Quantum Key Distribution as a Service

Joo Yeon Cho, Thomas Szyrkowiec, and Helmut Griesser

ADVA Optical Networking SE, Germany
{JCho, TSzyrkowiec, HGriesser}@advaoptical.com

Quantum Key Distribution (QKD) is a method for secure key establishment based on fundamental laws of quantum physics. QKD is already a matured technology which can be adopted to real-life applications. Field tests of QKD technology have been done over long distances of the order of 100km, e.g. [7, 3]. Commercial QKD systems are currently available in the market.

Nevertheless, QKD has not been widely deployed as practical security technology, mainly due to the expensive hardware and the requirement for a dedicated optical link. Multi-user QKD networks have been extensively investigated to provide cost-effective QKD systems. In [4], an upstream quantum access network is proposed to allow multiple end-users to share the most expensive component, i.e. the single photon detector of a network node. In [7, 5], a key management server is introduced to act as a trusted authority and provide secure keys to users. The integration of QKD systems into commercial telecommunication networks has been demonstrated in [8, 2], thereby removing the constraint of a dedicated QKD link using a dark fiber.

In this paper, we propose to provide QKD as a service (QaaS) without any dedicated hardware requirements for users. A user reserves a pair of QKD servers in the cloud, let these QKD servers perform a QKD protocol, and receives a generated secret key from the QKD server in a secure way. The proposed system model with 3-node is shown in Fig. 1a.

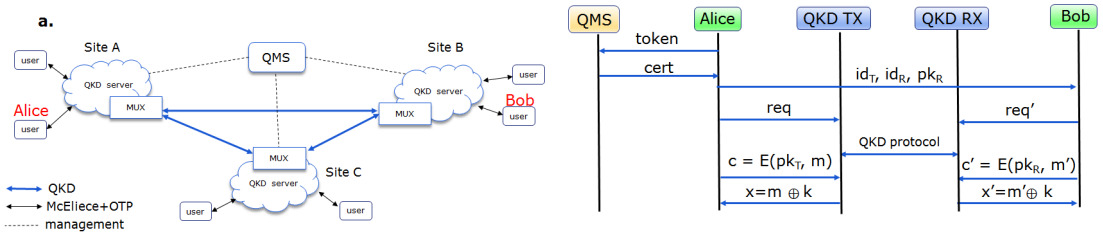

Fig. 1. a. A system model for QKD as a service. QMS stands for QKD Management Server. **b**. A key agreement protocol.

Imagine that Site A, B and C in Fig. 1a are three military base camps which are remotely located. A QKD server is installed at each camp and all QKD servers are inter-connected through optical fibers or an optical free-space link. Any pair of QKD servers can perform a QKD protocol such as the BB84 protocol [1]. Since each base camp is regarded as a safe zone, an internal user is allowed to connect a local QKD server through a conventional channel. Hence, Alice and Bob in Fig. 1a let their local QKD servers perform a QKD protocol and import a freshly generated secret key from their local QKD servers through a conventional channel.

A main challenge of QaaS is to design a secure key agreement protocol between two users via QMS and two QKD servers. We propose a quantum-safe key agreement protocol based

on the McEliece cryptosystem for this task. A similar challenge was introduced in the Tokyo QKD Network [7] but no hints were given on how QKD keys could be securely supplied to applications such as a secure mobile phone.

McEliece Cryptosystem The McEliece cryptosystem is a public key cryptosystem based on error correcting codes, first presented in 1978 [6]. It remains unbroken since proposed, including attacks using quantum computers.

A private key consists of a generator matrix $\mathbf{G}$, an invertible binary matrix $\mathbf{S}$ and a random permutation matrix $\mathbf{P}$. The matrix $\hat{\mathbf{G}} = \mathbf{S} \cdot \mathbf{G} \cdot \mathbf{P}$ and the error correcting capability t forms the public key. A message m is multiplied by the public key to produce a codeword and t random errors are added to the codeword to produce a ciphertext. Without knowledge of the specific code used, the errors cannot be corrected and therefore the original message cannot be recovered. Since S is invertible, the legitimate receiver can reverse the transformations of G, correct the errors by using the decoding algorithm, and recover the original message.

Key Agreement Protocol Assume that Alice and Bob perform a key agreement protocol. The proposed protocol is shown in Fig. 1b.

