IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 20, 2017, accepted December 21, 2017, date of publication January 1, 2018, date of current version February 28, 2018.

Digital Object Identifier 10.1109/ACCESS.2017.2788411

An Anti-Quantum Transaction Authentication Approach in Blockchain

WEI YIN, QIAOYAN WEN, WENMIN LI, HUA ZHANG, (Member, IEEE), AND ZHENGPING JIN
State key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
Corresponding author: Hua Zhang (zhanghua_288@bupt.edu.cn)

This work was supported by NSFC under Grant 61502044.

ABSTRACT Blockchain is a new distributed and decentralized technology, and gradually attracts worldwide attention, but it is vulnerable to quantum attacks that would solve elliptic curve digital logarithm problem, which is mainly used for transaction authentication in blockchain. The key needed for authentication comes from the wallet. To ensure that the size of the wallet is fixed and easy to manage, deterministic wallets are required to be used. But if existing anti-quantum signature schemes, such as lattice-based signature are used directly in blockchain to solve the problem, it would have made the wallet bloat. In this paper, we present a novel anti-quantum transaction authentication scheme in the blockchain. In order to construct lightweight nondeterministic wallets, the key point is that public and private keys are generated from a set of master public and private key(Seed Key). We leverage on Bonsai Trees technology and propose a new authentication method which can extend a lattice space to multiple lattice spaces accompanied by the corresponding key. Every signature of a transaction uses a lattice space so as to ensure the randomness and the security of the master private key. And we give the complete security proof and analysis. This paper provides the theoretical support for the application of blockchain in the post quantum age.

INDEX TERMS Lattice, blockchain, transaction authentication, signature.

I. INTRODUCTION

Blockchain technology sets off a technological revolution and industrial revolution in the global world, it is considered to be subversive innovation of the computing model after the mainframe, personal PC and the Internet. The core idea of the blockchain is to use a decentralized distributed block storage structure and point-to-point transmission to help users reach a consensus without the control of the authority center [9]. This feature attracts a number of organizations to research how to use blockchain technology to achieve a variety of decentralized applications, for example, the People's Bank of China has deployed important forces to explore the application of blockchain technology in China's financial sector; In 2015, the Bank of England took the lead in using blockchain technology to propose the concept, proposition and model of central bank's digital money [21]; In December of the same year, the United States Nasdaq launched the first securities trading platform Linq based on the blockchain technology [22].

The blockchain technology adopts basic cryptographic algorithms and schemes for consensus and transaction authentication, such as hash functions, digital signatures and so on. But these technologies can not satisfy the security requirements in the complex business environment and the attacks that may appear in the future. With the modern network information society tending to globalization and nationalization, the requirements for information security are not only basic security goals such as tamper resistant, trade disavowing resistant, security and trustworthy, but also stronger demand of privacy protection and identity authentication. Once the blockchain has been applied to the financial industry, cloud storage and other fields, its security mechanism and business model are not easy to change. This requires that the research of the blockchain technology security should consider not only the existing means of attack, but also security threats which may appear in coming years, such as quantum attack.

Specifically, in the transaction authentication, the blockchain technology is based on the elliptic curve digital signature algorithm (ECDSA) [7], [8], which can not cope with the quantum attack in the actual network which will appear in the future. If anyone uses the Shor algorithm [23] to derive a user's private key from a public key to sign a variety of unauthorized transactions, or an attacker forged a

user signature, it means that the legitimate users will lose all their assets and privacy.

In terms of resisting quantum attacks, the research of lattice cryptography is fruitful, which lays the foundation for the design of anti-quantum attack signature scheme which is suitable for blockchain. In 2008, Gentry *et al.* [13] defined lattice-based construction of preimage sampleable trapdoor functions(PSFs), and a hash and sign digital signature scheme which is provable security in the random oracle model based on the SIS problem. But the security of scheme in random oracle model cannot guarantee the security after the instantiation of the scheme. In 2010, Cash et al. demonstrated additional useful features of lattice trapdoors based on GPV's work, known as bonsai tree technology [28]. These were used to construct digital signature and IBE schemes without random oracles, as well as hierarchical versions. However, the length of public key and private key in the schemes are large. Micciancio et al. turned from short bases as generic lattice trapdoors, to the gadget based trapdoors for q-ary SIS/LWE lattices developed in [2], simplified the private key extraction way in the signature scheme based lattice. And researchers recently study the rationality that the preimage from the uniform distribution of small scope, reduce the computational complexity of the preimage sampleable trapdoor functions, and improve the efficiency implementation of the signature scheme. We have adapted the above results to our scheme in blockchain.

The signature schemes in the research work [14], [16], [19] above have been advanced in the aspect of security and the key size, but still cannot be applied to blockchain directly. Because in blockchain, we advocate that different addresses are used in different transaction in order to avoid the user identity exposure. If the existing signature scheme had been introduced in the blockchain, the direct approach is to use multiple seeds to generate multiple addresses. However, it would have made the currency wallet bloat for many seed keys need to be stored in the wallet. We propose a new signature scheme which make the currency wallet lightweight, which has only one pair of public and private key as seed. Meanwhile, this paper puts forward the method of extract the user's address from the public key. So the lattice based signature scheme in blockchain not only has the theory value, but also provide security against quantum attack in distributed applications based on blockchain.

A. OUR CONTRIBUTION

1) We take into account quantum attack in the blockchain, and propose a novel transaction authentication scheme, which is suitable for blockchain. Specifically, we adopt the lattice based bonsai tree signature, which achieves property that many sub-private keys are derived from the seed in the deterministic wallet of blockchain, and its security could be reduced to the SIS hard problem [20]. Our signature is different from previous ones because the extended lattice and corresponding private key could be generated firstly and then the signature is generated according to the message, rather than the extended lattice with private key is determined by the message and then generate the signature. The length of signature in our scheme is $\mathcal{O}(1)$ rather than $\mathcal{O}(k)$ in the [28], which is more suitable for storage in blockchain.
2) We give a standard transaction model that could be resist quantum attack, while maintaining the wallet lightweight. This paper, with the analysis of non-deterministic(random) wallet and deterministic (seeded) wallet, studies why previous lattice based signature schemes do not apply to blockchain.

