Cryptanalysis of the arbitrated quantum signature protocols

Fei Gao,* Su-Juan Qin, Fen-Zhuo Guo, and Qiao-Yan Wen

State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China

(Received 22 June 2011; published 29 August 2011)

As a new model for signing quantum messages, arbitrated quantum signature (AQS) has recently received a lot of attention. In this paper we study the cryptanalysis of previous AQS protocols from the aspects of forgery and disavowal. We show that in these protocols the receiver, Bob, can realize existential forgery of the sender's signature under known message attack. Bob can even achieve universal forgery when the protocols are used to sign a classical message. Furthermore, the sender, Alice, can successfully disavow any of her signatures by simple attack. The attack strategies are described in detail and some discussions about the potential improvements of the protocols are given. Finally we also present several interesting topics on AQS protocols that can be studied in future.

DOI: 10.1103/PhysRevA.84.022344 PACS number(s): 03.67.Dd, 03.67.Ac

I. INTRODUCTION

Cryptography is the approach to protect data secrecy in a public environment. As we know, the security of most classical cryptosystems is based on the assumption of computational complexity and might be susceptible to the strong ability of quantum computation [1,2]. Fortunately, this difficulty can be overcome by quantum cryptography [3]. Different from its classical counterpart, quantum cryptography is the combination of quantum mechanics and cryptography, where the security is ensured by physical principles such as the Heisenberg uncertainty principle and the quantum no-cloning theorem. Now quantum cryptography has attracted a great deal of attention because it can stand against quantum attack. Quite a few branches of quantum cryptography have been studied in recent years, including quantum key distribution (QKD) [4–6], quantum secret sharing [7–9], quantum secure direct communication [10–12], and quantum identity authentication [13,14].

Message authentication and digital signature are important branches of cryptography [15]. The former provides the ability to ensure a message's origin and integrity. It is used to prevent a *third party* from masquerading as the legitimate users or substituting a false message for a legitimate one. The latter can provide not only the ability of message authentication, but also the function of nonrepudiation. It is used mainly to prevent the cheat from the *legitimate users*, including forging the sender's signature by the receiver, and repudiating the signature by the sender.

As we know, the quantum nature makes quantum messages quite different from classical ones. Compared with their counterparts in classical cryptography, the authentication [16–19] and signature [20–24] of a quantum message are more difficult. In Ref. [17], Barnum *et al.* pointed out that if one wants to securely authenticate a quantum message he or she must do a perfect encryption on it. That is to say, anyone else can learn nothing about the content of an authenticated quantum message. Consequently, in a quantum signature protocol, which has the function of authentication, the receiver of a signed quantum message cannot learn anything about the content. However, in an application of signature it is generally necessary for the receiver to learn something about the content of the signed message. As a result, they drew the conclusion that signing a quantum message is impossible.

Though Barnum *et al.*'s conclusion created a serious obstacle for quantum message signature, the study of the quantum signature scheme has not been stopped. In 2002 Zeng and Keitel proposed a pioneering arbitrated quantum signature (AQS) protocol, which can be used to sign both a classical message and a quantum one [20]. In this protocol, the sender (signer), Alice, prepares more than one copy of a quantum message to be signed so that at least one copy among them exists in the signed message in the manner of plaintext. Consequently, the receiver (verifier), Bob, can not only learn the content of the signed quantum message but can also verify the signature with the help of the arbitrator, Trent, which is not contrary to Barnum *et al.*'s conclusion. To verify the validity of a signature, a necessary and important technique, i.e., probabilistic comparison of two unknown quantum states [25], is introduced in Ref. [20]. This work gave an elementary model to sign a quantum message, which overcomes Barnum *et al.*'s limit and is feasible in theory. In 2009 Li *et al.* presented a Bell-states-based AQS protocol, which simplified Zeng *et al.*'s protocol by replacing Greenberger-Horne-Zeilinger states with Bell ones as the carrier [23]. Recently, Zou *et al.* further simplified this protocol by achieving AQS without entangled states [24]. Both of them still preserve the merits in Zeng *et al.*'s protocol.

Cryptanalysis plays an important role in the development of cryptography. It estimates a protocol's security level, finds potential loopholes, and tries to overcome security issues. As pointed out by Lo and Ko, *breaking* cryptographic systems was as important as *building* them [26]. In the study of quantum cryptography, quite a few effective attack strategies have been proposed, such as intercept-resend attacks [27], entanglement-swapping attacks [28,29], teleportation attacks [30], dense-coding attacks [31–33], channel-loss attacks [34,35], denial-of-service attacks [36,37], correlation-extractability attacks [38–40], Trojan horse attacks [41,42], and participant attacks [29,33]. Understanding those attacks will be helpful for us to design new schemes with high security.

