Quantum Information Processing and Communication: Strategic report on current status, visions and goals for research in Europe

Version 1.7, April 2010
Roadmap committee members

R. Blatt (Innsbruck)
H. Briegel (Innsbruck)
D. Bruss (Düsseldorf)
T. Calarco* (Ulm)
J.I. Cirac (Garching)
D. Deutsch (Oxford)
J. Eisert (London & Potsdam)
A. Ekert (Cambridge)
C. Fabre (Paris)
N. Gisin (Geneva)
P. Grangier (Palaiseau)
M. Grassl (Karlsruhe)
S. Haroche (ENS Paris)
A. Imamoglu (Zürich)
J. Kempe (Orsay)
L. Kouwenhoven (Delft)
S. Kröll (Lund)
G. Leuchs (Erlangen)
M. Lewenstein (Barcelona)
D. Loss (Basel)
N. Lütkenhaus (Erlangen)
S. Massar (Brussels)
J. E. Mooij (Delft)
M. B. Plenio (Ulm)
E. Polzik (Copenhagen)
S. Popescu (Bristol)
G. Rempe (Garching)
M. Santha (Orsay)
A. Sergienko (Boston)
D. Suter (Dortmund)
R. Thew (Geneva)
J. Twamley (Sydney)
L. Vandersypen (Delft)
A. Wallraff (Zürich)
G. Wendin (Göteborg)
R. Werner (Braunschweig)
A. Winter (Bristol)
J. Wrachtrup (Stuttgart)
P. Zanardi (Los Angeles)
A. Zeilinger (Vienna)
P. Zoller (Innsbruck)

*Editing author

Document coordination: **QUIE2T WorkPackage 2**
Editing & Composing: **D. Binosi**

Table of Content

- Quantum Information Processing and Communication: Strategic report on current status, visions and goals for research in Europe
  - Table of Content
  - 1. Executive Summary
    - 1.1 Overview of QIPC Research and its goals for the coming five to ten years
      - 1.1.1 Quantum Communication
      - 1.1.2 Quantum Computation
      - 1.1.3 Quantum Information Sciences - Theory
      - 1.1.4 Summary of short- and long-term goals
      - 1.1.5 Synergies and integration
    - 1.2 The leading role of European researchers

- 1.3 Recommendations for funding on the EU and National level
- 2. Introduction: The major vision and goals of QIPC
- 3. Different aspects of QIPC research in Europe
  - 3.1 QIPC research in Europe - European union level
  - 3.2 National funding
  - 3.3 Local funding
  - 3.4 Other funding
  - 3.5 QIPC research in the international context
  - 3.6 The European flavor, vision and goals
  - 3.7 QIPC in a wider scientific and technological context
- 4. Assessment of current results and outlook on future efforts
  - 4.1 Quantum Communication
    - 4.1.1 Detectors
    - 4.1.2 Sources
    - 4.1.3 Quantum memories and interfaces
    - 4.1.4 Towards High Rates
    - 4.1.5 Towards Long Distances - Quantum Repeaters
    - 4.1.6 Towards Long Distances - Satellite Quantum Communication
    - 4.1.7 New Applications and Protocols
  - 4.2 Quantum Computation
    - 4.2.1 Trapped ions
    - 4.2.2 Neutral atoms, molecules and cavity QED
    - 4.2.3 Superconducting circuits
    - 4.2.4 Semiconductor quantum dots
    - 4.2.5 Linear Optics
    - 4.2.6 Impurity spins in solids and single molecular clusters
  - 4.3 Quantum Information Sciences - Theory
    - 4.3.1 Theory of quantum computing
    - 4.3.2 Quantum error correction and control
    - 4.3.3 Theory of entanglement and quantum channels
    - 4.3.4 (De)coherence and quantum effects in complex quantum systems
    - 4.3.5 Links between quantum information science and quantum many-body theory
    - 4.3.6 European perspective
  - 4.4 Quantum Information Technologies
    - 4.4.1 Applications of QIPC (quantum enabled technologies)
    - 4.4.2 Technologies needed to advance QIPC (quantum enabling technologies)
  - 4.5 Fundamental issues about QIPC physics

1. Executive Summary

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 Overview of QIPC Research and its goals for the coming five to ten years

1.1.1 Quantum Communication

Quantum Communication is the art of transferring quantum states from one place to another. The general idea is that quantum states encode quantum information: hence quantum communication also implies transmission of quantum information and the distribution of quantum resources such as entanglement. Quantum Communication covers aspects of basic physics as well as of practical relevance. Additionally, it will take care of the whole “wiring” inside a quantum computer, i.e., contribute to the quantum interface. Already now, one of its outstanding results is the emerging technology of quantum cryptography, which promises absolute secure transmission of the key codes that are essential to encrypt messages with tamper proof security. More specifically, any encryption scheme entails the distribution of a secret key among legitimate users; as the key must be transmitted between sender and recipient, it is susceptible to interception by an eavesdropper. For a secret key made of classical bits, none of the two parties will ever know that their communication has been intercepted. Not so if the key is carried out by a quantum communication channel. Qubits, unlike classical bits, do not possess definite values, such as the 0 or 1; rather, they represent a so-called coherent superposition of physical states (e.g., the polarisations of a photon). The laws of quantum mechanics imply that the mere act of observing a quantum bit modifies it, causing it to change its quantum state. The eavesdropper’s attempt to intercept the secret key made of qubits will therefore be manifest to both parties.

Quantum cryptography is now developing from the initial approach known as point-to-point Quantum Key Distribution (QKD), towards the management of quantum-based security over many-node networks, that are running in various places worldwide (Europe, Japan). Presently, technical problems are controlled well enough so that secure transmissions over a few tens of kilometres can be implemented. However, non-trivial problems emerge for really long-distance communication (hundreds to thousand of kilometres), and in the quest for higher bit rates. High-flux single photon sources as well as entangled photon sources should be developed in order to enhance secure medium range quantum communication. At present photons are the only suitable system for medium-distance quantum communication, as they maintain a robust quantum state throughout transmission, can be detected efficiently and with low levels of noise (other systems, such as atoms or ions, can be used for building quantum memories but not to propagate qubits over long distances).

Nonetheless, even light signals, whether viewed classically or quantum-mechanically, are dampened exponentially with distance in both optical fibres and free space. Both fundamental and more applied efforts are needed to address the problems facing the production, detection and distribution of qubits. In classical optical telecommunication, this problem is solved by using simple devices known as repeaters that amplify and reshape the transmitted signal. However, these are of no use for quantum communication: they are intrinsically noisy and create so many errors that any quantum key being transmitted would not survive. This is related to the fact that a classical repeater breaks down quantum entanglement, a purely quantum phenomenon associated with very strong, non-classical correlations between the states of two widely separated qubits. In parallel, novel protocols (for instance based on entangled qudits), that could enhance the fault-tolerance of quantum communication schemes, need further investigation. Entanglement is a crucial element in quantum communication schemes, which allows one to ‘teleport’ qubits directly to their destination, avoiding transmission losses. So quantum communication must reinvent the repeater concept, using quantum hardware that preserves entanglement. A further motivation for entanglement-based

schemes comes from security based on Bell Inequalities, so called “Device Independent” security proofs that need to be studied and demonstrated experimentally.

Real world medium-distance quantum communication. If Quantum Communication is to become, on the 5 to 10 year time-scale, an established technology, backing up the quantum cryptography “boxes” which are already commercialised, several scientific as well as technological gaps have to be filled. While in recent years we have seen free space quantum communication over 144km and fibre demonstrations over 200km, both in field trials, many barriers remain. In particular, when demonstrating the feasibility of ‘real world’ medium-distance quantum communication both in optical fibres and in free space, a significant increase in the qubit transfer rate by several orders of magnitude will be required. These goals, together with the one of realising long-distance secure quantum networks will be significantly advanced by developing quantum repeaters Achieving these goals will require facing a number of non-trivial challenges, needing very strong interaction between fundamental and applied research.

Quantum repeaters. In the long term a quantum repeater would actually be a small, dedicated, quantum processor, incorporating quantum memories, which, whilst feasible, requires a significant effort and is perhaps the most important technological hurdle facing QIFT. So far we have seen some first experimental steps towards elements needed for a quantum repeater, but there is much work to be done. Some of the basic elements that need to be developed and demonstrated are: medium range entanglement between memories, teleportation between different memories. The exact number of qubits that would have to be stored and processed in such a repeater, to ensure high-fidelity quantum communication over thousands of kilometres, is an open issue and highly dependent on the protocol. Nonetheless, it is likely to be in the range of tens or hundreds – much lower than the number required for a fully-fledged quantum computer. Therefore it is more likely that we will have secure global quantum communication before quantum code breaking.

1.1.2 Quantum Computation

Classical physics is at the root of present-day information processing: strings of bits (discrete digital states) are represented and processed in electronic devices (registers, logic gates etc.) through quantities such as charges, voltages, or currents. In Quantum Computing and more generally in Quantum Information Processing (QIP), one makes instead use of the laws of quantum mechanics replacing bits with qubits, two-state quantum systems that do not possess in general the definite values of 0 or 1 of classical bits, but rather are in a so-called ‘coherent superposition’ of the two. Full exploitation of this additional freedom implies that new processing devices (quantum registers, quantum logic gates etc.) need to be designed and implemented. As several sets of universal quantum gates acting on one and two qubits are known, a large scale quantum computer can in principle be built, provided the quantum physical system used meets some basic requirements (the so-called DiVincenzo criteria) on scalability, faithful initialization, manipulation, transmission and readout of qubits, and long coherence times with respect to the gate operation time. At present, a number of physical systems are under investigations for their suitability to implement a quantum computer. These include trapped ions and neutral atoms, cavity quantum electrodynamics (CQED), solid state devices (such as superconducting qubits, possibly in combination with circuit CQED, and spin qubits), all-optical devices, as well as impurity spins in solids, single molecular magnets etc.. During the last few years remarkable progress, measured in terms of the aforementioned DiVincenzo criteria, towards demonstrating the basic building blocks of a quantum computer have been reported in these systems. At present no fundamental physical roadblocks seem in sight for building a scalable quantum computer including error correction. However, a mixture of significant technological challenges and some open physical questions remain to be answered. At the same time it is premature to select a winner, rather research should progress on a broad front across all physical disciplines which studies these systems in view of scalability, coherence and speed of QIP, in particular also concerning their reliability, fault tolerance and use of error correction. Finally, development of a computer architecture must be complemented by interfacing with quantum communication to allow building of quantum networks. Ultimately, the goal must be to transfer this academic knowledge about the control and measurement of quantum systems to industry. Major

international companies have shown interest and support for developing and providing systems suitable for quantum manipulation.

Few-qubit applications. A first short range goal is the realization of a few-qubit general purpose quantum computer including error correction, as a test bed for demonstrating operation of a quantum computer. In parallel, however, special effort must be made to further develop few qubit applications which range from quantum information processing and quantum communication all the way to quantum assisted precision measurements.

Many-qubit specialized applications. As a second short range goal, special purpose quantum computers with a large number of qubits should be developed. A highly relevant example is provided by quantum simulators, programmable quantum systems whose dynamics can be engineered such that it reproduces the dynamics of other many body quantum systems of interest, e.g., atoms in optical lattices simulating high temperature superconducting systems and/or quantum phase transitions. Full simulation of a quantum mechanical system consisting only of a few hundred particles (spins) requires in fact classical computing resources in terms of memory of the order of the number of atoms in the visible universe – clearly demonstrating the inadequacy of any classical computer for this task. Quantum simulators could be the first nontrivial applications of quantum information, providing answers to problems which are fundamentally beyond classical computing capacities, such as the study of microscopic properties of materials permitting free variation of system parameters, an accurate description of chemical compounds and reactions, or find out the reason why free quarks are not found in Nature.

Quantum interfaces. In the long term a first goal is the development of hybrid technologies and architectures for quantum computation, including interfaces between them. This will stretch the theoretical and experimental resources of many branches 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, but rather a number of different technologies complementing each other: some will be more suitable for quantum memories, some for quantum processing, and some for quantum communication and so on. Therefore, in addition to developing individual technologies, interfaces between the latter are also needed, so that different qubit ‘memories’ (atoms/ions, quantum-dots, squids) and carriers of quantum information (atoms/ions, photons, phonons, electrons) can be interconnected.

Fault-tolerant gates and architectures. A second long range goal is the demonstration of fault-tolerant quantum logic gates, by the engineering of sub-microscopic systems in which qubits affect each other in a controllable way, while avoiding at the same time undesired couplings with the environment leading to decoherence. Applying to quantum computers the traditional network model, simple quantum logic gates would be connected up into quantum networks. However, the more interacting qubits are involved, the harder it tends to be to engineer the interaction that would display the quantum behaviour, and 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. It has been proven that if decoherence-induced errors are small (and satisfy certain other achievable conditions), they can be corrected faster than they occur, even if the error correction machinery itself is error-prone. The requirements for the physical implementation of quantum fault tolerance are, however, very stringent, and can be met either by improving technology or by going beyond the network model of computation and designing new, inherently fault-tolerant, architectures for quantum computation. One candidate for such an alternative architecture, e.g., might be the one-way quantum computer model, in which errors can classically be fed-forward and corrected. At the end however, a fault-tolerant quantum computer will most likely be achieved by an optimized combination of both strategies.

Implementation theory. Theory must continue to play a leading role in guiding and supporting experimental developments. Aside from finding and investigating fundamentally new algorithms especially suited for quantum computing, the various implementations require continuous theoretical work especially finding physical solutions where mere technology is yet too cumbersome. For example, operations in specially designed “decoherence free subspaces”, i.e., physically tailored systems less susceptible to technical errors, will be an important feature in finding an optimum system and optimized algorithms. Therefore, the theoretical work will have to cover a wide range of physical systems and technologies.

1.1.3 Quantum Information Sciences - Theory

Our conception of what a computation is has been altered drastically during history, since the times of Leibniz, Babbage and Turing. The result of this remarkable history of ideas – computers as we know them today – has changed our modern society significantly. Yet, the development of computing and communication devices has not come to a stop. Recent developments have shown, in fact, that we are at the beginning of a new era of harnessing the laws of nature, using quantum physics for unprecedented and very powerful ways of information processing. The development of Quantum Information Science (QIS) has been driven by theoretical work of scientists working on the boundary between Physics, Computer Science, Mathematics, and Information Theory. In the early stages of this development, 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 in turn form the basis for all future technologies which employ, control and manipulate matter and radiation at the quantum level. While the development of QIS has started as early as in the 80’s, the field has gained significant momentum in the last decade. Major triggers were the discovery of fast quantum algorithms and the identification of concrete physical systems in which a quantum computer could be realized. In the meantime, a broad spectrum of research activities can be observed, ranging from the study of fundamental concepts such as quantum entanglement, to novel applications such as quantum simulators, and with significant spin-off also to other fields of research. In many of these activities, European research has played a leading role and has established a strong set of world leading centres. It is important to realize that theoretical 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. The following list nevertheless tries to highlight the main current areas of quantum information theory as it has been described in more detail in the strategic report.

Quantum algorithms & complexity. Quantum algorithms will be one of the most powerful applications of quantum computers. We know only a few examples up to date, such as Shor’s factoring algorithm, but new techniques and protocols are currently being developed. This area remains one of the cornerstones of research in QIC.

Computational models & architectures. There are many different ideas of how to make quantum systems compute. New computer models, which have only recently been developed, are providing new agendas to formulate quantum algorithms. At the same time, they have opened new ideas for physical implementations of a quantum computer, and we expect new methods for fault-tolerant computation that will make it technologically less challenging to realize scalable devices in the laboratory.

Geometric and topological methods. These methods represent an alternative approach to the realization of quantum computing. They have intrinsic fault-tolerant properties that do not need an active error detection and recovery; however, the overhead that one has to pay are longer operation times, so that much work must still be done to identify which of the available schemes suit better to quantum computation.

Quantum simulations. Quantum simulators may become the first short-term application of quantum computers, since with modest requirements one may be able to perform simulations which are impossible with classical computers. They could be used for a variety of purposes, e.g., 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.

Quantum error correction & purification. Despite its amazing power, a quantum computer will be a rather fragile device, susceptible to disturbances and errors. Fortunately, methods have been

developed to protect such a device against disturbances and imperfections, as long as these are small enough. These methods are constantly being improved and refined, but there is still a lot of work to be done until we can run a quantum computer reliably.

Theory of entanglement. Entanglement represents a novel and particularly strong form of correlations which is not present in classical systems. It is a key resource in quantum information science and, at the same time, one of the most prominent features of quantum physics. Insights in the theory of entanglement will continue to have broad implications, and applications will lie not only within the field of QIS itself, but also in other areas of physics, such as field theory and condensed matter physics.

Multi-partite entanglement & applications. Research on multi-particle entanglement has emerged recently, and it is expected to have an impact on novel protocols for quantum information processing. Multi-partite entangled states represent keys resources, both for quantum computers and for novel communication schemes with several users such as quantum-secret sharing, quantum voting etc. Alternatively one can consider multi-partite fingerprinting schemes that would allow for the determination of whether or not a number of databases are identical with very little resources.

Noisy communication channels. In practice, all communication channels such as optical fibres are subject to some level of noise. Such noise can destroy the crucial entanglement or other quantum properties that are needed, e.g., for security or to reduce communication complexity. A proper understanding of how one can communicate via noisy quantum channels and of the capacities of such channels is at the heart of the study of quantum communication tasks.

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. 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, it yields new perspectives, raising hopes of gaining a deeper understanding of the very basis of quantum mechanics. In particular, quantum information theory can provide deeper understanding of dynamics of open quantum systems.

Spin-off to other fields. A very exciting aspect of theoretical work in QIS is the impact that it is beginning to gain on other fields of science. Examples are given by the theory of classical computing, by field theory, and by condensed matter physics. 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. 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 significantly 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.

1.1.4 Summary of short- and long-term goals

For convenience of synthesis, we summarize in a table a short list of objectives for the next and more distant future of quantum computing and quantum communication (the internal ordering of such lists does not necessarily reflect chronology). The great diversity and openness of the field of quantum information theory prevents from drawing a similar list for that particular subfield.

	Quantum Computing	**Quantum Communication**
5 years goals	Demonstrate: • Devices realizing quantum algorithms with up to 10 qubits • Fault tolerant computing	• Build a quantum repeater with two nodes • Entangle two remote quantum memories • Lab demonstration of Device Independent QKD

	and error correction on small scale systems • Distributed quantum algorithm • Different classes of entangled states up to 10 qubits • Quantum simulation of a system that cannot be simulated classically	
10 years goals	• Large dimension quantum memory • Quantum algorithm with up to 50 qubits • Quantum simulation of a key problem in science • Quantum algorithm with fault tolerant error correction	• Satellite quantum communication • 1000 km quantum cryptography • Multi-node quantum networks • Realization of new quantum protocols

1.1.5 Synergies and integration

QIPC is a new conceptual framework, a new way of looking at things with deep reaching consequences from network security to understanding the structure of the physical reality. It covers a broad spectrum of activities, from researching the foundations of quantum mechanics between the microscopic and the macroscopic level, to the development of patented industrial applications like quantum key distribution devices. The three domains of QIPC, quantum computation, communication and theory, are all closely connected, and within these domains there are a variety of different approaches that are all striving towards the same goal - integrated quantum systems. This integration will provide the next great challenge and inspiration for QIPC. In recent years tremendous progress has been made in all three fields, improved distances and fidelities in quantum cryptography and teleportation, coherent control of atomic systems for processing and theory is making daily advances in developing a basis for the theory of quantum computer science. Characteristic of the work within QIPC is that proof-of-principle advances in each of the sub-domains are used when pursuing the work in the other sub-domains and this is a key issue for developing QIPC as an integrated science and the basis of future and emerging technology. The experimental demands on the next phase of QIPC research will have a larger focus on integration of components and their reliability as the field moves from research oriented problems to applied and even commercial quantum technologies. Still an even closer interplay between theory and experiment will be needed in order to achieve complete realistic schemes for coherent manipulation and high-precision performance. These efforts will eventually lead to a pool of reliable technologies for the different components of a quantum architecture, much like it happens now for classical computers where magnetic, optical and electric bits are used for storage, transmission and processing of information, respectively. Clearly, it is too early to pick the winner implementation for the practical realization of a working quantum device: it is even possible that the best technology is still to be developed. The already ongoing integration among different research communities (for instance those working on solid-state and on atom/quantum optical systems) is a solid basis for further pushing these effort to integrating actual devices. An avenue that theory needs to embrace in order for efficient implementations to be developed is a deeper understanding of entanglement, which is a quantum feature that permeates the whole QIPC; its complexity just started being appreciated and much is left to investigate both in terms of formal theoretical description and of its applications. One also needs to fully explore the potentials of the available physical systems in order to invent new communication protocols, to investigate algorithmic consequences of physical assumptions, and to develop new computational algorithms, both implementable with a small-scale quantum computer and exploiting the immense power entailed in quantum parallelism.

