Computers, Materials & Continua CMC, vol.63, no.2, pp.845-859, 2020

Post-Quantum Blockchain over Lattice

Xiao Zhang[1, 2, 3], Faguo Wu[1, 2, 3], Wang Yao[1, 2, 3, *], Wenhua Wang[4] and Zhiming Zheng[1, 2, 3]

Abstract: Blockchain is an emerging decentralized architecture and distributed computing paradigm underlying Bitcoin and other cryptocurrencies, and has recently attracted intensive attention from governments, financial institutions, high-tech enterprises, and the capital markets. Its cryptographic security relies on asymmetric cryptography, such as ECC, RSA. However, with the surprising development of quantum technology, asymmetric cryptography schemes mentioned above would become vulnerable. Recently, lattice-based cryptography scheme was proposed to be secure against attacks in the quantum era. In 2018, with the aid of Bonsai Trees technology, Yin et al. [Yin, Wen, Li et al. (2018)] proposed a lattice-based authentication method which can extend a lattice space to multiple lattice spaces accompanied by the corresponding key. Although their scheme has theoretical significance, it is unpractical in actual situation due to extremely large key size and signature size. In this paper, aiming at tackling the critical issue of transaction size, we propose a post quantum blockchain over lattice. By using SampleMat and signature without trapdoor, we can reduce the key size and signature size of our transaction authentication approach by a significant amount. Instead of using a whole set of vectors as a basis, we can use only one vector and rotate it enough times to form a basis. Based on the hardness assumption of Short Integer Solution (SIS), we demonstrate that the proposed anti-quantum transaction authentication scheme over lattice provides existential unforgeability against adaptive chosen-message attacks in the random oracle. As compared to the Yin et al. [Yin, Wen, Li et al. (2018)] scheme, our scheme has better performance in terms of energy consumption, signature size and signing key size. As the underlying lattice problem is intractable even for quantum computers, our scheme would work well in the quantum age.

Keywords: Blockchain, post quantum, lattice, random oracle.

[1] School of Mathematics and Systems Science, Beihang University, and Key Laboratory of Mathematics, Informatics and Behavioral Semantics, Ministry of Education, Beijing, 100191, China.

[2] Peng Cheng Laboratory, Shenzhen, 518055, China.

[3] Beijing Advanced Innovation Center for Big Data and Brain Computing, Beihang University, Beijing, 100191, China.

[4] Aviation Industry Development Research Center of China, Beijing, China.

[*] Corresponding Author: Wang Yao. Email: yaowang@buaa.edu.cn.

Received: 20 July 2019; Accepted: 20 August 2019.

1 Introduction

Blockchain, originally block chain, is a continuously growing list of records, called blocks, which are linked and secured using cryptography and one of the most prominent applications of blockchain are cryptocurrencies. The World Economic Forum (WEF) has identified blockchain technology as one of its six mega-trends in a new report broadly aimed at outlining the expected transition to a more digital and connected world. WEF forecasted that around 10% of global gross domestic product (GDP) is likely to be stored on the blockchain by 2027. Fixing the holes in the Internet of Things. Although Bitcoin is the most famous blockchain application, blockchain technology is a core, underlying technology with promising application prospects in many industries and can be applied into diverse applications far beyond cryptocurrencies, like financial services, risk management, internet of things (IoT) to public and social services [Jiang, Wang, Wang et al. (2019); Agyekum, Opuniboachie, Sifah et al. (2019); Yang, He, Xu et al. (2019); Yang, Zhu, Liang et al. (2019)].

Elliptical Curve Digital Signature Algorithm (ECDSA) cryptography in use by the Bitcoin Core, Ethereum, Bitcoin Cash, and enterprise blockchains such as Multi-Chain and Hyperledger projects Fabric, and Sawtooth Lake [Campbell (2019)]. Elliptic curve cryptography is vulnerable to quantum computing, since Shor's algorithm can be easily modified to decrypt messages sent with elliptic curves. This is impossible for the computing power of the current calculations to break Blockchain system. But within a decade, quantum computers will be able to break a blockchain's cryptographic codes. Recent advances in quantum computing seem to suggest it is only a matter of time before general quantum computers become a reality. Grover's algorithm [Grover (1996)] might also affect symmetric encryption and hashing, but we currently do not know how to get more than a quadratic speedup over a classical computer. It is estimated that it will take 4,000 qubits to break the strongest encryption standards of today. Many researchers have pointed out that blockchain cannot resist quantum attacks [Aggarwal, Brennen, Lee et al. (2017); Fedorov, Kiktenko and Lvovsky (2018)].

Post-quantum cryptography is a new branch of cryptography interested in a suite of algorithms which are believed to be secure even against attackers equipped with quantum computer. There are four main branches of postquantum cryptosystems: based on Codes, on Multivariate Public Key Cryptosystem (MPKC), on Hash or on lattice. Lattice-based cryptography may be an alternative cryptography since it is proved to be hard even for quantum computers. Furthermore, lattice-based cryptography has many appealing properties, for example, it can be implemented efficiently, it relies on the worst case problem which comes with uniquely strong security guarantees [Micciancio and Regev (2004)]. Besides, we can construct some special cryptography schemes based on lattice, such as Fully Homomorphic Encryption (FHE) and Attribute-Based Encryption (ABE) for arbitrary circuits. In recent years, lattice-based cryptography has a tremendous growth and some efficient signature schemes have been proposed [Guneysu, Lyubashevsky and Poppelmann (2012); Tian and Huang (2014); Xie, Hu, Gao et al. (2016); Wu, Zhang, Wang et al. (2019); Gu, Xie and Gu (2019)].

