Computers, Materials & Continua CMC, vol.61, no.2, pp.711-726, 2019

A New Anti-Quantum Proxy Blind Signature for Blockchain-Enabled Internet of Things

Chaoyang Li[1, 2, 3], Gang Xu[2], Yuling Chen[1, *], Haseeb Ahmad[4] and Jian Li[3]

Abstract: Blockchain technology has become a research hotspot in recent years with the prominent characteristics as public, distributed and decentration. And blockchain-enabled internet of things (BIoT) has a tendency to make a revolutionary change for the internet of things (IoT) which requires distributed trustless consensus. However, the scalability and security issues become particularly important with the dramatically increasing number of IoT devices. Especially, with the development of quantum computing, many extant cryptographic algorithms applied in blockchain or BIoT systems are vulnerable to the quantum attacks. In this paper, an anti-quantum proxy blind signature scheme based on the lattice cryptography has been proposed, which can provide user anonymity and untraceability in the distributed applications of BIoT. Then, the security proof of the proposed scheme can derive that it is secure in random oracle model, and the efficiency analysis can indicate it is efficient than other similar literatures.

Keywords: Blockchain, blockchain-enabled internet of things, quantum computers, proxy blind signature.

1 Introduction

Blockchain has gained much attention in recent years with its public, distributed, decentration and chronological characteristics. It is usually considered as a reliable database with high Byzantine fault tolerance (Fig. 1), and used in finance, cloud computing, IoT systems and other applications. Bitcoin is the first application of the blockchain technology, which constructs a peer-to-peer electronic cash system [Nakamoto (2008)]. BIoT has a promising outlook to build more efficient and resource-saving industrial systems, which can solve many problems in the centralized cloud systems and platforms [Banafa (2017)]. And it also can realize peer-to-peer transmission between unfamiliar users and build a distributed and append-only block storage structure among the trustless environment.

[1] Guizhou University, Sate Key Laboratory of Public Big Data, Guiyang, 550025, China.

[2] Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Post and Telecommunications, Beijing, 100876, China.

[3] School of Computer Science, Beijing University of Post and Telecommunications, Beijing, 100876, China.

[4] Department of Computer Science National Textile University, Faisalabad, 37610, Pakistan.

[*] Corresponding Author: Yuling Chen. Email: ylchen3@gzu.edu.cn.

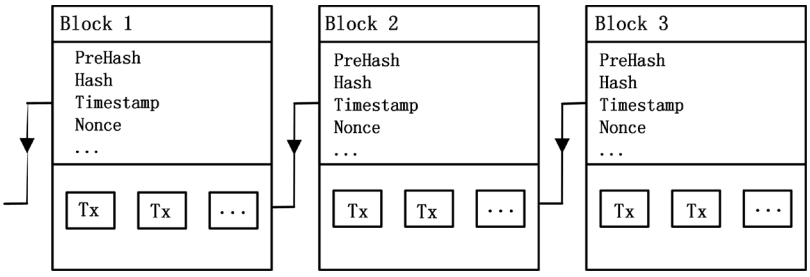

Figure 1: Structure of the blockchain. As the block contains a number of transactions in the latest time period, and the head of block contains the *PreHash*, *Hash*, *Timstamp*, and so on. Here, *PreHash* is the Hash value of the former block; *Hash* is the Hash value of this block; *Timstamp* is the setup time of this block

So far, IoT has gained more attraction in many fields, such as manufacturing, logistics, retailing and pharmaceutics. Since the high level of heterogeneity of IoT devices, the openness of wireless channel and limited resources of IoT devices, there are a number of serious security problems and challenges in IoT systems [Sicari, Rizzardi, Grieco et al. (2015); Pang, Liu, Zhou et al. (2017); Li, Wang, Li et al. (2018)]. Wang et al. [Wang and Wang (2014)] pointed that the former cryptography, such as symmetric cryptography protocols and hash-based user authentication protocols, are vulnerable to user anonymity and smart card security breach attack. Therefore, the public-key cryptography, for example the elliptic curve cryptography (ECC), can be used to strengthen the security for WSNs [Yeh, Chen, Liu et al. (2011); Shi and Gong (2013)]. However, the former two protocols cannot satisfy user anonymity and untraceability. Then, Jiang et al. [Jiang, Ma, Wei et al. (2016)] presented an ECC-based untraceable authentication scheme, which was computational efficiency. Recently, Li et al. [Li, Peng, Niu et al. (2017)] has presented a three-factor user authentication protocol based on ECC to secure WSNs, and it declares that can eliminate the weaknesses of former protocols.

Unfortunately, the quantum attacks take a significant threaten to most current digital signature schemes used for authentication in current blockchain-enabled systems along with the development of quantum computing and quantum communication [Li, Chen, Xu et al. (2015); Xu, Chen, Li et al. (2015); Qu, Cheng, Liu et al. (2018); Liu, Xu, Yang et al. (2018); Chen, Wang, Xu (2019); Chen, Sun, Xu et al. (2017); Jiang, Xu, Xu et al. (2018)]. As the classical mathematic hard problems widely applied in most asymmetric cryptosystems, such as the integer's factorization problem and discrete logarithm problem, can be solved by the quantum computer with super-polynomial speedup. While in Bitcoin system, the Elliptic Curve Digital Signature Algorithm (ECDSA) used which is constructed by the discrete logarithm problem. However, Shor's algorithm [Shor (1999)] can solve the integer factorization problem and discrete logarithm problem with exponential speedup by the quantum Fourier transform [Nielsen and Chuang (2000)]. And Grover's algorithm [Grover (1996); Jiang, Wang, Xu et al. (2018)] can search the objective from solution space with quadratic speedup. As it can decrease the complexity of seeking the pre-image for a certain function value to $O(\sqrt{n})$, here the complexity of the classical brute force search is $O(n)$ (Classical attack). Hence, by using the Grover algorithm, the adversary can easily

destroy the current blockchain-enabled systems in two ways:

- It can make full control over the generation of new blocks, as the acquisition of accounting rights depends on finding a particular hash value in POW-enabled blockchain systems.
- It can tamper the transaction records in former blocks equipped with greater computing power by speeding up the generation of nonce.

