Quantum Technologies Roadmap

List of contents

1. Introduction

1.1 Quantum Computation

1.2 Quantum Communication

1.3 Quantum Simulation

1.4 Quantum Information Theory

1.5 Quantum Metrology, Sensing and Imaging

1.6 Quantum Control

2. Assessment of current results and outlook on future efforts

2.1.Quantum Computation

2.2 Quantum Communication

2.3 Quantum Simulation

2.4 Quantum Information Theory

2.5 Quantum Metrology, Sensing and Imaging

2.6 Quantum Control

1. Introduction

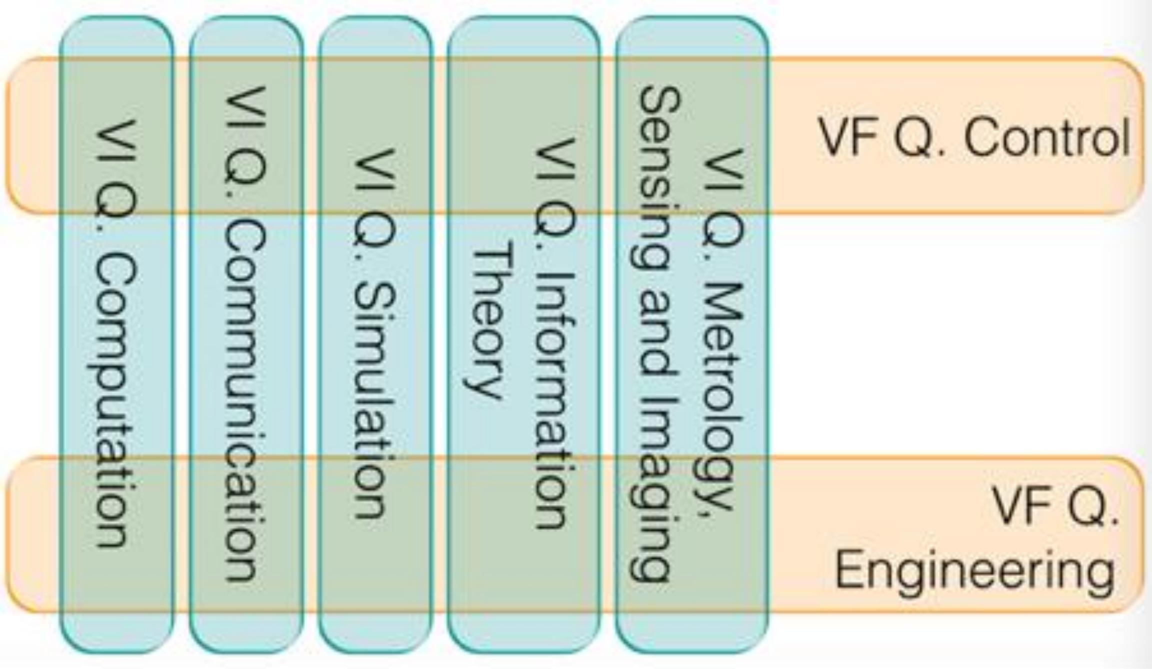
Quantum Information Science (QIS) concerns the study, control and manipulation of quantum systems with the goal of achieving information processing and communication beyond the limits of the classical world. It is a deeply interdisciplinary field, lying in the cross-over of areas such as quantum physics, condensed matter physics, computer science, mathematics or electrical engineering. Having a genesis that can be traced back to the origins of quantum theory itself — with the discovery of genuinely quantum features as quantum entanglement— the field of QIS is nowadays a well-established one. It has been successful not only at understanding the peculiarities of quantum theory and the deep connection between information processing capabilities and physical support at a theoretical level; it also brought technology to a new and broader physical framework, providing fundamentally new capabilities. And in fact, these quantum technologies offer much more than cramming more and more bits to silicon and multiplying the clock–speed of the ubiquitous microprocessors. They support entirely new modes of computation with qualitatively new and powerful algorithms based on quantum principles —that do not have any classical analogues—, they offer provably secure communications, simulation capabilities unattainable with classical processors, sensors and clocks with unprecedented sensitivity and accuracy, or the pioneering generation of certified genuine randomness. Although established, Quantum Information Science is still a fluid creative field with emerging new directions. Examples are the novel applications on the fields of quantum gravity, quantum chemistry and even biology.

Europe is a longstanding and essential contributor for the development of QIS as an whole, with European research institutions playing a leading role at providing many of the ground-breaking results of the field, both at the theoretical, experimental and industry spin-off level.

This document comprises the 2015 edition of the European roadmap for Quantum Information Processing and Communication. Its purpose is to serve as a scientific document that gathers the major achievements and state-of-the-art of the different areas of QIS at this moment in time, as well as the challenges and short-, mid- and long- term goals tracing (possible) routes for the future development of the field.

As in previous editions, this roadmap is organised according to the framework for interaction and coordination of the scientific branches of the EU research community on quantum technologies. The recent growth of the QIS field has triggered the expansion of the previous three scientific branches —represented by Virtual Institutes (VIs)— into a set of five VIs and two Virtual Facilities (VFs). The VIs are application oriented: the Virtual Institute of Quantum Communication, the Virtual Institute of Quantum Computation, the Virtual Institute of Quantum Information Theory, the Virtual Institute of Quantum Simulation and the Virtual Institute of Quantum Metrology, Sensing, and Imaging. The VFs have a horizontal character and provide tools and techniques to enable the work at the different VIs.

As mentioned, there are two VFs : the Virtual Facility of Quantum Control and the Virtual Facility of Quantum Engineering. Each VI and VF unites some prominent experts in the corresponding field, providing a contact point for consultation and feedback in the relevant areas. These different bodies have partially overlapping research agendas to facilitate close collaborations, complementing rather than duplicating each other.



Coordinator	A. Acin

Virtual Institute	**Computation**	**Simulation**	**Communication**	**Sensing**	**Theory**
Director	D. Esteve	I. Bloch	N. Gisin	I. Walmsley	I. Cirac
Executive Secretary	A. Wallraff	S. Kuhr	R. Thew	F. Jelezko	M. Wolf
Members	R. Blatt	J. Bloch	P. Grangier	M. Plenio	H. Buhrman
	D. DiVincenzo	J. Eisert	R. Renner	E. Polzik	M. Troyer
	D. Loss	M. Inguscio	G. Ribordy	J. Wrachtrup	S. Wehner
	P. Zoller	M. Lewenstein	A. Shields	K. Banaszek	R. Werner
		L. Vandersypen	R. Ursin		A. Winter

Virtual Facility	**Engineering**	**Control**
Director	C. Marcus	S. Glaser
Executive Secretary	J. Morton	F. Wilhelm

The present version roadmap is structured around the seven areas and has been prepared in collaboration with the Directors and Executive Secretaries of all the VIs and VFs. For each of the areas, it describes the main objectives, the state-of-the-art, future challenges and short-, mid- and long- term goals. In section 1.1, one can find a summary of these contents for every VI/VF; a more detailed and technical description is found in chapter 2, along with the list of needs each Virtual Institute has on the areas covered by the supporting Virtual Facilities. The organisation of chapter 2 follows a general structure, which is although flexible enough to accommodate the specific needs of each VI/VF.

1.1 Quantum Computation

A quantum computer is a device that harnesses some of the basic laws of quantum mechanics in order to solve problems in more efficient ways than classical (standard) computers. The main objective in the field of quantum computation is to build such a device. Other objectives include the development of quantum algorithms to solve specific problems, and the creation of interfaces between quantum computers and communication systems. The construction of a quantum computer with thousands of quantum bits would have tremendous consequences on the security in communications (like the internet), by breaking most of everyday used cryptography. It would also allow us to solve certain problems that the most powerful super computers are not able to solve now or in the near future, and possibly never; in particular, those dealing with quantum many-body systems, as they appear in different fields of physics, chemistry, and material science.

We already know that the basic principles of quantum computation are correct and there is no fundamental obstacle in constructing such a powerful machine. The basic building blocks of a quantum computer have been demonstrated with many different technologies, including trapped ions, neutral atoms, photons, NV-centres in diamonds, quantum dots, and superconducting devices. Small prototypes have been built using some of those technologies, and some of the quantum algorithms have been demonstrated. The most advanced technologies at the moment are trapped ions and superconducting qubits. With the first one, coherent control has been achieved with up to 15 qubits. Although the control of the latter is still not at the level of the first, it has the potentiality of being scaled up much more easily. With both technologies, proof-of-principle experiments on quantum error correction have been carried out.

Despite the strong efforts devoted by many scientists during the last years, the objective of building a quantum computer remains as a central challenge in science. The main obstacle to build a quantum computer is the presence of decoherence, i.e., undesired interactions between the computer’s constituents and the environment. Standard isolation is not a valid solution, since it seems impossible to reach the levels of isolation that are required in large computations. Therefore, the construction of such a device will require the use of quantum error correction techniques. It is not clear, however, which (already or not yet existing) technology will be optimally suited for the implementation of such techniques in a scalable way and/or in distributed settings. On a different note, we only know a limited class of problems where a quantum computer could overcome the limitations of classical ones, and thus theoretical studies for applications of such devices need to be further pursued.

Some specific future directions of research include:

1. Further development of all current technologies to understand their limitations and find ways around them.
2. Assessment of the capabilities of different technologies for being scaled up.

3. Optimisation of the performance of error correcting codes, by both increasing the error threshold and decreasing the overhead of required qubits.
4. Investigation of new ways of performing quantum computation, in particular based on self-correcting codes (as they appear in topological systems).
5. Development of new quantum algorithms and search for problems where quantum computers will be required.
6. Development of quantum complexity theory and its application to many body physics.
7. Building interfaces between quantum computers and communication systems.
8. Development of quantum-proof cryptography to achieve forward-in-time security against possible future decryption (by quantum computers) of encrypted stored data.

1.2 Quantum Communication

Quantum Communication is the art of transferring quantum states from one place to another. The general idea is that quantum states encode quantum information: hence quantum communication also implies transmission of quantum information and the distribution of quantum resources such as entanglement. Quantum Communication covers aspects ranging from basic physics to practical applications that are relevant to society today. From an application point of view, a major interest has been focused on Quantum Key Distribution (QKD), as this offers a provably secure way to establish a confidential key between distributed partners. This has the potential to solve long-standing and central security issues in our information based society as well as emerging problems associated with long term secure storage (e.g. for health records and infrastructure) and will be critical for the secure operation of applications involving the Internet of Things (IoT) and cloud networking.

In the last years the field has seen enormous progress, as QKD systems have gone from table-top experiments to compact and autonomous systems and now a growing commercial market. More generally there has been an explosion in the number of groups active in the field working on increasingly diverse physical systems. Quantum memories and interfaces have moved from theory to a wide range of proof-of-principle demonstrations with encouraging results for the future. Conceptually, the idea of device independent quantum information processing made its appearance and has already started to find experimentally feasible applications.

Quantum cryptography is now developing from the initial point-to-point QKD systems, towards the management of quantum-based security over many-node networks that are running in various places worldwide. Presently, technical problems are controlled well enough so that secure transmissions over a few hundred kilometres can be implemented. Indeed, in recent years, we have seen free space quantum communication over 144km and fibre demonstrations over 300km. However, non-trivial problems emerge for really long-distance communication (hundreds to thousand of kilometres), and in the quest for higher bit rates. If Quantum Communication is to become, on the 5 to 10-year time-scale, an established technology backing up the quantum cryptography “boxes” which are already commercialised, several scientific as well as technological gaps have to be filled.

In particular, when demonstrating the feasibility of ‘real world’ quantum communication beyond a few hundred kilometres, Trusted-Node backbone and access network architectures that chain together many QKD links, will facilitate the commercial impact of QKD. Low-cost devices for access networks and even hand-held devices, exploiting integrated photonic technologies, are already under development. Achieving these goals will require facing a number of non-trivial challenges, needing very strong interaction between fundamental and applied research as well as quantum and conventional cryptographers. In the long-term, quantum repeater technologies, based on quantum memories will be required. This effort spans fundamental research to pure engineering challenges and will need to build on the trusted-node networks that are already taking shape.

Quantum Random Number Generators (QRNG) are one of the most fundamentally fascinating and practically useful quantum technology applications with a direct application in QKD systems. Our information-based society consumes a lot of random numbers for a wide range of applications, e.g., cryptography, PINs, lotteries, numerical simulations, etc. The production of random numbers at high rates is technically challenging; at the same time, given the pervasiveness of the deployment of random numbers, poor random number generators can be economically very damaging. Importantly, from a commercial perspective, higher rate and lower cost approaches continue to be demonstrated. For example, recently it has been shown that the camera in mobile phones can be used as a QRNG, opening the door to potentially massive commercial opportunities.

These quantum communication applications are also reliant on a wide range of component technologies: photon sources, detectors, quantum memories, and (frequency conversion) interfaces for connecting disparate systems. The long-term success of quantum communication is reliant on pursuing both the immediate need for commercial ready QRNGs and QKD systems and demonstrating their operation in real-world networks, but also for the next generation of devices and systems for a quantum-safe European digital infrastructure.

Some grand challenges for research include:

1. Exploit quantum integrated photonics for cheaper and faster devices (QRNG) and systems (QKD) with increased robustness and functionality.
2. Significantly advance performance characterisitics of all component technologies: photon sources; interfaces; quantum memories, and detectors.
3. Demonstration of practical, autonomous, systems capable of performing continuous secure key distribution > 100 Mbps rates, e.g. over MAN distances
4. Create a quantum-safe secure backbone and access networks connecting the major cities in Europe, exploiting trusted-node technologies.
5. Develop the core technologies and new protocols for quantum repeaters that work with cryptographic capabilities and eavesdropping detection, enabling long-distance end-to-end quantum-secure links.
6. Bring quantum and classical cryptographers together to develop new algorithms, protocols and applications, like quantum credit cards, quantum money and quantum keys.
7. Develop protocols for the security of long-lived systems and secret sharing exploiting quantum and classical cryptographic techniques.
8. Practical device-independent-inspired protocols with explicit assumptions about security analysis and fully composable security within a quantum network.
9. Standards and certification for QKD systems, component devices (QRNG) and protocols, included integration in standardised telecom blade chassis.

1.3 Quantum Simulation

Despite over a century of research effort, interacting quantum systems still provide some of the most profound and intriguing challenges to our understanding of systems in Nature. Some systems of quantum chemistry of already a moderately large number of constituents can already be no longer tackled on classical supercomputers. Similarly, many interacting condensed-matter systems are still posing open questions when it comes to predicting their properties. A paradigmatic example of this type is high-Tc superconductivity of cuprates, where it is believed that the basic physics is largely captured by an array of weakly coupled 2D Hubbard models for electrons, i.e. spin-½ fermions. Even a simplified paradigmatic version confined to a 2D plane does not allow for an accurate treatment, leading to controversy, e.g., on the precise phase diagram or the character of the transitions. Classical supercomputers cannot accurately solve or simulate such interacting many-body system in all generality, simply because the scaling of the effort in the system size is daunting.

In the last decades, such problems relating to the behavior of interacting quantum many-body systems were heavily studied with supercomputers, making use of the fact that the available computing power has increased rapidly. Despite enormous successes, there are significant limitations when it comes to the simulation of quantum dynamics on classical computers, due to the very unfavorable scaling of resources with system size required to perform certain kinds of classical simulations of static or dynamical quantum properties, putting them out of reach even of supercomputers.

Quantum computers promise to overcome these limitations and thus to gain an understanding of the physical world at the microscopic level that seems unattainable using numerical simulations on classical computers. Alas, in the foreseeable future, these devices are unlikely to be realized on a scale that would actually be useful for practical purposes. While state-of-the art experiments are already capable of preparing and controlling large ensembles of atoms, the application of arbitrary unitary gates, which would be needed for a quantum computer, seems very challenging even from a conceptual point of view. This leads to the more pragmatic approach of embracing the experimental limitations and still using the experiment to solve problems that are completely out of the reach of classical simulations. This more realistic and ambitious approach gives rise to the concept of a quantum simulator.

Quantum simulation builds upon a long tradition of simulation in the classical realm: The 20th century can be seen as the age of information and computers. But, even supercomputers have their limitations. For this reasons already in classical computer science the concept of special purpose computers has been developed. Such “classical simulators” are unlike universal classical computers – they can only simulate or calculate certain restricted class of models describing Nature. For example, the best simulations of classical disordered systems, such as spin glasses, are nowadays obtained with such computers of special purpose - “classical simulators”. Similarly, the simulation of the aerodynamics of cars in a wind tunnel can be seen as a classical special purpose computation in this sense.

The basic idea of a quantum simulator is both ingenious and rather simple: Instead of trying to simulate quantum dynamics on standard computers, one intentionally and artificially reproduces the quantum dynamics on another quantum system, under precisely controlled conditions in the laboratory. This approach allows for reproducing known physical systems in a setting where a plethora of different ways of probing and measuring the system is available, for example by emulating a solid state system on a much larger length scale, such that optical resolution of individual atoms can be achieved.

The basic idea of a quantum simulator is due to Feynman, who not only “invented” the concept in a keynote speech. He also addressed rather subtle issues of the mutual efficient inter-convertibility of different quantum systems, anticipating a scientific discussion about the precise validity in quantum mechanics of the Church Turing thesis, which captures how well computer architectures can simulate each other. Yet, it is only now, with experimental procedures having progressed to an extent that such controlled quantum many-body dynamics is really conceivable that quantum simulation has developed into a burgeoning field of research. By now, many realistic experimental candidate systems exist, which already demonstrated their potential to truly outperform classical computers. These include for example ultra-cold atoms in optical lattices, ultra-cold trapped ions, atoms in arrays of cavities, ultra-cold atoms near nano-structures, arrays of quantum dots, superconducting circuits, photons in linear optics devices, as well as photons/polaritons in arrays of cavities.

1.4 Quantum Information Theory

Our conception of what a computation is has been altered drastically during history, since the times of Leibniz, Babbage and Turing. The result of this remarkable history of ideas – computers as we know them today – has changed our modern society significantly. Yet, the development of computing and communication devices has not come to a stop. Recent developments have shown, in fact, that we are at the beginning of a new era of harnessing the laws of nature, using quantum physics for unprecedented and very powerful ways of information processing. The development of Quantum Information Theory (QIT) has been driven by theoretical work of scientists working on the boundary between Physics, Computer Science, Mathematics, and Information Theory.

In the early stages of this development, theoretical work has often been far ahead of experimental realization of these ideas. At the same time, theory has provided a number of proposals of how to implement basic ideas and concepts from quantum information in specific physical systems. These ideas are now forming the basis for successful experimental work in the laboratory, driving forward the development of tools that will in turn form the basis for all future technologies which employ, control and manipulate matter and radiation at the quantum level.

While the development of QIT has started as early as in the 80's, the field has gained significant momentum in the last decades. Major triggers were the discovery of fast quantum algorithms and the identification of concrete physical systems in which a quantum computer could be realized. In the meantime, a broad spectrum of research activities can be observed, ranging from the study of fundamental concepts such as quantum entanglement, to novel applications such as quantum simulators, and with significant spin-off also to other fields of research.

In many of these activities, European research has played a leading role and has established a strong set of world leading centers. It is important to realize that theoretical activities are often interdisciplinary in nature and span a broad spectrum of research in which the different activities are benefiting from each other to a large degree. Thus it does not seem to be advisable to concentrate research on too narrowly defined topics only. The following list nevertheless tries to highlight the main current areas of quantum information theory as it is described in more detail in the strategic report below.

Quantum algorithms & complexity

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

Computational models & architectures

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

Geometric and topological methods

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

Quantum simulations

Quantum simulators may become the first short-term application of quantum computers, since with modest requirements one may be able to perform simulations that are impossible with classical computers. They could be used for a variety of purposes, e.g., to obtain an accurate description of chemical compounds and reactions, to gain deeper understanding of high temperature superconductivity, or to find out the reason why quarks are always confined.

Quantum error correction & purification

Despite its amazing power, a quantum computer will be a rather fragile device, susceptible to disturbances and errors. Fortunately, methods have been developed to protect such a device against disturbances and imperfections, as long as these are small enough. These methods are constantly being improved and refined, but there is still a lot of work to be done until we can run a quantum computer reliably.

Theory of entanglement

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

Multi-partite entanglement & applications

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

Noisy communication channels

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

Fundamental quantum mechanics and decoherence

Quantum information was born, in part, via research on the famous Einstein-Podolski-Rosen paradox and the issue of quantum non-locality. It is now understood that non-locality is one of the central aspects of quantum mechanics. More generally, quantum information profits substantially from studying the fundamental aspects of quantum mechanics and, at the same time, it yields new perspectives, raising hopes of gaining a deeper understanding of the very basis of quantum mechanics. In particular, quantum information theory can provide deeper understanding of dynamics of open quantum systems.

Spin-off to other fields

A very exciting aspect of theoretical work in QIT is the impact that it is beginning to gain on other fields of science. Examples are given by the theory of classical computing, by field theory, thermodynamics, quantum gravity and in particular by condensed matter physics. Many of the questions that are now being asked in this area can only be answered or even formulated correctly because of the many insights and techniques gained in the research in entanglement theory in recent years.

1.5 Quantum metrology, sensing and imaging

Specific quantum phenomena such as coherence and entanglement can be exploited to develop new modes of measurements, sensing, and imaging that offer unprecedented levels of precision, spatial and temporal resolution, and possibly auto-compensation against certain environmental factors, such as dispersion. These promising applications require development of techniques robust to noise and imperfections, i.e., fit to real-world scenarios. Quantum technologies will benefit, in particular, time and frequency standards, light-based calibration, gravitometry, magnetometry, accelerometry, including the prospects of offering new medical diagnostic tools.

Reaching quantum-enhanced precision beyond standard quantum limits in metrology relies on generating non-classical collective states of atoms and non-classical multi-photon states of light. Extensive effort has been dedicated to these goals with proof-of-principle demonstrations in the atomic domain and the first squeezed-light-enhanced operation of a gravitational wave detector with practical suppression of vacuum fluctuations. Novel concepts, such as systems with an effective negative mass or negative frequency have been shown to be capable of providing magnetometry with virtually unlimited sensitivity. Possibilities to define new frequency standards have been explored with the readout based on quantum logic techniques borrowed directly from the field of quantum computing and with entangled atoms providing ultimate quantum sensitivity. Enormous progress has been made on single photon sources, both deterministic and heralded, that can be used for optical calibration as well as a building block for photonic quantum communication and computing. Artificial atoms (such as nitrogen vacancy centres) have been investigated as ultra-precise sensors e.g. in magnetometry.

Original techniques are needed to make quantum-enhanced metrology and sensing deployable in non-laboratory environments. Because of the wide range of prospective applications and their specificity, a broad range of physical platforms needs to be considered, including (but not limited to) trapped ions, ultra-cold atoms and room-temperature atomic vapours, artificial systems such as quantum dots and defect centres, as well as all-optical set-ups based e.g. on nonlinear optical interactions. Thorough theoretical analysis of noise mechanisms is needed, leading to feasible proposals that will be subsequently implemented to realise quantum-enhanced strategies.

In particular the following points need to be addressed:

1. Novel sources of non-classical radiation and methods to engineer quantum states of matter are required to attain quantum-enhanced operation;
2. Develop detection schemes that are optimised with respect to extracting relevant information from physical systems, with optimisation criteria selected for specific applications. These techniques may find applications in other photonic technologies, e.g. increasing transmission rates in optical communication;

3. Micro- and nano-fabrication of quantum sensors including integration with fiber networks;
4. Development of hybrid quantum sensors that use optimal quantum interfaces for transduction of signals across the electromagnetic radiation spectrum;
5. Compact solutions for quantum imaging, allowing for the interconversion of detected frequencies including preservation of coherence, as well as quantum ranging and timing that can suppress the spatial/temporal spread of transmitted signals;
6. Implementation of entanglement assisted atom clocks;
7. Study of the performance of quantum sensing protocols in realistic regimes including noise and losses;
8. Extend the reach of quantum sensing and metrology into other fields of science to uncover novel natural phenomena, e.g. biology, fundamental physics, high-energy physics, quantum gravity.

1.6 Quantum Control

Control turns scientific knowledge into technology. The objective of quantum control is to devise and implement control by tailoring external fields such that the dynamics of the quantum system realises a given task in the best possible way. Tasks include the preparation of useful quantum states as well as implementation of complete quantum operations. Success of control is measured by a suitable fidelity and the search accounts for laboratory/experimental/physical constraints on pulse feasibility, energy etc. Quantum control links the goals of quantum technologies with hardware platforms. By taking into account hardware imperfections it helps both to overcome them and to identify the performance limits set by these imperfections.

Quantum control is applied in areas as diverse as quantum information processing, spectroscopy in almost every frequency regime from RF in NMR, microwave to the optical range in quantum information, and recently for EUV and XUV radiation. It is part of the current effort to engineer quantum technologies from the bottom up. Recent achievements include measurement with quantum limited sensitivity of nanoscale magnetic fields with a single nitrogen-vacancy centre; creation of entangled spin states in diamond for quantum memories and networks; state engineering of a Bose-Einstein condensate for quantum sensing; and implementation of precise quantum gates in a superconducting quantum processor.

Quantum-enabled technologies will be based on quantum interference and entanglement. Quantum optimal control will be crucial to reach the precision of operations required for quantum technologies within given constraints of time and power. This statement is based on the established experience that quantum optimal control allows to improve the relevant figure of merit by one to two orders of magnitude without requiring any other changes. Quantum control is thus the tool of choice to enable tasks that have been tackled with limited success but could not yet be realised to the desired fidelity/accuracy with more standard approaches. This improvement will make the decisive difference in reaching the next level in the process of taking quantum technologies from proof-of-principle demonstrations to real applications.

New goals include:

1. Develop applications to quantum communication and information security - frequency conversion, quantum repeaters, and non-traditional transmission lines.
2. Fully understand control of open systems, including use of dissipation to assist in coherent control, e.g. for the initialisation of many-body quantum simulators.
3. Develop methods to confine dynamics in controllable decoherence-free subspaces.
4. Broaden the base of physical systems quantum control is applied on.

5. Explore controlled quantum systems enabled by quantum control - ultracold chemistry as a tool for quantum engineering and spectroscopy with novel light sources as a new approach to e.g. imaging of many-body quantum dynamics.
6. Develop versatile, robust and platform-independent control technology that can be readily adapted to and implemented in quantum simulation.

2. Assessment of current results and outlook on future efforts

2.1 Quantum Computation

Quantum mechanics resources for computation

In order to perform computing in a classical machine with a von Neumann architecture, information takes the form of registers of bits with values 0 or 1, stored in electronic elements using electric charges, currents, magnetisation, etc, and processed using logic gates. In the case of Quantum Computing, and more generally Quantum Information Processing (QIP), one manipulates quantum registers storing N quantum bit (qubit) states (|0> and |1>) built usually from atomic, optical, or electronic systems. The register is now a Hilbert space spanned by the 2^N basis states $|01, \dots, 0N>, \dots, |11, \dots, 1N>$. It has been proven in the beginning of the 1990s that the richness of quantum systems provides enough resources for performing computational tasks beyond the reach of classical computers. The complexity classes of computational problems (defined for a classical Turing machine) get scrambled for quantum hardware, meaning that some problems considered before as hard become tractable on a quantum Turing machine.

The most standard quantum computation model is the quantum equivalent of the classical circuit model. For such quantum 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 realised by a controllable quantum system, provided the physical system meets the following requirements (DiVincenzo criteria):

1. System is comprised of well characterised qubits and allows for scalability;
2. Ability to initialise 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;

Various systems are nowadays used for implementing quantum processors, all-optical devices, trapped ions and neutral atoms, cavity quantum electrodynamics (CQED) systems and the closely related circuit QED (cQED), superconducting qubit circuits, impurity spins in semiconductors, spins, molecular magnets, etc, plus suitable combinations of all these when possible and helpful. Quite excellent qubits have been obtained experimentally, with a sizeable progress of solid-state qubits during the recent years. However, quantum processors based on the unitary evolution of a qubit register have only been able to demonstrate very elementary instances of quantum algorithms or protocols. The main reason is that they face the so-called scalability wall, which comprises integrating a large number of qubits, correcting quantum errors during their processing with gates, and achieving high fidelity readout. Different fault-tolerant architectures are now developed for addressing these scalability issues, but none has yet been demonstrated on a scale large enough for making a quantum computer.

Other routes, noticeably measurement-based quantum computing and adiabatic quantum computing have been proposed. Although they also face scalability issues, the nature of the challenges to overcome is different. The recent significant implication of large companies such as Google, Intel, Microsoft and IBM in academic or academic-like labs is nevertheless a clear sign that achieving QC is seriously considered. The recent sale by D-Wave of a few machines implementing adiabatic quantum computing, or at least some form of quantum assisted annealing, also shows that quantum computing is seriously considered as a possible alternative for performing high performance computing in the future. Quantum simulation follows a different route, and is treated in this roadmap in a separate section, which shows its growing interest.

Few-qubit test-beds

Operating few-qubit devices provides a test bed for all functions of a quantum computer. Achieving the full error-correction of a qubit, i.e. maintaining it alive in despite decoherence, is a Holy Grail now within reach. Implementing algorithms or protocols piling a huge number of gates while maintaining an excellent fidelity, and achieving high-fidelity readout of large registers, is also within reach of different implementations. Although a small quantum processor does not make a useful quantum computer, it is a mandatory intermediate step for probing concepts. It may also provide an operational platform for quantum simulation.

Toward scalable architectures for the gate model

Performing the unitary evolution of about 100 logical qubits, i.e. fitted with quantum error correction, is needed for overcoming present-day classical processors. This number clearly requests the development of a scalable architecture combining all the needed functionalities. The different strategies suited to the different implementations will have to be implemented and probed. All of them imply some redundancy for making robust logical qubits. For trapped ions, making 2D traps seems to be necessary; for superconducting qubits, the surface code architecture that requires a full square array of qubits provides a fault-tolerant solution, but with a very large overhead in terms of physical resources. Specific architectures taking benefit of the peculiarities of each system will have to be developed.

Alternative QC architectures

Given the difficulty to implement fault-tolerant architectures in gate-based processors, an in-depth investigation of other routes is needed. In Measurement-Based Quantum Computing, one prepares an initial entangled state of a qubit register, often a cluster state, which provides the resource needed for computing. One then applies simple gates, followed by single qubit readout operations. Although quantum error correction still is an issue, it takes a different form, possibly easier to implement practically. Furthermore, this strategy is definitively better suited for some implementations such as the linear optics quantum computer. Here, the initial state is based on Bell states and/or single photon sources that can now be produced with high fidelity.

In Adiabatic Quantum Computing (AQC), one follows the evolution of the ground state of an ensemble of interacting qubits when its Hamiltonian adiabatically evolves from a trivial one to a more subtle one, whose ground state encodes the solution of a searched problem up to a polynomial cost transformation. Although it is thought that D-Wave machines may not implement full AQC, understanding the effect of decoherence and thermal excitation on their performance is presently a major issue. Note that these machines already solve non-trivial problems beyond the reach of existing gate-based quantum processors for which quantum speed-up was demonstrated on elementary instances of quantum algorithms. This architecture is also attracting a huge interest because it suits well optimisation problems in general and machine learning.

Making more robust qubits

In parallel to the development of scalable architectures for existing qubits, other types of qubits with better performance in terms of quantum coherence will be investigated. Among them, the new type of spin qubit in nuclear-spin free silicon is opening an appealing route for which a full processor architecture is however still missing. Note that the possible compatibility of these qubits with the fabrication methods of the microelectronics industry presents a major interest.

Quantum interfaces

Whatever the quantum computer architecture that makes it, establishing remote quantum connections between units will be necessary. Given the only solution foreseen being the transmission of telecom photons, establishing quantum interfaces between qubits in computing units and optical quantum communication channels is a major issue, closely related to the repeater node problem in quantum communications. Here, a joint effort of all QIP communities is requested, from quantum optics and atomic physics to solid-state devices.

More theory needed

Although the theoretical corpus of QIP is already sizeable, an important effort is still needed. The questions below just give a flavour of some of the numerous issues to be addressed. On the algorithmic side, the range of real problems for which QC truly provides a winning advantage is not well identified, and the match between problems and existing architectures is not understood. On the architecture side, one has to find the fault-tolerant schemes best suited to each architecture, and that allow experimentalists to perform computing tasks as advanced as possible given existing imperfections. This points to a closer synergy between theory and experience that Europe could help to build, and that could be key to the development of a functional quantum computer.

2.1.1 Trapped ions

A. Physical approach and perspectives

Ion trap quantum computing typically operates on a qubit register formed by a linear string of ions confined in a Paul trap. Each physical qubit is based on two internal levels of a single ion; these levels are either defined within a Zeeman or hyperfine manifold or correspond to a forbidden optical transition. Single-qubit operations use microwave or laser fields, while two-qubit operations in most experiments employ laser fields [1]. Although the trapped-ion approach for quantum computing fulfills in principle all the DiVincenzo criteria, most of which have already been demonstrated experimentally, scaling up to large number of qubits remains an open challenge [2]. Important efforts have been devoted to the development of micro-fabricated traps, which should allow for a scalable implementation, but technical and materials science issues remain. As a medium-term goal, quantum simulation experiments with strings of ions in Paul traps and 2D arrays in Penning traps are being pursued with the goal of turning the ions into an interacting quantum-many body system [3].

B. State-of-the-art

The DiVincenzo criteria are currently met as follows:

1. Quantum algorithms have been performed on strings of up to seven ions confined in a linear trap [4]. Longer chains of up to 20 ions and 2D crystals of up to ~300 ions have been trapped and used for quantum state engineering [5] or quantum simulation [6-8]. Scaling an ion trap quantum processor to a much larger number of qubits, together with the necessary trapping and control hardware is in principle feasible. However, such a large-scale device is currently beyond reach, and the status of the first DiVincenzo criterion is still uncertain.
2. Ion strings are cooled to the ground state of the trapping potential, and the qubit register can be initialised with a state preparation error below 10^{-3} for a single qubit [9].
3. For hyperfine qubits, coherence times above 10min have been observed; a coherence time of 50s could be obtained without the use of a magnetic shield [9]. In optical qubits, the coherence time is limited by the decay out of the metastable state, which is, e.g., ~1 s for calcium ions. This is still orders of magnitude longer than the typical two-qubit gate duration ~10 μs.
4. Single-qubit manipulation can now be realised with a gate error $\sim 10^{-6}$ [9], while two-qubit gates have an error as low as $\sim 10^{-3}$ [10]. Two-qubit gates are typically based on laser schemes (Cirac-Zoller gate, conditional phase gate, Mølmer-Sørensen gate), but alternatives relying on microwave fields are being investigated [11, 12]. Ultrafast laser gates have been demonstrated for single ions, with a ~50 ps gate time [13]. The application of this technique to two-qubit gates is ongoing. Gate schemes using Rydberg states of ions are

another possible approach; laser excitation of a trapped ion to Rydberg states has been obtained recently [14].

5. State-dependent light scattering is routinely used for qubit readout; detection errors as low as ~10^{-4} have been reported [15].
6. Conversion from stationary to flying qubits has been demonstrated [16]. The original DiVincenzo criteria assumed that a bidirectional interface would be necessary for quantum information transfer between remote sites. Since then, however, heralded protocols for quantum information transfer have been developed and implemented, e.g., a qubit teleportation protocol between remote trapped ions [17].
7. Quantum information can also be transferred over shorter distances by physically transporting the trapped ions within a quantum processor, which has been realised experimentally with high fidelity [18].

From this list, the one requirement that has not been experimentally demonstrated yet is the scalability. Nevertheless, there are well-defined approaches for scaling up ion trap quantum processors using microfabricated traps and photonic interconnects [2]. These schemes together with the relatively high fidelities obtained for all required quantum operations and the successful implementation of a number of small-scale quantum algorithms make trapped ion systems a possible candidate for large-scale quantum computing.

In recent years, there has been progress towards a scalable implementation. A complete set of methods for scalable quantum computing has been demonstrated [19], including qubit transport and sympathetic laser cooling using a second co-trapped ion species. Repetitive quantum error correction has been realised [20], as well as fault-tolerant topological encoding of a qubit [4]. Scaling of the trap architecture is being investigated very actively; a variety of micro-fabrication techniques and electrode configurations have been devised to that end [21]. A difficulty encountered in miniaturised ion traps is the marked growth of the electric-field noise in the vicinity of trap surfaces, which causes unwanted motional heating. This issue has been addressed in micro-fabricated traps by operating at cryogenic temperatures [22], or by applying an in-situ ion bombardment treatment to the surface of the trap [23]; both approaches provide a reduction of the electric-field noise by about two orders of magnitude. However, an understanding of the physical mechanisms responsible for this noise is still lacking [24].

Quantum simulation experiments with linear chains of up to 20 ions have been carried out, realising variable-range Ising interactions including spin frustration [6, 7]. For the simulation of two-dimensional spin models, planar crystals of up to 300 ions in Penning traps are being investigated [8] as well as the creation of microfabricated 2D rf-trap arrays [25]. In addition to the analogue simulation approach, digital simulation of coherent and dissipative processes has been investigated as well.

C. Challenges

Ion trap setups have been a successful platform for the demonstration of small-scale quantum information processing, with long qubit coherence times and high fidelities demonstrated for state preparation, single- and two-qubit gates, and state detection. However, a number of challenges remain on the path to a large-scale quantum processor based on trapped ions:

- The fidelity of two-qubit gates needs further improvement in order to allow for quantum error correction with a manageable overhead in resources. This will require technical improvements, in particular in the intensity stability and switching of laser sources;
- The two-qubit gate time needs to be reduced, perhaps by employing proposed schemes for ultrafast laser gates;
- Although impressive progress has been made, scaling the trap architecture has proven a difficult task. In recent years, elaborate trap layouts have been realised using microfabrication processes [21], and high-fidelity gate operations have been demonstrated on micro-fabricated traps [9, 10]. Still, all the experiments performed so far using micro-fabricated traps have been limited to a small number of ions. The electric-field noise near trap surfaces, which is an obstacle to the miniaturisation of complex ion trap structures, has been reduced by two orders of magnitude [22, 23]; however, further improvements may be necessary for high-fidelity operations in highly miniaturised traps. Furthermore, there have been demonstrations of optics and electronics integration with micro-fabricated ion traps, but further developments are needed for large-scale devices.

D. Short-term goals (0-5 years)

- Improve two-ion gate fidelity to reach the threshold for quantum error correction schemes with low resource overhead;
- Demonstrate ultrafast two-ion gates ($t_{gate} << 1$ μs);
- Improve the fidelity of microwave-based two-ion gates;
- Investigate two-ion gates with Rydberg ions;
- Demonstrate quantum error correction with registers of ~5 qubits;
- Improve characterisation of states and processes for large systems;
- Further reduce the electric-field noise close to trap surfaces, perhaps by combining low-temperature operation and in-situ surface treatment;
- Demonstrate high-fidelity gates in multiple ion registers on a micro-fabricated trap;
- Realise a many-body system with a complexity beyond what can be simulated classically.

E. Medium-term goals (5-10 years)

- Implement repetitive quantum error correction without decoding the quantum information;
- Demonstrate quantum operations with multiple logical qubits;
- Integrate optics and control electronics in a scalable micro-fabricated trap;

- Demonstrate high-fidelity quantum information transport between ion registers on a micro-fabricated trap, and between three or more networked traps;
- Develop verification methods for quantum simulators.

F. Long-term goals (>10 years)

- Maintain the coherence of a logical qubit indefinitely through quantum error correction;
- Demonstrate a large-scale quantum computation system.

