Cryptanalysis of the Multilinear Map on the Ideal lattices

Jung Hee Cheon[1], Changmin Lee[1]

Seoul National University (SNU), Republic of Korea

Abstract. We improve the *zeroizing* attack on the multilinear map of Garg, Gentry and Halevi (GGH). Our algorithm can solve the Graded Decisional Diffie-Hellman (GDDH) problem on the GGH scheme when the dimension n of the ideal lattice $\mathbb{Z}[X]/(X^n+1)$ is $O(\kappa\lambda^2)$ as suggested for the κ-linear GGH scheme.
The zeroizing attack is to recover a basis of an ideal generated by a secret element $\boldsymbol{g} \in \mathbb{Z}[X]/(X^n+1)$ from the zero testing parameter and several encodings in public. It can solve the DLIN and subgroup decision problems, but not the GDDH problem on the GGH scheme for the suggested dimension n due to the hardness of the smallest basis problem and the shortest vector problem on the ideal lattice. In this paper, we propose an algorithm to find a short vector in the ideal lattice $\langle \boldsymbol{g} \rangle$ by applying a lattice reduction to a sublattice obtained from the Hermit Normal Form of $\langle \boldsymbol{g} \rangle$. This attack utilizes that the determinant of the lattice $\langle \boldsymbol{g} \rangle$ is not large. We further show that if $\boldsymbol{g}$ has a large residual degree, one can find a short element of $\boldsymbol{g}$ in polynomial time of n. In order to resist the proposed attacks, it is required that $n = \tilde{\Omega}(\kappa^2\lambda^3)$ and the positive generator of $\langle \boldsymbol{g} \rangle \cap \mathbb{Z}$ is large enough.

Keywords: Multilinear maps, graded encoding schemes, zeroizing attack, Hermite normal form

1 Introduction

Multilinear Maps. After Boneh and Silverberg [BS02] investigated 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 cryptographic multilinear maps are suggested by Coron, Lepoint, and Tibouchi (CLT) [CLT13]. The GGH and CLT approximate multilinear maps are constructed based on ideal lattices and a variant of the approximate greatest common divisor problem, respectively. They lead to various applications [ABP14] [Att14,BP13,BLMR13,GGHZ14,GLW14,Zha14,Zim14] to name a few. Some of them are based of the hardness of the GDDH (Graded Decisional Diffie-Hellman) problem on multilinear maps, and the others are based on Subgroup Membership

(SubM), Decision Linear (DLIN) or External DH (XDH) problems on multilinear maps.

In the first public draft of [GGH13], the SubM, DLIN, and XDH problems were regarded to be hard on the GGH constructions, but it was reported in the later version that they can be solved by so called a *zeroizing attack* introduced by the authors of [GGH13]. The zeroizing attack is to recover a basis of an ideal generated by a secret element $\boldsymbol{g} \in \mathbb{Z}[X]/(X^n+1)$ from the zero testing parameter and several encodings in public. It cannot solve the GDDH problem on the GGH scheme for the suggested dimension n due to the hardness of the smallest basis problem and the shortest vector problem on the ideal lattice.

In case of the CLT scheme, it has been claimed [CLT13] that the zeroizing attack can not be applied directly and so the SubM, DLIN, XDH problems remain hard on their constructions. However, an adaptation of the zeroizing attack to the CLT constructions was proposed by Cheon et. al [CHL$^+$14] and leads to a total break of the CLT scheme (i.e. the secret elements are revealed) as well as the SubM, DLIN, and XDH problems.

To resist this attack against the CLT scheme, Gentry, Halevi, Maji, and Sahai [GHMS14], and Boneh, Wu and Zimmerman [BWZ14] suggested two candidate fixes of the CLT scheme. However, Coron, Lepoint and Tibouchi [CLT14] showed that two fixes are still not secure by extending *Cheon et. al's attack* in [CHL$^+$14]. So far, no multilinear map constructions are known to provide hardness of the SubM, DLIN or XDH problems and many applications based on them lost their meanings.

Contribution. We improve the zeroizing attack on the GGH scheme by introducing two algorithms to find a shorter vector on the ideal lattice than the previous. Our attack scenario is as follows: First, we apply the zeroizing attack as in [GGH13] to find a basis of the ideal lattice $\langle \boldsymbol{g} \rangle$ of $\mathbb{Z}[X]/(X^n+1)$ in the GGH scheme. Second, we show that a vector in $\langle \boldsymbol{g} \rangle$ of size $< q^{3/8}/(2n^2)$ can be used to solve the Graded Decisional Diffie-Hellman (GDDH) problem on the GGH scheme in polynomial time. Finally, to find this short vector, we compute the Hermit Normal Form (HNF for short) of this ideal lattice. We are done if it has a basis vector of size $< q^{3/8}/(2n^4)$, whose probability will be analyzed later. Otherwise we use our *reduction algorithm on a sublattice* to find a short vector of $\langle \boldsymbol{g} \rangle$. We show that this second algorithm finds a short vector $< q^{3/8}/(2n^2)$ in polynomial time of n, which is a result of the BKZ algorithm, when $n = O(\kappa\lambda^2)$ as suggested for the κ-linear GGH scheme with overwhelming probability (with exception of about 2^{-n} probability).

Our strategy to find a short vector of $\langle \boldsymbol{g} \rangle$ starts with computing the Hermit Normal Form $\mathrm{HNF}(\boldsymbol{g})$ of the ideal lattice $\langle \boldsymbol{g} \rangle$. Our first approach comes from a theoretical result. We observe that the Hermit Normal Form of an ideal lattice is of very special form, and prove that the algebraic norm of a prime ideal $\boldsymbol{g} \in \mathbb{Z}[x]/(X^n+1)$ over $\mathbb{Q}$ is p^f for some integral prime p and a positive integer f. Then we have

$$\mathrm{HNF}(\boldsymbol{g}) = \begin{pmatrix} I_{n-f} & O \\ A & pI_f \end{pmatrix}$$

for $A \in \mathbb{Z}^{(n-f)\times f}$, where I_f and I_{n-f} are the identity matrix of size f and $(n-f)$, respectively. Since $\mathrm{N}(\boldsymbol{g}) = p^f = \det(\mathrm{HNF}(\boldsymbol{g})) \leq (\sigma\sqrt{n})^n$ with overwhelming probability, size p of the last f columns of $\mathrm{HNF}(\boldsymbol{g})$ are less than $(\sigma\sqrt{n})^{n/f}$. This value is asymptotically less than $q^{3/8}/(2n^4)$ when $f \geq \sqrt{n}$. It is well-known that f is the order of p modulo $2n$ with $p^f \equiv 1 \mod 2n$. So $f \geq \sqrt{n}$ is satisfied with high probability if $p \mod 2n$ is uniformly distributed. It would be interesting to see how $p \mod 2n$ is distributed when the coefficients of $\boldsymbol{g}$ follow the Gaussian distribution.

