Int J Theor Phys (2010) 49: 2035–2044
DOI 10.1007/s10773-010-0387-1

Novel Quantum Deterministic Key Distribution Protocols with Entangled States

Nan-Run Zhou · Li-Jun Wang · Jie Ding · Li-Hua Gong · Xiang-Wu Zuo

Received: 29 January 2010 / Accepted: 19 May 2010 / Published online: 4 June 2010

Abstract By utilizing Bell states and GHZ states, two quantum deterministic key distribution (QDKD) protocols are presented to hand over the previously deterministic key to the intended receiver. The proposed QDKD protocols have two-way authentications, and then the eavesdropping and impersonation can be detected easily. The deterministic key itself is not transmitted over the channel and the receiver Bob infers his key in an indirect manner with the relationship between Alice's messages and his own measurement results, which guarantees the security of the deterministic key. Different from the quantum key distribution protocols yielding random keys, the proposed QDKD protocols can distribute the pre-deterministic keys securely, which are of great significance in the filed of key management.

Keywords Quantum deterministic key distribution · Entangled state · Key management · Quantum cryptography · Information security

1 Introduction

Perfectly secure communication between two legitimate parties can be achieved if they share beforehand a common sequence of bits, i.e., a key, which can be used to encrypt a message to be transmitted through a classical public channel, thus how to distribute the key securely is of importance for secure communication. However, the communicators Alice and Bob often need to exchange secret messages directly without any pre-shared private key or one usually needs to transmit information securely in a deterministic way. Quantum secure direct communication (QSDC) has been presented as a new solution to achieve these goals. In 2002, Beige et al. proposed a deterministic cryptographic scheme with single-photon two-qubit

N.-R. Zhou (✉) · L.-J. Wang · J. Ding · L.-H. Gong · X.-W. Zuo
Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China
e-mail: znr21@163.com

L.-J. Wang
e-mail: wlij85@163.com

states and showed how one could exploit the deterministic nature for direct secure communication [1]. Subsequently, Bostrom and Felbinger presented the "ping-pong protocol" with Einstein-Podolsky-Rosen (EPR) entangled pairs to allow the direct communication and to distribute the key in a deterministic manner that the sender Alice determined the bits and the receiver Bob decoded them [2]. The transmission efficiency of ping-pong protocol is much higher than that of nondeterministic protocols [3, 4]. Several alternative protocols tailored along the ping-pong protocol were proposed to improve the security [5–7]. Different from the ping-pong protocol, two deterministic secure direct communication protocols without using entanglement were presented respectively [6, 7], especially, in Ref. [7], the security for direct communication is analyzed in detail. Gao et al. presented a scheme based on entanglement swapping by using GHZ states for transmission of information from two parties to a common party [8]. Chen et al. proposed a double-entanglement-based quantum cryptography protocol that was both efficient and deterministic and the security of the protocol was based on Bell's theorem [9]. Man et al. proposed a new secure deterministic bidirectional communication protocol without using entanglement, where two legitimate users can simultaneously exchange their different secret messages in a direct way with a set of communication devices [10]. In 2008, Hwang et al. presented a deterministic BB84 protocol as deterministic secure quantum direct communication that not only inherited the unconditional security of the original BB84 protocol but also enabled the receiver to deterministically measure and decode all qubits from the sender [11]. Jiang et al. proposed two new deterministic secure quantum communication protocols by utilizing auxilians [12]. In 2009, without the need of photon storing technique, Dong et al. proposed a deterministic secure quantum communication against collective-dephasing noise by using EPR pairs and auxiliary photons [13]. There is another kind of QSDC protocols that verify the perfection of the channel and identify the communicators' identification before transmitting secret messages. In 2006, Lee et al. proposed two quantum direct communication protocols with user authentication, where Alice can directly send the secret message to Bob without any previously shared secret after authentication [14]. Yang et al. presented an efficient QSDC scheme with authentication based on quantum entanglement and polarized single photons [15], where EPR pairs were used to transmit secret messages and the polarized single photons were used for authentication and eavesdropping detection. Wang et al. proposed two QSDC schemes by combining ideas of user authentication and direct communication with dense coding [16]. Liu et al. presented two efficient quantum direct communication protocols with authentication, which can be generalized to multiparty quantum direction communication [17]. Yen et al. presented a communication protocol capable of achieving secure quantum direct communication with mutual authentication by exploiting the entanglement swapping and local unitary operations [18]. Han et al. proposed a deterministic QSDC protocol by exploiting dense coding and continuous variable operations, where two photon sequences are used to check the security of the channels and the continuous variable operations are performed on the travel photons to enhance the security [19].