G. Key references

[1] R. Blatt and D.J. Wineland, “Entangled states of trapped atomic ions”, Nature 453, 1008 (2008)
[2] C. Monroe and J. Kim, “Scaling the Ion Trap Quantum Processor”, Science 339, 1164 (2013)
[3] R. Blatt and C.F. Roos, “Quantum simulations with trapped ions”, Nature Phys. 8, 277 (2012)
[4] D. Nigg *et al.*, “Quantum computations on a topologically encoded qubit”, Science 345, 302 (2014)
[5] T. Monz *et al.*, “14-Qubit Entanglement: Creation and Coherence”, Phys. Rev. Lett. 106, 130506 (2011)
[6] K. Kim *et al.*, “Quantum simulation of frustrated Ising spins with trapped ions”, Nature 465, 590 (2010)
[7] P. Jurcevic *et al,* “Quasiparticle engineering and entanglement propagation in a quantum many-body system”, Nature 511, 202 (2014)
[8] J.W. Britton *et al.*, “Engineered two-dimensional Ising interactions in a trapped-ion quantum simulator with hundreds of spins” , Nature 484, 489 (2012)
[9] T.P. Harty *et al.*, “High-Fidelity Preparation, Gates, Memory, and Readout of a Trapped-Ion Quantum Bit”, Phys. Rev. Lett. 113, 220501 (2014)
[10] C.J. Ballance *et al.*, “High-fidelity two-qubit quantum logic gates using trapped calcium-43 ions”, arXiv:1406.5473 (2014)
[11] C. Ospelkaus *et al.*, “Microwave quantum logic gates for trapped ions”, Nature 476, 181 (2011)
[12] N. Timoney *et al.*, “Quantum gates and memory using microwave-dressed states”, Nature 476, 185 (2011)
[13] W.C. Campbell *et al.*, “Ultrafast Gates for Single Atomic Qubits”, Phys. Rev. Lett. 105, 090502 (2010)
[14] T. Feldker *et al.*, “Rydberg Excitation of a Single Trapped Ion”, Phys. Rev. Lett. 115, 173001 (2015)
[15] A.H. Myerson *et al.*, “High-Fidelity Readout of Trapped-Ion Qubits”, Phys. Rev. Lett. 100, 200502 (2008)
[16] A. Stute *et al.*, "”, Nature Photon. 7, 219 (2013)
[17] S. Olmschenk *et al.*, “Quantum Teleportation Between Distant Matter Qubits”, Science 323, 486 (2009)
[18] R.B. Blakestad *et al.*, “Quantum-state transfer from an ion to a photon”, Phys. Rev. Lett. 102, 153002 (2009)

[19] J.P. Home *et al.*, “Complete Methods Set for Scalable Ion Trap Quantum Information Processing”, Science 325, 1227 (2009)
[20] P. Schindler *et al.*, “Experimental Repetitive Quantum Error Correction”, Science 332, 1059 (2011)
[21] M.D. Hughes *et al.*, “Microfabricated ion traps”, Contemp. Phys. 52, 505 (2011)
[22] J. Labaziewicz *et al.*, “Suppression of Heating Rates in Cryogenic Surface-Electrode Ion Traps”, Phys. Rev. Lett. 100, 013001 (2008)
[23] D.A. Hite *et al.*, “100-Fold Reduction of Electric-Field Noise in an Ion Trap Cleaned with In Situ Argon-Ion-Beam Bombardment”, Phys. Rev. Lett. 109, 103001 (2012)
[24] M. Brownnutt *et al.*, “Ion-trap measurements of electric-field noise near surfaces”, Rev. Mod. Phys. 87, 1419 (2015)
[25] R.C. Sterling *et al.*, “Fabrication and operation of a two-dimensional ion-trap lattice on a high-voltage microchip”, Nature Commun. 5, 3637 (2014)

2.1.2 Quantum Computing with Linear Optics

A. Physical approach and perspectives

In linear-optical quantum computing (LOQC), interaction between separate photonic qubits is induced by measurement, rather than by direct interaction via nonlinear media as in other approaches to quantum computing. There are two main physical architectures for LOQC: these are based on a proposal by Knill, Laflamme and Milburn [1] — the KLM architecture — and by Raussendorf and Briegel [2] — the one-way quantum computer using cluster states.

KLM allows universal and scalable LOQC using only sources of single photons, linear optics, photon-counting measurements and feed-forward. KLM's seminal work is based on the important findings of Gottesman, Chuang and Nielsen concerning the role of teleportation for universal quantum computing. The physical resources for universal (optical) quantum computation in the KLM scheme are multi-particle entangled states and (entangling) multi-particle projective measurements.

The cluster-state approach to LOQC exploits measurement-based quantum-computing schemes with photons as physical qubits. In this approach, quantum algorithms are implemented by a series of adaptive single-qubit rotations and measurements on a cluster state, which is a highly entangled multi-particle state. A series of theoretical proposals have shown that the cluster-state approach can achieve several orders of magnitude reductions in overall complexity compared to KLM, vastly relaxing the demands on physical implementation of LOQC [3,4,5].

B. State-of-the-art

Although a full performant quantum computer is yet a (probably) long -term goal, important steps have already been taken in its direction. The control of large entangled states has been achieved [6, 7], which we have seen is an essential resource for some models of computation. Small-scale algorithms have been demonstrated experimentally [8-10], including on more alternative computational models based on quantum walks [11] or boson sampling [12-14]. Different single-photon sources have been obtained, either based on parametric down-conversion (bright [15] and heralded [16,17] sources) or based on quantum dots (bright [19] and suitable for highly-indistinguishable photons [18]). Also several chip-based quantum photonics systems are already available, namely reconfigurable integrated waveguide devices [20] and integration of photon sources and waveguide circuits together on-chips [21]. Finally, single-photon detectors have seen a significant technological advance: waveguide superconducting nanowire detectors [22,23], interference and detection on chip [25] and quantum-dot source and photon detection on chip [26]. The highest reported efficiency has been attained in [24].

C. Challenges

- Developing complete architectures for LOQC and finding hard bounds on the required performance of photonic components;
- Investing in source and detector technologies: the development of high-flux sources of single and entangled photons, as well as photon-number resolving detectors;
- Capability to generate high-fidelity, large multi-photon entangled states. This will be of crucial importance for generating large resources states for cluster-state quantum computing;
- Developing a complete hardware platform with integration of the generation, manipulation, and detection of photons on integrated photonic circuits;
- Efficient classical control of massive error-corrected quantum circuitry on nanosecond timescales.

D. Short-term goals (0-5 years)

Goals for theoretical work on LOQC

- Improved physical models of quantum photonic components (e.g. quantum dots) in photonics structures;
- Improved error-correction algorithms based on experimental device characteristics;
- Hard limits for hardware performance for experimentalists;
- Efficient methods to characterise large, lossy, entangled photonic systems;
- Useful quantum protocols for small-scale LOQC (e.g. applications of Boson Sampling);
- New protocols (e.g. finding optimal optical networks).

Goals for experimental work

- 6-8 photon experiments without post-selection;
- Integration of sources with low-loss circuits;
- Implementation of active feed-forward on chip;
- High-efficiency high-yield detectors;
- Sufficiently good quantum memory/buffers based on theoretical requirements.

E. Medium-term goals (5-10 years)

- Transition to control of quantum interference with ten's of photons;
- Demonstration of boson sampling beyond practical classical computation limits;
- Circuits with quantum repeaters beating direct transmission rates;
- Demonstration of full tunability of integrated devices;
- Demonstration of small-scale quantum computation below-threshold for fault-tolerant operation.

F. Long-term goals (>10 years)

- Demonstration of large-scale quantum computation below-threshold for fault-tolerant operation.
- Integration of control and full-systems engineering.

G. Key references

[1] E. Knill, R. Laflamme, G. J. Milburn, "A scheme for efficient quantum computation with linear optics", Nature 409, 46 (2001).
[2] R. Raussendorf, H. J. Briegel, "A one-way quantum computer'', Phys. Rev. Lett. 86, 5188 (2001).
[3] M. A. Nielsen, "Optical Quantum Computation Using Cluster States", Phys. Rev. Lett. 93, 040503 (2004).
[4] D. E. Browne and T. Rudolph, Resource-Efficient Linear Optical Quantum Computation, Phys. Rev. Lett. 95, 010501 (2005).
[5] M. Gimeno-Segovia, P. Shadbolt, D. E. Browne, T. Rudolph, "From Three-Photon Greenberger-Horne-Zeilinger States to Ballistic Universal Quantum Computation", Phys. Rev. Lett. 115, 020502 (2015).
[6] C. Lu et al., "Experimental entanglement of six photons in graph states", Nature Phys. 3, 91 (2007).
[7] Gao et al., "Experimental demonstration of a hyper-entangled ten-qubit Schrödinger cat state", Nature Phys. 6, 331 (2010).
[8] R. Kaltenbaek, J. Lavoie, B. Zeng, S. D. Bartlett, K. J. Resch, "Optical one-way quantum computing with a simulated valence-bond solid", Nature Phys. 6, 850 (2010).
[9] P. Walther, K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer, A. Zeilinger, "Experimental one-way quantum computing", Nature 434, 169 (2005).
[10] A. Politi, J. C. F. Matthews, J. L. O'Brien, "Shor's Quantum Factoring Algorithm on a Photonic Chip", Science 325, 1221 (2009).
[11] A. Peruzzo et. al. "Quantum Walks of Correlated Photons", Science 329, 1500 (2010).
[12] M. Tillmann, B. Dakić, R. Heilmann, S. Nolte, A. Szameit, P. Walther, "Experimental boson sampling", Nature Photon. 7, 540 (2013).
[13] N.Spagnolo, et al., "Experimental validation of photonic boson sampling", Nature Photon. 8, 615 (2014).
[14] J. Carolan, et al. On the experimental verification of quantum complexity in linear optics Nature Photon. 8, 621 (2014).

[15] R. Krischek et al.,"Ultraviolet enhancement cavity for ultrafast nonlinear optics and high-rate multiphoton entanglement experiments", Nature Photon. 4, 170 (2010).
[16] C. Wagenknecht et al., "Experimental demonstration of a heralded entanglement source", Nature Photon. 4, 549 (2010).
[17] S. Barz, ,G. Cronenberg, A. Zeilinger, P. Walther, "Heralded generation of entangled photon pairs", Nature Photon. 4, 553 (2010).
[18] Y.-J. Wei et al., "Deterministic and robust generation of single photons from a single quantum dot with 99.5% indistinguishability using adiabatic rapid passage", Nano Lett.14, 6515 (2014).
[19] O. Gazzano, S. Michaelis de Vasconcellos, C. Arnold, A. Nowak, E. Galopin, I. Sagnes, L. Lanco, A. Lemaître, P. Senellart, "Bright solid-state sources of indistinguishable single photons", Nature Commun. 4:1425 (2013).
[20] J. Carolan, et al. "Universal Linear Optics", Science 349, 711 (2015).
[21] J. W. Silverstone, et al. "On-chip quantum interference between silicon photon-pair sources", Nature Photon. 8, 104 (2014).
[22] J. P. Sprengers, et al., "Waveguide superconducting single-photon detectors for integrated quantum photonic circuits", Appl. Phys. Lett. 99, 181110 (2011).
[23] W. H. P. Pernice, C. Schuck, O. Minaeva, M. Li, G. N. Goltsman, A. V. Sergienko, H.X. Tang, "High-speed and high-efficiency travelling wave single-photon detectors embedded in nanophotonic circuits", Nature Commun. 3: 1325 (2012).
[24] F. Marsili, et al. "Detecting single infrared photons with 93% system efficiency", Nature Photon. 7, 210 (2013).
[25] C. Schuck, Xiang Guo, Linran Fan, Xiao-Song Ma, Menno Poot, Hong X. Tang, "Quantum interference in heterogeneous superconducting-photonic circuits on a silicon chip", arXiv:1511.07081.
[26] G. Reithmaier, S. Lichtmannecker, T. Reichert, P. Hasch,1 K. Müller, M. Bichler, R. Gross, J. J. Finley, "On-chip time resolved detection of quantum dot emission using integrated superconducting single photon detectors", Sci. Rep. 3:1901 (2013).

2.2.3 Superconducting circuits

A. Physical approach and perspectives

Quantum computation with superconducting circuits exploits the intrinsic coherence of the superconducting state, into which all electrons are condensed. In addition, the Josephson effect is used to generate circuit non-linearity without associated dissipation, an essential component for realising quantum bits and for generating amplification in the microwave-frequency range.

Superconducting qubits are anharmonic, multi-level artificial atoms, of which two levels are used as effective quantum bits. These atoms store quantum information in different degrees of freedom: charge, flux or phase. The distinction in terms of charge, flux, and phase qubits is now outdated: all superconducting qubits are now closest to the phase regime than to the charge regime, making them less sensitive to charge noise and thereby more coherent. This trend includes the transmon (also called Xmon), the dominant qubit in use currently.

Superconducting circuits are fabricated with thin-film technology and operated at temperatures below 50 mK. Qubit measurements are typically performed by probing the transmission properties (amplitude and phase) of resonators that are either capacitively or inductively coupled to the qubits. Coupling between qubits is easily made strong, especially using coupling capacitors or transmission-line resonators and 3D cavities in a circuit/cavity quantum electrodynamics (cQED) architecture. Resonators and cavities provide opportunities for coupling widely different types of qubits in hybrid devices, including atoms, ions and impurity spins in quantum dots, crystals, and microtraps.

Industry interest in superconducting quantum computing has sharply risen in recent years. IBM has steadily expanded its team in Yorktown Heights and begun a new line of research in quantum simulation in Zurich. In 2014, Google partnered with the group of J. Martinis at UC Santa Barbara. This year, Intel has partnered with the group of L. DiCarlo and colleagues in Delft. Finally, Canadian company D-Wave continues to build devices of increasing scale based on inductively coupled superconducting flux qubits (1000+ qubits at present) controlled using superconducting, rapid single-flux quantum technology. Recent experiments provide evidence of quantum annealing in these systems, but claims of computational speedup remain the source of heated debate.

B. State-of-the-art

Referring to the DiVincenzo criteria [6], the state of the art for QIP with superconducting quantum circuits can be described as follows:

1. Quantum processors with 4-9 qubits have been demonstrated. The total number of quantum elements (including resonators) on-chip is approaching 20. These processors are controlled using room-temperature electronics;
2. Simple quantum error correction protocols have been realised [1-3], including repetition codes and surface-code sub-lattices;
3. First experiments in analog [4] and digital [5, 6] quantum simulation have been realised;
4. Universal gate operations: single-qubit operations are performed with microwave and DC pulses, achieving fidelities in excess of 99.9% [7];
5. Two-qubit gate operations and entangling gates achieve fidelities in excess of 99.5% [7];
6. The use of parametric amplification (also based on Josephson circuits) to boost readout signals allows routinely achieving single-shot, non-demolition qubit measurement with fidelity exceeding 99%. The bandwidth of parametric amplifiers has been extended from tens of MHz to several GHz, greatly facilitating scalability of quantum measurements [8].
7. Feedback control, wherein application of a gate is conditioned in real time on the outcome of a measurement, is demonstrated [9]. Feedback-based qubit reset is increasingly used as a means of qubit initialisation, replacing standard relaxation into the ground state, which becomes less efficient as qubit coherence time continues to grow.

8. Longer coherence times: improved understanding of the dominant role of dielectric loss and its source has allowed coherence times to reach up to ~80 microseconds in 2-D chips, and ~150 microseconds in 3-D structures. Transmission-line resonators achieve photon relaxation times of ~50 microseconds, while 3D cavities have crossed the millisecond. Other sources of decoherence, including the effect of quasiparticle tunnelling across junctions, photon shot noise, etc., have been identified theoretically and quantified experimentally;
9. Quantum memories: All essential functions (write, read, and reset) of a spin-based quantum memory for a superconducting qubit have been demonstrated [10], albeit with limited efficiency;
10. Quantum interfaces to flying qubit for optical communications: research is at the early development state, with recent demonstrations of conversion from microwave to optical light [11].
11. Fundamental experiments have demonstrated the use of quantum bath engineering to autonomously stabilise two-qubit entanglement [12] and suppress qubit energy relaxation [13].

C. Challenges

- Superconducting qubits are manufactured, not natural, and are therefore sensitive to imperfections (limiting yield and reproducibility of device parameters). This requires optimisation of the production process in order to reduce imperfections.
- These circuits operate below 50 mK and therefore require dilution refrigeration technology. This need poses an extra challenge for the engineering of a large-scale quantum computer beyond a few hundred qubits.

D. Short-term goals (0-5 years)

- Realise an extensible quantum processor architecture, allowing copy-pasting of unit cells to increase qubit numbers with ease; Essential developments include transitioning from millimetre to centimetre scale chips, and from lateral to vertical coupling of all control signals to the chip;
- Realise the ~50-qubit circuits required for the demonstration of quantum fault tolerance;
- Realise an extensible, non-quantum electronic architecture for control of the quantum circuit, operating either at room temperature, cryogenically, or a combination of both;
- Successfully use a quantum error correction code to preserve encoded quantum data longer than would be possible with the constituent physical qubits;
- Develop tune-up schemes that do not really on traditional but unscalable methods such as state and process tomography;
- Develop automatic tune-up of quantum processors using numerical optimisation and optimal control;

- Demonstrate the interconversion of quantum data from one microwave qubit onto a flying, optical qubit with high quantum efficiency.

E. Medium-term goals (5-10 years)

- Demonstrate quantum fault tolerance: improved protection of encoded quantum data by added redundancy (more physical qubits) in a quantum error correcting code;
- Realise a quantum processor accommodating several logical qubits;
- Demonstrate small quantum networks, with links allowing the distribution of pairwise entanglement across nodes;

F. Long-term goals (>10 years)

- Perform a quantum algorithm, such as Grover's or Deutsch-Jozsa, using multiple logical qubits;
- Solve a technologically relevant quantum chemistry problem using quantum simulation (analog or digital);
- Realise a quantum repeater using a (hybrid) superconducting circuit for memory and flying photons for communication, making use of a high-efficiency microwave-optical interface.

G. Key references

[1] J. Kelly, et al., State preservation by repetitive error detection in a superconducting quantum circuit, Nature 519, 66 (2015).
[2] D. Ristè, S. Poletto, M. Z. Huang, A. Bruno, V. Vesterinen, O. P. Saira, and L. DiCarlo, Detecting bit-flip errors in a logical qubit using stabilizer measurements, Nature Communications 6, 6983 (2015).
[3] A. D. Corcoles, E. Magesan, S. J. Srinivasan, A. W. Cross, M. Steffen, J. M. Gambetta, and J. M. Chow, Demonstration of a quantum error detection code using a square lattice of four superconducting qubits, Nature Communications 6 (2015).
[4] C. Eichler, J. Mlynek, J. Butscher, P. Kurpiers, K. Hammerer, T. J. Osborne, and A. Wallraff, Exploring interacting quantum many-body systems by experimentally creating continuous matrix product states in superconducting circuits, arXiv:1508.06471 (2015).
[5] R. Barends, et al., Digital quantum simulation of fermionic models with a superconducting circuit, Nature Communications 6 (2015).
[6] Y. Salathé, et al., Digital quantum simulation of spin models with circuit quantum electrodynamics, Physical Review X 5, 021027 (2015).
[7] R. Barends, et al., Superconducting quantum circuits at the surface code threshold for fault tolerance, Nature 508, 500 (2014).
[8] C. Macklin, K. O'Brien, D. Hover, M. E. Schwartz, V. Bolkhovsky, X. Zhang, W. D. Oliver, and I. Siddiqi, A near–quantum-limited Josephson traveling-wave parametric amplifier, Science 350, 307 (2015).
[9] D. Ristè and L. DiCarlo, Digital feedback in superconducting quantum circuits, ArXiv:1508.01385 (2015).
[10] C. Grezes, Towards a spin-ensemble quantum memory for superconducting qubits, PhD Thesis, University Paris VI, 2015.

[11] R. W. Andrews, R. W. Peterson, T. P. Purdy, K. Cicak, R. W. Simmonds, C. A. Regal, and K. W. Lehnert, Bidirectional and efficient conversion between microwave and optical light, Nature Physics 10, 321 (2014).
[12] S. Shankar, et al., Autonomously stabilized entanglement between two superconducting quantum bits, Nature 504, 419 (2013).
[13] K. W. Murch, S. J. Weber, K. M. Beck, E. Ginossar, and I. Siddiqi, Reduction of the radiative decay of atomic coherence in squeezed vacuum, Nature 499, 62 (2013).

2.1.4 Electronic semiconductor qubits

A. Physical approach and perspectives

Semiconductor transistors form the backbone of today's electronics industry. The same core technology has been applied successfully in the field of QIPC. Employing nanofabrication techniques, quantum dots have been defined in which individual electrons can be confined. Also isolated donors have been positioned in semiconductor substrates and used to trap individual electrons. In both cases, the spin of one or more electrons is considered the most promising qubit representation, since spin coherence is longer than the coherence of charge states or other degrees of freedom. These devices can be measured and controlled fully electrically, again much like transistors in today's digital electronics. Until recently, most efforts focused on GaAs based quantum dots. In the last few years, increasing attention goes to group IV materials such as silicon and germanium, as they offer longer spin coherence times. Overall, the wide set of semiconductor materials available offers a range of tunable parameters, such as high-spin-orbit coupling for faster manipulation (InAs), or low nuclear spin concentrations for longer spin coherence times (Si, SiGe).

B. State-of-the-art

Two main technologies are used to form electrically controlled spin qubits, quantum dots and donors. Quantum dots are formed via lithographically defined gate patterns on top of 2D or 1D electron systems. Donors are either implanted through small apertures or positioned by STM lithography. Despite these differences, much of the underlying physics is the same in these two systems. The state-of-the art is as follows:

- Quantum dot circuits with up to five quantum dots have been controllably loaded with electrons;
- High-fidelity qubit initialisation of more than 99.9% has been realised;
- High-fidelity single-shot read-out of up to three spin qubits was demonstrated with fidelities of ~97% on average;
- Single-spin coherent rotations have been demonstrated both using magnetic and using electrical driving, with gate fidelities in excess of 99%;
- Coherent exchange of two spins in a double quantum has been demonstrated;
- Coherent coupling of two double-dot spin states has been demonstrated, exploiting capacitive coupling;

- Quantum dot spin states have been probed and controlled using superconducting resonators;
- Relaxation times (T1) from milliseconds to many seconds have been observed, and the relaxation mechanism has been established;
- Spin dephasing times (T2*) have been measured in GaAs (~10 ns), natural silicon (~1 microsecond) and in isotopically enriched silicon (~200 microseconds) have been measured in isotopically enriched 28Si, and the main decoherence mechanism has been established;
- Partial control of the nuclear spin environment (the main source of decoherence) has been achieved in GaAs, extending T2* to about 1 microsecond;
- Dynamical decoupling T2's have been measured up to 200 microseconds in GaAs, 0.5 ms in natural silicon and 0.5 second in 28Si;
- Qubit states have been transferred back and forth between the electron and nuclear spin of donors;
- Single nuclear spin memory times (using dynamical decoupling) of up to 30 seconds have been recorded;
- Electrons have been shuttled between quantum dots separated by about one micron propelled by surface acoustic waves;
- Hybrid dot-donor devices have been realised, and joint spin states have been observed.

In summary, all the ingredients for an elementary quantum processor have been realised and integrated in dots, and all ingredients except two-qubit gates have been realised in donors. Initialisation, read-out and gate fidelities are steadily improving, in some cases already exceeding 99%, the threshold for popular error correction schemes. Particularly promising is the recent increase in T2* by a factor of 10^4. Even stronger increases in dynamical decoupling decay times offer great promise for qubit memories. These important improvements have been the result of materials developments (silicon qubits) and nuclear spin feedback schemes (GaAs). Scaling up qubit arrays along a 1D array is proceeding well, especially in dots. Several avenues for distant on-chip coupling and/or transferring of qubits arranged in a 2D array are being explored.

C. Challenges

Looking ahead, we identify a number of challenges that need to be overcome in order to push electrically controlled electron spin qubits to the next level:

- Poor qubit uniformity and background disorder currently must be compensated for by tedious tuning of gate voltages;
- Low-frequency charge noise has been considerably reduced over the past ten years, but still sometimes slows down experiments (as some retuning is needed when background charges move);
- An increased understanding of the microscopic origin of high-frequency charge noise, and a reduction of charge noise levels, is needed to improve the fidelity of gates based on spin exchange, capacitive coupling, and other gates sensitive to electric fields;

- Creating precisely positioned donor arrays remains a challenge;
- Whereas many theoretical ideas have been put forward, a coupling mechanism and/or geometry that is suitable for creating 2D arrays of spin qubits remains to be demonstrated experimentally;
- Efficient schemes need to be developed to wire up increasing numbers of qubits on a chip operating at cryogenic temperatures;
- Compact, low-cost electronics (possibly in part cryogenic electronics) needs to be developed for read-out and control of increasing numbers of qubits.

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

- Automated calibration of devices;
- Understanding and mitigating origin and effect of electrical noise sources on spin qubits;
- Minimising number of gates-per-qubit to aid scaling up;
- 'Unit cell' demonstration of a 2D spin qubit architecture towards scalable fault-tolerant operation;
- Robust and secure sources for high-purity semiconductor materials;
- Quantum simulation with arrays of 10-20 spin qubits;
- Coupling multiple physical spin qubits to achieve a fault-tolerant logical qubit.

E. Medium-term goals (5-10 years)

- Coupling of multiple logical qubits;
- Quantum simulation with arrays of up to 1000 high-fidelity spin qubits;
- Integration of classical and quantum electronics in a cryogenic environment;
- Implementation of techniques such as on-chip multiplexing to efficiently control 2D gate arrays.

F. Long-term goals (>10 years)

- Universal gate-based quantum computation with fully integrated software and hardware layers;
- Wafer-scale fabrication of quantum processor chips.

G. Key references

[1] D. Loss and D. DiVincenzo, ''Quantum computation with quantum dots'', *Phys. Rev. A* **57**, 120 (1998).
[2] B. Kane, "A silicon-based nuclear spin quantum computer", *Nature* **393**, 133 (1998);
[3] R. Hanson, L.P Kouwenhoven, J.R. Petta, S. Tarucha, and L.M.K. Vandersypen, "Spins in few-electron quantum dots", *Rev. Mod. Phys*. **79**, 1217 (2007)
[4] J. J. L. Morton, D. R. McCamey, M. A. Eriksson and S. A. Lyon, "Embracing the quantum limit in silicon computing", *Nature* **479**, 345 (2011)
[5] F. A. Zwanenburg *et al*. "Silicon quantum electronics" *Rev. Mod. Phys*. **85**, 961 (2013)

2.1.5 Impurity spins in solids and single molecular clusters

A. Physical approach and perspectives

Storage and processing of information can be carried out using individual atomic and molecular spins in condensed matter. Systems falling into this category include dopant atoms in semiconductors like phosphorous or deep donors in silicon or color centers in diamond, nitrogen or phosphorus atoms in molecules like C60, rare earth ions in dielectric crystals and unpaired electrons at radiation induced defects or free radicals in molecular crystals.

The main attraction of spins in low-temperature solids is that they can store quantum information for up to several thousand seconds [1], on the other hand certain spin systems are shielded well enough from their environments such that room temperature operation seem feasible. Specific systems have been selected based on criteria like: dephasing time, optical access, single quantum state readout, and nanostructuring capabilities. While most of these systems are scalable in principle, technical progress in single quantum state readout, addressability and nanoengineering is necessary.

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

B. State-of-the-art

Impurity spins

Atomic and molecular spins in solids have received considerable attention as qubits. Already Kane's [1] proposal has underlined the basic challenges and opportunities of such systems in quantum computing. In the meantime, a number of related systems like dilute rare earth ions, colour centres, random deep donors in silicon with optically controlled spin and defects in wide and narrow band gap semiconductors have underlined their potential usefulness in QIP [2]. Most approaches use electron or nuclear spin degrees of freedom as quantum bits. The specific advantages of spin systems includes long decoherence times [3] and access to highly advanced methods for precise manipulation of quantum states. The experimental techniques that have made liquid state NMR the most successful QIP technique in terms of precise manipulation of quantum states so far are currently being transferred to solid-state systems. These systems may be able to overcome the scalability problems that plague liquid state NMR while preserving many of the advantages of today's liquid state work Large scale quantum simulator based on nuclear spin in diamond was proposed recently [4]. Robust control of solid state quantum registers allowed to realise repetitive error correction protocols [5].

Optically active defects (colour centres) also were used to realise high fidelity entanglement via optical channel and using magnetic dipolar coupling [6,7]. Dense ensembles of colour centres were shown to be promising candidates for building quantum memories for superconducting qubits [8].

In detail, the following landmark results that have been achieved:

- Magnetic resonance on single defects detected by charge transport and single spin state measurements by optical techniques;
- Multipartite entanglement of single defects based on magnetic dipolar coupling
- Quantum teleportation between distant colour centres based on optical channels;
- Quantum error correction;
- Accurate preparation and readout of ensemble qubit states. Arbitrary single-qubit operations characterised by quantum state tomography with a fidelity >99,9%;
- The preparation of Bell states with electron and nuclear spin ensembles as well as a three qubit Deutsch-Jozsa algorithm has been achieved.

Single molecular magnets

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

Recent important achievements are:

- Proposals for the implementation of the Grover's algorithm in high spin SMMs [4], and of universal solid state quantum devices in antiferromagnetic spin clusters;
- Synthesis of specific molecules providing promising test-beds for scalable schemes [5];
- Entanglement of states belonging to different molecules inspired both synthesis of new molecular dimers and elaboration of specific quantum algorithms that exploit some features of molecular clusters;
- Spin qubits can be coupled to a superconducting microwave cavity that acts as a 'quantum bus', as it is usually done for superconducting qubits;
- It has been demonstrated that the nuclear spin of an individual metal atom embedded in a single-molecule magnet can be read out electronically.

C. Challenges

Impurity spins

The strength of defect centre 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 more than 95 %). Substantial progress in the nano-positioning of single dopants with respect to control electrodes has been achieved. On the other hand, nano-positioning and creation yield of defects is still a major challenge (which has seen dramatic progress for phosphorus in silicon and colour centres in diamond). However there are schemes, based on deep donors in Si and optically active defects in diamond, where nano-positioning is not crucial. For defects in silicon, instead the randomness is exploited so as to make maximum use of spatial and spectral selection to isolate qubits and their interactions. For colour centres in diamond, long distant entanglement can be realised based on optical coupling.

Single molecular magnets

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

D. Short-term goals (0-5 years)

Impurity spins

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

- Defects in diamond heads towards generation of coupled defect centre arrays and incorporation into photonic structures. For this, advanced nano-implantation techniques as well as production of photonic cavities need to be improved in order to achieve long coherence time of defects in nano-engineered material;
- For rare earth crystals, short term goals include faster gate operations using pulses developed by optimal control theory, demonstration of two-qubit gates and the development of single ion readout capabilities for scaling up to several qubits;
- For the scheme based on deep donors in Si or diamond, short term goals are demonstrations of all the key steps of fabrication, preparation, readout, and manipulation.

Single molecular magnets

The main goals can be summarised as follows:

- To engineer new molecular clusters for the optimisation of the coherent dynamics of spins, and design, synthesise and characterise controlled molecular linkers between spin clusters;

- To set up experiments for the direct observation of coherent dynamics (for instance Rabi oscillations, spin echo experiments), and probe, understand and reduce the intrinsic decoherence mechanisms in specific cluster qubits;
- To develop computational schemes exploiting the features of molecular cluster qubits, and study different functionalities (f.i. switchability) of molecules useful for specific tasks in complex architectures of QIP.

E. Medium-term goals (5-10 years)

Impurity spins

- The medium term perspectives for phosphorus in silicon are the demonstration of single spin readout and two qubit operations. Major efforts are concentrated in the US and Australia;
- 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;

Single molecular magnets

- Definition of reliable procedures for preparing, characterising and positioning (arrays of) molecular spin cluster qubits;

F. Long-term goals (>10 years)

Impurity spins

- Coupling of defects in wide band gap semiconductors to an optical cavity mode allowing to reach high cooperativity. Implantation of defects with nm accuracy in registry with control electrodes. Optical addressing of single defects within dense defect arrays using optical super-resolution techniques and magnetic field gradients;
- For rare earth ions, efforts should be joined with crystal growth research (inorganic chemistry) to create appropriate materials for larger scale systems. Techniques should also be developed for entangling remote systems to achieve full scalability;
- Few-qubit (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;
- Large scale (>100 qubits) quantum simulators based on implanted colour centres and optically initialised self-assembled nuclear spins in crystal lattice

Single molecular magnets

- Development of models and experimental methods for efficient read-out.

G. Key references

[1] B. Kane, “A silicon-based nuclear spin quantum computer”, Nature 393, 133 (1998) [2] R. Hanson, D. Awschalom. "Coherent manipulation of single spins in semiconductors" Nature 453, 1043 (2008), P. Neumann et al. "Multipartite entanglement of single spins in diamond", Science 320, 1326 (2008) [3] E.

Yablonowitch, H.W. Jiang, H. Kosaka, H.D. Robinson, D.S. Rao, T. Szkopek "Optoelectronic quantum telecommunications based on spins in semiconductors" , Proc. IEEE 91, 761 (2003)
[4] Cai JM, Retzker A, Jelezko F, Plenio MB. A large-scale quantum simulator on a diamond surface at room temperature. Nature Physics 9:168-173 (2013)
[5] Waldherr G, Wang Y, Zaiser S, Jamali M, Schulte-Herbruggen T, Abe H, et al. Quantum error correction in a solid-state hybrid spin register. Nature 506:204 (2014)
[6] Dolde F, Bergholm V, Wang Y, Jakobi I, Naydenov B, Pezzagna S, et al. High-fidelity spin entanglement using optimal control. Nature Communications 5, 3371 (2014)
[7] W. Pfaff, B. Hensen, H. Bernien, S. B. van Dam, M. S. Blok, T. H. Taminiau, M. J. Tiggelman, R. N., Schouten, M. Markham, D. J. Twitchen, R. HansonUnconditional quantum teleportation between distant solid-state qubits, Science 345, 532–535 (2014)
[8] C. Grezes, B. Julsgaard, Y. Kubo, M. Stern, T. Umeda, J. Isoya, H. Sumiya, H. Abe, S. Onoda, T. Ohshima, V. Jacques, J. Esteve, D. Vion, D. Esteve, K. Mølmer, and P. Bertet, Multimode Storage and Retrieval of Microwave Fields in a Spin Ensemble, Phys. Rev. X 4, 021049 (2014) [9] M.N. Leuenberger, D. Loss, "Quantum Computing in Molecular Magnets'', Nature 410, 789 (2001)
[10] F. Troiani A. Ghirri, M. Affronte, P. Santini, S. Carretta, G. Amoretti, S. Piligkos, G. A. Timco, R. E. P. Winpenny, "Molecular engineering of antiferromagnetic rings for quantum Computation", Phys. Rev. Lett. 94, 207208 (2005)

2.1.6 Virtual Facilities needs

Quantum Engineering

- High-bandwidth circuitry at cryogenic temperatures with integrated classical control.
- Fast optical switching (GHz) (low latency, low loss, low noise);
- Low-loss interconnects;
- High-extinction filters (for sources);
- Integration of quantum-dot sources into photonic systems;
- Compatibility of different materials architectures;
- Improved control of variability in components for large architecture.
- Materials: Purity of materials must be provided. Requirements range from elemental purity in the case of all semiconductors, through to isotopic enrichment, for materials such as Si and SiGe to benefit from the longest possible coherence times and highest fidelities, and minimising unintentional defects for reducing background disorder;
- Nano & micro fabrication: Patterning of nano-scale gates to define quantum dots, control lines, and spin-readout devices, in some cases down to ~20nm feature sizes with similar pitches. In the near term this can be achieved with direct-write methods such as EBL. In the longer-term methods such as deep UV lithography will be required for wafer-scale production;

- Scalable gate architectures: Each spin qubit requires at least one gate, and often several gates, in order to (e.g.) define quantum dots and achieve selective control and readout. Solutions such as on-chip multiplexed gate arrays are required to achieve high-density qubits in a scalable architecture;
- Cryogenics: All electronic semiconductor qubits being currently explored require operation at cryogenic temperatures, typically in a dilution fridge below 50 mK. Further development is required in cryogenics to increase sample space and cooling power to accommodate a combination of quantum and classical electronics;
- Cryo-compatible control electronics: Controlling spin qubits requires a suite of DC and RF control electronics – typically these are synthesised at room temperature and fed down to the device at cryogenic temperatures. This becomes impractical for a large number of devices, requiring solutions for compact, low-power cryo-compatible control electronics;
- Control software: Desired quantum operations as part of some algorithm must be interleaved with the necessary low-level control operations for fault-tolerance in order to perform a practical operation. These low-level operations will often require fast-feedback operation. Software will be required to fit within the compiled layer and the hardware layer;
- Compilers: As with all quantum computing implementations, compilers are required to convert required quantum algorithms into a sequence of implementable operations.

Quantum Control

- Spin manipulation and control in quantum dots, optimal control.
- Previous work has made use of dynamical decoupling methods to extend qubit coherence times – these methods are expected to continue being used in the future, to various extents depending on the precise system and noise sources
- Previous work on spin ensembles in semiconductors has also made use of optimal control sequences to increase single qubit gate fidelities in the presence of (e.g.) inhomogeneous broadening, and such methods are likely to be used in semiconductor spin qubits to achieve high-fidelity gates in the presence of low-frequency noise.

2.2 Quantum Communication

Quantum communication is the art of transferring a quantum state from one location to another. In this way, information or resources such as entanglement, can be distributed between distant locations. The communication of qubits will be an essential ingredient in taking advantage of quantum technologies, from quantum computing and simulation to secure communication based on quantum key distribution (QKD). The first application of quantum communication, quantum cryptography, deals with the distribution of shared secret random numbers for sharing cryptographic keys.

Quantum random number generators (QRNG) are central to many cryptographic primitives as well as having application areas ranging from gaming and lotteries to high performance computing. Quantum random number generators are one of the most fundamentally fascinating and practically useful applications of quantum technologies. Our information-based society consumes large quantities of random numbers for a wide range of applications like, e.g., cryptography, PINs, lotteries, numerical simulations, etc. The production of random numbers at high rates is technically challenging; at the same time, given the pervasiveness of the deployment of random numbers, poor random number generators can be economically very damaging. Quantum physics provides the only true source of randomness in Nature. Moreover, in the basic configuration (a photon impinging on a beam splitter followed by two detectors associated to the bit values 0 and 1) the origin of the randomness is clearly identified. Today's commercial quantum random number generators have rates of around 4Mbps, although prototype devices are already reaching Gbps rates. Their drawback is a significant cost compared to other approaches, but one expects that (near) future QRNG will provide higher rates at lower costs. For example, recently it has been shown that the camera in mobile phones can be used as a QRNG, opening the door to potentially massive commercial opportunities.

QKD is of major interest, as it offers for the first time a provably secure way to establish a confidential key between distant partners. In QKD, the key is first tested, and if the test succeeds, used in standard cryptographic applications – with the major addition that the security of the key relies solely on the laws of quantum physics and the ability to implement the protocol as defined by the theory. This has the potential to solve long-standing and central security issues in our information based society. The first commercial systems have been on the market for over ten years and are currently installed around the world, running continuously and autonomously for over 8 years. In the laboratory, the next generation of systems are being developed with a view to addressing the non-trivial challenges of reducing costs, increasing bit rates, and extending quantum communication over longer distances.

Practical issues of network operation, dealing with amplifiers, switching and multiplexing in fibre networks, represents one of the most important quantum engineering challenges. To extend communication distances, approaches based on 'trusted-node' configurations – point-to-point QKD systems linked together at secure locations – provide the most obvious way forward towards developing Pan-European, even global, quantum communication networks – a Quantum Backbone. The goal being to make the national and European communication 'quantum-safe'. This is an ambitious and important task and will require both quantum and classical, cryptographic solutions working together. In particular, the arrival of the Internet of Things, virtual and software-define networks, place increasing demands on security and represent areas where quantum technologies could play a pivotal role.

In order to go beyond simply ‘quantum-safe’ networks to completely quantum secure networks, ‘trusted nodes’ need to be replaced by fully-quantum systems – quantum repeater architectures. Alternatively, satellite configurations, i.e., free space systems, could be used as trusted repeaters, the in-orbit location of satellites helping to ensure their protection. Satellite systems are currently being developed and tested to meet the associated demands. Several countries already have planned missions to launch quantum systems for further testing.

One of the emerging areas of interest for quantum communication schemes is in connecting the nodes within quantum computers or simulators, which can either be all located in one lab, or more interestingly, in distributed scenarios -- the tools from quantum communication playing the role of wiring circuits for these quantum computers. While many challenges for proof-of-principle laboratory demonstrations remain, even for short-range communication, the transition to deployment in real-world environments defines a new set of challenges for quantum technologies.
The issues of scale, range, reliability, and robustness that are critical for quantum communication technologies cannot be resolved by incremental improvements, but rather need to be addressed by making them the focal point of the research and technology development agenda. To succeed, this needs to target both the underlying technologies, ranging from fundamental aspects of engineering quantum devices and systems to interfacing these with integrated photonics, fast (classical) opto-electrical systems and FPGA systems, as well as the end-user applications themselves and the operation in communication networks.

In particular, the following need to be addressed:

1. Quantum Cryptography: Increased adoption of integrated photonics, improved detection, electronics and control systems, to facilitate the commercialisation of QKD technologies. Improved operation in real-world networks and extension to virtual and software-defined networks. New protocols, beyond QKD, like quantum digital signatures and ever-lasting secure storage, are needed to extend the benefits of quantum security to other applications.
2. Quantum Networks: Demonstration of trusted-node, and quantum repeater architectures will be essential for increasing distances to continental, and even global, scales. Quantum repeater concepts will also be critical in the

context of computation and simulation, both for short distance scales (local) or long, (distributed), processing systems. This requires hybrid systems linking quantum sources, interfaces, memories and detectors with performance significantly greater than the current state of the art, as well as theoretical engineering work to determine resilient protocols and architectures that can combat errors in practise.