B. PAPER OUTLINE

Our paper is organized as follows. In section 2, we describe basic structure and quantum attack of the blockchain. In section 3, we review some facts, results on lattice and average-case SIS hard problems. In section 4, we construct a signature scheme that suits for the blockchain and give a detailed proof. We design our anti-quantum transaction authentication in section 5. In section 6, we conclude the paper.

II. BLOCKCHAIN AND QUANTUM ATTACKS

The technology of blockchain attracts more and more attention on its application and researches since the paper ''Bitcoin: A Peer-to-Peer Electronic Cash System'' proposed by a Japanese researcher called Bitcoin [24] in 2009. The blockchain can be defined narrow and generalized. The narrow blockchain is a kind of data structure in which the data block is connected like a chain ordered by the time sequence. It is a distributed general ledger with non-central node which can not be modified due to the adoption of cryptography technology. The generalized blockchain is an non-central infrastructure which is based on the chain of data block, storage block and supports programming.

The technique of the blockchain solves the two long-standing problem of digital currency: Double Spending Problem and Byzantine General Problem [25]. In the environment of virtual digital currency, a malicious user can pay twice by the same digital currency. In the traditional economic environment, the Double Spending Problem can be avoided naturally because the currency exists in the form of physical entity. The revolutionary contribution of blockchain technology is that the various user node validate transaction and achieve consensus through the proof of work [12] without the participation of the third party. The Byzantine Generals Problem is that how to reach a consensus and further to build mutual trust among the mutual distrust nodes in a distributed system environment. By using the digital signature scheme and the consensus algorithm, the blockchain technology can establish trusted system without the authority center for the first time.

Bitcoin is the most successful application of blockchain technology. Bitcoin can be currently converted into legal currency in most countries. According to the CoinDesk

estimates, there are about 60 thousand merchants that accept the bitcoin transactions now, and China is the fastest growing bitcoin trading country in the world. Bitcoin can be considered as a blockchain based digital currency. Bitcoin system is decentralized, and network nodes need not trust each other. Every node in the system collects transactions in the network and records these information in current block through the cryptographic algorithm in the period of time. And a hash of the block can be used to verify the valid transaction and connect them to the next block, then upload the block to public chain once in a while.

A. THE STRUCTURE OF THE BLOCKCHAIN

The blockchain is composed of blocks, each block consists of two parts: block header and block body [26]. The block header contains the current version number, the target hash value of the previous block, the timestamp, and the random number which is a solution of a hash computation problem. The block body contains the transaction data in the current network, which is recorded in the form of Merkle tree [10]. The block header contains the hash value of the previous block [11], and connects to the next block. So every block in the blockchain is linked together, form such an integral chain (see Figure 1).

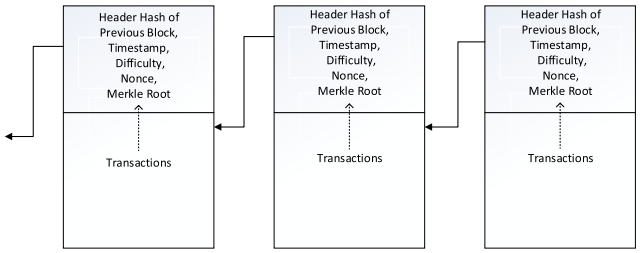

FIGURE 1. The structure of the blockchain.

Current blockchain network is a decentralized and distributed ledger, each user is only identified with its unique address, the address is derived from the public key, and private key is under the control of user. When the user **A** is ready to send money to the user **B**, he signs a transaction with his own private key. The transaction would block a consumption, declares that only the recipient who meets the blocking conditions will be able to spend these funds. Specifically, the user **A** adds a signature which is signed by his private key in the transaction, declares that only those who provide the legal signature of recipient **B** can spend the money. Because the corresponding legal signature can only be generated by **B** with his private key. And funds are transferred safely in the procedure.

User **A** marks the receiver by an address, which could be a series of numbers. Every node in the network would do the following operations when it receives the users transaction:

1) The receiver would check that the signature in the transaction is valid or not. If the signature is not valid, the receiver rejects the transaction.
2) The receiver would check whether there is enough money in the quoted delivery address to complete this transaction. If not, the receiver rejects the transaction.
3) The database is updated, and funds is transferred from one account to another.

A requirement of anonymous is that the true identities of **A** and **B** are not learned by every node in the network [27]. Another important detail is that the users address is not determined by the system network, since the public key and the private key are closely linked, they are generated in the user's device. There is no limit on the number of addresses, in fact, the system encourages that users generate multiple addresses to achieve privacy protection.

Blockchain technology does not require users to register in advance, even the users could transfer funds without informing addresses with each other. The user **A** and user **B** can be paired in some other ways, such as email and smartphone. In centralized system, the funds are under the control of a centralized entity authority. The authority takes charge of user registration and transfer funds. On the contrary, to transfer funds is solely controlled by the private key of user in the decentralized system.

The so-called wallet is a private keys container, which stores files and simple data. In other words, the wallet contains only the private keys instead of the digital currency such as Bitcoin. Each user has a wallet which contains a number of private keys, and user signs transactions with his own private key to prove their ownership of the funds. The digital currency is stored in the block.

