QIPC

QUANTUM INFORMATION PROCESSING AND COMMUNICATION

Strategic report on current status, visions and goals for research in Europe

Version 1.1, June 2005

Editing author: **Peter Zoller**
Institut für Quantenoptik und Quantenformation
Österreichische Akademie der Wissenschaften
Technikerstrasse 21 a
A-6020 Innsbruck
E-mail: peter.zoller@uibk.ac.at

Contributing authors: **Th. Beth** (Karlsruhe), **R. Blatt** (Innsbruck), **H. Briegel** (Innsbruck), **D. Bruss** (Düsseldorf), **T. Calarco** (Trento), **J.I. Cirac** (MPQ Garching), **D. Deutsch** (Oxford), **J. Eisert** (London & Potsdam), **A. Ekert** (Cambridge), **C. Fabre** (Paris), **N. Gisin** (Geneva), **P. Grangier** (Orsay), **M. Grassl** (Karlsruhe), **S. Haroche** (ENS Paris), **A. Imamoglu** (ETH Zürich), **A. Karlson** (EC Brussels), **J. Kempe** (LRI Orsay), **L. Kouwenhoven** (TU Delft), **S. Kröll** (Lund), **G. Leuchs** (Erlangen), **M. Lewenstein** (Barcelona), **D. Loss** (Basel), **N. Lütkenhaus** (Erlangen), **S. Massar** (Brussels), **J. E. Mooij** (TU Delft), **M. B. Plenio** (London), **E. Polzik** (Copenhagen), **S. Popescu** (Bristol), **G. Rempe** (MPQ Garching), **A. Sergienko** (Boston), **D. Suter** (Dortmund), **J. Twamley** (Maynooth), **G. Wendin** (Göteborg), **R. Werner** (Braunschweig), **A. Winter** (Bristol), **J. Wrachtrup** (Stuttgart), **A. Zeilinger** (Vienna), **P. Zoller** (Innsbruck)

Editing assistant: **D. Binosi** (Innsbruck)

FOREWORD

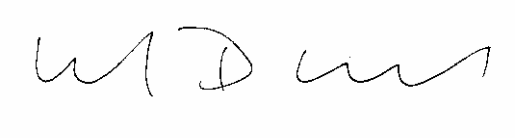
Quantum Information Processing and Communication (QIPC) is a new scientific field which opens unconventional perspectives for information processing. Quantum physics has revolutionized science in the 20th century. The exploitation of quantum effects may revolutionize information processing in the 21st 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 the conception of devices capable of performing tasks which could not be accomplished before. They may radically change the way we communicate and compute.

European scientists have been at the forefront of QIPC research since the beginning. The unit *Future and Emerging Technologies* (FET) has been very successful in attracting to the IST program the best research teams in Europe. QIPC is a proactive initiative in FP5 and FP6, as well as an important part of the FET Open scheme. This strategic report shows that the research community has been able to organize itself and to present in a comprehensive way the major challenges, visions and goals. It will determine the strategic research agenda in Europe for the next decade. This is a living document, which will be continuously revised and updated in order to serve as a guideline both to scientists and decision makers. It is a useful instrument that can help monitor and steer the program.

We are also pleased to say that at the time of printing the Nobel Committee announced the three winners of the Nobel Prize for Physics 2005. One of them is Prof. Theodor Hänch from Max-Planck Institute in Germany. He received the Nobel Prize for his research in quantum optics, which placed Europe in the lead in this field. It has triggered the development of new research areas like QIPC. We are happy to note that Prof. Hänch is actually part of the teams of two FET projects: ACQUIRE (Atomics Chips for Quantum Information Research) and ACQP (Atom Chip Quantum Processor).

The current version of the strategic report includes an extensive introduction with an overview of FET activities, national programs and the position of Europe with respect to our worldwide competitors. The main text of the document contains a scientific assessment of current results and an outlook of future efforts. It is divided in three parts corresponding to the three main research directions: quantum communication, quantum computing and quantum information science. At the end, the prospects for applications and commercial exploitation are discussed.

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



Ulf Dahlsten
Director Emerging Technologies and Infrastructures
DG Information Society and Media

1. EXECUTIVE SUMMARY

QIPC overview

Quantum Information Processing and Communication (QIPC) has the potential to revolutionize many areas of science and technology. It exploits fundamentally new modes of computation and communication, because it is based on the physical laws of quantum mechanics instead of classical physics. It holds the promise of immense computing power beyond the capabilities of any classical computer, it guarantees absolutely secure communication, and it is directly linked to emerging quantum technologies, such as, for example, quantum based sensors. The worldwide interest in the subject may be gauged by the recent significant increase of funding in quantum information technology; in particular in the United States, Canada, Australia and in some countries in Asia (see section 2.2). Europe has played a leading role in the early development of QIPC, and, given appropriate research infrastructure and suitable funding, European researchers are well positioned to maintain Europe at the forefront of the field. However, this requires a significant effort at national level and a consolidation, coordination and unification of many national projects and initiatives under one common European umbrella with the lead of the research program of the European Commission. For Europe to remain competitive in this field in the future there is an urgent need for a substantial EU-programme in QIPC.

1.1 GOALS OF QIPC RESEARCH IN THE COMING FIVE TO TEN YEARS

While QIPC belongs mainly to basic research, where key advances are often outcomes of curiosity driven research, there is nonetheless a clear set of goals for QIPC in the coming five to ten years:

Quantum Computing goals

- In quantum computing the goal for the next ten years is to develop a few-qubit general-purpose quantum processor including error correction, as a model system to demonstrate quantum algorithms and various quantum computing architectures, and with emphasis on potential scalability. While at present certain physical systems can be identified as prime candidates, it is essential to pursue this goal on a broad basis of competing approaches, allowing hybridization and cross fertilization between different fields (e.g., quantum optics, individual atoms and ions, as well as solid state). In addition, interfaces (with direct relevance for quantum communication) and model systems should be developed for connecting quantum computers in small networks. Parallel to these developments special purpose quantum computers with a few tens of qubits, or more, should be developed, e.g. to act as quantum simulators. The ultimate goal is to construct laboratory models of quantum computers which outperform classical computers on whatever nontrivial problem.

Quantum Communication goals

- In quantum communication, the short-term goal is to develop quantum cryptography towards becoming an established technology and a commercial product. A scientific goal is to demonstrate long-distance quantum communication both in optical fiber and in free space. On the 5-10 year time scale, the goals are to gain several orders of magnitude on the secret bit rate and to demonstrate quantum repeaters. The latter will require the implementation of error correction, entanglement purification, quantum interfaces and quantum memories. Each of the mentioned four requirements constitutes a serious scientific challenge. In particular, the main challenge will be the development of a quantum memory that outperforms the simple, but insufficient, «photon in a fiber loop» technique.

QIPC Theory goals

- Theory must on one hand continue to play a leading role in guiding and supporting experimental developments. On the other hand fundamental

theoretical issues must be pursued. The most important one is the formulation of a quantum information theory, a quantum counterpart to the classical theory of information, computation and communication. This implies the search for new quantum algorithms, new computational models and architectures, as well as quantum communication and entanglement manipulation protocols. A key element is a deeper understanding of entanglement in quantum theory. This includes the understanding of decoherence (an intrinsic property of quantum systems interacting with their environment), which leads to the detrimental effects of imperfections and noise. It is necessary to find ways to overcome them, for example with quantum error correction and purification. It will lead both to a deeper understanding of quantum theory per se, but it is also in direct connection to experimental implementations. Finally, the links of quantum information theory to other branches of physics must be developed, e.g. to condensed matter physics.

1.2 THE LEADING ROLE OF EUROPEAN RESEARCHERS IN QIPC

Europe as a leader in QIPC research

European researchers have been from the outset prominent in setting the agenda of, and leading, the worldwide research efforts in quantum information science, in friendly competition with similar efforts and programs in the US, Australia, Canada, Japan and China. This includes pioneering work on the foundations of the quantum theory of computation, quantum algorithms, and the discovery of entangled state quantum cryptography, which generated a spate of new research that established a vigorously active new area of physics, computer science and cryptology. Many subsequent seminal contributions, inspired by the 1994 Shor's quantum factoring algorithm, such as ways of implementing quantum computation using ion traps, quantum dots, cavity QED, optical lattices and a number of other technologies, novel computational architectures, methods of error correction and fault tolerant quantum computation originated in Europe. A unique feature and strength of European research is the broad range of activities and expertise, linking coherently efforts from experimental realization all the way to basic theoretical questions in quantum information science and quantum physics.

1.3 RECOMMENDATIONS FOR FUNDING ON THE EU AND NATIONAL LEVEL

QIPC has established itself as one of the key new multidisciplinary fields between theoretical and experimental physics, computer science and mathematics. Continued competitiveness of the EU and its member nations requires a significant effort both on the European and national level

QIPC in FP7

- QIPC must take a prominent and established position in EU research efforts, e.g. in the Seventh Framework Programme for Research of the European Commission (FP 7), and find its counterpart in national programs.

Structure of fundings

- The structure of the funding must account for the interdisciplinary character of the field, and must support a spectrum of activities across different disciplines from experimental to theoretical physics, computer sciences and mathematics.

Links with industry

- Links with industry must be developed, both on the level of possible commercial exploitation, and in research programs making new technologies available, outside the capabilities and know-how of traditional QIPC basic-research oriented laboratories. In particular, links with micro- and nano-fabrication facilities and related technology centers must be strengthened, and

QIPC spin-off new quantum technologies like quantum sensors and high precision measurement devices ought to be encouraged.

References: The US Roadmap for Quantum Computing and Quantum Cryptography is available at http://qist.lanl.gov

2. INTRODUCTION: THE MAJOR VISIONS AND GOALS OF QIPC

Classical information is no longer enough

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.

Quantum information goes beyond it

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

Quantum bits and superposition

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 parallelism

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.

The power of quantum computation

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.

Entanglement: a new resource

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.

The power of quantum communication

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.

Challenges at the quantum level

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.

Building quantum hardware

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 satisfies 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.

Harnessing decoherence in quantum communications

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 fibers and free space.

Satellite global quantum communications

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.

Quantum simulators

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.

Quantum simulators and real-world applications

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.

Scalable quantum technologies

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.

A new way of harnessing Nature

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.

3. DIFFERENT ASPECTS OF QIPC RESEARCH IN EUROPE

Quantum Information Processing and Communication (QIPC) is a vigorously active cross-disciplinary field drawing upon theoretical and experimental physics, computer science, engineering, mathematics, and material science. Its scope ranges from fundamental issues in quantum physics to prospective commercial exploitation by the computing and communications industries.

3. 1 QIPC RESEARCH IN EUROPE – EUROPEAN UNION LEVEL

Role of the FET Unit for QIPC

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 recognized by FET – the Future and Emerging Technologies part 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.

Precursors of QIPC proactive initiatives

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.

The QCEPP Pathfinder Project

During 1998 the QCEPP working group (the so-called Pathfinder Project) laid the bases for the research field of Quantum Information Processing and Communications at European level and was the first endeavor explicitly addressing 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 organizing the research community, by stimulating it to reach critical mass within a short time period and by building the support for the launch of QIPC as a Proactive Initiative.

FP5 QIPC Proactive Initiatives

In FP5 (1999–2002) FET launched QIPC as a Proactive Initiative (PI). It was implemented via 'calls for proposals' directly targeted to QIPC and a certain amount of the FET budget was reserved in advance. There were two calls for proposals and 25 projects were launched with total cost of 41 M€ and 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 organized. 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 forums give the opportunity for interactions between the members of the projects and for cross-fertilization.

FET-QIPC in FP6

In FP6 (2003–2006) QIPC continues as a FET PI. 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. If successful, the 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.

FP6 QIPC Integrated Projects

The proposed research goes clearly beyond the state-of-the-art, which confirms the strong European presence in QIPC and the progress made in the last years. 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 in Europe.

QIPC in FET-Open

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 or allows filling the time gap between dedicated QIPC calls.

ERA-Pilot QIST

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: complete and regularly update the QIPC roadmap document; elaborate a map of European research teams and expertise; collect information on national initiatives and programs; collect information on international initiatives and programs; propose coordination and synergies between national and EC initiatives; propose benchmarking; organize conferences, etc.

Quantum cryptography: a success story

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.

3. 2 QIPC RESEARCH IN EUROPE – NATIONAL LEVEL

QIPC 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. So far we know that national initiatives of a certain size are the following:

- **Austria**: QIST, consisting of University of Innsbruck, University of Vienna, Austrian Academy of Science, ARC Seibersdorf research as well as the industrial partner Siemens Austria (within the proposed ERA-Pilot represented by Academy of Science and ARC Seibersdorf research)
- **Belgium**: PHOTON – Interuniversity Attraction Pole (IUAP), funded by the federal government, coordinates research in quantum information; additional

funding of quantum information research by the Fonds National de la Recherche Scientifique (FNRS)

- **Denmark**: QUANTOP – Danish National Research Foundation Center for Quantum Optics, Universities of Aarhus and Copenhagen
- **Denmark/Sweden**: Øresund-region, consisting of the universities of Lund, Copenhagen, Aarhus and the Technical Universities in Lyngby and Göteborg.
- **France**: "National Initiative on Quantum Information", part of the "French National Program in Nanoscience".
- **Germany**: "DFG-Schwerpunkt: Quanteninformationsverarbeitung" (end 2005) and several programs by individual states.
- **Italy**: The National Research Center NEST (National Enterprise for nanoscience and nanotechnology) has been established that contains Quantum Information as well.
- **Poland**: The network of the Laboratory of Physical Foundations of Information Processing, which is coordinated by the Center for Theoretical Physics of the Polish Academy of Sciences
- **Slovakia**: Quantum information program by the Slovakian Academy of Science (Bratislava).
- **Sweden**: SSF QIP consortium, Chalmers Göteborg, and KTH, Stockholm
- **United Kingdom**: QIP IRC (Quantum Information Processing Interdisciplinary Research Collaboration), consisting of the universities of Bristol, Cambridge, Hertfordshire, Leeds, Oxford (within the QIST-consortium), Sheffield, and York, Imperial College and University College in London as well as the industrial partners Hewlett Packard, Hitachi, National Physics Laboratories, Qinetiq, and Toshiba.

Need for coordination between national and European level

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, we can keep or reach critical mass in various sub-fields. Experience and knowledge should be shared and neither efforts nor funding should be duplicated. Funding will ultimately have to concentrate efforts in sub-fields to certain geographical regions (centers of excellence) in order to achieve the highest possible impact. This need will have to be balanced with the need to keep a European dimension of research while building on already existing centers of excellence in certain areas across Europe.

3.3 QIPC RESEARCH IN THE INTERNATIONAL CONTEXT

QIPC's own identity as a research field

Quantum information processing has become a scientific discipline with its own identity during the last ten years. The advent of quantum cryptography in the 80s and then the recognition of quantum computing in the 90s, for example using Shor's algorithm, provided the motivation and have been the starting point of serious experimental and theoretical efforts to realize QIPC at large.

Europe is at the leading edge of QIPC research

Through the activities of the 2000-2004 EC FP5 FET-PI QIPC programme, Europe has, in the main, been at the leading edge of QIS worldwide. The early spearheading of this high-risk R&D effort by the EC has aided in the creation of a number of national investments in QIS with the research area now reaching a more mature stage of medium/high risk. Until now, European publication output and quality has been on a par with the US (Fig. 1), while other nations have begun systematic ramp-up in QIS

investments. To retain our leading position in research and to capitalize on the Commission's already significant investments in QIS (€35M in FP5), it is vital to ensure that the EC investment in QIS remains competitive with the US and other national/continental QIS investors. Our current intelligence indicates (see Table 1), that a Commission investment of €7M/yr. will compete very poorly with the US, who now federally invests ~$100MUSD/yr.

Country	QIS Investment (Millions)/yr		MEUROS[1]	Descriptions				
USA	100	USD	75	Sources: National Institute of Standards: C. Williams http://qubit.nist.gov/qiset-PDF/Williams.QISET2004.pdf	USARMY: http://www.aro.army.mil/research/qcbaa05.pdf	DoD/ONR MultiUniversity Research Initiatives MURI: http://www.onr.navy.mil/02/baa/docs/04_021.pdf	DARPA/NSF/ARDA/NIST/NSA/DoD(ARO,ONR,AFSOR)/NASA	FoQus: http://www.darpa.mil/dso/solicitations/sn04-08.htm http://qubit.nist.gov/FoQuS/foqus.html http://www.informationweek.com/showArticle.jhtml?articleID=20000170 http://www.itutilitypipeline.com/showArticle.jhtml?articleId=20300535&printableArticle=true
Japan	25	USD	25	Sources: ERATO Projects: http://www.jst.go.jp/erato/project/tts_P/tts_P.html http://www.jst.go.jp/erato/project/irkk_P/irkk_P.html	ICORP: http://www.jst.go.jp/inter/ongoing.htm	CREST: http://www.jst.go.jp/kisoken/crest/	PRESTO: http://www.jst.go.jp/kisoken/presto/	
Canada	20	CAD	12	Sources: 130M$CAD investment in Institute for Quantum Computing at U. Waterloo and Perimeter Institute at Waterloo, most of which is for QIS over next 6 years.	Canadian Research Chairs: http://www.chairs.gc.ca/	iCore Funding: Institute for Quantum Information Science Calgary: http://www.iqis.org/media/itm/2004-04-16ucalgary/		
Australia	10	AUD	6	Sources: Australia Research Council Centres of Excellence and Foundation Fellowships				
Europe	8[2]	€	8	Sources: See Footnote.				
Singapore	8	SGD	4	Source: Singaore's Agency for Science, Technology and Research http://www.a-star.edu.sg/astar/index.do				
China	4	€	4	Sources: Chinese Academy of Sciences: http:// www.cas.cn	National Fundamental Research Program from the Ministry of Science and Technology http://www.most.gov.cn	Ministry of Education http://www.moe.edu.cn		

[1] **(19/12/04)**

[2] Following the completion of the FP5 FET QIPC programme on 31/12/05, the only EC QIS R&D will arise from the FP6 QIPC programme and FET Open. Gauging the total expenditure in the period 2005-2009 (4 yrs), in the Integrated Project QIPC programme to be €25M and FET Open to be €8M we arrive at the above estimate.

Disclaimer: information collected by Jason Twamley, updated to the best of current knowledge and subject to possible mistakes

Funding policies and European QIPC competitiveness

Indeed, Australia, with a population of 20 million (EU population is ~450 million), will be federally investing, $8MAUS/yr. (€5M/yr.), in a coherent QIS effort through its National Centers of Excellence. Among the strongest threats to Europe's lead role in Q/NIST/IS is the US FoQuS programme. The FoQuS programme (by the US Defense Advanced Research and Projects Agency), was initially tabled in early 2004 with a specific targeting of quantum computer QIS in a single project funded to ~$90MUSD over four years, with worldwide researcher participation. This programme has not yet been fully launched but remains under consideration by the US for 2005. With the very significant international targeting of QIS ramping up around the world it is imperative that Europe remains competitive. QIS R&D support on the scale of ~€8M/year puts Europe at the lower end of worldwide QIS funding support. With such a potential decrease in international competitiveness, there is considerable risk that European research in QIS and the resulting technology developments (commercial and defense), will not be sustainable, leaving Europe reliant on importing such developed QIS technology from abroad.

