IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 21, 2021, accepted April 8, 2021, date of publication April 29, 2021, date of current version May 7, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3076598

Lattice Attacks on NTRU Revisited

JINGGUO BI[1] AND LIDONG HAN[2]
[1]School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China
[2]School of Information Science and Engineering, Hangzhou Normal University, Hanzhou 310018, China

Corresponding author: Jingguo Bi (jguobi@bupt.edu.cn)

This work was supported in part by the Fundamental Research Funds for the Central Universities under Grant 2021RC29, and in part by the National Natural Science Foundation of China under Grant 61702153 and Grant 61972050.

ABSTRACT NTRU cryptosystem was proposed by J. Hoffstein, J.Pipher and J.H. Silverman in 1996, whose security is related to the hardness of finding sufficient short vectors in NTRU lattice with dimension $2N$. Many researchers conjecture that the private key vector is indeed the shortest vector in the lattice in most cases. However, no formal proof has been provided in the literature before to the best of our knowledge. In this paper, we revisit the lattice attack on NTRU and present a new dimension reduction attack on NTRU without considering the pattern of private polynomials. More precisely, we show that one can recover a group of equivalent private keys by solving shortest vector problem in a new dimension-reduced lattice with dimension $N + k$, $k < N$, where k is related to the specific parameters selected. As a corollary of our attack, we prove that the private key vector and its rotations are the shortest vectors of the original NTRU lattice with an overwhelming probability, which confirms the conjecture of the length of the shortest vector of the original NTRU lattice.

INDEX TERMS Dimension reduction, key-recovery attack, lattice attack, NTRU, short vector.

I. INTRODUCTION

The NTRU cryptosystem [13] is one of fastest public-key cryptosystems, which consists of encryption (called NTRUEncrypt) and digital signatures (called NTRUSign). Compared with the traditional public-key cryptosystems based on factoring or discrete logarithm, the NTRU cryptosystem is more efficient and has the potential resistance to quantum computers. Because the encryption (or signature) and decryption (or verification) speeds are highly fast and require small amount of memory, it is suitable for enhancing the security in constrained devices. So far, NTRU has been issued as the *IEEE P1363.1* standards [15] and the *ASC X9.98* standards [1]. Since it was proposed in 1996, the security or insecurity of the NTRU scheme has been a hot research topic in the past nearly twenty years.

For the security of NTRU, the authors of NTRU [13] and Coppersmith and Shamir [4] showed that one can heuristically recover the secret key from the public key by searching a sufficiently short vector of the NTRU lattice. Since then, NTRU cryptosystem have been considered as a lattice-based scheme although it is based on polynomial arithmetic. Based on this lattice, the inventors of NTRU proposed the conservative extrapolation of the running times of the best known lattice reduction algorithm. It is worth mentioning that the authors did not show whether the private key vector is the shortest vector of the NTRU lattice defined in [4], [13]. Many researchers conjecture that the private key vector is indeed the shortest vector in the lattice in most cases. Bi and Cheng [2] showed that the length of the private key vector is at most constant times of the length of shortest vector of NTRU lattice based on the incompressibility method from the theory of Kolmogorov complexity.

In fact, the main attacks on NTRU primitives have bypassed the hard lattice problems in the last nearly twenty years. This was notably the case for the decryption failure attacks [6], [12], [16] on NTRUEncrypt, the attacks [5], [8], [9], [20] on NTRUSign [11]. Beside lattice reduction, the other two effective methods to choose an accurate NTRUEncrypt security parameters are: a meet-in-the-the-middle attack due to Odlyzko and the hybrid lattice-reduction and meet-in-the-the-middle attack due to Howgrave-Graham [10].

A. RELATED WORK

NTRU cryptosystem can be translated into a short vector problem in a special class of lattice [4], [13]. More specifically, the NTRU lattice L consists of all integer row vectors of the form (X, Y) such that $Y = XH \mod q$, where q is

The associate editor coordinating the review of this manuscript and approving it for publication was Wei Huang.

a public positive integer and H is an $N \times N$ public cyclic matrix. From the key generation algorithm, the private key vector (f, g) is a short vector in NTRU lattice. Together with its rotation, (f, g) constructs half of a reduced basis of NTRU lattice. It was showed that one can recover the secret key by finding a sufficiently short vector of NTRU lattice with dimension $2N$ [4], [13].

