A Self Proxy Signature Scheme Over NTRU Lattices

11

Sonika Singh and Sahadeo Padhye

Abstract

The concept of self proxy signature (SPS) scheme was proposed by Kim and Chang in 2007. In a self proxy signatures, the signer wants to protect his original keys by generating temporary key pairs for a time period and then revoke them. The temporary keys can be generated by delegating the signing right to himself. Thus, in SPS the user can prevent the exposure of his private key from repeated use. If we are considering the existence of quantum computers, then scheme proposed by Kim and Chang's is no more secure since its security is based on the hardness of discrete logarithm assumption. In this paper we propose the first lattice based self proxy signature scheme. Since hard problems of lattices are secure against quantum attacks, therefore, our proposed scheme is secure against quantum computer also. We designed our scheme on NTRU lattices since NTRU lattices are most efficient lattices than general lattices.

Keywords

NTRU lattices · Proxy signature scheme · Random oracle · SIS problem · Identity based signatures

11.1 Introduction

Digital signature schemes are very important and significant primitives for constructing secure systems and are used in most of real world applications and security protocols. The proxy signature scheme is a kind of digital signature scheme firstly proposed by Mambo et al. [12] in 1996. It can be widely used in different situations, such as e-election, cloud computing, e-commerce etc. In proxy signature scheme, an original signer can delegate his signing rights to a proxy signer to sign on any document for a period of time. The proxy signer constructs a proxy private key by using the information given to him. Then he can use his signing rights to sign any document with his proxy private key by using a normal digital signature scheme. After getting the message and signatures from proxy signer, the verifier gets the public proxy key and verifies the correctness of signatures by using a normal digital signature scheme. After the concept of a proxy signature scheme proposed by Mambo et al., many effective proxy signature schemes [9, 10, 17, 22, 25, 27] etc. have been proposed by researchers based on discrete logarithmic problem (DLP). In 2007, Y.S. Kim and J.H. Chang [8] proposed a new type of digital signature scheme using DLP and they called it self proxy signature scheme. The idea behind self proxy signature is to keep the private key secret and generate temporary proxy keys to sign on any document on behalf of original key. So, in a self proxy signature scheme, a user Alice can delegates her signing rights to herself recursively. By using a self proxy signature scheme, the user Alice can generate many proxy public and private key pairs and can use them simultaneously. He can revoke the temporary private and public keys pair easily. Due to this fact, Kim et al. [8] considered their self proxy signature scheme for practical purposes and secure since their scheme satisfies all the security requirements of a proxy signature scheme. But, due to Shor's algorithm [18, 19], schemes based on DLP are not safe against quantum computers. Additionally, this scheme was analysed later in 2012 by S. Mashhadi [14, 24]. They showed that an adversary can forge a valid self proxy signature for any message by using different ways and proposed an improvement to remove the pointed out security leaks in Kim et al.'s scheme. After Kim et al. [8] scheme, several self proxy schemes have been proposed . As like, in 2010, Salevi et al. proposed ID Based self proxy signatures [16]. They gave a formal security model for identity based self proxy signatures and showed

S. Singh (✉) · S. Padhye
Department of Mathematics, Motilal Nehru National Institute of Technology, Allahabad, India

S. Latifi (ed.), *Information Technology – New Generations*, Advances in Intelligent Systems and Computing 738,
https://doi.org/10.1007/978-3-319-77028-4_11

that the scheme by Kim et al. [8] is existentially forgeable. They proposed a generic identity based self proxy signature scheme and proved the security in random oracle assumption. Later, in 2012, V. Verma also gave identity based version of a self proxy signature scheme with warrant [23]. Later, in 2013, Tahat et al. [21] proposed an efficient self proxy signature scheme based on ECDLP(elliptic curve discrete logarithm problem). They claimed that their scheme require less number of operations than Mashhadi scheme [14] and so is more efficient than Mashhadi scheme. The discrete logarithm problem is no more intractable after the quantum computers become reality. Therefore it is quite better to construct a scheme based on lattices, since lattices are considered as the best and strongest candidate for post quantum cryptography. The cryptographic schemes based on lattices are supported by worst case hardness assumption and Bernstein's conjuncture [1] that lattice can withstand quantum attacks. The running time of lattice based scheme are quadratic polynomial in respect of cubic polynomial of DLP and Factoring based scheme. The NTRU lattices [4–7] are better than general lattices. With general lattices, a scheme can suffer with large key sizes and large signature sizes. By motivating and considering all these facts, here, we are proposing a self proxy signature scheme relies on NTRU lattices in this paper and prove that it holds all the security requirements like distinguishability, unforgeability, verifiability and undeniabilty.

