2017

Choosing Parameters for the Subfield Lattice Attack Against Overstretched NTRU

Dung Hoang Duong
Kyushu University, Japan Science Technology Agency, hduong@uow.edu.au

Masaya Yasuda
Kyushu University, Japan Science Technology Agency, yasuda@imi.kyushu-u.ac.jp

Tsuyoshi Takagi
Kyushu University, Japan Science Technology Agency

Choosing Parameters for the Subfield Lattice Attack Against Overstretched NTRU

Abstract

Albrecht et al. [1] at Crypto 2016 and Cheon et al. [4] at ANTS 2016 independently presented a subfield attack on overstretched NTRU problem. Their idea is to map the public key down to the subfield (by norm and trace map respectively) and hence obtain a lattice of smaller dimension for which a lattice reduction algorithm is efficiently applicable. At Eurocrypt 2017, Kirchner and Fouque proposed another variant attack which exploits the presence of orthogonal bases within the cyclotomic number rings and instead of using the matrix of the public key in the subfield, they use the multiplication matrix by the public key in the full field and apply a lattice reduction algorithm to a suitable projected lattice of smaller dimension. They also showed a tight estimation of the parameters broken by lattice reduction and implementation results that their attack is better than the subfield attack.

In this paper, we exploit technical results from Kirchner and Fouque [12] for the relative norm of field elements in the subfield and we use Hermite factor for estimating the output of a lattice basis reduction algorithm in order to analyze general choice of parameters for the subfield attack by Albrecht et al. [1]. As a result, we obtain the estimation for better choices of the subfields for which the attack works with smaller modulus. Our experiment results show that we can attack overstretched NTRU with modulus smaller than that of Albrecht et al. and of Kirchner and Fouque.

Disciplines

Engineering | Science and Technology Studies

Publication Details

Duong, D. Hoang., Yasuda, M. & Takagi, T. (2017). Choosing Parameters for the Subfield Lattice Attack Against Overstretched NTRU. Lecture Notes in Computer Science, 10599 79-91. Information Security 20th International Conference, ISC 2017, Ho Chi Minh City, Vietnam, November 22-24, 2017, Proceedings

Choosing Parameters for the Subfield Lattice Attack against overstretched NTRU

Dung Hoang Duong[1,2], Masaya Yasuda[1,2], and Tsuyoshi Takagi[1,2]

[1] Institute of Mathematics for Industry, Kyushu University,
744 Motooka Nishi-ku, Fukuoka 819-0395, Japan
[2] JST, CREST,
4-1-8 Honcho, Kawaguchi, Saitama, 332-0012, Japan
{duong,yasuda,takagi}@imi.kyushu-u.ac.jp

Abstract. Albrecht et al. [1] at Crypto 2016 and Cheon et al. [4] at ANTS 2016 independently presented a subfield attack on overstretched NTRU problem. Their idea is to map the public key down to the subfield (by norm and trace map respectively) and hence obtain a lattice of smaller dimension for which a lattice reduction algorithm is efficiently applicable. At Eurocrypt 2017, Kirchner and Fouque proposed another variant attack which exploits the presence of orthogonal bases within the cyclotomic number rings and instead of using the matrix of the public key in the subfield, they use the multiplication matrix by the public key in the full field and apply a lattice reduction algorithm to a suitable projected lattice of smaller dimension. They also showed a tight estimation of the parameters broken by lattice reduction and implementation results that their attack is better than the subfield attack.

In this paper, we exploit technical results from Kirchner and Fouque [12] for the relative norm of field elements in the subfield and we use Hermite factor for estimating the output of a lattice basis reduction algorithm in order to analyze general choice of parameters for the subfield attack by Albrecht et al. [1]. As a result, we obtain the estimation for better choices of the subfields for which the attack works with smaller modulus. Our experiment results show that we can attack overstretched NTRU with modulus smaller than that of Albrecht et al. and of Kirchner and Fouque.

1 Introduction

The NTRU encryption scheme is one of the first cryptosystems based on lattices proposed in 1998 by Hoffstein, Pipher and Silverman [11]. Up to present, `NTRUEncrypt` remains secure and is considered as one of the fastest post-quantum public key encryption schemes. The NTRU assumption is that, given the quotient ring $R = \mathbb{Z}[x]/(\phi(x))$ where $\phi(x)$ is a polynomial of degree n and q a positive integer, finding a "short" element in

$$\Lambda_h^q = \{(x, y) \in R^2 \mid hx = y \bmod q\}$$

is hard. Here h is the public polynomial in $R_q = \mathbb{Z}_q[x]/(\phi(x))$ which is of the form $h = gf^{-1} \bmod q$, where f and g are sampled from R such that they have small coefficient norms and f is invertible modulo q. In the original proposal [11], the authors used R to be the convolution ring $\mathbb{Z}[x]/(x^n - 1)$ and the coefficients of f and g are normally taken from the set $\{-1, 0, 1\}$. Even though there is no efficient attack against `NTRUEncrypt`, there is no security reduction to a hard mathematical problem; see [10] for current updates on the security of classical `NTRUEncrypt`. It is later recommended by Lyubashevsky and Micciancio [14] to replace the polynomial $x^n - 1$ by the cyclotomic polynomial $x^n + 1$ with n a power of 2, based on which they constructed a hash function proven collision-resistant under the assumed hardness of worse-case lattice problem over ideal lattices. Stehlé and Steinfeld used the polynomial $x^n + 1$ and defined a variant of `NTRUEncrypt`. They showed that if f and g are sampled from a Gaussian distribution with wide enough standard deviation, then `NTRUEncrypt` is proven to be secure under the hardness of lattice problems in ideal lattices; see [15] for more details. In this paper, we consider only the cyclotomic number ring $R = \mathbb{Z}[x]/(x^n + 1)$ where n is a power of 2.

