Enhanced arbitrated quantum signature scheme using Bell states*

Wang Chao(王 朝)†, Liu Jian-Wei(刘建伟), and Shang Tao(尚 涛)

School of Electronic and Information Engineering, Beihang University, Beijing 100191, *China*

(Received 22 August 2013; revised manuscript received 26 November 2013; published online 20 April 2014)

We investigate the existing arbitrated quantum signature schemes as well as their cryptanalysis, including intercept-resend attack and denial-of-service attack. By exploring the loopholes of these schemes, a malicious signatory may successfully disavow signed messages, or the receiver may actively negate the signature from the signatory without being detected. By modifying the existing schemes, we develop counter-measures to these attacks using Bell states. The newly proposed scheme puts forward the security of arbitrated quantum signature. Furthermore, several valuable topics are also presented for further research of the quantum signature scheme.

Keywords: arbitrated quantum signature, intercept-resend attack, denial-of-service attack

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.1088/1674-1056/23/6/060309

1. Introduction

Quantum cryptography,[1,2] known as the combination of quantum mechanics and cryptography, has become one of the most important research areas in quantum information science. Quite a few branches of quantum cryptography have been studied in recent years, including quantum key distribution (QKD),[3–8] quantum secret sharing (QSS),[9–12] quantum secure direct communication (QSDC),[13–16] and so on. As a crucial branch of quantum cryptography, the quantum signature is attracting more and more attention and, thus, various kinds of quantum signature schemes have been proposed, such as: quantum proxy signature,[17–20] quantum blind signature,[21–24] and quantum arbitrated signature, etc.[25–38]

Message authentication and digital signature are two important research fields in cryptography. The former is used to ensure the authenticity and integrity of the transmitted message, which can prevent an external participant from pretending to be a legitimate user or tampering with the message without being detected. The latter is used for not only authenticating the message but also to provide the function of nonrepudiation, which can prevent an internal participant, such as the receiver forging the sender's signature or the sender denying her own signature. However, the authentication and signature of a quantum message are more difficult compared with their counterparts in classical cryptography. In Ref. [39], Barnum *et al.* pointed out that signing a quantum message is impossible, although authenticating a quantum message can be accomplished.

Fortunately, Zeng and Keitel proposed an arbitrated quantum signature (AQS) scheme, ZK scheme for short[25] in 2002. This work gives an elementary model to sign a quantum message, which overcomes Barnum *et al.*'s limit[39] and can be realized in practice. Subsequently, Curty *et al.*'s comment on ZK scheme and Zeng's response for this comment were put forward to further discuss the scheme in succession.[26,27] In 2009, Li *et al.*[28] presented another AQS scheme based on Bell states, which simplifies the ZK scheme while preserving its merits by replacing Greenberger–Horne–Zeilinger (GHZ) states with Bell states as the carrier. As we know, a secure quantum signature scheme should satisfy two security requirements; that is, unforgeability and undeniability. For unforgeability, neither the signature receiver nor an attacker can forge a signature or change the content of a signature. The signature should not be reproducible by any other person. For undeniability, the signatory who has sent her/his signature to the signature receiver, cannot later deny having provided her/his signature. Moreover, the signature receiver cannot deny the receipt of the signature. However, can these proposed AQS schemes satisfy the two basic security properties and really secure against the common attack strategies, such as the participant forgery attack, intercept-resend attack, a denial-of-service (DoS) attack, etc.?

Accordingly, many researchers have paid considerable attention to the improvements and the security analysis of these AQS schemes.[25–33] As pointed out in Refs. [29] and [30], many of the above-mentioned AQS schemes[25–28] have a common security problem in that the unforgeability cannot be satisfied. It is shown that the receiver, Bob, can validly modify the transmitted pair of message and signature to achieve existential forgery of the signature by launching an existential forgery attack. Meanwhile, Choi *et al.* in Ref. [30] found that Bob's forgery can be prevented by modifying the encryption method, an important part of AQS, and provided an extended encryption algorithm to achieve this. Moreover, Zhang

*Project supported by the National Natural Science Foundation of China (Grant No. 61272501), Beijing Natural Science Foundation (Grant No. 4132056), and the National Key Basic Research Program of China (973 Program) (Grant No. 2012CB315905).

†Corresponding author. E-mail: wangchaopaper@126.com

© 2014 Chinese Physical Society and IOP Publishing Ltd

et al.[31] have recently further improved the security of the AQS schemes based on Choi *et al.*'s improvement against the existential forgery attack so that unforgeability is satisfied in these AQS schemes.

However, we carefully find that the undeniability requirement cannot be satisfied in the aforementioned AQS schemes,[25–33] and there are still two open problems that need to be solved urgently. One is how to construct an AQS scheme to stand against a special kind of DoS attack strategy. In Ref. [32], Zou *et al.* showed that the AQS schemes can be repudiated by the receiver Bob if a special case of DoS attack is performed. That is, the arbitrator, Trent, cannot solve the dispute between the signatory and the receiver when the receiver repudiates the integrity of a signature. By using a public board, Zou *et al.* proposed two AQS schemes to conquer this shortcoming. Unfortunately, Hwang *et al.*[33] showed that the same security problem may still exist in Zou *et al.*'s schemes. The other is how to protect the previous proposed AQS schemes from the intercept-resend attack launched by the signatory. As Gao *et al.* discussed in Ref. [29], the signatory, Alice, can successfully disavow any message she ever signed by the intercept-resend attack. Intuitively, these security flaws could be serious if the signature occurs in a practical application environment, such as an electronic trading system or an electronic ordering system, etc.

In this work, we investigate the cryptanalysis and the corresponding improvements of the previous proposed AQS schemes, and construct a novel enhanced AQS scheme. In our presented scheme, some improvements are put forward to recover the security against the DoS attack: a) the necessary steps of the scheme are modified elaborately, which makes Alice have no chance to send the incorrect information without being detected; and, b) the security check technique[40] is employed to enable the signed quantum data to be tamperproof. With our improved ideas, the DoS attack and the intercept-resend attack cannot properly work, such that the undeniability requirement is satisfied. Moreover, we also give the detailed security analysis of our improved scheme and discuss several valuable topics about AQS scheme that can be studied in future.

