Journal of Lasers, Optics & Photonics
ISSN: 2469-410X

Hirota, J Laser Opt Photonics 2016, 3:1
DOI: 10.4172/2469-410X.1000129

Research Article Open Access

Importance and Applications of Infinite Dimensional Non-Orthogonal Quantum State

Osamu Hirota*

Quantum ICT Research Institute, Tamagawa University, Tokyo, Japan

Abstract

This paper introduces remarkable achievement in theory on non-orthogonal state in quantum optics that can describe macroscopic quantum effect, and gives a survey of theorems in quantum information science based on non-orthogonal state. Then it is shown that these provide potential applications to Quantum Methodology such as quantum reading, quantum imaging and to Quantum Enigma Cipher which is a general model of physical cipher.

Keywords: 03.67.Dd; 42.50.Lc; Entangled coherent state; Quantum illumination; Quantum reading; Quantum imaging; Quantum Enigma cipher

Introduction

Non-orthogonal quantum states in infinite dimensional space are playing a special role in foundation of quantum mechanics. For example, the Gaussian state is a typical state that was considered at beginning of history of quantum theory. The explicit importance of Gaussian quantum states such as coherent state was certified by Glauber [1], Sudarshan et al. [2] in quantum optics for understanding a nature of laser. More progress has been given by Yuen [3] who discovered a special properties of generalized coherent state known as two-photon coherent state (squeezed state), and a method to verify them experimentally, and its applications were opened up by Hirota [4] and Shapiro [5]. Then entanglement of non-orthogonal quantum state such as two-mode squeezed state and quasi-Bell entangled coherent state [6] stimulate another interesting subject in physics.

On the other hand, many fundamental theorems in quantum information science were developed based on non-orthogonal quantum state. In fact, a problem of discrimination of non-orthogonal quantum states through quantum measurement, that was pioneered by Helstrom [7], is a typical example. To formulate quantum communication theory, several researchers generalized from Bayes criterion to Neyman-Peason , Minimax criteria, and Shannon mutual information which play different roles in each other. Thus, theory of non-orthogonal state is a foundation for quantum information science.

In this paper, I describe a survey of theory of non-orthogonal quantum state in the sections II and III, and discuss a generation method for such states including entangled coherent state and Schrodinger cat state in the section IV.

Then progress of a basic theory for quantum information science such as quantum communication theory is introduced. In the section VI, I discuss potential applications of theoretical achievements on non-orthogonal quantum state to Quantum Methodology such as quantum illumination, quantum reading and quantum imaging. These performances in a real situation may be drastically improved by entangled state based on infinite dimensional state. Furthermore, it will be suggested for future works that quantum imaging has a potential of a real application for a new type of camera by connecting the original theory and Volterra-Wiener theory. In the section VII, the concept of a new physical cipher so called Quantum Enigma Cipher is described, in which the security is ensured by a combination of a mathematical encryption and physical randomization of its ciphertext.

Basis of Quantum Optics

Quantum optical field

Glauber unified a formulation on classical and quantum optical field that is described by

$$\nabla^2 E(r,t) = \frac{1}{c^2}\frac{d^2 E(r,t)}{dr^2} \quad (1)$$

where the electric field is given by

$$E(r,t) = i\sum_k \left(\frac{\hbar\omega_k}{4\pi\varepsilon_0}\right)^{1/2}[a_k u_k(r)e^{-i\omega_k} - a_k^{\dagger} u_k(r)e^{i\omega_k}] \quad (2)$$

Here uk (r) is mode function. This mode is called Q-mode which corresponds to infinite dimensional Hilbert space H_S. Observables in the mode are described by photon annihilation and creation operators as follows:

$$a = (X_C + iX_S)$$

$$a^{\dagger} = (X_C - iX_S) \quad (3)$$

where $[a_k, a_{k'}^{\dagger}] = \delta_{k,k'}$.

The quantum state is a vector in the space H_S.

$$|\Psi> \in H_S$$

$$|||\Psi>|| = 1 \quad (4)$$

where whole state vectors are normalized.

Basic states of Q-mode

Since Q-mode means an infinite dimensional Hilbert space, the state vector is represented by a linear superposition of orthonormal vector such as Fock state |n>. The representative state is a coherent state which was discussed by Glauber [1] to explain coherence property of laser light. Then coherent state is given

$$a\,|\alpha> = \alpha\,|\alpha>$$

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

Received May 07, 2016; **Accepted** May 17, 2016; **Published** May 19, 2016

Citation: Hirota O (2016) Importance and Applications of Infinite Dimensional Non-Orthogonal Quantum State. J Laser Opt Photonics 3: 129. doi:10.4172/2469-410X.1000129

$$|\alpha>=\sum_n \frac{\alpha^n}{n!} e^{-|\alpha|^2/2}|n> \quad (5)$$

where

$$\alpha =<\alpha|a|\alpha>=<X_c>+i<X_s>$$

$$|\alpha|^2=<n>=<\alpha|a^\dagger a|\alpha> \quad (6)$$

The coherent state is a typical example of the non-orthogonal state in Q-mode as follows:

$$<\alpha_1|\alpha_2>=exp(-\frac{1}{2}|\alpha_1|^2-\frac{1}{2}|\alpha_1|^2+\alpha_1^*\alpha_2) \quad (7)$$

This provides the over completeness in the space such as

$$\frac{1}{\pi}\int|\alpha><\alpha|d^2\alpha = I \quad (8)$$

Where I is the identity operator on H_s. Another example of the basic state is so called Two-photon coherent state (Squeezed state) [3,8]. Let us define the following operator $b \quad \mu a \quad \nu a^\dagger$, $|\mu|^2-|\nu|^2=1$. Then two-photon coherent state is given

$$b|\beta>_g=\beta|\beta>_g \quad (9)$$

$$|\beta>_g=\sum_n \frac{1}{\sqrt{n!\mu}}(\frac{\nu}{2\mu})^{n/2}H_n(\frac{\beta}{\sqrt{\mu\nu}})e^{(-\frac{1}{2}|\beta|^2+\frac{\nu^*}{2\mu}\beta^2)}|n> \quad (10)$$

where

$$\beta =<\alpha|b|\alpha>=\mu\alpha+\nu\alpha^*$$

$$\alpha=\mu\beta-\nu\beta^* \quad (11)$$

and this is non-orthogonal state as follows:

$${}_g<\beta_1|\beta_2>_g\neq 0 \quad (12)$$

In addition, it also provides over completeness

$$\frac{1}{\pi}\int|\beta>_g<\beta|d^2\beta = I \quad (13)$$

where I is the identity operator.

Glauber-Sudarshan representation

The Galuber-Sudarshan representation is for describing the phase space distribution of a quantum system in the phase space formulation. It provides useful applications in laser theory and especially coherence theory, and given as follows [1,2]:

$$\rho_{GS}=\int P(\alpha)|\alpha><\alpha|d^2\alpha$$

$$\Xi(\lambda)=\int<\alpha|e^{\lambda a^\dagger-\lambda^* a}|\alpha>P(\alpha)d^2\alpha \quad (14)$$

First order mutual coherence function is defined as follows:

$$G^1(r_1,r_2,\tau)=Tr\{\rho_{GS}E^\dagger(r_1,t_1)E(r_2,t_2)\} \quad (15)$$

Higher order mutual coherence function can also be defined. Here we give the second order mutual coherence function.

$$G^2(r_1,r_2,\tau)$$

$$=Tr\{\rho_{GS}E^\dagger(r_1,t_1)E^\dagger(r_2,t_2)E(r_2,t_2)E(r_1,t_1)\} \quad (16)$$

In the subsequent sections, I will provide useful applications of the above theories.

