Toward high capacity and secure global quantum communication

Masahide Sasaki and Te Sun HAN
Quantum ICT Laboratory, Advanced ICT Research Institute
NICT
4-2-1, Nukuikita, Koganei-city, Tokyo 184-8795, Japan
psasaki@nict.go.jp and han@nict.go.jp

Hiroyuki Endo
Department of Applied Physics,
Waseda University,
Okubo 3-4-1, Shinjuku, Tokyo 169-8555, Japan,
h-endo-1212@ruri.waseda.jp,

Quantum info-communication technologies directly control the quantum mechanical properties of photons. Then one can go beyond the capabilities of conventional technologies. For example, quantum communication can achieve the ultimate channel capacity of optical link maximizing the rate in bits/s/Hz/photon. Quantum cryptography can ensure unbreakable secure communications even by any future technologies. These two have been studied separately so far. Recently, however, one has started to see a new merged scheme, where both efficient transmission and provable security can be realized simultaneously, reaching the secrecy capacity as the maximum rate in secure bits/s/Hz/photon. We present the latest results on this new scheme, especially on theory and implementation in space.

Keywords—Quantum communicastion, Quantum cryptography, Spase laser communication

I. INTRODUCTION

Deep space optical communications will potentially provide 10 to 100 times larger data links over present radio frequency (RF) communications, because optical communication systems have a wider bandwidth, a larger capacity, lower power consumption, more compact equipment, greater security against eavesdropping, and smaller interference, compared to RF communications [1]. One typical feature of space optical communications which most differs from RF communications is that the link is quantum limited. Received optical power is very limited, usually at the photon level. In addition, photon energy in the optical domain is much larger than that in the RF domain, surpassing the energy scale thermal and background noises in the communication systems. Therefore quantum mechanical effect, such as discrete nature of light, becomes essential. Space optical communications systems must be designed based on quantum communication theory.

In this paper we first discuss an issue of the channel capacity of optical communications system. We show the attainable limit of the channel capacity, and compare several practical schemes from the viewpoint of how they can get close to the channel capacity limit. We then discuss an issue on how to realize high capacity and secure links. We particularly concern physical layer cryptography which can ensure the provable security, that is, the security which cannot be broken by any powerful computing technologies. Physical layer cryptography is based on appropriate coding techniques designed by considering physical properties of the main channel between the sender and the receiver, and the wiretap channel to an eavesdropper.

Quantum cryptography or more specifically quantum key distribution (QKD) is a typical example of physical layer cryptography. Demonstrating QKD in Space is one of grand challenges in the field of quantum and optical communications. However, the final key rates are expected to be very poor for securing practical data links. One might naturally ask whether QKD is the best solution for securing optical links in Space. QKD assumes that an eavesdropper (Eve) can have unlimited physical abilities and computational power. Under this extreme assumption, the unconditional security is ensured in principle. However, this requirement is sometimes too much. In the case of space optical links in a line of sight between the sender (Alice) and the receiver (Bob), if Eve is in the channel, then she is easily visible. Alice and Bob can tell Eve is there. So what Eve should do is to hide from the legitimate users away from the channel, and try to collect scattered light to get information from Alice. Thus one may limit the ability of Eve. Then in such a degraded condition for Eve, Alice and Bob can realize a much higher transmission rate with the probable security. Theoretical predictions in this line are presented.

II. CHANNEL CAPACITIES OF SPACE OPTICAL CHANNELS

A. Channel capacity formula

The channel capacity in classical communication theory by Shannon is determined by the noise power of the system N and by the amount of available signal power P and bandwidth W as

$$C = W \log (1 + \eta P/N W) \tag{1}$$

where η is the channel transmittance. The extension of this formula to the quantum domain has been studied for many years, and today we know the following formula [2]

$$C_Q = \max_{N_k} \sum_k g(\eta_k N_k) \tag{2}$$

where $g(x)=(x+1)\log(x+1)-x \log x$ is the entropic function, and N_k is the average photon number for mode k, which is determined by the power constraint

$$W\sum_k hf_kN_k = P. \tag{3}$$

where h is the Plank constant and f_k is the frequency of mode k. This formula specifies the channel capacity of a linear loss optical channel under the power constraint, after the fully quantum mechanical optimization of encoding and decoding strategies are made. The physical scheme to attain this capacity is also known. The optimal encoding is given by the dense coherent modulation, which is completely conventional coherent communications technology. The optimal decoding, on the other hand, essentially requires utilizing quantum effects. Namely this should consists of quantum computing with coherent states to transform the received codeword state into an appropriate quantum state, and the final measurement on it afterward. This is referred to as quantum collective decoding, or simply quantum decoder [3, 4].

