Quantum stream cipher by the Yuen 2000 protocol: Design and experiment by an intensity-modulation scheme

Osamu Hirota* and Masaki Sohma†
Research Center for Quantum Information Science, Tamagawa University 6-1-1, Tamagawa-gakuen, Machida, Tokyo, 194-8610, Japan

Masaru Fuse‡
Panasonic (Matsushita Electric Industrial Co., Ltd.), Osaka, Japan

Kentaro Kato§
21st century COE program, Chuo University, Tokyo, Japan
(Received 23 April 2005; published 26 August 2005)

We investigate the Yuen 2000 (so-called Y-00)-protocol, which can realize a randomized stream cipher with high bit rate (Gbit/s) for long distances (several hundreds km). The randomized stream cipher with randomization by quantum noise based on the Y-00 protocol is called a quantum stream cipher in this paper, and it may have security against known plaintext attacks which has no analog with any conventional symmetric key ciphers. We present a simple cryptanalysis based on an attacker's heterodyne measurement and a quantum unambiguous measurement to make clear the strength of the Y-00 protocol in real communication. In addition, we give a design for the implementation of an intensity-modulation scheme and report an experimental demonstration of 1 Gbit/s quantum stream cipher through a 20-km-long transmission line.

DOI: 10.1103/PhysRevA.72.022335 PACS number(s): 03.67.Dd, 42.50.Lc

I. INTRODUCTION

It is very difficult to devise encryption schemes with "provable security" in conventional cryptography. So far, we have two schemes for encryption with provable security. One of the methods is one-time pads supported by a quantum key distribution. The other is a kind of randomized stream cipher. Recently, most efforts to realize encryption with provable security have been devoted to the quantum key distribution invented by Bennett and Brassard in 1984 (the BB84 protocol) [1]. We emphasize the greatness of this achievement which opened a new scientific realm. However, there is a big gap between experimental realization and the real communication network requirement. In addition, unfortunately, one may say that there is no practical unconditionally secure protocol that has ever even been theoretically proposed. Furthermore, any kind of quantum repeater cannot guarantee a high key rate. The key rate decreases exponentially with respect to the distance [2]. This might be equivalent to a no-repeater scheme. Even if a quantum repeater with a quantum media transform is employed [3], there is very little improvement, because no perfect quantum efficiency of medium transformation exists. There is no means of improving such a poor performance. So we would like to point out that the key generation is very important, but it is very narrowminded to define quantum cryptography only by the BB-84 protocol and similar principles [4]. Thus, it is preferable to investigate a quantum symmetric key cipher with information theoretic security based on quantum and optical communication. In 2000, Yuen announced that his new protocol, the so-called Yuen 2000 (Y-00) protocol, may provide a randomized stream cipher with information theoretic security by randomization based on quantum noise and additional mathematical schemes [5,6]. This scheme is called a quantum stream cipher, or $\alpha\eta$ scheme by the Northwestern University group. In conventional cryptography, there is no known complexity-based proof at all on any scheme under known plaintext attacks on keys. It is an interesting subject to show, by a concrete scheme, that the quantum stream cipher by the Y-00 protocol has a potential of the information theoretic security against known plaintext attacks.

In Refs. [7,8] we gave a framework of the concrete security analysis for a quantum stream cipher by the Y-00 protocol. In this paper, we shall show how to apply the results of these papers [7,8] to security analysis and a design and experimental demonstration of the quantum stream cipher by an intensity modulation. However, a general proof of the security of the quantum stream cipher by the Y-00 protocol still remains to be given. The direction of the proof has been suggested by Yuen [6].

II. INFORMATION THEORETICALLY SECURE STREAM CIPHER

First, we will denote the definition of the information theoretic security. Let us assume that the eavesdropper Eve has the following abilities.

(i) She has a computer with unlimited computation power.

(ii) She has unlimited memory capacity

When Eve cannot decode plaintext or keys even if she has the above computational power, the cryptography is informa-

*Also at 21st century COE program, Chuo University. Electronic address: hirota@lab.tamagawa.ac.jp
†Electronic address: sohma@eng.tamagawa.ac.jp
‡Electronic address: fuse.masaru@jp.panasonic.com
§Electronic address: kkatop@ieee.org

tion theoretically secure. Many works on protocols with information theoretic security have been already published in journals of information theory and cryptography. In the following, we will introduce some examples.

A. One-time pad

The definition of perfect secrecy—that is, information theoretic security against any kind of the criteria—is $H(X|Y)=H(X)$, where X and Y are plaintext and ciphertext, respectively. It means that the plaintext X and the ciphertext Y as a function of X are statistically independent. In order to realize such a perfect secrecy, the condition $H(X)\leqslant H(K)$ is required [9] whenever Eve has access to precisely the same information as legitimate users. This situation, in which Eve and Bob can get the same ciphertext, is reasonable in a conventional communication network. In this situation, one of methods to realize perfect secrecy is the one-time pad or Vernum cipher which is a kind of stream cipher. However, as mentioned above, it requires a secret key which is at least as long as the plaintext message. If an infinite key for the one-time pad can be sent through a secure communication, then the one-time pad makes sense in real communications. So far, many researchers in quantum-information science have proposed protocols in order to realize a secure key distribution which are guaranteed by quantum effects in the communication process. The BB-84, Ekert 1991 (E-91), and Bennett 1992 (B-92) protocol are typical examples of such protocols.

