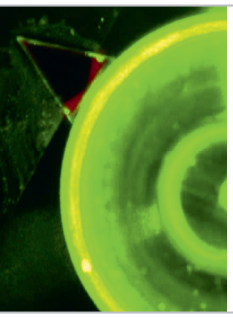
DOMINIQUE ELSER, CHRISTOPH MARQUARDT AND GERD LEUCHS
MAX PLANCK INSTITUTE FOR THE SCIENCE OF LIGHT, ERLANGEN

Quantum engineering with optical technology

Quantum engineering promises technical solutions with perspectives, which no other technology can offer: Quantum computers will be able to solve problems that still flummox supercomputers today, and quantum cryptography ensures verifiably secure communications. Despite the promise of future technological applications, quantum technologies are still important fields of basic research – and therefore the domain of the Max Planck Society, which was named after the discoverer of quantum physics. An important aspect is the contribution of optical sciences to quantum technologies. This relates in particular to the fields of quantum communication and cryptography. These two fields, which are being investigated at the Max Planck Institute for the Science of Light in Erlangen, are the subject of this article.



QUANTUM COMPUTERS WILL BE ABLE TO RESOLVE SPECIAL TASKS THAT EVEN SUPERCOMPUTERS FAIL AT. QUANTUM CRYPTOGRAPHY CAN VERIFIABLY ENSURE TAP-PROOF COMMUNICATIONS.

At the heart of quantum physics is Heisenberg's uncertainty principle. Generally speaking, quantum physics only yields information about probabilities but no precise predictions for measurements on a given single quantum system. This sounds more like a show-stopper than an advantage. However, the fact that a quantum system in an unknown state cannot be unambiguously characterized by measurements also opens up unimagined possibilities. A system can only be characterized by averaging over many identical measurements, provided that the exact same state is prepared and measured very often. This property is unique. It is found only in quantum systems, and it provides an invaluable advantage, namely that the basic laws of nature make it impossible in general to generate perfect copies of a quantum system the state of which is unknown to the observer.

On the one hand, this means that any attempt to carry out measurements will leave visible traces, meaning that an eavesdropper is unable to listen in to a conversation and not being discovered. On the other hand, two quantum systems can still be entangled. This means that although independent measurements of each system are very imprecise, suitable measurements of the two systems taken together can be perfectly correlated. Only if the value of the first measurement is known then it is possible to predict the outcome of a measurement on the second system precisely. This is one of the principles underlying the concept of a quantum computer.

A third aspect, which is important for cryptography, among other applications, is the generation of perfectly random numbers. Random numbers produced by computers today are generated by means of algorithms and can therefore be reproduced in principle – hence, the term "pseudo-random" numbers indicating the restriction. By contrast, according to the current state of knowledge, the randomness of the result of a quantum measurement is absolute. Quantum physics even allows conclusions to be drawn as to whether a second party might have identical random numbers: If a quantum system is in a pure quantum state, it cannot be entangled with any other system. The random number sequence is then unique.

At this point, a definition is needed of exactly what constitutes a quantum system. Generally speaking, an object or "system" is a quantum system if its properties are dominated by quantum physical effects. Examples include individual quantum objects such as single photons, single atoms, single vacancy centres in a solid or single electrons. However, even in a collection of many such objects, quantum properties can still dominate: for example a system comprising many millions of atoms if they form a Bose-Einstein condensate, a group of electrons if they are in a superconducting state, or a collection of photons if they are in a coherent state, as in laser light.

Research at the Max Planck Institute for the Science of Light (MPL) deals with the sources, i.e. the generation of photonic quantum systems, as well as the implementation of communication protocols and the characterization of quantum systems by measurements. Of course, all three aspects are needed for applications. The beauty of optical quantum technologies is that they can take advantage of the platform of highly advanced optical telecommunication used in optical fibre links or realized in coherent satellite-based communication.

