Theoretically efficient high-capacity quantum-key-distribution scheme

G. L. Long [1,2,3,4] and X. S. Liu [1,5]

[1] *Department of Physics, Tsinghua University, Beijing 100084, People's Republic of China*

[2] *Key Laboratory for Quantum Information and Measurements, Ministry of Education, Beijing 100084, People's Republic of China*

[3] *Institute of Theoretical Physics, Chinese Academy of Sciences, Beijing 100080, People's Republic of China*

[4] *Center for Atomic, Molecular and NanoSciences, Tsinghua University, Beijing 100084, People's Republic of China*

[5] *Department of Physics, Shandong Normal University, Jinan 250015, People's Republic of China*

(Received 6 July 2001; published 1 February 2002)

A theoretical quantum key distribution scheme using Einstein-Podolsky-Rosen (EPR) pairs is presented. This scheme is efficient in that it uses all EPR pairs in distributing the key except those chosen for checking eavesdroppers. The high capacity is achieved because each EPR pair carries 2 bits of key code.

DOI: 10.1103/PhysRevA.65.032302 PACS number(s): 03.67.Dd, 03.65.Ud, 42.79.Sz, 89.70.+c

Since languages became the tool for communication, the desire and need to transmit secret messages from one person to another began. Thus humans invented cryptography—a way to transmit information so that it is unintelligible and therefore useless to those who are not meant to have access to it. The most important classic cryptographic scheme is the public-key cryptosystem [1]; its safety relies on the high complexity of the underlying mathematical problems, for instance the factorization of large numbers. But with the development of quantum computation, especially the Shor's algorithm for factoring big numbers, the systems once seemingly unbroken in practice will be accessed easily. Now in the information community, the safety of transmission of secret information is becoming more and more important. One essential theme of secure communication is to distribute secret keys between senders and receivers. Quantum mechanics, one of the greatest discoveries of the 20th century, has now entered the field of cryptography: if the key distribution makes use of quantum states, an eavesdropper cannot measure them without disturbing them. The principle of quantum mechanics can help to make the key distribution secure. Up to now, there have already been several quantum key distribution (QKD) schemes: BB84 protocol [2], the Einstein-Podolsky-Rosen (EPR) scheme [3,4], B92 [5], the 4+2 protocol [6], the six-state protocol [7], the Goldenberg/Vaidman scheme [8], the Koashi/Imoto scheme [9], the recent Cabello protocol [10], and so on.

Experimental research on QKD is progressing very fast, for instance the optical–fiber experiment of BB84 and B92 protocols have been realized upto 48 km [11] and experimentation in the free space of the B92 scheme has been achieved over a distance of 1 km [12], and very recently up to 1.6 km during daylight [13].

Before presenting our scheme, we first introduce the notations. An EPR pair is one of the four Bell states

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle),$$

$$|\psi_3\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle),$$

$$|\psi_4\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle). \quad (1)$$

Alice and Bob agree beforehand that $|\psi_1\rangle$, $|\psi_2\rangle$, $|\psi_3\rangle$, $|\psi_4\rangle$ are encoded as 00,01,10,11 respectively. This coding increases the capacity of our scheme. An ordered N EPR particle pair sequence is denoted by $[(P_1(1), P_1(2)), (P_2(1),P_2(2)), \ldots,(P_i(1),P_i(2)), \ldots, (P_N(1),P_N(2))]$. We denote $P_i(1)$ for one particle in the ith EPR pair, and $P_i(2)$ for the other, and $i=1,2,\ldots,N$. We call $P_i(1)$ the EPR partner particle of $P_i(2)$ and vice versa. The order of these N EPR pairs is maintained throughout the QKD process. We can also take one EPR partner particle $P_i(1)$ from each EPR pair $(P_i(1),P_i(2))$ to form an EPR partner particle sequence $[P_1(1),P_2(1),\ldots,P_i(1),\ldots,P_N(1)]$. A Bell-basis measurement is a joint measurement of two particles onto the four Bell basis states.

