

A Dynamical Bifurcation of Distinguishability in Thermalization Processes, from Classical to Quantum

KENTARO IMAFUKU[†] and HIDEKI IMAI^{†,‡}

We study a distinction problem of two heat baths with given information from ancilla (quantum or classical two level system) which is interacting with the heat baths. Analysing dynamics of ancilla system in a Markov approximation region, we show that the process in which “quantum ancilla” acquires the quantum distinguishability is described as a bifurcation process from the time evolution of classical distinguishability.

1. Introduction

During the last twenty years, quantum system has been found being an important resource for several informational tasks such as cryptography, communication, and computation¹⁾. They are expected to provide us functions we cannot reach with classical resources, and are keeping a position of the most attractive research targets. They have been actively studied in a crossing field of several existing subjects of quantum mechanics, cryptography, informatics, and computation theory. With a background of highly developed nanotechnologies, some of ideas of that are being implemented in the real world. We can safely say that we are in an exciting moment of the history of information science.

On the other hand, it is also fact that a distance of theories and realities are somehow increasing. Sometimes we discuss just theoretical ideas without paying any attention to realities. Of course, when we are interested in estimation of bounds of some informational abilities of given quantum resources for example, assumptions of arguments don't have to be based on realities at all. However, in order to make some idea going into any application, we surely have to pay (a bit of) attentions to things which happens in the real world. In particular, consideration of “time scales” or “dynamics” is a necessary path to make our idea feasible. For instance, it would be meaningless to consider any applications of quantum states which take as long time as life time of universe to be pre-

pared. Moreover, physical observable (or state) is not unique target on which we can speak of “dynamics”. In fact, as to be seen here, it is also possible to discuss dynamics of “informatic ability” defined through some “informatic tasks” associated with physical (evoluting) states. That can be nontrivial even in cases where the state evolution is rather well understood.

With the above general circumstances, our interest in the present article is such dynamical aspect of informational abilities, and we would discuss a time evolution of “distinguishability” of two physical objects with information through some physical ancilla. More precisely, our goal is to see how quantum systems as ancilla dynamically obtain its advantage with respect to classical systems. As an specific but interesting example, we analyse the dynamics of distinguishability for two macroscopic heat baths with simple but fundamental ancilla, i.e. quantum two level system (qubit system) or with classical two level system (cbit system), and see how the deviation of quantum information from classical information would “dynamically” come up in their thermalization processes.

2. Set up

2.1 Game

Let us make our problem clear by introducing the following two-party game. Notice that our purpose here is not to propose game being fair against malicious players, but just to explain situation we focus on. Therefore we are assuming that Alice and Bob always follow the rule of the game.

- (1) Alice (with heat bath) and Bob (with ancilla) agree to use two (inverse) temperature (β_0, β_1) as parameters of the game.

[†] Research Center for Information Security, National Institute of Advanced Industrial Science and Technology (AIST)

[‡] Institute of Industrial Science, the University of Tokyo

- (2) Choosing one of the two temperature β_j with probability π_j ($j = 0$ or 1), Alice prepares heat bath whose state is equilibrium of the chosen temperature.
- (3) Getting information from the ancilla prepared by Bob, which would physically interact with the heat bath prepared by Alice, Bob guesses the temperature chosen by Alice.
- (4) If his guess is correct, Bob wins. Otherwise Alice wins.

Through this game, the distinguishability can be defined as the probability of Bob's winning when Bob takes his best strategies.

2.2 Physical Description

First of all, let us consider a description of the problem where Bob has one qubit as his ancilla. Since we have to discuss dynamics, we start from the following Hamiltonian which gives us physical description of the model (which is so called spin-boson model²⁾) with small coupling constant λ :

$$H_{tot} = H_A + H_B + \lambda H_I \tag{1}$$

where H_A is a Hamiltonian of heat bath system:

$$H_A = \int dk \omega_k a_k^\dagger a_k, \tag{2}$$

H_B is a Hamiltonian of ancilla system:

$$H_B = \frac{\omega_0}{2} \sigma_z, \tag{3}$$

H_I is an interaction Hamiltonian between heat bath and ancilla:

