International Journal of Security and Its Applications
Vol.9, No.1 (2015), pp.77-88
http://dx.doi.org/10.14257/ijsia.2015.9.1.09

New Arbitrated Quantum Signature Scheme without Entangled state

Jiang guanXiong [1]* and Zhang Jun[1,2]

[1]*Department of Computer, ShaoXing University, 312000, China*
[2]*Key Laboratory of E-Business and Information Security, Hangzhou Normal University, Hangzhou 310036, China)*
zscasjgx@foxmail.com

Abstract

Arbitrated quantum signature (AQS) schemes use quantum cryptography to ensure their security, and the schemes provide that the signature receiver verifies the signature with the arbitrator's assistance. Very recently, Gao and Choi found in some previous AQS schemes, the receiver, Bob can counterfeit the signer's signature under known message. Additionally, the paper gives the security analysis of the AQS scheme, and results show that not only the receiver, but also the attacker can forge the signature in the AQS scheme. Furthermore, the signer can successfully disavow any message she ever signed. To conquer these shortcomings, this paper gives a new AQS scheme without quantum entangled state; it uses special quantum logic gate and new quantum one-time pads to ensure its security. Compares with other previous AQS schemes, the new scheme has following advantages: (1) the new scheme guarantees the receiver and the attacker cannot forge the signature; (2) Because the new scheme does not use quantum entangled states, so it can reduce the complexity of implementation and provides a higher efficiency in transmission; (3) The receiver, Bob has verified the signature's integrity, so Alice cannot disavow her having signed message.

Keywords: *Arbitrated quantum signature (AQS), Entangled state, Pauli operation*

1. Introduction

Digital signature is very important in cryptography. The digital signature has the function of non-disavowal and message authentication. Because of impossible of counterfeiting or disavowing, digital signature is very important in the modem electronic data processing system. Arbitrated signature is a special signature, which provides the sender sign the signature, and the receiver verifies the signature with the arbitrator's assistance.

As everyone know, the security of traditional digital signature is based on the assumption of mathematical computational complexity, such as the discrete logarithm problem (DLP) or factoring large numbers problem(RSA). However, if quantum computer is invented someday, most of the traditional digital signature schemes would be broken easily by Shor's algorithm [1]. Differs from the classical cryptography, quantum cryptography ensure its security by physical principles. The quantum cryptography gives us unconditional security by quantum no-cloning theorem and the Heisenberg uncertainty principle.

So, many researchers and scholars had shown interests in quantum signature schemes and some progress has been made on quantum signature schemes [2-16]. Quantum signature depends on fundamental laws of quantum key distribution (QKD) [17-18], which can be proved to be unconditional security [19-22].

If the quantum signature scheme is secure, it must satisfies two characteristics: (1) no one include the receiver can forge the signature, even if the attacker intercepts the signature; (2) the signer cannot disavow her having signed the message and the receiver

ISSN: 1738-9976 IJSIA

cannot disavow his having receiving the signature. There were some arbitrated quantum signature (AQS) schemes with quantum message are not secure [2, 4, 8]. As the Ref. [9] proposed, the receiver Bob can achieve existential forgery of the signer Alice's signature under known message attack, and the signer Alice can disavow any of her signatures in Li's AQS scheme; similarly, Choi had showed that the Zeng's scheme was not be secure too [10].

In this paper, we study the some AQS scheme using entangled states and find there are some shortcomings in the AQS scheme. (1) Similarly as the Ref. [9, 10] proposed, the receiver, Bob also can use known message attack and forge the signature. (2) More seriously, because the signer, Alice does not encrypt her measurement, so anyone can achieve universal forgery of Alice's signature. (3) Because the receiver, Bob doesn't verify the signature's integrity, it gives the signer, Alice to disavow her having signing the message.

2. Brief Review of arbitrated quantum signature (AQS) scheme using Quantum Entangled States

Step 1: the receiver Bob gets her private key shared with the arbitrator Chile by BB84 or EPR protocol, it can be proved unconditional security. Similarly, the signer Alice also gets his private key shared with the arbitrator Chile. Therefor Chile had the Alice's and Bob's private key, so she can help Bob to verify the signature.

Step 2: The signer, Alice generates *n EPR* pairs or GHZ pairs $|\varphi> = \{|\varphi_1>, |\varphi_2>, \cdots\cdots, |\varphi_n>\}$, with

$$|\varphi_i> = \frac{1}{\sqrt{2}}(|0_A 0_B> + |1_A 1_B>) \quad or \quad |\varphi_i> = \frac{1}{\sqrt{2}}(|0_A 0_B 0_C> + |1_A 1_B 1_C>) \qquad \textbf{(1)}$$

Then, Alice distributes one particle of *EPR* pairs or GHZ to Bob, and the other to herself.