In order to construct quantum-secured blockchain, Chalkias et al. [Chalkias, Brown, Hearn et al. (2018)] proposed Block chained Post-Quantum Signatures based on the blockchain

architecture and existing Merkle tree-based signature schemes, and their scheme and it provides more reliable quantum-security estimates because of its rooting in a secure cryptographic hash function. Yin et al. [Yin, Wen, Li et al. (2018); Li, Chen, Chen et al. (2018)] construct lightweight nondeterministic wallets and proposed new anti-quantum transaction authentication method for blockchain over lattice. However, for those lattice post quantum blockchain schemes, the generation of node signing keys requires lattice basis delegation techniques, such as ExtBasis and RandBasis. Since the signing key size and the signature length will increase dramatically after lattice basis delegation, those post quantum blockchain schemes would be inefficient in practice. In this paper, inspired by Tian et al. [Tian and Huang (2014)] aiming at tackling the critical issue of transaction size, we propose a post quantum blockchain over lattice. By using SampleMat and signature without trapdoor, we can reduce the key size and signature size of our transaction authentication approach by a significant amount. Instead of using a whole set of vectors as a basis, we can use only one vector and rotate it enough times to form a basis. Based on the hardness assumption of Short Integer Solution (SIS), we demonstrate that the proposed anti-quantum transaction authentication scheme over lattice provides existential unforgeability against adaptive chosen-message attacks in the random oracle.

The remainder of this paper is organized as follows. Section 2 presents structure of blockchain and vulnerabilities of modern blockchain networks to a quantum computer. Section 3 gives some necessary preliminaries of our scheme. Section 4 describes our post quantum blockchain scheme in detail. Section 5 gives formal security proof of our scheme in random oracle. Section 6 presents the comparison between our scheme and one existing scheme in terms of signature size and signing key size. Finally, we concluded our work in Section 7.

2 Blockchain and quantum threat

2.1 Blockchain

Blockchain is an electronic ledger that can be openly shared among disparate users, creating an unchangeable record of their transactions. Each digital record or transaction is time-stamped and linked to the previous one in the thread called a block, and it allows users to participate in the ledger. Since each block is linked to a specific participant, Blockchain can be updated by a consensus between the participants in the system, and when new data is entered, it cannot be erased. Thus ensuring a secure and verifiable record of every transaction made in the Blockchain. The structure of the Blockchain is shown in Fig. 1.

(1) Hash: Hash value of its content.

(2) Pre.Hash: Hash value of the previous block.

(3) Mekle Root: Hash value of the previous block.

(4) Transaction: Some transactions data over a period of time in whole blockchain network.

Two important security features of Bitcoin come from the PoW (proof-of-work) and the asymmetry of cryptographic signatures in their protocols. The so-called asymmetry means that the operation can be easily performed from one direction, but it is difficult to proceed from the other direction. The purpose of the proof of workload is to prevent a

party from manipulating the blockchain alone, resulting in double spend. The basic principle of workload proof is that the client needs to do a certain difficulty to get a result, but the verifier can easily check whether the client actually does the corresponding work through the result. The second feature, the cryptographic signature, is used to authorize the transaction. It is the easiest to attack before a transaction is broadcast but added to the blockchain. If the key can be decrypted by the public key of the broadcast at this time, the key can be used to broadcast a new transaction from the original address to its own address, and the transaction can be entered into the blockchain first. Take all the bitcoins in the original address. The HASH function SHA-256 and elliptic curve digital signature algorithm (ECDSA) are used to ensure that Bitcoin is spent only by their rightful owners. If you can complete the cracking of the above two problems within a certain time, it will break the security system of Bitcoin.

