

A global network of spacecraft and ground stations, distributing secret encryption keys by means of quantum technology, could meet emerging and long-term threats to data security.

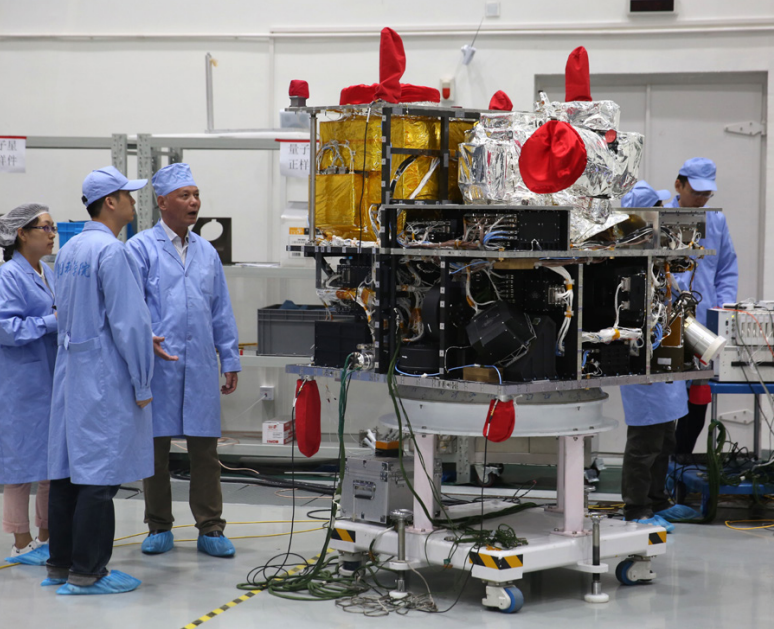
Composite photo taken on 9 November 2016 shows a satellite-to-Earth link established between the *Micius* spacecraft and the quantum communication ground station in Xinglong, north China's Hebei Province.

Xinhua/Jin Liwang via Getty Images

Satellite-Based QKD

Imran Khan, Bettina Heim, Andreas Neuzner
and Christoph Marquardt





The Chinese quantum satellite Micius—shown here before its 2016 launch, in its integration hall at Shanghai Engineering Center for Microsatellites—is one of several missions, with varying scopes, that are bringing space-based QKD closer to reality. Micius involved a huge platform carrying a technology demonstrator, whereas missions aiming to commercialize satellite-based QKD will need to target a miniaturized, more cost-effective approach.

©Cai Yang/Xinhua via ZUMA Wire

On 29 September 2017, the first intercontinental video conference using quantum encryption took place, between the presidents of the Austrian and Chinese academies of science. The cryptographic key pair used by the stations in Vienna and Beijing had been generated using an optical quantum key distribution (QKD) payload aboard the Chinese satellite Micius—part of the QUESS (Quantum Experiments at Space Scale) mission, which was brought into orbit in August 2016 and carries a series of quantum-optical experiments.

The achievement was of more than just academic interest. As computing technology becomes ever more powerful, and particularly with rapid advances in quantum computing, the long-term security of existing encryption schemes looks increasingly under threat. A space-based QKD infrastructure could prove an important approach—indeed, perhaps the only really viable long-term solution—to securing worldwide communications. Here, we provide an overview of QKD's principles and engineering challenges, and how a satellite-based QKD network might roll out in the coming years.

Why QKD?

Today's interest in QKD arises largely from rapid progress in another quantum technology: quantum computing. A quantum computer exploits the laws of quantum mechanics to perform computations on physical quantum systems rather than classical bits. While quantum computers have long been regarded mainly as an academic curiosity, recent experimental advances, coupled with massive public and private investments in quantum research and development, has made them a more realistic prospect.

Exciting as these developments are, the advent of quantum computers could mean trouble for information

security—at least as it's handled today. A quantum computer would, for example, be capable of solving the prime-number factorization problem exponentially faster than classical computers. Asymmetric encryption, now widely used both for authentication and for data transmission, relies on the difficulty of solving just such mathematical problems. The development of effective quantum computers would thus make currently deployed asymmetric cryptography obsolete, potentially leading to a fatal breakdown of current infrastructure. Given that upgrades to critical infrastructure can take a decade or more, quantum computers pose a real threat.

While classical cryptographic techniques that protect against known quantum computer algorithms might be developed, QKD could offer long-term security against *any* future quantum computer attack. That's because QKD rests on fundamental physical principles rather than specific mathematical assumptions. Ultimately, provable secure communication boils down to the distribution of a unique secret key, used to encrypt a message, that is completely random, as long as the message, and is used only once. QKD offers a solution to establish such a key remotely between two distinct parties.