1.2 The leading role of European researchers

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 must take a prominent and established position in EU research efforts, e.g., in the Seventh Framework Programme for Research of the European Commission (FP7), and find its counterpart in national programs. 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 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 vision and goals of QIPC

The theory of classical computation was laid down in the 1930s, was implemented within a decade, became commercial within another decade, and dominated the world's economy half a century later. However, the classical theory of computation is fundamentally inadequate. It cannot describe information processing in quantum systems such as atoms or molecules. Yet logic gates and wires are becoming smaller and soon they will be made out of only a handful of atoms. If this process is to continue in the future, new, quantum technology must replace or supplement what we have now. In addition, quantum information technology can support entirely new modes of information processing based on quantum principles. Its eventual impact may be as great as or greater than that of its classical predecessor.

While conventional computers perform calculations on fundamental pieces of information called bits, which can take the values 0 or 1, quantum computers use objects called quantum bits, or qubits, which can represent both 0 and 1 at the same time. This phenomenon is called quantum superposition. Such inherently quantum states can be prepared using, for example, electronic states

of an atom, polarized states of a single photon, spin states of an atomic nucleus, electrodynamical states of a superconducting circuit, and many other physical systems. Similarly, registers made out of several qubits can simultaneously represent many numbers in quantum superpositions.

Quantum processors can then evolve initial superpositions of encoded numbers into different superpositions. During such an evolution, each number in the superposition is affected and the result is a massive parallel computation performed in a single component of quantum hardware. The laws of quantum mechanics then allow this information to be recombined in certain ways. For instance, quantum algorithms can turn a certain class of hard mathematical problems into easy ones – the factoring of large numbers being the most striking example so far. Another potential use is code-breaking, which has generated a great deal of interest among cryptologists and the data security industry.

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

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

While the central concepts of quantum information sciences have initially been developed for qubits, the alternative possibility to realize quantum informational and computational tasks using continuous variables has been investigated more recently. The use of quantum information carriers that have a continuous spectrum, such as the quadrature amplitudes of the quantized light field, has several potential advantages over qubit-based processes. Such advantages lie in the prospect for higher optical data rates and simpler processing tools, based upon standard telecommunication techniques. Another significant strength of this paradigm is that the light-atoms quantum interface can be designed for continuous variables, so that atomic continuous-variable systems can be used as a memory for light.

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

In principle we know how to build a quantum computer: we start with simple quantum logic gates and connect them up into quantum networks. A quantum logic gate, like classical gates such as AND and OR, is a very simple computing device that performs one elementary quantum operation, usually on one or two qubits, in a given time. However, the more interacting qubits are involved, the harder it tends to be to engineer the interaction that would display the quantum behaviour. The more components there are, the more likely it is that quantum information will spread outside the quantum computer and be lost into the environment, thus spoiling the computation. This process is called decoherence. Thus the task is to engineer sub-microscopic systems in which qubits affect each other but not the environment. The good news is that it has been proved that if decoherence-induced errors are small (and 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.

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.

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

The next thing on the horizon is a quantum simulator. This is a quantum system in which the interactions between the particles could be engineered to simulate another complex system in an efficient way – a task that is inherently intractable on classical, but not quantum, technology. Building quantum simulators would allow, for example, the development of new materials, accurate description of chemical compounds and reactions, or a deeper understanding of high temperature superconductivity. The goal is to push the existing quantum technologies, such as optical lattices, to their limits and build quantum simulators within a decade or so.

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

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

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

Research in Quantum Information Processing and Communication (QIPC) has a high risk nature and long-term outlook which is very much in scope of information and communication technologies (ICT). The “Future and Emerging Technologies” programme (FET) being part of the ICT research theme of European Commission has as early as in the mid 90’s recognized the potential of QIPC. From the

very beginning FET has been successful in attracting the best research teams in Europe to its collaborative programme, more recently including also excellent teams in USA, Australia and Asia. It is fair to say that the pathfinder role of FET has been crucial for the development of the QIPC research domain in Europe.

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

During 1998 the QCEPP working group (the so-called Pathfinder Project) laid the bases for the research field of QIPC at European level and was the first endeavour 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.

The proactive initiative QIPC and its successors

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 finished at the end of 2005. Integrating the projects arising from the Open scheme with those supported through the proactive initiative and coordinate the work of all these projects was a main priority of the proactive initiative in FP5. Important traditions were also established at that time. Each year since the beginning of the proactive initiative two major events have been 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.

In FP6 (2003–2006) QIPC continued as a FET PI. There was one call for Integrated Projects (IP) in September 2004. Three Integrated Projects succeeded in the evaluations and started in November 2005 with a contract for four years and total EU funding of 25 M€:

- SCALA – Scalable Quantum Computing with Light and Atoms (9.4 M€) with a focus on the realization of a scalable quantum computer, by using individually controlled atoms, ions and photons;
- QAP – Qubit Applications (9.9 M€) with a focus on qubit applications that are based on photonic, atomic and solid state systems;
- EuroSQIP – European Superconducting Quantum Information Processor" (6M€): with a focus on developing a 3-5-qubit quantum information processor on platforms based on Josephson junction technology.

In FP7 (2007-2013) the proactive initiave took on the new name “Quantum Information Foundations and Technologies” (QI-FT) and organized a call for proposals in 2009. Besides the ongoing objective to exploit the quantum nature of information for new ways of computing and communication, projects should also develop entanglement-enabled quantum technologies with a general potential for application in ICT. Three projects started in February 2010 with a total EU funding of 15 million Euros. Remarkably, also research groups from outside Europe were attracted by these projects coming from the US, Australia and Singapore.

- AQUTE (5.3 M€) strives to realise an atomic, molecular and optical (AMO)-based

quantum-information processor involving up to 10 qubits and capable to simulate quantum systems, to develop novel hybrid quantum systems, and to explore novel theoretical concepts, such as dissipative quantum computation.
- Q-ESSENCE (4.7 M€) pursues the hybridization of quantum information media with a focus on making networks, long-distance entanglement, applications, and verification. These outcomes will be reached through the underpinning science and enabling technologies such as light-matter interfaces providing faithful interconversion between different physical realizations of qubits or quantum information concepts that solve problems of limited trust and privacy intrusion.
- SOLID(5.0 M€) is to develop small solid-state hybrid systems on common platforms based on microwave and optical nano-photonic cavities for the purpose of performing elementary quantum information processing tasks. Various types of solid-state qubits will be connected to these "hubs": Josephson junction circuits, quantum dots and NV centres in diamond. Focus is on design, fabrication, characterization, combination, and operation of quantum-coherent hybrid registers involving 3-9 qubits.

QIPC in the FET OPEN scheme

Also in FP7 a significant number of FET OPEN projects have been working on QIPC topics with a total funding of about 30 M€ (status February 2010). These are

- COMPAS - Computing with mesoscopic photonic and atomic states (2.1 M€);
- COQUIT - Collective quantum operations for information technologies (1.5 M€);
- CORNER - Correlated noise effects in quantum information processing (2.7 M€);
- GEOMDISS - Geometric phases, pumping, and dissipation in quantum devices (2.1 M€);
- HIDEAS - High Dimensional Entangled Systems (4.6 M€);
- HIP - Hybrid Information Processing (2.8 M€);
- MIDAS - Macroscopic interference devices for atomic and solid-state systems: quantum control of super-currents (3.1 M€);
- MINOS - Micro- and nano-optomechanical systems for ICT and QIPC (3.1 M€);
- MOLSPINQIP - Molecular spin Clusters for Quantum Information Processes (2.7 M€);
- NAME-QUAM - Nanodesigning of atomic and molecular quantum matter (2.8 M€);
- PICC - Physics of Ion Coulomb Crystals (3.0 M€);
- QUANTIP - Quantum integrated photonics (3.2 M€);
- QUEVADIS - Quantum engineering via dissipation (1.4 M€);
- **SCOPE** - Single Cooper pairs electronics (2.6 M€)

The QIPC coordination actions

Since 2005 a series of Coordination Action Projects has supported the QIPC initiative. Their goal is to collaborate with the QIPC FET proactive initiative in developing a strategy and in carrying out common activities. ERA-Pilot QIST started out to promote QIPC research in Europe and to give recommendations to European and national authorities on policy, structuring, coordination and funding. One of its important contributions was the stimulation of the QIPC Roadmap and the compilation of information about national and international QIPC programmes. Its successor QUROPE aimed at structuring the European QIPC research community around the FET QIPC proactive initiative and covered a large spectrum of activities like: developing a common European vision, strategy and goals for QIPC research, updating the QIPC roadmap, increasing the public awareness and aim at broad dissemination activities; developing a map of European QIPC groups; organizing scientific meetings; creating links with industry and developing international collaboration outside of Europe. QUROPE entertained close links to some 80 research groups and was instrumental to give the European QIPC community a strong voice.

In February 2010 the project **QUIE2T** has taken over the coordination tasks from QUROPE. It aims at strengthening and advancing the European scientific and technological excellence in the field of Quantum Information Foundations and Technologies (QIFT) and fostering the FET Proactive in a similar way as QUROPE did. It also aims at setting up a sustainable research network, structured around four Virtual Institutes for Quantum Computation, Quantum Communication, Quantum

Information Sciences and Quantum Technologies, and promoting it at the European level.

Finally the ERA-NET initiative **CHIST-ERA** (started in December 2009) though not entirely devoted to the QIPC field, will have QIPC as a topic in its first joint transnational call for projects (opening in September 2010) for an approximate volume of 10 M€.

QIPC in other parts of the EU framework programme for research

While the QIPC research activities have been initiated in the FET programme, they turned out to develop ramifications relevant to other EU programmes dealing with ICT and research in general. These were either driven by the potential of technological application or the scientific impact on neighbouring disciplines.

The strategic objective on Security of the IST Research Program had funded SECOQC – "Development of a Global Network for Secure Communication based on Quantum Cryptography" with 11.35 M€ in FP6 . The consortium comprises 40 excellent research groups in the field of applied quantum cryptography to realize an open network for dependable and secure long-range quantum communication building upon a Quantum Key Distribution (QKD) technology. The functionality of the developed architecture has been successfully demonstrated in the end of 2008. In addition the consortium published a White Paper on Quantum Key Distribution and Quantum Cryptography (2007) and started activities on standardization of the developed technolgy.

The objective on organic photonics and other disruptive Technologies has funded in FP7 one QIPC project: QuRep (1.9 M€) on quantum repeaters for secure long-distance communications in state-of-the-art optical fibre-based telecommunication networks.

Other projects in the area of QIPC funded by the European Commission research program in general are the two Marie Curie research training networks funded by the Marie Curie program of DG RTD. They are CONQUEST: "Controlled Quantum Coherence and Entanglement in Sets of Trapped Particles" and ATOMCHIPS.

Role of the FET QIPC proactive initiatives

The FET QIPC proactive initiative and its successors play a leading role in connecting the European research activities in the field. Besides providing important funds for research activities they strive to

- Foster collaboration between research groups in different countries;
- Facilitate exchange of knowledge, students and researchers between different groups;
- Establish free movement of knowledge as a fifth freedom in Europe besides people, goods, capital and services;
- Plan pan-European events and dissemination activities to promote a comprehensive public image of the field through conferences, workshops, common European web portal;
- Structure and strengthen the research community;
- Establish and maintain a dialogue with research managers in the member states and at the European level;
- Define a common strategy for research;
- Establish a dialogue with industry;
- Create international alliances and a strategy for international collaboration.

In each of the objectives listed above significant progress has been made. Particular highlights have been

- The establishment of a research agenda which is called QIPC strategic report on current status, visions and goals for research in Europe. 40 leading scientists in QIPC have contributed to this research agenda. It was published in 1999 for the first time with and since then regularly updated. This version is the 6th update;
- The organization of QIPC conferences. A biannual international conference series on quantum

information science and technologies has been started and become a big success. In the last two editions in Barcelona (2007) and in Rome (2009) the organizers could attract more than 300 participants not only from Europe, but also from Asia and the US;
- The raising of interest from relevant industry. The coordination actions managed to create links with industrial players active in communication and networking technologies. For example industry sessions have been organized at the QIPC conferences and a dialogue with interested companies has been established. Some of them even joined a research consortium with QIPC scientists to run the European project SECOQC. Overall the ground has been prepared for the swift up-take of commercially interesting results coming out of the QIPC research activities;
- The attraction of international partners to collaborative EU research projects. While the QIPC activities have started as a European research programme with mainly partners from Europe, it turned out that more and more research groups from overseas are eager to join in. In consequence the number of international partners in the QIPC projects hase risen in the last calls to about 10% of the total. This development is supported by the availability of funding for these partners under certain conditions such as unique expertise of the partner. The experiences have been very positive so far;
- The acknowledgement of QIPC researchers' scientific work through numerous prestigious Prizes including the Nobel Prize in Physics (2005) to mention one. The community is also proud to count more than 10 grantees of the European Research Council amongst them.

In the future EU's strategy will be to further foster the QIPC activities with a view to stimulate and facilitate the collaboration of the national funding agencies at European level and to create the conditions for a fast transition of scientific results to new technologies. First steps towards stronger collaboration with national and regional funding bodies have been taken. The CHIST-ERA project with partners from 9 different member states will implement a joint call for proposals in the second half of 2010 in the frame-work of a ERA-NET action. Furthermore, an ERA-NET plus action in the research domain of QIPC is planned for the year 2012. And last, but not least the QIPC community intends to participate in the flagship initiatives being lauched by the FET programme from 2012 onwards. These European initiatives are supposed to start long-term, visionary, goal-driven and large-scale research programmes in ICT targeting key scientific breakthroughs with a strong basis potential for technological innovation and economic exploitation.

In conclusion, there is good hope that the field of QIPC will keep and even increase its momentum as a locomotive in longterm ICT research and will eventually contribute to the transformation of scientific results into commercially applicable technologies for the benefit of the whole European society.

3.2 National funding

As a basic research field, QIST is still traditionally funded by the different national governmental organisation depending on the country (ministry, governmental agency etc.). These agencies fund every research topics and QIST is typically a small percentage of the overall budget (in the percent range). However many of them have recently developed focus program or umbrella topics for QIST.

The identified main national founders for each country are the following

- **Austria**
  - Austrian Federal Ministry of Transport, Innovation and Technology (BMVIT)
  - Austrian Research Promotion Agency (FFG)
  - Zentrum für Innovation und Technologie GmbH
  - City of Vienna
  - Austrian Science Fund (FWF)
  - Tiroler Zukunftsstiftung
- **Belgium**

    - Fund for Scientific Research - Flanders/Belgium (FWO)
    - Fondation National de la Recherche Scientifique (FNRS)
    - Communauté Française de Belgique
    - Belgian Federal Science Policy Office
- **Bulgaria**
    - Ministry of Education and Science
    - National Science Fund
- **Czech Republic**
    - Ministry of Education
    - Czech Science Fundation
    - Förderagentur der Republik Tschechien (GACR)
    - Förderagentur der Akademie der Wissenschaften (AVCR)
    - Ministry of Defense, Ministry of Interior
- **Cyprus**
    - Research Promotion Foundation (RPF)
- **Denmark**
    - Danish National Research Foundation (DG)
    - Ministry of Science Technology and Innovation
    - Strategic Research Centre for Nano Science
    - Danish Research Agency (FORSK)
    - Danish Agency for Science, Technology and Innovation (FIST)
- **Estonia**
    - Estonian Science Foundation (EstSF)
    - Ministry of Education and Research
    - Ministry of Economics Affairs and Communication
    - EE Enterprise Estonia
- **Finland**
    - Academy of Finland
    - National Technology Agency of Finland (TEKES)
- **France**
    - Agence Nationale pour la Recherche (ANR)
    - Région Ile de France (Paris area), which supports QIST trough two main channels:
        - Institut Francilien de Recherche sur les Atomes Froids (IFRAF)
        - Centre de compétence NanoSciences Ile de france (C'NANO)
    - Région Rhone-Alpe
    - Centre National de la recherche Scientifique (CNRS)
    - Ministère de la Recherche
    - Délégation Générale pour l'armement (DGA)
    - Direction de la Recherche Technologique
    - ANVAR (L'agence francaise de l'innovation)
    - Ministère de l'Économie des Finances et de l'Industrie
- **Germany**
    - Deutsche Forschungsgemeinschaft (DFG)
    - Bayerisches Staatsministerium
    - Landesstiftung BW
    - Max-Planck-Society
    - VDI Technologiezentrum GmbH
    - Projektträger im DLR (PT-DLR)
- **Greece**
    - Ministry of Development
    - General Secretariat for Research and Technology (GSRT)
- **Hungary**
    - Ministry of Education
    - Hungarian Scientific Research Fund
    - Hungarian Academy of Science
    - National Office for Research and Technology (NKTH)
- **Ireland**
    - Advisory Science Council (ASC)
    - Science Foundation of Ireland (SFI)

    - Irish Research Council for Science, Engineering and Technology (IRCSET)
- **Italy**
    - Italian National Research Council (CNR)
    - Ministry for Education and Research (MIUR)
    - Istituto Nazionale di Fisica Nucleare (INFN)
    - Istituto Nazionale di Alta Matematica (INDAM)
    - Istituto Nazionale di Ricerca Metrologica (iNRiM)
    - Regione Piemonte
    - San Paolo Fundation
    - Nanotechnology lab
    - QIPC is also one of the two scientific lines that CNISM (Consorzio Interuniversitario per le Scienze Fisiche della Materia) decided to support
- **Luxembourg**
    - Fonds National de la Recherche
- **Netherlands**
    - Foundation for Fundamental Research on Matter (FOM)
    - Netherlands Organization for Scientific Research
    - The Technology Foundation (STW)
- **Poland**
    - Ministry of Science and Higher Education
    - Ministry of Science and Information Technology
    - Polish Academy of Sciences
    - Polish National Centre for Research and Development (NCBiR)
- **Portugal**
    - Science and Technology Foundation (FCT)
    - Innovation Agency (AdI)
- **Russia**
    - Russian Foundation for Basic Research
- **Slovakia**
    - Research and Development Support Agency (APVV)
    - Quantum Information program of the Slovakian Academy of Science
- **Spain**
    - Ministry of Education and Science (MEC)
    - Ministry of Science and Innovation (MCINN)
    - University of Barcelona
    - Generalitat de Catalunya
    - Madrid General Government
- **Sweden**
    - Knowledge Foundation
    - Swedish Foundation for Strategic research (SSF) via the QIP consortium (Chalmers, Göteborg, and KTH, Stockholm)
    - Swedish Research Council (VR) – Natural and Engineering Sciences
    - Swedish foundation for International Cooperation
    - The Swedish Royal Academy of Science
- **Switzerland**
    - Swiss National science Foundation (SNF)
- **Turkey**
    - Tubitak-Uekae
- **United Kingdom**
    - Royal Society
    - Research Council
    - DTI Department of Trade and Industry
    - Engineering and Physical Sciences Research council (EPSRC)
    - Defence Science and Technology Laboratory (DSTL)

3.3 Local funding

As a highly promising field, QIST is often supported at the local level (city or region). Several examples in Europe have led to the creation of centers for Quantum Information, sometimes in a more general context. This funding can be quite stable in time, and usually consists in particular of a large startup sum, but also in a more long-term support. One can cite for instance:

- The region of Catalonia in Spain strongly supported the creation of the Institute for Photonic Science (ICFO) in 2002 in Barcelona, which has a strong emphasis on QIST. This institute is meant to be permanent and, when at full size, will employ up to 300 people;
- The Region of Tyrol and the city of Innsbruck in Austria also supported the creation of the Institute for Quantum Optics and Quantum Information (IQOQI); this centre was mentioned as "an example of outstanding quality" for activity in atomic molecular and optical physics research in a recent report of the US National Research Council;
- The Region Paris-Ile-de-France through the creation of the Francilian Institute for Research on Cold Atoms (IFRAF), which comprises more than 30 groups from 6 different laboratories in Greater Paris;
- The United Kingdom is funding an Interdisciplinary Research Collaboration (IRC) in QIPC between leading research universities and industrial laboratories. The initiative started in April 2004 with a funding level of 15M€ in four years;
- The German ministery for education and research (BMBF) launched in January 2010 a programme on quantum communication as part of its strategic initiative "IKT 2020".

