ISSN 2186-6570

Towards a New Way of Quantum Communication: Getting Around the Shannon Limit of Cryptography

Osamu Hirota and Masaki Sohma

Quantum ICT Research Institute, Tamagawa University
6-1-1 Tamagawa-gakuen, Machida, Tokyo 194-8610, Japan

Tamagawa University Quantum ICT Research Institute Bulletin, Vol.1, No.1, 1-13, 2011

Tamagawa University Quantum ICT Research Institute Bulletin
Vol.1 No.1 : 1-13 (2011)

Towards a New Way of Quantum Communication: Getting Around the Shannon Limit of Cryptography

Osamu Hirota and Masaki Sohma
Quantum ICT Research Institute, Tamagawa University
6-1-1 Tamagawa-gakuen, Machida, Tokyo 194-8610, Japan
E-mail: hirota@lab.tamagawa.ac.jp

***Abstract*—This paper surveys a new way for research of quantum cryptography. The conventional cipher is designed by a mathematical algorithm and its security is evaluated by the complexity of the algorithm for the cryptanalysis and ability of computers. This kind of cipher cannot exceed the Shannon limit of cryptography, and it can be decrypted with probability one in principle by trying all the possible keys against the data length equal to the secret key length. A cipher based on quantum effect so called physical cipher may exceed the Shannon limit of the cryptography. The quantum stream cipher by α/η or Yuen-2000 protocol (Y-00) which operates at Gbit/sec is a typical example of such a cipher, and may exceed the Shannon limit. In this paper, we show an existence of cipher which exceeds the Shannon limit, and discuss practical realization methods for them. First, the conditions to exceed the Shannon limit are summarized. Then we discuss the generalized secret capacity of the wiretap channel model supported by a secret key to discuss an existence of cipher exceeding the Shannon limit. The generalized secret capacities for space communication and fiber communication are given. In general, one needs quantum optimum receiver to realize such capacity. But when bandwidth limitation of users is deleted or the eavesdropper has a device limit, a cipher scheme exceeding the Shannon limit may be realized merely by the conventional optical communication devices which are affected by quantum noise at optical signal measurement.**

I. Introduction

A new network scheme so called "Cloud computing system" based on data centers has recently attracted considerable attention. In that system, all data are communicated via a high speed optical network between a customer and data center or between data centers. There is a serious threat so called "Eavesdropper data center business", which means the eavesdropper can get all data from the transmission line and sell specific data selected by the protocol analyzer to malicious people who wants to get the secret data. This is a new business model of hacker in the era of cloud computing system.

Thus far, the standard encryption systems based on purely mathematical algorithm have been employed to ensure the security of the data base. However, it is still difficult to quantitatively guarantee the security. Furthermore the eavesdropper can store the correct ciphertext from the line. So one cannot deny the possibility of the decipherment of stored ciphertext by the discovery of the mathematical algorithm, or by the development of high speed computers. Especially, if the eavesdropper knows the certain plaintext and the corresponding ciphertext, she may launch the known plaintext attack to data length equal to the key length. Thus, in principle, the key of the mathematical cipher can be revealed. Consequently, the eavesdropper may apply the key to the past correct ciphertext stored in her data center, and finally can retrieve the information data from past to present.

The emerging development of physical cipher at the physical layer suggests a new way of building secure cloud computing system. A new concept of random cipher based on quantum noise has been proposed [1]. It is called quantum noise randomized stream cipher or simply quantum stream cipher. The representative concrete protocol is α/η or Y-00, and several implementation schemes have been realized [2,3,4]. The most important feature of this cipher is that the eavesdropper cannot get the correct ciphertext from the line, though the legitimate user can. That is, the ciphertext:Y^B of the legitimate user and the ciphertext:Y^E of the eavesdropper may be different as $Y^B \neq Y^E$. Furthermore, the ciphertext of the eavesdropper becomes random by the real noise in her receiver. Thus, the security is guaranteed by performance limitation of the eavesdropper's receiver to get the ciphertext and cryptanalysis ability to received ciphertext. This opens a new paradigm for the cryptology. Indeed one can realize a cipher exceeding the Shannon limit of cryptography. In the following sections, we will discuss a new cryptography based on physical principle.

II. Challenge in Network Security

A. Outline and Examples of Network Attacks

The most serious challenge that the existing network systems, such as Internet, are facing is considered their vulnerability to the attacks on the server and network terminal buffer. This is because the server and network terminal, which store information and are remotely accessible from the outside, are likely to become easy targets of the attacks from willful groups. Therefore, their main cryptographic concern has been the authentication in accessing a server and the protection of the data stored there.

However, there is also a possibility of eavesdropping by extracting signals from telecommunication lines, which is more effective. Radio communication system is, in particular, vulnerable to eavesdropping. In general, cable communication system is supposed to be secure, but such a myth that "cable communication system is secure" has no scientific basis. In the 21st century, the amount of information in both personal and institutional communication systems increased massively and a large-capacity communication system serves as transmission system. In particular, a high-speed photonic network plays a central role in data transmission for large-capacity inter-institutional communications. It is undoubtedly optical communication cables that are the most vulnerable in the communication systems. Considering its economical cost, it is practically impossible to provide sufficient protection with the entire optical communication cables for tapping prevention.

Through the experiment to confirm the possibility of eavesdropping in optical communication lines in practical use, we have proved such eavesdropping is possible without great difficulty, which results have already been presented in some conferences, and were also published in some of the newspapers on the Japanese industries.

Security issues have become an increasing challenge and high speed cipher will be expected to play a greater role in developing such security.

B. Modern Mathematical cipher and its Challenges

Security of modern mathematical cipher is evaluated by the mathematical complexity of pseudo random number generator (PRNG) to scramble plaintext or one-way function. Under the existing cryptographic theory, exhaustive search (brute force attack) is capable of deciphering any and all symmetric-key ciphers or public key systems. However, considering that even a quantum computer needs several thousand years to complete its exhaustive search, cipher-breaking by exhaustive search shall be deemed impossible in the actual world. In other words, when there is no other way than exhaustive search to crack a certain mathematical cipher, such cipher cannot be deciphered in any application and, therefore, shall be deemed unbreakable, which is reasonable enough. (However, the quantum cryptography community claims a cipher which can be cracked only by exhaustive search as "breakable." It means they are ignoring the real physical limitation for the universe.)

On the other hand, at present, with regard to actual mathematical cipher, it is impossible to guarantee that there is no inverse calculation algorithm against its encryption algorithm. In other words, the challenge mathematical cipher is facing is that there is an undeniable possibility that the shortcut for decipher will be discovered by someone. However, the mathematical cipher community claims that deciphering mathematical ciphers is impossible as long as they are quantitatively secure against the currently known attacks. From the users' point of view, such assumption is unacceptable.

Under such circumstances, it is one-time pad that may be, in principle, unbreakable. In this cipher, both sender and receiver prepare as many secret keys as the plaintext, and one key is allocated per plaintext to be encrypted. Therefore, transmission of a large amount of encrypted plaintext requires a large amount of pre-shared secret keys. However, the following feature is necessary in order to make this cipher unbreakable in principle.

Remark 1: Key sequence shall be true random numbers in order to make one-time pad unbreakable for any plaintext.

C. Information theoretic security analysis in classical cipher

In 1949, the historical paper on security by Shannon was opened to the public. Shannon defined the perfect secrecy or unconditional security by

$$I(X;Y) = 0, \forall X \tag{1}$$

where $I(X;Y)$ is the mutual information, X and Y are plaintext and ciphertext, respectively. To realize this situation, one needs the one time pad under the Shannon's condition so called the Shannon limit in cryptography that can be described as follows [5]:

$$H(X|Y) \leq H(K_s) \tag{2}$$

In this scheme, any plaintext can be securely transmitted through any communication channel against the unbounded adversary. Even if the subsets of the plaintext are known, the attacker cannot predict the remained key sequence. So it may be called information theoretically secure.