Early wallet stores a set of randomly generated private keys. That is, the wallet generates sufficient private keys when the system is initialized and each private key is used only once. This wallet, which is hard to manage, back-up and import, has gradually been replaced by deterministic(seeded) wallet. The disadvantage of the random wallet is that if it generates private keys a lot at the beginning, the wallet must saves all the copies, this also indicates that the wallet needs backup regularly. Moreover, this wallet would bring the problem of reusing address: the addresses associate with multiple transactions and reuse of address would reduce the privacy. A number generated randomly is regarded as a seed, which is stored in the deterministic wallet. All the private keys are derived from the seed. The system creates a simple backup at the beginning of the initialization therefore the seed is enough to recover all private keys. So the deterministic wallet is encouraged to use in blockchain technology. (see Figure 2)

B. QUANTUM ATTACKS ON THE BLOCKCHAIN

The elliptic curve digital signature algorithm (ECDSA) [7], [8] is adopted in the current blockchain technology. The specific process is as follows: we regrad a randomly generated private key k as a starting point, multiply G which is randomly generated point defined on the curve by the private key k and obtain another point K, which is the corresponding public key $K = k * G$. This process can only be calculated in one direction, that is, K can be obtained from

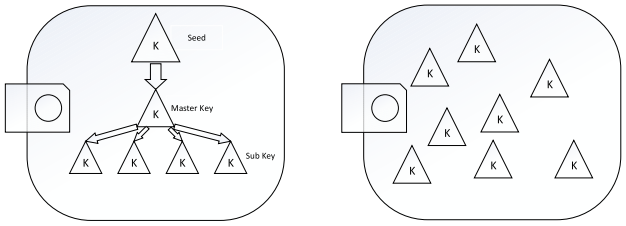

FIGURE 2. The two wallets.

known k easily, but not vice versa. Because the cryptographic algorithm is one-way function, the private key can generate the public key, and cannot be derived from the public key.

In particular, the user's addresses in the blockchain are obtained by multiplying the seed by the different k, then we obtain different public keys. An address is a string of numbers and letters, which are generated by SHA256 algorithm, RIPEMD160 algorithm and a series of code algorithm. We can share our address with user who trade with us. The advantage is that a seed can generate multiple addresses, the corresponding wallet only need to store a seedthis can be consistent with the property of the deterministic wallet.

However, the current blockchain can not resist quantum attacks that will appear in the actual network in the future. If any adversary utilizes the Shor algorithm [23] to achieve the private key that derived from the elliptic curve public key, then the adversary can sign various unauthorized transactions or forge users valid signature, which means that the user will lose all his assets and the right of privacy.

Therefore, it is an urgent problem that how the blockchain technology resist the quantum attack in the future. This paper gives a lattice based signature scheme, which can realize the security authentication in quantum environment.

III. PRELIMINARIES OF THE LATTICE

A. LATTICE AND RELATED FACTS

Definition 1 (Integer Lattice [13], [15]): Let $B = [b_1| \ldots |b_m] \in \mathbb{R}^{m\times m}$ *be an* $m \times m$ *matrix whose columns are linearly independent vectors* $b_1, \ldots, b_m \in \mathbb{R}^m$. *The m-dimensional full-rank lattice* Λ *generated by B is the set,*

$$\Lambda = \mathcal{L}(B) = \{y \in \mathbb{R}^m \quad s.t. \quad \exists s \in \mathbb{Z}^m, y = Bs = \sum_{i=1}^{m} s_i b_i\}$$

Here, we are interested in integer lattices, i.e., when $\mathcal{L}$ *is contained in* $\mathbb{Z}^m$. *We let* $det(\Lambda)$ *denote the determinant of* Λ.

Definition 2 (q-Ary Lattice [1], [3], [4]): For prime q, $A \in \mathbb{Z}_q^{n\times m}$ *and* $u \in \mathbb{Z}_q^n$, *define:*

$$\Lambda(A)_q := \{e \in \mathbb{Z}^m \quad s.t. \exists s \in \mathbb{Z}_q^n \quad where A^\top s = e(mod q)\}$$
$$\Lambda_q^\perp(A) := \{e \in \mathbb{Z}^m \quad s.t. Ae = 0(mod q)\}$$
$$\Lambda_q^u(A) := \{e \in \mathbb{Z}^m \quad s.t. Ae = u(mod q)\}$$

We can observe that if $t \in \Lambda_q^u(A)$ *then* $\Lambda_q^u(A) = \Lambda_q^\perp(A) + t$ *and hence* $\Lambda_q^u(A)$ *is a shift of* $\Lambda_q^\perp(A)$

Definition 3 (Gram-Schmidt Norm [1], [3], [4]): Let S be a set of vectors $S = \{s_1, \ldots, s_k\}$ *in* $\mathbb{R}^m$. *We use the following standard notations:*

- $\|S\|$ denotes the L_2 length of the longest in S, i.e., $\max_{1\le i\le k}\|s_i\|$.
- $\tilde{S} := \{\tilde{s}_1, \ldots, \tilde{s}_k\} \subset \mathbb{R}^m$ denotes the Gram-Schmidt orthogonalization of the vectors $s_1, \ldots, s_k$ taken in that order.

Lemma 1 ([16], Lemma 7.1): There is a deterministic poly-time algorithm ToBasis(S, B) that, given a full rank set S of lattice vectors in $\Lambda = \mathcal{L}(B)$, *outputs a basis T of* Λ *such that* $\|\tilde{t}_i\| \le \|\tilde{s}_i\|$ *for all i.*

Theorem 1: Let $q \geqslant 3$ *be odd and* $m := \lceil 6nlogq \rceil$. *There is a probabilistic polynomial -time algorithm* **TrapGen**(q,n) *that outputs a pair* $(A \in \mathbb{Z}_q^{n\times m}, S \in \mathbb{Z}^{n\times m})$ *such that A is statistically close to a uniform matrix in* $\mathbb{Z}_q^{n\times m}$ *and S is a basis for* $\Lambda_q^\perp(A)$ *satisfying*

$$\|\widetilde{S}\| \leqslant O(\sqrt{nlogq}) \quad and \quad \|S\| \leqslant O(nlogq)$$

with all but negligible probability in n.

We give an outline of Gaussian distributions over lattice. For any $s > 0$ and dimension $m \ge 1$, the Gaussian function $\rho_s : \mathbb{R}^m \to (0, 1]$ is defined as $\rho_s(\mathbf{x}) = exp(-\pi\|\mathbf{x}\|^2/s^2)$. For any coset $\Lambda_{\mathbf{y}}^\perp(A)$, and probability zero elsewhere. We summarize several facts from the literature about discrete Gaussian over lattices, again specialized to our family of interest.

