A Quantum Multi-agent Blind Signature Scheme

Jingjing Chen 1 and Fucheng You*

1 Beijing Institute of Graphic Communication, China, 102600, Beijing
*Corresponding author’s e-mail: youfucheng@bigc.edu.cn

Abstract. With the development of information society, people are increasingly concerned about the security problems caused by information leakage, and digital signatures play an irreplaceable and important role in the protection of information security, which replace traditional manual signatures and seals in the network environment and have important roles such as anti-forgery, anti-tampering, anti-replay, identifiable identity and confidentiality [1]. However, with the in-depth study of quantum mechanics, it has been found that the confidentiality mechanism of classical digital signatures is under serious threat. Since quantum computing is a parallel operation with exponentially increasing operational capability, a series of complex mathematically difficult problems can be rapidly overcome. Based on the above, this paper proposes a multiple agent blind signature scheme, which adopts the key technologies such as the Unitary transformation and Hadamard gate operation, and adds multiple agent signature to quantum signature to improve the efficiency of the protocol, and adds blind signature to improve the security of the protocol. At the same time, the scheme uses quantum key distribution to ensure its unconditional security, which is applicable in systems such as electronic voting and electronic payment, and has certain anti-attack capability [2].

1. Introduction
Digital signature, as an important part of cryptography, has been widely used to provide secure electronic communication and is one of the most popular and operational techniques for identifying the signer and verifying whether the information has been tampered with [3]. In the communication process, it provides authentication services and anti-denial services, among others. The security of digital signatures is mainly based on difficult problems such as the discrete logarithm problem over the domain of prime numbers, the elliptic curve problem, and the factorization problem for large ensembles [4-6].

Quantum signature is different from the traditional digital signature, which is a new signature system using quantum physics approach to realize the idea of digital signature, and its security is guaranteed by the basic principles of quantum mechanics, such as the uncertainty principle and the unclonable theorem [7]. Since quantum computing is a parallel operation with exponentially increasing operational capability, it can rapidly overcome a series of complex mathematical difficulties of classical digital signatures[8].

In 2001, since Zeng [9] proposed a scheme for quantum signatures using the entanglement properties of GHZ three-body entangled states, thus opening up a new dimension of in-depth research on quantum signatures. Yang et al. proposed a multi-agent quantum group signature scheme with threshold shared authentication for classical messages [10]. Shi et al. proposed a discrete quantum Fourier transform-based Zhou et al. proposed a publicly certifiable quantum proxy signature [11], which is based on the properties of EPR entangled pairs and the Unitary transformation, and the signature is generated without using the verifier's key. Xu proposed a new quantum proxy signature
scheme [12] that does not use entangled states, which uses only a single particle, making the protocol easy to implement.

Traditional proxy signatures use only one proxy signer for proxy operation, and the power is too centralized. And when this proxy signer is dishonest, it may cause man-in-the-middle attack and make the signature not work properly. Therefore the original signer authorizes multiple proxy signers to produce a valid signature only when multiple proxy signers work simultaneously, and thus people started to study multiple proxy signature protocols [13].

In the signing process, the message owner does not want the signer to know the specific content of the signed document or message, while the owner of the document or message is required to get the signature of the signer about the real document or message, and then the blind signature appears [14]. The operation process of blind signature is as follows: the message owner blinds the data to be signed and sends the blinded message to the signer, when the signer receives the blinded message, he does not know the specific content of the message, but only proves that he already knows the message, and uses some method to sign the blinded message, and then sends it back to the message owner, who receives the message blinded by the signer and removes the blinded message. After receiving the message signed by the signer's blind signature, the blind factor is removed and the signature of the original message is obtained from the blind signature [15].

In order to solve the problems presented above and improve the security and efficiency of quantum signatures, a new quantum multi-agent blind signature scheme is proposed in this paper. This scheme uses the Unitary transformation and Hadamard gate as the main technical support, and in the subsequent analysis, we can learn that this scheme not only satisfies the general quantum signature with non-repudiation and non-forgeability, but also, due to the inclusion of multiple agents and the blind process, this scheme is also blind, untraceable, and can resist certain attacks.