Entanglement of Q-mode

Basis of entanglement

Entanglement and its information-theoretic aspects have been studied by many authors [9-13]. Here I give a short survey of the theory of entanglement that I will later apply to quasi-Bell states. For a pure entangled state of a bipartite system $|\Psi\rangle_{AB}$, the measure of entanglement defined as [9,14]:

$$E_n(|\Psi\rangle_{AB})=-\mathrm{Tr}\rho_A\log\rho_A, \quad \rho_A=\mathrm{Tr}_B|\Psi\rangle_{AB}\langle\Psi|, \quad (17)$$

is called "entropy of entanglement". This quantity enjoys two kinds of information-theoretic interpretations. One is that $E_n()$ gives the entanglement of formation, which is defined as the asymptotic number k of standard singlet states required to faithfully locally prepare n identical copies of a system in the bipartite state $|\Psi\rangle_{AB}$ for very large k and n. The other is that $E_n()$ gives the amount of distillable entanglement, which is the asymptotic number of singlets k that can be distilled from n identical copies of $|\Psi\rangle_{AB}$. With either of these definitions of k and n, $E_n()$ satisfies

$$\lim_{n,k\to\infty}\frac{k}{n}=E_n(|\Psi\rangle_{AB}). \quad (18)$$

For pure states we can rewrite

$$E_n(|\Psi\rangle_{AB})=H\left(\frac{1}{2}(1+\sqrt{1-C(|\Psi\rangle_{AB})^2})\right) \quad (19)$$

where H(x)=−x log x−(1−x) log(1−x) is the binary entropy function and $C(|\Psi\rangle_{AB})$ is "concurrence" defined by $C(|\Psi\rangle_{AB})=|_{AB}\langle\Psi|\tilde{\Psi}\rangle_{AB}|$ with $|\tilde{\Psi}\rangle_{AB}=\sigma|\Psi\rangle^*_{AB}$. The above expression is valid for mixed states of two qubit systems as well [12]. For mixed states of qubits one may also define an expression for the entanglement of formation [9,12,13]. It is defined as the average entanglement of the pure states of a decomposition $\rho=\sum_i p_i|\psi\rangle_i\langle\psi_i|$ of the density operator ρ, minimized over all decompositions [9].

$$E_n(\rho)=\min\sum_i p_i E_n(|\psi_i\rangle). \quad (20)$$

In general, it is difficult to find the exact amount of entanglement of formation except for special cases. However, there is a lower bound which is expressed in terms of a quantity called "fully entangled fraction", which we denote by $f_{(\rho)}$ and is defined as

$$f(\rho)=\max\langle e|\rho|e\rangle, \quad (21)$$

where the maximum is over all completely entangled states $|e\rangle$. A lower bound on the entanglement of formation is [9]

$$E_n(\rho)\geq h[f(\rho)], \quad (22)$$

where

$$h[f(\rho)]=\begin{cases} H[\frac{1}{2}+\sqrt{f(1-f)}] & (f\geq\frac{1}{2}) \\ 0 & (f<\frac{1}{2}) \end{cases} \quad (23)$$

Usually in order to construct entangled states one writes superpositions of orthogonal states. For instance the standard Bell basis uses states like $|\updownarrow\rangle$ and $|\leftrightarrow\rangle$, and of course its properties are well known. Our concern here is what kind of properties appear if we have superpositions of non-orthogonal states. In the following, I will clarify properties of entangled states of non-orthogonal states such as coherent states based on the above basic theory.

Entanglement of orthogonal states

Let us assume that two states |+>,|−> are orthogonal each other such as <+|−>=0. One can form the following entangled states so called Bell state.

$$\begin{cases} |\Psi_1\rangle_{AB} &= \frac{1}{2}(|+\rangle_A|-\rangle_B+|-\rangle_A|+\rangle_B) \\ |\Psi_2\rangle_{AB} &= \frac{1}{2}(|+\rangle_A|-\rangle_B-|-\rangle_A|+\rangle_B) \\ |\Psi_3\rangle_{AB} &= \frac{1}{2}(|+\rangle_A|+\rangle_B+|-\rangle_A|-\rangle_B) \\ |\Psi_4\rangle_{AB} &= \frac{1}{2}(|+\rangle_A|+\rangle_B-|-\rangle_A|-\rangle_B) \end{cases} \quad (24)$$

Entangled state of non-orthogonal states

Let us consider entangled states based on two non-orthogonal states $|\psi_1\rangle$ and $|\psi_2\rangle$ such that $\langle\psi_1|\psi_2\rangle=\kappa$ where k is real. We can define a set of 4 entangled states as follows [7]:

$$\begin{cases} |\Psi_1\rangle_{AB} &= h_1(|\psi_1\rangle_A|\psi_2\rangle_B+|\psi_2\rangle_A|\psi_1\rangle_B) \\ |\Psi_2\rangle_{AB} &= h_2(|\psi_1\rangle_A|\psi_2\rangle_B-|\psi_2\rangle_A|\psi_1\rangle_B) \\ |\Psi_3\rangle_{AB} &= h_3(|\psi_1\rangle_A|\psi_1\rangle_B+|\psi_2\rangle_A|\psi_2\rangle_B) \\ |\Psi_4\rangle_{AB} &= h_4(|\psi_1\rangle_A|\psi_1\rangle_B-|\psi_2\rangle_A|\psi_2\rangle_B) \end{cases} \quad (25)$$

where $\{h_i\}$ are normalization constants: $h_1=h_3=1/\sqrt{2(1+\kappa^2)}$, $h_2=h_4=1/\sqrt{2(1-\kappa^2)}$. We call these states "quasi-Bell states". They are not orthogonal each other. In fact, for κ real their Gram matrix $G_{ij}=|_{AB}\langle\Psi_i|\Psi_j\rangle_{AB}|$ becomes

$$G=\begin{pmatrix} 1 & 0 & D & 0 \\ 0 & 1 & 0 & 0 \\ D & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad (26)$$

where D=2k/(1+k2). If the basic states are orthogonal (k=0), then these states reduce to standard Bell states. Let us discuss the entropy of entanglement for the above states. We first calculate the reduced density operators of the quasi-Bell states. They are $\rho_A^{(1)}=\rho_A^{(3)}$ and $\rho_A^{(2)}=\rho_A^{(4)}$ with

$$\rho_A^{(1)}=\frac{1}{2(1+\kappa^2)}\{|\psi_1\rangle_A\langle\psi_1| \quad (27)$$

$$+\kappa|\psi_1\rangle_A\langle\psi_2|+\kappa|\psi_2\rangle_A\langle\psi_1|+|\psi_2\rangle_A\langle\psi_2\},$$

$$\rho_A^{(2)}=\frac{1}{2(1-\kappa^2)}\{|\psi_1\rangle_A\langle\psi_1| \quad (28)$$

$$-\kappa|\psi_1\rangle_A\langle\psi_2|-\kappa|\psi_2\rangle_A\langle\psi_1|+|\psi_2\rangle_A\langle\psi_2|\}.$$

The eigenvalues of the above density operators $\rho_A^{(1)}$ (or $\rho_A^{(3)}$) are given in terms of the Gram matrix elements G_{ij} as follows,

$$\lambda_{1/1}=\frac{1+G_{13}}{2}=\frac{(1+\kappa)^2}{2(1+\kappa^2)}, \quad (29)$$

$$\lambda_{2/1}=\frac{1-G_{13}}{2}=\frac{(1-\kappa)^2}{2(1+\kappa^2)},$$

and for $\rho_A^{(2)}$ (or $\rho_A^{(4)}$) we have

$$\lambda_{1/2}=\frac{1+G_{24}}{2}=\frac{1}{2}, \quad \lambda_{2/2}=\frac{1-G_{24}}{2}=\frac{1}{2}. \quad (30)$$

