Computer Systems Science & Engineering
DOI:10.32604/csse.2021.017507
BlockChain Technology

A Novel PoW Scheme Implemented by Probabilistic Signature for Blockchain

Bo Mi[1], Yuan Weng[1], Darong Huang[1,*], Yang Liu[1] and Yuqing Gan[2]

[1]Institute of Information Science and Engineering, Chongqing Jiaotong University, Chongqing, 400074, China
[2]Electrical and Electronics Engineering Department, The University of Sheffield, Sheffield, S102TT, United Kingdom
[*]Corresponding Author: Darong Huang. Email: drhuang@cqjtu.edu.com
Received: 01 February 2021; Accepted: 16 March 2021

Abstract: PoW (Proof of Work) plays a significant role in most blockchain systems to grant an accounting right over decentralized participants and ensure tamper resistance. Though hash functions are generally exploited for PoW due to their merits on summering, anti-collision, and irreversibility, they cannot certify that the bookkeeper is exactly the worker. Thereafter, such insistence may lead to abuse or even embezzlement of computing power for the benefit of malicious miners. To preserve the functionality of PoW but also bind the miners' signing keys with their works, we build a post-quantum PoW scheme by changing the approximate closest vector norm for probabilistic NTRUSign. Different from the schemes based on hash functions, our scheme takes signing as the proof of work where signature verification is just the evidence of block reward. We also presented a method to adjust the difficulty of signing by modifying the probability of generating a correct signature. The performance of our scheme is also analyzed theoretically and experimentally, which implies its practicability and advantages.

Keywords: Proof of work; NTRUSign; Burr distribution; blockchain

1 Introduction

Blockchain is now an important carrier of electronic money due to its advantage of tamper resistance. In addition to the field of electronic cash [1], academia [2–5] also suggests using blockchain to combat cybercrime, curb network rumors, or make the IoT (Internet of Things) more credible. Thanks to the difficulty of a hash collision, hash function-based PoW schemes are generally deemed secure and reliable for digital currencies [6]. However, Wang's team [7] has already realized a rapid collision for MD5 (Message-Digest Algorithm 5) and SHA-1 in 2004 and 2005, which implies the vulnerabilities of other hash functions and also the fragility of most PoW. Moreover, with the advent of the quantum era, the consensus mechanism originally used in the blockchain is now facing more challenges. As explored by Zhang et al. [8], Gao et al. [9], Fernández-Caramès et al. [10], and Li et al. [11], there is a great gap between the development of blockchain and its resistance against quantum machines.

As for space occupation, the size of each block is quite limited within blockchains. Taking BTC (bitcoin) for example, a block can only be generated smaller than 1 M bytes to ensure the efficiency and security of the chain. When exploiting the hash function to achieve PoW, the node who wins the right to generate a block

must write a nonce together with his reward in it. These data will inevitably cause waste of storage if the block is small. To address such issue, Xiao et al. [12] suggested replacing the hash puzzle (generating a specific hash value by changing the nonce) by solving the SAT (Propositional Satisfiability) problem as a competition, Liu et al. [13] presented a PoW scheme based on ECDLP (Elliptic Curve Discrete Logarithm Problem), while Shahriar et al. [14] exploited parallel mining instead of solo mining for PoW which also accelerated the rate of block generation.

In consideration of the aforementioned problems, we base the security of PoW on a well-studied problem named appr-CVP (approximate Nearest Vector Problem) [15] over lattice for block generation. Such a problem is provided with the merit of anti-quantum whose difficulty can also be adjusted by changing the precision of approximation. Thanks to the reduction between NTRUSign (Signature Protocol of Number Theory Research Unit) and appr-CVP, we take signing as the proof of work to testify the right of block generation. Combing the processes of signing with mining also brings about a significant property that the bookkeeper cannot usurp unauthorized computing powers unless exposing his secret key. To mimic the capacity of dynamic block generation rate as in bitcoin, our scheme is capable of controlling the probability of signing success for NTRUSign [16]. The core concept of our scheme is to carry out signing and mining at the same time, implying that the miners' signing keys are bounded with their works and their reward records can be omitted in blocks. Besides, the signatures can be verified in batches, thus the authenticity of the block can also be quickly verified without tracing the sources along with the hash values block by block.

