Practical security analysis of a quantum stream cipher by the Yuen 2000 protocol

Osamu Hirota*

Research Center for Quantum Information Science, Tamagawa University, 6-1-1, Tamagawa-gakuen, Machida, Tokyo, 194-8610, Japan

(Received 26 May 2007; published 7 September 2007)

There exists a great gap between one-time pad with perfect secrecy and conventional mathematical encryption. The Yuen 2000 (Y00) protocol or $\alpha\eta$ scheme may provide a protocol which covers from the conventional security to the ultimate one, depending on implementations. This paper presents the complexity-theoretic security analysis on some models of the Y00 protocol with nonlinear pseudo-random-number-generator and quantum noise diffusion mapping (QDM). Algebraic attacks and fast correlation attacks are applied with a model of the Y00 protocol with nonlinear filtering like the Toyocrypt stream cipher as the running key generator, and it is shown that these attacks in principle do not work on such models even when the mapping between running key and quantum state signal is fixed. In addition, a security property of the Y00 protocol with QDM is clarified. Consequently, we show that the Y00 protocol has a potential which cannot be realized by conventional cryptography and that it goes beyond mathematical encryption with physical encryption.

DOI: 10.1103/PhysRevA.76.032307 PACS number(s): 03.67.Dd, 42.50.Lc

I. INTRODUCTION

Although cryptanalysis on conventional ciphers still requires an unreasonable amount of time, these ciphers may be decrypted with new technological or mathematical advances. A scheme of one time pad forwarded by quantum key distribution (QKD) is one candidate to obtain provable security. However, this essentially suffers from device imperfections that limit the desirable gigabit per second key rate, networking, and system stability. In addition, symmetric key encryption forwarded by QKD cannot improve the essential security. Furthermore, a system based on QKD has difficulty in being applied to the network infrastructure in the real world.

Meanwhile, in 2000, a different concept of quantum cryptography was proposed. It is a kind of stream cipher randomized by quantum noise from measurement of signals with coherent state. The scheme is called Y00 protocol (Y00) or $\alpha\eta$ scheme [1,2] which consists of M-ary modulator for coherent states signals and pseudo random number generator (PRNG) as a driver for basis selection in the modulator. The most simple form consisting of a modulator and a linear feedback shift register (LFSR) is the basic model for an explanation of the principle. The security is designed by controlling the quantum noise effect based on quantum communication theory.

Y00 protocol might be an attractive new quantum cryptography which can realize the ultra high speed data encryption for optical networks. In fact, so far, many remarkable experiments by the basic model have been demonstrated by using phase modulation by the Kumar group [2,3] and intensity modulation schemes by us [4]. Recently a system of 2.5 Gbit/s, 50 Km long in a field network has been demonstrated by using the intensity modulation scheme with some randomizations for running key [5].

If this type of quantum cryptography has provable practical security, it can be immediately applied to the real optical networks, because it can be implemented by conventional optical communication realm and devices. To realize provable practical security which means unbreakable in the real world, we need a general model [1] of the Y00 protocol which consists of a general encryption box as the driver and additional randomizations. The principle and basic features of the security have been explained in [6,7]. They point out that a complete security analysis on Y00 protocol is still difficult because there are so many parameters which the designers can choose. Here let us classify the security levels of a general model of Y00 protocol which should be proved.

(i) Provable practical security against mathematical and physical decryptions on stream ciphers.

(ii) Existence of unicity distance for ciphertext only attack on key and known plaintext attack.

(iii) Full information theoretic security against known plaintext attack in a weak power region.

As the first step, it is meaningful that one considers the case (i) which is a concrete security analysis on specific models of Y00 protocol based on well-known attacks on conventional stream ciphers.

Algebraic attacks and correlation attacks are the most appropriate attacks on conventional stream ciphers. Especially, an algebraic attack is powerful against nonlinear filtering type of stream cipher [8–10]. A correlation attack [11,12] which has been developed in conventional cryptology may be a more meaningful attack on Y00 type protocols than the brute force attack and others. Recently, Donnet *et al.* pointed out a weakness of the basic model by applying a fast correlation attack [13]. Prior to their paper, we mentioned with every opportunity that the basic model with very short key length can be attacked by several correlation attacks. That is, the criticism of the type of Donnet's claim is not detrimental for Y00 protocol security. In fact, we have already shown the fact that Y00 protocol with quantum noise diffusion mapping (QDM) has immunity against any conventional fast correlation attack under the wedge approximation [14]. Even so, there is still discussion on this issue.

Thus we are concerned with practical security of Y00 protocol and conventional mathematical encryption. First, we make clear a difference of purpose between Y00 protocol and one-time pad which provides the perfect secrecy. It is not

*hirota@lab.tamagawa.ac.jp

the perfect secrecy but the ultimate security under the fixed short key that Y00 protocol aims at. It means the establishment of a new theory for encryption protocol.

The purpose of this paper is to clarify what kind of general property is attained by Y00 protocol when an operation is limited only to one period of the PRNG as running key generator of Y00 protocol. That is,

$$N < 2^{|K_s|} - 1, \tag{1}$$

where N is a length of running key sequence. In addition, we will clarify the difference of Y00 protocol security from the conventional stream cipher, by showing that any known algebraic or correlation attack does not work. Furthermore, we will give more detailed property of quantum noise diffusion mapping: QDM which enhances effectively the quantum noise effect even if the quantum noise is small. So it is shown that any known algorithmic attack does not work as the cryptanalysis on Y00 protocol. Finally, we verify that Y00 protocol has a great potential which cannot be realized by conventional cryptography.

II. YUEN-2000 PROTOCOL

A. Basic model

Here let us describe the basic model of Y00 protocol. The transmitter of the basic model of Y00 protocol consists of a LFSR with a seed key(or secret key K_s) and M-ary signal modulator, and the receiver consists of the same LFSR as the transmitter, but the optical receiver can employ a binary detection. Alice and Bob share a secret key K_s. The key length is $|K_s| = 100-1000$ bits. The key is extended to a running key by a LFSR. The length of the running key is $|K_R| < 2^{|K_s|}$ from Eq. (1). The output bit sequence of the LFSR, i.e., the running key K_R is divided into blocks of $\log M$ bits, and each $\log M$ bits is regarded as the running key: $K_R = \{1,2,\ldots,K_i,\ldots,\}$, and $K_i \in \{1,2,\ldots,M\}$. A running key sequence is called keystream. The function taking the running key to the signal phase of coherent state is called mapping or mapper. In the basic model, the regular mapping is employed. That is, the mapping pattern from running keys to bases of coherent states is given by the following relation:

$$\mathcal{L} = \begin{pmatrix} K_i \\ \theta_i \\ x \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots & M \\ \theta_1 & \theta_2 & \theta_3 & \theta_4 & \ldots & \theta_M \\ 0 & 1 & 0 & 1 & \ldots & 0 \end{pmatrix}, \tag{2}$$

where the mapping $K_i \rightarrow \theta_i$ means that $K_i \rightarrow \{\theta_i, \theta_i + \pi\}$, and $\pi > \theta_{i+1} > \theta_i > 0$, and x corresponds to the bit value on the upper plane of the phase space, respectively. In this case, the running key corresponds to the basis $\{|\alpha e^{i\theta_i}\rangle, |\alpha e^{i(\theta_i+\pi)}\rangle\}$. That is, when a running key appears, a coherent state basis corresponding to the running key is chosen. Then, the data $x \in X$ is transmitted by $|\alpha e^{i\theta_i}\rangle$ or $|\alpha e^{i(\theta_i+\pi)}\rangle$ which is one of the two coherent states as the basis. Quantum state sequences emitted from the transmitter can be described as follows:

$$\begin{aligned} |\Psi\rangle &= |\alpha(K_R,X)\rangle_1 |\alpha(K_R,X)\rangle_2 |\alpha(K_R,X)\rangle_3 \ldots \\ &= |\alpha_i\rangle_1 |\alpha_j\rangle_2 |\alpha_k\rangle_3 \ldots , \end{aligned} \tag{3}$$

where $|\alpha_i\rangle$ is one of $2M$ coherent states, $\alpha_i = |\alpha| e^{i\theta_i}$, and $i,j,k \in \mathcal{M} = (1-2M)$. Alice and Bob have to design the number of basis and signal distance between the neighboring states which satisfy

$$|\langle \alpha_i | \alpha_{i+1} \rangle|^2 \sim 1. \tag{4}$$

On the other hand, there is a simple modification in the mapping process so called irregular mapping.

