Eur. Phys. J. D **36**, 203–228 (2005)
DOI: 10.1140/epjd/e2005-00251-1

THE EUROPEAN PHYSICAL JOURNAL D

Quantum information processing and communication

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

P. Zoller[1,2,a], Th. Beth[3,†,b], D. Binosi[1,4,c], R. Blatt[1,5,b], H. Briegel[1,2,b], D. Bruss[6,b], T. Calarco[7,4,b], J.I. Cirac[8,b], D. Deutsch[9,b], J. Eisert[10,11,b], A. Ekert[12,b], C. Fabre[13,b], N. Gisin[14,b], P. Grangiere[15,b], M. Grassl[3,b], S. Haroche[16,b], A. Imamoglu[17,b], A. Karlson[18,b], J. Kempe[19,b], L. Kouwenhoven[20,b], S. Kröll[21,b], G. Leuchs[22,b], M. Lewenstein[23,b], D. Loss[24,b], N. Lütkenhaus[25,b], S. Massar[26,b], J.E. Mooij[27,b], M.B. Plenio[10,b], E. Polzik[28,b], S. Popescu[29,b], G. Rempe[8,b], A. Sergienko[30,b], D. Suter[31,b], J. Twamley[32,b], G. Wendin[33,b], R. Werner[34,b], A. Winter[35,b], J. Wrachtrup[36,b], and A. Zeilinger[37,b]

[1] Institut für Quantenoptik and Quanteninformation der Österreichischen Akademie der Wissenschaften, 6020 Innsbruck, Austria
[2] Institut für Theoretische Physik, Universität Innsbruck, 6020 Innsbruck, Austria
[3] Universität Karlsruhe, Institut für Algorithmen und Kognitive Systeme, 76131 Karlsruhe, Germany
[4] ECT*, 38050 Villazzano (TN), Italy
[5] Institut für Experimentalphysik, Universität Innsbruck, Innsbruck, Austria
[6] Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, 40225 Düsseldorf, Germany
[7] CRS BEC-INFM Dipartimento di Fisica, Università di Trento, 38050 Povo, Italy
[8] Max-Planck-Institut für Quantenoptik, 85748 Garching, Germany
[9] Centre for Quantum Computation, Clarendon Laboratory, University of Oxford, Oxford OX1 3PU, UK
[10] QOLS, Imperial College London, London SW7 2BZ, UK
[11] Universität Potsdam, Institut für Physik, 14469 Potsdam, Germany
[12] DAMTP, University of Cambridge, Cambridge CB3 0WA, UK
[13] LKB, École Normale Supérieure et Université Pierre et Marie Curie, 75252 Paris Cedex 05, France
[14] Université de Genéve GAP-Optique, 1211 Genève 4, Switzerland
[15] Laboratoire Charles Fabry de l'Institut d'Optique, Centre Universitaire, 91403 Orsay, France
[16] Département de Physique de l'École Normale Supérieure, 75005 Paris Cedex, France
[17] Institut für Quantenelektronik, 8093 Zürich, Germany
[18] FET, DG INFSO, European Commission, 1049 Brussels, Belgium
[19] Université de Paris-Sud, 91405 Orsay Cedex, France
[20] QTG, Kavli Intstitute of Nanoscience Delft, Delft University of Technology, 2628CJ Delft, The Netherlands
[21] Lund Institute of Technology, Division of Atomic Physics, 22100 Lund, Sweden
[22] Lehrstuhl für Optik, Institut für Optik, Information und Photonik (Max-Planck-Forschungsgruppe), 91058 Erlangen, Germany
[23] ICFO - Institut de Ciències Fotòniques, 08034 Barcelona, Spain
[24] Department of Physics and Astronomy, University of Basel, 4056 Basel, Switzerland
[25] Institut für Theoretische Physik I, Universität Erlangen-Nürnberg, 91058 Erlangen, Germany
[26] Laboratoire d'Information Quantique, Université Libre de Bruxelles, 1050 Brussels, Belgium
[27] Kavli Intstitute of Nanoscience Delft, Delft University of Technology, 2628CJ Delft, The Netherlands
[28] Niels Bohr Institute, Copenhagen University, 2100, Denmark
[29] University of Bristol, H.H. Wills Physics Laboratory, Bristol BS8 1TL, UK
[30] Department of Electrical and Computer Engineering, Boston University, Boston MA 02215, USA
[31] Fachbereich Physik, Universität Dortmund, 44221 Dortmund, Germany
[32] Department of Mathematical Physics, Logic Building, National University of Ireland, Maynooth, Co. Kildare, Ireland
[33] Department of Microtechnology and Nanoscience - MC2, Chalmers University of Technology, 412 96 Göteborg, Sweden
[34] Institut für Mathematische Physik, TU Braunschweig, 38106 Braunschweig, Germany
[35] Department of Mathematics, University of Bristol, Bristol BS8 1TW, UK
[36] Universität Stuttgart, Physikalisches Institut, 70550 Stuttgart, Germany
[37] Institut für Experimentalphysik, Universität Wien, 1090 Wien, Austria

Received 12 August 2005
Published online 13 September 2005 –

[a] Editing author
[b] Contributing author
[c] e-mail: daniele.binosi@uibk.ac.at, editing assistant

Abstract. We present an excerpt of the document "Quantum Information Processing and Communication: Strategic report on current status, visions and goals for research in Europe", which has been recently published in electronic form at the website of FET (the Future and Emerging Technologies Unit of the Directorate General Information Society of the European Commission, `http://www.cordis.lu/ist/fet/qipc-sr.htm`). This document has been elaborated, following a former suggestion by FET, by a committee of QIPC scientists to provide input towards the European Commission for the preparation of the Seventh Framework Program. Besides being a document addressed to policy makers and funding agencies (both at the European and national level), the document contains a detailed scientific assessment of the state-of-the-art, main research goals, challenges, strengths, weaknesses, visions and perspectives of all the most relevant QIPC sub-fields, that we report here.

Dedicated to the memory of Prof. Th. Beth, one of the pioneers of QIPC, whose contributions have had a significant scientific impact on the development as well as on the visibility of a field that he enthusiastically helped to shape since its early days.

PACS. 03.67.-a Quantum information

Foreword

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. QIPC has burgeoned in Europe over the last decade, producing high-level scientific results, and eventually reaching critical mass in many of its subfields, where European research is currently at the leading edge.

The potential of QIPC was quickly recognized by FET, the Future and Emerging Technologies Unit of the Directorate General Information Society of the European Commission, whose pathfinder activity played a crucial role for the development of the field in Europe. At the 5th European QIPC Workshop (September 2004 in Rome) a special session was organized by FET, titled "Perspectives for QIPC in the Seventh Framework Program". The main point was that input towards the European Commission would be needed on the part of the scientific community for the preparation of the Seventh Framework Program. There was a general discussion on the actions to be taken with the aim to promote QIPC research in Europe, strengthen its image in a coherent way, unify the research community by elaborating a common European strategy and goals, and, especially, provide the required input to the European Commission, reaching in an appropriate way decision makers. It was then decided (i) to write a strategic report including an assessment of current results and an outlook on future efforts, and (ii) to expand the strategic report with a detailed technical assessment, to draw up a summary of long and medium term goals, and to express visions and challenges for QIPC in Europe. P. Zoller was nominated as the editing author and the coordinator of a committee in charge of this. Work on the document started immediately afterwards, involving the contributors to the present paper.