It is worth mentioning that our scheme is not a trivial combination between PoW and NTRUSign. In the original NTRUSign scheme, the author only estimated the success rate of signing, without any detailed analysis of the range probability for correct signature. Based on NTRUSign, we carefully analyzed the distribution of the signing success and exploit such distribution to construct our scheme which replaces the hash puzzle. During the process of derivation, we used the joint distribution of multiple independent exponential distributions to manipulate the distribution parameters after signing, thus the parameters can be well-fitted via burr distribution [17] in the gamma function family. We also programmed the entire signing process in C language to verify the reliability of such distribution. Based on mathematical analysis, the cumulative probability function of the burr distribution [18,19] was practically used to select the parameters which coordinate with an expected workload, as verified in our experiment.

For clarity, we will first take BTC as an instance to present related concepts of PoW as well as the construction of NTRUSign.

PoW: The PoW technology used in Bitcoin was proposed by Satoshi Nakamoto to ensure that the distributed system can achieve even unification in an untrusted environment. Within each Bitcoin block, the hash value of all transactions needs to be included as the root of a Merkle tree [20] together with a nonce, the hash value of its parent block, and some parameters such as timestamps.

To pack a block according to the protocol, each node should calculate the hash value of the block header appended with a nonce. When the generated hash value is smaller than a certain value, the packaging will succeed. During the packing process, a specific threshold can be designated to ensure the difficulty of packing, which is related to blocking speed due to the uniform distribution of output hashes.

The primary reason for choosing the hash puzzle as the way of block generation is because the hash function is irreversible and collision-resistant while summarizing the data. The anti-collision feature can mainly be described as: for a message A, the hash operation H returns $a \leftarrow H(A)$, while the probability of finding another message B with the same value is bounded by $P(H(A) = H(B)|A \neq B) < 1/2^{256}$. Therefore, to construct a valid hash value, the adversary can only resort to exhaustive enumeration. In BTC, the problem of scrambling for accounting rights is solved by the above characteristic of the hash puzzle. Suppose that we use SHA-256 to generate a hash value with n prefixed 0 bits, then each

participant can only exhaust the random nonces to achieve a valid hash value since the probability is just $1/2^n$, it can be seen that it is almost impossible for two participants to complete the puzzle at the same time while completing for accounting right.

NTRUSign: The scheme of NTRUSign was proposed by Hoffstein, based on the approximate nearest vector problem over a lattice. It maps a message digest to a random point in a $2N$-dimensional space and solves the appr-CVP problem by finding its nearest lattice point. Thus, lattice point can be used as the signature. The authenticity of the signature can be verified by estimating the distance between the coded message and the signature.

In Hoffstein's scheme, the signer can use the shortest vector basis as his private key and easily find the nearest lattice point via this basis [21]. The public base is an inferior base with a Hadamard ratio of less than 0.1 after elementary transformation, which is can be deemed as the verifying key. It is NP-hard to solve appr-CVP under the inferior base that the verifier cannot forge the signature but quickly verify it. The security of NTRUSign was also proofed in different situations in Hoffstein's paper.

To generate the signature, we use rounding to map the message digest on the rational field to obtain an approximate lattice point. The error of the rounding is the distance to detect whether the signature is valid. Using the Euclidean center norm for expression, we found that though the discarded signatures obey gamma distribution as a whole, specific distributions are still different. In the next chapter, we will introduce the mathematical background and solve the above problem of distribution in Chapter 3, then use gamma distribution to achieve controllable probabilistic signatures.

2 Mathematical Background

The protocol suite of NTRU works over the quotient ring R/qR, for $R = Z[X]/(X^N - 1)$. There are two polynomials $f \in R, g \in R$ whose orders are $N - 1$ and can be mulitiplied via

$$f * g = \sum_{k=0}^{N-1} (f \odot g)_k X^K \in R, \tag{1}$$

where $(f \odot g)_k = \sum_{i+j \equiv k(modN)} f_i \cdot g_j (0 \le k \le N)$.