2. Fundamentals

2.1. Key Generation

The key generator randomly generates n 0,1 strings of length n. These strings are the key $A_i$ (1 ≤ i ≤ n), and the x 0,1 strings of length n are used to do the operation as follows to get

$$K = A_1 \oplus A_2 \oplus \cdots \oplus A_n$$

Let $K_{C_T} = K$

2.2. Hadamard gate

The Hadamard gate changes $|0\rangle$ to $|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ and $|1\rangle$ to $|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$. Since $H^2 = I$, going through two consecutive Hadamard gates is equivalent to not performing any operation.

The Hadamard gate corresponds to the unitary operator as

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

The Hadamard gate acts as a transform on the quantum bits, and the result of the transform is shown below.

$$H|0\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) = |+\rangle$$

$$H|1\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = |-\rangle$$
3. The proposed scheme

In scheme, the message owner is Alice. There are $n$ proxy signatories $\{\text{Bob}_1, \text{Bob}_2, \ldots, \text{Bob}_n\}$, and each of them can sign for Charlie. The message receiver is David, and the trusted original signer is Charlie. There is also a trusted arbitrator called Trent.

There is a contingency that for some reasons Charlie cannot sign the file or message, so he delegates some proxy signers to sign, and the signature is valid only after all these proxy signers have performed the signing operation. The scheme concludes three phases as follows: the initialising phase, the signing phase, and the verifying phase.

3.1. Initializing phase

The message sequence which is needed to signed is $m = m_1, m_2, \ldots, m_n \in \{0, 1\}$ and the initialization procedure is described below.

Step 1 According to the BB84 protocol or B92 protocol, there is unconditional security between the keys. Therefore Alice and Charlie share an $n$-bit classical bit key $K_{AC}$, and Charlie and Trent also share an $n$-bit classical key $K_{CT}$.

Step 2 There are $n$ proxy signatories who have an $n$-bit classical key $A_i$ ($1 \leq i \leq n$) for each of them and they share the keys with the trusted original signer Charlie.

3.2. Signing phase

Alice uses the key $K_{AC}$ to blind the message sequence $m$ and the rules are as follows. It converts the message $m$ into ciphertext to obtain the quantum message sequence $m'$ where

$$
|m(i)\rangle = \begin{cases}
|0\rangle, & \text{if } m(i) = 0, \quad K_{AC}(i) = 0 \\
|1\rangle, & \text{if } m(i) = 1, \quad K_{AC}(i) = 0 \\
|+\rangle, & \text{if } m(i) = 0, \quad K_{AC}(i) = 1 \\
|-\rangle, & \text{if } m(i) = 1, \quad K_{AC}(i) = 1
\end{cases}
$$

Step 1 In order to resist interception of retransmission attacks, Alice chooses some decoy particles which are in the states of $|0\rangle, |1\rangle, |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ or $|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$, records their quantum states and insertion position. Then, Alice inserts them into the quantum message sequence $|m\rangle$ randomly. In this way, a new quantum message sequence which is noted as $|m'\rangle$ was produced. After the above operation, Alice sends $|m'\rangle$ to the first idle proxy signer which was noted as $B_1$.

Step 2 After $B_1$ receives $|m'\rangle$, he needs to remove the decoy partials. $B_1$ tells Alice his receiving of $|m'\rangle$, and Alice posts all the information of the decoy partials. At the same time, based on the known
information and the error threshold, $B_1$ determines whether there is an eavesdropper, and the protocol is terminated if or when the error rate is greater than a certain threshold, otherwise the next step is performed.

Step 3 Then $B_1$ removes all the decoy partials in $|m\rangle$ according to the above information which are inserted before. And he gets the original quantum message sequence and uses the key $A_1$ to sign the message. After his signing, message sequence $|m\rangle$ which was signed is noted as $|m_1\rangle$. After the end of above operation, $B_1$ also does the same operation as Alice. $B_1$ chooses some decoy particles which are in the states of $|0\rangle$, $|1\rangle$, $|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ or $|\pm\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$, records their quantum states and insertion position. Then $B_1$ inserts them into the quantum message sequence $|m_1\rangle$ randomly. And now, after a series of operation, the quantum sequence is noted as $|m_1\rangle$. $B_1$ sends it to the next proxy signer, denoted as $B_2$.

Step 4 According to the above description, all the proxy signatories do the same operation as $B_1$. That is, the proxy signatories receive the message from the previous proxy signatories, remove the decoy particles, signs it, and then randomly insert the decoy particles before sending it to the next proxy signatore. And the last one to sign the message is called $B_n$. $B_n$ finishes his signature and sends the quantum sequence $|m_n\rangle$ to the trusted arbitrator which is called Trent. At this point, all proxy signatories complete their signatures and hand them over to the trusted arbiter for verification.

