An Algorithm for NTRU Problems and Cryptanalysis of the GGH Multilinear Map without a low level encoding of zero

Jung Hee Cheon, Jinhyuck Jeong, Changmin Lee

Seoul National University (SNU), Republic of Korea

Abstract. Let $\boldsymbol{h}$ and $\boldsymbol{g}$ be polynomials of bounded Euclidean norm in the ring $\mathbb{Z}[X]/\langle X^n+1\rangle$. Given polynomial $[\boldsymbol{h}/\boldsymbol{g}]_q \in \mathbb{Z}_q[X]/\langle X^n+1\rangle$, the NTRU problem is to find $\boldsymbol{a},\ \boldsymbol{b} \in \mathbb{Z}[X]/\langle X^n+1\rangle$ with small Euclidean norm such that $[\boldsymbol{a}/\boldsymbol{b}]_q = [\boldsymbol{h}/\boldsymbol{g}]_q$. We propose an algorithm to solve the NTRU problem which runs in $2^{O(n/\log^{2-\epsilon} q)}$ time for some $0 < \epsilon < 2$ when $\|\boldsymbol{g}\|, \|\boldsymbol{h}\|$ and $\|\boldsymbol{g}^{-1}\|$ are in some range. The main technique of our algorithm is to reduce a problem on a field to one in a subfield.
Recently, the GGH scheme, the first candidate of a (approximate) multilinear map, was known to be insecure by the Hu-Jia attack using encodings of zero, but no polynomial time attack was known without them. Our algorithm can be directly applied to construct level-0 encodings of zero and so utilized to attack the GGH scheme without encodings of zero in polynomial time of its security parameter.

Keywords: NTRU, GGH Multilinear Maps, Ideal Lattice, Shortest Vector Problem

1 Introduction

The NTRU problem is to find a pair of small polynomial whose ratio matches up to given a ratio of two small polynomials [HPS98]. After introduced for the security of a public key encryption scheme NTRU, the assumption that this NTRU problem is to be hard to solve, so-called NTRU assumption, has been used for the security grounding of various cryptographic schemes such as signature schemes [HHGP$^+$03,DDLL13], fully homomorphic encryption [LATV12,BLLN13] and candidates for cryptographic multi-linear maps [GGH13,LSS14,ACLL14]. Not broken until now, the NTRU assumption is getting more attention as one of the candidates for the post-quantum public-key crypto system. A variant of NTRU problem can be stated as follows:

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

In the original NTRU problem, $\boldsymbol{h}$ and $\boldsymbol{g}$ are sampled from the some distribution of R. We consider the variant version to attack multilinear maps [GGH13].

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 $\phi_n = X^n + 1$, $B = \min\{\frac{q}{2D\sqrt{n}}, \frac{q}{2N\sqrt{n}}\}$, $D_1 = D^2\sqrt{n/2}$, $N_1 = 2ND\sqrt{n/2}$, and $B_1 = \min\{\frac{q}{2D_t\sqrt{n}}, \frac{q}{2N_t\sqrt{n}}, \frac{q}{2nN^2\|\boldsymbol{g}^{-1}\|\sqrt{n}}\}$ 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 applying repeatedly, we then use lattice reduction algorithms to find a short element. Since the latter has smaller dimension, lattice reduction algorithms require less running time to produce a short element, which results in an algorithm on the NTRU problem. It runs in $2^{O(n/\log^{2-\epsilon} q)}$ time for some $0 < \epsilon < 2$ when $\|\boldsymbol{g}\|, \|\boldsymbol{h}\|$ and $\|\boldsymbol{g}^{-1}\|$ are in some range. For example, when $n = \lambda^2$ and $\log q = \lambda$, the running time is of polynomial in λ.

As an application of our work, we propose an attack of the GGH multilinear maps [GGH13] without any encodings of zero. The GGH maps were proposed by Garg *et al.* and broken by so called a zeroizing attack by Hu and Jia [HJ15]. Since their attack extensively utilizes 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 concurrent and independent works on this problem). Our algorithm can be directly applied to construct level-0 encodings of zero. We then can utilize them to attack the GGH scheme without encodings of zero in polynomial time of its security parameter. Our GGH attack requires one known plaintext/ciphertext pair as well as public parameters.

Technical overview. A natural approach for the NTRU problem is to convert it to a Shortest Vector Problem (SVP) in an ideal lattice. Let $\phi_n(X) = X^n + 1$ when n is a power of 2. For any polynomial $\boldsymbol{f} = [\boldsymbol{h}/\boldsymbol{g}]_q = \sum_{i=0}^{n-1} f_i X^i \in R := \mathbb{Z}[X]/\langle X^n + 1\rangle$, one may consider it as a vector $(f_0, \cdots, f_{n-1})^T$. Then, the product $\boldsymbol{gf} = \sum_{i=0}^{n-1} g_i X^i \boldsymbol{f}$ of two polynomials $\boldsymbol{f}$ and $\boldsymbol{g}$ in R is contained in a lattice $\mathcal{M}_{\boldsymbol{f}}$ generated by $\{\boldsymbol{f}, X\boldsymbol{f}, \cdots, X^{n-1}\boldsymbol{f}\}$. We aim to obtain an element $\tilde{\boldsymbol{g}} \in \mathbb{Z}[X]/\langle\phi(X)\rangle$ satisfying $\|\tilde{\boldsymbol{g}}\|$ and $\|[\tilde{\boldsymbol{g}}\boldsymbol{f}]_q\|$ are small. To obtain such a $\tilde{\boldsymbol{g}} \in \mathbb{Z}[X]/\langle\phi(X)\rangle$, one can naturally contemplate the following column lattice:

$$\Lambda_{\boldsymbol{f}} = \begin{pmatrix} I & 0 \\ M_{\boldsymbol{f}} & qI \end{pmatrix},$$

where I is the identity matrix of size n and $M_{\boldsymbol{f}}$ is a basis matrix of $\mathcal{M}_{\boldsymbol{f}}$ juxtaposed by $\{\boldsymbol{f}, X\boldsymbol{f}, \cdots, X^{n-1}\boldsymbol{f}\}$.

Given a lattice vector $\boldsymbol{u} = (u_0, \cdots, u_{2n-1})^T$ of Λ_f satisfying $|u_i| < q/2$ for $n \le i \le 2n-1$, we take $\boldsymbol{g}' = \sum_{i=0}^{n-1} u_i X^i$ and $\boldsymbol{h}' = \sum_{i=0}^{n-1} u_{n+i} X^i$ so that $\boldsymbol{h}' = [\boldsymbol{g}'\boldsymbol{f}]_q$ and $\boldsymbol{f} = [\boldsymbol{h}'/\boldsymbol{g}']_q$. Therefore, if one can find a small lattice point $\boldsymbol{u}$ such that $\sqrt{\sum_{i=0}^{n-1} u_i} \le \frac{q}{2\|\boldsymbol{h}\|\sqrt{n}}$ and $\sqrt{\sum_{i=n}^{2n-1} u_i} \le \frac{q}{2\|\boldsymbol{g}\|\sqrt{n}}$, it becomes a solution

of $NTRU_{\phi,q,D,N,B}$. However, the dimension $2n$ of the lattice is too large for most applications, where the hardness of the NTRU problem comes from.

