Security analyses and improvement of arbitrated quantum signature with an untrusted arbitrator

Xiangfu Zou[1]   Daowen Qiu[2,3]   Paulo Mateus[3]

[1] School of Mathematics & Computational Science,
Wuyi University, Jiangmen 529020, China

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

[3] SQIG–Instituto de Telecomunicações,
Departamento de Matemática, Instituto Superior Técnico,
University of Lisbon, Av. Rovisco Pais 1049-001, Lisbon, Portugal

Abstract

Very recently, an *arbitrated quantum signature* (AQS) scheme of classical message with an untrusted arbitrator was presented[Eur. Phys. J. D **61**(3), 773 (2011)]. In this paper, the security of the AQS scheme with an untrusted arbitrator is analyzed. An AQS scheme with an untrusted arbitrator should satisfy the unforgeable property and undeniable property. In particular, the malicious verifier can not modify a message and its signature to produce a new message with a valid signature, and the dishonest signer who really has sent the message to the verifier which the verifier accepted as an authentic one cannot later deny having sent this message. However, we show that, in the AQS scheme with an untrusted arbitrator, the dishonest signer can successfully disavow his/her signature and the malicious verifier can counterfeit a valued signature for any message by known message attack when he has received a message-signature pair. Then, we suggest an improved AQS scheme of classical message with an untrusted arbitrator that can solve effectively the two problems raised above. Finally, we prove the security of the improved scheme.

Keywords: Quantum cryptography; Quantum signature; Arbitrated quantum signature; Known message attack

1 Introduction

The most spectacular discovery in quantum computing to date is that 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 that most of the classical public key cryptography are not secure if quantum computers could be available someday. Fortunately, quantum key distribution depends on the fundamental laws of quantum physics to provide unconditional security [2–9]

A digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature makes the receiver believe that the message was created by a known sender and not altered in transit. Digital signatures are commonly used for the cases where it is important to detect forgery or tampering, such as:

software distribution and financial transactions. Similar to the 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 turn to investigate quantum signatures and authentication, which is supposed to provide an alternative scheme with unconditional security. Since Gottesman and Chuang [10] proposed the first quantum digital signatures scheme based on weak quantum one-way functions, a lot of progress has been made on quantum signatures [11–24]. For instance, Zeng and Keitel [13] proposed an *arbitrated quantum signature* (AQS) scheme with many merits. This AQS scheme was further discussed in the corresponding comments [25, 26]. It can sign both known and unknown quantum states. Also, it was claimed that the unconditional security is ensured by using the correlation of Greenberger-Horne-Zeilinger (GHZ) triplet states [27, 28] and quantum one-time pads [29]. Li *et al.* [14] presented an arbitrated quantum signature scheme using 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. However, the authors [24] found that the existing AQS schemes [13, 14] can be repudiated by the receiver Bob, and proposed two improved AQS schemes to conquer this shortcoming.

Ingemarsson and Simmons [30] pointed out that there is nobody trusted by all of the participants in commercial and/or international applications. Note that, in the arbitrated signature schemes [13, 14, 26] mentioned above, all communications involve an arbitrator who has access to the contents of the messages. The security of most arbitrated signature schemes [13, 14, 26] depends heavily on the trustworthiness of the arbitrators. Nevertheless, in real applications, the arbitrator may be compromised, that is, the existing arbitrated schemes [13, 14, 26] could not prevent the arbitrator from attacking, i.e., impersonation or forgery. Cao and Markowitch [31] thought that arbitrated signature scheme proposed by Zeng and Keitel [13, 26] is artificial because its security entirely depends on the presence of a trustworthy arbitrator. Therefore, Yang *et al.* [32] considered the issue of arbitrated signature of classical messages with an untrusted arbitrator and illustrated its feasibility. However, in this paper, we will show that the AQS scheme with an untrusted arbitrator [32] is insecure.

