IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 11, 2018, accepted March 19, 2018, date of publication April 18, 2018, date of current version June 5, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2827203

A Secure Cryptocurrency Scheme Based on Post-Quantum Blockchain

YU-LONG GAO[1], XIU-BO CHEN[1,2], YU-LING CHEN[2], YING SUN[3], XIN-XIN NIU[1,2], AND YI-XIAN YANG[1,2]

[1]State Key Laboratory of Networking and Switching Technology, Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China
[2]Guizhou Provincial Key Laboratory of Public Big Data, Guizhou University, Guiyang 550025, China
[3]Beijing Electronic Science and Technology Institute, Beijing 100070, China

Corresponding author: Xiu-Bo Chen (flyover100@163.com)

This work was supported in part by the NSFC under Grant 61671087, Grant 61272514, Grant 61170272, and Grant 61003287, in part by the Major Science and Technology Support Program of Guizhou Province under Grant 20183001, in part by the Fok Ying Tong Education Foundation under Grant 131067, and in part by the Open Foundation of Guizhou Provincial Key Laboratory of Public Big Data under Grant 2017BDKFJJ007.

ABSTRACT Nowadays, blockchain has become one of the most cutting-edge technologies, which has been widely concerned and researched. However, the quantum computing attack seriously threatens the security of blockchain, and related research is still less. Targeting at this issue, in this paper, we present the definition of post-quantum blockchain (PQB) and propose a secure cryptocurrency scheme based on PQB, which can resist quantum computing attacks. First, we propose a signature scheme based on lattice problem. We use lattice basis delegation algorithm to generate secret keys with selecting a random value, and sign message by preimage sampling algorithm. In addition, we design the first-signature and last-signature in our scheme, which are defined as double-signature. It is used to reduce the correlation between the message and the signature. Second, by combining the proposed signature scheme with blockchain, we construct the PQB and propose this cryptocurrency scheme. Its security can be reduced to the lattice short integer solution (SIS) problem. At last, through our analysis, the proposed cryptocurrency scheme is able to resist the quantum computing attack and its signature satisfies correctness and one-more unforgeability under the lattice SIS assumption. Furthermore, compared with previous signature schemes, the sizes of signature and secret keys are relatively shorter than that of others, which can decrease the computational complexity. These make our cryptocurrency scheme more secure and efficient.

INDEX TERMS Blockchain, post-quantum, lattice, cryptocurrency, security.

I. INTRODUCTION

With the in-depth study of computer network technology and cryptography, more and more research results have been applied in our daily life, such as mobile cloud computing [1], [2], dynamic searchable symmetric encryption [3], secure multiparty computation [4], [5], especially online transaction. Online transaction has to rely on financial institutions serving as trusted third parties mostly, but it may cause leakage of personal privacy and security threats. Nakamoto designed a peer-to-peer electronic cash system and described the blockchain for the first time [6]. Using a public ledger, Bitcoin is transacted as cryptocurrency in this decentralized system. In the Bitcoin, blockchain establishes a decentralized consensus about the order of transactions among a large number of members who need not to know or trust anyone. Furthermore, each block references the hash of the previous block. This establishes a link between these blocks, thus, it creates a blockchain. Then, by combining peer-to-peer network, cryptographic algorithm, distributed data storage and a decentralized consensus mechanism, blockchain technology provides a way for people that record in a secure and verifiable manner, and it can prevent double spending effectively [7]–[10].

In particular, blockchain 2.0 has been presented which includes hyperledger and smart contract technology, complex contracts are created and enforced automatically [11], [12]. In addition, blockchain integrates the cryptographic algorithm, the hash algorithm and distributed network technology together [13]. It feels more like a distributed super-ledger system that relies on maintenance

of all users, transactions can not be forged and altered intuitively.

Besides, the public-key cryptography plays a very fundamental role in the security of blockchain. Currently, Elliptic Curves Cryptography (ECC) is used in blockchain. Its security is based on the intractability of elliptic curve discrete logarithm problem. The main functions of the public-key cryptography are as follows.

(1) Using private key to generate the signature of message, and the signer can not deny it.

(2) Preventing transaction message from being maliciously forged.

(3) Public key is used to participate in address exchange as the receiving address of cryptocurrency.

(4) Private key is used to protect and manage cryptocurrency.

At present, classical cryptographic algorithm is still used in blockchain technology. The security of classical cryptographic algorithm mainly depends on intractability of elliptic curve discrete logarithm problem or integer factorization problem. However, with the research on quantum computing, quantum computer can have powerful parallel computing ability which becomes a great threat to classic cryptographic algorithm. Shor proposed quantum algorithms for finding discrete logarithms and factoring integers on a quantum computer which can break the RSA, DSA and ECDSA algorithms [14]. Both U.S. National Security Agency (NSA) and National Institute of Standards and Technology (NIST) pointed out that the necessity for transition to quantum-resistant schemes is increasing. In 2015, NSA issued a statement that NSA decided to adopt the post-quantum cryptography instead of suite B algorithm because of potential threats of quantum computer. NSA also planned to transition from ECC to post-quantum cryptography. In addition, NIST announced its plan for a public call for post-quantum schemes to construct new public-key cryptography standards [15].

We consider that traditional classical cryptography will be cracked, including the ECC algorithm, and there are few relevant researches on the security of blockchain. Therefore, targeting at this issue, we design a post-quantum blockchain and apply it to cryptocurrency scheme.

In order to resist the quantum computing attack, people proposed post-quantum cryptography. In particular, lattice-based cryptography is widely believed to be able to resist quantum computing attacks [16]. Ajtai [17] and [18] proposed a stochastic and short lattice construction algorithm that can be proved to be secure. In 2008, Gentry *et al.* [19] proposed new cryptographic constructions include trapdoor functions with preimage sampling. In 2010, Rückert [20] designed the Lattice-based Blind Signature Scheme (LBSS) which is the first lattice-based blind signature scheme which uses the trapped trapdoor one-way function. Additionally, he also proposed the Lattice-based Identity-based Signature Scheme (LIBSS) [21]. In 2010, Cash *et al.* [22] proposed a new cryptographic definition which is called bonsai tree based on hard lattice. And other proxy signature scheme had been proposed [23]. Agrawal *et al.* [24] presented a technique for delegating a short lattice basis. The algorithm can keep the lattice dimension unchanged which can improve the efficiency of the lattice-based cryptographic scheme. Zhang and Sang [25] and Zhang and Ma [26] proposed proxy blind signature schemes from lattice basis delegation. In order to satisfy the strong unforgeability, Zhang et al used proxy key and private key to sign the message respectively. Gu *et al.* [27] presented a signature scheme provably secure in the random oracle model. Yan *et al.* [28] presented an identity-based signcryption from lattices.