Hence, the entropy of entanglement is

$$E(|\Psi_1\rangle_{AB})=E(|\Psi_3\rangle_{AB}) \quad (31)$$

$$=-\frac{1+D}{2}\log\frac{1+D}{2}-\frac{1-D}{2}\log\frac{1-D}{2},$$

and

$$E(|\Psi_2\rangle_{AB})=E(|\Psi_4\rangle_{AB})=1, \quad (32)$$

Because G_{13}=D, and G_{24}=0. Thus $|\Psi_2\rangle_{AB}$ and $|\Psi_4\rangle_{AB}$ are maximally entangled, even though the entangled states consist of non-orthogonal states in each subsystem. So, these states are called H-state:

$$|\Psi_2\rangle_{AB}=|H_1\rangle=h_2(|\psi_1\rangle_A|\psi_2\rangle_B-|\psi_2\rangle_A|\psi_1\rangle_B)$$

$$|\Psi_4\rangle_{AB}=|H_2\rangle=h_4(|\psi_1\rangle_A|\psi_1\rangle_B-|\psi_2\rangle_A|\psi_2\rangle_B) \quad (33)$$

These results are true for arbitrary non-orthogonal states with $\langle\psi_1|\psi_2\rangle=\langle\psi_2|\psi_1\rangle=\kappa$ and do not depend on the physical dimension of the systems.

Quasi-Bell states based on bosonic coherent states

Let us consider two coherent states of a bosonic mode $\{|\alpha\rangle,|-\alpha\rangle\}$, e.g., let $\pm\alpha$ be the coherent amplitude of a light field. Using previous notation, we have $\kappa=\langle\alpha|-\alpha\rangle=\exp\{-2|\alpha|^2\}$.

Tombesi et al. [15]and Sanders [16] discussed properties of the following entangled state:

$$|\Psi_1\rangle_{AB}=h(|\alpha\rangle_A|\beta\rangle_B+|\gamma\rangle_A|\delta\rangle_B) \quad (34)$$

where $|\alpha\rangle,|\beta\rangle,|\gamma\rangle,|\delta\rangle$ are coherent states, and h is a normalization constant. This is called entangled coherent state. Here we apply the previous discussion to entangled coherent state. Then one can construct the quasi Bell entangled coherent states as follows [7]:

$$\begin{cases} |\Psi_1(\alpha)\rangle_{AB} &= h_1(|\alpha\rangle_A|-\alpha\rangle_B+|-\alpha\rangle_A|\alpha\rangle_B) \\ |\Psi_2(\alpha)\rangle_{AB} &= h_2(|\alpha\rangle_A|-\alpha\rangle_B-|-\alpha\rangle_A|\alpha\rangle_B) \\ |\Psi_3(\alpha)\rangle_{AB} &= h_3(|\alpha\rangle_A|\alpha\rangle_B+|-\alpha\rangle_A|-\alpha\rangle_B) \\ |\Psi_4(\alpha)\rangle_{AB} &= h_4(|\alpha\rangle_A|\alpha\rangle_B-|-\alpha\rangle_A|-\alpha\rangle_B) \end{cases} \quad (35)$$

Here we have that $|\Psi_2\rangle_{AB}$ and $|\Psi_4\rangle_{AB}$ provide one e-bit of entanglement independent of α and these are H-state.

$$|\Psi_2(\alpha)\rangle_{AB}=|H_1>$$

$$|\Psi_4(\alpha)\rangle_{AB}=|H_2> \quad (36)$$

On the other hand, $|\Psi_1(\alpha)\rangle_{AB}$ and $|\Psi_3(\alpha)\rangle_{AB}$ are maximally entangled states only in the limit α→∞.

The average photon numbers of the reduced states of the quasi Bell entangled coherent states read

$$\langle n_A^{(1)}\rangle=\frac{(1-\kappa^2)}{(1+\kappa^2)}|\alpha|^2, \quad \langle n_A^{(2)}\rangle=\frac{(1+\kappa^2)}{(1-\kappa^2)}|\alpha|^2. \quad (37)$$

This is shown in the following way. The characteristic functions of the quasi Bell entangled coherent states are given by

$$C(\xi,\eta)=\mathrm{Tr}[|\Psi\rangle_{AB}\langle\Psi|\exp(\xi a_A^\dagger)\exp(-\xi^* a_A)$$

$$\times\exp(\eta a_B^\dagger)\exp(-\eta^* a_B)]$$

$$\times\exp\{-(|\xi|^2+|\eta|^2)/2\} \quad (38)$$

They can be calculated, with the result

$$C(\xi,\eta|i=1,2)=$$

$$h_i^2\exp\{-(|\xi|^2+|\eta|^2)/2\}\{\exp(A_1-B_1)\alpha$$

$$+\exp(-A_1+B_1)\alpha\pm\exp(A_2-B_2)\alpha$$

$$\pm\exp(-A_2+B_2)\alpha\} \quad (39)$$

$$C(\xi,\eta|i=3,4)=$$

$$h_i^2\exp\{-(|\xi|^2+|\eta|^2)/2\}\{\exp(A_1+B_1)\alpha$$

$$+\exp(-A_1-B_1)\alpha \pm \exp(A_2+B_2)\alpha$$

$$\pm \exp(-A_2-B_2)\alpha\} \quad (40)$$

where $A_1=(\xi-\xi^*), A_2=(\xi+\xi^*), B_1=(\eta-\eta^*), B_2=(\eta+\eta^*)$. The characteristic functions are indeed not Gaussian.

Mixtures of quasi Bell entangled coherent states

We can construct a quasi-Werner mixed state based on quasi-Bell states by

$$W=F|\Psi_2\rangle_{AB}\langle\Psi_2| \quad (41)$$
$$+\frac{1-F}{3}\{|\Psi_1\rangle_{AB}\langle\Psi_1|+|\Psi_3\rangle_{AB}\langle\Psi_3|+|\Psi_4\rangle_{AB}\langle\Psi_4|\},$$

where 0≤F≤1. If $|\Psi_1\rangle_{AB}$, $|\Psi_2\rangle_{AB}$, $|\Psi_3\rangle_{AB}$, $|\Psi_4\rangle_{AB}$ are Bell states, then the above equation gives a standard Werner state [17]. It is known that the fully entangled fraction of the Werner state is F, and the entanglement of formation of the Werner state is given by

$$E_n(W)=H\left(\frac{1}{2}+\sqrt{F[1-F]}\right). \quad (42)$$

The fully entangled fraction of the quasi Werner state is analogously given by

$$f(W)={}_{AB}\langle\Psi_2|W|\Psi_2\rangle_{AB}=F, \quad (43)$$

because the quasi Bell states are orthogonal to each other, except for the pair of states $|\Psi_1\rangle_{AB}$ and $|\Psi_3\rangle_{AB}$, as one can see from the Gram matrix G. However, the quasi Werner state and Werner state are completely different states. In particular, the eigenvalues of quasi Werner states are different from those of Werner states. The eigenvalues of the density operator are given by those of the modified Gram matrix [18]. For the quasi Werner state, the Gram matrix is

$$G_W=\begin{pmatrix} \frac{1}{3}(1-F) & 0 & \frac{1}{3}(1-F)D & 0 \\ 0 & F & 0 & 0 \\ \frac{1}{3}(1-F)D & 0 & \frac{1}{3}(1-F) & 0 \\ 0 & 0 & 0 & \frac{1}{3}(1-F) \end{pmatrix} \quad (44)$$

As a result, we have F, $\frac{1}{3}(1-F)$, $\frac{1}{3}(1+D)(1-F)$, $\frac{1}{3}(1-D)(1-F)$ as the eigenvalues of the quasi Werner state.