On the 10th of May, the QIPC strategic document reached a stable version that was published in electronic form at the IST-FET website (`http://www.cordis.lu/ist/fet/qipc-sr.htm`). It will be soon published as an official publication of the European Commission, and, in the future, will continue to be updated regularly as a "living document" in the context of the project ERA-Pilot QIST.

Besides being a document addressed to policy makers and funding agencies (both at the European and national level), the strategic report has an added scientific value in the form of a detailed technical assessment of the state-of-the-art (at the end of 2004), main research goals, challenges, strengths, weaknesses, visions and perspectives of all the most relevant QIPC sub-fields. This complete overview of the (European) QIPC research cannot be found anywhere else. The present paper contains these parts as excerpted from the strategic report itself.

1 Introduction: the major visions 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.

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.

2 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.

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 cryptokeys whose privacy is guaranteed by the laws of Nature. Quantum key distribution is already making its first steps outside laboratories both for fiber based networks and also for communication via satellites. However, significant more basic research is necessary to increase both the secret bit rate and the distance. This is the field of Quantum Communication.
- 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.

3 Assessment of current results and outlook on future efforts

3.1 Quantum communication

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

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

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

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

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

3.1.1 Fiber based systems

Towards higher bit rates

1. Fast electronics, this includes fast sources and fast and low-loss phase modulators. This is mainly a (non-trivial) engineering problem.
2. Improved detectors: lower dark counts (<10–6 per ns), shorter dead times (<1 μs), less time-jitter (<100 ps) and higher detection efficiency (>15%). This is a non trivial solid state physics challenge.
3. Invent and investigate new protocols inspired by existing and reliable components, like "decoy states" [1] and the SARG protocol [2]. Also protocols based on fast homodyne detection methods can be thought of, such as the continuous variables protocols [3]. This is mainly a matter of the physicists' imagination!

4. It is known that existing classical communication procedures and security proofs do not make optimal use of the correlations that are generated in the physical set-up and can be improved. Further improvement in secure key rate can follow from a scenario of trusted sending and receiving devices which cannot be manipulated by an eavesdropper. It would also be valuable to have security proofs easier to understand for classical cryptographers.
5. Single-photon sources have made spectacular progress in the last years [4], but it is not clear yet whether they will be able to fulfill practical needs for high repetition rates, high coupling efficiency and electronic cooling (no liquid helium). It is not even necessary to use single photon sources since also QKD with weak laser pulses can be proven to be secure; see e.g. [5]. Moreover, the performance of ideal single photon sources can also be achieved using laser pulses with a phase reference, as has been proven by a recent analysis by Koashi [6]. Fourier-transform limited single-photon sources with negligible time-jitter could also be used as building blocks for linear optics quantum computing.
6. Quantum communication with entangled states will be important to further develop quantum teleportation and entanglement swapping in view of their possible use in connection future quantum computers.

Towards longer distances

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

1. Improve the detectors: lower dark counts automatically increase the distance. However, the bit rate decreases exponentially with distance.
2. Improve the fibers: air-core photonic band-gap fibers have the potential to surpass silica fibers. (Even pure silica core photonic bandgap fibers could improve on today's telecom fibers, but only by at most 0.05 dB/km). This is a tremendous engineering challenge, with applications which would impact the whole field of optical telecommunications!
3. Use quantum relays exploiting quantum teleportation and entanglement swapping [7]. Dividing the connection in sections allows one to open the receiving detector less frequently, lowering thus the dark-count rate. For any given detector efficiency, this allows one to gain a factor of about 5 in distance. But the maximal distance is still limited and the bit rate still decreases exponentially with distance. Quantum relays require entangled photon sources. It should be stressed that quantum relays are anyway necessary for quantum repeaters. Today's longest distance demonstration is a quantum teleportation lab experiment connecting three 2 km long sections. The next crucial milestone in this direction will be a field demonstration over tens of km of entanglement swapping.
4. Use quantum repeaters: fully developed quantum repeaters have the potential of extending quantum communication to arbitrary long distances with a constant bit rate [8]. It is extremely challenging physics and still basic research. A quantum repeater requires a quantum memory. The latter has to outperform an optical fiber delay loop. This important milestone is described in Section 3.1.3.

Quantum continuous variables

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

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

New applications and protocols

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

between single photon and continuous variable protocols, and the search for more efficient and fast ways of distributing keys.

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

3.1.2 Free space systems

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

Towards space quantum communication

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

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

Several studies are currently underway and suggest the feasibility of space-based experiments based on current technologies [9].

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

1. free-space distribution of entanglement over distances above 5 km;
2. implementation of active and/or adaptive optics techniques for single photons;
3. free-space teleportation of a single-photon state;
4. free-space entanglement swapping;
5. free-space quantum cryptography (with discrete or continuous variables) demonstration of single-photon uplinks to a satellite;
6. demonstration of a single-photon down-link from a satellite;
7. quantum cryptography between two widely separated locations on Earth via satellites;
8. development of narrow-band sources of entangled photons for daylight operation;
9. implementation of an entangled-photon source on a satellite;
10. teleportation of a photon state up to a satellite;
11. teleportation of a photon state between two ground locations via a satellite;
12. teleportation of a photon state down from a satellite;
13. satellite-satellite quantum communication.

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

3.1.3 Quantum interfaces and memory

An interface between quantum information carriers (quantum states of light) and quantum information storage and processors (atoms, ions, solid state) is an integral part of a full-scale quantum information system. In classical communication information is transferred encoded in pulses of light. The pulses are detected by photodetectors, transformed into electrical current pulses, amplified by electronics, and sent to computers, phones, etc. This transformation of light into electrical signals forms classical light-matter interface. In quantum information processing simple classical detection of light is inadequate for recording into memory, because it destroys the quantum

state by adding extra noise to it. Hence a quantum interface has to be developed. Instead of direct transformation of light pulses into electrical pulses, as in classical communication, quantum state transfer of light qubits (or continuous variables) with atomic qubits (or continuous variables) has to be developed in QIPC. Certain kinds of quantum interfaces, based on cavity QED, are discussed in Section 6.2 with an emphasis on computing tasks. Other kinds of quantum interfaces, such as quantum memory and long-distance quantum teleportation of long lived atomic states, are important for communication and quantum secret sharing tasks. It is obvious that long lived entanglement shared over a long distance requires transfer of entanglement from light (the long distance carrier) to atoms (the long lived objects). Such transfer can only be done via a special light-atoms quantum interface. Distant long lived entangled objects can serve as secure "quantum identification cards". These kinds of tasks can be address via such physical implementations as atomic ensembles, which are easier to implement and to scale.

Currently various aspects of light-atoms quantum interface and memory are investigated both in Europe[1] and in the US[2].