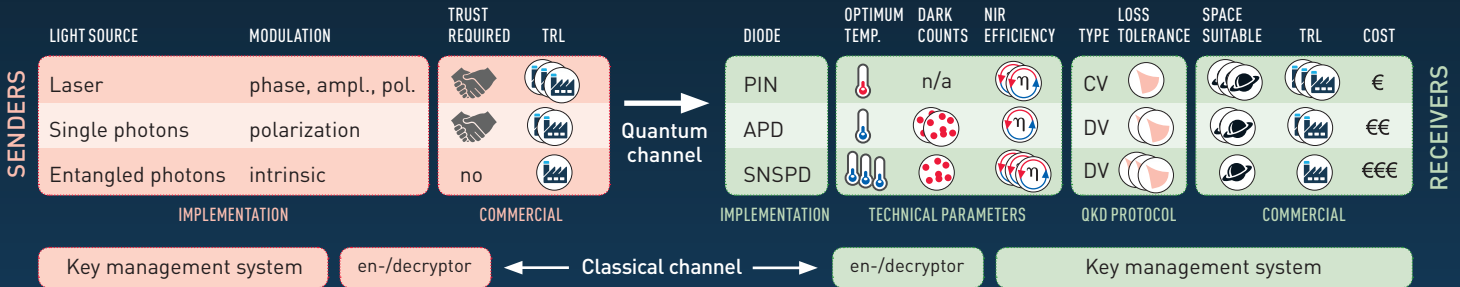
How QKD works

At the core of QKD is the fundamental principle that, generally, quantum states cannot be copied exactly and become altered in the process of attempting to copy them. The underlying physics involves so-called non-orthogonal quantum states, which fundamentally cannot be discriminated without error.

In a typical “prepare-and-measure” QKD protocol, the **sender** (“Alice”) prepares a set of quantum states that are non-orthogonal with respect to a specific degree of freedom of light (polarization, amplitude, phase or time) and sends them to a **receiver** (“Bob”) over an optical link. To listen in on the communication, an **eavesdropper** (“Eve”) needs to perform a measurement on the sent light pulses. Even if she uses a nondestructive measurement technique—and, in fact, Eve is assumed to be bound

Building a QKD system

While in principle all QKD protocols operate the same way and rest on the same core principles, in practice the complexity of implementation can dramatically vary with the specifically selected protocol and its associated components, the choice of which involve numerous trade-offs. (As with any cryptologic technology, real-world implementation needs to be carefully engineered to match the assumptions in the theoretical security proofs.)



TRL= Technology Readiness Level. NIR= near infrared. A larger number of symbols indicates a higher value for the discussed parameter.

SENDING

For use as light source for QKD, polarization-modulated single photons are an obvious choice, but can be quite challenging to implement. As an alternative, some QKD protocols use weak pulses of laser light, modulated in phase, amplitude or polarization. Using weak pulses significantly reduces the technical complexity and has only a minor impact on the protocol's key-distribution efficiency, but maintains the paradigm of physically provable security. Imprinting quantum information onto the light at a high rate is done by either switching between different light sources with fixed modulation parameters (for example, polarizations), or employing commercial amplitude, phase or polarization modulators, which can be operated at telecom bandwidths and up to several GHz.

Both single-photon and laser-light schemes assume that the QKD receiver intrinsically trusts the QKD sender. The only light sources that do not require such intrinsic trust are the least developed: sources involving entangled photon pairs, which rely on pair generation of differently polarized photons by a nonlinear medium. The nonlinear process imparts an intrinsic randomness to the generation of these pairs.

SECURING

The security of all QKD protocols relies on the availability of truly random numbers. Random-number generation techniques based on quantum mechanics include sending single photons onto a beam splitter, measuring the random phase of a laser when switched on or measuring the quantum vacuum using homodyne detection.

RECEIVING

The transmitted light can be detected either with single-photon detectors or using homodyne detection. Single-photon detectors include avalanche photodiodes (APDs), which require thermoelectric cooling and have quantum efficiencies of some 20 percent, and superconducting nanowire single-photon detectors (SNSPDs), which require liquid-helium cryogenics and achieve quantum efficiencies of around 80 percent. Note that these values are for near infrared (NIR) diodes. Homodyne detection involves balanced PIN diode-based detectors, which can operate at room temperature and have quantum efficiencies of 50 to 99 percent. The tolerable loss depends on the chosen protocol; at present, discrete-variable (DV) protocols can tolerate greater losses than continuous-variable (CV) protocols. PIN diodes have good characteristics for use in space, whereas APDs suffer from increases in dark counts due to radiation, and the cooling requirements of SNSPDs make their use in space very challenging.

only by the laws of physics—her measurement causes an unavoidable back-action onto the measured degree of freedom, and will thus always leave a trace in the signal.