$$H_I = \int dk g(k) (\sigma_+ a_k + \sigma_- a_k^\dagger), \tag{4}$$

where σ_\pm are defined $\sigma_\pm = \sigma_x \pm i\sigma_y$ where $\sigma_{x,y,z}$ is the usual Pauli Matrix, a_k and a_k^\dagger is annihilation and creation operator of k -mode bose particle (they hold the following commutation relation $[a_k, a_{k'}^\dagger] = \delta(k - k')$), and $g(k)$ is a proper cut-off function which holds

$$\gamma = \int dk |g(k)|^2 \delta(\omega_k - \omega_0) \neq 0. \tag{5}$$

The preparation of heat bath by Alice in equilibrium state of temperature β_j corresponds to her preparation of Gaussian mean zero quantum state $\langle \cdot \rangle$ characterised the following correlation matrices⁴⁾:

$$\begin{pmatrix} \langle a_k^\dagger a_{k'} \rangle, & \langle a_k^\dagger a_{k'}^\dagger \rangle \\ \langle a_k a_{k'} \rangle, & \langle a_k a_{k'}^\dagger \rangle \end{pmatrix} = \begin{pmatrix} \frac{1}{e^{\beta_j \omega_k} - 1} & 0 \\ 0, & \frac{e^{\beta_j \omega_k}}{e^{\beta_j \omega_k} - 1} \end{pmatrix} \delta(k - k'). \tag{6}$$

Let us suppose that Bob prepares his ancilla's

state in ρ_0 at $t = 0$, and he makes his system interact with the heat bath prepared by Alice. In this case, the time-evolved state of the ancilla ρ_t can be formally described as

$$\rho_t^{(\beta_j)} = \text{tr}_A (e^{-iH_{tot}\tau} \rho_0 \otimes \mu_{\beta_j} e^{-iH_{tot}\tau}) \tag{7}$$

where μ_{β_j} is a formal representation of state of heat bath which is characterised by the above correlation matrix, and tr_A denotes a partial trace over the degree of freedom of the heat bath.

Considering a time rescaling with van Hove limit^{3),4)} $\gamma t \rightarrow t/\lambda^2$ and $\lambda \rightarrow 0$ we obtain a master equation:

$$\frac{d}{dt} \rho_t^{(\beta_j)} = -\mathcal{L}^{(\beta_j)} \rho_t^{(\beta_j)} \tag{8}$$

whose formal solution is given as

$$\rho_t^{(\beta_j)} = e^{-\mathcal{L}^{(\beta_j)} t} \rho_0 \tag{9}$$

where

$$\begin{aligned} \mathcal{L}^{(\beta)} = & -\frac{e^{\beta\omega_0}}{e^{\beta\omega_0} - 1} \left(\sigma_- \cdot \sigma_+ - \frac{1}{2} \{ \sigma_+ \sigma_-, \cdot \} \right) \\ & - \frac{1}{e^{\beta\omega_0} - 1} \left(\sigma_+ \cdot \sigma_- - \frac{1}{2} \{ \sigma_- \sigma_+, \cdot \} \right). \end{aligned} \tag{10}$$

Let us remind us that the equation describes the dynamics in a course-grained time scale in which the influence from bosonic environment seems to be white noise^{4),5)}. The dominant effect of environment to the dynamics is well figured out in this time scale as the exponential decaying process⁶⁾. In other words, we are neglecting phenomena described in a much shorter time scale than the exponential decay process of the system. That can be considered as analogue to the fact that we introduce a larger time scale than mean free time of particle in medium when we describe the dynamics with Langevin equation. Now let us consider classical counterpart of the above situation. In the game introduced in the above, Bob would be supposed to use a classical two level system as his ancilla. That means, we have to employ a balance equation instead of the quantum master Eq. (8). From physical point of view, feasible balance equation should be equation associating the eigenstates of H_S , and its stationary solution must be physically correct equilibrium state

