Security analysis and improvements of arbitrated quantum signature schemes

Xiangfu Zou[1,2,*] and Daowen Qiu[1,3,†]

[1]*Department of Computer Science, Sun Yat-sen University, Guangzhou 510006, China*

[2]*School of Mathematics and Computational Science, Wuyi University, Jiangmen 529020, China*

[3]*SQIG–Instituto de Telecomunicações, Departamento de Matemática, Instituto Superior Técnico, Universidade Técnica de Lisboa, Av. Rovisco Pais,1049-001 Lisbon, Portugal*

(Received 30 July 2010; published 21 October 2010)

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. For signing quantum messages, some arbitrated quantum signature (AQS) schemes have been proposed. It was claimed that these AQS schemes could guarantee unconditional security. However, we show that they can be repudiated by the receiver Bob. To conquer this shortcoming, we construct an AQS scheme using a public board. The AQS scheme not only avoids being disavowed by the receiver but also preserves all merits in the existing schemes. Furthermore, we discover that entanglement is not necessary while all these existing AQS schemes depend on entanglement. Therefore, we present another AQS scheme without utilizing entangled states in the signing phase and the verifying phase. This scheme has three advantages: it does not utilize entangled states and it preserves all merits in the existing schemes; the signature can avoid being disavowed by the receiver; and it provides a higher efficiency in transmission and reduces the complexity of implementation.

DOI: 10.1103/PhysRevA.82.042325 PACS number(s): 03.67.Dd, 03.67.Ac

I. INTRODUCTION

The most spectacular discovery in quantum computing to date is that a quantum computer can efficiently perform some tasks which are likely not feasible on a classical computer. For example, Shor's quantum algorithm [1] can solve efficiently two enormously important problems: the problem of finding the prime factors of an integer and the discrete logarithm problem. This means most of the classical public key cryptography would not be secure if quantum computers were available someday. Fortunately, quantum cryptography depends on fundamental laws of quantum physics to provide unconditional security [2–10]. Quantum key distribution (QKD) is the core of quantum cryptography.

Digital signature and authentication is an essential ingredient of classical cryptography and has been employed in various applications. Similar to classical public key cryptography, most classical digital signature schemes based on the public key cryptography can be broken by Shor's algorithm [1]. So, many researchers and scholars have begun to investigate quantum signature and authentication, which is supposed to provide an alternative scheme with unconditional security. Recently, some progress has been made on quantum signature [11–23]. In particular, an *arbitrated quantum signature* (AQS) scheme providing many merits had been proposed by Zeng and Keitel [13]. Indeed, this AQS scheme has been further discussed in the corresponding comments [24,25]. The scheme can sign both known and unknown quantum states. Also, it is claimed that the unconditional security is ensured by using the correlation of Greenberger-Horne-Zeilinger (GHZ) triplet states [26] and quantum one-time pads [27].

Very recently, Li *et al.* [14] have presented an arbitrated quantum signature scheme using two-particle entangled Bell states instead of GHZ states. The scheme using Bell states can preserve the merits in the original scheme [13] while providing a higher efficiency in transmission and reducing the complexity of implementation.

A secure arbitrated (quantum) signature scheme should satisfy two conditions: one is that the signature should not be forged by the attacker (including the malicious receiver) and the other is the impossibility of disavowal by the signatory and the receiver [13,14,25]. However, we find that the existing AQS schemes [13,14,25] can be repudiated by the receiver Bob. To conquer this shortcoming, we construct an AQS scheme using a public board. The AQS scheme can not only avoid being disavowed by the receiver but also can preserve all merits in the existing schemes.

Furthermore, we observe that the main functions of quantum entangled states (GHZ states and Bell states) in the schemes of Refs. [13,14,25] and in the foregoing scheme are to assist Alice to transfer quantum states to Bob. However, Alice transfers quantum states to the arbitrator by the ciphertext encrypted with the secret key K_A. Similarly, Alice can transfer quantum states to Bob with a shared secret key. Considering that the preparation, distribution, and keeping of entangled states are not easily implemented by the present-day technologies, we construct an AQS scheme without using quantum entangled states.

The remainder of this article is organized as follows. First, in Sec. II, we briefly recall some notions and notations concerning AQS schemes. In particular, we review the technique of comparing two unknown quantum states presented in Ref. [28] and discuss related properties. Then, in Sec. III, we show that the existing AQS schemes [13,14,25] can be repudiated by the receiver Bob. Afterward, in Sec. IV, we construct an AQS scheme similar to the scheme in Ref. [14] which cannot be repudiated by the receiver Bob, and we discover that this technique can be used to improve the AQS scheme using GHZ states [13,25]. Subsequently, in Sec. V, we discuss the security of the AQS scheme proposed in the previous section. In particular, in Sec. VI, we show that entanglement is not necessary and construct an AQS scheme without using

*xf.zou@hotmail.com.

†issqdw@mail.sysu.edu.cn

entangled states. Furthermore, in Sec. VII, we discuss the security of the second presented AQS scheme. In addition, in Sec. VIII, we compare the second AQS scheme presented with the existing schemes and outline its main merits. Finally, in Sec. IX, we draw conclusions.

II. PRELIMINARIES

In this section, we first briefly recall some notions and notations concerning AQS. In general, the other notations used in this article will be explained whenever new symbols appear. Then, we review the technique of comparing two unknown quantum states which was first presented in Ref. [28] and improved in Ref. [14]. Finally, we give an example that we need to use the arbitrated signature.

A. Some notions and notations concerning AQS

The digital signature is an analogy to handwritten signature, and the quantum signature is a quantum version of the classical signature. Similarly, the arbitrated signature scheme is a signature finished with the help of an arbitrator, where an arbitrator is a disinterested third party trusted to complete a protocol [29]. Here "trusted" means that all people involved in the protocol accept what he says as true and what he does as correct, as well as that he will complete his part of the protocol.

The notations, which are necessary to better understand the subsequent results, are given as follows.

We use Pauli matrices σ_x and σ_z to denote X and Z gates, respectively. Let $|P\rangle$ be a quantum message as $|P\rangle = |P_1\rangle \otimes |P_2\rangle \otimes \cdots \otimes |P_n\rangle$ with $|P_i\rangle = \alpha_i|0\rangle + \beta_i|1\rangle$.

For convenience, E_K denotes the quantum one-time pads encryption, proposed by Boykin and Roychowdhury [27], according to some key $K \in \{0,1\}^*$ satisfying $|K| \geqslant 2n$ as follows:

$$E_K(|P\rangle) = \bigotimes_{i=1}^{n} \sigma_x^{K_{2i-1}} \sigma_z^{K_{2i}} |P_i\rangle, \tag{1}$$

where K_j denotes the jth bit of K. Similarly, M_K denotes the unitary transformation

$$M_K(|P\rangle) = \bigotimes_{i=1}^{n} \sigma_x^{K_i} \sigma_z^{K_i+1} |P_i\rangle. \tag{2}$$

B. The technique of comparing two unknown quantum states

The comparison of known quantum states can be definitely made while the comparison of unknown quantum states cannot. Nevertheless, the error probability of determining whether two quantum bit strings are identical can be made small enough by adopting the approach in Ref. [28]. In particular, this method has been improved and specified in Ref. [14].

Now, we review the technique of comparing two unknown quantum states [28] and study related properties. Suppose we need to compare whether or not two states $|\phi\rangle$ and $|\psi\rangle$ are identical. This is accomplished with one-sided error probability by the procedure that measures and outputs the first qubit of the state

$$(H \otimes I)(\text{CSWAP})(H \otimes I)|0\rangle|\phi\rangle|\psi\rangle.$$

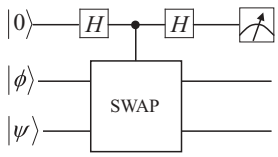

FIG. 1. The circuit of comparing two unknown quantum states.

