A New Efficient Blind Quantum Signature Scheme Based on Entanglement Swapping

Yun SONG∗
School of Computer Science, Shaanxi Normal University, Xi’an 710062, China
∗Corresponding author

Keywords: Quantum cryptography, Blind quantum signature, GHZ states, Entanglement swapping.

Abstract. According to the principle of quantum entanglement swapping of GHZ states, this paper put forward a blind signature scheme based on quantum entanglement. Without performing any unitary operation, all participants just need to do Bell measurements on new entangled particles emerging from entanglement swapping of GHZ states to complete blind signature and verification. It is not difficult to prove that the proposed scheme processes the features of nonforgeability, non-disavowal and blindness. Furthermore, compared to some other blind signature schemes on entangled states, our scheme is more efficient because except a few decoy particles, only 2 GHZ states are required for signing each 3 bits in the message.

Introduction

Digital signatures, proposed by Diffe and Hellman [1], aim to be applied between the document owner and the signer to certify the identity of legal messages as well as the authenticity of a signature. But the ordinary digital signature cannot guarantee the message owner’s anonymity, which fails to satisfy the new application requirements in the area of electronic commerce. In a blind signature scheme, a message could be signed by another party, signatory, who knows nothing about the content.

After the quantum mechanism appears [2-4], classical blind signatures based on mathematical complexity may be easily broken. In the light of one-way function, Gottesman et al. [5] come up with the first quantum signature. Zeng et al. [6] put forward an arbitrated signature according to GHZ states. Since then, many quantum signature strategies have been proposed [7-14]. In 2009, Wen et al. [15] presented a weak blind signature using EPR pairs. But Naseri [16] found that the previous scheme failed to fully implement the role of a blind signature. Shortly afterwards, Wang et al. [17] found a blind signature scheme. This scheme comprises two stages of signature and link-recovery. Afterwards, He et al. [18] pointed out this kind of scheme cannot conform to the requirements of nonforgeability. Considering verifiable property, using $\chi-type$ entangled states, a blind quantum signature was presented by Yin et al. [19] in 2011. According to GHZ states, Wang et al. [20] pointed out a weak blind quantum signature scheme. Tian et al. [21] proposed a proxy blind signature scheme in terms of the quantum correlations among three particles in a GHZ triplet, which can possess both proxy and blind attributes. On basis of quantum entanglement swapping of Bell states, Zhang and Li [22] analyze the advantage of their weak blind quantum signature scheme. In accordance with feature of five-particle entangled state, a new quantum blind signature scheme was presented by Zeng et al. [23] which made use of Vernam method to blind messages.

In this paper, on the basis of entanglement swapping of GHZ entangled states, we put forward a blind quantum signature. Before using GHZ states, the proposed scheme operates each particle of the GHZ state, which is different from the previous scheme with entangled states. We establish a one-to-one correspondence between the family of every three bits to be signed and the set of all the local operations utilized to act on one particle of GHZ states. Moreover, in terms of the correlation of quantum entanglement swapping between initial GHZ states and GHZ states after local unitary operations, the implementation of the verification phase becomes much easier. What’s more, only 2 GHZ states are required for signing each 3 bits in the message, which makes our scheme more efficient and more practical compared to some other blind signature schemes on entangled states.
Preliminaries

The complete orthonormal set of the GHZ states is

\[
|GHZ_{xyz}\rangle_{ABC} = \frac{1}{\sqrt{2}} \left[ |0, y, z\rangle_{ABC} + (-1)^x |1, y \oplus 1, z \oplus 1\rangle_{ABC} \right],
\]

(1)

Where \( A, B, C \) denote the three qubits in a GHZ state, \( x, y, z \in \{0, 1\} \). Let \( I = |0\rangle\langle 0| + |1\rangle\langle 1|, \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|, \sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|, i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0| \) be local unitary operators which are employed to act on one qubit of the GHZ state. Table 1 shows the results of encoding information by using operations.