$$\rho_{st} = \frac{1}{Z_{\beta_j}} e^{-\beta_j H_S} \tag{11}$$

where

$$Z_{\beta_j} = \text{tr} \left(e^{-\beta_j H_S} \right). \tag{12}$$

Notice that the diagonal part of Eq. (8) (in the basis diagonalizing σ_z) has closed form (and doesn't affect the evolution of off diagonal part of $\rho_t^{(\beta_j)}$) and can be considered as a balance equation between two eigenstates of H_S . Moreover the stationary solution of the diagonal part of equation is exactly (11). Thus we can employ the diagonal part of Eq. (8) as a physically feasible classical counterpart of Eq. (8) itself^{4),5)}. Therefore the state at time t of classical ancilla can be given by Eq. (9) for diagonally prepared ρ_0 . We denote it as

$$\tilde{\rho}_t^{(\beta_j)} := e^{-\mathcal{L}^{(\beta_j)} t} \rho_0 \tag{13}$$

for *diagonally prepared* ρ_0 . Needless to say, $\tilde{\rho}_t^{(\beta_j)}$ is always diagonal state by definition as it should be.

2.3 Distinguishability

First, let us consider an optimal success probability of the distinction between $\rho_t^{(\beta_0)}$ (with probability π_0) and $\rho_t^{(\beta_1)}$ (with probability π_1). As usual distinction problem for quantum states⁷⁾, let us introduce a POVM to distinguish $\rho_t^{(\beta_0)}$ and $\rho_t^{(\beta_1)}$. Considering positive operator E_j ($E_0 + E_1 = I$) associated a measured value j , when Bob gets j as a consequence of a measurement described by E_0 and E_1 , we suppose that Bob will conclude that the measured state was $\rho_t^{(\beta_j)}$. In this case, the probability that Bob will correctly judge his state according to his measurement is given as

$$\begin{aligned} p_{E_0, E_1}(\rho_t^{(\beta_0)}, \rho_t^{(\beta_1)}) \\ = \pi_0 \text{tr} \left(E_0 \rho_t^{(\beta_0)} \right) + \pi_1 \text{tr} \left(E_1 \rho_t^{(\beta_1)} \right) \end{aligned} \tag{14}$$

and the optimal success probability Bob can achieve by proper choice of his POVM can be obtained as

$$\begin{aligned} p(\rho_t^{(\beta_0)}, \rho_t^{(\beta_1)}) = \max_{E_0, E_1} p_{E_0, E_1}(\rho_t^{(\beta_0)}, \rho_t^{(\beta_1)}) \\ = \pi_0 + \sum \text{positive eigen value of } \Lambda \end{aligned} \tag{15}$$

where

$$\Lambda = \pi_1 \rho_t^{(\beta_1)} - \pi_0 \rho_t^{(\beta_0)}. \tag{16}$$

(Pay attention that the optimal success probability doesn't depend on the picture of the time evolution of the state). Remember that Bob can choose his initial state of ancilla. Finally we can define the distinguishability of the two heat bath prepared by Alice as

$$P_{\text{qubit}}(t) = \max_{\rho_0} \left[p(\rho_t^{(\beta_0)}, \rho_t^{(\beta_1)}) \right]. \tag{17}$$

Notice that we can easily introduce classical counterpart of (17) in an exactly same way as the above.

$$P_{\text{bit}}(t) = \max_{\rho_0 \in \Omega_D} \left[p(\tilde{\rho}_t^{(\beta_0)}, \tilde{\rho}_t^{(\beta_1)}) \right]. \tag{18}$$

where Ω_D is a set of all diagonal states. Pay attention that E_0 and E_1 giving $p(\tilde{\rho}_t^{(\beta_0)}, \tilde{\rho}_t^{(\beta_1)})$ always represents a diagonal projection measurement since the states are diagonal. That is coincide with the fact that Bob's ancilla is classical object.

3. Analysis

Here let us analyse the behaviour of $P_{\text{qubit}}(t)$ and $P_{\text{bit}}(t)$ defined in the previous section.