The rest of this paper is organized as follows. In Section 2, we first review the related works about AQS schemes, and in Section 3 we discuss the two open problems on the AQS schemes. Then, in Section 4 and Section 5, we propose an enhanced AQS scheme and give the corresponding security analysis in detail, respectively. Finally, in Section 6, our conclusions are summarized.

2. Related works

In this section, we first briefly recall some notions and notations involved in the AQS scheme. Then, we describe the elementary model of an AQS scheme. Here we introduce Li *et al.*'s scheme[28] with Bell states as an example because the scheme and the attack strategy are similar to that in Ref. [25].

2.1. Notions and notations

The quantum signature is a quantum version of the classical signature, which is an analogy to handwritten signature. Similarly, the arbitrated quantum signature scheme is a signature implemented with the help of an arbitrator; that is, the third trusted party. In other words, in an arbitrated quantum signature scheme, the arbitrator is a disinterested third party trusted to complete the whole process of the signature. Here, "trusted" means that all the participants involved in the arbitrated quantum scheme accept what he says as true and what he does as correct, as well as which he will complete his part of the signature scheme.

To better understand the subsequent AQS scheme, some notations are defined, as follows. An AQS scheme involves three participants, namely, the signatory Alice, the receiver Bob, and the arbitrator Trent, and includes three phases: an initializing phase, a signing phase, and a verifying phase. In the AQS scheme, the quantum message signed by the signatory Alice, is denoted with $|P\rangle = \otimes_{i=1}^{n} |P_i\rangle$ where $|P_i\rangle = \alpha_i|0\rangle + \beta_i|1\rangle$. Here note that, if the known quantum message is to be signed, the number of the copies of $|P\rangle$ is arbitrary, whereas if the quantum message to be signed is unknown, three copies of $|P\rangle$ are necessary.[32] In addition, the quantum one-time-pad (QOTP) encryption and the rotation transformation are defined with E_K and R_K, respectively, that is,

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

Here the secret key $K \in \{0,1\}^*$ should satisfy $|K| \geq 2n$ proved by Boykin and Roychowdhury,[41] K_i and $|P_i\rangle$ are the i-th bit of K and $|P\rangle$, respectively, and σ_x and σ_z are the Pauli matrices.

2.2. The elementary model of AQS

In this subsection, the elementary model of an AQS scheme is described by taking Li *et al.*'s AQS scheme as an example. The procedure of the AQS scheme, initializing phase, signing phase, and verifying phase, can be seen in the following steps.

(i) Initializing phase

(i)-1 Trent shares the secret keys K_A and K_B with Alice and Bob, respectively, through some unconditionally secure quantum key distribution protocols.[3–8]

(ii)-2 Trent prepares n Bell states $|\phi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle \otimes \cdots \otimes |\phi_n\rangle$ with $|\phi_i\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}$, and distributes all A particles to Alice and all B particles to Bob via a secure and authenticated method.[39,42–47]

(ii) Signing phase

(ii)-1 Alice creates three copies of the qubit string $|P\rangle = \otimes_{i=1}^{n}|P_i\rangle$ related to the message with $|P_i\rangle = \alpha_i|0\rangle + \beta_i|1\rangle$, and encrypts one copy of $|P\rangle$ into $|R_A\rangle$ in terms of the shared secret key K_A with Trent; that is, $|R_A\rangle = R_{K_A}(|P\rangle)$.

(ii)-2 Alice performs Bell measurement on each qubit in the second copy of $|P\rangle$ and the corresponding qubit A in each Bell state, and obtains the measurement result $|M_A\rangle = \otimes_{i=1}^{n}|M_A^i\rangle$ according to the following equation:

$$\begin{aligned}|\psi_i\rangle_{PAB} &= |P_i\rangle \otimes |\phi_i\rangle_{AB} \\ &= (\alpha_i|0\rangle + \beta_i|1\rangle)_P \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB} \\ &= \frac{1}{2}\big[|\Phi_{PA}^{+}\rangle_i(\alpha_i|0\rangle + \beta_i|1\rangle)_B \\ &\quad + |\Phi_{PA}^{-}\rangle_i(\alpha_i|0\rangle - \beta_i|1\rangle)_B \\ &\quad + |\Psi_{PA}^{+}\rangle_i(\alpha_i|1\rangle + \beta_i|0\rangle)_B \\ &\quad + |\Psi_{PA}^{-}\rangle_i(\alpha_i|1\rangle - \beta_i|0\rangle)_B\big], \end{aligned} \tag{1}$$

where $|M_A^i\rangle \in \{|\Phi_{PA}^{+}\rangle_i, |\Phi_{PA}^{-}\rangle_i, |\Psi_{PA}^{+}\rangle_i, |\Psi_{PA}^{-}\rangle_i\}$, is one of the four Bell states.

(ii)-3 Alice generates the signature $|S\rangle = E_{K_A}(|M_A\rangle, |R_A\rangle)$ of the message $|P\rangle$ by QOTP encryption algorithm using K_A.

(ii)-4 Alice transmits the signature $|S\rangle$ and the third copy of $|P\rangle$ to Bob.

(iii) Verifying phase

(iii)-1 Bob encrypts $|S\rangle$ and $|P\rangle$ using K_B by QOTP, that is, $|Y_B\rangle = E_{K_B}(|S\rangle, |P\rangle)$, and sends $|Y_B\rangle$ to Trent.

(iii)-2 Using K_A and K_B, Trent decrypts $|Y_B\rangle$ and obtains $|P\rangle$, $|M_A\rangle$, and $|R_A{}'\rangle$. Then, he compares whether $|R_A{}'\rangle = R_{K_A}(|P\rangle)$ by probabilistic comparison of quantum states.[48] If it holds, he sets the verification parameter $V = 1$; Otherwise, he sets $V = 0$.

