A Quantum Key Distribution Protocol Based on the EPR Pairs and Its Simulation

Jian Li[1,2], Hengji Li[2(✉)], Chaoyang Li[2], Leilei Li[2], Yanyan Hou[1,2], Xiubo Chen[3], and Yuguang Yang[4]

[1] Center for Quantum Information Research, ZaoZhuang University, ZaoZhuang 277160, Shandong, China
[2] School of Computer Science, Beijing University of Posts Telecommunications, Beijing 100876, China
lihj@bupt.edu.cn
[3] Information Security Center, State Key Laboratory Networking and Switching Technology, Beijing University of Posts Telecommunications, Beijing 100876, China
[4] Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China

Abstract. A novel quantum key distribution protocol based on entanglement and dense coding is proposed, which does not need to store the qubits. Every four particles is divided into a group, of which $\{(1,2),(3,4)\}$ or $\{(1,3),(2,4)\}$ are in entanglement. Some of the groups are used to transfer the message, and the others are used to check the eavesdropping. In the message mode, the authorized party needn't to know the location information of the group, he only needs to make the unitary operation to the first and the forth of the group. Also, the trade-off between information and disturbance is calculated under the intercept-measure-resend attack and entanglement-measure attack, which tells that the protocol is asymptotically secure. Moreover, the quantum circuit simulation of the protocol is shown.

Keywords: Quantum key distribution · Entanglement · Quantum circuit simulation

With the rapid development of information technology and quantum physics [1], the quantum cryptography has become one of the rapidly developing applications of the quantum information theory. It employs quantum laws such as uncertainty principle and no-cloning theorem to solve the important problem of telecommunication channels protection from eavesdropping by the unauthorized users like Eve. It is provably secure against eavesdropping attack, in that, as a

Supported by the National Natural Science Foundation of China (Grant No. U1636106, No.61472048, No. 61671087, No. 61572053).

H. Song et al. (Eds.): SIMUtools 2019, LNICST 295, pp. 288–301, 2019.
https://doi.org/10.1007/978-3-030-32216-8_28

matter of fundamental principle, the secret data can not be comprised unknowingly to the illegitimate users of the channel.

In the last decade, researchers has made dramatic progress in the field of quantum cryptography. One of the quantum cryptography direction is the quantum key distribution (QKD), whose object is to create a common random key between two remote authorized users. Since Bennnett and Brassard presented the pioneer QKD protocol (BB84 protocol) [2] in 1984, a lot of attention has been focused on the protocol. In 1989, IBM and Montreal university first completed the experiment of quantum cryptography [3], which verified the feasibility of BB84 protocol. In ref [4], the researchers gave the proof of security of the BB84 protocol. Besides the BB84 protocol, there are some other typical schemes, such as Ekert 1991 protocol (Ekert91) [5], Bennett-Brassard-Mermin 1992 protocol (BBM92) [6], six-state protocol [7] and so on. In recent years, there are some new protocols proposed and developments of QKD, such as Refs [8–18].

Different from QKD, quantum secure direct communication (QSDC) protocol is designed for providing unidirectional communication in which information content is specified by the sender. Long et al. proposed the first QSDC protocol [19]. Later, Boström and Felbinger put forward a famous QSDC protocol based on EPR pairs, which is called "Ping-pong" protocol [20]. Since then, researchers have published many enhancements and modification of the ping-pong protocol, including superdense coding [21], usage of GHZ states for two [22] and multiparty [23] communication and so on. Many QSDC protocols were presented, including the protocols without using entanglement [24–28], the protocols using entanglement [29–32] and two-way QSDC protocols [33–38].

In above QSDC protocols, the transmitted message is the secret instead of random key bits. That is to say, the security requirements in the QSDC schemes are more stricter than the QKD protocol, because the message transmitted can never leaked out regardless of whether the eavesdropping would be detected or not. For example, researchers have found many security problems [39,40] in the ping-pong protocol when it is used as QSDC.

One of the technical difficulties that have been unable to overcome is the ultrashort storage time of quantum state. At present, the world record of quantum state storage time is only 3 ms at Heifei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics. All protocols that need to store quantum states in process have some limitations on the operability, like the ping-pong protocol, in which, the storage of one photon is necessary for a duration corresponding to twice the distance between Alice and Bob.

Considering the storage time limitation, in this paper, a new protocol for QKD based on entanglement and dense coding is proposed, which does not need to store quantum states in process. We emphasize that here, we restrict our protocol as just a QKD process instead of QSDC to have a more perfect secure communication. Then the securities of the protocol is analyzed. Moreover, the efficient quantum circuit simulation of the protocol is presented, which will be necessary to implement this protocol in experiment.

1 New QKD Protocol

For simplicity, this protocol is represented as GEQKD.

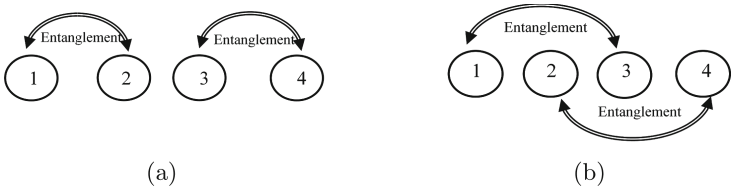

Fig. 1. The entanglement of two types of location

Firstly, every four bits of all classical bits is divided into a group in the GEQKD protocol and two EPR pairs are prepared for every group according to the entanglement. Then Bob transfers the two EPR states to Alice through the quantum channel. Secondly, After Alice receiving the EPR pairs, he only performs the unitary transformation on the first and fourth particle of each group and then transmit the group particles to Bob by the quantum channel. Lastly, Bob performs the correct Bell basis measurement based on the position information that he records previously, and compares the results with the EPR pairs that he previously sent. Then Bob can get the unitary operation performed by Alice and decodes the classical bits that Alice sends.

