nature photonics

REVIEW ARTICLE

PUBLISHED ONLINE: 31 JULY 2014 | DOI: 10.1038/NPHOTON.2014.149

Secure quantum key distribution

Hoi-Kwong Lo[1†], Marcos Curty[2†] and Kiyoshi Tamaki[3†]

Secure communication is crucial in the Internet Age, and quantum mechanics stands poised to revolutionize cryptography as we know it today. In this Review, we introduce the motivation and the current state of the art of research in quantum cryptography. In particular, we discuss the present security model together with its assumptions, strengths and weaknesses. After briefly introducing recent experimental progress and challenges, we survey the latest developments in quantum hacking and countermeasures against it.

With the rise of the Internet, the importance of cryptography is growing daily. Each time we make an online purchase with our credit cards or conduct financial transactions using Internet banking, we should be concerned about secure communication. Unfortunately, the security of conventional cryptography is often based on computational assumptions. For instance, the security of the RSA scheme[1] — the most widely used public-key encryption scheme — is based on the presumed hardness of factoring. Consequently, conventional cryptography is vulnerable to unanticipated advances in hardware and algorithms, as well as to quantum code breaking, such as Shor's efficient algorithm[2] for factoring. This is potentially problematic as government and trade secrets are kept for decades. An eavesdropper, Eve, may simply save communications sent in 2014 and wait for technological advances. If she is able to factorize large integers in say 2100, she could retroactively break the security of data sent in 2014.

In contrast, quantum key distribution (QKD), the best-known application of quantum cryptography, promises to achieve the Holy Grail of cryptography — unconditional security in communication. In unconditional security, or more precisely ε-security (see the section "Security model of QKD"), Eve is not restricted by computational assumptions, but only by the laws of physics. QKD is a remarkable solution to long-term security as, in principle, it offers security for eternity. Unlike conventional cryptography, which allows Eve to store a classical transcript of communications, in QKD, once a quantum transmission has been completed, there is no classical transcript for Eve to store. See Box 1 for background information on secure communication and QKD.

Achievements and future goals in QKD. On the theoretical side, a landmark accomplishment has been rigorous security proofs of QKD protocols. Recently, a 'composable' definition[3,4] of the security of QKD has been obtained. Stable QKD over long distances has been achieved in both fibres[5] and free space[6]. Commercial QKD systems are currently available on the market. Field-test demonstrations of QKD networks have been conducted[7–14]. High-detection-efficiency single-photon detectors at telecom wavelengths have been developed[15–18]. In short, QKD is already mature enough for real-life applications. Figure 1 shows the tremendous progress that has been made in free-space QKD over the past two decades. It compares the first laboratory demonstration performed in 1992[19] (Fig. 1a) with two recent QKD implementations, one that connected two Canary

Box 1 | Secure communication and QKD

Secure communication: Suppose a sender, Alice, wants to send a secret message to a receiver, Bob, through an open communication channel. Encryption is needed. If they share a common string of secret bits, called a key, Alice can use her key to transform a plaintext into a ciphertext, which is unintelligible to Eve. In contrast, Bob, with his key, can decrypt the ciphertext and recover the plaintext. In cryptography, the security of a cryptosystem should rely solely on the secrecy of the key. The question is how to distribute a key securely? In conventional cryptography, this is often done by trusted couriers. Unfortunately, in classical physics, couriers may be bribed or compromised without the users noticing it. This motivates the development of QKD.

QKD: The best-known QKD protocol (BB84) was published by Bennett and Brassard in 1984[23]. Alice sends Bob a sequence of photons prepared in different polarization states, which are chosen at random from two conjugate bases. For each photon, Bob randomly selects one of the two conjugate bases and performs a measurement. He records the outcome of his measurement and the basis choice. Alice and Bob broadcast their measurement bases via an authenticated channel. They discard all polarization data sent and received in different bases and use the remaining data to generate a sifted key. To test for tampering, they compute the quantum bit error rate of a randomly selected subset of data and verify that it is below a certain threshold value. They generate a secure key by applying classical post-processing protocols, such as error correction and privacy amplification. This key can be used to make the communication unconditionally secure by using a one-time-pad protocol[109].

One-time-pad protocol: The message is represented by a binary string. The key is also a binary string of the same length as the message. For encryption, a bitwise exclusive OR (XOR) is performed between the corresponding bits of the message and the key to generate a ciphertext. Decryption is done by performing a bitwise XOR between the corresponding bits of the ciphertext and the key. For a one-time pad to be secure, the key should not be reused.

[1]Center for Quantum Information and Quantum Control, Department of Physics and Department of Electrical and Computer Engineering, University of Toronto, Toronto, Ontario M5S 3G4, Canada, [2]EI Telecomunicación, Department of Signal Theory and Communications, University of Vigo, E-36310 Vigo, Pontevedra, Spain, [3]NTT Basic Research Laboratories, NTT Corporation, 3-1, Morinosato-Wakamiya, Atsugi-shi, Kanagawa 243-0198, Japan. †All authors contributed equally to this work. *e-mail: hklo@comm.utoronto.ca; mcurty@com.uvigo.es; tamaki.kiyoshi@lab.ntt.co.jp

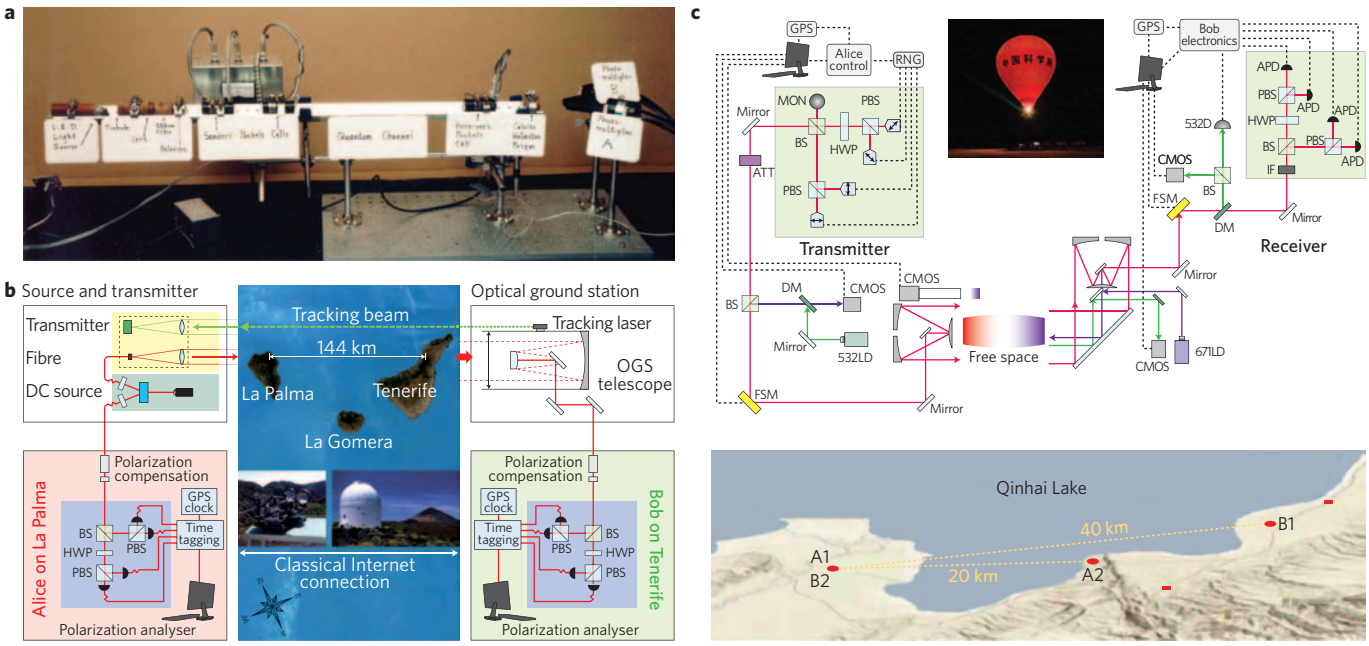

Figure 1 | Progress in free-space QKD implementations. a, First free-space demonstration of QKD[19] realized two decades ago over a distance of 32 cm. The system uses a light-emitting diode (LED) in combination with Pockels cells to prepare and measure the different signal states. **b**, Entanglement-based QKD set-up connecting the two Canary Islands La Palma and Tenerife[6]. The optical link is 144 km long. OGS, optical ground station; GPS, Global Positioning System; PBS, polarizing beamsplitter; BS, beamsplitter; HWP, half-wave plate. **c**, Schematic of a decoy-state BB84 QKD experiment between ground and a hot-air balloon[20]. This demonstration may be considered a first step towards realizing QKD between ground and low-Earth-orbit satellites. MON, monitor window; ATT, attenuator; DM, dichroic mirror; 532LD, 532 nm laser; FSM, fast steering mirror; 671LD, 671 nm laser; 532D, 532 nm detector; IF, interference filter; CMOS, complementary metal–oxide–semiconductor. Figure adapted with permission from: **a**, ref. 19, © 1992 IACR; **b**, ref. 6, © 2007 NPG; **c**, ref. 20, © 2013 NPG.

