Security of quantum key distribution with non-I.I.D. light sources

Yuichi Nagamatsu*,[1] Akihiro Mizutani,[1] Rikizo Ikuta,[1] Takashi Yamamoto,[1] Nobuyuki Imoto,[1] and Kiyoshi Tamaki[2]

[1] *Graduate School of Engineering Science, Osaka University, Toyonaka, Osaka 560-8531, Japan*
[2] *NTT Basic Research Laboratories, NTT Corporation, 3-1, Morinosato-Wakamiya Atsugi-Shi, 243-0198, Japan*
* *nagamatsu@qi.mp.es.osaka-u.ac.jp*

Introduction – Quantum key distribution (QKD) enables two distant parties to share a secret key. Although QKD is secure [1], there is a gap between theory and practice. In fact, real-life QKD may *not* be secure because component devices in QKD systems may deviate from the theoretical models assumed in security proofs. To solve this problem, it is necessary to construct the security proof under as realistic assumptions as possible on the source and the measurement unit. Here, we prove the security of QKD under realistic assumptions on the source. Importantly, the validity of our assumptions can be verified in the experiments, and therefore, our proof is an important step to guarantee the practical security of QKD. Before describing our main results, let us review the related works. According to [2], the key rate decreases rapidly with the slight state preparation flaws and with the increase of the channel losses. The problem was solved by the loss-tolerant protocol [3, 4], and as a result, the key rate is almost independent of the flaw. The requirements in [3, 4] are that the distribution of the sending states is independently and identically distributed (I.I.D.) and the distribution is exactly known. In practice, however, due to imperfections of experimental devices, the requirements are not always fulfilled.

Main results – Here, we generalize the idea of [3] to prove the security of QKD under the assumption that each of the three sending single-photon states is a mixture of pure states within a certain range (R_1, R_2, R_3, respectively) on the Bloch sphere except with a small probability ε. (FIG. 1 (a)). As long as this assumption holds, it does not matter at all how the actual states distribute within each of the range nor whether their distributions are I.I.D. or not. We also assume that the laser pulses are perfectly phase-randomized, and the mode of the pulse is independent of the choice of the sending states. Based on our security analysis, we show the resulting key generation rate (FIG. 2) for the special case where the phase modulator is the main source of the state preparation flaw and the widths of R_1, R_2, R_3 are $\pm\theta$, and the phase distributions are the Gaussian distribution ($\varepsilon = 10^{-10}$) (see FIG. 1. (b)). In this simulation, we employ the phase encoding scheme and the asymptotic decoy state method [5]. Also, we assume the fiber-based QKD system with a channel transmittance 0.2 [dB/km], the total transmittance of the measurement unit is 0.15, the dark count rate is 5×10^{-7}, and the efficiency of the error correcting code is 1.22. FIG. 2 indicates the feasibility of QKD over long distances with practical sources.

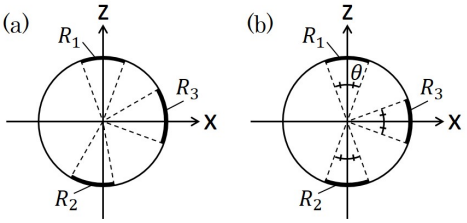

FIG. 1: (a)Three prepared states are mixture of pure states within R_1, R_2, R_3 on the Bloch sphere, respectively. (b)The special case of (a) for the simulation, where the widths of R_1, R_2 and R_3 are same ($\pm\theta$) and the centers are $0°, 180°, 90°$.

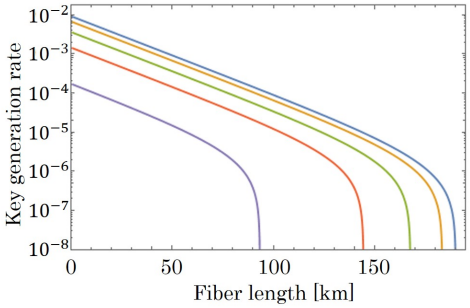

FIG. 2: Secret key generation rate (per pulse) vs fiber length for FIG. 1 (b) with $\theta = 0°, 1°, 3°, 5°, 7°$ (from right to left).

Conclusion – We proved the security of a QKD protocol with non-I.I.D. light sources. Importantly, the validity of our assumptions can be verified in the experiments. Our work is an important step to construct a truly secure QKD with realistic devices.

Acknowledgment – YN acknowledges support from the JSPS Grant-in-Aid for Scientific Research(A) 25247068 and (B) 15H03704. KT acknowledges support from the National Institute of Information and Communications Technology (NICT) and the ImPACT program.

[1] P. W. Shor *et al.*, Phys. Rev. Lett. **85**, 441 (2000).
[2] D. Gottesman *et al.*, Quantum Inf. Compt. **5**, 325 (2004).
[3] K. Tamaki *et al.*, Phys. Rev. A **90**, 052314 (2014).
[4] A. Mizutani *et al.*, arXiv:1504.0815.
[5] H.-K. Lo *et al.*, Phys. Rev. Lett. **94**, 230504 (2005).