Vol 16 No 8, August 2007
1009-1963/2007/16(08)/2215-04

Chinese Physics

© 2007 Chin. Phys. Soc.
and IOP Publishing Ltd

An efficient quantum key distribution protocol with orthogonal product states*

Yang Yu-Guang(杨宇光)[a)b)] and Wen Qiao-Yan(温巧燕)[c)]

[a)] *College of Computer Science and Technology, Beijing University of Technology, Beijing* 100022, *China*
[b)] *State Key Laboratory of Information Security (Graduate School of Chinese Academy of Sciences), Beijing* 100022, *China*
[c)] *School of Science, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*

(Received 30 November 2006; revised manuscript received 24 January 2007)

An efficient quantum key distribution (QKD) protocol with orthogonal product states in the $3 \otimes 3$ Hilbert space is presented. The sender, Alice, disorders the orthogonal product state sequence and sends it to Bob. After Alice has published the matching information of the particle sequence, Bob recovers the correct correspondences and makes an orthogonal measurement on the orthogonal product states to obtain the information sent by Alice. Finally, security analysis is also made.

Keywords: quantum key distribution, orthogonal product state, orthogonal basis measurement
PACC: 0365, 4230

1. Introduction

Cryptography is used mainly to transmit secret messages. With the development of quantum computation, especially the proposal of Shor's algorithm,[1] the base of the most important classical cryptographic scheme is shocked. But at the same time, the principles of quantum mechanics have also shed new light on the field of cryptography as these fundamental laws guarantee the secrecy of quantum cryptosystems. Any intervention of an eavesdropper, traditionally called Eve, must leave some trace which can be detected by the legal users of the communication channel. A lot of attention has been paid to the quantum key distribution (QKD)[2−15] since the BB84 protocol[2] was presented.

In most of the existing QKD protocols, the participants choose randomly one of two sets of measuring bases (MBs), the intrinsic efficiency of these protocols is usually 50%. The favoured-measuring-basis technique[13] and the measuring-basis-encrypted technique[6] were used for improving the intrinsic efficiency. Deng and Long proposed an order-rearrangement idea[16] about the QKD. The basic idea of order-rearrangement is that the sender, Alice, mixes up the correct correlation of the particles in the Einstein–Podolsky–Rosen (EPR) pairs so that Eve does not know which two particles are the particles in an EPR pair and he cannot perform Bell-basis measurement to steal the secret information. Later, Alice restores the correct correspondence of particles and obtains the result with Bell-basis measurement. The idea of order-rearrangement has been introduced into quantum secure direct communication, for example the protocols in Refs.[17,18].

In this paper, we present an efficient QKD protocol with orthogonal product states in the $3 \otimes 3$ Hilbert space. The sender, Alice, disorders the orthogonal product state sequence and sends it to Bob. After Alice has published the matching information of the particle sequence, Bob recoveries the correct correspondences and makes an orthogonal measurement on the orthogonal product states to obtain the information sent by Alice. Finally, the security analysis is made. The protocol is feasible with quantum storage[19,20] which makes delayed measurement possible.

The proposed QKD scheme has three advantages. Firstly, there is no need to prepare any entanglement. Secondly, the intrinsic efficiency is nearly 100%, and all the particles in the orthogonal product states except those used for eavesdropping check are retained for key distribution. Lastly, each orthogonal product

*Project supported by the National High Technology Development Program of China (Grant Nos 2006AA01Z419 and 2006AA01Z440), the Major Program of the National Natural Science Foundation of China (Grant No 90604023), the National Research Foundation for the Doctoral Program of Higher Education of China (Grant No 20040013007), National Laboratory for Modern Communications Science Foundation of China (Grant No 9140C1101010601).

state carries 3 bits of information because any state in a complete set is not used.

2. Quantum key distribution scheme

For a $3 \otimes 3$ system, one of the two-qutrit bases in a complete set $\{|\Psi_l\rangle\}$ is as follows:

$$
\begin{aligned}
\Psi_1 &= |0\rangle_1 \frac{1}{\sqrt{2}}(|0\rangle_2 + |2\rangle_2),\\
\Psi_2 &= \frac{1}{\sqrt{2}}(|1\rangle_1 + |2\rangle_1)|2\rangle_2,\\
\Psi_3 &= |2\rangle_1 \frac{1}{\sqrt{2}}(|0\rangle_2 + |1\rangle_2),\\
\Psi_4 &= \frac{1}{\sqrt{2}}(|0\rangle_1 + |1\rangle_1)|1\rangle_2,\\
\Psi_5 &= \frac{1}{\sqrt{2}}(|0\rangle_1 - |1\rangle_1)|1\rangle_2,\\
\Psi_6 &= |2\rangle_1 \frac{1}{\sqrt{2}}(|0\rangle_2 - |1\rangle_2),\\
\Psi_7 &= \frac{1}{\sqrt{2}}(|1\rangle_1 - |2\rangle_1)|2\rangle_2,\\
\Psi_8 &= |0\rangle_1 \frac{1}{\sqrt{2}}(|0\rangle_2 - |2\rangle_2),\\
\Psi_9 &= |1\rangle_1|0\rangle_2, \qquad (1)
\end{aligned}
$$

where the subscripts 1, 2 denote the first and second particles in an orthogonal product state sent to Bob, respectively.

