Quantum key distribution via quantum encryption

Yong-Sheng Zhang, Chuan-Feng 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 9 November 2000; published 28 June 2001)

A quantum key distribution protocol based on quantum encryption is presented in this Brief Report. In this protocol, the previously shared Einstein-Podolsky-Rosen pairs act as the quantum key to encode and decode the classical cryptography key. The quantum key is reusable and the eavesdropper cannot elicit any information from the particle Alice sends to Bob. The concept of quantum encryption is also discussed.

DOI: 10.1103/PhysRevA.64.024302 PACS number(s): 03.67.Dd, 03.65.Ud

The aim of quantum information science is to use nonclassical features of quantum systems to achieve performance in communication and computation that is superior to that achievable with systems based solely on classical physics. For example, current methods of public-key cryptography base their security on the supposed (but unproven) computational difficulty in solving certain problems, such as finding the prime factors of large numbers — these problems have not only been unproven to be difficult, but have actually been shown to be computationally "easy" in the context of quantum computation [1]. In contrast, it is now generally accepted that techniques of quantum cryptography can allow completely secure communications between distant parties [2]. The problem that the proposed protocols solve is how to enable two protagonists, "Alice" and "Bob," who share no secret information initially, to transmit a secret message x, for example, a cryptographic key, under the nose of an adversary "Eve," who is free to eavesdrop on all their communications.

In quantum key distribution (QKD), which is one of the important cryptographic tasks, Alice and Bob's classical communication is supplemented by a quantum channel, which Eve is also free to eavesdrop on if she dares. Because of the fragile nature of quantum information, any eavesdropping disturbs the quantum transmission in a way likely to be detected by Alice and Bob. The security of protocols for QKD, such as the Bennett-Brassard 1984 (BB84) [3] and the Bennett 1992 protocol (B92) [4] is based on the premise that nonorthogonal states cannot be cloned or discriminated exactly. Ekert's [5] and Cabello's [6] protocols are based on the nonlocal correlation of Einstein-Podolsky-Rosen (EPR) state. The orthogonal states' quantum QKD protocols are based on splitting transmission of one bit information into two steps [7]. We categorize all the protocols mentioned above as source-encrypting QKD, for their methods are making an alternative choice on the basis of the source [3–6] or splitting the source into two parts [7] .

On the other hand, the nonlocal correlation of the EPR [8] state has been applied to do much work in quantum information field, such as quantum teleportation [9], quantum dense coding [10], QKD [5], reducing the complexity of communication [11], etc. However, other applications of the EPR state in quantum information field are get to be discovered.

In this Brief Report, we present a QKD scheme using a method different from the protocols mentioned above. This protocol is a quantum encryption, i.e., using the quantum key to encode and decode the classical information. And the previously shared reusable EPR state acts as the quantum key. The information will not be leaked or eavesdropped without being known by the communication parties. We call it channel-encrypting QKD, compared with the previous protocols.

The QKD process of this protocol consists of the following steps. Alice and Bob have previously shared some quantity of the EPR pairs serving as the quantum key

$$|\Phi^+\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle). \tag{1}$$

When the process begins, the two parties rotate their particle's state by angle θ, respectively. The rotation can be described as

$$R(\theta)=\begin{pmatrix}\cos\theta & \sin\theta\\ -\sin\theta & \cos\theta\end{pmatrix}. \tag{2}$$

The state $|\Phi^+\rangle$ does not change under bilateral operation of $R(\theta)$. The purpose of this operation is to prevent the other parties from eavesdropping. (The detailed interpretation and the selection of θ will be given later in this paper.) Then Alice selects a value of a bit (0 or 1) and prepares a carrier particle γ in the corresponding state $|\psi\rangle$ ($|0\rangle$ or $|1\rangle$) randomly. The classical bit and the state $|\psi\rangle$ are only known by Alice herself. Alice uses the particle β_A of the entangled pairs and γ in state $|\psi\rangle$ to do a controlled-NOT (CNOT) operation (β_A is the controller and γ is the target) and the three particles will be in a GHz state

$$|\Psi\rangle=\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)_{\beta_A\beta_B\gamma},\quad \text{when}\,|\psi\rangle=|0\rangle,$$

$$\text{or}\ |\Psi\rangle=\frac{1}{\sqrt{2}}(|001\rangle+|110\rangle)_{\beta_A\beta_B\gamma},\quad \text{when}\ |\psi\rangle=|1\rangle. \tag{3}$$

