Computers, Materials & Continua CMC, vol.63, no.1, pp.301-313, 2020

An Efficient and Practical Quantum Blind Signature Protocol with Relaxed Security Model

Jun Zhang[1, *], Hao Xiao[2], Hongqun Zhai[1] and Xiaoli Meng[3]

Abstract: Blind signature has a wide range of applications in the fields of E-commerce and block-chain because it can effectively prevent the blind signer from getting the original message with its blindness. Owing to the potential unconditional security, quantum blind signature (QBS) is more advantageous than the classical ones. In this paper, an efficient and practical quantum blind signature scheme relaxed security model is presented, where quantum superposition, decoy qubits and hash function are used for the purpose of blindness. Compared with previous QBS scheme, the presented scheme is more efficient and practical with a relaxed security model, in which the signer's dishonest behavior can be detected other than being prevented as in other QBS schemes.

Keywords: Blind signature, quantum superposition, decoy qubit, hash function, relaxed security model.

1 Introduction

The blind signature (BS) was first proposed by Chaum [Chaum (1983)] in 1983. In a blind signature scheme, the receiver of the signature Bob, also can ask the signer Alice to sign a message without revealing the message m to the signer. There is a physical analogy of BS: The receiver of the signature can put his printed message in an envelope with copy ink and ask the signer to sign on the envelope. Hence the receiver can get the signature without revealing the message to the signer. The blind signature can effectively prevent the blind signer from getting the original message because of its blindness, so it has a wide range of applications in the fields of E-commerce and block-chain, such as untraceable payment [Chaum (1983); Kutubi, Alam, Tahsin et al. (2017)], anonymous secure e-voting [Lin, Hwang and Chang (2003)], secure cloud computing [Cheon, Jeong and Shin (2019); Zhu, Tan, Zhang et al. (2017)], etc. And all of these classical BS schemes are based on some unproven mathematical assumptions, such as RSA [Bellare, Namprempre, Pointcheval et al. (2003)], lattice [Tian, Zhang and Wei (2016)], Diffie-Hellman [Boldyreva (2003)], and so on.

However, with the development of quantum computers, Shor's algorithm would easily

[1] School of Information Engineering, Jiangsu Maritime Institute, Nanjing, 21100, China.

[2] School of Information Engineering, Huzhou University, Huzhou, 313000, China.

[3] Department of Electronic Engineering, Hartland Community College, Illinois, 60629, USA.

[*] Corresponding Author: Jun Zhang. Email: zhangjunjmi@163.com.

Received: 19 June 2019; Accepted: 18 July 2019.

break most of the classical digital signature schemes, whose security mainly depend upon the classical mathematical problems, such as the factorizations of large integer and the discrete logarithm problems [Shor (1994, 1997)]. Therefore, those classic solutions that rely on unproven mathematical assumptions face enormous challenges. And some researchers tried to utilize quantum mechanics theory to solve some classical tasks, such as quantum key distribution (QKD) [Bennett and Brassard (1984); Ekert (1991)], quantum key agreement [Chong and Hwang (2010); Huang, Su, Liu et al. (2017); Liu, Xu, Yang et al. (2018)], quantum secure direct communication [Liu, Chen, Li et al. (2008); Liu, Chen, Ma et al. (2009)], quantum private comparison [Liu, Liu, Wang et al. (2013, 2014); Liu, Liu, Chen et al. (2014); Liu, Liu, Liu et al. (2014)], quantum sealed-bid auction [Liu, Wang, Ji et al. (2014); Liu, Wang, Yuan et al. (2016)], quantum remote state preparation [Liu, Chen, Liu et al. (2015); Qu, Wu, Wang et al. (2017)], quantum steganography [Qu, Cheng and Wang (2019); Qu, Li, Xu et al. (2019)], delegating quantum computation [Liu, Chen, Ji et al. (2017)], quantum database query [Liu, Gao, Chen et al. (2019)], and even quantum machine learning [Liu, Gao, Yu et al. (2018), Liu, Gao, Wang et al. (2019)].

Especially, there are also many constructions of quantum BS scheme. A weak QBS is firstly presented in Wen et al. [Wen and Niu (2009)] based on EPR pairs. Here, weakness means that the signature is traceable. That is to say, once some disagreement happens, the signature can be traced back to the message owner with the help of a third party. In order to solve the problem, a QBS scheme based on two-state vector formalism is proposed [Qi and Zheng (2010)], however, it was crypt-analyzed and improved later [Yang and Tzonelih (2013)]. Since then, More QBS schemes are constantly being proposed, such as the quantum group BS scheme without entanglement [Xu and Huang (2011)], QBS based on χ-type 4-qubit entangled state [Yin and Ma (2012)]. A QBS scheme with unlinkability, which means the signature cannot be linked to the message owner, is presented [Shi and Zhang (2015)]. But later, the unlinkable QBS scheme was shown to be insecure [Luo and Shang (2017)]. Later, a QBS scheme based on quantum matrix encoding and QKD [Lai and Luo (2017)] is presented. As mentioned above, most of the existing schemes either sign and verify in a bitwise manner or make use of QKD.