The remainder of this paper is organized as follows. First, in Section 2, we briefly review the AQS scheme with an untrusted arbitrator [32]. Then, in Section 3, we recall the security requirements of the AQS scheme of classical message with an untrusted arbitrator [32]. Afterwards, in Section 4, we show that the dishonest signer can successfully disavow his/her signature and the malicious verifier can counterfeit a valued signature when he has received a message-signature pair. Moreover, in Section 5, we suggest an improved AQS scheme with an untrusted arbitrator which can solve effectively the problems raised above. In addition, in Section 6, we show the security of the improved AQS scheme with an untrusted arbitrator. Finally, in Section 7, we make a conclusion.

2 Review of the AQS scheme with an untrusted arbitrator

In the interest of readability, in this section, we briefly review the AQS scheme with an untrusted arbitrator in Ref. [32].

The AQS scheme with an untrusted arbitrator includes three parts: The set-up phase, the signature phase, and the verification phase where the verification phase includes two security checking phases. As the other AQS schemes, the AQS scheme with an untrusted arbitrator also involves three participants: The signer Alice, the verifier Bob, and the arbitrator Trent, where Alice sends a classical message M to Bob through Trent's arbitration. The scheme is described as follows.

2.1 Scheme set-up

(1) Alice shares her k-bit secret key K_A with the arbitrator through quantum key distribution (QKD) protocols [2–4], which were proved to be unconditionally secure [5, 6].

(2) Likewise, Bob obtains his k-bit secret key K_B shared with the arbitrator.

(3) To prevent the arbitrator's forgery attack, Alice sends Bob a k-bit secret key K_s through QKD protocols.

2.2 Signature phase

(1) Alice chooses a random number $r_1 \in \{0,1\}^{k-k_1}$ and computes $R_A = r_1 \| H(M, ID_A, ID_B, r_1, T)$, where the role of T and the random number r_1 is to determine the time of this session and resist the replay attack. ID_A and ID_B are the identity of Alice and Bob, "$\|$" denotes "concatenate" and hash function $H(\cdot) : \{0,1\}^* \to \{0,1\}^{k_1}$ is used to generate a digest. Here, the value of k_1 depends on the chosen hash function.

(2) Then she generates the signature $|R_A\rangle$ by encoding the string R_A in terms of the key K_A and K_s, denoted as $E_{(K_s \oplus K_A)}[R_A]$. The value of $K_A^i \oplus K_s^i$ determines the encoding basis, i.e., if $K_A^i \oplus K_s^i$ is 0, $(R_A)^i$ is encoded with the basis $\{|0\rangle, |1\rangle\}$; else if $K_A^i \oplus K_s^i$ is 1, $(R_A)^i$ is encoded with the basis $\{|+\rangle, |-\rangle \| |\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)\}$, where $K_A^i \oplus K_s^i$ denotes the ith bit of the secret key $K_A \oplus K_s$. Afterwards, before Alice sends $|R_A\rangle$ to the arbitrator, she inserts a certain number of qubits into the sequence at random positions with the probability p_d. All these qubits are randomly in one of the four nonorthogonal states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, which can be used to check eavesdropping. Then she sends the quantum string containing the signature $|R_A\rangle$ to the arbitrator.

2.3 The first security checking phase

(1) When the arbitrator receives the quantum string, he informs Alice of the fact.

(2) After hearing from the arbitrator, Alice first publishes the positions and the *measuring bases* (MBs) of the sampling particles.

(3) The arbitrator measures the sampling particles in the received sequence in the same MBs and then publishes his measurement results.

(4) Alice can check eavesdropping by comparing the arbitrator's measurement results with the initial states of the sampling particles. If the error rate is lower than a predetermined small value ε_1, Alice confirms that no eavesdropper exists and announces this fact. Then she sends the strings M, ID_A, ID_B to Bob via a classical channel and the strings ID_A, ID_B to the arbitrator via a classical channel. Otherwise, they abort the communication.

