# Two-way protocols for quantum cryptography with a nonmaximally entangled qubit pair

Kaoru Shimizu,[1,2,*] Kiyoshi Tamaki,[1] and Hiroyuki Fukasaka[2,1]

[1]*NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosato-Wakamiya, Atsugi, Kanagawa 243-0198, Japan*

[2]*Nara Institute of Science and Technology, 8916-5 Takayama-cho, Ikoma, Nara 630-0192, Japan*

(Received 26 December 2008; published 19 August 2009)

This paper proposes a scheme for quantum cryptography with a nonmaximally entangled qubit pair. In a two-way configuration similar to quantum super dense coding, a two-bit key can be distributed by a round trip of one particle of the qubit pair and received by an appropriate joint measurement with the other. The security of our scheme is based on the quantum-mechanical impossibility of local unitary transformation between certain nonmaximally entangled states. Although an eavesdropper, Eve, can always identify the quantum state and intercept the key, it is impossible for her to resend the state with a unity probability and the legitimate parties inevitably detect her. Our protocol is also capable to quantum secure direct communication.

DOI: 10.1103/PhysRevA.80.022323 PACS number(s): 03.67.Dd, 03.65.Ud

## I. INTRODUCTION

The fundamental laws of quantum mechanics ensure the security of quantum cryptography thus making it possible for legitimate parties to distribute private keys in a secure way by communicating with a quantum object [1]. In particular, the security of the standard protocols for quantum cryptography relies directly on the uncertainty principle as regards a set of nonorthogonal quantum states, where an eavesdropper cannot access a classical bit carried by the quantum object without leaving a back action of the illegitimate intervention [1,2].

There are certain other protocols that employ different aspects of quantum mechanics to guarantee security. Goldenberg and Vaidman presented a quantum cryptography scheme based on orthogonal states that are represented by the superposition of two localized wave packets [3,4]. Recently, Boström and Felbinger proposed the "ping-pong protocol" with maximally entangled states of a qubit pair [5]. Based on the idea of the quantum super dense coding [6], they proposed a simple framework for the secure transmission of one bit of information encoded by the local operation on one particle of the qubit pair. Detailed security studies and improvements have been reported for the ping-pong protocol [7,8].

This paper presents another framework for the two-way protocol, where a two-bit key can be distributed with one particle of a qubit pair. Instead of using standard maximally entangled states [5,6], our framework utilizes nonmaximally entangled states [9]. The security of the protocol is based on the quantum-mechanical constraint for a state transformation between nonmaximally entangled states of a qubit pair. Our proposed scheme can be executed with a two-way configuration similar to the quantum super dense coding that we outline below [6]. (i) Alice prepares the Bell state $|\Phi^{+}\rangle_{AB}$ composed of a pair of particles $A$ and $B$ and sends only particle $B$ to Bob. (ii) Bob can transform the initial Bell state $|\Phi^{+}\rangle_{AB}$ to any of four different Bell states;

$$|\Phi^{\pm}\rangle = (|11\rangle \pm |00\rangle)/\sqrt{2} \quad \text{and} \quad |\Psi^{\pm}\rangle = (|10\rangle \pm |01\rangle)/\sqrt{2}$$

by applying the appropriate local spin rotation for particle $B$ and therefore can encode two bits of information in the pair. (iii) Bob returns particle $B$ to Alice. (iv) Alice can decode the two bits of information by performing a joint measurement for the pair with the Bell state basis.

At first glance, the quantum super dense coding appears to be secure from eavesdropping. This is because Alice, who retains particle $A$, seems to be the only person who can decode the two bits of information. However, this is incorrect. An eavesdropper Eve can always impersonate Alice by inserting a dummy Bell state $|\Phi^{+}\rangle_{EB'}$ so that she can intercept the two bits of information and then encode the same information again by manipulating particle $B$ sent back to Alice.

The insecurity of the quantum super dense coding is attributed to the fact that the four different Bell states $\{|\Phi^{+}\rangle, |\Phi^{-}\rangle, |\Psi^{+}\rangle, |\Psi^{-}\rangle\}$ are the maximally entangled states of a qubit pair, and therefore Eve can always transform the initial Bell state $|\Phi^{+}\rangle$ to any of the Bell states in a deterministic way by accessing only particle $B$. This observation, however, enables us to design a scheme for secure communication by replacing the orthogonal set of Bell states with an orthogonal set of certain nonmaximally entangled states. This paper is in line with this motivation. Section II describes characteristics of a set of nonmaximally entangled states for a qubit pair. Section III describes our basic protocol of quantum cryptography with the nonmaximally entangled qubit pair. Sections IV and V improve the basic protocol in such a way that a two-bit key can be distributed with particle $B$.

## II. CHARACTERISTICS OF NONMAXIMALLY ENTANGLED STATES

As Alice always retains particle $A$, the only unitary operation possible for Bob is the local spin rotation $F_B$ for particle $B$;

$$\begin{aligned} F_B(\alpha,\beta,\gamma) &= \begin{bmatrix} e^{i(\alpha+\gamma)/2}\cos(\beta/2) & e^{-i(\alpha-\gamma)/2}\sin(\beta/2) \\ -e^{i(\alpha-\gamma)/2}\sin(\beta/2) & e^{-i(\alpha+\gamma)/2}\cos(\beta/2) \end{bmatrix} \\ &= \cos(\beta/2)\cos[(\alpha+\gamma)/2]E_B \\ &\quad + i\cos(\beta/2)\sin[(\alpha+\gamma)/2]Z_B \\ &\quad - i\sin(\beta/2)\sin[(\alpha-\gamma)/2]X_B \\ &\quad + i\sin(\beta/2)\cos[(\alpha-\gamma)/2]Y_B. \end{aligned} \tag{1}$$

[*] Corresponding author; shimizu@will.brl.ntt.co.jp

©2009 The American Physical Society

Here $(\alpha,\beta,\gamma)$ means the Euler angles for spin rotation. All the possible spin rotations can be expressed with the identity matrix $E_B$ and a set of three different Pauli matrices $X_B$, $Y_B$, and $Z_B$ as shown above.

By adjusting the Euler angles, Bob can transform the initial Bell state $|\Phi^+\rangle$ into any Bell state as $iX_B|\Phi^+\rangle_{AB} = i|\Psi^+\rangle_{AB}$, $iY_B|\Phi^+\rangle_{AB}=-|\Psi^-\rangle_{AB}$, and $iZ_B|\Phi^+\rangle_{AB}=i|\Phi^-\rangle_{AB}$. The four different Bell states are the maximally entangled states of the qubit pair. Here we introduce the concurrence $C$ to quantify the entanglement for the qubit pair [10]. All the maximally entangled states are characterized with $C=1$ and can be transformed into each other by an appropriate local spin rotation $F_B(\alpha,\beta,\gamma)$.