Coppersmith and Shamir [6] showed that in order to break an NTRU cryptosystem, it suffices to find a short multiple of the secret key (f, g). The goal of the attack against NTRU problem then is to find a short enough vector in Λ_h^q, which is corresponding to an integral lattice of dimension $2n$; such a short vector will be a short multiple of the secret key (f, g) (see Theorem 8).

Albrecht et al. [1] and Cheon et al. [4] independently at Crypto 2016 and ANTS 2016 proposed a subfield attack on NTRU. Their idea, attributed to Gentry, Szydlo, Jonsson, Nguyen and Stern [9], is to exploit the presence of a subfield $\mathbb{L}$ in the cyclotomic number field $\mathbb{K} = \mathbb{Q}[x]/(x^n + 1)$. They then map the public key h down to the subfield $\mathbb{L}$ using the relative norm and trace map respectively. The obtained element h' in the subfield $\mathbb{L}$ gives rise to the NTRU problem with the associated lattice $\Lambda_{h'}^q$ of dimension much smaller than Λ_h^q. A solution for this NTRU problem in $\mathbb{L}$ will later be lift to a solution for the NTRU problem in the full field $\mathbb{K}$, and hence solves NTRU problem with large (overstretched) modulus q. At Eurocrypt 2017, Kirchner and Fouque [12] proposed a variant of the attack and claim that their attack is more efficient than that of Albrecht et al.'s and Cheon et al.'s. Their idea is to exploit the presence of orthogonal basis within the cyclotomic number ring and hence instead of mapping the public key down to the subfield, they use the projected lattices to the subring corresponding to the subfield. Their implementation results show that their attack is applicable with smaller modulus q compared to the subfield attack by Albrecht et al. The aforementioned attacks [1,4,12] against overstretched NTRU problem then can break several instances of NTRU-based cryptosystems, such as multilinear maps GGH13 [8], and fully homomorphic encryption LTV [13] and YASHE [3].

Our contribution. In this paper, we use tighter bound for norms of elements in the corresponding subfield from Kirchner and Fouque [12] and use the Hermite factor for approximating the output of a lattice reduction algorithm (e.g., LLL)

to analyze the subfield attack by Albrecht et al. [1]. As a result, we derive better choice for the subfield for which the attack is applicable with smaller modulus q. Our implementation results support our theoretical estimation for the choice of the subfield (see Table 1):

- For the same $n = 2^{11}$, with the choice of subfield $\mathbb{L}$ such that $|\mathbb{K} : \mathbb{L}| = 4$ while Albrecht et al. (cf. Table 5 in [1]) chose $\mathbb{L}$ such that $|\mathbb{K} : \mathbb{L}| = 8$, we can break the NTRU problem with $\log(q) = 72$ while Albrecht et al. succeeded with $\log(q) = 95$; it is a tradeoff that we have to work on a higher dimension lattice. Our succeeded modulus $\log(q) = 72$ for $n = 2^{11}$ is close to $\log(q) = 70$ of Kirchner and Fouque which is the smallest succeeded modulus and both have the same choice for the subfield to attack.
- For $n = 2^{12}$, with the choice of subfield $\mathbb{L}$ such that $|\mathbb{K} : \mathbb{L}| = 8$ while Albrecht et al. (cf. Table 6 in [1]) chose $\mathbb{L}$ such that $|\mathbb{K} : \mathbb{L}| = 16$ (same as Kirchner and Fouque), we can break the NTRU problem with $\log(q) = 135$ while Albrecht et al. succeeded with $\log(q) = 190$. Our succeeded modulus $\log(q) = 120$ for $n = 2^{12}$ is better than $\log(q) = 144$ of Kirchner and Fouque.

What we notice from experimental results of Kirchner and Fouque is that, although their method succeeded with small modulus q, it does not guarantee the success of larger modulus, whereas the subfield attack yields the exact limit of success, like in our and Albrecht et al.'s experiments.

2 Preliminaries

Let n be a 2-power number and $m = 2n$. Let $\mathbb{K} = \mathbb{Q}[x]/(x^n+1)$ be the cyclotomic number field. Let $\mathbb{L}$ be the subfield of $\mathbb{K}$ of degree n' with $n = rn'$. Let G be the Galois group of $\mathbb{K}$ over $\mathbb{Q}$ and H the subgroup of G fixing $\mathbb{L}$. Let $R = \mathcal{O}_{\mathbb{K}} = \mathbb{Z}[x]/(x^n+1)$ be the ring of integers of $\mathbb{K}$. Define the relative norm $\mathrm{N}_{\mathbb{K}/\mathbb{L}} : \mathbb{K} \to \mathbb{L}$ by

$$\mathrm{N}_{\mathbb{K}/\mathbb{L}}(a) = \prod_{\psi \in H} \psi(a).$$

and denote $L : \mathbb{L} \hookrightarrow \mathbb{K}$ be the canonical inclusion.