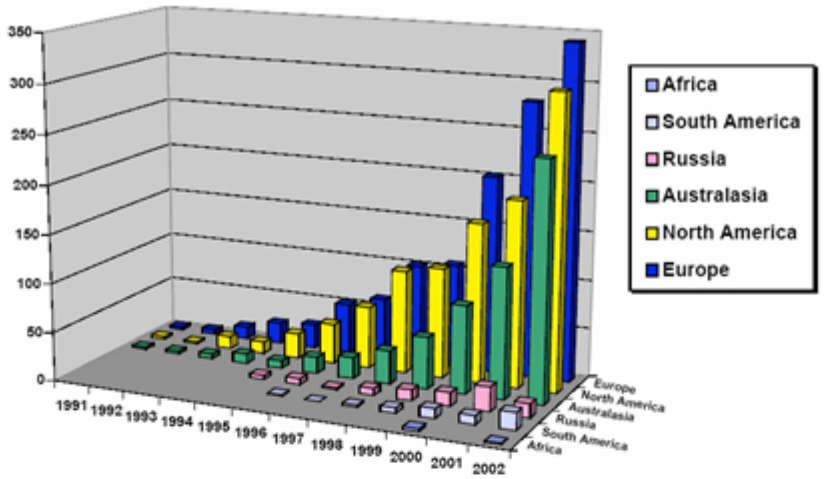


Fig.1: Number of QIS peer-reviewed publications per year and country/continent (from QUIPROCONE)

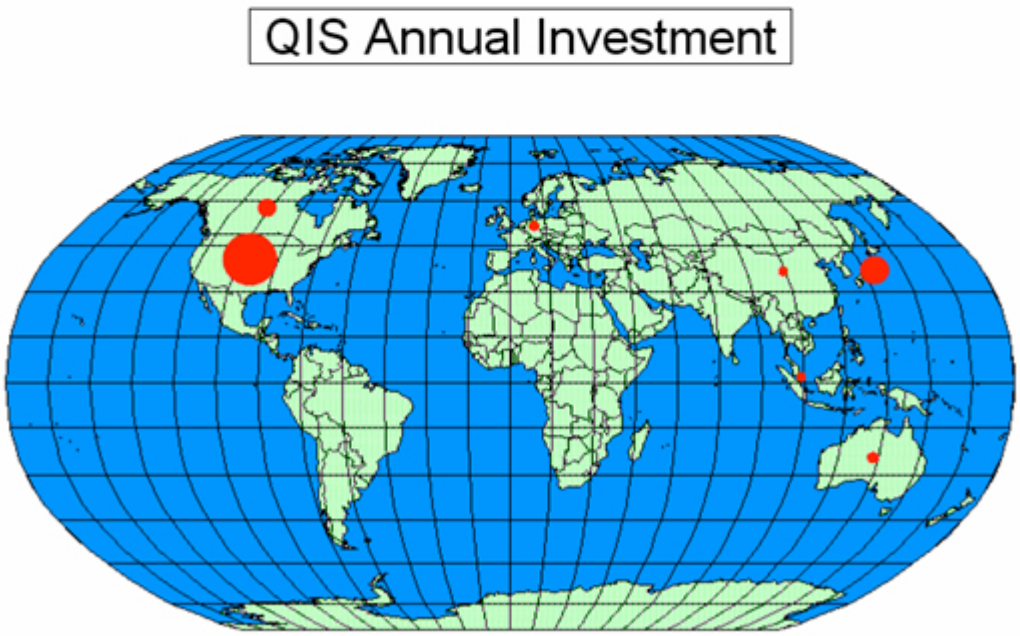


Fig.2: Worldwide investments in QIS R&D (from table above)

3.4 THE EUROPEAN FLAVOR, VISIONS AND GOALS

The broad scope of the European effort

In comparison with the international QIPC programs, the characteristics of the European effort are its broader scope, beyond the focus on specific issues like security or special applications like factoring, as for example in the US and in Australia. Moreover, there is a much stronger theoretical component and emphasis on fundamental physics. Clearly, Europe has achieved a critical mass in this much broader context of QIPC which includes both theoretical and experimental physics: atomic physics, quantum optics and laser physics, high energy and mathematical physics, condensed matter, etc., as well as from other disciplines like computer science, mathematics, material science, several areas in engineering, etc.

The European vision

The European vision is to advance quantum information processing in such a wider context which includes the spectrum from fundamental quantum physics to applications in science and engineering.

Novelty and Innovation

To remain competitive Europe should nurture QIS technology innovation from fundamental research

From basic research to spin-off technologies

One of the most challenging aspects in creating a new technology is the transition of basic research with its accompanying spin-off technologies, into more application driven research where inherently QIS based applications are researched and developed. The earliest such QIS-driven application is quantum cryptography with a number of QCrypto SMEs already in operation worldwide. General purpose quantum computation, e.g. for factoring of large integers and related applications maybe a long-term goal. But quantum memories/repeaters and multiparty QIS software, will be developed in the next five years with the potential for even greater innovation and SME/Multinational commercialisation. Although there have been efforts by the US and others to make this transition to a more innovation based QIS research community, they have not succeeded so far and Europe, through FP6 QIPC-PI, has the opportunity to begin facilitating this transition and in this way could gain at least a two-year competitive advantage over others. The particular emphasis by the project QAP to build a complete QIS R&D pipeline from fundamental research in computer science, quantum algorithms and quantum information theory through to experimental development, where the overall emphasis is to develop truly QIS based applications in the medium-term, is unique in the world. No other nation/continent has managed to create such a synergy. Some of the FET-PI QIPC Integrated Projects contain over 13% industrial partner effort and this connection to industry will be proactively targeted and ramped up over the coming five years through the cooperative efforts of FET-PI QIPC IPs. The inclusion of a variety of QIS projects, some focused on fundamental research and some focused on applications, in the FET-PI will put Europe in a strategic position worldwide.

Convergence

QIS research is expanding beyond its traditional boundaries as device complexity grows and many different physical QIS elements are integrated.

Convergence of IT towards QIS

There is a convergence of many information technologies towards QIS. Examples include, integrated photonics research both linear & nonlinear, quantum effects in nanotechnology & materials science, interfacing classical information systems with quantum-atomic systems, quantum solid-state systems, and quantum photonic-systems. Such emerging plurality of QIS is already recognized by the NSF, where QIS R&D has a presence in many Divisions of the NSF, e.g. Physics, Computer-Communication Foundations, Nanoscale Science and Engineering, and Information Technology Research Divisions. Thus, the QIS portfolio encompasses some of the E-Nano R&D effort.

European Research Area

QIS has the potential to bring the vision of a true European Research Area into being.

Potential for a standalone ERA

QIS R&D is expanding throughout Europe with significant New-States contributions (Poland/Slovakia). The European QIS research community is well organized (thanks to previous networking initiatives by the EC), and many nations will work coherently in a recently funded ERA-NET project in Quantum Information Science and Technology (ERA Pilot-QIST). The creation of truly European Research Area is essential and justifies additional funds for the QIPC programme.

3.5 FUNDING AT EUROPEAN LEVEL – PRESENT AND FUTURE ISSUES

QIPC in Europe has reached critical mass

The field of QIPC has matured in Europe during the last ten years. There is critical mass in Europe in all main areas of research. The original vision of building a general purpose quantum information processor is still far beyond our reach, but obviously it remains high on our agenda of research priorities. It is too early to pick the winner implementation for its practical realization and it is possible that the concrete technology is still to be developed. At this stage we need to keep a diversity of different approaches and funding needs in order to increase the probability of success and to ensure continuity. On the other hand other areas of QIPC like quantum information, quantum communication, quantum cryptography, quantum simulations, spin-off applications, etc., seem closer to achieving a number of landmark results. It is therefore necessary to ensure concentration of efforts, coordination of activities and appropriate funding at European level in these fields.

Need for carefully planned fundings

Funding must carefully balance between focusing on specific promising areas and topics, while being open towards a whole spectrum of existing research fields and the possibility of new ones opening up. FET has attempted to provide continuous funding for solutions which proved promising while at the same time encouraging new ideas via its Open scheme and in its proactive initiatives. The need for continuity and increase of funding necessitates commitment from the funding agencies and the active collaboration of researchers to position QIPC research in a larger strategic and political context.

Strategic documents to support policy-making

Breakthroughs of the type needed to make QIPC a reality cannot be expected to follow a precise timetable. However, there is a need at each point in time to have a clear understanding of the results obtained, the challenges and the objectives. In order to achieve the ambitious goals, funding needs to be based on an assessment of the strengths and weaknesses in present research. This will be assisted by creating and updating strategic documents integrating the following information:

- A general roadmap-type document with detailed technical assessment of the state-of-the-art, main research goals, challenges, outlook, etc. for each sub-field.
- A map of European research teams, centers of excellence, main fields of research, etc.
- A list of national and regional initiatives, funding schemes and organizations, projects, etc.
- A list of international initiatives, including funding agencies and schemes, list of projects, etc., as well as information about roadmap-type documents and reports. The main countries involved are the US, Canada, Japan, Australia, China, Korea, Singapore, etc.

An initial version should be written as soon as possible, with regular updates and improvements to follow.

Working towards a common European strategy

It is clear that QIPC research has gained an important European dimension which is crucial for its further development. Actions and activities initiated by FET aim to build a European identity and to express a unified image of the QIPC research in Europe. We need to work towards a common European strategy and goals which give rise to new opportunities. It is therefore necessary to expand and strengthen activities and funding on European level. The Seventh Framework Program (2007- 2010) is in the process of preparation. The main lines of the design of FP7 will be established during 2005. It is crucial that the QIPC research community in Europe gives input to the EC for this process.

3.6 QIPC IN A WIDER SCIENTIFIC AND TECHNOLOGICAL CONTEXT

A new paradigm for computation and communication

QIPC has arisen in response to a variety of converging scientific and technological challenges. The main one being the limits imposed on information processing by the fundamental laws of physics. Research shows that quantum mechanics provides completely new paradigms for computation and communication. Today the aim of QIPC is to understand how the fundamental laws of quantum physics can be harnessed to improve the acquisition, transmission, and processing of information. The classical theory of information and computation, developed extensively during the twentieth century, although undeniably very successful up to now, cannot describe information processing at the level of atoms and molecules. It has to be superseded by a quantum theory of information. What makes the new theory so intellectually compelling is that the results are so surprising and with so far reaching consequences.

QIPC is mature for 'out of the lab' applications

During the last ten years, QIPC has already established the most secure methods of communication, and the basic building blocks for QIPC have been demonstrated in technologically challenging experiments. Efficient quantum algorithms have been invented, and in part implemented, and one of the first non-trivial applications will be the development of quantum simulators with potential applications in, for example, material sciences. On the technological side these developments are closely related to improving atomic clocks and frequency standards.

QIPC is intrinsically multidisciplinary

Future advances in the field will require the combined effort of people with expertise in a broad range of research areas. At the same time, the new conceptual and technical tools developed within QIPC may prove fruitful in other fields, in a process of cross-fertilization encompassing a wide variety of disciplines (including, for instance, quantum statistics, quantum chaos, thermodynamics, neural networks, adaptive learning and feedback control, chemistry, quantum control, complex systems). This profoundly interdisciplinary character is one of the most exhilarating aspects of the field. Its potential is being recognized by commercial companies all over the world. A new profile of scientists and engineers is being trained to confront the challenges that lie beyond the end of the VLSI scaling. It is clear that advances in QIPC will become increasingly critical to the European competitiveness in information technology during the coming century.

Need for an early dialogue between policy, science and industry

Yet, at the moment most activities are focused on basic research in universities and there is very limited collaboration between QIPC scientists and industry. To maintain and develop competitiveness within this field in comparison to other research areas enhanced structuring and co-ordination of efforts on a European level are necessary. At the same time, a strong QIPC field ready for future industrial applications requires the involvement of relevant industry as well. In this sense an early dialogue needs to be established between science, policy, and industry in order to develop a common vision about the future of QIPC in Europe.

Potential QIPC spin-offs

QIPC is definitely centered in the realm of basic research with its own distinct goals and applications in computation, communication and information processing in all its aspects. Furthermore QIPC research will have a deep impact on several EU strategic

priorities. There is significant potential impact on technology, economics and social issues. In addition there are several spin-offs with applications in other fields of science, engineering and technology:

Quantum Key Distribution

- The rapid growth of information technology has made our lives both more comfortable and more efficient. However, the increasing amount of traffic carried across networks has left us vulnerable. Cryptosystems are usually used to protect important data against unauthorized access. Security with today's cryptography rests on computation complexity, which can be broken with enormous amounts of calculation. In contrast, quantum cryptography delivers secret crypto-keys whose privacy is guaranteed by the laws of Nature. Quantum key distribution is already making its first steps outside laboratories both for fiber based networks and also for communication via satellites. However, significant more basic research is necessary to increase both the secret bit rate and the distance. This is the field of Quantum Communication.

New computational models and architectures

- The development of quantum information theory together with the development of quantum hardware will have a significant impact on computer science. Quantum algorithms, as for example Shor's algorithm for factorizing numbers with implications for security of classical crypto-protocols, indicate that quantum computers can perform tasks that classical computers are believed not to be able to do efficiently. A second example is provided by quantum simulations far beyond the reach of conventional computers with impact on various fields of physics, chemistry and material science. In addition, QIPC is redefining our understanding of how "physical systems compute", emphasizing new computational models and architectures.

Synergy with nanotechnologies

- QIPC is related to the development of nanotechnologies. Devices are getting smaller and quantum effects play an increasingly important role in their basic functioning, not only in the sense of placing fundamental limits, but also opening new avenues which have no counterpart in classical physics. At the same time development of quantum hardware builds also directly on nanotechnologies developed for our present day computing and communication devices, and provides new challenges for engineering and control of quantum mechanical systems far beyond what has been achieved today. An example is the integration of atom optical elements including miniaturized traps and guides on a single device, capable of working as a quantum gyroscope, with extremely large improvements in sensitivity both for measuring tiny deviations of the gravitational field, as well as for stabilizing air and space navigation. In spintronics, a new generation of semiconductor devices is being developed, operating on both charge and spin degrees of freedom together, with several advantages including non-volatility, increased data processing speed, decreased electric power consumption, and increased integration densities compared to conventional semiconductor devices.

Quantum metrology

- Quantum mechanics offers to overcome the sensitivity limits in various kinds of measurements, for example in ultra-high-precision spectroscopy with atoms, or in procedures such as positioning systems, ranging and clock synchronization via the use of frequency-entangled pulses. Entanglement of atoms can help to overcome the quantum limit of state-of-the-art atom clocks which has been already reached by leading European teams. On the other hand, the quantum regime is being entered also in the manipulation of nanomechanical devices like rods and cantilevers of nanometer size, currently under investigation as sensors for the detection of extremely small forces and displacements. Another example is the field of quantum imaging, where

quantum entanglement is used to record, process and store information in the different points of an optical image. Furthermore, quantum techniques can be used to improve the sensitivity of measurements performed in images and to increase the optical resolution beyond the wavelength limit.

4. ASSESSMENT OF CURRENT RESULTS AND OUTLOOK ON FUTURE EFFORTS

4.1 QUANTUM COMMUNICATION

Quantum communication is the art of transferring a quantum state from one location to another. Quantum cryptography was discovered independently in US and Europe. The American approach, pioneered by Steven Wiesner, was based on coding in non-commuting observables, whereas the European approach was based on correlations due to quantum entanglement. From an application point of view the major interest is Quantum Key Distribution (QKD), as this offers for the first time a provably secure way to establish a confidential key between distant partners. This key is then first tested and, if the test succeeds, used in standard cryptographic applications. This has the potential to solve a long-standing and central security issue in our information based society.

While the realisation of quantum communication schemes is routine work in the laboratory, non-trivial problems emerge in long-distance applications and high bit rate systems. At present, the only suitable system for long-distance quantum communication is photons. Other systems such as atoms or ions are studied thoroughly; however their applicability for quantum communication schemes is not feasible within the near future, leaving photons as the only choice for long-distance quantum communication. One of the problems of photon-based schemes is the loss of photons in the quantum channel. This limits the bridgeable distance for single photons to the order of 100 km with present silica fibers and detectors. Recent quantum cryptography experiments already come close to such distances. In principle, this drawback can eventually be overcome by subdividing the larger distance to be bridged into smaller sections over which entanglement can be teleported. The subsequent application of so-called "entanglement swapping" and "quantum memory" may result in transporting of entanglement over long distances. Additionally, to diminish decoherence effects possibly induced by the quantum channel, quantum purification might be applied to eventually implement a full quantum repeater.

There are two media that can propagate photons: optical fibers and free space. Each of these two possible choices implies the use of the corresponding appropriate wavelength. For optical fibers, the classical telecom choices are 1300 and 1550 nm and any application in the real world of quantum communication in fibers has to stick to this choice. For free space the favored choice is either at shorter wavelengths, around 800 nm, where efficient detectors exist, or at much longer wavelengths, 4-10 microns, where the atmosphere is more transparent.

Recall that quantum physics can deliver «correlations with promises». In particular it can deliver at two locations strictly correlated strings of bits with the promise that no copy of these bits exist anywhere in the universe. This promise is guaranteed by the laws of Nature, they do not rely on any mathematical assumption. Consequently, such two strings of correlated bits provide perfect secure keys ready to be used in standard crypto-systems. However, for quantum physics to holds its promise, truly quantum objects, like photons, have to be send from one location to the other. Since quantum object interacting with the environment lose their quantumness, i.e. become classical object, it is crucial to isolate the photons during their propagation. Consequently, it is of strategic importance to develop the technology to send photons from one location to a distant one while preserving its truly quantum nature. The test of this quantumness consists in measuring the correlations and proving that they do violate a certain inequality, known as the Bell inequality.

From the present situation, where commercial systems already exist, there are three main directions to be pursued, which we review one after the other.

4.1.1 FIBER BASED SYSTEMS

Towards higher bit rates

1. Fast electronics, this includes fast sources and fast and low-loss phase modulators. This is mainly a (non-trivial) engineering problem.

2. Improved detectors: lower dark counts (<10-6 per ns), shorter dead times (<1μs), less time-jitter (<100 ps) and higher detection efficiency (>15%). This is a non trivial solid state physics challenge.
3. Invent and investigate new protocols inspired by existing and reliable components, like "decoy states" [1] and the SARG protocol [2]. Also protocols based on fast homodyne detection methods can be thought of, such as the continuous variables protocols [3]. This is mainly a matter of the physicists' imagination!
4. It is known that existing classical communication procedures and security proofs do not make optimal use of the correlations that are generated in the physical set-up and can be improved. Further improvement in secure key rate can follow from a scenario of trusted sending and receiving devices which cannot be manipulated by an eavesdropper. It would also be valuable to have security proofs easier to understand for classical cryptographers.
5. Single-photon sources have made spectacular progress in the last years [4], but it is not clear yet whether they will be able to fulfill practical needs for high repetition rates, high coupling efficiency and electronic cooling (no liquid helium). It is not even necessary to use single photon sources since also QKD with weak laser pulses can be proven to be secure; see e.g. [5]. Moreover, the performance of ideal single photon sources can also be achieved using laser pulses with a phase reference, as has been proven by a recent analysis by Koashi [6]. Fourier-transform limited single-photon sources with negligible time-jitter could also be used as building blocks for linear optics quantum computing.
6. Quantum communication with entangled states will be important to further develop quantum teleportation and entanglement swapping in view of their possible use in connection future quantum computers.