*gaofei_bupt@hotmail.com; also at the State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China.

When we analyze the security of a digital signature protocol, we generally pay attention to two important security requirements; i.e., the signature should not be forged by the attacker (including the receiver) and the signer cannot disavow his or her signature. In classical cryptography, as far as the forgery is concerned, the attacks can be classified into the following three models [43]:

(1) *key-only attack*, where the attacker knows only the public verification key;

(2) *known message attack*, where the attacker is given valid signatures for a variety of messages known by the attacker but not chosen by the attacker; and

(3) *adaptive chosen message attack*, where the attacker previously knows signatures on arbitrary messages of the attacker's choice.

Furthermore, the attack generally results in three kinds of results:

(1) *universal forgery*, which results in the ability to forge signatures for any message (also called *total break* if the signing key is obtained);

(2) *selective forgery*, which results in a signature on a message of the attacker's choice; and

(3) *existential forgery*, which results in some valid message and signature pairs not already known to the attacker.

In this paper we study the cryptanalysis of AQS protocols and focus on the forgery by the receiver, Bob, and the repudiation by the signer, Alice. Taking protocols in Refs. [23,24] as examples, we show that, in the circumstance of known message attack, Bob can give lots of existential forgeries of Alice's signature. More seriously, when the protocols are used to sign a classical message, Bob can achieve universal forgery of Alice's signature. Furthermore, Alice can successfully disavow the signature she signed for Bob. Therefore, some improvements on these AQS protocols are urgently needed.

The rest of this paper is organized as follows. In Secs. II and III we respectively analyze the security of AQS protocols in Refs. [23] and [24], where the protocols are briefly recalled and particular attack strategies are demonstrated. Some useful discussions are given in Sec. IV, and Sec. V is our conclusion.

II. ANALYSIS OF THE AQS PROTOCOL WITH BELL STATES

In this section we first introduce the quantum one-time pad algorithm, which is helpful to understand our attack strategies. Then the AQS protocol with Bell states [23] is described briefly and our security analysis follows.

A. Quantum one-time pad

As the analog of the classical one-time pad, the quantum one-time pad (QOTP), also called the quantum Vernam cipher [44], uses classical key bits to encrypt quantum states. This cipher plays an important role in AQS protocols and it is meaningful for us to make it clear. Boykin and Roychowdhury proved that $2n$ random classical bits are both necessary and sufficient for encrypting any unknown state of n qubits in an informationally secure manner [45]. Suppose $|P\rangle = \bigotimes_{i=1}^{n} |p_i\rangle$ is a quantum message composed of n qubits $|p_i\rangle = \alpha_i|0\rangle + \beta_i|1\rangle$, and the key is $K \in \{0,1\}^{2n}$. The QOTP encryption E_K on the quantum message can be described by

$$|C\rangle = E_K|P\rangle = \bigotimes_{i=1}^{n} \sigma_x^{k^{2i}} \sigma_z^{k^{2i-1}} |p_i\rangle, \tag{1}$$

where k^j denotes the jth bit of K, and σ_x and σ_z are Pauli operations. The corresponding decryption D_K is

$$D_K|C\rangle = \bigotimes_{i=1}^{n} \sigma_z^{k^{2i-1}} \sigma_x^{k^{2i}} |c_i\rangle, \tag{2}$$

where $|c_i\rangle$ denotes the ith qubit of the ciphertext $|C\rangle$.

B. AQS protocol with Bell states

The AQS protocol with Bell states [23] is as follows.

1. Initializing phase

Alice and Bob share a key with the arbitrator, Trent, i.e., K_A and K_B respectively, and n Bell states $|\psi_i\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ are shared between Alice and Bob.

2. Signing phase

(S1) Alice obtains three copies of the quantum message $|P\rangle = \bigotimes_{i=1}^{n} |p_i\rangle$ to be signed.

(S2) Using the key K_A, Alice encrypts one copy of $|P\rangle$ into $|R_A\rangle$, where

$$|R_A\rangle = E'_{K_A}|P\rangle = \bigotimes_{i=1}^{n} M_{k_A^i}|p_i\rangle. \tag{3}$$

Here $M_{k_A^i} = \sigma_x$ when k_A^i, the ith bit of K_A, is 0, while $M_{k_A^i} = \sigma_z$ when $k_A^i = 1$.

(S3) Alice performs Bell measurements on each qubit in the second copy of $|P\rangle$ and the corresponding qubit in the Bell states, obtaining the measurement result $|M_A\rangle = \bigotimes_{i=1}^{n} |m_A^i\rangle$, where $|m_A^i\rangle$ are random Bell states. The aim of this step is to send the second copy of the message to Bob by teleportation via the Bell states previously shared between them.