To overcome this obstacle, we consider a subfield K_m of $K_0 := \mathbb{Q}[X]/\langle X^n+1\rangle$ with extension degree m, and the trace of $f \in K_0$ over K_m:

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

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

Multilinear Maps. After Boneh and Silverberg [BS02] suggested a concept of cryptographic multilinear maps and their applications such as multipartite Diffie-Hellman and an efficient broadcast encryption in 2002, it has been a long lasting open question to construct cryptographic multilinear maps. In 2013, after about one decade, approximate cryptographic multilinear maps are first proposed by Garg, Gentry, and Halevi (GGH) [GGH13] . Not much later, second and third cryptographic multilinear maps are suggested by Coron, Lepoint, and Tibouchi (CLT) [CLT13], and Craig Gentry, Sergey Gorbunov, and Shai Halevi [GGH15], respectively. However, none of them have a reduction to standard hardness problem such as subset sum problem. In fact, the first two schemes with low level encodings of zero are known to be insecure [CHL$^+$15,HJ15], so called zeroizing attack. The last candidate is also broken [Cor15]. Although the fixed scheme of [CLT13] is proposed by the same authors of [CLT15] to resist zeroizing attack against the CLT scheme, it is also shown to be insecure [CLR15].

On the other hand, both [GGH13] scheme and [CLT13] scheme without any encodings of zero, which are used as basic tools for constructing applications such as indistinguishable obfuscations, have still not been analyzed yet.

Related work. Recently for GGH multilinear maps without encodings of zero, two more concurrent and independent cryptanalytic works have been announced simultaneously: One by Albrecht, Bai, and Ducas [MA16] and the other by Miles, Sahai, and Zhandry [MSZ16].

The first introduces a very similar reduction from $NTRU_{\phi_n,q,D,N,B}$ into $NTRU_{\phi_{n/2},q,D_1,N_1,B_1}$. But they used the norm function instead of the trace function in our algorithm and so happened to have larger N_1 than ours, when $N > 2D$. That results in quantum polynomial time or subexponential time attack on GGH without encodings of zero. However, they provided rich analysis for NTRU-like homomorphic encryptions LTV [LATV12] and YASHE [BLLN13], and multilinear maps GGH with some implementations.

The second introduces a polynomial time attack algorithm against the GGH multilinear maps, so called *annihilation attacks*. Using non-linear polynomials,

it also leads to a polynomial time break of the GGH scheme without low level encodings of zero.

Organization. In Section 2, we introduce some notations and preliminaries related to ideal theory and Galois theory. In Section 3, we state useful properties and their proof used to solve the $NTRU$ problem. In Section 4, we explain the GGH scheme briefly and present our algorithm to attack the GGH scheme using our theorem.

2 Preliminaries

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

We define $\iota : \mathbb{Z}_q \longrightarrow \mathbb{Z}$ by $[x]_q \in \mathbb{Z}_q \mapsto x \in \mathbb{Z}$ for $-\frac{q}{2} < x \leq \frac{q}{2}$. We extend this map into R_q applying to each coefficient. By abuse of notation, we omit this ι unless confused to identify $[x]_q \in \mathbb{Z}_q$ with an integer x when $-\frac{q}{2} < x \leq \frac{q}{2}$.

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 $R := \mathbb{Z}[X]/\langle X^n+1\rangle$. Especially, K is a Galois extension of $\mathbb{Q}$ and we denote by $\mathrm{Gal}(K/\mathbb{Q})$ the Galois group of K over $\mathbb{Q}$. As in technical overview, for any polynomial $\boldsymbol{f} = \sum_{i=0}^{n-1} f_i X^i \in K$, we consider it as a column vector $(f_0, \cdots, f_{n-1})^T$. When we need an inverse of element $\boldsymbol{a} \in R$, we usually consider the inverse in K with notation $\boldsymbol{a}^{-1}$. If we want to consider it in R_q not in K, then we denote it by $\left[\boldsymbol{a}^{-1}\right]_q$. 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 lattice $\mathcal{M}$. For an element $\boldsymbol{g} \in R$, we denote by $\langle \boldsymbol{g} \rangle$ be the principal ideal in R generated by $\boldsymbol{g}$, whose basis consists of $\{\boldsymbol{g}, X\boldsymbol{g}, \ldots, X^{n-1}\boldsymbol{g}\}$. By identifying a polynomial $\boldsymbol{g} = \sum g_i X^i \in R$ with a vector $(g_{n-1}, g_{n-2}, \ldots, g_0)^T$ in $\mathbb{Z}^n$, we can apply a lattice theory to the algebraic ring R and an algebraic ring theory to the ideal lattice $\langle \boldsymbol{g} \rangle$.

For a polynomial $\boldsymbol{u} \in R$ and a basis $\mathcal{B} := \{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\}$, we denote by $\boldsymbol{u} \bmod \mathcal{B}$ the reduction of $\boldsymbol{u}$ modulo the fundamental region of lattice $\mathcal{B}$, i.e, $\boldsymbol{u} \bmod \mathcal{B}$ is the unique representation of $\boldsymbol{u} \in R$ such that $\boldsymbol{u} - (\boldsymbol{u} \bmod \mathcal{B}) \in \mathcal{B}$ and $\boldsymbol{u} \bmod \mathcal{B} = \sum_{i=0}^{n-1} \alpha_i \boldsymbol{b}_i$ for $\alpha_i \in (-1/2, 1/2]$. For a polynomial $\boldsymbol{u}, \boldsymbol{v} \in R$, we use the notations $\boldsymbol{u} \bmod \boldsymbol{v}$ as $\boldsymbol{u} \bmod \mathcal{V}$, where $\mathcal{V}$ is a basis $\{\boldsymbol{v}, X\boldsymbol{v}, \ldots, X^{n-1}\boldsymbol{v}\}$. By

definition of $\boldsymbol{u} \bmod \boldsymbol{v}$, it is of the form $\sum_{i=0}^{n-1} \alpha_i X^i \boldsymbol{v}$ for $\alpha_i \in (-1/2, 1/2]$. Hence its Euclidean norm size is bounded by $\sum_{i=0}^{n-1} \|X^i \boldsymbol{v}\|/2 = \sum_{i=0}^{n-1} \|\boldsymbol{v}\|/2 = \frac{n}{2}\|\boldsymbol{v}\|$.

Next, we introduce useful lemmas related to ideal lattices.

Lemma 1 *For any $\boldsymbol{a}, \boldsymbol{b} \in R$, $\|\boldsymbol{ab}\| \leq \|\boldsymbol{a}\| \cdot \|\boldsymbol{b}\| \cdot \sqrt{n}$.*

Proof. The k-th coefficient of $\boldsymbol{ab}$ 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 $\|\boldsymbol{a}\| \cdot \|\boldsymbol{b}\|$. Since each coefficient is smaller than $\|\boldsymbol{a}\| \cdot \|\boldsymbol{b}\|$, $\|\boldsymbol{ab}\| \leq \|\boldsymbol{a}\| \cdot \|\boldsymbol{b}\| \cdot \sqrt{n}$.

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

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

Using Lemma 2, if one can find the $\boldsymbol{c}$ satisfying lemma 2, $\boldsymbol{c}$ is of the form $\boldsymbol{c} = \boldsymbol{dg}$ for some small $\boldsymbol{d} \in \mathbb{Z}[X]/\langle X^n + 1\rangle$. Then multiplying it to $[\boldsymbol{hg}^{-1}]_q$, one can obtain, a small multiple of $\boldsymbol{h}$, $\boldsymbol{dh}$. Hence, $\boldsymbol{dh}$ and $\boldsymbol{dg}$ become a solution of 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 $\rho_\sigma(x) = exp(-\pi\|x\|^2/\sigma^2)$, $\rho_\sigma(L) = \sum_{x \in L} \rho_\sigma(x)$. We use a notation $a \leftarrow \mathcal{D}$ to denote choosing an element a according to the distribution of $\mathcal{D}$.