Blind Quantum Signature Scheme Based on Entanglement Swapping

Our scheme has three parties involved: Alice who is the message owner, blind the original message; In the case of not knowing the content of the message, Charlie signs on the blind message as a signatory; Bob is considered as the verifier, verifying the signature validity and the authenticity of the message. The scheme is composed of three parts: initial phase, blind signature generation phase and verification phase.

Initializing Phase

This phase prepares GHZ entanglement triples and generates keys.

**Step 1.1** The secret key \( k_{CB} \) is shared between Bob and Charlie. The secret key \( k_{BA} \) is shared between Bob and Alice. The above keys are all distributed through the QKD protocols.

**Step 1.2** Alice prepares \( 2l + 2s \) GHZ states. These GHZ states are divided into \( l + s \) groups in which every group has two GHZ states \( |GHZ_{000}\rangle_{123} \) and \( |GHZ_{000}\rangle_{456} \).

Blind Signature Generation Phase

**Step 2.1.** Alice produces a bit sequence \( m = \{m_1, m_2, ..., m_l\} \), with \( m_i \in \{0,1\} \), for the message which is expected to be signed by Bob.

| secret message | Operator | local unitary operators on \( |GHZ_{000}\rangle_{ABC} \) | result |
|----------------|----------|---------------------------------------------|--------|
| 000            | \( \sigma_1 \) | \( I \otimes I \otimes I \)                  | \( |GHZ_{000}\rangle_{ABC} \) |
| 001            | \( \sigma_2 \) | \( I \otimes I \otimes \sigma_x \)          | \( |GHZ_{001}\rangle_{ABC} \) |
| 010            | \( \sigma_3 \) | \( I \otimes \sigma_x \otimes I \)          | \( |GHZ_{010}\rangle_{ABC} \) |
| 011            | \( \sigma_4 \) | \( a_x \otimes I \otimes I \)               | \( |GHZ_{011}\rangle_{ABC} \) |
| 100            | \( \sigma_5 \) | \( I \otimes I \otimes \sigma_z \)          | \( |GHZ_{100}\rangle_{ABC} \) |
| 101            | \( \sigma_6 \) | \( I \otimes I \otimes -i\sigma_y \)        | \( |GHZ_{101}\rangle_{ABC} \) |
| 110            | \( \sigma_7 \) | \( I \otimes -i\sigma_y \otimes I \)        | \( |GHZ_{110}\rangle_{ABC} \) |
| 111            | \( \sigma_8 \) | \( i\sigma_y \otimes I \otimes I \)         | \( |GHZ_{111}\rangle_{ABC} \) |

**Step 2.2** Alice records the positions of \( s \) groups. For \( l \) groups, as shown in Table 1, Alice determines the corresponding operator to operate on one photon of \( |GHZ_{000}\rangle_{456} \) in each group according to every three classical bits in the message \( m \). For instance, if \( m_0 = \{101001000\} \), then the operators Alice utilized is \( \sigma = \{\sigma_6, \sigma_2, \sigma_1\} \). The following sequences are divided by Alice:
\[ S_1 = \{P_i(1), P_2(1), \ldots, P_{i+s}(1)\}, \quad S_2 = \{P_i(2), P_2(2), \ldots, P_{i+s}(2)\}, \]

\[ S_3 = \{P_i(3), P_2(3), \ldots, P_{i+s}(3)\}, \quad S_4 = \{P_i(4), P_2(4), \ldots, P_{i+s}(4)\}, \]

\[ S_5 = \{P_i(5), P_2(5), \ldots, P_{i+s}(5)\}, \quad S_6 = \{P_i(6), P_2(6), \ldots, P_{i+s}(6)\}, \]

Where \( P_i(1), P_i(2), \ldots, P_i(6) \) are the order of particles in the two GHZ states in the \( i-th \) group from \( 1+s \) groups in Step (1.2) and \( 1 \leq i \leq l + s \). Alice keeps \( S_1, S_2 \) with himself and delivers two sequences \( S_3, S_4 \) to Charlie, two sequences \( S_5, S_6 \) to Bob. Alice has to affirm whether each agent has received two sequences via classical communication.