Islands[6] (Fig. 1b) and another that connected a ground station with a hot-air balloon[20] (Fig. 1c).

What are researchers aiming to do now? As discussed in the rest of the Review, they are striving to bridge the gap between theory and practice in order to guarantee unconditional security in actual QKD implementations. Other major research challenges in the field are developing high-speed QKD systems and realizing the ability to multiplex strong classical signals with weak quantum signals in the same optical fibre (for example, by wavelength-division multiplexing). Moreover, researchers are studying QKD network set-ups containing both trusted and untrusted nodes. The feasibility of ground-to-satellite QKD has also attracted a lot of research attention[20,21].

Security model of QKD

Intuitively speaking, the security of QKD is measured with respect to a perfect key distribution scheme in which Alice and Bob share a true random secret key. More precisely, we say that a QKD system is ε-secure if and only if the probability distribution of an outcome of any measurement performed on the QKD scheme and the resulting key deviates by at most ε from that of the perfect key distribution protocol and the perfect key[3,4]. A typical value for ε is 10^{-10}. However, in principle, Alice and Bob could select ε as small as they wish by just applying sufficient privacy amplification.

Of course, because a secret key is a resource for other cryptographic protocols (for example, the one-time pad method), it is not enough to consider the security of the QKD protocol alone. Instead, one has to evaluate the security of the generated key when it is employed in a cryptosystem. This notion is known as 'composable' security. Fortunately, QKD is composably secure[3,4,22]. That is, if we have a set of cryptographic protocols (which may include QKD), each of them having a security parameter ε_i, as part of a certain cryptographic scheme, then the security of the whole system is given by $\sum_i \varepsilon_i$.

Progress in security proofs. Having presented the security definition of QKD, we next discuss the security of a particular QKD implementation, the BB84 scheme[23]. In its original theoretical proposal of QKD, Alice sends Bob single-photon states. However, as practical and efficient single-photon sources have yet to be realized, most implementations of the BB84 protocol are based on phase-randomized weak coherent pulses (WCPs) with a typical average photon number of 0.1 or higher. These states can be easily prepared using standard semiconductor lasers and calibrated attenuators. The main drawback of these systems is that some signals may contain more than one photon prepared in the same quantum state. If Eve performs, for instance, the so-called photon-number-splitting attack[24] on the multiphoton pulses, she could obtain full information about the part of the key generated with them without causing any noticeable disturbance. That is, in the BB84 scheme, only the single-photon states sent by Alice and detected by Bob can provide a secure key. Fortunately, to distil a key from these single-photon contributions, it is enough if Alice and Bob can estimate a lower bound for the total number of such events; that is, they do not need to identify which particular detected pulses originated from single-photon emissions[25]. In the case of the BB84 scheme, this estimation procedure must assume the worst-case scenario in which Eve blocks as many single-photon pulses as possible. As a result, it turns out that its key generation rate scales as η^2, where η denotes the transmittance of the quantum channel. This quantity has the form $\eta = 10^{-\alpha d/10}$, where α is the loss coefficient of the channel measured in dB km^{-1} ($\alpha \approx 0.2$ dB km^{-1} for standard commercial fibres) and d is the covered distance measured in kilometres.

In reality, however, Eve may not be monitoring the quantum channel and performing a photon-number-splitting attack. To improve the achievable secret key rate in general, it is thus necessary to more precisely estimate the amount of single-photon pulses detected by Bob. This can be done using the so-called

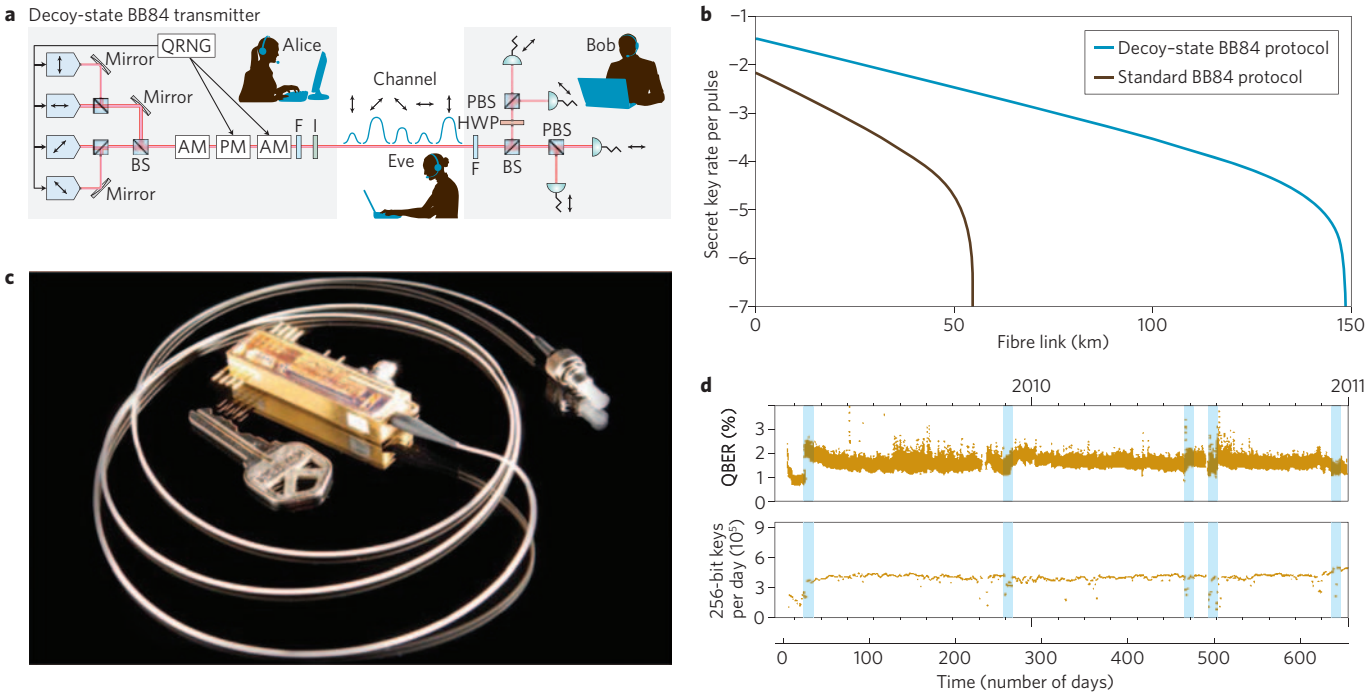

Figure 2 | Experimental QKD. a, Schematic of the decoy-state BB84 protocol[26–35] based on polarization coding. Four lasers are used to prepare the polarizations needed in BB84. Decoy states are generated with an amplitude modulator (AM). On Bob's side, a 50:50 beamsplitter (BS) is used to passively ensure a random measurement basis choice. Active receivers are also common. PM, phase modulator; F, optical filter; I, optical isolator; HWP, half-wave plate; PBS, polarizing beamsplitter; QRNG, quantum random number generator. **b**, Lower bound on the secret key rate (per pulse) in logarithmic scale for a BB84 set-up with two decoys (blue line)[29]. In the short-distance regime, the key rate scales linearly with the transmittance, η. Standard BB84 protocol without decoy states (dark brown line)[23,25]; its key rate scales as η^2. **c**, Photograph of a fibre-coupled modularly integrated decoy-state BB84 transmitter based on polarization coding[37]; it produces decoy-state BB84 signals at a repetition rate of 10 MHz. **d**, Performance of the SwissQuantum network[9]. This network was operated for more than 18 months in Geneva, Switzerland. The data shown in the figure correspond to a QKD link of 14.4 km; they highlight the stability of current QKD set-ups. QBER, quantum bit error rate. Figure adapted with permission from: **c**, ref. 37, © 2013 LANL; **d**, ref. 9, © 2011 IOP.

decoy-state method[26–35], which can basically reach the performance of single-photon sources, where the key generation rate scales linearly with η. Its procedure is as follows. Instead of sending signals of equal intensity, Alice first chooses the intensity for each signal at random from a set of prescribed values. States sent with one particular intensity are called signal states, whereas states sent with other intensities are called decoy states. Once Bob has detected all the signals, Alice broadcasts the intensity used for each pulse. A crucial assumption here is that all other possible degrees of freedom of the signals (apart from the intensity) are equal for all of them. This way, even if Eve knows the total number of photons contained in a given pulse, her decision on whether to send that signal to Bob cannot depend on its intensity. That is, Eve's decision is based on what is known *a priori*. Consequently, the probability of a detection event given that Alice sent a single-photon pulse is the same for both the signal and decoy pulses. As a result, Alice and Bob can more precisely estimate the fraction of detected events that arise from single photons. This technique is rather general and is also very useful for other quantum cryptographic protocols[36].

