数理解析研究所講究録
982巻 1997年 148-159

Quantum Cryptography Modulating the Spontaneous Emission Rate of Photons

量子暗号理論と実験

Hideaki Matsueda, Fumiaki Shibata*, and Chikako Uchiyama**

Department of Information Science, Kochi University
2-5-1 Akebono-cho, Kochi 780, Japan
phone: +81-888-44-8334, FAX: +81-888-44-8361,
e-mail: matsueda @ is.kochi-u.ac.jp

**Department of Physics, Ochanomizu University*
Bunkyo-ku, Tokyo 112, Japan

***Department of Electrical Engineering and Computer Science*
Yamanashi University, 4 Takeda, Yamanashi 400, Japan

Abstract

A novel method of quantum cryptography is proposed, together with a mathematical theory on the basis of nonequilibrium statistical mechanics. The proposed method involves the controlled randomness in the spontaneous emission of photons. Uncertainties in spontaneous photon emission, beam-splitting, and superposition improve the cryptographic security.

A quantum communication channel is mathematically equivalent to a model of spin relaxation when the Schwinger bosons are introduced. Effects of quantum mechanical devices on the propagating signals are expressed as rotation operators in the spin coherent state representation. Effect of an eavesdropper is represented by a phase shifter.

The concept of "controlled randomness" is introduced to construct quantum cryptographic systems. This could be implemented by using microcavities with which the rate of spontaneous emission is controlled. In theory, this controlled randomness is analyzed with the use of the Kubo-Anderson model of spin relaxation.

1. Introduction

The fact that C. E. Shannon published his theory of cryptography[1] a year after his information theory of 1948, is an example which obviously shows the parallelism between the researches in cryptography and physics of information. In 1976, the first proposal of public key cryptography was published[2], starting a new research area which has been actively studied since then. It is interesting to combine the key distributions in cryptography and the quantum theory involving uncertainties of many kinds. The former was devised on the bases of number theory, but on the contrary, in the latter, the major concern lies in continuously varying probability and uncertainty. Therefore, the combination of these theories differing in nature is expected to bear novel breakthroughs[3-14].

The history of quantum cryptography may date back at least to the latter part of 1960s, when an idea of coding which uses the uncertainty principle of quantum mechanics was proposed by S. Wiesner [3]. However, it had been a couple of decades until this proposal was recognized as a method of cryptographic key distribution, by C. H. Bennett and G. Brassard, with an experimental result[4-6]. The applicability of a quantum mechanical thought experiment known as the Einstein-Podolsky-Rosen(EPR) paradox[7-10] to cryptography, has also been discussed in 1990's, by A. K. Ekert and others[11-13].

In this paper, a novel method to implement the secret key transmission is proposed, together with mathematical formulas for it. This method involves a dual uncertainties in spontaneous emission of photons, and in beam-splitting and superposition, improving the security of cryptographic communications intrinsically.

In this method, photonic pulse trains with random intervals are generated by spontaneous emission, in such a way that the photon generation is controlled in an on/off manner for each bit period by the transmitter (the sender or Alice) [14-16]. Then the pulse train is divided, essentially into 2 communication channels (2 waveguides or optical fibers) by means of a beam splitter, and transmitted separately over a distance. At the receiver's (Bob's) site, both pulse trains are superposed by means of another beam splitter, to regenerate the original crypto-signals encoded by the controlled spontaneous emission [14-16].

Moreover, it is also possible to merge the two channels into one channel and still keeping the independence of the two pulse trains, if the two are launched into the one channel with different timing. This could be done by a Mach-Zehnder interferometer at the transmitter's site, and the time lag between the two pulse trains are canceled for a considerable amount of photons by another Mach-Zehnder interferometer at the receiver's site, as in the method of C. H. Bennett [12] and other researchers [17]. It is also interesting to consider the possible combination of the method proposed in this paper and the privacy

amplification procedure [23].

The mathematical formulas are derived on the basis of nonequilibrium statistical mechanics[16,18-22], for the proposed quantum cryptographic method. Effects of quantum mechanical devices on the propagating signals, are expressed by rotation operators in the spin coherent state representation. Effect of an eavesdropper is represented by a phase shifter. Furthermore, the concept of "controlled randomness" is introduced to understand both the artificial inhibition of spontaneous emission, and the setting of the average rate of spontaneous emission within each non-inhibited bit interval, in the proposed quantum cryptography.