Rest of the sections in this paper is organized as follows. In Sect. 11.2, we give some required preliminaries used in our proposed scheme and then some related work (Kim and Chang self proxy scheme) is described in Sect. 11.3. The proposed self proxy signature scheme over NTRU lattices is given in Sect. 11.4. In Sect. 11.5, we provide a formal security proof for our scheme. Finally, in section 5 we conclude the paper.

11.2 Preliminaries

11.2.1 Notations

We will use the following notations throughout the paper-N is being security parameter and some power of 2. R is a polynomial ring $\frac{Z[X]}{X^N+1}$. The polynomials in ring R have degree $N-1$. R_q is a polynomial ring R with coefficients in Z_q i.e. $\frac{Z_q[X]}{X^N+1}$. q is a large modulus to which each coefficient is reduced. The polynomial f is the NTRU's private key polynomial and g is a polynomial used for generating the public key of NTRU cryptosystem [5, 6] from its private key f. The operation $\star$ is convolution multiplication operation. The polynomial h is NTRU's public key, given by $h = f_q^{-1} \star g \bmod q$. $||x||$ denotes the Euclidean norm of x and $||x||_1$ is l_1- norm which is given by $||x||_1 = \sum_{i=1}^{N} |x|_i$.

11.2.2 Definitions

We are giving some definitions that are very useful in this article.

Definition 1 (Self Proxy Signature Scheme) A self proxy signature scheme consists of the following algorithms—(assume Alice is the signer and Bob is the verifier.)

1. **Setup:** In this algorithm, Alice generates her private and public key pair as in a normal digital signature scheme.
2. **ProxyKeyGen:** Here, Alice constructs her temporary self proxy private and public key pair for a given time period. She publishes the proxy public key publicly available and can be revoked publicly.
3. **SelfProxySignGen:** The signer Alice here generates the signature on a message by using her private self proxy key and sends the signature and message pair to a verifier.
4. **SelfProxysignVfy:** The verifier Bob (say) using public proxy key checks the signature and message for verification.

Definition 2 (Secure Self Proxy Signature Scheme) A self proxy signature scheme is called secure if it satisfies following properties.

1. **Undeniability:** According to this property, a signer can not repudiate that he signed the document.
2. **Verifiability:** According to this property, a self proxy signature should be verified by anyone.
3. **Unforgeability:** No one can generate the valid self proxy signature except the original signer.
4. **Distinguish-ability:** The self proxy signatures should be distinguishable from normal signatures.

Definition 3 (NTRU Lattice) The NTRU lattice related to h and q is a full rank lattice in $\mathbb{Z}^{2N}$, given by

$$L_{h,q} = \{(u, v) : u + v \star h = 0 \; mod \; q\}.$$

The NTRU lattices are generated by the rows of the matrix

$$A_{h,q} = \begin{bmatrix} \mathcal{A}_{N,q}(h) & I_N \\ qI_N & O_N \end{bmatrix}$$

where $\mathcal{A}_N(h)$ is an anti-circulant matrix whose ith row contains of the coefficients of the polynomial hx^i mod (X^N+1).

11.2.3 Gaussian on Lattices

Discrete Gaussian Distribution: Gaussian sampling is a method given by Gentry et al. [3] to use a short basis as a trapdoor without revealing any information about the short basis. The $N-$ dimensional Gaussian distribution

$$\rho_{s,c}(x) = e^{-\pi \frac{||(x-c)||^2}{s^2}}$$

where $s \in R^m$ is standard deviation and vector $c \in Z^m$ is center.

For any lattice L, $\rho_{s,c}(L) = \sum_{x \in L} \rho_{s,c}(x)$. The probability mass function of the discrete Gaussian distribution is $D_{L,s,c}(x) = \rho_{s,c}(x)/_{s,c}(L)$.