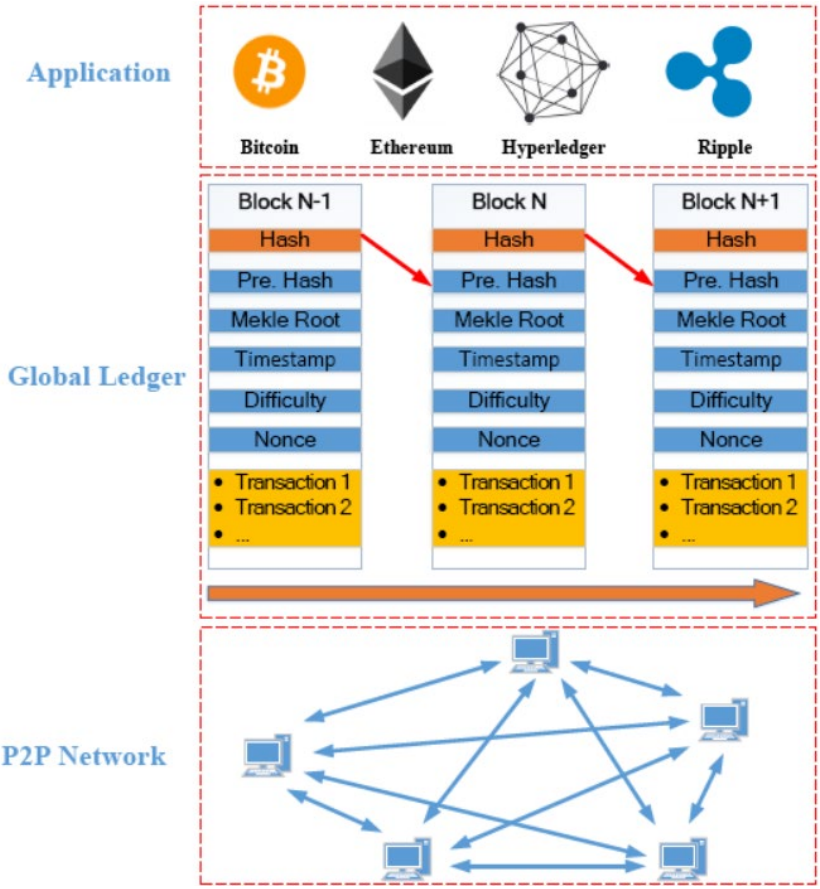

Figure 1: Structure of the blockchain

2.2 Quantum computer

Quantum computers, first theorized by physicist Richard Feynman in 1982 [Feynman

(1992)], have promised a new era of computing. For decades, theoretical physicists and computer scientists have been compiling evidence that quantum computers will eventually leave our current top-of-the-line supercomputers in the dust. The theory has only recently translated into significant real-world advances, with NASA, the CIA and Google working on a quantum computer. IBM announced a 50-quantum bit (qubit) quantum computer which is called "quantum supremacy" in November 10, 2017, and Google announced a 72-qubit universal quantum computer that promises the same low error rates in May 5, 2018. The threat from quantum computers is certainly real and not just for blockchain technology. Any information that is currently stored using conventional cryptography will become unsecure as soon as the first powerful-enough quantum computer is switched on. Computer scientists now warn the machines will cripple existing encryption methods and destroy bitcoin's technological foundations. Andersen Cheng, co-founder of Post Quantum, a U.K. cybersecurity firm, said that bitcoin will end the day the first quantum computer arrives. He said the quantum computer will undermine the cryptography surrounding bitcoin's public and private keys. Authentications in blockchain are made using the Elliptic Curve Digital Signature Algorithm (ECDSA) which cannot cope with the quantum attack by Shor algorithm [Shor (1999)].

Quantum computer may happen in the foreseeable future, which will have big influences on existing blockchain. These influences can be described as follows.

(1) Hash Pre-image: The hash function must have "pre-image resistance" and "collision resistance", furthermore, it needs to have "second pre-image resistance". A perfect hash function of output size "n" bits in blockchain still offers strong resistance which means 2 to the n/2 power or above under quantum computer with Grover algorithm [Brassard, Hoyer and Tapp (1997)]. For example, in Bitcoin, with SHA-256, a 256 bits output. In this case, best quantum computer with Grover algorithm would still need 2 to the 128 power of simultaneous operations to break pre-image resistance. Therefore, Hash function in blockchain is secure under quantum computing.

(2) Reusing Addresses: A transaction between two individuals contains the information about the public keys of the sender and receiver. While conventional computers do not possess the necessary computational power to derive a private key from a public key, quantum computer could do it rather easily. Therefore, once the transaction is published in the entire network, the public key is exposed, and the corresponding private key is no longer safe. Although some applications of blockchain technology, such as bitcoin, require that the address be changed after each transaction, this is not always followed in practice.

(3) Transactions: As shown in Fig. 1, once a transaction has been recorded in the in block N, and this transaction is placed on the blockchain with several blocks following it, then this transaction is reasonably secure against quantum attacks. As long as you try to tamper with the processed information in block N (double spending attack) with quantum computer, the following blocks will change, other nodes in the entire network will notice this change. Therefore, quantum computer cannot tamper with the processed transaction. However, once a public key was previously exposed in the transaction, and the corresponding public key was not modified after the transaction, hacker can easily use this account to generate new transaction as he/she want with quantum computer.

According to the above mentioned analysis, the biggest impact of quantum computers on

the blockchain is that hacker can easily utilize the defects of the traditional authentication to use the victim's account to generate new transactions, which will have a devastating effect on the blockchain system.

Quantum computers are hanging over the security of our information like a sword of Damocles. The economic system of cryptocurrencies would become all but useless since it would be possible for hackers to steal your coins, commit fraud and control the blockchain. If someone could easily steal your bitcoins, it would not be good for Bitcoin's reputation. Therefore, if nothing is done to update the protocols, cryptocurrencies will crash once quantum computers become available [Fedorov, Kiktenko and Lvovsky (2018)].

3 Preliminaries

3.1 Notations

In this paper, following notations would be used.

(1) N is security parameter, it is a power of 2.

(2) $||x||$ denotes the Euclidean norm of x.

(3) $x \| y$ denotes the connection of two string x and y.

(4) $R_q = \mathbb{Z}_q / (X^N + 1)$ denotes the ring of polynomials modulo $X^N + 1$ with coefficients in $\mathbb{Z}_q$.

3.2 Lattice

An $n-$dimensional integer lattice L is a discrete subgroup of $\mathbb{Z}^n$, it is generated by independent vectors $v_1, v_2, \cdots, v_n \in \mathbb{Z}^n$ through the following way:

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

The basis of L are vectors $v_1, v_2, \cdots, v_n \in \mathbb{Z}^n$, and lattice's rank is the integer n.

Definition 1 Given integers q, m, n and a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, the $q-ary$ lattices are defined as follow

$$\Lambda_q(\mathbf{A}) = \{S \in \mathbb{Z}^m : x = \mathbf{A}^T S = u(\mathrm{mod} q)\} \tag{2}$$

$$\Lambda_q^{\perp}(\mathbf{A}) = \{S \in \mathbb{Z}^m : x = \mathbf{A}^T S = 0(\mathrm{mod} q)\} \tag{3}$$

From the above definition, these two types of lattices are dual to each other.