It is clear that this proposal involves quantum mechanical phenomena and formulas, and naturally be included in the quantum cryptography. This will contribute to expand the research fields of cryptography, both in theory and in experiments, as well as to provide a physical mean to improve the security of secret communication.

2. Cryptography using controlled spontaneous emission of photons and beam splittings

Photons are emitted in either mechanism of induced emission or spontaneous emission. The former is widely used as the principle of laser operations. The latter is a typical quantum mechanical effect, in which photons are emitted at random timing. This may be regarded as an uncertainty of spontaneous emission. However, possibility to alter the randomness of the spontaneous emission has been suggested since at least 5 decades ago[24-28], and recently the inhibition of the spontaneous emission in some particular wavelength has been demonstrated, in a microcavity or in special structures[26-28]. There is no reason why this mechanism could not be used to controll the randomness for many purposes, including the cryptography.

It is possible to suppress the spontaneous emission for prescheduled time intervals, resulting a modulation of spontaneous emission rate between the natural value and zero, by changing the size of the microcavity, the feature of the structure[15,16,29], or the state of the medium in the cavity. If AC (or dynamic) Stark effect is used to change the state of the medium, very high speed modulation above 10 Gbps (10^{10} bits per second) is possible [15,16,30].

The controlled randomness described above may be combined with the other randomnesses of beam-splitting to constitute a entirely novel cryptographic method, as depicted in Fig. 1. In this scheme, the on and off of the spontaneous emission generate bits of signal. The length of a bit is set for example to be the average interval of the spontaneous emission of a photon or a photon cluster in the on state. This average interval is variable as a function of temperature, and is adjustable by the transmitter in agreement with the receiver's condition.

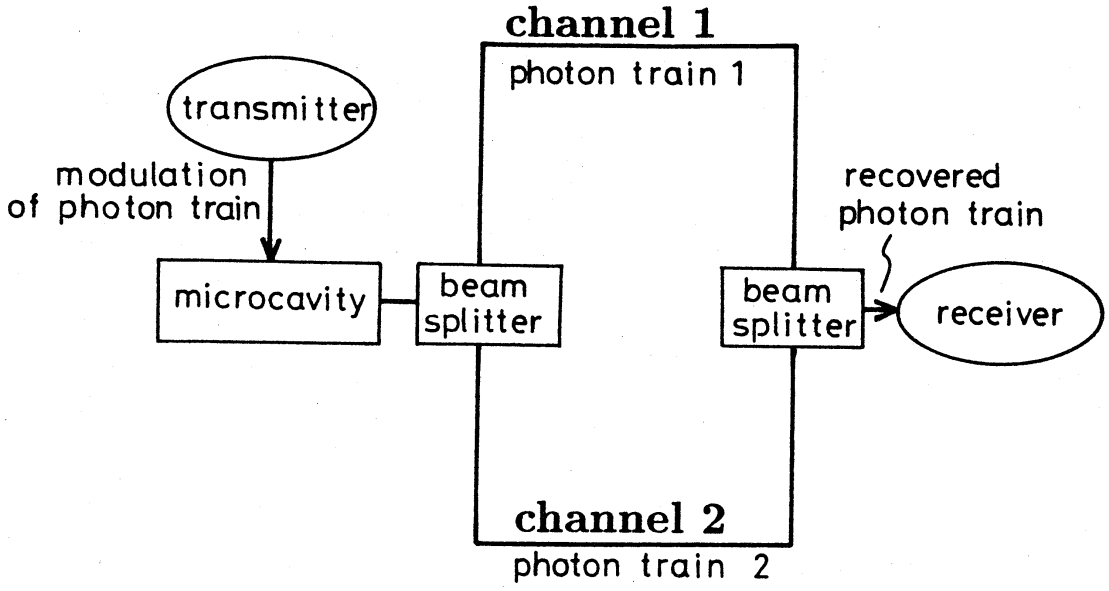

Figure 1. A cryptographic system with controlled spontaneous emission of photons.