Therefore, how to resist the incoming quantum attacks becomes a more important research topic. In recently years, some promising visions have been invested which can weak above threats effectively, such as the quantum-resistant cryptography, post-quantum blockchain (PQB), quantum hashing and quantum network time machine. As the lattice-based cryptography [Gentry, Peikert and Vaikuntanathan (2008); Ajtai (1996); Zhang and Ma (2014); Zhu, Tan, Zhu et al. (2018); Yin, Wen, Li et al. (2018)] and the Hash-based cryptography [Dong, Zhang, Zhang et al. (2014); Jiang, Jiang and Ling (2014)] can significantly resist the quantum attack, which are also more appropriate for the transaction authentication in current blockchain system. And the quantum informational vision system, for example the post-quantum blockchain, is the conjugate of classical blockchain system and quantum-resist cryptography [Gao, Chen, Sun et al. (2018); Li, Chen, Chen et al. (2018)]. While the storage structure is classical and the communication protocol is quantum [Xu, Chen, Dou et al. (2015); Qu, Wu, Wang et al. (2017); Liu, Wang, Yuan et al. (2016); Wei, Chen, Niu et al. (2015); Xu, Chen, Dou et al. (2016); Qu, Chen, Ji et al. (2018); Liu, Gao, Yu et al. (2018); Chen, Tang, Xu et al. (2018)]. Then, the quantum hashing is a more robust system than the binary hash system against various distortions, though they have the same intermediate hash values [Jin and Yoo (2009)]. While the quantum network time machine a novel design of quantum blockchain which was claimed as a quantum blockchain using entanglement in time. Meanwhile, it is also a more promising method against the quantum attacks [Rajan and Visser (2018)].

Lattice cryptography served as a candidate for the quantum-resistant methods, which has more advantages than any other theories and is suitable for the blockchain-enabled systems. In 2008, Gentry et al. [Gentry, Peikert and Vaikuntanathan (2008)] proposed the first lattice-based signature scheme which is provable secure in the random oracle based on SIS problem [Ajtai (1996)]. And there is a novel cryptographic primitive has been presented which was called the preimage sample function (PSF). Recently, based on the lattice cryptography, some anti-quantum cryptographic schemes have been presented to strength the protection of the transaction authentication process in blockchain network. Zhang et al. [Zhang and Ma (2014)] proposed an identity-based proxy blind signature scheme based on lattice cryptography, and it showed that the proposed scheme was secure in standard model. Recently, Zhu et al. [Zhu, Tan, Zhu et al. (2018)] proposed an efficient identity-based proxy blind signature for semi-offline service, which showed that it could satisfy anti-quantum security. And Yin et al. [Yin, Wen, Li et al. (2018)] adopted Bonsai Tree technology to generate the private keys from the seed key, which could construct a lightweight nondeterministic wallet for anti-quantum transaction authentication. While Gao et al. [Gao, Chen, Sun et al. (2018); Li, Chen, Chen et al. (2019)] presented a secure cryptocurrency scheme based a lattice-based double-signature

scheme in PQB.

The proxy blind signature can provide delegation and anonymous authentication to protect the user's privacy, which was widely used in e-cash, voting and oblivious transfer. For some situations in BIoT, user must delegate his signing rights to another user, and the transaction information should be covert but verifiable. Therefore, in this paper, an anti-quantum proxy blind signature depend on the lattice cryptography has been presented, which can strength the transaction information security in the blockchain-enabled platforms for BIoT. And the proposed scheme not only can provide remarkable result against the quantum attacks, but can satisfy the properties of user anonymity and untraceability. In addition, the security proof of the proposed scheme has been proved secure in random oracle model, while the efficiency comparison also has been analyzed with some similar literatures.

The organization of this paper is as follows: some lattice theories and some related facts have been given in Section 2. A lattice-based proxy blind signature scheme has been proposed in Section 3. While the security proof has been presented in Section 4. And discussed the application in BIoT systems in Section 5. Then, the efficiency comparison and conclusion are shown in Section 6.

2 Preliminary

2.1 Some lattice theories

Definition* 1** ***(Lattice) *[Micciancio and Regev (2013)]: Let* $B=[b_1,b_2,...,b_n]\in R^{m\times m}$ *be a* $m\times m$ *matrix, here* $b_1,b_2,...,b_n$ *are linearly independent vectors. Based on* $B\in R^{m\times m}$, *the lattice* Λ *is a set* $\Lambda(B)=\{Bx:x\in Z^m\}$.

Given a matrix $A\in Z_q^{n\times m}$ and $u\in Z_q^n$, here q is a prime number. And following are the two-dimensional q-ary *lattices*:

$$\begin{cases}\Lambda_q^{\perp}(A):=\{y\in Z^m \mid Ay=o \bmod q\}\\ \Lambda_q^{u}(A):=\{y\in Z^m \mid Ay=u \bmod q\}\end{cases} \tag{1}$$

where the two lattices are dual to each other under normalization, just as

$\Lambda_q^{\perp}(A)=q\cdot\Lambda_q(A)^*$ and $\Lambda_q(A)=q\cdot\Lambda_q^{\perp}(A)^*$.

