New multilinear maps from ideal lattices

Gu Chunsheng
School of Computer Engineering, Jiangsu University of Technology, Changzhou 213001, China
E-mail: chunsheng_gu@163.com

Sep 16, 2015

Abstract. Recently, Hu and Jia presented an efficient attack on the GGH13 map. They show that the MPKE and WE based on GGH13 with public tools of encoding are not secure. Currently, an open problem is to fix GGH13 with functionality-preserving. By modifying zero-testing parameter and using switching modulus method, we present a new construction of multilinear map from ideal lattices. Our construction maintains functionality of GGH13 with public tools of encoding, such as the applications of GGH13-based MPKE and WE. The security of our construction depends upon new hardness assumption.
Keywords. Multilinear maps, Ideal lattices, Multipartite Diffie-Hellman key exchange, Witness encryption, Zeroizing attack

1 Introduction

Current graded encoding schemes [GGH13, CLT13, GGH15] suffer from zeroizing attacks [GGH13, CHL+15, CGH+15, HJ15], which were used to break many applications and hardness assumptions based on these graded encoding schemes. These zeroizing attacks are all using zero-testing procedure to setup a system of equations in the secret parameters of scheme, and solve the system of equations to obtain the needed quantities.

The CLT13 scheme is completely broken by an extension of zeroizing attack from Cheon et al. [CHL+15]. To fix the CLT13 construction, Garg, Gentry, Halevi and Zhandry [GGH+14], and Boneh, Wu and Zimmerman [BWZ14] respectively presented two candidate fixes of multilinear maps over the integers. However, Coron et al. [CGH+15] extended Cheon et al.'s attack [CHL+15] to setting where no encoding of zero below top level are available. As a result, these two fixes [GGH+14, BWZ14] of the CLT13 scheme can also be defeated using a variant of Cheon et al.'s zeroizing attack [CGH+15]. Recently, Coron, Lepoint and Tibouchi [CLT15] presented a new version of the CLT13 construction by modifying zero-testing parameter. Currently, no polynomial time attacks are found for the CLT15 scheme.

The GGH13 scheme is first suffered from the weak discrete logarithm attack presented by authors themselves [GGH13]. By using the weak-DL attack, one can get related information of some secret parameters in the scheme such as basis of secret element. As a result, some problems, such as the subgroup membership problem and the decisional linear problem, are become easy. Very recently, Hu and Jia [HJ15a] presented an efficient weak-DL-based attack on the GGH13 scheme, which breaks the GGH-based applications on multipartite key exchange (MPKE) and witness encryption (WE) based on the hardness of 3-exact cover problem. To fix the GGH13 scheme, Gentry, Halevi and Lepoint recently described a variant of the GGH13 candidate scheme [GGH13a], in which the linear zero-testing procedure from [GGH13a] is replaced by a quadratic (or higher-degree) procedure. However, Brakerski et al. [BGH+15] have showed that this variant of the GGH13 scheme fails to thwart zeroizing attacks. Thus, it is still an open problem to immunize the GGH13 scheme against zeroizing attacks.

The GGH13 map. The GGH13 map works in a polynomial ring $R=\mathbb{Z}[x]/\langle x^n+1\rangle$, where n is a positive integer. A random large integer q, a secret short ring element $\mathbf{g}\in R$, and a secret random invertible element $\mathbf{z}\in R_q=R/qR$ are chosen during generating the public parameters of the GGH13 construction. A plaintext element $\mathbf{e}$ in $R/\mathbf{g}R$ is encoded at level-k as $\left[\mathbf{c}/\mathbf{z}^k\right]_q$, where $\mathbf{c}$ is a small element in the coset $e_I=\mathbf{e}+\mathbf{rg}$ for some $\mathbf{r}\in R$. Encodings at the same level can be added and subtracted as long as the numerator of the sum of the encodings is not reduced modulo q. Similarly, encodings at levels i, j can be multiplied so long as the numerator of the product of the encodings is not reduced modulo q. A zero-testing parameter $\mathbf{p}_{zt} = \left[\mathbf{h}\mathbf{z}^{\kappa} / \mathbf{g}\right]_q$ is presented to test for zero at a level-κ encoding. Given a level-κ encoding $\mathbf{u} = \left[\mathbf{c} / \mathbf{z}^{\kappa}\right]_q$, one computes $\left[\mathbf{u} \cdot \mathbf{p}_{zt}\right]_q$ and checks if the norm of $\left[\mathbf{u} \cdot \mathbf{p}_{zt}\right]_q$ is smaller than q to determine whether $\mathbf{u}$ is zero.

