IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 28, 2018, accepted December 10, 2018, date of publication December 17, 2018,
date of current version January 7, 2019.

Digital Object Identifier 10.1109/ACCESS.2018.2886554

A New Lattice-Based Signature Scheme in Post-Quantum Blockchain Network

CHAO-YANG LI[1,2], XIU-BO CHEN[1,3], YU-LING CHEN[3], YAN-YAN HOU[4], AND JIAN LI[2,4]

[1]Information Security Center, State Key Laboratory of Networking and Switching Technology,
Beijing University of Post and Telecommunications, Beijing 100876, China
[2]School of Computer Science, Beijing University of Post and Telecommunications, Beijing 100876, China
[3]Guizhou University, Sate Key Laboratory of Public Big Data, Guizhou Guiyang, 550025, China
[4]Center for Quantum Information Research, Zaozhuang University, Zaozhuang 277160, China

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

This work was supported in part by the National Natural Science Foundation of China Grant U1636106, Grant 61671087, and Grant 61170272, in part by the Natural Science Foundation of Beijing Municipality under Grant 4182006, in part by the Major Science and Technology Support Program of Guizhou Province under Grant 20183001, and in part by the Open Foundation of Guizhou Provincial Key Laboratory of Public Big Data under Grant 2018BDKFJJ016 and Grant 2018BDKFJJ018.

ABSTRACT Blockchain technology has gained significant prominence in recent years due to its public, distributed, and decentration characteristics, which was widely applied in all walks of life requiring distributed trustless consensus. However, the most cryptographic protocols used in the current blockchain networks are susceptible to the quantum attack with rapid development of a sufficiently large quantum computer. In this paper, we first give an overview of the vulnerabilities of the modern blockchain networks to a quantum adversary and some potential post-quantum mitigation methods. Then, a new lattice-based signature scheme has been proposed, which can be used to secure the blockchain network over existing classical channels. Meanwhile, the public and private keys are generated by the Bonsai Trees technology with *RandBasis* algorithm from the root keys, which not only ensure the randomness, but also construct the lightweight nondeterministic wallets. Then, the proposed scheme can be proved secure in random oracle model, and it is also more efficient than similar literatures. In addition, we also give the detailed description of the post-quantum blockchain transaction. Furthermore, this work can help to enrich the research on the future post-quantum blockchain (PQB).

INDEX TERMS Blockchain, quantum computer, lattice-based signature, post-quantum blockchain.

I. INTRODUCTION

Blockchain technology has a tendency to make significant change for all walks of life in the near future, which can help to realize consensus in the trustless environment. Beginning with the first functional blockchain proposed by Nakamoto in 2008 as the backbone of the Bitcoin cryptocurrency [1], the successful experience attracts a number of organizations to research how to use blockchain technology to construct varieties of decentralized applications in recent years. Until now, there are over 1300 kinds of blockchain-enabled cryptocurrencies existing in the world, such as Bitcoin, Ethereum, Ripple, etc. According to incomplete estimates, the cryptocurrencies market is currently worth over 150 billion USD. Therefore, it is important to pay attention on the security of blockchain-enabled systems against the current or future attacks from the classical and quantum adversaries.

Blockchain is a term used widely to describe a public, distributed, decentration and append-only database structure with high Byzantine fault tolerance. Without the third authority center, blockchain technology can help unfamiliar users realize peer-to-peer transmission and establish a distributed block storage structure in the trustless environment (See Fig.1). It can solve the Byzantine General Problem [2] and Double Spending Problem which are generally existing in the virtual digital currency. A typical modern blockchain for cryptocurrency applications consists of two main parts: a Proof-of-work (PoW) protocol for delegating the creation of new blocks and a signature scheme for transaction verification.

Bitcoin and most modern blockchain-enabled systems use a system known as PoW to achieve distributed consensus. PoW can help find a nonce with the required zero bits to determine the block's builder. And it also can solve the problem of determining representation to form the longest timestamp chain. In order to eliminate the computational power of attackers, many modern blockchain networks are seeking

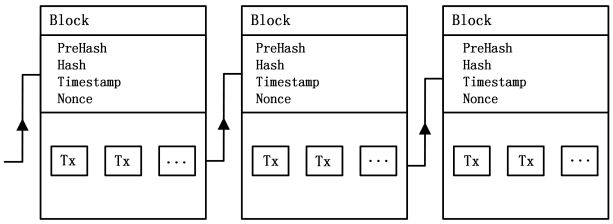


FIGURE 1. The structure of blockchain.

to replace PoW with an alternate block delegation procedure known as Proof-of-stake (PoS) [3]. It can reduce the energy costs of appending new blocks compared with the PoW based blockchain networks. The security of PoS is based on economic limitations as the fifty-one percent attacks can significantly devalue the large enough stake holders' position [4]. Meanwhile, there are any other consensus mechanisms have been presented, such as Delegated proof-of-stake (DPoS) [5] and Practical Byzantine fault tolerance (PBFT) [6].

In addition, an asymmetric signature scheme is used to authenticate the spending of coins. When a user wants to create a new transaction, he first transfers a coin by signing a hash of the previous transaction and the next owner's public key. Then, the transaction will be broadcasted to the whole blockchain network, and simultaneously verified by the miner and collected into a block. By the PoW, one node obtains rights to append the new block to the chain. While all nodes always keep working on extending the longest chain to deter the branching problem. In the end, all the transactions packaged in this block are not considered finalized until following six blocks have been confirmed and attached to the blockchain.