3.1 Solution of Master Equation (8)

For a given initial condition

$$\rho_0 = \frac{1}{2} (1 + \vec{a} \cdot \vec{\sigma}), \tag{19}$$

one can easily find the solution of (8) as

$$e^{-\mathcal{L}^{(\beta_j)} t} \rho_0 = \frac{1}{2} \left(I + \vec{a}^{(j)}(t) \cdot \vec{\sigma} \right) \tag{20}$$

where

$$\vec{a} = (a_x, a_y, a_z), \tag{21}$$

$$\vec{a}^{(j)}(t) = (a_x^{(j)}(t), a_y^{(j)}(t), a_z^{(j)}(t)) \tag{22}$$

and

$$a_x^{(j)}(t) = e^{-\frac{\gamma_j}{2} t} a_x \tag{23}$$

$$a_y^{(j)}(t) = e^{-\frac{\gamma_j}{2} t} a_y \tag{24}$$

$$a_z^{(j)}(t) = e^{-\gamma_j t} a_z - \tanh \frac{\beta_j \omega_0}{2} (1 - e^{-\gamma_j t}) \tag{25}$$

with

$$\gamma_j = \coth \frac{\beta_j \omega_0}{2}. \tag{26}$$

Note that classical solution $\tilde{\rho}_t^{(\beta_j)}$ can be easily obtained as particular case of the above ($a_x = a_y = 0$).

3.2 Estimation of $P_{\text{qubit}}(t)$ and $P_{\text{bit}}(t)$

Now let us estimate Eq. (15), substituting Eq. (20) into it. For simplicity, we restrict ourselves to the case where $\pi_0 = \pi_1 = 1/2$. In this cases, we obtain

$$p(\rho_t^{(\beta_0)}, \rho_t^{(\beta_1)}) = \frac{1}{2} + \frac{1}{4} d_t^{(\beta_0, \beta_1)} \tag{27}$$

where

$$\begin{aligned} d_t^{(\beta_0, \beta_1)} &= \sqrt{\sum_{j=x, y, z} (a_j^0(t) - a_j^1(t))^2} \\ &= \left(F_{\beta_0, \beta_1}^2(t/2) (a_x^2 + a_y^2) \right) \end{aligned} \tag{28}$$

$$+ (F_{\beta_0\beta_1}(t)a_z + G_{\beta_0\beta_1}(t))^2)^{1/2} \quad (29)$$

with

$$F_{\beta_0\beta_1}(t) = e^{-\gamma_0 t} - e^{-\gamma_1 t} \quad (30)$$

$$G_{\beta_0\beta_1}(t) = -\tanh \frac{\beta_0 \omega_0}{2} (1 - e^{-\gamma_0 t}) + \tanh \frac{\beta_1 \omega_0}{2} (1 - e^{-\gamma_1 t}) \quad (31)$$

Remembering $a_x^2 + a_y^2 + a_z^2 \leq 1$, we can bound $d_t^{(\beta_0, \beta_1)}$ as

$$d_t^{(\beta_0, \beta_1)} \leq \sqrt{f_t(a_z)} \quad (32)$$

where

$$f_t(a_z) = A_{\beta_0\beta_1}(t)(a_z - B_{\beta_0\beta_1}(t))^2 + C_{\beta_0\beta_1}(t), \quad \text{for } -1 \leq a_z \leq 1, \quad (33)$$

and

$$A_{\beta_0\beta_1}(t) = (F_{\beta_0\beta_1}^2(t) - F_{\beta_0\beta_1}^2(t/2)) \quad (34)$$

$$B_{\beta_0\beta_1}(t) = -\frac{F_{\beta_0\beta_1}(t)G_{\beta_0\beta_1}(t)}{F_{\beta_0\beta_1}^2(t) - F_{\beta_0\beta_1}^2(t/2)} \quad (35)$$

$$C_{\beta_0\beta_1}(t) = F_{\beta_0\beta_1}^2(t/2) - \frac{G_{\beta_0\beta_1}^2(t)F_{\beta_0\beta_1}^2(t/2)}{F_{\beta_0\beta_1}^2(t) - F_{\beta_0\beta_1}^2(t/2)} \quad (36)$$

Notice that $f_t(a_z)$ is always positive.

The equality of Eq. (32) holds when $a_z^2 = 1 - a_x^2 - a_y^2$. That means that the upper bound is achieved when Bob prepares his initial state of his ancilla in pure state. In classical case, a_z is restricted to $a_z = \pm 1$ since initial state must be diagonal.