(iii)-3 Trent gets back $|P\rangle$ from $|R_A{}'\rangle$ if the equation that $|R_A{}'\rangle = R_{K_A}(|P\rangle)$ holds, and then sends the encrypted message $|Y_{T_B}\rangle = E_{K_B}(|M_A\rangle, |S\rangle, |P\rangle, V)$ to Bob.

(iii)-4 Bob decrypts the received message and obtains $|M_A\rangle$, $|S\rangle$, $|P\rangle$, and V. If $V = 1$, he goes on to the next step; Otherwise, he considers the signature has been obviously forged and rejects it.

(iii)-5 Bob performs the corresponding unitary transformations on B particles in his hand according to the measurement result $|M_A\rangle$ and the correlations in Eq. (1), and obtains one copy of $|P\rangle$, denoted with $|P_B{}'\rangle$. He then compares it with the copy received from Trent. If $|P_B{}'\rangle = |P\rangle$, Bob accepts the signature $|S\rangle$ of the message $|P\rangle$; otherwise, he rejects it.

3. The open problems on AQS schemes

In this section, we point out that there are two open problems in the previous AQS schemes: the intercept–resend attack and the special DoS attack. We first introduce the two attack strategies, and then discuss why the signatory Alice can archive the disavowal of any signed message, and the signature receiver Bob is also able to implement the disavowal of the received signature, respectively, by the corresponding attack strategy. In addition, to demonstrate the attack strategy clearly, we give a practical application instance of the special DoS attack.

3.1. Discussion of the intercept-resend attack

The intercept–resend attack is one of the most common attack strategies and it usually works well in many AQS schemes. This attack strategy means that the attacker (including the malicious participant) can intercept the transmitted quantum message and modify it in his favor, and then send the changed quantum message to the receiver as normal. As illustrated in Ref. [29], by launching the intercept–resend attack, the signatory Alice can successfully disavow any message she ever signed. How this attack strategy is carried out and why it can be achieved in the AQS schemes are discussed below.

Taking Li *et al.*'s scheme as an example, suppose Alice signs a quantum message $|P\rangle = \otimes_{i=1}^{n}|P_i\rangle$ according to the corresponding steps, and sends the pair of message and signature $(|P\rangle, |S\rangle)$ to Bob. When Trent sends the encrypted message $|Y_{T_B}\rangle = E_{K_B}(|M_A\rangle, |S\rangle, |P\rangle, V)$ to Bob in Step (iii)-3, Alice can intercept this message and modify the related qubits in $|S\rangle$ so that the signature of $|P\rangle$ is not valid any more. What is worse, Bob cannot discover Alice's modification because of having no knowledge of K_A when he receives the message in Step (iii)-4. Then, the integrity verification of the message will be passed and the signature will finally be accepted. Therefore, when the dispute appears, Alice can disavow this signature of $|P\rangle$ by announcing that it is not the one she signed or it has been illegally altered by Bob. Interestingly, the arbitrator Trent will stand on the side of Alice in this circumstance.

Now, we give a more clearly description of this attack strategy. First, the original singed pair of the quantum message and the corresponding signature $(|P\rangle, |S\rangle)$ is indeed signed by Alice and thus the verification performed by Trent will be passed successfully in Step (iii)-2, i.e., the verification parameter is set to $V = 1$. Second, Alice only modified $|S\rangle$ which is a ciphertext for Bob and not useful for Bob's verification in Step (iii)-5, Bob will accept the signature without noticing Alice's attack. Third, when the dispute appears, Bob can only provide the changed signature pair, denoted with $(|P\rangle, |\tilde{S}\rangle)$ where $|\tilde{S}\rangle \neq |S\rangle$, to Trent and require his judgment. Obviously, the modified pair of message and signature will not pass Trent's verification and thus Trent will support Alice while believing that the signature was forged by Bob.

In essence, quantum encryption, only for hiding quantum information securely, cannot provide the tamperproof property. The main reasons why the AQS scheme is susceptible

to the intercept–resend attack are that the number and the order of the qubits in $(|M_A\rangle, |S\rangle, |P\rangle, V)$ are determinate, and the encryption of QOTP is qubit by qubit. Thus, Alice can find the corresponding qubits of $|S\rangle$ in the transmitted ciphertext and then only modify them while leaving others unchanged, so that the verification is passed successfully without noticing Alice's attack. Similarly, the same security problem may still exist in these AQS schemes,[25–33] which is an open problem at present. Consequently, in order to stand against this attack strategy, these AQS schemes should provide that the signed quantum data must be tamperproof.

3.2. Discussion on the special DoS attack

A special case of DoS attack was introduced by Zou *et al.* in Ref. [32]. This DoS attack means that Bob admits receives some signature but denies that the signature is correct. By this attack strategy, Bob can actively repudiate the integrality of the signature from Alice and reject it when the current situation is not in his favor. In order to prevent the special attack, based on Li *et al.*'s scheme,[28] Zou *et al.* put forward two improved AQS schemes, but Hwang *et al.* in Ref. [33] pointed out that both of them are still vulnerable to this attack. Why can Bob achieve it successfully? Here we provide the detailed discussion taking Li *et al.*'s scheme as an instance.

It is a fact that in Step (iii)-5 the case $|P_B{}'\rangle \neq |P\rangle$ will happen if Alice generates $|\psi_i\rangle_{PAB}$ by another quantum message $|\tilde{P}_i\rangle$ instead of $|P_i\rangle$ in Step (ii)-2, or lets $|S\rangle = E_{K_A}(|\tilde{M}_A\rangle, |R_A\rangle)$ where $|\tilde{M}_A\rangle \neq |M_A\rangle$ in Step (ii)-3. Note that Trent cannot check whether the $|M_A\rangle$ in $|S\rangle$ is correct or not, because the Bell measurement is performed by Alice who is the only one who knows the corresponding measurement result in the signing phase. Consequently, when Bob claims $|P_B{}'\rangle \neq |P\rangle$ in Step (iii)-5, one or more of the following three cases may occur:

1) Bob told a lie due to some reason.

