Quantum secret sharing using product states

Li-Yi Hsu*
Department of Physics, Chung Yuan Christian University, Chung-Li, 32023, Taiwan, Republic of China

Che-Ming Li
Institute and Department of Electrophysics, National Chiao Tung University, Hsinchu 30050, Taiwan, Republic of China
(Received 19 June 2003; revised manuscript received 28 May 2004; published 28 February 2005)

This study proposes quantum secret sharing protocols using product states. The first two protocols adopt the quantum key distribution protocol using product states [Guo *et al.*Phys. Rev. A **64**, 042301 (2001)]. In these two protocols, the sender does not reveal any information about the qutrits until confirming that each receiver has received a qutrit. This study also considers the security and some possible eavesdropping strategies. In the third proposed protocol, three-level Bell states are exploited for qutrit preparation via nonlocality swapping.

DOI: 10.1103/PhysRevA.71.022321 PACS number(s): 03.67.Dd, 03.67.Hk

I. INTRODUCTION

The problem of secret sharing is as follows. Alice, the president of a bank, wants to give access to a vault to two vice presidents, Bob and Charlie. Alice knows that one of them, and only one, may be dishonest and she does not know who is the honest one. Nevertheless, any classical secret sharing cannot prevent an eavesdropper with unlimited power from accessing secret bits. On the other hand, it is believed that secret communication using quantum bits can be absolutely secure. In quantum physics, one cannot take a measurement without perturbing the system. That is, an eavesdropper cannot access full information without being detected in quantum secret communication. Recently, people have become interested in quantum secret sharing. Hillery *et al.* introduced the quantum secret sharing protocol using Greenberger-Horne-Zeilinger (GHZ) states [1]. Moreover, Koashi and Imoto considered the correlation of the two-qubit Bell state in their quantum secret sharing scheme [2]. Karimipour *et al.* then proposed *d*-level secret sharing via entanglement swapping [3]. Furthermore, Cabellos suggested a quantum secret sharing scheme using entanglement swapping between three-qubit GHZ states and two-qubit Bell states [4]. Also, Bagherinezhad and Karimipour introduced the protocol for quantum secret sharing based on the reusable GHZ states as secure carriers [5]. In addition, Hillery and Mimih considered quantum secret sharing with restricted classical communication [6]. Nevertheless, the above quantum secret sharing protocols cannot be implemented without entangled states.

This study proposes some quantum secret sharing protocols using product states. The obvious advantage of the first two proposed protocols is that there is no need to prepare any entanglement. In quantum cryptography, the nonorthogonality of the state vectors is exploited to detect any possible eavesdropping. For example, using the BB84 or B92 protocols, quantum key distribution can be performed without entanglement [7,8]. Therefore, performing quantum secret sharing using product states is possible. Notably, Guo *et al.* considered quantum key distribution using the orthogonal product states [9,10]. In the protocol of Guo *et al.*, the sender has to prepare one of the two-qutrit bases in a complete set $\{|\psi_l\rangle\}$:

$$
\begin{aligned}
&|\alpha_i\rangle\ |\beta_i\rangle\\
&|\psi_1\rangle = |1\rangle\ |0\rangle,\\
&|\psi_2\rangle = |0\rangle\ \frac{1}{\sqrt{2}}(|0\rangle + |2\rangle),\\
&|\psi_3\rangle = |0\rangle\ \frac{1}{\sqrt{2}}(|0\rangle - |2\rangle),\\
&|\psi_4\rangle = |2\rangle\ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),\\
&|\psi_5\rangle = |2\rangle\ \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle),\\
&|\psi_6\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\ |1\rangle,\\
&|\psi_7\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\ |1\rangle,\\
&|\psi_8\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle)\ |2\rangle,\\
&|\psi_9\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle)\ |2\rangle. \qquad (1)
\end{aligned}
$$

This study writes the Hilbert space of the bipartite complete set basis as $H_A \otimes H_B$. That is, every $|\psi_l\rangle$ with state index l can be written as $|\alpha_l\rangle \otimes |\beta_l\rangle$, where $|\alpha_l\rangle \in H_A$ and $|\beta_l\rangle \in H_B$, respectively. Bennett *et al.* proved that full information of an

*Electronic address: lyhsu@phys.cts.nthu.edu.tw

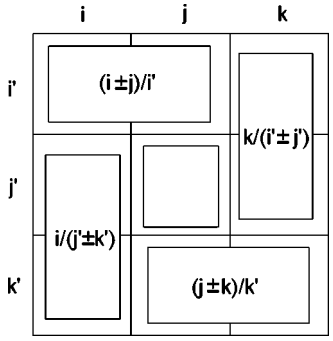

FIG. 1. The complete set $((i,j,k),(i',j',k'))$. The complete set $\{|\psi_l\rangle\}$ can represented as **(**(0, 1, 2),(1, 0, 2)**)**. There are two horizontal dominos and two vertical dominos. For example, the horizontal domino $(i \pm j)/i'$ represents two states $(1/\sqrt{2})(|i\rangle+|j\rangle)\otimes|i'\rangle$ and $(1/\sqrt{2})(|i\rangle-|j\rangle)\otimes|i'\rangle$; the vertical domino $k/(i' \pm j')$. This domino represents two states $(1/\sqrt{2})|k\rangle\otimes(|i'\rangle+|j'\rangle)$ and $(1/\sqrt{2})|k\rangle\otimes(|i'\rangle - |j'\rangle)$.

unknown $|\psi_l\rangle$ is inaccessible via local operations and classical communication unless the specific joint measurement is performed [11]. Hence, the nonlocality without entanglement is embedded in the complete set $\{|\psi_i\rangle\}$ [11]. These nonlocal complete sets of product states are graphically illustrated in Fig. 1. In addition, as shown in Fig. 1, indices i, j, k, i', j', and k' can be rearranged as different nonlocal complete sets. This study denotes the nonlocal complete sets as that in Fig. 1 by $((i,j,k),(i',j',k'))$. For example, the complete set $\{|\psi_l\rangle\}$ can be denoted as **(**(0, 1, 2),(1, 0, 2)**)**. It is easy to verify that $((i,j,k),(i',j',k'))$ and $((k,j,i),(k',j',i'))$ indicate the same complete set. Consequently, in the three-level two-partite system, 18 complete sets of product states possess nonlocality without entanglement.

It is noteworthy to examine the complete set $((i,j,k),(i',j',k'))$. Figure 1 contains four rectangular dominos: two horizontal dominos and two vertical dominos. The two horizontal dominos in Fig. 1 are denoted by $(i \pm j)/i'$ and $(j \pm k)/k'$, respectively. Similarly, the two vertical dominos in Fig. 1 are denoted by $i/(j' \pm k')$ and $k/(i' \pm j')$, respectively. Obviously, these 18 nonlocal complete sets contain nine different horizontal dominos and nine different vertical dominos. In addition, the nonlocality in the complete set $((k,j,i),(k',j',i'))$ is preserved even if the $|j\rangle\otimes|j'\rangle$ state is excluded [11]. In this study, the sender never sends states of the $|j\rangle\otimes|j'\rangle$ kind. That is, the sender always sends some state lying in some horizontal or vertical domino.

