An Algorithm for CSPR Problems and Cryptanalysis of the GGH Multilinear Map without an encoding of zero

Jung Hee Cheon, Jinhyuck Jeong, Changmin Lee

Seoul National University (SNU), Republic of Korea

Abstract. We describe a polynomial time algorithm to solve the Computational Small Polynomial Ratio Problem in current parameter, which is to find a short element of an ideal $\langle \boldsymbol{g} \rangle \subset \mathbb{Z}[X]/\langle X^n + 1 \rangle$ when $\|\boldsymbol{g}\|$ is smaller than some constant B (in $\mathbb{Q}[X]/\langle X^n+1 \rangle$) and a somewhat small multiple of $\boldsymbol{g}^{-1}$ (in R_q) is given.
In GGH scheme, which is the first candidate of a (approximate) multilinear map, the algorithm, using any encodings, can be directly applied to obtain the any secret elements. Recently, the GGH scheme was known to be insecure by so called zeroizing attack [HJ15], when an encoding of zero is published. Hence, this work leads to showing that GGH scheme without an encoding of zero is also insecure.

Keywords: Computational Small Polynomial Ratio(CSPR) problem, multilinear maps.

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) [GGH13a] . 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 encoding of zero, which are used as basic tools for constructing applications such as indistinguishable obfuscations, have still not analyzed yet.

Contribution. In current parameters, we propose an algorithm for solving the Computational Small Polynomial Ratio Problem(or CSPR) whose decisional version is originally proposed in [LATV12] for the security of their fully homomorphic encryption (FHE). This algorithm can be applied to attack for GGH-like schemes without encodings of zero(or private GGH) such as asymmetric multilinear map suggested in [GGH$^+$13b,BR13], for example.

Problem 1 (Computational Small Polynomial Ratio Problem) *Let $\phi_n(X) \in \mathbb{Z}[X]$ be a polynomial of degree n, let $q \in \mathbb{Z}$ be an integer. The Computational Small Polynomial Ratio Problem $CSPR_{\phi_n,q,B}$ is to find $\boldsymbol{a}, \boldsymbol{b} \in R := \mathbb{Z}[X]/\langle\phi_n(X)\rangle$ with small Euclidean norm such that $[\boldsymbol{b}/\boldsymbol{a}]_q = \boldsymbol{f}$ for given a polynomial $\boldsymbol{f} = [\boldsymbol{h}/\boldsymbol{g}]_q$, where $\boldsymbol{g}$ and $\boldsymbol{h}$ are sampled from R and the size of these is bounded by B (conditioned on $\boldsymbol{g}$ being invertible over $R_q = R/qR$).*

Problem 2 (Decisional Small Polynomial Ratio Problem) *Let $\phi_n(x) \in \mathbb{Z}[X]$ be a polynomial of degree n, let $q \in \mathbb{Z}$ be an integer. The Decisional Small Polynomial Ratio Problem $DSPR_{\phi_n,q,B}$ is to distinguish between the following two distributions:*

- *a polynomial $\boldsymbol{f} = \boldsymbol{h}/\boldsymbol{g}$, where $\boldsymbol{g}$ and $\boldsymbol{h}$ are sampled from $R := \mathbb{Z}[X]/\langle\phi_n(X)\rangle$ and the size of these is bounded by B (conditioned on $\boldsymbol{g}$ being invertible over $R_q = R/qR$), and*
- *a polynomial $\boldsymbol{f}$ sampled uniformly at random over R_q.*

In this problem, the fact B is very small compared with q. That is why the name of this problem is 'Small Polynomial' Ratio Problem.

The following theorem is the detailed result of our work, to solve the $CSPR_{\phi_n,q,B}$, which will be proved later in Section 3.

Theorem 1 *Let q and $m \in \mathbb{Z}$ be integers, and B a positive real number. Then, for $\phi_n(X) = X^n + 1$ with n a power of 2, we can reduce $CSPR_{\phi_n,q,B}$ into $CSPR_{\phi_{n/2},q,B^2\sqrt{2n}}$.*

Repeating the theorem t times, we can reduce the $CSPR_{\phi_n,q,B}$ to $CSPR_{\phi_{n/2^t},q,B_t}$ for some constant B_t. If $n/2^t$ is small to find a short vector, one can solve the $CSPR_{\phi_{n/2^t},q,B_t}$ and this solution can be used to solve the $CSPR_{\phi_n,q,B}$.