**Step 2.3** After confirming that Bob and Charlie have obtained the sequences, Alice announces the positions of \( s \) sample groups. Bob and Charlie measure their decoy photons randomly either in the \( Y \)-basis (i.e. \( \{+y = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), -y = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)\}) or

\[ X \)-basis (i.e. \( \{|+x = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), -x = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}), \]

then inform Alice of their measurement results. Then Alice detect the presence of eavesdroppers. He can compare the results of Bob and Charlie with his own and determine error rate. If the error rate is high, then they terminate this process. Otherwise, Alice acknowledges two agents and proceeds the scheme.

**Step 2.4** Alice performs the Bell measurement on \( i-th \) two-particle pairs \( \{P_i(1), P_i(4)\} \) for \( 1 \leq i \leq l + s \) and controls his measured information to the classical bit strings \( M_A = \{m_i^{n_1}, m_i^{n_2}, \ldots, m_i^{n_x}\} \). Alice encrypts \( M_A \) with \( k_{BA} \) and sends \( M_A^{*} = E_{k_{BA}}(M_A) \) to signatory Charlie directly. In addition, Alice uses \( H : \{0,1\} \rightarrow \{0,1\}^{2^n} \) to obtain \( H(m) \) and encrypts \( H(m) \) in accordance with \( K_{BA} \) and gets \( M = E_{k_{BA}}(H(m)) \). Then Alice transmits \( M \) to verifier Bob.

**Step 2.5** Charlie performs the Bell measurement on \( i-th \) two-particle pairs \( \{P_i(2), P_i(5)\} \) for \( 1 \leq i \leq l + s \) and converts his measured information to the classical bit strings \( M_C = \{m_i^{n_1}, m_i^{n_2}, \ldots, m_i^{n_x}\} \). Then Charlie utilizes key \( k_{CB} \) to encrypts \( M_C \) and \( M_A^{*} \)

\[ S_C = E_{k_{CB}}(M_C, M_A^{*}) \]

Then Charlie sends \( S_C \) to Bob.

### Verifying Phase

**Step 3.1** After having received \( S_C \), Bob decrypts \( S_C \) with \( k_{CB} \) to get \( M_A^{*} \) and then use \( k_{BA} \) to decrypt \( M_A^{*} \) to obtain \( M_A \).

**Step 3.2** Bob performs the Bell measurement on \( i-th \) two-particle pairs \( \{P_i(3), P_i(6)\} \) for
$1 \leq i_j \leq l+s$, $1 \leq j \leq l$ and transforms his measured result sequence to the classical bit strings $M_B = \left\{ m_i^{(1)} n_i^{(3)}, m_i^{(2)} n_i^{(3)}, \ldots, m_i^{(3)} n_i^{(3)} \right\} \left\{ m_j^{(1)} n_j^{(3)} \right\} \in \{00, 10, 01, 11\}, 1 \leq i_j \leq l+s, 1 \leq j \leq l$.

**Step 3.3** With announced Bell measurement outcomes $M_A, M_B$ and $M_C$, Bob can compute $(x, y, z)_{\text{M}_C}$ which is the subscript of $\left\{ \text{GHZ}_{\text{M}_C} \right\}_{456}$ in the $i_j$-th GHZ state group transferred from $\left\{ \text{GHZ}_{\text{M}_C} \right\}_{456}$ by using local unitary operators in Step 2.2. All the above outcome values satisfy the relationship $x = m_i^{(0)} + m_i^{(2)} + m_i^{(3)}$, $y = n_i^{(0)} + n_i^{(2)}$, $z = n_i^{(0)} + n_i^{(3)}$, where $m_i^{(0)} n_i^{(3)} \in \{00, 10, 01, 11\}$ represent the measurement results of parties Alice, Bob and Charlie, $1 \leq i_j \leq l+s$, $1 \leq j \leq l$ and $f \in \{1, 2, 3\}$. Bob obtains $m' = \left( (x, y, z)_{\text{M}_C}(x, y, z)_{\text{M}_C}, \ldots, (x, y, z)_{\text{M}_C} \right)$ and keeps going to use the same hash function $H$ to calculate the hash result of $H(m')$.

