New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG IOP Institute of Physics

ROADMAP • OPEN ACCESS

The quantum technologies roadmap: a European community view

To cite this article: Antonio Acín *et al* 2018 *New J. Phys.* **20** 080201

New Journal of Physics

The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

CrossMark

OPEN ACCESS

RECEIVED
2 October 2017

REVISED
17 May 2018

ACCEPTED FOR PUBLICATION
6 July 2018

PUBLISHED
16 August 2018

ROADMAP

The quantum technologies roadmap: a European community view

Antonio Acín[1,2], Immanuel Bloch[3,4], Harry Buhrman[5], Tommaso Calarco[6], Christopher Eichler[7], Jens Eisert[8], Daniel Esteve[9], Nicolas Gisin[10], Steffen J Glaser[11], Fedor Jelezko[6], Stefan Kuhr[12], Maciej Lewenstein[1,2], Max F Riedel[6], Piet O Schmidt[13,14], Rob Thew[10], Andreas Wallraff[7], Ian Walmsley[15] and Frank K Wilhelm[16]

[1] ICFO-Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, E-08860 Castelldefels (Barcelona), Spain
[2] ICREA,Passeig de Ll. Campanys, 23, E-08010 Barcelona, Spain
[3] Fakultät für Physik, Ludwig-Maximilians-Universität München, Schellingstrasse 4, D-80799 Munich, Germany
[4] Max-Planck-Institut für Quantenoptik, Hans-Kopfermann-Str. 1, D-85748 Garching, Germany
[5] QuSoft, CWI, and University of Amsterdam, Sciencepark 123 1098 XG, Amsterdam, The Netherlands
[6] University Ulm and Center for Integrated Quantum Science and Technology (IQST), Albert-Einstein-Allee 11, D-89081 Ulm, Germany
[7] ETH Zurich, Department of Physics, CH-8093 Zürich, Switzerland
[8] Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, D-14195 Berlin, Germany
[9] Service de Physique de l'Etat Condensé, CEA-Saclay, F-91191 GIF-SUR-YVETTE, France
[10] Group of Applied Physics, University of Geneva, CH-1211 Geneva 4, Switzerland
[11] Department of Chemistry, Technical University of Munich, Lichtenbergstrasse 4, D-85747 Garching, Germany
[12] University of Strathclyde, Department of Physics, SUPA, Glasgow G4 0NG, United Kingdom
[13] QUEST Institute for Experimental Quantum Metrology, Physikalisch-Technische Bundesanstalt, D-38116 Braunschweig, Germany
[14] Institut für Quantenoptik, Leibniz Universität Hannover, D-30167 Hannover, Germany
[15] Clarendon Laboratory, Department of Physics, University of Oxford, Oxford OX1 3PU, United Kingdom
[16] Theoretical Physics, Saarland University, D-66123 Saarbrücken, Germany

E-mail: tommaso.calarco@uni-ulm.de

Keywords: quantum theory, quantum coomputing, quantum simulation, quantum sensing, quantum communication, quantum technologies, quantum control

Abstract

Within the last two decades, quantum technologies (QT) have made tremendous progress, moving from Nobel Prize award-winning experiments on quantum physics (1997: Chu, Cohen-Tanoudji, Phillips; 2001: Cornell, Ketterle, Wieman; 2005: Hall, Hänsch-, Glauber; 2012: Haroche, Wineland) into a cross-disciplinary field of applied research. Technologies are being developed now that explicitly address individual quantum states and make use of the 'strange' quantum properties, such as superposition and entanglement. The field comprises four domains: quantum communication, where individual or entangled photons are used to transmit data in a provably secure way; quantum simulation, where well-controlled quantum systems are used to reproduce the behaviour of other, less accessible quantum systems; quantum computation, which employs quantum effects to dramatically speed up certain calculations, such as number factoring; and quantum sensing and metrology, where the high sensitivity of coherent quantum systems to external perturbations is exploited to enhance the performance of measurements of physical quantities. In Europe, the QT community has profited from several EC funded coordination projects, which, among other things, have coordinated the creation of a 150-page QT Roadmap (http://qurope.eu/h2020/qtflagship/roadmap2016). This article presents an updated summary of this roadmap.

Contents

1. Introduction

Max F Riedel, Tommaso Calarco
University Ulm and Center for Integrated Quantum Science and Technology (IQST), Albert-Einstein-Allee 11, D-89081 Ulm, Germany

Within the last two decades, quantum technologies (QT) have made tremendous progress, moving from Nobel Prize award-winning experiments on quantum physics[17] into a cross-disciplinary field of applied research. Technologies are being developed now that explicitly address individual quantum states and make use of the 'strange' quantum properties, such as superposition and entanglement. The field comprises four domains: quantum communication, where individual or entangled photons are used to transmit data in a provably secure way; quantum simulation, where well-controlled quantum systems are used to reproduce the behaviour of other, less accessible quantum systems; quantum computation, which employs quantum effects to dramatically speed up certain calculations, such as number factoring; and quantum sensing and metrology, where the high sensitivity of coherent quantum systems to external perturbations is exploited to enhance the performance of measurements of physical quantities.

Recently QT have received a lot of public attention: governments have launched large research programmes on QT, such as the Chinese programme (which includes the launch of a satellite and the instalment of a quantum key distribution (QKD) link between Beijing and Shanghai) or the European QT flagship initiative, summing up to several billion Euros of public funding for the field worldwide. At the same time, large multinational companies, including Google, IBM, Intel, Microsoft and Toshiba, have started to invest heavily in QT, especially in quantum computing and quantum communication. Also, a number of start-up companies were established during the last decade which successfully offer QT to specialised markets.

One success factor for the rapid advancement of QT is a well-aligned global research community with a common understanding of the challenges and goals. In Europe, this community has profited from several EC funded coordination projects, which, among other things, have coordinated the creation of a 150-page QT Roadmap [2]. This article presents an updated summary of this roadmap. Besides sections on the four domains of QT, we have included sections on quantum theory and software and on quantum control, as both are important areas of research that cut across all four domains (see figure 1). Each section, after a short introduction to the domain, gives an overview on what is, in the authors' opinion, its status and main challenges and then describes the advances in science and technology foreseen by the authors for the next ten years and beyond.

It is important to note that, although this roadmap is based on European coordination efforts and all authors are Europeans, the scientific and technological status as well as the challenges and required advancement described in this roadmap are not perceived by the authors as specific to Europe, but global to the field of QT. The priorities of the European quantum flagship are developed, based on this assessment.

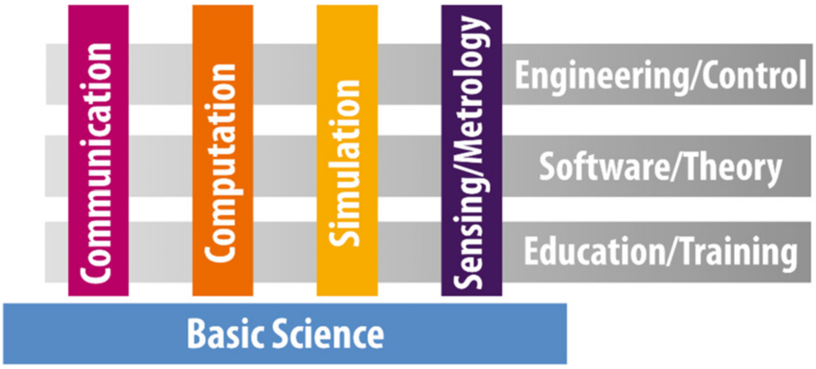

Figure 1. Structure of the research field of quantum technologies, according to final report of the High-Level Steering Committee on the European QT flagship initiative [1].

[17] 1997:Chu,Cohen-Tanoudji, Phillips; 2001:Cornell, Ketterle,Wieman; 2005:Hall,Hänsch,Glauber; 2012:Haroche,Wineland.

2. Quantum communication

Rob Thew, Nicolas Gisin
Group of Applied Physics, University of Geneva, CH-1211 Geneva 4, Switzerland

Introduction. Quantum communication involves the generation and use of quantum states and resources for communication protocols. Its main applications are in provably secure communication, long-term secure storage, cloud computing and other cryptography-related tasks, as well as in the future, a secure 'quantum web' distributing quantum resources like entanglement, nonlocality, randomness and connecting remote devices and systems. Typically, the underlying protocols are built on quantum random number generators (QRNG) for secret keys and QKD for their secure distribution. The archetypal QRNG involves a photon impinging on a beam splitter followed by two detectors associated to the bit values 0 and 1, where the origin of the randomness is clearly identified. QKD systems take this one step further to distribute this randomness in a correlated way; such that two parties share the same random string in a private and secure fashion. Secure solutions based on quantum encryption are importantly also immune to attacks by quantum computers (QCs), and are commercially available today, as is quantum random number generation. Indeed, 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.