With QSDC, the communicators Alice and Bob can exchange secret messages directly without firstly generating a private key and then encrypting the secret messages and sending to the other party through another classical communication. Moreover, the above-mentioned protocols can achieve secure deterministic direct communication and the multitask aspect gained from determinism: in principle, Alice can transmit either a meaningless random string of symbols, performing a quantum key distribution (QKD), or a meaningful one, like the message itself, performing a direct communication. However, except for the QSDC protocols based on authenticated quantum or classical channels [14–19], the other QSDC protocols used for transmitting secret keys are not secure enough and the information can be more or less obtained by the eavesdropper.

In real-life applications, one usually needs to transmit a previously deterministic secret or key to the intended receiver securely, e.g., if the key to a locked secret is destroyed, one needs a same copy of the deterministic key to decrypt the secret. The deterministic key as the secret message can be directly transmitted via QSDC to the specified receiver. However, the sender Alice needs to send the travel qubit back to the receiver Bob, thus some information about the deterministic key will inevitably leak to the eavesdropper Eve and Eve may reproduce the deterministic key according to the information obtained by monitoring the channel. That is to say, QSDC protocols are not suitable to distribute the pre-deterministic key, where the intrinsically deterministic characteristic does not contribute to security but efficiency of the protocols. Without utilizing entanglement, Eusebi and Mancini presented an extension to a d-ary alphabet of a deterministic quantum key distribution protocol and showed that the security of the protocol was maximal for $d = 3$ [20]. In the year of 2010, we proposed two quantum deterministic key distribution (QDKD) protocols to hand over the pre-deterministic key to the specific target by exploiting the authenticated quantum entangled channel with detailed security analyses, which can also be used as a secure identification protocol since usually identity information is also a deterministic secret string [21]. The goal of the QDKD protocols is distinguished from that of the existing QKD protocols only generating a random secret sequence of bits, where no one, including the sender and the receiver, knows the ultimate key until the QKD protocol runs over. In this paper, we present two novel QDKD protocols with entangled states. To guarantee the security of the deterministic key, the communication channel and the communicators are authenticated before key distribution.

This work is organized as follows. Two QDKD protocols are presented in Sect. 2. In Sect. 3, the security and efficiency of the proposed QDKD protocols are analyzed in detail and a brief conclusion is drawn in Sect. 4.

2 QDKD Protocols with Entangled States

Task: Alice needs to transmit a pre-deterministic key string to the specified receiver Bob securely.

2.1 QDKD Protocol with Bell States

Suppose the used Bell states are in $|\phi^+\rangle_{A_iB_i} = \frac{1}{\sqrt{2}}(|0\rangle_{A_i}|0\rangle_{B_i} + |1\rangle_{A_i}|1\rangle_{B_i})$ and $|\psi^+\rangle_{A_iB_i} = \frac{1}{\sqrt{2}}(|0\rangle_{A_i}|1\rangle_{B_i} + |1\rangle_{A_i}|0\rangle_{B_i})$, where $i = 1, 2, \ldots, n+2m+r$. The QDKD protocol with these Bell states consists of the following steps:

(1) Alice prepares $2m+n+r$ EPR correlation pairs randomly in quantum states $|\phi^+\rangle_{A_iB_i}$ and $|\psi^+\rangle_{A_iB_i}$ represented by the number 0 and 1, respectively, and then sends photon B_i to Bob and reserves photon A_i.
(2) On receiving the photons, Bob returns an acknowledgment to Alice with the number of the received photons.
(3) If the number of the received photons acknowledged by Bob is $2m+n+r$, Alice goes to the next step; or else Alice terminates the QDKD protocol.
(4) Alice chooses m photons randomly and measures them with random measurement bases, and then announces the positions/orders of the m photons, the number of their corresponding entangled states, measurement results and measurement bases.

