Quantum networks: where should we be heading?

To cite this article: Masahide Sasaki 2017 Quantum Sci. Technol. 2 020501

View the article online for updates and enhancements.
Quantum networks: where should we be heading?

Masahide Sasaki
Quantum ICT Advanced Development Center, National Institute of Information and Communications Technology, 4-2-1, Nukuikita, Koganei, Tokyo 184-8795 Japan
E-mail: psasaki@nict.go.jp

Keywords: quantum key distribution, quantum repeater, quantum network, secret sharing, physical layer cryptography

Abstract
Quantum key distribution network has become a reality in practical environment. Quantum repeaters have been explored in various physical systems and their combinations. For practical use of them, these new paradigms must be combined with existing or emerging infrastructures of communication and security systems. In this article, we discussed how quantum network can be combined with modern cryptographic technologies in fibre network and with emerging mobile terminals in wireless network, creating new solutions for the future cryptographic and communication systems. Our discussions are summarised in a roadmap.

1. Introduction
Quantum key distribution (QKD) is the most promising application of quantum information technologies. When the key as long as the message to be sent is prepared by QKD and used only once, namely by one-time pad (OTP), the encrypted message can never be decrypted by any amount of computation, even by the most powerful computers. QKD can be implemented with currently available laser sources, optical components and photon/photo detectors. The key generation rate of a state-of-the-art system is about 1 Mbps at most over a reasonable fibre distance, say 50 km, per channel. The key generation rate decreases exponentially as the link distance increases, resulting in about 10 kbps at 100 km. At present networking of QKD is made by using trusted nodes in such a way that a key is relayed up to a terminal by OTP encapsulation, spending the keys generated in neighbouring QKD links [1–6]. The largest QKD network constructed in China [7] consists of four metropolitan QKD networks in Beijing, Jinan, Hefei, and Shanghai, and a 2000 km backbone connecting them by 32 trusted nodes. Very recently quantum science satellite was launched, aiming at the demonstration of QKD and quantum communications in the global scale [8].

Quantum repeaters are expected to extend the distances between trusted nodes. They allow for fully quantum networking in which the entanglement can be swapped and relayed via quantum nodes, and finally shared between any distant terminals [9, 10]. The entanglement thus shared can be used for QKD which has higher resistance against side channel attacks [11–13]. Quantum repeaters can also allow connecting quantum computers, enabling quantum internet [14]. To this end, quantum processors and memories as well as interfaces with photons must be developed and implemented onto a circuit. Extensive researches on quantum repeaters have been conducted using various physical systems, such as cavity-QED system with atoms or ions [15–17], quantum dot [18, 19], atomic ensemble in laser cooling or solid state device [20], and colour centres in diamond [21–23]. However, for them to be deployed in practical environments, further research and development are still needed.

Although QKD has already been commercialised and QKD networks have become a reality, the size of the market is still niche at present. It should be noted that even when technologies of QKD and quantum repeaters themselves are well matured sometime in the future, it does NOT necessarily mean that potential users such as governments, enterprises and consumers will start to use them. Today, various cryptographic functions such as authentication, signature, key exchange, encryption, secret computation and so on, are realised in communication infrastructures and computing systems by using public key cryptography, symmetric key...
cryptography, hash functions, secret sharing and so on. These cryptographic technologies are cost effective, and have already been used for a long time. In military and national security purposes, trusted courier systems for key delivery have been operated even for a longer time. It may be a tough and time-consuming task for QKD to be adopted for wider use in the existing security infrastructure, because the function of QKD itself is limited only to point-to-point symmetric key exchange, and because its performance is still limited. It should be important to invest more effort in developing total security systems which really need QKD as an essential part, and also provide all the necessary cryptographic functions in a comprehensive manner.

One such example is a distributed storage network to protect critical data securely for a long-term by using secret sharing. This scheme requires private channels connecting data servers to protect perfect confidentiality in data transmission. Algorithmic cryptography based on computational security cannot be adopted for this purpose of long-term security. QKD provides the very solution for it. However, secret sharing and QKD themselves cannot ensure the integrity of data in storage. The integrity protection can be done by modern cryptography (digital signatures and commitments) because it is sufficient to ensure the short-term security for a certain period, and the validity of the original data can be prolonged for any length of time by renewing the digital signatures and commitments with appropriate security parameters. All these technologies need to be combined for the long-term secure storage network.