Experimental implementations

Experimental realizations of QKD have progressed greatly over the past two decades. In practice, signal transmission can be done through free space (using a wavelength of around 800 nm) or through optical fibres (using the second or third telecom windows; that is, wavelengths around 1,310 nm and 1,550 nm, respectively). Also, current set-ups use different degrees of freedom to encode the relevant information into the optical pulses. As already mentioned, an obvious choice for this is to employ the polarization state of the photons. This technique, known as polarization coding, is mostly used in free-space QKD links. For optical fibre transmission, however, one usually selects other coding options, for example, phase coding, time-bin coding or frequency coding. This is because polarization in standard fibres is more susceptible to disturbances resulting from birefringence and environmental effects.

Figure 2a shows how conceptually simple the basic set-up for the decoy-state BB84 protocol is when Alice and Bob employ polarization coding. The expected secret key rate (per pulse) as a function of the distance is illustrated in Fig. 2b. The cut-off point at which the secret key rate drops to zero depends on the system parameters (especially the channel transmission and the efficiency and dark count rate of Bob's detectors); it is typically around 150–200 km. As shown in Fig. 2b, the corresponding lower bound on the secret key rate for the standard BB84 protocol without decoy states is much lower. Figure 2c shows a photograph of a fibre-coupled modularly integrated decoy-state BB84 transmitter developed by the Los Alamos group[37]. It is similar in size to an electro-optic modulator.

Alice and Bob may further extend the covered distance by using entanglement-based QKD protocols[38–41], as these schemes can tolerate higher losses (up to about 70 dB) than WCP-based protocols. For instance, they could employ a parametric downconversion source to generate polarization-entangled photons that are distributed between them. This source could be even controlled by Eve, and it can be placed in the middle between the legitimate users. On the receiving side, both Alice and Bob measure the signals received using, for example, a BB84 receiver like the one shown in Fig. 2a. However, this approach has two drawbacks: the systems are more complex than those based on WCPs and their secret key rate is

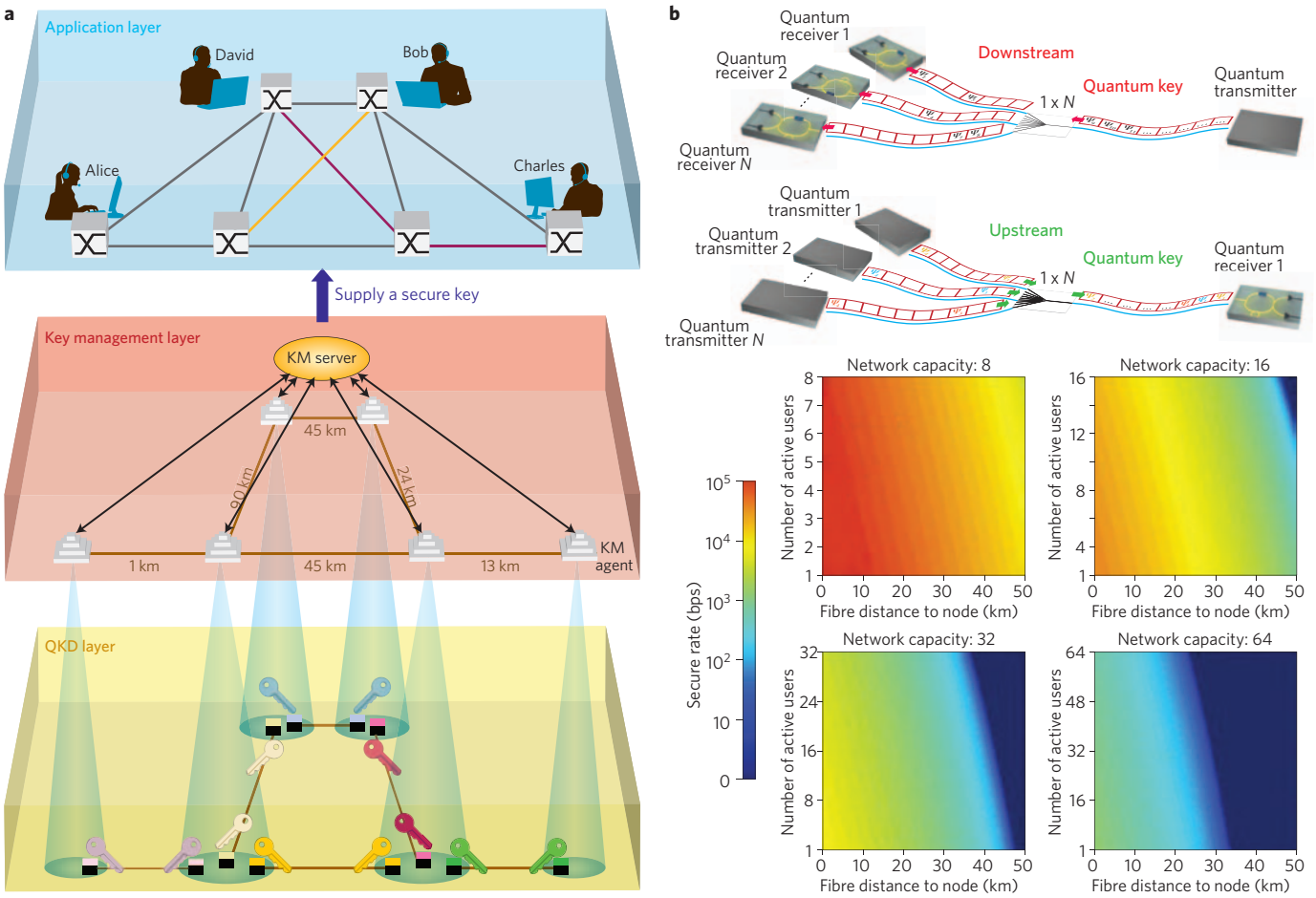

Figure 3 | QKD networks. a, Schematic of the layer structure of the Tokyo QKD network[13], which is based on a trusted node architecture. From the users' perspective, the QKD layer and the key management layer can be treated as a black box that supplies them with a secure key. They can be used in applications such as secure video meetings and secure communication via smart phones. Different QKD networks have been implemented in other countries (see, for instance, refs 7–12). **b**, (Upper subfigure) Downstream versus upstream passive quantum access network. In the upstream approach[14], single-photon detectors are located only at the network node. This may reduce the costs of the network and allow its detectors' bandwidth to be used more efficiently. Estimated secret key rate per user for an upstream solution as a function of the distance and the number of active users in the network for various network capacities (lower subfigure). Figure **b** adapted with permission from ref. 14 © 2013 NPG.

usually lower in the low-loss regime. As an alternative to polarization coding, one could also use, for instance, energy–time-entangled photon pairs.

For shorter distances (say below 100 km), other solutions exist that are simpler to implement experimentally. These are the distributed-phase-reference QKD protocols[42–44]. They differ from standard QKD schemes in that now Alice encodes the information coherently between adjacent pulses, rather than in individual pulses. This approach includes the differential-phase-shift[42,43] and the coherent-one-way[44] protocols. In the former, Alice prepares a train of WCPs of equal intensity and modulates their phases. On the receiving side, Bob uses a one-bit-delay Mach–Zehnder interferometer followed by two single-photon detectors to measure the incoming pulses. Similarly, in the coherent-one-way protocol all pulses share a common phase, but now Alice varies their intensities.

An important issue in any QKD implementation is its reliability and robustness in a real-life environment. Figure 2d shows the performance as a function of time of a QKD link from the SwissQuantum network installed in Geneva, Switzerland[9]. It demonstrates the high stability of current QKD systems.

The above-described protocols belong to the discrete-variable QKD schemes. Another interesting option is to use continuous-variable QKD systems[45–47]. The key feature of this solution is that now the detection device consists of (homodyne or heterodyne) measurements of the light-field quadratures. Consequently, these protocols can be implemented with standard telecom components and do not require single-photon detectors, making them also very suitable for experimental realizations.

QKD components and data processing. The following components are typically needed for the optical layer of a QKD system.

Light sources. Attenuated laser pulses can be used as the signal source in QKD. It is standard to model the signal as a WCP. Applying a global phase randomization causes the state to become a classical mixture of Fock states (that is, states of different photon numbers) with a Poissonian distribution.

Single-photon detectors. Single-photon detection is the ultimate limit of light detection. It is important not only in QKD applications, but also in sensitive measurements in astronomy and biomedical physics. Traditionally, two types of detectors have been widely used in QKD: silicon detectors and InGaAs detectors. Silicon detectors are broadly employed for visible wavelengths (for example, 800 nm) and in free-space implementations. They have rather high detection efficiencies of around 50%. InGaAs avalanche photodiodes are often

used at telecom wavelengths and for fibre optic communications. Previously, they suffered from low detection efficiencies of around 15% and had rather long dead times after a detection event, which severely limited the detection repetition rate to only a few megahertz. In the past few years, however, new detector technologies have been developed for QKD applications, including self-differencing avalanche photodiodes[48,49], the sine-wave gating technique[50–52], a hybrid approach that combines these two methods[53], and superconducting nanowire single-photon detectors (SNSPDs)[15]. All these approaches enable detection repetition rates of the order of gigahertz. Also, the detection efficiency of InGaAs avalanche photodiodes has been improved to about 50% at a wavelength of 1,310 nm (ref. 18), and new types of SNSPDs with very high detection efficiencies of around 93% have been developed[15–17]. The main drawback of these novel SNSPDs[15–17], however, is their operating temperature, which is currently of the order of 0.1 K. The dark count rate of these high-efficiency SNSPDs[15–17] is of the order of 100 Hz; it can be substantially improved by better rejection of ambient photons using optical band-pass filters at the input port of SNSPDs[54].