Our protocol is as follows:

(1) Alice produces an ordered N EPR pair sequence: $[(P_1(1), P_1(2)), (P_2(1), P_2(2)), \ldots, (P_i(1),P_i(2)), \ldots,(P_N(1),P_N(2))]$.

(2) Then Alice takes one particle from each EPR pair to form an ordered EPR partner particle sequence: $[P_1(2), P_2(2), P_3(2), \ldots,P_N(2)]$. The rest of the EPR partner particles form another ordered EPR partner particle sequence: $[P_1(1), P_2(1), P_3(1), \ldots,P_N(1)]$. Alice sends to Bob one ordered EPR partner particle sequence: $[P_1(2), P_2(2), P_3(2), \ldots,P_N(2)]$.

(3) After Bob receives the ordered EPR partner particle sequence, randomly he chooses a sufficiently large subset among the EPR partner sets and performs measurement on the particles in the subset. The result of this measurement will be either 0 or 1. Bob stores the rest of the particles of his EPR particle sequence.

(4) Then Bob tells Alice through a classical channel (such as a telephone line) that he has received the particle sequence, and the particles that he has chosen to measure in a

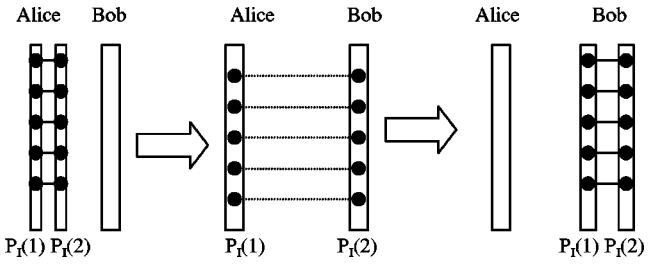

FIG. 1. Schematic illustration of the new QKD scheme.

certain direction. After hearing from Bob, Alice then performs measurement on the partner subset of those particles whose partner has been measured by Bob. Alice and Bob then publicly compare the results of these measurements to check eavesdropping. We refer to this procedure as the first eavesdropping check.

(5) If they are certain that there is no eavesdropping, then Alice sends Bob the remaining EPR particle sequence: $[P_1(1), \quad P_2(1), \quad P_3(1), \ldots, P_N(1)]$. Of course, the particles that have been measured are dropped from this particle sequence.

(6) After Bob receives these N particles, he takes one particle from each particle sequence in order and performs Bell-basis measurement on them. He records the results of the measurements.

(7) Alice and Bob choose a sufficiently large subset of these Bell-basis measurement results to determine if the QKD is successful. If the error rate in this check is below a certain threshold, then the Bell-basis measurement results are taken as raw keys. We refer to this procedure as the second eavesdropping check.

The procedure is shown in Fig. 1. During the transmission of the second particle sequence, Eve cannot access the EPR pairs, and hence cannot steal the key. Her action just causes disturbance to the key, which in fact is a kind of destruction. The second eavesdropping check is designed for detecting this. In practice, this procedure may well be combined with the privacy amplification procedure in the postprocessing stage of QKD. Next we discuss the security of the protocol.

First, the scheme is secure against direct measurement by Eve. In this attack, Eve intercepts the first particle sequence and makes measurements on them, then she resends these measured particle sequence to Bob. Because of Eve's measurement, all the EPR pairs, with one particle sequence at Alice's hand and the other particle set at Bob's hand, are destroyed. During the first eavesdrop checking procedure, Eve's destruction is not detectable because Bob's measurement will yield exactly the same results as Eve's which is consistent with the results of Alice's measurement. However during the second eavesdropping check, Eve's action is easily detected. Because the EPR pairs have collapsed, Bob will have only 50% probability of obtaining the right result when Bob uses the Bell-basis measurement to ''read'' his ''EPR'' particle pairs. For instance, suppose $|00\rangle+|11\rangle$ is collapsed into $|00\rangle$ by Eve's interception. Since

$$|00\rangle=\frac{1}{\sqrt{2}}|\psi_1\rangle+\frac{1}{\sqrt{2}}|\psi_2\rangle,$$

Bob has only a 50% chance of obtaining $|\psi_1\rangle$ when he makes a Bell-basis measurement. In order words, the error rate will be as high as 50%, and this can be easily detected. Eve cannot obtain any useful information from this destructive attack.

