

An algorithm for NTRU problems and cryptanalysis of the GGH multilinear map without a low-level encoding of zero

Jung Hee Cheon, Jinhyuck Jeong and Changmin Lee

ABSTRACT

Let \mathbf{f} and \mathbf{g} be polynomials of a bounded Euclidean norm in the ring $\mathbb{Z}[X]/\langle X^n + 1 \rangle$. Given the polynomial $[\mathbf{f}/\mathbf{g}]_q \in \mathbb{Z}_q[X]/\langle X^n + 1 \rangle$, the NTRU problem is to find $\mathbf{a}, \mathbf{b} \in \mathbb{Z}[X]/\langle X^n + 1 \rangle$ with a small Euclidean norm such that $[\mathbf{a}/\mathbf{b}]_q = [\mathbf{f}/\mathbf{g}]_q$. We propose an algorithm to solve the NTRU problem, which runs in $2^{O(\log^2 \lambda)}$ time when $\|\mathbf{g}\|, \|\mathbf{f}\|$, and $\|\mathbf{g}^{-1}\|$ are within some range. The main technique of our algorithm is the reduction of a problem on a field to one on a subfield. The GGH scheme, the first candidate of an (approximate) multilinear map, was recently found to be insecure by the Hu–Jia attack using low-level encodings of zero, but no polynomial-time attack was known without them. In the GGH scheme without low-level encodings of zero, our algorithm can be directly applied to attack this scheme if we have some top-level encodings of zero and a known pair of plaintext and ciphertext. Using our algorithm, we can construct a level-0 encoding of zero and utilize it to attack a security ground of this scheme in the quasi-polynomial time of its security parameter using the parameters suggested by Garg, Gentry and Halevi [‘Candidate multilinear maps from ideal lattices’, *Advances in cryptology — EUROCRYPT 2013* (Springer, 2013) 1–17].

1. Introduction

The NTRU problem is to find a pair of polynomials with small coefficients whose ratio matches a given ratio of two polynomials with small coefficients [17]. Since the introduction of the security of the public-key encryption scheme NTRU, it has been assumed that this NTRU problem is difficult to solve, the so-called NTRU assumption, and NTRU has been used for the security grounding of various cryptographic schemes such as signature schemes [11, 16], fully homomorphic encryption schemes [5, 20], and candidates for cryptographic multilinear maps [3, 12, 19]. As it has not been broken until now, the NTRU assumption has received more and more attention as a candidate for post-quantum public-key cryptosystems. A variant of NTRU problem can be stated as follows.

PROBLEM 1 (A variant of the NTRU problem). Let $\phi_n(X) \in \mathbb{Z}[X]$ be a polynomial of degree n , $q \in \mathbb{Z}$ be an integer, and D, N , and B be real numbers. The NTRU problem $NTRU_{\phi_n, q, D, N, B}$ is to find $\mathbf{a}, \mathbf{b} \in R := \mathbb{Z}[X]/\langle \phi_n(X) \rangle$ with a Euclidean norm smaller than B such that $[\mathbf{b}/\mathbf{a}]_q = \mathbf{h}$ for a given polynomial $\mathbf{h} = [\mathbf{f}/\mathbf{g}]_q$, where \mathbf{f} and \mathbf{g} are sampled from R and have Euclidean norms bounded by D and N , respectively.

In the original NTRU problem, \mathbf{f} and \mathbf{g} are sampled from some distribution of R [17, § 1][†]. We consider this variant version to attack multilinear maps [12].

Received 22 February 2016.

2010 Mathematics Subject Classification 11Y16 (primary), 68Q25, 68W40 (secondary).

Contributed to the Twelfth Algorithmic Number Theory Symposium (ANTS-XII), Kaiserslautern, Germany, 29 August–2 September 2016.

[†] \mathbf{f} and \mathbf{g} are sampled to satisfy that $\mathbf{f} = p\mathbf{f}'$ and $\mathbf{g} - 1 = p\mathbf{g}'$ for a small integer p and the polynomials \mathbf{f}' and \mathbf{g}' in R with the coefficients in $\{-1, 0, 1\}$.

In this paper, we propose a polynomial-time reduction from $NTRU_{\phi_n, q, D, N, B}$ into $NTRU_{\phi_n/2, q, D_1, N_1, B_1}$, where $\phi_n = X^n + 1$, $B = \min\{q/2D\sqrt{n}, q/2N\sqrt{n}\}$, $D_1 = D^2\sqrt{n}/2$, $N_1 = 2ND\sqrt{n}/2$, and $B_1 = \min\{q/2D_t\sqrt{n}, q/2N_t\sqrt{n}, q/2nN^2\|\mathbf{g}^{-1}\|\sqrt{n}\}$ for a power n of 2. Our algorithm is to reduce the problem defined over a ring $\mathbb{Z}[X]/\langle X^n + 1 \rangle$ to one over a subring $\mathbb{Z}[X]/\langle X^{n/2} + 1 \rangle$. After repeated applications, we then use lattice reduction algorithms to find a short element. Since the latter has a smaller dimension, lattice reduction algorithms require a lower running time to produce a short element, which results in an algorithm for the NTRU problem. The algorithm runs in $2^{O(\log^2 \lambda)}$ time when $\|\mathbf{g}\|$, $\|\mathbf{f}\|$, and $\|\mathbf{g}^{-1}\|$ are within some range. For example, when $n = \lambda^2$ and $\log q = \lambda$, the running time is quasi-polynomial in λ . However, when $n = \lambda^3$ and $\log q = \lambda$, the running time is still exponential in λ . As an application of our work, we propose an attack of GGH multilinear maps [12] without any low-level encodings of zero. GGH maps were proposed by Garg *et al.* and broken by a so-called zeroizing attack by Hu and Jia [18]. Since their attack extensively utilizes low-level encodings of zero, it does not work without them, and no polynomial-time attack was known without them until recently (refer to the ‘related work’ subsection for the concurrent and independent works on this problem). Our algorithm can be directly applied to construct a level-0 encoding of zero, even when we are not given any low-level encodings of zero. We can then utilize them to attack the GGH scheme without low-level encodings of zero in the polynomial time of its security parameter. Our GGH attack requires a known pair of plaintext and ciphertext, some top-level encodings of zero, and the public parameters.

Technical overview. A natural approach for the NTRU problem is to convert it into a shortest vector problem (SVP) on an ideal lattice. Let $\phi_n(X) = X^n + 1$ when n is a power of 2. For any polynomial $\mathbf{h} = [\mathbf{f}/\mathbf{g}]_q = \sum_{i=0}^{n-1} h_i X^i \in R := \mathbb{Z}[X]/\langle X^n + 1 \rangle$, one may consider it as a vector $(h_0, \dots, h_{n-1})^T$. Then, the product $\mathbf{g}\mathbf{h} = \sum_{i=0}^{n-1} g_i X^i \mathbf{h}$ of the two polynomials \mathbf{h} and \mathbf{g} in R is contained in the lattice $\mathcal{M}_{\mathbf{h}}$ generated by $\{\mathbf{h}, X\mathbf{h}, \dots, X^{n-1}\mathbf{h}\}$. We aim to obtain an element $\tilde{\mathbf{g}} \in \mathbb{Z}[X]/\langle \phi(X) \rangle$ such that $\|\tilde{\mathbf{g}}\|$ and $\|[\tilde{\mathbf{g}}\mathbf{h}]_q\|$ are small. To obtain such a $\tilde{\mathbf{g}} \in \mathbb{Z}[X]/\langle \phi(X) \rangle$, one can naturally contemplate the column lattice

$$\Lambda_{\mathbf{h}} = \begin{pmatrix} I & 0 \\ M_{\mathbf{h}} & qI \end{pmatrix},$$

where I is the identity matrix of size n , and $M_{\mathbf{h}}$ is a basis matrix of $\mathcal{M}_{\mathbf{h}}$ juxtaposed by $\{\mathbf{h}, X\mathbf{h}, \dots, X^{n-1}\mathbf{h}\}$. Given a lattice vector $\mathbf{u} = (u_0, \dots, u_{2n-1})^T$ of Λ_f satisfying $|u_i| < q/2$ for $n \leq i \leq 2n - 1$, we take $\mathbf{g}' = \sum_{i=0}^{n-1} u_i X^i$ and $\mathbf{f}' = \sum_{i=0}^{n-1} u_{n+i} X^i$ so that $\mathbf{f}' = [\mathbf{g}'\mathbf{h}]_q$ and $\mathbf{h} = [\mathbf{f}'/\mathbf{g}']_q$. Therefore, if one can find a small lattice point \mathbf{u} such that $\sqrt{\sum_{i=0}^{n-1} u_i^2} \leq q/2\|\mathbf{f}\|\sqrt{n}$ and $\sqrt{\sum_{i=n}^{2n-1} u_i^2} \leq q/2\|\mathbf{g}\|\sqrt{n}$, it becomes a solution of $NTRU_{\phi, q, D, N, B}$. However, the dimension $2n$ of the lattice is too large for most applications, which is the origin of the difficulty of the NTRU problem. To overcome this obstacle, we consider a subfield K_m of $K_0 := \mathbb{Q}[X]/\langle X^n + 1 \rangle$ with the extension degree m and the trace of $f \in K_0$ over K_m :

$$\text{Tr}(\mathbf{h}) = \left[\sum_{i=1}^m \sigma_i(\mathbf{h}) \right]_q = \left[\sum_{i=1}^m \left(\sigma_i(\mathbf{f}) \prod_{j \neq i} \sigma_j(\mathbf{g}) \right) / \prod_{i=1}^m \sigma_i(\mathbf{g}) \right]_q.$$