$$\mathcal{L} = \begin{pmatrix} K_i \\ \theta_i \\ x \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots & M \\ \theta_{27} & \theta_{184} & \theta_9 & \theta_{78} & \ldots & \theta_5 \\ 0 & 1 & 0 & 1 & \ldots & 0 \end{pmatrix}. \tag{5}$$

This irregular mapping may provide good protection against fast correlation attacks.

Let us specify the strategy of Eve who does not know key. We have to consider two cases as follows.

(i) Eve does not know data bits.

(ii) Eve knows long data bit sequences.

In the first case, when Eve wants to get the data bit by her measurement, she is required to use the quantum optimum receiver for two mixed states which transmit the data 0 or 1. In any situation, the data security may be guaranteed by an appropriate design of signals. On the other hand, when Eve wants to know the running keystream, she needs the quantum optimum receiver [15] to discriminate the following M mixed states in the case (i):

$$\rho(K_i) = \frac{1}{2}|\alpha_i\rangle\langle\alpha_i| + \frac{1}{2}|\alpha_{M+i}\rangle\langle\alpha_{M+i}|, \tag{6}$$

where $i = 1,2,\ldots M$. In the case (ii), the target becomes M pure states.

If Eve uses a heterodyne measurement as a sub-optimum mode by mode receiver, Eve's ability can approximately be evaluated by the following

$$P_e(i+1|i) = \frac{1}{2} - \frac{1}{\sqrt{2\pi}} \int_0^{t_0} \exp(-t^2/2)dt \sim 0.5, \tag{7}$$

where $t_0 = \pi|\alpha|/2M$ for the phase modulation scheme [2,3], and $t_0 = |\alpha_{\max} - \alpha_{\min}|/4M$ for amplitude or intensity modulation scheme [4]. This corresponds to the error probability between neighboring states, and gives the degree of the quantum noise effect on the quadrature amplitude α. Thus Eve has to measure the sequence, and errors in the measured data are inevitable. Such an error may provide a randomization by quantum noise at the measurement. This fact means that Y00 protocol is a cipher randomized by quantum measurement noise. Despite that, Bob can decrypt the measured data. Indeed the decision making of legitimate users contains no error or few errors because of the measurement with the key. This corresponds to no encryption for Bob. Thus, a crucial point of Y00 protocol is to realize an encryption by the unavoidable error of Eve. So it is clear that Y00 protocol is an encryption by quantum noise.

B. Base of attacks

In physical cryptography, Eve's sophisticated quantum measurement cannot enable her to determine the quantum signals if she does not have the key. This is one of advantages of the physical cryptography. In order to proceed her cryptanalysis, Eve has to launch the conventional decryption methods such as ciphertext-only attacks (CTA) and known plaintext attacks (KPA), after her measurement. In the former attack, Eve attempts to find plaintext or seed key only by ciphertext. In the latter, Eve attempts to find seed key of PRNG by many pairs of known plaintext and corresponding ciphertext. However, a relation between CTA and KPA on Y00 protocol differs from that of the conventional cipher. In the conventional stream cipher, the ciphertext is given by the data bit and the running key as follows:

$$Y_E = X \oplus K. \tag{8}$$

When the data sequence is totally random, the sequence of ciphertext is also completely random. In Y00 protocol, the information of data and running key can be separately measured. That is, even if the data sequence is totally random, running keystream does not have the complete randomness. Thus, the ciphertext-only attack on key is very important for Y00 protocol. This seems to be a weakness of Y00 protocol, but it is not for following reasons.

(i) Difference of security against CTA and KPA in the conventional cipher is large.

(ii) Difference of security against CTA and KPA in the Y00 protocol is small.

If we can guarantee the security against CTA on key for Y00 protocol, it may automatically assures a sufficient security against KPA and vice versa.

C. Quantitative criterion of physical process in attack

Each time slot conveying quantum state is called qumode. We classify the model of the quantum detection method of the attacker as follows.

(i) Individual qumode measurement which is mode by mode measurement).

(ii) Collective qumode measurement which measure a sequence of quantum states as one quantum state.

These are formulated by quantum detection theory pioneered by Helstrom, Holevo, and Yuen [15].

In the case of the individual qumode measurement, the quantum noise region which causes errors in Eve's observation is not so large. Let Γ be the number of error of running key symbol due to quantum noise in this region [7]. In general, Γ is a function of $\kappa = \langle \alpha_{i+1} | \alpha_i \rangle$: $\Gamma(|\kappa|)$, here it is approximately given as

$$\Gamma(|\kappa|) \sim \frac{M}{|\alpha|}\text{:PSK},$$

$$\Gamma(|\kappa|) \sim \frac{M}{|\alpha_{\max} - \alpha_{\min}|}\text{:ASK (or IMDD)}, \tag{9}$$

where PSK is phase shift keying, ASK is amplitude shift keying, and IMDD is intensity modulation and direct detection scheme, respectively. This adds the following complexity by coherent state quantum noise to the PRNG as the driver of the M-ary modulation in the model

$$Q_1 = \Gamma(|\kappa|)^{|K_s|/\log M}, \tag{10}$$

This is called an assisted brute force search complexity [6,7].

All the conventional cryptanalyses on Y00 protocol have to be applied through the individual qumode measurement process. Our main results will be shown on the security level (i) listed in Sec. I based on this qumode measurement. The collective qumode measurement will be shortly discussed in Sec. IV.

D. General model of Y00 protocol

The basic model of Y00 protocol consists of LFSR and a simple deterministic mapping from running key to physical signal. In some practical use, it is sufficient, but in general, the basic model does not have sufficient security. Yuen has emphasized that the original concept of Y00 protocol includes more general model which consists of a general PRNG and any kind of mapping scheme. So the fundamental problem of the security of Y00 protocol is how to design the total system consisting of PRNG and M-ary modulator to realize required security. Although as running key generator we can employ LFSR as PRNG which cannot be used as the conventional cipher, we are interested in how much security is improved by replacing LFSR with nonlinear filtering in the basic model. In addition, we would like to know what kind of general property is obtained by using QDM and nonlinear filtering.

In the following sections, we will give a security analysis on a model consisting of nonlinear filtering as PRNG and a simple regular mapping, and a model consisting of LFSR or nonlinear filtering and QDM against joint attack.