However, it is impossible to realize $I(X;Y) = 0$ in practical system. If one wants to relax the condition of Eq(1) such as

$$I(X;Y) < \epsilon \tag{3}$$

instead of being 0, one can consider a natural intermediate notion of security between the unconditional security and computational security. It would be some kind of "statistical security". The most serious fact in this notion is that it is impossible to discuss the meaningful security only by the mutual information, no matter how we interpret "information", if it is not zero. It shows only quantitative evaluation for the statistical independence between a plaintext and ciphertext. Consequently, any user cannot understand the meaning of the ϵ .

So far, many attempts have been made to discuss the perfect security against the unbounded adversary under the condition Eq(2). For example, A.Russell-H.Wang [6], and Y.Dodis-A.Smith [7] claims that if one can assume only the message space with high entropy, it is realizable. However, they do not employ the mutual information to evaluate the security. Rather, they employ the notions of

semantic security or indistinguishability, and evaluate the variational distance or ϵ-indistinguishability.

Let $\epsilon \in [0,1]$ be real number. If, for an arbitrary distribution of a plaintext $P_X \in \mathcal{P}(\mathcal{X})$ and for an arbitrary map $f : \mathcal{C} \to \{0,1\}$, there exists a random variable G_f that depends on f but is independent of X so that for every $h : \mathcal{X} \to \{0,1\}$, it holds that

$$|\Pr\{f(C) = h(X)\} - \Pr\{G_f = h(X)\}| \leq \epsilon \quad (4)$$

The system is called statistical ϵ-semantic security.

If, $\forall m_0, \forall m_1 \in \mathcal{X}$, $\forall f : \mathcal{C} \to \{0,1\}$, the encryption system satisfies

$$|\Pr\{f(C) = 1)|X = m_0\} - \Pr\{f(C) = 1)|X = m_1\}| \leq \epsilon \quad (5)$$

the system is called statistical ϵ-indistinguishability. This is based on the binary decision theory, so it is weaker than the semantic security.

Unfortunately, these notions and evaluations have the same problem that of the mutual information when they are not zero. That is, the formulation is only mathematical interest and does not provide real meaningful security. Although there are many interpretations of ϵ, these justifications should be given from the different theoretical framework. Especially the probability interpretations such as "indistinguishable advantage"or "failure probability", and so on are not justified. In fact, the user or customer of such ciphers cannot understand the meaning in the real world of the security by the quantitative value of ϵ.

In addition, the assumption of the high entropy of the message space is unrealistic in reality. Even if their systems exist, in the network communication, one requires the evaluation against the known plaimtext attack. If $H(X) \sim 0$, it means the statistical attack or the known plaintext attack:KPA. Under the condition Eq(2), if the attacker can apply the KPA based on the subsets of the plaintext, she can try to predict the remained key sequence. In this setting, they may not claim any security at present.

The above example implies the two instructive matters to pursue the quantitative security. One is that the mutual information, variational distance and so on are not adequate to evaluate the quantitative measure of security, and the other is that the immunity against the known plaintext attack is necessary, as long as we consider the symmetric key cipher including one time pad under the leaked information.

Thus, to pursue the quantitative security analysis, one needs more sophisticated theory even in the classical scheme. That is, before we formulate the quantum theory of information theoretic security, we have to go back to the classical theory. The quantum formulation of the analogy of the classical theory is not adequate.

III. Hybrid cipher consisting of one time pad and key distribution

A. Background

It would be better if one time pad which is in principle unbreakable is realized. This idea makes methodological research for secure key distribution attractive. The most secure key distribution is a person's carrying hard disks loaded with random numbers. To this day, such method has been taken with regard to hotline ciphers designated for military and governmental use.

The invention of public-key cryptography in modern era is called a revolution in contemporary cryptographic technology. An important characteristic of public-key cryptography is that it enables cryptographic communications without pre-shared keys. Unfortunately, it requires substantial time in transmitting a large amount of encrypted plaintexts and is not suitable for real time communication. However, this characteristic enables transmission of secret keys for symmetric-key cipher to communicators without pre-shared key. In this sense, public-key cryptography is a historical invention.

On the other hand, will the hybrid cipher become unbreakable if a large amount of secret keys are thus transmitted as preliminary communication arrangements and one time pad is operated with such keys ? The answer is "no." Since the security of public-key system is algorithm-dependent, it is, in principle, breakable. In other words, it is possible that public-key system is in principle cracked and encryption keys are released beforehand.

In light of the discussion above, in order to realize unbreakable one time pad, key distribution should be unconditionally secure and the shared key sequence should be truly random. To cope with such strict requirements,

(i) one has to realize a leak free system, and

(ii) one has to develop the quantitative security analysis which can provide the meaningful security notion.

B. Quantum key distribution and its security evaluation

Quantum information community believes that it is possible to realize the unconditionally secure key distribution by applying the quantum theory. This is why quantum key distribution:QKD has been proposed. The basic protocol of QKD is BB84, whose underlying principle is that eavesdroppers are detected by the perturbation on optical signal. In order that this principle may be functional, it is necessary to use, as an optical source, imperceptible single photon signals. Therefore, this technology is sometimes called single photon quantum key distribution technology. In addition, it requires the pre-shared secret key for a message authentification.

The communication model of such QKD system can be described as follows: First, the single photon communication to send the key sequence is made. Second, the error

correction is applied. In accordance with the theoretical study of QKD, they claim that it is possible to estimate the amount of information leaked to attackers by calculation based on system parameter. With these estimated figures, authorized communicators can disable certain part of their own accumulated key sequences through the means called "privacy amplification", and minimize the amount of information leaked to eavesdropper Eve.

Finally, the system of the final setting goes to the situation as follows. The mutual information between Alice and Eve: $I(K;Y^B)_{AE}$ satisfies

$$I(K;Y^E)_{AE}/n < \epsilon \tag{6}$$

where Y^E is the observation of Eve, and she may estimate K based on Y^E if the mutual information is not zero. So far, almost all researchers on QKD believed that the security of QKD can be guaranteed by minimizing the quantity of information on key sequence which is available to eavesdropper through communication lines. In other word, given the quantity of information per slot, which is available for Eve through communication lines, is $I(X;Y^E)_{AE}/n$, the following formula can be derived.

$$I(K;Y^E)_{AE}/n < \epsilon = 2^{-nE(R)} \tag{7}$$

$E(R)$ corresponds to system specification on the coding, and n is the number of transmitted bits.

One time pad will be operated by using the key sequence generated by such communication protocol (final key). It was believed that when the quantity of information per slot in a key sequence leaked to Eve was exponentially small, such a system was unconditionally secure. That is, if a quantum key distribution system which can exponentially minimize the quantity of information leaked to Eve as Eq(7), the key sequence transmitted by such key distribution is unconditionally secure and one time pad using such keys can attain perfect secrecy.

However, unless $nE(R)$ goes to infinite, this theory may have no significance. That is, this theory does not clarify how the quantity of information is related to cryptographic security for the generated key sequence. In fact, the main theoretical articles have treated the behavior approaching to zero mutual information. So even if they insist an asymptotical meaning, they have difficulty to answer the above requirement.

If n is a real finite, one needs more sophisticated theory on the evaluation of the cryptographic security on the generated key and also on the one time pad based on the final key sequence. That is, in the realm of quantitatively secure cryptographic theory, the security standard for cipher is established by setting up a particular valuation standard for computational complexity and cryptanalytic attack. Nevertheless, the present theories [8] for information theoretic security on QKD under the finite n have not yet succeeded in evaluating quantitative security for the concrete QKD system [9,10].