Photonic pulse trains are generated by this controlled spontaneous emission mechanism, encoding signals in each bit interval which is the average emission period of a photon cluster in the on bit. In practice, the beam splitter may be considered to divide the photonic pulse train into the 2 channels, in a random manner. This is the uncertainty of beam-splitting. Therefore, an eavesdropper who has access to only one of the channels, will misread the signal with probability 1/2 per bit. Then the probability of correct reading will decrease with the nth power of 1/2, if the number of bits n is increased. However, the legitimate receiver recovers the original photon train, superposing the photon trains from the 2 channels with sufficient precision in time, and reads it to complete the communication.

It may also be possible to merge the two channels into one, employing a couple of Mach-Zehnder interferometer, as mentioned in previous section. In this case, each pulse may better consists of multiple number of photons. The multi-photon pulse could also be generated by the controlled spontaneous emission, for example increasing the temperature of the microcavity.

3. Mathematical basis for quantum cryptographic systems

Mathematically, it is possible to regard the communication system shown in Fig.1 as a series connection of 4 terminal devices[18-22,31], i.e. 2 beam splitters, and 1 phase shifter as an eavesdropper between the 2 beam splitters. Each one of the 2 lines connecting these 4 terminal devices corresponds to either of the 2 branched channels respectively. One of the input and output pair of the 4 terminal device is shortcircuited at the eavesdropper, resulting in a 2 terminal device. The propagation of signal is represented as the trans-

formation of the state of the system, which may be expressed by so-called spin coherent state, $|\boldsymbol{z}\rangle$, where $\boldsymbol{z}$ is defined as a vector of 2 components representing the 2 channels [19,20].

We first give a systematic method to describe the channel based on four terminal devices [18,31]. A typical device such as a beam splitter shown in Fig.1 is characterized by a 2×2 matrix $\mathcal{T}$,

$$\boldsymbol{a}_{out} = \mathcal{T}\boldsymbol{a}_{in} \tag{1}$$

where the vector operator $\boldsymbol{a}$ is defined by,

$$\boldsymbol{a} = \begin{pmatrix} a_+ \\ a_- \end{pmatrix} \tag{2}$$

where $+$ and $-$ represent the two channels respectively. Each component of eq.(2) satisfies the boson commutation relation

$$[a_\pm, a_\pm^\dagger] = 1 \tag{3}$$

where a and $a^\dagger$ are an annihilation operator and a creation operator respectively, corresponding to the propagating photons.

Eq.(1) gives input-output relation when the signals pass through the device. As a typical example, we consider a beam splitter (90° coupler) characterized by,

$$\mathcal{T}^x = \begin{pmatrix} \cos(\alpha/2) & -i\sin(\alpha/2) \\ -i\sin(\alpha/2) & \cos(\alpha/2) \end{pmatrix}. \tag{4}$$

The beam splitter at the transmitter site in Fig.1 corresponds to this 4 terminal device having no input into one of the input terminal, and at the receiver's site one of the output terminal is discarded.

There is another type of representation for the input-output relation, employing the spin coherent states $|\boldsymbol{z}\rangle$ [19,20,31],

$$a_\pm |\boldsymbol{z}\rangle = z_\pm |\boldsymbol{z}\rangle \tag{5}$$

which has a remarkable transformation property,

$$R[\zeta, \hat{\boldsymbol{n}}]\,|\boldsymbol{z}\rangle = |\mathcal{R}[\zeta, \hat{\boldsymbol{n}}]\boldsymbol{z}\rangle \tag{6}$$

where R and $\mathcal{R}$ are rotation operators of the angle ζ aroud the axis of the unit vector $\hat{\boldsymbol{n}}$, acting, respectively, on the state $|\boldsymbol{z}\rangle$ and the two component vector $\boldsymbol{z}$ given as,

$$\boldsymbol{z} = \begin{pmatrix} z_+ \\ z_- \end{pmatrix} \tag{7}$$

and if $\boldsymbol{\sigma}$ is the vector Pauli matrix, $\mathcal{R}[\zeta, \hat{\boldsymbol{n}}] = e^{-\frac{i}{2}\zeta \hat{\boldsymbol{n}}\cdot\boldsymbol{\sigma}}$.

A standard procedure leads to the equivalence between $\mathcal{T}^x$ and $\mathcal{R}^x$ for a beam splitter [18,31],

$$\mathcal{R}^x = \mathcal{T}^x \tag{8}$$

where,

$$\mathcal{R}^x = e^{-\frac{i}{2}\alpha\sigma_x} \tag{9}$$

with angle α and a component σ_x of the Pauli matrix.