3. Implementation and Security: Increasingly complex quantum networks of disparate technologies require new approaches for ensuring security. Quantum hacking is necessary for challenging and improving the device and system technologies. Device Independent and Self Testing systems provide a new perspective with the potential to minimise security assumptions, and hence simplify the security of real-world quantum communication systems. Certification and standards are critical challenges to be addressed for the commercial uptake of quantum communication technologies. In this regard ETSI have established an Industry Specification Group to develop industrial standards for QKD and the Quantum-safe Security working group has been formed to address key generation and transmission methods and to help industry understand quantum-safe methods for protecting their networks and data.

From the present situation, where commercial systems already exist, we briefly review the underlying foundational technologies and more generally, quantum communication from the perspective of increasing rates and distances to solutions extending point-to-point QKD towards complex quantum networks for the distribution of quantum resources and for performing new protocols.

2.2.1 Quantum Random Number Generators (QRNG)

A. Physical approach and perspective

QRNGs have proven to be one of the most surprising quantum technologies commercialised so far, having found novel applications in lotteries, on-line gambling and PIN generation, as well as those that were expected such as computation and simulation. There is a wide range of approaches that vary depending on the target application. For example, low-cost schemes, perhaps only requiring relatively low rates, are well suited to these novel applications, while high-speed schemes, which could be more expensive, are well suited to problems of real-time random number generation for simulations and modelling in high-performance computing.

B. State-of-the-art

The archetypal QRNG involves a photon impinging on a beamsplitter followed by two detectors associated to the bit values 0 and 1. Whether the photon is reflected or transmitted at the beamsplitter is a fundamentally random process and as there is only one photon at a time, only one detector will register this random outcome. Commercial devices of this nature are commercially available, with rates 4Mbps, although four can be placed on a PCI board, extending this to 16Mbps [1], and more recently up to 50Mbps [2]. Continuous variable schemes have also been demonstrated [3]. Significant increases in the rates have been realised through schemes based on phase diffusion in pulsed laser diodes [4], gain switched laser diodes [5] and amplified spontaneous emission from an erbium-doped fibre [6], with generation rates in the Gbps regime. In the context of low cost devices, it has been recently shown how the camera in a mobile phone can be exploited as a QRNG [7].

An important characteristic for random numbers, especially in the context of security, is that they need to be private. Also important is the optimisation of the latency between the external random bit request signal and the moment when the bit is generated. It is necessary that all the physical processes relevant to the generation of a bit happen after the request signal and that the production of a bit upon that request has absolute efficiency [11]. These requirements make the random numbers suitable even for most demanding applications, such as loophole-free Bell tests.

The field of QRNGs addresses these demands, and theoretical work has even shown how to realise Device-Independence of randomness amplification [8]. Device-independent protocols require the loophole-free violation of a Bell inequality. Indeed, correlations arising in Bell tests are based only on the input/output probabilities and can be used to determine the correct operation of a device or system. Therefore, very little trust is needed in the correct manufacturing of the devices: faulty behaviour can be detected, and will not lead to an unknown security leak. DI-QRNGs are experimentally challenging, although a demonstration has been made, albeit with extremely low rates [9]. A less restrictive approach, in-between normal QRNGs and device-independent, is 'Self-testing', where schemes have been demonstrated experimentally with improved rates [10].

C. Challenges

QRNGs are actively being researched around the world and, while China is increasing its activity, Europe is certainly one of the leaders in both theory and experiments. There is increasing demand on the reduction of size and cost of QRNGs, for example for their generation in mobile phones or on small chips that can be included in server systems, but also other devices as security for the Internet of Things. For high-speed requirements, like real time RNG for high-performance computing, size and cost are less of a constraint, but cannot be completely ignored. Target rates should be in the tens of Gbps.

From the theoretical perspective, work is required in developing protocols for the use of quantum generated random numbers in security protocols for small devices as well as bridging the gap between standard QRNGs and DI-QRNGs. Self-testing schemes are one possibility, but other approaches that sacrifice some of the security of DI-QRNGs for higher rates (including low latency or lower costs) may help towards certification, verification and even meeting QRNG standards.

D. Short-term goals (0-5 years)

- Realising chip-based QRNG devices.
- Improved detectors for higher rates, as required for high performance computing and simulation, as well as for high-speed QKD schemes.
- New concepts and ideas for the generation of quantum random numbers.

E. Medium-term goals (5-10 years)

- Realising QRNGs reaching high rates (around 10Gbps).

F. Long-term goals (>10 years)

- Practical solutions for self-testing or device independent RNGs

G. Key references

[1] http://www.idquantique.com/random-number-generation
[2] H. Fürst, *et al.,* "High speed optical quantum random number generation", Opt. Exp. 18, 13029 (2010), http://www.qutools.com/products/quRNG
[3] C. Gabriel, *et al.*, "A generator for unique quantum random numbers based on vacuum states", Nature Phot. 4, 711 (2010)
[4] C. Abellan, *et al.,* "Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode", Opt. Exp., 22, 1645 (2014)
[5] Z Yuan *et al,* "Robust random number generation using steady-state emission of gain-switched laser diodes", Appl. Phys. Lett. 104, 261112 (2014)
[6] A. Martin, *et al.*, "Quantum Random Number Generation for 1.25-GHz Quantum Key Distribution Systems", J. Lightwave Tech., 33, 2855 (2015)
[7] B. Sanguinetti, *et al.,* "Quantum Random Number Generation on a Mobile Phone", Phys. Rev. X 4, 031056 (2014)
[8] A. Mattar, *et al.*, "Optimal randomness generation from optical Bell experiments", New J. Phys., 17, 022003 (2015)
[9] S. Pironio, *et al.*, "Random numbers certified by Bell's theorem", Nature 464, 1021 (2010)
[10] T. Lunghi, *et al.*, "Self-Testing Quantum Random Number Generator", Phys. Rev. Lett. 114, 150501 (2015)

2.2.2 Quantum Key Distribution systems

A. Physical approach and perspective

QKD systems are the most advanced quantum communication technologies. Designed for operation in existing optical networks, fibre-based systems have been commercially available for more than ten years and run constantly and autonomously in locations all around the world. There are significant efforts both in engineering these systems for lower costs, increasing rates, and network operation, as well as more fundamental research efforts for next generation devices and systems, ranging from hand-held to access network and backbone technologies. Schemes involving both discrete and continuous variable encodings, as well as free-space, satellite-based, and fibre optic systems are currently under investigation.

Fibre Systems

Several groups are currently working on fibre QKD systems that encode in polarisation, phase, photon number and time-bins, using both discrete or continuous-variables (CV). Weak-pulse (laser pulses attenuated to the single photon level) encoding schemes are by far the most practical and advanced approaches. The research pursuit is primarily directed at improved detector performance and greater use of integration, both on the quantum level as well as the quantum-classical interface and information processing. Integrated photonics has advanced sufficiently such that it can now be considered for replacing some components in the QKD systems, which should have a significant impact on the costs of commercial products. It should be noted that while classical telecom components (such as phase and amplitude modulators) already operate for 40+Gbps systems, their characteristics are not sufficiently good for quantum schemes. Operation on data carrying fibres has been a recent but necessary step for reducing the implementation cost and moving beyond niche, high-security applications.

Device-independent concepts that, while still using the same telecom-compatible components, can overcome potential side-channel hacking attacks, have made significant progress recently and are an important step forward towards certification of these systems. Most notable are measurement-device-independent (MDI) and detector-device-independent (DDI) schemes that overcome attacks and manipulation of the QKD system's detectors.

Free Space Systems

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

The European Space Agency (ESA) has supported various studies in the field of quantum physics and quantum information science in space for several years. The mission proposal Space-QUEST (Quantum Entanglement for Space Experiments) has the objective of performing space-to-ground quantum communication tests from the International Space Station (ISS). The launch plan is compatible with 2017.

B. State-of-the-art

QKD schemes face fundamental distance limits and recent experiments have approached them for both fibre and free space schemes. In fibre optical systems, >300 km has been achieved [1] as well as demonstrations that QKD and classical communication channels can co-exist [2], even at 20 Gbps data transmission and Mbps secure key rates [3] and on installed 40Gbps links [4], using standard network multiplexing technologies. Work on multi-user, quantum access networks, has also been demonstrated based on simple and cost-effective telecommunication technologies [5]. Integrated photonics has sufficiently matured and recently a chip-based demonstration of QKD functionality was made [6]. CV systems [7] are much more sensitive to distance, though 80 km has been realised in the lab [8]; chip-based demonstrations are also envisioned [9]. Sustained key rates exceeding 1 Mbps have been demonstrated [10] and recently extended to 2.38 Mbps over 35km of fibre [3]. There are also extensive field trials taking place in the Canary Island involving several leading European groups as part of a European Space Agency feasibility study for quantum communication via satellite [11]. A weak pulse free-space QKD scheme has been demonstrated over >144 km [12]. In a related experiment, the Matera Laser Ranging Observatory (MLRO) in Southern Italy served as transceiver station for faint-pulse exchange with a low-Earth-orbit (LEO) retro-reflecting satellite at a perigee of 1485 km [13], which was recently extended to a distance of 7000km by using a medium-Earth-orbit satellite [14]. Quantum communication of qubits encoded in the polarisation of single photons was also demonstrated with LEO satellites [15]. This latter study showed the feasibility of a very limited QKD payload, based on a phase-modulated retroreflector, as a convenient alternative to the transmitter state generator and telescope. A multi-photon teleportation experiment was also demonstrated in a free-space link [16], which is an important step for future quantum networks. The practical limits of information capacity are being studied, both for time-bin qubits in fibre-optic systems as well as orbital-angular-momentum photonic states for free-space experiments [17].

C. Challenges

Europe and Japan are the clear leaders for fibre systems, with China rapidly progressing; it is currently building a 2000km network with over 40 trusted-nodes already running. The central challenge for QKD systems is for lower costs, possibly exploiting integrated photonics, as well as increasing rates, either simply by higher clock rates or through multiplexing multiple signals or systems. This also represents a crucial step to reduce the payload size and weight, optimise coupling and increase of the secure key rate for satellite deployment. These systems are generally the most applied and hence the most likely to lead to commercial systems. Satellite systems are faced with re-engineering the systems to cope with being launched into the space and operating there. A major challenge is to have greater collaboration between quantum and classical cryptographers, to improve practical operation and security. In all cases, the integration of multiple components for fast, efficient and continuous operation is perhaps the most demanding engineering challenge for all of these systems. The challenges for detectors, outlined in the following section, will also have a significant impact here.

D. Short-term goals (0-5 years)

- Certification for QKD systems;
- Small, low-cost, QKD systems, exploiting integrated photonics, in a standardised telecom blade chassis;
- Demonstration of practical, autonomous, systems capable of performing continuous secure key distribution > 10 Mbps rates, e.g. over MAN distances;

- Demonstration of passive and programmable multiplexing of multiple quantum channels as well as quantum and classical channels to increase rates and reduce infrastructure costs associated with fibre bandwidth and network architectures;
- Develop and demonstrate schemes exploiting complex spatial mode structures as decoherence-free states in free space channels, both, discrete and CV, that don't suffer due to turbulence and diffraction;
- LEO communication demonstrations for quantum communication;
- Full finite-size security analysis in the practically realisable parameter regime;
- Bridge gap between quantum and classical cryptographic schemes.

E. Medium-term goals (5-10 years)

- Demonstration of practical, autonomous, systems capable of performing continuous secure key distribution at >100 Mbps rates, e.g. over MAN distances;
- Day light QKD implementations from LEO orbit;
- Reliable and cheap 'on chip' QKD, directly available as a computer board, with price and packaging similar to present day QRNGs.

F. Long-term goals (> 10 years)

- Demonstration of practical, autonomous, systems capable of performing continuous secure key distribution > 1 Gbps rates, e.g. over MAN distances;
- GEO communication demonstrations for quantum communication
- Practical semi-device-independent protocols with explicit assumptions about security analysis;
- Fully composable security within a quantum network.

G. Key references

[1] B. Korzh, *et al.*, “Provably secure and practical quantum key distribution over 307 km of optical fibre”, Nature Photonics 9, 163 (2015)
[2] P. Eraerds, *et al.*, “Quantum key distribution and 1 Gbps data encryption over a single fibre”, New J Phys. 12, 063027 (2010)
[3] K Patel, *et al*, “Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks”, Applied Physics Letters 104, 051123 (2014)
[4] I. Choi, *et al.*, " Field trial of a quantum secured 10Gb/s DWDM transmission system over a single installed fiber”, Optics Express, 22, 23121 (2014)
[5] B. Fröhlich, *et al.*, “A quantum access network”, Nature 501, 69 (2013)
[6] P. Sibson *et al.*, “Chip-based Quantum Key Distribution”, arXiv:1509.00768 (2015)
[7] E. Diamanti and A. Leverrier, “Distributing Secret Keys with Quantum Continuous Variables: Principle, Security and Implementations”, Entropy 17, 6072 (2015)
[8] P. Jouguet, *et al.*, “Experimental demonstration of long-distance continuous-variable quantum key distribution”, Nature Photonics 7, 378 (2013)
[9] M. Ziebell, *et al.*, Proceedings of CLEO/Europe-EQEC, Munich, 21–25 June 2015

[10] A. R. Dixon, *et al.*, “Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate”, Opt. Exp. 16, 18790 (2008)
[11] R. Ursin, *et al.*, “The marathon race to an new atomic kilogram”, Europhysics News 40, 23 (2009)
[12] T. Schmitt-Manderbach, *et al.*, “Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km”, Phys. Rev. Lett. 98, 010504 (2007)
[13] P. Villoresi, *et al.*, “Experimental verification of the feasibility of a quantum channel between space and Earth”, New J. Phys. 10, 033038 (2008)
[14] D. Dequal, *et al.,* “Experimental single photon exchange along a space link of 7000 km”, Phys. Rev. A 93, 010301 (2016)
[15] G. Vallone*, et al*., “Experimental Satellite Quantum Communications”, Phys. Rev. Lett. 115, 040502 (2015)
[16] X-S. Ma, *et al.,* “Quantum teleportation over 143 kilometres using active feed-forward”, Nature 489, 269 (2012)
[17] M. Krenn, *et al*., “Communication with spatially modulated light through turbulent air across Vienna”, New J. Phys., 16, 113028 (2014)

2.2.3 Quantum Networks

A. Physical approach and perspective

Quantum networks extend from one-to-many access networks and trusted node backbone networks, built on weak-pulse QKD systems, to more advanced entanglement-based scenarios including quantum repeaters. The goal is to work towards a Pan-European quantum network based on backbone and access architectures to ensure a quantum-safe information infrastructure. Important aspects of implementation and security for new applications and protocols will be discussed in subsequent sections.

A long-term goal is to construct a fully quantum backbone network that will consist of quantum channels connecting nodes of small quantum processors. In contrast to point-to-point connections, such a quantum network could enable the creation of entanglement between any two points on earth. Quantum communication also allows secure access to the first quantum computer mainframes by other users in the network, who themselves only have simpler quantum devices, i.e. quantum computing in the 'cloud'. This is of interest since the first quantum computers are likely to be scarce. It could, however, be useful for 'blind quantum computation', i.e., the idea of letting an untrusted server do quantum computations on private data, with the security guarantee that the server is 'blind', in the sense that it has no access to the data.

The foundations of these architectures rely on the distribution and control of entanglement across complex quantum networks. Central to realising this is the most fascinating quantum phenomenon, teleportation. The development of complex quantum networks provides one of the most significant challenges in experimental and theoretical quantum physics today. By definition, this is highly multi-disciplinary and requires hybrid approaches on both a conceptual and technological level. Another motivation for using entanglement-based networks is that they could enable device-independent QKD, guaranteeing security independent of the devices being used.

Trusted Node Networks

Since the SECOQC QKD network demonstration in 2008 illustrated the concept of trusted-node QKD [1], the concept has been widely exploited. In any QKD scheme, the communicating parties must be in secure locations. Therefore, these can also be used to realise switching stations between multiple QKD systems, provided the operators at these nodes can be trusted. This trust requirement could be overcome by using classical, or even post-quantum, encryption protocols on the nodes, thus realising a quantum-safe network. This field is primarily dominated by fibre systems though it does open up the possibility for satellite systems to connect to a larger and more complex quantum network. These ideas have been demonstrated in networks in Vienna, Switzerland, Japan, South Africa and Canada and many trusted node networks are running continuously, both at a research and commercial level. Quantum networks are under construction in China (a 2000km backbone link between several local area networks), the UK (two large-scale metro networks connected by a backbone link) and Japan, and there are proposals for networks in Switzerland, Italy, South Korea and USA.

Entanglement Networks and Teleportation

Trusted-node networks provide one solution for extending quantum communication distances and complexity. Networks for the distribution of quantum resources in general will require entanglement-based schemes. Realising this requires quantum repeaters, but although their development progresses (along with the quantum memories necessary for their operation), it lags many years behind that of trusted node networks.

There remain significant challenges for the distribution of entanglement through complex fibre optic networks. For example, the synchronisation and stabilisation of these networks and the high-fidelity Bell state measurements (joint measurements between two systems, two photons or two electrons) necessary for teleportation and entanglement swapping, which are at the heart of all quantum repeater protocols, remain a considerable challenge. Similarly, for satellite systems where much of the Bell state measurements, teleportation and entanglement swapping need to adapt from stationary ground based systems to moving, satellite targets. There are several scenarios possible such as satellite to ground, or low orbiting platforms, as well as ground to (trusted) satellite schemes. Recently, the concept of a heralded qubit amplifier has been proposed in the context of device independent QKD. Indeed, this teleportation-based primitive has far-reaching applications for quantum networks, contributing to overcome loss and also herald the storage of quantum states in quantum memories. Field trials will be essential to understand their practical limits. Furthermore, understanding how to characterise and quantify these increasingly complex systems is an on-going problem that needs to go beyond standard approaches of quantum state and process tomography, especially if the security of the system is to be assured in a distributed network architecture. This effort represents a grand challenge for quantum network engineering.

Quantum Repeaters

In classical communication, information is transferred by modulating the intensity or phase of light fields. The amplitude of these modulations are detected (directly or interferometrically) by photodetectors, transformed into electrical current pulses, amplified by electronics, and sent to computers, phones, etc. This transformation of light into electrical signals forms a classical light-matter interface. In quantum information processing, this simple approach is inadequate as it destroys essential quantum characteristics as entanglement. Quantum communication requires a coherent storage interface - a quantum memory. Quantum memories are central to the concept of quantum repeaters. Quantum repeaters work by breaking large distances up into smaller ones, where entanglement can be distributed and stored in quantum memories. Once all of these smaller links are entangled, Bell state measurements can be used to join them together, thus increasing the communication link distance for a fully-quantum backbone network architecture. These quantum memories can also be thought of as small quantum processors and hence the idea of using similar techniques for connecting the nodes of a quantum computer or simulator.

There is a significant number of proposals for realising quantum network nodes ranging from atomic ensembles (cold and hot gases and solid state systems) and linear optics - perhaps the simpler and more advanced approach - to atom, ion and NV centre approaches that could take advantage of deterministic entanglement swapping operations. Other approaches based on quantum dots have been proposed, as well as hybrid schemes that combine coherent states and individual quantum systems.

Apart from the experimental work, realising such quantum networks requires theoretical work to design and validate realistic protocols. Some examples are to find benchmark parameters for quantum communication that can be used to assess and guide the design of quantum repeater architectures. A crucial feature is to identify and develop methods for distributing entanglement efficiently, using practical realistic quantum devices that can only perform slightly imperfect operations on a small number of qubits. Approaches based on quantum error correction, that negate the necessity of quantum memory, have been proposed. A recent review outlines the advantages of different approaches and different generations of quantum repeater architectures and highlights the engineering challenges they face [2]. A more detailed discussion on quantum memories is presented below and a detailed review of ensemble approaches using linear optics and discussions on several others can be found here [3].

B. State-of-the-art

Trusted node QKD systems have shown systems capable of fully automated operation, including self-compensation for environmental influences on the fibre link. The demonstrations have involved one-time pad encrypted telephone communication, secure (AES encryption protected) video-conferencing and re-routing experiments, highlighting basic mechanisms for quantum network functionality. In the SECOQC network built in 2008, the highest secure key rates was ~3 Kbps for a 32 km link with 7.5dB loss. Since then, the Tokyo QKD network has realised secure bit rates, which are over two orders of magnitude higher, despite higher loss (~14dB). Furthermore, several networks have shown continuous operation over extended periods of many months. Recently, experiments have addressed passive optical network (PON) implementations for QKD, covering 20 channels in the telecom band [4] and demonstrating the feasibility of point to multipoint (up to 64) networks [5]. Multiplexing of QKD and conventional data with a bandwidth of 40 Gbps has been demonstrated on installed fibre [6].

Teleportation experiments in the real world have been demonstrated in the Swiss fibre optic network (3x2 km) [7] as well as free-space transmission of teleported states in China (97 km) [8] and in the Canary Islands (144 km) [9]. The first marks an important step towards fibre-based quantum repeaters, and the second towards satellite systems. The synchronisation of independent sources for entanglement swapping has been realised using cw [10] and fs pulsed systems [11]. These results highlight the two extremes of operation, in terms of photon bandwidth, for such experiments. First proof-of-principle experiments for heralded amplification of qubits have been shown for Fock state, polarisation and time-bin qubits have been realised [12].

Quantum repeaters represent one of the most rapidly evolving areas of activity in the field and progress is largely linked to the work on quantum memories and interfaces, which will be discussed in the following sections. Here we focus on the demonstration of key primitives for quantum repeater links. Entanglement between photonic (flying qubits) and quantum memory systems has been demonstrated for atomic ensembles [13], single atoms [14,15] and solid state systems based on rare-earth ions [16], as well as NV centers [17]. The generation of entanglement between quantum memory nodes has also been shown for multiple candidate systems, including atomic ensembles [18], single atoms [19,20] and rare-earth ions [21] as well as diamonds over 1km [22]. Teleportation between quantum memories and photons has reached distances of 25km for multimode rare-earth ions schemes [23], importantly demonstrating Bell state measurements after both the qubit and half the entangled state have each been transmitted over 12.5km, marking an important milestone for real-world teleportation protocols. Deterministic teleportation between nodes in ensembles [18] and diamonds [17] provides an important landmark for the scalability of quantum networks.

Behind all of these experiments is an increased activity in more applied aspects of quantum communication, related to the synchronisation and stabilisation of distributed quantum networks involving a wide range of different quantum technologies.

C. Challenges

There is no clear leader for quantum networks and long distance quantum communication with dedicated programs in place across Europe and in the USA, Canada, Japan, Australia and China. In the next 5-10 years, we should see fibre optic systems that can beat the direct-transmission QKD distance limitation of around 300-400 km. Initially, quantum repeaters that can function over 1-10 km will provide the building blocks for longer transmission systems- these are the building blocks can provide a scalable route towards Pan-European and even global scale quantum communication. These distances will obviously need to be extended further, but not necessarily by much, since classical communication links are of the order of 50-100 km between amplification stages. One of the important aspects for quantum repeaters is the scaling of multiple quantum repeater links. Scalable quantum repeater systems will ensure that the concatenation of multiple links will extend quantum communication distances beyond this fundamental (loss-based) limit and away from the point-to-point network topologies. Another important aspect is to realise significant bit rates for quantum repeater links.

Efforts in the next few years should be focused on engineering quantum repeaters to work towards a quantum-safe backbone communication network, in unison with sources, interfaces and detectors specifically adapted to long distance transmission and demonstrating high fidelity Bell-state measurements. Challenges and directions of future work are thus similar to those already mentioned for these different technologies and, while many aspects have been realised, all need to be improved and demonstrated in one system. Furthermore, all the component quantum technologies, sources, detectors, as well as quantum memories and interfaces, are of critical importance for the quantum repeaters and these are discussed in detail in following sections.

D. Short-term goals (0-5 years)

- Certified trusted node systems;
- Field demonstrations of multiplexed and trusted node QKD systems running autonomously with Mbps secure key rates;
- Field demonstrations of quantum relays, exploiting quantum teleportation and entanglement swapping, over tens of kms with high fidelity (>90%) Bell-state measurements.

E. Medium-term goals (5-10 years)

- Commercial trusted-node QKD network;
- Incorporate deterministic strategies for sources, storage and entanglement swapping;
- Demonstrate coupling, via an optical quantum channel, between different quantum processing nodes;
- Increase rates of entanglement generation between network nodes;
- Demonstrate the distribution of multi-partite entanglement in a quantum network;
- Multi-node quantum repeater demonstration;

- Quantum repeater prototype beating the direct transmission distance.

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

- Demonstrate entanglement purification, distillation, and error correction primitives;
- Demonstrate quantum repeater >1000km.

G. Key references

[1] M. Peev *et al.*, “The SECOQC quantum key distribution network in Vienna”, New J. Phys. 11, 075001 (2009)
[2] S. Muralidharan, *et al.*, “Efficient long distance quantum communication”, arXiv:1509.08435 (2015)
[3] N. Sangouard, *et al.*, “Quantum repeaters based on atomic ensembles and linear optics”, Rev. Mod. Phys. 83, 33 (2011)
[4] J. Mora *et al.*, “Simultaneous transmission of 20x2 WDM/SCM-QKD and 4 bidirectional classical channels over a PON”, Opt. Exp. 20, 16358 (2012)
[5] B. Fröhlich, *et al.*, “A quantum access network”, Nature 501, 69 (2013)
[6] I. Choi, *et al.*, “Field trial of a quantum secured 10Gb/s DWDM transmission system over a single installed fiber”, Optics Express, 22, 23121 (2014)
[7] O. Landry, *et al.*, “Quantum teleportation over the Swisscom telecommunication network”, J. Opt. Soc. Am. B 24, 398 (2007)
[8] J. Yin, *et al.*, “Quantum teleportation and entanglement distribution over 100-kilometre free-space channels”, Nature 488, 185 (2012)
[9] X. S. Ma *et al.*, “Quantum teleportation over 143 kilometres using active feed-forward”, Nature 489, 269 (2012)
[10] M. Halder *et al.*, “Entangling independent photons by time measurement”, Nature Physics, 3, 692 (2007)
[11] R. Kaltenbaek *et al.*, “High-fidelity entanglement swapping with fully independent sources”, Phys. Rev. A, 79, 040302(R) (2009)
[12] N. Bruno, *et al.*, “Heralded amplification of photonic qubits”, Optics Express, 24, 125 (2016)
[13] H. Krauter, et al., “Deterministic quantum teleportation between distant atomic objects”, Nature Physics 9, 400 (2013)
[14] T. Wilk, *et al.*, “Single-Atom Single-Photon Quantum Interface”, Science 317, 488 (2007)
[15] W. Rosenfeld, *et al.*, “Towards Long-Distance Atom-Photon Entanglement”, Phys. Rev. Lett. 101, 260403 (2008)
[16] C. Clausen, *et al.*, “Quantum storage of photonic entanglement in a crystal”, Nature 469, 508 (2011)
[17] W. Pfaff, *et al.,* “Unconditional quantum teleportation between distant solid-state quantum bits”, Science 345, 532 (2014)
[18] K. Hammerer, *et al.*, “Quantum interface between light and atomic ensembles”, Rev. Mod. Phys. 82, 1041 (2010)
[19] S. Ritter, *et al.*, “An elementary quantum network of single atoms in optical cavities”, Nature 484, 195 (2012)

[20] J. Hofmann, *et al.*, “Heralded Entanglement Between Widely Separated Atoms”, Science 337, 72 (2012)
[21] I. Usmani, *et al.,* “Heralded quantum entanglement between two crystals”, Nature Photonics 6, 234 (2012)
[22] H. Bernien, *et al.*, “Heralded entanglement between solid-state qubits separated by three metres”, Nature 497, 86 (2013)
[23] F. Bussières, *et al.*, “Quantum teleportation from a telecom-wavelength photon to a solid-state quantum memory”, Nature Photonics 8, 775 (2014)

2.2.4 Implementation and Security

A. Physical approach and perspective

QKD is synonymous with security based solely on the laws of quantum physics. However, as with any security technologies, there are always potential weaknesses due to imperfections in the implementation. In the case of QKD, there are increasing efforts on testing quantum systems - quantum hacking - as researchers attempt to find potential side-channels or implementation weaknesses, which mean that the device is no longer described by its (idealistic) security model. There appear to be two strategies to deal with this issue: either building better devices that have no implementation flaws or defining the security in a way that is independent of the device and its implementation. The applied effort is focused on the first possibility with companies and (ethical) hackers working closely to test systems. Nonetheless, there is a clear need to bridge the gap between these idealistic security models and practical implementations with minimal assumptions. The same is true for the implementations of quantum protocols beyond QKD.

The move towards network operation requires closer collaboration with network engineers to deal with issues of operating in environments with optical amplifiers and switching stations. Concepts of virtual and software defined networks (SDN) also brings along an operational complexity that requires expertise from outside the traditional quantum technology community. There is increasing interest from industry to work towards resolving the associated challenges. As commercial systems reach for greater market uptake, these efforts are becoming increasingly important to assist with certification as well as developing standards for quantum communication devices and systems.

Recently researchers have revisited an idea that has been around since the first proposal for entanglement-based QKD [1]. This approach has been labelled Device-Independent QKD (DI-QKD) as it treats the devices as black boxes. The security is dependent solely on using a few input-output probabilities to calculate a relatively simple inequality – a Bell inequality. If the inequality is violated, the system is secure, independent of the internal workings of the device. Concepts such as device independent security and more recently, self-testing systems, provide a new paradigm, not only for security, but for characterising complex, distributed, quantum networks. We expect that the DI paradigm will be extended to quantum cryptographic protocols at large.

B. State-of-the-art

Dealing with implementation issues at an applied level requires close collaboration between those building and selling the QKD systems, technologies, operating networks and services, and those testing them. This approach has been well demonstrated for recent detection of side-channels [2]. Another approach to avoid tampering with the system is based on a 'quantum fuse'; if the system is probed, for example, with a strong laser pulse, the link is 'broken'. DI-QKD, on the other hand, is a relatively new concept and its experimental application requires unprecedented performance of the systems and component technologies. A couple of recent papers have started to bring this into the realms of experimental feasibility [3, 4]. Central to this was the concept of heralded photon amplifiers [5], which have also been realised experimentally in the visible [6, 7] and more recently, telecom regimes for Fock state and time-bin qubits [8]. Recently, the first loophole free Bell test were performed [9] which shows that DI security is in principle possible, although it is important to greatly increase the rate at which we can hope to produce encryption keys. Self-testing is another related concept where the effort is to minimise assumptions and to help better characterising quantum systems and technologies. This has primarily been a theoretical effort [10-12], although recently a first demonstration of a self-testing QRNG has been made [13]. The adaptation and demonstration of DI-QKD will also be important for future secure networks. In a further extension of this idea, heralded photon amplifiers have been proposed in a recent quantum repeater protocol [14] that is not only one of the most efficient but it also hints at the potential for DI scenarios across quantum networks. Perhaps the most promising approach is between the two extremes, where some components of the systems are made robust against attacks, such as measurement device independent (MDI) QKD [15] and detector device independent (DDI) QKD [16], which have recently been realised. A recent experiment [17] demonstrated a secure key rate over 1 Mbps for MDI-QKD, comparable to the best values achieved for conventional QKD.

C. Challenges

Efforts on both improved testing of quantum systems and device independent security have similar goals, but approach the task from different directions. Both have the aim of minimising the assumptions involved in secure quantum communication systems and to bridge the gap between the theoretical proofs and the practical security of the final implementation. European theory groups have been a driving force in this area, especially for the later, although experimental initiatives have already started in several European groups, as well as in China, Japan, Singapore, Canada and Australia.

D. Short-term goals (0-5 years)

- Security proofs for QKD systems that are optimised to cope with a wide range of experimental parameters including finite key lengths;
- Certification of QKD components and systems;

- Practical security against collective attacks, as well as quantum and classical side channels applied to practical systems;
- Experimental demonstrations of self-testing concepts;
- Experimental implementations that minimise side-channels and information leakage.

E. Medium-term goals (5-10 years)

- Practical security against collective attacks as well as quantum and classical side channels applied to trusted node networks – exploiting quantum and classical encryption techniques;
- Lab demonstration of device-independent QKD over 10km.

F. Long-term goals (> 10 years)

- Practical security for multi-node, switchable, quantum repeater networks.

G. Key references

[1] A. Ekert, "Quantum cryptography based on Bell's theorem", Phys. Rev. Lett. 67, 661 (1991)
[2] L. Lydersen *et al.,* "Hacking commercial quantum cryptography systems by tailored bright illumination", Nature Photonics 4, 686 (2010)
[3] A. Acín *et al.,* "Device-Independent Security of Quantum Cryptography against Collective Attacks", Phys. Rev. Lett. 98, 230501 (2007)
[4] N. Gisin, *et al.,* "Proposal for Implementing Device-Independent Quantum Key Distribution Based on a Heralded Qubit Amplifier", Phys. Rev. Lett. 105, 070501 (2010)
[5] T. Ralph and A. Lund, "Nondeterministic Noiseless Linear Amplification of Quantum Systems", Quantum Communication Measurement and Computing Proceedings of 9th International Conference, Ed. A. Lvovsky, 155 (AIP, New York 2009) - arXiv:0809.0326v1 (2009)
[6] G. Y. Xiang *et al.,* "Heralded noiseless linear amplification and distillation of entanglement", Nature Photonics 4, 316 (2010)
[7] F. Ferreyrol *et al.*, "Implementation of a Nondeterministic Optical Noiseless Amplifier", Phys. Rev. Lett. 104, 123603 (2010)
[8] N. Bruno, *et al.*, "Heralded amplification of photonic qubits", Optics Express, 24, 125 (2016)
[9] B. Hensen *et al*., "Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres", Nature 526, 682 (2015); L. K. Shalm, *et al.,* Phys. Rev. Lett. 115, 250402 (2015); M. Giustina, *et al.,* Phys. Rev. Lett. 115, 250401 (2015);
[10] D. Mayers and A. Yao, "Self testing quantum apparatus", Quantum Inform. Comput. 4, 273 (2004)
[11] M. McKague, *et al.,* "Robust Self Testing of the Singlet", J. Phys. A 45, 455304 (2012)
[12] C. C. W. Lim *et al*., "Device-Independent Quantum Key Distribution with Local Bell Test", Phys. Rev. X 3, 031006 (2013)
[13] T. Lunghi, *et al.*, "Self-Testing Quantum Random Number Generator", Phys. Rev. Lett. 114, 150501 (2015)

[14] J. Minar, *et al.,* "Quantum repeaters based on heralded qubit amplifiers", Phys. Rev. A 85, 032313 (2012)
[15] Y. Liu, *et al*., "Experimental Measurement-Device-Independent Quantum Key Distribution", Phys. Rev. Lett. 111, 130502 (2013)
[16] C.C.W. Lim *et al*., "Detector-device-independent quantum key distribution", Appl. Phys. Lett. 105, 221112 (2014)
[17] L. Comandar *et al.*, "Quantum cryptography without detector vulnerabilities using optically-seeded lasers", Nature Photonics 10, 312 (2016)

2.2.5 New Applications and Protocols

A. Physical approach and perspective

The field of quantum communication is still very young, having been essentially unknown until 25 years ago. As such, one should expect new ideas and leave open space for fundamental research. From the theoretical point of view, many quantum protocols have already been discovered for cryptographic tasks as well as applications beyond cryptography. Yet, we expect that the expansion of QKD systems into mainstream communication networks will spur many new applications to address emerging demands on our digital society. As mentioned, random numbers are a fundamental resource for many cryptographic and computational applications. If the size and cost of QRNG can be reduced, this will open up an enormous potential market, especially for the Internet of Things, whose potential is already under the scope of industry.

Digital Signatures is another primitive where a quantum analogue has recently been demonstrated. Bit commitment has also been demonstrated between Switzerland and Singapore, again exploiting standard QKD systems. Position-based cryptography provides a way to use the geographical location of a person as their (only) credential. There is an increasing interest as well in virtual, or software defined, networks, whose security could be facilitated by quantum-based encryption schemes. A major societal challenge for the whole world is the security of long-lived systems, even ever-lasting secure storage for example in securing health records over human lifetimes (around 1 century). This is a problem that looks out of reach for a purely algorithm-based approach, but initial proposols for this combine quantum and classical cryptographic techniques, for signatures, as well as secret sharing for data at rest combined with one-time pad, i.e. QKD, encryption for data in transit.

An area of interest that is emerging is related to exploiting quantum clocks to time stamp events. The security of such service could take advantage of quantum encryption. This would have the interesting possibility that both the clock signals, also used by national metrology labs, could be multiplexed with QKD signals, thus reducing overheads in developing quantum networks across Europe. Further afield, there are even proposals to use entanglement between distant telescopes to improve their precision and satellite-based systems would open up the possibility for tests on the foundations of quantum physics: for instance, the measurement of entanglement and the violation of Bell's inequalities by observers in moving and accelerated reference frames can test possible gravity-induced decoherence and shed light on the wave-function collapse.

Apart from that, there are still many open theoretical questions of crucial importance for quantum cryptography. These are related to the tolerance to noise of current protocols (both with one and two-way communication), the connection between single photon and continuous variable protocols, the search for more efficient and faster ways of distributing keys and quantifying their security. This requires studying the possibilities and limitations of quantum cryptography for general protocols when implemented with realistic quantum devices that are unavoidably subject to some imperfections.

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 manipulations and subsequent measurements by another two-step procedure that first measures the quantum states and then performs classical communication protocols on the resulting data to complete the task. Such an approach would be preferential in real implementations, as is illustrated in the case of quantum key distribution. It is important to study under which circumstances such a replacement can be done. As the complexity of quantum networks increases we also need to develop measurement and certification schemes that are both robust and that scale more favourably.

A relatively new idea is using quantum memories to perform local operations and store the results while the classical communication is going on in communication protocols, which require local operations and classical communication (LOCC). Transforming ideas of percolation to quantum networks is a relatively new concept, but one that also opens some fascinating possibilities for network distribution of entanglement. On a high level, an effective distribution of entanglement also demands a careful allocation of resources as given by an analogue of routing protocols for quantum networks.

B. State-of-the-art

In the domain of quantum cryptography, the possibility of a cheat sensitive quantum protocol to perform a private search on a classical database [1] has been proposed and recently experimental demonstrated [2]. Two-party cryptographic protocols, like bit commitment have also been shown to be feasible in an entanglement-based protocol [3] and more in a field trial between Switzerland and Singapore using commercial QKD systems [4]. Schemes for synchronising clocks [5] or performing 'blind computations' [6] have been proposed. A return to some of the foundational concepts has seen Bell inequalities find renewed importance for device-independent security [7] and the concept of device-independent quantum information processing is finding applications far beyond QKD. Important progress has also been made in developing new protocols for quantum repeater architectures themselves. A key concept that was recently introduced is the multimode capacity of quantum memories, which allows orders of magnitude increases in distribution rates [8]. Combining this with approaches that serialise distribution and even reduce the need for quantum memories [9] may hold the potential for high rates and long distances. The concept of heralded photon amplifiers opens up new possibilities for distributing quantum resources, for example, DI-QKD [10] and heralded quantum memories for quantum repeaters [11] both in the context of secure communication; however, these concepts should find a much broader field of applications. More concepts and detailed discussions can be found in a recent review paper on 'cryptography beyond QKD' [12].

C. Challenges

Quantum technologies are still very much in their infancy, and as such, we expect new application to arise as more groups, especially end-users, start to understand their potential.

D. Short-term goals (0-5 years)

- Investigate and demonstrate new protocols for QKD and beyond, possibly inspired by existing protocols as well as systems that combine aspects of quantum and classical cryptography;
- Develop tools to analyse general quantum cryptographic protocols to ensure robust implementation in the presence of losses and errors;
- Develop protocols for the security of long-lived systems and secret sharing exploiting quantum and classical cryptographic techniques.

E. Medium-term goals (5-10 years)

- Develop new quantum repeater protocols that are robust with respect to loss and low component efficiencies, and explore new verification strategies for multipartite quantum networks;
- Develop protocols for multi-node, and switchable, quantum networks.

F. Long-term goals (> 10 years)

- Quantum protocols for complex tasks (such as payment systems, electronic money).

