Quantum Key Distribution in the Real World

Hokkaido Univ., ○Akihisa Tomita

E-mail: tomita@ist.hokudai.ac.jp

Continuing efforts have been made to develop practical quantum key distribution (QKD) systems on the installed fiber networks since early 2000s [1]. Recently, several groups have demonstrated high-speed QKD systems [2,3] with GHz-clock frequency working stably on the installed-fiber networks [4-7]. Along with the hardware development, an efficient key management protocol [7] has been implemented to construct a QKD platform to supply information-theoretically secure key for multiple applications. The highly available QKD platform is expected to promote social deployment of the QKD technology.

Nevertheless, there remains an obstacle that makes the potential users hesitate to accept this emerging technology; they won't innovate their secure communication systems unless convinced that a QKD system at hand is really secure. The deployment of QKD technology therefore requires security certification, test-and-measurement method, and security criteria, acceptable for non-experts. To this end, we re-examine the assumptions of security analysis to extract potential loopholes and develop evaluation methods with devices available in common laboratories. We also improve the protocol to make it immune to the newly discovered imperfection.

In this talk, we present the current QKD technology. We consider possible imperfection in the devices and their effects. Based on the consideration, we define test items, characterization and criteria for an implementation of Bennett & Brassard 1984 protocol with decoy method. This protocol is the oldest, but the security theory has been well established.

We will focus on the transmitter in this talk, because the quality of the transmitted photon states is crucial to security certification, and all the receiver imperfections can be circumvented in principle [8]. We have investigated items of phase correlation between pulses and intensity fluctuation in a gain-switched semiconductor laser, and fluctuations in the intensity modulators. We will present characterization method and results, as well as the improvement in the system design to satisfy the criteria.

References

1. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
2. J. F. Dynes, *et al*., Opt. Ex. **20**, 16339 (2012).
3. K. Yoshino, *et al*., Opt. Ex. **21**, 31395 (2013).
4. C. Elliott, *et al*., arXiv:quant-ph/0503058v2.
5. D. Stucki, *et al*., New J. Phys. **13**, 123001, (2011).
6. M. Peev, *et al*., New J. Phys. **11**, 075001 (2009).
7. M. Sasaki, *et al*., Opt. Express, **19**, 10387 (2011).
8. H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).