Our second algorithm is to find a short vector in the ideal lattice $\langle \boldsymbol{g} \rangle$ by applying a lattice reduction to a sublattice obtained from the Hermit Normal Form of $\langle \boldsymbol{g} \rangle$. We observe that when the determinant of the lattice $\langle \boldsymbol{g} \rangle$ is not so large, applying a lattice reduction algorithm to a sublattice could give a shorter vector within the same computational time than the original lattice. More precisely, the size of the short vector produced by lattice reduction algorithms in time $2^{O(t)}$ is about $2^{\frac{n'}{t}} \cdot \det(L)^{\frac{1}{n'}}$, when applied to a lattice L of dimension n'. So if $\det L = O(2^{n^2/t})$, this value has a minimum for $n' = \sqrt{t \log \det(L)} < n$. In general, we cannot say that the determinant of sublattice is smaller than that of lattice. However, this problem is avoidable using the HNF. By taking a sublattice generated by the last $n' = \sqrt{t \log \det(L)}$ columns of $\mathrm{HNF}(\boldsymbol{g})$, we obtain an appropriate sublattice. Following the parameter setting proposed by GGH scheme, $n = O(\kappa\lambda^2)$, $\log q = O(\kappa\lambda)$, and $\det L \leq (n\sqrt{\lambda})^n$ with overwhelming probability. In that case, the size $2^{n'/t} \det(L')^{1/n'}$ is smaller than $\leq q^{3/8}/2n^4$ if $t > \log n\sqrt{\lambda}$. To avoid this attack, it is required that $n = \tilde{\Omega}(\kappa^2\lambda^3)$.

Open problems. To be secure against our attacks, a residual degree of prime ideal $\langle \boldsymbol{g} \rangle$ must be small. It would be an interesting problem to investigate how to sample such $\boldsymbol{g}$ efficiently while the coefficients follow the Gaussian distribution.

Organization. In Section 2, we introduce some preliminaries related to an ideal lattice and Gaussian distribution. In Section 3, we recall the GGH scheme and the GDDH problem. In Section 4, we analyze Hermite normal forms of prime ideal lattices in $\mathbb{Z}[X]/(X^n+1)$. In Section 5, we present our algorithm to solve the GDDH problem on the GGH scheme and propose new parameter setting to resist it.

2 Preliminaries

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

For an integer q, we use the notations $\mathbb{Z}_q := \mathbb{Z}/(q\mathbb{Z})$ and $R_q := \mathbb{Z}_q[X]/(X^n+1) = R/qR$. We denote by $x \bmod p$ or $[x]_p$ the number in $\mathbb{Z} \cap \left(-\frac{p}{2}, \frac{p}{2}\right]$, which is congruent to x modulo p. For $\boldsymbol{u} \in \mathbb{Z}^n$ or R, $[\boldsymbol{u}]_q$ and $\|\boldsymbol{u}\|$ denote the reduction of $\boldsymbol{u}$ modulo q and the Euclidean norm of $\boldsymbol{u}$, respectively. We use bold letters to

denote vectors or ring elements in $\mathbb{Z}^n$ or R.

Ideal Lattice. An n-dimension full-rank lattice $L \subset \mathbb{R}^n$ is the set of all $\mathbb{Z}$-linear combinations of n linearly independent vectors. Let $\det(L)$ denote the determinant of lattice L. 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 $(g_{n-1}, g_{n-2}, \ldots, g_0)$ in $\mathbb{Z}^n$, we can apply some lattice theory to the algebraic ring R and also use some algebraic ring theory to analyze $\langle \boldsymbol{g} \rangle$.

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. $\boldsymbol{u}$ is the unique representation $\boldsymbol{u} \bmod \mathcal{B} \in R$ 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 $\alpha_i \in (-1/2, 1/2]$.

When given two elements $\boldsymbol{a}$ and $\boldsymbol{b}$ in the polynomial ring R, the following lemma is useful for estimating the boundary of norm $\|\boldsymbol{ab}\|$.

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 CauchySchwartz inequality, it is smaller than $\|\boldsymbol{a}\| \cdot \|\boldsymbol{b}\|$. Since each coefficient is smaller than $\|\boldsymbol{a}\| \cdot \|\boldsymbol{b}\|$, $\|\boldsymbol{ab}\| \leq \|\boldsymbol{a}\| \cdot \|\boldsymbol{b}\| \cdot \sqrt{n}$. □

Norm of an Ideal. We define the norm of an ideal $\mathcal{I} \subset R$, $\mathrm{N}_{K/\mathbb{Q}}(\mathcal{I})$ or $\mathrm{N}(\mathcal{I})$ for short, relative to $\mathbb{Q}$ and K, by cardinality of the quotient ring $R/\mathcal{I}$. When $\mathcal{I}$ is generated by one element $\boldsymbol{h} \in R$, $\mathrm{N}(\boldsymbol{h}) := \mathrm{N}(\langle \boldsymbol{h} \rangle)$ satisfies $\mathrm{N}(\boldsymbol{h}) = \prod_{\sigma \in \mathrm{Gal}(K/Q)} \sigma(\boldsymbol{h})$.

For a prime ideal $\wp_i$, we recall $\mathrm{N}(\wp_i) = p^f$ for some integral prime $p \in \mathbb{Z}$ and a positive integer f, called a *residual degree* of $\wp_i$ with respect to K and $\mathbb{Q}$

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 $\mathcal{D}$.

Smoothing parameter. For a lattice L and real $\epsilon > 0$, a smoothing parameter $\eta_\epsilon(L)$ is defined as the smallest s satisfying $\rho_{1/s}(L^* - \{0\}) < \epsilon$, where L^* is the dual lattice of $L := \{\boldsymbol{r} \in \mathbb{R}^n; \langle \boldsymbol{r}, \boldsymbol{x} \rangle \in \mathbb{Z} \text{ for any } \boldsymbol{x} \in L\}$ for the inner product $\langle \cdot, \cdot \rangle$.

Lemma 2. *[MR07, Lemma 3] Given a lattice L of dimension n and a constant $0 < \epsilon < 1$, suppose that $\sigma \geq \eta_\epsilon(L)$. Then we have*

$$\Pr_{\boldsymbol{u} \leftarrow D_{L,\sigma}} \left(\|\boldsymbol{u}\| \geq \sigma\sqrt{n} \right) \leq \frac{1+\epsilon}{1-\epsilon} 2^{-n}$$

By Lemma 2, when $\sigma \geq \eta_\epsilon(L)$ and x is sampled from $D_{L,\sigma}$, $\|x\| \leq \sigma\sqrt{n}$ with overwhelming probability.

