A QUANTUM SECURE DIRECT COMMUNICATION PROTOCOL for SENDING A QUANTUM STATE and ITS SECURITY ANALYSIS

YUMIKO MURAKAMI
Mitsubishi Electric Corporation
Information Technology R&D Center
5-1-1, Ohuna, Kamakura City, Kanagawa
JAPAN

MASAKI NAKANISHI
Nara Institute of Science and Technology
Graduate school of Information Science
8916-5, Takayama-cho, Ikoma City, Nara
JAPAN

SHIGERU YAMASHITA
Nara Institute of Science and Technology
Graduate school of Information Science
8916-5, Takayama-cho, Ikoma City, Nara
JAPAN

YASUHIKO NAKASHIMA
Nara Institute of Science and Technology
Graduate school of Information Science
8916-5, Takayama-cho, Ikoma City, Nara
JAPAN

MANABU HAGIWARA
Advanced Industrial Science and Technology
Research Center for Information Security
1-18-13, Sotokanda, Chiyoda-ku, Tokyo
JAPAN

Abstract: These days, quantum secret communication algorithms different from quantum key distribution protocol have been proposed, which are called quantum secure direct communication protocols. These do not aim to have a key agreement between two communicators, but, to send a secret message directly using quantum devices. In this paper, we propose a new quantum secret direct communication protocol which has advantages over the current ones and also discuss its security analysis against the man-in-the-middle attack.

Key–Words: Quantum secure direct communication, Quantum key distribution, No-cloning inequality, Depolarizing channel

1 Introduction

Although the perfect secret communication protocol has been one of the most interesting issues in human history, we do not have any perfectly secure symmetric key encryption schemes yet, except one-time pad. The dilemma that a secure key distributuion is needed for a secure data transmission seems to be resolved by the appearance of public key cryptosystems (PKCs). However, they have some problems, e.g., the heavy workload and the security based on the computational assumption. Furthermore, most of the current PKCs are considered to be broken by the appearance of quantum computers. The quantum key distribution (QKD) protocol [1] realized a key distribution scheme with unconditional security (that is, not based on any computational assumption.) This is a protocol that the distant two parties can have the same random private classical key by using quantum devices. This so-called BB84 triggered the growth of constructions of secure quantum cryptosystems. These days, there are so many QKD algorithms and the unconditional security of each protocol is discussed from various angles. QKD stands on the position that, for safe data transmission, it is enough to agree on the same key by communicators securely, which has not been realized with symmetric key encryption.

These days, different approaches of quantum secret communication protocols have been taken, and especially we focus on one of them, called quantum secure direct communication (QSDC) protocols

[2, 3, 5, 6, 8, 9, 7, 10, 11]. A QSDC protocol basically enables a direct secret transmission without key agreement in the process. Compared to QKD, QSDC has a big difference that a sender can transfer the *desired* data, not random. In this paper, we propose a new QSDC protocol, which has some advantages over the other QSDCs or some QKDs. The current QSDCs have some undesirable features that: (1) transmittable information is limited to be classical; and (2) many EPR pairs or GHZ states are required. In particular, the latter is not a good feature because of the technical difficulty. Our QSDC protocol solves these problems. First, it can carry an arbitrary quantum state. This indicates that the protocol can be used as a quantum communiocation scheme between two hubs of quantum network; Second, no entanglement resource is employed. In additional, an eavesdropper on a channel can be detected efficiently. In general, to increase the detection rate, many dummy qubits are required. But, in our protocol, the detection rate increases by the *rally* of a message; Last, our protocol tolerates against photon-number-splitting (PNS) attacks. Because the encoding operations applied to the secret quantum state never be announced at any step of the protocol. So, even if Eve obtains the perfect copy of the secret qubit, it is not enough to unveil the secret perfectly. Thus, an ideal strict photon generator is not required in our protocol.

However, obviously, the PNS attack is not the only eavesdropping. In this paper, we show that our protocol is secure against the *man-in-the-middle attack* that Eve pretends to be Bob. In other words, the probability that the attack goes well is extremely small, or the quality of the copy of the secret gets really worse if she wants to increase the success probability.

In the next section, Sec. 2, some basics required to understand our prooves are explained. In Sec. 3, our new QSDC protocol is presented. In Sec. 4, we show that the protocol is secure against the man-in-the-middle attack.