Some Important Results about discrete Gaussian distribution [11, 15]:

1. For a real positive α and any $v \in Z^m$, if $\sigma = \omega(||v||\sqrt{logm})$, then

$$\Pr[x \leftarrow D_\sigma^m : \frac{D_\sigma^m(x)}{D_{\sigma,v}^m(x)} < e^{\frac{12}{\alpha}+\frac{1}{2\alpha^2}}] = 1 - 2^{100}$$

   where $\omega(.)$ is the non-asymptotic tight lower bound. If $\sigma = \alpha||v||$, then

$$\Pr[x \leftarrow D_\sigma^m : \frac{D_\sigma^m(x)}{D_{\sigma,v}^m(x)} = O(1)] = 1 - 2^{\omega(logm)}$$

2. For any $\sigma > 0$ and positive integer m,

$$\Pr[x \leftarrow D_\sigma^1 : ||x|| > 12\sigma] < 2^{-100}$$

$$\Pr[x \leftarrow D_\sigma^m : ||x|| > 2\sigma\sqrt{m}] < 2^{-m}$$

3. For given any $N-$dimensional lattice L, center $c \in R^N$, $\varepsilon > 0$ and $s > 2\eta_\varepsilon(L)$, for any $x \in L$,

$$D_{L,s,c}(x) \leq \frac{1+\varepsilon}{1-\varepsilon} 2^{-N}$$

   where $2\eta_\varepsilon(L)$ is the smoothing parameter of lattice L.

11.2.4 Master Key Generation

Master key generation algorithm is the most important part of a lattice based signature scheme because it generates secret keys. It works as follows:

Algorithm-1 $MasterKeyGen(N, q)$

```
Input : $N, q \in Z, \sigma > 0$
Output : $(msk, mpk) \in R^{2N \times 2N} \times R_q^\star$
Sample $f$ and $g$ from $D_{Z^N,\sigma}$
if $||f|| > \sigma\sqrt{N}$ or $||g|| > \sigma\sqrt{N}$ or $f$ ( mod $q$) $\notin R_q^\star$ or $g$ ( mod $q$) $\notin R_q^\star$ then
    Restart
end if
if max( $||(g, -f)||, ||(\frac{g\overline{f}}{f\overline{f}+g\overline{g}})||$) $> 1.17\sqrt{g}$ then
    Restart
end if
Define $\rho_f = \prod_{i=2}^{n-1} f(x^i) \bmod (x^N + 1)$ and $\rho_g$ similarly.
Compute $k_f$ and $k_g$ satisfy $\rho_f f + k_f(x^N+1) = R_f$, $\rho_g f + k_g(x^N + 1) = R_g$ where $R_f = resultant(f, x^N + 1)$, $R_g = resultant(g, x^N + 1)$
if $(R_f, R_g) \neq 1$ then
    Restart
end if
Find $\alpha$ and $\beta$ satisfy $\alpha R_f + \beta R_g = 1$ by extended Euclidean algorithm i.e. $(\alpha\rho_f)f + (\beta\rho_g)g = 1 + k(x^N + 1)$
Let $F = q\beta\rho_g$, $G = q\alpha\rho_f$, then $f \star G - g \star F = q$.
return KGC's public key $mpk = h = f^{-1}g$, KGC's secret keys $msk$ as
```

$$msk = B = \begin{bmatrix} \mathcal{A}(g) & -\mathcal{A}(f) \\ \mathcal{A}(G) & -\mathcal{A}(F) \end{bmatrix}$$

where $\mathcal{A}(g), -\mathcal{A}(f), \mathcal{A}(G), -\mathcal{A}(F)$ are anti-circulant matrices whose ith row contains the coefficients of the polynomial $gx^i \bmod (X^N + 1)$, $fx^i \bmod (X^N + 1)$, $Gx^i \bmod (X^N + 1)$ and $Fx^i \bmod (X^N + 1)$, respectively.

Note. In our proposed scheme, we are assuming KGC as signer Alice itself.

