Appl. Phys. B (2016) 122:130
DOI 10.1007/s00340-016-6353-8

Applied Physics B
Lasers and Optics

Quantum technology: from research to application

Wolfgang P. Schleich[1] · Kedar S. Ranade[1] · Christian Anton[2] · Markus Arndt[3] · Markus Aspelmeyer[4] · Manfred Bayer[5] · Gunnar Berg[6] · Tommaso Calarco[7] · Harald Fuchs[8] · Elisabeth Giacobino[9] · Markus Grassl[10] · Peter Hänggi[11] · Wolfgang M. Heckl[12] · Ingolf-Volker Hertel[13] · Susana Huelga[14] · Fedor Jelezko[15] · Bernhard Keimer[16] · Jörg P. Kotthaus[17] · Gerd Leuchs[10] · Norbert Lütkenhaus[18] · Ueli Maurer[19] · Tilman Pfau[20] · Martin B. Plenio[14] · Ernst Maria Rasel[21] · Ortwin Renn[22] · Christine Silberhorn[23] · Jörg Schiedmayer[24] · Doris Schmitt-Landsiedel[25] · Kurt Schönhammer[26] · Alexey Ustinov[27] · Philip Walther[28] · Harald Weinfurter[29] · Emo Welzl[19] · Roland Wiesendanger[30] · Stefan Wolf[31] · Anton Zeilinger[4] · Peter Zoller[32]

Received: 29 January 2016 / Accepted: 1 February 2016

Abstract The term quantum physics refers to the phenomena and characteristics of atomic and subatomic systems which cannot be explained by classical physics. Quantum physics has had a long tradition in Germany, going back nearly 100 years. Quantum physics is the foundation of many modern technologies. The first generation of quantum technology provides the basis for key areas such as semiconductor and laser technology. The "new" quantum technology, based on influencing individual quantum systems, has been the subject of research for about the last 20 years. Quantum technology has great economic potential due to its extensive research programs conducted in specialized quantum technology centres throughout the world. To be a viable and active participant in the economic potential of this field, the research infrastructure in Germany should be improved to facilitate more investigations in quantum technology research.

Table of Contents

The following article is the re-publication of a text of previously published under the German National Academy of Sciences Leopoldina, acatech (the National Academy of Science and Engineering), the Union of the German Academies of Science and Humanities (ed.) (2015): Quantum Technology: From research to application. Halle (Saale), 64 pages. **ISBN**: 978-3-8047-3343-5. The German National Library lists this publication in the German National Bibliography; detailed bibliographic information can be accessed online at http://dnb.d-nb.de.

This paper is part of the topical collection "Quantum Repeaters: From Components to Strategies" guest edited by Manfred Bayer, Christoph Becher and Peter van Loock.

✉ Christian Anton
christian.anton@leopoldina.org

1 Institut für Quantenphysik, Universität Ulm, 89069 Ulm, Germany

2 Department Science-Policy-Society, German National Academy of Sciences Leopoldina, Jägerberg 1, 06108 Halle, Germany

3 Faculty of Physics, VCQ & QuNaBioS, University of Vienna, Boltzmanngasse 5, 1090 Vienna, Austria

4 Vienna Center for Quantum Science and Technology (VCQ), Faculty of Physics, University of Vienna, 1090 Vienna, Austria

5 Experimentelle Physik 2, Technische Universität Dortmund, 44227 Dortmund, Germany

6 Institut für Physik, Martin-Luther-Universität Halle-Wittenberg, 006120 Halle, Germany

7 Institut für Komplexe Quantensysteme, Universität Ulm, 89069 Ulm, Germany

8 Physikalisches Institut, Westfälische Wilhelms-Universität Münster, Wilhelm-Klemm Str. 10, 48149 Münster, Germany

9 Université de Paris, Paris, France

10 Max Planck Institute for the Science of Light, 91058 Erlangen, Germany

[11] Institut für Physik, Universität Augsburg, Universitätsstr. 1, 86135 Augsburg, Germany

[12] Oskar-von-Miller Lehrstuhl für Wissenschaftskommunikation, School of Education & Physik Department, Technische Universität München, c/o Deutsches Museum, Museumsinsel 1, 80538 Munich, Germany

[13] Max-Born-Institut (MBI), im Forschungsverbund Berlin e.V, Max-Born-Institut Max-Born-Straße 2A, 12489 Berlin, Germany

[14] Institute of Theoretical Physics, Universität Ulm, Albert-Einstein-Allee 11, 89069 Ulm, Germany

[15] Institut für Quantenoptik, Universität Ulm, Albert-Einstein-Allee 11, 89081 Ulm, Germany

[16] Max-Planck-Institut für Festkörperforschung, Heisenbergstraße 1, 70569 Stuttgart, Germany

[17] Fakultät für Physik and Center for NanoScience (CeNS), Ludwig-Maximilians-Universität, Geschwister-Scholl-Platz 1, 80539 Munich, Germany

[18] Institute for Quantum Computing and Department of Physics & Astronomy, University of Waterloo, Waterloo, Canada

[19] Department of Computer Science, ETH Zurich, Zurich, Switzerland

[20] Physikalisches Institut and Center for Integrated Quantum Science and Technology, Universität Stuttgart, Pfaffenwaldring 57, 70550 Stuttgart, Germany

[21] Institut für Quantenoptik, Leibniz-Universität Hannover, Welfengarten 1, 30167 Hannover, Germany

[22] Institut für Sozialwissenschaften, Universität Stuttgart, Seidenstr. 36, 70174 Stuttgart, Germany

[23] Applied Physics, University of Paderborn, Warburger Strasse 100, 33098 Paderborn, Germany

[24] Vienna Center for Quantum Science and Technology, Atominstitut, TU Wien, Stadionallee 2, 1020 Vienna, Austria

[25] Lehrstuhl für Technische Elektronik, Technische Universität München, Arcisstr. 21, 80333 Munich, Germany

[26] Institut für Theoretische Physik, Georg-August-Universität Göttingen, Friedrich-Hund-Platz 1, 37077 Göttingen, Germany

[27] Physikalisches Institut, Karlsruhe Institute of Technology, 76131 Karlsruhe, Germany

[28] Faculty of Physics, University of Vienna, Boltzmanngasse 5, 1090 Vienna, Austria

[29] Faculty of Physics, Ludwig-Maximilians-Universität, 80799 Munich, Germany

[30] Department of Physics, University of Hamburg, Jungiusstraße 11, 20355 Hamburg, Germany

[31] Faculty of Informatics, Universita della Svizzera Italiana, Via G. Buffi 13, 6900 Lugano, Switzerland

[32] Institute for Theoretical Physics, University of Innsbruck, 6020 Innsbruck, Austria

1 Foreword

Quantum technology is a relatively new and very interdisciplinary field of research and development but one that has had a long tradition in Germany. A greater integration of basic research, development and application in this area could open up promising scientific and business opportunities, particularly in Germany.

While quantum physics and quantum technology undoubtedly pose great challenges in its scientific communication, the authors of this report have succeeded in making the basic physical phenomena underlying the new generation of quantum technology comprehensible to non-specialists so that they too can gain a good overview of the future prospects for this field of research.

We hope that this report will draw attention to the enormous innovation potential of quantum technology. With this in mind, we would like to encourage new ways of promoting this field of research and development. A close collaboration between the various disciplines can unfold new dynamic innovations and pave the way to application and industrial implementation.

The report is divided into two parts. Section 2 presents the scientific foundations of quantum technology, an overview of the research area and its fields of application and outlines ways in which the use of quantum physics effects can be exploited. Section 3 explains the individual areas of research in detail.

We would like to thank all those involved with the working group and the reviewers very much for their contributions to this report.

Halle (Saale) and Berlin, Germany, June 2015

2 Section A: Future of quantum technology

2.1 Introduction

Key summary

- The term quantum physics refers to the phenomena and characteristics of atomic and subatomic systems which cannot be explained by classical physics. Quantum physics has had a long tradition in Germany, going back nearly 100 years.
- Quantum physics is the foundation of many modern technologies. The first generation of quantum technology provides the basis for key areas such as semiconductor and laser technology.
- The “new” quantum technology, based on influencing individual quantum systems, has been the subject of research for about the last 20 years.
- Quantum technology has great economic potential due to its extensive research programs conducted in specialized quantum technology centres throughout the world. To be a viable and active participant in the economic potential of this field, the research infrastructure in Germany should be improved to facilitate more investigations in quantum technology research.

Those involved with quantum technology and their basic physical principles quickly come up against considerable challenges.

Quantum physical effects do not directly correspond to our experience of daily life. It is difficult to comprehend that a particle can take two different paths if not observed in the interim and that the two particles, millions of light-years apart, can behave in the same way as if they were somehow linked by an invisible connection.

These phenomena have long been the subject of puzzlement in physics and have led to intensive debate, so it is to be expected that this report will prove challenging to many readers. Our objective is to demonstrate that it is worth considering the phenomenon of quantum physics and the technologies based on them as they are part of an already emerging field of specific applications and, in other areas, have the potential to substantially improve on current technological solutions.

	Prof. Dr. Reinhard F. Hüttl	*Prof. Dr. Günter Stock*
President	President	President
German National Academy of Sciences Leopoldina	acatech – National Academy of Science and Engineering	Union of the German Academies of Science and Humnities

In recent decades, quantum technology has become established as a new field of research that, building on the research results from physics, mathematics and computer science, has resulted in a wealth of new ideas and concepts for technical applications.

The insights of quantum physics are the foundation of quantum technology. These insights comprise all theories and formal theoretical concepts and their interpretations formulated to describe atomic and subatomic systems, which form the basis for solid state physics and the physics of atoms and molecules as well as theoretical chemistry among other things.

Without quantum physics many discoveries and inventions of the past century would not have been possible because the principles of quantum mechanics play a key role in these. Among them are lasers, atomic clocks and satellite positioning (GPS) and in particular the entire field of electronics, including computers, the internet and mobile communications.

These technologies are also referred to as first generation quantum technology.

In recent years it has become clear that the use of further quantum mechanical effects, which go far beyond those principles used up to now, has opened up possibilities for a myriad of new technical applications. The first technical applications of the second generation of quantum technology are now being developed based on the findings of basic research.

This **new quantum technology** is the focus of this report.

One example of application is the reliable transmission of information, which is of central importance in our digital society. Data encryption using quantum cryptography could increase the security of data transmission, taking it to a completely new level. In April 2004, the first bank transfer using a protocol with quantum cryptography was made in Vienna.[1] Switzerland used quantum cryptography for the first time in its National Council elections in 2007 to secure networks for vote counting against tampering.[2]

Although there are already companies specializing in quantum cryptography in the UK (TOSHIBA Technologies, Cambridge), France (THALES and SeQureNet, Paris), Switzerland (idQuantique, Geneva) and the US (MagiQ Technologies, New York), there are currently no companies in Germany developing products based on quantum technology.

Quantum sensors capable of delivering more precise measurements of gravity in the Earth's magnetic field and rotation are also conceivable. Applications of quantum technology could be used in the search for raw materials or for earthquake prediction. Changes in the environment, such as a rise in sea level due to climate change, could be monitored with great accuracy using quantum sensors.

In listing these examples of application, it is clear that, at present, the discussion is comprised largely of the application possibilities. In contrast to many other fields of science, the scientific foundations for application of quantum technology are not yet entirely understood.

This is why some of the discussion later in this report may appear vague.

Research in new quantum technology is generally basic research, although individual applications are emerging or have already been developed on a laboratory scale. Nevertheless, Germany should not refrain from research and development in quantum technology not only because of its long-term technological potential (specific areas of application as described in Section 3) but also because of its impacts on related fields of no less importance, such as information and communication technology.

A number of quantum technology centres for basic research and technical applications have been established over the past few years in Canada, the US, Korea, Russia and Japan.[3] The innovation potential of quantum technology is also increasingly attracting the interest of private enterprise, primarily in the US.[4]

Germany has a long tradition of scientific work in quantum physics. Based on these traditional structures, research groups with various focal points have emerged in different regions of Germany in recent years. Some examples of such regional focus are:

- Munich and Erlangen in the field of quantum information;

[1] http://www.wissenschaft.de/technik-kommunikation/physik/-/journal_content/56/12054/1119998/Welt-weit-erste-quantenkryptografisch-verschl%C3%BCs-selte-Bank%C3%BCberweisung/ (last accessed: 17 February 2015).

[2] http://www.heise.de/tr/artikel/Photonen-als-Wahl-helfer-280423.html (last accessed: 17 February 2015).

[3] Among these is the Institute for Quantum Computing in Waterloo, Canada, with start-up funding of around CAD 300 million. It is currently the largest centre for quantum information worldwide. The Center for Quantum Technologies in Singapore has been part of the national university since 2007 and is being funded for 10 years with start-up financing of SGD 158 million. In the US, the Joint Quantum Institute was established with the joint financing by the National Institute of Standards and Technology (NIST) and the University of Maryland (College Park). It is also the sponsor for a start-up in South Korea, with which the Max Planck Institute is also involved. In Japan, quantum cryptography is supported by a consortium which includes Toshiba, Mitsubishi and Japanese Telecom. In the UK at present, €270 million are allocated by the Engineering and Physical Sciences Research Council for a program intended to support the application of technologies based on quantum physics.

[4] For example, former board members of Blackberry-RIM, Mike Lazaridis and Douglas Fregin, have established an investment fund of $100 million to support new businesses and spinoffs for quantum technology in Canada ("Quantum Valley"). In the US, the Quantum Wave Fund (http://qwcap.com, last accessed: 18 February 2015) is a venture capital company making targeted investments in quantum technology.

Fig. 1 A particle can take two paths simultaneously if it is not observed in the interim (Charles Addams, *The New Yorker*, 1940)

- Ulm and Stuttgart for integrated quantum sciences and technology;
- Berlin, Braunschweig, Bremen, Hamburg and Hanover for quantum sensor technology and metrology; and
- Aachen and Jülich in the field of quantum computing.

As a first step toward promoting greater collaboration, joint institutes, excellence initiatives and cooperation agreements have been established, among these the Center for Integrated Quantum Science and Technology (IQST) in Stuttgart and Ulm, the Hannover Institute of Technology (HITec) and the Center for Optical Quantum Technologies in Hamburg.

Supporting and expanding these regional research efforts and developing them into research centres with sustainable structures of international significance is an important task for the future. Moreover, in the medium and long term it will be important to initiate and support knowledge exchange and cooperation between research and industry.

Greater collaboration in many disciplines, particularly among engineering groups, could open up new prospects for the development of technology and production in Germany. Encouraging such greater collaboration and supporting the exchange of knowledge between science and business is another objective of this report.

This report explains the basic physical principles of quantum technology and outlines their potential for application and the scientific challenges involved. The focal points of current research are presented in Section 3 of the report ("Detailed Information").