Thus the lower bound of the entropy of formation of quasi Werner state is the same as that of Werner state.

Application of entangled coherent state

After discovery of the complete entanglement of H-state, van Enk and Hirota opened up applications [19] such as teleportation and quantum repeater. Especially, serial works of van Enk stimulated an investigation of entangled coherent state by Wang [20], and Jeong, et al. [21].

Generation of Propagating Entangled Coherent State

Let us survey a generation of entangled coherent state which was proposed by van Enk et al. [22]. Entangled state in propagating mode is essential for applications which involve the above example. For a propagating mode, the state $|\alpha\rangle$ should be understood as a continuous mode coherent state. In a simple one-dimensional picture one can define creation and annihilation operators $b^\dagger(\omega)$ and b(ω) for each mode frequency ω. An eigenstate of the annihilation operator

$$b(\omega)|\{\tilde{\alpha}(\omega)\}\rangle=\tilde{\alpha}(\omega)|\{\tilde{\alpha}(\omega)\}\rangle \quad (45)$$

can alternatively be written as a single mode coherent state by introducing a new mode operator by

$$c_1=\int d\omega\phi_1(\omega)^* b(\omega) \quad (46)$$

with $\phi_1(\omega)=\tilde{\alpha}(\omega)/\sqrt{\int d\omega|\tilde{\alpha}(\omega)|^2}$. The state $|\{\tilde{\alpha}(\omega)\}\rangle$ is an eigenstate of c_1 with eigenvalue $\alpha=\sqrt{\int d\omega|\tilde{\alpha}(\omega)|^2}$, and this, with c_1 properly defined, is what we mean by a coherent state $|\alpha\rangle$ from now on. Equivalently, we may rewrite all of this in terms of time dependent functions, operators and modes by introducing Fourier transforms

$$b(t)=\frac{1}{\sqrt{2\pi}}\int d\omega b(\omega)exp(-i\omega t), \quad (47)$$

$$\phi_1(t)=\frac{1}{\sqrt{2\pi}}\int d\omega\phi_1(\omega)exp(-i\omega t), \quad (48)$$

$$c_1=\int dt\phi_1(t)^* b(t) \quad (49)$$

This way one can define independent modes by introducing a complete orthogonal set of functions $\{\phi_i(t)\}$ satisfying

$$\int dt\phi_i(t)\phi_j^*(t)=\delta_{ij} \quad (50)$$

$$\sum\phi_i^*(t)\phi_i(t')=\delta(t-t') \quad (51)$$

Let us consider here the ideal version of a scheme to produce a propagating entangled coherent state. Consider an optical Fabry-Perot cavity with two identical mirrors characterized by a decay rate r. The cavity mode is described by a single mode annihilation operator $c(t)$. If that mode is weakly coupled to a single two level atom, and the cavity is driven by two input fields $b_{in}^{(1)}(\omega)$ and $b_{in}^{(2)}(\omega)$, a standard calculation shows that the Fourier-transformed annihilation operator of the cavity mode, c(ω), is

$$c(\omega)=\frac{\sqrt{r}(b_{in}^{(1)}(\omega)+b_{in}^{(2)}(\omega))}{i(\omega-\omega_c)-r+g^2/(i(\omega-\omega_A)-\tau/2)} \quad (52)$$

Where ω_c is the resonance frequency of the cavity, ω_A is the resonance frequency of the atom, g is the coupling between atom and cavity mode, and τ is the spontaneous decay rate of the atom. The output fields emanating from the cavity are, according to standard input-output theory, determined by

$$b_{out}^{(k)}(\omega_c)=b_{in}^{(k)}(\omega_c)+\sqrt{r}c(\omega) \quad (53)$$

for k=1,2. For an atom far off-resonance with the cavity, or to be more precise, when $|\omega c-\omega A|\gg g^2/r$, all light at $\omega=\omega_c$ will be transmitted:

$$b_{out}^{(1)}(\omega_c)=-b_{in}^{(1)}(\omega_c),\quad b_{out}^{(2)}(\omega_c)=-b_{in}^{(2)}(\omega_c) \quad (54)$$

On the other hand, if the atomic resonance frequency is chosen such that $\omega_A=\omega_{c+}\tau/2$, and we are in the strong coupling regime where $g^2\gg r\tau$, then the cavity resonance is shifted by so much that all light at $\omega=\omega_c$ will be reflected:

$$b_{out}^{(1)}(\omega_c)=b_{in}^{(1)}(\omega_c),\quad b_{out}^{(2)}(\omega_c)=b_{in}^{(2)}(\omega_c) \quad (55)$$

Now we consider an atom in an equal superposition $(|g_1\rangle+|g_2\rangle)/\sqrt{2}$ of two non-degenerate ground states, where there is a resonant coupling from $|g_1\rangle$ at the cavity frequency, while $|g_2\rangle$ is off-resonant. Given two coherent input fields $|\alpha\rangle_k$ for k-1,2 at a frequency $\omega=\omega_c$, the atom-cavity system will then enact the transformation

$$(|g_1\rangle+|g_2\rangle)|\alpha\rangle_1|\alpha\rangle_2\rightarrow|g_1\rangle|-\alpha\rangle_1|-\alpha\rangle_2+|g_2\rangle|\alpha\rangle_1|\alpha\rangle_2 \quad (56)$$

If one subsequently performs a measurement on the atom in the $|\pm\rangle = (|g_1\rangle \pm |g_2\rangle)/\sqrt{2}$ basis, an entangled coherent state $|\Psi_4\rangle_{AB}$ will have been generated if the the outcome was $|-\rangle$. The probability to get that measurement outcome is $P_- = \frac{1}{2}(1 - exp(-4|\alpha|^2))$ which tends to zero for $\alpha \to 0$. With a probability $P_+ = 1 - P_-$ one produces the state $|\Psi_3\rangle$.

Another method is a generation based on cat state [19], and it was demonstrated experimentally by Grangier's group in 2009 [23]. Since this issue is one of fundamental problems in quantum optics, results by Grangier's group should be appreciated.

On the other hand, superposition of macroscopic coherent state is an important subject before that one discusses on entangled coherent state. A generation method based on photon subtraction was proposed in 1997 [24], and it was experimentally demonstrated by Grangier's group [25]. Furthermore, theoretical and experimental progress have been given by NICT group [26] and Scully's group [27].

Thus, subject of quantum states based on coherent state should be focused for development of quantum optics and quantum information science.

Main Theorems in Quantum Information Science

A role of quantum information science is to verify potential applications of fundamental nature of quantum mechanics. To do so, quantum communication theory was developed. In this section, I will describe the fact that non-orthogonal states play a very important role in such a theory.

Quantum detection theory for non-orthogonal states

Quantum detection theory makes clear the fundamental limit for the discrimination among quantum states. Basically, if a set of quantum states is non-orthogonal each other, no one can discriminate without error. In the following, the formulations are shown.

Let us first describe the theory of quantum Bayes criterion.

Theorem: {*Roman type*} [7]

The quantum limitation (average error probability) for the discrimination for two quantum states ρ_1 and ρ_2 is given by

$$P_e = \frac{1}{2} - \| p_1\rho_1 - p_2\rho_2 \| \tag{57}$$

where ρ_1, and ρ_2 are a priori probabilities.