With the rapid development of quantum computers, the encryption algorithms underlying the security of modern blockchain networks is based on assumptions of intractability for certain tasks for classical adversaries, which do not necessarily hold for adversaries equipped with quantum computers. In order to resist these quantum attacks, Post-Quantum Blockchain (PQB) equipped with anti-quantum signature scheme should be a helpful solution to improve the security of transaction processing in Post-Quantum Blockchain network (P-QBN). Recently, [7] and [8] presented quantum resisting signature schemes based on lattice cryptography for transaction authentication in blockchain-enabled systems. However, there will be more other methods which can mitigate the quantum attacks, and it is important to pay more attention on these vulnerabilities and potential solutions.

A. OUR CONTRIBUTION

- We give an analysis of the vulnerabilities of modern blockchain networks to a quantum adversary by the two popular Shor and Grover algorithms, and summarize four kinds of potential post-quantum mitigation methods in section II.
- We propose a new lattice-based signature scheme, which can be used to secure the blockchain network over existing classical channels. And the bonsai tree technology has been used to generate the sub-public and sub-private keys, which can maintain the wallet lightweight. Moreover, security of the proposed signature scheme is based on the Short Integer Solution (SIS) problem. In addition, the security proof indicates that the proposed signature scheme is strongly unforgeable under adaptively chosen message attack in random oracle model. And the size of the public key, private key and signature is smaller than the similar literatures, which can decrease computational complexity and increase the implementation efficiency.
- We give a detail description of the post-quantum blockchain transaction in three cases. The proposed signature scheme can protect the transaction implementation in the P-QBN from quantum attacks.

B. PAPER ORGANIZATION

Following is the organization of this paper: In section II, an overview of the vulnerabilities of modern blockchain networks to a quantum adversary and some potential post-quantum mitigation methods are provided. In section III, given some lattice theoretical knowledge and related facts. In section IV, a new lattice-based signature scheme has been proposed for P-QBN, while the security proof and efficiency comparison have been presented. In section V, described the detail steps of the post-quantum blockchain transaction. At last, given the conclusion in section VI.

II. QUANTUM VULNERABILITIES AND POST-QUANTUM MITIGATION

A. QUANTUM VULNERABILITIES

Unfortunately, the digital signature schemes used for transaction authentication in most blockchain networks present a significant vulnerability to a quantum adversary along with the rapid development of quantum computer [9]. As everyone knows, the quantum computer can afford super-polynomial speedup to solve the classical mathematic hard problems over a finite Abelian group, which is widely used in most modern asymmetric cryptosystems. Meanwhile, attacks on the popular digital signature schemes can be cast as an instance of the Abelian Hidden Subgroup Problem (HSP) [10]. For example, the RSA cryptosystem is built upon the finite Abelian group Z_n^*; and the Elliptic Curve Digital Signature Algorithm (ECDSA) used in Bitcoin is constructed with a finite Abelian group structure based on elliptic curves. Then, the integer factorization, the discrete logarithm, and other instances of the Abelian HSP can be reduced to the problem of period finding, while this problem can be solved by the Fourier transform performed on quantum computer [11]. Moreover, Shor's algorithm [12] also can provide an exponential speedup for integer factorization and the discrete logarithm problem by the quantum Fourier transform. By this, the digital signature algorithms applied in most current blockchain systems will be broken. Even worse, the users'

private information will be exposed to the adversary, and their property will suffer great loss.

PoW systems mainly rely on solving a searching problem. Equipped with a quantum computer, Grover's algorithm [13] can provide a quadratic speedup for all searching problems. As it can seek the pre-image to a function value in time of order $O(\sqrt{n})$, which is more significantly faster than the classical brute force search in time $O(n)$ (Classical attack). Therefore, there are two ways to attack the blockchain-enabled systems based on the Grover's algorithm.

- One is that it can be used to search for hash collision, which can be used to replace blocks in situ without disturbing the integrity of the blockchain.
- The other is that it can speed up the generation of nonce in mining time, making the reconstruction of the chain from a modified block forward much faster, thereby opening the attack of regenerating the chain by undermining the computational effort of extension.

As a consequence, it not only can dominate the generation of the new blocks by mining faster, but also can easily rewrite the history of the tamper-resistant transaction records. Therefore, these vulnerabilities should be paid more attention, and it is urgent to seek potential solutions to resist these attacks.

B. SOME POST-QUANTUM MITIGATION

In order to resist the quantum attack, a lot of efforts have been invested by many researchers in recently years. As a whole, there are some visions which have much promising to counter these threats as follows:

- Quantum-resistant cryptography. Developing quantum-resistant (e.g. Post-quantum) cryptographic tools, such as the Hash-based cryptography and the lattice-based cryptography, is more practical for the current blockchain network.
- Post-quantum blockchain (PQB). PQB is the quantum informational vision system, which is classical blockchain system equipped with the post-quantum cryptography or the classical blockchain storage structure with quantum communication.
- Quantum hashing. Quantum hashing has been considered as a more robust system against various distortions than the binary hash system using the same intermediate hash values [14].
- Quantum networked time machine. Reference [15] has presented a conceptual design for a quantum blockchain using entanglement in time, which is a more novel method for resisting quantum attack compared with the current classical blockchain.

Quantum-resistant cryptography will be some classical algorithms which can mitigate the attack from quantum computer. Although some digital signature algorithms based on prime factorization of large numbers and discrete logarithms can be easily solved by Shor's algorithm on a sufficiently powerful quantum computer. There always exist a number of promising classical cryptographic systems that are believed to be robust against the attacks from neither classical nor quantum devices [16], such as the hash-based cryptography, code-based cryptography, lattice-based cryptography and multivariate-quadratic-equations cryptography.