2.2 Fundamentals of quantum technology

Key summary

- Quantum mechanics arose at the start of the twentieth century and was initially criticized because of its contradictions with conventional notions of physics. Today it is one of the undisputed foundations of physics.
- One typical characteristic of quantum mechanics is that a particle, such as an electron, can exhibit wave behaviour.
- Other important quantum effects subject to particular interest recently include superpositions, entanglement, uncertainty relations and many-body effects.
- Quantum technology widely used today includes semiconductors, lasers and satellite navigation. This first-generation quantum technology is based primarily on the quantum physics principle of coherence.
- Potential technologies of the second generation—the "new" quantum technology—are based on of the use of individual quantum systems, many-body effects and entanglement.

Alongside relativity theory, quantum physics has been one of the most important fields in physics since the twentieth century. Its findings have far-reaching effects on all fields of natural science and engineering, particularly in physics, chemistry, electrical engineering, information technology and medical technology, and increasingly in biology as well.

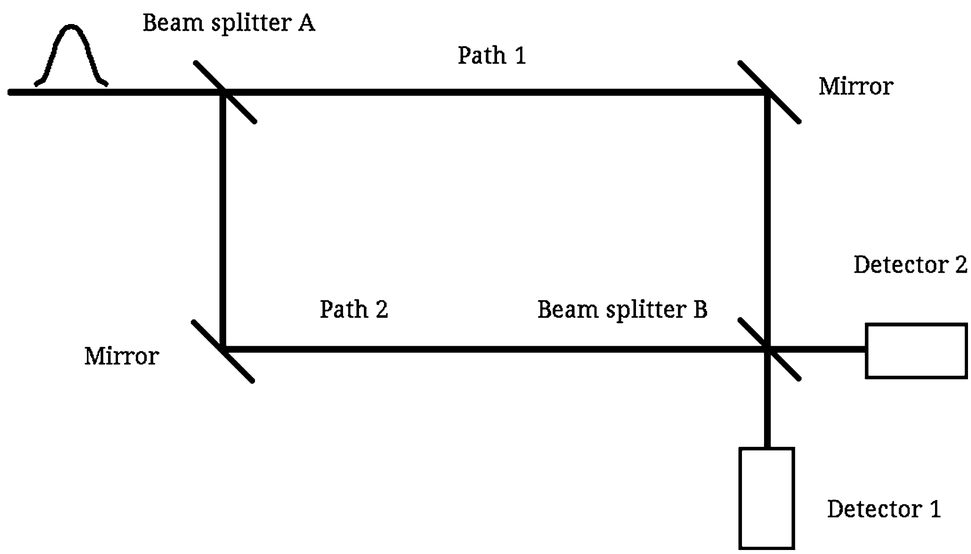

Fig. 2 In a doubleslit experiment, the photon can take two different paths at the beam splitter A. Depending on whether beam splitter B is used or removed, the wave or particle properties of the photon are measured

Important theoretical works since the beginning of the twentieth century that laid the foundation for the development of quantum mechanics are, in particular:

- Planck's explanation of the spectrum of an ideal black body (1900),
- Einstein's explanation of the photoelectric effect (1905),
- the Bohr–Sommerfeld atomic model (from 1913), the further development of which is a quantum mechanical model that forms the basis for our modern understanding of the structure of matter, and
- de Broglie's matter wave hypothesis (1924)

The actual development of quantum mechanics occurred in 1925 and in 1926 in two formulations which initially appeared to be very different: matrix mechanics[5] (Werner Heisenberg,[6] Max Born and Pascual Jordan) and wave mechanics[7] (Erwin Schrödinger). In early 1926, it seemed, for a short time, as if there were two very different systems to explain the atomic world. However, Schrödinger himself soon demonstrated the complete agreement of matrix and wave mechanics.[8] Quantum mechanics then continued to expand into the 1930s as an independent and coherent conceptual framework.

Even more than eight decades after this groundbreaking work, the lessons and principles of quantum mechanics are difficult for non-specialists to understand because they often have no analogies in the experience of daily life and are not perceptible to the human senses (see Fig. 1). On the other hand, these effects often provoke great fascination so they are often featured even in popular science media.

Science and technology is of ever greater use in the world of a micro-scale and nano-scale with the help of new instrument technology. Without quantum physics, many discoveries and inventions of the past century, such as transistors, lasers (see Highlight 1-1), atomic clocks and satellite positioning (GPS), would not have been possible.

Highlight 1-1: New technologies—The history of the laser

The development of lasers is an example of how the introduction of a new technology can secure a lasting competitive advantage. Trumpf introduced laser technology for industrial material processing in 1979. Later, the company used the disk laser developed by Adolf Giesen in 1994 at the University of Stuttgart to become a technology leader for lasers and a dominant player on the world market. This development was strongly facilitated by close cooperation with research institutes such as the Fraunhofer Institute for Laser Technology in Aachen and the University of Stuttgart laser technologies institute IFSW. This head start in knowledge of laser technology also brought about further innovation and new companies in Germany in production technology (such as laser material processing for joining, cutting and drilling), medical devices (such as optical coherence tomography and surgical methods using lasers) and measurement technology (such as laser rangefinders). These wide-ranging early advantages of knowledge in key areas such as laser technology continue to contribute to the long-term competitiveness of German industry.

Source: Grötker [7]

2.2.1 *Quantum physics as a scientific theory*

It was not just the descriptive difficulties of quantum mechanics that gave even the greatest physicists of the twentieth century headaches. The problem was also that it shook the foundations of classical mechanics and its entire view of the world. Thus, many physicists doubted, as was also the case with relativity theory, that it was in

[5] Born et al. [2].

[6] A further important advance in the understanding of the general structure of the Heisenberg approach was provided by Paul Dirac in 1925.

[7] Schrödinger [12].

[8] Schrödinger [13].

fact a correct description of nature. One of the best-known examples for this is a publication by Albert Einstein, Boris Podolsky and Nathan Rosen from 1935. The authors described a thought experiment, known today as the Einstein–Podolsky–Rosen paradox or EPR paradox for short. They considered a quantum mechanical system comprising of two adjacent particles, which are subsequently separated and sent in different directions. According to quantum mechanics, they form a single system regardless of their distance from one another, even if it is light years, and they have a fixed, total momentum as long as neither of the particles is disturbed. However, the distribution of the total momentum between the two particles has not yet been determined. Only when a measurement is performed on one particle is the system "compelled" to apply a distribution, so that the corresponding property is also immediately determined for the other particle. If, for example, the total momentum of the pair of particles is known, then measuring the momentum of one particle reveals the momentum of the other. Einstein, Podolsky and Rosen concluded from this that the momentum of the two particles must already be fixed prior to the measurement, because otherwise the particles, which are now far apart from one another, would have to communicate at more than the speed of light. The theory of relativity prohibits this, however, and Einstein spoke disparagingly of "spooky action at a distance"[9] in quantum mechanics.

"Hidden local variables" which define the outcome of such an experiment from the beginning were proposed as a possible solution to the paradox. In 1964, John Bell proposed an inequality which shows that the classical view in the form of a theory of hidden local variables satisfies certain conditions which are violated by quantum physics. It is possible to check this inequality by experiments and determine whether hidden local variables play a role or—as quantum mechanics assumes—not. Since the 1970s, physicists have performed increasingly refined experiments for this. Even if all questions have not been completely resolved, all the results so far support quantum mechanics and not, for example, the deliberations of Einstein. The test of this inequality is among the prerequisites for secure message transmission using quantum systems (quantum communication and quantum cryptography).

Thus, quantum mechanics is a theory which can correctly describe experiments from many different areas of physics both qualitatively and quantitatively.

Nearly all of modern physics rests directly or indirectly on its foundation.

[9] A. Einstein, B. Podolsky, N. Rosen "Can quantum-mechanical description be considered complete?", Physical Review, **47**, p. 777 [5].

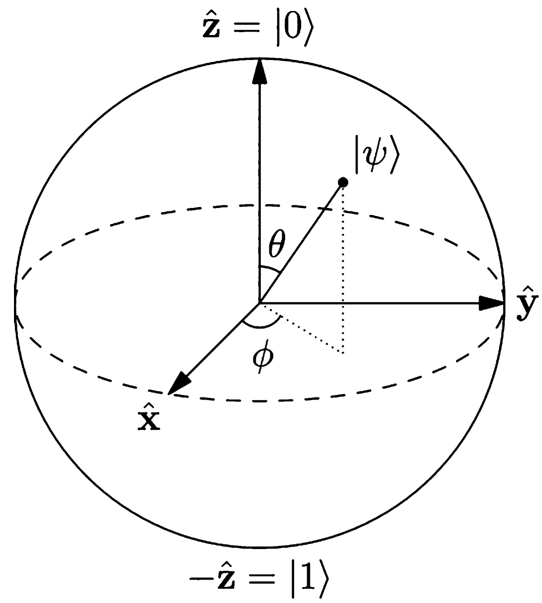

Fig. 3 On the three-dimensional Bloch sphere (with x-, y-, and z-axes) the north and south poles correspond to the two classical states, whereas a quantum state can be at any point on the surface of the sphere. The degree of superposition for a state |Ψ> from the classical states |0> and |1> on the z-axis is indicated by the polar angle θ, while the azimuthal angle ϕ describes the purely quantum mechanical phase. [Image source: Wikipedia/User: Smite-Meister (license: CC BY-SA 3.0)]

2.2.2 *Principles of quantum technology*

It is characteristic of quantum mechanics that a particle, such as an electron, can exhibit wave behaviour. The property of these waves to superimpose is referred to as "coherence" or "interference capacity".

In rough terms this can be understood as the "quantumness" of a system. This is lost if the system loses its interference capacity, which is referred to as "decoherence". However, in contrast to sound or water waves, this wave does not have a directly observable size without additional means, only the amplitude, i.e. the oscillation, can be measured, not the phase of the wave.

The combined nature of wave and particle or wave-particle dualism is well-demonstrated in doubleslit experiments (Fig. 2). In these, a single photon (particle of light) is passed through a beam splitter[10] and the two partial beams are directed to one point via two mirrors.

The observer can now decide whether or not to place a second beam splitter at the point of intersection at the back. In the first case, the superposition pattern of the two partial beams is measured, i.e. the wave properties of the photon. This set-up is also referred to as a Mach–Zehnder

[10] In this case, a semitransparent mirror, which partly allows a wave to pass and partly reflects it.

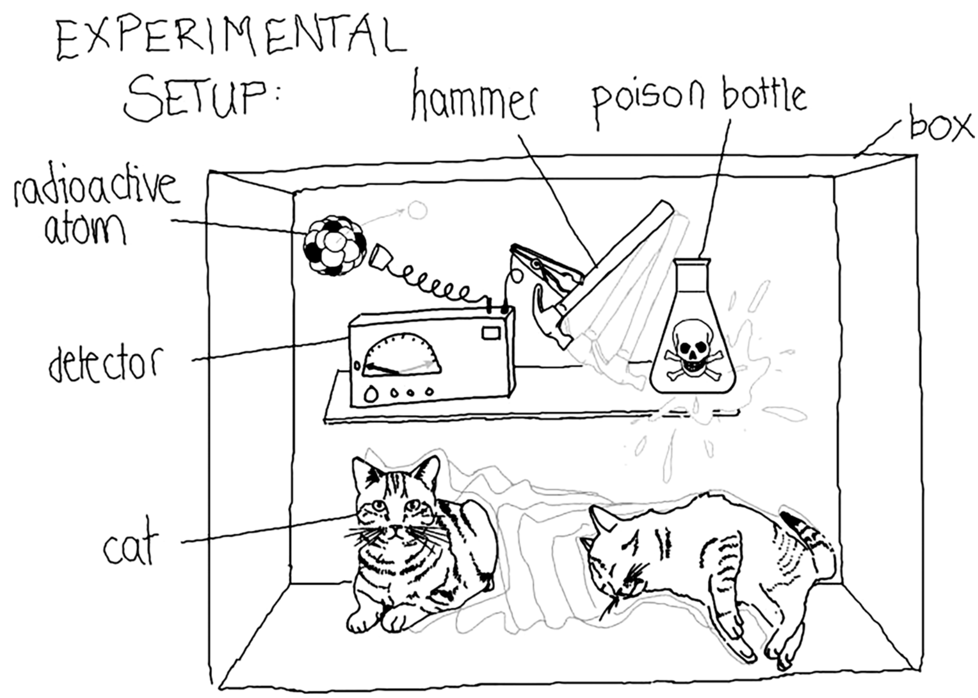

Fig. 4 Schrödinger's cat: prior to measurement, the cat is in a superposition of the states (1) live cat, non-decayed atomic nucleus and (2) dead cat, decayed atomic nucleus. (Diagram—Lara Hartjes, Ulm)

interferometer. In the second case, the observer determines which path the photon has taken at the first beam splitter, i.e. the particle property of the light; this setup is referred to as the Hanbury Brown and Twiss experiment.

Now the second beam splitter can also be placed in the beam's path after the photon has already passed through the first beam splitter. According to the incorrect classical assumption, the photon would already have had to "decide" upon a path. However, in fact, the interference of the photon with itself is obtained once again, which results from the superposition of the two partial waves, which is recognized after several runs with individual photons.

The following section briefly addresses four important phenomena of quantum mechanics: superpositions, entanglement, uncertainty relations and many-body effects. Today, quantum technology of the first generation already makes use of superposition states. In second-generation quantum technology, the use of entangled states and many-body states will assume greater importance.

2.2.2.1 Superpositions The state of a classical system is determined unambiguously, for example, a lamp is either lit or not. The lamp also assumes its state when not observed. The simplest systems have two possible states, "on" or "off", "0" or "1". Computer science refers to such binary conditions as a "bit". The quantum mechanical analogue to a bit, the quantum bit, or "qubit" for short, can also assume superposition states in addition to the states "0" and "1". For example, an individual particle could assume a state which can be referred to as 80 % "0" and 20 % "1". If one were now to produce many qubits in this state and determine the bit values, 80 % of the cases would be measured as "0" and 20 % as "1". In contrast to daily experience, in which the bit value of each individual bit is already fixed prior to measurement, in quantum mechanics this value is undefined and is assumed only in the course of measurement. What is important for the whole spectrum of quantum technology is the possibility to process such superpositions without making a measurement in the meantime.

The state can be illustrated using the Bloch sphere (Fig. 3), named after the physicist Felix Bloch. When it is compared with the globe of the Earth, the north and south poles correspond to the classical states "0" and "1" respectively, and all the points on the surface of the globe to the quantum mechanical superposed states.

The probabilities of measuring one of the two classical values are found by projecting the latitude on to the Earth's axis. The longitude at which the state is found indicates its phase. Though this is unimportant for measuring a bit value, it is important in quantum mechanics.

2.2.2.2 Entanglement The entanglement of objects is another phenomenon of quantum mechanics for which classical physics has no equivalent.

It results directly from the possibility of superposing states even in multi-particle systems. Entanglement was introduced in 1935 by the Austrian physicist Erwin Schrödinger, who responded to the EPR paradox mentioned above in a three-part article.