Standard linear optical components. Polarizing beamsplitters, beamsplitters, amplitude modulators and phase modulators are widely used in QKD applications.

Random number generators. Random numbers are needed for basis choice, bit value choice, phase randomization, intensity choice in the decoy-state method as well as for data post-processing. High-speed random number generation is a key bottleneck in current QKD. Fortunately, a lot of research has been conducted in the area. Quantum mechanics offers true randomness originating from the laws of physics[55]. A simple way to build a quantum random number generator is to send a WCP through a 50:50 beamsplitter and put two single-photon detectors on the two outgoing arms. The generated bit value (0 or 1) depends on which detector detects a photon. Other methods[56–58] also exist for designing quantum random number generators, including using phase noise[59].

Classical post-processing techniques. Processes such as post-selection of data (typically called sifting), error correction and privacy amplification are used to correct errors in the quantum transmission and to remove any residual information that Eve might have on the raw key. The final result is a key shared by Alice and Bob that Eve almost certainly has absolutely no information about. Current bottlenecks in high-speed QKD are the computational complexity of classical post-processing protocols and the need to process huge amounts of raw data in a very short time. Fortunately, advances have been made for algorithm speed-up using hardware-based solutions[5] (for example, the use of a field programmable gate array).

Authenticated channel. For QKD to work, Alice and Bob need to share an authenticated classical channel in addition to a quantum channel. Fortunately, this requires only a rather short authentication key, which may be provided in the initial shipment of the QKD system in a tamper-resistant device. Once a QKD session has succeeded, the authentication key can be refurbished from the key generated by QKD. In this sense, QKD is a key growing protocol. If no key is initially shared between Alice and Bob, they may also use a classical solution for authentication based on computational assumptions via a certifying authority, which is a standard protocol in the Internet. Provided that such an authentication scheme is unbroken for a short time during the first QKD session, the first QKD session will be secure and will generate the subsequent authentication keys.

Industrial/application perspectives. The field of QKD is of both fundamental and industrial interest. As mentioned above, commercial products offering encryption solutions based on this technology are already available. Also, QKD networks have been recently deployed in the USA[7], Austria[8], Switzerland[9], China[10–12] and Japan[13]. As an example, Fig. 3a shows the current structure of the Tokyo QKD network[13]. It uses an architecture based on trusted nodes, which are separated by distances in the range 1–90 km. The network consists of three main layers: a QKD layer, a key management layer and an application layer. In the QKD layer, QKD systems that connect neighbouring nodes continuously (that is, without any maintenance) generate secret key material[5,60]. This key, which is of the order of 300 Kbps when the link loss is around 14.5 dB (ref. 13), is forwarded to a key management agent placed in the key management layer. This agent monitors the key generation rate and the amount of stored keys.

Secure communication is possible between any nodes in the network by relaying on the secret key that is controlled by the command of the key management server. From the viewpoint of users, the QKD layer and the key management layer can be treated as a black box that supplies them with a secure key. Such a network could be employed, for instance, to provide secure communications with smart phones. Whenever a user needs a fresh secret key to protect her communication over the phone, she could connect to the QKD network and store the obtained key on her device for later use[13]. The Toshiba and Los Alamos groups have recently proposed new architectures for QKD networks: Fig. 3b compares the upstream passive quantum access network implemented by Toshiba[14] with a downstream approach and Fig. 2c shows the compact transmitter prepared by the Los Alamos group[37].

QKD systems have been used in the Swiss national elections to protect the line that transmitted the ballots to the counting station. They have also been used to secure a communication link at the 2010 FIFA Soccer World Cup in Durban, South Africa. Other potential applications of QKD include offsite backup, enterprise private networks, critical infrastructure protection, backbone protection and high-security access networks.

Technological challenges. As mentioned in the introduction, researchers are working on designing and building high-speed QKD systems[61] and the ability to multiplex strong classical signals with weak quantum signals in the same optical fibre[62–64]. Theorists are developing sophisticated techniques for increasing the key generation rate (which is currently limited to about 1 Mbps (refs 60,65–68)) and deal properly with various device imperfections of QKD implementations. To extend the distance of QKD, the ideas of both trusted and untrusted relay nodes have been studied. There has also been much interest in the concept of ground-to-satellite QKD. We survey some of these recent efforts here.

Multiplexing techniques. Very recently, a field test has been performed of a QKD system that multiplexes two quantum channels in the third telecom window using wavelength-division multiplying[5]. A very stable key generation rate was obtained from both channels over 30 days of operation without maintenance. This promising result supports the possibility of using wavelength-division multiplying techniques in QKD to increase its secure bit rate. Importantly, alternative results have also shown that quantum signals can also be combined with strong conventional telecom traffic in the same fibre[62–64], thus showing the feasibility of integrating QKD into existing fibre optical networks. In ref. 63, for example, a QKD channel is located at 1,310 nm, while classical channels use the third telecom window. A slight drawback of this solution, however, is the higher transmission loss of the fibre at 1,310 nm, which limits the achievable QKD rate and distance. In an alternative approach, Patel *et al.* used wavelengths around 1,550 nm in both the quantum and classical channels (refs 62,64). This permitted, for instance, a secure key rate exceeding 1 Mbps over 35 km of