3 A Multilinear Map based on Ideal lattice

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-1 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 drawing the coefficient vector $\boldsymbol{r}$ during re-randomization of newly generated level-1 encodings

Garg *et al.* suggested to set the parameters satisfying the following conditions:

- $n = \tilde{O}(\kappa \cdot \lambda^2)$ to thwart lattice reduction attacks.
- $q \geq 2^{8\kappa\lambda} \cdot n^{64\kappa} \cdot \lambda^{12\kappa}$ to support functionality from [GGH13, Lemma 4].
- $m = O(n^2)$: to apply leftover hash lemma from [GGH13, Theorem 1].
- $\sigma = \sqrt{\lambda n}$ to satisfy $\sigma \geq \eta_{2^{-\lambda}}(\mathbb{Z}^n)$.
- $\sigma' = \lambda n^{3/2}$ to satisfy $\sigma' \geq \eta_{2^{-\lambda}}(\mathcal{I})$.
- $\sigma^* = 2^\lambda$ to be large enough so that the resulting distribution of rerandomization process drown the initial vector.

3.1 The GGH Scheme

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

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

Sample $\boldsymbol{g} \leftarrow D_{R,\sigma}$ until $\|\boldsymbol{g}^{-1}\| \leq n^2$ and $\mathcal{I} = \langle \boldsymbol{g} \rangle$ is a prime ideal in R.
Sample $\boldsymbol{z} \leftarrow R_q$.
Sample $\boldsymbol{a} \leftarrow D_{1+\mathcal{I},\sigma'}$ and set a level-1 encoding of 1, $\boldsymbol{y} = \left[\frac{\boldsymbol{a}}{\boldsymbol{z}}\right]_q$.
Sample $X = \{\boldsymbol{b}_i \boldsymbol{g}\} \leftarrow D_{\mathcal{I},\sigma'}$ and set a level-1 encoding of 0, $\boldsymbol{x}_i = \left[\frac{\boldsymbol{b}_i \boldsymbol{g}}{\boldsymbol{z}}\right]_q$ for each $i \leq m$.
Sample $\boldsymbol{h} \leftarrow D_{R,\sqrt{q}}$ and set a zero-testing parameter $\boldsymbol{p}_{zt} = \left[\frac{\boldsymbol{h}}{\boldsymbol{g}}\boldsymbol{z}^\kappa\right]_q$.

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

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 $\boldsymbol{c}_i = [\boldsymbol{c}\boldsymbol{y}^{i-j}]_q$.

Re-randomizing level-1 encodings: $\boldsymbol{c}' \leftarrow \mathsf{reRand}(\mathsf{params}, \boldsymbol{c})$.
Given a level-1 encoding $\boldsymbol{c}$, sample $r_i \leftarrow D_{\mathbb{Z},\sigma^*}$ for $1 \le i \le m$ and compute $\boldsymbol{c}' = [\boldsymbol{c} + \sum_{i=1}^{m} r_i \boldsymbol{x}_i]_q$.

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: $\mathsf{isZero}(\mathsf{params}, \boldsymbol{p}_{zt}, \boldsymbol{c}) =^? 0/1$.
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 $MSB_{\log q/4-\lambda}([\boldsymbol{p}_{zt} \cdot \boldsymbol{c}]_q)$.

3.2 Hardness Assumptions

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

GDDH, GCDH.
For an adversary A and parameters λ, κ, we consider the following process in the GGH scheme.
1. Choose $(\mathsf{params}, \boldsymbol{p}_{zt}) \leftarrow \mathsf{InstGen}(1^\lambda, 1^\kappa)$.
2. Sample $\boldsymbol{a}_j \leftarrow D_{R,\sigma'}$ for each $0 \le j \le \kappa$.
3. Set $\boldsymbol{u}_j \leftarrow$ reRand(params, enc(params,1,$\boldsymbol{a}_j$)) for all $0 \le j \le \kappa$.
4. Choose $\boldsymbol{b} \leftarrow D_{R,\sigma'}$.
5. Set $\hat{\boldsymbol{u}}=\boldsymbol{a}_0 \times \prod_{i=1}^{\kappa} \boldsymbol{u}_i$ and $\hat{\boldsymbol{u}}' \leftarrow \mathsf{reRand}(\mathsf{params}, \mathsf{enc}(\mathsf{params}, \kappa, \prod_{i=0}^{\kappa} \boldsymbol{a}_i))$.
6. Set $\boldsymbol{u}=\boldsymbol{b} \times \prod_{i=1}^{\kappa} \boldsymbol{u}_i$ and $\boldsymbol{u}' \leftarrow \mathsf{reRand}(\mathsf{params}, \mathsf{enc}(\mathsf{params}, \kappa, \prod_{i=1}^{\kappa} \boldsymbol{b} \cdot \boldsymbol{a}_i))$.

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

$$\{\mathsf{params}, \boldsymbol{p}_{\mathsf{zt}}, \boldsymbol{u}_0, \ldots, \boldsymbol{u}_\kappa\}.$$

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

$$\mathcal{D}_{DDH} = \{\mathsf{params}, \boldsymbol{p}_{\mathsf{zt}}, \boldsymbol{u}_0, \ldots, \boldsymbol{u}_\kappa, \hat{\boldsymbol{u}}'\} \quad \text{and} \quad \mathcal{D}_{\mathsf{R}} = \{\mathsf{params}, \boldsymbol{p}_{\mathsf{zt}}, \boldsymbol{u}_0, \ldots, \boldsymbol{u}_\kappa, \boldsymbol{u}'\}.$$

4 Hermite normal form of prime ideal lattice

In this section, we discuss about Hermite normal forms of prime ideal lattices. Hermite normal form is, by intuition, a triangularization over a principal ideal domain. A matrix with integer entries is in (column) Hermite normal form (HNF, for short) if

1. (Zero rows) All nonzero columns (columns with at least one nonzero element) are left to any columns of all zeros (all zero columns, if any, are at the right of the matrix).
2. (Triangular) The first nonzero entry from the above (called, the pivot) of a nonzero column is always strictly to the below of the pivot of the column left to it. Moreover, it is positive.
3. (Modulus Reduction) All the entries in a row left to a pivot are nonnegative and strictly smaller than the pivot.

Note that the HNF of a matrix over $\mathbb{Z}$ is unique.

