Quantum key distribution scheme with orthogonal product states

Guo-Ping Guo, Chuan-Feng Li,* Bao-Sen Shi, Jian Li, and Guang-Can Guo†
Laboratory of Quantum Communication and Quantum Computation and Department of Physics, University of Science and Technology of China, Hefei 230026, People's Republic of China
(Received 12 February 2001; published 6 September 2001)

The general conditions for the orthogonal product states of the multistate systems to be used in quantum key distribution (QKD) are proposed, and a novel QKD scheme with orthogonal product states in the 3×3 Hilbert space is presented. We show that this protocol has many distinct features such as great capacity and high efficiency. The generalization to $n\times n$ systems is also discussed and an asymptotic limit of 1/2 for the eavesdropper's success probability is obtained.

DOI: 10.1103/PhysRevA.64.042301 PACS number(s): 03.67.Dd, 03.65.Ta

I. INTRODUCTION

Cryptography is created to satisfy the people's desire of transmitting secret messages. With the development of quantum computation, especially the proposal of Shor's algorithm [1], the base of the most important classic cryptographic scheme was 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, Eve, must leave some trace that can be detected by the legal users of the communication channel. All kinds of quantum key distribution (QKD) schemes, such as the Bennett-Brassard 1984 (BB84) protocol [2], the Bennett 1992 (B92) protocol [3], and the electron paramagnetic resonance (EPR) scheme [4] have been proposed. Recently, quantum cryptography with three-state systems was also introduced [5]. Experimental research on QKD is also progressing fast, for instance, the optical-fiber experiment of BB84 and B92 protocols have been realized up to 48 km [6], and QKD in free space for the B92 scheme has been achieved over 1 km distance [7].

In Ref. [8], Goldenberg and Vaidman first presented a quantum cryptography based on orthogonal states. Then there is the quantum-cryptographic scheme involving two truly orthogonal states [9]. The basic technique is to split the transfer of one bit of information into two steps, ensuring that only a fraction of the bit of information is transmitted at a time. Then the no-cloning theorem of orthogonal states [10] guarantee its security. Based on the impossibility of cloning nonorthogonal mixed states, the no-cloning theorem of orthogonal states says that the two (or more) orthogonal states $\rho_i(AB)$ of the system composed of A and B cannot be cloned if the reduced density matrices of the subsystem that is available first (say A) $\rho_i(A)=\mathrm{Tr}_B[\rho_i(AB)]$ are nonorthogonal and nonidentical, and if the reduced density matrices of the second subsystem are nonorthogonal. It is a very surprising result since it means that entanglement is not vital for preventing cloning of orthogonal states. In the case of a composite system made of two subsystems, if the subsystems are only available one after the other, then there are various cases that orthogonal states cannot be cloned.

For the multistate systems, Bennett *et al.* have shown that there are orthogonal product pure states in the 3×3 Hilbert space and proved that these states may have some degree of nonlocality without entanglement [11]. There was also an experimental demonstration of three mutually orthogonal polarization states [12], where biphotons are used as multistate systems.

We propose the general conditions for the orthogonal product states of the multistate composite systems to be used in QKD, then present a QKD scheme with the orthogonal product states of a 3×3 system that has several distinct features, such as high efficiency and great capacity. The generalization to the n-state systems, and eavesdropping is analyzed where a limit of 1/2 for the success probability of an efficient eavesdropping strategy is found as n becomes large enough.

II. THE QKD SCHEME WITH ORTHOGONAL PRODUCT STATES

In the present QKD scheme with orthogonal product states in the $n\times n$ Hilbert space, the transmission processing is the same as the QKD scheme with common orthogonal states [8]. The information is encoded in the holistic state of the two particles, and these two particles are sent separately to ensure that any eavesdropper cannot hold both particles at the same time. Since only an orthogonal product state are employed, operations on one subsystem have no effect on the other. There are some basic conditions for any set of orthogonal product states in the n-state composite systems to be used in the present QKD scheme: for any density matrix of any subsystem $\rho_i(P)$ there must be at least one $\rho_j(P)$ that is both nonidentical and nonorthogonal to $\rho_i(P)$. (P represents subsystem A or B; i and j represent different states of the set.) Then from the point of view of any subsystem [10], the standard no-cloning theorem [13] is satisfied, and this guarantees the security of the protocol. What is more, we can transmit $2\log_2 n$ bits of information, double the value of the existing QKD protocol with usual orthogonal states [8,9]. It is evident that this is the maximal information that can be transmitted by the $n\times n$ system.

For a 2×2 system, there are obviously no such orthogo-

*Electronic address: cfli@ustc.edu.cn
†Electronic address: gcguo@ustc.edu.cn

nal product states that satisfy the orthogonal states cryptography conditions. The reason is that if $\rho_0(P)$ are nonidentical and nonorthogonal to $\rho_1(P)$, then $\rho_0(A)\otimes\rho_0(B)$ cannot be orthogonal to $\rho_1(A)\otimes\rho_1(B)$.

