Chin. Ann. Math. Ser. B
41(5), 2020, 657–664
DOI: 10.1007/s11401-020-0225-6

Chinese Annals of Mathematics, Series B

Vulnerable Public Keys in NTRU Cryptosystem*

Liqing XU[1] Hao CHEN[1] Chao LI[2] Longjiang QU[2]

Abstract In this paper the authors give an efficient bounded distance decoding (BDD for short) algorithm for NTRU lattices under some conditions about the modulus number q and the public key $\mathbf{h}$. They then use this algorithm to give plain-text recovery attack to NTRU*Encrypt* and forgery attack on NTRU*Sign*. In particular the authors figure out a weak domain of public keys such that the recent transcript secure version of NTRU signature scheme NTRUMLS with public keys in this domain can be forged.

Keywords Lattice, CVP, NTRU Lattice
2000 MR Subject Classification 11H06, 52C07

1 Introduction

1.1 SVP and approximating SVP

A lattice $\mathbf{L}$ is a discrete subgroup in $\mathbb{R}^n$ generated by several linear independent vectors $\mathbf{b}_1, \cdots, \mathbf{b}_m$ over the ring of integers, where $m \leq n$, $\mathbf{L} := \{a_1\mathbf{b}_1 + \cdots + a_m\mathbf{b}_m : a_1 \in \mathbb{Z}, \cdots, a_m \in \mathbb{Z}\}$. The volume $\mathrm{vol}(\mathbf{L})$ of this lattice is $\sqrt{\det(\mathbf{B} \cdot \mathbf{B}^\tau)}$, where $\mathbf{B} := (b_{ij})$ is the $m \times n$ generator matrix of this lattice, where $\mathbf{b}_i = (b_{i1}, \cdots, b_{in}) \in \mathbb{R}^n$, $i = 1, \cdots, m$, are base vectors of this lattice. The length of the shortest non-zero lattice vectors is denoted by $\lambda_1(\mathbf{L})$. The famous shortest vector problem (SVP for short) is as follows: Given an arbitrary $\mathbb{Z}$ basis of an arbitrary lattice $\mathbf{L}$, find a lattice vector with length $\lambda_1(\mathbf{L})$ (see [12]). The approximating SVP $\mathrm{Gap\,SVP}_{f(m)}$ is to find some lattice vectors of length within $f(m)\lambda_1(\mathbf{L})$, where $f(m)$ is an approximating factor as a function of the lattice dimension m (see [12]). A breakthrough result of Ajtai [1] shows that SVP is NP-hard under the randomized reduction. Another breakthrough proved by Micciancio asserts that approximating SVP within a constant factor is NP-hard under the randomized reduction (see [12]). For the latest development we refer to [10]. It has been proved that approximating SVP within a quasi-polynomial factor is NP-hard under the randomized reduction.

Since the publication of [5], block Korkine-Zolotarev (BKZ for short) type algorithms with extreme pruning enumerations of large blocksizes $50 - 150$ as subroutines were proposed such

Manuscript received January 2, 2019.
[1]The College of Information Science and Technology/College of Cyber Security, Jinan University, Guangzhou 510632, China. E-mail: lqxul@jnu.edu.cn haochen@jnu.edu.cn
[2]The College of Liberal Arts and Science, National University of Defence Technology, Changsha 410073, China. E-mail: lichao_nudt@sina.com ljqu_happy@hotmail.com
*This work was supported by the National Natural Science Foundation of China (Nos. 11531002, 61722213, 61572026) and by the Major Program of Guangdong Basic and Applied Research (No. 2019B030302008).

that relative "shorter" lattice bases can be reduced from arbitrary given lattice bases. These algorithms can be used to solve some NTRU challenge problems (see [3, 5]).