As the PQB, there are some literatures [17]–[20] which have added quantum features into classical blockchain to resist the quantum computer attacks. Reference [21] added a QKD network layer into the current blockchain system to protect the relevant sub-algorithm against the quantum attacks. However, the number of QKD authenticated communications for the block creation procedure in the scheme scales as $O(n^2)$. It is likely not viable for securing a full-scale cryptocurrency, but may be useful for securing smaller distributed databases. There are existing many protocols which encode and store information in a quantum system to make the information tamper-proof. Especially, there has a proposal for ''Quantum Bitcoin'' [22], which uses a classical blockchain ledger to store transaction data but quantum methods to mine a block and verify the transactions. And there also exist some quantum bit commitment protocols which may be considered as a type of alternative to digital signature schemes. Additionally, [23] gave a detailed discussion about PQB. While, a proposal for an unconditional secure blockchain over quantum internet has been presented. For example, a secure multi-party coin flipping protocol can be used in a blockchain network as a source of entropy to elect a block creator in a PoS scheme. To establish a unconditionally secure blockchain over quantum channels, in the ideal case, one could conceive of a scheme that used quantum digital signatures for signing transactions together with a PoS-based consensus procedure using unconditionally secure multi-party coin flipping over QKD secured channels. In addition, the scalability of this ideal system will be improved by the research on the communication-efficient unconditionally secure multi-party coin flipping.

Quantum hashing incorporates uncertainty in the hash values rather than uses definitive hash values in binary hashing, which can improve the robustness of the binary hashing systems by effectively eliminating the effects of the distortion in binary encoding [14]. Nevertheless, this is a novel method for multimedia identification. Whether this method is suitable for designing cryptographic algorithms against quantum attacks still needs further exploration and research.

Quantum networked time machine is a conceptual design for quantum blockchain. As in [15], they took the temporal GHZ (Greenberger-Horne-Zeilinger) state of photons as the blockchain. Which provides the crucial quantum advantage by the entanglement in time comparing with the entanglement in space. In this conceptual system, a temporal Bell state has been taken as the block which can contain two classical records, and a growing temporal GHZ state has been taken as a chain into which the temporal Bell state can be recursively projected by fusion process [24]. This work presents a significant development of classical blockchains and the realistic possible of the pure quantum blockchain.

III. LATTICE AND RELATED FACTS

A. RELATED LATTICE KNOWLEDGE

As for the post-quantum mitigation, lattice cryptography is appropriate for the designing of quantum resisting signature scheme in P-QBN. In 2008, [25] presented the first provable secure lattice-based signature scheme in which a novel cryptographic primitive called the preimage sample function (PSF), while this scheme was designed in the random oracle and which can be reduced to the short integer solution (SIS) problem [26]. References [27] and [28] designed two novel signature schemes in the standard model by the bonsai tree technology, which could extend the trapdoor lattice basis to a high-dimension trapdoor basis. However, the public key and private key size in above two schemes are large, because the authentication keys must consist of a group of matrices which result in the large space size of the authentication keys. Then, [29] proposed a more efficient lattice-based signature scheme, and this scheme could achieve the security under adaptively chosen message attack. Recently, [30] has given an implementation and evaluation of a lattice-based key-policy attribute-based encryption scheme. And [7], [8] presented the anti-quantum cryptographic schemes based on the lattice cryptography to strength the transaction authentication process in P-QBN. Here, [7] took the Bonsai Tree technology to construct a lightweight nondeterministic wallets and proposed a new anti-quantum transaction authentication method for blockchain; and [8] gave a simple definition of the PQB, and presented a secure lattice-based cryptocurrency scheme based on PQB. Although the former mentioned lattice-based cryptographic schemes can provide the theoretical support for the application of blockchain in the post quantum age, but they are not efficient and practical in P-QBN.

In this paper, a new lattice-based signature scheme for the P-QBN has been proposed. Here, the sub-public and private keys are generated by the Bonsai Trees technology from the root keys. And more importantly, we take **RandBasis** algorithm along with the **ExtBasis** algorithm, which not only can construct a lightweight nondeterministic wallets, but also can ensure the randomness of the sub-private keys. Moreover, the proposed lattice-based signature scheme can provide security against quantum attacks in P-QBN. Following are some lattice facts which construct the foundation of the constitution and security proof for the proposed scheme.

B. SOME LATTICE FACTS

Definition 1 (Lattice [31]): Let $B = [b_1, b_2, \ldots, b_n] \in R^{m\times m}$ be an $m \times m$ matrix whose columns are linearly independent vectors. The lattice Λ generated by $B \in R^{m\times m}$ is the set

$$\Lambda(B) = \{Bx : x \in Z^m\}$$

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

$$\begin{cases} \Lambda_q^{\perp}(A) := \{y \in Z^m | Ay = 0 \ mod \ q\} \\ \Lambda_q^{u}(A) := \{y \in Z^m | Ay = u \ mod \ q\} \end{cases}$$

Here, these lattices are dual to each other, up to normalization, namely, $\Lambda_q^{\perp}(A) = q \cdot \Lambda_q(A)^*$ and $\Lambda_q(A) = q \cdot \Lambda_q^{\perp}(A)^*$.