(S4) Alice encrypts $|M_A\rangle$ and $|R_A\rangle$ by K_A, obtaining the signature $|S\rangle = E_{K_A}(|M_A\rangle \otimes |R_A\rangle)$, where E_{K_A} denotes the encryption of QOTP.

(S5) Alice sends the signature and the third copy of message $|S\rangle \otimes |P\rangle$ to Bob.

3. Verifying phase

(V1) Bob encrypts the signed message by QOTP, obtaining $|Y_B\rangle = E_{K_B}(|S\rangle \otimes |P\rangle)$, and sends it to Trent.

(V2) Trent decrypts the received ciphertext with K_B and K_A, obtaining $|P\rangle$, $|M_A\rangle$, and $|R_A\rangle$, and then verifies whether $|R_A\rangle = E'_{K_A}|P\rangle$ by probabilistic comparison of quantum states [25]. If it is, he sets $r = 1$, otherwise $r = 0$.

(V3) Trent recovers $|S\rangle$ and $|P\rangle$ (note that the compared states can be recovered after the comparison if they are indeed equal), reads out (and replicates) Alice's measurement result $|M_A\rangle$, and sends $|Y_{TB}\rangle = E_{K_B}(|M_A\rangle \otimes |S\rangle \otimes |P\rangle \otimes |r\rangle)$ to Bob. Here E_{K_B} denotes the QOTP encryption using the key K_B.

(V4) Bob decrypts the received ciphertext and judges whether $r = 1$. If not, he believes the signature is forged and stops the protocol.

(V5) According to $|M_A\rangle$, Bob can obtain the second copy of the quantum message via the teleportation by Alice. Then he compares it with the copy received from Trent. Bob accepts Alice's signature when they are equal; otherwise he rejects it.

C. Analysis of the AQS protocol with Bell states

Now we analyze how the above protocol achieves the functions of a digital signature. To show this, we begin with the role of the arbitrator, Trent. In this protocol, Trent knows K_A and he can do the comparison whether $|R_A\rangle = E'_{K_A}|P\rangle$ in step V2. When this equation holds, it implies that the signed message has really come from Alice because others do not know K_A. Note that, after the verifying phase, all three copies of the quantum messages will be transmitted to Bob and Trent will have none of them. Furthermore, Trent does not know the content of the quantum message because he cannot read it, owing to its quantum feature. Therefore, by sending his judgment result r to Bob, Trent can only tell Bob whether this signed message originated from Alice. That is to say, if $r = 1$, Trent ensures that Alice sent a certain quantum message (to Bob) but the content is unknown to him.

Based on the above analysis, there must be a way for Trent to resolve disputes between Alice and Bob, though the protocol does not describe it clearly. Otherwise it is just like a protocol for message authentication instead of a digital signature. It is not difficult to imagine the situation where dispute appears, that is, Bob says that Alice signed a message $|\mathcal{P}\rangle$ [46] for him but Alice announces that she did not sign such a message for Bob (maybe she indeed signed a message for Bob before but it is not $|\mathcal{P}\rangle$). In this condition Trent requires Bob to provide the message $|\mathcal{P}\rangle$ and Alice's corresponding signature $|\mathcal{S}\rangle$, decrypts $|\mathcal{S}\rangle$ with K_A (obtaining $|\mathcal{M}_A\rangle$ and $|\mathcal{R}_A\rangle$), and then verifies whether $|\mathcal{R}_A\rangle = E'_{K_A}|\mathcal{P}\rangle$, which is just like the process in step V2. If the comparison result is positive, Trent concludes that $|\mathcal{P}\rangle$ is indeed Alice's signed message and Alice is disavowing her signature. On the contrary, Trent believes the signature is forged by Bob if the result is negative.

1. *Bob's forgery*

Let us see the possibility for Bob to forge a valid signed message of Alice first. As analyzed in Ref. [23], it looks like Bob can counterfeit Alice's signature only when he knows the key K_A because in this condition he can provide $|\mathcal{P}\rangle$ and $|\mathcal{S}\rangle = E_{K_A}(|\mathcal{M}_A\rangle \otimes |\mathcal{R}_A\rangle)$ such that $|\mathcal{R}_A\rangle = E'_{K_A}|\mathcal{P}\rangle$. But K_A is the key shared between Alice and Trent via QKD, which will be kept unknown to Bob. Consequently, it is impossible for Bob to forge Alice's signature in this manner. Then an interesting question arises: is there another way for Bob to give a valid counterfeit of Alice's signature? Equivalently, can Bob successfully forge a signature without K_A? As we know, Bob, as the receiver of Alice's signature, indeed possesses Alice's valid signature of a certain message. Therefore, he has the advantage to perform a known message attack. In the following we show that Bob can achieve existential forgery, where many valid message and signature pairs can be found.