In order to figure out some characteristics of HNFs of prime ideal lattices, we remind the following lemmas.

Lemma 3. *For a prime element $\boldsymbol{g}$ of R, there exists a prime p in $\mathbb{Z}$ such that $\langle \boldsymbol{g} \rangle \cap \mathbb{Z} = p\mathbb{Z}$.*

Lemma 4. *Let n be a power of 2 and $\boldsymbol{g}$ a prime element of $R = \mathbb{Z}[X]/(X^n + 1)$ with $\langle \boldsymbol{g} \rangle \cap \mathbb{Z} = p\mathbb{Z}$ for an odd prime p. Then we have $\mathrm{N}(\boldsymbol{g}) = p^f$ for the smallest positive integer f satisfying $p^f \equiv 1 \bmod 2n$.*

Lemma 5. *Given an element $\boldsymbol{g}$ of $R = \mathbb{Z}[X]/(X^n + 1)$, we have*

$$\mathrm{N}(\boldsymbol{g}) = \prod_{\sigma \in Gal(K/\mathbb{Q})} \sigma(\boldsymbol{g}) = \det[\boldsymbol{g}, x\boldsymbol{g}, \ldots, x^{n-1}\boldsymbol{g}].$$

Theorem 1. *Let n be a power of 2 and $\boldsymbol{g}$ be a prime element of $R = \mathbb{Z}[X]/(X^n + 1)$ with $\mathrm{N}(\boldsymbol{g}) = p^f$ for an odd prime p and a positive integer f. The Hermit Normal Form of $\boldsymbol{g}$ is of following form:*

$$HNF(\boldsymbol{g}) = \begin{pmatrix} I_{n-f} & O \\ A & pI_f \end{pmatrix} = \begin{pmatrix} 1 & & & & & & & \\ 0 & 1 & & & & & & \\ 0 & 0 & 1 & & & & & \\ \vdots & & & \ddots & & & & \\ 0 & 0 & 0 & \ldots & 1 & & & \\ a_{1,1} & a_{1,2} & a_{1,3} & \ldots & a_{1,n-f} & p & & \\ a_{2,1} & a_{2,2} & a_{2,3} & \ldots & a_{2,n-f} & 0 & p & \\ \vdots & & & & & \vdots & \ddots & \\ a_{f,1} & a_{f,2} & a_{f,3} & \ldots & a_{f,n-f} & 0 & 0 \ldots & p \end{pmatrix}$$

for some $a_{i,j} \in \mathbb{Z} \cap [0, p)$.

Proof. Let us denote by d_i the i-th diagonal entry of HNF($\boldsymbol{g}$). First, since $\langle \boldsymbol{g} \rangle \cap \mathbb{Z} = p\mathbb{Z}$ by Lemma 4, the ideal $\langle \boldsymbol{g} \rangle$ contains px^i for any positive integer i as well as p. Since the HNF is triangular, the i-th column itself should generate a vector corresponding to a polynomial px^{n-i} and so the i-th diagonal entry d_i is a divisor of p.

Next, we claim that $d_i = 1$ implies $d_1 = \cdots = d_{i-1} = 1$. If $d_i = 1$, $\langle \boldsymbol{g} \rangle$ contains a polynomial $\boldsymbol{f} = x^{n-i} + f_{n-i-1}x^{n-i-1} + \ldots + f_0$. For each $0 \leq j < i$ we have $x^{i-j}\boldsymbol{f} = x^{n-j} + \cdots + f_0 x^{i-j} \in \langle \boldsymbol{g} \rangle$ which implies $d_j = 1$.

Furthermore, $\mathrm{N}(\boldsymbol{g}) = \det[\boldsymbol{g}, x\boldsymbol{g}, \ldots, x^{n-1}\boldsymbol{g}] = p^f$ implies $\prod_{i=1}^{n} d_i = p^f$. Combining the above three arguments, we can conclude that $d_1 = \cdots = d_{n-f} = 1$ and $d_{n-f+1} = \cdots = d_n = 1$.

Finally, we claim that if $d_i = p$ then the i-th column of HNF($\boldsymbol{g}$)is $p\boldsymbol{e}_i$ where $\boldsymbol{e}_i$ is the i-th elementary vector. We use an induction on i reversely from n to 1. For $i = n$, it is clear that the n-th column is $p\boldsymbol{e}_n$ while $f > 0$. Suppose the claim holds for all j with $i < j \leq n$ and $d_i = p$. Then the i-th column is represented by $px^{n-i} + a_{n-i-1}x^{n-i-1} + \ldots + a_0$ for some $a_i \in \mathbb{Z}$. Since $px^{n-i} \in \langle \boldsymbol{g} \rangle$, $a_{n-i-1}x^{n-i-1} + \ldots + a_0$ must be generated by $\{\boldsymbol{h}_{i+1}, \ldots, \boldsymbol{h}_n\}$, where $\boldsymbol{h}_s$ is the s-th column of HNF($\boldsymbol{g}$) and so equal to $p\boldsymbol{e}_{n-s+1}$ by the induction hypothesis. Hence, a_i must be multiple of p and $a_i = 0$, which conclude the proof. □

5 An Attack on the GDDH problem of the GGH scheme

In this section, we propose an algorithm for the GDDH problem of the GGH scheme. Our algorithm consists of three parts. The first part is the zeroizing attack to find a basis of $\langle \boldsymbol{g} \rangle$, which is introduced in [GGH13]. The second part is to find the shortest vector of $\langle \boldsymbol{g} \rangle$ using HNF. The third part is to perform a lattice reduction algorithm on reduced dimension to solve the GDDH on the GGH scheme.

5.1 Finding a basis of $\langle \boldsymbol{g} \rangle$

First, we briefly recall the zeroizing attack on the GGH scheme. The GGH has $\{\boldsymbol{y}, \boldsymbol{x}_j, \boldsymbol{p}_{zt}, n, q\}$ as a public parameter and $\{\boldsymbol{z}, \boldsymbol{g}\}$ as a secret parameter. By publishing a zero-testing parameter $\boldsymbol{p}_{zt}$, any user can decide whether two elements encode the same coset or not: For a given level-κ encoding $\boldsymbol{u} = [\boldsymbol{c}/\boldsymbol{z}^\kappa]_q$, the quantity $[\boldsymbol{u} \cdot \boldsymbol{p}_{zt}]_q = [\boldsymbol{h} \cdot \boldsymbol{c}/\boldsymbol{g}]_q$ is small if and only if $\boldsymbol{c} \in \langle \boldsymbol{g} \rangle$, i.e., $\boldsymbol{u}$ is an encoding of zero. The existence of zero-testing parameter creates a weak point in the scheme.