Hu-Jia attack. Assume that $\mathrm{par}_0 = \left\{q, \mathbf{y}, \mathbf{x}_i, i \in [\![\tau]\!], \mathbf{p}_{zt}\right\}$ is the public parameters of the GGH13 map, where $\mathbf{y} = \left[(1+\mathbf{ag}) / \mathbf{z}\right]_q$, $\mathbf{x}_i = \left[(\mathbf{a}_i\mathbf{g}) / \mathbf{z}\right]_q, i \in [\![\tau]\!]$. Given an arbitrary level-k encoding $\mathbf{u} = \left[\mathbf{c} / \mathbf{z}^{k}\right]_q$, one computes using zeroizing attack

$$\mathbf{v}_{k,i,j} = \left[\mathbf{u} \cdot \mathbf{x}_i^j \cdot \mathbf{y}^{\kappa-k-j} \cdot \mathbf{p}_{zt}\right]_q = \left[\mathbf{hc}(\mathbf{a}_i)^j \mathbf{g}^{j-1} (1+\mathbf{ag})^{\kappa-k-j}\right]_q,$$

where $1 \le k < \kappa, 1 \le j < \kappa$ and $k + j \le \kappa$.

Since $\mathbf{v}_{k,i,j}$ is not reduced modulo q, $\mathbf{v}_{k,i,j}$ contains a factor $\mathbf{g}$ when $1 < j$. As a result, one can obtain a basis of the secret element $\mathbf{g}$. Based on the weak-DL attack, Hu and Jia [HJ15a] have broken two applications of MPKE and WE based on the GGH13 map.

Our contribution. Our main contribution is to construct a new multilinear map using ideal lattices. Our construction improves the GGH13 map in three aspects: introducing new noise term by using three-encodings, modifying zero-testing parameter, and using switching modulus technique. Our construction maintains the same functionality as the GGH13 map. We briefly describe our construction as follows.

We first choose large integers q_1, q_2, q_3, secret short ring elements $\mathbf{g}_1, \mathbf{g}_2, \mathbf{g}_3 \in R$, and secret random invertible elements $\mathbf{z}_t \in R_{q_t} = R / q_t R$. A plaintext element $\mathbf{e}$ in $R / \mathbf{g}R$ is encoded at level-k as $\left(\left[\mathbf{c}_1 / \mathbf{z}_1^k\right]_{q_1}, \left[\mathbf{c}_2 / \mathbf{z}_2^k\right]_{q_2}, \left[\mathbf{c}_3 / \mathbf{z}_3^k\right]_{q_3}\right)$, where $\mathbf{c}_1$ is a small element in the coset $e_I = \mathbf{e} + \mathbf{r}_1\mathbf{g}_1$ for some $\mathbf{r}_1 \in R$ such that $\mathbf{c}_1 = \mathbf{c}_2$ and $\mathbf{c}_1 = \mathbf{c}_3 \bmod \mathbf{g}_3$. For this three-encodings, we design new zero-testing parameters

$$\mathbf{p}_{zt,1} = \left[\mathbf{h}_{1,0}\mathbf{z}_0 + \mathbf{z}_1^{\kappa}\left(\mathbf{h}_1 \cdot \left[\mathbf{g}_1^{-1}\right]_{q_1} + \mathbf{h}_2 \cdot \left[\mathbf{g}_2^{-1}\right]_{q_1} + \mathbf{h}_3 \cdot \left[\mathbf{g}_3^{-1}\right]_{q_1}\right)\right]_{q_1},$$