Next, we consider the 3×3 system. A general set of orthonormal product states in this Hilbert space is as follows

$$\Psi_1=|1\rangle_A(a|1\rangle_B+b|0\rangle_B),$$

$$\Psi_2=|1\rangle_A(b^*|1\rangle_B-a^*|0\rangle_B),$$

$$\Psi_3=(c|1\rangle_A+d|0\rangle_A)|2\rangle_B,$$

$$\Psi_4=(d^*|1\rangle_A-c^*|0\rangle_A)|2\rangle_B,$$

$$\Psi_5=|2\rangle_A(e|0\rangle_B+f|2\rangle_B),$$

$$\Psi_6=|2\rangle_A(f^*|0\rangle_B-e^*|2\rangle_B),$$

$$\Psi_7=(g|0\rangle_A+h|2\rangle_A)|1\rangle_B,$$

$$\Psi_8=(h^*|0\rangle_A-g^*|2\rangle_A)|1\rangle_B,$$

$$\Psi_9=|0\rangle_A|0\rangle_B, \tag{1}$$

where a, b, c, d, e, f, g, h are complex numbers, and $|a|^2+|b|^2=|c|^2+|d|^2=|e|^2+|f|^2=|g|^2+|h|^2=1$, the single-particle basis states $|0\rangle$, $|1\rangle$, and $|2\rangle$ are orthonormal.

This set of states has been proven to have some degree of nonlocality without entanglement, when $a=b=c=d=e=f=g=h=1/\sqrt{2}$ [11]. For the general case, no satisfactory proof for the existence of the nonlocality has yet been found. But if they satisfy the conditions mentioned above, they can still be used in this QKD scheme.

The process of this QKD scheme is as follows: Alice prepares two particles A and B randomly in one of the nine orthogonal product states shown above and sends particle A to Bob, and when Bob receives it, he informs Alice through an open classical channel. Then Alice sends out particle B. When particles A and B are both in the hand of Bob, he makes a collective orthogonal measurement using the basis of Eqs. (1) to determine in which state the two-particle system has been prepared. After a sequence of this procedure, they can share a random bit string, which is the raw key. In order to find possible eavesdropping, Alice and Bob randomly compare some bits to verify whether the correlations have been destroyed. If the key is true with as high a probability as they require, it can be believed that there is no eavesdropper and all of the rest of the results can be used as a cryptographic key. Otherwise, all the key is discarded and it must be redistributed.

What is vital to this scheme is that Alice sends the second particle only when the first one reaches Bob, to eliminate the possibility of any eavesdropper to possess the two particles at the same time. This protocol has some distinct features. As all of the raw key, except a small portion chosen for checking eavesdroppers are usable, it is very efficient (nearly 100%), and it has large capacity since $\log_2 9$ bits information is transmitted by a 3×3 system.

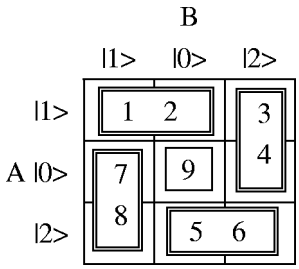

FIG. 1. The graphical depiction of the set of orthogonal product states in the 3×3 Hilbert space.

III. EAVESDROPPING AND THE GENERALIZATION TO THE *n*-STATE SYSTEM

We first consider one 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 result of the first one and sends it to Bob.

The particular eavesdropping is as follows: Eve intercepts particle A and makes an orthogonal measurement in the basis $\{|0\rangle,|1\rangle,|2\rangle\}$. Suppose particle A is found in state $|1\rangle_A$, Eve knows that the two-particle states of A and B are Ψ_1, Ψ_2 with probability 1/9, respectively, or Ψ_3, Ψ_4 with probability $|c|^2/9$ and $|d|^2/9$, respectively. Then she sends it to Bob. When particle B comes, she intercepts it too and measures it in the basis $\{|2\rangle_B, a|1\rangle_B+b|0\rangle_B, b^*|1\rangle_B-a^*|0\rangle_B\}$ and then sends it to Bob. If Eve sees that particle B is in $a|1\rangle_B+b|0\rangle_B$ or $b^*|1\rangle_B-a^*|0\rangle_B$, then obviously, (ignoring noise), she knows that the two-particle state is Ψ_1 or Ψ_2. In this case, she is lucky enough to conceal from Alice and Bob, for the two-particle state is not disturbed. And if Eve finds particle B in state $|2\rangle_B$, then the two-particle state is Ψ_3 or Ψ_4, which has collapsed to $|1\rangle_A|2\rangle_B$, then Bob has the partial probability of $|c|^2$ or $|d|^2$ to find the two-particle state in Ψ_3 or Ψ_4, respectively. So it is clear that for the case where Eve measures the particle A in the state $|1\rangle_A$, the probability for her to eavesdrop without being detected is $(2+|c|^4+|d|^4)/9$. Analyzed in the same way, the total probability that Eve eavesdrops the key information without being detected is

$$P_3=5/9+2(|c|^4+|d|^4+|h|^4+|g|^4)/9. \tag{2}$$

Then it is evident that P_3 gets the minimal value of 7/9 when $|c|^2=|d|^2=|h|^2=|g|^2=1/2$.