Technical overview. We explain a naive approach to solve the $CSPR_{\phi_n,q,B}$ with $\phi_n(X) = X^n + 1$ when n is a power of 2. For any polynomial $\boldsymbol{f} = [\boldsymbol{h}/\boldsymbol{g}]_q = \sum_{i=0}^{n-1} f_i X^i \in R$, one can consider it as a vector $(f_0, \cdots, f_{n-1})^T$. We use $\boldsymbol{f}$ to denote a polynomial or vector unless there is confusion. Then, the product $\boldsymbol{g}\boldsymbol{f} = \sum_{i=0}^{n-1} g_i X^i \boldsymbol{f}$ of two polynomials $\boldsymbol{f}$ and $\boldsymbol{g}$ in $\mathbb{Z}[X]/\langle\phi(X)\rangle$ is contained in a lattice $\mathcal{M}_{\boldsymbol{f}}$ generated by $\{\boldsymbol{f}, X\boldsymbol{f}, \cdots, X^{n-1}\boldsymbol{f}\}$. To obtain a $\tilde{\boldsymbol{g}} \in \mathbb{Z}_q[X]/\langle\phi(X)\rangle$ satisfying $\|\tilde{\boldsymbol{g}}\|$ and $\|[\tilde{\boldsymbol{g}}\boldsymbol{f}]_q\|$ are small, 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 $\{\boldsymbol{f}, X\boldsymbol{f}, \cdots, X^{n-1}\boldsymbol{f}\}$. If we are given a lattice vector $\boldsymbol{u} = (u_0, \cdots, u_{2n-1})^T$ satisfying $|u_i| < q/2$ for $n \leq i \leq 2n-1$, then we have $\sum_{i=0}^{n-1} u_{n+i}X^i = \left[\sum_{i=0}^{n-1} u_i X^i \boldsymbol{f}\right]_q$. Therefore, if one can find a small lattice point, it becomes a solution of $CSPR_{\phi,q,\chi}$. The dimension $2n$, however, is too large to find it. To overcome this obstacle, we decompose $\boldsymbol{f} = [\boldsymbol{h}/\boldsymbol{g}]_q$ as a sum of odd degree terms and even degree terms. Put $\boldsymbol{f} = [\boldsymbol{h}_0/\boldsymbol{g}]_q + [\boldsymbol{h}_1/\boldsymbol{g}]_q X$, where $[\boldsymbol{h}_i/\boldsymbol{g}]_q \in \mathbb{Z}_q[X^2]/\langle X^n+1\rangle$ for $i = 0,\ 1$. If $\boldsymbol{h}_0$ is dominated for some $poly(n, \|\boldsymbol{h}\|)$ and one restrict the space $\mathbb{Z}[X]/\langle X^n+1\rangle$ to only $\mathbb{Z}[X^2]/\langle X^n+1\rangle \approx \mathbb{Z}[Y]/\langle Y^{n/2}+1\rangle$, then $\boldsymbol{F}_0 = [\boldsymbol{h}_0/\boldsymbol{g}]_q$ can be considered as another instance of $CSPR_{\Phi,q,B'}$ with $\Phi(Y) = Y^{n/2}+1$ and the dimension of $\Lambda_{\boldsymbol{F}_0}$ is half of that of $\Lambda_{\boldsymbol{f}}$. By adapting same arguments to dimension 4, one can find one of the smallest vector of lattice and it would be a solution of the original $CSPR_{\phi,q,B}$ problem. In this study, we show that $\boldsymbol{h}_0$ is dominated, when n is a power of two. Hence, we can solve the $CSPR_{\phi,q,B}$ using this technique.