Bob then detects the quantum states and compares a portion of his results to the states originally sent by Alice. This is the so-called information reconciliation phase of the protocol, part of the post-processing (for which an

additional classical channel is needed, typically using existing infrastructure). An increased error rate in Bob's measurement data reveals Eve's presence—that is, an eavesdropping on the distribution—and, thus, the protocol is aborted and a secret key pair can't be established.

The security of each QKD protocol relies on the fact that after the protocol's execution (that is, after post-processing),

Satellite-Based QKD

1. In a sender-in-space QKD architecture, quantum states are generated aboard the satellite and sent towards earth.

QKD send system

2. The quantum states (orange) are sent in a low-divergence beam accompanied by a strong beacon light with higher divergence (green) that allows the ground station to actively track the satellite.

3. While propagating through the vacuum of space, nearly diffraction-limited divergence of the two beams can be maintained.

4. Upon entering the atmosphere, turbulences generate wavefront distortions leading to atmospheric seeing and a further increased divergence of the beams sent from space.

5. A beacon light at a different wavelength (red) is sent from the ground station towards the satellite. Analyzing the collected satellite's beacon light (green) can be used to actively correct for wavefront errors on the collected quantum signal (orange) using adaptive optics.

QKD receive system

Quantum Satellite in LEO (Low Earth orbit)

600 km (propagation through vacuum)

20 km (atmospheric propagation)

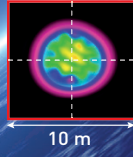
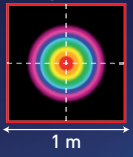
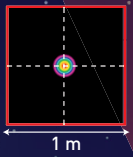


Illustration by Phil Saunders

Eve possesses only a vanishingly small probability of guessing the key—an “information-theoretic” level of security that contrasts with conventional cryptography, the security of which depends on the assumed difficulty of specific mathematical problems. This information-theoretic security means that QKD is immune against current and future attacks from quantum computers.

Out of the lab, and into orbit

Several companies are working to commercialize QKD technology. These include IDQ (Switzerland), which has been selling QKD systems for integration into optical-fiber networks for more than 15 years. China also has a big commercial effort under way, with companies including QuantumCTek, CAS and Huawei. Other commercial entities have formed dedicated quantum groups, such as Toshiba in the United Kingdom, Batelle in the United States, and Huawei in Germany. And startup companies focusing on QKD have been founded worldwide, often in collaboration with scientific institutes or individual working groups. With the working principles of QKD well established, current efforts focus on how to implement sensitive QKD channels using an existing fiber optic communication network that already carries a multitude of classical WDM channels.

Yet, while the development of metropolitan, short-link QKD in fiber systems is advancing, long-distance communication, both for government communication and business infrastructure, is far more important in meeting the security threat posed by quantum computers. Interconnecting local QKD networks over great distances faces a big technological hurdle: amplification or simple reception and retransmission of quantum states alters their properties and is thus fundamentally incompatible with QKD. That sets a distance limit of around 100 km for terrestrial applications of QKD in practical optical-fiber networks. While one solution might lie in a “quantum repeater” that allows single light quanta to be stored, re-sent and potentially manipulated without altering their state, such a technology is still in its infancy and far from ready for practical application. Another solution, links with many trusted (that is, protected) nodes, is not economical or practical in most cases.

Surprisingly, a viable solution is taking a detour in space—that is, using satellites that distribute secure keys to ground stations via free-space optical links. Propagation losses, which scale exponentially in fiber, scale only quadratically in free space. For example, a 600-km fiber link between Munich and Berlin would

Interconnecting QKD networks over great distances faces big technological hurdles. One solution is taking a detour in space.

have a nominal loss of 120 dB assuming a very optimistic loss of 0.2 dB/km, making a QKD link unfeasible. A 600-km free-space link with a low-Earth orbit (LEO) satellite could be realized with 50 dB of loss with reasonable aperture sizes, which is acceptable for some current QKD protocols.