Here H is the Hadamard transform, which maps $|b\rangle \to \frac{1}{\sqrt{2}}[|0\rangle + (-1)^b|1\rangle]$, SWAP is the operation $|\phi\rangle|\psi\rangle \to |\psi\rangle|\phi\rangle$, and CSWAP is the controlled SWAP (controlled by the first qubit). The circuit for this procedure is illustrated in Fig. 1. By tracing through the execution of this circuit, one can determine that the final state before the measurement is

$$\tfrac{1}{2}|0\rangle(|\phi\rangle|\psi\rangle + |\psi\rangle|\phi\rangle) + \tfrac{1}{2}|1\rangle(|\phi\rangle|\psi\rangle - |\psi\rangle|\phi\rangle). \tag{3}$$

Measuring the first qubit of this state produces outcome $|1\rangle$ with probability $\frac{1}{2} - \frac{1}{2}(\langle\phi|\psi\rangle)^2$. This probability is 0 if $|\phi\rangle = |\psi\rangle$ and is at least $\frac{1}{2}(1-\delta^2) > 0$ if $\langle\phi|\psi\rangle = \delta$. Thus, the test determines which case holds with one-sided error $\frac{1}{2}(1+\delta^2)$.

If we compare $|\phi\rangle^{\otimes m}$ and $|\psi\rangle^{\otimes m}$, we only need to perform independent comparison of $|\phi\rangle$ and $|\psi\rangle$ m times. For any $\varepsilon > 0$, the error probability of the comparison can be reduced to $[\frac{1}{2}(1+\delta^2)]^m < \varepsilon$, if we choose a suitable m and compare $|\phi\rangle^{\otimes m}$ and $|\psi\rangle^{\otimes m}$. This case was discussed further in Ref. [14].

Refs. [14,28] discussed only the comparison of two pure states. However, in the AQS scheme, we cannot affirm that the quantum states compared do not entangle with other quantum states. Eve (or Alice) may use some auxiliary quantum states which are entangled with one of the compared quantum states. Eve (or Alice) can manipulate the quantum states by operating on the auxiliary quantum states after Bob accepting the signature. So, we need to consider the situation described in Fig. 2, where $|\phi\rangle$ is a pure state and $|\alpha\rangle$ a two-particle entangled state. We need to compare the state $|\phi\rangle$ and the state of the first particle in $|\alpha\rangle$. Without loss of generality, we can suppose $|\alpha\rangle = a|\phi\rangle|x\rangle + b|\phi^\perp\rangle|y\rangle$, where $|\phi^\perp\rangle$ is the orthogonal pure state to $|\phi\rangle$, a and b are two nonzero complex numbers with $|a|^2 + |b|^2 = 1$, and $|x\rangle$ and $|y\rangle$ are two unknown pure states. This is accomplished with one-sided error probability by the procedure that measures and outputs the first qubit of the state

$$(H \otimes I_{234})(\text{CSWAP} \otimes I_4)(H \otimes I_{234})|0\rangle|\phi\rangle|\alpha\rangle.$$

Here H is the Hadamard transform performing on the first particle and CSWAP is the controlled SWAP (controlled by the first particle) performing on the second particle and the third

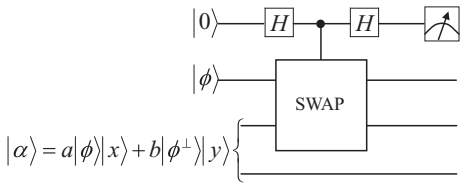

FIG. 2. The comparing circuit where one particle is in an entangled state.

particle. By tracing through the execution of this circuit, one can determine that the final state before the measurement is

$$a|0\rangle|\phi\rangle|\phi\rangle|x\rangle + \frac{b}{2}|0\rangle(|\phi\rangle|\phi^{\perp}\rangle + |\phi^{\perp}\rangle|\phi\rangle)|y\rangle + \frac{b}{2}|1\rangle(|\phi\rangle|\phi^{\perp}\rangle - |\phi^{\perp}\rangle|\phi\rangle)|y\rangle. \quad (4)$$

Measuring the first qubit of this state produces outcome $|1\rangle$ with probability $\frac{|b|^2}{2}$. This probability is 0 if and only if $b = 0$, that is, $|\alpha\rangle = |\phi\rangle|x'\rangle$. Thus, the test determines which case holds with the one-sided error $1 - \frac{|b|^2}{2}$.

C. An example using the arbitrated signature

Now, we give an example that we need the arbitrated signature in our real life (a similar example can be found in Ref. [29]).

Example 1. Bob is selling a car to Alice, a stranger. Alice wants to pay by check, but Bob has no way of knowing if the check is good. Bob wants the check to be cleared before he turns the title over to Alice. Alice, who does not trust Bob any more than he trusts her, does not want to hand over a check without receiving a title.

Bankers trusted by both of them can arbitrate protocols. Alice can use a certified check to buy a car from Bob:

(1) Alice writes a check and gives it to the bank.

(2) After putting enough of Alice's money on hold to cover the check, the bank certifies the check and gives it back to Alice.

(3) Bob gives the title to Alice and Alice gives the certified check to Bob.

(4) Bob deposits the check.

This protocol works because Bob trusts the banker's certification. Bob trusts the bank to hold Alice's money for him.

III. SECURITY ANALYSIS OF THE EXISTING AQS SCHEMES

A secure arbitrated (quantum) signature scheme should satisfy two conditions: one is that the signature should not be forged by the attacker (including the malicious receiver) and the other is the impossibility of disavowal by the signatory and the receiver [13,14,25]. However, in the following, we will show that the signature of the existing schemes [13,14,25] can be disavowed by the receiver Bob.

A. The AQS scheme using Bell states [14]

In the interest of readability, we briefly recall the AQS scheme using Bell states [14], and the details can be found in Ref. [14]. The scheme involves three participants, namely, the signatory Alice, the receiver Bob, and the arbitrator Trent, and includes three phases, the initializing phase, the signing phase, and the verifying phase.

1. Initializing phase

Step I1. Alice shares her secret key K_A with the arbitrator through quantum key distribution protocols [2–4], which were proved to be unconditionally secure [5,6]. Likewise, Bob obtains his secret key K_B shared with the arbitrator.

Step I2. The arbitrator that should be trusted by both Alice and Bob generates n Bell states $|\psi\rangle = (|\psi_1\rangle,|\psi_2\rangle,\ldots,|\psi_n\rangle)$ with $|\psi_i\rangle = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$, where the subscripts A and B correspond to Alice and Bob, respectively. Then the arbitrator distributes one particle of each Bell state to Alice and the other to Bob employing a secure and authenticated method [11,12].

2. Signing phase

Step S1. Alice obtains a qubit string $|P\rangle = (|P_1\rangle,|P_2\rangle,\ldots,|P_n\rangle)$ related to the message $|P_i\rangle = \alpha_i|0\rangle + \beta_i|1\rangle$. Here note that if the known quantum states are to be signed, then an arbitrary number of copies of $|P\rangle$ can be prepared, whereas, if the quantum states to be signed are unknown, then three copies of $|P\rangle$ are necessary (one to be combined with the Bell states, one to produce the secret qubit string $|R_A\rangle$, and the other to be sent to Bob). However, if the dimension of $|P\rangle$ is not sufficiently large, more copies are needed to obtain a lower error probability of comparison tests for unknown quantum states and then reduce the failure probability of the verifying phase.

