Quantum secure direct communication with high-dimension quantum superdense coding

Chuan Wang,[1] Fu-Guo Deng,[1,2] Yan-Song Li,[1] Xiao-Shu Liu,[1] and Gui Lu Long[1,3]
[1]*Key Laboratory for Quantum Information and Measurements, and Department of Physics, Tsinghua University, Beijing 100084, People's Republic of China*
[2]*The Key Laboratory of Beam Technology and Materials Modification of Ministry of Education, and Institute of Low Energy Nuclear Physics, Beijing Normal University, Beijing 100875, People's Republic of China*
[3]*Key Laboratory for Atomic and Molecular NanoSciences, Tsinghua University, Beijing 100084, People's Republic of China*
(Received 26 November 2004; published 28 April 2005)

A protocol for quantum secure direct communication with quantum superdense coding is proposed. It combines the ideas of block transmission, the ping-pong quantum secure direct communication protocol, and quantum superdense coding. It has the advantage of being secure and of high source capacity.

DOI: 10.1103/PhysRevA.71.044305 PACS number(s): 03.67.Hk, 03.65.Ud, 03.67.Dd

Preventing information from leaking to an illegitimate user is one of the most important issues today. Quantum key distribution (QKD) provides a secure way for creating a private key. QKD has progressed quickly [1–8] since Bennett and Brassard presented the standard BB84 QKD protocol in 1984 [1]. Recently, quantum secure direct communication (QSDC) was proposed and actively pursued [9–17]. With QSDC, Alice and Bob can exchange secret messages directly without first generating a private key and then encrypting the secret message and send to the other party through another classical communication. The QSDC protocol proposed by Beige *et al.* [9] is a scheme with one communication in the quantum channel and another communication in the classical channel. The protocols in Refs. [14,15] work similarly. Boström and Felbinger put forward a ping-pong QSDC protocol following the idea of quantum dense coding [5] with Einstein-Podolsky-Rosen (EPR) pairs [18]. It is a quasisecure direct communication protocol [19]. Cai *et al.* modified the ping-pong protocol with single photons [13] and with a similar quasisecurity property [12]. Deng *et al.* proposed a two-step QSDC protocol [11] with entangled pairs. A quantum secure direct communication protocol based on polarized single photons has also been proposed [12]. One special property in the protocols in Refs. [11,12] is the introduction of quantum data block transmission for security in QSDC. To guard the secret message, one has to ensure the security of a block of quantum data before encoding the secret message. When errors exist, error correction and quantum privacy amplification [20] can be used to maintain its security.

In this paper, we present a QSDC protocol with quantum superdense coding in high-dimension Hilbert space [5,21–23]. The protocol has the feature of high capacity and appears to provide better security than that obtainable with a two-dimensional entangled quantum system. Moreover, it saves the quantum swapping operation.

Quantum superdense coding follows the ideas in quantum dense coding [5] and is shown in Fig. 1. The d-dimension Bell-basis states in a symmetric channel are [1,21,24,25]

$$|\Psi_{nm}\rangle = \sum_j e^{2\pi ijn/d}|j\rangle \otimes |j+m \bmod d\rangle/\sqrt{d}, \qquad (1)$$

where $n,m=0,1,\ldots,d-1$. The unitary operations

$$U_{nm} = \sum_j e^{2\pi ijn/d}|j+m \bmod d\rangle\langle j| \qquad (2)$$

can transform the Bell-basis state

$$|\Psi_{00}\rangle = \sum_j |j\rangle \otimes |j\rangle/\sqrt{d} \qquad (3)$$

into the Bell-basis state $|\Psi_{nm}\rangle$, i.e., $U_{nm}|\Psi_{00}\rangle = |\Psi_{nm}\rangle$. For two-party communication, one particle can carry $\log_2 d^2$ bits of information. In a nonsymmetric quantum channel, the two particles of the entangled quantum system have different dimensions [22,23]. For example, the first particle has p dimensions and the second one has q dimensions. Then the capacity is $\log_2 pq$.

Now we use a qutrit system to illustrate the direct secure quantum communication protocol with high-dimension entangled pairs. First, the receiver, Bob, prepares a sequence of N entangled qutrit states in $|\Psi_{00}\rangle_{\mathrm{HT}}$. For the qutrit system, there are nine generalized Bell-basis states [21]. Bob separates the N entangled qutrit pairs into two particle sequences. One sequence, the travel sequence (T-sequence for short), is formed by taking out one qutrit from each pair, and the remaining qutrits form another sequence, the home-sequence (H-sequence for short). Bob retains the H-sequence and sends the T-sequence to Alice through a quantum channel.

