Quantum Information Processing (2019) 18:3
https://doi.org/10.1007/s11128-018-2116-2

High-efficiency quantum digital signature scheme for signing long messages

Hao Zhang[1,2,3] · Xue-Bi An[4,5] · Chun-Hui Zhang[1,2,3] · Chun-Mei Zhang[1,2,3,4] · Qin Wang[1,2,3,4]

Received: 30 May 2018 / Accepted: 8 November 2018

Abstract
Quantum digital signature (QDS) is based on the laws of quantum physics, and can provide unconditional security for signing messages between remote multi-party users. To date, different QDS protocols have been proposed and corresponding security analysis has been done. Just most security analyses are directed against signing single-bit messages, and the security cannot be ensured when signing multi-bit messages if one simply puts blocks together. Recently, T.Y. Wang et al. analyzed the security under this situation and gave a solution for eliminating potential eavesdropping attacks. However, its efficiency is relatively low since they need to consume more than $2n$-bit signatures to sign a classical n-bit message. In this paper, we propose a high efficient approach for signing multi-bit messages. As a result, the efficiency can be improved with 36.92% when signing a 128-bit message compared with using T.Y. Wang et al.'s method. And the improvement is even larger when signing longer messages.

Keywords Quantum digital signature · Multi-bit messages · High efficiency

✉ Qin Wang
qinw@njupt.edu.cn

[1] Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China

[2] Broadband Wireless Communication and Sensor Network Technology, Key Lab of Ministry of Education, NUPT, Nanjing 210003, China

[3] Telecommunication and Networks, National Engineering Research Center, NUPT, Nanjing 210003, China

[4] Key Laboratory of Quantum Information, CAS, University of Science and Technology of China, Hefei 230026, China

[5] State Key Laboratory of Cryptology, P. O. Box 5159, Beijing 100878, China

Published online: 16 November 2018

1 Introduction

Quantum digital signature (QDS) guarantees the information-theoretic security of a signed message, including nonrepudiation, unforgeability as well as transferability. Since the original QDS protocol [1] was proposed by Gottesman and Chuang, a lot of researches trying to make QDS practical have been going on. With the development of quantum technology, some QDS protocols [2–7] can be implemented on QKD systems [8–20]. According to equalities (13)–(15) in [5], the security of signing a single-bit message will increase exponentially as the length of a signature grows linearly. Although the original QDS protocol is unconditionally secure against the most general coherent attacks for single-bit messages, it will be unsafe if we iterate the building block directly for signing multi-bit messages [21]. If Alice directly signs a multi-bit message without any preprocessing, a dishonest participant may tamper with the message-signature pair on the semantic and make the new message-signature pair valid. For example, Alice sends a message-signature pair (Don't pay Bob 100$ Sig(Don't) Sig(pay) Sig(Bob) Sig(100$)) to Bob. When Bob receives it, he changes the pair into (pay Bob 100$, Sig(pay) Sig(Bob), then sends to Charlie. Obviously, it is also valid. If Charlie accepts it, it means that Bob successfully forged a message.

T.Y. Wang et al. pointed out the problem and proposed a method to eliminate its insecurity from the naive way of iteration for signing multi-bit messages [21]. Briefly speaking, all labels of signatures are predetermined and put into a sequence, and then the message to be signed is encoded into a new sequence which is triple than the original one. Afterwards, they improved their scheme [22], which, however, still needs more than twice the number of bits for signing multi-bits classical messages. It means that half of the efficiency will be sacrificed to guarantee the security of long messages with QDS.

Here, we present a more efficient proposal to solve the problem of insecurity arising from signing long messages via QDS. Our scheme provides a method to calculate the minimum number of signature blocks for a message of a given size. The paper is arranged as follows: In Sect. 2, we describe the proposal, analyze the security as well as summarize some formulas for calculating. In Sect. 3, we compare it with the previous scheme, and then the results and discussions are expounded. Finally, summaries are given in Sect. 4.

2 A more efficient proposal

In this section, we outline our efficient proposal among three parties, a signer named Alice, and two receivers named Bob and Charlie, for signing multi-bit messages at the same security level of a single-bit message. For instance, three probabilities are all less than 10^{-4} while signing each bit, namely the probability of successfully forging $\mathbb{P}_{\text{forge}}$, the probability of successfully repudiation $\mathbb{P}_{\text{repudiation}}$, and the probability of an honest abort, $\mathbb{P}_{\text{abort}}$. More parties are possible, but special care should be taken to address colluding adversaries [7,8].

