A method of enciphering quantum states

2001 J. Phys. A: Math. Gen. 34 2723

(http://iopscience.iop.org/0305-4470/34/13/305)

INSTITUTE OF PHYSICS PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND GENERAL

J. Phys. A: Math. Gen. **34** (2001) 2723–2741 www.iop.org/Journals/ja PII: S0305-4470(01)20554-X

A method of enciphering quantum states

Hiroo Azuma[1,3] **and Masashi Ban**[2]

[1] Mathematical Engineering Division, Canon Research Center, 5-1, Morinosato-Wakamiya, Atsugi-shi, Kanagawa, 243-0193, Japan
[2] Advanced Research Laboratory, Hitachi Ltd, Hatoyama, Saitama, 350-0395, Japan

E-mail: hiroo@crc.canon.co.jp, hiroo.azuma@qubit.org and m-ban@harl.hitachi.co.jp

Received 21 December 2000

Abstract

In this paper, we propose a method of enciphering quantum states of two-state systems (qubits) for sending them in secrecy without entangled qubits shared by two legitimate users (Alice and Bob). This method has the following two properties. First, even if an eavesdropper (Eve) steals qubits, she can extract information from them with only a certain probability at most. Second, Alice and Bob can confirm that the qubits are transmitted between them correctly by measuring a signature. If Eve measures m qubits one by one from n enciphered qubits and sends alternative ones (the intercept/resend attack), the probability that Alice and Bob do not notice Eve's action is equal to $\left(\frac{3}{4}\right)^m$ or less. Passwords for decryption and the signature are given by classical binary strings and they are disclosed through a public channel. Enciphering classical information by this method is equivalent to the one-time pad method with distributing a classical key (random binary string) by the BB84 protocol. If Eve takes away qubits, Alice and Bob lose the original quantum information. If we apply our method to a state in iteration, Eve's success probability decreases exponentially. We cannot examine security against the case that Eve makes an attack using entanglement. This remains to be solved in the future.

PACS numbers: 0367, 4265, 0365B, 4250D

1. Introduction

Since considerable progress has been made in quantum information and computation theory, many researchers have, through quantum mechanics [1], been trying to realize a level of information processing that we have never had previously. At the same time, researchers have been studying the application of the uncertainty principle, the quantum no-cloning theorem and entanglement between quantum systems to cryptography [2]. The BB84 protocol is considered to be an effective method for key distribution. By combining it with the one-time pad method,

[3] Present address: Centre for Quantum Computation, Clarendon Laboratory, Parks Road, Oxford OX1 3PU, UK.

we obtain a highly secure cryptography [3–5]. On the other hand, quantum teleportation is considered to be an excellent method for sending arbitrary quantum states between two parties [6, 7].

The BB84 protocol is used for the secure distribution of a classical key (binary string) to two legitimate users (Alice and Bob). Choosing a basis vector at random from four basis vectors, the rectilinear basis $\{|0\rangle, |1\rangle\}$ and the circular basis $\{(1/\sqrt{2})(|0\rangle \pm |1\rangle)\}$, as a state of a photon (a two-state system or a qubit), Alice sends it to Bob. Bob measures a transmitted photon in an orthonormal basis that he chooses from two bases (rectilinear and circular) at random and independently of Alice.

Not being consistent with each other, the rectilinear basis and the circular basis are called conjugate bases. The result of a measurement with an incorrect basis is random. If an eavesdropper (Eve) steals a photon from the channel, measures it in a basis chosen at random, and sends an alternative one, Alice and Bob will find an inconsistency with a probability of $\frac{1}{4}$ or more and notice Eve's eavesdropping. In this way, by using the uncertainty principle, the BB84 protocol reveals Eve's illegal act.

Ekert proposed another protocol for distributing a classical key by transmitting pairs of qubits in EPR states, $|\Psi^-\rangle = (1/\sqrt{2})(|01\rangle - |10\rangle)$, apart to Alice and Bob from a source [8]. They detect Eve by Bell's theorem. Considering a simplified protocol of Ekert, Bennett *et al* showed it was equivalent to BB84 [9]. From these successive works, it has been recognized that we do not need to use entanglement to distribute a classical key using quantum mechanics. (But, by combining the entanglement purification protocol with Ekert's protocol, we can distribute a classical key with high secrecy [10].)

Quantum teleportation is used for transmitting an arbitrary state from Alice to Bob. They share an EPR-pair of qubits beforehand. Alice carries out the Bell-measurement on both a one-qubit state $|\psi\rangle$ that she wants to send and her qubit of the EPR-pair. Receiving a result of her measurement, Bob can construct $|\psi\rangle$ from his qubit of the EPR-pair. A characteristic of this method is that classical information and non-classical information of $|\psi\rangle$ are divided perfectly and only the classical information is sent through the public channel. If they share the EPR-pair correctly, Eve can neither eavesdrop on the state nor destroy it in principle.

These methods are related to the quantum no-cloning theorem. It tells us there is no unitary transformation that makes accurate clones of arbitrary quantum states [2]. In the BB84 protocol, it gives an effect as follows. Not knowing which basis is chosen for a qubit (photon) that she extracts from the quantum channel, rectilinear or circular, Eve cannot make a clone of the qubit and keep it. What she can do is only to measure the qubit in a proper basis and send an alternative one that depends on the result of the measurement to Bob. In the quantum teleportation, the following point is important. Because Alice can neither measure $|\psi\rangle$ without disturbance nor make an accurate clone of it, she cannot extract information from $|\psi\rangle$ at all. During the whole process, Alice and Bob have no knowledge about $|\psi\rangle$.

In quantum teleportation, Alice and Bob have to share an EPR-pair of qubits beforehand. After being emitted by a source, this pair flies towards them apart through a quantum channel. Therefore, for example, if Eve takes away the qubit that Bob is supposed to have and sends an alternative one to him, she succeeds in eavesdropping. To avoid such a problem, Alice and Bob need to share a lot of EPR-pairs and to purify them [10].

In this paper, we consider a method for enciphering arbitrary quantum states for sending them in secrecy without entangled qubits shared by Alice and Bob beforehand. In our method, there are two points as follows (see figure 3 in section 3).

First, even if Eve takes away qubits, she can extract quantum information from them with only a certain probability at most. (If Eve measures m qubits one by one from n enciphered

qubits and sends alternative ones, the probability that Alice and Bob do not notice Eve's act is equal to $\left(\frac{3}{4}\right)^m$ or less. We assume Eve makes only the intercept/resend attack [4].) Alice applies a unitary operator U_i which is chosen at random from a set of operators $\mathcal{M} = \{U_j\}$ to an arbitrary n-qubit state $|\Psi\rangle$ that she wants to send in secrecy. The subscript i of U_i is a password for decryption. Not knowing which operator is chosen from $\mathcal{M}$, Eve regards the enciphered state as a mixed state of $U_j|\Psi\rangle$ for all $U_j \in \mathcal{M}$ with equal probability. If Alice prepares $\mathcal{M}$ so that the density operator of the mixed state may be in proportion to the identity operator $\boldsymbol{I}$, Eve cannot extract the information of $|\Psi\rangle$ at all without the password i. The reason for this is that even if Eve puts auxiliary qubits on the density operator $\rho = (1/2^n)\boldsymbol{I}$, applies unitary transformations to it, or measures it, she cannot extract $|\Psi\rangle$. After confirming that the quantum state is transmitted correctly, Alice releases the password i in our protocol. Therefore, to extract information from $|\Psi\rangle$, Eve has to eavesdrop without disturbing Alice and Bob's certification process. (This technique has been also discussed by two groups, Boykin and Roychowdhury, and Mosca *et al* [11]. They have shown the following result. When we define $\mathcal{M}$ as a set of tensor products of the Pauli matrices, the number of the operators $\{U_i\}$ becomes minimum and the subscript i is represented by a $2n$-bit string.)

Second, Alice and Bob can confirm that a quantum state received by Bob is a genuine one sent by Alice. Not having knowledge about the n-qubit state $|\Psi\rangle_Q$ at all, they do not notice Eve replace the genuine qubits with alternative ones. Therefore, they need to confirm that the qubits Bob receives are genuine. (It seems like authentication of the identity of a correspondent on networks.) In our method, after putting an n-qubit state $|a\rangle_S$ ($a \in \{0, 1\}^n$) that represents her signature on $U_i^Q|\Psi\rangle_Q$, Alice makes entanglement between qubits of each pair in the system Q and S. Here, we call the quantum system which represents the transmitted information Q and the quantum system which represents the signature S. Then, to forbid Eve for making clones of qubits, Alice applies an operator chosen at random from $\mathcal{L} = \{\boldsymbol{I}, H, \sigma_x, H\sigma_x\}$ to each qubit, where H is called the Hadamard transformation and it causes $|0\rangle \to (1/\sqrt{2})(|0\rangle + |1\rangle)$, $|1\rangle \to (1/\sqrt{2})(|0\rangle - |1\rangle)$, and σ_x is one of the Pauli matrices and it causes $|0\rangle \to |1\rangle$, $|1\rangle \to |0\rangle$. Hence, quantum information of each qubit is encoded in a basis chosen at random from two conjugate bases (rectilinear and circular). Therefore, if Eve does anything on the qubits, Alice and Bob can find an inconsistency and detect Eve with at least a certain probability. This is essentially the same technique used in BB84. In our method, certification of a correspondent and detection of Eve are done at the same time. The second password for decryption is which operators are chosen from $\mathcal{L}$.

Because the passwords and the signature represented by classical binary strings are transmitted by the public channel, Eve also knows them. If $|\Psi\rangle_Q$ represents classical information (a product state of $|0\rangle$ and $|1\rangle$), our protocol is equivalent to the one-time pad method with classical key distribution by BB84.

If Alice and Bob apply our enciphering method to a state in iteration, the probability that Eve gets quantum information with a fidelity of 1 decreases exponentially. (If they encipher a one-qubit state with N qubits, the probability is given by $\left(\frac{3}{4}\right)^{N/2}$.) We can regard it as a privacy amplification process. We cannot examine security against the case that Eve makes an attack with using entanglement. This remains to be solved in the future.