However, if the two distant parties know the order of the local measurements, then both can access full information via local operations and classical communication. For instance, the unknown state is one of the bases in the nonlocal complete set $((i,j,k),(i',j',k'))$ and, moreover, the unknown state is known to lie in one of the horizontal dominos. To distinguish the unknown state, at first, the local measurement is performed on the Hilbert space H_B in the basis $\{|0\rangle, |1\rangle, |2\rangle\}$. The conditioned local measurement then can be performed on the Hilbert space H_A. If the outcomes of the measurement on H_B are $|i'\rangle$ and $|k'\rangle$, the conditioned local measurements are then to be performed in the basis $\{|i\rangle+|j\rangle, |i\rangle - |j\rangle, |k\rangle\}$ and $\{|j\rangle+|k\rangle, |j\rangle-|k\rangle, |i\rangle\}$, respectively. This approach is now accessible to full information via local operations and classical communication. In other words, nonlocality is embedded in the unknown *order* of the local measurements. That is, since whether an unknown state lies in a horizontal domino or a vertical domino is unknown, the correct order of local measurements cannot still be known.

This study proposes three quantum secret sharing protocols. The first two proposed protocols are based on these nonlocal complete sets. Reviewing the quantum key distribution protocol of Guo *et al.* is helpful. The protocol is as follows [10]: (1) The sender, Alice, sends the receiver, Bob, one qutrit of a basis state in the complete set $\{|\psi_l\rangle\}$. (2) After receiving the qutrit, Bob informs Alice, via classical communication, that he has received the qutrit. (3) Alice sends the other qutrit. (4) Bob performs the measurement in the $\{|\psi_l\rangle\}$ basis. The key feature of this protocol is that Alice does not send the second qutrit before ensuring that Bob has received the first qutrit. Thus, Eve, the eavesdropper, is incapable of performing any joint measurement on the two sent qutrits without being detected. However, this protocol implicitly assumes that the sending order is always the same. For example, Alice and Bob both preagree that Alice *always* sends $|\alpha_l\rangle \in H_A$ in step (1) and then sends $|\beta_l\rangle \in H_B$ in step (3). If the Hilbert space of the $\{|\psi_l\rangle\}$ basis is permuted, the complete set **(**(0, 1, 2),(1, 0, 2)**)** becomes another different complete set **(**(2, 0, 1),(0, 1, 2)**)** and vice versa. Thus, the protocol of Guo *et al.* is modified as follows. Alice randomly exchanges the sending order in steps (1) and (3). As a result, in step (4), Bob does not know that the first received qutrit is $|\alpha_l\rangle$ or $|\beta_l\rangle$. Bob performs his joint measurement randomly in the basis of the complete set either **(**(0, 1, 2),(1, 0, 2)**)** or **(**(2, 0, 1),(0, 1, 2)**)**. In the next step, Bob must tell Alice his measurement basis via classical communication. Alice then informs Bob which outcomes are to be disregarded via classical communication. Significantly, Alice and Bob consider the permutation effect of the Hilbert spaces. This modified protocol is now adaptable to be used in quantum secret sharing. In the quantum secret sharing protocol of Hillery *et al.* or Koashi and Imoto, the three-qubit GHZ states or two-qubit Bell states are invariant under the permutation of Hilbert space. In effect, the eavesdropper does not have to consider the effect of the permutation of Hilbert space. However, such an effect is the advantage of the proposed protocol to prevent successful cheating.

This paper is organized as follows. Section II considers the effect of the permutation of Hilbert space using a simpler protocol. Section III then explores another protocol, which is the generalization of the protocol in Sec. II. Section IV analyzes the security and investigates some possible eavesdropping strategies on the protocols I and II. Section V discusses the third protocol based on nonlocality swapping. Finally, Sec. VI then draws some conclusions.

II. QUANTUM SECRET SHARING PROTOCOL VIA PRODUCT STATE: PROTOCOL I

In the following proposed protocols, the secret is the state index l of the prepared qubit system $|\psi_l\rangle$. Since the state $|j\rangle$

$\otimes|j'\rangle$ is discarded, the state index of the other eight basis vectors in the complete set $\mathbf{((}i,j,k\mathbf{),(}i',j',k'\mathbf{))}$ can be encoded as three bits in the binary representation. That is, the sender splits the information of three secret bits, l, via sending each receiver a qutrit—i.e., sending $|\alpha_l\rangle$ and $|\beta_l\rangle$ to Bob and Charlie, respectively. The task of the receivers is to determine the state index of the transmitted two-qutrit system. Only when the receivers access full information of the product states do they decode the secret bits correctly. This study now considers how to modify the quantum key distribution of Guo *et al.* for quantum secret sharing. The proposed quantum secret sharing protocol is as follows.

Protocol I

Preparation phase

(1) Alice creates two ordered qubit sets of $\mathfrak{B}$ and $\mathfrak{C}$, where

$$\mathfrak{B}=\{|\alpha_{l_1}\rangle_{S_1},|\alpha_{l_2}\rangle_{S_2},\ldots,|\alpha_{l_n}\rangle_{S_n}\} \tag{2}$$

and

$$\mathfrak{C}=\{|\beta_{l_1}\rangle_{S_1},|\beta_{l_2}\rangle_{S_2},\ldots,|\beta_{l_n}\rangle_{S_n}\}. \tag{3}$$

Notably, $|\alpha_{l_i}\rangle_{S_i}\otimes|\beta_{l_i}\rangle_{S_i}$ is a basis vector of the complete set either $\mathbf{((}0,\ 1,\ 2\mathbf{),(}1,\ 0,\ 2\mathbf{))}$ with $S_i=0$ or $\mathbf{((}2,\ 0,\ 1\mathbf{),(}0,\ 1,\ 2\mathbf{))}$ with $S_i=1$. In addition, Alice permutes the element order in set $\mathfrak{C}$ based on the bijective function $r^{-1}(x)$:

$$r^{-1}(x)=y,\ \text{and}\ r(x)\neq x\ \forall\ x,\quad y=1,\ldots,n. \tag{4}$$

That is, the xth element in the ordered set $\mathfrak{C}$ now becomes the $[r^{-1}(x)]$th element. Therefore, the new ordered set $\mathfrak{C}'$ is

$$\mathfrak{C}'=\{|\beta_{l_{r(1)}}\rangle_{S_{r(1)}},|\beta_{l_{r(2)}}\rangle_{S_{r(2)}},\ldots,|\beta_{l_{r(n)}}\rangle_{S_{r(n)}}\}. \tag{5}$$

(2) Alice prepares two n-bit strings b and b'. Then she performs the three-level Hadama transformation

$$H=\begin{pmatrix}1 & 1 & 1\\ 1 & \omega & \omega^2\\ 1 & \omega^2 & \omega\end{pmatrix},\quad \omega=\exp\left(\frac{2\pi i}{3}\right), \tag{6}$$

on ith qutrits in the sets $\mathfrak{B}$ and $\mathfrak{C}'$ if the ith bits of b and b' are 1, respectively.