One consequence of the Heisenberg uncertainty principle is that, within certain limits, the measurement of a quantum system results in random values. This randomness is fundamentally different from the randomness we are familiar

with in everyday life, for example the drawing of a playing card. The drawn card only seems random because we cannot precisely track how the cards were shuffled. When we play cards on the computer, randomness generation is hidden from our eyes even more. Computers use deterministic mathematical calculations to generate pseudorandom numbers. Such processes appear random only if we do not know all the parameters of the algorithms.

The situation is different if we use the measurement of a quantum system to generate randomness. In this case, the randomness is not based on insufficient knowledge of the generating process. On the contrary, the evolution of a quantum system is fully deterministic. The randomness arises from the quantum-mechanical measurement process itself. At MPL we are working on the technical implementation of such a random process using quantum states of light. The measurement process in this case is performed as a homodyne measurement, meaning that the actual signal is interfered with a bright laser beam. In this way it is even possible to highly sensitively detect very small signals. Homodyne measurements on many identically generated light states allow one to precisely determine this state.

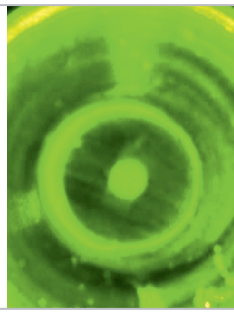
For a single measurement on a quantum system, however, randomness prevails. To exploit this as a perfect set of dice, it is not even necessary to send a light signal into the detector. Even if the signal at the input of the detector is "zero", i.e. when the lowest possible level is present, the unavoidable quantum uncertainty of the field remains. If we now repeatedly carry out homodyne measurements on many identically prepared signals of this type, we obtain an arbitrarily long series of truly and uniquely random numbers.

The implementation of a random number generator based on the homodyne principle makes it possible to largely utilize existing integrated optical technologies. This makes it feasible to implement the device on the scale of a USB memory stick. The MPL is currently working on such miniaturization in collaboration with the Austrian Institute of Technology and the company Roithner Lasertechnik.

Quantum random number generators are not yet sufficiently advanced and miniaturized to enter the mass market. Nevertheless, there are many applications that require true, unpredictable random numbers; for example, simulations of technical systems as well as climate and financial models often have to rely on random numbers of a high quality. In such applications, the use of computer-generated pseudorandom numbers can lead to unnoticed errors. Truly random numbers are also of crucial importance in the field of data security. For example, the cryptographic keys that are most widely used in data communication are based on random numbers. Poorly random numbers make the life of hackers easier.

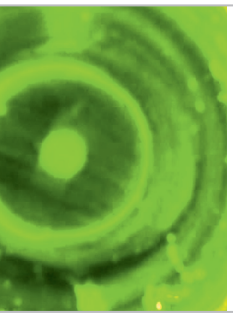
The one-time use of truly random numbers could prevent an attacker from breaking the code of cryptography systems. However, for lack of truly and uniquely random number series, today's systems have to use pseudorandom numbers for their keys, and these are generated by deterministic mathematical methods. This may set the bar very high for eavesdroppers if a great deal of computing power is required to crack the key, but it cannot guarantee absolute security. Although attackers do not yet have the necessary computing power and users can be lulled into a sense of security, attackers can in fact tap into the traffic with a view to breaking the encryption at a later date once the required computing power becomes available. For highly sensitive data this is simply unacceptable.

THE GREAT APPEAL OF OPTICAL QUANTUM TECHNOLOGIES IS THEIR ABILITY TO USE THE PLATFORM OF HIGHLY ADVANCED OPTICAL TELECOMMUNICATIONS.



Perfectly random numbers are not in themselves sufficient to ensure reliable data transfer if only the sender has them. The secret key must also be exchanged between the sender and the receiver in such a way that an eavesdropper is unable to intercept it. At present, asymmetric algorithmic techniques, generally known as public key methods, are used to exchange keys. It has been shown that some popular algorithmic methods for secure key distribution will become insecure as soon as a quantum computer with a sufficiently large quantum-computing register becomes available. But even without quantum computers being available, none of the non-quantum key distribution protocols are absolutely secure in the sense that no mathematical proof of security is known.