2) Alice deliberately sent incorrect information to Bob. Alice generated $|\psi_i\rangle_{PAB}$ using another $|\tilde{P}_i\rangle$ rather than $|P_i\rangle$ in Step (ii)-2, or generates the signature $|S\rangle = E_{K_A}(|\tilde{M}_A\rangle, |R_A\rangle)$ with $|\tilde{M}_A\rangle \neq |M_A\rangle$ in Step (ii)-3.

3) Eve intercepted the communication transmissions and disturbed some message, such as $|S\rangle$, $|Y_B\rangle$, and $|Y_{T_B}\rangle$.

Obviously, in this situation the arbitrator, Trent, is not able to judge correctly which case happened, so that the dispute between Alice and Bob cannot be solved when Bob claims $|P_B{}'\rangle \neq |P\rangle$. Therefore, in Li *et al.*'s scheme, Bob can actively disavow Alice's signature without being detected by performing this DoS attack strategy.

To better understand this attack strategy, we further compare Zou *et al.*'s scheme[32] with Li *et al.*'s scheme.[28] Here, we mainly describe the two supplementary steps in Zou *et al.*'s scheme (for more detail, see Ref. [32]), since most steps are similar to those in Li *et al.*'s scheme. First, in Step (ii)-1, the signatory Alice encrypts all the three copies of the quantum message $|P\rangle$ into $|P'\rangle = E_r(|P\rangle)$ using QOTP encryption, where $r \in \{00, 01, 10, 11\}^n$, is a random number. Second, after Trent's verification, Bob gets back $|P'_B\rangle$ and compares whether $|P_B{}'\rangle = |P'\rangle$. If they are equal, Bob informs Alice to publish r on the public board in Step (iii)-5. According to the equation $|P'\rangle = E_r(|P\rangle)$, then Bob can recover $|P\rangle$ from $|P'\rangle$ and retains $(|S_A\rangle, r)$ as Alice's signature.

It is not difficult to see that there are two main differences in Zou *et al.*'s scheme. In the first place, all three copies of quantum message $|P\rangle$ are sent in the form of ciphertext due to the using of QOTP encryption E_r; In the second place, the parameter r is introduced to prevent Bob from obtaining the message content before he accepts it. In Zou *et al.*'s opinions, introducing the two modifications can protect the scheme from this special DoS attack, but it does not work out.

According to Zou *et al.*'s analysis, only when Bob obtains the random value r from Alice in the end, can he get back the message $|P\rangle$ from $|P'\rangle$. Once he obtains the random value r, Bob would have no chance to disavow Alice's signature of $|P\rangle$. Whereas, it is totally unnecessary for Bob to obtain the original message $|P\rangle$, if he would like to negate the signature from Alice. He only needs to claim that $|P_B{}'\rangle \neq |P'\rangle$ when $|P_B{}'\rangle = |P'\rangle$ in Step (iii)-5 before requesting the value of r from Alice. In that way, Trent will be not able to arbitrate the dispute between Alice and Bob, because one or more of the aforementioned three cases may also occur in such a condition.

3.3. An application instance

In a practical application, the special DoS attack strategy may bring out very serious consequences. Taking the popular electronic order system as an instance, where Alice is a buyer and Bob is a company. For the company, Bob, his only concern is that whether he can get the great benefit from the current market. When the current market is not in his favor, it does not matter whether he can obtain the parameter r to recover the signed order from Alice, because Bob knows that, due to the order, he will lose a fortune. Therefore, Bob may tell a lie and say that because of $|P_B{}'\rangle \neq |P'\rangle$ (in fact $|P_B{}'\rangle = |P'\rangle$) he cannot accept the corresponding signed contract from Alice. As can be imagined, to get her own benefit, Alice will insist that the contract she has signed for the message $|P\rangle$ is valid and she has never sent the incorrect information to Bob. Now, the dispute appears, but there is no way for Trent to settle it. That is, Trent cannot judge which one of the following three cases happened: Bob told a lie, Alice sent incorrect information, or Eve disturbed the electronic order system.

Based on the above analysis, it is obvious that Zou *et al.*'s scheme is still vulnerable to the special DoS attack, which is

also discussed in Hwang *et al.*'s comment but without giving a valid solution.[33] How to enhance these AQS schemes[25–33] to resist this special DoS attack; that is, avoid being disavowed for the integrality of the signature by the receiver Bob? At present, this is still an open problem that needs to be solved.

4. Our enhanced AQS scheme

In this section, we present an enhanced AQS scheme, in which some important improvements are put forward. Our proposed AQS scheme is constructed with Bell states, because the schemes with Bell states can preserve the merits of the scheme with GHZ states while providing a higher efficiency in transmission and reducing the complexity of implementation.[28] The improved scheme also involves three participants, namely, the signatory Alice, the receiver Bob, and the arbitrator Trent, and includes three phases: initializing phase, signing phase, and verifying phase. The process of our improved scheme is described as follows and figure 1 illustrates the communications in this scheme.

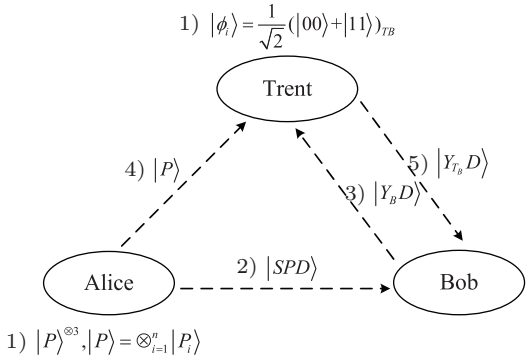


Fig. 1. The sketch of the communications in our enhanced AQS scheme. The dashed arrow denotes the quantum channel used for transmitting the quantum information, the quantum state, and the numbers with half a parenthesis indicate the transmitted message and the corresponding message delivery order, respectively.