Discussion on information theoretic security requires the clarification of the relation between the quantity of leaked information and cryptographic security. It is reasonable to evaluate the concrete cryptographic security in information theoretic context based on the possibilities that keys sent by communicators are estimated through the data leaked to Eve. This is also true when the generated key is used as the secret key in one time pad or the conventional symmetric key ciphers. Such issues have been very clearly pointed out in the public paper in QCMC-2006 by H.P.Yuen [11] as shown in the next subsection.

Thus, we have doubts about the claim that Eq(7) can provide a meaningful evaluation of the security. We will show the fact in the next subsection.

C. Hybrid cipher based on Quantum key distribution: (Composition security)

Here we would like to make the situation of the QKD clear. Let us consider the hybrid cipher consisting of one time pad and QKD. How can we realize the perfect secrecy of this hybrid cipher ? The attack strategies in this quantum scheme are complicated. The eavesdropper against QKD system has already leaked information even though it is very small. Thus, one has to establish the semantic security against any kind of attacks including the known plaintext attack under a quantitative measure with operational meaning. Otherwise, one cannot say that this scheme is useful in the current technology.

The known plaintext attack in the quantum setting is also very complicated. We have to consider two cases. One is that Eve has quantum memory, the other is that Eve has no quantum memory. The former is the most essential. That is, the locking theory which was pioneered by D.P.DiVincenzo and B.M.Terhal [12] plays very important role. In fact, Renner and Konig pointed out that the system is insecure when Eve uses the locking information in the known plaintext attack [13,14]. Furthermore, F.Dupuis, J.Florjanczyk, P.Hayden, D.Leung [15] have generalized the locking theory and they have shown that the system is completely insecure when the security is ensured by the mutual information. These examples imply that the mutual information evaluating the leak does not play a sufficient role.

Renner and his coworkers [13,14] have attempted to overcome the known plaintext attack based on the locking theory, and they have proposed the trace distance to evaluate the security of the whole scheme. In addition, several researchers have given a bound of the trace distance by a performance of error correction code. However, H.P.Yuen pointed out in 2009 and 2010 that Renner's trace distance cannot give complete proof in cryptographic importance [9,10]. Here the cryptographic importance means that the user of such a cipher can understand how much secure is the concrete protocol of QKD. Nobody can hear the answer on the above question from Hayashi and

his coworker though they claim again the unconditional security under the trace distance [8].

It is commonly acknowledged that these discussions are very important for the progress in science and technology. All researchers should not skip such discussions. Despite it, it seems that the QKD researchers ignore the criticism and do not respond. Thus, at present, one cannot say that there is a solid theory of the unconditionally secure QKD, though so many researchers discussed these issues.

More serious fact to ensure the information theoretic security is that any abstract mathematical flame as discussed above cannot ensure the operationally meaningful security. If one wants to discuss the above issue, one should go back to the classical system. So far users in the real world did not care a cipher with the information theoretic security, even though many mathematical analysis have been given. The reason is that the researchers of such mathematical issue never say a practical application of own research. Contrary to our expectation, the researchers of QKD insist a practical application in the real world, claiming the information theoretic security. If so, they have responsibility to clarify at least the cryptographic meaning of own evaluation schemes.

Although these research subjects are very important in science, the author would like to point out that one does not need unconditionally secure key distribution by such a fragile technology to realize a hybrid cipher. If one wants to realize unbreakable cipher, the real frontier in cryptography is to invent a cipher with information theoretic security under that the secret key is short. That is, it is how break the Shannon limit of cryptography by physical phenomena.

D. Communication performance

A single photon technology including quantum key distribution and quantum information processing has serious technical limitation and inconsistency of the present information technology. So far, a great effort has been devoted to realizing quantum technology based on single photon or qubit. However, many interesting ideas encountered the technical difficulty in the practice such as a requirement of bit/sec performance even if they have physical importance. Now quantum key distribution is facing the same situation. That is, to realize unbreakable cipher, one has to employ the hybrid cipher consisting of QKD and one time pad. Unfortunately there is a serious technical limitation on the trade-off between speed and distance. Fig.1 shows an example. One can understand the low performance as the communication as follows.

The QKD system with only several Mbit/sec can be replaced by one time pad based on the hard disk of several Tera bytes for random number conveyed by car or train, which is the conventional scheme of one time pad. To be appreciated as the modern communication technology, it has to provide more than Gbit/sec without

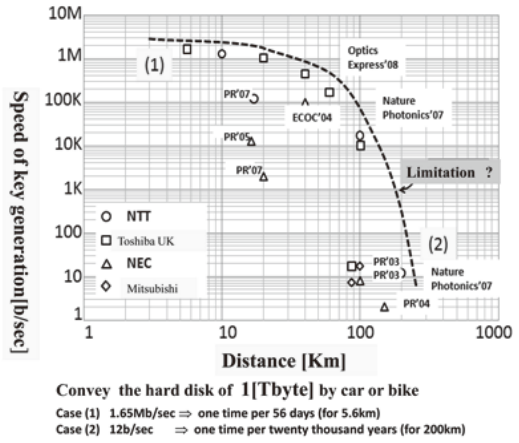

Fig. 1. Trade-off between speed and distance to show impractical performance.

any condition. That is, the hybrid cipher consisting of one time pad and QKD with several Mbit/sec has no technical advantage. Thus the system employing the one time pad with QKD is useless. To avoid such an impractical property, some groups proposed the hybrid cipher consisting of the mathematical cipher and QKD. However, the security of this scheme is limited by the security of the mathematical cipher even if the secret key can be changed many times. In principle, there is no difference between the conventional cipher and such a hybrid cipher. Thus if one cannot remove such trade off, QKD scheme does not offer a benefit to the cryptology in the real world, even if the QKD is attractive technology for providing the key distribution, So we should develop another way.

E. Tokyo demonstration on quantum key distribution by NICT is merely single photon communication

Domestic companies such as NEC, Mitsubishi Electric Corporation and NTT guided by NICT have developed their test models which are ready for application to the actual optical communication system as quantum communication devices. In 2010, they demonstrated the network test in Tokyo, and NICT claimed in a Japanese TV program that NICT group succeeded in the realization of secure QKD network. Also Mitsubishi group claimed in a newspaper such that they had succeeded the demonstration of the secure hybrid cipher of QKD and one time pad for smart phone. In addition, group of NII claimed in a newspaper such that they had succeeded the realization of a prototype of a quantum repeater applicable to 10000 km secure QKD system.

In order to commercialize single-photon quantum cipher, various test models have been developed nationally and globally. Also, journals and international institutes of physics say that unconditionally secure single-photon quantum cipher is now closer to practical use. However,

considering its poor communication characteristic as indicated in Figure 1, single photon quantum cipher scarcely functions as a system. Then, how can its security be guaranteed? Although the results of several eavesdropping experiments have been released and some of them have reported that a single-photon quantum cipher is not unconditionally secure, the community of quantum key distribution has paid no attention to such experiments or reports. However, a decisive eavesdropping experiment was reported in the Nature Photonics [16]. The results of these experiment are summarized as follows: "Eavesdropping experiment on two commercially available single-photon quantum ciphers with off-the-shelf components revealed that it was possible to acquire a full key sequence without leaving any trace."

These vulnerabilities are fundamental ones. If the result of this experiment had not been published, QKDs all over the world would have been insidiously defeated. NICT still ignores this fact and still insists the government funding.