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

Then she sends γ to Bob. Bob uses his corresponding particle β_B to do a CNOT operation on γ again. Now the key particles β_A and β_B and the carrier particle γ are in the same state as the initial state

$$|\Psi'\rangle=|\Phi^+\rangle\otimes|\psi\rangle. \tag{4}$$

Bob measures γ and will get the classical bit corresponding to state $|\psi\rangle$.

To assess the secrecy of their communication, Alice and Bob select a random part of their bit string and compare it over the classical channel. Obviously, the disclosed bits cannot then be used for encryption anymore. If their key had been intercepted by an eavesdropper, the correlation between the values of their bits would have been reduced. Eve's eavesdropping strategies and the security of this protocol will be discussed later in this paper.

If the QKD round succeeds, Alice and Bob retain all of the entangled states and can reuse them the next time. If the round fails, the parties discard all particles which were used until that point. In this case, Alice and Bob have to start again with new keys (EPR pairs).

We now discuss the security of this protocol. First, Eve can intercept the particle Alice sends to Bob and then resend it or another particle to Bob. However, Eve cannot elicit any information from the particle she intercepted, because it is in the maximally mixed state

$$\rho=\frac{1}{2}(|0\rangle\langle 0|+|1\rangle\langle 1|), \tag{5}$$

in spite of the bit value Alice sends out. If Eve sends this particle after disturbing it or sends another particle to Bob, it will introduce error when Bob decodes it by using the quantum key. If the state of the particle sent by Alice has been changed, the final state assumed is

$$\rho_i=\sum_{k=1}^{2} p_{ik}|\Psi'_{ik}\rangle\langle\Psi'_{ik}|,$$

$$|\Psi'_{ik}\rangle=a'_{ik}|0\rangle+b'_{ik}|1\rangle. \tag{6}$$

The average error rate of the classical key Alice transmits to Bob will be $\frac{1}{2}$.

The second eavesdropping strategy is to entangle with the key. Eve can intercept the particle γ Alice sends to Bob and use it and her own particle in state $|0\rangle$ or $|1\rangle$ to do a CNOT operation (her own particle is the target and γ is the controller). Then Eve resends γ to Bob. After Bob's decoding operation, Eve's particle is entangled with the key. It seems that Eve can use her particle to decode Alice's particle next time as Bob does. However, Eve cannot know in which state she is entangled with the key and cannot get any information of the state Alice sends to Bob. To detect this eavesdropping strategy, Alice and Bob can do a bilateral rotation $R(\theta)$ on the key (EPR pairs in state $|\Phi^+\rangle$) before Alice does the CNOT operation. The state of the maximally entangled two particles will be unchanged in this case. If Eve has entangled her particle with Alice and Bob's particles in the state $|\Phi\rangle_{ABE}=1/\sqrt{2}(|000\rangle+|111\rangle)$ [or $|\Phi\rangle_{ABE}=1/\sqrt{2}(|001\rangle+|110\rangle)$]. In the second round, the entangled state will be changed to

$$\begin{aligned}|\Phi\rangle_{ABE}=&\cos^2\theta\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)\\&+\sin^2\theta\frac{1}{\sqrt{2}}(|110\rangle+|001\rangle)\\&+\sin\theta\cos\theta\frac{1}{\sqrt{2}}(|011\rangle-|100\rangle)\\&+\sin\theta\cos\theta\frac{1}{\sqrt{2}}(|101\rangle-|010\rangle)\end{aligned} \tag{7}$$