Since the numerator and denominator are elements in K_m bounded by $m\|\mathbf{f}\| \cdot \|\mathbf{g}\|^{m-1}n^m$ and $\|\mathbf{g}\|^m n^m$, respectively, if they are smaller than q , we can construct another instance of the NTRU problem on K_m where the dimension of $\Lambda_{\text{Tr}(\mathbf{h})}$ is that of $\Lambda_{\mathbf{h}}$ divided by m . By optimizing m such that finding a small vector on the reduced lattice is possible with the BKZ algorithm, one can reach our results.

Multilinear maps. Since Boneh and Silverberg [4] suggested the concept of cryptographic multilinear maps and their applications such as multipartite Diffie–Hellman and efficient broadcast encryption in 2002, the construction of cryptographic multilinear maps has been a long-standing open question. In 2013, approximate cryptographic multilinear maps were first proposed by Garg, Gentry, and Halevi (GGH) [12]. Soon after, cryptographic multilinear maps were also suggested by Coron, Lepoint, and Tibouchi (CLT) [9], and Gentry, Gorbunov, and Halevi [13]. However, none of these maps have a reduction to a standard difficulty problem such as the subset sum problem. In fact, the first two schemes with low-level encodings of zero are known to be insecure [6, 18] via the so-called zeroizing attack. The last candidate has also been broken [8]. Although the fixed scheme of [9] was proposed by the same authors of [10] to resist the zeroizing attack against the CLT scheme, it was also shown to be insecure [7]. On the other hand, both the [12] and [9] schemes without any encodings of zero, which are used as basic tools for constructing applications such as indistinguishable obfuscations, have still not been analyzed.

Related work. In 2002, a technique was suggested to reduce the dimension of an ideal lattice by Gentry and Szydło [14]. They consider a subring of a given ring $\mathbb{Z}[X]/\langle X^n - 1 \rangle$ consisting of the fixed elements by the ring automorphism $\sigma : X \mapsto X^{n-1}$. There is, however, no guarantee that one can apply this technique repeatedly to reduce the dimension more efficiently.

For GGH multilinear maps without encodings of zero, two more concurrent and independent cryptanalytic works have recently been announced simultaneously, which can overcome the previous flaw: one by Albrecht, Bai and Ducas [2] and the other by Miles, Sahai, and Zhandry [21]. The first introduces a very similar reduction from $NTRU_{\phi_n, q, D, N, B}$ to $NTRU_{\phi_{n/2}, q, D_1, N_1, B_1}$. Albrecht *et al.* provided a rich analysis of the NTRU-like homomorphic encryptions LTV [20] and YASHE [5] and GGH multilinear maps with some implementations. Using the norm function instead of the trace function in our algorithm, they proposed a quantum-polynomial-time or subexponential-time attack on GGH without low-level encodings of zero. In our work, we can achieve the same, but slightly better, results using the trace function. Moreover, through our new approach, we can obtain an algorithm to attack GGH scheme without low-level encodings of zero in quasi-polynomial time.

The second introduced a polynomial-time attack algorithm against the GGH multilinear maps, the so-called *annihilation attack*. Using nonlinear polynomials, it also leads to a polynomial-time break of the GGH scheme without low-level encodings of zero.

Organization. In §2 we introduce some notation and preliminary information related to ideal theory and Galois theory. In §3 we state some useful properties and their proofs used to solve the *NTRU* problem. In §4 we briefly explain the GGH scheme and present our algorithm for attacking the GGH scheme using our theorem.

2. Preliminaries

Notation. For an integer q , we use the notation $\mathbb{Z}_q := \mathbb{Z}/(q\mathbb{Z})$ and $[R]_q := \mathbb{Z}_q[X]/\langle X^n + 1 \rangle = R/qR$. We denote the number in \mathbb{Z}_q within the range $(-q/2, q/2]$ by $(x \bmod q)$ or $[x]_q$, which is congruent to x modulo q . For $\mathbf{u} = \sum_{i=0}^{n-1} u_i X^i \in R$, $[\mathbf{u}]_q = \sum_{i=0}^{n-1} [u_i]_q X^i$ and $\|\mathbf{u}\|$ denote the Euclidean norm of \mathbf{u} .

We define $\iota : \mathbb{Z}_q \rightarrow \mathbb{Z}$ by $[x]_q \in \mathbb{Z}_q \mapsto x \in \mathbb{Z}$ for $-q/2 < x \leq q/2$. We extend this map to $[R]_q$ by applying it to each coefficient. In an abuse of notation, we omit ι unless it will be confused when identifying $[x]_q \in \mathbb{Z}_q$ with an integer x when $-q/2 < x \leq q/2$.

Throughout this paper, we assume that an integer n is a power of 2. Then, $K := \mathbb{Q}[X]/\langle X^n + 1 \rangle$ is a number field with the ring of integers $R := \mathbb{Z}[X]/\langle X^n + 1 \rangle$. In particular, K is a Galois extension of \mathbb{Q} , and we denote the Galois group of K over \mathbb{Q} by $\text{Gal}(K/\mathbb{Q})$.

As in the technical overview, we consider any polynomial $\mathbf{h} = \sum_{i=0}^{n-1} h_i X^i \in K$ to be a column vector $(h_0, \dots, h_{n-1})^T$. When we need an inverse of an element $\mathbf{a} \in R$, we usually consider the inverse in K with the notation \mathbf{a}^{-1} . If we want to consider it in $[R]_q$ and not in K , then we denote it by $[\mathbf{a}^{-1}]_q$. We use bold letters to denote vectors or ring elements in \mathbb{Z}^n or R .

Ideal lattice. An n -dimension full-rank lattice $\mathcal{M} \subset \mathbb{R}^n$ is the set of all \mathbb{Z} -linear combinations of n linearly independent vectors. Let $\det(\mathcal{M})$ denote the determinant of the lattice \mathcal{M} . For an element $\mathbf{g} \in R$, we denote the principal ideal in R generated by \mathbf{g} by $\langle \mathbf{g} \rangle$, whose basis consists of $\{\mathbf{g}, X\mathbf{g}, \dots, X^{n-1}\mathbf{g}\}$. By identifying a polynomial $\mathbf{g} = \sum g_i X^i \in R$ with a vector $(g_{n-1}, g_{n-2}, \dots, g_0)^T$ in \mathbb{Z}^n , we can apply lattice theory to the algebraic ring R and algebraic ring theory to the ideal lattice $\langle \mathbf{g} \rangle$. For a polynomial $\mathbf{u} \in R$ and a basis $\mathcal{B} := \{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n\}$, we denote the reduction of \mathbf{u} modulo the fundamental region of lattice \mathcal{B} by $\mathbf{u} \bmod \mathcal{B}$; that is, $\mathbf{u} \bmod \mathcal{B}$ is the unique representation of $\mathbf{u} \in R$ such that $\mathbf{u} - (\mathbf{u} \bmod \mathcal{B}) \in \mathcal{B}$ and $\mathbf{u} \bmod \mathcal{B} = \sum_{i=0}^{n-1} \alpha_i \mathbf{b}_i$ for $\alpha_i \in (-1/2, 1/2]$. For the polynomials $\mathbf{u}, \mathbf{v} \in R$, we use the notation $\mathbf{u} \bmod \mathbf{v}$ as $\mathbf{u} \bmod \mathcal{V}$, where \mathcal{V} is a basis $\{\mathbf{v}, X\mathbf{v}, \dots, X^{n-1}\mathbf{v}\}$. By the definition of $\mathbf{u} \bmod \mathbf{v}$, it is of the form $\sum_{i=0}^{n-1} \alpha_i X^i \mathbf{v}$ for $\alpha_i \in (-1/2, 1/2]$. Hence, the size of its Euclidean norm is bounded by $\sum_{i=0}^{n-1} \|X^i \mathbf{v}\|/2 = \sum_{i=0}^{n-1} \|\mathbf{v}\|/2 = (n/2)\|\mathbf{v}\|$. Next, we introduce some useful lemmas related to ideal lattices.

