Secure and Efficient Signature Scheme Based on NTRU for Mobile Payment

Yunhao Xia¹, Lirong You², Zhe Sun² and Zhixin Sun¹

¹Nanjing University of Posts and Telecommunications, Key Lab of Broadband Wireless Communication and Sensor Network Technology, Nanjing, P. R. China
²Zhongtian Technology Corporation, Nantong, P. R. China

Email: 2015070108@njupt.edu.com, youlr@chinaztt.com, sunz@chinaztt.com, sunzx@njupt.edu.cn

Abstract. Mobile payment becomes more and more popular, however the traditional public-key encryption algorithm has higher requirements for hardware which is not suitable for mobile terminals of limited computing resources. In addition, these public-key encryption algorithms do not have the ability of anti-quantum computing. This paper researches public-key encryption algorithm NTRU for quantum computation through analyzing the influence of parameter q and k on the probability of generating reasonable signature value. Two methods are proposed to improve the probability of generating reasonable signature value. Firstly, increase the value of parameter q. Secondly, add the authentication condition that meet the reasonable signature requirements during the signature phase. Experimental results show that the proposed signature scheme can realize the zero leakage of the private key information of the signature value, and increase the probability of generating the reasonable signature value. It also improve rate of the signature, and avoid the invalid signature propagation in the network, but the scheme for parameter selection has certain restrictions.

1. Introduction

With the widespread use of third-party mobile payment, mobile payment has become a serious area of cyber-crime [1]. During the process of mobile payment, the user needs to send the relevant information about the payment, including the order information, payment information, user or merchant information and so on. These data are related to the security of users' funds, which will have serious consequences if they are exploited by lawbreakers. On the other hand, with the advent of the shor quantum algorithm [2] and the rapid development of quantum computers, the threat of RSA and ECC is increasing. With the improvement of computing performance, the low-security public-key encryption algorithm applied to mobile terminals is no longer safe. The security of third-party mobile payment becomes an important obstacle to mobile payment development and popularization [3].

In the face of the threat of quantum computing to the traditional encryption system, this paper researches public-key encryption algorithm NTRU for quantum computation, which is applicable to the terminal of finite computing resources. In order to satisfy the non-repudiation of information, the main method is digital signature. The classic digital signature schemes are RSA [4] and ECC [5]. These two algorithms have the properties of the public key that can be decrypted correctly using the private key, thus can be used directly as the signature algorithm. However, the efficiency of RSA signature algorithm is very low, and the efficiency of ECC signature algorithm is much slower than that of NTRU. The encryption system NTRU [6] is based on the polynomial ring, and it avoids the
modular arithmetic of the big integer power, which only involves the addition and subtraction of polynomials and multiplication. The efficiency of encryption algorithm NTRU is better than RSA and ECC, and encryption algorithm NTRU is considered to be the most future public-key encryption algorithm. However, the encryption algorithm NTRU encrypt using private key and this will leak the information of private key. Therefore, this paper redesigns the signature algorithm based on NTRU.

The rest of paper is organized as follows: Section 2 introduces some related work to our research. In section 3, we propose an improved signature algorithm based on NTRU for the defects, and analyze the security and operation performance. Conclude our paper in the section 4.

2. Related Works

Ajtai provided a ground-breaking conclusion [7]: the security of any cryptographic system based on some of the lattice problems is equivalent to the most difficult password system, and presented the AD encryption based on the most difficult case of u-SVP (unique Shortest Vector Problem)[8]. The scheme can be proved to be safe, but the system is inefficient and cannot meet the practical requirements. Park in [9] proposed a NFC mobile payment system based on zero-knowledge digital signature of NTRU, instead of using users’ private information directly, thus ensuring the security of users’ privacy. One innovation of the scheme was the use of NTRU encryption technology, achieving user authentication. However, the shortcomings of proposed method were obvious: the digital signature technology of NTRU was still immature. The NTRU encryption algorithm was applied to PKI in [10], which was found to have a large advantage in speed and the CA certificate was generated faster compared with PKI using RSA.