III. SECURITY ANALYSIS ON SOME MODELS OF Y00 PROTOCOL

It is well known that the most powerful attacks on stream ciphers are algebraic attacks [8–10] and fast correlation attacks which are basically known plaintext attack on the conventional cipher. In this section, we will clarify that both of attacks do not work on the Y00 protocol scheme with appropriate design, even when the key length is a relatively short one like $|K_s| \sim 100$.

A. Algebraic attack on Y00 protocol with nonlinear PRNG

When the basic model with LFSR is not sufficient for proven practical security, we can introduce a general model of Y00 protocol. Here we will employ, as an example of the general model of Y00 protocol, a nonlinear PRNG and the regular mapping, and show that the security as cipher of the PRNG itself is not crucial.

1. Ciphertext-only attack on key

It is clear that the security of Y00 protocol against ciphertext-only attack on data is no question. However, the real problem is ciphertext-only attack on key. In Y00 protocol scheme, attackers can get the running keystream which is independent of the sequence of plaintext, by direct measurement of M-ary signal. So this seems to be a weakness of Y00 protocol compared with conventional ciphers. However, it is not true as shown in this section.

Let us assume that binary keystream scheme in which the state of LFSR and keystream are composed of a sequence of bits z_i, and let L be the connection function that computes the next state of the LFSR. Then we employ nonlinear Boolean function f. A composite PRNG by LFSR and nonlinear Boolean function is called filtering type. In the conventional cryptanalysis, the problem is to find the initial state of the LFSR given some output sequence $\{z_i\}$. In the case of Y00 protocol, attacker has to measure $\{z_i\}$, so the output sequence is disturbed by quantum noise.

Here we apply the well known fast algebraic attack. It is described as follows:

(i) Set up a system of equation in the unknowns K_s and z_i.

(ii) Reduce the overall degree in a precomputation step.

(iii) Insert the observed keystream bits into the identifiers z_i.

(iv) Recover K_s by solving the resulting system of equations.

where the system means the PRNG as the driver of Y00 protocol. In order to explain the attack, we employ a nonlinear filtering like the Toyocrypt cipher, because its property is well known. In the Toyocrypt cipher, one has LFSR of 128 bits states, and the degree of the Boolean function f is 63.

Let $(k_0,k_1,\ldots,k_{127})$ be the initial state of LFSR, then the output of the nonlinear filtering is given by

$$z_0 = f(k_0,k_1,\ldots,k_{127}),$$

$$z_1 = f(L(k_0,k_1,\ldots,k_{127})),$$

$$z_2 = f(L^2(k_0,k_1,\ldots,k_{127})),$$

$$\vdots$$

$$z_N = f(L^{N-1}(k_0,k_1,\ldots,k_{127})), \tag{11}$$

where we assume $N<2^{|K_s|}$. The goal of the attack is to recover the initial state $(k_0,k_1,\ldots,k_{127})$ of the LFSR from some N keystream bits $z_0,z_1,\ldots$, by solving multivariate equations. Many algorithms have been proposed to solve such nonlinear multivariate equations, for example, XL algorithm, Gröbner bases method and so on [8–10]. It is known that XL provides a good method to decrypt the Toyocrypt cipher, in which the system of equation becomes 2^{16} equations of degree 4 with 128 variables for 2^{16} observed bits. Recently, it has been clarified that XL is a modification of Gröbner bases computation.

So the most general algebraic attack is an algebraic cryptanalysis using Gröbner bases. Here we apply an attack based on the Gröbner bases which can provide an efficient tool for solving systems of polynomial equations such as Eq. (10). First we have to set up the "ideal" I_N of the target system. The ideal is given by the following set:

$$I_N = \langle z_0 - f(k_0,k_1,\ldots,k_{127}), z_1 - f(L(k_0,k_1,\ldots,k_{127})),\ldots,z_N - f(L^{N-1}(k_0,k_1,\ldots,k_{127}))\rangle. \tag{12}$$

When $|K_s|<N$, the system is called overdefined. The Gröbner bases computation gives a simpler list of generators of the ideal. That is, the Gröbner bases of the ideal gives the solution of the system of equations. At present, the most efficient algorithm to compute the Gröbner bases is F_5 algorithm invented by Faugere [10]. The algorithm F_5 first computes the DRL (degree reverse lexicographic) order Gröbner basis of $\langle z_0 - f(k_0,k_1,\ldots,k_{127})\rangle$, and then a Gröbner basis of $\langle z_0 - f(k_0,k_1,\ldots,k_{127}), z_1 - f[L(k_0,k_1,\ldots,k_{127})]\rangle$, and so on.The complexity of the Gröbner bases computation is given by

$$O(|K_s|2^{|K_s|}) > O(e^{\eta|K_s|}) > O(|K_s|^{d\omega}), \tag{13}$$

where the first term corresponds to the brute force search, the second is a general complexity for the Gröbner bases computation, and the third is the best one at present under some conditions, and where $\eta=\log(\log|K_s|)/\log|K_s|$, d is the degree of the polynomial, and $\omega\sim 3$ is the exponent of the complexity of the part of linear equations, respectively.

Let us consider the basic Y00 protocol with running key generator of the nonlinear filtering as an example. The running key is defined by $\log M$ bits of z_i. By quantum noise, some bits of $\log M$ bits suffer the error. The errors of Y00 protocol with the mapping Eq. (2) occur mainly at a few bits of the lower position of $\log M$ bits. It is described by

$$(z_{t+\log M},\ldots z_{t+3}\oplus e_3, z_{t+2}\oplus e_2, z_{t+1}\oplus e_1) \quad \forall\ t, \tag{14}$$

where e_i is error bit. The eavesdropper needs the consecutive output bits of at least $N=|K_s|$ bits to solve the system of equations with the number of variables $|K_s|$. However, the system of equation cannot be uniquely determined due to the error of the measurement of $|K_s|/\log M$ qumode sequence. The possible number of the system of equations is

$$N_{\mathrm{eq}} = Q_1 = \Gamma(|\kappa|)^{|K_s|/\log M}. \tag{15}$$

Here F_5 algorithm for the Gröbner bases computation requires consecutive bit sequence. Let us collect many measured bits $N>|K_s|$ as the running key in order to set the overdefined equations. Then the possible number of equations for the overdefined system is

$$N_{\mathrm{eq}} = Q_2 = \Gamma(|\kappa|)^{N/\log M} \tag{16}$$

To solve each N equations in Q_2, Eve has the complexity Eq. (12). Even if the running time to compute the Gröbner bases is zero, Eve still has Q_1 possibility, because she has no way to determine which solution is correct in Q_1. Thus, the algebraic attacks on Y00 protocol is not effective.

2. Known-plaintext attack

In the case of known-plaintext attack, Eve knows some plaintexts and corresponding ciphertexts. In this case, the error region of the running key is reduced by adjusting the known plaintext. However, when we employ polarity changing which alternate between 0 and 1 in the same basis [overlapping shift keying (OSK) in our paper [16]), the region becomes the same as the case of ciphertext-only attack.

As mentioned in the above subsection, Eve can get the running keystream independent of the sequence of plaintext. The algebraic attack is the cryptanalysis to running key sequence itself in conventional cryptography, which means the known-plaintext attack. Hence the above fact brings that the knowledge on the plaintext does not help the algebraic attack itself in this case. Consequently, there is no difference between ciphertext-only attack and known-plaintext attack in the algebraic attack on Y00 protocol. After the computation of the Gröbner bases, Eve still has possibility of Q_1. However, in the known plaintext attack, she can try the brute force search. That is, she can compare the known plaintext with the result of the binary detection process with the possible key. So in principle, she can decrypt Y00 protocol. However the complexity is

$$Q_2 O(|K_s|^{d\omega}) Q_1 \gg 2^{|K_s|} \tag{17}$$

where $O(|K_s|^{d\omega})$ is the complexity for the nonlinear filtering itself. In the case of the Toyocrypt cipher, that is small, but it requires computation of Q_2 times of the Gröbner bases complexity.