Second, the scheme is secure against the intercept-resend attack. Suppose Eve intercepts the particle sequence $\{P_i(2), i=1,\ldots,N\}$ and keeps it, but she cannot make a Bell-basis measurement because she does not possess the other particle sequence. In order to obtain the other particle sequence, she must send a fake particle sequence to Bob so that Bob can notify Alice. The particle sequence sent by Eve to Bob may well be a particle sequence from an EPR pair sequence $[(P_1^*(1),P_1^*(2)), \quad (P_2^*(1),P_2^*(2)), \ldots, (P_i^*(1),P_i^*(2)), \ldots,(P_N^*(1), \quad P_N^*(2))]$. However this can be detected easily during the first eavesdropping check. Bob randomly chooses a subset of particles and measures them. After Bob tells Alice what particles he has measured, Alice measures the corresponding particles at her hands. Then Alice and Bob publicly compare their results. If Bob's particle sequence is the fake particle sequence sent by Eve, half of his results during the first eavesdropping check will be inconsistent with that of Alice's. Eve will easily be detected. We can see this more clearly by studying the mutual information defined as [10]

$$I(X:Y)=H(X)-H(X|Y),$$

where $H(X)=-\Sigma_i p(x_i)\log_2 p(x_i)$ is the Shannon entropy, which is a function of the probabilities $p(x_i)$ of all possible values of X, and the sum is over those i with $p(x_i)>0$. $H(X|Y)$ is the expected entropy of X once one knows the value of Y, and is given by

$$H(X|Y)=\sum_j p(y_j)\left[-\sum_i p(x_i|y_j)\log_2 p(x_i|y_j)\right].$$

If there is no eavesdropping, the mutual information between Alice and Bob is $I_{AB}=2$, and the mutual information between Alice and Eve is zero. When there is eavesdropping, the mutual information between Alice and Eve is $I_{AE}=2$, and the mutual information between Alice and Bob is $I_{AB}=0$. Eavesdropping in this scheme is easily detected. This is compared with the BB84 protocol in which Eve eavesdrops with the same method as Bob, $I_{AB}=5/8\log_2 5+3/8\log_2 3-2\doteq 0.046$, and $I_{AE}=I_{EB}=3/4\log_2 3-1\doteq 0.189$. When there is no eavesdropping, the mutual information between Alice and Bob in the BB84 scheme is $I_{AB}=3/4\log_2 3-1\doteq 0.189$.

Third, the scheme is safe against the opaque attack strategy. In this strategy Eve intercepts every signal and measures them. If she gets a result, she just let the signal go. Otherwise she destroys the signal completely. In our scheme Eve cannot use this strategy, because Alice sends to Bob only one particle sequence at a time. This particle sequence is useless without the other particle sequence. If Eve tries to hide something, the QKD process simply stopped.

Like other QKD protocols using orthogonal states, one distinct feature of our scheme is its high efficiency in terms of number of keys sent to the number of EPR pairs (par-

ticles) used [10]. This is different from the EPR protocol or the BB84 protocol where only half of the EPR pairs or particles are used as keys. We now study the efficiency of the scheme. The information-theoretic efficiency defined in Ref. [10] is

$$\eta = \frac{b_s}{q_t + b_t}, \tag{2}$$

where b_s is the number of secret bits received by Bob, q_t is the number of qubit used, and b_t is the number of classical bits exchanged between Alice and Bob during the QKD process. Here the classical bits used for eavesdrop checking have been neglected. As has been discussed by Cabello [10], in the BB84 protocol, $b_s = 0.5$, $q_t = 1$, and $b_t = 1$. $b_t = 1$ bit is used to indicate whether Alice and Bob use the same measuring apparatus. In this way, the efficiency of BB84 is 25% Similarly the EPR protocol is 50%. The protocol present here becomes 100%.