2 Asymmetric universal cloning machine and the depolarizing probability

Consider an asymmetric universal cloning machine produces whose two copies emerge from *depolarizing channels*. Through the channel, a quantum state ρ is depolarized as it is replaced by the maximum mixed state, $I/2$, with probability p and it is left untouched with probability $1-p$. The consequent quantum state, $\mathcal{E}_p(\rho)$, is described as

$$\mathcal{E}_p(\rho) = (1-p)\rho + p\frac{I}{2}. \tag{1}$$

The fidelity of $\mathcal{E}_p(\rho)$ is described as

$$\begin{aligned} & F(\rho, \mathcal{E}_p(\rho)) \\ = \; & Tr\sqrt{\rho}((1-p)\rho + pI/2)\sqrt{\rho} \\ = \; & 1 - \frac{p}{2}. \end{aligned} \tag{2}$$

Because, for arbitrary ρ, $I/2 = (\rho + X\rho X + Y\rho Y + Z\rho Z)/4$, equation (3) can be rewritten as follows.

$$\begin{aligned} \mathcal{E}_p(\rho) &= (1-\frac{3p}{4})\rho + \frac{p}{4}(X\rho X + Y\rho Y + Z\rho Z) \\ &= (1-p')\rho + \frac{p'}{3}(X\rho X + Y\rho Y + Z\rho Z) \end{aligned} \tag{3}$$

where $p' = 3p/4$. We can see the depolarizing channel as the noise such that the probabilities of applying of operators I, X, Y, Z to a quantum system are $(1-p'), p'/3, p'/3, p'/3$, respectively.

Now, consider the two copies of ρ which emerge from the depolarizing channels, $\gamma_1 = \mathcal{E}_p(\rho), \gamma_2 = \mathcal{E}_q(\rho)$. By equation (3), the two are depolarized with probability p' and q' respectively. The relationship between the probabilities is described by *no-cloning inequality* [4],

$$\begin{aligned} & p' + \sqrt{p'q'} + q' \geq 3/4 \\ \therefore \; & p + \sqrt{pq} + q \geq 1 \end{aligned} \tag{4}$$

3 The model and protocol

First, we describe the key idea of our direct communication protocol. Suppose the situation that a sender (Alice) wants to send a secret message to a receiver (Bob) securely, but they have no key agreement in advance.

Physically, they achieve the purpose as Fig. 1. Alice has a treasure box and wants to send it to Bob. First, Alice locks the box. She holds the key in her hands and sends the box to Bob by post or something. Bob can never open it unless he has Alice's key. He puts a new lock on the box, and holds his key and sends the box back to Alice. Alice opens her lock and sends the box to Bob. Finally, Bob gets the treasure just by his key. At every transmission, the box is locked by either key. An eavesdropper who does not have the keys cannot open the box.

This method has both of advantage and disadvantage. ADVANTAGE: This method needs no key agreement. A sender and a receiver simply have their

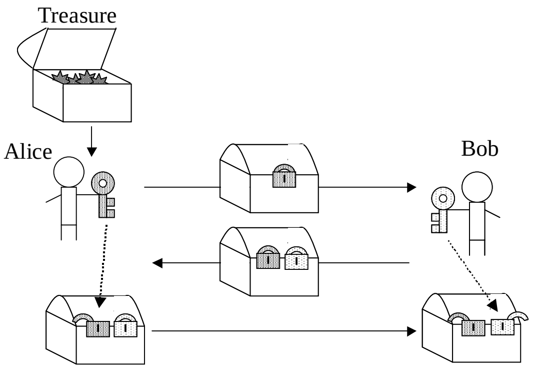

Figure 1: Physical implementation

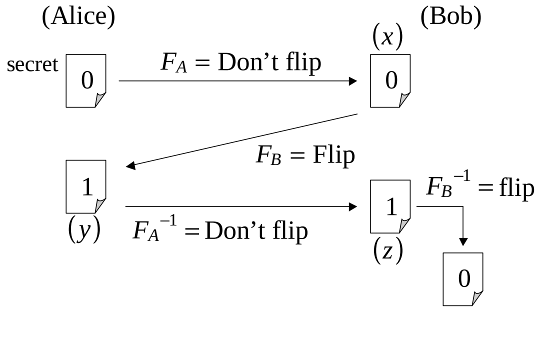

Figure 2: Digital implementation

private keys in their keeping. This means the tolerance of some attacks such as a PNS attack. DISADVANTAGE: The classical (digital) implementation of this method cannot achieve good security against the man-in-the-middle attack.