**Step 3.4** Bob decrypts $M = E_{k_B}(H(m))$ with $k_B$ to get $(H(m))$. If $H(m') = (H(m))$, thus we can conclude that Charlie’s signature is valid and the signature is correspond to the message. Otherwise, Bob does not recognize this signature.

### Analysis of the Proposed Scheme

#### Security Analysis

**Impossibility of Forgery.** First, both QKD protocol and a classical one-time pad algorithm applied in the proposed scheme can guarantee the nonforgeability. For dishonest agents or eavesdropper Eve, it is impossible for them to forge Charlie’s signature, because the signature $S_C$ is generated from the QKD protocol and GHZ entanglement swapping. If Alice wants a successful forgery Charlie’s signature, she not only needs to obtain the key $k_{CB}$ but also the Bell measurement $M_C$ of signatory Charlie. Since the key $k_{CB}$ is dispensed by an unconditionally secure QKD protocol, the probability of success is close to zero. Furthermore, inferring the Bell measurement $M_C$ is out of the question for Alice by his measurement results. The correlativity of the results after entanglement swapping will be destroyed if Alice replaces Charlie’s measurement results with the wrong one. What’s more, forging Alice’s message and corresponding signature is difficult for both Bob and Eve. When Alice and Charlie take advantage of Bell basis to measure their own two-particle pairs, the Bell measurement results of Bob is deterministic. Hence, if Alice does not approve the signed message, Charlie will check his outcomes to verify Bob’s signature and corresponding message. Thus, it is easier to see that it is more difficult for third-party attacker Eve’s forgery because he has fewer rights than other agents. Similarly, our scheme adds an extra verification step that Charlie himself cannot forge Alice’s initial message and signature for some benefits. If Charlie intends to forge Alice’s initial message successfully, he must access the key $k_{BA}$ to obtain $M_A$, which is impossible due to secure quantum QKD protocol. We can come to the conclusion that no one can forge Charlie’s signature as well as Alice’s message for his own benefits without being detected.

**Impossibility of Disavowal.** The secret key $k_{CB}$ is shared between Bob and Charlie. The secret key $k_{BA}$ is shared between Bob and Alice. The above keys are all distributed through the QKD protocols. Alice cannot deny his message since $M$ contains $k_{BA}$, which is a secret key stored by Alice and Bob. Charlie cannot disavow his signature since his $S$ contains $k_{CB}$, which is a secret key stored by Charlie and Bob. Similarly, Bob cannot disavow to acknowledge a valid signature because he has a secret key $k_{CB}$ stored by Charlie and Bob.

**Blindness.** In the presented scheme, since the message is encrypted by $K_{AB}$, the signer Charlie knows nothing about the message to be signed. Therefore, the proposed scheme meets the blindness requirement.
Efficiency Analysis

Several existing [20-23] solutions are compared with ours. According to [24], \( \eta = \frac{B_m}{Q(t) + B(t)} \), where \( B_m \) is the length of the signature message, \( Q \) and \( B \) are the number of quantum bits and the classical bits transmitted in the scheme respectively.