The shortest vector problem (SVP) and short integer solution (SIS) problem are two hard computational problems in lattice cryptography. And the hardness of SIS problem is the foundation of lattice-based signature scheme, which also widely used in one-way and collision-resistant hash functions, identification schemes and digital signatures.

Definition 2 (SVP problem) *[Ajtai (1996)]: Given lattice* $L=L(B)$, *B is the basis, output a shortest nonzero lattice vector, i.e.,* $aV\in L$ *satisfying* $\|v\|=\lambda_1(L)$.

Definition 3 (SIS problem) *[Ajtai (1996)]: Given the system parameters n, m, q,* β, *and* $A\in Z_q^{n\times m}$ *is a uniform and random matrix. Output a nonzero integer vector* $v\in Z_q^m$

satisfying $\| v \| \leq \beta$ *and* $Av = 0 \bmod q$.

Gaussian Distribution: *With the standard deviation* $\sigma \in R$, *and the center* $c \in R^n$, *the un-normalized definition of Gaussian distribution is*

$$\rho_{c,\sigma}(x) = \exp(\frac{-\| x-c \|^2}{2\sigma^2}) \tag{2}$$

In order to decreasing the signature size, ***Lemma 1*** about the discrete Gaussian distribution are used in our proxy blind signature scheme.

Lemma 1 *[Micciancio and Regev (2007)]: For* $k \geq 1$, *it satisfies* $\Pr[\| z \| > k\sigma\sqrt{m} : z \leftarrow D_\sigma^m] < k^m e^{\frac{1}{2}(1-k^2)}$. *And then, for any vector* $v \in R^m$ *and* $\sigma, r > 0$, *we can get*

$$\Pr[|< z, v >| > r : z \leftarrow D_\sigma^m] < 2e^{-\frac{r^2}{2\|v\|^2\sigma^2}} \tag{3}$$

2.2 Security model

As for security, the proxy blind signature scheme should satisfy the three fundamental properties: ***non-authorization unforgeable***, ***blindness*** and ***one-more unforgeability*** [Ruckert (2010)].

Non-authorization unforgeable: The adversary cannot obtain anything about the proxy private key secretly established between the user and the proxy signer without authorization.

Blindness: The experiment $Exp_{S,BS}^{blind}$ denotes the notion of blindness, where the adversarial signer S^* try to forge the valid signature in three modes: *find*, *issue* and *guess*. Then, in mode *find*, randomly chooses two messages M_0, M_1 and interacts with two different users in mode *issue*. According to the coin flip *b*, the two different users obtain blind signature for the messages M_b, M_{1-b}, respectively. And in mode *guess*, by seeing the unblinded signatures respect to M_0, M_1 in the original order, the signer should guess the bit *b*. Neither of the two different users's algorithms cannot output a valid signature, the adversarial signer declares failure and does not get any information of the valid signature. In addition, note that we allow the adversary to keep a state that is fed back in subsequent calls. A blind signature scheme *BS* is $(t, \delta) - blind$, if there does not exist an adversary S^* that wins the above experiment with probability at least δ within the time at most *t*, where the probability is defined as $Adv_{S^*,BS}^{blind} = |\Pr ob[Exp_{S^*,BS}^{blind} = 1] - \frac{1}{2}|$. Thus, a blind signature scheme is *statistically* blind if the blind signature scheme is $(\infty, \delta) - blind$ with the negligible probability δ.

One-more unforgeability: The other security property is one-more unforgeability, which ensures that once completed interaction can only generate one signature between the

signer and the user. Experiment $Exp_{U^*,BS}^{omf}$ can show the interaction between the adversarial user and the honest signer, as the j valid signatures can be obtained with at least $l < j$ completed interactions. Note H is a set of random oracles, the formal definition of blind signature scheme is BS is $(t, q_{Sign}, q_H, \delta)-$ one-more unforgeability, if there does not exist an adversary A, running in time at most t, making at most q_{Sign} signature queries and at most q_H hash oracle queries, can win the former defined experiment with negligible probability δ.

3 Lattice-based proxy blind signature scheme

Now, we will present the new proposed lattice-based proxy blind signature scheme, which mainly contains three parts: key generation, delegation generation and proxy blind signature generation. in this chapter, we will present the new proposed lattice-based proxy blind signature scheme, which mainly contains three parts: key generation, delegation generation and proxy blind signature generation.

Key Generation: Chosen κ as the system security parameter, and some other parameters n, q, κ, u, σ, η are same as Ducas et al. [Ducas, Durmus, Lepoint et al. (2013)]. Note that the public key is a $n \times m$ matrix $A \in Z_{2q}^{n \times m}$ and the private key is a $n \times m$ matrix $S \in Z_{2q}^{m \times n}$, while they satisfy $AS = qI_n (\mathrm{mod}\, 2q)$. And the public and private keys of the proxy signer are $A_P \in Z_{2q}^{n \times m}$ and $S_P \in Z_{2q}^{m \times n}$, which also satisfy $A_P S_P = qI_n (\mathrm{mod}\, 2q)$. As the bimodal Gaussian distribution can make the reject sampling more efficient, this paper will applied it in the proposed scheme, while the detail steps of reject sampling are described in Jiang et al. [Jiang, Liang, Liu et al. (2017)].

Delegation Generation: Firstly, the user signs the proxy signature certificate W with his public and private keys, and sends the proxy warrant $W_{A \leftarrow B}$ to the proxy signer. Here, this proxy signature certificate W contains the agent identity, proxy signature authority and authorization expiration date. Next, the proxy signer verifies the proxy warrant and generates the proxy public and private keys with proxy warrant for the proxy blind signature.