Our proposal has two stages, a distribution stage, which is exactly the same as previous protocols, and a messaging stage, where the participants use their keys generated from the previous stage to sign messages in a different way.

2.1 Distribution stage

Before describing the process of distribution stage, we first introduce the key generation protocol (KGP). Essentially, two parties, for instance, Alice an Bob, perform the quantum part of QKD to generate raw keys, but do not proceed to error correction or privacy amplification. This means that Alice and Bob will generate different (but correlated) strings that are not entirely secret [5]. Then, Alice–Bob and Alice–Charlie individually use the KGP to generate two different keys of length L for each possible message bit $m_i = 0_i$ or 1_i, $i = 1, 2, \ldots, n$, where n means the length of a classical message in binary for future signature. So, Alice has four different keys, $A^B_{0_i}$, $A^B_{1_i}$, $A^C_{0_i}$, $A^C_{1_i}$, for each i, the length of total keys in Alice's hands is $4nL$. Bob and Charlie each has $2nL$ length of keys, $K^B_{0_i}$, $K^B_{1_i}$ held by Bob and $K^C_{0_i}$, $K^C_{1_i}$, held by Charlie, separately. All of these keys are labeled and sequential. Then, Bob and Charlie exchange half of their keys (as well as the corresponding positions) via secret classical channel (for example, QKD) symmetrically.

2.2 Messaging stage

As stated in [22], Alice encodes a classical message $M = m_1||m_2||\cdots||m_n, m_i \in \{0, 1\}, i = 1, 2, \ldots, n$, into $\hat{M}$ using a specific coding rule. We use a simple formula to express it as follows:

$$\hat{M} = 1_1||1_2||0||m_1||0||m_2||0||m_3||\cdots||0||m_n||1_1||1_2, \tag{1}$$

where n is the length of a classical message in binary, mentioned above, and the double bar $||$ denotes the concatenation between bits. Therefore, the length of $\hat{M}$ can be calculated, and equal to $2n + 4$. Then, she signs $\hat{M}$ with corresponding keys.

In our proposal, the message M will be encoded into

$$\begin{aligned} \tilde{M} &= 1_1||1_2||\cdots||1_{x+1}||0||m_1||m_2||\cdots||m_x||0|| \\ &\qquad ||m_{x+1}||m_{x+2}||\cdots||m_{2x}||0|| \\ &\qquad \cdots \\ &\qquad ||m_{\lfloor \frac{n}{x} \rfloor x+1}||m_{\lfloor \frac{n}{x} \rfloor x+2}||\cdots||m_n||0||1_1||1_2||\cdots||1_{x+1}, \end{aligned} \tag{2}$$

where x refers to the coding interval, i.e., the encoder inserts a bit “0” for every x-bits in the original sequence, and $\lfloor\cdot\rfloor$ means round down function. Here, the coding rule is that the encoder replenishes a ‘0’ in the head of M, and another in the tail. Then, the encoder inserts a ‘0’ every x bits. Besides, the encoder adds ‘1’ with a number of $x + 1$ to both the start and the end. Here, we denote the length of $\tilde{M}$ by h, and we will give a formula to calculate it later. Below are the steps of message stage in our scheme.

1. Alice checks whether her keys are enough to sign $\tilde{M}$ bits. If not, she requests an execution of the distribution stage. Otherwise, she encodes M into $\tilde{M}$ using the rule above.
2. Then, she chooses corresponding signatures from $\{A^B_{0_i}, A^B_{1_i}, A^C_{0_i}, A^C_{1_i}\}$ to form $\mathrm{Sig}(\tilde{M})$ for signing $\tilde{M}$. She sends the message-signature pair $(M, \mathrm{Sig}(\tilde{M}))$ to the desired recipient (say Bob).

$$\mathrm{Sig}(\tilde{M}) = \mathrm{Sig}(\tilde{m}_1)||\mathrm{Sig}(\tilde{m}_2)||\cdots||\mathrm{Sig}(\tilde{m}_h) \tag{3}$$