For each $q \in \mathbb{Z}$ and $h \in R$, the set $M_{h,q} = \{(u, v) \in R^2 | v \equiv u * h(modq)\}$ is an R-module of rank 2 ($M_{h,q}$ is also a lattice of $2N$-dimensions) while all elements of R can be represented as $f = \sum_{i=0}^{N-1} r_i X^i$. Therefore, the length of f is naturally measure as the centered Euclidean norm of its coefficient vector that $||\mathrm{f}|| = \sqrt{\sum_{\mathrm{i}=0}^{\mathrm{N}-1} \mathrm{r}_\mathrm{i}^2 - \left(\frac{1}{\mathrm{N}}\right)\left(\sum_{\mathrm{i}=0}^{\mathrm{N}-1} \mathrm{r}_\mathrm{i}\right)^2}$. The norm imposed between two elements on $M_{h,q}$, or more generally on $(u, v) \in R^2$, is thus the component-wise Euclidean norm $||(u, v)||^2 = ||u||^2 + ||v||^2$. Also, it is obvious that $||\mathrm{f}|| = \frac{1}{\mathrm{N}} \sum_{\mathrm{i}<\mathrm{j}} \left(\mathrm{f}_\mathrm{i} - \mathrm{f}_\mathrm{j}\right)^2$.

Noting that d_f numbers of the coefficients in f should be set to 1 while the rest coefficients are 0. Then, the norm of it is $||f|| = \sqrt{d_f(1 - d_f/N)}$.

Definition 1: The real-valued function of $R^n || \cdot ||$ is a vector norm, which satisfies:

(1) Positive definiteness: $||x|| \ge 0$, and $||x|| = 0$ only when $x = 0$.

(2) Homogeneity: $||kx|| = |k| \cdot ||x||$ for any $k \in R$.

(3) Triangle inequality: $||x + y|| \le ||x|| + ||y||$.

In our research, we will use some basic probability distributions to analyze the Euclidean center norm of the approximate shortest vector. That is to say $X \sim Exponential(\lambda)$ for $\sum_{i=1}^{N} X_i \sim gamma(c, k)$,

and the probability density function of the burr distribution over the generalized gamma burr distribution is defined as

$$f(x;c,k)=ck\frac{x^{c-1}}{(1+x^{c})^{k+1}}. \tag{2}$$

Then we change the scale of the burr to λ to get

$$f(x;c,k,\lambda)=\frac{ck}{\lambda}(\frac{x}{\lambda})^{c-1}\left[1+(\frac{x}{\lambda})^{2}\right]^{-k-1}. \tag{3}$$

Correspondingly, the corresponding cumulative distribution function is

$$F(x;v,k,\lambda)=1-\left[1+\left(\frac{x}{\lambda}\right)^{c}\right]^{-k} \tag{4}$$

From the next chapter, we will begin to construct the overall algorithmic inference process.

3 Algorithm Design

In this chapter, we will introduce the construction of NTRUSign in detail and analyze its probability distribution. NTRUSign's basic operations are addition and multiplication over a polynomial ring, so the algorithm is very efficient. Meanwhile, the signature is quantum-resistant because it is based on a lattice puzzle. Therefore, the scheme is more secure than the hash puzzle in the blockchain.

3.1 The Proposed PoW Scheme Combined with Signing

Firstly, the message should also be rounded to its nearest integer. For any message $a\in\mathbb{Q}$, denote $[a]$ as the rounding of a, where $[a]=a-\{a\}$ for $\{a\}\leq 0.5$. Similarly, as for polynomial f, $[f]$ and $\{f\}$ are respectively obtained by carry out the the same operation on its coefficients.

The algorithm can be mainly divided into three steps, that

1) *KeyGeneration*: $(Pk,Sk)\leftarrow KeyGen(N,q,d_f,f_g,S,t)$

1. Input initial integers $N,q,d_f,d_g,S\geq 0$ as security parameters and a state $t=$ "standard" or "transpose".

2. Generate S private lattice bases and one public lattice basis to execute the following process.

Let $i=S$, and $i\geq 0$, then

(a) randomly select f and $g\in R$, where the number of 1 in those polynomials are d_f and d_g respectively;

(b) find a pair of polynomials $F,G\in R$ with small coefficients, satisfying $f*G-F*g=q$;

(c) when $t=$"standard", set $f_i=f,f_i'=F$, while when $t=$ "transpose", let $f_i=f,f_i'=g$, Then compute $h_i\equiv f_i*f_i'(modq)$;

(d) let $i=i-1$ unless $i=0$.

