SCIENCE CHINA
Information Sciences

• LETTER •

June 2020, Vol. 63 169501:1–169501:3
https://doi.org/10.1007/s11432-018-9851-6

Quantum key distribution based on single-particle and EPR entanglement

Leilei LI[1], Jian LI[1*], Yan CHANG[2], Yuguang YANG[3] & Xiubo CHEN[4]

[1]*School of Computer Science, Beijing University of Posts and Telecommunications, Beijing* 100876*, China;*
[2]*Department of Network Engineering, Chengdu University of Information Technology, Chengdu* 610225*, China;*
[3]*College of Computer Science and Technology, Beijing University of Technology, Beijing* 100124*, China;*
[4]*School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing* 100876*, China*

Received 20 September 2018/Revised 25 December 2018/Accepted 1 March 2019/Published online 13 March 2020

Citation Li L L, Li J, Chang Y, et al. Quantum key distribution based on single-particle and EPR entanglement. Sci China Inf Sci, 2020, 63(6): 169501, https://doi.org/10.1007/s11432-018-9851-6

Dear editor,

The theoretical security of the quantum secure communication protocols can be proved with the law of quantum mechanics, when the classical communication protocols' security can only depend on the computational complexity [1, 2]. Based on the quantum BB84 protocol [3] and the quantum MEQKD protocol [4], we present a QKD (quantum key distribution) protocol based on a single-particle and an EPR (Einstein-Podolsky-Rosen) entanglement pair, which is called the quantum TEQKD protocol. Compared with MEQKD, TEQKD sends one single-particle and one EPR Entanglement pair at one time. What's more, the security of the TEQKD protocol in individual Man-in-the-Middle attacks is also analyzed, an eavesdropping behavior will cause at least a bit error rate of 62.5%. In order to achieve the same detection effect, the TEQKD needs 22 quantum key bits as the detection sequence, while the MEQKD needs 33 qubits [4]. Similar to MEQKD, TEQKD does not need to store the qubits state. In this study, we also analyze the problems about photon loss and PNS attacks, we also try to give an idea to solve the problem with continuous variable generalization and decoy state technique.

Firstly, the detail introduction of TEQKD protocol should be given. Different from the BB84 protocol, the TEQKD only uses the Z-basis: $B_Z = \{|0\rangle, |1\rangle\}$ and a single-particle $|0\rangle$ and $|1\rangle$. What's more, TEQKD prepares another EPR pairs and combines the single particle with EPR pairs into a three-particles state. The sender Alice and receiver Bob agree the relationship between the classical bits and the quantum bits (qubits) as

$$\begin{aligned} &0 \leftrightarrow |0\rangle, \quad 1 \leftrightarrow |1\rangle, \\ &00 \leftrightarrow |\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \\ &01 \leftrightarrow |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \\ &10 \leftrightarrow |\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \\ &11 \leftrightarrow |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \end{aligned} \tag{1}$$

The complete process of the TEQKD can be described as the following 6 steps:

(1) Alice divides every three classical bits (cbits) into a group and numbers them into $(1, 2, 3)$.

(2) Alice prepares enough EPR pairs and single particles, then encodes the cbits into qubits. Alice uses pos $= i, i \in \{2, 3\}$ to record the position of the single particle. According to (1), if the classical bits are $\{001\}$, Alice will send $\{|\Phi^+\rangle_{12}|1\rangle_3\}$ (pos $= 3$) or $\{|\Phi^-\rangle_{13}|0\rangle_2\}$ (pos $= 2$), just as shown in Figure 1. Alice records the location information pos and sends the qubits to Bob.

* Corresponding author (email: lijian@bupt.edu.cn)

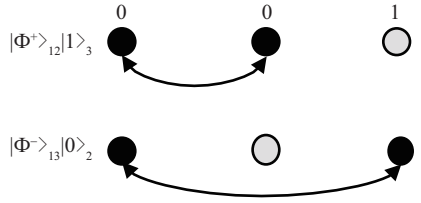

Figure 1 Alice encodes 001 into $|\Phi^+\rangle_{12}|1\rangle_3$ or $|\Phi^-\rangle_{13}|0\rangle_2$.