$$\mathbf{p}_{zt,2} = \left[\mathbf{z}_2^{\kappa}\left(\mathbf{h}_{1,0}\mathbf{z} + (\mathbf{h}_2 + \mathbf{h}_{2,0}\mathbf{g}_2)\left\lfloor q_2 / q_1 \cdot \left[\mathbf{g}_2^{-1}\right]_{q_1}\right\rfloor\right)\right]_{q_2},$$

$$\mathbf{p}_{zt,3} = \left[\mathbf{z}_3^{\kappa}(\mathbf{h}_3 + \mathbf{h}_{3,0}\mathbf{g}_3)\left\lfloor q_3 / q_1 \cdot \left[\mathbf{g}_3^{-1}\right]_{q_1}\right\rfloor\right]_{q_3},$$

where $\mathbf{z}_0 \in R_{q_1}, \mathbf{z} = \left\lfloor q_2 / q_1 \cdot \left[\mathbf{z}_0 / \mathbf{z}_1^{\kappa}\right]_{q_1}\right\rfloor$.

Given a level-κ encoding $(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)$, one computes $\mathbf{v} = \left[\left\lfloor \frac{q_3}{q_1} \cdot \left[\mathbf{u}_1 \cdot \mathbf{p}_{zt,1}\right]_{q_1}\right\rfloor - \left\lfloor \frac{q_3}{q_2} \cdot \left[\mathbf{u}_2 \cdot \mathbf{p}_{zt,2}\right]_{q_2}\right\rfloor - \left[\mathbf{u}_3 \cdot \mathbf{p}_{zt,3}\right]_{q_3}\right]_{q_3}$ and checks if the norm of $\mathbf{v}$ is smaller than q_3 to determine whether $\mathbf{u}$ is zero.

Now, using the weak-DL attack, one can no longer obtain a basis of $\mathbf{g}_1$. The aim that we include $\mathbf{z}_0, \mathbf{z}$ in the zero-testing parameters is to thwart the Coron et al. attack [CGH+15]. Since the successful key of the attack [CGH+15] is to obtain simple equations over the rational by zero-testing procedure. The details are described in Section 4.

Furthermore, our construction seemly supports more applications than the GGH13 map. Owing to adding new noise term, one can no longer yield a basis of $\mathbf{g}_1$. Hence, we conjecture that the membership group problem (SubM) and the decisional linear (DLIN) problem are hard in our construction. However, in the GGH13 map, one can compute non-reduced ring elements over modulus q_3 and a basis of $\mathbf{g}_1$. As a result, the SubM problem and the DLIN problem are easy in the GGH13 map.

Our second contribution is to describe the applications of MPKE and WE using our new multilinear map. Since these applications are attacked by [HJ15a], fix for them is urgently required. The construction of MPKE and WE based on our map are same as ones based on GGH13.

Organization. Section 2 recalls some background. Section 3 describes our new construction using ideal lattices. Section 4 gives security analysis for our construction. Section 5 presents two applications of MPKE and WE based on our construction. Finally, Section 6 draws conclusion.

2 Preliminaries

2.1 Notations

We denote $\mathbb{Z},\mathbb{Q},\mathbb{R}$ the ring of integers, the field of rational numbers, and the field of real numbers. We take n as a positive integer and a power of 2. Notation $[\![n]\!]$ denotes the set $\{1,2,\cdots,n\}$, and $[a]_q$ the absolute minimum residual system $[a]_q = a \bmod q \in (-q/2, q/2]$. Vectors and matrices are denoted in bold, such as $\mathbf{a},\mathbf{b},\mathbf{c}$ and $\mathbf{A},\mathbf{B},\mathbf{C}$. The j-th entry of $\mathbf{a}$ is denoted as a_j, the element of the i-th row and j-th colomn of $\mathbf{A}$ is denoted as $A_{i,j}$ (or $A[i,j]$). Notation $\|\mathbf{a}\|_\infty$ ($\|\mathbf{a}\|$ for short) denotes the infinity norm of $\mathbf{a}$. The polynomial ring $\mathbb{Z}[x]/\langle x^n+1\rangle$ is denoted by R, and $\mathbb{Z}_q[x]/\langle x^n+1\rangle$ by R_q. The elements in R and R_q are denoted in bold as well. Similarly, notation $[\mathbf{a}]_q$ denotes each entry (or each coefficient) $a_i \in (-p/2, p/2]$ of $\mathbf{a}$.