The attack gets as inputs several encodings $\boldsymbol{x}_j$ of zero, one encoding $\boldsymbol{y}$ of one, and a zero testing parameter $\boldsymbol{p}_{zt}$ as follows:

- $\boldsymbol{y} = [\boldsymbol{a}/\boldsymbol{z}]_q$, a level-1 encoding of 1, namely $\boldsymbol{a} \in 1 + \mathcal{I}$ and $\boldsymbol{a}$ is small,
- $\boldsymbol{x}_j = [\boldsymbol{b}_j\boldsymbol{g}/\boldsymbol{z}]_q$, a level-1 encoding of 0, with $\boldsymbol{b}_j$ small,
- $\boldsymbol{p}_{zt} = [\boldsymbol{h}\boldsymbol{z}^\kappa/\boldsymbol{g}]_q$, $\boldsymbol{h} \in R$ appropriately small, the zero-testing parameter.

The attack consists of the following three steps. For the detail, we refer to the [GGH13].

Step 1. Compute level-κ encodings of zero and get the equations in R by multiplying by the zero-testing parameter: Let $\boldsymbol{u} = \boldsymbol{d}/\boldsymbol{z}^t$ be a level-t encoding of some message $\boldsymbol{d} \bmod \mathcal{I}$. Then

$$\begin{aligned}\boldsymbol{f}_u &= [\boldsymbol{u} \cdot \boldsymbol{x}_j \cdot \boldsymbol{p}_{zt} \cdot \boldsymbol{y}^{\kappa-t-1}]_q = \left[\frac{\boldsymbol{d}}{\boldsymbol{z}^t} \cdot \frac{\boldsymbol{b}_j \cdot \boldsymbol{g}}{\boldsymbol{z}} \cdot \frac{\boldsymbol{h}\boldsymbol{z}^\kappa}{\boldsymbol{g}} \cdot \frac{\boldsymbol{a}^{\kappa-t-1}}{\boldsymbol{z}^{\kappa-t-1}}\right]_q \\ &= \underbrace{\boldsymbol{d} \cdot \boldsymbol{b}_j \cdot \boldsymbol{h} \cdot \boldsymbol{a}^{\kappa-t-1}}_{\ll q}.\end{aligned}$$

Note that the last term in the above equation consists of only small elements, so that the equality holds without modulus reduction by q. Therefore we can obtain various multiples of $\boldsymbol{h}$ (in R) for various $\boldsymbol{u}$ and $\boldsymbol{x}_j$.

Step 2. We regard a polynomial $a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in R_q$ as a column vector $(a_{n-1}, \ldots a_1, a_0)^T \in \mathbb{Z}_q^n$. From $O(n)$ multiples of $\boldsymbol{h}$, compute a basis of $\langle \boldsymbol{h} \rangle$ in time $O(n^3)$ arithmetic operations. Using a similar procedure, compute a basis of $\langle \boldsymbol{h} \cdot \boldsymbol{g} \rangle$.

Step 3. Finally, we obtain a multiple of $\langle \boldsymbol{g} \rangle$ by dividing $\boldsymbol{a} \in \langle \boldsymbol{h} \cdot \boldsymbol{g} \rangle$ by $\boldsymbol{b} \in \langle \boldsymbol{h} \rangle$ in K. In generally, $\boldsymbol{a}/\boldsymbol{b}$ is in K not R. By multiplying some $s \in \mathbb{Z}$ to $\boldsymbol{a}/\boldsymbol{b}$ such that $s\boldsymbol{a}/\boldsymbol{b} \in R$, we can get a multiple of $\boldsymbol{g}$. From many multiples of $\boldsymbol{g}$, compute a basis of $\langle \boldsymbol{g} \rangle$.

5.2 Solving the GDDH problem

We refer to Section 6.3.3 in [GGH13] to solve the GDDH problem with short vector of $\langle \boldsymbol{g} \rangle$. Assume that we have a short vector in $\langle \boldsymbol{g} \rangle$ smaller than a constant M. We explain how to use this short vector of $\langle \boldsymbol{g} \rangle$ in order to solve the GDDH problem in the GGH scheme. Given a distribution $\{\mathsf{params}, \boldsymbol{p}_{zt}, \boldsymbol{u}_0 := \mathsf{enc}_1(\boldsymbol{m}_0), \ldots, \boldsymbol{u}_\kappa := \mathsf{enc}_1(\boldsymbol{m}_\kappa), \hat{\boldsymbol{u}}\}$, the GDDH problem is to determine whether it is from $\mathcal{D}_{\mathrm{DDH}}$ or from $\mathcal{D}_{\mathrm{R}}$.

Our strategy is to compute a coset of m_0 modulo the ideal $\langle \boldsymbol{g} \rangle$ in two different ways: one from $\boldsymbol{u}_0$ and the other from $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_\kappa, \{\hat{\boldsymbol{u}}\}$. If this distribution is $\mathcal{D}_{DDH}$, they are identical, which can be checked easily with a basis of $\mathcal{I} := \langle \boldsymbol{g} \rangle$. Otherwise, they would be different with high probability.

Computing a coset of $\boldsymbol{m}_0$ from $\boldsymbol{u}_0$. By multiplying $\boldsymbol{x}_j$, $\boldsymbol{y}$ and $\boldsymbol{p}_{zt}$ several times to $\boldsymbol{u}_0$ and $\boldsymbol{y}$, we obtain the following two level-κ encodings of zero:

$$\begin{aligned}\boldsymbol{f}_0 &:= \boldsymbol{u}_0 \boldsymbol{x}_j \boldsymbol{y}^{\kappa-2} \boldsymbol{p}_{zt} \equiv \boldsymbol{m}_0 \boldsymbol{b}_j \boldsymbol{h} \bmod \mathcal{I} \\ \boldsymbol{f}_1 &:= \boldsymbol{x}_j \boldsymbol{y}^{\kappa-1} \boldsymbol{p}_{zt} \equiv \boldsymbol{b}_j \boldsymbol{h} \bmod \mathcal{I}.\end{aligned}$$

By computing $\boldsymbol{f}_0/\boldsymbol{f}_1 \bmod \mathcal{I}$, we can recover $\boldsymbol{m}_0 \bmod \mathcal{I}$. Since $R/\mathcal{I}$ is a finite field having p^f order elements, computing $\boldsymbol{f}_1^{-1} \bmod \mathcal{I}$ can be done in time

$O(f^2 \log^2 p)$ via isomorphism, or more directly with a matrix computation in time $O(f^3 \log^2 p)$.

