2010 International Conference on E-Business and E-Government

Changeable Threshold Signature Scheme Based on Lattice Theory

Tao Feng
School of Computer and Communication
Lanzhou University of Technology
Lan'zhou, China
fengt@lut.cn

Yongguo Gao
School of Computer and Communication
Lanzhou University of Technologle
Lan'zhou, China
gaoyg@lut.cn

Jianfeng Ma
Ministry of Education Key Laboratory of Information Security
Xidian University
Xi'an, China
jfma@mail.xidian.edu.cn

Abstract—**The current changeable threshold signature schemes are generally based on RSA or ECC algorithm. They often have shortcomings of the large amount of calculation, need the dealer to participate in when adjusting the threshold etc. This paper introduced the related concepts and theories of lattice, proposed a novel changeable threshold signature scheme and analyzed the essential security , it based on the changeable threshold Shamir secret sharing scheme and NTRUSign signature algorithm. The scheme has the following properties: It is mainly based on polynomial multiplication and integer coefficient modular arithmetic and needn't introduce exponential operation; It needn't redistribute the subsecret and modify the group public key when changing threshold; The scheme guarantees threshold security, robustness and unforgeability.**

Keywords- *threshold signature; lattice; secret sharing; NTRUSign*

I. INTRODUCTION

The (t,n) threshold signature is a scheme which private key is divided into n shares, in such a way that any t players can generate partial signature to sign message on behalf of group, but any set of less than t participants cannot learn anything about the signature. Since Desmedt and Frankel firstly proposed RSA-based threshold signature scheme [1], threshold signature research field have made a large number of achievements. With the further research in recent years, many researchers paid more attention to the safety, efficiency and practicality of threshold signature and proposed a number of extension application schemes, such as threshold proxy signature [2], identity-based threshold signature [3], etc.

Lee presented a changeable threshold signature scheme with multi-strategy in 2001[4], which can adjust the threshold flexibly according to the properties of the document, and later researchers proposed more changeable threshold signature schemes [5, 6]. However, these schemes generally based on RSA and ECC public key cryptosystem and consequently need large amount of calculation during signature generation and certification process. When changing the threshold there needs to restart the entire system and more communication cost between the dealer and participants, or needs to change the original member's private key and group's public key. These deficiencies of threshold signature lead to its application scope are limited.

Lattice is a typical linear algebra structure. Using NP-hard problem based on lattice to construct a new cryptosystem is widely concerned by the scholars in the field of cryptography. The public key cryptosystems which based on lattice NP-hard problem including AD (Ajtai-Dwork), GGH (Goldreich, Goldwasser, Halevi) and NTRU (Number Theory Research Unit), etc. But AD and GGH cryptosystems have been cracked due to some defects. Nevertheless, NTRU is a promising public key cryptosystem which security is based on lattice Approximating Closest Vector Problem (Appr-CVP). At present there is no known method which can break the cryptosystem, although the cryptography academic circles proposed a variety of attack methods against the NTRU. Compared with the traditional public key cryptosystem such as RSA and ECC, NTRU cryptosystem can be run more efficiently [7]. In order to use the fine properties of NTRU algorithm in the field of digital signature, a variety of NTRU-class signature algorithms such as NTRUSign etc has been proposed [8-11]. Ron Steinfeld et al proposed two kinds of lattice-based changeable-threshold secret sharing scheme [12,13] , they respectively based on standard Shamir threshold secret sharing scheme and the Chinese remainder theorem.

In this paper we present a lattice-based changeable threshold signature scheme which based on changeable threshold Shamir secret sharing scheme and NTRUSign algorithm. It can satisfies the properties of the threshold signature, can adjust the threshold without participation of the dealer and reduce the communication and implementation cost. It also needn't to redistribute the subsecrets and modify the group public key when changing the threshold. The scheme has advantages of efficiency and practicality of NTRU cryptosystem and without compromising the security.