It is clear that the above feature on the security cannot be attained by nonrandom ciphers of conventional cryptography.

B. Fast correlation attack

As we have seen, the fast algebraic attack is an appropriate attack to solve an overdefined system of error-free nonlinear equations. On the other hand, the fast correlation attack is devised to solve an over-defined system of noisy nonlinear and linear equations. It is defined as follows:

(i) The n-bits segment of the output sequence from the LFSR with $|K_s|$ is regarded as a certain $(n, |K_s|)$ code.

(ii) The corresponding n-bit segment of nonlinear combiner output is the corresponding noisy codeword passing through a binary symmetric channel with error probability $p = \frac{1}{2} - \epsilon$.

(iii) To find the initial state of one of many LFSRs assuming known connection polynomial based on decoding theory.

Since a model of security analysis of Y00 protocol can be described by a noisy channel model consisting of running key sequence as input and measurement result as output, it is reasonable to apply correlation attacks to Y00 protocol. Recently, S.Donnet *et al.* have tried such an attack on the basic model of Y00 protocol with LFSR as running key generator [13]. However, their method is basically equal to a conventional fast correlation attack based on decoding algorithm and provides an efficient result only against a toy model with very short key length, because the correlation between running key sequence and measurement symbols is not efficiently used. Consequently, a complexity of their method has still exponential even for the basic model of Y00 protocol with a simple LFSR and the regular mapping. Hence, one cannot say it is successful as Yuen and Nair have explained [17]. We always emphasize that the basic model is a model for the principle, though it has still good performance. Recently, many improved fast correlation attacks have been proposed as "decimation attack" [18], "conditional correlation attack" [19], and so on. These may be effective against a noise model which come from the non-linearity, and provide important improvement. However, in the case of Y00 protocol, the noise is a real noise, and one can control the noise effect by several ideas as shown in the following section. Consequently, the success condition for the fast correlation attacks can be broken. Thus, these attacks cannot provide an essential improvement against the stream ciphers based LFSR which allow long key length as Y00 protocol based on the real noise. In spite of the above fact, it is meaningful to discuss how to apply the fast correlation attack on Y00 protocol with a short key length nonlinear filtering like the Toyocrypt cipher as the driver for the selection of basis of physical signals, when the quantum noise effect is small.

One cannot directly apply any fast correlation attack to decrypting Y00 protocol with nonlinear filtering. That is, one needs to take into account the correlation between the running key sequence of the output of the nonlinear filtering and the measured sequence as the major analysis. So we may expect that Y00 protocol with nonlinear filtering driver has the great security against correlation attacks, as also pointed out in [17] for any nonlinear ENC used for Y00 protocol. In the following, we will demonstrate this feature of Y00 protocol. Since there are many types of correlation attack, we show these features one by one. The first case is as follows.

(i) Precomputation of the linear complexity of the nonlinear filtering.

(ii) Proceed the fast correlation attack on equivalent LFSR with the linear complexity.

In general, the nonlinear filtering of the degree of d has the following linear complexity

$$C_L = \sum_{i=1}^{d} \binom{|K_s|}{i} \gg |K_s| = 128 \tag{18}$$

So the problem becomes that of fast correlation attack on LFSR with the key length of C_L. In the case of the Toyocrypt cipher, $C_L \sim 2^{100}$, and $C_L \sim 2^{68}$ for LILI-128. Thus, some conventional fast correlation attacks do not work in practice.

The second case is to make a cascade channel model for non linear filtering and quantum noise channel. A typical method to make a channel mode is that of Siegenthaler [20] to construct an equivalent combiner system of LFSRs, depending on the nonlinear Boolean function. Basically this uses properties of the cross correlation function between the driving maximum length sequence of LFSR and the produced running keystream. But the method itself is not feasible. On the other hand, the direct application of the fast correlation attack on the filtering has no guarantee that it will succeed. Some modifications are proposed based on the fast correlation attack [21]. But they require a full period of the LFSR output without an error, and there is no progress along this purpose. Thus, in Y00 protocol, such an idea is not feasible.

Let us consider an application of the decimation attack as the third case. In this regard, a dedicated fast correlation attack on the basic Y00 protocol consisting of a LFSR has been proposed [22]. The feature of this attack is basically to use bits fraction with small error rate of $\log M$ bits sequence translated from the measured running key symbol and to solve appropriate many linear equations to identify the LFSR. That is, it is a combined method of fast correlation and algebraic attacks. When the driver is a LFSR, the output sequence has information on structure of the LFSR per each $2|Ks|$ bits (linear complexity). So necessary equations may become comparatively feasible. However, in the case of Y00 protocol with nonlinear filtering, the target is nonlinear and their attack stands outside the scope of validness. If it is regarded as an equivalent LFSR, the equivalent key length against this attack is exponential, because the linear complexity is exponential. So in their analysis, the complexity of the processing also becomes exponential, even if the quantum noise effect is so small. Thus, such an attack does not work for a general Y00 protocol model.

We have shown in this section that the present powerful attacks on stream cipher do not work on the basic model of Y00 protocol with nonlinear filtering as running key generator even when the quantum noise effect is small. Consequently, Y00 protocol has such an interesting property that a security of the system is drastically improved by compensating a property of the quantum noise encryption and the driver itself. We emphasize that the security of running key generator as the driver is not crucial. In fact, the Toyocrypt cipher can be completely decrypted, but it cannot if Y00 protocol is used on top.

In this section, we do not claim that Y00 protocol with nonlinear filtering as the driver can protect the security against any conventional attack under the unlimited computational power, but in the next section we will discuss such a possibility.

IV. QUANTUM NOISE DIFFUSION MAPPING: QDM

A. Scheme

The method mentioned in the above section is regarded as a kind of product cipher of an encryption box and a physical encryption part. In order to enhance the complexity of the basic model, we can employ many different randomizations on the physical encryption part itself.

These are realized by physical controls on the modulator in Y00 protocol such as keyed randomization, no keyed randomization, and so on. We first describe a definition of keyed mapping from running keys to physical signals as a parameter of coherent states. In the basic scheme, the mapping function is given by Eq. (2). In general, although keyed randomizations increase the attack complexity but they do not affect information theoretic security of the basic model. However, some schemes can provide a drastic complexity increasing. Let us classify the keyed randomization.

Definition 1. A randomization that a mapping from running keys to signals is randomized by an additional running key is called *mixing*.

Definition 2. A randomization that an additional running key can enhance quantum noise effect is called *quantum noise diffusion mapping*.

Clearly a mixing is only to randomize the relation between running keys and signals. So they provide some improvement against certain weakness such as nonuniformity of Eve's error in the basic scheme. The latter case can improve security. A polarity randomization belongs to this category, but it affects only neighboring signal. So these are *partial QDM* which cannot provide the full diffusion effect $\Gamma = M$.

Even when the quantum noise effect is small, we can attain full diffusion by the quantum noise diffusion mapping (QDM) which was introduced by us [14]. In fact, it has been shown that QDM provides immunity against fast correlation attacks without any additional quantum effect.