Quantum memory for light and quantum repeaters

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

State of the art: proposals for quantum memory for light have been put forward during the past decade, in Europe and in the US. Recently the first quantum memory for a weak coherent pulse has been demonstrated [10]. A quantum memory which is to be used for storage, and not for quantum processing, is based on a simple physical system consisting of a small cell filled with atomic gas at room temperature — an atomic ensemble. Demonstrated quantum state storage time of up to 4 ms corresponds to propagation time over a distance of about 1000 km. The storage cell works close to the free space propagation wavelength.

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

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

Long distance atomic teleportation and repeaters

State of the art: atomic teleportation over a distance of a fraction of a millimeter has been recently demonstrated by two groups, in Europe and in the US. Long distance teleportation of atomic states requires interface with light. A significant progress has been achieved on the way towards implementation of a repeater primarily by US groups [Monroe, Kimble, and Kuzmich]. Entanglement of atomic ensembles at a distance of half a meter has been demonstrated in Europe [11]. The technology is simple and relies on glass cells filled with atomic gas at room temperature. At present the technology is limited to near infrared wavelength suitable for free space propagation.

Vision and perspectives: long distance deterministic teleportation will allow realization of distributed quantum networks. Extension of entanglement of atomic ensembles to up to a kilometer is possible with specially designed optical set-ups. For yet longer distances quantum repeaters proposed in Europe present an option. Towards this goal a combination of a repeater with entangled trapped ions will be useful. Another possible way to realize an efficient repeater is to use atomic ensemble quantum memory [10] to store one photon of an entangled pair produced by downconversion. The repeater approach may allow teleportation of atomic states over many kilometers.

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

1. extending memory capabilities to single photon/qubit storage;

[1] Copenhagen University (E. Polzik); University of Aarhus, Denmark (K. Molmer and M. Drewsen); Max Planck Institute for Quantum Optics, Garching, Germany (I. Cirac and G. Rempe); Institute for Photonic Sciences, Barcelona, Spain (M. Mitchel); University of Kaiserslautern, Germany (M. Fleischhauer); University of Heidelberg, Germany (J. Schmiedmayer); and Lab Kastler Brossel, CNRS, Paris (M. Pinard and E. Giacobino).

[2] Harvard University (M. Lukin); Caltech (J. Kimble), University of Michigan, Ann Arbor (Ch. Monroe); and Georgia Institute of Technology, Atlanta (A. Kuzmich).

2. achieving efficient retrieval of the stored quantum state;
3. improving the fidelity of storage;
4. exploring other types of atomic/solid state ensembles useful for storage applications; solid-state system, atoms on a chip.

3.2 Quantum computing

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

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

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

At present, there are a number of technologies under investigation for their suitability to implement a quantum computer. No single technology meets currently all of these requirements in a completely satisfactory way. Therefore, the ongoing research on quantum information processing is highly interdisciplinary, diverse and requires a coordinated effort to create synergies while the common goal is the implementation of a working quantum processor. While at present several approaches have demonstrated basic gate operations and are even able to prove that quantum computing has become reality with few qubits, large scale quantum computation is still a vision which requires ongoing research for many years to come.

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

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

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

3.2.1 Quantum computing with trapped ions

A. Physical approach and perspective

Ion trap quantum computation is based on schemes devised by Cirac and Zoller [12]. 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 [13].

Currently, experimental ion trap QIP is pursued by 10 groups worldwide, 6 of which are located in Europe[3], 3 groups are currently setting up ion trap experiments for QIP in Europe[4], and three more groups are dealing with the theory aspects[5].

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 two and three trapped ions are routinely loaded to a linear trap.

[3] R. Blatt (Innsbruck, A), M. Drewsen (Aarhus, DK), P. Gill (Teddington, UK), W. Lange (Sussex, UK), A. Steane (Oxford, UK), Ch. Wunderlich (Maynooth, Ei).

[4] J. Eschner (Barcelona, E), T. Schaetz (MPQ Garching, D), F. Schmidt-Kaler (Ulm, D).

[5] J.I. Cirac (MPQ Garching, D), K. Molmer (Aarhus, DK) and P. Zoller (Innsbruck, A).

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

C. Strengths and weaknesses

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

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

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

D. Short-term goals (next 3–5 years) (cf. also [13])

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

E. Long-term goals (2010 and beyond) (cf. also [13])

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

3.2.2 Atoms and cavity QED

A. Physical approach and perspective

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

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

- Firstly, a gate operation is performed by means of a controlled collision of two qubits. Such collisions require the preparation of a well-defined quantum state of atomic motion, as can be achieved by either cooling single atoms into the ground state of the trapping potential (bottom-up approach), or by loading a Bose-Einstein condensate into an optical lattice (top-down approach). Both the bottom-up and the top-down approach offer the possibility of a massive parallelism,

with many pairs of atoms colliding at once. The top-down approach is ideal to develop a quantum toolbox for simulating nontrivial many-body systems.

- Secondly, a gate operation is performed by exchanging a photon between two individual qubits. Such a scheme can be implemented with free-space atoms emitting photons in a random direction (probabilistic approach), or with atoms in high-finesse cavities where the strong atom-photon coupling guarantees full control over photon emission and absorption (deterministic approach). The latter approach is realized either with Rydberg atoms in microwave cavities or with ground-state atoms in optical cavities. If each atom resides in its own cavity, the scheme guarantees addressability and scalability in a unique way. As quantum information is exchanged via flying photons, the individual qubits of the quantum register can easily be separated by a large distance. The photon-based scheme is therefore ideal to build a distributed quantum network.

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

Besides performing discrete gate operations according to a predefined algorithm, neutral-atom systems are ideal for simulating quantum many-body systems. In general, quantum systems are very hard to simulate, given the fact that the dimension of the corresponding Hilbert space grows exponentially with the number of particles. This hinders our ability to understand the physical properties of general materials with a classical computer. However, using a quantum computer, it should be possible to simulate other quantum systems in a very efficient way.

Currently, both schemes of performing a gate operation with neutral atoms (collision or photon-exchange) are investigated experimentally in several dozen laboratories worldwide, about half of them located in Europe[6]. In fact, European theory groups have played a crucial role in the development of QIPC science from the very beginning. The close collaboration between experiment and theory in Europe is unique, partly because of the support provided by the European Union.

B. State of the art

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

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

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

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

1. Probabilistic approach in free space:
   - a single trapped atom has been entangled with a single photon.
2. Deterministic approach using microwave cavities: circular Rydberg atoms and superconducting cavities are proven tools for fundamental tests of quantum mechanics and quantum logic:
   - complex entanglement manipulations on individually addressed qubits with long coherence times have been realized;
   - gates have been demonstrated;
   - new tools for monitoring decoherence of mesoscopic quantum superpositions have been developed.