3. Release the public key Pk: $h=h_0\equiv f_{0'}*{f_0}^{-1}modq$.

4. Secretly keep the private key Sk:$\{f_i,f_{i'},h_i\},i=0,\ldots,S$.

2) *Signing*: $(D,s)\leftarrow Sign(Sk,Pk,D,U)$

1. Let $s=0,i=S$ and $m=D$.

2. Use the private key Sk to sign as below.

When $i \geq 0$,

(a) let $x = \left[-(\frac{1}{q})m * f_{i'}\right], y = \left[(\frac{1}{q})m * f_i\right], s_i = x * f_i + y * f_{i'}$;

(b) when $i \geq 1$, let $m = s_i * (h_i - h_{i-1}) modq$;

(c) let $s = s + s_i$ and$i = i - 1$ until $i = 0$.

3. Verify the validity of the signature by computing $b = ||(s, s * h - m(modq)||$.If $b \geq U$, then regenerate D to sign. And return (D, s) otherwise.

3) *Verification*:1or0 $\leftarrow Ver(D, s, Pk)$

1. Compute $m = D, b = ||s, s * h - m(modq)||$.

2. If $b \leq U$, then the signature is valid and returns 1. Or else, returns 0.

According to the above signature process, it is clear that the success probability of signing is related to the Euclidean center norm of $(s, s * h - m(modq)$. In the following, we will analyze the distribution of this norm.

3.2 Functional Analysis of NTRUSign's Cumulative Probability

During the signing process, we intend to find a set of approximate vectors $(x, y) \in R$ such that $x * (f, g) + y * (F, G) \approx (0, m)$ for $m \in R/qR$. Using the private base we can compute

$$(x', y') = (0, m)\begin{pmatrix} f & g \\ F & G \end{pmatrix}^{-1} = \frac{1}{q}(0, m)\begin{pmatrix} G & -g \\ -F & f \end{pmatrix} = (-\frac{m * F}{q}, \frac{m * f}{q}), \tag{5}$$

Then, let $x = [x'], y = [y']$, he has

$$s = \left[-(\frac{1}{q}) * m * F\right] * f + \left[(\frac{1}{q})m * f\right] * F \approx (0, 0) \tag{6}$$

Theorem 1: If $f * G - g * F = q$ and $h = f^{-1} * g$, then $s * (g, G) \equiv s * h(modq)$.

Proof : Since

$$\begin{aligned} s * h &= (\left[-(\tfrac{1}{q})m * F\right] * f + \left[(\tfrac{1}{q})m * f\right] * F) * f^{-1} * g(mod\ q) \\ &\equiv \left[-\left(\tfrac{1}{q}\right)m * F\right] * g + \left[\left(\tfrac{1}{q}\right)m * f\right] * F * f^{-1} * g + q\left[\left(\tfrac{1}{q}\right)m * f\right] * f^{-1} (\text{mod } q) \\ &= \left[-\left(\tfrac{1}{q}\right)m * F\right] * g + \left[\left(\tfrac{1}{q}\right)m * f\right] * f^{-1} * G(\text{mod } q). \end{aligned}$$

Then, $m \approx s * (g, G) \equiv s * h(modq)$.

So, we have

$$||(0, m) - (s, s * h(modq))||^2 = ||\{x\} * f + \{y\} * F||^2 + ||\{x\} * g + \{y\} * f^{-1} * G||^2. \tag{7}$$

To obtain the distribution of the Eq. (7), we can also assume that the distributions of X and Y are uniform distributions between $(-B, B)$, thus Eq. (7) can be approximately expressed as

$$||f|| * \left(\sum_{t=1}^{N} X_i^2 - \tfrac{1}{N}\left(\sum_{t=1}^{N} X_i\right)^2 + \sum_{t=1}^{N} Y_i^2 - \tfrac{1}{N}\left(\sum_{t=1}^{N} Y_i\right)^2\right) +$$

$$||g||*(\sum_{t=1}^{N} X_i^2 - \frac{1}{N}(\sum_{t=1}^{N} X_i)^2 + \sum_{t=1}^{N} Y_i^2 - \frac{1}{N}(\sum_{t=1}^{N} Y_i)^2) \tag{8}$$