Classical implementation and the problem
Fig. 2 illustrates a digital implementation. Alice has a secret binary sequence, s, say 0 in the figure for simplicity. She encodes it by operation F_A="Don't flip" for example and sends $x = F_A(s) = 0$ to Bob. Bob similarly encodes the data by operation F_B="Flip," independent from F_A, and sends $y = F_B(x) = 1$ back to Alice. Alice decodes the bit by F_A^{-1} ="Don't flip" and sends $z = F_A^{-1}(y) = 1$ to Bob. Bob decodes z by F_B^{-1} ="Flip" and gets the secret data, $F_B^{-1}(z) = 0$.

An eavesdropper, Eve, keeps watching the transmission channel. She makes a copy of every transmitted data, x, y and z, and gets the secret since $x \oplus y \oplus z = s$. The reasons why she needs no special efforts to get the secret data are as follows:

- the data encoding is whether flip or not;
- anybody can see the transmitted data without destruction; and
- anybody can make a perfect copy of the transmitted data.

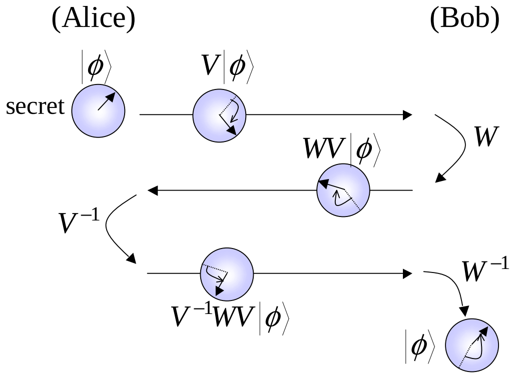

Figure 3: Naive quantum implementation

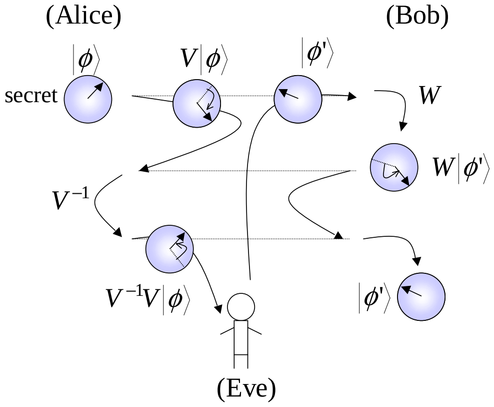

Figure 4: Eve's man-in-the-middle attack

Next, let's consider the following naive quantum implementation.

Quantum implementation
Fig. 3 illustrates the framework of our quantum implementation. Alice has a secret of a single-qubit state to be sent which is described as a unit-length vector of Bloch sphere, $|\phi\rangle$. Let S be Pauli group, e.g., $S = \{\sigma_i | 0 \le i \le 3\}$. Alice chooses an operator, $V \in S$ randomly, applies it to $|\phi\rangle$, and sends it to Bob through a quantum channel. (Needless to say, $V|\phi\rangle$ appears a maximally mixed state for others.) Bob also independently chooses an operator, $W \in S$, applies it to $V|\phi\rangle$, and sends it back to Alice. Alice applies $V^\dagger$ to $WV|\phi\rangle$ and sends it to Bob. Last of all, Bob applies $W^\dagger$ to $V^\dagger WV|\phi\rangle$ and gets the secret, $|\phi\rangle$.

In this implementation, the eavesdropping as in the classical implementation does not work well, because

- nobody can "see" the state of the qubit and calculate the difference between the two arbitrary quantum states without destruction; and

- nobody can make a perfect copy of an unknown quantum state.

However, Eve can make an active attack as Fig. 4, the man-in-the-middle attack. Eve intercepts the transmitted qubit from Alice to Bob and gets it back to Alice directly, pretending she is Bob. Alice opens her lock and sends state $V^\dagger V|\phi\rangle$ to Bob. Eve has only to steal the qubit.

We improve this weak and naive implementation and introduce the following QSDC protocol.

