Arbitrated Proxy Signature Scheme Based on Quantum Cryptography

Wang xiuqing* and Zhang Jun

1Department of Computer, ShaoXing University, 312000, China
zscaswxq@126.com

Abstract

Proxy signature is a special signature which provided the signer can delegate his signing capability to others. The proxy signature provides that the original signer can delegate his signing permission to a proxy signer, and the proxy signer can replace the original signer to sign the message. In this paper, we propose a proxy signature scheme based on ideas from classical proxy signature schemes and quantum cryptography. The scheme is implemented by Bell states and a symmetrical quantum key cryptosystem. Compile with classical proxy signature schemes, the new scheme can guarantee the security by using quantum key distribution and one-time pads. And it also can prove that the scheme have the characteristics of non-counterfeit, non-disavowal and traceability. Furthermore, the new scheme uses a special quantum encryption to ensure the receiver cannot forge the signature. The validity of the new scheme can be verified, and it is a secure proxy signature scheme.

Keywords: arbitrated proxy signature; quantum mechanics; unconditional security

1. Introduction

The traditional signature provides the signer with the secret key to sign a message, and the signature receiver can verify the signature with the signer’s corresponding public key. But, on many occasions, once the signer can’t sign message for some reasons, we hope the signer can delegate his signing capability to others, who can sign the message on behalf of an original signer. This scheme is proxy signature, the concept of proxy signature was first proposed by Mambo in 1996 [1]. In a proxy signature scheme, an original signer could authorize his proxy agent to other signer, who is called the proxy signer, and the proxy signer can sign messages to generate proxy signatures on behalf of the original signer. Proxy signature is very important in the modern electronic data processing systems, and it has a wide application in many areas such as electronic-business and electronic-banking, etc.

The first quantum signature scheme was proposed by Zeng and Christoph H. Keite in 2002 [2], in this scheme, both known and unknown quantum states could be signed. The algorithm is implemented by a symmetrical quantum key cryptosystem and Greenberger-Horne-Zeilinger (GHZ) triplet states and quantum one-time pads. In 2004, Lee and C Horng etc proposed two quantum signature schemes with message recovery, one scheme uses a public board and the other does not, and the schemes provide a higher efficiency in transmission [3]. In 2010, Zou show that in Ref [4], they found that the receiver Bob can repudiate the signature, then they proposed two arbitrated quantum signature scheme (AQS) schemes, one used a public board; the other didn’t utilize entangled states in the signing phase and the verifying phase. These schemes used quantum one-time pads to ensure their schemes, but traditional quantum one-time pads didn’t suit for the quantum signature. Gao shown that in these protocols the receiver, Bob, can realize existential forgery of the sender’s signature under known message attack, and, the sender, Alice, can successfully disavow any of her signatures by simple attack [5]. After that, Jeong Woon Choi pointed out there exist an existential forgery attack that can validly modify the
transmitted pair of message and signature [6]. And Tzonelih Hwang found the attacker can get the signer Alice’s private key by Trojan-horse attack [7].

In this paper, an efficient quantum proxy signature protocol with Bell states is proposed. In the new scheme, one particle of the Bell pairs is delivered to the proxy signer while the other particle to the signature receiver. The proxy signer measures her particle to sign the message, and the receiver could verify the proxy signature according to his correlation of the Bell pair. If some disagreement happens, the arbitrator could be traced. By using of quantum key distribution and quantum one-time pad, the new scheme can guarantee the attacker cannot forge the signature and the signer cannot disavow the signature.

2. The Improved Quantum One-time Pads Encryption

2.1. The Notion Concerning Quantum One-time Pads (QOTP)

Some AQS schemes use quantum one-time pads (QOTP) to ensure the signer cannot forge the signature and the signer cannot disavow the signature. Quantum one-time pads use Pauli \((I, \delta_x, \delta_z, \delta_x \delta_z)\) matrices to encrypt one quantum bit, where \(\delta_x\) and \(\delta_z\), which denotes X and Z gates. Suppose \(|m_i\rangle = \alpha |0\rangle + \beta |1\rangle\), and the key \(K \in \{0,1\}^n\). The QOTP encryption \(E_k\) on the quantum message can be described by

\[
|C_i\rangle = E_k(|m_i\rangle) = \delta_x^{k_i} \delta_z^{k_{i-1}} |m_i\rangle
\]

where \(k_i\) denotes the \(i^{th}\) bit of \(K\). The corresponding decryption \(D_k\) is

\[
|m_i\rangle = D_k(|C_i\rangle) = \delta_z^{k_{i-1}} \delta_x^{k_i} |C_i\rangle
\]

Boykin and Roychowdhury proved that \(2N\) random traditional binary bits can encrypt unknown state of \(N\) quantum bits. And without the private key, no one can get the original bits.