Inspired by the researches and analyses above, we consider that lattice-based cryptography becomes a hot research topic of post-quantum cryptography now and we can use it to enhance the security of blockchain. By combining post-quantum cryptography with blockchain together, we provide a more secure and efficient cryptocurrency scheme. The main contributions of this paper are summarized as follows.

(1) We propose a new signature scheme based on lattice. We use lattice basis delegation algorithm to generate secret keys with selecting a random value, and use preimage sampling algorithm to sign message. In addition, we design the first-signature and last-signature in our scheme which are defined as double-signature. It can reduce the correlation between the message and signature. Besides, the security of the signature scheme depends on the lattice SIS problem.

(2) We present the definition of PQB for the first time. In particular, by combining the proposed signature scheme based with blockchain, we construct the PQB and provide a secure cryptocurrency scheme that can resist quantum computing attacks.

(3) Through our analysis, the signature of the cryptocurrency scheme satisfies the correctness and can resist quantum computing attacks. Under the standard hardness assumption of the SIS, this scheme is proven to be one-more unforgeable in the standard model. In addition, the size of our scheme's signature is shorter than its counterpart in other schemes, which can decrease the computational complexity of our proposed cryptocurrency scheme.

The remainder of this paper is organized as follows. In Section II, we mainly introduce the transaction in the blockchain, the lattice problems and some lemmas. In Section III, we present the definition of the post-quantum blockchain and propose our signature scheme. By using the PQB based on lattice, we also provide a new cryptocurrency scheme. In Section IV, we analyze our proposed cryptocurrency scheme from correctness, one-more unforgeability, security and efficiency. Some concluding remarks are given in Section V.

II. PRELIMINARIES

Before we introduce our signature scheme, we should give descriptions of the transaction in blockchain, lattice-based cryptography and some lemmas.

A. TRANSACTION IN BLOCKCHAIN

Unspent Transaction Output (UTXO) is used to prevent double spending. Every transaction consists of transaction inputs and transaction outputs, and these transactions constitute a chain structure. Transaction inputs have to be unspent transaction outputs, that is to say, outputs of previous transactions that have not yet been spent. All legitimate transactions can be traced back to the output of one or more transactions. The beginning is the reward of mining and the end of the transaction is unspent transaction output.

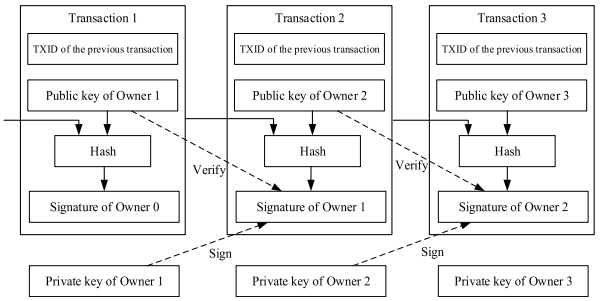

FIGURE 1. Transaction in Bitcoin based on blockchain.

A Bitcoin is defined as a chain of digital signatures [6], and each block contains a reference to a previous block. As shown in Fig. 1, by signing the hash of transaction 1 and Owner 2's public key, Owner 1 transfers the coin to the Owner 2. Other miners can verify the signature of transaction 2. Owner 2 has the ownership of the Bitcoin. When the Owner 2 wants to spend this coin, he can use his private key to generate the transaction 3 in this way above.

B. LATTICES AND HARD PROBLEMS

We use $\mathbb{R}, \mathbb{Z}$ to denote the set of all reals and the set of positive integers, respectively. Let $\mathbb{R}^m$ be the m-dimensional Euclidean vector space with its usual topology. In the following content, $m \in \mathbb{Z}, n \in \mathbb{Z}, m \geq n$. L and Λ denote lattice, the orthogonal lattice corresponding to Λ is represented by $\Lambda^{\perp}$, vector $\mathbf{x} = (x_1, x_2, \cdots, x_{n-1}, x_n)^T$ in the space $\mathbb{R}^m$, and its Euclidean norm is denoted by $\|\mathbf{x}\| = \sqrt{x_1^2 + x_2^2 + \cdots x_{n-1}^2 + x_n^2}$.

Definition 1 (Lattice [29]): Given n-linearly independent vectors $\mathbf{v_1}, \mathbf{v_2}, \cdots, \mathbf{v_n} \in \mathbb{R}^m$, lattice L generated by them is the set of vectors

$$\mathbf{L}(\mathbf{v_1}, \mathbf{v_2}, \cdots, \mathbf{v_n}) = \left\{ \sum_{i=1}^{n} a_i \mathbf{v_i} \,|a_i \in \mathbb{Z}, i = 1, \cdots, n \right\} \quad (1)$$

$V = [\mathbf{v_1}, \mathbf{v_2}, \cdots, \mathbf{v_n}]$ is known as a basis of the lattice L. The same lattice can be represented by different lattice bases. Given a prime number q,a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, define:

$$\Lambda_q(\mathbf{A}) = \left\{ y \in \mathbb{Z}^m \,\middle|\, y = \mathbf{A}^T \mathbf{x} \bmod q, \mathbf{x} \in \mathbb{Z}^n \right\}, \quad (2)$$

$$\Lambda_q^{\perp}(\mathbb{A}) = \left\{ y \in \mathbb{Z}^m \,|\mathbf{A}y = 0 \bmod q \right\}. \quad (3)$$

Definition 2 (Lattice SIS Problem): Given an integer q, a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, and a real constant $v > 0$, find a nonzero vector $\mathbf{x} \in \mathbb{Z}^m$ such that $\mathbf{Ax} \equiv 0 \bmod q$ and $\|\mathbf{x}\| \leq v$.

Based on the hardness of SIS problem, for any polynomial-bounded m, v and any prime $q \geq v \cdot \omega\sqrt{n \log n}$, solving SIS on the average is as hard as approximating the shortest independent vector problem (SIVP) in the worst case.

Definition 3 ([30] Smoothing Parameter): For an m-dimensional lattice $\mathbf{\Lambda}$, and positive real $\varepsilon > 0$. Its smoothing parameter $\eta_\varepsilon(\mathbf{\Lambda})$ is the smallest s such that $\rho_{1/s}(\Lambda^* \setminus \{0\}) \leq \varepsilon$.

C. TRAPDOOR AND LEMMAS

Lemma 1 [19]: For a lattice L with dimensional m and rank n, $\mathbf{c} \in \mathbb{R}^m$, positive real $\varepsilon < \exp(-4\pi)$ and $s \geq \eta_\varepsilon(L)$, for random $\mathbf{x} \in L$ such that $D_{L,s,\mathbf{c}}(\mathbf{x}) \leq \frac{1+\varepsilon}{1-\varepsilon} 2^{-n}$.

