Multiparty Quantum Secret Sharing of Quantum States with Quantum Registers*

GUO Ying(郭迎)[1,2], ZENG Gui-Hua(曾贵华)[1**], CHEN Zhi-Gang(陈志刚)[2]

[1] *Department of Electronic Engineering, Shanghai Jiaotong university, Shanghai 200030*

[2] *Department of Communication Engineering, Central South University, Changsha 410083*

(Received 4 January 2007)

A quantum secret sharing scheme is proposed by making use of quantum registers. In the proposed scheme, secret message state is encoded into multipartite entangled states. Several identical multi-particle entanglement states are generated and each particle of the entanglement state is filled in different quantum registers which act as shares of the secret message. Two modes, i.e. the detecting mode and the message mode, are employed so that the eavesdropping can be detected easily and the secret message may be recovered. The security analysis shows that the proposed scheme is secure against eavesdropping of eavesdropper and cheating of participants.

PACS: 03. 67. Dd, 03. 65. Ud

Physically, a quantum secret sharing (QSS) scheme is a method of encrypting quantum or classical message into a multi-partite entanglement state and then the generated state is distributed among several quantum systems (shares). Each of shares has no information about the secret message while it can be reproduced by collecting several shares. Accordingly, QSS schemes are likely to play important roles in secure operations of distributed quantum computation, sharing difficult-to-construct ancillary states and joint sharing of quantum money.

Since the first QSS scheme was proposed by using three-particle and four-particle GHZ states,[1] this kind of schemes have attracted much attention both theoretically and experimentally.[2−12] Especially, the QSS scheme proposed in Ref. [9] makes the (k, n)-threshold QSS scheme possible. In the (k, n)-threshold QSS scheme, an arbitrary quantum state is distributed into n shares so that any k out of n shares can reproduce the initial state while any $k-1$ or less shares have no information about it. After that, it was shown that any general access structure is consistent with the monotonicity and the no cloning theorem can be realized by a QSS scheme.[3] In addition, experimental demonstrations of the threshold scheme were reported.[4,12] However, the implementing processes of these schemes do not seem to be straightforward. Recently, it has been demonstrated that controlled-NOT (CNOT) gates can be realized simply and expediently in experiment,[13,14] which may be useful for sharing a secret message with the same effect.

In this Letter, we propose a new QSS scheme which encrypts a quantum message into a multi-partite entanglement state. The proposed scheme is a $(2, 3)$-threshold QSS scheme. Instead of constructing a look-up table to allow legal participants to determine the remaining participants' information, the present QSS lets legal participants extract the deterministic secret message without the assistance of the remaining participants. In the proposed scheme, the message state is entangled by the dealer using CNOT gate at the encoding stage, and the secret message may be restored with another CNOT gate under the cooperation of any two of three participants at the discovery stage. We use entanglement of the encoded state to check the perfectness of quantum channel for all participants, and any intervention of eavesdroppers and cheating of participants can be detected. For the general case, i.e. the $(u+1, N)$-threshold QSS scheme, the dealer of the secret message must apply several CNOT gates on the prepared states to entangle the secret message, and any $u+1$ of N participants should apply the same number of CNOT gates to disentangle the state to restore the secret message. In the following we present our scheme in detail.

Suppose the dealer expects to share a single-qubit secret message to three distant parties (i.e. Alice, Bob and Charlie), and any two of receivers can recover the secret message only by their mutual assistance. To reach this goal we propose the following QSS scheme.

(i) Assume that the secret message is denoted by

$$|\phi_m\rangle = \alpha|0_m\rangle + \beta|1_m\rangle, \tag{1}$$

where $|\alpha|^2 + |\beta|^2 = 1$. To insert the secret message into three shares, the dealer generates a tri-particle entanglement state $|\Psi_1\rangle = C_{am}(|\Phi\rangle \otimes |\phi_m\rangle)$ by combining the secret message $|\phi_m\rangle$ and a prepared EPR pair $|\Phi\rangle = \frac{1}{\sqrt{2}}(|0_a 1_b\rangle - |1_a 0_b\rangle)$, where the subscripts a, b and m represent the three different particles p_a, p_b and p_m, respectively; and C_{am} is a CNOT gate applying on p_a (the controlled qubit) and p_m (the target qubit). The generated tri-particle entanglement state may be expressed as

$$|\Psi_1\rangle = \frac{1}{\sqrt{2}}(\alpha|0_a 1_b 0_m\rangle + \beta|0_a 1_b 1_m\rangle - \alpha|1_a 0_b 1_m\rangle$$

* Supported by the National Natural Science Foundation of China under Grant Nos 60472018 and 60573127.