B. Randomized stream cipher

In a conventional cryptsystem, the stream cipher is implemented by a pseudo-random-number generator with a short secret key and XOR operation with plaintext data bit. For a symmetric key cipher as direct data encryption, the main criteria of the security are given as follows.

(i) Ciphertext-only attack (CTA) on data and on key: To get plaintext or the key, Eve can know only the ciphertext from her measurement.

(ii) Known and chosen plaintext attack (KTA): To get the key, Eve can know nonuniform statistics for some plaintexts and corresponding ciphertexts or insert chosen plaintext data into the encryption system (for example, inserts all 0 sequence as plaintext in some periods). Then Eve tries to determine the key from input and output. Using the key, Eve can determine the remaining data from the ciphertexts.

(iii) Repetition attack: Since the secret key is fixed, it has a period. Eve can apply CTA and KTA over many periods when the key is reused.

We can summarize the performance of the conventional stream cipher by the unicity distance defined by Shannon [9]. For the ciphertext-only attack on the key, the unicity distance is as follows:

$$n_u = \min\{n: H(K|Y^n) = 0\}. \tag{1}$$

For the known plaintext attack, it can be modified to

$$n_{Gu} = \min\{n: H(K|Y^n, X^n) = 0\}. \tag{2}$$

As an example, the unicity distance is sometimes given as follows:

$$n_u \sim \frac{H(X)}{D}, \tag{3}$$

where D is the redundancy of the plaintext sequence. When the statistics of plaintext is uniform, the unicity distance becomes infinite. Shannon called ciphers with $n_u=\infty$ "ideal ciphers." This is the information theoretic security against ciphertext-only attacks on data. However, the unicity distance of many conventional stream ciphers against known plaintext attacks is finite and sometimes it is

$$u_{Gu} \sim H(K). \tag{4}$$

For example, let us use a linear feedback shift register (LFSR) as a pseudo-random-number generator. Eve can know the secret key when she gets $2|K|$ bits (key and shift parameter uncertainty) as the running key from a pseudo-random-number generator. Thus the stream ciphers are surely broken by a brute force attack only for known plaintext attacks, but not for ciphertext-only attacks and not for known nonuniform plaintext statistics attacks when the length of known plaintext is smaller than the unicity distance. Although there are several proposals which have better performance than that of Eq. (4), no one has succeeded to show the lower bound. Again, the symmetric key ciphers are in principle insecure. This derives from the fact that the security is given only by the key uncertainty.

There is another theoretical issue in discussions of the information theoretically secure stream cipher. It is called a "randomized stream cipher," which was long known even to Gauss. The randomized stream cipher means that ciphertexts are randomized. In modern cryptography, they are designed based on an information theoretic approach and are discussed by Schnorr, Diffie, Maurer, and Cachin [10]. Maurer devised a randomized stream cipher for which one can prove that Eve obtains no information in Shannon's sense about plaintext with probability close 1. But his protocol works under the assumption that the memory capacity of Eve is limited [11]. This approach provides an information theoretic notion of security under a memory restriction. However, unfortunately, it is difficult to implement a practical system with high-speed processing. Thus, it is very difficult to realize an information theoretically secure symmetric key cipher based only on a mathematical algorithm. Yuen, however, points out that it may be possible when one employs randomization by quantum noise. In the following sections, we will show the concrete scheme and the performance of Yuen's so-called Y-00 protocol.

III. QUANTUM COMMUNICATION FOR QUANTUM CRYPTOGRAPHY

In any quantum cryptography such as the BB-84, B-92, E-91, and Y-00 protocol, information is a classical bit sequence. That is, information is the true random bits for the key distribution and the plaintext bits for direct data encryption. The essential assumption in quantum communication for classical information is that quantum states are known to the legitimate users. So classical bits are mapped onto a set of known quantum states. They are transmitted passing

through a completely positive map (cp map) and discriminated by a quantum measurement process described by a positive-operator-valued measure (POVM). Then, a receiver gets classical bits as information by measurements. This model is called the Helstrom-Holevo-Yuen formalism for quantum communication [12–14]. Let us give a brief introduction. The source and output in the quantum communication model are described by a density operator for an ensemble of quantum states which conveys classical information as follows:

$$\rho_{Tin} = \sum p_i \rho_i, \quad \rho_{Tout} = \sum p_i \epsilon(\rho_i), \tag{5}$$

where i is an index corresponding to symbols as classical information and ϵ is a cp map. The discrimination among quantum states at the output of the channel is described by the POVM

$$\Pi_j \geqslant 0, \quad \sum \Pi_j = I, \tag{6}$$

where I is a unit operator. Then a conditional probability for each trial of the measurement is given by

$$P(j|i) = \mathrm{Tr}\, \epsilon(\rho_i)\Pi_j. \tag{7}$$

The minimization problem of the average error probability based on the above equation is called quantum detection theory, which is a fundamental formalism in quantum information science:

$$P_e = \min_{\Pi} \left\{ 1 - \sum p_i \,\mathrm{Tr}\, \epsilon(\rho_i)\Pi_i \right\}. \tag{8}$$

The complete theory has been given by Helstrom, Holevo, and Yuen *et al.*. As a result, we have [12–14] the following theorem.