Summing up the above argument, we can estimate $P_{\text{qubit}}(t)$ and $P_{\text{bit}}(t)$ as the followings:

$$P_{\text{qubit}}(t) = \frac{1}{2} + \frac{1}{4} \max_{-1 \leq a_z \leq 1} \sqrt{f_t(a_z)} \quad (37)$$

and

$$P_{\text{bit}}(t) = \frac{1}{2} + \frac{1}{4} \max_{a_z = -1, 1} \sqrt{f_t(a_z)}. \quad (38)$$

3.3 Bifurcation of $P_{\text{qubit}}(t)$ from $P_{\text{bit}}(t)$

Since the a_z -dependence of them (or $f_t(a_z)$) hardly depend on Eqs. (34) and (35), we have to see them rather carefully. We can safely assume $\beta_0 > \beta_1$ without losing any generality. In this case, one can check the followings:

- (1) $A_{\beta_0\beta_1}(t)$ is a monotonic increasing function (for $t \geq 0$) such that $A_{\beta_0\beta_1}(0) = -\infty$ and $A_{\beta_0\beta_1}(\infty) = 0$.
- (2) $B_{\beta_0\beta_1}(t)$ is a monotonic increasing function (for $t \geq 0$) such that $B_{\beta_0\beta_1}(0) = -\infty$ and $B_{\beta_0\beta_1}(\infty) = 0$.
- (3) In particular, there exists t^* such that

$$B_{\beta_0\beta_1}(t^*) = -1.$$

Observing Eqs. (33), (37), (38) and the above, one can easily get the following results:

$$P_{\text{qubit}}(t) = \begin{cases} \frac{1}{2} + \frac{1}{4} \sqrt{f_t(-1)} & \dots \text{ for } 0 \leq t \leq t^* \\ \frac{1}{2} + \frac{1}{4} \sqrt{f_t(B_{\beta_0\beta_1}(t))} & \dots \text{ for } t^* < t \end{cases} \quad (39)$$

and

$$P_{\text{bit}}(t) = \begin{cases} \frac{1}{2} + \frac{1}{4} \sqrt{f_t(-1)} & \dots \text{ for } 0 \leq t. \end{cases} \quad (40)$$

In order to achieve the distinguishability in Eq. (39) for $t > t^*$, Bob has to prepare the initial state of qubit in a pure state whose a_z is given as $a_z = B_{\beta_0\beta_1}(t)$.

One can find that the advantage of quantum distinguisher (who can handle a qubit as ancilla) with respect to classical distinguisher (who can handle a classical two level system as ancilla) doesn't exist before the critical time t^* and that it does appear in a bifurcational way⁸⁾ at $t = t^*$. In other words, quantum distinguisher takes a *finite time* t^* to get quantum advantage.

4. Summary and Remarks

Let us summarise what we can see in the analysis.

- (1) $P_{\text{bit}}(0) = P_{\text{qubit}}(0) = 1/2$, which simply means that what Bob can do at $t = 0$ is pure guess without additional hint. Since the interaction starts at $t = 0$, ancilla can give Bob only few information and doesn't help Bob's guess so much.

- (2) $P_{\text{bit}}(t \rightarrow \infty) \rightarrow P_{\text{qubit}}(t \rightarrow \infty) \rightarrow P_\infty$ where

$$P_\infty = \frac{1}{2} + \frac{1}{4} \left(\tanh \left(\frac{\beta_0 \omega_0}{2} \right) - \tanh \left(\frac{\beta_1 \omega_0}{2} \right) \right).$$

That means that the quantum distinguisher would lose his advantage in the asymptotic region of large time t . This can be naturally expected as a consequence of de-coherence (i.e., thermalization) of qubit ancilla through the interaction with heat bath. In a usual use of thermometer, we measure temperature of physical object after the thermometer achieves equilibrium state with the object. In this sense, the way of measurement of temperature by thermometer corresponds to our asymptotic result.