Lemma 1 (The Trapdoor Sampling Algorithm [32]): For any prime $q = poly(n)$ and $m \geq cnlogq$, where $c > 0$ is a fixed constant, there is a probabilistic polynomial time algorithm that, on input 1^n, outputs a matrix $A \in Z_1^{n\times m}$, and a full-rank set $S \subset \Lambda^{\perp}(A)$, where the distribution of A is statistically close to the uniform distribution, and $||S|| \leq O(nlogq)$. In particular, the set S can be efficiently converted to a trapdoor basis T of the lattice $\Lambda_q^{\perp}(A)$.

Lemma 2 [33]: For any n-dimensional lattice Λ, vector $c \in R^n$, and reals $0 < \epsilon < 1$, $s \geq \eta_{\epsilon}(\Lambda)$, we have

$$\Pr_{x\sim D_{\Lambda,s,c}} ||x - c|| > s\sqrt{n} \leq \frac{1+\epsilon}{1-\epsilon} \cdot 2^{-n}$$

Lemma 3 [25]: There is a randomized nearest-plan algorithm, called **SampleD**, that samples from a discrete Gaussian $D_{\Lambda,s,c}$ over any lattice Λ. In each iteration, the algorithm chooses a plan at random by sampling from an appropriate discrete Gaussian over the integers Z.

Lemma 4 (Extending Control [27]): There is a deterministic polynomial-time algorithm **ExtBasis** with the following properties: given an arbitrary $A \in Z_q^{n\times m}$ whose columns generate the entire group Z_q^n, an arbitrary basis $S \in Z^{m\times m}$ of $\Lambda^{\perp}(A)$, and an arbitrary $\bar{A} \in Z^{m\times \bar{m}}$, **ExtBasis**$(S, A' = A||\bar{A})$ outputs a basis S' of $\Lambda^{\perp}(A) \subseteq Z^{m+\bar{m}}$ such that $||\tilde{S'}|| = ||\tilde{S}||$. Moreover, the same holds even for any given permutation of the columns of A'(e.g., if columns of $\bar{A}$ are both appended and prepended to A).

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

Lemma 5 (Randoming Control [27]): Let S is a m-dimension integer lattice Λ, and $s \geq ||\tilde{S}||\omega(\sqrt{logn})$, then there exists a PPT algorithm **RandBasis**(S, s), which outputs the basis S' of lattice Λ and $||S'|| \leq s\sqrt{m}$. Moreover, for any two bases S_0, S_1 of the same lattice and any $s \geq max\{||\tilde{S_0}||, ||\tilde{S_1}||\}$, the outputs of **RandBasis**(S_0, s) and **RandBasis**(S_1, s) are within $negl(n)$ statistical
distance.

The security of the known lattice-based signature schemes is based on the hardness of the SIS problem, which was first proposed in [26] and has been widely used in one-way and collision-resistant hash functions, identification schemes and digital signatures. Following is the formal definition of the SIS problem.

Definition 2 (SIS Problem): Given a uniform and random matrix $A \in Z_q^{n\times m}$ and parameters n, m, q, β, the goal of the SIS problem is to find a nonzero integer vector $v \in Z_q^m$ such that $||v|| \leq \beta$ and $Av = 0(modq)$.

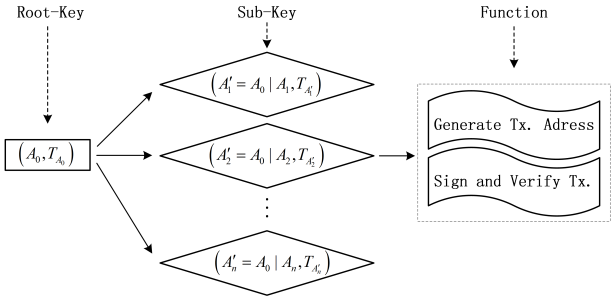


FIGURE 2. The Bonsai tree lattice-based keys generation.

IV. THE PROPOSED SIGNATURE SCHEME

A. DETAIL STEPS

Let the secure parameter n be a prime number, $m = 2nlogq$, $q = poly(n)$, and a secure hash function $H : \{0,1\}^* \to \{0,1\}^k$. Here $\tilde{L} \geq O(\sqrt{nlogq})$, and the Gaussian parameter $s = \tilde{L}\omega(\sqrt{logn})$.

Setup: On input the security parameter (SIS parameters) n and q. And according to **Lemma 1**, select a uniformly random $n \times m$- matrix $A_0 \in Z_q^{n\times m}$ with a basis T_{A_0} such that $||\tilde{T_{A_0}}|| \leq O(\sqrt{nlogq})$. Then, save (A_0, T_{A_0}) as the root lattice basis, and generate the sub-public and private keys by the bonsai tree algorithm [27, Fig. 2].

Gen: Choose two n uniformly random $n \times m$ matrixes $A_i = \{A_1, A_2, \ldots, A_n\}, i = 1, \ldots, n$ and $B_j = \{B_1, B_2, \ldots, B_l\}, j = 1, \ldots, l$. Then, calculate $A_i' = A_0 + A_i$, denote as $A_i' = \{A_1', A_2', \ldots, A_n' \in Z_q^{n\times m}\}$, and set them as the public keys for signature verification. Next, use the two algorithms **ExtBasis** and **RandBasis** to generate the corresponding secret keys as following:

$$T_{A_i'} \leftarrow \textbf{RandBasis}(\textbf{ExtBasis}(T_{A_0}, A_i' = A_0|A_i, s), s) \quad (1)$$

Then, the public keys are used for transaction (Tx.) address generation, and the public and private keys pairs $\{(A_1', T_{A_1'}), \ldots, (A_n', T_{A_n'})\}$ are used for transaction signing and verification in P-QBN. Here, to achieve the goal of user's identity anonymous, we agree that the public and private keys pair $(T_{A_i'}, A_i')$ must only be used for one time.