This paper is organized as follows. In section 2, we explain how Alice and Bob forbid Eve from extracting the original quantum information and how they confirm that the qubits are transmitted correctly. In section 3, we explain the whole protocol and discuss how Bob confirms that he receives qubits. In section 4, we discuss security of our protocol against Eve's intercept/resend attack on each qubit. In section 5, we discuss privacy amplification process. In section 6, we give a brief discussion.

2. Enciphering quantum states

In this section, we explain how Alice and Bob forbid Eve to extract the original quantum information and how they confirm the qubits are transmitted correctly.

First, we consider transforming an arbitrary quantum state so that Eve cannot recover an original quantum state. For simplicity, we consider an arbitrary one-qubit state for a while and we describe its density operator as ρ defined on a two-dimensional Hilbert space $\mathcal{H}_2$. We assume Alice wants to send ρ to Bob in secrecy. She does not know ρ at all, because her partial measurement destroys it.

Alice prepares a set of operators,

$$\mathcal{M} = \{\sigma_j : j = 0, x, y, z\} \tag{1}$$

where $\sigma_0 = \boldsymbol{I}$ (the identity operator) and $\{\sigma_x, \sigma_y, \sigma_z\}$ are the Pauli matrices. Taking

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{2}$$

for an orthonormal basis, we write them as

$$\begin{aligned} \boldsymbol{I} &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad & \sigma_x &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ \sigma_y &= \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix} \qquad & \sigma_z &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \end{aligned} \tag{3}$$

$\mathcal{M}$ may be disclosed in public. Choosing an operator σ_i from $\mathcal{M}$ at random, Alice carries out the following unitary transformation:

$$\rho \to \sigma_i \rho \sigma_i^{\dagger}. \tag{4}$$

She keeps the subscript i secret as a password and never tells it to anyone. Because the subscript takes a value from $\{0, x, y, z\}$, the password can be represented by two-bit classical information.

Not knowing which transformation Alice applies to the qubit, Eve has to regard the state as

$$\rho' = \tfrac{1}{4} \sum_{j=0,x,y,z} \sigma_j \rho \sigma_j^{\dagger}. \tag{5}$$

Generally, the density operator ρ satisfies $\rho^{\dagger} = \rho$, $\mathrm{Tr}\,\rho = 1$, $0 \leqslant \lambda_1 \leqslant 1$, $0 \leqslant \lambda_2 \leqslant 1$ and $\lambda_1 + \lambda_2 = 1$, where λ_1, λ_2 are eigenvalues of ρ. Hence, we can describe an arbitrary ρ as

$$\rho = \tfrac{1}{2}(\boldsymbol{I} + \boldsymbol{a} \cdot \boldsymbol{\sigma}) \tag{6}$$

where $\boldsymbol{a} = (a_1, a_2, a_3)$ is a three-component real vector and $0 \leqslant \sum_{k=1}^{3} a_k^2 \leqslant 1$. Because

$$\rho' = \tfrac{1}{2}\boldsymbol{I} + \tfrac{1}{8} \sum_{j=0,x,y,z} \boldsymbol{a} \cdot \sigma_j \boldsymbol{\sigma} \sigma_j^{\dagger} \tag{7}$$

and

$$\sigma_j \sigma_k \sigma_j = \begin{cases} \sigma_k & j = 0 \quad \text{or} \quad j = k \\ -\sigma_k & j \neq k \quad \text{and} \quad j, k \in \{x, y, z\} \end{cases} \tag{8}$$

there is no contribution from the second term of (7). We obtain

$$\rho' = \tfrac{1}{2}\boldsymbol{I}. \tag{9}$$

Therefore, even if Eve takes away ρ', she cannot extract information from it at all, because she does not know the password i.

An arbitrary n-qubit density operator ρ_n is given by

$$\rho_n = \frac{1}{2^n}\left(\boldsymbol{I} + \sum_{\boldsymbol{k}\in\{0,x,y,z\}^n, \boldsymbol{k}\neq(0,\ldots,0)} a_{\boldsymbol{k}} U_{\boldsymbol{k}}\right) \tag{10}$$

where

$$U_{\boldsymbol{k}} = \sigma_{k_1} \otimes \cdots \otimes \sigma_{k_n} \tag{11}$$

and $a_{\boldsymbol{k}}$ ($\boldsymbol{k} \in \{0, x, y, z\}^n$, $\boldsymbol{k} \neq (0, \ldots, 0)$) is real. (In (10), $\boldsymbol{I}$ represents the identity operator for n-qubit states.) Choosing an operator U_i from

$$\mathcal{M}_n = \{U_{\boldsymbol{k}} : U_{\boldsymbol{k}} = \sigma_{k_1} \otimes \cdots \otimes \sigma_{k_n}, \boldsymbol{k} \in \{0, x, y, z\}^n\} \tag{12}$$

at random, Alice applies it to ρ_n for encryption as $\rho_n \to U_i \rho_n U_i^\dagger$. If Eve takes away the density operator given by

$$\begin{aligned}\rho_n' &= \frac{1}{4^n} \sum_{\boldsymbol{j}\in\{0,x,y,z\}^n} U_{\boldsymbol{j}} \rho_n U_{\boldsymbol{j}}^\dagger \\ &= \frac{1}{2^n}\boldsymbol{I} + \frac{1}{4^n \cdot 2^n} \sum_{\boldsymbol{j},\boldsymbol{k}\in\{0,x,y,z\}^n, \boldsymbol{k}\neq(0,\ldots,0)} a_{\boldsymbol{k}} U_{\boldsymbol{j}} U_{\boldsymbol{k}} U_{\boldsymbol{j}}^\dagger \\ &= \frac{1}{2^n}\boldsymbol{I}\end{aligned} \tag{13}$$

she cannot extract information from ρ_n' at all. Even if she puts auxiliary systems on ρ_n', applies unitary transformations to it, or carries out measurements, she cannot obtain ρ_n. The password of $\boldsymbol{i}$ is given by a $2n$-bit string. (This technique is also discussed by two groups, Boykin and Roychowdhury, and Mosca *et al* as mentioned in section 1 [11].)

Next, we explain how Alice and Bob confirm that the qubits are transmitted between them correctly. If Eve takes away ρ_n' and sends an alternative state $\tilde{\rho}_n$ to Bob, he carries out the inverse operation on the state that he receives as $\tilde{\rho}_n \to U_i \tilde{\rho}_n U_i^\dagger$. Not having knowledge about the original ρ_n at all, Alice and Bob do not notice that what Bob gets is a fake.

To avoid this problem, they put a signature on ρ_n. Reading it, they can confirm that Bob receives the state transmitted from Alice correctly. It is important that Eve cannot change the signature. For simplicity, we describe the state as a ket vector $\forall|\Psi\rangle_Q \in \mathcal{H}_2^n$ instead of the density operator ρ_n for a while. If the n-qubit state is given by a mixed state, we can give a similar discussion. We call the system that represents the quantum information Q and the system that represents the signature S.

Preparing an n-bit random string $\forall \boldsymbol{a} = (a_1, \ldots, a_n) \in \{0, 1\}^n$ as her signature, Alice attaches a qubit $|a_k\rangle_S$ to the kth qubit of

$$U_i^Q|\Psi\rangle_Q = \sum_{\boldsymbol{x}\in\{0,1\}^n} c_{\boldsymbol{x}}|x_1\rangle \cdots |x_n\rangle \in \mathcal{H}_2^n. \tag{14}$$

Applying the controlled-NOT (C-NOT) gate to the kth pair as in figure 1, she obtains

$$|x_k\rangle_Q|a_k\rangle_S \to |x_k\rangle_Q|a_k \oplus x_k \bmod 2\rangle_S \qquad \text{for} \quad k = 1, \ldots, n. \tag{15}$$

Choosing $L_{k,1}^Q, L_{k,2}^S \in \mathcal{L} = \{\boldsymbol{I}, H, \sigma_x, H\sigma_x\}$ at random, she applies them to the qubits of the pair, where

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{16}$$

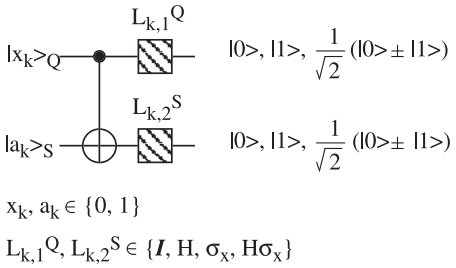

Figure 1. The second encryption by Alice.

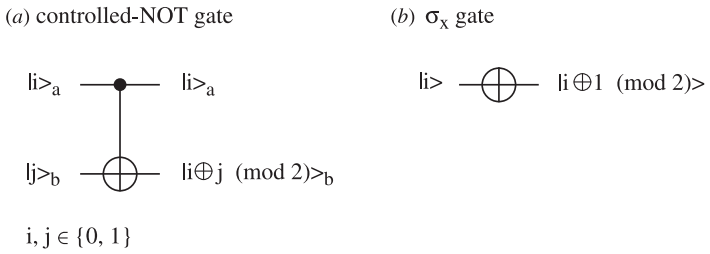

Figure 2. Typical quantum gates.

Alice repeats this operation on the $k = 1, \ldots, n$th qubit, and we write the whole transformation as $V_{\boldsymbol{\alpha}}^{QS}$. $\boldsymbol{\alpha}$, where represents which operators are chosen from $\mathcal{L}$. The second password $\boldsymbol{\alpha}$ is given by a classical $4n$-bit string.

We often describe successive operations on qubits as a network such as figure 1. A horizontal line represents a qubit and time proceeds from left to right. Figure 2 shows examples of unitary transformations applied to qubits. Figures 2(*a*) and (*b*) represent the C-NOT gate and σ_x, respectively [12].