Step 3: For (i=1 to n), Alice combines each qubit message state $|P_i>$ with the *EPR* pairs or GHZ pairs $|\varphi_i>$, then she gets the result $|A_i>$, denoted by $|A>=|\varphi> \otimes |P>$

Step 4: Alice measures the Bell $|A>$ and gets the measurement $|M_{A_i}>$, with $|M_{A_i}> \in \{|\psi^+>, |\psi^->, |\phi^+>, |\phi^->\}$.

Step 5: Alice generates the quantum signature with quantum one-time pads by Alice's private key[23], denoted as $|S>= E_{K_A}(|P>)$.

Step 6: Alice sends the quantum signature $|S>$, the quantum message $|P>$ and the measurement $|M_A>$ to the signature receiver Bob through a quantum channel.

Step 7: When the receiver Bob receives the quantum signature, he sends the quantum signature to the arbitrator Chile directly.

Step 8: Subsequently, the arbitrator Chile generates the encrypted message $|S'>= E_{K_A}(|P>)$ with quantum message $|P>$ and Alice's private key. Then, Chile compares $|S'>$ with $|S>$ as the *Ref.[24]*.

Step 9: After that, the arbitrator Chile use Bob's private key to encrypt the judgment *V*, the quantum signature $|S>$ and the quantum message $|P>$; then, she sends it back to the receiver Bob.

Step 10: Finally, Bob recovers the quantum message $|P_B>$ by quantum teleportation. Then, Bob compares the quantum message $|P>$ with the recovered

message $|P_B>$ as the *Ref.*[25], if $|P>=|P_B>$, Bob accepts the signature; otherwise, he rejects the signature.

3. Security Analysis These AQS Schemes

There were some shortcomings in these AQS schemes. First, anyone can successfully forge the signer's signature by simple attack. Second, similar with the Ref. [9, 10], the receiver Bob can counterfeit the signer's signature under known message.

3.1. The Attacker, Eve Can Forge the Signature

When the attacker, Eve Intercepts the signature, she can forge these arbitrated quantum signature (AQS) by Pauli operation.

3.1.1. The First Forge Method: In *Step 6*, Alice transfers the quantum signature $|S>$, the quantum message $|P>$ and the measurement $|M_A>$ to Bob directly, instead of encrypting $(|P>,|S>,|M_A>)$. So it gives Eve chance to forge the signature.

Although the attacker doesn't know the context of the quantum signature $|S>$, the context of the quantum message $|P>$ and Alice's private key K_A, she also can forge the signature. Because the traditional quantum one-time pads don't suit for the quantum signature, the receiver Bob can successfully forge a signature after he receives a valid signature pairs. According to these AQS schemes, from the Eq.(1), we can know a valid signature $|S>$ of quantum message $|P>$ should be

$$|S>=E_{K_A}(|P>)=\bigotimes_{i=1}^{n}\sigma_x^{K_{A2i-1}}\sigma_z^{K_{A2i}}|P_i> \quad (2)$$

Note that, the attacker, Eve cannot know Alice's secret key K_A, but he has a valid encrypted quantum message and the quantum signature pairs $(|P>,|S>)$. Now, the problem is, can Eve find another pair of quantum signature when he receives a valid quantum signature $|S>$? In fact, Eve also can find a valid another signature pair $|S'>$ for the quantum message $|P'>$ from the known message attack. If Eve performs $Pauli\{I,\delta_X,\delta_Z,\delta_X\delta_Z\}$ operation on each qubit in the quantum message $|P>$, and gets another quantum information $|P'>$. Then he performs the same *Pauli* operation on each qubit in quantum string $|S>$, and gets $|S'>$. The pair $(|P'>,|S'>)$ will also be a valid quantum message and quantum signature. The forge attack method can be described as follows:

(1) When Alice transfers $(|P>,|S>,|M_A>)$ to Bob, the attacker, Eve intercepts it.

(2) For (i=1 to n), Eve performs *Pauli* operation U_i on every quantum signature $|S_i>$, $U_i\in\{I,\delta_X,\delta_Z,\delta_X\delta_Z\}$, then he gets the forged signature $|S'>$

$$|S'>=U|S>=\bigotimes_{i=1}^{n}U_i|S_i> \quad (3)$$

(3) For (i=1 to n), Eve performs the same *Pauli* operation U_i on every encrypted quantum message $|P_i>$, then she gets the forged quantum message $|P'>$

$$| P' >= U \ | P >= \bigotimes_{i=1}^{n} U_i \ | P_i > \quad (4)$$

But there is only one question, that is the receiver recovers the quantum message $| P >$ by the measurement $| M_A >$. So, if Eve only forges the quantum signature $U | S >$ and forges the quantum message $U | P >$, because the recovered message $| P >$ will not equal to $U | P >$, in Step 10, the receiver Bob would find some one has forged the signature. So Eve must forge the measurement $| M_A >$.