Europe has a leading role for point 6, while it is competing with the US for 3 and 4 (and also with Japan for 5). US and Japan are ahead concerning 1 and 2.

Towards longer distances

In today's system the distance is limited by the fiber loss and the detector dark-counts: at large distances the dark-counts dominate the signal. To improve the distance one can, from the simplest and less effective to the most challenging and most effective:

1. Improve the detectors: lower dark counts automatically increase the distance. However, the bit rate decreases exponentially with distance.
2. Improve the fibers: air-core photonic band-gap fibers have the potential to surpass silica fibers. (Even pure silica core photonic bandgap fibers could improve on today's telecom fibers, but only by at most 0.05 dB/km). This is a tremendous engineering challenge, with applications which would impact the whole field of optical telecommunications!
3. Use quantum relays exploiting quantum teleportation and entanglement swapping [7]. Dividing the connection in sections allows one to open the receiving detector less frequently, lowering thus the dark-count rate. For any given detector efficiency, this allows one to gain a factor of about 5 in distance. But the maximal distance is still limited and the bit rate still decreases exponentially with distance. Quantum relays require entangled photon sources. It should be stressed that quantum relays are anyway necessary for quantum repeaters. Today's longest distance demonstration is a quantum teleportation lab experiment connecting three 2 km long sections. The next crucial milestone in this direction will be a field demonstration over tens of km of entanglement swapping.
4. Use quantum repeaters: fully developed quantum repeaters have the potential of extending quantum communication to arbitrary long distances with a constant bit rate [8]. It is extremely challenging physics and still basic research. A quantum repeater requires a quantum memory. The latter has to outperform an optical fiber delay loop. This important milestone is described in section 4.1.3.

In this subfield, Europe is presently the leader; except for the first one, where the US and Japan are ahead.

Quantum continuous variables

Besides qubits, quantum continuous variables (QCV) have emerged as a new tool for developing novel quantum communication and information processing protocols. Encoding quantum continuous information into the quadrature of a light mode, or into the collective spin variable of a mesoscopic atomic ensemble, has proven to be a very interesting alternative to the standard concept of quantum bits. Several experimental breakthroughs have been achieved recently demonstrating this concept, namely the quantum teleportation of a coherent state, the preparation of distant entangled atomic ensembles, or the implementation of a quantum key distribution scheme relying on coherent states Beyond these major experimental results, a large number of theoretical ideas have appeared in the literature, proposing to use QCV for achieving dense coding, entanglement purification or distillation, error correcting codes, cloning or telecloning, memories based on light-atoms interfaces, etc. In addition, some fundamental studies have been carried out on the entanglement of multimode Gaussian states, or on the capacity of Gaussian quantum channels.

These results are stimulating more research work, with many theoretical and experimental developments, especially in the directions of improved and/or novel quantum communication and secret sharing protocols, quantum memories and quantum repeaters using the light-atoms quantum interface, and the use of squeezed, or entangled, or even non-Gaussian states of light in order to make some new information processing with continuous variables possible.

New applications and protocols

The field of quantum communication is still very young, having been essentially unknown until 10 years ago. One should expect new ideas and leave open space for basic research. From the theoretical point of view, there are several problems that have to be considered in the context of quantum communication. First of all, since the field is still very young, one should expect new applications related to both the efficiency as well as the secrecy in communications. Examples of the first can be connected to secret voting protocols, digital signatures, or fingerprinting. Examples of the second field could be, for example, connected to dense coding, or agenda protocols. Apart from that, there are still several theoretical open questions of crucial importance for quantum cryptography. They are related to the tolerance to noise of current protocols (both with one and two way communication), the connection between single photon and continuous variable protocols, and the search for more efficient and fast ways of distributing keys

Quantum communication protocols can be often understood as entanglement manipulation protocols. An important class of these protocols delivers classical data with properties derived from the underlying quantum state. For this class the question arises whether one can replace the quantum manipulation and subsequent measurement by another two-step procedure that first measures the quantum states and then performs classical communication protocols on the resulting data to complete the task. Such an implementation would be preferential in real implementation, as is illustrated in the case of quantum key distribution. It is important to study under which circumstances such a replacement can be done.

Key references

[1] W.-Y. Hwang, "*Quantum Key Distribution With High Loss: Towards Global Secure Communications*", Phys. Rev. Lett. **91**, 057901 (2003).

[2] V. Scarani, A. Acín, G. Ribordy, and N.s Gisin, "*Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations*", Phys. Rev. Lett. **92**, 057901 (2004).

[3] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf and Philippe Grangier, "*Quantum key distribution using gaussian-modulated coherent states*", Nature **421**, 238 (2003).

[4] A. Beveratos, R. Brouri, T. Gacoin, A. Villing, J.-P. Poizat, and P. Grangier, "*Single Photon Quantum Cryptography*", Phys. Rev. Lett. **89**, 187901 (2002); E. Waks, K Inoue, C. Santori, D.

Fattal, J. Vuckovic, G. S. Solomon, and Y. Yamamoto, "*Quantum cryptography with a photon turnstile device*", Nature **420**, 762 (2002).

[5] H. Inamori, N. Lütkenhaus, D. Mayers, "*Unconditional Security of Practical Quantum Key Distribution*", quant-ph/0107017, http://xxx.arxiv.org.

[6] M. Koashi, "*Unconditional Security of Coherent-State Quantum Key Distribution with a Strong Phase-Reference Pulse*", Phys. Rev. Lett. **93**, 120501 (2004).

[7] B. C. Jacobs, T. B. Pittman, and J. D. Franson, "*Quantum relays and noise suppression using linear optics*", Phys. Rev. **A 66**, 052307 (2002); D. Collins, N. Gisin, H. D. Riedmatten, "*Quantum relays for long distance quantum cryptography*", Journal of Modern Optics **52**, 735-753 (2005).

[8] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "*Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication*", Phys. Rev. Lett. **81**, 5932 (1998).

4.1.2 FREE SPACE SYSTEMS

Despite the achievements of quantum communication experiments, the distances over which entanglement can be distributed in a single section, i.e. without a quantum repeater in-between, are by far not of a global scale. Experiments based on present fiber technology have demonstrated that entangled photon pairs can be separated by distances ranging from several hundreds of meters up to 10 km in the field (and 50 km in the lab), but no improvements by orders of magnitude are to be expected. On the other hand, optical free-space links could provide a unique solution to this problem since they allow in principle for much larger propagation distances of photons due to the low absorption of the atmosphere in certain wavelength ranges. Also, the almost non-birefringent character of the atmosphere guarantees the preservation of polarization entanglement to a high degree. Free-space optical links have been studied and successfully implemented already for several years for their application in quantum cryptography based on faint classical laser pulses. Recently a next crucial step was demonstrated, namely the distribution of quantum entanglement via a free-space link, which was verified by violating a Bell inequality between two distant receivers without a direct line of sight between them.

Towards Space Quantum Communication

Terrestrial free-space links suffer from obstruction of objects in the line of sight, from possible severe attenuation due to weather conditions and aerosols and, eventually, from the Earth's curvature. They are thus limited to distances typically of the same order as the fiber links. To fully exploit the advantages of free-space links, it will be necessary to use space and satellite technology. By transmitting and/or receiving either photons or entangled photon pairs to and/or from a satellite, entanglement can be distributed over truly large distances and thus would allow quantum communication applications on a global scale.

A significant advantage of satellite links is that the attenuation of a link directly upwards to a satellite is comparable to about 5–8 km horizontal distance on ground. Proof-of-principle experiments for such distances in free space exist for weak laser pulses.

Several studies are currently underway and suggest the feasibility of space-based experiments based on current technologies [1-4].

Many of the goals to be achieved in free-space quantum communication are shared with fiber-based technology, e.g. the improvement of detectors or the development of quantum repeater technology. Additional challenges and goals are

1. Free-space distribution of entanglement over distances above 5 km.
2. Implementation of active and/or adaptive optics techniques for single photons.
3. Free-space teleportation of a single-photon state.
4. Free-space entanglement swapping.

5. Free-space quantum cryptography (with discrete or continuous variables) demonstration of single-photon uplinks to a satellite.
6. Demonstration of a single-photon down-link from a satellite.
7. Quantum cryptography between two widely separated locations on Earth via satellites.
8. Development of narrow-band sources of entangled photons for daylight operation.
9. Implementation of an entangled-photon source on a satellite.
10. Teleportation of a photon state up to a satellite.
11. Teleportation of a photon state between two ground locations via a satellite.
12. Teleportation of a photon state down from a satellite.
13. Satellite-satellite quantum communication.

Evidently this line of research necessitates both significant basic investigation as well as very specific and advanced technological development. At present various considerations and studies of feasibility are being undertaken. These focus on issues like the possible use of the existing telescopes for optical communication with satellites, e.g. OGS on Tenerife, or the requirements for satellite-based sources of photonic quantum states. Given sufficient funding it should be possible to have a first source of entangled photons on a satellite within about 10 years from now.

Key references

[1] M. Aspelmeyer, T. Jennewein, M. Pfennigbauer, W. Leeb, A. Zeilinger, "*Long-Distance Quantum Communication with Entangled Photons using Satellites*", IEEE Journal of Selected Topics in Quantum Electronics, special issue on 'Quantum Internet Technologies', Vol. **9**, 1541-1551 (2003).

[2] M. Aspelmeyer, H. R. Böhm, C. Brukner, R. Kaltenbaek, M. Lindenthal, J. Petschinka, T. Jennewein, R. Ursin, P. Walther, A. Zeilinger, M. Pfennigbauer, W. R. Leeb, Final Report, Report within ESA/ESTEC/Contract No. 16358/02/NL/SFe (2003).

[3] J. G. Rarity, P. R. Tasper, P. M. Gorman, and P. Knight, "*Ground to satellite secure key exchange using quantum cryptography*", New J. Physics **4**, 82.1-82.21, (2002).

[4] J. E. Nordholt, R. Hughes, G. L. Morgan, C. G. Peterson and C. C. Wipf, "*Present and future quantum key distribution*", Proc. of SPIE, Free-Space Laser Communication Technologies XIV, Vol. **4635**, 116–126 (2002).

4.1.3 QUANTUM INTERFACES AND MEMORY

An interface between quantum information carriers (quantum states of light) and quantum information storage and processors (atoms, ions, solid state) is an integral part of a full-scale quantum information system. In classical communication information is transferred encoded in pulses of light. The pulses are detected by photodetectors, transformed into electrical current pulses, amplified by electronics, and sent to computers, phones, etc. This transformation of light into electrical signals forms classical light-matter interface. In quantum information processing simple classical detection of light is inadequate for recording into memory, because it destroys the quantum state by adding extra noise to it. Hence a quantum interface has to be developed. Instead of direct transformation of light pulses into electrical pulses, as in classical communication, quantum state transfer of light qubits (or continuous variables) with atomic qubits (or continuous variables) has to be developed in QIPC. Certain kinds of quantum interfaces, based on cavity QED, are discussed in part 6.2 with an emphasis on computing tasks. Other kinds of quantum interfaces, such as quantum memory and long-distance quantum teleportation of long lived atomic states, are important for communication and quantum secret sharing tasks. It is obvious that long lived entanglement shared over a long distance requires transfer of entanglement from light (the long distance carrier) to atoms (the long lived objects). Such transfer can only be done via a special light-atoms quantum interface. Distant long lived entangled objects can serve

as secure "quantum identification cards". These kinds of tasks can be address via such physical implementations as atomic ensembles, which are easier to implement and to scale.

Currently various aspects of light-atoms quantum interface and memory are investigated mainly by the European groups at Copenhagen University (E. Polzik); University of Aarhus, Denmark (K. Molmer and M. Drewsen); Max Planck Institute for Quantum Optics, Garching, Germany (I. Cirac and G. Rempe); Institute for Photonic Sciences, Barcelona, Spain (M. Mitchel); University of Kaiserslautern, Germany (M. Fleischhauer); University of Heidelberg, Germany (J. Schmiedmayer); and Lab Kastler Brossel, CNRS, Paris (M. Pinard and E. Giacobino). In the US this research is primarily carried out at Harvard University (M. Lukin); Caltech (J. Kimble), University of Michigan, Ann Arbor (Ch. Monroe); and Georgia Institute of Technology, Atlanta (A. Kuzmich).

Quantum memory for light and quantum repeaters

For coherent pulses used in classical communications, a classical approach via simple detection limits the fidelity of the memory to 50%. For non-classical states the fidelity of the classical memory is even lower. Classical communications where weak pulses of light of different colors are sent in parallel (frequency multiplexing) approach quantum limits exponentially with time (at today's pace it will be reached by 2020). Hence new - quantum - approaches to memory have to be considered for both quantum and classical communications.

State of the art: Proposals for quantum memory for light have been put forward during the past decade, in Europe and in the US. Recently the first quantum memory for a weak coherent pulse has been demonstrated in Europe [1]. A quantum memory which is to be used for storage, and not for quantum processing, is based on a simple physical system consisting of a small cell filled with atomic gas at room temperature – an atomic ensemble. Demonstrated quantum state storage time of up to 4 msec corresponds to propagation time over a distance of about 1000 km. The storage cell works close to the free space propagation wavelength.

Visions and perspectives: Quantum memory provides a stored version of quantum cryptography and quantum secret sharing (in the long run, counterfeit proof bank cards, etc). It also poses a potential threat to quantum cryptography via more efficient eavesdropping protocols, and hence has to be taken seriously in quantum communication security issues. Quantum memory for light provides a necessary ingredient for quantum networks, as discussed in the next section. Future work on quantum memory based on the atomic ensemble approach should be concentrated on

1. Extending memory capabilities to single photon/qubit storage.
2. Achieving efficient retrieval of the stored quantum state.
3. Improving the fidelity of storage.
4. Quantum error correction necessary for achieving extra long storage times.
5. Memory micro-cell arrays for multi-channel storage including quantum image storage – quantum holograms.
6. Exploring other types of atomic/solid state ensembles useful for storage applications; solid-state system such as those used for slow light experiments are potentially suitable for quantum memory and should be investigated.
7. Developing probabilistic repeater schemes possibly integrated using atoms on chip technology.

European labs are presently ready to tackle each of the above strategic challenges.

Long distance atomic teleportation and repeaters

State of the art: Atomic teleportation over a distance of a fraction of a millimeter has been recently demonstrated by two groups, in Europe and in the US. Long distance teleportation of atomic states requires interface with light. A significant progress has been achieved on the way towards implementation of a repeater primarily by US groups [Monroe, Kimble and Kuzmich]. Entanglement of

atomic ensembles at a distance of half a meter has been demonstrated in Europe [2]. The technology is simple and relies on glass cells filled with atomic gas at room temperature. At present the technology is limited to near infrared wavelength suitable for free space propagation.

Vision and perspectives: Long distance deterministic teleportation will allow realization of distributed quantum networks. Extension of entanglement of atomic ensembles to up to a kilometer is possible with specially designed optical setups. For yet longer distances quantum repeaters proposed in Europe present an option. Towards this goal a combination of a repeater with entangled trapped ions will be useful. Another possible way to realize an efficient repeater is to use atomic ensemble quantum memory [1] to store one photon of an entangled pair produced by downconversion. The repeater approach may allow teleportation of atomic states over many kilometers.

Challenges and directions of future work are similar to those listed for quantum memory, i.e.:

1. Extending memory capabilities to single photon/qubit storage.
2. Achieving efficient retrieval of the stored quantum state.
3. Improving the fidelity of storage.
4. Exploring other types of atomic/solid state ensembles useful for storage applications; solid-state system, atoms on a chip.

Key research groups in Europe have been shown in the beginning of the section.

Key references

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

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

4.2 QUANTUM COMPUTING

Information processing nowadays is commonly implemented using quantities such as charges, voltages, or currents in electronic devices which operate on the basis of classical physics. Instead, Quantum Computing (QC) and more generally, quantum information processing (QIP) employ the laws of quantum mechanics for information processing. For such devices, corresponding building blocks are quantum bits (qubits) and quantum registers, and the basic gate operations are given by logical and coherent operations on individual qubits (single qubit operations) and controlled coherent interactions between two qubits (two-qubit operations) such that the state of the target qubit is changed conditional to the state of the controlling qubit.

In principle, a large scale quantum computer can be built using these primitives which must be realized by a controllable quantum system, provided the physical system meets the following requirements (DiVincenzo criteria):

1. System is comprised of well characterized qubits and allows for scalability.
2. Ability to initialize the state of the qubits.
3. System provides long coherence times, much longer than a gate operation time.
4. A universal set of gates is experimentally feasible.
5. Qubit specific measurement capability.
6. Ability to interconvert stationary and flying qubits.
7. Faithful transmission of flying qubits between specified locations.

At present, there are a number of technologies under investigation for their suitability to implement a quantum computer. No single technology meets currently all of these requirements in a completely

satisfactory way. Therefore, the ongoing research on quantum information processing is highly interdisciplinary, diverse and requires a coordinated effort to create synergies while the common goal is the implementation of a working quantum processor. While at present several approaches have demonstrated basic gate operations and are even able to prove that quantum computing has become reality with few qubits, large scale quantum computation is still a vision which requires ongoing research for many years to come.

The long-term goal in quantum computation is, of course, a large-scale quantum computer which will be able to efficiently solve some of the most difficult problems in computational science, such as integer factorization, quantum simulation and modeling, intractable on any present or conceivable future classical computer.

Therefore, the general problems to be solved for QC and QIP are in particular:

- Identification of the best suitable physical system which allows for scalability, coherence and fast implementation of QIP.
- Engineering and control of quantum mechanical systems far beyond anything achieved so far, in particular concerning reliability, fault tolerance and using error correction.
- Development of a computer architecture taking into account quantum mechanical features.
- Development of interfacing and networking techniques for quantum computers.
- Investigation and development of quantum algorithms and protocols.
- Transfer of academic knowledge about the control and measurement of quantum systems to industry and thus, acquisition of industrial support and interest for developing and providing quantum systems.

4.2.1 QUANTUM COMPUTING WITH TRAPPED IONS

A. Physical approach and perspective

Ion trap quantum computation is based on schemes devised by Cirac and Zoller [1]. A quantum register is provided by strings of ions, each representing a physical qubit. The system satisfies in principle all DiVincenzo criteria and most of the criteria have been experimentally demonstrated. While the originally proposed system is scalable in principle, practical scalability requires additional techniques such as interconnecting via photons (flying qubits) or moving one or more ions to operate as a messenger for quantum information. A more comprehensive summary of ion trap QIP is contained in the US QIST roadmap [2].