3.3 Discrete gaussian distribution

In lattice-based signature scheme, Gaussian series are very effective techniques which are

widely used:

Definition 2 $\mathbf{s} \in \mathbb{R}^m$ is standard deviation, vector $\mathbf{c} \in \mathbb{Z}^m$ is center, the Gaussian function is defined as

$$g_{\mathbf{s},\mathbf{c}}(x) = e^{\frac{-\pi^2 ||x-\mathbf{c}||^2}{2\mathbf{s}^2}} \tag{4}$$

The discrete Gaussian distribution over Λ with center $\mathbf{c}$ and parameter $\mathbf{s}$ is defined as

$$G_{\Lambda,\mathbf{s},\mathbf{c}}(x) = \frac{g_{\mathbf{s},\mathbf{c}}(x)}{\sum_{x\in\Lambda} g_{\mathbf{s},\mathbf{c}}(x)} \tag{5}$$

Definition 2 $\sigma \in \mathbb{R}^m$ is standard deviation, vector $\mathbf{c} \in \mathbb{Z}^m$ is center, the continuous normal distribution is defined as

$$\rho^m_{\sigma,\mathbf{c}}(x) = (\frac{1}{\sqrt{2\pi\sigma^2}})^m e^{\frac{-||x-\mathbf{c}||^2}{2\sigma^2}} \tag{6}$$

The discrete normal distribution over $\mathbb{Z}^m$ with center $\mathbf{c}$ and parameter σ is defined as

$$D^m_{\Lambda,\sigma,\mathbf{c}}(x) = \frac{\rho^m_{\sigma,\mathbf{c}}(x)}{\sum_{x\in\mathbb{Z}^m} \rho^m_{\sigma,c}(x)} \tag{7}$$

When $\mathbf{c} = 0$, we can simply write $\rho^m_{\sigma,\mathbf{c}}(x), D^m_{\sigma,\mathbf{c}}(x)$ as $\rho^m_\sigma, D^m_\sigma$.

According to Lyubashevsky [Lyubashevsky (2012)], when the discrete normal distribution in dimension m with standard deviation σ, Lyubashevsky proposed some important properties of Discrete Gaussian distribution which are described as the following Lemma

Lemma 1 $\forall \sigma > 0$ and $m \in \mathbb{Z}^+$

(1) $Pr[x \in D^1_\sigma : |x| > 12\sigma] < 2^{-100}$;

(2) $Pr[x \in D^m_\sigma : ||x|| > 2\sigma\sqrt{m}] < 2^{-m}$

Lemma 2 For any $v \in \mathbb{Z}^m$ and any positive real α, if $\sigma = \omega(||v||\sqrt{\log m})$, where $\omega(.)$ is the non-asymptotic tight lower bound, then we have

$$Pr[x \in D^m_\sigma : D^m_\sigma(\mathbf{x}) / D^m_{\sigma,v} = o(1)] = 1 - 2^{\omega \log m} \tag{8}$$

More specifically, when $\sigma = \alpha||v||$, we can derive the following probability

$$Pr[x \in D^m_\sigma : D^m_\sigma(\mathbf{x}) / D^m_{\sigma,v} < e^{12/\alpha + 1/(2\alpha^2)}] > 1 - 2^{-100} \tag{9}$$

3.4 Short bases of lattices

Short basis of a lattice is an important concept in many lattice-based signature schemes.

In this paper, we recall three useful theorems on short lattice bases.

Theorem 1 [Alwen and Peikert (2011)] Let $q \geq 3$ be odd and $m > 5n\log q$. There is a probabilistic polynomial-time (PPT) algorithm $\mathbf{TrapGen}(q,n)$ that outputs a matrix $\mathbf{A} \in \mathbb{Z}_q^{m\times n}$ and a basis $\mathbf{B} \in \mathbb{Z}^{m\times m}$ of $\Lambda^{\perp}(\mathbf{A})$ such that $\mathbf{A}$ is statistical close to uniform, $\|\mathbf{B}\| \leq O(n\log q)$ and its Gram-Schmidt orthogonalization $\|\overline{\mathbf{B}}\| \leq O(\sqrt{n\log q})$ with overwhelming probability.

Theorem 2 [Gentry and Peikert (2008)] Let $m \geq n$ be an integer and q be prime. Let $\Lambda^{\perp}(\mathbf{A})$ be a lattice defined by matrix $\mathbf{A} \in \mathbb{Z}_q^{m\times n}$ and $\mathbf{B}$ be a basis of $\Lambda^{\perp}(\mathbf{A})$. If $\mathbf{s} \geq \|\overline{\mathbf{B}}\| \cdot \omega(\sqrt{\log n})$, then for any $\mathbf{u} \in \mathbb{Z}_q^n$, there is a probabilistic polynomial-time (PPT) algorithm $\mathbf{SamplePre}(\mathbf{A},\mathbf{B},\mathbf{s},\mathbf{u})$ that outputs a vector $\mathbf{v} \in \Lambda^{\mathbf{u}}(\mathbf{A})$ from a distribution that is statistical close to uniform $G_{\Lambda,s,c}(x)$.

Theorem 3 [Tian and Huang (2014)] Let $m \geq n$ and $k \geq 2$ be positive integer, and let q be prime. Let $\Lambda^{\perp}(\mathbf{A})$ be a lattice defined by matrix $\mathbf{A} \in \mathbb{Z}_q^{m\times n}$ and $\mathbf{B}$ be a basis of $\Lambda^{\perp}(\mathbf{A})$. If $\mathbf{s} \geq \|\overline{\mathbf{B}}\| \cdot \omega(\sqrt{\log n})$, then for any $\mathbf{U} \in \mathbb{Z}_q^{n\times k}$, there is a probabilistic polynomial-time (PPT) algorithm $\mathbf{SampleMat}(\mathbf{A},\mathbf{B},\mathbf{s},\mathbf{U})$ that outputs a matrix $\mathbf{S} \in \mathbb{Z}^{m\times k}$ from a distribution that is statistical close to $G_{\Lambda^{\mathbf{U}}(\mathbf{A}),s}(x)$ where $\mathbf{AS} = \mathbf{U} \bmod q$ and $\|\mathbf{S}\| \leq s\sqrt{m}$ with overwhelming probability where $G_{\Lambda^{\mathbf{U}}(\mathbf{A}),s}(x) = G_{\Lambda^{\mathbf{u}_1}(\mathbf{A}),s}(x) \times \cdots \times G_{\Lambda^{\mathbf{u}_k}(\mathbf{A}),s}(x)$.

