A secure quantum key distribution scheme based on variable quantum encoding algorithms

Zhiwen Zhao (赵志文)[1], Yi Luo (罗 翼)[1*], Zhangji Zhao (赵章骥)[2], and Haiming Long (龙海明)[1],

[1] *Department of Electronics, School of Information, Beijing Normal University, Beijing 100875, China*

[2] *Department of Physics, School of Science, Harbin Institute of Technology, Harbin 150001, China*

[*] *Corresponding author: fwly2718@sina.com*

Received October 8, 2010; accepted December 7, 2010; posted online February 24, 2011

The security of the quantum secret key plays a critical role in quantum communications. Thus far, one problem that still exists in existing protocols is the leakage of the length of the secret key. In this letter, based on variable quantum encoding algorithms, we propose a secure quantum key distribution scheme, which can overcome the security problem involving the leakage of the secret key. Security analysis shows that the proposed scheme is both secure and effective.

OCIS codes: 270.5565, 270.5568.

doi: 10.3788/COL201109.032702.

In 1969, Wiesner from Columbia University raised, for the first time, that information can be kept secret due to characteristics of quantum mechanics; in 1984, this principle was put into practice[1]. The protocol BB84 was presented as the first quantum key distribution protocol in the whole world. Since then, some protocols based on the characteristics of quantum mechanics have appeared, such as quantum secure direct communication (QSDC)[2−11], quantum signature (QS)[12], quantum key distribution (QKD)[13−19], quantum identification authentication (QIA)[20−22], and so on.

As one of the earliest areas in the research of quantum information, quantum key distribution has already been taken as a solid step forward. At present, apart from the protocol BB84, the main key distribution protocols include protocols B92, E91, and SARG04, to name a few. With these protocols, legal users are able to discover an attacker Eve in time while it is in the process of intercepting, measuring, or retransferring particles in the quantum channel. Therefore, these protocols are reliable concerning the security of communication. However, if Eve does nothing but collect particles during the course of data transmission, the attacker can obtain information on how many particle communicators have transferred, through which Eve can acquire N, the length of secret key. Moreover, Eve can speculate any bit at random with an accuracy rate of 0.5^N. Most people think that the security of secret key is high enough during the transmission even if the length of secret key is leaked. This assumption is based on the characteristics of quantum mechanics (e.g., quantum no-cloning theorem, Einstein-podolsky-Rosen (EPR) entanglement, and so on[1,18,19]). However, if the length of the secret key is not long enough, it is easy for the key to be cracked by an attacker. Moreover, with the improvement and application of quantum computing, the security of the secret key length plays an important role for a deciphering message. For example, in the encryption algorithm, which depends on the complexity of the prime factorization of large number, the complexity of deciphering for an L-bit large number will fall to $o(L^3)$ from $o(2^{\frac{1}{2}L})$ on a quantum computer[23].

In this letter, putting the security performance into consideration for a secure quantum communication, a new scheme of quantum key distribution is proposed in order to overcome the defect mentioned above. In the new scheme, two communicators should firstly transfer a particle sequence with N bits, where every particle randomly stands for one of the four coding solutions (i.e., one bit, two bits, three bits, or four bits). Secondly, the two communicators send another particle sequence to explain the coding rule of particles. Finally, the receiver will decode the first sequence according to the second sequence.

Prior to discussing our scheme, we denote $|0\rangle$ and $|1\rangle$ as the up and down eigenstates of σ_z, and then denote $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ as the up and down eigenstates of σ_x. Then, we can also define four Bell states as follows:

$$\psi_{12}^{+} = (|10\rangle_{12} + |01\rangle_{12})/\sqrt{2} = (|++\rangle_{12} - |--\rangle_{12})/\sqrt{2}, \quad (1)$$

$$\psi_{12}^{-} = (|10\rangle_{12} - |01\rangle_{12})/\sqrt{2} = (|-+\rangle_{12} - |+-\rangle_{12})/\sqrt{2}, \quad (2)$$

$$\psi_{12}^{+} = (|00\rangle_{12} + |11\rangle_{12})/\sqrt{2} = (|++\rangle_{12} - |--\rangle_{12})/\sqrt{2}, \quad (3)$$

$$\psi_{12}^{-} = (|00\rangle_{12} - |11\rangle_{12})/\sqrt{2} = (|+-\rangle_{12} - |-+\rangle_{12})/\sqrt{2}, \quad (4)$$

where the subscripts 1 and 2 denote the two correlated particles in an EPR pair.