LEMMA 1. For any $\mathbf{a}, \mathbf{b} \in R = \mathbb{Z}[X]/\langle X^n + 1 \rangle$, $\|\mathbf{ab}\| \leq \|\mathbf{a}\| \cdot \|\mathbf{b}\| \cdot \sqrt{n}$.

Proof. The k th coefficient of \mathbf{ab} is of the form $\sum_{i+j=k} a_i b_j - \sum_{i+j=n+k} a_i b_j$. By the Cauchy-Schwartz inequality, it is smaller than $\|\mathbf{a}\| \cdot \|\mathbf{b}\|$. Since each coefficient is smaller than $\|\mathbf{a}\| \cdot \|\mathbf{b}\|$, $\|\mathbf{ab}\| \leq \|\mathbf{a}\| \cdot \|\mathbf{b}\| \cdot \sqrt{n}$. □

LEMMA 2. Let \mathbf{g} be an element of $\mathbb{Z}[X]/\langle X^n + 1 \rangle$ and $\mathbf{f} \in \mathbb{Z}[X]/\langle X^n + 1 \rangle$ be a relative prime to \mathbf{g} . If $\mathbf{c} \in \mathbb{Z}[X]/\langle X^n + 1 \rangle$ satisfies $\|\mathbf{c}\| < q/(2\|\mathbf{f}\|\sqrt{n})$ and $\|[\mathbf{c} \cdot \mathbf{f} \cdot \mathbf{g}^{-1}]_q\| < q/(2\|\mathbf{g}\|\sqrt{n})$, then \mathbf{c} is contained in the ideal $\langle \mathbf{g} \rangle$.

Proof. Let $\mathbf{w} := [\mathbf{c} \cdot \mathbf{f} \cdot \mathbf{g}^{-1}]_q$. Then $[\mathbf{gw}]_q = [\mathbf{cf}]_q$. Since $\|\mathbf{w}\| < q/(2\|\mathbf{g}\|\sqrt{n})$, we have $\|\mathbf{gw}\| \leq \|\mathbf{g}\| \cdot \|\mathbf{w}\| \cdot \sqrt{n} \leq q/2$ and $\|\mathbf{cf}\| \leq \|\mathbf{c}\| \cdot \|\mathbf{f}\| \cdot \sqrt{n} \leq q/2$. Therefore, $\mathbf{gw} = \mathbf{cf}$ in $\mathbb{Z}[X]/\langle X^n + 1 \rangle$. Because $\mathbf{cf} \in \langle \mathbf{g} \rangle$ and \mathbf{f} is a relative prime to \mathbf{g} , we can conclude $\mathbf{c} \in \langle \mathbf{g} \rangle$. □

Using Lemma 2, if one can find \mathbf{c} that satisfies Lemma 2, \mathbf{c} is of the form $\mathbf{c} = \mathbf{dg}$ for some small $\mathbf{d} \in \mathbb{Z}[X]/\langle X^n + 1 \rangle$. Then, by multiplying it by $[\mathbf{fg}^{-1}]_q$, one can obtain a small multiple of \mathbf{f} , \mathbf{df} . Hence, \mathbf{df} and \mathbf{dg} become a solution of the NTRU problem.

Gaussian distribution. Given $\sigma > 0$, the discrete Gaussian distribution over the set L with zero mean is defined as $\mathcal{D}_{L,\sigma}(x) = \rho_\sigma(x)/\rho_\sigma(L)$ for any $x \in L$, where $\rho_\sigma(x) = \exp(-\pi\|x\|^2/\sigma^2)$ and $\rho_\sigma(L) = \sum_{x \in L} \rho_\sigma(x)$. We use the notation $a \leftarrow \mathcal{D}$ to denote the choice of an element a according to the distribution of \mathcal{D} .

Norm and trace of a field. For a finite extension K of a field F , the trace $\text{Tr}_{K/F}(\alpha)$ and norm $N_{K/F}(\alpha)$ of $\alpha \in K$ over F are defined as the trace and determinant of the linear transformation M_α that maps $x \in K$ to $\alpha x \in K$, respectively, that is, $\text{Tr}_{K/F}(\alpha) = \sum a_{i,i}$ and $N_{K/F}(\alpha) = \det(a_{i,j})$, where $a_{i,j}$ is the matrix for M_α with respect to any basis of K over F . For $\alpha, \beta \in K$ and $a \in F$, the map $\text{Tr}_{K/F}$ and $N_{K/F}$ satisfy the following properties:

- (1) $\text{Tr}_{K/F}(\alpha) = \sum_{\sigma \in \text{Gal}(K/F)} \sigma(\alpha)$ and $N_{K/F}(\alpha) = \prod_{\sigma \in \text{Gal}(K/F)} \sigma(\alpha)$ if K is a Galois extension of F ;
- (2) $\text{Tr}_{K/F}(\alpha + \beta) = \text{Tr}_{K/F}(\alpha) + \text{Tr}_{K/F}(\beta)$, $N_{K/F}(\alpha\beta) = N_{K/F}(\alpha)N_{K/F}(\beta)$;
- (3) $\text{Tr}_{K/F}(a \cdot \alpha) = a \cdot \text{Tr}_{K/F}(\alpha)$, $N_{K/F}(a \cdot \alpha) = a^{[K:F]} \cdot N_{K/F}(\alpha)$;
- (4) $\text{Tr}_{K/F}(a) = [K : F] \cdot a$, $N_{K/F}(a) = a^{[K:F]}$.

3. Main theorem

In this section, we discuss how the NTRU problem with a given input $[\mathbf{f}/\mathbf{g}]_q$ is reduced to the NTRU problem with an input whose denominator and numerator have half of the degree of \mathbf{f} and \mathbf{g} . Throughout this section, let $n = 2^s$ and denote $\mathbb{Q}[X^{2^t}]/\langle X^n + 1 \rangle$ and $\mathbb{Z}[X^{2^t}]/\langle X^n + 1 \rangle$ by K_t and R_t , respectively, with $0 \leq t \leq s$. Note that $K_s := \mathbb{Q} \leq K_{s-1} \leq \dots \leq K_0 = \mathbb{Q}[X]/\langle X^n + 1 \rangle$, where $A \leq B$ denotes that A is a subfield of B . Since K_0 is a Galois extension field of K_1 with a degree of 2, $\text{Gal}(K_0/K_1)$ is a group of order 2. That is, $\text{Gal}(K_0/K_1) = \{\text{id}, \sigma\}$, satisfying $\sigma(X) = -X$; therefore, $\sigma^2 = \text{id}$, where id is the identity map. For an element $\mathbf{h}, \mathbf{g} \in R \subset K_0$, the following elements are contained in $R_1 \subset K_1$:

$$\begin{aligned} \text{Tr}_{K_0/K_1}(\mathbf{h}) &= \mathbf{h} + \sigma(\mathbf{h}), \\ N_{K_0/K_1}(\mathbf{h}) &= \mathbf{h} \cdot \sigma(\mathbf{h}), \\ \text{Tr}_{K_0/K_t}(\mathbf{h}\sigma(\mathbf{g})) &= \mathbf{h}\sigma(\mathbf{g}) + \sigma(\mathbf{h})\mathbf{g}, \end{aligned}$$

since they are fixed by $\text{Gal}(K_0/K_1)$. Note that these elements have only $n/2$ terms, and the last one lies in $2 \cdot R_1$. Generally, for $0 < t \leq s$, K_0 is a Galois extension field of K_t with a degree of 2^t and the Galois group $G_t := \text{Gal}(K_0/K_t) = \{\sigma_0 = \text{id}, \sigma_1, \dots, \sigma_{2^t-1}\}$. For an element $\mathbf{h}, \mathbf{g} \in R \subset K_0$, the following elements are contained in $R_t \subset K_t$:

$$\begin{aligned} \sum_{i=0}^{2^t-1} \sigma_i(\mathbf{h}) &= \mathbf{h} + \sigma_1(\mathbf{h}) + \dots + \sigma_{2^t-1}(\mathbf{h}), \\ \prod_{i=0}^{2^t-1} \sigma_i(\mathbf{h}) &= \mathbf{h} \cdot \sigma_1(\mathbf{h}) \cdot \dots \cdot \sigma_{2^t-1}(\mathbf{h}), \\ \text{Tr}_{K_0/K_t}(\mathbf{h}\sigma_1(\mathbf{g})\sigma_2(\mathbf{g}) \dots \sigma_{2^t-1}(\mathbf{g})), & \end{aligned}$$

since they are fixed by $\text{Gal}(K_0/K_t)$. Moreover, these elements have only $n/2^t$ terms, and the last one lies in $2^t \cdot R_t$. Using this property, we can obtain the following theorem, which is the main theorem of this paper.