IV. Wiretap channel model

The well known wiretap channel is one of the information theoretically secure communication scheme. The basic theorem of the wiretap channel claims that there exists a coding to ensure the information theoretic security when

$$I(X;Y^B)_{AB} > I(X;Y^E)_{AE} \tag{8}$$

where X is the data. In general, this scheme does not need the secret key before communications. So it is very attractive concept, but it is impractical because of the condition of Eq(8), and unrealistic coding. If one considers the finite case, one has also the same problem as the hybrid cipher based on QKD. However, this concept is an important because it may ensure an existence of the information theoretically secure cipher in principle if the above condition is satisfied. So one may borrow this model in order to pioneer a new frontier when there is a difficulty to show a concrete scheme.

V. Information theoretic basis for security of physical stream cipher

It is well known that the Shannon limit of the symmetric key cipher derives a pessimistic theorem which justifies the one time pad. If the Shannon limit can be exceeded, one does not need hybrid cipher of QKD and one time pad. In this section, we give a survey of a new type of information theoretic basis on the symmetric key cipher.

A. Security against ciphertext only attack

In the conventional cipher, the ciphertext Y is determined by the information bit X and running key K_R. This is called non random cipher. However, one can introduce more general cipher system so called random cipher by noise such that the cipheretext is defined as follows:

$$Y_n = f(X_n, K_{R(n)}, r_n) \tag{9}$$

where r_n is noise. In the Shannon theory for non random or random symmetric key cipher, the information theoretic security on key is given by

$$H(K_s|Y) \leq H(K_s) \tag{10}$$

In addition, the information theoretic security on data is given by the following.

Theorem 1(Shannon, 1949 [5])
The information theoretic security against ciphertext only attack on data has the following limit.

$$H(X|Y) \leq H(K_s) \tag{11}$$

This is called Shannon limit for the symmetric key cipher. Although the equality of Eq(10),(11) can be realized, there is no way to exceed the Shannon limit in the conventional cipher. To exceed the Shannon limit is essential for secure fresh key generation by communication or information theoretic security against known plaintext attack in the symmetric key cipher.

A random cipher by noise may provide a new category of the cipher, and so far many randomized stream ciphers have been proposed in the literature of cryptology. However, at present, there does not exist an attractive cipher. The reason comes from the fact that the ciphertext of eavesdropper and that of legitimate user are the same.

It has been pointed out that there exists an attractive cipher, which gets out the frame of the Shannon theory of cryptology, by means of the combination of the concept of the private randomization of Gauss and the communication system. The crucial property of such a cipher is that the ciphertexts of eavesdropper and legitimate user may be different. Then it has a potential to exceed the Shannon limit. We call such a new random cipher exceeding the Shannon limit "Gauss-Yuen type of cipher". Yuen [17] discussed the necessary and sufficient conditions to exceed the Shannon limit. In the following, we will introduce the basis of cipher that exceeds the Shannon limit.

Theorem 2: Let us denote the ciphertexts of legitimate user and eavesdropper as follows:

$$\begin{aligned} {Y_n}^B &= \{{y_1}^B, {y_2}^B, {y_3}^B, \dots\}, \\ {Y_n}^E &= \{{y_1}^E, {y_2}^E, {y_3}^E, \dots\} \end{aligned} \tag{12}$$

The necessary condition to exceed the Shannon limit is that the ciphertext of eavesdropper and that of legitimate user are different [9].

$${Y_n}^B = f(X_n, K_{R(n)}, {r_n}^B) \neq {Y_n}^E = f(X_n, K_{R(n)}, {r_n}^E) \tag{13}$$

Still the sufficient condition to exceed the Shannon limit is not strict, but if the following relation is retained, one can say that the cipher exceeds the Shannon limit [6,7].

$$H(X|Y^E, K_s) > H(X|Y^B, K_s) = 0 \qquad (14)$$

This needs indeed the quantum effect in the receiver. (Y^E, K_s) means that key is given after measurement. The above equation means that eavesdropper cannot pin down the information bit even if she gets a secret key after her measurement of the ciphertext.

B. Security against known plaintext attack (Qualitative property)

The conventional cipher which belongs to the Shannon class has the following property.

Theorem 3: Any conventional symmetric key cipher with the seed key length($|K_s|$ bits) can, in principle, be broken with probability one by the sample $|K_s|$ bits of the running key under known plaintext attack.

Thus there is no way to realize the information theoretic security against known plaintext attack (ITS against KPA) by the conventional cipher. However, there is a possibility of ITS against KPA when the ciphertext of the eavesdropper and legitimate user are different and it far exceeds the Shannon limit.

In general sense, such a cipher may be evaluated by the extension theorem on the spurious key under the known plaintext attack as follows [18]:

$$\bar{N}_k \geq 2^{H(K_s) - I_n(X_n, K_s, {Y_n}^E)} - 1, \qquad (15)$$

where $I_n(X_n, K_s, {Y_n}^E)$ is n-th extended mutual information (accessible information) from the transmitter to the eavesdropper. Or, more generally, it is evaluated by [18]

$$\mathcal{S}(n) = \max_{{Y_n}^E} \max_{K_s \in \mathbf{K_{YE}}} P(K_s|{Y_n}^E, X_n) \qquad (16)$$

The ITS against KPA can be realized only by far exceeding the Shannon limit. However, it is difficult to evaluate the concrete property of the KPA by the above method. We will need more fundamental work to formulate the quantitative theory of ITS against KPA.

VI. General model exceeding the Shannon limit and generalized secret capacity

A candidate scheme to exceed the Shannon limit is "keyed communication in quantum noise" (KCQ) invented by H.P.Yuen. In the following, we will introduce its basic concept.

A. Keyed communication in quantum noise

Let us describe the keyed communication in quantum noise. The legitimate users Alice and Bob share the secret key and PRNG to extend the secret key. The output of the PRNG is called running key sequence. The running key sequence drives the modulation scheme of optical communication system. That is, the optical signals corresponding to information bit are scrambled by running key sequence via the specific modulation scheme. Bob designs a receiver to demodulate the modulated optical signal by using the secret key and PRNG. The mechanism itself of the receiver enables us to demodulate the information bit. The eavesdropper Eve without the information on secret key cannot apply the optimum receiver to demodulate the optical signals modulated by the running key sequence and information bit sequence. That is, the information on the secret key enables the legitimate users to take the advantage of the signal to noise ratio or the error performance of the receiver to demodulate the optical signals than that of Eve.

Here we summarize the scheme. The optical signals of various form created by PRNG and information bit correspond to ciphertext in the sense of cryptology. Bob can demodulate the information bit without error, but Eve suffers from the tremendous error by quantum noise at observation of optical signals. Eve cannot obtain the correct ciphertext. Thus one may have a possibility of $Y^B \neq Y^E$ which is the necessary condition to exceed the Shannon limit.

B. KCQ scheme as generalized wiretap channel

We here can show an existence of a scheme which can exceed the Shannon limit by means of a generalized wiretap channel though it is not rigorous proof. Let us classify the schemes to realize a cipher based on the KCQ principle as follows:

(i) The legitimate user can use the quantum optimum receiver designed by the quantum communication theory: Quantum optical communication.
(ii) The legitimate user uses the conventional optical receiver: Optical communication.

The case (i) is the fundamental problem to guarantee the theoretical capability, and the case (ii) is an important issue to find the practical application of a cipher exceeding the Shannon limit. In this section, we discuss the case (i). For the case (ii), we will discuss in the next section.

Here let us describe the wiretap channel model based on KCQ principle. The channel between Alice and Bob contains less noise than that of Eve because of the secret key. A secret key and PRNG create the difference of signal to noise ratio at each signal slot between Alice-Bob channel and Alice-Eve channel. So one can apply the concept of the conventional wiretap channel. In order to realize such a situation, we have to find the phenomena

such that the receiver performance with the true key is better than that of without key. We can describe the general model for the above concept as follows [9]:

(i) The key corresponds to the information on the system parameters of transmitter. The legitimate receiver with key can adjust all system parameter using the key information. In such a situation, the legitimate receiver enjoys the quantum gain of the receiver performance depending on key. That is, the ciphertext is $Y^B(K_s)$.
(ii) The eavesdropper's receiver without key does not know all the system parameters of the transmitter to estimate what kind of modulation scheme is used, so she has to employ the universal receiver which is independent of the signal forms. As a result, she cannot enjoy the quantum gain.

