Quantum Key Distribution Based on Random Grouping Bell State Measurement

Dan Song and Dongxu Chen

***Abstract*—We propose a four-qubit quantum key distribution protocol via two Bell states which constitute a transmitted unit from the sender to the receiver in each communication. An encryption here is designed by randomly grouping four qubits of a unit into two new couples, which is a way to increase the possibility of detecting the eavesdropper. Ultimately, the receiver randomly measures this grouped unit with two Bell state measurements. From the comparison of grouping information of these four qubits, we find that the two sides in a valid communication can discover the illegal party in the channel. In the proposed protocol, the receiver measures the unit when he receives it instantly, which is an efficient way to overcome the ultrashort storage time of quantum state.**

***Index Terms*—Quantum communication, quantum key distribution, Bell state measurement.**

I. Introduction

QUANTUM key distribution (QKD) is a promising technology to protect the security of classical information in quantum epoch [1]. It enables two parties to share a secret key with unconditional security, which can then be used to encrypt and decrypt messages. Many works have been conducted to promote the development of QKD protocols. In 1984, it was Bennett and Brassard who first introduced the QKD protocol by using two mutually unbiased bases of photon's polarization degree of freedom [2]. Later Ekert proposed another QKD protocol which was called E91 based on Einstein-Podolsky-Rosen (EPR) pairs [3]. After that, various QKD protocols are theoretically proposed and experimentally realized, such as QKD protocols designed with single-photon [4], multiple states [5] and Bell state [8]. Among these works, photons are extensively used to carry information because they are easy to manipulate and they transmit at light speed.

As the quantum channel, Bell state was firstly proposed by [6] and verified to be the maximally entangled state of a two-qubit quantum system. Compared with other multi-qubit states, such as W state, GHZ state and cluster state, Bell state is easier to prepare via nonlinear process [7]. In reference [8], two parties share the secret key by comparing the form of initial Bell state and the outcome of entanglement swapping. Then, [9] improved the total efficiency of the communication to 100% compared with the former 50% in [8]. [10] presented the first authenticated semi-quantum key distribution protocol without using authenticated classical channels based on Bell states. In this paper, we propose a protocol to prevent the eavesdropper with lower qubit error rate and shorter detecting key bits based on a four-qubit state which consists of two couples of Bell states.

In our protocol, a group of four-qubit state are prepared each time and sent from the sender to the receiver. The receiver performs quantum state measurement immediately after he receives the qubits. Compared with the two-way protocols where the quantum state needs to be preserved until the tranmission is finished in [8] and [9], our protocol can overcome the ultrashort coherence time of quantum states. Every four qubits form a unit to transfer information from the sender to the receiver in each communication. The four qubits are sent in random order by the sender and received by the receiver in a randomly grouping measurement. Our calculation shows that the qubit error rate is 4.17%, which is lower than 46.875% in [11]. Furthermore, only 11 bits are needed to detect the eavesdropper in our QKD protocol which is smaller than 72 bits in BB84 protocol [2] with the same security.

II. QKD protocol based on four-qubit states

A. Quantum channel with Bell state

[8] and [9] proposed two QKD protocols, both used Bell states distributed from the sender to the receiver. In their protocols, two pairs of Bell states are shared between two legal parties of communication. The sender and the receiver both keep two qubits entangled with each other. After the simultaneous Bell state measurement (BSM) of the two parties, there exists an entanglement swapping among these four qubits.

To be more specific, let's denote the four qubits of two Bell states as P_1, P_2, P_3 and P_4. Entanglement exists between P_1 and P_2, P_3 and P_4. After BSM of the two sides, P_1 and P_3, P_2 and P_4 become entangled, respectively. However, the two sides still need to keep their qubits during communication, and it is challenging to store qubits in the state of the art.