Recent progress of mobile terminals such as automotive cars, unmanned aerial vehicles (UAVs) and satellites promises for a new field of information and communications technology (ICT). These mobile terminals are connected via wireless networks, and provide a variety of new services. Data-intensive sensors mounted on them produce a large amount of data, which can hardly be handled using conventional RF communications only. Free space optical (FSO) communication has evolved as a promising alternative for high-capacity data links in space. FSO communication is much harder to eavesdrop because of the directionality of laser beam, hence it can potentially form highly secure backbone links. In fact, it can provide a platform for QKD if photon counters or quantum-limited photo detectors are combined, which enables hack-proof data links, and it can also provide physical layer cryptography if appropriate error-correcting codes and signal processing for key distillation are combined that can ensure information theoretically secure data links under the condition of the line-of-sight. QKD and physical layer cryptography will be important topics in the new field of mobile communications network [24].

In this article, we pick up two topics; (1) how to combine modern cryptography and QKD for implementing a long-term integrity and confidentiality protection system, which relies on fibre networks and (2) how to introduce QKD and physical layer cryptography to the emerging mobile communications network, which relies on wireless network in space. We analyse what the important requirements in these use cases are and discuss the new challenges of the next decade.

2. QKD as one of cryptographic technologies

QKD is a means to share a symmetric key between two distant parties, Alice and Bob, in a secure way even against an eavesdropper, Eve, who has unbounded ability. This is an important cryptographic function, but only a part of functions those are required in cryptographic systems and infrastructures. Figure 1 roughly summarises main cryptographic technologies in a diagram of functions versus operation speed. Here, the four representative functions are shown: encryption, key exchange, digital signature and computation over encrypted data in a storage system. In current infrastructures, public key cryptography is used for issuing digital signatures as well as for key exchange between any two cryptographic parties, constructing the current key exchange infrastructure, namely, public key infrastructure (PKI). Encryption is then carried out by symmetric key cryptography with the seed key which has been exchanged in the PKI. This is because symmetric key cryptography can operate faster than public key cryptography. Computation over encrypted data is becoming an important task in cloud computing. Some public key crypto-schemes allow the computation of some operations on cipher texts (e.g., additions, multiplications, quadratic functions, etc.), and are referred to as homomorphic encryption. A crypto-scheme that supports arbitrary computation on cipher texts is known as fully homomorphic encryption. Lattice-based public key cryptography enjoys this feature. This crypto-scheme is also a representative example of post-quantum public key cryptography, which can be expected to resist quantum computer attacks. Security agencies and organisations recommend a transition from public key cryptography to post-quantum one. In this diagram, QKD is placed in the lower-left corner because it realises key exchange and encryption with a lower key rate. Physical layer cryptography [25–28] is another scheme for key exchange and encryption, and realises higher speed and longer distance, under some bounded assumptions on Eve's capability to access the channel.

QKD network can also realise key exchange infrastructure. It is, however, totally different in nature from the PKI. The former is based on one-to-one protocol, while the latter realises one-to-many and many-to-one protocols and allows key exchange between any nodes in the Internet. So QKD network is NOT what should be
replaced with the PKI. QKD network is something for very specific high-end applications which really need information theoretic security, and which can never be achieved by other crypto-techniques. In the next section, we discuss one possible killer application of QKD.

3. Long-term integrity and confidentiality protection system

Information theoretic security ensured by QKD itself is for data transmission, not for data storage. However, prime targets of malicious attacks are more likely data at rest (storage) rather than data in transit. Sensitive data relevant to human genome and health, which are stored in data centres require protection throughout their lifetime or even longer, like a century timescale [29]. Digital archives are also increasing, which are less sensitive but deserve everlasting storage, being kept unaltered. Although post-quantum public key cryptography can be expected to resist quantum computer attacks, there is no clue for the very long-term resistance. The requirements for long-term secure data storage system are summarised in Table 1.

