ISSN 2186-6570

Quantum Random Cipher with Phase Mask Encryption

Masaki Sohma and Osamu Hirota

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

Tamagawa University Quantum ICT Research Institute Bulletin, Vol.2, No.1, 5-7, 2012

Vol.2 No.1 : 5-7 (2012)

Quantum Random Cipher with Phase Mask Encryption

Masaki Sohma
Quantum Information Science Research Center, Quantum ICT Research Institute, Tamagawa University
6-1-1 Tamagawa-gakuen, Machida, Tokyo 194-8610, Japan
E-mail: sohma@eng.tamagawa.ac.jp

***Abstract*—On the basis of fundamental idea of Yuen, we present a new type of quantum random cipher, where pulse position modulated signals are encrypted in the picture of quantum Gaussian wave form.** [1]

I. Introduction

The concept of quantum random cipher was proposed by H. P. Yuen and implemented through phase shift keying (PSK) modulation and intensity modulation (IM), which are called $\alpha\eta$ system or Y00 system. These systems enable us to realize high speed direct data transmission with security protected by physical phenomena. Moreover Yuen gave another implementation of quantum random cipher by using coherent pulse position modulation (CPPM) and shown that N-ary detection can overcome the limitation on the binary detection advantage of optimal quantum receiver for PSK or IM signal states [7]. In this paper we discuss phase mask encryption for CPPM according to Yuen's idea [10]. In Sect. II we give a description of coherent pulse position modulation in terms of quantum Gaussian waveform. In Sect. III we formulate phase mask encryption on the basis of the idea of canonical encryption.

II. Quantum random cipher with coherent pulse position modulation

A. Basic structure of quantum random cipher

We briefly explain a configuration of quantum random cipher (Fig. 1). Alice modulates her classical message ℓ to obtain a signal state ρ^ℓ. Then the signal state is transformed into an encrypted state $\tilde{\rho}^\ell$ by a unitary operator U_k, which is randomly chosen via a running key k generated by using PRNG on a secret key **K**. We assume the encrypted state $\tilde{\rho}^\ell$ is sent through the ideal channel. Since the secret key **K**, PRNG and map $k \to U_k$ are shared by Alice and Bob, Bob can apply the unitary operator $U_k^\dagger$ to the received state $\tilde{\rho}^\ell$ and obtains the signal state ρ^ℓ. Thus Bob can receive a classical message ℓ' with a very small error by applying the optimum detection to ρ^ℓ. In contrast, Eve does not know the secret key **K** and hence she must detect encrypted state $\tilde{\rho}^\ell$ directly. This makes Eve's error probability worse than Bob's one.

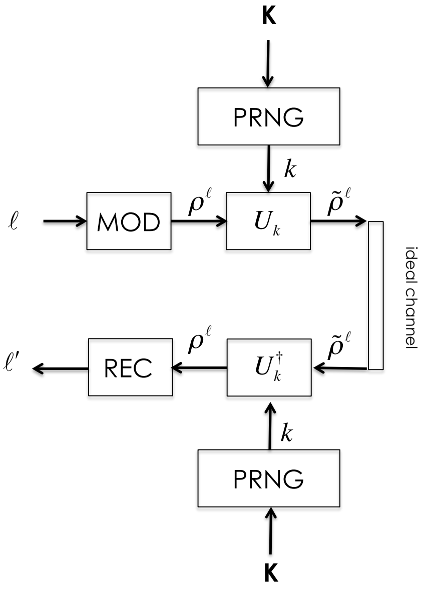

Fig. 1. configuration of quantum random cipher system

B. Coherent Pulse Position modulation

Alice uses the coherent pulse position modulation where classical information ℓ corresponds to the quantum signal

$$|\Phi_\ell\rangle = |0\rangle_1 \otimes \cdots \otimes |\sqrt{S}\rangle_\ell \otimes \cdots \otimes |0\rangle_N, \tag{1}$$

with a fixed positive real number S and $\ell = 1, ..., N$. Bob gets information from the signal by individual direct detection. Then the error probability of Bob is given as

$$P_{Bob} = (1 - 1/N)e^{-S}. \tag{2}$$

For example, $P_{Bob} \approx 10^{-9}$ for $S = 20$, $N >> 1$.

C. Quantum Gaussian Waveform

In order to describe the unitary operator in the section III, we summarize the description of the electromagnetic field generated by a signal source. Here, for simplicity, we use the Holevo's notations given in the section IV.4 [15]. Note that more realistic ones can be found in [11].