Lemma 2 [30]: For any lattice L with dimensional m and rank n, $\mathbf{c} \in span(L)$, a real $\varepsilon \in (0, 1)$, $s \geq \eta_\varepsilon(L)$, we have

$$\Pr_{\mathbf{x} \leftarrow D_{L,s,c}} \left[\|\mathbf{x} - \mathbf{c}\| > s\sqrt{m} \right] \leq \frac{1+\varepsilon}{1-\varepsilon} 2^{-n}. \quad (4)$$

Gentry et al. proposed an algorithm *SampleD* that samples from a discrete Gaussian over any lattice. *SampleD* takes some n-dimensional basis $\mathbf{A} \in \mathbb{Z}^{n \times m}$ of rank m, Gaussian parameter s that is related to the length $\|\mathbf{A}\|$ of the basis, a center $\mathbf{c} \in \mathbb{R}^n$, and efficiently outputs a sample from (a distribution close to) $D_{L(\mathbf{A}),s,\mathbf{c}}$.

Lemma 3 [19]: For any lattice basis $\mathbf{A} \in \mathbb{Z}^{m \times n}$, any real $s \geq \|\mathbf{A}\| \, \omega(\sqrt{\log n})$ and any $\mathbf{c} \in \mathbb{R}^m$, the output distribution of *SampleD*($\mathbf{A}$, s, $\mathbf{c}$) is within negligible statistical distance of $D_{\mathbf{L(A)},s,\mathbf{c}}$.

Lemma 4 [19]: Let $q > 2$, a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and $\mathbf{B}$ is a basis of $\Lambda_q^{\perp}(\mathbf{A})$, and Gaussian parameter $s \geq ||\tilde{\mathbf{B}}|| \omega(logm)$. Then any vector $\mathbf{y} \in \mathbb{Z}_q^n$, algorithm *SamplePre*($\mathbf{A}$, $\mathbf{B}$, $\mathbf{y}$, s) outputs a vector $\mathbf{e} \in Z_q^m$ from a distribution that is statistically close to $D_{\Lambda_q^{\perp}(\mathbf{A}),s}(x)$.

Lemma 5 [19]: For any prime $q = poly(n)$ and any $m \geq 5n \lg q$, there is a probabilistic polynomial-time algorithm *TrapGen*(1^n) that outputs a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and a full-rank set $\mathbf{S} \subset \Lambda^{\perp}(\mathbf{A}, q)$. The distribution of $\mathbf{A}$ is statistically close to uniform over $\mathbb{Z}_q^{n \times m}$ and the length $\|\mathbf{S}\| \leq L = m^{1+\varepsilon} \wedge \varepsilon > 0$.

Lemma 6 [24]: Given a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and an m-dimensional lattice $\Lambda_q^{\perp}(\mathbf{A})$, then input a basis $\mathbf{T}$ of the lattice $\Lambda_q^{\perp}(\mathbf{A})$ which has nonsingular matrix $\mathbf{R} = \mathbf{T}^{-1}$ and $\mathbf{R} \in \mathbb{Z}^{m \times m}$, input a Gaussian parameter $s \geq \left\|\tilde{\mathbf{T}}\right\| m^d \omega(\lg^{d+1}(m))$, *BasisDel*($\mathbf{A}$, $\mathbf{R}$, $\mathbf{T}$, s) can output a basis $\mathbf{B}$ of $\Lambda^{\perp}(\mathbf{AR}^{-1})$ with overwhelming probability $\left\|\tilde{\mathbf{B}}\right\| \leq s\sqrt{m}$.

III. CRYPTOCURRENCY SCHEME BASED ON PQB

We firstly present the definition of post-quantum blockchain. Then we introduce our proposed signature scheme based on lattice. Finally, we provide a secure cryptocurrency scheme based on PQB that can resist quantum computing attacks.

A. FORMAL DEFINITION AND SECURITY MODEL

Definition 4: The signature scheme in this paper consists of four algorithms as follows:

Setup(n): Input a security parameter n, the *Setup*algorithm outputs the master secret key MK and public parameters PP.

KeyGen(PP, MK, ms): Input the public parameters PP, the master secret key MK and an identity ms, the *KeyGen*algorithm outputs a signing key skcorresponding with ms.

Sign(PP, msg, sk, ms): Input the public parameters PP, a message msg and a signing key $sk$of the user with identity ms, the *Sign*algorithm outputs a signature e.

Verify(PP, msg, e, ms): Input the public parameters PP, a signature e, a message $msg$and an identity ms, the *Verify*algorithm outputs 1 if the signature e is valid and 0 otherwise.

Definition 5: The security model of our scheme which is existentially unforgeable against chosen message is described by the following game.

Setup. The challenger C runs the algorithm *Setup*(n) to generate public parameters $PP$and MK, and sends PP to the adversary A.

Private key query. Adversary A issues a query on identity ms, the challenger C runs the algorithm *KeyGen*(PP, MK, ms) and returns a signing key $sk$to adversary A.

Sign query. Adversary A issues a query on message $msg$and identity ms, the challenger C runs the algorithm *Sign*(PP, msg, sk, ms) and returns a signature e to adversary A.

Forgery. The adversary A outputs a signature e of message msg, A wins the game if:

(i) *Verify*(PP, e, msg, ms) $= 1$.

(ii) (e, msg, ms) has never been submitted to sign query.

B. POST-QUANTUM BLOCKCHAIN

This paper is concerned with the study on the security of blockchain. As described in Section I, Quantum computing attack seriously threatens the security of blockchain, and related research is still less. Therefore, in this paper, we use post-quantum cryptography to enhance the security of blockchain. At first, we give the definition of post-quantum blockchain.

Definition 6 (PQB): PQB is a secure blockchain technology which combines post-quantum cryptography and blockchain technology together. This means that PQB not only has the advantages of blockchain but also can resist attacks by quantum computer effectively. We think PQB should satisfy these following four conditions.

(1) PQB is a combination of post-quantum cryptography and blockchain technology;

(2) PQB is able to resist known classical attack methods;

(3) PQB is able to resist the known quantum algorithm attacks, such as Shor algorithm, Grover algorithm;

(4) Signature scheme in PQB has the linkable or traceable property.

Besides, post-quantum cryptography includes Hash function-based cryptography, Lattice-based cryptography, Code-based cryptography, Multivariate cryptography and other post-quantum cryptography algorithms. By using these algorithms, PQB can resist the quantum computing attack and guarantee the security of secret keys.

Definition 7: The security model of PQB scheme is described by the following content.

Step1: *Setup*(n) User A inputs a security parameter n, the *Setup*algorithm outputs the master secret key MK and public parameters PP.