Suppose Alice and Bob try to connect to each other secretly. At the beginning, Alice wants to send K, the secret key of M bits, to Bob. They should comply with the following steps to complete the secure transmission of the secret key.

Step 1: Alice encodes the secret key K first. The information of 0, 01, 010, and 0110 in the secret key K is encoded into $|0\rangle$ randomly, and that of 1, 10, 101 and 1001 is encoded into $|1\rangle$ randomly. Then, the sequence R with N qubits ($N \leq M$) is produced at the side of Alice, and $R = (|r_1\rangle, |r_2\rangle, \cdots, |r_N\rangle)$.

Step 2: Alice randomly creates ξ particles $|+\rangle$ or $|-\rangle$ and inserts them into the sequence R randomly such that a new sequence R with the length of $N + \xi$ is formed. Then, Alice sends the new sequence R to Bob. Once Bob receives the sequence of particles, Alice publicly announces the particles' positions at the sequence R. Afterwards, Bob should test whether or not these particles

© 2011 Chinese Optics Letters

are $|+\rangle$ or $|-\rangle$. If they are not, it can be said that the sequence has been damaged by attacker Eve or other factors, and Alice and Bob should stop the communication; if they are, they should move to the next step.

Step 3: Bob prepares a sequence of $2N + 2\delta$ EPR pairs, denoted as A-sequence, in such a way that all the EPR pairs in odd orders are in the same state ϕ^+, and all the EPR pairs in even orders are in the state ψ, which has been randomly selected from one of the four Bell states $\{\psi^+, \psi^-, \phi^+, \phi^-\}$. We denote the $2N + 2\delta$ EPR pairs in the A-sequence as $\left\{\left(a_1^1, a_2^1\right), \left(a_1^2, a_2^2\right), \cdots, \left(a_1^n, a_2^n\right), \cdots, \left(a_1^{2N+2\delta}, a_2^{2N+2\delta}\right)\right\}$, where the superscripts 1, 2, 3,$\cdots$, i, $\cdots$, $2N{+}2\delta$ indicate the order of each EPR pair in the sequence, and the subscripts 1 and 2 represent the different particles of each EPR pair, respectively. Alice then takes the first particle from each EPR pair in the A-sequence to form a particle sequence $\left\{a_1^1, a_1^2, \cdots, a_1^n, \cdots, a_1^{2N+2\delta}\right\}$, denoted as A$_1$-sequence. The remaining partner particles compose of another particle sequence $\left\{a_2^1, a_2^2, \cdots, a_2^n, \cdots, a_2^{2N+2\delta}\right\}$, denoted as A$_2$-sequence. Bob sends the A$_1$-sequence to Alice and keeps the A$_2$-sequence with him. After receiving the A$_1$-sequence, Alice publicly confirms that she has received the A$_2$-sequence.

Step 4: In order to check the security of the quantum channel between Bob and Alice, they carry out the following procedures to ensure that the A$_1$-sequence has not been eavesdropped on during the transmission.

1) Bob randomly selects δ pairs of adjacent particles in the A$_2$-sequence and tells Alice the positions of the selected particles through the classical channel.

2) Hereafter, Bob performs single photon measurement on each of the selected particles with σ_z basis or σ_x basis at random. He then informs Alice of his measurement bases and the results he obtained using these.

3) Alice performs single photon measurement on the partner particles of EPR pairs in the A$_1$-sequence with the same measuring basis as Bob. She then compares the measurement results with those of Bob.

According to the procedure described above, the measurement results of Bob and Alice should be completely the same if there are no eavesdroppers in the quantum channel. Consequently, with the comparison of the measurement results, Alice can evaluate the error rate of the transmission of the A$_1$-sequence. If the error rate exceeds the threshold, they should terminate the scheme immediately; otherwise, they can continue to the next step.