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

2 Preliminaries

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 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 $R_q := \mathbb{Z}_q[X]/\langle X^n+1\rangle = R/qR$. 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 $\boldsymbol{u} \in \mathbb{Z}^n$ 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 identify $[x]_q \in \mathbb{Z}_q$ for $0 \leq x < q$ with $x \in \mathbb{Z}$. Formally, we define $\iota : \mathbb{Z}_q \longrightarrow \mathbb{Z}$ by $[x]_q \in \mathbb{Z}_q \mapsto x \in \mathbb{Z}$ for $0 \leq x < q$. We extend this map into R_q applying to each coefficient. By abusion of notation, we omit this ι unless confused. 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 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 $\|\boldsymbol{a}\| \cdot \|\boldsymbol{b}\|$, $\|\boldsymbol{ab}\| \leq \|\boldsymbol{a}\| \cdot \|\boldsymbol{b}\| \cdot \sqrt{n}$. □

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) $\mathrm{Tr}_{K/F}(\alpha) = \sum_{\sigma \in Gal(K/F)} \sigma(\alpha)$ if K is a Galois extension of F
$\mathrm{N}_{K/F}(\alpha) = \prod_{\sigma \in Gal(K/F)} \sigma(\alpha)$
(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 Proof of Main Theorem

In this section we introduce how we can reduce CSPR with a given input $[\boldsymbol{h}/\boldsymbol{g}]_q$ into CSPR with an input of which denominator has the half degree of $\boldsymbol{h}$. Throughout this section, let n be a power of 2, $n = 2^s$, and denote $\mathbb{Q}[X^{2^t}]/\langle X^n + 1\rangle$ by K_t with $0 \leq t \leq s$. Note that $K_s := \mathbb{Q} \subset K_{s-1} \subset \cdots \subset K_0 = \mathbb{Q}[X]/\langle X^n + 1\rangle$.

Since K_0 is a Galois extension field of K_t with degree 2^t, the set $B = \{1, X, \ldots, X^{2^t-1}\}$ forms a basis of K_0 over K_t. It means that any $\boldsymbol{f} \in K_0 =$

$\mathbb{Q}[X]/\langle X^n+1\rangle$ can be uniquely represented as $\boldsymbol{f} = \sum_{i=0}^{2^t-1} \boldsymbol{f}_i X^i$ with $\boldsymbol{f}_i \in K_t = \mathbb{Q}[X^{2^t}]/\langle X^n+1\rangle$ which is a linear combination of B. First we state a useful lemma.

Lemma 2 *For any* $\boldsymbol{f} = \sum_{i=0}^{2^t-1} \boldsymbol{f}_i X^i \in \mathbb{Q}[X]/\langle X^n+1\rangle$ *with* $0 \le t \le s$ *and* $\boldsymbol{f}_i \in \mathbb{Q}[X^{2^t}]/\langle X^n+1\rangle$*, we have*

$$\mathrm{Tr}_{K_0/K_t}(\boldsymbol{f}) = 2^t \boldsymbol{f}_0.$$

Proof. First we note that $\mathrm{Tr}_{K_0/K_t}(X^i) = 0$ for $1 \le i < 2^t$ because the K_t-linear transformation M_{X^i}, which maps $\boldsymbol{a} \in K_0$ to $\boldsymbol{a}X^i \in K_0$, has a matrix representation whose diagonal entries are zero with respect to basis $B = \{1, X, \ldots, X^{2^t-1}\}$. Since K_0 is an extension field of K_t, we can compute

$$\begin{aligned}
\mathrm{Tr}_{K_0/K_t}(\boldsymbol{f}) &= \sum_{\sigma\in\mathrm{Gal}(K_0/K_t)} \sigma(\boldsymbol{f}) = \sum_{\sigma\in\mathrm{Gal}(K_0/K_t)} \sigma\left(\sum_{i=0}^{2^t-1} \boldsymbol{f}_i X^i\right) \\
&= \sum_{\sigma\in\mathrm{Gal}(K_0/K_t)} \sum_{i=0}^{2^t-1} \sigma(\boldsymbol{f}_i)\sigma(X^i) = \sum_{\sigma\in\mathrm{Gal}(K_0/K_t)} \sum_{i=0}^{2^t-1} \boldsymbol{f}_i \cdot \sigma(X^i) \\
&= \sum_{i=0}^{2^t-1} \left\{ \boldsymbol{f}_i \sum_{\sigma\in\mathrm{Gal}(K_0/K_t)} \sigma(X^i) \right\} = \boldsymbol{f}_0 2^t + \sum_{i=1}^{2^t-1} \boldsymbol{f}_i \cdot \mathrm{Tr}_{K_0/K_t}(X^i) \\
&= 2^t \boldsymbol{f}_0.
\end{aligned}$$

□

Using this lemma, 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* B *a positive real number. Then, for* $\phi_n(X) = X^n + 1$ *with* n *a power of* 2*, we can reduce* $CSPR_{\phi_n,q,B}$ *into* $CSPR_{\phi_{n/2},q,B^2\sqrt{2n}}$.