11.2.5 Hardness Assumption

Our signature scheme relies on small integer solution (SIS) problem and approximate shortest vector problem over NTRU lattices.

Definition 4 (SIS (Small Integer Solution) Problem Over Ring) $R(SIS_{q,m,\beta}^\phi)$. With the parameters q, m, ϕ and β, SIS problem can be defined as—If we are given m uniformly and independently chosen polynomials $a_1, a_2, \ldots, a_m$ in R_q, then to find non-zero $t \in \overline{a}$ satisfying the conditions $||t|| \leq \beta$ where $\overline{a} = \{(t_1, t_2, \ldots, t_m) \in R^m$ such that $\sum_i t_i a_i = 0 \bmod q\}$.

Definition 5 (SIS Problem Over NTRU Lattices) ($SIS^{\kappa}_{q,1,2,\beta}$). Stehle and Steinfeld [20] showed that statistical distance between R^* and the distribution of $h = \frac{g}{f}$ is $2^{10N}q^{-\lfloor\epsilon N\rfloor}$, which is negligible.

For SIS problem on NTRU lattice, set $R = \frac{Z[x]}{x^{N+1}}$ and let κ be distribution that chooses small f and g according to sampling algorithm $Sampler(B, \sigma, c)$, $A_{h,q} = (h, 1) \in R_q^{1\times 2}$ and $h = \frac{g}{f}$. The problem is to find (z_1, z_2) that satisfies the conditions $A_{h,q}(z_1, z_2)^T = 0 \bmod q$ and $||(z_1, z_2)|| \leq \beta$.

Definition 6 (γ Approximate Shortest Vector Problem) ($\gamma-$ SVP). For the NTRU lattice $L_{h,q}$ generated by the basis $A_{h,q}$, the shortest vector problem is to find the vector $(u, v) \in L_{h,q}$ such that $||(u, v)|| \leq ||(s, t)||$, $(s, t) \in L_{h,q}$. So, $\gamma-$ SVP is to find the vector $(u, v) \in L_{h,q}$ such that $||(u, v)|| \leq \gamma\lambda_1 L_{h,q}$, where $\lambda_1 L_{h,q}$ is the successive minimum of $L_{h,q}$.

Remark 1 According to the definitions of $\gamma-$ SVP and ($SIS^{\kappa}_{q,1,2,\beta}$), smallest integer solution problem is equal to the approximate shortest vector problem when $\frac{\beta}{\lambda_1 L_{h,q}} = \gamma$. Hence, our proposed scheme relies on the hardness of approximate shortest vector problem on the NTRU lattices against polynomial time algorithms and approximate shortest vector problem $\gamma-$SVP is a NP-hard problem with $\gamma < 1 + 1/n^{\epsilon}$ [2].

11.3 The Proposed Self Proxy Signature Over NTRU Lattice

We are presenting here a new self proxy signature scheme over NTRU lattices. Only two candidates are participating in the proposed self proxy signature scheme, an original signer Alice and a verifier Bob. The proposed scheme have three probabilistic polynomial time algorithms, *Setup*, $Self ProxySignKeyGen$, $Self ProxySignGen$ and a deterministic algorithm $Self ProxySignVfy$ algorithm. The underlying hardness of the proposed scheme is the hardness of $\gamma-$SVP and SIS problem over NTRU lattices. These algorithms are as follows :

1. **Setup** (N)**:** Here we consider the same parameter setup as given in [26]. On input of the security parameter N, this algorithm outputs the public parameters as follows:

   Let $q =$ Poly($N)(q \geq 3)$, $\varepsilon \in \left(0, \frac{lnN}{lnq}\right)$, $s = \Omega(N^{3/2}\sigma)$, where $\Omega(.)$ is the asymptotic lower bound and Poly(N) is the polynomial function of security parameter N. Then,

   1. Choose two hash functions $H_1 : \{0, 1\}^\star \rightarrow Z_q^{N\times k}$ and $H_2 : \{0, 1\}^\star \rightarrow \{v : v \in \{-1, 0, 1\}^k, ||v||_1 \leq k\}(k$ being a positive integer).
   2. Run the algorithm $MasterKeyGen$ to generate system's master key (msk, mpk).
   3. Public parameters of our proxy signature system are (N, q, H_1, H_2).