Theorem 1. Signals with nonorthogonal states cannot be distinguished without error, and optimum lower bounds for error rate exist.

When the error probability is 1/2, there is no way to distinguish them. The other important one is the no-cloning theorem clarified by Wootters-Zurek, Yuen, and Buzek-Hillery [15] as follows.

Theorem 2. Nonorthogonal states cannot be cloned with perfect fidelity and with probability 1.

The most important cp map (communication channel) in the real world is the energy loss channel with 20–100 dB loss. A selection of input quantum states for the channel is one of the interesting problems in quantum communications. But we have the following result [16].

Theorem 3. The input state which keeps the pure state passing through the energy loss channel is the only coherent state.

So we can understand that a desirable state is a coherent state. The question is whether a coherent state is appropriate or not when we take into account two criteria: the efficiency and the security as requirements to quantum communication for quantum cryptography. The Y-00 protocol will verify that the communication by a coherent state can satisfy these two criteria.

IV. YUEN Y-00 PROTOCOL

A. Basic concept

A symmetric key cipher is a scheme that the legitimate users, Alice and Bob, share a secret key. A block cipher and a part of stream ciphers belong to this category. However, they are in principle insecure, because the security is given only by key uncertainty. The problem is whether we can realize the information theoretically secure cipher under a coherent-state system with a finite secret key. In the quantum communication model for quantum cryptography, we have to consider two channels of Alice and Bob and of Alice and Eve. Let us describe them by ϵ_{AB} and ϵ_{AE}. In general, ϵ_{AE} is an ideal channel while ϵ_{AB} is a noisy channel. Even so, the basic performance of cryptography is to prevent the leak of secret information from the channel of legitimate users. In a physical cryptography like quantum cryptography, one may take a method to eliminate Eve's information obtained by her measurement from ϵ_{AE}. In order to realize such a situation, one needs "advantage creation" under the ultimate physical law. It means that the disadvantage of Bob can be got rid of by some processing, while the performance of Eve, who has the unlimited power of computer and physical resources, is superior to that of Bob's in the original situation.

According to quantum detection theory we have the following properties for the average error probability:

$$P_e(\mathrm{BP}) < P_e(\mathrm{BM}),\ P_e(\mathrm{BP}) < P_e(\mathrm{MP}), \tag{9}$$

where BP, BM, and MP mean binary pure state, binary mixed state, and M-ary pure state, respectively. The problem is how to apply the above principle of quantum detection theory to cryptography. Yuen proposes a protocol which combines a shared secret key for legitimate users and a specific quantum state modulation scheme. *This can be called the initial shared key advantage* in a noisy channel. By this advantage, the legitimate users can establish the "advantage creation" under parameters with finite size in the protocol for noisy channel. As a result, one can see a basic principle to guarantee the security as follows [6].

Principle of security. The optimum quantum measurements with a key and without a key have different performance.

An unknown key corresponds to classical randomness. The security of the conventional symmetric key cipher is guaranteed by this classical randomness. However, in Yuen's protocol, a classical randomness is used to make a difference in the performances of quantum measurements. It means that if Eve does not know the key, the quantum limitation of her measurement is enhanced by classical randomness. As a result, Eve has to search for the data or the key based on her measurement results with an unavoidable error. For an explanation of this principle, Yuen gives a simple example in the case without any design as follows [6]: Let us assume that the information source is binary coherent states and the ultimate error performances for a receiver with a key or without a key are

$$P_e^B \sim \exp(-4S) \text{ vs } P_e^E \sim \exp(-2S), \tag{10}$$

where $S=\langle n\rangle$ is signal photon per pulse. These are the error rates derived from the condition that the key be known to Eve after her measurement or that she use her measurement result to pin down the data for various different possible key values. This fact gives us an advantage creation under the ultimate physical law, so it leads to unconditionally secure key generation for the any key length of the initial key, and it also gives a basis for information theoretically secure direct data encryption. The above example is not what we use as a practical quantum cryptography. It only shows a principle. For practical use, we need several additional contrivances. The essential problem is how to extend the above principle towards practical quantum cryptography.