Lemma 2 [20], Lemma 4.4: For any n-dimensional lattice Λ, *vector* $\mathbf{c} \in \mathbb{R}^n$, *and reals* $0 < \epsilon < 1$, $s \geqslant \eta_\epsilon(\Lambda)$, *we have*

$$\Pr_{\mathbf{x}\sim\mathcal{D}_{\Lambda,s,\mathbf{c}}}\{\|\mathbf{x} - \mathbf{c}\| > s\sqrt{n}\} \leqslant \frac{1+\epsilon}{1-\epsilon}\cdot 2^{-n}$$

Lemma 3 [13]: There is a randomized nearest-plane algorithm, called **SampleD**, *that samples from a discrete Gaussian* $D_{\Lambda,s,c}$ *over any lattice* Λ. *In each iteration, the algorithm chooses a plane at random by sampling from an appropriate discrete Gaussian over the integers* $\mathbb{Z}$.

Lemma 4 [13]: There are two significant PPT algorithms in our construction: **SampleGaussian**$(A, T_A, \sigma, \mathbf{c})$ *and* **SamplePre**(A, T_A, σ, u), *the former returns* $x \in \Lambda_q^\perp(A)$ *drawn from a distribution statistically close to* $\mathcal{D}_{\Lambda,s,\mathbf{c}}$, *and the latter returns* $x \in \Lambda_q^u(A)$ *sampled from a distribution statistically close to* $\mathcal{D}_{\Lambda_q^u(A),\sigma}$, *whenever* $\Lambda_q^u(A)$ *is not empty, where* T_A *be a basis for* $\Lambda_q^\perp(A)$ *and* $\sigma \geqslant \|\widetilde{T_A}\|\omega(\sqrt{logm})$, *for* $\mathbf{c} \in \mathbb{R}^m$ *and* $u \in \mathbb{Z}_q^n$.

In this section we lay out the framework and main techniques for the cultivation of bonsai tree [28]. Here we describe how an arborist extend its control of a lattice to an arbitrary higher dimensional extension, without any loss of quality in the resulting basis.

Lemma 5 ([28], Lemma 3.2): There is a deterministic polynomial-time algorithm **ExtBasis** *with the following properties: given an arbitrary* $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ *whose columns generate the entire group* $\mathbb{Z}_q^n$, *an arbitrary basis* $\mathbf{S} \in \mathbb{Z}^{m\times m}$ *of* $\Lambda^\perp(\mathbf{A})$, *and an arbitrary* $\bar{\mathbf{A}} \in \mathbb{Z}_q^{n\times\bar{m}}$, **ExtBasis**$(\mathbf{S}, \mathbf{A}' = \mathbf{A}\|\bar{\mathbf{A}})$ *outputs*

a basis $\mathbf{S}'$ *of* $\Lambda^{\perp}(\mathbf{A}') \subseteq \mathbb{Z}^{m+\bar{m}}$ *such that* $\|\tilde{\mathbf{S}}'\| = \|\tilde{\mathbf{S}}\|$. *Moreover, the same holds even for any given permutation of the columns of* $\mathbf{A}'$*(e.g., if columns of* $\bar{\mathbf{A}}$ *are both appended and prepended to* $\mathbf{A}$*).*

The algorithm **ExtBasis** works as follow: the **ExtBasis**$(\mathbf{S}, \mathbf{A}')$ computes and outputs an $\mathbf{S}'$ of the form $\mathbf{S}' = \begin{pmatrix} \mathbf{S} & \mathbf{W} \\ \mathbf{0} & \mathbf{I} \end{pmatrix} \in \mathbb{Z}^{m'*m'}$, where $m' = m + \bar{m}$, $\mathbf{I} \in \mathbb{Z}^{\bar{m}*\bar{m}}$, and $\mathbf{W} \in \mathbb{Z}^{m*\bar{m}}$ is an arbitrary solution to $\mathbf{AW} = -\bar{\mathbf{A}} \in \mathbb{Z}_q^{n*\bar{m}}$(not necessarily short solution). Note that $\mathbf{W}$ exists by the hypothesis that $\mathbf{A}$ generates $\mathbb{Z}_q^n$, and it may be computed efficiently using, e.g., Gaussian elimination.

B. SHORT INTEGER SOLUTION

The short integer solution (SIS) problem was first proposed in the pioneering work of Ajtai [17]. This hard-on-average problem is to find a short nonzero integer solution to the homogeneous linear equations $A\mathbf{e} = \mathbf{0}(\mathrm{mod}q)$, where $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ is uniformly random. The problem is syntactically equivalent to finding short nonzero vectors in $\Lambda^{\perp}(\mathbf{A})$, and has been regarded as the foundation for some primitives in the cryptography such as one-way function, anti-collusion hash function, digital signature. A more formal definition is given below:

Definition 4 [20]: The small integer solution problem SIS (in the ℓ_2 *norm) is as follows: given an integer q, a matrix* $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$*, and a real* β*, find a nonzero integer vector* $\mathbf{e} \in \mathbb{Z}^m$ *such that* $\mathbf{Ae} = 0(\mathrm{mod}q)$ *and* $\|\mathbf{e}\|_2 \leqslant \beta$.

There is a variant problem, which is to find a short solution to a inhomogeneous linear equations.

Definition 5: The inhomogeneous small integer solution problem ISIS (in the ℓ_2 *norm) is as follows: given an integer q, a matrix* $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$*, a syndrome* $\mathbf{u} \in \mathbb{Z}_q^n$*, and a real* β*, find an integer vector* $\mathbf{e} \in \mathbb{Z}_q^m$ *such that* $\mathbf{Ae} = \mathbf{u}(\mathrm{mod}q)$ *and* $\|\mathbf{e}\|_2 \leqslant \beta$.