Currently, experimental ion trap QIP is pursued by 10 groups worldwide, 6 of which are located in Europe [R. Blatt (Innsbruck, A), M. Drewsen (Aarhus, Dk), P. Gill (Teddington, UK), W. Lange (Sussex, UK), A. Steane (Oxford, UK), Ch. Wunderlich (Maynooth, Ei)], 3 more groups are currently setting up ion trap experiments for QIP in Europe [J. Eschner (Barcelona, E), T. Schaetz (MPQ Garching, D), F. Schmidt-Kaler (Ulm, D)].

On the theory side there is J.I. Cirac (MPQ Garching, D), K. Molmer (Aarhus, DK) and P. Zoller (Innsbruck, A)

B. State of the art (November 2004)

With trapped ions, qubits are implemented using either two levels out of the Zeeman- or hyperfine manifold or employing a forbidden optical transition of alkaline earth, or alkaline earth-like ions. The DiVincenzo criteria are currently met as follows:

1. Strings of two and three trapped ions are routinely loaded to a linear trap.
2. Ion strings can be cooled to the ground state of the trapping potential, and thus are prepared for implementing the Cirac-Zoller scheme. Using various techniques of individual ion manipulation, the register can be initialized to arbitrary internal and external states.

3. Qubit decay times for individual hyperfine qubits of more than 10 minutes have been observed, however, this requires magnetic-field "insensitive" transitions. For optical transitions, decoherence is limited by spontaneous decay which, however, is orders of magnitudes slower than a single gate operation.
4. Individual ion manipulation (pulsed Rabi oscillations), as well as two-qubit gate operations (Cirac-Zoller gate, geometric phase gate) have been demonstrated.
5. State-sensitive light scattering (observation of quantum jumps) is routinely used with trapped ions and detection efficiencies of more than 99.9% are readily obtained.
6. For converting stationary (ion) qubits into flying (photon) qubits, the techniques of cavity quantum electrodynamics (CQED) are used and several experiments are currently under way, no results are available at this time.
7. Faithful transmission of photonic qubits between two quantum computer nodes was theoretically shown to be feasible; a transfer protocol is available, however, at this time no experimental work is carried out yet. Instead, over short distances, and for the transfer of quantum information within a quantum processor, ions can be moved and/or teleportation protocols may be used.

C. Strengths and weaknesses

At present, ion trap QIP provides most of the requirements for first-generation quantum computation experiments. In particular, the long coherence times of the ionic two-level systems provide a robust quantum memory. Moreover, the near-unity state detection and the availability and operability of a universal set of gate operations make it already a test-bed for small-scale quantum computation. Furthermore, techniques to build large-scale ion trap quantum computers were outlined and their function was shown in first steps.

On the downside, motional decoherence by stochastically fluctuating fields (originating from trap electrodes) is not completely understood and must be reduced. Spontaneous emission must be avoided by all means; therefore decoherence-free subspaces need to be explored. Current technical constraints, such as the availability of laser sources, their respective stability and purity as well as fast optical detection and switching, need to be improved.

However, aside from the technical difficulties of scaling ion trap QIP up to larger devices, there is no fundamental problem in sight.

D. Short-term goals (next 3-5 years) (cf. also [2])

- Improve coherence of qubits by using magnetic field "insensitive" transitions, or decoherence free subspaces (for optical qubits).
- Reduce trap size and thus increase speed of operations.
- Identify and reduce sources of motional decoherence (needed for smaller traps).
- Implement error correction with 3 and 5 qubits, correct for phase and spin flip errors.
- Develop an "ion chip" as the basic building block for scaling ion trap QIP.
- Improve laser intensity and phase stability to reach fault-tolerant limits.
- Realize a "logical" qubit including error correction, i.e. encode a stable logical qubit in 5 physical qubits ("keeping a logical qubit alive").
- Interface stationary and flying qubits.
- Demonstrate more quantum algorithms.
- Logical qubit operations (single L-qubits operations, gates between L-qubits).
- Identify an optimal ion.

E. Long-term goals (2010 and beyond) (cf. also [2])

- Develop ion chips with integrated optics and electronics.
- Operations with several L-qubits.
- Fault-tolerant operations with multiple qubits.

F. Key references

[1] J.I. Cirac and P. Zoller, *"Quantum computation with cold trapped ions"*, Phys. Rev. Lett. **74**, 4091 (1995).

[2] D. Wineland, *"Ion trap approaches to quantum information processing and quantum computing"*, in 'A Quantum Information Science and Technology Roadmap, Part 1: Quantum Computation', Version 2.0, section 6.2 and references therein; available from http://qist.lanl.gov.

4.2.2 ATOMS AND CAVITY QED

A. Physical approach and perspective

Neutral-atom based systems are so far the only systems for QIPC in which both a significant control over few-particle system has been obtained and realizations of large-scale systems are already present in the laboratory. Neutral-atom systems provide excellent intrinsic scalability because the properties of an ensemble of atoms do not dramatically differ from an individual atom. Quantum information with neutral atoms therefore provides a unique opportunity to test and develop experimentally relevant QIPC schemes for large-scale systems.

All QIPC schemes based on neutral atoms employ a quantum register with trapped atoms carrying quantum information in internal atomic states. The schemes differ, however, in the way individual qubits are coupled during a gate operation. The schemes can roughly be divided into two categories:

- Firstly, a gate operation is performed by means of a controlled collision of two qubits. Such collisions require the preparation of a well-defined quantum state of atomic motion, as can be achieved by either cooling single atoms into the ground state of the trapping potential (bottom-up approach), or by loading a Bose-Einstein condensate into an optical lattice (top-down approach). Both the bottom-up and the top-down approach offer the possibility of a massive parallelism, with many pairs of atoms colliding at once. The top-down approach is ideal to develop a quantum toolbox for simulating nontrivial many-body systems.
- Secondly, a gate operation is performed by exchanging a photon between two individual qubits. Such a scheme can be implemented with free-space atoms emitting photons in a random direction (probabilistic approach), or with atoms in high-finesse cavities where the strong atom-photon coupling guarantees full control over photon emission and absorption (deterministic approach). The latter approach is realized either with Rydberg atoms in microwave cavities or with ground-state atoms in optical cavities. If each atom resides in its own cavity, the scheme guarantees addressability and scalability in a unique way. As quantum information is exchanged via flying photons, the individual qubits of the quantum register can easily be separated by a large distance. The photon-based scheme is therefore ideal to build a distributed quantum network.

In principle, the two schemes of implementing gates can be combined in one-and-the-same setup, for example by using atoms trapped in micro-magnetic potential wells produced by micron-sized current carrying wires or microscopic permanent magnets deposited on a chip. Such atom-chips are very promising building blocks for quantum logic gates because of their small size, intrinsic robustness, strong confinement, and potential scalability.

Besides performing discrete gate operations according to a predefined algorithm, neutral-atom systems are ideal for simulating quantum many-body systems. In general, quantum systems are very hard to simulate, given the fact that the dimension of the corresponding Hilbert space grows exponentially with the number of particles. This hinders our ability to understand the physical properties of general

materials with a classical computer. However, using a quantum computer, it should be possible to simulate other quantum systems in a very efficient way.

Currently, both schemes of performing a gate operation with neutral atoms (collision or photon-exchange) are investigated experimentally in several dozen laboratories worldwide, about half of them located in Europe. The European groups working with a controllable number of atoms include I. Bloch (Mainz, D), T. Esslinger (Zurich, CH), P. Grangier (Orsay, F), S. Haroche (Paris, F), D. Meschede (Bonn, D), G. Rempe (Garching, D), H. Walther (Garching, D), and H. Weinfurter (Munich, D). Several other groups are presently setting up new experiments, including W. Ertmer (Hanover, D), E. Hinds (London, UK), J. Reichel (Paris, F), and J. Schmiedmayer (Heidelberg, D). The experimental program is strongly supported by implementation-oriented theory groups like H. Briegel (Innsbruck, A), K. Burnett (Oxford, UK), J. I. Cirac (Garching, D), A. Ekert (Cambridge, UK), P. L. Knight (London, UK), M. Lewenstein (Barcelona, E), K. Mølmer (Aarhus, Dk), M. B. Plenio (London, UK), W. Schleich (Ulm, D), P. Tombesi (Camerino, I), R. Werner (Braunschweig, D), M. Wilkens (Potsdam, D), and P. Zoller (Innsbruck, A). In fact, European theory groups have played a crucial role in the development of QIPC science from the very beginning. The close collaboration between experiment and theory in Europe is unique, partly because of the support provided by the European Union.

B. State of the art

The strength of using neutral atoms for QIPC is their relative insensitivity against environmental perturbations. Their weakness comes from the fact that only shallow trapping potentials are available. This disadvantage is compensated by cooling the atoms to very low temperatures. So far, several different experimental techniques to control and manipulate neutral atoms have been developed:

Optical tweezers and arrays of optical traps are ideal to perform collisional gates:

1. Bottom-up approach:
   - Single atoms were trapped with a large aperture lens, thus providing a three-dimensional sub-wavelength confinement.
   - Single atoms were also loaded into the antinodes of a one-dimensional standing wave, and excited into a quantum superposition of internal states.
   - This superposition was preserved under transportation of the atoms, and coherent write and read operations on individual qubits were performed.
   - Moreover, a small number of atoms were loaded into a two-dimensional array of dipole traps made with a microlens array, and the atoms were moved by moving the trap array.
2. Top-down approach:
   - Single atoms were loaded into the antinodes of a three-dimensional optical lattice, by starting from a Bose-Einstein condensate and using a Mott transition.
   - A highly parallelized quantum gate was implemented by state-selectively moving the atoms, and making them interact using cold collisions. This landmark experiment has pioneered a new route towards large-scale massive entanglement and quantum simulators with neutral atoms.

Cavity QED, possibly in combination with optical dipole traps, is the most promising technique for realizing an interface between different carriers of quantum information:

1. Probabilistic approach in free space:
   - A single trapped atom has been entangled with a single photon.
2. Deterministic approach using microwave cavities: Circular Rydberg atoms and superconducting cavities are proven tools for fundamental tests of quantum mechanics and quantum logic:

- Complex entanglement manipulations on individually addressed qubits with long coherence times have been realized.
- Gates have been demonstrated.
- New tools for monitoring decoherence of mesoscopic quantum superpositions have been developed.

3. Deterministic approach with optical cavities:
   - The strong atom-photon coupling has been employed to realize a deterministic source of flying single photons, a first step towards a true quantum-classical interface.
   - With single photons, two-photon interference effects of the Hong-Ou-Mandel type have been observed. These experiments demonstrate that photons emitted from an atom-cavity system show coherence properties well suited for quantum networking.
   - Moreover, single atoms were optically trapped inside a cavity.
   - A novel cooling technique avoiding spontaneous emission was successfully implemented.

Atom chips: The ability to magnetically trap and cool atoms close to a surface of a micro-fabricated substrate has led to an explosive development of atom chips in the past few years. The main achievements include:

1. Cooling of atoms to quantum degeneracy (Bose-Einstein condensation).
2. Transport of an ensemble of atoms using a magnetic conveyor belt.
3. Manipulation of atoms with electric and optical fields.
4. Very long coherence times by using appropriate qubit states.
5. Multilayer atom chips with sub-μm resolution and smooth magnetic potentials.

All of the achievements reported in this section have been realized within European labs, and in many cases they are purely European achievements, in the sense that they are not to be found in labs outside Europe.

C. Present challenges

Most neutral-atom systems have not yet demonstrated two-qubit operations, and some of them not even a single-qubit operation, mainly because the technology to perform single-atom experiments is relatively new (less than 10 years).

Optical tweezers and arrays of optical traps are most advanced in manipulating neutral-atom qubits.

1. In the bottom-up approach, the main challenges are first to implement a two-qubit quantum gate, e.g., using a controlled collision of two atoms, and then to increase the size of the quantum register to more than 2 atoms.
2. In the top-down approach, full addressability of each individual qubit of the closely spaced register is one of the main challenges.
3. In both approaches, the speed of a gate must eventually be increased by implementing a collision which exhibits a large cross section, for example by involving Rydberg atoms or molecular (e.g., Feshbach) interactions.

Cavity QED: The main difficulty in implementing QIPC protocols in present demonstration experiments is the enormous technological complexity required to obtain full control over both atoms and photons at the single-particle level.

1. The probabilistic approach suffers from the low efficiency of photon generation and detection, and the large solid angle of photon emission for a free-space atom.
2. The deterministic approach employing microwave cavities has intracavity-photon generation and absorption efficiencies close to 100%, and the implementation of simple algorithms is in view.
    - One of the main challenges is the demonstration of scalability. The preparation of a non-local entangled and possibly mesoscopic quantum state shared between two remote cavities is a major task.
    - Another challenge is the realization of quantum feedback or error correction schemes to preserve the quantum coherence of the field stored in a cavity with a finite quality factor.
3. The deterministic approach utilizing optical cavities has led to photon-emission efficiencies of up to about 30 %. Challenges are
    - To entangle in a deterministic manner a single atom with a single photon,
    - and to teleport the quantum states between distant photon-emitting and photon-receiving atoms.
    - In order to integrate individual quantum-network nodes into a scalable quantum-computing network, a set of individually addressable atoms located in different cavities must be implemented.
    - Moreover, single-photon quantum repeaters which are necessary to communicate quantum information over large distances need to be developed.
    - Ultimately, the gate speed should be increased by installing a few-wavelength long cavity. The combination of such a micro-cavity with presently available trapping and cooling techniques is a challenge.

In both the microwave and the optical domains, a method of deterministically transporting single atoms in and out of a cavity, for example by means of an optical conveyor belt, is needed to address the individual atoms of a stationary quantum register.

Atom chips: Despite their recent achievements, experiments with atom chips are still facing a large number of challenges for implementing QIPC.

1. An efficient scheme to address, manipulate and detect a single qubit in the microtrap of an atom chip must be developed.
2. A quantum memory, that is the reading and writing of quantum information into single atoms or atomic ensembles must be realized.
3. Next, a two-qubit quantum gate, for example by employing a controlled collision, must be implemented.
4. The full demonstration of the potential provided by atom chips requires the realization of large-scale integration, e.g., with several 10 qubits.
5. Potential roughness very close (μm) to micro-fabricated structures is of concern for qubit storage and transport. Even though for current-carrying structures the problem can be solved and compensated for by the design and fabrication methods as developed recently, micro-structures with fewer defects might be needed for permanent magnets.
6. Merging atom-chip technology and cavity QED is promising. High-finesse miniature optical or microwave cavities can be coupled to ground state or Rydberg atoms trapped on a chip. Coherence preserving trap architectures are an important first step towards a fully scalable architecture combining the best of both worlds.

All of the strategic challenges in this section represent current or planned activity at European labs.

D. Key references

A tutorial review on QIPC with atoms, ions and photons can be found in, e.g.:

[1] C. Monroe, "*Quantum Information Processing with Atoms and Photons*", Nature **416**, 238-246 (2002).

[2] J.I. Cirac and P. Zoller, "*New Frontiers in Quantum Information with Atoms and Ions*", Physics Today 38-44 (March 2004).

4.2.3 SUPERCONDUCTING CIRCUITS

A. Physical approach and perspective

Quantum computation with superconducting circuits exploits the intrinsic coherence of the superconducting state, into which all electrons are condensed. Quantum information is stored in the number of superconducting electrons (charge qubit), in the direction of a current (flux qubit) or in oscillatory states (phase qubit). Systems are fabricated with thin film technology and operated at temperatures below 100 mK. Measurements are performed with integrated on-chip instruments. Coupling between qubits can be made strong. In principle the system is scalable to large numbers. The US QIST roadmap gives more detailed information and references, though not quite up to date [1]. A general background is provided in [2].

Approximately 30 groups work on superconducting quantum bits in Europe, Japan, China and the USA. European groups in experiments are: D. Esteve and D. Vion (Saclay, F), J. Rooij and H. Harmans (Delft, NL), P. Delsing (Chalmers, S), A. Zorin (PTB, D), E. Ilichev (Jena, D), A. Ustinov (Erlangen, D), F. Hekking, O. Buisson (Grenoble, F), J. Pekola (Helsinki, FI), S. Paroanu Jyväskyla, FI), D. Haviland (KTH, Stockholm, S) (and others. In theory: G. Schön, (Karlsruhe, D), R. Fazio (Pisa, I) A. Wilhelm (München, D), G. Wendin (Chalmers, S), M. Grifoni (Regensburg, D), G. Falci (Catania, I), K. Bruder (Basel, CH), and others.

B. State of the art (November 2004)

1. Qubits can be readily fabricated with suitable parameters. Small variation of qubit parameters can be achieved.
2. Initialization proceeds by relaxation into the ground state before quantum operations start.
3. Single qubit operations are performed with microwave pulses or DC pulses.
4. 1-pulse Rabi oscillations and 2-3 pulse Ramsey or spin-echo signals have been realized.
5. Decoherence times of several microseconds have been observed, shortest time needed for a basic quantum operation is several nanoseconds.
6. a) With charge 2-qubit systems a controlled-not gate has been realized with DC pulses. b) The presence of coupling has been demonstrated in flux qubits with spectroscopy.
7. Strong coupling, allowing exchange of a single photon, has been achieved between a harmonic oscillator and a qubit in two different types of qubit.
8. Rabi oscillation between two Josephson junction qubits has been achieved, and simultaneous single-shot readout has been performed to detect the anticorrelations in a Bell state.

All of these results have been achieved within Europe, apart from 6.a) (Japan) and 8 (USA).

C. Strengths and weaknesses

Strengths:

- High potential for scalable integrated technology.
- Strong coupling between qubits possible.
- Flexible opportunities with different qubit types.

- Mature background technology, 20 years of experience.
- Driver of applications in solid-state quantum engineering.
- Long history of pushing the limits of measurement towards quantum limits.
- Low-temperature or superconducting technologies necessary for integration with solid state microtraps for hybrid systems.

Weaknesses:

- Coherence limited by defects in tunnel barriers.
- Slight variation in qubit parameters associated with fabrication.

D. Short-term goals (next 3-5 years)

- Realize reliable two-qubit gates in all types of qubits.
- Realize non-destructive single shot readout of individual qubits in multi-qubit circuits
- Improve fidelity of operation and readout.
- Investigate and eliminate main sources of decoherence.
- Develop junctions with lower 1/f noise.
- Realize fully controllable three-qubit clusters within a generally scalable architecture.
- Develop switchable coupling between qubits.
- Realize systems of multiple qubits coupled through common harmonic oscillator buses – solid-state cavity QED.
- Demonstrate teleportation and rudimentary quantum error correction.
- Make first experimental tests of quantum algorithms with 3-5 qubits.

All of the above goals are among the priorities and can be achieved by European labs.

E. Long-term goals (2010 and beyond) (cf. also [2])

- Develop multi-qubit circuits (5-10 or more).
- Improve fidelity to the level needed for large-scale application.
- Develop interfaces to microwave and optical transmission lines.
- Develop interfaces for hybrid solutions to long term storage and communication.

All of the above goals are among the priorities and can be achieved by European labs.

F. Key references

[1] T.P. Orlando, "*Superconducting approaches to Quantum Information Processing and Quantum Computing*", in 'A Quantum Information Science and Technology Roadmap, Part 1: Quantum Computation', Version 2.0, section 6.7 and references therein; available from http://qist.lanl.gov.