(4) For (i=1 to n), Bob forges the *i*th measurement $| M_{A_i}' >$ with the *i*th *Pauli* operation $U_i \{I, \delta_X, \delta_Z, \delta_X \delta_Z\}$ and the *i*th measurement $| M_{A_i} >$

The results of the measurement $| M_{A_i}' >$ is described as the *Table1*.

Table 1. The Result of the Forged Measurement

$\| M_{A_i}' >$	*The measurement* $\| M_{A_i} >$			
U_i	$\| \psi^+ >$	$\| \psi^- >$	$\| \phi^+ >$	$\| \phi^- >$
I	I	δ_Z	δ_X	$\delta_X \delta_Z$
δ_X	δ_X	$\delta_X \delta_Z$	I	δ_Z
δ_Z	δ_Z	I	$\delta_X \delta_Z$	δ_X
$\delta_X \delta_Z$	$\delta_X \delta_Z$	δ_X	δ_Z	I

The equation can be described as follows:

$$| M_{A_i}' >= U_i \ | M_{A_i} > \quad (5)$$

(5) The attacker, Eve sends the forged signature $(| P' >, | S' >, | M_A' >)$ to Bob.

And the forged signature $(| P' >, | S' >)$ is a valid signature, and no one can find that the attacker Eve has forged the signature. Because $\{E_K, U\} \in \{I, \delta_X, \delta_Z, \delta_X \delta_Z\}$, according to the commutative relations among *Pauli* operations, it can get the equation

$$U_i \sigma_x^{K_{2i-1}} \sigma_z^{K_{2i}} \ | P_i >= \pm (\sigma_x^{K_{2i-1}} \sigma_z^{K_{2i}} U_i \ | P_i >) \quad (6)$$

Because, every qubit $| P_i >= \alpha_i | 0 > + \beta_i | 1 >$ is a pure state of a single particle. Therefore, all the minus signs in Eq. (6) are global phases and can be omitted. So, we can get

$$U_i \sigma_x^{K_{2i-1}} \sigma_z^{K_{2i}} \ | P_i >= \sigma_x^{K_{2i-1}} \sigma_z^{K_{2i}} U_i \ | P_i > \quad (7)$$

As the *Eq.(6)* proposed, $| P_i' >= U_i \ | P_i >$, so, we can get the signature result $| S_A' >$ from the Eq.(5, 6, 7)

$$| S' >= \bigotimes_{i=1}^{n} U_i \sigma_x^{K_{2i-1}} \sigma_z^{K_{2i}} \ | P_i >= \bigotimes_{i=1}^{n} \sigma_x^{K_{2i-1}} \sigma_z^{K_{2i}} U_i \ | P_i >= \bigotimes_{i=1}^{n} \sigma_x^{K_{2i-1}} \sigma_z^{K_{2i}} \ | P_i' > \quad (8)$$

As the *Ref.[25]* proposed, the receiver, Bob recovers the quantum message $|P_B'>$ from the forged measurement $|M_A'>$ and EPR state $|B>$

$$|P_B'>=\bigotimes_{i=1}^{n}(M_{A_i}'|B_i>)=\bigotimes_{i=1}^{n}U_i(M_{A_i}|B_i>)=\bigotimes_{i=1}^{n}U_i|P_i>=\bigotimes_{i=1}^{n}|P_i'>=|P'> \quad (9)$$

From the *Eq.(9)*, we can know $|S'>=U|S>=E_{K_A}(U|P>)=E_{K_A}(|P'>)$, so the arbitrator, Chile regards the signature is signed by the signer. And from the *Eq.(9)*, it can get the result $|P_B>=|P'>$, so the receiver Bob hold the forged signature as Alice's signature $U|S>$ for the quantum message $U|P>$. Hence, Eve can forge the signature $(U|P>,U|S>,U|M_A>)$, and Bob regards the forged signature $U|S>$ is a valid signature for the quantum message $\bigotimes_{i=1}^{n}\sigma_z^{r_{2i}}\sigma_x^{r_{2i-1}}U_i|P_i>$.

3.1.2. The Second Forge Method: *In Step 9:* The arbitrator Chile generates $E_{K_B}(|P>,|S>,V)$ and sends it back to the Bob, it can be described

$$E_{K_B}(|P>,|S>,V)=E_{K_B}(|P>)\otimes E_{K_B}(|S>)\otimes E_{K_B}(V) \quad (10)$$

Because Bob only compares the recovered quantum message $|P_B>$ with the original quantum message $|P>$, the quantum signature $|S>$ is not involved in Bob's verification. So, if Alice sign the quantum message $|P>$ correctly, and no one intercepts $|S>$, $E_{K_B}(|P>,|S>,V)$, the equation $|S>=E_{K_A}(|P>)$ would hold, so the judgment *V*=1. If Eve intercepts $E_{K_B}(|P>,|S>,V)$, she can generate any quantum string $|S'>$. And Bob would regard the forged signature $D_{K_B}(|S'>)$ is valid signature. Here $D_{K_B}(|S'>)$ means decrypts $|S'>$ with Bob's private key K_B. The attack method as follows:

(1) In *step 9*, Chile sends $E_{K_B}(|P>,|S>,V)$ to Bob, while the attacker, Eve intercepts it, and then she generates another quantum string $|S'>=(|s_1'>,|s_2'>,\cdots\cdots,|s_n'>)$.