To guard the security of the T-sequence, Alice chooses randomly a portion of the T-sequence particles, forms a first-sample particle sequence, and performs *single-qutrit* measurement randomly in some conjugate measuring basis (MB). For the qutrit system, there are four such complete bases [28]. The Z-MB is composed of the following three

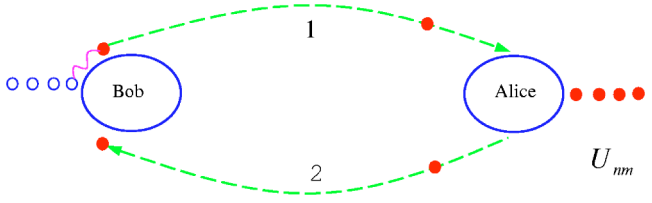

FIG. 1. (Color online) Schematic demonstration of quantum superdense coding. The U_{nm} is the unitary operation for encoding.

eigenvectors: $|Z_{-1}\rangle=|0\rangle$, $|Z_0\rangle=|1\rangle$, and $|Z_{+1}\rangle=|2\rangle$. The X-MB is chosen as

$$|x_{-1}\rangle = \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle),$$

$$|x_0\rangle = \frac{1}{\sqrt{3}}(|0\rangle + e^{2\pi i/3}|1\rangle + e^{-2\pi i/3}|2\rangle), \quad (4)$$

$$|x_{+1}\rangle = \frac{1}{\sqrt{3}}(|0\rangle + e^{-2\pi i/3}|1\rangle + e^{2\pi i/3}|2\rangle).$$

The two other bases are formed by

$$\frac{1}{\sqrt{3}}(e^{2\pi i/3}|0\rangle + |1\rangle + |2\rangle) \quad \text{and cyclic permutation} \quad (5)$$

and

$$\frac{1}{\sqrt{3}}(e^{-2\pi i/3}|0\rangle + |1\rangle + |2\rangle) \quad \text{and cyclic permutation}. \quad (6)$$

These conjugate bases have the following property: any basis vectors $|e_j\rangle$ and $|e_u\rangle$ belonging to different measuring bases satisfy the relation $|\langle e_j|e_u\rangle|^2=\frac{1}{3}$. For instance, $|\Psi_{00}\rangle$ in the MB Z with $d=3$ shown in Eq. (3) can be rewritten in the X-MB as $|\Psi_{00}\rangle=(1/\sqrt{3})(|x_{-1}\rangle|x_{-1}\rangle+|x_0\rangle|x_{+1}\rangle+|x_{+1}\rangle|x_0\rangle)$. When a single qutrit is measured in the X-MB, it gives equal probability to all three different eigenvalues. Similarly, $|\Psi_{00}\rangle$ can be decomposed in terms of the other two bases. Alice measures each particle in the first-sample sequence randomly in one of these bases. Alice then tells Bob the position and the type of measuring basis of the particles of the first-sample sequence, and Bob makes single-qutrit measurement on the corresponding particles in his H-sequence, in the same measuring basis as Alice's. Then Bob publicly announces the result of his measurement for the first-sample particles. Upon this, Alice can determine the security of her T-sequence. This constitutes the first eavesdropping check.

If there are no errors, then Alice concludes that the T-sequence is safe. In order to encode the secret message, Alice and Bob agree that the unitary operations U_{00}, U_{01}, U_{02}, U_{10}, U_{11}, U_{12}, U_{20}, U_{21}, and U_{22} represent the secret message 00, 01, 02, 10, 11, 12, 20, 21, and 22, respectively. Alice has to choose randomly from the T-sequence a subset of particles. This forms the second-sample sequence. The particles after subtracting the two sampling sequences are the message carriers of QSDC, and we call them the M-sequence. Alice performs superdense coding operations on the particles in the M-sequence and performs randomly one superdense coding operation on each of the particles in the second-sample sequence. Then Alice sends the encoded particle sequence, namely the T-sequence after subtracting the first-sample sequence, back to Bob. Upon receiving the encoded particle sequence, Bob performs a joint generalized Bell-basis measurement and reads the result: the message carried out by the M-sequence and the random operations on the second-sampling sequence particle. Then Alice announces the positions of the second-sample particles, and Bob announces the results of these sample particles. In this way, Alice and Bob can check if there is eavesdropping in the transmission from Alice to Bob.