1.2 NTRU*Encrypt* and NTRU*Sign*

The parameters of NTRU systems are as follows: Let N be a prime number, for example $N = 401$, p be a small prime number, for example, $p = 3$, and q be a large modulus number which is a prime power, for example, $q = 2^{11} = 2048$. Set $\Re = \mathbb{Z}[x]/(x^N - 1)$. Then $\Re_q = \mathbb{Z}/q\mathbb{Z}[x]/(x^N - 1)$ and $\Re_p = \mathbb{Z}/p\mathbb{Z}[x]/(x^N - 1)$. $\mathbf{B}_N(d)$ is the set of all polynomials of degree $N - 1$ with d coefficients equal to 1 and other coefficients equal to 0, $\mathbf{T}_N(d)$ is the set of all polynomials of degree $N - 1$ with d coefficients equal to 1, $d - 1$ coefficients equal to -1 and other coefficients equal to 0. Pick one random polynomial $\mathbf{f} \in \mathbf{B}_N(d_f)$ such that $\mathbf{f}$ is invertible in both $\Re_q$ and $\Re_p$. The inverses in $\Re_q$ and $\Re_p$ are denoted by $\mathbf{f_q}^{-1}$ and $\mathbf{f_p}^{-1}$ respectively. Pick one random $\mathbf{g} \in \mathbf{B}_N(d_g)$. $\mathbf{f}$ and $\mathbf{g}$ are private keys. The polynomial $\mathbf{h} = \mathbf{g}\mathbf{f_q}^{-1} \in \Re_q$ is the public key. The plaintext $\mathbf{m}$ is in $\Re_p$. Pick a random $\mathbf{r} \in \mathbf{B}_N(d_r)$. The encryption is $\mathbf{c} \equiv p\mathbf{r}\mathbf{h} + \mathbf{m} \bmod q$. The decryption is $\mathbf{c}' \equiv \mathbf{c}\mathbf{f} = p\mathbf{r}\mathbf{g} + \mathbf{m}\mathbf{f} \bmod q$. Then put the coefficients of $\mathbf{c}'$ in the interval $[-\frac{q}{2}, \frac{q}{2}]$ and the above module q equality holds over $\mathbf{Z}$. Hence $\mathbf{c}'\mathbf{f_p}^{-1} \equiv \mathbf{m} \bmod p$ holds with high probability. In most cases this recovers the plaintext $\mathbf{m}$.

The key recovery is to find the secret key$(\mathbf{f}, \mathbf{g})$. For appropriate parameters it can be solved by finding a shortest non-zero lattice vector in the lattice $\mathbf{L_h}$ which is spanned by the rows of the following matrix:

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & h_0 & h_1 & \cdots & h_{N-1} \\ 0 & 1 & \cdots & 0 & h_{N-1} & h_0 & \cdots & h_{N-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & h_1 & h_2 & \cdots & h_0 \\ 0 & 0 & \cdots & 0 & q & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & q & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & q \end{pmatrix}.$$

This matrix is of the following form:

$$\begin{pmatrix} \mathbf{I}_N & \mathbf{H} \\ \mathbf{0}_N & q\mathbf{I}_N \end{pmatrix},$$

where $\mathbf{H}$ is the circulant matrix of $\mathbf{h} = (h_0, h_1, \cdots, h_{N-1})$. Since $(\mathbf{0}, \mathbf{c}) = (p\mathbf{r}, p\mathbf{r}\mathbf{h}) + (-p\mathbf{r}, \mathbf{m})$, where $(p\mathbf{r}, p\mathbf{r}\mathbf{h})$ is in the lattice $\mathbf{L_h}$, notice that $\|(-p\mathbf{r}, \mathbf{m})\| \leq \left(\frac{p-1}{2}\right)\sqrt{d_r} + \left(\frac{p-1}{2}\right)\sqrt{N}$. The recovery of the plaintext from the public key $\mathbf{h}$ and the ciphertext $\mathbf{c}$ can be solved by finding a closest lattice vector in $\mathbf{L_h}$ to the vector $(\mathbf{0}, \mathbf{c})$. We refer to [8, 11, 15] for the detail.

We refer to [8, 11, 15] for the detail of the NTRU*Sign*. In the NTRU*Sign* scheme $\mathbf{f}$ and $\mathbf{g}$ are chosen randomly in $\mathbf{T}_N(d_f)$ and $\mathbf{T}_N(d_g)$. The forgery attack can be transformed to the following problem: For a given vector $(\mathbf{0}, \mathbf{m}) \in \mathbb{R}^{2N}$, find a lattice vector $\mathbf{v} \in \mathbf{L_h}$ such that $\|(\mathbf{0}, \mathbf{m}) - \mathbf{v}\| \leq \mathbf{B_{forgery}}$, $\mathbf{B_{forgery}} = \frac{N}{6}\sqrt{\delta(d)(12 + \beta^2 N)}$ (see [11]), where $\delta(d) = \frac{2d+1}{N} - \frac{1}{N^2}$ and β is a constant depending on $N, p, q, d = d_f = d_g$ (see [8, Table 11.8]).

In both NTRU*Encrypt* and NTRU*Sign* we note that $\mathbf{h}$ is not uniformly distributed in the space $\Re_q$, while in the Ring-LEW case, $\mathbf{a}$ is chosen uniformly at random in $\mathbb{Z}_q^d$. We refer to [2, 6–8, 11, 13, 16] and references therein for attacks and security analysis on NTRU systems. In particular it was showed in [16] that the distribution of public keys is statistically indistinguishable from uniform distribution if private keys are sampled from some Gaussian distributions. In a recent paper [4] Bernstein et al proposed to use the polynomial $x^p - x - 1$ to replace $x^N - 1$ in NTRU systems to avoid some recent attacks exploiting special algebraic structures (see [2]).