Step2: *KeyGen*(PP, MK, ms) A inputs the public parameters PP, the master secret key MK and an identity ms, the *KeyGen*algorithm outputs public key and private key (pk_a, sk_a), and pk_a has been used to receive the cryptocurrency by Alice in transaction $tx1$. User B generates his own public key and private key (pk_b, sk_b) by the above step.

Step3: B transmits his public key pk_b to A.

Step4: A uses pk_b and $tx1$ to generate message M, then A publishes the public parameters PP.

Step5: *Sign*(PP, sk_a, M) A inputs the public parameters PP, message M and a signing key sk_a, the *Sign*algorithm outputs a signature e.

Step6: A uses the signature e and pk_b to generate transaction$tx2$ and transmits it in the P2P network.

Step7: *Verify*(PP, pk_a, M, e) Miners verify the correctness of the signature e and whether transaction $tx2$ satisfies UTXO. If the above conditions are satisfied, the transaction $tx2$ is included in a new block.

On one hand, it is necessary to ensure the security of signing key. On the other hand, the signatures are linkable so that each transaction can be traced for preventing double spending. Therefore, in the PQB, if there is a quantum algorithm which can return a signing key sk_a to adversary A. and A can use it to generate a legal signature. Or if user A has issued a transaction $tx2$ by signing the hash of transaction $tx1$. Then, A can issue a new transaction $tx2'$ by signing the hash of transaction $tx1$ again without being discovered. We consider this PQB scheme is not secure.

C. SIGNATURE SCHEME BASED ON LATTICE

In this section, we will describe our signature scheme based on lattice. We use $\mathbb{R}, \mathbb{Z}, \mathbb{Z}^+$ to denote the set of all reals, the set of integers and the set of positive integer respectively. The security parameter is a positive integer n, q is a prime and $q \geq 2$, $m \geq 5n \lg q$, and $H : \{0,1\}^* \rightarrow \mathbb{Z}_q^{m \times m}$ is a collision-resistant hash function. The scheme is described as follows.

Setup(1^n)*:* Sender selects a security parameter n.

(1) According to lemma 5, sender uses *TrapGen*(1^n) to generate a uniformly random matrix $\mathbf{A_0} \in \mathbb{Z}_q^{n \times m}$ with a corresponding short basis $\mathbf{S}_0 \in \Lambda^{\perp}(\mathbf{A_0}, q)$. $\mathbf{S}_0 \in \mathbb{Z}_q^{m \times m}$ is sender's master key $MK = \mathbf{S}_0$.

(2) The hash function that takes as input the message msg, outputs $M = H(msg)$ and $M \in \{0,1\}^d$, d is the length of message M. Sender selects random and independent vectors

$\mathbf{C_1}, \mathbf{C_2}, \cdots, \mathbf{C_d} \in \mathbb{Z}_q^n$. Sender obtains the public parameter $PP = \langle \mathbf{A_0}, \mathbf{C_1}, \mathbf{C_2}, \cdots, \mathbf{C_d} \rangle$.

KeyGen(PP,ms,MK): Sender selects a random message ms and inputs master key MK, public parameter PP and Gaussian parameter s.

Using basis delegation technique in lemma 6, sender runs $BasisDel(\mathbf{A_0}, \mathbf{H(ms)}, \mathbf{S_0}, s)$ to output sender's private key $\mathbf{S}_{ms}$ for signing the message. In addition, $\mathbf{S}_{ms}$ is a basis of $\mathbf{\Lambda}^{\perp}(\mathbf{A_0H(ms)}^{-1})$, and the public key which correspond with private key is $\mathbf{A_1} = \mathbf{A_0H(ms)}^{-1}$.

$Sign(PP, \mathbf{S}_{ms}, M)$: The sender does as follows.

(1) Uniform random select $t \in D = \left\{ t \in R \left| \|t\|^{-1} \leq s \right. \right\}$, then do $\mathbf{u} \leftarrow SampleD(\mathbf{A}_1, s)$.

(2) Compute $\boldsymbol{\mu} = t \sum_{i=1}^{d} (-1)^{M[i]} \mathbf{C}_i + \mathbf{A}_1\mathbf{u}$ and output $\boldsymbol{\mu}$.

(3) According to lemma 4, sender uses algorithm $SamplePre(\mathbf{A}_1, \mathbf{S}_{ms}, \boldsymbol{\mu}, s)$ to obtain the first-signature $\mathbf{e}' \in \mathbb{Z}_q^m$.

(4) Verify $\left\|\mathbf{e}'\right\| \leq s\sqrt{m}$ and $\mathbf{e}' \neq \mathbf{0}$. From lemma 2 and lemma 4, we know it is satisfied with overwhelming probability. If it is not satisfied, sender returns back and selects t again.

(5) Compute $\mathbf{e} = t^{-1}(\mathbf{e}' - \mathbf{u})$, and $\mathbf{e}$ is the last-signature of message me.

$Verify(PP, \mathbf{A}_1, msg, \mathbf{e})$: Every users can verify the correctness of $(msg, \mathbf{e})$ as follows.

(1) Verify $\mathbf{e} \neq \mathbf{0}$ and $\|\mathbf{e}\| \leq 2s^2\sqrt{m}$.

(2) Verify $\mathbf{A}_1\mathbf{e} = \sum_{i=1}^{d} (-1)^{M[i]} \mathbf{C}_i$.

(3) Verify $M = H(msg)$.

If the above equations are satisfied, it means that the signature is the generated by the sender, otherwise this output is rejected.

Our lattice-based signature scheme is introduced in Section III-C. We use and modify the model of identity-based signature scheme. In our scheme, there is no the third party and users generate their secret keys with selecting a random value. By using this key generation method in the blockchain, four advantages are summarized below:

(1) Generating the user's public key and private key based on the random value increases the security of the private key.

(2) It is hard for adversary Eve to forge a valid signature which will be analyzed in Section IV-B.

(3) Users are anonymous in the blockchain, our scheme does not use identity information which can weaken the role of identity information in the signature scheme and protect users' privacy.

(4) The users can obtain a large number of keys for transactions which is practical in application.

In addition, we also design the first-signature $\mathbf{e}'$ and last-signature $\mathbf{e}$ in our scheme, and we define them as double-signature. The first-signature is generated by the forward sampling algorithm. Then users perform to signature recovery operation get the last-signature $\mathbf{e} = t^{-1}(\mathbf{e}' - \mathbf{u})$. This fuzzy processing can reduce the correlation between message and corresponding signature.