   It should be noted that each signature block is labeled and the whole is sequential. Also, the opposite keys which are not used in $\mathrm{Sig}(\tilde{M})$ should be destroyed when Alice sent the pair out. For example, if Alice used $A^B_{0_i}, A^C_{0_i}$ to sign a "0_i", $A^B_{1_i}, A^C_{1_i}$ should be abandoned too.
3. Bob transforms the message M into $\tilde{M}$ making use of the same rule when he receives the pair. Then, he separately checks every bit-signature pair $(\tilde{m}_i, \mathrm{Sig}(\tilde{m}_i))$ using the parts of his keys received directly from Alice and symmetrically from Charlie. If every bit-signature is fewer than $s_a(L/2)$ mismatches in both halves of the key, where $s_a < 1/2$ is a small threshold determined by the parameters and the desire security level of the protocol, then Bob accepts the message. And he will forward the message-signature pair that he received from Alice to Charlie. But he may be not forward it immediately. And that is allowed.
4. Charlie tests for mismatches in the same way, but using a different threshold in order to prevent from repudiation by Alice. If the number of mismatches in both halves of his key is below $s_v(L/2)$, Charlie will accept the bit-signature, where s_v is another threshold, with $0 < s_a < s_v < 1/2$. If all bit-signature pairs pass and are sequential, then Charlie accepts the message. Otherwise, Charlie rejects it, and claims to abort the protocol this time.

In step (2), Alice sends the message-signature pair $(M, \mathrm{Sig}(\tilde{M}))$ to Bob rather than $(\tilde{M}, \mathrm{Sig}(\tilde{M}))$. The purposes of that are all participants follow the same coding rule but don't need another decoding rule and reduce classical communication.

2.3 Security analysis

The security of signing a single-bit message has been proven in [2–5]. During distribution stage, the labels of all keys for each message bit are predetermined and sequential. So, all bit-signature pairs in each message-signature pair are in sequence.

Proposition An opponent Eve cannot forge a legal message-signature pair from arbitrary number of pairs which were sent from the signer and under the following three conditions:

1. Only the start and the end own the special codeword $1_1||1_2||\cdots||1_{x+1}$;
2. All bit-signature pairs in this message-signature pair are sequential;
3. Each bit-signature pair must pass the verification.

Before proving the proposition formally, we first list three necessary preliminaries:

Lemma 1 *Suppose that* $C = c_1||c_2||\cdots||c_t$*,* $c_i \in \{0||m_1||m_2||\cdots||m_x\}$*,* $m_j \in \{0,1\}$*,* $i = 1,2,\ldots,t$*,* $j = 1,2\ldots,x$*,* $t \geq 1$*,* $x \geq 1$*, is a bit sequence, then* $1_1||1_2||\cdots||1_{x+1} \notin C$*.*

Lemma 2 *Suppose that* $C = 1_1||1_2||\cdots||1_{x+1}||c_1||c_2||\cdots||c_t||1_1||1_2||\cdots||1_{x+1}$*,* $c_i \in \{0||m_1||m_2||\cdots||m_x\}$*,* $m_j \in \{0,1\}$*,* $i = 1,2,\ldots,t$*,* $j = 1,2\ldots,x$*,* $t \geq 1$*,* $x \geq 1$*, is a bit sequence, then it is impossible to find a sequence* $C' = 1_1||1_2||\cdots||1_{x+1}||c'_1||c'_2||\cdots||c'_k||1_1||1_2||\cdots||1_{x+1}$ *with* $c'_i \in \{0||m_1||m_2||\cdots||m_x\}$*,* $m_j \in \{0,1\}$*,* $i = 1,2,\ldots,k$*,* $j = 1,2\ldots,x$ *such that* $C' \subsetneqq C$*. Note that here all* c'_i *in* C' *are in sequence.*

Lemma 3 *Suppose that* $C_f = 1_1^f||1_2^f||\cdots||1_{x+1}^f||c_1^f||c_2^f||\cdots||c_{t_f}^f||1_1^f||1_2^f||\cdots||1_{x+1}^f$*,* $c_i^f \in \{0||m_1||m_2||\cdots||m_x\}$*,* $i = 1,2,\ldots,t_f$*,* $j = 1,2\ldots,x$*,* $f = 1,2,\ldots,l$*,* $t_f \geq 1, x \geq 1, l \geq 1$*, it is impossible to find a sequence* $C' = 1_1||1_2||\cdots||1_{x+1}||c'_1||c'_2||\cdots||c'_{t'}||1_1||1_2||\cdots||1_{x+1}$ *with* $c'_i \in \{0||m_1||m_2||\cdots||m_x\}$*,* $m_j \in \{0,1\}$*,* $i = 1,2,\ldots,t'$*,* $j = 1,2\ldots,x$ *such that* $C' \subseteq C_1||C_2||\cdots||C_l$ *except* $C' = C_f$*,* $f = 1,2,\ldots,l$*.*