II. PRELIMINARIES

A. Standard NTRU Lattice

1) Standard NTRU Lattice and Vector Norm

Definition 1: NTRU lattice constructed in polynomials ring $(R,+,\otimes)$, $R=Z_q[x]/(x^N-1)$. Polynomial $h(X)\in R$ can

The National High-Tech Research and Development Plan of China (2007AA01Z429); The National Natural Science Foundation of China (60972078); Universities Basic Scientific Research Operation Cost of Gansu Province (2009); The Natural Science Foundation of Gansu Province of China(2007GS04823); The Ph.D. Programs Foundation of Lanzhou University of Technology (BS14200901); Funds of Key Lab of Fujian Province University Network Security and Cryptology(09A006).

978-0-7695-3997-3/10 $26.00 © 2010 IEEE
DOI 10.1109/ICEE.2010.335

IEEE computer society

be denoted as $h(X)$=h_0+h_1X+h_2X^2+⋯+$h_{N\text{-}1}$X$^{N\text{-}1} \in R$ or $h(X) = (h_0, h_1, \cdots, h_{N\text{-}1})$. The lattice L_h associated with $h(X)$ is a vector set of $(u,v) \in R \times R \cong Z^{2N}$ to satisfy the relationship of convolution modulo q $v(X) = h(X) * u(X) (\bmod\ q)$. Where "*" represent convolution multiplication of ring $R = \mathrm{Z}_q[x]/(x^N - 1)$. Convolution modulo of polynomials $h(X)$ and $u(X)$ is defined as: $v(X) = h(X) * u(X)(\bmod\ q) = v_0 + v_1 \mathrm{X} + v_2 \mathrm{X}^2 + \cdots + v_{N\text{-}1} \mathrm{X}^{N\text{-}1}$, $v_k = \sum_{i+j=k(\bmod\ N)} h_i \cdot u_j (\bmod q)$.

Definition 2: $p-$ norm of n -dimensional vector v is defined as $\| v \|_p = (\sum_{i=1}^{n} |v_i|^p)^{1/p}, p \geq 1$ .When $p = 2$, $\|v\|_2$ also known as Euclidean norm(abbreviate for $\|v\|$).Then a natural measure of size in R is the centered Euclidean norm: $\| v \| = (\sum_{i=0}^{n-1} |v_i|^2 - (1/n)(\sum_{i=0}^{n-1} |v_i|)^2)^{1/2}$, the component-wise Euclidean norm is: $\|(u,v)\|^2 = \|u\|^2 + \|v\|^2$.

2) *NP-hard problems of Lattice theory*

Approximate Closest Vector Problem (Appr-CVP): given a lattice $B \in \mathbb{Z}^{m \times n}$ and a target vector $t \in \mathbb{Z}^m$, find a vector $B_x (x \in \mathbb{Z}^n \setminus \{0\})$ in the approximate closest distance to target vector t , such that for all $B_y \in \mathbb{Z}^n \setminus \{0\}$, $\|B_x - t\| \leq \gamma \cdot \|B_y - t\|$, Where γ is an approximation factor related to the lattice dimension of N [14].

At present there is no known effective algorithm to against Appr-CVP, but when the lattice dimension is lower (less than 300), the problem can be an effective approximate by use of lattice reduction algorithms in polynomial running time. A.K.Lenstra et al presented the solution (LLL algorithm) about Appr-SVP with polynomial running time where approximation factor $\gamma = n^{1/2} 2^{n/2}$ [15]. Babai has shown how to convert the LLL algorithm into a CVP approximation algorithm with polynomial running time which achieves approximation factor $\gamma = n^{1/2} 2^{n/2}$ [16].

B. *Changeable threshold Shamir Secret-Sharing scheme*

The (t,n) threshold Secret Sharing divided secret k into a series of interrelated shares and distribute to group members $P = \{P_1, P_2, \ldots, P_n\}$, each of whom holds a shadow of secret k . In practice, the threshold to recover the secret could be changed according to the property of secret. In [12] Ron Steinfeld et al proposed the detailed contents of lattice-based threshold changeability for standard Shamir secret-sharing scheme.

For a finite set S , denote by $\#S$ the size of S .For any set S and integer n , denote by S^n the set of all n -tuples of elements from S and by $D(S^n)$ the set of all n -tuples of distinct elements from S . For integer n , denote by $[n]$ the set $\{1,2,\ldots,n\}$. For integers a and p , denote a mod p by $\lfloor a \rfloor_p$ .For a ring R , denote the set of all polynomials of degree at most t with coefficients in the ring R by $R[x;t]$.