[6] The European groups working with a controllable number of atoms include I. Bloch (Mainz, D), T. Esslinger (Zurich, CH), P. Grangier (Orsay, F), S. Haroche (Paris, F), D. Meschede (Bonn, D), G. Rempe (Garching, D), H. Walther (Garching, D), and H. Weinfurter (Munich, D). Several other groups are presently setting up new experiments, including W. Ertmer (Hanover, D), E. Hinds (London, UK), J. Reichel (Paris, F), and J. Schmiedmayer (Heidelberg, D). The experimental program is strongly supported by implementation-oriented theory groups like H. Briegel (Innsbruck, A), K. Burnett (Oxford, UK), J.I. Cirac (Garching, D), A. Ekert (Cambridge, UK), P.L. Knight (London, UK), M. Lewenstein (Barcelona, E), K. Mølmer (Aarhus, DK), M.B. Plenio (London, UK), W. Schleich (Ulm, D), P. Tombesi (Camerino, I), R. Werner (Braunschweig, D), M. Wilkens (Potsdam, D), and P. Zoller (Innsbruck, A).

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

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

1. cooling of atoms to quantum degeneracy (Bose-Einstein condensation);
2. transport of an ensemble of atoms using a magnetic conveyor belt;
3. manipulation of atoms with electric and optical fields;
4. very long coherence times by using appropriate qubit states;
5. multilayer atom chips with sub-μm resolution and smooth magnetic potentials.

C. Present challenges

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

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

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

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

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

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

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

1. An efficient scheme to address, manipulate and detect a single qubit in the microtrap of an atom chip must be developed.
2. A quantum memory, that is the reading and writing of quantum information into single atoms or atomic ensembles must be realized.
3. Next, a two-qubit quantum gate, for example by employing a controlled collision, must be implemented.
4. The full demonstration of the potential provided by atom chips requires the realization of large-scale integration, e.g., with several 10 qubits.
5. Potential roughness very close (μm) to micro-fabricated structures is of concern for qubit storage and transport. Even though for current-carrying structures the problem can be solved and compensated for by the design and fabrication methods as developed recently, micro-structures with fewer defects might be needed for permanent magnets.

6. Merging atom-chip technology and cavity QED is promising. High-finesse miniature optical or microwave cavities can be coupled to ground state or Rydberg atoms trapped on a chip. Coherence preserving trap architectures are an important first step towards a fully scalable architecture combining the best of both worlds.

A tutorial review on QIPC with atoms, ions and photons can be found in, e.g., [14,15].

3.2.3 Superconducting circuits

A. Physical approach and perspective

Quantum computation with superconducting circuits exploits the intrinsic coherence of the superconducting state, into which all electrons are condensed. Quantum information is stored in the number of superconducting electrons (charge qubit), in the direction of a current (flux qubit) or in oscillatory states (phase qubit). Systems are fabricated with thin film technology and operated at temperatures below 100 mK. Measurements are performed with integrated on-chip instruments. Coupling between qubits can be made strong. In principle the system is scalable to large numbers. The US QIST roadmap gives more detailed information and references, though not quite up to date [16]. A general background is provided in [17].

Approximately 30 groups work on superconducting quantum bits in Europe[7], Japan, China and the USA.

B. State of the art

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

C. Strengths and weaknesses

Strengths:

- high potential for scalable integrated technology;
- strong coupling between qubits possible;
- flexible opportunities with different qubit types;
- mature background technology, 20 years of experience;
- driver of applications in solid-state quantum engineering;
- long history of pushing the limits of measurement towards quantum limits;
- low-temperature or superconducting technologies necessary for integration with solid state microtraps for hybrid systems.

Weaknesses:

- coherence limited by defects in tunnel barriers;
- slight variation in qubit parameters associated with fabrication.

D. Short-term goals (next 3–5 years)

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

E. Long-term goals (2010 and beyond) (cf. also [17])

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

[7] D. Esteve and D. Vion (Saclay, F), J. Rooij and H. Harmans (Delft, NL), P. Delsing (Chalmers, S), A. Zorin (PTB, D), E. Ilichev (Jena, D), A. Ustinov (Erlangen, D), F. Hekking, O. Buisson (Grenoble, F), J. Pekola (Helsinki, FI), S. Paroanu Jyväskyla, FI), D. Haviland (KTH, Stockholm, S) (and others. In theory: G. Schön, (Karlsruhe, D), R. Fazio (Pisa, I) A. Wilhelm (München, D), G. Wendin (Chalmers, S), M. Grifoni (Regensburg, D), G. Falci (Catania, I), K. Bruder (Basel, CH), and others.

3.2.4 Semiconductor quantum dots

A. Physical approach and perspective

III-V Semiconductor heterostructures (e.g. GaAs, InP, InAs, etc.) form the backbone of today's opto-electronics combining ultrafast electronics (e.g. HEMT), low-power optics together with the conversion between electronics and optics. The industrial development of this material class has also been fruitfully utilized in the field of QIPC. Employing nanofabrication and/or self-assembling techniques, quantum dots have been defined that can be addressed electrically and/or optically. The emerging field of quantum opto-electronics can provide an interface between solid state qubits and single-photon quantum optics. The most important recent results pertaining to this subfield are described in [18–22].

Currently, quantum dot (QD) spin based quantum information processing (QIP) is pursued by 10 groups worldwide, 5 of which are located in Europe[8].

B. State of the art

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

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

[8] L. Kouwenhoven (Delft, NL), K. Ensslin (ETH-Zurich, CH), G. Abstreiter (TU-Munich, D), Ch. Bayer (Dortmund, D) and A. Imamoglu (ETH-Zurich, CH)], as well as D. Loss (Basel, CH) on the theory side.

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

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

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

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

C. Short-term goals (next 3–5 years)

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

represent a major step for implementing quantum information processing in optically active quantum dots.

D. Long-term goals (2010 and beyond)

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

The opto-electronic properties of III-V semiconductor quantum dots can already find applications on a mid-term timescale. There are proposals for quantum repeaters (i.e. necessary devices in long distance quantum communication) based on III-V semiconductors. Repeaters generally require small qubit circuits capable of Bell state measurements and storage of a quantum state in combination with single photon detectors and emitters. A recent scheme [23] shows that even with low efficiency, high fidelity can be reached in long-distance communication.

3.2.5 Linear optics quantum computation

A. Physical approach and perspective

Optical quantum computing (OQC) exploits measurement-based quantum computing schemes with photons as physical qubits. The interaction between separate photonic qubits is induced by measurement, as opposed to a direct interaction via nonlinear media. The two main physical architectures for OQC are based on proposals by Knill, Laflamme and Milburn [24], the KLM architecture, and by Raussendorf and Briegel [25], the one-way quantum computer with cluster states:

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

B. State of the art

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

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

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

Enabling technologies for OQC are:

- characterization of photonic quantum states and processes. A complete, tomographic, characterization of individual devices is indispensable for error-correction and has quite progressed within the last years. Quantum process tomography, invented by Chuang and Nielsen, can be used to fully characterize a quantum gate, probing either with a range of input states or a single multi-qubit state. Based on the information gained from a complete process characterization it was recently shown how to estimate (and bound) the error probability per gate;
- development of single photons and/or entangled photon sources is required for OQC. Currently, no source of timed single photons or entanglement is available. In the meantime, bright, albeit non-deterministic sources

of correlated photons or entangled-photon pairs are critical to allow on-going evaluation of circuit technology as it is developed. Ultra bright and compact sources, some fiber-coupled to improve mode quality, have been developed. Relatively brighter sources (though not yet in absolute terms) have been demonstrated using periodically-poled nonlinear waveguides;
- high-fidelity multi-qubit measurements (in the KLM scheme) and reliable preparation of multi-qubit states (in both the KLM and the cluster state scheme).