Entanglement can be illustrated with a thought experiment which has become known as "Schrödinger's cat" (Fig. 4). A cat is confined in a box containing a poison capsule. The capsule is connected to a detector, which is triggered if a specific, individual radioactive atomic nucleus decays. When this decay is detected, the poison is released, killing the cat.

In physical terms, the cat has two states: alive and dead. The same is true of the atomic nucleus: decayed and not decayed. The state of the cat and the state of the atomic nucleus are not independent of one another, however. The cat is either alive and the nucleus non-decayed or the cat is dead and the nucleus is decayed—the cat and the atomic nucleus are entangled. An observer who cannot see inside the box knows neither the state of the cat nor that of the atomic nucleus. The observer also does not know whether the atomic nucleus will decay after 5 min or after 100 years, because for each point in time there is only a probability that the atomic nucleus has decayed. The observer can only indicate the total state comprising the cat and atomic nucleus as an entanglement—the subsystems are inseparably linked to one another. This type of correlation is in fact even stronger than it appears here. It has been demonstrated that the quantum correlations for particular measurements are stronger than possible in classical physics.

The second-generation quantum technology—the "new" quantum technology—aims to use the properties of entangled states in a selective way. To accomplish this, these states must be able to be generated, processed and read experimentally. In addition to complete entanglement as in the case above, partially entangled states can also be generated and processed. Quantum entanglement theory allows the degree of entanglement to be described mathematically and measured experimentally.

2.2.2.3 Uncertainty relations A third important phenomenon of quantum mechanics is uncertainty relations, best known as described by Werner Heisenberg in 1927. In general there are variables, such as the location and velocity of an individual particle, which cannot be measured exactly at the same time. If the location of the particle is measured, this influences the velocity of the particle (and vice versa). At first glance, this effect appears to be disturbing, but quantum cryptography (see Section 3.2), for example, is only possible because of it. Cryptography is intended to facilitate secure transmission of data between sender and receiver.

Since listening in on a message always constitutes a measurement, a listener inevitably causes a noticeable disturbance in the transmission of the message, which can be recognized by the sender and receiver. Quantum cryptography makes use of this principle.

2.2.2.4 Many-body effects Quantum systems also have the special feature that they can only be distinguished by measurements. Classical, macroscopic objects can be distinguished from other similar objects by marking, but this is not possible with a quantum system. For example, one cannot number the electrons in an atom; they are, therefore, not distinguishable.

Quantum mechanical particles have an intrinsic property which has no classical counterpart: they have intrinsic angular momentum, also called "spin". It can only assume discrete values—positive half-integer or integer multiples of the value ħ (ħ is Planck's constant, h, divided by 2π). Particles with half-integer spins are referred to as fermions; those with integer spins are known as bosons.[11] Examples of fermions are the components of an atom such as protons, neutrons and electrons, while photons (light particles) are bosons.

These two particle classes exhibit fundamentally different behaviour near absolute zero. When bosons are cooled to extreme low temperatures, they all assume the same state, a macroscopic quantum state, forming a Bose–Einstein condensate. Two fermions, on the other hand, can never have the same state. However, in particular cases they can form pairs which behave like bosons. This effect is responsible for superconduction, for example, where the electrical resistance of many metals disappears below the transition temperature. These metals then conduct current without loss.

2.3 Approaches to research and application

Key summary

- In a digital society, the security of data transmission is of central importance. In this regard, quantum cryptography can make an important contribution by improving encryption technologies. It is important to conduct research in quantum cryptography at a national and European level to avoid dependence on other countries in this sensitive area.
- The current debate over data security, privacy and spying underscores the importance of early and comprehensive technology impact assessment, because a possible quantum computer and quantum cryptography could result in radical changes to data security standards.
- Developments in the field of quantum technology also affect the development of important supporting technologies, such as cooling systems, laser chemistry, measurement and processing methods.
- The establishment of regional support and development centres could pool scientific competencies and create an environment that facilitates and promotes technological spin-offs.

2.3.1 Topics of basic research

The field of research for quantum technology is unusual in that applications can be derived directly from basic

[11] Named after Enrico Fermi (1901–1954) and Satyendranath Bose (1894–1974) respectively.

research.[12] Various areas of research have benefited from an understanding of concepts from quantum physics, such as superposition, entanglement and many-body effects.

These include:

- Quantum cryptography with the development of protocols;
- Quantum information theory;
- Miniaturization; and
- Quantum biology, e.g. to produce an “artificial leaf” for energy conversion by photosynthesis.

In view of the current state of knowledge, but also due to the fact that it is a new area, it cannot be predicted at this time which of these fields will play the greatest role in future applications. Thus close attention should be paid to the development of this entire area of knowledge so that fields which offer promising opportunities can be recognized early on.

There are already attempts to develop model systems for simple applications in application-oriented basic research. Areas to which this applies include:

- The transmission of quantum information over great distances, and the increase of transmission and repetition rates;
- Improved use of quantum mechanical effects for precision measurements;
- The development of thermoelectric generators;
- The feasibility of quantum machines; and
- The development of nanomagnetic logic (spin logic).

Research and development in the application of quantum technology is still in its early stages with, at most, laboratory scale test equipment already available.

This can, however, be used to show that the technological objectives are achievable in principle. The following section describes particularly promising areas in more detail.

2.3.2 *Fields of application*

2.3.2.1 Quantum communication and cryptography Quantum cryptography can increase the security of data transmission. If the conventional internet security systems, for whose reliability there is no mathematical proof, fail, the resulting damage would be staggering in scope. In conjunction with conventional methods, quantum cryptography facilitates secure data transmission between two points and (for example, using quantum repeaters) in the future also in quantum networks. A key feature of quantum cryptography is that even if encrypted messages are intercepted and stored, they cannot be deciphered, not even in the future with improved technology. Quantum cryptography thus enables the long-term security of data (see also “Focal points of current research”).

2.3.2.2 Quantum computers Research into quantum computers is needed to make a realistic estimate of possible threats to conventional cryptographic systems and to take necessary defensive measures.

Data transmission and the development of quantum computers are among the specific future fields of application for quantum technology.

However, up to now there have only been model systems to prove the basic principles. Work is necessary here to develop components such as ion traps, neutral atoms and solid bodies (for example, as carriers of quantum dots) so that they are functionally mature as the basic elements of such computers. This also applies to the methods needed for error correction and the construction of large systems which enable the computing capacity required.

Quantum computers for specific problems such as factorization could be a first step toward experimental implementation of sufficiently large all-purpose quantum computers.[13] Close cooperation with computer science is essential here.

2.3.2.3 Quantum sensor technology and quantum metrology It is now possible to achieve very precise control of the quantum states of individual atoms. These controlled quantum states can be used in sensors. Sensors of the order of magnitude of atoms can provide exact, largely interference-free measurements of magnetic and electrical fields with nanometer precision. This is why they can play an essential role in technologies such as ultrasensitive magnetic resonance. Other important components of such technologies would be nonclassical light states and quantum entanglement.[14] Nonclassical light would enable super-high resolution imaging methods to be achieved in microscopy and innovative sensor technology. Moreover, new quantum technology could facilitate more reliable definition of the basic units of physical measurement. Efforts are currently underway to find a suitable, practical method for the basic

[12] For example, since 2012 industry has supported the Alcatel-Lucent’s Bell Labs guest professorship at the Friedrich-Alexander-University in Erlangen-Nuremberg, which researches practical applications together with the Max Planck Institute for the Science of Light.

[13] The decomposition of a natural number into a product of prime numbers is of great importance for encryption methods.

[14] Classical optics usually treats light as a wave. If light is considered at fundamental quantum level, this wave consists of discrete particles (photons).

unit of mass to replace the original kilogram used with the measurement of elementary values. This has long since been the case for the measurement of length and time.

2.3.2.4 Supporting technology Another distinctive feature of quantum technology is that it requires numerous sophisticated "supporting technologies" to produce quantum systems and maintain operation reliably over a longer period of time. This means that an investment in the development of particular quantum technology also promotes the advancement of other key technologies. This includes the development of:

- Cooling systems;
- Micro-production methods;
- Solid-state physical quantum systems;
- Quantum electronics (including single electron transistors);
- Laser chemistry (synthesis and analytical applications); and
- Measurement and processing methods.

Synergies are to be expected because the supporting technology developed for quantum technology applications will also accelerate the further development of conventional information technology, sensors and robotics as well as high sensitivity diagnostics.

2.3.3 Integration of research and application development

The uncertainties illustrated above pose particular challenges for industry to transform the results of basic research in quantum technology into products viable for the market. Thus, scientific research institutes will have to be the initial drivers of industrial implementation. In order to do this, the extensive, highly complex, specially created experimental equipment in research institutes will also have to be used to develop prototypes of products using quantum technology.[15] Current support schemes such as the EXIST research transfer initiative[16] of the German Federal Ministry of Economic Affairs and Energy provide support opportunities for spin-offs from research institutes.

Companies focused on quantum technology arise primarily in places where technical knowledge, equipment and administrative support by regional research institutions are available. The creation of quantum technology centres based on the current research groups could anchor and promote the development of individual technology as has been the case in the US, Canada, the UK and Switzerland. These centres could each focus on different aspects of quantum technology from basic research all the way to application.

It is highly advisable for Germany to have centres with focal points of research based on the current regional scientific and technological expertise. The activities of the centres should then be coordinated at a national level. Theoretical working groups, on the other hand, could also benefit greatly from the establishment of a "virtual" centre as well as working with the experimental research centres.

Highlight 3-1: Technological impact assessment

The further development and impact of quantum technology are not yet clearly foreseeable. Thus, informed assessments of possible consequences are not without considerable uncertainty. It is therefore important to identify expectations, different assessments and views at an early stage and to discuss these impartially. There are essentially two models which have been established in practice for assessing the impact of technology. The "expert model" is based on the assumption that questions of assessing the effects of technology are entirely cognitive in nature and, thus, can be answered by the knowledge of experts, for example in committees of technical investigators.

The "participative model" assumes that knowledge-based criteria alone cannot answer concerns regarding estimated benefits versus accompanying negative consequences to be expected and the acceptance resulting from this. Accordingly, qualitative and normative aspects especially can only be addressed with the involvement of future users and legal decision-making committees (such as parliaments).

Surveys of the general public show that the unknown is quickly seen as imponderable and associated with too much risk. However, the basic attitude toward new technology changes significantly as soon as a clear benefit for users emerges.

The impact assessment of quantum technology should make use of both models, the expert and the participative, as complementary views to seek exchanges between experts, representatives of social interests and the concerned public. The objective should be to initiate a constructive discussion about opportunities and expectations as well as risks and gaps in knowledge.

Platforms focused on promoting dialogue should be created to encourage open discussion and the sharing of knowledge and the latest developments in quantum technology; they should go beyond a mere communication of technical knowledge. Possible options here are:

- Web-based formats intended for discourse, not limited to just presentation.
- Expert blogs (with a comment function).
- A central website where readers can learn about the latest developments in science and business and get information about events and dates and discuss in forums.
- Hands-on exhibitions and visitor laboratories could offer interactive explanations of quantum physics principles and their current and possible applications; traveling exhibitions could also be created. Experience at a number of places (Stuttgart, Ulm and Erlangen) can be called upon for this.

[15] As shown by the example of the Center for NanoScience (CeNS) at Ludwig-Maximilians-Universität Munich, this is a suitable way to facilitate technology spinoffs. http://www.cens.de/ (last accessed: 18 February 2015). accessed: 18 February 2015).

[16] http://www.exist.de/exist-forschungstransfer/ (last accessed: 18 February 2015).

Source: The Allensbach Institute and the German National Academy of Sciences Leopoldina [10]

2.4 Summary and outlook

Quantum technology makes use of quantum physics principles. They have an interdisciplinary focus and benefit from fields beyond physics, such as mathematics, chemistry, electrical engineering and computer science.

Germany is one of the countries where quantum physics began. More than 100 years after its fundamental discoveries, quantum physics remains the basis of many modern technologies, such as semi-conductors and lasers. These technologies are also referred to as "first generation" quantum technology.

There is considerable potential for the **new generation of quantum technology**. Areas for application include information processing and secure communications, highly sensitive sensors for measurement, standardization and medicine. To develop quantum technology successfully, it is essential to improve and refine numerous conventional fields of technology, such as cooling systems and micro-production methods, laser chemistry and nanotechnology. In other words, the focused development of quantum technology also has a positive effect on the further development of supporting technology.

A prominent example for the potential of the new generation of quantum technology is quantum information theory and its applications to secure data transmission. According to the natural laws of quantum physics, a third party (such as an unauthorized listener) inevitably disturbs the transmission of a message, which can be detected by the sender and the receiver.

Quantum cryptography makes use of this principle, for example in the transmission of data using quantum states of light. In contrast to current cryptography, its approach is not based on plausible, mathematically unproven assumptions, but rather on laws of nature. This enables quantum cryptography, which has already been tested in initial model experiments, to reach a new level of security in transmission.

Moreover, in the future quantum information theory could also result in the development of more powerful concepts for computers and computing methods. Conventional computer technology, which is the basis for data processing and communication, will inevitably reach its limits due to increasing information density and integration in ever smaller components.

Quantum technology is indispensable for the continued miniaturization of electronics.

For measurement technology, the use of quantum effects could achieve previously unimagined sensitivity and precision, significantly improving the measurement of times, masses and currents. This creates possible application for ultraprecise GPS and navigation systems and for medical diagnostic equipment.

The new quantum technology is largely still in the basic research stage.

Thus making quantum physical effects usable in the new generation of quantum technology requires even greater research efforts. Quantum cryptography is currently the most developed subfield of the new generation of quantum technology, also with respect to its economic utility.

Although many of the basic discoveries for the new generation of quantum technology have taken place in Germany, so far no company in the country has attempted to commercially exploit the new quantum physical effects.

This report identifies the current structure for research and support as one of the main problems. On account of the interdisciplinary character of quantum technology, the support for their individual aspects is spread widely across different subject areas. The expertise is also correspondingly distributed over a variety of locations and thus not well noted by industry. This report aims to show that the focused and systematic support of quantum technology, particularly with respect to technical implementation, can create the environment in which innovative products could arise in the medium term. By establishing suitable research centres and clusters, structures should be developed in which the various processing steps for the development of new quantum technology can be undertaken collaboratively to the greatest extent possible.

Moreover, to keep pace in the field of quantum technology internationally, engineering education needs to be supplemented accordingly. Basic knowledge of quantum phenomena should be part of undergraduate studies, a fundamental part of the curricula in the same way that mechanics is, for example. This is particularly important for electrical engineering and information technology courses, because the first applications are anticipated to come in these fields.

3 Section B: Detailed information—focal points of current research

3.1 Introduction

Tasks to be accomplished with the new quantum technology range from solving abstract mathematical problems to very specific tasks of implementation which involve not just physicists and mathematicians, but computer scientists, electrical engineers, chemists, biologists and surveying engineers. Subject areas involved include information theory, computability theory, communication security, signal processing and ground surveys. The new research area of quantum technology is thus greatly dependent on interdisciplinary collaboration among various previously separate fields of expertise.