or

$$\begin{aligned}|\Phi\rangle_{ABE}=&\cos^2\theta\frac{1}{\sqrt{2}}(|001\rangle+|110\rangle)\\&+\sin^2\theta\frac{1}{\sqrt{2}}(|111\rangle+|000\rangle)\\&+\sin\theta\cos\theta\frac{1}{\sqrt{2}}(|010\rangle-|101\rangle)\\&+\sin\theta\cos\theta\frac{1}{\sqrt{2}}(|100\rangle-|011\rangle),\end{aligned} \tag{8}$$

under the bilateral rotation. The error rate of the bit that Alice sends to Bob will be $2\cos^2\theta\sin^2\theta$. So if $\theta=\pi/4$, the error rate the eavesdropping caused will reach $\frac{1}{2}$. Thus the communication parties can select $\theta=\pi/4$ as the bilateral rotation angle in every round and Eve cannot get any useful information of the bit string they transmit.

Then we consider the more generic attacking. Assume that Eve can use her own system and the qubits sent by Alice to do a completely positive trace preserving map

$$\Lambda(\rho)=\sum_i V_i\rho V_i^\dagger \quad \text{with} \quad \sum_i V_iV_i^\dagger=I \tag{9}$$

on them, where I denotes the identity operator on the Hilbert space of the whole system's state. It is known [12] that the map is also of the form

$$\Lambda(\rho)=\mathrm{Tr}_C[U\rho\otimes\omega U^\dagger], \tag{10}$$

where ω is a state on the additional system C, and U is the unitary transformation on the joint system. So Eve's completely positive trace preserving map is equal to a unitary transformation on a larger system, and we can only consider the case in which Eve tries to obtain the information by unitary transformation on her own entire system and the qubit sent by Alice.

Suppose that Eve's system has entangled with Alice and Bob's key in the state

$$\frac{1}{\sqrt{2}}(|0\rangle|0\rangle|\psi_0\rangle+|1\rangle|1\rangle|\psi_1\rangle)_{ABE}\otimes|0\rangle_I, \tag{11}$$

where $|0\rangle_I$ is an indicator qubit for Eve to detect Alice's sending qubit and there is no restriction on the form of $|\psi_0\rangle$ and $|\psi_1\rangle$. After Alice and Bob do a bilateral rotation $R(\theta)$, Alice does a CNOT operation on the sending qubit and sends it out. Then Eve does a unitary transformation on the sending qubit and her own system. She expects that the indicator will be the same as the sending qubit. Assume that the unitary transformation has the universal form

$$U|i\rangle_S|\psi_k\rangle_E|j\rangle_I=(a_{ijk}|0\rangle|\psi_{aijk}\rangle|0\rangle+b_{ijk}|0\rangle|\psi_{bijk}\rangle|1\rangle + c_{ijk}|1\rangle|\psi_{cijk}\rangle|0\rangle+d_{ijk}|1\rangle|\psi_{dijk}\rangle|1\rangle)_{SEI}, \tag{12}$$

where $i,j,k=0,1$ and there is no restriction on the final states of $|\psi\rangle_E$.

If the attack strategy is successful, it requires that the output of the indictor qubit be the same as the sending qubit. However, when we compute the unitary transformation in Eq. (12) to satisfy this condition, we find that all the factors in Eq. (12) must be equal to 0. It means that the unitary transformation for a successful attacking strategy does not exist and the protocol is secure under this type of attack strategy. In fact, Eve's system and the sending qubit are in the reduced state

$$\rho=\frac{1}{4}(|0\rangle\langle 0|+|1\rangle\langle 1|)_S\otimes(|\psi_0\rangle\langle\psi_0|+|\psi_1\rangle\langle\psi_1|)_E\otimes|0\rangle_I\langle 0|, \tag{13}$$

whether the qubit sent by Alice is $|0\rangle$ or $|1\rangle$. So Eve has no way to distinguish them and obtain the qubit sent by Alice. Even if Eve adopts stronger strategies that would cause fewer errors and thus might be able to hide her presence in channel noise, she will obtain no information of the classical bit Alice sends to Bob, though she cannot be found.