   The signer Alice computes $t = H_1(ID_A)$, where ID_A is Alice's identity and sets her private signing key $SK = (S_1, S_2)$ such that $S_1 + S_2 \star h = t$ by using master secret key msk and applying $Sampler(B, \sigma, (t, 0))$.
2. **SelfProxySignKeyGen:** In this phase, signer Alice constructs a message warrant W and the temporary self proxy signing private and public key pair with her original signing key $SK = (S_1, S_2)$ as follows:

   Alice construct a warrant W consists of public key of signer Alice and a valid time period T i.e. $W = (PK, T)$.

   For constructing self proxy keys, Alice first chooses $r_1, r_2 \in_R Z_q^{N\times k}$ randomly and computes $r_1 + r_2 \star h = u$ and makes u is a public quantity. Then, she sets her self proxy private signing key $SK_{sp} = (S_3, S_4)$ with $S_3 = S_1 t H_1(W) - r_1$ and $S_4 = S_2 t H_1(W) - r_2$. The self proxy signing public key is $PK_{sp} = t^2 H_1(W) - u$.
3. **SelfProxySignGen:** Let m be the message to be signed. The self proxy signature on message m is generated as follows.
   1. Randomly select $y_1, y_2 \in D_{Z^N, \sigma}$.
   2. Compute $U = H_2(y_1 + y_2 h, m)$
   3. Now, the signer computes $Z_1 = S_3 U + y_1$ and $Z_2 = S_4 U + y_2$.
   4. The signer generates the triplets (Z_1, Z_2, U) with probability $min\left(\frac{D_{Z^N, \sigma}}{MD_{Z^N, \sigma, SK_{sp}U}}, 1\right)$, where $M = O(1)$.
   5. Now, As a result, (W, Z_1, Z_2, U) is defined as the self proxy signature on message m of signer Alice by using temporary self proxy signing key.
4. **SelfProxySignVefy:** Now, after obtaining self proxy signature from the signer, the verifier verifies the signature in the following manner.
   1. Obtain the public key of signer from the public ID board.
   2. Verify whether $||Z_1, Z_2|| \leq 2s\sqrt{2N}$ and $H_2(hZ_2 + Z_1 - [t^2 - u]H_1(W)U, m) = U$ holds or not. If holds, then accept the signature as a valid signature, otherwise reject it.

Correctness: The correctness of the scheme is given as follows

$hZ_2 + Z_1 - [t^2 H_1(W) - u]U$

$= h(S_4 U + y_2) + (S_3 U + y_1) - [t^2 H_1(W) - u]U$

$= hS_4 U + hy_2 + S_3 U + y_1 - [t^2 H_1(W) - u]U$

$= (hS_4 + S_3)U + (hy_2 + y_1) - [t^2 H_1(W) - u]U$

$= [(hS_2 t + S_1 t)H_1(W) - (r_2 \star h + r_1)]U + (hy_2 + y_1) - [t^2 H_1(W) - u]U$

$= [(hS_2 + S_1)t H_1(W) - u]U + (hy_2 + y_1) - [t^2 H_1(W) - u]U$

$= [t^2 H_1(W) - u]U + (hy_2 + y_1) - [t^2 H_1(W) - u]U$
$= (hy_2 + y_1)$
Hence, $H_2(hZ_2 + Z_1 - [t^2 H_1(W) - u]U, m) = U$.

By combining the results of [11], the distribution of Z_i is very close to $D_{Z^N,s}$. Therefore, we have $||Z_i|| < 2s\sqrt{N}$ by the result of [15] with a probability of at least $1-2^N$. Hence, the inequality $||Z_1, Z_2|| \leq 2s\sqrt{2N}$ is with an overwhelming probability.

11.4 Security Analysis

In this section we describe that the proposed scheme satisfies all security properties of a self proxy signature scheme.