** Email: ghzeng@sjtu.edu.cn

©2007 Chinese Physical Society and IOP Publishing Ltd

$$- \beta|1_a 0_b 0_m\rangle). \quad (2)$$

Because the dealer knows everything (e.g. the secret message and the prepared two-particle entanglement state), to generate the same entanglement states is possible. Thus, the dealer generates n ($n \geq 4$) identical entanglement states $|\Psi_i\rangle$ with $i = 1, 2, \ldots, n$ ($|\Psi_1\rangle = |\Psi_2\rangle = \cdots = |\Psi_n\rangle$) using the same message. After these operations, the evolved $3n$ particles are stored respectively in three different registers R_a, R_b, and R_c. The arranged sequences of the particles are shown in Fig. 1.

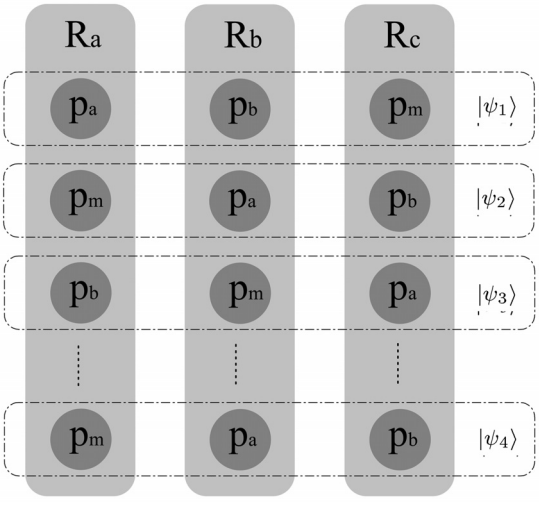

Fig. 1. Arrangement of the particles p_a, p_b and p_m of the state $|\Psi_1\rangle, |\Psi_2\rangle, \ldots, |\Psi_n\rangle$ in three different quantum registers R_a, R_b, and R_c.

We note here that three particles in each row are entangled but all particles in each quantum register are independent. One may find that the secret message is divided into three shares and carried by three different quantum registers, i.e. R_a, R_b, and R_c. Finally, the dealer sends three registers R_a, R_b, and R_c to Alice, Bob and Charlie, respectively, so that participants hold shares of the secret message. In addition, the dealer announces to Alice, Bob and Charlie the particle sequences in their registers.

(ii) After receiving the registers, the participants reconcile and divide randomly the corresponding particles in their registers into two modes, i.e. the detecting mode and message mode. There are $n_1 = n - 3$ particles in the detecting mode for each participant. This mode is employed to detect the channel disturbance (noise and Eve's eavesdropping etc.). In the message mode there are only three particles in each quantum register. However, three particles are different in each register. For example, particles in three registers may be respectively $\{p_a^i, p_b^i, p_m^k\}$, $\{p_b^i, p_m^j, p_a^k\}$ and $\{p_m^i, p_a^j, p_b^k\}$, where i, j, k denote sequence-numbers of particles in the quantum register. The message mode will be employed for the recovery of the secret message.

(iii) In the detecting mode, each participant selects correspondingly n_1 particles from the hold register. Then all of the participants measure independently the particles of each entanglement state with the measurement basis (MB) $\mathcal{M}_1$ or $\mathcal{M}_2$, where $\mathcal{M}_1 = \{|u\rangle, |v\rangle\}$ and $\mathcal{M}_2 = \{|x\rangle, |y\rangle\}$ with $|u\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|v\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, $|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$ and $|y\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$. For example, Alice, Bob and Charlie may choose randomly one MB to measure the first particle corresponding to the state $|\Psi_1\rangle$ in their registers. Based on the relations $|0\rangle = \frac{1}{\sqrt{2}}(|u\rangle + |v\rangle) = \frac{1}{\sqrt{2}}(|x\rangle + |y\rangle)$ and $|1\rangle = \frac{1}{\sqrt{2}}(|u\rangle - |v\rangle) = \frac{1}{\sqrt{2}i}(|x\rangle - |y\rangle)$, the state $|\Psi_1\rangle$ can be expressed as