Let us consider the periodic operator-valued function

$$X(t) = \sum_j \sqrt{\frac{2\pi\hbar\omega_j}{T}} \left(a_j e^{-i\omega_j t} + a_j^\dagger e^{i\omega_j t} \right) \tag{3}$$

[1] This paper was revised in April 2014.

where $[0,T]$ is the observation interval and $\omega_j = 2\pi j/T$. We assume the mode a_j is described by the Gaussian states $\rho_j(\alpha_j)$ with the first two moments given by

$$\begin{aligned} \mathrm{Tr}\rho_j(\alpha_j)a_j &= \alpha_j, & (4)\\ \mathrm{Tr}\rho_j(\alpha_j)a_j^\dagger a_j &= N_j + |\alpha_j|^2. & (5)\end{aligned}$$

Then the whole process $X(t)$ is characterized by the product Gaussian states $\rho_\alpha = \otimes_j \rho_j(\alpha_j)$, such that

$$\mathrm{Tr}\rho_\alpha X(t) = \alpha(t) \tag{6}$$

$$\begin{aligned} \mathrm{Tr}\rho_\alpha \frac{1}{4\pi}\int_0^T X(t)^2 dt =& \sum_j \hbar\omega_j(N_j + \frac{1}{2}) \\ &+ \frac{1}{4\pi}\int_0^T \alpha(t)^2 dt. \end{aligned} \tag{7}$$

Here $\alpha(t)$ is a classical signal for quantum Gaussian channel,

$$\alpha(t) = \sum_j \sqrt{\frac{2\pi\hbar\omega_j}{T}}(\alpha_j e^{-i\omega_j t} + \bar{\alpha}_j e^{i\omega_j t}), \tag{8}$$

where $\bar{\alpha}_j$ is a complex conjugate of α_j. Now let us rewrite the CPPM quantum signal $|\Phi_\ell\rangle$ by using the representation of quantum Gaussian waveform. The classical signal corresponding to $|\Phi_\ell\rangle$ is given by

$$\alpha^\ell(t) = \alpha_c(t)\chi_{I_\ell}(t) \tag{9}$$

where

$$\alpha_c(t) = \sqrt{NS}K_c e^{-i\omega_c t} + c.c., \tag{10}$$

$$\chi_{I_\ell}(t) = \left\{ \begin{array}{ll} 1 & t \in I_\ell \\ 0 & t \in [0,T] \setminus I_\ell \end{array} \right. , \tag{11}$$

$K_c = \sqrt{2\pi\hbar\omega_c/T}$, ω_c is a carrier frequency and $I_\ell = [(\ell-1)T/N, \ell T/N]$. Then Gaussian state corresponding to the classical signal $\alpha^\ell(t)$ is given by

$$\rho^\ell = \otimes_j \rho_j(\alpha_j^\ell), \quad \rho_j(\alpha_j^\ell) = |\alpha_j^\ell\rangle\langle\alpha_j^\ell|, \tag{12}$$

where we obtain the values of α_j^ℓ from the Fourier series expansion of $\alpha^\ell(t)$:

$$\alpha^\ell(t) = \sum_j \sqrt{\frac{2\pi\hbar\omega_j}{T}}\left(\alpha_j^\ell e^{-i\omega_j t} + \bar{\alpha}_j^\ell e^{i\omega_j t}\right). \tag{13}$$

Here, from the relation

$$\alpha^\ell(t) = \alpha^1(t - \frac{\ell-1}{N}T), \quad \ell = 1, ..., N, \tag{14}$$

we have

$$\alpha_j^\ell = \alpha_j^1 e^{i\omega_j(\ell-1)T/N} = \alpha_j^1 e^{i2\pi j(\ell-1)/N}. \tag{15}$$

III. Canonical Encryption

A. General Definition of Gaussian States

We consider the Weyl operator

$$V(z) = \exp i\sum_{j\in J}(z_j^q q_j + z_j^p p_j), \tag{16}$$

where z is a real vector with the elements z_j^q, z_j^p, $j \in J = \{j; \omega_j \in V_{\omega_c}\} = \{j_1, ..., j_M\}$ and

$$\begin{aligned} q_j &= \sqrt{\hbar/2\omega_j}(a_j + a_j^\dagger) \\ p_j &= i\sqrt{\hbar\omega_j/2}(a_j^\dagger - a_j). \end{aligned} \tag{17}$$