- The user randomly chooses $y_1 \leftarrow D_{\sigma_3}^m$ and $t_1 \leftarrow \{0,1\}^n$. Next, he computes u_1 with his own public key A, private key S and the proxy signature certificate W

$$\begin{cases} c_1 = H(Ay_1 \bmod 2q, m) \\ u_1 = y_1 + (-1)^{t_1} Sc_1 \end{cases} \tag{4}$$

  Then, he will output the signature Warrant $W_{A \leftarrow B}(W, u_1, c_1)$ with probability $\min(\frac{D_{\sigma_0}^m(u_1)}{M_0 D_{c_1,\sigma_0}^m(u_1)}, 1)$, and send it to the proxy signer.

- When the proxy signer receives the signature Warrant $W_{A \leftarrow B}(W, u_1, c_1)$, she will

reject it if $\| u_1 \| > B_2$ and $\| u_1 \|_\infty > q/4$, and accept it if the following equation holds:

$$c_1 = H(Au_1 + qc_1 \bmod 2q, W) \tag{5}$$

- The proxy signer generates the proxy public and private keys for the next proxy blind signature generation. Here, she chooses $M \leftarrow H_1(W_{A \leftarrow B})$ and computes

$$\begin{cases} A_P = A_1 * M^T \\ S_P = M * S_1 \end{cases} \tag{6}$$

Proxy Blind Signature Generation: When the delegation has been established between the user and the proxy signer, they will implement the following algorithms to generate the proxy blind signature. And through the following four algorithms: ***Blinding Algorithm***, ***Signing Algorithm***, ***Unblinding Algorithm*** and ***Verifying Algorithm***, a legitimate proxy blind signature will be generated as shown in following:

- The proxy signer randomly chooses $r \leftarrow D_{\sigma_2}^m$, and computes $x \leftarrow A_P r$ with his own public key A_P. Then, she sends (r, x) to the user.
- This is the ***Blinding Algorithm***. When the user receivers (r, x) from the proxy signer, he first randomly chooses $y_2 \leftarrow D_{\sigma_3}^m$ and $t_2 \leftarrow \{0,1\}^n$. Next, he computes u_2 with the proxy signer's public key A_P and the message *m*

$$\begin{cases} c_2 = H(x + A_P y_2 \bmod 2q, m) \\ u_2 = (-1)^{t_2} c_2 \end{cases} \tag{7}$$

Then, he will output blind message u_2 with probability $\min(\frac{D_{\sigma_1}^m(u_2)}{M_1 D_{c_2,\sigma_1}^m(u_2)}, 1)$, and send it to the proxy signer.

- This is the ***Signing Algorithm***. When the proxy signer receivers blind message u_2 from the user, she computes *z* with her own private key S_P and the former selected *r*

$$z = r + S_P u_2 \tag{8}$$

Then, she will output the signature *z* of the blind message with probability $\min(\frac{D_{\sigma_2}^m(z)}{M_2 D_{S_P u_2,\sigma_2}^m(z)}, 1)$, and send it to the user.

- This is the ***Unblinding Algorithm***. When the user receivers the signature *z* from the user, he computes *e* with the former selected y_2

$$e = y_2 + z \tag{9}$$

Then, he will output the proxy blind signature *e* of the original message with

probability $\min(\frac{D^m_{\sigma_3}(e)}{M_3 D^m_{y_2,\sigma_3}(e)},1)$, and send it to the proxy signer.

- This is the ***Verifying Algorithm***. The generated proxy blind signature will be rejected if $\| e \| > B_2$ and $\| e \|_\infty > q/4$, and accepted if the following equation holds:

$$c_2 = H(A_P e + q c_2 \bmod 2q, m) \tag{10}$$

By this time, a legal proxy blind signature has been generated as the above Eq. (10) through certification. And the simple processes of the proposed proxy blind signature scheme can be description as follows in Fig. 2.

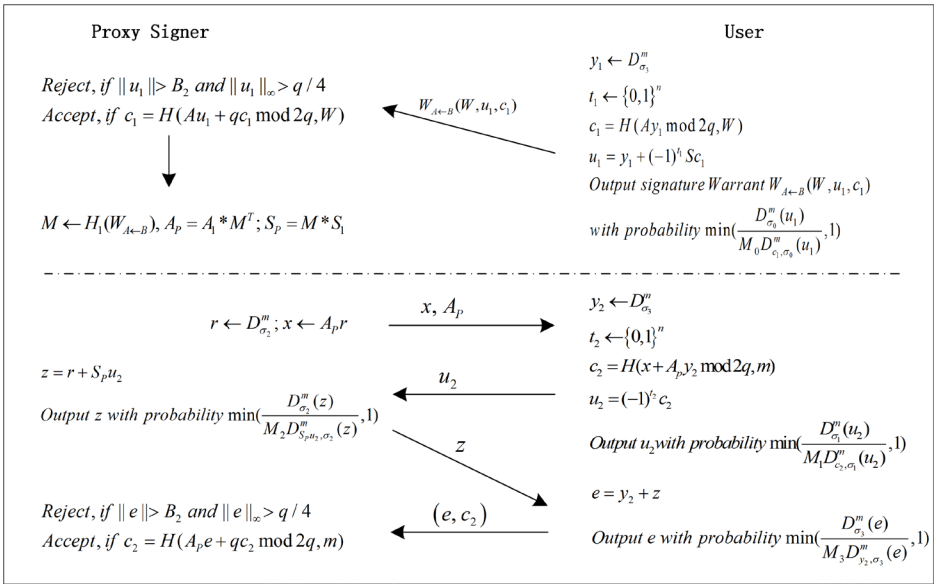

Figure 2: The lattice-based proxy blind signature scheme

4 Security proof

In this phase, the verifier will verify whether the proxy Blind signature $< e, c_2 >$ is legal or not firstly. If $\| e \| > B_2$ or $\| e \|_\infty > q/4$, the signature will be rejected. Otherwise, the correctness of the proposed proxy blind signature is mainly depending on equation $A_P e + q c_2 = x + A_P y_2 \bmod 2q$, and detail of it is showing as follows:

$$\begin{aligned} A_P e + q c_2 &= A_P(r + S_P u_2) + A_P y_2 + q c_2 \\ &= A_P r + (-1)^{t_2} A_P S_P c_2 + A_P y_2 + q c_2 \\ &= x + A_P y_2 + (-1)^{t_2} q c_2 + q c_2 \\ &= x + A_P y_2 \bmod 2q \end{aligned} \tag{11}$$