(3) Each time Alice sends the qutrits A ($|\alpha_{l_i}\rangle_{S_i}\in H_A$) and B ($|\beta_{l_{r(i)}}\rangle_{S_{r(i)}}\in H_B$) to Bob and Charlie, respectively. Once Bob and Charlie receive one qutrit, they publicly announce the facts, respectively. Then Alice sends $|\alpha_{l_{i+1}}\rangle_{S_{i+1}}$ and $|\beta_{l_{r(i+1)}}\rangle_{S_{r(i+1)}}$ after she confirms their respective receptions.

(4) After sending all qutrits and confirmation, Alice announces the strings b and b'. Bob and Charlie perform H^{-1} on qutrits A and B for which b and b' are 1, respectively.

(5) Alice publicly announces the function $r(m)$. Eventually, Bob and Charlie share n qutrit pairs $|\alpha_{l_i}\rangle_{S_i}\otimes|\beta_{l_i}\rangle_{S_i}$, $i=1,\ldots,n$.

(6) Alice announces the information (k,k') of the picked n' qutrit pairs. Then Bob performs the measurement on $|\alpha_{l_i}\rangle_{S_i}$ using either the basis $\{|i\rangle,|j\rangle,|k\rangle\}$ or $\{(1/\sqrt{2})(|i\rangle+|j\rangle),(1/\sqrt{2})(|i\rangle-|j\rangle),|k\rangle\}$. Charlie performs the measurement on $|\beta_{l_i}\rangle_{S_i}$ using either the basis $\{|i'\rangle,|j'\rangle,|k'\rangle\}$ or $\{(1/\sqrt{2})(|i'\rangle+|j'\rangle),(1/\sqrt{2})(|i'\rangle-|j'\rangle),|k'\rangle\}$. They publicly announce their respective measurement results. Alice discards the results with the outcomes of inappropriate measurement bases. If there are too many errors for the remaining outcomes, Alice aborts the secret. Otherwise, the other $(n-n')$ qutrit pairs are used in the revealing phase.

Revealing phase

(7) To know the state index l_i of $|\alpha_{l_i}\rangle_{S_i}\otimes|\beta_{l_i}\rangle_{S_i}$, Bob and Charlie discuss who performs the first local measurement in the basis $\{|0\rangle,|1\rangle,|2\rangle\}$ and then the other performs the conditioned local measurement. For example, Bob and Charlie access a random independent coin flip. If the coin is 0 (1), Bob (Charlie) and Charlie (Bob) should perform the first and the conditioned local measurements, respectively. In this study, F and S denote the receivers, who perform the first and conditioned measurements, respectively. F tells S his measurement outcome in private.

(8) The receiver S performs the second local measurement and then broadcasts the measurement basis and consequently tells the receiver F his measurement outcome in private.

(9) Alice tells Bob and Charlie which outcomes should be disregarded owing to the incorrect local measurement order. In this protocol, either $|0\rangle\otimes|1\rangle$ or $|1\rangle\otimes|0\rangle$ are disregarded.

(10) This study divides the measurement outcomes based on correct measurement into two subsets: those for which Bob performs the first local measurement, denoted by $\mathcal{B}$, and those for which Charlie performs the first local measurement, denoted by $\mathcal{C}$. On average, there are about equal element numbers of subsets $\mathcal{B}$ and $\mathcal{C}$. Alice randomly selects half of the elements from subsets $\mathcal{B}$ and $\mathcal{C}$, respectively, after which Bob and Charlie then broadcast the selected measurement outcomes, respectively. As a result, Alice checks these outcomes to detect possible eavesdropping behavior. If too many errors occur, Alice announces to abort the secrets.

The proposed protocol is described in detail. At first, we explain steps (1), (2), and (3), which are the essential differences from the protocol of Guo *et al.* [16]. Suppose Eve intercepts the qutrits $|\alpha_{l_i}\rangle_{S_i}$ and $|\beta_{l_{r(i)}}\rangle_{S_{r(i)}}$ for any i in step (3). Then Eve can perform some joint measurement on $|\alpha_{l_i}\rangle_{S_i}$ and $|\beta_{l_{r(i)}}\rangle_{S_{r(i)}}$ before resending one qutrit pair. In this case, Eve can get very little information because she cannot measure $|\alpha_{l_i}\rangle_{S_i}\otimes|\beta_{l_i}\rangle_{S_i}$ jointly. In the protocol of Guo *et al.*, Alice can send a qutrit at one time [10]. In the proposed protocol, Alice can send two qutrits at a time in step (3). On the other hand, suppose Eve wants to access full information of single qutrit $|\alpha_{l_i}\rangle_{S_i}$ ($|\beta_{l_{r(i)}}\rangle_{S_{r(i)}}$). In this case, Eve has to know b_i (b_i') at least. Therefore, step (2) is to reduce Eve's mutual information when she attacks on only a qutrit. Correspondingly, Alice and Bob recover all $|\alpha_{l_i}\rangle_{S_i}$'s and $|\beta_{l_{r(i)}}\rangle_{S_{r(i)}}$'s in step (4). In step (5), Bob rearranges the order of all $|\beta_{l_{r(i)}}\rangle_{S_{r(i)}}$'s so that Alice and Bob's ith qutrits are $|\alpha_{l_i}\rangle_{S_i}$'s and $|\beta_{l_{r(i)}}\rangle_{S_{r(i)}}$, respectively.