$$\begin{aligned}|\Psi_1\rangle =& \frac{1}{2\sqrt{2}}((|u_a u_b\rangle - |v_a v_b\rangle) \otimes (\alpha - \beta)(|0_m\rangle - |1_m\rangle) \\ &+ (|v_a u_b\rangle - |u_a v_b\rangle) \otimes (\alpha + \beta)(|0_m\rangle + |1_m\rangle)) \\ =& \frac{1}{2\sqrt{2}i}((|x_a x_b\rangle - |y_a y_b\rangle) \otimes (\alpha - \beta)(|0_m\rangle - |1_m\rangle) \\ &+ (|y_a x_b\rangle - |x_a y_b\rangle) \otimes (\alpha + \beta)(|0_m\rangle + |1_m\rangle)). \end{aligned} \quad (3)$$

It implies that Charlie's measurement outcomes are decided by Alice and Bob's MB. If Alice and Bob choose the same MB in $\mathcal{M}_1$ (or $\mathcal{M}_2$) to measure their particles, Charlie's should obtain the state $\frac{\alpha - \beta}{2}|v_m\rangle$ (or $\frac{\alpha - \beta}{2i}|v_m\rangle$). If Alice and Bob choose the different MB in $\mathcal{M}_1$ (or $\mathcal{M}_2$) to measure their particles, Charlie's should obtain the state $\frac{\alpha + \beta}{2}|u_m\rangle$ (or $\frac{\alpha + \beta}{2i}|u_m\rangle$). In a similar way, the other correction relations of particles of the entangled state $|\Psi_i\rangle$ may be described in Table 1. Based on the correction relations of particles of each entanglement state, the participants may judge whether the quantum channel is eavesdropped by Eve or destroyed by the noise. If the correction relations are perfect, the participants proceed with the following steps. Otherwise, QSS is aborted.

Table 1. Relations of MBs and the states of Alice, Bob and Charlie. For simplicity, the subscript m on the states of Charlie has been omitted.

	$\|u_b\rangle$	$\|v_b\rangle$	$\|x_b\rangle$	$\|y_b\rangle$
$\|u_a\rangle$	$\frac{\alpha-\beta}{2}\|v\rangle$	$\frac{-\alpha+\beta}{2}\|u\rangle$	$\frac{-\beta\|x\rangle - i\alpha\|y\rangle}{2}$	$\frac{-\beta\|y\rangle + i\alpha\|x\rangle}{2}$
$\|v_a\rangle$	$\frac{\alpha+\beta}{2}\|u\rangle$	$\frac{\beta-\alpha}{2}\|v\rangle$	$\frac{\beta\|y\rangle - i\alpha\|x\rangle}{2}$	$\frac{\beta\|x\rangle + i\alpha\|y\rangle}{2}$
$\|x_a\rangle$	$\frac{\alpha\|x\rangle + i\beta\|y\rangle}{2}$	$\frac{-\alpha\|y\rangle + i\beta\|x\rangle}{2}$	$\frac{\alpha-\beta}{2i}\|v\rangle$	$\frac{-\alpha-\beta}{2i}\|u\rangle$
$\|y_a\rangle$	$\frac{\alpha\|y\rangle - i\beta\|x\rangle}{2}$	$\frac{-\alpha\|x\rangle - i\beta\|y\rangle}{2}$	$\frac{\alpha+\beta}{2i}\|u\rangle$	$\frac{\beta-\alpha}{2i}\|v\rangle$

(iv) Cooperation of any two participants may restore the secret message $|\phi_m\rangle$ by making use of the remaining entanglement states, i.e. the message mode. Without loss of generality, we assume that Bob and

Charlie select the first corresponding particles p_b and p_m of the state $|\Psi_1\rangle$ from their own registers. They perform CNOT gate C_{bc} on p_b and p_m, i.e.

