Toward Quantum Photonic Network

Masahide Sasaki[1] *

[1]*National Institute of Information and Communications Technology,*

Abstract. We review current attempts on photonic network, quantum communication and quantum cryptography, and then discuss our challenge to merge them to make quantum photonic network. Our first challenge is to establish a new theory on physical layer cryptography, which can characterize the tradeoff between high capacity transmission and provably secure communication under the cost constraint.

Keywords: Quantum communication, quantum cryptography, secrecy capacity

Photonic network is an emerging infrastructure of optical communications. It specifically means a transparent network based on all optical processing nodes, instead of conventional nodes based on electrical processing. It is to utilize broadband of optical fields and to resolve the speed limit and heating of electrical devices, aiming at realizing power-efficient high-capacity communications network. This attempt should eventually reach quantum communications technology which controls and detect the signals at the quantum level, and will realize the maximum capacity for a given energy and bandwitdh resources.

Network security has been implemented so far by computer algorithms as software. Its security relies on computational complexity of mathematical problems, and hence cannot be provable. Moreover, insisting on this technology means to rely on electrical processing, contradicting the evolution of photonic network.

Quantum cryptography is a means to secure photonic network. It provides the provable security by quantum key distribution (QKD), which is unbreakable by any future technologies. However, its speed and distance are still limited, preventing a merger with photonic network. Actually, the extreme assumption that an eavesdropper can have unbounded ability, enables one to prove the unconditional security in a clear manner. It instead imposes the stringent conditions on the implementation, not only limiting the transmission rate and distance but also narrowing an operation margin.

While quantum cryptography in the present form can be an option for high-end applications, another kind of scheme not only with provable security but also with improved usability should be pursued, even by restricting the range of security assumptions into a compromised one. However, it is not trivial at all to find a balance point between the security and the usability. Rather, it turns out to be a harder problem of optimization for a variety of parameters.

Quantum photonic network is a prospective paradigm which would be realized by unifying photonic network technology, quantum communication and quantum cryptographic technologies. Its architecture should be based on a new theoretic framework which can design optimal tradeoff points between high capacity transmission and provable security, for required communication tasks.

In this paper, we first review current attempts on photonic network, quantum communication and quantum cryptography, and then discuss our challenge to merge them to make quantum photonic network. Our first challenge is to establish a new theory on physical layer cryptography, which can characterize the tradeoff between high capacity transmission and provably secure communication under the cost constraint [1].

The provable security is more or less based upon the analysis of physical properties of a communications channel. Given a channel model, security proof is made information theoretically by showing the existence of error correcting codes that can effectively establish the statistical independence between the legitimate users and the eavesdropper. The theoretical basis was laid by Wyner in 1975, as the wiretap channel.

Under the wiretap channel assumption that channel characteristics for an eavesdropper (Eve) is worse than that for the legitimate receiver (Bob), which can be a reasonable compromise on Eve, we study characterization of efficient and reliable communication to Bob, and security against Eve, simultaneously. More specifically we derive the upper bounds on the decoding error for Bob, $\epsilon_n^B \leq 2e^{-nF(R_B,R_E)}$, and the leaked information to Eve, $\delta_n^E \leq 2e^{-nH(R_E)}$, as a function of code length n, the transmission rate R_B and the randomness rate R_E under the cost constraint. The exponent $F(R_B, R_E)$ is known as the reliability function introduced by Galleger, specifying how rapid the decoding error decreases as code length n, and is extended to the secrecy capacity context in this work. The exponent $H(R_E)$ is introduced in this work may be referred to as the security function, which specifies how rapid the leaked information decreases as code length n.

These functions are the dual quantities, and can formulate the trade-off between the transmission rate for Bob and the security against Eve at the finite code length. Numerical results on these quantities will be presented.

References

[1] T.-S. Han, H. Endo, and M. Sasaki, Reliability and Security Functions of the Wiretap Channel under Cost Constraint arXiv:1307.0608 [cs.IT], 2013.

*psasaki@nict.go.jp