Key rate enhancement using qutrit states for uncharacterized quantum key distribution

Yonggi Jo[1] and Wonmin Son[1,2]

[1] *Department of Physics, Sogang University, 35, Baekbeom-ro, Mapo-gu, Seoul 04107, Republic of Korea*
[2] *Department of Physics, University of Oxford, Parks Road, Oxford OX13PU, United Kingdom*

Quantum cryptography is a matured application of quantum informational theory that exploits quantum mechanical principle. At the very core of the protocol, there is a procedure called quantum key distribution (QKD) [1], generating a secure key between two distant parties, Alice and Bob, under a potential attack by a malicious eavesdropper called Eve. So far, there have been many research works to prove the security of QKD, based upon the quantum mechanical principles [2, 3].

It is notable that the early proposal of the QKD protocols uses a two-dimensional quantum state, called qubit. Due to the extensible structure of Hilbert space, it is expected that the high dimensional quantum system can carry more information per single quanta, as compared with qubit. Until now, exploiting the high-dimensional quantum state was extensively discussed in various contexts. There are discussions about applying high-dimensional quantum states for QKD protocol as well. They are to prove the security of QKD using d-dimensional quantum system which is generalized version of the original QKD protocol [4, 5]. The results show that QKD using high-dimensional quantum states can achieve a higher upper bound of the error rate, which ensures a higher unconditional security of the channel in an ideal situation.

On the other hand, security of the practical QKD system has been scrutinized in detail. Many security proofs have been made under the assumptions that all devices are trusted or well characterized for perfect security. However, in a practical situation, it is necessary to consider the circumstance that untrusted devices are used, as they can be provided by malicious eavesdropper. In that circumstance, a manipulative side-channel attack against the detector is possible. In order to extend the notion of ultimate security, a device-independent QKD (DI-QKD) protocol was proposed in 2007 [6]. However, it has been turned out that DI-QKD is difficult to be implemented in practice, because it requires a high-quality entanglement source, low-loss communication channel, and highly efficient detectors. Compensating the practicality, measurement-device-independent QKD (MDI-QKD) protocol was proposed in 2012 [7]. In the MDI-QKD scheme, all types of possible side channel attack exploiting imperfection of detectors are overcome by separating detectors from Alice and Bob. For the separation, potentially untrusted third party, called Charlie, is introduced for their QKD. From the fact that Charlie only acts as a referee to build up the correlation between Alice and Bob, he cannot access to the encoded message as like eavesdropper and it guarantees the a posteriori unbounded security between Alice and Bob.

Thus, by using MDI-QKD, we can overcome most of side channel attacks when the major security issues are caused by the detector imperfection [8]. In the meanwhile, the practical MDI-QKD still suffers from its low key rate as compared to BB84 protocol. MDI-QKD needs the BSM setup that has only 50% success probability using linear optical elements [9]. Such a low success probability of BSM is the main cause of a low key generation rate in MDI-QKD.

In this work, we propose a MDI-QKD protocol using 3-dimensional quantum state (3d-MDI-QKD) that allows for an improvement of the secret key rate as compared to the original protocol with qubits. We analyze the security of 3d-MDI-QKD under the circumstance that the states are generated from imperfect communication sources, noted as uncharacterized sources assumption. We use the mismatched-basis statistics in security analysis for 3d-MDI-QKD with uncharacterized sources, as it was originally proposed for qubit MDI-QKD in [10]. Here, we show that there is an improvement of the security in 3d-MDI-QKD as compared with qubit MDI-QKD, even if the communication sources are uncharacterized. We evaluate the secret key rate of 3d-MDI-QKD with regard to different realistic experimental factors and identify the regime where 3d-MDI-QKD is more secure than qubit MDI-QKD.

The preprint of the paper may be found at [11].

[1] C. H. Bennett and G. Brassard, *in Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE Press, New York, 1984) p. 175.

[2] D. Deutsch, A. Ekert, R. Jozsa, C Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).

[3] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[4] N. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).

[5] T. Durt, D. Kaszlikowski, J. Chen, and L. Kwek, Phys. Rev. A **69**, 032313 (2004).

[6] A. Acín, N. Gisin, and L. Masanes, Phys. Rev. Lett. **97**,

120405 (2006).
[7] H. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[8] H. Lo, M. Curty, and K. Tamaki, Nat. Photonics **8**, 595 (2014).
[9] N. Lütkenhaus, J. Calsamiglia, and K.-A. Suominen, Phys. Rev. A **59**, 3295 (1999).
[10] Z. Yin, C. Fung, X. Ma, C. Zhang, H. Li, W. Chen, S. Wang, G. Guo, and Z. Han, Phys. Rev. A **90**, 052319 (2014).
[11] Y. Jo, and W. Son, arXiv:1606.07882 (2016).