We note that the relation eq.(8) is a special case of a more general relation,

$$\boldsymbol{\mathcal{R}} = \boldsymbol{\mathcal{T}} \tag{10}$$

for an arbitrary Euler rotation.

Thus we have found an essentially equivalent transformation property both for the operators and the states when the signals propagate through the devices. It should be emphasized that the correspondence of eq.(10) holds good only when the spin coherent state representation is applied.

In addition to the beam splitter, we need the transformation matrix for a phase shifter,

$$\mathcal{T}^z = \begin{pmatrix} e^{i\gamma_+} & 0 \\ 0 & e^{i\gamma_-} \end{pmatrix} \tag{11}$$

which causes the phase shift $\gamma_\pm$ in the $(\pm)$ channels. Again a standard procedure leads to the equivalence between the operators [18,31],

$$\mathcal{R}^z = \mathcal{T}^z \tag{12}$$

where $\mathcal{R}^z$ is the phase shift operator given as,

$$\mathcal{R}^z = e^{-\frac{i}{2}(\gamma_- - \gamma_+)\sigma_z} \tag{13}$$

having a component σ_z of the Pauli matrix which acts on the vector $\boldsymbol{z}$.

4. Time evolution theory for the quantum channels

Let a density matrix of a quantum system at time τ be $W(\tau)$. Then, after a time interval ϵ we have,

$$W(\tau + \epsilon) = U(\epsilon)W(\tau)U(\epsilon)^\dagger \tag{14}$$

where $U(\epsilon)$ is an unitary transformation matrix. We are now in a position to construct the system using the transformation property and eq.(13) described in previous section. An input state of quantum channel in Fig.1 is assumed to be the spin coherent state$|z_{in}(\tau)\rangle$, namely,

$$W(\tau) = |z_{in}(\tau)\rangle \langle z_{in}(\tau)| \tag{15}$$

which is divided by the beam splitter as can be seen from Fig.1,

$$W(\tau + \epsilon_1) = |\mathcal{R}^x(\alpha_1) z_{in}(\tau)\rangle \langle \mathcal{R}^x(\alpha_1) z_{in}(\tau)| \tag{16}$$

where $\mathcal{R}^x$ is given by eq.(9) with the rotation angle,

$$\alpha_1 = \omega_1 \epsilon_1 \tag{17}$$

of which angular frequency ω_1 characterizes the property of the beam splitter.

Then in the (+) channel we meet with the eavesdropper who perturbs the state of the system giving a phase shift γ_+ during time interval ϵ_2,

$$W(\tau + \epsilon_1 + \epsilon_2) = |\mathcal{R}^z(\gamma_2)\mathcal{R}^x(\alpha_1) z_{in}(\tau)\rangle \langle \mathcal{R}^z(\gamma_2)\mathcal{R}^x(\alpha_1) z_{in}(\tau)| \tag{18}$$

where $\mathcal{R}^z$ is given by eq.(13). In eq.(18) we have included γ_- for generality defining

$$\gamma_2 = \gamma_- - \gamma_+ \tag{19}$$

$$= (\omega_- - \omega_+)\epsilon_2. \tag{20}$$

Finally, the signals propagating through the (+) and (−) channels are superposed by the second beam splitter,

$$\begin{aligned} &W(\tau + \epsilon_1 + \epsilon_2 + \epsilon_3) \\ &\quad = |\mathcal{R}^x(\alpha_3)\mathcal{R}^z(\gamma_2)\mathcal{R}^x(\alpha_1) z_{in}(\tau)\rangle \langle \mathcal{R}^x(\alpha_3)\mathcal{R}^z(\gamma_2)\mathcal{R}^x(\alpha_1) z_{in}(\tau)| \\ &\quad = |z_{out}(t)\rangle \langle z_{out}(t)| \end{aligned} \tag{21}$$

where

$$\alpha_3 = \omega_3 \epsilon_3 \tag{22}$$

and

$$t = \tau + \epsilon_1 + \epsilon_2 + \epsilon_3. \tag{23}$$

5. Signal detection theory for the quantum cryptographic system

The output signal is detected by the receiver shown in Fig.1. That is, the probability density to find the quantum system in the spin coherent state $|z\rangle$ is obtained in the form,

$$P(z,t) = \langle z_{out}| W(t) |z_{out}\rangle \tag{24}$$

$$= \exp[-|z - z_{out}(t)|^2] \tag{25}$$

where

$$z_{out}(t) = \mathcal{R}^x(\alpha_3)\mathcal{R}^z(\gamma_2)\mathcal{R}^x(\alpha_1)z_{in}(\tau)\ . \tag{26}$$