(I) Initializing phase

(I)-1 Alice and Bob share a secret key with the arbitrator Trent, i.e., K_{AT} and K_{BT}, respectively.[3–8]

(I)-2 The arbitrator, Trent, generates n Bell states denoted with $|\phi_i\rangle = \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{TB}$, where $1 \le i \le n$. Then, he sends all the B particles to Bob via a secure and authenticated way,[39,42–47] while retains all the T particles in his own hand.

(II) Signing phase

(II)-1 Alice creates a message string of n qubits, denoted with $|P\rangle = \otimes_{i=1}^{n}|P_i\rangle$, where $|P_i\rangle = \alpha_i|0\rangle + \beta_i|1\rangle$, and two copies of it.

(II)-2 Alice obtains $|R_A\rangle$ by applying a random rotation $R_{K_{AT}}$ to one copy of $|P\rangle$ according to the shared secret key K_{AT} as follows:

$$|R_A\rangle = R_{K_{AT}}(|P\rangle) = \bigotimes_{i=1}^{n} \sigma_x^{K_{AT_i}} \sigma_z^{K_{AT_i}\oplus 1} |P_i\rangle . \quad (2)$$

(II)-3 Alice makes a quantum signature $|S\rangle$ by applying the QOTP encryption $E_{K_{AT}}$ to $|R_A\rangle$. That is,

$$|S\rangle = E_{K_{AT}}(|R_A\rangle) = \bigotimes_{i=1}^{n} \sigma_x^{K_{AT_{2i-1}}} \sigma_z^{K_{AT_{2i}}} |R_{A_i}\rangle . \quad (3)$$

Here, $|R_{A_i}\rangle$ denotes the i-th qubit of $|R_A\rangle$.

(II)-4 Alice prepares a set of decoy states $|D\rangle$,[49–51] randomly chosen from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, and randomly inserts the decoy states into $|S\rangle$ and the second copy of $|P\rangle$ to form a new sequence $|SPD\rangle$. Then, she sends the new sequence $|SPD\rangle$ to Bob.

(III) Verifying phase

(III)-1 Upon receiving $|SPD\rangle$, Bob performs the first security check.[40] If there is no error, Bob extracts $|S\rangle$ and $|P\rangle$ from $|SPD\rangle$, and encrypts them with K_{BT} into $|Y_B\rangle$ by QOTP encryption algorithm; that is, $|Y_B\rangle = E_{K_{BT}}(|S\rangle, |P\rangle)$. Otherwise, he considers there is eavesdropping in the quantum channel and aborts the process.

The first security checking process is described in the following steps: i) Alice announces the positions and the measuring bases of the decoy states to Bob. ii) Bob performs the corresponding measurement of the decoy states and then publishes the measurement results to Alice via the classical channel. iii) Alice checks the existence of eavesdropping by comparing Bob's measurement results with the corresponding initial decoy states in $|D\rangle$. If the error rate is lower than a predetermined level, Alice informs Bob to continue the scheme. Otherwise, she terminates the communication.

(III)-2 Bob picks out the decoy states from $|SPD\rangle$ and randomly inserts them into $|Y_B\rangle$ to form the new sequence $|Y_BD\rangle$, and then send $|Y_BD\rangle$ to Trent.

(III)-3 Once Trent receives $|Y_BD\rangle$, he performs the similar security check as that in Step (III)-1. If there is no eavesdropper, Trent separates $|Y_B\rangle$ from $|Y_BD\rangle$, and decrypts $|Y_B\rangle$ with the shared keys K_{AT} and K_{BT} to obtain $|P'\rangle$ and $|R_A\rangle$. He then compares whether the decryption results satisfies that $|R_A\rangle = R_{K_{AT}}(|P'\rangle)$. If they are equal, Trent sets the verification parameter $V = 1$; Otherwise, he sets $V = 0$.

(III)-4 Trent recovers $|S\rangle$ and $|P'\rangle$ (i.e., $|P\rangle$) (note that the compared states can be recovered after the comparison if they are indeed equal) and informs Alice to send the third copy of $|P\rangle$ to him.

(III)-5 After receiving the third copy of $|P\rangle$ from Alice, Trent compares whether $|P'\rangle = |P\rangle$. If they are equal, Trent performs Bell measurement on qubit T in each Bell state and the corresponding qubit in the third copy of $|P\rangle$. The measurement results $|M_T\rangle = \otimes_{i=1}^{n}|M_T^i\rangle$ are obtained according to the following equation, where $|M_T^i\rangle$ is one of the four Bell states,

$$\begin{aligned} |\psi_i\rangle_{PTB} &= |P_i\rangle \otimes |\phi_i\rangle_{TB} \\ &= (\alpha_i|0\rangle + \beta_i|1\rangle)_P \otimes \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{TB} \end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{2}[\left|\Phi_{PT}^{+}\right\rangle_i(\alpha_i|0\rangle+\beta_i|1\rangle)_B \\
&+\left|\Phi_{PT}^{-}\right\rangle_i(\alpha_i|0\rangle-\beta_i|1\rangle)_B \\
&+\left|\Psi_{PT}^{+}\right\rangle_i(\alpha_i|1\rangle+\beta_i|0\rangle)_B \\
&+\left|\Psi_{PT}^{-}\right\rangle_i(\alpha_i|1\rangle-\beta_i|0\rangle)_B]. \qquad (4)
\end{aligned}
$$

Trent encrypts $|M_T\rangle, |S\rangle, |P\rangle$, and V with K_{BT}, that is, $|Y_{T_B}\rangle = E_{K_{BT}}(|M_T\rangle, |S\rangle, |P\rangle, V)$. He then randomly inserts the decoy states in his hand to $|Y_{T_B}\rangle$ to form $|Y_{T_B}D\rangle$, and sends them to Bob.