Three similar lemmas have been proven in [22], and here we extend them to the scenario that the length of codewords is $x+1$. The methods utilized to prove these three lemmas are classification discussion and mathematical induction. In our extended lemmas, the definition domain of c_i is extended to $c_i \in \{0||m_1||m_2||\cdots||m_x\}, m_j \in \{0,1\}$, $j = 1,2\ldots,x$. Compared with $c_i \in \{00,01\}$, it is conspicuous that the difference between two domains is in that $m_1||m_2||\cdots||m_x$ instead of 0 or 1. According to the substitution method, these three extended lemmas are also valid.

Next, we will prove the proposition presented above.

Proof Every message sent from the signer has two special codewords $1_1||1_2||\cdots||1_{x+1}$ at the head and tail separately, and all of the signature keys are labeled and sequential. In our coding rule, encoders insert a 0 every x bits. Now, we suppose Eve can forge a legal message $\tilde{M}'$ from one or several legal messages $\tilde{M}_1, \tilde{M}_2, \ldots, \tilde{M}_f$, $f \geq 1$ which the signer sent to him.

1. According to Lemma 1, Eve cannot find continuous $1_1||1_2||\cdots||1_{x+1}$ in the encoded message $\tilde{M}$ except at the start or the end.
2. Eve cannot forge any bit-signature, which has been proven previously. And all bit-signature pairs are in sequence, so Eve has no way to change their relative position. That is the meaning what Lemma 2 points out. Therefore, Eve can only reproduce $\tilde{M}' = \tilde{M}$.
3. The above two conclusions manifest that it is impossible for Eve to forge a legal message and corresponding signature from one signed message-signature pair. Besides, as indicated in Lemma 3, Eve cannot forge a legal message-signature pair from multi-pairs. If Eve tries to recombine two or more pairs without changing any pairs, the special codeword $1_1||1_2||\cdots||1_{x+1}$ will prevent Eve from making a success. It results in that Eve makes another identical $\tilde{M}_f$.

To sum up, Eve can only reproduce exactly the same message sent from the signer. In other words, Eve is unable to forge a legal message. With these, the proposition has been proven, and so is the security of our general proposal for signing long messages. □

2.4 Calculation methods

In this part, a formula is presented to calculate the minimum length of a message actually signed which the original message is coded into, and we define the efficiency of QDS for signing long messages.

As shown in (1), the coded message contains three parts, the original message, the inserted '0' and the added '1'. So a 'n' bits message is encoded into a 'h' bits message:

$$h = n + \lfloor \frac{n}{x} \rfloor + 2x + 4, \tag{4}$$

where x is the coding interval and $1 \leq x \leq n,\ \ x \in Z_+$. Z_+ means the set of positive integers. Every possible x represents a specific scheme. The efficiency is defined as

$$\eta = \frac{n}{h}. \tag{5}$$

Obviously, η approaches the maximum as h tends to be minimum. Therefore, we can optimize x to get the minimal h, and then obtain the maximal η in the case where n is given. If n is changed, it will cause the optimal value of x, but it doesn't matter with the optimization method.

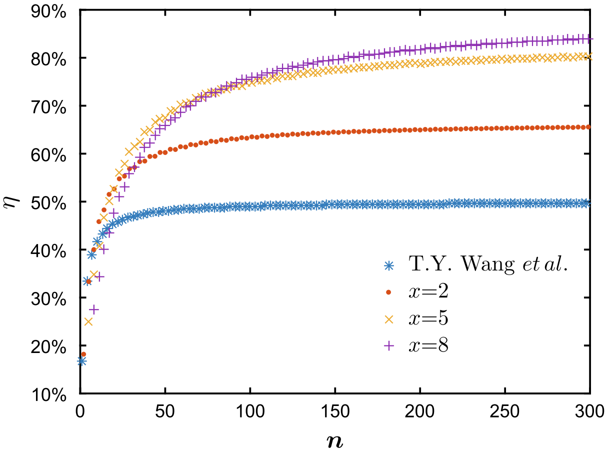

Fig. 1 Comparisons of signature efficiency among four different schemes. x means the coding interval, and different x represents different scheme. η means the efficiency of signing a message with n bits