2.2 Lattices and Ideal Lattices

An n-dimension full-rank lattice $L \subset \mathbb{R}^n$ is the set of all integer linear combinations $\sum_{i=1}^n y_i \mathbf{b}_i$ of n linearly independent vectors $\mathbf{b}_i \in \mathbb{R}^n$. If we arrange the vectors $\mathbf{b}_i$ as the columns of matrix $\mathbf{B} \in \mathbb{R}^{n\times n}$, then $L = \{\mathbf{B}\mathbf{y} : \mathbf{y} \in \mathbb{Z}^n\}$. We say that $\mathbf{B}$ spans L if $\mathbf{B}$ is a basis for L. Given a basis $\mathbf{B}$ of L, we define $P(\mathbf{B}) = \{\mathbf{B}\mathbf{y} \mid \mathbf{y} \in \mathbb{R}^n, \forall i : -1/2 \le y_i < 1/2\}$ as the parallelization corresponding to $\mathbf{B}$. Let $\det(\mathbf{B})$ denote the determinant of $\mathbf{B}$.

Given $\mathbf{g} \in R$, let $I = \langle \mathbf{g} \rangle$ be the principal ideal lattice in R generated by $\mathbf{g}$, whose $\mathbb{Z}$-basis is $Rot(\mathbf{g}) = (\mathbf{g}, x\cdot\mathbf{g}, ..., x^{n-1}\cdot\mathbf{g})$.

Given $\mathbf{c} \in \mathbb{R}^n, \sigma > 0$, the Gaussian distribution of a lattice L is defined as $\forall \mathbf{x} \in L$, $D_{L,\sigma,\mathbf{c}} = \rho_{\sigma,\mathbf{c}}(\mathbf{x}) / \rho_{\sigma,\mathbf{c}}(L)$, where $\rho_{\sigma,\mathbf{c}}(\mathbf{x}) = \exp(-\pi \|\mathbf{x}-\mathbf{c}\|^2 / \sigma^2)$, $\rho_{\sigma,\mathbf{c}}(L) = \sum_{x\in L} \rho_{\sigma,\mathbf{c}}(\mathbf{x})$. In the following, we will write $D_{\mathbb{Z}^n,\sigma,0}$ as $D_{\mathbb{Z}^n,\sigma}$. We denote a Gaussian sample as $\mathbf{x} \leftarrow D_{L,\sigma}$ (or $\mathbf{d} \leftarrow D_{I,\sigma}$) over the lattice L (or ideal lattice I).

2.3 Multilinear Maps

Definition 2.1 (Multilinear Map [BS03]). For $\kappa+1$ cyclic groups $G_1,...,G_\kappa,G_T$ of the same order q, a κ-multilinear map $e: G_1\times\cdots\times G_\kappa \to G_T$ has the following properties:

(1) Elements $\{g_j \in G_j\}_{j=1,...,\kappa}$, index $j\in[\![\kappa]\!]$, and integer $a\in\mathbb{Z}_q$ hold that

$$e(g_1,\cdots,a\cdot g_j,\cdots,g_\kappa)=a\cdot e(g_1,\cdots,g_\kappa)$$

(2) Map e is non-degenerate in the following sense: if elements $\{g_j \in G_j\}_{j=1,...,\kappa}$ are generators of their respective groups, then $e(g_1,\cdots,g_\kappa)$ is a generator of G_T.