Norm and Trace of Field For a finite extension K of a field F, the trace $\mathrm{Tr}_{K/F}(\alpha)$ and norm $\mathrm{N}_{K/F}(\alpha)$ of $\alpha \in K$ over F is defined as the trace and determinant of the linear transformation M_α which maps $x \in K$ to $\alpha x \in K$ respectively, i.e, $\mathrm{Tr}_{K/F}(\alpha) = \sum a_{i,i}$ and $\mathrm{N}_{K/F}(\alpha) = \det(a_{i,j})$ where $a_{i,j}$ is the matrix for M_α with respect to any base of K over F. The map $\mathrm{Tr}_{K/F}$ and $\mathrm{N}_{K/F}$ satisfy the following properties:

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

for $\alpha, \beta \in K$ and $a \in F$.

3 Main Theorem

In this section we introduce how we can reduce NTRU problem with a given input $[\boldsymbol{h}/\boldsymbol{g}]_q$ into NTRU problem with an input whose denominator and numerator have the half degree of $\boldsymbol{h}$ and $\boldsymbol{g}$. 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 $0 \le t \le s$. Note that $K_s := \mathbb{Q} \le K_{s-1} \le \cdots \le K_0 = \mathbb{Q}[X]/\langle X^n+1\rangle$, where $A \le B$ denotes A is a subfield of B.

Since K_0 is a Galois extension field of K_1 with degree 2, $\mathrm{Gal}(K_0/K_1)$ is a group of order 2. That is, $\mathrm{Gal}(K_0/K_1) = \{id, \sigma\}$ satisfying $\sigma(X) = -X$ and so $\sigma^2 = id$ where id is the identity map. For an element $\boldsymbol{f}, \boldsymbol{g} \in R \subset K_0$, the following elements are contained in $R_1 \subset K_1$:

$$\begin{aligned} Tr_{K_0/K_1}(\boldsymbol{f}) &= \boldsymbol{f} + \sigma(\boldsymbol{f}) \\ N_{K_0/K_1}(\boldsymbol{f}) &= \boldsymbol{f} \cdot \sigma(\boldsymbol{f}) \\ Tr_{K_0/K_t}(\boldsymbol{f}\sigma(\boldsymbol{g})) &= \boldsymbol{f}\sigma(\boldsymbol{g}) + \sigma(\boldsymbol{f})\boldsymbol{g}, \end{aligned}$$

since these are fixed by the $\mathrm{Gal}(K_0/K_1)$. Note that these elements have only $n/2$ terms and the last one lies in $2 \cdot R_1$.

Generally, for $0 < t \le s$, K_0 is a Galois extension field of K_t with degree 2^t and the Galois group $G_t := \mathrm{Gal}(K_0/K_t) = \{\sigma_0 = id, \sigma_1, \ldots, \sigma_{2^t-1}\}$. For an element $\boldsymbol{f}, \boldsymbol{g} \in R \subset K_0$, the following elements are contained in $R_t \subset K_t$:

$$\begin{aligned} &\sum_{i=0}^{2^t-1} \sigma_i(\boldsymbol{f}) = \boldsymbol{f} + \sigma_1(\boldsymbol{f}) + \cdots + \sigma_{2^t-1}(\boldsymbol{f}) \\ &\prod_{i=0}^{2^t-1} \sigma_i(\boldsymbol{f}) = \boldsymbol{f} \cdot \sigma_1(\boldsymbol{f}) \cdot \cdots \cdot \sigma_{2^t-1}(\boldsymbol{f}) \\ &Tr_{K_0/K_t}(\boldsymbol{f}\sigma_1(\boldsymbol{g})\sigma_2(\boldsymbol{g}) \cdots \sigma_{2^t-1}(\boldsymbol{g})), \end{aligned}$$

since these are fixed by the $\mathrm{Gal}(K_0/K_t)$. 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 get the following theorem which is the main theorem in this paper.

Theorem 1 *Let q and $m \in \mathbb{Z}$ be integers, and let D, and N be positive real numbers. Put $B = \min\{\frac{q}{2D\sqrt{n}}, \frac{q}{2N\sqrt{n}}\}$. Then, for $\phi_n(X) = X^n + 1$ with $n = 2^s$ and $0 < t \le s$, we can reduce $NTRU_{\phi_n,q,D,N,B}$ into $NTRU_{\phi_{n/2^t},q,D_t,N_t,B_t}$ where $B_t = \min\{\frac{q}{2D_t\sqrt{n}}, \frac{q}{2N_t\sqrt{n}}, \frac{q}{2nN^2\|\boldsymbol{g}^{-1}\|\sqrt{n}}\}$, $D_t = D^{2^t} \prod_{j=1}^{t} \sqrt{n/2^j}$, $N_t = ND^{2^t-1} \prod_{j=1}^{t} \sqrt{n/2^j}$.*

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

$$Tr_{K_0/K_t}\left(\frac{\boldsymbol{h}}{\boldsymbol{g}}\right) = \frac{\boldsymbol{h}}{\boldsymbol{g}} + \sigma_1\left(\frac{\boldsymbol{h}}{\boldsymbol{g}}\right) + \cdots + \sigma_{2^t-1}\left(\frac{\boldsymbol{h}}{\boldsymbol{g}}\right) = \frac{Tr_{K_0/K_t}(\boldsymbol{h}\sigma_1(\boldsymbol{g})\sigma_2(\boldsymbol{g}) \cdots \sigma_{2^t-1}(\boldsymbol{g}))}{\prod_{i=0}^{2^t-1} \sigma_i(\boldsymbol{g})}$$

in K_t satisfying:

- $\prod_{i=0}^{2^t-1} \sigma_i(\boldsymbol{g}) \in R_t$, and $Tr_{K_0/K_t}(\boldsymbol{h}\sigma_1(\boldsymbol{g})\sigma_2(\boldsymbol{g})\cdots\sigma_{2^t-1}(\boldsymbol{g})) \in 2^t \cdot R_t$,
- $\left\| \frac{Tr_{K_0/K_t}(\boldsymbol{h}\sigma_1(\boldsymbol{g})\sigma_2(\boldsymbol{g})\cdots\sigma_{2^t-1}(\boldsymbol{g}))}{2^t} \right\| \leq ND^{2^t-1} \prod_{j=1}^{t} \sqrt{n/2^j}$,
- $\left\| \prod_{i=0}^{2^t-1} \sigma_i(\boldsymbol{g}) \right\| \leq D^{2^t} \prod_{j=1}^{t} \sqrt{n/2^j}$.

Therefore, we can see $\left[\frac{Tr_{K_0/K_t}(\boldsymbol{h}\sigma_1(\boldsymbol{g})\sigma_2(\boldsymbol{g})\cdots\sigma_{2^t-1}(\boldsymbol{g}))/2^t}{\prod_{i=0}^{2^t-1}\sigma_i(\boldsymbol{g})} \right]_q$ as a new instance for $NTRU_{\phi_{n/2^t},q,D_t,N_t,B_t}$ where $D_t = D^{2^t} \prod_{j=1}^{t} \sqrt{n/2^j}$, $N_t = ND^{2^t-1} \prod_{j=1}^{t} \sqrt{n/2^j}$, $B_t = \min\{\frac{q}{2D_t\sqrt{n}}, \frac{q}{2N_t\sqrt{n}}, \frac{q}{2nN^2\|\boldsymbol{g}^{-1}\|\sqrt{n}}\}$.