Proof. Suppose we are given $[\boldsymbol{h}/\boldsymbol{g}]_q$ where $\boldsymbol{g}$ and $\boldsymbol{h}$ are sampled from the set $\{\boldsymbol{P} \in R = \mathbb{Z}[X]/\langle\phi(X)\rangle : \|\boldsymbol{P}\| < B\}$. Note that $\dfrac{\boldsymbol{h}}{\boldsymbol{g}}$ can be written over $K = \mathbb{Q}[X]/\langle X^n+1\rangle$ as

$$\frac{\boldsymbol{h}}{\boldsymbol{g}} = \frac{\boldsymbol{h}_0}{\boldsymbol{g}} + \frac{\boldsymbol{h}_1}{\boldsymbol{g}} X$$

such that $\dfrac{\boldsymbol{h}_i}{\boldsymbol{g}} \in R_1 = \mathbb{Z}[X^2]/\langle X^n+1\rangle$ for $i = 0,\ 1$.

By Lemma 2, we get $\frac{2\boldsymbol{h}_0}{\boldsymbol{g}} = Tr_{K_0/K_1}\left(\frac{\boldsymbol{h}}{\boldsymbol{g}}\right) = \frac{\boldsymbol{h}}{\boldsymbol{g}} + \sigma\left(\frac{\boldsymbol{h}}{\boldsymbol{g}}\right)$ where $G = Gal(K_0/K_1) = \{id, \sigma\}$. Multiplying $\boldsymbol{g}\sigma(\boldsymbol{g})$, we have

$$2\boldsymbol{h}_0\sigma(\boldsymbol{g}) = \boldsymbol{h}\sigma(\boldsymbol{g}) + \sigma(\boldsymbol{h})\boldsymbol{g}$$

which is fixed by G and so lies in $R_1 = \mathbb{Z}[X^2]/\langle X^n+1\rangle$. Since it has $n/2$ terms, we also have an inequality $\|2\boldsymbol{h}_0\sigma(\boldsymbol{g})\| = \|\boldsymbol{h}\sigma(\boldsymbol{g})+\sigma(\boldsymbol{h})\boldsymbol{g}\| \leq 2\cdot\sqrt{n/2}\cdot B\cdot B = B^2\sqrt{2n}$.

On the other hand, one can notice that the norm of $\boldsymbol{g}\sigma(\boldsymbol{g}) \in R_1$ is bounded by $B^2\sqrt{n/2} \leq B^2\sqrt{2n}$ since it is also fixed by G. Finally, substituting X' for X^2, we can consider $\left[\frac{2\boldsymbol{h}_0}{\boldsymbol{g}}\right]_q = \left[\frac{2\boldsymbol{h}_0\sigma(\boldsymbol{g})}{\boldsymbol{g}\sigma(\boldsymbol{g})}\right]_q$ as a new instance for $CSPR_{\phi_{n/2},q,B^2\sqrt{2n}}$.

Now, suppose that we can find a $\boldsymbol{c} \in R_1$ such that both $\|\boldsymbol{c}\|$ and $\left\|\left[\boldsymbol{c}\cdot\frac{2\boldsymbol{h}_0\sigma(\boldsymbol{g})}{\boldsymbol{g}\sigma(\boldsymbol{g})}\right]_q\right\|$ are small such that $\boldsymbol{c}$ is of the form $\boldsymbol{c} = \boldsymbol{g}\cdot\sigma(\boldsymbol{g})\cdot\boldsymbol{d}$ with small $\boldsymbol{d} \in R$. If we define $\boldsymbol{b} = [\boldsymbol{c}]_q \cdot \left[\frac{\boldsymbol{h}}{\boldsymbol{g}}\right]_q = [\sigma(\boldsymbol{g})\cdot\boldsymbol{d}\cdot\boldsymbol{h}]_q = \sigma(\boldsymbol{g})\cdot\boldsymbol{d}\cdot\boldsymbol{h}$, then we have $\left[\frac{\boldsymbol{b}}{\boldsymbol{c}}\right]_q = \left[\frac{\boldsymbol{h}}{\boldsymbol{g}}\right]_q$ which implies we solve the original CSPR problem. □

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 [GGH13a] 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
- σ: the basic Gaussian parameter for drawing the ideal generator $\boldsymbol{g}$
- σ': the Gaussian parameter for sampling level-zero 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 $\|\boldsymbol{g}^{-1}\| \leq n^2$ and $\mathcal{I} = \langle\boldsymbol{g}\rangle$ is a prime ideal in R.