The operations that we have discussed are summarized as follows:

$$\begin{aligned} |\Psi\rangle_Q &\to U_{\boldsymbol{i}}^{Q}|\Psi\rangle_Q && \text{(first password } \boldsymbol{i}\text{)} \\ &\to |\boldsymbol{a}\rangle_S \otimes U_{\boldsymbol{i}}^{Q}|\Psi\rangle_Q && \text{(signature } \boldsymbol{a}\text{)} \\ &\to V_{\boldsymbol{\alpha}}^{QS}(|\boldsymbol{a}\rangle_S \otimes U_{\boldsymbol{i}}^{Q}|\Psi\rangle_Q) && \text{(second password } \boldsymbol{\alpha}\text{)}. \end{aligned} \tag{17}$$

Double encryption prevents Eve from using $|\boldsymbol{a}\rangle_S$ maliciously. If $V_{\boldsymbol{\alpha}}^{QS}$ is not applied to the state, Eve may take away all of the qubits, keep $U_{\boldsymbol{i}}^{Q}|\Psi\rangle_Q$ and send a fake version of $|\boldsymbol{a}\rangle_S \otimes |\tilde{\Psi}\rangle_Q$ to Bob.

If Eve does anything to the kth qubit of Q, the signature of $|a_k\rangle_S$ is destroyed and Bob's probability of failure in the certification process is bounded from below. This is caused by the fact that conjugate bases chosen at random represent the systems Q and S and there is entanglement between Q and S. If she does anything to the kth qubit of S, we can obtain a similar result. We estimate the probability that Alice and Bob notice Eve's illegal act in section 4.

3. The protocol for secure transmission

We consider a protocol for transmitting an arbitrary quantum state $\forall|\Psi\rangle_Q \in \mathcal{H}_2^n$ from Alice to Bob in secrecy against Eve's eavesdropping by using the encryption method discussed in the

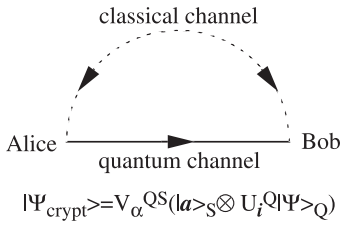

Figure 3. Secure transmission between Alice and Bob.

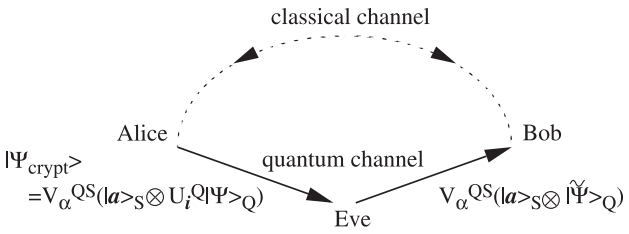

Figure 4. Eve's strategy for eavesdropping.

previous section. Alice and Bob do not have knowledge about $|\Psi\rangle_Q$ at all. Both of them can use the following two channels.

- The classical channel. It transmits classical binary strings in public. Eve can make accurate copies of them, but she cannot alter them.
- The quantum channel. It transmits sequences of qubits (quantum information). Eve can interact with them, but she cannot make accurate copies of them.

Alice sends qubits to Bob according to the following protocol (see figure 3).

(a) Alice sends $|\Psi_{\rm crypt}\rangle \equiv V_{\boldsymbol{\alpha}}^{QS}(|\boldsymbol{a}\rangle_S \otimes U_{\boldsymbol{i}}^{Q}|\Psi\rangle_Q)$ of $2n$ qubits to Bob through the quantum channel.
(b) Receiving $2n$ qubits, Bob breaks off the quantum channel and reports arrival of them to Alice through the classical channel.
(c) Receiving the report from Bob, Alice tells Bob what transformation $V_{\boldsymbol{\alpha}}^{QS}$ is through the classical channel. (She discloses the $4n$-bit password $\boldsymbol{\alpha}$.)
(d) Applying $V_{\boldsymbol{\alpha}}^{QS\dagger}$ to the state that he has received and measuring the signature, Bob tells Alice a result of the measurement (an n-bit string) through the classical channel.
(e) Receiving the n-bit string from Bob, Alice examines whether it coincides with the signature $\boldsymbol{a}$ or not. If it coincides with her original signature, she tells Bob what transformation $U_{\boldsymbol{i}}^{Q}$ is through the classical channel. (She discloses the $2n$-bit password $\boldsymbol{i}$.) If it does not coincide, she concludes Eve has eavesdropped on qubits and stops the protocol.
(f) Bob applies $U_{\boldsymbol{i}}^{Q\dagger}$ to the state that he has and obtains the original state $|\Psi\rangle_Q$.

In this protocol, it is important that Bob confirms the arrival of $2n$ qubits ($|\Psi_{\rm crypt}\rangle$ or Eve's fake) and breaks off the quantum channel at the second step. To understand the reason for this, we assume the following case (see figure 4). Although $|\Psi_{\rm crypt}\rangle$ is still halfway on the channel, Bob reports the arrival of qubits to Alice by mistake, and she discloses $V_{\boldsymbol{\alpha}}^{QS}$ through the classical channel. Eve may take away $|\Psi_{\rm crypt}\rangle$, apply $V_{\boldsymbol{\alpha}}^{QS\dagger}$ to it, and obtain $|\boldsymbol{a}\rangle_S \otimes U_i|\Psi\rangle_Q$ before Bob receives qubits. Eve can keep $U_i|\Psi\rangle_Q$, combine a false state $|\tilde{\Psi}\rangle_Q$ with $|\boldsymbol{a}\rangle_S$ and send $V_{\boldsymbol{\alpha}}^{QS}(|\boldsymbol{a}\rangle_S \otimes |\tilde{\Psi}\rangle_Q)$ to Bob. If the quantum channel is still open, Bob

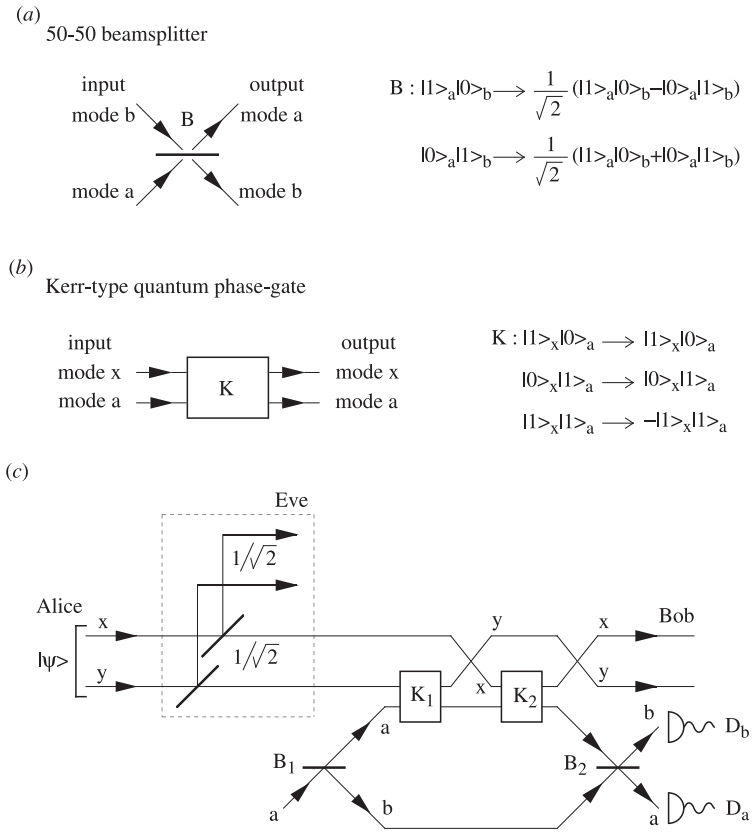

Figure 5. The photon counting measurement with nonlinear optical devices.

receives $V_{\alpha}^{QS}(|\boldsymbol{a}\rangle_S \otimes |\tilde{\Psi}\rangle_Q)$. Because the signature is correct, Alice and Bob cannot notice Eve's illegal act. Alice discloses U_i^Q in public and finally Eve gets $|\Psi\rangle_Q$.

To avoid this problem, Bob needs to verify that a batch of qubits ($|\Psi_{\text{crypt}}\rangle$ or Eve's fake) has arrived. For example, it is good for Bob to use the following method.

We construct a qubit from a pair of optical paths (modes) that are represented by x and y in figure 5(c) [13]. We describe a state where there is no photon on a mode as $|0\rangle$ and a state where there is a photon on a mode as $|1\rangle$. Writing a state where no photon is on the mode x and one photon is on the mode y as $|0\rangle_x \otimes |1\rangle_y = |01\rangle$, we regard $|01\rangle$ as logical $|\bar{0}\rangle$. We regard $|1\rangle_x|0\rangle_y$ as logical $|\bar{1}\rangle$ similarly. Hence, we can write an arbitrary state of a qubit as

$$|\psi\rangle = \alpha|01\rangle + \beta|10\rangle = \alpha|\bar{0}\rangle + \beta|\bar{1}\rangle \qquad \text{for} \quad |\alpha|^2 + |\beta|^2 = 1. \tag{18}$$

We assume Eve puts a 50–50 beamsplitter halfway on the quantum channel to take away photons. A state of a photon is a superposition of a state that it is on the side of Bob and a state that it is on the side of Eve with amplitude $1/\sqrt{2}$ each,

$$\frac{1}{\sqrt{2}}|\text{photon on the side of Bob}\rangle + \frac{1}{\sqrt{2}}|\text{photon on the side of Eve}\rangle. \tag{19}$$

To examine whether the qubit of $|\psi\rangle$ has come on his own side or not, Bob prepares another auxiliary photon and applies nonlinear interaction between the logical photon on mode x or y and the auxiliary one. In the optical system of figure 5(c), if the photon counter D_a detects the

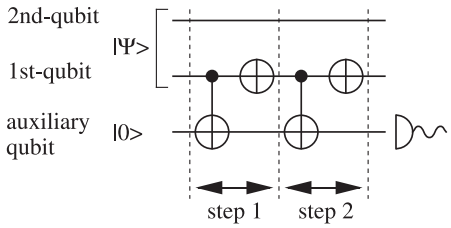

Figure 6. A quantum network for photon counting.

auxiliary photon, the logical photon is projected into the state that it is on the side of Bob. On the other hand, D_b's detection projects the logical photon into the state that it is on the side of Eve.