Theorem 1 shows an effective technique on how to generate a short basis of an approximate uniform lattice. ***Theorem 2*** shows a result on how to solve a kind of SIS problems with a short lattice basis. ***Theorem 3*** introduces an efficient algorithm $\mathbf{SampleMat}$ to extract each user's signing key that is a short matrix $\mathbf{S}$ satisfying $\mathbf{AS} = \mathbf{U} \bmod q$ for some user-defined matrix $\mathbf{U}$, it is an extension of the preimage sampling algorithm $\mathbf{SamplePre}$ of ***Theorem 2***.

3.5 Rejection sampling technique

The conception of the Rejection Sampling Technique is to eliminate the relationship between signing key and output signature, the algorithm as Algorithm 1.

Algorithm 1 Rejection Sampling Technique

Input: Message u ,a matrix A randomly sampled from $\mathbb{Z}_q^{m\times n}$, $\mathbf{S}$ (signature key) sampled from $\{-d,\cdots,0,\cdots,d\}^{m\times k}$, $H:\{0,1\}^* \to \{v : v \in \{-1,0,1\}^k, \|v\| < \kappa\}$,Where

$d << q^{n/m}, k \in \mathbb{Z}$ and $<< m$, κ is constant and $2^{\kappa} \cdot \binom{k}{\kappa} \geq 2^{100}$ .Then there exists a constant $M = O(1)$.

Output: Vector $\mathbf{z}$ and $\mathbf{c}$

1. Obtain $\mathbf{y}$ randomly from D_{σ}^{m}
2. $\mathbf{c} = H(A\mathbf{y}, u)$
3. $\mathbf{z} = \mathbf{Sc} + \mathbf{y}$
4. $(\mathbf{z}, \mathbf{c})$ with probability $min(\frac{D_{\sigma}^{m}(\mathbf{z})}{MD_{\mathbf{Sc},\sigma}(\mathbf{z})}, 1)$

3.6 Hardness assumption

The security of our quantum-resistant blockchain for the post-quantum age relies on the hardness of SIS problem.

Definition 3 For an integer modular homogeneous scheme $\mathbf{Av} = 0(\mathrm{mod}q)$, get a proper solution $\mathbf{v} \in \mathbb{Z}^{m}$ where $q \in \mathbb{Z}^{m}$, $\mathbf{A} \in \mathbb{Z}_{q}^{n \times m}$, $\| \mathbf{v} \| \leq \beta$ and β is a real value, respectively.

Micciancio et al. [Micciancio and Regev (2004)] have proved that for any polynomial-bound m, β and any prime p, with small factors and the Gaussian measure, there is no difference between the hardness of average case harness of SIS and some worst case lattice problems, such as SVP (Shortest Vector Problem).

4 Our construction

Our Post-Quantum Blockchain involves a few parameters defined below:

(1) Real M, $m > 5n\log q$, $q \geq 3$, k, security parameter n and λ are positive integers.

(2) Bound $\overline{L} = O(\sqrt{n\log q})$. Gaussian parameter $s = \overline{L} \bullet \omega(\sqrt{\log n})$. $\sigma = 12\lambda sm$. Hash functions $H_1 = \{0,1\}^{*} \rightarrow \{\mathbf{v} : \mathbf{v} \in \{-1,0,1\}^{k}, \| \mathbf{v} \| \leq \lambda\}$.

In Blockchain system, address is a string that consists of numbers and letters.

4.1 Address generation

The process of generating addresses are presented as follows:

(1) Generator runs algorithm $\mathbf{TrapGen}(q, n)$ to output an approximate uniform matrix $\mathbf{A} \in \mathbb{Z}_{q}^{n \times m}$ along with a short basis $\mathbf{B}_{\mathbf{A}} \in \mathbb{Z}^{m \times m}$ of $\Lambda^{\perp}(\mathbf{A})$ and its Gram-Schmidt orthogonalization $\| \overline{\mathbf{B}_{\mathbf{A}}} \| \leq O(\sqrt{n\log q})$ with overwhelming probability. $(\mathbf{A}, \mathbf{B})$ to be saved as seed lattice basis in the wallet.

(2) Generator randomly chooses $\mathbf{A_1}, \mathbf{A_2}, \cdots, \mathbf{A_n} \in \mathbb{Z}_q^{n \times m}$. Generator concatenates the matrices $\mathbf{A_1}, \mathbf{A_2}, \cdots, \mathbf{A_N}$ behind $\mathbf{A}$ which are denoted by $\mathbf{A}_1^{'} = \mathbf{A} \,||\, \mathbf{A_1}$, $\mathbf{A}_2^{'} = \mathbf{A} \,||\, \mathbf{A}_2$, $\cdots$, $\mathbf{A}_N^{'} = \mathbf{A} \,||\, \mathbf{A}_N \in \mathbb{Z}_q^{n \times 2m}$. In order to generate the different sub-public and private keys, Generator runs algorithm $\mathbf{SampleMat}(\mathbf{A}, \mathbf{B}, \mathbf{s}, \mathbf{A_i})$ to obtain the corresponding sub private key $\mathbf{S_1}, \mathbf{S_2}, \cdots, \mathbf{S_N} \in \mathbb{Z}^{m \times k}$.