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

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

Publish $\mathsf{params} = (n, q, \kappa)$ 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 $\boldsymbol{c}_i = \left[\frac{\boldsymbol{c}}{\boldsymbol{z}^{i-j}}\right]_q$.

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

Next, we introduce a quantitative variant of [GGH13a, Lemma 3, 4] required in zero-testing procedure, which plays an important role to prove our main theorem.

Lemma 3 *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 $\boldsymbol{g}$ and $\|\boldsymbol{h}\| \le M$ for some constant $M < q$. If $\boldsymbol{c} \in \mathbb{Z}[X]/\langle X^n+1\rangle$ satisfies $\|\boldsymbol{c}\| < q/(2M\sqrt{n})$ 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, $[\boldsymbol{g}\boldsymbol{w}]_q = [\boldsymbol{c}\boldsymbol{h}]_q$. Since $\|\boldsymbol{w}\| < q/(2\|\boldsymbol{g}\|\sqrt{n})$, we have $\|\boldsymbol{g}\boldsymbol{w}\| \le \|\boldsymbol{g}\| \cdot \|\boldsymbol{w}\| \cdot \sqrt{n} \le q/2$ and $\|\boldsymbol{c}\boldsymbol{h}\| \le \|\boldsymbol{c}\| \cdot \|\boldsymbol{h}\| \cdot \sqrt{n} \le q/2$. Therefore, $\boldsymbol{g}\boldsymbol{w} = \boldsymbol{c}\boldsymbol{h}$ in $\mathbb{Z}[X]/\langle X^n + 1\rangle$. Because $\boldsymbol{c}\boldsymbol{h} \in \langle\boldsymbol{g}\rangle$ and $\boldsymbol{h}$ is relative prime to $\boldsymbol{g}$, we can conclude $\boldsymbol{c} \in \langle\boldsymbol{g}\rangle$. □

Using Lemma 3, if one can find the $\boldsymbol{c}$ satisfying lemma 3, $\boldsymbol{c}$ is of the form $\boldsymbol{c} = \boldsymbol{d}\boldsymbol{g}$ for some small $\boldsymbol{d} \in \mathbb{Z}[X]/\langle X^n + 1\rangle$. Then multiplying it to $[\boldsymbol{h}\boldsymbol{g}^{-1}]_q$, one can obtain, a small multiple of $\boldsymbol{h}$, $\boldsymbol{d}\boldsymbol{h}$. Hence, $\boldsymbol{d}\boldsymbol{h}$ and $\boldsymbol{d}\boldsymbol{g}$ become a solution of CSPR.

4.2 Attack to GGH

Considering GGH13, one can notice that the theorem in section 3 can be applied to attack the GGH scheme. To explain the attack, we refer to parameters in [ACLL14], which is proposed to implement asymmetric multilinear maps without encodings of zero. Let $\boldsymbol{u}_1 = [\boldsymbol{a}_1/\boldsymbol{z}]_q$, $\boldsymbol{u}_2 = [\boldsymbol{a}_2/\boldsymbol{z}]_q$ be valid level-1 encodings of GGH scheme. Then, we have $\|\boldsymbol{a}_i\| \le n^{3.5}$, $1 \le i \le 2$. The ratio of $\boldsymbol{u}_1$ to $\boldsymbol{u}_2$ in R_q are equivalent to $\left[\frac{\boldsymbol{a}_1}{\boldsymbol{a}_2}\right]_q$. Here we assume $\boldsymbol{a}_1$ and $\boldsymbol{a}_2$ are relative prime. From

Lemma 3, if one can find a $\boldsymbol{c} \in \mathbb{Z}[X]/\langle X^n+1\rangle$ such that $\|\boldsymbol{c}\| \leq q/(2n^{3.5}\sqrt{n})$ and $[\boldsymbol{c}\boldsymbol{a}_1/\boldsymbol{a}_2]_q \leq q/(2n^{3.5}\sqrt{n})$, then $\boldsymbol{c}$ is in $\langle \boldsymbol{a}_2\rangle$. To find a such vector, naturally, one may consider the following lattice.