(2) Eve forges $E_{K_B}(|P>)\otimes|S_A'>\otimes E_{K_B}(V)$, then she sends it backs to Bob.

Because Eve does not modify the message $E_{K_B}(|P>)$ and the judgment $E_{K_B}(V)$, so $|P_B>=|P>$ and *V=1*. And Bob cannot discover Alice's modification on $|S>$ because he does not know the Alice's private K_A. Hence Bob accepts the signature and holds $D_{K_B}(|S'>)=\bigotimes_{i=1}^{n}\delta_Z^{K_{B,2i-1}}\delta_X^{K_{B,2i}}|s_i'>$ as Alice's signature for the quantum message $|P>$.

The forge method is very simple and easy to understand. First, the signed message $(|P>,|S>)$ is really signed by Alice, and Chile will set the judgment (*V = 1*). Second, because Eve only modified the ciphertext $|S>$, and it is not useful for

Bob's verification. So Bob would accepts the forged signature $D_{K_B}(|S'>)$, and holds $\bigotimes_{i=1}^{n} \delta_Z^{K_{B,2i-1}} \delta_X^{K_{B,2i}} |s_i'>$ as Alice's signature for the quantum message $|P>$.

3.2. The Signer can Disavow her Having Signed the Message

The signer, Alice also can cheat in these AQS protocols. That is, Alice can successfully disavow any message she ever signed.

Suppose Alice signs a message according to the *Step 1* to the *Step 6*, and sends $(|P>,|S>,|M_A>)$ to Bob. Because Alice sign the message correctly, so Chile sets the judgment V=1. When Chile sends $E_{K_B}(|P>) \otimes E_{K_B}(|S>) \otimes E_{K_B}(V)$ to Bob, Alice intercepts it, then she modifies some qubits of the $E_{K_B}(|S>)$. Because Alice only changes $E_{K_B}(|S>)$, so the recovery quantum message $|P_B>=|P>$ and $V=1$. Hence Bob accepts the signature. Thus, if Alice announces that it is not the one she ever signed or it was illegally modified by Bob. In this situation, Because of $|S> \neq E_{K_A}(|P>)$, the arbitrator, Chile will stand on the side of Alice and regards Bob's has modified the signature [9].

On the other hand, because not only the receiver but also the attacker can forge the signature under known message, if there are some arguments between Alice and Bob, Alice can disavow her having signed the message. If Bob holds $|S>$ as Alice's signature for the quantum message $|P>$, while Alice can claim that the signature has been forge someone, and she claims the valid signature is $U|S>$ for the quantum message $U|P>$. And in this situation, no one can detect whether Alice tell a lie or not. So, Alice can disavow the signature.

4. New Arbitrated Quantum Signature Scheme without Entangled state

Supposes $|P>=\bigotimes_{i=1}^{n} |p_i>$ be quantum message, with $|p_i>=\alpha_i|0>+\beta_i|1>$. The new scheme involves three partners, Alice is defined as the signer; Bob is defined as the receiver; and Chile is defined as the arbitrator, who helps Bob to verify the signature.

4.1. Initialization Stage

Step I1: the signer, Alice obtains her signing private keys shared with the arbitrator Chile through quantum key distribution (QKD) protocols, where K_A denote Alice's private, and $K_A \in \{0,1\}^*$, which can be proved unconditionally secure [19-22]. Similarly, the receiver, Bob obtains his verifying private key K_B shared with the arbitrator Chile, and K_B denote Bob's private key.

Step I2: Alice gets her transmission private key $K_{AB}\{K_{AB_1}, K_{AB_2}, \cdots, K_{AB_n}, \cdots\}$ with the receiver Bob.

4.2. Signing Stage

Step S1: The signer, Alice generates four copies of quantum string message $|P>$ (two copies to produce the secret qubit string $|P'>$, and two copies to generate the signature $|S_A>$).

Step S2: Alice chooses a number $r \in \{0,1\}^{2n}$ randomly, and then she encrypts four copies quantum message $|P>$ into the cipher text $|P'>$ with quantum one-time pads [23]

$$|P'>=\bigotimes_{i=1}^{n}\delta_X{}^{r_{2i-1}}\delta_Z{}^{r_{2i}}\,|p_i>=\bigotimes_{i=1}^{n}|p_i'> \tag{11}$$

Step S3: Alice uses her signing private key K_A to encrypts two copies $|P'>$ into two copies quantum signature $|S_A>$ (denotes as $|S_{A1}>, |S_{A2}>$),

$$|S_A>=M_{K_A}(|P'>)=\bigotimes_{i=1}^{n}H^{K_{A_{2i-1}}}S^{K_{A_{2i}}}(|p_i'>)=\bigotimes_{i=1}^{n}|s_{A_i}> \tag{12}$$