Step 5: Alice performs unitary operations to particles of even numbers in the A$_1$-sequence according to her way of coding presented in Step 1 expressed as

$$0 \text{ or } 1 \rightarrow U_{00} = |0\rangle\langle 0| + |1\rangle\langle 1|, \tag{5}$$

$$01 \text{ or } 10 \rightarrow U_{01} = |0\rangle\langle 1| + |1\rangle\langle 0|, \tag{6}$$

$$010 \text{ or } 101 \rightarrow U_{10} = |0\rangle\langle 1| - |1\rangle\langle 0|, \tag{7}$$

$$0110 \text{ or } 1001 \rightarrow U_{11} = |0\rangle\langle 0| - |1\rangle\langle 1|. \tag{8}$$

After these operations, the A$_1$-sequence is transformed into $\left\{a_1^1, U_{\rm A}^1 a_1^2, \cdots, a_1^{2i-1}, U_{\rm A}^i a_1^{2i}, \cdots, a_1^{2N-1}, U_{\rm A}^N a_1^{2N}\right\}$, $i \in \{1, 2, \cdots, N\}$. Thus the created EPR pairs by Bob turns into $\left\{\phi_{\rm AB}^+, U_A^1 \psi_{\rm AB}, \phi_{\rm AB}^+, U_{\rm A}^2 \psi_{\rm AB}, \cdots, \phi_{\rm AB}^+, U_{\rm A}^N \psi_{\rm AB}\right\}$.

Table 1. Process of Recovering ($\phi^+_{\mathbf{AB}}$, $\boldsymbol{U}^i_{\mathbf{A}}\psi_{\mathbf{AB}}$) According to ($|\boldsymbol{A}\rangle_{\mathbf{13}}$, $|\boldsymbol{B}\rangle_{\mathbf{24}}$)

$(\phi_{12}^+, U_{\rm A}^i \psi_{34})$	$(\|A\rangle_{13}, \|B\rangle_{24})$
$(\phi_{12}^+, \phi_{34}^+)$	$(\phi_{13}^+, \phi_{24}^+), (\phi_{13}^-, \phi_{24}^-), (\psi_{13}^+, \psi_{24}^+), (\psi_{13}^-, \psi_{24}^-)$
$(\phi_{12}^+, \phi_{34}^-)$	$(\phi_{13}^+, \phi_{24}^{24}), (\phi_{13}^-, \phi_{24}^-), (\psi_{13}^+, \psi_{24}^-), (\psi_{13}^-, \psi_{24}^+)$
$(\phi_{12}^+, \psi_{34}^+)$	$(\phi_{13}^+, \psi_{24}^+), (\phi_{13}^-, \psi_{24}^-), (\psi_{13}^+, \phi_{24}^+), (\psi_{13}^-, \phi_{24}^-)$
$(\phi_{12}^+, \psi_{34}^-)$	$(\phi_{13}^+, \psi_{24}^-), (\phi_{13}^-, \psi_{24}^+), (\psi_{13}^+, \phi_{24}^-), (\psi_{13}^-, \phi_{24}^+)$

Step 6: Alice performs a Bell-basis measurement (BM) on the particles $\left(a_1^{2i-1}, U_{\rm A}^i a_1^{2i}\right)$, and publishes the measurement outcomes using the classical channel. Bob then performs a BM on the particles $\left(a_2^{2i-1}, a_2^{2i}\right)$. According to the initial states of each EPR pair and Alice's BM outcomes, Bob can recover $(\phi_{\rm AB}^+, U_{\rm A}^i \psi_{\rm AB})$ as presented in Table 1. Now Bob knows the state of $U_{\rm A}^i \psi$ and the initial state of ψ; thus, he can deduce $U_{\rm A}^i$.

Step 7: After obtaining $U_{\rm A}^1, U_{\rm A}^2, \cdots, U_{\rm A}^N$, Bob is now able to decode $R = (|r_1\rangle, |r_2\rangle, \cdots, |r_N\rangle)$ on the basis of encoding rules, where the decoding result is denoted by K'. In order to ensure that K' is the same as the secret key Alice wants Bob to obtain, Bob then randomly selects θ-bit classical information from K', and encodes 0 and 1 into $|0\rangle$ or $|-\rangle$ randomly and $|1\rangle$ or $|+\rangle$ randomly, respectively. Therefore, a θ-qubit sequence T is formed, after which Bob sends it to Alice.