Research in quantum technology is conducted at various, partially overlapping levels:

- **Since the 1980s, basic research has laid the cornerstone for quantum information and communication**, i.e. information processing and communication based on quantum physics. Quantum cryptography according to Bennett and Brassard [1] is directly connected to uncertainty relations [9]; a related idea from Ekert [6] goes back to the EPR paradox (from Einstein et al. [5]). The processing and observation of an individual quantum system comprised significant experimental progress for this. Many basic questions still remain unresolved, and answering them will undoubtedly provide important new insights for future quantum technologies.
- The better individual quantum systems of the most diverse kinds—photons, atoms, ions, molecules, spins, etc.—are understood and mastered, the more pressing it becomes to **develop integrated architectures of quantum systems**. For this, individual quantum systems are integrated in a support structure so that they can be used for specific applications (these constructs are referred to as hybrid quantum systems). Numerous individual quantum systems can be controlled using integrated components such as atom and ion traps, waveguides and optomechanical elements. Successful integration of quantum systems in architectures which can be produced with current micro-production methods would greatly advance the development of applications.
- The **applications of quantum technology** make the methods of quantum physics usable in a practical way. While applications for sensors and measurement technology should be developed relatively soon, the development of quantum simulators and computers is expected to take some time. Quantum simulators could allow macroscopic quantum phenomena such as superconduction[17] to be calculated and optimized for new materials. This is not possible even with the best computers available today. This could, in turn, enable the application of power transmission lines based on superconducting materials with no electrical resistance. Developments in quantum technology could also be useful for conventional applications. One objective of quantum computer research, for example, is to produce integrated circuits for individual photons, which contain both sources and detectors on a single chip. This could lead to the development of new optical components with very low light output. Efficient simulation of many-body systems can help achieve a better understanding of transport processes in biological systems, for example. Conversely, technical developments in the field of quantum technology also always provide new stimulus for basic research.

[17] Superconductors are materials whose electrical resistance disappears below a transition temperature.

The research landscape can, along-side the various levels, also be described in terms of the different areas in which researchers are working both theoretically and experimentally. These include:

- The **transmission of quantum states**, in particular using light (photons), which is based primarily on laser technology and fibre optics and opens up new possibilities, such as quantum communication and cryptography;
- The **processing of quantum states** in quantum computers and the necessary theoretical basis for this, such as quantum algorithms and quantum information theory;
- **Improvement and refinement of existing technologies**, particularly in the areas of sensor and measurement technology; and
- **Theoretical basic research**, for example in the control and regulation of quantum systems or to understand biological processes such as photosynthesis.

The individual subfields of quantum technology are presented in detail in the following section to provide the reader with an overview of the scope of this field.

3.2 Quantum communication and cryptography

Cryptography is intended to enable secure transmission of data between sender and receiver even if a third party intercepts the transmission. In symmetric encryption, the sender and receiver need to encrypt and decode the message with a key which is known only to them and not to an eavesdropper. These keys are usually a long chain of randomly sequenced digits. The exchange of keys for the encryption is a security risk and also needs to be protected against interception. The security of the methods often used today with a public key for the sender and a private key, known only to the receiver, is known as public key cryptography and is based on mathematical operations that are asymmetrical with regard to the complexity of their calculation. One example is the factorization of large numbers, which is inefficient and thus difficult, whereas the reverse operation, the multiplication of numbers, is simple. Thus considered, conventional cryptography is still caught in a spiral that started thousands of years ago of continuous improvement of both the encryption methods and the interception methods. As long as there is no mathematical proof that rules out the existence of an efficient algorithm for the factorization, for example, conventional cryptography will not reach the end of this spiral. From what we know today, it is possible that this kind of algorithm, one that runs efficiently on conventional computers, could be discovered at any time, or indeed has already been found but is being kept secret. This is an unsettling thought and one which underscores the importance of quantum cryptography,[18] which provides demonstrably secure methods for generating and distributing secret keys. Unlike other conventional methods of classical cryptography, it can be demonstrated by mathematical means that particular quantum cryptography methods remain secure even if the eavesdropper uses all means available within the laws of nature, even a quantum computer.[19]

This has never been possible before in the history of secret messages. The part of these methods relevant to quantum physics can be divided into three steps:

- The sender (generally) generates light as an information carrier (for example, a single-photon excitation of a particular light mode) in an exactly defined quantum state.
- The light is transmitted to the receiver via a channel (e.g. a cable or airwaves).
- The receiver measures the light in an exactly defined manner.

This technique also enables the creation of a truly random number generator, which has a series of applications itself.

3.2.1 Security aspects of quantum cryptography

The oldest and best studied methods for quantum cryptography are the BB84 and Ekert protocols.[20] The former uses individual photons, the latter entangled ones. The security of both protocols has already been proven subject to very general prerequisites, but their practical implementation is difficult, because the experimental requirements are very high.

However, there are technical limits to the implementation of the three-stage method. In particular, the light transmission is subject to signal losses and transmission errors. Since these errors can also always be interpreted as an attempt by an eavesdropper to intercept the transmission, additional processing of the measurement data is then required to counteract any knowledge an eavesdropper may have gained regarding parts of the key. There are models with which the generation rates of the key bits can be calculated under realistic conditions. Calculations within this model are often difficult, because signals and detectors are not described by simple qubits and qubit measurements, but instead by systems of light states. However, for the most important protocols it has been demonstrated that not just single photon sources but also simpler laser sources are suitable for the generation of secure keys. One variant of the BB84 protocol can already generate several million secret key bits per second. The next objective is to find better combinations of signal coding and measurement procedures to achieve a high key rate even over long transmission distances, for which quantum systems with more than two states are particularly suitable. The advancement of detection methods is also important for this.

There is hope of using new theoretical approaches to achieve better insight into the functioning of the protocols and improve their security and efficiency. There are attacks against conventional cryptography which use the power consumption and the computing time of the technical equipment to provide clues regarding the key or the plain text. There are also side-channel attacks against quantum cryptography which are only possible if the implementation is incomplete. This shows that the security of quantum cryptography systems must always be considered as a whole and in practical application. New “device-independent” protocols are now being researched with the intention of simplifying the assumptions of proof regarding the exact functionality of the equipment used. This should close the side channels or at least make them controllable.

3.2.2 Photonic quantum systems

Quantum communication and cryptography work almost exclusively with quantum states of light (photons). These can be achieved with comparatively low technical effort, sent over great distances and have nearly ideal quantum behaviour. They have proved useful in recent decades, particularly for the study of basic questions in physics. Experimental tests of Bell’s theorem, for example, very often use entangled states of photons.

Nonlinear interaction processes are usually used to generate quantum states such as individual photons or entangled photon pairs. The use of integrated optics such as waveguide chips, fibre optics and optically coupled

[18] In September 2014, the European Telecommunication Standards Institute (ETSI) published an extensive report on the subject of quantum cryptography. The report “Quantum Safe Cryptography and Security” (ISBN 979-10-92620-03-0) is available at the following link: http://docbox.etsi.org/Workshop/2014/201410_CRYPTO/Quantum_Safe_Whitepaper_1_0_0.pdf (last accessed: 19 February 2015).

[19] The key phrase “post-quantum cryptography” is used to describe investigations by computer scientists into conventional methods which remain secure if quantum computers are available to solve the factorization problem, for example. These methods do not achieve the fundamental security of quantum cryptography, but they are expected to be simpler to implement.

[20] Named after Charles H. Bennett (*1943) and Gilles Brassard (*1955) and Artur Ekert (*1961) respectively. A protocol in this case is understood to be a series of handling instructions, at the conclusion of which success (in this context a key) or failure occurs.

networks have made the generation of quantum states more efficient and improved their quality. This has also advanced the miniaturization of the components required to build complex quantum networks. Further efforts are needed to provide even better waveguides and fibres (such as photonic fibreoptic cables) for use in quantum systems. To accomplish this, certain relevant parameters must be adapted to the needs of quantum information processing based on quantum optical considerations. On account of the sensitivity of the quantum nature of light, the latest technical production methods are required and the existing structures designed for use in conventional nonlinear optics need to be improved.

Another important task in quantum communication is to increase transmission rates by generating high-quality quantum states quickly in simple systems. The laser systems used to generate the necessary ultrashort light pulses are still something of a weak point here. They are, in part, still rather difficult to set up and are not sufficiently stable. The next generation of such systems needs to be significantly more robust, with less noise. Basic work for this and prototypes are currently under development. They also need to have higher repetition rates and greater average power with improved spatial and spectral properties.

To substantiate the quantum properties of light, detectors are required which can record the photon counts of even very weak light (single photons) with few errors. Current photon detectors still cannot distinguish between low photon counts of 1, 2, 3, etc. Development is in progress for detectors which can also measure the number of photons. However, up to now they are limited in at least one of the relevant performance requirements, such as efficiency, no noise, time resolution, repetition rates or wavelengths and must be operated at very low temperatures, so that better cooling methods are also needed.

Analytical methods currently available to verify quantum properties in experiments can also be developed and refined further. This could also be done with alternative methods of characterization and simplified detector types. Advances in wavelength conversion can also contribute to improved interfaces for efficient transmission in optical fibres and measurements.

3.2.3 Outlook for quantum communication and cryptography

For quantum cryptography to be widely usable, it must also work for transmission over long distances. Although currently, transmission over distances of several hundred kilometres is possible, the use of quantum mechanical relay stations, also known as quantum repeaters, is under investigation to bridge longer distances; their technology is closely related to the possibility of remote transmission of quantum states (quantum teleportation).[21] Studies are also being conducted on how to construct quantum networks from point-to-point connections and integrate these in existing telecommunication networks. There have also been attempts to establish quantum communication channels supported by satellites.

Quantum communication will be used for more than just generating keys. Other cryptographic protocols, such as digital signatures and anonymous database queries are also conceivable. Apart from cryptographic applications, it can also facilitate technical improvements, for example by using quantum effects to increase the data flow in fibre optic cables. Far in the future it can also lead to protocols which could solve particular applications with significantly less effort than is possible with conventional technology, such as the synchronization of calendars or the comparison of long texts.

The simplest methods of quantum cryptography function without processing entangled states, and some corresponding equipment is already commercially available. Quantum cryptography is currently the most developed subfield in the quantum technology of the second generation, also with respect to its economic utility.

3.3 Quantum information and quantum computers

Quantum information technology arises from the understanding that both the representation and the processing of information are closely linked with physics. The laws of nature limit the fundamental possibilities of information processing (for example, by uncertainty relations). But it is important to know which calculation models are suited for an efficient simulation of nature. Both of these aspects are of great importance in theory and practice:

- The miniaturization of conventional semiconductor-based computer technology will reach practical thermodynamic and quantum mechanical limits in the near future. The question arises whether Moore's Law—the doubling of performance capacity for integrated circuits and thus also for computers about every 18 months—can continue to apply, and if so, how.
- On the other hand, in theoretical computer science, the fundamental possibilities and limits of information processing are being studied based on a simplified, abstract model and natural law dictates which model can be used. According to the current state of knowledge, this model is no longer just a machine with a representation

[21] The German Federal Ministry of Research and Technology supports the investigation of basic science for quantum communication as part of the IKT 2020 development scheme.

of binary logic, but rather the *quantum computer*. There are several reasons for this: (1) The laws of nature allow its construction in principle; (2) We know of no other computing model with greater performance which is achievable in principle; (3) It appears to be more powerful than conventional computers for particular applications.

The performance capacity of a quantum computer is seen by its ability to efficiently perform tasks which were previously very time-consuming. A quantum computer can, for example, run Shor's algorithm, decomposing large numbers efficiently into their factors and calculating discrete logarithms. Efficient algorithms to solve this problem on conventional computers are not known. If a larger quantum computer were really built, as is anticipated, then it could break all the major conventional public key methods (cryptography as well as authentication), which would have disastrous consequences for security on the internet.

The key components of a conventional computer are processor, bus system, register and memory. Computing operations are performed using lattices or logic gates. Analogously, a quantum computer is comprised of quantum logic gates, quantum memory, etc. However, quantum logic gates are very susceptible to interference. Interaction with the environment can lead to decoherence and the loss of interference capacity for the system, which makes error correction methods necessary. It has been demonstrated that the quantum computer is possible if the quality of the individual components were above a certain threshold. Alongside this lattice-based implementation, there are also other proposals, such as the disposable quantum computer, in which a skilfully prepared state is measured only once in a particular sophisticated way, and a result is obtained.

A practical and relevant intermediate step on the path to the "all-purpose quantum computer" could be the development of quantum simulators, which can efficiently simulate only particular quantum algorithms, such as the dynamics of other quantum systems.

The system intended to create a quantum computer must usually meet the following DiVincenzo criteria[22]:

1. The system consists of well-determined qubits and is able to be scaled to any size.
2. It is possible to impose a fixed, pure state on the system (initialization).
3. The coherence time of the system is significantly longer than the operation time of a gate.
4. A universal set of quantum gates is implemented from which all quantum operations can be composed.
5. The individual qubits can be measured.

Two additional requirements are set for use in communication:

1. Stationary qubits and flying qubits (photons) can be transformed into one another.
2. The flying qubits can be transmitted between particular locations situated apart from one another.

There are a series of approaches for creating quantum computers. Systems such as ion traps and neutral atoms are presented in the following section; in the section after that, solid-state physical systems.

3.3.1 Ion traps

One way of creating a quantum computer experimentally is the use of ions which are held in a trap. This concept is based on work by Cirac and Zoller from 1995.[23] The quantum register, i.e. the qubits, with which the quantum information is to be processed, consists of a chain of ions, often from alkali earth metals. From the multitude of states that such an ion can assume, only two very particular levels can be chosen. The remaining levels should remain unoccupied, but this cannot always be guaranteed due to interference.

In principle, this kind of system meets all the DiVincenzo criteria, and the majority of these requirements have already been implemented experimentally.

Although the original schema is basically scalable, in practical use additional technologies are necessary, such as linking of widely distant qubits using photons or by the displacement of ions to transport quantum information.

With ion trap-based quantum computers, the qubits can be implemented in two ways. Either two levels of the Zeeman or the hyperfine structure of an ion are used or a forbidden optical transition. It is currently possible to place up to 14 ions in traps, and by cooling the ion chains, these can be brought to the ground state of the trap's potential. Certain hyperfine structure levels result in mean lifetimes of up to 10 min if they are not sensitive to magnetic fields. For optical transitions, spontaneous decomposition limits the coherence time; however this is of an order of magnitude greater than an individual gate operation. Mean lifetimes of up to several seconds can be achieved using decoherence-free subsystems (see Section 3.5.1).

[22] Named after David P. DiVincenzo (*1959); D. P. DiVincenzo [4]. Topics in Quantum Computers. In: L. Kowenhoven, G. Schön and L.L. Sohn (pub.): Mesoscopic Electron Transport. NATO ASI Series E. No. 345, Kluwer Academic Publishers, Dordrecht (1997), p. 657.

