Quantum secure direct communication with χ-type entangled states

Song Lin,[1,2,*] Qiao-Yan Wen,[1] Fei Gao,[1] and Fu-Chen Zhu[3]
[1]*State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China*
[2]*School of Mathematics and Computer Science, Fujian Normal University, Fuzhou 350007, China*
[3]*National Laboratory for Modern Communications, P.O. Box 810, Chengdu 610041, China*
(Received 1 October 2008; published 23 December 2008)

In this paper, a quantum secure direct communication protocol with χ-type entangled states $|\chi^{00}\rangle_{3214}$ is proposed. We analyze the security of this protocol and prove that it is secure in ideal conditions. Then, an alternative way is presented to ensure the security of this protocol in a noisy channel. Moreover, this protocol utilizes quantum superdense coding to achieve a high intrinsic efficiency and source capacity. The practical implementation of this protocol is also discussed.

DOI: 10.1103/PhysRevA.78.064304 PACS number(s): 03.67.Dd, 03.65.Ud

I. INTRODUCTION

As we know, the task of cryptography is to transmit a secret message between two remote parties, Alice and Bob, in such a way that no eavesdropper can read it. All classical cryptosystems except for one-time pad [1] are based on computational complexity assumptions. That is, the security is conditional. Fortunately, quantum key distribution (QKD), which was proposed by Bennett and Brassard first [2], can overcome this obstacle skillfully. Since the security of QKD is assured by the quantum mechanics principles rather than difficulty of computation, these kinds of protocols have unconditional security in theory. Hence, the hybrid cryptosystem, QKD and one-time pad, is a perfect one to accomplish this task.

Recently, quantum secure direct communication (QSDC), a branch of quantum cryptography, has been presented and pursued. Different from QKD, QSDC allows messages to be transmitted directly in a deterministic and secure manner. In 2002, Beige *et al.* [3] proposed the first QSDC scheme. Afterwards, lots of QSDC schemes were presented, such as the schemes based on EPR pairs [4–8], single particle [9–11], and multipartite entangled state [12–15].

In this paper, an efficient QSDC protocol is proposed, based on four-qubit χ-type entangled state [16,17]

$$|\chi^{00}\rangle_{3214} = \frac{1}{2\sqrt{2}}(|0000\rangle - |0011\rangle - |0101\rangle + |0110\rangle + |1001\rangle + |1010\rangle + |1100\rangle + |1111\rangle)_{3214}, \quad (1)$$

where the subscripts denote different particles. Later we analyze the security of this protocol and prove that it is secure in ideal conditions. Furthermore, the case of this protocol in a noisy channel is studied, and an alternative way to ensure the practical security is presented.

II. QUANTUM SECURE DIRECT COMMUNICATION SCHEME WITH χ-TYPE ENTANGLED STATE

The genuine state $|\chi^{00}\rangle_{3214}$ has many interesting properties. For example, performing Pauli operation on the qubits 3 and 1, respectively, can construct an orthonormal basis set $FMB=\{|\chi^{ij}\rangle_{3214}=\sigma_3^i\sigma_1^j|\chi^{00}\rangle_{3214}|i,j=0,1,2,3\}$ for the four-qubit Hilbert space. Here, σ^i is one of the four Pauli operators, i.e.,

$$\sigma^0 = I = |0\rangle\langle 0| + |1\rangle\langle 1|, \quad \sigma^1 = |0\rangle\langle 1| + |1\rangle\langle 0|,$$
$$\sigma^2 = |0\rangle\langle 1| - |1\rangle\langle 0|, \quad \sigma^3 = |0\rangle\langle 0| - |1\rangle\langle 1|. \quad (2)$$

Meanwhile, these states are maximally entangled states and both the corresponding reduced density matrices of the qubits (3,1) and (2,4), are equal to the complete mixture, $\rho = \frac{1}{4}(|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + |11\rangle\langle 11|)$. Hence, no experiment performed on the qubits (3,1) or (2,4) can discriminate these states. But a measurement on four qubits can perfectly distinguish these states from each other. Armed with these features, we can encode four bit of information in the state $|\chi^{00}\rangle_{3214}$. To ensure that no eavesdropper can have access to the four particles together at any time, the transformation of these four particles is divided into two steps, which is the same as the protocol proposed by Deng *et al.* [5]. Hence, two legal users should apply the eavesdropping check before the message is encoded.