Since NTRU was introduced [13] in 1996, no significant weakness of NTRU lattice has been found in the last nearly twenty years. Based on the cyclic structure of NTRU lattice, May and Silverman [18], [21] proposed a zero-forcing method to decrease the dimension of NTRU lattice. Specifically, they showed that the private vector and its rotations have some kind of pattern of zeros. Let r denote the number of zeros, they showed that one can recover the private keys by solving the short vector problem in a new $2N - r$ dimension lattice. Unlike their method, we do not consider the pattern of private polynomial and its rotations. Reversely, our method can combine with this zero-forcing attack easily, and the hybrid attack will further decrease the dimension of the NTRU lattice.

B. OUR RESULTS

In this paper, we revisit the lattice attack on NTRU cryptosystem and present a new dimension reduction attack on NTRU without considering the pattern of private polynomials. Just like the methods in [4], [13], our attack can be considered as a key-recovery attack. The basic idea of our method is as follows, note that the private key vector (f, g) is a group of small solutions of the system of modular linear equations $Y = XH \mod q$, with N equations and $2N$ variables. Because the components of the private key vector are binary (or trinary), the space of private key set is not big enough compared with q. Intuitively, we do not need N equations, but only need partial equations can uniquely determine a group of private key. More precisely, we define a new lattice with the dimension $N+k$, where the integer $k < N$ can be determined by specific chosen parameters, and show that one can recover the private key vector by solving the shortest vector problem of this new lattice. As a corollary of our method, we show that the private key vector and its rotations are the shortest vectors in the original NTRU lattice with an overwhelming probability, which improve the results of [2]. To the best of our knowledge, this is the first formal proof of this conclusion in the literature.

Given a random lattice, it is common sense that the existed lattice reduction algorithms can find the shortest vector more easily when the ratio between the length of the shortest vector and the short vector's length predicts by Gaussian Heuristic increases. In another word, when the short vector's length is approximating to the Gaussian Heuristic, the lattice reduction algorithms will be hard to pick out the short vector. In our new dimension-reduced lattice attack on NTRU, the dimension decreases, however, the determinant of the new lattice decreases in the same time. Compares with the original lattice attack, the ratio defined before is decreasing, so the lattice reduction algorithm will spend more times in our attack than the original attack. We did experiments for our new lattice attack and the original lattice attack on NTRU, and the experiments data validate this conclusion especially when N is bigger than 100. From this point of view, our new attack does not hurt the security of the NTRU.

C. ROAD MAP

The rest of the paper is organized as follows. In Section 2, we review some backgrounds about lattices, NTRU algorithms and lattice attacks on NTRU. In Section 3, we present and prove our new lattice attack on NTRU. Finally, we conclude this paper in Section 4.

II. PRELIMINARIES

A. LATTICES

Let $\mathbb{R}^m$ be the m-dimensional Euclidean space. A lattice in $\mathbb{R}^m$ is the set

$$L(\mathbf{b_1}, \ldots, \mathbf{b_n}) = \{\sum_{i=1}^{n} x_i \mathbf{b_i} : x_i \in \mathbb{Z}\}$$

of all integral combinations of n linearly independent vectors $\mathbf{b_1}, \ldots, \mathbf{b_n} \in \mathbb{R}^m$. The *dimension* of a lattice L is the dimension n of the linear span of L. The sequence of vectors $\mathbf{b_1}, \ldots, \mathbf{b_n}$ is called a *lattice basis* and A lattice can be conveniently represented by a matrix $\mathbf{B}$, where $\mathbf{b_1}, \ldots, \mathbf{b_n}$ are the row vectors. The *determinant* of the lattice L is defined as square root of Gram determinant $\det_{1 \le i,j \le n} < \mathbf{b_i}, \mathbf{b_j} >$, where $< \mathbf{b_i}, \mathbf{b_j} >$ is the inner product of the vectors $\mathbf{b_i}, \mathbf{b_j}$, that is

$$\det(L(\mathbf{B})) = \sqrt{\det(\mathbf{B}\mathbf{B}^T)} \tag{1}$$

The most famous computational problem on lattices is the shortest vector problem (SVP): Given a basis of a lattice L, find a vector $\mathbf{u} \in L$, such that $\| \mathbf{v} \| \geq \| \mathbf{u} \|$ for any vector $\mathbf{v} \in L \setminus \mathbf{0}$. The following is a well-known theorem on the upper bound of the shortest vector length in lattice L.