The Heisenberg uncertainty principle comes into play here, too. In the quantum era, the exchange of information between two parties to generate a key will no longer be done on the basis of classical digital bits, but with the aid of quantum states. Unlike digital bits, quantum states cannot be copied perfectly due to the uncertainty principle. Thus, an attacker cannot intercept information about the generated key unnoticed. The laws of physics ensure that no unauthorized person is able to eavesdrop on and obtain encrypted communications. This is referred to as information-theoretic security in contrast to the aforementioned weaker security based on the current unavailability of sufficient computing power. Quantum key distribution achieves both: it delivers perfect random numbers and achieves information-theoretic security for key distribution.



WE ARE COLLABORATING WITH PARTNERS ON THE MINIATURIZATION OF A QUANTUM RANDOM NUMBER GENERATOR. TRULY RANDOM NUMBERS CAN BE USED IN A WIDE RANGE OF APPLICATIONS.

A number of quantum optical methods are available for implementing a quantum key exchange. The best-known method uses discrete particles of light called photons. This method has been extensively studied and developed, theoretically and exerimentally, around the world over the past 30 years. In practice, however, several challenges have emerged: the single-photon method requires specially developed hardware, which cannot be easily integrated into existing telecommunication infrastructures. Consequently, synergies with currently widespread optical data communication systems tend to be small. The situation is different with the relatively newer quantum communication using continuous variables that is being developed by the MPL and others. Instead of discrete particles of light, this method is based on certain properties of light waves, which, unlike their energy, are continuous variables, e.g. the amplitude of the waves. The Heisenberg uncertainty principle not only allows for the generation of true randomness but also facilitates its distribution between two distant parties. A secret key can then be produced based on this distributed randomness.

Key distribution with continuous variables can be implemented using largely conventional optical telecommunication components and can therefore be easily integrated into existing communication networks. The main difference between widespread optical communication and quantum communication is the role played by the uncertainty principle. Whereas quantum uncertainty, as a disturbing factor, can lead to errors in optical data communication, it is deliberately exploited in quantum communication to generate a secret key.

Quantum key distribution with continuous variables is also highly insensitive to disturbance from other light sources. This makes it possible to operate quantum communication systems in parallel with bright optical systems without mutual interference. The MPL is working with companies in the fields of information technology and data security to realize this method in real-life optical fibre networks.

Besides transmission through optical fibres, communication networks also require free-space channels, i.e. channels for transmission through air or vacuum, for example to communicate with moving objects. The MPL is a world leader in the transmission of continuous variable quantum states through the atmosphere. It has been shown that even sensitive quantum properties can survive the journey through the turbulent atmosphere relatively intact. Using a specially developed technique based on, among other things, the homodyne method, continuous quantum states have been transmitted over a distance of 1.6 km above the houses and streets of Erlangen.

At first glance, the distances achieved appear to be much to small to compete with the distances achieved with quantum communications through optical fibres. But the line of sight towards a satellite, overlaps only little with the atmosphere. Atmospheric disturbance along this path is only around three times as large as along the 1.6-kilometre demonstration route. The success of the feasibility study therefore suggests that this technique can also be used over transcontinental distances provided that the transmission is relayed by satellites.

Researchers around the world are pursuing the ambitious goal of operating satellite-based quantum communication. China and Japan, but also Canada are investing in such projects on a major scale for the following reason: At present, quantum key distribution has been successful in optical fibre cables over distances that are typical within big cities. But it

is currently impractical to integrate cities in a global quantum network over fibre optic links. Unlike optical data communication, quantum states cannot be amplified along the way. Conventional amplification is tantamount to copying the information, which is fundamentally impossible in the case of unknown quantum information.

By contrast, optical links in space do not require intermediate amplifiers because of the significantly lower signal losses and can therefore bridge substantially greater distances. Satellites with quantum communication capabilities are very interesting both from the perspective of future applications and for fundamental research. From a practical point of view, satellites can provide the backbone for the global exchange of quantum keys.

In addition to these application-oriented perspectives, satellite-based quantum communication opens up new horizons in fundamental research. It is speculated that quantum communication and quantum information processing are affected by the earth's gravitational field in a still unknown way and that this might become noticeable in future highly sensitive applications. Preliminary theoretical approaches are already available. Experimental data obtained by satellite-based quantum communication could act as an important stimulus.