The model of our protocol

The model of our protocol is defined as follows. There are two noiseless channels between Alice and Bob, an unauthenticated quantum channel and an authenticated classical (public) channel. We take no thought of loss of qubits and assume that the quantum communication devices, e.g., a photon generator and a detector, are ideal instruments which don't make any mistakes. Alice and Bob, in advance, agree on a set of unitary operators, S, such that for any two distinct elements V and W in S, $W^\dagger V^\dagger W V|\phi\rangle = e^{i\theta} I|\phi\rangle$ and $\sum_{V\in S}\frac{1}{|S|}V|\phi\rangle\langle\phi|V^\dagger$ is a maximally mixed state, Pauli group for example.

The procedure

The numbers k and r are determined in advance based on the security parameter, where k is the number of dummy qubits and r is the number of rounds.

(P1) **(Setup)** Alice has a secret of a single-qubit state. Set $i = 1$.

(P2) **(Alice's encoding phase)** If $i = r$, jump to phase (P5). Alice chooses an operation, V_i, from S randomly and applies it to the secret qubit. Alice newly prepares k qubits (we call them dummies), where each is in the random initial state in the 2-dimensional Hilbert space. Alice randomly picks out one position from $k+1$ positions and puts the encoded secret there and the dummies in the other positions at random. Alice sends this sequence of qubits (the secret and dummies) to Bob.

(P3) **(Bob's encoding phase)** Bob randomly chooses $k+1$ operators from S and applies them to the received sequence. He permutes the order of the sequence and sends it back to Alice. At this moment, he does not know which operation is applied to the secret, but, let the operation be W_i for convenience.

(P4) **(Detection phase)** Alice informs Bob of the reception and the positions of dummies in (P2). Bob announces his permutation and the operators applied to dummies through the classical channel. By using these information, Alice cancels Bob's operations for dummies and runs a detection test, which is the measurement of every dummy with respect to the initial state and its orthonormal state. When the answer is not "being in the initial state," Alice and Bob abort this protocol. Otherwise, set $i = i+1$. Go back to phase (P2).

(P5) **(Alice's decoding phase)** Alice applies $V_i = (V_{i-1}V_{i-2}\cdots V_1)^\dagger$ to the secret qubit. Alice prepares k dummies in the random states and randomly picks out one position from $k+1$ positions and puts the secret qubit there and the dummies in the other positions at random. Alice sends the sequence to Bob.

(P6) **(Detection phase)** Bob informs Alice of the reception. Alice announces the position of dummies and their initial states. Bob runs the detection test similarly to (P4). If any of the dummies has changed, they abort this protocol.

(P7) **(Bob's decoding phase)** Bob applies $W_i = (W_{i-1}W_{i-2}\cdots W_1)^\dagger$ to the secret qubit and gets the original secret.

In our protocol, resending the secret is restricted, because it is impossible to make a perfect copy of an unknown quantum state. We leave the issue out of consideration in this paper.

4 The security analysis of the proposed protocol

Eve cannot directly know the secret by keeping watch on a transmission channel because every quantum state on the channel is maximally mixed. In our protocol, a sender and a receiver do not have a key agreement in advance nor in the process nor afterward, but instead they individually encode the secret by their private keys and *shuttle* the qubit any number of times. We consider Eve makes a man-in-the-middle attack as Fig. 5. In our protocol, encoding is the sequence of the quantum operations that Alice/Bob chooses randomly at all rounds but the last, and the subsequence does not help to decode at all. So, if once Bob has applied an operation to the secret, there is no chance intuitively for Eve to remove the Bob's operation because $V_r\cdots V_{i+1}\mathbf{W_i}V_i\cdots V_1|\phi\rangle$ is a maxi-

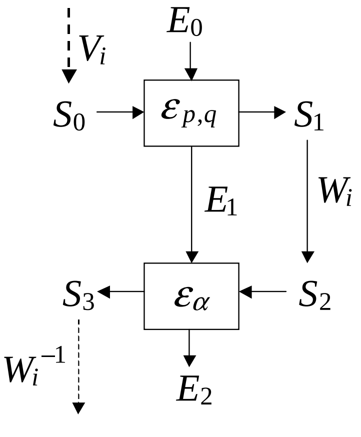

Figure 5: Eve's attack

mally mixed state. Eve has to repeats this man-in-the-middle attack every round. But, in fact, the secret is always buried in dummies, and thus Eve guesses the position of the secret qubit and attacks. This is illustrated by Fig. 5. Eve first entangles the emitted quantum system from Alice, S_0, (consisting of the secret qubit and dummies,) with her arbitrary quantum system E_0. Then she applies a cloning operator to combined system S_0E_0 and sends system S_0 to Bob. E_0 is not necessarily a single-qubit system, but Eve can extract a single-qubit clone from E_0. She should get it back to Alice in the ideal man-in-the-middle attack, however, it would bring the higher detection rate at the subsequent test by Alice. So she entangles E_1 with S_2, applies a unitary operator to them, and sends system S_2 to Alice.