2.4 Verification phase

(1) The arbitrator decrypts $|R_A\rangle$ using the key K_A and gets $E_{K_s}[R_A]$. That is, if K_A^i is 0, he performs I operation on $(|R_A\rangle)^i$; else if K_A^i is 1, he performs on $(|R_A\rangle)^i$ the operation $\hat{H}$, where $\hat{H} = \frac{1}{\sqrt{2}}\left[\begin{array}{cc} 1 & 1 \\ 1 & -1 \end{array}\right]$. Then the arbitrator encrypts the qubit string $E_{K_s}[R_A]$ with K_B, denoted as $E_{(K_s \oplus K_B)}[R_A]$. For instance, if K_B^i is 0, $(E_{K_s}[R_A])^i$ is intact; else if K_B^i is 1, he performs on $(E_{K_s}[R_A])^i$ the operation $\hat{H}$. To check eavesdropping in the arbitrator-Bob quantum channel, the arbitrator inserts a certain number of photons into the sequence at random positions with the probability p_c. All these checking photons are randomly in one of the four nonorthogonal states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Then the arbitrator sends the qubit string to Bob.

(2) Bob first performs the second security check. If no error occurs, Bob decrypts $E_{(K_s \oplus K_B)}[R_A]$ using the keys K_B and K_s and gets $R_A' = r_1' \| H'$. In detail, if $K_B^i \oplus K_s^i$ is 0, Bob measures $(E_{(K_s \oplus K_B)}[R_A])^i$ with the basis $\{|0\rangle, |1\rangle\}$. Otherwise, Bob measures $(E_{(K_s \oplus K_B)}[R_A])^i$ with the basis $\{|+\rangle, |-\rangle\}$.

(3) To verify the signature, Bob has to get the help of Alice to obtain the knowledge of T. He asks Alice to publish T. Using the classical strings M, ID_A, ID_B and T sent from Alice, Bob can compute $H(M, ID_A, ID_B, r_1', T)$ and compare it with H'. If $H(M, ID_A, ID_B, r_1', T) = H'$, he can judge that the message comes from Alice and authenticate the authenticity of Alice and the integrity of the message M. The signature key K_s are updated to $K_s \oplus r_1' \| H'$. Otherwise, Bob rejects and they have to establish some new secret keys.

2.5 The second security checking phase

(1) After hearing from Bob, the arbitrator first publishes the positions and the MBs of the sampling particles.

(2) Bob measures the sampling particles in the received sequence in the same MBs and then publishes his measurement results.

(3) The arbitrator then checks eavesdropping by comparing Bob's measurement results with the initial states of the sampling particles. If the error rate is lower than a predetermined small value ε_2, the arbitrator confirms that no eavesdropper exists and announces this fact.

3 The security requirements of the AQS scheme with an untrusted arbitrator

In this section, we further recall the security requirements of the AQS scheme with an untrusted arbitrator [32].

3.1 Unforgeable property

(1) *The outside opponent.* The outsider cannot impersonate Alice to send a forged message to the verifier Bob, and/or tamper the message sent from Alice to Bob.

(2) *The verifier.* The dishonest verifier who never received the message from Alice cannot present the correct evidence of having received it.

(3) *The arbitrator.* The dishonest arbitrator cannot send a message to Bob which Bob will accept as authentic.

3.2 Undeniable property

(1) *The signer.* The dishonest signer who really has sent the message to Bob which Bob accepted as authentic cannot later deny having sent this message.

(2) *The verifier.* The dishonest verifier who has verified the signature cannot later deny his involvement.

3.3 Discussion about the arbitrator

By the security requirements of the AQS scheme with an untrusted arbitrator [32], we only need to consider the arbitrator's forging and impersonating. The discussions of the disavowal attack by the arbitrator collaborating with Alice and the disavowal attack by the arbitrator collaborating with Bob are not necessary for the AQS with an untrusted arbitrator. In fact, they can not be achieved in AQS schemes including the original scheme [32]. The disavowal attack by the arbitrator collaborating with Alice is not avoidable. If the arbitrator collaborating with the signer Alice disavowals the signature, Bob could not prove their disavowal to other people though he can discover their disavowal. Similarly, the disavowal attack by the arbitrator collaborating with Bob is not avoidable. According to this view, the untusted arbitrator Trent is semi-honest. Trent is not completely untrustworthy. Under normal circumstances, Trent fulfills his duties seriously when Alice sends a quantum signature to Bob. However, we need to prevent Trent to forge Alice's signature and impersonate Alice to send a signature for his interests.