The first idea was proposed as follows [17,18]. Let us prepare M sets of two coherent states with a phase difference π. These are the basis for the transmission of data. We assume that Alice and Bob share a secret key K. The key is stretched by a pseudo-random-number generator (PRNG). Let K' be the pseudo random number from the PRNG. The random decimal number with mod M generated from the block,

$$K'/\log_2 M \equiv \bar{K}' = (\bar{k}_1', \bar{k}_2', \dots), \tag{11}$$

of the pseudo random number is called the running key. A basis is randomly selected by the running key $\bar{K}'$. The data bit is transmitted by the selected basis. The numbering of the basis set is $\{1,2,3,\dots\}$ from around $\theta=0$ to $\theta=\pi$ on the phase space. As a result, the M-ary keying has M different basis based on $2M$ coherent states. So the data bit is mapped onto one of $2M$ coherent states randomly, but of course its modulation map has a definite relationship, which is opened. Bob knows the key and the running key, so his measurement is always the correct binary detection for signals with large signal distance. Since Eve does not know the key, she has to employ basically $2M$-ary detection or other methods. But these are not better than Bob's measurement.

B. Signal design

Alice and Bob in the Y-00 protocol share a secret key K. The key is stretched by a pseudo-random-number generator. The length of the running key is $|K'|$. The data bit is sent by a binary phase shift keying using one of M bases chosen by random decimal numbers generated from the block $\bar{K}' = (\bar{k}_1', \bar{k}_2', \dots)$ of the pseudo random number. So the data bit is mapped onto one of the $2M$ coherent states randomly. Quantum-state sequences emitted from the transmitter can be described as follows:

$$|\Psi\rangle = |\alpha^j\rangle_1 |\alpha^k\rangle_2 |\alpha^l\rangle_3 \cdots, \tag{12}$$

where $|\alpha^j\rangle$ is one of $2M$ coherent states, $\alpha^j = \alpha^j{}_c + i\alpha^j{}_s$, and $j,k,l \in \mathcal{M} = (1-2M)$. In the phase modulation scheme (PSK), the coherent states are described by positions on a circle in the phase-space representation. The radius corresponds to the amplitude or average photon number per pulse at the transmitter. The positions on the circle correspond to phase information of the light wave. If the number of basis is M, then the signal distance between neighboring states is about

$$\Delta_{PM} \cong \frac{2\pi|\alpha|}{2M}. \tag{13}$$

On the other hand, for the amplitude modulation scheme (ASK), it is given by

$$\Delta_{AM} = \frac{|\alpha_{max} - \alpha_{min}|}{2M}. \tag{14}$$

For direct intensity modulation of the laser diode,

$$\Delta_{IM} = \frac{|\alpha_{max}|^2 - |\alpha_{min}|^2}{2M}, \tag{15}$$

where α_{max} and α_{min} are the maximum and minimum amplitudes, respectively. The quantum noise of a coherent state is described by a two-dimensional Gaussian distribution of variance: 1/2 each or a one-dimensional Gaussian of variance:1/4 if one uses heterodyne or homodyne, respectively. Alice and Bob will design the number of bases which satisfies

$$P_e(i,i+1) = \frac{1}{2} - \frac{1}{\sqrt{2\pi}} \int_0^{t_0} \exp(-t^2/2) dt = 0.2 - 0.5, \tag{16}$$

where $t_0 = \Delta_{PM}/2 = \pi|\alpha|/2M$ for the phase modulation scheme and $t_0 = \Delta_{AM}/2$ for the amplitude or intensity modulation scheme. This corresponds to the error probability between neighboring states. But it is not a real error probability of Eve. The real error probability of Eve depends on her strategy and quantum measurement scheme. It is easy to show the numerical examples of the error probability between neighboring states with respect to signal power and number of bases in the amplitude or intensity modulation scheme. For example, $P_e(i,i+1)$ is about 0.45 when $|\alpha_{max}| = 100$, $|\alpha_{min}| = 80$, and $M = 100$.

V. KNOWN AND CHOSEN PLAINTEXT ATTACK

A general framework of attacks on data and on key in the stream cipher is explained in Ref. [19], in which the probability distribution of the plaintext message in ciphertext-only attacks is uniform, according to the attacker, and it is nonuniform in known plaintext attacks. If Eve knows the deterministic plaintext, it corresponds to the chosen plaintext attack. We are concerned with security when Eve can insert her deterministic plaintext. So in this section, our discussions will be devoted to the chosen plaintext attack which is the special case of known plaintext attacks.

A. Heterodyne measurement

Let us consider the stream cipher by the general PRNG of the unicity distance $u_{Gn} = f(|K|)$, where $f(|K|)$ is a function of $|K|$. The conventional stream cipher has the structure

$$c_i = x_i \oplus k_i', \tag{17}$$

where k_i' is the running key. In this case, if Eve knows some plaintexts ($x_i \in \hat{X}$) and the corresponding ciphertext bit sequence, the output sequence as the ciphertext corresponds to the running key. If Eve knows the plaintext bits of $|\hat{X}| = f(|K|)$ and corresponding ciphertext bits, she can determine the secret key by a well-known algorithm and can decode the plaintext of the remaining bit sequence:

$$|K'| - f(|K|). \tag{18}$$

When the PRNG is a LFSR, $f(|K|)=2|K|-1$, and $|K'| \sim 2^{|K|}$. Since, in general, the $f(|K|)$ is finite in the conventional stream ciphers, they are not secure.