After the initial time τ, the input signal is fed into the quantum channel at every multiple of unit time Δt. Then, we detect the output signals at the time points $t + n \cdot \Delta t (n = 0, 1, 2, \cdots)$ according to the rule of eq.(26),

$$z_{out}(t + n \cdot \Delta t) = \mathcal{R}^x(\alpha_3)\mathcal{R}^z(\gamma_2)\mathcal{R}^x(\alpha_1)z_{in}(\tau + n \cdot \Delta t)\ . \tag{27}$$

6. A theory for the controlled randomness

The input signal is fully characterized by the complex quantity,

$$z_{in}(\tau) = \begin{pmatrix} z_{in,+}(\tau) \\ z_{in,-}(\tau) \end{pmatrix} = \begin{pmatrix} r_+(\tau)e^{i\phi_+(\tau)} \\ r_-(\tau)e^{i\phi_-(\tau)} \end{pmatrix} \tag{28}$$

which is a consequence of the signal generation by the microcavity. This formula is well known in the Kubo-Anderson model of random frequency modulation for spin relaxation phenomena [32,33].

For our models of quantum cryptography, it is essential to introduce randomness into the input signal eq.(28) in order to impede eavesdroppings [14-16]. In other words, when the quantities $r_\pm(\tau)$ and/or $\phi_\pm(\tau)$ are randomly modulated in the microcavity shown in Fig.1, the messages bear randomness.

We have incorporated the messages into $r_\pm(\tau)$ of eq.(28) by changing the cavity length or the quantum electrodynamical state of the medium, while the phases $\phi_\pm(\tau)$ are kept constant. When the eavesdropper observes the signals, he is perplexed by random intervals of the messages. Moreover, even if the the encodement action of the transmitter was correct, some of the signals are missing because there is a possibility that no spontaneous emission occurs within a single keying interval. This causes little problem for the transmitter and the receiver. Because they know the operating condition of the cavity. And hence, the errors can be corrected by suitable (error rate dependent) repetition of massage transmission.

Furthermore, there is another possibility to control the randomness. Consider oscillators having complex coordinates $z_\pm(\tau)$. When time evolution of $z_\pm(\tau)$ is determined by,

$$\frac{d}{d\tau}z_\pm(\tau) = i[\omega_{0\pm} + \omega_\pm(\tau)]z_\pm(\tau) \tag{29}$$

where $\omega_\pm(\tau)$ is a random function of time. Eq.(29) has a solution of the form,

$$z_{in,\pm}(\tau) = r_\pm(\tau)e^{i\phi_\pm(\tau)} \tag{30}$$

where,

$$\phi_{\pm}(\tau) = \omega_{0,\pm}\tau + \int_0^{\tau} dt\omega_{\pm}(t). \tag{31}$$

Additional signals are generated by on-off encodements of $\phi_{\pm}(\tau)$, besides the modulation of $r_{\pm}(\tau)$. This is a kind of frequency modulation with central (angular) frequencies of $\omega_{0,\pm}$. As an illustration example, let us assume that the stochastic quantity $\omega_{\mu}(\tau)(\mu = +, -)$ can take only two values $\pm\Delta$. Then, the carrier of the generated signals will have the two possible frequencies, the higher frequency $\omega_{0\mu} + \Delta$ and the lower frequency $\omega_{0\mu} - \Delta$, at random. Therefore, the eavesdropper is largely perplexed by this randomness, i.e., he will at least miss half of the messages because he will observe the message signals by setting his frequency at one of the jumping frequencies.