4 Security analyses of AQS scheme with an untrusted arbitrator

In this section, we first give an example using AQS schemes with an untrusted arbitrator [32]. Then, we show that the dishonest signer can successfully disavow his/her signature and the malicious verifier can counterfeit a valued signature for any message when he has received a message-signature pair.

4.1 An example using AQS scheme with an untrusted arbitrator

In this subsection, we give an example needing arbitrated signature schemes with an untrusted arbitrator. As the Ref. [32], we consider such a scenario in a local network of a company. There is a rigid hierarchy of management in the company. That is, the general manager directly charges the department manager, and each department manager directly charges the staffs in his department.

Example 1 *In a company, the general manager Alice sends a classical message M to a department manager Bob by the AQS scheme with an untrusted arbitrator [32]. The network* *administrator of the company, Trent, is the arbitrator in the AQS scheme. Several days later, there is a dispute between the signer Alice and the verifier Bob. Alice says that the message is M_1. However, Bob declares that the message sent by Alice is M_2 and $M_2 \neq M_1$.*

In the following subsections, we will show that all people including the arbitrator Trent can not settle the dispute.

4.2 The signer's disavowal

In this subsection, we show that the dishonest signer Alice can successfully disavow her signature.

In Ref. [32], it was thought that the dishonest signer Alice can not intercept and forge quantum signature when Trent sends it to Bob because she does not know the secret key K_B and the correct positions of the checking qubits inserted in the quantum string. Therefore, Alice's forgery attack will introduce errors in Bob's measurement outcomes of checking bits. However, Alice can disavow her signature.

As Example 1, there is a dispute between Alice and Bob. Alice says that the sending message is M_1 while Bob declares that the message sent by Alice is M_2. Suppose that, the real sending message $M = M_2$ and Alice disavowed her signature message by declaring the sending message "$M = M_1$". Clearly, Bob knows that the message received from Alice is M_2 and $M_2 \neq M_1$. However, Bob has not enough evidence to prove Alice's disavowal.

Bob received M, ID_A, ID_B and T from Alice, and $|R_A\rangle = E_{K_s}[R_A]$ with $R_A = r_1 \| H(M, ID_A, ID_B, r_1, T)$ from Trent. However, these are not enough to prove Alice's disavowal. Note that, *Trent does not know the contents of $|R_A\rangle$ because he does not know the secret key K_s.* Thereby, Trent knows nothing but Alice has sent some signature to Bob. When Alice says that she sent "M_1, ID_A, ID_B and T" to Bob and $|R_1\rangle = E_{K_s}[R_1]$ with $R_1 = r_1 \| H(M_1, ID_A, ID_B, r_1, T)$ to Trent while Bob declares that he received "M_2, ID_A, ID_B and T" from Alice and $|R_2\rangle = E_{K_s}[R_2]$ with $R_2 = r_1 \| H(M_2, ID_A, ID_B, r_1, T)$ from Trent. Trent can not arbitrate. Similarly, nobody can resolve this dispute between Alice and Bob.

By the discussion above, the signer can disavow her signature successfully.

4.3 The verifier's counterfeiting

In this subsection, we show that the malicious verifier can counterfeit a valued signature when he has received a message-signature pair.

In Ref. [32], it was considered only that the malicious verifier Bob intercepts and forges quantum signature $|R_A\rangle$ when Alice sends it to Trent. This can not succeed because Bob cannot distinguish the information qubits and the checking qubits. However, Bob can counterfeit Alice's signature after he receives it from Trent.

In Example 1, there is a dispute between Alice and Bob. Alice says that the sending message is M_1 while Bob declares that the message sent by Alice is M_2. Suppose that, the real sending message $M = M_1$ and Bob disavowed his receiving M_1 with Alice's signature by declaring "the sending message M is M_2". Clearly, Alice knows that the sending message is M_1 and $M_1 \neq M_2$. However, Alice has not enough evidence to prove Bob's disavowal.