The density operator ρ is called Gaussian if its quantum characteristic function has the form

$$\mathrm{Tr}\rho V(z) = \exp\left[im^T z - \frac{1}{2}z^T A z\right], \tag{18}$$

with mean vector m and correlation matrix A. In particular, the Gaussian state ρ_ℓ given by Eq. (12) has the mean vector:

$$m = \Omega_M(x_{j_1}, y_{j_1}, ..., x_{j_M}, y_{j_M})^T \tag{19}$$

with $\alpha_j = x_j + iy_j$ and

$$\Omega_M = \oplus_{m=1}^M \left[\begin{array}{cc} \sqrt{2\hbar/\omega_{j_m}} & 0 \\ 0 & \sqrt{2\hbar\omega_{j_m}} \end{array}\right], \tag{20}$$

and the correlation matrix:

$$A_M = \oplus_{m=1}^M \left[\begin{array}{cc} \hbar/2\omega_{j_m} & 0 \\ 0 & \hbar\omega_{j_m}/2 \end{array}\right] = \frac{1}{4}\Omega_M^2. \tag{21}$$

B. Symplectic Transformation

The transformation $L : \mathbb{R}^{2M} \to \mathbb{R}^{2M}$ is called symplectic, when the corresponding Weyl operator $\tilde{V}(z) = V(L^T z)$ satisfies

$$\tilde{V}(z)\tilde{V}(z') = \exp\left[\frac{i}{2}\Delta(z,z')\right]\tilde{V}(z+z') \tag{22}$$

with $\Delta(z,z') = \hbar\sum_{j\in J}(z_j'^q z_j^p - z_j^q z_j'^p)$ We denote the totality of symplectic transformation by $\mathrm{Sp}(M,\mathbb{R})$. It follows from Stone-von Neumann theorem that there exists the unitary operator U satisfying

$$V(L^T z) = U^\dagger V(z) U \tag{23}$$

for any $L \in \mathrm{Sp}(M,\mathbb{R})$. We call such derived operator U the *unitary operator associated with symplectic transformation* L. Then the characteristic function of $\tilde{\rho}^\ell = U\rho^\ell U^\dagger$ is given by

$$\begin{aligned} \tilde{\phi}(z) =& \mathrm{Tr}\tilde{\rho}^\ell V(z) = \mathrm{Tr}\rho^\ell U^\dagger V(z) U \\ =& \mathrm{Tr}\rho^\ell V(L^T z) = \exp\left[i(Lm)^T z - \frac{1}{2}z^T L A_M L^T z\right] \end{aligned} \tag{24}$$

Our interest is devoted to the case where the state $\tilde{\rho}^\ell$ has the form of $\otimes_{j\in J}|\tilde{\alpha}_j^\ell\rangle\langle\tilde{\alpha}_j^\ell|$. Then the symplectic transformation should satisfy the condition $LA_ML^T = A_M$, which means

$$\Omega_M^{-1}L\Omega_M(\Omega_M^{-1}L\Omega_M)^T = I_{2M} \tag{25}$$

i.e.

$$\Omega_M^{-1}L\Omega_M \in \mathrm{O}(2M)\cap\mathrm{Sp}(M,\mathbb{R})\cong\mathrm{U}(M) \tag{26}$$

where $\mathrm{U}(M)$ denotes the totality of $M\times M$ unitary matrices, and $\mathrm{O}(2M)$ the totality of $2M\times 2M$ orthogonal matrices.

C. Canonical Encryption

In the canonical encryption, we encrypt the message using unitary operator U_k associated with L_k satisfying Eq. (26). In the isomorphism $\mathrm{O}(2M)\cap\mathrm{Sp}(M,\mathbb{R})\cong\mathrm{U}(M)$, an element of $\mathrm{O}(2M)\cap\mathrm{Sp}(M,\mathbb{R})$,

$$\begin{pmatrix} r_{11}R(\theta_{11}) & \cdots & r_{1M}R(\theta_{1M}) \\ \vdots & \ddots & \vdots \\ r_{M1}R(\theta_{M1}) & \cdots & r_{MM}R(\theta_{MM}) \end{pmatrix}, \tag{27}$$

corresponds to

$$\begin{pmatrix} r_{11}e^{i\theta_{11}} & \cdots & r_{1M}e^{\theta_{1M}} \\ \vdots & \ddots & \vdots \\ r_{M1}e^{i\theta_{M1}} & \cdots & r_{MM}e^{\theta_{MM}} \end{pmatrix} \in \mathrm{U}(M). \tag{28}$$

with $r_{i,j}\in\mathbb{R}$ and $R(\theta_{jk})$ is a rotation matrix. We denote the unitary matrix corresponding to $\Omega_M^{-1}L_k\Omega_M$ by U_k . Then we can find the Gaussian state $\rho^\ell = \otimes_{j\in J}\rho_j(\alpha_j^\ell)$ is encrypted into

$$\tilde{\rho}^\ell = \otimes_{j\in J}\rho_j(\beta_j^\ell) \tag{29}$$

with

$$(\beta_{j_1}^\ell, ..., \beta_{j_M}^\ell)^T = U_{L_k}(\alpha_{j_1}^\ell, ..., \alpha_{j_M}^\ell)^T. \tag{30}$$