In figure 5(c), there are beamsplitters B which apply $SU(2)$ transformations to logical kets $\{|\bar{0}\rangle, |\bar{1}\rangle\}$ as in figure 5(a), and Kerr-type devices K which induce nonlinear interactions between two incoming photons as in figure 5(b). The device K shifts the phase of a wavefunction by π only if a pair of photons comes into it. (Turchette *et al* succeed in shifting the phase by $\Delta \sim 16^\circ$ [14].)

To clarify the operation of figure 5(c), we describe it by a network of quantum gates in figure 6 [15]. Assuming the first and the second qubits are in an arbitrary entangled state $|\Psi\rangle_Q$, we examine whether the first qubit exists or not by measuring an auxiliary qubit system A. When we write the whole system as

$$|\Psi\rangle_Q|0\rangle_A = \sum_{i,j\in\{0,1\}} c_{ij}|i\rangle_2|j\rangle_1|0\rangle_A \tag{20}$$

$|\Psi\rangle_Q|0\rangle_A$ is transformed as follows in figure 6,

$$\begin{aligned}|\Psi\rangle_Q|0\rangle_A &= \sum_i (c_{i0}|i\rangle_2|0\rangle_1 + c_{i1}|i\rangle_2|1\rangle_1)|0\rangle_A \\ &\xrightarrow{\text{step 1}} \sum_i (c_{i0}|i\rangle_2|1\rangle_1|0\rangle_A + c_{i1}|i\rangle_2|0\rangle_1|1\rangle_A) \\ &\xrightarrow{\text{step 2}} \sum_i (c_{i0}|i\rangle_2|0\rangle_1 + c_{i1}|i\rangle_2|1\rangle_1)|1\rangle_A \\ &= |\Psi\rangle_Q|1\rangle_A. \end{aligned} \tag{21}$$

Therefore, measuring an auxiliary system as shown in figures 5 and 6 for each channel, Bob can examine whether all of the qubits have arrived or not.

4. Security against eavesdropping

It is difficult to consider all strategies Eve may take. In this section, we assume Eve to make only the intercept/resend attack. Eve measures each transmitted qubit with a proper basis independently and sends an alternative one according to the result of the measurement [4]. We pay attention to the following fact. Eve cannot extract information about $|\Psi\rangle_Q$ at all without getting the first password $\boldsymbol{i}$ of $U_i^Q|\Psi\rangle_Q$, because the enciphered density operator is in proportion to $\boldsymbol{I}$ for her. Therefore, Eve needs to keep her illegal action secret from Alice and Bob during their authentication process so that Alice may disclose the first password $\boldsymbol{i}$. In this section, we estimate a probability that Alice and Bob fail to notice Eve's illegal act.

For simplicity, we assume that $|\Psi\rangle_Q$ is an arbitrary n-qubit product state for a while. At the first encryption, Alice applies $\forall U_i^Q = \sigma_{i_1} \otimes \cdots \otimes \sigma_{i_n}$ to $|\Psi\rangle_Q = |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$. Hence, $U_i^Q|\Psi\rangle_Q$ is also a product state and we may treat each qubit independently.

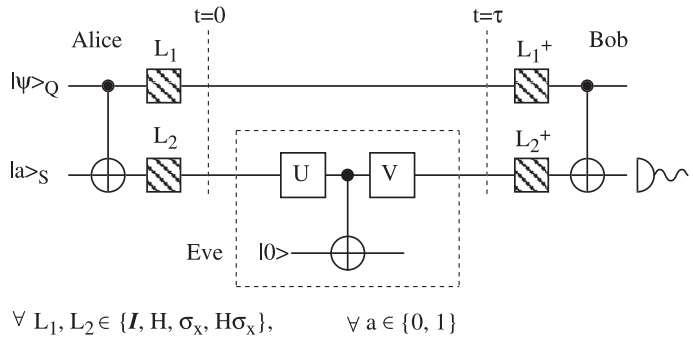

Figure 7. Eve's intercept/resend attack on the system S.

We write the kth qubit ($\forall k \in \{1, \ldots, n\}$) of $U_i^Q|\Psi\rangle_Q$ as $|\psi\rangle_Q = \alpha|0\rangle_Q + \beta|1\rangle_Q$ and the kth qubit of the signature as $|a\rangle_S$ ($a \in \{0, 1\}$). A state that Alice sends at $t = 0$ in figure 7 is given by

$$\alpha L_1|0\rangle_Q L_2|a\rangle_S + \beta L_1|1\rangle_Q L_2|a \oplus 1\rangle_S. \tag{22}$$

Bob measures only the system S at $t = \tau$. If he gets $|a\rangle_S$, Alice and Bob consider that the state is transmitted correctly. Bob uses the following projection operator for the measurement:

$$\Pi_{L_1,L_2}^{QS} = (L_1|0\rangle\langle 0|L_1^\dagger)_Q \otimes (L_2|a\rangle\langle a|L_2^\dagger)_S + (L_1|1\rangle\langle 1|L_1^\dagger)_Q \otimes (L_2|a \oplus 1\rangle\langle a \oplus 1|L_2^\dagger)_S. \tag{23}$$

Here, we assume Eve makes an attack only on the qubit of the system S as in figure 7 (U and V are arbitrary unitary transformations applied to one qubit). We write the dynamical process of S as a completely positive linear map \$ that represents Eve's intercept/resend attack on S [16]. Hence, the density operator ρ^S at $t = 0$ evolves to $\$(\rho^S)$ at $t = \tau$. We can write the state of QS at $t = \tau$ as

$$\begin{aligned}\rho_{L_1,L_2}^{QS}(\tau) = {} & |\alpha|^2(L_1|0\rangle\langle 0|L_1^\dagger)_Q \otimes \$(L_2|a\rangle\langle a|L_2^\dagger)_S \\ & + \alpha\beta^*(L_1|0\rangle\langle 1|L_1^\dagger)_Q \otimes \$(L_2|a\rangle\langle a \oplus 1|L_2^\dagger)_S \\ & + \beta\alpha^*(L_1|1\rangle\langle 0|L_1^\dagger)_Q \otimes \$(L_2|a \oplus 1\rangle\langle a|L_2^\dagger)_S \\ & + |\beta|^2(L_1|1\rangle\langle 1|L_1^\dagger)_Q \otimes \$(L_2|a \oplus 1\rangle\langle a \oplus 1|L_2^\dagger)_S. \end{aligned} \tag{24}$$

We can write the probability P that Bob obtains $|a\rangle_S$ as

$$\begin{aligned} P &= \mathrm{Tr}_{QS}[\rho_{L_1,L_2}^{QS}(\tau)\Pi_{L_1,L_2}^{QS}] \\ &= |\alpha|^2\langle a|L_2^\dagger\$(L_2|a\rangle\langle a|L_2^\dagger)L_2|a\rangle + |\beta|^2\langle a \oplus 1|L_2^\dagger\$(L_2|a \oplus 1\rangle\langle a \oplus 1|L_2^\dagger)L_2|a \oplus 1\rangle. \end{aligned} \tag{25}$$

Seeing this, we find the following fact. Although the initial state $|\psi\rangle_Q$ of the system Q is a superposition of $|0\rangle$ and $|1\rangle$, we may regard the state as a mixed state of $|\psi\rangle_Q = |0\rangle$ and $|\psi\rangle_Q = |1\rangle$ with classical probability for evaluating P.

Therefore, the probability of Bob's authentication is equal to an average of probabilities that a network of quantum gates in figure 8 gives $|\phi\rangle_S$ as an outcome from an incoming state

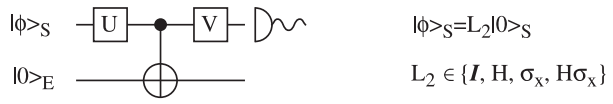

Figure 8. Eve's intercept/resend attack on one qubit.

$|\phi\rangle_S = L_2|0\rangle_S$ for all of $L_2 \in \mathcal{L}$. Here, we evaluate P as follows. U and V are arbitrary unitary transformations applied to one qubit. We assume U is defined as

$$U|\varphi_0\rangle = |0\rangle \qquad U|\varphi_1\rangle = |1\rangle \tag{26}$$

where $\{|\varphi_0\rangle, |\varphi_1\rangle\}$ is a certain orthonormal basis of $\mathcal{H}_2$. Then, we write $|\phi\rangle = c_0|\varphi_0\rangle + c_1|\varphi_1\rangle$. The state is transformed on the network of figure 8 as

$$\begin{aligned} |\phi\rangle_S|0\rangle_E &= (c_0|\varphi_0\rangle_S + c_1|\varphi_1\rangle_S)|0\rangle_E \\ &\xrightarrow{U} (c_0|0\rangle_S + c_1|1\rangle_S)|0\rangle_E \\ &\xrightarrow{\text{C-NOT}} c_0|0\rangle_S|0\rangle_E + c_1|1\rangle_S|1\rangle_E \\ &\xrightarrow{V} c_0V|0\rangle_S|0\rangle_E + c_1V|1\rangle_S|1\rangle_E. \end{aligned} \tag{27}$$

Seeing (27), we find that Eve measures the enciphered qubit in the basis $\{|\varphi_0\rangle, |\varphi_1\rangle\}$ and sends a ket vector of a basis $\{V|0\rangle, V|1\rangle\}$ according to the result of the measurement. Hence, we can write the probability P_ϕ that Bob gets the correct signature for $|\phi\rangle_S$ in spite of Eve's illegal act as

$$P_\phi = |c_0|^2|\langle\phi|V|0\rangle|^2 + |c_1|^2|\langle\phi|V|1\rangle|^2. \tag{28}$$