The concrete contents of standard Shamir (t,n) threshold secret sharing scheme $ShaTSS = (GC, D, C)$ and the algorithm $ShaTSS'$ which can change the threshold (t,n) into (t',n) we used in this paper can see [12].

III. THE CHANGEABLE THRESHOLD SIGNATURE SCHEME

A. *Initialization*

Without loss of generality, assume that there were n members $P = \{P_1, P_2, \ldots, P_n\}$, denote an authorized subset $L = \{P_1, P_2, \ldots, P_l\} (t \leq l \leq n)$.

This scheme requires a trusted center (TC):

(1)Build NTRUSign signature algorithm, given public parameters set $(N, q, d_f, d_g, n, T, \mathcal{N})$, for integer N, q, d_f, d_g, n , denote N lattice dimension, $\mathcal{N}$ a norm bound. String T represents "standard" or "transpose" is one of the operating modes of NTRUSign algorithm.

(2)TC generates a Public lattice basis B_0 and n Private lattice basis $B_i (1 \leq i \leq n)$.

Set $i = n$, while $i \geq 0$:

ⅰ. Input parameters $(N, q, d_f, d_g, n, T, \mathcal{N})$ .TC randomly choose $f, g \in R$ ($\|f\| = \|g\| = \mathrm{O}(\sqrt{N})$) to be binary with d_f , d_g ones respectively, the remaining coefficients are zeros. Compute polynomials $F, G \in R$ such that $f{*}G\text{-}g{*}F{=}q$ ($\|F\| = \sqrt{N/12\|f\|}$), f, g, F, G must be protected in secret.

ⅱ. If T = "standard", set $f_i = f, f_i' = F$; if T = "transpose", set $f_i = f, f_i' = g$, $h_i = f_i^{-1} \otimes f_i' (\bmod \mathrm{q})$, $i = i - 1$.

(3)Output lattice basis parameters $\{f_i, f_i', h_i\}$, $i = 0, \cdots, n$. For each group member $p_i (i = 1, 2, \cdots, n)$, where (f_i, f_i') is private key, h_i is public key.

(4) TC encode $\{f_i, f_i', h_i\}$ as a bit string k and share secret k using standard Shamir threshold secret sharing scheme, build the polynomial $a(x) = k + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1} \in \mathbb{Z}_p[x : t-1]$, where $a(0) = k$, the i th share is $\sigma_i = \lfloor a(\alpha_i) \rfloor_p$,for $i = 1, 2, \ldots, n$.

(5) TC send private lattice basis parameters $\{f_i, f_i', h_i\}$ and share $\sigma_i = \lfloor a(\alpha_i) \rfloor_p$ through secret communication channel to

the participants p_i respectively, and broadcast public key $h = h_0 \equiv f_0^{-1} \otimes f_0'$ (mod q) of public lattice basis B_0.

B. Partial Signature Generation

Suppose t participants in authorized subset L to sign the document D on behalf of group. Firstly, participants use their private lattice basis parameters $\{f_i, f_i', h_i\}(1 \le i \le t)$ generate partial signature in turn.

Step1: The first participant p_1 input digital document D and public key h_0 of B_0, set $r = 0$;

Step2: Set $s_0 = 0$ .Encode r as a bit string. Set $m_0 = H(D \| r)$, where " $\|$ "denotes concatenation. Set $m = m_0$.

Step3 : Participant p_1 generate partial signature s_1 use his private key (f_1, f_1') :

Define two symbols: for any $a \in \mathbb{Q}$, let $\ulcorner a \lrcorner$ denote the integer closest to a , and define $\{a\} = a - \ulcorner a \lrcorner$ .If A is a polynomial with rational coefficients, let $\ulcorner \mathrm{A} \lrcorner$ and $\{\mathrm{A}\}$ be A with the indicated operation applied to each coefficient. Set

$$\mathrm{x} = \ulcorner -(1/q)m \otimes f_1' \lrcorner \tag{1}$$

$$\mathrm{y} = \ulcorner -(1/q)m \otimes f_1 \lrcorner \tag{2}$$

$$\mathrm{s}_1 = \mathrm{x} \otimes f_1 + \mathrm{y} \otimes f_1' \tag{3}$$

$$m_1 = s_1 \otimes (h_1 - h_0) \ mod \ \mathrm{q} \tag{4}$$

$$s_1 = s_1 + s_0 \tag{5}$$

Participant p_1 output partial signature (h_1, m_1, s_1) , and send it to the second participant p_2 in the authorized subset.