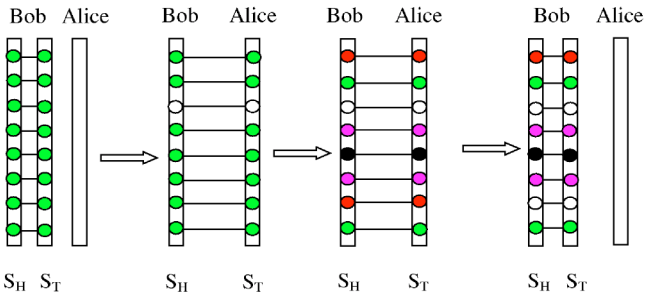

FIG. 2. (Color online) Illustration of the QSDC protocol with a sequence of entangled particle pairs. Two particles linked with a line are in a Bell-basis state. The T-sequence is traveling forth and back from Bob to Alice.

After one batch of N entangled particles is transmitted, then another batch of N particles is followed. In this way, QSDC is performed until the communication session is ended.

Now, let us describe the principle of our QSDC protocol with a symmetric d-dimensional quantum channel; the case for a nonsymmetric quantum channel is very much the same with little modification. The schematic demonstration of this QSDC protocol is shown in Fig. 2. The steps are described in detail as follows.

(i) The receiver of the communication, Bob prepares a sequence of entangled particles in the generalized Bell-basis state $|\Psi_{00}\rangle_{\mathrm{HT}}$. Here the subscript indicates the home particle retained at home and traveling particle which travels through the quantum channel forth and back from Bob to Alice.

(ii) Bob takes one particle from each entangled particle pair to make up an ordered partner particle sequence, say $[\mathrm{P}_1(H),\mathrm{P}_2(H),\mathrm{P}_3,\ldots,\mathrm{P}_N(H)]$. It is called the home sequence or simply the H-sequence. The remaining partner particles compose another particle sequence $[\mathrm{P}_1(T),\mathrm{P}_2(T),\mathrm{P}_3(T),\ldots,\mathrm{P}_N(T)]$, and it is called the traveling sequence or the T-sequence for short, shown in Fig. 2. Here the subscript indicates the pair order in the sequence, i.e., the i represents the ith entangled particle pair.

(iii) Bob sends the T-sequence to the sender of the secret message, Alice, and then they check eavesdropping by the following method. (a) Alice chooses randomly some particles from the T-sequence, called the first-sample particles, and this forms the first-sample sequence, and she uses randomly one of several conjugate single-particle measuring bases to measure each of the first-sample particles. (b) Alice tells Bob the positions of the sample particle and the type of measurement basis (MB) of the first-sample particles. (c) Bob takes a suitable measurement on the corresponding particles with the same MBs as those of Alice's. (d) Alice and Bob then announce the result of their measurements on the first-sample particles publicly. (e) Bob compares his results with Alice's to determine whether Eve is monitoring the quantum channel. This is called the first eavesdropping check. If their results are correlated, they can continue the QSDC to the next step, otherwise they abort the quantum communication.

(iv) Alice encodes the secret message on the T-sequence with the superdense coding unitary operations U_{nm} and transmits it to Bob. Alice has to do something in order to do a second eavesdropping check. During the encoding procedure, Alice chooses randomly some particles in the T-sequence that are not chosen in the first eavesdropping, called the second-sample sequence, and performs on them using randomly one of the d^2 superdense coding unitary operations U_{nm}. This choice of second-sample sequence in the coding makes a second eavesdropping check possible. Alice keeps the positions and the unitary operation of the second-sample particles secret until Bob receives the encoded T-sequence. The particles in the T-sequence subtracting the first-sample and second-sample sequences are the message carriers of the QSDC. They are called the M-sequence. Alice performs encoding unitary operations on the M-sequence particles and a random unitary operation on the second-sample particle and sends the encoded particle sequences, which are a combination of the M-sequence and the second-sample sequence, to Bob.

(v) Bob performs the generalized joint Bell-basis measurement on the entangled qudit pairs because he has both the H-sequence and T-sequence at hand. Note that some of the entangled pairs have been used up in the first eavesdropping check.

(vi) Alice tells Bob the positions and the type of unitary operations on them of the second-sample particles. Upon getting this information, Bob compares with his own measurement results and completes the second eavesdropping check analysis.

(vii) If the error rate of the sampling pairs is reasonably low, Alice and Bob can correct the error in the secret message using an error-correction method, such as CASCADE [26] or the Calderbank-Shor-Steane (CSS) [27] coding methods. Otherwise, Alice and Bob abandon the results of the transmission and repeat the procedures from the beginning.