Here S is defined by $\begin{bmatrix}1 & 0\\ 0 & -i\end{bmatrix}$, it means that $S(\alpha|0>+\beta|1>)=\alpha|0>-i\beta|1>$. And H is the *Hadamard* transform, which is defined $H=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$

Step S4: Alice generates $|S_B>$ with her transmission private key K_{AB}.

$$|S_B>=M_{K_{AB}}(|S_{A1}>)=\bigotimes_{i=1}^{n}H^{K_{AB_{2i-1}}}S^{K_{AB_{2i}}}(|s_{A1_i}>) \tag{13}$$

Step S5: For convenient, the encrypted quantum message $|P'>$ denoted as $|P_1'>, |P_2'>$. Alice uses K_{AB} to generates the signature $|S>$ with quantum one-time pads [23],

$$|S>=E_{K_{AB}}(|P_1'>,|P_2'>,|S_{A2}>,|S_B>) \tag{14}$$

Then, she sends $|S>$ to Bob through a quantum channel.

4.3. Verification Stage

Step V1: The receiver, Bob decrypts $|S>$ with Alice's transmission private key K_{AB}, and gets $(|P_1'>,|P_2'>,|S_{A2}>,|S_B>)$.

Step V2: Bob decrypts $|S_B>$ by K_{AB}, and gets $|S_A'>$ as follows:

$$|S_A'>=D_{K_{AB}}(|S_B>)=\bigotimes_{i=1}^{n}S'^{K_{AB_{2i}}}H^{K_{AB_{2i-1}}}(|s_{B_i}'>) \tag{15}$$

Here S' is defined by $\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}$, it means that $S(\alpha|0>+\beta|1>)=\alpha|0>+i\beta|1>$

Step V3: First, Bob compares two quantum string $|S_A'>$ with $|S_{A2}>$ as the approach in *Ref.*[24]. Then he compares two quantum encrypted message $|P_1'>$ with $|P_2'>$. If $|S_A'>\neq|S_{A2}>$ or $|P_1'>\neq|P_2'>$, it means someone disturbs the

signature or Alice signs the message incorrectly, so Bob rejects the signature; otherwise if $|S_A'>=|S_{A2}>$ and $|P_1'>=|P_2'>$, Bob encrypts $|S_c>=E_{K_B}(|S_A'>,|P_1'>)$ with Bob's secret key K_B , then he sends $|S_c>$ to Chile.

Step V4: Chile decrypts $|S_c>$ by K_B , and gets $(|S_A'>,|P_1'>)$. Then, she generates $|S_A''>=M_{K_A}(|P_1'>)$ as the *Eq.*(15). After that, she compares two quantum string $|S_A''>$,$|S_A'>$ with the approach in *Ref.* [24]. If $|S_A''>=|S_A'>$, he sets the judgment *V*=1; otherwise , he sets *V* =0

At last she publishes *V* by the public board (or encrypts *V* and sends or sends it through a classical public communications channel).

Step V5: If *V* =1, Bob informs Alice to publish *r*, and Alice publishes *r* by the public board.

Step V6: Bob recovers the original quantum message $|P>$ by *r*,

$$|P>=E_r^{-1}(|P'>)=\bigotimes_{i=1}^{n}\delta_Z^{r_{2i}}\delta_X^{r_{2i-1}}|p_i'>=\bigotimes_{i=1}^{n}|p_i> \quad \textbf{(16)}$$

Finally, Bob holds ($|S_{A2}>$,*r*) as Alice's signature for the message $|P>$.

The communications in new arbitrated quantum signature scheme is described in Figure 1.

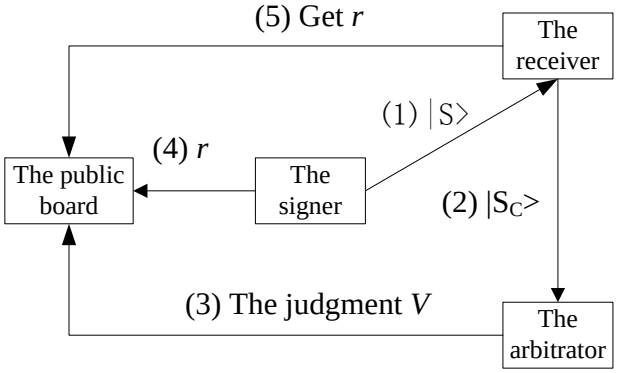

Figure 1. The Communications of New Scheme

5. Security Analysis of the New Scheme

5.1. Impossibility of Forgery

5.1.1. The Attacker Eve cannot Forge the Signature: Because the BB84 protocol or EPR protocol is unconditional secure, the attacker, Eve cannot get the Alice's transmission key K_{AB} . Without K_{AB} , Eve cannot generates $|S_B>=E_{K_{AB}}'(|S_{A1}>)$ and $|S>=E_{K_{AB}}(|P_1'>,|P_2'>,|S_{A2}>,|S_B>)$. So, if Eve substitutes Alice to sign the message. Bob and Chile will find Eve has forged the signature by comparing $|S_A''>$ with $|S_A'>$ or comparing $|S_A'>$ with $|S_{A2}>$. Similarly, Eve hasn't K_B and K_A , so she cannot forge $|S_c>=E_{K_B}(|S_A'>,|P_1'>)$ and forge $|S_A>=E_{K_A}'(|P'>)$. Therefore, Eve cannot forge the signature directly.