For the proxy blind signature scheme, it should resist the attack of the existence of strong unforgeable under the non-authorization (Shown in ***Theorem 1***). And it also should satisfy the properties of blindness (Shown in ***Theorem 2***) and one-more unforgeability (Shown in ***Theorem 3***).

Theorem 1: *The proposed proxy blind signature scheme can defeat strongly unforgeable under the non-authorization*.

Proof: As this kind of forgery, the adversary cannot obtain anything about the proxy private key, which is generated from the proxy warrant $W_{A\leftarrow B}$ secretly established between the user and the proxy signer. If the adversary has the ability that he can forge a valid proxy blind signature, it says that the adverasary can forge the delegation generation stage without knowing the original user's secret key. If so, it will indicate that the lattice-based signature scheme in Ducas et al. [Ducas, Durmus, Lepoint et al. (2013)] is not safe.

Theorem 2: *The proposed proxy blind signature scheme is statistically blind*.

Proof: Assume there exists two different users $U(p_k,u_b)$, $U(p_k,u_{1-b})$, the adversary has ability to attack the proposed scheme with advantage $Adv_{PBS}^{blind}(S^*)$ and $(u_b,u_{1-b})\leftarrow S^*(pk,sk)$. As for the blindness, we only show that the outputs u_2 and signature (c_2,e) are independent of their corresponding messages, note that $c_2\leftarrow\{v\in\{-1,0,1\}^k:\|v\|_1\le\kappa\}$. First, as the distribution of u_2, let u_b and u_{1-b} be generated by the interaction with the user $U(p_k,u_b)$ and $U(p_k,u_{1-b})$, respectively. Because the construction $u_2\leftarrow(-1)^{t_2}c_2$ and the output probability $\min(D_{\sigma_1}^m(u_2)/M_1D_{c,\sigma_1}^m(u_2),1)$, we tailored u_b and u_{1-b} to be distributed depending on the same distribution $D_{\sigma_1}^m$ by the rejection sampling lemma. Thus, the statistical distance $\Delta(u_b,u_{1-b})=0$, and they are distributed independently of the message being signed. Second, as the distribution of signature *e*, which is similar to u_2. Let e_b and e_{1-b} be the blind signature of $U(p_k,u_b)$ and $U(p_k,u_{1-b})$, respectively. Because the construction $e\leftarrow y_2+z$ and the output probability $\min(D_{\sigma_3}^m(e)/M_3D_{y_2,\sigma_3}^m(e),1)$ thus the statistical distance satisfies $\Delta(e_b,e_{1-b})=0$ by the rejection sampling lemma. Therefore, the generated blind signatures are independent of their corresponding messages. And then the proposed proxy blind signature is statistically blind to the adversarial S^*.

Theorem 3: *Assume there exists an adversary F who can forge a valid proxy blind signature with non-negligible probability* δ*, then there will exist a polynomial-time algorithm C which can solve* $SIS_{q,n,m,\beta}$ *problem for* $\beta=2B_2$.

Proof: The proposed proxy blind signature scheme follows the fact that the output is independent of the signing key. While the main outputs are the Hash value and signature of the message, so the ***Forger*** only need to make the ***Hash queries*** and ***Sign queries***. Then, if the adversary has ability to against the property of ***One-more unforgeability***, we will show that the simulator can find a solution of *SIS* problem.

Hash queries: Challenger *C* builds an initial empty list *List* 1 to store the hash value $Hash(m)$ of message *m*. When the ***Forger*** sends queries for message *m* to *C*, firstly he will check whether the pair $< m, Hash(m) >$ exists in the *List* 1 or not. If it is, *C* take $< m, Hash(m) >$ as the answer of the ***Forger***'s Hash queries; if not, *C* will compute the new hash value of message *m*, and send the new pair $< m, Hash(m) >$ to ***Forger*** and restore it to the *List* 1.

Sign queries: *C* holds an initial empty list *List* 2 which contains the blind signature pairs $< e, c_2 >$. When the ***Forger*** sends a queries for a signature about message *m*, firstly *C* will checks whether this pair $< e, c_2 >$ exists in the *List* 2. If it is, *C* will take pair $< m, e, c_2 >$ as the answer of the ***Forger***'s Sign queries; if not, *C* will run the blind signing process to generate a blind signature of the message *m*, send the new signature pair $< e, c_2 >$ to the ***Forger*** and restore it to the *List* 2.

Forge: Assume that *c* was the answer to a Hash query made by the ***Forger***, then by the Eq. (5), we can derive that $H(A_P e + qc_2, m) = H(A_P e' + qc_2, m')$ for the two different signature pairs $< m, e, c_2 >$ and $< m', e', c_2 >$. In case of $m \neq m'$ or $A_P e + qc_j \neq A_P e' + qc_j$, there makes a hash collision. Due to the property of Hash function, it is impossible to arise that phenomenon. Therefore, we can get $m = m'$ and $A_P e + qc_j = A_P e' + qc_j$ with overwhelming probability. Which also can yield the follow equation $A_P(e - e') = 0 \bmod 2q$, and we know that $e - e' \neq 0$. Hence, the *SIS* problem can be successfully solved.