We depict this set of states in the 3×3 Hilbert space in a visual graphical way [11] as Fig. 1 shows. The four dominoes represent the four pairs of states that involve superposition of the basis states $|0\rangle$, $|1\rangle$, or $|2\rangle$. It is obvious that this figure is fourfold rotation symmetric, and we will show later that this symmetry is one of the basic requirements for there to be two symmetrical eavesdropping strategies. From this figure we can obviously see that all the states included in one row, where particle A is in basis states, can be eavesdropped without being detected in this strategy. But for all other states, there is only a certain probability, the fourth power of the modulus of the probability amplitude of the

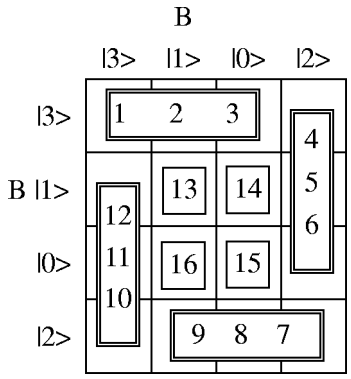

FIG. 2. The graphical depiction of the set of orthogonal product states in the 4×4 Hilbert space.

superposition states of particle A in the basis states, for Eve's successful eavesdropping. Then the total probability is P_3. Now let us consider the case of the $n\times n$ system. Since we only utilize orthogonal product states, and any superposition of n basis states that covers all the grids of any row (any column) in the graphic depiction will surely be distinguished by Eve, this will have no use in the present QKD scheme. In other words, any set of states including such a superposition state will violate the above conditions, then the possible superposition states can just be the ones of less than n basis states that cover no more than $n-1$ grids of the figures. The 4×4 system can be depicted in Fig. 2. We can see that the only difference between the figures of the 3×3 and 4×4 systems is that there are four states in the center of the 4×4 system, which can be eavesdropped without being detected. Then, generalized straightforwardly, the $2n\times2n$ system can be analyzed in a similar way as the $(2n-1)\times(2n-1)$ system. Thus, here we take the $(2n-1)\times(2n-1)$ system for example. $(n=2,3,4,\ldots,)$

Figure 3 depicts a set of orthogonal product states of the 5×5 system, which is generalized straightforwardly from the 3×3 system. For any complete set of orthogonal product states, the success probability for Eve to eavesdrop without being detected is

$$P_5=\left[9P_3+8+\left(\sum_{k,i,J}|\alpha_{J_{i_k}|3\rangle_B}|^4+\sum_{k,i,J}|\alpha_{J_{i_k}|4\rangle_B}|^4\right)\right]\Big/\ 25, \tag{3}$$

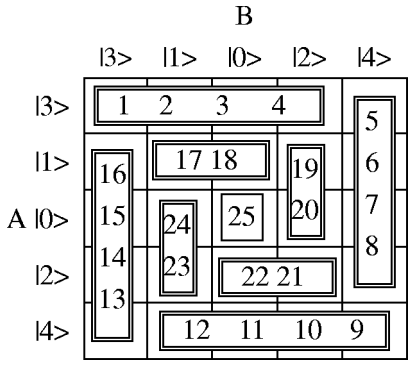

FIG. 3. The graphical depiction of the set of orthogonal product states in the 5×5 Hilbert space.

where $\alpha_{J_{i_k}|l\rangle_B}$ is the probability amplitude of the superposition states of particle A in the basis states and $\Sigma_J\alpha^2_{J_{i_k}|l\rangle_B}=1$ for any $|l\rangle_B$, k and i, and $|l\rangle_B$ means that particle B is in the basis state $|l\rangle_B$, k denotes dominoes in line $|l\rangle_B$, i_k denotes the superposition states in domino k, and J_{i_k} denotes the basis states that superposition state i_k involves, P_3 is Eve's success probability for the 3×3 system and 8/25 is the probability for states in row $|3\rangle_A$ and $|4\rangle_A$. We know from the graph that the dominoes in column $|3\rangle_B$ and $|4\rangle_B$ cover four grids in total (if five grids are covered, all the states in this column can be eavesdropped without being detected) and we have shown that $J_{i_k}\leqslant4$. It can be proved easily that P_5 reaches its minimal value 17/25 when P_3 gets its minimal value and only one domino is in column $|3\rangle_B$ or $|4\rangle_B$ and $|\alpha_{J_{i_k}|l\rangle_B}|^2=1/4$. This corresponds to the set of states depicted in Fig. 3. Then for the $(2n+1)\times(2n+1)$ system, the success probability is

$$P_{2n+1}=\left[(2n-1)^2P_{2n-1}+4n+\left(\sum_{k,i,J}|\alpha_{J_{i_k}|2n-1\rangle_B}|^4+\sum_{k,i,J}|\alpha_{J_{i_k}|2n\rangle_B}|^4\right)\right]\Big/\ (2n+1)^2. \tag{4}$$