THEOREM 1. *Let q and $m \in \mathbb{Z}$ be integers and let D and N be positive real numbers. Set $B = \min\{q/2D\sqrt{n}, q/2N\sqrt{n}\}$. Then, for $\phi_n(X) = X^n + 1$ with $n = 2^s$ and $0 < t \leq s$, we can reduce $\text{NTRU}_{\phi_n, q, D, N, B}$ to $\text{NTRU}_{\phi_{n/2^t}, q, D_t, N_t, B_t}$, where $B_t = \min\{q/2D_t\sqrt{n}, q/2N_t\sqrt{n}, q/2nN^2\|\mathbf{g}^{-1}\|\sqrt{n}\}$, $D_t = D^{2^t} \prod_{j=1}^t \sqrt{n/2^j}$, and $N_t = ND^{2^t-1} \prod_{j=1}^t \sqrt{n/2^j}$.*

Proof. Suppose we are given $[\mathbf{f}/\mathbf{g}]_q$, where \mathbf{g} and \mathbf{f} are sampled from the set $\{(\mathbf{g}, \mathbf{f}) \in R^2 = (\mathbb{Z}[X]/\langle \phi_n(X) \rangle)^2 : \|\mathbf{f}\| < N, \|\mathbf{g}\| < D\}$. We consider the useful element

$$\text{Tr}_{K_0/K_t} \left(\frac{\mathbf{f}}{\mathbf{g}} \right) = \frac{\mathbf{f}}{\mathbf{g}} + \sigma_1 \left(\frac{\mathbf{f}}{\mathbf{g}} \right) + \dots + \sigma_{2^t-1} \left(\frac{\mathbf{f}}{\mathbf{g}} \right) = \frac{\text{Tr}_{K_0/K_t}(\mathbf{f}\sigma_1(\mathbf{g})\sigma_2(\mathbf{g}) \dots \sigma_{2^t-1}(\mathbf{g}))}{\prod_{i=0}^{2^t-1} \sigma_i(\mathbf{g})}$$

in K_t which satisfies

- $\prod_{i=0}^{2^t-1} \sigma_i(\mathbf{g}) \in R_t$, and $\text{Tr}_{K_0/K_t}(\mathbf{f}\sigma_1(\mathbf{g})\sigma_2(\mathbf{g}) \dots \sigma_{2^t-1}(\mathbf{g})) \in 2^t \cdot R_t$;
- $\|\text{Tr}_{K_0/K_t}(\mathbf{f}\sigma_1(\mathbf{g})\sigma_2(\mathbf{g}) \dots \sigma_{2^t-1}(\mathbf{g}))/2^t\| \leq ND^{2^t-1} \prod_{j=1}^t \sqrt{n/2^j}$;
- $\|\prod_{i=0}^{2^t-1} \sigma_i(\mathbf{g})\| \leq D^{2^t} \prod_{j=1}^t \sqrt{n/2^j}$.

Therefore, we can see that $[(\text{Tr}_{K_0/K_t}(\mathbf{f}\sigma_1(\mathbf{g})\sigma_2(\mathbf{g})\dots\sigma_{2^t-1}(\mathbf{g}))/2^t)/\prod_{i=0}^{2^t-1}\sigma_i(\mathbf{g})]_q$ is a new instance of $NTRU_{\phi_{n/2^t},q,D_t,N_t,B_t}$, where $D_t = D^{2^t} \prod_{j=1}^t \sqrt{n/2^j}$, $N_t = ND^{2^t-1} \prod_{j=1}^t \sqrt{n/2^j}$, and $B_t = \min\{q/2D_t\sqrt{n}, q/2N_t\sqrt{n}, q/2nN^2\|\mathbf{g}^{-1}\|\sqrt{n}\}$. Now, suppose that a solution $(\mathbf{a}_t, \mathbf{b}_t) \in R_t$ of $NTRU_{\phi_{n/2^t},q,D_t,N_t,B_t}$ is known such that $[\mathbf{b}_t/\mathbf{a}_t]_q = [(\text{Tr}_{K_0/K_t}(\mathbf{f}\sigma_1(\mathbf{g})\sigma_2(\mathbf{g})\dots\sigma_{2^t-1}(\mathbf{g}))/2^t)/\prod_{i=0}^{2^t-1}\sigma_i(\mathbf{g})]_q$. Moreover, since \mathbf{g} and \mathbf{f} are relative primes with a high probability [2], we assume the coprimality of \mathbf{g} and \mathbf{f} . Then, by Lemma 2, \mathbf{a}_t is of the form $\mathbf{a}_t = \mathbf{d} \prod_{i=0}^{2^t-1} \sigma_i(\mathbf{g})$. After computing $[\mathbf{a}_t \cdot \mathbf{h}]_q = [\mathbf{d} \prod_{i=0}^{2^t-1} \sigma_i(\mathbf{g}) \cdot [\mathbf{f}/\mathbf{g}]_q]_q = [\mathbf{d}\mathbf{f} \prod_{i=0}^{2^t-1} \sigma_i(\mathbf{g})]_q$, set $\mathbf{a} = \mathbf{a}_t$ and $\mathbf{b} = [\mathbf{d}\mathbf{f} \prod_{i=1}^{2^t-1} \sigma_i(\mathbf{g})]_q$. Then, we can conclude that the pair (\mathbf{a}, \mathbf{b}) is a solution of $NTRU_{\phi_n,q,D,N,B}$ with following properties:

$$\begin{aligned} [\mathbf{b}/\mathbf{a}]_q &= [\mathbf{f}/\mathbf{g}]_q, \\ \|\mathbf{a}\| &\leq \frac{q}{2N_t\sqrt{n}} \leq \frac{q}{2N\sqrt{n}}, \\ \left\| \mathbf{d}\mathbf{f} \prod_{i=1}^{2^t-1} \sigma_i(\mathbf{g}) \right\| &= \left\| \mathbf{d}\mathbf{g}^{-1}\mathbf{f} \prod_{i=0}^{2^t-1} \sigma_i(\mathbf{g}) \right\| \leq \|\mathbf{a}_t\| \cdot \|\mathbf{g}^{-1}\| \cdot \|\mathbf{f}\| \cdot n \\ &< \frac{q}{2nN^2\|\mathbf{g}^{-1}\|\sqrt{n}} \cdot \|\mathbf{g}^{-1}\| \cdot N \cdot n \\ &= \frac{q}{2N\sqrt{n}}. \end{aligned}$$

The last inequality implies that $\mathbf{b} = [\mathbf{d}\mathbf{f} \prod_{i=1}^{2^t-1} \sigma_i(\mathbf{g})]_q$ is actually $\mathbf{b} = \mathbf{d}\mathbf{f} \prod_{i=1}^{2^t-1} \sigma_i(\mathbf{g})$ in R . Thus, we obtain the desired result. \square

Comparing with [2], our result works better when $N \geq D$ because the value of our N_1 is smaller than that of [2] while the values of D_1 are same.

THEOREM 2. *Let q be an integer, n a power of 2, and λ the security parameter. Let $\mathbf{h} = [\mathbf{f}/\mathbf{g}]_q$ be an instance of the $NTRU_{\phi_n,q,D,N,B}$ problem with the parameters $\log q = c_1 \cdot \lambda^\ell$, $n \leq c_2 \cdot \lambda^{2\ell}$, $N = q^a$, $0 < a < 1/2$, $D = \lambda^k < N$, $\phi_n(X) = X^n + 1$, and $B = \min\{q/2D\sqrt{n}, q/2N\sqrt{n}\}$. For $\beta > 0$ and $t \in \mathbb{Z}$, if*

$$2\beta^{n_t/2(\beta-1)+3/2}\sqrt{q} \leq B_t,$$

where $D_t = D^{2^t} \prod_{j=1}^t \sqrt{n/2^j}$, $N_t = ND^{2^t-1} \prod_{j=1}^t \sqrt{n/2^j}$, $B_t = \min\{q/2D_t\sqrt{n}, q/2N_t\sqrt{n}, q/2nN^2\|\mathbf{g}^{-1}\|\sqrt{n}\}$, and $n_t = n/2^t$, then the problem is solved in $2^{O(\beta)}$ time.

In particular, if $\|\mathbf{g}^{-1}\| \leq D^{2^t-1}/N \cdot \sqrt{n}^{t-2} \cdot 2^{t(t+1)/4}$ and $\beta = \log^2 \lambda$, the problem is solved in $2^{O(\log^2 \lambda)}$ time[†].

For example, when $n = \lambda^2$, $D = \lambda^2$, $N = q^{1/8}$, and $\log q = \lambda$, one can solve $NTRU_{\phi_n,q,D,N,B}$ in quasi-polynomial time in λ .