In this paper, based on quantum superposition, decoy qubits, and hash function, we present a novel QBS with a relaxed security model. Compared with other QBS scheme, our scheme is more efficient and practical. The relaxed security is that the signer Alice may get the message with non-negligible probability. But if she measures and gets the message, then with high probability the receiver of the BS Bob can find out this dishonest activity and make a complaint or refuse to conduct business with the signer, as punishment.

The paper is organized as follows. The definitions of QBS and our relaxed security model are given in Section 2, and our efficient and practical QBS Scheme is proposed in Section 3. In Section 4, we analyze the security of our QBS scheme, and finally make the conclusion in Section 5.

2 Preliminaries

In this section, we firstly present some definitions and security properties of quantum blind signature.

2.1 Some definitions

Definition 1. *Blind signature (BS)*. There are two parties Alice (the signer) and Bob (message owner). After the BS protocol, Bob can get the signature of his message m from Alice. While Alice knows nothing about the content of the message m.

Definition 2. Security properties of BS.

1) *Blindness*. When signing, Alice cannot see the content of the message m sent from Bob.

2) *Unforgeable*. For one implementation of the BS protocol, Bob can only get one signature for a chosen message m. Bob cannot forge another signature for another message m'.

Definition 3. *Relaxed blindness*. Alice may be dishonest and try to read the content of the message m. Originally the blindness requires that Alice cannot do this. In our relaxed version, Alice can do this, but his dishonest behavior will be found by Bob with high probability.

2.2 Quantum superposition and Holevo bound

Quantum superposition is a well-known property of quantum mechanics. For example, a qubit can be $|0\rangle$ and $|1\rangle$ at the same time such as $1/\sqrt{2}\,(|0\rangle + |1\rangle)$.

While a qubit can possess 2 states simultaneously, n qubit string can possess 2^n states at any single moment. But if one use n qubit string to send the classical message, the Holevo bound says that at most n bit classical message can be transmitted. The upper limit of information that Alice can get from Bob is determined by the Holevo's limit,

$$H(A:B) \leq S(\rho) - \frac{1}{n}\sum_{i=0}^{n-1} S\big(\rho(i)\big). \quad (1)$$

Here $S(\rho)$ denotes the Von Neumann entropy of quantum state ρ, $H(A:B)$ means the information Alice can get from Bob.

3 The efficient and practical QBS scheme with relaxed security model

We firstly introduce the basic process of blind signature and verification, which is shown in Fig. 1. Suppose sender Bob want to obtain a blind signature of message m from the signer Alice. Bob first blinds the message m and then sends the blinded message m' to the signer Alice. Alice signs the blinded message and sends the signature $sign(m')$ back to Bob. After Bob gets the signature, he removes the blinding and announces the message m and signature $sign(m)$. The verifier Charlie verifies the validity of the message and its signature by querying Alice.

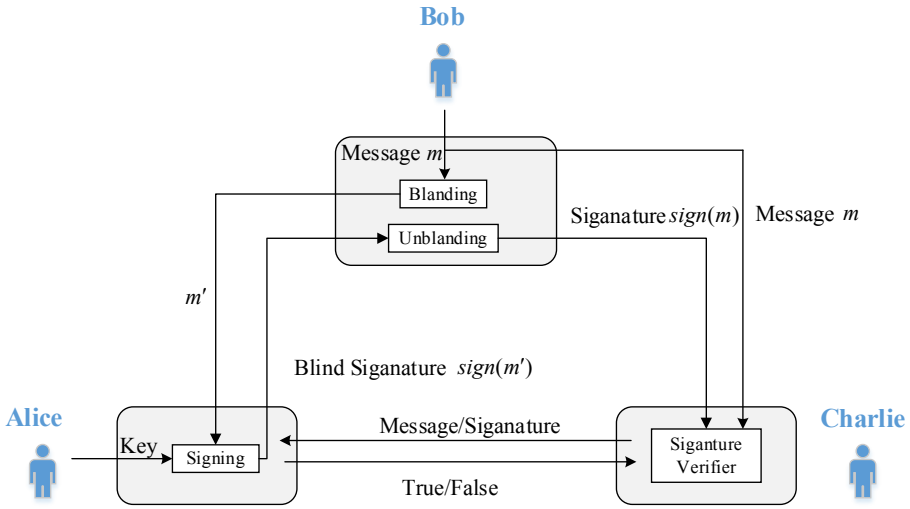

Figure 1: The whole process of blind signature and verification among signer Alice, message sender Bob and receiver Charlie