Transcript attack for NTRU*Sign* was proposed in [7] by exploiting many copies of signatures to get information about the private key. In 2006 Nguyen and Regev [13] gave a learning attack that the private key can be recovered from about 400 signatures. For the latest development we refer to [6, 14]. In 2009 Lyubashevsky proposed rejection sampling method and Hoffstein, Pipher, Schanck, Silverman, Whyer proposed a new transcript secure version of NTRU signature scheme in [9] to avoid the above attack. For the description of this scheme we refer to [9, 15]. This is the so-called NTRU modular lattice signature scheme, NTRUMLS for short. The underlying lattice problem is as follows: For any document $(\mathbf{s}_p, \mathbf{t}_p) \in \Re_p^2$, the signature to this document is a lattice vector $(\mathbf{s}, \mathbf{t}) \in \mathbf{L_h}$ satisfying

(1) $(\mathbf{s}_p, \mathbf{t}_p) \equiv (\mathbf{s}, \mathbf{t}) \bmod p$;

(2) $\|(\mathbf{s}, \mathbf{t})\|_\infty \leq \frac{q}{2} - B$, where B is a fixed bound and $\|\mathbf{x} = (x_1, \cdots, x_{2N})\|_\infty = \max\{|x_1|, \cdots, |x_{2N}|\}$. Here we should note $\|\mathbf{x}\|_\infty \leq \|\mathbf{x}\| \leq \sqrt{2N}\|\mathbf{x}\|_\infty$.

If a forger can find such a lattice vector $(\mathbf{s}, \mathbf{t})$ satisfying (1) and (2), then a signature of the document $(\mathbf{s}_p, \mathbf{t}_p)$ can be forged. The parameters $N = 661, p = 3, q = 9829081, B = 1487$ are suggested in [15]. The condition (2) can be replaced by $\|\mathbf{s}\|_\infty \leq \frac{q}{2} - B_s$ and $\|\mathbf{t}\|_\infty \leq \frac{q}{2} - B_t$. We refer to [9, 14–15].

2 Our Contribution—Vulnerable Public Keys in NTRU

Let N, p, q be as in Section 1 and ξ_N be a primitive N-th root of unity, where N is a prime as in the NTRU parameter setting. Let $\mathbf{h}$ be the public key as described in Section 1. We need the following quantities related to the public key $\mathbf{h}$. Set

$$\eta_i(\mathbf{h}) = h_0 + h_1\xi_N^i + \cdots + h_{N-1}\xi_N^{i(N-1)},$$

where $i = 0, 1, \cdots, N-1$. Set

$$\begin{aligned} D_1(\mathbf{h}) &= \min\{|\eta_0(\mathbf{h})|, |\eta_1(\mathbf{h})|, \cdots, |\eta_{N-1}(\mathbf{h})|\}, \\ D_2(\mathbf{h}) &= \max\{|\eta_0(\mathbf{h})|, |\eta_1(\mathbf{h})|, \cdots, |\eta_{N-1}(\mathbf{h})|\}, \\ \delta(\mathbf{h}) &= \max_{i_1 \neq i_2} |\eta_{i_1}(\mathbf{h}) - \eta_{i_2}(\mathbf{h})|. \end{aligned}$$

In the NTRU*Sign*, from Theorem 3.1 we can find a lattice vector $\mathbf{x} \in \mathbf{L_h}$ such that

$$\|(\mathbf{0}, \mathbf{m}) - \mathbf{x}\| \leq \frac{q\sqrt{N}}{2D_1(\mathbf{h})} + \frac{\sqrt{N}}{2} + \frac{\sqrt{N}D_2(\mathbf{h})}{2}.$$

When $D_1(\mathbf{h}) \approx D_2(\mathbf{h}) \approx \sqrt{q+1}$, this bound is approximating $\sqrt{Nq}$. If this bound is smaller than or equal to $\mathbf{B_{forgery}}$, a forged signature is easy for this NTRU*Sign* with this public key $\mathbf{h}$. We checked Table 11.8 in page 387 in [8], and this is not valid. However Theorem 3.1 gives a new constraint on the setting of NTRU*Sign* parameters and the public key.

When $\frac{q}{\|\mathbf{h}\|}$ is large, then Corollaries 3.1–3.3 imply that the recent transcript secure version NTRU signature scheme NTRUMLS described in [9, 14–15] is vulnerable for this public key. The suggested parameters in [9, Section 6] are vulnerable for our attack when $\|\mathbf{h}\|$ is not too large relative to q. We give the range of $D_1(\mathbf{h})$ and $D_2(\mathbf{h})$ in Table 1 for which the forgery is easy for any document $(\mathbf{s}_3, \mathbf{t}_3) \in \Re_3^2$. Parameters $N, p = 3, q, B_s, B_t$ are the same as in [9, Table 4].