Let us explain the basic idea. The encryption scheme consists of many mapping patterns, two linear feedback register, and M-ary modulation. The first LFSR with K_{s1} is used to choose a mapping pattern from many mapping patterns $\mathcal{L}_0, \mathcal{L}_1, \mathcal{L}_2, \ldots$. However, each mapping pattern of the set $\{\mathcal{L}_j\}$ is designed as follows:

$$\mathcal{L}_0 = \begin{pmatrix} K_i \\ \theta_s \\ x \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & \ldots & M \\ \theta_1 & \theta_2 & \theta_3 & \ldots & \theta_M \\ 0 & 1 & 0 & \ldots & 1 \end{pmatrix},$$

$$\mathcal{L}_1 = \begin{pmatrix} 2 & 3 & \ldots & M & 1 \\ \theta_1 + \delta & \theta_2 + \delta & \ldots & \theta_{M-1} + \delta & \theta_M + \delta \\ 0 & 1 & \ldots & 0 & 1 \end{pmatrix},$$

$$\mathcal{L}_2 = \begin{pmatrix} 3 & 4 & \ldots & 1 & 2 \\ \theta_1 + 2\delta & \theta_2 + 2\delta & \ldots & \theta_{M-1} + 2\delta & \theta_M + 2\delta \\ 0 & 1 & \ldots & 0 & 1 \end{pmatrix},$$

$$\vdots$$

$$\mathcal{L}_{M-1} = \begin{pmatrix} M & \ldots & M-1 \\ \theta_1 + (M-1)\delta & \ldots & \theta_M + (M-1)\delta \\ 0 & \ldots & 1 \end{pmatrix}, \qquad (19)$$

where $\delta = |\theta_{i+1} - \theta_i| / M$, and θ_i is the phase of the mapping pattern $\mathcal{L}_0$. This resolution is designed by Alice, but Bob does not need this resolution and his receiver scheme is the same as the basic Y00 protocol. That is, he uses the same binary detection.

The crucial point of this method is the shift permutation in the mapping and the size of δ. A mapping pattern is chosen by the random sequence of $\log M$ bits from the first LFSR with K_{s1}. After the selection of the mapping pattern, the second LFSR with K_{s2} assigns which basis should be used to transmit the information bit. Figure 1(a) shows a signal configuration with QDM, and 1(b) shows the relation among signal phases, running key, and data bits. Since both LFSRs are shared between Alice and Bob, the error performance of Bob has no serious degradation even the signal is received passing through the optical channel with energy loss.

In the implementation of this scheme, these two LFSRs should be completely independent of each other. That is, $\log M$ bits for $\mathcal{L}_j$ from LFSR$_1$ and $\log M$ bits for K_i from

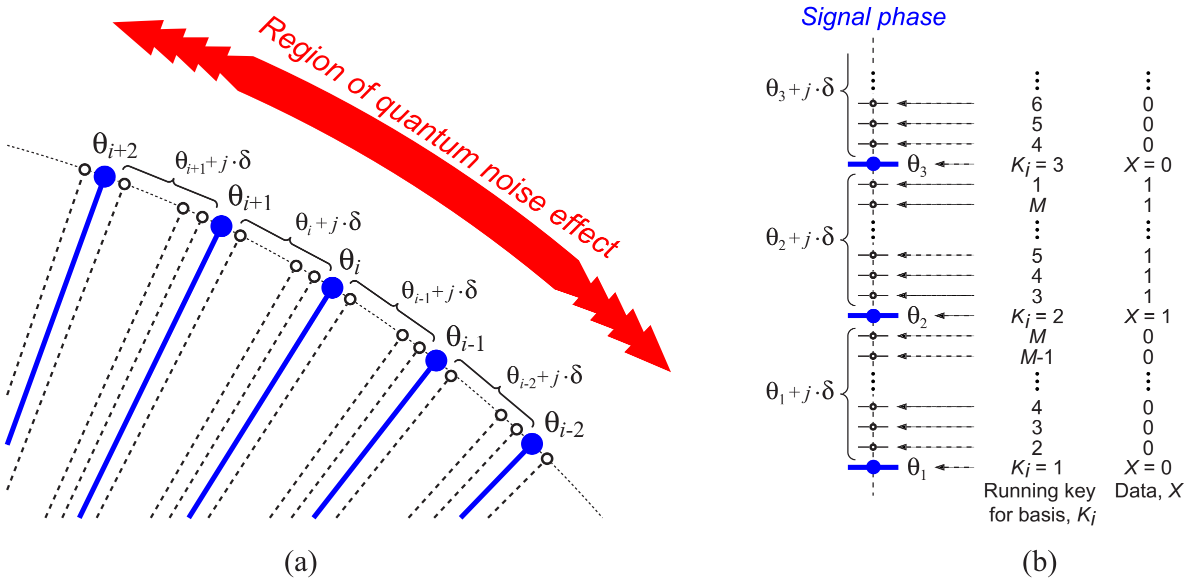
Region of quantum noise effect
θ_{i+2}
θ_{i+1}+j·δ
θ_{i+1}
θ_i+j·δ
θ_i
θ_{i-1}+j·δ
θ_{i-1}
θ_{i-2}+j·δ
θ_{i-2}
(a)
Signal phase
θ_3+j·δ
θ_2+j·δ
θ_1+j·δ
θ_3
θ_2
θ_1
6 5 4 K_i = 3 1 M 5 4 3 K_i = 2 M M-1 4 3 2 K_i = 1
0 0 0 X = 0 1 1 1 1 1 X = 1 0 0 0 0 0 X = 0
Running key for basis, K_i
Data, X
(b)

FIG. 1. (Color online) (a) Phase signal configuration of quantum noise diffusion mapping and (b) a relation among phase signals, running key, and data bit. θ_i is the phase of $\mathcal{L}_1$. j is the index of $\mathcal{L}_j$ and δ is $|\theta_2-\theta_1|/M$.

LFSR$_2$ should be independent. Here we shall point out some properties of QDM.

(i) From Eve's view of point, the driver as the target for decryption can be looked at as one LFSR with seed key K_{s1} or K_{s2}.

(ii) When one of two seed keys is recovered, the total system is broken such as

$$P(K_i|\mathcal{L}_j) = P(\mathcal{L}_j|K_i) \cong 1. \tag{20}$$

However, both keys are completely hidden by quantum noise.

B. Mathematical decryption

Here let us apply mathematical attacks which mean cryptanalysis based on the data observed from individual quantum measurements.

When the scheme of Y00 protocol with OSK, Eve has to discriminate $2M^2$ quantum states which have the phase difference δ to get information on data bits or running key for COA and KPA. The quantum noise in quantum measurements such as heterodyne receiver affects several states close to the true phase. That is, the standard deviation of the measured phase θ_m of mesoscopic coherent states $\{|\alpha_i\rangle\}$ is given as follows [23]:

$$\sigma = \Delta\theta_m > g|\theta_{i+1}-\theta_i|, \tag{21}$$

where g is an integer. It is easy to design the system for $g < 10$ such that $\Delta\theta_m$ is several times of $|\theta_{i+1}-\theta_i|$. Even if Eve can employ the quantum optimum receiver [15], the relation described by the above equation can hold by designing the number of M and the signal energy $|\alpha|^2$.