Similar to the discussion in Subsection 4.2, *Trent does not know the contents of $|R_A\rangle$ because he does not know the secret key K_s.* Thereby, Trent knows nothing but Alice has sent some signature to Bob.

When Bob lies that he received "M_2, ID_A, ID_B and T" from Alice and $|R_2\rangle = E_{K_s}[R_2]$ with $R_2 = r_1\|H(M_2, ID_A, ID_B, r_1, T)$ from Trent while Alice says that she sent "M_1, ID_A, ID_B and T" to Bob and $|R_1\rangle = E_{K_s}[R_1]$ with $R_1 = r_1\|H(M_1, ID_A, ID_B, r_1, T)$ to Trent. Trent can not arbitrate. Similarly, nobody can resolve this dispute between Alice and Bob.

By the discussion above, we know that Bob can successfully counterfeit Alice's signature for a new message M_2.

5 An improved arbitrated quantum signature scheme with an untrusted arbitrator

In this section, we give an improved arbitrated quantum signature scheme with an untrusted arbitrator of classical message. This scheme can solve effectively the problems raised above.

For convenience, we use $E_K[R]$ to denote that the classical message R is encoded into quantum states in terms of the key K as

$$(E_K[R])^i = \begin{cases} |0\rangle, \text{ if } K^i \oplus K_s^i{=}0 \,\&\, R^i{=}0, \\ |1\rangle, \text{ if } K^i \oplus K_s^i{=}0 \,\&\, R^i{=}1, \\ |+\rangle, \text{ if } K^i \oplus K_s^i{=}1 \,\&\, R^i{=}0, \\ |-\rangle, \text{ if } K^i \oplus K_s^i{=}1 \,\&\, R^i{=}1. \end{cases} \tag{1}$$

The setting of the improved AQS scheme with an untrusted arbitrator is as follows:

(1) Alice, Bob and Trent have an error-free quantum channel for their quantum communication;

(2) They have an unblocked public classical communication channel (or, a classical public board) which are assumed to be susceptible to eavesdropping but not to be the injection or alteration of messages.

The improved AQS scheme with an untrusted arbitrator also includes three parts: The set-up phase, the signature phase, and the verification phase where the verification phase includes two security checking phases. Also, it involves three participants: The signer Alice, the verifier Bob, and Trent, where Alice sends a classical message M to Bob through Trent's arbitration. The scheme is described as follows.

5.1 Scheme set-up phase

(1) Alice shares her k-bit signature key K_A with the arbitrator Trent by the quantum key distribution (QKD) protocols [2–4], which were proved to be unconditionally secure [5–9]. To prevent Trent's forgery attack, Alice shares a k-bit secret key K_s with Bob by QKD protocols.

(2) Similarly, Bob obtains his k-bit verification key K_B shared with Trent.

5.2 Signature phase

(1) Alice chooses a random number $r_1 \in \{0,1\}^{k-k_1}$ and computes $R_A = r_1\|H(M, ID_A, ID_B, r_1, T)$, where the role of T and the random number r_1 is to determine the time of this session and resist the replay attack. Here, the value of k_1 depends on the chosen hash function.

(2) Alice generates the signature $|R_A\rangle = E_{(K_s \oplus K_A)}[R_A]$. To check eavesdropping, she inserts a certain number of qubits, which are chosen randomly from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, into the sequence at random positions with the probability p_d. Afterwards, she sends the quantum string containing $|R_A\rangle$ to Trent.

5.3 The first security checking phase

(1) When Trent receives the quantum string, he informs Alice the fact.

(2) After hearing from Trent, Alice first publishes the positions and the MBs of the sampling particles by the public classical communication channel.

(3) Trent measures the sampling particles in the received sequence in the same MBs and then publishes his measurement results by the public classical communication channel.

(4) Alice can check eavesdropping by comparing Trent's measurement results with the initial states of the sampling particles. If the error rate is lower than a predetermined small value ε_1, Alice confirms that no eavesdropper exists and announces this fact. Then, Alice announces publicly M, ID_A, ID_B by the classical communication channel such that both Bob and Trent know them. Otherwise, they abort the communication.