Table 1 Vulnerable public keys in NTRUMLS

N	401	443	563	743	907
p	3	3	3	3	3
q	2^{15}	2^{16}	2^{16}	2^{17}	2^{17}
B_s	138	138	174	186	225
B_t	46	46	58	62	75
$D_1(\mathbf{h})$	≥ 80	≥ 63	≥ 70	≥ 81	≥ 91
$D_2(\mathbf{h})$	≤ 542	≤ 1037	≤ 946	≤ 1616	≤ 1453

In Table 2 the parameters N, p, q, B_s, B_t are the same as in [14, Table 4.2].

Table 2 Vulnerable public keys in NTRUMLS

N	401	439	593	743
p	3	3	3	3
q	2^{18}	2^{19}	2^{19}	2^{20}
B_s	240	264	300	336
B_t	80	88	100	112
$D_1(\mathbf{h})$	≥ 26	≥ 64	≥ 76	≥ 82
$D_2(\mathbf{h})$	≤ 4365	≤ 8317	≤ 6986	≤ 12491

From Theorem 3.2 the plaintext recovery from public key and ciphertext is possible when $\|\mathbf{m}\|$ and $\|\mathbf{r}\|$ are small. In the following table we list the conditions on $D_2(\mathbf{h})$ and $\delta(\mathbf{h})$ such that these public keys are vulnerable. The condition $\|\mathbf{m}\| \leq \sqrt{N}$ is automatically valid and $\|\mathbf{r}\|| \leq \frac{1}{2}\sqrt{N}$ is assumed (notice that $p = 3$). Parameters N, p, q are from [8, Table 11.1].

Table 3 Vulnerable public keys in NTRU*Encrypt*

N	401	449	547
p	3	3	3
q	2048	2048	2048
$\|\mathbf{r}\|$	≤ 10	≤ 11	≤ 12
$D_2(\mathbf{h}) - \delta(\mathbf{h})$	$20.024 - 32.918$	$21.2 - 31.52$	$23.4 - 28.5$
$D_2(\mathbf{h}) + N\delta(\mathbf{h})$	≤ 2048	≤ 2048	≤ 2048

If we allow $q = 4096$ for the same N and p we have the same table for vulnerable public keys without any condition on $\mathbf{m}$ and $\mathbf{r}$, since $\|\mathbf{m}\| \leq \sqrt{N}$ and $\|\mathbf{r}\| \leq \sqrt{N}$ are automatically valid when $p = 3$.

3 Main Results

For NTRU cryptosystem we have the following results for the lattice $\mathbf{L_h}$.

Theorem 3.1 *Let $N, p, q, \mathbf{h}, \mathbf{L_h}$ be as in the NTRU cryptosystem. Suppose that $D_1(\mathbf{h})$ and $D_2(\mathbf{h})$ are not zero. For any given vector $\mathbf{b} \in \mathbb{R}^N$, we can find a lattice vector $\mathbf{x} \in \mathbf{L_h}$ such that*

$$\|\mathbf{x} - (\mathbf{0}, \mathbf{b})\| \le \frac{q\sqrt{N}}{2D_1(\mathbf{h})} + \frac{\sqrt{N}}{2} + \min\Big\{\frac{\sqrt{N}D_2(\mathbf{h})}{2}, \frac{\sqrt{N}q}{2}\Big\}$$

within the complexity $O(N^3)$.

We set $\mathbf{v}_i = (1, \xi_N^i, \cdots, \xi_N^{i(N-1)})$, $i = 0, 1, \cdots, N-1$, where ξ_N is a primitive N-th root of unity.

Lemma 3.1 *The N vectors $\mathbf{v}_0, \mathbf{v}_1, \cdots, \mathbf{v}_{N-1}$ are orthogonal basis vectors of $\mathbf{C}^N$ with norm $\sqrt{N}$. The vector $\mathbf{v}_i$ is an eigenvector of the matrix $\mathbf{H}$ with eigenvalue $\eta_i(\mathbf{h}) = h_0 + h_1\xi_N^i + \cdots + h_{N-1}\xi_N^{i(N-1)}$.*

Set $\mathbf{U} = (\mathbf{v}_1^\tau, \cdots, \mathbf{v}_N^\tau)$. Then $\frac{1}{\sqrt{N}}\mathbf{U}$ is an unitary matrix. Set $\mathbf{G}$ the diagonal matrix with diagonal entries $\eta_0(\mathbf{h}), \cdots, \eta_{N-1}(\mathbf{h})$. Then the matrix $\mathbf{H} = \frac{1}{\sqrt{N}}\mathbf{U}\mathbf{G}\frac{1}{\sqrt{N}}\mathbf{U}^{-1}$.