Here we show more detailed property of the quantum noise diffusion mapping. Let θ_s be the actual signal phase as shown in Fig. 1. It is described by a function when we employ our QDM scheme [14] as follows:

$$\theta_s = \theta_s(x, K_i, \mathcal{L}_j), \tag{22}$$

where $\mathcal{L}_j$ is chosen by the running key from the first LFSR, and K_i is the running key from the second LFSR. Actually the information data bit x is sent by one of phases of the basis determined by K_i in the mapping pattern $\mathcal{L}_j$. Signal phases θ_s of $2M^2$ are uniquely determined by the parameters of $(x, K_i, \mathcal{L}_j)$. From θ_s, the measured phase θ_m is diffused according to a probability density $p(\theta_m|\theta_s)$ which corresponds to the quantum noise. Let us remind the wedge approximation, where-upon a quantum measurement the measured phase θ_m is uniformly distributed within a standard deviation: $\Delta\theta_m$ around θ_s and zero outside.

In order to launch a cryptanalysis on the Y00 protocol seed key, Eve surely needs the exact information of the running keys of two independent LFSRs from her quantum measurement. The effect of the quantum noise is not big enough. That is, the region that Eve cannot distinguish phase signals is only $\Delta\theta_m$. As a result, Eve can know a crude position of the signal on the phase space from her measurement. So she can obtain the information on the combination of $\log M$ bits for $\mathcal{L}_j$ and $\log M$ bits for K_i. As mentioned in the previous section, when we employ the independent two LFSRs, the information of the combination does not have an important meaning to the cryptanalysis.

Here let us assume that Eve's receiver is heterodyne or quantum optimum one. In any case, we have simultaneously as follows:

$$P(K_i|\theta_m) \cong P(K_i) = \frac{1}{M} \quad \forall\ \theta_m,$$

$$P(\mathcal{L}_j|\theta_m) \cong P(\mathcal{L}_j) = \frac{1}{M} \quad \forall\ \theta_m, \tag{23}$$

where the above equations are also independent of the plain text (see Fig. 1). This means that the scheme provides ran-

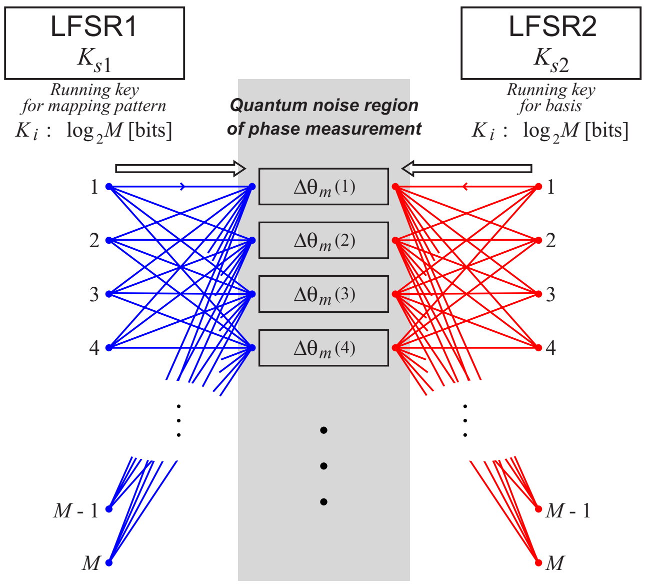

FIG. 2. (Color online) Configuration of noise effect to running key information. Running key K_i from the left LFSR1 selects $\mathcal{L}_i$, and running key K_i from the right LFSR2 selects basis K_i itself. All running keys for both basis and pattern are simultaneously hidden at any point on the full circle.

domization on the seed keys of both LFSRs (see Fig. 2). Thus, for K_i and $\mathcal{L}_j$

$$Q_1 = M^{|K_s|/\log M} = 2^{|K_s|}. \tag{24}$$

On the other hand, this gives simultaneously that the error of per bit level (compare Fig. 3 of Donnet [13]) is $\frac{1}{2}$ for all of $\log M$ bits. Thus Y00 protocol with QDM has no question against any fast correlation attack and algebraic attack. Since K_i and $\mathcal{L}_j$ on the drivers of the modulator have full error, any kind of conventional mathematical algorithm for decryption based on the individual attack does not work. That is, there is no short cut under the operation $N < 2^{|K_s|} - 1$ whenever the wedge approximation is valid. Thus Y00 protocol with QDM may provide just about ideal performance in the sense of the conventional cryptography. Even so, one cannot say that it has information theoretic security of even any level. In principle, Y00 protocol with QDM may be decrypted under the unlimited computer by joint attack which is a brute force attack.

C. Physical decryption

The cryptanalysis discussed in the above section claims that one can basically protect against mathematical decryption on the data observed from quantum measurement. On the other hand, there is a possibility of attack based on signal detection process. We here call it "*a physical decryption*." That is, it attempts directly to determine the running keystream by quantum detection scheme. If Eve can determine the exact running keystream, she can pindown the seed key by conventional cryptanalysis on the PRNG as the driver of Y00 protocol. We have two types such as "individual qumode detection process" and "collective qumode detection process." The latter is called "joint attack," when the process consists of both optimizations for collective qumode measurement process and cryptanalysis on PRNG. In the following, we describe mainly properties of the former type.

1. Basic model and QDM

Here let us assume that the attack is KPA and the PRNG is LFSR. In this case, the determination of the keystream of the length of $|K_s|$ is equal to decryption. The model is described in the following. One sequence of coherent states emitted from the transmitter is regarded as a code word state of the length $|K_s|$ or as one quantum state on the extended space $H_s^{\otimes m}$. So a number of possible code words is $2^{|K_s|}$. Eve's problem reduces to discrimination for such $2^{|K_s|}$ code words with minimum error probability. Quantum states for the code words are

$$|\Psi_1\rangle = |\alpha_1\rangle_1 |\alpha_1\rangle_2 |\alpha_1\rangle_3 \cdots |\alpha_1\rangle_m,$$

$$|\Psi_2\rangle = |\alpha_2\rangle_1 |\alpha_1\rangle_2 |\alpha_1\rangle_3 \cdots |\alpha_1\rangle_m,$$

$$|\Psi_3\rangle = |\alpha_1\rangle_1 |\alpha_2\rangle_2 |\alpha_1\rangle_3 \cdots |\alpha_1\rangle_m,$$

$$\vdots$$

$$|\Psi_{\mathcal{N}}\rangle = |\alpha_{\mathcal{N}}\rangle_1 |\alpha_{\mathcal{N}}\rangle_2 \cdots |\alpha_{\mathcal{N}}\rangle_m, \tag{25}$$

where $m = |K_s| / \log M$, and $\mathcal{N}$ is the number of code words.

Our target is to solve the following formula from known Helstrom-Holevo-Yuen formalism for quantum detection theory [15]:

$$\tilde{P}_e = \min \frac{1}{\mathcal{N}} \sum (1 - \langle \Psi_i | \Pi_i | \Psi_i \rangle),$$

or

$$\tilde{P}_d = 1 - \tilde{P}_e, \tag{26}$$

where $\{\Pi_i\}$ is detection operator or POVM (positive operator valued measure) which represents general quantum detection procedures, $|\Psi_i > \in H_s^{\otimes m}$ means a state of m length of M coherent states. This gives an evaluation of the decryption error.