Table 1 Key relationship in the QDKD protocol with Bell states

k_{A_i}	A_i	Alice tells Bob	B_i	Bob's bit	Bit flipping?	k_{B_i}
0	0	00	0	0	no	0
	1	10	1			
0	0	01	1	1	yes	0
	1	11	0			
1	0	10	0	1	no	1
	1	00	1			
1	0	11	1	0	yes	1
	1	01	0			

(5) Bob measures his counterpart with the same measurement bases as Alice and compares them with Alice's results. If the results are same or lightly away from each other, then Bob trusts the channel and Alice. Note that if the numbering bit received by Bob is 1, Bob flips his information bit, or else doesn't.
(6) Bob chooses m photons randomly from the rest $m+n+r$ photons and measures them with random measurement bases, and then announces the positions/orders of the m photons, their corresponding measurement results and measurement bases.
(7) Alice measures her counterpart with the same measurement bases as Bob and flips her resulting bit if the number of the entangled state is 1, and then compares them with Bob's results. If the results are same or lightly away from each other, Alice trusts the channel and Bob.
(8) Alice and Bob perform entanglement purification operation and obtain n entangled states from the rest $n+r$ Bell states.
(9) Alice measures her own n photons and tells Bob the measurement bases, the number of the corresponding entangled states and whether the resulting bit A_i is the same with the deterministic key bit k_{A_i} or not.
(10) Bob measures his own n photons with the same measurement bases as Alice and infers his key k_{B_i} with the relationship between Alice's messages and his own measurement results in Table 1. In Table 1, we suppose Alice and Bob choose the measurement bases $\{|0\rangle, |1\rangle\}$, which does not loss generality and impact the security. If Alice and Bob choose the measurement bases $\{|+\rangle, |-\rangle\}$, they appoint that $|+\rangle$ and $|-\rangle$ correspond to key bits 0 and 1, respectively. The first bit Alice tells Bob is $k_{A_i} \oplus A_i$, where 0 and 1 denote information "same" and "different", respectively. While the second one Alice tells Bob is the number of the corresponding entangled state.

In the QDKD protocol, $2m$ EPR pairs are used to detect the eavesdropping and identify the communicators, i.e., to guarantee the security of the channel; $n+r$ EPR pairs are used to purify n EPR pairs, i.e., to guarantee the stability of the channel; n EPR pairs are used to hand over the n bits deterministic key string.

2.2 QDKD Protocol with GHZ States

The above QDKD protocol with Bell states requires more classical communications. Motivated by this, we will modify the QDKD protocol with Bell states by employing Greenberger-Horne-Zeilinger (GHZ) states, and the modified QDKD protocol is as follows.

(1) Alice prepares $2m + n + r$ GHZ states $|\phi\rangle_{A_i B_{i_1} B_{i_2}} = \frac{1}{\sqrt{2}}(|0\rangle_{A_i}|1\rangle_{B_{i_1}}|0\rangle_{B_{i_2}} + |1\rangle_{A_i}|0\rangle_{B_{i_1}}|1\rangle_{B_{i_2}})$, and then sends photons B_{i_1} and B_{i_2} to Bob and reserves photon A_i, where $i = i_1 = i_2 = 1, 2, \ldots, n + 2m + r$.
(2) On receiving the photons, Bob returns an acknowledgment to Alice with the pairs of the received photons.
(3) If the pairs of the received photons acknowledged by Bob are $2m + n + r$, Alice goes to the next step; or else Alice terminates the protocol.
(4) Alice chooses m photons randomly and measures them with random measurement bases, and then announces the positions/orders of the m photons and their corresponding measurement results.
(5) Bob makes single photon measurements for his entangled pair (B_{i_1}, B_{i_2}) corresponding to Alice's photon A_i using computational bases $(|0\rangle, |1\rangle)$ and compares them with Alice's results. If the results are same or lightly away from each other, Bob trusts the channel and Alice.