1. **Alice** $\rightarrow$ **QMS** Alice sends a request to reserve a pair of QKD servers to QMS with the following information;

$$token = \{id_{Alice}, period, source, destination\}$$

   where *source* is a sender address and *destination* is a receiver address.

2. **QMS** $\rightarrow$ **Alice** QMS assigns a pair of QKD servers to Alice and sends back to Alice the following information:

$$cert = \{(id_T, id_R), (pk_T, pk_R), timestamp, sign_{QMS}\}$$

   where pk_T and pk_R are the public keys of the QKD transmitter and the QKD receiver, respectively. Note that id_T and id_R can be the IP addresses of QKD servers.

3. **Alice** $\rightarrow$ **QKD transmitter** Alice generates a random number m that is of the same length as the key k, encrypts it and sends it to the QKD transmitter

$$req = \{id_T, id_R, E(pk_T, m)\}$$

   Note that $E(pk, m)$ is a McEliece encryption function where pk is a public key and m is a message.

4. **Alice** $\rightarrow$ **Bob** Alice sends id_T, id_R and pk_R to Bob.

5. **Bob** $\rightarrow$ **QKD receiver** Bob generates a random number m' that is of the same length as the key k, encrypts it and sends it to the QKD receiver

$$req' = \{id_T, id_R, E(pk_R, m')\}$$

6. **QKD transmitter** $\rightarrow$ **Alice** The QKD transmitter performs a QKD protocol with the QKD receiver and generates a secret key k.
   The QKD transmitter computes $D(sk_T, E(pk_T, m)) = m$ and sends $x = k \oplus m$ to Alice. Note that $D(sk, c)$ is a McEliece decryption function where sk is a private key and c is a ciphertext.

7. **QKD receiver → Bob** The QKD receiver computes $D(sk_R, E(pk_R, m')) = m'$ and send $x' = k \oplus m'$ to Bob.
8. **Alice and Bob** Alice recovers $k = x \oplus m$ and Bob recovers $k = x' \oplus m'$.

The security of the proposed key agreement protocol is based on that of QKD, the McEliece cryptosystem and the OTP encryption. All of them are quantum-safe. Also, in the QaaS model, multiple users can perform the proposed protocol in parallel because multiple QKD signals can be multiplexed and transmitted through a single optical channel. This reduces the hardware cost significantly on the user side.

The proposed model can be seen as an alternative to the cloud key management service (KMS), which is currently available in the internet, e.g. Google cloud KMS, Amazon AWS KMS, and Microsoft Azure key vault. In cloud KMS, users can manage their key life cycle such as a key generation, usage, rotation and destruction in the cloud platform. However, there exists a risk that keys might be leaked by unknown attacks or human mistakes.

In the QaaS model, quantum bits cannot be recorded or cloned due to the laws of physics. QKD servers also never store secret keys that are generated by the QKD protocol. Hence the risk of a key leakage is significantly reduced.

References

1. C. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossin*, (1984), 175–179.
2. A. Ciurana, J. Martínez-Mateo, M. Peev, A. Poppe, N. Walenta, H. Zbinden, and V. Martín, *Quantum metropolitan optical network based on wavelength division multiplexing*, Opt. Express **22** (2014), no. 2, 1576–1593.
3. A. Dixon and et al., *77 day field trial of high speed quantum key distribution with implementation security*, `https://obj.umiacs.umd.edu/extended_abstracts/QCrypt_2016_paper_18.pdf` accessed on 06-04-2017, 2016.
4. B. Fröhlich and et al., *A quantum access network*, Nature **501** (2013), 69–72.
5. R. Hughes and et al., *Network-centric quantum communications with application to critical infrastructure protection*, `http://lanl.arXiv.org/abs/1305.0305` accessed on 06-04-2017, 2013.
6. R. J. McEliece, *A public-key cryptosystem based on algebraic coding theory*, Deep Space Network Progress Report, vol. 44, January 1978, pp. 114–116.
7. M. Sasaki and et al., *Field test of quantum key distribution in the tokyo qkd network*, Opt. Express **19** (2011), no. 11, 10387–10409.
8. K. Yoshino, T. Ochi, M. Fujiwara, M. Sasaki, and A. Tajima, *Maintenance-free operation of wdm quantum key distribution system through a field fiber over 30 days*, Opt. Express **21** (2013), no. 25, 31395–31401.