G. Key references

[1] V. Giovannetti *et al.*, “Quantum Private Queries”, Phys. Rev. Lett. 100, 230502 (2008)
[2] M. Jakobi *et al.*, “Practical private database queries based on a quantum-key-distribution protocol”, Phys. Rev. A 83, 022301 (2011)
[3] N. Ng *et al.*, “Experimental implementation of bit commitment in the noisy-storage model”, Nature Communications 3, 1326 (2012)
[4] T. Lunghi, *et al.,* “Experimental Bit Commitment Based on Quantum Communication and Special Relativity”, Phys. Rev. Lett. 111, 180504 (2013)
[5] A. Tavakoli, *et al.*, “Quantum Clock Synchronization with a Single Qudit”, Scientific Reports 5, 7982 (2015)

[6] A. Broadbent, *et al.*, “Universal blind quantum computation”, Symp. Found. Comp. Sci., FOCS '09 50th Annual IEEE, 517 (2009)
[7] A. Acín *et al.,* “Device-Independent Security of Quantum Cryptography against Collective Attacks”, Phys. Rev. Lett. 98, 230501 (2007)
[8] C. Simon *et al*., “Quantum Repeaters with Photon Pair Sources and Multimode Memories”, Phys. Rev. Lett. 98, 190503 (2007)
[9] W. J. Munro, *et al*., “Quantum communication without the necessity of quantum memories”, Nature Photonics 6, 777 (2012)
[10] N. Gisin, *et al*., “Proposal for Implementing Device-Independent Quantum Key Distribution Based on a Heralded Qubit Amplifier”, Phys. Rev. Lett. 105, 070501 (2010)
[11] J. Minar, *et al*., “Quantum repeaters based on heralded qubit amplifiers”, Phys. Rev. A 85, 032313 (2012)
[12] A. Broadbent, *et al*., “Quantum Cryptography Beyond Quantum Key Distribution”, Designs, Codes & Cryptography, 78, 351 (2016)

2.2.6 Sources

A. Physical approach and perspective

Sources of quantum light in the discrete variable regime have traditionally relied on spontaneous parametric down-conversion (SPDC) in bulk crystals. This has been extended to periodically poled materials and waveguided devices, which have significantly higher efficiencies. The development of all-fibre entanglement sources, based on four-wave mixing, provide several new approaches ranging from standard fibres to photonic crystal fibres. Four-wave mixing in integrated photonic devices has also matured to the point where multiple sources can be realised on a single chip. Deterministic sources that avoid probabilistic multi-pair events, associated with the previous schemes, have advanced to the point where entangled photon pairs can be generated by the optical or electrical excitation of the bi-exciton state of a semiconductor quantum dot. This has allowed a single LED-like device for generating entangled light to be realised. Recent progress on implementing photonic cavities and waveguides allows efficient out coupling of the emitted photons. Single photon sources based on NV diamond centres and single molecules in solids have been realised and progress continues on single photon sources in diverse materials for sources ranging from the visible up to 1310 nm, and 1550 nm. In the continuous variable regime, sources of squeezed and entangled light typically rely on either parametric oscillators in bulk crystals or the Kerr effect in optical fibres.

B. State-of-the-art

Two important parameters for quantum light sources are bandwidth (BW) and efficiency - both creation (brightness) and coupling into other systems. Furthermore, the sources need to be adapted and developed to the desired application, for example, there are currently few systems that approach quantum memory bandwidths (1-100 MHz). First steps in resolving these limitations have been made for atomic [1-5] and telecom [6] wavelengths. All-fibre entanglement sources based on four-wave mixing [7] can provide a high degree of non-degeneracy and are well suited to entanglement distribution in asymmetric architectures or for heralded photon sources. Engineering photon pair sources to produce pure, factorable states has progressed to the telecom regime for ps pulsed systems [8]. True single photon sources based on semiconductor quantum dots have been demonstrated at visible, near infra-red and fibre optic wavelengths. These quantum dots can be monolithically integrated into semiconductor light emitting diodes to form convenient electrically driven single photon sources. Recent advances include near unity out coupling efficiency [9,10], a two-photon interference visibility of 89% using resonant optical excitation [11], and indistinguishability of distinct sources through electric field tuning [12]. Entangled photon pairs have been generated from the biexciton cascade of an optically [13] or electrically [14] excited quantum dot. Recent advances include a Bell parameter of 2.59 [15], high indistinguishability of pairs [16], extension to fibre wavelengths [17] and the demonstration of quantum teleportation using entangled LEDs [18].

For free-space sources, both entangled photon pairs as well as single-photon sources, it is preferable to use shorter wavelengths than for fibre networks, to limit the diffraction on the sending aperture, which is especially important for very long optical communication links. Diverse approaches to continuous variable quantum state sources [19,20] are under development as well as nonlinear interactions in atomic gas cells for discrete and continuous variable non-classical light sources.

C. Challenges

Europe is currently leading in efforts towards coupling narrow-band photonic and atomic systems, as well as developing on-demand solid state sources, and plays a leading role for CV sources, competing with Australia and Japan. Pulsed systems in the telecom regime are now well developed in most places. There are several regimes of operation under study: atomic systems with narrow bandwidths for quantum repeaters, satellite-based schemes where bandwidth requirements are less critical but the generation rates need to compensate limited transmission time windows due to satellite availability, and in between both of these, pulsed systems for quantum fibre optical networks (teleportation and entanglement swapping) where robustness against fibre length fluctuations needs to be balanced with high rates. The increasing complexity and diversity of quantum communication systems has also seen a much more sophisticated approach taken to engineering the sources, and in particular, the nonlinear interactions that are needed. The engineering of factorable, or pure, states of light will be crucial for future quantum communication networks.

D. Short-term goals (0-5 years)

- Photon pair sources capable of high (GHz clock) rates with coupling >90% and high fidelity (>90% HOM visibility) between independent sources without spectral filtering;
- Multiple photon pair sources on integrated photonic chips with coupling >90% and high fidelity (>90% HOM visibility) between independent sources without spectral filtering;

- Quantum dot photon sources capable of high rates with coupling >90% and high fidelity (>90% HOM visibility) between independent sources without spectral filtering;
- Development of efficient, stable, and pure sources of squeezed, entangled and single photon states that are able to reliably generate and grow large cat states;
- Narrow band photon pair sources capable of efficiently coupling quantum memories to telecommunication fibre networks.
- Efficient frequency conversion between quantum dots, quantum memories and fibre optic systems.

E. Medium-term goals (5-10 years)

- Deterministic single photon and photon pair sources with coupling > 90% and high fidelity (>90% HOM visibility) between independent sources without spectral filtering;
- Space qualified photonic sources for satellite-based quantum communication.

F. Long-term goals (>10 years)

- Arrays of deterministic single photon and photon pair sources with coupling > 90% and high fidelity (>90% HOM visibility) between independent sources without spectral filtering, for multi-photon applications.

G. Key references

[1] M. L. Scholz, *et al.*, “Statistics of Narrow-Band Single Photons for Quantum Memories Generated by Ultrabright Cavity-Enhanced Parametric Down-Conversion”, Phys. Rev. Lett. 102, 063603 (2009)
[2] A. Haase, *et al.*, “Tunable narrowband entangled photon pair source for resonant single-photon single-atom interaction”, Opt. Lett. 34, 55 (2009)
[3] X. H. Bao, *et al.*, “Generation of Narrow-Band Polarization-Entangled Photon Pairs for Atomic Quantum Memories”, Phys. Rev. Lett. 101, 190501 (2008)
[4] J. S. Neergaard-Nielsen, *et al.*, “High purity bright single photon source”, Opt. Exp. 15, 7940 (2007)
[5] J. Fekete, *et al.*, “Ultranarrow-Band Photon-Pair Source Compatible with Solid State Quantum Memories and Telecommunication Networks”, Phys. Rev. Lett. 110, 220502 (2013)
[6] E. Pomarico, *et al.*, “Waveguide-based OPO source of entangled photon pairs”, New J. Phys. 11, 113042 (2009)
[7] A. R. McMillan, *et al.*, “Narrowband high-fidelity all-fibre source of heralded single photons at 1570 nm”, Opt. Exp., 17, 6156 (2009)
[8] N. Bruno *et al.,* “Pulsed source of spectrally uncorrelated and indistinguishable photons at telecom wavelengths”, Optics Express, 22, 17246 (2014)
[9] P. Lodahl, *et al.*, “Interfacing single photons and single quantum dots with photonic nanostructures”, Rev. Mod. Phys. 87, 347 (2015)
[10] N. Somaschi, et al., “Near-optimal single-photon sources in the solid state” Nature Phot., 10, 340 (2016)

[11] A Bennett *et al.*, "Cavity-enhanced coherent light scattering from a quantum dot", arXiv:1508.01637 (2015)
[12] R Patel *et al.*, "Two-photon interference of the emission from electrically tunable remote quantum dots", Nature Photonics 4, 632 (2010)
[13] R Stevenson *et al.*, "A semiconductor source of triggered entangled photon pairs", Nature 439, 179 (2006)
[14] C Salter *et al.*, "An entangled-light-emitting diode", Nature 465, 594 (2010)
[15] C Varnava *et al.*, "An entangled-LED driven quantum relay over 1 km", arXiv:1506.00518 (2015)
[16] M Muller *et al.*, "On-demand generation of indistinguishable polarization-entangled photon pairs", Nature Photonics 8, 224 (2013)
[17] M Ward *et al.*, "Coherent dynamics of a telecom-wavelength entangled photon source", Nature Communications 5, 3316 (2014)
[18] J Nilsson *et al.*, "Quantum teleportation using a light-emitting diode", Nature Photonics 7, 311 (2013)
[19] H. Vahlbruch *et al.*, "Observation of Squeezed Light with 10-dB Quantum-Noise Reduction", Phys. Rev. Lett. 100, 033602 (2008)
[20] R. Dong *et al.*, "Experimental evidence for Raman-induced limits to efficient squeezing in optical fibers", Opt. Lett. 33, 116 (2008)

2.2.7 Quantum memories and interfaces

A. Physical approach and perspective

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

B. State-of-the-art

The first quantum memory in mesoscopic cold atomic ensembles [1-3] achieved storage times of order of 10 microseconds, with a maximum storage and retrieval efficiency of 18%. Today, the state of the art in terms of storage time is around 100 ms [4], hence 10 thousand times longer. However, the storage efficiency in that experiment was only a few percent. The highest retrieval efficiencies demonstrated to date for single stored excitations are 50% in free space [5] and around 80% in cavities [6,7]. But these high efficiency demonstrations featured short storage times (a few microseconds or less). Recently Bao et al. [8] demonstrated a long-lived and efficient cold gas quantum memory, reaching 73% efficiency and 3 ms storage time. The highest combined write and retrieval efficiency of any quantum memory was achieved in a room-temperature atomic gas, achieving 78% [9]. Another demonstration featured a very large bandwidth of 1.5 GHz [10]. Storage and retrieval of quantum continuous variables has also been demonstrated in room-temperature atomic vapours [11-13]. Unconditional storage fidelities of up to 70% and storage times of a few milliseconds have been reached.

Solid-state quantum memories based on rare-earth doped crystals have gained interest, since the first demonstration of a memory at the single photon level in 2008 [14]. Storage efficiencies over 50% have been achieved [15], and storage times increased into the millisecond regime at the single photon level [16]. Storage of entanglement has also recently been demonstrated in rare-earth crystals [17-18], with storage efficiencies up to 20%. An important feature of these systems is the potential for multimode storage, with demonstrations up to 64 stored modes of weak coherent states has been shown [19] with conditional qubit fidelities of 93%. Recently rare-earth crystals have been interfaced with other quantum platforms, such as superconducting resonators [20] and photonic nano-cavities [21]. Frequency conversion quantum interfaces connecting atomic quantum memories to telecom wavelengths have also been developed [22, 23].

C. Challenges

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

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

- Improve input/output efficiencies and coupling to fibre optic channels for diverse quantum memories suitable for quantum repeaters;
- Improved quantum memory storage efficiency > 50%;
- Improved quantum memory storage time > 100ms;
- Improved multi-mode storage capacity > 100 modes;
- High efficiency coupling, including frequency conversion, from quantum memories to communication channels;
- Reduction of overall experimental complexity for future scalability.

E. Medium-term goals (5-10 years)

- Improved quantum memory storage efficiency > 70%;
- Efficient frequency conversion between microwave systems and quantum memories and between quantum memories and fibre networks;
- High fidelity storage (short storage times) > 95%.

F. Long-term goals (>10 years)

- Improved quantum memory storage efficiency > 90%;
- High Fidelity (> 95%), long lifetime (> 100ms), multimode (> 100 modes), high efficiency (> 90%) quantum memory (combined characteristics for a single system).

G. Key references

[1] T. Chaneliere, *et al.*, "Storage and retrieval of single photons transmitted between remote quantum memories", Nature 438, 833 (2005)
[2] M. D. Eisaman, *et al.*, "Electromagnetically induced transparency with tunable single-photon pulses", Nature 438, 837 (2005)
[3] K. S. Choi, *et al.*, "Mapping photonic entanglement into and out of a quantum memory", Nature 452, 67 (2008)
[4] A. G. Radnaev, *et al.*, "A quantum memory with telecom-wavelength conversion", Nature Phys. 6, 894 (2010)
[5] J. Laurat, *et al.*, "Efficient retrieval of a single excitation stored in an atomic ensemble", Opt. Exp. 14, 6912 (2006)
[6] J. Simon, *et al*., "Interfacing Collective Atomic Excitations and Single Photons", Phys. Rev. Lett. 98, 183601 (2007)
[7] E. Bimbard, *et al,* "Homodyne Tomography of a Single Photon Retrieved on Demand from a Cavity-Enhanced Cold Atom Memory", Phys. Rev. Lett. 112, 033601 (2014)
[8] X.-H. Bao, *et al*., "Efficient and long-lived quantum memory with cold atoms inside a ring cavity", Nature Physics 8, 517 (2012)
[9] M. Hosseini, *et al*., "Unconditional room-temperature quantum memory", Nature Phys. 7, 794 (2011)
[10] K. F. Reim, *et al*., "Single-Photon-Level Quantum Memory at Room Temperature", Phys. Rev. Lett. 107, 053603 (2011)
[11] B. Julsgaard, *et al*., "Experimental demonstration of quantum memory for light", Nature 432, 482 (2004)
[12] J. Appel, *et al.*, "Quantum Memory for Squeezed Light", Phys. Rev. Lett. 100, 093602 (2008)
[13] J. Cviklinski, *et al.*, "Reversible Quantum Interface for Tunable Single-Sideband Modulation", Phys. Rev. Lett. 101, 133601 (2008)
[14] H. de Riedmatten, *et al.*, "A solid-state light–matter interface at the single-photon level", Nature 456, 773 (2008)
[15] P. Jobez, *et al*., "Cavity-enhanced storage in an optical spin-wave memory", New J. Phys. 16, 083005 (2014)
[16] P. Jobez, *et al.,* "Coherent Spin Control at the Quantum Level in an Ensemble-Based Optical Memory", Phys. Rev. Lett. 114, 230502 (2015)
[17] C. Clausen, *et al.*, "Quantum storage of photonic entanglement in a crystal", Nature 469, 508 (2011)
[18] E. Saglamyurek, *et al.*, "Broadband waveguide quantum memory for entangled photons", Nature 469, 512 (2011)
[19] I. Usmani, *et al.*, "Mapping multiple photonic qubits into and out of one solid-state atomic ensemble", Nature Commun. 1, 12 (2010)

[20] S. Probst, *et al.*, “Anisotropic Rare-Earth Spin Ensemble Strongly Coupled to a Superconducting Resonator”, Phys. Rev. Lett. 110, 157001 (2015)
[21] T. Zhong, *et al*., “Nanophotonic coherent light-matter interfaces based on rare-earth-doped crystals”, Nature Communications 6, 8206 (2015)
[22] A. G. Radnaev, *et al*, “A quantum memory with telecom-wavelength conversion”, Nature Phys. 6, 894 (2010)
[23] B. Albrecht, *et al*, “A waveguide frequency converter connecting rubidium-based quantum memories to the telecom C-band”, Nature Comm 5, 3376 (2014)

2.2.8 Detectors

A. Physical approach and perspective

All photonic approaches to quantum information technology rely upon an efficient detection technology. Although single photon detectors are commercially available, these are relatively simple digital devices, which detect the presence or absence of one or more photons. Future detector technologies will not only need a dramatically higher detection efficiency but also considerable lower dark count rates, as well as a timing jitter that does not limit the transmission rates. The commercial detection systems are based on semiconductors, single photon avalanche photodiodes (SPADs), such as Silicon (400-1000 nm) and InGaAs/InP (1100-1700 nm). These are robust and generally only require electric cooling. Traditionally these detectors have operated at low rates, the InGaAs in particular usually needed to be gated at rates of around 1MHz, although recent approaches have seen this significantly increase into the GHz regime.

Alternative approaches include superconducting devices, either transition-edge sensors (TES) that have shown near unit efficiencies but remain relatively slow, or superconducting nanowire single photon detectors (SNSPD) that have been undergoing rapid development in the last few years. Initially developed using NbN, they were capable of high-speed operation (both low jitter and high count rates) but had only realised moderate efficiencies. Recently, SNSPD using WSi and MoSi, have been realised that combine high efficiency, low noise and fast operation all in one device. All of these superconducting devices have photon number resolution potential, which is useful for many entanglement-based protocols. The need for cryogenic cooling is offset by the potentially high performance.

For continuous variable (CV) measurements, single-photon resolution is not needed. There, apart from the quantum efficiency and bandwidth, the signal to noise ratio of the detector module is important. This is far from an extensive list, but focuses on the most advanced or promising technologies in the context of quantum communication.

B. State-of-the-art

A severe limitation of today’s photon detection technology is the maximum count rate. For example, InGaAs/InP SPADs have been traditionally operated in a gated mode with a maximum repetition frequency of 1-10MHz and a maximum count rate of 100kcps. However, this field has recently been reinvigorated with novel work on the operating electronics providing advances in rapid gating (GHz) [1,2] and continuous (free-running) [3] operation opening up new regimes of operation and performance. This is also being extended into the Si detection band with high efficiency, > 70% and PNR capabilities demonstrated [4]. The superconducting devices have demonstrated photon number resolution capability and high efficiency in TES > 90% systems [5]. Recently, SNSPDs using WSi have been realised that have high system detection efficiency (> 90%), low dark count rate (< 1 counts per second), low timing jitter (< 100 ps), and short reset time (< 100 ns) for telecom wavelengths [6]. Several start-up companies have already begun to commercialise the NbN SNSPD technologies. A new material, MoSi, has now shown efficiencies around 80% at 2.5K [7], which is far more practical temperature than either the TES or WSi devices. In the continuous variable regime, several groups report quantum efficiencies approaching 100% using commercially available PIN diodes with increasing bandwidth (>100MHz) and signal-to-noise ratios. Conceptually, the strict separation between discrete and continuous detection schemes is complemented by hybrid detection approaches [8,9]. A detailed review of single photon detectors has recently been realised [10].

C. Challenges

Europe and Japan are currently leading the way for the SPAD detection schemes, while the US is a clear leader for superconducting materials and devices. The development of SNSPDs is becoming more widespread, with Europe starting to play a leading role.

D. Short-term goals (0-5 years)

- Explore new operating regimes - faster (> 2 GHz clock rate), higher efficiency (> 25% for InGaAs/InP), and adapt devices (semiconductor and electronics) for specific applications, e.g. peak efficiency wavelengths;
- Develop local oscillator phase retrieval techniques for weak coherent state homodyne measurements in fibre systems;
- Recent improvements for detectors - dark counts (< 1 Hz), detection efficiency (> 90%), low jitter (< 100 ps) (demonstrated in a single system) need to reproduced by more groups, along with improved recovery times and detection rates.

E. Medium-term goals (5-10 years)

- High-speed (GHz detection rates) photon detectors, or detection schemes;
- Photon number resolving detectors with high efficiency (> 90%) and low noise (< 1 Hz) and low jitter (< 100 ps)

F. Long-term goals (>10 years)

- High-speed, high-efficiency, scalable photon detector arrays.
- On-chip photon detectors integrated with other quantum technologies and photonic circuits.

G. Key references

[1] Z. L. Yuan, *et al.*, “High speed single photon detection in the near infrared”, Appl. Phys. Lett. 91, 041114 (2007)
[2] J. Zhang *et al.*, “2.23 GHz gating InGaAs/InP single-photon avalanche diode for quantum key distribution”, Proceedings of the SPIE - The International Society for Optical Engineering, 76810Z (2010)
[3] B. Korzh, *et al.*, “Free-running InGaAs single photon detector with 1 dark count per second at 10% efficiency”, Appl. Phys. Lett. 104, 081108 (2014)
[4] O. Thomas, *et al.*, “Efficient photon number detection with silicon avalanche photodiodes”, Appl. Phys. Lett. 97, 031102 (2010)
[5] A. E. Lita, *et al.*, “Counting near-infrared single-photons with 95% efficiency”, Opt. Exp., 16, 3032 (2008)
[6] F. Marsili, *et al.*, “Detecting single infrared photons with 93% system efficiency”, Nature Photonics 7, 210 (2013)
[7] V. B. Verma, *et al.*, “High-efficiency superconducting nanowire single-photon detectors fabricated from MoSi thin-films”, Optics Express, 23, 33792 (2015)
[8] C. Wittmann, *et al.*, “Demonstration of Near-Optimal Discrimination of Optical Coherent States”, Phys. Rev. Lett., 101, 210501 (2008)
[9] F. Monteiro, *et al.,* “Revealing Genuine Optical-Path Entanglement”, Phys. Rev. Lett. 114, 170504 (2015)
[10] M. D. Eisaman, *et al.*, “Single-photon sources and detectors”, Rev. Sci. Instrum. 82, 071101 (2011)

2.2.9 Virtual Facilities needs

Quantum engineering

- Chip-based solutions for QRNGs to reduce size and cost, as well as to improve reliability;
- Faster electronics for increased application-dependent performance incorporating sources, detectors, QRNGs, low-loss phase and amplitude modulators and their integration. This is mainly a (non-trivial) 'quantum opto-electronics' engineering problem;
- Incorporate integrated photonics into prototype systems as well as develop low-cost, compact, possibly hand-held, QKD systems;
- High-speed (>10GHz) phase and amplitude modulators suitable for QKD;
- Develop integrated photonic chip solutions, using e.g. silicon photonics or InP photonics;
- Certification of QKD systems;
- High-speed electronics, e.g. FPGA, possibly including expansion for multi-Gbps QRNG with low latency;
- Develop and test quantum sources and detectors compatible with the harsh environment in space;
- Compact and robust high photon flux sources - depending on the architecture and protocol, e.g. the systems must operate in short burst when satellites are in view, or backbone fibre network operation;

- Robust systems that can be space certified and withstand launch g-forces as well as being immune against the radiation in space;
- Network ready (telecom standards) trusted nodes with multipoint and switchable functionality;
- Integrated photonic solutions for heralded photon, and qubit, amplifiers;
- Develop quantum repeater (Telecom) compatible quantum memories and interfaces;
- Tamper proof packaging for QKD systems;
- Optical fuse technology;
- New approaches and materials for high (GHz clock) rate photon pair sources;
- Integrated photonics for photon pair sources, also addressing issues of coupling to more complex waveguide circuits – passive and active - and detectors;
- Development of space certified photonic sources;
- Efficient interfacing of sources of photonic entanglement and memory devices;
- Improved materials: host crystals, isotopically and pure dopants, as well as implantation techniques and waveguide writing;
- Develop efficient filtering techniques for improved signal to noise characteristics;
- Small closed-cycle cryogenic coolers (T = 1-3K);
- New materials and device structures for improved photon detection characteristics;
- High speed, low latency electronics, suitable for single photon, photon number resolving, and array detection systems;
- Explore new materials for SNSPDs, e.g. that might operate at higher temperatures;
- Develop compact and robust (prototype) photon detection schemes for technology transfer;
- Develop solutions for single photon detectors exploiting, and compatible with, integrated photonics platforms.

Quantum Control

- Network systems management for multiplexing, switching and software defined (SDN) network operation;
- Development of more efficient error correcting codes, possibly hybrid quantum-classical schemes;
- Stabilisation and synchronisation for distributed entanglement-based networks;
- Network systems management for multiplexing, switching and software defined (SDN) network operation;
- Development of more efficient error correcting codes, possibly hybrid quantum-classical schemes;
- Optimised microwave spin echo techniques for long lifetimes;
- Optimised broadband (GHz) Pi-pulses;
- Optimised optical pumping techniques.

2.3. Quantum Simulation

The idea of quantum simulation goes back to Richard Feynman, who suggested that interacting quantum systems could be efficiently simulated employing other precisely controllable quantum systems, even in many instances in which such a simulation task is expected to be inefficient for standard classical computers [1].

In general, the classical simulation of quantum systems require exponentially large resources, as the dimension of the underlying Hilbert space scales exponentially with the system size. This scaling may be significantly altered by employing appropriate representations of the quantum state valid in specific situations. Tensor network methods such as the density-matrix renormalisation group (DMRG) approach [2] allow for assessing ground state properties in certain situations, and so do Monte Carlo sampling methods [3]. Still, such classical (and some quantum) simulation methods are generally applicable only to restricted classes of problems, and must come to an end at some point. In physical terms, the attainable systems sizes are often rather small and it seems highly unlikely that these classical tools will be powerful enough to provide a sufficient understanding of the full complexity of many-body quantum phenomena. In a language of complexity theory, approximating the ground state energy of local Hamiltonian problems is QMA-hard [4], and time evolution under local Hamiltonians is BQP complete [5], so both amount to computationally hard problems.

Quantum simulators promise to overcome some of these limitations. This section is structured in a way such that first general concepts of quantum simulation and theoretical ideas are being presented, before turning to elaborating on actual physical platforms that actually realise instances of quantum simulators.

2.3.1. General concepts of quantum simulation

A. Physical approach and perspective

The term quantum simulator refers to a number of closely related concepts of devices that aim at simulating complex quantum systems, making use of highly controlled quantum systems. One distinguishes

- static quantum simulators [6,7] - probing static properties of interacting quantum many-body systems such as ground state features - from
- dynamical quantum simulators [8,9], probing properties related to non-equilibrium.

In terms of how the simulation is performed, one discriminates

- digital quantum simulators [10] - which are based on quantum circuits implemented on a quantum computer, and may in principle be made fault tolerant - from
- analog quantum simulators, simulators that reconstruct the time evolution of an interacting quantum system under precisely controlled conditions [11]. The

perspective arising from analog simulators specifically is that a large number of constituents can be addressed and experimented with, even using architectures that are available with present technology.

Quantum simulation offers new insights into phenomena of complex quantum systems, with applications ranging from condensed matter physics over statistical physics, high-energy physics and possibly even energy transfer in biological systems [12]. It is conceivable that quantum simulators help to interpret measurement results originating from sophisticated measurement techniques, e.g., from 2D electronic spectroscopy [13].

Due to the precise control over the Hamiltonian parameters, such quantum simulators provide a deeper understanding of the effects of inter-particle interactions and their influence on the overall properties of the system and could therefore even be used in the quest to artificially engineer desirable materials. A first step in this endeavour is usually to identify the appropriate underlying Hamiltonian in the first place, which is then probed by the actual quantum simulation.

There are a number of physical platforms that allow for controlled quantum simulations, at different levels of maturity at the present stage. The subsequent subsection is entirely dedicated to discussing such architectures. Indeed, highly promising advances have been achieved in these different systems, which will be laid out in detail below. Experimental platforms for quantum simulation comprise

- ultra-cold atomic and molecular quantum gases, specifically systems of cold atoms in optical lattices or continuous systems confined by atom chips [2],
- ultra-cold trapped ions [7,10],
- polariton condensates in semiconductor nanostructures [14],
- circuit-based cavity quantum electrodynamics [15],
- arrays of quantum dots [16],
- Josephson junctions [17] and
- photonic platforms [18].

Any problem for which no satisfactory analytical solution or classical simulation approach is known is a potential candidate for a quantum simulation. Some examples include:

- Any ground state problem of an interacting quantum system that cannot be tackled with any classical method is a candidate for a quantum simulation [19]. This applies, in particular, to frustrated spin systems for which quantum Monte Carlo methods [3] are not applicable, or for which the sign problem is an obstacle. Strong interactions put systems out of reach for mean-field approaches or ones based on density functional theory. Paradigmatic examples of this sort are the Heisenberg anti-ferromagnet on the Kagomé lattice or an anisotropic triangular lattice.

- Unbiased Quantum Monte Carlo methods also specifically fail for fermionic models, such as the Hubbard model in two dimensions, which is a strong candidate to explain the mechanism behind cuprate high-temperature superconductors, in contrast to the situation in one spatial dimension [20]. Indeed, even for an array of weakly coupled 2D Fermi-Hubbard models for spin-½ electrons the phase diagram is under controversial debate.
- A similar situation holds true for quantum chromodynamics at large densities and temperatures, e.g., in a quark-gluon plasma, which again renders such problems particularly interesting for quantum simulations.
- Systems subject to synthetic gauge fields are candidates for quantum simulations and are beginning to be probed in the laboratory [21].
- Dynamical problems of quantum systems out of equilibrium are also important candidates. While it is possible to keep track of short-time dynamics in one-dimensional systems using tensor network methods [22-25], such as t-DMRG or other variants of the density-matrix renormalisation group approach [3], this is no longer true for long times, due to the linear growth of entanglement entropies [25] in time. This renders quenched many-body systems particularly suitable candidates for quantum simulations [8].
- Disordered systems (even at the level of mean field interactions) can also be inaccessible to classical simulation techniques. Indeed, results from Hamiltonian complexity suggest that such systems cannot be simulated efficiently in worst case complexity. In the quantum setting, such problems may be addressed using quantum simulated annealing that combines classical minimisation and optimisation steps with exploration of the configuration space due to quantum tunnelling. To this extent, photonic [48] or cold-atom and ion platforms seems highly promising to address such questions [49-50,35].
- It has been argued that properties in biological systems may be accessible to quantum simulations. This in particular applied to energy transfer in biological systems [12].
- Sampling problems such as boson sampling may in a sense be viewed as an instance of a quantum simulation [26].
- Physical systems inspired by gravitational physics (including quantum gravity) or cosmological questions can be explored.

B. State-of-the-art

As early as 1982, Richard Feynman suggested the idea of a quantum simulator, along with presenting the core concept of a quantum computer [1]. He observed that a classical Turing machine is presumably unable to efficiently simulate quantum dynamics and suggested that the hypothetical device of a quantum simulator may well be able to do so. He not only introduced the basic idea of a quantum simulator in his published script of a keynote speech, but discussed sophisticated notions of simulation times and notions of simulation, and even contemplated blueprints for potential architectures. This basic idea was further substantiated by work showing that a universal quantum computer was indeed able to efficiently keep track of the dynamics of any local quantum system [27], allowing for precise error analysis by means of the Trotter formula. Since then, the research field of quantum simulation has been flourishing and developing into a core field within quantum information processing in its own right, addressing notions of simulating complex quantum systems in several readings and ramifications.

A working definition of a quantum simulator can be given as follows: A quantum simulator is any physical quantum system precisely prepared or manipulated in a way aimed at learning some interesting property of an interacting complex quantum system. More specifically:

- A quantum simulator is an experimental system that mimics an interacting quantum system with many degrees of freedom (from condensed-matter, high-energy physics, cosmology or quantum chemistry).
- The simulated models have to solve an interesting problem and further our understanding of the challenges of the above-mentioned areas of physics.
- The simulated models should be expected to be computationally intractable for classical computers, and some evidence should be given for this expectation.
- A quantum simulator should allow for broad control of the parameters of the simulated model, and for control of the preparation, manipulation and detection of the states of the system.
- It can be helpful to be able to set the parameters in such a way that the model becomes tractable using classical simulations for purposes of validation. At the same time it should be clear that the certification of a quantum simulator does not necessarily require the efficient classical simulation of certain parameter regimes.

Quantum simulators are devices devised to outperform classical means of simulation. Before turning to architectures for quantum simulation, it is helpful to be reminded of classical simulation methods aimed at simulating quantum many-body systems. It is one of the key results of the field of Hamiltonian complexity to identify ultimate obstacles that any such classical simulation must face [19]: For example, to approximate the ground state energy of an interacting local Hamiltonian problem to within polynomial accuracy in the number of particles of the model is QMA-hard [4], limiting the hopes that a universal classical simulation of such models of key importance in condensed matter physics could be achieved. Still, for many practical purposes, classical simulations of quantum systems are possible for many models and in many regimes, at least to the level of a heuristic understanding.

- Integrable models in the sense of being Bethe integrable are known in one physical dimension [20]. Also, important instances of higher-dimensional quantum systems that can be exactly solved in a way are known (even though the precise meaning of an exact solution varies from method applied), such as the celebrated Kitaev model [28], or non-interacting models. Integrable models play a paradigmatic role as established benchmarks for numerical methods or quantum simulations.
- Various kinds of mean field methods can be used to describe static, thermodynamic and even dynamical properties of certain quantum systems well [29]. These methods include various kinds of Hartree and Hartree-Fock methods,

Gross-Pitaevskii type approaches for bosons, Bogoliubov-de Gennes theory, Bardeen-Cooper-Schrieffer theory, Gutzwiller ansatz and others. Mean field methods typically work comparably well for weakly interacting systems in high dimensions, when the role of quantum fluctuations is less significant.

- Variational methods, such as the Ritz method, can be used to obtain upper bounds on the ground state energy and sometimes even a "perfect" ansatz for the many body ground state wave function can be provided - as it happens e.g. in the case of the fractional quantum Hall effect (FQHE) and Laughlin wave function [30].
- Tensor network methods can be seen as refined instances of variational methods. The DMRG approach [3] that simulates ground states of interacting 1D quantum systems essentially to machine precision can be viewed as a variational principle over matrix product states [22]. The reason that such approaches work so well is that ground states of gapped models satisfy what is called an area law for the entanglement entropy [25]. Tensor network methods also allow for the classical simulation of classes of interacting higher-dimensional systems [23-25].
- If applicable, quantum Monte Carlo methods are powerful methods to simulate interacting quantum systems by means of suitable sampling techniques. Numerical algorithms requiring polynomial effort are e.g. known to exactly study static properties of bosonic systems without geometric frustration [3,31].
- Density-functional theory is particularly important in materials science to investigate the electronic structure principally in the ground state of many-body systems. It is enormously useful then interactions are not too strong [32]. Viewed from the perspective of complexity theory, it is an QMA-hard problem to find the universal functional in density functional theory [33].

In all physical architectures mentioned [6-12,14-18], enormous progress towards realising a fully-fletched quantum simulator have been achieved in recent years. This will be discussed in detail in the subsequent subsection. From the conceptual perspective, it seems important to note that steps towards realising dynamical analogue simulators have been experimentally implemented [8,34-36], including disordered models [35], in a way that show evidence of the quantum simulator outperforming classical supercomputers [3,34,35]. Here, quenched many-body dynamics is kept track of, going beyond what the best classical simulation algorithms can achieve. Digital simulation is progressing at a similar pace [10,37], where the real-time dynamics of lattice gauge theories in a few-qubit quantum simulator has been monitored. The realisation of a fully-fletched either digital or analogue quantum simulator for which there is a strong claim of outperforming classical computers is still outstanding.

C. Challenges

Quantum simulations allow to probe and explore properties of complex quantum systems under precisely controlled conditions, with significant progress both in theory and experiment. Still, from the conceptual perspective, some problems are still open. This includes in particular the

- identification of models which are presumably computationally difficult for classical simulations, and yet interesting and important from a physical point of view, the
- development of validation and verification tools for quantum simulators and classical simulation methods that can be used to capture the functioning of the quantum simulator in certain regimes and the
- design of experimental setups and implementations.

In all of these aspects there has been an enormous progress over the last 10 years: still there are very many open problems and challenges [38,39]. Some computational complexity results relating to tasks of quantum simulators are known, such as the QMA-hardness of approximating ground state energies [4] which not even a presumed quantum computer can overcome. Other similar results, such as the computational difficulty of computing long-time dynamics [5], leave room for the computational superiority of quantum simulators over classical ones [34,35]. Still, one has be aware that these are results in worst case complexity, leaving room for improvements of classical simulation methods for practically relevant scenarios.

An important milestone in the quest for realising quantum simulators is to achieve what is often called ‘quantum supremacy’. This term refers to realising some quantum machine or simulator for which a strong claim can be made that it outperforms classical devices in their computational power [40]. So-called intermediate problems such as boson sampling [26], or - possibly more to the point of quantum simulation - instantaneous quantum polynomial time (IQP) circuits [41], may be key to identifying quantum simulators that fulfill the promise of achieving ‘quantum supremacy’. These are tasks that do not relate to universal quantum computing, but for which there is still strong evidence that no efficient classical algorithm can be found.

A key challenge is to find out whether the device has actually correctly performed the quantum simulation. This constitutes a particular important and intriguing problem in situations that are not classically attainable: The quantum simulator is performing tasks that one cannot efficiently keep track of, and still one would like to have evidence that the quantum simulator has functioned accurately. A commonly applied approach is that even the entire family of models characterised by some parameters to be quantum simulated may be inaccessible by classical means - still in suitable regimes of parameters these models become fully or at least partially accessible for classical simulation. In some instances, the statements on the correctness of a quantum simulation can be made even without having to predict the outcome of the simulation [42]. Novel tools of tomography or state certification [43-47] allow for learning about the unknown quantum state at a given instance in time.

At the same time, profound conceptual questions arise: If error correction and fault tolerance are not available, it is still not fully understood to what extent quantum simulators outperform classical computers. The verification and certification require classical simulation methods to be feasible in parameter regimes of functioning of quantum simulators. Nevertheless, if a concise answer to this and related questions can be established, quantum simulators will surely play a pivotal role in our study of quantum many-body physics and allow to tackle the many intriguing and complex challenges related to it. Moreover, even before these questions of verification and certification are completely resolved, analogue quantum simulators give us a novel tool to explore and understand robust features in interacting many-particle quantum systems that are beyond the reach of classical computers.

D. Short-term goals (0-5 years)

- Identify quantum simulation schemes that have the potential to reach quantum supremacy.
- Find experimentally realisable schemes for quantum simulation in existing architectures.

E. Medium-term goals (5-10 years)

- Realise quantum simulators that show superior performance compared to classical simulators in a strong sense.
- Identify the potential of simulating lattice gauge theories, high-Tc superconductors, topological systems, and systems from quantum chromodynamics.

F. Long-term goals (>10 years)

- Perform large-scale quantum simulations to tackle key questions in physics, materials science and quantum chemistry.

G. Key references

[1] R. Feynman, Simulating physics with computers, Int. J. Theor. Phys. 21, 467 (1982).
[2] S. R. White, Density matrix formulation for quantum renormalisation groups, Phys. Rev. Lett. 69, 2863 (1992).
[3] S. Trotzky, L. Pollet, F. Gerbier, U. Schnorrberger, I. Bloch, N.V. Prokof'ev, B. Svistunov, M. Troyer, Suppression of the critical temperature for superfluidity near the Mott transition: validating a quantum simulator, Nature Phys. 6, 998-1004 (2010).
[4] A. Y. Kitaev, A. H. Shen, and M. N. Vyalyi. Classical and quantum computation, Graduate Studies in Mathematics 47, AMS (2002).
[5] K. G. H. Vollbrecht and J. I. Cirac, Quantum simulators, continuous-time automata, and translationally invariant systems, Phys. Rev. Lett. 100, 010501 (2008).
[6] I. Bloch, J. Dalibard, S. Nascimbène, Quantum simulation with ultracold atomic gases, Nature Phys. 8, 267 (2012).
[7] R. Blatt and C. F. Roos, Quantum simulation with trapped ions, Nature Phys. 8, 277 (2012).
[8] S. Trotzky, Y. A. Chen, A. Flesch, I. P. McCulloch, U. Schollwoeck, J. Eisert, I. Bloch, Probing the relaxation towards equilibrium in an isolated strongly correlated 1D Bose gas, Nature Phys. 8, 325 (2012).