Another feature of our scheme is its high capacity since the four possible states of the EPR pair carry two bits of information, whereas in the EPR scheme(BB84) each adopted EPR pair (particle) carries only one bit of information, in other words, N adopted EPR pairs can send $2N$ bits of key in our scheme.

Townsend has introduced a protocol to distribute secret keys to multiusers over optical fiber networks [14]. Townsend's protocol is a one-to-any protocol, where Alice acts as a single controller to establish and update a distinct secret key with each network user. An any-to-any protocol has been proposed to allow any two users to establish a secret key over an optical network by Phoenix *et al.* [15]. The present scheme can be generalized to distribute secret keys to multiple legitimate users. The present is different from the previous two protocols in that the secret keys are common to all legitimate users. The procedure is given in the following. After Alice has sent the keys to Bob, Bob can create an EPR pair sequence that carries the raw keys. Then he sends this EPR pair sequence to another legitimate user, Clare, using the same procedure as before. The key protocols common to Alice, Bob, and Clare are those Bell-basis measurement results that are not chosen to check eavesdropping. In this way, the protocol can be generalized to a multiparty common key distribution protocol.

The implementation of the protocol proposed here requires commensurate effort. Since it employs Bell-state measurements, its practical implementation is difficult. Nevertheless, it is worth noting that the operations employed here are all realizable in principle, for instance, the Bell-basis measurement was used in dense coding [16]. Recently complete Bell measurement has been realized in the experiment [17]. The sending of EPR partner particles was used in quantum clock synchronization [18]. Storage of light has been realized recently [19,20], and this may well serve to register the coming particle sequences and to store them. However, for a realistic implementation of the QKD scheme here, the efficiency of the Bell-basis detection and the length of time of photon storage need to be enhanced.

In conclusion, we propose a new QKD scheme that is secure, efficient, and has high capacity.

Discussions with Dr. Koashi are gratefully acknowledged. The authors are grateful for financial support from the China National Natural Science Foundation, The Major State Basic Research Development Program, Contract No. G200077407, the Hangtian Science Foundation, and The Fok Ying Tung Science Foundation for financial support.

[1] W. Diffie and M. Hellman, IEEE Trans. Inf. Theory **IT-22**, 644 (1997).
[2] 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.
[3] A. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[4] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[5] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[6] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995).
[7] D. Bruβ, Phys. Rev. Lett. **81**, 3018 (1998).
[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] A. Cabello, Phys. Rev. Lett. **85**, 5635 (2000).
[11] R. J. Hughes, G. L. Morgan, and C. G. Peterson, J. Mod. Opt. **47**, 533 (2000); quant-ph/9904038.
[12] W. T. Buttler *et al.*, Phys. Rev. Lett. **81**, 3283 (1998).
[13] W. T. Buttler *et al.*, Phys. Rev. Lett. **84**, 5652 (2000).
[14] P. D. Townsend, Nature (London) **385**, 47 (1997).
[15] S. J. D. Phoenix, S. M. Barnett, P. D. Townsend, and K. J. Blow, J. Mod. Opt. **42**, 1155 (1995).
[16] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[17] Y. Kim, S. P. Kulik, and Y. Shih, Phys. Rev. Lett. **86**, 1370 (2001).
[18] R. Jozsa, D. S. Abrams, J. P. Dowling, and C. P. Williams, Phys. Rev. Lett. **85**, 2010 (2000).
[19] D. F. Phillips, A. Flieischhauer, A. Maier, A. L. Walsworth, and M. D. Lukin, Phys. Rev. Lett. **86**, 783 (2001).
[20] C. Liu, Z. Dutton, C. H. Behroozi, and L. V. Hau, Nature (London) **409**, 490 (2001).