Let us generalize to M-ary case. That is, a set of quantum states is given as $\{\rho_i, i=1,2,3\ldots M\}$. The criterion of quantum Beys strategy is as follows:

$$\min_{\Pi} \sum_i \sum_j \xi_i C_{ji} Tr \rho_i \Pi_i \tag{58}$$

where, $\pi=\{\pi_j\}$ is POVM(positive operator valued measure). As usual, we define the risk operator as follows:

$$W_j \equiv \sum_{j=1}^{M} \xi_i C_{ji} \rho_i \tag{59}$$

$$\Gamma = \sum_{j=1}^{M} \Pi_j W_j = \sum_{j=1}^{M} W_j \Pi_j \tag{60}$$

In general, we consider $C_{ji}=1(i/=j)$, $C_{ji}=0$ (i=j). Then the criterion becomes average error probability P_e.

$$\min_{\Pi} P_e = \min_{\Pi} (1 - \sum_i \xi_i Tr \rho_i \Pi_i) \tag{61}$$

Theorem: {Holevo [28], Yuen [29]}

The optimum condition for M-ary quantum Bayes strategy with respect to POVM is

$$\begin{aligned} &(W_j - \Gamma)\Pi_j = \Pi_j (W_j - \Gamma) = 0, \quad \forall j \\ &\Pi_j (W_i - W_j)\Pi_i = 0, \quad \forall i, j \\ &W_j - \Gamma \geq 0, \quad \forall j \end{aligned} \tag{62}$$

where

$$W_j \equiv \sum_{j=1}^{M} \xi_i C_{ji} \rho_i$$

$$\Gamma = \sum_{j=1}^{M} \Pi_j W_j = \sum_{j=1}^{M} W_j \Pi_j \tag{63}$$

where $C_{ji}=1(i\neq j)$, $C_{ji}=0$ (i=j).

In case of quantum minimax strategy, the criterion is given by

$$P_{em} = \min_{\{\Pi_j\}} \cdot \max_{\{\xi_i\}} \left\{ 1 - \sum_{i=1}^{M} \xi_i Tr \rho_i \Pi_j \right\} \tag{64}$$

Theorem: {Hirota – Ikehara [30]}

Let $\{\xi_i\}$ and $\{\pi_j\}$ be a priori probability and POVM, respectively. Then we have

$$\min_{\{\Pi_j\}} \cdot \max_{\{\xi_i\}} P_e = \max_{\{\xi_i\}} \cdot \min_{\{\Pi_j\}} P_e \tag{65}$$

Theorem: {Hirota – Ikehara [30]}

The optimum conditions for POVM is given by

$$\begin{aligned} &Tr\rho_i\Pi_i = Tr\rho_j\Pi_j, \qquad \forall i, j \\ &(W_j - \Gamma)\Pi_j = \Pi_j (W_j - \Gamma) = 0, \qquad \forall j \\ &\Pi_j (W_i - W_j)\Pi_i = 0, \qquad \forall i, j \\ &W_j - \Gamma \geq 0, \qquad \forall j \end{aligned} \tag{66}$$

where $C_{ji}=1(i\neq j)$, $C_{ji}=0$ (i=j).

Recently, the mathematical progress for quantum minimax theory has been given by D' Ariano et al. [31], Kato [32], Tanaka [33], and Nakahira et al. [34].

Classical capacity for quantum Gaussian channel

When Shannon mutual information is employed as a criterion for evaluation of communication performance, collective quantum measurement effect provides the following capacity formula for lossy Gaussian noise channel, which can be realized by coherent state signals or two-photon coherent state. This is quantum version of well known Shannon-Wiener formula in classical Gaussian channel. In fact, when S=<n>, it reduces to classical one. In addition, several features on difference between quantum and classical of classical capacity for several quantum channels were clarified by author's group.

Theorem: {Holevo – Sohma – Hirota [35]}

The classical capacity for quantum lossy Gaussian noise channel is given by

$$\begin{aligned} C_{HSH} &= \log(1 + \frac{S}{1 + < n >}) + S \log(1 + \frac{1}{S + < n >}) \\ &- < n > \log(\frac{1 + \frac{S}{< n >}}{1 + \frac{S}{1 + < n >}}) \end{aligned} \tag{67}$$

where S and <n> are received signal and noise photon number, respectively.

Theorem: {Hirota [36], Guha [37]}

The secret capacity for physical cipher based on coherent state is

$$C_{GS} = C_{HSH} - C_{Shannon} = \log(1+\frac{S^B}{1+<n>^B}) + S^B \log(1+\frac{1}{S^B+<n>^B}) - <n>^B \log(\frac{1+\frac{S^B}{<n>^B}}{1+\frac{S^B}{1+<n>^B}}) - \log(1+\frac{S^E}{1+<n>^E}) \quad (68)$$

Quantum data compression

Theorem: {Schumacher [38]}

Let us assume an ensemble of non-orthogonal quantum states such as $\{|\psi_i>, p(i)\}$. Then the density operator is given by

$$\rho = \sum_i p(i)|\psi_i><\psi_i| \quad (69)$$

$$\rho^{\otimes n} = \rho \otimes \rho \ldots \otimes \rho \quad (70)$$

The message can be compressed to a Hilbert space with dimension

$$dim H_S = 2^{n(H(\rho)+o(1))} \quad (71)$$

with negligible loss of fidelity when $n \mapsto \infty$

No-cloning theorem

Theorem: {Wootters – Zurek [39]}

Let us assume that $|\psi>_A, |\phi>_B$ are quantum states in two systems. There is no unitary operator on $H \otimes H$ such that for all states $|\psi>_A$, $|\phi>_B$

$$U(|\psi>_A \otimes |\phi>_B) = e^{ic(\psi,\phi)}|\psi>_A \otimes |\psi>_B \quad (72)$$

where ic(Ψ,ϕ) is a real number depending on $|\psi>_A, |\phi>_B$.

Applications of Non-orthogonal State to Quantum Methodology

Quantum illumination

The model of the quantum illumination was given by Lloyd [40] to improve the performance of the optical radar. One photon of an entangled photon is transmitted to a target, and another photon is retained in the receiver. The receiver operates joint measurement on the received light and the retained photon. He showed that quantum illumination scheme achieves an effective signal to background noise ratio. In any case, single photon scheme is useless. So a scheme with Gaussian states was proposed [41]. It employs an entangled signal and idler mode pair obtained from cw SPDC (Spontaneous parametric down-conversion). The output state is given as follows:

$$|\psi>_{SI} = \sum_n \sqrt{\frac{<n>_S^n}{(<n>_S+1)^{n+1}}}|n>_S|n>_I \quad (73)$$

Where <n>s is the average photon number per mode. The detection problem is to discriminate a density operator $\rho_{RI}^{(1)}$ of mixture of signal beam and background and $\rho_{RI}^{(2)}$ of only background.

The optimum average error probability is given by applying Helstrom receiver.

$$P_e = \frac{1}{2}(1-\sum_i \gamma_i^{(+)}) \quad (74)$$

where $\gamma_i^{(+)}$ is the non-negative eigenvalues of $\rho_{RI}^{(1)} - \rho_{RI}^{(2)}$.

Quantum reading

Formulation: The model of the quantum reading was proposed by Pirandola based on the concept of quantum illumination [42]. "It is to discriminate quantum states which are parametrized by reflection target". As an example, he examined the model for discrimination of quantum states affected by the different reflections r_0 and r_1. This corresponds to the model of ASK(amplitude shift keying) scheme. If reflection coefficients are $r_0 = 1$ and $r_1 << 1$, it imposes great energy loss effect. The typical systems in quantum information science suffer the degradation from the energy loss effect. If one employs the non-classical state in the above model, the loss effect has to be taken into account.