C. Strengths and weaknesses

Current drawbacks of the OQC approach are low photon creation rates, low photon detection efficiencies, and the difficulties with intermediate storage of photons in a quantum memory (see also Sect. 3.1.3). Advantages are obviously low decoherence (due to the photon's weak coupling to the environment), ultrafast processing, compatibility to fiber optics and integrated optics technologies and, in principle, straightforward scalability of resources. However, the low efficiencies quoted above are presently an important practical limitation to scalability, in the sense that they damp exponentially the success probability of most quantum operations.

D. Challenges

The main challenges for OQC can be summarized as follows:

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

3.2.6 Impurity spins in solids

A. Physical approach and perspective

Storage and processing of information can be carried out using individual atomic and molecular spins in condensed matter. Systems falling into this category include dopant atoms in semiconductors like phosphorus or deep donors in silicon or color centers in diamond, molecules like C60, rare earth ions in dielectric crystals and unpaired electrons at radiation induced defects or free radicals in molecular crystals. The main attraction of spins in low-temperature solids is that they can store quantum information for up to several thousand seconds [26]. 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.

Currently, 12 European research groups are engaged in QIP research regarding impurity spins in solids[9].

B. State of the art

Atomic and molecular spins in solids have received considerable attention as qubits. Already Kane's [26] 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 [27]. Most approaches use electron or nuclear spin degrees of freedom as quantum bits. The specific advantages of spin systems includes long decoherence times [28] and access to highly advanced methods for precise manipulation of quantum states. The experimental techniques that have made liquid state NMR the most successful QIP technique in terms of precise manipulation of quantum states so far are currently being transferred to solid-state systems. These systems may be able to overcome the scalability problems that plague liquid state NMR while preserving many of the advantages of today's liquid state work.

In detail the following landmark results have been achieved:

1. magnetic resonance on single defects detected by charge transport and single spin state measurements by optical techniques;
2. single and two qubit quantum gates on single defect spins in diamond;
3. for rare earth crystals preparation and readout of ensemble qubit states Rabi flops of a qubit, and qubit

[9] A. Briggs (Oxford, UK), P. Grangier (Orsay, F), O. Guillot-Noël and P. Goldner (Paris, F), S. Kröll (Lund, S), J.L. LeGouët (Orsay, F), M. Mehring (Stuttgart, D), K. Mølmer (Aarhus, DK), J.F. Roch (Cachan, F), M. Stoneham (London, UK), D. Suter (Dortmund, D), J. Twamley (Maynooth, IR), J. Wrachtrup (Stuttgart, D).

decoherence times on the order of seconds have been achieved. State control and quantum state tomography with a fidelity $> 90\%$ was shown;
4. the preparation of Bell states with electron and nuclear spin ensembles as well as a three qubit Deutsch-Jozsa algorithm has been achieved;
5. A scalable architecture has been developed for N@C60 on Si and decoherence times have been measured to be up to 1 s.

C. Strengths and weaknesses

The strength of defect center QIP in solids are the long decoherence times of spins even under ambient conditions and the precise state control. Depending on the system, electrical as well as optical single spin readout has been shown (fidelity of 80%). Substantial progress in the nanopositioning of single dopants with respect to control electrodes has been achieved. Weaknesses are: electrical and optical readout of spin states has been shown up to now for only a single type of defect. Nanopositioning of defects is still a major challenge (which has seen dramatic progress for phosphorus in silicon). However there are schemes, based on deep donors in Si, where nanopositioning is not needed. Instead the randomness is exploited so as to make maximum use of spatial and spectral selection to isolate qubits and their interactions. Manipulation and readout is optical. The situation is similar for rare earth crystals, but in this case a fully scalable scheme still needs to be developed.

D. Short-term goals (next 3–5 years)

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

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

E. Long-term goals (2010 and beyond)

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

3.3 Quantum information science-theory

3.3.1 Introduction

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

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

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

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

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

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

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

3.3.2 Quantum algorithms & complexity

Following Deutsch's fundamental work in 1985 that demonstrated the potential power of quantum algorithms and quantum computers [29], Shor demonstrated in 1994 that integers can be efficiently factorized on a quantum computer [30]. Factoring is the task of decomposing an integer, say 15, into a product of prime numbers: $15 = 3 \times 5$. 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 [31].

In parallel with the development of new quantum algorithms, new algorithmic techniques have been developed. Examples of these are adiabatic quantum computing which is a very versatile method of approaching virtually any computational task; and quantum random walks which have enabled important generalizations of Grover's search algorithm. There has also been considerable development of new protocols for quantum communication. The objective may be to carry out a task which is possible classically, but with significantly less communication, such as Quantum Fingerprinting or the Hidden Matching problem [32,33]. Or it may be to realize tasks which are impossible classically such as biased Coin Tossing and Quantum Bit String Generation, resilient and unconditionally secure Digital Signatures, or Private Information Retrieval. The importance of these latter tasks lies in their application to "mistrustful cryptography", this is the field of cryptography dealing with the problem of two or more people who do not trust each other, but must accomplish some goal together (for instance concluding a commercial deal, consulting a data base, etc.).We expect that the existing protocols will be improved and will gradually be implemented in the laboratory (as was recently the case for quantum bit string generation). We also expect the development of new protocols for quantum communication.

3.3.3 Computational models & architectures

There are many different ideas of how to make quantum systems compute [34–38]. While these different computational models are typically equivalent in the sense that one can simulate the other with only polynomial overheads in resources, they may be quite different in practice, when it comes to a particular class of problems. They also suggest different procedures to achieve fault tolerant computation, many of them yet to be explored in detail. At the moment the main contenders of fundamental architectures are:

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

Most recently, we have seen a series of theoretical work analyzing the connection between the different computational models. The benefit of these works lies in a better understanding of the capabilities and advantages of the individual models, and of the essential features of a quantum computer. In the future we expect that optimized models (i.e. taking the best out of the different approaches) will be developed. We also expect that these models will have an increasing impact on (i) the formulation of new quantum algorithms and (ii) the evaluation of physical systems regarding their suitability for fault-tolerant quantum computation. Both of these points are of great importance for the field: while new algorithms will further enlarge the range of applications for quantum computers, new methods for fault-tolerant computation will hopefully make it technologically less challenging to realize scalable quantum computers in the laboratory.

3.3.4 Quantum simulations

Quantum simulators may become the first application of quantum computers, since with modest requirements one may be able to perform simulations which are impossible with classical computers [39–44]. At the beginning of the 80's it was realized that it will be impossible to predict and describe the properties of certain quantum systems using classical computers, since the number of variables that must be stored grows exponentially with the number of particles. A quantum system in which the interactions between the particles could be engineered would be able to simulate that system in a very efficient way. This would then allow, for example, studying the microscopic properties of interesting materials permitting free variation of system parameters. Potential outcomes would be to obtain an accurate description of chemical compounds and reactions, to gain deeper understanding of high temperature superconductivity, or to find out the reason why quarks are always confined.