From now on, for simplicity, we write equations with density operators. Defining

$$\begin{aligned} &\rho_\phi = |\phi\rangle\langle\phi| \qquad \tilde{\rho}_0 = |\varphi_0\rangle\langle\varphi_0| \qquad \tilde{\rho}_1 = |\varphi_1\rangle\langle\varphi_1| \\ &\tilde{\rho}'_0 = V|0\rangle\langle 0|V^\dagger \qquad \tilde{\rho}'_1 = V|1\rangle\langle 1|V^\dagger \end{aligned} \tag{29}$$

we can write (27) as

$$\rho_\phi \to \$(\rho_\phi) = (\mathrm{Tr}\,\rho_\phi\tilde{\rho}_0)\tilde{\rho}'_0 + (\mathrm{Tr}\,\rho_\phi\tilde{\rho}_1)\tilde{\rho}'_1 \tag{30}$$

and (28) as

$$P_\phi = \mathrm{Tr}[\$(\rho_\phi)\rho_\phi]. \tag{31}$$

Four density operators $L_2|0\rangle\langle 0|L_2^\dagger$ ($L_2 \in \mathcal{L}$), emitted as $|\phi\rangle_S$ with equal probability, are described as

$$\rho_\updownarrow = \tfrac{1}{2}(\boldsymbol{I} + \sigma_z) \qquad \rho_\leftrightarrow = \tfrac{1}{2}(\boldsymbol{I} - \sigma_z) \qquad \rho_\odot = \tfrac{1}{2}(\boldsymbol{I} + \sigma_x) \qquad \rho_\otimes = \tfrac{1}{2}(\boldsymbol{I} - \sigma_x). \tag{32}$$

Then we define

$$\tilde{\rho}_i = \tfrac{1}{2}[\boldsymbol{I} + (-1)^i\boldsymbol{X}\cdot\boldsymbol{\sigma}] \qquad \tilde{\rho}'_j = \tfrac{1}{2}[\boldsymbol{I} + (-1)^j\boldsymbol{X}'\cdot\boldsymbol{\sigma}] \qquad \text{for} \quad i, j \in \{0, 1\} \tag{33}$$

where $\boldsymbol{X} = (X, Y, Z)$ and $\boldsymbol{X}' = (X', Y', Z')$ are arbitrary three-component real vectors with $|\boldsymbol{X}|^2 = |\boldsymbol{X}'|^2 = 1$. Using the following formula:

$$\mathrm{Tr}(\boldsymbol{I} + \boldsymbol{A}\cdot\boldsymbol{\sigma})(\boldsymbol{I} + \boldsymbol{B}\cdot\boldsymbol{\sigma}) = 2(1 + \boldsymbol{A}\cdot\boldsymbol{B}) \tag{34}$$

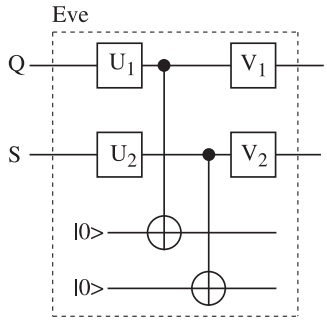

Figure 9. Eve's intercept/resend attack on the system Q and S.

and averaging four kinds of P_ϕ, we estimate $P_{\rm B}$ that Bob measures the correct signature in spite of Eve's illegal act at

$$P_{\rm B} = \tfrac{1}{4}(P_{\updownarrow} + P_{\leftrightarrow} + P_{\odot} + P_{\otimes}) = \tfrac{1}{4}(2 + XX' + ZZ') \leqslant \tfrac{3}{4}. \tag{35}$$

Therefore, the probability where Alice and Bob do not notice Eve make an attack by the network of figure 8 is $\frac{3}{4}$ or less. If Eve makes the intercept/resend attack on the system Q, we can give a similar discussion. Consequently, the probability that Alice and Bob do not notice Eve's attacks on m qubits (either Q or S in each pair) is at most $\left(\frac{3}{4}\right)^m$.

Next, we consider the case that Eve makes the intercept/resend attack on both qubits of a pair QS independently in figure 9 (U_1, U_2, V_1 and V_2 are arbitrary unitary transformations). Measuring ρ^{QS} transmitted from Alice, Eve sends the following density operator $\rho^{QS'}$ to Bob,

$$\rho^{QS'} = \$(\rho^{QS}) = \sum_{i,j\in\{0,1\}} {\rm Tr}(\rho^{QS}\tilde{\rho}_{Q,i}\tilde{\rho}_{S,j})\tilde{\rho}'_{Q,i}\tilde{\rho}'_{S,j} \tag{36}$$

where

$$\begin{aligned}
\tilde{\rho}_{Q,i} &= U_1^\dagger|i\rangle\langle i|U_1 = \tfrac{1}{2}[\boldsymbol{I} + (-1)^i\boldsymbol{X}_1\cdot\boldsymbol{\sigma}] \\
\tilde{\rho}_{S,j} &= U_2^\dagger|j\rangle\langle j|U_2 = \tfrac{1}{2}[\boldsymbol{I} + (-1)^j\boldsymbol{X}_2\cdot\boldsymbol{\sigma}] \\
\tilde{\rho}'_{Q,i} &= V_1|i\rangle\langle i|V_1^\dagger = \tfrac{1}{2}[\boldsymbol{I} + (-1)^i\boldsymbol{X}_3\cdot\boldsymbol{\sigma}] \\
\tilde{\rho}'_{S,j} &= V_2|j\rangle\langle j|V_2^\dagger = \tfrac{1}{2}[\boldsymbol{I} + (-1)^j\boldsymbol{X}_4\cdot\boldsymbol{\sigma}]
\end{aligned} \tag{37}$$

and $|\boldsymbol{X}_k|^2 = 1$ ($k = 1, \ldots, 4$).

Here, we can assume $|a\rangle_S$ to be $|0\rangle_S$ without losing generality. We write a transmitted state of Q as $|\psi\rangle_Q = \alpha|0\rangle + \beta|1\rangle$. Because Alice has 16 kinds of ways to send the state for $L_1, L_2 \in \mathcal{L}$, Bob's final probability for authentication is described as

$$P_{\rm B} = \tfrac{1}{16}\sum_{L_1,L_2\in\mathcal{L}} {\rm Tr}[\$(\rho^{QS}_{L_1,L_2})\Pi^{QS}_{L_1,L_2}]. \tag{38}$$

Writing the density operator of the state $\alpha L_1|0\rangle_Q L_2|0\rangle_S + \beta L_1|1\rangle_Q L_2|1\rangle_S$ that Alice sends to Bob as $\rho^{QS}_{L_1,L_2}$, we can describe its explicit form as

$$\begin{aligned}
\rho^{QS}_{L_1,L_2} = {}& |\alpha|^2(L_1|0\rangle\langle 0|L_1^\dagger)_Q \otimes (L_2|0\rangle\langle 0|L_2^\dagger)_S + \alpha\beta^*(L_1|0\rangle\langle 1|L_1^\dagger)_Q \otimes (L_2|0\rangle\langle 1|L_2^\dagger)_S \\
&+\beta\alpha^*(L_1|1\rangle\langle 0|L_1^\dagger)_Q \otimes (L_2|1\rangle\langle 0|L_2^\dagger)_S + |\beta|^2(L_1|1\rangle\langle 1|L_1^\dagger)_Q \otimes (L_2|1\rangle\langle 1|L_2^\dagger)_S.
\end{aligned} \tag{39}$$

The projection operator for Bob is given by

$$\Pi^{QS}_{L_1,L_2} = (L_1|0\rangle\langle 0|L_1^\dagger)_Q \otimes (L_2|0\rangle\langle 0|L_2^\dagger)_S + (L_1|1\rangle\langle 1|L_1^\dagger)_Q \otimes (L_2|1\rangle\langle 1|L_2^\dagger)_S. \tag{40}$$

Equation (38) is linear for $\rho^{QS}_{L_1,L_2}$. Therefore, we can divide (39) into terms for calculation.

First, we think about the first and fourth terms of (39). We write the first term as

$$\varrho^{QS}_{L_1,L_2} = (L_1|0\rangle\langle 0|L_1^\dagger)_Q \otimes (L_2|0\rangle\langle 0|L_2^\dagger)_S. \tag{41}$$

For example, if $L_1 = L_2 = \boldsymbol{I}$, we obtain

$$\varrho^{QS}_{\boldsymbol{I},\boldsymbol{I}} = \tfrac{1}{4}(\boldsymbol{I} + \sigma_z)_Q \otimes (\boldsymbol{I} + \sigma_z)_S \tag{42}$$

$$\Pi^{QS}_{\boldsymbol{I},\boldsymbol{I}} = \tfrac{1}{4}[(\boldsymbol{I} + \sigma_z)_Q \otimes (\boldsymbol{I} + \sigma_z)_S + (\boldsymbol{I} - \sigma_z)_Q \otimes (\boldsymbol{I} - \sigma_z)_S] \tag{43}$$

and

$$\mathrm{Tr}[\$(\varrho^{QS}_{\boldsymbol{I},\boldsymbol{I}})\Pi^{QS}_{\boldsymbol{I},\boldsymbol{I}}] = \tfrac{1}{2}(1 + Z_1Z_2Z_3Z_4). \tag{44}$$

From similar calculations, we obtain

$$\mathrm{Tr}[\$(\varrho^{QS}_{L_1,L_2})\Pi^{QS}_{L_1,L_2}] = \begin{cases} \frac{1}{2}(1 + Z_1Z_2Z_3Z_4) & \text{for} \quad L_1, L_2 \in \{\boldsymbol{I}, \sigma_x\} \\ \frac{1}{2}(1 + X_1X_2X_3X_4) & \text{for} \quad L_1, L_2 \in \{H, H\sigma_x\} \\ \frac{1}{2}(1 + Z_1X_2Z_3X_4) & \text{for} \quad L_1 \in \{\boldsymbol{I}, \sigma_x\},\ L_2 \in \{H, H\sigma_x\} \\ \frac{1}{2}(1 + X_1Z_2X_3Z_4) & \text{for} \quad L_1 \in \{H, H\sigma_x\},\ L_2 \in \{\boldsymbol{I}, \sigma_x\}. \end{cases} \tag{45}$$