Sign: Given the transaction message m, input $H(m) = (m[1], m[2], \ldots, m[l])$ and the secret key $T_{A_i'}$, the signer executes the following operations:

- If $m[j] = 1$, choose B_j; otherwise $m[j] = 0$, choose nothing. Then, let l^* be the Hamming weight of the message m, and set
$$B_m = (A_i||B_{j_1}|| \cdots ||B_{j_{l^*}})$$
- Combining the **SampleD** algorithm with **Lemma 4** to generate the signature $v \in Z_q^{(l^*+1)m}$ of the transaction message m.
$$v \leftarrow \textbf{SampleD}(\textbf{ExtBasis}(T_{A_i'}, B_m, s), s) \quad (2)$$

Verify: Input transaction message m and signature v, if
$$B_m v = 0(modq), ||v|| \leq s\sqrt{(l^*+1)m} \quad (3)$$
holds, accepted; otherwise, refused.

B. CORRECTNESS

Obviously, there is no doubt about the correctness of the proposed scheme. Let n be the security parameter, and the other system parameters are generated by the **Lemma 1** and **Lemma 4**. And the algorithms **ExtBasis**, **RandBasis** and **SampleD** can be correctly executed. The algorithm **ExtBasis** can extend the basis S of lattice $\Lambda_q^{\perp}(A)$ to a bigger dimension basis S' of lattice $\Lambda_q^{\perp}(A')$. But this algorithm can not guarantee the independence of the two bases S and S'. In this paper, combining with the algorithm **RandBasis**, it can randomize the output of algorithm **ExtBasis** and improve the security of the sub-secret keys. Meanwhile, the signature v is generated by the algorithms **SampleD** and **ExtBasis**, which will be accepted by the verification algorithm with maximum probability. Therefore, the proposed signature scheme is correct.

C. SECURITY PROOF

In this part, a detail security proof for the proposed signature scheme has been given below.

Theorem 1: The proposed signature scheme in P-QBN is strongly unforgeable under adaptively chosen message attack except the probability $\frac{\varepsilon}{lq_2}$.

Proof: Under this type of forgery, the proposed signature scheme is secure, if the following **Theorem 2** holds.

Theorem 2: Challenger $\mathscr{C}$ can solve a SIS instance with the probability $\frac{\varepsilon}{lq_2}$ (l is the length of the transaction message), if there is one adversary $\mathscr{A}$ who can break the proposed scheme with the probability ε under adaptively chosen message attack by q_2 times signing queries.

Proof: Assume the challenger $\mathscr{C}$ receives an SIS instance
$$SIS_{n,(l+2)m,q,2s\sqrt{(l+1)m}} = (\bar{B}, n, m, l, q, s) \quad (4)$$
here, $\bar{B} = (\bar{B_0}, \ldots, \bar{B_k})$ and $\bar{B_i} \in Z_q^{(l^*+1)m}$. Then, he wishes to derive a short vector v satisfying
$$\bar{B}v = 0(modq), ||v|| \leq s\sqrt{(l+1)m} \quad (5)$$

Setup: The challenger $\mathscr{C}$ executes $\mathscr{A}$ to obtain q_2 messages $m^{(1)}, \ldots, m^{(q_2)}$. Then, computes set $P = \{p|p \in \{0,1\}^{\leq k}\}$, here the smallest bit string p is not all of the $m^{(i)}$'s prefixion. According to [27], this kind of set can be computed in polynomial-time, and the number of p is at most lq_2.

Next, $\mathscr{C}$ randomly chooses $p \in P$, and sets the hamming weight and length of p is t and $|p|$, respectively. Then, $\mathscr{C}$ generates the public key as following:

- Randomly chooses $|p| - t$ trapdoor lattice $\Lambda_q^{\perp}(C_j)$ and trapdoor basis $T_j \in Z_q^{m\times m}$, here $C_j \in Z_q^{n\times m}$ and $j \neq t_i, i = 1, 2, \ldots, t$. Let $B = \bar{B}_0$.
- When $i < |p|$, let $B_{t_i} = \bar{B}_{t_i}$, here $0 < t_1, t_2, \ldots, t_t < |p|$ and $p_{t_i} = 1$. The others are defined as $A_j = B_j$ according the subscript.
- When $i > |p|$, let $B_i = \bar{B}_i$.

Then, the public keys are $(B_i, C_1, \ldots, C_k)$. The challenger $\mathscr{C}$ sends the public keys and parameters (n, m, q, s, k) to the

adversary $\mathscr{A}$ and begins the query-respond game. $\mathscr{C}$ keeps a list L to store the answers of the Sign queries.

Sign Queries: Assume that the adversary $\mathscr{A}$ obtains q_2 real hash value $m^{(1)}, \ldots, m^{(q_2)}$. $\mathscr{C}$ checks the list L to make sure it is fresh; otherwise, it returns the same answer. For a new message, $\mathscr{C}$ can generate the corresponding signature. we know that p is not the prefixion of $m^{(i)}$, but it can satisfy pseudo-randomness as the hash value. Then, removes the locations $t_1, t_2, \ldots, t_t$ from former $|p|$ locations, there still exists location of 1 with probability $1-(\frac{1}{2})^{|p|-t}$. Let this kind of location be t', and the corresponding public matrix is $B_{t'} = C_{t'}$. Therefore, $\mathscr{C}$ can obtain the lattice $\Lambda_q^{\perp}(B_{t'})$. Next, $\mathscr{C}$ can generate the signature v_i of the message $m^{(i)}$ based on trapdoor basis of lattice $\Lambda_q^{\perp}(C_{t'})$. Finally, $\mathscr{C}$ send v_i back to the adversary $\mathscr{A}$ and stored $(v_i, m^{(i)})$ into L.