3.1 The basic QBS scheme

Bob prepares the quantum superposition state as follows:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|m\rangle + |\bar{m}\rangle), \tag{2}$$

where $\bar{m}$ means the bit-wise NOT of m, e.g., if $m = 101$ then $\bar{m} = 010$. Then Bob sends these qubits to Alice, and Alice use a quantum signing algorithm to sign the qubits to get (It is kind of like that Alice sign both m and $\bar{m}$ simultaneously):

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|m\rangle|sign(m)\rangle + |\bar{m}\rangle|sign(\bar{m})\rangle). \tag{3}$$

Alice then send $|\Phi\rangle$ to Bob. Bob measure it with the computational basis. He will get m or $\bar{m}$ with equal probability of $1/2$ and the corresponding signature.

The problem with this simple construction is that Alice could measure $|\psi\rangle$ and get m or $\bar{m}$ with equal probability of $1/2$, and then sign and send back to Bob. For example, if Alice measures $|\psi\rangle$ and gets m, she can sign it and gets:

$$|\Phi'\rangle = |m\rangle|sign(m)\rangle. \tag{4}$$

And send this $|\Phi'\rangle$ back to Bob. Bob then measure it and get the message m and signature $sign(m)$. And Bob cannot know that Alice has already measure the state $|\psi\rangle$ and get the message m. The whole process can be sketched with Fig. 2.

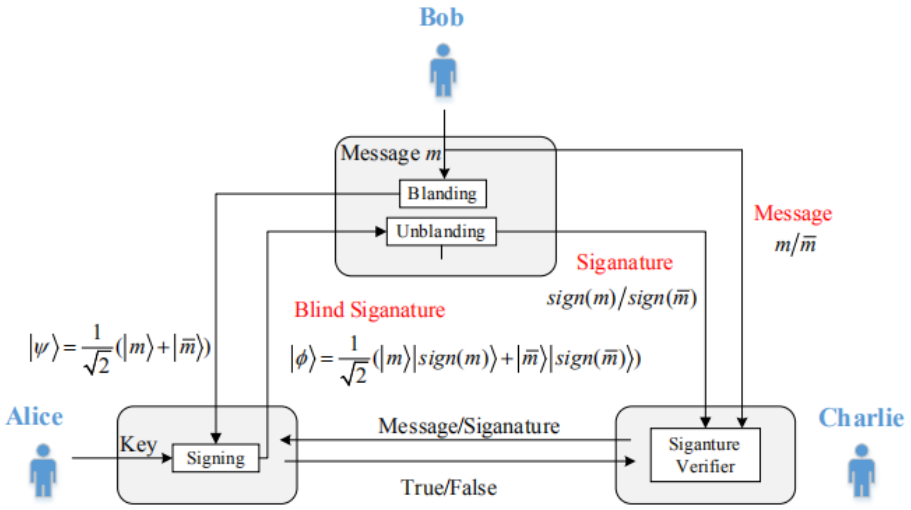

Figure 2: The process of basic QBS scheme with quantum superposition among Alice, Bob and Charlie

3.2 The QBS scheme with decoy qubits

In this subsection, we will make a little improvement on the quantum blind signature, and the detailed process can be shown in Fig. 3.