Now let us give an explicit process for GEQKD.

(p.1) Bob and Alice agree on that each of the four Bell states can carry two-quit classical information and encode $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$ and $|\Psi^-\rangle$ as 00, 01, 10 and 11, respectively.
(p.2) Bob prepares a large enough number of classical bits N in sequence and every four bits is divided into a group in order, which is called as C_i. Here the subscript indicates the group order in the sequence.
(p.3) Bob picks up one group in order, and numbers the four bits into $\{1, 2, 3, 4\}$. If all groups are took out, then go to p.7; otherwise then go to p.4.
(p.4) Bob prepares two EPR pairs based on the order of four bits of current group and dense coding mechanism, which is called the particles S_i (see Fig. 1). Meanwhile, Bob remembers the entanglement and the location information of the particles S_i and then transfers it to Alice by quantum channel.
(p.5) Alice receives the particles S_i. With probability c_1, she switches to control mode and proceeds with c.1, else he proceeds with m.1.
(c.1) Alice randomly chooses one location information $\{(1, 2), (3, 4)\}$ or $\{(1, 3),(2, 4)\}$ to extract every EPR pair and then makes the Bell basis measurement accordingly. Then Alice tells Bob which location he has chosen for each group and the outcomes $C_i^{'}$ of his measurements by classical channel.

(c.2) Bob receives the location information and the outcomes $C_i^{'}$ of her measurements. If she chooses incorrectly, discard the particles S_i and go to p.3. If she chooses correctly, Bob compare $C_i^{'}$ with the initial classical bits C_i. $C_i^{'} \neq C_i$: Eve is detected. Abort transmission. $C_i^{'} = C_i$: go to p.3.
(m.1) Alice makes one of the four unitary operations $\{I, X, Y, Z\}$ only to the first and the forth of the particles S_i. Table 1 shows the Bell states before and after the unitary operations. Then Alice sends the unitary particles $S_i^{'}$ back to Bob through quantum channel.
(m.2) Bob receives the particles $S_i^{'}$ and performs the correct Bell basis measurement based on the position information that he records previously. Then he compares his measurement results with the initial Bell states sent by himself and decodes the classical bits that Alice sends (see Table 1).
(p.6) Alice confirms that Bob receives the particles $S_i^{'}$. With probability c_2, she switches to control mode and proceeds with c.3, otherwise then go to p.3.
(c.3) Alice tells Bob the classical bits she transmits by classical channel.
(c.4) After Bob receiving the classical bits M_i, he compares M_i with the bits $M_i^{'}$ he decodes. $(M_i^{'} \neq M_i)$: Eve is detected. Abort transmission. $(M_i^{'} = M_i)$: go to p.3.
(p.7) confirming the safety of channel, Bob and Alice negotiate about the remaining raw key and perform the correction and privacy amplification, then obtain the final keys.

Table 1. The Bell states before and after the unitary operation

The initial	The end			
	$\|\Phi^+\rangle$	$\|\Phi^-\rangle$	$\|\Psi^+\rangle$	$\|\Psi^-\rangle$
$\|\Phi^+\rangle$	$I(00)$	$Z(01)$	$X(10)$	$Y(11)$
$\|\Phi^-\rangle$	$Z(01)$	$I(00)$	$Y(11)$	$X(10)$
$\|\Psi^+\rangle$	$X(10)$	$Y(11)$	$I(00)$	$Z(01)$
$\|\Psi^-\rangle$	$Y(11)$	$X(10)$	$Z(01)$	$Y(11)$

Table 2 shows the process that every group classical bits is transmitted to Bob after Alice performs the unitary transformation. Compared with MEQKD protocol proposed in the paper [8], GEQKD protocol makes full use of every group quantum bits while transmitting the message, instead of discarding half of the groups. Meanwhile, it can be found that the implementation of the GEQKD protocol is similar to the "Ping-pong" protocol, however, there are some fundamental differences. One is GEQKD protocol needs not to store the quit. Two is that only one particle of the EPR pair is sent in the ping-pong protocol, while two particles of the EPR pair are sent in the GEQKD protocol. Thus the eavesdropper Eve can perform the Bell basis measurement on the EPR pair to obtain the information.

Table 2. The example of the process that every group is transferred to Bob

Number of classical bits	1	2	3	4
Bobs random bit	1	0	1	1
Bob sending Bell states	$\|\Psi_{13}^{-}\rangle$	$\|\Phi_{24}^{-}\rangle$	$\|\Psi_{13}^{-}\rangle$	$\|\Phi_{24}^{-}\rangle$
Alices random bit	0	1	1	0
Bell states Alice measures and sends	Z	/	/	X
Bell states Bob measures	$\|\Psi_{13}^{+}\rangle$	$\|\Psi_{24}^{-}\rangle$	$\|\Psi_{13}^{+}\rangle$	$\|\Psi_{24}^{-}\rangle$
The message Bob decodes	0	1	1	0

2 Security of GEQKD Protocol

2.1 Intercept-Measure-Resend (IR) Attack

The family of individual attacks describes the most constrained attacks that have been studied. An important subfamily of individual attacks is the intercept-measure-resend (IR) attack, which Eve intercepts the quantum signal flying, performs the measurement on it, and conditioned on the result she obtains, she prepares a new quantum signal to the legitimate receiver. In the GEQKD protocol, in order to gain information about Alice's operation, Eve need to perform twice IR attacks. The first attack is in the quantum channel from Bob to Alice(B-A); the second attack is in the quantum channel from Alice to Bob(A-B).