Consider the ultrashort storage time of qubits, a novel QKD protocol is proposed with a four-qubit state consisting of two couples of Bell states expressed as equation (1). A group of four-qubit state is prepared each time to send to Bob for measurement immediately. What is different from [8] and [9] is, the sender sends all the qubits to the receiver and the reciever performs quantum state measurement immediately when he receives the qubits. This is a one way process. The two parties don't need to store the qubits thus the qubits are

D. Song is with the School of Informatics, Xiamen University, Xiamen 361005, China (e-mail: dansong@stu.xmu.edu.cn).

D. Chen is with the Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen 518055, China (e-mail: xdc.81@stu.xjtu.edu.cn).

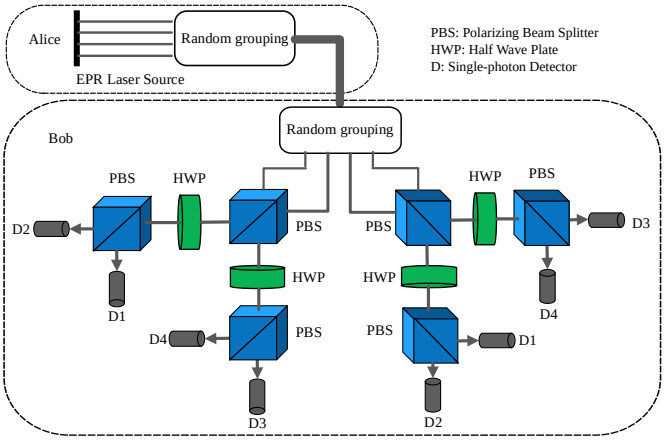

Fig. 1. The process of our QKD protocol. Alice prepares a four-qubit state and sends to Bob via quantum channel. Then Bob groups randomly and measures these qubits with Bell bases.

measured before they decoherence.

$$\begin{aligned} |C\rangle_{1234} &= |\Phi^-\rangle_{12} \otimes |\Phi^+\rangle_{34} \\ &= \frac{1}{2}(|\Phi^+\rangle_{13}|\Phi^-\rangle_{24} + |\Phi^-\rangle_{13}|\Phi^+\rangle_{24} + \\ &\quad |\Psi^+\rangle_{13}|\Psi^-\rangle_{24} + |\Psi^-\rangle_{13}|\Psi^+\rangle_{24}), \end{aligned} \quad (1)$$

the subscripts 1, 2, 3 and 4 indicate four correlated qubits. The Bell states are expressed as

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), |\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle).$$

From (1) we can see that the state becomes superposition of four states which means we can obtain four different outcomes by combinations of BSMs. Note that equation (1) represents only one special case, other two forms are shown for comparison in Table II with different groupings of qubits. In brief, there exists three forms of random grouping of these four qubits, of which only equation (1) is defined as the right one. This is the primary technique to encrypt the information during communication. The proposed protocol is illustrated in Fig. 1, where Alice and Bob are the legitimate sender and receiver, respectively.

B. Preliminaries

In this section, we show the details of the protocol in Fig. 1.

a) Step 1 state preparation: Alice prepares one group of the four-qubit state in equation (1). Each group consists of four qubits P_γ, $\gamma \in \{1, 2, 3, 4\}$. With such dense coding, the key information G of each group of the two Bell states is shown in Table I. Alice needs to record the information of qubits and the corresponding information G.

b) Step 2 qubit distribution: According to equation (1), Alice knows that the group order of these four qubits is $\{(P_1, P_3), (P_2, P_4)\}$. Then, Alice rearranges these four qubits randomly and sends them to Bob via quantum channel.

c) Step 3 grouping measurement: Bob receives the qubits and divides them into two parts randomly. Then he performs BSMs on the two parts then sends the grouping information and the measurement results to Alice via classical channel.