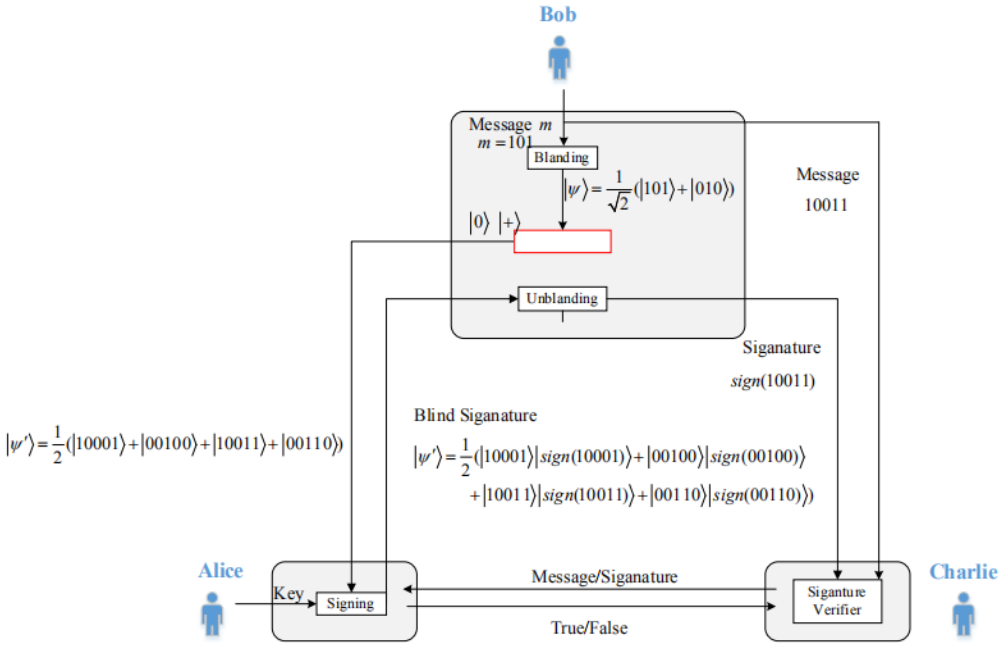

Figure 3: The process of basic QBS scheme with randomly inserted decoy qubits

To prevent the attack of Alice mentioned above, Bob could add some decoy qubits that are randomly chosen from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ to the state $|\psi\rangle$. As shown in Fig. 2, after Bob get the quantum signature from Alice, he can check the decoy qubit to ensure that Alice has not try to measure the message to steal the message. If Alice has measured the qubits, then Bob can find out this dishonesty with high probability.

Usually, the decoy qubits are inserted into the quantum message $|\psi\rangle$ at random positions, which are only known to Bob. But we should know that the signature finally got by Bob is a classical signature. And some positions of the message m (the decoy positions) should be interpreted as garbage and ignored when verifying. If these positions are random and only known to Bob, then there is a probability for Bob to reassign the decoy positions and interpret the signature of m to another message m'.

Let's give a simple example. Suppose Bob want to get a blind signature for message $m = 101$, then $\bar{m} = 010$. He randomly chose some positions and insert some decoy qubits. If he decide to insert a $|0\rangle$ at the second place and a $|+\rangle = 1/\sqrt{2}\,(|0\rangle + |1\rangle)$ at the third place, then:

$$|\psi\rangle = |101\rangle + |010\rangle, \tag{5}$$

$$|\psi'\rangle = |10001\rangle + |00100\rangle + |10011\rangle + |00110\rangle. \tag{6}$$

For clarity, we omit the overall normalized factor $1/\sqrt{2}$ for $|\psi\rangle$ and $|\psi'\rangle$. After Alice sign this message, Bob would get:

$$|\Phi\rangle = |10001\rangle|sign(10001)\rangle + |00100\rangle|sign(00100)\rangle + |10011\rangle|sign(10011)\rangle + |00110\rangle|sign(00110)\rangle. \tag{7}$$

Then Bob can measure the decoy qubits with the basis that is known to him. If he makes sure that Alice has not cheated, he can measure the whole state with the computational basis and he will get a random message of the four and the corresponding signature in the state $|\Phi\rangle$. Suppose he gets the state $|10011\rangle|sign(10011)\rangle$. Of course, this is a signature of Alice for message 10011. But Bob's original goal is to obtain a blind signature for 101. Well, Bob can declare that it is the first, third and fifth bits in 10011, i.e., 101, that are the message and the other two bits are just decoy bits and should be omitted.

But if Bob is dishonest, he can also declare that the first 3 bits 100 are the message and the later 2 bits are decoy bits and should be omitted. So, how should this kind of dishonest behavior of Bob be prevented?

3.3 The QBS scheme with decoy qubits and hash function

We can see that Bob can cheat like this is because the positions of the decoy qubits are random and only know to him. So if the positions are fixed, then Bob cannot cheat in this way. But of course, the positions cannot be totally fixed in every execution of the blind signature protocol with Alice, since Alice can somehow find out these positions (e.g., she sees a blind signature given by Bob). The idea is that the positions are determined by each message m, i.e., using $Hash(m)$ to specify the positions. So if m is known, the positions are fixed and Bob cannot cheat anymore.

How to insert the decoy according to the value $Hash(m)$? For example, if the output of

$Hash(m)$ is l-bit long, and we want to insert t decoy bits. We can use each block with l/t bits as the decoy positions, and insert the decoy qubit at these positions. The decoy qubit should be inserted one by one at the position specified by the ith l/t-bits long block. Maybe the value of a l/t-bits block exceeds the length of the current message (including the already inserted decoy qubits). The simple idea to solve this problem is to execute modulation operation over the total length of current message, and Fig. 4 gives the whole process of proposed QBS scheme with decoy qubits and hash function.

So intuitively, by using the hash function we can make sure that Bob cannot reinterpret the blind message he got to another message (See next subsection for detail).