Step4: The second participant p_2 with the same algorithm, input triplet (h_1, m_1, s_1) and his private key $\{f_2, f_2', h_2\}$ generate partial signature (h_2, m_2, s_2) , and send to the third participant p_3 .

……

Step t : The participant p_t output his partial signature (h_t, m_t, s_t) .

C. Threshold Signature Generation

The last participant p_t of authorized subset send his partial signature (h_t, m_t, s_t) to the signature generator who is a designated combiner (DC), DC is responsible for generating threshold signature.

DC collect the subshare σ_i holding by participants in authorized subset L where threshold is t and use standard Shamir (t,n) threshold secret sharing scheme combine the secret k and convert it into (f_0, f_0') , Then go to the following Step4 generate threshold signature.

When need convert t into $t' > t$, DC sending a broadcast message to each participant use $ShaTSS'$ algorithm convert his subshare σ_i into new subshare σ_i' . Then these participants recalculate their partial signature respectively and generate threshold signature by following steps:

Step1: Participants of authorized subset L send subshares $\sigma_i' (i = 1, \ldots, t')$ to DC, DC use these subshares to construct a full-rank lattice $L_{Sha}(\alpha_I, H, p)$, denote $\boldsymbol{t'} = (\sigma_{i_1}, \ldots, \sigma_{i_{t'}}, 0, 0, \ldots, 0) \in \mathbb{Z}^{t'+t}$.

Step2: Run the CVP approximation algorithm on lattice $L_{Sha}(\alpha_I, H, p)$ with target vector $\boldsymbol{t'} = (\sigma_{i_1}, \ldots, \sigma_{i_{t'}}, 0, 0, \ldots, 0) \in \mathbb{Z}^{t'+t}$. Return vector $c = (c_1, \ldots, c_{t'}, c_{t'+1}, \ldots, c_{t'+t})$, which is the approximating closest vector to $\boldsymbol{t'}$ in L_{Sha} .

Step3: Compute the recovered secret $k = \lfloor (p/H) \cdot c_{t'+1} \rfloor_p$ and convert into (f_0, f_0') .

Step4: Set

$$\mathrm{x} = \ulcorner -(1/q)m_{t'} \otimes f_0' \lrcorner \tag{6}$$

$$\mathrm{y} = \ulcorner -(1/q)m_{t'} \otimes f_0 \lrcorner \tag{7}$$

$$s_0 = \mathrm{x} \otimes f_0 + \mathrm{y} \otimes f_0' \tag{8}$$

$$s = s_{t'} + s_0 \tag{9}$$

Step5: Check the signature s , set

$$b = \| \, (s, \ s \otimes h_0 - m_0 (\mathrm{mod} \ q)) \, \| \tag{10}$$

If $b \ge \mathcal{N}$, set $r = r + 1$ and back to the partial signature generation phase Step1, , participants regenerate their own partial signature, then DC regenerate the threshold signature and output triplet (D, r, s) until $b < \mathcal{N}$.

D. Threshold Signature Verification

Verify the validity of threshold signature by the following steps:

Step1: Input a signed document (D, r, s) and the public key h_0 .

Step2: Encode r as a bit string. Set $m = H(D \| r)$.

Step3: Set $b = \| \, (s, \ s \otimes h_0 - m (\mathrm{mod} \ q)) \, \|$.

Step4: Output threshold signature valid if $b < \mathcal{N}$, invalid otherwise.

IV. SECURITY ANALYSIS

In this section we discuss about the security aspects of our proposed scheme. The notion of security of threshold signatures captures two properties:

（1）Robustness. Even if attacker can compromise $t-1$ members at most, the algorithm can still produce a valid signature.

（2）Unforgeability. Given system parameters, attackers ultimately can not forgery a threshold signature (D,r,s) of new message D .

Theorem 1 The proposed changeable threshold signature scheme guarantees threshold security and robustness.