According to the protocol, a valid signature of quantum message P should be in the form of

$$\begin{aligned}|S\rangle &= E_{K_A}(|M_A\rangle \otimes |R_A\rangle) = E_{K_A}(|M_A\rangle \otimes E'_{K_A}|P\rangle)\\ &= E_{K_A}|M_A\rangle \otimes E_{K_A}E'_{K_A}|P\rangle. \end{aligned} \tag{4}$$

Because $E_{K_A}|M_A\rangle$ has no contributions for Trent to resolve disputes, the key point is whether Bob can find a pair of qubit sequences $(|\mathcal{P}\rangle,|\mathcal{S}'\rangle)$ which satisfies the relation

$$|\mathcal{S}'\rangle = E_{K_A}E'_{K_A}|\mathcal{P}\rangle. \tag{5}$$

Note that now Bob does not know K_A, but he has a valid signed message $(|P\rangle,|S\rangle)$, which implies he has a pair $(|P\rangle,|S'\rangle)$ satisfying $|S'\rangle = E_{K_A}E'_{K_A}|P\rangle$. Can Bob find a valid pair $(|\mathcal{P}\rangle,|\mathcal{S}'\rangle)$ from the known $(|P\rangle,|S'\rangle)$? The answer is yes. In fact if Bob performs one Pauli operation on each qubit in $|P\rangle$, obtaining $|\mathcal{P}\rangle$, and the same operation on the corresponding qubit in $|S'\rangle$, obtaining $|\mathcal{S}'\rangle$, the pair $(|\mathcal{P}\rangle,|\mathcal{S}'\rangle)$ will be a valid signed message.

To see it more clearly, suppose $|P\rangle = \bigotimes_{i=1}^{n}|p_i\rangle$. Then $|S'\rangle$ is in the form of $|S'\rangle = \bigotimes_{i=1}^{n}|s'_i\rangle$, where

$$|s'_i\rangle = E_{k_A^{2i-1},k_A^{2i}}E'_{k_A^i}|p_i\rangle. \tag{6}$$

When Bob performs one Pauli operation U_i on every qubit pair $|p_i\rangle$ and $|s'_i\rangle$, he obtains

$$|\mathcal{P}\rangle = \bigotimes_{i=1}^{n} U_i|p_i\rangle \tag{7}$$

$$|\mathcal{S}'\rangle = \bigotimes_{i=1}^{n} U_i E_{k_A^{2i-1},k_A^{2i}}E'_{k_A^i}|p_i\rangle. \tag{8}$$

It is not difficult to see that $E_{k_A^{2i-1},k_A^{2i}}$ is the encryption of QOTP and $E'_{k_A^i}$ is also an encryption with Pauli operations. Therefore, the combination of these two encryptions $E_{k_A^{2i-1},k_A^{2i}}E'_{k_A^i}$ is still an encryption via one of four Pauli operations $\{I,\sigma_x,\sigma_z,\sigma_x\sigma_z\}$, where I is the identity operator and $\sigma_x\sigma_z = -i\sigma_y$. According to the commutative relations among Pauli operations, we have

$$U_i E_{k_A^{2i-1},k_A^{2i}}E'_{k_A^i} = \pm E_{k_A^{2i-1},k_A^{2i}}E'_{k_A^i}U_i, \tag{9}$$

and then

$$|\mathcal{S}'\rangle = \bigotimes_{i=1}^{n}\left(\pm E_{k_A^{2i-1},k_A^{2i}}E'_{k_A^i}U_i|p_i\rangle\right). \tag{10}$$

Note that every $|p_i\rangle$ is a pure state of a single particle, which is limited by the probabilistic comparison of two unknown quantum states [24]. In this condition, all the minus signs in Eq. (10) are global phases and can be omitted. Therefore, we have

$$|\mathcal{S}'\rangle = \bigotimes_{i=1}^{n} E_{k_A^{2i-1},k_A^{2i}}E'_{k_A^i}U_i|p_i\rangle = E_{K_A}E'_{K_A}|\mathcal{P}\rangle, \tag{11}$$

where Eq. (7) is used. Obviously, if Bob provides his counterfeit $(|\mathcal{P}\rangle,|\mathcal{S}'\rangle)$ to Trent, it will always pass the verification.

So far we have found a simple way for Bob to achieve existential forgery of Alice's signature under known message attack. The attack strategy can be described as follows.

