SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

Advantage of the key relay protocol over secure network coding

Go Kato * Mikio Fujiwara † Toyohiro Tsurumaru ‡

Keywords: Key Relay Protocol, Secure Network Coding, Quantum Key Distribution ...

Extended Abstract

The key relay protocol (KRP) plays an important role in improving the performance and the security of quantum key distribution (QKD) networks [1, 2, 3, 4]. On the other hand, there exists another research field called secure network coding (SNC; see, e.g., Refs. [5, 6]), which has the goal and structure similar to the KRP. The goal of this talk is to analyze differences and similarities between the KRP and SNC rigorously.

QKD realizes distribution of secret keys to players at distant locations (see, e.g., Refs. [7]). However, the communication distance achievable by a single QKD link is limited by the technological level of quantum optics [7]. KRPs are used to enable key distribution beyond such limitation of a single QKD link. The basic idea of the KRP is to pass a secret key of one QKD link on to another QKD link with the help of insecure public channels, such as the internet.

The KRP has similarities and differences with SNC. While they share the same goal of sharing secret messages, they differ in that 1) Public channels are available in KRPs, but not in SNC schemes, 2) KRPs use QKD links (or more generally, local key sources) while SNC schemes use secret channels, and 3) The messages in KRPs must be a random bit, while in SNC schemes each sender can freely choose its message.

Then the question naturally arises whether these differences are really essential. For example, is it not possible that there is actually a way of converting KRPs to SNC schemes, and that they are shown to be equivalent? The goal of this talk is to answer to this question. For the sake of simplicity, we will limit ourselves to the one-shot scenario, and also to the scenario where wiretap sets are restricted [6].

The outline of our results is as follows[8]. If we generalize SNC [5, 6] by adding public channels, then KRPs and SNC schemes (with public channels) on the same graph become equivalent. However, if we do not generalize SNC and limit ourselves to its conventional form without public channels, then there is a definite gap in security between the KRP and SNC: On some graphs a KRP achieves the better security than any SNC schemes without public channels. Hence the accumulation of past research on the conventional SNC is not sufficient to explore the potential of KRPs. This suggests that the KRP is a new research field.

References

[1] L. Salvail et al. “Security of trusted repeater quantum key distribution networks, ” Journal of Computer Security, vol. 18, pp. 61–87, Jan 2010.

[2] R. Alleaume, et al. “ Using quantum key distribution for cryptographic purposes: A survey, ” Theoretical Computer Science, vol. 560, pp. 62–81, 2014.

[3] T. R. Beals and B. C. Sanders, “ Distributed relay protocol for probabilistic information-theoretic security in a randomly-compromised network, ” in Information Theoretic Security, R. Safavi-Naini, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 29–39.

[4] ITU-T, “ Overview on networks supporting quantum key distribution, ” International Telecommunication Union, Geneva, Recommendation Y.3800, Oct. 2019.

[5] N. Cai and R. Yeung, “ Secure network coding, ” in Proceedings IEEE International Symposium on Information Theory,, 2002, pp. 323–.

[6] T. Cui, T. Ho, and J. Kliewer, “On secure network coding with unequal link capacities and restricted wiretapping sets, ” in 2010 IEEE Information Theory Workshop, 2010, pp. 1–5.

[7] F. Xu, et al. “ Secure quantum key distribution with realistic devices, ”Rev. Mod. Phys., vol. 92, p. 025002, May 2020.

[8] Go Kato, Mikio Fujiwara, and Toyohiro Tsurumaru, “ Advantage of the key relay protocol over secure network coding ” arXiv:2111.13328

* NTT Communication Science Laboratories, 3-1 Morinosato-Wakamiya, Atsugi, Kanagawa, 243-0198, Japan
† NICT, Nukui-kita, Koganei, Tokyo 184-8795, Japan
‡ Mitsubishi Electric Corporation, Information Technology R&D Center, 5-1-1 Ofuna, Kamakura-shi, Kanagawa, 247-8501, Japan