The eavesdropping check is based on another property of the state $|\chi^{00}\rangle_{3214}$. If one makes a measurement on the qubits 2 and 4 in the basis $BMB_1=\{|0+\rangle,|0-\rangle,|1+\rangle,|1-\rangle||\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)\}$, the χ-type entangled state will collapse and the other particles will end up in a corresponding two-qubit entangled state. The state $|\chi^{00}\rangle_{3214}$ may be rewritten in the following way, simply by regrouping terms:

$$|\chi^{00}\rangle_{3214} = \frac{1}{2}(|\Phi_1^-\rangle|0+\rangle + |\Phi_1^+\rangle|0-\rangle + |\Psi_1^-\rangle|1+\rangle + |\Psi_1^+\rangle|1-\rangle)_{3124}. \quad (3)$$

Here, $|\Phi_1^\pm\rangle = \frac{1}{\sqrt{2}}(|\phi^+\rangle \pm |\psi^-\rangle)$ and $|\Psi_1^\pm\rangle = \frac{1}{\sqrt{2}}(|\psi^+\rangle \pm |\phi^-\rangle)$, where $|\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ and $|\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$ are the four Bell states. The four states $|\Phi_1^\pm\rangle$ and $|\Psi_1^\pm\rangle$ form another orthonormal basis AMB_1 for the two-qubit Hilbert space. It can be seen that there are four possible results: $|\Phi_1^-\rangle|0+\rangle$, $|\Phi_1^+\rangle|0-\rangle$, $|\Psi_1^-\rangle|1+\rangle$, and $|\Psi_1^+\rangle|1-\rangle$. Furthermore, these results appear with equal probability, that is, 1/4. Obviously, there exists the similar correlation of the measurement results

*Corresponding author; lins95@gmail.com

if we measure the qubits (3,1) and (2,4) in the basis $AMB_2=\{|\Phi_2^{\pm}\rangle,|\Psi_2^{\pm}\rangle\}$ and $BMB_2=\{|+0\rangle,|-0\rangle,|+1\rangle,|-1\rangle\}$, respectively. Utilizing this feature, Alice and Bob can design a defense strategy to guard against eavesdropping in the transmission. Let us give an explicit description of the protocol as follows.

(1) Alice and Bob agree that the four Pauli operations represent two-bit classical information, respectively,

$$\sigma^0 \mapsto {}'00', \quad \sigma^1 \mapsto {}'01', \quad \sigma^2 \mapsto {}'10', \quad \sigma^3 \mapsto {}'11'. \quad (4)$$

(2) Alice prepares an ordered four-qubit state sequence $[P_1^1,P_1^1,P_3^1,P_4^1,P_1^2,P_2^2,\ldots,P_3^n,P_4^n]$. Here, the subscripts 1, 2, 3, and 4 represent four different particles in one χ-type entangled state and the superscripts 1, 2, 3, …, and n indicate the entangled pair orders in the sequence. These entangled particle pairs are all in the state $|\chi^{00}\rangle_{3214}$. Alice takes one particle from each entangled pair to form four ordered particle sequences: $S_1:[P_1^1,P_1^2,\ldots,P_1^n]$, $S_2:[P_2^1,P_2^2,\ldots,P_2^n]$, $S_3:[P_3^1,P_3^2,\ldots,P_3^n]$, $S_4:[P_4^1,P_4^2,\ldots,P_4^n]$. She keeps particle sequences S_1 and S_3, and sends the particles in sequences S_2 and S_4 to Bob.