5.4 Verification phase

(1) Trent gets $E_{K_s}[R_A]$ by decrypting $|R_A\rangle$ with the key K_A, i.e.,

$$(E_{K_s}[R])^i = \begin{cases} (|R_A\rangle)^i, & \text{if } K_s^i{=}0, \\ \hat{H}(|R_A\rangle)^i, & \text{if } K_s^i{=}1, \end{cases} \tag{2}$$

where $\hat{H} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$. Then, Trent encrypts the qubit string $E_{K_s}[R_A]$ with K_B, i.e.,

$$(E_{(K_s \oplus K_B)}[R_A])^i = \begin{cases} (E_{K_s}[R])^i, & \text{if } K_B^i{=}0, \\ \hat{H}(E_{K_s}[R])^i, & \text{if } K_B^i{=}1. \end{cases} \tag{3}$$

To check eavesdropping in Trent-Bob quantum channel, Trent inserts a certain number of qubits, which are chosen randomly from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, into the sequence at random positions with the probability p_c. Then, Trent sends the qubit string to Bob.

(2) Bob first performs the second security check. If no error occurs, Bob decrypts $E_{(K_s \oplus K_B)}[R_A]$ using the keys K_B and K_s and gets $R'_A = r'_1 \| H'$. In detail, if $K_B^i \oplus K_s^i$ is 0, Bob measures $(E_{(K_s \oplus K_B)}[R_A])^i$ with the basis $\{|0\rangle, |1\rangle\}$. Otherwise, Bob measures $(E_{(K_s \oplus K_B)}[R_A])^i$ with the basis $\{|+\rangle, |-\rangle\}$.

(3) To verify the signature, Bob asks Alice to publish T.

(4) Alice announces publicly T by the classical communication channel such that both Bob and Trent know it.

(5) Using the classical strings M, ID_A, ID_B and T published by Alice, Bob can compute $H(M, ID_A, ID_B, r'_1, T)$ and compare it with H'. If $H(M, ID_A, ID_B, r'_1, T) = H'$, he judges that the message comes from Alice and authenticates the authenticity of Alice

and the integrity of the message M. Bob announces publicly the fact that Alice's signature is authenticated or not. If it is authenticated, Trent records the messages M, ID_A, ID_B, and T to prevent dissensions. Otherwise, they abort this scheme (They may begin a new signature scheme, i.e., they go to the step (1) of the scheme set-up phase).

5.5 The second security checking phase

(1) After hearing from Bob, Trent first publishes the positions and the MBs of the sampling particles.

(2) Bob measures the sampling particles in the received sequence in the same MBs and then publishes his measurement results.

(3) Trent then checks eavesdropping by comparing Bob's measurement results with the initial states of the sampling particles. If the error rate is lower than a predetermined small value ε_2, Trent confirms that no eavesdropper exists and announces publicly this fact.

The essential differences between the improved scheme and the original scheme [32] are the step (4) of the first security checking phase and the steps (3)–(5) of the verification phase.

6 Security discussions of the improved scheme

In this section, we discuss the security of the improved AQS scheme with an untrusted arbitrator. In particular, we show the improved scheme can resist the two attacks introduced in Section 4.

6.1 Unforgeable property

The outside opponent. The outsider opponent Eve cannot impersonate Alice to send a forged message to the verifier Bob because she does not know the keys K_A and K_s. Similarly, she can not tamper the message because she does not know the keys K_A and K_s, and the positions of the sampling particles.

The verifier. Note that, Alice need announce publicly the messages M, ID_A and ID_B in the step (4) of the first security checking phase and publishes T in the step (4) of the verification phase. Furthermore, the arbitrator Trent need record the messages M, ID_A, ID_B, and T in the step (4) of the verification phase. Thereby, the dishonest verifier Bob can never counterfeit a valued signature for any new message even though he has received a message-signature pair. Otherwise, Trent can find out Bob's counterfeiting because the counterfeit message is different from the message M, or the time stamp is different from the time stamp T.