According to Theorem 1, Eq. (11) can be expressed as $(1/\mathrm{N})||a||*\sum_{;i<j \atop j<N}(X_i - X_j)^2$, for a is constant. We now know that X is a uniform distribution between $(-B, B)$. Let $R = X_i - X_j$, the probability distribution of R is

$$f_R(r) = \begin{cases} \frac{\sqrt{2}(r+B)}{B^2}, -B < r < 0 \\ \frac{\sqrt{2}(B-r)}{B^2}, 0 \le r < B \end{cases}. \tag{9}$$

And the distribution $Z = R^2$ can be obtained as

$$f_z(Z) = \begin{cases} \frac{2\sqrt{2}}{B} - \frac{2\sqrt{2z}}{B^2}, 0 < z < B^2 \\ 0, \text{ other} \end{cases} \tag{10}$$

Using the exponential distribution: $f(x; \frac{2\sqrt{2}}{B}) = \begin{cases} \frac{2\sqrt{2}}{B} e^{-\frac{2\sqrt{2}}{B}x}, (x \ge 0) \\ 0, \text{ other} \end{cases}$ to approximately represent the original R distribution, it can be observed that the difference between the two distributions is insignificant as in Fig. 1.

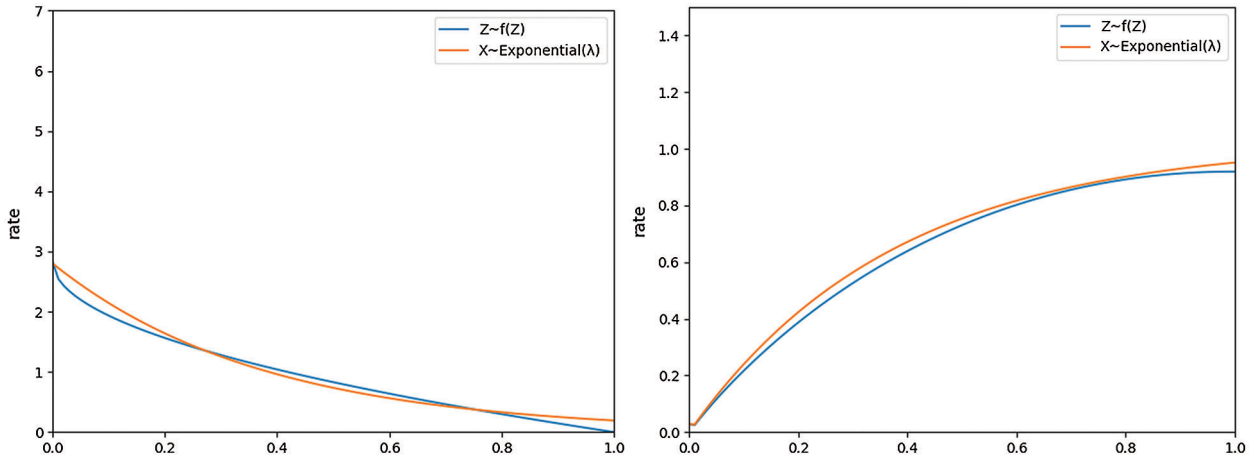

Figure 1: Z and R probability distribution(lift) and probability cumulative(right) function

Then we can approximate $||(0, m) - (s, s * h(modq))||^2$ as the result of adding multiple independent exponential distributions (with different parameters). Obviously, the resulting distribution lay within the class of the gamma distribution family, so we can use the burr distribution to fit the distribution function.

According to simulation, the cumulative distribution function can be obtained as

$$F(U^2) = 1 - [1 + (U^2/62000)^{22.4179}]^{-0.0799}. \tag{11}$$

Therefore, when the success probability of the singing needs to be less than P, we only have to set $P \le F(U^2)$ and adjust U to control the probability of a successful signature.

3.3 Application in Blockchain

In this section, we will introduce how to control the success rate of singing by changing the threshold of U in NTRUSign's. In summary, the probability distribution of the signature will be mainly explored.