(III)-6 Bob performs the eavesdropping check again and decrypts the received cipher text to obtain $|M_T\rangle$, $|S\rangle$, $|P\rangle$, and V. If $V=0$, Bob considers the signature has been obviously forged and rejects it. Otherwise, he goes on to the further verification.

(III)-7 According to the Bell measurement results $|M_T\rangle$ and the corresponding relationship in Eq. (4), Bob recovers $|P_B\rangle$ by performing the following unitary transformations on B particles

$$
\left|\Phi_{PT}^{+}\right\rangle \to I, \left|\Phi_{PT}^{-}\right\rangle \to \sigma_z, \left|\Psi_{PT}^{+}\right\rangle \to \sigma_x, \left|\Psi_{PT}^{-}\right\rangle \to \sigma_z\sigma_x. \qquad (5)
$$

If $|P_B\rangle = |P\rangle$, Bob accepts Alice's signature $|S\rangle$ for the quantum message $|P\rangle$. Otherwise, he rejects it.

5. Security analysis

In this section, we analyze the security of our improved AQS scheme in detail, and show that our proposed scheme is secure against the certain attack strategies such as intercept–resend attack, DoS attack, etc. Aiming at the unforgeability of the existing AQS schemes.[25–33] Gao *et al.* in Ref. [29] and Choi *et al.* in Ref. [30] have studied it deeply and proposed some potential improvements to resist the existential forgery attack. Moreover, recently, Zhang *et al.* in Ref. [31] further improved the security of the AQS scheme, and thus the unforgeability is enhanced in these AQS schemes. Fortunately, the corresponding improvements can be introduced into our proposed AQS scheme compatibly to provide the unforgeability. Therefore, here we only focus on analyzing why the intercept–resend attack and the special DoS attack can no longer work well, and how the undeniability is enhanced in our proposed scheme.

The undeniability of an AQS scheme requires that the signatory cannot deny having signed a message that has a valid signature. Moreover, the verifier who has verified the signature cannot later deny his/her involvement. In the following subsections, we show the impossibility of disavowal by the signatory and the impossibility of disavowal by the verifier, respectively.

5.1. Impossibility of disavowal by the signatory

In Section 3, we have discussed the intercept–resend attack, and showed that using this attack strategy Alice can disavow this signature of $|P\rangle$ by announcing that it is not the one she ever signed or it is illegally altered by Bob. The reason why the intercept–resend attack can be achieved is that the attacker can manipulate the corresponding qubits in the transmitted ciphertext she or he wants to modify. However, in our proposed AQS scheme, it is impossible for an attacker to perform this attack without being detected. Next, we give the detailed security analysis.

In contrast from the previous AQS schemes, the security check technique with decoy states is employed in our enhanced AQS scheme, which ensures the security of the transmitted ciphertext; that is, the attacker who disturbs the order or changes the state of the qubit can be detected successfully. The method inserting random decoy states enables the signed quantum data to be tamperproof so that the attacker cannot determinate which is the corresponding qubit when they attempt to modify the transmitted quantum message. Also, the outside attacker will be discovered if he or she disturbs the communication. Because the decoy states are randomly chosen from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, the attacker can only obtain the correct result of a decoy state with the probability $3/4$ without knowing the corresponding information of the position and the measurement basis. Obviously, the probability of passing the security check successfully for the attacker is $(3/4)^l$ for l decoy particles, which will be arbitrarily small if l is large enough.

Suppose that the malicious participant Alice performs a similar intercept–resend attack strategy on our enhanced AQS scheme as stated in Section 3. That is, when the arbitrator Trent sends the quantum message $|Y_{T_B}D\rangle$, made up of the ciphertext $|Y_{T_B}\rangle$ and the randomly inserted decoy states, to Bob in Step (III)-5, Alice intercepts this message and attempts to modify the corresponding qubits in $|S\rangle$ leaving other qubits unchanged. Obviously, Alice is not able to find the corresponding qubits of $|S\rangle$ in the intercepted quantum message because these decoy states are inserted into $|Y_{T_B}\rangle$ randomly, which disturbs the order of the qubits in $|Y_{T_B}\rangle$. In addition, the eavesdropping also will be discovered after the security check is performed in Step (III)-6. Therefore, when Alice carries out this attack strategy, she will be surely detected in the security check phase and have no chance to disavow the corresponding signature in our enhanced AQS scheme.

5.2. Impossibility of disavowal by the receiver

Now we consider the other security issue in our improved scheme; that is, the impossibility of disavowal by the receiver. Although the undeniability of an AQS scheme has been discussed in Ref. [32], Hwang *et al.* in Ref. [33] pointed out that the malicious receiver, Bob, still can disavow the integrity of the quantum signature by a special DoS attack. In particular, we find that there is a common security flaw that is unsolved in these AQS schemes.[25–33] Hence, here we only focus on

analyzing how this special DoS attack is prevented such that the undeniability is satisfied in our proposed scheme.

The intrinsic reason why the DoS attack can work well in these AQS schemes,[25–33] is that Trent cannot arbitrate the dispute between Alice and Bob, which is demonstrated in detail in Section 3. Owing to the following two important improvements, our enhanced AQS scheme can prevent the special DoS attack successfully.

1) The security check technique with decoy states, which is illustrated above.

2) The necessary steps of the scheme are modified elaborately. For instance, in the verification phase of our improved scheme, the Bell measurement is performed by Trent rather than Alice, and the process of verifying the quantum message, that is, Trent compares whether $|P'\rangle$ equals $|P\rangle$ sent from Alice, is supplemented in Step (III)-5, which gives Alice no chance to send the incorrect information without being detected.

In essence, the core idea of our proposed AQS scheme is that the improvements enable Trent to judge which one of the aforementioned three cases has happened when the dispute appears between Alice and Bob. Suppose Bob performs the DoS attack in our improved scheme as before, he would claim that $|P_B{}'\rangle \neq |P'\rangle$ when $|P_B{}'\rangle = |P'\rangle$ in Step (III)-7. Consequentially, Trent would have to come forward to solve the dispute. Obviously, Bob can be caught having told a lie. The reasons are listed as follows.