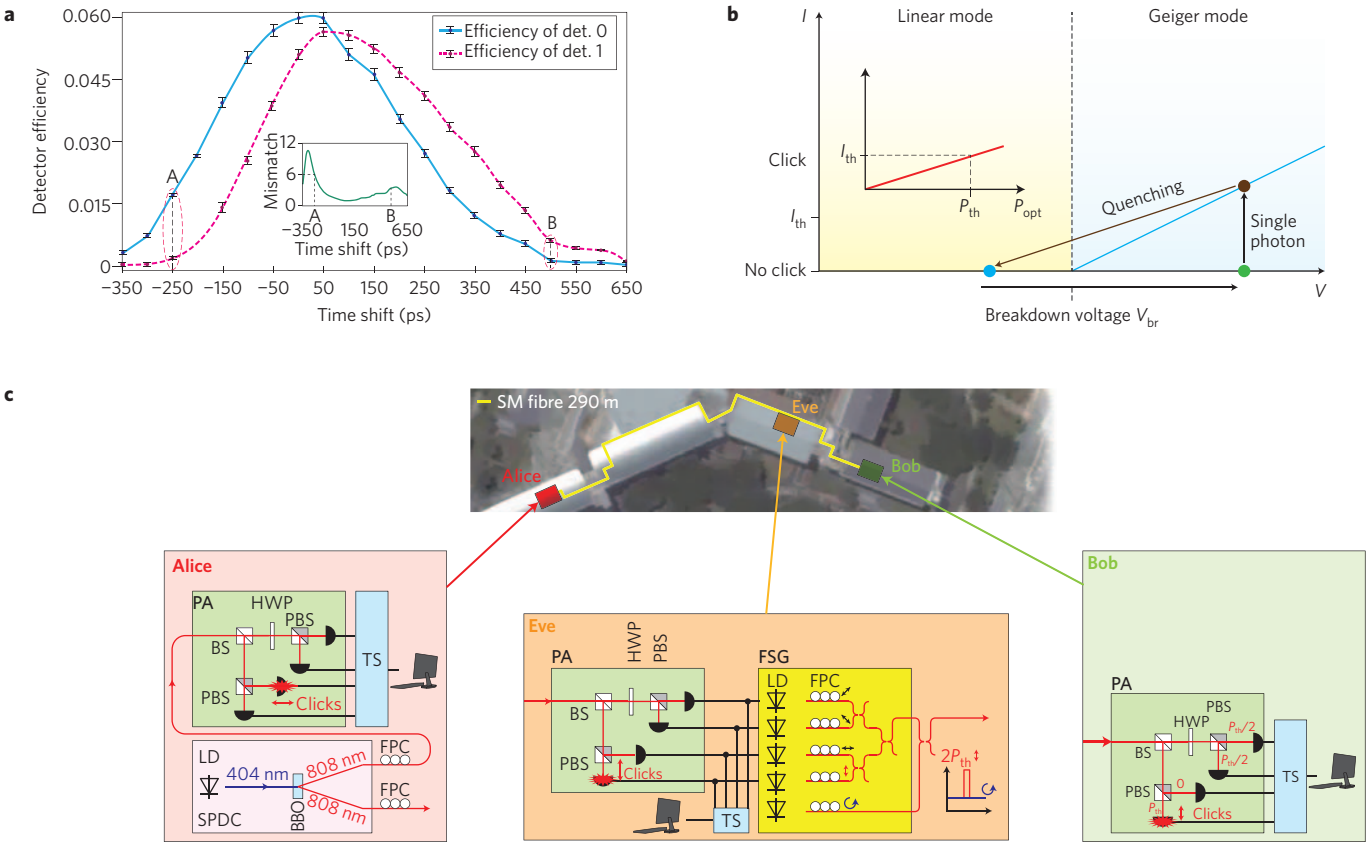

Figure 4 | Examples of quantum hacking. a, Experimentally measured detection efficiency mismatch between two detectors from a commercial QKD system versus time shifts[76]. Eve could exploit this to perform a time-shift attack[75]; that is, she could shift the arrival time of each signal such that one detector has a much higher detection efficiency than the other. **b**, Working principle of the detector blinding attack[80]. By shining intense light onto the detectors, Eve can make them leave Geiger-mode operation (used in QKD) and enter linear-mode operation. In so doing, she can control which detector produces a 'click' each given time and learn the entire secret key without being detected. **c**, Full-field implementation of a detector blinding attack on a running entanglement-based QKD set-up[83]. HWP, half-wave plate; PBS, polarizing beamsplitter; BS, beamsplitter; LD, laser diode; SPDC, spontaneous parametric downconversion, BBO; β-barium-borate crystal; FPC, fibre polarization controller; TS, timestamp unit; PA, polarization analyser; FSG, faked-state generator. Figure adapted with permission from: **a**, ref. 76 © 2008 APS; **b**, ref. 80 © 2010 NPG; **c**, ref. 83 © 2011 NPG.

fibre to be achieved when the intensity of the classical signals was around −18.6 dBm (ref. 62). Remarkably, the same research group has shown that QKD is also possible in a high data laser power environment of around 0 dBm (ref. 64). In this case, the secret key rate is of the order of hundreds of kilobits per second over 25 km of fibre. On the other hand, it turns out that continuous-variable QKD systems can also be quite robust against noise from strong telecom traffic due to multiplexing[69,70]. This is because the local oscillator acts as a 'mode selector'[71] to suppress the noise.

Development of theory. The key generation rate can also be increased by developing better security analysis. A practical security proof must account for statistical fluctuations arising from the finite data size. Therefore, the development of more-sophisticated techniques for such analysis can result in higher key rates[22,72,73]. Also, one could include modifications in the protocol such as, for instance, the use of a biased basis choice.

Extending QKD coverage. Up to this point, we have discussed different approaches for integrating QKD into existing fibre optical networks and for improving the key rate of a system. Another important parameter is the covered distance, which is typically limited to about 350 km (if entanglement-based schemes are used). Of course, this upper limit could be extended by employing ultralow-loss fibres[44]. In general, a simple solution for overcoming this distance limitation is to use trusted nodes, just as in the QKD networks described above. However, many trusted nodes are required to achieve secure communication over long distances (say over 10,000 km). Another possible solution is to use satellites, which could be employed as either trusted or untrusted nodes. In the former case, the satellite can be viewed as a trusted courier that can perform QKD as well as travel very fast in a certain orbit. In this way, QKD could be performed over the entire globe in the future. Indeed, a preliminary QKD experiment between ground and a hot-air balloon has been performed recently[20] (see also ref. 21). This demonstration is illustrated in Fig. 1c. It represents a first step towards realizing QKD between ground and low-earth-orbit satellites. Here, the development of accurate pointing techniques is a key technology. Satellites could also be employed to build a QKD network with untrusted nodes by using, for example, measurement-device-independent (MDI) QKD[74] (to be discussed below in the subsection "Countermeasures"), where the parties on the ground send quantum signals to the satellites that perform a joint measurement on the incoming signals. One could also place the source of an entanglement-based QKD protocol on a satellite and the receivers on the ground.

Quantum hacking and countermeasures

QKD is theoretically secure, but are experimental implementations of QKD also secure? Security proofs rely on assumptions, some of which are quite natural (such as the validity of quantum

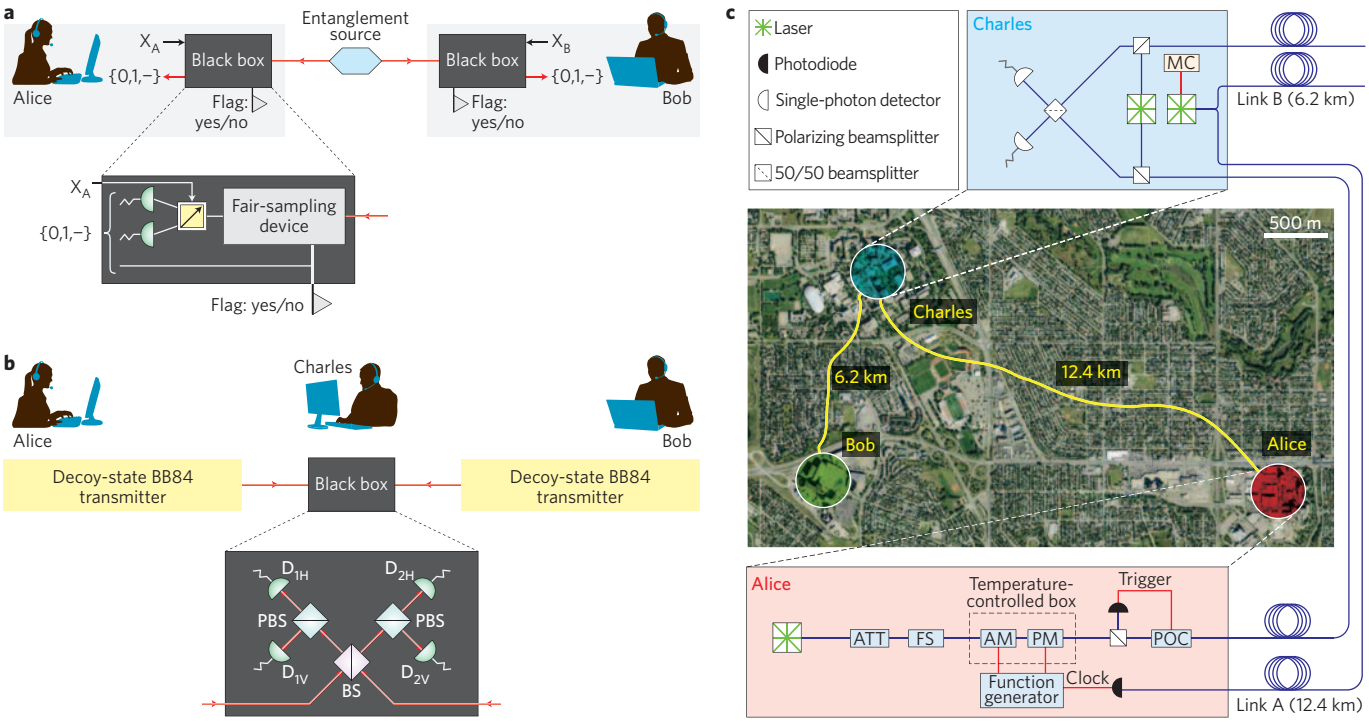

Figure 5 | Examples of countermeasures against quantum hacking. a, Schematic of DI-QKD[96–99]. Alice and Bob can prove the security of the protocol based on the violation of an appropriate Bell inequality. To overcome the channel loss, the system can include a fair-sampling device[100,101]. In principle, DI-QKD can remove all side channels in a QKD implementation. **b**, Schematic representation of MDI-QKD[74]. Alice and Bob prepare WCPs in different BB84 polarization states and send them to an untrusted relay Charles, who is supposed to perform a Bell-state measurement that projects the incoming signals into a Bell state. MDI-QKD removes all detector side channels, which can be regarded as the Achilles heel of QKD. MDI-QKD has the advantage over DI-QKD of being feasible with current technology. Indeed, proof-of-principle demonstrations have been already done[104,105], and real QKD implementations have been realized[106,107]. BS, beamsplitter; PBS, polarizing beamsplitter; D, single-photon detector. **c**, Field-test proof-of-principle demonstration of MDI-QKD realized in Calgary, Canada[104]. MC, master clock; AM, amplitude modulator; PM, phase modulator; ATT, variable attenuator; POC, polarization controller; FS, frequency shifter. Figure **c** reproduced with permission from ref. 104 © 2013 APS.

mechanics), whereas others are more severe (for example, that Alice and Bob have accurate and complete descriptions of their physical apparatuses). Unfortunately, real-life realizations of QKD often have imperfections, so that they rarely conform to the theoretical models used to prove their security. As a result, there is a gap between the theory and practice of QKD. Even though QKD has been proved in principle to be secure, practical systems may contain security loopholes (so-called side-channels), which Eve may exploit to learn the distributed key without being detected.