Suppose Bob has a valid signed message of Alice, i.e., $(|P\rangle,|S\rangle)$, and he performs $\bigotimes_{i=1}^{n} U_i$ (U_i is any Pauli operation) on the qubits in $|P\rangle$, and the same operations on the last n qubits in $|S\rangle$ (i.e., $|S'\rangle$). The resulting new pair $(|\mathcal{P}\rangle,|\mathcal{S}\rangle)$ must be a successful forgery. Because each U_i can be selected from four Pauli operations at will, at least 4^n-1 different forgeries can be found by Bob [the original one, $(|P\rangle,|S\rangle)$, is not included]. Therefore, Bob can select the most preferred message $|\mathcal{P}\rangle_{\rm pr}$ from them and say that it is the message Alice signed to him. In this condition, Trent will always stand on the side of Bob although Alice is greatly aggrieved. Note that Bob can directly perform his attack when he just received Alice's signed message or after the verifying phase, where he needs to launch the dispute and requires Trent's judgment.

Finally, there is another thing which should be emphasized. As was pointed out in Ref. [23], the AQS protocol with Bell states can be used to sign both quantum messages and classical ones. It is not difficult to imagine that Bob can achieve universal forgery of Alice's signature under known message attack if the signed message is classical. For example, suppose Bob has a valid signed message of Alice, i.e., $(|P\rangle,|S\rangle)$, where $|P\rangle=\bigotimes_{i=1}^{n}|p_i\rangle$ is a classical message, that is, $|p_i\rangle=|0\rangle$ or $|1\rangle$. If Bob wants to forge Alice's signature on the message $|Q\rangle=\bigotimes_{i=1}^{n}|q_i\rangle$ ($|q_i\rangle=|0\rangle$ or $|1\rangle$), he just chooses the Pauli operations

$$\bigotimes_{i=1}^{n} U_i=\bigotimes_{i=1}^{n}\sigma_x^{p_i\oplus q_i} \tag{12}$$

in the above attack, where $\oplus$ represents the addition module 2. In this circumstance, as a result, Bob can forge Alice's signature on any classical message he wants.

2. Alice's disavowal

Above we have shown that Bob can forge Alice's signature successfully. Now we consider the other security issue in quantum signature, i.e., Alice's disavowal. In fact, Alice can also cheat in this AQS protocol. That is, Alice can successfully disavow any message she ever signed.

Suppose Alice signs a message (e.g., a contract) $|P\rangle=\bigotimes_{i=1}^{n}|p_i\rangle$ according to the steps in the protocol and sends $(|P\rangle,|S\rangle)$ to Bob. When Trent sends $|Y_{TB}\rangle=E_{K_B}(|M_A\rangle\otimes|S\rangle\otimes|P\rangle\otimes|r\rangle)$ to Bob in step V3, Alice modifies the states of the ciphertext corresponding to the last n qubits in $|S\rangle$ (i.e., $|S'\rangle$), so that the resulting states of these qubits (denoted as $|S^A\rangle$) are not a valid signature of $|P\rangle$ anymore. Note that Alice can find these qubits in the ciphertext and then disturb them while leaving others unchanged because the qubit numbers in $|M_A\rangle$, $|S\rangle$, $|P\rangle$, and $|r\rangle$ are determinate, and the encryption of QOTP is qubit by qubit. Furthermore, Bob cannot discover Alice's modification on $|S'\rangle$ because he does not know K_A. Thus when Bob requires Alice to fulfill this contract at a later time, Alice can disavow this contract by announcing that it is not the one she ever signed or it was illegally modified by Bob. In this circumstance, interestingly, Trent will stand on the side of Alice.

This attack is very simple and not difficult to understand. First, the original signed message $(|P\rangle,|S\rangle)$ is really signed by Alice and then it will pass the verification of Trent ($r=1$). Second, because Alice only modified $|S\rangle$, which is a ciphertext for Bob and not useful for Bob's verification in step V5, Bob will accept this signature without noticing Alice's attack. Third, when dispute appears, Bob provides $(|P\rangle,|S^A\rangle)$ to Trent and requires his judgment. Obviously the modified signature will not pass Trent's verification and consequently Trent will agree with Alice, believing that the signature was forged by Bob.

III. ANALYSIS OF THE AQS PROTOCOL WITHOUT ENTANGLED STATES

In Ref. [24] Zou *et al.* improved the above AQS protocol to prevent the disavowal of Bob and proposed a new AQS protocol without using entangled states. Here we take the new protocol as our example to show that it is also susceptible to our attacks. Because the protocol and the attack strategies are similar to that in Sec. II, we describe them just in brief words.

A. AQS protocol without using entangled states

The AQS protocol without using entangled states [24] is as follows.