The number field $\mathbb{K}$ (or $\mathbb{L}$) is viewed as a Euclidean $\mathbb{Q}$-vector space by endowing with the inner product

$$\langle a, b \rangle = \sum_{e} e(a)\bar{e}(b),$$

where e ranges over all the n (or n') embeddings $e : \mathbb{K} \to \mathbb{C}$ and $\bar{e}$ its complex conjugate. This defines a Euclidean norm denoted by $\|.\|$. Define the operator norm $|.|$ as

$$|a| = \sup_{x \in \mathbb{K}^*} \frac{\|ax\|}{\|x\|}.$$

It is easy to check that $|a|$ is equal to $\max_e |e(a)|$, the maximal absolute complex embedding of a, and that $\|L(a)\|^2 = r\|a\|^2$, $|L(a)| = |a|$. Moreover for any $a \in \mathbb{K}$, one has

$$|a| \leq \|a\| \leq \sqrt{n} \cdot |a|,$$

and using the inequality of arithmetic and geometric means yields

$$|\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(a)| \leq \left(\frac{\|a\|}{\sqrt{n}}\right)^n. \tag{1}$$

The discriminant of the number field $\mathbb{K}$ is denoted by $\Delta_{\mathbb{K}}$. One has that $\sqrt{|\Delta_{\mathbb{K}}|} = \mathrm{Vol}(\mathcal{O}_{\mathbb{K}})$ and

$$\mathrm{Vol}(a\mathcal{O}_{\mathbb{K}}) = \left|\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(a)\right| \cdot \sqrt{|\Delta_{\mathbb{K}}|}.$$

Lemma 1 ([12, Lemma 1])**.** *Let $M \subseteq \mathbb{K}^d$ be a discrete $\mathcal{O}_{\mathbb{K}}$-module of rank 1. Then for any $0 \neq v \in M$, one has*

$$\mathrm{Vol}(M) \leq \left(\frac{\|v\|}{\sqrt{n}}\right)^n \cdot \sqrt{|\Delta_{\mathbb{K}}|}.$$

Proof. Since the rank of M is 1, one can build a $\mathbb{K}$-linear isometry from $\mathbb{R} \otimes M$ to $\mathbb{K} \otimes \mathbb{R}$. Hence we can assume that $d = 1$. Let v be a non-zero vector in M, then $v\mathcal{O}_{\mathbb{K}} \subseteq M$, which implies

$$\mathrm{Vol}(M) \leq \mathrm{Vol}(v\mathcal{O}_{\mathbb{K}}) = \mathrm{N}_{\mathbb{K}/\mathbb{Q}}(v) \cdot \sqrt{|\Delta_{\mathbb{K}}|} \leq \left(\frac{\|v\|}{\sqrt{n}}\right)^n \cdot \sqrt{|\Delta_{\mathbb{K}}|},$$

where the last inequality follows from (1). □

Definition 2 (**Gaussian Distribution**)**.** *Given $s > 0$, the discrete Gaussian distribution over the lattice $\mathcal{L}$ with zero mean is defined as $\mathcal{D}_{\mathcal{L},s}(x) = \rho_s(x)/\rho_s(\mathcal{L})$ for any $x \in L$, where $\rho_s(x) = \exp(-\pi\|x\|^2/s^2)$, $\rho_s(\mathcal{L}) = \sum_{x\in\mathcal{L}} \rho_s(x)$.*

Lemma 3. *For any lattice $\mathcal{L}$, any $t \geq 1$, then*

$$\Pr_{x\leftarrow\mathcal{D}_{\mathcal{L},s}}\left[\|\mathbf{x}\| > st\sqrt{\frac{n}{2\pi}}\right] < \exp(-n(t-1)^2/2).$$

It follows from Lemma 3 (by taking $t = \sqrt{2\pi}$) that $\|x\| \leq s\sqrt{n}$ with high probability.

Definition 4 (**NTRU Problem**)**.** *Given a ring $R = \mathbb{Z}[x]/(x^n+1)$ as above, a modulus q, a distribution $\mathcal{D}$ on R, and a target norm B. The NTRU problem is defined as the following: given $h = [gf^{-1}]_q$ where f, g are sampled from $\mathcal{D}$ (with the condition that f is invertible modulo q), find a vector $(x, y) \in R^2$ such that $(x, y) \neq (0, 0) \mod q$ and of Euclidean norm less than B in the lattice*

$$\Lambda_h^q = \{(x, y) \in R^2 : hx - y = 0 \bmod q\}.$$

One can express a basis $\mathbf{B}$ for Λ_h^q as follows

$$\mathbf{B} = \begin{pmatrix} q\mathbf{I}_n & \mathbf{h} \\ 0 & \mathbf{I}_n \end{pmatrix} \tag{2}$$

where $\mathbf{I}_n$ is the identity matrix of degree n and $\mathbf{h}$ stands for an $n \times n$ matrix whose i-th column is the coefficient vector of the polynomial $x^{i-1} \cdot \mathbf{h} \bmod x^n + 1$.