Theorem 1 (Minkowski): Any lattice L of dimension n contains a non-zero vector $\mathbf{v}$ with

$$||\mathbf{v}|| \le \sqrt{n} \det(L)^{\frac{1}{n}}$$

For random lattices, one can expected the shortest vector length by Gaussian Heuristic.

Theorem 2 (Gaussian Heuristic): let $\mathbf{v}$ be a shortest vector of any random lattice L of dimension n, then

$$||\mathbf{v}|| \approx \sqrt{\frac{n}{2\pi e}} \det(L)^{\frac{1}{n}}$$

Gaussian Heuristic can be thought as the probable length of the shortest vector of a random lattice. If the actual shortest vector of a lattice L is significantly shorter than the estimation length by Gaussian Heuristic, it seems that LLL and other lattice reduction algorithms can find the shortest vector more easily.

B. DESCRIPTION OF THE NTRU CRYPTOSYSTEM

The operations of the NTRU cryptosystem take place in the ring of truncated polynomials $R = \mathbf{Z}[X]/(x^N - 1)$, where N is a chosen prime. For a polynomial $f \in R$, we can represent f as $f = \sum_{i=0}^{N-1} f_i x^i$, where f_i denotes the coefficient of x^k for $0 \le i \le N-1$. The convolution product $h = f * g$ of two polynomials f and g in R is defined by

$$h_k = \sum_{i+j \equiv k \mod N} f_i \cdot g_j$$

where each h_i, f_i, g_i represents the coefficient of h, f, g respectively.

To describe an implementation of the NTRUEncrypt encryption primitive, the following parameters are specified:

- N This degree parameter in NTRUEncrypt is chosen to be prime to prevent attacks due to Gentry [7].
- p, q Two relatively prime integers p and q, or alternatively p is a polynomial of degree $N-1$ and a prime number $q \nmid 2^N - 1$.
- L_f, L_g Private Key Spaces. Sets of small polynomials from which the private keys are selected.

Let R, R_p, and R_q be the convolution polynomial rings

$$R = \mathbf{Z}[x]/(x^N - 1), \quad R_p = (\mathbf{Z}/p\mathbf{Z})[x]/(x^N - 1).$$
$$R_q = (\mathbf{Z}/q\mathbf{Z})[x]/(x^N - 1).$$

For any positive integers d_1 and d_2, define the set

$$T(d_1, d_2) = \left\{ a(x) \in R : \begin{array}{l} a(x) \text{ has } d_1 \text{ coefficients} \\ \text{equal to } 1, d_2 \text{ coefficients} \\ \text{equal to } -1; \text{ has all} \\ \text{other coefficients equal to } 0 \end{array} \right\}$$

and the set

$$B(d) = \left\{ a(x) \in R : \begin{array}{l} a(x) \text{ has } d \text{ coefficients equal to } 1; \\ \text{has all other coefficients equal to } 0 \end{array} \right\}$$

There are many implementations of the NTRU cryptosystems [3], [13], [14]. The specific methods of parameters selection are different. Generally, the private key sets L_f and L_g are set to be $T(d_1, d_2)$ or $B(d_3)$ for d_1, d_2 and d_3 proportional to N. To prevent an exhaustive search attack, $|L_f|$ and $|L_g|$ have to be large. In this paper, we mainly analyze the trinary case. For the other cases of the parameter generation algorithms, we will analyze them in the full paper.

Randomly choose $f \in L_f = T(d_f, d_f - 1)$ and $g \in L_g = T(d_g, d_g)$ such that f is invertible in the polynomial rings R_p and R_q. Calculate $F_p = f^{-1}$ in R_p and $F_q = f^{-1}$ in R_q. Compute

$$h = F_q * g \tag{2}$$

in R_q. Then, the public key is h and the Private key is (f, F_p).

In this paper, we mainly focus on the lattice attack on NTRU, which is a kind of key-recovery attack. So we omit the specific Encryption and Decryption phase of NTRU cryptosystem. For the complete description of NTRU, we refer to [3], [13], [14].

