towards creation and manipulation of ever-smaller features. For example, the dimensions of modern test proteins on a surface in drug discovery and of solid-state patterns in semiconductor manufacturing are well below the wavelength of light. The existing characterization

techniques such as fluorescent-marker visualization in biophotonics and electron scanning microscopy in nanotechnology are intrinsically invasive techniques often modifying the physical and chemical structure of the materials and altering the performance of the device after its characterization.

Optical technologies can provide non-invasive evaluation while simultaneously satisfying the constraint of smaller than the wavelength dimensions when the broad range of spectral components is employed. For example, conventional spectroscopic ellipsometry has already found its way in testing the morphology of protein samples in drug discovery and critical dimensions evaluation in nanotechnology. The use of simultaneous frequency and polarization entanglement present in SPDC leads to a unique possibility of simultaneous measurement of phase and group velocity parameters in the same experiment. With ultra-broadband spectrum of entangled sources, one can expect that the contrast and resolution of quantum spectroscopic measurement of biological objects such a folded and unfolded proteins on a surface will be superior over their classical counterparts.

The next five to seven years will see the rapid development of quantum measurement technologies. The design and characterization of novel few-qubits entangled states specifically engineered to match the requirements of quantum measurement in biophysics and modern solid-state nanotechnologies will serve as fuel for this process. One of the signs of this new century is a greater role of industrial research and development centers in pursuit of quantum technologies. The early participation of industry is facilitating future acceptance of new quantum technologies by both scientific and industrial environments and their incorporation into wide practice by developing integrated quantum measurement devices (sensors) and compact quantum circuits. The effectiveness and the future impact of quantum ideas in the world of optical measurement will strongly depend on the ease with which researchers in industry will be able to adopt rather disruptive quantum changes and incorporate novel ideas into their research and development plans.

References

[1] D. Bohm, Quantum Theory (Englewood Cliffs, NJ: Prentice Hall), (1951)

[2] C. K. Hong, Z. Y. Ou, and L. Mandel, Phys. Rev. Lett., v. 59, 2044 (1987)

[3] Review: A. V. Sergienko “Quantum Metrology With Entangled Photons”, in CXLVI International School of Physics "Enrico Fermi", T. J. Quinn, S. Leschiutta, and P. Tavella (Eds.), (IOS Press, Amsterdam ISBN 1 58603 167 8) (2001)

[4] Review: A. Migdall,"Correlated-Photon Metrology Without Absolute Standards," Physics Today **52**, 41-46 (1999)

[5] Review: A. V. Sergienko and G. S. Jaeger “Quantum Information Processing and Precise Optical measurement with Entangled-Photon Pairs”, Contemporary Physics, v. **44**, 341-356 (2003)

[6] M. B. Nasr, B. E. A. Saleh, A. V. Sergienko, and M. C. Teich “Dispersion-Cancelled and Dispersion-Sensitive Quantum Optical Coherence Tomography”, Optics Express, v. **12**, pp. 1353-1362 (2004)

[7] S. Carrasco, J. P. Torres, and L.Torner, A. Sergienko, B. E. A. Saleh, and M. C. Teich "Enhancing the Axial Resolution of Quantum Optical Coherence Tomography by Aperiodic Quasi-Phase-Matching", Optics Letters, **v. 29**, 2429-2431 (2004)

[8] N. Gisin, J. Brendel, H. Zbinden, A. Sergienko, A. Muller "Twin-photon techniques for fiber measurement", quant-ph/9807063 (1998)

Contact information of the authors of this article:
Alexander V. Sergienko
Department of Electrical & Computer Engineering
Boston University
8 Saint Mary's Street
Boston, Massachusetts 02215-2421, USA
E-mail: AlexSerg@bu.edu
Web page: http://people.bu.edu/alexserg