2.2. New Quantum One-time Pads

Supposed the quantum message is \(|P\rangle = \bigotimes_{i=1}^n |P_i\rangle\), with \(|P_i\rangle = \alpha_i |0\rangle + \beta_i |1\rangle\), and the encrypted private key is \(K \in \{0,1\}^n\). The new QOTP encryption \(E_k\) on the classic message can be described by

\[
|C\rangle = E_k(|P\rangle) = \bigotimes_{i=1}^n (H^{k_i} T^{k_{i-1}} |P_i\rangle)
\]

Here \(H\) is the Hadamard transform, \(H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\). And \(T\) is defined by

\[
T = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{\sqrt{2}}(1-i) \end{pmatrix}
\]

it means that

\[
T (\alpha |0\rangle + \beta |1\rangle) = \alpha |0\rangle + \frac{1}{\sqrt{2}}(1-i)\beta |1\rangle
\]

Because

\[
\begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{\sqrt{2}}(1-i) \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{\sqrt{2}}(1+i) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I \quad \text{and} \quad HH = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I
\]
So the corresponding decryption $D_x$ to the quantum one-time pad is described as follows:

$$|M> = D_x (|C>) = \bigotimes_{i=1}^n (T^{h_1}H^{h_2}|c_i>) \quad (5)$$

Where $|c_i>$ denotes the $i$th quantum bit of the quantum ciphertext $C$. $T = \begin{bmatrix} 1 & 0 \\ 0 & \frac{1}{\sqrt{2}}(1+i) \end{bmatrix}$, which means that

$$T^i (\alpha |0>+\beta |1>) = \alpha |0> + \frac{1}{\sqrt{2}} \beta (1+i) |1> \quad (6)$$

In order to include the noncommutative property in the quantum signature, the paper simply takes advantage of the new QOTP use a random rotation and one-time pads.

3. Arbitrated Quantum Signature with Bell Entangled States

$|P> = \{|p_1>, |p_2>, \ldots, |p_n>\}$ is a quantum bits string, with $|p_i> = \alpha, |0> + \beta, |1>$ and $||\alpha||^2 + ||\beta||^2 = 1$. If $|P>$ is known quantum states, it can be prepared any copies and if $|P>$ is unknown quantum states, three copies of $|P>$ are necessary, one to be sent to the proxy signer $Alice_p$ to produce the secret qubit string $|R>$, one to be sent to the receiver Bob to generate $|R_o>$, the other sends to the arbitrator to verify the signature. The message $m = \{m_1, m_2, \ldots, m_n\}$ is classic N-bits message, where $m_i \in \{0, 1\}$. By using of Bell states and new quantum one-time pads, the new scheme can resist forge attack as above mentioned. In the new quantum proxy signature scheme, five characters are defined as follows:

$Alice_o$: $Alice_o$ is defined as the original signer, who delegates his signing capability to proxy signer, so the proxy signer can sign the message replacing the original signer.

$Alice_p$: $Alice_p$ is defined as the proxy signer, who gets $Alice_o$’s signing capability and signs the message, and then she sends her signature to the arbitrator and the receiver.

Bob: Bob is defined as the signature receiver, who receives the quantum signature and verifies the signature with the arbitrator’s help.

Charlie: Charlie is defined as the arbitrator, who is trusted by the signers (include original signer and the proxy signer) and the signature receiver Bob, he helps Bob to verify whether the signature is valid.

Eve: The attacker, who wants to forge the signature or replace the proxy signer to sign the message.

3.1. System Initialing Phase

- **Step I1**: The original signer $Alice_o$ gets his secret key $K_{op}$ shared with the proxy signer $Alice_p$ through quantum key distribution protocols. Likewise, $Alice_o$, $Alice_p$ and Bob share their secret key $K_o$, $K_p$, $K_b$ with the arbitrator Charlie, where $K_o$, $K_p$, $K_b$ denote $Alice_o$’s, $Alice_p$’s and Bob’s secret key.