Eve has no knowledge of EPR location information $\{(1,2),(3,4)\}$ or $\{(1,3),(2,4)\}$ sent by Bob, she can only guess which quit pairs to measure in. If she chooses correctly, she measures the correct Bell states as sent by Bob, and resends the correct Bell states to Alice. After Alice performs her coding operation, to decode the message that Alice encodes, Eve measures the Bell states again with the same location as the first IR attack. It should be noted that the Bell states does not collapse due to the correct location choice, thus Eve will not be detected. Table 3 gives an example of the process that Eve eavesdrops when she chooses correctly.

However, if she chooses incorrectly, the two quits are not entangled and the states sent to Alice cannot be the same as the states sent by Bob, which will make Eve detected with a certain probability in the control mode. It is worth noting that due to the existence of entanglement swapping, the new two bits will be entangled when she chooses incorrectly. Furthermore, when entering the control mode, the detection probability is $\frac{3}{4}$ in both B-A (Considering the case A chooses correctly, or the detection fails) and A-B quantum channel. Next, we will take the initial state $|\Psi_{13}^{-}\rangle|\Phi_{24}^{-}\rangle$ as an example to explain it.

Assuming that the initial state is $|\Psi_{13}^{-}\rangle|\Phi_{24}^{-}\rangle$, after Eve's measurement in the wrong location, it will become

$$|\Psi_{13}^{-}\rangle|\Phi_{24}^{-}\rangle = \frac{1}{2}(|\Psi_{12}^{-}\rangle|\Phi_{34}^{-}\rangle + |\Phi_{12}^{+}\rangle|\Psi_{34}^{+}\rangle - |\Phi_{12}^{-}\rangle|\Psi_{34}^{-}\rangle - |\Psi_{12}^{+}\rangle|\Phi_{34}^{+}\rangle), \quad (1)$$

Table 3. The example of the process that Eve eavesdrops (the right location choice)

Number of classical bits	1	2	3	4
Bobs random bit	1	0	1	1
Bob sending Bell states	$\|\Psi_{13}^-\rangle$	$\|\Phi_{24}^-\rangle$	$\|\Psi_{13}^-\rangle$	$\|\Phi_{24}^-\rangle$
Bell states Eve measures and sends	$\|\Psi_{13}^-\rangle$	$\|\Phi_{24}^-\rangle$	$\|\Psi_{13}^-\rangle$	$\|\Phi_{24}^-\rangle$
Alices random bit	0	1	1	0
Bell states Alice measures and sends	Z	/	/	X
Bell states Eve measures again	$\|\Psi_{13}^+\rangle$	$\|\Psi_{24}^-\rangle$	$\|\Psi_{13}^+\rangle$	$\|\Psi_{24}^-\rangle$
The message Eve decodes	0	1	1	0
Bell states Bob measures	$\|\Psi_{13}^+\rangle$	$\|\Psi_{24}^-\rangle$	$\|\Psi_{13}^+\rangle$	$\|\Psi_{24}^-\rangle$
The message Bob decodes	0	1	1	0

Suppose that Eve's measurement yields $|\Phi_{12}^+\rangle|\Psi_{34}^+\rangle$ with the probability $\frac{1}{4}$, which can be expanded as

$$|\Phi_{12}^+\rangle|\Psi_{34}^+\rangle = \frac{1}{2}(|\Phi_{13}^+\rangle|\Psi_{24}^+\rangle + |\Phi_{13}^-\rangle|\Psi_{24}^-\rangle + |\Psi_{13}^+\rangle|\Phi_{24}^+\rangle + |\Psi_{13}^-\rangle|\Phi_{24}^-\rangle), \tag{2}$$

then Alice performing a measurement using a correct sequence after Eve's measurement using an incorrect sequence will yield $|\Psi_{13}^-\rangle|\Phi_{24}^-\rangle$ with the probability of $\frac{1}{4}$, that is to say, Eve is not be detected. Similarly, the other three possible outcomes of Eve's measurement will yield $|\Psi_{13}^-\rangle|\Phi_{24}^-\rangle$ with the probability of $\frac{1}{4}$ after Alice performing a measurement. Therefore, the detection probability is $p_1 = 1 - 4 * \frac{1}{4} * \frac{1}{4} = \frac{3}{4}$ in B-A quantum channel.