Current status. Currently, typical fibre-based QKD systems can only function over distances of around 100 km for commercial systems, although academic prototypes can push this to around 300 km [3], which is limited by transmission loss in optical fibres; quantum information is secure because it cannot be cloned, but for the same reason it cannot be relayed through conventional repeaters. In classical optical telecommunication, the problem of loss is solved by using simple optical amplifiers that restore the transmitted signal. However, these are of no use for quantum communication as they are intrinsically noisy and create so many errors that any quantum key being transmitted would not survive. So, quantum communication must reinvent the repeater concept, using quantum hardware that preserves the quantum nature, the entanglement. Therefore, repeaters based on trusted nodes or fully quantum devices, possibly involving satellites, are needed to reach global distances. Trusted node relays consist of multiple QKD systems that are chained together to build longer and more complex fibre networks, which can provide backbone or access [4] network architectures but require a trusted environment where the devices can be connected together. Satellites [5] and high altitude platform stations (HAPS), which include drone-based scenarios, provide an alternative approach and potentially complimentary solution. Fully quantum-secure solutions for long-distance quantum networks, based on quantum repeaters exploiting multimode quantum memories, aim to increase the distances between trusted nodes as well as providing the ability to distribute entanglement to distant locations for interfacing with quantum processors or sensors and provide opportunities for novel applications. Quantum repeaters [6] allow one to break the transmission distance up into shorter distances where entanglement can be prepared and stored in a quantum memory—a device capable of storing quantum states. Once the different sections are ready they can be connected by so-called Bell-state measurements until the entire communication length is entangled, for example, allowing one to 'teleport' qubits directly to their destination, thus avoiding transmission losses. There is currently enormous activity in developing quantum memories using a wide variety of physical platforms [7] that are both efficient (information is not lost) and offer scalable solutions for the grand challenge of continental and global scale quantum-secure communication and entanglement distribution.

There is also currently a great deal of theoretical work taking place on developing new protocols and new approaches to certifying systems, for example, their security. This work on new protocols and certification takes several different approaches from work bringing quantum and classical security experts together [8] to developing practical security proofs, or those coming from a more fundamental perspective, i.e. studies of nonlocality in what are called 'device-independent' protocols [9], or related 'self-testing' strategies. Certification is also starting to take into account commercial considerations to have devices and systems certified for compliance with industry standards. Standards themselves represent an important challenge that has begun to be addressed by research projects that bring together industry and academics, as well as national metrology labs, such as Metrology for Industrial Quantum Communication and Optical Metrology for Quantum-Enhanced Secure Telecommunication.

Advances in science and technology needed to meet future challenges. Quantum communication is both a broad field, addressing numerous tasks and applications, but also one that spans research and engineering challenges from fundamental to applied and towards the development of prototype devices and systems as well as managing their functionality in diverse network architectures. It is also a field in which there is an incredible

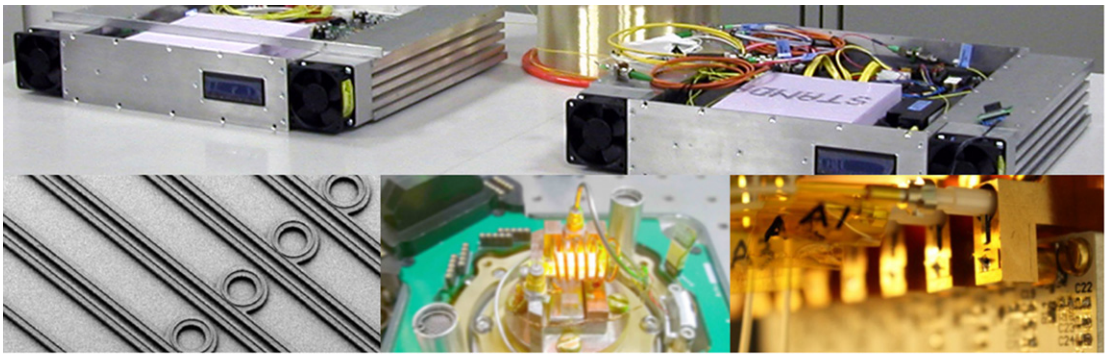

Figure 2. University prototype QKD system capable of autonomous operation over distance >300 km. Integrated photonics, such as micro-resonators, provide a compact source for entangled photon pair generation as well as quantum frequency conversion. Quantum memories are crucial and rapidly developing technologies for quantum repeaters. Here we see a solid state (rare-earth ion) but there are a wide spectrum of physical systems being exploited. Improved materials and electronics are providing a new generation of superconducting nanowire single photon detectors with almost ideal performance.

range of possible technology platforms that can be exploited for any given task. Figure 2 illustrates a small example of this diversity. As such, we will not give a detailed roadmap of what is required in all of these different platforms, but focus on the current and future challenges that are being targeted.

Foreseeable within the next three years is the development of autonomous QKD systems over metropolitan distances that will address low deployment costs, high secure key rates (>10 Mbps) and multiplexing. It is expected that integrated photonic solutions will be critical in these efforts. Certification and standards for quantum communication devices and systems will be established, as required by the security community, industry, ESA and government organisations. QRNGs e.g. for use as components of cheap devices will be developed targeting high-volume markets or high-speed systems, including entropy source and application interface. QRNG and QKD devices and systems will address issues of practicality, compactness, high-rates, or include novel approaches that address security vulnerabilities or certification challenges. To extend QKD beyond the direct communication distance limit (>500 km), the underlying technologies for trusted nodes, quantum repeaters, HAPS and satellites will need to be developed. Quantum repeater and multipartite entanglement-based network building blocks are aiming to demonstrate improved performance for core technologies, including: efficient and scalable quantum memories and interfaces; frequency conversion; teleportation; entanglement distillation; error correction; sources of single photons and entanglement, and detectors. Practical protocols and efficient algorithms for quantum networks, e.g. digital signatures, position based verification, secret sharing, oblivious data searching, will be developed. Solutions that use both classical and quantum primitives will also be explored to ensure compatibility with existing infrastructure as well as working towards long-term, future-proof, security.

In 6 years, we will likely see QKD in test-bed networks, demonstrating long distances via trusted-nodes, HAPS or satellites, as well as multi-node or switchable intra-city networks, all of which will require large-scale infrastructure projects to be initiated. Autonomous QKD systems suitable for low-cost volume manufacturing as well as systems targeting increased (>100 Mbps) secure key rates over metropolitan distances will be targeted. Quantum repeaters and entanglement-based networks beating direct communication distances will be demonstrated. Hardware and software for entanglement-based networks will be developed, including multipartite and device-independent-inspired protocols, with explicit and demonstrable assumptions about security, e.g. for QRNG as well as QKD over >10 km.

In the long-term it is important to consider not only the research but the innovation environment that will have been created and what will follow. The long-term objectives of the quantum communication community include: generalised use of autonomous QKD systems and networks; device independent QRNG systems and QKD over metro-area distances; quantum cryptography over >1000 km, and protocol demonstrations, e.g. cloud computing, on photonic networks connecting remote quantum devices or systems.

To ensure the success of all of these objectives there is a need for dedicated engineering support for all of these activities across the research and development spectrum. These engineering, as well as control, solutions are aiming to enable scaling and volume manufacturing, e.g. development of high-speed electronics and opto-electronics, including FPGA/ASIC, integrated photonics, packaging, compact cryo-systems, and other key enabling technologies, to provide solutions compatible with operating in existing communication networks. This will also need support in terms of theory and software development of protocols and applications that build on, or go beyond, standard QRNG- and QKD-based primitives, as well as novel approaches for their certification, including methods to test and assess the performance of quantum networks; more efficient algorithms and security proofs targeting practical systems, including the combination of classical and quantum encryption techniques for holistic security solutions and expanding the potential application market.

Conclusion. The security of our information-based society is of rapidly increasing importance. The long-term secure management of data in transit and at rest is of paramount importance for society and the economy as well as our infrastructures and services, our prosperity, as well as for political stability. These risks are augmented by growing technological threats such as the development of a QC, which makes the most commonly used asymmetric cryptography algorithms vulnerable and poses a systemic threat to long-term security. Quantum communication provides solutions that can be integrated into existing infrastructure and protocols as well as opening up new application regimes. These ambitious objectives, and the innovative environment being developed to realise them, should form a solid basis to ensure that QT play a leading role in the science, technology and digital economy of the 21st century.

We thank the many members of the community who have contributed to the content of this article, in particular P Grangier, R Renner, G Ribordy, A J Shields, and R Ursin.

3. Quantum computation

Frank K Wilhelm[1], *Daniel Esteve*[2], *Christopher Eichler*[3], *Andreas Wallraff*[3]
[1]Theoretical Physics, Saarland University, D-66123 Saarbrücken, Germany
[2]Service de Physique de l'Etat Condensé, CEA-Saclay, F-91191 GIF-SUR-YVETTE, France
[3]ETH Zurich, Department of Physics, CH-8093 Zürich, Switzerland

Introduction. A QC based on the unitary evolution of a modest number of robust logical qubits ($N > 100$) operating on a computational state space with 2^N basis states would outperform conventional computers for a number of well identified tasks. A viable implementation of a QC has to meet a set of requirements known as the DiVincenzo criteria: that is, a QC operates on an easily extendable set of well characterised qubits (1) whose coherence times are long enough for allowing coherent operation (2) and whose initial state can be set (3). The qubits of the system can be operated on logically with a universal set of gates (4) and the final state can be measured (5). To allow for communication, stationary qubits can be converted into mobile ones (6) and transmitted faithfully (7). It is also understood that it is essential for the operation of any QC to correct for errors that are inevitable and much more likely than in classical computers. Note that the last two are crucial for some but not all applications or platforms.