Now, suppose that a solution $(\boldsymbol{a}_t, \boldsymbol{b}_t) \in R_t$ of $NTRU_{\phi_{n/2^t},q,D_t,N_t,B_t}$ is known such that $[\boldsymbol{b}_t/\boldsymbol{a}_t]_q = \left[\frac{Tr_{K_0/K_t}(\boldsymbol{h}\sigma_1(\boldsymbol{g})\sigma_2(\boldsymbol{g})\cdots\sigma_{2^t-1}(\boldsymbol{g}))/2^t}{\prod_{i=0}^{2^t-1}\sigma_i(\boldsymbol{g})} \right]_q$. Moreover, since $\boldsymbol{g}$ and $\boldsymbol{h}$ are relative prime with high probability [MA16], we assume the coprimality of $\boldsymbol{g}$ and $\boldsymbol{h}$. Then, by Lemma 2 , $\boldsymbol{a}_t$ is of the form $\boldsymbol{a}_t = \boldsymbol{d}\prod_{i=0}^{2^t-1}\sigma_i(\boldsymbol{g})$. Computing $[\boldsymbol{a}_t \cdot \boldsymbol{f}]_q = \left[\boldsymbol{d}\prod_{i=0}^{2^t-1}\sigma_i(\boldsymbol{g}) \cdot [\boldsymbol{h}/\boldsymbol{g}]_q\right]_q = \left[\boldsymbol{dh}\prod_{i=1}^{2^t-1}\sigma_i(\boldsymbol{g})\right]_q$, put $\boldsymbol{a} = \boldsymbol{a}_t$ and $\boldsymbol{b} = \left[\boldsymbol{dh}\prod_{i=1}^{2^t-1}\sigma_i(\boldsymbol{g})\right]_q$. Then, we can conclude that the pair $(\boldsymbol{a}, \boldsymbol{b})$ is a solution of $NTRU_{\phi_n,q,D,N,B}$ with following properties:

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

The last inequality implies $\boldsymbol{b} = \left[\boldsymbol{dh}\prod_{i=1}^{2^t-1}\sigma_i(\boldsymbol{g})\right]_q$ is actually $\boldsymbol{b} = \boldsymbol{dh}\prod_{i=1}^{2^t-1}\sigma_i(\boldsymbol{g})$ in R. Thus, we get the desired result. □

Theorem 2 *Let q be an integer, n be a power of 2, and λ be a security parameter. Let $\boldsymbol{f} = [\boldsymbol{h}/\boldsymbol{g}]_q$ be an instance of $NTRU_{\phi_n,q,D,N,B}$ problem with setting*

$\log q = \lambda^\ell$, $n \le \lambda^{2\ell+1}$, $N = q^a$, $0 < a < 1/2$, $D = \lambda^k < N$, $\|\boldsymbol{g}^{-1}\| < \lambda^2$, $\phi_n(X) = X^n + 1$, *and* $B = \min\{\frac{q}{2D\sqrt{n}}, \frac{q}{2N\sqrt{n}}\}$. *For* $\beta > 0$ *and* $t \in \mathbb{Z}$, *if*

$$2\beta^{\frac{n_t}{2(\beta-1)}+\frac{3}{2}}\sqrt{q} \le B_t$$

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

In particular, $B_t = \dfrac{q}{2N_t\sqrt{n}}$ *and* $\beta = \dfrac{n}{\log^{2-\epsilon} q}$, *for some* $0 < \epsilon < 2$, *the problem is solved in* $2^{O(n/\log^{2-\epsilon} q)}$ *time.*

For example, when $n = \lambda^2$, $D = \lambda^2$, $N = q^{1/8}$, and $\log q = \lambda$, one can solve the $NTRU_{\phi_n,q,D,N,B}$ in polynomial time in λ. In case of $n = \lambda^3$, $D = \lambda^2$, $N = q^{1/8}$, and $\log q = \lambda$, one can solve the problem in $2^{\tilde{O}(\lambda)}$ time.

Proof. By Theorem 1, one can obtain a new instance $[\mathrm{Tr}_{K/K_t}([\boldsymbol{h}/\boldsymbol{g}]_q)/2^t]_q \in R_q \cap R_t$ for $NTRU_{\phi_{n_t},q,N_t,D_t,B_t}$ where $N_t < N/\lambda^k \cdot \left(n\lambda^k/2\right)^{2^t}$, $D_t < \left(n\lambda^k/2\right)^{2^t}$, and $B_t = \min\{\frac{q}{2N_t\sqrt{n_t}}, \frac{q}{2D_t\sqrt{n_t}}, \frac{q}{nN^2\|\boldsymbol{g}^{-1}\|}\}$. Now, we consider the following column lattice $\mathcal{M}_t$:

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

where I_{n_t} is the identity matrix of 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 $\iota(X^{i2^t}[\mathrm{Tr}_{K/K_t}([\boldsymbol{h}/\boldsymbol{g}]_q/2^t]_q))$ for $0 \le i < n/2^t$. In other words, for $[\mathrm{Tr}_{K/K_t}([\boldsymbol{h}/\boldsymbol{g}]_q)/2^t]_q = \sum_{j=0}^{n_t-1} f_j X^{j2^t}$, the i-th column of Λ_t is of the form $(-f_{n_t-i}, \cdots, -f_{n_t-1}, f_0, \cdots f_{n_t-i-1})^T$.

Using the BKZ algorithm with block size β, one can obtain an element in $\mathcal{M}_t$

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

with $\|\boldsymbol{u}_t\| \le 2\beta^{\frac{n_t-1}{2(\beta-1)}+\frac{3}{2}}\det(\mathcal{M}_t) = 2\beta^{\frac{n_t-1}{2(\beta-1)}+\frac{3}{2}}\sqrt{q}$ [HPS11]. Take $\boldsymbol{c} = \sum_{i=0}^{n_t-1} u_i X^{i2^t}$ $\in \mathbb{Z}[X^{2^t}]/\langle X^n+1\rangle$. Then we have $[\boldsymbol{c} \cdot [\mathrm{Tr}_{K/K_t}([\boldsymbol{h}/\boldsymbol{g}]_q)/2^t]_q]_q = \sum_{i=0}^{n_t-1} u_{n_t+i} X^{i2^t}$ $\in \mathbb{Z}[X^{2^t}]/\langle X^n+1\rangle$. Moreover, if we choose t such that

$$2\beta^{\frac{n_t}{2(\beta-1)}+\frac{3}{2}}\sqrt{q} \le B_t, \tag{1}$$

then $\|\boldsymbol{c}\|$ and $\|\boldsymbol{c} \cdot \mathrm{Tr}_{K/K_t}([\boldsymbol{h}/\boldsymbol{g}]_q)]_q\|$ satisfy

$$\|\boldsymbol{c}\| < \|\boldsymbol{u}_t\| \le 2\beta^{\frac{n_t-1}{2(\beta-1)}+\frac{3}{2}}\sqrt{q} \le B_t \le \frac{q}{2N_t\sqrt{n_t}}$$
$$\|\boldsymbol{c} \cdot \mathrm{Tr}_{K/K_t}([\boldsymbol{h}/\boldsymbol{g}]_q)]_q\| < \|\boldsymbol{u}_t\| \le 2\beta^{\frac{n_t-1}{2(\beta-1)}+\frac{3}{2}}\sqrt{q} \le B_t \le \frac{q}{2D_t\sqrt{n_t}}.$$

In other words, $\boldsymbol{c}$ satisfies the conditions of Lemma 2. Therefore, $\boldsymbol{c}$ is in $\langle \mathrm{N}_{K/K_t}(\boldsymbol{g})\rangle \subset \langle \boldsymbol{g}\rangle$. Note that $\boldsymbol{c}$ is of the form $\boldsymbol{c} = \boldsymbol{d}\cdot \mathrm{N}_{K/K_t}(\boldsymbol{g}) = \boldsymbol{d'g} \in R_t$.