TABLE I
THE DENSE ENCODING RULE BETWEEN THE GROUPING BELL MEASUREMENT BASES AND THE BINARY RANDOM SEQUENCE G

(P_1, P_3)	(P_2, P_4)	G
$\|\Phi^+\rangle$	$\|\Phi^-\rangle$	00
$\|\Phi^-\rangle$	$\|\Phi^+\rangle$	01
$\|\Psi^+\rangle$	$\|\Psi^-\rangle$	10
$\|\Psi^-\rangle$	$\|\Psi^+\rangle$	11

TABLE II
THE DIFFERENT GROUPINGS OF THE FOUR QUBITS BY BOB

Bob's grouping	Verdict	Announced number
$(P_1, P_3)\&(P_2, P_4)$	Right	1
$(P_1, P_2)\&(P_3, P_4)$	Wrong	0
$(P_1, P_4)\&(P_2, P_3)$	Wrong	0

d) Step 4 results comparison: Alice compares the results from Bob with her reserved information of P_γ. If Alice gets a coincident comparison, she announces '1', and then the communication can proceed to step 5 or returns to step 1. Otherwise, she announces '0' and the communication returns to step 1 or ends. The different groupings of the four qubits by Bob are shown in Table II.

e) Step 5 raw key acquirement: Alice and Bob obtain a long binary sequence as the raw key R after multiple communications. If we define R_A and R_B as the raw keys belonging to Alice and Bob, respectively. Alice randomly selects parts of R_A in different positions as her agreement key C_A and announces the corresponding positions. Then, Bob chooses the agreed key C_B in the same location in R_B.

f) Step 6 privacy amplification: Bob chooses a set of C_B bits as the parity bits D_B and announces D_B along with its corresponding positions. Alice selects her D_A in the same way and compares it with D_B. If the bit error rate is smaller than the threshold, the communication is secure and they can proceed to step 7; if not, they need to return to step 1 or terminate this communication.

g) Step 7 final key acquirement: The final keys R'_A and R'_B are used to encrypt the secret message through the communication. Theoretically, $R'_A = R'_B$, R'_A is the raw key R_A without C_A under ideal condition, the same as R'_B.

C. Analyses of the qubit error rate with different groupings

We can see that there are three different kinds of groupings from Table II. One is right, another two are wrong. Therefore, the probability of correctly grouping four qubits by Bob is $\frac{1}{3}$. If there is no eavesdropper in the communication channel, the qubit error rate ε_0, which is the threshold during one communication, can be calculated as following.

(1) Bob divides the four qubits into the wrong grouping $\{(P_1, P_2), (P_3, P_4)\}$.

$$\begin{aligned} |C\rangle_{1234} &= \frac{1}{2}(|0000\rangle + |0011\rangle - |1100\rangle - |1111\rangle)_{1234} \\ &= 2(|\Phi^-\rangle_{12}|\Phi^+\rangle_{34}). \end{aligned} \quad (2)$$

In this case, he will only get $|\Phi^-\rangle_{12}|\Phi^+\rangle_{34}$. Bob will get the

right binary random sequence $G = 01$ with the probability of $\frac{1}{4}$ according to Table I.

(2) Bob gets the correct measurement results via the other wrong grouping, $\{(P_1, P_4), (P_2, P_3)\}$.

$$\begin{aligned} |C\rangle_{1234} &= \frac{1}{2}(|0000\rangle + |0011\rangle - |1100\rangle - |1111\rangle)_{1234} \\ &= \frac{1}{2}(|\Phi^+\rangle_{14}|\Phi^-\rangle_{23} + |\Phi^-\rangle_{14}|\Phi^+\rangle_{23} + \\ &\quad |\Psi^+\rangle_{14}|\Psi^-\rangle_{23} + |\Psi^-\rangle_{14}|\Psi^+\rangle_{23}). \end{aligned}$$

By BSM, he can obtain four correct measurement results $\{|\Phi^+\rangle, |\Phi^-\rangle\}$, $\{|\Phi^-\rangle, |\Phi^+\rangle\}$, $\{|\Psi^+\rangle, |\Psi^-\rangle\}$ and $\{|\Psi^-\rangle, |\Psi^+\rangle\}$. As a result, Bob will get the right binary random sequence G with the probability of $\frac{4}{4} = 1$ even he makes a wrong grouping.