B. Numerical simulation of space optical communications

Figure 1 shows the channel capacities for various schemes for space optical communications in terms of transmission rates in Gbits/sec versus the transmission distance [5]. The line on the top entitled "All band quantum decoder" indicates the ultimate capacity of a lossy optical channel when quantum decoder can be implemented which can work on all bands of electromagnetic field modes. This ultimate capacity can be simply expressed as as

$$C = \frac{\pi}{\ln 2}\sqrt{\frac{2\eta P}{3h}}. \tag{4}$$

No one can go beyond this limit, no matter how much capacity one wants. Thus quantum theory tells us that, we will be able to extend a Tbps link to Mars from Earth if such an all band quantum decoder is available.

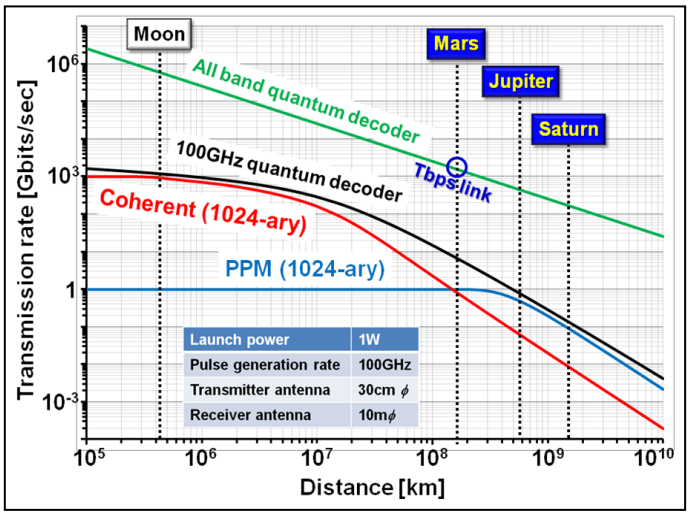

Fig. 1. The channel capacities for various schemes for space optical communications in terms of transmission rates in Gbits/sec versus the transmission distance.

The line on the next top titled "100GHz quantum decoder" represents the performance which will be attained if quantum decoder working on 100GHz bandwidth is available. This can be a reasonable reference for the upper bound of practically attainable performances with near future technologies. Two schemes are compared under this upper bound. One is 1024-ary coherent communication scheme based on homodyne detection. The other is pulse position modulation (PPM) scheme. Both schemes assume a 100GHz pulse generation rate. For shorter distances, such as up to Moon, coherent communication scheme realizes the performance close to the quantum bound of 100GHz bandwidth. On the other hand, for longer distances beyond Mars, PPM scheme achieves better performance approaching the quantum bound.

III. PHYSICAL LAYER CRYPTOGRAPH

In this section we discuss secure communications with the probable security. Let us first consider two extreme cases; the most secure communications, that is, QKD, and a high capacity space optical link where there is nothing to do with security. Bennett-Brassard 1984 (BB84) scheme using decoy states is known to be the currently most sophisticated and matured QKD scheme, which can ensure the unconditional security, in principle. Its performance is depicted in Fig. 2, entitled "Decoyed BB84". Here we assume that the pulse generation rate is 1GHz which corresponds to currently highest speed of fast QKD systems. The dark count probability is assumed to be 10^{-6} per pulse, that is, 1000 counts per sec, which is typical for the current detectors used in QKD systems. The final key rate is typically 100kbps at a distance of -20 dB loss, roughly corresponding to a 100km distance for a low loss fiber. The key rate rapidly falls down at a distance of -40 dB loss, which is roughly a link budget for a LEO-to-ground distance in space optical communication. The curve entitled "Tele-amplified BB84" represents a scheme with quantum relay to extend a distance. One sees that there is a tradeoff between the final key rate and the distance, namely extension of distance sacrifices the key rate. Decoyed BB84 hardly generates the secure key at around -40dB, while tele-amplified BB84 can make a QKD link over longer distances. But it may still be a poor rate.