Note that If Alice's measurement result is 0 (1), Bob's measurement results should be 10 (01). Alice and Bob appoint that above two correspondences represent information "same" and others represent information "different".
(6) Bob chooses m pairs of photons randomly from the rest $m + n + r$ pairs of photons and makes single photon measurements with computational bases $(|0\rangle, |1\rangle)$, and then announces the positions/orders of the m pairs of photons and their corresponding measurement results.
(7) Alice measures her counterparts with random measurement bases and compares them with Bob's results. If the results are the same as or lightly away from each other, Alice trusts the channel and Bob.
(8) Alice and Bob perform entanglement purification operation and obtain n GHZ states from the rest $n + r$ GHZ states.
(9) Alice measures her own n photons and tells Bob the resulting bit A_i is the same as or different from the deterministic key bit k_{A_i}.
(10) Bob measures his own n pairs of photons with Bell bases and infers his key k_{B_i} according to the relationship between Alice's messages and his own measurement results in Table 2. In Table 2, the bit 0 (1) Alice tells Bob represents information "same (different)". Furthermore, if Bob receives information "different" over the classical channel, he flips each of the corresponding resulting bits B_i to obtain his key k_{B_i}.

Note that the QDKD protocol with GHZ states is only suitable to transmit the key 01 or 10, while the key 00 and 11 can't be transmitted directly. Thus, Alice needs to take measures to deal with the key prior to the transmission, for instance, the bit 0 can be inserted into the middle of two key bits 11, i.e., $11 \rightarrow 101$ and the bit 1 can be inserted into the middle of two key bits 00, i.e., $00 \rightarrow 010$. Thus, three bits 101 can be divided into two parts: 10 and 1, and then the bits 10 are transmitted to Bob and the corresponding position of such an inserted bit 0 should be recorded, while the key bit 1 together with the next key bit will be transmitted to Bob as described in the QDKD protocol with GHZ states. Likewise, three bits 010 can be also transmitted to Bob and the corresponding position of the inserted bit 1 should be recorded. After the deterministic key is handed over to Bob, Alice tells Bob which bits are not the key bits, and then Bob deletes the inserted bits at the corresponding positions. After the above-mentioned operations, Bob can obtain the key bits 00 and 11.

It is easily known that the modified protocol with GHZ states requires less classical communications than the QDKD protocol with Bell states. Moreover, the QDKD protocol with Bell states only transmits 1 key bit with two entangled photons, while the modified

Table 2 Key relationship in the QDKD protocol with GHZ states

k_{A_i}		A_i	Alice tells Bob	B_i	k_{B_i}	
10		0	0	10	10	
		1	1	01		
01		0	1	10	01	
		1	0	01		
	10	0	0	10	10	
11→ 101		1	1	01		101→ 11
00→ 010	01	0	1	10	01	010→ 00
		1	0	01		

protocol transmits 2 key bits by employing three entangled photons once. Compared with the QDKD protocol with Bell states, the modified protocol with GHZ states saves the precious quantum resources.

3 Analyses of QDKD Protocols

3.1 Security Analysis

The security of the proposed QDKD protocols is the most important aspect. Here, we mainly analyze the QDKD protocol with Bell states. An eavesdropper Eve cannot have access to Alice's photons, so all her operations are restricted to the transmitted photons Alice sends to Bob. While they are useless before Alice measures her own photons with random measurement bases, because the photons have no information with the key prior to the measurement. The QDKD protocol is realized by utilizing the entangled states $|\phi^+\rangle_{A_iB_i}$ and $|\psi^+\rangle_{A_iB_i}$ simultaneously, thus the uncertainty of information increases, and Eve also doesn't know which measurement basis is chosen by Alice and Bob in the process of transmitting the key information, so the difficulty of eavesdropping enlarges.