These initiatives can either, as for ICFO, create a new centre of excellence, or as in the case of IFRAF, construct a new centre of excellence from an existing pool of competence. In most cases the local funding is motivated by the development of a high-impact scientific field and high-level research, and it has a beneficial impact on local industry and economy.

3.4 Other funding

As possible applications of QIST become likely to appear in the near future, start-ups have begun to emerge. The main interest so far is in quantum cryptography, in particular Quantum Key Distribution.

The oldest European company is IdQuantique, spin-off from the university of Geneva in 2001. Several new appeared recently: **SmartQuantum**, created in 2004 in Lagnon, France, **Qutools** in Munich, Germany. Other competing start-ups for early adopters on the market are **MagiQ**, **Optemax**, and **Qinetiq** from the USA. These companies are mostly spin-off of QIST research groups, funded through the usual start-up scheme: university incubators at the early stage of their existence, then business angels or hedge funds to sustain them beyond their first years of existence. They mainly develop commercial fibered QKD systems, but most of them admit that there is no real market for such system yet. There is however already a small but active market for Quantum-based Random Number Generators (**IdQuantique**).

Quantum computing has also aroused interest for possible commercial applications. However the investment required and the timescale for developing a commercial quantum computer are much larger than for a QKD system.There is no start-up interested in developing a quantum computer in Europe so far, the only example known being in Canada, where one company (D-Wave) has been created in 1999.

Several very large companies have also interest in QIST, with a focus on applied system research and components. In Europe, the main companies involved are Toshiba (UK), Thalès (France), France Telecom (France), Philips (Netherlands), Pirelli (Italy), Hitachi (UK) Hewlett-Packard (UK). Worldwide, companies such as IBM and NEC are also involved in QIST. The companies either have their own lab (Toshiba, HP, IBM), and/or can alternatively fund research groups (Philips). It has proven practically impossible to obtain reliable information about the amount of investment in QIST by these companies.

Another interesting source of funding is the **European Space Agency (ESA)**. Several 50 k€ feasibility studies on Quantum Communication in space were successfully completed since 2002 and one experimental terrestrial 200 k€ study over 144 km horizontal free-space link is ongoing. Within ESA's science program, the proposal Space-QUEST (to place a QKD terminal onboard the International Space Station) was rated as 'outstanding'. Several European industries submitted proposals to develop a prototype engineering model of a faint laser and entangled photon source with a total budget of 600 k€. In the second half of 2008 a study on the feasibility of a QKD system on various future satellite missions is expected with 300k€. So far more than 1Mio€ have been spent on the different studies under evaluation at the time this report was made. But the overall budget for the Space-QUEST project, if it is accepted, would be approximately 80 M€ until 2014, with approximately 20% devoted to basic research. If successful, this would make ESA a major funding source for QIST in Europe.

3.5 QIPC research in the international context

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.

Through the activities of the FET proactive initiatives in FP5, FP6 and now FP7, 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 (and even superior) with the US, while other nations have begun systematic ramp-up in QIS investments.

In the last years, significant growths in the research efforts within the field of QIST have been made worldwide. Especially the US has fostered their research activities, supported by a number of public funding agencies (for example the National Science Foundation and the Defense Advanced Research Projects Agency). To retain our leading position in research and to capitalize on the Commission's already significant investments in QIS (50M€ in FP5 and FP6, 45M€ in FP7), it is vital to ensure that the EU investment in QIS remains competitive with the US and other national/continental QIS investors.

In the figure below we plot the 2008 funding figures in the QIPC area for the US, Canada, Japan and Europe. QIS R&D support on the scale of ~15M€/year puts Europe below average 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.

QIPC funding/year in the US, Japan, Canada and Europe. We take only into account the money spent according to a coordinated joint programming agenda (that is for European National funding is not kept into acount)

3.6 The European flavor, vision and goals

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 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

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

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 and molecular-ICT R&D effort.

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

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 covering partially Quantum Information Science and Technology (CHIST-ERA). The creation of a truly European Research Area is essential and justifies additional funds for the QIPC programme.

3.7 QIPC in a wider scientific and technological context

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.

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. 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.

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.

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:

- 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 (QKD) 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.
- 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.
- 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 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. The communication of qubits will be an important ingredient in taking full advantage of what is possible with quantum technologies, from quantum computing to unconditionally secure communication based on quantum key distribution The first application, quantum cryptography, was discovered independently in the 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 has focused on 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 basic quantum communication schemes is becoming routine work in the laboratory, non-trivial problems emerge in high bit rate systems and long-distance applications. The transition from proof-of-principle laboratory demonstrations to deployment in real-world environments defines a new set of challenges in the QIFT domain. The issues of scale, range, reliability, and robustness that are critical in this transition cannot be resolved by incremental improvements, but rather need to be addressed by making them the focal point of the research and technology development agenda. This needs to target both the underlying technologies:

- Detectors
- Sources
- Quantum Memories and Interfaces

as well as their integration for specific applications, such as:

- High rate, fibre or free space quantum communication
- Quantum Repeaters
- Satellite-based communication links

There are key technological limitations for high-speed quantum communication and fundamental roadblocks for long distances. A significant speed limitation on the distribution of true randomness, a

resource for many security protocols including QKD, is due to relatively slow (~4Mbps) quantum random number generators (QRNGs) – see Appendix A. Novel schemes and advanced entanglement enabled technologies, using and possibly combining both discrete and continuous variable encoding aspects, will be required for the next generation devices to surpass current rate limitation. The distances over which quantum information can be communicated face fundamental limitations due to transmission losses in the quantum channels, both free space and fibre. In fibre, this limit is a few hundred kilometres. Recent quantum cryptography experiments already come close to such distances but with impractically low distribution rates. There are two possible solutions to overcome this limitation: use free space systems in satellite configurations; or, use quantum repeaters, a theoretical concept proposed in 1998 the analogue of fibre optical amplifiers that made global fibre communication feasible. The later requires quantum interfaces or memories for the inter-conversion from photonic (distribution) to atomic (storage) systems.

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 exists anywhere in the universe. This promise is guaranteed by the laws of Nature and does not rely on any mathematical assumption. Consequently, these strings of correlated bits provide perfectly secure keys ready to be used in standard crypto-systems. However, for quantum physics to hold its promise, the quantumness of these distributed systems needs to be ensured. Consequently, it is of strategic importance to not only develop the technology to distribute quantum resources, such as entanglement from one location to a distant one but to be able to ensure that its truly quantum nature is preserved. A key test of this quantumness consists in measuring the correlations and proving that they violate a certain inequality, known as the Bell inequality. Following on from this is the idea of “Device Independent” security proofs that provide one possibility for characterising the quantum nature of a system. Practical and feasible schemes to test these device independent approaches and ensure the quantum nature of systems will be crucial as communication links and networks become more complex.

From the present situation, where commercial systems already exist, we briefly review the underlying foundational technologies and more generally, quantum communication from the perspective of high-rate and long-distance solutions and how to characterise and optimise these systems and resources.

4.1.1 Detectors

Physical approaches and perspectives

All photonic approaches to quantum information technology rely upon an efficient detection technology. Although single photon detectors are commercially available, these are simple digital devices, which detect the presence or absence of one or more photons. Future detector technologies will not only have to have a dramatically higher detection efficiency but also considerable lower dark count rates as well as a timing jitter that does not limit the transmission rates. The commercial detection systems are based on semiconductor avalanche photodiodes (APDs) such as Si (400-1000nm) and InGaAs/InP (1100-1700nm). These are robust and generally only require electric cooling. Recent alternatives include superconducting devices, either transition-edge sensors (TES) that have shown efficiencies > 90% but remain relatively slow, or superconducting nanowire single photon detectors (SNSPD) that are faster (both low jitter and high count rates) but have only realised efficiencies ~ 25%. Both of these have demonstrated photon number resolution capability. The need for cryogenic cooling is offset by the potentially high performance. For continuous variable (CV) measurements single photon resolution is not needed. There, apart from the quantum efficiency and bandwidth, the signal to noise ratio of the detector module is important. This is not an extensive list, but focuses on the most advances or promising technologies in the context of quantum communication.

European groups working in this field include – for APDs: S. Cova (Milan, I), A. Shields, (TREL, UK), H. Zbinden (Geneva, CH), J. Rarity (Bristol, UK), G. Buller (Heriot-Watt, UK), A. Giudice (Micro Photon devices, I), G. Ribordy (id Quantique, CH):- for superconducting devices: G. Gol`tsman (Moscow, RU),

A. Fiore (Eindhoven, NL), V. Zwiller & T.M. Klapwijk (Delft, NL), R. Leoni & S. Pagano (CNR Rome, I), J-C. Villegier & J-Ph. Poizat (CEA Grenoble, F).

State of the art

A severe limitation of today's photon detection technology is the maximum count rate. For example, InGaAs/InP APDs have been traditionally operated in a gated mode with a maximum repetition frequency of 1-10 MHz and a maximum count rate of 100 kcps. However, this field has recently been reinvigorated with novel work on the operating electronics providing advances in rapid gating (GHz) [1] and continuous (free-running) [2] operation opening up new regimes of operation and performance. The superconducting devices have demonstrated photon number resolution capability and high efficiency: TES > 90% [3]; SNSPD ~24% [4]. The later capable of a significantly higher count rate (potentially GHz) and lower timing jitter (<100ps). In the continuous variable regime, several groups report quantum efficiencies approaching 100% using commercially available PIN diodes with increasing bandwidth (> 100 MHz) and signal-to-noise ratios. Conceptually, the strict separation between discrete and continuous detection schemes is complemented by hybrid detection approaches [5].

Challenges

Europe and Japan are currently leading the way for the APD detection schemes, while the US is a clear leader for superconducting devices. The main challenges for APDs are:

- Explore these new operating regimes – faster (> 2 GHz), higher efficiency (> 25% for InGaAs/InP);
- Adapt devices (semiconductor & electronics) for specific applications, e.g. peak efficiency wavelengths;
- Transfer these recent advances to the commercial sector.

For CV detection schemes

- Faster, compact and stable homodyne, heterodyne and hybrid detectors that can be integrated in all-fibre systems;
- Local oscillator phase retrieval techniques for weak coherent states have to be developed for homodyne measurements after fibre channels;
- The optical detection of the signal has to be optimised for free space systems to prevent losses that degrade the CV states (high overall quantum efficiency).

For superconducting detectors

- Fabrication of detectors in cavity structures for high efficiency;
- Improve fabrication and coupling to increase the efficiency and robustness;
- Demonstrate the detectors: lower dark counts (<1Hz), increased detection efficiency (> 70%), low jitter (< 100ps) and photon number resolving capabilities;
- All of these characteristics in one device.

[1] Z. L. Yuan, B. E. Kardynal, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. 91, 041114 (2007)
[2] R. T. Thew, D. Stucki, J.-D. Gautier, and H. Zbinden, A. Rochas, App. Phys. Lett., 91, 201114 (2007)
[3] A. E. Lita, A. J. Miller, and S-W. Nam, Opt. Exp., 16, 3032 (2008)
[4] X. Hu et al., Opt. Lett., 34, 3607 (2009)
[5] C. Wittmann, M. Takeoka, K.N. Cassemiro, M. Sasaki, G. Leuchs, and U.L. Andersen, Phys. Rev. Lett., 101, 210501 (2008)

4.1.2 Sources

Physical approaches and perspectives

Sources of quantum light in the discrete variable regime have traditionally relied on spontaneous parametric down-conversion (SPDC) in bulk crystals. This has been extended to waveguides in periodically poled materials that have significantly improved performance. The development of all-fibre entanglement sources, based on four-wave mixing are a promising solution that needs further investigation. Deterministic sources that avoid probabilistic multi-pair events, associated with the previous schemes, have advanced to the point where entangled photon pairs can be generated by the optical excitation of the bi-exciton state of a semiconductor quantum dot. Other single photon sources based on NV diamond centres and single molecules in solids have been realised and progress continues on single photon sources in diverse materials for sources ranging from the visible up to 1550nm. In the continuous variable regime sources of squeezed and entangled light typically rely on either parametric oscillators in bulk crystals or the Kerr effect in optical fibres.

European groups working in this field include: J. Rarity (Bristol, UK), A. Zeilinger (Vienna, AT), A. Shields, (TREL, UK), N. Gisin & H. Zbinden (Geneva, CH), I. Walmsley (Oxford, UK), O. Benson (Berlin, D), M. Mitchell & J. Eschner (ICFO, E), J-W. Pan (Heidelberg, D), C. Silberhorn (Erlangen, D), S. Suage (Stockholm, SW), V. Sandoghdar (Zurich, CH), A. Beveratos (Paris, F), A. Fiore (Eindhoven, NL), J. Wrachtrup & F. Jelezko (Stuttgart, D), G. Leuchs (Erlangen, D)

State of the art

Two important parameters for quantum light sources are bandwidth (BW) and efficiency – both creation (brightness) and coupling into other systems. Furthermore, the sources need to be adapted and developed to the desired applications, for example, there are currently few systems that approach quantum memory bandwidths (1-100 MHz). First steps in resolving these limitations have been made for atomic [1] and telecom [2] wavelengths. These waveguide sources demonstrate high brightness and are capable of saturated performance (limited by multiple-pair probabilities). All-fibre entanglement sources based on four-wave mixing [3] provide a high degree of non-degeneracy that may also be useful to couple telecom wavelength with quantum memories. For free-space sources, both entangled photon pairs as well as single photon sources it is preferable to use shorter wavelengths than for fibre networks. This is to limit the diffraction on the sending aperture, which is especially important for very long optical communication links, e.g. between geo-stationary orbiting satellites as well as the communication to a future moon or even a Mars base. Diverse approaches to continuous variable quantum state sources [4, 5], are under development as well as nonlinear interactions in atomic gas cells for CV non-classical light sources.

Challenges

There is no clear global leader on high-rate photon-pair sources, however, Europe is leading in efforts towards coupling photonic and atomic systems despite the only report of actual coupling coming from Japan, while Europe plays a leading role for CV sources, competing with Australia and Japan. There are two extremes of operation under study – for atomic systems with narrow bandwidths and for satellite-based schemes where BW requirements are less critical but the generation rates need to compensate limited transmission time windows due to satellite availability. The main challenges for photon sources are:

- High single & photon-pair rates (rates should be BW limited and take into consideration all intrinsic source losses, such as coupling and filtering);
- High fidelity (> 90% HOM visibility) between multiple sources;
- Improved coupling of generated photons into the quantum channel (single > 50% & photon pairs > 70%);
- Match bandwidths with quantum memories;
- Single-photon sources have made spectacular progress in the last years, but there are still open questions as to whether they can realise high repetition rates, high coupling efficiency

and electronic cooling (no liquid helium);
- Development of efficient, stable and pure sources of squeezed, entangled and single photon states;
- Combine efficient squeezing and single photon detection to reliably generate and grow large cat states;
- Use quantum relays exploiting quantum teleportation and entanglement swapping. Dividing the connection into sections allows one to open the receiving detector less frequently, thus lowering the dark-count rate. It should be stressed that quantum relays are a necessary stepping-stone towards quantum repeaters;
- The next crucial challenge in this direction will be a field demonstration over tens of km of entanglement swapping and high fidelity (> 90%) Bell-State measurements.

[1] M, L. Scholz, et al., Phys. Rev. Lett., 102, 063603 (2009); A. Haase, et al., Opt. Lett., 34, 55 (2009); X. H. Bao, et al., Phys. Rev. Lett. 101, 190501 (2008); J. S. Neergaard-Nielsen, et al., Opt. Exp., 15, 7940 (2007)
[2] E. Pomarico, et al, New J. Phys., 11 113042 (2009)
[3] J. Fulconis et al., Phys. Rev. Lett. 99, 120501 (2007)
[4] H. Vahlbruch et al, Phys. Rev. Lett. 100, 033602 (2008)
[5] R. Dong et al. Opt. Lett. 33, 116 (2008)

4.1.3 Quantum memories and interfaces

Physical approaches and perspectives

An interface between quantum information carriers (quantum states of light) and quantum information storage and processors (atoms, ions, solid state systems) is an integral part of a full-scale quantum information system. Advances with atomic gases and trapped ions have been steady and new efforts on rare earth ions in solids have recently made considerable gains. Recent efforts in the EU project QAP have seen diverse systems making key proof-of-principle demonstrations of long storage times, high efficiency, and high fidelities. An important aspect arising from this work is the need for multiplexing (space, time, frequency) to increase potential distribution rates. In the context of quantum communication, the goal for all of these approaches is integration with photonic (flying qubit) systems and their operation in complete quantum repeater architectures and protocols.

European groups working in this field include: N. Gisin & H. Zbinden (Geneva, CH), E. Polzik (Copenhagen, DK), H. Weinfurter (Munich, D), S. Kröll (Lund, SW), J-L. Le Gouet (Paris, F), E. Giacobino (CNRS, Paris, F), J. Rarity (Bristol, UK), A. Shields, (TREL, UK), M. Mitchell & J. Eschner (ICFO, E), I. Walmsley (Oxford, UK)

State of the art

We have already seen single photons stored in mesoscopic cold atomic ensembles [1] with storage times of order of 10 μs, with a maximum storage and retrieval efficiency of 18%. Heralded entanglement between spatially separated ensembles has been achieved [2] and entanglement between single photons and stored collective spin excitations has been demonstrated [3]. The best retrieval efficiencies demonstrated to date for single stored excitations are 50% in free space [4] and 84% in cavities [5]. Recently, the storage duration of single collective excitations has been improved up to several ms [6], although again with lower retrieval efficiencies (~20%). Storage and retrieval of quantum continuous variables has also been demonstrated in atomic vapours [7] and in cold ensembles [8]. In ensemble based solid-state quantum memories, a light-matter interface at the single photon level has been realised recently [9], importantly with multimode (4-mode) storage and high conditional fidelity (98%). Bright light pulses have been stored for more than 1 s [10] and with efficiencies higher than 45 % (for short storage times) in doped crystals. For quantum dot systems NV-centres in diamond and single molecules in solids, quantum interference between two photons emitted from two remote emitters is still under investigation [11].

Challenges

Europe and the US are both well advanced with a range of architectures under study, however, this remains a fledgling domain within the field of QIFT and the field and the range of architectures and materials under investigation is rapidly expanding so we concentrate here on those most closely focused on quantum communication oriented applications. Key challenges for quantum memories and interfaces are:

- Achieving efficient storage and retrieval for the quantum state;
- Increasing storage time;
- Improving the fidelity of storage;
- Improving multi-mode storage capacity;
- Coupling from the quantum memories to communication channels;
- All of these in one single system.

[1] T. Chaneliere et al., Nature, 438, 833 (2005); M. D. Eisaman, et al., Nature, 438, 837, (2005); K. S. Choi, et al., Nature, 452, 67 (2008)
[2] C.W. Chou, et al., Nature, 438, 828 (2005)
[3] D.N. Matsukevich, et al., Phys. Rev. Lett., 95, 040405 (2005); H. de Riedmatten, et al., Phys. Rev. Lett., 97, 113603 (2006)
[4] J. Laurat, et al., Opt. Exp. 14, 6912 (2006)
[5] J. Simon et al., Phys. Rev. Lett. 98, 183601 (2007)
[6] B. Zhao, et al., Nat Phys 5, 95 (2009); R. Zhao, et al., Nat. Phys., 5, 100, (2009)
[7] B. Julsgaard, et al., Nature, 432, 482, (2004); J. Appel, J., et al., Phys. Rev. Lett., 100, 093602 (2008); J. Cviklinski, et al., Phys. Rev. Lett., 101, 133601 (2008)
[8] K. Akiba, et al., New J. Phys., 11, 013049 (2009)
[9] H. de Riedmatten, et al., Nature 456, 773 (2008)
[10] E. Fraval, et al., Phys. Rev. Lett., 95, 030506 (2005)
[11] K. Sanaka, et al., Phys. Rev. Lett., 103, 053601 (2009); R. Lettow, et al., Opt. Exp., 15, 15842 (2007)

4.1.4 Towards High Rates

Physical approaches and perspectives

Fibre

Groups are currently working on fibre systems that encode in polarisation, phase, photon number and time-bins, using both discrete or continuous variables (CV). Weak-pulse encoding schemes are by far the most practical but entanglement based schemes lay a solid foundation for longer distance communication schemes involving repeaters. The extension to multiplexed systems has been a recent but necessary step.