In contrast, when the quantum state of the spin pair is a nonmaximally entangled state, the transformation between two different orthogonal states is not always possible with the local spin rotation $F_B$ even when the two states are characterized with the same concurrence value. For example, here we introduce two different entangled states $\{|\mu^1\rangle,|\mu^2\rangle\}$ as follows:

$$\begin{aligned}|\mu^1\rangle &= \cos\,\theta|\Phi^+\rangle_{AB} - \sin\,\theta|\Phi^-\rangle_{AB}\\ &= \cos(\theta+\pi/4)|11\rangle_{AB} + \cos(\theta-\pi/4)|00\rangle_{AB},\end{aligned} \tag{2a}$$

$$\begin{aligned}|\mu^2\rangle &= \sin\,\theta|\Phi^+\rangle_{AB} + \cos\,\theta|\Phi^-\rangle_{AB}\\ &= \cos(\theta-\pi/4)|11\rangle_{AB} - \cos(\theta+\pi/4)|00\rangle_{AB},\end{aligned} \tag{2b}$$

where $\theta$ is a parameter angle set at $0<\theta<\pi/4$. The entangled states $|\mu^1\rangle$ and $|\mu^2\rangle$ are orthogonal and have the same concurrence value $C=|\cos 2\theta|$ less than unity.

As the concurrence must be invariant for all the entangled states that are transformable with the local spin rotation $F_B$, Bob cannot alter the initial Bell state $|\Phi^+\rangle_{AB}$ into either $|\mu^1\rangle$ or $|\mu^2\rangle$ by any local spin rotation. Actually, the spin rotation $F_B(-\theta,0,-\theta)$ results in $\cos\,\theta|\Phi^+\rangle_{AB} - i\,\sin\,\theta|\Phi^-\rangle_{AB}$ instead of the expected $|\mu^1\rangle(=\cos\,\theta|\Phi^+\rangle_{AB}-\sin\,\theta|\Phi^-\rangle_{AB})$.

Moreover, the states $|\mu^1\rangle$ and $|\mu^2\rangle$ cannot be transformed into each other by any local spin rotation even when they have the same concurrence value $|\cos 2\theta|$. We can confirm this point as follows. We assume that (i) the initial state of the spin pair is $|\mu^1\rangle$ and Bob has particle $B$, and (ii) he wants to transform $|\mu^1\rangle$ to $|\mu^2\rangle$. As the quantum state of particle $A$ is out of Bob's control, his desired transformation is equivalent to the change in the density matrix of particle $B$ from $\rho^{\,1)} \equiv \mathrm{Tr}_A|\mu^1\rangle\langle\mu^1|$ to $\rho^{\,2)} \equiv \mathrm{Tr}_A|\mu^2\rangle\langle\mu^2|$, where the state of particle $A$ is traced out. The density matrices are given by

$$\rho^{\,1)} = \begin{bmatrix}\cos^2(\theta+\pi/4) & 0\\ 0 & \cos^2(\theta-\pi/4)\end{bmatrix},$$

$$\rho^{\,2)} = \begin{bmatrix}\cos^2(\theta-\pi/4) & 0\\ 0 & \cos^2(\theta+\pi/4)\end{bmatrix}.$$

These two density matrices exhibit different diagonal matrices except for $\theta=0$. Hence, there is no unitary operation for particle $B$ that can transform the state $|\mu^1\rangle$ into $|\mu^2\rangle$.

The pair of orthogonal states $|\mu^1\rangle$ and $|\mu^2\rangle$ is a set of nonmaximally entangled states that are not transformable with the local spin rotation $F_B$ while having the same concurrence. To transform the initial Bell state $|\Phi^+\rangle_{AB}$ in a unitary way to either state $|\mu^1\rangle$ or $|\mu^2\rangle$, Bob has to manipulate the state of particle $B$ depending on the quantum state of particle $A$. This involves the interaction of the two spins and is impossible for Bob to execute without accessing particle $A$.

Nevertheless, if Bob can introduce an appropriately designed local nonunitary operation for particle $B$ and his ancilla, it is not impossible for Bob to execute a nondestructive projection to either state $|\mu^1\rangle$ or $|\mu^2\rangle$ while having knowledge of the projection result. His local nonunitary operation is as follows. (i) Bob prepares an ancilla that is defined in a two-dimensional Hilbert space $\{|\phi^1\rangle_C,|\phi^2\rangle_C\}$ and sets the initial state $|\phi^1\rangle_C$. (ii) Bob executes the following entangling operation $K_{BC}$ for particle $B$ of the Bell state $|\Phi^+\rangle_{AB}$ and his ancilla;

$$K_{BC}|\Phi^+\rangle_{AB}|\phi^1\rangle_C = |\Phi^+\rangle_{AB}|\phi^1\rangle_C/\sqrt{2} + i|\Phi^-\rangle_{AB}|\phi^2\rangle_C/\sqrt{2} \tag{3a}$$

(iii) Bob then performs a projection measurement for his ancilla by using another basis $\{|\varphi^1\rangle_C,|\varphi^2\rangle_C\}$ so that the quantum state of the whole system can be represented by

$$K_{BC}|\Phi^+\rangle_{AB}|\phi^1\rangle_C = |\mu^1\rangle|\varphi^1\rangle_C/\sqrt{2} + |\mu^2\rangle|\varphi^2\rangle_C/\sqrt{2}, \tag{3b}$$

where $|\varphi^1\rangle_C=\cos\,\theta|\phi^1\rangle_C - i\,\sin\,\theta|\phi^2\rangle_C$ and $|\varphi^2\rangle_C = \sin\,\theta|\phi^1\rangle_C + i\,\cos\,\theta|\phi^2\rangle_C$. His projection outcome $|\varphi^1\rangle_C/|\varphi^2\rangle_C$ for the ancilla reveals the resulting quantum state $|\mu^1\rangle/|\mu^2\rangle$ of the qubit pair. However, it is impossible for Bob to manipulate particle $B$ and the ancilla in such a way that either desired state can be achieved in a deterministic way.

## III. PRIVATE KEY DISTRIBUTION PROTOCOL WITH NONMAXIMALLY ENTANGLED STATES

In a two-way configuration similar to quantum super dense coding, Alice and Bob can distribute a one-bit private key by communicating with particle $B$ provided that they replace the Bell states with the nonmaximally entangled states $|\mu^1\rangle$ and $|\mu^2\rangle$. This section describes the basic concept of a two-way protocol for quantum cryptography with a nonmaximally entangled qubit pair.