Remark 5. *Coppersmith and Shamir [6] showed that recovering short enough vectors may be sufficient; the NTRU Problem is essentially to recover the secret key (f, g). Hence, in order to attack the NTRU problem, we need to find a short non-zero vector (x, y) of Λ_h^q. We follow Albrecht et al. [1] to require that the solution (x, y) to have norm at most $q^{3/4}$.*

Heuristic 6 (Lattice reduction algorithms)**.** *There is an algorithm which, given as input a basis of a d-dimensional integer lattice L, outputs a non-zero vector v of L such that*

$$\|v\| \leq \delta_L \cdot \mathrm{Vol}(L)^{1/d}.$$

Here $\delta_L = c^d$ is the Hermite factor of a lattice reduction used for the lattice L. One has ([7]):

(i) $c \cong 1.0219$ *for LLL algorithm on average for* $d \geq 100$.
(ii) $c \cong 1.0128$ *for BKZ algorithm with block size* 20 *on average.*

Remark 7. *Heuristic 6 holds for random lattices (cf. [7]). For NTRU lattices* (2)*, if the modulus q is large, then the NTRU lattices* (2) *contain vectors shorter than $(0, \ldots, 0, q, 0, \ldots, 0)$, and hence a lattice reduction algorithm (e.g. LLL) can recover a multiple of the secret key. Experiments in Table 2 and Table 3 show that the root Hermite factor c for which our attack succeeds is much smaller than the approximation in Heuristic 6.*

3 Overview of the subfield lattice attack

Let $\mathbb{K} = \mathbb{Q}[x]/(x^n + 1)$ with n a 2-power. Denote by $\mathbb{L} = \mathbb{Q}[x^r]/(x^n + 1)$ a subfield of $\mathbb{K}$ with $n = rn'$. Let $\mathcal{D}_{\mathcal{O}_\mathbb{K},s}$ be the discrete Gaussian distribution over $\mathcal{O}_\mathbb{K}$ with standard deviation s, and let q be an integer. We consider the NTRU problem with f, g withdrawn from $\mathcal{D}_{\mathcal{O}_\mathbb{K},s}$ such that f is invertible modulo q. Set $h = gf^{-1} \bmod q$ and consider the NTRU lattice

$$\Lambda_h^q = \{(x, y) \in \mathcal{O}_\mathbb{K}^2 \ \mid \ hx = y \bmod q\}.$$

The subfield attack by Albrecht et al. [1] works in three steps as the following.

- Step 1: Norming down the public vector h to an element h' in the subfield $\mathbb{L}$
- Step 2: Using a lattice reduction algorithm of the lattice $\Lambda_{h'}^q$ in the subfield $\mathbb{L}$ which has dimension smaller than the original lattice.
- Step 3: Lifting up the results from Step 2 to the full field $\mathbb{K}$ and prove that they are short vectors in the lattice Λ_h^q, which are short multiples of secret key (f, g).

3.1 Norming down to the subfield

Let $h' = \mathrm{N}_{\mathbb{K}/\mathbb{L}}(h), g' = \mathrm{N}_{\mathbb{K}/\mathbb{L}}(g)$ and $f' = \mathrm{N}_{\mathbb{K}/\mathbb{L}}(f)$. Then $f', g' \in \mathcal{O}_{\mathbb{L}}$ and (f', g') is a vector of the following lattice

$$\Lambda_{h'}^q = \left\{(x', y') \in \mathcal{O}_{\mathbb{L}}^2 \mid h'x' = y' \bmod q\right\}$$

and depending on the parameters, it may be an unusually short one. We now have reduced our NTRU problem in the full field $\mathbb{K}$ (for the lattice Λ_h^q) to the NTRU problem in the subfield $\mathbb{L}$ (for the lattice $\Lambda_{h'}^q$). The lattice $\Lambda_{h'}^q$ has dimension $2n'$ and volume $q^{2n'}$.

3.2 Lattice reduction in the subfield

We now apply a lattice reduction algorithm (cf. Theorem 6) to the lattice $\Lambda_{h'}^q$ we obtain a non-zero vector $(x', y') \in \Lambda_{h'}^q$ of norm

$$\|(x', y')\| \leq \delta_{\mathbb{L}} \cdot \mathrm{Vol}(\Lambda_{h'}^q)^{1/2n'}.$$

where $\delta_{\mathbb{L}} = c^{2n'}$ is the Hermite factor of the lattice $\Lambda_{h'}^q$, and c is a constant depending on the corresponding lattice algorithm (cf. Theorem 6).

The following shows that if the vector (x', y') is short enough then it must be an $\mathcal{O}_{\mathbb{L}}$-multiple of (f', g').

Theorem 8 ([12, Theorem 8])**.** *Let $f', g' \in \mathcal{O}_{\mathbb{L}}$ be such that $\langle f' \rangle$ and $\langle g' \rangle$ are coprime ideals and that $h'f' = g' \bmod q\mathcal{O}_{\mathbb{L}}$ for some $h' \in \mathcal{O}_{\mathbb{L}}$. If $(x', y') \in \Lambda_{h'}^q$ has length satisfying*

$$\|(x', y')\| < \frac{n'q}{\|(f', g')\|}$$

then $(x', y') = v(f', g')$ for some $v \in \mathcal{O}_{\mathbb{L}}$.