When the adversary $\mathscr{A}$ completes q_2 times sign queries, $\mathscr{A}$ can output a new forged signature v^* of a new message $\bar{m}$, and $B_{\bar{m}}v^* = 0(modq)$, $||v^*|| \leq s\sqrt{(t+1)m}$, here j^* is the hamming weight of $\bar{m}$ and the matrix $B_{\bar{m}}$ is same as the sign algorithm. Otherwise, p is not the prefixion of $\bar{m}$, and the matrix $B_{\bar{m}}$ is the concatenation by part of the matrixes $\bar{A}_0, \bar{B}_{t_1}, \ldots, \bar{B}_{t_t}, \bar{B}_{|p|}, \bar{B}_{|p|+1}, \bar{B}_k$. According to the relation of the matrix $B_{\bar{m}}$ and $\bar{B}$, $\mathscr{C}$ can cascade matrixes in the corresponding location and change $B_{\bar{m}}$ to $\bar{B}$, while he also can cascade vector 0 in the corresponding location and change vector v^* to $\bar{v}^*$. Here, $\bar{B}\bar{v}^* = 0(modq)$, and $||\bar{v}^*|| \leq s\sqrt{(t+1)m} \leq s\sqrt{(l+1)m}$, hence $\mathscr{C}$ can obtain a legitimate solution for the SIS instance.

In the other hand, by simple computation, the existing probability of location t' is $1-(\frac{3}{4})^{|p|}$, and $(\frac{3}{4})^{|p|}$ is negligible. Without loss generality, assume that p is the shortest bit string of P, hence bit string $p||0$ and $p||1$ are not the prefixion of any $m^{(i)}$. For example, if p is the prefixion of bit string p', then p' is not the prefixion of any $m^{(i')}$. Here the number of the bit string p' with length l is $2^{l-|p|}$. Because there are no more than lq_2 bit strings and p is the shortest bit string, hence $lq_2 2^{l-|p|}$ and $|p| \geq log_2(lq_2)$. Therefore, every bit string in P satisfies $|p| \geq log_2(lq_2)$. The probability $(\frac{3}{4})^{|p|}$ is negligible as $(\frac{3}{4})^{|p|} \leq (\frac{3}{4})^{log_2(lq_2)}$. As we know that the bit string p has chosen uniform randomly, then the probability of p with the prefixion of message m^* is $\frac{1}{lq_2}$. And $\mathscr{C}$ can solve the SIS problem with the probability $\frac{1}{lq_2}(1-(\frac{3}{4})^{log_2(lq_2)}) \approx \frac{1}{lq_2}$.

D. EFFICIENCY COMPARISON

Assume that the parameters (n, m, q, l) are the same in this paper and the similar literatures, then Table 1 shows the details of the efficiency comparison results. In [8], unfortunately, the signature size of the proposed scheme does not like the alleged $mlogq$, which should be $2mlogq+l$ according to the two equations of steps (2) and (5) in the sign phase. Even worse, coupled with the two algorithms **SampleD** and **SamplePre**, the method of double signatures will make the signature more complexity and inefficient. And comparing with the famous Bonsai trees signature scheme [27] and the identity-based signature scheme from bonsai trees [28], the size of the public and private key has been decreased with significative degree in the proposed signature scheme. And the signature size of the proposed scheme is smaller than that in [27]. Additionally, the method of public and private keys generation can improve the key generation efficiency and eliminate the wallet redundance. Therefore, this proposed lattice-based signature scheme can not only resist quantum attack, but also be more suitable for the transaction implementation in P-QBN.

TABLE 1. Comparison with similar literatures.

Scheme	Public key size	Secret key size	Signature size
Ref. [8]	$(l+1)mnlogq$	m^2logq	$2mlogq+l$
Ref. [27]	$(2l+1)mnlogq$	$4m^2logq$	$(l+1)mlogq$
Ref. [28]	$3mnlogq$	$5m^2logq$	$2mlogq$
This scheme	$mnlogq$	m^2logq	$(l/2+1)mlogq$

V. THE POST-QUANTUM BLOCKCHAIN TRANSACTION

Equipping with the former proposed quantum-resistant signature scheme, the current blockchain-enabled systems can resist the quantum attacks, which can be considered as PQB. And the post-quantum blockchain transaction will be protected by the post-quantum cryptographic scheme.

Case 1 (Transaction Preparation): Whether the general user or the miner, they are all serving as different independent entities to construct the distributed blockchain network. The transaction address is the most important thing for transaction implementation. Here, the address is generated from the public key. In order to resist the statistical attack, one new address will be generated from a different public key for a new transaction. Therefore, every user in the blockchain network should store much more public and private keys pairs for new transactions, and the wallet will become more bloat. However, the lightweight wallet designed in the former proposed signature scheme can solve this problem, which only need store the root key. By decreasing the wallet redundancy, it is more suitable for the transaction implementation in blockchain.