To describe an arbitrary quantum state of the qubit pair, we introduce another set $\{|\mu^3\rangle,|\mu^4\rangle\}$ of nonmaximally entangled states;

$$|\mu^3\rangle = \cos\,\theta|\Psi^+\rangle_{AB} - \sin\,\theta|\Psi^+\rangle_{AB}, \tag{4a}$$

$$|\mu^4\rangle = \sin\,\theta|\Psi^+\rangle_{AB} + \cos\,\theta|\Psi^+\rangle_{AB}. \tag{4b}$$

The entangled states $|\mu^3\rangle$ and $|\mu^4\rangle$ are orthogonal and have the same concurrence value $C=|\cos 2\theta|$ in the same way as $|\mu^1\rangle$ and $|\mu^2\rangle$. Moreover, the states $|\mu^3\rangle$ and $|\mu^4\rangle$ are not transformable with the local spin rotation $F_B$. The set of four different nonmaximally entangled states

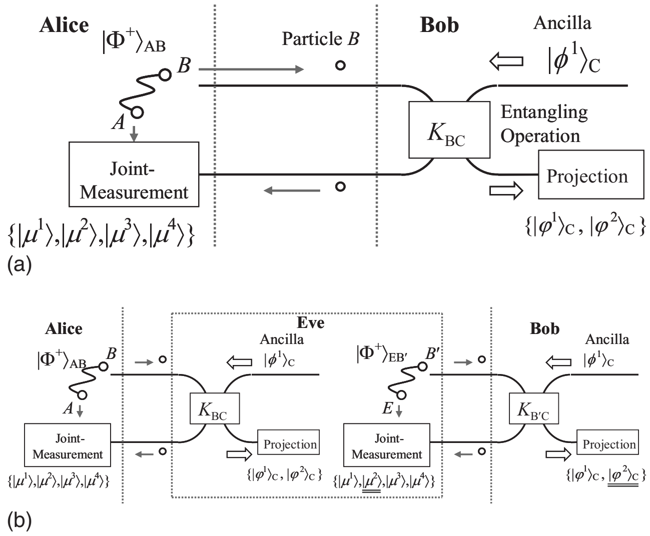
Alice
$|\Phi^+\rangle_{AB}$
Particle $B$
$B$
$A$
Bob
Ancilla
$|\phi^1\rangle_C$
$K_{BC}$
Entangling Operation
Joint-Measurement
Projection
$\{|\mu^1\rangle,|\mu^2\rangle,|\mu^3\rangle,|\mu^4\rangle\}$
$\{|\varphi^1\rangle_C,|\varphi^2\rangle_C\}$
(a)
Alice
Eve
Bob
Ancilla
$|\phi^1\rangle_C$
$|\Phi^+\rangle_{AB}$
$|\Phi^+\rangle_{EB'}$
$B$
$B'$
$A$
$E$
$K_{BC}$
$K_{B'C}$
Joint-Measurement
Projection
$\{|\mu^1\rangle,|\mu^2\rangle,|\mu^3\rangle,|\mu^4\rangle\}$
$\{|\varphi^1\rangle_C,|\varphi^2\rangle_C\}$
$\{|\mu^1\rangle,\underline{\underline{|\mu^2\rangle}},|\mu^3\rangle,|\mu^4\rangle\}$
$\{|\varphi^1\rangle_C,\underline{\underline{|\varphi^2\rangle_C}}\}$
(b)

FIG. 1. (a) Schematic configuration for protocol A. (b) Intercept and resend strategy of an eavesdropper for protocol A.

$\{|\mu^1\rangle,|\mu^2\rangle,|\mu^3\rangle,|\mu^4\rangle\}$ is a complete orthogonal basis for the qubit pair. However, the states $|\mu^1\rangle$ and $|\mu^3\rangle$ are mutually transformable with the local spin rotation $iX_B$. This relation also holds for the pair of states $|\mu^2\rangle$ and $|\mu^4\rangle$.

We propose a two-way protocol for quantum key distribution. Figure 1(a) shows the configuration of the quantum channel.

*Protocol A.* Distribution of one bit of key.

(A1) Alice prepares the Bell state $|\Phi^+\rangle_{AB}$ of the qubit pair and sends particle $B$ to Bob while retaining particle $A$.

(A2) Bob prepares the ancilla system $\{|\phi^1\rangle_C,|\phi^2\rangle_C\}$ and executes the local nonunitary operation for particle $B$ as detailed in the previous section. His local nonunitary operation is composed of the entangling operation $K_{BC}$ for particle $B$ with the ancilla and a subsequent projection measurement for the ancilla with the basis $\{|\varphi^1\rangle_C,|\varphi^2\rangle_C\}$. The resulting outcome $|\varphi^1\rangle_C/|\varphi^2\rangle_C$ means $R_B=1/R_B=0$. He then returns particle $B$ to Alice.

(A3) For the pair of particles $A$ and $B$, Alice performs a joint measurement with the projection basis $\{|\mu^1\rangle,|\mu^2\rangle,|\mu^3\rangle,|\mu^4\rangle\}$ instead of the Bell state basis. She regards the projection result $|\mu^1\rangle/|\mu^2\rangle$ as $R_A=1/R_A=0$ and discards the other two outcomes $|\mu^3\rangle$ and $|\mu^4\rangle$ as errors.

(A4) Alice and Bob sample a sufficiently large number of pairs so that they can compare the resulting bit values $R_A$ and $R_B$. If they can observe the expected coincidence $R_A=R_B$ for sufficient pairs, they are convinced that no illegitimate party has accessed the quantum channel. Hence, they can obtain an identical sequence of random bits $R$ from the remaining pairs and use it as a private key.

In step (A2) of protocol A, Bob cannot control the result of his projection measurement in a deterministic way while he can generate a bit consisting of an intrinsic random number. The probabilistic nature of the projection measurement is not an obstacle with respect to Alice and Bob distributing a random number for secret key use. In contrast, this makes it impossible for an eavesdropper to resend the random number.

Figure 1(b) describes the intercept and resend strategy of the eavesdropper. As mentioned in Sec. I, Eve can impersonate Alice by inserting a dummy Bell state $|\Phi^+\rangle_{EB'}$ and can intercept $R_B$ generated by Bob. Let us assume that Eve receives the state $|\mu^2\rangle_{EB'}$ and knows $R_B=0$. Although Eve's interception is successful, it is impossible for her to resend the state $|\mu^2\rangle_{AB}$ with a unity probability. This is because she cannot transform the initial Bell state $|\Phi^+\rangle_{AB}$ into her desired state $|\mu^2\rangle_{AB}$ in a unitary way. If she employs a local nonunitary operation to execute the projection to either state $|\mu^1\rangle$ or $|\mu^2\rangle$, she fails to resend the intercepted state with a half probability and is detected by Alice and Bob. Nobody can eavesdrop successfully provided that Alice retains particle $A$.

Nevertheless, Eve can reduce the probability of detection by employing an improved resend strategy. Specifically, she can choose an appropriate local spin rotation $F_B$ so that the square inner product can be maximized for the states $|\mu^2\rangle$ and $F_B|\Phi^+\rangle_{AB}$. The maximum value of the squared inner product is $\cos^2\theta$ and the detection probability can be minimized to $\sin^2\theta$. The detection probability becomes zero for the limitation $\theta\rightarrow 0$, where the set of states $\{|\mu^1\rangle,|\mu^2\rangle\}$ approaches the maximally entangled states $\{|\Phi^+\rangle_{AB},|\Phi^-\rangle_{AB}\}$.