- **Step I2**: The arbitrator Charlie generates $N$ Bell states $|\varphi> = \{|\varphi_1>, |\varphi_2>, \ldots, |\varphi_N>\}$, where
After that, for $i \in \{1, \ldots, N\}$, Charlie distributes one particle of Bell state $|\varphi_i\rangle$ to $Alice_p$ with a secure, authenticated method and the other to himself.

3.2. Proxy Share Generation Phase

In this phase, the original signer $Alice_o$ delegates her signing capability to the proxy signers $Alice_p$, so $Alice_p$ can sign the message.

- **Step P1**: $Alice_o$ informs the receiver Bob and the arbitrator Charlie that she delegates her signing capability to $Alice_p$.
- **Step P2**: $Alice_o$ generates her proxy information $|w\rangle = \{|w_1\rangle, |w_2\rangle, \ldots, |w_y\rangle\}$, where $|w\rangle$ includes the information of proxy signers and other information.
- **Step P3**: $Alice_o$ encrypts $|W\rangle = E_{K_w}|w\rangle$ and $|\delta\rangle = E_{K_s}|w\rangle$ using the approach in Eq.(12).
- **Step P4**: $Alice_o$ sets $|A\rangle = E_{K_{ow}}(|W\rangle, |\delta\rangle)$, and sends $|A\rangle$ to the proxy signer $Alice_p$.
- **Step P5**: $Alice_p$ decrypts $|A\rangle$, and gets $|w\rangle, |W\rangle, |\delta\rangle$. Then she gets $|W\rangle^\prime = E_{K_{ow}}(|w\rangle)$ by $K_{op}$.
- **Step P6**: $Alice_p$ compares $|W\rangle^\prime$ with $|W\rangle$ from the Ref.[9]. If $|W\rangle^\prime = |W\rangle$, it means that $Alice_p$ has capability to sign the message, otherwise, it means that $Alice_o$ doesn’t delegate her signing capability to $Alice_p$ or Eve attacks $|A\rangle$, so $Alice_p$ must let $Alice_o$ regenerate $|A\rangle$.

3.3. Signing Phase

- **Step S1**: $Alice_p$ encrypts $m$ into qubit message $|R\rangle = \{|r_1\rangle, |r_2\rangle, \ldots, |r_x\rangle\}$ with her secret key $K_p = (K_{p_1}, K_{p_2}, \ldots, K_{p_y})$. The transform method defines as follows:

$$|r_i\rangle = E_{K_{mi}}(|P\rangle) = H^{K_i}T^m|P\rangle$$  \hspace{1cm} (8)

Similar with the Ref [8], the encrypt method can ensure unconditionally secure.

- **Step S2**: For $i \in \{1, \ldots, N\}$, $Alice_p$ combines each qubit message state $|r_i\rangle$ and the Bell state $|\varphi_i\rangle$, then she obtains the three-particle entangled state $|B_i\rangle$:

$$|B_i\rangle = |R\rangle \oplus |\varphi_i\rangle = \left(|B_1\rangle, |B_2\rangle, \ldots, |B_x\rangle\right) \quad \text{where}$$

$$|B_i\rangle = |r_i\rangle \oplus |\varphi_i\rangle = \frac{1}{2}(|\psi_{i1}\rangle > (\alpha_i|0\rangle + \beta_i|1\rangle) + \frac{1}{2}(|\psi_{i2}\rangle > (\alpha_i|0\rangle - \beta_i|1\rangle)$$

$$+ \frac{1}{2}(|\phi_{i1}\rangle > (\beta_i|0\rangle + \alpha_i|1\rangle) + \frac{1}{2}(|\phi_{i2}\rangle > (\alpha_i|1\rangle - \beta_i|0\rangle)$$  \hspace{1cm} (9)

- **Step S3**: $Alice_p$ measures the three-particle entangled state $|B\rangle$ and obtains $|M\rangle = \{|M_1\rangle, |M_2\rangle, \ldots, |M_y\rangle\}$, where $|M_i\rangle = \{|\psi_{i1}\rangle, |\psi_{i2}\rangle, |\phi_{i1}\rangle, |\phi_{i2}\rangle\}$. 

---

380  

Copyright © 2015 SERSC
( | _M_i_ > Denotes the Alice_p’s measurement result to the ith entangled particles).

- Step S4: Alice_p uses her secret key \( \kappa_p \) to generate signature with the quantum one-time pad algorithm as the Eq. (7)

\[
| S > = E_{\kappa_p} ( | M > , | R > , | w > , | \delta > )
\]

(10)

Then she sends her signature |S> to the arbitrator Charlie through a quantum channel.