European groups working in this field include: N. Gisin & H. Zbinden (Geneva, CH), A. Shields, (TREL, UK), A. Zeilinger (Vienna, AT), J. Rarity (Bristol, UK), G. Leuchs (Erlangen, D), P. Grangier (Paris, F), P.D. Townsend (Cork, IRL), G. Ribordy (id Quantique, CH).

Free Space

Many current free-space systems focus on polarisation based encoding. Traditionally dominated by discrete variable systems, work on CV systems has recently been reinvigorated. The CV squeezed states offer potentially higher key rates and longer distances than coherent state CV protocols. The potential for using non-Gaussian states and higher dimensional Hilbert spaces (complex spatial modes/polarisation patterns) may increase the efficiency and capacity of quantum information

protocols.

European groups working in this field include: A. Zeilinger (Vienna, AT), H. Weinfurter (Munich, D), J. Rarity (Bristol, UK), G. Leuchs, (Erlangen, D).

State of the art

The recent SECOQC QKD network demonstration illustrated the range of different approaches that are currently being developed in Europe [1]. It also demonstrated two other important points: the idea of a trusted-node quantum network; and that different architectures could be made to work transparently on one network. All QKD systems were fully automated, including self-compensation for environmental influences on the fibre link. The demonstration involved one-time pad encrypted telephone communication, a secure (AES encryption protected) video-conference with all deployed nodes and a number of rerouting experiments, highlighting basic mechanisms for quantum network functionality. The average link length was between 20 and 30 km, the longest link 83 km. This is an important interim step (before quantum repeaters) as point-to-point quantum key distribution schemes approach their distance limits. Recent experiments have approached these limits for both weak pulse schemes, with > 144 km for field trials in free-space [2] and > 200km in fibre [3] - as well as > 200km in fibre for entanglement-based schemes [4] and 25km for CV systems [5] in the lab.

Challenges

Europe is a clear leader in this domain with the US and Japan not far behind and China rapidly approaching. The central challenge for point-to-point systems is to increase rates, either simply by higher clock rates or through multiplexing multiple signals or systems. The integration of multiple components for fast, efficient and continuous operation is perhaps the most demanding obstacle. Key challenges are:

- Faster electronics for increased application-dependent performance incorporating sources, detectors, QRNGs, low-loss phase and amplitude modulators and their integration. This is mainly a (non-trivial “quantum opto-electronics”) engineering problem;
- Integrated optics design (waveguides/fibres/circuits) for more compact and robust sources and interfaces;
- Extension of GHz clock rates into the MHz continuous secure key distribution regime;
- Multiplexed quantum and classical channels for increased communication bandwidth;
- Fast (> GHz), low-loss (< 1dB) optical switching;
- Invent and investigate new protocols inspired by existing and reliable components, like “decoy states” [6], SARG [7] and COW [3] protocols. Look at systems that combine aspects of discrete and CV operation. This is mainly a matter of the physicists’ imagination;
- Determine the benefit of free space links using polarisation variables – these prevent dephasing of the CV quantum states with respect to local oscillator phases used in homodyne measurements and straylight is effectively filtered by the homodyne measurement, thus facilitating the implementation of daylight links;
- Quantum communication with entangled states will be important to further develop quantum teleportation and entanglement swapping in view of their possible use in connecting future quantum networks.

[1] M. Peev, et al., New J. Phys. 11 075001 (2009)
[2] T. Schmitt-Manderbach, et al., Phys. Rev. Lett. 98, 010504 (2007)
[3] D. Stucki, et al., Opt. Exp., 17, 13326 (2009)
[4] J. F. Dynes, et al., Opt. Exp., 17, 11440 (2009)
[5] J. Lodewyck et al.,Phys. Rev. A 76, 042305 (2007)
[6] W.-Y. Hwang, Phys. Rev. Lett. 91, 057901 (2003)
[7] V. Scarani, et al., Phys. Rev. Lett. 92, 057901 (2004)

4.1.5 Towards Long Distances - Quantum Repeaters

Physical approaches and perspectives

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 a classical light-matter interface. In quantum information processing, this simple approach is inadequate as it destroys the quantum aspect. Quantum communication requires a coherent storage interface – quantum repeaters. There are a significant number of proposals for realising quantum repeaters ranging from atomic ensembles (cold and hot gases and solid state systems) and linear optics – perhaps the simpler and more advanced approach, to atom and ion approaches - that could take advantage of deterministic entanglement swapping operations. Other approaches based on NV centres in diamonds and quantum dots have been proposed as well as hybrid schemes that combine coherent states and individual quantum systems. A detailed review of ensemble approaches using linear optics and discussions on several others can be found here [1].

State of the art

Great progress has been made in this direction in the last few years by European groups, on the photonic side, with real world teleportation (3x2km, field) [2] and entanglement swapping experiments (lab) [3] as well as proof-of-principle repeater links [4] based on atomic ensembles. Significant progress continues on the way towards implementation of a repeater, by US groups (Lukin, Monroe, Kimble, Kuzmich and Vuletich) where a strong experimental effort on Electromagnetically Induced Transparency (EIT) stored light and quantum memories involving ensembles as well as single atoms can be identified and by European groups (Pan, Gisin, Polzik, Weinfurter) covering ensembles, in gas and solids, and single atom systems. Entanglement between single trapped ions/atoms/quantum-dots and single photons [5] at distances of up to 300 m and coherence times of several 100 μs [6] have been shown. Entanglement fidelities up to 90% were reported. Probabilistic entanglement between two single trapped ions at over 1 m distance has been demonstrated via two-photon interference on a beamsplitter [7]. Much of the recent development towards quantum repeaters has focused on quantum memories and interfaces and hence much of the state of the art is already mentioned there.

European groups working in this field include: H. Weinfurter (Munich, D), N. Gisin & H. Zbinden (Geneva, CH), J.W. Pan (Heidelberg, D), Schmiedmayer (Vienna, AT) E. Polzik (Copenhagen, DK), J. Rarity (Bristol, UK), E. Giacobino (CNRS, Paris, F).

Challenges

In the next 5-10 years we should see fibre optic systems that can beat the direct-transmission distance limitation of around 300-400 km. Initially, quantum repeaters that can function over 1-10 km will provide the building blocks for longer transmission systems – it is these building blocks that provide a scalable route towards pan-European and even global scale quantum communication. These distances will obviously need to be extended further, but not necessarily by much. We note that classical communication links are of the order of 50-100 km between amplification stages. The important aspect for quantum repeaters is the scaling of multiple quantum repeater links. Scalable quantum repeater systems will ensure that the concatenation of multiple links will extend quantum communication distances beyond this fundamental (loss-based) limit. Effort in the next few years should be focused on engineering the sources, interfaces and detectors specifically adapted to long distance transmission and working in unison – long coherence lengths, and high fidelity Bell-State measurements and work towards input/output coupling of photons to Quantum Memories etc. Challenges and directions of future work are thus similar to those already mentioned for quantum detectors, sources and memories and while many aspects have been demonstrated, all need to be improved and demonstrated in the one systems, i.e.:

- Extending memory capabilities to single photon/qubit storage in diverse media;

- Exploring hybrid approaches that combine both discrete and CV aspects for improved performance;
- Develop probabilistic repeater schemes, possibly integrated using atoms on chip technology;
- Integrated solutions such as CNOT gates on optical circuits or circuits that connect multiple elements: source; detector; interface, on a chip;
- Incorporate deterministic strategies for sources, storage and entanglement swapping;

[1] N. Sangouard, C. Simon, H. de Riedmatten, N. Gisin, arXiv:0906.2699v2 (2009)
[2] O. Landry, et al., J. Opt. Soc. Am. B, 24, 398 (2007)
[3] M. Halder, et al., Nature Physics, 3, 692 (2007); R. Kaltenbaek, et al., Phys. Rev. A, 79, 040302(R) (2009)
[4] C.W. Chou, et al., Science, 316 1316 (2007); Z-S Yuan, et al., Nature 454, 1098 (2008)
[5] B. B. Blinov, et al., Nature, 428, 153 (2004); J. Volz, et al., Phys. Rev. Lett., 96, 030404 (2006); R. M. Stevenson, et al., Phys. Rev. Lett., 101, 170501 (2008)
[6] W. Rosenfeld, et al., Phys. Rev. Lett., 101, 260403 (2008)
[7] D. N. Matsukevich , et al., Phys. Rev. Lett., 100, 150404 (2008)

4.1.6 Towards Long Distances - Satellite Quantum Communication

Physical approaches and perspectives

The European Space Agency ESA has supported various studies in the field of quantum physics and quantum information science in space for several years [1]. Quantum Communication has now reached a sufficient maturity level to allow for space qualification of the relevant components. The mission proposal Space-QUEST (Quantum Entanglement for Space Experiments) has been submitted to the European Life and Physical Sciences in Space Program and is now in the planning phase with ESA. The objective is to perform space-to-ground quantum communication tests from the International Space Station (ISS) as a first proof-of-principle demonstration of quantum communication using space-based platforms. The launch plan is compatible with 2014.

European groups working in this field include: A. Zeilinger (Vienna, AT), H. Weinfurter (Munich, D), J. Rarity (Bristol, UK), C. Barbieri & P. Villoresi (Padova, I), S. Cova (Milan, I), I. Walmsley (Oxford, UK), R. Renner (Zurich, CH), P. Martoloni (Rome, I), M. Dušek (Olomouc, CZ), M. Bourennane (Stockholm, SW) as well as an international team of 40 scientist on the Space-QUEST Topical Team as a scientific advisory committee.

State of the art

Many of the recent advances have focused on collaborative work taking place in the Canary Islands by several leading European groups. The key results range from highly practical aspects such as the implementation of detection synchronisation based on the ultra-stable clocks provided by the global positioning system (GPS), an active low bandwidth (tip-tilt) beam control for a free-space long-distance quantum communication link and more generally interfacing quantum communications with existing hardware for earth-based optical satellite communication: (1) the Optical Ground Station (OGS) of the European Space Agency ESA on the Canary Island Tenerife acted as the receiver station for a free-space long-distance quantum communication link [2]; (2) the Matera Laser Ranging Observatory (MLRO) in Southern Italy served as transceiver station for faint-pulse exchange with a low-earth orbit retro-reflecting satellite at a perigree of 1485 km [3]. Other important steps included: the demonstration of a continuous 24h free-space QKD link in the Vienna SECOQC network over 200 m; a design study for a satellite-based entangled photon source has been completed in collaboration with the European Space Agency ESA; and the quantum key distribution over 144 km (between the Canary Islands of La Palma and Tenerife) has been extended to entanglement-based distribution.

Challenges

The European groups have taken a leading role in this endeavour, although the current Space-Quest consortium also consists of groups in Australia, Japan and the US while Japan has independent plans for a QKD launch in 2013. The key challenges are:

- Development of compact & robust high photon flux sources – depending on the architecture and protocol, the systems must operate in short burst when satellites are in view;
- Develop novel CV protocols that could be immune to the high loss that exist in these links;
- Study complex spatial mode structures as decoherence-free states in free space channels, that don't suffer by turbulences / diffraction (discrete and CV);
- Robust systems that can for example withstand launch g-forces;
- Space certification for component technologies.

[1] J. Armengol et al., Acta Astronautica 63, 165 (2008); R. Ursin et al., Europhysics News, 40, 26 (2009)
[2] R. Ursin, et. al., Nature Physics, 3, 481 (2007); A. Fedrizzi, et.al., Nature Physics. 5, 389 - 392 (2009); T. Scheidl et al., arXiv:0811.3129 (2008)
[3] P Villoresi et al., New J. Phys., 10 033038 (2008)

4.1.7 New Applications and Protocols

Approach and perspectives

The field of quantum communication is still very young, having been essentially unknown until 15 years ago. As such, one should expect new ideas and leave open space for fundamental 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 efficiency and secrecy in communication. 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 many open theoretical questions of crucial importance for quantum cryptography. These 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 faster ways of distributing keys and quantifying their security.

For some quantum communication applications it can be useful to operate in a larger dimension Hilbert space. This can be obtained by preparing two photons entangled in more than one degree of freedom (hyper-entangled) for increasing the number of qubits or making more efficient measurements. Other proposals concern the generation of d-level quantum systems (qudits) by using different degrees of freedom. 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 approach would be preferential in real implementations, as is illustrated in the case of quantum key distribution. It is important to study under which circumstances such a replacement can be done. The adaptation and demonstration of device independent QKD will also be important for future secure networks. A relatively new idea could be using quantum memories to perform local operations and store the results while the classical communication is going on in communication protocols, which require local operations and classical communication (LOCC) are required. Transforming ideas of percolation to quantum networks has been a relatively new concept but one that opens some fascinating possibilities for network distribution of entanglement.

European groups working in this field include: S. Massar & N. Cerf (Brussels, B), A. Acin (ICFO, E), N. Gisin (Geneva, CH), M. Plenio (Ulm, D), J Eisert (Potsdam, D), R. Renner & S. Wolf (Zurich, CH), R.

Werner (Braunschweig, D), H. Buhrman (Amsterdam, NL).

State of the art

Important progress has been made in developing new protocols for quantum repeater architectures. A key concept that was recently introduced was the multimode capacity of quantum memories, which allows orders of magnitude increases in distribution rates [1]. Combining this with approaches that serialise distribution [2] may hold the potential for high rates and long distance. The possibility of a cheat sensitive quantum protocol to perform a private search on a classical database [3] have also been proposed with potential for experimental demonstrations foreseen. A return to some of the foundational concepts of QIFT has seen Bell inequalities find renewed importance for so-called “Device Independent” security [4].

Challenges

The main challenges for new applications and protocols are:

- Explore new verification strategies of single and multipartite quantum information links;
- Realize new modes of teleportation as a quantum communication primitive;
- Security proofs need to be optimised to cope with a wide range of experimental parameters (e.g. excess noise). The quantum channel can be verified by effective entanglement measures and / or Bell inequalities;
- CV QKD protocols should be optimised to reduce the impact of decoherence and/or noise in the channel;
- 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;
- Develop new quantum repeater protocols that are robust with respect to loss & low component efficiencies;
- Lab demonstration of device-indpendent QKD;
- Break with the paradigm that noise is necessarily harmful and innovate tools of state engineering and quantum information protocols based on noise and measurements.

[1] C. Simon, et al., Phys. Rev. Lett., 98, 190503 (2007)
[2] W.J. Munro et al., arXiv:0910.4038v1 (2009)
[3] V. Giovannetti, et al., Phys. Rev. Lett., 100, 230502 (2008)
[4] A. Acín, et al., Phys. Rev. Lett., 98, 230501 (2007)

4.2 Quantum Computation

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 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]. Another related approach is to use electrons confined in a scalable system composed by an array of Penning traps. This scheme was devised by Ciaramicoli et al [3]. Although not yet experimentally implemented, it conceivably satisfies all the DiVincenzo criteria as well.

Currently, experimental ion trap QIP is pursued by about 20 groups worldwide, 12 of which are located in Europe [R. Blatt (Innsbruck, AT), T. Coudreau (Paris,F), M. Drewsen (Aarhus, DK), J. Eschner (Saarbrücken, DE), P. Gill (Teddington, UK), W. Hensinger (Sussex), W. Lange (Sussex, UK), T. Schätz (MPQ, DE), F. Schmidt-Kaler (Mainz, DE), D. Segal (London, UK), A. Steane (Oxford, UK), Ch. Wunderlich (Siegen, DE). Experiments with trapped electrons are currently being set up only in Europe by the groups of G. Werth (Mainz, DE) and F. Schmidt-Kaler (Mainz, DE).

On the theory side there is J.I. Cirac (MPQ Garching, DE), K. Molmer (Aarhus, DK), M. Plenio (Ulm, DE), E. Solano (Bilbao,ES) and P. Zoller (Innsbruck, AT); for trapped electrons P. Tombesi (Camerino, IT).

B. State of the art

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 up to eight 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 entangling gate operations coupling the qubits via joint motional modes of the ion strings (Cirac-Zoller scheme or geometric gates). 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. Long-lived quantum memory (T > 1s) using magnetic field independent qubit levels and decoherence-free subspaces have been demonstrated. Also, an entangling gate for logical qubits has been demonstrated where each logical qubit was composed of two ion-qubits.
4. Individual ion manipulation (pulsed Rabi oscillations), as well as two-qubit gate operations (Cirac-Zoller gate, geometric phase gate, entangling gate) have been demonstrated with entangling fidelities of up to 99%. Multi-particle entangled states using 3-8-ion GHZ-states and 3-8-ion W-state have been also achieved.
5. State-sensitive light scattering (observation of quantum jumps) is routinely used with trapped ions and detection efficiencies of up 99.99% have been reported.
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. Ion-photon entanglement has been used to probabilistically entangle ions in remote ion traps.
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 (3-5 years)

- 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;
- Identify an optimal ion.

E. Long-term goals (10 years and beyond)

- Develop ion chips with integrated optics and electronics;
- Operations with several L-qubits;
- Fault-tolerant operations with multiple qubits;
- Show the feasibility of fault-tolerant quantum processors with trapped electrons.

E. 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
[3] G. Ciaramicoli, I. Marzoli and P. Tombesi “Scalable Quantum Processor with Trapped Electrons”, Phys. Rev. Lett. 91, 017901(2003).

4.2.2 Neutral atoms, molecules and cavity QED

A. Physical approach and perspective

Neutral atoms and molecules provide a promising test bed for the development of scalable general purpose quantum processors, and for quantum simulators as special purpose quantum computers involving a very large number of qubits. As in the case of ions, qubits can be represented by long-lived internal atomic and molecular states in electronic ground states (hyperfine levels, rotational states), or in metastable excited electronic states, which can be manipulated by optical and microwave fields. The unique promises of neutral atom quantum computing rest in particular on the well developed cooling and trapping techniques, as exemplified by laser cooling, realization of Bose Einstein condensates and quantum degenerate Fermi gases, in combination with optical, magnetic and electric traps, realized in free space or in cavities or on atom chips. Such techniques provide an ideal starting point to build and prepare large scale quantum registers with high fidelity. At present these trapping and cooling techniques are being extended to molecules, including, for example, electric on-chip traps for polar molecules. The scenarios of quantum computing with neutral atoms are directly linked to the development of specific trapping techniques. First, traps can be developed allowing the independent manipulation of the centre-of-mass degrees of freedom of individual atoms and molecules, including the addressing of single qubits, which is a necessary requirement for general purpose quantum computing; and massively parallel, identical manipulations of large number of qubits, as realized for example in optical lattices, are relevant in the context of quantum simulators of translation invariant condensed matter systems.

Entanglement of neutral atom or molecule qubits is based on the following physical mechanisms

- Controlled qubit-dependent two-particle interactions, as for example in cold coherent collisions, cavity-assisted collisions, or dipole-dipole interactions between highly excited atomic states (Rydberg states); this kind of approach essentially provide deterministic entanglement and quantum gates;
- Entanglement between distant qubits generated via photon exchange, which plays the role of a quantum data bus; this approach is most often related to the idea of entanglement swapping, and it is usually probabilistic: a measurement must be successful for the entangled state to be generated.

Both scenarios can be played either in free space, or by using cavity QED techniques, where the atomic or molecular qubit is strongly coupled to a high-Q cavity. This can be done in the optical domain by coupling to an electronic excitation, or in the microwave regime for a transition between Rydberg states or rotational states of a polar molecule. Two-qubit gates between distant qubits can be achieved via photon exchange as quantum data bus, in close formal analogy to the phonon data bus of collective oscillation modes in trapped ions. These cavity QED setups also provide a natural interface to quantum communication with photons.