In A-B quantum channel, Alice performs the unitary operations Z and X on the first and the forth of the particles, respectively, which will make the state $|\Phi_{12}^+\rangle|\Psi_{34}^+\rangle$ as a result of Eve's measurement using an incorrect sequence become $|\Psi_{12}^+\rangle|\Psi_{34}^-\rangle$. Then Eve measures the Bell states again with the same location as the first IR attack. At this time, the Bell states will not collapse because of Eve's measurement using an correct sequence and Eve can obtain the message Alice encodes by comparing the result $|\Psi_{12}^+\rangle|\Psi_{34}^-\rangle$ with the result $|\Phi_{12}^+\rangle|\Psi_{34}^+\rangle$ of the first eavesdropping. Then, Eve transfers the state $|\Psi_{12}^+\rangle|\Psi_{34}^-\rangle$ to Bob through quantum channel. After Bob receiving it, he performs the Bell basis measurement according to the location information he records previously. Due to entanglement swapping, the state $|\Psi_{12}^+\rangle|\Psi_{34}^-\rangle$ will yield one of the following four possible results with equal probability:

$$|\Phi_{13}^-\rangle|\Phi_{24}^+\rangle, |\Phi_{13}^+\rangle|\Phi_{24}^-\rangle, |\Psi_{13}^+\rangle|\Psi_{24}^-\rangle, |\Psi_{13}^-\rangle|\Psi_{24}^+\rangle, \tag{3}$$

The initial state $|\Psi_{13}^-\rangle|\Phi_{24}^-\rangle$ sent to Alice should become $|\Psi_{13}^+\rangle|\Psi_{24}^-\rangle$ after Alice's unitary operations (Z,X), which indicates that Eve is not detected with the probability of $\frac{1}{4}$ in A-B quantum channel. Similarly, the other three possible outcomes of Eve's measurement will yield $|\Psi_{12}^+\rangle|\Psi_{34}^-\rangle$ with the probability of $\frac{1}{4}$ after Bob performing a measurement on the intercepted Bell states. Therefore,

the detection probability is $p_2 = 1 - 4 * \frac{1}{4} * \frac{1}{4} = \frac{3}{4}$ in B-A quantum channel. Table 4 shows the examples of the process that Eve eavesdrops while choosing the wrong location. Group 1 and Group 2 stand for the cases that Eve is detected and not detected, respectively.

The probability Eve chooses the incorrect EPR location is 50% (assuming Alice chooses randomly), therefore, the detection probability in B-A quantum channel and A-B quantum channel is $d_1 = \frac{1}{2} * \frac{1}{2} * p_1 = \frac{3}{16}$ (the probability that Alice chooses correctly is $\frac{1}{2}$) and $d_2 = \frac{1}{2} * p_2 = \frac{3}{8}$, respectively.

If Alice randomly selects n groups of bits to announces the message she encodes by public channel, then Bob compares n corresponding groups of key bits with the initial random bits (thus discarding them as key bits, as they are no longer secret), the probability he find disagreement and identify the presence of Eve is $P_d = 1 - (\frac{5}{8})^n$. In order to detect an eavesdropper with the probability of 0.99999999, Alice and Bob need to compare $n = 40$ key bits, while Alice and Bob need to compare $n = 72$ key bits.

Table 4. The example of the process that Eve eavesdrops (the wrong location choice)

	Group 1 (detected)				Group 2 (not detected)			
Number of classical bits	1	2	3	4	1	2	3	4
Bobs random bit	1	0	1	1	1	0	1	1
Bob sending Bell states	$\|\Psi_{13}^-\rangle$	$\|\Phi_{24}^-\rangle$	$\|\Psi_{13}^-\rangle$	$\|\Phi_{24}^-\rangle$	$\|\Psi_{13}^-\rangle$	$\|\Phi_{24}^-\rangle$	$\|\Psi_{13}^-\rangle$	$\|\Phi_{24}^-\rangle$
Bell states Eve measures and sends	$\|\Psi_{13}^-\rangle$	$\|\Phi_{24}^-\rangle$	$\|\Psi_{13}^-\rangle$	$\|\Phi_{24}^-\rangle$	$\|\Psi_{13}^-\rangle$	$\|\Phi_{24}^-\rangle$	$\|\Psi_{13}^-\rangle$	$\|\Phi_{24}^-\rangle$
Alices random bit	0	1	1	0	0	1	1	0
Bell states Alice measures and sends	Z	/	/	X	Z	/	/	X
Bell states Eve measures again	$\|\Psi_{13}^+\rangle$	$\|\Psi_{24}^-\rangle$	$\|\Psi_{13}^+\rangle$	$\|\Psi_{24}^-\rangle$	$\|\Psi_{13}^+\rangle$	$\|\Psi_{24}^-\rangle$	$\|\Psi_{13}^+\rangle$	$\|\Psi_{24}^-\rangle$
The message Eve decodes	0	1	1	0	0	1	1	0
Bell states Bob measures	$\|\Phi_{13}^-\rangle$	$\|\Phi_{24}^+\rangle$	$\|\Phi_{13}^-\rangle$	$\|\Phi_{24}^+\rangle$	$\|\Psi_{13}^+\rangle$	$\|\Psi_{24}^-\rangle$	$\|\Psi_{13}^+\rangle$	$\|\Psi_{24}^-\rangle$
The message Bob decodes	1	0	0	1	0	1	1	0