On the other hand, PSK(phase shift keying) scheme to realize the classical digital memory does not have a loss effect. We will employ PSK scheme such that the memory on the classical disk consists of the flat and concave which correspond to "0" and "1", respectively.

The difference of two schemes ASK and PSK is not important in the case of classical state, but they make great difference in the case of non-classical states. Thus, PSK scheme was introduced by Hirota [43]. This model can be described by an unitary operator as follows:

$$U(\theta) = exp(-\theta a^\dagger a) \quad (75)$$

where a and † are the annihilation and creation operator in bosonic system, respectively.

The reading method in the current PSK scheme is to illuminate the laser light (coherent state) on a disk, and to read the phase difference of returned light. That is, the signal states of light to discriminate are

$$|\alpha(0)\rangle = I|\alpha\rangle \quad (76)$$

$$|\alpha(1)\rangle = U(\theta)|\alpha\rangle \quad (77)$$

where I is the identity operator.

Error free quantum reading [43]: Let us consider the detection problem of the above model. Here we restrict the problem to the binary detection. So detection targets are two quantum states. Since the phase difference will be π, the problem is to read the phase shift π from the steady state or input state.

The coherent states are prepared in the current classical disk system, and the target signal model becomes as follows:

$$|\alpha(0)\rangle = I|\alpha\rangle = |\alpha\rangle \quad (78)$$

$$|\alpha(1)\rangle = U(\theta=\pi)|\alpha\rangle = |-\alpha\rangle \quad (79)$$

If one employs the conventional homodyne receiver to discriminate the above quantum states, the limitation is imposed by so called quantum shot noise limit. So this is the standard quantum limit in the modern information technology. If one employs the injection back effect [44] to a laser diode to detect the phase delay of the reflection from a disk as the conventional system, the sensitivity is inferior to a homodyne receiver, though it is a typical scheme. However, in general, one can enjoy the Helstrom bound to overcome the standard quantum measurement which is achieved by a homodyne receiver.

Let us employ $|\Psi_2(\alpha)\rangle_{AB}$ (H_1-state) as the light source and

Helstrom receiver. The *B* mode is illuminated to a memory disk. The reflection effect $U_B(\theta)$ operates on B mode, so the channel model is

$$\varepsilon_{A\otimes B} = I_A \otimes U_B(\pi) \tag{80}$$

Then, the target states become as follows:

$$|H_1\rangle_{AB} = h_2(|\alpha\rangle_A|\alpha\rangle_B - |-\alpha\rangle_A|-\alpha\rangle_B)$$
$$|H_2\rangle_{AB} = \varepsilon_{A\otimes B}h_2(|\alpha\rangle_A|\alpha\rangle_B - |-\alpha\rangle_A|-\alpha\rangle_B)$$
$$= h_2(|\alpha\rangle_A|-\alpha\rangle_B - |-\alpha\rangle_A|\alpha\rangle_B) \tag{81}$$

Thus, the input state $|H_1\rangle_{AB} = |\Psi_2\rangle_{AB}$ is changed to $|H_2\rangle_{AB} = |\Psi_4\rangle_{AB}$. The inner product between the above two entangled coherent states in quasi Bell state is

$${}_{AB}\langle H_1|H_2\rangle_{AB} = 0 \tag{82}$$

That is, the inner product becomes zero, and it is independent of the energy of light source. This is a property of the quasi Bell state. To check this special property, one can examine the different phase shift as follows:

$$|\langle H_1|I_A \otimes U_B(\theta)|H_1\rangle| > 0 \tag{83}$$

where $\theta \neq \pi$.

Finally, let us employ the quantum optimum receiver for the binary pure state of two modes. The ultimate detection performances of systems with the coherent state and *H*-state are given, respectively, as follows:

$$P_e(Coherent) = \frac{1}{2}[1 - \sqrt{1 - 4\xi_0\xi_1 exp(-4|\alpha|^2)}]$$
$$P_e(H-state) = 0 \tag{84}$$

Thus, one can see that the property of H-state provides an attractive improvement, and this property can be obtained only by the combination of H-state and the quantum optimum receiver. Although there are many non-classical states, almost all is not changed from the input state to the orthogonal state to the original input state just by reflection. So we interpret that such an effectiveness of the H-state comes from a special symmetry which is a feature of H-state.

On the other hand, different applications of entangled coherent state are developed by Munro's group [45].

Quantum ghost imaging

Quantum imaging is one of attractive applications of new physical phenomena. Especially ghost imaging is a technology to synthesize target image by means of certain correlation between signal beam and reference beam. In original proposal [46] and experiment [47], an entanglement light was employed in the system. By lively investigation, it was clarified that ghost imaging does not represent a true quantum, and that the function can be realized by semi-quantum or classical resource. This fact is reasonable in the world of science and technology, because any useful technologies in real world should be realized by classical way, and these functions may be enhanced by quantum nature. The important fact is that this function can be realized only at optical field. In addition, a special feature of ghost imaging is to have immunity against atmospheric turbulence. To analyze it, one can employ the extended Huygens-Fresnel principle.

$$E(r',t) = \int E(r,t)\frac{k_0 e^{ik_0(L+|r'-r|^2/2L)}}{i2\pi L}e^{\phi(r',r)}dr \tag{85}$$

where $\phi(r',r)$ is a complex valued random process due to turbulence.

Thus, based on Glauber's coherence theory and the above formula, unified theory has been presented by Erkmen and Shapiro [48], Hardy and Shapiro [49]. The basic formula is given by following the average cross correlation function.

$$< R(r_{ccd}) >= K\int d\tau_1 \int d\tau_2 \int dr h(t-\tau_1)h(t-\tau_2)$$
$$\times < E_R^{\dagger}(r_{ccd},\tau_1)E_T^{\dagger}(r,\tau_2)E_R(r_{ccd},\tau_1)E_T(r,\tau_2) > \tag{86}$$

Their works give a great contribution towards a real development of this technology. However, one can see easily the fact that their model includes highly non-linear random process in which Volterra-Wiener theory is applicable. Based on the above, a general design theory as space-time quantum Wiener receiver theory has been developed by the present author, and it will be reported in the subsequent paper.

Quantum Enigma Cipher

In this section, I will give a general framework of a physical cipher as application of quantum detection theory and no cloning theorem for non-orthogonal states.

Concept

The general network systems need to be protected from interception by unauthorized parties. The most serious attack is "Cyber attack against Layer-1 (physical layer such as optical communication line)", because technologies of coupler for tapping have been developed by several institutes. In addition, there are many optical monitor ports for network maintenance. In fact, physical layer of high speed data link is a defenseless. To date, that protection has been provided by classical encryption systems. However, such technologies cannot ensure the provable security, and also the eavesdropper can obtain the correct ciphertext: *C* of mathematical cipher for payload at Layer-2, and she can store it in memory devices. Thus, we cannot rule out the possibility that the cipher may be decrypted by future development of algorithm and computer science.

The best way to protect high speed data is to physically randomize signals as the ciphertext of a mathematical cipher. This is called physical random cipher. The most important feature of this physical random cipher is that the eavesdropper cannot get the correct ciphertext of mathematical cipher, for example a stream cipher by PRNG (pseudo random number generator), from communication lines, while the legitimate user can get it and he can decrypt based on a knowledge of secret key of PRNG.

First example was proposed by Yuen as "Keyed communication in quantum noise(KCQ)"in 2000 [50]. In his scheme, the mathematical cipher is used to select optical communication basis to transmit binary bit data. So the optical signals correspond to ciphertext of the mathematical cipher. Thus a modulation scheme becomes an encryption box for electric data sequence. A legitimate user can get the correct ciphertext, but an eavesdropper cannot get the correct ciphertext, because she does not know which communication basis is used and her received signals are randomized by large effect of quantum noise due to mismatch in communication basis.