3.4. Verification Phase

- Step V1: The arbitrator Charlie decrypts |S> with Alice_p’s secret key \( \kappa_p \), and gets \( ( | M > , | R > , | w > , | \delta > ) \).
- Step V2: Charlie generates \( | \delta’ > = E_{\kappa_p} ( | w > ) \), and compares |\delta’> with |\delta>, if \( | \delta’ > = | \delta > \), she sets \( v_i =1 \); else she sets \( v_i =0 \).
- Step V3: Charlie recover the qubits information \( | R^’ > = \{ | r_1 > , | r_2 > , …, | r_n > \} \) with the Eq. (18) and the Alice_p’s measurement \( | M > \).

Where \( | _M_i_ > \in \{ | \Psi_{11} > , | \Psi_{12} > , | \Phi_1 > , | \Phi_2 > \} \). Charlie implements the corresponding transformations denoted as Eq. (20) on the her particles of the Bell states. For example, if Alice_p’s measurement result to the ith Bell state \( | R_i > \) is \( | \Psi_{12} > \), then the arbitrator’s measurement result must be \( ( | \alpha > , | 0 > - | \beta > , | 1 > ) \), and she can recover |\( r_i’ \)> by applying the identity transformation \( \delta_z \) \( ( | \alpha > , | 0 > - | \beta > , | 1 > ) \). So For \( i \in \{ 1, ..., N \} \), the arbitrator can recover the qubits \( | R^’ > \) by applying the identity transformation as follows:

\[
| \Phi_{12} > \rightarrow \delta_z, | \Phi_{12} > \rightarrow \delta_z
\]

(11)

- Step V4: The arbitrator compares two quantum states \( | R^’ > \) with \( | R > \). If \( | R^’ > = | R > \), he sets \( v_i =1 \); otherwise he sets \( v_i =0 \).
- Step V5: For \( i \in \{ 1, ..., N \} \), Charlie generates \( | R_i > = \{ | r_{1, i} > , | r_{2, i} > , …, | r_{N, i} > \} \), generate \( | R_i > = \bigoplus \{ E_{K_i, XOR(\kappa_p)} ( | R^’ > ) ( | R^’ > = \{ | r_1 > , | r_2 > , …, | r_n > \} ) \},\)

\[
\begin{align*}
\text{XOR is used to implement binary addition in computers. It means that if } \kappa_p’ & = k_p’; \\
\text{Charlie sets } | r_i > & = | r_i’ > ; \text{ else if } \kappa_p’ & \neq k_p’; \text{ the arbitrator sets} | r_i > & = H ( | r_i’ > ).
\end{align*}
\]

- Step V6: Charlie announces the verification parameter \( ( v_i, v_j ) \) by the public board. Then, she randomly chooses a number \( r \in \{ 0, 1 \}^n \), and transforms the |\( \delta > \) into secret qubits message \( | \delta^’ > = E_r ( | \delta > ) \). Then, Charlie regenerates \( | S > = E_{\kappa_p} ( | M > , | R > , | w > , | \delta^’ > ) \) with Alice_p’s secret key \( \kappa_p \).
- Step V7: Charlie uses Bob’s secret key to encrypt \( | S_{\rho_{bob}} > = E_{\kappa_p} ( | S > , | \delta^’ > , | R_i > ) \), with the quantum one-time pad algorithm, then sends \( | S_{\rho_{bob}} > \) to Bob through a quantum channel.
- Step V8: If \( v_i =0 \) or \( v_j =0 \) Bob rejects the signature; else if \( v_i =1 \) and \( v_j =1 \), he decrypts \( | S_{\rho_{bob}} > \) with \( \kappa_p \), and gets \( ( | S > , | \delta^’ > , | R_i > ) \).
Step V9: Bob generates $|R_s \rangle$ with $|P \rangle$ and Bob’s secret key $k_p$ as Eq.(16). Then he compares two quantum states $|R_s \rangle$, $|R_s \rangle$. If $|R_s \rangle \neq |R_s \rangle$, Bob rejects the signature; otherwise, he informs Charlie by the public board to publish $r$.

Step V10: Charlie publishes $r$ by the public board. Then Bob decrypts $|\delta \rangle$ and gets $|\delta \rangle$. Finally, Bob accepts $(|S \rangle, |\delta \rangle, |R_s \rangle, r)$ as proxy signature for the message $m$. The communications in AQS Scheme 1 are described in Figure 1.