Hoffstein, Pipher, and Silverman in [11] presented NSS signature scheme based on the difficulty of finding CVP of recent vector problems in the grid. The scheme adopted the structure of NTRU algorithm, so the speed of encryption and decryption was relatively fast. Later, Silverman and Mironov in [12] presented the attack on the signature restoring private key. Subsequently, Hoffstein, Pipher and Silverman in [13] proposed the strengthening version of NSS for the attack of Silverman. However, Gentry and Szydlo researched the characteristics of R-NSS as a single secret key, and in [14] presented a large number of attacks on the signature restoring private key by combining the maximal common factor method. And then, Hoffstein in [15] proposed the NTRUSign algorithm, which has a large structural change compared with NSS and R-NSS algorithm, and its secret key is not the characteristic of a single secret key, using a linear combination of secret keys. However, Nguyen in [16] recovered the private key by a large number of valid signature values according to the characteristics of the uniform distribution of NTRUSign secret-key coefficient. Hu in [17] proposed an improved signature scheme based on R-NSS according to the problem of leaking private key of R-NSS and NTRUSign. Li in [18] proposed a novel identity based undeniable signature scheme, and the paper analyzed the proposed scheme was unfalsified and anonymous under stochastic prediction mode.

Melchor in [19] proposed a method to hide the leaking NTRUSign signature value through gaussian noise. At the same time, a strong parameter setting scheme was proposed according to the latest attack on NTRUSign to realize zero knowledge of signature value and anti-counterfeiting attack. Zhang in [20] presented a new type of NTRU signature algorithm based on CVP problem, and the efficiency was about 1/7 faster than the signature algorithm designed by Hu [17]. However, the proposed method did not disturb the private key directly by signing the private key, so the algorithm still has the problem of leaking private key. Hoffstein J, Pipher J, Schanck J in [21] proposed a new signature scheme based on NTRU, called NTRUMLS. The results showed that the security and efficiency of the scheme were relatively high, but the probability of generating reasonable signature was lower and cannot meet the requirement of mobile payment signature. At the same time Xie in [22] put forward a kind of identity signature scheme based on NTRU lattice, and the security of the scheme was based on \gamma.SVP difficult problems. An obvious advantage of the proposed method was the efficiency is higher than the same digital signature scheme based on grid.

As a result, the researches on the signature scheme of NTRU were mainly the improvement of NSS, R-NSS and NTRUSign. On one hand, proposed solutions for the classic attack schemes, and on the other, proposed new signature schemes based on NTRU. However, few of the above were suitable for
mobile payment. Firstly, NSS, R-NSS and NTRUSign exist the problem of leaking private key. Besides, the probability of reasonable signature value of signature scheme based on NTRU is less than 1, and even some valid probability of signature scheme cannot meet the practical demand. Therefore, it was not suitable for application in a large number of users in mobile payment.

3. Secure and Efficient Signature Scheme For Mobile Payment

Through the research of the proposed signature scheme NTRUMLS [21] by Hoffstein, the analysis showed that the proposed method can realize zero knowledge of signature value. But the proposed scheme had the problem that the effective of signature value was low. For a lot of users of mobile payments, a large number of invalid signature value would greatly aggravate network congestion and the burden of service systems. This paper proposes two ways to improve the signature probability of NTRUMLS by analyzing the influence factors of the probability of reasonable signature value of NTRUMLS. Firstly, select reasonable parameter to narrow down the space to find a valid signature, and ensure that the signature value has a larger probability in the L∩R range. Secondly, during the process of signature, filtrate the conditions that satisfy a valid signature value, and we can ensure that the generated signature values are reasonable.

3.1. Increasing the probability of reasonable signature

According to the related parameters recommended by NTRUMLS [21], the probability of reasonable signature value generated by NTRUMLS is shown in table 3.1.

| NTRUMLS parameters(N, p, q, B_s, B_t) | Probability of reasonability signature |
|--------------------------------------|---------------------------------------|
| (401,3,2^18,240,80)                  | 38%                                   |
| (439,3,2^19,264,88)                  | 55%                                   |
| (593,3,2^19,300,100)                 | 41%                                   |
| (743,3,2^20,336,112)                 | 53%                                   |

Table 3.2 The Probability Generated By Another Parameters

| NTRUMLS parameters(N, p, q, B_s, B_t) | Probability of reasonability signature |
|--------------------------------------|---------------------------------------|
| (443,3,2^16,138,46)                  | 8%                                    |
| (563,3,2^16,174,58)                  | 2%                                    |
| (743,3,2^17,186,62)                  | 6%                                    |
| (907,3,2^17,225,75)                  | 2%                                    |

In regard to the probability of reasonable signature value generated by NTRUMLS, this paper can be inspired by another parameters.