Taking the probability c_1 and c_2 of the decoy mode into account, the effective transmission rate, i.e. the number of message bits per protocol run, is $(1-c_1)(1-c_2)$, which is equal to the probability for a message transfer. Therefore, if Eve wants to eavesdrop one message transfer without being detected, the probability for this event reads

$$\begin{aligned} s(c_1, c_2, d_1, d_2) &= (1-c_1)(1-c_2) + [c_1(1-d_1) + (1-c_1)c_2 \\ &(1-d_2)](1-c_1)(1-c_2) + [c_1(1-d_1) + (1-c_1)c_2(1-d_2)]^2 \\ &(1-c_1)(1-c_2) + \cdots = \frac{(1-c_1)(1-c_2)}{1-[c_1(1-d_1) + (1-c_1)c_2(1-d_2)]} \end{aligned} \tag{4}$$

Then the probability of successful eavesdropping $I = 4n$ bits is

$$s(I, c_1, c_2, d_1, d_2) = \left(\frac{(1-c_1)(1-c_2)}{1-[c_1(1-d_1) + (1-c_1)c_2(1-d_2)]} \right)^{I/4} \tag{5}$$

In the limit $I \to \infty$ (a message or key of infinite length) we have $s \to 0$, so the GEQKD protocol is asymptotically secure. For example, a convenient choice of the control parameter is $c_1 = \frac{1}{2}, c_2 = \frac{1}{2}$, where on the average every four bit is a control bit. The probability that Eve successfully eavesdrops 8 group of key bits is as low as $s \approx 0.011$. In Fig. 2, the eavesdropping success probability as a function of the information gain I is plotted for $c_1 = \frac{1}{2}, c_2 = \frac{1}{2}$.

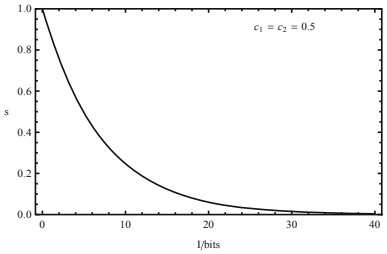

Fig. 2. Eavesdropping success probability as a function of the maximal eavesdropping information.

2.2 The Entanglement-Measure Attack

Since Alice makes the unitary operations only to the first and the forth of the particles S_i, Eve only needs to perform the entanglement-measure attack on the first and the forth of the particles S_i (If Eve eavesdrop all the bits of the particles S_i, the detection probability will become larger [41]). After performing the attack operation $\hat{E}$, the states $|0\rangle$ and $|1\rangle$ become

$$\hat{E} \otimes |0, \chi\rangle = \alpha|0, \chi_{00}\rangle + \beta|1, \chi_{01}\rangle, \hat{E} \otimes |1, \chi\rangle = \beta^{'}|0, \chi_{10}\rangle + \alpha^{'}|1, \chi_{11}\rangle, \quad (6)$$

where $|\chi_{00}\rangle, |\chi_{01}\rangle, |\chi_{10}\rangle$ and $|\chi_{11}\rangle$ are the pure ancillary states uniquely determined by $\hat{E}$.

Firstly, let us calculate the detection probability in the B-A channel. Consider one certain checking pair, it is in the state $|\Phi^+\rangle$ at the beginning. After Eve's attack operation with exchanging the position of the second and the third qubit, it is changed to

$$|\Phi^+\rangle_{Eve} = \frac{1}{\sqrt{2}}(\alpha|0, 0, \chi_{00}\rangle + \beta|1, 0, \chi_{01}\rangle + \beta^{'}|0, 1, \chi_{10}\rangle + \alpha^{'}|1, 1, \chi_{11}\rangle) \quad (7)$$

When Alice performs a Bell measurement on the EPR pair in the control mode, the detection probability is

$$d = p(|\Phi^-\rangle) + p(|\Psi^+\rangle) + p(|\Psi^-\rangle) = 1 - p(|\Phi^+\rangle), \quad (8)$$

Where p denotes probability. As a result, a lower bound of d is obtained:

$$d_l = p(|\Psi^+\rangle) + p(|\Psi^-\rangle) = |\beta|^2 \leq d. \tag{9}$$

As for Eve, one qubit of the EPR pair is indistinguishable from the complete mixture, so these qubits are considered in either of the states $|0\rangle$ or $|1\rangle$ with equal probability 0.5. Let us at first consider the case where Bob sends $|0\rangle$.

After Eve's attack operation and Alice encoding of the unitary operations I, X, Y and Z with the probabilities p_0, p_1, p_2 and p_3, respectively, the state can be written in the orthogonal basis $|0, \chi_{00}\rangle, |0, \chi_{01}\rangle, |1, \chi_{10}\rangle, |1, \chi_{11}\rangle$

$$\rho = \begin{pmatrix} (p_0+p_3)|\alpha|^2 & (p_0-p_3)\alpha\beta^* & 0 & 0 \\ (p_0-p_3)\alpha^*\beta & (p_0+p_3)|\beta|^2 & 0 & 0 \\ 0 & 0 & (p_1+p_2)|\alpha|^2 & (p_1-p_2)\alpha\beta^* \\ 0 & 0 & (p_1-p_2)\alpha^*\beta & (p_0+p_3)|\beta|^2 \end{pmatrix} \tag{10}$$

where $p_0+p_1+p_2+p_3 = 1$. The maximal information I_0 that Eve can eavesdrop is $I_0 = \sum_{i=0}^{3} -\lambda_i \log_2 \lambda_i$, where $\lambda_i (i = 0, 1, 2, 3)$ are the eigenvalues of ρ.