Firstly, the outside attacker, Eve, will not pass the eavesdropping check. Suppose in Step (III)-1 or Step (III)-3 the attacker, Eve, intercepts the transmitted message, such as $|SPD\rangle$ or $|Y_BD\rangle$, etc. According to the above analysis, it is obvious that she is unable to know which corresponding qubit she wants to modify. Furthermore, even though Eve disturbs the communication process, she will surely be detected with the probability of $1-(3/4)^l$ approximating to 1 due to the security check of the decoy states.

Secondly, Alice will be discovered if she sends incorrect information to the receiver. Doubtlessly, in our improved AQS scheme, Alice cannot obtain the Bell measurement result $|M_T\rangle$ and also has no chance to alter it because the operations, including performing the Bell measurement and encrypting the message $(|M_T\rangle, |S\rangle, |P\rangle, V)$, are all achieved by Trent rather than Alice in Step (III)-5. Moreover, even though Alice deliberately sends incorrect quantum message $|\tilde{P}\rangle$ instead of $|P\rangle$ to Trent before the Bell measurement in Step (III)-5, her malicious activity will also be discovered owing to the comparison of $|\tilde{P}\rangle$ and $|P\rangle$.

Therefore, when the dispute appears between Alice and Bob, Trent can exclude the above two possibilities out of the aforementioned three cases. The only remaining possibility is that Bob told a lie when he received the valid signature of $|P\rangle$ from Alice. Consequently, Bob cannot disavow the integrity of the quantum signature any more by launching the special DoS attack.

In addition, the receiver Bob also can deny having verified a signature from Alice by Trojan-horse attacks. In quantum cryptography, Trojan-horse attacks including the invisible photon eavesdropping (IPE) and delay photon eavesdropping are always used by malicious attacker to steal the participant's secret key. In Ref. [33], Hwang *et al*. have described the IPE and delay photon attacks on Zou *et al*.'s scheme, and demonstrated that the signatory Alice or the outside attacker can obtain Bob's secret key without being detected. Bob can claim that the outside attacker Eve or Alice has tampered the transmitted message, so he can deny having verified the signature.

In experiment, IPE attack utilizes the fact that the single photon detector is only sensitive to the photon with a special wavelength.[52,53] Therefore, an attacker can select the spy photon with the wavelength different from that used by the legitimate users, which will be invisible to Bob's detector. However, in contrast to the IPE attack, the delay photon attack employs a spy photon with the same wavelength as the legitimate photon.[54–56] In experiment, there is a "door" (a time window) of the optical device which is open only during a short time; that is, only when the qubits arrive.[52] An attacker can insert the spy photon after the legitimate photon with a delay time, shorter than the "door" of Bob's optical device, to launch the delay photon attack. For the above-mentioned two situations, Bob cannot find the existence of the spy photon and will perform the exact same operation on them when he performs his unitary operation on the legitimate photon. Once both of them are sent to Trent, the attacker can capture the spy photon and deduce Bob's secret key by performing an appropriate measurement. In order to protect our enhanced AQS scheme from the Trojan-horse attacks, two additional devices, a wavelength filter and a photon number splitter (PNS),[54–56] should be inserted in front of Bob's devices to filter out the illegitimate photon signal in Step (III)-1. That is, when the received photons pass through both devices, the photon signal with an illegitimate wavelength will be first filtered out. Then, Bob chooses a sufficiently large subset of photons randomly and splits each sampling signal with a PNS (in practical application, a photon beam splitter with PBS: 50/50 is more feasible). By performing the measurement on the two signals after the PNS with the measure bases $Z = \{|0\rangle, |1\rangle\}$ and $X = \{|+\rangle, |-\rangle\}$ chosen randomly, Bob can detect the delay photon attack, such that our enhanced AQS scheme is secure against the Trojan-horse attacks and Bob cannot achieve the disavowal of Alice's signature.

6. Conclusion and further works

In this study, we investigated the existing AQS schemes as well as their cryptanalysis, and put forward an enhanced AQS scheme. More importantly, we have pointed out that most of the existing AQS schemes can be cracked by a special DoS attack, which is an open problem that needs to be solved urgently. By launching this attack strategy, a malicious receiver, Bob, can actively negate the signature from Alice, without being detected, to get some benefits in his favor. To overcome this security flaw, we have presented some important improvements and discussed how the arbitrator solves the dispute when Bob claims a failure in the signature verification phase in detail. Meanwhile, we also demonstrated that another security problem, that is, the signatory, Alice, can successfully disavow any message she ever signed by the intercept–resend attack, which can be made up owing to the proposed improvements. Moreover, we have shown the security of our enhanced AQS scheme for these certain attacks. To further improve the AQS scheme, in our opinion, the following topics should be studied in the future.

I) As mentioned in the AQS schemes, quantum state comparison techniques[48] is commonly used. However, as we know, only a probabilistic result can be given when two unknown quantum states are compared. If only a few qubits are changed when they are sent to the receiver in some phase, it may not be discovered with certain probability. Therefore, can we construct a hash function on quantum message to make a deterministic comparison similar to the cryptographic hash function in classic quantum signature scheme?

II) To resist Trojan-horse attacks, a wavelength filter and a PNS should be added in front of Bob's devices before performing any operations. However, Bob should select enough quantum states for the Trojan-horse detection, which may destroy the integrity of the quantum signature pair. Therefore, how to further improve the AQS scheme to avoid the Trojan-horse attacks will be an interesting research topic.