If a participant wants to generate a legal block, he should use NTRUSign to generate a successful signature for the transaction ledger. In Fig. 2, it can be shown that if we use the NTRUSign scheme, reward records are no longer needed.

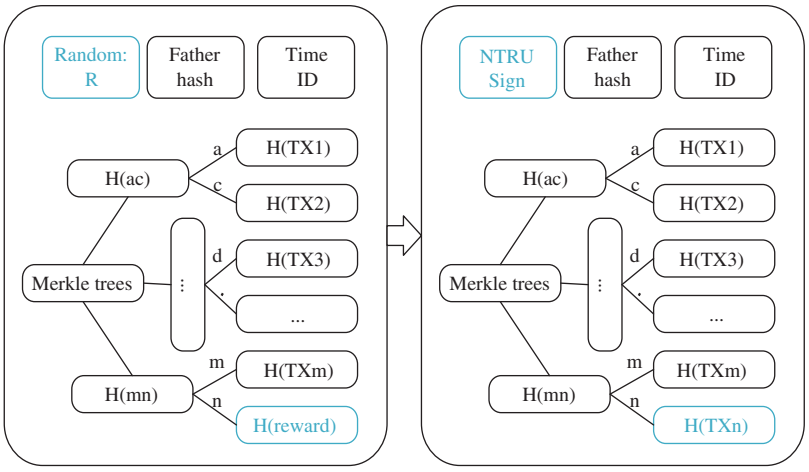

Figure 2: Block structure of hash puzzle-based scheme (left) versus Block structure of NTRUSign-based scheme (right)

In practice, the validity of the block signature should be verified before billing. Once the signature is valid, the reward record can be automatically reduced from the corresponding block (because the signing is computed by the rewarded participant), thus adding the consumption records together to generate a general ledger. The process of grabbing block generation rights is as below.

(1) Encode the data m' and randomly generate an r by $(M, r) \leftarrow Encode(m', r)$

1. Divided m' into 251 pieces that $m' = m_{1'}|m_{2'}|\ldots|m_{251'}$, where | represents the cascade symbol.

2. Let $m_i = m_i'|r$ and $m = m_1|m_2|\ldots|m_{251}$.

3. After performing the SHA-160 operation over m, then map it to Z_p to obtain the encoded data $M_i' = H(m_i) mod\ p$ for $M = \sum_{i=0}^{N-1} M_i' X^i$.

(2) Sign M as the proof of work via $(m', r, s) \leftarrow SIGN(n, P, M, r)$

1. Generate $(Pk, Sk) \leftarrow KeyGen(N, q, d_f, d_g, S, t)$.

2. According to $1/2^n = P = 1 - [1 + (U^2/62000)^{22.4179}]^{-0.0799}$ to adjust U.

3. Compute the signature as $(M, s) \leftarrow Sign(Sk, Pk, M, U)$.

4. If the signing is successful, return (m', r, s), re-encode m' or else.

For now, we have shown how to use NTRUSign to replace the hash puzzle with the same capacity of PoW. In the next chapter, we will analyze the above scheme to validate its security and corecctness.

4 Experiment and Analysis

To verify the reliability of our scheme, we should prove that the above probability function is very close to the actual experimental probability distribution.

We first employed the C language to program the signing algorithm of NTRUSign and set the security parameters as $N = 251, q = 128, d_f = 73, d_g = 71, S = 0, t =''standard''$. Then, we signed 6 million sets of data and recorded the values of $||(0, m) - (s, s * h(modq))||^2$. Comparing with the burr distribution with the actual experimental data distribution we got their difference as in Fig. 3:

