Toward a security certificated communication systems

Akihisa Tomita
Graduate School of Information Science and Technology, Hokkaido University,
Sapporo, 060-0814, Japan

1 Introduction

This tutorial will consider the construction of a security-certificated communication system based on quantum key distribution (QKD.) The introduction will present reasons to use QKD to keep the high-level secret for a long time. Then, the notion of the secure key distribution will be introduced. The main part of the talk is devoted to security certification on a practical QKD system. Finally, if time allows, a prospect for a secure communication network based on the secret key provided by QKD will be given.

Fiber communication has been thought to be secure, because electromagnetic wave is much more confined than in copper cables. Recently, leaked photons from fiber bents can be detected by a high-sensitive photon detector [1]. This fact implies the vulnerability of the optical fiber communication, and necessity of data encryption. Modern cryptographic technologies have been developed and widely applied, which is based on the computational complexity, or hardness to crack the encrypted data.

The modern cryptography, however, may not be secure enough to transmit highly security-concerning information, such as diplomatic and military messages for governments, and genetic information for individuals. Those data should be protected against the highest available computing power for a long time, say, 60-100 years (that is, life-span of the message or human.) This property is called forward secrecy (FS,) which ensures that encrypted messages will not be decrypted many years after being duplicated and recorded. Key exchange protocols based on a public-key algorithm such as RSA don't pose FS, so that all the encrypted messages can be read once the secret key used in the key exchange protocol is known. Actually, secrecy of the secret key is not perfect; it can be leaked by improper implementation, or simply from a hard-disk of a scrapped server. Even a key exchange protocol with FS may be compromised. The protocol should be updated to keep up with the progress of decipher technology. The obsolete algorithms are often left usable for the sake of compatibility. The modern public key cryptsystems have thus weakness in practice, besides the intrinsic issue that they rely on an unproven computational assumptions.

Quantum key distribution (QKD) is an protocol that enables remote parties to share common random numbers (key) through a quantum communication channel that may be under full control of eavesdroppers. The information theoretical security ensures that the protocol remains secure, regardless of technological progress. No updating nor legacy-algorithm problems will appear.

2 Security notion of QKD [2]

QKD offers the universal composerability (UC) [3]; when QKD is used as a part of a cryptsystem, security of QKD will be unaffected, if other parts of the system are compromised. The UC property is desirable for secure cryptsystems. It is shown to be identical to the indistinguishable encryptions under adoptive chosen cipher text attack (IND-CCA2) for public key crypt-algorithms. IND-CCA2 is the strongest notion in the modern cryptography, and only a few algorithms are proven to be IND-CCA2. QKD provides the strongest security in terms of the security notion of the modern cryptography.

The UC security of QKD is described as follows: QKD under the adversary with unbounded (only limited by the laws of physics) power is indistinguishable with the ideal proto-

col where the adversary is separated and gains no information on the key. Formally, a QKD protocol is ε-secure, if the total density operator ρ_{AE}, which represents the state of the legitimate user (Alice) and the eavesdropper (Eve) after the protocol, satisfies

$$\|\rho_{AE} - \rho_A^{\text{ideal}} \otimes \rho_E\| \leq \varepsilon. \quad (1)$$

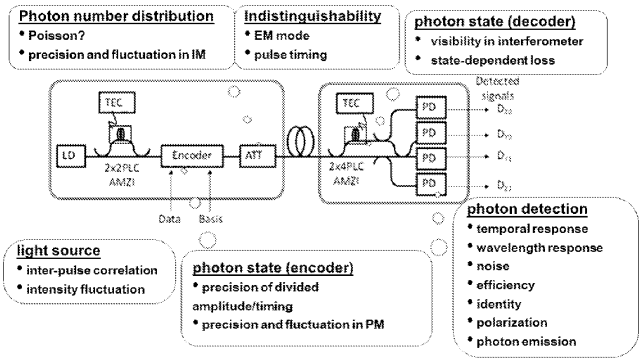
The ideal state $\rho_A^{\text{ideal}} \otimes \rho_E$ gives Eve no information on Alice's final state. Since no physical process increases trace norm distance $\|\cdots\|$, the distinguishability will never improved, which implies UC. The inequality (1) has been proven for QKD protocols [4], where ε is bounded by the phase error rate estimated from transmission and error rate in quantum communication. Currently, the most studied protocol is decoy BB84, where the quantum communication encoded with two bases as in original BB84 protocol is performed with different light intensities (mean photon numbers.) Security of decoy BB84 protocol is established even for finite-length code [5].

3 Security certification

The QKD equipment in practice, however, contains some imperfections, which may prevent us from direct application of the security proof. We treat the imperfections with the following procedure: (i) listing the assumptions behind the security proof, (ii) evaluating the imperfections; measurement of the deviation from the assumptions and estimation of the increase of the sacrifice bits due to the deviation, (iii) improving the equipment and the theoretical model and/or security proof.

The assumptions behind the security proof can be classified into three categories. The first one is random choice. Key values, bases, test bits, decoy pulse position, and hash functions should be chosen randomly. The choice should be unpredictable and unmeasurable for Eve. Otherwise, she can simply guess or measure the key. The second one is the countermeasure to the side-channel to restrict the attacks only on the quantum communication channel. It is necessary to harness the quantum mechanical properties for limiting Eve's information gain. We should consider the attacks to control quantum devices by applying signals beyond the specifications. The final one is the assumptions on the security theory, which vary for theories. For example, Koashi [4] assumes (a) identical detection efficiency for different basis, (b) known photon number distribution from the transmitter, (c) no phase correlation between pulses.

In the evaluation, we should built a realistic model of the equipment, and relate the assumptions to the device characteristics to be measured quantitatively, as depicted in the figure.



Current researches are quantifying the imperfections of the devices and their impacts, while improving the system performance. The QKD-based secure communication systems will stem on the security certification, the stable and easy operation, and the efficient key management. These three items are indispensable, and current studies develop steadily to fulfill the requirements for deployment.

References

[1] M. Fujiwara, *et al.*. *Opt Express*, 18(21): 22199–22207, 2010.

[2] See review by V. Scarani,*et al.*, *Rev. Mod. Phys.*, 81: 1301, 2009.

[3] M. Ben-Or,*et al.*, The universal composable security of quantum key distribution. In*Theory of Cryptography* Springer Berlin Heidelberg, 2005. pp. 386-406.

[4] M. Koashi. *New J. Phys.* , 11: 045018, 2009.

[5] M. Hayashi. *Phys. Rev. A* 76: 012329, 2007. erratum *ibid* 79: 019901, 2009.