(3) Bob chooses randomly a sufficiently large subset from S_2 and S_4 sequences and measures these particles (sample particles) in the bases BMB_1 or BMB_2. He stores the rest of his particles, and tells Alice the positions of the sample particles and his measurement basis through a classical channel. Then Alice measures the corresponding particles in the sequences S_3 and S_1 in the corresponding basis AMB_1 or AMB_2. Finally, Alice and Bob present their measurement outcomes to check quantum channels. If the error rate exceeds the threshold, Alice and Bob will discard these entangled particles and abort the protocol. Otherwise, they will securely use the remainder entangled pairs to communicate their secret message.

(4) In terms of her secret message, Alice applies the corresponding local unitary operation on the remainder of particles in her site (encoding particles). Suppose that Alice's secret is ${}'m_1m_2m_3m_4'$, where $m_i \in \{0,1\}$. She performs the operations $\sigma^{2m_1+m_2}$ and $\sigma^{2m_3+m_4}$ on the qubits 3 and 1, respectively. After that, Alice sends these encoding particles to Bob.

(5) After receiving these encoding particles, Bob measures the particles in his site in the basis *FMB* and gains the secret message transmitted by Alice fully.

III. SECURITY ANALYSIS

Suppose Eve is an evil attacker who wants to eavesdrop Alice's secret message without being detected. Let us start with considering the ideal conditions: There are no noises and losses in the quantum channel. In the following, we will prove that this protocol is secure in this case.

In the protocol, Eve has no access to the four qubits simultaneously. If Eve does not attack the transmission of the qubits 2 and 4, the encoding particles 3 and 1 are in the maximal mix state $\rho=\frac{1}{4}(|00\rangle\langle 00|+|01\rangle\langle 01|+|10\rangle\langle 10|+|11\rangle\langle 11|)$ no matter what Alice's operation is. That is, Eve cannot deduce the secret message only by measuring the encoding particles. Thus, the general attack strategy of Eve is depicted as follows. Eve prepares an ancilla E in the initial state $|\epsilon\rangle$. When the qubits 2 and 4 are propagated from Alice to Bob, Eve intercepts the travel particles, and makes the ancilla E interact unitarily with the qubits 2 and 4. Then, she sends these two qubits to Bob. When the encoding particles are transmitted to Bob, Eve captures the qubits 3 and 1, and makes a joint measurement on the encoding particles and the ancilla. In this way, she may gain information about the secret message. Later, it will be shown that Eve cannot achieve any information about the message in the condition that no errors are to occur.

In the eavesdropping process, Eve adds the ancilla E, and performs the unitary operation U on the particle 2, 4, and E. The most general operations Eve can do is able to be written as

$$\begin{aligned}
U: \quad & |00,\epsilon\rangle \to |00,\epsilon_{00}\rangle + |01,\epsilon_{01}\rangle + |10,\epsilon_{02}\rangle + |11,\epsilon_{03}\rangle \\
& |01,\epsilon\rangle \to |00,\epsilon_{10}\rangle + |01,\epsilon_{11}\rangle + |10,\epsilon_{12}\rangle + |11,\epsilon_{13}\rangle \\
& |10,\epsilon\rangle \to |00,\epsilon_{20}\rangle + |01,\epsilon_{21}\rangle + |10,\epsilon_{22}\rangle + |11,\epsilon_{23}\rangle \\
& |11,\epsilon\rangle \to |00,\epsilon_{30}\rangle + |01,\epsilon_{31}\rangle + |10,\epsilon_{32}\rangle + |11,\epsilon_{33}\rangle, \quad (5)
\end{aligned}$$

where $|\epsilon_{ij}\rangle$ $(i,j \in \{0,1,2,3\})$ are pure ancilla states uniquely determined by U. After this unitary interaction, the whole quantum system is in the state

$$\begin{aligned}
|\varphi\rangle = \tfrac{1}{2}[& |\phi^+\rangle(|00,\epsilon_{00}\rangle + |01,\epsilon_{01}\rangle + |10,\epsilon_{02}\rangle + |11,\epsilon_{03}\rangle) \\
& - |\psi^-\rangle(|00,\epsilon_{10}\rangle + |01,\epsilon_{11}\rangle + |10,\epsilon_{12}\rangle + |11,\epsilon_{13}\rangle) \\
& + |\psi^+\rangle(|00,\epsilon_{20}\rangle + |01,\epsilon_{21}\rangle + |10,\epsilon_{22}\rangle + |11,\epsilon_{23}\rangle) \\
& - |\phi^-\rangle(|00,\epsilon_{30}\rangle + |01,\epsilon_{31}\rangle + |10,\epsilon_{32}\rangle + |11,\epsilon_{33}\rangle)]_{3124E}. \quad (6)
\end{aligned}$$