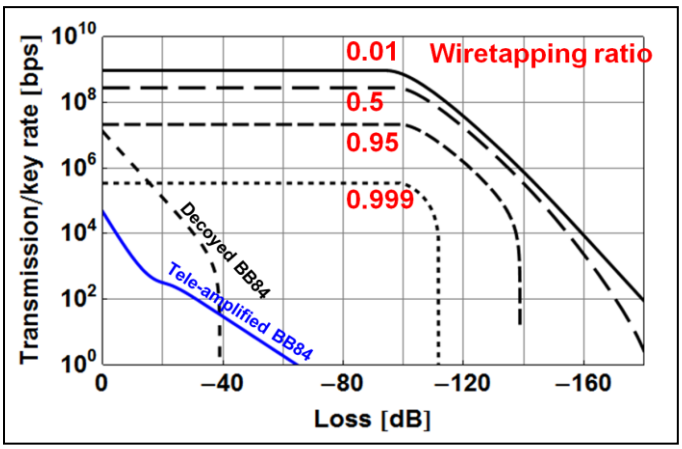

Fig. 2. A numerical example of the secrecy capacities for a wiretap channel. with various tapping ratio in red by an eavesdropper. Pulse position

modulation is assumed in free space laser link. In the left corner of figure, typical key rates in quantum key distribution are also shown.

The solid line on the top shows the transmission rate for an on-off keying scheme with direct detection by an on-off detector. Coding scheme is based on PPM. The pulse generation rate is again 1GHz, and the transmission power is assumed to be 1W. This scheme does not care about any security, but pursues merely attaining the maximum transmission rate within the available signal power. In the region where the transmission rate does not vary as a distance, the signal power is stronger enough than the noises, and the transmission rate is determined merely by the pulse generation rate. As the channel loss decreases below -100 dB, the transmission rate starts to decrease because the signal-to-noise ratio gets smaller.

Now there is a huge gap between the performances of the on-off keying scheme and BB84-QKD. One might naturally ask whether there are some intermediate schemes, which can provide higher capacity as well as strong enough security. The gap will hardly be filled simply by exploiting technological improvement of current QKD schemes. So we consider physical layer cryptography as an intermediate scheme to fill this gap. We make a reasonable compromise for security threats to widen the usability, and pursue high capacity, low power, and provable security at the same time.

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. See Fig. 3. Thus provably secure cryptography is also referred to as physical layer cryptography, and provable security is also called as the information-theoretic security.

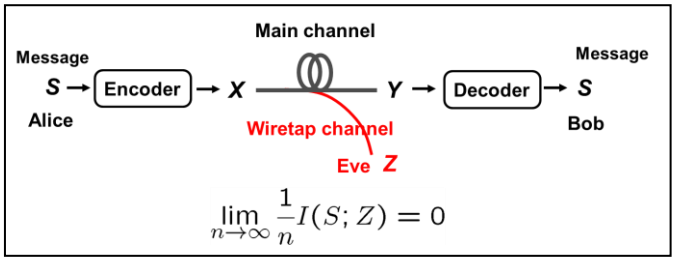

Fig. 3. Schematic of wiretap channel.

In physical layer cryptography, Eve's channel, i. e. wiretap channel is assumed to be worse than that of Bob, such as the signal-to-noise ratio of Eve is less than that for Bob. Then there exists a code that can transmit the amount of bits

$$C_S = \max_{P_x}[I(X;Y) - I(X;Z)] \tag{5}$$

faithfully per sec, making leaked information to Eve arbitrarily small. This is the difference between the mutual information for Alice-Bob and Alice-Eve. P_x is a priori probability of the symbol x. This quantity is called the secrecy capacity, that is, the maximum rate of reliable transmission with the provable security. This is the provable security, whose theoretical basis was first laid by Wyner [6]. In the coding scheme for the wiretap channel, one should add not only redundancy to perform error correction but also randomness for privacy amplification to deceive Eve.

Now the secrecy capacity is estimated for the on-off keying scheme in the wiretap channel in space optical communication. Parameters are the available power for transmission, the channel transmittance, and background noise counts. For Bob, we denote the transmittance by η_y, and assume background counts λ_y of 10000 counts per sec. For Eve, we denote the transmittance by η_z, which is less (worse) than that of Bob ($\eta_z < \eta_y$) and assume background counts λ_z of 1 counts per sec which is much lower (better) than that of Bob. We then calculate the secrecy capacity under the constraint of transmission power. We vary the wiretapping ratio η_z/η_y from 0.01 to 0.999. In Fig. 2, one can see that we can cover wide area of performance of the provably secure communications with relatively high transmission rates.

Our next concern is the quantification of tradeoff between reliability and security. We want to estimate required resources for given levels of reliability for Bob and security against Eve. The redundancy and randomness should be minimal. So we now have two kinds of rates. One is the reliable transmission rate R_B for Bob, and the other is a randomness rate R_E to deceive Eve. Thus there are M of messages, and L of random choices (See Fig. 4). There are some candidates of security measures. We adopt the Kullback-Liebler (KL) distance between the output and target distributions at Eve, because it can quantify the strongest security in an information theoretic way. So we would like to make the Bob's decoding error and the Eve's KL distance as small as desired. To quantify these quantities in finite code length, we extended a notion of reliability function which is the error exponent, and have introduced a notion of the security function [7].