Lemma 3.2 *Then we have $D_1(\mathbf{h})\|\mathbf{x}\| \le \|\mathbf{H}\cdot\mathbf{x}\| \le D_2(\mathbf{h})\|\mathbf{x}\|$.*

Proof of Theorem 3.1 It is clear that the rows of the following matrix $\mathbf{B}$,

$$\begin{pmatrix} \mathbf{I}_N & \mathbf{H} \\ \mathbf{0} & q\mathbf{I}_N \end{pmatrix}$$

is a basis of the lattice $\mathbf{L_h}$. Then we need to find $(\mathbf{c}^1, \mathbf{c}^2) \in \mathbb{Z}^{2d}$ such that $(\mathbf{c}^1, \mathbf{c}^2)\cdot\mathbf{B}$ approximates $(\mathbf{0}, \mathbf{b})$. We have $(\mathbf{c}^1, \mathbf{c}^2)\cdot\mathbf{B} = (\mathbf{c}^1, \mathbf{c}^1\cdot\mathbf{H} + q\mathbf{c}^2)$.

Then $(\mathbf{c}^1\cdot\mathbf{H} + q\mathbf{c}^2)\cdot\mathbf{v}_i^\tau = \eta_i(\mathbf{h})\mathbf{c}^1\cdot\mathbf{v}_i^\tau + q\mathbf{c}^2\cdot\mathbf{v}_i^\tau$. This is to express the lattice $\mathbf{L_h}$ with the basis $\mathbf{v}_i$'s. We have $\mathbf{H}\cdot\mathbf{U} = \mathbf{U}\cdot\mathbf{G}$ and $\mathbf{H} = \frac{1}{\sqrt{N}}\mathbf{U}\cdot\mathbf{G}\big(\frac{1}{\sqrt{N}}\mathbf{U}^{*\tau}\big)$. Hence $\big(\mathbf{c}^1, \mathbf{c}^1\cdot\frac{1}{N}\mathbf{U}\cdot\mathbf{G}\cdot(\mathbf{U}^{*\tau}) + q\mathbf{c}^2\big)$ is the general form of lattice vectors in $\mathbf{L_h}$.

For any given $\mathbf{b} = (b_0, \cdots, b_{N-1})^\tau$, set $[b_i]$ the closest integer to $\frac{b_i}{q}$. We set $\mathbf{c}^2 = ([b_0], \cdots, [b_{N-1}])$. Then the coordinates of $\mathbf{b}' = \mathbf{b} - q\mathbf{c}^2$ are in the interval $[-\frac{q}{2}, \frac{q}{2}]$. Set $\mathbf{b}'' = \mathbf{b}'\mathbf{U}\cdot\mathbf{G}^{-1}\cdot\big(\frac{1}{N}\mathbf{U}^{*\tau}\big) \in \mathbb{R}^N$. Here we should notice that $\mathbf{U}\cdot\mathbf{G}^{-1}\cdot\big(\frac{1}{N}\mathbf{U}^{*\tau}\big) = \mathbf{H}^{-1}$ is a real matrix. We then solve the CVP problem to the vector $\mathbf{b}'' = \mathbf{b}'\mathbf{U}\cdot\mathbf{G}^{-1}\cdot\big(\frac{1}{N}\mathbf{U}^{*\tau}\big) \in \mathbb{R}^N$ in the lattice $\mathbb{Z}^N$. Then $\mathbf{b}'' = \mathbf{b}'\mathbf{U}\cdot\mathbf{G}^{-1}\cdot\big(\frac{1}{N}\mathbf{U}^{*\tau}\big) = -\mathbf{c}^1 + \mathbf{e}'$ by rounding the coordinates, where $\mathbf{c}^1 \in \mathbb{Z}^N$ and $\mathbf{e}'$ is a vector in $\mathbb{R}^N$ satisfying $\|\mathbf{e}'\| \le \frac{\sqrt{N}}{2}$ (the covering radius of the integer lattice $\mathbb{Z}^N$). Thus $\|\mathbf{c}^1\| \le \frac{q\sqrt{N}}{2D_1(\mathbf{h})} + \frac{\sqrt{N}}{2}$ from Lemma 3.2. Then the lattice vector $\mathbf{v} = (\mathbf{c}^1, \mathbf{c}^2)\cdot\mathbf{B}$ is the lattice vector in $\mathbf{L_h}$ satisfying

$$\|(\mathbf{0}, \mathbf{b}) - \mathbf{v}\| \le \frac{q\sqrt{N}}{2D_1(\mathbf{h})} + \frac{\sqrt{N}}{2} + \frac{\sqrt{N}D_2(\mathbf{h})}{2}.$$

By rounding the vector $\mathbf{e}'\mathbf{U}\cdot\mathbf{G}\cdot\big(\frac{1}{N}\mathbf{U}^{*\tau}\big) \in \mathbb{R}^N$ in the lattice $q\mathbb{Z}^N$, we get the conclusion.