In the case of $p_0 = p_1 = p_2 = p_3 = \frac{1}{4}$, the maximal information I_0 Eve can obtain is simplified as

$$I_0(d_l) = 1 - d_l \log_2 d_l - (1 - d_l) \log_2 (1 - d_l), \tag{11}$$

Then assume that Bob sends $|1\rangle$ rather than $|0\rangle$. The above security analysis can be done in full analogy, resulting in the same relations. And the information $I_1(d)$ Eve can get is $I_1(d_l) = I_0(d_l)$. Therefore, the maximal information that Eve can obtain is

$$I(d_l) = \frac{I_0(d_l) + I_1(d_l)}{2} = 1 - d_l \log_2 d_l - (1 - d_l) \log_2 (1 - d_l). \tag{12}$$

If Eve wants to obtain the full information (2 bits), the detection probability is $d_l = 0.5$, however, Eve can get 1 bit of information from each EPR pair with the error rate $d_l = 0$. In the A-B Channel, we still take the detection as d_l. Therefore, if Eve wants to eavesdrop one message transfer without being detected, the probability for this event reads

$$\begin{aligned} s(c_1, c_2, d_l) =& (1-c_1)(1-c_2) + \{\frac{c_1}{2}[1+(1-d_l)^2] + (1-c_1)c_2(1-d_l)^2\}(1-c_1)(1-c_2) \\ &+ \{\frac{c_1}{2}[1+(1-d_l)^2] + (1-c_1)c_2(1-d_l)^2\}^2(1-c_1)(1-c_2) + \cdots \\ =& \frac{(1-c_1)(1-c_2)}{1 - \{\frac{c_1}{2}[1+(1-d_l)^2] + (1-c_1)c_2(1-d_l)^2\}} \end{aligned} \tag{13}$$

Then the probability of successful eavesdropping $I = nI(d_l)$ bits is

$$s(I, c_1, c_2, d_l) = \left(\frac{(1-c_1)(1-c_2)}{1 - \{\frac{c_1}{2}[1+(1-d_l)^2] + (1-c_1)c_2(1-d_l)^2\}} \right)^{I/I(d_l)} \tag{14}$$

In the limit $I \to \infty$ (a message or key of infinite length) we have $s \to 0$, so the GEQKD protocol is asymptotically secure. For example, a convenient choice of the control parameter is $c_1 = \frac{1}{2}, c_2 = \frac{1}{2}$, where on the average every four bit is a control bit. The probability that Eve successfully eavesdrops 8 group of key bits is as low as $s \approx 0.0006$. In Fig. 3, the eavesdropping success probability as a function of the information gain I is plotted for $c_1 = \frac{1}{2}, c_2 = \frac{1}{2}$ and for different detection probabilities d which Eve can choose. Note that for $d_l < 0.5$, Eve can only gets one part of the message right and does not even know which part she has obtained.

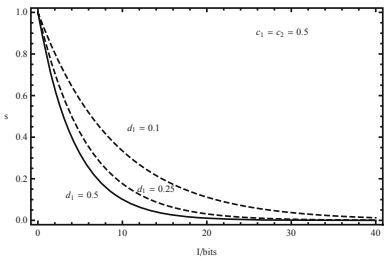

Fig. 3. Eavesdropping success probability as a function of the maximal eavesdropping information, plotted for a different detection probabilities d.

3 Quantum Circuit Simulation of GEQKD Protocol

At present, QKD has been studied widely in theory, however, only some important basic protocols, such as BB84 protocol [2], are implemented experimentally. Quantum circuit is essential to the practical realization of the protocol in experiment. It is well-known that any operation in quantum mechanics can be represented by a unitary evolution together with a measurement. Also, any unitary evolution can be accomplished by universal quantum logic gates [42]. Next, we will show the quantum circuit for implementing the proposed protocol.

Initially, Bob prepares four photons for each group, which are in the horizontal polarization state $|0\rangle$ or the vertical polarization state $|1\rangle$ randomly. Then he can choose the location information $\{(1,2),(3,4)\}$ or $\{(1,3),(2,4)\}$ to produce the EPR pairs. In order to achieve this goal, Bob need to perform Hadamard (H) and Controlled-Not (CNOT) gate based on the location information. After Alice obtains the photons, she applies the unitary operation on the first and the forth photon. After Bob receives the photons again, he makes the Bell state measurement (applying CNOT and H gate and then measuring with the basis $\{|0\rangle, |1\rangle\}$) based on the location information. Without loss of generality, we will take the location $\{(1,2),(3,4)\}$ as an example to present the quantum circuit.

Figure 4 gives the quantum circuit for implementing the proposed protocol under Eve's attack while Eve chooses correctly. Figure 5 shows the quantum

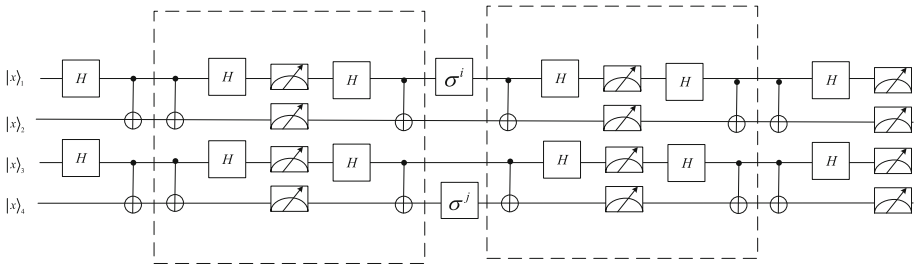

Fig. 4. Quantum circuit for implementing GEQKD protocol under Eve's attack while Eve chooses correctly. Where, $|x\rangle_i (i = 1, 2, 3, 4)$ represents the polarization state of the ith photon, which can be chosen as $|0\rangle$ or $|1\rangle$ randomly. In the dashed rectangle, Eve performs the Bell state measurement and re-prepare the new Bell state. σ^i and $\sigma^j (i, j = I, X, Y, Z)$ is the unitary operation performed by Alice to encode the classical bits.

circuit for implementing GEQKD protocol while Eve chooses incorrectly. In this case, due to the existence of entanglement swapping, the new two photons will be entangled, which means the first and third photon, the second and forth photon will be the Bell state, respectively.