Compared with table 3.1 and table 3.2, we can find that the change of parameters has a great influence on the probability of reasonable signature value generated by NTRUMLS. Therefore, this paper can be inspired by setting relevant parameters to improve the probability of reasonable signature value generated by NTRUMLS.

Firstly, this paper studies the correlation factors of the probability of reasonable signature value generated by NTRUMLS. For the convenience of research, this paper set \( B = \lfloor p^2 N / 4 \rfloor \) and \( B = B_s = B_t \). In this case, generating a reasonable signature value depends on whether the signature value is in the multidimensional polyhedral formed by lattice \( L(A - B_s, \frac{q}{2} - B_t) \). For valid signature value, the limit of its parameter is less than \( \frac{p}{2} - B \). Therefore, during the process of
setting parameters, q must be much larger than B, or the probability of generating a reasonable signature will be small. Consider the general form of signature value:

\[ (s, t) = (s_0, t_0) + (af + ag) \]  

(1)

In the formula (1) above, \( s_0, t_0 \in R(\frac{q}{2}) \), \( af \in R(p^2 N \sqrt{2}) \), \( ag \in R(p^2 N \sqrt{2}) \). Therefore:

\[ \|s, t\| \leq \frac{q}{2} + B \]  

(2)

In the formula (2) above, the coefficients of s and t are less than \( \frac{q}{2} - B \), and then we can obtain the probability of generating a reasonable signature value:

\[ P((s,t) is valid) = \left\{ \begin{array}{ll} \frac{q - B}{2} & \\
\frac{q + B}{2} & \end{array} \right\}^{2^N} \]  

(3)

Then make:

\[ q \approx \frac{kp^2 N^2}{4} \approx kNB \]  

(4)

We can obtain:

\[ P((s,t) is valid) = \left\{ \begin{array}{ll} \frac{q - B}{2} & \\
\frac{q + B}{2} & \end{array} \right\}^{2^N} \approx e^{-\kappa k} \]  

(5)

In the formula (5) above k is a small constant. From the above analysis, it can be seen that the probability of generating a reasonable signature is about \( e^{-\kappa k} \). And it is associated with constant k.

\[ k \approx \frac{q}{NB} \]  

(6)

Therefore, the improved method can be realized by raising constants k to improve the accuracy of generating a reasonable signature. The influence of constant k on the probability of generating a reasonable signature is shown in figure 3.1.

According to figure 3.1, constant \( k \approx 12 \) when the probability of generating a reasonable signature is about 50%. If we raise the constant k to 25, the probability of generating a reasonable signature will be greater than 70%. So it will be a feasible scheme by increasing the constant k. In the formula \( k \approx \frac{q}{NB} \), parameter N responds to the security of NTRUMLS, and therefore N cannot be changed. Parameters \( B_r, B_f \) are small adjustment of performance and safety, and smaller \( B_r, B_f \) can improve performance. However, it brings difficult to find suitable signature value. Therefore, according to the above analysis, it is possible to appropriately improve the value of parameter q. We
can know the relation between parameter $q$ and the probability of generating a reasonable signature according to formula (6) $k \approx \frac{q}{NB}$.

\[
\begin{align*}
\text{Table 3.3 The Probability Generated By Changed Parameter } Q \\
\text{NTRUMLS parameters (N, p, q, B_s, B_i) } & \quad \text{Probability of reasonability signature} \\
(401,3,2^{19},240,80) & \quad 62\% \\
(439,3,2^{20},264,88) & \quad 74\% \\
(593,3,2^{20},300,100) & \quad 64\% \\
(743,3,2^{21},336,112) & \quad 73\% 
\end{align*}
\]

Comparing table 3.1 with table 3.3, it can be seen that the probability of generating a reasonable signature value is obviously improved through double the value of parameter $q$. However, if you want to make the reasonable signature value close to 100%, the value of parameter $q$ will become very large, and the following will discuss the effect of parameter $q$ on the performance of NTRUMLS.
key structure of NTRUMLS is similar to the NTRU, so parameter q has little impact on the rate of NTRUMLS through the analysis above. Key sizes of NTRUMLS and cipher text size is related to parameters N, q has no effect on it. Therefore, in order to improve the probability of generating a reasonable signature value, the solution given in this paper is to improve the parameter q appropriately. Table 3.3 is the revised parameter q given in this paper.  