Then, two cases will be discussed, in which Bob measures the qubits 2 and 4 in a different basis, respectively.

On the one hand, Alice and Bob measure the sample particles in the basis AMB_1 and BMB_1, respectively. Here, the state $|\varphi\rangle$ can be rewritten as follows:

$$|\varphi\rangle = \tfrac{1}{2}(|\upsilon_1\rangle|0+\rangle + |\upsilon_2\rangle|0-\rangle + |\upsilon_3\rangle|1+\rangle + |\upsilon_4\rangle|1-\rangle)_{31E24}, \quad (7)$$

where

$$\begin{aligned}
|\upsilon_1\rangle = \frac{1}{\sqrt{2}}(& |\phi^+\rangle|\epsilon_{00}\rangle + |\phi^+\rangle|\epsilon_{01}\rangle - |\psi^-\rangle|\epsilon_{10}\rangle - |\psi^-\rangle|\epsilon_{11}\rangle \\
& + |\psi^+\rangle|\epsilon_{20}\rangle + |\psi^+\rangle|\epsilon_{21}\rangle - |\phi^-\rangle|\epsilon_{30}\rangle - |\phi^-\rangle|\epsilon_{31}\rangle)_{31E}, \\
|\upsilon_2\rangle = \frac{1}{\sqrt{2}}(& |\phi^+\rangle|\epsilon_{00}\rangle - |\phi^+\rangle|\epsilon_{01}\rangle - |\psi^-\rangle|\epsilon_{10}\rangle + |\psi^-\rangle|\epsilon_{11}\rangle \\
& + |\psi^+\rangle|\epsilon_{20}\rangle - |\psi^+\rangle|\epsilon_{21}\rangle - |\phi^-\rangle|\epsilon_{30}\rangle + |\phi^-\rangle|\epsilon_{31}\rangle)_{31E}, \\
|\upsilon_3\rangle = \frac{1}{\sqrt{2}}(& |\phi^+\rangle|\epsilon_{02}\rangle + |\phi^+\rangle|\epsilon_{03}\rangle - |\psi^-\rangle|\epsilon_{12}\rangle - |\psi^-\rangle|\epsilon_{13}\rangle \\
& + |\psi^+\rangle|\epsilon_{22}\rangle + |\psi^+\rangle|\epsilon_{23}\rangle - |\phi^-\rangle|\epsilon_{32}\rangle - |\phi^-\rangle|\epsilon_{33}\rangle)_{31E},
\end{aligned}$$

$$|v_4\rangle = \frac{1}{\sqrt{2}}(|\phi^+\rangle|\epsilon_{02}\rangle - |\phi^+\rangle|\epsilon_{03}\rangle - |\psi^-\rangle|\epsilon_{12}\rangle + |\psi^-\rangle|\epsilon_{13}\rangle + |\psi^+\rangle|\epsilon_{22}\rangle - |\psi^+\rangle|\epsilon_{23}\rangle - |\phi^-\rangle|\epsilon_{32}\rangle + |\phi^-\rangle|\epsilon_{33}\rangle)_{31E}. \quad (8)$$

According to Eq. (3), the following conditions should be satisfied to avoid introducing error:

$$\langle\Phi_1^+|v_1\rangle = \langle\Psi_1^-|v_1\rangle = \langle\Psi_1^+|v_1\rangle = 0,$$

$$\langle\Phi_1^-|v_2\rangle = \langle\Psi_1^-|v_2\rangle = \langle\Psi_1^+|v_2\rangle = 0,$$

$$\langle\Phi_1^-|v_3\rangle = \langle\Phi_1^+|v_3\rangle = \langle\Psi_1^+|v_3\rangle = 0,$$

$$\langle\Phi_1^-|v_4\rangle = \langle\Phi_1^+|v_4\rangle = \langle\Psi_1^-|v_4\rangle = 0. \quad (9)$$