[23] J. I. Cirac & P. Zoller. Quantum Computations with Cold Trapped Ions. Physical Review Letters [3], 4091–4094.

Today, the most important one- and two-qubit operations achieve high qualities of up to 99 %, and it is now possible to generate important entangled states (GHZ and W states) for quantum information processing. To measure them, a state-dependent light scattering is used with which detection efficiencies of 99.99 % can be achieved. To transfer the quantum information from the ions to photons—and vice versa—cavity quantum electrodynamics technology is used.

Ions spaced far apart from each other can be entangled with it, even if this entanglement can only occur with a particular probability. The ions can also be displaced mechanically over short distances within a quantum processor itself.

Quantum information processing with ion traps already currently meets most of the requirements for a quantum computer. Ionic two-level systems with their long coherence times are suitable as a robust quantum memory. Excellent measurement methods and the availability of a universal set of quantum gates from which any calculation operations can be generated make ion traps a good starting point for the first quantum computers. However, the problem remains that fluctuating electromagnetic fields and spontaneous decomposition can lead to decoherence. The lasers are also often not stable, and the optical measurements and circuits not fast enough. However, these are technical problems and no fundamental difficulties are to be expected.

3.3.2 Neutral atoms and molecules

Quantum computers and simulators can also be implemented based on neutral atoms and molecules, using long-lived internal states of atoms or molecules as qubits. These can be selectively influenced using light or microwave radiation.

Thanks to the laser cooling method and Bose–Einstein condensation, the technology for capturing cooling atoms is already very advanced making it possible to produce high-quality quantum registers. The technology is currently being extended to molecules.

Quantum computing with neutral atoms is based on new trap technologies. Traps are possible with which the centre of gravity movement of individual atoms and molecules can be controlled independently, which is a prerequisite for a quantum computer. A large number of qubits can now be controlled in parallel, for example in optical gates, which is particularly relevant for simulating solid-state systems. Entanglement can be generated in systems of neutral atoms using two mechanisms:

- Interaction of two particles by impacts due to short range forces or by long range forces, such as dipole forces between highly excited Rydberg states, thereby deterministically producing the entanglement
- An exchange of photons, which only produces the entanglement probabilistically, i.e. with a specific probability, i.e. when the photons are measured with a certain result.

Both mechanisms work in free space as well as with the use of cavity quantum electrodynamics. Atoms or molecules are saved in optical gates or in a chain of traps. The temporal evolution of the atoms is described by the Hubbard model, according to which the atoms jump around between the lattice sites and interact by impacts. Thus, cold atoms in a gate facilitate the simulation of solid-state many-body systems. Bose–Einstein condensates can also be placed in an optical lattice and the phase transitions therein observed between the superfluid and the Mott insulator phase. The latter makes it possible to occupy each lattice site with exactly one atom, which leads to a very large number of atom qubits, which can also be entangled with one another. This arrangement comprises the basis for a quantum simulator, for example for spin lattices with which the temporal evolution is decomposed into a sequence of gates comprising one- and two-qubit operations which can be performed on all qubits simultaneously. An important new development is the option to display individual atoms in an optical lattice and at least partly control them. In combination with interactions between the atoms, this opens up a way to measure individual atoms from a large number of entangled atoms.

Due to their relative insensitivity to environmental interference, neutral atoms can be used to store quantum information. However, at the present time only very weak trap potentials are available, which have to be compensated by cooling the atoms to very low temperatures. Three methods are currently available to capture and process neutral atoms and molecules:

- Optical tweezers and sequences of optical traps enable preparation of well-defined quantum states of atom movement, either by cooling individual atoms down to the ground state or by introducing a Bose–Einstein condensate to an optical lattice. Both approaches have the potential to control individual atoms and to parallelize this procedure.
- In atom chips, atoms are captured magnetically near the surface of a substrate and cooled. Due to their small size and robustness, they are suitable for use as components of larger quantum processors.
- Traps for polar molecules based on microwaves or electric fields are being investigated. They are important for experimental research.

Numerous methods of generating entangled states have been investigated that are based on interactions between atoms and employ these as information carriers either directly by impacts or dipole moments or indirectly by photons. Optical tweezers are suited as burst gates, and optical lattices enable parallel quantum gates by moving the atoms depending on their state. Without mechanical displacement and at room temperature, individual atoms can, in turn, be entangled via Rydberg blockade. This method is also very fast.

3.3.3 Cavity quantum electrodynamics

The technology of cavity quantum electrodynamics is being investigated for the construction of an interface between different carriers of quantum information. This interface can be configured probabilistically with atoms in free space, which send photons randomly in all directions.

A deterministic interface is obtained for atoms in a cavity (Rydberg atoms in microwave cavities, ground state atoms in optical cavities) or with parabolic mirrors in free space.

Placing each atom in its own cavity ensures addressability and scalability. The individual cavities can also be removed far away from one another, because the exchange of quantum information takes place via photons, which enables the construction of quantum networks.

3.3.4 Photons

Another possible way of implementing quantum computers is using photons.

Here qubits are frequently implemented by the polarization of photons. The oscillation directions of the electromagnetic field, horizontal and vertical, correspond here to the states “0” and “1” of the qubit, with every superposition of the states naturally possible. It is particularly easy to set the state of individual qubits, because the polarization can be manipulated easily with optical elements such as waveplates.

Other options to implement qubits are, for example, the number of photons, their path or their arrival time.

Photons have numerous additional advantages along with the simple implementation of gates for individual qubits.

These include their high mobility as well as the low interaction with the environment, which renders complex insulation (vacuum, cooling) unnecessary. Photonic qubits are thus very stable and have a long coherence time which means that they do not lose their quantum properties over a long period of time. This and the fact that they move at the speed of light make them ideal carriers for the transport of quantum information.

With today’s technology it is already possible to perform entangling operations between multiple qubits to a high quality; nevertheless, the complexity of the circuits which can currently be produced is still limited. The reasons for this are found at various points of a potential quantum computer.

For one, a source which reliably emits a specific number of photons has not yet been realised. With current sources, there is a certain probability that more photons will be emitted than desired, which falsifies the result. The emission of these photons is also random. That means that the exact time of an emission cannot be defined or predicted.

Also, the circumstance that photons hardly interact with their environment makes it difficult to couple different qubits with one another. However, this is generally necessary to perform calculations on a quantum computer. At the current time, such entangling operations between qubits can only be implemented probabilistically, i.e. the gate will only be executed correctly with a certain probability. This makes the expansion to a circuit comprising numerous operations difficult, because the probability that all gates are correctly executed results from the product of the individual probabilities of correctness and, thus, drops quickly if there are many defective gates. However, it has been demonstrated that this problem can be circumvented by using additional qubits and that photonic qubits enable efficient implementation of calculations.

A further challenge for the future is the implementation of storage options for photonic qubits. This is necessary, among other things, because photons move at the speed of light but many algorithms require the storage of information. Moreover, memories can be used to implement reliable sources for individual photons, because the randomly generated photons can then be stored and then emitted and output in a controlled manner at the desired time.

Quantum computers also need to be able to read the qubits generated, i.e. to be able to measure. Detectors are needed for this which, ideally, can detect 100 % of the photons reliably. This is not yet possible although much progress has been made in the field of detector technology in the last few years.

Another field that is advancing rapidly is the use of optical waveguides. These are the glass chips guided through a network of optical tracks. As the light is guided on fixed tracks, these chips enable an extremely stable interaction of different photons. Furthermore, these structures enable the implementation of quantum random walks which are not only used in various algorithms but also could also provide the basis for building a universal quantum computer.

As the construction of such a general quantum computer is still proving difficult, there are approaches for using some of the benefits of quantum technology without having to construct a universally usable quantum computer. One of these approaches is boson sampling which uses the special property of photons to solve mathematical problems that are very difficult for conventional computers to master.

Due to their numerous merits, qubits based on photons show promise for realising a quantum computer, particularly for implementations such as the disposable quantum computer with which, to the extent that a suitable initial state can be generated, measurements of individual qubits suffice to perform any calculation. On account of their mobility they are also the first choice for protocols which require the exchange of quantum information between different locations. However, in the years ahead, major challenges such as better sources, detectors and storage options must be overcome to make complex circuits comprised of many qubits.

3.4 Quantum information processing in solid bodies

Solid bodies exhibit very diverse electrical and optical properties which are attributable to the many different ways in which atoms can interact with one another and form bonds. In general one can attribute such bonding states to elementary excitations (quasi-particles are referred to in this context). If these have a discrete energy spectrum, then, in principle, any pair of states can be considered qubit.

However, studies have demonstrated that if the states are required not to decay over a sufficiently long period and must be capable of being processed well, then a large part of these excitations are ruled out. The reason for this is that the possible qubits are embedded in an environment with which they interact strongly, in contrast to free atoms, for example.

In this environment there are also other excitations present such as vibrations of the crystal lattice with which the qubit can interact and thus destroy its coherence.

A number of provisions are necessary to protect this coherence.

The fact that there is a search for suitable systems for qubits in solid bodies at all is due to the current state of information technology. The high degree of integration of the components is being extrapolated into the quantum range.

Since such components are predominantly based on solid bodies, there is hope that with them it will be possible to create especially compact, robust solutions for quantum computer hardware. Moreover, they may also be compatible with current micro- and nanoelectronics. Scalability is also a reason that is frequently given for the possibility of building quantum computers of any size without great effort. However, nearly all promising qubit systems must be operated at temperatures close to absolute zero, which requires an elaborate setup. This must also be scaled accordingly if systems comprised of many qubits are to be constructed. It is also unclear whether the coherence of the qubits can be maintained long enough when they are scaled in order to be able to process them.

In the following section, qubits are presented in two different systems: in superconductors and using impurities selectively doped in semiconductors and isolators. Some fundamental effects have been demonstrated with both of them, including their initialization, coherent processing and readout. It is still not clear, however, how the quality with which these operations are performed can be improved, how coupling between the qubits can be controlled and how to scale the systems.

One approach still in the initial stage of research is topological quantum computing in which the external interferences (decoherence) are reduced by utilizing global properties; fractional quantum Hall states, which occur in many semiconductors, are suited for this experimentally.

3.4.1 Qubits in superconductors

Electrical resistance causes information carried by an electric current to be lost.

However, if the superconductor is cooled below the transition temperature, the system of conduction electrons enters a macroscopic quantum state and resistance disappears. Thus, there are no losses in superconducting circuits. Very diverse quantized sizes can be used as qubits in such circuits. In contrast to qubits comprised of individual atoms or ions, they are macroscopic, with dimensions in the micron range and over one billion electrons.

A superconducting circuit has traditional electrical components such as coils and capacitors. If a voltage is applied, an anharmonic potential is produced in which Cooper pairs move. These are two paired electrons in each case, which carry the current in the superconductor. The qubit can be defined via two discrete potential states, and its behaviour can be controlled by changing the applied voltage. Examples of this are charge, flux and phase qubits for which the qubit is represented by two energy minima. With charge qubits, a potential with two minima in a sufficiently small circuit is used. In contrast, flux qubits use two opposing current flows coupled in a Josephson contact via a tunnel barrier.

Due to the low excitation energies of superconducting qubits, the circuits must be operated at temperatures of a few thousandths of a Kelvin.[24] Microwave pulses are used for excitation; advanced technologies are available today to produce these with precision. The transmission of the pulses from their point of generation to the chips lying in cooling devices takes place within nanoseconds, while the

[24] Unit of absolute temperature (0 °C = 273.15 K).

coherence times can comprise some microseconds, i.e. three orders of magnitude greater.

Direct coupling of the qubits can take place inductively or capacitively. For extended quantum information architectures, however, methods must be developed which enable selective coupling strength. This could be photon coupling in the microwave range, for which the qubits must be associated with waveguides. It has already been possible to process systems comprised of three to seven qubits on micro- to millisecond timescales and implement simple algorithms. Moreover, quantum correlations between qubits located a few millimetres from each other have been proven. It is now possible to read superconducting qubits in the nanosecond range. The main problem of super-conducting qubits at present is reducing the decoherence, which is a significant challenge for material science.

3.4.2 Defects in semiconductors and isolators

Spatially extended states in crystals generally have decay times which are too short to be of great use for quantum information processing. To ensure the longest possible coherence, the excitations must be spatially localized. On one hand, this localization leads to a discrete excitation spectrum, similar to that of atoms, and these localized centres are often referred to as "artificial atoms" even if their position is fixed in the solid body. The localization also shields them to a certain extent from the environment. We can differentiate between two principal model systems:

- Quantum dots, in which the free movement of charge carriers is suppressed in all spatial directions, and
- Foreign atoms (dopants) in an otherwise homogeneous crystal to which the electrons are bound.

In both systems, the charge states have proven unsuitable for implementing qubits, which is why current investigations focus primarily on spin excitations. There are very diverse production methods for quantum dots. Structures in which charge carriers are embedded in metallic gates by electric voltages are suitable for studying electrical transport. However, this effect is so weak that it can only be used at temperatures in the range of thousandths of a Kelvin. On the other hand, for optical investigations, self-organized quantum dots are more suitable, since due to their size they interact strongly with light fields of a few tens of nanometres. The potential strength makes operation at up to a few tens of Kelvin seem possible. In both cases, methods have been developed for initializing and reading the qubits that show a coherent processing of the spins.

The III–V semiconductor gallium arsenide provides quantum dots of the highest quality. The problem with this material is the high nuclear spin values of the atoms in the crystal. The hyperfine interaction of the charge carriers spin with the nuclear spin limits the coherence to microseconds. This time period can only be increased with great effort. Another possibility would be to use materials that are free of nuclear spin, such as isotopically pure silicon or graphene. The spin-orbit coupling is significantly less with these as well.

Some concepts envision the introduction of donor atoms. Phosphorus-doped silicon has also been proposed as a prototype. Here, the qubit is determined by the spin of a phosphorus electron. The hyperfine interaction with the phosphorus nuclear spin is not necessarily harmful in this case since the quantum information is also stored in the nuclear spin and can be read via the interaction with the electron spin. This effect enables a good quantum memory to be produced since the coherence time of nuclear spin can be in the range of minutes or even hours. But electron spins can also exhibit coherence times of seconds in isotopically pure silicon. With respect to their optical properties, dopants are significantly more homogeneous than self-organized quantum dots. The single-negative charged complex comprised of a nitrogen atom in conjunction with a void in diamond (nitrogen vacancy centre) has also proven promising. A series of applications have been demonstrated for this, such as fast optical initialization and long-lived coherence (milliseconds) at room temperature, as well as coherent processing and entanglement.

Along with the impurities mentioned in silicon and diamond, a series of other doping atoms are also under investigation in solid bodies. Further progress here also depends on the solution of material science problems with respect to the purity of the materials and the placement of the donor atoms. Like quantum dots, qubits can be coupled via magnetic interactions. The use of photons in microresonators is necessary to couple over larger distances. Up to now, microwaves are predominantly used to process the spins of impurities. Optical technologies could prove particularly interesting if it becomes possible to use the optical transition without the involvement of lattice vibrations.