For one-way quantum communication, there are two main eavesdropping means. One is intercept and resend attack and the other is entanglement attack. As to intercept and resend attack, when Alice sends the photon B_i to Bob, Eve may intercept this photon. The state of photon B_i intended for Bob is

$$\rho_{B_i} = \mathrm{Tr}_{A_i}\rho_{|\phi^+\rangle_{A_iB_i}} = \mathrm{Tr}_{A_i}\rho_{|\psi^+\rangle_{A_iB_i}} = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|), \tag{1}$$

where $i = 1, 2, \ldots, n + 2m + r$. From (1), it is easy to see that Eve can not obtain any information by this way even if the intercepted photon has been measured by Eve. Suppose Eve resends a fake particle in the state $|\varphi\rangle_E = \alpha|0\rangle + \beta|1\rangle$ ($|\alpha|^2 + |\beta|^2 = 1$) to Bob, which has no correlation with Alice's photon A_i. After receiving this fake particle, Bob measures it with random measurement basis and obtains the measurement result 0 (1) with probability $|\alpha|^2$ ($|\beta|^2$). Thus, the error rate is very easy to exceed the threshold, so Alice and Bob abort this round communication.

It is more clear to see that Eve can be easily detected by studying the mutual information [22] defined as

$$I(X;Y) = H(X) - H(X|Y), \tag{2}$$

where the Shannon entropy $H(X) = -\sum_i p(x_i)\log_2 p(x_i)$ is the function of the probability $p(x_i)$ of all possible values of X, and the sum is over those i with $p(x_i) > 0$. The expected entropy $H(X|Y)$ of X given the value of Y is expressed as

$$H(X|Y) = \sum_j p(y_j)\left[-\sum_i p(x_i|y_j)\log_2 p(x_i|y_j)\right]. \tag{3}$$

Since the key is transmitted by employing the maximum entangled states, in which each photon is in the completely mixed state, i.e., $\rho_{A_i} = \rho_{B_i} = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) = \frac{I}{2}$, thus the von Neumann entropy is

$$S(\rho_{A_i}) = S(\rho_{B_i}) = -\mathrm{tr}\left(\frac{I}{2}\log\frac{I}{2}\right) = 1 \text{ (bits/symbol)}. \tag{4}$$

While the mutual information between Alice and Bob is determined by the Holevo bound

$$I(X;Y) \le S(\rho) - \sum_i p_i S(\rho_i), \tag{5}$$

where $\rho = \sum_i p_i\rho_i$. In the proposed QDKD protocol, the used entangled states are all pure states, hence, $I(X;Y) \le S(\rho) = 1$ (bits/symbol). If there is no eavesdropping, the maximum mutual information $I(A;B)$ between Alice and Bob is 1 bits/symbol. However, if the eavesdropper Eve exists, $I(A;B) = 0$, while the mutual information between Alice (Bob) and Eve is $I(A;E) = 1$ ($I(B;E) = 1$) bits/symbol. Thus it is easy for Alice and Bob to detect Eve's intercept and resend attack.

For entanglement attack strategy, Eve prepares $2m + n + r$ EPR pairs in the states $|\phi^+\rangle_{C_iD_i} = \frac{1}{\sqrt{2}}(|0\rangle_{C_i}|0\rangle_{D_i} + |1\rangle_{C_i}|1\rangle_{D_i})$, $i = 1, 2, \ldots, 2m+n+r$. Eve monitors the channel and intercepts the photon B_i intended for Bob, and then performs Bell bases joint measurement on the photons B_i and C_i, thus the entanglement system of photon pairs (A_i, B_i) and (C_i, D_i) is

$$\begin{aligned}
|\psi\rangle_{A_iB_iC_iD_i} &= |\phi^+\rangle_{A_iB_i}\otimes|\phi^+\rangle_{C_iD_i}\\
&= \frac{1}{\sqrt{2}}(|0\rangle_{A_i}|0\rangle_{B_i} + |1\rangle_{A_i}|1\rangle_{B_i})\otimes\frac{1}{\sqrt{2}}(|0\rangle_{C_i}|0\rangle_{D_i} + |1\rangle_{C_i}|1\rangle_{D_i})\\
&= \frac{1}{2}[|\phi^+\rangle_{A_iD_i}|\phi^+\rangle_{B_iC_i} + |\phi^-\rangle_{A_iD_i}|\phi^-\rangle_{B_iC_i} + |\psi^+\rangle_{A_iD_i}|\psi^+\rangle_{B_iC_i}\\
&\quad + |\psi^-\rangle_{A_iD_i}|\psi^-\rangle_{B_iC_i}]
\end{aligned} \tag{6}$$