1. Initializing phase

Three keys K_{AB}, K_{AT}, and K_{BT} are shared between Alice and Bob, Alice and Trent, and Bob and Trent, respectively.

2. Signing phase

(S1) Alice obtains three copies of the quantum message $|P\rangle=\bigotimes_{i=1}^{n}|p_i\rangle$ and encrypts each of them into $|P'\rangle$ using a random number r as the key.
(S2) Alice performs the encryptions $|R_{AB}\rangle=E_{K_{AB}}|P'\rangle$, $|S_A\rangle=E_{K_{AT}}|P'\rangle$, and $|S\rangle=E_{K_{AB}}(|P'\rangle,|R_{AB}\rangle,|S_A\rangle)$ and sends $|S\rangle$ to Bob.

3. Verifying phase

(V1) Bob decrypts $|S\rangle$ and sends $|Y_B\rangle=E_{K_{BT}}(|P'\rangle,|S_A\rangle)$ to Trent.
(V2) Trent decrypts $|Y_B\rangle$ and verifies whether $|S_A\rangle=E_{K_{AT}}|P'\rangle$. He publishes $V_T=1$ and sends $|Y_B\rangle$ back to Bob if the equation holds; otherwise $V_T=0$.
(V3) Bob decrypts $|Y_B\rangle$ and verifies whether $|R_{AB}\rangle=E_{K_{AB}}|P'\rangle$. If it is, he publishes $V_B=1$; otherwise $V_B=0$.
(V4) When $V_T=V_B=1$, Bob accepts Alice's signature. In this condition Alice publishes r and Bob recovers $|P\rangle$ from $|P'\rangle$. Finally Bob stores $(|P\rangle,|S_A\rangle,r)$ as the signed message.

B. Analysis of the AQS protocol without using entangled states

Compared with the one with Bell states, this protocol mainly changes in two aspects. On the one hand, the message copy for Bob is sent in the manner of QOTP encryption instead of teleportation, by which Bell states are not needed anymore. On the other hand, the parameter r is introduced to prevent Bob from obtaining the message content before he accepts it. Obviously, the first change has no effect on the attack strategies we proposed above. Now we analyze how the second change influences the attacks.

As far as Bob's forgery is considered, the situation is just like that in the protocol with Bell states. For example, $|S_A\rangle$

is also the encryption of $|P'\rangle$ by QOTP, and Trent does not know the (quantum) message content from beginning to end. Therefore, Bob can forge a signature by performing Pauli operations $\bigotimes_{i=1}^{n} U_i$ on the qubits in $|P'\rangle$ and the same operations on the qubits in $|S_A\rangle$. In fact, introducing the parameter r brings only one difference; that is, if Bob wants to forge Alice's signature when he just received the signed message, he cannot choose suitable $\bigotimes_{i=1}^{n} U_i$ in order to obtain the fake message he prefers. This is because at that time the message $|P'\rangle$ is still a ciphertext encrypted by the unknown r. But Bob can still forge the signature after the verifying phase, where he launches the dispute and requires Trent's judgment. At that time, r has been published and Bob can choose suitable Pauli operations for him. As a result, Bob also achieves existential forgery of Alice's signature under known message attack. Similar to the situation in the protocol with Bell states, when the signed message is classical the forgery will become universal.

It is not difficult to see that introducing the parameter r has no influence on Alice's attack, i.e., disavowal. Because Trent will send $|S_A\rangle$ (in the form of ciphertext in $|Y_B\rangle$) back to Bob after his judgment, Alice still can disturb the states of the qubits in it so that $(|P\rangle,|S_A\rangle,r)$ is not a valid signed message anymore. Furthermore, this attack will not be discovered by Bob because he does not know K_{AT}. In this way Alice can successfully disavow her signature on any message she ever signed.

IV. DISCUSSIONS

Here we analyze the reasons why our attack strategies work in AQS protocols and try to find some ways to improve the protocols. Without loss of generality, we take the protocol with Bell states [23] as an example to give our analysis.

In our opinion, the following three facts are the main reasons why the AQS protocol is susceptible to our attacks.

(1) Trent does not know the content of the signed message because it is a quantum one. Therefore, when dispute appears, Trent can only require Bob to provide the signed message $(|P\rangle,|S\rangle)$ and can judge who is cheating by verifying whether Eq. (5) holds. This fact gives the chance for Alice or Bob to change the states of $|P\rangle$ and $|S\rangle$ without being discovered.

(2) Though it can achieve high security for data encryption, QOTP is not so suitable (or enough) for AQS. On the one hand, this algorithm encrypts data qubit by qubit. Thus Alice and Bob can easily find and modify the qubits they want to change in the ciphertext, leaving the others undisturbed. On the other hand, Pauli operations commute or anticommute with each other, which makes that $|P\rangle$ and $|S'\rangle$ still can pass Trent's verification after Bob's same Pauli operations on them. Therefore, Bob can give many existential forgeries based on one legal signed message.