For the $3 \otimes 3$ system, we just write out one of the various complete base forms, still 17 complete sets of product states possess nonlocality without entanglement.[21]

An ordered N orthogonal product state sequence is denoted with $[P_1(1), P_1(2); P_2(1), P_2(2); \ldots; P_i(1), P_i(2); \ldots; P_N(1), P_N(2)]$. $P_i(1)$ represents the first particle for Bob in the ith orthogonal product state, and $P_i(2)$ represents the second one, $i = 1, 2, \ldots, N$.

Because the information is encoded in the orthogonal product states, in order to prevent the secret information from eavesdropping, Alice cannot allow Eve to acquire simultaneously both particles in the orthogonal product states. If the correct correspondences of particles in the orthogonal product states are mixed up, Eve cannot know which two particles are in the same orthogonal product state.

In this scheme, we do not use the state $|1\rangle_1|0\rangle_2$ because the nonlocality in the complete set in Eq.(1) is preserved even if the $|1\rangle_1|0\rangle_2$ state is excluded.[22] So each product state can carry three-bit information.

The details of the present scheme are as follows:

(1) Alice and Bob agree that Ψ_1, Ψ_2, Ψ_3, Ψ_4, Ψ_5, Ψ_6, Ψ_7 and Ψ_8 represent classical information 000, 001, 010, 011, 100, 101, 110 and 111, respectively.

(2) Alice prepares an ordered N orthogonal product state sequence: $[P_1(1), P_1(2); P_2(1), P_2(2); \ldots; P_i(1), P_i(2); \ldots; P_N(1), P_N(2)]$ randomly in one of the nine orthogonal product states except $|1\rangle_1|0\rangle_2$. Alice makes a record of the orthogonal product states.

(3) Alice disorders the N orthogonal product state sequence and sends these particles to Bob one by one, namely, the particles are sent singely but not pairwise. For example, Alice sends the particles in the order of $P_2(1)$, $P_8(2)$, $P_{15}(1)$, $P_1(1)$, $P_2(2)$, $P_{30}(1)$, $P_{50}(2), \ldots, P_i(2), \ldots,$ and $P_N(2)$. And she makes a record of the positions of the transmitted particles.

(4) After Bob has received the $2N$ particles, Alice publishes the matching information of particles in the particle sequence. With this information, Bob obtains the correct correspondences of the particle sequence.

(5) Bob makes an orthogonal measurement on the basis in Eq.(1) and obtains his results as a raw key.

(6) In order to detect eavesdropping, Bob chooses randomly a subset of his results and publishes the positions and the outcomes. Alice and Bob make the error-rate analysis. If the error rate is lower than a threshold $\varepsilon_{\rm th}$, they can use the results as a raw key and distil a private key with error correction and privacy amplification; otherwise, they will abandon the results and repeat the quantum communication from the beginning.

Now we describe this scheme in detail. Steps (1) and (2) are obvious. We explain step (3). The goal of step (3) is to mix up the correct correspondences of particles in the orthogonal product states so that Eve cannot know which two particles are in the same orthogonal product state. Suppose that Eve intercepts the qutrits $P_i(1)$ and $P_j(2)$, then Eve can perform some joint measurement on the qutrits $P_i(1)$ and $P_j(2)$ on the basis in Eq.(1). However, the qutrits $P_i(1)$ and $P_j(2)$ are possibly not in an orthogonal product state in Eq.(1), and his measurement will cause errors. Eve still takes another strategy to obtain the information of single particle $P_i(1)$ ($P_j(2)$) by performing the local measurement on $P_i(1)$ ($P_j(2)$). However, because the qutrit $P_i(1)$ ($P_j(2)$) is chosen