or

$$\begin{aligned}
|\psi'\rangle_{A_iB_iC_iD_i} &= |\psi^+\rangle_{A_iB_i}\otimes|\phi^+\rangle_{C_iD_i}\\
&= \frac{1}{\sqrt{2}}(|0\rangle_{A_i}|1\rangle_{B_i} + |1\rangle_{A_i}|0\rangle_{B_i})\otimes\frac{1}{\sqrt{2}}(|0\rangle_{C_i}|0\rangle_{D_i} + |1\rangle_{C_i}|1\rangle_{D_i})\\
&= \frac{1}{2}[|\phi^+\rangle_{A_iD_i}|\psi^+\rangle_{B_iC_i} - |\phi^-\rangle_{A_iD_i}|\psi^-\rangle_{B_iC_i} + |\psi^+\rangle_{A_iD_i}|\phi^+\rangle_{B_iC_i}\\
&\quad - |\psi^-\rangle_{A_iD_i}|\phi^-\rangle_{B_iC_i}].
\end{aligned} \tag{7}$$

Eve sends the photon D_i to Bob. From (6), it is clearly known that Eve can infer which entangled state the photons A_i and D_i are in with her measurement results $|\phi^{\pm}\rangle_{B_iC_i}$ and $|\psi^{\pm}\rangle_{B_iC_i}$, while it is impossible for Eve to infer the state of photon pair (A_i, D_i) from (7). However, there are no correlations between the key and EPR pairs before the key is transmitted, so Eve can not obtain any information on the deterministic key. Moreover, this entanglement attack can be detected. From (6) and (7), it is easily known that the photons A_i and B_i are disentangled due to Eve's operations on the photons B_i and C_i. Thus, Alice's photon A_i and Bob's photon D_i are in the states $|\phi^{+}\rangle_{A_iD_i}$, $|\phi^{-}\rangle_{A_iD_i}$, $|\psi^{+}\rangle_{A_iD_i}$ and $|\psi^{-}\rangle_{A_iD_i}$ with probability 1/4, respectively. If the photon pair (A_i, D_i) is in the state $|\phi^{\pm}\rangle_{A_iD_i}$ and Alice and Bob measure their own photons with the same measurement bases, their measurement results are necessarily same. If the photon pair (A_i, D_i) is in the state $|\psi^{\pm}\rangle_{A_iD_i}$ and is measured with the same measurement bases, Alice's measurement results are different from Bob's. The states $|\phi^{\pm}\rangle_{A_iD_i}$ and $|\psi^{\pm}\rangle_{A_iD_i}$ are obtained with probability 1/2, respectively, so Alice's and Bob's corresponding measurement results are same or different with probability 1/2 respectively after Alice and Bob measure their own photons with the same measurement bases. In the QDKD process, Alice and Bob use $2m$ EPR pairs to detect the eavesdropping and identify the communicators, thus the probability of Eve being detected is $p_1 = \frac{1}{2} \times 1 + \frac{1}{2} \times [1 - (\frac{1}{2})^m] = 1 - (\frac{1}{2})^{m+1}$ if the rate of the states $|\psi^{+}\rangle_{A_iB_i}$ and $|\phi^{+}\rangle_{A_iB_i}$ is 1. When the rate of two states is up to 3, Eve can be detected with probability $p_2 = \frac{3}{4} \times 1 + \frac{1}{4} \times [1 - (\frac{1}{2})^m] = 1 - (\frac{1}{2})^{m+2}$. Thus, under the condition that Eve performs the entanglement attack by exploiting the state $|\phi^{+}\rangle_{C_iD_i} = \frac{1}{\sqrt{2}}(|0\rangle_{C_i}|0\rangle_{D_i} + |1\rangle_{C_i}|1\rangle_{D_i})$, the larger the rate of the states $|\psi^{+}\rangle_{A_iB_i}$ and $|\phi^{+}\rangle_{A_iB_i}$ is, the easier the eavesdropping detection is. So Eve can be detected with high probability when m is big enough. Suppose that the rate of the states $|\psi^{+}\rangle_{A_iB_i}$ and $|\phi^{+}\rangle_{A_iB_i}$ is 1 in the QDKD protocol and there is no eavesdropping, the maximum mutual information $I(A; B)$ is 1 bits/symbol. However, if Eve exists, the mutual information between Alice and Bob is