4. Security Analysis the New Scheme

In this section, we can show that the new quantum proxy signature scheme have the characteristics of impossibility of counterfeit, impossibility of disavowing; traceability.

Almost all the classic proxy signature schemes were based on the mathematical problem solving, such as DSA is based on the discrete logarithm problem (DLP), RSA signature is based on the factoring large numbers problem. Until now, these schemes are security and very difficult to broken. However, once quantum computers are invented someday, it is very easy to break those mathematical problem schemes by Shor’s algorithm.

Quantum signatures can ensure their unconditional security by using physical principles quantum no-cloning theorem and the Heisenberg uncertainty principle. Quantum no-cloning theorem implies it the attacker intercepted the signature; he cannot copy the same quantum bits by the quantum signature, so it means the attacker only can measure the quantum bits one-time. Therefore the attacker only can forge the signature one time, and it will destroy the sates of the quantum string. And in the classic digital signature, how to ensure the signer’s private cannot expose is very difficult. Because the BB84 protocol or EPR protocol is unconditional security, the attacker cannot get the signer’s private key, the sender Bob cannot get the Alice’s private key $k_A$ from the these quantum key distribution (QKD) protocols.

If the quantum signature scheme is secure, it means that no one can forge the signature, even if the attacker intercepts the signature, the attacker also cannot forge the signature.

4.1. Imposibility of Counterfeit

4.1.1. The Attacker Cannot Counterfeit the Signature

Lemma $P((H^k T^{k_{s-1}} | P_s = H^k T^{k_{s-1}} | P_s >) | K_{2s, 2s-1} = K_{2s, 2s-1}) = 1$ (12)

Original signer

Proxy signer

The arbitrator

The receiver

The public board

(1) |A><

(2) |S><

(3) (V1, V2)

(4) |Bob><

(5) A notice

(6) r

Figure 1. The Communications of the Quantum Proxy Signature Scheme
Where $K_{2,1,2-1}$ denotes (2i)-th,(2i-1)-th of the signer’s private key, $K'_{2,1,2-1}$ denotes (2i)-th,(2i-1)-th of the Attacker’s key; $P_i$ denotes i-th of the quantum string.

Proof, it can know that
\[
P((H^{k_i}\cdot T^{k_{i-1}} | P_i = H^{k_i}\cdot T^{k_{i-1}} | P_i >) \mid K_{2,1,2-1} = K'_{2,1,2-1}) =
\]
\[
P((H^{k_i}\cdot T^{k_{i-1}} | P_i = H^{k_i}\cdot T^{k_{i-1}} | P_i >) \mid K_{2,1,2-1} \neq K'_{2,1,2-1}) = 1/4
\]
\[
P(K_{2,1,2-1} = K'_{2,1,2-1}) = 1/4
\]

Lemma 2: $P((H^{k_i}\cdot T^{k_{i-1}} | P_i = H^{k_i}\cdot T^{k_{i-1}} | P_i >) \mid K_{2,1,2-1} \neq K'_{2,1,2-1}) = 0$ (13)

Proof, it can know that
\[
P((H^{k_i}\cdot T^{k_{i-1}} | P_i = H^{k_i}\cdot T^{k_{i-1}} | P_i >) \mid K_{2,1,2-1} = K'_{2,1,2-1}) =
\]
\[
P((H^{k_i}\cdot T^{k_{i-1}} | P_i = H^{k_i}\cdot T^{k_{i-1}} | P_i >) \mid K_{2,1,2-1} \neq K'_{2,1,2-1}) = 0
\]
\[
P(K_{2,1,2-1} \neq K'_{2,1,2-1}) = 3/4
\]

Theorem 1: $P((H^{k_i}\cdot T^{k_{i-1}} | P_i = H^{k_i}\cdot T^{k_{i-1}} | P_i >) = 1/4$

Proof,
\[
P((H^{k_i}\cdot T^{k_{i-1}} | P_i = H^{k_i}\cdot T^{k_{i-1}} | P_i >) = P((H^{k_i}\cdot T^{k_{i-1}} | P_i = H^{k_i}\cdot T^{k_{i-1}} | P_i >) \mid K_{2,1,2-1} = K'_{2,1,2-1}) + P((H^{k_i}\cdot T^{k_{i-1}} | P_i = H^{k_i}\cdot T^{k_{i-1}} | P_i >) \mid K_{2,1,2-1} \neq K'_{2,1,2-1})
\]
\[
P(K_{2,1,2-1} = K'_{2,1,2-1}) = 1/4
\]

So, if the attacker intercepts the quantum signature, he has the probability of $(1/4)^n$ to forge the signature. And if the attack compares $H^{k_i}\cdot T^{k_{i-1}} | P_i >$ with $H^{k_i}\cdot T^{k_{i-1}} | P_i >$, it will destroy two quantum strings. If n is very long, the attack cannot get the signer’s private key.