Step 8: After Alice receives T, Bob tells her the particles' positions in K' and the measuring bases used to measure these. Alice then performs single photon measurement on these and transforms her measurement results into classical information (where $|0\rangle$ and $|-\rangle$ are denoted by 0, $|1\rangle$ and $|+\rangle$ are denoted by 1). She then compares the transformed results with those bits in the same position of the secret key K. If they are the same, we may consider $K' = K$, that is, Bob has already obtained K.

Security performance is very important for a quantum key distribution scheme. Accordingly, the security of our protocol is now analyzed.

Firstly, in Step 2, an attacker Eve adopts the measurement-and-retransmission strategy: Eve measures the sequence R and creates a new sequence according to the measurement result. Then, Eve transfers it to Bob; because Eve has no idea where $|+\rangle$ or $|-\rangle$ has been inserted in R, Bob is able to find whether or not R is substituted in time. If Eve does nothing but listen, she can only obtain the length of the sequence with inserted trap bits.

Secondly, in Step 3, Eve can attack A$_1$-sequence. In the first instance, suppose Eve attempts to utilize the intercept-and-resend the strategy to attack A$_1$-sequence. In this case, Eve intercepts the qubits in the A$_1$-sequence and resends qubits as prepared by herself instead. Given that this attack method can destroy the entanglement correlation of the EPR pairs, the two legal users are able to detect the existence of Eve as long as they start the procedure of eavesdropping detection. Moreover, Eve adopts the measure-and-resend scheme to launch an attack. In this scenario, because Eve does not know the measurement basis of each qubit, her measurement on the qubits would lead to an increase of the error rate of data transmission; in turn, the increase of the error rate also can reveals the existence of Eve.

Finally, in Step 6, Alice publishes her measurement result, i.e., $|A\rangle_{13}$, which Eve can also obtain; however, Eve cannot recover the message $(\phi^{+}_{\rm AB}, U^{i}_{\rm A}\psi_{\rm AB})$ just by using $|A\rangle_{13}$. Now Eve cannot know the state of $U^{i}_{\rm A}\psi_{\rm AB}$ and $\psi_{\rm AB}$, leading to the inability to obtain the exact information about $U^{i}_{\rm A}$. Supposing Eve obtains the state of $|A\rangle_{13}$, because she has no idea of $|B\rangle_{24}$, only she can guess $U^{i}_{\rm A}\psi_{\rm AB}$ correct with the probability of 25%. In addition, in order to get $U^{i}_{\rm A}$, Eve has to guess $\psi_{\rm AB}$ (also the correct probability is 25%). In other words, the probability of Eve obtaining correct $U^{i}_{\rm A}\psi_{\rm AB}$ and $\psi_{\rm AB}$ simultaneously is 25% × 25% = 6.25%. Taking the possibility that Eve can obtain the correct $U^{i}_{\rm A}$ although she guesses $U^{i}_{\rm A}\psi_{\rm AB}$ and $\psi_{\rm AB}$ wrongly into consideration, the probability that Eve can obtain the correct $U^{i}_{\rm A}$ is no more than 25%.

In summary, in the protocol, the attacker Eve is only able to obtain the length of the sequence R without trap bits. At the same time, Eve can guess $U^{i}_{\rm A}$ at the probability of no more than 25%.

Thus, if Alice encodes the secret key of M bits to the particle sequence R of N qubits, Eve can only conclude that the length of K is between N and $4N$ bits. Accordingly, the probability that Eve is able to guess K correctly is expressed by:

$$\frac{0.5^{M}}{4N-N+1}=\frac{0.5^{M}}{3N+1}. \tag{9}$$

Therefore, it is more secure compared with other protocols. For example, if encoding 1-, 2-, 3-, and 4-bit classical information into a qubit with equal probability, we can obtain an equation as $N = 0.4M$, where M is the length of classical information and N is the length of the encoded quantum information. Given the encoding rule, the numbers of 1-, 2-, 3-, and 4-bit classical information are equal to $0.25N$, respectively. As such, we can obtain the equation as $0.25N \times 1 + 0.25N \times 2 + 0.25N \times 3 + 0.25\,N \times 4 = M$. In other words, $N = 0.4M$. In this situation, the probability that Eve can obtain a correct K is given by

$$\frac{0.5^{M}}{3N+1}=\frac{0.5^{M}}{1.2M{+}1}. \tag{10}$$

Obviously, the probability value is less than that of other protocols, where the value is 0.5^{M}. In this sense, security performance is much better.