Therefore, we obtain

$$\tfrac{1}{16}\sum_{L_1,L_2} \mathrm{Tr}[\$(\varrho^{QS}_{L_1,L_2})\Pi^{QS}_{L_1,L_2}] = \tfrac{1}{2} + \tfrac{1}{8}(X_1X_3 + Z_1Z_3)(X_2X_4 + Z_2Z_4). \tag{46}$$

Next, we think about the second and third terms of (39). We write the second term as

$$\Delta\varrho^{QS}_{L_1,L_2} = (L_1|0\rangle\langle 1|L_1^\dagger)_Q \otimes (L_2|0\rangle\langle 1|L_2^\dagger)_S. \tag{47}$$

For example, if $L_1 = L_2 = \boldsymbol{I}$, we obtain

$$\begin{aligned} &\Delta\varrho^{QS}_{\boldsymbol{I},\boldsymbol{I}} = \tfrac{1}{4}(\sigma_x + \mathrm{i}\sigma_y)_Q \otimes (\sigma_x + \mathrm{i}\sigma_y)_S \\ &\mathrm{Tr}[\$(\Delta\varrho^{QS}_{\boldsymbol{I},\boldsymbol{I}})\Pi^{QS}_{\boldsymbol{I},\boldsymbol{I}}] = \tfrac{1}{2}(X_1 + \mathrm{i}Y_1)(X_2 + \mathrm{i}Y_2)Z_3Z_4. \end{aligned} \tag{48}$$

From similar calculations, we obtain

$\mathrm{Tr}[\$(\Delta\varrho^{QS}_{L_1,L_2})\Pi^{QS}_{L_1,L_2}]$

$$= \begin{cases} & \epsilon = 1 & \epsilon = -1 \\ \frac{1}{2}(X_1 + \mathrm{i}\epsilon Y_1)(X_2 + \mathrm{i}\epsilon Y_2)Z_3Z_4 & (L_1, L_2) = (\boldsymbol{I}, \boldsymbol{I}) & (\sigma_x, \sigma_x) \\ -\frac{1}{2}(X_1 + \mathrm{i}\epsilon Y_1)(X_2 - \mathrm{i}\epsilon Y_2)Z_3Z_4 & (\boldsymbol{I}, \sigma_x) & (\sigma_x, \boldsymbol{I}) \\ \frac{1}{2}(Z_1 - \mathrm{i}\epsilon Y_1)(Z_2 - \mathrm{i}\epsilon Y_2)X_3X_4 & (H, H) & (H\sigma_x, H\sigma_x) \\ -\frac{1}{2}(Z_1 - \mathrm{i}\epsilon Y_1)(Z_2 + \mathrm{i}\epsilon Y_2)X_3X_4 & (H, H\sigma_x) & (H\sigma_x, H) \\ \frac{1}{2}(X_1 + \mathrm{i}\epsilon Y_1)(Z_2 - \mathrm{i}\epsilon Y_2)Z_3X_4 & (\boldsymbol{I}, H) & (\sigma_x, H\sigma_x) \\ -\frac{1}{2}(X_1 + \mathrm{i}\epsilon Y_1)(Z_2 + \mathrm{i}\epsilon Y_2)Z_3X_4 & (\boldsymbol{I}, H\sigma_x) & (\sigma_x, H) \\ \frac{1}{2}(Z_1 - \mathrm{i}\epsilon Y_1)(X_2 + \mathrm{i}\epsilon Y_2)X_3Z_4 & (H, \boldsymbol{I}) & (H\sigma_x, \sigma_x) \\ -\frac{1}{2}(Z_1 - \mathrm{i}\epsilon Y_1)(X_2 - \mathrm{i}\epsilon Y_2)X_3Z_4 & (H, \sigma_x) & (H\sigma_x, \boldsymbol{I}). \end{cases} \tag{49}$$

Consequently, we obtain

$$\frac{1}{16}\sum_{L_1,L_2}\mathrm{Tr}[\$(\Delta\varrho^{QS}_{L_1,L_2})\Pi^{QS}_{L_1,L_2}] = -\frac{1}{8}Y_1Y_2(Z_3 - X_3)(Z_4 - X_4). \tag{50}$$

Finally, obtaining

$$P_{\mathrm{B}} = \frac{1}{2} + \frac{1}{8}(X_1X_3 + Z_1Z_3)(X_2X_4 + Z_2Z_4) - \frac{1}{8}(\alpha\beta^* + \alpha^*\beta)Y_1Y_2(Z_3 - X_3)(Z_4 - X_4) \tag{51}$$

we can show $P_{\mathrm{B}} \leqslant \frac{3}{4}$ (see appendix A). Therefore, if $|\Psi\rangle_Q$ is an n-qubit product state and if Eve makes the intercept/resend attack on both qubits of a pair QS independently as in figure 9, the probability that Eve's illegal acts cannot be found is equal to $\frac{3}{4}$ or less per qubit.

In particular, if the transmitted information is classical, $|\Psi\rangle_Q$ is a product state of $|0\rangle$ and $|1\rangle$. All of the $2n$ qubits transmitted are in states chosen from four ket vectors of two conjugate bases at random. If we regard $\boldsymbol{a}$ as a key of an n-bit random string and $|\Psi\rangle_Q$ as an n-bit enciphered classical message, our method is equivalent to the one-time pad method with BB84. Assuming Eve makes attacks on m pairs of qubits in QS, we can estimate the probability of Eve's success in eavesdropping at $\left(\frac{3}{4}\right)^m$ or less.

Then, we consider the case where $|\Psi\rangle_Q$ is an arbitrary entangled state of n qubits. The enciphered state of $|\Psi\rangle_Q$ with U_i^Q is also entangled and it is given by (14).

First, we consider that Eve makes the intercept/resend attack on either one in a pair of qubits of the system Q and S as in figure 7. If Eve makes this attack on m pairs out of n pairs of the system QS, we can regard the transmission as sending an ensemble of product states, where each qubit is $|0\rangle$ or $|1\rangle$, with classical probabilities, such as (25). We can think in a similar way before and conclude that the probability that Eve's illegal act cannot be found is $\left(\frac{3}{4}\right)^m$ or less.

Next, we consider the case where Eve makes the attack on both qubits of a pair on the entangled system QS as in figure 9. If Eve makes this attack on m pairs out of n pairs, we can write the probability that Eve is not found as an equation which is similar to (51) and it is estimated as $\left(\frac{3}{4}\right)^m$ or less (see appendix B).

5. Privacy amplification process

From the previous discussion, we obtain the following results. If an arbitrary quantum state is enciphered by our method, the probability that Alice and Bob do not notice Eve is at most $\frac{3}{4}$ per qubit. (Both product and entangled states are available. We assume that Eve always makes eavesdropping with the intercept/resend attack.) Hence, if Eve makes attacks on m enciphered pairs, her success probability is given by $\left(\frac{3}{4}\right)^m$ and it decreases exponentially against m.

However, there is a problem. In our method, if Eve replaces a pair of enciphered qubits with a pair of random ones, Alice and Bob do not notice her illegal act with a probability of $\frac{1}{2}$. In this case, they disclose passwords and Eve obtains one qubit of original information with fidelity 1. It is important that Eve gets a correct qubit and she knows that she obtains the correct one.

Such a problem can also occur in BB84. It is possible that Alice and Bob share the same random binary string and Eve knows a few bits of it exactly. To overcome this problem, for example, Alice and Bob can choose some bits at random from the shared binary string and make a new bit from a summation of them with modulo 2 [4]. If they repeat this process and

create a new binary string that is shorter than the original one, Eve's expected information decreases to 0 in some asymptotic limit. Such a technique is called privacy amplification.

On the other hand, in our protocol, Eve's success probability for eavesdropping on one qubit cannot always reach 0. To decrease it to 0 asymptotically, Alice and Bob apply our protocol over and over again. To make the discussion simple, we consider encryption of one qubit of quantum information for a while.

Preparing an arbitrary one-qubit state $|\psi_1\rangle$ and a one-qubit signature $|a_1\rangle$ ($\forall a_1 \in \{0, 1\}$), Alice applies our protocol to $|\psi_1\rangle|a_1\rangle$ and generates an entangled two-qubit state $|\psi_2\rangle$. Then, she prepares other qubits $|a_2\rangle|a_3\rangle$ for a signature, and enciphers $|\psi_2\rangle|a_2\rangle|a_3\rangle$ again. She obtains a four-qubit state $|\psi_3\rangle$.

If Eve wants to obtain quantum information of $|\psi_1\rangle$ with fidelity 1, she has to interact with all four qubits of $|\psi_3\rangle$. For example, if Eve replaces $|\psi_3\rangle$ with four random qubits, Alice and Bob notice her illegal act with probability of $\left(\frac{1}{2}\right)^3 = \frac{1}{8}$, because they carry out the authentication process with $|a_1\rangle$, $|a_2\rangle$ and $|a_3\rangle$.

If Alice enciphers $|\psi_1\rangle$ for n times, the nth encryption needs 2^{n-1} signature qubits. If Eve makes attacks on all enciphered qubits of $|\psi_{n+1}\rangle$, the probability that Alice and Bob do not notice her act is $\left(\frac{3}{4}\right)^{N/2}$ at most, where $N = 2^n$ is the number of all enciphered qubits. (The probability $\frac{3}{4}$ comes from the fact that Alice enciphers the state with rectilinear and circular bases at random, and it does not depend on $|\psi_n\rangle$.) Hence, Eve's probability of success that she obtains $|\psi_1\rangle$ with fidelity of 1 decreases exponentially against the number of qubits, and reaches 0 in the limit of $N \to \infty$.

Another method is as follows. Alice and Bob share a random binary string beforehand as the first password (subscripts of Pauli matrices) in secrecy by BB84. Because they do not need to disclose it, Eve can never obtain information on $|\psi_1\rangle$ at all even in the case where they do not notice Eve's disturbance. In this method, the privacy amplification has to be done for BB84 actually.