Conversely, the distinction of temperatures by using “quantumness” (in finite time region) as discussed here is somehow beyond the philosophy (or physics) of usual thermometer. It might be interesting to generalise this idea and to consider something which can be called “quantum thermometer”.

- (3) The initial state which gives optimal distinguishability is always pure state. For the classical ancilla, the initial state is always given as

$$\tilde{\rho}_0 = \frac{1}{2}(I - \sigma_z) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \quad (41)$$

whereas that for quantum ancilla depends on time interaction time t as

$$\rho_0 = \begin{cases} \frac{1}{2}(I - \sigma_z) & \dots \text{for } t \leq t^* \\ \text{a pure state whose } a_z = B_{\beta_0\beta_1}(t) & \dots \text{for } t^* < t \end{cases}$$

- (4) Advantage of qubit ancilla with respect to classical two level ancilla appears at $t = t^*$ in a bifurcational way. That means that it takes a finite time t^* for quantum ancilla to get advantages from “quantumness”. Let us note that our argument is based on the master Eq. (8) which is derived under the Markov approximation, neglecting shorter time scale than the exponential decay process. That means the bifurcation process belongs to the large time scale which can be observed as easily as exponential decay, unlike quantum zenon effect which belongs to short time scale. It might be possible and interesting to construct a new cryptographic primitive based on the finite time gap found here.
- (5) Seeing the two contributions $F_{\beta_0\beta_1}^2(t/2)(1 - a_z^2)$ and $(F_{\beta_0\beta_1}(t)a_z + G_{\beta_0\beta_1}(t))^2$ in Eq. (29), one can find the bifurcation (or the appropriate choice of $a_z \neq -1$) is a consequence of the tradeoff between the positive contribution from the former and the negative contribution from the latter. In addition, one can find that the positive contribution comes up rather slowly than the negative contribution, and that can be considered as the essential mechanism of the bifurcation phenomena discussed in the present

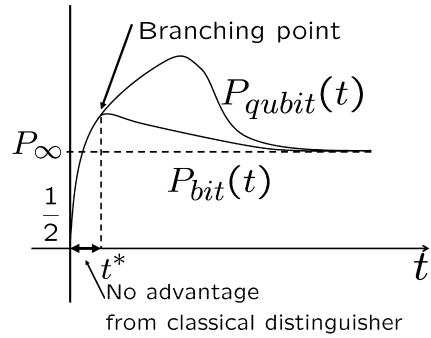


Fig. 1 Schematic graphs of $P_{qubit}(t)$ and $P_{bit}(t)$.

paper. The deviation of decaying speed of off-diagonal elements from that of diagonal one plays an important role in the phenomena. In general, there exists a constraint between the speeds of decaying modes of qubit system when the dynamics is described in a complete positive map which is a fundamental requirement to hold probability interpretation of quantum mechanics⁹⁾. From this point of view, the bifurcation phenomena we pointed out here seem deeply related to the fundamental requirement, although we have to pay a bit attention to appropriate choice of the classical counterpart for general case. (In the model we discussed here, we can choose the diagonal part associated to the energy eigenvalue of the system Hamiltonian as the classical counterpart. Pay attention that it is based on the classical physics of thermalization rather than mathematics).

Finally, it would be worthy to mention an interpretation of our argument based on quantum entanglementness. It is often said that entanglement is the origin of advantage of quantum resources¹⁾. On the other hand, our quantum advantage seems not to be based on any entanglement since we employ just one qubit as ancilla. However, one can see that our argument can be also understood in the context of entanglement actually as the following: Let us consider a general state of qubit

$$\rho = \frac{1}{2}(I + \vec{a} \cdot \vec{\sigma}). \quad (42)$$

Introducing vacuum $|0\rangle$ and one particle state $|1\rangle$ with respect to creation and annihilation operators of two spin-1/2 fermions u and d , we can equivalently rewrite the state as

$$\rho = \frac{1+a_z}{2}|1\rangle_u\langle 1| \otimes |0\rangle_d\langle 0| \quad (43)$$

$$+ \frac{1-a_z}{2}|0\rangle_u\langle 0| \otimes |1\rangle_d\langle 1| \quad (44)$$