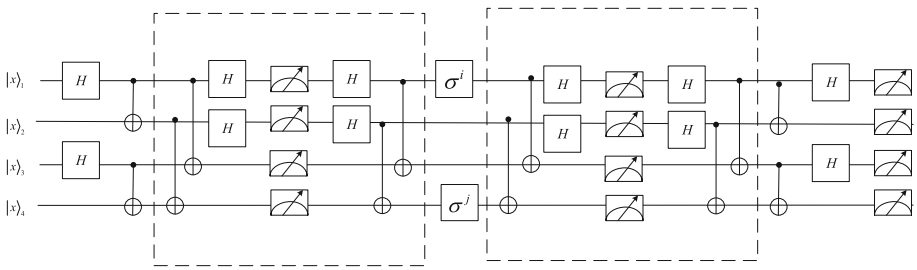

Fig. 5. Quantum circuit implementing GEQKD protocol under Eve's attack while Eve chooses incorrectly. Compared with Fig. 4, the difference takes places in the dashed rectangle. Eve chooses $\{(1, 3), (2, 4)\}$ to perform the Bell state and produce the new Bell state according to the location information $\{(1, 3), (2, 4)\}$.

4 Conclusion

In this paper, a novel QKD protocol is proposed and the security of this protocol is analyzed, which tells that the protocol is quasi-secure. Also, the efficient circuit simulation for implementing the proposed protocol is also constructed.

Compared with "Ping-pong" protocol, the proposed protocol needn't to store the qubit, which improves the maneuverability. What's more, the authorized

party can make full use of the quantum bits without causing the waste of quantum bits while transmitting the messages.

Note that in this paper the proposed protocol is used as QKD instead of QSDC. Equivalently, the bits obtained in this protocol constitute the random key (i.e. the raw key but not the secert message), which generates the final key after some later operations such as error correction and privacy amplification.

One of the localizations is that the preparation of Bell state used in the protocol is more difficult than the preparation of the single photon, while we believe that the problem will be solved with the advancement of technology.

The scheme is only a theoretical model and we don't consider about the non-ideal conditions such as imperfect devices and noisy situations. In the further work, the experiment of this protocol will be made in Heifei National Laboratory for Physics Sciences at Microscale and Department of Modern Physics.

References

1. Diffie, W., Hellman, M.: New directions in cryptography. IEEE Trans. Inf. Theory **22**(6), 644–654 (1976)
2. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. Theor. Comput. Sci. **560**(P1), 7–11 (2014)
3. Bennett, C.H., Bessette, F., Brassard, G., Salvail, L., Smolin, J.: Experimental quantum cryptography. J. Cryptol. **5**(1), 3–28 (1992)
4. Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. **85**(2), 441 (2000)
5. Ekert, A.K.: Quantum cryptography based on bells theorem. Phys. Rev. Lett. **67**(6), 661 (1991)
6. Bennett, C.H., Brassard, G., Mermin, N.D.: Quantum cryptography without bells theorem. Phys. Rev. Lett. **68**(5), 557 (1992)
7. Bruß, D.: Optimal eavesdropping in quantum cryptography with six states. Phys. Rev. Lett. **81**(14), 3018 (1998)
8. Li, J., Li, N., Li, L.L., Wang, T.: One step quantum key distribution based on EPR entanglement. Sci. Rep. **6**, 28767 (2016)
9. Wang, Q., Zhang, C.H., Luo, S., Guo, G.C.: An enhanced proposal on decoy-state measurement device-independent quantum key distribution. Quantum Inf. Process. **15**(9), 3785–3797 (2016)
10. Máttar, A., Acín, A.: Implementations for device-independent quantum key distribution. Phys. Scr. **91**(4), 043003 (2016)
11. Kawakami, S., Sasaki, T., Koashi, M.: Security of the differential-quadrature-phase-shift quantum key distribution. Phys. Rev. A **94**(2), 022332 (2016)
12. Fröhlich, B., et al.: Long-distance quantum key distribution secure against coherent attacks. Optica **4**(1), 163–167 (2017)
13. Hatakeyama, Y., Mizutani, A., Kato, G., Imoto, N., Tamaki, K.: Differential-phase-shift quantum-key-distribution protocol with a small number of random delays. Phys. Rev. A **95**(4), 042301 (2017)
14. Hwang, W.Y., Su, H.Y., Bae, J.: Improved measurement-device-independent quantum key distribution with uncharacterized qubits. Phys. Rev. A **95**(6), 062313 (2017)