The arbitrator. If the dishonest arbitrator forges Alice's signature for a new message, Bob may find out Trent's forging because the new message is different from the message M published by Alice in the step (4) of the first security checking phase. Similarly, the dishonest arbitrator can not replay signature because the signature $|R_A\rangle$ containing the time tamp T and the random number r_1. In addition, the dishonest arbitrator can not impersonate Alice to send a signature because the improved scheme needs Alice to publish publicly the messages

M, ID_A and ID_B in the step (4) of the first security checking phase and T in the step (4) of the verification phase.

In addition, the improved scheme can use the technics mentioned in the original paper [32] to resist the Trojan horse attacks.

6.2 Undeniable property

The signer. Note that, in this scheme, Alice need announce publicly the messages M, ID_A and ID_B in the step (4) of the first security checking phase and publish publicly T in the step (4) of the verification phase. Moreover, the messages M, ID_A, ID_B, and T have been recorded by Trent. Therefore, the dishonest signer who really has sent the message to Bob which Bob accepted as authentic cannot later deny having sent this message.

The verifier. The verifier Bob who really has verified the signature cannot later deny his involvement in because he need publish his measurement result in the step (2) of the second security checking phase, his verification of the message needs the help of Alice in the step (3) of the verification phase, and he announces publicly the fact that Alice's signature has been authenticated in the step (5) of the verification phase.

7 Conclusion

We analyzed the security of the AQS scheme with an untrusted arbitrator [32]. More specifically, we showed that the dishonest signer Alice can successfully disavow her signature and the malicious verifier can counterfeit a valued signature when he has received a message-signature pair. Therefore, we gave an improved AQS scheme of classical message with an untrusted arbitrator. This scheme can solve effectively the two problems raised above and its security was proved as well.

Acknowledgements

This work is supported in part by the National Natural Science Foundation (Nos. 61272058, 61073054, 60873055), the Natural Science Foundation of Guangdong Province of China (Nos. 10251027501000004, S2012040007324, S2012010008833), the Specialized Research Fund for the Doctoral Program of Higher Education of China (No. 20100171110042), the Foundation for Distinguished Young Talents in Higher Education of Guangdong Province of China (No. 2012LYM_0126), the Science and Technology Project of Jiangmen City of China (No. [2011]131), and the project of SQIG at IT, funded by FCT and EU FEDER projects QSec PTDC/EIA/67661/2006, AMDSC UTAustin/MAT/0057/2008, NoE Euro-NF, and IT Project QuantTel, FCT project PTDC/EEA-TEL/103402/2008 QuantPrivTel, FCT PEst-OE/EEI/LA0008/2013.

References

[1] Shor, P.W.: Algorithms for quantum computation: Discrete logarithms and factoring. In: Proceedings of Foundations of Computer Science, 1994, The 35th Annual Symposium on, pp. 124–134. IEEE (1994)

[2] Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, pp. 175–179. IEEE (1984)

[3] Ekert, A.K.: Quantum cryptography based on Bell's theorem. Physical Review Letters **67**(6), 661–663 (1991)

[4] Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Physical Review Letters **68**(21), 3121–3124 (1992)

[5] Lo, H.K., Chau, H.F.: Unconditional security of quantum key distribution over arbitrarily long distances. Science **283**(5410), 2050 (1999)

[6] Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Physical Review Letters **85**(2), 441–444 (2000)

[7] Mayers, D.: Unconditional security in quantum cryptography. Journal of the ACM (JACM) **48**(3), 351–406 (2001)

[8] Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography. Reviews of Modern Physics **74**(1), 145–195 (2002)

[9] Inamori, H., Lütkenhaus, N., Mayers, D.: Unconditional security of practical quantum key distribution. The European Physical Journal D: Atomic, Molecular, Optical and Plasma Physics **41**(3), 599–627 (2007)

[10] Gottesman, D., Chuang, I.: Quantum digital signatures. ArXiv:quant-ph/0105032 (2001)