A further possibility is disordered solid bodies in which atoms or smaller groups of atoms tunnel quantum mechanically between various positions. This effect was detected as the source of various anomalies in glasses at very low temperatures and produces noise and decoherence in solid state-based (as well as in nano- and optomechanical) circuits. Disturbances of this type are the main reason for decoherence of qubits in superconductors and occur in Josephson contacts. However, qubits in superconductors can also be used for spectroscopic measurements of individual tunnelling systems, which interact with the qubits whose disturbances show coherence times of microseconds and can therefore be used as quantum memory.

3.4.3 Nanomechanical quantum systems

There has been considerable advancement in recent years in the control of nanomechanical resonators, which oscillate as strings, bars or drums with dimensions below 100 nm in the frequency range of radio to microwaves. Their movement can now be slowed down to the quantum mechanical ground state. Methods used here include laser cooling developed for ion traps. With mechanical nano-oscillators made of silicon nitride strings and carbon nanotubes, the decoherence of the oscillation modes can already be controlled to produce coherence times of some fractions of a second. The coherent control of nanomechanical movement by coupling to electromagnetic radiation in optical or microwave cavities has now advanced so far that coherent coupling of individual photons to individual oscillation modes should soon be possible, for example in resonators made of carbon nanotubes.

Quantum nano-optomechanical systems and quantum nano-electromechanical systems have long since become an active field of research internationally and are also anticipated to trigger major advances in sensor and measurement technology.

Already today, mechanical nano-oscillators can measure changes in mass on the order of 10^{-21} g, thus proving the adsorption of individual atoms. The possibility of coherent control of nanomechanical movement through electromagnetic radiation also opens up prospects of achieving photon-controlled qubits on a nanomechanical basis for which there are interesting applications even in conventional coherent signal processing. Attempts are already in progress to replace the rather clumsy mechanical filter based on acoustic surface waves, which are found as discrete components in each mobile telephone, with nano-electromechanical filters which can be integrated directly into the silicon technology.

Practical applications are also possible today for mass, force and motion sensors, as are new ways of coherent nano-electromechanical signal processing. The increased sensitivity down to the range of individual oscillation quanta promises to be a valuable extension of solid-state-based quantum technology with nanomechanical elements.

3.4.4 Hybrid quantum systems

Overall it is becoming apparent that it will be difficult to identify a system which meets all requirements for coherence, coupling and processability. To a certain degree this is due to the nature of the matter, because efficient processing requires extensive opening of the system, which makes it susceptible to interference. Conversely, if the system is strongly shielded, it makes processing significantly more difficult. Various platforms are used for conventional computer hardware. Bits are represented either magnetically on hard drives or by charges on solid-state drives (SSDs), transported via pulses of current and processed in circuits.

In the same way, quantum computers will have to use the most suitable quantum system for each task, an individual approach to quantum hardware could thus prove to be insufficient. It will be necessary to combine various platforms such as atoms and solid bodies to make hybrid systems, to take advantage of the different strengths of the different systems. This will also require the development of suitable interfaces between the specified systems.

3.5 Theoretical and mathematical foundations

Theoretical and mathematical physics provides methods for describing the properties of composite systems that interact with each other or with the environment and studies the underlying principles.

As part of this, it brings together atomic, quantum, solid-state and biophysical research on one hand and the abstract models of quantum information theory and mathematics on the other. On this basis, methods are developed with which the coherence and entanglement of states can be controlled, optimized and protected. A key sub-area here is describing and avoiding decoherence with the objective of creating the basis for executing newly developed quantum algorithms and applications using quantum technology.

3.5.1 Quantum error correction

Quantum systems are particularly sensitive to environmental disturbances, particularly quantum memories and computers. The isolation and stabilization of quantum systems therefore plays a key role in quantum technology. As quantum information can only be copied and compared in exceptional cases without disturbing the state, many of the established concepts from conventional information processing are not directly transferable. Nevertheless, it is possible to protect quantum information against external disturbance and errors which can be caused by technical imperfections. There are two basic types of error correction:

- Passive methods store the quantum information so that it is disturbed as little as possible, for example in subsystems free of decoherence. However, this makes the processing of quantum information more difficult, and the technical limits mentioned remain.
- Active methods attempt to identify errors by measuring part of the quantum system and then to correct them. Of course, the necessary interaction with the system for this must occur in such a way that no more errors are

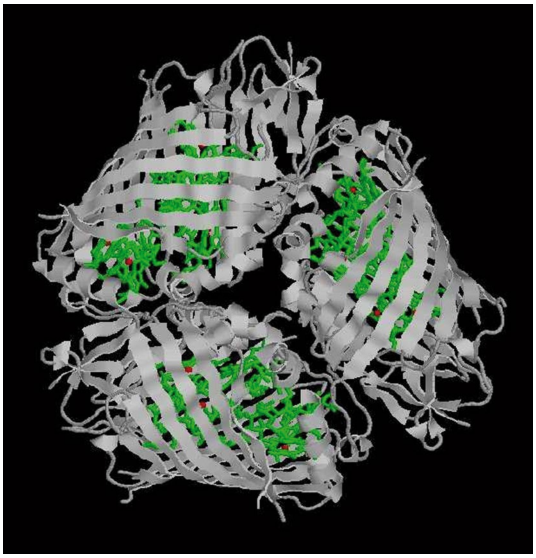

Fig. 5 The FMO complex in green sulphur bacteria carries light energy from chlorophyll (*green*) to reaction centres for chemical processes (*red*). The energy transport uses an interaction of coherence and decoherence. Wikipedia/Julian Adolphs (license: CC BY-SA 3.0)

created than are corrected. (This is known as fault-tolerant quantum computing.)

Many of the exact error mechanisms have not yet been adequately investigated in specific systems, it is usually very general error models that are considered on a theoretical level. More exact identification of error sources would facilitate adaptation of the error correction to specific systems. Methods for optimal control could also be used for this. Methods for stabilizing quantum systems could also lead to greater efficiency and precision in other quantum technologies.

3.5.2 Quantum information theory

In addition to the design of codes and correction methods, quantum information theory works on the general limits of information transmission and processing using quantum mechanical systems. For example, while two conventional information channels can carry twice as much information, in quantum mechanics the total capacity can exceed the two-fold measure of the two individual channels (superadditivity). Such effects occur not only when transmitting quantum information, but also when transmitting conventional information via quantum mechanical channels. Thus, quantum technology can also facilitate a better use of conventional resources.

On the other hand, due to superadditivity, the capacity of quantum channels is only precisely known in a few cases. Quantum capacity is, therefore, an important topic of research that opens up many scenarios: In addition to the transmission of conventional information or quantum information, there are investigations to determine whether and with what efficiency it is possible to transmit information via a particular quantum channel so that it remains concealed from a third-party (quantum cryptography). In certain cases, additional resources such as the exchange of entangled states or even an additional conventional two-way channel lead to more efficient systems.

3.5.3 Computability theory and complexity theory

Some algorithms have already been developed for quantum computers, which solve conventionally difficult problems such as the factorization of large numbers or the calculation of discrete logarithms efficiently. The difficulty of a problem is characterized generally in complexity theory by how the effort for the algorithm used relates to the length of the input register. For example, in the factorization problem the effort is the number of calculation operations and the input length is the number of digits of the number being factorized. However, up to now there are essentially only two types of quantum mechanical algorithms known which solve problems more efficiently than conventional computers: Shor's algorithm and Grover's algorithm, which are based on quantum Fourier transforms. Many unresolved questions remain here, including which types of conventionally difficult problems quantum computers can solve efficiently.

3.5.4 Nonequilibrium processes and quantum biology

It has been recognized in recent years that the interaction between a system and its environment can also have benefits. Entanglement can thus also be produced in stationary nonequilibrium systems. In the context of biological systems, this can lead to significantly increased transport efficiency for electronic excitations which significantly improves the efficiency of these systems. Biological systems are often characterized by strong interaction with the environment, and a synergy of coherence and decoherence can be important for their optimal function. Particularly in the biological environment, these effects have only recently been accessible for direct experimental testing.

They could bring about new applications and structures in which the interplay between quantum effects and the often unavoidable environmental noise is optimized. Key examples of systems under investigation in quantum biology are the Fenna–Matthews–Olson (FMO) complex (see Fig. 5) and other bacterial and vegetable light-harvesting complexes such as LH1, LH2 or PSII. In addition, magnetoreception in animals and the sense of smell in humans and animals is being studied, with prospects of triggering fundamentally new approaches in sensor technology.

3.5.5 Entanglement theory and the dynamics of multi-component quantum systems

A fundamental observation is that the number of parameters necessary to describe a multi-component system increases exponentially with the number of components. This explains, on the one hand, the high performance capacity of quantum computers, but on the other hand it also makes it difficult to characterize the conditions and dynamics of experimental quantum systems efficiently and to verify them. Methods to describe the dynamics of multi-component quantum systems are extremely important to provide theoretical support for the experimental research. The dynamics and probably the identification of ground and excited states in such systems are complex, and the effort to simulate them on conventional computers generally increases exponentially.

Solutions with new approaches combine methods from various fields of research, which must first be adapted to the particular requirements of quantum technology. These include methods from optimization theory, signal processing and the theory of strongly correlated systems. Various subject areas such as physics, mathematics, information theory and signal processing must be brought together in an interdisciplinary manner. This work can, in turn, be expected to have positive effects on conventional problems in the areas mentioned which have remained unsolved up to now.

3.6 Quantum control

The term quantum control is used to describe an entire class of modern methods for influencing physical and chemical reactions and processes with adapted laser pulses. The coherence properties of lasers play a key role here.

3.6.1 Development and methods

Since its invention in 1960, the laser has served as an ideal light source for both high-precision spectroscopy and the analysis of dynamic material processes. At the same time, the laser also raised hope that processes could be selectively influenced by its use.

In the beginning, such ideas were based primarily on the laser's monochromatism. The hope was that with selective excitation of particular vibration or electron states, specific chemical bonds could be broken up or formed. The laser was to function as a sort of "scissors and glue" for separating or forming individual bonds. However, despite considerable efforts over a number of decades, only rather limited success was achieved with this type of laser chemistry. In the early stages, apart from the successful exceptions, such as with isotope separation, the concepts failed primarily due to the high speed with which the energy supplied by the laser is distributed in solid bodies and in larger isolated molecules. In most cases, the laser only heated the material.

The situation changed dramatically in the late 1980s. The problem just described was overcome (or circumvented) by a number of important contributing developments which enabled reactions to be controlled using lasers; researchers learned how to apply the coherence properties of the laser selectively. The molecules studied were now understood as true quantum systems, which were excited to superposition states by superposing multiple laser fields concurrently or in a sophisticated time sequence. This allowed the population of excited system states to be selectively influenced just by a variation of the phase between two laser fields.

The second decisive advancement resulted from high-speed physics, which, since the late 1980s, has provided ultrashort laser pulses in a broad spectral range with increasing repetition rate and intensity. By focusing these ultrashort laser pulses on molecules, progress was achieved in femtochemistry, which was initially mainly applied to precision analysis of the temporal progression of physical and chemical processes.

Today, ultrahigh intensity laser pulses of just a few femtoseconds[25] can be produced in the visible spectrum. These comprise only a few oscillations of an electromagnetic wave, and their phasing can be precisely controlled. In the soft X-ray spectrum, pulses can now be produced with durations under 100 attoseconds. In the far infrared spectrum wave packets of less than a single oscillation can be produced, the electric field distribution of which can be measured exactly. In parallel to this development, efficient methods were developed to allow the available laser pulses to be shaped literally with a large spectral bandwidth and to be adapted in almost any way in their temporal and spectral progression.

These new possibilities were initially used to influence the chemical and physical behaviour of simple, free molecules and to allow reactions to run selectively. Incredible progress has been achieved, particularly in the past 15 years.

It has long been possible to study objects beyond the size of small molecules, from macromolecules and biological building blocks in solid and liquid form up to semiconductors and transparent materials for optoelectronic components.

Modern quantum control experiments are further distinguished by the use of sophisticated feedback methods. The high repetition rates of the femtosecond lasers used enables a particular experiment to be repeated thousands of times, varying the shape of the laser field used each time. After

[25] One femtosecond (fs) = 10^{-15} s; one attosecond (as) = 10^{-18} s.

each experiment, the result is compared with a prespecified target value, and the laser pulse used is modified until the desired outcome is achieved. Depending on the strategy applied, a distinction is made between adaptive and real-time feedback. Genetic algorithms modelled on biological development processes have proven to be particularly effective.

The close integration of theory and experiment is critical for these strategies to succeed. Both fundamental theoretical considerations for conducting such experiments and their limits are explored in the process, and favourable strategies for particular process types are estimated in advance. The various methods can be grouped together as "quantum physics for optimal control".

Finally, it should be noted that modern nuclear magnetic resonance spectroscopy in the broadest sense also uses coherent control strategies of the type discussed here. However, the objective is almost entirely focused on determining the structure of large molecules spectroscopically.

3.6.2 Applications and outlook

In the past two decades, new principles and efficient processes for quantum control have been developed based on cleverly shaped, ultrashort laser pulses. These have enabled physical and chemical reactions and processes to be influenced and controlled selectively. We cannot yet begin to predict the significance of the wealth of applications that this has made possible as, up to now, the basic concepts and methods have for the most part only been tested with relatively simple cases.

The exploration of the range of possibilities for quantum technology has only just begun.

Only a small selection of examples of the achievements and the areas and strategies currently under investigation can be outlined here. They range from optical quantum systems and technology, atoms and simple molecules, to semiconducting structures, the microprecision machining of transparent materials, and controlling larger molecules of biological relevance.

The optimization of laser systems is one of the most successful direct applications of adaptive feedback. This is used, for example, to generate optimized laser pulses. These methods have also been proven useful in building X-ray lasers in the laboratory or for the spatially modulated wave front control of pulsed lasers. Coherent feedback has also recently been tested successfully to suppress noise in laser systems. Beyond this, a whole range of optical measurement methods are conceivable, which can be improved by coherent control or would not be possible without it. Here, temporal and spectral formation of laser pulses are not the only key factors; their spatial influence will also play an increasingly important role The ability to modify the near field of focused light beams using adaptive feedback control leads opens up interesting prospects for nanostructuring materials.

This also leads to methods for material processing in the interior of transparent materials. Femtosecond laser pulses and adaptive feedback can be used to produce particularly uniform waveguides and other photonic structures, for example, or to achieve parallelization methods with spatial pulse shaping.

In contrast to initially overoptimistic expectations associated with the term "laser chemistry", quantum control is not expected to be usable for efficient chemical synthesis processes in the foreseeable future, even though many individual examples of efficient reactions have been demonstrated which can only be promoted or inhibited in this way. Basically, the cost per photon required is usually not in a reasonable proportion with the price of the reaction product produced. However, there are exceptions where successful, technically usable innovations by chemical synthesis can be expected.