In addition, we discuss the channel efficiency in this letter. Supposing that the condition is the same as the above example, if ξ, $\delta \ll N$, the efficiency should be expressed as

$$\frac{2.5N}{(N+\xi)+\xi+(2N+2\delta)+\delta+N}\approx\frac{2.5N}{4N}=62.5\%, \tag{11}$$

which is higher than the efficiencies of protocols BB84 (50%)[1], B92 (25%)[18], and E91 (22.5%)[19].

In conclusion, introducing variable quantum encoding algorithms, a secure quantum key distribution scheme is proposed in this letter. According to the encoding rule, Alice encodes the secret key K into sequence R randomly, after which Alice transfers R to Bob, along with another sequence describing the decoding rule. Finally Bob decodes the sequence R according to the decoding rule. This scheme can guarantee the security of information and prevent the length of the secret key from being leaked. Therefore, it is more secure and effective than other existing protocols.

References

1. C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* 175 (1984).
2. Y. Chen, Z.-X. Man, and Y.-J. Xia, Chin. Phys. Lett. **24,** 19 (2007).
3. G. L. Long and X. S. Liu, Phys. Rev. A **65,** 032302 (2002).
4. F.-G. Deng, G. L. Long, and X.-S. Liu, Phys. Rev. A **68,** 042317 (2003).
5. A.-D. Zhu, Y. Xia, Q.-B. Fan, and S. Zhong, Phys. Rev. A **73,** 022338 (2006).
6. Z.-X. Man and Y.-J. Xia, Chin. Phys. Lett. **24,** 15 (2007).
7. H. Ge and W.-Y. Liu, Chin. Phys. Lett. **24,** 2727 (2007).
8. F. Gao, S. Lin, Q.-Y. Wen, and F.-C. Zhu, Chin. Phys. Lett. **25,** 1561 (2008).
9. M.-J. Wang and W. Pan, Chin. Phys. Lett. **25,** 3860 (2008).
10. S.-J. Qin, Q.-Y. Wen, L.-M. Meng, and F.-C. Zhu, Chin. Phys. Lett. **26,** 020312 (2009).
11. F. Gao, F. Z. Guo, Q. Y. Wen, and F. C. Zhu, Sci. Chin. Ser. G: Phys. Mech. Astron. **51,** 559 (2008).
12. Z. Zhao, M. Naseri, and Y. Zheng, Opt. Commun. **283,** 3194 (2010).
13. A. P. Shurupov, S. S. Straupe, S. P. Kulik, M. Gharib, and M. R. B. Wahiddin, Europhys. Lett. **87,** 10008 (2009).
14. L. Zhang, C. Silberhorn, and I. A. Walmsley, Phys. Rev. Lett. **100,** 110504 (2008).
15. K. Wen, K. Tamaki, and Y. Yamamoto, Phys. Rev. Lett. **103,** 170503 (2009).
16. P. Eraerds, N. Walenta, M. Legré, N. Gisin, and H. Zbinden, New J. Phys. **12,** 063027 (2010).
17. C. Erven, X. Ma, R. Laflamme, and G. Weihs, New J. Phys. **11,** 045025 (2009).
18. C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69,** 2881 (1992).
19. A. K. Ekert, Phys. Rev. Lett. **67,** 661 (1991).
20. T. Mihara, Phys. Rev. A **65,** 052326 (2002).
21. W. van Dam, Phys. Rev. A **68,** 026301 (2003).
22. T. R. Beals, K. P. Hynes, and B. C. Sanders, New J. Phys. **11,** 085005 (2009).
23. D. Neuenschwander, Lecture Notes in Computer Science **3028,** 37 (2004).