Proof. By Theorem 1, one can obtain a new instance $[\text{Tr}_{K/K_t}([\mathbf{f}/\mathbf{g}]_q)/2^t]_q \in [R]_q \cap R_t$ for $NTRU_{\phi_{n_t},q,N_t,D_t,B_t}$. We now consider the column lattice

$$\mathcal{M}_t = \begin{pmatrix} I_{n_t} & 0 \\ \Lambda_t & qI_{n_t} \end{pmatrix},$$

[†]If \mathbf{h} and \mathbf{g} are sampled from continuous spherical Gaussian distributions, we can obtain a bound of $\|\mathbf{g}^{-1}\|$ with a high probability [2, Lemma 3].

where I_{n_t} is the identity matrix with size $n_t = n/2^t$, and $\Lambda_t \in \mathbb{Z}^{n_t \times n_t}$ is a matrix whose i th column is $\iota(X^{i2^t} [\text{Tr}_{K/K_t}([\mathbf{f}/\mathbf{g}]_q)/2^t]_q)$ for $0 \leq i < n/2^t$. In other words, for $[\text{Tr}_{K/K_t}([\mathbf{f}/\mathbf{g}]_q)/2^t]_q = \sum_{j=0}^{n_t-1} h_j X^{j2^t}$, the i th column of Λ_t is of the form $(-h_{n_t-i}, \dots, -h_{n_t-1}, h_0, \dots, h_{n_t-i-1})^T$. Using the BKZ algorithm with a block size β , one can obtain an element in \mathcal{M}_t ,

$$\mathbf{u}_t = (u_0, \dots, u_{n_t-1}, u_{n_t}, \dots, u_{2n_t-1})^T,$$

with $\|\mathbf{u}_t\| \leq 2\beta^{(n_t-1)/2(\beta-1)+3/2} \det(\mathcal{M}_t)^{1/2n_t} = 2\beta^{(n_t-1)/2(\beta-1)+3/2} \sqrt{q}$ [15]. Taking $\mathbf{c} = \sum_{i=0}^{n_t-1} u_i X^{i2^t} \in \mathbb{Z}[X^{2^t}]/\langle X^n + 1 \rangle$, we then have $[\mathbf{c} \cdot \text{Tr}_{K/K_t}([\mathbf{f}/\mathbf{g}]_q)/2^t]_q = \sum_{i=0}^{n_t-1} u_{n_t+i} X^{i2^t} \in \mathbb{Z}[X^{2^t}]/\langle X^n + 1 \rangle$. Moreover, if we choose t such that

$$2\beta^{n_t/2(\beta-1)+3/2} \sqrt{q} \leq B_t, \tag{3.1}$$

then $\|\mathbf{c}\|$ and $\|\mathbf{c} \cdot \text{Tr}_{K/K_t}([\mathbf{f}/\mathbf{g}]_q)\|_q$ satisfy

$$\begin{aligned} \|\mathbf{c}\| &< \|\mathbf{u}_t\| \leq 2\beta^{(n_t-1)/2(\beta-1)+3/2} \sqrt{q} \leq B_t \leq \frac{q}{2N_t\sqrt{n}}, \\ \|\mathbf{c} \cdot \text{Tr}_{K/K_t}([\mathbf{f}/\mathbf{g}]_q)\|_q &< \|\mathbf{u}_t\| \leq 2\beta^{(n_t-1)/2(\beta-1)+3/2} \sqrt{q} \leq B_t \leq \frac{q}{2D_t\sqrt{n}}. \end{aligned}$$

In other words, \mathbf{c} satisfies the conditions of Lemma 2. Therefore, \mathbf{c} is in $\langle N_{K/K_t}(\mathbf{g}) \rangle \subset \langle \mathbf{g} \rangle$. Note that \mathbf{c} is of the form $\mathbf{c} = \mathbf{d} \cdot N_{K/K_t}(\mathbf{g}) = \mathbf{d}'\mathbf{g} \in R_t$ for some $\mathbf{d}, \mathbf{d}' \in R$. Hence, by Theorem 1, a pair $(\mathbf{c}, [\mathbf{c} \cdot \mathbf{h}]_q)$ is a solution of $NTRU_{\phi_n, q, N, D, B}$. The running time of this procedure is dominated by that of the BKZ algorithm with a block size β , which is $\text{poly}(n, \log q) \cdot \mathcal{C}_{HKZ}(\beta)$ time, where $\mathcal{C}_{HKZ}(\beta) = 2^{O(\beta)}$ is the cost of the HKZ reduction in the dimension β [1, 15]. When $\|\mathbf{g}^{-1}\| \leq D^{2^t-1}/N \cdot \sqrt{n}^{t-2} \cdot 2^{t(t+1)/4}$, we obtain $B_t = q/2N_t\sqrt{n}$. To check that the above condition for β and t is satisfied, we have the following equivalence equation:

$$2\beta^{n_t/2(\beta-1)+3/2} \sqrt{q} \leq \frac{q}{2N_t\sqrt{n}} \tag{3.2}$$

$$\Leftrightarrow \left(\frac{n_t}{2(\beta-1)} + \frac{3}{2} \right) \log \beta + \log D_t - \log D + \frac{\log n}{2} + 2 < \frac{\log q}{2} - \log N. \tag{3.3}$$

To optimize the left-hand side of the inequality, we choose t such that

$$t = \left\lceil \log \sqrt{\frac{n \log \beta}{2k(\beta-1) \log \lambda}} \right\rceil.$$

Then, the left-hand side is asymptotic to

$$\begin{aligned} \left(\frac{n_t}{2(\beta-1)} + \frac{3}{2} \right) \log \beta + \log D_t - \log D + \frac{\log n}{2} + 2 &\approx \frac{n}{2^t \cdot 2(\beta-1)} \log \beta + 2^t \log \lambda^k + O(1) \\ &\approx 2\sqrt{\frac{n \log \beta \log \lambda^k}{2(\beta-1)}} + O(1), \end{aligned}$$

where the last approximation originates from the arithmetic-geometric mean. This implies that if one chooses $\beta = \log^2 \lambda$, then the last value is asymptotically smaller than $(1/2 - a) \log q$. Hence, one can obtain the results. \square

4. Application to GGH

In this section, we explain an attack algorithm, which is a different approach from [2], to solve the graded computational Diffie–Hellman (GCDH) problem of the GGH scheme without low-level encodings of zero when we are given some top-level encodings of zero and a known pair of plaintext and ciphertext.

4.1. *GGH scheme*

First, we briefly recall the Garg *et al.* construction. We refer to the original paper [12] for a complete description. The scheme relies on the following parameters:

- λ , the security parameter;
- κ , the multilinearity parameter;
- q , the modulus of a ciphertext;
- n , the dimension of a base ring;
- m , the number of level- κ encodings of zero in the public parameters;
- σ , the basic Gaussian parameter for drawing the ideal generator \mathbf{g} ;
- σ' , the Gaussian parameter for sampling level-zero elements;
- σ^* , the Gaussian parameter for constructing elements of nonzero level.

Instance generation. $(\text{params}, \mathbf{p}_{zt}) \leftarrow \text{InstGen}(1^\lambda, 1^\kappa)$. For a given λ and κ , the parameters (σ, σ', q, n) that satisfy the above conditions are determined, and $(\text{params}, \mathbf{p}_{zt})$ is output.

- Sample $\mathbf{g} \leftarrow \mathcal{D}_{R, \sigma}$ until $\|\mathbf{g}\|, \|\mathbf{g}^{-1}\| \leq n^2$ and $\mathcal{I} = \langle \mathbf{g} \rangle$ is a prime ideal in R .
- Sample $\mathbf{z} \leftarrow [R]_q$.
- Sample $X = \{\mathbf{b}_i \mathbf{g}\} \leftarrow \mathcal{D}_{\mathcal{I}, \sigma'}$ and set a level- κ encoding of zero, $\mathbf{x}_i = \left[\frac{\mathbf{b}_i \mathbf{g}}{\mathbf{z}^\kappa} \right]_q$ for each $i \leq m$.
- Sample $\mathbf{f} \leftarrow \mathcal{D}_{R, \sqrt{q}}$ and set a zero-testing parameter $\mathbf{p}_{zt} = \left[\frac{\mathbf{f}}{\mathbf{g}} \mathbf{z}^\kappa \right]_q$.

Publish $\text{params} = (n, q, \kappa, \{\mathbf{x}_i\})$ and \mathbf{p}_{zt} .

Sampling level-zero encodings: $\mathbf{a} \leftarrow \text{samp}(\text{params})$.

Sample $\mathbf{a} \leftarrow D_{\mathcal{I}, \sigma'}$.

Encodings at higher levels: $\mathbf{c}_i \leftarrow \text{enc}(\text{params}, i, \mathbf{c})$.

Given a level- j encoding \mathbf{c} for $j < i$, compute $\mathbf{c}_i = [\mathbf{c}' / \mathbf{z}^{i-j}]_q$, where $\mathbf{c}' - \mathbf{c} \in \langle \mathbf{g} \rangle$, and $\|\mathbf{c}'\| < \sigma^*$.