In the case of the quantum stream cipher, quantum noise effect is unavoidable, because the signal structure in the Y-00 protocol to any kind of measurement of Eve has the signal set of nonorthogonal states. In addition, the running key is the decimal number. So Eve cannot get exact ciphertext from her measurement. Here we assume that Eve can get all energy of the light wave from the transmitter at the point close to Alice, and she employs the heterodyne measurement when Eve measures the quadrature amplitudes α_c and α_s putting known plaintext to decide which basis was used. Since the quadrature amplitudes are noncommutative, the heterodyne measurement corresponds to the simultaneous measurement of noncommuting observables. So quantum noise is described by the variance $1/2$. Let us assume that the signal power is large and the number of bases is large enough. At that time, even if the measured number for the basis is 5, the true number can be 3 or 7. On the other hand, when we employ overlapping selection keying (OSK) as the modulation randomization [7], the errors of the measured data of Eve are induced mainly for the neighboring quantum states. That is, even if the measured number for the basis is 5, the true number can be 4 or 6. These are the minimum requirement for our design. So the error of the basis will be $J>3$, where J is the number of error bases. Since the quantum error for each measurement is statistically independent, in the individual measurement, the number of combination for $f(|K|)/\log_2 M$ slots which correspond to $f(|K|)$ bits in the output of the PRNG is given by

$$Q \cong J^{f(|K|)/\log_2 M}. \tag{19}$$

After the measurement, Eve has to transform the decimal number with error into the bit sequence and start the Berlekamp-Massey algorithm or several known algorithms. Since Eve's data contain errors by quantum noise, she cannot get the true secret key from the calculation by an algorithm based only on one trial of the known and chosen plaintext attack. So Eve cannot decode the remaining ciphertext sequence.

Here, if Eve can make Q copies of the output sequence of coherent states by a cloning procedure, she can try a brute force attack on Q copies, comparing the known and chosen plaintext and each decoded datum [7,20]. The near optimum cloning for the coherent state sequence is the beam splitter scheme. It means that Eve has to copy the sequence by means of division of the output light from Alice by Q beam splitters. So the copies are described as follows:

$$\begin{aligned}
|\Psi\rangle &= \left|\frac{\alpha^j}{Q}\right\rangle \left|\frac{\alpha^k}{Q}\right\rangle \left|\frac{\alpha^l}{Q}\right\rangle \cdots, \\
|\Psi\rangle &= \left|\frac{\alpha^j}{Q}\right\rangle \left|\frac{\alpha^k}{Q}\right\rangle \left|\frac{\alpha^l}{Q}\right\rangle \cdots, \\
|\Psi\rangle &= \left|\frac{\alpha^j}{Q}\right\rangle \left|\frac{\alpha^k}{Q}\right\rangle \left|\frac{\alpha^l}{Q}\right\rangle \cdots, \\
&\vdots
\end{aligned} \tag{20}$$

Here, when we assume that $\alpha=100-1000$, $M=100-2000$, and $|K|=100-1000$, the amplitude of the coherent state of Eve becomes $\alpha/Q \sim 0$. That is, the signal-to-noise ratio is zero. So Eve cannot get any information by the measurement or apply known and chosen plaintext attacks.

On the other hand, let us consider that Eve knows the plaintexts of more than Z bits defined by the following equation:

$$Z \equiv \frac{f(|K|)}{\log_2 M} Q. \tag{21}$$

In this case, the number of bits of the known and chosen plaintext, which Eve needs, increases exponentially with respect to the key length. Let $|K'|$ be the output bit length of the PRNG, and let us assume that the communication is stopped at a period of the PRNG. If the number of bits Z is

$$Z \ll |K'|/\log_2 M, \tag{22}$$

Eve may find the true key by Q-times measurements using possible Q keys and input-output data, because the number of keys is reduced to be Q by the first measurement for $f(|K|)/\log_2 M$ bit. As an example, when the PRNG is the LFSR,

$$Z \cong \frac{(2|K|-1)}{\log_2 M} J^{(2|K|-1)/\log_2 M} < 2^{|K|} - 1. \tag{23}$$

As a result, Eve can find the key at least by a brute force search. So the original scheme of the Y-00 protocol is the exponentially-search-based security against known and chosen plaintext attacks, when the power of the transmitter is large. However, if a PRNG provides

$$Z > |K'|/\log_2 M, \tag{24}$$

the brute force attack cannot be completed in a period of the PRNG. As a result, the success probability of the attack with an exponential number of the known and chosen plaintext does not become the unity. We shall here show an example. If we employ the nonlinear feedback shift register (NFSR) such as a "de Brujin sequence" as the pseudo-random-number generator [10], there exists a sequence with $f(|K|) \gg 2|K|$ and the period $2^{|K|}$. In this case, we get

$$Z \gg 2^{|K|}/\log_2 M. \tag{25}$$

We should emphasize that the security of the PRBG is not essential for the security of the Y-00 protocol. We only need the large linear complexity, because the security of the Y-00 protocol is guaranteed by preventing the trial of the brute force attack itself.