[2] D. Esteve, "*Superconducting qubits*", in 'Proceedings of the Les Houches 2003 Summer School on Quantum Entanglement and Information Processing', (D. Esteve and J.-M. Raimond, editors), Elsevier (2004).

4.2.4 SEMICONDUCTOR QUANTUM DOTS

A. Physical approach and perspective

III-V Semiconductor heterostructures (e.g. GaAs, InP, InAs, etc) form the backbone of today's opto-electronics combining ultrafast electronics (e.g. HEMT), low-power optics together with the conversion

between electronics and optics. The industrial development of this material class has also been fruitfully utilized in the field of QIPC. Employing nanofabrication and/or self-assembling techniques, quantum dots have been defined that can be addressed electrically and/or optically. The emerging field of quantum opto-electronics can provide an interface between solid state qubits and single-photon quantum optics.

Currently, quantum dot (QD) spin based quantum information processing (QIP) is pursued by 10 groups worldwide, 5 of which are located in Europe [L. Kouwenhoven (Delft, NL), K. Ensslin (ETH-Zurich, CH), G. Abstreiter (TU-Munich, D), Ch. Bayer (Dortmund, D) and A. Imamoglu (ETH-Zurich, CH)], as well as D. Loss (Basel, CH) on the theory side.

B. State of the art (November 2004)

The quantum dot qubits being developed in III-V semiconductors are based on the charge or spin properties of single electrons. Stable and reproducible quantum dots have been developed using split-gate techniques that can be loaded with exactly zero, one or two electrons. Electrical signals in the kHz to GHz range allow one to transfer reliably an individual electron from one quantum dot to another (Delft result). Circuits of such quantum dot devices form the basis for the Loss-DiVincenzo proposal (Basel result) exploiting the electron spin as the qubit degree of freedom. In this scheme the electron charge is used for manipulation of the carriers. The spin dynamics is largely decoupled from the charge motion and remains coherent over long time scales. An important aspect of the Loss-DiVincenzo proposal is the full on-off control over the two-qubit interaction. In split-gate quantum dots this control via the spin-spin exchange interaction can be realized simply by switching electrical gate voltages. Charged qubits were also discussed by the Oxford group, and served as a model for early implementations of quantum logic gates.

The current status in the field is the realization of highly controllable quantum dots in various labs. (The material and nanofabrication flexibility is certainly strong in this QIPC approach.) The spin qubit states as well as the two qubit superposition states are easily resolved in transport measurements. An all-electrical readout of individual spins (e.g. single shot measurements) has been realized (Delft result). An ensemble average provides values for the spin life time of the order of milliseconds. It is important to note that these values are measured in an electrical circuit with all components activated and thus they include the effects from a realistic back-action (Delft result).

Quantum dots are often referred to as artificial atoms. Some of the fundamental atom-like properties of optically active quantum dots, such as photon antibunching and presence of absorption/emission lines predominantly broadened by radiative recombination, have already been confirmed experimentally. In contrast to atoms and electrically-defined quantum dots discussed earlier, optically active quantum dots suffer from spatial and spectral inhomogeneity; i.e. each quantum dot has an energy and location that is a priori impossible to be determined with reasonable accuracy. This property has important but not necessarily negative consequences for their applications in quantum information processing.

Arguably, the most successful application of quantum dots in quantum information processing has been the realization of high-efficiency single-photon sources (first results from Imamoglu et al., now at ETH Zurich). The fact that quantum dots exhibit no center-of-mass motion and that they can be embedded in nano-cavity structures with ultra-small mode volumes, enabled generation of a train of optical pulses that never contain more than a single photon, with efficiency exceeding 30%. In addition to potential applications in unconditionally secure quantum key distribution, such a source could also be used to produce indistinguishable single- photon pulses that form the backbone of linear optics quantum information processing schemes.

Cavity QED has been a central element in many quantum optics based quantum computation proposals. Recently, three groups have reported the observation of strong-coupling regime for a single quantum dot embedded in a nano-cavity structure (Würzburg result). While these experiments relied on a random spatial and spectral coincidence between the quantum dot and cavity modes, recent advances in growth and processing have demonstrated that it is possible to deterministically locate a single quantum dot at the anti-node of a photonic crystal nano-cavity structure which is in turn spectrally resonant with the quantum dot exciton line (ETH Zurich result).

The progress in optical manipulation of quantum dot spins has been relatively slow. Deterministic charging of a single quantum dot with a single excess electron has been demonstrated by several groups. More recently, resonant laser transmission measurements on a single charged quantum dot have been used to demonstrate spin-selective optical absorption, or equivalently, Pauli-blocking of optical transitions (LMU and ETH-Zurich result).

C. Short-term goals (next 3-5 years)

- For Rabi oscillations of the one qubit spin states, on-chip ESR striplines are being developed. Such experiments are necessary for determining the T2 spin coherence. This material system then allows for further optimization of the coherence properties, for instance via making full use of the quantum Hall effect regime and further reduce the phase space for decoherence (these goals are within reach in the Delft lab).
- All-optical single-spin measurements based on Pauli blocking are likely to be observed within the next 2 years. The next step would then be conditional spin dynamics between two quantum dots that are coupled via spin-selective dipole-dipole interaction. This would represent a major step for implementing quantum information processing in optically active quantum dots.

D. Long-term goals (2010 and beyond)

III-V Semiconductors are unique in their conversion capabilities between electrons and photons. Recently this conversion has been demonstrated at the level of single electrons and single photons. For instance, electrically-controlled single photon sources (i.e. electroluminescence) have been realized (results from Cambridge, UK). Also the reverse route has been shown where light controls the generation of single electrons (results from Munich). In one such single-particle photoconductivity measurement the lifetime of an electron spin trapped in a self-assembled quantum dot was shown to exceed 20 milliseconds. The magnetic field dependence was in excellent agreement with theory (based on spin-orbit interaction).

The opto-electronic properties of III-V semiconductor quantum dots can already find applications on a mid-term timescale. There are proposals for quantum repeaters (i.e. necessary devices in long distance quantum communication) based on III-V semiconductors. Repeaters generally require small qubit circuits capable of Bell state measurements and storage of a quantum state in combination with single photon detectors and emitters. A recent scheme [6] shows that even with low efficiency, high fidelity can be reached in long-distance communication.

E. Key references

[1] D. Loss and D. DiVincenzo, "*Quantum computation with quantum dots*", Phys. Rev. **A 57**, 120–126 (1998).

[2] J. M. Elzerman, R. Hanson, L. H. Willems Van Bereven, B. Witkamp, L. M. Vandersypen, and L. P. Kouwenhoven, "*Single-shot read-out of an individual electron spin in a quantum dot*", Nature **430**, 431 (2004).

[3] M. Kroutvar, Y. Ducommun, D. Heiss, M. Bichler, D. Schuh, G. Abstreiter, and J. J. Finley, "Optically programmable electron spin memory using semiconductor quantum dots", Nature **432**, 81 (2004).

[4] A. Högele, M. Kroner, S. Seidl, and K. Karrai, M. Atatüre, J. Dreiser, and A. Imamoglu, A. Badolato, B. D. Gerardot, and P. M. Petroff "*Spin-selective optical absorption of singly charged excitons in a quantum dot*", cond-mat/0410506.

[5] J. P. Reithmaier, G. Sek, A. Löffler, C. Hofmann, S. Kuhn, S. Reitzenstein, L. V. Kelfysh, V. D. Kulakovskii, T. L. Reinecke, and A. Forchel, "*Strong coupling in a single quantum dot-semiconductor microcavity system*", Nature **432**, 197 (2004).

[6] L. Childress, J. M. Taylor, A. S. Sorensen, M. D. Lukin, "*Fault-tolerant Quantum Communication Based on Solid-state Photon Emitters*", quant-ph/0410123, http://arxiv.org.

4.2.5 LINEAR OPTICS QUANTUM COMPUTATION

A. Physical approach and perspective

Optical quantum computing (OQC) exploits measurement-based quantum computing schemes with photons as physical qubits. The interaction between separate photonic qubits is induced by measurement, as opposed to a direct interaction via nonlinear media. The two main physical architectures for OQC are based on proposals by Knill, Laflamme and Milburn [1], the KLM architecture, and by Raussendorf and Briegel [2], the one-way quantum computer with cluster states:

- **KLM** allows universal and scalable OQC using only single photons, linear optics and measurement. The by now seminal KLM work was based on the important findings of Gottesman, Chuang and Nielsen concerning the role of teleportation for universal quantum computing. The physical resources for universal (optical) quantum computation in the KLM scheme are multi-particle entangled states and (entangling) multi-particle projective measurements.
- **Cluster state quantum computing** has become an exciting alternative to existing proposals for quantum computing, and a linear optics approach is one way to implement this scheme. It consists of a highly entangled multi-particle state called cluster state. Single-qubit measurements are sufficient to implement scalable, universal quantum computation. Different algorithms only require a different "pattern" of single qubit operations on a sufficiently large cluster state. Since only single-particle projections are needed to operate such a one-way quantum computer, the cluster state approach might offer significant technological advantages over existing schemes for quantum computing: this includes reduced overall complexity and relaxed physical demands on the measurement process (as compared to sensitive multi-particle projections) as well as a more efficient use of physical resources.

B. State of the art (November 2004)

Important key elements for linear optics quantum computation, namely the generation of entangled states, quantum state teleportation and entanglement swapping have already been realized early in the field (e.g. teleportation in 1997 and entanglement swapping in 1998). The latest developments include realization of entanglement purification, freely propagating teleported qubits and feed-forward technology.

Several practical designs implementing the KLM scheme have subsequently been developed. Experimental methods for ultra-precise photonic quantum state creation, which serve as ancillas in the measurement-based schemes, now achieve typical fidelities above 99%. Using coincident detection there have been a range of demonstrations of nondeterministic two-qubit gates: a fully-characterized two-photon gate operating with >90% fidelity, four-photon CNOTgates both with entangled ancilla and with teleportation, a KLM nonlinear sign shift gate and a three-photon simulation of the entangled-ancilla gate. These gates can be made scalable with additional resources. Several of these gates have been used in simple applications such as demonstrations of quantum error encoding and generalized non-destructive quantum measurement circuits of two classical logic gates and Bell measurement for teleportation.

Proposals for the optical implementation of cluster state quantum computing have been put forward recently and are promising significant reductions in physical resources by two orders of magnitude as compared to the original KLM scheme. Separately, a variety of modifications to KLM has been suggested to also reduce resource requirements.

Enabling technologies for OQC are:

- Characterization of photonic quantum states and processes. A complete, tomographic, characterization of individual devices is indispensable for error-correction and has quite progressed within the last years. Quantum process tomography, invented by Chuang and Nielsen, can be used to fully characterize a quantum gate, probing either with a range of

input states or a single multi-qubit state. Based on the information gained from a complete process characterization it was recently shown how to estimate (and bound) the error probability per gate.

- Development of single photons and/or entangled photon sources is required for OQC. Currently, no source of timed single photons or entanglement is available. In the meantime, bright, albeit non-deterministic sources of correlated photons or entangled-photon pairs are critical to allow on-going evaluation of circuit technology as it is developed. Ultra bright and compact sources, some fiber-coupled to improve mode quality, have been developed. Relatively brighter sources (though not yet in absolute terms) have been demonstrated using periodically-poled nonlinear waveguides.
- High-fidelity multi-qubit measurements (in the KLM scheme) and reliable preparation of multi-qubit states (in both the KLM and the cluster state scheme).

C. Strengths and weaknesses

Current drawbacks of the OQC approach are low photon creation rates, low photon detection efficiencies, and the difficulties with intermediate storage of photons in a quantum memory (see also section 4.1.3). Advantages are obviously low decoherence (due to the photon's weak coupling to the environment), ultrafast processing, compatibility to fiber optics and integrated optics technologies and, in principle, straightforward scalability of resources. However, the low efficiencies quoted above are presently an important practical limitation to scalability, in the sense that they damp exponentially the success probability of most quantum operations.

D. Challenges

The main challenges for OQC can be summarized as follows:

- To achieve fault-tolerant quantum computing. The basic elements of fault-tolerance for OQC are becoming well understood. It has recently been shown that also optical cluster state QC may be performed in a fault-tolerant manner. Error models for KLM-style OQC have found that error thresholds for gates are above 1.78%.
- To reduce the resources required for OQC further and to find the limiting bounds on the required resources.
- To achieve massive parallelism of qubit processing by investing in source and detector technologies. Specifically, the development of high-flux sources of single photons and of entangled photons as well as photon-number resolving detectors will be of great benefit to achieve this goal.
- To generate high-fidelity, large multi-photon (or, more generally, many-particle) entangled states. This will be of crucial importance for cluster state quantum computing.
- To implement OQC architectures on smaller, integrated circuits. All of the current technologies involve either free space optics or combinations of free-space optics and optical fibers. To achieve long term scale-up, it will be essential to move to waveguide and integrated optics.

E. Key references:

[1] E. Knill, R. Laflamme, and G. J. Milburn, "*A scheme for efficient quantum computation with linear optics*", Nature **409**, 46 (2001).

[2] R. Raussendorf and H. J. Briegel, "*A one-way quantum computer*", Phys. Rev. Lett. **86**, 5188 (2001).

4.2.6 IMPURITY SPINS IN SOLIDS

A. Physical approach and perspective

Storage and processing of information can be carried out using individual atomic and molecular spins in condensed matter. Systems falling into this category include dopant atoms in semiconductors like phosphorous or deep donors in silicon or color centers in diamond, molecules like C60, rare earth ions in dielectric crystals and unpaired electrons at radiation induced defects or free radicals in molecular crystals. The main attraction of spins in low-temperature solids is that they can store quantum information for up to several thousand seconds [1]. Specific systems have been selected based on criteria like: dephasing time, optical access, single quantum state readout, and nanostructuring capabilities. While most of these systems are scalable in principle, technical progress in single quantum state readout, addressability and nanoengineering is necessary.

Research groups engaged in QIP research regarding impurity spins in solids in Europe include A. Briggs (Oxford, UK), P. Grangier (Orsay, F), O. Guillot-Noël and P. Goldner (Paris, F), S. Kröll (Lund, S), J.L. LeGouët (Orsay, F), M. Mehring (Stuttgart, D), K. Mølmer (Aarhus, DK), J.F. Roch (Cachan, F), M. Stoneham (London, UK), D. Suter (Dortmund, D), J. Twamley (Maynooth, IR), J. Wrachtrup (Stuttgart, D)

B. State of the art

Atomic and molecular spins in solids have received considerable attention as qubits. Already Kane's [1] proposal has underlined the basic challenges and opportunities of such systems in quantum computing. In the meantime a number of related systems like dilute rare earth ions, color centers, random deep donors in silicon with optically controlled spin and defects in wide and narrow band gap semiconductors have underlined their potential usefulness in QIP [2]. Most approaches use electron or nuclear spin degrees of freedom as quantum bits. The specific advantages of spin systems includes long decoherence times [3] and access to highly advanced methods for precise manipulation of quantum states. The experimental techniques that have made liquid state NMR the most successful QIP technique in terms of precise manipulation of quantum states so far are currently being transferred to solid-state systems. These systems may be able to overcome the scalability problems that plague liquid state NMR while preserving many of the advantages of today's liquid state work.

In detail the following landmark results have been achieved:

1. Magnetic resonance on single defects detected by charge transport and single spin state measurements by optical techniques.
2. Single and two qubit quantum gates on single defect spins in diamond.
3. For rare earth crystals preparation and readout of ensemble qubit states Rabi flops of a qubit, and qubit decoherence times on the order of seconds have been achieved. State control and quantum state tomography with a fidelity > 90% was shown.
4. The preparation of Bell states with electron and nuclear spin ensembles as well as a three qubit Deutsch-Jozsa algorithm has been achieved.
5. A scalable architecture has been developed for N@C60 on Si and decoherence times have been measured to be up to 1 s.

All of these are European achievements (point 3 was partly achieved in Australia).

C. Strengths and weaknesses

The strength of defect center QIP in solids are the long decoherence times of spins even under ambient conditions and the precise state control. Depending on the system, electrical as well as optical single spin readout has been shown (fidelity of 80%). Substantial progress in the nanopositioning of single dopants with respect to control electrodes has been achieved. Weaknesses are: Electrical and optical readout of spin states has been shown up to now for only a single type of defect.

Nanopositioning of defects is still a major challenge (which has seen dramatic progress for phosphorus in silicon). However there are schemes, based on deep donors in Si, where nanopositioning is not needed. Instead the randomness is exploited so as to make maximum use of spatial and spectral selection to isolate qubits and their interactions. Manipulation and readout is optical. The situation is similar for rare earth crystals, but in this case a fully scalable scheme still needs to be developed.

D. Short-term goals (next 3-5 years)

Impurity systems form a bridge for transferring quantum control techniques between atomic and solid state systems. Close interaction between the atomic physics and solid state communities is a key ingredient for achieving this.

- The mid term perspectives for phosphorus in silicon are the demonstration of single spin readout by 2005 and two qubit operations by 2006. Major efforts are concentrated in the US and Australia.
- Optical readout of defects in diamond heads towards a three qubit system and demonstration of teleportation by 2006. For further scaling advanced nanoimplantation techniques need to be developed.
- For rare earth crystals the expected developments in the near future (1 year) includes a proposal of a scalable scheme and the demonstration of two-qubit gates in this scheme. On a time scale of a few years, scaling up to several qubits will be investigated. These require either new and partly untested materials or development of single ion readout.
- For N@C60, single issue spin state readout should be demonstrated by 2005. For the scheme based on deep donors in Si or diamond, short term goals are demonstrations of all the key steps of fabrication, preparation, readout, and manipulation.

Excluding the first, all other goals are within reach of European laboratories.

E. Long-term goals (2010 and beyond)

- Coupling of defects in wide band gap semiconductors to an optical cavity mode. Implantation of defects with nm accuracy in registry with control electrodes. Improvement in optical detection efficiency by one order of magnitude to allow room temperature single-spin state read-out.
- For rare earth ions efforts should be joined with crystal growth research (inorganic chemistry) to create appropriate materials for larger scale systems. It can be expected that quantum computing in RE crystals will both contribute to and benefit from the development and knowledge base in the rare earth crystal area in general.
- Few-qubit device could be built on the basis of N@C60 by integrating nanopositioning of molecules with single-spin readout devices and control electronics.
- Few-qubit (up to perhaps 20 qubit) devices based on deep donors in silicon or silicon-compatible systems seem possible. Such devices should be linked into larger groups by flying qubits based largely on technology known from other fields. Achieving higher temperature is also of importance here.

F. Key references

[1] B. Kane, "*A silicon-based nuclear spin quantum computer*", Nature **393**, 133 (1998).

[2] S. Lloyd and C. Hammel, "*'Unique' qubit approaches to QIP and QC*", in "A Quantum Information Science and Technology Roadmap, Part 1: Quantum Computation", Version 2.0, section 6.8 and references therein; available from http://qist.lanl.gov.