3.4 Signature and verification

After the operations in Section 3.3, the final blind signature is $(\hat{m}, sign(\hat{m}),$ positions of m in $\hat{m}, \pm)$, where $+$ means the real message m bits are not flipped in $\hat{m}$, $-$ means flipped, and the Hash function, which is agreed beforehand such as Hash256 etc.

The real message is m, $\hat{m}$ is the message that some decoy bits has been inserted. To verify the signature, first check if the $(\hat{m}, sign(\hat{m}))$ pair are legitimate. Then compute $h(m)$ (m can be recovered from $\hat{m}$ and the specified positions and $\pm$), which should be interpreted as the positions that the decoy bits are.

Let's give a simple example. Suppose the blind signature is

$$(10001, sign(10001), (1st, 3th, 5th), +). \quad (8)$$

The first step is, of course, to verify $sign(10001)$ is legitimate or not. Based on the $+$ and the positions, we can recover the message should be 101. Then we should compute $Hash(101)$, if $Hash(101) = 1011$, which should be interpreted as the decoy positions should be at 2(10) and 3(11) to the original message 101, then we get 1*0*1, which match the $\hat{m} = 10001$. So the blind signature is legitimate.

If the blind signature is:

$$(00110, sign(00110), (1st, 3th, 5th), -). \quad (9)$$

First, we should verify $sign(00110)$. Then based on $-$ and positions we can recover $m = 101$ (the 1st, 3rd and 5th bits are 010, flip them to get 101). Then we can compute $Hash(m)$ and carry out verification just as above.

These two blind signatures can all appear if Bob's original message is $m = 101$.

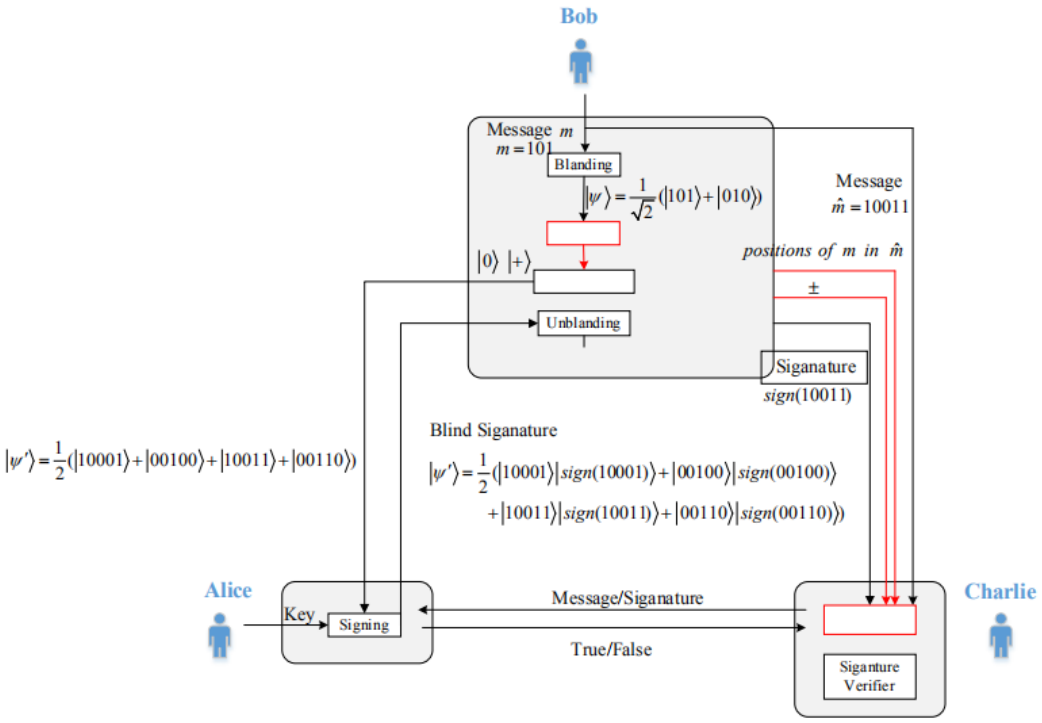

Figure 4: The process of QBS scheme with decoy qubits and hash function

4 Security and efficiency

4.1 Security analysis

In this section, we show that the QBS scheme above satisfies the security properties defined in Section 2, i.e., relaxed blindness and unforgeability.

1) Relaxed blindness

Alice cannot learn the message m without being detected by Bob, because of the decoy qubits.

If she tries to find out the message, she has to measure the state $|\psi'\rangle$. This measurement operation will destroy the state of the decoy qubits. Then Bob will detect this with high probability and find her cheating.