In summary, the results of the BSM can only be partially right in the first case or totally right in the second case. Therefore, Bob can acquire the right binary random sequence with the probability of $\frac{1}{2} \times \frac{1}{4} + \frac{1}{2} \times \frac{4}{4} = \frac{5}{8}$ when grouping wrongly. Hence, the qubit error rate ε_0 is,

$$\varepsilon_0 = 1 - (\frac{1}{3} + \frac{5}{8}) = \frac{1}{24} = 0.0417. \tag{3}$$

Note that if Bob chooses the right grouping with probability $\frac{1}{3}$, he can obtain the right binary random sequence with the probability of 1. Ultimately, the threshold in our protocol can be set to be 4.17%.

III. Security analyses

In this section, we analyze the security of our protocol under two major attacks: the intercept-resend attack and the Trojan Horse attack. Meanwhile, we assume the existence of an eavesdropper Eve in the communication channel.

A. The intercept-resend attack

The eavesdropper Eve can interact and resend a new four-qubit state to Bob so that he can acquire the information of the state. In this case, Eve plays the same role as Bob does in the communication. He can group the four-qubit state and measure it with Bell bases.

After step 2 of our protocol, the four qubits sent by Alice will transmit through the communication channel. Let's assume that Eve intercepts these four qubits and processes them in the same way as Bob does. Then, Eve resends his decoy four qubits to Bob. Let us discuss the different cases of the communication between Eve and Bob.

(1) Eve chooses the right grouping and acquires the right measurement results. Bob simultaneously chooses the right grouping. Now, there are three parties, Alice, Bob and Eve in the communication. There is a probability of p_1 that Eve can successfully filch the information,

$$p_1 = (\frac{1}{3} \times 1)_{Eve} \times (\frac{1}{3} \times 1)_{Bob} = \frac{1}{9}. \tag{4}$$

(2) Similarly, Eve can divide the qubits and obtain the measurement results correctly. Then, he sends the right decoy four-qubit state to Bob. After receiving them, Bob chooses a wrong grouping but yields a right measurement result. However, this group of state will be abandoned since in the comparison stage Alice and Bob can detect the wrong grouping.

$$p_2 = (\frac{1}{3} \times 1)_{Eve} \times (\frac{2}{3} \times \frac{1}{4} + \frac{2}{3} \times \frac{5}{8})_{Bob} = \frac{14}{72}. \tag{5}$$

(3)Eve chooses a wrong grouping but he gets a right measurement result while Bob chooses a right grouping.

$$p_3 = (\frac{2}{3} \times \frac{1}{4} + \frac{2}{3} \times \frac{5}{8})_{Eve} \times (\frac{1}{3} \times 1)_{Bob} = \frac{14}{72}. \tag{6}$$

(4) In the same way, Eve transmits the decoy state with a wrong grouping but Bob gets the right results. Meanwhile, Bob divides this decoy four-qubit state into wrong groups but obtain the right measurement result. In this case, the qubits will be abandoned because of the wrong grouping of Bob.

$$p_4 = (\frac{2}{3} \times \frac{1}{4} + \frac{2}{3} \times \frac{5}{8})_{Eve} \times (\frac{2}{3} \times \frac{1}{4} + \frac{2}{3} \times \frac{5}{8})_{Bob} = \frac{196}{576}. \tag{7}$$

In conclusion, there is a probability that Bob gets a wrong measurement result, i.e., the qubit error rate with existence of eavesdropper in our protocol can be calculated as (8).

$$\varepsilon_e = 1 - (\frac{1}{9} + \frac{14}{72} + \frac{14}{72} + \frac{196}{576}) = \frac{92}{576} = 0.1597. \tag{8}$$

Suppose Alice and Bob need to compare n bits of binary random sequence to detect Eve with the probability of $p_d = 0.999999999$ with

$$p_d = 1 - (1 - \varepsilon_e) = 1 - (\frac{92}{576})^n. \tag{9}$$

We can find a minimum value of $n = 11$ from equation (9). On the other hand, in BB84 protocol, Alice and Bob need to compare $n = 72$ bits to detect Eve with the same probability. From the aforementioned analyses, we can calculate the mutual information between Alice, Bob and Eve. The mutual information between Alice and Bob is

$$\begin{aligned} I(A;B) &= 1 - [-(1-\varepsilon_0)\log(1-\varepsilon_0) - \varepsilon_0 \log \varepsilon_0] \\ &= 1 + \frac{23}{24}\log\frac{23}{24} + \frac{1}{24}\log\frac{1}{24} = 0.7501. \end{aligned} \tag{10}$$

The mutual information between Alice and Eve is

$$I(A;E) = 1 - [-(1-\varepsilon_e)\log(1-\varepsilon_e) - \varepsilon_e \log \varepsilon_e] = 0.3664.$$

Therefore, the communication is secure since $I(A;B) > I(A;E)$. Furthermore, $I(A;B)$ in our protocol is greater than $I'(A;B) = 0.1887$ bit in BB84 protocol.