Today quantum processors are implemented using a range of physical systems. Quantum processors operating on registers of such qubits have so far been able to demonstrate many elementary instances of quantum algorithms and protocols. The development into a fully featured large QC faces a scalability challenge which comprises of integrating a large number of qubits and correcting quantum errors. Different fault-tolerant architectures are proposed to address these challenges. The steadily growing efforts of academic labs, startups and large companies are a clear sign that large scale quantum computation is considered a challenging but potentially rewarding goal.

Toward scalable architectures for the gate model. Controlling and error-correcting the unitary evolution of about 100 logical qubits will be a major milestone in the quest for overcoming present-day classical processors on specific tasks, e.g. in quantum chemistry or simulation. Realising logical qubits includes encoding in a larger number of physical qubits with sufficient functionality in a viable architecture. This may imply, for example, creating large scale 2D traps for ions or realising the surface code architecture for superconducting qubits. The most promising architectures for achieving fault tolerance may be specific to the respective platform but address common challenges.

Alternative architectures for quantum computing. Given the significant challenges of implementing fault-tolerant gate-based processors, alternative concepts subject to different sets of challenges are actively pursued. Most prominently, quantum assisted annealing is followed by companies such as D-wave systems, Google and a number of academic labs, with quantum speedup being unclear at best.

In the following, we will describe the current status and the advances in science and technology needed to meet the challenges for the five most important QC platforms.

Status and challenges

Trapped ions. Ion trap quantum computing typically operates on a qubit register formed by a linear string of ions confined in a Paul trap [10]. Each physical qubit is based on two internal levels of a single ion—defined within a Zeeman or hyperfine manifold or corresponding to a forbidden optical transition. Gate operations use microwave or laser fields.

Quantum algorithms have been performed on strings of up to seven ions confined in a linear trap. Longer chains of up to 20 ions and 2D crystals of up to ~300 ions have been trapped and used for quantum state engineering or simulation. Individual qubits can be initialised with error below $\sim 10^{-3}$, are controlled with gate errors of $\sim 10^{-6}$, and read out with an error of $\sim 10^{-4}$. Two-qubit gates have errors of $\sim 10^{-3}$. The conversion from stationary to flying qubits has been demonstrated, as well as the transfer of quantum information over short distances by physically transporting ions across a microchip. They can be benchmarked by gate fidelities between remote qubits [12].

Scalability remains the most significant challenge in ion systems [11] for which well-defined approaches based on micro-fabricated traps and photonic interconnects are developed. Various fabrication techniques and electrode configurations are investigated. Micro-fabricated 2D RF-trap arrays have already been successfully demonstrated. A difficulty encountered in miniaturised ion traps is the marked growth of the electric-field noise

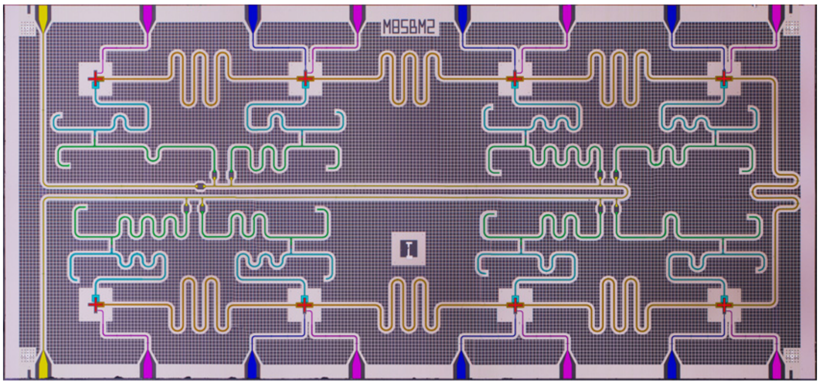

Figure 3. False-coloured image of an 8-qubit superconducting quantum processor fabricated at ETH Zurich. All eight qubits (red) are measured using a common readout line (yellow), by coupling each qubit (red) to a pair of readout resonator (cyan) and Purcell filter (green). Qubit control is enabled by individual charge lines (purple) and flux lines (blue). Coupling between nearest neighbour qubits is mediated by bus resonators (orange).

in the vicinity of trap surfaces causing unwanted motional heating. This issue has been addressed by operating at cryogenic temperatures, and/or by applying an *in situ* cleaning of the trap surface.

Further short- and mid-term goals specific to ions in microfabricated traps include demonstration of high-fidelity gates in multiple ion registers, operation of 2D traps, integration of optics and control electronics and demonstration of high-fidelity quantum information transport between ion registers, and between three or more networked traps.

Superconducting circuits. Quantum computation with superconducting circuits exploits the intrinsic coherence of superconductors and the Josephson effect as a resource of dissipationless non-linearity for making artificial atoms. Qubits are realised as resonant microwave circuits embedding a Josephson tunnel junction, of which the two lowest energy levels are used as an effective quantum bit [13]. Superconducting qubits are fabricated with thin-film technology, are probed and controlled with microwave radiation and can be strongly coupled to each other by circuit elements [14]. Superconducting resonators and cavities confine microwave photons with long-lived coherence and provide large zero-point electric and magnetic fields at selected locations. An example chip can be seen in figure 3. They hence 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 illustrating its potential. Processors with 4–17 qubits have demonstrated the basis of quantum error correction protocols, elementary quantum algorithms, and simulations. Universal gate operations are performed with fidelities in excess of 99.9% for single qubits and 99.5% for two-qubit gates. The use of optimised parametric amplification routinely enables single-shot, non-demolition qubit measurements with fidelities exceeding 99%. The coherence times of qubits are constantly increasing and have reached 150 μs, to be compared to projected times of two-qubit gates of around 100 ns. At the same time, fast classical control electronics, as required for real-time feedback, are rapidly advancing.

Designing and fabricating large scale superconducting circuits addressing all circuit elements without crosstalk is challenging. Microfabricated superconducting qubits are sensitive to imperfections in their fabrication limiting yield and reproducibility of device parameters. Both aspects require optimisation of design and production processes. Operation of devices below 50 mK requires refrigeration technology which is realisable beyond a few hundred qubits. Goals include to realise an extensible quantum processor architecture, allowing copy-pasting of unit cells, develop transitioning from millimetre to centimetre scale chips, and from lateral to vertical coupling of all control signals to the chip, realise an extensible, control electronic architecture for control of the quantum circuit, operating either at room temperature, cryogenically, or a combination of both, and develop automated tune-up and calibration procedures.

Electronic semiconductor qubits. In semiconductor host materials single electrons can be either trapped by isolated donor atoms, confined in ultra-small islands or using gate-defined potentials, or by topological effects. The spin degree of freedom in these systems is considered promising due to its long coherence time. These devices can be measured and controlled fully electrically and their fabrication exploits the same technologies as the semiconductor industry. Recently, group IV materials such as Si/SiGe have attracted increasing attention, as they offer long spin coherence times when using nuclear spin-free ^{28}Si isotopes.

Quantum dot circuits with up to five quantum dots have been controllably loaded. Single qubit gates have fidelities in excess of 99%, spin states are initialised with 99.9% fidelity, and single shot readout of up to three qubits was demonstrated with an average fidelity of 97%. Coherence times as long as $T2\ (T2^{*}) = 500\ (0.2)$ ms have been measured in isotopically enriched ^{28}Si. Coherent exchange coupling and interaction between two spins in a double dot have been demonstrated [15].

One of the main challenges remains the development and improvement of high fidelity two-qubit gates, particularly for donor spins. Various material needs to be investigated and eliminated. Further goals contain the 'unit cell' demonstration of a scalable 2D spin qubit architecture, identification of robust and secure sources for high-purity semiconductor materials and demonstration of precise positioning of donor arrays.

Impurity spins. Atomic and molecular spins in solids such as colour centres, rare earth ions, deep donors, and molecular magnets, can use both the electron and nuclear spin degrees of freedom as qubits. Control of these systems is typically achieved by combining highly advanced techniques from NMR with optical manipulation. These systems promise good shielding from the environment leading to long coherence time [16].

The most advanced platform so far are nitrogen vacancy centres in diamond. Initialisation and single shot spin readout are achieved with optical control, while single qubit gates employ microwave fields. Two-qubit gates between multiple spins are based either on magnetic dipolar interactions or on long distance optical coupling. Multipartite entanglement, quantum teleportation over long distances, quantum error correction, and elementary quantum algorithms have been demonstrated [17]. Despite recent progress, nano-positioning and the creation yield of defects is still a major and most pressing challenge.

Linear optics. Linear-optical quantum computing (LOQC) employs single photons, linear optics elements (discrete or on chip), photon-counting measurements, and feed-forward but avoids using direct photon interactions in nonlinear media. To date, there are two main physical architectures for LOQC: the scheme by Knill, Laflamme and Milburn (KLM), and the one-way quantum computing scheme. The KLM scheme is based on the preparation of multi-particle entangled states and (entangling) multi-particle projective measurements. One-way quantum computing exploits a series of adaptive single-qubit rotations and measurements applied to cluster states that provide the resource.