References

[1] Ong H and Schnorr C P 1991 *Eurocrypt* 90 *LNCS* **473** 432
[2] Brands S A 1994 *Crypto* 93 *LNCS* **773** 302
[3] Bennett C H and Brassard G 1984 *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (Bangalore, India) p. 175
[4] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[5] Zhou N R, Song H C, Gong L H and Liu Y 2012 *Acta Phys. Sin.* **61** 214203 (in Chinese)
[6] Zhu C H, Pei C X, Quan D X, Gao J L, Chen N and Yi Y H 2010 *Chin. Phys. Lett.* **27** 090301
[7] Yue X L, Wang J D, Wei Z J, Guo B H and Liu S M 2012 *Acta Phys. Sin.* **61** 184215 (in Chinese)
[8] Chen M J and Liu X 2011 *Chin. Phys. B* **20** 100305
[9] Zhang Z R, Liu W T and Li C Z 2011 *Chin. Phys. B* **20** 050309
[10] Zhu Z C, Zhang Y Q and Fu A M 2011 *Chin. Phys. B* **20** 040306
[11] Shi R H, Huang L S, Yang W and Zhong H 2011 *Chin. Phys. Lett.* **28** 050303
[12] Li X H, Duan X J, Zhou H Y and Deng F G 2009 *Chin. Phys. B* **18** 3710
[13] Zhu F C, Yang Y G and Wen Q Y 2007 *Chin. Phys.* **16** 1838
[14] Gu B, Huang Y G, Fang X and Zhang C Y 2011 *Chin. Phys. B* **20** 100309
[15] Lin S, Gao F and Liu X F 2011 *Chin. Phys. Lett.* **28** 030302
[16] Li C Y, Li X H, Deng F G and Zhou H Y 2008 *Chin. Phys. B* **17** 2352
[17] Yang Y G 2008 *Chin. Phys. B* **17** 415
[18] Wang T Y and Wei Z L 2012 *Quantum Inf. Process.* **11** 455
[19] Cao H J, Wang H S and Li P F 2013 *Int. J. Theor. Phys.* **52** 1188
[20] Wen X J, Chen Y Z and Fang J B 2013 *Quantum Inf. Process.* **12** 549
[21] Wang T Y and Wen Q Y 2010 *Chin. Phys. B* **19** 060307
[22] He L B, Huang L S, Yang W and Xu R 2012 *Chin. Phys. B* **21** 030306
[23] Zhang M, Xu G A, Chen X B, Yang S and Yang Y X 2013 *Int. J. Theor. Phys.* **52** 331
[24] Zou X F and Qiu D W 2013 *Quantum Inf. Process.* **12** 2071
[25] Zeng G H and Keitel C H 2002 *Phys. Rev. A* **65** 042312
[26] Curty M and Lütkenhaus N 2008 *Phys. Rev. A* **77** 046301
[27] Zeng G H 2008 *Phys. Rev. A* **78** 016301
[28] Li Q, Chan W H and Long D Y 2009 *Phys. Rev. A* **79** 054307
[29] Gao F, Qin S J, Guo F Z and Wen Q Y 2011 *Phys. Rev. A* **84** 022344
[30] Choi J W, Chang K Y and Hong D 2011 *Phys. Rev. A* **84** 062330
[31] Zhang K J, Zhang W W and Li D 2013 *Quantum Inf. Process.* **12** 2655
[32] Zou X F and Qiu D W 2010 *Phys. Rev. A* **82** 042325
[33] Hwang T, Luo Y P and Chong S K 2012 *Phys. Rev. A* **85** 056301
[34] Lee H, Hong C, Kim H, Lim J and Yang H J 2004 *Phys. Lett. A* **321** 295
[35] Yang Y G, Zhou Z, Teng Y W and Wen Q Y 2011 *Eur. Phys. J. D* **61** 773
[36] Luo M X, Chen X B, Yun D and Yang Y X 2012 *Int. J. Theor. Phys.* **51** 2135
[37] Li W, Fan M Y and Wang G W 2012 *Chin. Phys. B* **21** 120305
[38] Li W, Fan M Y and Wang G W 2011 *Acta Phys. Sin.* **60** 080302 (in Chinese)
[39] Barnum H, Crepeau C, Gottesman D, Smith A and Tapp A 2002 *Proceedings of the* 43*rd Annual IEEE Symposium Conference on Foundations of Computer Science* (IEEE, Los Alamitos) p. 449
[40] Hwang T, Chong S K, Luo Y P and Wei T X 2011 *Opt. Commun.* **284** 3144
[41] Boykin P O and Roychowdhury V 2003 *Phys. Rev. A* **67** 042317
[42] Cao C, Wang C, He L Y, Tong X, Lei M and Zhang R 2013 *J. Opt. Soc. Am. B* **30** 2136
[43] Cao C, Wang C, He L Y and Zhang R 2013 *Opt. Express* **21** 4093
[44] Wang C, Zhang Y and Zhang R 2011 *Opt. Express* **19** 25685
[45] Lee H, Lin J and Yang H J 2006 *Phys. Rev. A* **73** 042305
[46] Zhang Z J, Liu J, Wang D and Shi S H 2007 *Phys. Rev. A* **75** 026301
[47] Yen C A, Horng S J, Coan H S, Kao T W and Chou Y H 2009 *Quantum Inf. Comput.* **9** 0376
[48] Buhrman H, Cleve R, Watrous J and de Wolf R 2001 *Phys. Rev. Lett.* **87** 167902
[49] Lo H K, Ma X F and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[50] Jiao R Z, Zhang C and Ma H Q 2011 *Acta Phys. Sin.* **60** 110313 (in Chinese)
[51] Zhou Y Y and Zhou X J 2011 *Acta Phys. Sin.* **60** 100301 (in Chinese)
[52] Li X H, Deng F G and Zhou H Y 2006 *Phys. Rev. A* **74** 054302
[53] Cai Q Y 2003 *Phys. Rev. Lett.* **91** 109801
[54] Gao F, Guo F Z, Wen Q Y and Zhu F C 2008 *Phys. Rev. A* **77** 014302
[55] Deng F G, Li X H, Zhou H Y and Zhang Z J 2005 *Phys. Rev. A* **72** 044302
[56] Gisin N, Fasel S, Kraus B, Zbinden H and Ribordy G 2006 *Phys. Rev. A* **73** 022320