Furthermore, the new proxy signature scheme can resist the man-in-the-middle attacks. Suppose the attacker Eve wants to counterfeit Alice, to sign the message and sends the signature $|S > (|S> = E_{K_e}(|M >, |R >, |w >, |\delta >))$ to the Charlie. Because of the unconditional security of a quantum key distribution, Eve cannot get the Alice’s secret key $K_e$, and cannot generates $|S >$. Similarly, if Eve obtains the signature $|S >$, she cannot decrypt $|S >$ and cannot get any information of the $(|M >, |R >, |w >)$.  

4.1.2. The Original Signer Alice Cannot Counterfeit the Signature: Similarly, the original signer also cannot get the proxy signer’s private key. The schemes also can resist the original signer Alice, to forge the quantum signature. Suppose Alice is a malicious attacker, who wants to sign the message. Because she cannot know Alice’s secret key $K_e$ and cannot generate $|S > = E_{K_e}(|M >, |R >, |w >, |\delta >)$.

Theorem 2: $U_{m} \neq 1 => U_{m} H^{k_i}\cdot T^{k_{i-1}} | P_i > \neq H^{k_i}\cdot T^{k_{i-1}} U_{m} | P_i >$

Where $K_{2,1,2-1}$ denotes (2i)-th,(2i-1)-th of the private key,
\[
P_i = \alpha_i |0 > + \beta_i |1 >, H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \text{.} \text{And T is defined by } T = \begin{bmatrix} 1 & 0 \\ 0 & \frac{1}{\sqrt{2}}(1-i) \end{bmatrix} \text{.}
\]
Proof. It uses reductio ad absurdum, only to certify no two-dimensional matrix
\[ U_1 = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \neq I \quad \text{, satisfies} \quad U_1 E_{k_x,k_y} | P_x, P_y > = \pm E_{k_x,k_y} U_1 | P_x, P_y > \quad \text{, and only} \]
\[ U_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I, U_1 E_{k_x,k_y} | P_x, P_y > = \pm E_{k_x,k_y} U_1 | P_x, P_y > \]

1) Firstly, Suppose \( K_{21} = 0, K_{21} = 1 \),
\[ K_{21} = 0, K_{21} = 1 \Rightarrow U, T = \pm TU, \Rightarrow \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 -i \end{bmatrix} = \pm \begin{bmatrix} 1 & 0 \\ 0 & 1 +i \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \]
\[ \Rightarrow a (b - bd) = \pm a (c - ci), d \Rightarrow b = 0 \land d = 0 \]

2) Secondly, Suppose \( K_{21} = 1, K_{21} = 0 \)
\[ K_{21} = 0, K_{21} = 1 \Rightarrow U, H = \pm HU, \Rightarrow \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} \]
\[ \Rightarrow a a = \pm a a, d \Rightarrow a = d = 1 \]

So, only \( a = d = 1 \) and \( U_1 = I \), satisfies \( U_1 E_{k_x,k_y} | P_x, P_y > = \pm E_{k_x,k_y} U_1 | P_x, P_y > \), it means that the receiver cannot change the signature. Hence to any two-dimensional matrix

If the receiver is a malicious attacker, who wants to remove \( T \) or \( H \) without knowing the signer’s private key, while the new QOTP can ensure the \( H, T \) cannot be commutative. More rigorously, the paper proves that there are no nontrivial quantum operator \( U \) that commutes with both \( H \) and \( T \) operator up to a constant. So use this new quantum one-time pads, the receiver cannot use known message attack.