Indeed, this approach has been used in recent attacks on certain commercial and research QKD set-ups[75–90]. In these attacks, Eve exploited some imperfections in devices (especially single-photon detectors) to hack the system. This is not overly alarming at this stage, as current realizations of QKD are still in the battle-testing phase. The first versions of new commercial cryptographic schemes routinely contain some security flaws in their implementation, which are typically found and fixed during the battle-testing period. Consequently, the systems become increasingly secure. In addition, QKD is often combined with classical cryptography (for instance, by performing a bitwise XOR operation between a classical key and a key obtained with QKD), so that QKD can only enhance the final security of the whole system.

Table 1. Summary of various quantum hacking attacks against certain commercial and research QKD set-ups.

Attack	Target component	Tested system
Time shift[75–78]	Detector	Commercial system
Time information[79]	Detector	Research system
Detector control[80–82]	Detector	Commercial system
Detector control[83]	Detector	Research system
Detector dead time[84]	Detector	Research system
Channel calibration[85]	Detector	Commercial system
Phase remapping[86]	Phase modulator	Commercial system
Faraday mirror[87]	Faraday mirror	Theory
Wavelength[88]	Beamsplitter	Theory
Phase information[89]	Source	Research system
Device calibration[90]	Local oscillator	Research system

Quantum hacking. What kind of imperfections can Eve exploit to hack a QKD system? In principle, QKD secures only the communication channel, so Eve may try to attack both the source (that is, the preparation stage of the quantum signals) and the measurement device. Table 1 lists various attacks on QKD set-ups that have been proposed to date. The source is typically less vulnerable to attack, because Alice can prepare her quantum signals (for example, the polarization state of phase-randomized WCPs) in a fully protected environment that an eavesdropper cannot access. This environment can be achieved by, for instance, using optical isolators. Also, Alice can experimentally verify the quantum states emitted by employing, for example, random sampling techniques. It is thus reasonable to expect that Alice can characterize her source. Fortunately, in this situation, it is usually relatively easy to incorporate any imperfections in Alice's state preparation process in the security proof[25,91].

Bob's measurement device is more problematic, as Eve is allowed to send in any signal she desires, making it harder to protect Bob's

set-up against possible attacks. Indeed, most quantum hacking strategies are directed at Bob's single-photon detectors[75–85], which can be regarded as the Achilles heel of QKD. For instance, Eve could exploit their detection efficiency mismatch[75–78] (see Fig. 4a). However, the most important hacking attack so far against the detectors of a system is the detector-blinding attack[80]. Here, Eve shines bright light onto the detectors to make them enter linear-mode operation, so that they are no longer sensitive to single-photon pulses, but can detect only strong light pulses[80]. Consequently, Eve can effectively fully control which detector produces a 'click' at any given time by just sending Bob additional bright pulses. In this way, Eve can learn the entire secret key[83] (see Figs 4b,c). Another imperfection that could be exploited is the dead time of the detectors[84].

Countermeasures. A natural solution for recovering security in QKD implementations is to develop mathematical models that perfectly match the behaviour of all QKD components and systems, and then incorporate this information in a new security proof. Although this is plausible in theory, it is hard (if not impossible) to realize in practice, because of the complexity of QKD components. There are currently three main alternative approaches.

The first is to use security patches. It is generally quite easy to obtain a suitable countermeasure each time a security loophole is discovered[92–95]. Although this guarantees security against known attacks, new hacking strategies may defeat the system. This results in a similar scenario to that for most classical cryptographic techniques, as it abandons the provable security model of QKD.

The second approach is device-independent (DI) QKD[96–99]; it is depicted in Fig. 5a. Here, Alice and Bob treat their devices as two black boxes in that they do not need to fully characterize their different elements. The security of DI-QKD relies on the violation of a Bell inequality, which confirms the presence of quantum correlations. However, a loophole-free Bell test is still unavailable, because of the detection efficiency loophole (which requires a detection efficiency of around 80% or higher). Indeed, the high coupling and channel loss, together with the limited detection efficiency of current single-photon detectors, render DI-QKD highly impractical with current technology. Even if Alice and Bob try to compensate the channel loss by including a fair-sampling device (such as a qubit amplifier[100,101] or a quantum non-demolition measurement of the number of photons in a pulse), the resulting secret key rate of DI-QKD at practical distances is very limited (of the order 10^{-10} bits per pulse)[100,101]. Of course, technology is improving, and DI-QKD may become viable in the next 10–15 years. Thus, the first approach to counter the quantum hacking problem is ad hoc, whereas DI-QKD is currently impractical.

The third approach is MDI-QKD[74], which appears to be a potential viable solution to the quantum hacking problem (Figs 5b,c). The main advantage of this approach is that it allows Alice and Bob to perform QKD with untrusted measurement devices, which can even be manufactured by Eve. In other words, MDI-QKD completely removes the weakest part of a QKD realization and offers a way to bridge the gap between theory and practice. The security of MDI-QKD is based on the idea of time reversal[102,103]. Alice and Bob prepare quantum signals and send them to an untrusted relay, Charles/Eve, who is supposed to perform a Bell-state measurement on the signals received. The honesty of Charles can be verified by comparing a subset of the transmitted data. Most importantly, MDI-QKD can be implemented using standard optical components, including low-detection-efficiency detectors and highly lossy channels. The key rate of MDI-QKD is many orders of magnitude higher than that of DI-QKD, and the experimental feasibility of MDI-QKD has been demonstrated in both the laboratory and field tests[104–107]. The key assumption in MDI-QKD is that Alice and Bob trust their sources. As noted earlier, this may not be unreasonable, because, compared with single-photon detectors that receive unknown quantum states prepared by Eve, it is much easier for Alice and Bob to carefully monitor their own preparation process within their own laboratories. In fact, as mentioned above, source flaws can be taken care of in security proofs[25,91]. A slight drawback of MDI-QKD is that it has a lower secret key rate than the decoy-state BB84 protocol. This is because MDI-QKD requires two-fold coincidence detector events, which are suppressed due to the low detection efficiency of standard InGaAs single-photon detectors. This disadvantage can be overcome by using the above-mentioned SNSPDs with a 93% detection efficiency. Also, MDI-QKD could be used to build a QKD network with untrusted nodes, which would be desirable from a security standpoint.

Outlook

In an effort to further extend the distance of secure quantum communication, much research has focused on quantum repeaters[108], which allow entanglement to be swapped and distilled between pairs of entangled photons.

If MDI-QKD is widely deployed in the future, the focus of quantum hacking will shift towards attacking the source, rather than the detectors. It will then become important to re-examine the various security assumptions used (for example, the assumptions of single-mode operation, perfect global phase randomization and no side channels). Hence, the eternal conflict between code-makers and code-breakers is set to continue.

Owing to space limitations, this Review has focused on QKD. Other applications of quantum cryptography (including quantum secret sharing, blind quantum computing and quantum coin flipping) have been proposed, whereas others (such as quantum bit commitment) have been demonstrated to be impossible without additional assumptions.

In summary, we have highlighted the deep connections that exist between quantum cryptography and other areas of physics as well as mathematics and technology. For instance, the loopholes in the security of practical QKD systems are closely related to the loopholes in the testing of Bell's inequalities in the foundations of quantum mechanics. Quantum cryptography is also closely related to mathematics, information theory and statistics, as it widely uses concepts in those fields. Furthermore, quantum cryptography provides much impetus to the technological development of single-photon detectors, which can also have the potential to improve quantum metrology and sensing and contribute to the ultimate goal — the construction of large-scale quantum computers.

Received 13 November 2013; accepted 10 June 2014;
published online 31 July 2014

References

1. Rivest, R. L., Shamir, A. & Adleman, L. M. A method of obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **21,** 120–126 (1978).
2. Shor, P. W. Algorithms for quantum computation: discrete logarithms and factoring. in *Proc. 35th Ann. Symp. Found. Comp. Sci.* (ed. Goldwasser, S.) 124–134 (IEEE, 1994).
3. Ben-Or, M., Horodecki, M., Leung, D. W., Mayers, D. & Oppenheim, J. The universal composable security of quantum key distribution. in *Theory of Cryptography* (ed. Kilian, J.) **3378,** 386–406 (Springer, 2005).
4. Renner, R. & König, R. Universally composable privacy amplification against quantum adversaries. in *Theory of Cryptography* (ed. Kilian, J.) **3378,** 407–425 (Springer, 2005).
5. Yoshino, K., Ochi, T., Fujiwara, M., Sasaki, M. & Tajima, A. Maintenance-free operation of WDM quantum key distribution system through a field fiber over 30 days. *Opt. Express* **21,** 31395–31401 (2013).
6. Ursin, R. *et al.* Entanglement-based quantum communication over 144 km. *Nature Phys.* **3,** 481–486 (2007).
7. Elliott, C. *et al.* Current status of the DARPA Quantum Network. in *Proc. SPIE* (eds Donkor, E. J., Pirich, A. R. & Brandt, H. E.) **5815,** 138–149 (SPIE, 2005).
8. Peev, M. *et al.* The SECOQC quantum key distribution network in Vienna. *New J. Phys.* **11,** 075001 (2009).
9. Stucki, D. *et al.* Long-term performance of the SwissQuantum quantum key distribution network in a field environment. *New J. Phys.* **13,** 123001 (2011).