During 15 years, many prototype systems so called α/η or Y-00 protocol have been implemented and useful performances have been demonstrated in real optical networks [51-54].

Definition of quantum enigma cipher

Quantum Enigma Cipher is a general scheme for physical random

cipher, which may be a generalization of KCQ. Let us describe here the ideal quantum enigma cipher system.

The quantum enigma cipher consists of an integration of mathematical encryption box and physical randomization box. Here, the physical randomization means that optical signals as the ciphertext of a mathematical cipher are randomized by quantum noise when the eavesdropper observes optical signals with coherent states or another non-orthogonal state. Along with this concept, Quantum Enigma Cipher allows a secure high speed data transmission by means of the quantum noise randomization by a mathematical encryption box and signal modulation systems. Thus, we will define the quantum enigma cipher.

Definition Quantum Enigma Cipher is defined as a scheme which has the following property [55-60]:

Optical signals correspond to ciphertext of a mathematical cipher. The observation signals of legitimate's receiver are error free with a priori knowledge in communication systems. An eavesdropper's receiver suffer a serious error without a priori knowledge.

Examples of the implementation are as follows:

(a) Communication basis for transmission of data is scrambled by PRNG with a secret key [50].

(b) Mapping scheme between data for communication system and optical signal is scrambled by PRNG [61].

(c) Fusion of (a) and (b) [61]

(d) A priori probability for a set of coherent states is hidden as secret key against eavesdropper [56].

(e) A difference of error performance between legitimate and eavesdropper's receiver is created by entanglement resource in transmitter and receiver [59,62].

If the data for communication system is not encrypted by a mathematical cipher, one has to employ (a),(b) and (c). If the data is already encrypted by a mathematical cipher, one can employ one of {(d), (e)}.

In any scheme, the quantum enigma cipher has a mathematical encryption box and physical encryption box. The mathematical encryption box has a secret key of the length $|K_S|$ bits and PRNG for expansion of the secret key. The physical encryption box has a mechanism to create ciphertext as signal and it has a function to induces an error when the eavesdropper's receiver receives the ciphertext as signal. Consequently different ciphertext sequences are observed in the legitimate's receiver and the eavesdropper's receiver, respectively. A requirement for the physical randomization is

$$P_e(Eve) \gg P_e(Bob) \simeq 0 \tag{87}$$

This means that the error performance P_e of the eavesdropper becomes worse than that of the legitimate user, when they observe the ciphertext as signal in communication lines.

Security analysis

In the investigation for the quantitative evaluation of information theoretically secure scheme, Shannon mutual information, trace distance (statistical distance), and Holevo quantity are not appropriate as measure of security. In the following, I will give a guide for such a purpose.

Model: Let us describe a standard symmetric key encryption. A general symmetric key encryption Λ can be given by

$$\Lambda=([P_k], Enc, Dec) \tag{88}$$

where $[P_k]$ is key generation algorithm and it provides key sequence $K \in K$ depending on the probability P_K, Enc is an encryption algorithm which generates ciphertext C=Enc(K,M) where M is plaintext, Dec is a decryption algorithm which produces plaintext $M = Dec(K,C)$. In the case of symmetric key cipher, the secret key is fixed.

When Λ cannot be decrypted by means of computational resource, its security is evaluated by "Guessing probability" [58-60].

(i) Ciphertext only attack on data:

$$P_G(M) = \max_{M \in M} P(M \mid C) \tag{89}$$

(ii) Ciphertext only attack on key:

$$P_G(K) = \max_{K \in K} P(K \mid C) \tag{90}$$

On the other hand, when some plaintext M_K and ciphertext corresponding to them are known, it is called known plaintext attack. It is easy to generalize the above formula as follows:

(iii) Known plaintext attack on data:

$$P_{G_k}(M) = \max_{M \in M} P(M \mid C, M_k) \tag{91}$$

(iv) Known plaintext attack on key:

$$P_{G_k}(K) = \max_{K \in K} P(K \mid C, M_k) \tag{92}$$

If one needs an average, then one can define average guessing probability as follows:

$$\overline{P}_G(M) = \sum_{C \in C} P(C) \max_{M \in M} P(M \mid C) \tag{93}$$

In order to apply the above concept to quantum enigma cipher, one can employ the quantum detection theory for observation of ciphertext, and easily modify the formula of guessing probability. These are sometimes called maximum "a posteriori probability" guessing.

Evaluation of security: A mathematical encryption box produces the ciphertext of length at most $2^{|K_S|}$ bits. Because the key length is $|K_S|$ bits, when the eavesdropper gets the known plaintext of the length $|K_S|$ bits and ciphertext corresponding to them, she can pindown the secret key by the Brute force attack (trying $2^{|K_S|}$ key candidates). That is, the guessing probability is one. In addition, the sequence of the ciphertext has certain correlation because of the structure of PRNG. So the eavesdropper can investigate several mathematical algorithms to estimate the secret key.

In the ideal quantum enigma cipher, the eavesdropper's observation of the cipertext as signal in communication lines suffers error completely by quantum noise randomization, while the legitimate user does not. So the legitimate user can decrypt with the secret key, but the eavesdropper does not even if she gets the secret key after her observation of ciphertext as signal.

Thus, the guessing probability is

$$P_G(K_s) = 2^{-|K_s|} \tag{94}$$

even if she collects the ciphertext of $2^{|K_s|}$ bits. This means an immunity against the Brute force attack by computers. On the other hand, the quantum no cloning theorem may protect a physical Brute force attack by cloning whole quantum states, because a set of quantum states for

the quantum enigma cipher are designed by non-orthogonal state with very close signal distance each other.

Recently, 1 Gbit/sec physical random cipher as a first generation of quantum enigma cipher was demonstrated and Y-00 cipher of 100 Gbit/sec by wave length division multiplex was also demonstrated [54].

Conclusion

The contents of this paper was presented in the International conference on Quantum Physics and Nuclear Engineering held in London. However, I extended the contents based on historical flow on development of quantum information science. From my survey paper, it is expected that further applications of non-orthogonal states as macroscopic quantum state are discovered.