On the other hand, when the parameter angle $\theta$ is close to $\pi/4$, Eve can reduce the detection probability to $\cos^2 2\theta/2$ by accessing only particle $B$ with the $\{|1\rangle_B,|0\rangle_B\}$ basis. Her available information gain is given by $1+\cos^2(\theta+\pi/4)\log_2\{\cos^2(\theta+\pi/4)\}+\cos^2(\theta-\pi/4)\log_2\{\cos^2(\theta-\pi/4)\}$ which is less than unity. The states $\{|\mu^1\rangle,|\mu^2\rangle\}$ approach the product states $\{|00\rangle,|11\rangle\}$ for the limitation $\theta\rightarrow\pi/4$, where the detection probability and the available information gain approach zero and one bit, respectively. In conclusion, Alice and Bob should choose a parameter angle $\theta$ of around $\pi/7$ so that they can ensure a detection probability of at least 1/5. The Appendix provides a formal security proof concerning general individual attacks including the typical strategies described above.

However, the above security analysis is restricted to independent attacks to particle $B$ for each run of the protocol. If any classical or quantum error correction code is introduced for a set of sequential particles $B$, we have to consider collective or coherent attacks to the set. Full security analysis for those attacks is rather important [1] though this task is beyond the scope of this paper.

Finally, we should mention the tolerance to the transmission loss. If particle $B$ is transmitted through a very dissipative channel, Eve can escape detection by resending no particle whenever an undesirable result is obtained from her projection measurement. To conceal the unavoidable reduction in the transmission rate, Eve may secretly replace the dissipative channel with a lossless channel if such a transparent medium is available. However, Alice and Bob can defeat this strategy by introducing the following option:

*Option A5.* "Control mode." Bob sometimes measures particle $B$ with the $\{|1\rangle,|0\rangle\}$ basis and requests Alice to measure particle $A$ with the $\{|1\rangle,|0\rangle\}$ basis. Eve's strategy of inserting a dummy Bell state $|\Phi^+\rangle_{EB'}$ results in an unanticipated correlation for Alice and Bob with a half probability. This is exactly the control mode proposed in the ping-pong protocol [5].

## IV. ENHANCING KEY DISTRIBUTION CAPACITY AND SECURE DIRECT COMMUNICATION

Protocol A utilizes the two orthogonal states $\{|\mu^1\rangle, |\mu^2\rangle\}$ belonging to the complete orthogonal basis $\{|\mu^1\rangle, |\mu^2\rangle, |\mu^3\rangle|\mu^4\rangle\}$ of the qubit pair and therefore a one-bit key is distributed with particle $B$. This section shows that full use of the four orthogonal states enhances the key distribution capacity and also results in a scheme for quantum secure direct communication [11,12].

*Protocol B.* Distribution of two bits of key.

(B1) Alice prepares the Bell state $|\Phi^+\rangle_{AB}$ of the qubit pair and sends particle $B$ to Bob while retaining particle $A$.

(B2) Bob prepares the ancilla system $\{|\phi^1\rangle_C, |\phi^2\rangle_C\}$ and executes a local nonunitary operation for particle $B$ in the same way as (A2). His outcome $|\varphi^1\rangle_C / |\varphi^2\rangle_C$ means $R_B = 1/R_B = 0$.

(B3) Bob determines a bit $M_B \in \{1,0\}$. For $M_B = 1$ and $M_B = 0$, he applies nothing and the local spin rotation $iX_B$ on particle $B$, respectively. The local spin rotation $iX_B$ transforms the state $|\mu^1\rangle / |\mu^2\rangle$ into $|\mu^3\rangle / |\mu^4\rangle$. He then returns particle $B$ to Alice.

(B4) Alice performs a joint measurement for the pair of particles $A$ and $B$ with the measurement basis $\{|\mu^1\rangle, |\mu^2\rangle, |\mu^3\rangle, |\mu^4\rangle\}$. She registers her measurement results as follows:

$$|\mu^1\rangle \to (R_A, M_A) = (1,1), \quad |\mu^2\rangle \to (R_A, M_A) = (0,1),$$

$$|\mu^3\rangle \to (R_A, M_A) = (1,0), \quad |\mu^4\rangle \to (R_A, M_A) = (0,0).$$

(B5) Alice and Bob sample a sufficiently large number of pairs so that they can compare their bit values $R_A$ and $R_B$. If they can confirm the coincidence $R_A = R_B$ for a sufficient number of pairs, they can obtain the two-bit key $(R, M)$ from the remaining pair. Figure 2(a) shows the configuration for protocol B.

Hence, protocol B makes it possible for Alice and Bob to enhance the key distribution capacity to two bits with particle $B$. Bit $R$ is an intrinsic random number, while bit $M$ is a random number encoded by Bob. Although an eavesdropper, Eve, can resend bit $M$ with a unity probability, it is impossible for her to resend bit $R$ for the same reason as that described for protocol A.

Here a question arises as to whether or not Eve can obtain only bit $M$ without disturbing the quantum state regarding with bit $R$. The answer is "no" as explained in the following. Even if she accesses only particle $B$ that is returned to Alice, she can obtain no information on bit $M$. This is because the density matrices $\rho^M$ of particle $B$ are identical for $M = 1$ and $M = 0$, where $\rho^{M=1)} = (\rho^{1)} + \rho^{2)})/2$ and $\rho^{M=0)} = (\rho^{3)} + \rho^{4)})/2$ with $\rho^{i)} = \mathrm{Tr}_A |\mu^\iota\rangle\langle\mu^\iota|$ $(i = 1\text{–}4)$. Therefore, she must insert a dummy Bell state $|\Phi^+\rangle_{EB'}$ whenever she intercepts bit $M$ from an appropriate joint projection measurement for the pair of particles $E$ and $B'$. A nondestructive projection measurement (NDPM) to the orthogonal subspaces $\{|\mu^1\rangle, |\mu^2\rangle\}$ and $\{|\mu^3\rangle, |\mu^4\rangle\}$ makes it possible for Eve to reveal bit $M$ without accessing bit $R$.