C. LATTICE ATTACK ON NTRU

From (2), we have

$$fh = gg \mod (q, x^N - 1) \tag{3}$$

Define the cyclic matrix

$$H = \begin{pmatrix} h_0 & h_1 & \cdots & h_{N-1} \\ h_{N-1} & h_0 & \cdots & h_{N-2} \\ & \vdots & \ddots & \vdots \\ h_1 & h_2 & \cdots & h_0 \end{pmatrix}$$

and the NTRU lattice

$$L^{NTRU} = \begin{pmatrix} I & H \\ 0 & qI \end{pmatrix}. \tag{4}$$

Define $v = (f_0, f_1, \cdots, f_{N-1}, g_0, g_1, \cdots, g_{N-1})$, clearly, v and its rotations are belong to L^{NTRU}. Since $f_i \in \{-1, 0, 1\}$, v and its rotations will be N short vectors in L^{NTRU}. The security of the NTRU cryptosystem is related to the difficulty of finding short vectors in NTRU lattice [4], [13]. To make lattice reduction algorithm work more efficient, the researcher usually replace I with λI in L^{NTRU}. The specific value of λ can be chosen such that the actual shortest vector of L^{NTRU} shorter than the estimation length by Gaussian Heuristic.

Note that f is randomly chosen from $T(d_f, d_f - 1)$, the coefficients of f or its rotation would have r consecutive zeros or have the chosen pattern of zeros with high probability (see Table 2 of [18]). After chosen a suitable r, we can obtain a $2N - r$ dimension lattice by removing the corresponding r rows of the original NTRU lattice. May and Silverman [18] showed that one can recover the private keys by solving the short vector problem of this new dimension-reduced lattice. Generally, the time of finding short vectors is roughly proportional to the dimension of the lattice, this offers the possibility of significant speedup.

III. NEW LATTICE ATTACK ON NTRU

Firstly, we propose an assumption over the distribution of the coefficients of h.

Assumption 1: Let R_q^* represent the group of multiplication units of R_q. Randomly choose a polynomial $f \in L_f = T(d_f, d_f - 1)$, which is invertible in R_q^* and $g \in L_g = T(d_g, d_g)$, define F_q be the inverse of f in R_q^*, let $h = F_q * g \in R_q$, then each coefficient of h_i are distributed independent and uniformly over $\mathbf{Z}_q$.

In fact, if f is chosen randomly from R_q^*, then F_q is distributed uniformly over $\mathbf{Z}_q$. Therefore, $h = F_q * g$ is distributed uniformly over R_q. Here, we assume h has the similar property if f is randomly chosen from a subset of R_q^*.

Theorem 3: Given the NTRU parameters $N, q > 18$ and the public key $h = g * F_p$ in the ring R_q. Choose an integer $k = \lceil \frac{N \log(2\pi e)}{2 \log q - \log(2\pi e)} \rceil + 2$. Generate the new lattice L with the dimension $N + k$ below. Assume $v = (\hat{f}, \hat{g})$ is the shortest vector of lattice L, then with the probability $1 - \frac{1}{q}$, $\hat{f} = f'$,

$\hat{g} = g'$, where f' is one of the rotations of the private key f and g' is the first $k-$ continuous components of $f' * h$.

$$L = \begin{pmatrix} 1 & 0 & \cdots & 0 & h_0 & h_1 & \cdots & h_{k-1} \\ 0 & 1 & \cdots & 0 & h_{N-1} & h_0 & \cdots & h_{k-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & h_1 & h_2 & \cdots & h_k \\ 0 & 0 & \cdots & 0 & q & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & q & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & q \end{pmatrix} \quad (5)$$

Proof: Let f' be one of the rotations of the private key f and g' be the first $k-$ continuous components of $f' * h$. Obviously, the vector $\hat{v} = (f', g')$ is in L. Let $m = 2 \times d_f - 1$, then the length of $\|\hat{v}\| \leq R = \min\{\sqrt{m+k}, \sqrt{m+2d_g}\} \leq \sqrt{N+k}$.

