A Quantum Multi-Agent Blind Signature Scheme with Unordered Signatures

Jingjing Chen¹ and Fucheng You¹*

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

Abstract. With the development of information society, network security problems are becoming more and more serious, and digital signature as an authentication method is widely used in many fields such as information security and e-commerce, mainly to solve security problems such as forgery, repudiation, impersonation and tampering [1]. The latest quantum technology can overcome a series of difficult problems of classical digital signatures in a very short time. In this paper, we propose a quantum multi-proxy blind signature scheme, in which the original signer is unable to sign the document himself, and delegates multiple proxy signers to sign and verify the document, and the signature order of the proxy signers is not restricted. The scheme adopts techniques such as Unitary transformation and Hadamard gate, and uses quantum key distribution protocol to ensure its security, which improves the efficiency of signature, ensures the security of signature, and has certain anti-attack capability.

1. Introduction
Since the introduction of digital signatures, various signature methods have been proposed, and it is known from the literature [2-5] that most of them are based on classical cryptographic schemes. From the literature [6-9], it is known that the security of classical digital signature schemes is mainly based on the discrete logarithm problem over the prime number domain, the elliptic curve problem, and the factorization problem of large ensembles, which can be quickly cracked by quantum computers in a short time. Quantum signatures can be seen as an extension of classical digital signatures into the quantum domain, where the security of quantum signatures is not based on public key cryptography, but on quantum theories such as the uncertainty principle and the unclonability theorem.

Since 2001, when Zeng [10] first proposed a scheme for quantum signature using the entanglement properties of GHZ three-body entangled states, it has set off a boom in quantum signature research. Gottesman [11] proposed a quantum digital signature scheme based on quantum one-way functions, which enables multiple users to verify the same signed message. Lee [12] et al. proposed two quantum digital signature schemes based on automatic message recovery, which are arbitration signature schemes. Lü [13] proposed a quantum signature scheme based on GHZ three-body entangled state particles and quantum solid code, which is capable of signing unknown quantum states. Wen [14] proposed a multiple quantum signature scheme that can support multiple users to sign the same message. The in-depth study of quantum signatures has laid a good foundation for the study of quantum multiple agent signatures and quantum blind signatures.

When the original signer is unable to sign for some reason, his signature rights are delegated to a proxy signer, who is then allowed to generate a valid signature on behalf of the original signer [15]. Proxy signatures allow a proxy signer to sign a message on behalf of the original signer in the absence of the original signer. Sometimes, the original signer cannot trust a single proxy signer, so he assigns
his signature privileges to multiple proxy signers and then requires that a valid signature can be generated only when all proxy signers work together [16].

A well-performing quantum signature protocol should have the advantages of high security, high efficiency, and some resistance to attacks, so this scheme adds multiple proxy signers to quantum signatures to improve the efficiency of signatures and blind signatures to improve the security of signatures. This scheme not only satisfies the properties that general quantum signature schemes should have such as non-repudiation and non-forgeability, but also satisfies some special properties such as multi-proxy, blindness, and untraceability, so this scheme can be applied to systems such as e-voting and e-payment. At the same time, this scheme can resist some common attacks.

2. The proposed scheme
In this scenario, Alice is the message owner with x proxy signers {Bob1, Bob2, ..., Bobx}, Charlie is the message receiver, David is the trusted president, and Trent is the trusted message verifier.

Suppose that within a company, when David cannot sign a document himself and cannot trust a single proxy signer to sign the document, he delegates a certain number of proxy signers to sign the document. The scheme consists of three phases: an initialization phase, a proxy signing phase, and a verification phase.

2.1. Initializing phase
We assume that the message is \( M = m_1, m_2, ..., m_n \in \{0, 1\} \) and the initialization phase is described as follows.

Step 1 Alice and David share an n-bit classical bit key \( K_{AD} \), and Alice and Charlie also share an n-bit classical bit key \( K_{AC} \). These keys are generated by the BB84 protocol or B92 protocol, which guarantees the unconditional security of the keys.

Step 2 David and his delegated x proxy signer share a n-bit classical key \( A_i (1 \leq i \leq x) \), and David and Trent share an n-bit classical key \( K_{DT} \). These keys are also distributed using the BB84 protocol or B92 protocol.