Second, there are two steps to detect possible eavesdropping attacks. In the preparation phase, Alice tries to detect

possible attacks actively in step (6). Suppose Alice announces the information (k,k') for the i'th qutrit pair. In the error-free case, she expects that Bob or Charlie can find some $|\alpha_{l_{i'}}\rangle_{S_{i'}}$ or $|\beta_{l_{i'}}\rangle_{S_{i'}}$ if an appropriate measurement basis is exploited. As a result, deception can be detected if receivers announce wrong outcomes in the appropriate measurement basis. In the revealing phase, as previously stated, Bob and Charlie both have full access to information if they perform the local measurements in the correct order. In step (7), if Bob and Charlie randomly decide the person to perform the first local measurement in the basis $\{|0\rangle, |1\rangle, |2\rangle\}$, performing the local measurements in the correct order yields a probability $\frac{1}{2}$. For the present discussion, Bob is to be the receiver that performs the second local measurement. Meanwhile, honest Bob supposes that they both employ the correct order of local measurements and then he tries to guess the complete set to which this product state belongs. For example, Bob knows that Charlie's measurement outcome is $|1\rangle$ ($|2\rangle$). In addition, Bob guesses that the product state is a basis vector of the complete set **(**(0, 1, 2),(1, 0, 2)**)**. Consequently, Bob must measure his qutrit in the basis $\{(1/\sqrt{2})\times(|0\rangle\pm|1\rangle),|2\rangle\}$ **(**$\{(1/\sqrt{2})(|1\rangle\pm|2\rangle),|0\rangle\}$**)**. If the measurement outcome of honest Bob in step (8) is $|2\rangle$ ($|0\rangle$), he immediately knows that either they have employed the wrong measuring order or some eavesdropping has occurred. Alice learns the order of the local measurements in step (8). Therefore, in step (9), Alice can inform Bob and Charlie which measurement outcomes with the incorrect measurement orders is to be dropped over a classical channel. In the above example, if Bob expects that the measurement order is wrong but Alice tells Bob and Charlie to keep this outcome, honest Bob will immediately know that Charlie may have cheated. Moreover, since Bob and Charlie keep the measurement outcomes only when they employ the correct measuring orders, Bob and Charlie generally will have to drop half of the measurement outcomes in step (9).

III. QUANTUM SECRET SHARING PROTOCOL VIA PRODUCT STATE: PROTOCOL II

In the previous protocol, the secret can be revealed only when Bob and Charlie perform the local measurements in the correct order. In addition, the sent product state is one of the basis vectors of the complete set, either **(**$(i,j,k),(i',j',k')$**)** or **(**$(i',j',k'),(i,j,k)$**)**. In general, Alice can prepare a product state, which can be a basis vector lying in some domino of the 18 nonlocal complete sets. Therefore, protocol I can be modified as follows.

(a) As in step (1) of the protocol in Sec. II, Alice prepares a product state, which is one of the basis vectors of the 18 nonlocal complete sets. This study assumes the prepared product state to be one of the basis vectors of the complete set **(**$(i,j,k),(i',j',k')$**)**.

(b) Following the confirmation in step (5), Alice broadcasts the index (i',j',k') and (i,j,k). Notably, the correct local measurement order remains unknown to Bob and Charlie.

Now suppose the eavesdropper can intercept two-qutrit system $|\alpha_{l_i}\rangle_{S_i}\otimes|\beta_{l_i}\rangle_{S_i}$ simultaneously. In addition, Alice does not reveal any information of the complete set. The eavesdropper can employ the basis of a nonlocal complete set as the collective measurement basis. For example, suppose that Alice prepares $(1/\sqrt{2})(|i\rangle+|j\rangle)\otimes|i'\rangle$. The eavesdropper intercepts both qutrits and then performs some collective measurement with one of the 18 complete set basis. If he chooses one of the complete sets **(**$(i,j,k),(i',j',k')$**)**, **(**$(j,i,k),(i',j',k')$**)**, **(**$(i,j,k),(i',k',j')$**)**, or **(**$(j,i,k),(i',k',j')$**)** as the measurement basis, the eavesdropper can access full information without any disturbance. Therefore, the probability of successful and undisturbed eavesdropping is $\frac{2}{9}$.

In the quantum key distribution protocol of Guo *et al.*, the sender and receiver preagree on the sending order of qutrits and the measurement basis. The key point is that the sender must ensure that, after sending a qutrit, the receiver has also received a qutrit. In proposed protocol I and its modification, the receivers have to discuss the order of the local measurements. The following discussion investigates the quantum secret sharing protocol, in which the receivers do not need to discuss the local measurement order. In following discussion, each complete set is denoted by the corresponding index S_i. This protocol is as follows.

Protocol II

Preparation phase

The steps from (1) to (6) are just about equivalent to those in protocol I. The main difference is that the index S_i can be 0, 1,…, 17. Now Bob and Charlie are assumed to hold the ordered sets of $\mathfrak{B}$ and $\mathfrak{C}$ in Eqs. (2) and (3), respectively.

Revealing phase

(7) Alice broadcasts the n binary bit strings d as the appropriate local measurements. If the ith bit of d is 1 (0), Bob (Charlie) should F to perform the foremost local measurement on qutrit $|\alpha_{l_i}\rangle_{k_i}$ ($|\beta_{l_i}\rangle_{k_i}$). After the receiver F has performed the first local measurement in the basis $\{|0\rangle, |1\rangle, |2\rangle\}$, F broadcasts that he has performed his measurement. In addition, F privately informs the other receiver of the measurement outcome. For example, let Alice prepare $(1/\sqrt{2})(|i\rangle+|j\rangle)\otimes|i'\rangle$. Alice broadcasts that Charlie (F) performs the first local measurement in the basis $\{|0\rangle, |1\rangle, |2\rangle\}$.

(8) Each time Alice receives the broadcast of F, she then broadcasts the complete set to which the sent product states belong. Since $(1/\sqrt{2})(|i\rangle+|j\rangle)\otimes|i'\rangle$ is one basis of the four complete sets **(**$(i,j,k),(i',j',k')$**)**, **(**$(j,i,k),(i',j',k')$**)**, **(**$(i,j,k),(i',k',j')$**)**, and **(**$(j,i,k),(i',k',j')$**)**, Alice can publicly announce that the state of the prepared qutrits is one of the basis vectors in the complete set **(**$(i,j,k),(i',j',k')$**)**.

(9) Bob and Charlie must announce some portion of the secret bits to detect possible deception behaviors. Consequently, Bob and Charlie perform step (10) of the proposed protocol I.

The protocol used in this investigation is described in detail. Obviously, Alice initially does not reveal the sending order and measurement basis information, to prevent the eavesdropper from accessing full information without aware-

ness. For example, suppose that Alice prepares one of the following four states: $|k\rangle\otimes(1/\sqrt{2})(|i'\rangle\pm|j'\rangle)$ and $|i\rangle\otimes(1/\sqrt{2})(|j'\rangle\pm|k'\rangle)$. After Alice broadcasts the measuring order and the complete set basis $\mathbf{((}i,j,k\mathbf{),(}i',j',k'\mathbf{))}$ in step (8), Bob (F) performs the measurement in the basis $\{|0\rangle, |1\rangle, |2\rangle\}$. The outcome should be either $|k\rangle$ or $|i\rangle$. Bob then informs Charlie (S) of his outcome. After Alice broadcasts the measurement basis in step (8), Charlie performs his measurement in the basis $\{(1/\sqrt{2})(|i'\rangle\pm|j'\rangle, |k'\rangle\}$ or $\{(1/\sqrt{2})(|j'\rangle\pm|k'\rangle, |i'\rangle\}$, respectively. Charlie should tell Bob his outcome. As a result, Alice can share a secret bit with Bob and Charlie. Notably, if Bob is honest, he will not measure $|j\rangle$ in this example. If Bob measures $|j\rangle$, honest Bob immediately knows that some deception has occurred in the error-free condition.