The theoretical secret key rate is

$$R = I(A;B) - I(A;E) = 0.7501 - 0.3664 = 0.3837 > 0. \tag{11}$$

So, the binary random bits can be distilled after Alice and Bob perform key reconciliation and privacy amplification on the final key R'_A and R'_B . The transmission distance ℓ of the secret key is given by the qubit error rate ε [12], which is:

$$\varepsilon = \frac{\mu 10^{-\alpha \cdot \ell/10}\eta}{\mu 10^{-\alpha \cdot \ell/10}\eta + 2P_e}, \tag{12}$$

where $\mu = 4$ is the averaged qubit flux leaving from Alice, $10^{-\alpha \cdot \ell/10}$ represents the fiber attenuation through distance ℓ, η is the detection efficiency. Here, we set the channel loss to

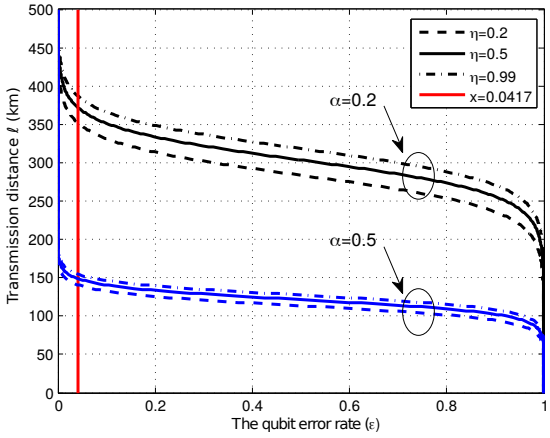

Fig. 2. The relationship between the transmission distance ℓ (km) and the qubit error rate ε.

be $\alpha = 0.2$ and $\alpha = 0.5$. Referring to [12], $P_e = 8.5 \times 10^{-7}$ is the probability of an error count per clock cycle. We set the values of η to be 0.2, 0.5 and 0.99. Figure 2 shows the relation between ℓ (km) and the qubit error rate ε. We can see that ℓ decreases with the increase of the channel loss. Meanwhile, the higher the detection efficiency of the communication η is, the larger the qubit error rate ε is. From Fig. 2, we can infer that there exists a further distance when $\varepsilon_e = 0.0417$ which is the qubit error rate in our protocol.

B. Trojan Horse attack

A QKD system may be probed by Eve by sending a bright light into the quantum channel and analyzing the back-reflection in a Trojan-horse attack. Eve occupies part of the quantum channel to probe the laser sent by Alice with an auxiliary source. Note that his detection scheme relies on the feature of the auxiliary source. Eve needs to remove part of the legitimate signal, compensating the introduced loss by an improved quantum channel. Hence, Eve needs to prepare a better channel which has less attenuation than the legitimate channel. Then, he can measure the intercepted state with a quantum memory.

With the Trojan Horse attack, the measurement that maximizes Eve's information gain is known [13],

$$I_E(|\nu|^2) = 1 - H(p), \tag{13}$$

where $p = \frac{1}{2}(1 + \sqrt{1 - |\langle \nu, 0|0, \nu\rangle|^2}) = \frac{1+\sqrt{2}|\nu|}{2}$ and $H(\cdot)$ is the binary entropy. $|\nu|^2$ is the mean photon number of Eve. Hence, (13) can be rewritten as,

$$I_E(|\nu|^2) \approx \frac{1}{ln(2)}|\nu|^2 + O(|\nu|^4). \tag{14}$$

From [13], if Alice's monitoring detector sets a limit to Eve's backscattered signal of 0.1 photon, then $0.095 \leq I_E(|\nu|^2) \leq 0.135$. The lower bound is

$$I_E^*(|\nu|^2) = 1 - \exp(-|\nu|^2). \tag{15}$$

In our protocol, the maximum mean photon number of Eve can be 0.4, so, $0.329 \leq I_E(|\nu|^2) \leq 0.448$. We can see that $I_{E(max)}(|\nu|^2) < I(A;B)$. Hence, the Trojan Horse attack can be prevented in our protocol.