The new scheme also can resist the first forge attack as above mentioned. If Eve wants to forge the signature as Sec.(3.1.1). While Alice sends the quantum signature $|S>=E_{K_{AB}}(|P_1'>,|P_2'>,|S_{A2}>,|S_B>)$ to Bob, if Eve intercepts it and forges the signature; then she generated another forged quantum signature $|S'>=UE_{K_{AB}}|P_1'>\otimes UE_{K_{AB}}|P_2'>\otimes UE_{K_{AB}}|S_{A2}>\otimes UE_{K_{AB}}|S_B>$, with $U\in\{I,\delta_X,\delta_Z,\delta_X\delta_Z\}$. After that, she sends $|S'>$ to Bob. Bob can detect Eve has forged the signature as follows:

First Bob gets the forged message $|P_1''>$ by decrypting $UE_{K_{AB}}|P_1'>$

$$|P_1''>=E_{K_{AB}}^{-1}(UE_{K_{AB}}|P_1'>)=U|P_1'> \quad (17)$$

Second Bob gets the forged signature $|S_B'>$ by decrypting $UE_{K_{AB}}|S_B>$

$$|S_B'>=E_{K_{AB}}^{-1}(UE_{K_{AB}}|S_B>)=U|S_B>=\bigotimes_{i=1}^{n}U_iH^{K_{AB_{2i-1}}}S^{K_{AB_{2i}}}(|s_{A1_i}>) \quad (18)$$

Then Bob gets $|S_{A2}'>$ by decrypting $UE_{K_{AB}}|S_{A2}>$

$$|S_{A2}'>=E_{K_{AB}}^{-1}(UE_{K_{AB}}|S_{A2}>)=U|S_{A2}>=\bigotimes_{i=1}^{n}U_iH^{K_{A_{2i-1}}}S^{K_{A_{2i}}}(|p_i'>) \quad (19)$$

After that, Bob decrypts $U|S_B>$ as the *Eq.*(18) and from the *Eq.*(19), we can get

$$|S_A'>=D_{K_{AB}}(U|S_B>)=\bigotimes_{i=1}^{n}S'^{K_{AB_{2i}}}H^{K_{AB_{2i-1}}}U_iH^{K_{AB_{2i-1}}}S^{K_{AB_{2i}}}H^{K_{A_{2i-1}}}S^{K_{A_{2i}}}(|p_i'>) \quad (20)$$

From *Eq.*(18,20), we can know

$$\bigotimes_{i=1}^{n}U_iH^{K_{A_{2i-1}}}S^{K_{A_{2i}}}(|p_i'>)\neq\bigotimes_{i=1}^{n}S'^{K_{AB_{2i}}}H^{K_{AB_{2i-1}}}U_iH^{K_{AB_{2i-1}}}S^{K_{AB_{2i}}}H^{K_{A_{2i-1}}}S^{K_{A_{2i}}}(|p_i'>) \quad (21)$$

$U_i\in\{\delta_X,\delta_Z,\delta_X\delta_Z\}$, so it can get $|S_{A2}'>\neq|S_A'>$. Therefore, Bob will find Eve has forged the signature. Similarly, if Eve intercepts $|S_c>$, she also cannot forge the signature. Because Bob verifies the signature's integrity by comparing $D_{K_{AB}}(|S_B>)$, $|S_{A2}>$. And Chile only sends the judgment *V* to Bob instead of sends the signature, so Eve has no chance to modify the signature, so she cannot forge the signature as the second forge method.

The new scheme also can resist the first forge attack as above mentioned. If Eve wants to forge the signature as Sec.(3.1.2). If the attacker Eve intercepts $E_{K_B}(|P>,|S>,V)$, and then she forges $E_{K_B}(|P>)\otimes|S'>\otimes E_{K_B}(V)$, then she sends it backs to Bob. It will also be finded by the receiver Bob, because in *Step V3:* Bob has compared two quantum string $|S_A'>$ with $|S_{A2}>$, it has verified the the signature, if Eve forged $|S'>$, Bob compars it with $|S_{A2}>$, and will find some one has forged the signature.

So, in the new AQS scheme, the attacker Eve cannot forge the signature.