In the following, we consider the vector $v = (s_0, s_1, \cdots, s_{N-1}, t_0, t_1, t_{k-1})$ which satisfies the conditions below:

$$\begin{cases} \|v\| \leq \|\hat{v}\| \\ v \in L \\ v \notin \{-\hat{v}, 0, \hat{v}\} \end{cases} \quad (6)$$

In the sequent part, we will consider the probability P that lattice L contains a short vector satisfies the conditions (6). Suppose vector $v = (s_0, s_1, \cdots, s_{N-1}, t_0, t_1, t_{k-1}) \in L$, then from the special structure of lattice L, the coordinates of v satisfies the following system of modular linear equations

$$\begin{cases} h_0 s_0 + h_{N-1} s_1 + \cdots + h_1 s_{N-1} \equiv & t_0 \\ h_1 s_0 + h_0 s_1 + \cdots + h_2 s_{N-1} \equiv & t_1 \\ \vdots & \\ h_{k-1} s_0 + h_{k-2} s_1 + \cdots + h_k s_{N-1} \equiv & t_{k-1} \end{cases} \mod q \quad (7)$$

From the Assumption 1, the coefficients h_i are distributed independent and uniformly over $\mathbf{Z}_q$, then random choose an invertible polynomial l from the private space L_f, then the coefficients of $h * l$ are distributed independent and uniformly over $\mathbf{Z}_q$. Let $s = (s_0, s_1, \cdots, s_{N-1})$ and $t = (t_0, t_1, \cdots, t_{k-1})$. Then,

$$\begin{aligned} P &= Pr(\exists v \in \mathbf{Z}^{N+k}, \text{ s.t. } \|v\| \leq \|\hat{v}\|, v \in L, \\ &\quad v \notin \{-\hat{v}, 0, \hat{v}\}) \\ &\leq Pr(\exists s \in \mathbf{Z}^N, \text{s.t. } s * h = t, \|s\|^2 \leq R_1^2, t \text{ fixed}) \\ &\quad \cdot |\{t \in \mathbf{Z}^k : \|t\|^2 \leq R_2^2\}| \\ &\leq q^{-k} \cdot |\{s \in \mathbf{Z}^N : \|s\|^2 \leq R_1^2\}| \cdot |\{t \in \mathbf{Z}^k : \|t\|^2 \leq R_2^2\}| \end{aligned}$$

where $R_1^2, R_2^2 \in \mathbf{Z}$ and $R_1^2 + R_2^2 = R^2$.
Note that

$$\begin{aligned} &|\{s \in \mathbf{Z}^N : \|s\|^2 \leq R_1^2\}| \cdot |\{t \in \mathbf{Z}^k : \|t\|^2 \leq R_2^2\}| \\ &= |\{s \in \mathbf{Z}^N : \sum_{R_1^2=1}^{R^2} \|s\|^2 = R_1^2\}| \cdot |\{t \in \mathbf{Z}^k : \\ &\quad \sum_{R_2^2=1}^{R^2-R_1^2} \|t\|^2 = R_2^2\}| \\ &= |\{\mathbf{v} \in \mathbb{Z}_q^{n+k} : \|\mathbf{v}\| \leq R\}| \end{aligned}$$

Let $N(n, R)$ denote the number of integer points in $B_n(R)$, where $B_n(R)$ represents the n-dimension ball centered at the origin with radius R. Denote

$$V = \{\mathbf{v} \in \mathbb{Z}_q^{n+k} | \ \|\mathbf{v}\| \leq R\}$$

Note that $|V| = N(n+k, R^2)$.

The probability P satisfies Equation (6) is

$$P \leq |V| \times q^{-k}$$

From [19], when $R > \sqrt{n/2}$, the number of integer points in $B_n(R)$ is

$$N(n, R) \approx (\frac{2\pi e}{n})^{n/2} R^n$$

That is,

$$P \leq \frac{(\frac{2\pi e}{N+k})^{\frac{N+k}{2}} (\sqrt{m+k})^{N+k}}{q^k} \leq \frac{(2\pi e)^{\frac{N+k}{2}}}{q^k} \quad (8)$$

Choose $k = \lceil \frac{N \log(2\pi e)}{2 \log q - \log(2\pi e)} \rceil + 2$, then $P \leq \frac{1}{q}$ for $q > 18$.

Then, vector $v = (\hat{f}, \hat{g})$ is the shortest vector of lattice L with the probability at least $1 - q^{-1}$.

Corollary 4: The private key vector (f, g) and its rotations are the shortest vectors of NTRU lattice L^{NTRU} with an overwhelming probability for $q > 18$.