It is worth pointing out the improvement of this protocol over the two-step QSDC protocol [11]. (i) A sequence of particles runs forth and back between Bob and Alice in this protocol just like the ping-pong protocol [10], whereas the two-particle sequence of particles is transmitted through the quantum channel from Alice to Bob in the latter. Theoretically this does not make any difference, but practically this reduces the demand on the equipment. Only Bob needs to prepare Bell-basis states and make Bell-basis measurement. (ii) Here the multidimensional Bell basis is used in this protocol instead of normal Bell-basis states. This increases the source capacity, and each particle can carry $\log_2 d^2$ bits of information. In addition, this protocol avoids the use of quantum swapping in the first eavesdropping check after the T-sequence transmitted from Bob to Alice. The reason is because Alice and Bob will detect Eve if she intercepts the particles in the T-sequence and resends some fake particles to Alice. Moreover, it appears that high-dimensional QSDC protocols provide better security than that obtainable with two-dimensional Bell-basis states, as has been discussed in detail in Ref. [28].

Like the two-step QSDC protocol [11], which is secure as Eve cannot steal the information about the secret message (in particular, its security can be enhanced with standard techniques such as quantum entanglement purification [29–31]), the present protocol is also secure as it can be reduced to a two-step QSDC protocol.

In summary, quantum secure direct communication can be done with quantum superdense coding in high dimension. We have provided a detailed realization of such a protocol. It has the advantage of not only having higher capacity, but also being more secure than the quantum communication protocols with a qubit system, as pointed out in Ref. [28]. Moreover, it is not necessary for Alice and Bob to do quantum swapping for the security of the transmission, and this QSDC can be used in a noisy channel with the help of quantum privacy amplification with quantum purification and quantum error correction.

This work is supported by the National Fundamental Research Program, Grant No. 001CB309308, China National Natural Science Foundation, Grants No. 60433050 and No. 10325521, and the SRFDP program of Education Ministry of China.

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[4] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[5] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[6] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[7] Y. S. Zhang, C. F. Li, and G. C. Guo, Phys. Rev. A **64**, 024302 (2001).
[8] G. L. Long and X. S. Liu, Phys. Rev. A **65**, 032302 (2002).
[9] A. Beige, B.-G. Englert, C. Kurtsiefer, and H. Weinfurter, Acta Phys. Pol. A **101**, 357 (2002); J. Phys. A **35**, L407 (2002).
[10] K. Boström and T. Felbinger, Phys. Rev. Lett. **89**, 187902 (2002).
[11] F. G. Deng, G. L. Long, and X. S. Liu, Phys. Rev. A **68**, 042317 (2003).
[12] F. G. Deng and G. L. Long, Phys. Rev. A **69**, 052319 (2004).
[13] Q. Y. Cai and B. W. Li, Chin. Phys. Lett. **21**, 601 (2004).
[14] F. L. Yan and X. Zhang, Eur. Phys. J. B **41**, 75 (2004).
[15] Z. J. Zhang and Z. X. Man, Chin. Phys. Lett. **22**, 18 (2005).
[16] Q. Y. Cai and B. W. Li, Phys. Rev. A **69**, 054301 (2004).
[17] Z. J. Zhang and Z. X. man, Chin. Phys. Lett. **22**, 22 (2005).
[18] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935); D. Bohm, *Quantum Theory* (Prentice Hall, Englewood Cliffs, NJ, 1951).

[19] A. Wójcik, Phys. Rev. Lett. **90**, 157901 (2003).
[20] F. G. Deng and G. L. Long, e-print quant-ph/0408102.
[21] X. S. Liu, G. L. Long, D. M. Tong, and F. Li, Phys. Rev. A **65**, 022304 (2002).
[22] A. Grudka and A. Wójcik, Phys. Rev. A **66**, 014301 (2002).
[23] F. L. Yan and M. Y. Wang, Chin. Phys. Lett. **21**, 1195 (2004).
[24] C. H. Bennett *et al.*, Phys. Rev. Lett. **70**, 1895 (1993).
[25] B. Zeng, X. S. Liu, Y. S. Li, and G. L. Long, Commun. Theor. Phys. **38**, 537 (2002).
[26] G. Brassard and L. Salrail, *Euro-cypt 193* Lectures Notes in Computer Seciences Vol. 765 (Springer-Verlag, New York 1994), pp. 410–423.
[27] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996); P. W. Shor, *ibid.* **52**, R2493 (1995); A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996); Proc. R. Soc. London, Ser. A **452**, 2551 (1996); Phys. Rev. A **54**, 4741 (1996).
[28] H. Bechmann-Pasquinucci and A. Peres, Phys. Rev. Lett. **85**, 3313 (2000).
[29] C. H. Bennett *et al.*, Phys. Rev. Lett. **76**, 722 (1996).
[30] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[31] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).