Step S2. Alice transforms the qubit string $|P\rangle$ into a secret qubit string $|R_A\rangle$ in terms of the key K_A. For instance,

$$|R_A\rangle = M_{K_A}(|P\rangle).$$

Step S3. Alice combines each message state and the Bell state by carrying out a joint measurement on both states and obtains the three-particle entangled state,

$$|\phi_i\rangle = |P_i\rangle \otimes |\psi_i\rangle \quad (5)$$

$$= \tfrac{1}{2}[|\Psi_{12}^{+}\rangle_A(\alpha_i|0\rangle_B + \beta_i|1\rangle_B) + |\Psi_{12}^{-}\rangle_A(\alpha_i|0\rangle_B - \beta_i|1\rangle_B) + |\Phi_{12}^{+}\rangle_A(\alpha_i|1\rangle_B + \beta_i|0\rangle_B) + |\Phi_{12}^{-}\rangle_A(\alpha_i|1\rangle_B - \beta_i|0\rangle_B)], \quad (6)$$

where $|\Psi_{12}^{+}\rangle_A,|\Psi_{12}^{-}\rangle_A,|\Phi_{12}^{+}\rangle_A$, and $|\Phi_{12}^{+}\rangle_A$ are the four Bell states [30].

Step S4. Alice implements Bell measurement on each three-particle entangled state $|\phi_i\rangle$ and obtains $\mathcal{M}_A = (\mathcal{M}_A^1,\mathcal{M}_A^2,\ldots,\mathcal{M}_A^n)$, where $\mathcal{M}_A^i$ represents one of the four Bell states.

Step S5. Alice generates the signature $|S\rangle = E_{K_A}(\mathcal{M}_A,|R_A\rangle)$ of the message $|P\rangle$ by encrypting $\mathcal{M}_A$ and $|R_A\rangle$ with the secret key K_A using the quantum one-time pad algorithm [27]. Note that $\mathcal{M}_A$, even if sometimes depicted by classical bits, can be transformed into qubits $|\mathcal{M}_A\rangle$ according to the Bell basis. Then both $|\mathcal{M}_A\rangle$ and $|R_A\rangle$ can be encrypted by quantum one-time pad algorithms [27].

Step S6. Alice transmits the signature $|S\rangle$ followed by the message $|P\rangle$ to Bob.

3. Verifying phase

Step V1. Bob encrypts $|S\rangle$ and $|P\rangle$ using the key K_B and sends the resultant outcomes $|Y_B\rangle = E_{K_B}(|S\rangle,|P\rangle)$ to the arbitrator.

Step V2.The arbitrator decrypts $|Y_B\rangle$ with K_B and gets $|S\rangle$ and $|P\rangle$. Then he decrypts $|S\rangle$ using K_A and obtains $\mathcal{M}_A$

and $|R'_A\rangle$ which should be compared with $|R_A\rangle = M_{K_A}(|P\rangle)$. If $|R'_A\rangle = |R_A\rangle$, the arbitrator sets the verification parameter $V = 1$; otherwise he sets $V = 0$.

Notice that this step includes quantum state comparison which was discussed in detail in Ref. [14] and Sec. II.

Step V3. The arbitrator obtains $|P\rangle$ from $|R_A\rangle$ according to the key K_A.

Step V4. The arbitrator sends the encrypted results $|Y_{TB}\rangle = E_{K_B}(\mathcal{M}_A, |S\rangle, |P\rangle, V)$ to Bob.

Step V5. Bob decrypts $|Y_{TB}\rangle$ and obtains $\mathcal{M}_A$, $|S\rangle$, $|P\rangle$, and V. If $V = 0$, Bob considers that the signature has been obviously forged and rejects it; otherwise, Bob goes on to the further verification.

Step V6. According to Alice's measurement outcomes $\mathcal{M}_A$ and Eq. (6), Bob obtains $|P'\rangle$ by implementing the corresponding transformations denoted as Eq. (7) on his particles of the Bell states:

$$|\Psi_{12}^+\rangle \to I, |\Psi_{12}^-\rangle \to \sigma_z, |\Phi_{12}^+\rangle \to \sigma_x, |\Phi_{12}^-\rangle \to \sigma_z\sigma_x. \quad (7)$$

For example, if Alice's measurement result is $|\Psi_{12}^+\rangle_A$, then the state in Bob's hand must be $\alpha_i|0\rangle_B + \beta_i|1\rangle_B$. Thus Bob can obtain $|P'\rangle$ by applying the identity transformation I. The other transformations can be elaborated in a similar way. Then he makes comparisons between $|P'\rangle$ and $|P\rangle$. Here the way of comparing $|P'\rangle$ and $|P\rangle$ is the same as that of comparing $|R'_A\rangle$ and $|R_A\rangle$ in Step V2. If $|P'\rangle = |P\rangle$, Bob accepts the signature $|S\rangle$ of the message $|P\rangle$; otherwise he rejects it.

B. Security analysis of the AQS schemes using Bell states in Ref. [14]

Here, we show that the signature of the AQS scheme using Bell states in Ref. [14] can be disavowed by Bob. Suppose the receiver Bob repudiates the receipt of the signature. Then, the arbitrator Trent also can confirm that Bob has received the signature $|S\rangle$ since he needs the assistance of Trent to verify the signature. For instance, the information of his key K_B is included in $|Y_B\rangle = E_{K_B}(|S\rangle, |P\rangle)$. Therefore Bob cannot disavow that he has received $|S\rangle$.

However, *Bob can repudiate the integrality* of the signature $|S\rangle$ because he can reject the signature in Step V6. Repudiating the integrality of the signature means that Bob admits receiving some signature $|S\rangle$ but denies the signature $|S\rangle$ being correct, that is, Bob can claim $|P'\rangle \neq |P\rangle$ and reject the signature $|S\rangle$ when $|P'\rangle = |P\rangle$. The case $|P'\rangle \neq |P\rangle$ can happen if Alice generates $|\phi_i\rangle$ by another message $|P'\rangle$ with $|P'\rangle \neq |P\rangle$ in Step S3 or lets $|S\rangle = E_{K_A}(\mathcal{M}'_A, |R_A\rangle)$ with $\mathcal{M}'_A \neq \mathcal{M}_A$ in Step S5. Note that the arbitrator Trent could not check whether the $\mathcal{M}_A$ in $|S\rangle$ is correct or not.

When Bob claims $|P'\rangle \neq |P\rangle$ in Step V6, one or more of the following three cases must have happened:

(1) Bob told a lie;

(2) Alice generated $|\phi_i\rangle$ by another message $|P'\rangle$ with $|P'\rangle \neq |P\rangle$ in Step S3 or made $|S\rangle = E_{K_A}(\mathcal{M}'_A, |R_A\rangle)$ with $\mathcal{M}'_A \neq \mathcal{M}_A$ in Step S5;

(3) Eve disturbed $|S\rangle$, $|Y_B\rangle$ or $|Y_{TB}\rangle$.

However, Trent and all the other people cannot confirm which case has happened indeed. Therefore, Bob can disavow the signature in the AQS scheme [14].

Example 2. As in Example 1, Bob is selling a car to Alice. Alice wants to pay by check, but Bob has no way of knowing if the check is good. Bob wants the check to be cleared before he turns the title over to Alice. Alice, who does not trust Bob any more than he trusts her, does not want to hand over a check without receiving a title. The banker Trent trusted by both of them arbitrates the scheme. When it is in the quantum era, Alice may use a quantum digital check to buy a car from Bob. If they trade by the AQS scheme in Ref. [14], the following case maybe happen.

Alice says she has signed a quantum check $|P\rangle$ for Bob. But, Bob says he has not received the correct quantum signature $|S\rangle$ of the quantum check $|P\rangle$ from Alice because he found $|P'\rangle \neq |P\rangle$ in Step V6. Due to the shortcoming of the AQS scheme in Ref. [14], the arbitrator Trent and all the other people cannot judge which one of the following cases has happened:

(1) Bob received Alice's correct signature for $|P\rangle$ but told a lie;

(2) Alice deliberately did not send the correct signature $|S\rangle$;

(3) Eve disturbed $|S\rangle$, $|Y_B\rangle$, or $|Y_{TB}\rangle$.