D. SECURE CRYPTOCURRENCY SCHEME BASED ON POST-QUANTUM BLOCKCHAIN

The proposed lattice-based signature scheme was introduced in Section III-C. According to the definition of PQB we presented in Section III-B, by combining the proposed signature scheme with blockchain together, we provide a secure cryptocurrency scheme and use it to complete a transaction between Alice and Bob.

We suppose that Alice and Bob trade through cryptocurrency scheme based on PQB, and Alice transfers her cryptocurrency to Bob. We use $\mathbb{R}, \mathbb{Z}$ to denote the set of all reals and the set of integers, n denotes the security parameter and $n \in \mathbb{Z}^+$. q is a prime and $q \geq 2$, $m \geq 5n \lg q$. $H : \{0,1\}^* \rightarrow \mathbb{Z}_q^{m \times m}$ is a collision-resistant hash function.

Step1: $Setup(1^n)$ Alice selects a security parameter n to run $TrapGen(1^n)$. According to the lemma 5, Alice generates a matrix $\mathbf{A_0} \in \mathbb{Z}_q^{n \times m}$ and corresponding short basis $\mathbf{S}_0 \in \Lambda^{\perp}(\mathbf{A_0}, q)$, which $\mathbf{S}_0 \in \mathbb{Z}_q^{m \times m}$ is Alice's master key $MK = \mathbf{S}_0$.

Step2: $KeyGen(PP, ms, MK)$ Alice selects a random value ms, then she can use lattice basis delegation algorithm $BasisDel(\mathbf{A_0}, \mathbf{H(ms)}, \mathbf{S}_0, s)$ to output her public key pk_a and private key sk_a, and pk_a has been used to receive the cryptocurrency by Alice in transaction $tx1$. Bob generates his own public key and private key (pk_b, sk_b) by the above steps. Then, Alice transfers her cryptocurrency to Bob with transaction $tx2$ as the follows.

Step3: Bob transmits his public key pk_b to Alice.

Step4: Alice computes $M = H(tx1, pk_b)$, the message $M \in \{0,1\}^d$, d is the length of M. Alice selects random and independent vectors $\mathbf{C_1}, \mathbf{C_2}, \cdots, \mathbf{C_d} \in \mathbb{Z}_q^n$, then Alice publishes the public parameter $PP = \langle \mathbf{A_0}, \mathbf{C_1}, \mathbf{C_2}, \cdots, \mathbf{C_d} \rangle$.

Step5: $Sign(PP, sk_a, M)$ Alice signs message M as follows.

(1) Select a random $t \in D = \{t \in R \,|\, \|t\| \geq 1/s\}$, and use sampling algorithm $SampleD(pk_a, s)$ to generate a vector $\mathbf{u}$.

(2) Compute $\boldsymbol{\mu} = t \sum_{i=1}^{d} (-1)^{M[i]} \mathbf{C_i} + pk_a\mathbf{u}$.

(3) Use algorithm $SamplePre(pk_a, sk_a, \boldsymbol{\mu}, s)$ to output the first-signature $\mathbf{e}' \in \mathbb{Z}_q^m$.

(4) Verify $\left\|\mathbf{e}'\right\| \leq s\sqrt{m}$ and $\mathbf{e}' \neq 0$. According to lemma 2 and lemma 4, we know it is satisfied with overwhelming probability. If it is not satisfied, Alice selects t again.

(5) Compute the last-signature $\mathbf{e} = t^{-1}(\mathbf{e}' - \mathbf{u})$.

Step6: Alice uses the signature $(\mathbf{e}, M)$ and pk_b to generate transaction$tx2$ and transmits it in the whole P2P network.

Step7: $Verify(PP, pk_a, M, e)$ Miners in the P2P network get this transaction$tx2$ and then verify the signature in it as the follows.

Miners verify

$$\|\mathbf{e}\| \leq 2s^2\sqrt{m} \wedge \mathbf{e} \neq \mathbf{0}, \tag{5}$$

and

$$pk_a\mathbf{e} = \sum_{i=1}^{d} (-1)^{M[i]} \mathbf{C}_i, \tag{6}$$

If these above equations (5) and (6) are satisfied, and $M = H(tx1, pk_b)$. It is shown that this signature is generated by Alice, otherwise the output is rejected. Miners verify whether transaction $tx2$ satisfies UTXO, then they include transaction $tx2$ in a new block. Through the blockchain consensus mechanism, miners compete for the right to add this block to chain.

Step8: By using consensus mechanism, miners can communicate among themselves and agree on a common set of validated transactions to be added to the ledger. The miner who gets the right to produce new block will be compensated.

Step9: When five blocks are added to the chain after this block, transaction$tx2$ will be confirmed. Then, Bob can get the cryptocurrency and spend it by using corresponding private key sk_b as the above steps.

IV. ANALYSIS

As we described in Section I, public-key cryptography plays a very fundamental role in the security of blockchain which is used for information encryption and identity authentication. In addition, the public key is used as the receiving address of the cryptocurrency and private key is used to manage and spend cryptocurrency. We consider that relationship between public-key cryptography and the security of blockchain is very close. Specifically, public-key cryptography is of great significance to the security of blockchain.

According to the definition of PQB in Section III-B, we use this signature scheme based on lattice as the public-key cryptography in PQB. The security of PQB is mostly equivalent to the security of our signature scheme, and so is our cryptocurrency scheme. Therefore, in Section IV, we analyze the cryptocurrency scheme in detail from correctness, one-more unforgeability, security and efficiency.

A. CORRECTNESS

Theorem 1: Our cryptocurrency scheme satisfies correctness.

Proof: The signature verification process is divided into two steps, and the correctness of an honest signature information is verified as follows.

The last-signature $\mathbf{e} = t^{-1}(\mathbf{e}' - \mathbf{u})$ and $\|\mathbf{e}\| = \left\|t^{-1}(\mathbf{e}' - \mathbf{u})\right\|$. According to lemma 3 and lemma 4, we have $\|\mathbf{u}\| \le s\sqrt{m}$ and $\left\|\mathbf{e}'\right\| \le s\sqrt{m}$. And $\|t\|^{-1} \le s$, so we have

$$\|\mathbf{e}\| \le \|t\|^{-1}\left(\left\|\mathbf{e}'\right\| + \|\mathbf{u}\|\right) \le 2s^2\sqrt{m}. \tag{7}$$