Quantum control methods have been developed with particular success in analytical applications and measurement technology and for applications in physical, chemical and biological research as well as nanotechnology. The study of many issues of basic research has benefited considerably from these methods, particularly from adaptive feedback. This is true, for example, for the investigation of photo-induced molecular reactions, the understanding of chemical reactions, catalysis, solution processes and corrosion research. Considerable progress was also achieved in the sensitive and selective determination of molecular states, the spatial orientation of molecules, and in analytical methods for chemistry and biology as a whole, which is important for medical and pharmaceutical research. Thus, for example, various protein functions can be documented with fluorescence microscopy, and mass spectrometry methods can be improved by using specially shaped, coherent femtosecond laser pulses to generate or partially fragment the molecular ions under investigation.

Particle acceleration studies with extreme intensity, ultrashort laser pulses are also promising.

Finally, considerations of using quantum control methods to harness molecular vibrations for quantum computers are worthy of note: this is a field with potential of great theoretical interest which has not yet been taken to the experimental level. This brings us back to the topics presented earlier in this section.

3.7 Atomic quantum sensors and matter wave optics

Atomic quantum sensors have the potential to become a key technology for the precise determination of a body's acceleration and rotation, particularly for basic research in physics. While classical optics exploits the properties of light waves, quantum mechanics states that even matter can behave like a wave under certain circumstances. Atomic quantum sensors use these wave properties of atoms and molecules.

Matter wave optics is still a new science, but its progress has been rapid, with a series of discoveries, some of which were honoured with the Nobel Prize (laser cooling in 1997 and Bose–Einstein condensation in 2001). Interferometry with nonclassical states of matter enables extremely high accuracy measurement; this is used, for example, to determine charges and masses or to measure gravitational waves. In the past, it was assumed that quantum objects are microscopically small, in contrast to visible objects, but macroscopic objects such as Bose–Einstein condensates show that this generalization is not correct.

Atomic quantum sensors can be used in very many ways, such as for the implementation of measurement units, determination of raw material reserves, navigation, the geological study of the Earth and environmental monitoring. Furthermore, atom- and molecule-based quantum sensors are already today able to provide precision measurements to test fundamental theories beyond the standard model or temporal variation of fundamental physical constants, thus contributing to our fundamental understanding of the world just as much as high-energy experiments with large accelerator facilities. In all these fields, their advantages arise directly from basic quantum effects, and considerable progress is to be expected with regard to performance, usability and efficiency, for example in the use of transportable components in satellites or on Earth.

3.7.1 Geological study of the Earth

Quantum sensors are extremely sensitive to gravity and to gravitational changes, to magnetic fields and to the rotation of the Earth and are, thus, particularly suited for applications in geological sciences and for Earth observation. For example, they can be used to precisely measure gravity on the Earth's surface and to produce gravitational maps. The applications for such gravitational cartography range from the search for raw materials such as petroleum and mineral deposits to plate tectonics and earthquake prediction, and measuring the effects of climate change such as the increase in sea level. Thus, even small improvements in measurement sensitivity can have an important social and economic impact. They could help to record the temporal change of the Earth's rotation axis, which cannot be predicted due to the complex processes in the interior of the Earth.

A primary advantage of quantum sensors is that they do not experience drift due to the principles on which they are based and thus do not require routine recalibration. As they do not require stabilized platforms, they are particularly well-suited for use in aviation and maritime applications. In the laboratory, rotation sensors have already surpassed the performance capabilities of conventional devices such as ring laser gyroscopes for aircraft navigation.[26] A quantum gyro scope could therefore be part of future navigation systems which do not rely on satellite positioning (such as GPS or Gali leo) and would also work under conditions of poor visibility in inner cities, in tunnels, in mountainous terrains and in forests.

3.7.2 Applications in space

Atomic quantum sensors are much more precise under zero gravity conditions than on Earth, which also makes them interesting for basic research in physics. They could be used as a long-term inertial reference for astronomy or space navigation or even for missions intended to describe and observe the Earth's gravitational field precisely. The sensors could be the key to new experiments, for example in gravitational wave astronomy or in the search for a general theory to unify quantum and gravitational theory—one of the primary objectives in physics since the twentieth century.

3.7.3 Measurement standards

Since quantum sensors detect the inner structure of atoms they are also suited for defining basic units of the international system of units (SI).[27] Atomic clocks have been used already to redefine the second as a unit of time and the metre as a unit of length. The unit for mass, the kilogram, is the last basic unit still defined by a material object of dubious longevity, the original kilogram. A promising approach to overcome this unsatisfying state of affairs is offered by the Watt balance, which determines mass by measuring electric current and resistance. Current and resistance can be expressed with very high precision using two quantum effects, the Josephson and quantum Hall effects, which leads to a link between the macroscopic mass and Planck's constant, a fundamental physical constant. Such a Watt balance requires a gravity reference of a precision hardly achievable with conventional sensors but which should be within the realm of possibility for a quantum gravimeter.

[26] A gyroscope is a device which determines spatial orientation.

[27] These SI (French, *Système international*) units include basic units such as the metre, kilogram, second, ampere and Kelvin.

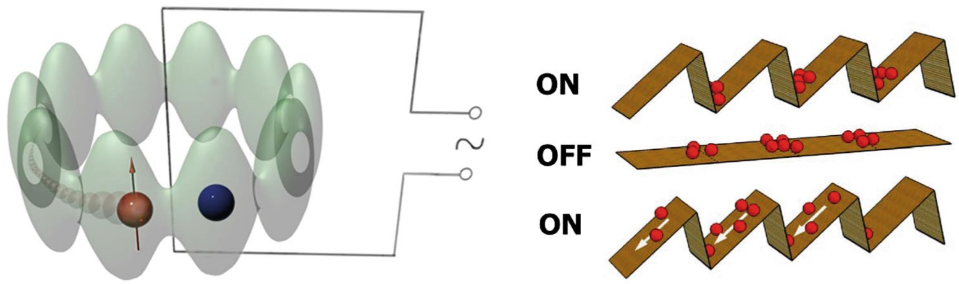

Fig. 6 *Left* An electric quantum engine—two atoms which can interact locally with one another are placed in a ring-shaped trap of light, with one (*red*) driven by a time-dependent magnetic field and working against external fields. On the *right* A quantum ratchet—by switching an asymmetrical sawtooth potential on and off, particles can be transported due to Brownian movement. (*Left* Ponomarev et al. [11]; *right* Hänggi [8])

3.8 Special quantum technology

3.8.1 Quantum electronics

Quantum electronics generally comprise all electronic components and systems in which the quantization of light, charge or electron spin is crucial for their function. Along with the interaction of photons with charges, relevant effects also include superconductivity (the formation of electron pairs) and nonvolatile flash memory (with the tunnel effect). Many parasitic effects such as shot and flicker noise are also based on quantum phenomena which are caused by the effect of individual charges.

On the other side are classically observable factors such as current or power of the macroscopic nature, not photons or electrons. Thanks to progress in micro- and nanoelectronics, structures can be made in which individual quantized charges, photons or spins do in fact form the signals or determine the functionality.

High sensitivity measurement techniques based on quantum effects play a key role in the development of such structures and systems, for example the tunnel effect in scanning tunnelling microscopy or exchange and correlation forces in exchange force microscopy.

Since only low signal strengths can be generated due to the very small dimensions involved, such nanoscale systems must be embedded in input and output structures (not part of quantum technology) in order to use them effectively. Like-wise, it must be possible to produce many similar structures. Satisfying both these conditions can be more difficult than implementing the element of quantum technology itself. One example is the single electron transistor, in which individual electrons control currents or charge packets comprised of single electrons are transported. Significant progress has been made towards a quantized current standard on this basis in recent years. Thus, currents in the nanoampere range can already be produced with great precision by single electron pumps. In the near future, such single electron pumps could help to close the "metrological triangle" comprised of current, voltage and frequency.

A further example which has attracted much attention recently is nanomagnetic logic. Here, the interaction of nanomagnets is used for non-volatile processing units which have the potential to be particularly low-loss. This offers several benefits, such as no electrical connection cables being required, because the interaction and the energy feed occur via magnetic fields. This interaction can take place in the plane and between nanomagnets arranged perpendicularly over one another, making a space-efficient, three-dimensional arrangement possible.

This concept is scalable to atomic sizes in principle, and recently the first spin-based logic elements comprised of single atoms on surfaces were demonstrated. Since, in this case, no electric charges flow, such purely spin-based nano components avoid problems which result in conjunction with contact resistances which are too large and insufficiently reproducible, as is otherwise characteristic of nanoelectronic components. Using the spin degree of freedom opens up new possibilities for atomic spin logic and memory components as well as for quantum information processing (quantum spintronics).

However, it requires that the nanoscale functional elements must be embedded in the macroscopic environment, for which high performance and secure input and output structures are required. If these components are used in large numbers, expensive equipment such as tunnelling microscopes, atomic force microscopes and the like are not suited as output units, but instead integrated interfaces must be created with the quantum technological elements. Simple solutions are input structures made of energized lines and output structures comprised of Hall sensors or GMR elements.[28]

[28] GMR = Giant Magnetoresistance; magnetic field-dependent resistance.

Coupling solid-state-like nanostructures and ultracold quantum gases is also interesting. Highly precise measurements could be performed with these, which are based on the state changes of an ultracold quantum gas and transmit electric signals in solid state-based nanoelectronic components for further processing.

During the transition from basic research to applied research, attention should be given at the earliest stage possible that the components required can be manufactured reproducibly and cost-effectively and that they work reliably under realistic conditions. One difficulty here is that operation at very low temperatures is required for many effects. In elements where only one or a few quantum are responsible for the function, the uncertainty relation also plays a large role.

3.8.2 Many-body correlations

In quantum mechanical systems, many-body correlations arise spontaneously, which also offer numerous technical possibilities for application. The best-known example is probably superconductors, which are used today in many ways in electronics, power current technology and medical devices. High temperature superconductors are of particular interest.

They already become superconductive at transition temperatures just below about −180 °C. The higher the transition temperature, the less effort required to cool superconducting components. One objective of basic research is to elucidate the mechanisms underlying superconduction so that the transition temperatures can be calculated mathematically. Spectroscopic and solid-state transport experiments are the primary means used for this, as well as analytical and numeric methods.

The use of ultracold gases for analogue quantum simulation of strongly interacting electron systems in solid bodies is a new research strategy currently subject to intense discussion, for which initial experiments have already been conducted. Starting from the fundamental understanding of quantum mechanical many-body systems up to now, work has begun to influence the microscopic interactions between quantum particles selectively in order to optimize the properties of a macroscopic number of particles. In laser-cooled atomic gases, the interactions between the atoms are relatively simple to influence. However, it is not easy to achieve the low temperatures required for the condensation of many-body systems. Ultrashort, precisely adapted light pulses over a broad frequency range are useful to control the phase behaviour of electron systems in the solid state within femto- or attoseconds. Here initial, promising experiments have been conducted as well.

Moreover, increasing progress is being made in applying the nano structuring methods established in semiconductor physics to materials with strongly interacting electron systems, thus selectively influencing the electronic correlations. A long-term objective is to stabilize macroscopically phase-coherent states such as superconduction even at room temperature, to further increase the application potential of quantum technology.

3.8.3 Quantum machines

If entire clouds of atoms can be selectively trapped and processed, then machines could be devised which can perform work using focused control and monitoring fields in a fully coherent manner, without friction losses. Possible concepts for this include Brownian quantum motors, single atom motors and hybrid structures. Motors on the smallest scale are designed for them using cold atoms in optical lattices and implemented experimentally (see Fig. 6). However, the lack of friction poses a challenge because it is difficult to start such machines and to stop them. However, the advantage of such applications would be that they can operate with degrees in efficiency close to one (in nonequilibrium).

Also interesting is the investigation of the statistical properties, such as quantum mechanical thermalisation and relaxation of finite quantum systems.

This can occur either in an isolated state or in conjunction with mutual interaction inside of constructed quantum architectures. Quantum machines are still currently the subject of basic research with theoretical and experimental feasibility studies.

3.8.4 Phononic quantum systems

Along with the quantization of light, charge and electron spin, the quantization of crystal lattice vibrations (phonons) also has many applications. It can be achieved in a manner similar to quantized electron systems such as quantum wells, quantum wires and quantum dots by combining materials of different mechanical properties such that the dimensions of the individual materials, thickness or diameter, are less than the mean free path of phonons. As in solid bodies, this is generally significantly larger than the de Broglie wavelength of electrons—300 nm versus 10 nm in silicon—electrical and thermal conductivity can be decoupled. The heat transmission by phonons can be suppressed while the electron system continues to behave in a classical manner. A 200-fold reduction in thermal conductivity was demonstrated in silicon nanowires using the effect described above, while the electrical conductivity was reduced to a mere tenth of its previous value. Possible applications for such a material include infrared detectors with which the sensor signal—the increase in temperature—is evaluated electrically. The parasitic heat bridge via a low impedance electrical feed line is largely avoided by this effect (meeting the high requirement for sensitivity).

A second application is thermoelectric generators which transforms the heat into usable electric energy. The distinguishing characteristic of efficient generators is that they have a high electrical conductivity (low internal resistance) in conjunction with low thermal conductivity (high parallel thermal resistance). The greater the ratio of electrical to thermal conductivity, the more efficiently the material transforms heat to electric energy. In addition, decoupling thermal conductivity from electrical conductivity leads to considerable improvement. A tripling of the ZT value[29] has already been demonstrated using such nanostructured materials versus the conventional value. The following example highlights the potential of thermoelectric generators: a 125 kW combustion engine produces on average about 5 kW of waste heat via the exhaust tract during an average driving cycle. With a thermoelectric generator with a ZT value of 25[30] and an efficiency of 6 %, the resulting average electrical power is 300 W, which would be sufficient to supply the onboard electronic system of a car with energy.

It is possible to produce phononic band gaps (phononic crystals) using periodically repeating structures. For example, this effect could play a role in components in which the phononically coupled relaxation of high energy excited quantum states is to be suppressed.

Such an effect makes hot-carrier solar cells with a potential theoretical efficiency of 66 % possible, in which excited charge carriers are extracted in the direction of the band edge high into the band prior to their relaxation, and their energy is used before recombination. The objective is to slow the recombination process for the extraction. In quantum dots made of cadmium sulphide, this process has already been slowed from 10 picoseconds to one nanosecond. However, this is far removed from timescales relevant to application, which are in the microsecond range. The examples show nonetheless the significance that basic research in phonon scattering in solid bodies can have for future applications.