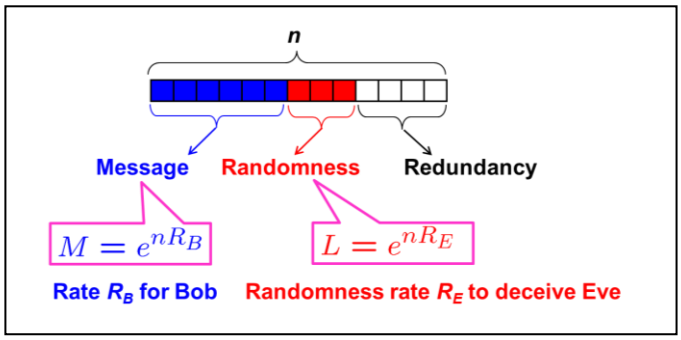

Fig. 4. Conceptual codeword structure and the rate R_B for Bob and the randomness rate R_E to deceive Eve, as well as numbers of message and randomness symbols.

The reliability function is the exponent of the Bob's decoding error as

$$\epsilon_n^B \le 2e^{-nF(q,R_B,R_E,+\infty)} \tag{6}$$

while the security function is the exponent of the Eve's KL distance as

$$\delta_n^E \le 2e^{-nH(q,R_E,n)} \tag{7}$$

These two quantities are dual to each other. They specify how rapid the decoding error and the KL distance decrease as code length *n*.

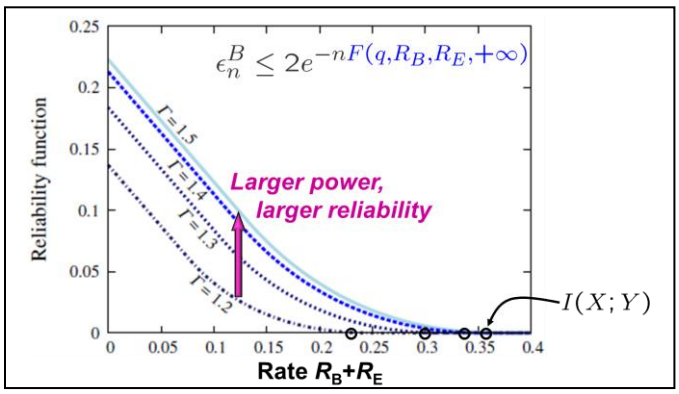

Fig. 5. The reliability functions for several powers.

In Fig. 5 the reliability functions for several cost constraints are plotted. Γ is understood as a given transmission power. As seen, larger power allows larger reliability. The horizontal axis is a sum of the rates R_B and R_E, which specify the ratios of message and randomness parts in the code, respectively. On the other hand, Fig. 6 plots the security functions. Larger power implies weaker security. The horizontal axis is the rate R_E for the resolvability.

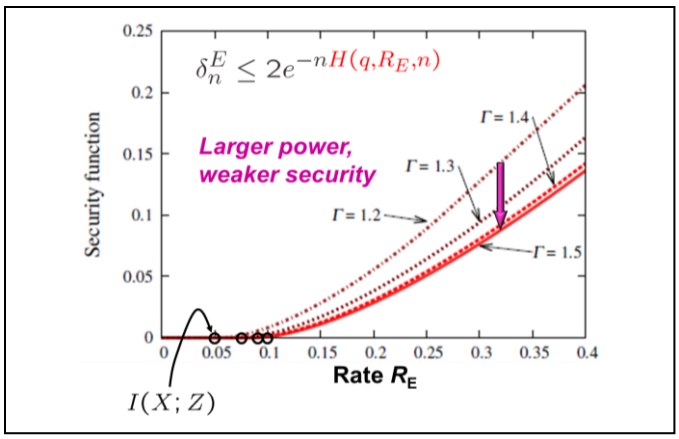

Fig. 6. The security functions for several powers.

In Fig. 7, we plot the reliability and security functions at the same time. The reliable transmission with the provable security is possible for the rates in the interval indicated by the arrow. Fig. 8 shows an example of the tradeoff engineering to increase the security, keeping the reliability of Bob. The randomness rate R_E is increased, while the rate for Bob R_B is decreased, keeping the sum of the two the same value. The change of the security function quantifies the increase of the security level.