$$\begin{aligned} C_{bc}|\Psi_1\rangle =& \frac{1}{\sqrt{2}}(\alpha|0_a1_b1_m\rangle + \beta|0_a1_b0_m\rangle - \alpha|1_a0_b1_m\rangle \\ & - \beta|1_a0_b0_m\rangle) \\ =& |\Phi\rangle \otimes |\phi'_m\rangle, \end{aligned} \tag{4}$$

where $|\phi'_m\rangle = \alpha|1_m\rangle + \beta|0_m\rangle$. After performing the operation $P_z = |0_m\rangle\langle 1_m| + |1_m\rangle\langle 0_m|$ on the resulting state $|\phi'_m\rangle$, Bob and Charlie obtain the secret message $|\phi_m\rangle$, i.e. $|\phi_m\rangle = P_z|\phi'_m\rangle$. In a similar way, Alice and Charlie (or Alice and Bob) can also obtain the state $|\phi'_m\rangle$ by performing CNOT gate C_{ca} on p_a and p_m of the state $|\Psi_2\rangle$ (or by performing CNOT gate C_{ab} on p_a and p_b of the state $|\Psi_3\rangle$),

$$\begin{aligned} C_{ca}|\Psi_2\rangle &= |\Phi\rangle \otimes |\phi'_m\rangle, \\ C_{ab}|\Psi_3\rangle &= |\Phi\rangle \otimes |\phi'_m\rangle. \end{aligned} \tag{5}$$

Thus, any two parties can obtain the secret message $|\phi_m\rangle$ after performing P_z on the resulting state $|\phi'_m\rangle$; however, no single communicator can gain the secret message. This implies that the proposed scheme is a (2, 3) quantum threshold scheme.

We note that the $3n$ particles are randomly stored in three different registers except that the three particles of the i^{th} row in Fig. 1 consists of the entanglement state $|\Psi_i\rangle$. Moreover, three participants can also share the secret message by making use of only one entanglement state used in the present scheme. Without loss of generality, assume that the state $|\Phi_1\rangle$ is utilized for sharing the secret message $|\phi_m\rangle$. In this case, Charlie, who owns the particle p_m, must take part in the communications to restore the secret message. Though Alice and Bob would recover the secret message, they can not extract the secret message from p_a and p_b since the secret message has been carried by the particle p_m hold by Charlie.

So far, we have presented a three-party QSS scheme. Now we are faced with the problem of protecting the secret message against Eve's eavesdropping and the dishonest participants' cheating. In the following we analyse the security of the proposed scheme.

Suppose Eve may access to the quantum channel. To acquire the secret message, Eve would capture the particles in the quantum registers and replace them with her own particles prepared in advance. However, this attack strategy can be detected by the participants using the correction relations of their single-qubit states of the three-particle entangled state in the detecting mode, i.e. step (iii). Even if in a serious case of an insider, say Bob, cooperating with Eve, the eavesdropping can also be detected. The present scheme is based on the three-qubit entanglement state, so the proof of the security is the same in essence as those in Ref. [1,7,15]. Thus the present scheme is secure against such a kind of attack strategy.

Assume that Eve who may be a collaborator of dishonest Bob follows a complicated strategy by entangling her ancilla system with the states of the receivers in the general form,

$$|\Xi\rangle_{abce} = \sum_{i,j,k} |i_a j_b k_m\rangle \otimes |\eta_{ijk}\rangle, \tag{6}$$

where $|\eta_{ijk}\rangle$ is an un-normalized state. Eve wants to make this entanglement in order that some useful information about the secret message can be collected in her ancilla system at the end of each round of sending and receiving. Eve is clever enough to entangle her state such that she does not perturb the values of the final qubits measured by every receiver when the scheme is run. She may obtain the ideal form of entanglement denoted by

$$\begin{aligned} |\Xi\rangle_{abce} =& \alpha|010\rangle|\eta_{010}\rangle + \beta|011\rangle|\eta_{011}\rangle - \alpha|101\rangle|\eta_{101}\rangle \\ & - \beta|100\rangle|\eta_{100}\rangle, \end{aligned} \tag{7}$$

where the subscripts a, b and m on the states of the receivers have been omitted. If Eve keeps any other states in Eq. (7), say one of the states in the set $\{|001\rangle|\eta_{001}\rangle, |000\rangle|\eta_{000}\rangle, |110\rangle|\eta_{110}\rangle, |111\rangle|\eta_{111}\rangle\}$, she can be detected by the participants.