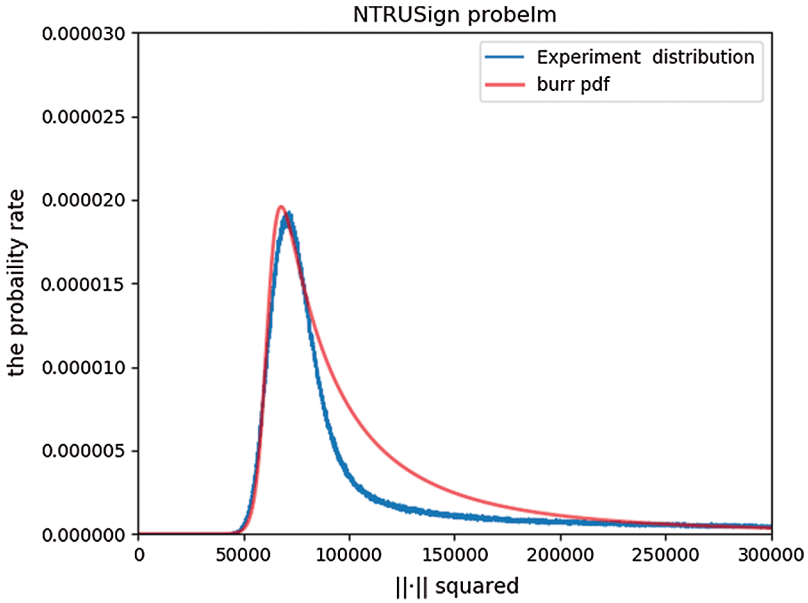

Figure 3: Comparison of burr distribution and experimental probability distribution

It can be seen that our predicted distribution is similar to the experimental result. When $||\cdot||$ is less than a certain value, their difference can be simply ignored.

To verify the accuracy of our experimental distribution, we signed 500,000 sets of data once again and counted the theoretical boundary of U according to Eq. (11) for $P = 1/2^n$. Meanwhile, the experimental results which are smaller than the boundary are also counted. As shown in Tab. 1.

Table 1: Experimental data related to signing success

P	Theoretically (U^2)	Times less than U^2
$1/2^6$	57969	4655
$1/2^7$	56083	1706
$1/2^8$	54326	637
$1/2^9$	52655	194
$1/2^{10}$	51051	63
$1/2^{11}$	49503	24
$1/2^{12}$	48005	5
$1/2^{13}$	46555	1

The experimental results demonstrated that the theoretical success probability is slightly greater than that of actual probability. However, since the conversion rules of the two are the same, it is feasible and secure when designing the data.

5 Conclusions and Open Problems

A novel PoW scheme combind with probabilistic signing was proposed in this paper. Our scheme can not only replace the hash puzzle in blockchain but also achieved fast block verification. However, there are still some problems to be addressed in the future.

Firstly, the probability distribution of successful singing is based on a set of commonly used parameters, without considering any possible disturbance (e.g., $S = 0$). Therefore, the relationship between the probability distribution and the secret key is not accurately obtained.

Secondly, this scheme has not implemented bathing signing to replace the PoW yet. With the advent quantum era, more and more probabilistic signing schemes will be based on lattices, so it is necessary to find a scheme that can perfectly fit parallel computing.

Thirdly, NTRUSign may expose the private lattice base [22] after multiple signings, which is considered the most significant flaw of it. Moreover, since the secret key of our scheme is only used to prove the workload, how to combine it with the function of transactions signing should be further studied.

Acknowledgement: We would like to express our very great appreciation to the reviewers for their detailed reviews and constructive comments. At the same time, we are also very grateful for the support of the fund project.

Funding Statement: This work was supported in part by the National Natural Science Foundation of P.R. China under Grants [61573076, 61703063, 61903053]; the Science and Technology Research Project of the Chongqing Municipal Education Commission of P.R. China under Grants [KJZD-K201800701, KJQN201900702, KJ1705121, KJ1705139]; the Program of Chongqing innovation and entrepreneurship for Returned Overseas Scholars of P.R. China under Grant cx2018110; and 2018 Team Building Project for Graduate Tutors in Chongqing under Grant JDDSTD2018001.

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

References

[1] Z. Deng, Y. Ren, Y. Liu, X. Yin, Z. Shen *et al.,* "Blockchain-based trusted electronic records preservation in cloud storage," *Computers Materials & Continua*, vol. 58, no. 1, pp. 135–151, 2019.

[2] G. Sun, S. Bin, M. Jiang, N. Cao, Z. Zheng *et al.,* "Research on public opinion propagation model in social network based on blockchain," *Computers, Materials & Continua*, vol. 60, no. 3, pp. 1015–1027, 2019.