The ISIS problem is phrased as a syndrome decoding problem, which is equivalent to the problem of decoding an arbitrary integer target point $\mathbf{t} \in \mathbb{Z}^m$ within the distance β on the lattice $\Lambda^{\perp}(\mathbf{A})$. Specifically, the syndrome of the target point is $\mathbf{u} = \mathbf{At}(\mathrm{mod}q)$, and the solution of the ISIS is a short error vector $\mathbf{e} \in \mathbb{Z}^m$, which has the same syndrome $\mathbf{u}$. Then the error vector yields a lattice point $\mathbf{v} = \mathbf{t} - \mathbf{e} \in \Lambda^{\perp}$ for $\mathbf{Av} = \mathbf{At} - \mathbf{Ae} = \mathbf{0}(\mathrm{mod}q)$, furthermore, $\mathbf{v}$ is within distance β of $\mathbf{t}$ [13].

Lemma 6 ([20], Lemma 4.4): For any n-dimensional lattice Λ*, vector* $\mathbf{c} \in \mathbb{R}^n$*, and reals* $0 < \epsilon < 1$, $s \geqslant \eta_{\epsilon}(\Lambda)$, *we have*

$$\Pr_{\mathbf{x}\sim\mathcal{D}_{\Lambda,s,\mathbf{c}}}\{\|\mathbf{x}-\mathbf{c}\| > s\sqrt{n}\} \leqslant \frac{1+\epsilon}{1-\epsilon}\cdot 2^{-n}$$

IV. OUR CONSTRUCTION OF BLOCKCHAIN FROM LATTICE

A. OUR CONSTRUCTION

Our solution construction is as follows: The scheme is begin with *TrapGen* which outputs public key $A_0 \in \mathbb{Z}_q^{n\times m}$ with a basis $T_{A_0} \in \mathbb{Z}_q^{m\times m}$(SIS parameters n and q) such that $\|\widetilde{T_{A_0}}\| \leqslant O(\sqrt{n\log q}), m = \mathcal{O}(n\log q)$, (A_0, T_{A_0}) to be saved as seed lattice basis in the wallet. Then bonsai tree algorithm [28] is used to generate sub-public and private keys, the procedure is as follows (see Figure 3).

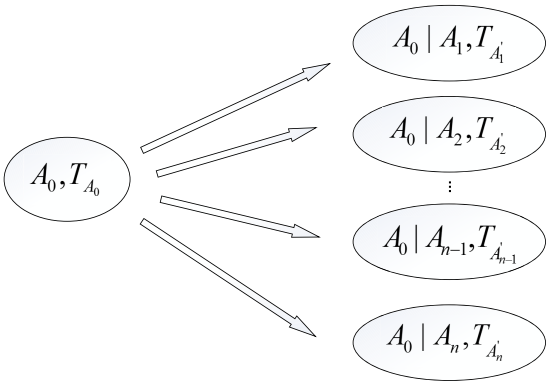

FIGURE 3. Generation of public and private keys.

The scheme is built upon a collection of efficient procedures given by (**Setup**, **Extending control**, **Sign**, **Verify**), and operates relative to a function $H = H_n : \{0,1\}^* \to R_n$ that is modelled as a random oracle. We concatenate some matrices $A_1, A_2, A_3, \cdots, A_n \in \mathbb{Z}_q^{n\times m}$ behind A_0, namely, denoted by $A_1', A_2', A_3', \cdots, A_n' = A_0|A_1, A_0|A_2, A_0|A_3, \cdots, A_0|A_n \in \mathbb{Z}_q^{n\times 2m}$. In order to generate the different sub-public and private keyswe invoke the algorithm **ExtBasis** to generate the corresponding sub private key, $T_{A_1'} \leftarrow \mathbf{ExtBasis}(T_{A_0}, A_1'), T_{A_2'} \leftarrow \mathbf{ExtBasis}(T_{A_0}, A_2'), T_{A_3'} \leftarrow \mathbf{ExtBasis}(T_{A_0}, A_3'), \cdots, T_{A_n'} \leftarrow \mathbf{ExtBasis}(T_{A_0}, A_n')$. Then perform the signing operation. The specific scheme is as follows:

- **Setup**(n): On input the security parameter(SIS parameters) n and q, using algorithm **TrapGen**(q, n) to select a uniformly random $n \times m - matrix\ A_0 \in \mathbb{Z}_q^{n\times m}$ with a basis T_{A_0} such that $\|\widetilde{T_{A_0}}\| \leqslant O(\sqrt{n\log q})$.
- **ExtendingControl**$(A_0, T_0, A_1, \cdots, A_n)$: Choose n uniformly random $n \times m$ matrix $(A_1, A_2, \cdots, A_n)$, using algorithm **ExtBasis**

$$\begin{aligned} T_{A_1'} &\leftarrow \mathbf{ExtBasis}(T_{A_0}, A_1' = A_0|A_1) \\ T_{A_2'} &\leftarrow \mathbf{ExtBasis}(T_{A_0}, A_2' = A_0|A_2) \\ T_{A_3'} &\leftarrow \mathbf{ExtBasis}(T_{A_0}, A_3' = A_0|A_3) \\ &\vdots \\ T_{A_n'} &\leftarrow \mathbf{ExtBasis}(T_{A_0}, A_n' = A_0|A_n) \end{aligned}$$

  public and private keys pairs are generated after the completion of operation: $(A_1', T_{A_1'}), (A_2', T_{A_2'}), (A_3', T_{A_3'}), \cdots, (A_n', T_{A_n'})$ are used for signature verification as part of user's wallet.
- **Sign**$(T_{A_i'}, M)$: Once the user initiates the transaction behavior with other users, he can sign the transaction with one private key of his wallet to ensure that others cannot forge signature except himself. Because each transaction is different (or at least has a different

timestamp), we do not consider a transaction and signature would be saved in the local storage. Public and private key used to be sign transaction are selected randomly from wallet.
Let

$$\varpi_M \leftarrow \mathsf{SamplePre}(T_{A_i'}, H(M)).$$

The Signature ϖ_M and the transaction M would be sent to the recipient together.