In general, a quantum secret sharing protocol can be modified to be a quantum key distribution as follows. Bob and Charlie are regarded as the same receiver. In addition, Alice can send the second qutrit only after confirming that the receiver has received the first one. As the sender does in step (4) of the proposed quantum secret sharing protocol II, Alice also broadcasts the measurement basis. Nevertheless, this protocol offers minimal advantage over the other quantum key distribution schemes.

This study examines how Alice performs the initial preparation. Alice can prepare two supplies of $|0\rangle$ and $|0+1\rangle$, respectively. To prepare the states $|1\rangle$ or $|2\rangle$, Alice can perform the unitary transformation M: $|t\rangle\rightarrow|t+1\rangle$ on $|0\rangle$ once or twice, respectively. Similarly, Alice also can prepare some $|i+j\rangle$ in this manner. If Alice has to prepare $|i-j\rangle$, she may perform the unitary transformation D: $\mathrm{diag}(1,-1,1)$ followed by Ms. Both D and M are one-qutrit unitary transformations. Consequently, Alice does not require any pairwise unitary transformation for the preparation. Therefore, physically realizing such preparation will be much easier than the preparation of the Bell states and GHZ states.

Finally, we compare the proposed protocols with quantum secret sharing using GHZ states [1]. In the error-free case, the efficiency of quantum secret sharing using either GHZ states or product states is nearly 100%. In the case of quantum secret sharing using GHZ states, leaving out any receiver, the rest can have no information about the secret bit. In the proposed protocols, any receivers can obtain mutual information even without classical communication. Consequently, Eve can gain some mutual information. The proposed protocols can reduce Eve's mutual information in steps (1) and (2). On the other hand, let Eve be able to entangle the sent qubits with ancilla qubits. If the GHZ entanglement introduces no errors into secret sharing procedures, an eavesdropper can gain no information in this way. Or if Eve can gain information about secret bits, inevitable errors must occur. In the proposed protocols, the ideal eavesdropping attack is to clone the untangled qutrit states perfectly. However, the nonorthogonality and no-clone theorem guarantee the impossibility of such an attack.

IV. SECURITY ANALYSIS OF PROTOCOLS I AND II

Now we consider the security of protocols I and II. Recall that four possible states $(\{|0\rangle, |1\rangle, (1/\sqrt{2})(|0\rangle+|1\rangle), (1/\sqrt{2})(|0\rangle-|1\rangle)\})$ are exploited in the BB84 protocol. Protocol II can be regarded as the hybrid of three BB84 protocols based on three different sets of four states $\{|i\rangle, |j\rangle, (1/\sqrt{2})\times(|i\rangle+|j\rangle), (1/\sqrt{2})(|i\rangle-|j\rangle)\}$, where (i,j) are (0, 1), (1, 2), (2, 0), respectively. In addition, the sender smashes the information (i,j) using three-level Hadama transformation. Furthermore, the sender must always confirm that the receiver has received the previous qutrit before the next qutrit is sent. Therefore, protocol II is much more secure than the ordinary BB84 protocol. As for protocol I, Guo *et al.* prove that, in their protocol, an eavesdropper cannot access full information even if an eavesdropper can intercept $(|\alpha_{l_i}\rangle\otimes|\beta_{l_i}\rangle)_{S_i}$ simultaneously. In addition, an eavesdropper can never intercept $(|\alpha_{l_i}\rangle\otimes|\beta_{l_i}\rangle)_{S_i}$ simultaneously in protocol I. To access full information in protocols I and II, an eavesdropper has to know the following information after intercepting and before resending the other's qutrit: the complete set index S_i, the strings b and b', and the function $r(m)$. In step (6) and the last step of protocols I and II, the sender checks possible eavesdropping. That is, Alice can always find the possible eavesdropping with higher probability than the BB84 protocol. Next we just consider some possible attacks. Further security proof is considered in Sec. V.

A. Misstate strategy

Since Bob and Charlie have to discuss Alice's preparation, the intuitive cheating is to lie to the honest receiver. For simplicity, let Bob and Charlie be receivers F and S, respectively. If the eavesdropper is receiver S, the simplest method of cheating is to misstate local measurement outcomes to the other receiver. However, such deception can be detected in step (6) because the honest receiver can choose and broadcast a portion of such false outcomes to the sender.

Moreover, the no-clone theorem guarantees that a perfect clone of possible nonorthogonal states is impossible [12]. In protocol II, if the eavesdropper, Bob or Charlie, takes the intercept-resend strategy, he can access full information using the correct basis with probability $\frac{2}{9}$. Otherwise, the eavesdropper will disturb the quantum state. Therefore, the probability of successful eavesdropping without disturbance is $\frac{2}{9}$. On the other hand, since receiver S is assumed to perform his measurement after receiver F, S always can access full information before F. Therefore, if S is the eavesdropper, S can cheat F by stating false outcomes. This condition also happens in other quantum secret sharing schemes. In some quantum secret sharing schemes, the two receivers have to discuss Alice's outcomes [1] or preparation [2]. In practice, either Bob or Charlie must expose his outcome to the other first. Inevitably, the second receiver to expose his outcome can always have access to full information before the other receiver. However, since the sender is aware of any of incorrect public measurement outcomes in step (6), false outcome statements can be detected.

In addition, the dishonest receiver F can also misstate the outcomes: For example, Alice prepares the product state $|k\rangle\otimes(1/\sqrt{2})(|i'\rangle+|j'\rangle)$. If the receiver F misstates his outcome as $|j\rangle$, receiver S can detect this cheating immediately after Alice broadcasts the complete set basis as $\mathbf{((}i,j,k\mathbf{),}$

(i',j',k')**)** in step (5). Meanwhile, if F misstates the outcome as $|i\rangle$, receiver S should perform his local measurement in the basis $\{(1/\sqrt{2})(|j'\rangle \pm |k'\rangle), |i'\rangle\}$. If the outcome is $|i'\rangle$ with probability $\frac{1}{2}$, S can immediately detect the cheating. In addition, Alice is definitely aware of this cheating if the outcome is broadcast in step (6). Therefore, any misstatements can be detected.