$$\begin{aligned} I(A; B) &= -\left[1 - \left(\frac{1}{2}\right)^{m+1}\right] \log_2 \left[1 - \left(\frac{1}{2}\right)^{m+1}\right] - \left(\frac{1}{2}\right)^{m+1} \log_2 \left(\frac{1}{2}\right)^{m+1} \\ &= -\left(1 - \frac{1}{2^{m+1}}\right) \log_2 \left(1 - \frac{1}{2^{m+1}}\right) + \frac{m+1}{2^{m+1}}. \end{aligned} \tag{8}$$

From (8), it is easily known that as the value of m increases, the mutual information $I(A; B)$ gradually decreases. If $m \to \infty$, $I(A; B) \to 0$. While the mutual information $I(A; E) = I(B; E) = 1$. Thus Alice and Bob can check Eve's entanglement attack.

In summary, it is clear to see that the proposed QDKD protocol with Bell states is secure. One can analyze the security of the QDKD protocol with GHZ states in a similar way.

3.2 Efficiency Analysis

Unlike the BB84 protocol [3] or the EPR protocol [4], where at most half of the particles or EPR pairs are used to yield key bits, in our proposed QDKD protocols, all of the EPR pairs except those for eavesdropping detection are used to transmit the pre-deterministic key bits to the receiver Bob. We now calculate and compare the efficiency of the two QDKD protocols. According to Ref. [22], the information-theoretical efficiency of a QKD protocol is defined as

$$\eta = \frac{b_s}{q_t + b_t}, \tag{9}$$

where b_s is the expected number of secret bits received by Bob, q_t is the number of qubits transmitted through the quantum channel, and b_t is the number of classical bits exchanged over the public channel between Alice and Bob. In the QDKD protocol with Bell states, transmitting one deterministic key bit to the receiver Bob needs to send one qubit and two classical bits, i.e., $b_s = 1$, $q_t = 1$, $b_t = 2$, if neglecting the classical bits used for eavesdropping detection. Thus, the efficiency of the QDKD protocol with Bell states is $\eta_1 = 33.3\%$.

Assume that the probability of the key bits 00 and 11 among the deterministic key bits in the QDKD protocol with GHZ states is 0.5. If the key bits 01 or 10 are transmitted to Bob, two qubits and one classical bit need to be transmitted to Bob simultaneously. It is shown that $b'_s = 2$, $q'_t = 2$, $b'_t = 1$ and the efficiency is $\eta' = 66.7\%$. However, if the key bits transmitted by Alice are 00 or 11, such key bits need to be dealt with as described in Sect. 2.2 before key distribution. After deterministic key distribution, Bob deletes the inserted bits at the corresponding positions. It is easily obtained that $b''_s = 2$, $q''_t = 3$, $b''_t = 1.5$ and the efficiency is $\eta'' = 44.4\%$ if the key bits are 00 or 11. Therefore, the average efficiency of the QDKD protocol with GHZ states is $\eta_2 = 55.6\%$, and then $\eta_2 > \eta_1$. Namely, the efficiency of the QDKD protocol with GHZ states is higher than that of the QDKD protocol with Bell states.

4 Conclusion

By exploiting quantum entangled states, i.e., Bell states and GHZ states, we present two QDKD protocols to transmit the deterministic key with detailed security analyses. Although the pre-deterministic key as the secret message can be directly transmitted with QSDC to the specified receiver, the deterministic key itself is not secure enough during transmission. While in the proposed QDKD protocols, the communicators' identities and the communication channel have been authenticated before transmitting the deterministic key, thus, the information about the deterministic key does not leak to any third party in our proposed QDKD protocols. It is proven that the proposed QDKD protocols can hand over the previously deterministic key to the specified target securely, which are distinguished from the typical quantum key distribution protocols that can only produce random keys. Furthermore, the proposed QDKD protocols are of great significance in the field of key management, since random key and deterministic key are equally significant in cryptography. When the random key previously preserved is lost, a new round distribution of the random key owes to QDKD. Especially, when the key to a locked secret is destroyed or lost, one needs to obtain a same copy of the deterministic key. To achieve this goal, one can usually encrypt the deterministic key with another secure key and transmit its ciphertext to the receiver, and the receiver decrypts the received ciphertext. This means is equal to QDKD protocols if there exist an unconditionally secure key and a secure and effective encryption algorithm [23, 24]. However, our proposed QDKD protocols can transmit the pre-deterministic key without the needs of a prior established key and the encryption/decryption algorithm.