For $\mathbf{A}_1(t^{-1}(\mathbf{e}' - \mathbf{u})) = t^{-1}(\mathbf{A}_1\mathbf{e}' - \mathbf{A}_1\mathbf{u})$, according to the lemma 4, the output $\mathbf{e}' \leftarrow SamplePre(\mathbf{A}_1, \mathbf{S}_{ms}, \boldsymbol{\mu}, s)$ satisfies $\mathbf{A}_1\mathbf{e}' = \boldsymbol{\mu}$. Thus we have $\boldsymbol{\mu} = t\sum_{i=1}^{d}(-1)^{M[i]}\mathbf{C}_i + \mathbf{A}_1\mathbf{u}$ and $\mathbf{A}_1\mathbf{e} = t^{-1}(\boldsymbol{\mu} - \mathbf{A}_1\mathbf{u})$. So

$$\begin{aligned}\mathbf{A}_1\mathbf{e} &= \mathbf{A}_1(t^{-1}(\mathbf{e}' - \mathbf{u})) = t^{-1}(\mu - \mathbf{A}_1\mathbf{u}) \\ &= t^{-1}(t\sum_{i=1}^{d}(-1)^{M[i]}\mathbf{C}_i + \mathbf{A}_1\mathbf{u}) - t^{-1}\mathbf{A}_1\mathbf{u} \\ &= \sum_{i=1}^{d}(-1)^{M[i]}\mathbf{C}_i. \end{aligned} \tag{8}$$

Through the analysis of the above equations (7) and (8), it is proved that the proposed cryptocurrency scheme satisfies the correctness and the signer can not deny his signature.

B. ONE-MORE UNFORGEABILITY

Juels *et al.* [31] and Pointcheval and Stern [32] analyzed the security of the signature scheme, and it needs to satisfy one-more unforgeability. If an adversary Eve exchanges the messages with an honest signer l times and gets l signatures, the probability of Eve forges a new $l+1$ message's valid signature is negligible, it means this signature scheme satisfies one-more unforgeability.

Theorem 2: The proposed signature scheme is existentially unforgeable against adaptive chosen message, assuming the hardness of lattice SIS problem.

Proof: Assume Eve is a polynomial-time adversary who can break our signature scheme and successfully forge a legitimate signature, the probability of success is ε. We construct a polynomial-time algorithm T who can use the adversary Eve as a subroutine to solve the lattice SIS problem with non-negligible probability. Algorithm T does so by interacting with the adversary Eve as follows.

Setup. Algorithm T does as follows.

(1) Select a random matrix $\mathbf{B} \in \mathbb{Z}_q^{n\times m}$ and corresponding short basis $\mathbf{T}_0 \in \Lambda^{\perp}(\mathbf{B})$.

(2) Select a matrix $\mathbf{R_1} \sim D_{m\times m}$, then run algorithm $BasisDel(\mathbf{B}, \mathbf{R_1}, \mathbf{T}_0, s)$ to put out a lattice basis $\mathbf{S}_0$ of $\Lambda^{\perp}\left(\mathbf{B}\mathbf{R}_1^{-1}\right)$.

By using $SampleD(\mathbf{B}, s)$, Algorithm T selects d random vectors $\mathbf{E_1}, \mathbf{E_2}, \cdots, \mathbf{E_d} \in \mathbb{Z}_q^m$ and these vectors $\mathbf{BE}_i$ distribution of $SampleD(\mathbf{B}, s, \mathbf{c})$ is within negligible statistical distance of $D_{\mathbf{L(B)},s,\mathbf{c}}$.

(3) Select $q_e - 1$ nonsingular matrices $\mathbf{R}_2, \mathbf{R}_3, \cdots, \mathbf{R}_{q_e} \sim D_{m\times m}$. Let $\mathbf{C}_i = \mathbf{BE}_i$, $\mathbf{A}_0 = \mathbf{BR}_1^{-1}$, the public parameter $PP = \langle \mathbf{A_0}, \mathbf{C_1}, \mathbf{C_2}, \cdots, \mathbf{C_d}\rangle$, master key is MK.

Private key queries. Selecting many random messages ms_x, $x = 1, 2, \cdots, q_e$, algorithm T computes $\mathbf{H}(\mathbf{ms_x}) = \mathbf{R}_x^{-1}$ and runs $BasisDel(\mathbf{A_0}, \mathbf{H}(\mathbf{ms_x}), \mathbf{S}_0, s)$ to generate corresponding private key $\mathbf{S}_x$, and sends $(\mathbf{A_0H}(\mathbf{ms_x})^{-1}, \mathbf{S}_x)$ to Eve.

Signature queries. Algorithm T selects the transactions of $\mathbf{A_0H}(ms_x)^{-1}$, and gets $\boldsymbol{\mu}_M$ of message M. Eve issues such a query on $(\boldsymbol{\mu}_M, \mathbf{A_0H}(\mathbf{ms_x})^{-1}, \mathbf{S}_i)$, runs algorithm $SamplePre$ to obtain $\mathbf{e}'_M \leftarrow SamplePre(\mathbf{A_0H}(\mathbf{ms_x})^{-1}, \mathbf{S}_i, \boldsymbol{\mu}_M, s)$.

Then algorithm T verifies $\left\|\mathbf{e}'_M\right\| \le s\sqrt{m}$. If it is satisfied, algorithm T holds the tuple $(ms_x, \boldsymbol{\mu}_M, \mathbf{e}'_M)$ and outputs the

first-signature $\mathbf{e}'_M$ to adversary Eve. By recovery operation, Eve gets the last-signature $(\mathbf{A_0H}(\mathbf{ms_x})^{-1}, M, \mathbf{e}_M)$.

Forgery. We suppose after a finite number of private key extraction queries and signature queries, adversary Eve can forge a signature $(\mathbf{A_0H}(\mathbf{ms_x})^{-1}, M, \mathbf{e}_M)$. It can be reduced to find a solution of the SIS problem, Adversary Eve succeeded in forging valid signature with the probability of ε.

According to our signature scheme, we know that the valid signature should satisfy the following equations

$$\|\mathbf{e}_M\| \leq 2s^2\sqrt{m} \wedge \mathbf{e}_M \neq \mathbf{0} \tag{9}$$

and

$$\mathbf{A_0H}(\mathbf{ms_x})^{-1}\mathbf{e}_M = \sum_{i=1}^{d}(-1)^{M[i]}\mathbf{C}_i. \tag{10}$$

Because $\mathbf{A_0H}(\mathbf{ms_x})^{-1} = \mathbf{BR}_x^{-1}\mathbf{R}_x = \mathbf{B}$ and $\mathbf{C}_i = \mathbf{BE}_i$, so we have

$$\mathbf{Be}_M = \mathbf{B}\sum_{i=1}^{d}(-1)^{M[i]}\mathbf{E}_i, \tag{11}$$

$$\mathbf{B}(\mathbf{e}_M - \sum_{i=1}^{d}(-1)^{M[i]}\mathbf{E}_i) = 0 mod q. \tag{12}$$

So we can have

$$\left\|\mathbf{e}_M - \sum_{i=1}^{d}(-1)^{M[i]}\mathbf{E}_i\right\| \leq \|\mathbf{e}_M\| + \left\|\sum_{i=1}^{d}(-1)^{M[i]}\mathbf{E}_i\right\| \leq 3s^2\sqrt{m}. \tag{13}$$

Because this solution is a non-zero solution to SIS problem with $(q, m, 3s^2\sqrt{m}, \mathbf{B})$, by the preimage min-entropy property, this non-zero solution with probability no less than $1 - 2^{-\omega(\lg m)}$. Adversary Eve succeeded in forging a valid signature with the probability of ε, and $pro(i = 1) = q_e^{-1}$. So the non-zero solution to this $SIS_{q,m,3s^2\sqrt{m},\mathbf{B}}$ problem with negligible probability $\left(1 - 2^{-\omega(\lg m)}\right) q_e^{-1}\varepsilon$.