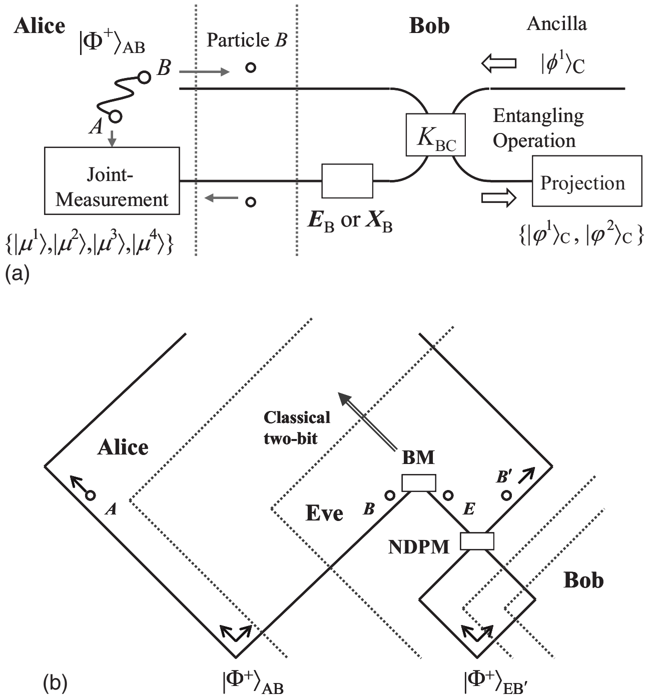

FIG. 2. (a) Schematic configuration for protocol B. (b) Eavesdropping strategy for reading bit $M$ without accessing bit $R$. NDPM, nondestructive projection measurement to the two orthogonal subspaces $\{|\mu^1\rangle, |\mu^2\rangle\}$ and $\{|\mu^3\rangle, |\mu^4\rangle\}$. BM, Bell state measurement.

Although Eve sends only particle $B'$ to Alice, she can resend the entangled state of particles $E$ and $B'$ provided that she can achieve quantum teleportation [13] for particle $E$ as shown in Fig. 2(b) by performing the Bell state measurement with particle $B$ and notifying Alice of the resulting Bell state for the local spin rotation on particle $A$. However, protocol B does not include such a notification process from Bob. Hence, Eve cannot complete the quantum teleportation.

*Protocol B′.* Secure direct communication.

In step (B3) of protocol B, Bob can encode a meaningful message in a bit $M$ sequence instead of encoding random numbers. Alice can decode the message from the sequence while examining the security of the channel by comparing bit $R$ for Alice and Bob. This results in a quantum channel for a kind of secure direct communication [11,12].

## V. DISTRIBUTING TWO-BIT INTRINSIC RANDOM NUMBER

Protocol B makes it possible for Alice and Bob to enhance the key distribution capacity to two bits with particle $B$, where one bit (bit $R$) is the intrinsic random number generated by Bob in a probabilistic way while the other bit (bit $M$) is encoded by Bob in a deterministic way. From a security viewpoint in the classical transmission of the cipher text encrypted with the distributed key, however, the distribution of a two-bit intrinsic random number is preferable. This is because an artificially constructed random number may degrade secrecy of the cipher text if a portion of the key generation algorithm is revealed by Eve.

The distribution of a two-bit intrinsic random number is possible for them by employing certain nonmaximally entangled states of a qubit pair. We introduce an orthogonal set of nonmaximally entangled states $\{|\Phi^1\rangle, |\Phi^2\rangle, |\Phi^3\rangle, |\Phi^4\rangle\}$ defined as

$$|\Phi^1\rangle = (|\Phi^+\rangle_{AB} + |\Phi^-\rangle_{AB})/2 + (|\Psi^+\rangle_{AB} + i|\Psi^-\rangle_{AB})/2, \tag{5a}$$

$$|\Phi^2\rangle = (|\Phi^+\rangle_{AB} + |\Phi^-\rangle_{AB}/2) - (|\Psi^+\rangle_{AB} + i|\Psi^-\rangle_{AB})/2, \tag{5b}$$

$$|\Phi^3\rangle = (|\Phi^+\rangle_{AB} - |\Phi^-\rangle_{AB})/2 + (|\Psi^+\rangle_{AB} - i|\Psi^-\rangle_{AB}/2), \tag{5c}$$

$$|\Phi^4\rangle = (|\Phi^+\rangle_{AB} - |\Phi^-\rangle_{AB}/2) - (|\Psi^+\rangle_{AB} - i|\Psi^-\rangle_{AB})/2. \tag{5d}$$

Here we call the set the Vaidman-Aharonov-Albert (VAA) basis [14]. As the concurrence of the VAA states is 0.5, no VAA state can be transformed from the initial Bell state $|\Phi^+\rangle_{AB}$ with the local spin rotation $F_B$ in a deterministic way. Moreover, the four different VAA states are not transformable with the local spin rotation $F_B$. Actually, the unitary transformation between $|\Phi^1\rangle$ and $|\Phi^2\rangle$ requires the global operation $\exp[i\pi(Z_A - Z_B)^2/4]$ for particles $A$ and $B$, where the operation includes their interaction and is therefore impossible for Bob. Other global operations $\exp[i\pi;(X_A - X_B)^2/4]$ and $\exp[i\pi(Y_A - Y_B)^2/4]$ result in unitary transformations $|\Phi^1\rangle \leftrightarrow |\Phi^3\rangle$ and, $|\Phi^1\rangle \leftrightarrow |\Phi^4\rangle$, respectively.

Nevertheless, Bob can change the initial Bell state $|\Phi^+\rangle_{AB}$ to any of the four VAA states in a probabilistic way by executing an appropriate local nonunitary operation for particle $B$. The local nonunitary operation is as follows. (i) Bob prepares an ancilla that is defined in the four-dimensional Hilbert space $\{|\phi^1\rangle_C, |\phi^2\rangle_C, |\phi^3\rangle_C, |\phi^4\rangle_C\}$ and sets the initial state at $|\phi^1\rangle_C$. (ii) Bob performs the entangling operation $M_{BC}$ for particle $B$ and his ancilla so that the state of the whole system can be represented by

$$M_{BC}|\Phi^+\rangle_{AB}|\phi^1\rangle_C = |\Phi^+\rangle_{AB}|\phi^1\rangle_C/2 + i|\Phi^-\rangle_{AB}|\phi^2\rangle_C/2 + i|\Psi^+\rangle_{AB}|\phi^3\rangle_C/2 + |\Psi^-\rangle_{AB}|\phi^4\rangle_C/2. \tag{6a}$$

(iii) Bob then executes the projection measurement for his ancilla with the basis $\{|\varphi^1\rangle_C, |\varphi^2\rangle_C, |\varphi^3\rangle_C, |\varphi^4\rangle_C\}$, where he can choose the basis so that the quantum state of the whole system is expressed as

$$M_{BC}|\Phi^+\rangle_{AB}|\phi^1\rangle_C = |\Phi^1\rangle|\varphi^1\rangle_C/2 + |\Phi^2\rangle|\varphi^2\rangle_C/2 + |\Phi^3\rangle|\varphi^3\rangle_C/2 + |\Phi^4\rangle|\varphi^4\rangle_C/2. \tag{6b}$$

Equation (6b) determines the one-to-one relationship between his projection result for the ancilla and the resulting VAA state for particles $A$ and $B$. Hence, he can generate a two-bit intrinsic random number.