From the preceding discussion and Example 2, Bob can repudiate the integrality of the signature in the AQS schemes in Ref. [14]. Similarly, the signature of the AQS schemes in Refs. [13,25] can be disavowed by Bob.

C. The AQS scheme using GHZ states [13,25]

Also, we simply recall the AQS scheme using GHZ states [13,25], and the details can be found in Refs. [13,25]. The scheme involves three participants, namely, the signatory Alice, the receiver Bob, and the arbitrator Trent, and includes three phases, the initializing phase, the signing phase, and the verifying phase.

1. Initializing phase

Step I1. Alice shares the secret key K_A with the arbitrator Trent by the quantum key distribution protocols [2–4] that were proved to be unconditionally secure [5–9]. Similarly, Bob shares the secret key K_B with Trent. The lengths of these keys depend on the chosen cryptographic algorithms in the signing and verifying phases.

Step I2. The arbitrator Trent that should be trusted by both Alice and Bob generates n GHZ states $|\psi\rangle = (|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_n\rangle)$ with $|\psi_i\rangle = \frac{1}{\sqrt{2}}(|000\rangle_{ABT} + |111\rangle_{ABT})$, where the subscripts A, B, and T correspond to Alice, Bob, and Trent, respectively. Then, Trent distributes the first particle of each GHZ state to Alice and the second to Bob.

2. Signing phase

Step S1. Alice presents three copies of the message state $|P\rangle = (|P_1\rangle, |P_2\rangle, \ldots, |P_n\rangle)$ related to the message $|P_i\rangle = \alpha_i|0\rangle + \beta_i|1\rangle$.

Step S2. Alice generates a random string $|R\rangle = M_{K_A}(|P\rangle) = (|R_1\rangle, |R_2\rangle, \ldots, |R_n\rangle)$.

Step S3. Alice obtains a four-particle state $|\phi_i\rangle$ via entangling the message state $|P_i\rangle$ and the GHZ state $|\psi\rangle$ according

to the equation

$$|\phi_i\rangle = |P_i\rangle \otimes |\psi_i\rangle \tag{8}$$

$$\begin{aligned} = \tfrac{1}{2}[&|\Psi_{12}^{+}\rangle_A(\alpha_i|00\rangle_{TB} + \beta_i|11\rangle_{TB}) \\ &+ |\Psi_{12}^{-}\rangle_A(\alpha_i|00\rangle_{TB} - \beta_i|11\rangle_{TB}) \\ &+ |\Phi_{12}^{+}\rangle_A(\alpha_i|11\rangle_{TB} + \beta_i|00\rangle_{TB}) \\ &+ |\Phi_{12}^{-}\rangle_A(\alpha_i|11\rangle_{TB} - \beta_i|00\rangle_{TB})]. \end{aligned} \tag{9}$$

Step S4. Alice executes Bell measurement on $|\phi_i\rangle$ and obtains the results $\mathcal{M}_A = (\mathcal{M}_A^1, \mathcal{M}_A^2, \ldots, \mathcal{M}_A^n)$, where $\mathcal{M}_A^i$ may be any of the four Bell states in $\{|\Psi_{12}^{+}\rangle, |\Psi_{12}^{-}\rangle, |\Phi_{12}^{+}\rangle, |\Phi_{12}^{-}\rangle\}$.

Step S5. Alice creates the signature $|S\rangle = K_A(\mathcal{M}_A, |R\rangle)$ of the message $|P\rangle$ using a quantum symmetrical key cryptosystem, for example, the quantum one-time pad algorithm [27].

Step S6. Alice sends the string of message $|P\rangle$ followed by the signature $|S\rangle$ to Bob.

3. *Verifying phase*

Step V1. Bob measures his GHZ particles and obtains the results $\mathcal{M}_B$, then he encrypts $\mathcal{M}_B$, $|S\rangle$, and $|P\rangle$ with his key K_B to obtain $|Y_B\rangle = K_B(\mathcal{M}_B, |S\rangle, |P\rangle)$. After that Bob sends $|Y_B\rangle$ to the arbitrator.

Step V2. The arbitrator gets $\mathcal{M}_B$, $|S\rangle$, and $|P\rangle$ via decrypting the received $|Y_B\rangle$. Then, he gets $\mathcal{M}_A$ and $|R'\rangle$ via decrypting $|S\rangle$. Furthermore, he generates a verification parameter V as

$$V = \begin{cases} 1, & \text{if } |R'\rangle = |R\rangle = M_{K_A}(|P\rangle); \\ 0, & \text{if } |R'\rangle \neq |R\rangle = M_{K_A}(|P\rangle). \end{cases} \tag{10}$$

Step V3. The arbitrator sends his GHZ particles, $|P\rangle$, and the encrypted result $|Y_{TB}\rangle = K_B(\mathcal{M}_A, \mathcal{M}_B, V, |S\rangle)$ to Bob.

Step V4. Bob obtains the arbitrator's GHZ particles. In addition, Bob obtains $\mathcal{M}_A$, $\mathcal{M}_B$, $|S\rangle$, and V via decrypting the received $|Y_{TB}\rangle$.

Step V5. Bob undertakes the first verification for Alice's signature $|S\rangle$ via the parameter V. If $V = 0$, the signature has obviously been forged and Bob may reject the message $|P\rangle$ immediately. If $V = 1$, Bob goes on to further verification in the next step.

Step V6. Bob performs the further verification via comparing $|P\rangle$ and $|P'\rangle$, where $|P'\rangle$ is obtained according to the correlation of the GHZ triplet state. If $|P'\rangle = |P\rangle$, the signature is completely correct and Bob accepts $|P\rangle$; otherwise, he should reject it.

D. Security analysis of the AQS schemes using GHZ states in Refs. [13,25]

Similar to the signature of the AQS scheme using Bell states [14], the signature of the AQS scheme using GHZ states [13,25] can be disavowed by the receiver Bob too.

Suppose receiver Bob repudiates the receipt of the signature. Then, the arbitrator Trent also can confirm that Bob has received the signature $|S\rangle$ since he needs the assistance of Trent to verify the signature. For instance, the information of his key K_B is included in $|Y_B\rangle = K_B(\mathcal{M}_B, |S\rangle, |P\rangle)$. So Bob cannot disavow that he has received $|S\rangle$. However, Bob can repudiate the integrality of the signature $|S\rangle$ because he can reject the signature in Step V6, that is, Bob can claim $|P'\rangle \neq |P\rangle$ and reject the signature $|S\rangle$ when $|P'\rangle = |P\rangle$. The case $|P'\rangle \neq |P\rangle$ can happen if Alice generates $|\phi_i\rangle$ by another message $|P'\rangle$ with $|P'\rangle \neq |P\rangle$ in Step S3 or lets $|S\rangle = K_A(\mathcal{M}'_A, |R\rangle)$ with $\mathcal{M}'_A \neq \mathcal{M}_A$ in Step S5. Note that the arbitrator Trent could not check whether the $\mathcal{M}_A$ in $|S\rangle$ is correct or not.

When Bob claims $|P'\rangle \neq |P\rangle$ in Step V6, one or more of the following three cases must have happened:

(1) Bob received Alice's correct signature for $|P\rangle$ but told a lie;

(2) Alice deliberately did not send the correct signature $|S\rangle$;

(3) Eve disturbed $|S\rangle$, $|Y_B\rangle$, or $|Y_{TB}\rangle$.

However, Trent and all the other people cannot confirm which case has happened indeed. Therefore, Bob can disavow the signature in the AQS scheme [13,25].

From the analysis above, we know that the existing AQS schemes cannot be applied because the signature can be disavowed by the receiver. Are there some techniques to improve the AQS schemes to avoid being disavowed for the integrality of the signature by the receiver Bob? In the following section, we will give a new AQS scheme which cannot be disavowed by the receiver.