3.8.5 Energy storage in quantized systems

Renewable energy systems such as wind turbines, solar cells and concentrated solar power (CSP) plants provide electrical current as primary energy. However, only CSP is viable for base load power, because the heat which is not required immediately for load requirements can be stored economically for days. Electrical energy from photovoltaic or wind power plants that is not needed immediately should, in the ideal case, be stored temporarily in electric storage media to prevent losses from energy conversion—to hydrogen, for example. However, particular applications, such as load distribution in electric supply networks, economical expansion of electromobility, independent sensor nodes for an "environmentally supported life" or mobile communication and information systems, are significantly dependent on the availability of an efficient, scalable and environmentally compatible storage of electrical energy. Electrical storage such as lithium ion batteries is still expensive, however, and limited in energy and power density as well as service life. Another problem of lithium ion batteries is the uneven, slower mobility of ions compared to capacitive energy storage, in which only electrons need to be moved. As a result, lithium ion batteries are not yet able to deliver or absorb high power peaks in short periods. Moreover, the ion exchange is associated with volume changes, which leads to mechanical stress of the electrode material and thus limits the service life of these batteries. In addition, the energy and power density achieved at present is insufficient and the system costs associated with key applications, such as electro-mobility, are too high. On the other hand, current capacitive energy storage media have too low of a specific energy storage to replace lithium ion batteries. However, due to their ability to charge and discharge quickly, they have been an active subject of research for years. Capacitive energy storage is distinguished by high electrical permittivity and high dielectric field strength. Applying an external electric field to classical dielectric materials creates a dipole field which opposes the external field. In the simplest case, this polarization is attributable to the microscopic displacement of the electron shell with respect to the positively charged nucleus, whose degree of deflection determines the strength of the polarization, the permittivity and the magnitude of capacitance.

Structures are now conceivable in which the effect of polarization no longer occurs on the atomic scale but between coupled quantum or nanostructures. The charge transfer necessary to form the dipole field is then assumed by the tunnel effect of the charge carriers between adjacent quantum structures. In such a system, the deflection of the dipole is no longer limited to fractions of the lattice constants, but instead can extend to several nanometres. This could allow high permittivity to be achieved due to the strong deflection of the dipoles despite the low volume density of quantum dots compared to solid state. It is thought that a system of coupled quantum dots could achieve specific energy storage densities of up to 1000 Wh/kg, which is five times the capacity of lithium ion batteries today.

[29] The ZT value is a dimensionless variable which affects the efficiency of thermoelectric generators. The larger its value, the closer the efficiency is to the thermodynamic maximum.

[30] The best materials known up to now have a ZT value of one.

3.9 Methodology

Participants in the working group

Coordinator

Prof. Wolfgang P. Schleich	Ulm University

Assistant to the coordinator

Dr Kedar S. Ranade	Ulm University

The following people contributed to this report
(* = member of the drafting committee)

Prof. Markus Arndt	University of Vienna (Austria)
Prof. Markus Aspelmeyer	University of Vienna (Austria)
Prof. Manfred Bayer*	TU Dortmund University
Prof. Gunnar Berg	Martin Luther University Halle-Wittenberg
Prof. Tommaso Calarco	Ulm University
Prof. Harald Fuchs	University of Münster
Prof. Elisabeth Giacobino	Paris-Sorbonne University (France)
Dr Markus Grassl	National University of Singapore
	Max Planck Institute for the Science of Light, Erlangen
Prof. Peter Hänggi	University of Augsburg
Prof. Wolfgang M. Heckl*	Deutsches Museum, Munich
	Technische Universität München
Prof. Ingolf-Volker Hertel	Max Born Institute, Berlin
	Humboldt-Universität zu Berlin
Prof. Susana Huelga	Ulm University
Prof. Fedor Jelezko	Ulm University
Prof. Bernhard Keimer	Max Planck Institute for Solid State Research, Stuttgart
Prof. Jörg P. Kotthaus*	Ludwig-Maximilians-Universität München
Prof. Gerd Leuchs*	Max Planck Institute for the Science of Light, Erlangen
Prof. Norbert Lütkenhaus	University of Waterloo (Canada)
Prof. Ueli Maurer	ETH Zurich (Switzerland)
Prof. Tilman Pfau*	University of Stuttgart
Prof. Martin B. Plenio	Ulm University
	Imperial College London (United Kingdom)
Prof. Ernst Maria Rasel*	Leibniz Universität Hannover
Prof. Ortwin Renn	University of Stuttgart
Prof. Christine Silberhorn	University of Paderborn
Prof. Jörg Schmiedmayer	University of Vienna (Austria)
Prof. Dr. Doris Schmitt-Landsiedel	Technische Universität München
Prof. Kurt Schönhammer	Georg-August-Universität Göttingen
Prof. Alexey Ustinov*	Karlsruhe Institute of Technology
Prof. Philip Walther	University of Vienna (Austria)
Prof. Harald Weinfurter*	Ludwig-Maximilians-Universität München
Prof. Emo Welzl	ETH Zurich (Switzerland)
Prof. Roland Wiesendanger	University of Hamburg
Prof. Stefan Wolf	ETH Zurich (Switzerland)
Prof. Anton Zeilinger	University of Vienna (Austria)
Prof. Peter Zoller	University of Innsbruck (Austria)

Contributors from industry

Dr Klaus Dieterich	Robert Bosch GmbH

Scientific consultants to the working group

Dr Christian Anton	German National Academy of Sciences Leopoldina
Dr Stefanie Westermann	German National Academy of Sciences Leopoldina

Reviewers

Prof. Alfons Bora	Bielefeld University
Prof. Wolfgang Ketterle	Massachusetts Institute of Technology: MIT
Prof. Carsten Könneker	Karlsruhe Institute of Technology
Prof. Christoph Kutter	Fraunhofer Research Institution for Microsystems and Solid
	State Technologies, Munich
Prof. Hans Wiesmeth	TU Dresden

3.9.1 Procedure

At the request of the German National Academy of Sciences Leopoldina, on 27 April 2009 the Standing Committee of the Leopoldina set up a working group on quantum technology.

In order to incorporate international developments in quantum technology, the working group led by Prof. Wolfgang Schleich organised the Conference on Quantum Technology, which was held on 8–9 May 2011 in the Deutsches Museum in Munich. As part of the event, 23 experts from eight different countries shed light on the latest experimental and theoretical developments to more than 200 participants. A detailed account of the conference can be found in the 2011 Leopoldina annual report.

In October 2011, the Center for Integrated Quantum Science and Technology IQST was opened at Ulm University. Dr Klaus Dieterich, chairman of the management board of corporate research at Bosch, gave a lecture on "Quantum Effects—An Opportunity for Industry?" at a symposium. After the event, Prof. Schleich asked Dr Dieterich to include his contribution in the current report.

The working group's drafting committee met on 11 April 2013 in the Deutsches Museum in Munich to prepare the summary and discuss key findings.

The first version of the manuscript was annotated by Manfred Lindinger (Frankfurt). Niels Boeing (Hamburg) edited the version of the statement intended for review, and Martin Radke (Bremen) edited the final version.

The Standing Committee of the German National Academy of Sciences Leopoldina adopted the report on 4 December 2014.

Appendix

Funding schemes and projects

A large number of projects and research groups in the area of quantum technology receive funding in Germany. Sponsors include the German Research Foundation (DFG), the Max Planck Society, the German Federal Ministry of Education and Research (BMBF), as well as a number of other regional organisations. The EU also provided funding as part of its fifth, sixth and seventh Framework Programmes.

A good overview of these projects is provided by the QIPC (Quantum Information Processing and Communication) roadmap QUROPE/QUIET2, available online at http://qurope.eu/projects/. The following is a list of some of these projects; the list serves as an example and is by no means exhaustive.

AQUTE	Atomic Quantum Technologies (EU Integrating project)
CORNER	Correlated Noise Errors in Quantum Information Processing (EU STREP project), 2008–11
FINAQS	Future Inertial Atomic Quantum Sensors
GOCE	Gravity Field and Steady-State Ocean Circulation Explorer
HIP	Hybrid Information Processing (EU STREP project), 2008–11
ICT 2020	Information and Communication Technologies (German Federal Ministry of Education and Research/BMBF) with the collaborative projects: • QuOReP (quantum repeater platform with quantum optical methods) • QuaHL-Rep (quantum semiconductor repeaters) • QUIMP (quantum interface between optical and microwave photons) • IQuRe (quantum repeater information theory)
IQS	Inertial Atomic and Photonic Quantum Sensors: Ultimate Performance and Application
LISA-II	Laser Interferometer Space Antenna II
PICC	Physics of Ion Coulomb Crystals (EU project), 2010–2013
Q-ESSENCE	Quantum Interfaces, Sensors, and Communication based on Entanglement (EU Integrating project), 2010–2014
QNEMS	Quantum Nanoelectromechanical Systems, an FET STREP EU project 2009–2012
QUANTUS	Quantum Gases in Microgravity
SECOQC	Secure Communication using Quantum Cryptography (Sixth EU Framework Programme)
SFB 450	Collaborative Research Centre for the Analysis and Control of Ultrafast Photoinduced Reactions
SFB 631	Solid State Based Quantum Information Processing: Physical Concepts and Materials Aspects, 2003–2015)
SFB/TRR 21	Control of Quantum Correlations in Tailored Matter (CO.CO.MAT)

In addition, support was provided for individual researchers through, for example, Alexander von Humboldt Professorships. These included David DiVincenzo (RWTH Aachen), Martin Plenio (Ulm) and Vahid Sandoghdar (Erlangen-Nürnberg).

Extended bibliography

Books

[1] Audretsch, J.: *Verschränkte Welt. Faszination der Quanten*, Wiley–VCH, 2002.
[2] Nielsen, M. A.; Chuang, I. L: *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.
[3] McManamon, P.; Willner, A. E. et al.: *Optics and Photonics – Essential Technologies for Our Nation,* The National Academies Press, 2013.
[4] Peres, A.: *Quantum Theory: Concepts and Methods,* Springer-Verlag, 1995.
[5] Renn, O.; Zwick, M. M.: *Risiko- und Technikakzeptanz*, Springer-Verlag, 1997.
[6] Zeilinger, A.: *Einsteins Schleier: Die neue Welt der Quantenphysik*, Goldmann Verlag, 2005.

Review articles

[1] Spektrum Dossier 4/2010: "Quanteninformation".
[2] "The Age of the Qubit: A new era of quantum information in science and technology", Institute of Physics, 2011.
[3] Cirac, J. I.; Zoller, P.: "New Frontiers in Quantum Information with Atoms and Ions", *Physics Today* (2004), pp. 38–44.
[4] Coffey, V. C.: "Next-Gen Quantum Networks", *Optics & Photonics News* (March 2013), pp. 34–41.

[5] Cronin, A. D.; Schmiedmayer, J.; Pritchard, D. E.: "Optics and interferometry with atoms and molecules", *Reviews of Modern Physics*, volume 81 (2009), pp. 1051–1129.
[6] Hänggi, P.: "Harvesting randomness", *Nature Materials*, volume 10 (2011), pp. 6–7.
[7] Ladd, T.D.; Jelezko, F.; Laflamme, R.; Nakamura, Y.; Monroe, C.; O'Brien, J.L.: "Quantum computers", *Nature*, volume 464 (2010), pp. 45–53.
[8] Leuchs, G.: "Wie viel Anschauung verträgt die Quantenmechanik?", *PdN – Physik in der Schule*, volume 62 (2013), p. 5.
[9] Monroe, C.: "Quantum Information Processing with Atoms and Photons", *Nature*, volume 416 (2002), pp. 238–246.
[10] Zoller, P. et al.: "Quantum information processing and communication", *The European Physical Journal D—Atomic, Molecular, Optical and Plasma Physics*, volume 36 (2005), pp. 203–228.

Individual works

[1] Aspect, A.; Dalibard, J.; Roger, G.: "Experimental Test of Bell's Inequalities using time-varying Analyzers", *Physical Review Letters*, volume 49 (1982), pp. 1804–1807.
[2] Bell, J. S.: "On the Einstein–Podolsky–Rosen-Paradox", *Physics*, volume 1 (1964), pp. 195–200.
[3] Bennett, C.H.; Brassard, G.: "Quantum Cryptography: Public Key Distribution and Coin Tossing", *Proceedings of IEEE International Conference on Computers, Systems & Signal Processing, Bangalore, India*, pp. 175–179 (1984).
[4] Cirac, J.I.; Zoller, P.: "Quantum Computations with Cold Trapped Ions", *Physical Review Letters*, volume 74 (1995), pp. 4091–4094.
[5] Einstein, A.; Podolsky, B.; Rosen, N.: "Can quantum-mechanical description of physical reality be considered complete?", *Physical Review*, volume 47 (1935), pp. 777–780.
[6] Ekert, A.K.: "Quantum cryptography based on Bell's Theorem", *Physical Review Letters*, volume 67 (1991), pp. 661–663.
[7] Feynman, R.P.: "Simulating physics with computers", *International Journal of Theoretical Physics*, volume 21 (1982), pp. 467–488.
[8] Heisenberg, W.: "Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik", *Zeitschrift für Physik*, volume 43 (1927), pp. 172–198.
[9] Joy, B.: "Why the future doesn't need us", *Wired*, April 2000 (see http://www.wired.com/wired/archive/8.04/joy_pr.html)
[10] Schrödinger, E.: "Die gegenwärtige Situation in der Quantenmechanik", *Die Naturwissenschaften*, volume 23 (1935), pp.807–812, 823–828, 844–849.

Literature

1. C.H. Bennett, G. Brassard, Quantum cryptography: public key distribution and coin tossing, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, vol. 175 (New York, 1984), pp. 175–179
2. M. Born, W. Heisenberg, P. Jordan, Zur Quantenmechanik II. Zeitschrift für Physik **35**, 557 (1926)
3. J.I. Cirac, P. Zoller, Quantum computations with cold trapped ions. Phys. Rev. Lett. **74**, 4091–4094 (1995)
4. D.P. DiVincenzo, Topics in quantum computers, in *Mesoscopic Electron Transport*, vol. 345, NATO ASI Series E, ed. by L. Kowenhoven, G. Schön, L.L. Sohn (Kluwer Academic Publishers, Dordrecht, 1997), p. 657
5. A. Einstein, B. Podolsky, N. Rosen, Can Quantum-mechanical description of physical reality be considered complete? Phys. Rev. **47**, 777 (1935)
6. A.K. Ekert, Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. **67**(6), 661–663 (1991)
7. R. Grötker, Wie der Laser ans Licht kam. Max Planck Forschung **4**(2009), 84–90 (2009)
8. P. Hänggi, Harvesting randomness. Nat. Mater. **10**, 6–7 (2011)
9. W. Heisenberg, Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik. Zeitschrift für Physik **43**, 172 (1927)
10. Institut für Demoskopie Allensbach, German National Academy of Sciences Leopoldina, *Die Synthe-tische Biologie in der öffentlichen Meinungsbildung*, Halle (Saale) (2015)
11. A.V. Ponomarev, S. Denisov, P. Hänggi, ac-Driven atomic quantum motor. Phys. Rev. Lett. **102**, 230601 (2009)
12. E. Schrödinger, Quantisierung als Eigenwertproblem. Ann. Phys. **79**, 361 (1926)
13. E. Schrödinger, Über das Verhältnis der Heisen-berg-Born-Jordan'schen Quantenmechanik zu der meinen. Ann. Phys. **79**, 734–756 (1927)