Proof: From the threshold signature generation protocol, we can see that if the number of participants is less than t' or participants are non-authorized subset, it is impossible to recover the private key (f_0,f_0') . Even if obtained partial signatures, cooperation of participants in authorized subset also needs to contribute their subshare σ_i and ultimately generate the formal threshold signature. Hence, the scheme has the threshold security. The malicious members attempt to forge signature use the old threshold with the old subshare σ_i they holding. But when $t'>t$, they only holding $n+1-t$ public values of σ_i and there still lack of $t'-t$ public value of σ_i , therefore, it is impossible to forge a valid threshold signature.

If threshold t need to be converted into t', DC only needs to send a broadcast message to all participants to use $ShaTSS'$ algorithm convert σ_i to σ_i' respectively, it does not need to change private lattice basis parameters $\{f_i,f_i',h_i\}$ and public lattice basis parameter h .

Theorem 2 The partial signature has the property of unforgeability.

Proof. In partial signature generation phase, an attacker attempts to forgery partial signature through fake a signer $p_i(1\le i\le n)$. In order to obtain partial signature $s_i = \mathrm{x}\otimes f_i + \mathrm{y}\otimes f_i'$ he must solve the private key (f_i,f_i') . But (f_i,f_i') is secretly sent to the p_i by TC, attacker can only get s_i . If the attacker attempts to forgery s_i from $h_i \equiv f_i^{-1}\otimes f_i'(\bmod q)$, he have to break the NP-hard Problem Appr-CVP in NTRU lattice to solve (f_i,f_i') . Currently known attack methods of effectively against Appr-CVP include meet-in-the-middle algorithm [17] and lattice reduction algorithm [18].

(1) Partial signature against combinatorial forgery. The private key $\{f_i,f_i',h_i\}$ is randomly selected in a known space Γ .A combinatorial attack can be accomplished via meet-in-the-middle technique to recover (f_i,f_i') from the public key h_i [17]. We denote the combinatorial security of polynomials draw from Γ as $Comb[\Gamma]$ .Then $Comb[\Gamma(d)]\ge \binom{N}{d+1}/\sqrt{N}$ .If attacker attempts to get (f_i,f_i') via meet-in-the-middle attack, he need enumerate $C_N^{d_f}$ of f_i and $C_N^{d_g}$ of f_i' (e.g. $C_{251}^{72}\approx 1.19\times 10^{64}$),therefore it could against combinatorial forgery.

(2) Partial signature against lattice reduction forgery. Point (f_i,f_i') is included in the NTRU lattice L_{h_i} , (f_i,f_i') and its transpose is the short vector lie in L_{h_i} . Adversary can also launch a lattice attack by attempting to solve the Appr-CVP, he can use lattice reduction methods LLL locate a short enough vector to replace (f_i,f_i') and then use the vector to forge partial signatures. The running time for NTRU lattice reduction can be roughly estimated by $\log(T)\ge AN+B$ for some experimentally-determined constants A and B. Reference [19] gives an estimated time to break NTRU cryptosystem, when the experiments were run on 400 MHz Celeron machies, attack algorithm is LLL and (N,A,B)=(251,0.104,-12.036) , the breaking time will be at least 1.06×10^{14} MIPS-years.

Theorem 3 The threshold signature has the property of unforgeability.

Proof. (1) Threshold signature against combinatorial forgery. If public parameters $(N,q,d_f,d_g,n,T,\mathcal{N})$ are fixed, an adversary is given m, the image of a digital document through the hash function H . His problem is to locate a s that $\|(s \bmod q\, ,\alpha(h*s-m)\bmod q\| < \mathcal{N}$, where $\sqrt{\frac{12}{N}}\le\alpha\le 1$ is a balance factor. The running time of the algorithm is dominated by the process of searching the S -space, the attacker's expected work before being able to forge a signature is: $p(N,q,\alpha,\mathcal{N})<\sqrt{\frac{\pi^{N/2}}{\Gamma(1+N/2)}\cdot\left(\frac{\mathcal{N}}{q\alpha}\right)^{N}}$. If k is the desired bit security level it will suffice to choose parameters so that $\sqrt{\frac{\pi^{N/2}}{\Gamma(1+N/2)}\cdot\left(\frac{\mathcal{N}}{q\alpha}\right)^{N}}$ is less than 2^{-k} .From the above we can see that the probability of forge a threshold signature is almost negligible.