On the other hand, in our proposed scheme, sender inputs a random value *ms*, master key *MK*, public parameter *PP*, Gaussian parameter *s* and uses basis delegation technique in lemma 6 to generate his secret keys. Because the *ms* is a random value and users can generate new secret keys easily for every transaction, just like one-time padding. In private key queries, only if adversary Eve obtains this value *ms*, can he forge a signature with the probability of ε.

Through the above analyses, adversary Eve forges a valid signature of message with negligible probability, and this scheme satisfies one-more unforgeability under the lattice SIS assumption. This completes the proof.

C. SECURITY

Through the researches on the lattice problems, many achievements have been obtained. The security of lattice-based cryptography depends on intractability of lattice problem, and many researchers have proven that some lattice problems are non-deterministic polynomial-hard (NP-hard). NP-hard means there is no efficient polynomial-time algorithm to crack the problem. In particular, Lattice-based cryptography is generally considered to have the advantage of resisting quantum computing attacks, and it can deal with the threat of quantum computer in the future. By using the theory of random lattice and the corresponding lattice basis, Gentry et al. presented new cryptographic constructions. He proposed a forward sampling trapdoor algorithm based on lattice SIS problem. And it has been proven to be able to resist quantum computing attacks

On one hand, in our proposed cryptocurrency scheme, we use short lattice delegation algorithm to generate user's secret keys. Then we sign the message by the preimage sampling algorithm with trapdoor, which is based on lattice problem $SIS_{s\sqrt{m}}$. Additionally, the lattice SIS problem in average-case can be reduced to the SIVP in the worst-case, and the lattice problem which is used in our scheme is able to resist quantum computing attacks. Therefore, it is shown that our cryptocurrency scheme based on PQB can resist quantum computing attacks.

On the other hand, as shown in step 7 and step 9 of our cryptocurrency scheme, the signatures are used to establish a link between these transactions. In this way, signatures are linkable so that every transaction can be traced, so double spending can be prevented in our cryptocurrency scheme.

D. EFFICIENCY

The efficiency of signature scheme mainly depends on the sizes of public key, signing key and signature. In the following content, $n \in \mathbb{Z}^+$, q is a prime number and $q \geq 2$, n, m, d denote security parameter, dimensional of lattice and the length of message, respectively.

TABLE 1. Comparison of lattice-based signature scheme.

Scheme	Public key size	Signing key size	Signature size	Security model
Ref.[23]	$3nm\log q$	$5m^2\log q$	$2m\log q$	Random oracle model
Ref.[25]	$3nm\log q$	$2m(m\text{-}n)\log q$	$3m\log q$	Random oracle model
Ref.[26]	$(mn+dm)\log q$	$m^2\log q$	$2m\log q$	Standard model
Ref.[27]	$nm\log q$	$m^2\log q$	$m\log q$	Random oracle model
Our work	$(mn+dm)\log q$	$m^2\log q$	$m\log q$	Standard model

The proposed signature scheme underlying the cryptocurrency scheme mainly adopts simple linear operations such as modular multiplication and modular addition, its computation efficiency is higher obviously. We provide the comparison of several lattice-based signature schemes in Table 1. As shown in Table 1, the sizes of public key, signing key and signature in our scheme are shorter than that in [23] and [25]. The signature size in our scheme is shorter than that in [26]. Compared with [27], our signature scheme has the advantage of provably security in the standard model. In summary, the proposed

signature scheme has relatively shorter signature and secret keys, which can decrease computational complexity of our proposed cryptocurrency scheme. Besides, it has the advantage of provably security in the standard model. Therefore, our cryptocurrency scheme is more secure and efficient.

V. CONCLUSIONS

We should actively deal with the threat of powerful parallel computing power that quantum computer has in the future. In section III, we present the definition of the post-quantum blockchain and introduce the proposed signature scheme based on lattice. Finally, we provide a secure cryptocurrency scheme. In section IV, we analyze this proposed cryptocurrency scheme. Its signature satisfies the correctness, one-more unforgeability under the SIS assumption. Moreover, the sizes of signature and secret keys are shorter so that it can decrease computational complexity of the proposed cryptocurrency scheme. In addition, the security of our scheme depends on the lattice problem SIS, it is shown that cryptocurrency scheme can resist quantum computing attacks. Compared with original cryptocurrency scheme, user's private key has the advantage of resisting quantum computing attack. In other words, cryptocurrency is more secure in this cryptocurrency scheme. It is shown that our cryptocurrency scheme is more secure and efficient. Our research will help us to protect the security of blockchain, which will be more practical under the present technical conditions. We also believe that the post-quantum blockchain is very significant for other blockchain applications in the future.