Finally, we have constructed an algorithm to find an element $\boldsymbol{c} = \boldsymbol{d}\mathrm{N}_{K/K_t}(\boldsymbol{g})$ with the size of it smaller than $\frac{q}{2N_t\sqrt{n_t}} < \frac{q}{2N\sqrt{n_t}}$ from $[\boldsymbol{h}/\boldsymbol{g}]_q$. By multiplying $\boldsymbol{c}$ to $\boldsymbol{f} = [\boldsymbol{h}/\boldsymbol{g}]_q$, one can obtain an element $[\boldsymbol{dh}\mathrm{N}_{K/K_t}(\boldsymbol{g})\boldsymbol{g}^{-1}]_q$. Since the Euclidean size of $\boldsymbol{dh}\mathrm{N}_{K/K_t}(\boldsymbol{g})\boldsymbol{g}^{-1}$ is smaller than $\|\boldsymbol{d}\mathrm{N}_{K/K_t}(\boldsymbol{g})\| \cdot \|\boldsymbol{h}\| \cdot \|\boldsymbol{g}^{-1}\| n \leq \frac{q}{2N_t\sqrt{n_t}} \cdot N \cdot \|\boldsymbol{g}^{-1}\| n \leq \frac{q}{nN^2\|\boldsymbol{g}^{-1}\|} \cdot N \cdot \|\boldsymbol{g}^{-1}\| n \leq \frac{q}{2N\sqrt{n}}$, $[\boldsymbol{c}\cdot\boldsymbol{f}]_q = \boldsymbol{dh}\mathrm{N}_{K/K_t}(\boldsymbol{g})\boldsymbol{g}^{-1}$. The second inequality comes from $B_t = \min\{\frac{q}{2N_t\sqrt{n_t}}, \frac{q}{2D_t\sqrt{n_t}}, \frac{q}{nN^2\|\boldsymbol{g}^{-1}\|}\}$ by assumption. Hence, a pair $(\boldsymbol{c}, [\boldsymbol{c}\cdot\boldsymbol{f}]_q)$ is a solution of $NTRU_{\phi_n,q,N,D,B}$.

Running time of this procedure is dominated by that of BKZ algorithm with block size β, which is $\mathrm{poly}(n, \log q)\cdot \mathcal{C}_{HKZ}(\beta)$ times where $\mathcal{C}_{HKZ}(\beta) = 2^{O(\beta)}$ is the cost of HKZ-reduction in dimension β [ADRSD14,HPS11].

Hence, if there exist $\beta > 0$ and $t \in \mathbb{Z}$ satisfying equation (1), one can solve the $NTRU_{\phi_n,q,N,D,B}$.

Since $B_t = \min\{\frac{q}{2D_t\sqrt{n}}, \frac{q}{2N_t\sqrt{n}}, \frac{q}{2nN^2\|\boldsymbol{g}^{-1}\|\sqrt{n}}\}$, B_t is asymptoctically $\frac{q}{2N_t\sqrt{n}}$. When $B_t = \frac{q}{2N_t\sqrt{n}}$, to check the above condition of β and t is satisfied, we have the equivalence equation:

$$
\begin{aligned}
& 2\beta^{\frac{n_t}{2(\beta-1)}+\frac{3}{2}}\sqrt{q} \leq \frac{q}{2N_t\sqrt{n_t}} \\
\Leftrightarrow\ & \left(\frac{n_t}{2(\beta-1)} + \frac{3}{2}\right)\log\beta + \log D_t - \log D + \frac{\log n_t}{2} + 2 < \frac{\log q}{2} - \log N
\end{aligned}
$$

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

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

Then the left hand side is asymptotic to the following:

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

where the last approximation comes from the arithmetic-geometric mean. It implies that if one choose $\beta = \frac{n}{(\log q)^{2-\epsilon}}$, for some $0 < \epsilon < 2$, then the last value is smaller than $(1/2 - a)\log q$ asymptotically. Hence, one can hold the results.

□

4 Application to GGH

In this section, we explain an attack algorithm to solve the GDDH problem of GGH scheme without low level encodings of zero.

4.1 The GGH Scheme

First, we briefly recall the Garg *et al.* construction. We refer to the original paper [GGH13] 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 base ring
m: the number of level-κ encodings of zero in public parameters
σ: the basic Gaussian parameter for drawing the ideal generator $\boldsymbol{g}$
σ': the Gaussian parameter for sampling level-zero elements
σ^*: the Gaussian parameter for constructing nonzero level elements

Instance generation: $(\mathsf{params}, \boldsymbol{p}_{zt}) \leftarrow \mathsf{InstGen}(1^\lambda, 1^\kappa)$.

For given λ and κ, determine the parameter (σ, σ', q, n) to satisfy the above conditions and output $(\mathsf{params}, \boldsymbol{p}_{zt})$.

Sample $\boldsymbol{g} \leftarrow \mathcal{D}_{R,\sigma}$ until $\|\boldsymbol{g}\|, \|\boldsymbol{g}^{-1}\| \leq n^2$ and $\mathcal{I} = \langle \boldsymbol{g} \rangle$ is a prime ideal in R.

Sample $\boldsymbol{z} \leftarrow R_q$.

Sample $X = \{\boldsymbol{b}_i \boldsymbol{g}\} \leftarrow \mathcal{D}_{\mathcal{I},\sigma'}$ and set a level-κ encoding of 0, $\boldsymbol{x}_i = \left[\dfrac{\boldsymbol{b}_i \boldsymbol{g}}{\boldsymbol{z}^\kappa}\right]_q$

for each $i \leq m$.

Sample $\boldsymbol{h} \leftarrow \mathcal{D}_{R,\sqrt{q}}$ and set a zero-testing parameter $\boldsymbol{p}_{zt} = \left[\dfrac{\boldsymbol{h}}{\boldsymbol{g}} \boldsymbol{z}^\kappa\right]_q$.

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

Sampling level-zero encodings: $\boldsymbol{a} \leftarrow \mathsf{samp}(\mathsf{params})$.
Sample $\boldsymbol{a} \leftarrow D_{\mathcal{I},\sigma'}$.

Encodings at higher levels: $\boldsymbol{c}_i \leftarrow \mathsf{enc}(\mathsf{params}, i, \boldsymbol{c})$.
Given a level-j encoding $\boldsymbol{c}$ for $j < i$, compute $\boldsymbol{c}_i = \left[\dfrac{\boldsymbol{c}'}{\boldsymbol{z}^{i-j}}\right]_q$, where $\boldsymbol{c}' - \boldsymbol{c} \in \langle \boldsymbol{g} \rangle$ and $\|\boldsymbol{c}'\| < \sigma^*$.

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

Zero-testing: $\mathsf{isZero}(\mathsf{params}, \boldsymbol{p}_{zt}, \boldsymbol{c}) \stackrel{?}{=} 0/1$.
Given a level-κ encoding $\boldsymbol{c}$, return 1 if $\|[\boldsymbol{p}_{zt} \cdot \boldsymbol{c}]_q\|_\infty < q^{3/4}$, and return 0 otherwise.

Extraction: $sk \leftarrow \mathsf{ext}(\mathsf{params},\ \boldsymbol{p}_{zt}, \boldsymbol{c})$.
Given a level-κ encoding $\boldsymbol{c}$, compute $MSB_{\log q/4-\lambda}([\boldsymbol{p}_{zt} \cdot \boldsymbol{c}]_q)$.