3.3. Verifying phase

Step 1 After Trent receives $|m_n\rangle$, he needs to remove the decoy partials. Trent tells $B_n$ his receiving of $|m_n\rangle$, and $B_n$ posts all the information of the decoy partials. At the same time, based on the known information and the error threshold, Trent determines whether there is an eavesdropper, and the protocol is terminated if or when the error rate is greater than a certain threshold, otherwise the next step is performed.

Step 2 Trent gets the quantum message sequence $|m_1\rangle$ by the above operations. Then he calls Alice to sends him the original quantum message sequence $|m\rangle$ to finish the verification.

Trent compares the quantum message sequence from $|m\rangle$ Alice and the quantum message sequence $|m_1\rangle$ he received, if they are the same, then he proves that he has received the correct message and the signature is valid, and sends the verified message to the message recipient David otherwise it is invalid.

4. Security analysis

4.1. Blindness

Suppose an internal or external attacker wants to intercept and retransmit the message, and since the attacker does not know the original message, the number of decoy particles Alice inserted in the sequence, and the quantum state, they will choose the correct message from $|0\rangle$, $|1\rangle$, $|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ or $|\pm\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ then it has $(1/4)^n$ probability of getting the correct message, and the correctness tends to 0 when $n$ is large enough.
4.2. Unforgeability
In this scheme, it is impossible for a dishonest internal or external attacker to forge messages and signatures.

Suppose an attacker wants to forge a signature, he needs the key required for the signature, but since the key is distributed directly through the BB84 protocol or the B92 protocol, he cannot forge the signature.

Suppose an attacker wants to forge a message. First, the message is blind, and the attacker needs to choose the correct quantum state from 
\[ |0\rangle, \ |1\rangle, \ |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \text{ or } |–\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \]
to compose the message sequence, and it has \((1/4)^n\) probability of getting the correct message, and the correctness tends to 0 when \(n\) is large enough.

4.3. Undeniability
In the signing process, messages are sent between the message sender, the proxy signer, the trusted message signer, and the trusted verifier via keys, which are distributed directly via the BB84 protocol or the B92 protocol. Therefore, Alice cannot deny that she sent the quantum message sequence, and the proxy signers cannot deny that they performed the signature. If one person denies having performed the operation in question, eventually Trent will verify the signature, and if the verification fails, the signature is invalid.

4.4. Unconditional security
All keys are distributed directly through BB84 protocol or B92 protocol during signing, blinding and message transmission with unconditional security. At the same time, this scheme machine and secure quantum communication channel, with instantaneous transmission, is not limited by distance, time and obstacles, thus ensuring the unconditional security of this scheme.

5. Example
Suppose Alice has a sequence of messages \(m=\{0,1,0,1,...\}\) (n bits), Charlie and Alice share the key \(K_{AC} = \{0,1,1,0,...\}\), then according to the above it follows that 
\[ |M\rangle = \{ |0\rangle, \ |–\rangle, \ |+\rangle, \ |1\rangle \}. \]

Suppose there are three proxy signers, \(A_1, A_2, A_3\), Charlie shares n-bit keys with \(A_1, A_2, A_3\), \(A_1 = \{0,1,1,...\}\), \(A_2 = \{1,0,1,0,...\}\), \(A_3 = \{0,1,0,0,...\}\), Charlie and Trent also share the n-bit key, and from the above, \(K_{CT} = A_1 \oplus A_2 \oplus A_3 = \{1,0,0,1,...\}\).