5.1.2. Bob cannot Forge the Signature: Suppose the receiver, Bob wants to replace Alice to sign the message. The scheme also can resist the receiver Bob forging signature. Because with the unconditionally secure quantum key distribution and the

use of quantum one-time pad algorithm, Bob cannot know Alice's secret key K_A, so Bob cannot generate $|S_A>=M_{K_A}(|P'>)$. And if Bob forge the signature, when the arbitrator compares $|S_A''>$ with $|S_A'>$, it will be detected by the arbitrator.

The new scheme not only uses *pauli* operation $\{I, \delta_X, \delta_Z, \delta_X\delta_Z\}$, but also uses logical gate S to ensure its security. It can see easily

$$U_i H^{r_{2i-1}} S^{r_{2i}} |p_i> \neq H^{r_{2i-1}} S^{r_{2i}} U_i |p_i> \quad (22)$$

In the *Eq.(21)*, U_i is any two-dimensional matrix. The new scheme also can resist forge attack as above mentioned. As the Eq.(22), it can know

$$\bigotimes_{i=1}^{n} U_i H^{K_{A_{2i-1}}} S^{K_{A_{2i}}} (|p_i'>) \neq \bigotimes_{i=1}^{n} H^{K_{A_{2i-1}}} S^{K_{A_{2i}}} U_i (|p_i'>) \quad (23)$$

From the Eq.(23), it can get the equation easily $\bigotimes_{i=1}^{n} H^{K_{A_{2i-1}}} S^{K_{A_{2i}}} \delta_X^{r_{2i-1}} \delta_Z^{r_{2i}} |p_i> \neq \bigotimes_{i=1}^{n} U_i H^{K_{A_{2i-1}}} S^{K_{A_{2i}}} \delta_X^{r_{2i-1}} \delta_Z^{r_{2i}} U_i |p_i>$, so Bob cannot forge the signature $(U|S_A>, r)$ for the message $U|P>$.

5.2. Impossibility of Disavowal

Because the arbitrator, Chile has the signer Alice's private key K_A and the receiver Bob's private key K_B, if Alice and Bob disavow their signature, the arbitrator Chile can make a judgment between them.

5.2.1. Alice cannot Disavow her Having Signed the Message: The arbitrator can confirm that the signer Alice had signed the quantum message. Because Alice generates $|S_A>=M_{K_A}(|P'>)$ with her signing private key K_A, if Alice signs the signature correctly, the equation $|S_A''>=|S_A'>$ would be hold, it means that Alice's private key K_A involves in the signature. Hence Alice cannot deny her having signed the message.

5.2.2. Bob cannot Disavow his Having Received the Signature: Similarly, Chile also can confirm that Bob had received the quantum signature $|S>$. Because the valid signature for the quantum message $|P>$ is $(|S_{A2}>, |P>)$. So if Bob want to get the valid signature, he must inform Alice to publish *r* by the public board, it means Bob has received the signature. Therefore Bob cannot disavow that he has received the signature.

5.3. Comparison with Other Quantum Signature Scheme

The new scheme doesn't use quantum entangled states, which can offer a higher efficiency in transmission. Compare with [2, 5-6, 8], the proposed scheme is more efficient in transmission and more security as stated in Table 2.

Table 2. The Quantity of the Transmitted Qubits for the AQS

Transmission	Zeng's scheme [2]	Lee's scheme using public board [5]	Lee's scheme without public board [5]	Li's scheme [6]	Zou's scheme [8]	New scheme
Alice→Bob	4*n*	3*n*	3n	4*n*	4*n*	4*n*
Bob→Chile	5*n*	5*n*	4n	4*n*	2*n*	*2n*
Chile→Bob	7*n* +1	6*n* +1	2n+2	6 *n* +1	2*n* +1	*0*
Chile publish	0	0	0	0	0	1
Alice publish	0	0	2n	0	2*n*	*2n*
Total amount	16n +1	14*n* +1	11n+2	14*n* +1	10*n* +1	8*n+1*
Impossibility of forgery	No	Yes	Yes	No	No	Yes
Impossibility of disavowal	No	No	No	No	Yes	Yes

6. Conclusions

This article has shown that in some AQS schemes, the receiver and the attacker can forge the signature and the signer can disavow her signature. To conquer these shortcomings, a new AQS scheme has been proposed. The scheme can provide its security by employing QKD techniques [17-18] and new quantum one-time pads. The proposed AQS scheme uses special quantum logical gate to resist known message attack. Compares with other AQS schemes [2, 5-6, 8], the new scheme can offer a higher efficiency in transmission. So it is an effective secure arbitrated quantum signature scheme.

Acknowledgements

This work was supported by Zhejiang Provincial Natural Science Foundation of China under Grant No. LQ12F02006.