[11] Barnum, H., Crépeau, C., Gottesman, D., Smith, A., Tapp, A.: Authentication of quantum messages. In: Foundations of Computer Science, 2002, The 43rd Annual IEEE Symposium on, pp. 449–458. IEEE (2002)

[12] Curty, M., Santos, D.J., Pérez, E., García-Fernández, P.: Qubit authentication. Physical Review A **66**(2), 022301 (2002)

[13] Zeng, G., Keitel, C.H.: Arbitrated quantum-signature scheme. Physical Review A **65**(4), 042312 (2002)

[14] Li, Q., Chan, W.H., Long, D.Y.: Arbitrated quantum signature scheme using Bell states. Physical Review A **79**(5), 054307 (2009)

[15] Lee, H., Hong, C., Kim, H., Lim, J., Yang, H.J.: Arbitrated quantum signature scheme with message recovery. Physics Letters A **321**(5), 295–300 (2004)

[16] Lu, X., Feng, D.: Quantum digital signature based on quantum one-way functions. In: Advanced Communication Technology, 2005 (ICACT 2005), The 7th International Conference on, vol. 1, pp. 514–517. IEEE (2004)

[17] Wang, J., Zhang, Q., Tang, C.: Quantum signature scheme with message recovery. In: Advanced Communication Technology, 2006 (ICACT 2006), The 8th International Conference, vol. 2, pp. 1375–1378. IEEE (2006)

[18] Wang, J., Zhang, Q., Tang, C.: Quantum signature scheme with single photons. Optoelectronics Letters **2**(3), 209–212 (2006)

[19] Wen, X., Liu, Y., Sun, Y.: Quantum multi-signature protocol based on teleportation. Zeitschrift fur Naturforschung A **62**(3/4), 147 (2007)

[20] Zeng, G., Lee, M., Guo, Y., He, G.: Continuous variable quantum signature algorithm. International Journal of Quantum Information **5**(4), 553–573 (2007)

[21] Yang, Y.G.: Multi-proxy quantum group signature scheme with threshold shared verification. Chinese Physics B **17**, 415 (2008)

[22] Lü, X., Feng, D.G.: An arbitrated quantum message signature scheme. Computational and Information Science pp. 1054–1060 (2005)

[23] Cao, Z., Markowitch, O.: Security analysis of one quantum digital signature scheme. In: Information Technology: New Generations, 2009 (ITNG'09), The Sixth International Conference on, pp. 1574–1576. IEEE (2009)

[24] Zou, X., Qiu, D.: Security analysis and improvements of arbitrated quantum signature schemes. Physical Review A **82**(4), 042325 (2010)

[25] Curty, M., Lütkenhaus, N.: Comment on "Arbitrated quantum-signature scheme". Physical Review A **77**(4), 046301 (2008)

[26] Zeng, G.: Reply to "Comment on 'Arbitrated quantum-signature scheme' ". Physical Review A **78**(1), 016301 (2008)

[27] Greenberger, D.M., Horne, M.A., Zeilinger, A.: Going beyond Bell's theorem. ArXiv:0712.0921 (2007)

[28] Greenberger, D.M., Bernstein, H.J., Horne, M.A., Shimony, A., Zeilinger, A.: Proposed GHZ experiments using cascades of down-conversions. In: Quantum Control and Measurement, vol. 1, p. 23 (1993)

[29] Boykin, P.O., Roychowdhury, V.: Optimal encryption of quantum bits. Physical Review A **67**(4), 042317 (2003)

[30] Ingemarsson, I., Simmons, G.: A protocol to set up shared secret schemes without the assistance of a mutually trusted party. In: Advances in Cryptology, 1990 (EUROCRYPT'90), pp. 266–282. Springer (2006)

[31] Cao, Z., Markowitch, O.: A note on an arbitrated quantum signature scheme. International Journal of Quantum Information **7**(6), 1205–1209 (2009)

[32] Yang, Y.G., Zhou, Z., Teng, Y.W., Wen, Q.Y.: Arbitrated quantum signature with an untrusted arbitrator. The European Physical Journal D: Atomic, Molecular, Optical and Plasma Physics **61**(3), 773–778 (2011)