(3) As the most important evidence when Trent resolves a dispute, $|S'\rangle$ is the ciphertext of $|P\rangle$ by encryption with the key K_A, which is unknown to Bob. When Trent sends $|S'\rangle$ back to Bob, it is totally unreadable for Bob and its integrity cannot be verified. This gives Alice the chance to intercept and modify $|S'\rangle$ without being discovered and then successfully disavow her signature later.

Based on the above analysis, the following two elementary manners can be used to improve the AQS protocol.

(1) After the verification, Trent does not send $|S'\rangle$ to Bob, but stores it in his hand. When dispute appears, Trent requires Bob to provide $|P\rangle$ and verifies the relation between $|P\rangle$ and the corresponding $|S'\rangle$ according to Eq. (5). In this way neither Alice nor Bob have a chance to modify $|S'\rangle$ after Trent's verification. But this improvement cannot prevent Bob's forgery when he just received the signed message (i.e., before Trent's verification). Furthermore, it also has another disadvantage; that is, Trent has to store one signature (like $|S'\rangle$) once a verification happens, which greatly increases his burden.

(2) Quantum message authentication can be introduced into the AQS protocol to ensure the integrity of the signature $|S'\rangle$. For example, before she sends it to Bob, Alice encodes $|S'\rangle$ with K_A into the authenticated message $|S'_A\rangle$. Thus Trent can verify its integrity when he receives $|S'_A\rangle$ from Bob. Similarly, Trent encodes $|S'_A\rangle$ with K_B into the authenticated message $|S'_{AB}\rangle$ before he sends it to Bob. Thus when he receives it, Bob can verify whether it was modified by Alice in the transmission. As a result, the attacks from both Alice and Bob can be prevented. Nevertheless, the suitable authentication scheme still needs further study [16–19].

In addition, the Hash function [15] is generally accepted to prevent existential forgery in a classical digital signature. If we have a Hash function on quantum message, it will be an effective way to stand against Bob's forgery. However, it cannot prevent Alice's disavowal, and the feasibility of such a Hash function also needs further study.

V. CONCLUSIONS

We analyze the security of AQS protocols [23,24] and give attack strategies for both Alice and Bob. It is shown that Bob can achieve existential forgery of Alice's signature under known message attack. More seriously, Bob can realize universal forgery when the signed message is classical. Furthermore, Alice can disavow any of her signatures in these protocols. The strategies are demonstrated in detail and some discussions on how to improve the protocols are presented.

As we pointed in Sec. I, the AQS protocols give an elementary model to sign a quantum message. To our knowledge, this is the only model which can overcome Barnum *et al.*'s limit [17] now, and is feasible in theory. Though we find insecurity in AQS protocols, the loopholes can be made up for by using, for example, quantum message authentication. Therefore, AQS protocols are still valuable and deserve further study. In our opinion, the following topics are interesting and can be studied in the future:

(1) A message authentication scheme can be designed which is suitable for AQS protocols.

(2) An AQS protocol can be designed where the message can be signed and verified by multiple parties.

(3) As we know, the comparison of two unknown quantum states [25] can only give a probabilistic result. If Bob changes only a few qubits (maybe the key qubits) in the signed message,

it will not be discovered with certain probability. How do we resolve this problem?

(4) In a real channel there will be noises, which makes a legal signed message change in the channel and it cannot pass the verification. Can AQS protocols overcome the influence of noise?

(5) The qubits in the signed message are limited to a pure single-particle state in AQS protocols because the state comparison circuit will not work as expected when its inputs are two mixed states. How do we realize the signature of a quantum message that includes mixed states (for example, some qubits in the message are entangled together)?

ACKNOWLEDGMENTS

We are grateful to the anonymous reviewer for helpful comments. This work is supported by NSFC (Grant Nos. 60873191, 60903152, 61003286, and 60821001), NCET (Grant No. NCET-10-0260), SRFDP (Grant Nos. 200800131016 and 20090005110010), the Beijing Nova Program (Grant No. 2008B51), the Key Project of Chinese Ministry of Education (Grant No. 109014), the Beijing Natural Science Foundation (Grant No. 4112040), the Fundamental Research Funds for the Central Universities (Grant Nos. BUPT2011YB01 and BUPT2011RC0505).