3.2. Adding Authentication Conditions for Signature

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

According to literature [20], if \( (s, t) \neq (s', t') \mod p \), then the probability of generating a reasonable signature value is 0. As a result, the first condition that determines whether the signature value is legal is \( (s, t) = (s', t') \mod p \cdot \). On the basis of improving parameter q of NTRUMLS, in this paper authentication scheme of the selected signature value is supplemented by the condition \( (s, t) = (s', t') \mod p \cdot \) to propose our signature scheme. For the reasonable signature value of NTRUMLS, the following conditions must be satisfied:

\[
\|s, t\| \leq \frac{q}{2} + B
\]

\[
(s, t) = (s', t') \mod p
\]

It is necessary to add a condition \( (s, t) = (s', t') \mod p \cdot \) to determine whether the value of the selected signature value is a reasonable signature value. This can prevent the invalid signature value from spreading in the network, resulting in the waste of network resources. The specific changes are as follows:

Signature:

Describe the proposed signature algorithm here.

Input: \((f, g, h, u)\) \(u\) is about the plaintext polynomials that will be signed and the coefficients of that polynomial \(\in \{-1,0,1\}\).

Output: \((s, t, u)\)

1: \((s', t') \leftarrow \text{Hash}(h, u)\)

2: Repeat

3: Randomly generate \(r \in R\left(\left\lfloor \frac{q}{2p} + \frac{1}{2}\right\rfloor\right)\), \(\lfloor \cdot \rfloor\) is getting the integers down

4: \(s_0 \leftarrow s' + pr\)

5: \(t_0 \leftarrow h \otimes s_0 \mod q\) and satisfy \(t_0 \in R\left(\frac{q}{2}\right)\)

6: \(a \leftarrow g^{-1} \otimes (t' - t_0 \mod p)\)

7: \((s, t) \leftarrow (s_0, t_0) + (a \otimes f, a \otimes g)\) determine whether \(|a \otimes f| \leq B_f \land |a \otimes g| \leq B_g\) \(|s|, |t| \leq \frac{q}{2} - B_s (s, t) = (s', t') \mod p\)

Output: \((s, t, u)\), otherwise repeat.

Authentication:
Describe the proposed authentication algorithm here.

Input: \((s, t, u, h)\)

1: \((s_p, t_p) \leftarrow \text{Hash}(h, u)\)
2: If \(t \neq h \otimes s \mod q\), output illegal and end, otherwise continue
3: If \(\|s\| > \frac{q}{2} - B_s\) or \(\|t\| > \frac{q}{2} - B_t\), output illegal and end, otherwise continue
4: If \((s, t) \neq (s_p, t_p) \mod p\) output illegal and end, otherwise output legal

3.3. Performance Analysis of Proposed Signature Scheme

Safety performance:

In this paper the proposed signature scheme is an improvement of NTRUMLS, and there is no significant change in the algorithm structure, so its security depends on NTRUMLS. According to analysis of the literature [20], this signature can guarantee the security of private key information. Therefore, the security of signature algorithm is fully guaranteed.

Efficiency performance:

In this paper, the proposed signature scheme is compared with that of NTRUMLS: firstly, the probability of parameter \(q\) is improved greatly, so that the probability of reasonable signature is improved. Second, the authentication conditions are added to avoid the illegal signature value spreading through the network. Table 3.4 reflects experiment contrast of the proposed signature scheme is given in this paper and NTRUMLS. Test environment is: the system is android 5.0, CPU is Intel Z3560 of dominant frequency of 1.8 GHz, memory is 4g. The result is the average of the data of 100.

| NTRUMLS \((N, p, q, B_s, B_t)\) | Secure level (bits) | Key generation time (ms) | Signature Time (ms) | Authenticity Time (ms) | probability of reasonable signature | Key size (bytes) |
|-------------------------------|---------------------|--------------------------|---------------------|-----------------------|----------------------------------|-----------------|
| \((401,3,2^18,240,80)\)        | 112                 | 23.431                   | 5.768               | 1.001                 | 38%                              | 853             |
| \((439,3,2^19,264,88)\)        | 128                 | 29.28                    | 4.456               | 1.113                 | 55%                              | 998             |
| \((593,3,2^19,300,100)\)       | 192                 | 52.873                   | 10.567              | 1.897                 | 41%                              | 1335            |
| \((743,3,2^20,336,112)\)       | 256                 | 79.653                   | 11.912              | 2.312                 | 53%                              | 1765            |
| \((401,3,2^19,240,80)\)        | 112                 | 25.727                   | 3.403               | 1.012                 | 62%                              | 853             |
| \((439,3,2^20,264,88)\)        | 128                 | 32.149                   | 2.629               | 1.125                 | 74%                              | 988             |
| \((593,3,2^20,300,100)\)       | 192                 | 58.054                   | 6.235               | 1.917                 | 64%                              | 1335            |
| \((743,3,2^21,336,112)\)       | 256                 | 87.458                   | 7.029               | 2.337                 | 73%                              | 1765            |