- **Verify**(A_i', M, ϖ_M): Accept if $\varpi_M \in D_n$ and $f_{A_i'}(\varpi_M) = H(M)$; else, reject.
If there are the other transaction generated, the algorithm above could be executed multiple times.

The correctness of the scheme is guaranteed by **Lemma 4** and **Lemma 5** in the section 3.

In principle, to achieve the goal of user identity anonymous, the used public and private keys $(T_{A_i'}, A_i')$ cannot be duplicate used.

B. EFFICIENCY ANALYSIS

We give a detailed efficiency analysis of our scheme. There are three algorithms in our signature scheme: TrapGen, ExtBasis and SamplePre. Seed key A_0 and T_0 are the input of the algorithm TrapGen. The size of A_0 and T_0 are $O(n^2log^2n)$, $O(n^2log^3n)$. The computation amount of ExtBasis mainly induced by solving linear equations $\mathbf{AW} = -\bar{\mathbf{A}}$(See Lemma 5), and note that $\mathbf{W}$ exists by the hypothesis that $\mathbf{A}$ generates $\mathbb{Z}_q^n$. Take the Gaussian elimination for an example, $\mathbf{W}$ could be computed efficiently. The algorithm complexity of Gaussian elimination is $O(n^3)$. ϖ_M is generated by SamplePre, which calling solving linear equations and SampleD(See Lemma 3) as subroutines. Assuming scalar operations in SampleD take unit time, the running time of the algorithm is $O(n^2)$ plus the running time of the n oracle calls. For example, we take $n = 330$, $m = 58531$, $q = 1.19e + 10$ [29], the storage size of public key A_i' is about 154MB, the private key $T_{A_i'}$ is about 537MB(different parameters selection for our scheme in Table 1). However, in the current blockchain structure, a block is only 1MB, which containing 4000 transactions, and one transaction is 250B. From this point of view, our program is not practical now, but it has theoretical significance.

C. SECURITY PROOF

Theorem 2: Our scheme in blockchain is strongly unforgeable under chosen message attack except the probability $\epsilon(n)$.

TABLE 1. Parameters selection for our shceme.

n	289	330	440
q	6.98e+9	1.19e+10	3.75e+10
m	50087	58531	81913
$\|sk\|$	403120KB	550452KB	538996KB
$\|pk\|$	115562KB	157833KB	309083KB
$\|\varpi\|$	260KB	308KB	442KB

Proof: We can prove that the scheme above is correct and complete according to the property of preimage sampleable trapdoor functions. Suppose there is an adversary forges a signature with probability $\epsilon(n)$ to break our scheme, then we reduce to a polynomial time algorithm $\mathcal{C}$ to solve the small integer solution problem SIS which is considered difficult in lattice cryptosystem, by finding a nonzero short integer vector. We describe the process as follows:

Step 1: We tag function f_A given matrix A, simulate random oracle H and signature oracle with adversary $\mathcal{A}$. Without loss of generality, we assume that the adversary $\mathcal{A}$ make a hash query of m before a signature query of m. In the other words, the simulator $\mathcal{C}$ answer the signature query after the hash query.

Step 2: In general, suppose the adversary $\mathcal{A}$ make a hash query about m^* prior to he give out a legal forged signature (m^*, ϖ^*). For each hash query about m of the adversary $\mathcal{A}$, the simulator $\mathcal{C}$ make $\varpi_m \leftarrow SampleDom(1^n)$, and stores (m, ϖ_m) in the local temporarily. Then the simulator $\mathcal{C}$ returns $f_A(\varpi_m) = A \cdot \varpi_m$ to the adversary $\mathcal{A}$ serves as an answer for hash query about m.

Step 3: For the signature query about m of the adversary $\mathcal{A}$, the simulator $\mathcal{C}$ search for the data (m, ϖ_m) in the local and returns ϖ_m to the adversary $\mathcal{A}$ serves as an answer for signature query about m.

Step 4: In this way, when the adversary $\mathcal{A}$ generates a forged signature (m^*, ϖ^*), the simulator $\mathcal{S}$ finds (m^*, ϖ_{m^*}) in the local and output $\varpi^* - \varpi_{m^*}$ as a solution to the SIS hard problem.

We now analyze the process of reduction above. First, the view of the adversary $\mathcal{A}$ in the simulated system which provided by $\mathcal{C}$ is equal to the real system. This point is guaranteed by the property of trapdoor functions:

1) The simulator $\mathcal{C}$ returns $H(m) = f_A(\varpi_m)$ for every different hash query, where $\varpi_m \leftarrow SampleDom$ that its output is uniform random. The output distribution are same with each other in both real system and simulation system.
2) The simulator $\mathcal{C}$ returns ϖ_m for every signature query about m after fixing $H(m)$. And the distribution of ϖ_m is from $SampleDom$ given the condition of $f_A(\varpi_m) = H(m)$.
3) For the signature query about m in the real system, the output signature from SamplePre with the help of the trapdoor, its distribution is same as signature generate from simulation system.