Proof: In Equation (8), let $k = N$, we have

$$P \leq \frac{(2\pi e)^N}{q^N}$$

For any integer $q > 18$, we have $\lim_{N \to \infty} q = 0$

In this corollary, we prove that the private key vector and its rotations are the shortest vectors of NTRU lattice with an overwhelming probability. It is not a surprising result. Many researchers conjecture that the private key vector is indeed the shortest vector in the lattice in most of cases. However, no formal proof has been provided to the best of our knowledge. Based on the incompressibility method from the theory of Kolmogorov complexity, the authors [2] showed that the length of the private key vector is at most constant times of the length of shortest vector of NTRU lattice. Our result can be considered as an improvement of theirs.

Corollary 5: In Theorem 3, we analyzed the trinary case of the private key vector. For the binary case, our method will work well and the value k will be smaller because the space of the private key set shrinks. In the other implementations of NTRU cryptosystem [3], [14], the private polynomial f is chosen as the form $1 + p * F$, where p is set to be $2 + x$ and 3 respectively, and F is chosen from the polynomials set $B(d_f)$. From the foundational property $f * h = g$ in R_q, we have $(1 + p * F) * h = g$, then $F * (p * h) - h = g$ in R_q. This is a closest vector problem, and we can construct a new lattice

using the embedding method [17], then we can obtain the similar conclusion by the same method.

Corollary 6: In our dimension reduced attack, the determinant of $\mathcal{L}$ is $\det(L) = q^k$, and the length of the target vector which we want to find is $|(f', g')| \approx \sqrt{2d_f + 1 + k}$. From Gaussian heuristic, we know the short vector length in $\mathcal{L}$ is approximate to $\sqrt{\frac{N+k}{2\pi e}} q^{\frac{k}{N+k}}$.

Let

$$f(k) = \frac{\sqrt{2d_f + 1 + k}}{\sqrt{\frac{N+k}{2\pi e}} q^{\frac{k}{N+k}}}.$$

Note that for $1 \leq k \leq N$, the function $f(k)$ is strictly decreasing as k increases. As we all know, since as $f(k)$ gets closer to 1, the existed lattice reduction algorithms will have more and more difficulty to pick out the target vector. The experiment data validate this conclusion. We did experiments for our new lattice attack and the original lattice attack on NTRU, when N is smaller than 100, our attack is more efficient than the original lattice attack. However, for the bigger N, the lattice reduction algorithm will spend more times than the original attack.

IV. CONCLUSION

In this paper, we revisit the lattice attack on NTRU. More precisely, we construct a new lattice with the dimension $N+k$, where $k < N$ can be chosen from the specific parameters of the cryptosystems, and then we prove with overwhelming probability, the vector corresponding to the private key is the shortest vector of the new lattice. As a corollary of our method, we prove that the private key vector and its rotations are the shortest vectors of the original NTRU lattice with an overwhelming probability.