IV. AQS SCHEME 1: AN AQS SCHEME CANNOT BE DISAVOWED BY BOB

We have known that the existing AQS schemes [13,14] cannot avoid being disavowed for the integrality of the signature by Bob. In this section, we will present a new AQS scheme that can avoid being disavowed for the integrality of the signature by the receiver Bob.

Note that the QKD schemes [2–4] utilize generally a public board or a classical public communications channel that cannot be blocked. Lee *et al.* [16] proposed an AQS scheme with a public board which can be adapted to sign classical messages. Also, we use a public board or a classical channel that cannot be blocked to improve the AQS schemes to avoid being disavowed for the integrality of the signature by Bob. Note that a public board and a classical public communications channel are assumed to be susceptible to eavesdropping but not to the injection or alteration of messages [2–4]. To avoid being disavowed by Bob, we must set that he cannot obtain whole signature when he verifies Alice's signature.

From Ref. [14], we know that the AQS scheme using Bell states [14] can preserve the merits in the AQS scheme using GHZ states [13,25] while providing a higher efficiency in transmission and reducing the complexity of implementation. Therefore, we improve the AQS scheme using Bell states such that its signature cannot be disavowed by Bob.

The presented scheme also involves three participants, namely, the signatory Alice, the receiver Bob, and the arbitrator Trent, and includes three phases, the initializing phase, the signing phase, and the verifying phase.

Suppose Alice needs to sign the quantum message $|P\rangle = |P_1\rangle \otimes |P_2\rangle \otimes \cdots \otimes |P_n\rangle$ with $|P_i\rangle = \alpha_i|0\rangle + \beta_i|1\rangle$ and has at least three copies of $|P\rangle$. To obtain a low enough error probability in the verifying phase, we can suppose that n is large enough; otherwise, we can use $|P\rangle^{\otimes m}$ instead of $|P\rangle$, where m is a large enough integer.

The AQS scheme is specified in the following.

A. Initializing phase

Step I1. Alice shares the secret key K_A with the arbitrator Trent by the quantum key distribution protocols [2–4] that were proved to be unconditionally secure [5–9]. Similarly, Bob shares the secret key K_B with Trent.

Step I2. Alice generates n Bell states $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$ with $|\psi_i\rangle = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$, where the subscripts A and B correspond to Alice and Bob, respectively. Then, Alice distributes one particle of each Bell state to Bob by employing a secure and authenticated method [11,12]. Alice and Bob can share n Bell sates of almost perfect fidelity even if they are far away from each other [5] through the use of quantum repeaters [31,32] and fault-tolerant quantum computation [33,34].

B. Signing phase

Step S1. Alice randomly chooses a number $r \in \{0,1\}^{2n}$ and transforms all $|P\rangle$ into secret qubit strings $|P'\rangle = E_r(|P\rangle)$.

Step S2. Alice generates $|S_A\rangle = E_{K_A}(|P'\rangle)$.

Step S3. Alice combines each secret message state $|P'_i\rangle$ and the Bell state and obtains the three-particle entangled state,

$$|\phi_i\rangle = |P'_i\rangle \otimes |\psi_i\rangle \tag{11}$$

$$\begin{aligned} &= \tfrac{1}{2}[|\Psi^+_{12}\rangle_A(\alpha'_i|0\rangle_B + \beta'_i|1\rangle_B) \\ &\quad + |\Psi^-_{12}\rangle_A(\alpha'_i|0\rangle_B - \beta'_i|1\rangle_B) \\ &\quad + |\Phi^+_{12}\rangle_A(\alpha'_i|1\rangle_B + \beta'_i|0\rangle_B) \\ &\quad + |\Phi^-_{12}\rangle_A(\alpha'_i|1\rangle_B - \beta'_i|0\rangle_B)], \end{aligned} \tag{12}$$

where $|\Psi^+_{12}\rangle_A, |\Psi^-_{12}\rangle_A, |\Phi^+_{12}\rangle_A$, and $|\Phi^+_{12}\rangle_A$ are the four Bell states [30] and $|P'\rangle = \alpha'_i|0\rangle_B + \beta'_i|1\rangle_B$.

Step S4. Alice implements Bell measurement on her two particles of each three-particle entangled state $|\phi_i\rangle$ and obtains $|\mathcal{M}_A\rangle = (|\mathcal{M}^1_A\rangle, |\mathcal{M}^2_A\rangle, \ldots, |\mathcal{M}^n_A\rangle)$, where $|\mathcal{M}^i_A\rangle$ represents one of the four Bell states. We would use quantum one-time pads encryption in the following, so, for convenience, we use the notation $|\mathcal{M}_A\rangle$ instead of $\mathcal{M}_A$.

Step S5. Alice transfers $|S\rangle = (|P'\rangle, |S_A\rangle, |\mathcal{M}_A\rangle)$ to Bob.

C. Verifying phase

Step V1. Bob encrypts $|P'\rangle$ and $|S_A\rangle$ using the key K_B and sends the result $|Y_B\rangle = E_{K_B}(|P'\rangle, |S_A\rangle)$ to Trent.

Step V2. Trent decrypts $|Y_B\rangle$ with K_B and gets $|P'\rangle$ and $|S_A\rangle$. Then he encrypts $|P'\rangle$ using K_A and obtains $|S_T\rangle$ which should be consistent with $|S_A\rangle$. If $|S_T\rangle = |S_A\rangle$, he sets the verification parameter $V = 1$; otherwise, he sets $V = 0$.

This step includes quantum state comparison. The technique of comparing two unknown quantum states was first presented in Ref. [28]. Then, this method was improved and specified in Ref. [14].

Step V3. Trent gets back $|P'\rangle$ from one of $|S_A\rangle$ (i.e., $|S_T\rangle$). Then, he sends the encrypted results $|Y_T\rangle = E_{K_B}(|P'\rangle, |S_A\rangle, V)$ to Bob.

Step V4. Bob decrypts $|Y_T\rangle$ and obtains $|S_A\rangle$, $|P'\rangle$, and V. If $V = 0$, Bob considers that the signature has been obviously forged and rejects it; otherwise, Bob goes on to the further verification.

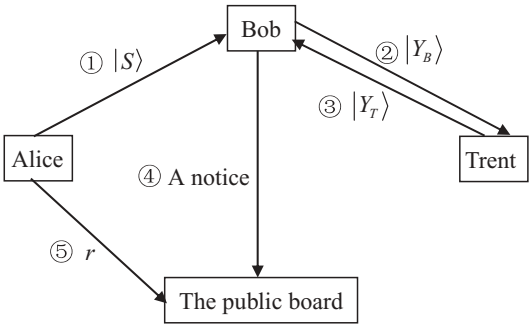

FIG. 3. The communications of the AQS Scheme 1.

Step V5. According to Alice's measurement outcomes $\mathcal{M}_A$ and the principle of teleportation, Bob obtains $|P'_B\rangle$ [10,14]. Then he makes comparisons between $|P'_B\rangle$ and $|P'\rangle$. Here the way of comparing $|P'_B\rangle$ and $|P'\rangle$ is the same as that of comparing $|S_T\rangle$ and $|S_A\rangle$ in Step V2. If $|P'_B\rangle \neq |P'\rangle$, Bob rejects the signature; otherwise, he informs Alice by the public board to publish r.

Step V6. Alice publishes r by the public board.

Step V7. Bob gets back $|P\rangle$ from $|P'\rangle$ by r and holds $(|S_A\rangle, r)$ as Alice's signature for the quantum message $|P\rangle$.

The communications in AQS Scheme 1 are described in Fig. 3.