In this scheme, we can freely control the jumping rate. This can be done as follows. There is a characteristic parameter of the model,

$$\alpha_c = \tau_c \cdot \Delta \tag{32}$$

where τ_c is the correlation time of $\omega_{\mu}(\tau)$ reflecting the microscopic fluctuation of the medium. When $\alpha_c \ll 1$, the modulation speed is fast while it is slow for $\alpha_c \gg 1$. As the transmitter and the receiver have a common consent on the value of α_c, they can determine an average "life time" to stay in the $+\Delta$ state. Roughly speaking, the larger α gives the larger life time. Control of the random jumping rate will give the eavesdropper much more difficulty in obtaining the correct signal messages.

We see that the lifetime of the spontaneous emission is determined by the temperature surrounding the cavity, while the "lifetime" to stay in $+\Delta$ state in this model is determined by α. We have thus clear correspondence between the two, i.e. the temperature and the theoretical life time. As a matter of course, the jumping rate, in turn, determines the proper modulation frequency of $r_{\pm}(\tau)$ for the inhibition of spontaneous emission.

7. Conclusions

After a historical overview of the quantum cryptography, a novel cryptographic method is proposed, giving the detailed constructions including a controlled spontaneous photon emitter, beam splitters, and bifurcated waveguiding channels. This method involves the uncertainties of controlled random spontaneous emission of photonic pulses, beam splittings, and superposition of random photon trains, increasing the security of the cryptography.

Moreover, in this method it is possible to merge the two channels into one, employing a couple of Mach-Zehnder interferometers to give and to cancel a time lag between the two

photonic puls trains. The speed of the modulation in the controlled randomness scheme could be beyond 10^{10}bps using, for example, AC Stark effect.

Mathematical formulas are given for the proposed cryptographic methods, showing the applicability of the nonequilibrium statistical mechanics to the problems of quantum cryptography. The propagation of crypto-signals are formulated as series of transformations, causing rotations of phase angles in the vector of spin coherent state. The result of a quantum cryptographical communication may be evaluated as the probability density to find the system in a desirable spin coherent state, using a density matrix of the whole procedure.

Quantum theory itself contains a lot of questions to be solved, including measurement processes and observations[7-13,34,35]. Therefore, the researches on quantum cryptography are expected to bring breakthroughs both in science and engineerings.

References

[1] C. E. Shannon, "Communication Theory of Secrecy Systems", Bell System Tech. J., 28, 656-715, 1949.

[2] W. Diffie and M. E. Hellman, "New Directions in Cryptography", IEEE Trans. Information Theory, IT-22, 644-654, 1976.

[3] S. Wiesner, "Conjugate Coding", SIGACT News 15, 78-88, 1983.

[4] C. H. Bennett and G. Brassard, "The dawn of a new era for quantum cryptography: The experimental prototype is working!", SIGACT News 20, 78-82, 1989.

[5] C. H. Bennett and G. Brassard, "Practical Quantum Oblivious Transfer and Bit Commitment", Crypto'91, session 8, proc. pp. 20-26, 1991.

[6] C. H. Bennett, F. Bessette, G. Brassard, and L. Salvail, J. Cryptology, 5, 3-28, 1992.

[7] A. Einstein, B. Podolsky, and N. Rosen, "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?", Phys. Rev., 47, 777-780, 1935.

[8] A. Aspect, P. Grangier, and G. Roger, "Experimental Tests of Realistic Local Theories via Bell's Theorem", Phys. Rev. Lett., 47, 460-463, 1981.

[9] A. Aspect, P. Grangier, and G. Roger, "Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A New Violation of Bell's Inequalities", Phys. Rev. Lett. 49, 91-94, 1982.

[10] A. Aspect, J. Dalibard, and G. Roger, "Experimental Test of Bell's Inequalities Using Time-Varying Analyzers", Phys. Rev. Lett., 49, 1804-1807, 1982.

[11] A. K. Ekert, J. G. Rarity, P. R. Tapster, and G. M. Palma, "Practical Quantum Cryptography Based on Two-Photon Interferometry", Phys. Rev. Lett., 69, 1293-1295, 1992.

[12] C. H. Bennett, "Quantum Cryptography Using Any Two Nonorthogonal States", Phys. Rev. Lett., 68, 3121-3124, 1992.

[13] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum Cryptography without Bell's Theorem", Phys. Rev. Lett., 68, 557-559, 1992.