As the first step, let us describe a physical decryption by the individual measurement. The detection operator can be constructed for each slot by so called square root measurement as follows [24–26]:

$$\Pi_i = |\mu_i\rangle\langle\mu_i|, \; |\mu_i\rangle = \hat{G}^{-1/2} |\alpha_i\rangle, \quad i = 1, 2, \ldots, M, \tag{27}$$

where

$$\hat{G} = \sum_i |\alpha_i\rangle\langle\alpha_i| \tag{28}$$

and where $\hat{G}$ is Gram operator, and its Gram matrix is given by

$$G=\begin{pmatrix}\langle\alpha_1|\alpha_1\rangle & \langle\alpha_1|\alpha_2\rangle & \langle\alpha_1|\alpha_3\rangle & \ldots \\ \langle\alpha_2|\alpha_1\rangle & \langle\alpha_2|\alpha_2\rangle & \ldots & \\ \langle\alpha_3|\alpha_1\rangle & \langle\alpha_3|\alpha_2\rangle & \ldots & \\ \vdots & & & \end{pmatrix}. \tag{29}$$

Let λ_i be eigenvalue of the Gram matrix. The correct detection probability is, in general, given by [24,25]

$$P_d=\frac{1}{M^2}\left|\sum\sqrt{\lambda_i}\right|^2. \tag{30}$$

The quantum gain comes from the cross term of eigenvalues in the above formula, for example, $\sqrt{\lambda_i\lambda_j}$. To calculate the eigenvalues of the Gram matrix with large size is difficult. However, we can simplify the eigenvalue problem when

$$|\kappa|^2=|\langle\alpha_{i+1}|\alpha_i\rangle|^2=e^{-2|\alpha|^2[1-\cos(\pi/M)]}\sim 1. \tag{31}$$

By numerical simulation, we have

$$P_d\sim 1-\frac{M-1}{M}|\kappa|^2,\quad |\kappa|^2\sim 1. \tag{32}$$

As a result, the detection probability of the code word is

$$\widetilde{P}_d\sim\left(1-\frac{M-1}{M}|\kappa|^2\right)^m. \tag{33}$$

This can be compared with $Q_1=\Gamma(|\kappa|)^m$ [see Eqs. (9) and (10)] as follows:

$$\widetilde{P}_d\sim\left(1-\frac{M-1}{M}|\kappa|\right)^m > Q_1^{-1}=\left(\frac{1}{\Gamma(|\kappa|)}\right)^m, \tag{34}$$

where $\Gamma(|\kappa|=1)=M$. The last term is the detection probability under the wedge approximation.

When we have QDM, in the above formula, the κ becomes

$$|\kappa|^2=e^{-2|\alpha|^2[1-\cos(\pi/M^2)]}\mapsto 1 \tag{35}$$

because of $\pi/M^2\sim 0$. Consequently, we have

$$\widetilde{P}_d\sim 2^{-|K_s|} \tag{36}$$

When Eve can get long data such as $l\times m$, the detection probability is

$$\widetilde{P}_{dl}=\sum\widetilde{P}_d=l\widetilde{P}_d. \tag{37}$$

Let us describe the case of the collective qumode measurement which may have a quantum gain in the quantum detection problems [27]. Performances and upper bounds of error probability of quantum code words is discussed in [28]. In this case, the Gram operator and the detection probability are given by

$$\hat{G}=\sum_i|\Psi_i\rangle\langle\Psi_i| \tag{38}$$

$$\widetilde{P}_d=\frac{1}{\mathcal{N}^2}\left|\sum_i\sqrt{\lambda_i}\right|^2 \tag{39}$$

An application of this scheme to the physical decryption has some difficulties. So we cannot give a result at present. However, in 2006, Nair gives a formula on upper bounding of the error probability in the case of known plaintext attack, applying a conceptual sequential decision processing on whole Hilbert space $H_s^{\otimes m}$ which can apply to any length of observed data [29].

2. Combination of DSR and QDM

If one cannot realize the ideal QDM which has $|\kappa|^2\mapsto 1$, one can apply a combination of DSR and QDM. The deliberate signal randomization (DSR) is an attractive method to enhance the security of Y00 protocol [1,17]. It requires some error correcting code to avoid the degradation of Bob's decoding process. The crucial point of the QDM is that it produces many regions on whole circle of phase plane which involve the full error on symbols for running key and mapping pattern (see Fig. 2). So even the quantum noise effect is small, Eve suffers the full error on symbols of running key and mapping patterns.

$$\begin{aligned}&\{K_i,\mathcal{L}_j\}\quad\forall\,(i,j)\mapsto\Delta\theta_m(1)\\&\{K_i,\mathcal{L}_j\}\quad\forall\,(i,j)\mapsto\Delta\theta_m(2)\\&\qquad\vdots\end{aligned} \tag{40}$$

In order to randomize the running key sequence against key correlations across data bits, we can employ DSR which cover $\Delta\theta_m$. Thus the advantage of this model is that one can use DSR to the periphery of the real signal, and there is no degradation in Bob's measurement. This is an important, because full DSR gives degradation for Bob as shown by numerical simulation [30]. By such a model, also we can expect both improvement of the wedge approximation and an essential improvement of the security.

The DSR in this case requires additional noise depending on true signal. Let $g(\theta_y|\theta_s)$ be the probability distribution of DSR. The effect of DSR is described as follows:

$$p(\theta_m|\theta_s)=\int p(\theta_m|\theta_y)g(\theta_y|\theta_s)d\theta_y\cong\frac{1}{\Delta\theta_m}, \tag{41}$$

where $p(\theta_m|\theta_y)$ is the probability distribution of the measured phase when the signal is θ_y. Then it is described as follows:

$$\theta_s=\theta_s(x,K_i,\mathcal{L}_j,r_k), \tag{42}$$

where the randomization r_k comes from DSR by random noise. If we employ DSR by Gaussian noise, each signal state is Gaussian mixed state as follows:

$$\rho_s=\int\int\mathcal{G}(\alpha_y|\alpha_s)|\alpha_y\rangle\langle\alpha_y|d\alpha_y\quad\forall\ s. \tag{43}$$

The signal set that Eve has to discriminate is Gaussian mixed states of $2^{|K_s|}$. When the signal state is Gaussian mixed state with a small signal to noise ratio, the quantum gain by the quantum optimum detection scheme in the collective and also individual quantum measurement becomes negligible and the optimum receiver becomes heterodyne receiver [31]. That is, when signal sets are pure states, the gain is the largest. So we do not need the full quantum analysis to get the error probability for this case. In general, the probability distribution of quadrature amplitude for the measurement of signal phases in the semi-classical analysis is Gaussian:

$$p(x_c,x_s:\theta_m|x_c,x_s:\theta_s) \sim \mathcal{G}(x_c,x_s:\theta_m|x_c,x_s:\theta_s). \tag{44}$$

Since we assume only the deliberation to cover a narrow range $\Delta\theta_m$, it does not affect the error performance of Bob. We can apply the formula of multiary by using heterodyne receiver and the result is

$$\tilde{P}_d \sim \left[1-\frac{M-1}{M}\mathrm{erfc}\left(\frac{|\alpha|\pi/M^2}{\sigma}\right)\right]^m, \tag{45}$$

where the part of $erfc(/)$ corresponds to the error probability between neighboring signals, and σ is the variance of the probability distribution of

$$p(x_c,x_s) = \mathrm{Tr}\rho_s\Pi(\text{heterodyne}) \tag{46}$$

and it is related to the DSR region driven by other noise source, and given by $\epsilon_q = |\alpha|\pi/M^2\sigma$. Thus one can easily have

$$\tilde{P}_d \sim 2^{-|K_s|}. \tag{47}$$

This suggests that this scheme may have the best security performance in the class of Y00 protocol consisting of high power laser and high speed LFSR. Here we have discussed only the case of individual qumode measurement. In the subsequent paper, we will discuss properties on collective qumode measurement.