Proof. We first prove that $B = \{(f', g'), (F', G')\}$ is a basis of the $\mathcal{O}_{\mathbb{L}}$-module $\Lambda_{h'}^q$ for some $(F', G') \in \mathcal{O}_{\mathbb{L}}^2$. By coprimity, there exist (F', G') such that $f'G' - g'F' = q \in \mathcal{O}_{\mathbb{L}}$. We note that

$$\begin{aligned} f'(F', G') - F'(f', g') &= (0, q); \\ g'(F', G') - G'(f', g') &= (-q, 0); \\ [f'^{-1}]_q(f', g') &= (1, h') \bmod q. \end{aligned}$$

Hence the module M generated by B contains $q\mathcal{O}_{\mathbb{L}}^2$ and $(1, h')$, i.e., $\Lambda_{h'}^q \subseteq M$. Moreover, $\det_{\mathbb{L}}(B) = f'G' - g'F' = q = \det_{\mathbb{L}}\{(1, h'), (0, q)\}$, we have $\mathrm{Vol}(M) = |\Delta_{\mathbb{L}}|q^{n'} = \mathrm{Vol}(\Lambda_{h'}^q)$ and therefore $M = \Lambda_{h'}^q$.

Denote by $\Lambda = (f', g')\mathcal{O}_{\mathbb{L}}$ and by Λ^* the projection of $(F', G')\mathcal{O}_{\mathbb{L}}$ orthogonally to Λ. We have $\mathrm{Vol}(\Lambda)\mathrm{Vol}(\Lambda^*) = q^{n'}\Delta_{\mathbb{L}}$. Let $0 \neq u \in \Lambda^*$ be a shortest vector in Λ^*. By Lemma 1, one has

$$\mathrm{Vol}(\Lambda) \leq \left(\frac{\|(f', g')\|}{\sqrt{n'}}\right)^{n'} |\Delta_{\mathbb{L}}|^{1/2}, \text{ and } \mathrm{Vol}(\Lambda^*) \leq \left(\frac{\|u\|}{\sqrt{n'}}\right)^{n'} |\Delta_{\mathbb{L}}|^{1/2}.$$

We deduce that $\lambda_1(\Lambda^*) = \|u\| \geq n'q/\|(f', g')\|$. The hypothesis implies that $\|(x', y')\| < \lambda_1(\Lambda^*)$. Hence $(x', y') \in \Lambda$ as desired. □

Remark 9. *It is proven in [1, Section 2.2] that with high probability (approximately 75%), f' and g' are coprime. However, the experiments succeeded even when they are not coprime.*

3.3 Lifting up the short vector

Assume that we have found a short non-zero vector $(x', y') \in \mathcal{O}_{\mathbb{L}}^2$ in the lattice $\Lambda_{h'}^q$ subject to the condition of Theorem 8, i.e., (x', y') is a short multiple of (f', g'). We now lift up (x', y') to $(x, y) \in \mathcal{O}_{\mathbb{K}}^2$ by computing

$$x = L(x') \text{ and } y = L(y') \cdot h/L(h') \bmod q \tag{3}$$

where $L : \mathbb{L} \hookrightarrow \mathbb{K}$ is the canonical inclusion map of $\mathbb{L} \subset \mathbb{K}$.

Obviously $(x, y) \in \Lambda_h^q$. It follows from Theorem 8 that $x' = vf', y' = vg'$ for some $v \in \mathcal{O}_{\mathbb{L}}$. Let $\bar{f} = L(f')/f$, $\bar{g} = L(g')/g$ and $\bar{h} = L(h')/h$. Note also that $\bar{f}, \bar{g}$ and $\bar{h}$ are integers over $\mathbb{K}$. We write

$$\begin{aligned} x &= L(x') = L(v) \cdot \bar{f} \cdot f \bmod q \\ y &= L(y') \cdot h/L(h') = L(v) \cdot \bar{f} \cdot g \bmod q \end{aligned}$$

and hence $(x, y) = u \cdot (f, g)$ is a multiple of (f, g), for $u = L(v) \cdot \bar{f} \in \mathcal{O}_{\mathbb{K}}$.

4 Revisiting Albrecht et al.'s attack [1]

In this section, we analyse the subfield attack proposed by Albrecht et al. [1]. First, we analyse in Section 4.1 theoretically the modulus q and yield better choice of r for which the subfield attack is feasible with smaller modulus q. In Section 4.2, we compare the theoretical estimation and implementation results.

4.1 Theoretical analysis

Set $D = s\sqrt{n}$ to be the upper bound for the norm of a secret polynomial sampling from the discrete Gaussian distribution $\mathcal{D}_{\mathcal{O}_{\mathbb{K}},s}$ over $\mathcal{O}_{\mathbb{K}}$ (see Lemma 3). Hence for $f, g \leftarrow \mathcal{D}_{\mathcal{O}_{\mathbb{K}},s}$, one has $\|f\|, \|g\| \leq D$. Let $\mathbb{L}$ be the subfield of $\mathbb{K}$ of degree n', i.e., $n = rn'$, and let

$$f' = \mathrm{N}_{\mathbb{K}/\mathbb{L}}(f),\ g' = \mathrm{N}_{\mathbb{K}/\mathbb{L}}(g),\ h' = \mathrm{N}_{\mathbb{K}/\mathbb{L}}(h).$$

Then

$$\|f'\| \leq \sqrt{n'}D^r,\ \|g'\| \leq \sqrt{n'}D^r,$$

and hence

$$\|(f', g')\| \leq \sqrt{2n'}D^r.$$

Table 1. Comparison of succeeded modulus $\log(q)$ for the subfield attacks. We use LLL algorithm as in Albrecht et al. and Kirchner-Fouque.