Up to this point, our discussion has assumed that the initial state is the ideal maximally entangled state $|\Phi^+\rangle$. Suppose, however, that this state is corrupted a little after it is reused for many times, due to nonexact operation or decoherence. Alice and Bob have a state described by the density matrix

$$\rho=(1-\epsilon)|\Phi^+\rangle\langle\Phi^+|+\epsilon\rho_1, \tag{14}$$

where ϵ is a parameter of the deviation of ρ from $|\Phi^+\rangle\langle\Phi^+|$ and ρ_1 is the density matrix of an arbitrary state. Our results are most easily presented using the *trace distance*, a metric on Hermitian operators defined by $T(A,B)=\mathrm{Tr}(|A-B|)$ [13], where $|X|$ denotes the positive square root of the Hermitian matrix X^2. From the above, we can get that $T(|\Phi^+\rangle\langle\Phi^+|,\rho)\leqslant 2\sqrt{\epsilon}$.

Ruskai [14] has shown that the *trace distance* contracts under physical processes. If all operations are exact in the next QKD process, since the state $|\Phi^+\rangle$ will be unchanged in the process, the density matrix ρ will be transformed to

$$\rho'=(1-\epsilon)|\Phi^+\rangle\langle\Phi^+|+\epsilon\rho_1', \tag{15}$$

and $T(|\Phi^+\rangle\langle\Phi^+|,\rho')\leqslant 2\sqrt{\epsilon}$.

The fidelities [15]

$$F(|\Phi^+\rangle\langle\Phi^+|,\rho)$$

and

$$F(|\Phi^+\rangle\langle\Phi^+|,\rho')$$

are both no less than $1-\epsilon$, so the probability that the QKD process fails is no more than ϵ. Therefore, we can say that this protocol is robust. To prevent the degeneration of the entangled state, technologies of quantum privacy amplification [16] and entanglement purification [17] can be used. These processes need only local quantum operation and classical communication (LQCC). However, the number of available entangled pairs will be reduced and need to be supplied by sending qubits.

In the case where Alice sends particles in a noisy channel, the channel can be described by the Kraus operator [12]

$$\rho'=\sum_\mu M_\mu^+\rho M_\mu, \tag{16}$$

$$M_0=\sqrt{1-p_1-p_2-p_3}I,\quad M_1=\sqrt{p_1}\sigma_1,$$
$$M_2=\sqrt{p_2}\sigma_2,\quad M_3=\sqrt{p_3}\sigma_3, \tag{17}$$

where I is the identity operator and σ_i are Pauli operators

$$I=\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad \sigma_1=\begin{pmatrix}0&1\\1&0\end{pmatrix},\quad \sigma_2=\begin{pmatrix}0&-1\\1&0\end{pmatrix},$$
$$\sigma_3=\begin{pmatrix}1&0\\0&-1\end{pmatrix}. \tag{18}$$

Since the original states Alice wants to send are orthogonal states in the basis $\{|0\rangle,|1\rangle\}$, after Bob's decoding and measurement, the error of the state will be projected to one of the three Pauli operators σ_i, with probability p_i, respectively. For error σ_1, the carrier bit is flipped and the EPR pair is not affected; for σ_3, the carrier bit is not affected but the state of the EPR pair is changed from $|\Phi^+\rangle$ to $|\Phi^-\rangle=(1/\sqrt{2})(|00\rangle-|11\rangle)$; and for σ_2, the carrier bit is flipped and the EPR state is changed to $|\Phi^-\rangle$. As discussed later in this paper, we can conquer the bit flip by duplication code, and the corruption of the EPR pairs is the same as mentioned above.