IV. Conclusion

We have analyzed a four-qubit QKD protocol theoretically. Our protocol can provide the encryption without inserting decoy qubits in the qubit sequence to detect the eavesdropper. [14] designed a QKD protocol based on decoy-state, which is more applicable in practical, with longer transmission distance in the state of the art. This is follow-up work since we analyse our protocol in practical implementation. With the increase of the randomness of grouping of four qubits in each unit by Bob, it will be more difficult for Eve to decode the classical information. Our results show that the security can be guaranteed and the storage of the qubits during the communication is not required. Furthermore, our protocol can be extended to distributing multiple qubits.

References

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Ltkenhaus, and M. Peev, "The security of practical quantum key distribution" *Rev. of Modern Phys.*, vol. 81 no. 3, pp. 1301-1305, 2009.

[2] C. H. Bennet, and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," *In Proc. Of IEEE Int'l Conf. on Computers, Systems and Signal Process.*, Bangalore, India, 1984, pp. 175-179.

[3] A. K. Ekert, "Quantum cryptography based on Bells theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661-663, 1991.

[4] W. Y. Liang, M. Li, Z. Q. Yin, W. Chen, S. Wang, X. B. An, G. C. Guo, and Z. F. Han, "Simple implementation of quantum key distribution based on single-photon Bell state measurement," *Phys. Rev. A*, vol. 92, no. 1, pp. 012319-012322, 2015.

[5] D. X. Chen, P. Zhang, H. R. Li, H. Gao, and F. L. Li, "Four-state quantum key distribution exploiting maximum mutual information measurement strategy," *Quantum Inf. Process.*, vol. 15, no. 2, pp. 881-891, 2016.

[6] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?", *Phys. Rev.*, vol. 47, no. 10, pp. 696-702, 1935.

[7] Y. H. Kim, S. P. Kulik, and Y. Shih, "Bell state preparation using pulsed non-degenerate two-photon entanglement," *Phys. Rev. A*, vol. 63, no. 6, pp. 90-93, 2001.

[8] G. Gao, "Quantum key distribution by comparing Bell states," *Opt. Commun.*, vol. 281, no. 4, pp. 876-879, 2008.

[9] H. Yuan, J. Song, L. F. Han, K. Hou, and S. H. Shi, "Improving the total efficiency of quantum key distribution by comparing Bell states," *Opt. Commun.*, vol. 281, no. 18, pp. 4803-4806, 2008.

[10] K. F. Yu, C. W. Yang, C. H. Liao, and T. Hwang, "Authenticated semi-quantum key distribution protocol using Bell states," *Quantum Inf. Process.*, vol. 13, no. 6, pp. 1457-1465, 2014.

[11] J. Li, N. Li, L. L. Li and T. Wang, "One step quantum key distribution based on EPR entanglement," *Sci. Rep.*, vol. 6, pp. 28767-28770, 2016.

[12] C. Gobby, Z. L. Yuan, and A. J. Shields, "Quantum key distribution over 122 km of standard telecom fiber," *Applied Phys. Lett.*, vol. 84, no. 19, pp. 3762-3764, 2004.

[13] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, "Trojan-horse attacks on quantum-key-distribution systems," *Phys. Rev. A*, vol. 73, no. 2, pp. 457-463, 2006.

[14] F. Z. Guo, L. Liu, A. K. Wang, and Q. Y. Wen, "Practical covert quantum key distribution with decoy-state method," *Quantum Inf. Process.*, vol. 18, no. 4, pp. 95, 2019.