One may argue that Eve may not want to completely avoid any error introduced into the distributed state and she may entangle her system to the state $|\Phi\rangle$ in order to reduce the error rate as low as possible, lower than the expected level of noise to escape the detection. Next, we show that even if we allow Eve a small error rate, she cannot find any form of entanglement of her system to the state $|\Phi\rangle$ to achieve the secret message.

Suppose that Eve entangles her system to the state $|\Psi_1\rangle$ in the general form

$$|\Xi\rangle_{abce} = \sum_{i=0}^{7} (\alpha|i\rangle|\eta_i^\alpha\rangle + \beta|i\rangle|\eta_i^\beta\rangle), \tag{8}$$

where for simplicity we have used binary notation for i. After performing $CNOT$ gate C_{bc}, Eve obtains

$$\begin{aligned} C_{bc}|\Xi\rangle_{abce} =& \sum_{i=0,1,4,5} (\alpha|i\rangle|\eta_i^\alpha\rangle + \beta|i\rangle|\eta_i^\beta\rangle) \\ & + \sum_{i=2,3,6,7} (\alpha|i\rangle|\eta_{i+(-1)^i}^\alpha\rangle + \beta|i\rangle|\eta_{i+(-1)^i}^\beta\rangle). \end{aligned} \tag{9}$$

In order to reduce the probability of unwanted qubits introduced into the distributed states below a tolerable threshold ϵ, she should choose the proper states $\{|\eta_i\rangle : 0 \le i \le 7\}$ such that

$$\alpha^2(\langle\eta_2^\alpha|\eta_2^\alpha\rangle + \langle\eta_5^\alpha|\eta_5^\alpha\rangle) + \beta^2(\langle\eta_3^\beta|\eta_3^\beta\rangle + \langle\eta_4^\beta|\eta_4^\beta\rangle) \ge 1 - \epsilon. \tag{10}$$

Thus, the probability of Eve obtaining the correct qubits can be calculated as

$$P_c = \alpha^2(\langle\eta_2^\alpha|\eta_2^\alpha\rangle + \langle\eta_5^\alpha|\eta_5^\alpha\rangle) + \beta^2(\langle\eta_3^\beta|\eta_3^\beta\rangle + \langle\eta_4^\beta|\eta_4^\beta\rangle). \tag{11}$$

Under this condition, the mutual information of Eve and the secret message can be calculated as

$$I(E, |\phi_m\rangle) = 1 - H(P_c), \tag{12}$$

where $H(x)$ is the Shannon binary entropy, i.e. $H(x) = -x \log x - (1-x)\log(1-x)$. To obtain the maximum information on the secret message, the tolerable threshold ϵ should be equal to $1/2$. Thus, the probability of detecting Eve is $P_d = 1/2$, which may be large enough for Eve to be detected by the participants in the detecting mode.

Compared to the previous QSS schemes,[1−12] the quantum registers, which play important roles in the proposed schemes, are employed. In addition, two modes are employed in procedures of the QSS. One mode is employed to check entanglement perfectness of the encoded state, and the other is employed to recover the secret messages. Thus, it is more convenient to detect Eve and restore the secret messages directly without pronouncing any classical information beforehand each scheme run. If an eavesdropper or a cheater has entangled an ancilla with three-particle state, errors will be introduced, which can be detected by the participants using $3n_1$ particles in the detecting mode. The security of the secret message is also guaranteed by the entanglement of the encrypted state as carried out in the previous schemes. However, the present scheme has an advantage that the legal participants can always restore the deterministic quantum message without the assistance of the remaining participants in the message mode.