[3] E. Yablonowitch, H.W. Jiang, H. Kosaka, H.D. Robinson, D.S. Rao, T. Szkopek "*Optoelectronic quantum telecommunications based on spins in semiconductors*" , Proc. IEEE **91**, 761 (2003).

4.3 QUANTUM INFORMATION SCIENCE -THEORY

4.3.1 INTRODUCTION

The development of quantum information science (QIS) was initially driven by theoretical work of scientists working on the boundary between Physics, Computer Science, Mathematics, and Information Theory. In the early stages of the development of QIS, theoretical work has often been far ahead of experimental realization of these ideas. At the same time, theory has provided a number of proposals of how to implement basic ideas and concepts from quantum information in specific physical systems. These ideas are now forming the basis for successful experimental work in the laboratory, driving forward the development of tools that will form the basis for all future technologies which employ, control and manipulate matter and radiation at the quantum level.

Today one can observe a broad and growing spectrum of theoretical activities. Investigations include, to name just a few examples,

- basic concepts such as entanglement and decoherence,
- characterization and quantification of (two- & multi-party) entanglement,
- novel quantum algorithms and communication protocols,
- capacities of noisy quantum communication channels,
- optimization of protocols for quantum cryptography,
- new computer models and architectures.

Another important class of theoretical work is concerned with implementations of these abstract concepts in real physical systems.

In fact, many of these theoretical proposals have formed the starting point as well as the guide for experimental work in the laboratories, as is described in the other sections of this document. Last, but not least, the transfer of concepts from quantum information theory to other fields of physics such as condensed matter physics or quantum field theory has proved fruitful and has attracted considerable interest recently.

It is important to realize that these activities are often interdisciplinary in nature and span a broad spectrum of research in which the different activities are benefiting from each other to a large degree. Thus it does not seem to be advisable to concentrate research on too narrowly defined topics only. Theory groups in Europe have been consistently delivered international leadership in the entire spectrum of research (see more below). This has been facilitated by a flexible and topically broad financing on European and national levels in the past.

In the following we give a brief outline of the current status and the perspectives of the main areas of quantum information theory.

4.3.2 QUANTUM ALGORITHMS & COMPLEXITY

Following Deutsch's fundamental work in 1985 that demonstrated the potential power of quantum algorithms and quantum computers, Shor demonstrated in 1994 that integers can be efficiently factorized on a quantum computer. Factoring is the task of decomposing an integer, say 15, into a product of prime numbers: 15=3*5. Its importance is immense because many modern cryptographic protocols (for instance the famous RSA cryptosystem) are based on the fact that factoring large integers, as well as computing discrete logarithms, is a hard problem on a classical computer. Shor's result means that quantum computers could crack most classical public-key cryptosystems used at present. It has lead to extensive work on developing new quantum algorithms. Progress has been made on the Hidden Subgroup problem (which generalizes Shor's algorithm) in the case of non-Abelian groups, like affine groups, the dihedral group, or solvable groups with small exponent. A quantum algorithm was discovered for finding solutions to Pell's equation, which is an important problem in algebraic number

theory. Strong links have been established between known quantum algorithms and lattice problems. Finally Grover's quantum "data base" search algorithm allows a quantum computer to perform an unstructured search quadratically faster than any classical algorithm.

In parallel with the development of new quantum algorithms, new algorithmic techniques have been developed. Examples of these are adiabatic quantum computing which is a very versatile method of approaching virtually any computational task; and quantum random walks which have enabled important generalizations of Grover's search algorithm. There has also been considerable development of new protocols for quantum communication. The objective may be to carry out a task which is possible classically, but with significantly less communication, such as Quantum Fingerprinting or the Hidden Matching problem. Or it may be to realize tasks which are impossible classically such as biased Coin Tossing and Quantum Bit String Generation, resilient and unconditionally secure Digital Signatures, or Private Information Retrieval. The importance of these latter tasks lies in their application to "mistrustful cryptography", this is the field of cryptography dealing with the problem of two or more people who do not trust each other, but must accomplish some goal together (for instance concluding a commercial deal, consulting a data base, etc.).We expect that the existing protocols will be improved and will gradually be implemented in the laboratory (as was recently the case for quantum bit string generation). We also expect the development of new protocols for quantum communication.

Key references

[1] D. Deutsch, "*Quantum Theory, the Church-Turing principle and the universal quantum computer*", Proc. R. Soc. Lond. **A 400**, 97 (1985).

[2] P.W. Shor, "*Algorithms for quantum computation, discrete log and factoring*", FOCS'35, 124 (1994).

[3] L. Grover, "*A fast quantum mechanical algorithm for database search*", STOC'28, 212 (1996).

[4] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, "*Quantum fingerprinting*", Phys. Rev. Lett. **87**, 167902 (2001).

[5] L. P. Lamoureux, E. Brainis, D. Amans, J. Barrett, and S. Massar, "*Provably secure experimental quantum bit string generation*", Phys. Rev. Lett. **94**, 050503 (2005)

4.3.3 COMPUTATIONAL MODELS & ARCHITECTURES

There are many different ideas of how to make quantum systems compute. While these different computational models are typically equivalent in the sense that one can simulate the other with only polynomial overheads in resources, they may be quite different in practice, when it comes to a particular class of problems. They also suggest different procedures to achieve fault tolerant computation, many of them yet to be explored in detail. At the moment the main contenders of fundamental architectures are:

- The gate or circuit model (computation realized by series of elementary unitary transformations on a few qubits at a time).
- The one-way quantum computer (computation realized by sequence of 1-bit measurements on a pre-entangled cluster state).
- Adiabatic computing (computation realized by smoothly changing a Hamiltonian, whose ground state, at the end of the process, encodes the solution of the given problem).
- Quantum cellular automata (quantum version of classical cellular automata).
- Quantum Turing machine (quantum version of classical Turing machine).

Most recently, we have seen a series of theoretical work analyzing the connection between the different computational models. The benefit of these works lies in a better understanding of the capabilities and advantages of the individual models, and of the essential features of a quantum computer. In the future we expect that optimized models (i.e. taking the best out of the different approaches) will be developed. We also expect that these models will have an increasing impact on (i) the formulation of new quantum algorithms and (ii) the evaluation of physical systems regarding their

suitability for fault-tolerant quantum computation. Both of these points are of great importance for the field: While new algorithms will further enlarge the range of applications for quantum computers, new methods for fault-tolerant computation will hopefully make it technologically less challenging to realize scalable quantum computers in the laboratory.

Key references

[1] D. Deutsch, "*Quantum computational networks*", Proc. R. Soc. Lond. **A 425**, 73 (1989).

[2] A. Barenco, C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J.A. Smolin, and H. Weinfurter, "*Elementary gates for quantum computation*", Phys. Rev. **A 52**, 3457 (1995).

[3] E. Farhi, J. Goldstone, S. Gutmann, J. Lapan, A. Lundgren, and D. Preda, "*A quantum adiabatic evolution algorithm applied to random instances of an NP-complete problem*", Science **292**, 472 (2001).

[4] B. Schumacher and R. Werner, "*Reversible cellular automata*", quant-ph/0405174, http://xxx.arxiv.org.

[5] R. Raussendorf and H.-J. Briegel, "*A one-way quantum computer*", Phys. Rev. Lett. **86**, 5188 (2001).

4.3.4 QUANTUM SIMULATIONS

Quantum simulators may become the first application of quantum computers, since with modest requirements one may be able to perform simulations which are impossible with classical computers. At the beginning of the 80's it was realized that it will be impossible to predict and describe the properties of certain quantum systems using classical computers, since the number of variables that must be stored grows exponentially with the number of particles. A quantum system in which the interactions between the particles could be engineered would be able to simulate that system in a very efficient way. This would then allow, for example, studying the microscopic properties of interesting materials permitting free variation of system parameters. Potential outcomes would be to obtain an accurate description of chemical compounds and reactions, to gain deeper understanding of high temperature superconductivity, or to find out the reason why quarks are always confined.

A quantum simulator is a quantum system whose dynamics can be engineered such that it reproduces the behaviour of another physical system which one is interested to describe. In principle, a quantum computer would be an almost perfect quantum simulator since one can program it to undergo any desired quantum dynamics. However, a quantum computer is very difficult to build in practice and has very demanding requirements. Fortunately, there are physical systems with which it is not known how to build a quantum computer, but in which one can engineer certain kind of interactions and thus simulate other systems which so far are not well understood. This is due to the fact that with classical computers it is impossible to reproduce their dynamics, given that the number of parameters required to represent the corresponding state grows exponentially with the number of particles. Examples are atoms in optical lattices or trapped ions. In those systems, one does not require to individually address the qubits, or to perform quantum gates on arbitrary pairs of qubits, but rather on all of them at the same time. Besides, one is interested in measuring physical properties (like magnetization, conductivity, etc.) which are robust with respect to the appearance of several errors (in a quantum computer without error correction, even a single error will destroy the computation). For example, to see whether a material is conducting or not one does not need to know with a high precision the corresponding conductivity.

Key references

[1] S. Lloyd, "*Universal Quantum Simulators*", Science **273**, 1073 (1996).

[2] N. Khaneja, R. Brockett, and S. J. Glaser, "*Time optimal control in spin systems*", Phys. Rev. **A 63**, 032308 (2001).

[3] E. Jané, G. Vidal, W. Dür, P. Zoller, and J. I. Cirac, "*Simulation of quantum dynamics with quantum optical systems*", Quant. Inf. Comp. **3**, 15 (2003).

[4] C. H. Bennett, J. I. Cirac, M. S. Leifer, D. W. Leung, N. Linden, S. Popescu, and G. Vidal, "*Optimal simulation of two-qubit Hamiltonians using general local operations*", Phys. Rev. **A 66**, 012305 (2002).

[5] M. A. Nielsen, M. J. Bremner, J. L. Dodd, A. M. Childs, and C. M. Dawson, "*Universal simulation of Hamiltonian dynamics for qudits*", Phys. Rev. **A 66**, 022317 (2002).

[6] P. Wocjan, D. Janzing, T. Beth, "*Simulating arbitrary pair-interactions by a given Hamiltonian: Graph-theoretical bounds on the time complexity*", Quantum Information and Computation **2**, 117 (2002).

4.3.5 QUANTUM ERROR CORRECTION & PURIFICATION

The ability to carry out coherent quantum operation even in the presence of inevitable noise is a key requirement for quantum information processing. Error correcting codes allow one to reduce errors by suitable encoding of logical qubits into larger systems. It has been shown that, with operations of accuracy above some threshold, the ideal quantum algorithms can be implemented. Recent ideas involving error correcting teleportation have made the threshold estimate more favorable by several orders of magnitude. This path has to be continued and adapted to realistic error models and to alternative models of quantum computation like the adiabatic model or the cluster model (see section 4.3.3).

At the same time, a fruitful connection to the theory of entanglement purification is emerging, which has been developed primarily in the context of quantum communication, and has been used in protocols such as the quantum repeater. Entanglement purification is a method to "distill" from a large ensemble of impure (low-fidelity) entangled states a smaller ensemble of pure (high-fidelity) entangled states. It seems that appropriately generalized procedures can be employed also in general quantum computation (e.g. for quantum gate purification, or for the generation of high fidelity resource states) while benefiting from the relaxed thresholds that exist for entanglement purification.

Key references

[1] A.M. Steane, "*General theory of quantum error correction and fault tolerance", in 'The physics of quantum information*', (D. Bouwmeester, A. Ekert, A. Zeilinger, eds.), pp. 242-252, Springer, Berlin (2000).

[2] J. Preskill, "*Fault-tolerant quantum computation*", in 'Introduction to quantum computation and information', (H.K. Lo, S. Popescu, T. Spiller, eds.) pp. 213-269, World Scientific, Singapore (1998).

[3] C.H. Bennett, D.P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "*Mixed-state entanglement and quantum error correction*", Phys. Rev. **A 54**, 3824 (1996).

[4] D. Deutsch, A. Ekert, R. Josza, C. Macchiavello, S. Popescu, and A. Sanpera, "*Quantum privacy amplification and the security of quantum cryptography over noisy channels*", Phys. Rev. Lett. **77**, 2818 (1996).

[5] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "*Quantum repeaters: The role of imperfect local operations in quantum communication*", Phys. Rev. Lett. **81**, 5932 (1998).

[6] A.M. Steane, "*Overhead and noise threshold of fault-tolerant quantum error correction*", Phys. Rev. **A 68**, 042322 (2003).

[7] E. Knill, "*Quantum computing with very noisy devices*", quant-ph/0410199, http://www.arxiv.org.

4.3.6 THEORY OF ENTANGLEMENT

Secret correlations are an important resource already in classical cryptography where, for perfect secrecy, sender and receiver hold two identical and therefore perfectly correlated code-books whose contents are only known to them. Such secret correlations can neither be created nor enhanced by public discussion. Entanglement represents a novel and particularly strong form of such secret correlations. Therefore, entanglement is a key resource in quantum information science. Its role as a resource becomes even clearer when one is considering a communication scenario between distant laboratories. Then, experimental capabilities are constrained to local operations and classical communication (LOCC) as opposed to general non-local quantum operations affecting both laboratories. This is an important setting in quantum communication but also distributed quantum computation and general quantum manipulations. The resulting theory of entanglement aims to answer three basic questions.

Firstly, we wish to characterize and verify entangled resources to be able to decide, ideally in an efficient way, when a particular state that has been created in an experimental set-up or a theoretical consideration contains the precious entanglement resource. Secondly, we wish to determine how entangled state may be manipulated under LOCC. In many situations an experimental setting will yield a certain type of entangled state that may suffer certain deficiencies. It may not be the correct type of state or it may have suffered errors due to experimental imperfections and be entangled. Once characterization methods have determined that the resulting state contains entanglement one can then aim to transform the initial state into the desired final state. Thirdly, it will be important to quantify the efficiency of all the processes and procedures as well as the entanglement resources that have been identified in the above two areas of research. If we have found entanglement in a state, then one will need to know how much of it there is.

Considerable progress in this area has been made in recent years, in particular in the case of bi-partite entanglement, but we are still far away from a comprehensive understanding of this key resource for quantum information processing. Research in this area will continue to play a central role in the field, and we expect that an increasing effort will be undertaken towards the classification and quantification of entanglement in multi-party entangled states. It is worth pointing out that insights in the theory of entanglement are not only important the field of QIS itself, but they have now reached the stage where they are being applied to other areas of physics (see the subsection 4.3.10).

Key references

[1] R.F. Werner, "*Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model*", Phys. Rev. **A 40**, 4277 (1989).

[2] M. Horodecki and P. Horodecki and R. Horodecki, "*Separability of mixed states: necessary and sufficient conditions*", Phys. Lett. **A 1**, 223 (1996).

[3] C.H. Bennett, H.J. Bernstein, S. Popescu and B. Schumacher, "*Concentrating partial entanglement by local operations*", Phys. Rev. **A 53**, 2046 (1996).

[4] V. Vedral and M.B. Plenio, "*Entanglement measures and purification procedures*", Phys. Rev. **A 57**, 1619 (1998).

[5] M.A. Nielsen, "*Conditions for a Class of Entanglement Transformations*", Phys. Rev. Lett. **83**, 436 (1999).

[6] A recent tutorial review was given by J. Eisert and M.B. Plenio, "*Introduction to the basics of entanglement theory in continuous-variable systems*", Int. J. Quant. Inf. **1**, 479 (2003).

4.3.7 MULTI-PARTY ENTANGLEMENT & APPLICATIONS

Research on multi-particle entanglement is on the one hand expected to be focused on novel protocols for quantum information processing in the multi-partite setting. Entanglement in quantum systems embodying more than two constituents is fundamentally different from two-party entanglement,

allowing for novel applications. This work on novel protocols includes work on instances of secret sharing or multi-partite fingerprinting. Notably, such multi-partite fingerprinting schemes would allow for the determination whether a number of databases are identical with little resources.

For quantum computation purposes it seems a major milestone to develop computation schemes that require minimal local control over interactions, such as in novel measurement-based computation schemes using multi-particle entangled resources as in cluster-state based approaches or in linear optics quantum computation. Alternatively, quantum cellular-automata based approaches may offer the potential of implementing quantum computation with little requirements of local control. Research work towards a complete understanding of the classification and quantification of multi-particle entanglement is expected to support such work, notably using methods from convex and global optimization, which give rise to novel methods for classification and quantification of entanglement. Laboratory quantum states such as random states or graph states as generalizations of cluster states may facilitate such studies.

On the other hand, there are good reasons to believe that a refined picture of criticality and phase transitions can be reached with the help of tools coming from the theory of entanglement. These ideas help in devising new simulation methods of ground states of many-body Hamiltonians in solid state physics (and many-body quantum systems in general). Finally, studies seem to indicate that questions in quantum field theory may become significantly more accessible using methods from entanglement theory (see also section 4.3.10).

Key references

[1] N. Linden, S. Popescu, B. Schumacher, and Westmoreland, "*Reversibility of local transformations of multiparticle entanglement*", quant-ph/9912039, http://xxx.arxiv.org.

[2] W. Dür, J. I. Cirac, and R. Tarrach, "*Separability and distillability of multiparticle quantum systems*", Phys. Rev. Lett. **83**, 3562 (1999).

[3] V. Coffman, J. Kundu, and W. K. Wootters, "*Distributed entanglement*", Phys. Rev. **A 61**, 052306 (2000).

[4] C. H. Bennett, S. Popescu, D. Rohrlich, J. A. Smolin, and A. V. Thapliyal, "*Exact and Asymptotic Measures of Multipartite Pure State Entanglement*", Phys. Rev. **A 63**, 012307 (2001).

[5] M. Hein, J. Eisert, and H. J. Briegel, "*Multi-party entanglement in graph states*", Phys. Rev. **A 69**, 062311 (2004).

4.3.8 NOISY COMMUNICATION CHANNELS

The proper understanding of the capacities of quantum communication channels is at the heart of the study of quantum communication tasks. Of particular importance are the transmission of classical or quantum information, or establishing secret key. But it is also known that one can use noise and perfect side communication to implement other cryptographic primitives like bit commitment and oblivious transfer. Channel capacities are of central interest in several different settings, being reflected notably by the classical capacity of quantum channels, quantum capacities, and entanglement-assisted capacities.

The central question is essentially what resources are required for transmitting classical or quantum information using quantum channels, such as optical fibers in a practical realization. A key problem is in particular whether an increased capacity can be obtained by employing entangled signal states (multiple uses) as opposed to single uses of the channel. This problem is widely known as the additivity problem for the Holevo capacity. There has been recent progress on this question, in particular linking this problem to seemingly unrelated additivity questions. In future work, this link between the different problems must be studied in more detail. For channels of salient interest this question will be directly addressed, using concepts of output purities. Novel methods from global optimization may be helpful here. For Gaussian channels, with practical importance in quantum communication with fibers, it seems within reach to find a complete answer to the above questions.

Finally, it is to be expected that more problems, as well as new perspectives, will arise when one considers multi-user channels, i.e., with more than one sender/receiver. While single-sender-receiver

settings serve well to study bipartite correlations, such problems have an immediate impact on understanding multi-partite correlations and their role in quantum communication via noisy channels.