We have given an AQS scheme using Bell states such that its signature cannot be disavowed by Bob. Similarly, we can improve the AQS scheme using GHZ states [13,25] such that its signature cannot be disavowed by Bob. To make the signature of the AQS scheme which uses GHZ states and cannot be disavowed by Bob, we only need to do the following two things:

(1) In the signing phase, Alice first chooses a random number $r \in \{0,1\}^{2n}$ and transforms all $|P\rangle$ into secret qubit strings $|P'\rangle = E_r(|P\rangle)$. Then, we use $|P'\rangle$ instead of $|P\rangle$ in all following steps.

(2) In the verifying phase, Bob informs Alice by the public board to publish r after he finishes his verifying. Then, Alice publishes r by the public board. Finally, Bob gets back $|P\rangle$ from $|P'\rangle$ by r and holds $(|S_A\rangle, r)$ as Alice's signature for the quantum message $|P\rangle$.

In order to achieve a higher efficiency in transmission, we can do the following improvement:

(3) In Step V1, Bob does not send his measuring result $|\mathcal{M}_B\rangle$ to the arbitrator (i.e., $|Y_B\rangle = K_B(|S\rangle, |P\rangle)$) and Trent need not send it back (i.e., $|Y_{TB}\rangle = K_B(|\mathcal{M}_A\rangle, V, |S\rangle)$). In addition, the arbitrator informs Alice and Bob by the public board to abort the scheme if he found the signature being forged.

V. SECURITY ANALYSIS OF AQS SCHEME 1

A secure quantum signature scheme should satisfy two requirements [13,14,25]: the signature should not be forged by the attacker (including the malicious receiver); the signature should not be disavowed by the signatory and the receiver.

We can show that the proposed AQS scheme can satisfy the two requirements.

A. Impossibility of forgery

If the attacker Eve tries to forge Alice's signature $|S_A\rangle$ for her own sake, she should know the secret keys K_A. However, this is impossible due to the unconditional security of quantum key distribution [5–9]. Besides, the use of a quantum one-time pad algorithm [27] enhances the security. Hence, the forgery for Eve is impossible.

If the malicious receiver Bob attempts to counterfeit Alice's signature $|S_A\rangle = E_{K_A}(|P'\rangle)$ to his own benefit, he also has to know Alice's secret key K_A to construct $|S_A\rangle$. However, the information that he can obtain betrays nothing about the secret keys K_A. Thus, Bob cannot get the correct $|S_A\rangle$. Therefore, he cannot forge Alice's signature.

In the worse situation, for instance, in which the secret key K_A is exposed to Eve, Eve still cannot forge the signature since she cannot create the appropriate $|\mathcal{M}_A\rangle$ related to the new message. Bob would find such forgery using the correlation of the Bell states because the further verification about $|P'_B\rangle = |P'\rangle$ could not hold without the correct $|\mathcal{M}_A\rangle$. But note that if Bob knows the key K_A, such forgery will not be avoided.

B. Impossibility of disavowal by the signatory and the receiver

If the signatory Alice and the receiver Bob disagree with each other, the arbitrator Trent trusted by both of them should be required to make a judgment.

Assume that Alice disavows her signature. Then, Trent can confirm that Alice has signed the message since the information of Alice's secret key K_A is involved in $|S_A\rangle$ of the signature $|S_A\rangle = E_{K_A}(|P'\rangle)$. Hence Alice cannot deny having signed the message.

Now, we show the signature cannot be disavowed by the receiver. It is clear that Bob must have received $|S\rangle = (|P'\rangle,|S_A\rangle,|\mathcal{M}_A\rangle)$ and known the secret key K_B by Step V2 and Step V5. By Step V4 and Step V5, we know $|S_A\rangle = E_{K_A}(|P'\rangle)$ and Bob can get $|P'_B\rangle$ with $|P'_B\rangle = |P'\rangle$ by using $|\mathcal{M}_A\rangle$. In addition, Bob can get r by Step V6 because the public board (or a classical public communications channel) cannot be blocked and is assumed not to be the injection or alteration of messages. From the aforementioned analysis, Bob can not disavow the receipt of $|S\rangle = (|P'\rangle,|S_A\rangle,|\mathcal{M}_A\rangle)$ and the random number r. This means that Bob cannot disavow the signature.

Especially, Bob could not claim $|P'_B\rangle \neq |P'\rangle$ when $|P'_B\rangle = |P'\rangle$ because he needs to recover the message $|P\rangle$. If Bob claims $|P'_B\rangle \neq |P'\rangle$, then he has not received the correct message $(|P'\rangle,|S_A\rangle,|\mathcal{M}_A\rangle)$.

C. Further discussion

Eve (or Alice) may use the following attack strategy to modify the quantum message $|P\rangle$. Eve (or Alice) uses some auxiliary quantum state $|Q\rangle$ that is entangled with $|P'\rangle$ which is the state sent to Bob in Step S5. After Bob finishes his verifying, Eve (or Alice) manipulates $|P'\rangle$ by operating on $|Q\rangle$. Can this strategy be a threat to the proposed scheme? The attack strategy is the same as the situation described in Fig. 2. From the discussion in Sec. II B, the probability of the measuring result being $|1\rangle$ is 0 if and only if $|\alpha\rangle = |\phi\rangle|x'\rangle$. This means $|\alpha\rangle$ is a product state. Therefore, Trent and Bob could find that there exists entanglement in Steps V2 and V5, respectively, if Eve (or Alice) attacked the presented AQS scheme by the strategy. Thereby, Eve (or Alice) cannot control $|P'\rangle$ by quantum entanglement if she wants to escape being found. This means that the proposed AQS scheme is robust against this strategy.

In the AQS scheme, Alice should publish the parameter r in the public board after Bob has finished his operations for verification. Somebody may worry that Alice does not put the correct r in the public board and Bob could not obtain the correct message $|P\rangle$. Yes, our AQS scheme gives Alice a chance to put any parameter r' (it may be not equal to r) in the public board. However, it is possible only that Alice can sign any quantum message. We could not limit Alice to sign any quantum message. If Alice puts a parameter r' with $r' \neq r$ in the public board, the receiver Bob and the arbitrator Trent only accept Alice's signature $(|S_A\rangle,r')$ for $E_{r'}^{-1}(E_r(|P\rangle))$ but not for $|P\rangle$. If Alice wants to send the message $|P\rangle$ with her signature of $|P\rangle$ to Bob, then she could only publish the correct parameter r.

Can any attacker change the parameter r to make it so Bob cannot receive the correct message $|P\rangle$? Note that, the public board (or the classical public communications channel) is assumed not to be blocked and not to be the injection or alteration of messages [2–4]. So, it would not happen.

Statement 1. It is necessary that Alice only send $|P'\rangle$ in the scheme. Bob can confirm that $|S_A\rangle$ is Alice's signature and get $|P\rangle$ in Step V5 if we use $|P\rangle$ instead of $|P'\rangle$ in the scheme. So, Bob does not need the random number r. This means that Bob has a chance to disavow the integrality of the signature as in the AQS schemes in Refs. [13,14].

Statement 2. If Bob does not receive the random number r, he cannot recover the message $|P\rangle$ by the security of the quantum one-time pad [27].

From the preceding discussion, the proposed AQS scheme is secure.

VI. AQS SCHEME 2: A SCHEME WITHOUT USING ENTANGLED STATES

Using present-day technologies, the preparation, distribution, and keeping of quantum entangled states are not easily implemented. It can be considered as some improvement that, to achieve some functions, a quantum scheme uses less or simpler quantum entangled states than the original scheme. For example, to construct an AQS scheme, Ref. [14] uses simpler two-particle entangled Bell states to replace three-particle entangled GHZ states in Ref. [13]. From the arbitrated quantum signature schemes in Refs. [13,14,25], we discover that the main functions of quantum entangled states, GHZ states and Bell states, are to assist Alice to transfer quantum states to Bob. However, Alice transfers quantum states to the arbitrator by the ciphertext encrypted with the secret key K_A. Similarly, Alice can transfer quantum states to Bob with a shared secret key. By this idea, we construct a new AQS scheme using a public board which does not use entangled quantum states in the signing phase and the verifying phase.