[14] H. Matsueda, "Methods of Quantum Cryptograph", Proc. 1994 Symp. on Cryptography and Information Security, Biwako Japan, paper SCIS94-15A, 8pp, Jan. 27-29, 1994.

[15] H. Matsueda, "Quantum Cryptography by Modulating Spontaneous Photon Emissions", Tech. Dig. The Pacific Rim Conf. on Lasers and Electro-Optics (CLEO/Pacific Rim'95), Makuhari Japan, paper P46, p.274, Jul. 10-14, 1995.

[16] H. Matsueda, F. Shibata, and C. Uchiyama, "Quantum Cryptography Modulating the Spontaneous Emission Rate of Light", the 15th Annual International Cryptology Conf. (Crypto'95), Santa Barbara USA, Rump Session, paper 21^h00, Aug. 29, 1995.

[17] P. D. Townsend, J. G. Rarity, and P. R. Tapster, "Enhanced Single Photon Fringe Visibility in a 10km-long Prototype Quantum Cryptography Channel", Elentron. Lett., 29, 1291-1293, 1993.

[18] F. Shibata and C. Uchiyama, "Theory of Quantum Communication Channels Based on Non-equilibrium Statistical Mechanics", submitted to J. Phys. Soc. Jpn.

[19] Y. Takahashi and F. Shibata, "Spin Coherent State Representation in Non-Equilibrium Statistical Mechanics", J. Phys. Soc. Jpn., 38 656-668, 1975.

[20] Y. Takahashi and F. Shibata, "Generalised Phase Space Method in Spin Systems - Spin Coherent State Representation", J.Stat.Phys., 14, 49-65,1976.

[21] F. Shibata and C. Uchiyama, "A Path Integral Theory of Relaxation I", Physica, 181A, 441-462, 1992.

[22] C. Uchiyama and F. Shibata, "A Path Integral Theory of Relaxation II ", Physica, 198A, 538-550, 1993.

[23] C. H. Bennett, G. Brassard, and J.-M. Robert, "Privacy Amplification by Public Discussion", SIAM J. Comput. 17, 210-229, 1988.

[24] E. M. Purcell, "Spontaneous Emission Probabilities at Radio Frequencies", Phys. Rev., 69, 681,1946.

[25] K. H. Drexhage, "Interaction of Light with Monomolecular Dye Layers", Progress in Optics, 12, ed. by E. Wolf (North Holland, New York) 163-232, 1974.

[26] R. G. Hulet, E. S. Hilfer, and D. Kleppner, "Inhibited Spontaneous Emission by a Rydberg Atom", Phys. Rev. Lett., 55, 2137-2140, 1985.

[27] E. Yablonovitch, "Inhibited Spontaneous Emission in Solid-State Physics and Electronics", Phys Rev. Lett., 58, 2059-2062, 1987.

[28] S. Haroche and D. Kleppner, "Cavity Quantum Electrodynamics", Physics Today, 42, 24-30, 1989.

[29] H. Matsueda, "Physical Basis of Optoelectronic Integration", Chap.2 of *'Optoelectronic Integration'*, ed. O. Wada (Kluwer Academic Publishers, Boston), 17-60, 1994.

[30] I. Averbukh, B. Sherman, and G. Kurizki, Enhanced Squeezing by Periodic Frequency Modulation under Parametric Instability Conditions", Pnys. Rev. A 50, 5301-5308, 1994.

[31] B. Yurke, S. L. McCall, and J. R. Klauder, "SU(2) and SU(1,1) Interferometers", Phys. Rev., A 33, 4033-4054, 1986.

[32] R. Kubo, "Note on the Stochastic Theory of Resonance Absorption", J. Phys. Soc. Jpn., 9, 935-944, 1954.

[33] P. W. Anderson, "A Mathematical Model for the Narrowing of Spectral Lines by Exchange or Motion", J. Phys. Soc. Jpn., 9, 316-339, 1954.

[34] R. J. Glauber, "Amplifiers, Attenuators, and Schrödinger's Cat", Ann. N. Y. Acad. Sci., 480, 336-372, 1986.

[35] *"Quantum Physics and the Universe"*, M. Namiki, Y. Aizawa, K. Maeda, and I. Ohba eds., special vol. of Vistas in Astronomy, (P. Beer, A. E. Roy, and R. E. White, eds.), Pergamon Press, 37, 1993.