Theorem 3.2 *Let $N, p, q, \mathbf{h}, \mathbf{L_h}, \mathbf{r}, \mathbf{m}, \mathbf{e}$ be as in the NTRU cryptosystem. Suppose that $D_1(\mathbf{h})$ and $D_2(\mathbf{h})$ are not zero and $D_2(\mathbf{h}) + N\delta(\mathbf{h}) \le q$. Suppose that $\mathbf{c} = p\mathbf{rh} + \mathbf{m}$ is valid in $\Re_q$, and unknowns $\mathbf{r}$ and $\mathbf{m}$ satisfy*

$$\|\mathbf{m}\| < D_2(\mathbf{h}) - \delta(\mathbf{h}) \le \frac{q}{2} \quad \text{and} \quad \|\mathbf{r}\| < \frac{q - 2\|\mathbf{m}\|}{2p(D_2(\mathbf{h}) - \delta(\mathbf{h}))}.$$

Then the unknown $(-p\mathbf{r}, \mathbf{m})$ in $(\mathbf{0}, \mathbf{c}) = (-p\mathbf{r}, \mathbf{m}) + (p\mathbf{r}, p\mathbf{rm})$ can be found within the complexity $O(N^3)$ by the bounded decoding algorithm in Theorem 3.1.

Proof Set $\mathbf{b} = \mathbf{b}' - q\mathbf{c^2}$ and

$$\mathbf{b}'' = \mathbf{b}'\mathbf{U} \cdot \mathbf{G}^{-1}\Big(\frac{1}{N}\mathbf{U}^{*\tau}\Big) = -\mathbf{c^1} + \mathbf{e}'.$$

Here $\mathbf{e}'$ is the difference $\mathbf{b}'\mathbf{U} \cdot \mathbf{G}^{-1} \cdot \big(\frac{1}{N}\mathbf{U}^{*\tau}\big) - \mathbf{c}^1$ of the the vector $\mathbf{b}'\mathbf{U} \cdot \mathbf{G}^{-1} \cdot \big(\frac{1}{d}\mathbf{U}^{*\tau}\big)$ to its closest lattice vector $\mathbf{c}^1 \in \mathbb{Z}^N$. We set $(\mathbf{0}, \mathbf{b}) - (-p\mathbf{r}, \mathbf{m}) = (\mathbf{c'}^1, \mathbf{c'}^2)\mathbf{H}$. If $\mathbf{c'}^1 \ne \mathbf{c}^1$ or $\mathbf{c'}^2 \ne \mathbf{c}^2$, then $\mathbf{m} \ne \mathbf{e}'\mathbf{U} \cdot \mathbf{G} \cdot \big(\frac{1}{N}^{*\tau}\big)$. This would imply that $\mathbf{eU} \cdot \mathbf{G}^{-1} \cdot \big(\frac{1}{N}\mathbf{U}^{*\tau}\big)$ has one coordinate bigger than 1 or smaller than -1, or $\mathbf{m} - \mathbf{e}'\mathbf{U} \cdot \mathbf{G} \cdot \big(\frac{1}{N}\mathbf{U}^{*\tau}\big)$ is a non-zero vector in the lattice $q\mathbb{Z}^N$. In any of above cases, this leads to a contradiction to the conditions $\|\mathbf{m}\| < D_2(\mathbf{h}) - \delta(\mathbf{h}) \le \frac{q}{2}$ and $\| - p\mathbf{r}\| < \frac{\frac{q}{2} - \|\mathbf{e}\|}{C_2(\mathbf{a}) - \epsilon(\mathbf{a})}$. Actually if $\mathbf{c'}^2 \ne \mathbf{c}^2$ and $\mathbf{c'}^1 = \mathbf{c}^1$, then $\|\mathbf{m}\| \ge \frac{q}{2}$. If $\mathbf{c'}^1 \ne \mathbf{c}^1$ and $\mathbf{c'}^2 = \mathbf{c}^2$, then $\mathbf{mU} \cdot \mathbf{G}^{-1} \cdot \big(\frac{1}{N}\mathbf{U}^{*\tau}\big)$ has one coordinate bigger than 1 or smaller than -1. Then $\|\mathbf{m}\| \ge D_1(\mathbf{h}) \ge D_2(\mathbf{h}) - \delta(\mathbf{h})$ from Lemma 3.2. If $\mathbf{c'}^1 \ne \mathbf{c}^1$ and $\mathbf{c'}^2 \ne \mathbf{c}^2$, then