Thus, the channel model of the legitimate users is the conventional quantum communication, while the channel model of the eavesdropper has no ability as the communication system when she has no key. However, if the eavesdropper can get the key or all the system parameters after her measurement by the universal receiver like heterodyne receiver, she can apply her knowledge to the measurement data. This situation corresponds to the classical communication system in which the procedure based on the pre-knowledge of the system is applied after the measurement.

Here we can apply the wiretap channel model under the advantage by a secret key. Let us define a generalized secret capacity as follows [19]:

$$\begin{aligned} C_{GS} &= C_H - C_{Shannon+key} \\ &= max\{H(X) - H(X|Y^B(K_s))\} \\ &- max\{H(X) - H(X|Y^E, K_s)\} \end{aligned} \quad (17)$$

where C_H is the Holevo capacity given by quantum optimum receiver with pre-knowledge of key and PRNG which correspond to the knowledge on signal form, and $C_{Shannon+key}$ is the Shannon capacity when the key is given after measurement.

We here show the concrete formula of the generalized secret capacities in the following. Let us recall the Holevo capacity for quantum Gaussian channel which is the most general channel model in quantum communication.

Theorem 4 (Holevo-Sohma-Hirota)[20]:
The capacity of quantum Gaussian channel is as follows:

$$\begin{aligned} C_{HSH} &= \log(1 + \frac{S}{1+ < n >}) \\ &+ S\log(1 + \frac{1}{S+ < n >}) \\ &- < n > \log(\frac{1 + \frac{S}{<n>}}{1 + \frac{S}{1+<n>}}) \end{aligned} \quad (18)$$

where S is the received signal photon, and $< n >$ is the external noise photon.

Consequently, the capacity of the legitimate user is the capacity:C_{HSH} for the quantum Gaussian channel. When eavesdropper can get the key after measurement, she can apply the conventional Shannon capacity formula :$C_{Shannon+key}$ for the quantum Gaussian channel.

(a) Space communication
Let us consider the down link of the space optical communication. The legitimate user and the eavesdropper can use the same power on the ground, so the secret capacity is

$$\begin{aligned} C_{GS} &= S\log(1 + \frac{1}{S+ < n >}) \\ &- < n > \log(\frac{1 + \frac{S}{<n>}}{1 + \frac{S}{1+<n>}}) \end{aligned} \quad (19)$$

In the meaning of Eq(14), we have

$$H(X|Y^B K_s) = 0 \quad (20)$$

$$\begin{aligned} H(X|Y^E, K_s) &= S\log(1 + \frac{1}{S+ < n >}) \\ &- < n > \log(\frac{1 + \frac{S}{<n>}}{1 + \frac{S}{1+<n>}}) \end{aligned} \quad (21)$$

(b) Fiber communication
In fiber communication, the eavesdropper can set the receiver at the transmitter side and use larger power than that of the legitimate user. So the generalized secret capacity is

$$\begin{aligned} C_{GS} &= \log(1 + \frac{S^B}{1+ < n >^B}) \\ &+ S^B\log(1 + \frac{1}{S^B+ < n >^B}) \\ &- < n >^B \log(\frac{1 + \frac{S^B}{<n>^B}}{1 + \frac{S^B}{1+<n>^B}}) \\ &- \log(1 + \frac{S^E}{1+ < n >^E}) \end{aligned} \quad (22)$$

where $(S^B, < n >^B)$ and $(S^E, < n >^E)$ are the received powers for the legitimate user and eavesdropper, respectively. The external noises come from the optical amplifier at the transmitter or the line. In this case, we have to take the energy loss of the transmission line into account to keep the positive secret capacity.

Thus in principle, there exist ciphers exceeding the Shannon limit, but the above formulae do not provide the concrete scheme of the ciphers. In the next section, we discuss the specific protocol of physical random cipher.

VII. Specific models of physical random cipher

We here introduce a concrete physical random cipher so called quantum stream cipher and its concrete realization model Yuen-2000 protocol:Y-00 (code name of the

development). Although it does not in general far exceed the Shannon limit, it is attractive in practical applications.

A. Yuen-2000 protocol

At present, there are several methods to carry out the Y-00 protocol. One is the phase modulation scheme [2] which uses M pairs of two coherent states $|\alpha e^{i\theta_j}>$ and $|\alpha e^{i(\theta_j+\pi)}>$, $j = 1, 2, \dots M$. The $logM$ bits signals from PRNG assign which basis to be employed in order to send the information bit, and the bit data is sent by one of the two coherent states as the basis. This is called PSK-Y00 (Code name in US is α/η). The other one is the amplitude (or intensity) modulation [4]. The amplitude modulation scheme does not need such a huge number of basis even if a high power laser is used, because the maximum (α_{max}) and minimum (α_{min}) amplitudes are fixed and the signal distance for the eavesdropper is set by $|\alpha_{max} - \alpha_{min}|/2M$ which is independent of the laser power. This is called ASK-Y00. When the signal is intensity, it corresponds to intensity shift keying and called ISK-Y00.

Transmitter and receiver share a secret key K_s. The key length is $|K_s| = 100 \sim 1000$ bits. The key is extended to a running key by a PRNG. The output bit sequence of the PRNG, i.e., the running key K_R is divided into blocks of $logM$ bits, and each $logM$ bits is regarded as the running key: $K_R = \{1, 2, \dots, K_i, \dots, M\}$. The length of the running key is $|K_R| < (2^{|K_s|} - 1)/logM$. The correspondence from the running key to the signal parameter of coherent state is called mapping or mapper. In the conventional, the regular mapping is employed. That is, the mapping pattern from running keys to parameters(amplitude, phase, intensity and so on) of coherent states is given by the following relation:

$$\begin{pmatrix} K_R \\ \alpha \\ X \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & M \\ \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \dots & \alpha_M \\ 0 & 1 & 0 & 1 & \dots & 0 \end{pmatrix}, \tag{23}$$

where the mapping $K_i \to \alpha_i$ means that $K_i \to \{\alpha_i, \alpha_i + A\}$, and plaintext X corresponds to the bit value, respectively. In this case, the running key corresponds to the basis $\{|\alpha e^{i\theta_i}\rangle, |\alpha e^{i(\theta_i+\pi)}\rangle\}$. Quantum state sequences emitted from the transmitter can be described as follows:

$$\begin{aligned} |\Psi\rangle &= |\alpha(K_R, X)\rangle_1 |\alpha(K_R, X)\rangle_2 |\alpha(K_R, X)\rangle_3 \dots \\ &= |\alpha_i\rangle_1 |\alpha_j\rangle_2 |\alpha_k\rangle_3 \dots, \end{aligned} \tag{24}$$

where $|\alpha_i\rangle$ is one of $2M$ coherent states, and $i, j, k \in \mathcal{M} = (1 \sim 2M)$.