6. Discussion

To understand our method more clearly, we consider a simple one and compare it with ours. For transmitting an n-qubit quantum state in secrecy, we can take the following method. Enciphering an n-qubit state ρ_n as (13), Alice prepares another n qubits as check ones that are given as $\{|0\rangle, |1\rangle\}$ or $\{(1/\sqrt{2})(|0\rangle \pm |1\rangle)\}$ at random respectively. Then, Alice permutes all of the $2n$ qubits at random and sends them to Bob.

Here, we assume Eve tries to eavesdrop on only one qubit of ρ_n. Because Eve does not know which qubits are check ones, the probability that Alice and Bob fail to notice Eve's illegal act can be $\left(\frac{1}{2}\right)\left[1 + \left(\frac{3}{4}\right)\right] = \frac{7}{8}$ as maximum, in spite of $\frac{3}{4}$ for our method. This is because we use entanglement in our method.

Even if Eve prepares an arbitrary one-qubit state by herself in spite of taking away a qubit from ρ_n, its expectation value of fidelity is equal to $\frac{1}{2}$. This shows that Eve's success probability of eavesdropping is always equal to $\frac{1}{2}$ or more. In our method, if Eve interacts with enciphered qubits, the probability of her success is equal to at most $\frac{3}{4}$ per qubit (without privacy amplification). It is similar to the BB84.

In this paper, the security against Eve's attack using entanglement is not considered (for example, the case where she uses a quantum computer for eavesdropping as in figure 10). In figure 10, it is difficult to evaluate the upper bound of the probability that Bob measures the signature correctly for arbitrary unitary transformations U_1, U_2, V_1 and V_2. For instance,

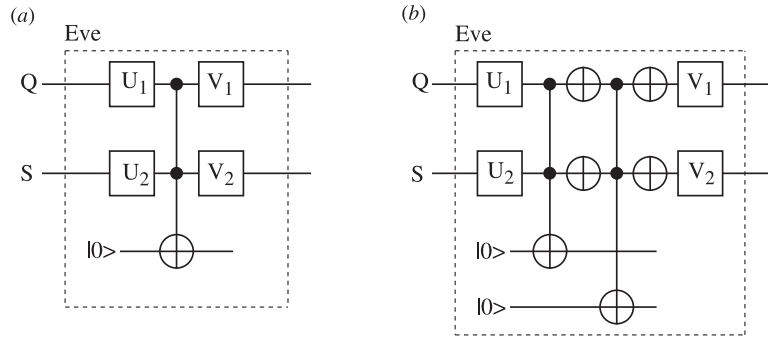

Figure 10. Eve's attack on the system QS by using entanglement.

assuming

$$U_1 = U_2 = V_1 = V_2 = U \qquad \text{where} \quad U = \begin{pmatrix} \cos(\pi/8) & \sin(\pi/8) \\ \sin(\pi/8) & -\cos(\pi/8) \end{pmatrix} \tag{52}$$

and $|\Psi\rangle_Q$ represents classical information (an n-qubit product state of $|0\rangle$ and $|1\rangle$), we obtain $P_{\mathrm{B}} = \left(\frac{13}{16}\right) > \left(\frac{3}{4}\right)$ for figure 10(a) and $P_{\mathrm{B}} = \left(\frac{11}{16}\right) < \left(\frac{3}{4}\right)$ for figure 10(b). Eavesdropping with U is equivalent to measuring and resending a qubit in the following basis:

$$|\varphi_i\rangle\langle\varphi_i| = \tfrac{1}{2}[\boldsymbol{I} + (-1)^i \boldsymbol{X}\cdot\boldsymbol{\sigma}] \qquad \boldsymbol{X} = \left(\frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}}\right) \tag{53}$$

which is called the Breidbart basis [4]. For figure 10(a), P_{B} may exceed $\frac{3}{4}$. But, the amount of information Eve can extract in figure 10(a) seems to be less than the amount of information she obtains by the intercept/resend attack on one qubit as in figure 7.

In our method, if Eve takes away qubits, Alice and Bob lose original information on them.

We mentioned in section 1 that the classical key distribution can be done using just uncertainty, and entanglement is not essential for it [8, 9]. On the other hand, for transmitting quantum states by quantum teleportation, entanglement plays an essential role [6]. Our method uses both properties.

Recently, a method for transmitting classical binary data (not a classical random string) in secrecy with a pair of entangled photons has been proposed [17]. It is characterized by the following facts. First, Alice and Bob prepare two conjugate bases on $\mathcal{H}_2^2$ each for encoding a message and measuring photons. Second, they use a two-dimensional subspace of $\mathcal{H}_2^2$ for encoding a binary digit.

Acknowledgments

We thank O Hirota, M Osaki, and H Inamori for helpful discussions. We also thank R de Wolf for useful comments. HA thanks M Okuda for encouragement.

Appendix A. The maximum value of P_{B} for a product state $|\Psi\rangle_Q$

Here, we show that P_{B} defined in (51) never exceeds $\frac{3}{4}$.

Because of $|\alpha|^2 + |\beta|^2 = 1$, we get $-1 \leqslant \alpha\beta^* + \alpha^*\beta \leqslant 1$. Hence, altering the signs of X_i as $X_i \to -X_i$ ($i = 1, \ldots, 4$), we can write the upper bound of P_{B} as

$$P_{\mathrm{B}} \leqslant \tfrac{1}{2} + \tfrac{1}{8} f_{\max} \tag{A1}$$

where $f_{\max}$ is the maximum value of

$$f = (X_1X_3 + Z_1Z_3)(X_2X_4 + Z_2Z_4) + Y_1Y_2(X_3 + Z_3)(X_4 + Z_4) \tag{A2}$$

with $|\boldsymbol{X}_i|^2 = 1$ and $X_i, Y_i, Z_i \geqslant 0$ for $i = 1, \ldots, 4$.

Seeing (A2), we give another form of f as follows:

$$f = |\boldsymbol{A} \cdot \boldsymbol{B}| \tag{A3}$$

where

$$\boldsymbol{A} = (X_1X_3 + Z_1Z_3, Y_1(X_3 + Z_3)) \tag{A4}$$

$$\boldsymbol{B} = (X_2X_4 + Z_2Z_4, Y_2(X_4 + Z_4)). \tag{A5}$$

(We pay attention to the fact that $\boldsymbol{A}$ and $\boldsymbol{B}$ are two-component real vectors.) From the Cauchy–Schwarz inequality, we obtain

$$f \leqslant |\boldsymbol{A}||\boldsymbol{B}|. \tag{A6}$$

Therefore, by estimating the maximum values of $|\boldsymbol{A}|$ and $|\boldsymbol{B}|$, we derive the upper bound of f.

We can write $|\boldsymbol{A}|^2$ in the following form:

$$|\boldsymbol{A}|^2 = (1 - Z_1^2)X_3^2 + (1 - X_1^2)Z_3^2 + 2(X_1Z_3)(Z_1X_3) + 2Y_1^2(X_3Z_3). \tag{A7}$$

On the other hand, from the arithmetic–geometric inequality, we obtain

$$\begin{aligned} &(X_1Z_3)(Z_1X_3) \leqslant \tfrac{1}{2}[(X_1Z_3)^2 + (Z_1X_3)^2] \\ &X_3Z_3 \leqslant \tfrac{1}{2}(X_3^2 + Z_3^2). \end{aligned} \tag{A8}$$

Therefore, we obtain

$$|\boldsymbol{A}|^2 \leqslant (1 + Y_1^2)(X_3^2 + Z_3^2) \leqslant 1 + Y_1^2 \leqslant 2. \tag{A9}$$

We obtain $|\boldsymbol{A}| \leqslant \sqrt{2}$. In a similar way, we obtain $|\boldsymbol{B}| \leqslant \sqrt{2}$. From these results, we can conclude that $f \leqslant 2$ and $f_{\max} = 2$.

Appendix B. The maximum value of P_{B} for an entangled state $|\Psi\rangle_Q$

We estimate the probability that Eve's illegal act cannot be found in the case where she makes the intercept/resend attack on m pairs of qubits on the system QS for an arbitrary entangled $|\Psi\rangle_Q$ of n qubits.

For simplicity, we assume $|\Psi\rangle_Q$ to be an arbitrary entangled state of a two-qubit system qq' at first,

$$|\Psi\rangle_Q = \sum_{i,j\in\{0,1\}} c_{ij}|i\rangle_q \otimes |j\rangle_{q'} \in \forall\mathcal{H}_2^2. \tag{B1}$$

Alice puts two qubits of the system S $(= ss')$ for the signature on the qubits of the system Q $(= qq')$, respectively. Then, she makes entanglement between the systems Q and S with C-NOT gates, applies $L_1, L_2, L_1', L_2' \in \mathcal{L}$ to four qubits q, s, q', s', respectively, and sends them to Bob (see figure 7). Eve makes the intercept/resend attacks on the systems q, s, q', s' respectively as shown in figure 9. We can assume the initial states of qubits s, s' that represent the signature to be $|0\rangle_s|0\rangle_{s'}$ without losing generality.

Writing the state sent by Alice as

$$\sum_{i,j\in\{0,1\}} c_{ij} L_1|i\rangle_q L_2|i\rangle_s \otimes L_1'|j\rangle_{q'} L_2'|j\rangle_{s'} \tag{B2}$$

we can describe the density operator explicitly as

$$\begin{aligned}\rho^{QS}_{L_1L_2L_1'L_2'} = (L_1L_2L_1'L_2') \sum_{i,j\in\{0,1\}} [&|c_{ij}|^2(|i\rangle\langle i|_q \otimes |i\rangle\langle i|_s) \otimes (|j\rangle\langle j|_{q'} \otimes |j\rangle\langle j|_{s'}) \\ &+c_{ij}c^*_{i\bar{j}}(|i\rangle\langle i|_q \otimes |i\rangle\langle i|_s) \otimes (|j\rangle\langle \bar{j}|_{q'} \otimes |j\rangle\langle \bar{j}|_{s'}) \\ &+c_{ij}c^*_{\bar{i}j}(|i\rangle\langle \bar{i}|_q \otimes |i\rangle\langle \bar{i}|_s) \otimes (|j\rangle\langle j|_{q'} \otimes |j\rangle\langle j|_{s'}) \\ &+c_{ij}c^*_{\bar{i}\bar{j}}(|i\rangle\langle \bar{i}|_q \otimes |i\rangle\langle \bar{i}|_s) \otimes (|j\rangle\langle \bar{j}|_{q'} \otimes |j\rangle\langle \bar{j}|_{s'})](L_1L_2L_1'L_2')^\dagger\end{aligned} \tag{B3}$$

where $\bar{i} = i + 1 \pmod 2$.