The control of large entangled states has been achieved experimentally [18, 19]. Small-scale algorithms have been demonstrated, including alternative computational models based on quantum walks. Complete architectures for LOQC still need to be developed and hard bounds on the required performance of photonic components have to be investigated theoretically.

Conclusion. Many implementations of quantum information processors share common goals. Improving coherence properties of qubits and enabling to enhance single and two-qubit gate fidelities, at least beyond the fault tolerant threshold, is a goal pursued throughout that will remain relevant in future. Within the next five years, demonstrations of error-corrected logical qubits with performance beyond the constituent physical qubits are to be achieved in a few implementations, as well as fault-tolerant gates on those logical qubits. To operate systems of many physical qubits in an extensible fashion, scalable classical control electronics and tune-up routines for large-scale quantum systems need to be realised and qubit operation quality needs to be made consistent over large systems. In five to ten years, demonstrations of quantum algorithms operating on logical qubits in a universal QC are envisaged. At the same time, functional quantum interfaces for short, medium and long distance communication between quantum computing modules are foreseen to be functional. On the time scale of ten years and beyond the demonstration of large scale quantum computation systems is pursued. With such systems solving technologically relevant algorithmic problems as outlined in the software and theory section, is expected to be feasible.

We thank the many members of the community who have contributed to the content of this article.

4. Quantum simulation

Jens Eisert[1], *Immanuel Bloch*[2,3], *Maciej Lewenstein*[4,5], *Stefan Kuhr*[6]
[1]Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, D-14195 Berlin, Germany
[2]Fakultät für Physik, Ludwig-Maximilians-Universität München, Schellingstrasse 4, D-80799 Munich, Germany
[3]Max-Planck-Institut für Quantenoptik, Hans-Kopfermann-Str. 1, D-85748 Garching, Germany
[4]ICFO-Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, E-08860 Castelldefels (Barcelona), Spain
[5]ICREA, Passeig de Ll. Campanys, 23, E-08010 Barcelona, Spain
[6]University of Strathclyde, Department of Physics, SUPA, Glasgow G4 0NG, United Kingdom

Introduction. 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 [20]. In general, the classical simulation of quantum systems requires 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. Similarly, solutions of certain classical optimisation problems, in particular NP-hard and NP-complete ones, require exponential resources. Numerical methods, such as tensor networks or the density-matrix renormalisation group approach, as well as quantum Monte Carlo sampling allow for computing of ground state properties in certain situations. Such classical simulation methods are generally applicable to restricted classes of problems and have their limitations. For example, the systems sizes that can be studied numerically on classical computers are often rather small and it seems unlikely that these classical tools will be powerful enough to provide a sufficient understanding of the full complexity of many-body quantum phenomena. In the language of complexity theory, approximating the ground-state energy of local Hamiltonian problems is quantum Merlin-Arthur (QMA) hard, and time evolution under local Hamiltonians is BQP (bounded error quantum polynomial time) complete, so both amount to computationally hard problems. Similarly, finding a ground-state energy of a classical spin glass, or solving the travelling salesman's problem, are computationally difficult. Quantum simulators promise to overcome some of these limitations.

Current status. In 1982, Richard Feynman 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 delineated blueprints for potential architectures [20]. This basic idea was further substantiated by work showing that a universal QC would indeed be able to efficiently keep track of the dynamics of any local quantum system, allowing for precise error analysis by means of the Trotter formula [21]. 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 interesting property of an interacting complex quantum or classical 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). Alternatively, it may serve to encode hard classical constrained optimisation problems (such as satisfiability).
- The simulated models should address a challenging problem and further our understanding in the addressed field.
- The simulated models should be expected to be computationally intractable or difficult for classical computers.
- A quantum simulator should allow for broad control of the parameters of the simulated model, as well as for control of the preparation, manipulation and detection of the states of the system. This feature can then be used to test models and hypothesis over a wide parameter regime in a precise fashion.

It can be helpful to be able to set the parameters of the quantum simulation in such a way that the model becomes tractable using classical simulations for purposes of validation through known 'reference results'. 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.

Before turning to architectures for quantum simulation, it is helpful to be reminded of classical simulation methods aimed at computing properties of quantum many-body systems. The new research field 'Hamiltonian complexity' aims to identify obstacles that any such classical simulation must ultimately face: for example, approximating the ground-state energy of an interacting local Hamiltonian problem to polynomial accuracy in the number of particles is QMA-hard, limiting the hopes that a universal classical simulation of key models in condensed-matter physics could be achieved. Similarly, many classical complex optimisation problems are proven to be NP (nondeterministic polynomial time) hard. Still, for many practical purposes, classical simulations of quantum and classical systems, including solving constrained optimisation problems are possible for specific models and in many regimes, at least to the level of a heuristic understanding.

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

- *static quantum simulators* [22, 26, 27], probing static properties of interacting systems such as ground-state features, from
- *quantum annealers* [28] approximating solutions to classical optimisation problems, employing quantum annealing/adiabatic methods, and
- *dynamical quantum simulators* [21, 22, 24], probing properties related to non-equilibrium [25].

In terms of how the simulation is performed, one discriminates

- *digital quantum simulators* [20, 21, 23], which are based on quantum circuits implemented on a QC, and may in principle be made fault tolerant,
- *analogue quantum simulators***,** simulators that reconstruct the time evolution of an interacting quantum system under precisely controlled conditions [22, 24, 26].

The advantage of analogue quantum simulators is that a large number of constituents can be addressed and experimented with, even using architectures that are available with present technology. Quantum simulations thereby offer new insights into phenomena of complex quantum systems, with applications ranging from condensed matter physics over statistical physics, high-energy physics, cosmology and possibly even notions of energy transfer in biological systems. It is conceivable that quantum simulators can also help to interpret measurement results originating from sophisticated measurement techniques applied to real materials, e.g., 2D electronic spectroscopy or transport measurements. Due to the precise control over the Hamiltonian parameters, 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 engineer materials with specialised properties. A first step in this endeavour is usually to identify the underlying model Hamiltonian, which is then probed by the actual quantum simulation.

There are a number of physical platforms that allow for controlled quantum simulations. Promising advances have been achieved in these different systems at different levels of maturity at the present stage. Experimental platforms [27] for quantum simulation comprise

- ultra-cold atomic and molecular quantum gases, specifically systems of cold atoms in optical lattices (see figure 4) or continuous systems confined by atom chips,
- ultra-cold trapped ions,
- polariton condensates in semiconductor nanostructures,
- circuit-based cavity quantum electrodynamics,
- arrays of quantum dots,
- Josephson junctions and superconducting qubits that already have commercial applications in quantum annealers, and
- photonic platforms, such as integrated waveguide structures.

Advances in science and technology needed to meet future challenges. Quantum simulations allow to probe and explore properties of complex quantum systems under precisely controlled conditions. Despite significant advances both in theory and experiment, from the conceptual perspective, several problems remain open. This includes in particular the

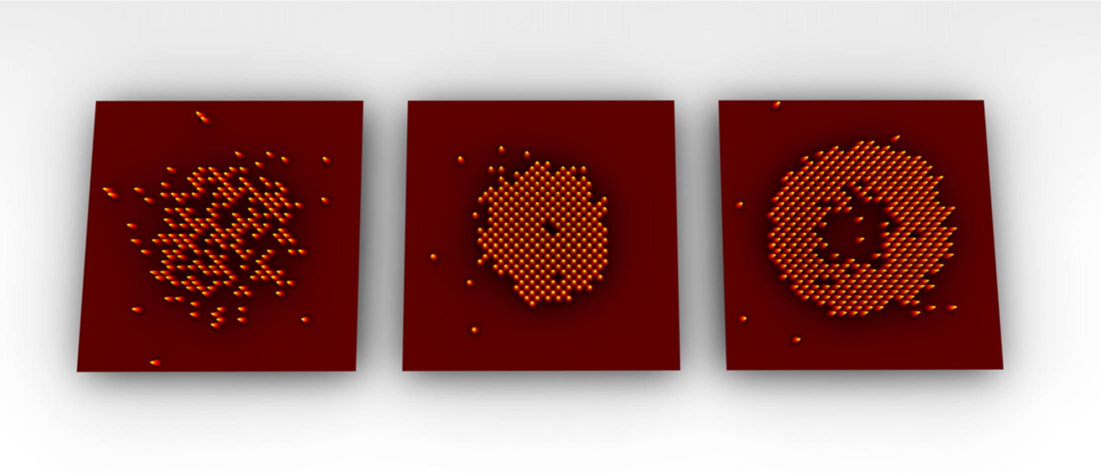

Figure 4. Reconstructed quantum gas microscope images of single atoms held in an optical lattice. The images indicate two different phases of matter: a weakly interacting BEC (left) and a strongly interacting bosonic Mott insulator (middle/right) for two different atom numbers. Such single photographic snapshots of quantum matter enable to probe and analyse interacting many-body systems in completely new ways. (Source: Max-Planck Institute of Quantum Optics.)

- identification of models that are 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 of sufficient size while at the same time exhibiting a high degree of control.

A key challenge is to find out whether the device has actually correctly performed the quantum simulation. This constitutes an 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 to assume, that even if the entire family of models to be quantum simulated is inaccessible by classical means, there are suitable parameter regimes for which 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 efficiently predict the outcome of the simulation.