(2) Threshold signature against lattice reduction attack forgery. An attacker can solve Appr-CVP through lattice reduction methods. He can try to locate a point $(s,\alpha\tau)\in L_h(\alpha)$ sufficiently close to $(0,\alpha m)$ that $\|s,\alpha(\tau-m)\|<\mathcal{N}$. The difficulty of using lattice reduction methods to accomplish this can be tied to a lattice constant: $\gamma(N,q,\alpha)=\frac{\mathcal{N}}{\sigma(N,q,\delta,\alpha)\sqrt{2N}}$, $\sigma(N,q,\delta,\alpha)=\sqrt{\frac{Nq\alpha}{\pi e}}$ is the expected length of the shortest vector. For fixed $\gamma(N,q,\alpha)$ and N/q the running time for lattice reduction to find a point $(s\,,\tau)\in \mathrm{L}_h(\alpha)$ satisfying $\|s,\tau-m\|<\gamma(N,q,\alpha)\sqrt{2N}\sigma(N,q,\delta,\alpha)$ estimated roughly as $\log(T)\ge AN+B$. Reference [20] indicate that lattice strength against forgery is maximized as well as attack be

computationally infeasible for a fixed N/q, when $\gamma(N,q,\alpha)$ is as small as possible.

(3) Threshold signature against transcript forgery. The threshold signature is generated by n private lattice basis $\{f_i, g_i, F_i, G_i\}(i=1,\ldots,n)$ and a public lattice basis $\{f, g, F, G\}$. Assume that $f*G - g*F = f_i*G_i - g_i*F_i = q$ for each i, and that $\|F_i\| = \sqrt{N/12\|f_i\|}$.

An attacker can list a long transcript of valid signatures to forge a signature pairs (D,s) of the form:

$$s = \varepsilon f + \varepsilon' g + \varepsilon_1 f_1 + \varepsilon_1' g_1 + \cdots + \varepsilon_n f_n + \varepsilon_n' g_n \tag{11}$$

$$\tau - m = \varepsilon F + \varepsilon' G + \varepsilon_1 F_1 + \varepsilon_1' G_1 + \cdots + \varepsilon_n F_n + \varepsilon_n' G_n \tag{12}$$

The expectation of $\hat{s}$ and $\hat{\tau} - \hat{m}$, given by (13) and (14) is:

$$E(\hat{s}) = (N/12)(\hat{f}_0 + \hat{g}_0 + \cdots + \hat{f}_n + \hat{g}_n) \tag{13}$$

$$E(\hat{\tau} - \hat{m}) = (N/12)(\hat{F}_0 + \hat{G}_0 + \cdots + \hat{F}_n + \hat{G}_n) \tag{14}$$

As shown in [8], for the usual NTRU lattice second moment information $E(\hat{s})$ and $E(\hat{\tau} - \hat{m})$ can be obtained with transcripts on the order of 10,000 signatures. At least 100 million signatures are required to obtain the fourth moment. In this scheme, for t' participants we add the t' perturbation to threshold signature. For one perturbation, the attacker attempts to recovers the sixth moment accurately, there required transcript lengths at least 2^{30} [20]. Therefore the threshold signature scheme for transcript forgery is computationally secure.

V. Conclusion

The special signature form such as threshold signature has widely application fields. In this paper, we present a changeable threshold signature scheme which is based on the changeable threshold Shamir secret sharing scheme and NTRUSign algorithm. The signature can be safely generated with different threshold and needn't to modify the group public key and redistribute the subsecrets when changing the threshold. Security analysis showed that proposed scheme is secure under the assumption of NTRU lattice Approximate Closest Vector Problem. The proposed scheme is mainly based on polynomial multiplication and modulus operator; it needn't to introduce exponential operation and has a faster pace of signature and certification without compromising the security.

References

[1] Desmedt.Y, Frankel.Y, "Shared generation of authenticators and signatures," Proc of Advances in Cryptology--Crypto'91.Santa Barbara, California, USA, 1991, pp.457- 469.