In this protocol, the previously shared EPR pairs act as a quantum key to encode and decode the classical cryptography key, and the quantum key is reusable. In classical cryptography, both the encryption key and the decoding key are random series, but they have a definite correlation. It is the randomness in the encryption key that makes the information secure and it is the correlation between the decoding key and the encryption key that makes the receiver able to extract the useful information from the cryptogram. Similar to the classical counterpart, in the quantum encryption we presented, from any party's point of view the quantum key is in a maximally mixed state. In fact, any single particle of the entangled pair is in a completely uncertain state. However, the states of the two parties' particles have strong quantum correlation, which is called entanglement, and have no classical counterpart. It is this correlation that makes the quantum encryption secure. Since this correlation cannot be produced by LQCC, the eavesdropper cannot establish this correlation with the sender. So the quantum key is reusable. In the classical case, the only crypto system that provides perfect secrecy is the "one time pad" system, in which the encryption key cannot be used repeatedly. The more interesting character of this QKD scheme is that, since the eavesdropper cannot elicit any information from the particle Alice sends to Bob, Alice can use classical error-correction code technology, such as the duplication code, to conquer the bit flip error.

From another point of view, this protocol can be regarded as a quantum channel encryption, i.e., a quantum key encrypts the quantum channel. In the QKD protocols presented before, the sender uses alternative choices of the basis of the source or sends out the qubit separately. In our protocol, the classical bit is represented by the normal orthogonal basis of the particle. If we regard the EPR pair as a part of the channel, the quantum channel is encrypted. The classical information source can be transmitted securely, without leaking, in this modified channel.

In practice, the previously shared EPR pairs can be realized by standing qubits, such as entangled atoms, and the single photons can serve as the flying qubits sent out by Alice. The interaction of atom and photon can be realized by the technology of cavity quantum electrodynamics (CQED). The theoretical schemes of this technology have been proposed [18] and the research in laboratory has made some progress [19]. So this protocol is expected to be realized in the laboratory in the near future.

In summary, we have presented the concept of quantum encryption and proposed a QKD scheme based on quantum encryption. This method has been used in quantum authentication [20] and can be used for the encryption of arbitrary quantum states [21].

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

[1] P. W. Shor, in *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science* (IEEE Computer Society Press, Los Alamitos, CA, 1984), pp. 124–133.

[2] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).

[3] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 1984* (IEEE, New York, 1984), p. 175.

[4] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[5] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[6] A. Cabello, Phys. Rev. A **61**, 052312 (2000); A. Cabello, e-print arXiv quant-ph/0009051.

[7] L. Goldenberg and L. Vaidman, Phys. Rev. Lett. **75**, 1239 (1995); M. Koashi and N. Imoto, *ibid.* **79**, 2383 (1997); T. Mor, *ibid.* **80**, 3137 (1998).

[8] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).

[9] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[10] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).

[11] R. Cleve and H. Buhrman, Phys. Rev. A **56**, 1201 (1997).

[12] K. Kraus, *States, Effects and Operations: Fundamental Notions of Quantum Theory* (Wiley, New York, 1991).

[13] G. Vidal, D. Jonathan, and M. A. Nielsen, Phys. Rev. A **62**, 012304 (2000).

[14] M. B. Ruskai, Rev. Math. Phys. **6**, 1147 (1994).

[15] R. Jozsa, J. Mod. Opt. **41**, 2315 (1994).

[16] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).

[17] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).

[18] T. Sleator and H. Weinfurter, Phys. Rev. Lett. **74**, 4087 (1995).

[19] H. Mabuchi, Q. A. Turchette, M. S. Chapman, and H. J. Kimble, Opt. Lett. **21**, 1393 (1996); S. Haroche, M. Brune, and J. M. Raimond, Philos. Trans. R. Soc. London, Ser. A **355**, 2367 (1997).

[20] Y.-S. Zhang, C.-F. Li, and G.-C. Guo, e-print arXiv quant-ph/0008044.

[21] D. W. Leung, e-print arXiv quant-ph/0012077.