References

[1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer [J]. SIAM REVIEW, vol. 41, no. 2, (**1999**), pp. 303 - 332.
[2] G. Zeng and C. H. Keitel, „Arbitrated quantum-signature scheme [J]", PHYSICAL REVIEW A, vol. 65, no. 4, (**2002**), pp. 12 - 17.
[3] M. Curty and N. Lütkenhaus, "Comment on 'Arbitrated quantum-signature scheme' [J]", PHYSICAL REVIEW A, vol. 77, no. 4, (**2008**), pp. 1-4.
[4] G. Zeng, "Reply to "Comment on 'Arbitrated quantum-signature scheme'" [J]", PHYSICAL REVIEW A, vol. 77, no. 1, (**2008**), pp. 1-5.
[5] H. Lee, C. Hong, H. Kim, H. Kim, J. Lim and H. J. Yang, "Arbitrated quantum signature scheme with message recovery [J]", Physics Letters A, vol. 321, no. 56, (**2004**), pp. 295 - 300.
[6] Q. Li, W. H. Chan and D.-Y. Long, « Arbitrated quantum signature scheme using Bell states [J]", PHYSICAL REVIEW A, vol. 79, no. 5, (**2009**), pp. 7-10.
[7] Y. Yu-Guang and W. QiaoYan, "Arbitrated quantum signature of classical messages against collective amplitude damping noise [J]", Optics Communications, vol. 283, no. 16, (**2010**), pp. 3198-3201.
[8] X. Zou and D. Qiu, "Security analysis and improvements of arbitrated quantum signature schemes [J]", PHYSICAL REVIEW A, vol. 82, no. 4, (**2009**), pp. 25-34.
[9] G. Fei, S.-J. Qin and F.-Z. Guo, "Cryptanalysis of the arbitrated quantum signature protocols [J]", PHYSICAL REVIEW A, vol. 84, no. 2, (**2011**), pp. 44-50.

[10] S.-K. Chong, Y.-P. Luo and T. Hwang, ”Comment on ‘New arbitrated quantum signature of classical messages against collective amplitude damping noise’ [J]”, Optics Communications, vol. 284, no. 3, (**2011**), pp. 893-895.
[11] T.-Y. Wang and Z.-L. Wei, “One-time proxy signature based on quantum cryptography [J]”, Quantum Inf. Process., vol. 11, no. 2, (**2012**), pp. 455-463.
[12] J. Zhang, “New Arbitrated Quantum Signature with Message Recovery [J]”, International Journal of Quantum Information, vol. 9, no. 6, (**2011**), pp. 1543-1551.
[13] T.-Y. Wang and Q.-Y. Wen, “Fair quantum blind signatures [J] », Chinese Physics B, vol. 19, no. 6, (**2010**), pp. 66-70.
[14] S. Qi, H. Zheng and W. Qiaoyan, “Quantum blind signature based on Two-State Vector Formalism [J]”, Optics Communications, vol. 283, no. 21, (**2010**), pp. 4408-4410.
[15] R. Xu, L. Huang and W. Yang, „Quantum group blind signature scheme without entanglement [J]”, Optics Communications, vol. 284, no. 14, (**2011**), pp. 3654-3658.
[16] L.-B. He, L.-S. Huang, W. Yang and R. Xu, “Cryptanalysis of fair quantum blind signatures [J]”, Chin. Phys., vol. 21, no. 3, (**2012**), pp. 6-10.
[17] A. K. Ekert, “Quantum cryptography based on Bell’s theorem [J]”, Physical Review Letters, vol. 67, no. 6, (**1991**), pp. 661-663.
[18] C. H. Bennett, “Quantum cryptography using any two nonorthogonal states [J]”, Physical Review Letters, vol. 68, no. 21, (**1992**), pp. 3121-3124.
[19] H.-K. Lo and H. F. Chau, “Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances [J]”, Science, vol. 283, no. 5, (**1999**), pp. 2050-2056.
[20] P. W. Shor and J. Preskill, “Simple Proof of Security of the BB84 Quantum Key Distribution Protocol [J]”, Physical Review Letters, vol. 85, no. 2, (**2000**), pp. 441-444.
[21] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, “Quantum cryptography”, Rev. Mod. Phys., vol. 74, (**2002**), pp. 145–195.
[22] H. Inamori, N. Lütkenhaus and D. Mayers, „Unconditional security of practical quantum key distribution [J]”, European Physical Journal D, vol. 41, no. 3, (**2007**), pp. 599-627.
[23] P.O. Boykin and V. Roychowdhury, “Optimal encryption of quantum bits [J]”, PHYSICAL REVIEW A, vol. 67, no. 4, (**2003**), pp. 17-22.
[24] H. Buhrman, R. Cleve, J. Watrous and R. de Wolf, “Quantum Fingerprinting [J]”, Physical Review Letters, vol. 87, no. 16, (**2001**), pp. 2 - 5.
[25] P. G. Kwiat, K. Mattle and H. Weinfurter, “New High-Intensity Source of Polarization-Entangled Photon Pairs [J]”, Physical Review Letters, vol. 75, no. 24, (**1995**), pp. 4337 - 4341.