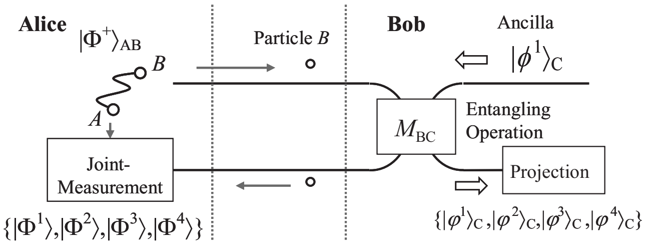
Alice
$|\Phi^+\rangle_{AB}$
B
A
Joint-Measurement
$\{|\Phi^1\rangle,|\Phi^2\rangle,|\Phi^3\rangle,|\Phi^4\rangle\}$
Particle B
Bob
Ancilla
$|\phi^1\rangle_C$
$M_{BC}$
Entangling Operation
Projection
$\{|\varphi^1\rangle_C,|\varphi^2\rangle_C,|\varphi^3\rangle_C,|\varphi^4\rangle_C\}$

FIG. 3. Schematic configuration for protocol C.

In a similar way to that of protocol A, secure distribution of a two-bit intrinsic random number is possible with the four different VAA states.

*Protocol C.* Distribution of two bit intrinsic random number

(C1) Alice prepares the Bell state $|\Phi^+\rangle_{AB}$ of the qubit pair and sends particle $B$ to Bob while retaining particle $A$.

(C2) Bob executes a local nonunitary operation for particle $B$ and his ancilla as described above. He then returns particle $B$ to Alice. He registers the result of his projection measurement as follows:

$$|\varphi^1\rangle_C \to R_B = 11, \quad |\varphi^2\rangle_C \to R_B = 10, \quad |\varphi^3\rangle_C \to R_B = 01, \quad |\varphi^4\rangle_C \to R_B = 00.$$

(C3) Alice performs a joint measurement for particles $A$ and $B$ with the VAA basis $\{|\Phi^1\rangle, |\Phi^2\rangle, |\Phi^3\rangle, |\Phi^4\rangle\}$. She registers her result as follows:

$$|\Phi^1\rangle \to R_A = 11, \quad |\Phi^2\rangle \to R_A = 10, \quad |\Phi^3\rangle \to R_A = 01, \quad |\Phi^4\rangle \to R_A = 00.$$

(C4) In the same way as step (A4) of protocol A, Alice and Bob examine the security of the quantum channel. Figure 3 shows the configuration for protocol C.

The amount of information available from particle $B$ is upper bound by $S[\Sigma_{i=1}^4 \rho_i/4] - \Sigma_{i=1}^4 S(\rho_i)/4$ with a reduced density matrix $\rho_i = \mathrm{Tr}_A|\Phi^i\rangle\langle\Phi^i|$ of particle $B$ and a von Neumann entropy $S(\rho) = -\mathrm{Tr}[\rho \log_2 \rho]$ [1]. The upper bound is evaluated at 0.654 bits and therefore an eavesdropper Eve inserts a dummy Bell state $|\Phi^+\rangle_{EB'}$ to intercept the two-bit information $R_B$. However, as with protocol A, Eve cannot resend the two bits with a unity probability and is inevitably detected. Eve can reduce the probability of detection to 1/4 by optimizing the local spin rotation $F_B$ for particle $B$. In fact, the value of $|\langle\Phi^1|F_B|\Phi^+\rangle|$ is maximized to 3/4 for $F_B(\pi/4, 2\sin^{-1}\sqrt{2/3}, 3\pi/4)$, where $F_B|\Phi^+\rangle = i3|\Phi^1\rangle - |\Phi^2\rangle - |\Phi^3\rangle - |\Phi^4\rangle/\sqrt{12}$.

We can modify protocol C as follows with a couple of maximally entangled qubit pairs. (i) Alice prepares the Bell state $|\Phi^+\rangle_{AB}$ and sends particle $B$ to Bob while retaining particle $A$, (ii) Bob also prepares the Bell state $|\Phi^+\rangle_{CD}$, (iii) Bob performs a joint measurement for particles $B$ and $C$ with the projection basis $\{|\Phi^1\rangle^*, |\Phi^2\rangle^*, |\Phi^3\rangle^*, |\Phi^4\rangle^*\}$, where the state $|\Phi^i\rangle^*$ ($i$=1–4) means the complex conjugate of the state $|\Phi^i\rangle$, and he then sends particle $D$ to Alice. (iv) Alice performs a joint measurement for particles $A$ and $D$ with the VAA projection basis $\{|\Phi^1\rangle,|\Phi^2\rangle,|\Phi^3\rangle,|\Phi^4\rangle\}$. (v) They can anticipate the following correlation for their projection results in accordance with

$$|\Phi^+\rangle_{AB}|\Phi^+\rangle_{CD}=\tfrac{1}{2}\{|\Phi^1\rangle_{AD}|\Phi^1\rangle^*_{BC}+|\Phi^2\rangle_{AD}|\Phi^2\rangle^*_{BC} + |\Phi^3\rangle_{AD}|\Phi^3\rangle^*_{BC}+|\Phi^4\rangle_{AD}|\Phi^4\rangle^*_{BC}\}, \qquad (7)$$

unless an eavesdropper is present.

A comparison with the ping-pong protocol [5] is worth mentioning. In the ping-pong protocol, Bob can distribute one bit in a secure way with particle $B$ by operating either $E_B$ or $Z_B$ while he must abandon the use of the other bit as regards $X_B$ or $Y_B=iX_BZ_B$. This is because the control mode mentioned in Sec. III (see option A5) is valid only for the security check for the former bit. Let us assume that Eve measures particle $B$ with the $\{|1\rangle,|0\rangle\}$ basis and then sends the obtained state to Alice. Eve can escape detection in the control mode while she can identify whether or not Bob operated $X_B$ by measuring the returned particle $B$ with the $\{|1\rangle,|0\rangle\}$ basis. In contrast, our protocols B and C make it possible for legitimate parties to distribute two-bit key with particle $B$.

If we are to complete the implementation of our protocols, we require a quantum operation gate. This has not yet been realized for photons. Nevertheless, a probabilistic implementation is possible for protocol A with a linear-optic setup using an entangled photon pair. We will report this linear-optic implementation elsewhere in the near future. The security aspects of our protocol relevant to collective attacks should be also analyzed in detail in future studies.

## VI. SUMMARY

If a quantum state of a pair of distant qubits is a nonmaximally entangled state, there are typical cases where two orthogonal quantum states $|\Psi^1\rangle_{AB}$ and $|\Psi^2\rangle_{AB}$ cannot be transformed into each other with a local unitary operation. Although a local nonunitary operation accompanied by a projection measurement is an alternative method for state transformation, the success or failure of the transformation is probabilistic and uncontrollable. We can utilize the above-mentioned characteristics of nonmaximally entangled states to demonstrate quantum cryptography in a two-way configuration similar to quantum super dense coding.