Adding and multiplying encodings: Given two encodings \mathbf{c}_1 and \mathbf{c}_2 of the same level, the sum of \mathbf{c}_1 and \mathbf{c}_2 is computed by $\text{Add}(\mathbf{c}_1, \mathbf{c}_2) = [\mathbf{c}_1 + \mathbf{c}_2]_q$. Given two encodings \mathbf{c}_1 and \mathbf{c}_2 , we multiply \mathbf{c}_1 and \mathbf{c}_2 by computing $\text{Mul}(\mathbf{c}_1, \mathbf{c}_2) = [\mathbf{c}_1 \cdot \mathbf{c}_2]_q$.

Zero testing: $\text{isZero}(\text{params}, \mathbf{p}_{zt}, \mathbf{c}) \stackrel{?}{=} 0/1$.

Given a level- κ encoding \mathbf{c} , return 1 if $\|[\mathbf{p}_{zt} \cdot \mathbf{c}]_q\|_\infty < q^{3/4}$; otherwise, return 0.

Extraction: $sk \leftarrow \text{ext}(\text{params}, \mathbf{p}_{zt}, \mathbf{c})$.

Given a level- κ encoding \mathbf{c} , compute $\text{MSB}_{\log q/4 - \lambda}([\mathbf{p}_{zt} \cdot \mathbf{c}]_q)$.

4.2. *Difficulty assumptions*

We recall the definitions of the graded decisional Diffie–Hellman problem (GDDH) and GCDH problems on which the security of the GGH scheme relies [12]. They do not seem to be reducible to more classical assumptions in generic ways.

GDDH, ext-GCDH, GCDH. For an adversary A and the parameters λ and κ , we consider the following process in the GGH scheme.

- (1) Choose $(q, \{\mathbf{x}_i\}, \mathbf{p}_{zt}) \leftarrow \text{InstGen}(1^\lambda, 1^\kappa)$.
- (2) Sample $\mathbf{m}_j \leftarrow \text{samp}(\text{params})$ for each $0 \leq j \leq \kappa$.
- (3) Set $\mathbf{u}_j = \mathbf{a}_j / \mathbf{z} \leftarrow \text{enc}(\text{params}, 1, \mathbf{m}_j)$ for all $0 \leq j \leq \kappa$.
- (4) Choose $\mathbf{r} \leftarrow D_{R, \sigma'}$.
- (5) Sample $\rho_j \leftarrow \{0, 1\}$ for $1 \leq j \leq m$.

- (6) Set $\hat{\mathbf{u}} = [\mathbf{a}_0 \times \prod_{i=1}^{\kappa} \mathbf{u}_i + \sum_j \rho_j \mathbf{x}_j]_q$.
- (7) Set $\mathbf{u} = [\mathbf{r} \times \prod_{i=1}^{\kappa} \mathbf{u}_i + \sum_j \rho_j \mathbf{x}_j]_q$.

The GCDH problem is to output a level- κ encoding of $\prod_{i=0}^{\kappa} \mathbf{m}_i + \mathcal{I}$ given the inputs

$$\{q, \{\mathbf{x}_i\}, \mathbf{p}_{zt}, \mathbf{u}_0, \dots, \mathbf{u}_{\kappa}\}.$$

The ext-GCDH problem is to output $\mathbf{v} \in R_q$ such that $\|\mathbf{v} - \mathbf{p}_{zt} \cdot \hat{\mathbf{u}}\| < q^{3/4}$ given the inputs

$$\{q, \{\mathbf{x}_i\}, \mathbf{p}_{zt}, \mathbf{u}_0, \dots, \mathbf{u}_{\kappa}\}.$$

The GDDH problem is to distinguish between two distributions, \mathcal{D}_{DDH} and \mathcal{D}_R , where

$$\mathcal{D}_{DDH} = \{q, \{\mathbf{x}_i\}, \mathbf{p}_{zt}, \mathbf{u}_0, \dots, \mathbf{u}_{\kappa}, \hat{\mathbf{u}}\} \quad \text{and} \quad \mathcal{D}_R = \{q, \{\mathbf{x}_i\}, \mathbf{p}_{zt}, \mathbf{u}_0, \dots, \mathbf{u}_{\kappa}, \mathbf{u}\}.$$

4.3. Attack on GGH

Considering [12], one may notice that the previous theorem in §3 can be applied to solve the GCDH problem, which is a security problem of the GGH scheme. More precisely, suppose we have

$$\{q, \{\mathbf{x}_i\}, \mathbf{p}_{zt}, \mathbf{u}_0, \dots, \mathbf{u}_{\kappa}\}.$$

Additionally, we assume that we have a pair of level-0 encodings $\bar{\mathbf{m}} \notin \langle \mathbf{g} \rangle$ and its level-1 encoding $\mathbf{b} = [(\bar{\mathbf{m}} + \mathbf{a}\mathbf{g})/\mathbf{z}]_q$. Our attack algorithm consists of the following three steps:

- Find a small element $\mathbf{c}\mathbf{g} \in \langle \mathbf{g} \rangle$.
- Compute a small level-1 encoding of $\bar{\mathbf{m}}^{-1}$ using $\bar{\mathbf{m}}, \mathbf{c}\mathbf{g}$.
- Recover an element \mathbf{m}'_0 in $R = \mathbb{Z}[X]/\langle X^n + 1 \rangle$ such that $\mathbf{m}'_0 - \mathbf{m}_0 \in \langle \mathbf{g} \rangle$.

Finally, we can compute \mathbf{m}' , which is a level- κ encoding of $\prod_{i=0}^{\kappa} \mathbf{m}_i + \langle \mathbf{g} \rangle$ using $\mathbf{m}'_0, \mathbf{u}_i$, and \mathbf{x}_1 . Then it becomes a solution of the GCDH problem. In this paper, we assume $\sigma' = n^{2.5}$ and $\sigma^* = n^3$.

4.3.1. *Step 1: Finding a small element of $\langle \mathbf{g} \rangle$.* Note that $\|\bar{\mathbf{m}} + \mathbf{a}\mathbf{g}\|, \|\mathbf{b}_i\mathbf{g}\|, \|\mathbf{a}_i\| \leq \sigma^* \sqrt{n} \leq n^{3.5}$, and $\|\bar{\mathbf{m}}\| \leq \sigma' \sqrt{n} \leq n^3$ with overwhelming probability. For convenience, we use the notation G_t to denote $\text{Gal}(K/K_t)$. Considering $[\mathbf{u}_1^{\kappa}/\mathbf{x}_1]_q = [\mathbf{a}_1^{\kappa}/\mathbf{b}_1\mathbf{g}]_q$, the sizes of the denominator and numerator are bounded by $n^{3.5\kappa} \sqrt{n}^{\kappa-1} < n^{4\kappa}$ and $n^{3.5}$, respectively. Using the algorithm in Theorem 2 for several $[\mathbf{a}_I/\mathbf{b}_j\mathbf{g}]_q := [\mathbf{a}_{i_1} \dots \mathbf{a}_{i_{\kappa}}/\mathbf{b}_j\mathbf{g}]_q$ for $I = [i_1, \dots, i_{\kappa}]$, $i_1, \dots, i_{\kappa} \in \{0, \dots, \kappa\}$, and $j \in \{1, \dots, m\}$, one can recover several multiples $\mathbf{c}_I \mathbf{b}'_j \mathbf{g}' \mathbf{b}_j \mathbf{g}$ of $N_{K/K_t}(\mathbf{g})$, where $\mathbf{b}'_j = \prod_{\sigma \in G_t \setminus \{\text{id}\}} \sigma(\mathbf{b}_j)$ and $\mathbf{g}' = \prod_{\sigma \in G_t \setminus \{\text{id}\}} \sigma(\mathbf{g})$. Multiplying these multiples by $[\mathbf{a}_I/\mathbf{b}_j\mathbf{g}]_q$, one can obtain $A_{I,j} = \mathbf{a}_I \mathbf{c}_I \mathbf{b}'_j \mathbf{g}'$. We remark that $A_{I,j}$ is in $R \setminus R_t$ because $A_{I,j}$ is not fixed for any subgroup of G_t , except the trivial group. Moreover, although $A_{I,j}$ is not in $\langle \mathbf{g} \rangle$, we have $\delta(A_{I,j}) = \delta(\mathbf{a}_I \mathbf{c}_I \mathbf{b}'_j \mathbf{g}') = \delta(\mathbf{a}_I \mathbf{c}_I) \cdot \prod_{\sigma \in G_t \setminus \{\delta\}} \sigma(\mathbf{b}\mathbf{g}) \in \langle \mathbf{g} \rangle$ for $\delta \in G_t \setminus \{\text{id}\}$. One can easily see that $\{\delta(A_{I,j})\}_{\delta \in G_t \setminus \{\text{id}\}}$ only have a common factor \mathbf{g} . Therefore, using $\{\delta(A_{I,j})\}_{\delta \in G_t \setminus \{\text{id}\}}$, we recover a basis matrix of the ideal lattice of $\langle \mathbf{g} \rangle$. Using $N_{K/K_t}(\mathbf{a})$ for $\mathbf{a} \in \langle \mathbf{g} \rangle$, which is a multiple of $N_{K/K_t}(\mathbf{g})$, one can also recover a basis matrix of the ideal lattice of $(N_{K/K_t}(\mathbf{g}))$. Now, using the β block-BKZ algorithm [15], one can obtain an element $\mathbf{c}\mathbf{g} \in (N_{K/K_t}(\mathbf{g}))$ such that $\|\mathbf{c}\mathbf{g}\| \leq 2\beta^{(n_t-1)/2(\beta-1)+3/2} \cdot n^{2^{t+1}}$.