Atoms and molecules can be stored in optical lattices, corresponding to an array of microtraps generated by counterpropagating laser fields. The dynamics of cold atoms loaded into optical lattices can be described by a Hubbard model, with atoms hopping between lattice sites, and interacting via collisions. Thus cold atoms in optical lattices provide a direct way to simulating condensed matter systems with a large number of bosons or fermions. In addition, loading an optical lattice from an atomic Bose Einstein condensate provides via the superfluid-Mott insulator transition the preparation of a Mott phase with exactly one atom per lattice site, and thus the preparation of a very large number of atomic qubits. These atoms can be entangled in parallel operations with qubit-dependent controllable 2-particle interactions, provided, for example, by coherent collisional interactions in combination with movable qubit (spin) dependent optical lattices. This provides the basis for a digital quantum simulator, for example of a spin lattice system, where the time evolution generated by the Hamiltonian is decomposed into a series of single and two-qubit gates performed in parallel on all qubits (spins).

A major recent development is the possibility to image and (at least partially) address individual atoms in optical lattices. When coupled to atom-atom interactions using either cold collisions or Rydberg dipole-dipole interactions, this opens the way to performing nearly individual measurements on large arrays of entangled atoms, which would be a crucial steps towards quantum simulators and even quantum computers.

For single atoms strongly coupled to an optical cavity, single photons for the purpose of exchanging quantum information between remote locations can be generated on demand and with high quantum efficiency. Protocols for generating a stream of photons with entanglement mediated and controlled by a single intracavity atom have been proposed. In addition to these deterministic mechanisms for entanglement, probabilistic protocols can be developed which are based on free space atoms emitting photons where entanglement is achieved by appropriate photon detection.

Currently, quantum computing with neutral atoms is investigated experimentally in several dozen laboratories worldwide, with half of them located in Europe. The European groups working with a controllable number of atoms include I. Bloch (Munich, DE), T. Esslinger (Zurich, CH), P. Grangier (Palaiseau, FR), S. Haroche (Paris, FR), D. Meschede (Bonn, DE), G. Rempe (Garching, DE), and H. Weinfurter (Munich, DE). Related experiments, sometimes done in an AMO context broader than QIP only, are also performed by W. Ertmer (Hannover, DE), E. Hinds (London, UK), J. Reichel (Paris, FR), and J. Schmiedmayer (Vienna, AT). The experimental program is strongly supported by implementation-oriented theory groups like H. Briegel (Innsbruck, AT), K. Burnett (Oxford, UK), J. I. Cirac (Garching, DE), A. Ekert (Cambridge, UK), P. L. Knight (London, UK), M. Lewenstein (Barcelona, ES), K. Mølmer (Aarhus, DK), M. B. Plenio (London, UK), W. Schleich (Ulm, DE), P. Tombesi (Camerino, IT), R. Werner (Braunschweig, DE), M. Wilkens (Potsdam, DE), & P. Zoller (Innsbruck, AT). 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, largely thanks to the support provided by the European Union.

B. State of the art

I. Quantum memories: 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 for trapping and manipulating neutral atoms have been developed:

Optical tweezers and arrays of optical traps allow for 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, or by loading a Bose-Einstein condensate into an optical lattice. Given recent developments, both approaches have the potential for individual atom manipulations, and for massive parallelism, with many pairs of atoms colliding at once. The landmark results attained are:

- 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; coherent write and read operations on individual qubits were performed.
- A small number of atoms were loaded into a two-dimensional array of movable dipole traps made with a microlens array.
- 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.
- Various imaging techniques (using large aperture lenses, or even electron beams) were developed to see individual sites and even individual atoms in planar (two-dimensional) optical lattices.

Atom chips: The ability to magnetically trap and cool atoms close to a surface of a micro-fabricated substrate (for example using micro-magnetic potential wells produced by micron-sized current carrying wires or microscopic permanent magnets) has led to an explosive development of atom chips in the past few years. Such devices are very promising building blocks for quantum logic gates due to their small size, intrinsic robustness, strong confinement, and potential scalability. The main accomplishments they have attained include:

- Cooling of atoms to quantum degeneracy (Bose-Einstein condensation);
- Transport of an ensemble of atoms using a magnetic conveyor belt;
- Very long coherence times by using appropriate qubit states;
- Multilayer atom chips with sub-μm resolution and smooth magnetic potentials;
- On-chip single-qubit rotation via two-photon transitions on hyperfine qubits. Single-atom detection using various techniques, including Fabry-Perot cavities;
- Advanced atom interferometry techniques using BEC on chips.

Traps for polar molecules at the individual level have recently been proposed, based on microwave or electric fields, and are the subject of growing experimental investigation. On the experimental side,

- Cold polar molecules at millikelvin temperatures have been produced by several different techniques, including deceleration of supersonic molecules, filtering of slow molecules from a thermal ensemble, Helium buffer gas cooling in a cryogenic environment, and more recently by direct photoassociation;
- Ensembles of cold polar molecules have been stored in magnetic or electric bottles.

Techniques using atomic ensembles either in vapour cells, optical traps, or cryo-cooled rare-earth doped crystals. These methods are extensively discussed under the "Quantum communications" heading, and we refer the reader to sections 4.1.3, 4.1.4, 4.1.5 for details. We note that studies related to quantum repeaters, involving both quantum memories and some data processing, are currently establishing a strong bridge between quantum communications and quantum computing, under the general goal of achieving efficient quantum information processing.

II. Entangling gates: a variety of schemes have been proposed theoretically, based on interatomic interactions which may be either direct (for instance collisional, possibly enhanced by Feshbach resonances, or between dipoles of Rydberg excited atoms) or mediated by a quantum data bus, i.e. a different degree of freedom (for instance photons, freely propagating or within a high-finesse cavity mode).

Optical tweezers and arrays of optical traps are ideal to perform collisional gates, which require the preparation of a well-defined quantum state of atomic motion. With optical lattices, highly parallelized quantum gates were 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. With single atoms in optical tweezers, a series of experiments in 2009-2010 were able to obtain fast atom-atom entanglement and quantum gates using the Rydberg blockade mechanism, as initially proposed in 2000. This scheme is very promising for neutral atoms, because it is very fast (sub-microsecond), does not require to move the atoms, and is relatively insensitive to the thermal motion of the trapped atoms.

Cavity QED, possibly in combination with optical dipole traps, is a very promising technique for realizing an interface between different carriers of quantum information, implemented either 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 can be realized both with Rydberg atoms in microwave cavities as well as 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. The main achievements in this sector include:

- Probabilistic approach in free space:
    - A single trapped atom has been entangled with a single photon;
    - Two-photon interference effects of the Hong-Ou-Mandel type between single photons emitted by separate atoms have been observed.
- 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, including quantum gates;
    - New tools for monitoring the decoherence of mesoscopic quantum superpositions have been developed.
- Deterministic approach with optical cavities:
    - The strong atom-photon coupling has been employed to realize a quasi-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;
    - Single atoms were optically trapped inside a cavity for such a long time that experiments can be performed with just one single atom, and cooling techniques avoiding spontaneous emission were successfully implemented;
    - Single individually addressable atoms were deterministically transported in and out of a cavity by means of an optical conveyor belt.

C. Present challenges

The technology needed to perform single-atom experiments is relatively new (less than 10 years), but it has done very significant progress recently. In particular, neutral-atom systems have now demonstrated two-qubit operations using Rydberg blockade.

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

- In optical tweezers and small-scale dipole trap arrays, following the successful implementation of two-qubit entangling quantum gates, the main challenge is to increase the size of the quantum register to more than 2 atoms;
- In optical lattices, addressability of individual qubit of the closely spaced register has been achieved, opening many exciting perspectives, e.g. towards quantum simulators, which are now developing very quickly;
- In both scenarios, the Rydberg blockade approach seems very promising due to its high speed and robustness with respect to atomic motion. However, a lot remain to be done to improve the gates fidelity.

Atom chips: experiments with atom chips are still facing a large number of challenges for implementing QIPC, but a lot of progress has been made.

- Coherent manipulations of Bose-Einstein condensates with state-dependent microwave potentials on an atom chip have been achieved, and a collisional quantum phase gate on an atom chip seems within reach;
- The full demonstration of the potential provided by atom chips requires the realization of large-scale integration, e.g., with several 10 qubits;
- Potential roughness very close (μm) to micro-fabricated structures is of concern for qubit storage and transport. For current-carrying structures the problem can be solved by the design and fabrication methods as developed recently, but micro-structures with fewer defects might be needed for permanent magnets;
- 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.

Polar molecules: Research with polar molecules has just started and, hence, is still facing a large number of experimental challenges. Some of these are:

- As laser cooling methods developed for atoms fail for molecules, new cooling techniques need to be developed to reach the ultracold regime;
- The number of molecules and their density needs to be increased before collisions can be observed in electric trapping experiments;
- Efficient molecule detection techniques must be developed in particular for experiments involving only single or a few molecules.

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.

- 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.
- 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 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.
- 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 the microwave domain, 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.

A major challenge for theory is to characterize and optimize the suitability of each of the available and proposed experimental systems as platforms for general-purpose quantum computing or rather for quantum simulation.

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)

Useful reviews on the physics in either many-body systems and Rydberg atoms, and their applications to QIP, can be found in, e.g.:

[3] Immanuel Bloch, Jean Dalibard, Wilhelm Zwerger, “Many-Body Physics with Ultracold Gases”, Rev. Mod. Phys. 80, 885 (2008)
[4] M. Saffman, T. G. Walker, and K. Mølmer, “Quantum information with Rydberg atoms”, Rev. Mod. Phys. 82, 2313 (2010).

4.2.3 Superconducting circuits

A. Physical approach and perspective

Quantum computation with superconducting Josephson junction (JJ) based circuits exploits the intrinsic coherence of the superconducting state, into which all electrons are condensed. The systems form effective two(multi)-level artifical atoms where quantum information is stored in different degrees of freedom: charge, flux or phase. The "old" distinction in terms of charge, flux, and phase qubits is however a bit outdated: all JJ-qubits are now closer to the phase regime than to the charge regime in order to defeat charge noise and achieve long coherence times. Systems are fabricated with thin film technology and operated at temperatures below 100 mK. Measurements are

performed with integrated on-chip detectors. Coupling between qubits can be made strong, especially using microwave resonators and cavities - circuit/cavity quantum electrodynamics (cQED). This also provides opportunities for coupling widely different types of qubits in hybrid devices, inluding atoms, ions and impurity spins in quantum dots, crystals, and microtraps. The state of the art is described in [1-5], including comprehensive technical accounts in [4,5].

About 30 groups work on superconducting quantum bits in Europe, Japan, China and the USA. European experimental groups: Saclay, France (D. Esteve, D. Vion, P. Bertet); Delft, The Netherlands (J. Mooij, C.P.J.M. Harmans); Chalmers, Sweden (P. Delsing, C. Wilson); ETH Zürich, Switzerland (A. Wallraff); PTB, Germany (A. Zorin); Jena, Germany (E. Ilichev); KIT Karlsruhe, Germany (A. Ustinov); Grenoble, France (O. Buisson); HUT, Helsinki, Finland (S. Paraoanu); TUM Munich (R. Gross); and others. European theory groups: KIT Karlsruhe , Germany (G. Schön, A. Shnirman); SNS Pisa, Italy (R. Fazio); LMU Munich (F. Marquardt); Chalmers, Sweden (V. Shumeiko, G. Johansson, G. Wendin); Catania, Italy (G. Falci, E. Paladino); Basel, Switzerland (C. Bruder); Grenoble, France (F. Hekking); Toulouse, France (D. Shepelyansky); Bilbao, Spain (E. Solano, J. Siewert); and others.

B. State of the art

Referring to the seven DiVincenzo criteria [6], the state of the art for QIP with JJ-qubits can be described as follows:

1. Qubits: systems with 2-4 qubits (charge, flux and phase) have been fabricated and investigated. Recent hybrid JJ-qubits (transmon [7,8], fluxonium [9]) are showing great promise due to lower sensitivity to noise.
2. Initialization: this proceeds via relaxation into the ground state on a timescale of microseconds.
3. Universal gate operations: high fidelity single qubit operations are performed with microwave and DC pulses. Two qubit gate operations and entangling gates with moderate-to-good fidelity have been achived for all major types of qubits (transmon [8], flux [10], phase [11]). Violation of a Bell inequality has been demonstrated with phase qubits [12].
4. Readout: a variety of qubit readout schemes is available, including single-shot switching [10-12] and dispersive [13,14] readout. QND measurement has been demonstrated with dispersive readout methods [13,14]. Low cross-correlation, simultaneous individual readout of two coupled qubits has been achieved for phase [12] and flux [13] qubits.
5. Long coherence times: coherence times of 1-10 microseconds have been observed in transmon and flux qubits, and of about 200 ns in phase qubits [5]. The shortest time needed for basic 1- and 2-qubit quantum operation is a few nanoseconds.
6. Quantum interfaces for qubit interconversion: there are currently several demonstrations of coherent transfer between JJ-qubits and microwave resonators (both lumped circuits and microwave cavities) (see [1-14]), including systematic population of a harmonic oscillator with 0-10 photons in pure Fock states and in arbitrary superpositions [15]. Of great interest for microwave engineering is the development of rapidly tunable microwave resonators [16].
7. Quantum interfaces to flying qubits for optical communication: research is at an embryonic stage, and there are so far no experimental investigations.

C. Strengths and weaknesses

Strengths:

- High potential for scalable integrated technology;
- Strong coupling between qubits using microwave resonators and cavities;
- Flexible opportunities with different types of superconducting qubits;
- Mature background technology, 20 years of experience;
- Long history of pushing the limits of measurement towards quantum limits;
- Great potential for providing a platform for large scale integration of solid-state qubits and QIP devices;
- Driver of applications in solid-state quantum engineering;

- Low-temperature or superconducting technologies necessary for integration with solid state microtraps for hybrid systems with atom and ions, or cold atoms and molecules;
- Great potential for meeting the challenge of developing microwave-optical interfaces;

Weaknesses:

- Qubits manufactured, not natural, and therefore sensitive to imperfections;
- Coherence times presently limited by defects in tunnel barriers and substrates to the 1-10 microsecond range;
- Coherence times seem to be limited by relaxation. Ulltimate limits of achievable relaxation times not known;

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

- Realize high-fidelity universal two-qubit gates in the most promising types of qubits;
- Realize non-destructive, high-fidelity 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 with large on/off ratio between qubits;
- Realize systems of multiple qubits of different types coupled through common harmonic oscillator buses - solid-state cavity QED;
- Demonstrate teleportation and qubit coding for quantum error correction;
- Make first experimental tests of quantum algorithms with 3-5 qubits.

E. Long-term goals (10 years and beyond)

- Develop multi-qubit circuits connecting several 5-6 qubit clusters (multi-core circuits);
- Improve fidelity to the level needed for large-scale application;
- Develop interfaces to microwave and optical transmission lines;
- Develop quantum interfaces between qubits with typical microwave frequencies and atoms with optical transitions;
- Develop interfaces for hybrid solutions to long term storage and communication;
- Demonstrate elementary quantum error correction, quantum feed-forward (pulse optimization) and quantum feedback.
- Simulation of simple quantum systems.

F. Key references

[1] Proceedings of Nobel Symposium 141: Qubits for Future Quantum Computers (ed. G. Johansson), Phys. Scr. T137 (2010)
[2] J. Clarke and F.K. Wilhelm: “Superconducting Qubits”, Nature Insight 453, 1031 (2008)
[3] R. J. Schoelkopf and S. M. Girvin, "Wiring up quantum systems", Nature 451, 664 (2008)
[4] G. Wendin and V.S. Shumeiko, "Quantum bits with Josephson junctions", Low Temp. Phys. 33, 724 (2007)
[5] J.M. Martinis, "Superconducting Phase Qubits", Quantum Information Processing 8, 81 (2009)
[6] http://qt.tn.tudelft.nl/~lieven/qip2007/QIP3_divincenzo_criteria.pdf [7] J.M. Fink, R. Bianchetti, M. Baur, M. Goeppl, L. Steffen, S. Filipp, P.J. Leek, A. Blais, and A. Wallraff: “Collective Qubit States and the Tavis-Cummings Model in Circuit QED”, Phys. Rev. Lett. 103, 083601 (2009)
[8] L. DiCarlo, J. M. Chow, J. M. Gambetta, L.S. Bishop, D. I. Schuster, J. Majer, A. Blais, L. Frunzio, S. M. Girvin, and R. J. Schoelkopf: “Demonstration of Two-Qubit Algorithms with a Superconducting Quantum Processor”, Nature 460, 240 (2009)
[9] V.E. Manucharyan et al., "Fluxonium: single Cooper pair circuit free of charge offsets", Science 326, 113-116 (2009)

[10] J.H. Plantenberg, P.C. de Groot, C.J.P.M. Harmans and J. E. Mooij, "Demonstration of controlled-NOT quantum gates on a pair of superconducting quantum bits", Nature 447, 14 (2007)
[11] R.C. Bialczak, M. Ansmann, M. Hofheinz, E. Lucero, M. Neeley, A. O'Connell, D. Sank, H. Wang, J. Wenner, M. Steffen, A. Cleland, J. Martinis, "Quantum Process Tomography of a Universal Entangling Gate Implemented with Josephson Phase Qubits", arXiv:0910.1118 [quant-ph]
[12] M. Ansmann, H. Wang, R.C. Bialczak, M.. Hofheinz, E. Lucero, M. Neeley, A. D. O'Connell, D. Sank, M. Weides, J. Wenner, A. N. Cleland and J..M. Martinis, "Violation of Bell's inequality in Josephson phase qubits", Nature 461, 504-506 (2009)
[13] P.C. de Groot, A.F. van Loo, J. Lisenfeld,2, R.N. Schouten, A. Lupascu, C.J.P.M Harmans, and J.E. Mooij, "Low-crosstalk bifurcation detectors for coupled flux qubits", submitted to Applied Physics Letters (2009)
[14] F. Mallet, F.R. Ong, A. Palacios-Laloy, F. Nguyen, P. Bertet, D. Viuon, and D. Esteve, "Single-shot qubit readout in circuit quantum electrodynamics" Nature Physics 5, 791 (2009)
[15] M. Hofheinz, H. Wang, M. Ansmann, R.C. Bialczak, E. Lucero, M. Neeley, A. D. O'Connell, D. Sank, J. Wenner, J.M. Martinis and A.N. Cleland, "Synthesizing arbitrary quantum states in a superconducting resonator", Nature 459, 546-549 (2009)
[16] M. Sandberg, C.M. Wilson, F. Persson, T. Bauch, G. Johansson, V. Shumeiko, T. Duty, and P. Delsing, "Tuning the field in a microwave resonator faster than the photon lifetime", Appl. Phys. Lett. 92, 203501 (2008)

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. Each quantum dot contains one electron, the spin of which serves as the qubit (earlier quantum dot work on electron charge qubits and on excitonic qubits has been phased out, because of the short coherence times). 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 ~20 groups worldwide, 11 of which are located in Europe [L. Kouwenhoven (Delft, NL), L. Vandersypen (Delft, NL), K. Ensslin (ETH-Zurich, CH), J. Finley (TU-Munich, DE), M. Bayer (Dortmund, DE), M. Atature (Cambridge, UK), D. Zumbuhl (Basel, CH) R. Warburton (Basel, CH) and A. Imamoglu (ETH-Zurich, CH)], as well as G. Burkard (Konstanz, DE), D. Loss (Basel, CH) and Y. Nazarov (Delft, NL) on the theory side.

B. State of the art

Two main technologies are used to form quantum dots, self-assembly and nanofabrication. Self-assembled quantum dots are controlled and detected mostly by optical means; lithographically defined quantum dots are controlled and detected electrically. Despite these differences, much of the underlying physics is the same in these two systems. The state-of-the art is as follows:

Lithographically defined quantum dots

- Quantum dot circuits with up to three quantum dots have been controllably loaded with electrons;
- Single-shot read-out of a single spin state was demonstrated;
- Single-spin coherent rotations have been demonstrated both using magnetic and using electrical driving;

- Coherent exchange of two spins in a double quantum has been demonstrated;
- Relaxation times (T1) from milliseconds to one second have been observed, and the relaxation mechanism has been established;
- Spin coherence times of ~1 microsecond have been measured, and the main decoherence mechanism has been established;
- Partial control of the nuclear spin environment (the main source of decoherence) has been achieved.