There have been partial solutions for these requirements. Secret sharing scheme satisfies confidentiality of storage, availability and functionality. In secret sharing, new multiple data (shares) are created from the original data by using a polynomial, and stored in multiple data servers (shareholders). Shamir’s \((k, n)\)-threshold scheme uses \(n\) shareholders, and restore the original data by collecting at least \(k (\leq n)\) of shares. With shares of \(k-1\) or less, the original data can never be reconstructed even with unlimited computing power. Provided that the number of corrupted shareholders is less than \(k\), and shares are exchanged through private channels, Shamir’s \((k, n)\)-threshold scheme ensures information theoretic confidentiality (i) for storage. Shares can be added and multiplied, so (iv) can be met. Even if shares up to \(n-k\) are lost, the original data can be reconstructed by using the \(k\) remaining shares, which provides availability (iii).

Secret sharing itself, however, cannot protect integrity (ii). Private channels should also be implemented somehow to protect confidentiality of data transmission, which is another important requirement in (i). These problems are solved by introducing QKD for ensuring confidentiality of data link, and also employing signature and authentication schemes for protecting integrity for a long term. All these technologies are combined on a

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Meaning</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>(i) Confidentiality</td>
<td>The data should be accessible only to authorised parties.</td>
<td>No computational but information theoretically secure encryption should be used.</td>
</tr>
<tr>
<td>(ii) Integrity</td>
<td>The data should remain unaltered.</td>
<td>Signature and authentication schemes should be employed.</td>
</tr>
<tr>
<td>(iii) Availability</td>
<td>The data should be available whenever required.</td>
<td>Redundant data backup and fail safe mechanism are needed.</td>
</tr>
<tr>
<td>(iv) Functionality</td>
<td>The data can be processed without decryption.</td>
<td>Full homomorphic encryption is desired.</td>
</tr>
</tbody>
</table>
network as the long-term integrity and confidentiality protection system, which is actually implemented in the Tokyo QKD network as shown in figure 2 [30, 31].

As for the integrity protection, it is sufficient to ensure short-term security for a certain period. In fact, commitments and timestamp chains can be used to prolong the validity of digital signatures for the original data for any length of time, being renewed on a regular basis [31, 32]. As for confidentiality of data link, private channels connecting the shareholders are realised by OTP encryption of shares using the keys from the QKD network [30, 31].

To complete the long-term integrity and confidentiality protection system, proactive share renewal mechanism [33, 34] must be further implemented because it is likely that the number of corrupted shareholders must increase as time elapses. This share renewal requires a lot of keys for OTP encryption. Current key generation rate of QKD actually limits data size to be handled. With the state-of-the-art QKD key rate (1 Mb s\(^{-1}\) over a standard fibre of 50 km), and for a typical share renewal time of 2 years, the data size would be a few Tera bytes, which corresponds to the size of human genome of a few thousands of persons. This size is not enough for practical applications. For dealing with realistic data size for one data centre, which is something like Peta byte at least, corresponding to the size of human genomes of million persons, the key generation rate should be a 1 Gb s\(^{-1}\) scale. Thus, to realise a killer application of QKD in data storage, the key generation rate needs to be much improved.

To increase the key generation rate, one should increase the repetition rate of photon detectors, multiplex quantum channels, and employ fast key distillation. Quantum channel multiplexing and fast key distillation will be straightforward by using integrated photonic technologies [35] and dedicated key distillation engines on semiconductor chips, respectively. On the other hand, increasing the repetition rate of photon detectors is not easy. A plausible approach at the moment is to apply a multi-pixel-array photon detector to each quantum channel so as to compensate the dead time at each pixel effectively for a faster count rate. It is expected that such a detector with low noise will be available at a low cost in the near future because a lot of efforts are paid on it, driven by a promising market of LIDAR technology for automotive cars.