The minimal probability can be obtained similarly:

$$\begin{aligned}\min\{P_{2n+1}\}&=[(2n-1)^2\min\{P_{2n-1}\}+4n+2]/(2n+1)^2\\&=1/2+(1+4n)/2(2n+1)^2,\end{aligned} \tag{5}$$

where $n\geqslant1$. We can deduce immediately that this value approaches 1/2 when n gets large enough.

Of course, there are other ways of plotting the graph symmetrically. But this set of states is the most secure. In fact, the value of $\min\{P_{2n+1}\}$ can be deduced straightforwardly from the symmetry of the plot. For any vertical domino contributes $1/(2n+1)^2$ to this value, any state in the horizontal dominoes and the state in the center each contributes $1/(2n+1)^2$. Due to the symmetry, there are at least $2n$ vertical or horizontal dominoes and $[(2n+1)^2-1]/2$ states in the horizontal dominoes.

For the $2n\times2n$ system, the same result can be reached. That is to say there is a limit of the probability of successful eavesdropping when the Hilbert space becomes large enough. And it is evident that in this strategy only particle A may be demolished, and particle B is not infected at all. The function of the operation to B that depends on the result of the measurement on A is just to extract more information.

Eve may adopt the complementary eavesdropping strategy, in which Eve tries to eavesdrop some information by intercepting and operating only on the second particle B, which may cause demolition to it. Then for the set of states in the $n\times n$ systems, whose graphic depictions are fourfold rotation symmetric, the probability to eavesdrop some infor-

mation without being detected is equal to that of the first strategy, i.e., P_n. But for those states without such symmetry, it can be verified that one of the success probabilities for the complementary strategies is larger than P_n. So we employ the symmetric states in the present scheme.

Of course, there are other strategies, for example, she can hold up the first particle *A* and send out a substitute particle *C* to Bob. When *B* comes, she makes a collective measurement under the two-particle orthogonal basis, then sends out a particle *D* in the state of *B*. In this strategy, Eve can eavesdrop the information entirely, but the probability for her to pass the checking process is only $1/n$, which tends to zero, for the state of particle *C* is randomly chosen from an *n*-dimensional Hilbert space.

IV. CONCLUSION

We have proposed the general conditions for the orthogonal product states to be used in QKD, then presented a QKD scheme with the orthogonal product states of a 3×3 system that has several distinct features, such as high efficiency and great capacity. The generalization to the *n*-state systems, and eavesdropping is analyzed where an asymptotic limit of 1/2 for the success probability of an efficient eavesdropping strategy is found as *n* becomes large enough.

ACKNOWLEDGMENT

This work was supported by the National Natural Science Foundation of China.

[1] P.W. Shor, in Proceedings of the 35th Annual Symposium on Fundamentals of Computer Science, 1994, p. 20.
[2] C.H. Bennett and G. Brassard, *Advances in Cryptology*, Proceedings of the Ctypto84 (Springer-Verlag, Berlin, 1984), p. 475.
[3] C.H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[4] A. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[5] H.B. Pasquinucci and A. Peres, Phys. Rev. Lett. **85**, 3313 (2000).
[6] R.J. Hughes, G.L. Morgan, and C.G. Peterson, J. Mod. Opt. **47**, 533 (2000).
[7] W.T. Butter, Phys. Rev. Lett. **84**, 5652 (2000).
[8] L. Goldenberg and L. Vaidman, Phys. Rev. Lett. **75**, 1239 (1995).
[9] M. Koashi and N. Imoto, Phys. Rev. Lett. **79**, 2383 (1997).
[10] T. Mor, Phys. Rev. Lett. **80**, 3137 (1998).
[11] C.H. Bennett, D.P. Divincenzo, C.A. Fuchs, T. Mor, E. Rains, P.W. Shor, and J. A. Smolin, Phys. Rev. A **59**, 1070 (1999).
[12] T. Tsegaye, J. Soderholm, M. Atature, A. Trifonov, G. Bjork, A.V. Sergienko, B.E.A. Saleh, and M.C. Teich, Phys. Rev. Lett. **85**, 5013 (2000).
[13] W.K. Wootters and W.H. Zurek, Nature (London) **299**, 802 (1982).