This scheme has no requirement on the signature order, assuming that the signature order is \(A_3, A_1, A_2\), and the specific operation procedure is shown in the following table.

| Description | 1   | 2   | 3   | 4   |
|-------------|-----|-----|-----|-----|
| \(m\)       | 0   | 1   | 0   | 1   |
| \(|M\rangle\) | \(|0\rangle\) | \(|–\rangle\) | \(|+\rangle\) | \(|1\rangle\) |
| After A\(_3\) signature | \(|0\rangle\) | \(|1\rangle\) | \(|+\rangle\) | \(|1\rangle\) |
| After A\(_1\) signature | \(|0\rangle\) | \(|–\rangle\) | \(|0\rangle\) | \(|–\rangle\) |
| After A\(_2\) signature | \(|+\rangle\) | \(|–\rangle\) | \(|+\rangle\) | \(|–\rangle\) |
| After Trent verification | \(|0\rangle\) | \(|–\rangle\) | \(|+\rangle\) | \(|1\rangle\) |

6. Conclusion
In this paper, we propose a new quantum multiple agent blind signature scheme, whose security is based on the basic principles of quantum mechanics and is less susceptible to cracking compared to
classical digital signatures. The scheme first uses the features of blind signature to blind the message and protect the message content from being leaked. When the original signer is unable to sign the document, it is authorized to delegate multiple proxy signers to work on the document in turn, and the signature may be valid only when they all complete specific operations. Moreover, there is no requirement for the order of the signatures of multiple proxy signers, which greatly improves the efficiency of signing. The main technique relies on the Unitary transformation and Hadamard gate operation, and the keys are generated by BB84 protocol or B92 protocol, which ensures the unconditional security of the scheme. According to the security analysis, the scheme is blind, non-forgable, non-repudiation, and unconditionally secure, and can withstand certain attacks.

Acknowledgments
This research was supported by Joint Funding Project of Beijing Municipal Commission of Education and Beijing Natural Science Fund Committee (KZ201710015010), initial funding for the Doctoral Program of BIGC (27170120003/022), BIGC Project (Eb202004) and BIGC Project (Ec202007).

References
[1] Van Wang Qian. A review of coding-based digital signature techniques [J]. Digital Technology and Applications,2020,38(09):186-189.
[2] Xie Guo. Quantum agent blind signature and its application [D]. Shaanxi Normal University,2019.
[3] https://www.zhihu.com/question/382360558/answer/1110373364
[4] Feng Yanyan; Zhang Qian; Shi Jinjing; Chen Shuhui; Shi Ronghua. Quantum Proxy Signature Scheme with Discrete Time Quantum Walks and Quantum One-Time Pad CNOT Operation. [J]Applied Sciences Volume 10, Issue 17. 2020. PP 5770-5770
[5] Xiangjun Xin; Qinglan Yang; Fagen Li. Quantum proxy signature with provable security.[J]Modern Physics Letters A Volume 35, Issue 24. 2020.
[6] Xu-Feng Niu; Wen-Ping Ma; Bu-Qing Chen; Ge Liu; Qi-Zheng Wang.: A Quantum Proxy Blind Signature Scheme Based on Superdense Coding.[J]International Journal of Theoretical PhysicsVolume 59, Issue 4. 2020. PP 1121-1128
[7] Du Chengbin. Design and analysis of multiple blind signature protocols for quantum agents [D]. Anhui University,2017.
[8] Zhang, J., Bai, W., Wang, Y.: Non-interactive ID-based proxy re-signature scheme for IoT based on mobile edge computing. IEEE Access 7, 37865–37875 (2019)
[9] Zeng Guihua, Ma Wenping, Wang Xinmei, Zhu Hongyi. A signature scheme based on quantum cryptography[J]. Journal of Electronics,2001,29(8);1098-1100.
[10] Yu-Guang Y . Multi-proxy quantum group signature scheme with threshold shared verification [J] . Chinese Physics B, 2008, 17(2) : 415.
[11] Shi J,Shi R,Tang Y,et al.A multiparty quantum group signature scheme for the entangled-state message with quantum Fourier transform [J]. Quantum Information Processing, 2011, 10(5) :653-670.
[12] Xu G . Novel quantum proxy signature without entanglement [J] . International Journal of Theoretical Physics, 2015, 54(8) : 2605-2612.
[13] Liang JW, Liu XS. A multiple agent blind signature scheme based on quantum characteristics[J]. Information Network Security,2018(07):55-59.Xu G . Novel quantum proxy signature without entanglement [J] . International Journal of Theoretical Physics. 2015. 54 (8) : 2605-2612.
[14] Chaum, D.: Blind signature for untraceable payments. Advances in cryptology. In: Proceeding of Crypto82, pp. 199–203. Springer, New York (1983)
[15] Su Q., Zheng H., Qiaoyan W., Wenmin L.: Quantum blind signature based on two-state vector formalism. Opt. Commun. 283(21), 4408–4410 (2010)