And depending on the proof [Ducas, Durmus, Lepoint et al. (2013)], assume that the c_j is a response which *C* gives to the ***Forger***. We can set this blind signature as $< e, c_j >$ for message *m*, and choose different random values $c'_j, ..., c'_s \leftarrow B^{\kappa}$. Then, by the *Forking Lemma* [Bellare and Neven (2006)], we can get the probability of $c'_j \neq c_j$:

$$P(c'_j \neq c_j) = (\delta - \frac{1}{B_k^n}) * (\frac{\delta - 1/B_k^n}{t} - \frac{1}{B_k^n}) \tag{12}$$

Form above simulation, the ***Forger*** can generate another new blind signature pair $< e', c'_j >$, which satisfy $A_P e + qc_j \neq A_P e' + qc'_j$. Based on the former designing, the

proxy public and private key in the proposed scheme can also satisfy $A_P S_P = (A_1 * M^T) * (M * S_1) = A_1 S_1 = qI_n \bmod 2q$. And then

$$A_P(e - e') = q(c_j - c'_j) I_n \bmod 2q \tag{13}$$

Since $c_j \neq c'$, we can have $e - e' \neq 0 \bmod 2q$. And, we will have $\| e \|_\infty, \| e' \|_\infty \leq q/4$ with overwhelming probability, thus $\| e - e' \|_\infty < q/2$. As we also know that $q(c_j - c'_j) \bmod 2q = 0$, and we let $v = e - e' \neq 0 \bmod 2q$, then we have $A_P v = 0 \bmod 2q$. Note that $\| v \| \leq \beta$, and the *v* is one of the *SIS* problem's solution with $\beta = 2B_2$.

5 The transaction implementation in BIoT

Equipping with the former proposed proxy blind signature scheme, current BIoT systems will have enough ability to resist the quantum attacks. It also can provide delegation and anonymous authentication to protect the user's privacy.

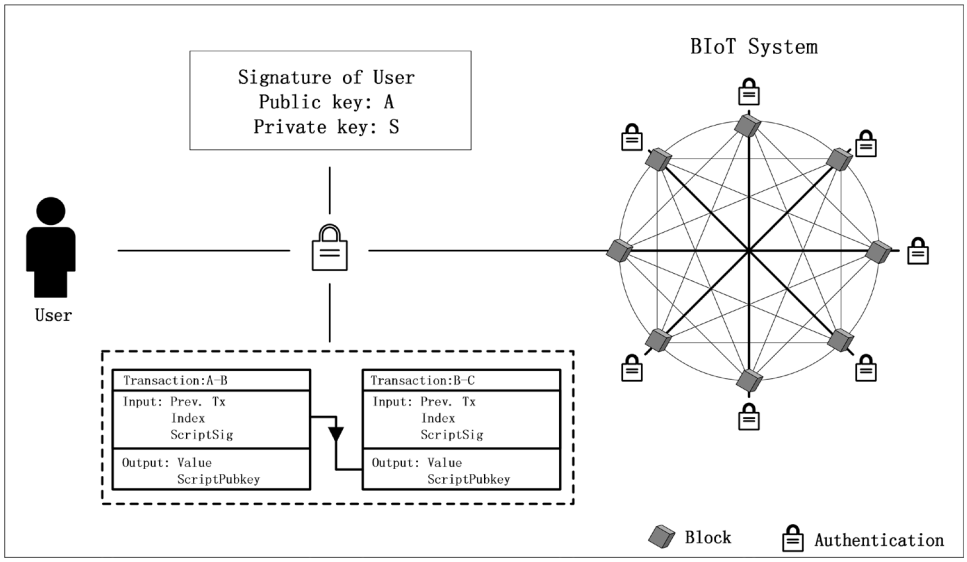

Figure 3: The transaction implementation

In the distributed blockchain-enabled systems, the general user and the miner are different independent entities who have different function to maintain the whole network. More importantly, the transaction address is essential for transaction implementation, which is generated by the public key. Here, the user should generate many more public keys for the generation of the every new address to prevent the statistical attack. Then, for a transaction, it is a data structure with different inputs and outputs. As the inputs are the *Previous tx.*, *Index* and *ScriptSig*, here *Previous tx*. denotes the Hash value of previous transaction; *Index* denotes the value index of previous *tx*.'s output; and *ScriptSig*

is the signature of transaction creator. Meanwhile, the outputs are the *Value* and *ScriptPubkey* which are the value of this transaction and the receiver's public key, respectively (Fig. 3).

For the general user, two users A and B can establish one transaction by the following four steps:

- First, the user A initiates a transfer request with user B.
- Second, the user B chooses one pair of his unused public and private key, generates a new address and sends it to user A for transaction implementation.
- Third, the user A establish a new transaction with above mentioned inputs and outputs, and broadcasts it to the whole blockchain network.
- Last, this transaction will be collected and verified by the miners, and it is finished until the record is confirmed and stored in the BIoT system.

Here, some more important issues should be noted. The reward for the miner's work of establishing the new block should also be recorded as a general transaction in the blockchain. And once one new block has been established, the compensation deal for the miner will become valid and the reward bitcoin will be consumable for the general transaction. In addition, the more important thing is that the total input amount and output amount of the transaction should be equal. While the total inputs may come from one or more wallet address of the sender. And the sender may need to prepare a new address to receive the surplus inputs if the input amount is more than required.