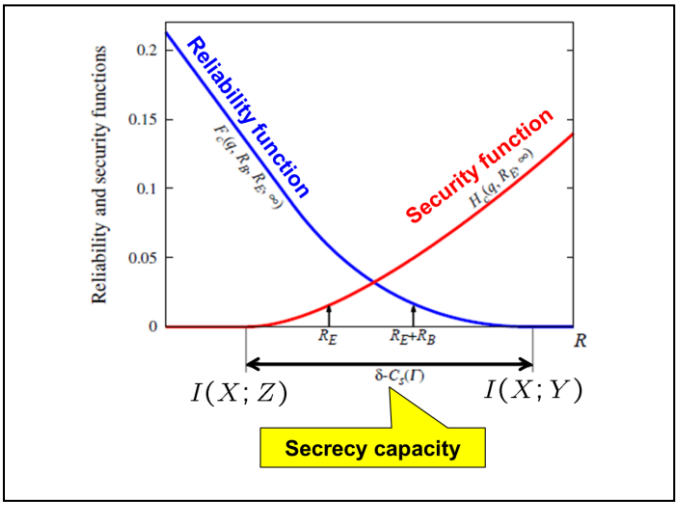

Fig. 7. The reliability and security functions.

IV. DISCUSSION AND OUTLOOK

Next important challenge is to design good constructive wiretap code which can get close to the secrecy capacity. For an ideal detector system with infinite bandwidth (very small time resolution), the on-off keying scheme turns to be a Poisson channel. For Poisson channels we already know an explicit code construction to attain the capacity, which was proposed by Wyner. This is one of equal weight codes. It was also shown by Laourine and Wagner [8] that the Wyner code can also attain the secrecy capacity of Poisson channel. So our next work will be to implement physical layer cryptography in a free space Poisson wiretap channel using Wyner code.

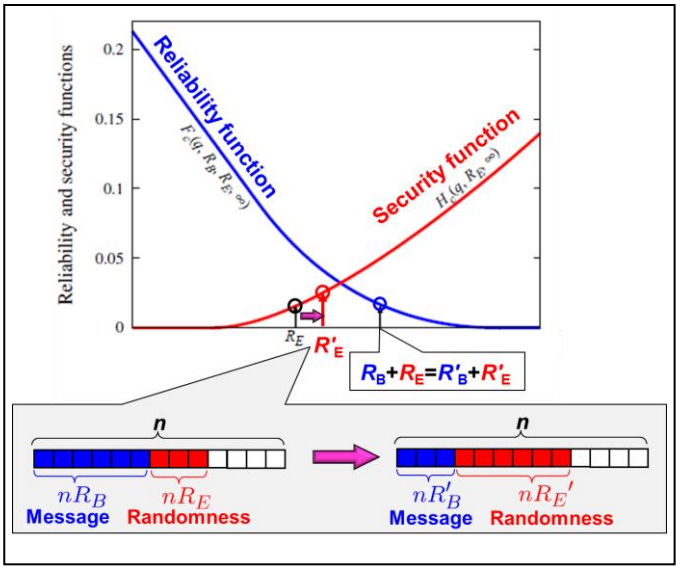

Fig. 8. Example of the tradeoff engineering to increase the security, keeping the reliability of Bob.

ACKNOWLEDGMENT

This work was supported by the Founding Program for World-Leading Innovative R&D on science and Technology (FIRST).

REFERENCES

[1] M. Toyoshima, "Trends in satellite communications and the role of optical free-space communications [Invited]," Journal of Optical Networking, vol. **4**, pp. 300–311, (2005).

[2] V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, J. H. Shapiro, and H. P. Yuen, "Classical capacity of the lossy bosonic channel: The exact solution". Phys. Rev. Lett., vol. 92, 027902/1-4 (2004).

[3] M. Sasaki, K. Kato, M. Izutsu, and O. Hirota, "Quantum channels showing superadditivity in classical capacity," Phys. Rev. A 58, pp. 146–158 (1998).

[4] M. Fujiwara, M. Takeoka, J. Mizuno, and M. Sasaki, "Exceeding the classical capacity limit in a quantum optical channel." Phys. Rev. Lett., vol. 90, 167906/1-4, (2003).

[5] A. Waseda, M. Sasaki, M. Takeoka, M. Fujiwara, M. Toyoshima, and A. Assalini, "Numerical Evaluation of PPM for Deep-Space Links," J. Opt. Commun. Netw. 3(6), pp. 514–521 (2011).

[6] A. D. Wyner, Bell Syst. Tech. J., vol. 54, no. 8,1355-1387 (1975).

[7] 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.

[8] A. Laourine and A. B.Wagner,"The degraded Poisson wiretap channel," IEEE Transactions on Information Theory, vol.IT-58, no.12, pp.7073-7085 (2012).