from the non-orthogonal set $\left\{|0\rangle_1,\ \frac{1}{\sqrt{2}}(|1\rangle_1+|2\rangle_1),\right.$ $|2\rangle_1,\ \frac{1}{\sqrt{2}}(|0\rangle_1+|1\rangle_1),\ \frac{1}{\sqrt{2}}(|0\rangle_1-|1\rangle_1),\ \frac{1}{\sqrt{2}}(|1\rangle_1-$ $|2\rangle_1)\Big\}\left(\left\{\frac{1}{\sqrt{2}}(|0\rangle_2+|2\rangle_2),\ |2\rangle_2,\ \frac{1}{\sqrt{2}}(|0\rangle_2+\right.\right.$ $\left.\left.|1\rangle_2),|1\rangle_2,\ \frac{1}{\sqrt{2}}(|0\rangle_2-|1\rangle_2),\ \frac{1}{\sqrt{2}}(|0\rangle_2-|2\rangle_2)\right\}\right)$, according to the Heisenberg uncertainty principle of quantum mechanics, Eve's local measurement will obtain no useful information and cause errors. In step (4), Bob obtains the correct correspondences of his particles. That is, Bob's ith qutrit pair are $P_i(1)$ and $P_i(2)$, respectively. Step (6) is used to detect any possible eavesdropping attack. Bob chooses randomly a subset of his results and publishes the positions and the outcomes. In the error-free case, Alice expects that Bob can find some $P_i(1)$ and $P_i(2)$. For example, if the state prepared is Ψ_2, then Alice considers that Bob should announce 001. However, if Bob announces 010,011,100 or 101, Alice takes it that Eve exists and aborts the protocol.

3. Security analysis

Now, we consider the security of the present scheme. Recall that four possible states $\left(\left\{|0\rangle,\ |1\rangle,\ \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle),\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\right\}\right)$ are exploited in the BB84 protocol. This scheme can be regarded as the hybrid of three BB84 protocols based on three different sets of four states $\left\{|i\rangle,\ |j\rangle,\ \frac{1}{\sqrt{2}}(|i\rangle-|j\rangle),\frac{1}{\sqrt{2}}(|i\rangle+|j\rangle)\right\}$, where (i,j) are (0,1),(1,2),(2,0), respectively. The permutation of particles and the eavesdropping check in steps (6) can find the possible eavesdropping with higher probability than the BB84 protocol and that in Ref.[23]. In Ref.[23], Eve takes an efficient eavesdropping strategy. In this strategy, Eve measures the first particle from Alice and sends it to Bob. She measures the second particle corresponding to the measurement of the first one and sends it to Bob. In our security analysis of the present scheme, we assume Eve to take an attack similar to that in Ref.[23].

For simplicity of description and in contrast with that in Ref.[23], we assume the first particle in each orthogonal product state to be arranged in the odd position and the second one in the even position.

When the particle order is rearranged, Eve has to choose randomly a measurement basis for each particle in the particle sequence. We just need to calculate the information entropy obtained by Eve and the probability for Eve not to be detected. Compared with the case with no order-rearrangement operation on the particle sequence, we draw a conclusion that it is more secure than the case with no order-rearrangement operation on the particle sequence.

For simplicity and without loss of generality, we just consider the ith and $(i+1)$th particles (i is odd) in the particle sequence. Also we assume that Eve performs a measurement on the ith particle on the basis $\{|0\rangle,\ |1\rangle,|2\rangle\}$. Because Eve does not know which two particles are in an orthogonal product state, he cannot perform a proper measurement on the $(i+1)$th particle according to the measurement of the ith particle. He has to choose randomly a measurement basis, different from that in Ref.[23] where Eve can choose a corresponding measurement basis conditional on the measurement of the first particle. Now we discuss three cases, i.e. three different measurement bases that Eve chooses. Case 1: Eve performs a measurement on the $(i+1)$th particle on the basis $\{|0\rangle,|1\rangle,\ |2\rangle\}$. Case 2: Eve performs a measurement on the $(i+1)$th particle on the basis $\{|0\rangle+|2\rangle,\ |0\rangle-|2\rangle,\ |1\rangle\}$. Case 3 with the basis $\{|0\rangle+|1\rangle,\ |0\rangle-|1\rangle,\ |2\rangle\}$ is similar to case 2.

In case 1, the information entropy for each pair of particles obtained by Eve is I(Alice: Eve) $=H(Y)-$ $-H(Y|X)=\log_2 8-8/8=2$. Here X denotes the variable of the initial states and Y denotes the measurements.

Detection probability d is calculated as follows: $d=(1/8\times1/2\times1/2+1/8\times1/2\times1/2)\times8=1/2$.

In case 2, the information entropy for each pair of particles obtained by Eve is I (Alice: Eve) $=$ $H(Y)-H(Y|X)=\log_2 8-10/8=4/7$. Detection probability d is obtained as follows:

$$\begin{aligned} d= &\{1/8\times0+(1/8\times1/2\times1/2\times3/4)\times4\\ &+[(1/8\times1/4\times3/4)\times2+1/8\times1/2\times1/2]\\ &+[(1/8\times1/2\times1/2)\times2]\}\times2\\ &+(1/8\times1/2\times1/2)\times2\\ =&\ 17/32. \end{aligned}$$

Case 3 with the basis $\{|0\rangle+|1\rangle,\ |0\rangle-|1\rangle,\ |2\rangle\}$ is similar to case 2.