Thus a global QKD network of ground stations and satellites, using laser light to send secure secret keys, could bridge the cryptographic gap between cities and across oceans. And, since keys can be distributed and stored for later use in a key management system, such a system need not rely strongly on weather conditions, which have to be taken into account in other optical free-space links.

Alice, Bob, and the satellite

Satellite-based QKD can basically work in two different ways:

Prepare and measure. In prepare-and-measure protocols, quantum states are sent between a satellite and a ground station. The satellite establishes a secret key between the satellite itself and Alice (the first ground station), and afterwards a second key between itself and Bob (the second ground station). The satellite then combines these two secret keys with a mathematical operation and broadcasts it, such that only Alice and Bob can decode the counterpart of the key. Here, the satellite acts as a single trusted node, and a certain level of trust has to be attributed to the operator (which is often the case, for example, in communications within large organizations or infrastructure).

Entanglement-based. Here, Alice's and Bob's ground stations measure quantum correlations between two beams of entangled photons sent by the satellite at the same time. The great advantage is that neither Alice nor Bob needs to trust the satellite any more. As with prepare-and-measure protocols, this class of protocols eliminates Eve's ability to intentionally manipulate the photon pair on behalf of the satellite. A disadvantage is that the need for simultaneous reception of the two beams means that the satellite needs a line-of-sight connection with both ground stations at the same time. Further, the required correlations suffer from loss in

both channels, drastically reducing the final key rate. While some groundbreaking mid-2017 results from the Chinese QUESS mission offered a proof of principle, a viable solution will need sources that can boost the generation rate of "space-proof" entangled photons by several orders of magnitude.

Making spaceborne QKD work

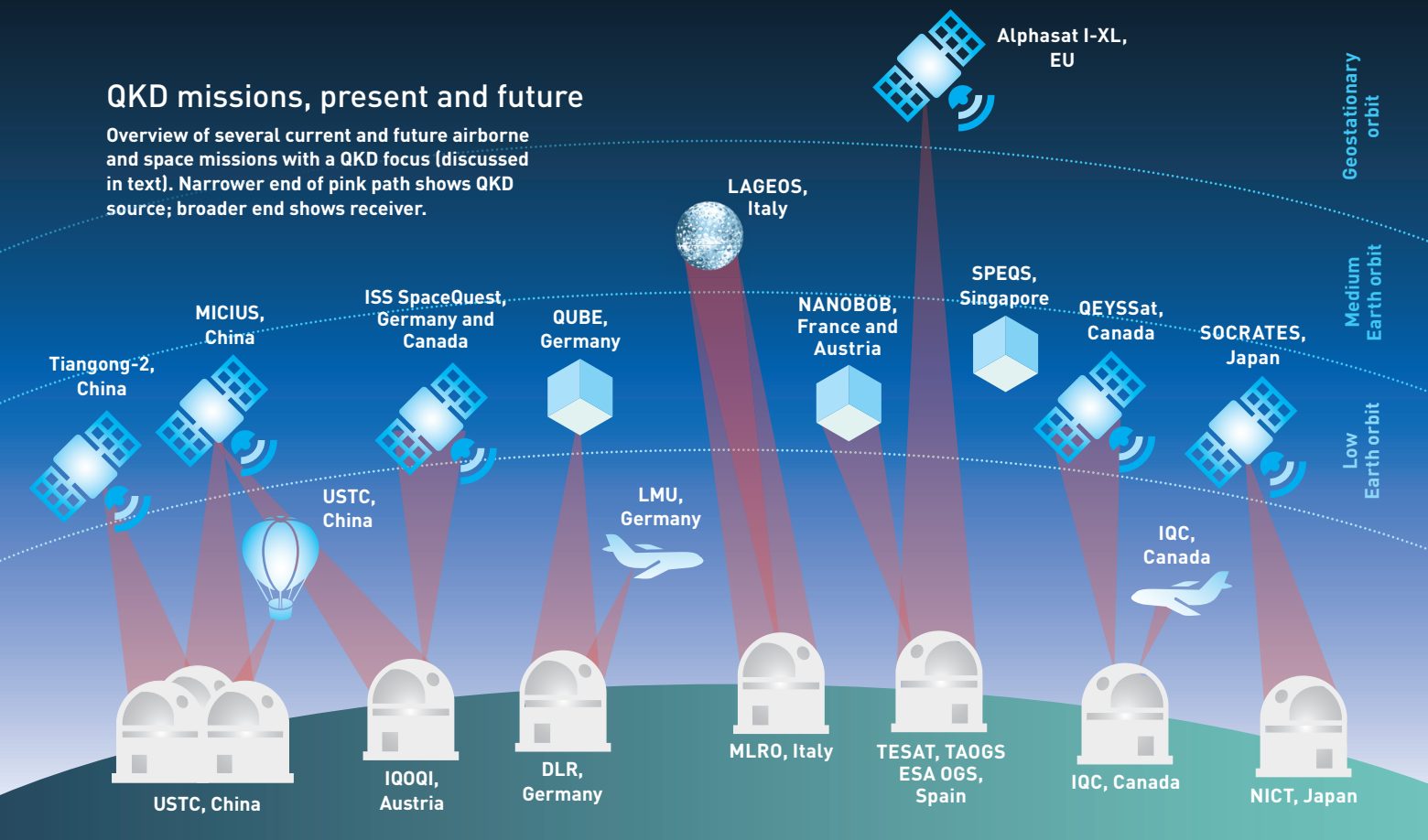
Quantum communication with satellites has all the demands of conventional laser communication in space, a field whose technology is already matured and that thus, conveniently, can be transferred to a large extent. Performing QKD between a ground station and a moving satellite platform requires additional optical components, such as telescopes and tracking mechanisms to establish an optical link. Initial acquisition and tracking often involves using mutually exchanged beacon lights at a wavelength different from the quantum signal, but travelling collinearly, to be split off from the quantum signal using dichroic optics.