According to table 3.4, the key generation time and authentication time of the proposed signature scheme are slightly higher than NTRUMLS in the key generation phase. This is because the parameter \(q\) is twice larger, which slightly increases the calculation of the key generation, but this is small. The worst time complexity of key generation of the proposed signature scheme in this paper is \(O(N^3)\). As can be seen from the above data, the parameter \(N\) has great influence on proposed signature scheme, and \(q\) has little influence on its speed. The result also verifies the discussion of the key generation and decryption speed of the parameter \(q\) for NTRU.

In theory, the parameter \(q\) becomes larger and the signature time will become longer in the signature phase. But there will be a significant reduction in the time of generating signature. This is because the signature phase is a process of finding a reasonable signature, and if the selected signature value does not meet the criteria, the signature process will be repeated until it is found to satisfy the given condition. In this paper, the parameter \(q\) of the proposed signature is larger than that of
NTRUMLS, and it will greatly increase the probability of generating a reasonable signature value. Then each time the signature process filtering the reasonable signature, the math expectation is smaller, which significantly reduces the signature time. In the meantime, to avoid the illegal signature value which meet the condition $\|s, t\| \leq \frac{q}{2} + B$ and not meet the condition $(s, t) = (s, t) (\mod p)$ to be sent to the validation party, in the proposed signature scheme the authentication conditions are supplemented during the signature phase, in order to ensure that all signature values are valid. The verification condition is the mode of the signature value, so the calculation is very small, and the influence of the signature time is very small, so the signature time can be shortened greatly.

At the same time, under the condition of parameter q of the proposed signature scheme in this paper change for 2 times, the key size and signature size have no change. So the proposed scheme is secure and efficient which can raise the speed and probability of generating reasonable signature value.

4. Conclusion
This paper researches the non-repudiation of data in mobile payment process, considering traditional RSA, ECC and other signature schemes are less efficient and do not have the ability of anti-quantum attack, and we introduce the signature scheme based on NTRU in this paper. However, several classical NTRU signature algorithms, include NSS, R-NSS, NTRUSign, exist the problem of leaking private key information and the classical NTRU signature algorithms NTRUMLS, which has unsatisfactory probability of generating a reasonable signature value. On the basis of these classical signature scheme, this paper proposed an efficient and secure signature scheme which is suitable for mobile payment by increasing the value of parameter q and adding the authentication condition that meet the reasonable signature requirements during the signature phase. Experimental results show that the proposed signature scheme can realize the zero leakage of the private key information of the signature value, and increase the probability of generating the reasonable signature value. It also improve rate of the signature, and avoid the invalid signature propagation in the network, but the scheme for parameter selection has certain restrictions.

5. Acknowledgment
This research is supported by the National Natural Science Foundation of China (NO.61672299, NO61373135). The authors thank the sponsors for their support and the reviewers for helpful comments.