[3] B. Bordel, R. Alcarria, D. Martín and Á. Sánchez-Picot, "Trust provision in the internet of things using transversal blockchain networks," *Intelligent Automation & Soft Computing*, vol. 25, no. 1, pp. 155–170, 2019.

[4] S. Ding, J. Cao, C. Li, K. Fan and H. Li, "A novel attribute-based access control scheme using blockchain for IoT," *IEEE Access*, vol. 7, pp. 38431–38441, 2019.

[5] J. Liu, X. Sun and K. Song, "A food traceability framework based on permissioned blockchain," *Journal of Cyber Security*, vol. 2, no. 2, pp. 107–113, 2020.

[6] S. Nakamoto, "A Peer-to-Peer electronic cash system," 2008. [Online]. Available at: https://bitcoin.org/bitcoin.pdf.

[7] X. Wang, D. Feng, X. Lai and H. Yu, "Collisions for hash functions MD4, MD5, HAVAL-128 and RIPEMD," *IACR Cryptol. ePrint Arch*, vol. 2004, pp. 1–199, 2004.

[8] X. Zhang, F. Wu, W. Yao and W. Wang, "Post-quantum blockchain over lattice," *Computers, Materials & Continua*, vol. 63, no. 2, pp. 845–859, 2020.

[9] Y. L. Gao, X. B. Chen, Y. L. Chen, Y. L. Sun, Y. Niu *et al.,* "A secure cryptocurrency scheme based on post-quantum blockchain," *IEEE Access*, vol. 6, pp. 27205–27213, 2018.

[10] T. M. Fernández-Caramès and P. Fraga-Lamas, "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks," *IEEE Access*, vol. 8, pp. 21091–21116, 2020.

[11] C. Li, Y. Xu, J. Tang and W. Liu, "Quantum blockchain: A decentralized, encrypted and distributed database based on quantum mechanics," *Journal of Quantum Computing*, vol. 1, no. 2, pp. 49–63, 2019.

[12] Z. J. Xiao and Y. Tang, "Useful workload proof consensus mechanism based on satisfiability problems," *Software Guide*, vol. 19, no. 8, pp. 72–75, 2020.

[13] Z. J. Liu, F. G. Zhang and H. B. Tian, "ECDLP-based proof of work scheme design," *Chinese Journal of Cryptography*, vol. 7, no. 4, pp. 511–521, 2020.

[14] H. S. Shahriar and Q. H. Mahmoud, "Improving transaction speed and scalability of blockchain systems via parallel proof of work," *Future Internet*, vol. 12, no. 8, pp. 125, 2020.

[15] R. Kailar, "Accountability in electronic commerce protocols," *IEEE Transactions on Software Engineering*, vol. 22, no. 5, pp. 313–318, 1996.

[16] J. Hoffstein, "NTRUSIGN: Digital signatures using the NTRU lattice," in *Cryptographers' Track at the RSA Conference*, Berlin, Heidelberg, Germany: Springer, pp. 122–140, 2003.

[17] F. A. Bhatti, G. G. Hamedani, M.Ç. Korkmaz and M. Ahmad, "On the modified burr XII-power distribution: Development, properties, characterizations and applications," *Pakistan Journal of Statistics and Operation Research*, vol. 2019, pp. 61–85, 2019.

[18] W. I. Burr, "Cumulative frequency functions," *Annals of Mathematical Statistics*, vol. 13, no. 2, pp. 215–232, 1942.

[19] O. Kehinde, A. Osebi and D. Ganiyu, "A new class of generalized burr III distribution for lifetime data," *International Journal of Statistical Distributions and Applications*, vol. 4, no. 1, pp. 6–21, 2018.

[20] R. C. Merkle, "A digital signature based on a conventional encryption function," in *Theory and Application of Cryptographic Techniques*. Berlin, Heidelberg, Germany: Springer, pp. 369–378, 1987.

[21] B. Bi, D. Huang, B. Mi and H. Pan, "Efficient LBS security-preserving based on NTRU oblivious transfer," *Wireless Personal Communications*, vol. 108, no. 4, pp. 2663–2674, 2019.

[22] A. A. Kamal and A. M. Youssef, "Fault analysis of the NTRUSign digital signature scheme," *Cryptography and Communications*, vol. 4, no. 2, pp. 131–144, 2012.