Before the discussion of security analysis, let us show the total picture of the rally under the influence of Eve and define some notations. Fig. 6 illustrates the flow of a single-qubit. $\rho_i, \rho'_i, \eta_i, \eta'_i$ are the mixed states of a single-qubit on the quantum channel. V_i/W_i is Alice's/Bob's operation. Note that $V_r \cdots V_1 = I$ and $W_r \cdots W_1 = I$. Eve keeps watching on every transmission and can touches any of the qubits. Take the i-th round transmission as an example. Eve makes a copy of ρ_i, defined by μ_i. $\mathcal{E}_{p_i,q_i}$ means such a noisy channel, a *depolarizing channel*, where p_i and q_i relates the accuracy of the clone μ_i and ρ_i respectively. Then, Eve returns η'_i to Alice, the mixture of μ_i and η_i: $\eta'_i = \alpha_i\mu_i + (1-\alpha_i)\eta_i$, where α_i is a classical probability. At the last, Eve makes a clone of ρ_r, which is also the clone of $|\psi_0\rangle$ in this attack. We call it ρ_E.

μ_i and ρ'_i are the two copies of ρ_i which emerge from depolarizing channel as seen in Sec.2. Then, by

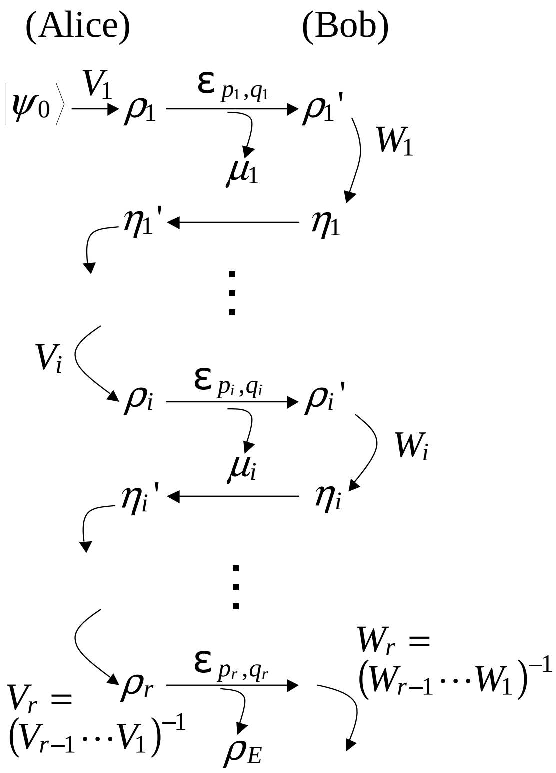

Figure 6: The procedure

equation (2), they can be rewritten as

$$\begin{aligned} \mu_i &= (1-p_i)\rho_i + p_i I/2, \\ \rho'_i &= (1-q_i)\rho_i + q_i I/2. \end{aligned}$$

Thus,

$$\begin{aligned} \rho_i &= V_i \eta'_{i-1} V_i^\dagger \\ &= V_i\{\alpha_{i-1}\mu_{i-1} + (1-\alpha_{i-1})I/2\}V_i^\dagger \\ &= V_i\{\alpha_{i-1}\{(1-p_{i-1})\rho_{i-1} + p_{i-1}I/2\} \\ &\qquad\qquad + (1-\alpha_{i-1})I/2\}V_i^\dagger \\ &= \alpha_{i-1}(1-p_{i-1})V_i\rho_{i-1}V_i^\dagger \\ &\qquad\qquad + (1-\alpha_{i-1}(1-p_{i-1}))I/2, \\ \cdots & \\ &= \prod_{m=1}^{i-1}\alpha_m(1-p_m)V_i\cdots V_1|\psi_0\rangle\langle\psi_0|V_1^\dagger\cdots V_i^\dagger \\ &\qquad\qquad + \{1-\prod_{m=1}^{i-1}\alpha_m(1-p_m)\}I/2. \end{aligned}$$