10. Chen, T.-Y. *et al.* Field test of a practical secure communication network with decoy-state quantum cryptography. *Opt. Express* **17,** 6540–6549 (2009).
11. Chen, T.-Y. *et al.* Metropolitan all-pass and inter-city quantum communication network. *Opt. Express* **18,** 27217–27225 (2010).
12. Wang, S. *et al.* Field test of wavelength-saving quantum key distribution network. *Opt. Lett.* **35,** 2454–2456 (2010).
13. Sasaki, M. *et al.* Field test of quantum key distribution in the Tokyo QKD network. *Opt. Express* **19,** 10387–10409 (2011).
14. Fröhlich, B. *et al.* A quantum access network. *Nature* **501,** 69–72 (2013).
15. Marsili, F. *et al.* Detecting single infrared photons with 93% system efficiency. *Nature Photon.* **7,** 210–214 (2013).
16. Rosenberg, D., Kerman, A. J., Molnar, R. J. & Dauler, E. A. High-speed and high-efficiency superconducting nanowire single photon detector array. *Opt. Express* **21,** 1440–1447 (2013).
17. Miki, S., Yamashita, T., Terai, H. & Wang, Z. High performance fiber-coupled NbTiN superconducting nanowire single photon detectors with Gifford-McMahon cryocooler. *Opt. Express* **21,** 10208–10214 (2013).
18. Restelli, A., Bienfang, J. C. & Migdall, A. L. Single-photon detection efficiency up to 50% at 1310 nm with an InGaAs/InP avalanche diode gated at 1.25 GHz. *Appl. Phys. Lett.* **102,** 141104 (2013).
19. Bennett, C. H., Bessette, F., Brassard, G., Salvail, L. & Smolin, J. Experimental quantum cryptography. *J. Cryptol.* **5,** 3–28 (1992).
20. Wang, J.-Y. *et al.* Direct and full-scale experimental verifications towards ground-satellite quantum key distribution. *Nature Photon.* **7,** 387–393 (2013).
21. Nauerth, S. *et al.* Air-to-ground quantum communication. *Nature Photon.* **7,** 382–386 (2013).
22. Lim, C. C. W., Curty, M., Walenta, N., Xu, F. & Zbinden, H. Concise security bounds for practical decoy-state quantum key distribution. *Phys. Rev. A* **89,** 022307 (2014).
23. Bennett, C. H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. in *Proc. IEEE Int. Conf. Comp. Systems Signal Processing* 175–179 (IEEE, 1984).
24. Huttner, B., Imoto, N., Gisin, N. & Mor, T. Quantum cryptography with coherent states. *Phys. Rev. A* **51,** 1863–1869 (1995).
25. Gottesman, D., Lo, H.-K., Lütkenhaus, N. & Preskill, J. Security of quantum key distribution with imperfect devices. *Quant. Inf. Comp.* **5,** 325–360 (2004).
26. Hwang, W.-Y. Quantum key distribution with high loss: toward global secure communication. *Phys. Rev. Lett.* **91,** 057901 (2003).
27. Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94,** 230504 (2005).
28. Wang, X.-B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94,** 230503 (2005).
29. Ma, X., Qi, B., Zhao, Y. & Lo, H.-K. Practical decoy state for quantum key distribution. *Phys. Rev. A* **72,** 012326 (2005).
30. Zhao, Y., Qi, B., Ma, X., Lo, H.-K. & Qian, L. Experimental quantum key distribution with decoy states. *Phys. Rev. Lett.* **96,** 070502 (2006).
31. Peng, C.-Z. *et al.* Experimental long-distance decoy-state quantum key distribution based on polarization encoding. *Phys. Rev. Lett.* **98,** 010505 (2007).
32. Rosenberg, D. *et al.* Long-distance decoy-state quantum key distribution in optical fiber. *Phys. Rev. Lett.* **98,** 010503 (2007).
33. Schmitt-Manderbach, T. *et al.* Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Phys. Rev. Lett.* **98,** 010504 (2007).
34. Yuan, Z. L., Sharpe, A. W. & Shields, A. J. Unconditionally secure one-way quantum key distribution using decoy pulses. *Appl. Phys. Lett.* **90,** 011118 (2007).
35. Liu, Y. *et al.* Decoy-state quantum key distribution with polarized photons over 200 km. *Opt. Express* **18,** 8587–8594 (2010).
36. Wehner, S., Curty, M., Schaffner, C. & Lo, H.-K. Implementation of two-party protocols in the noisy-storage model. *Phys. Rev. A* **81,** 052336 (2010).
37. Hughes, R. J. *et al.* Network-centric quantum communications with application to critical infrastructure protection. Preprint at http://lanl.arXiv.org/abs/1305.0305 (2013).
38. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67,** 661–663 (1991).
39. Ma, X., Fung, C.-H. F. & Lo, H.-K. Quantum key distribution with entangled photon sources. *Phys. Rev. A* **76,** 012307 (2007).
40. Treiber, A. *et al.* Fully automated entanglement-based quantum cryptography system for telecom fiber networks. *New J. Phys.* **11,** 045013 (2009).
41. Poppe, A. *et al.* Practical quantum key distribution with polarization-entangled photons. *Opt. Express* **12,** 3865–3871 (2004).
42. Inoue, K., Waks, E. & Yamamoto, Y. Differential phase shift quantum key distribution. *Phys. Rev. Lett.* **89,** 037902 (2002).
43. Takesue, H. *et al.* Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors. *Nature Photon.* **1,** 343–348 (2007).
44. Stucki, D. *et al.* High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres. *New J. Phys.* **11,** 075003 (2009).
45. Grosshans, F. *et al.* Quantum key distribution using gaussian-modulated coherent states. *Nature* **421,** 238–241 (2003).
46. Qi, B., Huang, L.-L., Qian, L. & Lo, H.-K. Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers. *Phys. Rev. A* **76,** 052323 (2007).
47. Jouguet, P., Kunz-Jacques, S., Leverrier, A., Grangier, P. & Diamanti, E. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nature Photon.* **7,** 378–381 (2013).
48. Yuan, Z. L., Kardynal, B. E., Sharpe, A. W. & Shields, A. J. High speed single photon detection in the near infrared. *App. Phys. Lett.* **91,** 041114 (2007).
49. Dixon, A. R. *et al.* Ultrashort dead time of photon-counting InGaAs avalanche photodiodes. *Appl. Phys. Lett.* **94,** 231113 (2009).
50. Namekata, N., Sasamori, S. & Inoue, S. 800 MHz single-photon detection at 1550-nm using an InGaAs/InP avalanche photodiode operated with a sine wave gating. *Opt. Express* **14,** 10043–10049 (2006).
51. Liang, X.-L. *et al.* Fully integrated InGaAs/InP single-photon detector module with gigahertz sine wave gating. *Rev. Sci. Instrum.* **83,** 083111 (2012).
52. Wu, Q.-L., Namekata, N. & Inoue, S. Sinusoidally gated InGaAs avalanche photodiode with direct hold-off function for efficient and low-noise single-photon detection. *Appl. Phys. Express* **6,** 062202 (2013).
53. Zhang, J., Thew, R., Barreiro, C. & Zbinden, H. Practical fast gate rate InGaAs/InP single-photon avalanche photodiodes. *Appl. Phys. Lett.* **95,** 091103 (2009).
54. Shibata, H., Takesue, H., Honjo, T., Akazaki, T. & Tokura, Y. Single-photon detection using magnesium diboride superconducting nanowires. *Appl. Phys. Lett.* **97,** 212504 (2010).
55. Pironio, S. *et al.* Random numbers certified by Bell's theorem. *Nature* **464,** 1021–1024 (2010).
56. Williams, C. R. S., Salevan, J. C., Li, X., Roy, R. & Murphy, T. E. Fast physical random number generator using amplified spontaneous emission. *Opt. Express* **18,** 23584–23597 (2010).
57. Jofre, M. *et al.* True random numbers from amplified quantum vacuum. *Opt. Express* **19,** 20665–20672 (2011).
58. Abellán, C. *et al.* Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode. *Opt. Express* **22,** 1645–1654 (2014).
59. Qi, B., Chi, Y.-M., Lo, H.-K. & Qian, L. High-speed quantum random number generation by measuring phase noise of a single-mode laser. *Opt. Lett.* **35,** 312–314 (2010).
60. Dixon, A. R., Yuan, Z. L., Dynes, J. F., Sharpe, A. W. & Shields, A. J. Continuous operation of high bit rate quantum key distribution. *Appl. Phys. Lett.* **96,** 161102 (2010).
61. Choi, I., Young, R. J. & Townsend, P. D. Quantum key distribution on a 10Gb/s WDM-PON. *Opt. Express* **18,** 9600–9612 (2010).
62. Patel, K. A. *et al.* Coexistence of high-bit-rate quantum key distribution and data on optical fiber. *Phys. Rev. X* **2,** 041010 (2012).
63. Chapuran, T. E. *et al.* Optical networking for quantum key distribution and quantum communications. *New J. Phys.* **11,** 105001 (2009).
64. Patel, K. A. *et al.* Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks. *Appl. Phys. Lett.* **104,** 051123 (2014).
65. Dixon, A. R., Yuan, Z. L., Dynes, J. F., Sharpe, A. W. & Shields, A. J. Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate. *Opt. Express* **16,** 18790–18979 (2008).
66. Zhang, Q. *et al.* Megabits secure key rate quantum key distribution. *New J. Phys.* **11,** 045010 (2009).
67. Tanaka, A. *et al.* High-speed quantum key distribution system for 1-Mbps real-time key generation. *IEEE J. Quant. Electron.* **48,** 542–550 (2012).
68. Walenta, N. *et al.* 1 Mbps coherent one-way QKD with dense wavelength division multiplexing and hardware key distillation. in *Proc. 2nd Ann. Conf. Quantum Cryptography* (2012).
69. Qi, B., Zhu, W., Qian, L. & Lo, H.-K. Feasibility of quantum key distribution through dense wavelength division multiplexing network. *New J. Phys.* **12,** 103042 (2010).
70. Jouguet, P. *et al.* Experimental demonstration of the coexistence of continuous-variable quantum key distribution with an intense DWDM classical channel. in *Proc. 3rd Ann. Conf. Quantum Cryptography* (2013).
71. Raymer, M. G., Cooper, J., Carmichael, H. J., Beck M. & Smithey, D. T. Ultrafast measurement of optical-field statistics by dc-balanced homodyne detection. *J. Opt. Soc. Am. B* **12,** 1801–1812 (1995).
72. Hayashi, M. & Tsurumaru, T. Concise and tight security analysis of the Bennett–Brassard 1984 protocol with finite key lengths. *New J. Phys.* **14,** 093014 (2012).
73. Curty, M. *et al.* Finite-key analysis for measurement-device-independent quantum key distribution. *Nature Commun.* **5,** 3732 (2014).
74. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108,** 130503 (2012).
75. Qi, B., Fung, C.-H. F., Lo, H.-K. & Ma, X. Time-shift attack in practical quantum cryptosystems. *Quant. Inf. Comp.* **7,** 73–82 (2007).