However, there are some tasks in quantum simulation, such as approximating ground state energies, which not even a presumed QC can overcome. Other aspects, such as the difficulty of computing long-time dynamics of many-body quantum systems, leave room for a computational quantum advantage of quantum simulators over classical ones, often eluded to as ‘quantum supremacy’. Quantum annealers provide approximate solutions to NP-hard problems, but it is still unclear in what precise sense quantum simulators will provide an advantage over classical simulations [28], this being a research area under active consideration. At the same time, another profound conceptual question arises: if error correction and fault tolerance are not available, it is still not fully understood to what extent verified quantum simulators and annealers can outperform classical computers.

Conclusion. If a concise answer to this and related questions can be established, quantum simulators will play a pivotal role in our study of quantum many-body physics and allow to tackle the many complex challenges related to it. Moreover, even before these questions of verification and certification are completely resolved, which can reasonably be expected to be true within the next five to ten tears, analogue quantum simulators give us a novel tool to explore and understand features in interacting many-particle quantum systems and optimisation problems that are beyond the reach of classical computers. As a long-term goal beyond the next ten years, it is expected that large-scale quantum simulations can be performed to tackle key questions in physics, materials science and quantum chemistry.

We thank the many members of the community who have contributed to the content of this article.

5. Quantum metrology, sensing, and imaging

Fedor Jelezko[1], *Piet O Schmidt*[2,3], *Ian Walmsley*[4]
[1]University Ulm and Center for Integrated Quantum Science and Technology (IQST), Albert-Einstein-Allee 11, D-89081 Ulm, Germany
[2]QUEST Institute for Experimental Quantum Metrology, Physikalisch-Technische Bundesanstalt, D-38116 Braunschweig, Germany
[3]Institut für Quantenoptik, Leibniz Universität Hannover, D-30167 Hannover, Germany
[4]Clarendon Laboratory, Department of Physics, University of Oxford, Oxford OX1 3PU, United Kingdom

Introduction. Measurement is the basis not only of science, which demands empirical quantitative assessment of phenomena, but also of commerce, which requires standards for metrology, without which there can be 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 characterisation, fundamental science from the sub-nano to the galactic scale as well as determining the fundamental constants relied upon for industry and commerce.

The central concept of a sensor is that a probe interacts with an appropriate system, the properties of which are of interest, which changes of state of the probe. Measurements of the probe reveal the parameters that characterise the system. In quantum-enhanced sensors, the probe is generally prepared in a particular non-classical state. The encounter with the system typically 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 system parameters to be made, and thus the sensor response to be determined. The precision of this estimate as a function of the resources used (e.g. the number of particles in the probe or measurement time) is a measure of the effectiveness of the sensor. The best classical sensors exhibit a precision that scales proportionally to the square root of the number of particles N in the probe (known as the standard quantum limit, SQL) whereas the best quantum sensors can in principle attain a precision that scales as N (known as the Heisenberg limit).

Quantum enhanced sensing promises significant improvements in the precision with which properties of a wide range of systems can be estimated. The platforms for implementing new sensor protocols range from the nanoscale, by means of localised spins to the planetary scale, based on photons. Some platforms are already close to commercial application, others require new science and engineering to be fully viable. In the next sections we describe the current status and the advances in science and technology needed to meet the challenges for the most important quantum sensor platforms.

Current status

Atom and optical sensors

Photonic sensors. Practical designs for ultra-bright sources of quantum light with reduced noise [29] and entanglement together with development of novel principles for engineering practically useful quantum states and measurements [30] have revolutionised photonic quantum sensing. For instance, recent demonstrations have shown the possibilities for multi-photon interferometry beyond the classical limit [31], and it has been shown that weak field homodyning could yield enhanced resolution in phase detection. Early 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 imaging [32]. In addition to quantum correlated photon states, (macroscopic) squeezed states of light can be also used as a resource for quantum-enhanced sensing. Currently squeezed light techniques are in use in GEO600, and will be adopted by LIGO [33]. Squeezed light strategies are in development for deployment in a next-generation gravitational-wave detector, the Einstein Telescope. Squeezed light has also been exploited to resolve a small beam displacement, which in turn has been used to perform quantum-enhanced micro-rheology on a living cell [34].

Atomic 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. Sensors using micro-Bose–Einstein condensates enable exotic quantum states that allow precision sensing of fields near surfaces, for instance. Current atomic gravity sensors offer absolute measurements at the nano-g level or gravity gradient sensitivities surpassing a 100 pico-g change over 1 m distances [35, 36]. The potential impact includes

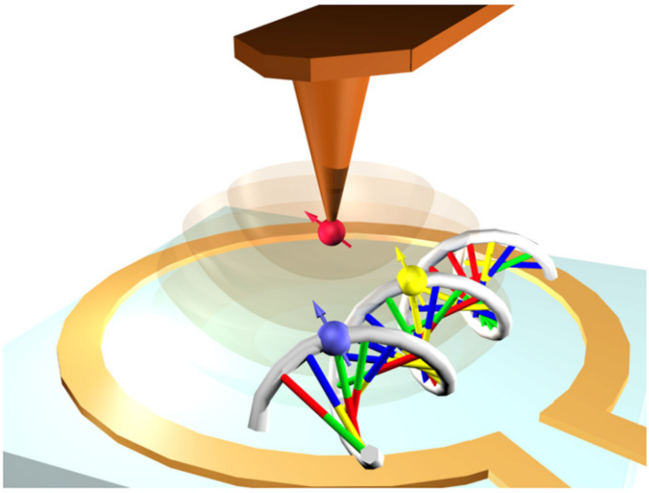

Figure 5. Artistic depiction of a spin based quantum sensor for unravelling structure of single biomolecules.

infrastructure, 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.

Quantum clocks. Atomic clocks are the most established example of quantum technology, having been used since 1967 for international timekeeping. Optical clocks currently under investigation range from neutral atoms in optical lattices and singly charged ions and molecules to highly-charged ions and even nuclear transitions [37]. Neutral atoms offer a high signal-to-noise ratio but are in general more susceptible to external fields and collisional shifts, requiring their environment to be well-controlled. In contrast, single ion setups can be very simple and technologically less demanding to achieve a similar level of accuracy as their neutral atom counterparts at the expense of longer averaging times. So far most of quantum clocks were limited by SQL, but first demonstrations of enhanced SNR through spin squeezing in microwave clocks have been reported [37].

Quantum imaging. Related to precision sensing using light is the idea of image acquisition. One analogy is that an image is a set of parameters that characterise the object, acquired in a massively parallel manner. This intrinsic feature of optical imaging enables exploitation of the different degrees of freedom of light: its spatial and temporal (or, equivalently, directional and frequency) structure, to enable optical resolution beyond the standard wavelength limit, with low light levels, or in the presence of strong background illumination. For instance, one proposed application is in quantum microlithography, where the quantum entanglement of the spatial degrees of freedom of light beams is able to affect matter at a scale smaller than the wavelength by patterning substrates by means of intensity correlations. 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. Correlations between quantum light beams enables new modes of imaging such as so-called ‘ghost imaging’ in which an image of an object that is illuminated by one beam is acquired by a camera looking at a different beam, that did not impinge on the object.

Spin-qubit-based sensing. Sensing using spin qubits is a relatively new and upcoming field in quantum sensing. While sensing magnetic fields comes most naturally for spin sensors [38] and is of crucial importance for several fields for science including chemistry, biology, medicine and material science, spin-based sensing of a variety of different quantities, including temperature, electric field and pressure as well as force or optical near-fields has been demonstrated with diamond defect and defects in silicon carbide. All rely on the long living quantum coherence of spins to build robust, calibration free sensors. These devices operate by measuring the quantum phase accumulated by a qubit in the presence of the external perturbation. Coherent control of qubits including dynamical decoupling techniques is crucial for achieving best performance.

At present quantum spin sensors are targeting the following benchmarks: high sensitivity; spatial resolution; spectral and temporal resolution (when measuring AC fields). Note that high sensitivity and spectral resolution in quantum metrology requires long spin coherence times, which often is not compatible with room temperature operation for variety solid state qubits (crucial for applications in life sciences). 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. Figure 5 depicts the use of such a sensor for the structural analysis of single biomolecules.

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. Nano-electromechanical systems (NEMS) and MEMS can now be measured 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, and real time quantum feedback, among many others [39]. 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 realise 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 visible photons to the telecommunication band or realising 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.

Advances in science and technology needed to meet future challenges

Atomic and optical sensors. 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. Nonetheless, for all platforms, certain entangled states can give considerable improvements above the SQL. 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. Atomic sensors typically suffer from lower losses than photonic sensors, but are more subject to dephasing noise. For cold atomic ensembles, the ability to prepare the initial probe states limits the repetition rate of the sensor, whereas for hot ensembles atomic motion is the limiting factor. In both cases, chip-scale integration will be important for space, mobile and personalised sensors. Further, combining photonic and atomic platforms may yield new capabilities [40]. The instability of all optical clocks is currently limited by the residual noise of the clock laser. The challenge is to further improve existing techniques for laser frequency stabilisation based on e.g. cavities, spectral hole burning, or even lasing on a clock transition. New clock technology needs to be combined with reductions in size, weight, power consumption and cost to enable field applications e.g. in relativistic geodesy and navigation.