(3) Generator maps matrixes $\mathbf{A}_1^{'}, \mathbf{A}_2^{'}, \cdots, \mathbf{A}_N^{'}\} \in \mathbb{Z}_q^{n \times 2m}$ into the corresponding vector $\mathbf{V_1}, \mathbf{V_1}, \cdots, \mathbf{V_N} \in \mathbb{Z}_q^{1 \times 2nm}$.

(4) Generator obtains N different addresses $\mathbf{Ad_1}, \mathbf{Ad_2}, \cdots, \mathbf{Ad_N}$ through Secure Hash Algorithm **SHA256**), RACE Integrity Primitives Evaluation Message Digest (**RIPEMD160**) algorithm and **Base58Check** encoding algorithm, that is, $\mathbf{Ad_i} = \mathbf{Base58Check}(\mathbf{RIPEMD160}(\mathbf{SHA256}(\mathbf{V_i})))$.

The structure of the Address Generation is shown in Fig. 2.

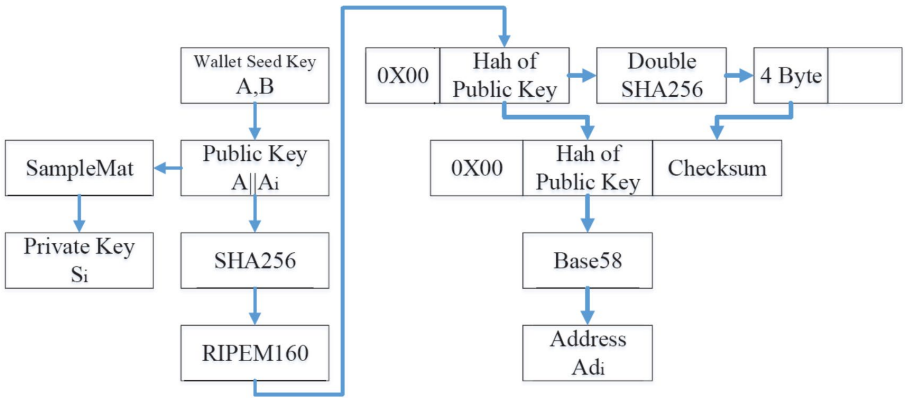

Figure 2: Address generation of post quantum blockchain

4.2 Transaction over lattice

In our post-quantum blockchain system, transaction process between node *Alice* and node *Bob* is as follows (We assume that *Alice* is a purchaser and *Bob* is a supplier):

(1) Node *Alice* initiates the transaction M request.

(2) Node *Bob* selects a pair of sub-public and private keys $B_i^{'}$, $\mathbf{S}_{Bi}$ from his wallet, and generates an address $\mathbf{Ad}_{Bi}$ through the above mentioned **Address Generation** steps, then *Bob* sends address to *Alice*.

(3) In order to prevent an attacker from forging a signature, *Alice* signs the transaction M with one private key of his wallet. The signature works as follows.

A. *Alice* selects a random $\mathbf{y} \in D_\sigma^m$.

B. *Alice* computes $\mathbf{c} = H_1(\mathbf{Ay}, M)$.

C. *Alice* computes $\mathbf{z} = \mathbf{S_i c} + \mathbf{y}$.

D. Output the signature $Sig = (\mathbf{z}, \mathbf{c})$ with probability $min(\frac{D_\sigma^m(\mathbf{z})}{MD_{\mathbf{S_i c},\sigma}(\mathbf{z})}, 1)$. If nothing is output, repeat the above steps.

(4) The transaction M, signature $(\mathbf{z}, \mathbf{c})$ and public key $\mathbf{A}_i^{'} = \mathbf{A} \,||\, \mathbf{A}_i$ are broadcast to the P2P Network.

(5) Every computer in the P2P Network checks (validate) the transaction against following validation rules that are set by the creators of the specific blockchain network. On input the public parameter, message M, public key $\mathbf{A}_i^{'} = \mathbf{A} \,||\, \mathbf{A}_i$ and signature $Sig = (\mathbf{z}, \mathbf{c})$, the signature on transaction M is valid if and only if $\| \mathbf{z} \| \leq 2\sigma\sqrt{m}$ and $\mathbf{c} = H_1(\mathbf{Az} - \mathbf{A_i c}, M)$.

Correctness of proposed scheme.

Proof According to above construction, we can see that for any message transaction M as well as public key $\mathbf{A}_i^{'} = \mathbf{A} \,||\, \mathbf{A}_i$, then we have

$$H_1(\mathbf{Az} - \mathbf{A_i c}, M) = H_1(\mathbf{Az} - \mathbf{AS_i c}, M) = H_1(\mathbf{A}(\mathbf{z} - \mathbf{S_i c}), M) = H_1(\mathbf{Ay}, M) = \mathbf{c} \quad (10)$$

Therefore, we have $\mathbf{c} = H_1(\mathbf{Az} - \mathbf{A_i c}, M)$ satisfied. According to **Lemma** 1, $\| \mathbf{z} \| \leq 2\sigma\sqrt{m}$ satisfied with probability at least $1 - 2^{-m}$.

5 Security proof

Theorem 4 The proposed post quantum blockchain system is existential unforgeable against adaptive chosen message and address attacks in the random oracle model under the hardness assumption of SIS problem.

Proof Assume that $\mathcal{A}$ is a polynomial-time adversary who breaks our Post-Quantum Blockchain scheme with non-negligible probability. We construct an algorithm $\mathcal{C}$ that can use the adversary $\mathcal{A}$ as a subroutine to solve a hard SIS problem with non-negligible probability. The steps are described as follows.