2.2. Signing phase
Alice uses the key \( K_{AD} \) shared with David to blind the message \( M \) and convert the message into ciphertext to obtain the quantum message sequence \( |M \rangle \).

Step 1 Alice randomly inserts some sample photons in the states \( |0 \rangle, |1 \rangle, |+\rangle = \frac{|0 +1\rangle}{\sqrt{2}} \) or \( |-\rangle = \frac{|0 -1\rangle}{\sqrt{2}} \) into the quantum message sequence \( |M \rangle \) to form a new quantum message sequence \( |M' \rangle \), Alice records their insertion positions and quantum states, and sends \( |M' \rangle \) to the idle proxy signer, noted as \( B_1 \), with no requirement on the signature order of the proxy signer when signing.

Step 2 After \( B_1 \) receives \( |M' \rangle \), he tells Alice that he has received it, Alice announces the position and quantum state of the randomly inserted photon, and \( B_1 \) selects the corresponding measurement base for measurement according to the quantum state announced by Alice. After the measurement, the error rate is calculated, and if the error rate is greater than a certain threshold, the protocol is terminated, otherwise the next step is executed.

Step 3 \( B_1 \) removes the inserted photons in \( |M' \rangle \) according to the position announced by Alice to get the original quantum message sequence \( |M \rangle \). \( B_1 \) uses his own key \( A_1 \) to perform the signature operation on \( |M \rangle \) to get the signed quantum sequence \( |M_1 \rangle \), and similarly, insert some sample photons of \( |0 \rangle, |1 \rangle, |+\rangle = \frac{|0 +1\rangle}{\sqrt{2}} \) or \( |-\rangle = \frac{|0 -1\rangle}{\sqrt{2}} \) into the sequence \( |M_1 \rangle \), noted as \( |M'_1 \rangle \), are sent to the next idle proxy signer, denoted \( B_2 \).

Step 4 \( B_2 \) performs the same operation as \( B_1 \), as described in Step 2, until all proxy signers have completed their signatures, and the last one to complete the signature, noted as \( B_x \) sends the final sequence of formed quantum signatures, noted as \( |M'_x \rangle \), to the message recipient Charlie and the trusted message verifier Trent.
2.3. Verifying phase

Step 1 After Charlie and Trent receive the quantum signature sequence $|M_1\rangle$, Bob announces the position and quantum state of the sample photon and then measures it, and if the error rate is greater than a certain threshold, the protocol is terminated, otherwise the next step is executed.

Step 2 Charlie uses the key $K_{AC}$ to solve the obtained quantum message sequence $|M_2\rangle$ and sends it to Trent for verification.

Step 3 Trent uses the key $K_{DT}$ to perform the verification operation, gets the quantum message sequence $|M_3\rangle$ and tells Alice that the verification operation has been completed, Alice again prepares the quantum message sequence $|M_4\rangle$ and sends it to Trent, who compares the quantum message sequence $|M_4\rangle$ from Alice, the quantum message sequence $|M_2\rangle$ from Charlie, and the quantum message sequence $|M_1\rangle$ which he received. If all three are the same, then the message recipient Charlie is proven to have received the correct message and the signature is valid, otherwise invalid.

3. Security Analysis

3.1. External Attacks

Suppose an attacker wants to intercept a retransmission, and since he does not know how many numbers of $|0\rangle$, $|1\rangle$, $|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ or $|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ sample photons are inserted at which positions in the sequence of quantum messages, the attacker will only be able to intercept the retransmission by trying to arrive at the correct quantum message and not being detected with probability $(1/4)^n$, $n$ being the number of samples, and the probability tends to zero when $n$ is large enough.

Suppose the attacker wants to forge the signature, but the key $A_i$ $(1 \leq i \leq x)$ of the proxy signer Bob, $(1 \leq i \leq x)$ is distributed through the BB84 protocol or B92 protocol with unconditional security, so the attacker cannot forge the signature.

3.2. Unforgeability

Suppose Alice, the message owner, wants to forge a signature, but since she does not have the key $A_i$ $(1 \leq i \leq x)$ for any of the proxy signers, she cannot forge the signature.