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. In particular, new measurement protocols as well as post-processing of the measurement outcomes can be further optimised. For instance, feedback-based protocols, dynamical decoupling, and optimal control may all add new capabilities to quantum sensing protocols., such as reducing the effect of technical noise and using the available resources in the most efficient way. Powerful methods from signal processing, which have already yielded fruit in the design and assessment of sensor performance, could be applied to minimise the measurement effort to extract the desired signal.

Spin-qubit-based sensing. Although first proofs of principle demonstration show high potential of diamond sensing devices for magnetic field sensing, key challenges that 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 bio-analytical applications, integration into existing analytical devices like fluorescence microscopes is needed.

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 the Heisenberg limit.

Applications of NV magnetometers in life sciences and medicine depend on the ability to insert nanodiamonds doped with colour centres into cells. Sensing 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). A remaining challenge is the size reduction of nanodiamonds as well as their versatile surface functionalisation allowing selective protein targeting.

Optomechanical sensors. 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 preparation of 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 band-gap architectures and substrate-free levitated topologies, which will eventually allow quantum operation at room temperature.

Conclusion. The potential impact of quantum sensors is broad and considerable. A variety of different platforms enables quantum-enhanced measurement of time, space, rotation, as well as gravitational, electrical and magnetic fields. All these technologies find important applications in fields as physics, chemistry, biology, medicine or data storage and processing.

We thank the many members of the community who have contributed to the content of this article.

6. Quantum control

Frank K Wilhelm[1], *Steffen J Glaser*[2]
[1]Theoretical Physics, Saarland University, D-66123 Saarbrücken, Germany
[2]Department of Chemistry, Technical University of Munich, Lichtenbergstrasse 4, D-85747 Garching, Germany

Introduction. 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.

The challenge to manipulate nature at the quantum level offers a huge potential for current and future applications both in traditional applications and in modern QT. It is part of the effort to engineer QT 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. 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 distinct from classical control problems.

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 [42] which is very detailed and covers both first- and second generation QT.

Current status. 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. Closed loop techniques involve the use of feedback to stabilise a given system state or to obtain a desired quantum input-out gain. As in classical engineering, the mathematical problem is controller design. In the quantum situation this can be measurement-based or fully coherent [43].

Currently, the theory of controllability is well and rigorously understood for closed systems with finite-dimensional state space and there is solid understanding of the Markovian open case as well as a few results outside those paradigms. Analytical solutions are available for simple, low-dimensional as well as pseudoadiabatic systems. Although numerical approaches such as gradient ascent, quasi-Newton, Newton and Krotov methods have reached a reasonable maturity and lead to robust and tailored software packages [44, 46, 47], many opportunities exist to significantly improve their performance. They are complemented by gradient-free approaches including the chopped random basis (CRAB) method [45, 49]. Important challenges include increasing the speed of algorithms, broadening the base of controllability research and to integrate these techniques with a broader base of platforms.

Quantum optimal control is standing on the shoulders of its early applications in standard nuclear magnetic resonance (NMR) spectroscopy and atomic physics. They have pioneered standardisation and software packages and currently pursue robust ensemble control as a central goal, which is also important for maturing second-generation QT as many of the challenges in quantum sensing and computing are closely related [48].

Successful implementation of QT needs to be carried out with sufficient accuracy, despite imperfections and potentially detrimental effects of the surroundings. Quantum optimal control toolboxes allow to identify the performance limits for a given device implementation and show how to reach those limits of operation. In order to obtain these results, the quantum optimal control methodology has been adapted to the requirements of QT, specifically including open system effects and optimising for quantities like entanglement capabilities directly. They were adapted to nonlinear dynamics as found in BECs.

Quantum optimal control is related to information theory. It provides a practical means to explore decoherence-free subspaces or other noise-avoiding strategies as well as cooling schemes needed, e.g. to motionally cool levitating superconducting spheres. It is also related to quantum engineering by providing a solid mathematical framework for some engineering tasks. These include control of open systems and coherence control such as enhancing the lifetime of quantum memories by dissipative state engineering. More globally,

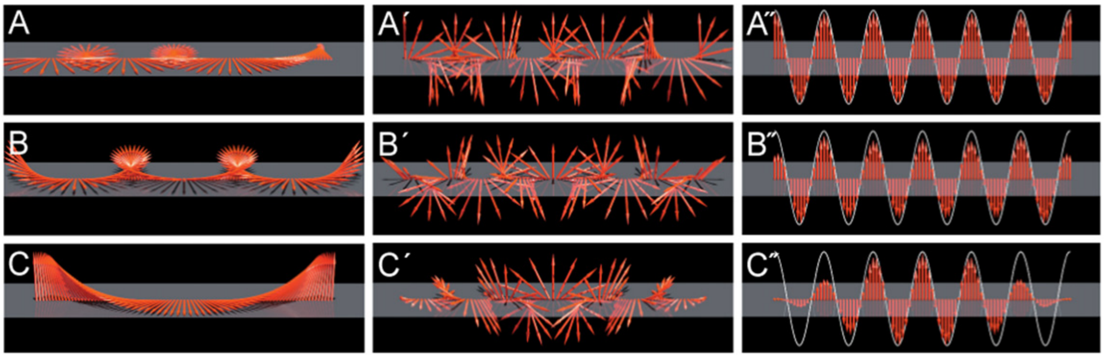

Figure 6. Offset-dependence of the Bloch vector during the course of a Ramsey experiment using three different pulse sequences with the same maximum amplitudes: (A)–(A″) concurrently optimised broadband excitation and flip-back pulses that cancel each other's imperfections in a cooperative fashion, (B)–(B″) individually optimised broadband pulses of the same duration, and (C)–(C″) standard rectangular pulses. The offset-dependent orientation of the Bloch vector is shown after the excitation pulse (left panels) and after a delay followed by a flip-back pulse (centre panels). The right panels show the corresponding *z* component of the final Bloch vector and the white curves represent the desired ideal Ramsey fringe pattern (adapted from Braun and Glaser 2014 *New J. Phys.* **16** 115002).

both together aim at the convergence of optimal control and experimentation including calibration uncertainties and other constraints.

Advances in science and technology needed to meet future challenges. A key family of mid-term challenges to optimal control is to improve and reach convergence between theory and experiment in more platforms than previously. With this, 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.

In the long run, when scaling quantum technology, control needs to scale with it. Meeting this challenge is necessary for proper functioning in a world that is only partially quantum. Next to finding these controls, benchmarking their success will be of nearly equal importance.

Applications in quantum communication. Quantum communication connects to quantum optimal control mostly at the light–matter interface. Currently, many proposals for transport as well as photon storage were made. Going forward, quantum control will develop into schemes to stabilise networks with feedback and optimise interconversion between stationary and flying qubits.

Applications in quantum computation. The ongoing theme here is the optimal design of powerful gates and state preparation schemes. Single-qubit gates were made robust against frequency crowding and slow fluctuations, even in complex Hilbert spaces and control schemes were constructed that make active use of environmental degrees of freedom. This needs to be driven towards robustness even in multi-qubit architectures and to the case of large inhomogeneity as common in semiconductor spin qubits. Going to optimal two-qubit gates, optimal control helps finding faster strategies solving the platform-specific challenges of high fidelity, error correction, long-distance entanglement, and robustness. Optimal control also needs to improve performance of qubit measurement and reset. Speeding up gates and combinations of gates and transport will remain a challenge. With promising starts in closed-loop fine tuning in superconducting qubits, the automation of control design and its integration with error correction as processors are scaled needs to be further developed. In the long run, optimal control is a crucial ingredient for quantum compilers and a scalable language for the assembly of elementary or complex gates in multi-qubit systems. Next to the gate-based model of quantum computing, quantum optimal control proposals for preparing cluster states have been made and can be extended.

Applications in quantum simulation. Quantum simulation is proving to be a flexible and inspiring field for applications of quantum optimal control, e.g. in the platform for quantum simulation in optical lattices. There, it has contributed to improved loading of atoms and found serendipitous solutions for local control. This should be broadened into the optimal and robust creation of more complex entangled states both for this and for other simulation platforms. They can be taken out of equilibrium to help study the emergence of thermodynamic laws, e.g. for spin systems, proposals for preparation of many-body entangled non-classical states were made.

For quantum simulation as special purpose quantum computing, optimal control helps explore fidelity limits in the presence of noise, both Markovian and non-Markovian as it occurs, e.g., in collision models. It will be used to keep control and operation fidelity high during the aggressive scaling anticipated in simulation and in the long-run be pivotal in verifying and validating simulations that are performed without or with limited error correction.

Applications in quantum sensing. Starting from its foundation in NMR, see above, quantum optimal control is naturally applied to quantum sensing. For example, the concurrent optimisation of pulses with the ability to cancel each other's imperfections was demonstrated to yield ultra-broadband Ramsey experiments (see figure 6).

Protocols for sensing using spins of NV centres in diamond were already developed and are expected to be further improved to protect from noise while enhancing the signal both by improving decoupling and preparing squeezed states. Non-classical states are a key ingredient to sensing and were also proposed for BECs [41] and photons in a cavity. A further application challenge in optimal control for sensing is to use feedback and adaptive settings for extracting phases and other parameters in the best way possible.