B. Y-00 with quantum optimum receiver

We assume that the legitimate user Bob has the binary quantum optimum receiver. Such quantum optimum receiver has to know all system parameter before the measurement is done. In this situation the system parameter corresponds to the key. That is, the output of the measurement is $Y^B(K_s)$. The performance is given by Helstrom bound as follows [21]:

$$\bar{P}_e = \frac{1}{2}[1 - \sqrt{1 - \exp(-S)}] \tag{25}$$

When there is no key, one needs to receive the signal by the universal receiver like heterodyne receiver. According to the quantum detection theory, the conventional receiver like heterodyne and so on have no quantum gain in the measurement process. Thus the error performance of the heterodyne with key after measurement is

$$\bar{P}^{(Binary)}_{e(Het+key)} > \bar{P}_e = \frac{1}{2}[1 - \sqrt{1 - \exp(-S)}], \tag{26}$$

So even if Eve gets the key after measurement, she cannot get the same information as the legitimate user. By designing the power region which provides the difference of performance between both receivers, so one has

$$H(X|Y^E, K_s) > 0 \tag{27}$$

Thus, we can in principle get a cipher exceeding the Shannon limit.

C. Wiretap channel by Y-00

Again we assume that the legitimate user Bob can employ the quantum optimum receiver. The difference between the individual quantum measurement and the conventional receiver is not large. That is, the quantum gain may be 3 dB in the power. In order to amplify the quantum gain, one can introduce the coding and the collective decoding as the wiretap channel. The legitimate user has the secret key and PRNG, and the coding scheme consists of the binary coherent states. Then the user can employ the collective quantum optimum receiver for the codeword by the binary coherent states. Here let us discuss the noiseless attenuation channel as a simple example. In this case, the Holevo capacity is given by [22]

$$\begin{aligned} &C_H = \\ &(\frac{1 + |<\alpha_i|\alpha_{M+i}>|}{2}) \log(\frac{2}{1 + |<\alpha_i|\alpha_{M+i}>|}) + \\ &(\frac{1 - |<\alpha_i|\alpha_{M+i}>|}{2}) \log(\frac{2}{1 - |<\alpha_i|\alpha_{M+i}>|}) \end{aligned} \tag{28}$$

where $|\alpha_i>$,$|\alpha_{M+i}>$ are received coherent states. The eavesdropper needs the heterodyne receiver because she does not have the key. The generalized secret capacity is

$$C_{GS} = C_H - C_{Heterodyne+key} \tag{29}$$

However, the capacity with key after measurement for eavesdropper is still unknown. So we cannot explicitly show the generalized secret capacity. We will report in the subsequent paper. In any case, the capacity of the eavesdropper will be smaller than that of the legitimate user.

At present, the concrete coding scheme for the wiretap channel is unknown. So we will still need an investigation of such a coding theory.

VIII. Security of physical random cipher by basic Y-00

In this section, we explain the difference of the security of a mathematical cipher and a physical random cipher by a basic Y-00. A basic Y-00 means that communication systems (transmitter and receiver) for Alice and Bob consist of the conventional optical devices. That is, the quantum effect is only quantum noise at measurement of each signal slot. In this setting, Bob can avoid the effect of quantum noise by the receiver with secret key, The legitimate receiver is the conventional optical receiver, and the ciphertext is Y^B and not $Y^B(K_s)$. That is, $H(X|Y^B, K_s) = 0$. But Eve cannot avoid the quantum noise effect because her receiver does not have the secret key. That is, she has to employ the receiver to discriminate the whole signal value of $2M$.

In the following, we compare a mathematical cipher with Y-00 by a conceptual model. The reader will understand the meaning of randomization of ciphertext.

A. Mathematical cipher

First, let us survey the conceptual theory of a mathematical cipher. The legitimate users Alice and Bob share a secret short key (for example 256 bits) and PRNG. The short key bits are extended by PRNG. The output of the PRNG is called running key :K_R. The length of K_R is about $2^{256}-1$. So Alice can send the plaintext of $2^{256}-1$ without specific bit sequence pattern. A ciphertext is given by running key and information bit as follows:

$$Y = X \oplus K_R \tag{30}$$

The ciphertext is sent from Alice to Bob via the transmission line. Bob receives a ciphertext :Y^B, and Eve also obtains from the line a ciphertext :Y^E. In the mathematical cipher, Eve can obtain the exact ciphertext which is the same as Y^B. That is,

$$Y^E = Y^B \tag{31}$$

First, Eve will try to find a mathematical algorithm for estimating the secret key based on the structure information of PRNG. Second, she makes simultaneous equations such as

$$\begin{aligned} &F(X_1, K_{R(1)}) = Y_1 \\ &F(X_2, K_{R(2)}) = Y_2 \\ &F(X_3, K_{R(3)}) = Y_3 \\ &\vdots \end{aligned} \tag{32}$$

where Y_i are ciphertext at each signal slot i observed by Eve. Third, she will try to solve such simultaneous equations. If the calculation procedure requires exponential time complexity, it will be called secure in the sense of computational complexity.

B. Basic Y-00

In the case of Y-00, Eve has to employ the receiver to discriminate the whole signal value of $2M$. Let Γ be the masking by quantum noise which means the number of signal randomized by quantum noise. When the masking region is $\Gamma \leq M$, the possibility of the secret key is given by

$$Q = \Gamma^{|K_s|/\log M} \tag{33}$$

where $|K_s|$ is the key length. If $\Gamma = M$,

$$Q = 2^{|K_s|} \tag{34}$$

Here, if Eve employs only an individual bit crypto analysis, we have

$$H(K_s|Y^E) = H(K_s) \tag{35}$$

But one cannot claim the above result against more general attack. In fact, the above feature can be realized also by a classical method so called deliberate signal randomization (DSR) [1], giving $\Gamma = M$. However, a realization only by DSR has no possibility of $Y^B \neq Y^E$. In this case, let us assume that Eve can set the $2M$-ary detection and establish the perfect synchronization, and also that she gets the secret key and running key after observation. Consequently, she can decrypt the data even if $\Gamma = M$. That is,

$$H(X|Y^E, K_s) = 0 \tag{36}$$

Thus this scheme cannot exceed the Shannon limit.

Let us go back to a realization by quantum noise. In this case, we can expect a situation of $Y^B \neq Y^E$ as discussed in the following sections, so there is a possibility of the information theoretic security against KPA for longer data than that of the conventional cipher. Thus, although Y-00 protocol itself can be operated by classical setting, it is not equivalent to the conventional cipher, and it has many attractive potentials as the symmetric key cipher as shown in the following.

Alice and Bob share a secret short key (for example 256 bits) and PRNG. The output of the PRNG is running key :K_R. The length of K_R is about $2^{256}-1$. The running key randomly selects an optical modulation scheme or the modulation parameter to produce random optical signals. That is, running key and information bit directly scrambles optical signal at an optical transmitter, and such optical signals correspond to ciphertext which is called physical ciphertext.

Bob receives physical ciphertext and he demodulates such ciphertext by a receiver with running key the same as Alice. He directly obtains information bit at the output of the receiver. Eve has to demodulate physical ciphertext by a receiver without running key. To do so, she needs to receive physical ciphertext itself. However, quantum noise at the receiver disturbs to obtain the exact ciphertext. That is, her ciphertext includes error by true

noise as shown in Eq(33). Thus, Eve cannot establish the correct simultamenous equations as follows:

$$\begin{aligned} &F(X_1, K_{R(1)}) =? \\ &F(X_2, K_{R(2)}) =? \\ &F(X_3, K_{R(3)}) =? \\ &\vdots \end{aligned} \tag{37}$$

The above example enable us to understand the great advantage of physical random cipher. Thus a physical random cipher has a possibility of $Y^B \neq Y^E$ which is the necessary condition to exceed the Shannon limit. More detailed explanation is given in the journal paper [23].

IX. Exceeding the Shannon limit under some conditions

In the practical use, it will be preferable that the legitimate user can use the conventional optical receiver. Under some conditions, we can construct a cipher exceeding the Shannon limit by the conventional optical devices. In the following, we will show some examples of such cases.

A. Relaxation of bandwidth restriction

The coherent pulse position modulation (CPPM) cryptosystem has been proposed as a quantum cipher permitting asymptotical system parameters [1,9]. That is, when the restriction of the bandwidth for the users is relaxed, one can realize a cipher exceeding the Shannon limit by the conventional optical devices.