B. Intecept-resend strategy

For simplicity, we just consider $r(m)=m$. Either dishonest Bob (F) or dishonest Charlie (S) can take the intercept-resend strategy. In the quantum key distribution protocol of Guo *et al.*, the eavesdropper can only perform local measurements. In the protocol presented here, the eavesdropper can perform any joint measurement. However, only when the eavesdropper performs a correct collective or local measurement on these two intercepted qutrits can the eavesdropper access full secret information. Otherwise, the eavesdropper will fail to know the secret. For example, in protocol I, the eavesdropper intercepts the product state $|0\rangle \otimes (1/\sqrt{2})(|0\rangle + |2\rangle)$. If the eavesdropper performs the measurement in the basis of the complete set **(**(2, 0, 1),(0, 1, 2)**)**, he will get $(1/\sqrt{2})(|0\rangle \pm |2\rangle) \otimes |0\rangle$ or $(1/\sqrt{2})(|0\rangle \pm |1\rangle) \otimes |2\rangle$ with equal probability $\frac{1}{4}$. The corresponding density matrix is

$$\frac{1}{4}(|00\rangle\langle 00| + |20\rangle\langle 20| + |02\rangle\langle 02| + |12\rangle\langle 12|). \tag{7}$$

Apparently, the eavesdropper cannot gain any information from this density matrix. As a result, the eavesdropper can perform successful eavesdropping with probability $\frac{1}{2}$.

This study considers that, in protocol II, dishonest Bob (F) intercepts Charlie's qutrit and resends a qutrit to Charlie before Alice's first broadcast in step (4). This study assumes that Bob sends Charlie the qutrit $|l'\rangle$, which is equally likely to be $|0\rangle$, $|1\rangle$, or $|2\rangle$. Also, it is assumed that Alice sends the quantum system $|k\rangle \otimes (1/\sqrt{2})(|i'\rangle + |j'\rangle)$ or $|k\rangle \otimes (1/\sqrt{2})(|i'\rangle - |j'\rangle)$, and then announces that the corresponding complete set is **(**$(i,j,k),(i',j',k')$**)**. In addition, Charlie should perform his local measurement in the basis $\{(1/\sqrt{2})(|i'\rangle \pm |j'\rangle), |k'\rangle\}$ after Bob tells him the faithful outcome. If $|l'\rangle = |j'\rangle$ or $|i'\rangle$ and Bob honestly tells Charlie the outcomes, then Charlie fails to detect the deception. Nevertheless, if the outcomes are public in step (6), Alice can detect the cheating with probability $\frac{1}{2}$. If $|l'\rangle = |k'\rangle$, Bob must misstate his outcome to be certain of avoiding Charlie's detection. Nevertheless, Alice can definitely detect such cheating if the outcomes are public in step (6).

This study now assumes that dishonest Charlie, receiver S, intercepts Bob's qutrit and resends the qutrit $|l\rangle$, which can be $|0\rangle$, $|1\rangle$, or $|2\rangle$ with equal probability. Again this study assumes that Alice sends the receivers the quantum system $|k\rangle \otimes (1/\sqrt{2})(|i'\rangle + |j'\rangle)$ and then announces that the corresponding complete set is **(**$(i,j,k),(i',j',k')$**)**. If $|l\rangle = |j\rangle$, Bob can directly detect the cheating in step (5) since Bob's outcomes should be either $|i\rangle$ or $|k\rangle$. If $|l\rangle = |k\rangle$, the eavesdropping is ineffective. In addition, Charlie's misstatement is detected in step (6). If $|l\rangle = |i\rangle$, Charlie may misstate his outcome. However, Alice can detect such cheating in step (6). Suppose that the eavesdropper performs the intercept-resend strategy on every pair of sent qutrits. In this example, only when Charlie resends Bob $|k\rangle$ and tells Bob the faithful outcome will Charlie not be found to be cheating. In other words, dishonest Charlie's cheating must be detected. Importantly, the eavesdropper cannot know the measuring order in advance. That is, Alice can prevent Trojan horse attacks quite well [13]. Otherwise the proposed protocol will be ineffective.

C. Guo–Li–Shi–Li–Guo strategy

For simplicity, we just consider $r(m)=m$. The quantum key distribution protocol of Guo *et al.* considers the following eavesdropping strategy. The eavesdropper, Bob or Charlie, intercepts the other's qutrit. The eavesdropper performs the orthogonal measurement on one qutrit in the basis $\{|0\rangle, |1\rangle, |2\rangle\}$. Based on the outcome, the eavesdropper performs another orthogonal measurement on the other qutrit in some different basis. Guo *et al.* used only one complete set $\{|\psi_i\rangle\}$. Now suppose that the eavesdropper takes such an eavesdropping strategy in our quantum secret sharing protocol II. The eavesdropper first performs an orthogonal measurement on a single qutrit in the basis $\{|0\rangle, |1\rangle, |2\rangle\}$. Without loss of generality, the first outcome can be allowed to be $|0\rangle$. Furthermore, the eavesdropper infers that the probability of the states $|0\rangle \otimes (1/\sqrt{2})(|i'\rangle \pm |j'\rangle)$ **(**$(i',j')=(0,1),(1,2)$, or $(2,0)$**)** and $|0 \pm k\rangle \otimes |k'\rangle$ ($k=1$, 2 and $k'=0,1,2$) may be prepared with equal probability. Finally, suppose the eavesdropper guesses that the state is one of the states $|0\rangle \otimes |i' \pm j'\rangle$. The eavesdropper then can perform the nonorthogonal measurement with the following six positive-valued operators:

$$\Pi_{0\pm1} = \frac{1}{2}|0 \pm 1\rangle\langle 0 \pm 1|, \quad \Pi_{1\pm2} = \frac{1}{2}|0 \pm 2\rangle\langle 0 \pm 2|,$$

$$\Pi_{2\pm1} = \frac{1}{2}|2 \pm 1\rangle\langle 2 \pm 1|, \tag{8}$$

where $|0 \pm 1\rangle$ denotes the states $(1/\sqrt{2})(|0\rangle \pm |1\rangle)$ and so on. It is easy to verify that $\Sigma_{i,j}(\Pi_{i+j} + \Pi_{i-j}) = 1$, where 1 denotes the identity operator. Alice is assumed to prepare $|0\rangle \otimes |i'' + j''\rangle$. In this case, the rate that state $|i'' + j''\rangle$ projects into the $\Pi_{i''+j''}$ is $\frac{1}{2}$. In this way, the probability that an eavesdropper can access full information without awareness is $\frac{1}{4}$.