$$+ \frac{a_z - ia_y}{2}|1\rangle_u\langle 0| \otimes |0\rangle_d\langle 1| \quad (45)$$

$$+ \frac{a_z + ia_y}{2}|0\rangle_u\langle 1| \otimes |1\rangle_d\langle 0| \quad (46)$$

on a Hilbert space $\mathcal{H}_u \otimes \mathcal{H}_d$. One can see immediately that the lack of off-diagonal elements in Eq. (42) corresponds to the lack of Eqs. (45) and (46) in this representation. Moreover Eqs. (45) and (46) are necessary for the state to be entangled state over the Hilbert space \mathcal{H}_u and \mathcal{H}_d . In other words, our quantum distinguisher who makes use of the off-diagonal element of Eq. (42) can be considered as a distinguisher who can collectively measure an entangled state on $\mathcal{H}_u \otimes \mathcal{H}_d$ whereas our classical distinguisher can measure individually a reduced state on \mathcal{H}_u (or \mathcal{H}_d).

Acknowledgments This work was supported by the project on “Research and Development on Quantum Cryptography” of National Institute of Information and Communications Technology as part of the programme “Research and Development on Quantum Communication Technology” of the Ministry of Public Management, Home Affairs, Posts and Telecommunications of Japan.

References

- 1) For example, Nilsen, M.A. and Chuang, I.L.: *Quantum Computation and Quantum Information*, Cambridge University Press (2000).
- 2) Leggett, A.J., Chakravarty, S., Dorsey, A.T., Fisher, M.P.A., Garg, A. and Zwerger, W.: Dynamics of the dissipative two-state system, *Rev. Mod. Phys.*, Vol.59, pp.1–85 (1987).
- 3) Van Hove, L.: Quantum-mechanical perturbations giving rise to a statistical transport equation, *Physica*, Vol.21, pp.517–540 (1955).
- 4) Accardi, L., Lu, Y.G. and Volovich, I.V.: *Quantum Theory and Its Stochastic Limit*, Springer-Verlag (2002).
- 5) Walls, D.F. and Milburn, G.J.: *Quantum Optics*, Springer (1994).
- 6) Facchi, P. and Pascazio, S.: *Physica*, A271, pp.133–146 (1999).
- 7) For example, Fuchs, C.A.: Just Two Nonorthogonal Quantum States, *Quantum Communication, Computing, and Measurement 2*, Kumar, P., D’Ariano, G.M. and Hirota, O. (Eds.), pp.11–16. quantu-ph/9810032, Kluwer, Dordrecht (2000).
- 8) Haken, H.: *Synergetics, An Introduction*, Springer, Berlin (1983); *Advanced Synergetics*, Springer, Berlin (1987); *Information and Self-Organization*, Springer, Berlin (1988).
- 9) Kimura, G.: Restriction on relaxation times derived from the Lindblad-type master equations for 2-level systems, *Phys. Rev.*, A 66, 062113 (2002).

(Received February 3, 2005)

(Accepted July 4, 2005)

(Online version of this article can be found in the IPSJ Digital Courier, Vol.1, pp.436–441.)



Kentaro Imafuku received his B.E., M.E. and Ph.D. degrees in physics from Waseda University in 1994, 1996 and 2000 respectively. Currently he is a Researcher at Research Center for Information Security, National Institute of Advanced Industrial Science and Technology.

In 1997, he was appointed as a Research Associate at department of physics, Waseda University. He had been in University of Roma Torvergata as JST/JSPS Overseas Research Fellow for two years, since 2001. Since 2003, he had been a Postdoctoral fellow at Institute of Industrial Science, the University of Tokyo. He is a member of JSP.



Hideki Imai received the B.E., M.E. and Ph.D. degrees in electrical engineering from the University of Tokyo in 1966, 1968, and 1971, respectively. Currently, he is a Professor at the Institute of Industrial Science, the University of Tokyo.

He is also the Director of Research Center for Information Security, National Institute of Advanced Industrial Science and Technology. He is the Chair of CRYPTREC (Cryptography Techniques Research and Evaluation Committee of Japan) and the Junior Past President of IEEE Information Theory Society. Fellow of IEEE and IEICE.