Transmitter encodes her classical messages by the block encoding where n-bit block j ($j = 1, ..., N = 2^n$) correponds to the pulse position modulation (PPM) quantum signals with N slots,

$$|\Phi_j\rangle = |0\rangle_1 \otimes \cdots \otimes |\alpha_0\rangle_j \otimes \cdots \otimes |0\rangle_N. \tag{38}$$

In addition, the transmitter has the unitary operator U_{K_i} on $\mathcal{H}^{\otimes N}$ to PPM quantum signals $|\Phi_j\rangle$, where K_i of U_{K_i} corresponds to a parameter for the rotation, and is regarded as the running key. Thus, CPPM quantum signal states are generated as follows:

$$|\Psi_{j,K_i}\rangle = |\alpha_{1j}\rangle_1 \otimes \cdots \otimes |\alpha_{Nj}\rangle_N \tag{39}$$

which are sent to the legitimate receiver. Here the unitary operator U_{K_i} is randomly chosen via runnning key K_i generated by using pseudo-random number generator (PRNG) on a secret key K_s. Let us assume an ideal channel. Since the secret key K_s and the map $K_i \to U_{K_i}$ are shared by transmitter and receiver, the legitimate receiver has the unitary operator $U_{K_i}^\dagger$ to the received CPPM quantum signal $|\Psi_{j,K_i}\rangle$ and obtain PPM quantum signal $|\Phi_j\rangle$. The legitimate receiver decodes the message by the direct detection, which is known to be a suboptimal detection for PPM signals [24]. Then the block error rate is given by

$$P_e^{dir} = (1 - \frac{1}{N})e^{-|\alpha_0|^2} < e^{-|\alpha_0|^2}, \tag{40}$$

where $e^{-|\alpha_0|^2} \approx 0$ for sufficently large signal energy $S = |\alpha_0|^2$. In contrast, the eavesdropper does not know the secret key K_s and hence she must detect the CPPM quantum signal states directly. Here we can assume the following. Since the universal receiver is heterodyne, the attacker employs it and she gets the secret key and running key after measurement. Thus, we have

$$H(X|Y^B, K_s) \sim 0 \tag{41}$$

$$H(X|Y^E, K_s) \sim H(X), \quad n >> 1 \tag{42}$$

According to the above analysis, one needs a large number of n when the signal energy is large. Here we give a requirement of channel bandwidth for the secure communication by CPPM. Let us assume that the signal band width is W_s when there is no coding. In this scheme, first one has to transform the n input information bit sequence to PPM signal with 2^n slots. Second, such PPM signals are converted into CPPM with the same slots. If one wants to transmit such CPPM signal with no delay, the required bandwidth is

$$W_{CPPM} = \frac{2^n}{n} W_s \tag{43}$$

Thus, the bandwidth exponentially increases with respect to n. Since one needs the large n to ensure the security, one needs a huge bandwidth. This is an example that one can provide the cipher exceeding the Shannon limit without any quantum device.

B. Security based on physical complexity and device limit

In the conventional mathematical cipher, there is a theory to ensure the ITS when a memory size of the legitimate users is greater than that of the eavesdropper Eve. A physical cipher does not need such a condition. But we can discuss the similar concept based on some conditions.

First we assume that there exist limitations to realize a receiver to demodulate all the optical signals or physical limit of number to prepare receivers for the brute force attack with respect to all candidate of secret key. Through whole discussion, the capability of the computer is not relevant.

The first assumption means that Eve needs devices which have size of the universe or the number of elementary particle in the universe. This guarantees that the brute force attack by the physical trial of all kind of key is impossible. This is called security based on "physical complexity". If one can realize this situation, one does not need information theoretically secure cipher, because already it is unbreakable.

As a more practical situation, we can assume that Eve cannot realize the perfect M-ary receiver. The implementation of the M-ary receiver by the current technology is difficult when $M >> 1$. In this case, even if we employ the basic Y-00, there exists a possibility of the realization of ciphers which exceed the Shannon limit.

At present it is difficult to specify the device limit of the conventional optical receiver. However, we can give some examples. To implement ISK-Y00 with 4096 signal levels, we use the digital to analog converter(DAC). The eavesdropper has to discriminate 4096 signal levels by implementing analog to digital converter (ADC). In the current technology, when the speed of the signal is 2.5 Gbit/sec $\sim$ 10 Gbit/sec, there does not exist ADC to discriminate 4096 signals, while the implementation of DAC is not so difficult for such a performance. The resolution may be 7 bit for 2.5 Gbit/sec $\sim$ 10 Gbit/sec signals. The badness of resolution of ADC enhances equivalently the quantum noise effect. The quantitative analysis on this situation will be given near future.

On the other hand, a synchronization is a fundamental function in the modern digital communication. In the case of the mathematical cipher, Eve can obtain the exact signals from the transmission line. So she can recover any synchronization. In the case of Y-00, the ciphertext is randomized and Eve cannot recover whole synchronizations in all layer only from the observation data via the transmission line. Thus, she cannot apply KPA even if she knows any known plaintext. Of course, if she has no limitation, she can do it, but it would be not practical.

Thus, if we can assume either or both of the above limitation , the basic ISK-Y00 may enjoy the security performance exceeding the Shannon limit and ITS against KPA. Further advantage of such a physical cipher is to ensure the security until the perfect device is developed, and the eavesdropper cannot apply the perfect device to the past ciphertext, because of the insufficient accurateness of the measured ciphertext. In the case of the conventional mathematical cipher, all the past ciphertext can be decrypted if the algorithm for the decryption is invented in the future.

X. Present status of experiment

A. Intensity shift keying Y-00

At present we cannot implement any quantum optimum receiver. Hence as the first generation of the quantum stream cipher, we have developed the basic ISK-Y00 which can be used in the commercial network system. Figure 2 shows the transceiver for the basic ISK-Y00 which operates at 2.5 Gbit/sec with 4096 signals levels. This has a potential to transmit 40 km without amplifier and about 500 km with amplifiers as the repeater. The masking effect in practice has been theoretically and experimentally analyzed to the above system [25,26]. When Eve has to use the conventional receiver, the masking effect is $\Gamma = 150 \sim 250$, if we assume that the resolution of ADC is 12 bits.

Thus, our first target in experiment is not to establish information theoretic security, but it is to establish " physical complexity based cipher" with quantitative security guarantee. In order to ensure the provable security

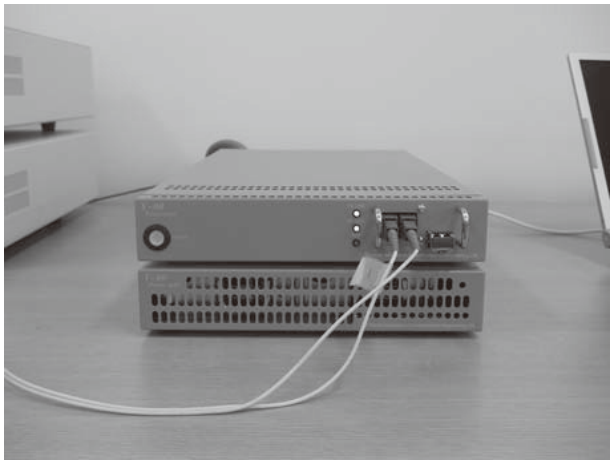

Fig. 2. Transceiver for the ISK-Y00 with information theoretic security under device limit condition, which operates at 2.5 Gbit/sec with 4096 signal levels. The transmission power is 1 mW.

such as security based on physical complexity which is independent of computational power, we need to implement various additional randomization [27,28]. We have a plan to implement such randomization, and quadrature amplitude modulation scheme to improve information efficiency [29].