REFERENCES

[1] H. Li, D. Liu, Y. Dai, T. H. Luan, and X. S. Shen, "Enabling efficient multi-keyword ranked search over encrypted mobile cloud data through blind storage," *IEEE Trans. Emerg. Topics Comput.*, vol. 3, no. 1, pp. 127–138, Mar. 2015.
[2] H. Li, D. Liu, Y. Dai, T. H. Luan, and S. Yu, "Personalized search over encrypted data with efficient and secure updates in mobile clouds," *IEEE Trans. Emerg. Topics Comput.*, vol. 6, no. 1, pp. 97–109, Jan./Mar. 2018.
[3] H. Li, Y. Yang, Y. Dai, J. Bai, S. Yu, and Y. Xiang, "Achieving secure and efficient dynamic searchable symmetric encryption over medical cloud data," *IEEE Trans. Cloud Comput.*, to be published, doi: 10.1109/TCC.2017.2769645.
[4] X. Liu, S. Li, X. Chen, G. Xu, X. Zhang, and Y. Zhou, "Efficient solutions to two-party and multiparty millionaires' problem," *Secur. Commun. Netw.*, vol. 2017, May 2017, Art. no. 5207386, doi: 10.1155/2017/5207386.
[5] X. Liu, S. Li, J. Liu, X. Chen, and G. Xu, "Secure multiparty computation of a comparison problem," *SpringerPlus*, vol. 5, no. 1, p. 1489, 2016.
[6] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[7] P. Giungato, R. Rana, A. Tarabella, and C. Tricase, "Current trends in sustainability of bitcoins and related blockchain technology," *Sustainability*, vol. 9, no. 12, p. 2214, 2017.
[8] C. Decker and R. Wattenhofer, "Information propagation in the bitcoin network," in *Proc. IEEE 13th Int. Conf. Peer-Peer Comput. (P2P)*, Trento, Italy, Sep. 2013, pp. 1–10.
[9] G. Zyskind and O. Nathan, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Secur. Privacy Workshops (SPW)*, San Jose, CA, USA, May 2015, pp. 180–184.
[10] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, "The blockchain as a decentralized security framework," *IEEE Consum. Electron. Mag.*, vol. 7, no. 2, pp. 18–21, Mar. 2018.
[11] A. Anjum, M. Sporny, and A. Sill, "Blockchain standards for compliance and trust," *IEEE Cloud Comput.*, vol. 4, no. 4, pp. 84–90, Jul. 2017.
[12] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
[13] I. Eyal, "Blockchain technology: Transforming libertarian cryptocurrency dreams to finance and banking realities," *Computer*, vol. 50, no. 9, pp. 38–49, 2017.
[14] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. IEEE 35th Annu. Symp. Found. Comput. Sci.*, Santa Fe, NM, USA, Nov. 1994, pp. 124–134.
[15] C. Cheng, R. Lu, A. Petzoldt, and T. Takagi, "Securing the Internet of Things in a quantum world," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 116–120, Feb. 2017.
[16] K. Lauter, "Postquantum opportunities: Lattices, homomorphic encryption, and supersingular isogeny graphs," *IEEE Security Privacy*, vol. 15, no. 4, pp. 22–27, Aug. 2017.
[17] M. Ajtai, "Generating hard instances of lattice problems," in *Proc. 28th Annu. ACM Symp. Theory Comput.*, Philadelphia, PA, USA, May 1996, pp. 99–108.
[18] M. Ajtai, "Generating hard instances of the short basis problem," in *International Colloquium on Automata, Languages, and Programming*. Berlin, Germany: Springer, Jul. 1999, pp. 1–9.
[19] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proc. 14th Annu. ACM Symp. Theory Comput.*, Victoria, BC, Canada, May 2008, pp. 197–206.
[20] M. Rückert, "Lattice-based blind signatures," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, Dec. 2010, pp. 413–430.
[21] M. Rückert, "Strongly unforgeable signatures and hierarchical identity-based signatures from lattices without random oracles," in *Proc. Int. Workshop Post-Quantum Cryptogr.*, May 2010, pp. 182–200.
[22] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, "Bonsai trees, or how to delegate a lattice basis," *J. Cryptol.*, vol. 25, no. 4, pp. 601–639, 2010.
[23] L. L. Zhang and Y. Sang, "A lattice-based identity-based proxy signature from bonsai trees," *Int. J. Adv. Comput. Technol.*, vol. 4, no. 20, pp. 99–104, 2012.
[24] S. Agrawal, D. Boneh, and X. Boyen, "Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE," in *Proc. Adv. Cryptol. Conf. CRYPTO*, Santa Barbara, CA, USA, Aug. 2010, pp. 98–115.
[25] L. Zhang and Y. Sang, "Proxy blind signature scheme from lattice basis delegation," *Int. J. Adv. Comput. Technol.*, vol. 4, no. 21, pp. 329–336, 2012.
[26] L. Zhang and Y. Ma, "A lattice-based identity-based proxy blind signature scheme in the standard model," *Math. Problems Eng.*, vol. 2014, Sep. 2014, Art. no. 307637.
[27] C. Gu, L. Chen, and Y. Zheng, "ID-based signatures from lattices in the random oracle model," in *Proc. Int. Conf. Web Inf. Syst. Mining*, Oct. 2012, pp. 222–230.
[28] J. Yan, L. Wang, M. Dong, Y. Yang, and W. Yao, "Identity-based signcryption from lattices," *Secur., Commun. Netw.*, vol. 8, no. 18, pp. 3751–3770, 2015.
[29] D. Micciancio and O. Regev, "Lattice-based cryptography," in *Post-Quantum Cryptography*. Berlin, Germany: Springer, 2009, pp. 147–191.
[30] D. Micciancio and O. Regev, "Worst-case to average-case reductions based on Gaussian measures," *SIAM J. Comput.*, vol. 37, no. 1, pp. 267–302, 2007.
[31] A. Juels, M. Luby, and R. Ostrovsky, "Security of blind digital signatures," in *Proc. Annu. Int. Cryptol. Conf.*, Aug. 1997, pp. 150–164.
[32] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *J. Cryptol.*, vol. 13, no. 3, pp. 361–396, 2000.

YU-LONG GAO received the M.S. degree in computer technology from Henan Polytechnic University, Jiaozuo, Henan, China, in 2017. He is currently pursuing the Ph.D. degree with the Beijing University of Posts and Telecommunications. His research interests include information security and cryptography.

XIU-BO CHEN received the Ph.D. degree from the Beijing University of Posts and Telecommunications in 2009. She is currently an Associate Professor with the School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing, China. Her research interests include cryptography, information security, quantum network coding, and quantum private communication.

YU-LING CHEN received the B.S. degree from Taishan University in 2006 and the M.S. degree from Guizhou University in 2009. She is currently an Associate Professor with the Guizhou Provincial Key Laboratory of Public Big Data, Guizhou University, Guiyang, China. Her recent research interests include cryptography and information security.

YING SUN received the Ph.D. degree from the Beijing University of Post and Telecommunications in 2010. She is currently an Assistant Professor with the Beijing Electronic Science and Technology Institute, Beijing, China. Her research interests include quantum computation and quantum cryptography.

XIN-XIN NIU received the M.S. degree from the Beijing University of Posts and Telecommunications in 1988 and the Ph.D. degree from The Chinese University of Hong Kong in 1997. She is currently a Professor with the School of Cyberspace Security, Beijing University of Posts and Telecommunications. Her research interests include network security, digital watermarking, and digital rights management.

YI-XIAN YANG received the M.S. degree in applied mathematics and the Ph.D. degree in electronics and communication systems from the Beijing University of Posts and Telecommunications, Beijing, China, in 1986 and 1988, respectively. He has authored over 40 national and provincial key scientific research projects, published over 300 high-level papers, and 20 monographs. His research interests include cryptography, information and network security. He was elected for the Yangtze River Scholar Program Professor Award, the National Outstanding Youth Fund Award, and the National Teaching Masters.