We have proposed a three-party QSS scheme based on three different quantum registers. This scheme can be generalized to a multi-party QSS scheme for the multi-qubit message. Suppose that there are N parties. Firstly the dealer prepares a two-particle state $|\Phi\rangle$ and the $(N-2)$-qubit secret message

$$|\Theta\rangle = \sum_{i=0}^{2^{N-2}-1} \alpha_i |i\rangle, \tag{13}$$

where $\sum_{i=0}^{2^{N-2}-1} |\alpha_i|^2 = 1$. The dealer chooses randomly u ($u \leq N-2$) qubits of $|\Theta\rangle$ (denoted by $p_m^{(u)}$) as the target qubits, and performs CNOT gates $C_{ap_m^{(u)}}$ on p_a and $p_m^{(u)}$ of the state $|\Phi\rangle \otimes |\Theta\rangle$ to generate an N-qubit entanglement state, i.e.

$$|\Psi_1^{(G)}\rangle = C_{ap_m^{(u)}}(|\Phi\rangle \otimes |\Theta\rangle). \tag{14}$$

In similar ways, the dealer obtains n ($n \geq N+1$) identical N-qubit entanglement states $|\Psi_i^{(G)}\rangle$ for $i = 1, 2, \ldots n$, i.e. $|\Psi_1^{(G)}\rangle = |\Psi_2^{(G)}\rangle = \cdots = |\Psi_n^{(G)}\rangle$. These states are stored respectively in N registers R_a, R_b, $R_c, \ldots$, in which all particles of these N-qubit states are arranged with different sequences in the similar way as described in Fig. 1. The dealer sends N registers R_a, R_b, R_c, ... to N participants, i.e. Alice, Bob, Charlie, ..., respectively. In the detecting mode, all of the participants can check the security of particle-transmission channel by making use of the relations of N single-qubit states of the N-particle entangled state as described in the detecting mode in three-partite QSS scheme. In the message mode, Bob and u other parties who hold $p_m^{(u)}$ qubits of the target qubits of the state $|\Theta\rangle$ in Eq. (14) are needed to restore the secret message $|\Theta\rangle$. After applying CNOT gates $C_{bp_m^{(u)}}$ on p_b and $p_m^{(u)}$, they obtain

$$C_{bp_m^{(u)}} |\Psi_1^{(G)}\rangle = |\Phi\rangle \otimes |\Theta'\rangle. \tag{15}$$

Utilizing the same ways as in the proposed three-party QSS scheme, these $u+1$ receivers gain the secret message $|\Theta\rangle$ after applying the operation P_z on these u target qubits of the resulting state $|\Theta'\rangle$. This implies that the present scheme is a $(u+1, N)$ quantum threshold scheme.

In summary, we have proposed a three-party QSS scheme using quantum registers with two communication modes. The secret message is encoded by the dealer into a three-particles entangled state, and every particle is distributed to three different registers. Then two modes are employed for the eavesdropping and cheating detections and the secret message recovery, respectively. In the detecting mode, the participants check Eve's eavesdropping and the dishonest participants' cheating on the transmitted state. In the message mode, the cooperation of any two participants may recover the deterministic secret message. Security analysis shows that the proposed scheme is secure against Eve's eavesdropping and the participants' cheating. Finally, we generalize the proposed three-party QSS scheme to a multi-party QSS scheme.

References

[1] Hillery M, Buzek V and Berthiaume A 1999 *Phys. Rev.* A **59** 1829
[2] Karlsson A, Koashi M and Imoto N 1999 *Phys. Rev.* A **59** 162
[3] Gottesman D 2000 *Phys. Rev.* A **61** 042311
[4] Tittel W, Zbinden H and Gisin N 2001 *Phys. Rev.* A **63** 042301
[5] Karimipour V and Bahraminasab A 2002 *Phys. Rev.* A **65** 042320
[6] Chau H F 2002 *Phys. Rev.* A **66** 060302
[7] Bagherinezhad S and Karimipour V 2003 *Phys. Rev.* A **67** 044302
[8] Guo G P and Guo G C 2003 *Phys. Lett.* A **310** 247
[9] Cleve R, Gottesman D and Lo H K 1999 *Phys. Rev. Lett.* **83** 648
[10] Bandyopadhyay S 2000 *Phys. Rev.* A **62** 012308
[11] Hsu L Y 2003 *Phys. Rev.* A **68** 022306
[12] Lance A M, Symul T, Bowen W P, Sanders B C and Lam P K 2004 *Phys. Rev. Lett.* **92** 177903
[13] Pittman T B and Franson J D 2003 *Phys. Rev. Lett.* **90** 240401
[14] Rohde P P, Pryde G J et al 2005 *Phys. Rev.* A **72** 039906
[15] Waks E, Zeevi A and Yamamoto Y 2002 *Phys. Rev.* A **65** 052310