Table 1 Comparisons of signing 128-bits message. x means the coding interval, and different x represents different scheme. η means the efficiency of signing a message with n bits

n = 128 bits				
x	$\lvert\hat{M}\rvert_h$	$\lvert\tilde{M}\rvert_h$	η (%)	$\Delta\eta$ (%)
2	260	200	64.00	23.08
5	260	167	76.65	35.77
7, 8, 9, 10	260	164	78.05	36.92
11	260	165	77.58	36.54

$\lvert\hat{M}\rvert_h$ represents the value derived from the new scheme of T.Y. Wang et al. [22]. $\lvert\tilde{M}\rvert_h$ means the value which is derived from our proposal. $\Delta\eta$ is the improved efficiency over T.Y. Wang et al.'s scheme

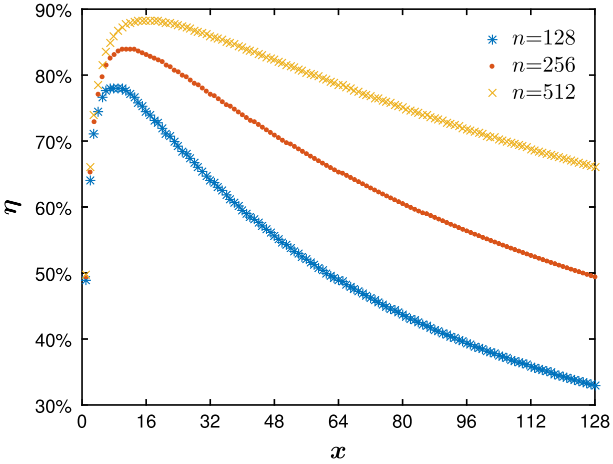

Fig. 2 Comparisons of signature efficiency among different sizes of messages. x means the coding interval, and different x represents different scheme. η means the efficiency of signing a message with n bits

3 Results of improvement

For signing a 'n' bits message, at least $2n + 4$ bits are needed to be signed in the previous scheme, and hence the efficiency can be expressed as $n/(2n+4)$. Compared to the previous scheme, our proposal has $\Delta\eta$ efficiency improved,

$$\Delta\eta = \frac{n/h - n/(2n+4)}{n/(2n+4)} = 1 - \frac{h}{2n+4}. \tag{6}$$

We compared the efficiency of our present work with T.Y. Wang et al.'s work [22], and corresponding simulation results are shown in Fig. 1. Actually, T.Y. Wang et al.'s work is a just special case of our new proposal which corresponds to the case when x = 1. In order to make a vivid comparison, here we choose three different values of x and compare their efficiency with using T.Y. Wang et al.'s work. We can see from Fig. 1 that our new scheme can exhibit dramatically improved performance than T.Y. Wang et al.'s. Moreover, in order to display the detailed information, we list out the signature efficiency for different x when signing a 128-bit message, see Table 1. We find from

Table 1 that the signature efficiency is not a monotonously increasing function of x. Furthermore, we plot out the variation of the signature efficiency with the value of x by fixing the message length at 128 bits, 256 bits and 512 bits, respectively, as shown in Fig. 2. One can always find out an optimal value of x with the highest efficiency for certain messages by the calculation methods. Moreover, our present scheme can show even more merits when the size of the message is getting longer.

4 Conclusion

In summary, we provide a more efficient proposal for solving the insecurity problem in signing long messages via QDS. For most cases, one can always find an optimal solution by using our scheme. Simulation results indicate that our present work can dramatically improve the final signature efficiency compared with existing schemes when signing multi-bit messages. In addition, it can be easily realized with the current technology, and thus looks very promising in the implementation of QDS.

Acknowledgements The authors thank Xing-Yu Zhou, Kang Liu, Jia-Ming Chen and Jian-Rong Zhu for enlightened discussions.

Funding We gratefully acknowledge the financial support from the National Key R&D Program of China through Grant Nos. 2018YFA0306400, 2017YFA0304100, the National Natural Science Foundation of China through Grants Nos. 61475197, 61590932, 11774180, 61705110, the Natural Science Foundation of the Jiangsu Higher Education Institutions through Grant No. 17KJB140016, the Natural Science Foundation of Jiangsu Province through Grant No. BK20170902, the Priority Academic Program Development of Jiangsu Higher Education Institutions, and the Postgraduate Research and Practice Innovation Program of Jiangsu Province through Grant No. 46002CX17792.