[9] J. Eisert, M. Friesdorf, C. Gogolin, Quantum many-body systems out of equilibrium, Nature Phys. 11, 124 (2015).
[10] B. P. Lanyon, C. Hempel, D. Nigg, M. Müller, R. Gerritsma, F. Zähringer, P. Schindler, J. T. Barreiro, M. Rambach, G. Kirchmair, M. Hennrich, P. Zoller, R. Blatt, C. F. Roos, Universal digital quantum simulation with trapped ions, Science 334, 57 (2011).
[11] M. Lewenstein, A. Sanpera, V. Ahufinger, Ultracold atoms in optical lattices: Simulating quantum many-body systems, Oxford University Press, Oxford, (2012).
[12] I. Georgescu, S. Ashhab, and F. Nori, Quantum simulation, Rev. Mod. Phys. 86, 153 (2014).
[13] A. Lemmer, C. Cormick, C. T. Schmiegelow, F. Schmidt-Kaler, M. B. Plenio, Two-dimensional spectroscopy for the study of ion Coulomb crystals, Phys. Rev. Lett. 114, 073001 (2015).
[14] I. Carusotto and C. Ciuti, Quantum fluids of light, Rev. Mod. Phys. 85, 299 (2013).
[15] Y. Zhang et al., Quantum phases in circuit QED with a superconducting qubit array, Sci. Rep. 4, 4083 (2014); A. Houck et al., On-chip quantum simulation with superconducting circuits, Nature Phys. 8, 292 (2012); Wallraff, D. I. Schuster, A. Blais, L. Frunzio, R.-S. Huang, J. Majer, S. Kumar, S. M. Girvin, R. J. Schoelkopf, Circuit quantum electrodynamics: Coherent coupling of a single photon to a Cooper pair box, Nature 431, 162 (2004).
[16] P. Barthelemy and L.M.K. Vandersypen, Quantum dot systems: a versatile platform for quantum simulations, Annalen der Physik 10, 808 (2013).
[17] A. van Oudenaarden and J. E. Mooij, One-dimensional Mott insulator formed by quantum vortices in Josephson Junction arrays, Phys. Rev. Lett. 76, 4947 (1996).
[18] A. Aspuru-Guzik and P. Walther, Photonic quantum simulators, Nature Phys. 8, 285 (2012).
[19] S. Gharibian, Y. Huang, Z. Landau, S. W. Shin, Quantum Hamiltonian complexity, Found. Tr. Th. Comp. Sc. 10, 159 (2015).
[20] F. H. L. Essler, H. Frahm, F. Göhmann, A. Klümper, V. E. Korepin, The one-dimensional Hubbard model, Cambridge University press (1993).
[21] D. Marcos, P. Rabl, E. Rico, P. Zoller, Superconducting circuits for quantum simulation of dynamical gauge fields, Phys. Rev. Lett. 111, 110504 (2013).
[22] D. Perez-Garcia, F. Verstraete, M. M. Wolf, J. I. Cirac, Matrix product state representations, Quantum Inf. Comp. 7, 401 (2007).
[23] R. Orús, A practical introduction to tensor networks: Matrix product states and projected entangled pair states, Ann. Phys. (N.Y.) 349, 117 (2014).
[24] F. Verstraete, J.I. Cirac, V. Murg, Matrix product states, projected entangled pair states, and variational renormalization group methods for quantum spin systems, Adv. Phys. 57,143 (2008).
[25] J. Eisert, M. Cramer, M. B. Plenio, Area laws for the entanglement entropy, Rev. Mod. Phys. 82, 277 (2010).
[26] S. Aaronson, A. Arkhipov, The computational complexity of linear optics, arXiv:1011.3245.
[27] S. Lloyd, Universal quantum simulators, Science 273, 1073 (1996).

[28] A. Y. Kitaev, Anyons in an exactly solved model and beyond, Ann. Phys. 321, 2 (2006).
[29] P. M. Chaikin, T. C. Lubensky, Principles of condensed matter physics, Cambridge University Press (2007).
[30] R. B. Laughlin, Anomalous quantum Hall effect: An incompressible quantum fluid with fractionally charged excitations, Phys. Rev. Lett. 50, 1395 (1983).
[31] M. P. Nightingalea and C. J. Umrigar, Quantum Monte Carlo methods in physics and chemistry, Springer (1999).
[32] R. G. Parr and W. Yang, Density-functional theory of atoms and molecules, Oxford University press (1989).
[33] S. Aaronson, Computational complexity: Why quantum chemistry is hard, Nature Physics 5, 707 (2009).
[34] S. Braun, M. Friesdorf, S. S. Hodgman, M. Schreiber, J.P. Ronzheimer, A. Riera, M. del Rey, I. Bloch, J. Eisert, U. Schneider, Emergence of coherence and the dynamics of quantum phase transitions, PNAS 112, 3641 (2015).
[35] J.-Y. Choi, S. Hild, J. Zeiher, P. Schauß, A. Rubio-Abadal, T. Yefsah, V. Khemani, D. A. Huse, I. Bloch, C. Gross, Exploring the many-body localization transition in two dimensions, Science 352, 1547 (2016).
[36] P. Jurcevic, B. P. Lanyon, P. Hauke, C. Hempel, P. Zoller, R. Blatt, C. F. Roos, Observation of entanglement propagation in a quantum many-body system, Nature 511, 202 (2014).
[37] E. A. Martinez, C. A. Muschik, P. Schindler, D. Nigg, A. Erhard, M. Heyl, P. Hauke, M. Dalmonte, T. Monz, P. Zoller, R. Blatt, Real-time dynamics of lattice gauge theories with a few-qubit quantum computer, Nature 534, 516-519 (2016).
[38] P. Hauke, F. M. Cucchietti, L. Tagliacozzo, I. Deutsch, M. Lewenstein, Can one trust quantum simulators? Rep. Prog. Phys. 75, 082401 (2012).
[39] T. H Johnson, S. R Clark, and D. Jaksch, What is a quantum simulator?, EPJ Quantum Technology 1, 10 (2014).
[40] J. Preskill, Quantum computing and the entanglement frontier, arXiv:1203.5813.
[41] M. J. Bremner, A. Montanaro, D. J. Shepherd, Average-case complexity versus approximate simulation of commuting quantum computations, arXiv:1504.07999.
[42] D. Hangleiter, M. Kliesch, M. Schwarz, J. Eisert, Direct certification of a class of quantum simulations, arXiv:1602.00703.
[43] D. Gross, Y.-K. Liu, S. T. Flammia, S. Becker, J. Eisert, Quantum state tomography via compressed sensing, Phys. Rev. Lett. 105, 150401 (2010).
[44] M. Cramer, M.B. Plenio, S.T. Flammia, D. Gross, S. D. Bartlett, R. Somma, O. Landon-Cardinal, Y-K. Liu, D. Poulin, Efficient quantum state tomography, Nature Comm. 1, 149 (2010).
[45] A. Steffens et al., Towards experimental quantum field tomography with ultracold atoms, Nature Comm. 6, 7663 (2015).
[46] C. Schwemmer, G. Toth, A. Niggebaum, T. Moroder, D. Gross, O. Gühne, H. Weinfurter, Experimental comparison of efficient tomography schemes for a six-qubit state, Phys. Rev. Lett. 113, 040503 (2014).
[47] L. Aolita, C. Gogolin, M. Kliesch, J. Eisert, Reliable quantum certification for photonic quantum technologies, Nature Comm. 6, 8498 (2015).

[48] M. Segev, Y. Silberberg, DN Christodoulides, Nature Photonics. 7 (2013).
[49] J. Billy et al., Nature 453, 891 (2008)
[50] G. Roati et al., Nature 453, 895 (2008)

2.3.2 Experimental platforms for quantum simulators

A. Physical approach and perspective

A number of experimental platforms have been considered for realising quantum simulators [14]. Each such architecture has their specific advantages and allows for a different range of system controls.

- The first - and up to now most prominent - implementation of analogue quantum simulation is constituted by cold atoms in optical lattices [1,2], artificial crystals made from interference of laser light. This gives rise to effective condensed-matter type systems in the laboratory with unprecedented control over parameters, and with routine system sizes around 10 000 atoms. Short and long-range interactions are highly controllable, e.g., via Feshbach resonances, dipole-dipole or cavity-mediated interactions and artificial gauge fields with fully tuneable 'field strengths' have been realised.
- Similarly, ultra-cold atoms near nano-structures constitute an important platform for quantum simulators, specifically to probe systems out of equilibrium [3]. Here again, large system sizes can be reached, but different kinds of read-out and preparation are feasible for this kind of continuous quantum many-body system.
- Trapped ions have achieved some of the most remarkable levels of control for single and few particle systems up to 20-30 ions and are at present scaling up to realise larger scale systems. Their fast cycle times, superb control and observation techniques has enabled them to act as efficient quantum simulators [4]. Trapped ions are the most important architecture to date to build digital quantum simulators, and they offer opportunities as analogue quantum simulators for systems with long-range interactions.
- Polaritons or exciton-polariton systems in arrays of micro-cavities provide a versatile and scalable photonic platform for quantum simulation of dissipative non-linear systems and for which local addressing is specifically feasible [5-9].
- Large arrays of semiconductor quantum dots have been used to simulate the Mott-Hubbard model in the atomic limit [23] and allow for quantum simulations of the most interesting part of the phase diagram, where temperature is much smaller than the hopping energy scale, which in turn is much smaller than the on-site interaction energy [10,24]. In small quantum dot arrays, effects such as spin superexchange were demonstrated [25].
- Superconducting circuits constitute an important platform for quantum simulations where progress was particularly fast in recent years [11,12]. The quantum particles in these systems are circuit excitations rather than atoms with conserved particle number, superconducting simulators can by particularly useful in accessing non-equilibrium physics. Depending on circuit design and coupling

methods, superconducting qubits can be realised as charge, flux, or phase qubits, and used for digital or analogue simulation.
Photons in linear and nonlinear optics devices allow for quantum simulations [13]. These systems range from small systems using discrete optics to larger setting in waveguide arrays and allow for an enormous degree of control, especially when combined with photonic lattices and waveguide structures. Such photonic waveguides allow for a large flexibility in engineering disordered quntum systems to e.g. study Anderson localization of light [27] or to form tailored energy bands with topological properties [28-30]. It is important to note that topological photonic systems allow the direct visualization of topologically-protected transport, where optical beams propagate unidirectionally, without being scattered by defects, imperfections, and being completely immune to the shape of the samples and their boundaries [29]. In the same vein, such topological photonic systems exhibit intriguing phenomena also at the single photon level and with entangled photonic states. For example, the quantum correlations survive for very long time spans, and always remain highly localized in spite of disorder and scattering that normally hamper the quantum and classical evolution in the system [31]. In addition, the photons' intrinsic property of being mobile provides technological advances for implementing intermediate computation such as boson sampling [26] or quantum transport simulations.

Overviews over several platforms and their recent developments are collected in the review articles in Rev. Mod. Phys. [14] in Nature Physics [15], as well as the other articles in the Nature Physics Insight Issue on quantum simulation [1, 4, 9, 10].

B. State-of-the-art
Different platforms of quantum simulators have experienced rapid development in recent years. In the field of ultra-cold atoms, many of the key achievements build on optical lattice systems, beginning with the seminal realisation of the superfluid-to Mott insulator transition [16], which was followed by the implementation of the Fermi-Hubbard model [17], taking steps towards the above mentioned quantum simulation of interacting fermionic lattice models in two dimensions. More recently, as far as cold atoms in optical lattices are concerned, quantum-gas microscopes have enabled single-site resolved imaging and control of a many-body system at an unprecedented level [18]. In bulk systems, without optical lattices, quantum simulation of many-body fermionic quantum systems has allowed, e.g., the measurement of the equation of state in the unitarity limit, which proved useful in discriminating between different theoretical approaches, and calibrating approximate classical numerical techniques [1].

For trapped ions [4], the extraordinary level of control of motional and internal quantum states has enabled the realisation of a prototype of a digital quantum simulator [19] as well as analogue quantum simulation of different spin systems, including ones with long-ranged interactions [20]. In these trapped ions systems, also dynamical many-body effects can be probed, such as questions related to open systems dynamics [21], or propagation of correlations after quenches [20]. This includes also the emergence and frustration of magnetism with variable-range interactions in a quantum simulator [22].

In solid state systems, polariton condensates confined in semiconductor structures allow one to study non-equilibrium open systems dynamics, spin orbit coupling and magnetism in highly versatile and engineered lattices structures [9]. Arrays of quantum dots or superconducting circuits are currently being developed to implement large-scale quantum simulation platforms in other solid-state systems. Indeed, demonstrating scalability, circuits containing 512 qubits have already been fabricated, even though aspects of coherence are yet to be explored.

Photonic quantum systems allow for quantum simulations of smaller size quantum systems and were used to simulate quantum walks [32], boson sampling [26], topological phases [28] and disordered systems [27]. In a different way, they mimic two-spin orbitals, or frustrated valence-bond states [10]. Here, technological advances in waveguide technologies and micro-optics promise to allow for the integration of single-photon sources, tunable optical circuits and photon detectors on single chip-scale devices. Similarly, recent effort in the coupling many optical oscillators – laser oscillators or parametric oscillators -have been shown to simulate statistical physics problems such as Ising [33] and other spin problems [34].

C. Challenges

One of the strengths of the present day quantum simulation platforms is their capability to handle large-scale many-body systems (few hundred to few thousand particles) and their ability to carry out relevant simulations that are already intractable on classical computers today. The observation and control techniques employed in experiments have also enabled completely new ways to probe and control many-body systems, e.g., allowing one to reveal non-local order parameters or detect dynamical correlations as well as thermal and quantum fluctuations in-situ.

A challenge is to minimise the sacrifice on individual control and operation fidelity as the systems grow in size, when compared to the very high fidelity that can be achieved with few-qubit systems. Furthermore, one should push the actual limits on controlling of systems parameters down to the level of setting individual couplings and interactions locally in such larger scale systems of a few hundred to thousand qubits. Finally, verification of the error of a quantum simulation is limited today to simple adiabaticity checks and can require both further experimental and theoretical work to give tighter bounds on the computational error of such a quantum simulation.

From a theoretical point of view the degree of control can be seen as a major strength of present approaches for quantum simulation. In an experimental reality, the degree of control is practically always lesser than expected, but sometimes nature offers serendipitous solutions. Challenges to be addressed relate to measurement prescriptions, which are in several instances still quite limited, and methods of readout and certification.

Regarding the specific experimental platforms, a good summary of their strengths and weaknesses is given e.g. in Ref. [14]. Neutral atom systems are easily scalable to hundreds or thousands of particles and the recent advances of quantum-gas microscopes have even enabled single-particle control and readout [18]. Trapped ions offer currently the best degree of control regarding individual qubit readout and control, in particular for digital quantum simulation, but the number of particles in systems with single-particle control is currently limited to a few ten atoms at most.

Superconducting circuits and spin qubits in quantum dots offer also the possibility of individual control and readout, and one of their advantages is the possibility of using conventional microchip fabrication techniques to create larger-scale systems. Photons in linear optics devices allow for an enormous degree of flexibility and control, however scaling to larger system sizes is a challenge, in particular due to the great challenge of a controlled generation of single photons. The experimental platforms comprising quantum dots or cavity arrays have the advantage of good individual control and readout, however scaling to larger system sizes is still a challenge. In the case of excitonic polaritons, scalability of lattices is well mastered, while challenges remain for the control of interaction strength.

D. Short-term goals (0-5 years)

One general short-term goal for quantum simulators is to realise new phases of matter and probe matter in previously unexplored parameter regimes. Lowering temperatures and entropies of many-body systems can help in this respect, as this has almost always led to the discovery of novel quantum phases of matter. Such tailored quantum-correlated states of matter could also help in metrological applications ranging from atomic clocks to precision quantum sensors. Almost all platforms outlined above (atoms, ions, polaritons, photons, quantum dots, superconducting arrays, photonic systems) aim at increasing their respective system sizes that should push the application potential for quantum simulators in diverse fields of science. A key short-term goal is to design simplified schemes with less restrictive requirements on the parameters, an imperative that applies to all of the mentioned architectures.

The short-term goals for the different experimental platforms can be defined as follows:

- Ultracold atoms: Increase control possibilities and system sizes, further lower entropy and temperature, engineering of long-range interactions, band structure engineering, simulations of spin models, non-equilibrium phenomena, development of advanced potential shaping methods using holographic and DMD imaging techniques, study of quantum transport in novel regimes and with single atom sensitivity

- Trapped ions: Explore atom-laser interactions leading to spin Hamiltonians other than Ising or XY, obtain better control over phononic degrees of freedom, demonstrate 50-ion simulations while retaining single-particle control, implement single-particle control in planar crystals in Penning trap experiments, explore the use of magnetic field gradients or Rydberg interactions for engineering entangling interactions, increase two-qubit gate fidelity to >99% in digital quantum simulations with about 10 ions, experimental characterization of complex quantum states resulting from quantum simulations
- Superconducting platforms: Simulate spin systems on frustrated geometries, and small-scale fermionic models such as Hubbard-type models or quantum chemistry models. Explore extensions towards a 2D geometry by investigating effective multi-qubit interactions. Realize resonator arrays that mediate effective photon-photon interactions. Explore techniques to gain real-space information through single-site addressability. Demonstrate quantum phase transitions in driven dissipative systems. Explore lattice topologies for synthetic gauge fields. Study hybrid analog - digital simulation techniques. Explore quantum variational algorithms based on the controlled generation and measurement of relevant classes of many-body quantum states.
- Photonic platforms: The short-term goals for photonic platforms are to increase the number of photons and to decrease the photon loss, in particular when using integrated waveguide technology. This goes hand in hand with the optimization of single-photon detectors by exploiting superconducting technology (nanowire detectors and transition edge sensors) for achieving detection efficiencies close to unity. For photonic lattice and waveguide systems, the short-term challenge is to increase the strength of the nonlinear interactions such that long-term quantum evolutions can be employed. Another short-term goal is to carry out the first experiments with entangled photonic states in topological photonic systems, such as photonic topological insulators, and test their increased robustness and ability to sustain scattering and the presence of defects while maintaining their highly localized quantum correlations.
- Polaritons: Enhancement and control of polaritonic non-linearity; Increase control possibilities of polariton lifetime and lattice optical quality; Band structure and spin orbit coupling engineering; Quantum Hall states of light; Ultrafast quantum correlation measurements.
- Quantum-dot arrays: Improvements in quantum dot uniformity and scaling of quantum dot arrays.

E. Medium-term goals (5-10 years)

Medium -term goals for the different experimental platforms are

- Ultracold atoms: Realising fully & individually controllable couplings at the single lattice site scale Investigation of strongly interacting quantum gases in gauge fields, Optimization of system performances with respect to controllability, simulation speed and verification.

- Trapped ions: Simulate spin Hamiltonians in two-dimensional microtrap arrays with flexible geometries, simulation of spin-phonon models, increase coherence time to allow for adiabatically evolving ground states, investigate quench dynamics with >100 ions, characterize entanglement growth in dynamical simulations, combine coherent with dissipative interactions for investigation of open systems, compare trapped-ion simulation results with other platforms simulating the same model
- Superconducting platforms: Scale qubit circuits to a 2D topology while maintaining individual qubit control and flexible inter-qubit couplings. Solve the relevant technical challenges in terms of connectivity. Integrate basic error-correction elements into the quantum algorithms. Simulate strongly correlated 2D spin models and fermionic models by implementing effective multi-qubit interactions. Implement hybrid digital-analog simulators which are able to simulate problems with a complexity that require the computational power of state-of-the art supercomputers for validation. Realize a 2D photonic lattice with a large number of lattice sites and single-site addressability to address an open question in the study of dynamical phase transitions. Demonstrate quantum speed-up with a quantum variational algorithm applied for example to a quantum chemistry problem.
- Photons: A major mid-term goal for photonic systems is the development of deterministic single- and multi-photon sources, either via active multiplexing techniques of probabilistic sources or via tailored solid-state emitters (quantum dots, quantum memory etc). This together with the fabrication of tunable large-scale interferometric networks (potentially even in three-dimensions) will enable the demonstration of the quantum supremacy via boson sampling and other related quantum simulations. In addition, the realization of photon-photon interactions by strong nonlinear media such as atom-light hybrid systems (e.g. cavity-QED, nanostructured graphene, cold atoms etc.) is expected. This will dramatically improve the scalability of two-photon gates and thus open up the possibility of complex analog and digital photonic quantum simulators (Heisenberg interacting spins etc.). For photonic lattice and waveguide systems the mid-term goals include: increasing the strength of the quantum interactions to the level that single photons interact strongly. This has been a long-standing challenge in photonics and it can be accomplished in various ways. These can range from attaching atoms (at resonance with the EM field) to the photonic systems in a cavity-QED type platform superimposed on the waveguide arrays (photonic lattices) or further developing the platform of Rydberg-atoms to encompass tens of atoms, or by making use of new photonic platforms where the interactions is extremely strong – to the level that single photons interact with one another.
- Polaritons: Create strongly correlated polariton phases in engineered lattices; Simulation of new quantum phases for polaritons; topologically protected quantum phases of light; Critical exponents in driven dissipative phase transitions.
- Quantum-dot arrays: Demonstrate quantum supremacy using quantum dot arrays, for instance to simulate problems in quantum magnetism or Mott-Hubbard physics with fermions.

F. Long-term goals (> 10 years)

One long-term challenge is to extend the reach of quantum simulations into other fields of science in addition to condensed matter physics, e.g. quantum field theories in high-energy physics, cosmology (simulation of non-equilibrium dynamics), chemistry and material science. Already now first efforts in this direction have emerged, however more connections will be explored and realised in the coming years and lead to fruitful interactions between the fields.

We expect thus that in long-term quantum simulators will allow us to get understanding and control of i) high Tc superconductivity, ii) lattice gauge theories out of equilibrium; iii) quantum dynamics in strongly correlated systems, iv) systems with topological order, v) quantum glasses and spin glasses, vi) frustrated anti-ferromagnetism, vii) itinerant ferromagnetism, and viii) non-equilibrium quantum dynamics. Novel methods of classical simulations (tensor network states) combined with quantum Monte Carlo, and perturbation theory will allow to verify and certify quantum simulators in wide aspects. It will then also be clear what features can be efficiently verified without actually classically simulating the quantum device. This also asks for methods of certification beyond and complementing more conventional quantum state tomography. Even if not all detailed goals will be realised, one can expect enormous progress in this area, as well as significant spin-offs into other systems of simulation and the control of complex quantum systems.

Specific long-term goals for the different experimental platforms include:

- Ultracold atoms: Application of cold atom to even more diverse quantum simulations e.g. in QED, QCD, or cosmological systems. Development of correlated many-body states for advanced atomic clocks and metrology and advanced control of fully programmable interactions and couplings (even over longer ranges).
- Superconducting platforms: Solve technologically relevant problems in quantum chemistry, biology or material science, which are inaccessible to a classical computer simulation. Simulate the ground state of the Hubbard model and determine whether its properties capture the phenomenology of high-Tc superconductors. Solve technologically relevant optimization problems by encoding into Ising spin glass problems. Integrate fault-tolerant gate operations into digital quantum simulations. Map out the full phase diagram of driven-dissipative Jaynes-Cummings type lattice systems, providing benchmark data for classical computer simulations like quantum Monte Carlo methods.
- Photonic platforms: The long-term goal is to develop an all-integrated quantum simulator, where the photon sources (e.g. cavity solid-state systems), complex but tunable interferometric networks and detection units are integrated on one chip. The precise quantum control of dozens or even hundreds of photons hold the promise to provide insights into new material properties and transport phenomena. However, at this stage new matter-light hybrid quantum simulators might have evolved, which provide particular advantages with respect to single-platform quantum simulators.

- Traped ions: Demonstrate digital quantum simulation using quantum error correction techniques, analog simulations of two-dimensional spin models, simulate quantum chemistry problems.
- Polaritons: Hybrid quantum systems with polaritons; polaritonic quantum devices;

G. Key references

[1] I. Bloch, J. Dalibard, S. Nasciembène, "Quantum simulation with ultracold atomic gases", Nature Phys. 8, 267 (2012).
[2] M. Lewenstein, A. Sanpera, V. Ahufinger, "Ultracold atoms in optical lattices: Simulating quantum many-body systems", Oxford University Press, Oxford (2012).
[3] M. Gring, M. Kuhnert, T. Langen, T. Kitagawa, B. Rauer, M. Schreitl, I. Manets, D. A. Smith, E. Dealer, J. Schmiedmayer, "Relaxation and pre-thermalization in an isolated quantum system", Science 337,1318 (2012).
[4] R. Blatt and C. F. Roos, "Quantum simulation with trapped ions', Nature Phys. 8, 277 (2012).
[5] M. J. Hartmann, F. G. S. L. Brandao, and M. B. Plenio, "Strongly interacting polaritons in coupled arrays of cavities", Nature Physics 2, 849 (2006).
[6] A. D. Greentree, C. Tahan, J. H. Cole, and L. C. L. Hollenberg, "Quantum phase transitions of light", Nature Physics 2, 856 (2006).
[7] M. Abbarchi et al., "Macroscopic quantum self-trapping and Josephson oscillations of exciton polaritons", Nature Phys. 9, 275 (2013).
[8] N. Y. Kim, Y. Yamamoto, S. Utsunomiya, K. Kusudo, S. Höfling, A. Forchel, "Exciton-polariton condensates in zero-, one-, and two-dimensional lattices", Physics of quantum fluids (Springer), 157 (2013); N. Y. Kim, Y. Yamamoto, "Exciton-polariton quantum simulators", arXiv:1510.08203 (2015).
[9] T. Jacqmin et al., Direct Observation of Dirac Cones and a Flatband in a Honeycomb Lattice for Polaritons, Phys. Rev. Lett. 112, 116402 (2014).
[10] T. Byrnes, N. Y. Kim, K. Kusudo, and Y. Yamamoto, Quantum simulation of Fermi-Hubbard models in semi- conductor quantum-dot arrays, Phys. Rev. B 78, 075320 (2008).
[11] Y. Zhang et al., "Quantum phases in circuit QED with a superconducting qubit array", Sci. Rep. 10.1038/srep04083 (2014).
[12] M. R. Geller, J. M. Martinis, A. T. Sornborger, P. C. Stancil, E. J. Pritchett, H. You, and A. Galiautdinov, "Universal quantum simulation with prethreshold superconducting qubits: Single-excitation subspace method", Phys. Rev. A 91, 062309 (2015).
[13] A. Aspuru-Guzik and P. Walther, "Photonic quantum simulators", Nature Phys. 8, 285 (2012).
[14] I. Georgescu et al., "Quantum simulation", Rev. Mod. Phys. 86, 153 (2014).
[15] J. I. Cirac and P. Zoller, "Goals and opportunities in quantum simulation", Nature Phys. 8, 264 (2012).
[16] M. Greiner et al., "Quantum phase transition from a superfluid to a Mott insulator in a gas of ultracold atoms", Nature 415, 39 (2002).

[17] R. Jördens et al., "A Mott insulator of fermionic atoms in an optical lattice", Nature 455, 204 (2008); U. Schneider et al., Metallic and insulating phases of repulsively interacting fermions in a 3D optical lattice, Science 322, 1520 (2008).
[18] W. S. Bakr et al., A quantum gas microscope for detecting single atoms in a Hubbard-regime optical lattice, Nature 462, 74 (2009); J. F. Sherson et al., Single-atom-resolved fluorescence imaging of an atomic Mott insulator, Nature 467, 68 (2010).
[19] B. Lanyon et al., Universal digital quantum simulation with trapped ions, Science 334, 57 (2011).
[20] P. Jurcevic, B. P. Lanyon, P. Hauke, C. Hempel, P. Zoller, R. Blatt, C. F. Roos, Quasiparticle engineering and entanglement propagation in a quantum many-body system Nature 511, 202 (2014); P. Richerme, Z.-X. Gong, A. Lee, C. Senko, J. Smith, M. Foss-Feig, S. Michalakis, A. V. Gorshkov, and C. Monroe, Non-local propagation of correlations in quantum systems with long-range interactions, Nature 511, 198 (2014).
[21] J. T. Barreiro et al, An open-system quantum simulator with trapped ions, Nature 470, 486 (2011).
[22] R. Islam et al., Emergence and frustration of magnetism with variable-range interactions in a quantum simulator, Science 340, 583 (2013).
[23] A. Singha et al, Two-dimensional Mott-Hubbard electrons in an artificial honeycomb lattice, Science 332, 1176 (2011).
[24] P. Barthelemy and L.M.K. Vandersypen, Quantum dot systems: a versatile platform for quantum simulations, Annalen der Physik 10-11, 808 (2013).
[25] T.A. Baart, T. Fujita, C. Reichl, W. Wegscheider, L.M.K. Vandersypen, Coherent spin-exchange via a quantum mediator, arXiv:1603.03433.
[26] J. B. Spring et al., Boson sampling on a photonic chip Science 339, 798 (2013); M. Tillmann, M. et al., Experimental boson sampling. Nature Photonics 7, 540 (2013); A. Crespi et al., Integrated multimode interferometers with arbitrary designs for photonic boson sampling, Nature Photonics 7, 545 (2013).
[27] M. Segev, Y. Silberberg, D.N. Christodoulides, Anderson localization of light, Nature Photonics 7,197 (2013).
[28] M.C. Rechtsman, et al., Photonic Floquet topological insulators, Nature 496, 196 (2013).
[29] M.C. Rechtsman, et al., Strain-induced pseudomagnetic field and photonic Landau levels in dielectric structures, Nature Photonics 7, 153 (2013).
[30] M. Hafezi, et al., Imaging topological edge states in silicon photonics, Nature Photonics 7, 1001 (2013).
[31] M.C. Rechtsman, et al., Topological protection of photonic path entanglement, Optica 3, 925 (2016).
[32] H.B. Perets et al., Realization of quantum walks with negligible decoherence in waveguide lattices, Phys. Rev. Lett. 100, 170506 (2008).
[34] T. Inagaki, et al., Large-scale Ising spin network based on degenerate optical parametric oscillators, Nature Photonics 10, 415–419 (2016).
[35] M. Nixon, E. Ronen, A.A. Friesem, and N. Davidson, Observing geometric frustration with thousands of coupled lasers, Phys. Rev. Lett. 110, 184102 (2013).

2.4 Quantum Information Theory

The development of quantum information science (QIT) 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 QIT, theoretical work has often been far ahead of experimental realisation 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 that employ, control and manipulate matter and radiation at the quantum level.

Today we see clearly two important roads towards quantum information processing. On the one hand the steady and impressive progress on the quantum hardware side, delivering for example systems with a small number (<20) of qubits. On the other we observe a strong need for quantum software. Success in quantum information processing will depend on advances in both quantum hardware and quantum software. Moreover, success will depend in the interaction between the two. Investigations related to quantum information theory and quantum software include, to name just a few examples,

1. Novel quantum algorithms;
2. Quantum communication protocols;
3. Novel quantum cryptographic protocols;
4. Basic concepts such as entanglement and decoherence;
5. Characterisation and quantification of (two- & multi-party) entanglement;
6. Capacities of noisy quantum communication channels;
7. Optimisation of protocols for quantum cryptography;
8. New quantum computer models and architectures;
9. New tools for the study of quantum systems with many degrees of freedom such as strongly correlated lattice systems;
10. Novel ideas to explore complex quantum systems;
11. Quantum simulation methods to simulate quantum systems.

An important class of theoretical work is concerned with implementations of these abstract concepts in real physical systems, such as trapped ions, ultra-cold ions in optical lattices, superconducting qubits, quantum dots, photons, etc. In fact, many of these theoretical proposals have formed the starting point as well as the guide for experimental work in the laboratories, as is described in the other sections of this document. What is more, the transfer of concepts from quantum information theory to other fields of physics such as condensed matter physics or quantum field theory has proved very fruitful and has attracted considerable interest recently.

It is important to realise that these activities are often interdisciplinary in nature and span a broad spectrum of research in which the different activities are benefiting from each other to a large degree. Thus it does not seem to be advisable to concentrate research on too narrowly defined topics only. Theory groups in Europe have been consistently attained international leadership in the entire spectrum of research (see more below). This has been facilitated by a flexible and topically broad financing on European and national levels in the past. This leadership will have great economical value in a quantum enabled information processing age. Just as software for classical computers enables the classical hardware and brings great economical benefits, the same will be true for quantum software.

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

2.4.1 Quantum Information Processing

Quantum algorithms and complexity

A. Introduction

Following Deutsch's fundamental work in 1985 that demonstrated the potential power of quantum algorithms and quantum computers, Shor demonstrated in 1994 that large integers can be efficiently factored on a quantum computer. Factoring is the task of decomposing an integer into a product of prime numbers, for example 15=3x5. Its importance is immense because many modern cryptographic protocols (such as the famous RSA cryptosystem) are based on the well-supported assumption 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. Grover's quantum "database search" algorithm allows a quantum computer to perform an unstructured search quadratically faster than any classical algorithm. Although Grover only yields a quadratic speed-up over classical algorithms, it is widely applicable to computer science tasks, like sorting, matrix multiplication, bipartite matching to name a few. For such problems quantum computers give an important advantage over classical computers.

B. State-of-the-art

Shor’s algorithm has led 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, which are sometimes touted as "hard problems" that could replace factoring and discrete logarithms in classical cryptography. Grover’s algorithm can be cast in terms of quantum random walks, which has in turn led to new quantum algorithms for searching game trees and other problems. These algorithms will be very useful in the area of algorithmic game theory, scientific computing, etc. Contrary to expectations, it has very recently been shown that one can even obtain faster-than-quadratic quantum speed-ups for some problems like this. Recently a new quantum algorithm has been developed for approximating solutions to systems of linear equations, giving an exponential advantage over any classical algorithm.

In order to understand to what extent quantum computers outperform classical computers, we need to determine where efficient quantum computation (that is, the complexity class "BQP"), fits within the classification of complexity classes like P, NP, and PSPACE. General methods for proving limitations of quantum computers have been developed and applied with great success, the two most notable ones being the polynomial method and the quantum adversary method. We know now that the latter method is optimal; hence what was originally designed to be a lower bound method can also be used to find new algorithms, and in fact some faster quantum algorithms for (for example) graph problems have been found this way.

C. Challenges

A constant challenge in this field is to find new examples of quantum algorithms that outperform the best classical algorithms. In this line of research, it is important to understand when quantum systems can be efficiently simulated on a classical computer. This allows identifying special cases where quantum resources do not lead to any significant improvement over classical computation. Insights into such limitations of quantum computers can then possibly be exploited in quantum-resistant classical cryptography.

D. Key references

[1] D. Deutsch, "Quantum theory, the Church-Turing principle and the universal quantum computer", Proc. R. Soc. Lond. A 400, 97 (1985)
[2] P. W. Shor, "Algorithms for quantum computation, discrete log and factoring", 35th FOCS, 124 (1994)
[3] L. Grover, "A fast quantum mechanical algorithm for database search", 28th STOC, 212 (1996)
[4] A. Ambainis, D. Aharonov, J. Kempe and U. Vazirani, "Quantum walks on graphs", 33rd STOC (2001)
[5] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf, "Quantum lower bounds by polynomials", Journal of the ACM 48(4) (2001)
[6] A. Ambainis, "Quantum lower bounds by quantum arguments", Journal of Computer and System Sciences 64, 750 (2002)
[7] E. Farhi, J. Goldstone and S. Gutmann. "A Quantum Algorithm for the Hamiltonian NAND Tree" [quant-ph/0702144]
[8] A. W. Harrow, A. Hassidim, and S. Lloyd, "Quantum algorithm for solving linear systems of equations", Phys. Rev. Lett. 15, 150502 (2009)
[9] R. Jozsa and A. Miyake, "Matchgates and classical simulation of quantum circuits", Proc. R. Soc. A 464, 3089 (2008)
[10] A. Ambainis, K. Balodis, A. Belovs, T. Lee, M. Santha and J. Smotrovs, "Separations in Query Complexity Based on Pointer Functions", [arXiv:1506.04719] (2015)

Computational models and architectures

A. Introduction

There are many different ideas on how to make quantum systems compute. While these different computational models are typically equivalent in the sense that one can simulate the other with only polynomial overheads in resources, they may be quite different in practice, when it comes to a particular class of problems. They also have to satisfy very different needs from the perspective of the requirements on the hardware. What is more, they suggest different procedures to achieve fault-tolerant computation, many of them yet to be explored in detail.

B. State-of-the-art

At the moment, the main contenders of fundamental architectures are:

1. The gate or circuit model (computation realised by series of elementary unitary transformations on a few qubits at a time);
2. The one-way quantum computer (computation realised by a sequence of 1-bit measurements on a pre-entangled cluster state) and alternative, more general schemes for measurement-based quantum computing;
3. Adiabatic computing (computation realised by smoothly changing a Hamiltonian, whose ground state, at the end of the process, encodes the solution of the given problem);
4. Quantum cellular automata (quantum versions of classical cellular automata);
5. Quantum Turing machines (quantum versions of classical Turing machines);
6. Dissipation-driven quantum computation (computation realised by dissipative dynamics).

Most recently, we have seen a series of theoretical work analysing the connection between the different computational models. The benefit of these works lies in a better understanding of the capabilities and advantages of the individual models, and of the essential features of a quantum computer. It will also turn out what model will eventually give rise to the most feasible architecture.

C. Challenges

In the future we expect that optimised 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 realise scalable quantum computers in the laboratory.

D. Key references

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

[2] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, "Elementary gates for quantum computation", Phys. Rev. A 52, 3457 (1995)
[3] E. Farhi, J. Goldstone, S. Gutmann, J. Lapan, A. Lundgren, and D. Preda, "A quantum adiabatic evolution algorithm applied to random instances of an NP-complete problem", Science 292, 472 (2001)
[4] B. Schumacher and R. Werner, "Reversible cellular automata", [quant-ph/0405174]
[5] R. Raussendorf and H.-J. Briegel, "A one-way quantum computer", Phys. Rev. Lett. 86, 5188 (2001)
[6] D. Gross and J. Eisert, "Novel schemes for measurement-based quantum computation", Phys. Rev. Lett. 98, 220503 (2007)
[7] S. Diehl, A. Micheli, A. Kantian, B. Kraus, H. P. Büchler, and P. Zoller, "Quantum states and phases in driven open quantum systems with cold atoms", Nature Physics 4, 878 (2008)
[8] F. Verstraete, M. M. Wolf, and J. I. Cirac, "Quantum computation, quantum state engineering, and quantum phase transitions driven by dissipation", Nature Physics 5, 633 (2009)

Quantum simulation

A. Introduction

Quantum simulators may become the first application of quantum computers, since with modest requirements one may be able to perform simulations that are impossible with classical computers. At the beginning of the 80's it was realised 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 or static properties can be engineered such that it reproduces the behaviour of another physical system which one is interested to describe. The former can be conceived in a "digital" fashion, where continuous dynamics is approximated by gates using a Trotter formula, or in an analogue way. In principle, a universal quantum computer would be an almost perfect quantum simulator since one can program it to undergo any desired quantum dynamics. However, a quantum computer is very difficult to build in practice and has very demanding requirements. Fortunately, there are physical systems in which one can engineer certain kind of interactions and thus simulate other systems which so far are not well understood.

B. State-of-the-art

Key experimental platforms for quantum simulators are ultra-cold atoms in optical lattices, trapped ions, quantum dots, superconducting qubits, or photons. All those architectures have seen a remarkable progress in recent years. Quantum dots and superconducting qubits have been added to the list more recently. In those systems, one does not necessarily require to individually address the qubits, or to perform quantum gates on arbitrary pairs of qubits, but rather on all of them at the same time. Ideas like optical superlattices or the suitable exploitation of Feshbach resonances in the former class of physical systems add further flexibility. Besides, one is interested in measuring physical properties (like magnetisation, conductivity, etc.) which are robust with respect to the appearance of several errors (in a quantum computer without error correction, even a single error will destroy the computation). For example, to see whether a material is conducting or not one does not need to know with a high precision the corresponding conductivity. Molecular energies within chemical precision can also be computed by quantum simulations. The use of 30 to 100 qubits for those algorithms exceeds the limitations of classical computing of molecular energies.

C. Challenges

Important theoretical open questions are related to certifying success of a quantum simulation or to show hardness of the equivalent classical problem. Another challenge is to assess how the errors will be reflected in the quality of the computation, or even to show that fault-tolerant error correction is not required in order to solve problems that are interesting in other fields of science.

D. Key references

[1] S. Lloyd, "Universal quantum simulators", Science 273, 1073 (1996)
[2] “Quantum Simulation”, Nature Physics Insight, 8, 263 (2012).
[3] Special Issue on Quantum Simulation, Ed. R. Blatt, I. Bloch, J. I. Cirac, and P. Zoller, Annalen der Physik, 525, 739 (2013).
[4] M. A. Nielsen, M. J. Bremner, J. L. Dodd, A. M. Childs, and C. M. Dawson, "Universal simulation of Hamiltonian dynamics for qudits", Phys. Rev. A 66, 022317 (2002)
[5] S. Trotzky, Y.-A. Chen, A. Flesch, I. P. McCulloch, U. Schollwock, J. Eisert, and I. Bloch,, "Probing the relaxation towards equilibrium in an isolated strongly correlated 1D Bose gas", Nature Physics 8, 325 (2012)
[6] P. Hauke, F. M. Cucchietti, L. Tagliacozzo, I. Deutsch, and M. Lewenstein, "Can one trust quantum simulators?", Rep. Prog. Phys. 75, 082401 (2012)

Topological quantum information processing and computation

A. Introduction

Topological quantum computation (TQC) is an approach to quantum information processing that eliminates decoherence at the hardware level by encoding quantum states and gates in global, delocalised properties of the hardware medium. Most of the current quantum computing schemes assume nearly perfect shielding from the environment. Decoherence makes quantum computing prone to error and non-scalable, allowing only for very small “proof-of-principle” devices. Error correction software can in principle solve this problem, but progress along this path will take a long time. While much of the current research on other approaches to quantum computation is focused on improving control over well-understood physical systems, TQC research promises fundamental breakthroughs. Delocalised, or topological degrees of freedom are intrinsically immune to all forms of noise which do not impact the entire medium at once and coherently. For media that exhibit an energy gap, kept at low enough temperatures, this is in fact all conceivable noise. If such materials can be constructed or found in nature, they will allow a much cleaner and faster realisation of scalable quantum computation than other schemes.