[1] P. W. Shor, Proc. Annu. Symp. Found. Comput. Sci. **35**, 124 (1994).
[2] L. K. Grover, in *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing* (ACM, New York, 1996), p. 212.
[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[4] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984* (IEEE, New York, 1984), p. 175.
[5] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[6] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[7] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).
[8] M. Hillery, V. Buzěk, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
[9] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).
[10] G. L. Long and X. S. Liu, Phys. Rev. A **65**, 032302 (2002).
[11] K. Boström and T. Felbinger, Phys. Rev. Lett. **89**, 187902 (2002).
[12] F. G. Deng, G. L. Long, and X. S. Liu, Phys. Rev. A **68**, 042317 (2003).
[13] M. Dusek, O. Haderka, M. Hendrych, and R. Myska, Phys. Rev. A **60**, 149 (1999).
[14] G. Zeng and W. Zhang, Phys. Rev. A **61**, 022303 (2000).
[15] B. Schneier, *Applied Cryptography* (Wiley, New York, 1996).
[16] M. Curty, D. J. Santos, E. Pérez, and P. García-Fernández, Phys. Rev. A **66**, 022301 (2002).
[17] H. Barnum, C. Crépeau, D. Gottesman, A. Smith, and A. Tapp, in *Proceedings of the 43rd Annual IEEE Symposium on the Foundations of Computer Science* (IEEE Computer Society Press, Washington DC, 2002), p. 449.
[18] E. Pérez, M. Curty, D. J. Santos, and P. García-Fernández, J. Mod. Opt. **50**, 1035 (2003).
[19] L. Yang, e-print arXiv:quant-ph/0309200.
[20] G. Zeng and C. H. Keitel, Phys. Rev. A **65**, 042312 (2002).
[21] M. Curty and N. Lütkenhaus, Phys. Rev. A **77**, 046301 (2008).
[22] G. Zeng, Phys. Rev. A **78**, 016301 (2008).
[23] Q. Li, W. H. Chan, and D. Y. Long, Phys. Rev. A **79**, 054307 (2009).
[24] X. Zou and D. Qiu, Phys. Rev. A **82**, 042325 (2010).
[25] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, Phys. Rev. Lett. **87**, 167902 (2001).
[26] H. Lo and T. Ko, Quantum Inf. Comput. **5**, 41 (2005).
[27] F. Gao, F. Z. Guo, Q. Y. Wen, and F. C. Zhu, Phys. Rev. Lett. **101**, 208901 (2008).
[28] Y. S. Zhang, C. F. Li, and G. C. Guo, Phys. Rev. A **63**, 036301 (2001).
[29] F. Gao, S. Qin, Q. Wen, and F. Zhu, Quantum Inf. Comput.**7**, 329 (2007).
[30] F. Gao, Q. Wen, and F. Zhu, Chin. Phys. B **17**, 3189 (2008).
[31] F. Gao, S. Qin, F. Guo, and Q. Wen, IEEE J. Quantum Electron. **47**, 630 (2011).
[32] L. Hao, J. Li, and G. Long, Sci. China Phys. Mech. Astron. **53**, 491 (2010).
[33] S. Qin, F. Gao, Q. Wen, and F. Zhu, Phys. Lett. A **357**, 101 (2006).
[34] A. Wójcik, Phys. Rev. Lett. **90**, 157901 (2003).
[35] A. Wójcik, Phys. Rev. A **71**, 016301 (2005).
[36] Q. Y. Cai, Phys. Rev. Lett. **91**, 109801 (2003).
[37] F. Gao, F. Z. Guo, Q. Y. Wen, and F. C. Zhu, Phys. Rev. A **77**, 014302 (2008).
[38] F. Gao, Q. Y. Wen, and F. C. Zhu, Phys. Lett. A **360**, 748 (2007).
[39] F. Gao, S. Lin, Q. Y. Wen, and F. Zhu, Chin. Phys. Lett. **25**, 1561 (2008).
[40] F. Gao, S. Qin, Q. Wen, and F. Zhu, Opt. Commun. **283**, 192 (2010).
[41] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. A **73**, 022320 (2006).
[42] F. G. Deng, X. H. Li, H. Y. Zhou, and Z. J. Zhang, Phys. Rev. A **72**, 044302 (2005).
[43] S. Goldwasser, S. Micali, and R. Rivest, SIAM J. Comput. **17**, 281 (1988).
[44] D. W. Leung, Quantum Inf. Comput. **2**, 14 (2002).
[45] P. O. Boykin and V. Roychowdhury, Phys. Rev. A **67**, 042317 (2003).
[46] For the sake of clarity, hereafter we use script letters, such as $|\mathcal{P}\rangle$ or $|\mathcal{S}\rangle$, to denote the quantum states (including message, signature, and intermediate states) that are questionable with respect to their origin (e.g., the ones that are forged by Bob).