4. Quantum networks in space

4.1. Emerging mobile communications network

Most quantum networks so far have assumed wired channels (optical fibres) and nodes at fixed locations. On the other hand, the recent progress of mobile terminals such as automotive cars, drones and satellites is remarkable and encourages the exploration of a new frontier of research on quantum wireless network.

The availability of small-size and low-cost satellites as well as low-cost launches, has led to a rapid growth in satellite constellation programmes for remote sensing and communications. New unmanned aerial vehicles (UAVs) that can continue to fly in the stratosphere for many years using solar power supply, will enable high altitude platforms (HAPs) for sensing and communications. Data-intensive sensors mounted in these mobile terminals produce a large size of data for a short time. It is becoming hard to transmit these data only by RF bands because they are already congested. Free space optical (FSO) communications are expected to realise
high-throughput data links for this purpose. Figure 3 depicts a perspective view of such a network. FSO communications can be used in satellite constellation, HAPs, satellite-ground data link and ad-hoc data link between small UAVs (drones). Drones promise to provide cost-effective, on-demand connectivity with flexible and dynamical networking, constituting low altitude platforms, thanks to their mobility, such as moving any directions and staying stationary in the air.

FSO communications can also be used for key exchange for secure communications if physical random number generators and key distillation processing are additionally implemented in the FSO system. Key exchange tasks using QKD or physical layer cryptography can be executed in a certain interval between data link missions. QKD in space is expected to cover a global scale that was not possible by fibre networks on earth. Physical layer cryptography can also be a natural option, because line-of-sight condition for FSO communications validates the assumption that Eve’s capability to access the main channel is physically bounded, and also because it realises long distance and high-rate key exchange. Information theoretic security ensured by these technologies has a significant meaning for protecting critical information in emerging mobile communications network.

4.2. QKD and physical layer cryptography

Pioneering free space QKD experiments in practical environment were done in [36, 37]. Since then, there have been significant efforts, and free space QKD and quantum teleportation over a long distance of 144 km were demonstrated [38, 39]. Recently, free space QKD experiments were extended to airborne-to-ground [40], and a moving platform consisting of a vibrating turntable and a balloon [41]. In these works, the receiver was located at a fixed place, simulating a downlink from satellite to ground. Recently, QKD experiments with a moving receiver were demonstrated, namely with a moving truck [42] and an airborne [43], demonstrating the viability of an uplink QKD satellite mission, which allows for source flexibility as well as relaxed requirements on processing and storage. These achievements have demonstrated the readiness of quantum technology and the supporting classical technology (optical tracking and acquisition, compact implementation for limited payload etc) for deployment of QKD in mobile platforms such as HAPs and drone networks. In particular, UAVs and drones can get close to each other to establish a QKD link over a shorter distance, and then move apart after key exchange mission is completed. Free space QKD will find a new field in mobile communications network.

Improving the performance of free space QKD is an ongoing challenge. On the other hand, physical layer cryptography is also attractive in this direction because it is suitable to wireless communications especially in the line-of-sight links, and can realise higher speed and longer distance [44, 45]. In physical layer cryptography, one allows some compromised but realistic assumptions on Eve’s ability to access the channel, often referred to as the wiretap channel. The channel from Alice to Bob is called the main channel. Physical layer cryptography includes two kinds of schemes: (1) secrecy message transmission [25, 26] and (2) secret key agreement [27, 28]. Secrecy message transmission does not require crypto-key, but just employs channel coding design based on channel characteristics of the main channel to Bob and the wiretap channel to Eve. Secret key agreement uses not
only the main channel but also the public channel for key distillation. QKD can be regarded as an extreme example of secret key agreement in the sense that Eve’s ability is not bounded.

In figure 4, estimated rates of QKD and physical layer cryptography as well as a rate of optical communication are plotted as a function of channel transmittance to Bob, \( \eta_y \), in dB. The one-dotted line represents a performance for decoyed BB84 QKD with currently available devices. The key rate rapidly falls down at a distance corresponding to \(-40 \text{ dB}\) channel transmittance, which is roughly the best link budget for a low-earth-orbit-to-ground link including beam divergence, atmospheric loss, and system loss. To extend the distance further while keeping the unconditional security, one should rely on quantum repeaters by implementing non-classical light sources and quantum memories in UAVs at intermediate nodes as well as realising highly efficient optical coupling. Along with progress of UAV’s mobility, quantum mobile repeater network will be an exciting challenge.