From Eqs. (8) and (9), we obtain

$$|\epsilon_{00}\rangle = |\epsilon_{11}\rangle, \quad |\epsilon_{22}\rangle = |\epsilon_{33}\rangle,$$

$$|\epsilon_{01}\rangle = |\epsilon_{10}\rangle, \quad |\epsilon_{23}\rangle = |\epsilon_{32}\rangle,$$

$$|\epsilon_{20}\rangle = |\epsilon_{21}\rangle = |\epsilon_{30}\rangle = |\epsilon_{31}\rangle = \mathbf{0},$$

$$|\epsilon_{02}\rangle = |\epsilon_{03}\rangle = |\epsilon_{12}\rangle = |\epsilon_{13}\rangle = \mathbf{0}, \quad (10)$$

where **0** is denoted as a null vector.

On the other hand, Bob measures the sample particles in the basis BMB_2. Similar to the method used above, the following constraints can be deduced,

$$|\epsilon_{00}\rangle = |\epsilon_{22}\rangle, \quad |\epsilon_{11}\rangle = |\epsilon_{33}\rangle,$$

$$|\epsilon_{02}\rangle = |\epsilon_{20}\rangle, \quad |\epsilon_{13}\rangle = |\epsilon_{31}\rangle,$$

$$|\epsilon_{10}\rangle = |\epsilon_{12}\rangle = |\epsilon_{30}\rangle = |\epsilon_{32}\rangle = \mathbf{0},$$

$$|\epsilon_{01}\rangle = |\epsilon_{03}\rangle = |\epsilon_{21}\rangle = |\epsilon_{23}\rangle = \mathbf{0}, \quad (11)$$

As a result, from Eqs. (11) and (12), we find that the whole system is in the state

$$|\varphi\rangle = |\chi^{00}\rangle_{3214}|\epsilon_{00}\rangle_E. \quad (12)$$

From the above equation, it is evident that $|\varphi\rangle$ is a product of a χ-type entangled state $|\chi^{00}\rangle_{3214}$ and the ancilla. This implies that Eve cannot gain more information about measurements on the qubits 3 and 1 from observing the ancilla. Consequently, Eve cannot gain any information about Alice's bit in the condition that no errors are to occur.

Now, let us consider another case, in which Eve executes a common attack that may not be the optimal one. Eve intercepts all the travel particles and sends some fake particles to Bob. After the coding done by Alice with quantum operation, Eve measures the travel particles in the basis *FMB*, and obtains the secret message completely. However, the eavesdropping check process described in step (3) can resist this attack. If the particles are selected as sample particles, we know only when they measure the original particles from the χ-type entangled state $|\chi^{00}\rangle_{3214}$ can Alice and Bob have the correlative results perfectly. This means that no matter what fake particles Eve sends to Bob, Eve's action will introduce 75% error rate in the results of the eavesdropping check. In the similar attack, the error rates of the other famous QSDC protocols, which were proposed in Refs. [4,10,5] respectively, are 50%, 37.5%, and 50%, separately. Hence, the presented protocol is more sensitive to eavesdropping compared with the other protocols [4,5,10].