Finally, we make an average for the three cases and obtain the mutual information between Alice and Eve and detection probability

$$I = (\log_2 8 - 8/8) \times 1/3 + (\log_2 8 - 10/8) \times 2/3 = 11/6.$$

$$d = 1/2 \times 1/3 + 17/32 \times 2/3 = 25/48.$$

Obviously, compared with the case with no order-rearrangement operation,[23] the accessible information entropy by Eve is reduced and the perturbation introduced is increased.

In addition, in contrast with the scheme in Ref.[23] where Alice sends the second particle only when the first one reaches Bob, to eliminate the possibility for any eavesdropper to possess the two particles at the same time, our scheme has no such constraint, i.e. the particles can be transmitted simultaneously.

Next, we consider the case of coherent measurement attack. For Eve, the possible states after Alice's order-rearrangement operation are non-orthogonal and he never distinguishes between them deterministically. So this scheme really has the same essence as BB84-type protocols. Coherent measurement attack on the BB84-type protocols has been discussed in Refs.[24,25] where they are proved to be secure. So this scheme is also secure.

In addition, under practical conditions, the detection efficiency is not equal to 1, and the quantum channel is noisy. These details of security analysis are important and merit detailed analysis, and they are not studied in this paper.

4. Conclusions

In this protocol, an efficient QKD protocol with orthogonal product states in the $3 \otimes 3$ Hilbert space is presented. The sender, Alice, disorders the orthogonal product state sequence and sends it to Bob. After Alice has published the matching information of the particle sequence, Bob recoveries the correct correspondences and makes an orthogonal measurement on the orthogonal product states to obtain the information sent by Alice. And the security analysis is also made.

The proposed QKD scheme has three advantages. Firstly, there is no need to prepare any entanglement. Secondly, the intrinsic efficiency is nearly 100%, and all the particles in the orthogonal product states except those used for eavesdropping check are retained for key distribution. Lastly, each orthogonal product state carries 3 bits of information because one state in a complete set is not used.

References

[1] Shor P W 1994 *Proceedings of the 35th Annual Symposium on Fundamentals of Computer Science* (FOCS) 124

[2] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing,* Bangalore, India (IEEE, New York) 173

[3] Ekert A 1991 *Phys. Rev. Lett.* **67** 661

[4] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557

[5] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121

[6] Hwang W Y, Koh I G and Han Y D 1998 *Phys. Lett.* A **244** 489

[7] Goldenberg L and Vaidman L 1995 *Phys. Rev. Lett.* **75** 1239

[8] Long G L and Liu X S 2002 *Phys. Rev.* A **65** 032302

[9] Koashi M and Imoto N 1997 *Phys. Rev. Lett.* **79** 2383

[10] Gao T, Yan F L and Wang Z X 2005 *Chin. Phys.* **14** 893

[11] Yang Y G, Wen Q Y and Zhu F C 2005 *Acta Phys. Sin.* **12** 5544 (in Chinese)

[12] Yang Y G, Wen Q Y and Zhu F C 2005 *Acta Phys. Sin.* **12** 5549 (in Chinese)

[13] Lo H K, Chau H F and Ardehali M 2005 *J. Cryptology* **18** 133

[14] Tittel W, Zbinden H and Gisin N 1999 *Phys. Rev.* A **59** 4150

[15] Funk A C and Raymer M G 2002 *Phys. Rev.* A **65** 042307

[16] Deng F G and Long G L 2003 *Phys. Rev.* A **68** 042315

[17] Zhu A D, Xia Y, Fan Q B and Zhang S 2006 *Phys. Rev.* A **73** 022338

[18] Wang J, Zhang Q and Tang C J 2006 *Phys. Lett.* A **358** 256

[19] Philips D F, Fleischhauer A, Mair A and Walsworth R L 2001 *Phys. Rev. Lett.* **86** 783

[20] Sun C P, Li Y and Liu X F 2003 *Phys. Rev. Lett.* **91** 147903

[21] Bennett C H, DiVincenzo D P, Fuchs C A, Mor T, Rains E, Shor P W, Smolin J A and Wootters W K 1999 *Phys. Rev.* A **59** 1070

[22] Hsu L Y and Li C M 2005 *Phys. Rev.* A **71** 022321

[23] Guo G P, Li C F, Shi B S, Li J and Guo G C 2001 *Phys. Rev.* A **64** 042301

[24] Cirac J I and Gisin N arxiv:quant-ph/9702002 v1

[25] Bechmann-Pasquinucci H and Gisin N 1999 *Phys. Rev.* A **59** 4238