Conclusion. The long-term goal of quantum optimal control for QT is to gain a thorough understanding of optimal solutions and 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.

We thank the many members of the community who have contributed to the content of this article.

7. Quantum software and theory

Antonio Acín[1,2], *Harry Buhrman*[3]
[1]ICFO-Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, E-08860 Castelldefels (Barcelona), Spain
[2]ICREA, Passeig de Ll. Campanys, 23, E-08010 Barcelona, Spain
[3]QuSoft, CWI, and University of Amsterdam, Sciencepark 123 1098 XG, Amsterdam, The Netherlands

Introduction. Computers connected through networks, as we know them today, have changed modern society fundamentally, but their development is far from over. In fact, we are just starting to harness the laws of quantum physics to process information in unprecedented ways. Since the development of the first quantum algorithms and protocols there has also been steady and impressive progress on the hardware side, delivering quantum systems with a small number (<20) of qubits and quantum networks ranging over several hundreds of kilometres. With this progress, the need for quantum software and theory to exploit these novel QT, understanding their power but also their limitations, becomes more and more urgent. In the following sections, we highlight the current status and future challenges of this theoretical effort structured along three main research directions: quantum software for computing, quantum software for networks and theory.

Current status

Quantum software for computing. Quantum algorithms are fundamentally different from their classical counterparts because qubits can be in a superposition of 0 and 1. This means that with n qubits one can potentially perform exponentially many (2^n), computations in parallel. However, it is difficult to extract the answer from such a superposition as observing the system collapses it. This is where quantum software is needed. Shor showed in 1994 [50] that numbers can be factored more efficiently by QCs, an immensely important discovery given that the security of many modern cryptographic protocols (such as RSA) are based on the assumption that factoring large integers is a computationally hard task. Other algorithms were developed for a wide range of problems such as for example searching, sorting and many other applications [51]. One of the first practical applications of QCs may be quantum simulation [52], as even modest devices have the potential to perform simulations that would be infeasible with classical computers. There exist physical systems in which the interactions necessary for simulation can be engineered without the need for a full QC. With 100–150 logical qubits, molecular energies can be computed to great precision and accuracy, far exceeding the limitations of classical computers. Carrying out coherent quantum operations despite noise is a key challenge. Active strategies (error-correcting codes [53]) as well as passive ones (error-avoiding codes) have been introduced. Recent developments have reduced the noise threshold estimate for quantum error correction by several orders of magnitude. Topological quantum computation encodes quantum states and gates in global, delocalised properties of the hardware medium, which are more immune to all forms of noise that do not impact the entire medium at once and coherently. Protocols for the certification of correct quantum computation become essential in all these setups. Methods to test arbitrary computations with little overhead have been proposed, as well as other approaches to test QCs based on interactive-proof systems. On the other hand, new algorithms for the efficient simulation of quantum models have been developed, for instance based on tensor-network techniques. Finally, different architectures for quantum computation have been proposed, such as the gate or circuit model, adiabatic quantum computing, and quantum cellular automata, among others.

Quantum software for networks. Just as quantum algorithms can lead to an exponential speed-up for computational problems, quantum communication can lead to exponential savings in the number of (qu)bits that must be transmitted to solve distributed problems [54]. Some of these protocols have already been implemented, such as the quantum-fingerprinting scheme and the vector in a subspace problem. Cryptographic protocols also take place on networks and quantum resources allow, for certain problems, security guarantees that are impossible to achieve classically. QKD [55], for instance, allows two mutually trusting parties to generate a shared secret key. QKD systems are already commercially available. Cryptographic tasks where the sender and receiver do not trust each other require additional assumptions, limiting the adversary's computational or physical power. In the first case, there are quantum proposals for quantum cloud computation (blind computation), quantum money, and position-based cryptography. Limiting the adversary's physical power, i.e. amounts of quantum memory or entanglement or guaranteed space-like separation between participants, leads to a broad range of protocols which are easy to implement on existing hardware. Another line of research is quantum-safe or post-quantum cryptography where protocols are proven to be secure based on the hardness of certain problems, such as lattice problems. To make optimal use of quantum networks it is required to understand how to distribute quantum resources over them. Recently, there have been a few breakthroughs with respect to the non-additivity of quantum and classical information capacity and the key problem of identifying information capacities has been solved for a significant subset of channels. Protocols for entanglement distribution are necessary for long-distance quantum communication and the vision of a quantum internet [56]. As for computation, certification methods have also been introduced in the context of networks, for instance to certify the presence of entangled states or the security of quantum channels.

Quantum information theory. As its classical counterpart, quantum information theory aims at identifying the laws and the ultimate limits governing any information process based on quantum effects. Theoretical frameworks known as resource theories have been developed to understand quantum resources, such as entanglement [57], non-locality [58], quantum randomness or secret bits. Efficient strategies to estimate relevant quantum properties have also been designed. From a fundamental perspective, these concepts have been applied to understand what makes quantum physics special, devise novel no-go theorems for classical simulation of quantum physics or the quantum-vs-classical transition, also necessary to understand decoherence. Finally, quantum information concepts have successfully been applied to other domains in science, such as many-body physics [59], quantum chemistry and biology, quantum thermodynamics, quantum gravity, high-energy physics and even to solve open problems in classical information and computation theory.

Advances in science and technology needed to meet future challenges

Quantum software for computing. A constant challenge in this field is to find new quantum algorithms that outperform the best classical algorithms. However, quantum algorithms cannot yield an advantage for every problem; in fact, they usually do not, and understanding also these limitations will be critical, for instance in developing quantum-resistant classical and quantum cryptography, or to derive no-go theorems for quantum computation, see for instance [60]. Most of the existing algorithms do not make reference to any specific implementation and often cannot be implemented on the 50–100 qubit platforms available in the medium term. In the coming years, new algorithms and applications will be developed for these small platforms with a limited number of qubits where classical simulation is impossible, aiming at demonstrating ‘quantum supremacy’. In this direction, it is important to understand how these medium-size quantum processors can be used to simulate systems of physical relevance, for example in quantum chemistry, material science or high-energy physics. Assessing the impact of errors on computation quality remains a challenge and will require more efforts. In standard computation, new schemes for error correction and fault-tolerant computation, including ideas from topological quantum computation, need to be designed so that the level of noise that can be tolerated under realistic error models in near-future quantum systems is increased. In simulation, the impact of errors needs to be understood: while a single error in a QC without error correction is fatal, a small error in, say, a measurement of conductivity is less critical. Certifying a given quantum computation when a classical simulation is impossible represents another challenge and here improved algorithms for the classical simulation of quantum processes will be essential. Finally, first steps in extending machine learning and artificial intelligence applications to the quantum realm have taken place and it is expected that more algorithms will be designed in the next years. In a longer term, efforts will also have to devote to create a proper software toolchain for QCs including different layers of abstraction and tools, an essential step for an optimal use of resources [61].

Quantum software for networks. Finding new protocols for distributed computation also remains a challenge. For that, we need to understand the power that the entanglement-assisted communication model offers. Here, it will be again important to understand how to adapt existing or design new protocols for the near-future implementations. Concerning QKD, the development of device-independent techniques is essential to design implementations robust against existing hacking attacks. A major theoretical, and also experimental, challenge is to make these proposals practical. Recently, loophole free Bell tests have been achieved, but further work is required to speed up the rate at which we could hope to generate a key in QKD. It is also important to extend cryptographic applications beyond QKD. Improvements should be expected in the design for protocols involving non-trusted parties, which usually require computational or physical assumptions. In general, limiting the adversary’s physical power, i.e. amounts of quantum memory or entanglement or computational power, will lead to a broad range of protocols which are easy to implement on existing or near-future hardware. Remaining challenges include more complicated tasks such as secure identification. We also expect more efficient protocols for post-quantum cryptography. Finally, more work is needed to optimise the quantum resources for communication over quantum networks. Further investigation is needed to identify similarities and differences between classical and quantum network theory, and to consider practical constraints like channel uncertainty, finite block size, and limited entanglement.

Quantum information theory. To understand the full power of quantum effects, instrumental theories for quantum information resources, such as number of qubits, entanglement, various aspects of secrecy, study of randomness or channel capacities will need to be developed. Assessing the successful implementation of quantum protocols will require the design of efficient and scalable methods for the estimation, detection and certification of quantum properties. We also expect quantum information concepts and techniques to have impact on other research fields. A quantitative theory of entanglement could provide new insights into the exact structure of correlations of many-body systems, possibly leading to new algorithms for their simulation. This may lead to the identification of novel phases of matter from a quantum information perspective and for quantum information purposes. The role of quantum coherences in biological and thermodynamic processes also requires further investigation.

We expect that some important headway will be made by the challenges and milestones above within the next five years. In particular implementations on small quantum systems as they become available. Also new schemes for error correction and fault-tolerance amenable to such small systems. With additional manpower and new insights, it is also expected that new quantum algorithms will be developed within the next 5 years.

Conclusion. Software, protocols, and quantum information theory are essential for an optimal development of QT. Until now, most of the effort has focused on identifying the ultimate limits for quantum information processing. In the next 5–10 years, a parallel effort will be devoted to understand what can be done with the first generations of small quantum processors, identifying for instance quantum computation protocols whose classical simulation is infeasible or realisation of protocols with unprecedented levels of security. In the long term, these two efforts are expected to converge, providing the tools to attain the ultimate limits for quantum information processing with the, by then, existing technologies.