We consider a phase mask encryption as an example of the canonical encryption. If $r_{ij}=\delta_{ij}$ holds for $i,j=1,...,M$ in Eq. (28), the cannonical encryption is called a *phase mask encryption* and the matrix (28) is denoted by $U(\theta_{11},...,\theta_{NN})$. The phase mask encryption can be realized by the liquid crystal modulator (LCM) or the acousto-optic modulator (AOM). We assume N is a prime number. Then in the right-hand side of Eq. (15), we have

$$\{e^{i2\pi j_m(\ell-1)/N}; \ell=1,...,N\} = \{e^{i2\pi n/N}; n=1,...,N\}, \tag{31}$$

if the value of j_m is not divisible by N. So it is natural to consider the phase mask encryption given by

$$U_{L_k} = U(2\pi k_1/N', ..., 2\pi k_M/N'), \tag{32}$$

where N' is a multiple of N and $k=(k_1,...,k_M)$ with $0\le k_m < N'$ is a key generated from PRNG. Then each $\beta_{j_m}^\ell$ in Eq. (30) takes values of the form

$$\alpha_{j_m}^1 e^{i2\pi n'/N'}, \quad n'=1,...,N'. \tag{33}$$

IV. Discussions

Let us consider the inequality

$$H(X_n|KY_n^E) > H(X_n|KY_n^B), \tag{34}$$

where X_n is a random variable for plaintext, Y_n^E is a random variable for Eve's ciphertext obtained from the measurement without the secret key $\mathbf{K}$ and Y_n^B is a random variable for Bob's ciphertext obtained from the measurement with the secret key $\mathbf{K}$. If the inequality (34) holds, we can say that the cipher exceeds the Shannon limit [3]. In this setting Eve may use not only the ciphertext Y_n^E but also the secret key $\mathbf{K}$ in order to estimate X_n. The security considered in such a situation is called everlasting security [3]. Our random cipher is expected to achieve it. In future work we will show this through detailed evaluation of Eve's error probability.

References

[1] O.Hirota, M.Sohma, M.Fuse, and K.Kato, *Physical Review A vol-72*, 022335 (2005)

[2] O.Hirota, *Physical Review A, vol-76*, 032307 (2007)

[3] O.Hirota, *The 29th Symposium on Cryptography and Information Security* (2012)

[4] H.P.Yuen, *arxiv.org:quant-ph*, 0322062 (2003)

[5] G.A.Borbosa, E.Corndorf, G.S.Kanter, P.Kumar, and H.P.Yuen, *Physical Review Letters, vol-90*, 227901 (2003)

[6] R.Nair and H.P.Yuen, *Physics Letters A, vol-372*, p7091 (2008)

[7] H. P. Yuen, *IEEE. J. Selected topics in Quantum Electronics, vol.15*, no.6,pp. 1630-1645 (2009)

[8] H.P.Yuen,R.Nair, E.Corndorf, G.S.Kanter, and P.Kumar, *Quantum Information and Computation, vol-8*, p561 (2006)

[9] H. P. Yuen, J. H. Shapiro, *IEEE Trans. on Information Theory, vol. IT-26, no.1*, pp. 78-92 (1980)

[10] H. P. Yuen, *Quantum Cryptography QKD and KCQ*, presented at Tamagawa University, Japan, June 15th (2011)

[11] H. P. Yuen, J. H. Shapiro, *IEEE Trans. on Information Theory, vol. IT-24, no.6*, pp. 657-668 (1978)

[12] R.Nair, H.P.Yuen, E.Corndorf, T.Eguchi, and P.Kumar, *Physical Review A, vol-74*, p052309 (2006)

[13] H. Yuen, R. Kennedy, M. Lax, *IEEE Trans.Information Theory, vol-IT21*, pp.125-134 (1975)

[14] A. S. Holevo. *Probabilistic and Statistical Aspect of Quantum Theory*, North-Holland (1982)

[15] A. S. Holevo. *Tamagawa University Research Review, vol.4* (1998)

[16] C.E.Shannon *Bell system technical Journal, vol-28* , pp656-715 (1949)

[17] R. G. Gallager *Information Theory and Reliable Communication*, John Wiley & Sons (1968)