Free-space optical communications suffer from the effect of local atmospheric turbulence, which introduces wavefront distortions. Channel losses when sending light towards a satellite are particularly large, as wavefront errors present after the first few kilometers of propagation in the atmosphere will continue to diverge the beam during transmission through vacuum. In the opposite case of receiving light sent from the satellite, a beam of low divergence is propagated through vacuum, and additional divergence due to atmospheric turbulence becomes relevant only on the last few kilometers.

This asymmetry in the optical link through the atmosphere makes the choice between "flying-receiver" and "flying-sender" architectures an interesting top-level design decision in satellite QKD. While the link losses are larger when putting the receiver into space, having the sender on ground allows for a greater flexibility to use protocols involving more exotic quantum states. For QKD protocols involving single-photon pulses, a receiver in space also benefits from greatly relaxed requirements for onboard memory, as only the single photons actually received in space generate data. The choice of scenario depends largely on the technical boundary conditions, both on the satellite and on ground.

QKD missions, present and future

Overview of several current and future airborne and space missions with a QKD focus (discussed in text). Narrower end of pink path shows QKD source; broader end shows receiver.



Finally, the influence of stray photons on the receivers needs to be minimized, by focusing on operation during nighttime and using narrowband filters. Homodyne detection can even permit daylight operation, as it allows for additional spatial and spectral filtering due to the interference with a bright reference laser as a local oscillator.

A variety of technical difficulties specific to spaceflight must also be overcome. These include the impact on sensitive equipment of launch vibration loads and other shock loads during spaceflight; exposure to heat and a hostile radiation environment outside of the protection of Earth's magnetosphere, which requires dedicated thermal management and the use of radiation-hardened, redundant electronic and optical components; and a range of other space-specific parameters that all factor into a specific component's technology-readiness level (TRL). Increasing the TRL goes along with a multi-step qualification process, addressing each of the outlined difficulties in dedicated test campaigns.

The current state of play

A number of projects are under way to bring QKD satellites into orbit, with demonstrations ranging from in-orbit verification of QKD-relevant technology to establishing fully automatized links and key exchange with optical ground stations (see figure above). The Chinese Micius

spacecraft, the Japanese SOTA laser communication terminal onboard the microsatellite SOCRATES, and a recently published Chinese experiment with a small payload on Tiangong-2 Space Lab have already demonstrated space-to-ground QKD. Academic working groups in Munich, Germany, and Waterloo, Canada, have demonstrated QKD links between airplanes and ground stations in flying-sender and flying-receiver configurations, respectively.

All of the missions mentioned above involved dedicated QKD hardware. In contrast, an academic-industrial team based at the Max-Planck Institute for the Science of Light in Germany performed measurements with optical telecom equipment not originally designed for QKD—specifically the Tesat laser communication terminal aboard the Alphasat satellite in geostationary orbit (36,000 km). A coherent receiver on ground showed that the signal was quantum-noise-limited, thereby demonstrating that the system could serve as a foundation for building a QKD satellite.

Other recent experiments include a hot-air balloon experiment in China, and a photon-reflection experiment carried out between the Italian Matera Laser-Ranging Observatory (MLRO) and the LAGEOS satellite, which carries a multitude of corner-cube reflectors.