Computing a coset of $\boldsymbol{m}_0$ from $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_\kappa, \hat{\boldsymbol{u}}\}$. Suppose we have an element $\boldsymbol{dg} \in \mathcal{I}$ satisfying $\|\boldsymbol{dg}\| < M$ for some $\boldsymbol{d} \in R$, where M is a constant less than $q^{3/8}/2n^4$. By multiplying $\boldsymbol{dg}$ to $\boldsymbol{p}_{zt}$ in R_q, we obtain a new zero-testing parameter $\boldsymbol{p}'_{zt} = [\boldsymbol{dhz}^\kappa]_q \in R_q$.

Suppose $\hat{\boldsymbol{u}}$ is a valid level-κ encoding of $\prod_{i=0}^{\kappa} m_i$. Then $\|\boldsymbol{z}^\kappa \hat{\boldsymbol{u}}\|$ is smaller than $q^{1/8}$ by parameter setting of the GGH scheme, and so

$$\begin{aligned}\|\hat{\boldsymbol{u}}\boldsymbol{p}'_{zt}\| = \|\hat{\boldsymbol{u}}\boldsymbol{dhz}^\kappa\| &\le \|\boldsymbol{z}^\kappa \hat{\boldsymbol{u}}\| \cdot \|\boldsymbol{h}\| \cdot \|\boldsymbol{dg}\| \cdot \|\boldsymbol{g}^{-1}\| \cdot \sqrt{n^3} \\ &\le q^{1/8} \cdot q^{1/2}\sqrt{n} \cdot M \cdot n^2 \cdot \sqrt{n^3} = q^{5/8} \cdot n^4 \cdot M < q/2.\end{aligned}$$

Since each entry of $\hat{\boldsymbol{u}}\boldsymbol{p}'_{zt}$ is smaller than $q/2$, we have

$$[\hat{\boldsymbol{u}}\boldsymbol{p}'_{zt}]_q = (\boldsymbol{z}^k \hat{\boldsymbol{u}})\boldsymbol{dh} \equiv \boldsymbol{dh} \prod_{i=0}^{\kappa} \boldsymbol{m}_i \bmod \mathcal{I}.$$

Similarly from $\prod_{i=1}^{\kappa} \mathsf{enc}_1(\boldsymbol{m}_i)$, we obtain $\boldsymbol{dh} \prod_{i=1}^{\kappa} \boldsymbol{m}_i \bmod \mathcal{I}$. By dividing $\boldsymbol{dh} \prod_{i=0}^{\kappa} \boldsymbol{m}_i$ by $\boldsymbol{dh} \prod_{i=1}^{\kappa} \boldsymbol{m}_i$ in $R/\mathcal{I} \simeq \mathbb{F}_{p^f}$, we can recover $\boldsymbol{m}_0 \bmod \mathcal{I}$.

It should be identical with $\boldsymbol{m}_0 \bmod \mathcal{I}$ computed from $\boldsymbol{u}_0$. However, if $\hat{\boldsymbol{u}}$ is sampled from $\mathcal{D}_R$, they are not same with high probability. So we can solve the GDDH problem.

5.3 Finding a short vector of $\langle \boldsymbol{g} \rangle$

Now, we will show how to get a shorter vector by applying a lattice reduction algorithm to a sublattice rather than the original lattice. It is certain that the shortest vector of the sublattice cannot be shorter than that of the original lattice. Since the asymptotic factor of the lattice reduction algorithm is exponential in the dimension, however, the reduction algorithm on the sublattice might give a shorter vector that one on the original lattice when the determinant of the lattice is not so large.

More precisely, we assume as a rule of thumb in lattice reductions that the size of the short vector produced by lattice reduction algorithms in time $2^{O(t)}$ is about $2^{\frac{n}{t}} \cdot \det(L)^{\frac{1}{n}}$, when applied to a lattice L of dimension n. When applied to a sublattice L' of L with $\det L' = \det L$, this size becomes $2^{\dim(L')/t} \det L^{1/\dim(L')}$, which has a minimum value when $\dim(L') = \sqrt{t \log \det(L)}$. So if n is larger than this optimal dimension, or equivalently $\det L = O(2^{n^2/t})$, we can have a sublattice L' producing a shorter vector computationally.

The last step of this strategy is to find a sublattice whose determinant is not larger than that of the original lattice, which is not always true for all the

lattices. Using HNF, however, we can choose an appropriate sublattice by taking the last n' column vectors of $\mathrm{HNF}(\langle \boldsymbol{g} \rangle)$.

Let us apply this scenario to the lattice $\langle \boldsymbol{g} \rangle$. From Lemma 5, we can see that $\mathrm{N}(\boldsymbol{g})$ is bounded by $\|\boldsymbol{g}\|^n$. When each entry of $\boldsymbol{g}$ is chosen according to the parameter generation of the GGH, its Euclidean norm is bounded by $\sigma\sqrt{n}$ with overwhelming probability by Lemma 2. We can see that $\mathrm{N}(\boldsymbol{g}) \leq (\sqrt{n}\sigma)^n$ with overwhelming probability. In that case, $2^{\frac{n'}{t}} \cdot \det(L)^{\frac{1}{n'}}$ is minimized into $2^{2\sqrt{(n/t)\log\sqrt{n}\sigma}}$ at $n' = \sqrt{nt\log\sqrt{n}\sigma}$. For $\sigma = \sqrt{\lambda n}$ as in the parameter setting of the GGH, if we take a sublattice L' with dimension $n' = \sqrt{nt\log\sqrt{n}\sigma} < n$, one can compute a short vector of size $2^{2\sqrt{(n/t)\log n\sqrt{\lambda}}}$ in time $2^{O(t)}$. This short vector is less than $q^{3/8}/(2n^4)$ as required in our attack, if $t > \log(\kappa\lambda)$ which implies that the algorithm takes $2^{O(t)} = \mathrm{poly}(\kappa\lambda)$ time complexity.

Setting the parameter of the GGH scheme. To avoid this attack, $q^{5/8} \cdot n^4 \cdot 2^{\sqrt{\frac{n\log(\sigma\sqrt{n})}{\lambda}}}$ must be larger than $q/2$, or equivalently $q \leq (2n^4 \cdot 2^{\sqrt{\frac{n\log(\sigma\sqrt{n})}{\lambda}}})^{8/3}$. The GGH parameter setting requires q to satisfy

$$2^{8\kappa\lambda} \cdot n^{64\kappa} \cdot \lambda^{12\kappa} \leq q \leq 2^{\frac{n}{\lambda}}.$$

Since $2^{\frac{n}{\lambda}} > (2n^4 \cdot 2^{\sqrt{\frac{n\log(\sigma\sqrt{n})}{\lambda}}})^{8/3}$, we have a new parameter condition on q as follows:

$$2^{8\kappa\lambda} \cdot n^{64\kappa} \cdot \lambda^{12\kappa} \leq q \leq (2n^4 \cdot 2^{\sqrt{\frac{n\log(\sigma\sqrt{n})}{\lambda}}})^{8/3}.$$

Such q can exist only if

$$\sqrt{\frac{n\log(\sigma\sqrt{n})}{\lambda}} + 4\log n + 1 > (8\kappa\lambda + 64\kappa\log n + 12\kappa\log\lambda) \cdot 3/8,$$

which is satisfied only in $n = \tilde{\Omega}(\kappa^2 \cdot \lambda^3)$.