On the other hand, even if we employ the LFSR, it is easy to provide the relation of Eq. (24) by additional randomizations [6,7] such as the breaking of phase locking or the rotation of the axis of the phase plain in the phase modulation scheme, and the sifting of the center line of the amplitude in the intensity modulation scheme. As a result, we have

$$Q \cong M^{2|K|/\log_2 M} = 2^{2|K|}. \tag{26}$$

So again, the brute force attack cannot be completed in a period of the PRNG. Thus, if the attack is only the brute force attack, it is at least secure during about $|K'|/\log_2 M$ data bits, even if Eve has an infinite power of computing and infinite memory capacity. This means that the quantum stream cipher with an *appropriate design* is secure against the known and chosen plaintext attack, if Eve can only carry out the brute force attack under the heterodyne measurement.

On the reuse of the key, for LFSR with $|K|=100$, the legitimate users need not to change the key for more than 10^{12} years, when the bit rate of the modulator is 1 Gbit/s. So the quantum stream cipher has no problem with a repetition of the secret key whenever the PRNG is not reset.

B. Indirect measurement

There is a possibility of the attack based on indirect measurements and post-processing which can reduce the quantum noise effect. In fact, there have been some criticisms against the Y-00 protocol based on such an indirect measurement [21] but they are wrong. Here we analyze the subjects related to those criticisms. The typical method of the reduction of noise effects is to measure an indirect observable of the signal, which a certain modulation scheme connects. Indeed, the M-ary keying is taken to be

$$l_i = x_i \oplus \tilde{k}_i, \tag{27}$$

where l_i is one of two regions separated by an appropriate axis on the phase space or on the line of the strength of the amplitude. If the fundamental axis is horizontal, l_0 is upper plain, l_1 is down plain, and x_i is data bit. $\tilde{k}_i$ is 0 for even number and 1 for odd number in the running key of the M-ary assignment [7,17]. For example, $(l_i=\mathrm{up}, \tilde{k}_i=\mathrm{even}) \rightarrow x=1$, $(\mathrm{up}, \mathrm{odd}) \rightarrow x=0$, $(\mathrm{down}, \mathrm{even}) \rightarrow x=0$, and $(\mathrm{down}, \mathrm{odd}) \rightarrow x=1$. However, we should denote that $\tilde{k}_i$ is the result of the mapping from the running key of decimal number as follows:

$$\bar{k}_i' = 1,3,5, \ldots \rightarrow \tilde{k}_i = 1,$$

$$\bar{k}_i' = 2,4,6, \ldots \rightarrow \tilde{k}_i = 0. \tag{28}$$

The essential point of the attack is to measure the indirect observable l_i. However, since the observable does not contain information of the data bit, Eve has to try a brute force attack on the data in a ciphertext-only attack. Moreover, the error of the measurement for l_i is unavoidable. That is, the density operators of the signal sets for up and down measurements are

$$\rho_{up} = \sum_{up} \frac{1}{M} |\alpha_i\rangle\langle\alpha_j|, \tag{29}$$

$$\rho_{down} = \sum_{down} \frac{1}{M} |\alpha_j\rangle\langle\alpha_j|. \tag{30}$$

It is easy to show the quantum limit, which is the most rigorous lower bound of error probability for this signal [12,22]. When the coherent state is mesoscopic $\langle n\rangle \sim 10000$ and 1000 of M in the phase-modulation scheme, the error is about 0.1%. As a result, we have $H(X|Y) > H(K)$. If we employ an additional randomization, the error becomes 1/2.

In the case of the known and chosen plaintext attack, even if the system is error free, then the measurement results of l_i only tell whether the running key is even or odd. Eve cannot get a true running key from the information of whether it is even or odd. Besides, the system is not error free. So it does not work. The above results will deny several criticisms based on the noise reduction by the indirect measurement method. The detailed discussion is also given in Ref. [23].

C. Quantum unambiguous measurement

Let us discuss the chosen plaintext attack based on a collective quantum unambiguous measurement. Again, Eve knows plaintexts of $2|K|-1$ bits, and she prepares a quantum unambiguous measurement which can be applied to quantum-state sequences of $(2^{|K|}-1)/\log M$. When one of the quantum-state sequences of the set is transmitted from Alice, Eve will measure it by her unambiguous measurement. The success probability is evaluated by an exact calculation and also the following property [8].

Remark. The upper bound of average success probability in the quantum unambiguous measurement is smaller than the quantum optimum solution in the quantum detection theory for the same state ensemble.