Self-assembled quantum dots

- High fidelity initialization of an electron spin was achieved using optical pumping;
- Single spin measurement using Faraday roation has been demonstrated;
- Long electron spin lifetime has been measured;
- Quantum nature of light generated by a strongly coupled quantum dot cavity system has been demonstrated;
- Optical pumping of a single hole and coherent population trapping have been demonstrated;
- Coherent rotation of a single spin has been achieved;
- Photon blockade in a quantum dot cavity system has been demonstrated;
- Optically controlled exchange interaction between two quantum dots has been realized;
- Partial control of nuclear spin environment has been achieved.

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

- Integrate electrically controlled single-qubit gates, two-qubit gates and single-shot read-out into a single device;
- Demonstrate optically controlled single- and two-qubit gates;
- Realize coupling between spins on a chip, via striplines or on-chip cavities;
- Interconvert between single electron spins and single-photon polarization (standing qubit to flying qubit conversion);
- Make control of the otherwise random nuclear Overhauser field routine, in order to extend the dephasing times;
- Extend system size from two qubits to three;
- Implement simple quantum algorithms, error correction protocols, etc.;
- Explore and compare alternative semiconductor materials for quantum dots.

D. Long-term goals (10 years and beyond)

- Develop multi-qubit circuits in a scalable architecture;
- Improve fidelity to the level needed for fault tolerance;
- Demonstrate a quantum repeater (photon to spin to photon conversion).

E. Key references

[1] D. Loss and D. DiVincenzo, ‘‘Quantum computation with quantum dots’’, Phys. Rev. A 57, 120–126 (1998)
[2] R. Hanson, L.P Kouwenhoven, J.R. Petta, S. Tarucha, and L.M.K. Vandersypen, "Spins in few-electron quantum dots", Reviews of Modern Physics 79, 1217 (2007)
[3] R. Hanson and D.D. Awschalom, "Coherent manipulation of single spins in semiconductors ", Nature 453, 1043 (2008)

4.2.5 Linear Optics

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. KLM's seminal work is 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 possible implementation. It consists of a highly entangled multi-particle state called a cluster state, combined with single-qubit measurements and feedforward. These constituents are sufficient to implement scalable, universal quantum computation. Different algorithms only require different “patterns” of single-qubit operations on a sufficiently large cluster state. Since only single-particle projections, together with the ability to construct the initial highly entangled cluster state, 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.

Currently, the linear optics approach to quantum computation is pursued by the following European groups: K. Banaszek (Torun, PL) , M. Bourennane (Stockholm, SE), F. DeMartini (Rome, IT), N. Gisin (Geneva, CH), P. Grangier (Orsay, FR), A. Karlsson (Stockholm, SE), P. Mataloni (Rome, IT), J. OBrien(Bristol,UK), J. Pan (Heidelberg,DE), J. Rarity (Bristol, UK), A. Shields (Cambridge, UK), I. Walmsley (Oxford, UK), H. Weinfurter (Munich, DE), and A. Zeilinger (Vienna, AT).

B. State of the art

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:

- The generation of entangled states of up to 6 photons [3] and 10 qubits [4] by utilizing more degrees of freedom per qubit;
- Cavity-enhanced source of multi-photon states (see, e.g., [5]);
- The heralded generation of entangled states [6];
- The fast feed-forward technology [7];
- The use of generalized measurements to optimally use finite computational resources [8];
- The demonstration of quantum gates on states that are available “for free” in physical systems via ground-state cooling [9].

Several practical designs implementing the KLM scheme have been developed. Experimental methods for the preparation of photonic quantum states that serve as ancillas in the measurement-based schemes now achieve typical fidelities above 99%. Using post-selected events based on coincidence detection has allowed for a range of demonstrations of non-deterministic two-qubit gates: a fully characterized two-photon gate operating with >90% fidelity, four-photon CNOT gates both with entangled ancilla and with teleportation, a KLM non-linear 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 correction and Bell measurement for teleportation.

Proposals for the optical implementation of cluster-state quantum computing have been put forward and are promising significant reductions in physical resources by two orders of magnitude as compared to the original KLM scheme. Moreover, a variety of modifications have been suggested to reduce the resource requirements in KLM architectures. The realization of photonic four-qubit cluster states allowed to demonstrate the feasibility of one-way quantum computing through a universal set of one- and two-qubit operations, as well as the implementation of Grover's search algorithm [10]. An essential element of one-way quantum computing is to feed-forward the results of measurements to sequentially occurring measurements in order to correct naturally occurring errors during the computation. This has been achieved in a recent experiment using linear optics [7]. Nevertheless, linear optics, as well as other state-of-the-art techniques of implementing one-way quantum computing algorithms, are still limited to a finite amount of resources available for computational algorithms. As long as this limitation exists, it is paramount to optimize the use of existing resources. For example, it has been shown that the use of generalized measurements can reduce the necessary resources for a given algorithm significantly [8].

Integration of linear optics technology is an important step towards the practical implementation of large-scale computational networks. Recent achievements in this direction were to manipulate single-photon states and multi-photon entanglement directly on-chip [11]. A compiled version of Shor's algorithm has been implemented on an integrated wave-guide chip[12], and quantum walks of correlated particles offer the possibility of studying large-scale quantum interference and quantum simulation [13].

Enabling technologies for OQC are:

- High-efficiency photon detectors based on superconducting materials. In particular, this is a prerequisite for high-fidelity multi-qubit measurements (for the KLM scheme) and the reliable preparation of multi-qubit states (for both the KLM and the cluster state scheme);
- Certifying the fidelity of quantum processes and states. The complexity of tomographically reconstructing a quantum state increases exponentially with the size of the system. Novel methods aim at reducing the number of measurements necessary for the characterization of resource states for quantum information processing;
- Development of single-photon and/or entangled-photon sources is required for OQC. Currently, photon sources combining high-rate and high-quality generation of timed single photons or entanglement are under intense research. In the meantime, bright, albeit non-deterministic sources of correlated photons or entangled-photon pairs are critical to allow for the development and evaluation of circuit technology. Ultra-bright and compact sources have been developed, in particular, using periodically-poled nonlinear waveguides.

C. Strengths and weaknesses

One of the main advantages of photonic implementations of quantum computing are low decoherence (due to the photon's weak coupling to the environment), fast processing, compatibility to fiber optics and integrated optics technologies. Another advantage of OQC is that the active feed forward necessary in the one-way model can be implemented via fast optical switches. With present technologies this can be done in less than 100 nanoseconds (in the future probably down to 10 nanoseconds) [7]. Optical quantum systems are also very promising for realizing either digital quantum simulators [10], which are based on discrete gate operations, or analog quantum simulators, where an initial quantum state is prepared and then continuously evolved to the quantum state of interest. It is the particular advantage of photons that single-qubit operations can be achieved with almost unity fidelity and that tuneable inter-qubit interactions can be achieved among arbitrary qubits. Current drawbacks of the OQC approach are low photon-creation rates, low photon-detection efficiencies, and the difficulties with the intermediate storage of photons in a quantum memory (see also Section 4.1.3). The low efficiencies quoted above are presently an important practical limitation to the scalability of optical circuits, in the sense that they exponentially damp the success probability of most quantum operations.

D. Challenges

The main challenges for fault-tolerant OQC can be summarized as follows:

- Error models for KLM-style OQC have found that error thresholds for gates in order to achieve fault tolerance are above 1.78%. While this has been achieved for small cluster states [8], it remains a challenge for more complex systems;
- To further reduce the resources required for OQC 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 find more efficient ways to characterize the quality of states generated for use in various quantum information-processing protocols;
- The integration of the generation, manipulation and detection of photons on integrated circuits is a prerequisite for the implementation of scalable OQC architectures. Recent work has shown tremendous progress towards that goal (see, e.g., [13]).

E. Key references

[1] E. Knill, R. Laflamme, G. J. Milburn, “A scheme for efficient quantum computation with linear optics’’, Nature 409, 46 (2001).
[2] R. Raussendorf ,H. J. Briegel, “A one-way quantum computer’’, Phys. Rev. Lett. 86, 5188 (2001).
[3] C. Lu et al., “Experimental entanglement of six photons in graph states”, Nature Physics 3, 91 (2007).
[4] Gao et al. , “Experimental demonstration of a hyper-entangled ten-qubit Schrödinger cat state”, Nature Phys. 6, 331 (2010).
[5] R. Krischek et al.,"Ultraviolet enhancement cavity for ultrafast nonlinear optics and high-rate multiphoton entanglement experiments", Nature Photonics 4, 170 (2010)
[6] C. Wagenknecht et al., “Experimental demonstration of a heralded entanglement source”, Nature Photonics 4, 549 (2010); Barz et al., “Heralded generation of entangled photon pairs”, Nature Photonics 4, 553 (2010).
[7] R. Prevedel et al., "High speed linear optics quantum computing using active feed-forward", Nature 445, 65 (2007).
[8] D. N. Biggerstaff et al., "Cluster-State Quantum Computing Enhanced by High-Fidelity Generalized Measurements.", Phys. Rev. Lett. 103, 240504 (2009) .
[9] R. Kaltenbaek, J. Lavoie, B. Zeng, S. D. Bartlett, K. J. Resch, “Optical one-way quantum computing with a simulated valence-bond solid”, Nature Physics 2010 (in Press).
[10] P. Walther et al., “Experimental one-way quantum computing”, Nature 434, 169 (2005).
[11] J. C. F. Matthews, A. Politi, A. Stefanov, J. L. O'Brien, “Manipulation of multiphoton entanglement in waveguide quantum circuits”, Nature Photon 3, 346 (2009).
[12] A. Politi et al., Shor’s Quantum Factoring Algorithm on a Photonic Chip, Science 325, 1221 (2009). [13] A. Peruzzo et. al. “Quantum Walks of Correlated Photons”, Science 329, 1500 (2010).

4.2.6 Impurity spins in solids and single molecular clusters

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, nitrogen or phosphorus atoms in 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] on the other hand certain spin systems are shielded well enough from their environments such that room temperature operation seem feasible. 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.

Another solid basis for quantum information processing, which relies on new molecules engineered with features suitable for qubit encoding and entanglement, is provided by Single Molecular Magnets (SMMs). Current research activity focuses on the control of the coherent spin dynamics in molecular spin clusters, which implies the control of decoherence mechanisms both at synthetic level and in terms of modelling. While most of the experiments are currently performed on bulk crystals, the final goal of manipulating single molecular spins is drawing increasing attention towards the grafting of molecules at surfaces and the development of techniques for readout.

Research groups engaged in QIP research regarding impurity spins in solids in Europe include A. Briggs (Oxford, UK), P. Grangier (Orsay, FR), O. Guillot-Noël and P. Goldner (Paris, FR), W. Harneit (Berlin, DE), S. Kröll (Lund, SE), J.L. LeGouët (Orsay, FR), M. Mehring (Stuttgart, DE), K. Mølmer (Aarhus, DK), J.F. Roch (Cachan, FR), M. Stoneham (London, UK), D. Suter (Dortmund, DE), J. R. Hanson (Delft, NL), J. Wrachtrup (Stuttgart, DE). Research groups working on QIP with molecular spin clusters in Europe include D. Loss (Basel, CH), B. Barbara and W. Wernsdorfer (Grenoble, FR), M. Affronte and F. Troiani (Modena, IT), D. Gatteschi (Florence , IT), R. E. P. Winpenny and G. Timco (Manchester, UK).

B. State of the art

Impurity spins: 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:

- Magnetic resonance on single defects detected by charge transport and single spin state measurements by optical techniques.
- Multipartite entanglement on single defect spins as well as mutual coherent coupling between distant defect spins in diamond.
- Accurate preparation and readout of ensemble qubit states. Arbitrary single-qubit operations characterised by quantum state tomography with a fidelity >90% in rare earth crystals.
- The preparation of Bell states with electron and nuclear spin ensembles as well as a three qubit Deutsch-Jozsa algorithm has been achieved.
- A scalable architecture has been developed for N@C60 on Si and decoherence times have been measured to be up to 1 s.

Single molecular magnets: Quantum dynamics of spins in molecular clusters has been deeply studied by a number of fundamental works in the last decade. Decoherence and dephasing mechanisms have been investigated in assemblies: the intrinsic coherence times are expected to be longer than microseconds (preliminary experiments provide a lower bound of few tens of ns); similarly, the switching rates for one-qubit and two-qubit gates are estimated to be on the order of hundreds of picoseconds.

Recent important achievements are:

- Proposals for the implementation of the Grover's algorithm in high spin SMMs [4], and of universal solid state quantum devices in antiferromagnetic spin clusters;
- Synthesis of specific molecules providing promising test-beds for scalable schemes [5];
- Entanglement of states belonging to different molecules inspired both synthesis of new molecular dimers and elaboration of specific quantum algorithms that exploit some features of molecular clusters.

C. Strengths and weaknesses

Impurity spins: 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.

Single molecular magnets: The bottom-up approach used by supra-molecular chemistry offers simple and relatively cheap processes for the fabrication of quantum nanosized molecules exhibiting multi-functionality like the switchability of magnetic states with light, resonance at RF-MW radiation, etc. Moreover, the control on and the sharp definition of eigenstates and eigenvalues in magnetic molecules provides an extraordinary stimulus for the development of new quantum algorithms and schemes. In the latter case, the main issue would be to prove that single, isolated molecules behave not much differently from what is observed in experiments performed on assemblies of molecules.

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

Impurity spins: 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 and two qubit operations. Major efforts are concentrated in the US and Australia.
- Defects in diamond heads towards generation of coupled defect center arrays and incorporation into photonic structures. For this advanced nanoimplantation techniques as well as production of photonic cavities needs to be refined.
- For rare earth crystals short term goals include faster gate operations using pulses developed by optimal control theory, demonstration of two-qubit gates and the development of single ion readout capabilities for scaling up to several qubits.
- 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.

Single molecular magnets: The main goals can be summarized as follows:

- To engineer new molecular clusters for the optimization of the coherent dynamics of spins, and design, synthesize and characterize controlled molecular linkers between spin clusters;
- To set up experiments for the direct observation of coherent dynamics (for instance Rabi oscillations, spin echo experiments), and probe, understand and reduce the intrinsic decoherence mechanisms in specific cluster qubits;

- To develop computational schemes exploiting the features of molecular cluster qubits, and study different functionalities (f.i. switchability) of molecules useful for specific tasks in complex architectures of QIP.

E. Long-term goals (10 years and beyond)

For **impurity spins** the main long-term challenges are

- Coupling of defects in wide band gap semiconductors to an optical cavity mode. Implantation of defects with nm accuracy in registry with control electrodes. Optical addressing of single defects within dense defect arrays;
- For rare earth ions, efforts should be joined with crystal growth research (inorganic chemistry) to create appropriate materials for larger scale systems. Techniques should also be developed for entangling remote systems to achieve full scalability;
- 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.

For **single molecular magnets**, the long-term challenges can be summarized as follows:

- Definition of reliable procedures for preparing, characterising and positioning (arrays of) molecular spin cluster qubits;
- Development of models and experimental methods for efficient read-out.

F. Key references

[1] B. Kane, “A silicon-based nuclear spin quantum computer”, Nature 393, 133 (1998)
[2] R. Hanson, D. Awschalom. "Coherent manipulation of single spins in semiconductors" Nature 453, 1043 (2008), P. Neumann et al. "Multipartite entanglement of single spins in diamond", Science 320, 1326 (2008)
[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] M.N. Leuenberger, D. Loss, “Quantum Computing in Molecular Magnets’’, Nature 410, 789 (2001)
[5] F. Troiani A. Ghirri, M. Affronte, P. Santini, S. Carretta, G. Amoretti, S. Piligkos, G. A. Timco, R. E. P. Winpenny, “Molecular engineering of antiferromagnetic rings for quantum Computation”, Phys. Rev. Lett. 94, 207208 (2005)

4.3 Quantum Information Sciences - Theory

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,

- Novel quantum algorithms;
- Quantum communication protocols;
- Novel quantum cryptographic protocols;
- Basic concepts such as entanglement and decoherence;
- Characterization and quantification of (two- & multi-party) entanglement;
- Capacities of noisy quantum communication channels;
- Optimization of protocols for quantum cryptography;
- New quantum computer models and architectures;
- New tools for the study of quantum systems with many degrees of freedom such as strongly correlated lattice systems;
- Novel ideas to explore complex quantum systems;
- Quantum simulation methods to simulate quantum systems.

An important class of theoretical work is concerned with implementations of these abstract concepts in real physical systems, such as trapped ions, ultra-cold ions in optical lattices, or systems from cavity-QED.

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. What is more, the transfer of concepts from quantum information theory to other fields of physics such as condensed matter physics or quantum field theory has proved very 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 attained 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.

4.3.1 Theory of quantum computing

Quantum algorithms and 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. Although Grover's only yields a quadratic speed-up over classical algorithms it can be widely used in computer science tasks, like sorting, matrix multiplication bipartite matching to name a few. For all these problems quantum computers give an important advantage over classical computers. Grover's algorithms can be cast in terms of quantum random walks which has lead recently to new quantum algorithms for searching game trees. These algorithms will be widely applicable in the area of algorithmic game theory, scientific computing etc.

Very recently a new quantum algorithm has been developed for approximating solutions to linear equations. This algorithm demonstrates an exponential advantage over any classical algorithm. In order to understand to what extent quantum computers outperform classical computers we need to determine where efficient quantum computation, BQP, fits within the classification of complexity classes, like P, NP, and PSPACE. General methods for proving impossibility results, that is limitations of quantum computers, have been developed and applied with great success. Notable are the polynomial method and the quantum adversary method.

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] A. Ambainis, D. Aharonov, J. Kempe and U. Vazirani, "Quantum walks on graphs", 33rd ACM Symp. on Theory of Computing (2001)
[5] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf, "Quantum lower bounds by polynomials",Journal of the ACM 48(4) (2001)
[6] A. Ambainis, "Quantum lower bounds by quantum arguments", Journal of Computer and System Sciences 64, 750 (2002)
[7] E. Farhi, J. Goldstone and S. Gutmann. "A Quantum Algorithm for the Hamiltonian NAND Tree" [quant-ph/0702144]
[8] A. W. Harrow, A. Hassidim, and S. Lloyd, "Quantum algorithm for solving linear systems of equations", Phys. Rev. Lett. 15, 150502 (2009)

Quantum communication protocols

Following the success of quantum algorithms quantum communication complexity was developed by initial work of Yao (qubit model) and Cleve and Buhrman (entanglement assisted model). The setting is that of multiple quantum computers trying to solve computational tasks, minimizing the amount of communication. There has also been considerable development of new protocols for quantum communication over the last decade. Useful protocols that found applications outside that of communication complexity are Quantum Fingerprinting and the Hidden Matching problem. These protocols demonstrate an exponential improvement in the communication over classical protocols. Applications are in many areas, like interactive games and approximation algorithms, lower bound for classical and quantum computers, as well as the development of new non-locality tests. Main open questions in this area are to understand the power that entanglement assisted model offers. This is poorly understood, but recently some progress has been made by connecting this question for restricted games, called XOR games, to functional analysis. An intriguing interplay between quantum communications complexity, non-locality, approximation algorithms, and functional analysis is becoming available.

Key references
[1] A. Yao, "Quantum circuit complexity", Proceedings of the 1993 IEEE 34th Annual Foundations of Computer Science, 352 (1993)
[2] H. Buhrman, R. Cleve, and A. Wigderson, "Quantum vs. classical communication and computation", Proceedings of the 30th Annual ACM Symposium on Theory of Computing (STOC 1998)
[3] R. Cleve, P. Høyer, B. Toner, and J. Watrous, "Consequences and limits of nonlocal strategies", Proc. of 19th IEEE Conference on Computational Complexity (2004)
[4] D. Gavinsky, J. Kempe, I. Kerenidis, R. Raz, and R. de Wolf, "Exponential separations for one-way quantum communication complexity, with applications to cryptography", SIAM Journal on Computing, 38, 1695 (2008)
[5] Z. Bar-Yossef, T. S. Jayram, I. Kerenidis, "Exponential separation of quantum and classical one-way communication complexity", SIAM J. Comput. 38 (2008)
[6] J. Briët, H. Buhrman, T. Lee, and T. Vidick, "Multiplayer XOR games and quantum communication complexity with clique-wise entanglement", [quant-ph/0911.4007]
[7] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf, "Nonlocality and communication complexity",

Rev. Mod. Phys. 81 (2010)

Quantum cryptographic protocols

The most import feat of quantum computers is that they can efficiently factor integers into their prime factors. This in turns means that most of the cryptographic protocols that are used today, whose security is based on the assumption that factoring is hard, will be rendered obsolete once a quantum computer is built. But all is not lost, quantum information processing opens up possibilities that are classically impossible. The well known key distribution protocol, due to Bennett and Brassard, establishes that two parties, who trust each other, can generate a secret shared key in such a way that if there is an eavesdropper trying to obtain the key or part thereof, will be detected with high probability. Once a secure key is established classical protocols, like the one-time pad, allow for secure message transmission. Such secure key distribution schemes are classically impossible! Moreover quantum key distribution schemes (QKD) are already commercially available.