V. QUANTUM SECRET SHARING PROTOCOL VIA PRODUCT STATE: PROTOCOL III AND A SIMPLE PROOF OF SECURITY

In this section, we propose another protocol similar to the Ekert protocol [14]. Recently, many researches focused on proving the unconditional security of the quantum key distribution [15,16]. The main theme of proof is to purify the raw two-level Bell states and then measure the syndrome of the stabilizer code [17]. As a result, the receiver and sender can share perfect Bell states. Nevertheless, in this paper, three-level qutrits are exploited. To prove the unconditional

security of protocols I and II, we first introduce the nonlocality swapping [18]

$$|\Psi_{00}\rangle_{(1,2)}|\Psi_{00}\rangle_{(3,4)} = \frac{1}{3}\sum_{l=1}^{9} |\psi_l\rangle_{S_i,(1,4)}|\psi_l\rangle_{S_i,(2,3)}, \quad (9)$$

where 1, 2, 3, 4 are qutrit indices and $|\Psi\rangle_{(i,j)}$ is the three-level Bell state:

$$|\Psi_{00}\rangle_{(i,j)} = \frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle). \quad (10)$$

Alice holds the qutrits 1 and 4. Bob and Charlie hold qutrits 2 and 3, respectively. Alice performs the measurement in the basis $\{|\psi_l\rangle_{S_i}=|\alpha_l\rangle_{S_i}\otimes|\beta_l\rangle_{S_i}\}$ of some complete set of set index S_i, where $i=0,\ldots,17$. In this way, Bob and Charlie possess $|\alpha_l\rangle_{S_i}$ and $|\beta_l\rangle_{S_i}$, respectively. It is noteworthy that it is nonlocality rather than entanglement which is preserved after the measurement [18]. Therefore, the main idea of the proposed protocol III is as follows. The sender and each receiver initially share the first and second halves of each $|\Psi_{00}\rangle$. After performing the purification and the purity test, the sender and each receiver can share perfect three-level Bell states [13]. Then the sender performs nonlocality swapping and then publicly announces the set index. Finally, the two receivers discuss the state index of the shared states at hand. Nevertheless, few papers investigate how to purify multilevel Bell states. Here we propose a quantum privacy amplification algorithm (QPA algorithm) on three-level Bell states as follows [19]. (1) The sender performs the three-level Hadama transformation and the receiver performs the inverse Hadama transformation. (2) The sender and receiver each perform two instances of the quantum bilateral controlled-NOT (CNOT) operations,

$$|a\rangle|b\rangle \rightarrow |a\rangle|a \oplus b \bmod 3\rangle, a,b \in \{0,1,2\}, \quad (11)$$

between the control pair and target pair. Notably, any of the control pairs and the target pair comprise two qutrits in the initial state $|\Psi_{00}\rangle$. (3) The sender and each receiver then measure the target qutrits in the basis $\{|0\rangle, |1\rangle, |2\rangle\}$. Each receiver publicly announces the measurement outcomes. If the sender finds that the outcomes coincide, they keep the control pair for the next round and discard the target pair. Notably, it is Alice who decides whether a target pair should be kept. In this way, the eavesdropper's forgery will fail the proposed QPA algorithm. We denote the three-level Bell basis by $|\Psi_{jk}\rangle$, where

$$|\Psi_{jk}\rangle = \frac{1}{\sqrt{3}}\sum_{l=0}^{2} \omega^{lk}|l\rangle|l+j \bmod 3\rangle, \quad j,k=0,1,2. \quad (12)$$

In addition, the fidelity of the state $|\Psi_{jk}\rangle$ is denoted by p_{jk}. After one round of the proposed QPA algorithm, the new density matrix comprises the survived controlled pairs with $\{\tilde{p}_{jk}\}$, where

$$\tilde{p}_{00} = N^{-1}(p_{00}^2 + p_{10}^2 + p_{20}^2), \quad (13)$$

$$\tilde{p}_{01} = N^{-1}(p_{00}p_{10} + p_{10}p_{20} + p_{20}p_{00}),$$

$$\tilde{p}_{02} = N^{-1}(p_{00}p_{20} + p_{10}p_{00} + p_{20}p_{10}), \quad (14)$$

$$\tilde{p}_{10} = \tilde{A}_{20} = N^{-1}(p_{01}p_{02} + p_{11}p_{12} + p_{21}p_{22}), \quad (15)$$

$$\tilde{p}_{11} = \tilde{A}_{22} = N^{-1}(p_{01}p_{12} + p_{11}p_{22} + p_{21}p_{02}),$$

$$\tilde{p}_{12} = \tilde{A}_{21} = N^{-1}(p_{01}p_{22} + p_{11}p_{02} + p_{21}p_{12}), \quad (16)$$

and the normalization constant $N=(p_{00}+p_{10}+p_{20})^2+2(p_{01}+p_{11}+p_{21})(p_{02}+p_{12}+p_{22})$. Our simulation of the iterative mapping in Eq. (16) is shown in Fig. 2. Therefore, if the sender and each receiver perform the above QPA algorithm iteratively, they can purify the three-level Bell state $|\Psi_{00}\rangle$ with the initial diagonal element $p_{00}>0.5$. Furthermore, if the initial diagonal elements $p_{10}=p_{20}=0$, we can purify $|\Psi\rangle$ even with the initial diagonal element $p_{00}>\sqrt{2}-1$.

After purifying the raw entanglement, the sender and each receiver measure the syndrome of the three-ary—i.e., nonbinary—stabilizer code for purity testing [17]. In other words, three-ary quantum stabilizer codes are required for purity. Recently, nonbinary quantum stabilizer codes have been studied [20–25]. There must exist three-ary quantum stabilizer codes that encode m qutrit into n qutrit and can correct t "nice" errors T^kR^l, where

$$T:|p\rangle \rightarrow |p+1 \bmod 3\rangle, \quad R:|p\rangle \rightarrow \exp\left(\frac{2p\pi i}{3}\right)|p\rangle \quad (17)$$

[21]. On the other hand, it is easy to verify

$$|\Psi_{kl}\rangle = (1\otimes T^kR^l)|\Psi_{00}\rangle, \quad \forall\, l,m=0,1,2. \quad (18)$$

Suppose that the states shared between Alice and each receiver are assumed to be nearly in state $|\Psi_{00}\rangle^{\otimes n}$. The sender and each receiver can correct t nice errors via quantum error correction codes [15,16,26]. Still, each receiver should broadcast the necessary measurement results. It is the sender that performs the needed local operations for error correcting. As a result, the sender can share perfect state $|\Psi_{00}\rangle^{\otimes m}$. Next, the sender performs the nonlocality swapping. Now we propose protocol III of quantum secret sharing as follows.

Protocol III

Preparation phase

(1) The sender Alice and the each receiver of Bob and Charlie agree on some stabilizer purity testing. In addition, Alice prepares two strings of Bell states

$$\{|\Psi_{00}\rangle_{B_1}, |\Psi_{00}\rangle_{B_2}, \ldots, |\Psi_{00}\rangle_{B_{n'}}\}$$

and

$$\{|\Psi_{00}\rangle_{C_1}, |\Psi_{00}\rangle_{C_2}, \ldots, |\Psi_{00}\rangle_{C_{n'}}\}$$

.

(2) Alice selects two random n'-bit strings b and b'. Alice performs the three-level Hadama transformation on the second half of $|\Psi_{00}\rangle_{B_i}$ and $|\Psi_{00}\rangle_{C_i}$ if the ith bitvalues of b and b' are 1, respectively.