(3) Suppose that there is no bit loss in the transmission process. After receiving the qubits from Alice, Bob randomly chooses pos = 2 or 3 to take the Bell measurement on the EPR entanglement and the B_Z measurement on the single-particle.

(4) After taking the measurement, Bob publics the pos information to Alice, they will discard the different pos situations and only keep the same pos situation like the quantum BB84 protocol.

(5) Alice and Bob sample some keys and public them to the public channel, then calculate the bit error rate(ε). If there is no Eve, ε will less than the threshold value θ and the quantum channel is safe. If $\varepsilon \geqslant \theta$, Alice and Bob think there is an eavesdropper, they will interrupt this communication and restart a new one.

(6) Alice and Bob confirm that the channel is safe, they will transmit the remaining keys to obtain the raw key. They will get the final key after some post-processing steps such as error correction and privacy amplification. The process of error correction and privacy amplification can be introduced in a classical method and we will not discuss in this study.

Let us analyze the security of the TEQKD protocol. Suppose that the eavesdropper Eve takes intercept-resend attacks during the communication, according to the Heisenberg's uncertainty principe and no-clone theory, Eve must re-prepare the Bell state and send it to Bob. Eve does not know which location is the Bell state, so she randomly chooses the pos, that will cause a qubit error rate ε.

If there is no Eve, after discarding the different pos, the bit error rate ε_0 between Alice and Bob is 0. The bit error rate only caused by the situation that Eve chooses the wrong pos but Bob chooses the right pos. This probability is $p_0 = 1/4$. Supposed the function $m(x,\ \text{pos})$ is the measurement result when the input qubits group is x and the position of the single-particle is pos $\in \{2, 3\}$.

Suppose Alice sends 001 $\leftrightarrow |\Phi^-\rangle_{13}|0\rangle_2$, Eve chooses $\text{pos}_E = 3$ and Bob chooses $\text{pos}_B = 2$. The measurement result of Eve is $m_e = m_E(|\Phi^-\rangle_{13}|0\rangle_2,\ 3)$:

$$\begin{cases} m_e = \frac{1}{\sqrt{2}}(|Q_1\rangle_{12}|0\rangle_3 - |Q_2\rangle_{12}|1\rangle_3), \\ |Q_1\rangle = \frac{1}{\sqrt{2}}(|\Phi^+\rangle + |\Phi^-\rangle), \\ |Q_2\rangle = \frac{1}{\sqrt{2}}(|\Psi^+\rangle - |\Psi^-\rangle). \end{cases} \tag{2}$$

Eve will get four measurement results $\{000, 010, 101, 111\}$ with the same probability of $(1/2)^2 = 1/4$. With the same idea, the measurement result of Bob when Eve resends $|\Phi^+\rangle_{12}|0\rangle_3$ can be analyzed as $m_b = m_B(|\Phi^+\rangle_{12}|0\rangle_3,\ 2)$:

$$\begin{cases} m_b = \frac{1}{\sqrt{2}}(|Q_3\rangle_{13}|0\rangle_2 + |Q_4\rangle_{13}|1\rangle_2), \\ |Q_3\rangle = \frac{1}{\sqrt{2}}(|\Phi^+\rangle + |\Phi^-\rangle), \\ |Q_4\rangle = \frac{1}{\sqrt{2}}(|\Psi^+\rangle - |\Psi^-\rangle). \end{cases} \tag{3}$$

The other three situations are same like (3). Bob still has 1/4 probability to get $|\Phi^-\rangle_{13}|0\rangle_2$ when Eve chooses the wrong position of single-particle. When there is an Eve, the probability p_r that Bob can still get the right measurement result is

$$p_r = p_0 + \frac{1}{2} \times \frac{1}{4} = \frac{3}{8}. \tag{4}$$

If Bob chooses the wrong position of the single-particle, the measurement results will be discarded after Alice and Bob public their position information, so the whole bit error rate caused by Eve can be calculated:

$$\varepsilon = 1 - p_r = \frac{5}{8} = 0.625. \tag{5}$$

If Alice and Bob want to find out the Eve, Alice samples the length of n qubits to Bob as the detection sequence, the probability of detecting the eavesdropping behavior is

$$P_d = 1 - (1 - \varepsilon)^n = 1 - \left(\frac{3}{8}\right)^n. \tag{6}$$

To detect an eavesdropper with the probability of $P'_d = 1 - 10^{-9}$, Alice and Bob need to compare at least $n = 22$ key bits in TEQKD while 33 key bits in MEQKD [4].