Theorem 1 *The proposed self proxy signature scheme entertains the unforgeability property.*

Proof The proposed self proxy signature scheme relies on SIS problem (or in particular $\gamma - SVP$). The security against forgeability is explained as follows :

We are assuming that an attacker wants to forge the self proxy signature. He can mount attack on the scheme in two manners—the first manner is to compute the private self proxy key SK_{sp}, and the second manner is to forge the valid self proxy signature without the self proxy private key. In the first way, the attacker has to compute SK_{sp} from PK_{sp} or to generate SK_{sp} with the help of the information (W, Z_1, Z_2, U) that is transferred from signer to verifier. Howbeit, it is computationally difficult to compute SK_{sp} from PK_{sp} or from (W, Z_1, Z_2, U) because it is SIS problem over NTRU lattices. Therefore, it is computationally hard to compute SK_{sp} for the attacker. In the second manner, the attacker has to get the valid signature (Z_1, Z_2, U) on the message document m without the private key SK_{sp}. Since the second condition for verification is also a SIS problem over NTRU lattices, so attacker has to solve SIS problem to forge the signature [26].

Since both the two attacks are not viable, therefore, it is computationally difficult to the attacker to forge the self proxy signature. Therefore, the proposed scheme holds the unforgeability property. □

Theorem 2 *The self proxy signature scheme satisfies the undeniability property.*

Proof As the requirement of undeniability property, the signer can not repudiate the valid message and its signature. In our proposed self proxy signature scheme, at the time of verification of the self proxy signature (W, Z_1, Z_2, U), the warrant W is also checked, and the publicly available information t^2 and u of the proxy signer and the master's public key h are used in the verification step. Therefore, the signer can not deny after signing on any message. □

Theorem 3 *The self proxy signature scheme holds the distinguish-ability property.*

Proof In the proposed self proxy signature scheme, the signer's identity, temporary public key and message warrant are used at the verification step of the self proxy signature (W, Z_1, Z_2, U). Thus, we can assume it as a self proxy signature instead of a normal signature. Hence, anyone can distinguish the self proxy signatures from normal signatures. If the signer sign the document with his original keys, the verification process will not hold. Therefore, the proposed signature scheme holds the distinguish-ability property. □

Theorem 4 *The proposed self proxy signature scheme entertains the verifiability property.*

Proof A scheme is said to be verifiable if the verifier can be assured of the signer's agreement on the signed message. In the proposed scheme, the verification phase is done with the help of the signer's identity and temporary public key. Therefore, any verifier can verify the signer's agreement on the signed message. Moreover, the verifier can recover the self proxy public key by public information. Hence, the proposed scheme satisfies the verifiability property. □

11.5 Conclusion

We proposed a new self proxy signature over NTRU lattices which is secure against quantum computer. Using this scheme, a user can delegate his signing right to himself for a period of time. The signer can have several ephemeral public and private key pairs and use them simultaneously. Our signature scheme is secure because it entertains all the security properties—verifiability, undeniability, distinguish-ability and unforgeability of a proxy signature scheme.

References

1. D.J. Bernstein, Introduction to post-quantum cryptography, in *Post-Quantum Cryptography*, ed. by D.J. Bernstein, J. Buchmann, E. Dahmen (Springer, Berlin, 2009), pp. 1–14
2. J.Y. Cai, A. Nerurkar, Approximating the SVP to within a factor (1+1/dim) is NP-hard under randomized reductions. J. Comput. Syst. Sci. **59**(2), 221–239 (1998)
3. C. Gentry, C. Peikert, V. Vaikuntanathan, Trapdoors for hard lattices and new cryptographic constructions, in *40th Annual ACM Symposium on Theory of Computing* (2008), pp. 197–206
4. J. Hermans, F. Vercauteren, B. Preneel, Speed records for NTRU, in *Topics in Cryptology-CT-RSA* (Springer, Basel, 2010), pp. 73–88