4.3.2. *Step 2: Computing a small level-1 encoding of \bar{m}^{-1} .* Using a pair $(\bar{\mathbf{m}}, \mathbf{b} = [(\bar{\mathbf{m}} + \mathbf{a}\mathbf{g})/\mathbf{z}]_q)$, one can recover a level-1 encoding of 1 as follows. Since we know a basis matrix of $\langle \mathbf{g} \rangle$, one can compute $\hat{\mathbf{e}}$ such that $\hat{\mathbf{e}}\bar{\mathbf{m}} + \hat{\mathbf{e}}'\mathbf{g} = 1$ for some $\hat{\mathbf{e}}' \in R$. Then $\mathbf{e} := (\hat{\mathbf{e}} \bmod \mathbf{c}\mathbf{g})$ is the inverse of $\bar{\mathbf{m}}$ in $R/\langle \mathbf{g} \rangle$. Moreover, its size is smaller than $\|\mathbf{c}\mathbf{g}\| \cdot n/2$.

4.3.3. *Step 3: Computing \mathbf{m}' .* We refer to [12, §6.3.3] to solve the GCDH problem with the short vector $\mathbf{c}\mathbf{g} \in \langle \mathbf{g} \rangle$. We explain how to use $\mathbf{c}\mathbf{g}$ in order to solve the GCDH problem in the GGH scheme. First, by applying Theorem 2 to $\mathbf{b}^{\kappa}/\mathbf{x}_1 = (\bar{\mathbf{m}} + \mathbf{a}\mathbf{g})^{\kappa}/\mathbf{b}_1\mathbf{g}$, one can obtain

$\mathbf{d}(\bar{\mathbf{m}} + \mathbf{a}\mathbf{g})^\kappa$ and $\mathbf{d}\mathbf{b}_1\mathbf{g}$ for some $\mathbf{d} \in R$. Now, compute $\mathbf{G} \in R$ such that $\mathbf{e}^\kappa \cdot \mathbf{d}(\bar{\mathbf{m}} + \mathbf{a}\mathbf{g})^\kappa - \mathbf{G}\mathbf{d}\mathbf{b}_1\mathbf{g} = \mathbf{e}^\kappa \cdot \mathbf{d}(\bar{\mathbf{m}} + \mathbf{a}\mathbf{g})^\kappa \bmod \mathbf{d}\mathbf{b}_1\mathbf{g}$ and also compute $\mathbf{b}' = \mathbf{e}^\kappa \mathbf{b}^\kappa - \mathbf{G}\mathbf{x}_1$. Similarly, compute $\mathbf{G}' \in R$ such that $\mathbf{b}'' = \mathbf{e}^{\kappa-1} \cdot \mathbf{b}^{\kappa-1} \mathbf{u}_0 - \mathbf{G}'\mathbf{x}_1$. Then, \mathbf{b}' and \mathbf{b}'' have the following forms:

$$\mathbf{b}' = \left[\frac{\mathbf{e}^\kappa \cdot (\bar{\mathbf{m}} + \mathbf{a}\mathbf{g})^\kappa \bmod \mathbf{b}_1\mathbf{g}}{\mathbf{z}^\kappa} \right]_q = \left[\frac{\mathbf{a}'\mathbf{g} + 1}{\mathbf{z}^\kappa} \right]_q,$$

$$\mathbf{b}'' = \left[\frac{\mathbf{e}^{\kappa-1} \cdot (\bar{\mathbf{m}} + \mathbf{a}\mathbf{g})^{\kappa-1} \mathbf{m}_0 \bmod \mathbf{b}_1\mathbf{g}}{\mathbf{z}^\kappa} \right]_q = \left[\frac{\mathbf{a}''\mathbf{g} + \mathbf{m}_0}{\mathbf{z}^\kappa} \right]_q$$

for some small \mathbf{a}' and $\mathbf{a}'' \in R$. The sizes of the numerators of \mathbf{b}' and \mathbf{b}'' are bounded by $\|\mathbf{b}_1\mathbf{g}\| \cdot n/2 \leq n^{4.5}/2$. By using $\mathbf{c}\mathbf{g}$, \mathbf{b}' , \mathbf{b}'' , and \mathbf{p}_{zt} , one can obtain the following zero-testing values \mathbf{h} and \mathbf{h}_0 :

$$\mathbf{h} := \iota([\mathbf{b}' \cdot \mathbf{p}_{zt} \cdot \mathbf{c}\mathbf{g}]_q) = \iota([\mathbf{a}'\mathbf{g} + 1] \cdot \mathbf{f} \cdot \mathbf{c}]_q),$$

$$\mathbf{h}_0 := \iota([\mathbf{b}'' \cdot \mathbf{p}_{zt} \cdot \mathbf{c}\mathbf{g}]_q) = \iota([\mathbf{a}''\mathbf{g} + \mathbf{m}_0] \cdot \mathbf{f} \cdot \mathbf{c}]_q).$$

If $\|\mathbf{h}\|$ is smaller than $q/2$, \mathbf{h} is actually $(\mathbf{a}'\mathbf{g} + 1) \cdot \mathbf{f} \cdot \mathbf{c}$ in R . Since the size of \mathbf{h} is smaller than $\|\mathbf{c}\mathbf{g}\| \|\mathbf{g}^{-1}\| \cdot \|\mathbf{f}\| \cdot \|\mathbf{a}'\mathbf{g} + 1\| \cdot n \leq \beta^{(n_t-1)/2(\beta-1)+3/2} \cdot n^{2^{t+1}} n^8 \sqrt{q}$, we use the following equation to check the condition:

$$\beta^{(n_t-1)/2(\beta-1)+3/2} \cdot n^{2^{t+1}} n^8 \sqrt{q} \leq \frac{q}{2} \tag{4.1}$$

$$\Leftrightarrow \left(\frac{n_t}{2(\beta-1)} + \frac{3}{2} \right) \log \beta + \log n^{2^{t+1}} + 8 \log n + 1 < \frac{\log q}{2}. \tag{4.2}$$

This inequality is asymptotically the same as equation (3). Hence, when $\beta = \log^2 \lambda$, the size of \mathbf{h} is smaller than $q/2$. For the same condition, \mathbf{h}_0 has the same bound and is of the form $(\mathbf{a}''\mathbf{g} + \mathbf{m}_0) \cdot \mathbf{f} \cdot \mathbf{c}$. Assuming that \mathbf{h} has an inverse in $R/\langle \mathbf{g} \rangle$, we can compute $\mathbf{m}'_0 := \mathbf{h}_0/\mathbf{h} = \mathbf{m}_0 \bmod \langle \mathbf{g} \rangle$. Then, \mathbf{m}'_0 is a level-0 encoding of \mathbf{m}_0 . Note that we are given a top-level encoding of zero, $\mathbf{x}_1 = [\mathbf{b}_1\mathbf{g}/\mathbf{z}^\kappa]_q$. Multiplying $\mathbf{d}\mathbf{b}_1\mathbf{g}$ with $[\prod_{i=1}^\kappa \mathbf{u}_i/\mathbf{x}_1]_q$, we can recover $\mathbf{d} \prod_{i=1}^\kappa \mathbf{a}_i$. Now, we compute $(\mathbf{m}'_0 \cdot \mathbf{d} \prod_{i=1}^\kappa \mathbf{a}_i) \bmod \mathbf{d}\mathbf{b}_1\mathbf{g}$, which is of the form $\mathbf{m}'_0 \cdot \mathbf{d} \prod_{i=1}^\kappa \mathbf{a}_i - \mathbf{G}''\mathbf{d}\mathbf{b}_1\mathbf{g}$ for some $\mathbf{G}'' \in R$. Since \mathbf{d} is the common factor, it is the same as $\mathbf{d} \cdot ((\mathbf{m}'_0 \cdot \prod_{i=1}^\kappa \mathbf{a}_i) \bmod \mathbf{b}_1\mathbf{g}) = \mathbf{d} \cdot (\mathbf{m}'_0 \cdot \prod_{i=1}^\kappa \mathbf{a}_i - \mathbf{G}''\mathbf{b}_1\mathbf{g})$. We remark that the size of $(\mathbf{m}'_0 \cdot \prod_{i=1}^\kappa \mathbf{a}_i) \bmod \mathbf{b}_1\mathbf{g}$ is bounded by $\|\mathbf{b}_1\mathbf{g}\| n < n^5$, and it is an element of the coset $\prod_{i=0}^\kappa \mathbf{m}_i + \langle \mathbf{g} \rangle$. Now we compute $\mathbf{m}'_0 \cdot \prod_{i=1}^\kappa \mathbf{u}_i - \mathbf{G}''\mathbf{x}_1$, which has the following form:

$$\left[\frac{(\mathbf{m}'_0 \cdot \prod_{i=1}^\kappa \mathbf{a}_i) \bmod \mathbf{b}_1\mathbf{g}}{\mathbf{z}^\kappa} \right]_q.$$