B. Coherent pulse position modulation

Another candidate to exceed the Shannon limit without any quantum device is coherent pulse position modulation scheme: CPPM. This CPPM requires the realization of the unitary transformation to generate CPPM quantum signal from PPM. Such transformations can be implemented by combination of half mirror and phase rotation mirror, but to generate the CPPM quantum signals with uniform distance for all the signal, we need also a large number of elements. For example let us consider $2^n = 8$ PPM signals with $2^n = 8$ slots. When we implement the unitary transformation by the phase rotation, we need 24 phase rotations to ensure the uniform signal in CPPM. This means that the basis of the scramble by LFSR is 24 bit which is already big size in the practice. So we have to solve the size problem of the implementation of the unitary transformation.

Thus we need more detailed consideration for the practical use of CPPM. In our future work, we will specify the realization method of CPPM.

XI. Conclusion

We have summarized the theoretical basis on ciphers exceeding the Shannon limit. Then we have introduced the secret capacity model supported by secret key to clarify a feature of cipher exceeding the Shannon limit, and given the concrete secret capacities for space communication and fiber communication. We have also discussed the mitigation of the theoretical constraint to exceed the Shannon limit and shown some examples.

At present, ISK-Y00 operated under the device limit of the eavesdropper to obtain a cipher exceeding the Shannon limit is the most realistic. However, although we suggest that an assumption of the device limit to exceed the Shannon limit is reasonable in the real world, we will improve the present system from the device limit to the device independent in near future by introducing elaborate randomization.

ACKNOWLEDGMENT

We are grateful T. Usuda and K.Kato, and F.Futami for fruitful discussions.

REFERENCES

[1] H.P.Yuen, A new approach to quantum cryptography, *arxiv.org:quant-ph*, 0322062, 2003.

[2] G.A.Borbosa, E.Corndorf, G.S.Kanter, P.Kumar, and H.P.Yuen, Secure communication using mesoscopic coherent state, *Physical Review Letters, vol-90*, 227901, 2003.

[3] E.Corndorf, C.Liang, G.S.Kanter, P.Kumar, and H.P.Yuen, Quantum noise randomized data encryption for wavelength division multiplexed fiber optic network, *Physical Review A, vol-71*,062326, 2005.

[4] O.Hirota, M.Sohma, M.Fuse, and K.Kato, Quantum stream cipher by Yuen 2000 protocol: Design and experiment by intensity modulation scheme, *Physical Review A vol-72*, 022335, 2005.

[5] C.E.Shannon, A mathematical theory of secrecy system, *Bell system technical Journal, vol-28* , pp656-715, 1949.

[6] A.Russel and H.Wang, How to fool an unbounded adversary with a short key, *IEEE. Trans. Information theory, vol-52*, pp1130-1140, 2006.

[7] Y.Dodis and A.Smith, Entropic security and the encryption of high entropy messages, *IACR Cryptology e-print at http://eprint.iacr.org./2004/219*, 2004.

[8] M.Hayashi, Upper bounds of eavesdroppers's performances in finite-length code with decoy method, *Physical Review A, vol-76*, 012329, 2007.

[9] H.P.Yuen, Key generation: Foundation and a new quantum approach, *IEEE J. Selected topics in Quantum Electronics, vol-15*, no-6, pp1630-1645, 2009.

[10] H.P.Yuen, Fundamental quantitative security in quantum key generation, *Physical Review A, vol-82*, 062304, 2010.

[11] H.P.Yuen, *Proceedings of QCMC-2006 edited by Hirota, Shapiro and Sasaki, NICT Press*,pp163-171,2007.

[12] D.Vincenzo M.Horodecki, D.Leung, J.Smolin,and B.Terhal, Locking classical correlation in quantum state, *Physical Review Letters, vol-92*, 067902, 2004.

[13] R.Renner and R.Konig, Universally composable privacy amplification against quantum adversaries, *Second Theory of Cryptography conference TCC, Springer Lecture Note vol-3378*, pp407-425, 2005.

[14] R.Konig, R.Renner,A.Bariska, and U.Maurer, Small accessible quantum information does not imply security, *Physical Review Letters, vol-98*, 140502,2007.

[15] F.Dupuis, J.Florjanczyk, P.Hayden, and D.Leung, Locking classical information, *quant-ph* , 1011.1612, 2010.

[16] L.Lydersen,C.Wiechers,C.Wittmann, D.Elser, J.Skaar, and V.Makarov, Hacking commercial quantum cryptography system by tailored bright illumination, *Nature photonics, vol-4*, pp686-689, 2010.
F.Xu, B.Qi, and H.K.Lo, Experimental demonstration of phase-remapping attack in a practical quantum key distribution system, *New Jornal of Physics, vol-12*, 113026, 2010.
H.W.Li, et al, Attacking practical quantum key distribution system with wavelength dependent beam splitter and multi-wavelength sources, arXiv:1110.4574v1[quant-ph], Oct.2011.

[17] H.P.Yuen,R.Nair, E.Corndorf, G.S.Kanter, and P.Kumar, On the security of alpha-eta: response to some attacks on quantum based cryptographic protocols, *Quantum Information and Computation, vol-6*, p561, 2006.

[18] R.Nair and H.P.Yuen, Comment on Exposed key weakness of $\alpha\eta$, *Physics Letters A*, vol-372, p7091, 2008.

[19] O.Hirota, Beyond the Shannon limit by quantum stream cipher Y-00 and Holevo-Sohma-Hirota theorem, *Technical Report of IEICE of Japan, ISEC-2009-72*, pp7-14, 2009. O.Hirota, T.Iwakoshi, M.Sohma, and F.Futami, Quantum stream cipher beyond the Shannon limit of symmetric cipher and the possibility of experimental demonstration *SPIE conference on quantum communication and quantum imaging VIII; Proc. of SPIE, vol-7815*, 2010.

[20] A.S.Holevo, M.Sohma, and O.Hirota, Capacity of quantum Gaussian channels, *Physical Review A, vol-59*, no-3, pp1820-1828, 1999.

[21] C.W.Helstrom, Quantum detection and estimation, *Academic Press*, 1976.

[22] M.Osaki, M.Ban and O.Hirota, The maximum mutual information without coding for binary quantum state signals, *Journal of Modern Optics, vol-45*, no-2, pp269-282,1998.

[23] O.Hirota, Practical security analysis of quantum stream cipher by Yuen 2000 protocol, *Physical Review A, vol-76*, 032307, 2007

[24] H. Yuen, R. Kennedy, M. Lax, Optimum testing of multiple hypotheses in quantum detection theory, *IEEE Trans.Information Theory, vol-IT21*, pp.125-134,1975

[25] T.Iwakoshi, F.Futami, and O.Hirota, Quantitative Analysis of Quantum Noise Masking in Quantum Stream Cipher by Intensity Modulation Operating at G bit/sec Data Rate, *SPIE Security and defense, Proceedings vol-8189*, 2011.

[26] F.Futami and O.Hirota, Masking of 4096-level intensity modulation signals by noises for secure communication employing Y-00 cipher protocol, *Europian conference on optical communication, ECOC-2011* , 2011.

[27] O.Hirota and K.Kurosawa, Immunity against correlation attack on quantum stream cipher by Yuen 2000 protocol, *Quantum Information Processing vol-6*, no-2, pp81-91, 2007.

[28] K.Kato, and O.Hirota, Randomization techniques for the intensity modulation based quantum stream cipher and progress of experiment, *SPIE. Proceedings,vol-8163*, 2011.

[29] K.Kato, and O.Hirota, Quantum stream cipher part V; optimum modulation scheme and the implementation of DSR, *SPIE. Proceedings, vol-6710*, 2007.