$\log(n)$	$t = \log(r)$	Succeeded $\log(q)$	Method	Estimated $\log(q)$
9	2	40	Ours	44
10	2	52	Ours	63
11	3	95	Albrecht et al. [1]	109
11	2	70	Kirchner and Fouque [12]	
11	**2**	**72**	**Ours**	98
12	4	190	Albrecht et al. [1]	208
12	4	144	Kirchner and Fouque [12]	
12	**3**	**120**	**Ours**	148

Applying a lattice reduction algorithm to the lattice $\Lambda^q_{h'}$, we obtain a non-zero vector (x', y') of norm

$$\|(x', y')\| \leq c^{2n'}\sqrt{q},$$

and therefore

$$\|(x', y')\| \cdot \|(f', g')\| \leq c^{2n'}\sqrt{2n'}D^r\sqrt{q}.$$

It follows from Lemma 1 that if

$$c^{2n'}\sqrt{2n'}D^r\sqrt{q} < n'q \tag{4}$$

then (x', y') will be a multiple of (f', g'). Inequality (4) is equivalent to

$$4n'\log(c) + 2r\log(s) + r\log(n) + 1 - \log(n') < \log(q). \tag{5}$$

Notice that

$$\begin{aligned} 4n'\log(c) + 2r\log(s) + r\log(n) &= \frac{4n\log(c)}{r} + r(2\log(s) + \log(n)) \\ &\geq 2\sqrt{4n\log(c)(2\log(s) + \log(n))} \end{aligned}$$

with equality if and only if

$$r = \sqrt{\frac{4n\log(c)}{2\log(s) + \log(n)}}\ . \tag{6}$$

Hence the choice of r in (6) optimizes the left-hand side of (5), and hence yields the estimation of the modulus q that makes NTRU problem vulnerable to the subfield attack.

4.2 Implementation results

In Table 1, we show our choice of r, which is the index of the subfield $\mathbb{L}$ in $\mathbb{K}$, to which we apply the subfield attack, and compare the actual succeeded values

of $\log(q)$ by our, Albrecht et al.'s [1] and Kirchner-Fouque's experiments. As in previous works of Albrecht et al. and Kirchner-Fouque, we use LLL algorithm in our experiments. We take $s = \sqrt{2/3}$, and use constant $c = 1.0219$ (see Heuristic 6) for estimating the choice of r. Experimental results for the cases $n = 2^{11}$ and $n = 2^{12}$ can be seen from Table 2 and Table 3 respectively. The requirement for success of the attack is that the obtained solution (x, y) is a multiple of (f, g) and has norm at most $q^{3/4}$ (following Albrecht et al. [1]).

- For $n = 2^{11}$, we choose $r = 2^2$ which is the same as Kirchner-Fouque and different from Albrecht et al. (vs. $r = 2^3$). We succeeded with $\log(q) = 72$, which is much smaller than $\log(q) = 90$ by Albrecht et al. and close to $\log(q) = 70$ by Kirchner-Fouque.
- For $n = 2^{12}$, we choose $r = 2^3$ whereas Albrecht et al. and Kirchner-Fouque's chose $r = 2^4$. We succeeded with $\log(q) = 120$ which is smaller than $\log(q) = 190$ by Albrecht et al. and $\log(q) = 144$ by Kirchner-Fouque.

The last column of Table 1 gives our estimated values of breakable $\log(q)$ in the subfield attack which are larger than the results from experiments. One reason is that our estimation for the upper bound of the norms of $\mathrm{N}_{\mathbb{K}/\mathbb{L}}(f)$ and $\mathrm{N}_{\mathbb{K}/\mathbb{L}}(g)$ is not tight; for example, for $n = 2^{12}$, our estimated for $\log(\|(f', g')\|)$ is around 57.75 while it is approximately 46 by experiments.

Table 2 shows our implement results for the subfield attack against NTRU problem for $n = 2^{11}$ in which we choose the subfield $\mathbb{L} \leq \mathbb{K}$ with $|\mathbb{K} : \mathbb{L}| = r$ and $\log(r) = 2$ according to (6). Note that for the case $\log(q) = 70, 71$, the attack is successful, i.e. the obtained results are multiple of the secret key (f, g), but they are not short enough as required. Table 3 shows our implement results for the subfield attack against NTRU problem for $n = 2^{12}$ in which we choose the subfield $\mathbb{L} \leq \mathbb{K}$ with $|\mathbb{K} : \mathbb{L}| = r$ and $\log(r) = 3$ according to (6). Experimental results for $n = 2^9$ and $n = 2^{10}$ are shown in the Appendix.