Definition 2.2 (κ-Graded Encoding System [GGH13]). A κ-graded encoding system over R is a set system of $S=\{S_j^{(\alpha)}\subset R:\alpha\in R, j\in[\![\kappa]\!]\}$ with the following properties:

(1) For every index $j\in[\![\kappa]\!]$, the sets $\{S_j^{(\alpha)}:\alpha\in R\}$ are disjoint.

(2) Binary operations '$+$' and '$-$' exist, such that every α_1,α_2, every index $j\in[\![\kappa]\!]$, and every $u_1\in S_j^{(\alpha_1)}$ and $u_2\in S_j^{(\alpha_2)}$ hold that $u_1+u_2\in S_j^{(\alpha_1+\alpha_2)}$ and $u_1-u_2\in S_j^{(\alpha_1-\alpha_2)}$, where $\alpha_1+\alpha_2$ and $\alpha_1-\alpha_2$ are the addition and subtraction operations in R respectively.

(3) Binary operation '$\times$' exists, such that every α_1,α_2, every index $j_1,j_2\in[\![\kappa]\!]$ with $j_1+j_2\le\kappa$, and every $u_1\in S_{j_1}^{(\alpha_1)}$ and $u_2\in S_{j_2}^{(\alpha_2)}$ hold that $u_1\times u_2\in S_{j_1+j_2}^{(\alpha_1\times\alpha_2)}$, where $\alpha_1\times\alpha_2$ is the multiplication operation in R and j_1+j_2 is the integer addition.

3 Our new construction

Setting the parameters. Let λ be the security parameter, κ the multilinearity level, n the dimension of elements of R. Concrete parameters are set as $\sigma=\sqrt{\lambda n}$, $\sigma'=\lambda n^{1.5}$, $\sigma^*=2^\lambda$, $q_1,q_2\ge 2^{8\kappa\lambda}n^{O(\kappa)}$, $m=2$, $n>\widetilde{O}(\kappa\lambda^2)$, $\tau=O(n^2)$, $\rho=O(n)$.

3.1 Construction

Instance generation: $(\text{par})\leftarrow\text{InstGen}(1^\lambda,1^\kappa)$.

(1) Choose two primes $q_t\ge 2^{8\kappa\lambda}n^{O(\kappa)}, t\in[\![3]\!]$ with $q_1>2^\lambda\cdot q_2>2^{2\lambda}\cdot q_3$.

(2) Choose $\mathbf{g}_t\leftarrow D_{\mathbb{Z}^n,\sigma}, t\in[\![3]\!]$ in R so that $\|\mathbf{g}_t^{-1}\|<n^2$.

(3) Choose $\mathbf{a}_1,\mathbf{b}_3,\mathbf{a}_{1,i},\mathbf{b}_{3,i}\leftarrow D_{\mathbb{Z}^n,\sigma'}, i\in[\![\tau]\!]$ in R;

Choose $\mathbf{h}_{t,0},\mathbf{h}_t\leftarrow D_{\mathbb{Z}^n,\sqrt{q_3}}, t\in[\![3]\!]$ in R.

(4) Choose uniformly random elements $\mathbf{z}_0\leftarrow R_{q_1}$, $\mathbf{z}_t\leftarrow R_{q_t}, t\in[\![3]\!]$ with $\mathbf{z}_t^{-1}\in R_{q_t}$.

(5) Set $\mathbf{e}_1=(\mathbf{a}_1\mathbf{g}_1+1)\bmod \mathbf{g}_3$, namely $\mathbf{a}_1\mathbf{g}_1+1=\mathbf{b}_1\mathbf{g}_3+\mathbf{e}_1$ so that $\|\mathbf{b}_1\|<n^2$;

$\mathbf{e}_{1,i}=(\mathbf{a}_{1,i}\mathbf{g}_1)\bmod \mathbf{g}_3, i\in[\![\tau]\!]$, namely $\mathbf{a}_{1,i}\mathbf{g}_1=\mathbf{b}_{1,i}\mathbf{g}_3+\mathbf{e}_{1,i}$ so that $\|\mathbf{b}_{1,i}\|<n^2$.