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

3.3.5 Quantum error correction & purification

The ability to carry out coherent quantum operation even in the presence of inevitable noise is a key requirement for quantum information processing [45,46]. 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 Sect. 3.3.3).

At the same time, a fruitful connection to the theory of entanglement purification is emerging, which has been developed primarily in the context of quantum communication, and has been used in protocols such as the quantum repeater [47–51]. Entanglement purification is a method to "distill" from a large ensemble of impure (low-fidelity) entangled states a smaller ensemble of pure (high-fidelity) entangled states. It seems that appropriately generalized procedures can be employed also in general quantum computation (e.g. for quantum gate purification, or for the generation of high fidelity resource states) while benefiting from the relaxed thresholds that exist for entanglement purification.

3.3.6 Theory of entanglement

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

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

Considerable progress in this area has been made in recent years, in particular in the case of bi-partite

entanglement [52–57], 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 Sect. 3.3.10).

3.3.7 Multi-party entanglement & applications

Research on multi-particle entanglement is on the one hand expected to be focused on novel protocols for quantum information processing in the multi-partite setting [58–62]. 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 Sect. 3.3.10).

3.3.8 Noisy communication channels

The proper understanding of the capacities of quantum communication channels is at the heart of the study of quantum communication tasks. Of particular importance are the transmission of classical or quantum information, or establishing secret key. But it is also known that one can use noise and perfect side communication to implement other cryptographic primitives like bit commitment and oblivious transfer. Channel capacities are of central interest in several different settings, being reflected notably by the classical capacity of quantum channels, quantum capacities, and entanglement-assisted capacities [63–67].

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

Finally, it is to be expected that more problems, as well as new perspectives, will arise when one considers multi-user channels, i.e., with more than one sender/receiver. While single-sender-receiver settings serve well to study bipartite correlations, such problems have an immediate impact on understanding multi-partite correlations and their role in quantum communication via noisy channels.

3.3.9 Fundamental quantum mechanics and decoherence

Quantum information was born, in part, via research on the famous Einstein-Podolski-Rosen paradox and the issue of quantum non-locality. In turn, quantum information led the discussion to move beyond purely qualitative aspects of non-locality to defining and investigating quantitative aspects [68–74]. 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.

3.3.10 Spin-off to other fields

A very exciting aspect of theoretical work in QIS is the impact that it is beginning to make on other fields of science [75–79]. In the case of classical computing such insights include the first exponential bounds on certain locally decodable codes, classical proof systems for lattice problems, bounds on the query complexity of local search problems, an efficient classical cryptographic scheme whose security is based on quantum considerations, and a quantum method to compute how many Toffoli gates are required to realize a reversible classical computation. The potential that QIS is offering for classical computing and mathematics may be understood by the following analogy. Real analysis is a very successful discipline but it contained a number of unsolved problems that were only solved by considering complex numbers, i.e. going to a larger space in which to describe the problem. By analogy we expect that moving from classical state space into the much larger quantum mechanical state space we will find novel approaches towards the solution of problems that ostensibly lie entirely within the classical realm. As the enormous size of the quantum mechanical state space is due to entanglement, one may view this as a further consequence of entanglement and a further justification for the importance of the study of entanglement (see Sect. 3.3.6).

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

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

3.3.11 European perspective

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

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

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

3.4 Fundamental issues about QIPC physics

QIPC relies on the manipulation and control of ensembles of qubits behaving according to the counter-intuitive laws of quantum physics. Most generally, though, quantum features are washed out in systems made of large numbers of particles. This decoherence phenomenon defines a kind of boundary between the microscopic world, where the quantum laws are dominant, and the macroscopic world, which behaves classically in spite of its underlying quantum nature. This boundary is fuzzy however. It largely reflects

our lack of ability to isolate completely the system under study from its environment, made of a very big number of uncontrolled particles. By developing clever schemes, physicists and quantum information scientists are finding ways to fight this environment-induced decoherence. Some methods rely on the observation and manipulation of the environment itself, combined with feedback procedures counteracting the effects of decoherence on the system under study. Other methods, borrowing from the error correction schemes of classical computers, are at least in principle even more powerful. They are based on the redundant coding of the information in an ensemble of entangled qubits, monitoring the effects of decoherence on a subset of these qubits and applying correction procedures on others to restore the initial quantum state affected by decoherence. The progress towards the implementation of these methods, a prerequisite for large scale quantum computing to ever become feasible, is discussed in other parts of this report.

Here, we focus on other aspects of this field of research. The first is of a pedagogical nature. By attempting to "harness" the quantum laws and make them useful to achieve logical tasks, QIPC scientists are, in some way, changing our view of the quantum-classical boundary. In the discussions of the founding fathers of quantum theory, this boundary was explored in thought experiments dealing with the principles of quantum measurements where microscopic systems are put in contact with macroscopic meters. Many QIPC experiments with atoms and photons can be viewed as modern realizations of these thought experiments. By doing them, physicists get more familiar with quantum concepts such as complementarity and wave particle duality. These experiments are now included in all modern textbooks of quantum physics. This pedagogical element must not be underestimated. The formation of an intuition for the quantum world is certainly an important ingredient in the education of students in physics and the study of QIPC is an excellent way to acquire this intuition. The students attracted by the esthetical qualities of this physics will be the researchers of tomorrow, who will apply their skills to QIPC or to other fields.

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

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

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

4 Prospects for applications and commercial exploitation

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

Quantum communication

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

Quantum computing

Quantum information processing in the sense of fault tolerant quantum computing for large-scale numerical algorithms (for example Shor's algorithm) is the ultimate goal. Within the next few years one expects few-qubit quantum computer with applications to quantum repeaters, for example. On the intermediate time scale one goal is to beat classical computations on whatever (non-trivial) problem. This could be achieved, for example, with specialized quantum computing, as with quantum simulators (see Sect. 3.3.4) where a system with more than 30 qubits is already beyond the reach of any foreseeable classical machine

Quantum metrology

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

Large scale laser interferometers with kilometer arm lengths are currently being built or started operating in Europe, the USA and Japan with the hope to achieve the first direct detection ever of gravitational waves and thus to open a new field of astronomy. For these detectors the classical sensitivity limit is a serious restriction. It is likely that for the first detection one will have to implement continuous variable entangled light beams in the two interferometer arms to overcome the classical limit. Scientists in Europe and Australia have recently demonstrated the required quantum noise squeezing of laser light at kilohertz frequencies.