15. Lizama-Pérez, L.A., López, J.M., De Carlos López, E.: Quantum key distribution in the presence of the intercept-resend with faked states attack. Entropy **19**(1), 4 (2016)
16. Lai, H., Luo, M.X., Zhan, C., Pieprzyk, J., Orgun, M.A.: An improved coding method of quantum key distribution protocols based on fibonacci-valued oam entangled states. Phys. Lett. A **381**(35), 2922–2926 (2017)
17. Pastorello, D.: A quantum key distribution scheme based on tripartite entanglement and violation of CHSH inequality. Int. J. Quantum Inf. **15**(05), 1750040 (2017)
18. Wang, Y., Bao, W.S., Bao, H.Z., Zhou, C., Jiang, M.S., Li, H.W.: High-dimensional quantum key distribution with the entangled single-photon-added coherent state. Phys. Lett. A **381**(16), 1393–1397 (2017)
19. Long, G.L., Liu, X.S.: Theoretically efficient high-capacity quantum-key-distribution scheme. Phys. Rev. A **65**(3), 032302 (2002)
20. Boström, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. **89**(18), 187902 (2002)
21. Cai, Q.Y., Li, B.W.: Improving the capacity of the boström-felbinger protocol. Phys. Rev. A **69**(5), 054301 (2004)
22. Gao, T., Yan, F.L., Wang, Z.X.: Deterministic secure direct communication using GHZ states and swapping quantum entanglement. J. Phys. A: Math. Gen. **38**(25), 5761 (2005)
23. Chamoli, A., Bhandari, C.: Secure direct communication based on ping-pong protocol. Quantum Inf. Process. **8**(4), 347–356 (2009)
24. Deng, F.G., Long, G.L.: Secure direct communication with a quantum one-time pad. Phys. Rev. A **69**(5), 052319 (2004)
25. Qing-Yu, C., Bai-Wen, L.: Deterministic secure communication without using entanglement. Chin. Phys. Lett. **21**(4), 601 (2004)
26. Lucamarini, M., Mancini, S.: Secure deterministic communication without entanglement. Phys. Rev. Lett. **94**(14), 140501 (2005)
27. Jiang, D., Chen, Y., Gu, X., Xie, L., Chen, L.: Deterministic secure quantum communication using a single d-level system. Sci. Rep. **7**, 44934 (2017)
28. Guerra, A.G.A.H., Rios, F.F.S., Ramos, R.V.: Quantum secure direct communication of digital and analog signals using continuum coherent states. Quantum Inf. Process. **15**(11), 4747–4758 (2016)
29. Wang, C., Deng, F.G., Li, Y.S., Liu, X.S., Long, G.L.: Quantum secure direct communication with high-dimension quantum superdense coding. Phys. Rev. A **71**(4), 044305 (2005)
30. Li, J., Song, D., Li, R., Lu, X.: A quantum secure direct communication protocol based on four-qubit cluster state. Secur. Commun. Netw. **8**(1), 36–42 (2015)
31. Li, J., Pan, Z., Sun, F., Chen, Y., Wang, Z., Shi, Z.: Quantum secure direct communication based on dense coding and detecting eavesdropping with four-particle genuine entangled state. Entropy **17**(10), 6743–6752 (2015)
32. Zhao, X.L., Li, J.L., Niu, P.H., Ma, H.Y., Ruan, D.: Two-step quantum secure direct communication scheme with frequency coding. Chin. Phys. B **26**(3), 030302 (2017)
33. Nguyen, B.A.: Quantum dialogue. Phys. Lett. A **328**(1), 6–10 (2004)
34. Wang, H., Zhang, Y.Q., Liu, X.F., Hu, Y.P.: Efficient quantum dialogue using entangled states and entanglement swapping without information leakage. Quantum Inf. Process. **15**(6), 2593–2603 (2016)

35. Zarmehi, F., Houshmand, M.: Controlled bidirectional quantum secure direct communication network using classical XOR operation and quantum entanglement. IEEE Commun. Lett. **20**(10), 2071–2074 (2016)
36. Kao, S.H., Hwang, T.: Controlled quantum dialogue robust against conspiring users. Quantum Inf. Process. **15**(10), 4313–4324 (2016)
37. Zhou, N.R., Li, J.F., Yu, Z.B., Gong, L.H., Farouk, A.: New quantum dialogue protocol based on continuous-variable two-mode squeezed vacuum states. Quantum Inf. Process. **16**(1), 4 (2017)
38. Liu, Z.H., Chen, H.W.: Cryptanalysis and improvement of efficient quantum dialogue using entangled states and entanglement swapping without information leakage. Quantum Inf. Process. **16**(9), 229 (2017)
39. Wójcik, A.: Eavesdropping on the ping-pong quantum communication protocol. Phys. Rev. Lett. **90**(15), 157901 (2003)
40. Fu-Guo, D., Xi-Han, L., Chun-Yan, L., Ping, Z., Hong-Yu, Z.: Eavesdropping on theping-pong'quantum communication protocol freely in a noise channel. Chin. Phys. **16**(2), 277 (2007)
41. Gao, F., Guo, F.Z., Wen, Q.Y., Zhu, F.: Comparing the efficiency of different detection strategies of the ping-pong protocol. Sci. China Ser. G-Phys. Mech. Astron. **39**(2), 161–166 (2009)
42. Barenco, A., Bennett, C.H., Cleve, R., et al.: Elementary gates for quantum computation. Phys. Rev. A **52**, 3457 (2017)