$$\mathcal{M} = \begin{pmatrix} I & 0 \\ \Lambda & qI \end{pmatrix},$$

where I is the identity matrix of the size n and $\Lambda \in \mathbb{Z}^{n\times n}$ is a matrix whose i-th column is $\iota(X^i[\boldsymbol{a}_1/\boldsymbol{a}_2]_q)$, for $0 \leq i < n$. The dimension of this lattice, however, is too large to find a lattice point satisfying lemma 3 from lattice reduction algorithms such as LLL and BKZ algorithm. Therefore, using the above theorem, we deal with a lattice whose degree is lower than that of original lattice. In reduced dimension, one can find the lattice point satisfying lemma 3 from lattice reduction algorithm.

By Theorem 1, for $[\boldsymbol{a}_1/\boldsymbol{a}_2]_q = \sum_{i=0}^{2^t-1} [\boldsymbol{a}_{1i}/\boldsymbol{a}_2]_q X^i$ with $[\boldsymbol{a}_{1i}/\boldsymbol{a}_2]_q \in R_t$, $[2^t\boldsymbol{a}_{10}/\boldsymbol{a}_2]_q$ is equivalent to $[2^t\boldsymbol{a}_{10}\boldsymbol{G}_t/(\boldsymbol{a}_2\boldsymbol{G}_t)]_q$, where $\boldsymbol{G}_t = \prod_{\delta\in \mathrm{Gal}(K_0/K_t)\setminus id} \delta(\boldsymbol{a}_2)$ satisfying $2^t\boldsymbol{a}_{10}\boldsymbol{G}_t, \quad \boldsymbol{a}_2\boldsymbol{G}_t \in R_t$ and the size of each representation is bounded by

$$n^{3.5}2^{(3t-1)/2}(n^4/(2\sqrt{2}))^{2^t-1} \text{ and } n^{3.5}2^{(t-1)/2}(n^4/(2\sqrt{2}))^{2^t-1},$$

respectively. For convenience, we denote the first as M_t, the last as $B_t = M_t/2^t$, and n_t as $n/2^t$. To apply lemma 3, both bound must be smaller than q. In [ACLL14] parameter settings, t is to be smaller than 7. Now, we consider the following column lattice $\mathcal{M}_t$:

$$\mathcal{M}_t = \begin{pmatrix} I_t & 0 \\ \Lambda_t & qI_t \end{pmatrix},$$

where I_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. Each column of Λ_t is $\iota(X^{i2^t}[2^t\boldsymbol{a}_{10}\boldsymbol{G}_t/\boldsymbol{a}_2\boldsymbol{G}_t]_q)$, for $0 \leq i < n/2^t$.

Here, we use a lattice reduction algorithm such as LLL algorithm. By experimental results, for m dimensional lattice $\mathcal{L}$, the size of LLL algorithm's output is bounded by $1.0219^m \det \mathcal{L}^{1/m}$. Using the lattice reduction algorithm, one can obtain an element in $\mathcal{M}_t$

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

with $\|\boldsymbol{u}_t\| \leq 1.0219^{n_t}\sqrt{q}$. Take $\boldsymbol{c} = \sum_{i=0}^{n_t} u_i X^{2^t i} \in \mathbb{Z}[X^{2^t}]/\langle X^n+1\rangle$. Then $[\boldsymbol{c}\cdot 2^t\boldsymbol{a}_{10}\boldsymbol{G}_t/\boldsymbol{a}_2\boldsymbol{G}_t]_q = \sum_{i=0}^{n_t} u_{n_t+i}X^{2^t i} \in \mathbb{Z}[X^{2^t}]/\langle X^n+1\rangle$. Moreover, if t satisfies

$$1.0219^{n_t}\sqrt{q} \leq \frac{q}{2M_t\sqrt{n_t}},$$

then,

$$\|\boldsymbol{c}\| < \|\boldsymbol{u}_t\| \leq 1.0219^{n_t}\sqrt{q} \leq \frac{q}{2M_t\sqrt{n_t}}$$
$$\|[\boldsymbol{c}\cdot 2^t\boldsymbol{a}_{10}\boldsymbol{G}_t/\boldsymbol{a}_2\boldsymbol{G}_t]_q\| < \|\boldsymbol{u}_t\| \leq 1.0219^{n_t}\sqrt{q} \leq \frac{q}{2M_t\sqrt{n_t}} \leq \frac{q}{2B_t\sqrt{n_t}}.$$