6. References
[1] Emmeline Taylor. “Mobile payment technologies in retail: a review of potential benefits and risks,” International Journal of Retails & Distribution Management, vol. 44, 2016, pp. 159-177, doi:10.1108/IJRDM-05-2015-0065.
[2] Shor P W. “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,” Society for Industrial and Applied Mathematics, vol. 41, 1999, pp. 303-332, doi:10.1137/S0036144598347011.
[3] Yong Wang, Christen Hahn, Kruttika Sutrave. “Mobile payment security, threats, and challenges,” Mobile and Secure Services (MobiSecServ), 2016 Second International Conference on. 26-27 Feb, 2016, pp. 1-5, doi:10.1109/MOBISECSERV.2016.7440226.
[4] B R Ambedkar, Ashwani Gupta and S S Bedi. “Confidentiality of Group Digital Signature Using Proposed Public Keys Encryption Algorithm,” International Journal of Engineering Science and Computing, vol. 6, 2016, pp. 2304-2307, doi:10.4010/2016.550.
[5] Deepti Jyotiyan, Varun P Saxena. “Fault attack for scalar multiplication over finite field (E(Fq)) on Elliptic Curve Digital Signature algorithm,” Recent Advances and Innovations in Engineering (ICRAIE), 2016 International Conference on, 23-25 Dec, 2016, doi:10.1109/ICRAIE.2016.7939539.
[6] Sonika Singh, Sahadeo Padhye. “Generalisations of NTRU cryptosystem,” Security and Communication Networks, vol. 9, 2016, pp. 6315-6334, doi:10.1002/sec.1693.
[7] Ajtai M. “Generating hard instances of lattice problems,” Proceedings of the 28th Annual ACM Symposium on Theory of Computing, 1996, pp. 99-108, doi:10.1145/237814.237838.

[8] Ajtai M, Dwork C. “A public-key cryptosystem with worst-case/average-case equivalence,” Proceedings of the 29th Annual ACM Symposium on Theory of Computing, 1997, pp. 284-293, doi:10.1145/258533.258604.

[9] Park S W, Lee I Y. “Anonymous authentication scheme based on NTRU for the protection of payment information in NFC mobile environment,” Journal of Information Processing Systems, vol. 9, 2013, pp. 461-476, doi:10.3745/JIPS.2013.9.3.461.

[10] Mironov I. “A note on cryptanalysis of the preliminary version of the NTRU Signature scheme,” IACR Cryptology ePrint Archive, vol. 5, 2001, pp. 1-6.

[11] Hoffstein J, Silverman J H. “NSS: An NTRU lattice-based signature scheme,” International Conference on the Theory and Application of Cryptographic Techniques, 2001, pp. 211-228.

[12] Mironov I. “A note on cryptanalysis of the preliminary version of the NTRU Signature scheme,” IACR Cryptology ePrint Archive, vol. 5, 2001, pp. 1-6.

[13] Hoffstein J, Pipher J, Silverman J H. “Enhanced encoding and verification methods for the NTRU signature scheme,” Previously posted on http://www.ntru.com/technology/tech.technical.html, 2001.

[14] Gertry C, Szydlo M. “Cryptanalysis of the revised NTRU signature scheme,” Advances in Cryptology-Eurocrypt 2002, Berlin: Springer-Verlag, 2002, pp. 299-320.

[15] Hoffstein J, Howgrave-Graham N, Pipher J, et al. “NTRUSIGN: Digital signatures using the NTRU lattice,” Topics in cryptology—CT-RSA 2003, Springer Berlin Heidelberg, 2003, pp. 122-140.

[16] Nguyen P Q, Regev O. “Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures,” Journal of Cryptology, vol.22, April 2009, pp. 139-160, doi:10.1007/s00145-008-9031-0

[17] Yupu Hu. “A Novel NTRU-Class Digital Signature Scheme,” CHINESE JOURNAL OF COMPUTERS, vol.31, Sep. 2008, pp. 1661-1666.

[18] Li S, Wang C, Xu M, et al. “A novel identity based undeniable signature scheme,” Conference Anthology, IEEE, 1-8 Jan 2013, pp.1-5, doi:10.1109/ANTHOLOGY.2013.6784885.

[19] Melchor C A, Boyen X, Deneuville J C, et al. “Sealing the leak on classical NTRU signatures,” International Workshop on Post-Quantum Cryptography, 2014, pp. 1-21, doi: 10.1007/978-3-319-11659-4_1

[20] Zhang Juanmei, Cao Jie, Liu Nianyi, Yang Yatao, Li Zichen. “A New Design of Digital Signature Scheme Based on NTRU,” JOURNAL OF SICHUAN UNIVERSITY(ENGINEERING SCIENCE EDITION), vol. 47, 2015, pp. 49-53.

[21] Hoffstein J, Pipher J, Schanck J M, et al. “Transcript secure signatures based on modular lattices,” International Workshop on Post-Quantum Cryptography, 2014, pp. 142-159, doi:10.1007/978-3-319-11659-4_9

[22] XIE J, HU Y, GAO J, et al. “Efficient identity-based signature over NTRU lattice,” Frontiers of Information Technology & Electronic Engineering, vol. 17, 2015, pp. 135-142, doi:10.1631/FITEE.1500197.