In addition, a subtle attack strategy, denial-of-service (DoS) attack [18], should be considered in ideal conditions. For our protocol, Eve attacks particles 3 and 1 during the transmission of these particles in step (4). In this case, her action cannot be detected certainly since the attack only happens on the encoding particles. Therefore, Eve is able to make Bob's measurement results and Alice's secret message irrelevant even if she cannot attain any information about the secret message. It is evident that one can use the method mentioned in Ref. [18] to resist this attack in our protocol. Here, another way is presented, in which classical message authentication process is adopted. The alternative method is depicted briefly as follows. Before the encoding operation done by Alice, she chooses an apt one-way hash function h, where $h:\{0,1\}^l \rightarrow \{0,1\}^c$, and tells it to Bob via public classical channel. Then she calculates the authentication message $h(m)$, and encodes the message $m+h(m)$ on the travel particle sequence. At the end of the protocol, Bob obtains the message $m'+h(m)'$, and then determines whether the message has been tampered with or not by comparing $h(m')$ with $h(m)'$. By this means, we can also defense the DoS attack in our protocol.

For the sake of completeness, we now discuss the security of the presented scheme in a noisy channel. In a QSDC scheme, the secret message is transmitted directly. This means that classical privacy amplification step, which is essential for the unconditional security of QKD in the presence of noise, does not exist in QSDC. Hence, how to transmit a secret message directly and securely over a noisy channel becomes a problem for QSDC. Recently, Deng *et al.* [19] provides a method using quantum privacy amplification technique to solve this problem. Although quantum privacy amplification is principally possible, it is still difficult in recent technology, especially for multipartite entangled state. Here, utilizing all-or-nothing transform (AONT), we proposed an alternative method to ensure the security of QSDC in the case of noise, which will be depicted in the following.

An AONT [20] is a transformation f mapping a sequence $M=\{m_1,m_2,\ldots,m_n\}$ to another sequence $S=\{s_1,s_2,\ldots,s_l\}$. This kind of transformation generally satisfied the following conditions: (1). Given all $\{s_1,s_2,\ldots,s_l\}$ it is easy to compute M; (2). If any one of the s_i is missing then it is difficult to obtain any information about any m_j. Armed with AONT, we can preprocess the secret message at the beginning of our protocol to resist the attack proposed in [21]. That is, Alice performs f transformation on the message before encoding it on the particles. In this instance, even if Eve is able to eavesdrop a fraction of the transmitted message bits for the case of a noisy channel, she cannot obtain any information about Alice's secret message.

For example, the bit error rate of the noisy channel is $\frac{1}{7}$. In terms of the above secure analysis, we know that Eve steals

all secret messages and introduces 75% error rate. In this case, Eve replaces the noisy channel by an ideal one, and then intercepts a fraction $\frac{1}{5}$ of the particles during the first transmission. Her action can be hidden by the channel noise. In this way, Eve has a probability of 20% of obtaining one bit of message without being detected. To stand against this kind of attack, Alice performs the transformation $f: F_8^1 \rightarrow F_8^3$ on the secret message, where F_8 is a finite field of order 8. For any $m \in F_8$, we define $f(m)=s=(s_1,s_2,s_3)$ with $s_1=\lambda_1 \oplus \lambda_2 \oplus m$, $s_2=\lambda_2 \oplus \lambda_3 \oplus m$, $s_3=\lambda_3 \oplus \lambda_1 \oplus m$. Here λ_1, λ_2, $\lambda_3 \in F_8$ are chosen by Alice randomly, and $\oplus$ represents addition modulo 8. After that, Alice makes use of the presented protocol to transmit the message s. After obtaining the message s, Bob can infer the secret message $m=s_1 \oplus s_2 \oplus s_3$ without the requirement of any additional information. However, Eve steals the message m only when she can obtain the messages s_1, s_2, and s_3 fully. In this case, the probability of Eve eavesdropping one bit of information is $(\frac{1}{5})^3=0.8\%$. Hence, the security of the protocol in a noisy channel is improved at the cost of decreasing the transmission rate.

From the above discussion, it is shown that the security of the presented protocol in the presence of noise can arbitrarily be increased. However, the efficiency, which is an important criterion of a protocol, will be decreased greatly. As said in Ref. [22], infinite security needs infinite cost, which means that the practical interest is zero. Hence, when implementing the presented protocol in real circumstance, it is reasonable to choose an appropriate AONT in accordance with the security level of a secret message. Moreover, an additional point needs to be noted. The modified protocol is very sensitive to error. Hence, in terms of the noisy rate, an apt classical error-correction step should be interposed in our protocol. Considering the same scenarios as the above example, we may adopt [7,4] Hamming code to correct the error introduced by the channel noise. In addition, it is evident that the proposed method can also be used to improve the security of the existing QSDC protocol over a noisy channel.