References

1. Glauber R (1963) Coherent and incoherent states of the radiation field Physical Review Letters 131: 2766.
2. Sudarshan ECG (1963) Equivalence of semi classical and quantum mechanical description of statistical light beam. Physical Review Letters 10: 277.
3. Yuen HP (1976) Two photon coherent state of the radiation field Physical Review A-13: 2226.
4. Hirota O (1977) Generalized quantum measurement theory and its applications for quantum communication theory. Transaction of IECE of Japan J60-A: 701.
5. Yuen HP, Shapiro JH (1978) Optical communication with two-photon coherent state-part I. Quantum-state propagation and quantum-noise IEEE Trans Information theory 24: 657.
6. Helstrom CW (1976) Quantum detection and estimation theory Academic press New York USA.
7. Hirota O (2001) Entangled state based on non-orthogonal state Proceedings of QCMC-2000.
8. Walls DF, Milburn GJ (2008) Quantum Optics (Springer New York).
9. Bennett CH, Bernstein HJ, Popescu S, Schumacher B (1996) Concentrating partial entanglement by local operations Physical Review A-53: 2046.
10. Bennett CH, DiVincenzo DP, Smolin JA, Wootters WK (1996) Mixed state entanglement and quantum error correction. Physical Review A-54: 3824.
11. Vedral V, Plenio MB (1998) Entanglement measures and purification procedures. Physical Review A-57: 1619.
12. Hill S, Wootters WK (1997) Entanglement of a pair of quantum bits. Physical Review Letters 78: 5022.
13. Wootters WK (1998) Entanglement of formation of an arbitrary state of two quits. Physical Review Letters 80: 2245.
14. Barnett SM, Phoenix SJD (1989) Entropy as a measure of quantum optical correlation Physical Review A-40: 2404.
15. Tombesi P, Mecozzi R (1987) Generation of macroscopically distinguishable quantum states and detection by squeezed vacuum technique. Journal of Optical Society of America B-4: 1700.
16. Sanders BC (1992) Entangled coherent state Physical Review A-45: 6811.
17. Werner RF (1989) Quantum states with EPR correlations admitting a hidden variable model Physical Review A-40: 4277.
18. Hirota O (2000) Applicable Algebra in Eng Commun and Computing 10: 401.
19. Van Enk SJ, Hirota O (2001) Entangled coherent states: Teleportation and de coherence Physical Review A-64: 022-313.
20. Wang X (2001) Quantum teleportation of entangled coherent state Physical Review 64: 022-302.
21. Jeong H, Kim MS, Lee J (2001) Quantum information processing for a coherent superposition state via a mixed entangled coherent channel. Physical Review A-64: 052-308.
22. Hirota O, van Enk SJ, Mabuchi H (2003) Application generation and test of symmetric entangled coherent state Proceedings of QCMC-2002.
23. Ourjoumtsev A, Ferreyrol F, Tualle-Brouri R, Grangier P (2009) Preparation of non-local superposition of quasi-classical light state. Nature Physics 5: 189.
24. Dakna M, Anhut T, Opatrny T, Knoll L, Welsch D, et al. (1997) Generating Schrodinger-cat-like states by means of conditional measurements on a beam splitter. Physical Review A-55: 3184.
25. Ourjoumtsev A, Tualle-BR, Laurat J, Grangier P (2006) Generating optical Schrodinger kittens for quantum information processing Science 31283.
26. Takahashi H, Wakui K, Suzuki S, Takeoka M, Hayasaka K, et al. (2008) Generation of large-amplitude coherent state superposition via ancilla-assisted photon-subtraction. Physical Review Letters 101: 233-605.
27. Wang D, Cai H, Liu R, Scully MO (2016) Schrodinger cat state generated by quantum gated photonic gauze field arXivorgquant-pharXiv:160208009.
28. Holevo AS (1973) Statistical decision theory for quantum systems Journal of Multivariate Analysis 3: 337.
29. Yuen HP, Kennedy R, Lax M (1975) Optimum testing of multiple hypotheses in quantum detection theory IEEE Trans Information Theory 21: 125.
30. Hirota O, Ikehara S (1982) Minim ax strategy in the quantum detection theory and its application to optical communication. Trans of the IECE of Japan E65: 627.
31. D' Ariano, Suchi MF, Kahn J (2005) Minimax quantum state discrimination Physical Review A-72: 032-310.
32. Kato K (2011) Minimax receiver for a binary pure quantum state signal Process of IEEE ISIT pp: 1077-1081.
33. Tanaka F (2012) Non-informative priori in the quantum statistical model of pure states. Physical Review A-85: 062-305.
34. Nakahira K, Kato K, Usuda T (2013) Minimax strategy in quantum signal detection with inconclusive results. Physical Review A-88: 032-314.
35. Holevo AS, Sohma M, Hirota O (1999) Capacity of quantum Gaussian channels Physics Rev A-59: 18-20.
36. Hirota O, Iwakoshi T, Sohma M, Futami F (2010) Quantum stream cipher beyond the Shannon limit of symmetric cipher and the possibility of experimental demonstration. Proceedings of SPIE on Quantum communication and quantum imaging 7815.
37. Guha S, Hayden P, Krovi HL, loyd SL, Shapiro JH, et al. (2014) Quantum enigma machines and the locking capacity of a quantum channel. Physical Review X-4011016.
38. Shumacher B (1995) Quantum coding Physical Review A-512738.
39. Wootters W, Zurek W (1982) A single quantum cannot be cloned Nature 299: 802.
40. Lloyed S (2008) Enhanced sensitivity of photo-detection via quantum illumination Science 321: 1465.
41. Tan SH, Erkmen B, IGiovannetti V, Guha S, Lloyed S, et al. (2011) Quantum illumination with Gaussian states. Physical Review Letters 101: 253-601.
42. Pirandola S (2011) Quantum reading of a classical digital memory. Physical Review Letters 106: 090-504.
43. Hirota O (2011) Error free quantum reading by quasi Bell state of entangled coherent state arXivorgquant-pharXiv: 1108-4163.
44. Hirota O, Suematsu Y (1979) Noise properties of injection lasers due to reflected waves. IEEE Journal of Quantum Electronics QE-25: 142.
45. Joo J, Munro WJ, Spiller TP (2011) Physical Review Letters 107: 083-601.
46. Belinskii A, Klyshko D (1994) Two photon optics: diffraction holography and transformation of two dimensional signals. Soviet Physical JETP 78: 259.
47. Pittman T, Shih YH, Strekalov DV, Sergienko AV (1995) Optical imaging by means of two photon quantum entanglement Physical Review A-52 R3429.
48. Erkmen BI, Shapiro JH (2008) Unified theory of ghost imaging with Gaussian state light Physical Review A-77: 043-809.
49. Hardy ND, Shapiro JH (2011) Reflective ghost imaging through turbulence Physical Review A-84: 063-824.
50. Yuen HP (2003) KCQ: A new approach to quantum cryptography I ar Xivorgquant-pharXiv: 0311061.

51. Borbosa GA, Corndorf E, Kanter GS, Kumar P, Yuen HP (2003) Secure communication using meso scopic coherent state. Physical Review Letters 90: 227-901.

52. Corndorf E, Liang C, Kanter GS, Kumar P, Yuen HP, et al. (2005) Quantum noise randomized data encryption for wavelength division multiplexed fiber optic network. Physical Review A-71: 062326.

53. Hirota O, Sohma M, Fuse M, Kato K (2005) Quantum stream cipher by Yuen 2000 protocol: Design and experiment by intensity modulation scheme. Physical Review A-72: 022335.

54. Futami F (2014) Experimental demonstrations of Y-00 cipher for high capacity and secure fiber communications Quantum Information Processing 13: 2277.

55. Hirota O (2013) Quantum Enigma Cipher: protecting optical network for cloud computing system Reader's Review. United Airline Vol-70.

56. Hirota O (2013) Cyber-attack against optical communication system and its defense technology-Toward development of Quantum Enigma. Cipher-IEICE Technical Meeting on Optical Community System: OCS 113: 90.

57. Hirota O, Futami F (2013) Quantum Enigma Cipher Manyousya Publishing Company in Japanese.

58. Hirota O (2015) Towards quantum enigma cipher-a protocol for Gbit/sec encryption based on discrimination property of non-orthogonal quantum state-Tamagawa University Quantum ICT Research Institute Bulletin.

59. Hirota O (2015) Towards Quantum Enigma Cipher-II Tamagawa University Quantum ICT Research Institute Bulletin: 533.

60. Hirota O (2015) Towards Quantum Enigma Cipher-III Tamagawa University Quantum ICT Research Institute Bulletin: 537.

61. Hirota O, Kurosawa K (2007) Immunity against correlation attack on quantum stream cipher protocol Quantum Information Processing Vol-681.

62. Shapiro JH, Zhang Z, Wong FNC (2014) Secure communication via quantum illumination Quantum Information Processing 13: 21-71.