REFERENCES

[1] *ASC X9.98. Lattice-Based Polynomial Public Key Establishment Algorithm for the Financial Services Industry*. [Online]. Available: http://webstore.ansi.org/RecordDetail.aspx?sku=ANSI+X9.98-2010
[2] J. Bi and Q. Cheng, "Lower bounds of shortest vector lengths in random NTRU lattices," *TAMC*, pp. 143–155, 2012.
[3] *Consortium for Efficient Embedded Security. Efficient Embedded Security Standards ♯1: Implementation Aspects of NTRUEncrypt and NTRUSign, Version 2*, Jun. 2003.
[4] D. Coppersmith and A. Shamir, "Lattice attacks on NTRU," in *Advances in Cryptology—EUROCRYPT'97*. 1997.
[5] L. Ducas and P. Q. Nguyen, "Learning a zonotope and more: Cryptanalysis of NTRUSign countermeasures," in *Advances in Cryptology—ASIACRYPT 2012*. 2012, pp. 433–450.
[6] N. Gama and P. Q. Nguyen, "New chosen-ciphertext attacks on NTRU," in *Public Key Cryptography—PKC 2007* (Lecture Notes in Computer Science), vol. 4450, T. Okamoto and X. Wang, Eds. 2007, pp. 89–106, 2007.
[7] C. Gentry, "Key recovery and message attacks on NTRU-composite," in *Advances in Cryptology—EUROCRYPT 2001* (Lecture Notes in Computer Science), vol. 2045. New York, NY, USA: Springer-Verlag, 2001.
[8] C. Gentry, J. Jonsson, J. Stern, and M. Szydlo, "Cryptanalysis of the NTRU signature scheme (NSS) from Eurocrypt 2001," in *Advances in Cryptology—ASIACRYPT 2001* (Lecture Notes in Computer Science), vol. 2248. New York, NY, USA: Springer-Verlag, 2001.
[9] C. Gentry and M. Szydlo, "Cryptanalysis of the revised NTRU signature scheme," in *Advances in Cryptology—EUROCRYPT 2002* (Lecture Notes in Computer Science), vol. 2332. New York, NY, USA: Springer-Verlag, 2002.
[10] N. Howgrave-Graham, "A hybrid meet-in-the-middle and lattice reduction attack on NTRU," in *Advances in Cryptology—CRYPTO 2007*, vol. 4622, A. Menezes, Ed. Berlin, Germany: Springer, 2007, pp. 150–169.
[11] J. Hoffstein, N. A. Howgrave-Graham, J. Pipher, J. H. Silverman, and W. Whyte, "NTRUSIGN: Digital signatures using the NTRU lattice," in *Topics in Cryptology—CT-RSA 2003* (Lecture Notes in Computer Science), vol. 2612. New York, NY, USA: Springer-Verlag, 2003.
[12] N. Howgrave-Graham, P. Q. Nguyen, D. Pointcheval, J. Proos, J. H. Silverman, A. Singer, and W. Whyte, "The impact of decryption failures on the security of NTRU encryption," in *Proc. 23rd Cryptol. Conf. (Crypto)*, in Lecture Notes in Computer Science, vol. 2729. New York, NY, USA: Springer-Verlag, 2003, pp. 226–246.
[13] J. Hoffstein, J. Pipher, and J. Silverman, "NTRU: A ring-based public key cryptosystem," in *Algorithmic Number Theory* (Lecture Notes in Computer Science), vol. 1423. New York, NY, USA: Springer-Verlag, 1998, pp. 267–288.
[14] N. Howgrave-Graham, J. H. Silverman, and W. Whyte, "Choosing parameter sets for NTRUEncrypt with NAEP and SVES-3," in *Topics in Cryptology—CT-RSA 2005* (Lecture Notes in Computer Science), vol. 3376, A. J. Menezes, Ed. Berlin, Germany: Springer, 2005, pp. 118–135.
[15] *IEEE P1363.1. Lattice-Based Public-Key Cryptography*. [Online]. Available: http://grouper.ieee.org/groups/1363/
[16] E. Jaulmes and A. Joux, "A chosen-ciphertext attack against NTRU," in *Advances in Cryptology—CRYPTO 2000* (Lecture Notes in Computer Science), vol. 1880. New York, NY, USA: Springer-Verlag, 2000.
[17] R. Kannan, "Algorithmic geometry of numbers," *Annu. Rev. Comput. Sci.*, vol. 2, no. 1, pp. 231–267, Jun. 1987.
[18] A. May and J. H. Silverman, "Dimension reduction methods for convolution modular lattices," in *Cryptography and Lattices* (Lecture Notes in Computer Science), vol. 2146. New York, NY, USA: Springer-Verlag, 2001.
[19] J. E. Mazo and A. M. Odlyzko, "Lattice points in high-dimensional spheres," *Monatshefte für Math.*, vol. 110, no. 1, pp. 47–61, Mar. 1990.
[20] P. Q. Nguyen and O. Regev, "Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures," in *Advances in Cryptology—EUROCRYPT 2006* (Lecture Notes in Computer Science). New York, NY, USA: Springer-Verlag, 2006.
[21] J. H. Silverman. "Dimension-reduced lattices, zero-forced lattices, and the NTRU public key cryptosystem," NTRU Cryptosyst., Tech. Rep. ♯13 (Version 1).

JINGGUO BI received the B.Sc. and Ph.D. degrees in information security from Shandong University, in 2007 and 2012, respectively. He is currently an Associate Researcher with the School of Cyberspace Security, Beijing University of Posts and Telecommunications. His research interests include public key cryptography, cloud computing, and post-quantum cryptography.

LIDONG HAN received the B.S. and Ph.D. degrees in information security from Shandong University, Ji'nan, China, in 2005 and 2010, respectively. He held a postdoctoral position with the Institute for Advanced Study, Tsinghua University, Beijing. He is currently working with the School of Information Science and Engineering, Hangzhou Normal University. His research interests include public key cryptography, cloud computing, and authentication.