In other words, $\boldsymbol{c}$ satisfies the conditions of lemma 3. Therefore, $\boldsymbol{c}$ is in $\langle \boldsymbol{a}_2\boldsymbol{G}_t\rangle$. Note that $\boldsymbol{c}$ is of the form $\boldsymbol{c} = \boldsymbol{d}\boldsymbol{a}_2\boldsymbol{G}_t = \boldsymbol{d}'\boldsymbol{a}_2 \in R_t$ since $\boldsymbol{c}$ lies in $\langle \boldsymbol{a}_2\boldsymbol{G}_t\rangle \subset R_t$. Multiplying it to $[\boldsymbol{a}_1/\boldsymbol{a}_2]_q$, one can obtain $\boldsymbol{d}'\boldsymbol{a}_1 \in R$. Running time of these procedures is dominated by that of LLL algorithm, which is polynomial time algorithm in dimension of a lattice and $\log q$. Hence, this attack is carried out in polynomial time, if above t exists. Several parameter settings with such t are proposed in Section 4.3. Finally, we have constructed an algorithm to find an element $\boldsymbol{d}'\boldsymbol{a}_1$ from $[\boldsymbol{a}_1/\boldsymbol{a}_2]_q$. Using this algorithm to several $[\boldsymbol{a}_1/\boldsymbol{a}_i]_q$, one can recover $\boldsymbol{d}_i'\boldsymbol{a}_1$ Applying averaging attacks and Gentry-Szydlo algorithm to $\{\boldsymbol{c}_i\}$, explained in [GGH13a, Section 7.2, 7.3], one can recover $\boldsymbol{a}_2$. It implies that one can recover $\boldsymbol{z}$ and any secret elements in GGH scheme.

4.3 Application with practical parameter setting

To apply our attack, we computed appropriate t on some [ACLL14] parameter settings for GGH. Table 1 provides some numerical values including $\log 1.0219^{n_t}\sqrt{q}$ and $\log \frac{q}{2M_t\sqrt{n_t}}$ meaning we can apply our attack with these settings.

Table 1: Numerical results

λ	κ	n	$\log q$	t	$\log 1.0219^{n_t}\sqrt{q}$	$\log \frac{q}{2M_t\sqrt{n_t}}$
52	6	2^{15}	2117	4	1122.508244	1175
52	9	2^{15}	3086	4	1607.008244	2144
52	14	2^{16}	4966	5	2547.008244	2959
52	19	2^{16}	6675	5	3401.508244	4668
52	25	2^{17}	9196	6	4662.008244	4932
52	52	2^{18}	19898	7	10013.008244	10865
80	6	2^{16}	2289	3	1400.532977	1784
80	9	2^{16}	3314	4	1785.016488	2308
80	14	2^{17}	5288	5	2772.016488	3153
80	19	2^{17}	7089	5	3672.516488	4954
80	25	2^{18}	9721	6	4988.516488	5201
80	38	2^{18}	14649	6	7452.516488	10129

In Table 1, λ is the security parameter, κ is the multilinearity parameter.

5 Conclusion

After GGH scheme providing encoding of zero is known to be insecure, the CSPR 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 CSPR. By applying the method to GGH scheme, we could attack the GGH scheme. Therefore, our results imply that security of the GGH scheme is not guaranteed not depending on whether we are given a small encoding of zero or not.

Our algorithm to solve the CSPR heavily relies on the fact that n is a power of two. Hence it would be an interesting problem to find how to solve the CSPR for general n.

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.

[BR13] Zvika Brakerski and Guy N Rothblum. Obfuscating conjunctions. In *Advances in Cryptology–CRYPTO 2013*, pages 416–434. 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.

[GGH13a] Sanjam Garg, Craig Gentry, and Shai Halevi. Candidate multilinear maps from ideal lattices. In *Eurocrypt*, volume 7881, pages 1–17. Springer, 2013.

[GGH+13b] Shelly Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Anant Sahai, and Brent Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. In *Foundations of Computer Science (FOCS), 2013 IEEE 54th Annual Symposium on*, pages 40–49. IEEE, 2013.

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

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

[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.