State-of-the-art atom clocks developed in Europe have reached the level of accuracy limited by quantum noise of

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

Quantum technologies

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

It is also possible to generate quantum entanglement between the spatial degrees of freedom of light, which enables us to use quantum effects to record, process and store information in the different points of an optical image, and not only on the total intensity of light. One can then take advantage of a characteristic feature of optical imaging, which is its intrinsic parallelism. This opens the way to an ambitious goal, with a probable significant impact in a mid-term and far future: that of massively parallel quantum computing. In a shorter perspective, quantum techniques can be used to improve the sensitivity of measurements performed in images and to increase the optical resolution beyond the wavelength limit, not only at the single photon counting level, but also with macroscopic beams of light. This can be used in many applications where light is used as a tool to convey information in very delicate physical measurements, such as ultra-weak absorption spectroscopy, Atomic Force Microscopy etc. Detecting details in images smaller than the wavelength has obvious applications in the fields of microscopy, pattern recognition and segmentation in images, and optical data storage, where it is now envisioned to store bits on areas much smaller than the square of the wavelength. Furthermore, spatial entanglement leads to completely novel and fascinating effects, such as "ghost imaging", in which the camera is illuminated by light which did not interact with the object to image, or "quantum microlithography", where the quantum entanglement is able to affect matter at a scale smaller than the wavelength.

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

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

5 Conclusions

At present, as it should be clear from the reported state of the art, QIPC belongs mainly to basic research, where key advances are often unplanned outcomes of curiosity driven research. Nevertheless, there is a clear set of conclusions concerning the goals for QIPC in the coming five to ten years that can be drawn.

- **Quantum computing**: in quantum computing the goal for the next ten years is to develop a few-qubit general-purpose quantum processor including error correction, as a model system to demonstrate quantum algorithms and various quantum computing architectures, and with emphasis on potential scalability. While at present certain physical systems can be

identified as prime candidates, it is essential to pursue this goal on a broad basis of competing approaches, allowing hybridization and cross fertilization between different fields (e.g., quantum optics, individual atoms and ions, as well as solid state). In addition, interfaces (with direct relevance for quantum communication) and model systems should be developed for connecting quantum computers in small networks. Parallel to these developments special purpose quantum computers with a few tens of qubits, or more, should be developed, e.g. to act as quantum simulators. The ultimate goal is to construct laboratory models of quantum computers which outperform classical computers on whatever nontrivial problem.

- **Quantum communication**: in quantum communication, the short-term goal is to develop quantum cryptography towards becoming an established technology and a commercial product. A scientific goal is to demonstrate long-distance quantum communication both in optical fiber and in free space. On the 5–10 year time scale, the goals are to gain several orders of magnitude on the secret bit rate and to demonstrate quantum repeaters. The latter will require the implementation of error correction, entanglement purification, quantum interfaces and quantum memories. Each of the mentioned four requirements constitutes a serious scientific challenge. In particular, the main challenge will be the development of a quantum memory that outperforms the simple, but insufficient, "photon in a fiber loop" technique.
- **QIPC theory**: theory must on one hand continue to play a leading role in guiding and supporting experimental developments. On the other hand fundamental theoretical issues must be pursued. The most important one is the formulation of a quantum information theory, a quantum counterpart to the classical theory of information, computation and communication. This implies the search for new quantum algorithms, new computational models and architectures, as well as quantum communication and entanglement manipulation protocols. A key element is a deeper understanding of entanglement in quantum theory. This includes the understanding of decoherence (an intrinsic property of quantum systems interacting with their environment), which leads to the detrimental effects of imperfections and noise. It is necessary to find ways to overcome them, for example with quantum error correction and purification. It will lead both to a deeper understanding of quantum theory per se, but it is also in direct connection to experimental implementations. Finally, the links of quantum information theory to other branches of physics must be developed, e.g. to condensed matter physics.

It would be very difficult to list extensively all sources of support for the results reviewed here. Beside several national funding programs, a major role in this sense has been played by the Future and Emerging Technologies part of the Information Society Technologies program established by the European Commission under the Sixth Framework Program, which is gratefully acknowledged by all authors of the present paper.

References

1. W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003)
2. V. Scarani, A. Acín, G. Ribordy, N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004)
3. F. Grosshans, G. van Assche, J. Wenger, R. Brouri, N.J. Cerf, P. Grangier, Nature **421**, 238 (2003)
4. A. Beveratos, R. Brouri, T. Gacoin, A. Villing, J.-P. Poizat, P. Grangier, Phys. Rev. Lett. **89**, 187901 (2002); E. Waks, K Inoue, C. Santori, D. Fattal, J. Vuckovic, G. S. Solomon, Y. Yamamoto, Nature **420**, 762 (2002)
5. H. Inamori, N. Lütkenhaus, D. Mayers, e-print `arXiv:quant-ph/0107017`
6. M. Koashi, Phys. Rev. Lett. **93**, 120501 (2004)
7. B.C. Jacobs, T.B. Pittman, J.D. Franson, Phys. Rev. A **66**, 052307 (2002); D. Collins, N. Gisin, H.D. Riedmatten, J. Mod. Opt., **52**, 735 (2005)
8. H.-J. Briegel, W. Dür, J. I. Cirac, P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998)
9. M. Aspelmeyer, T. Jennewein, M. Pfennigbauer, W. Leeb, A. Zeilinger, special issue on 'Quantum Internet Technologies', IEEE J. Sel. Top. Quant. Electr. **9**, 1541 (2003); M. Aspelmeyer, H.R. Böhm, C. Brukner, R. Kaltenbaek, M. Lindenthal, J. Petschinka, T. Jennewein, R. Ursin, P. Walther, A. Zeilinger, M. Pfennigbauer, W.R. Leeb, Final Report, Report within ESA/ESTEC/Contract No. 16358/02/NL/SFe (2003); J.G. Rarity, P.R. Tasper, P.M. Gorman, P. Knight, New J. Phys. **4**, 82.1 (2002); J.E. Nordholt, R. Hughes, G.L. Morgan, C.G. Peterson, C.C. Wipf, Proc. SPIE, Free-Space Laser Commun. Technol. XIV **4635**, 116 (2002)
10. B. Julsgaard, J. Sherson, J.I. Cirac, J. Fiurášek, E.S. Polzik, Nature **432**, 482 (2004)
11. B. Julsgaard, A. Kozhekin, E.S. Polzik, Nature **413**, 400 (2001)
12. J.I. Cirac, P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995)
13. 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`
14. C. Monroe, Nature **416**, 238 (2002)
15. J.I. Cirac, P. Zoller, Physics Today 38-44 (March 2004)
16. T.P. Orlando, *Superconducting approaches to Quantum Information Processing and Quantum Computing*, in A Quantum Information Science and Technology Roadmap, Part 1: Quantum Computation, Version 2.0, Section 6.7 and references therein; available from `http://qist.lanl.gov`
17. D. Estève, *Superconducting qubits*, in Proceedings of the Les Houches 2003 Summer School on Quantum Entanglement and Information Processing, edited by D. Esteve, J.-M. Raimond (Elsevier, 2004)
18. D. Loss, D. DiVincenzo, Phys. Rev. A **57**, 120 (1998)
19. J.M. Elzerman, R. Hanson, L.H. Willems Van Bereven, B. Witkamp, L.M. Vandersypen, L.P. Kouwenhoven, Nature **430**, 431 (2004)