By the above mention, its numerator is in the coset $\prod_{i=0}^\kappa \mathbf{m}_i + \langle \mathbf{g} \rangle$, and its size is bounded by n^5 . Hence, it is a valid level- κ encoding of $\prod_{i=0}^\kappa \mathbf{m}_i$, and the GCDH problem is solved. In summary, we obtain the following corollary.

COROLLARY 3. *Given $\{n, q, \{\mathbf{x}_i\}, \mathbf{m}, \mathbf{b}, \mathbf{p}_{zt}, \mathbf{u}_0, \dots, \mathbf{u}_\kappa\}$ of the GGH scheme parameters, where n is $\Theta(\lambda^2)$, $\log q = \Theta(\lambda)$, \mathbf{x}_i is a level- κ encoding of zero, \mathbf{m} is a level-0 nonzero encoding, \mathbf{b} is a level-1 encoding of \mathbf{m} , and \mathbf{u}_i is a level-1 encoding of \mathbf{m}_i , one can compute $\text{enc}_\kappa(\prod_{i=0}^\kappa \mathbf{m}_i)$, which is a solution of the GCDH problem in the GGH scheme in $2^{O(\log^2 \lambda)}$.*

According to this corollary, using the parameters suggested by [12] causes an attack for a security ground of this scheme in the quasi-polynomial time of its security parameter. Thus, n must be at least $\Omega(\lambda^3)$ when $\log q = \Theta(\lambda)$ with the security parameter λ to avoid our attack.

5. Conclusion

Since the GGH scheme that provides an encoding of zero was found to be insecure, a variant of the NTRU problem has received considerable attention because of the security grounding of the GGH scheme without an encoding of zero. In this work, we described how to find a small solution of the variant of the NTRU problem using a reduction technique. By applying our proposed algorithm to the GGH scheme, we could attack the GCDH problem in the GGH scheme. Therefore, our results imply that there is no guarantee for the security of the GGH scheme when we are given a small encoding of zero and also when we are not given a small encoding of zero.

Acknowledgements. The authors thank Martin Albrecht, Shi Bai, Leo Ducas for helpful discussions. The authors were supported by a National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIP) (No. 2014R1A2A 1A11050917).

References

1. D. AGGARWAL, D. DADUSH, O. REGEV and N. STEPHENS-DAVIDOWITZ, ‘Solving the shortest vector problem in 2^n time via discrete Gaussian sampling’, Preprint, 2014, [arXiv:1412.7994](https://arxiv.org/abs/1412.7994).
2. M. R. ALBRECHT, S. BAI and L. DUCAS, ‘A subfield lattice attack on overstretched NTRU assumptions: cryptanalysis of some FHE and graded encoding schemes’, *Advances in cryptology — CRYPTO 2016* (Springer, Berlin, 2016) 153–178.
3. M. R. ALBRECHT, C. COCIS, F. LAGUILLAUMIE and A. LANGLOIS, ‘Implementing candidate graded encoding schemes from ideal lattices’, *Advances in cryptology — ASIACRYPT 2015* (Springer, Berlin, 2015) 752–775.
4. D. BONEH and A. SILVERBERG, ‘Applications of multilinear forms to cryptography’, *Topics in algebraic and noncommutative geometry*, Contemporary Mathematics 324 (eds C. G. Melles, J.-P. Brasselet, G. Kennedy, K. Lauter and L. McEwan; American Mathematical Society, Providence, RI, 2003) 71–90.
5. J. W. BOS, K. LAUTER, J. LOFTUS and M. NAEHRIG, ‘Improved security for a ring-based fully homomorphic encryption scheme’, *Cryptography and coding 2013* (Springer, Berlin, 2013) 45–64.
6. J. H. CHEON, K. HAN, C. LEE, H. RYU and D. STEHLÉ, ‘Cryptanalysis of the multilinear map over the integers’, *Advances in cryptology — EUROCRYPT 2015* (Springer, Berlin, 2015) 3–12.
7. J. H. CHEON, C. LEE and H. RYU, ‘Cryptanalysis of the new CLT multilinear maps’, *Advances in cryptology — EUROCRYPT 2016* (Springer, Berlin, 2016) 509–536.
8. J.-S. CORON, ‘Cryptanalysis of GGH15 multilinear maps’, *Advances in cryptology — CRYPTO 2016* (Springer, Berlin, 2016) 607–628.
9. J.-S. CORON, T. LEPOINT and M. TIBOUCHI, ‘Practical multilinear maps over the integers’, *Advances in cryptology — CRYPTO 2013* (Springer, Berlin, 2013) 476–493.
10. J.-S. CORON, T. LEPOINT and M. TIBOUCHI, ‘New multilinear maps over the integers’, *Advances in cryptology — CRYPTO 2015* (Springer, Berlin, 2015) 267–286.
11. L. DUCAS, A. DURMUS, T. LEPOINT and V. LYUBASHEVSKY, ‘Lattice signatures and bimodal Gaussians’, *Advances in cryptology — CRYPTO 2013* (Springer, Berlin, 2013) 40–56.
12. S. GARG, C. GENTRY and S. HALEVI, ‘Candidate multilinear maps from ideal lattices’, *Advances in cryptology — EUROCRYPT 2013* (Springer, Berlin, 2013) 1–17.
13. S. GARG, C. GENTRY and S. HALEVI, ‘Graph-induced multilinear maps from lattices’, *Theory of cryptography 2015* (Springer, Berlin, 2015) 498–527.
14. C. GENTRY and M. SZYDLO, ‘Cryptanalysis of the revised NTRU signature scheme’, *Advances in cryptology — EUROCRYPT 2002* (Springer, Berlin, 2002).
15. G. HANROT, X. PUJOL and D. STEHLÉ, ‘Terminating BKZ’, IACR Cryptology ePrint Archive 2011, <https://eprint.iacr.org/2011/198>.
16. J. HOPFSTEIN, N. HOWGRAVE-GRAHAM, J. PIPHER, J. H. SILVERMAN and W. WHYTE, ‘NTRUSIGN: digital signatures using the NTRU lattice’, *Topics in cryptology — CT-RSA 2003* (Springer, Berlin, 2003) 122–140.
17. J. HOPFSTEIN, J. PIPHER and J. H. SILVERMAN, ‘NTRU: a ring-based public key cryptosystem’, *Algorithmic number theory 1998* (Springer, Berlin, 1998) 267–288.
18. Y. HU and H. JIA, ‘Cryptanalysis of GGH map’, *Advances in cryptology — EUROCRYPT 2016* (Springer, Berlin, 2016) 537–565.
19. A. LANGLOIS, D. STEHLÉ and R. STEINFELD, ‘GGHlite: more efficient multilinear maps from ideal lattices’, *Advances in cryptology — EUROCRYPT 2014* (Springer, Berlin, 2014) 239–256.

20. A. LÓPEZ-ALT, E. TROMER and V. VAIKUNTANATHAN, 'On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption', *Proceedings of the Forty-Fourth Annual ACM Symposium on Theory of Computing 2012* (ACM, New York, NY, 2012) 1219–1234.
21. E. MILES, A. SAHAI and M. ZHANDRY, 'Annihilation attacks for multilinear maps: cryptanalysis of indistinguishability obfuscation over GGH13', *Advances in cryptology — CRYPTO 2016* (Springer, Berlin, 2016) 491–520.

Jung Hee Cheon
Seoul National University
1 Gwanak-ro
Gwanak-gu
Seoul 151-742
Republic of Korea
jhcheon@snu.ac.kr

Jinhyuck Jeong
Seoul National University
1 Gwanak-ro
Gwanak-gu
Seoul 151-42
Republic of Korea
wlsyrlkd@snu.ac.kr

Changmin Lee
Seoul National University
1 Gwanak-ro
Gwanak-gu
Seoul 151-742
Republic of Korea
cocomi11@snu.ac.kr