In the blockchain network, the broadcasted transactions will be verified firstly by the miner. Then, the valid transactions will be packaged into a temporary block. When a miner obtains the right for establishing the new block, the temporary block created by this miner will be attached in the longest chain as the newest block. After this, when another new block has been established, all the transactions in this block have been verified for one time. Then, these transactions will be verified for many times by attaching more and more new blocks at the end of the longest chain, since the blockchain is an append-only chain where the new block is established with the former block. In general, the transactions in this block cannot be tampered after six blocks since that there needs huge computation to rebuild six blocks. Therefore, the blockchain can store the transaction information as an inalterable record and make them more secure in the BIoT system.

6 Efficiency and conclusion

Assume the parameters (n, m, q, k, σ) in this paper are the same as that in the similar literatures, then Tab. 1 shows the efficiency comparison results in detail. As comparing with Zhang et al. [Zhang and Ma (2014); Ruckert (2010), the size of public key, private key and signature are all bigger than the proposed scheme. In addition, our scheme can resist the quantum attacks.

Table 1: Comparison with similar literatures

Scheme	Public key size	Secret key size	Signature size
Zhang and Ma (2014)	$3mnlogq$	$3mnlogq$	$(mn+dm)\log(12\sigma)$
Ruckert (2010)	$mnlog(2q+1)$	$mnlog(2q+1)$	$2m\log(12\sigma)$
This scheme	$mnlog2q$	$mnlog2q$	$m\log(12\sigma)$

In this paper, the proposed lattice-based proxy blind signature can provide high security level for the systems and applications of BIoT. It not only can resist the quantum attacks, but can provide agency transaction and anonymous authentication properties. Then, the security analysis in random oracle model and efficient comparison of the proposed scheme have been given, and the results show that our scheme is secure and more efficient. Moreover, this work also can help to rich the security research of BIoT.

Acknowledgement: Project supported by NSFC (Grant No. U1836205), the Major Scientific and Technological Special Project of Guizhou Province (Grant No. 20183001), the Foundation of Guizhou Provincial Key Laboratory of Public Big Data (Grant No. 2018BDKFJJ016), and the Foundation of State Key Laboratory of Public Big Data (Grant No. 2018BDKFJJ018), CCF-Tencent Open Fund WeBank Special Funding (CCF-WebankRAGR20180104).

References

Ajtai, M. (1996): Generating hard instances of lattice problems. *Proceedings of the Twenty-Eighth annual ACM Symposium on Theory of Computing*, pp. 99-108.

Banafa, A. (2017): IoT and blockchain convergence: benefits and challenges. https://www.researchgate.net/publication/322056480.

Bellare, M.; Neven, G. (2006): Multi-signatures in the plain public-key model and a general forking lemma. *Proceedings of the 13th ACM Conference on Computer and Communications Security*, pp. 390-399.

Chen, X. B.; Tang, X.; Xu, G.; Dou, Z.; Chen, Y. L. et al. (2018): Cryptanalysis of secret sharing with a single d-level quantum system. *Quantum Information Processing*, vol. 17, no. 9, pp. 225.

Chen, X. B.; Sun, Y. R.; Xu, G.; Jia, H. Y.; Qu, Z. et al. (2017): Controlled bidirectional remote preparation of three-qubit state. *Quantum Information Processing*, vol. 16, no, 10, pp. 244.

Chen, X. B.; Wang, Y. L.; Xu, G.; Yang, Y. X. (2019): Quantum network communication with a novel discrete-time quantum walk. *IEEE Access*. https://doi.org/10.1109/ACCESS.2018.2890719.

Dong, H. H.; Zhang, Y. F.; Zhang, Y. F.; Yin, B. S. (2014): Generalized bilinear differential operators, binary bell polynomials, and exact periodic wave solution of boiti-leon-manna-pempinelli equation. *Abstract and Applied Analysis*, vol. 2014.

Ducas, L.; Durmus, A.; Lepoint, T.; Lyubashevshy, V. (2013): Lattice signatures and bimodal Gaussians. *Advances in Cryptology*, vol. 8042, pp. 40-56.

Gao, Y. L.; Chen, X. B.; Sun, Y. L.; Niu, X. X.; Yang, Y. Y. (2018): A secure cryptocurrency scheme based on post-quantum blockchain. *IEEE Access*, vol. 6, pp. 27205-27213.

Gentry, C.; Peikert, C.; Vaikuntanathan, V. (2008): Trapdoors for hard lattices and new cryptographic constructions. *Proceedings of the fortieth annual ACM Symposium on Theory of Computing*, vol. 14, no. 133, pp. 197-206.

Grover, L. (1996): A fast quantum mechanical algorithm for database search. *Twenty-Eighth ACM Symposium on Theory of Computing*, pp. 212-219.

Jiang, D. H.; Xu, Y. L.; Xu, G. B. (2019): Quantum signature based on local indistinguishability of orthogonal product states. *International Journal of Theoretical Physics*.

Jiang, D. H.; Wang, X. J.; Xu, G. B.; Lin, J. Q. (2018): A denoising-decompostition model combing TV minimisation and fractional derivatives. *East Asia Journal Applied Mathematics*, vol. 8, pp. 447-462.

Jiang, Q.; Ma, J. F.; Wei, F. S.; Tian, Y. L.; Shen, J. et al. (2016): An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks. *Journal of Network & Computer Applications*, vol. 76, pp. 37-48.

Jiang, T. S.; Jiang, Z. W.; Ling, S. (2014): An algebraic method for quaternion and complex least squares coneigen-problem in quantum mechanics. *Applied Mathematics & Computation*, vol. 249, pp. 222-228.