In the proposed scheme, we can see that only 2 GHZ states are required for signing each 3 bits in the message except a few checking particles. To be specific, in the initializing phase, Alice transfers \( 2(2l + 2pl) \) to Charlie and Bob totally, where \( p \) is the ratio of eavesdropping particles; in the signing phase, the number of bits transmitted among three parties is \( 8l \); the length of the signature message is \( 3l \). So \( \eta = \frac{B_m}{Q(t) + B(t)} = \frac{l}{4l + \frac{4}{3}pl} \). Calculated in the same way, in [20] [21] [22] and [23], the efficiency are \( \frac{l}{7l + 2pl} \), \( \frac{l}{9l + 4pl} \), \( \frac{l}{14l + 4pl} \) and \( \frac{l}{9l + 3pl} \), respectively. There are some other notations used in Table 2 which are defined as follows: \( l_c \) refers to the number of classical bits (quantum bits) in each transmitted step, \( C(Q) \) denotes a classical (quantum) one-time pad and \( |\phi \rangle _n \) refers to entangled \( n – qubit \) state. Table 2 compares the proposed scheme with the previous ones in terms of complexity and efficiency.

Conclusion

In this study, based on the theory of quantum entanglement swapping, we proposed a practical and efficient blind signature scheme. The proposed signature scheme has following advantages over other protocols. First of all, the proposed scheme operates GHZ state first before

| Comparative items                  | Ref.[20] | Ref.[21] | Ref.[22] | Ref.[23] | Our scheme |
|------------------------------------|----------|----------|----------|----------|------------|
| Signature ability                 |          |          |          |          |            |
| signature length                  | 1        | 1        | 1        | 1        | 3l         |
| Space complexity                  |          |          |          |          |            |
| key storage                       | 2l       | 5l       | 4l       | 3l       |            |
| Particle distribution              |          |          |          |          |            |
| transmission                      |          |          |          |          |            |
| quantity                         | 2(l + pl)| 4(l + pl)| 4(l + pl)| 3(l + pl)| 4(l + pl)  |
| Encryption algorithm              |          |          |          |          |            |
| quantity                         |          |          |          |          |            |
| algorithm                         | 2C       | 3C + 2Q  | 4C + 3Q  | C + 4Q   | 3C         |
| Entangled states                  |          |          |          |          |            |
| consumption                       |          |          |          |          |            |
| quantity for above               | (l + pl)| (l + pl)| (l + pl)| (l + pl)| (l + pl)  |
| signature length                  |          |          |          |          |            |
| Efficiency                        |          |          |          |          |            |
| signature efficiency              | \( \frac{l}{7l + 2pl} \) | \( \frac{l}{9l + 4pl} \) | \( \frac{l}{14l + 4pl} \) | \( \frac{l}{9l + 3pl} \) | \( \frac{l}{4l + \frac{4}{3}pl} \) |
| efficiency for \( P = \frac{1}{2} \) | 12.5%    | 9%       | 6.2%     | 9.5%     | 21.4%      |
applying it. Secondly, in order to complete blind signature and verification, only Bell measurements on new entangled particles are needed. Thirdly, only 2 GHZ states are required for signing each 3 bits in the message except a few checking particles. Besides, the proposed signature scheme possesses the features of non-forgery, non-disavowal and blindness.

Acknowledgement

This work was supported by the National Natural Science Foundation of China (61602291, 61802241, 11601302), China Postdoctoral Science Foundation (2018M633456), China Scholarship Council (201806875032) and Natural Science Basic Research Plan in Shaanxi Province of China (2019JQ-472).