76. Zhao, Y., Fung, C.-H. F., Qi, B., Chen, C. & Lo, H.-K. Quantum hacking: experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Phys. Rev. A* **78,** 042333 (2008).
77. Makarov, V., Anisimov, A. & Skaar, J. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Phys. Rev. A* **74,** 022313 (2006).
78. Makarov, V., Anisimov, A. & Skaar, J. Erratum: effects of detector efficiency mismatch on security of quantum cryptosystems [Phys. Rev. A **74**, 022313 (2006)]. *Phys. Rev. A* **78,** 019905 (2008).
79. Lamas-Linares, A. & Kurtsiefer, C. Breaking a quantum key distribution system through a timing side channel. *Opt. Express* **15,** 9388–9393 (2007).
80. Lydersen, L. *et al.* Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photon.* **4,** 686–689 (2010).
81. Yuan, Z. L., Dynes, J. F. & Shields, A. J. Avoiding the blinding attack in QKD. *Nature Photon.* **4,** 800–801 (2010).
82. Lydersen, L. *et al.* Reply to "Avoiding the blinding attack in QKD". *Nature Photon.* **4,** 801 (2010).
83. Gerhardt, I. *et al.* Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nature Commun.* **2,** 349 (2011).
84. Weier, H. *et al.* Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors. *New J. Phys.* **13,** 073024 (2011).
85. Jain, N. *et al.* Device calibration impacts security of quantum key distribution. *Phys. Rev. Lett.* **107,** 110501 (2011).
86. Xu, F., Qi, B. & Lo, H.-K. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. *New J. Phys.* **12,** 113026 (2010).
87. Sun, S.-H., Jiang, M.-S. & Liang, L.-M. Passive Faraday-mirror attack in a practical two-way quantum-key-distribution system. *Phys. Rev. A* **83,** 062331 (2011).
88. Huang, J.-Z. *et al.* Quantum hacking on continuous-variable quantum key distribution system using a wavelength attack. *Phys. Rev. A* **87,** 062329 (2013).
89. Tang, Y.-L. *et al.* Source attack of decoy-state quantum key distribution using phase information. *Phys. Rev. A* **88,** 022308 (2013).
90. Jouguet, P., Kunz-Jacques, S. & Diamanti, E. Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution. *Phys. Rev. A* **87,** 062313 (2013).
91. Tamaki, K., Curty, M., Kato, G., Lo, H.-K. & Azuma, K. Loss-tolerant quantum cryptography with imperfect sources. Preprint at http://lanl.arXiv.org/abs/1312.3514 (2013).
92. Yuan, Z. L., Dynes, J. F. & Shields, A. J. Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography. *Appl. Phys. Lett.* **98,** 231104 (2011).
93. Lydersen, L., Makarov, V. & Skaar, J. Comment on "Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography". *Appl. Phys. Lett.* **99,** 196101 (2011).
94. Yuan, Z. L., Dynes, J. F. & Shields, A. J. Response to "Comment on 'Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography'" *Appl. Phys. Lett.* **99,** 196102 (2011).
95. Honjo, T. *et al.* Countermeasure against tailored bright illumination attack for DPS-QKD. *Opt. Express* **21,** 2667–2673 (2013).
96. Mayers, D. & Yao, A. Quantum cryptography with imperfect apparatus. in *Proc. 39th Ann. Symp. Foundations Comp. Sci.* 503–509 (IEEE, 1998).
97. Masanes, L., Pironio, S. & Acín, A. Secure device-independent quantum key distribution with causally in-dependent measurement devices. *Nature Commun.* **2,** 238 (2011).
98. Reichardt, B. W., Unger, F. & Vazirani, U. Classical command of quantum systems. *Nature* **496,** 456–460 (2013).
99. Vazirani, U. & Vidick, T. Fully device independent quantum key distribution. Preprint at http://lanl.arXiv.org/abs/1210.1810 (2012).
100. Gisin, N., Pironio, S. & Sangouard, N. Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier. *Phys. Rev. Lett.* **105,** 070501 (2010).
101. Curty, M. & Moroder, T. Heralded-qubit amplifiers for practical device-independent quantum key distribution. *Phys. Rev. A* **84,** 010304(R) (2011).
102. Biham, E., Huttner, B. & Mor, T. Quantum cryptographic network based on quantum memories. *Phys. Rev. A* **54,** 2651–2658 (1996).
103. Inamori, H. Security of practical time-reversed EPR quantum key distribution. *Algorithmica* **34,** 340–365 (2002).
104. Rubenok, A., Slater, J. A., Chan, P., Lucio-Martinez, I. & Tittel, W. Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks. *Phys. Rev. Lett.* **111,** 130501 (2013).
105. Ferreira da Silva, T. *et al.* Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits. *Phys. Rev. A* **88,** 052303 (2013).
106. Liu, Y. *et al.* Experimental measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **111,** 130502 (2013).
107. Tang, Z. *et al.* Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **112,** 190503 (2014).
108. Briegel, H.-J., Dür, W., Cirac, J. I. & Zoller, P. Quantum repeaters: the role of imperfect local operations in quantum communication. *Phys. Rev. Lett.* **81,** 5932–5935 (1998).
109. Vernam, G. S. Cipher printing telegraph systems: for secret wire and radio telegraphic communications. *J. Am. Inst. Electr. Eng.* **45,** 109–115 (1926).

Acknowledgements

The authors thank K. Azuma, C. H. Bennett, M. Fujiwara, G. Kato, N. Matsuda, N. Namekata, T. Ochi, B. Qi, L. Qian, M. Sasaki, H. Shibata, H. Takesue, F. Xu, K. Yoshino, Q. Zhang, Y. Zhao and the anonymous referees for their valuable comments and suggestions. We specially thank C. H. Bennett and R. J. Hughes for allowing us to use photographs of the first experimental demonstration of QKD and of the first-generation, modularly integrated QKarD respectively in this Review. We thank Z. Tang for technical support in formatting our manuscript. We acknowledge support from the European Regional Development Fund (ERDF), the Galician Regional Government (projects CN2012/279 and CN 2012/260, "Consolidation of Research Units: AtlantTIC"), NSERC, the CRC program, the Connaught Innovation Award, and the project "Secure Photonic Network Technology" as part of the project UQCC by the National Institute of Information and Communications Technology (NICT) of Japan, as well as from the Japan Society for the Promotion of Science (JSPS) through its Funding Program for World-Leading Innovative R&D on Science and Technology (FIRST Program).

Additional information

Correspondence and requests for materials should be addressed to H.-K.L.

Competing financial interests

H.-K.L. is a named inventor on US Patent #8,554,814, "Random signal generator using quantum noise" (2013), which is related to the methods described in ref. 59. M.C. is a named inventor on patents and pending patents related to the methods described in refs 57 and 58. K.T. declares no competing financial interests other than his employment with NTT, Basic Research Lab.