B. State-of-the-art

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

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

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

C. Challenges

The research objectives cover all aspects of topological quantum computation. First of all, those related to experimental advances, like to devise ways of assessing the evidence of topological phases suitable for TQC, to design, simulate and build devices for fully scalable topological memory and gates, to propose engineered experimental realisations of topological phases, or to characterise topological phases and topological phase transitions, and link this scaling to properties of the topological entanglement entropy. From a more abstract point of view, it is necessary to develop theoretical and algorithmic aspects of topological quantum computation as a new quantum computing paradigm, to expand analytical and numerical computing skills for the FQHE and other topological systems, as well as to show robustness of topological order under local Hamiltonian perturbations or for finite temperature.

D. Key references

[1] C. Nayak, S. H. Simon, A. Stern, M. Freedman, and S. Das Sarma, "Non-Abelian anyons and topological quantum computation", Rev. Mod. Phys. 80, 1083 (2008)
[2] G. P. Collins, "Computing with quantum knots", Scientific American 294, 56 (2006)
[3] M. H. Freedman, M. J. Larsen, and Z. Wag, "A modular functor which is universal for quantum computation", Commun. Math. Phys. 227, 605 (2002)
[4] A. Yu. Kitaev, "Fault-tolerant quantum computation by anyons", Ann. Phys. 303, 1 (2003)
[5] G. Kells, J. K. Slingerland, and J. Vala, "Description of Kitaev's honeycomb model with toric-code stabilizers", Phys. Rev. B 80, 125415 (2009)
[6] W. Bishara, P. Bonderson, C. Nayak, K. Shtengel, and J. K. Slingerland, "Interferometric signature of non-Abelian anyons", Phys. Rev. B 80, 155303 (2009)
[7] M. Dolev, M. Heiblum, V. Umansky, A. Stern, and D. Mahalu, "Observation of a quarter of an electron charge at the : nu = 5/2 quantum Hall state", Nature 452, 829 (2008)
[8] I. P. Radu, J. B. Miller, C. M. Marcus, M. A. Kastner, L. N. Pfeiffer, and K. W. West, "Quasiparticle properties from tunneling in the nu = 5/2 fractional quantum hall state", Science 320, 899 (2008)
[9] S. Gladchenko, D. Olaya, E. Dupont-Ferrier, B. Doucot, L. B. Ioffe, and M. E. Gershenson, "Superconducting nanocircuits for topologically protected qubits", Nature Physics 5, 48 (2008)
[10] R. L. Willett, L. N. Pfeiffer, and K. W. West, "Measurement of filling factor 5/2 quasiparticle interference with observation of charge e/4 and e/2 period oscillations", Proc. Natl. Acad. Sci. 106, 8853 (2009)
[11] M. B. Hastings, "Topological order at non-zero temperature", Phys. Rev. Lett. 107, 210501 (2011)

Quantum error correction and purification

A. Introduction

The ability to carry out coherent quantum operations even in the presence of inevitable noise is a key requirement for quantum information processing. To cope with this decoherence problem, active strategies (quantum error correcting codes) as well as passive ones (error avoiding codes) have been developed. Error correcting codes allow one to reduce errors by suitable encoding of logical qubits into larger systems.

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

B. State-of-the-art

In the case of error correcting codes 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 favourable by several orders of magnitude. DFSs have been experimentally demonstrated in a host of physical systems, and their scope extended by generalising the idea of symmetry-aided protection to noiseless subsystems.

C. Challenges

More research needs to be done in the path of increasing the noise threshold below which error-correcting codes guarantee successful computation. Namely, new solutions must be adapted to realistic error models and to alternative models of quantum computation like the adiabatic model or the cluster model.

A fruitful connection with the theory of entanglement purification, which has been developed primarily in the context of quantum communication, and has been used in protocols such as the quantum repeater, is also emerging. Entanglement purification or distillation is a method to "distill'' from a large ensemble of impure and noisy (low-fidelity) entangled states a smaller ensemble of pure (high-fidelity) entangled states. Remarkably, not all entangled states can be distilled, which implies the existence of an irreversible form of entanglement known as bound entanglement. It seems that appropriately generalised 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.

D. Key references

[1] A. M. Steane, "General theory of quantum error correction and fault tolerance", in 'The physics of quantum information', (D. Bouwmeester, A. Ekert, A. Zeilinger, eds.), pp. 242-252, Springer, Berlin (2000)
[2] J. Preskill, "Fault-tolerant quantum computation", in "Introduction to quantum computation and information", (H. K. Lo, S. Popescu, T. Spiller, eds.) pp. 213-269, World Scientific, Singapore (1998)
[3] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed-state entanglement and quantum error correction", Phys. Rev. A 54, 3824 (1996)
[4] P. Zanardi and M. Rasetti, "Noiseless Quantum Codes", Phys. Rev. Lett. 79, 3306 (1997)

[5] D. Deutsch, A. Ekert, R. Josza, C. Macchiavello, S. Popescu, and A. Sanpera, "Quantum privacy amplification and the security of quantum cryptography over noisy channels", Phys. Rev. Lett. 77, 2818 (1996)
[6] M. Horodecki, P. Horodecki, R. Horodecki, "Mixed-state entanglement and distillation: Is there a 'bound' entanglement in nature?", Phys. Rev. Lett. 80, 5239 (1998)
[7] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum repeaters: The role of imperfect local operations in quantum communication", Phys. Rev. Lett. 81, 5932 (1998)
[8] A. M. Steane, "Overhead and noise threshold of fault-tolerant quantum error correction", Phys. Rev. A 68, 042322 (2003)
[9] E. Knill, "Quantum computing with very noisy devices", Nature 434, 39 (2005)

Geometric methods for fault-tolerant quantum computing

A. Introduction

An alternative approach to achieve fault-tolerant quantum computation is by geometric means. In this approach, quantum information is encoded in a set of energy degenerate states, depending on dynamically controllable parameters. Quantum gates are then enacted by driving the control parameters along suitable loops. These transformations, termed holonomies, are suitable to realise a set of universal quantum gates.

B. State-of-the-art

Implementation schemes of geometrical computation have been proposed for several different physical systems, most notably for trapped ions. The existing protocols for fault tolerant quantum computation have been specifically designed for phenomenological uncorrelated noise.

C. Challenges

Few results are known for a scenario with memory effects, i.e. non-Markovian noise, arising from the Hamiltonian interaction with the environment. In particular this raises the question of fault tolerant schemes for phenomenological noise with memory.

D. Key references

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

2.4.2 Quantum Communication

Communication through noisy quantum channels

A. Introduction

The proper understanding of the capacities of quantum communication channels is at the heart of the study of quantum communication tasks. Of particular importance are the transmission of classical or quantum information, or establishing secret keys. The general framework for distilling classical keys from quantum states have been also established, opening the possibility of secure communication on extremely noisy channels. But it is also known that one can use noise and perfect side communication to implement other cryptographic primitives like bit commitment and oblivious transfer. Channel capacities are of central interest in several different settings, being reflected notably by the classical capacity of quantum channels, quantum capacities, and entanglement-assisted capacities.

B. State-of-the-art

The central question is essentially what resources are required for transmitting classical or quantum information using quantum channels, such as optical fibres in a practical realisation. A problem that was left open until recently was whether an increased capacity can be obtained by employing entangled signal states (multiple uses) as opposed to single uses of the channel. This problem is widely known as the additivity problem for the Holevo capacity or - as it turned out, equivalently, the additivity problem for the minimum output entropy. This problem could recently be solved in seminal work, in that it turned out that entangled inputs indeed do help. Similarly, it has been shown theoretically that two quantum channels, each with a quantum capacity of zero, can have a non-zero capacity when used together. The key problem of identifying the classical information capacity for Gaussian channels - in the context of the promising field of continuous-variable quantum information, with practical importance in quantum communication with fibres - has recently been solved for a significant subset of channels.

C. Challenges

Many of the previous findings open up new exciting questions about the role of entanglement in quantum communication. Also, the exact relationship between entanglement and the correlations useful for establishing secret keys is not yet entirely understood, despite recent progress in this direction. Further lines of practically relevant research concern channels with uncertainty, channels with memory and the behaviour of transmission rates in the non-asymptotic regime.
It is to be expected that more problems, as well as new perspectives, will arise when one considers multi-user channels, i.e. with more than one sender/receiver. While single-sender-receiver settings serve well to study bipartite correlations, such problems have an immediate impact on understanding multi-partite correlations and their role in quantum communication via noisy channels. Also, quantum analogues of certain basic classical network theory primitives have been identified,

and the evidence for new non-classical features, such as negative partial information established. Further investigations will be needed to identify differences and similarities in the classical and quantum network theories.

D. Key references

[1] C. H. Bennett, G. Brassard, C. Crépeau, and M.-H. Skubiszewska, "Practical quantum oblivious transfer", Lecture Notes in Computer Science 576, 351 (1991)
[2] S. Holevo, "The capacity of the quantum channel with general signal states", IEEE Trans. Inf. Theory 44, 269 (1998)
[3] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, "Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem", Phys. Rev. Lett. 83, 3081 (1999)
[4] P. W. Shor, "Equivalence of additivity questions in quantum information theory", Commun. Math. Phys. 246, 453 (2004)
[5] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim "Secure key from bound entanglement", Phys. Rev. Lett. 94, 160502 (2005)
[6] P. Hayden and A. Winter, "Counterexamples to the maximal p-norm multiplicativity conjecture for all p > 1", Comm. Math. Phys. 284, 263 (2008)
[7] M. B. Hastings, "A counterexample to additivity of minimum output entropy", Nature Physics 5, 255 (2009)
[8] G. Smith and J. Yard, Science 321, 1812 (2008)
[9] V. Giovannetti, A.S. Holevo, R. Garcia-Patron, "A solution to the Gaussian optimizer conjecture", Comm. Math. Phys. 334, 1553 (2015)
[10] S. Bäuml, M. Christandl, K. Horodecki, A. Winter, "Limitations on Quantum Key Repeaters", Nature Communications 6, 6908 (2015)

Quantum communication complexity

A. Introduction

Just as quantum algorithms can lead to exponential speedup for computational problems, quantum communication can lead to exponential savings in the number of bits that need to be transmitted in order to solve a certain distributed computational problem. This idea was developed following initial work of Yao (qubit model) and Cleve and Buhrman (entanglement assisted model, in which entanglement between the protocol participants has already been generated ahead of time).

B. State-of-the-art

One the one hand, useful protocols have been found, for example, to solve the Hidden Matching and Vector-in-Subspace problems as well as a test for equality by means of quantum fingerprinting. These protocols demonstrate an exponential improvement in the communication over classical protocols. Some of these protocols have been experimentally realised.

On the other hand, communication complexity tries to establish the ultimate limits of how much communication can be saved by using a quantum protocol. An intriguing interplay between quantum communications complexity, non-locality, approximation algorithms, and functional analysis is becoming available. Ideas from quantum communication complexity thus find applications in many areas, like interactive games and approximation algorithms, lower bound for classical and quantum computers, as well as the development of new non-locality tests.

C. Challenges

A permanent open problem consists of finding quantum protocols for other communication tasks, which provide significant communication savings when compared to classical protocols. Also, one of the main open questions in quantum communication protocols is to understand the power that the entanglement assisted model offers. This is poorly understood, in part because it remains a great mathematical challenge to determine whether there exist certain non-local behaviours that would require an infinite amount of entanglement to be realised.

D. Key references

[1] A. Yao, "Quantum circuit complexity", Proceedings of the 1993 IEEE 34th Annual Foundations of Computer Science, 352 (1993)
[2] H. Buhrman, R. Cleve, and A. Wigderson, "Quantum vs. classical communication and computation", Proceedings of the 30th Annual ACM Symposium on Theory of Computing (STOC 1998)
[3] R. Cleve, P. Høyer, B. Toner, and J. Watrous, "Consequences and limits of nonlocal strategies", Proc. of 19th IEEE Conference on Computational Complexity (2004)
[4] D. Gavinsky, J. Kempe, I. Kerenidis, R. Raz, and R. de Wolf, "Exponential separations for one-way quantum communication complexity, with applications to cryptography", SIAM Journal on Computing, 38, 1695 (2008)
[5] Z. Bar-Yossef, T. S. Jayram, I. Kerenidis, "Exponential separation of quantum and classical one-way communication complexity", SIAM J. Comput. 38 (2008)
[6] J. Briët, H. Buhrman, T. Lee, and T. Vidick, "Multiplayer XOR games and quantum communication complexity with clique-wise entanglement", Quantum Information and Computation, 13 (3-4), 334-360, (2013)
[7] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf, "Nonlocality and communication complexity", Rev. Mod. Phys. 81 (2010)
[8] M. Junge, C. Palazuelos, D. Perez-Garcia, I. Villanueva, and M. M. Wolf, "Operator Space theory: a natural framework for Bell inequalities", Phys. Rev. Lett. 104, 170405 (2010)
[9] B. Klartag and O. Regev. Quantum one-way communication is exponentially stronger than classical communication. In Proceedings of 43rd ACM STOC (2011)
[10] L. Mancinska and T. Vidick, "Unbounded entanglement in non-local games", in Proceedings of ICALP, 8572, 835-846 (2014)

Quantum cryptographic protocols

A. Introduction

The most import feat of quantum computers is that they can efficiently factor integers into their prime factors. This in turns means that most of the cryptographic protocols that are used today will be rendered obsolete once a quantum computer is built, because their security crucially relies on the assumption that factoring is difficult. Significantly, any secrets that are protected by such methods today will be revealed by a quantum computer in the future.

Fortunately, not all is lost since quantum information processing allows security guarantees that are impossible to achieve classically. In particular, quantum communication can protect secrets even if the attacker has a quantum computer. Quantum key distribution (QKD) such as the well known protocol due to Bennett and Brassard, allows two mutually trustful parties to generate a shared secret key in such a way that an eavesdropper trying to obtain the key – or even part thereof – can be detected with overwhelming probability. Once a secure key is established, classical encryption protocols, like the one-time pad, allow for secure message transmission.

B. State-of-the-art

QKD systems are already commercially available. While many QKD protocols exist whose security is proven mathematically, there are proposals for new protocols for which it may be easier to achieve high rates of key generation in an implementation, but which call for further theoretical analysis.

It is natural and important to determine what other protocols are possible using quantum technologies. One of the protocols already proposed is blind quantum computation, which allows a client who has just a very simple quantum device to securely perform computations on a remote quantum computer mainframe. This is of interest since the first quantum computers are likely to be scarce. Theoretical proposals have already been shown to be experimentally feasible on very small quantum computers. Another example of proposed protocols are recently improved protocols for quantum money allowing classical verification. We expect that as quantum communication continues to mature, the development of new protocols will continue.

Nevertheless, not all cryptographic tasks can be solved securely using quantum communication without making additional assumptions. Concretely, it was realised by Mayers, Lo and Chau that cryptographic tasks in which the sender and receiver do not trust each other cannot be realised without such additions. Examples are secure identification and bit commitment. As before, however, this does not mean that all is lost. On the one hand, quantum information processing is able to realise weaker forms of cryptographic tasks that are still impossible classically such as biased Coin Tossing, weak forms of Quantum String Commitment, and Digital Signatures. On the other hand, security is possible in general under mild assumptions. A very promising one is the bounded, or more generally noisy-storage model. The assumption is that it is impossible to build quantum memories that can reliably store huge amounts of qubits for a few seconds – where right now it is difficult to store even one qubit for such a long time. However, security can always been attained by sending more qubits than a particular memory can handle. Security in this model is guaranteed into the future, in the sense that an attacker who acquires a larger quantum memory tomorrow cannot retroactively break the security of a protocol executed today. Protocols have been proposed that allow for secure implementations of the cryptographic building blocks bit commitment and oblivious transfer, and also more general tasks like position verification. These protocols are easy to implement in a similar fashion than QKD, and the feasibility of some of them has already been demonstrated experimentally. Other assumptions that have been explored include a guaranteed space-like separation between protocol participants to achieve time-limited security, or a restriction on the number of qubits an attacker can manipulate at a given moment.

C. Challenges

A challenge to be addressed is to realise more complicated tasks such as secure identification in practise, as well as the discovery of efficient protocols for other cryptographic problems. We can also hope to find classical protocols that are secure under computational assumptions even if the attacker has a quantum computer, like current cryptographic protocols are secure under the (unproven) assumption that factoring is hard. This line of research is part of post-quantum cryptography. Progress has been made by Regev who developed a protocol based on the hardness of certain lattice problems. We expect that there will be a fruitful interplay between QKD and post-quantum cryptography, and post-quantum cryptography can help with the management of authentication keys in QKD.

D. Key references

[1] C. H. Bennett and G. Brassard, ``Quantum cryptography: Public key distribution and coin tossing'', in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, p. 175 (1984)
[2] A. Ambainis, "A new protocol and lower bounds for quantum coin flipping'', Journal of Computer and System Sciences, 134 (2004)
[3] A. Chailloux and I. Kerenidis, ``Optimal quantum strong coin flipping'', 50th Annual Symposium on Foundations of Computer Science (FOCS) (2009)
[4] L-P. Lamoureux, E. Brainis, D. Amans, J. Barrett, and S. Massar ``Provably secure experimental quantum bit-string generation'', Phys. Rev. Lett. 94, 050503(4) (2005)
[5] N. Ng, S. Joshi, C. Chia, C. Kurtsiefer and S. Wehner, "Experimental implementation of bit commitment in the noisy-storage model", Nature Communications, 3,1326 (2012).
[6] F. Pastawski, N. Y. Yao, L. Jiang, M. D. Lukin, and J. I. Cirac, "Unforgeable Noise-Tolerant Quantum Tokens", PNAS 109(40), 16079-16082 (2012)
[7] H. Buhrman *et al.*, "Position-Based Quantum Cryptography: Impossibility and Constructions", SIAM J. Comput., 43(1), 150-178 (2014)
[8] S. Wehner, C. Schaffner, and B. Terhal, "Cryptography from Noisy Storage", Phys. Rev. Lett. 100, 220502 (2008)
[9] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography'', In Proc. 37th ACM Symp. on Theory of Computing (STOC), 84 (2005).
[10] A. Childs, "Secure assisted quantum computation", Quantum Information and Computation, 5(6), 456-466 (2005)

[11] Y. Liu, "Building one-time memories from isolated qubits", in Proceedings of Innovations in Theoretical Computer Science (ITCS), 269-286 (2013)

Device independent certification of security

A. Introduction

Device-independent quantum information processing represents a novel approach in which the goal is to design information protocols whose performance is independent of the internal working of the devices used in the implementation. The new framework exploits the non-local correlations exhibited by local measurements on entangled quantum particles, which certify the quantumness of the underlying state and measurements. That is, the quantumness is certified by the violation of a Bell inequality.

B. State-of-the-art

This new approach allows a qualitative increase of the security of quantum cryptography: security in QKD can be certified from the observed measurement statistics rather than relying on a complete theoretical model of the device. Specifically, security can be achieved even if the source of entangled states is not controlled and/or the measurement in the devices unknown. Device independence is also possible for the generation and quantification of certified quantum randomness. The same basic philosophy can be applied to "self testing of quantum computers": by using quantum non locality one can test (in polynomial time) that a quantum computer indeed operates as it should, without the need to model how individual gates act, or the need to carry out the full tomography of the whole computer. Finally, these techniques may also find an application in much more general estimation problems, even certifying properties of nature itself, since they allow us to estimate interesting internal properties of an unknown system only from the observed statistics.

C. Challenges

From a theoretical point of view, the main goal is to understand the possibilities and limitations of the device-independent approach. We expect that device independent security is possible for many other quantum cryptographic protocols. The challenge is to find good models and new protocols that allow the certification of quantum devices for their secure use in quantum cryptographic protocols at large.

From a more practical point of view, a major theoretical and experimental challenge is to make these proposals practical. Recently, the first loophole free Bell test was achieved by using entanglement between electron spins in diamond. This demonstrates that device independent security is indeed feasible, but further work is required to speed up the rate at which we could hope to generate key in QKD. This is in part a theoretical challenge calling for improvements in the existing protocols and their analysis, or relaxing some of the assumptions. Furthermore, a specific challenge is to prove security for device independent QKD in the most paranoid model for any violation of a Bell inequality.

D. Key references

[1] D. Mayers and A. Yao, "Self testing quantum apparatus", Quantum Inform. Comput. 4, 273 (2004)
[2] J. Barrett, L. Hardy, and A. Kent, "No Signalling and Quantum Key Distribution", Phys. Rev. Lett. 95, 010503 (2005)
[3] A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-independent security of quantum cryptography against collective attacks", Phys. Rev. Lett. 98, 230501 (2007)
[4] L. Masanes, S. Pironio, and A. Acin, "Secure device-independent quantum key distribution with causally independent measurement devices", Nature Comm. 2, 238 (2011)
[5] S. Pironio et al., "Random numbers certified by Bell's theorem", Nature 464, 1021 (2010)
[6] R. Colbeck and A. Kent, "Private randomness expansion with untrusted devices", Journal of Physics A 44, 095305 (2011)
[7] M. Hendrych et al., "Experimental estimation of the dimension of classical and quantum systems", Nature Phys. 8, 588 (2012)
[8] J. Ahrens, P. Badziag, A. Cabello, and M. Bourennane, "Experimental device-independent tests of classical and quantum dimensions", Nature Phys. 8, 592 (2012)
[9] N. Gisin, S. Pironio, and N. Sangouard, "Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplification", Phys. Rev. Lett. 105, 070501 (2010)
[10] B. Hensen et al., “Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometers”, Nature (2015); http://nature.com/articles/doi:10.1038/nature15759
[11] B. Reichardt, F. Unger, and U. Vazirani, “Classical command of quantum systems”, Nature, 496, 456-460 (2013).

2.4.3 Quantum Correlations

Theory of entanglement

A. Introduction

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 characterise 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 characterisation methods have determined that the resulting state contains entanglement one can then aim to transform the initial state into the desired final state;
- Thirdly, we aim at quantifying 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.

B. State-of-the-art

While the problem of entanglement detection has been shown to be hard, there exist numerical techniques that work well in many situations. For the experimental verification of this resource, the tool of entanglement witnesses allows detecting entanglement with local measurements only, and thus is easily implementable with present technology. Considerable progress in answering the above basic questions area has been made in recent years, in particular in the case of bi-partite entanglement.

C. Challenges

We are still far away from a comprehensive understanding of entanglement, which undoubtedly is a 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 to the field of QIS itself, but they have now reached the stage where they are being applied to other areas of physics.

D. Key references

[1] R. F. Werner, "Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model", Phys. Rev. A 40, 4277 (1989)
[2] M. Horodecki, P. Horodecki and R. Horodecki, "Separability of mixed states: necessary and sufficient conditions", Phys. Lett. A 1, 223 (1996)
[3] C. H. Bennett, H. J. Bernstein, S. Popescu and B. Schumacher, "Concentrating partial entanglement by local operations", Phys. Rev. A 53, 2046 (1996)
[4] V. Vedral and M. B. Plenio, "Entanglement measures and purification procedures", Phys. Rev. A 57, 1619 (1998)
[5] M. A. Nielsen, "Conditions for a class of entanglement transformations", Phys. Rev. Lett. 83, 436 (1999)

[6] M. Bourennane, M. Eibl, C. Kurtsiefer, S. Gaertner, H. Weinfurter, O. Guehne, P. Hyllus, D. Bruss, M. Lewenstein, and A. Sanpera, “Experimental detection of multipartite entanglement using witness operators”, Phys. Rev. Lett. 92, 087902 (2004)
[7] M. Horodecki, J. Oppenheim, and A. Winter, "Partial information can be negative”, Nature 436, 676 (2005)
[8] L. Gurvits, "Quantum matching theory (with new complexity theoretic, combinatorial and topological insights on the nature of the quantum entanglement)", arXiv:quant-ph/0201022.
[9] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, "Distinguishing separable and entangled states", Phys. Rev. Lett. 88, 187904 (2002)
[10] Recent tutorial reviews include M. B. Plenio and S. Virmani, “An introduction to entanglement measures”, Quant. Inf. Comp. 7, 1 (2007); R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, “Quantum entanglement”, Rev. Mod. Phys. 81, 865 (2009)
[11] A.W. Harrow, A. Natarajan, X. Wu, "An improved semidefinite programming hierarchy for testing entanglement", arXiv:1506.08834 (2015)

Multi-party entanglement and applications

A. Introduction

Research on multi-particle entanglement has two major applications. The first lies in the heart of quantum information science and is focused on novel protocols for quantum information processing in the multipartite setting. Since entanglement in quantum systems embodying more than two constituents is fundamentally different from two-party entanglement, novel applications are expected to be found.
The second application is a spin-off towards the field of many-body systems. Indeed, 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.

B. State-of-the-art

Multipartite protocols that have been developed include instances of secret sharing or multipartite fingerprinting. Notably, such multipartite fingerprinting schemes would allow for the determination whether a number of databases are identical with little resources.

Using the concepts developed in entanglement theory it was possible to devise new simulation methods of ground states of many-body Hamiltonians in solid-state physics (and many-body quantum systems in general). Moreover, studies seem to indicate that questions in quantum field theory may become significantly more accessible using methods from entanglement theory.

C. Challenges

Research on genuinely multipartite quantum information protocols is still taking its first steps. It is expected that future work will be able to explore the richness of multipartite quantum correlations, with direct application in e.g. network scenarios.

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 optimisation, which give rise to novel methods for classification and quantification of entanglement. Laboratory quantum states such as random states or graph states as generalisations of cluster states may facilitate such studies.

D. Key references

[1] N. Linden, S. Popescu, B. Schumacher, and M. Westmoreland, "Reversibility of local transformations of multiparticle entanglement", quant-ph/9912039
[2] W. Duer, G. Vidal, and J. I. Cirac, "Three qubits can be entangled in two inequivalent ways", Phys. Rev. A 62, 062314 (2000)
[3] V. Coffman, J. Kundu, and W. K. Wootters, ``Distributed entanglement'', Phys. Rev. A 61, 052306 (2000)
[4] C. H. Bennett, S. Popescu, D. Rohrlich, J. A. Smolin, and A. V. Thapliyal, "Exact and asymptotic measures of multipartite pure state entanglement", Phys. Rev. A 63, 012307 (2001)
[5] A. Acin, D. Bruss, M. Lewenstein, and A. Sanpera, "Classification of mixed three-qubit states", Phys. Rev. Lett. 87, 040401 (2001)
[6] M. Hein, J. Eisert, and H.-J. Briegel, "Multi-party entanglement in graph states", Phys. Rev. A 69, 062311 (2004)
[7] B. Kraus, "Local unitary equivalence of multipartite pure states", Phys. Rev. Lett. 104, 020504 (2010)

Quantum correlations in condensed matter systems

A. Introduction

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

B. State-of-the-art

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

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

Ideas of quantum information science can hence relate to

- Fundamental issues of the complexity of a classical description of quantum many-body systems in a language of computer science;
- A reassessment of the functioning of existing methods such as the Density Matrix Renormalisation Group (DMRG) approach, and,
- The development of novel feasible and efficient algorithms specifically for two-dimensional or fermionic systems, opening up new perspectives in the simulation of strongly correlated quantum many-body systems. These have recently been shown to outperform the best existing methods for some problems. (Details of the corresponding quantum algorithms are currently being worked out. Although solving the ground state properties of models like the Hubbard model is QMA hard, in many cases of practical relevance such quantum simulations can be performed with a circuit depth that grows polynomially and often linearly (up to logarithmic corrections) with system size.)

C. Challenges

The above demonstrates that research on entanglement, its characterisation, 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.

In the mid-term future, the simulation of quantum many body systems will be one of the first feasible applications of small to medium scale quantum computers. Such simulations may be the first applications where small quantum computers have the potential of outperforming any competing classical algorithm.

D. Key references

[1] K. Audenaert, J. Eisert, M. B. Plenio, and R. F. Werner, "Entanglement properties of the harmonic chain", Phys. Rev. A 66, 042327 (2002)

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

[3] M. B. Plenio, J. Eisert, J. Dreissig, and M. Cramer, "Entropy, entanglement, and area: Analytical results for harmonic lattice systems", Phys. Rev. Lett. 94, 060503 (2005)

[4] F. Verstraete and J. I. Cirac, "Renormalization algorithms for quantum many-body systems in two and higher dimensions", cond-mat/0407066

[5] J. Kempe, A. Kitaev, and O. Regev, "The complexity of the local Hamiltonian problem", SIAM Journal of Computing, Vol. 35, 1070 (2006)

[6] G. Vidal, "Entanglement renormalization", Phys. Rev. Lett. 99, 220405 (2007)

[7] L. Amico, R. Fazio, A. Osterloh, and V. Vedral, "Entanglement in many-body systems", Rev. Mod. Phys. 80, 517 (2008)

[8] F. Verstraete, J. I. Cirac, V. Murg, "Matrix product states, projected entangled pair states, and variational renormalization group methods for quantum spin systems", Adv. Phys. 57, 143 (2008)

[9] J. Eisert, M. Cramer, M. B. Plenio, "Area laws for the entanglement entropy", Rev. Mod. Phys. 81 (2010)

[10] Philippe Corboz, T. M. Rice, Matthias Troyer, "Competing states in the *t-J* model: uniform *d*-wave state versus stripe state", Phys. Rev. Lett. 113, 046402 (2014)

[11] N. Schuch and Frank Verstraete, "Computational complexity of interacting electrons and fundamental limitations of density functional theory", Nature Physics 5, 732 (2009).

[12] D. Wecker, M. B. Hastings, N. Wiebe, B. K. Clark, C. Nayak, M. Troyer, "Solving strongly correlated electron models on a quantum computer" Phys. Rev. A (2015), in press

Connection between QIP and quantum chemistry

A. Introduction

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

B. State-of-the-art

New ideas inspired by quantum information theory relate to proofs of hardness of certain questions in quantum chemistry, as well as to new simulation methods of such physical systems, contributing to the wider context of gaining a deeper understanding of complex quantum systems. For example, it has been shown that finding the exact density functional of density functional theory is a QMA hard problem.

C. Challenges

Quantum chemistry is one of the fields where quantum computers may have a large commercial impact, since quantum chemical problems can be simulated with polynomial complexity on quantum computers. Recent advances have achieved a substantial reduction in the degree of the polynomial scaling with number of electrons thus making such simulations for commercially interesting problems feasible on medium scale quantum computers.

D. Key references

[1] A. Klyachko, "Quantum marginal problem and N-representability", J. Phys. A Conf. Ser. 36, 72 (2006)
[2] Y.-K. Liu, M. Christandl, and F. Verstraete, "N-representability is QMA-complete", Phys. Rev. Lett. 98, 110503 (2007)
[3] N. Schuch and F. Verstraete, “Computational complexity of interacting electrons and fundamental limitations of density functional theory”, Nature Physics 5, 732 (2009).
[4] J.D. Whitfield, J. Biamonte, and A. Aspuru-Guzik, “Simulation of Electronic Structure Hamiltonians Using Quantum Computers”, Molecular Physics 109, 735 (2011)
[5] M.B. Hastings, D. Wecker, B. Bauer, M. Troyer, “Improving Quantum Algorithms for Quantum Chemistry”, Quantum Information and Communication 15, 1 (2015)

2.4.4 Quantum effects, quantum foundations and relations to other fields

Fundamental quantum mechanics and decoherence

A. Introduction

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

B. State-of-the-art

In fact, information concepts have been successfully applied to get a better understanding of which correlations are possible within our current description of nature, based on quantum physics and why quantum physics is not maximally non-local.

C. Challenges

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.

D. Key references

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

[2] L. Viola, "On quantum control via encoded dynamical decoupling", quant-ph/0111167

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

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

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

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

[7] D. Perez-Garcia, M.M. Wolf, C. Palazuelos, I. Villanueva, and M. Junge, "Unbounded violation of tripartite Bell inequalities", Comm. Math. Phys. 279, 455 (2008)

[8] M. Navascués, S. Pironio, and A. Acín, "A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations", New J. Phys. 10, 073013 (2008)

[9] M. Pawlowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Zukowski, "Information causality as a physical principle", Nature 461, 1101 (2009)

Quantum effects in opto-mechanical and nano-mechanical systems

A. Introduction

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

B. State-of-the-art

Following a remarkably fast-paced development in cooling techniques using radiation pressure, largely driven by a European research effort, the laser cooling of a nano-mechanical oscillator into its quantum ground state has been achieved recently, opening up new perspectives for using such devices in QIPC applications. In the last years, ground state cooling of several nano-mechanical systems has been achieved.

C. Challenges

One of the major challenges nowadays is to reach the single-phonon non-linear regime, where non-Gaussian states can be created. There have been several theoretical proposals to reach that regime, although none of them has been experimentally demonstrated. Another challenge is to levitate nano or microspheres, and cool them to the ground state, in order to test fundamental questions related to decoherence, or for applications. Besides all that, new applications of such devices are also highly desired.

D. Key references

[1] C. Fabre, M. Pinard, S. Bourzeix, A. Heidmann, E. Giacobino, and S. Reynaud, "Quantum-noise reduction using a cavity with a movable mirror", Phys. Rev. A 49, 1337 (1994)
[2] S. Mancini, V. I. Manko, and P. Tombesi, "Ponderomotive control of quantum macroscopic coherence", Phys. Rev. A 55, 3042 (1997)
[3] I. Martin, A. Shnirman, L. Tian, and P. Zoller, "Ground-state cooling of mechanical resonators", Phys. Rev. B 69, 125339 (2004)
[4] J. Eisert, M. B. Plenio, S. Bose, and J. Hartley, "Towards quantum entanglement in nanoelectromechanical devices", Phys. Rev. Lett. 93, 190402 (2004)
[5] D. Vitali, S. Gigan, A. Ferreira, H. R. Böhm, P. Tombesi, A. Guerreiro, V. Vedral, A. Zeilinger, and M. Aspelmeyer, "Optomechanical entanglement between a movable mirror and a cavity field", Phys. Rev. Lett. 98, 030405 (2007)
[6] F. Marquardt and S. M. Girvin, "Optomechanics", Physics 2, 40 (2009)
[7] M. Wallquist, K. Hammerer, P. Zoller, C. Genes, M. Ludwig, F. Marquardt, P. Treutlein, J. Ye, and H. J. Kimble, arXiv:0912.4424 [quant-ph]
[8] O. Arcizet, P.-F. Cohadon, T. Briant, M. Pinard, and A. Heidmann, "Radiation-pressure cooling and optomechanical instability of a micro-mirror", Nature 444, 71 (2006)

[9] D. Kleckner and D. Bouwmeester, "Sub Kelvin optical cooling of a micromechanical resonator", Nature 444, 75 (2006)
[10] S. Gigan *et al.*, "Self-cooling of a micro-mirror by radiation pressure", Nature 444, 67 (2006)
[11] A. Schliesser, P. Del'Haye, N. Nooshi, K. J. Vahala, and T. J. Kippenberg, "Radiation pressure cooling of a micromechanical oscillator using dynamical backaction", Phys. Rev. Lett. 97, 243905 (2006)
[12] A. D. O'Connell *et al.*, "Quantum ground state and single-phonon control of a mechanical resonator", Nature 464, 697 (2010)
[13] J. Chan, T. P. Mayer Alegre, A. H. Safavi-Naeini, J. T. Hill, A. Krause, S. Groeblacher, M. Aspelmeyer, and O. Painter, "Laser cooling of a nanomechanical oscillator into its quantum ground state", Nature 478, 89 (2011)

Quantum thermodynamics

A. Introduction

Quantum Thermodynamics has been rapidly emerging at the intersection of Quantum Information Theory and many-body physics over the past decade. It connects macroscopic thermodynamics with microscopic insights and new information-theoretic methods from Quantum Information Theory, such as non-asymptotic entropy measures, high-dimensional geometry, and tensor-network states. Quantum Thermodynamics affords a deeper understanding of the foundations of Statistical Mechanics, and on the other hand allows the treatment of relevant mesoscopic situations, such as biochemical processes, where a purely thermodynamic description is too coarse.

B. State-of-the-art

The long-standing issues of equilibration and thermalisation have now been understood to involve both kinematic and dynamic aspects. The former explain how equilibrium states can arise due to quantum entanglement. Secondly, microscopic conditions related to the absence of dynamical symmetries have been identified that will lead to equilibration. In another vein, several frameworks have been established to capture the macroscopic notions of work and heat in microscopic terms, most notably based on so-called resource theories and single-shot entropies. Out-of-equilibrium situations are investigated more easily than in traditional Thermodynamics, where non-equilibrium entropy is a controversial notion. The eminent classical fluctuation relations have been generalised to encompass quantum fluctuations and the laws of thermodynamics are formalised and quantified taking into account insight from Quantum Information Science.

C. Challenges

The challenge for Quantum Thermodynamics is to identify simple but physically suitable coarse-grained descriptions in order to connect the microscopic formalism with macroscopic phenomena. The connection to Quantum Information Science brings a new viewpoint that is operational, focuses on resources and uses descriptions that are as model independent as possible. With this in mind the field aims at a deeper understanding of the emergence and speed of thermalisation and equilibration, the limitations of cooling, information erasure and work extraction as well as the efficiency of heat engines and catalysts.

D. Key references

[1] S. Popescu, A. J. Short, A. Winter, "Entanglement and the foundations of statistical mechanics", Nat. Phys. 2, 754 (2006)
[2] P. Reimann, "Foundation of Statistical Mechanics under Experimentally Realistic Conditions", Phys. Rev. Lett. 101, 190403 (2008)
[3] J. Goold, M. Huber, A. Riera, L. del Rio, P. Skrzypczyk, "The role of quantum information in thermodynamics - a topical review", arXiv:1505.07835 [quant-ph] (2015)
[4] L. del Rio, J. Aberg, R. Renner, O. Dahlsten, V. Vedral, "The thermodynamic meaning of negative entropy", Nature 474, 61 (2011)
[5] M. Horodecki, J. Oppenheim, "Fundamental limitations for quantum and nanoscale thermodynamics", Nat. Commun. 4, 2059 (2013)
[6] F. G. S. L. Brandao, M. Horodecki, J. Oppenheim, J. M. Renes, R. W. Spekkens, "Resource Theory of Quantum States Out of Thermal Equilibrium", Phys. Rev. Lett. 111, 250404 (2013)
[7] F. Brandao, M. Horodecki, N. Ng, J. Oppenheim, S. Wehner, "The second laws of quantum thermodynamics", Proc. Natl. Acad. Sci. 112, 3275 (2015)
[8] M. Campisi, P. Talkner, P. Hanggi ,"Fluctuation Theorem for Arbitrary Open Quantum Systems", Phys. Rev. Lett. 102, 210401 (2009)
[9] J. L. England, "Statistical physics of self-replication", J. Chem. Phys. 139, 121923 (2013)
[10] N. Linden, S. Popescu, and P. Skrzypczyk, "How Small Can Thermal Machines Be The Smallest Possible Refrigerator", Phys. Rev. Lett. 105, 130401 (2010)

Spin-offs to other fields

A. Introduction

In the last years, results and tools from quantum information science have found their way into various other fields and disciplines. These are often fields where quantum mechanics plays a role, albeit not necessarily the leading one, and where quantum information science leads to novel perspectives. Two examples of this kind are the appearance of quantum information science in bio-physics and in quantum gravity, which will in the following be briefly discussed.

B. State-of-the-art

The experimental observation of quantum coherence during excitation energy transfer and the subsequent elucidation of the role that noise and coherent dynamics plays in such systems represent a very intriguing recent development at the boundary of quantum physics and biology. An increasing number of biological systems are now being investigated for the possible functional role of quantum dynamics including for example magneto-reception in birds and olfaction. The question to what extent quantum dynamics plays a role in biological systems is now receiving increasing attention from the perspective of quantum information theory. Indeed, principles and techniques, numerical, analytical and conceptual, that have been developed over the last two decades in quantum information science may find a new area of application here and contribute to an understanding of the role of noise, coherent dynamics and their interplay in such systems. This potentially fruitful new arena is now beginning to be explored bringing together quantum information scientists with bio-physicists from theory and experiment thus opening up a new arena of interdisciplinary research.

Similar development can be seen in a different direction of theoretical physics that tries to relate space-time geometry, gravity and quantum theory. The Bekenstein-Hawking formula for the entropy of black holes as well as the related black-hole information paradox already suggest the use of information theoretic tools in the quest for quantum gravity. Methods of quantum information theory have indeed begun to solve and sharpen problems in quantum field theory and quantum gravity, while at the same time rising new questions. The renormalisation group, a central tool in quantum field theory, starts to appear in a new light; quantum computational complexity enters the evolution of the geometry behind the black hole horizon; the holographic entanglement entropy connects quantum information theory with space-time geometry; quantum error correcting codes are invoked to describe the boundary state in ADS/CFT; and a careful analysis of entanglement seems to suggest that the black-hole horizon may have to be replaced by a firewall.

C. Challenges

The exact role of quantum effects, such as entanglement and coherences, in biological processes is still poorly understood and deserves further investigation. The connection between quantum information concepts and quantum gravity also seem promising and deserve further study.