Here, we let $|\psi_i\rangle = V_i \cdots V_1 |\psi_0\rangle$ and rewrite ρ_i simply as follows:

$$\begin{aligned} \rho_i &= \prod_{m=1}^{i-1}\alpha_m(1-p_m)\,|\psi_i\rangle\langle\psi_i| \\ &\qquad\qquad + \{1-\prod_{m=1}^{i-1}\alpha_m(1-p_m)\}I/2. \end{aligned} \tag{5}$$

Similarly to ρ_i, μ_i can be rewritten with $|\psi_i\rangle$ as follows.

$$\begin{aligned}\mu_i &= (1-p_i)\rho_i + p_i I/2 \\ &= \prod_{m=1}^{i-1}\alpha_m \prod_{m=1}^{i}(1-p_m)\,|\psi_i\rangle\langle\psi_i| \\ &\qquad + \{1-\prod_{m=1}^{i-1}\alpha_m\prod_{m=1}^{i}(1-p_m)\}I/2. \quad (6)\end{aligned}$$

Now we are ready to go to the security analysis.

Definition 1 *A protocol is secure if and only if an eavesdropper can obtain the information about the secret message with the fidelity $|F(|\psi_0\rangle\langle\psi_0|,\rho_E) - 1/2| \le o(2^{-s})$, where $|\psi_0\rangle$ is the state of the original secret; ρ_E is the clone state of $|\psi_0\rangle$ Eve reconstructs; and s is the security parameter the sender decides.*

Theorem 2 *When Alice and Bob use s^2 dummies and repeat the rally $2s$ times, our protocol is secure against a man-in-the-middle attack defined above.*

Before the proof of this theorem, we introduce some lemmas.

Lemma 3 *If $\exists i, F(\rho_i,\rho_i') \ge 1-O(\delta)$, then $F(\rho_i,\mu_i) \le 1/2+O(\delta)$.*

(Proof) Let $F(\rho_i,\rho_i') = F_B$ and $F(\rho_i,\mu_i) = F_E$. By equation (2), $F_B = 1-p_i/2 \ge 1-O(\delta)$ and $F_E = 1-q_i/2$. By no-cloning inequality (4),

$$\sqrt{(1-F_B)(1-F_E)} \ge 1/2-(1-F_B)-(1-F_E).$$

Therefore,

$$\begin{aligned}O(\sqrt{\delta}) &\ge \sqrt{1-F_B} \\ &\ge \sqrt{(1-F_B)(1-F_E)} \\ &\ge 1/2-(1-F_B)-(1-F_E) \\ &\ge 1/2-(1-F_E)-O(\delta) \\ \therefore F_E &\le 1/2+O(\delta)\end{aligned}$$

□

Lemma 4 *Let ε and δ be positive real numbers less than 1. Suppose that for some i, $|F(\rho_i,|\psi_i\rangle\langle\psi_i|) - 1/2| \le \varepsilon$, where $|\psi_i\rangle = V_i\cdots V_1|\psi_0\rangle$. If $F(\rho_i,\rho_i') \ge 1-O(\delta)$, $|F(|\psi_i\rangle\langle\psi_i|,\mu_i)-1/2| \le O(\delta\varepsilon)$.*

(Proof) By equations (2) and (5), the fidelity between ρ_i and $|\psi_i\rangle$ is given as

$$F(\rho_i,|\psi_i\rangle\langle\psi_i|) = 1/2\{1+\prod_{m=1}^{i-1}\alpha_m(1-p_m)\}.$$

$$\therefore \prod_{m=1}^{i-1}\alpha_m(1-p_m)/2 \le \varepsilon$$

By lemma 3, $F(\rho_i,\mu_i)-1/2 = 1/2(1-p_i) \le O(\delta)$. Therefore,

$$\begin{aligned}&F(|\psi_i\rangle\langle\psi_i|,\mu_i)-1/2 \\ =\ &1/2\prod_{m=1}^{i-1}\alpha_m\prod_{m=1}^{i}(1-p_m) \\ =\ &1/2\prod_{m=1}^{i-1}\alpha_m(1-p_m)\cdot(1-p_i) \\ \le\ &O(\delta\varepsilon)\end{aligned}$$