[2] Jiang Han, Xu Qiu-liang, Zhou Yong-bin, "Threshold proxy signature scheme based on RSA cryptosystems," Chinese Journal of Computers. 2007, 30(2):241-247. (In Chinese)

[3] Liu Hong-wei, Xie Wei-xin, Yu Jian-ping, Zhang Peng, "Efficiency identity-based threshold group signature scheme," Journal on Communications, 2009,30(5):122-127. (In Chinese)

[4] Lee. N. Y, "Threshold signature scheme with multiple signing policies, "IEEE Proc Comput Digit Tech, 2001, 148 (2), pp.93-99.

[5] Wang Xiao-ming, Chen Huo-yan, Fu Fang-wei, "Dynamic threshold group signature scheme," Chinese Journal of Computers, .2004,27(9):1182-1186. (In Chinese)

[6] Pang Liao-jun, Jiao Li-chen, "Changeable threshold signature scheme without a trusted center," Acta Electronica Sinica, 2008, 36(8): 1559-1563. (In Chinese)

[7] J. Hoffstein, J. Pipher, J. H. Silverman, "NTRU: a ring-based public key cryptosystem," In Algorithmic Number Theory.Berlin: Springer -Verlag, LNCS 1423,1998, pp.267 -288.

[8] J. Hoffstein, N. Howgrave-Graham, J. Pipher, J. Silverman, W Whyte, "NTRUSign: digital signatures using the NTRU lattice ," In Topics in cryptology CT-RSA 2003. Berlin: Springer -Verlag, LNCS 2612, 2003, pp.122-140.

[9] J. Hoffstein, J Pipher, J. H. Silverman, "NSS:An NTRU lattice-based signature scheme ," Advanced in Eurocrypt'01.Berlin: Springer -Verlag, LNCS 2045, 2001, pp.123-137.

[10] J. Hoffstein, J. Pipher, J. H. Silverman, " Enhanced encoding and verification methods for the NTRU signature scheme," NTRU Cryptosystems Technical note#017 . http : // www.ntru.com/cryptolab/tech_notes.htm, 2001.

[11] Hu Yu-pu, "A novel NTRU-class digital signature scheme," Chinese Journal of Computers, .2008, 31(9):1661-1666. (In Chinese)

[12] Ron Steinfeld, Josef Pieprzyk, Huaxiong Wang, "Lattice-based threshold changeability for standard Shamir secret-sharing schemes," IEEE transactions on information theory. 2007, Vol. 53, No. 7, pp.2542-2558.

[13] Ron Steinfeld, Josef Pieprzyk, Huaxiong Wang, "Lattice-based threshold changeability for standard CRT secret-sharing schemes," Finite Fields and Their Applications. 2006, Vol. 12, No. 4, pp.653-680.

[14] I. Dinur, G. Kindler and S. Safra, "Approximating CVP to within almost polynomial factors is NP-hard," In 39th Annual Symposium on Foundations of Computer Science, Palo Alto, California, IEEE.7-10 Nov,1998.

[15] A. K. Lenstra, H. W. Lenstra and L. Lovasz, "Factoring polynomials with rational coefficients," Mathematische Annalen, 261(1982) , pp.515–534.

[16] L. Babai, "On Lovasz' lattice reduction and the nearest lattice point problem," Combinatorica, 6, 1986, pp.1-13

[17] N. Howgrave-Graham, J. H. Silverman, W. Whyte, "A meet-in-the-middle attack on an NTRU private key," NTRU Cryptosystems Technical note#004, version 2.http://www.ntru.com/cryptolab, 2003

[18] N.Gama, Howgrave-Graham. N, P. Q. Nguyen, "Symplectic lattice reduction and NTRU," Advances in Cryptology-Eurocrypt 2006. Berlin: Springer -Verlag, LNCS 4004, 2006, pp.233–253.

[19] J. Hoffstein, Jospeh. H. Silverman, W. Whyte, "Estimated breaking times for NTRU lattices,"NTRU Cryptosystems Technical note#012, Version 2.http://ntru.com/cryptolab/pdf/NTRUTech012v2.pdf,2003

[20] J. Hoffstein, N. Howgrave-Graham, J. Pipher, J. H. Silverman and W. Whyte, "Performance improvements and a baseline parameter generation algorithm for NTRUSign," http://eprint.iacr.org/,2005.