Case 2 (Transaction Implementation): In fact, a transaction is a data structure which includes input and output. As input with the *Previous tx*, *Index* and *ScriptSig*, here *Previous tx* is the Hash value of the previous transaction; the *Index* is the value index of the previous tx.'s output; and the *ScriptSig* is the transaction owner's signature. While output with the *Value* and *ScriptPubkey*, which are the value of transaction and the receiver's public key, respectively (see Fig. 3).

As the general user, if the user A wants to send some bitcoins through a transaction to user B, they will execute the following three steps to accomplish this transaction (see Fig. 4). Firstly, the user A initiates a transfer request. Secondly, the user B selects one public and private keys pair, generates an address and sends it to user A for transaction implementation. Last, the user A creates this transaction and broadcasts it to the whole network. Additionally, It is important to emphasize that the total input amount of the transaction

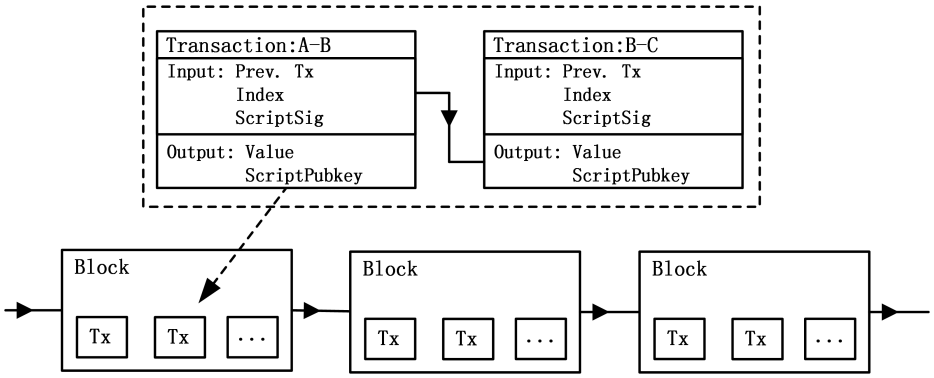


FIGURE 3. The transaction verification.

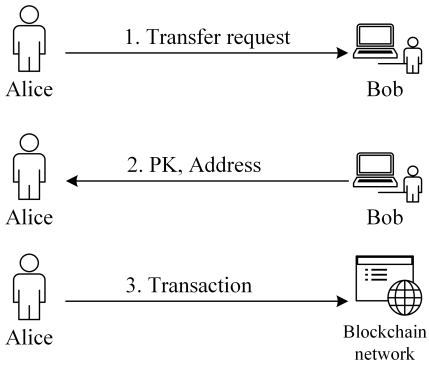


FIGURE 4. The transaction implementation.

must be equal to the total output amount. And if the user A's output amount is bigger than the required amount, he should create a new address to receive surplus bitcoins.

As the miner, the reward for establishing a new block has also been recorded as a transaction in the blockchain. In the mining process, every miner will create a special reward transaction in the temporary block which also contains the transactions broadcasted in the whole blockchain network in the latest time period. Once one miner obtains the rights for establishing the new block, the compensation deal he added will become consumable for the general transaction.

Case 3 (Transaction Confirmation): As the transactions were broadcasted to the network and verified by the miner, they will be collected and packaged into the temporary block. When the block for the latest time period has been established, the temporary block will become the new block. And all the transactions in this block have been verified for one time by attaching the new block into the longest chain. From now on, these transactions in this block will be verified many times along with the following new blocks established, since the new block is established based on the former block. In general, after six blocks, these transactions cannot be modified because of the huge computation for rebuilding six blocks. At this point, a transaction has been stored as an inalterable record in the blockchain.

VI. CONCLUSION

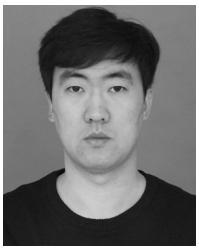
In this paper, we fist give an overview of the vulnerabilities of modern blockchain networks to the adversary who equipped with a quantum computer. With the analysis of the weakness, some works should be commenced on developing anti-quantum cryptographic tools. In section II-*B*, some potential post-quantum mitigation methods have been summarized, which are possible to weaken the quantum attacks effectively. Maybe there will be more significant methods which can intrinsically resist the quantum attacks, and it is interesting to pay more attention.

Then, a new lattice-based signature scheme has been proposed, which can be used to secure the blockchain network over existing classical channels. In the key generation phase, we combine the algorithm **RandBasis** with the algorithm **ExtBasis** to generate the sub-private keys for verifying the transaction message, which can randomize the output of algorithm **ExtBasis** and improve the security of the users' private information. Furthermore, the security proof shows that the proposed signature scheme is secure against the adaptively chosen message attack in random oracle, and the comparison results indicate that it is more efficient than similar literatures. Therefore, this scheme is more suitable for the transaction implementation in P-QBN. Additionally, the quantum blockchain which was considered as the quantum networked time machine can be investigated as a desirable solution to the quantum attacks. Moreover, this work also can help to rich the research on the future PQB in post-quantum age.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Tech. Rep., 2008. [Online]. Available: https://bitco.in/pdf/bitcoin.pdf
[2] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," *ACM Trans. Program. Lang. Syst.* , vol. 4, no. 3, pp. 382–401, 1982.
[3] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, 2014.
[4] I. Bentov, A. Gabizon, and A. Mizrahi, "Cryptocurrencies without proof of work," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Berlin, Germany: Springer, 2016, pp. 142–157.
[5] D. Larimer, "Delegated proof-of-stake (DPOS)," Whitepaper, 2014.
[6] M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," *ACM Trans. Comput. Syst.*, vol. 20, no. 4, pp. 398–461, 2002.