Several projects currently under preparation focus on technology maturation rather than operating provable

QKD has matured from a laboratory curiosity to a realistic technology—and spaceborne links are a key piece of the puzzle.

secure links. The National University of Singapore has tested entangled-photon sources on board a nanosatellite. QUBE, an effort within the German national quantum technologies funding scheme QUTEQA, will develop a nanosatellite that includes a quantum payload with different sources, partially in integrated photonic-chip technology. The QEYSSat project, funded by the Canadian government, aims at bringing a microsatellite into orbit carrying a polarization-resolved single-photon detection system—thus, in contrast to many other missions, using a receiver-in-space architecture. The mission is based on components developed for space and used in airborne demonstration experiments by the same group, including radiation-hard single-photon detection systems, a fine-pointing system and a polarization-mapping assembly. Other nanosatellite projects are forming; a U.K.-led consortium plans a CubeSat Quantum Communications Mission, and France and Austria are collaborating on a project called NanoBob.

In the framework of an ESA-funded Phase A/B study, a consortium formed by the University of Waterloo and the German aerospace company OHB System currently plans to use the same subsystems developed by the University of Waterloo for an experiment aboard the International Space Station. The experiment, called SpaceQuest, will try to observe a quantum-physical effect called gravitationally induced decoherence, with QKD being a secondary science objective.


The outlook

QKD has matured from a laboratory curiosity to a realistic technology—and the realization of global QKD links via spaceborne trusted nodes constitutes a key piece of the puzzle. Spaceborne and terrestrial QKD complement each other: The development of individual local metropolitan QKD networks on fiber can allow high key data rates, while trusted nodes in space avoid the problem of attenuation in optical fibers (and the impossibility of using classical amplification or relay stations without compromising the quantum security) for long-haul communications between those metro networks.

The result could be steady progress to a global QKD infrastructure. And, given the large synergy between the development of classical satellite optical free-space

communication and QKD links, the field is advancing fast. Also driving this strong dynamic is an ever-growing public interest in quantum technologies in general and in related funding schemes. In Europe, for example, ESA's ScyLight initiative, the Quantum Flagship and other national initiatives have helped to shape agendas. Commercial partners are teaming up with academic groups to create economically viable solutions. The primary users of proven long-term security will most likely be governments and large organizations seeking to protect critical infrastructure.

Rather than completely replacing classical cryptologic infrastructure, QKD will likely complement existing and novel classical cryptographic schemes. Analyzing the system and identifying usage scenarios of QKD thus represents an important next step in development—and resolving the open questions will require multidisciplinary and even multinational input. Finally, customers will need to trust the system and its providers, as they cannot verify the whole, complex QKD stakeholder structure and must instead rely on a chain of certifications and standards. National and international institutions are at work on this crucial step as well.

And the progress comes not a moment too soon. As work continues on a new generation of more powerful computers, the threat to deployed encryption is becoming increasingly urgent. The clock is ticking. 

Imran Khan and Christoph Marquardt are with the Max-Planck-Institute for the Science of Light, Erlangen, Germany, and the upcoming QKD startup InfiniQuant (infiniquant.com). Bettina Heim (bettina.heim@ohb.de) and Andreas Neuzner are with OHB System AG, Wessling, Germany.

References and Resources

- ▶ R. Bedington et al. *npj Quantum Inf.* **3**, 30 (2017).
- ▶ V. Scarani et al. *Rev. Mod. Phys.* **81**, 1301 (2009).
- ▶ S. Nauert et al. *Nat. Photon.* **7**, 382 (2013).
- ▶ H.-K. Lo et al. *Nat. Photon.* **8**, 595 (2014).
- ▶ Z. Tang et al. *Phys. Rev. Appl.* **5**, 054022 (2016).
- ▶ J. Yin et al. *Science* **356**, 1140 (2017).
- ▶ S.-K. Liao et al. *Nature* **549**, 43 (2017).
- ▶ K. Günthner et al. *Optica* **4**, 611 (2017).
- ▶ C. J. Pugh et al. *Quant. Sci. Technol.* **2**, 024009 (2017).
- ▶ H. Takenaka et al. *Nat. Photon.* **11**, 502 (2017).
- ▶ D. K.-L. Oi et al. *EPJ Quantum Technol.* **4**, 6 (2017).
- ▶ S.-K. Liao. *Chin. Phys. Lett.* **34**, 090302 (2017).