$$\mathbf{b} = \mathbf{c}^2 q + \mathbf{b}' = \mathbf{c}^2 q + \mathbf{c}^1\mathbf{UG}\Big(\frac{1}{N}\mathbf{U}^{*\tau}\Big) + \mathbf{e}' = \mathbf{c'}^2 q + \mathbf{c'}^1\mathbf{UG}\Big(\frac{1}{N}\mathbf{U}^{*\tau}\Big) + \mathbf{m}.$$

This implies that

$$\Big\|\mathbf{c'}^1\mathbf{UG}\Big(\frac{1}{d}\mathbf{U}^{*\tau}\Big)\Big\| \ge \|\mathbf{c}^2 q - \mathbf{c'}^2 q + \mathbf{b}'\| - \|\mathbf{m}\| \ge \frac{q}{2} - \|\mathbf{m}\|.$$

Then

$$\|\mathbf{c'}^1\| = \| - p\mathbf{r}\| \ge \frac{\frac{q}{2} - \|\mathbf{m}\|}{D_1(\mathbf{h})} \ge \frac{\frac{q}{2} - \|\mathbf{m}\|}{D_2(\mathbf{h}) - \delta(\mathbf{h})}.$$

The conclusion is proved.

Corollary 3.1 *In the transcript secure NTRUMLS described in* [24]*, if*

$$\frac{3q\sqrt{N}}{2D_1(\mathbf{h})} + \frac{3\sqrt{N}}{2} + \frac{3D_2(\mathbf{h})\sqrt{N}}{2} + 2\|\mathbf{s}_p\| + \|\mathbf{t}_p\| \le \frac{q}{2} - B,$$

a signature for this document $(\mathbf{s}_p, \mathbf{t}_p)$ can be forged.

Proof We require $\mathbf{c}^1 \in 3\mathbb{Z}^N$ and $\mathbf{c}^2 \in 3\mathbb{Z}^N$ in the proof of Theorem 3.1 and a lattice vector

$$\|(\mathbf{0}_p, \mathbf{t}_p) - (\mathbf{s}, \mathbf{t})\| \le \frac{3q\sqrt{N}}{2D_1(\mathbf{h})} + \frac{3\sqrt{N}}{2} + \frac{3D_2(\mathbf{h})\sqrt{N}}{2}$$

can be found. Then

$$\|(\mathbf{s}_p, \mathbf{t}_p) - (\mathbf{s}, \mathbf{t})\| \le \frac{3q\sqrt{N}}{2D_1(\mathbf{h})} + \frac{3\sqrt{N}}{2} + \frac{3D_2(\mathbf{h})\sqrt{N}}{2} + \|\mathbf{s}_p\|$$

and

$$\|(\mathbf{s},\mathbf{t})\| \le \frac{3q\sqrt{N}}{2D_1(\mathbf{h})} + \frac{3\sqrt{N}}{2} + \frac{3D_2(\mathbf{h})\sqrt{N}}{2} + \|\mathbf{s}_p\| + \|(\mathbf{s}_p,\mathbf{t}_p)\|.$$

The conclusion follows directly.

Since the coordinates of $\mathbf{s}_p$ and $\mathbf{t}_p$ are in the interval $[-\frac{p-1}{2}, \frac{p-1}{2}]$, $2\|\mathbf{s}_p\| + \|\mathbf{t}_p\| \le \frac{3(p-1)}{2}\sqrt{N}$. We have the following result about the vulnerable public keys in NTRUMLS.

Corollary 3.2 *In the NTRUMLS described in* [15]*, if*

$$\frac{3q\sqrt{N}}{2D_1(\mathbf{h})} + \frac{3\sqrt{N}}{2} + \frac{3D_2(\mathbf{h})\sqrt{N}}{2} + \frac{3(p-1)}{2}\sqrt{N} \le \frac{q}{2} - B$$

holds for this public key $\mathbf{h}$*, then the signature for any document can be forged for this NTRUMLS using this public key.*

In the setting of parameters of transcript secure version of NTRU signature scheme in [15] (see [13, Section 6]), parameters $N = 661, p = 3, q = 9829081$ and $B = 1407$ were suggested. For a public key $\mathbf{h}$ satisfying $\frac{490955}{D_1(\mathbf{h})} + \frac{D_2(\mathbf{h})}{2} \le 62987$, from Corollary 3.2 the forgery signature for any document is easy. Thus the NTRUMLS's with the public keys satisfying

$$\frac{490955}{D_1(\mathbf{h})} + \frac{D_2(\mathbf{h})}{2} \le 62987$$

are vulnerable.