5 Conclusion

In this work, we exploit technical results from Kirchner and Fouque [12] to reanalyze the subfield attack by Albrecht et al. [1] against the overstretched NTRU problem. We derives better choices of the subfields for which the attack is successful with smaller modulus. Our experiments show that our succeeded modulus is much smaller than that of Albrecht et al. [1]. However, with our choices of subfields, we have to work with lattices of higher dimensions (as twice as those of Albrecht et al.) and hence the attack takes longer. Our implementation results for the case $n = 2^{11}$ (with same choice of subfield) are close to that of Kirchner and Fouque [12] ($\log(q) = 72$ vs. $\log(q) = 70$), while for the case $n = 2^{12}$ (with different choice of subfield), we can break the NTRU problem with smaller modulus ($\log(q) = 120$ vs. $\log(q) = 144$). Whereas Kirchner and Fouque's method can break NTRU problem with smaller modulus q in some cases (e.g, $n = 2^{11}$), it does not guarantee to succeed with bigger q, in contrast to the subfield attack which gives the exact limit of success. Recently, Cheon et al. [5] proposed an

Table 2. Implementation results for $n = 2^{11}$ and $\log(r) = 2$. Here we work with lattices of dimension $2n' = 1024$. The third column rhf stands for root Hermite factor obtained from our experiments (cf. the constant c in Heuristic 6)

$\log(q)$	$\log(\|\|(f', g')\|\|)$	rhf	$\log(\|\|(x', y')\|\|)$	$\log(\|\|(x, y)\|\|)$	Is $\|\|(x, y)\\| \leq q^{3/4}$?
95	21.40	0.9925	36.37	36.75	Yes
94	21.19	0.9934	37.30	37.66	Yes
93	21.37	0.9933	36.61	36.90	Yes
92	21.20	0.9936	36.63	36.81	Yes
91	21.28	0.9938	36.44	36.66	Yes
90	21.34	0.9942	36.42	36.60	Yes
89	21.30	0.9944	36.33	36.47	Yes
88	21.27	0.9949	36.49	36.55	Yes
87	21.35	0.9952	36.45	36.57	Yes
86	21.12	0.9959	37.05	37.24	Yes
85	21.17	0.9958	36.35	36.61	Yes
84	21.24	0.9962	36.42	36.78	Yes
83	21.15	0.9966	36.54	36.63	Yes
82	21.27	0.9973	37.11	37.28	Yes
81	21.26	0.9971	36.29	36.53	Yes
80	21.26	0.9979	37.00	37.13	Yes
79	21.18	0.9978	36.31	36.45	Yes
78	21.53	0.9983	36.56	36.75	Yes
77	21.22	0.9989	36.92	37.18	Yes
76	21.30	0.9992	36.87	37.17	Yes
75	21.28	0.9992	36.46	36.66	Yes
74	21.12	0.9996	36.42	36.49	Yes
73	21.45	1.0003	36.97	37.03	Yes
72	21.33	1.0005	36.80	36.92	Yes
71	21.27	1.0223	68.17	74.70	No
70	21.33	1.0225	67.89	73.70	No

attack against overstretched NTRU problem which exploits the existence of the sublattice in the NTRU lattice similar to that of Kirchner and Fouque. Their attack can apply for NTRU problem with general modulus polynomial $\phi(x)$ and they also give an improved subfield attack. One of our future work is to give a complete comparison between those attacks against overstretched NTRU problem.

Acknowledgments

We are grateful for the anonymous reviewers for their useful comments and suggestions. The first author would like to thank Martin Albrecht, Shi Bai and Paul Kirchner, for their kindness and helpful discussions. This work was supported by JST CREST Grant Number JPMJCR14D6, Japan. The first author thanks the Japanese Society for the Promotion of Science (JSPS) for financial support under grant KAKENHI 16K17644.

Table 3. Implementation results for $n = 2^{12}$ and $\log(r) = 3$. Here we work with lattices of dimension $2n' = 1024$

$\log(q)$	$\log(\|(f', g')\|)$	rhf	$\log(\|(x', y')\|)$	$\log(\|(x, y)\|)$	Is $\|(x, y)\| \leq q^{3/4}$?
150	46.31	0.9898	59.88	60.35	Yes
149	45.71	0.9903	60.12	60.62	Yes
148	46.11	0.9951	59.75	60.25	Yes
147	46.22	0.9910	60.23	60.82	Yes
146	46.91	0.9913	60.13	60.56	Yes
145	45.47	0.9914	59.81	60.48	Yes
144	46.11	0.9918	59.97	60.28	Yes
143	45.79	0.9921	59.84	60.22	Yes
142	45.87	0.9924	59.84	60.22	Yes
141	45.55	0.9929	60.05	60.51	Yes
140	46.20	0.9934	60.31	60.58	Yes
135	46.45	0.9948	59.88	60.28	Yes
130	46.26	0.9965	59.82	60.36	Yes
125	45.90	0.9984	60.14	60.42	Yes
120	45.77	0.9998	59.83	60.17	Yes
115	46.34	1.0225	90.41	119.21	No
100	45.87	1.0224	82.81	104.21	No