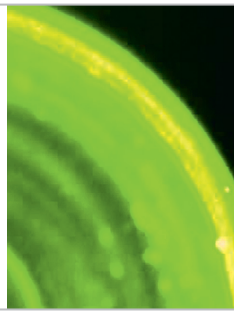
Methods based on continuous variables benefit from the currently available technology of optical data communications also in the field of satellite communications. The German company Tesat-Spacecom together with the German Aerospace Center (DLR) has developed a system for optical data communication with satellites. The system is essentially based on the same methods as those used at MPL Erlangen for quantum communication with continuous variables. Thus, the option exists to upgrade existing satellite systems to handle quantum communication. With this approach, the realization of satellite-based quantum communication can build on existing investments and will not require as much expenditure for new developments as in other projects.

In cooperation with Tesat-Spacecom and DLR, the MPL is currently evaluating this approach by conducting test measurements on optical satellite links that have recently been installed. These measurements can be used to determine the optimum operating parameters for satellite-based quantum communication so that future satellite systems can be upgraded accordingly.

The Heisenberg uncertainty principle relates to two "complementary" variables, such as position and velocity. Physics allows to reduce the uncertainty in one of the two variables, but at the cost of greater uncertainty in the complementary variable. This is referred to figuratively as squeezing the uncertainty like squeezing a balloon in one direction so that it stretches in the perpendicular direction. This concept can also be applied to light beams and can increase the accuracy of measurements significantly. Squeezed light can enhance the sensitivity of interferometers and belongs to the repertoire of the scientists operating gravitational wave detectors who have recently achieved a major breakthrough.

In the field of quantum communication, the squeezing of light states opens up hitherto largey unused means to boost efficiency. However, it should be noted that squeezed light is particularly sensitive to signal degradation, as the one which can occur during transmission through the atmosphere. MPL has therefore developed a source of squeezed light that is relatively insensitive to such degradation. The suitability of this source has been demonstrated over a 1.6-kilometre test track in Erlangen.

OPERATING QUANTUM COMMUNICATIONS VIA SATELLITE CURRENTLY STILL REMAINS AN AMBITIOUS OBJECTIVE. SEVERAL COUNTRIES ARE NEVERTHELESS INVESTING HEAVILY IN SUCH PROJECTS.



In certain quantum communication scenarios, the use of single photons is still advantageous. This is, however, associated with higher development costs for suitable sources. The aim is therefore to develop compact, stable and highly tuneable sources of single photons. A principle that has long been known in acoustics, the whispering gallery, can also be exploited in optics.

Well-known acoustic whispering galleries can be found e.g. in the domes of St. Paul's Cathedral in London, St.Peter's Basilica in Rome and Jameh Mosque at Isfahan. Sound waves travel along the dome's inner walls so that a whisper on one side of the dome is focused to and audible on the

other side. This acoustic principle can also be applied to light waves. MPL develops high-quality optical whispering-gallery resonators that are suitable for the efficient generation of single photons. On the one hand, the wavelength of the photon falls within a narrow band that approximates a well defined discrete wavelength and therefore a pure light colour; on the other hand, the wavelength can be adjusted over a broad range. Given these properties, the photon sources are suitable for many applications e.g. in quantum information technology and in the life sciences.

CLOSING REMARKS

Quantum technology in general and photonic quantum technology in particular have created hitherto unknown opportunities based on the counterintuitive concepts of quantum physics. To this end, quantum technology must be made suitable for use, and training programmes must be modified accordingly.

The significance of this development, which is still in its infancy, is highlighted by a study published in 2015 by the German National Academy of Sciences Leopoldina under the chairmanship of Wolfgang Schleich and in cooperation with partner academies. It presents the fundamentals of quantum technology and the new opportunities that it is creating to the wider public. The Max Planck Society has also produced a film on the subject which is publicly available:
https://www.youtube.com/watch?v=3sheEy1rNGI

We thank Ulrike Bauer-Buzzoni for carefully proof reading the manuscript.