It is natural and important to figure out what other protocols are possible using quantum technology. Unfortunately it was realized by Mayers, Lo and Chau that the schemes that are rendered insecure by Shor's factoring algorithm, asymmetric or public key cryptography, can not be unconditionally secure in the quantum world, something that KQD is. This again does not mean all is lost. Quantum information processing is able to realize tasks which are impossible classically such as biased Coin Tossing and Quantum Bit String Generation, Quantum String Commitment, resilient and unconditionally secure Digital Signatures, or Private Information Retrieval. 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.

Another strand has initiated secure protocols under mild assumptions. A very promising one is the bounded storage model. The assumption is that it is impossible to build quantum memories that store reliably huge amounts of qubits for a few seconds. Currently storing reliably a single qubit for a millisecond is already very challenging. It turns out that schemes, similar in flavor to QKD, allow for secure, under the bounded storage assumption, quantum implementations of a primitive called oblivious transfer (OT). Having this primitive as a building block allows one to build all cryptographic schemes that are used in practice today. More important these implementations appear technically not much more demanding than those of QKD.

However when have built a quantum computer that is able to efficiently and reliably factor integers, we need to find cryptographic protocols that are secure under computational assumptions, like current cryptographic protocols are secure under the assumption that factoring is hard. This line of research is part of post quantum cryptography. Progress has been made by Regev who developed a protocol based on the hardness of certain lattice problems. But these schemes are still too inefficient to be of practical use.

Key references
[1] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing”, in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, p. 175 (1984)
[2] A. Ambainis, “A new protocol and lower bounds for quantum coin flipping”, Journal of Computer and System Sciences, 134 (2004).
[3] A. Chailloux and I. Kerenidis, “Optimal quantum strong coin flipping”, 50th Annual Symposium on Foundations of Computer Science (FOCS) (2009).
[4] H. Buhrman, M. Christandl, P. Hayden, and H-K. Lo, and S. Wehner, “Security of quantum bit string commitment depends on the information measure”, Phys. Rev. Lett. 97, 250501 (2006).
[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(4) (2005).
[6] O. Regev, “On lattices, learning with errors, random linear codes, and cryptography”, In Proc. 37th ACM Symp. on Theory of Computing (STOC), 84 (2005).

Computational models and 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 have to satify very different needs from the perspective of the requirements on the hardware. What is more, they 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) and alternative, more general schemes for measurement-based quantum computing;
- 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 versions of classical cellular automata);
- Quantum Turing machines (quantum versions of classical Turing machines);
- Dissipation-driven quantum computation (computation realized by dissipative dynamics).

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. It will also turn out what model will eventually give rise to the most feasible architecture. 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]
[5] R. Raussendorf and H.-J. Briegel, "A one-way quantum computer", Phys. Rev. Lett. 86, 5188 (2001)
[6] D. Gross and J. Eisert, "Novel schemes for measurement-based quantum computation", Phys. Rev. Lett. 98, 220503 (2007)
[7] S. Diehl, A. Micheli, A. Kantian, B. Kraus, H. P. Büchler, and P. Zoller, "Quantum states and phases in driven open quantum systems with cold atoms", Nature Physics 4, 878 (2008)
[8] F. Verstraete, M. M. Wolf, and J. I. Cirac, "Quantum computation, quantum state engineering, and quantum phase transitions driven by dissipation", Nature Physics 5, 633 (2009)

Quantum simulation

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 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.

Key examples are ultra-cold atoms in optical lattices or trapped ions, both architectures having seen great progress in recent years. In those systems, one does not necessarily 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. Ideas like optical superlattices or the suitable exploitation of Feshbach resonances in the former class of physical systems add further flexibility. 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. Molecular energies within chemical precision can also be computed by quantum simulations. Such computations are among the smallest applications of quantum computing. The use of 30 to 100 qubits for those algorithms exceeds the limitations of classical computing of molecular energies.

Key references
[1] S. Lloyd, "Universal quantum simulators", Science 273, 1073 (1996)
[2] 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)
[3] 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)
[4] 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)
[5] A. Aspuru-Guzik, A. D. Dutoi, P. J. Love, and M. Head-Gordon, “Simulated quantum computation of molecular energies”, Science 309, 1704 (2005)
[6] D. Jaksch and P. Zoller, "The cold atom Hubbard toolbox", Ann. Phys. 315, 52 (2005)
[7] M. J. Hartmann, F. G. S. L. Brandao and M. B. Plenio, "Complex dynamics in coupled arrays of micro-cavities", Laser and Photonics Reviews 6, 527 (2008)
[8] I. Bloch, J. Dalibard, and W. Zwerger, "Many-body physics with ultracold gases", Rev. Mod. Phys. 80, 885 (2008)

4.3.2 Quantum error correction and control

Topological quantum information processing and computation

Topological quantum computation (TQC) is an approach to quantum information processing that eliminates decoherence at the hardware level by encoding quantum states and gates in global, delocalized properties of the hardware medium.

Most of the current quantum computing schemes assume nearly perfect shielding from the environment. Decoherence makes quantum computing prone to error and nonscalable, allowing only for very small "proof of principle" devices. Error correction software can in principle solve this problem, but progress along this path will take a long time. While much of the current research on other approaches to quantum computation is focused on improving control over well-understood physical systems, TQC research promises fundamental breakthroughs.

Delocalized, or topological degrees of freedom are intrinsically immune to all forms of noise which do not impact the entire medium at once and coherently. For media which exhibit an energy gap, kept at low enough temperatures, this is in fact all conceivable noise. If such materials can be constructed or found in nature, they will allow a much cleaner and faster realization of scalable quantum computation than other schemes.

TQC can be realized in effectively planar (2D) systems whose quasiparticles are anyons, that is they have nontrivial exchange behavior, different from that of bosons or fermions. If, in a system of three or more anyons, the result of sequential exchanges depends on the order in which they are performed, they are called non-Abelian anyons. Systems with non-abelian anyons allow for scalable quantum computation: many-anyon systems have an exponentially large set of topologically protected low-energy states which can be manipulated and distinguished from one another by experimental techniques, such as anyon interferometry recently realized in fractional quantum Hall systems.

A physical system which harbours anyons is said to be topologically ordered, or in a topological phase. One of the most important goals is to study such phases and their non-Abelian anyonic quasiparticles. The most advanced experiments in this direction are done in the context of the fractional quantum Hall effect (FQHE), where phases with fractionally charged Abelian anyons have already been seen and strong experimental evidence for the existence of non-Abelian anyons is emerging. In addition, very promising results have recently been obtained on engineered topologically ordered phases in Josephson junction arrays.

In addition to its natural fault-tolerance, topological quantum computation - though computationally equivalent to the conventional quantum circuit model - is a unique operational model of computation, which represents an original path to new quantum algorithms. New algorithms for approximation of certain hard #P hard computational problems have already been developed and this is opening up new areas of quantum algorithmic research.

The research objectives cover all aspects of topological quantum computation and include:

- Produce clear experimental evidence of topological phases suitable for TQC;
- design, simulate and build devices for fully scalable topological memory and gates;
- develop theoretical and algorithmic aspects of topological quantum computation as a new quantum computing paradigm;
- characterize topological phases and topological phase transitions, and link this scaling to properties of the topological entanglement entropy;
- propose engineered experimental realizations of topological phases;
- develop analytical and numerical computing skills for the FQHE and other topological systems;

Key references

[1] C. Nayak, S. H. Simon, A. Stern, M. Freedman, and S. Das Sarma, "Non-Abelian anyons and topological quantum computation", Rev. Mod. Phys. 80, 1083 (2008)
[2] G. P. Collins, "Computing with quantum knots", Scientific American 294, 56 (2006)
[3] M. H. Freedman, M. J. Larsen, and Z. Wag, "A modular functor which is universal for quantum computation", Commun. Math. Phys. 227, 605 (2002)
[4] A. Yu. Kitaev, "Fault-tolerant quantum computation by anyons", Ann. Phys. 303, 1 (2003)
[5] G. Kells, J. K. Slingerland, and J. Vala, "Description of Kitaev's honeycomb model with toric-code stabilizers", Phys. Rev. B 80, 125415 (2009)
[6] W. Bishara, P. Bonderson, C. Nayak, K. Shtengel, and J. K. Slingerland, "Interferometric signature of non-Abelian anyons", Phys. Rev. B 80, 155303 (2009)
[7] M. Dolev, M. Heiblum, V. Umansky, A. Stern, and D. Mahalu, "Observation of a quarter of an electron charge at the : nu = 5/2 quantum Hall state", Nature 452, 829 (2008)
[8] I. P. Radu, J. B. Miller, C. M. Marcus, M. A. Kastner, L. N. Pfeiffer, and K. W. West, "Quasiparticle

properties from tunneling in the nu = 5/2 fractional quantum hall state", Science 320, 899 (2008)
[9] S. Gladchenko, D. Olaya, E. Dupont-Ferrier, B. Doucot, L. B. Ioffe, and M. E. Gershenson, "Superconducting nanocircuits for topologically protected qubits", Nature Physics 5, 48 (2008)
[10] R. L. Willett, L. N. Pfeiffer, and K. W. West, "Measurement of filling factor 5/2 quasiparticle interference with observation of charge e/4 and e/2 period oscillations", Proc. Natl. Acad. Sci. 106, 8853 (2009)

Quantum error correction and purification

The ability to carry out coherent quantum operation even in the presence of inevitable noise is a key requirement for quantum information processing. To cope with this decoherence problem, active strategies (quantum error correcting codes) as well as passive ones (error avoiding codes) have been developed.

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).

In error avoiding codes, no active monitoring/intervention on the system is in principle necessary, since errors are simply circumvented. Error avoiding is based on the symmetry structure of the system-environment interaction that in some circumstances allows for the existence of decoherence-free subspaces (DFS), i.e. subspaces of the system Hilbert state-space over which the dynamics is still unitary. The prototype noise model for which this situation occurs is provided by the so-called collective decoherence, where all the qubits are affected by the environment in the same way. For encoding a single logical noiseless qubit for general collective decoherence (dephasing), four (two) physical qubits are needed. DFSs have been experimentally demonstrated in a host of physical systems, and their scope extended by generalizing the idea of symmetry-aided protection to noiseless subsystems.

A fruitful connection with the theory of entanglement purification, which has been developed primarily in the context of quantum communication, and has been used in protocols such as the quantum repeater, is also emerging. Entanglement purification or distillation is a method to “distill” from a large ensemble of impure and noisy (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] P. Zanardi and M. Rasetti, “Noiseless Quantum Codes”, Phys. Rev. Lett. 79, 3306 (1997)
[5] 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)
[6] 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)
[7] A. M. Steane, "Overhead and noise threshold of fault-tolerant quantum error correction", Phys. Rev. A 68, 042322 (2003)
[8] E. Knill, "Quantum computing with very noisy devices", Nature 434, 39 (2005)

Geometric methods for fault-tolerant quantum computing

An alternative approach to achieve fault-tolerant quantum computation is by geometric means. In this approach, quantum information is encoded in a set of energy degenerate states, depending on dynamically controllable parameters. Quantum gates are then enacted by driving the control parameters along suitable loops. These transformations, termed holonomies, are suitable to realize a set of universal quantum gates. Implementation schemes of geometrical computation have been proposed for several different physical systems, most notably for trapped ions. The existing protocols for fault tolerant quantum computation have been specifically designed for phenomenological uncorrelated noise, while few results are known for a scenario with memory effects, i.e. non-Markovian noise, arising from the Hamiltonian interaction with the environment. In particular this raises the question of fault tolerant schemes for phenomenological noise with memory.

Key references
[1] J. A. Jones, V. Vedral, A. Ekert, and G. Castagnoli, “Geometric quantum computation using nuclear magnetic resonance”, Nature 403, 869 (2000)
[2] P. Zanardi and M. Rasetti, “Holonomic quantum computation”, Phys. Lett. A 264, 94 (1999)
[3] L.-M. Duan, J. I. Cirac, and P. Zoller, “Geometric manipulation of trapped ions for quantum computation”, Science 292, 1695 (2001)
[4] R. Alicki, M. Horodecki, P. Horodecki, and R. Horodecki, “Dynamical description of quantum computing: Generic non-locality of quantum noise”, Phys. Rev. A 65, 062101 (2002)
[5] M. Terhal and G. Burkard, “Fault-tolerant quantum computation for local non-Markovian noise”, Phys. Rev. A 71, 012336 (2005)

Quantum control theory for quantum information devices

Quantum error correction enables fault-tolerant quantum computation to be performed, provided that each elementary operation meets a certain fidelity threshold, but unfortunately, this puts extremely demanding constraints on the allowable errors. Threshold estimates vary between 0.01% to fractions of a percent, but none of the candidate physical implementations available to date has met such requirements yet. Therefore the main open challenge is a practical one: Will the necessary fidelity ever be reached in practice for elementary operations, and maintained while scaling up qubit number and system complexity? This will ultimately determine the winning hardware platform for future quantum information devices, analog to what has happened with silicon for conventional computing.

One feature is common to all candidate QIP implementations: the need for an extremely accurate control of the quantum dynamics at the individual level, with much better precision than has been achieved before. Optimal control theory is a very powerful set of methods developed over the last decades to optimize the time evolution of a broad variety of complex systems, from aeronautics to economics. The basic underlying idea is to pick a specific path in parameter space to perform a specific task. This is expressed mathematically by a cost functional that depends on the state of the system and is minimized with respect to some control parameters. More recently, this approach is being successfully applied to quantum systems, e.g., in the context of ultra-fast laser pulses and light-assisted molecular reactions. A big advantage is that, in a quantum-mechanical situation, the goal can be reached via interference of many different paths in parameter space, rather than just one. This allows, for instance, to exploit faster non-adiabatic processes, allowing to perform more gate operations within the decoherence time, which is crucial to apply fault-tolerant error correction. In future work, these ideas will also be more closely tied to methods of quantum systems identification.

Over the last few years, quantum optimal control theory (QOCT) has been applied to different aspects of quantum information processing, in particular to the implementation of scalable quantum gates with real physical systems. The figure of merit to be optimized in this case is the fidelity, defined as the projection of the physical state obtained by actually manipulating the chosen system onto the logical state that the gate aims at obtaining. Several examples, from atoms in optical lattices and atom chips to trapped ions and superconducting charge qubits, have indicated systematic improvements in fidelity beyond the fault-tolerance threshold, taking into account

experimentally available configurations and known sources of imperfection.

Key references
[1] N. Khaneja, R. Brockett, and S. J. Glaser, “Time optimal control in spin systems”, Phys. Rev. A 63, 032308 (2001)
[2] T. Schulte-Herbrueggen, A. K. Spoerl, N. Khaneja, S. J. Glaser, "Optimal control-based efficient synthesis of building blocks of quantum algorithms seen in perspective from network complexity towards time complexity", Phys. Rev. A 72, 042331 (2005)
[3] C. Brif, R. Chakrabarti, and H. Rabitz, "Control of quantum phenomena: Past, present, and future", arXiv:0912.5121 [quant-ph]
[4] K. Singer, U. Poschinger, M. Murphy, P. Ivanov, F. Ziesel, T. Calarco, and F. Schmidt-Kaler, "Experiments with atomic quantum bits - essential numerical tools", arXiv:0912.0196 [quant-ph]

4.3.3 Theory of entanglement and quantum channels

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. For the experimental verification of this resource, the tool of entanglement witnesses allows to detect entanglement with local measurements only, and thus is easily implementable with present technology. 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 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, 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] M. Bourennane, M. Eibl, C. Kurtsiefer, S. Gaertner, H. Weinfurter, O. Guehne, P. Hyllus, D. Bruss, M. Lewenstein, and A. Sanpera, “Experimental detection of multipartite entanglement using witness operators”, Phys. Rev. Lett. 92, 087902 (2004)
[7] M. Horodecki, J. Oppenheim, and A. Winter, "Partial information can be negative”, Nature 436, 676 (2005)
[8] Recent tutorial reviews include M. B. Plenio and S. Virmani, “An introduction to entanglement measures”, Quant. Inf. Comp. 7, 1 (2007); R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, “Quantum entanglement”, Rev. Mod. Phys. 81, 865 (2009)

Multi-party entanglement and 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 M. Westmoreland, "Reversibility of local transformations of multiparticle entanglement", quant-ph/9912039
[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)

Device independent certification of security in quantum information

Device independent quantum information processing is a new approach in which one uses the

non-local correlations exhibited by local measurements on entangled quantum particles to certify the quantumness of the underlying state and measurements. That is the quantumness is certified by the violation of a Bell inequality. This approach allows a qualitative increase of the security of quantum cryptography: QKD becomes secure even if the source of entangled states is not controlled and/or the measurement devices unknown. The measurement devices could even be supplied by an adversary, and QKD remains secure.

The same basic philosophy can be applied to "self testing of quantum computers": by using quantum non locality one can test (in polynomial time) that a quantum computer indeed operates as it should, without the need to model how individual gates act, or the need to carry out the full tomography of the whole computer. A major theoretical and experimental challenge is to make these proposals practical. On the experimental side by realising long distance Bell inequality violation with the detection loophole closed, on the theoretical side by improving the security proofs.

Key references
[1] Ll. Masanes, R. Renner, M. Christandl, A. Winter, and J. Barrett, "Unconditional security of key distribution from causality constraints", quant-ph/0606049
[2] A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-independent security of quantum cryptography against collective attacks", Phys. Rev. Lett. 98, 230501 (2007)
[3] Ll. Masanes, "Universally-composable privacy amplification from causality constraints", Phys. Rev. Lett. 102, 140501 (2009)

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 keys. The general framework for distilling classical keys from quantum states have been also established, opening the possibility of secure communication on extremely noisy channels. 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 problem that was left open until recently was 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 or - as it turned out, equivalently, the additivity problem for the minimum output entropy. This problem could recently be solved in seminal work, in that it turned out that entangled inputs indeed do help. In contrast, for Gaussian channels - in the context of the promising field of continuous-variable quantum information, with practical importance in quantum communication with fibers - it is now known that additivity holds true. These findings open up new exciting questions about the role of entanglement in quantum communication. Also, the exact relationship between entanglement and the correlations useful for establishing secret keys is not yet entirely understood.

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. Also, quantum analogues of certain basic classical network theory primitives have been identified, and the evidence for new non-classical features, such as negative partial information established. Further investigations will be needed to identify differences and similarities in the classical and quantum network theories.

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] P. W. Shor, "Equivalence of additivity questions in quantum information theory", Commun. Math. Phys. 246, 453 (2004)
[5] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim “Secure key from bound entanglement”, Phys. Rev. Lett. 94, 160502 (2005)
[6] P. Hayden and A. Winter, "Counterexamples to the maximal p-norm multiplicativity conjecture for all p > 1", Comm. Math. Phys. 284, 263 (2008)
[7] M. B. Hastings, "A counterexample to additivity of minimum output entropy", Nature Physics 5, 255 (2009)
[8] S. Lloyd, V. Giovannetti, L. Maccone, N.J. Cerf, S. Guha, R. Garcia-Patron, S. Mitter, S. Pirandola, M. B. Ruskai, J.H. Shapiro, and H. Yuan, "Proof of the bosonic minimum output entropy conjecture", arXiv:0906.2758 [quant-ph]

"Quantum proofs" for classical problems

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. The entanglement between two systems cannot be shared with many others, a principle called ‘monogamy’: this leads to a fruitful relationship between entanglement theory and classical cryptography, and in particular between entanglement distillation and the classical key agreement scenario. Since the two schemes shares similar objects, quantities and relations, it is expected that the parallel growth of these domains will lead to a deeper understanding of both of them. In this sense, quantum information theory offers novel proof tools for "quantum proofs" for classical problems, hence quantum information theory having a significant impact outside quantum theory.