Key references

[1] C. H. Bennett, G. Brassard, C. Crépeau, and M.-H. Skubiszewska, "*Practical quantum oblivious transfer*", Lecture Notes in Computer Science **576**, 351 (1991).

[2] S. Holevo, "*The capacity of the quantum channel with general signal states*", IEEE Trans. Inf. Theory **44**, 269 (1998).

[3] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, "*Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem*", Phys. Rev. Lett. **83**, 3081 (1999).

[4] G. G. Amosov, A. S. Holevo, and R. F. Werner, "*On some additivity problems in quantum information theory*", Problems in Information Transmission **36**, 305 (2000).

[5] P. W. Shor, "*Equivalence of additivity questions in quantum information theory*", Commun. Math. Phys. **246**, 453 (2004).

4.3.9 FUNDAMENTAL QUANTUM MECHANICS AND DECOHERENCE

Quantum information was born, in part, via research on the famous Einstein-Podolski-Rosen paradox and the issue of quantum non-locality. In turn, quantum information led the discussion to move beyond purely qualitative aspects of non-locality to defining and investigating quantitative aspects. In particular, it is now understood that non-locality is one of the central aspects of quantum mechanics. More generally, quantum information profits substantially from studying the fundamental aspects of quantum mechanics and, at the same time, yields new points of view, raising hopes of gaining a deeper understanding of the very basis of quantum mechanics.

The study of decoherence is intertwined with the field of quantum information science in at least three ways. Key challenges of the next years in the study of decoherence with methods, tools and intuition from quantum information science will include the following:

- To understand the fundamental role of classical correlations and entanglement in the decoherence process itself, and to flesh out the robustness of entangled states under typical decoherence processes.
- To engineer further ways to prevent decoherence in applications of quantum information processing, by exploiting decoherence-free subspaces, entanglement distillation, and dynamical decoupling procedures as bang-bang control.
- To support and contribute to experiments on decoherence to further understand the quantum to classical transition, and to determine what decoherence models are appropriate in what contexts.

Key references

[1] J. Eisert and M. B. Plenio, "*Quantum and classical correlations in quantum Brownian motion*", Phys. Rev. Lett. **89**, 137902 (2002).

[2] W. Dür and H. J. Briegel, "*Stability of macroscopic entanglement under decoherence*", Phys. Rev. Lett. **92**, 180403 (2004).

[3] A. R. R. Carvalho, F. Mintert, and A. Buchleitner, "*Decoherence and multipartite entanglement*", Phys. Rev. Lett. **93**, 230501 (2004).

[4] P. Zanardi and M. Rasetti, "*Noiseless quantum codes*", Phys. Rev. Lett. **79**, 3306 (1999)

[5] L. Viola, "*On quantum control via encoded dynamical decoupling*", quant-ph/0111167, http://xxx.arxiv.org.

[6] R. F. Werner and M. M. Wolf, "*Bell inequalities and entanglement*", Quant. Inf. Comp. **1**, 1 (2001).

[7] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, D. Roberts, "*Non-local correlations as an information theoretic resource*", Phys. Rev. **A 71**, 022101 (2005).

4.3.10 SPIN-OFF TO OTHER FIELDS

A very exciting aspect of theoretical work in QIS is the impact that it is beginning to make on other fields of science. In the case of classical computing such insights include the first exponential bounds on certain locally decodable codes, classical proof systems for lattice problems, bounds on the query complexity of local search problems, an efficient classical cryptographic scheme whose security is based on quantum considerations, and a quantum method to compute how many Toffoli gates are required to realize a reversible classical computation. The potential that QIS is offering for classical computing and mathematics may be understood by the following analogy. Real analysis is a very successful discipline but it contained a number of unsolved problems that were only solved by considering complex numbers, i.e. going to a larger space in which to describe the problem. By analogy we expect that moving from classical state space into the much larger quantum mechanical state space we will find novel approaches towards the solution of problems that ostensibly lie entirely within the classical realm. As the enormous size of the quantum mechanical state space is due to entanglement, one may view this as a further consequence of entanglement and a further justification for the importance of the study of entanglement (see section 4.3.6).

Relatively recently the study of the role of entanglement in infinitely extended quantum many-body systems and quantum field theories has attracted considerable interest. Many of the questions that are now being asked in this area can only be answered or even formulated correctly because of the many insights and techniques gained in the research in entanglement theory in recent years. These results have already born fruits in the development of novel simulation techniques for quantum many-body systems – generalization of the Density Matrix Renormalization Group (DMRG) method –, novel facets of correlations and phase transitions in spin systems and quantum field theories and solutions of longstanding open questions.

This demonstrates that the research into entanglement, its characterization, manipulation and quantification will not only continue to have impact within quantum information but is now reaching the stage where its insights are being applied to other areas of physics, with potentially enormous benefits, both intellectually but perhaps also commercially.

Key references

[1] I. Kerenidis and R. de Wolf, "*Exponential lower bound for 2-query locally decodable codes via a quantum argument*", quant-ph/0208062, http://xxx.arxiv.org.

[2] S. Popescu, B. Groisman and S. Massar, "*Lower bound on the number of Toffoli gates in a classical reversible circuit through quantum information concept*", quant-ph/0407035, http://xxx.arxiv.org.

[3] J. I. Latorre, E. Rico, and G. Vidal, "*Ground state entanglement in quantum spin chains*", Quant. Inf. Comp. **4**, 048 (2004).

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

[5] M. B. Plenio, J. Eisert, J. Dreissig and M. Cramer, "*Entropy, Entanglement, and Area: Analytical Results for Harmonic Lattice Systems*", Phys. Rev. Lett. **94**, 060503 (2005).

4.3.11 EUROPEAN PERSPECTIVE

As shown in the examples above, quantum information science is a broad interdisciplinary effort whose key aim is to provide a theoretical basis for the control and exploitation of nature at the level of individual quanta. European research has played a leading role in its development and has established a strong set of world leading centers. The field is thriving and strongly expanding both by continuing enhancement of efforts in existing sub-areas but also through the innovation of new research directions.

A key area is the development of new approaches towards the realization of quantum information processing, both at the device dependent and independent level, as well as the concrete exploration of existing experiments that aim towards the practical implementation of quantum information processing. European researchers have made pioneering contributions to this area both on the theoretical level and, often in close collaboration, also experimentally. Major centers exist in various European countries (see below). These centers form the cores of a number of EU networks providing a level of interconnection on the European level.

Quantum information science has emerged from groundbreaking purely theoretical work and its major breakthroughs so far have generally been theory driven. This abstract work addresses entanglement theory, quantum algorithms, quantum communication and the applications of QIS to other fields such as condensed matter physics, field theory and the solution of problems in classical information theory by quantum methods. Researchers involve physicists, mathematicians, computer scientists and engineers demonstrating its strongly interdisciplinary character. Europe has made groundbreaking contributions to this area that has led the development of the field as a whole. It should be noted that the research landscape in these theoretical areas is still fluid and novel directions continue to emerge. A particular growth area is the application of the ideas emerging in QIS to other areas of physics, mathematics and computer science, often providing entirely new problem solving techniques to existing areas. Intuitively this is due to the ability to access the full quantum mechanical state space rather than the much smaller classical state space which permits novel techniques to attack previously unsolved problems. Many new insights can be expected from this approach that will drive science forward in many areas.

Major centers exist in Austria, Belgium, Denmark, France, Germany, Netherlands, Poland, Spain, UK, and Switzerland. They have been linked through various EU project and the EU Network of Excellence QUIPROCONE as well as over the last five years through a European Science Foundation program on QIS addressing the need for this type of research for strong interconnections, the ability for informal collaborative visits to facilitate exchange of ideas. This is of particular importance in those aspects of theoretical research that are strongly interdisciplinary and where no single country possesses a critical mass of research.

Theoretical research in QIS in Europe has prospered through the efficient support for collaboration by the European Union, the European Science Foundation and the national funding bodies. In the face of growing international competition from North America, Japan and Australia it will be essential that flexible support compatible with innovative work will continue to be provided.

4.4 FUNDAMENTAL ISSUES ABOUT QIPC PHYSICS

QIPC relies on the manipulation and control of ensembles of qubits behaving according to the counter-intuitive laws of quantum physics. Most generally, though, quantum features are washed out in systems made of large numbers of particles. This decoherence phenomenon defines a kind of boundary between the microscopic world, where the quantum laws are dominant, and the macroscopic world, which behaves classically in spite of its underlying quantum nature. This boundary is fuzzy however. It largely reflects our lack of ability to isolate completely the system under study from its environment, made of a very big number of uncontrolled particles. By developing clever schemes, physicists and quantum information scientists are finding ways to fight this environment-induced decoherence. Some methods rely on the observation and manipulation of the environment itself, combined with feedback procedures counteracting the effects of decoherence on the system under study. Other methods, borrowing from the error correction schemes of classical computers, are at least in principle even more powerful. They are based on the redundant coding of the information in an ensemble of entangled qubits, monitoring the effects of decoherence on a subset of these qubits and applying correction procedures on others to restore the initial quantum state affected by decoherence. The progress towards the implementation of these methods, a prerequisite for large scale quantum computing to ever become feasible, is discussed in other parts of this report.

Here, we focus on other aspects of this field of research. The first is of a pedagogical nature. By attempting to "harness" the quantum laws and make them useful to achieve logical tasks, QIPC scientists are, in some way, changing our view of the quantum-classical boundary. In the discussions of

the founding fathers of quantum theory, this boundary was explored in thought experiments dealing with the principles of quantum measurements where microscopic systems are put in contact with macroscopic meters. Many QIPC experiments with atoms and photons can be viewed as modern realizations of these thought experiments. By doing them, physicists get more familiar with quantum concepts such as complementarity and wave particle duality. These experiments are now included in all modern textbooks of quantum physics. This pedagogical element must not be underestimated. The formation of an intuition for the quantum world is certainly an important ingredient in the education of students in physics and the study of QIPC is an excellent way to acquire this intuition. The students attracted by the esthetical qualities of this physics will be the researchers of tomorrow, who will apply their skills to QIPC or to other fields.

More fundamentally, these experiments also raise some issues at the forefront of physics. In QIPC, physicists learn to build systems of increasing size in quantum superposition, the Schrödinger cat states. This research is still in its infancy and many important issues remain to be explored, some of which are listed here non-exhaustively:

- **Size of mesoscopic superpositions.** This concept remains to be defined in a more quantitative way. Present experiments involve big molecules following spatially separated paths in an interferometer, large numbers of photons stored in different states in boxes or propagating freely in laser beams and currents rotating in opposite directions in superconducting circuits. Large ensembles of atoms entangled with each other via their interaction with polarized laser beams share common features with these mesoscopic superpositions. Experiments with entangled Bose Einstein condensates of ultra cold atoms are also developing, completing this zoo of Schrödinger cat states. Clearly, the mass of the system (what about the photonic cat states?) or the number of particles involved (should we count the quarks in the molecular cat systems?) are not universal parameters to measure the magnitude of a given state superposition. Attempts to define a universal distance between the parts of the mesoscopic wave functions have been made and should be refined, to permit a meaningful comparison between experiments performed under very different conditions on disparate systems.
- **Non locality of mesoscopic superpositions.** Non locality has been investigated in great details so far on simple microscopic systems (pairs of photons or ions). It remains to be studied on larger systems. Mesoscopic objects made of many atoms or photons can now be built, in which the two parts of the wave function correspond to different locations in space, separated by a truly macroscopic distance. In the case of photons, this relies on the realization of some kind of non linear beam splitter device which, in a way very different from an ordinary beam splitter, collectively channels all the photons, at the same time, in one arm and in the other of an interferometer. Experiments with up to four photons have already been realized and non local cat states involving much larger photon numbers are in the making. Similar ideas are being developed to channel Bose Einstein condensed atoms collectively in different final positions. These systems combine the weirdness of the Schrödinger cat (large objects in state superpositions) and the strangeness of non locality. In simple two-particle systems, the amount of non-locality is measured by the degree of violation of Bell's inequalities. Versions of these inequalities for mesoscopic systems have been proposed. Testing them on large non local Schrödinger cat states remains to be done. The effect of decoherence on the violation of these mesoscopic versions of Bell's inequalities remains largely to be studied.
- **QIPC, gravitation and beyond.** In QIPC physics, the coupling to environment is considered to be electromagnetic. There is however another kind of environment against which no shielding exists, due to the gravitational field permeating all space. Decoherence induced by the fluctuations of gravitational waves of cosmological origin has been estimated theoretically. It is found to be negligibly small on atoms or molecules, and exceedingly efficient on large objects, for which it is by far more important than electromagnetic decoherence. The transition appears to occur for objects of the order of Planck's mass (22 micrograms). Observing gravitational decoherence would be a daunting task, the challenge

being to isolate effectively from electromagnetic influence objects made of many trillions of atoms. Experiments attempting to prepare quantum superpositions of states of a tiny mirror placed at the tip of a cantilever could be a first step in this direction. Even if gravitational effects are not of concern for QIPC applications, they are of a fundamental interest because they link the quantum-classical boundary to fundamental cosmological issues. Experiments on gravitational decoherence will not be realized in the near future, but thinking about them brings together scientists from quantum optics, mesoscopic physics, theoretical physics and cosmology. Deep questions such as the connection between information theory and black hole physics are also fruitfully debated, even though applications are not to be expected. Finally, these issues cannot be separated from a fundamental question about the future of quantum theory itself. Including gravitation into a comprehensive quantum framework has up to now eluded the efforts of theorists. A majority believes that such a comprehensive theory will retain the essential features of the present quantum theory, notably state superpositions and probabilistic behavior. Some however, who dislike the idea that "God is playing dice", hope that the new theory will reestablish some kind of classical determinism. There would then exist another kind of decoherence, more fundamental than the environment induced one. All attempts to build such theories so far have failed, but this does not deter their advocates. To test experimentally possible theories of this kind will be exceedingly difficult. It will imply, as a prerequisite, a very good control of the largely dominant environment induced decoherence. If a limitation to quantum laws as we know them were found at a given size scale, it would have tremendous consequences on our view of Nature, going far beyond the discussion about the feasibility of a quantum computer.

5. PROSPECTS FOR APPLICATIONS AND COMMERCIAL EXPLOITATION

The main thrust of the ongoing investigations still belongs to basic research. However, a few areas can be already identified which are closer to potential applications and even for commercial exploitation.

Quantum communication

Commercial quantum cryptography products

In the 1990's Europe took clearly the lead in quantum cryptography with groups like BT and Oxford/DERA team in the UK, Geneva University in Switzerland and the Universities of Innsbruck and of Vienna in Austria. However, today the competition is hard. About simultaneously as the European company id Quantique (www.idQuantique.com), a company in the US announces a commercial quantum cryptography product (www.MagiQtech.com). Another European company which developed a commercial quantum key distribution scheme is Elsag plc. A serious European competitor in entanglement based quantum cryptography is Singapore, where Christian Kurtsiefer and his team, in collaboration with researchers from NIST, are building and testing QKD at NUS. In the last two years Japan appeared very strongly on the global scene with major industrial players devoting entire development teams to quantum key distribution systems: NEC, Mitsubishi, Toshiba and NTT among others (the 2 first ones did already present prototypes). Moreover the Japanese government widely supports university research in quantum communication. It is noteworthy that Japan opted almost exclusively for weak-laser-pulse quantum cryptography in optical fibers at a wavelength of 1550nm using time-bin encoding. Considering the various technologies, both the US and Japan compete directly with Europe in Quantum Cryptography based on weak pulses. In contrast, the European leadership in entanglement-based quantum cryptography and quantum communication is uncontested at present.

Quantum computing

Specializing quantum computing: quantum simulators

Quantum information processing in the sense of fault tolerant quantum computing for large-scale numerical algorithms (for example Shor's algorithm) is the ultimate goal. Within the next few years one expects few-qubit quantum computer with applications to quantum repeaters, for example. On the intermediate time scale one goal is to beat classical computations on whatever (non-trivial) problem. This could be achieved, for example, with specialized quantum computing, as with quantum simulators (see section 4.3.4) where a system with more than 30 qubits is already beyond the reach of any foreseeable classical machine

Quantum metrology

Entanglement as a resource for precise measurements

Entangled states provide instances of the most fragile objects ever known, because they are extremely sensitive to interaction with the environment. This sensitivity can be exploited to overcome the classical limits of accuracy in various kinds of measurements, for example in ultra-high-precision spectroscopy, or in procedures such as positioning systems, ranging and clock synchronization via the use of frequency-entangled pulses: for instance, in the latter case, picosecond resolution at 3 km distance has been attained. Entangled photon pairs can be used also for absolute calibration of detectors independently of black-body radiation (i.e. of temperature), without the need to refer to a standard source.

Gravitational waves detection may require entangled light beams

Large scale laser interferometers with kilometer arm lengths are currently being built or started operating In Europe, the USA and Japan with the hope to achieve the first direct detection ever of gravitational waves and thus to open a new field of astronomy. For these detectors the classical sensitivity limit is a serious restriction. It is likely that

for the first detection one will have to implement continuous variable entangled light beams in the two interferometer arms to overcome the classical limit. Scientists in Europe and Australia have recently demonstrated the required quantum noise squeezing of laser light at kilohertz frequencies.

Beyond the limits of state-of-the-art atom clocks

State-of-the-art atom clocks developed in Europe have reached the level of accuracy limited by quantum noise of atoms. Entanglement of atoms in clocks may allow surpassing this limit by generation of spin squeezed states of atoms. Work towards this goal is going on in Europe and in the US. Single quantum particles can be used as nanoscopic probes of external fields. Along these lines, atomic-scale (up to 60 nm) resolution in the measurement of the spatial structure of an optical field via a single ion, as well as sub-shot-noise atomic magnetometry via spin squeezing and real-time feedback, have been already experimentally demonstrated. On the other hand, the quantum regime is being entered also in the manipulation of nanomechanical devices like rods and cantilevers of nanometer size, currently under investigation as sensors for the detection of extremely small forces and displacements.

Quantum technologies

Commercial quantum random numbers generators

A simple example is the use of quantum randomness to generate random numbers. Such random numbers are truly random, in contrast to the pseudo-random numbers that classical computers generate. Using tools from quantum communication, one can develop such a quantum random generator that is much faster than the other physical generators, e.g. those based on the rather slow thermal fluctuations. A first commercial product is available, see www.idquantique.com.

Quantum imaging

It is also possible to generate quantum entanglement between the spatial degrees of freedom of light, which enables us to use quantum effects to record, process and store information in the different points of an optical image, and not only on the total intensity of light. One can then take advantage of a characteristic feature of optical imaging, which is its intrinsic parallelism. This opens the way to an ambitious goal, with a probable significant impact in a mid-term and far future: that of massively parallel quantum computing. In a shorter perspective, quantum techniques can be used 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. This can be used in many applications where light is used as a tool to convey information in very delicate physical measurements, such as ultra-weak absorption spectroscopy, Atomic Force Microscopy etc. Detecting details in images smaller than the wavelength has obvious applications in the fields of microscopy, pattern recognition and segmentation in images, and 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 "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 affect matter at a scale smaller than the wavelength.