□

Lemma 5 *Suppose that $F(\rho_{i_1},\rho_{i_1}')$,..., $F(\rho_{i_n},\rho_{i_n}') \ge 1-O(\delta)$, where i_1,...,i_n are mutually distinct, then $|F(|\psi_0\rangle\langle\psi_0|,\rho_E)-1/2| \le O(\delta^n)$.*

(Proof) Without loss of generality, $i_1 < i_2 < \cdots < i_n$. Suppose $|F(\rho_{i_1},|\psi_{i_1}\rangle\langle\psi_{i_1}|) - 1/2| = \varepsilon$, then $|F(|\psi_{i_1}\rangle\langle\psi_{i_1}|,\mu_{i_1})-1/2| \le O(\delta\varepsilon)$, by lemma 4 and thus $1/2\prod_{m=1}^{i_1-1}\alpha_m\prod_{m=1}^{i_1}(1-p_m) \le O(\delta\varepsilon)$.

$$\begin{aligned}\therefore\ &|F(\rho_{i_2},|\psi_{i_2}\rangle\langle\psi_{i_2}|)-1/2| \\ =\ &1/2\{\prod_{m=1}^{i_2-1}\alpha_m(1-p_m)\} \\ \le\ &1/2\{\prod_{m=1}^{i_2-2}\alpha_m(1-p_m)\} \\ \le\ &\cdots \\ \le\ &1/2\{\prod_{m=1}^{i_1-1}\alpha_m(1-p_m)\} \\ \le\ &O(\delta\varepsilon)\end{aligned}$$

By lemma 4, $|F(|\psi_{i_2}\rangle\langle\psi_{i_2}|,\mu_{i_2})-1/2| \le O(\delta^2\varepsilon)$. By repeated this, $|F(|\psi_{i_n}\rangle\langle\psi_{i_n}|,\mu_{i_n})-1/2| \le O(\delta^n)$. Therefore,

$$\begin{aligned}F(|\psi_0\rangle\langle\psi_0|,\rho_E)-1/2 &= 1/2\prod_{m=1}^{r-1}\alpha_m(1-p_m) \\ &\le 1/2\prod_{m=1}^{i_n-1}\alpha_m\prod_{m=1}^{i_n}(1-p_m) \\ &\le O(\delta^n).\end{aligned}$$

□

Lemma 6 *If $F(\rho_i,\rho_i') < 1-\Omega(\delta)$, the probability that Eve passes the detection test by Alice in the i-th transmission is $(1-\Omega(\delta))^k$ at most, where k is the number of dummy qubits.*

(Proof) It should be noted that, in our protocol, the qubit carrying the secret message is not an object of the detection test, but dummy qubit is. First, let us consider the average probability that Eve passes the detection test in the i-th transmission per dummy qubit. Eve returns $\eta_i' = \alpha_i\mu_i + (1-\alpha_i)\eta_i$ to Alice and Alice performs the detection test on $W_i^\dagger \eta_i' W_i$. The fidelity between $W_i^\dagger \eta_i' W_i$ and ρ_i corresponds to the likelihood that Eve passes the detection test.

$$\begin{aligned}
&W_i^\dagger \eta_i' W_i \\
&= \alpha_i W_i^\dagger \mu_i W_i + (1-\alpha_i)\rho_i' \\
&= \alpha_i W_i^\dagger \{(1-p_i)\rho_i + p_i I/2\} W_i \\
&\qquad + (1-\alpha_i)\{(1-q_i)\rho_i + q_i I/2\} \\
&= \{\alpha_i(1-p_i)W_i^\dagger \rho_i W_i + (1-\alpha_i(1-p_i))I/2\} + \\
&\quad \{(1-\alpha_i)(1-p_i)\rho_i + (1-(1-\alpha_i)(1-p_i))I/2\} \\
&\qquad\qquad - I/2.
\end{aligned}$$

Let $\lambda = \alpha_i(1-p_i)W_i^\dagger \rho_i W_i + (1-\alpha_i(1-p_i))I/2$ and $\xi = (1-\alpha_i)(1-p_i)\rho_i + (1-(1-\alpha_i)(1-p_i))I/2$. By the linearity,

$$F(W_i^\dagger \mu_i W_i, \rho_i) = F(\rho_i, \lambda) + F(\rho_i, \xi) - F(\rho_i, I/2).$$