4.2 Hardness Assumptions

We recall the definition of the Graded Decisional Diffie-Hellman problem (GDDH) and Graded Computational Diffie-Hellman problem (GCDH) on which the security of GGH scheme relies [GGH13]. These do not seem to be reducible to more classical assumptions in generic ways.

GDDH, ext-GCDH, GCDH.
For an adversary A and parameters λ, κ, we consider the following process in the GGH scheme.
1. Choose $(q,\ \{\boldsymbol{x}_i\},\ \boldsymbol{p}_{zt}) \leftarrow \mathsf{InstGen}(1^\lambda, 1^\kappa)$.
2. Sample $\boldsymbol{m}_j \leftarrow \mathsf{samp}(\mathsf{params})$ for each $0 \le j \le \kappa$.
3. Set $\boldsymbol{u}_j = \dfrac{\boldsymbol{a}_j}{\boldsymbol{z}} \leftarrow \mathsf{enc}(\mathsf{params},\ 1,\ \boldsymbol{m}_\mathsf{j})$ for all $0 \le j \le \kappa$.
4. Choose $\boldsymbol{r} \leftarrow D_{R,\sigma'}$.
5. Sample $\rho_j \leftarrow \{0,1\}$ for $1 \le j \le m$
6. Set $\hat{\boldsymbol{u}} = \left[\boldsymbol{a}_0 \times \prod_{i=1}^{\kappa} \boldsymbol{u}_i + \sum_j \rho_j \boldsymbol{x}_j\right]_q$.
7. Set $\boldsymbol{u} = \left[\boldsymbol{r} \times \prod_{i=1}^{\kappa} \boldsymbol{u}_i + \sum_j \rho_j \boldsymbol{x}_j\right]_q$.

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

$$\{q, \{\boldsymbol{x}_i\}, \boldsymbol{p}_{zt}, \boldsymbol{u}_0, \ldots, \boldsymbol{u}_\kappa\}.$$

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

$$\{q, \{\boldsymbol{x}_i\}, \boldsymbol{p}_{zt}, \boldsymbol{u}_0, \ldots, \boldsymbol{u}_\kappa\}.$$

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

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

4.3 Attack to GGH

Considering GGH13, one can notice that the theorem in section 3 can be applied to solve the GCDH problem, which is the security problem of the GGH scheme. More precisely, suppose we have

$$\{q,\ \{\boldsymbol{x}_i\},\ \boldsymbol{p}_{zt},\ \boldsymbol{u}_0, \cdots, \boldsymbol{u}_\kappa\}.$$

Additionally, we assume that we have a pair of level-0 encoding $\bar{\boldsymbol{m}} \notin \langle \boldsymbol{g} \rangle$ and its level-1 encoding $\boldsymbol{b} = \left[\dfrac{\bar{\boldsymbol{m}} + \boldsymbol{a}\boldsymbol{g}}{\boldsymbol{z}}\right]_q$. Our attack algorithm consists of three steps:

- First, find a small element $\boldsymbol{cg} \in \langle \boldsymbol{g} \rangle$.
- Next, compute a small level-1 encoding of $\bar{\boldsymbol{m}}^{-1}$ using the $\bar{\boldsymbol{m}}, \boldsymbol{cg}$
- Last, recover a element $\boldsymbol{F}$ in $R = \mathbb{Z}[X]/\langle X^n + 1 \rangle$ such that $\boldsymbol{F} - \boldsymbol{m}_0 \in \langle \boldsymbol{g} \rangle$.

Finally, we can compute $\boldsymbol{m'}$, which is a level-κ encoding of $\prod_{i=0}^{\kappa} \boldsymbol{m}_i + \langle \boldsymbol{g} \rangle$ using $\boldsymbol{F}$, $\boldsymbol{u}_i$, and $\boldsymbol{x}_1$. Then it becomes a solution of 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 $\langle \boldsymbol{g} \rangle$

Note that $\|\bar{\boldsymbol{m}} + \boldsymbol{\alpha g}\|, \|\boldsymbol{b}_i \boldsymbol{g}\|, \|\boldsymbol{a}_i\| \leq \sigma^* \sqrt{n} \leq n^{3.5}$ and $\|\bar{\boldsymbol{m}}\| \leq \sigma' \sqrt{n} \leq n^3$ with overwhelming probability. For convenience, we use the notation G_t to denote $\mathrm{Gal}(K/K_t)$. Considering $[\boldsymbol{u}_1^{\kappa}/\boldsymbol{x}_1]_q = [\boldsymbol{a}_1^{\kappa}/\boldsymbol{b}_1 \boldsymbol{g}]_q$, the size of denominator and numerator is bounded by $n^{3.5\kappa}\sqrt{n}^{\kappa-1} < n^{4\kappa}$ and $n^{3.5}$, respectively. Using the algorithm of Theorem 2 to several $[\boldsymbol{a}_I/\boldsymbol{b}_i \boldsymbol{g}]_q := [\boldsymbol{a}_{i_1} \cdots \boldsymbol{a}_{i_\kappa}/\boldsymbol{b}_j \boldsymbol{g}]_q$, for $I = [i_1, \cdots, i_\kappa]$, $i_1, \cdots, i_\kappa \in \{0, \cdots, \kappa\}$ and $j \in \{1, \cdots, m\}$, one can recover several multiples $\boldsymbol{c}_I \boldsymbol{b'_j} \boldsymbol{g'} \boldsymbol{b}_j \boldsymbol{g}$ of $\mathrm{N}_{K/K_t}(\boldsymbol{g})$, where $\boldsymbol{b'_j} = \prod_{\sigma \in G_t \setminus \{id\}} \sigma(\boldsymbol{b_j})$ and $\boldsymbol{g'} = \prod_{\sigma \in G_t \setminus \{id\}} \sigma(\boldsymbol{g})$. Multiplying it to $[\boldsymbol{a}_I/\boldsymbol{b}_j \boldsymbol{g}]_q$, one can obtain $A_{I,j} = \boldsymbol{a}_I \boldsymbol{c}_I \boldsymbol{b'_j} \boldsymbol{g'}$. We remark that $A_{I,j}$ is in $R \setminus R_1$, because $A_{I,j}$ is not fixed for any subgroup of G_t except trivial group. Moreover, although $A_{I,j}$ is not in $\langle \boldsymbol{g} \rangle$, for $\delta \in G_t \setminus \{id\}$, $\delta(A_{I,j}) = \delta(\boldsymbol{a}_I \boldsymbol{c}_I \boldsymbol{b'_j} \boldsymbol{g'}) = \delta(\boldsymbol{a}_I \boldsymbol{c}_I) \cdot \prod_{\sigma \in G_t \setminus \{\delta\}} \sigma(\boldsymbol{bg}) \in \langle \boldsymbol{g} \rangle$. One can easily see that $\{\delta(A_{I,j})\}_{\delta \in G_t \setminus \{id\}}$ only have a common factor $\boldsymbol{g}$. Therefore, using $\{\delta(A_{I,j})\}_{\delta \in G_t \setminus \{id\}}$, we recover a basis matrix of the ideal lattice of $\langle \boldsymbol{g} \rangle$. Using $\mathrm{N}_{K/K_t}(\boldsymbol{a})$ for $\boldsymbol{a} \in \langle \boldsymbol{g} \rangle$, which is a multilple of $\mathrm{N}_{K/K_t}(\boldsymbol{g})$, one can also recover a basis matrix of the ideal lattice of $\langle \mathrm{N}_{K/K_t}(\boldsymbol{g}) \rangle$. Now, using β block-BKZ algorithm [HPS11], one can obtain an element $\boldsymbol{cg} \in \langle \mathrm{N}_{K/K_t}(\boldsymbol{g}) \rangle$ such that $\|\boldsymbol{cg}\| \leq 2\beta^{\frac{n_t - 1}{2(\beta-1)} + \frac{3}{2}} \cdot n^{2^{t+1}}$, which has a optimized value smaller than $2\beta^{\sqrt{\frac{n \log_\beta n}{(\beta-1)} + \frac{3}{2}}}$ when $t = \left\lceil \frac{1}{2} \log \frac{n}{2\beta \log_\beta n} \right\rfloor$.