If we use the condition $\|\mathbf{s}\|_\infty \le \frac{q}{2} - B_s$ and $\|\mathbf{t}\|_\infty \le \frac{q}{2} - B_t$ as in [9, 14], we have the following result.

Corollary 3.3 *In the NTRUMLS described in* [13, 23]*, if*

$$\frac{3q\sqrt{N}}{2D_1(\mathbf{h})} + \Big(p + \frac{1}{2}\Big)\sqrt{N} \le \frac{q}{2} - B_s$$

and

$$\frac{3D_2(\mathbf{h})\sqrt{N}}{2} + \frac{p-1}{2}\sqrt{N} \le \frac{q}{2} - B_t$$

hold for this public key $\mathbf{h}$*, then the signature for any document can be forged for this NTRUMLS using this public key.*

References

[1] Ajtai, M., The shortest vector problem in L_2 is NP-hard for randomized reduction, *STOC*, 1998, 10–19.

[2] Albrecht, M. R., Shi, B. and Ducas, L., A subfield lattice attack on overstreched NTRU assumption cryptanalysis of some FHE and graded encoding schemes, Crytpology ePrint Archive, https://eprint.iacr.org/2016/127.

[3] Aono, Y., Wang, Y., Hayashi, T. and Takagi, T., Improved progressive BKZ algorithms and their precise cost estimation by sharp simulator, Advances in Cryptology-*Eurocrypt* 2016, 789–819, Lecture Notes in Comput. Sci., 9665, Spring-Verlag, Berlin, 2016.

[4] Bernstein, D., Chuengsatiansup, C., Lange, T. and van Vredendaal, C., NTRU Prime: Reducing attack surface at low cost, Selected Areas in Cyptography-SAC 2017, 235–260, Lecture Notes in Comput. Sci., 10719, Spring-Verlag, Cham, 2018.

[5] Chen, Y. and Nguyen, P. Q., BKZ2.0: Better lattice security estimates, Asiacrypt 2011, Lecture Notes in Computer Science 7073, 1–20, http://www. di.ens.fr/ ychen/research/.

[6] Ducas, L. and Nguyen, P. Q., Learning a zonotope and more: Cryptanalysis of NTRU*Sign* countermeasuresm, Asiacrypt 2012, Lecture Notes in Computer Science 765, 433–450.

[7] Gentry, C. and Szydlo, M., Cryptanlysis of revised NTRU signature scheme, Eurocrypt 2002, Lecture Notes in Computer Science 2332, 299–320.

[8] Hoffstein, J., Howgrave-Graham, N., Pipher, J. and Whyte, W., Practical Lattice-Based Cryptography: NTRU*Encrypt* and NTRU*Sign*, 349–390, the LLL algorithms, Information Setting and Cryptogolgy, Nguyen P. Q. and Vallèe, B.(eds.), Springer-Verlag, Berlin, Heidelberg, 2010.

[9] Hoffstein, J., Pipher, J., Schanck, J. M., et al., Transcript secure signatures based on modular lattices, version 2, https://eprint.iacr.org/2014/457. DOI: 10.10071978-3-642-02295-1-11

[10] Khot, S., Hardness of approximating the shortest vector problem, *Journal of ACM*, **52**, 2005, 789–808.

[11] Lindner, R., Current attacks on NTRU, Diploma Thesis, Techology University of Darmstadt, Hesse-Darmstadt, 2006.

[12] Micciancio, D. and Goldwasser, S., Complexity of Lattice Problems, A Cryptographic Perspective, The Kluwer International Series in Engineering and Computer Science, 671, Kluwer Academic Publishers, Boston, MA, 2002.

[13] Nguyen, P. Q. and Regev, Q., Learning a parallelpiped: Cryptanalysis of GGH and NTRU signatures, Eurocrytp 2006, Lecture Notes in Computer Science 4004, 215–233.

[14] Schanck, J. M., Practical lattice cryptosystems, NTRU*Encrypt* and NTRUMLS, Master thesis, Waterloo University, Ontario, 2015.

[15] Silverman, J. H., NTRU and lattice-based crypto, Past, Presnet and Future, The mathematics of post-quantum cryptography, DIMACS Center, Rutgers University, January 12–16, New Jersey, 2015.

[16] Stehlé, D. and Steinfeld, R., Making NTRU*Encrypt* and NTRU*Sign* as secure as standard worst-case problems over ideal lattices, Eurocrypt 2011, Lecture Notes in Computer Science 6632, 24–47.