To avoid being disavowed by Bob, similar to AQS Scheme 1, the new AQS scheme utilizes a public board or a classical public communications channel that cannot be blocked. Note that a public board and a classical public communications channel are assumed to be susceptible to eavesdropping but not to the injection or alteration of messages [2–4].

This new scheme also involves three participants, namely, the signatory Alice, the receiver Bob, and the arbitrator Trent, and includes three phases, the initializing phase, the signing phase, and the verifying phase. Similarly, suppose Alice needs to sign the quantum message $|P\rangle = |P_1\rangle \otimes |P_2\rangle \otimes \cdots \otimes |P_n\rangle$ with $|P_i\rangle = \alpha_i|0\rangle + \beta_i|1\rangle$ and has at least three copies of $|P\rangle$. To obtain a low enough error probability in the verifying phase, we also suppose that n is large enough; otherwise, we use $|P\rangle^{\otimes m}$ instead of $|P\rangle$, where m is a large enough integer.

A. Initializing phase

Step I1′. Alice shares the secret keys K_{AT} and K_{AB} with Trent and Bob, respectively, by using the quantum key distribution protocols [2–4] that were proved to be unconditionally secure [5–9]. Similarly, Bob shares the secret key K_{BT} with Trent.

B. Signing phase

Step S1′. Alice randomly chooses a number $r \in \{0,1\}^{2n}$ and computes $|P'\rangle = E_r(|P\rangle)$ and $|R_{AB}\rangle = M_{K_{AB}}(|P'\rangle)$.

Step S2′. Alice generates $|S_A\rangle = E_{K_{AT}}(|P'\rangle)$.

Step S3′. Alice generates her signature $|S\rangle = E_{K_{AB}}(|P'\rangle,|R_{AB}\rangle,|S_A\rangle)$ and sends it to Bob. If they are far away from each other, they can use quantum repeaters [31,32] and fault-tolerant quantum computation [33,34] to ensure the signature $|S\rangle$ is being transferred perfectly.

C. Verifying phase

Step V1′. Bob decrypts $|S\rangle$ with K_{AB} and gets $|P'\rangle$, $|R_{AB}\rangle$, and $|S_A\rangle$. Then, he generates and sends $|Y_B\rangle = E_{K_{BT}}(|P'\rangle,|S_A\rangle)$ to Trent.

Step V2′. Trent decrypts $|Y_B\rangle$ and obtains $|P'\rangle$ and $|S_A\rangle$ depending on the secret key K_{BT}.

Step V3′. Trent obtains $|P'_T\rangle = E^{-1}_{K_{AT}}(|S_A\rangle)$ and compares it with $|P'\rangle$ using the approach in Refs. [14,28]. If $|P'_T\rangle = |P'\rangle$, he sets the verification parameter $V_T = 1$; otherwise he sets $V_T = 0$. He announces the verification parameter V_T by the public board. If $V_T = 0$, he regenerates $|Y_B\rangle$ and sends it back to Bob.

Step V4′. If $V_T = 0$, Bob rejects the signature; otherwise, Bob decrypts $|Y_B\rangle$ and obtains $|P'\rangle$ and $|S_A\rangle$. Then, he gets $|P'_B\rangle = M^{-1}_{K_{AB}}(|R_{AB}\rangle)$ and compares it with $|P'\rangle$ using the approach in Refs. [14,28]. If $|P'_B\rangle = |P'\rangle$, he sets the verification parameter $V_B = 1$; otherwise he sets $V_B = 0$. He announces the verification parameter V_B by the public board.

Step V5′. If $V_B = 0$, Alice and Trent abort the scheme; otherwise, Alice publishes r by the public board.

Step V6′. Bob gets back $|P\rangle$ from $|P'\rangle$ by r and holds $(|S_T\rangle,r)$ as Alice's signature for the quantum message $|P\rangle$.

The communications in AQS Scheme 2 are described in Fig. 4.

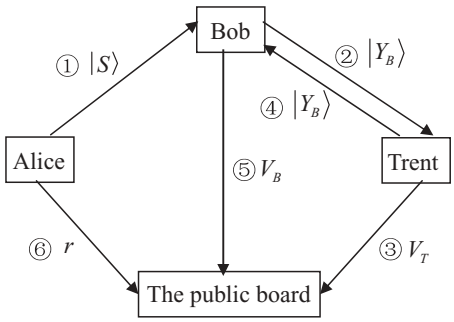

FIG. 4. The communications of AQS Scheme 2.

VII. SECURITY ANALYSIS OF AQS SCHEME 2

The impossibility of forgery of AQS Scheme 2 can be discussed as that of AQS Scheme 1. The quantum key distribution [2–9] and quantum one-time pad algorithm [27] enhance the security of K_{AT}. Thus, Bob and Eve do not know the secret keys K_{AT}. Hence, the forgery is impossible. Similarly, we can prove the impossibility of being disavowed by Alice because the information of Alice's secret key K_{AT} is involved in $|S_A\rangle$. Here, we only discuss the impossibility of being disavowed by the receiver Bob.

If AQS Scheme 2 has ended normally, it is clear that Bob must know the secret key K_{AB} by Step V2′ and $|P'\rangle = M^{-1}_{K_{AB}}(|R_{AB}\rangle)$ by Step V4′. Furthermore, Bob must have the secret key K_{BT} and $|P'\rangle = E^{-1}_{K_{AB}}(|S_T\rangle)$ by Step V2′ and Step V3′. In addition, Bob can obtain the random parameter r and get back $|P\rangle$ from $|P'\rangle$ by Step V6′ and Step V7′ because the public board (or the classical public communications channel) cannot be blocked and is assumed not to be the injection or alteration of messages. By the unconditional security of the QKD [5–9] and the quantum one-time pad [27], other people could not know both K_{AB} and K_{BT}. So, Bob cannot disavow the receipt of the signature $|S\rangle$ and the random number r.

Especially, Bob could not claim $|P'_B\rangle \neq |P'\rangle$ when $|P'_B\rangle = |P'\rangle$ because he needs the random parameter r to recover the message $|P\rangle$. If Bob claims $|P'_B\rangle \neq |P'\rangle$, then he has not received the correct signature $|S\rangle$.

Because we use the same technique to compare unknown quantum states, Eve (or Alice) cannot use auxiliary quantum states to control $|P'\rangle$ by quantum entanglement if she wants to escape being found. Therefore, AQS Scheme 2 is robust against this strategy, too.

Similar to AQS Scheme 1, Alice should publish the parameter r in the public board after Bob's verification. AQS Scheme 2 gives Alice a chance to put any parameter r' (it may be not equal to r) in the public board. However, this only seems that Alice can sign any quantum message. We could not limit Alice to sign any quantum message. If Alice puts a parameter r' with $r' \neq r$ in the public board, the receiver Bob and the arbitrator Trent only accept Alice's signature for $E^{-1}_{r'}(E_r(|P\rangle))$ but not the signature for $|P\rangle$. If Alice wants to send the message $|P\rangle$ with her signature of $|P\rangle$ to Bob, she could only publish the correct parameter r.

Note that the public board (or a classical public communications channel) is assumed not to be blocked and not to be the injection or alteration of messages [2–4]. Therefore, any

TABLE I. Comparison of the transmitted qubits' quantity.

Transmission	The scheme using Bell states [14]	The second proposed scheme
Alice→Bob	$4n$	$3n$
Bob→Trent	$4n$	$2n$
Trent→Bob	$6n+1$	$2n$
Trent publishes	0	1
Bob publishes	0	1
Alice publishes	0	$2n$
Total amount	$14n+1$	$9n+2$

attacker cannot change the parameter r to make Bob not able to receive the correct message $|P\rangle$.