In the result, the simulator $\mathcal{C}$ simulates the real signature system perfectly. And the adversary $\mathcal{A}$ gives a forged signature (m^*, ϖ^*) with probability ϵ. Since there is ϖ_{m^*} in the local and ϖ^* is a valid signature, then we have $f_A(\varpi^*) = H(m^*) = f_A(\varpi_{m^*})$. So we regard $(\varpi_{m^*} - \varpi^*)$ as a solution to the SIS hard problem. Here we show that $\varpi_{m^*} \neq \varpi^*$. There are two situations that require some thought to make sure $\varpi_{m^*} \neq \varpi^*$:

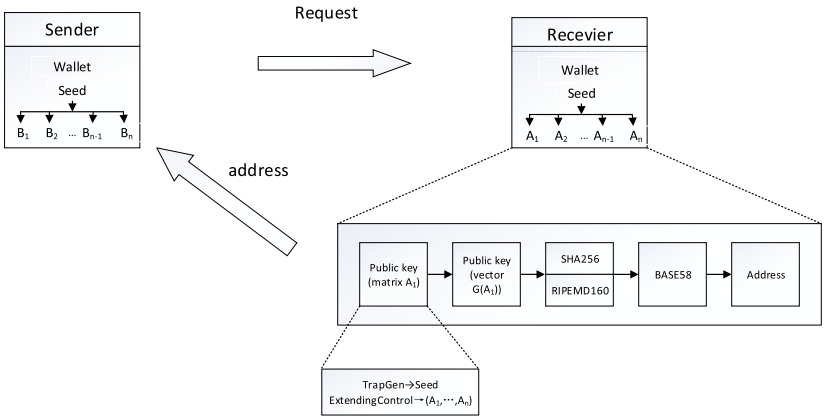

FIGURE 4. The address generation.

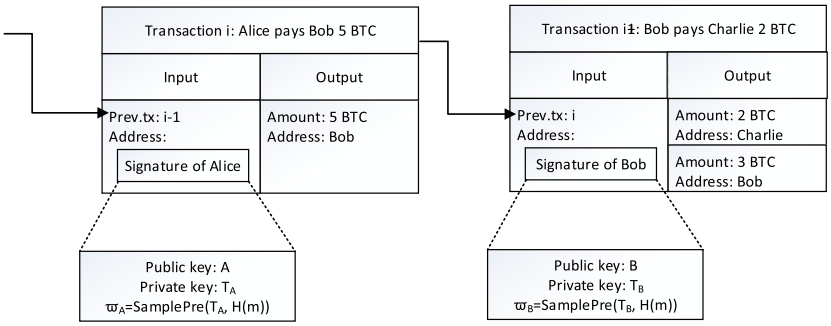

FIGURE 5. The lattice based transaction.

1) If the adversary $\mathcal{A}$ asks signature query about message m and receives ϖ_{m^*} as an answer, we have $\varpi_{m^*} \neq \varpi^*$ since the (m^*, ϖ^*) is a forged signature.
2) If the adversary $\mathcal{A}$ do not ask signature query except hash query about m, then the simulator $\mathcal{C}$ stores (m^*, ϖ_{m^*}) in the local since signature ϖ_{m^*} is produced in the during of hash query. Based on the property of min-entropy preimage, the min-entropy of ϖ_{m^*} is minimum value given the condition of $f_A(\varpi_{m^*}) = H(m^*)$, so it is hard to get ϖ_{m^*}. And the hash query and ϖ_{m^*} is independent of each other in the view of the adversary $\mathcal{A}$, so we come up with the min-entropy of ϖ_{m^*} is $w(logn)$.
3) Combining the above two points, the probability of $\varpi_{m^*} = \varpi^*$ is $2^{-w(logn)}$ at most.

Finally, we summarize that the probability of the simulator $\mathcal{C}$ sovles the SIS hard problem is close to $\epsilon(n)$. □

V. ANTI-QUANTUM TRANSACTION AUTHENTICATION

A. ADDRESS AND PROTOCOL

The address is a string that consists of numbers and letters. Different from previous generation methods of public and private keys, public and private keys are generated simultaneously in our signature scheme, that is, the private key has no use for the generation of public key. Now we give the process of generating addresses from public keys. The public key is a matrix $A \in \mathbb{Z}_q^{n*2m}$ in our scheme, and an algorithm that mapping a matrix into a vector is given. For a matrix $A = (a_1, a_2, a_3, \cdots, a_{2m}) \in \mathbb{Z}_q^{n*2m}$, define an algorithm $G(A) = (a_1^\top \| a_2^\top \| a_3^\top \| \cdots \| a_{2m}^\top) \in \mathbb{Z}_q^{1*2nm}$. The hash of public key is generated through SHA256 algorithm and RIPEMD160 algorithm, and the final address is generated by Base58Check encoding. The following is a procedure:

1) A sender initiates a transfer request.
2) The receiver selects a pair of public and private keys from his wallet, and the public key is used to generate address.
3) The receiver sends the address to the sender, and then the sender generates a transaction for the address.
4) This transaction is broadcast to the whole network node, and this process is finished until the record is confirmed and recorded in the blockchain (see Figure 4).

B. TRANSACTIONS

A standard transaction model is shown below (see Figure 5). A transaction is a data structure includes input and output. The sender invokes an old accepted transaction in the input, and puts the recipient in the output. Now suppose Alice wants to transfer 5 bitcoins to Bob, Bob selects a pair of public and private keys from his wallet and sends his address to Alice. Alice creates a transaction and puts the Bob's address in the output location. Bob wants to send 2 bitcoins to Charlie

in another day. He needs to create a new transaction that invokes the transaction from Alice as the input. An important principle is that the total input amount of the transaction and the total output amount must be equal. In order to just send Charlie 2 bitcoins, an additional output need to be set to return the change (the remaining 3 bitcoins are returned to himself). And he can invoke the transaction to spend the 3 bitcoins later. After all the outputs are set to ensure that the input and output are equal, Bob can sign the transaction with his private key in his wallet.

VI. CONCLUSION

In this paper, we propose a new signature authentication scheme for blockchain, which is different from the elliptic curve signature scheme in the existing of blockchain technology. It can resist the attack of quantum algorithm in the future. Moreover, our scheme achieves the security that strong unforgeable under chosen message attack except a negligible function and we give the security proof. The security of our signature could be reduced the SIS hard problem on the lattice. Our work has important theoretical significance and provides new thought for the design and development of anti-quantum blockchain technology in the coming decades.