V. CONCLUSION

We have discussed differences of the feature of security of the conventional ciphers and the Y00 protocol. In the case of the basic model of the Y00 protocol, one cannot attain the information theoretic security against ciphertext-only attack by only perfect random data (plain text), while it is done in the case of the conventional cipher. This seems a weakness, but it is not. Yuen has emphasized that even if the basic model of the Y00 protocol has such a feature, a general model of the Y00 protocol may provide security which cannot be attained by the conventional cipher in the sense of both complex-theoretic and information-theoretic security. This paper has provided concrete examples to show that the Y00 protocol indeed has the potential to greatly improve security beyond conventional cryptography.

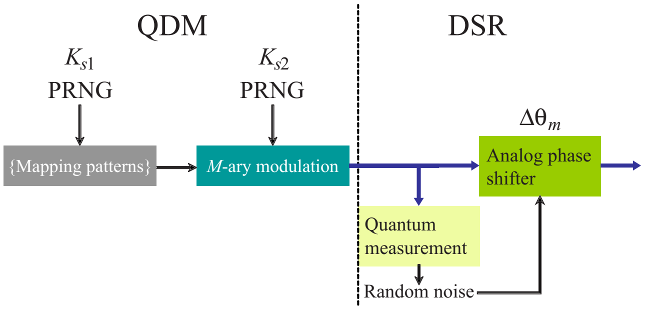

FIG. 3. (Color online) An experimental implementation system of the generalized quantum noise diffusion mapping. This is applicable to ASK when the shifter is replaced by amplitude modulation.

ACKNOWLEDGMENTS

We are grateful to K. Kato for discussions, to Hitachi Information and Communication Engineering, and Panasonic for experimental collaboration. This work was supported by National Institute of Information and Communications Technology under Grant No. NICT-11901.

APPENDIX (EXPERIMENTAL FEASIBILITY)

In order to realize DSR+ QDM model, we need a signal dependent random noise, because the diffusion region depends on the signal phase: θ_s. Here we show how to introduce DSR by random noise in practice. Figure 3 shows a concrete scheme of an implementation of the model. As shown in Fig. 3, one can obtain the high speed random noise by the measurement of a part of the transmitted light. This is one realization of the high speed random noise generation proposed by Yuen, and is also an application of quantum effects of the coherent state. The part of DSR in the system requires analog phase shift modulation for PSK and amplitude shift for IMDD without delay between noise generation and the data slot. Since the data rate of our system is 2.5 Gbit/s at present, and 10 Gbit/s at the next system, we need to check the feasibility of the analog modulation scheme by noise as described in Fig. 3. Our present experimental system of the Y00 protocol based on IMDD already has a DSR by LFSR with the same key length as LFSR for the running key [32]. So we have tried to exchange the LFSR for DSR to quantum noise obtained from the direct measurement of the coherent state transmitted from the transmitter in our IMDD scheme, and confirmed the feasibility of such a scheme at 2.5 Gbit/s. We still have difficulties for an implementation of a part of QDM, because we need a high speed modulator which can accept signals driven from the many mapping patterns. However, in the subsequent paper, we will report the detailed experimental results on the IMDD system with the combination of DSR by noise and QDM for a metropolitan network with 200 km long in a city.

[1] H. P. Yuen, e-print arXiv:quant-ph/0311061V6.

[2] G. A. Barbosa, E. Corndorf, P. Kumar, and H. P. Yuen, Phys. Rev. Lett. **90**, 227901 (2003).

[3] E. Corndorf, C. Liang, G. S. Kanter, P. Kumar, and H. P. Yuen, Phys. Rev. A **71**, 062326 (2005).

[4] O. Hirota, M. Sohma, M. Fuse, and K. Kato, Phys. Rev. A **72**, 022335 (2005).

[5] S. Akutsu, T. Hosoi, Y. Doi, M. Honda, and K. Harasawa, *Digest of QCMC-06* (NICT Press, Tsukuba, 2006).

[6] H. P. Yuen, R. Nair, E. Corndorf, G. K. Kanter, and P. Kumar, Quantum Inf. Comput. **8**, 561 (2006).

[7] R. Nair, H. P. Yuen, E. Corndorf, T. Eguchi, and P. Kumar, Phys. Rev. A **74**, 052309 (2006).

[8] N. T. Courtois, *Advances in Cryptography-CRYPT'2003* (Springer-Verlag, Berlin, 2003), pp. 176–194.

[9] J. C. Faugere, J. Pure Appl. Algebra **139**, 61 (1999).

[10] J. C. Faugere and G. Ars, Report of Institute National Research for Information and Automatic, INRIA Report RR-4739 (2003).

[11] W. Meier and O. Straffelbach, J. Cryptography **1**, 159 (1989).

[12] T. Johansson and F. Jonsson, *Advances in Cryptography-CRYPT'99* (Springer-Verlag, Berlin, 1999), pp. 181–197.

[13] S. Donnet, A. Thangaraj, M. Bloch, J. Cussey, J. M. Merolla, and L. Larger, Phys. Lett. A **356**, 406 (2006).

[14] O. Hirota and K. Kurosawa, Quantum Inf. Process. **6**, 81 (2007).

[15] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).

[16] O. Hirota, K. Kato, M. Sohma, and T. Usuda, *Proceedings of Quantum Communication and Imaging*, Proc. SPIE Vol. 5161 (SPIE, Bellingham, WA, 2003).

[17] H. P. Yuen and R. Nair, Phys. Lett. A **364**, 112 (2007).

[18] M. J. Mihaljevic, M. P. C. Fossorier, and H. Imai, *INDOCRYPT 2005, LNCS 3797* (Springer-Verlag, Berlin, 2005), pp. 155–168.

[19] B. Lohlein (unpublished).

[20] T. Siegenthaler, IEEE Trans. Comput. **34**, 81 (1985).

[21] R. Forre, *Advances in Cryptology, EUROCRYPT'89* (Springer-Verlag, Berlin, 1990), pp. 586–589.

[22] M. J. Mihaljevic, K. Imafuku, and H. Imai, *Proceedings of 2007 Symposium on Cryptography and Information Security* (IEICE of Japan, Nagasaki, 2007).

[23] J. H. Shapiro and S. R. Shepard, Phys. Rev. A **43**, 3795 (1991).

[24] M. Ban, K. Kurokawa, R. Momose, and O. Hirota, Int. J. Theor. Phys. **36**, 1269 (1997).

[25] M. Osaki, O. Hirota, and M. Ban, J. Mod. Opt. **45**, 269 (1998).

[26] K. Kato, M. Osaki, M. Sasaki, and O. Hirota, IEEE Trans. Commun. **47**, 248 (1999).

[27] M. Sasaki, K. Kato, M. Izutsu, and O. Hirota, Phys. Rev. A **58**, 146 (1998).

[28] O. Hirota, Appl. Algebra Eng. Commun. Comput. **10**, 401 (2000).

[29] R. Nair, Ph.D. thesis, Northwestern University, 2006 (unpublished).

[30] T. Usuda, *Proceedings of 1st Y00 Symposium* (Chuo Univ. Press, Tokyo, 2006).

[31] M. Sasaki, R. Momose, and O. Hirota, Phys. Rev. A **55**, 3222 (1997).

[32] K. Hosoi, K. Harasawa, M. Honda, S. Akutsu, Y. Kobayashi, and O. Hirota, *National Convention Record of IEICE of Japan*, Proceedings of General Conference of National Convention of IEICE Japan, B-10-80 (IEICE of Japan, Aichi, 2007).