(6) Set $\mathbf{y}_1=\left[\dfrac{\mathbf{a}_1\mathbf{g}_1+1}{\mathbf{z}_1}\right]_{q_1}$ and $\mathbf{x}_{1,i}=\left[\dfrac{\mathbf{a}_{1,i}\mathbf{g}_1}{\mathbf{z}_1}\right]_{q_1}$;

$$\mathbf{y}_2 = \left[\frac{\mathbf{a}_1\mathbf{g}_1+1}{\mathbf{z}_2}\right]_{q_2} \quad \text{and} \quad \mathbf{x}_{2,i} = \left[\frac{\mathbf{a}_{1,i}\mathbf{g}_1}{\mathbf{z}_2}\right]_{q_2};$$

$$\mathbf{y}_3 = \left[\frac{\mathbf{b}_3\mathbf{g}_3+\mathbf{e}_1}{\mathbf{z}_3}\right]_{q_3} \quad \text{and} \quad \mathbf{x}_{3,i} = \left[\frac{\mathbf{b}_{3,i}\mathbf{g}_3+\mathbf{e}_{1,i}}{\mathbf{z}_3}\right]_{q_3}.$$

(7) Set $\mathbf{z} = \left\lfloor \frac{q_2}{q_1}\left[\frac{\mathbf{z}_0}{\mathbf{z}_1^{\kappa}}\right]_{q_1} \right\rceil$.

(8) Set $\mathbf{p}_{zt,1} = \left[\mathbf{h}_{1,0}\mathbf{z}_0 + \mathbf{z}_1^{\kappa}\left(\mathbf{h}_1 \cdot \left[\mathbf{g}_1^{-1}\right]_{q_1} + \mathbf{h}_2 \cdot \left[\mathbf{g}_2^{-1}\right]_{q_1} + \mathbf{h}_3 \cdot \left[\mathbf{g}_3^{-1}\right]_{q_1}\right)\right]_{q_1}$,

$\mathbf{p}_{zt,2} = \left[\mathbf{z}_2^{\kappa}\left(\mathbf{h}_{1,0}\mathbf{z} + (\mathbf{h}_2 + \mathbf{h}_{2,0}\mathbf{g}_2)\mathbf{g}_{2,q_2}^{-1}\right)\right]_{q_2}$,

$\mathbf{p}_{zt,3} = \left[\mathbf{z}_3^{\kappa}(\mathbf{h}_3 + \mathbf{h}_{3,0}\mathbf{g}_3)\mathbf{g}_{3,q_3}^{-1}\right]_{q_3}$,

where $\mathbf{g}_{2,q_2}^{-1} = \left\lfloor (q_2/q_1) \cdot \left[\mathbf{g}_2^{-1}\right]_{q_1} \right\rceil, \mathbf{g}_{3,q_3}^{-1} = \left\lfloor (q_3/q_1) \cdot \left[\mathbf{g}_3^{-1}\right]_{q_1} \right\rceil$.

(9) Output the public parameters $\text{par} = \left\{\left\{q_t, \mathbf{y}_t, \{\mathbf{x}_{t,i}\}_{i\in[\![\tau]\!]}, \mathbf{p}_{zt,t}\right\}_{t\in[\![3]\!]}\right\}$.

Generating level-k encoding: $(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3) \leftarrow \text{Enc}(\text{par}, k, \mathbf{d})$.

(1) Sample $\mathbf{r}_i \leftarrow D_{\mathbb{Z}^n,\sigma^*}, i \in [\![\tau]\!]$;

(2) Given $\mathbf{d} \leftarrow D_{\mathbb{Z}^n,\sigma'}$, compute $\mathbf{u}_t = \left[\mathbf{d}\cdot(\mathbf{y}_t)^k + \sum_{i=1}^{\tau}\mathbf{r}_i \cdot (\mathbf{x}_{t,i})^k\right]_{q_t}, t \in [\![3]\!]$;

(3) Output $(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)$ as a level-k encoding of $\mathbf{d}$.