4.3.2 Step 2: Computing a small level-1 encoding of $\bar{\boldsymbol{m}}^{-1}$

Using a pair $\left(\bar{\boldsymbol{m}}, \boldsymbol{b} = \left[\frac{\bar{\boldsymbol{m}} + \boldsymbol{ag}}{\boldsymbol{z}} \right]_q \right)$, one can recover a level-1 encoding of 1 as follows. Since we know a basis matrix of $\langle \boldsymbol{g} \rangle$, one can compute $\hat{\boldsymbol{e}}$ such that $\hat{\boldsymbol{e}} \bar{\boldsymbol{m}} + \hat{\boldsymbol{e}}' \boldsymbol{cg} = 1$ for some $\hat{\boldsymbol{e}}' \in R$. Then, $\boldsymbol{e} := (\hat{\boldsymbol{e}} \bmod \boldsymbol{cg})$ and $\boldsymbol{e}^{\kappa} := (\hat{\boldsymbol{e}}^{\kappa} \bmod \boldsymbol{cg})$ are the inverses of $\bar{\boldsymbol{m}}$ and $\bar{\boldsymbol{m}}^{\kappa}$ in $R/\langle \boldsymbol{g} \rangle$, respectively. Moreover, these size are smaller than $\|\boldsymbol{cg}\| n/2$.

4.3.3 Step 3: Computing the $\boldsymbol{m'}$

We refer to Section 6.3.3 in [GGH13] to solve the GCDH problem with short vector $\boldsymbol{cg} \in \langle \boldsymbol{g} \rangle$. We explain how to use $\boldsymbol{cg}$ in order to solve the GCDH problem in

the GGH scheme. First, by applying Theorem 2 to $\boldsymbol{b}^\kappa/\boldsymbol{x}_1 = (\bar{\boldsymbol{m}}+\boldsymbol{ag})^\kappa/\boldsymbol{b}_1\boldsymbol{g}$, one can obtain $\boldsymbol{d}(\bar{\boldsymbol{m}}+\boldsymbol{ag})^\kappa$ and $\boldsymbol{db}_1\boldsymbol{g}$. Now compute $\boldsymbol{G} \in R$ such that $\boldsymbol{d}(\bar{\boldsymbol{m}}+\boldsymbol{ag})^\kappa - \boldsymbol{Gdb}_1\boldsymbol{g} = \boldsymbol{d}(\bar{\boldsymbol{m}}+\boldsymbol{ag})^\kappa \bmod \boldsymbol{db}_1\boldsymbol{g}$ and also compute $\boldsymbol{b}' = \boldsymbol{b}^\kappa - \boldsymbol{Gx}_1$. Similarly, compute $\boldsymbol{G}' \in R$ such that $\boldsymbol{b}'' = \boldsymbol{b}^{\kappa-1}\boldsymbol{u}_0 - \boldsymbol{G}'\boldsymbol{x}_1$. By using $\boldsymbol{u}_0, \boldsymbol{u}_1, \ldots, \boldsymbol{u}_\kappa$, $\boldsymbol{cg}$, $\boldsymbol{b}$, $\boldsymbol{e}$, $\boldsymbol{e}^\kappa$, and $\boldsymbol{p}_{zt}$, one can obtain the following zero-testing values $\boldsymbol{f}$ and $\boldsymbol{f}_0$:

$$\boldsymbol{f} := \iota\left(\left[\boldsymbol{e}^\kappa \cdot \boldsymbol{b}' \cdot \boldsymbol{p}_{zt} \cdot \boldsymbol{cg}\right]_q\right) = \iota\left(\left[\boldsymbol{e}^\kappa \cdot (\bar{\boldsymbol{m}}+\boldsymbol{ag})^\kappa \bmod \boldsymbol{b}_1\boldsymbol{g}\cdot\boldsymbol{h}\cdot\boldsymbol{c}\right]_q\right)$$
$$\boldsymbol{f}_0 := \iota\left(\left[(\boldsymbol{e}^{\kappa-1} \bmod \boldsymbol{cg})\cdot \boldsymbol{b}'' \cdot \boldsymbol{p}_{zt}\cdot\boldsymbol{cg}\right]_q\right) = \iota\left(\left[\boldsymbol{e}^{\kappa-1} \bmod \boldsymbol{cg}\cdot(\bar{\boldsymbol{m}}+\boldsymbol{ag})^{\kappa-1}\boldsymbol{a}_0 \bmod \boldsymbol{b}_1\boldsymbol{g}\cdot\boldsymbol{h}\cdot\boldsymbol{c}\right]_q\right).$$

Since the size of $\boldsymbol{f}$ is smaller than $\|\boldsymbol{cg}\|^2 \cdot n/2 \cdot \|\boldsymbol{b}_1\boldsymbol{g}\| \cdot n/2 \cdot \|\boldsymbol{h}\|\|\boldsymbol{g}^{-1}\| \cdot n^2 \leq 4\beta^{4\cdot\sqrt{\frac{n\log_\beta n}{(\beta-1)}}+3} n^9\sqrt{q}$, it is asymptotically smaller than $q/2$ when $\beta = \lambda^{1-\gamma}$ for some $0 < \gamma < 1$ and $\boldsymbol{f}$ is actually $\boldsymbol{e}^\kappa \cdot (\bar{\boldsymbol{m}}+\boldsymbol{ag})^\kappa \bmod \boldsymbol{b}_1\boldsymbol{g}\cdot\boldsymbol{h}\cdot\boldsymbol{c}$ in R. Then $\boldsymbol{f}$ is of the form $(1+\boldsymbol{Jg})\boldsymbol{hc}$ for some $\boldsymbol{J} \in R$. On the same condition, $\boldsymbol{f}_0$ has the same bound and is of the form $(\boldsymbol{m}_0+\boldsymbol{J}'\boldsymbol{g})\boldsymbol{hc}$ for some $\boldsymbol{J}' \in R$.

Assuming that $\boldsymbol{f}$ has an inverse in $R/\langle(\boldsymbol{g})\rangle$, we can compute $\boldsymbol{F} := \boldsymbol{f}_0/\boldsymbol{f} = \boldsymbol{m}_0 \bmod \langle\boldsymbol{g}\rangle$. Then, $\boldsymbol{F}$ is a lelvel-0 enconding of $\boldsymbol{m}_0$. Note that we are given a top level encoding of zero, $x_1 = \left[\frac{\boldsymbol{b}_1\boldsymbol{g}}{\boldsymbol{z}^\kappa}\right]_q$. Using the alogirhm of Theorem 2 to $[\prod_{i=1}^{\kappa}\boldsymbol{u}_i/\boldsymbol{x}_1]_q$, we can recover $\boldsymbol{db}_1\boldsymbol{g}$ and $\boldsymbol{d}\prod_{i=1}^{\kappa}\boldsymbol{a}_i$. Now compute $(\boldsymbol{F}\cdot\boldsymbol{d}\prod_{i=1}^{\kappa}\boldsymbol{a}_i) \bmod \boldsymbol{db}_1\boldsymbol{g}$. It is of the form $\boldsymbol{F}\cdot\boldsymbol{d}\prod_{i=1}^{\kappa}\boldsymbol{a}_i - \boldsymbol{Gdb}_1\boldsymbol{g}$ for some $\boldsymbol{G} \in R$. Since $\boldsymbol{d}$ is the common factor, it is same to $\boldsymbol{d}\cdot((\boldsymbol{F}\cdot\prod_{i=1}^{\kappa}\boldsymbol{u}_i) \bmod \boldsymbol{b}_1\boldsymbol{g}) = \boldsymbol{d}\cdot(\boldsymbol{F}\cdot\prod_{i=1}^{\kappa}\boldsymbol{a}_i - \boldsymbol{Gb}_1\boldsymbol{g})$. We remark that the size of $(\boldsymbol{F}\cdot\prod_{i=1}^{\kappa}\boldsymbol{a}_i) \bmod \boldsymbol{b}_1\boldsymbol{g}$ is bounded by $\|\boldsymbol{b}_1\boldsymbol{g}\|n < n^5$ and it is an element of a coset $\prod_{i=0}^{\kappa}\boldsymbol{m}_i + \langle\boldsymbol{g}\rangle$. Now compute $\boldsymbol{F}\cdot\prod_{i=1}^{\kappa}\boldsymbol{u}_i - \boldsymbol{Gx}_1$. Then it has the following form