Of course, Alice may try to guess where are the message qubits and where are the decoy qubits. If she guess right, she can measure the message qubits only to avoid alter the decoy qubits, since all the message qubits are encoded in the computational basis $(|0\rangle, |1\rangle)$.

But Alice does not know the message m and $Hash(m)$, she can only guess the decoy qubits' positions rightly with negligible probability. So her successful probability is negligible.

2) Unforgeability

First the signature $sign(\hat{m})$ itself is unforgeable, of course, according to the security of the original signature scheme.

Another way of forging is that Bob may try to re-interpret the blind signature to another message m', instead of m.

For this cheating strategy to work, Bob has to fabricate the message m' and $Hash(m')$, with the restriction that m' added with decoy bits that are positioned by $Hash(m')$ should be the same with the original signed message (by Alice) $\hat{m}$.

The successful probability of this cheating behavior is negligible. Bob know $\hat{m}$, he can choose any bit of $\hat{m}$ at any position as the new message m0. But once m' is chosen, the decoy positions are also fixed, i.e., $Hash(m')$ is also fixed.

According to the collision-resistant property of the hash function, given a message m together with a fixed string h. The probability of $Hash(m) = h$ is, of course, negligible.

For the example given the BS in the previous section:

$$(10001, sign(10001), (1st, 4th, 5th), +), \tag{10}$$

which is the BS for message 101. Bob may try to re-interpret it as:

$$(10001, sign(10001), (3rd, 4th, 5th), +), \tag{11}$$

i.e., as the BS for message 001, then the decoy positions should be 1 and 2. This requires that $Hash(001) = 0110$. Of course, the successful probability is negligible in a practical setting.

But there are many ways Bob can choose the message m', namely $\binom{|\hat{m}|}{|m|}$ ways. So, the probability of forge could still be non-negligible.

To circumvent this, we ask Bob to submit $Hash(m)$ for signing instead of the original message m. Then later even if Bob can fabricate another m' as described above. Still based on the pre-image resistance security of the hash function, Bob can not find any meaningful message with the specified hash value. This is also very common in the classical signature scheme, where a hash value of the message is signed instead of the original message itself.

Another Bob's attack strategy is that Bob can choose another basis other than the computational basis to measure the quantum signature send back from Alice. Or he can manipulate the quantum signature first and then measure it to try to find more information. But as we mentioned above, by the well-known Holevo bound, whatever he can only get n bit information at most from n qubit quantum message. So, he cannot get more than one classical signature from the quantum message send back by Alice.

4.2 Comparison with other QBS schemes

Compared with other QBS schemes, our scheme is more efficient and practical. As shown in Tab. 1, we can see most other QBS scheme works in a bit-by-bit manner and for each bit of the message usually a pair of EPR entangled particles, or 4-bit χ-type entangled particles are required. While our QBS scheme, the message is signed as a whole, not in a bitwise manner, so there is no need to generate entangled particles for each bit.

In most other QBS schemes, the blind signature can only be verified once, mostly because the quantum particles can only be measured once. While our final blind signature is classical, and can be verified as many times as you want.

Table 1: Comparison among our scheme and other QBS schemes

QBS	Bitwise	Entanglement	Verification Times	Designated Verifier	QKD
[Wen and Niu (2009)]	Yes	EPR	Once	Yes	Yes
[Yin and Ma (2012)]	Yes	4-bit χ-type	Once	Yes	Yes
[Shi and Zhang (2015)]	Yes	EPR	Once	Yes	Yes
[Lai and Luo (2017)]	NO	NO	Once	Yes	Yes
Ours	NO	NO	Multiple Times	NO	NO

Also in other QBS schemes, QKD is often used for sharing private one-time pad keys between parties, while in our scheme no such QKD operation is required. The QBS in [Lai and Luo (2017)] also is not worked in a bit-by-bit manner and also make no use of entanglement, but it stil has a designated verifier and can be verified only once and make use of QKD.

5 Conclusion

A novel quantum blind signature scheme is presented. In this scheme, quantum superposition and decoy qubits are used for blindness purpose. To be specific, if the signer Alice is dishonest and try to see the message in the qubits, then with high probability this will be found by Bob (the receiver of the BS), and then Bob can refuse to conduct any more business with Alice as punishment.

Compared with existing QBS scheme, our QBS scheme has some unique characteristics. The final blind signature is classical, thus can be verified many times. While many other QBS scheme can only be verified once. Also, our QBS scheme is not signed or verified in a bitwise manner and make no use of QKD, so can be more efficient compared with those bitwise and QKD-based QBS scheme.