Eavesdropping on the state $\rho^{QS}_{L_1L_2L_1'L_2'}$, Eve transforms it to the following state:

$$\$(\rho^{QS}_{L_1L_2L_1'L_2'}) = \sum_{i,j,k,l\in\{0,1\}} \mathrm{Tr}(\rho^{QS}_{L_1L_2L_1'L_2'} \tilde{\rho}_{q,i}\tilde{\rho}_{s,j}\tilde{\rho}_{q',k}\tilde{\rho}_{s',l}) \tilde{\rho}'_{q,i}\tilde{\rho}'_{s,j}\tilde{\rho}'_{q',k}\tilde{\rho}'_{s',l} \tag{B4}$$

where

$$\begin{aligned} \tilde{\rho}_{q,i} &= \tfrac{1}{2}[\boldsymbol{I} + (-1)^i \boldsymbol{X}_1 \cdot \boldsymbol{\sigma}], & \tilde{\rho}_{s,j} &= \tfrac{1}{2}[\boldsymbol{I} + (-1)^j \boldsymbol{X}_2 \cdot \boldsymbol{\sigma}] \\ \tilde{\rho}'_{q,i} &= \tfrac{1}{2}[\boldsymbol{I} + (-1)^i \boldsymbol{X}_3 \cdot \boldsymbol{\sigma}], & \tilde{\rho}'_{s,j} &= \tfrac{1}{2}[\boldsymbol{I} + (-1)^j \boldsymbol{X}_4 \cdot \boldsymbol{\sigma}] \\ \tilde{\rho}_{q',k} &= \tfrac{1}{2}[\boldsymbol{I} + (-1)^k \boldsymbol{X}_1' \cdot \boldsymbol{\sigma}], & \tilde{\rho}_{s',l} &= \tfrac{1}{2}[\boldsymbol{I} + (-1)^l \boldsymbol{X}_2' \cdot \boldsymbol{\sigma}] \\ \tilde{\rho}'_{q',k} &= \tfrac{1}{2}[\boldsymbol{I} + (-1)^k \boldsymbol{X}_3' \cdot \boldsymbol{\sigma}], & \tilde{\rho}'_{s',l} &= \tfrac{1}{2}[\boldsymbol{I} + (-1)^l \boldsymbol{X}_4' \cdot \boldsymbol{\sigma}] \end{aligned} \tag{B5}$$

and $|\boldsymbol{X}_k|^2 = |\boldsymbol{X}_k'|^2 = 1$ $(k = 1, \ldots, 4)$. Bob measures it with the projection operator,

$$\begin{aligned}\Pi^{QS}_{L_1L_2L_1'L_2'} = &(L_1L_2)(|0\rangle\langle 0|_q \otimes |0\rangle\langle 0|_s + |1\rangle\langle 1|_q \otimes |1\rangle\langle 1|_s)(L_1L_2)^\dagger \\ &\otimes(L_1'L_2')(|0\rangle\langle 0|_{q'} \otimes |0\rangle\langle 0|_{s'} + |1\rangle\langle 1|_{q'} \otimes |1\rangle\langle 1|_{s'})(L_1'L_2')^\dagger.\end{aligned} \tag{B6}$$

The probability that Bob measures the correct signature is given by

$$\begin{aligned} P_{\mathrm{B}} = \left(\tfrac{1}{16}\right)^2 &\sum_{L_1,L_2\in\mathcal{L}} \sum_{L_1',L_2'\in\mathcal{L}} \mathrm{Tr}\left[\$(\rho^{QS}_{L_1L_2L_1'L_2'})\Pi^{QS}_{L_1L_2L_1'L_2'}\right] \\ &= \left[\tfrac{1}{2} + \tfrac{1}{8}(X_1X_3 + Z_1Z_3)(X_2X_4 + Z_2Z_4)\right]\left[\tfrac{1}{2} + \tfrac{1}{8}(X_1'X_3' + Z_1'Z_3')(X_2'X_4' + Z_2'Z_4')\right] \\ &\quad + \sum_{i,j\in\{0,1\}} \left\{c_{ij}c^*_{i\bar{j}}\left[\tfrac{1}{2} + \tfrac{1}{8}(X_1X_3 + Z_1Z_3)(X_2X_4 + Z_2Z_4)\right]\right. \\ &\quad \times\left[-\tfrac{1}{8}Y_1'Y_2'(Z_3' - X_3')(Z_4' - X_4')\right] \\ &\quad +c_{ij}c^*_{\bar{i}j}\left[-\tfrac{1}{8}Y_1Y_2(Z_3 - X_3)(Z_4 - X_4)\right]\left[\tfrac{1}{2} + \tfrac{1}{8}(X_1'X_3' + Z_1'Z_3')(X_2'X_4' + Z_2'Z_4')\right] \\ &\quad \left.+c_{ij}c^*_{\bar{i}\bar{j}}\left[-\tfrac{1}{8}Y_1Y_2(Z_3 - X_3)(Z_4 - X_4)\right]\left[-\tfrac{1}{8}Y_1'Y_2'(Z_3' - X_3')(Z_4' - X_4')\right]\right\}. \end{aligned} \tag{B7}$$

From $\sum_{i,j\in\{0,1\}} |c_{ij}|^2 = 1$, we obtain $|\sum_{i,j\in\{0,1\}} c_{ij}c^*_{i\bar{j}}| \leqslant 1$, $|\sum_{i,j\in\{0,1\}} c_{ij}c^*_{\bar{i}j}| \leqslant 1$ and $|\sum_{i,j\in\{0,1\}} c_{ij}c^*_{\bar{i}\bar{j}}| \leqslant 1$. Therefore, using the result obtained in appendix A, we can conclude

$$P_{\mathrm{B}} \leqslant \left(\tfrac{1}{2} + \tfrac{1}{8} f_{\max}\right)^2 = \left(\tfrac{3}{4}\right)^2. \tag{B8}$$

(We pay attention to a fact that each term of P_{B} can be gathered with a binomial coefficient.) When Eve attacks on m pairs out of enciphered qubits generated from an arbitrary n-qubit entangled state $|\Psi\rangle_Q$, we obtain $P_{\mathrm{B}} \leqslant \left(\frac{3}{4}\right)^m$.

References

[1] Deutsch D and Jozsa R 1992 *Proc. R. Soc.* A **439** 553–8
Shor P W 1994 Algorithms for quantum computation: discrete logarithms and factoring *Proc. 35th Ann. Symp. on Foundations of Computer Science* ed S Goldwasser (Los Alamitos, CA: IEEE Computer Society) pp 124–34
Shor P W 1997 *SIAM J. Comput.* **26** 1484–509

[2] Wootters W K and Zurek W H 1982 *Nature* **299** 802–3

[3] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing (Bangalore, 1984)* pp 175–9

[4] Bennett C H, Bessette F B, Brassard G, Salvail L and Smolin J 1992 *J. Cryptology* **5** 3–28

[5] Bennett C H, Brassard G and Ekert A K 1992 *Sci. Am.* **267** no 4 50–7

[6] Bennett C H, Brassard G, Crépeau C, Jozsa R, Peres A and Wootters W K 1993 *Phys. Rev. Lett.* **70** 1895–9

[7] Bouwmeester D, Pan J-W, Mattle K, Eibl M, Weinfurter H and Zeilinger A 1997 *Nature* **390** 575–9
Furusawa A, Sørensen J L, Braunstein S L, Fuchs C A, Kimble H J and Polzik E S 1998 *Science* **282** 706–9

[8] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661–3

[9] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557–9

[10] Bennett C H, Brassard G, Popescu S, Schumacher B, Smolin J A and Wootters W K 1996 *Phys. Rev. Lett.* **76** 722–5
Deutsch D, Ekert A, Jozsa R, Macchiavello C, Popescu S and Sanpera A 1996 *Phys. Rev. Lett.* **77** 2818–21
Bennett C H, DiVincenzo D P, Smolin J A and Wootters W K 1996 *Phys. Rev.* A **54** 3824–51

[11] Boykin P O and Roychowdhury V 2000 Optimal encryption of quantum bits *Los Alamos Preprint* quant-ph/0003059
Mosca M, Tapp A and de Wolf R 2000 Private quantum channels and the cost of randomizing quantum information *Los Alamos Preprint* quant-ph/0003101

[12] Feynman R P 1996 *Feynman Lectures on Computation* (Reading, MA: Addison-Wesley)
Barenco A, Bennett C H, Cleve R, DiVincenzo D P, Margolus N, Shor P, Sleator T, Smolin J and Weinfurter H 1995 *Phys. Rev.* A **52** 3457–67

[13] Chuang I L and Yamamoto Y 1995 *Phys. Rev.* A **52** 3489–96

[14] Turchette Q A, Hood C J, Lange W, Mabuchi H and Kimble J 1995 *Phys. Rev. Lett.* **75** 4710–3

[15] Gottesman D 1997 Stabilizer codes and quantum error correction *PhD Thesis* California Institute of Technology *Los Alamos Preprint* quant-ph/9705052

[16] Schumacher B 1996 *Phys. Rev.* A **54** 2614–28
Fujiwara A and Algoet P 1999 *Phys. Rev.* A **59** 3290–4

[17] Shimizu K and Imoto N 1999 *Phys. Rev.* A **60** 157–66