Adaptation to the GGHLite scheme. To improve the efficiency of GGH scheme, Langlois, Stehle and Steinfeld [LSS14] constructed GGHLite. Using Renyi divergence, they reanalyze the GGH scheme and get a new parameter reduced than the original scheme: $\sigma = O(n\log n)$, $q \geq n^{84\kappa} \cdot \kappa^{4\kappa}$ and $n \geq \lambda\log q = \Omega(\kappa\lambda\log\lambda)$. Then the inequality $2^{\sqrt{\frac{n\log(\sigma\sqrt{n})}{\lambda}}} + 4\log n + 1 \geq q^{3/8}$ yields $n = \tilde{\Omega}(\lambda \cdot (\kappa\log\lambda)^2)$, which is a bit larger than the original $n = O(\lambda \cdot \kappa\log\lambda)$.

5.4 Finding a short vector of $\langle \boldsymbol{g} \rangle$ with large residual degree

In case of residual degree f being large, we can find a short vector of $\langle \boldsymbol{g} \rangle$ easily. In the cyclotomic field case, the residual degree f is the least positive integer satisfying $p^f \equiv 1 \bmod 2n$, i.e. f is the order of p in $\mathbb{Z}_{2n}^*$. We can estimate the order of p from the following lemma:

Lemma 6. *[NZM08, Theorem 2.43] Suppose that $a \geq 3$. The order of $5 \pmod{2^a}$ is 2^{a-2}. The numbers $\pm 5, \pm 5^2, \ldots, \pm 5^{a-2}$ form a system of reduced residues $(mod\ 2^a)$. Hence, suppose that n is power of 2, then $\mathbb{Z}_{2n}^* \simeq \mathbb{Z}_2 \times \mathbb{Z}_{n/2}$, where $\mathbb{Z}_{2n}^*$, $\mathbb{Z}_2 \times \mathbb{Z}_{n/2}$ are characterized by a multiplication and addition, respectively.*

By Lemma 6, for an arbitrary odd prime $p \in \mathbb{Z}$, order of p is approximately such as:

$$|p| = \begin{cases} \dfrac{n}{2^i} \text{ with } \dfrac{1}{2^i} \text{ probability } i \in [1, \log n - 1) \\ 2 \quad \text{with } \dfrac{3}{n} \text{ probability} \\ 1 \quad \text{with } \dfrac{1}{n} \text{ probability} \end{cases}$$

So f is very large with high probability assuming $p \bmod 2n$ is uniformly distributed over $\mathbb{Z}_{2n}^*$. However, when $\boldsymbol{g}$ is sampled from $D_{\mathbb{Z},\sigma}$, p is characterized by $\langle \boldsymbol{g} \rangle \cap \mathbb{Z} = p \cdot \mathbb{Z}$. In case of this, we don't know the distribution of order of p. Assume f is larger than $\sqrt{t \log \det(L)}$. Then

$$p = \det(L')^{\frac{1}{d}} = 2^{\frac{d}{t}} \cdot \det(L')^{\frac{1}{d}} \leq 2^{\frac{d}{t}} \cdot \det(L)^{\frac{1}{d}} \leq 2^{\frac{n}{t}} \cdot \det(L)^{\frac{1}{n}}$$

If p is smaller than $q^{3/8}/2n^4$, the last vector of $\mathrm{HNF}(\boldsymbol{g})$ can be used to solve the GDDH problem by modifying zero-testing parameter in Section 5.2. Hence, in just polynomial time for n (we only use the zeroizing attack and computing the Hermite normal form), we can solve the GDDH problem. It suggests another parameter condition. When $\boldsymbol{g}$ is sampled from $D_{R,\sigma}$, the residual degree of p must be very small.

References

[ABP14] M. Abdalla, F. Benhamouda, and D. Pointcheval. Disjunctions for hash proof systems: New constructions and applications. *IACR Cryptology ePrint Archive*, 2014:483, 2014.

[Att14] N. Attrapadung. Fully secure and succinct attribute based encryption for circuits from multi-linear maps. *IACR Cryptology ePrint Archive*, 2014:772, 2014.

[BLMR13] D. Boneh, K. Lewi, H. Montgomery, and A. Raghunathan. Key homomorphic PRFs and their applications. In *Proc. of CRYPTO*, pages 410–428. Springer, 2013.

[BP13] F. Benhamouda and D. Pointcheval. Verifier-based password-authenticated key exchange: New models and constructions. *IACR Cryptology ePrint Archive*, 2013:833, 2013.

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

[BWZ14] Dan Boneh, David J. Wu, and Joe Zimmerman. Immunizing multilinear maps against zeroizing attacks. Cryptology ePrint Archive, Report 2014/930, 2014. http://eprint.iacr.org/.

[CHL+14] Jung Hee Cheon, Kyoohyung Han, Changmin Lee, Hansol Ryu, and Damien Stehle. Cryptanalysis of the multilinear map over the integers. 2014. http://eprint.iacr.org/.

[CLT13] J.-S. Coron, T. Lepoint, and M. Tibouchi. Practical multilinear maps over the integers. In *Proc. of CRYPTO*, pages 476–493. Springer, 2013.

[CLT14] Jean-Sebastien Coron, Tancrede Lepoint, and Mehdi Tibouchi. Cryptanalysis of two candidate fixes of multilinear maps over the integers. Technical report, Cryptology ePrint Archive, Report 2014/975, 201 4. http://eprint. iacr. org, 2014.

[GGH13] S. Garg, C. Gentry, and S. Halevi. Candidate multilinear maps from ideal lattices. In *Proc. of EUROCRYPT*, volume 7881 of *LNCS*, pages 1–17. Springer, 2013.

[GGHZ14] S. Garg, C. Gentry, S. Halevi, and M. Zhandry. Fully secure functional encryption without obfuscation. Cryptology ePrint Archive, Report 2014/666, 2014.