[7] W. Yin, Q. Wen, W. Li, H. Zhang, and Z. Jin, "An anti-quantum transaction authentication approach in blockchain," *IEEE Access*, vol. 6, pp. 5393–5401, 2018.
[8] Y.-L. Gao, X.-B. Chen, Y.-L. Chen, Y. Sun, X.-X. Niu, and Y.-X. Yang, "A secure cryptocurrency scheme based on post-quantum blockchain," *IEEE Access*, vol. 6, pp. 27205–27213, 2018.
[9] D. Aggarwal, G. K. Brennen, T. Lee, M. Santha, and M. Tomamichel. (2017). "Quantum attacks on Bitcoin, and how to protect against them." [Online]. Available: https://arxiv.org/abs/1710.10377
[10] R. Jozsa, "Quantum factoring, discrete logarithms, and the hidden subgroup problem," *Comput. Sci. Eng.*, vol. 3, no. 2, pp. 34–43, Mar. 2001.
[11] M. A. Nielsen and I. Chuang, "Quantum computation and quantum information," pp. 558–559, 2002.
[12] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Rev.*, vol. 41, no. 2, pp. 303–332, 1999.
[13] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. 28th ACM Symp. Theory Comput.*, 1996, pp. 212–219.
[14] M. Jin and C. D. Yoo, "Quantum hashing for multimedia," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 4, pp. 982–994, Dec. 2009.
[15] D. Rajan and M. Visser. (2018). "Quantum blockchain using entanglement in time." [Online]. Available: https://arxiv.org/abs/1804.05979
[16] D. J. Bernstein, "Introduction to post-quantum cryptography," in *Post-Quantum Cryptography*. Berlin, Germany: Springer, 2009, pp. 1–14.
[17] K. P. Kalinin and N. G. Berloff. (2018). "Blockchain platform with proof-of-work based on analog Hamiltonian optimisers." [Online]. Available: https://arxiv.org/abs/1802.10091
[18] D. Sapaev, D. Bulychkov, F. Ablayev, A. Vasiliev, and M. Ziatdinov. (2018). "Quantum-assisted blockchain." [Online]. Available: https://arxiv.org/abs/1802.06763
[19] A. Behera and G. Paul, "Quantum to classical one-way function and its applications in quantum money authentication," *Quantum Inf. Process.*, vol. 17, no. 8, p. 200, 2018.
[20] L. Tessler and T. Byrnes. (2017). "Bitcoin and quantum computing." [Online]. Available: https://arxiv.org/abs/1711.04235
[21] E. Kiktenko *et al.*, "Quantum-secured blockchain," *Quantum Sci. Technol.*, vol. 3, no. 3, p. 035004, 2017.
[22] J. Jogenfors. (2016). "Quantum bitcoin: An anonymous and distributed currency secured by the no-cloning theorem of quantum mechanics." [Online]. Available: https://arxiv.org/abs/1604.01383
[23] A. Tan. (2018). *Post-Quantum Blockchain*. [Online]. Available: http://andrewt.me/assets/documents/phy372-final-report.pdf
[24] E. Megidish, T. Shacham, A. Halevy, L. Dovrat, and H. S. Eisenberg, "Resource efficient source of multiphoton polarization entanglement," *Phys. Rev. Lett.*, vol. 109, p. 080504, Aug. 2012.
[25] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proc. 14th Annu. ACM Symp. Theory Comput.*, 2008, pp. 197–206.
[26] M. Ajtai, "Generating hard instances of lattice problems," in *Proc. 28th Annu. ACM Symp. Theory Comput. ACM*, 1996, pp. 99–108.
[27] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, "Bonsai trees, or how to delegate a lattice basis," in *Advances in Cryptology—EUROCRYPT*. Berlin, Germany: Springer, 2010, pp. 523–552.
[28] 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.
[29] L. Ducas and D. Micciancio, "Improved short lattice signatures in the standard model," in *Proc. Annu. Cryptol. Conf.* Berlin, Germany: Springer, 2014, pp. 335–352.
[30] W. Dai *et al.*, "Implementation and evaluation of a lattice-based key-policy ABE scheme," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 5, pp. 1169–1184, May 2018.
[31] D. Micciancio and O. Regev, "Lattice-based cryptography," in *Post-Quantum Cryptography*. Berlin, Germany: Springer, 2009, pp. 147–191.
[32] F. Laguillaumie, A. Langlois, B. Libert, and D. Stehlé, "Lattice-based group signatures with logarithmic signature size," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.* Berlin, Germany: Springer, 2013, pp. 41–61.
[33] 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.



CHAO-YANG LI received the M.S. degree from the Zhengzhou University of Light Industry, Zhengzhou, 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, cryptography, and blockchain.

XIU-BO CHEN received the Ph.D. degree from the Beijing University of Posts and Telecommunications, Beijing, China, in 2009, where she is currently an Associate Professor with the School of Cyberspace Security. 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, Guiyang, China, in 2009. She is currently an Associate Professor with the Guizhou Provincial Key Laboratory of Public Big Data, Guizhou University. Her recent research interests include cryptography and information security.

YAN-YAN HOU received the M.S. degree from Shandong Normal University, in 2007. She is currently an Assistant Professor with Zaozhuang University, Zaozhuang, China. Her research interest is quantum information security.

JIAN LI received the Ph.D. degree from the Beijing Institute of Technology, in 2005. He is currently a Professor with the School of Computer, Beijing University of Posts and Telecommunications, Beijing, China. His research interests include information security and quantum cryptography.