Our QBS scheme is a combination of classical signature with quantum cryptography, and quantum superposition and decoy qubits are used mainly for blindness purpose. One shortcoming of our scheme is that the blindness property is relaxed to cheat-sensitiveness, not total blindness, and the security still rely on the classical signature scheme, i.e., not totally quantum and unconditional. These could be our future research direction for improvement.

Acknowledgment: The authors would like to thank the anonymous reviewers and editor for their comments that improved the quality of this paper. This work was supported by 2018 Provincial Key Research and Development Program (Social Development) Project of Jiangsu Province (No. BF2018719), and 2018 Provincial Key Research and Development Program (Modern Agriculture) Project of Jiangsu Province (No. 2018301).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report

regarding the present study.

References

Bellare, M.; Namprempre, C.; Pointcheval, D.; Semanko, M. (2003): The one-more-RSA-inversion problems and the security of Chaum's blind signature scheme. *Journal of Cryptology*, vol. 16, no. 3, pp. 185-215.

Bennett, C. H.; Brassard, G. (1984): Quantum cryptography: public key distribution and coin tossing. *International Conference on Computers, Systems & Signal Processing*, pp. 175-179.

Boldyreva, A. (2003): Threshold signatures, multisignatures and blind signatures based on the Gap-Diffie-Hellman-group signature scheme. *Public Key Cryptography*, pp. 31-46.

Chaum, D. (1983): Blind signatures for untraceable payments. *Advances in Cryptology*, pp. 199-203.

Cheon, J. H.; Jeong, J.; Shin, J. S. (2019): Cryptoanalysis on 'a round-optimal lattice-based blind signature scheme for cloud services'. *Future Generation Computer Systems-the International Journal of Escience*, vol. 95, pp. 100-103.

Chong, S. K.; Hwang, T. (2010): Quantum key agreement protocol based on BB84. *Optics Communications*, vol. 283, no. 6, pp. 1192-1195.

Ekert, A. K. (1991): Quantum cryptography based on Bell's theorem. *Physical Review Letters*, vol. 67, no. 6, pp. 661.

Huang, W.; Su, Q.; Liu, B.; He, Y. H.; Fan, F. et al. (2017): Efficient multiparty quantum key agreement with collective detection. *Scientific Reports*, vol. 7, no. 1, pp. 15264.

Kutubi, M. A. A.; Alam, K. M. R.; Tahsin, R.; Ali, G.; Chong, P. H. J. et al. (2017): An offline electronic payment system based on an untraceable blind signature scheme. *Ksii Transactions on Internet and Information Systems*, vol. 11, no. 5, pp. 2628-2645.

Lai, H.; Luo, M.; Pieprzyk, J.; Qu, Z.; Li, S. et al. (2017): An efficient quantum blind digital signature scheme. *Science China Information Sciences*, vol. 60, no. 8, 082501.

Lin, I. C.; Hwang, M. S.; Chang, C. C. (2003): Security enhancement for anonymous secure e-voting over a network. *Computer Standards & Interfaces*, vol. 25, no. 2, pp. 131-139.

Liu, W.; Chen, H.; Li, Z.; Liu, Z.; Xiao, F. (2008): Efficient quantum secure direct communication with authentication. *Chinese Physics Letters*, vol. 25, no. 7, pp. 2354-2357.

Liu, W.; Chen, H.; Ma, T.; Li, Z.; Liu, Z. et al. (2009): An efficient deterministic secure quantum communication scheme based on cluster states and identity authentication. *Chinese Physics B*, vol. 18, no. 10, pp. 4105-4109.

Liu, W.; Liu, C.; Wang, H.; Jia, T. (2013): Quantum private comparison: a review. *IETE Technical Review*, vol. 30, no. 5, pp. 439-445.

Liu, W.; Liu, C.; Chen, H.; Liu, Z.; Yuan, M. et al. (2014): Improvement on "an efficient protocol for the quantum private comparison of equality with W state". *International Journal of Quantum Information*, vol. 12, no. 1, pp. 1804-1813.

Liu, W.; Liu, C.; Liu, Z.; Liu, J.; Geng, H. (2014): Same initial states attack in Yang et al.'s quantum private comparison protocol and the improvement. *International Journal of Theoretical Physics*, vol. 53, no. 1, pp. 271-276.

Liu, W.; Liu, C.; Wang, H.; Liu, J.; Wang, F. et al. (2014): Secure quantum private comparison of equality based on asymmetric W state. *International Journal of Theoretical Physics*, vol. 53, no. 6, pp. 1804-1813.

Liu, W.; Wang, F.; Ji, S.; Qu, Z.; Wang, X. (2014): Attacks and improvement of quantum sealed-bid auction with EPR pairs. *Communications in Theoretical Physics*, vol. 61, no. 6, pp. 686-690.