References

1. Martin Albrecht, Shi Bai and Léo Ducas. "A subfield lattice attack on overstretched NTRU assumptions - Cryptanalysis of some FHE and Graded Encoding Schemes", Advances in Cryptology – CRYPTO 2016, volume 9814 of LNCS, pp. 153–178, Springer 2016.
2. Wojciech Banaszczyk, "New bounds in some transference theorems in the geometry of numbers", Mathematische Annalen, volume 296, issue 1, pages 625–635, 1993.
3. Joppe W. Bos, Kristin Lauter, Jake Loftus and Michael Naehrig. "Improved Security for a Ring-Based Fully Homomorphic Encryption Scheme". In: Stam M. (eds) Cryptography and Coding – IMACC 2013, volume 8308 of LNCS, pp. 45–64, Springer 2013
4. Jung Hee Cheon, Jinhyuck Jeong and Changmin Lee. "An algorithm for NTRU problems and cryptanalysis of the GGH multilinear map without an encoding of zero", ANTS XII 2016, LMS J. Comput. Math. 19 (Special issue A), pp. 255-266, 2016.
5. Jung Hee Cheon, Minki Hhan and Changmin Lee, "Cryptanalysis of the overstretched NTRU problem for general modulus polynomial", ePrint 2017/484, available from `https://eprint.iacr.org/2017/484`
6. Don Coppersmith and Adi Shamir. "Lattice attacks on NTRU", Advances in Cryptology – EUROCRYPT 1997, volume 1233 of LNCS, pages 52–61, Springer 1997.
7. Nicolas Gama and Phong Q. Nguyen. "Predicting lattice reduction", Advances in Cryptology – CRYPTO 2008, volume 4965 of LNCS, pp. 31–51, Springer 2008.
8. Sanjam Garg, Craig Gentry and Shai Halevi. "Candidate Multilinear Maps from Ideal Lattices". Advances in Cryptology – EUROCRYPT 2013, volume 7881 of LNCS, pp. 1–17, Springer 2013.

9. Craig Gentry and Michael Szydlo, "Cryptanalysis of the revised NTRU signature scheme", Advances in Cryptology – EUROCRYPTO 2002, volume 2332 of LNCS, pp. 299–320, Springer 2002
10. Jeffrey Hoffstein, Jill Pipher, John M. Schanck, Joseph H. Silverman, William Whyte and Zhenfei Zhang. "Choosing parameters for NTRUEncrypt". Topics in Cryptology CT-RSA 2017, volume 10159 of LNCS, pp. 3–18, Springer 2017.
11. Jeffrey Hoffstein, Jill Pipher and Joseph H. Silverman. "NTRU: a ring-based public key cryptosystem". In *Algorithmic number theory*, pp. 267–288, Springer 1998.
12. Paul Kirchner and Pierre-Alain Fouque. "Revisiting Lattice Attacks on Overstretched NTRU Parameters", Advances in Cryptology – EUROCRYPTO 2017, volume 10210 of LNCS, pp. 3–26, Springer 2017.
13. Adriana López-Alt, Eran Tromer and Vinod Vaikuntanathan . "On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption". In *Proceedings of the forty-fourth annual ACM symposium on Theory of computing* – STOC 2012, pp. 1219–1234. ACM 2012
14. Vadim Lyubashevsky and Daniele Micciancio. "Generalized compact knapsacks are collision resistant", International Colloquium on Automata, Languages and Programming – ICALP 2006, volume 4052 of LNCS, pp. 144–155, Springer 2006
15. Damien Stehlé and Ron Steinfeld. "Making NTRUEncrypt and NTRUSign as secure as worst-case problems over ideal lattices". Advances in Cryptology – EUROCRYPT 2011, volume 6632 of LNCS, pp. 27–47, Springer 2011.

Appendix

Table 4 and Table 5 show implementation results for the case $n = 2^9$ and $n = 2^{10}$ respectively, with the same choice of subfield $\mathbb{L}$ such that $|\mathbb{K} : \mathbb{L}| = 4$.

Table 4. Implementation results for $n = 2^9$ and $\log(r) = 2$

$\log(q)$	$\log(\|(f', g')\|)$	rhf	$\log(\|(x', y')\|)$	$\log(\|(x, y)\|)$	Is $\|(x, y)\| \leq q^{3/4}$?
44	17.07	0.9950	20.16	20.39	Yes
43	17.11	0.9960	20.03	20.40	Yes
42	17.19	0.9978	20.22	20.34	Yes
41	17.15	0.9997	20.40	20.63	Yes
40	17.18	0.9996	19.85	20.14	Yes
39	17.12	1.0228	27.83	41.71	No
38	17.21	1.0215	26.87	40.67	No

Table 5. Implementation results for $n = 2^{10}$ and $\log(r) = 2$

$\log(q)$	$\log(\|\|(f', g')\|\|)$	rhf	$\log(\|\|(x', y')\|\|)$	$\log(\|\|(x, y)\|\|)$	Is $\|\|(x, y)\|\| \leq q^{3/4}$?
63	19.31	0.9926	26.07	26.23	Yes
62	19.24	0.9931	25.95	26.09	Yes
61	19.15	0.9942	26.27	26.43	Yes
60	19.14	0.9943	25.85	26.09	Yes
59	19.31	0.9955	26.23	26.58	Yes
58	19.46	0.9964	26.38	26.61	Yes
57	19.21	0.9965	25.95	26.37	Yes
56	19.14	0.9976	26.24	26.50	Yes
55	19.40	0.9982	26.22	26.48	Yes
54	19.19	0.9988	26.16	26.24	Yes
53	19.09	0.9996	26.21	26.49	Yes
52	19.08	1.0000	26.05	26.22	Yes
51	19.22	1.0223	41.83	54.24	No
50	19.43	1.0221	41.15	53.19	No