Step 1 Given the security parameter n, the algorithm $\mathcal{C}$ first randomly picks a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and secure hash function $H_1 = \{0,1\}^* \to \{\mathbf{v} : \mathbf{v} \in \{-1, 0, 1\}^k, \|\mathbf{v}\| \leq \lambda\}$, and then sends the public parameters $\mathbf{A}$, H_1 to the adversary $\mathcal{A}$.

Step 2 When $\mathcal{A}$ issues *Public Key* query on addresses $\mathbf{Ad_i}$. Although bitcoin advice different addresses are used in different transactions in order to avoid the user identity (Public

Key) exposure, basically no one obeys. Therefore, in the quantum age, when a transaction is signed, the public key $\mathbf{A}||\mathbf{A_i}$ gets revealed and private key $\mathbf{S_i}$ is no longer safe.

Step 3 When $\mathcal{A}$ issues H_1 query on $(\mathbf{Ay}, M)$. $\mathcal{C}$ looks up it in $H_1 - list$ which is a list of tuples $(\mathbf{A_i y_i}, M_i, \mathbf{c_i})$ and is initially empty. If $\mathcal{C}$ finds a matched tuple $(\mathbf{Ay}, M, \mathbf{c})$, then output $\mathbf{c}$ as response. Otherwise, $\mathcal{C}$ randomly selects $\mathbf{c}$ from $\{\mathbf{v} \in \{-1,0,1\}^k, ||\mathbf{v}|| \le \lambda\}$, stores $(\mathbf{Ay}, M)$ $H_1 - list$ and output $\mathbf{c}$.

Step 4 To obtain a signature on message M with regard to public key $\mathbf{A_i}$, $\mathcal{A}$ issues such a query on $(\mathbf{A_i}, M)$, Upon receiving the query, $\mathcal{C}$ runs the signature algorithm $Sign(PP, M, \mathbf{S_i})$ and outputs signature $Sig = (\mathbf{z}, \mathbf{c})$.

Step 5 After finishing the above queries, adversary $\mathcal{A}$ finally outputs a valid forgery $(\mathbf{z}', \mathbf{c}')$ of address $\mathbf{Ad_i}$ on transaction M with non-negligible probability. Therefore, the specific SIS problem that algorithm $\mathcal{C}$ will attack is finding a non-zero vector $\mathbf{X}$ that satisfies the condition $\mathbf{AX} = \mathbf{0} \bmod q$ and $||\mathbf{X}|| \le (4\sigma + 2s\lambda)\sqrt{m}$. Algorithm $\mathcal{C}$ is run again to solve this problem. Adversary $\mathcal{A}$ obtains the same random tape but different outputting sequence of $H_1 - query$ from $\mathcal{C}$. Adversary $\mathcal{A}$ outputs a new forgery $(\mathbf{z}^*, \mathbf{c}^*)$ of address $\mathbf{Ad_i}$ on transaction M where $\mathbf{c}^* \neq \mathbf{c}'$.

$$\mathbf{Az}' - \mathbf{P_i c}' = \mathbf{Az}^* - \mathbf{P_i c}^* \tag{11}$$

Substituting $\mathbf{P_i} = \mathbf{AS_i}$ into the above equation, then we have

$$\mathbf{A}(\mathbf{z}' - \mathbf{z}^* + \mathbf{S_i c}^* - \mathbf{S_i c}') = 0 \tag{12}$$

According to the **Lemma** 1, $||\mathbf{z}'|| \le 2\sigma\sqrt{m}$ and $||\mathbf{z}^*|| \le 2\sigma\sqrt{m}$, with overwhelming probability. Furthermore, $||\mathbf{S_i c}^*|| \le s\lambda\sqrt{m}$ and $||\mathbf{S_i c}|| \le s\lambda\sqrt{m}$ with overwhelming probability based on previous parameter selection, then we have

$$||\mathbf{z}' - \mathbf{z}^* + \mathbf{S_i c}^* - \mathbf{S_i c}'|| \le (4\sigma + 2s\lambda)\sqrt{m} \tag{13}$$

Step 5 If $\mathbf{z}' - \mathbf{z}^* + \mathbf{S_i c}^* - \mathbf{S_i c}' \neq 0$, then it is an effective solution of Short Integer Solution problem. Now we should prove $\mathbf{z}' - \mathbf{z}^* + \mathbf{S_i c}^* - \mathbf{S_i c}' \neq 0$ with overwhelming probability. Since $\mathbf{c}^* \neq \mathbf{c}'$. According to the Property 4 of Collision-Resistant preimage sampleable functions [Lyubashevsky (2012)], the probability that algorithm $\mathcal{C}$ can solve the SIS is at least $1 - 2^{\omega \log m}$.

6 Performance evaluation

We compared our scheme with Li et al.'s [Li, Chen, Chen et al. (2018)] scheme in Tab. 1 in terms of sub private key size and signature size of transaction. Here, N and λ are

security parameters, m is an integer lager than $5N\log q$, $L = o(\sqrt{n\log q})$, $\sigma = 12\lambda sN$ and $M = \omega(\sqrt{\log q})$, respectively. $\overline{s} = s\sqrt{(c+1)m}\omega(\sqrt{\log n})$, $\hat{s} = sm\omega(\log^{3/2} n)$. One can easily check that the signing key size and the signature length of our scheme are both much smaller than Li et al.'s [Li, Chen, Chen et al. (2018)] scheme.