The solid line represents an achievable rate of optical communication based on on-off keying, assuming 10 W laser, a pulse generation rate of 1 GHz, and a dark count rate of 100 cps.

Figure 4. Comparison of rates of QKD, physical layer cryptography and optical communication as a function of channel transmittance to Bob, \( \eta_y \), in dB. All three schemes assume an optical wavelength centred at 1550 nm and a pulse generation rate of 1 GHz. As for QKD, we assume a decoyed BB84 QKD system with a total dark count rate of 100 cps. Physical layer cryptography employs pulse position modulation (PPM) coding based on an on-off keying scheme. Both Bob and Eve employ on-off detectors, whose dark count rates are \( \lambda_y = 1000 \text{ cps} \) and \( \lambda_z = 1 \text{ cps} \), respectively. The dashed and dotted lines represent secrecy rates for Eve’s tapping ratio \( \eta_z / \eta_y = 0.95 \) and 0.999, respectively. This ratio is equivalent to that of Eve’s signal power/Bob’s signal power. The solid line represents an achievable rate of optical communication based on on-off keying, assuming 10 W laser, a pulse generation rate of 1 GHz, and a dark count rate of 100 cps.

5. Summary and future dreams

We discussed how quantum network can be combined with modern cryptographic technologies in fibre network and with emerging mobile terminals in wireless network, creating new solutions for the future cryptographic and communication systems. Our discussions can be summarised in the roadmap shown in figure 5.

The state-of-the-art QKD system can realise a key generation rate of about 1 Mbps over a 50 km fibre, realising metropolitan QKD network. The key generation rate decreases exponentially, resulting in about 10 kbps at 100 km, which corresponds to the performance of intercity QKD network. In next decade, we would like to expect that 1 Gbps QKD link will be available over a metropolitan scale, satellite QKD link will generate a
key at 1 kbps, and mobile QKD with UAVs will realise 100 kbps key generation. The technology of 1 Gbps QKD link leads us to a long-term secure storage network combined with secret sharing scheme and modern cryptography, which will be of practical use for protecting critical data around 2030. In this era, satellite constellation and UAV networks will be of practical use. To ensure information theoretically secure communication with a throughput higher than 100 Mbps, physical layer cryptography will be promising. Nation-wide QKD network with 10 Mbps throughput will also be available. Quantum repeater, whose rate is about 1 kbps, will probably find its practical application to ultra-high resolution telescope, namely longer-baseline telescopes using quantum repeaters [46]. In 2035 or later, quantum repeater technology will be applicable to cryptographic application at a rate something around 10 kbps. Building fully quantum networks itself, especially connecting different kinds of quantum systems via photons for quantum repeater, should deserve for the pursuit in its own right, and should create new science and unforeseen applications. The ultimate goals in a few decades is to realise quantum safe infrastructure in fibre and wireless networks, in which post-quantum cryptography, QKD and physical layer cryptography will be integrated.

Acknowledgements

The author thanks M Fujiwara, M Takeoka, K Yoshino, A Tajima, A Tomita, K Tamaki, J Braun, J Buchmann, D Demirel, M Geihs, S Moriai, A Waseda and W Ogata for their collaborations. This work was supported in part by the ImPACT Programme of the Cabinet Office, Japan.

References

[21] Togan E et al 2010 Quantum entanglement between an optical photon and a solid-state spin qubit Nature 466 730–4
[22] Hensen B et al 2015 Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres Nature 526 682–6
[27] Maurer U M 1992 Conditionally-perfect secrecy and a provably-secure randomized cipher J. Cryptol. 5 53–66
[38] Schmitt-Manderbach T et al 2007 Experimental demonstration of free-space decoy-state quantum key distribution over 144 km Phys. Rev. Lett. 98 010504
[40] Nauerth S et al 2013 Air-to-ground quantum communication Nature Photon. 7 382–6