Suppose all the proxy signers Bob, $(1 \leq i \leq x)$ want to collude to forge a signature, but since they do not have any information about the key $K_{AD}$, they cannot prepare a valid sequence of quantum messages $|M\rangle$ and the trusted verifier Trent compares the sequence of quantum messages from Bob, and Alice, and if they are not equal, then the verification cannot be passed.

3.3. Undeniability

The message owner Alice cannot deny the quantum message sequence $|M\rangle$ she sent. Because the message sequence $|M\rangle$ contains the key $K_{AD}$ that only Alice and David know, once Alice denies it, David can determine whether the message was sent by Alice based on whether the message sequence $|M\rangle$ contains the key $K_{AD}$.

No proxy signer Bob, $(1 \leq i \leq x)$ can deny that he performed the signature. If one of the proxy signers denies signing, the trusted verifier Trent eventually compares the sequence of quantum messages from Bob, and Alice, and if they are not equal, then the verification fails.

4. Conclusion

In this paper, we propose a quantum multi-agent blind signature scheme with unordered signatures, which uses the Unitary transformation to complete the signing and verification process, and the key is generated by BB84 protocol or B92 protocol to ensure the unconditional security of the key, so that the original signer can delegate more than one person to sign, and the order of the signatures is not restricted, which greatly improves the efficiency of the signature. The scheme security analysis is elaborated from three aspects, which proves that the scheme can resist certain attacks and has unforgeability and undeniability.
Acknowledgments
This research is 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] Chen, Kaibing. Blind signatures and their applications [J]. Journal of Chuzhou Vocational and Technical College,2006(01):59-61
[2] Li, X., Chen, K., Sun, L. Certificateless signature and proxy signature schemes from bilinear pairings. Lith. Math. J. 45(1), 76–83 (2005).
[3] Zhang J., Wu, Q. An improved nominative proxy signature scheme for mobile communication. IEICE Trans. Inf. Syst. E88-D(7), 1697–1699 (2005).
[4] 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).
[5] Patonico, S., Shabisha, P., Braeken, A., Touhai, A., Steenhaut, K.: Elliptic curve-based proxy re-signcryption scheme for secure data storage on the cloud. In: Concurrency and Computation-Practice & Experience. https://doi.org/10.1002/cpe.5657 (2020).
[6] Shor, P.W.: Algorithms for quantum computation: discrete logarithm and factoring. In: Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, pp. 124–134. IEEE Computer Society Press (1994).
[7] Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. 26(5), 1484–1509 (1997).
[8] Grover, L.K.: Quantum mechanics helps in searching for a needle in a haystack. Phys. Rev. Lett. 79(2), 325–328 (1997).
[9] Huang, Y., Su, Z., Zhang, F., et al.: Quantum algorithm for solving hyper elliptic curve discrete logarithm problem. Quantum Inf. Process. 19(62), 1–17 (2020).
[10] Zeng Guihua, Ma Wenping, Wang Xinmei, Zhu Hongyi. A signature scheme based on quantum cryptography[J]. Journal of Electronics,2001,29(8);1098-1100.
[11] Gottesman D, Chuang I. Quantum digital signatures[ DB/ OL]
[12] http://arxiv.org/abs/quant-ph/0105032.pelf,2001-05-08.
[13] Lee H, Hong C, Kim H, et al. Arbitrated quantum signature scheme with message recovery [J]. Physics Letters A, 2004, 321(5-6):295-300.
[14] Lü X, Feng D G. An arbitrated quantum message signature scheme[A].CIS2004, Lecture Notes in Computer Science 3314 [ C]. Heidelberg:Springer,2004.1054-1060.
[15] Mambo, M., Usuda, K., Okamoto, E. Proxy signature: delegation of the power to sign messages. IEICE Trans. Fundam. E79-A(5), 1338–1354 (1996).
[16] Huawang Qin, Wallace K. S. Tang, Raylin Tso. Efficient quantum multi-proxy signature. 2019, 18(2):53. Mettam, G.R., Adams, L.B. (2009) How to prepare an electronic version of your article. In: Jones, B.S., Smith, R.Z. (Eds.), Introduction to the Electronic Age. E-Publishing Inc., New York. pp. 281-304.