IV. DISCUSS AND SUMMARY

Before giving a conclusion, it is worthwhile to review the whole system of the presented protocol in practical implementation. First, in terms of the real situation, Alice and Bob choose appropriately a one-way hash function h, an ANOT transformation f, and a classical error-correcting encoding algorithm e. Second, according to the secret message m, Alice utilizes the presented QSDC protocol to transmit the message $s=e\{f[m+h(m)]\}$. Finally, after receiving the message s, Bob can obtain the secret message m by performing the corresponding inverse operations on s.

In summary, we have shown that χ-type entangled state $|\chi^{00}\rangle_{3214}$ can be used to secure direct communication in such a way that the transmission of four particles containing the secret message divides into two steps. Adopting quantum superdense coding makes the presented protocol achieve a high efficiency. Meanwhile, Wang and Yang [17] presented a simple scheme for generating such a state and measuring it in the basis *FMB*. Thus, the presented protocol is feasible in recent technology. Furthermore, the security of the protocol is discussed in detail. Besides proving that the protocol is safe in ideal conditions, we propose a method to ensure the security of this protocol in the case of noise. The implementation of the presented method is only concerned with classical operation. Hence, our proposal offers a more practical and realistic alternative to the existing QSDC protocol over a noisy channel, as compared with quantum privacy amplification.

ACKNOWLEDGMENTS

This work was supported by the NHTRDP (863 Program) of China (2006AA01Z419); NSFC (Nos. 60873191, 60821001, and 90604023); the National Laboratory for Modern Communications Science Foundation of China (9140C1101010601); NSF of Beijing (4072020); and the Foundation of Fujian Education Bureau (JA08044).

[1] G. Vernam, J. Am. Inst. Electr. Eng. **55**, 109 (1926).
[2] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.
[3] A. Beige *et al.*, Acta Phys. Pol. A **101**, 357 (2002).
[4] K. Boström and T. Felbinger, Phys. Rev. Lett. **89**, 187902 (2002).
[5] F. G. Deng *et al.*, Phys. Rev. A **68**, 042317 (2003).
[6] A. D. Zhu *et al.*, Phys. Rev. A **73**, 022338 (2006).
[7] C. Wang *et al.*, Phys. Rev. A **71**, 044305 (2005).
[8] F. G. Deng *et al.*, Phys. Lett. A **359**, 359 (2006).
[9] F. G. Deng and G. L. Long, Phys. Rev. A **69**, 052319 (2004).
[10] M. Lucamarini and S. Mancini, Phys. Rev. Lett. **94**, 140501 (2005).
[11] J. Wang *et al.*, Phys. Lett. A **358**, 256 (2006).
[12] C. Wang *et al.*, Opt. Commun. **253**, 15 (2005).
[13] H. Lee, J. Lim, and H. J. Yang, Phys. Rev. A **73**, 042305 (2006).
[14] X. R. Jin *et al.*, Phys. Lett. A **354**, 67 (2006).
[15] J. Wang *et al.*, Opt. Commun. **266**, 732 (2006).
[16] Y. Yeo and W. K. Chua, Phys. Rev. Lett. **96**, 060502 (2006).
[17] X. W. Wang and G. J. Yang, Phys. Rev. A **78**, 024301 (2008).
[18] Q. Y. Cai, Phys. Rev. Lett. **91**, 109801 (2003).
[19] F. G. Deng and G. L. Long, Phys. Rev. A **72**, 016302 (2005).
[20] R. L. Rivest, *Fast Software Encryption 97*, LNCS 1267 (Springer-Verlag, Berlin, 1997).
[21] H. Hoffmann *et al.*, Phys. Rev. A **72**, 016301 (2005).
[22] N. Gisin *et al.*, Rev. Mod. Phys. **74**, 145 (2002).