[GHMS14] Craig Gentry, Shai Halevi, Hemanta K. Maji, and Amit Sahai. Zeroizing without zeroes: Cryptanalyzing multilinear maps without encodings of zero. 2014. http://eprint.iacr.org/.

[GLW14] C. Gentry, A. B. Lewko, and B. Waters. Witness encryption from instance independent assumptions. *IACR Cryptology ePrint Archive*, 2014:273, 2014.

[LSS14] A. Langlois, D. Stehlé, and R. Steinfeld. GGHLite: More efficient multilinear maps from ideal lattices. In *Proc. of EUROCRYPT*, LNCS, pages 239–256. Springer, 2014.

[MR07] Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on gaussian measures. *SIAM Journal on Computing*, 37(1):267–302, 2007.

[NZM08] Ivan Niven, Herbert S Zuckerman, and Hugh L Montgomery. *An introduction to the theory of numbers*. John Wiley & Sons, 2008.

[Zha14] M. Zhandry. Adaptively secure broadcast encryption with small system parameters. *IACR Cryptology ePrint Archive*, 2014:757, 2014.

[Zim14] J. Zimmerman. How to obfuscate programs directly. *IACR Cryptology ePrint Archive*, 2014:776, 2014.

A Proof of Lemmas

Lemma 3. For prime $\boldsymbol{g}$ in $R = \mathbb{Z}[X]/(X^n + 1)$, there exists some prime integer p in $\mathbb{Z}$ such that $\langle \boldsymbol{g} \rangle \cap \mathbb{Z} = p\mathbb{Z}$.

Proof. Consider an embedding homomorphism ϕ from $\mathbb{Z}$ to R and the projection homomorphism π from R to $R/\langle \boldsymbol{g} \rangle$. The Kernel $\langle \boldsymbol{g} \rangle \cap \mathbb{Z} \subset \mathbb{Z}$ of $\pi \cdot \phi$ is a prime ideal of $\mathbb{Z}$ so that, for some prime $p \in \mathbb{Z}$, $\langle \boldsymbol{g} \rangle \cap \mathbb{Z} = p \cdot \mathbb{Z}$ □

Lemma 4. Let n be a power of 2 and $\boldsymbol{g}$ a prime element of $R = \mathbb{Z}[X]/(X^n + 1)$ with $\langle \boldsymbol{g} \rangle \cap \mathbb{Z} = p\mathbb{Z}$ for an odd prime p. Then we have $\mathrm{N}(\boldsymbol{g}) = p^f$ for the smallest positive integer f satisfying $p^f \equiv 1 \bmod 2n$.

Proof. Since $\langle \boldsymbol{g} \rangle$ is a prime ideal in R and $p \in \langle \boldsymbol{g} \rangle$, the quotient ring $R/\langle \boldsymbol{g} \rangle$ is a finite field with characteristic p. When f is the smallest positive integer satisfying $p^f \equiv 1 \bmod 2n$, for any $\boldsymbol{a}(x) \in R/\langle \boldsymbol{g} \rangle$,

$$\boldsymbol{a}(x)^{p^f} = \boldsymbol{a}(x^{p^f}) = \boldsymbol{a}(x) \bmod \langle \boldsymbol{g} \rangle.$$

Therefore the minimality of f gives $|R/\langle \boldsymbol{g} \rangle| = p^f$ i.e $\mathrm{N}(\langle \boldsymbol{g} \rangle) = p^f$. □

Lemma 5. Given an element $\boldsymbol{g}$ of $R = \mathbb{Z}[X]/(X^n + 1)$, we have

$$\mathrm{N}(\boldsymbol{g}) = \prod_{\delta \in \mathrm{Gal}(K/\mathbb{Q})} \delta(\boldsymbol{g}) = \det[\boldsymbol{g}, x\boldsymbol{g}, \ldots, x^{n-1}\boldsymbol{g}].$$

Proof. When $\boldsymbol{g}$ is a primitive element of R over $\mathbb{Q}$, let $F(X) = \sum_{i=0}^{n} a_i X^i$ be the minimal polynomial of $\boldsymbol{g}$ over $\mathbb{Q}$. Then R is isomorphic to $\mathbb{Q}[X]/\langle F[X] \rangle$, and $\{1, \boldsymbol{g}, \ldots, \boldsymbol{g}^{n-1}\}$ is a basis for R over $\mathbb{Q}$. Moreover $a_0 = \prod_{\delta \in \mathrm{Gal}(K/\mathbb{Q})} \delta(\boldsymbol{g}) = \mathrm{N}(\boldsymbol{g})$. The matrix M of the multiplication endomorphism $m_g(\boldsymbol{a}) = \boldsymbol{g}\boldsymbol{a}$, for $\boldsymbol{a} \in R$, with relative to this basis is

$$M = \begin{pmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & \ldots & 0 & -a_2 \\ \vdots & \vdots & \ddots & & \vdots \\ 0 & 0 & \ldots & 1 & -a_{n-1} \end{pmatrix}$$

having its determinant a_0. Since determinant does not depend on bases and $\{1, x, \ldots, x^{n-1}\}$ is also basis of R, the determinant of matrix of the m_g with relative to this bases is $\det[\boldsymbol{g}, x\boldsymbol{g}, \ldots, x^{n-1}\boldsymbol{g}] = a_0 = \mathrm{N}(\langle \boldsymbol{g} \rangle)$.

Now, consider the general case. Put $F[X] = \sum_{i=0}^{m} a_i X^i$ and $r = n/m$. Then $\mathrm{N}(\boldsymbol{g}) = a_0^r$. Let $\{y_i\}_{i=1,\ldots,m}$ be a basis for $\mathbb{Q}[X]/\langle F[X] \rangle$ over $\mathbb{Q}$ and $\{z_i\}_{i=1,\ldots,r}$ a basis for R over $\mathbb{Q}[X]/\langle F[X] \rangle$. Then $\{y_i z_j\}$ is a basis for R over $\mathbb{Q}$. Let M be the matrix for multiplication by $\boldsymbol{g}$ in $\mathbb{Q}[X]/\langle F[X] \rangle$ with relative to the basis $\{y_i\}$. Ordering lexicographically the basis $\{y_i z_j\}$, the matrix M' of the m_g in R with relative to this basis is

$$M' = \begin{pmatrix} M & 0 & \ldots & 0 \\ 0 & M & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & M \end{pmatrix}$$

Similarly to above paragraph, we can get $\det[\boldsymbol{g}, x\boldsymbol{g}, \ldots, x^{n-1}\boldsymbol{g}] = a_0^r = \mathrm{N}(\langle \boldsymbol{g} \rangle)$. □