References

1. Gottesman, D., Chuang, I.: Quantum digital signatures. arXiv:quant-ph/0105032 (2001)
2. Dunjko, V., Wallden, P., Andersson, E.: Quantum digital signatures without quantum memory. Phys. Rev. Lett. **112**(4), 040502 (2014)
3. Wallden, P., Dunjko, V., Kent, A., Andersson, E.: Quantum digital signatures with quantum-key-distribution components. Phys. Rev. A **91**(4), 042304 (2015)
4. Yin, H.L., Fu, Y., Chen, Z.B.: Practical quantum digital signature. Phys. Rev. A **93**(3), 032316 (2016)
5. Amiri, R., Wallden, P., Kent, A., Andersson, E.: Secure quantum signatures using insecure quantum channels. Phys. Rev. A **93**(3), 032325 (2016)
6. Puthoor, I.V., Amiri, R., Wallden, P., Curty, M., Andersson, E.: Measurement-device-independent quantum digital signatures. Phys. Rev. A **94**(2), 022328 (2016)
7. Arrazola, J.M., Wallden, P., Andersson, E.: Multiparty quantum signature schemes. Quantum Inf. Comput. **6**(0435), 435–464 (2016)
8. Collins, R.J., Donaldson, R.J., Dunjko, V., Wallden, P., et al.: Realization of quantum digital signatures without the requirement of quantum memory. Phys. Rev. Lett. **113**(4), 040502 (2014)
9. Donaldson, R.J., Collins, R.J., Kleczkowska, K., et al.: Experimental demonstration of kilometer-range quantum digital signatures. Phys. Rev. A **93**(1), 012329 (2016)
10. Collins, R.J., Amiri, R., Fujiwara, M., et al.: Experimental transmission of quantum digital signatures over 90 km of installed optical fiber using a differential phase shift quantum key distribution system. Opt. Lett. **41**(21), 4883–4886 (2016)
11. Yin, H.L., Fu, Y., Liu, H., et al.: Experimental quantum digital signature over 102 km. Phys. Rev. A **95**(3), 032334 (2017)

12. Yin, H.L., Wang, W.L., Tang, Y.L., et al.: Experimental measurement-device-independent quantum digital signatures over a metropolitan network. Phys. Rev. A **95**(4), 042338 (2017)
13. Roberts, G.L., Lucamarini, M., Yuan, Z.L., et al.: Experimental measurement-device-independent quantum digital signatures. Nat. Commun. **8**(1), 1098 (2017)
14. Collins, R.J., Amiri, R., Fujiwara, M., et al.: Experimental demonstration of quantum digital signatures over 43 dB channel loss using differential phase shift quantum key distribution. Sci. Rep. **7**(1), 3235 (2017)
15. Wang, C., Song, X.T., Yin, Z.Q., et al.: Phase-reference-free experiment of measurement-device-independent quantum key distribution. Phys. Rev. Lett. **115**(16), 160502 (2015)
16. Yin, H.L., Chen, T.Y., Yu, Z.W., et al.: Measurement-device-independent quantum key distribution over a 404 km optical fiber. Phys. Rev. Lett. **117**(19), 190501 (2016)
17. Wang, C., Yin, Z.Q., Wang, S., Chen, W., Guo, G.C., Han, ZFu: Measurement-device-independent quantum key distribution robust against environmental disturbances. Optica **4**(9), 1016–1023 (2017)
18. Zhang, C.H., Zhou, X.Y., Ding, H.J., Zhang, C.M., Guo, G.C., Wang, Q.: Proof-of-principle demonstration of passive decoy-state quantum digital signatures over 200 km. Phys. Rev. Appl. **10**, 034033 (2018). https://doi.org/10.1103/PhysRevApplied.10.034033
19. Wang, Q., Chen, W., Xavier, G., et al.: Experimental decoy-state quantum key distribution with a sub-poissionian heralded single-photon source. Phys. Rev. Lett. **110**(9), 090501 (2008)
20. Wang, Q., Wang, X.B.: Simulating of the measurement-device independent quantum key distribution with phase randomized general sources. Sci. Rep. **4**(4), 4612 (2014)
21. Wang, T.Y., Cai, X.Q., Ren, Y.L., Zhang, R.L.: Security of quantum digital signatures for classical messages. Sci. Rep. **5**, 9231 (2015)
22. Wang, T.Y., Ma, J.F., Cai, X.Q.: The postprocessing of quantum digital signatures. Quantum Inf. Process. **16**(1), 19 (2017)