Acknowledgements The work is supported by the National Natural Science Foundation of China (Grant No. 10647133), the Natural Science Foundation of Jiangxi Province, China (Grant Nos. 2007GQS1906 and 2009GQS0080), the Research Foundation of the Education Department of Jiangxi Province (Grant No. [2007]22), and the Scientific Research Start-up Foundation for the Recruitment Talent of Nanchang University of China.

References

1. Beige, A., Englert, B.G., Kurtsiefer, C., Weinfurter, H.: J. Phys. A, Math. Gen. **35**, 407 (2002)

2. Bostrom, K., Felbinger, T.: Phys. Rev. Lett. **89**, 187902 (2002)
3. Bennett, C.H., Brassard, G.: In: Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, pp. 175–179. IEEE Press, New York (1984)
4. Ekert, A.K.: Phys. Rev. Lett. **67**, 661 (1991)
5. Deng, F.G., Long, G.L.: Phys. Rev. A **69**, 052319 (2004)
6. Cai, Q.Y., Li, B.W.: Chin. Phys. Lett. **21**, 601 (2004)
7. Lucamarini, M., Mancini, S.: Phys. Rev. Lett. **94**, 140501 (2005)
8. Gao, T., Yan, F.L., Wang, Z.X.: J. Phys. A, Math. Gen. **38**, 5761 (2005)
9. Chen, Z.B., Zhang, Q., Bao, X.H., Schmiedmayer, J., Pan, J.W.: Phys. Rev. A **73**, 050302 (2006)
10. Man, Z.X., Xia, Y.J., Zhang, Z.J.: Int. J. Quantum Inf. **4**, 739 (2006)
11. Hwang, T., Li, C.M., Lee, N.Y.: Int. J. Mod. Phys. C **19**, 625 (2008)
12. Jiang, H.J., Cao, W.Z., Li, C.: Int. J. Quantum Inf. **6**, 493 (2008)
13. Dong, L., Xiu, X.M., Gao, Y.J., Chi, F.: Opt. Commun. **282**, 1688 (2009)
14. Lee, H., Lim, J., Yang, H.: Phys. Rev. A **73**, 042305 (2006)
15. Yang, Y.G., Wen, Q.Y., Zhu, F.C.: Chin. Phys. **16**, 1838 (2007)
16. Wang, M.J., Pan, W.: Chin. Phys. Lett. **25**, 3860 (2008)
17. Liu, W.J., Chen, H.W., Li, Z.Q., Liu, Z.H.: Chin. Phys. Lett. **25**, 2354 (2008)
18. Yen, C.A., Horng, S.J., Goan, H.S., Kao, T.W., Chou, Y.H.: Quantum Inf. Comput. **9**, 376 (2009)
19. Han, L.F., Chen, Y.M., Yuan, H.: Commun. Theor. Phys. **51**, 648 (2009)
20. Eusebi, A., Mancini, S.: Quantum Inf. Comput. **9**, 950 (2009)
21. Zhou, N.R., Wang, L.J., Ding, J., Gong, L.H.: Phys. Scr. **81**, 045009 (2010)
22. Cabello, A.: Phys. Rev. Lett. **85**, 5635 (2000)
23. Zhou, N.R., Liu, Y., Zeng, G.H., Xiong, J., Zhu, F.C.: Physica A **375**, 693 (2007)
24. Zhou, N.R., Zeng, G.H., Nie, Y.Y., Xiong, J., Zhu, F.C.: Physica A **362**, 305 (2006)