Table 1: Comparion between our scheme and Li et al.'s scheme

	[Li, Chen, Chen et al. (2018)]	Our Scheme
Sub Private Key Size	$(m(c+1))^2 \log\ (\overline{s}\sqrt{(c+1)m})$	$mk \log\ (s\sqrt{m})$
Signature Size	$m(c+1)\log\ (\overline{s}\sqrt{(c+1)m}) + n$	$m \log 12\sigma + \lambda\ (\log\ k + 1)$

Whereas signing a transaction in the scheme of Li et al. [Li, Chen, Chen et al. (2018)] to run the more complicated algorithm **SamplePre** . Moreover, the sub private key generation algorithm in our scheme is the algorithm **SampleMat** , which is much faster than the algorithm **RandBasis** and **ExtBasis** used in the sub private key generation algorithms of Li et al. [Li, Chen, Chen et al. (2018)] scheme. Therefore, we can conclude that our Post-Quantum Blockchain scheme is more efficient in terms of both communication and computation overhead.

7 Conclusion

With the surprising development of quantum computer and blockchain, constructing a quantum-secure efficient blockchain scheme has become a priority. Lattice is one of the existing quantum-secure cryptographic primitive. In this work, we introduced Post-Quantum Blockchain over Lattice that does not employ the key generation and signature framework of Li et al. The ideas and techniques used in this work make our scheme perform better than others based on lattices. Our scheme is existentially unforgeable in the random oracle model under the SIS assumption. However, the size of our Post-Quantum Blockchain is still bigger than conventional non-quantum schemes such as RSA, ECDSA. We intend to investigate the construction of more practical lattice-based blockchains in the future.

Acknowledgement: The authors wish to express their appreciation to the reviewers for their helpful suggestions which greatly improved the presentation of this paper. This work was supported by the Major Program of National Natural Science Foundation of China (11290141).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

Aggarwal, D.; Brennen, G. K.; Lee, T.; Santha, M.; Tomamichel, M. (2017): Quantum attacks on bitcoin, and how to protect against them. arXiv:1710.10377.

Agyekum, O.; Opuniboachie, K.; Xia, Q.; Sifah, E. B.; Gao, J. et al. (2019): A secured proxy-based data sharing module in IoT environments using blockchain. *Sensors*, vol. 19, no. 5, pp. 12-35.

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

Alwen, J.; Peikert, C. (2011): Generating shorter bases for hard random lattices. *Theory of Computing Systems*, pp. 535-553.

Brassard, G.; Hoyer, P.; Tapp, A. (1997): Quantum cryptanalysis of hash and claw-free.

Campbell, S. R. (2019): Evaluation of post-quantum distributed ledger cryptography. *Journal of the British Blockchain Association*, vol. 2, no. 1, pp. 76-79.

Chalkias, K.; Brown, J.; Hearn, M.; Lillehagen, T.; Nitto, I. et al. (2018): Blockchained post-quantum signatures. *IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 1196-1203.

Fedorov, A. K.; Kiktenko, E. O.; Lvovsky, A. I. (2018): Quantum computers put blockchain security at risk. *Nature*, pp. 465-470.

Feynman, R. P. (1982): Simulating physics with computers. *International Journal of Theoretical Physics*, vol. 21, no. 6, pp. 467-488.

Gentry, C.; Peikert, C.; Vaikuntanathan, V. (2008): Trapdoors for hard lattices and new cryptographic constructions. *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*, pp. 197-206.

Grover, L. K. (1996): A fast quantum mechanical algorithm for database search. arXiv:quant-ph/9605043.

Gu, Y.; Xie, X.; Gu, C. (2019): A new NTRU-type public-key cryptosystem over the binary field. *Computers, Materials & Continua*, vol. 60, no. 1, pp. 305-316.

Guneysu, T.; Lyubashevsky, V.; Poppelmann, T. (2012): Practical lattice based cryptography: a signature scheme for embedded systems. *Cryptographic Hardware and Embedded Systems*, pp. 530-547.

Jiang, Y.; Wang, C.; Wang, Y.; Gao, L. (2019): A cross-chain solution to integrating multiple blockchains for IoT data management. *Sensors*, vol. 19, no. 9, pp. 20-42.

Li, C. Y.; Chen, X. B.; Chen, Y. L.; Hou, Y. Y.; Li, J. (2018): A new lattice-based signature scheme in post-quantum blockchain network. *IEEE Access*, vol. 7, pp. 2026-2033.

Lyubashevsky, V. (2012): Lattice signatures without trapdoors. *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 738-755.

Micciancio, D.; Regev, O. (2004): Worst-case to average-case reductions based on gaussian measures. *IEEE Symposium on Foundations of Computer Science*, vol. 37, no. 1, pp. 372-381.

Shor, P. W. (1999): Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *Quantum Entanglement and Quantum Information*, vol. 41, no. 6, pp. 303-332.

Tian, M.; Huang, L. (2014): Efficient identity-based signature from lattices. *International Information Security Conference*, pp. 321-329.

Wu, F.; Yao, W.; Zhang, X.; Wang, W.; Zheng, Z. (2019): Identity-based proxy signature over NTRU lattice. *International Journal of Communication Systems*, vol. 32, no. 3, e3867.

Xie, J.; Hu, Y. P.; Gao, J. T.; Gao, W. (2016): Efficient identity-based signature over NTRU lattice. *Frontiers of Information Technology & Electronic Engineering*, vol. 17, no. 2, pp. 135-142.

Yang, J.; He, S.; Xu, Y.; Chen, L.; Ren, J. (2019): A trusted routing scheme using blockchain and reinforcement learning for wireless sensor networks. *Sensors*, vol. 19, no. 4, pp. 970.

Yang, M.; Zhu, T.; Liang, K.; Zhou, W.; Deng, R. H. (2019): A blockchain-based location privacy-preserving crowdsensing system. *Future Generation Computer Systems*, vol. 94, pp. 408-418.

Yin, W.; Wen, Q.; Li, W.; Zhang, H.; Jin, Z. (2018): An anti-quantum transaction authentication approach in blockchain. *IEEE Access*, vol. 6, pp. 5393-5401.