D. Key references

[1] G. S. Engel, T. R. Calhoun, E. L. Read, T.-K. Ahn, T. Mancal, Y-C. Cheng, R. E. Blankenship, and G. R. Fleming, "Evidence for wavelike energy transfer through quantum coherence in photosynthetic complexes", Nature 446, 782 (2007)
[2] G.D. Scholes, G.R. Fleming, A. Olaya-Castro, and R. van Grondelle, “Lessons from nature about solar light harvesting”, Nature Chemistry 3, 763 (2011)
[3] M. Mohseni, P. Rebentrost, S. Lloyd, and A. Aspuru-Guzik, "Environment-assisted quantum walks in photosynthetic energy transfer", J. Chem. Phys. 129, 174106 (2008)
[4] M. B. Plenio and S. F. Huelga, "Dephasing assisted transport: Quantum networks and biomolecules", New J. Phys. 10, 113019 (2008)
[5] A. Olaya-Castro, C. F. Lee, F. Fassioli-Olsen, and N. F. Johnson, "Efficiency of energy transfer in a light-harvesting system under quantum coherence", Phys. Rev. B 78, 085115 (2008)
[6] F. Caruso, A. W. Chin, A. Datta, S. F. Huelga, and M. B. Plenio, "Highly efficient energy excitation transfer in light-harvesting complexes: The fundamental role of noise-assisted transport", J. Chem. Phys. 131, 105106 (2009)

[7] K. Schulten, Th. Ritz, and S. Adem, “A model for photoreceptor-based magnetoreception in birds”, Biophys. J. 78, 707 (2000); J.M. Cai, G.G. Guerreschi and H. J. Briegel, “Quantum control and entanglement in a chemical compass”, Phys. Rev. Lett. 104, 220502 (2010)
[8] L. Turin, "A Spectroscopic Mechanism for Primary Olfactory Reception", Chem. Senses 21, 773 (1996); M. I. Franco, L. A. Turin, A. Mershin, and E. M. Skoulakis, "Molecular vibration- sensing component in Drosophila melanogaster olfaction", Proc. Nat. Acad. Sci. 108, 3797 (2011)
[9] “Quantum effects in biological systems”, Edited by M. Mohseni, Y. Omar, G. Engel, and M. B. Plenio, Cambridge University Press 2012
[10] J.M. Maldacena, "Eternal black holes in anti-de Sitter", JHEP 04, 021 (2004)
[11] S. Ryu, and T. Takayanagi, "Holographic derivation of entanglement entropy from the anti–de Sitter space/conformal field theory correspondence", Phys. Rev. Lett. 96, 18 181602 (2006); H. Casini, M. Huerta, and R. C. Myers, "Towards a derivation of holographic entanglement entropy", JHEP 5,1 (2011)
[12] F. Pastawski, B. Yoshida, D. Harlow, and J. Preskill, "Holographic quantum error-correcting codes: Toy models for the bulk/boundary correspondence", JHEP 06, 149 (2015)
[13] A.Almheiri, D.Marolf, J.Polchinski,and J.Sully, "Black holes: complementarity or firewalls?", JHEP 2,1 (2013); D. Harlow and P. Hayden, "Quantum computation vs. firewalls", JHEP 1306, 085 (2013)
[14] J. Oppenheim and W. G. Unruh, "Firewalls and flat mirrors: An alternative to the amps experiment which evades the Harlow-Hayden obstacle", JHEP 1403, 120 (2014)

"Quantum proofs" for classical problems

A. Introduction

Thepotential that QIT is offering for classical computing and mathematics may be illustrated by the following analogy: real analysis is a very successful discipline, but some of its problems were only solved properly by considering complex numbers, i.e., by going to a larger space in which to describe the problem. By analogy, moving from classical state space into the much larger quantum mechanical state space we find novel approaches towards the solution of problems that ostensibly lie entirely within the classical realm. Quantum information theory thus offers novel proof tools and a novel perspective on classical problems, having a growing impact outside of quantum theory itself.

B. State-of-the-art

In the case of classical computing, insights provided by QIT include the first exponential bounds on certain locally decodable codes, classical proof systems for lattice problems, bounds on the classical 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 realise a reversible classical computation. Recently, a 20-year old open problem on the non-existence of efficient linear programs whose associated polytope projects to the traveling salesman polytope was solved, inspired by earlier results about quantum communication protocols. Similarly, recent ideas from quantum state tomography and quantum compressed sensing are now routinely used in classical compressed sensing and the theory of image processing. On the side of pure mathematics, quantum information ideas have led to the proof of a longstanding conjecture in functional analysis.

The entanglement between two systems cannot be shared with many others, a principle called monogamy: this leads to a fruitful relationship between entanglement theory and classical cryptography, and in particular between entanglement distillation and the classical key-agreement scenario. Since the two schemes share similar objects, quantities and relations, it is expected that the parallel growth of these domains will lead to a deeper understanding of both of them. For instance, it has been conjectured that there exists a classical cryptographic analogue of bound entanglement, named bound information. While its existence remains unproven for two parties, a proof has been obtained in a multipartite scenario.

C. Challenges

The problem of bound information remains open since its existence was conjectured in 2000 [3]. Another line of research that deserves further investigation is the connection between decidability and quantum physics. In last years, it has been noted that many questions in quantum information theory, and also quantum physics, are algorithmically undecidable [9]. It is important to understand which problems fit into this category.

D. Key references

[1] I. Kerenidis and R. de Wolf, "Exponential lower bound for 2-query locally decodable codes via a quantum argument", Journal of Computer and System Sciences, 69(3):395-420 (2004)

[2] S. Popescu, B. Groisman and S. Massar, "Lower bound on the number of Toffoli gates in a classical reversible circuit through quantum information concepts", Phys. Rev. Lett. 95, 120503 (2005)

[3] N. Gisin and S. Wolf, "Linking classical and quantum key agreement: Is there “Bound information”?" in Proceedings of CRYPTO 2000, Lecture Notes in Computer Science vol. 1880, pp. 482-500, Springer (2000)

[4] A. Acin, J. I. Cirac and Ll. Masanes, "Multipartite bound information exists and can be activated", Phys. Rev. Lett. 92, 107903 (2004)

[5] D. Gross, Y.-K. Liu, S. Flammia, S. Becker and J. Eisert, "Quantum state tomography via compressed sensing", arXiv:0909.3304 [quant-ph]; D. Gross, "Recovering low-rank matrices from few coefficients in any basis", arXiv:0910.1879 [quant-ph]

[6] A. Drucker and R. de Wolf, "Quantum proofs for classical problems", Theory of Computing, Graduate Surveys 2 (2011)

[7] J. Briet, H. Buhrman, T. Lee and T. Vidick, "All Schatten spaces endowed with the Schur product are Q-algebras", Journal of Functional Analysis 262(1), 2012

[8] S. Fiorini, S. Massar, S. Pokutta, H. R. Tiwary, and R. de Wolf, "Exponential Lower Bounds for Polytopes in Combinatorial Optimization", Journal of the ACM, 62(2):17 (2015)
[9] T. Cubitt, D. Perez-Garcia and M. M. Wolf, “Undecidability of the Spectral Gap”, Nature 528, 207-211 (2015)

2.5 Quantum Metrology, Sensing and Imaging

Measurement is the basis not only of science, which demands empirical quantitative assessment of phenomena, but also of commerce, for without agreed standards of metrology, there is no common basis for the exchange of goods and services, including information. For these reasons, sensors are a vitally important technology, underpinning, for instance, navigation, geo-prospecting, chemical and materials analysis and characterization, fundamental science from the sub-nano- to the galactic scale as well as determining the fundamental constants relied upon for industry and society.

The central concept of a sensor is that a probe interacts with a system that carries the property of interest, and changes of state of the probe. Measurements of the probe may reveal the parameters of this property. In quantum-enhanced sensors, the probe is generally prepared in a particular non-classical state. The encounter with the system modifies this state both usefully (by responding to the parameter of interest) and detrimentally (by erasing or decohering the probe). Properly designed measurements then determine in what way and to what degree the state of the probe has been altered by the encounter. This enables an estimate of the sensor parameters to be made, and thus the sensor response to be determined. The precision of this estimate as a function of the resources used is a measure of the effectiveness of the sensor.

In the quantum domain, there often uncertainties in the outcome of measurements even for probes and systems prepared in pure quantum states: this is a natural consequence of their quantum character. Nonetheless, and perhaps surprisingly, quantum phenomena have proven to be a valuable resource for devising measurement, sensing and imaging technologies that go beyond those available in a purely classical framework.

Quantum-enhanced metrology is concerned with a single task: preparing a quantum state that is sensitive to a parameter, ϕ, and implementing a measurement on that state so that the uncertainty in the measurement of the parameter, $\Delta\phi$, is lower than the uncertainty that would be obtained by using the same number of classical resources. Typically, only the scaling behaviour of $\Delta\phi$ with the number of particles in the state, N, is considered, since at large enough N a class of states that provides only a constant factor improvement can always be beaten by one that has a more favourable scaling. The tightest known limit on precision is given by the Heisenberg limit (HL), $\Delta\phi > \Delta\phi_{HL} = 1/\sqrt{\nu}N$, where ν is the number of experimental trials.

It is know that both quantum coherence (such as, in photonic interferometric sensing, a single-mode squeezed state) and quantum entanglement (such as a two-mode *N00N* state (a superposition of *N (0)* photons in one mode with *0 (N)* photons)) can be used to achieve this precision. These commonly used resources are now being used to obtain groundbreaking levels of sensor operation.

The impact of quantum sensing technologies is broad and considerable. From ultra-high-precision spectroscopy and microscopy, positioning systems, clocks, gravitational, electrical and magnetic field sensors, to optical resolution beyond the wavelength limit. All these technologies find important applications in fields as physics, chemistry, biology, medicine or data storage and processing.

There is also the opportunity that quantum-enhanced sensor technologies will allow scientists to probe physics beyond current laws of nature, such as, for instance, the violation of Lorenz invariance, testing string theory predictions (by means of precise measurements of the electron dipole moment), and probing fundamental decoherence emerging from new physics (providing understanding for the emergence of the classical world from the quantum world).

Attaining quantum-enhanced precision beyond standard quantum limits relies on generating, manipulating and measuring non-classical single-particle or collective many-body quantum states, a demanding task from an experimental perspective. Although proof-of-principle results have been obtained, much work is needed in order to generalise these results to noisy real-world scenarios, in particular, original techniques are necessary. Because of the wide range of prospective applications and their specificity, a broad range of physical platforms needs to be considered, including (but not limited to) trapped ions, ultra-cold atoms and room-temperature atomic vapours, nano- and micromechanical oscillators, artificial systems such as quantum dots and defect centres, as well as all-optical set-ups based e.g. on nonlinear optical interactions.

2.5.1. Quantum metrology

A. Physical approach and perspective

Quantum entanglement provides instances of quantum states of objects that can be designed to be robust against unwanted noise, while at the same time being extremely sensitive to the quantity we need to measure. This sensitivity can be exploited to overcome the classical limits of accuracy in various kinds of measurements, for example in ultra-high-precision spectroscopy and microscopy, or in procedures such as positioning systems, ranging and clock synchronisation via the use of frequency-entangled pulses.

Nonetheless, although states with less than maximal entanglement can nevertheless provide enhanced sensor performance, this always comes with the cost that they cannot achieve the full Heisenberg limit. [17] This bound can in principle by attained even in noisy sensors by means of quantum error correction (i.e. using feedback) in order to stabilize the system.[18]

For instance, in the latter case, picosecond resolution at 3 km distance has been attained. Large-scale laser interferometers with kilometre arm lengths are operating in Europe, the USA and Japan with the goal to directly observe gravitational waves and thus to open a new field of astronomy. The first detection of a gravitational wave recently occurred at the advanced LIGO interferometer [1]. It currently operates at the quantum shot noise level, but a significantly higher rate of events can be expected by injecting the interferometer with squeezed light. A collaboration of scientists from Europe, USA and Australia (LIGO Scientific Cluster) has recently reported around 3dB quantum noise reduction in the sensitivity of the gravitational wave detector in Germany (GEO600) [2] and in the USA (LIGO) [3] through injection of squeezed laser light at kilohertz frequencies. A noise reduction of 10dB corresponds to an increased sensitivity of 1000 in the event rate, and thus for the advanced LIGO interferometer, it leads to an event rate of about 20000 per year.

State-of-the-art atom clocks and atom interferometric inertial sensors have reached the level of accuracy limited by quantum noise of atoms. Entanglement of atoms in these devices may allow surpassing this limit by generation of spin or number squeezed states of atoms. Work towards this goal is going on in Europe and in the US. Atoms may as well be used to probe their environment. Hence, we can nowadays cool atoms at few nanoKelvin above absolute zero, where their quantum behaviour, e.g. wave properties, is dominant. Using these matter-waves in interferometers allows today to precisely measure gravity, rotation and acceleration. For instance, work towards using atom accelerometer in space to test the equivalence principle at the quantum level is going on in Europe. Matter-wave interferometry is also likely to extend the observation window of gravitational wave detectors on ground thanks to their exquisite sensitivity to spatial gravitational fluctuations, as proposed by the French MIGA consortium.

Magnetometers based on thermal atom ensembles already show spin squeezing, allowing them to surpass the sensitivity of SQUID magnetometers, but without the need of cooling. The potential of brain monitoring relating to dementia, epilepsy and trauma research, has triggered extensive activities in the development of these sensors in the US and in Europe.

Single quantum particles can be used as nanoscopic probes of external fields. Along these lines, atomic-scale (up to few nanometers) resolution in the measurement of the spatial structure of an optical field via a single ion, as well as sub-shot-noise atomic magnetometry via spin squeezing and real-time feedback have been already experimentally demonstrated. Solid-state implementations of quantum sensors exploit the quantum features of artificial atoms such as defect colour centres, most prominently nitrogen vacancies in diamond. They are now being used as ultrasensitive probes for magnetic and electric fields, with enhanced resolution through quantum control techniques. While electron spin resonance in diamond NV centres was known for a long time, it took the understanding of interaction between a spin with a many-body spin bath, i.e. quantum many body physics, to develop such exquisite magnetic field sensors that surpass existing sensing capabilities by many orders of magnitude. It allows performing NMR on a single nuclear spin, and it is expected to yield to single molecule NMR at ambient conditions. The quantum properties of these single spins within fluorescent particles are now also being used to study in-situ dynamical probes of biological environments, for example by optically detecting magnetic resonance of individual fluorescent nano-diamonds that are distinguished through their individual Rabi frequency inside living cells. Such single-spin probes in biological systems may open up a host of new possibilities for quantum-based imaging in the life sciences.

The performance of such sensors can be improved by means of hybrid devices. For example, by combining two non-equivalent physical systems one may harness the strengths and avoid the weaknesses of the individual systems. For instance the combination of magnetic materials with diamond sensors enables enhancement of field sensing.[19] A second example is the combination of a relatively fragile quantum object such as an electron spin with a stable quantum object such as a nuclear spin in such as way as to use the fragile system for sensing and the stable system for accumulating the result in a manner that leads to superior performance.[18]

The quantum regime is being explored and applied also in the manipulation of mechanical devices like rods and cantilevers as well as levitated particles of nanometer scale, currently under investigation as sensors for the detection of extremely small forces and displacements. Several groups in both Europe and the US have now achieved preparation and control of nano- and micromechanical systems in the quantum regime, including squeezed and entangled states of motion as well as real-time quantum feedback, reaching measurement sensitivities at and beyond the standard quantum limit. In addition, hybrid optomechanical devices, which comprise electrical, microwave or optical systems together with micro- and nano-mechanical transduction, provide a new platform for the processing of quantum signals, including low-noise amplification, optical-to-microwave conversion and other on-chip sensing architectures.

B. State of the art

Photonic sensors

One of the main steps in the development of quantum states of light and quantum entanglement tools was a practical design of ultra-bright sources of correlated photons and development of novel principles of entangled states engineering. This also includes entangled states of higher dimensionality and entangled quantum states demonstrating simultaneous entanglement in several pairs of quantum variables (hyper-entanglement), and calibration of single-photon detectors without any need for using traditional blackbody radiation sources. This unique possibility of self-referencing present in the optical system that is distributed in space-time is the main advantage of quantum correlation and entanglement. The fact that spontaneous parametric down-conversion (SPDC) is initiated by vacuum fluctuations serves as a universal and independent reference for measuring the optical radiation brightness (radiance). It gives the possibility of accurately measuring the infrared radiation brightness without the need of using very noisy and low sensitivity infrared detectors. Development of periodically poled nonlinear structures has opened the road for practical implementation of sources with high intensity of entangled-photon flux and with ultra-high spectral bandwidth for biomedical coherence imaging. Recent demonstrations have shown the possibilities for multi-photon interferometry beyond the classical limit. It has been shown that weak field homodyning could yield enhanced resolution in phase detection.

First experimental implementations of quantum ellipsometry indicated the high potential of quantum polarisation measurement while the first demonstration of quantum microscopy with NOON states demonstrated the potential of using fragile quantum states in an application [4]. The basic physical principles of optical coherence tomography with dispersion cancellation using frequency entangled photon pairs for sub-micron biomedical imaging have been demonstrated in model environments. The use of quantum correlations led to the design of a new technique for characterising chromatic dispersion in fibres. The intrinsically quantum interplay between the polarisation and frequency entanglement in CSPDC gave rise to a polarisation mode dispersion measurement technique that provides an order of magnitude enhancement in the resolution.

In addition to quantum correlated photon states, (macroscopic) squeezed states of light can be also used as a viable source for quantum-enhanced sensing. The technology of squeezed light sources has been significantly advanced in recent years with demonstrated noise suppression down to 95% of the shot noise level. This technology has now matured to a point where real-life applications can be explored. Besides the demonstrations of quantum-enhanced gravitational wave interferometry, squeezed light has been exploited to resolve a small beam displacement [5], which in turn has been used to perform quantum-enhanced microrheology on a living cell [6].

Quantum Imaging

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.

All high-end applications such as imaging, microscopy, and spectroscopy are multi-parameter problems. Rather than using raster-scanning a sample, different pixels (spatial, temporal, spectral) can be estimated simultaneously. Indeed, it was shown in 2013 that for a fixed number of photons, simultaneous estimation of multiple pixels is always more efficient than estimating them individually [15]. It relies on multimode or multipartite quantum correlations whose role had never before been identified and exploited in quantum sensing and imaging, owing to single-phase estimation being the focus of attention. Over the last couple of years though however, some experimental advances have been made in the direction of multiple phase estimation, exploiting multiphoton states, and this novel effect can benefit immensely from the development of multi-mode entangled photonic states. Applications such as the quantum enhanced phase retrieval have also exploited this, and other applications in networked quantum sensors have been proposed in the USA.

Fixed photon number states are always more vulnerable to losses as compared to unlimited photon number states. This is because the loss of photons (which is likely to be higher for higher photon numbers) in a fixed photon number state reduces its number variance more drastically than that of an infinite photon number state, and it is the number variance that ultimately determines the precsion of any estimation procedure. Therefore, states with a fixed average energy (number) rather than fixed maximum energy (number) are much more attractive for realistic sensing applications. Most common among these are squeezed states (more generally Gaussian states), which are relatively easily produced and manipulated, and have a proved track record in quantum-enhanced sensing.

Very recently, multi-mode imaging with Gaussian states have been studied [16]. It suggests that there may be fundamental limits to what can be achieved with multi-mode Gaussian systems, which reveals aspects of multimode quantum Gaussian systems that were unknown. Limitations of Gaussian systems in quantum communication and computation are well understood, but the identification of such a possible limitation in metrology applications is novel. Research in fundamental quantum information metrology is therefore needed to fully explore the scope of possibilities here. These studies will have long ranging implications not just in optical sensing, but also the rapidly developing field of quantum opto-mechanical sensors.

Atom-based sensors

The past decades has seen dramatic progress in our ability to manipulate and coherently control the motion of individual as well as small ensembles of atoms. The exquisite control of matter waves now offers the prospect of a new generation of force sensors of unprecedented sensitivity and accuracy, from applications in navigation and geophysics, to tests of general relativity or study of highly-entangled quantum states. Thanks to the latest technological developments, the first commercial sensors using this quantum technology are now available. A matter-wave interferometer is performed by applying successive beam-splitting processes to an ensemble of atoms, followed by detection of the atoms in each of the two output channels. Splitting is achieved using an appropriate light pulse, which changes an atom from an initial quantum state to a superposition of two different quantum states with different velocities. With matter-waves, interferometers are usually based on the Mach-Zehnder design. As with light, the interference fringes observed in the output of the matter-wave interferometer reveal differences in the path of the two matter-waves: a longer path, an interaction with an obstacle in one of the path, etc. The accumulation of phase along the two paths leads to interference at the last beam-splitter, producing complementary probability amplitudes in the two output channels. In contrast to a light-based interferometer, where the electromagnetic waves travel at the speed of the light, the atomic waves in an atom interferometer, travel at much slower speed, and thus spend a much longer time interrogating the sample. These interferometers are consequently more sensitive to their environment than their optical counterpart; up to 10^{11} times for the same interferometer area and signal to noise.

Atomic gravity sensors

2016 celebrates the 25th anniversary of atom interferometry, which harnesses the sensitivity of quantum superposition to create ultra-precise sensors for gravity, rotation, magnetic fields and time, surpassing their best classical counterparts. Owing to their maturity, they are ready for translation into commercial products and spin-offs such as AOSense (Stanford), Muquans (Bordeaux) and AtomicSense (Florence) are starting to engage in the market for gravity sensors and clocks. In addition developments towards space missions have driven the development of robust technologies, e.g. leading to atom interferometry in drop tower experiments [7]. Current atomic gravity sensors offer absolute measurements at the nano-g level or gravity gradient sensitivities surpassing a 100 pico-g change over 1m distances. These sensitivities are sufficient to open up a completely new era in imaging objects under the ground. The potential impact includes urban infrastructure with less roadworks and reduced water losses, climate research, geophysics and underground aquifer control, enhanced oil and mineral recovery, carbon storage and natural disaster pre-warning in the area of earthquakes and volcano activity.

Although these effects become visible with current state-of-the art sensitivities, a wide economic uptake and full benefit up to consumer devices will only be possible with significant miniaturization and improvements in sensitivity per volume and bandwidth. Scaling approaches using multi-photon atom optics have shown impressive advances with up to 100-fold improvement, however more is needed and current devices are still limited by atomic shot noise. Here entanglement of the atomic source promises another improvement of several orders of magnitude as recently demonstrated in a proof-of-principle experiment [8]. This might ultimately enable smart-phone sized detectors opening disruptive consumer applications, e.g.

allowing everyone to check subsurface pipes to prevent subsidence and sink holes as easily as one can now checking for electrical cables in the walls of buildings.

Atomic clocks

Atomic clocks are the most established example of quantum technology, having been used since 1967 for international timekeeping. The performance of today's best atomic clocks has reached remarkable levels, in terms of both stability and accuracy, making it possible to measure time and frequency more precisely than any other physical quantity. As a result, precision timing is now ubiquitous and underpins many aspects of our daily lives. Technologies that are now taken almost for granted by the majority of the population, such as mobile phones, the internet and global satellite navigation systems, all depend critically on time and frequency standards for their proper operation. While chip-scale atomic clocks (CSAC) based on miniature packaged vapor cells and ubiquitous in navigation and telecommunications, a new generation of clocks may be realized when using the recent advances of chip-scale microresonators based optical frequency combs, that are fabricated using semiconductor processing techniques and enable dramatic reduction of size, weight and power of the necessary clockwork to create optical atomic clocks.

Optomechanical sensors

In the past decade a technological and scientific paradigm shift has taken place around the optical and quantum control of nano- and micromechanical devices. Following quantum control of ions, molecules, as well as electrical circuits, NEMS (nano-electromechanical systems) and MEMS can now be read out and controlled at the quantum level by coupling them to optical cavities or superconducting microwave circuits. Recent demonstrations include squeezed mechanical states and QND measurements of mechanical motion, quantum coherent coupling in the optical and microwave domain, optomechanical ponderomotive squeezing and entanglement, a photon-phonon interface, real time quantum feedback, among many others. Current research in this field explores the physical limits of hybrid opto- and electro-mechanical devices for conversion, synthesis, processing, sensing and measurement of electromagnetic fields, from radio and microwave frequencies to the terahertz domain. The ability to modulate, interconvert, amplify or measure electromagnetic fields in this spectral region, is relevant to a number of existing application domains, specifically medicine (e.g. MRI imaging), security (e.g. Radar and THz monitoring)positioning, as well as timing and navigation (oscillators). At the same time, optomechanical systems provide an on-chip architecture to realize e.g. sensing, acceleration measurements, as well as low-noise amplification and novel non-reciprocal microwave components. While such devices can be used already in a classical context, where measurement of weak signals is relevant, extending the operation range into the quantum regime opens applications also in quantum science and technology, including quantum frequency translation from of visible photons to the telecommunication band,, or realizing single-photon optical-to-microwave conversion, as well as sensors e.g. for charge, magnetic fields or mass. In addition the ability to operate such optomechanical transducers in a regime where quantum noise plays a role also enables to create compact quantum noise calibrated thermometers.

C. Challenges

It remains a challenge for the field to demonstrate experimentally that it is possible to surpass the standard quantum or interferometric limits (SQL/SIL) in lossy sensors. In the case of photonic sensors, for example, it is known that the classes of quantum states that achieve this depend on the degree of loss, and that the Heisenberg scaling limit is never achieved when losses are present. However, there can be large swathes across the parameter regime where a quantum photonic sensor can be better than anything possible classically, even in the presence of losses. Historically, detector efficiencies were a limitation, but the recent development of superconducting photon counting detectors (transition edge, nanowire) has shifted the bottleneck to coupling losses between different segments of the sensor. This coupling efficiency, which is typically restricted to 60%-65% is eventually limited by the mode overlap of the photons emerging from the sources such as waveguides and being coupled into optical fibres leading to detectors.

Nonetheless, certain states can give better improvements above the SQL than others. Squeezed states are certainly more robust for larger losses and have been used to improve the SNR in interferometric sensors, and for these states improving coupling of the probe to the sensor and reducing losses are key improvements.

New measurement protocols as well as post-processing of the results can be further optimized. For instance, feedback-based protocols, dynamical decoupling, optimal control may all add new capabilities to quantum sensing protocols.[18] Powerful methods from signal processing, which have already yielded fruit in the design and assessment of sensor performance, could be applied to minimize the measurement effort to extract the desired signal and to extract the signal from a potentially noise set of measurement data in the optimal manner. Methods of this type have the potential to improve sensing and metrology experiments considerably, even in some cases by order of magnitude.

So-called non-Gaussian states (referring to the non-Gaussian nature of the Wigner representation of the density operator) can do better when losses are smaller, and in situations where very low numbers of photons are required (perhaps because of sensor or sample damage or response). However, going beyond the SIL in this regime has not yet been achieved. Beyond this, the obvious technological point is whether it is possible to achieve improvements in precision for lower cost (in $/£/€ terms) in a real instrument using quantum correlations or noise reduction.

Indeed, theoretical study of quantum sensing remains a critical element in order to examine the fundamental limits of metrology. Theory will help to inform the experimentalist how much more effort needs to be expended to attain the known bounds. Further a proof that establishes a tight bound on a metrology scheme also very clearly specifies as set of assumptions and resources. This in turn guides thinking towards trying to obviate these assumptions, which may then lead to even more powerful sensing and metrology schemes.

D. Short-term goals (0-5 years)

- Demonstration of sub-SIL single parameter estimation using near-optimal non-Gaussian states
- New algorithms for adaptive estimation of single parameters using minimal data.
- New algorithms for multi-parameter estimation, with assessment of robustness to system imperfections.
- Demonstration of large-scale quantum sensors and quantum sensor networks in laboratories.
- Development of proof of principle quantum-enhanced microscopes without post-selection.
- Development of compact, field deployable optomechanical devices for low noise amplification, conversion, or modulation of electromagnetic fields
- Development of optomechanical sensors for sensing of acceleration, mass, charge.

E. Medium-term goals (5-10 years)

- Demonstration of quantum enhancements in sensors where there are intrinsic constraints on in-sensor power (i.e. where there is a maximum input optical power due to e.g. sample damage)
- Demonstration of a 'cheap" sensor technology with quantum-enhanced performance
- Development of sensor networks with enhanced precision.
- Demonstration of multiple parameter estimation beyond the SQL, in the first instance using post-selection (leading to feasible quantum enhanced imaging scenarios).
- Compact, field usable, quantum sensors.
- Compact, integrated field deployable optomechanical sensors
- Demonstration of portable, chipscale atomic clocks with enhanced stability using optical transitions and chipscale frequency combs.
- Compact optomechanical quantum correlation based noise thermometers for temperature measurements

F. Long-term goals (>10 years)

- Development of practical sub SQL/SIL imaging systems for e.g. biological microscopy, quantum materials (e.g. phase transitions).
- Quantum sensor networks with additional functionality, such as secure readout, or long-distance sensor arrays using quantum memories.

- Development of quantum sensors arrays for underground survey/GW detection enhancement
- Developments of field usable quantum sensors for navigation.
- All integrated chip scale atomic clocks and frequency comb technology for timing, navigation and communication.

G. Key references

[1] B. P. Abbott et al. (LIGO Scientific Collaboration and Virgo Collaboration), “Observation of Gravitational Waves from a Binary Black Hole Merger”, Phys. Rev. Lett. 116, 061102 (2016)
[2] The LIGO Scientific Collaboration, “A gravitational wave observatory operating beyond the quantum shot-noise limit”, Nature Phys. 7, 962 (2011)
[3] J. Aasi, *et al.*, “Enhanced sensitivity of the LIGO gravitational wave detector by using squeezed states of light”, Nature Photon. 7, 613 (2013)
[4] T. Ono *et al.*, “An entanglement-enhanced microscope”, Nature Comm. 4, 2426 (2013)
[5] N.Treps *et al.*, “Surpassing the Standard Quantum Limit for Optical Imaging Using Nonclassical Multimode Light”, Phys. Rev. Lett. 88, 203601 (2002)
[6] M. A. Taylor *et al.*, “Biological measurement beyond the quantum limit”, Nature Photon. 7, 229 (2013)
[7] H. Müntinga *et al.*, “Interferometry with Bose-Einstein Condensates in Microgravity”, Phys. Rev. Lett. 110, 093602 (2013)
[8] O. Hosten, N.J. Engelsen, R. Krishnakumar, and M.A. Kasevich, “Measurement noise 100 times lower than the quantum-projection limit using entangled atoms”, Nature 529, 505 (2016)
[9] M. Jachura, R. Chrapkiewiz, R. Demkowicz-Dobrzanzski, W. Wasilewski, and K. Banaszek, “Restoring quantum enhancement in realistic two-photon interferometry using spatial information”, arXiv:1504.05435 (2015)
[10] A. A. Berni, T. Gehring, B. M. Nielsen, V. Händchen, M. G. A. Paris and U. L. Andersen, “Ab initio quantum-enhanced optical phase estimation using real-time feedback control”, Nature Photonics 9, 577 (2015)
[11] L. Childress and R. Hanson, “Diamond NV centers for quantum computing and quantum networks”, MRS Bulletin 38, 134 (2013)
[12] J. Nunn, “Quantum engineering: Diamond envy”, Nature Phys. 9, 136 (2013)
[13] G. Waldherr, J. Beck, *et al.*, “High-dynamic-range magnetometry with a single nuclear spin in diamond”, Nature Nanotechnology 7, 105 (2012)
[14] L. P. McGuinness, *et al.*, “Quantum measurement and orientation tracking of fluorescent nanodiamonds inside living cells”, Nature Nanotechnology 6, 358 (2011).
[15] P. C. Humphreys, M. Barbieri, A. Datta, and I. A. Walmsley, “Quantum Enhanced Multiple Phase Estimation” Phys. Rev. Lett. **111,** 070403 (2013).
[16] C. Gagatsos, D. Branford, and A. Datta, “Gaussian systems for quantum enhanced multiple phase estimation” arXiv:1605.04819 (2016).

[17] aS.F. Huelga, C. Macchiavello, T. Pellizzari, A.K. Ekert, M.B. Plenio and J.I. Cirac. "On the improvement of frequency standards using quantum entanglement." Phys. Rev. Lett. **79**, 3865 – 3868 (1997)
[18] Th. Unden, P. Balasubramanian, D. Louzon, Y. Vinkler, M.B. Plenio M. Markham, D. Twitchen, I. Lovchinsky, A.O. Lovchinsky, M.D. Lukin, A. Retzker, B. Naydenov, L. McGuinness and F. Jelezko, "Quantum metrology enhanced by repetitive quantum error correction.", Phys. Rev. Lett. **116**, 230502 (2016))
[19] J.M. Cai, F. Jelezko and M.B. Plenio. "Hybrid sensor based on colour centres in diamond and piezoactive layers.", Nature Comm. **5**, 4065 (2014)

2.5.2 Spin quantum sensors

A. Physical approach and perspective

Spin qubit based sensing

Sensing using spin qubits is a relatively new and upcoming field in quantum sensing. Sensing magnetic field comes most naturally for spin sensors [1,2] and is of crucial importance for several fields for science including chemistry, biology, medicine and material science. Meanwhile, sensing of a whole variety of different quantities has been demonstrated with diamond defect. Among those are temperature [3, 4], electric field [5] and pressure as well as force [6] or optical near-fields. Sensors rely on the long living quantum coherence of spins to build robust, calibration free sensors. These devices often called quantum sensors operate by measuring quantum phase accumulated by a qubit and coherent control of qubits including dynamical decoupling technique is crucial for achieving best performance.

At present quantum sensors are targeting the following benchmark

- Achieving high sensitivity
- Reaching high spatial resolution
- Achieving high spectral and temporal resolution (when measuring AC fields)
- Ability to perform non-invasive measurements
- Ability to operate under ambient conditions
- Integration into compact low energy consumption devices

Using qubits is crucial for all the benchmarks mentioned above. Different material systems have been to demonstrate sensing. Among those are defects in diamond and silicon carbide [7]. Note that high sensitivity and spectral resolution for qubit based sensing requires long spin coherence times, which often is not compatible with room temperature operation for variety solid state qubits. Single spin qubits in diamond are outstanding in this respect, since the diamond lattice allows for millisecond coherence time of electronic spins even under ambient conditions [8].

B. State of the art

Diamond sensors

Multiparameter sensing with diamond defects. Diamond defects are known to detect magnetic fields via the Zeeman effect (see below). They have been used to measure electric fields down to measuring the field of a single electron charge via residual spin orbit coupling. By their fine structure splitting they get sensitive to lattice expansion and spin phonon interaction. NV centres allow to measure pressure and force. When integrated into mechanical devices they are sensitive to vibrations. The have been used to measure optical near fields.

AC magnetic field sensing with single NV centres. Early demonstrations of diamond magnetic field sensing were performed using optically detected magnetic resonance (ODMR) on single colour centres. The sensitivity of such devices is solely limited by photophysical and spin parameters of NV centre (fluorescence quantum yield, contrast of optically detected magnetic resonance signal and spin coherence time) and reaches a few nano-tesla for a one second measurement time. Note that this sensitivity was demonstrated for AC field measurements where combination of dynamical decoupling (spin echo) can be combined with sensing protocols.

Spectroscopic measurement of AC fields and applications in nanoscale NMR and EPR. NV centre in diamond can be generated very close (a few manometers) the diamond surface by ion implantation or incorporation of nitrogen into lattice during CVD growth. Such proximity to the diamond interface allows bringing diamond sensors in close proximity to samples containing electron and nuclear spins. At nanometer standoff distances the field created by a single electron or nucleus is within the range of sensitivity of a single NV diamond magnetometer. Shallow NV centres have been shown to be able to detect NMR and EPR signal s from mesoscopic spin ensemble and even single electron and nuclear spins.

Scanning probe magnetometer. Although the spatial resolution of NV magnetometer is high, imaging depths is quite limited by fast decay of dipolar field associated with electron and nuclear spins. That´s why magnetic imaging over scales exceeding a few nanometers requires multiple NVs and parallel detection of signal or scanning probe magnetometer. Both approaches were demonstrated experimentally and applied to nuclear magnetic resonance spectroscopy. The imaging of single electron spins has been demonstrated.

Exploring multiqubit diamond registers for metrology. Future development of diamond magnetometers will critically depend on the ability to explore quantum entanglement for reaching better sensitivities. Similar to optical metrology technique where squeezing and non-classical state of light allow for better performance of sensors, entanglement in small spin clusters in diamond allow for better performance of diamond magnetometers. This can include for example creation of Bell states insensitive to global field fluctuation but sensitive to gradients. Such diamond magnetic field gradient sensor will allow to explore decoherence free subspaces and reach longer coherence time. Another interesting avenue is a combination of quantum error correction protocols and sensing. Fully protected qubit of course cannot be used for sensing, but protection again certain type of noise allows to open a channel for metrology. Complementary to conventional dynamical decoupling techniques, quantum error correction allow protection against noise of any frequency (but low amplitude).

Sensing based on ensembles of NV centers. Sensitivity of diamond magnetometers can be improved also by increasing number of sensing qubits, and preparation of these qubits in appropriate quantum states. For example, hyperpolarization of diamonds for enhanced NMR and MRI reduces the noise inherent a quantum sensor. This approach, that does not demand the preparation of entangled states, has the potential to deliver a useful technological application in the foreseeable future.

Dense NV ensembles have been shown to reach sub-picoTesla sensitivity for a one-second measurement time. Future directions of sensitivity improvement rely on improvement of diamond material (reducing inhomogeneity of spins associated with imperfections in diamond lattice and presence of unwanted defects). Sensitivities of a few ten femto Tesla per one second averaging times are projected.
Other spin sensors. Other spin systems do allow for similar tasks than NV centres in diamond. Prominent examples are spin defects in SiC. Single defects have been detected and measurement of magnetic and electric fields as well as strain has been reported. An up to seven times higher strain induced shift is measured.

C. Challenges

Future direction in diamond magnetometry.

From sensing technologies to devices. Although first proofs of principle demonstration show high potential of diamond sensing devices for magnetic field sensing, key challenges than need to be addressed in order to bring this technique to application is integration in user-friendly prototype. Depending on the application, this comprises optical integration and combination with control electronics. For medical and bioanalytical applications, integration into existing analytical devices like fluorescence microscopes is needed.
Quantum correlations for magnetometry. Quantum control tools open new technique that will improve sensitivities and open new application areas. So far quantum entanglement between spins remained widely unexplored. For example, concentration of NV centres for ensemble NV magnetometry was adjusted to be low enough to avoid dipole dipole coupling between spins. On the other hand such coupling provides an opportunity to generate squeezing in dense spin systems and reach sensitivities approaching Heisenberg limit. Optimal control technique allowing to reduce the effects of inhomogeneity and to generate the desired target coupling Hamiltonian will be crucial for such demonstrations.
Nanodiamonds for life science applications. Applications of NV magnetometers in life sciences and medicine depend on the ability to insert NV sensors into cells. First demonstrations of ODMR measurement on nanocrystals embedded in living cells show that quantum sensing can be performed in biological tissues. Next challenge is to attach sensors (diamond nanocrystals with incorporated NV centres) to particular proteins. Sensing ability can be combined with other functionalities of nanodiamonds (for example their use as drug delivery devices or markers for ultra-sensitive MRI enabled by hyperpolarisation of nuclear spins in diamond lattice). A remaining challenge is the size reduction on nanodiamonds as well as their versatile surface functionalisation.

Vector magnetometry. Recent results have been obtained on the simultaneous estimation of all the dimensions a multidimensional field [9]. This requires generation of entangled states of several spins, but in the early stages can involve only a couple of spins that have been already entangled. The same methodology can be used to perform the estimation of any Hamiltonian in general, which would be very useful in understanding novel quantum phases and exotic materials.

F. Short-term goals (0-5 years)

- Demonstrate single biomolecule NMR in vitro and in vivo
- Label free MRI of single molecules
- Single molecule EPR in vivo
- Measurement of current in nanostructures
- Application to micro- and nanomagnetism
- Integration for compact magnetic field sensors
- Hyperpolarised MRI based on colour centers in diamond.