$$\frac{(\boldsymbol{F}\cdot\prod_{i=1}^{\kappa}\boldsymbol{a}_i) \bmod \boldsymbol{b}_1\boldsymbol{g}}{z^\kappa}.$$

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

Corollary 3 *Given* $\{n, q, \{\boldsymbol{x}_i\}, \boldsymbol{m}, \boldsymbol{b}, \boldsymbol{p}_{zt}, \boldsymbol{u}_0, \cdots, \boldsymbol{u}_\kappa\}$ *of the GGH scheme parameters, where* n *is* $\Theta(\lambda^2)$, $\log q = \Theta(\lambda)$, $\boldsymbol{x}_i$ *is a level-*κ *encoding of zero,* $\boldsymbol{m}$ *is a level-*0 *nonzero encoding,* $\boldsymbol{b}$ *is a level-1 encoding of* $\boldsymbol{m}$ *and* $\boldsymbol{u}_i$ *is a level-*1 *encoding of* $\boldsymbol{m}_i$*, one can take some* $0 < \epsilon < 2$ *and* $0 < \gamma < 1$ *assymtoticaly which*

leads to compute an $\mathsf{enc}_\kappa(\prod_{i=0}^{\kappa} \boldsymbol{m}_i)$ *which is a solution of GCDH problem in the GGH scheme in the* $\max\{2^{O(n/\log^{2-\epsilon} q)}, 2^{O(\lambda^{1-\gamma})}\}$.

5 Conclusion

After GGH scheme providing encoding of zero is known to be insecure, the variant of NTRU has received a lot of attention because of the security grounding of GGH scheme without encoding of zero. In this work, we described how to find a small solution of the variant of NTRU using reduction technique. By applying the method to GGH scheme, we could attack the GCDH problem in GGH scheme. Therefore, our results imply that there is no guarantee for the security of the GGH scheme not only when we are given a small encoding of zero but also when we are not given.

References

[ACLL14] Martin R Albrecht, Catalin Cocis, Fabien Laguillaumie, and Adeline Langlois. Implementing candidate graded encoding schemes from ideal lattices. In *Advances in Cryptology–ASIACRYPT 2015*, pages 752–775. Springer, 2014.

[ADRSD14] Divesh Aggarwal, Daniel Dadush, Oded Regev, and Noah Stephens-Davidowitz. Solving the shortest vector problem in 2^n time via discrete gaussian sampling. *arXiv preprint arXiv:1412.7994*, 2014.

[BLLN13] Joppe W Bos, Kristin Lauter, Jake Loftus, and Michael Naehrig. Improved security for a ring-based fully homomorphic encryption scheme. In *Cryptography and Coding*, pages 45–64. Springer, 2013.

[BS02] D. Boneh and A. Silverberg. Applications of multilinear forms to cryptography. *Contemporary Mathematics*, 324:71–90, 2002.

[CHL+15] Jung Hee Cheon, Kyoohyung Han, Changmin Lee, Hansol Ryu, and Damien Stehlé. Cryptanalysis of the multilinear map over the integers. In *Advances in Cryptology–EUROCRYPT 2015*, pages 3–12. Springer, 2015.

[CLR15] Jung Hee Cheon, Changmin Lee, and Hansol Ryu. Cryptanalysis of the new clt multilinear maps. *IACR-ePrint (http://eprint. iacr. org/2015/934)*, 2015.

[CLT13] Jean-Sébastien Coron, Tancrede Lepoint, and Mehdi Tibouchi. Practical multilinear maps over the integers. In *Advances in Cryptology–CRYPTO 2013*, pages 476–493. Springer, 2013.

[CLT15] Jean-Sebastien Coron, Tancrede Lepoint, and Mehdi Tibouchi. New multilinear maps over the integers. In *Advances in Cryptology–CRYPTO 2015*, pages 267–286. Springer, 2015.

[Cor15] Jean-Sébastien Coron. Cryptanalysis of GGH15 multilinear maps. *IACR Cryptology ePrint Archive*, 2015:1037, 2015.

[DDLL13] Léo Ducas, Alain Durmus, Tancrède Lepoint, and Vadim Lyubashevsky. Lattice signatures and bimodal gaussians. In *Advances in Cryptology–CRYPTO 2013*, pages 40–56. Springer, 2013.

[GGH13] Sanjam Garg, Craig Gentry, and Shai Halevi. Candidate multilinear maps from ideal lattices. In *Eurocrypt*, volume 7881, pages 1–17. Springer, 2013.

[GGH15] Craig Gentry, Sergey Gorbunov, and Shai Halevi. Graph-induced multilinear maps from lattices. In *Theory of Cryptography*, pages 498–527. Springer, 2015.

[HHGP+03] Jeffrey Hoffstein, Nick Howgrave-Graham, Jill Pipher, Joseph H Silverman, and William Whyte. Ntrusign: Digital signatures using the ntru lattice. In *Topics in cryptologyCT-RSA 2003*, pages 122–140. Springer, 2003.

[HJ15] Yupu Hu and Huiwen Jia. Cryptanalysis of GGH map. Technical report, Cryptology ePrint Archive, Report 2015/301, 2015.

[HPS98] Jeffrey Hoffstein, Jill Pipher, and Joseph H Silverman. Ntru: A ring-based public key cryptosystem. In *Algorithmic number theory*, pages 267–288. Springer, 1998.

[HPS11] Guillaume Hanrot, Xavier Pujol, and Damien Stehlé. Terminating bkz. *IACR Cryptology ePrint Archive*, 2011:198, 2011.

[LATV12] 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*, pages 1219–1234. ACM, 2012.

[LSS14] Adeline Langlois, Damien Stehlé, and Ron Steinfeld. Gghlite: More efficient multilinear maps from ideal lattices. In *Advances in Cryptology–EUROCRYPT 2014*, pages 239–256. Springer, 2014.

[MA16] Léo Ducas Martin Albrecht, Shi Bai. A subfield lattice attack on overstretched ntru assumptions: Cryptanalysis of some fhe and graded encoding schemes. Cryptology ePrint Archive, Report 2016/127, 2016. http://eprint.iacr.org/.

[MSZ16] Eric Miles, Amit Sahai, and Mark Zhandry. Annihilation attacks for multilinear maps: Cryptanalysis of indistinguishability obfuscation over ggh13. Cryptology ePrint Archive, Report 2016/147, 2016. http://eprint.iacr.org/.