4.1.3. The Proxy Signer Alice_p Cannot Counterfeit the Signature: Similarly, if the proxy signer Alice_p wants to sign another unauthorized message \( m' \) for her benefit, it also can be detected by the receiver Bob. Because at the verifying phase, Bob generates \( | R_{k'} > \) from the classic message \( m \) and judges whether \( | R_k > = | R_{k'} > \). If Alice_p signs another message \( m' \), then \( | R_{k'} > \neq | R_k > \), and it can be detected by Bob. If the original signer Alice_o doesn’t delegate her signing capability to Alice_p, while Alice_p wants to sign the message, it also can be detected by the arbitrator. Because Alice_p cannot know Alice_o’s secret key \( K_{o} \), so she cannot generate \( | \delta > = E_{k_o} (| w >) \).

Hence without the original signer Alice_o’s authorization, Alice_p cannot sign the message.

4.1.4. The Receiver Bob Cannot Counterfeit the Signature: Suppose the receiver Bob is a malicious attacker, who wants to counterfeit Alice_p to sign the message. If successful, it is beneficial for him because Bob can replace Alice_p’s signature and sign a new signature to a message favorable to him. Because with the unconditionally secure quantum key distribution and the use of quantum one-time pad algorithm, Bob cannot know Alice_p’s secret key \( K_{p} \). So Bob can’t counterfeit the signature \( | S > \). If Bob forges \( (| S_{a} >, | \delta_{a} >, | R_{b} >, | r_{b} >) \), it will be detected by the Charlie, because Charlie decrypts \( | S_{a} > \) and gets \( (| M >, | R >, | w >, | \delta_{a} >) \), then she
can find Bob had forged the signature by comparing $|\delta_\beta\rangle$ with $E_{K_\beta}(|w\rangle)$ and comparing $|R_\gamma\rangle$ with $\otimes_{i=1}^n \delta_{i}^{(K_i\oplus X_{OKE}(K_i))}|R_i\rangle$, it would be detected by Charlie. Hence Bob cannot forge the proxy signature.

4.2. Impossibility of Disavowing

The schemes also can resist the original signer Alice$_o$, the proxy signer Alice$_p$ and the receiver Bob disavowing the signature. Because the arbitrator Charlie is trusted by Alice$_o$, Alice$_p$ and Bob, so if they disavow their signature, Charlie can make a judgment between them.

4.2.1. The Original Signer Alice$_o$ Cannot Her Authorization: If Alice$_o$ confirm that that she hasn’t delegated her signing capability to the proxy signer Alice$_p$, it would be detected by Charlie. Because Alice$_o$ generates $|\delta\rangle = E_{K_\delta}(|w\rangle)$, so Alice$_o$’s secret key $K_\delta$ was involved in $|\delta\rangle$, hence Alice$_o$ cannot disavow that she delegates her signing capability to the proxy signer Alice$_p$.

4.2.2. The Proxy Signer Alice$_o$ Cannot Her Has Signing the Quantum Signature: If Alice$_p$ disavows her signature, the arbitrator can confirm that Alice$_p$ has signed the message. Because Alice encrypts her signature $|S\rangle = E_{K_p}(|M\rangle, |R\rangle, |w\rangle, |\delta\rangle)$ with her secret key $K_p$. And Charlie can get the $(|M\rangle, |R\rangle, |w\rangle, |\delta\rangle)$ by decrypting $|S\rangle$. Hence Alice$_p$ cannot deny having signed the message.

4.2.3. The Receiver Bob Cannot Her Has Receiving the Quantum Signature: Similarly, if Bob disavows receipt of the signature, Charlie also can confirm that Bob has received the signature $|S_{Bob}\rangle$. The valid proxy signature is $(|M\rangle, |w\rangle, |\delta\rangle, |R_\gamma\rangle)$, but Bob only obtains $(|M\rangle, |w\rangle, |\delta^*\rangle, |R_\gamma\rangle)$, so if Bob wants to get the signature information $|\delta\rangle$, he must inform Charlie to publish $r$ by the public board. Therefore Bob cannot disavow that he has received $|S_{Bob}\rangle$. Hence Bob’s denial is impossible.

5. Conclusions

In this paper, we present an arbitrated proxy signature scheme based on quantum cryptography. In our scheme, the signatory is kept the original signer can delegate his signing capability to others. Different from previous classical proxy signature scheme, the security of our scheme is guaranteed by the quantum one-time pad and quantum key distribution. And the new scheme ensures the signature receiver cannot disavow receipt of the signature. Hence, it is unconditionally secure.

Acknowledgements

This work is supported in part by the Zhejiang Provincial Natural Science Foundation of China under Grant (No. LQ12F02006).
References