The quantum unambiguous measurement (QUM) for M symmetric coherent states is formulated by Chefles and Barnett [24]. The success probability is given by the formula

$$P_D(\mathrm{QUM}) = M \min_{k=1,2,3,\ldots,M} |c_k|^2, \tag{31}$$

where

$$|c_k|^2 = \frac{1}{M} \sum_{j=1}^{M} e^{2\pi i jk/M} e^{|\alpha|^2 (e^{2\pi i j/M}-1)}. \tag{32}$$

In fact, in the case of the individual measurement, the success probability of the quantum unambiguous measurement on $M=2000$ symmetric coherent states with $(|\alpha|^2=\langle n\rangle = 10\,000)$ is given by van Enk [25] as follows:

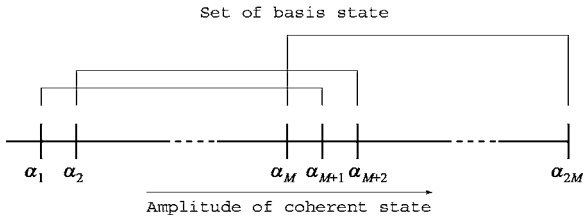

FIG. 1. Design of the basis for amplitude (intensity) modulation.

$$P_D(\mathrm{QUM}) = 3 \times 10^{-12} < \frac{1}{M} = 5 \times 10^{-4} < P_D(\mathrm{Bayes}) \sim 2 \times 10^{-1}, \tag{33}$$

where $1/M$ is a pure guessing. And also, the success probability for collective QUM is given by

$$\mathbf{P}_D(\mathrm{QUM}) \sim 0 < 2^{-|K|} < \mathbf{P}_D(\mathrm{Bayes}). \tag{34}$$

Thus, the success probability is less than that of pure guessing. So in general it does not work.

VI. COMMUNICATION DISTANCE

Here, we analyze how long we can communicate under such a secure condition. Let us assume that the amplitude attenuation parameter of the channel between Alice and Bob is κ. The amplitude of Bob is given by $\kappa\alpha$. When the situation is as follows:

$$\kappa\alpha > \frac{\alpha}{Q}, \tag{35}$$

Even if Eve has a correct key, the error is greater than that of Bob. The signal distance for Bob in the case of phase modulation is given by

$$d_P = 2\kappa|\alpha|, \tag{36}$$

and that for the intensity modulation is

$$d_I = \tfrac{1}{2}\kappa^2(|\alpha_{\max}|^2 - |\alpha_{\min}|^2). \tag{37}$$

If there is no device noise, the error probability of Bob is given by d_P or d_I. The attenuation parameter κ, which can keep as

$$P_e^B < P_e^E, \tag{38}$$

determines the communication distance. As a result, the scheme of the intensity modulation can communicate within at least 100 km with 1 Gbit/s. Application of an optical amplifier will be reported in the subsequent paper. See also Ref. [19].

VII. EXPERIMENTAL RESULT

Several demonstrations of the quantum stream cipher by phase modulation have been reported by the Northwestern University group [17–19]. We would like to realize the quantum stream cipher by the intensity modulation [7,8] which is widely used in conventional optical fiber network systems. In order to verify the excellent feature of the Y-00 protocol by the intensity-modulation scheme, we show an experiment which was done by the Panasonic and our group announced on 30 March 2005.

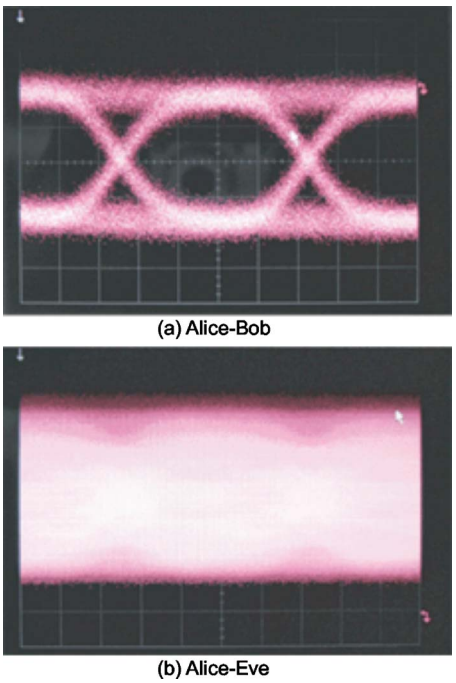

FIG. 2. (Color online) Eye patterns of Bob (top) and Eve (bottom). The eye pattern of Eve has no eye opening, which makes it impossible to discriminate with all of the threshold for the M-ary signals.

Let us give again a brief explanation of the scheme. The maximum and minimum amplitudes of the transmitter are fixed. We divide it into $2M$. So we have M sets of basis state $\{(A_1,A_2),(B_1,B_2),\ldots\}$. The total set of basis states is shown in Fig. 1. Here, the output intensities are the square of each amplitude. In addition, we employ OSK [7] which means that data bits are sent by switching randomly each basis: $(A_1=0,\ A_2=1)$ or $(A_1=1,\ A_2=0)$, $(B_1=0,\ B_2=1)$ or $(B_1=1,\ B_2=0)$, and so on. The system consists of the distributed-feedback laser diode of wavelength $\lambda=1.550\ \mu$m and photodiode which works under the 10 Gbit/s and room temperature. The linearity of the laser diode can be applicable to the analog modulation and the number of bases: M are controlled from 100 to 200. The output power of the laser diode is 0 dBm at continuous operation, and the launch power is kept between about from −25 to −20 dBm by the attenuator. The running key is generated by the hardware LFSR with secret key of 20 bits. The data rate for the modulation is 1 Gbit/s, and the transmission line is about 20 km spool of single-mode fiber. The decision levels of the decoding system of Bob are automatically controlled by the hardware LFSR with the same secret key as the transmitter. In addition, the systems of three parties are completely synchronized. The difference is only with a key or without a key. As a result, the detection scheme of Bob is binary and that of Eve is $2M$-ary.