5. J. Hoffstein, J. Pipher, J.H. Silverman, NTRU: a new high speed public key cryptosystem (1996, preprint). Presented at the rump session of Crypto96
6. J. Hoffstein, J. Pipher, J.H. Silverman, NTRU : a ring based public key cryptosystem, in *Proceedings of ANTS*, LNCS, vol. 1423 (Springer, Cham, 1998), pp. 267–288
7. J. Hoffstein, J.H. Silverman, Optimizations for NTRU, in *Public-key Cryptography and Computational Number Theory* (DeGruyter, Berlin, 2000)
8. Y.S. Kim, J.H. Chang, Self proxy signature scheme. Int. J. Comput. Sci. Netw. Secur. **7**(2), 335–338 (2007)
9. S. Lal, A.K. Awasthi, Proxy blind signature scheme. J. Inf. Sci. Eng. Cryptol. ePrint Archive. Report 2003/072. Available at http://eprint.iacr.org/
10. Z.H. Liu, Y.P. Hu, H. Ma, Secure proxy multi-signature scheme in the standard model, in *Proceeding of the 2nd International Conference on Provable Security (ProvSec'08), Oct 30 Nov 1, Shanghai*. LNCS, vol. 5324 (Springer, Berlin, 2008), pp. 127–140
11. V. Lyubashevsky, Lattice signatures without trapdoors, in *31st Annual International Conference on the Theory and Applications of Cryptographic Techniques* (2012), pp. 738–755
12. M. Mambo, K. Usuda, E. Okamoto, Proxy signatures: delegation of the power to sign messages. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. **79**(9), 1338–1354 (1996)
13. M. Mambo, K. Usuda, E. Okamoto, Proxy signatures for delegating signing operation, in *3^{rd} ACM Conference on Computer and Communication Security(CCS'96)* (1996), pp. 48–57
14. S. Mashhadi, A novel secure self proxy signature scheme. Int. J. Netw. Secur. **14**(1), 2226 (2012)
15. P.Q. Nguyen, O. Regev, Learning a parallelepiped : cryptanalysis of GGH and NTRU signatures, in *24th Annual International Conference on the Theory and Applications of Cryptographic Techniques* (2006), pp. 271–288
16. S.S.D. Selvi, S.S. Vivek, S. Gopinath, C.P. Rangan, Identity based self delegated signature-self proxy signatures, in *Network and System Security (NSS)* (2010), pp. 568–573
17. S.H. Seo, K.A. Shim, S.H. Lee, A mediated proxy signature scheme with fast revocation for electronic transaction, in *Proceeding of the 2nd International Conference on Trust, Privacy and Security in Digital Business, Aug 22–26, Copenhagen*. LNCS, vol. 3592 (Springer, Cham, 2005), pp. 216–225
18. P. Shor, Algorithms for quantum computation: discrete logarithms and factoring, in *Proceedings of 35th Annual IEEE Symposium on Foundations of Computer Science* (IEEE, Piscataway, 1994), pp. 124–134
19. P. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. **26**, 1484–1509 (2006)
20. D. Stehle, R. Steinfeld, Making NTRUEncrypt and NTRUSign as secure as standard worst-case problems over ideal lattices (2013), Cryptology ePrint Archive 2013/004. Available from http://eprint.iacr.org/2013/004
21. N. Tahat, K.A. Alzubi, I. Abu-Falahah, An efficient self proxy signature scheme based on elliptic curve discrete logarithm problems. Appl. Math. Sci. **7**(78), 3853–3860 (2013)
22. Z. Tan, Z. Liu, C. Tang, Digital proxy blind signature schemes based on DLP and ECDLP. MM Research Preprints, No. 21, MMRC AMMS (Academia Sinica, Beijing, 2002), pp. 212–217
23. V. Verma, An efficient identity based selff proxy signature scheme with warrant. Int. J. Comput. Sci. Commun. **3**(1), 111–113 (2012)
24. G. Wang, Designated-verifier proxy signature schemes, in *Security and Privacy in the Age of Ubiquitous Computing (IFIP/SEC 2005)* (Springer, New York, 2005), pp. 409–423
25. G. Wang, F. Bao, J. Zhou, R.H. Deng, Security analysis of some proxy signatures, in *Information Security and Cryptology - ICISC 2003*. LNCS, vol. 2971 (Springer, Cham, 2004), pp. 305–319
26. J. Xie, Y.P. Hu, J.T. Gao, W. Gao, Efficient identity based signature over NTRU lattice. Front. Inf. Technol. Electron. Eng. **17**(2), 135–142 (2016)
27. Y. Yu, Y. Sun, B. Yang, Multi-proxy signature without random oracles. Chin. J. Electron. **17**(3), 475–480 (2008)