Statement 3. Similar to AQS Scheme 1, it is necessary that we only send $|P'\rangle$ in the scheme. Bob can confirm that $|S\rangle$ is Alice's signature and get $|P\rangle$ in Step V4′ if we use $|P\rangle$ instead of $|P'\rangle$ in the scheme. So, Bob need not ask Alice to publish the random number r that means Bob has a chance to disavow the receipt of the correct signature $|S\rangle$.

VIII. COMPARING AQS SCHEME 2 WITH OTHER AQS SCHEMES

AQS Scheme 2 without using entangled states cannot be disavowed by the receiver Bob while it maintains all other merits of the AQS scheme using Bell states in Ref. [14] and the AQS scheme using GHZ states in Refs. [13,25]. The scheme can be adapted to both known and unknown quantum states and still provides unconditional security by employing QKD techniques [2–10] and quantum one-time pads [27]. Furthermore, AQS Scheme 2 is more efficient in the following two aspects.

One is that the total number of the transmitted qubits (bits), when n-qubit message is signed, is decreased as described in Table I. By Ref. [14], we know that the AQS scheme using Bell states is more efficient than that using GHZ states. So, we only need to compare it with the scheme using Bell states in Ref. [14]. Though Alice needs to publish the $2n$-bit random string r, the total number of the transmitted qubits (bits) decreases more than 35 percent.

Statement 4. When the n-qubit message is signed by AQS Scheme 1, the total number of the transmitted qubits (bits) is $10n+c$, where c is a constant. Therefore, the total number of the transmitted qubits (bits) is less than that of the AQS schemes in Refs. [13,14]. Because we find that $|\mathcal{M}_A\rangle$ is not useful to the arbitrator Trent, Bob does not send $|\mathcal{M}_A\rangle$ to Trent in ASQ Scheme 1.

The other is that the complexity of implementing the scheme is reduced. Though the proposed scheme with a public board needs some local operations, it need not prepare and send Bell states and GHZ states because it does not use entangled states.

From the previous discussions, we conclude that AQS Scheme 2 achieves a higher efficiency in transmission and can be implemented easily.

IX. CONCLUSIONS

In this article, we have shown that the existing AQS schemes [13,14] can be repudiated by the receiver Bob. To conquer this shortcoming, we have constructed two AQS schemes. These two schemes can be adapted to both known and unknown quantum states and still provide unconditional security by employing QKD techniques [2–10] and quantum one-time pads [27]. The proposed AQS schemes use a public board or a classical public communications channel that are assumed to be susceptible to eavesdropping but not to the injection or alteration of messages [2–4].

To avoid being disavowed by Bob, we should set that he cannot obtain the whole signature when he verifies Alice's signature. In the first AQS scheme, Alice only signs an encrypted quantum message. To recover this encrypted message, Bob has to ask Alice to publish the encryption key r. This means Bob has no chance to repudiate the signature. Furthermore, we have found that the measuring result $|\mathcal{M}_A\rangle$ is not useful to the arbitrator Trent in the first presented schemes. Therefore, Bob does not send $|\mathcal{M}_A\rangle$ to Trent in the AQS scheme. This makes the traffic of the scheme be decreased.

In particular, we have discovered that quantum entanglement is not necessary whereas the AQS schemes in Refs. [13,14] and the first proposed AQS scheme depend on entanglement. Therefore, we have presented the second AQS scheme which does not use quantum entangled states in the signing phase and the verifying phase. The second AQS scheme has three advantages. First, it does not utilize entangled states while it can preserve all merits in the first scheme and the existing schemes [13,14]. Second, the signature can avoid being disavowed by the receiver. Third, it provides a higher efficiency in transmission and reduces the complexity of implementation.

ACKNOWLEDGMENTS

The authors are grateful to the referee for invaluable suggestions that help us improve the quality of the article. This work is supported in part by the National Natural Science Foundation (Nos. 60873055 and 61073054), the Natural Science Foundation of Guangdong Province of China (No. 10251027501000004), the Fundamental Research Funds for the Central Universities (No. 10lgzd12), the Program for New Century Excellent Talents in University (NCET) of China, and the project of SQIG at IT, funded by FCT and EU FEDER projects Quantlog POCI/MAT/55796/2004 and QSec PTDC/EIA/67661/2006, IT Project QuantTel, NoE Euro-NF, and the SQIG LAP initiative.

[1] P. W. Shor, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (IEEE, Los Alamitos, 1994), p. 124; SIAM Rev. **41**, 303 (1999).

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

[3] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[4] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[5] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[6] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[7] D. Mayers, J. Assoc. Comput. Mach. **48**, 351 (2001).
[8] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[9] H. Inamori, N. Lütkenhaus, and D. Mayers, Eur. Phys. J. D **41**, 599 (2007).
[10] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, UK, 2000).
[11] H. Barnum, C. Crépeau, D. Gottesman, A. Smith, and A. Tapp, in *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science* (IEEE, Los Alamitos, 2002), p. 449.
[12] M. Curty, D. J. Santos, E. Pérez, and P. García-Fernández, Phys. Rev. A **66**, 022301 (2002).
[13] G. H. Zeng and C. H. Keitel, Phys. Rev. A **65**, 042312 (2002).
[14] Q. Li, W. H. Chan, and D. Y. Long, Phys. Rev. A **79**, 054307 (2009).
[15] D. Gottesman and I. Chuang, e-print arXiv:quant-ph/0105032.
[16] H. Lee, C. Hong, H. Kim, J. Lim, and H. J. Yang, Phys. Lett. A **321**, 295 (2004).
[17] X. Lü and D. G. Feng, in *Proceedings of the First International Symposium on Computational and Information Science* (Springer, Berlin, 2004), p. 1054.
[18] J. Wang, Q. Zhang, and C. J. Tang, in *Proceedings of the Eighth International Conference on Advanced Communication Technology* (IEEE, New York, 2006), p. 1375.
[19] X. J. Wen, Y. Liu, and Y. Sun, Z. Naturforsch. A **62a**, 147 (2007).
[20] G. H. Zeng, M. Lee, Y. Guo, and G. Q. He, Int. J. Quantum. Inform. **5**, 553 (2007).
[21] Y. G. Yang, Chin. Phys. B **17**, 415 (2008).
[22] X. Lü and D. Feng, in *Proceedings of the Seventh International Conference on Advanced Communication Technology* (IEEE, Korea, 2005), p. 514.
[23] Z. Cao and O. Markowitch, in *Proceedings of the Sixth International Conference on Information Technology: New Generations* (IEEE, Las Vegas, 2009), p. 1574.
[24] M. Curty and N. Lütkenhaus, Phys. Rev. A **77**, 046301 (2008).
[25] G. H. Zeng, Phys. Rev. A **78**, 016301 (2008).
[26] D. M. Greenberger, M. A. Horne, and A. Zeilinger, in *Bells Theorem, Quantum Theory, and Conceptions of Universe*, edited by M. Kaftos (Kluwer, Dordrecht, 1989); D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, Am. J. Phys. **58**, 1131 (1990).
[27] P. O. Boykin and V. Roychowdhury, Phys. Rev. A **67**, 042317 (2003).
[28] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, Phys. Rev. Lett. **87**, 167902 (2001).
[29] B. Schneier, *Applied Cryptography: Protocols, Algorthms, and Source Code in C*, 2nd ed. (Wiley & Sons, New York, 1996).
[30] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, Phys. Rev. Lett. **75**, 4337 (1995).
[31] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).
[32] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, Nature (London) **414**, 413 (2001).
[33] D. Aharonov and M. Ben-Or, in *Proceedings of the 29th Annual ACM Symposium on Theory of Computing* (ACM, New York, 1997), p. 176.
[34] P. W. Shor, in *Proceedings of the 37th Symposium on Foundations of Computer Science* (IEEE, Los Alamitos, 1996), p. 56.