REFERENCES

[1] S. Agrawal and X. Boyen, "Identity-based encryption from lattices in the standard model," *Manuscript*, Jul. 2009. [Online]. Available: http://crypto.stanford.edu/~xb/ab09/latticeibe.pdf
[2] D. Micciancio and C. Peikert, "Trapdoors for lattices: Simpler, tighter, faster, smaller," *EuroCrypt*, vol. 7237, pp. 700–718, 2012.
[3] S. Agrawal, D. Boneh, and X. Boyen, "Efficient lattice (H) IBE in the standard model," in *Advances in Cryptology—EUROCRYPT*, vol. 6110. Springer, 2010, pp. 553–572.
[4] M. Blaze, G. Bleumer, M. Strauss, "Divertible protocols and atomic proxy cryptography," in *Advances in Cryptology—EUROCRYPT*. Springer, 1998, pp. 127–144.
[5] A. A. Shamir "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979.
[6] K. Singh, C. P. Rangan, and A. K. Banerjee, "Lattice based identity based proxy re-encryption scheme," *J. Internet Serv. Inf. Secur.*, vol. 3, nos. 3–4, pp. 38–51, 2013.
[7] V. S. Miller, "Use of elliptic curves in cryptography," in *Proc. Conf. Theory Appl. Cryptogr. Techn.*, 1985, pp. 417–426.
[8] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 177, pp. 203–209, 1987.
[9] A. M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. Philadelphia, PA, USA: O'Reilly Media, 2014.
[10] R. C. Merkle, "Protocols for public key cryptosystems," in *Proc. IEEE Symp. Secur. Privacy*, Apr. 1980, p. 122.
[11] V. Buterin, "A next-generation smart contract and decentralized application platform," White Paper, 2014. [Online]. Available: https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf
[12] D. Larimer, "Delegated proof-of-stake (DPOS)," BitShare, White Paper, 2014. [Online]. Available: http://107.170.30.182/security/delegated-proof-of-stake.php
[13] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proc. 4th Annu. ACM Symp. Theory Comput.*, 2008, pp. 197–206.
[14] D. Cash, D. Hofheinz, and E. Kiltz, "How to delegate a lattice basis," IACR Cryptol. ePrint Arch., Tech. Rep. 2009/351, 2009, p. 351.
[15] D. Micciancio and O. Regev, "Lattice-based cryptography," in *Post-Quantum Cryptography*. Berlin, Germany: Springer, 2009, pp. 147–191.
[16] D. Micciancio and S. Goldwasser, *Complexity of Lattice Problems: A Cryptographic Perspective*. Berlin, Germany: Springer, 2002.
[17] M. Ajtai, "Generating hard instances of lattice problems," in *Proc. 28th Annu. ACM Symp. Theory Comput.*, 1996, pp. 99–108.
[18] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *J. ACM*, vol. 56, no. 6, p. 34, 2009.
[19] R. Cramer, I. Damgård, and M. Keller, "On the amortized complexity of zero-knowledge protocols," in *Advances in Cryptology—CRYPTO*, vol. 5677. Springer, 2009, pp. 177–191.
[20] 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.
[21] G. Danezis and S. Meiklejohn, "Centrally banked cryptocurrencies," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2016, pp. 1–14.
[22] (2015). *Nasdaq Launches Enterprise-Wide Blockchain Technology Initiative*. [Online]. Available: http://www.marketwatch.com/story/nasdaq-launches-enterprise-wide-blockchain-technology-initiative-2015-05-11
[23] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, Nov. 1994, pp. 124–134.
[24] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Tech. Rep., 2008. [Online]. Available: https://bitco.in/pdf/bitcoin.pdf
[25] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," *ACM Trans. Program. Lang. Syst.*, vol. 4, no. 3, pp. 382–401, Jul. 1982.
[26] Y. Yuan and F. Y. Wang, "Blockchain: The state of the art and future trends," *Acta Automatica Sinica*, vol. 42, no. 4, pp. 481–494, 2016.
[27] I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous distributed E-cash from bitcoin," in *Proc. IEEE Symp. Secur. Privacy*, May 2013, pp. 397–411.
[28] D. Cash *et al.*, "Bonsai trees, or how to delegate a lattice basis," *J. Cryptology*, vol. 25, no. 4, pp. 601–639 , 2010.
[29] R. Markus and M. Schneider, "Estimating the security of lattice-based cryptosystems," IACR Cryptol. ePrint Arch., 2010, p. 137.

WEI YIN received the B.S. degree in mathematics and applied mathematics from Huaibei Normal University, Huaibei, China, in 2012. He is currently pursuing the Ph.D. degree at the Beijing University of Posts and Telecommunications. His research interests include public key cryptography, lattice cryptography, and provable security.

QIAOYAN WEN received the B.S. and M.S. degrees in mathematics from Shaanxi Normal University, Xi'an, China, in 1981 and 1984, respectively, and the Ph.D. degree in cryptography from Xidian University, Xi'an, in 1997. She is currently a Professor with the Beijing University of Posts and Telecommunications. Her current research interests include coding theory, cryptography, information security, Internet security, and applied mathematics.

WENMIN LI received the B.S. and M.S. degrees in mathematics and applied mathematics from Shaanxi Normal University, Xian, China, in 2004 and 2007, respectively, and the Ph.D. degree in cryptology from the Beijing University of Posts and Telecommunications, Beijing, China, in 2012. She is currently a Post-Doctoral Researcher with the Beijing University of Posts and Telecommunications. Her research interests include cryptography and information security.

HUA ZHANG received the B.S. degree in telecommunications engineering and the M.S. degree in cryptology from Xidian University, in 1998 and 2005, respectively, and the Ph.D. degree in cryptology from the Beijing University of Posts and Telecommunications in 2008. She is currently an Associate Professor with the Beijing University of Posts and Telecommunications. Her research interests include cryptography, information security, and network security.

ZHENGPING JIN received the B.S. degree in math and applied math and M.S. degree in applied math from Anhui Normal University, in 2004 and 2007, respectively, and the Ph.D. degree in cryptography from the Beijing University of Posts and Telecommunications in 2010. He is currently a Lecturer with the Beijing University of Posts and Telecommunications. His research interests include cryptography, information security, Internet security, and applied mathematics.