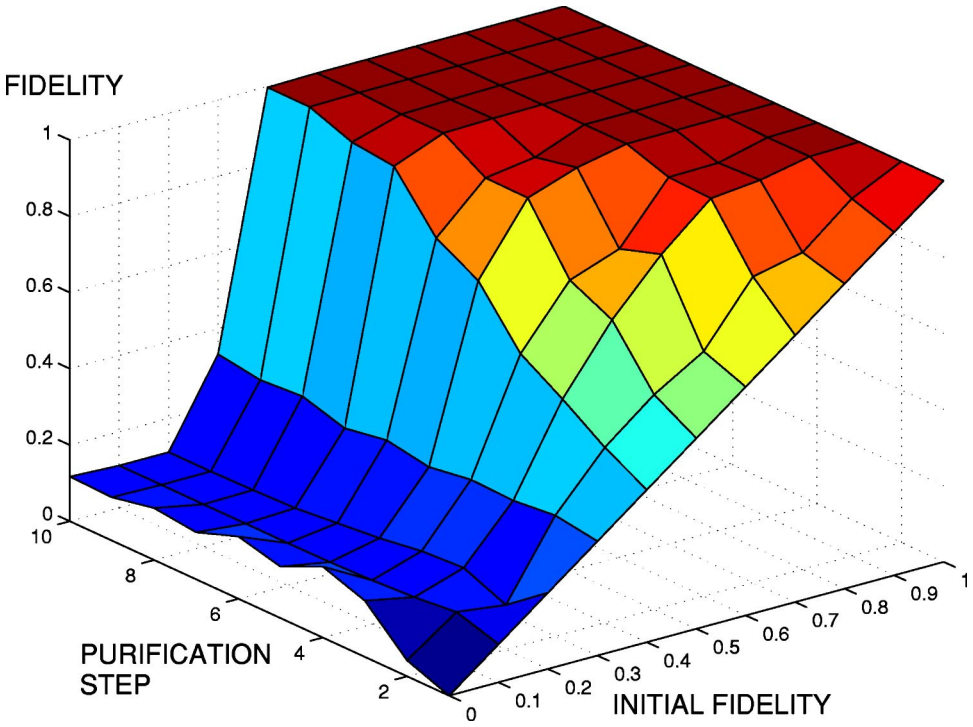

FIG. 2. (Color online) Average fidelity of the proposed three-level quantum privacy amplification, which is a function of the initial fidelity and the number of iterations.

(3) Alice sends the second half of each $|\Psi_{00}\rangle_{B_i}$ and $|\Psi_{00}\rangle_{C_i}$, $i=1,\ldots,n'$, respectively. Alice holds the first half of $|\Psi_{00}\rangle_{B_i}$ and $|\Psi_{00}\rangle_{C_i}$, $i=1,\ldots,n'$.

(4) When Bob and Charlie receive their qutrits, they inform Alice that they have received the qutrit over a classical channel, respectively.

(5) Alice announces the bit strings b and b' after she confirms that all qutrits have been received. Bob and Charlie then perform the three-level inverse Hadama transformation on the qutrits where b and b' are 1, respectively.

(6) Alice and each of Bob and Charlie perform the proposed QPA algorithm to purify $|\Psi_{00}\rangle$. Notably, Alice decides whether the purification is successful. If they fail to purify $|\Psi_{00}\rangle$, Alice aborts the secret. Otherwise, Alice performs the following steps.

(7) Next they have to perform purity testing via measuring the syndrome of the preagreed stabilizer code [17].

(8) Alice performs nonlocality swapping in the basis of the complete set $\mathbf{((}i,j,k),(i',j',k')\mathbf{)}$ with set index S_i.

Revealing phase

(9) Alice publicly announces the set index S_i of the measurement basis and who should perform the foremost measurement via classical communication.

(10) Bob and Charlie discuss the state index of the qutrits at hand.

(11) Bob and Charlie must announce some portion of the secret bits to detect possible deception behaviors. Consequently, Bob and Charlie perform step (6) of the proposed protocol I.

After nonlocality swapping, Bob and Charlie have to discuss the state index of the shared product state based on Alice's announcement. The eavesdropper can forge the measurement results. Moreover, the eavesdropper can forge the measurement results in the error-correction process of distillation. Eventually, the sender and each receiver could share some Bell states other than $|\Psi_{00}\rangle$. In this case, the state of the qutrits 1 and 4 is not identical that of the qutrits 2 and 3 after the nonlocality swapping in Eq. (9). Therefore, any misstatement can be detected in step (11).

VI. CONCLUSION

This study introduces how to perform the quantum secret sharing via product states. These three proposed protocols can split information and detect eavesdropping simultaneously using product states. Since the proposed protocols I and II in this study do not require any entanglement, their physical realization is very feasible. This study also investigates possible eavesdropping attacks. In addition, this study can revise the quantum key distribution protocols using product states as the quantum secret sharing protocols using product states. Furthermore, we provide a simple proof of protocols I and II.

ACKNOWLEDGMENT

L.Y.H. would like to thank the National Science Council of the Republic of China for financially supporting this research under Contract No. NSC. 93–2119–M-033–001.

[1] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
[2] M. Koashi and N. Imoto, Phys. Rev. Lett. **79**, 2383 (1997).
[3] V. Karimipour, A. Bahraminasab, and S. Bagherinezhad, Phys. Rev. A **65**, 042320 (2002).
[4] A. Cabello, e-print quant-ph/0009025.
[5] S. Bagherinezhad and V. Karimipour, Phys. Rev. A **67**, 044302 (2003).
[6] M. Hillery and J. Mimih, Phys. Rev. A **67**, 042304 (2003).
[7] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), p. 175.
[8] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[9] L. Goldenberg and L. Vaidman, Phys. Rev. Lett. **75**, 1239 (1995).
[10] G.-P. Guo, C.-F. Li, B.-S. Shi, J. Li, and G.-C. Guo, Phys. Rev. A **64**, 042301 (2001).
[11] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, Tal Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **59**, 1070 (1999).
[12] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).
[13] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[14] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[15] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[16] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[17] H. Barnum, C. Crépeau, D. Gottesman, A. Smith, and A. Tapp, in *Proceedings of The 43rd Annual IEEE Symposium on Foundations of Computer Science (FOCS'02)* (IEEE, New York, 2002), pp. 16–19.
[18] L. Y. Hsu, Phys. Rev. A **65**, 062302 (2002).
[19] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).
[20] E. Knill, e-print quant-ph/9608048.
[21] A. Ashikhmin and E. Knill, IEEE Trans. Inf. Theory **47**, 3065 (2001).
[22] E. Rains, e-print quant-ph/9703048.
[23] A. Ashikhmin and S. Litsyn, IEEE Trans. Inf. Theory **45**, 1206 (1999).
[24] R. Matsumoto and T. Uyematsu, IEICE Trans. Fundamentals **83**, 1206 (2000).
[25] E. Knill, e-print quant-ph/9608049.
[26] Charles H. Bennett, David P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).