20. M. Kroutvar, Y. Ducommun, D. Heiss, M. Bichler, D. Schuh, G. Abstreiter, J.J. Finley, Nature **432**, 81 (2004)
21. A. Högele, M. Kroner, S. Seidl, K. Karrai, M. Atatüre, J. Dreiser, A. Imamoglu, A. Badolato, B.D. Gerardot, P.M. Petroff e-print arXiv:cond-mat/0410506
22. J.P. Reithmaier, G. Sek, A. Löffler, C. Hofmann, S. Kuhn, S. Reitzenstein, L.V. Kelfysh, V.D. Kulakovskii, T.L. Reinecke, A. Forchel, Nature **432**, 197 (2004)
23. L. Childress, J.M. Taylor, A.S. Sorensen, M.D. Lukin, e-print arXiv:quant-ph/0410123
24. E. Knill, R. Laflamme, G.J. Milburn, Nature **409**, 46 (2001)
25. R. Raussendorf, H.J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001)
26. B. Kane, Nature **393**, 133 (1998)
27. S. Lloyd, C. Hammel, *Unique' qubit approaches to QIP and QC*, in A Quantum Information Science and Technology Roadmap, Part 1: Quantum Computation, Version 2.0, Section 6.8 and references therein; available from http://qist.lanl.gov
28. E. Yablonowitch, H.W. Jiang, H. Kosaka, H.D. Robinson, D.S. Rao, T. Szkopek, Proc. IEEE **91**, 761 (2003)
29. D. Deutsch, Proc. R. Soc. Lond. A **400**, 97 (1985)
30. P.W. Shor, *Algorithms for quantum computation, discrete log and factoring*, FOCS'35, p. 124 (1994)
31. L. Grover, *A fast quantum mechanical algorithm for database search*, STOC'28, p. 212 (1996)
32. H. Buhrman, R. Cleve, J. Watrous, R. de Wolf, Phys. Rev. Lett. **87**, 167902 (2001)
33. L.P. Lamoureux, E. Brainis, D. Amans, J. Barrett, S. Massar, Phys. Rev. Lett. **94**, 050503 (2005)
34. D. Deutsch, Proc. R. Soc. Lond. A **425**, 73 (1989)
35. A. Barenco, C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J.A. Smolin, H. Weinfurter, Phys. Rev. A **52**, 3457 (1995)
36. E. Farhi, J. Goldstone, S. Gutmann, J. Lapan, A. Lundgren, D. Preda, Science **292**, 472 (2001)
37. B. Schumacher, R. Werner, e-print arXiv:quant-ph/0405174
38. R. Raussendorf, H.-J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001)
39. S. Lloyd, Science **273**, 1073 (1996)
40. N. Khaneja, R. Brockett, S.J. Glaser, Phys. Rev. A **63**, 032308 (2001)
41. E. Jané, G. Vidal, W. Dür, P. Zoller, J.I. Cirac, Quant. Inf. Comp. **3**, 15 (2003)
42. C.H. Bennett, J.I. Cirac, M.S. Leifer, D.W. Leung, N. Linden, S. Popescu, G. Vidal, Phys. Rev. A **66**, 012305 (2002)
43. M.A. Nielsen, M.J. Bremner, J.L. Dodd, A.M. Childs, C.M. Dawson, Phys. Rev. A **66**, 022317 (2002)
44. P. Wocjan, D. Janzing, T. Beth, Quant. Inf. Comput. **2**, 117 (2002)
45. A.M. Steane, *General theory of quantum error correction and fault tolerance*, in The physics of quantum information, edited by D. Bouwmeester, A. Ekert, A. Zeilinger (Springer, Berlin, 2000), pp. 242-252
46. J. Preskill, *Fault-tolerant quantum computation*, in Introduction to quantum computation and information, edited by H.K. Lo, S. Popescu, T. Spiller (World Scientific, Singapore, 1998), pp. 213-269
47. C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, W.K. Wootters, Phys. Rev. A **54,** 3824 (1996)
48. D. Deutsch, A. Ekert, R. Josza, C. Macchiavello, S. Popescu, A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996)
49. H.-J. Briegel, W. Dür, J.I. Cirac, P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998)
50. A.M. Steane, Phys. Rev. A **68**, 042322 (2003)
51. E. Knill, e-print arXiv:quant-ph/0410199
52. R.F. Werner, Phys. Rev. A **40**, 4277 (1989)
53. M. Horodecki, P. Horodecki, R. Horodecki, Phys. Lett. A **1**, 223 (1996)
54. C.H. Bennett, H.J. Bernstein, S. Popescu, B. Schumacher, Phys. Rev. A **53**, 2046 (1996)
55. V. Vedral, M.B. Plenio, Phys. Rev. A **57**, 1619 (1998)
56. M.A. Nielsen, Phys. Rev. Lett. **83**, 436 (1999)
57. A recent tutorial review was given by J. Eisert, M.B. Plenio, Int. J. Quant. Inf. **1**, 479 (2003)
58. N. Linden, S. Popescu, B. Schumacher, M. Westmoreland, e-print arXiv:quant-ph/9912039
59. W. Dür, J.I. Cirac, R. Tarrach, Phys. Rev. Lett. **83**, 3562 (1999)
60. V. Coffman, J. Kundu, W.K. Wootters, Phys. Rev. A **61**, 052306 (2000)
61. C.H. Bennett, S. Popescu, D. Rohrlich, J.A. Smolin, A.V. Thapliyal, Phys. Rev. A **63**, 012307 (2001)
62. M. Hein, J. Eisert, H.J. Briegel, Phys. Rev. A **69**, 062311 (2004)
63. C.H. Bennett, G. Brassard, C. Crépeau, M.-H. Skubiszewska, Lect. Notes Comp. Sci. **576**, 351 (1991)
64. S. Holevo, IEEE Trans. Inf. Theory **44**, 269 (1998)
65. C.H. Bennett, P.W. Shor, J.A. Smolin, A.V. Thapliyal,
66. G.G. Amosov, A.S. Holevo, R.F. Werner, Prob. Inf. Transm. **36**, 305 (2000)
67. P.W. Shor, Commun. Math. Phys. **246**, 453 (2004)
68. J. Eisert, M.B. Plenio, Phys. Rev. Lett. **89**, 137902 (2002)
69. W. Dür, H. J. Briegel, Phys. Rev. Lett. **92**, 180403 (2004)
70. A.R.R. Carvalho, F. Mintert, A. Buchleitner, Phys. Rev. Lett. **93**, 230501 (2004)
71. P. Zanardi, M. Rasetti, Phys. Rev. Lett. **79**, 3306 (1999)
72. L. Viola, e-print arXiv:quant-ph/0111167
73. R.F. Werner, M.M. Wolf, Quant. Inf. Comp. **1**, 1 (2001)
74. J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, D. Roberts, Phys. Rev. A **71**, 022101 (2005)
75. I. Kerenidis, R. de Wolf, e-print arXiv:quant-ph/0208062
76. S. Popescu, B. Groisman, S. Massar, e-print arXiv:quant-ph/0407035
77. J.I. Latorre, E. Rico, G. Vidal, Quant. Inf. Comp. **4**, 048 (2004)
78. F. Verstraete, D. Porras, J.I. Cirac, Phys. Rev. Lett. **93**, 227205 (2004)
79. M.B. Plenio, J. Eisert, J. Dreissig, M. Cramer, Entropy, Phys. Rev. Lett. **94**, 060503 (2005)