References

[1] W. Diffie, M. Hellman, New directions in cryptography, J. IEEE Trans. Inf. Theory. 22 (1976) 644-654
[2] L.H. Gong, H.C. Song, C.S. He, Y. Liu, N. Zhou, A continuous variable quantum deterministic key distribution based on two-mode squeezed states, J. Phys. Scr. 89 (2014) 035101.
[3] J.J. Shi, R.H. Shi, X.Q. Peng, Y. Li, Y. Guo, Distributed quantum packet transmission in nonmaximally entangled relay system, J. Int. J. Th. Phys. 54 (2015) 1128-1141.
[4] N.R. Zhou, J.F. Li, Z.B. Yu, et al., New quantum dialogue protocol based on continuous-variable two-mode squeezed vacuum states. Quantum Inf. Process, J. 16 (2017) 4-16.
[5] D. Gottesman, I.L. Chuang, Quantum digital signature arXiv: quant-ph/0105032v2 (2001)
[6] G.H. Zeng, C.H. Keitel, Arbitrated quantum-signature scheme, J. Phys. Rev. A 65 (2002) 042312.
[7] T. Shang, K. Li, J. Liu, Measurement-Device Independency Analysis of Continuous-Variable Quantum Digital Signature, J. Entropy 20 (2018) 291.
[8] P. Grünwald, M. Aßmann, J. Heckötter, et al., Signatures of Quantum Coherences in Rydberg Excitons, J. Phys.rev.lett. 117 (2016) 133003.
[9] S. Safaei, D.A. Mazziotti, Quantum signature of exciton condensation, J. Phys. Rev. B 98 (2018) 045122.
[10] S. Yun, Z. H. Li, Y.M. Li, A dynamic multiparty quantum direct secret sharing based on generalized GHZ states, J. Quantum Inf Process. 17 (2018) 244.
[11] H. Zhang, X.B. An, C. H. Zhang, et al., High-efficiency quantum digital signature scheme for signing long messages, J. Quantum Inf Process. 18 (2019) 3.
[12] N. Lörch, E. Amitai, A. Nunnenkamp, et al., Genuine Quantum Signatures in Synchronization of Anharmonic Self-Oscillators, J. Phys. rev.lett. 117 (2016) 073601.
[13] H. Wu, L. Yong, Z.B. Yang, et al., Quantum signature for laser-driven correlated excitation of Rydberg atoms, J. Phys.Rev. A 95 (2017) 013842.
[14] P.Jason, M. Johansson, Quantum signatures of charge flipping vortices in the Bose-Hubbard trimer, J. Phys.Rev. E 94 (2016) 052215.
[15] X.J. Wen, X.M. Niu, L.P. Ji, Y. Tian, A weak blind signature scheme based on quantum cryptography, J.Opt. Commun 282 (2009) 666-669.
[16] M. Naseri, A weak blind signature based on quantum cryptography, J. Int. J. Phys. Sci 6 (2011)
[17] T.Y. Wang, Q.Y. Wen, Fair quantum blind signatures, J. Chin. Phys. B 19 (2010) 060307.

[18] L.B. He, L.S. Huang, W. Yang, R. Xu, Cryptanalysis of fair quantum blind signatures, J. Chin. Phys. B 21 (2012) 030306.

[19] X.R. Yin, W. P. Ma, W.Y. Liu, A blind quantum signature scheme with $\chi$-type entangled states, J. Int. J. Theor. Phys. 51 (2012) 455-461.

[20] M. M. Wang, X.B. Chen, Y. X. Yang, A blind quantum signature protocol using the GHZ states, J. Sci. China 56 (2013) 1636-1643.

[21] Y. Tian, H. Chen, G. Yan, et al., A proxy blind signature scheme based on quantum entanglement, J. Optical \& Quantum Elec. 45 (2013) 1297-1305.

[22] M.H. Zhang, H.F. Li, Weak blind quantum signature protocol based on entanglement swapping, J. Photonics Research, 3 (2015) 324.

[23] C. Zeng, J.Z. Zhang, S.C. Xie, A Quantum Proxy Blind Signature Scheme Based on Genuine Five-Qubit Entangled State, J. Int. J. Theor. Phys. 56 (2017) 1762-1770.

[24] J. Wang, Q.Zhang, C.J. Tang: Quantum signature scheme with single photons, J. Optoelectronic Lett. 2 (2006) 0209.