We thank the many members of the community who have contributed to the content of this article, in particular I Cirac, M Troyer, S Wehner, R Werner, A Winter, and M Wolf.

ORCID iDs

Daniel Esteve https://orcid.org/0000-0003-4089-4582

References

[1] http://tinyurl.com/qt-hlsc-report
[2] http://qurope.eu/h2020/qtflagship/roadmap2016
[3] Korzh B, Lim C C W, Houlmann R, Gisin N, Li M J, Nolan D, Sanguinetti B, Thew R and Zbinden H 2015 Provably secure and practical quantum key distribution over 307 km of optical fibre *Nat. Photon.* **9** 163
[4] Fröhlich B, Dynes J F, Lucamarini M, Sharpe A W, Yuan Z and Shields A J 2013 A quantum access network *Nature* **501** 69
[5] Scheidl T, Wille E and Ursin R 2013 Quantum optics experiments using the international space station: a proposal *New J. Phys.* **15** 043008
[6] Sangouard N, Simon C, de Riedmatten H and Gisin N 2011 Quantum repeaters based on atomic ensembles and linear optics *Rev. Mod. Phys.* **83** 33
[7] Bussières F, Sangouard N, Afzelius M, de Riedmatten H, Simon C and Tittel W 2013 Prospective applications of optical quantum memories *J. Mod. Phys.* **60** 1519
[8] Buchmann J A, Braun J, Demirel D and Geihs M 2017 Quantum cryptography: a view from classical cryptography *Quantum Sci. Technol.* **2** 020502
[9] Acín A and Masanes L 2016 Certified randomness in quantum physics *Nature* **540** 213
[10] Blatt R and Wineland D J 2008 Entangled states of trapped atomic ions *Nature* **453** 1008
[11] Monroe C and Kim J 2013 Scaling the ion trap quantum processor *Science* **339** 1164
[12] Home J P *et al* 2009 Complete methods set for scalable ion trap quantum information processing *Science* **325** 1227
[13] Nakamura Y, Pashkin Y A and Tsai J S 1999 Coherent control of macroscopic quantum states in a single-cooper-pair box *Nature* **398** 786
[14] Devoret M and Schoelkopf R J 2013 Superconducting circuits for quantum information: an outlook *Science* **339** 1169
[15] Watson T F *et al* 2018 A programmable two-qubit quantum processor in silicon *Nature* **555** 633–7
[16] Tosi G *et al* 2017 Silicon quantum processor with robust long-distance qubit couplings *Nat. Commun.* **8** 450
[17] Waldherr G *et al* 2014 Quantum error correction in a solid-state hybrid spin register *Nature* **506** 204–7
[18] Meany T *et al* 2016 Engineering integrated photonics for heralded quantum gates *Sci. Rep.* **6** 25126
[19] Yoshikawa J-I *et al* 2016 Generation of one-million-mode continuous-variable cluster state by unlimited time-domain multiplexing *APL Photon.* **1** 060801
[20] Feynman R 1982 Simulating physics with computers *Int. J. Theor. Phys.* **21** 467
[21] Lloyd S 1996 universal quantum simulators *Science* **273** 1073–8
[22] Bloch I, Dalibard J and Nascimbène S 2012 Quantum simulation with ultracold atomic gases *Nat. Phys.* **8** 267
[23] Blatt R and Roos C F 2012 Quantum simulation with trapped ions *Nat. Phys.* **8** 277
[24] Trotzky S *et al* 2012 Probing the relaxation towards equilibrium in an isolated strongly correlated 1D Bose gas *Nat. Phys.* **8** 325
[25] Eisert J, Friesdorf M and Gogolin C 2015 Quantum many-body systems out of equilibrium *Nat. Phys.* **11** 124
[26] Lewenstein M, Sanpera A and Ahufinger V 2012 *Ultracold Atoms in Optical Lattices: Simulating Quantum Many-body Systems* (Oxford: Oxford University Press)
[27] Georgescu I *et al* 2014 Quantum simulation *Rev. Mod. Phys.* **86** 153
[28] Albash T, Rønnow T F, Troyer M and Lidar D A 2015 Reexamining classical and quantum models for the D-wave one processor *Eur. Phys. J. Spec. Top.* **224** 111
[29] Vahlbruch H, Mehmet M, Danzmann K and Schnabel R 2016 Detection of 15 dB squeezed states of light and their application for the absolute calibration of photoelectric quantum efficiency *Phys. Rev. Lett.* **117** 110801
[30] Kacprowicz M, Demkowicz-Dobrzański R, Wasilewski W, Banaszek K and Walmsley I A 2010 Experimental quantum-enhanced estimation of a lossy phase shift *Nat. Photon.* **4** 357–60
[31] Slussarenko S, Weston M M, Chrzanowski H M, Shalm L K, Verma V B, Nam S W and Pryde G J 2017 Unconditional violation of the shot-noise limit in photonic quantum metrology *Nat. Photon.* **11** 700–3
[32] Ono T, Okamoto R and Takeuchi S 2013 An entanglement-enhanced microscope *Nat. Commun.* **4** 2426
[33] Chua S S Y, Slagmolen B J J, Shaddock D A and McClelland D E 2014 Quantum squeezed light in gravitational-wave detectors *Class. Quantum Grav.* **31** 18
[34] Taylor M A *et al* 2013 Biological measurement beyond the quantum limit *Nat. Photon.* **7** 229
[35] Degen C L, Reinhard F and Cappellaro P 2017 Quantum sensing *Rev. Mod. Phys.* **89** 035002
[36] Pezzè L, Smerzi A, Oberthaler M K, Schmied R and Treutlein P 2016 Non-classical states of atomic ensembles: fundamentals and applications in quantum metrology arXiv:1609.01609
[37] Ludlow A D, Martin M B, Jun Y, Peik E and Schmidt P O 2015 Optical atomic clocks *Rev. Mod. Phys.* **87** 637–701
[38] Balasubramanian G *et al* 2008 Nanoscale imaging magnetometry with diamond spins under ambient conditions *Nature* **455** 648
[39] Aspelmeyer M, Kippenberg T J and Marquardt F 2014 Cavity optomechanics *Rev. Mod. Phys.* **86** 1391
[40] Wolfgramm F, Vitelli C, Beduini F A, Godbout N and Mitchell M W 2013 Entanglement-enhanced probing of a delicate material system *Nat. Photon.* **7** 28
[41] van Frank S, Negretti A, Berrada T, Bücker R, Montangero S, Schaff J-F, Schumm T, Calarco T and Schmiedmayer J 2014 Interferometry with non-classical motional states of a Bose–Einstein condensate *Nat. Commun.* **5** 4009
[42] Glaser S J *et al* 2015 Training Schrödinger's cat: quantum optimal control, strategic report on current status, visions and goals for research in Europe *Eur. Phys. J.* D **69** 1–24
[43] Gough J and James M R 2009 Quantum feedback networks: Hamiltonian formulation *Commun. Math. Phys.* **287** 1109–32
[44] Khaneja N, Reiss T, Kehlet C, Schulte-Herbrüggen T and Glaser S J 2005 Optimal control of coupled spin dynamics: design of NMR pulse sequences by gradient ascent algorithms *J. Magn. Reson.* **172** 296
[45] Doria P, Calarco T and Montangero S 2011 Optimal control technique for many-body quantum dynamics *Phys. Rev. Lett.* **106** 190501
[46] Reich D, Ndong M and Koch C P 2012 Monotonically convergent optimization in quantum control using Krotov's method *J. Chem. Phys.* **136** 104103

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

[48] Dolde F *et al* 2014 High-fidelity spin entanglement using optimal control *Nat. Commun.* **5** 3371

[49] Egger D J and Wilhelm F K 2014 Adaptive hybrid optimal quantum control for imprecisely characterized systems *Phys. Rev. Lett.* **112** 240503

[50] Shor P W 1994 Algorithms for quantum computation, discrete log and factoring *35th FOCS* p 124

[51] Montanaro A 2016 Quantum algorithms: an overview *npj Quantum Inf.* **2** 15023

[52] Trabesinger A 2012 Quantum simulation *Nat. Phys.* **8** 263

[53] Lidar D and Brun T 2013 *Quantum Error Correction* (Cambridge: Cambridge University Press)

[54] Buhrman H, Cleve R, Massar S and de Wolf R 2010 Nonlocality and communication complexity *Rev. Mod. Phys.* **82** 665

[55] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing (Bangalore)* p 175

[56] Kimble J 2008 The quantum internet *Nature* **453** 1023

[57] Horodecki R, Horodecki P, Horodecki M and Horodecki K 2009 Quantum entanglement *Rev. Mod. Phys.* **81** 865

[58] Brunner N, Cavalcanti D, Pironio S, Scarani V and Wehner S 2014 Bell nonlocality *Rev. Mod. Phys.* **86** 419

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

[60] Svore K M and Troyer M 2016 The quantum future of computation *Computer* **49** 21

[61] Chong F T, Franklin D and Martonosi M 2017 Programming languages and compiler design for realistic quantum hardware *Nature* **549** 180