Liu, W.; Chen, Z.; Liu, C.; Zheng, Y. (2015): Improved deterministic n-to-one joint remote preparation of an arbitrary qubit via EPR pairs. *International Journal of Theoretical Physics*, vol. 54, no. 2, pp. 472-483.

Liu, W.; Wang, H.; Yuan, G.; Xu, Y.; Chen, Z. et al. (2016): Multiparty quantum sealed-bid auction using single photons as message carrier. *Quantum Information Processing*, vol. 15, no. 2, pp. 869-879.

Liu, W.; Chen, Z.; Ji, S.; Wang, H.; Zhang, J. (2017): Multi-party semi-quantum key agreement with delegating quantum computation. *International Journal of Theoretical Physics*, vol. 56, no. 10, pp. 3164-3174.

Liu, W.; Xu, Y.; Yang, C. N.; Gao, P.; Yu, W. (2018): An efficient and secure arbitrary N-party quantum key agreement protocol using Bell states. *International Journal of Theoretical Physics*, vol. 57, no. 1, pp. 195-207.

Liu, W.; Gao, P.; Yu, W.; Qu, Z.; Yang, C. N. (2018): Quantum relief algorithm. *Quantum Information Processing*, vol. 17, no. 10, pp. 280.

Liu, W.; Gao, P.; Liu, Z.; Chen, H.; Zhang, M. (2019): A quantum-based database query scheme for privacy preservation in cloud environment. *Security and Communication Networks*, vol. 2019, no. 14, pp. 4923590.

Liu, W.; Gao, P.; Wang, Y.; Yu, W.; Zhang, M. (2019): A unitary weights based one-iteration quantum perceptron algorithm for non-ideal training sets. *IEEE Access*, vol. 7, pp. 36854-36865.

Luo, Y. P.; Tsai, S. L.; Hwang, T.; Kao, S. H. (2017): On "a new quantum blind signature with unlinkability". *Quantum Information Processing*, vol. 16, no. 4, pp. 87.

Qi, S.; Zheng, H.; Qiaoyan, W.; Wenmin, L. (2010): Quantum blind signature based on two-state vector formalism. *Optics Communications*, vol. 283, no. 21, pp. 4408-4410.

Qu, Z.; Wu, S.; Wang, M.; Sun, L.; Wang, X. (2017): Effect of quantum noise on deterministic remote state preparation of an arbitrary two-particle state via various quantum entangled channels. *Quantum Information Processing*, vol. 16, no. 12, pp. 306.

Qu, Z.; Cheng, Z.; Wang, X. (2019): Matrix coding-based quantum image steganography algorithm. *IEEE Access*, vol. 7, pp. 35684-35698.

Qu, Z.; Li, Z.; Xu, G.; Wu, S.; Wang, X. (2019): Quantum image steganography protocol based on quantum image expansion and grover search algorithm. *IEEE Access*, vol. 7, pp. 50849-50857.

Shi, W. M.; Zhang, J. B.; Zhou, Y. H.; Yang, Y. G. (2015): A new quantum blind signature with unlinkability. *Quantum Information Processing*, vol. 14, no. 8, pp. 3019-3030.

Shor, P. W. (1994): Algorithms for quantum computation: discrete logarithms and factoring. *35th Annual Symposium on Foundations of Computer Science*, pp. 124-134.

Shor, P. W. (1997): Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *Siam Journal on Computing*, vol. 26, no. 5, pp. 1484-1509.

Tian, H. B.; Zhang, F. G.; Wei, B. D. (2016): A lattice-based partially blind signature. *Security and Communication Networks*, vol. 9, no. 12, pp. 1820-1828.

Wen, X.; Niu, X.; Ji, L.; Tian, Y. (2009): A weak blind signature scheme based on quantum cryptography. *Optics Communications*, vol. 282, no. 4, pp. 666-669.

Xu, R.; Huang, L.; Yang, W.; He, L. (2011): Quantum group blind signature scheme without entanglement. *Optics Communications*, vol. 284, no. 14, pp. 3654-3658.

Yang, C. W.; Hwang, T.; Luo, Y. P. (2013): Enhancement on "quantum blind signature based on two-state vector formalism". *Quantum Information Processing*, vol. 12, no. 1, pp. 109-117.

Yin, X. R.; Ma, W. P.; Liu, W. Y. (2012): A blind quantum signature scheme with χ-type entangled states. *International Journal of Theoretical Physics*, vol. 51, no. 2, pp. 455-461.

Zhu, H. F.; Tan, Y. A.; Zhang, X. S.; Zhu, L. H.; Zhang, C. Y. et al. (2017): A round-optimal lattice-based blind signature scheme for cloud services. *Future Generation Computer Systems- International Journal of Escience*, vol. 73, pp. 106-114.