## ACKNOWLEDGMENTS

We thank Dr. F. Morikoshi and Dr. M. Koashi for fruitful comments and suggestions.

## APPENDIX

If an eavesdropping strategy is restricted to an individual attack, we can prove the security of protocol A in a general way. Figure 4 shows the schematic configuration of the eavesdropping strategies in two-way protocols. (i) Eve prepares an ancilla and sets the initial state $|\gamma\rangle_E$. (ii) Eve performs the first entangling operation $J_{BE}$ for her ancilla $|\gamma\rangle_E$ and particle $B$ that is sent to Bob. (iii) Bob performs an entangling operation $K_{BE}$ for particle $B$ and his ancilla $|\phi^1\rangle_C$ and then returns particle $B$. (iv) Eve performs a second entangling operation $L_{BE}$ for her ancilla and particle $B$ that is sent to Alice. (v) Eve executes an appropriate projection measurement for her ancilla to read out bit $R$.

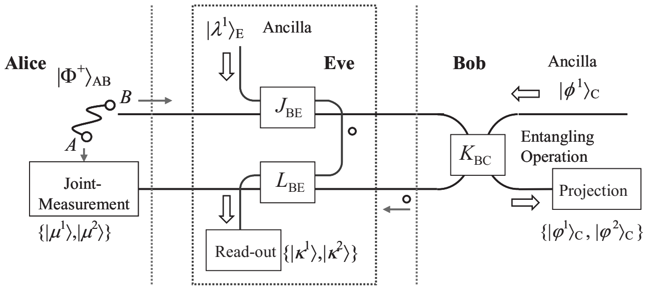

FIG. 4. General eavesdropping strategy for protocol A.

Eve is successful in her eavesdropping if she can choose $J_{BE}$ and $L_{BE}$ so that the final quantum state of the whole system is expressed as

$$|\xi\rangle_{ABCE}=\frac{1}{\sqrt{2}}|\mu^1\rangle_{AB}|\varphi^1\rangle_C|\kappa^1\rangle_E+\frac{1}{\sqrt{2}}|\mu^2\rangle_{AB}|\varphi^2\rangle_C|\kappa^2\rangle_E, \qquad (A1)$$

where the set $\{|\kappa^1\rangle_E,|\kappa^2\rangle_E\}$ is the read-out basis for her ancilla. Her resultant $|\kappa^1\rangle_E/|\kappa^2\rangle_E$ determines the bit value $R=1/R=0$. Just before step (iii), the quantum state of the whole system must be represented by $K^{-1}_{BC}(L^{-1}_{BE}|\xi\rangle_{ABCE})$. At the same time, the quantum state must also be expressed as the product state $(J_{BE}|\Phi^+\rangle_{AB}|\gamma\rangle_E)\otimes|\phi^1\rangle_C$. This is because the state preparation of Bob's ancilla $|\phi^1\rangle_C$ is independent of the quantum states of the spin pair and Eve's ancilla. Therefore, we can prove the impossibility of eavesdropping by showing the fault in the equation below

$$K^{-1}_{BC}(L^{-1}_{BE}|\xi\rangle_{ABCE})=(J_{BE}|\Phi^+\rangle_{AB}|\gamma\rangle_E)\otimes|\phi^1\rangle_C \qquad (A2)$$

for a parameter region of $0<\theta<\pi/4$.

We should rewrite the final state $|\xi\rangle_{ABCE}$ by using the standard bases $\{|\Phi^+\rangle_{AB},|\Phi^-\rangle_{AB}\},\{|\phi^1\rangle_C,|\phi^2\rangle_C\}$ and $\{|u^1\rangle_E,|u^2\rangle_E\}$ for the qubit pair, Bob's ancilla and Eve's ancilla, respectively,

$$\begin{aligned}|\xi\rangle_{ABCE}=&\frac{1}{2}|\Phi^+\rangle_{AB}|\phi^1\rangle_C(|u^1\rangle_E+\cos 2\theta|u^2\rangle_E)\\&-\frac{i}{2}\sin 2\theta|\Phi^+\rangle_{AB}|\phi^2\rangle_C|u^2\rangle_E\\&-\frac{1}{2}\sin 2\theta|\Phi^-\rangle_{AB}|\phi^1\rangle_C|u^2\rangle_E+\frac{i}{2}|\Phi^-\rangle_{AB}|\phi^2\rangle_C(|u^1\rangle_E\\&-\cos 2\theta|u^2\rangle_E). \qquad (A3)\end{aligned}$$

The basis $\{|u^1\rangle_E,|u^2\rangle_E\}$ is related to the read-out basis $\{|\kappa^1\rangle_E,|\kappa^2\rangle_E\}$ as

$$|u^1\rangle_E=\begin{bmatrix}1\\0\end{bmatrix}_E=\frac{1}{\sqrt{2}}(|\kappa^1\rangle_E+|\kappa^2\rangle_E),$$

$$|u^2\rangle_E = \begin{bmatrix} 0 \\ 1 \end{bmatrix}_E = \frac{1}{\sqrt{2}}(|\kappa^1\rangle_E - |\kappa^2\rangle_E).$$

We can express the inverse entangling operation $L_{BE}^{-1}$ as

$$L_{BE}^{-1} = \begin{bmatrix} P & Q \\ R & S \end{bmatrix}_E,$$

where the operators $P$, $Q$, $R$, and $S$ are the local spin rotations $F_B$ for particle $B$ of the spin pair. These operators are represented by

$$P = \cos Y_E \begin{bmatrix} \exp(ix_p)\cos y_p & \exp(iz_p)\sin y_p \\ -\exp(-iz_p)\sin y_p & \exp(-ix_p)\cos y_p \end{bmatrix}_B,$$

$$Q = \sin Y_E \begin{bmatrix} \exp(ix_q)\cos y_q & \exp(iz_q)\sin y_q \\ -\exp(-iz_q)\sin y_q & \exp(-ix_q)\cos y_q \end{bmatrix}_B,$$

$$R = -\sin Y_E \begin{bmatrix} \exp(ix_r)\cos y_r & \exp(iz_r)\sin y_r \\ -\exp(-iz_r)\sin y_r & \exp(-ix_r)\cos y_r \end{bmatrix}_B,$$

$$S = \cos Y_E \begin{bmatrix} \exp(ix_s)\cos y_s & \exp(iz_s)\sin y_s \\ -\exp(-iz_s)\sin y_s & \exp(-ix_s)\cos y_s \end{bmatrix}_B.$$