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
[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
[3] N. Gisin and S. Wolf “Linking classical and quantum key agreement: Is There “Bound information”?” in Proceedings of CRYPTO 2000, Lecture Notes in Computer Science vol. 18889, pp. 482-500, Springer (2000)
[4] A. Acin, J. I. Cirac, and Ll. Masanes “Multipartite bound information exists and can be activated”, Phys. Rev. Lett. 92, 107903 (2004)
[5] D. Gross, Y.-K. Liu, S. T. Flammia, S. Becker, and J. Eisert, "Quantum state tomography via compressed sensing", arXiv:0909.3304 [quant-ph]; D. Gross, "Recovering low-rank matrices from few coefficients in any basis", arXiv:0910.1879 [quant-ph]
[6] A. Drucker and R. de Wolf, "Quantum proofs for classical problems", arXiv:0910.3376 [quant-ph]

4.3.4 (De)coherence and quantum effects in complex quantum systems

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] P. Zanardi and M. Rasetti, "Noiseless quantum codes", Phys. Rev. Lett. 79, 3306 (1999)
[2] L. Viola, "On quantum control via encoded dynamical decoupling", quant-ph/0111167
[3] W. Dür and H. J. Briegel, "Stability of macroscopic entanglement under decoherence", Phys. Rev. Lett. 92, 180403 (2004)
[4] A. R. R. Carvalho, F. Mintert, and A. Buchleitner, "Decoherence and multipartite entanglement", Phys. Rev. Lett. 93, 230501 (2004)
[5] R. F. Werner and M. M. Wolf, "Bell inequalities and entanglement", Quant. Inf. Comp. 1, 1 (2001)
[6] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, and D. Roberts, "Non-local correlations as an information theoretic resource", Phys. Rev. A 71, 022101 (2005)
[7] D. Perez-Garcia, M.M. Wolf, C. Palazuelos, I. Villanueva, and M. Junge, "Unbounded violation of tripartite Bell inequalities", Comm. Math. Phys. 279, 455 (2008)
[8] M. Navascués, S. Pironio, and A. Acín, "A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations", New J. Phys. 10, 073013 (2008)

Quantum effects in opto-mechanical and nano-mechanical systems

Recently, partly driven by experimental progress, theoretical ideas have been proposed to cool mechanical physical systems such as massive micro-mirrors to close to their quantum ground state, giving rise to observable quantum effects. In particular, opto-mechanical systems, where mechanical degrees of freedom are coupled to coherent optical systems, allow for such a cooling by suitably exploiting radiation pressure effects. Indeed, the preparation of such systems in superposition or entangled states appears within reach. Such systems may give rise to ultra-sensitive force sensors as well as to primitives for quantum information devices. They can also be combined with other physical architectures to give rise to promising hybrid architectures.

Key references
[1] C. Fabre, M. Pinard, S. Bourzeix, A. Heidmann, E. Giacobino, and S. Reynaud, "Quantum-noise reduction using a cavity with a movable mirror", Phys. Rev. A 49, 1337 (1994)
[2] S. Mancini, V. I. Manko, and P. Tombesi, "Ponderomotive control of quantum macroscopic coherence", Phys. Rev. A 55, 3042 (1997)
[3] I. Martin, A. Shnirman, L. Tian, and P. Zoller, "Ground-state cooling of mechanical resonators",

Phys. Rev. B 69, 125339 (2004)
[4] J. Eisert, M. B. Plenio, S. Bose, and J. Hartley, "Towards quantum entanglement in nanoelectromechanical devices", Phys. Rev. Lett. 93, 190402 (2004)
[5] D. Vitali, S. Gigan, A. Ferreira, H. R. Böhm, P. Tombesi, A. Guerreiro, V. Vedral, A. Zeilinger, and M. Aspelmeyer, "Optomechanical entanglement between a movable mirror and a cavity field", Phys. Rev. Lett. 98, 030405 (2007)
[6] F. Marquardt and S. M. Girvin, "Optomechanics", Physics 2, 40 (2009)
[7] M. Wallquist, K. Hammerer, P. Zoller, C. Genes, M. Ludwig, F. Marquardt, P. Treutlein, J. Ye, and H. J. Kimble, arXiv:0912.4424 [quant-ph]

Quantum coherence in biological systems

The question to which quantum coherence and entanglement plays a role in biological systems is receiving increasing attention also from a perspective of quantum information theory. There is experimental evidence that in the functioning of the energy transport in photosynthetic light-harvesting complexes, such as the Fenna-Matthews-Olson photosynthetic complex, long-lived coherence effects may play an important role. Quantum information ideas can contribute to an understanding of the role of noise, stochastic resonance effects, coherence, entanglement and quantum-walk-like dynamics in such systems. Hence, principles and techniques, both numerical and analytical, that have been developed over the last decade in quantum information science may find a new area of application here. This potentially fruitful new arena is now beginning to be explored bringing together quantum information scientists with bio-physicists from theory and experiment thus opening up a new arena of interdisciplinary research.

Key references

[1] G. S. Engel, T. R. Calhoun, E. L. Read, T.-K. Ahn, T. Mancal, Y-C. Cheng, R. E. Blankenship, and G. R. Fleming, Nature 446, 782 (2007)
[2] A. Olaya-Castro, C. F. Lee, F. Fassioli-Olsen, and N. F. Johnson, "Efficiency of energy transfer in a light-harvesting system under quantum coherence", Phys. Rev. B 78, 085115 (2008)
[3] M. Mohseni, P. Rebentrost, S. Lloyd and A. Aspuru-Guzik, "Environment-assisted quantum walks in photosynthetic energy transfer", J. Chem. Phys. 129, 174106 (2008)
[4] M.B. Plenio and S.F. Huelga, "Dephasing assisted transport: Quantum networks and biomolecules", New J. Phys. 10, 113019 (2008)
[5] H. J. Briegel and S. Popescu, "Entanglement and intra-molecular cooling in biological systems? - A quantum thermodynamic perspective", arXiv:0806.4552 [quant-ph]
[5] F. Caruso, A. W. Chin, A. Datta, S. F. Huelga, and M. B. Plenio, "Highly efficient energy excitation transfer in light-harvesting complexes: The fundamental role of noise-assisted transport", J. Chem. Phys. 131, 105106 (2009)

4.3.5 Links between quantum information science and quantum many-body theory

Complexity of simulating many-body systems

In recent years, a strong link between quantum information science and the study of condensed matter systems has been established, in particular to research on strongly correlated quantum systems, so systems that play a key role in the understanding of phenomena such as high-temperature superconductivity. This link is less surprising as it may at first seem: After all, quantum correlations are distributed and shared in an intricate manner in ground states of local quantum many-body systems. The quantitative theory of entanglement can provide new insights into the exact structure of such quantum correlations, in turn opening up new perspectives for the development of new algorithms for the simulation of such quantum many-body problems. Indeed, the significant findings in this field may be seen as a further justification for the importance of the study of entanglement.

Notably, ground states of local systems typically satisfy what is called an "area law", in that the

entanglement of a subregion scales only with the surface area of that region. That is to say, they have very little entanglement, an assertion that can be made quantitative. Exploiting this observation, one arrives at the insight that only few effective degrees of freedom are being exploited by natural systems, compared to the exponentially larger Hilbert space. Suitably parameterizing this set by means of what is called tensor networks hence gives rise to new efficient simulation algorithms for the study of strongly correlated systems. Matrix-product states, projected entangled pair states, tree tensor networks or states from entanglement renormalization from a real-space renormalization ansatz are examples of such an approach. These are sets of states, described by polynomially many real parameters, for which one can still efficiently compute local expectation values by means of suitable tensor contractions, and which still grasp the essential physics of the problem.

In such a language, certain elementary obstacles of classical simulations of quantum systems such as in time evolution also become clear, and quantitative links to the theory of criticality and quantum phase transitions can be established. Ideas like Lieb-Robinson bounds, relating to the speed of information propagation in quantum lattice systems, provide key insights into the distribution of correlations in local quantum many body problems with respect to static of dynamical properties. Ideas of quantum information science can hence relate to

- Fundamental issues of the complexity of a classical description of quantum many-body systems in a language of computer science;
- A reassessment of the functioning of existing methods such as the Density Matrix Renormalization Group (DMRG) approach, and
- The development of novel feasible and efficient algorithms specifically for two-dimensional or fermionic systems, opening up new perspectives in the simulation of strongly correlated quantum many-body systems.

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] K. Audenaert, J. Eisert, M. B. Plenio, and R. F. Werner, “Entanglement properties of the harmonic chain”, Phys. Rev. A 66, 042327 (2002)
[2] J. I. Latorre, E. Rico, and G. Vidal, "Ground state entanglement in quantum spin chains", Quant. Inf. Comp. 4, 048 (2004)
[3] 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] F. Verstraete and J. I. Cirac, "Renormalization algorithms for quantum many-body systems in two and higher dimensions", cond-mat/0407066
[5] J. Kempe, A. Kitaev, and O. Regev, "The complexity of the local Hamiltonian problem", SIAM Journal of Computing, Vol. 35, 1070 (2006)
[6] G. Vidal, "Entanglement renormalization", Phys. Rev. Lett. 99, 220405 (2007)
[7] L. Amico, R. Fazio, A. Osterloh, and V. Vedral, "Entanglement in many-body systems", Rev. Mod. Phys. 80, 517 (2008)
[8] F. Verstraete, J. I. Cirac, V. Murg, "Matrix product states, projected entangled pair states, and variational renormalization group methods for quantum spin systems", Adv. Phys. 57, 143 (2008)
[9] J. Eisert, M. Cramer, M. B. Plenio, "Area laws for the entanglement entropy", Rev. Mod. Phys. 81 (2010)

Connection between QIP and quantum chemistry

Related to the previous field, quantum information theory can help in gaining an understanding the quantum correlations that are present in physical problems from quantum chemistry. Ideas of monogamy and entanglement distribution are related to the quantum representability problem,

being of key importance in theoretical quantum chemistry. New ideas inspired by quantum information theory relate to proofs of hardness of certain questions in quantum chemistry, as well as to new simulation methods of such physical systems, contributing to the wider context of gaining a deeper understanding of complex quantum systems.

Key references
[1] A. Klyachko, "Quantum marginal problem and N-representability", J. Phys. A Conf. Ser. 36, 72 (2006)
[2] Y.-K. Liu, M. Christandl, and F. Verstraete, "N-representability is QMA-complete", Phys. Rev. Lett. 98, 110503 (2007)

4.3.6 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 as well as 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 Quantum Information Technologies

Even if the main thrust of the ongoing investigations in QIPC still belongs to basic research, one can already identify some of its areas that are closer to potential applications and even ready for commercial exploitation. In particular:

- **Quantum Communication** has already reached the market: two companies – the European idQuantique and the US one MagiQ) announced almost simultaneously the availability of a commercial quantum cryptography product. Other European companies developed commercial quantum key distribution scheme such as Elsag plc and SmartQuantum; moreover, in Japan major industrial players – NEC, Mitsubishi, Toshiba and NTT among others – started to allocate entire development teams to QKD systems (which did result in NEC and Mitsubishi already presenting working prototypes).
- **Quantum Computation** promises to deliver in the mid-term few-qubit quantum simulators which could be used to simulate the dynamics of complex systems (notice that a system with more than 30 qubits would be already beyond the reach of any foreseeable classical machine). Such few-qubit quantum computers will have also applications in quantum communication (as quantum repeaters), where they will be used to extend the working distances of quantum key distribution protocols beyond the current limitations.
- **Quantum Information Science – Theory** can also provide applications in the form of new classical simulation techniques for quantum many-body systems. Results from entanglement theory have in fact already led to fruitful generalizations of, e.g., the density matrix renormalization group method. The development of improved simulation techniques will lead to a deeper understanding of strongly correlated quantum systems (e.g., high-Tc superconductors, quantum magnets, etc.), which are of central interest in several areas of physics and that, in turn, will provide the basis for new technological applications.

Furthermore, a fresh look at QIPC from the broadest possible perspective also allows the identification of technologies that have gone past the proof-of-principle phase and are approaching the real world deployment stage. These Quantum Information Technologies (QITs) which are designed to control and manipulate entanglement for (quantum) information processing and communication, can be split into two main categories, being

- either technologies which represents genuine applications of QIPC (quantum information enabled technologies),
- or technologies which are needed for further advancing the field of QIPC (quantum information enabling technologies).

In what follows we detail the most promising technologies belonging to the first category, and the most needed ones as far as the second category is concerned.

4.4.1 Applications of QIPC (quantum enabled technologies)

Quantum Random Number Generators (QRNG)

Our information based society consumes lots of random numbers for a wide range of applications like, e.g., cryptography, PIN numbers, lotteries, numerical simulations, etc. The production of random numbers at high rates is technically challenging; at the same time, given the pervasiveness of the deployment of random numbers, poor random number generators can be economically very damaging. Today, there are three kinds of random number generators on the market: computer-based pseudo-random number generators, discretised thermal noise and quantum based.

The first kind produces sequences of numbers that look random, but are in fact the result of a deterministic process. The second kind is based on the complexity of thermal noise; however thermal relaxation times make these random number generators relatively slow, in the range of tens of Kbit/second. On the other hand, quantum physics provides the only truly source of randomness in Nature. Moreover, in the basic configuration (a photon impinging on a beam splitter followed by two detectors associated to the bit values 0 and 1) the origin of the randomness is clearly identified. Today’s commercial quantum random number generators produce about 4 Mbit/second. Their drawback is a significant cost compared to thermal noise based devices, but one expects that (near) future QRNG will provide higher rates at lower costs.

Quantum Metrology

Entangled states provide instances of objects that can be designed to be very robust to unwanted noise, while at the same time being extremely sensitive to a quantity we need to measure. 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 synchronisation via the use of frequency-entangled pulses. For instance, in the latter case, picosecond resolution at 3 km distance has been attained. Large scale laser interferometers with kilometre 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 limits. Scientists in Europe and Australia have recently demonstrated the required quantum noise reduction (through squeezing) of laser light at kilohertz frequencies.

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 few nanometers) 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. In addition, the quantum regime is being explored and applied 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.

One of 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 polarisation 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 characterising chromatic dispersion in fibers. The intrinsically quantum interplay between the polarisation and frequency entanglement in CSPDC gave rise to a polarisation mode dispersion

measurement technique that provides an order of magnitude enhancement in the resolution.

Quantum Imaging

It is possible to generate quantum entanglement between the spatial degrees of freedom of light, an aspect which enables one 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.

4.4.2 Technologies needed to advance QIPC (quantum enabling technologies)

Quantum Interfaces

Quantum interfaces between quantum information carriers (quantum states of light) and quantum information storage and processors (atoms, ions, solid state) are required as essential parts of a full-scale quantum information system. Such interfaces should thus be developed for connecting quantum computers in small networks, or more generally for quantum communication purposes. Let us first contrast the quantum technology required here to its classical counterpart. In classical optical communication, information is transferred encoded in pulses of light, which are possibly amplified, and then detected by photo detectors, transformed into electrical current pulses, amplified by electronics, and sent to computers, phones, etc. This transformation of light into electrical signals forms a classical light-matter interface. But in quantum information processing, classical amplification or detection of light is inadequate, because it destroys the quantum state by adding extra noise to it. Hence a quantum interface has to be developed, in order to transfer the quantum state of light qubits (or light continuous variables) to or from atomic qubits (or atomic continuous variables). Quantum interfaces usually involve storage elements (quantum memories), and processing elements (deterministic or conditional quantum gates). They often involve also long-distance quantum teleportation of long lived atomic states, which allow for communication and quantum secret sharing tasks. Such long lived entanglement shared over a long distance requires transfer of entanglement from light (the long distance carrier) to atoms (the long lived objects), realized by the quantum interface. Many different quantum technologies can be used to implement the interfaces, e.g. atomic ensembles, cavity QED, solid state devices, etc.

Heralded entangled photon-pair sources

Point to point earth based quantum communication is limited in distance by the losses of optical fibers. For long distance quantum communication (>500km) protocols with quantum repeaters are needed. Such schemes require, among other things, high quality sources of pairs of entangled photon, either on demand or heralded. Today’s sources are probabilistic, based on spontaneous parametric down conversion. Future sources should keep or improve on the optical quality of the existing ones (compatible with single-mode optical fibers, Fourier-transform limited, and coherence length of several centimetres), provide larger rates and yields (probability of a photon pairs) while

reducing the probability of multi-pairs. The exact type of entanglement is not essential, but should involve two photons, one in each of two quantum channels (i.e. the entanglement obtained by bunching two single photons on a beam splitter is not appropriate). At least one of the photons should be at the telecom wavelength around 1.55 microns. Depending on the protocol, the second photon can be around the same wavelength or at a shorter one, below one micron (but one should bear in mind that future progress in quantum communication protocols may affect the required specifications).

Chip traps for quantum computing

The DiVincenzo criteria for quantum computing are currently approached from different directions. To date, ion traps offer the possibility to precisely manipulate and read out single qubits and to perform entangling gate operations, while the size of the system is currently limited to a few qubits. In contrast, with neutral atoms large ensembles of entangled qubits have been created while the manipulation of single atoms and their detection present a major challenge. Both these approaches – bottom up for ions and top down for atoms – need to be further developed to take quantum computation the next scale. Chip technology for trapping ions or neutral atoms will play a major role in this development. For neutral atoms, chip traps offer precise positioning that enables controlled interactions and detection of single atom states. The first on-chip implementation of a high-finesse fibre resonator has very recently been demonstrated, offering at the same time a tool for manipulation, entanglement and detection of ions. In addition, this should be used in the future to establish an interface between stationary (atoms) and flying qubits (photons). For ions, the chip traps serve to increase the number of qubits that can be handled. The segmentation of trap electrodes in microscopic traps allows for a multitude of miniature ion traps on one chip. Future developments have to meet two major challenges: finding a trap technology that features small heating rates and long coherence times, and a trap design that allows for transport of the ions (along with their contained quantum information) between all miniature traps on the chip. An integration of optical cavities as demonstrated for neutral atoms would be desirable, too.

4.5 Fundamental issues about QIPC physics

QIPC relies on the manipulation and control of ensembles of qubits behaving according to the laws of quantum physics. From the perspective of classical macroscopic physics, and indeed for the normal world-view not trained on quantum phenomena, these laws are counter-intuitive. In this sense QIPC aims to turn paradoxes into products. On the other hand, macroscopic physics is itself ultimately based on the quantum laws. This raises the question why the paradoxical traits of quantum mechanics do not manifest themselves in everyday experience, i.e., how the classicality of the world emerges from quantum mechanics. Roughly, the answer is that the quantum paradoxes all require the superposition principle, i.e., coherence, and that in complex systems coherence is shifted to less and less accessible degrees of freedom and thus effectively lost. This process, known as "decoherence" is thus a crucial element for the formation of the world as we know it. Seen form the other side, i.e., a QIPC application, decoherence is the universal enemy, ever trying to wash out the hard won coherence. In either case decoherence marks the boundary between quantum and classical phenomena.

The quantum-classical boundary which is set by decoherence has a very rich structure. It is certainly not merely a question of system size, since suitable collective degrees of freedom of some large systems can exhibit remarkable coherence in some collective degrees of freedom. Many clever ways of extending the quantum side for QIPC have been designed. Clearly, a sufficient isolation from the environment at large is required. 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 concerns a change in physical world-view, which is stimulated by QIPC research, and is spreading to the physics community and, possibly, to the society as a whole. In the discussions of the founding fathers of quantum theory, the quantum-classical boundary was explored in thought experiments, often with paradoxical conclusions. Many QIPC experiments with atoms and photons can be viewed as modern realizations of these thought experiments. This stimulates a much more concrete view of the old paradoxes, both theoretically, through establishing new ways to model quantum phenomena and the discovery of new principles, and experimentally through a fantastically increased control of fully coherent processes. This body of knowledge is now making its way into the teaching of quantum physics at universities. The formation of an reliable 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 aesthetical qualities of this physics will be the researchers of tomorrow, who will apply their skills to QIPC or to other fields.

Secondly, and perhaps 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:

- **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 or the number of particles involved 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.