G. Medium-term goals (5-10 years)

- High resolution NMR on single biomolecules
- Sensing brain signals
- Highly polarised qubits for magnetic resonance imaging
- Entanglement based sensors
- Low temperature magnetometers for solid-state research
- Gyroscopes
- First prototypes commercial by start-up companies

H. Long-term goals (>10 years)

- Elucidation of structure and dynamics of single molecules
- Non-invasive brain imaging
- Commercially available devices for quantum enhanced biosensing

I. Key references

[1] G. Balasubramanian, I.Y. Chan, R. Kolesov, M. Al-Hmoud, J. Tisler, C. Shin, *et al.* "Nanoscale imaging magnetometry with diamond spins under ambient conditions", Nature 455, 648 (2008)

[2] J.R. Maze, P.L. Stanwix, J.S. Hodges, S. Hong, J.M. Taylor, P. Cappellaro, *et al.* "Nanoscale magnetic sensing with an individual electronic spin in diamond", Nature 455, 644 (2008)

[3] G. Kucsko, P. C. Maurer, N.Y. Yao, M. Kubo, H.J. Noh, P.K. Lo, *et al.,* "Nanometre-scale thermometry in a living cell", Nature 500, 54 (2013)

[4] P. Neumann, I. Jakobi, F. Dolde, C. Burk, R. Reuter, G. Waldherr, *et al.,* "High-Precision Nanoscale Temperature Sensing Using Single Defects in Diamond", Nano Letters 13, 2738 (2013)

[5] F. Dolde, H. Fedder, M.W. Doherty, T. Nobauer, F. Rempp, G. Balasubramanian, *et al.* "Electric-field sensing using single diamond spins", Nature Physics 7, 459 (2011)

[6] J. Cai, F. Jelezko, and M.B. Plenio, "Hybrid sensors based on colour centres in diamond and piezoactive layers", Nature Communications 5, 4065 (2014)

[7] D.J. Christle, A.L. Falk, P. Andrich, P.V. Klimov, J.U.l. Hassan, N.T. Son, *et al.*, "Isolated electron spins in silicon carbide with millisecond coherence times". Nature Materials 14, 160 (2015)
[8] G. Balasubramanian, P. Neumann, D. Twitchen, M. Markham, R. Kolesov, N. Mizuochi, *et al.*, "Ultralong spin coherence time in isotopically engineered diamond", Nature Materials 8, 383 (2009)
[9] T. Baumgratz and A. Datta, "Quantum enhanced estimation of a multi-dimensional field", Phys. Rev. Lett. 116, 030801 (2016)

2.5.3. Optomechanical sensors

Recent developments in fabrication technology have enabled a new class of sensors based on micro- and nano-mechanical structures that are coupled to optical or microwave fields. This class of sensors, which are able to measure force, mass, and acceleration use optical readout at or beyond the quantum limit to overcome the limits to sensitivity over a wide bandwidth that arise from thermal and electrical noise. Radiation pressure can provide feedback and control for such devices, which can be prepared in quantum states of mechanical motion that enable increased sensor performance [1]. A prerequisite for quantum state control is initialization of the mechanical system in its motional quantum ground state, which has been achieved for mechanical devices operating in the MHz to GHz regimes, both through direct cryogenic cooling [2] and laser cooling [3]. This allows the generation of quantum states of motion, which are crucial for reaching measurement sensitivities beyond the standard quantum limit. Last year, 3 groups in the US and Europe were able to observe squeezed states of motion at the level of 1 dB below the vacuum fluctuations in nanomechanical oscillators coupled to superconducting circuits [4]. In other experiments, two-mode squeezing in form of entanglement between mechanical motion and a microwave cavity field has been demonstrated [5], as well as non-Gaussian states of motion involving single phonons [2, 6]. Depending on the physical implementation, coherence times (T2) up to several μs have been observed.

Real-time feedback at the thermal decoherence rate has been demonstrated [7], paving the way for measurement-based quantum control. Current efforts combine such feedback control with optically levitated nanoparticles in high vacuum [8], which promise unprecedented performance in force sensing. Only recently, using a nanoparticle trapped in an optical lattice, zepto-Newton force sensitivity has been demonstrated at room temperature [9]. Future research will add the ability to prepare motional quantum states to enable a next generation of room-temperature quantum sensors.

Hybrid optomechanical devices, which comprise electrical, microwave or optical systems together with micro- and nano-mechanical transduction, provide a new platform for the processing of quantum signals. The strong effective optical nonlinearities, provided by the optomechanical coupling, allows to implement sensing-relevant architectures including the on-chip generation of squeezed light

[10] or the production of optomechanical isolators exploiting non-reciprocal behavior. An extinction ratio of over 10 dB at telecommunications wavelengths was reported recently [11]. Other applications include dispersion management via optomechanically induced transparency [12], coherent frequency conversion between disparate optical fields [13] and the conversion of signals from the microwave to the optical domain [14]. This enables low-noise amplification of electromagnetic signals (e.g. the optical detection of radio-waves through nanomechanical transduction [15]) and, ultimately, the optical detection of single microwave quanta.

Measurement sensitivities near or at the standard quantum limit are now being achieved [16]. In two recent experiments, quantum back action, which defines the SQL, has been evaded successfully: in one case through a quantum non-demolition (QND) measurement using a microwave cavity [4], in another case through a hybrid system employing a mechanical oscillator and a cloud of atoms by exploiting a so-called quantum-mechanics-free subspace [17].

Functionalized micromechanical oscillators have been used for several years to detect single spins, and a wide variety of devices that couple spin and motional degrees of freedom exists. Recently, coherent sensing of a mechanical resonator using a NV spin qubit has been demonstrated [18], which can be considered a first step towards a spin-phonon interface. Coupling between spin and mechanical motion has also been demonstrated using optically levitated nanodiamonds [19]. Strain-mediated coupling between a quantum dot and mechanical motion has also been shown in a device that offers good light-extraction efficiency and ultra-strong coupling [20], as well as in a diamond optomechanical oscillator [21].

[1] M. Aspelmeyer, T. J. Kippenberg, F. Marquardt, Cavity Optomechanics, Rev. Mod. Phys. 86, 1391 (2014).
[2] A. D. O'Connell et al., Quantum ground state and single-phonon control of a mechanical resonator, Nature 464, 697–703 (2010).
[3] J. D. Teufel et al., Sideband cooling of micromechanical motion to the quantum ground state, Nature 475, 359–363 (2011); J. Chan et al., Laser cooling of a nanomechanical oscillator into its quantum ground state, Nature 478, 89–92 (2011)
[4] E. E. Wollman et al., Quantum squeezing of motion in a mechanical resonator, Science 349, 952–955 (2015); J.-M. Pirkkalainen et al., Phys. Rev. Lett. 115, 243601 (2015); F. Lecocq et al., Quantum Nondemolition Measurement of a Nonclassical State of a Massive Object, Phys. Rev. X 5, 041037 (2015).
[5] T. A. Palomaki et al., Entangling mechanical motion with microwave fields. Science 342, 710–3 (2013).
[6] K. C. Lee et al., Entangling macroscopic diamonds at room temperature. Science 334, 1253–6 (2011); R. Riedinger et al., Non-classical correlations between single photons and phonons from a mechanical oscillator, Nature 530, 313–316 (2016).
[7] D. J. Wilson et al. Measurement-based control of a mechanical oscillator at its thermal decoherence rate. Nature 524, 325-329 (2015).

[8] V. Jain et al., Direct Measurement of Photon Recoil from a Levitated Nanoparticle, Phys. Rev. Lett. 116, 243601 (2016).
[9] G. Ranjit et al., Zeptonewton force sensing with nanospheres in an optical lattice. Phys. Rev. A **93**, 053801 (2015).
[10] A. H. Safavi-Naeini et al., Squeezed light from a silicon micromechanical resonator, Nature 500, 185–189 (2013).
[11] F. Ruesink, M.-A. Miri, A. Alù, E. Verhagen, Nonreciprocity and magnetic-free isolation based on optomechanical interactions, arxiv: 1607.07180 (2016)
[12] S. Weis et al., Optomechanically induced transparency, Science 330, 1520–3 (2010); T. P. M. Alegre et al., Electromagnetically induced transparency and slow light with optomechanics, Nature 472, 69–73 (2011).
[13] J. T. Hill et al., Coherent optical wavelength conversion via cavity optomechanics, Nature Communications **3**, 1196 (2012).
[14] J. Bochmann et al., Nanomechanical coupling between microwave and optical photons, Nat. Phys. 9, 712–716 (2013); R. W. Andrews et al., Bidirectional and efficient conversion between microwave and optical light, Nat. Phys. 10, 321–326 (2014).
[15] T. Bagci et al., Optical detection of radio waves through a nanomechanical transducer., Nature 507, 81–5 (2014).
[16] T. P. Purdy, R. W. Peterson, C. a Regal, Observation of radiation pressure shot noise on a macroscopic object., Science 339, 801–4 (2013).
[17] C. B. Møller et al., Back action evading quantum measurement of motion in a negative mass reference frame, arxiv: 1608.03613 (2016).
[18] S. Kolkowitz et al., Coherent sensing of a mechanical resonator with a single-spin qubit., Science 335, 1603–6 (2012).
[19] L. P. Neukirch et al., Multi-dimensional single-spin nano-optomechanics with a levitated nanodiamond, Nature Photonics **9**, 653 (2015).
[20] I. Yeo et al., Strain-mediated coupling in a quantum dot-mechanical oscillator hybrid system, Nature Nanotechnology **9**, 106 (2014).
[21] J. Teissier et al., Strain Coupling of a Nitrogen-Vacancy Center Spin to a Diamond Mechanical Oscillator, Phys. Rev. Lett. **113**, 020503 (2014).

Challenges:
Materials and fabrication challenges have a strong bearing on current optomechanical devices. A significant medium-term challenge is to fabricate hybrid nano-optomechanical systems in combination with standard CMOS processing, thereby making them compatible with current manufacturing methods.

Reducing optical losses will allow on-chip architectures to exploit full quantum control, e.g., via coherent feedback, perform full quantum state tomography, etc. In turn, this will allow to produce quantum states that are known to improve sensing and transduction sensitivity. Lower-absorption materials are also crucial in reducing the thermal load on devices. In combination with a wide variety of different methods, including pulsed protocols, using squeezed light, etc., this would help to extend the quantum regime to lower frequencies and larger masses, which enables broader sensing capabilities. Alternative routes to drastically reducing mechanical dissipation include the use of phononic bandgap architectures and substrate-free levitated topologies, which will eventually allow quantum operation at room temperature.

Increasing the coupling between the different quantum components of an optomechanical system is crucial. Strong coupling at the single-photon level, where a single photon shifts the mechanical oscillator by a distance comparable to the extent of its ground-state wavefunction, has not yet been demonstrated.

The coupling between spins and phonons in functionalised optomechanical devices also needs to be improved for quantum-enhanced sensing to be practical. Levitated nanodiamond optomechanical devices, which provide a promising route towards quantum-enabled magnetometry, have yet to solve the problem of stably trapping nanodiamonds under ultra-high vacuum conditions. Quantum state engineering in levitated systems, using either passive or active feedback, has not yet been achieved.

short term goals:

- Observing manifestly quantum behaviour in sub-MHz optomechanical devices.
- Optomechanical transduction of single microwave photons.
- Coherent quantum feedback for quantum control of optomechanics.
- Ground-state cooling and quantum control of levitated functionalised optomechanical devices for quantum-enabled spin sensing.

mid-term:

- Quantum-enhanced positioning, inertial nagivation, and timing devices.
- Large-scale quantum mechanical superpositions with increased sensitivity to external fields and forces
- Strongly coupled hybrid optomechanical devices that can coherently transduce information between spin degrees of freedom and optics.

long-term:

- Coherent optomechanical photonic devices (routers, multiplexers, and frequency conversion) operating at the single-photon level.
- Quantum-enhanced optomechanical vector magnetometers.
- Room-temperature optomechanical quantum sensors

2.5.4 Quantum clocks

The atomic clocks used as primary standards for international timekeeping are caesium fountain microwave atomic clocks, the best of which have accuracies of around 1 part in 10^{16} [1]. However these are laboratory-sized clocks and are confined to a small number of national measurement laboratories worldwide. For many applications size, weight and power consumption may be more critical factors than achieving the best possible stability and accuracy. As a result, a range of commercial microwave atomic clocks has been developed, from which the best option for a particular application can be selected.

A new generation of atomic clocks is now being developed, based on optical rather than microwave reference transitions [2, 3]. This new technology has already brought about a step change in performance, and is likely in future to lead to a redefinition of the second within the International System of Units. Optical clocks based on laser-cooled atoms trapped in an optical lattice have demonstrated fractional frequency instabilities of $2\times10^{-16}\,\tau^{-1/2}$, where τ is the averaging time in seconds, and estimated systematic frequency uncertainties as low as 2 parts in 10^{18} [4]. Estimated systematic frequency uncertainties of optical clocks based on the alternative technology of single laser-cooled trapped ions have reached similar levels [5] although the limited signal to noise achievable with a single ion means that multi-ion architectures will be required to reach competitive stabilities [6]. However further work is required to verify the estimated uncertainties of the clocks, with most information about the reproducibility of optical clocks presently coming from independent absolute frequency measurements made in different laboratories, which are limited by the uncertainty of the local caesium primary standards.

The satellite-based techniques routinely used to compare microwave clocks constructed in different laboratories are insufficient for the new generation of optical clocks. On a continental scale, new approaches to time and frequency transfer using optical fibres offer the best prospects for optical clock comparisons at a level commensurate with their performance [7]. However the extension of these techniques to intercontinental optical clock comparisons presents a severe challenge and hence alternatives such as transportable optical clocks or enhanced satellite-based methods are also being explored [8]. Portable optical atomic clocks, when combined with suitably high performance techniques for comparing the operating frequencies of clocks in well-separated locations, will open up completely new applications such as clock-based geodesy [9].

A European-scale infrastructure for high accuracy clock comparisons would put the region in the forefront of the field. This could be achieved by investment in a pan-European optical fibre network for time and frequency comparison and dissemination, building upon existing (mainly national) networks but addressing the crucial question of long-term sustainability. Such a network would exploit the European advantage of a uniquely high density of high performing optical atomic clocks, to validate the estimated uncertainty budgets of next-generation primary frequency standards, to characterise and evaluate portable clocks developed in collaboration with industry and to form a backbone for future applications of these clocks, for example in geodesy.

The main challenge to proliferation of the new generation of clocks is to develop higher stability and accuracy, combined with reductions in size, weight, power consumption and cost. New portable and robust clocks, both microwave and optical, are required with a range of target performance levels suited to a range of new and increasingly demanding applications. The ultimate aim would be to produce miniature devices that are cheap and simple to use, and that can be integrated into both current and future systems.

References

[1] T. P. Heavner, E. A. Donley, F. Levi, G. Costanzo, T. E. Parker, J. H. Shirley, N. Ashby, S. Barlow and S. R. Jefferts, "First accuracy evaluation of NIST-F2", Metrologia 51, 174 (2014).

[2] N. Poli, C. W. Oates, P. Gill, G. M. Tino, "Optical atomic clocks", La Rivista del Nuovo Cimento 36, 555 (2013).

[3] A. D. Ludlow, M. M. Boyd, J. Ye, E. Peik and P. O. Schmidt, "Optical atomic clocks", Rev. Mod. Phys. 87, 637 (2015).

[4] T. L. Nicholson, S. L. Campbell, R. B. Hutson, G. E. Marti, B. J. Bloom, R. L. McNally, W. Zhang, M. D. Barrett, M. S. Safronova, G. F. Strouse, W. L. Tew and J. Ye, "Systematic evaluation of an atomic clock at 2×10^{-18} total uncertainty", Nature Communications 6, 6896 (2015).

[5] N. Huntemann, C. Sanner, B. Lipphardt, C. Tamm and E. Peik, "Single-ion atomic clock with 3×10^{-18} systematic uncertainty", Phys. Rev. Lett. 116, 063001 (2016).

[6] J. Keller, T. Burgermeister, D. Kalincev, J. Kiethe and T. E. Mehlstäubler, "Evaluation of trap-induced systematic frequency shifts for a multi-ion optical clock at the 10^{-19} level", Journal of Physics Conference Series 723, 012027 (2016).

[7] K. Predehl, G. Grosche, S. M. F. Raupach, S. Droste, O. Terra, J. Alnis, T. Legero, T. W. Hänsch, T. Udem, R. Holzwarth and H. Schnatz, "A 920-kilometer optical fiber link for frequency metrology at the 19th decimal place", Science 336, 441 (2012).

[8] H. S. Margolis, R. M. Godun, P. Gill, L. A. M. Johnson, S. L. Shemar, P. B. Whibberley, D. Calonico, F. Levi, L. Lorini, M. Pizzocaro, P. Delva, S. Bize, J. Achkar, H. Denker, L. Timmen, C. Voigt, S. Falke, D. Piester, C. Lisdat, U. Sterr, S. Fogt, S. Weyers, J. Gersl, T. Lindvall and M. Merimaa, "International timescales with optical clocks", p. 908 in Proceedings of the 2013 Joint Meeting of the International Frequency Control Symposium and European Frequency and Time Forum (2013).

[9] R. Bondarescu, M. Bondarescu, G. Hetényi, L. Boschi, P. Jetzer and J. Balakrishna, "Geophysical applicability of atomic clocks: direct continental geoid mapping", Geophys. J. Int. 191, 78 (2012).

2.5.5 Virtual Facilities needs

Quantum engineering

• Determining classes of quantum states may be most effective for particular sensor applications

• State design and construction using feasible laboratory resources For instance, recent work has shown that accessing additional degrees of freedom beyond that used to encode the state of the sensor can provide additional precision in phase estimation [8].

- improved photodetection capability, including high-efficiency photon-number resolving detectors operating at or near room temperature, in integrated packages (e.g. waveguide-based photonic circuits) for optimum interoperability.
- Designs for multi parameter sensing involving changing control parameters,
- Development of solid-state quantum spin sensors both in the periphery of the sensor, and in the sensor material and spins themselves.
    - For ultra-sensitive NMR, single spins inproximity to surfaces
    - Design of ancillary nuclear spins as quantum memories or for e.g. error correction, including the choice of proper nuclear spins
    - QEC algorithm design
    - Mitigation of background fields
- Integration of spins into complex structures such as nano mechanical devices
- Classical control of the sensor periphery of the sensor.
- Optimising light extraction. E.g. defects in SiC are significantly more advanced than diamond, as elaborate photonic structures in these materials exist.
- Efficient coupling of excitation light sources for optical spin alignment, especially for integrated sensor designs.
- Improved infrastructure for high accuracy clock comparisons is required. A pan-European optical fibre network for time and frequency comparison and dissemination, building upon existing (mainly national) networks but sustainably over the long-term.
- Progressive development in clock stability and accuracy, combined with reductions in size, weight, power consumption and cost.

Quantum control

- Development of adaptive estimation strategies to determine an unknown phase with no prior assumption [9].
- Application of feedback control of systems and signal estimation techniques to quantum devices
- Optimization of system designs with constraints of feasible laboratory implementations (perhaps, ideally, as convex constraints) for new sensor designs.
- Improved sensor dynamic range by dedicated quantum control, generating optimzed filter functions rendering sensitivity to specific frequencies of the parameter to be measured only.
- Control strategies for nuclear quantum memories for e.g. error correction and high resolution requires high fidelity optimal control pulses.
- For ensemble-based sensors, optimised quantum control is needed to generate desired target states. For example, in interacting spin systems engineering spin squeezed states would be a prime target.

2.6. Quantum Control

It is control that turns scientific knowledge into technology. The general goal of quantum control is to actively manipulate dynamical processes of quantum systems, typically by means of external electromagnetic fields or forces. The objective of quantum optimal control is to devise and implement shapes of pulses of external fields or sequences of such pulses, that reach a given task in a quantum system in the best possible way. Quantum control builds on a variety of theoretical and technological advances from the fields of mathematical control theory and numerical mathematics all the way to devising better electronic devices such as arbitrary-waveform generators with sub nanosecond time resolution or stronger magnetic fields.

The challenge to manipulate nature at the quantum level offers a huge potential for current and future applications. Traditionally the field is rooted in first-generation ensemble quantum technologies such as nuclear magnetic resonance and in chemical physics. Useful applications of quantum optimal control in these first generation technologies range from magnetic resonance imaging and spectroscopy and the precise control of chemical reactions. This foundation is now transferred to the second-generation quantum technologies based on superposition, entanglement and many body quantum systems that are described in this roadmap.

Quantum optimal control is part of the effort to engineer quantum technologies from the bottom up, and many striking examples of surprising and non-intuitive - but extremely efficient and robust - quantum control techniques have been discovered in recent years. Examples of important current applications are the precise measurement of magnetic fields with nanometer scale resolution using NV centres in diamond, state engineering of Bose-Einstein condensates and high-fidelity quantum gates in superconducting quantum processors.

Quantum control is a strategic cross-sectional field of research, enabling and leveraging current and future quantum technology applications. While the precise way to manipulate the behaviour of these systems may differ — from ultrafast laser control to radio waves —, the control, identification and system design problems encountered share commonalities, while at the same time being quite distinct from classical control problems. Quantum control requires bringing together expertise from mathematical and numerical optimal control theory as well as experience of practitioners from different application areas of quantum control. The further development of this field of research offers many beneficial effects for today's and tomorrow's society, related to health through faster, better, safer diagnostics and treatment, secure communication in a digital world, highly accurate navigation systems, more efficient and clean harvesting of solar power, the search for resources, efficient energy storage and transportation, quantum machines and precision sensing and monitoring of the environment.

The European quantum control community has come together in the FP 7 coordination action QUAINT that persists to be connected through the website www.quantumcontrol.eu. The community has written its own roadmap which is very detailed and covers both first- and second generation quantum technologies. In the following, we are going to outline status and challenges in key areas of quantum control as it serves as an enabler to other areas of quantum technologies. It also contains short pieces on status and challenges of quantum control as a developing tool to optimally serve that purpose.

2.6.1 Tools and Mathematics

A. Approach and definitions

In general, quantum control theory is addressing two fundamental questions, that of controllability, i.e., what control targets are accessible and that of control design, i.e. how can a target be reached. Approaches for control design can be open-loop or closed-loop. In the latter case, the specific nature of quantum measurements needs to be taken into account. Open loop techniques include approaches based on the Pontryagin maximum principle, i.e., quantum optimal control, with solutions obtained analytically or numerically. Optimal control theory does not make any restrictive assumptions on the quantum system and also experimental constraints and robustness requirements can be fully taken into account (the latter is called simultaneous controllability) and is hence broadly applicable.

Research groups in this area are in applied mathematics departments and sometimes in physics, chemistry, and engineering.

B. State-of-the-art

The theory of controllability is well and rigorously understood for closed systems with finite-dimensional state space, based on the rank of the generated Lie algebra. For infinite-dimensional systems, obstructions to controllability have been derived and in special cases, controllability proofs were successful.
Some results in simultaneous / ensemble controllability were obtained.
For open quantum systems in the Markovian limit, a semigroup picture has been developed.
Analytical solutions for simple, low-dimensional systems have been found.
Numerical approaches: Gradient ascent, Quasi-Newton, Newton, Krotov, robust and tailored software packages (QuTiP, Simpson, Dynamo, SPINACH) have reached good maturity, they are complemented by gradient-free approaches (CRAB, AdHOC).
Initial understanding of the control optimisation landscape has been obtained.
Invariant-based engineering and superadiabatic drives have been constructed
Measurement-based and coherent feedback has been formulated.

C. Challenges

The main challenge of controllability research is to extend its notions from the simple structure of closed systems to open systems, understanding rigorously what states and what transformations can be reached. In algorithms design the main challenge is to itegrate these techniques with a broader base of physical platforms.

In feedback control, it remains open to see whether or not fully quantum controllers perform better than classical ones.

D. Short-term goals (0-5 years)

- Full understanding of controllability for systems with a mixed spectrum.
- Better understanding of controllability in Markovian open systems.
- Efficient numerical techniques for optimal control of open systems.
- Improved link to experiments, understanding of control complexity.

E. Medium-term goals (5-10 years)

- Optimise tradeoff between invasiveness and control in feedback.
- First understanding of controllability in non-Markovian open systems.

F. Long-term goals (>10 years)

- Adaptation of controllability and control design theory to real-life conditions.
- Develop rigorous framework to integrate theory and experiment.

G. Key references

[1] Thomas Chambrion, Paolo Mason, Mario Sigalotti, and Ugo Boscain, “Controllability of the discrete spectrum schrodinger equation driven by an external field”, Annales de l'Institut Henri Poincare Non, Linear Analysis 26, 329 (2009)
[2] B. Bonnard, M. Chyba, and D. Sugny, “Time-Minimal Control of Dissipative Two-Level Quantum Systems: The Generic Case”, IEEE Trans. Automat. Control 54, 2598 (2009)
[3] G. Dirr, U. Helmke, I. Kurniawan, and T. Schulte-Herbruggen, “Lie-semigroup structures for reachability and control of open quantum systems: Kossakowski-Lindblad generators form Lie wedge to Markovian channels.”, Reports on Mathematical Physics 64, 93 (2009)
[4] C. Altafini and F. Ticozzi. “Modeling and control of quantum systems: An introduction”, IEEE Trans. Automat. Control 57,1898 (2012)
[5] Karine Beauchard, Jean-Michel Coron, and Pierre Rouchon, “Controllability issues for continuous spectrum systems and ensemble controllability of bloch equations”, Communications in Mathematical Physics 296, 525 (2010)
[6] G. Dridi, M. Lapert, J. Salomon, S. J. Glaser, D. Sugny, “Discrete-valued-pulse optimal control algorithms: application to spin systems”, Phys. Rev. A 92, 043417 (2015)
[7] N. Khaneja, R. Brockett, and S. J. Glaser, “Time optimal control in spin systems”, Phys. Rev. A 63, 032308 (2001).
[8] N. Khaneja, T. Reiss, C. Kehlet, Thomas Schulte-Herbrüggen, and Steffen J. Glaser, “Optimal control of coupled spin dynamics: design of NMR pulse sequences by gradient ascent algorithms”, J. Magn. Reson., 172, 296 (2005).
[9] P. Doria, T. Calarco, and S. Montangero, “Optimal control technique for many-body quantum dynamics”, Phys. Rev. Lett., 106, 190501 (2011).
[10] D. Reich, M. Ndong, and C.P. Koch, “Monotonically convergent optimization in quantum control using Krotov’s method”, J. Chem. Phys., 136, 104103 (2012).

[11]S. Machnes, U. Sander, S. J. Glaser, P. de Fouquières, A. Gruslys, S. Schirmer, and T. Schulte-Herbrüggen, "Comparing, optimizing, and benchmarking quantum-control algorithms in a unifying programming framework", Phys. Rev. A, 84, 022305, (2011).

2.6.2 Selected applications in NMR and AMO physics

A. Approach and definitions

The wide range of applications of nuclear magnetic resonance (NMR) and some instances of atomic, molecular and optical (AMO) physics are considered "Quantum 1.0" (rather than "Quantum 2.0") technologies because typically they are based on ensembles of quantum systems (rather than individual quantum systems). However, initially motivated by NMR and AMO applications, powerful optimal control techniques were developed, which are also extremely useful (if not indispensable) for QIPC applications. Most notably, the task of designing the time-optimal implementation of a desired unitary operation, such as quantum gates or entire quantum algorithms, is identical for the case of individual quantum systems and for the case of an ensemble of quantum systems. Furthermore, experimental uncertainties in experiments involving individual quantum systems can be included in the design of robust quantum control schemes by simultaneously optimising the performance for a (virtual) ensemble of quantum systems for a range of system parameters. Again, the techniques of ensemble control are identical for virtual and real ensembles of quantum systems.

In fact, many QIPC techniques have originated in magnetic resonance and laser spectroscopy. The widely used quantum optimal control algorithm (GRAPE) was developed in the context of nuclear magnetic resonance, (albeit with a clear - and explicitly stated - perspective of potential applications in QIPC) and for example its use in electron spin resonance techniques have resulted in improved quantum sensing using diamond defects. Closed-loop learning control methods from laser chemistry inspired superconducting qubits control, early quantum factorisation demonstrations were carried out using NMR systems, etc. This section describes optimal control concepts that are crucial for both "Quantum 1.0" and "Quantum 2.0".

Spins were among the first quantum systems to be externally controlled in the time domain. The relevance of NMR to chemical, biological, and particularly medical applications has created a large community as well as a large industry producing spectrometers and scanners for NMR spectroscopy and medical imaging and has strongly advanced quantum control. Mathematically, the problem of controlling spins is isomorphic to that of controlling qubits -- spins do therefore provide a convenient testing ground and a major source of inspiration for quantum control techniques. Electromagnetic pulse shaping hardware development has been pioneered in NMR (radio frequencies) and later extended to ESR (microwaves), where a number of quantum information and communication technologies are located. The most direct transfer of spin resonance techniques to QIPC is in the field of nitrogen vacancy centres in diamond and other impurity spin systems. Dynamic nuclear polarisation methods, also pioneered in spin resonance, presently find application in pre-polarisation of solid-state qubits.

The community in this area is vast and many highly accomplished researchers make great internal progress.

B. State-of-the-art

- Study of coherence in real molecules

Improvement of cooling rates of molecules in theory and practice, comprising an important case of preparation of ground states also relevant for quantum simulation.

- Robust/broadband control of nuclear spins, i.e., controlling spins with unknown/uncertain parameters as they occur in sensing or quantum computing with manufactured systems.
- Highly selective control of individual spins.
- Efficient spin-spin decoupling sequences.
- Dynamical nuclear polarisation DNP in simple model systems which paves the way to reducing decoherence in spin baths such as GaAs.

C. Challenges

In laser control of chemical reactions, the key challenge is to engineer reactions that do not occur otherwise. In spin resonance, the challenge is to deal with the complexities of ever increasing size and resolution demands driven by life-science applications.

D. Short-term goals (0-5 years)

- Easy to use optimal control algorithms and software packages

Laser control of energy transfer and light harvesting in real molecules..

E. Mid-term goals (5-10 years)

- Full control of a chemical reaction.
- Trapping and more efficient cooling of molecules.

F. Long-term goals (> 10 years)

- A general platform for the manipulation and detection of individual nuclear spins.

G. Key references

[1] F. Dolde, V. Bergholm, Y. Wang, I. Jakobi, B. Naydenov, S. Pezzagna, J. Meijer, F. Jelezko, P. Neumann, T. Schulte-Herbrüggen, J. Biamonte, J. Wrachtrup, “High-fidelity spin entanglement using optimal control”, Nature Comm. 5, 3371 (2014)

[2] S. J. Glaser, U. Boscain, T. Calarco, C. P. Koch, W. Köckenberger, R. Kosloff, I. Kuprov, B. Luy, S. Schirmer, T. Schulte-Herbrüggen, D. Sugny, and F. K. Wilhelm, “Training Schrödinger’s cat: quantum optimal control”, Strategic report on current status, visions and goals for research in Europe, Eur. Phys. J. D 69, 279/1-24 (2015).

[3] P. E. Spindler, Y. Zhang, B. Endeward, N. Gershenzon, T. E. Skinner , S. J. Glaser, T. F. Prisner, “Optimal control pulses for increased excitation bandwidth in EPR”, J. Magn. Reson. 218, 49 (2012).
[4] V. Jacques, P. Neumann, J. Beck, M. Markham, D. Twitchen, J. Meijer, F. Kaiser, G. Balasubramanian, F. Jelezko, and J. Wrachtrup, “Dynamic polarization of single nuclear spins by optical pumping of nitrogen-vacancy color centers in diamond at room temperature”, Phys. Rev. Lett. 102, 057403 (2009).

2.6.3. Applications of optimal control for quantum technologies

A. Approach and definitions

Quantum technologies exploit quantum coherence and entanglement as essential elements of quantum physics. Applications include high-precision measurements and sensing, which would reach unprecedented sensitivity, the simulation of physical and biological systems, which would be impossible to study otherwise, and quantum information processing, which would allow to solve computationally hard problems. Successful implementation of quantum technologies faces the challenge to preserve the relevant nonclassical features at the level of device operation. More specifically, each task of the device operation needs to be carried out with sufficient accuracy, despite imperfections and potentially detrimental effects of the surroundings. Quantum optimal control not only provides toolboxes that allow for identifying the performance limits for a given device implementation, it also provides the protocols for realising device operation within those limits.
In order to obtain these results, the quantum optimal control methodology had to be adapted to the requirements of Quantum Technologies. Optimisation algorithms had to be derived for specific quantum gates, dissipative evolution as seen in the reduced system dynamics, or exploiting invariants in system-bath models, optimisation up to local equivalence classes, which can also be used for arbitrary perfect entanglers or optimising for many-body entanglement.

Moreover, control techniques were adapted to non-linear dynamics as found in a BEC and to general dynamics, functionals and couplings to be controlled. In addition to efficient numerical optimal control tools such as the GRAPE and Krotov algorithms that are useful in many QIPC applications, the chopped random basis (CRAB) method has been demonstrated to be very useful in many-body systems. This approach has made it possible to interface the time-dependent density matrix renormalisation group (t-DMRG) with the optimisation of a relatively small number of control parameters. Other techniques specifically cover robustness against experimental fluctuations or noise or filters in experimental implementation of controls.

B. State of the art

Prominent tasks include the preparation of useful quantum states as well as implementation of quantum operations.

In quantum communication

- Theoretical proposals for the transport of atoms and ions, transport in a spin chain, and photon storage.

In quantum computing

- Error resistant single-qubit gates with trapped ions; single qubit gates without the need for invoking the rotating wave approximation in nitrogen vacancy centres in diamond.
- In superconducting qubit circuits, leakage to non-computational states and other impact of frequency crowding can be avoided thanks to optimal control results. Closed-loop optimal control enables fine-tuning of gates allowing them to reach consistent record fidelities.
- Design and implementation of unitary maps have recently been demonstrated in a 16-dimensional Hilbert space, spanned by the electron and nuclear spins of individual Cesium atoms.
- The use of control methods in a broader sense has allowed to extend the coherence of a qubit, realised by the electron spin in a NV centre, using dynamical decoupling.
- Theoretical proposals for preparation of cluster-states and quantum registers.
- Theoretical proposals for high-fidelity quantum gates such as two-qubit gates with neutral atoms in dipole traps, on atom chips or with Rydberg atoms, two-qubit gates between ions and between an ion and an atom, error-correcting qubit gates of electron and nuclear spins within single NV centres, entangling gates between distant NV centres, robust two-qubit gates for superconducting systems.
- Retention of universality in spite of limited local control by using environmental degrees of freedom.

In quantum simulation

- Improved loading of an ultracold atomic gas into an optical lattice.
- Serendipitous solutions for local control.
- Theoretical proposal: nonclassical states in a spin chain, many-body entangled states.
- Evaluation of the Jones polynomial, a central invariant in knot theory, in an algorithm equivalent to deterministic quantum computing with a single pure qubit.
- Fidelity limits on two-qubit gates due to decoherence were studied for Markovian as well as non-Markovian time evolutions (the latter crucial in collision models).

In quantum sensing

- Preparation of nonclassical motional states of a Bose-Einstein condensate with optimised control sequences for wavepacket interferometry.
- Spectroscopy protocol for imaging nanoscale magnetic fields in diamond.
- Theoretical proposals: preparation of squeezed states, nonclassical states in a cavity for improved field resolution.
- Basic optimisation of superconducting qubit readout.
- Stabilisation of a quantum state with predefined photon number via real-time closed-loop feedback, including the noise back-action of controls onto the system.

C. Challenges

With the drive of application in quantum technologies, the main goal is to reach convergence between theory and application over a wide range of platforms.

D. Short-term goals (0-5 years)

Communication

- Assist enabling efficient interconversion between flying qubits and quantum memories via coherent atom-photon coupling, with and without cavities.
- Assist in development of hybrid quantum-classical error correction schemes.

Computing

- Robust implementation of gates in a multi-qubit architecture, i.e. stability against fluctuations in the external control fields.
- Faster two-qubit gates in ion traps.
- Optimised readout of qubits as well as fast reset in the regime of long lifetime.

Simulation

- Optimal as well as robust generation of multi-particle entangled states for a variety of quantum technology platforms.
- Exploit the dynamics of quantum many-body systems beyond equilibrium and understand the microscopic origin of thermodynamic laws.
- Keep control and operation fidelity high as the number of qubits is scaled up.

Quantum information theory

- Reduce impact of decoherence by finding schemes that explore decoherence-free subspaces, find pulses decoupled from noise (bang-bang control and its smooth generalisations).

Sensing

- Enhance the sensitivity of the defect spins in diamond employed as quantum probes via improved protection from environmental noise e.g. through dynamical decoupling techniques, thus guiding their dynamic range and tayloring filter functions; include higher harmonics of the signal to this, create spin-squeezed spin ensemble states.
- Demonstrate the practical usefulness of engineered quantum states, for example in quantum metrology.

Engineering

- Control of open quantum systems, decoherence control.
- Convergence of numerical optimal control and experimentation in many platforms, including handling of calibration uncertainties and other experimental constraints.

D. Mid-term goals (5-10 years)

The field of quantum technologies has matured to the point that quantum enhancement is explored beyond quantum computation only. Devices such as quantum simulators or quantum sensors are currently under active development. Control methods will be crucial to operate these devices reliably and accurately. This involves the device preparation, or reset, the execution of the desired time evolution, and the readout of the result. These tasks set the agenda for the next few years.

Communication

- Develop schemes to stabilise entanglement-based networks via feedback.

Computing

- Compatibility with and automatisation of error correction.
- For trapped ions, combine quantum gates with ion transport in segmented traps using optimal control techniques.
- Quantum compilation and a scalable assembler of elementary gates (up to 10 qubits) into many qubits.
- Optimised spin manipulation quantum dots for linear optics.
- Further develop automatic tune-up of quantum processors, make them resistant to manufacturing uncertainty.
- Extend dynamical decoupling for quantum dot spins.
- Pulses robust against inhomogeneous broadening in semiconductor spin qubits.
- Adapt to randomness of fabrication in impurity spins.

Simulation

- Preparation of entangled ground states and other many-body quantum states of increasing complexity, with and without optimal control.
- Fast and accurate quantum gates for quantum simulation.
- Optimal verification and validation of quantum simulators that are not operated as fault-tolerant quantum computers.

Quantum information theory

- Adapt cooling schemes originally developed for molecules to help cooling levitating superconducting spheres to their ground state.

Sensing

- Further development of feedback and adaptive control methods for phase measurements without prior assumption, extension to multi-parameter problems.

Engineering

- Modular approach from simple to complicated pulses in theory, improved pulse shaping in experiment.
- Enhance the lifetime of quantum memories using dissipative state engineering
- Implement reliable strategies for the control of mesoscopic systems.

E. Long-term goals (>10 years)

Several current quantum technology platforms show a strong scaling potential. Thus in the long term, control schemes need to be made scalable. This represents a severe challenge, but meeting this challenge will make quantum control a basic building block of every quantum technology and ensure, at the same time, their proper functioning in a world that is only partially quantum. Take the examples of superconducting qubits, NV centres or spins in Si, where imperfections in fabrication are inevitable and need to be mitigated by controlled. Further along, qubit controls should (to a certain extent) be robust to the influences of the rest of the architecture they are placed in. Independent of a specific platform, error correction at large, for instance by toric codes, is one of the strategic long-term goals that is expected to benefit from control techniques given recent advances by randomised benchmarking. Need to make consistent with the rest of the roadmap (from authors). To this end, system-identification protocols matched with optimal control modules will be of importance.

In short, quantum control will be the means to get the most performance out of an imperfect system and combine challenging physics at the few-qubit level with engineering at the multi-qubit level. This should aim for example at enabling quantum simulations that are impossible on classical computers.
In other words, the long-term goal of quantum optimal control for quantum technologies is to develop a software layer enhancing the performance of quantum hardware for tasks in computing, simulation, communication, metrology and sensing beyond what is achievable by classical means, enabling the achievement of quantum supremacy.

F. Key references

[1] T. Häberle, D. Schmid-Lorch, K. Karrai, F. Reinhard, and J. Wrachtrup, “High-Dynamic-Range Imaging of Nanoscale Magnetic Fields Using Optimal Control of a Single Qubit”, Phys. Rev. Lett. 111, 170801 (2013)
[2] C. Sayrin, I. Dotsenko, X. Zhou, B. Peaudecerf, T. Rybarczyk, S. Gleyzes, P. Rouchon, M. Mirrahimi, H. Amini, M. Brune, J.-M. Raimond, and S. Haroche, “Real-time quantum feedback prepares and stabilizes photon number states”, Nature 477, 73 (2011).
[3] S. van Frank, A. Negretti, T. Berrada, R. and Bücker, S. Montangero, J.-F. Schaff, T. Schumm, T. Calarco, and J. Schmiedmayer, “Interferometry with non-classical motional states of a Bose--Einstein condensate”, Nat. Comm. 5, 4009 (2014).
[4] D.J. Egger and F.K. Wilhelm, “Adaptive hybrid optimal quantum control for imprecisely characterized systems”, Phys. Rev. Lett. 112, 240503 (2014).
[5] M. Braun, S. J. Glaser, “Concurrently Optimized Cooperative Pulses in Robust Quantum Control: Application to Broadband Ramsey-Type Pulse Sequence Elements”, New J. Phys. 16, 115002 (2014).
[6] S. Rosi, A. Bernard, N. Fabbri, L. Fallani, C. Fort, M. Inguscio, T. Calarco, and S. Montangero, “Fast closed-loop optimal control of ultracold atoms in an optical lattice”, Phys. Rev. A 88,021601 (2013).

[7] D.M. Reich, N. Katz, and C.P. Koch, ‘Exploiting non-markovianity for quantum control’, Sci. Rep., 5:12430 (2015).