Quantum optical metrology

The success in quantum science and engineering has created several extremely valuable optical tools that operate exclusively under the rules of quantum mechanics and offer practical optical measurement and characterization techniques (quantum optical metrology) that have clear advantages over existing technologies.

The main step in the development of quantum correlation and quantum entanglement tools was a practical design 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), and calibration of single-photon detectors without any need for using traditional

blackbody radiation sources. This unique possibility of self-referencing present in the optical system that is distributed in space-time is the main advantage of quantum correlation and entanglement. The fact that spontaneous parametric down-conversion (SPDC) is initiated by vacuum fluctuations serves as a universal and independent reference for measuring the optical radiation brightness (radiance). It gives the possibility of accurately measuring the infrared radiation brightness without the need of using very noisy and low sensitivity infrared detectors. Development of periodically poled nonlinear structures has opened the road for practical implementation of sources with high intensity of entangled-photon flux and with ultra high spectral bandwidth for biomedical coherence imaging. Recent demonstrations have shown the possibilities for multi-photon interferometry beyond the classical limit. It has been shown that weak field homodyning could yield enhanced resolution in phase detection. First experimental implementations of quantum ellipsometry indicated the high potential of quantum polarization measurement. The basic physical principles of optical coherence tomography with dispersion cancellation using frequency entangled photon pairs for sub-micron biomedical imaging have been demonstrated in model environments. The use of quantum correlations led to the design of a new technique for characterizing chromatic dispersion in fibers. The intrinsically quantum interplay between the polarization and frequency entanglement in CSPDC gave rise to a polarization mode dispersion measurement technique that provides an order of magnitude enhancement in the resolution.

APPENDIX: QUANTUM BASED TECHNOLOGIES

A. QUANTUM IMAGING

A.1 LANDMARK RESULTS

The aim of Quantum Imaging is to demonstrate that one can take advantage at the same time of the quantum mechanical aspects of light and of the fundamental and intrinsic parallelism of optical signals to develop new techniques in the processing of information at the quantum level. This kind of study is a rather new subject of quantum optics, and is in its infancy for most of its aspects. The first step was to produce, characterize, and implement first uses of spatially entangled non-classical light. Landmarks results obtained so far in Europe are the following:

The "quantum laser pointer": it has been experimentally demonstrated that it was possible to improve the measurement of the position of the center of a light beam at the Angstrom level, beyond the shot noise limit, in the two directions of the image plane.

Observation of a spatial quantum correlation in parametric down conversion: the intensity difference measured on symmetric pixels of the signal and idler images produced by pulsed parametric down-conversion in the macroscopic regime has been shown to be below the photon noise limit. Let us stress that the observed quantum effect is a pure spatial one, and not a temporal one, as was obtained by all previous experiments.

Observation of noiseless image parametric amplification: the pixel to pixel fluctuations in an image have been shown to be less degraded by the phase-sensitive pulsed parametric amplification than if one would have used a classical amplifier of the same gain. Here also, it is an effect measured on spatial averages, and not on spatially resolved temporal fluctuations.

Precise assignment of classical and quantum features in "two-photon imaging": this paradoxical technique allows one to obtain the image of an object by recording all the light that it scatters, and not its spatial distribution, provided that the measurement is made in coincidence with a spatially resolved measurement performed on a second light beam correlated with the first one. It turns out that it is essentially an effect related to classical spatial correlations.

A.2 VISIONS, PROSPECTS, CHALLENGES AND ROADBLOCKS

First important results have been obtained, and a worldwide community exists now on the subject. A lot of research work remains indeed to be done, on the experimental side, to improve the quality of the production of spatial entanglement both in the continuous wave and in the pulsed regime, but also on the theoretical side, to find more practical applications of spatial entanglement to information technologies. A promising alley of research is certainly the use of orbital angular momentum of light to convey and process quantum information.

A.3 HOW EACH AREA RELATES TO THE OTHERS AND TO THE GLOBAL PICTURE?

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 alley of research is undoubtedly interesting and requires collaborative work between the quantum computing and quantum imaging communities.

A.4 POTENTIAL APPLICATIONS

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 and quantum optics in general. At a first level, they can

directly use the improvements brought by quantum effects and demonstrated by laboratory experiments, even though their 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 the level of quantum noise.

B. QUANTUM OPTICAL MEASUREMENT TECHNOLOGIES

B.1 PHYSICAL APPROACH AND PERSPECTIVE

The success in quantum science and engineering has created several extremely valuable optical tools that operate exclusively under the rules of quantum mechanics and offering practical optical measurement and characterization techniques (quantum optical metrology) that has clear advantages over existing technologies.

The main step in the development of quantum correlation and quantum entanglement tools was a practical design 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).

B.2 STATE OF THE ART AND PRACTICAL EXAMPLES (NOVEMBER 2004)

- Calibration of single-photon detectors without any need for using traditional blackbody radiation sources. This unique possibility of self-referencing present in the optical system that is distributed in space-time is the main advantage of quantum correlation and entanglement.
- The fact that SPDC is initiated by vacuum fluctuations serves as a universal and independent reference for measuring the optical radiation brightness (radiance). Gives the possibility of accurately measuring the infrared radiation brightness without the need of using very noisy and low sensitivity infrared detectors.
- Development of periodically poled nonlinear structures has opened the road for practical implementation of sources with high intensity of entangled-photon flux and with ultra high spectral bandwidth for biomedical coherence imaging.
- Recent demonstrations have shown the possibilities for multi-photon interferometry beyond the classical limit.
- It has been shown that weak field homodyning could yield enhanced resolution in phase detection.
- First experimental implementations of quantum ellipsometry indicated the high potential of quantum polarization measurement.
- The basic physical principles of optical coherence tomography with dispersion cancellation using frequency entangled photon pairs for sub-micron biomedical imaging has been demonstrated in model environment.
- The use of quantum correlation led to the design of a new technique for characterizing chromatic dispersion in fibers.
- The intrinsically quantum interplay between the polarization and frequency entanglement in SPDS gave rise to a polarization mode dispersion measurement technique that provides an order of magnitude enhancement in the resolution.

B.3 FUTURE DIRECTIONS AND CHALLENGES

The need for ultra-high resolution non-invasive optical measurement is one of the novel challenges with modern biophotonics and nanotechnology moving towards creation and manipulation of nanoscale

features. The existing characterization techniques are intrinsically invasive and often change the physical and chemical structure after its characterization.

Optical technologies can provide the non-invasive character of evaluation and satisfy the constraint of measuring dimensions that are smaller than the wavelength of light when a broad optical spectrum is employed.

B.4 SHORT-TERM GOALS (NEXT 3-5 YEARS)

- Evaluation and characterization of quantum states entangled in polarization, frequency, and direction of propagation.
- Engineering and technological design of hyper-entangled quantum states utilizing artificially created complex one- and two-dimensional periodically modulated nonlinear structures.
- The design of states with a super-broadband spectrum and with a high degree of polarization entanglement for biomedical applications and for quantum spectroscopic ellipsometry.
- Developing generators of quantum states of light of interest to high-resolution interferometry or lithography such as "NOON" states using linear optics.
- The quantum enhanced resolution in phase measurement using entangled multi-photon states and weak field homodyning.
- Developing multi-spectral quantum ellipsometry for characterization of non-isotropic samples of polymers, organic materials, biological objects, and nanoscale semiconductor patterns.
- Developing quantum optical coherence tomography using dispersion cancellation effect to reach sub-micron axial resolution in biological tissue.
- Developing quantum super-resolution microscopy with polarization-entangled photons and with a two-photon single atom laser.
- Developing compact fiber-based sub-systems for practical demonstration of quantum-optical measurement schemes and fiber sensors.
- Developing integrated solid-state quantum measurement tools and sensors by manipulating photonic qubits using nonlinear-optical and semiconductor materials.

B.5 LONG-TERM GOALS (2010 AND BEYOND)

Development of integrated entangled-photon circuits for specific quantum optical metrology applications that are ready for incorporation in technological processes.

B.6 KEY REFERENCES

[1] A. V. Sergienko and G. S. Jaeger "*Quantum Information Processing and Precise Optical measurement with Entangled-Photon Pairs*", Contemporary Physics, vol. **44**, 341-356 (2003).

[2] A. Migdall, "*Correlated-Photon Metrology Without Absolute Standards*", Physics Today **52**, 41 (1999).

[3] A. V. Sergienko "*Quantum Metrology With Entangled Photons*", in CXLVI International School of Physics 'Enrico Fermi', (T. J. Quinn, S. Leschiutta, and P. Tavella, editors), IOS Press, Amsterdam (ISBN 1 58603 167 8) ,715-746 (2001).

CONTRIBUTING AUTHORS

Name	Affiliation	City and country	Email-address
Th. Beth	Universität Karlsruhe Institut für Algorithmen und Kognitive Systeme	Am Fasanengarten 5 D-76131 Karlsruhe Tel.: +49 721 608 4205 Fax: +49 721 608 55022	EISS_Office@ira.uka.de
R. Blatt	Institut für Experimentalphysik, Universität Innsbruck	Technikerstr. 25, A - 6020 Innsbruck, Austria Tel.: +43 512 507 6350 Fax: +43 512 507 2952	Rainer.Blatt@uibk.ac.at
	Institut für Quantenoptik und Quanteninformation der Österreichischen Akademie der Wissenschaften	Technikerstr. 21A, A-6020 Innsbruck, Tel.: +43 512 507 4720 Fax: +43 512 507 9815	
H. Briegel	Institut für Theoretische Physik, Universität Innsbruck	Technikerstr. 25, A - 6020 Innsbruck, Austria Tel.: +43 512 507 6202 Fax: +43 512 507 2961	Hans.Briegel@uibk.ac.at
	Institut für Quantenoptik und Quanteninformation der Österreichischen Akademie der Wissenschaften	Technikerstr. 21A, A-6020 Innsbruck, Tel.: +43 512 507 4740 Fax: +43 512 507 9815	
D. Bruss	Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf	Universitätsstraße 1, Gebäude 25.32 D-40225 Düsseldorf Tel.: +49 211 81-10679	bruss@thphy.uni-duesseldorf.de
T. Calarco	Istituto Nazionale per la Fisica della Materia Bose-Einstein Condensation, Trento, Italy	BEC-INFM Dipartimento di Fisica Università di Trento Via Sommarive 14 I-38050 Povo, Italy Tel.: +39 0461 881525	calarco@ect.it
J. Ignacio Cirac	Max-Planck-Institut für Quantenoptik	Hans-Kopfermann-Strasse 1 D-85748 Garching, Germany Tel.: +49 89 32905-705 Fax: +49 89 32905-336	Ignacio.Cirac@mpq.mpg.de
D. Deutsch	Centre for Quantum Computation, Clarendon Laboratory, University of Oxford	Parks Road, Oxford OX1 3PU, UK Tel: Fax:	david.deutsch@qubit.org

Name	Affiliation	City and country	Email-address
J. Eisert	Imperial College London QOLS, Physics Department and Institute for Mathematical Sciences	Prince Consort Road London SW7 2BZ, UK Tel.: +44-2075947724 Fax: +44-2075947714	jense@imperial.ac.uk
	Universität Potsdam, Institut für Physik	Am Neuen Palais 10 14469 Potsdam, Germany Tel.: +49 331 977 1817 Fax: +49 331 977 1767	jense@quantum.physik.uni-potsdam.de
A. Ekert	Centre for Quantum Computation Department of Applied Mathematics and Theoretical Physics (DAMTP) University of Cambridge	Wilberforce Road Cambridge CB3 0WA , UK Tel.: +44 (0) 1223 760 394 Fax: +44 (0) 1223 765 900	artur.ekert@qubit.org
C. Fabre	Laboratoire Kastler Brossel Ecole Normale Supérieure et Université Pierre et Marie Curie	Campus Jussieu case 74 75252 Paris cedex 05, France Tel: +33 1 44 27 73 27	fabre@spectro.jussieu.fr
N. Gisin	Université de Genéve GAP-Optique	Rue de l'École-de-Médecine 20 CH-1211 Genève 4, Suisse Tel.: +41 22 379 65 97 Fax: +41 22 379 39 80	nicolas.gisin@physics.unige.ch
P. Grangier	Laboratoire Charles Fabry de l'Institut d'Optique	Bat. 503, Centre Universitaire, 91403 Orsay, France Tel.: +33 1 69 35 87 66 Fax: +33 1 69 35 88	philippe.grangier@iota.u-psud.fr
M. Grassl	Universität Karlsruhe Institut für Algorithmen und Kognitive Systeme	Am Fasanengarten 5, D-76131 Karlsruhe Tel.: +49 721 608 6299 Fax: +49 721 608 55022	grassl@ira.uka.de
S. Haroche	Département de Physique de l'Ecole Normale Supérieure	24 rue Lhomond, 75005 Paris, France Tel.: +33-1 44323420 Fax: +33-1 45350076	haroche@physique.ens.fr
A. Imamoglu	Institut für Quantenelektronik Wolfgang-Pauli-Str. 16	ETH Hönggerberg, HPT G 12 8093 Zürich Tel.: +41 1 633 45 70	atac.imamoglu@iqe.phys.ethz.ch
A. Karlson	Future and Emerging Technologies, DG INFSO, European Commission	BU33 - 3/18, B-1049 Brussels, Belgium Tel: +32 2 29 62 377 Fax: +32 2 29 68 390	Antonella.Karlson@cec.eu.int
J. Kempe	Université de Paris-Sud	LRI - Bát. 490 91405 Orsay Cedex, France	kempe@lri.fr

Name	Affiliation	City and country	Email-address
L. Kouwenhoven	Quantum Transport Group Kavli Intstitute of Nanoscience Delft Delft University of Technology	Lorentzweg 1, 2628CJ Delft, The Netherlands Tel.: +31 (0)15 278 6064 Fax: +31 (0)15 278 5527	leo@qt.tn.tudelft.nl
S. Kröll	Division of Atomic Physics Lund Institute of Technology (LTH)	Box 118, SE-22100 Lund Tel.: +46-22 29 626 Fax: +46-22 24 250	Stefan.Kroll@fysik.lth.se
G. Leuchs	Lehrstuhl für Optik Institut für Optik, Information und Photonik (Max-Planck-Forschungsgruppe)	Staudtstr. 7 / B2 D-91058 Erlangen Tel.: +49 9131 / 85 2 8371 Fax: +49 9131 / 13508	leuchs@physik.uni-erlangen.de
M. Lewenstein	ICFO - Institut de Ciències Fotòniques	C/ Jordi Girona 29, Nexus II 08034 Barcelona, Spain Tel: +34 93 205 86 91	maciej.lewenstein@icfo.es
D. Loss	Department of Physics and Astronomy University of Basel	Klingelbergstrasse 82 CH-4056 Basel, Switzerland Tel.: +41 (0)61 267 3749 Fax: +41 (0)61 267 1349	Daniel.Loss@unibas.ch
N. Lütkenhaus	Institut für Theoretische Physik I Universität Erlangen-Nürnberg	Staudtstr. 7/B2 Office 01.501 91058 Erlangen Tel.: + 49-9131-8528375 Fax: + 49-9131-13508	norbert.luetkenhaus@physik.uni-erlangen.de
S. Massar	Laboratoire d'Information Quantique and QUIC Université Libre de Bruxelles	Avenue F.D. Roosevelt 50 (CP165/59) B-1050 Brussels, Belgium Tel.: +32-2-650.29.73 Fax: +32-2-650.29.41	smassar@ulb.ac.be
J. E. Mooij	Kavli Institute of Nanoscience Delft University of Technology	Lorentzweg 1 2628 CJ, Delft, The Netherlands Tel.: +31-15-2784276 Fax: +31-15-2617868	j.e.mooij@tnw.tudelft.nl
M. B. Plenio	Imperial College London Department of Physics Quantum Optics and Laser Science	South Kensington campus, Rm 6M02B Huxley Building, London SW7 2AZ, UK Tel.: +44 (0) 20 7594 7754 Fax: +44 (0) 20 7594 7714	m.plenio@imperial.ac.uk
E. Polzik	Niels Bohr Institute Copenhagen University	Blegdamsvej 17, København Ø, 2100, Denmark Tel.: +353 25424 Fax: +353 25217	polzik@phys.au.dk

Name	Affiliation	City and country	Email-address
S. Popescu	University of Bristol H.H.Wills Physics Laboratory	Royal Fort Tyndall Avenue Bristol BS8 1TL Tel.: +44 (0) 117 928 8731 Fax: +44 (0) 117 925 5624	S.Popescu@bristol.ac.uk
G. Rempe	Max-Planck-Institut für Quantenoptik	Hans-Kopfermann-Str. 1 D-85748 Garching Germany Tel.: +49 - (0)89 / 32905701 Fax: +49 - (0)89 / 32905311	gerhard.rempe@mpq.mpg.de
A. Sergienko	Department of Electrical and Computer Engineering Boston University	8 Saint Mary's St. Boston, MA 02215 Tel.: (617) 353-6564; Fax: (617) 353-6440	AlexSerg@bu.edu
D. Suter	Fachbereich Physik Universität Dortmund	Universität Dortmund 44221 Dortmund Tel.: +49 231 755 3512 Fax: +49 231 755 3652	Dieter.Suter@physik.uni-dortmund.de
J. Twamley	Department of Mathematical Physics, Logic Building National University of Ireland	National University of Ireland, Maynooth, Co. Kildare, Ireland Tel.: +353 (0)1 708-6017 Fax: +353 (0)1 708-3359	Jason.Twamley@may.ie
G. Wendin	Department of Microtechnology and Nanoscience - MC2 Chalmers University of Technology	Kemivägen 9 S-412 96 Göteborg Sweden Tel.: +46-31-772 3189 Fax: +46-31-772 1919	goran.wendin@mc2.chalmers.se
R. F. Werner	Institut für Mathematische Physik TU Braunschweig	Mendelssohnstr. 3 38106 Braunschweig Germany Tel.: +49-531-391-5200 Fax: +49-531-391-8183	R.Werner@tu-bs.de
A. Winter	Department of Mathematics University of Bristol	University Walk Bristol BS8 1TW, United Kingdom	a.j.winter@bris.ac.uk
J. Wrachtrup	Universität Stuttgart 3. Physikalisches Institut	Pfaffenwaldring 57 D-70550 Stuttgart Tel.: +49 711 685-5277 Fax: +49 711 685-5281	j.wrachtrup@physik.uni-stuttgart.de
A. Zeilinger	Institut für Experimentalphysik Universität Wien	Boltzmanngasse 5 1090 Wien Austria Tel.: +43 1 4277 51201 Fax: +43 1 4277 9512	zeilinger-office@exp.univie.ac.at

Name	Affiliation	City and country	Email-address
P. Zoller	Institut für Theoretische Physik, Universität Innsbruck	Technikerstr. 25, A - 6020 Innsbruck, Austria Tel.: +43 512 507 6202 Fax: +43 512 507 2961	Peter.Zoller@uibk.ac.at
	Institut für Quantenoptik und Quanteninformation der Österreichischen Akademie der Wissenschaften	Technikerstr. 21A, A-6020 Innsbruck, Tel.: +43 512 507 4780 Fax: +43 512 507 9815	