The angle $Y_E$ rotates the spin state of Eve's ancilla. The inverse entangling operation $L_{BE}^{-1}$ must be a unitary operation. The vector representation is also employed for Bob's ancilla;

$$|\phi^1\rangle_C = \begin{bmatrix} 1 \\ 0 \end{bmatrix}_C, \quad |\phi^2\rangle_C = \begin{bmatrix} 0 \\ 1 \end{bmatrix}_C.$$

The inverse entangling operation $K_{BE}^{-1}$ is expressed as

$$K_{BC}^{-1} = \begin{bmatrix} E/\sqrt{2} & -iZ/\sqrt{2} \\ -iZ/\sqrt{2} & E/\sqrt{2} \end{bmatrix}_C.$$

Finally, the quantum state $K_{BC}^{-1}(L_{BE}^{-1}|\xi\rangle_{ABCE})$ can be represented by

$$\begin{aligned} K_{BC}^{-1}(L_{BE}^{-1}|\xi\rangle_{ABCE}) = {} & \frac{1}{\sqrt{8}}\{(\hat{\eta}_1|\Phi^+\rangle_{AB} + \hat{\eta}_2|\Phi^-\rangle_{AB})|u^1\rangle_E \\ & + (\hat{\eta}_3|\Phi^+\rangle_{AB} + \hat{\eta}_4|\Phi^-\rangle_{AB})|u^2\rangle_E\}|\phi^1\rangle_C \\ & - \frac{i}{\sqrt{8}}\{(\hat{\vartheta}_1|\Phi^+\rangle_{AB} + \hat{\vartheta}_2|\Phi^-\rangle_{AB})|u^1\rangle_E \\ & + (\hat{\vartheta}_3|\Phi^+\rangle_{AB} + \hat{\vartheta}_4|\Phi^-\rangle_{AB})|u^2\rangle_E\}|\phi^2\rangle_C, \end{aligned} \tag{A4}$$

where

$$\hat{\eta}_1 = P + (\cos 2\theta)Q - (\sin 2\theta)ZQ, \quad \hat{\eta}_2 = -(\sin 2\theta)Q + ZP - (\cos 2\theta)ZQ,$$

$$\hat{\eta}_3 = R + (\cos 2\theta)S - (\sin 2\theta)ZS, \quad \hat{\eta}_4 = -(\sin 2\theta)S + ZR - (\cos 2\theta)ZS,$$

$$\hat{\vartheta}_1 = ZP + (\cos 2\theta)ZQ + (\sin 2\theta)Q, \quad \hat{\vartheta}_2 = -(\sin 2\theta)ZQ - P + (\cos 2\theta)S,$$

$$\hat{\vartheta}_3 = ZR + (\cos 2\theta)ZS + (\sin 2\theta)S, \quad \hat{\vartheta}_4 = -(\sin 2\theta)ZS - R + (\cos 2\theta)Q.$$

To reveal the fault in Eq. (A2), we should introduce a pair of un-normalized states $|\psi_1\rangle$ and $|\psi_2\rangle$ as

$$|\psi_1\rangle \equiv \hat{\eta}_1|\Phi^+\rangle_{AB} + \hat{\eta}_2|\Phi^-\rangle_{AB} = (\hat{\eta}_1 + \hat{\eta}_2 Z)|\Phi^+\rangle_{AB},$$

$$|\psi_2\rangle \equiv \hat{\eta}_3|\Phi^+\rangle_{AB} + \hat{\eta}_4|\Phi^-\rangle_{AB} = (\hat{\eta}_3 + \hat{\eta}_4 Z)|\Phi^+\rangle_{AB}.$$

Equation (A2) is true if and only if the condition $\langle\psi_1|\psi_1\rangle + \langle\psi_2|\psi_2\rangle = 8$ is satisfied so that the second term containing $|\phi^2\rangle_C$ can varnish on the right-hand side of Eq. (A4). We can evaluate the norms as

$$\langle\psi_1|\psi_2\rangle = 4[\cos^2 y_p \cos^2 Y_E + (\sin^2 2\theta \cos^2 y_q + \cos^2 2\theta \sin^2 y_q)\sin^2 Y_E],$$

$$\langle\psi_2|\psi_2\rangle = 4[\cos^2 y_r \sin^2 Y_E + (\sin^2 2\theta \cos^2 y_s + \cos^2 2\theta \sin^2 y_s)\cos^2 Y_E].$$

Here $\cos^2 y_p$ and $\cos^2 y_r$ can be chosen as unity. In contrast, the term $\sin^2 2\theta \cos^2 y_q + \cos^2 2\theta \sin^2 y_q$ is less than unity unless $\theta = 0$ or $\theta = \pi/4$. Hence, Eq. (A2) cannot be satisfied except when $\theta = 0$ and $\theta = \pi/4$. Therefore the impossibility of eavesdropping is proved for protocol A.

Eavesdropping is possible for $\theta = 0$ and $\theta = \pi/4$. In the former case, the states $|\mu^1\rangle$ and $|\mu^1\rangle$ of the qubit pair become the maximally entangled states $|\Phi^+\rangle_{AB}$ and $|\Phi^-\rangle_{AB}$, respectively. Here, Eve's use of the ancilla is equivalent to the insertion of a dummy Bell state. In the latter case, the states $|\mu^1\rangle$ and $|\mu^1\rangle$ become $|00\rangle$ and $|11\rangle$, respectively.

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000), Chap. 12.6.

[2] For a review including experimental studies, see N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[3] L. Goldenberg and L. Vaidman, Phys. Rev. Lett. **75**, 1239 (1995).

[4] M. Koashi and N. Imoto, Phys. Rev. Lett. **79**, 2383 (1997).

[5] K. Boström and T. Felbinger, Phys. Rev. Lett. **89**, 187902 (2002); This is the original proposal of the ping-pong protocol, where the Bell state $|\Psi^+\rangle_{AB}$ is prepared by Bob as the initial

state and Alice can encode one-bit with $|\Psi^+\rangle_{AB}$ or $|\Psi^-\rangle_{AB}$ by local operation $E_B$ or $Z_B$ on particle $A$. To perform a security check, Alice and Bob introduce the control mode as mentioned in Sec. III.

[6] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).

[7] A. Wójcik, Phys. Rev. Lett. **90**, 157901 (2003).

[8] Q. Y. Cai, Phys. Rev. Lett. **91**, 109801 (2003); Q. Y. Cai and B. W. Li, Phys. Rev. A **69**, 054301 (2004).

[9] P. S. Bourdon, E. Gerjuoy, J. P. McDonald, and H. T. Williams, Phys. Rev. A **77**, 022305 (2008).

[10] W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).

[11] A. Beige, B. G. Englert, C. Kurtsiefer, and H. Weinfurter, Acta Phys. Pol. A **101**, 357 (2002).

[12] K. Shimizu and N. Imoto, Phys. Rev. A **60**, 157 (1999).

[13] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[14] L. Vaidman, Y. Aharonov, and D. Z. Albert, Phys. Rev. Lett. **58**, 1385 (1987).