According to [5], if the mutual information Bob gets from Alice $I(A : B)$ is larger than the mutual information Eve gets from Alice $I(A : E)$, the quantum protocol is security after privacy amplification:

$$\Delta = I(A : B) - I(A : E) > 0. \tag{7}$$

According to [5, 6], if the bit error rate between Alice and Bob $\epsilon_d > 0.11$, Eve will be detected, suppose the probability that Eve detects the communication is $\gamma \in [0, 1]$ and γ should satisfy

$$\epsilon_d = 0 \times (1 - \gamma) + \varepsilon \times \gamma < 0.11. \tag{8}$$

The value of γ should satisfy $\gamma < 0.176$, according to [4], Δ should satisfy the following equation:

$$\begin{cases} \Delta \geqslant 1 - 2 \times (I_0 + I_1), \\ 0 < \gamma < 0.176, \\ I_0 = -(1 - \frac{5}{8}\gamma) \log_2 (1 - \frac{5}{8}\gamma), \\ I_1 = -(\frac{5}{8}\gamma) \log_2 (\frac{5}{8}\gamma), \end{cases} \tag{9}$$

when $\gamma \in (0, 0.176)$, the value of Δ can be calculated by Python3, which always satisfies $\Delta > 0$, so the TEQKD's security has been proved by the mutual information theory. The final key rate is determined by the probability that Eve takes an eavesdropping $\gamma < 0.176$. If $\gamma \geqslant 0.176$ Alice and Bob will detect Eve, they will discard this communication and restart a new one. So the final key rate R can be described as

$$R = \begin{cases} 1 - 2H(\varepsilon \times \gamma), & 0 < \gamma < 0.176, \\ 0, & \gamma \geqslant 0.176. \end{cases} \tag{10}$$

TEQKD is extremely sensitive to photon loss, based the idea of the GG02 protocol [7]. The continuous variable can be introduced to the single-particle in TEQKD protocol, the continuous variable states will not change the process of the TEQKD:

(1) Alice prepares 2 random sequences $\{x_A\}$ and $\{p_A\}$ which obey the Gaussian distribution with mean 0, prepares corresponding coherent states and sends them to Bob.

(2) After receiving continuous variable states from Alice, Bob randomly chooses x basis or p basis to take a measurement.

(3) The follow-up steps are similar to the BB84 protocol: Bob publics the measurement basis he uesed and Alice only keeps the right basis to obtain the raw key. After the post-processing, Alice and Bob finally obtain the final key.

There is another problem should be analyzed that the practical single photon source is unobtainable in practical. TEQKD should take the PNS attacks into consideration during the security analysis. Based the idea of preventing PNS attacks with decoy state technique, the sender Alice randomly chooses the sources of light with different intensities as signal state or decoy state, Eve will take the same PNS attacks in every state. After receiving the states, Bob measures the different response ratio between the single state and decoy state. If there is an eavesdropping, the ratio will change and Eve will be detected. Discussing the security of TEQKD under PNS attacks will be our further work.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. U1636106, 61572053).

References

1 Li J, Li N, Zhang Y, et al. A survey on quantum cryptography. Chin J Electron, 2018, 27: 223–228
2 Wang N, Fu J S, Bhargava B K, et al. Efficient retrieval over documents encrypted by attributes in cloud computing. IEEE Trans Inform Forensic Secur, 2018, 13: 2653–2667
3 Bennett C H, Brassard G. An update on quantum cryptography. In: Advances in Cryptology. Berlin: Springer, 1984. 196: 475–480
4 Li J, Li N, Li L L, et al. One step quantum key distribution based on EPR entanglement. Sci Rep, 2016, 6: 28767
5 Shor P W, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol. Phys Rev Lett, 2000, 85: 441–444
6 Scarani V, Gisin N. Quantum communication between N partners and Bell's inequalities. Phys Rev Lett, 2001, 87: 117901
7 Grosshans F, Grangier P. Continuous variable quantum cryptography using coherent states. Phys Rev Lett, 2002, 88: 057902