Considering $W_i \in S$,

$$\begin{aligned}
\lambda &= \frac{1}{4}\Sigma_j\{\alpha_i(1-p_i)\sigma_j^\dagger \rho_i \sigma_j \\
&\qquad + (1-\alpha_i(1-p_i))I/2\} \\
&= I/2. \\
\therefore F(\rho_i, \lambda) &= 1/2. \\
F(\rho_i, \xi) &= 1/2 + 1/2(1-\alpha_i)(1-q_i). \\
\therefore F(W_i^\dagger \mu_i W_i, \rho_i) &= 1/2 + 1/2(1-\alpha_i)(1-q_i) - 1/2 \\
&\leq 1 - q_i/2 \\
&= F(\rho_i, \rho_i') \\
&\leq 1 - \Omega(\delta).
\end{aligned}$$

Therefore, the probability that all the k dummies pass the detection test is $(1-\Omega(\delta))^k$. □

This lemma follows the next corollary.

Corollary 7 *If for $i = i_1, ..., i_n$, $F(\rho_i, \rho_i') < 1 - \Omega(\delta)$, the probability that Alice detects Eve through this protocol is at least $1 - (1-\Omega(\delta))^{kn}$.*

Now, we are ready to prove Theorem 2.

(Proof of Theorem 2) First, we consider a eavesdropper, Eve, makes an attack such that for $i = i_1, ..., i_{r/2}, ...$ (all mutually distinct), $F(\rho_i, \rho_i') \leq 1 - \Omega(1/s)$. Alice detects Eve by the end with probability $1 - (1-\Omega(\delta))^{kn/2}$ at least, by Corollary 7, and the protocol aborts in the middle. In this case, it is clear that $F(|\psi_0\rangle\langle\psi_0|, \rho_E) = 1/2$. Thus, this Eve can obtain the information about the secret with the extremely low probability averagely.

Then, Eve takes an attack such that for $i = i_1, ..., i_{r/2}, ...$ (all mutually distinct), $F(\rho_i, \rho_i') \geq 1 - O(1/s)$. By lemma 5,

$$\begin{aligned}
&|F(|\psi_0\rangle\langle\psi_0|, \rho_E) - 1/2| \\
&\leq O(s^{-r'}) \\
&\leq O(s^{-r/2}) \\
&\leq O(2^{-s}).
\end{aligned}$$

□

Acknowledgements This work was supported in part by KAKENHI (16092218), (18700011),(19700010).

References:

[1] C. H. Bennett and G. Brassard, Quantum cryptography: public key distribution and coin tossing, In Proc. IEEE International Conf. Computers, Systems, and Signal Processing, *Math. Nachr.*, 1984.

[2] K. Bostroem and T. Felbinger, Deterministic Secure Direct Communication Using Entanglement, *Phys. Rev. Lett. 89 187902*, 2002.

[3] Q. Y. Cai and B. W. Li, Improving the capacity of the Bostroem-Felbinger protocol, *Phys. Rev. A. 69, 054301*, 2004.

[4] N. J. Cerf, Pauli Cloning of a Quantum Bit, *Phys. Rev. Lett. 84, 4497*, 2000.

[5] F. G. Deng and G. L. Long, Secure direct communication with a quantum one-time pad, *Phys. Rev. A. 69, 052319*, 2004.

[6] T. Gao, F. L. Yan and Z. X. Wang, Quantum secure direct communication by Einstein-Podolsky-Rosen pairs and entanglement swapping, *quant-ph/0406083*, 2004.

[7] C. Wang, F. G. Deng, Y. S. Li, X. S. Liu and G. L. Long, Quantum secure direct communication with high-dimension quantum superdense coding, *Phys. Rev. A. 71, 044305*, 2005.

[8] J. Wang, Q. Zhang and C. J. Tang, Quantum secure direct communication without using perfect quantum channel, *quant-ph/0511092*, 2005.

[9] J. Wang, Q. Zhang and C. J. Tang, Multiparty controlled quantum secret direct communication using Greenberger-Horne-Zeilinger state, *quant-ph/0602166*, 2006.

[10] J. Wang, Q. Zhang and C. J. Tang, Quantum secure direct communication based on order rearrangement of single photons, *quant-ph/0603100*, 2006.

[11] Z. H. Zhang and Z. X. Man, Deterministic secure direct communication by using swapping quantum entanglement and local unitary operations, *quant-ph/0403218*, 2004.