Jiang, Z. L.; Liang, Y. D.; Liu, Z. C.; Wang, X. (2017): Lattice-based proxy signature scheme with reject sampling method. *International Conference on Security, Pattern Analysis, and Cybernetics*, pp. 558-563.

Jin, M.; Yoo, C. D. (2009): Quantum hashing for multimedia. *IEEE Transaction on Information Forensics and Security*, vol. 4, no. 4, pp. 982-994.

Li, C. Y.; Chen, X. B.; Chen, Y. L.; Hou, Y. Y.; Li, J. (2019): A new lattice-based signature scheme in post-quantum blockchain network. *IEEE Access*, vol. 7, pp. 2026-2033.

Li, J.; Chen, X. B.; Xu, G.; Yang, Y. X.; Li, Z. P. (2015): Perfect quantum network coding independent of classical network solutions. *IEEE Communications Letters*, vol. 19, no, 2, pp. 115-118.

Li, L.; Wang, Z.; Li, Y.; Shen, H.; Lu, J. (2018): Hopf bifurcation analysis of a complex-valued neural network model with discrete and distributed delays. *Applied Mathematics & Computation*, vol. 330, pp. 152-169.

Li, X.; Peng, J. Y.; Niu, J. W.; Wu, F.; Liao, J. G. et al. (2017): A robust and energy efficient authentication protocol for industrial internet of things. *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1606-1615.

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

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

Micciancio, D.; Regev, O. (2007): Worst-case to average-case reductions based on Gaussian measures. *SIAM Journal on Computing*, vol. 37, no. 1, pp. 267-302.

Micciancio, D.; Regev, O. (2013): Lattice-based cryptography. *Encyclopedia of Cryptography & Security*, vol. 85, no. 1-2, pp. 131-141.

Nakamoto, S. (2008): Bitcoin: a peer-to-peer electronic cash system.

https://bitcoin.org/bitcoin.pdf.

Nielsen, M.; Chuang, I. (2000): *Quantum Computation and Quantum Information*, vol. 70, no. 5, pp. 558-559. Cambridge University Press.

Pang, Z. H.; Liu, G. P.; Zhou, D.; Sun, D. (2017): Data-based predictive control for networked nonlinear systems with packet dropout and measurement noise. *Journal of System Science and Complexity*, vol. 30, no. 5, pp. 1072-1083.

Qu, Z. G.; Chen, S. Y.; Ji, S.; Ma, S. Y.; Wang, X. J. (2018): Anti-noise bidirectional quantum steganography protocol with large payload. *International Journal of Theoretical Physics*, vol. 57, no. 6, pp. 1-25.

Qu, Z. G.; Cheng, Z. W.; Liu, W. J.; Wang, X. J. (2018): A novel quantum image steganography algorithm based on exploiting modification direction. *Multimedia Tools and Applications*.

Qu, Z. G.; Wu, S. Y.; Wang, M. M.; Sun, L.; Wang, X. J. (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. 306, pp. 1-25.

Rajan, D.; Visser, M. (2018): Quantum blockchain using entanglement in time. https://arxiv.org/abs/1804.05979.

Ruckert, M. (2010): Lattice-based blind signatures. *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 413-430.

Shi, W. B.; Gong, P. (2013): A new user authentication protocol for wireless sensor networks using elliptic curves cryptography. *International Journal of Distributed Sensor Networks*, vol. 2013, no. 730831, pp. 51-59.

Shor, P. (1999): Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Review*, vol. 41, no. 2, pp. 303-332.

Sicari, S.; Rizzardi, A.; Grieco, L. A.; Coen-Porisini, A. (2015): Security, privacy and trust in internet of things. *Computer Networks*, vol. 76, pp. 146-164.

Wang, D.; Wang, P. (2014): Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks. *Ad Hoc Networks*, vol. 20, no. 2, pp. 1-15.

Wei, Z. H.; Chen, X. B.; Niu, X. X.; Yang, Y. X. (2015): The quantum steganography protocol via quantum noisy channels. *International Journal of Theoretical Physics*, vol.

54, no. 8, pp. 2505-2515.

Xu, G.; Chen, X. B.; Dou, Z.; Li, J. X.; Liu, X. et al. (2016): Novel criteria for deterministic remote state preparation via the entangled six-qubit state. *Entropy*, vol. 18, no. 7, pp. 267.

Xu, G.; Chen, X. B.; Duo, Z.; Yang, Y. X.; Li, Z. P. (2015): A novel protocol for multiparty quantum key management. *Quantum Information Processing*, vol. 14, no. 8, pp. 2959-2980.

Xu, G.; Chen, X. B.; Li, J.; Wang, C.; Yang, Y. X. et al. (2015): Network coding for quantum cooperative multicast. *Quantum Information Processing*, vol. 14, no. 11, pp. 4297-4322.

Yeh, H. L.; Chen, T. H.; Liu, P. C.; Kim, T. H.; Wei, H. W. (2011): A secured authentication protocol for wireless sensor networks using elliptic curves cryptography. *Sensors*, vol. 11, no. 5, pp. 4767-4779.

Yin, W.; Wen, Q. Y.; Li, W. M.; Zhang, H.; Jin, Z. G. (2018): An anti-quantum transaction authentication approach in blockchain. *IEEE Access*, vol. 6, no. 99, pp. 5393-5401.

Zhu, H. F.; Tan, Y. A.; Zhu, L. H.; Zhang, Q. X.; Li, Y. Z. (2018): An efficient identity-based proxy blind signature for semioffline services. *Wireless Communications and Mobile Computing*, vol. 2018.

Zhang, L. L.; Ma, Y. Q. (2014): A lattice-based identity-based proxy blind signature scheme in the standard model. *Mathematical Problems in Engineering*, vol. 2014, no. 1.