In this experiment, we assumed that the technology level of Bob and Eve would be the same. Figure 2 shows the eye

patterns for encrypted 1 Gbit/s of Bob (top) who knows the key and of Eve (bottom) who does not know the key, respectively. This scheme corresponds to a ciphertext-only attack for Eve. In these experiments, Bob is located at the end of the 20-km-long line and Eve is located at the transmitter. This figure clearly shows that Bob's error performance is better than that of Eve.

More sophisticated experiments with the demonstration of the heterodyne attack and the application to a highly dense TV system will be reported in the subsequent paper.

VIII. CONCLUSION

In this paper, we have analyzed some security problems of the quantum stream cipher by the Y-00 protocol, in which brute-force complexity-based security is applied and a certain condition for the design is given to guarantee the security. As a result, the quantum stream cipher can be secure against known and chosen plaintext attacks by a heterodyne measurement or quantum unambiguous measurement during $|K'|/\log_2 M$ of data bits which corresponds to a period of PRNG. Experimentally, we have implemented and demonstrated the system of the quantum stream cipher by the intensity modulation scheme with the data rate of 1 Gbit/s for 20-km-long fiber line. However, the demonstrated system has the security in which the security of the conventional stream cipher is enhanced by quantum noise randomization. This provides the randomized stream cipher which has a high rate and high security that cannot be realized by any kind of conventional symmetric key cipher. In subsequent experiments, we will implement several randomizations.

ACKNOWLEDGMENTS

We are grateful to S.J. van Enk and T.Usuda for discussions and to S. Furusawa and T. Ikushima of Panasonic for experimental collaboration. This work was supported by Panasonic funding.

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.
[2] D. Collins, N. Gisin, and H. de Riedmatten, J. Mod. Opt. **52**, 735 (2005).
[3] H. Kosaka, Solid State Phys. **39**, 44 (2004).
[4] F. Grosshans, G. van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature (London) **421**, 238 (2003).
[5] H. P. Yuen, in *Proceedings of QCMC'00, Capri, 2001*, edited by P. Tombesi and O. Hirota (Plenum Press, New York, 2001).
[6] H. P. Yuen, e-print quant-ph/0311061, V6.
[7] O. Hirota, K. Kato, M. Sohma, T. Usuda, and K. Harasawa, Proc. SPIE **5551**, 206, (2004).
[8] O. Hirota, K. Kato, M. Sohma, and M. Fuse, e-print quant-ph/0410006.
[9] C. E. Shannon, Bell Syst. Tech. J. **28**, 656 (1949).
[10] B. Schneier, *Applied Cryptography* (Wiley, New York, 2003).
[11] U. M. Maurer, *Advances in Cryptography-EUROCRYPT* (Springer-Verlag, Berlin, 1991), p. 361.
[12] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic, New York, 1976).
[13] A. S. Holevo, *Statistical Structure of Quantum Theory* (Springer, Berlin, 2001).
[14] H. P. Yuen, R. S. Kennedy, and M. Lax, IEEE Trans. Inf. Theory **21**, 125 (1975).
[15] V. Buzek and M. Hillery, Phys. World **14**, 25 (2001).
[16] C. W. Helstrom, Opt. Commun. **37**, 174 (1981).
[17] G. A. Barbosa, E. Corndorf, P. Kumar, and H. P. Yuen, Phys. Rev. Lett. **90**, 227901 (2003).
[18] E. Corndorf, G. Barbosa, C. Liang, H. P. Yuen, and P. Kumar, Opt. Lett. **28**, 2040 (2003).
[19] E. Corndorf, C. Liang, G. S. Kanter, P. Kumar, and H. P. Yuen, Phys. Rev. A (to be published).
[20] H. K. Lo and T. M. Ko, Quantum Inf. Comput. **5**, 40 (2005).
[21] T. Nishioka, T. Hasegawa, H. Ishizuka, K. Imafuku, and H. Imai, Phys. Lett. A **327**, 28 (2004).
[22] K. Kato and O. Hirota, IEEE Trans. Inf. Theory **49**, 3312 (2003).
[23] H. P. Yuen, P. Kumar, E. Corndorf, and R. Nair, e-print quant-ph/00407067V2.
[24] A. Chefles and S. M. Barnett, Phys. Lett. A **250**, 223 (1998).
[25] S. J. van Enk, e-print quant-ph/0207138; and (private communication).