Adding encodings: $(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3) \leftarrow \text{Add}\left(\text{par}, k, (\mathbf{u}_{1,1}, \mathbf{u}_{2,1}, \mathbf{u}_{3,1}), \cdots, (\mathbf{u}_{1,s}, \mathbf{u}_{2,s}, \mathbf{u}_{3,s})\right)$.

(1) Given s level-k encodings $(\mathbf{u}_{1,l}, \mathbf{u}_{2,l}, \mathbf{u}_{3,l})$, compute $\mathbf{u}_t = \left[\sum_{l=1}^{s}\mathbf{u}_{t,l}\right]_{q_t}, t \in [\![3]\!]$.

(2) Output a level-k encoding $(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)$.

Multiplying encodings: $(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3) \leftarrow \text{Mul}\left(\text{par}, 1, (\mathbf{u}_{1,1}, \mathbf{u}_{2,1}, \mathbf{u}_{3,1}), \cdots, (\mathbf{u}_{1,k}, \mathbf{u}_{2,k}, \mathbf{u}_{3,k})\right)$.

(1) Given k level-1 encodings $(\mathbf{u}_{1,l}, \mathbf{u}_{2,l}, \mathbf{u}_{3,l})$, compute $\mathbf{u}_t = \left[\prod_{l=1}^{k}\mathbf{u}_{t,l}\right]_{q_t}, t \in [\![3]\!]$.

(2) Output a level-k encoding $(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)$.

Zero testing: $\text{isZero}\left(\text{par}, (\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)\right)$.

Given a level-κ encoding $(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)$, to determine whether $\mathbf{u}_1$ is a level-κ encoding of zero for $\mathbf{g}_1$, we compute $\mathbf{v} = \left[\left\lfloor \frac{q_3}{q_1} \cdot \left[\mathbf{u}_1 \cdot \mathbf{p}_{zt,1}\right]_{q_1} \right\rceil - \left\lfloor \frac{q_3}{q_2} \cdot \left[\mathbf{u}_2 \cdot \mathbf{p}_{zt,2}\right]_{q_2} \right\rceil - \left[\mathbf{u}_3 \cdot \mathbf{p}_{zt,3}\right]_{q_3}\right]_{q_3}$ and check whether $\|\mathbf{v}\|$ is short:

$$\text{isZero}\left(\text{par}, (\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)\right) = \begin{cases} 1 & \text{if } \|\mathbf{v}\| < q_3^{3/4} \\ 0 & \text{otherwise} \end{cases}.$$

Extraction: $sk \leftarrow \text{Ext}\left(\text{par}, (\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)\right)$.

Given a level-κ encoding $(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)$, we compute

$\mathbf{v}=\left[\left[\frac{q_3}{q_1}\cdot\left[\mathbf{u}_1\cdot\mathbf{p}_{zt,1}\right]_{q_1}\right]-\left[\frac{q_3}{q_2}\cdot\left[\mathbf{u}_2\cdot\mathbf{p}_{zt,2}\right]_{q_2}\right]-\left[\mathbf{u}_3\cdot\mathbf{p}_{zt,3}\right]_{q_3}\right]_{q_3}$, and collect $\eta=(\log q)/4-\lambda$ most-significant bits of each of the n coefficients of $\mathbf{v}$:

$$\mathrm{Ext}\left(\mathrm{par},\left(\mathbf{u}_1,\mathbf{u}_2,\mathbf{u}_3\right)\right)=\mathrm{Extract}_s\left(\mathrm{msbs}_\eta\left(\mathbf{v}\right)\right).$$

Remark 3.1 In our construction, switching modulus and using $\mathbf{z}_0,\mathbf{z}$ in the zero-testing parameters are to avoid the attack in [CGH+15].

3.2 Correctness

Lemma 3.2 The algorithm $\mathrm{InstGen}(1^\lambda,1^\kappa)$ runs in polynomial time.

Lemma 3.3 The encoding $\left(\mathbf{u}_1,\mathbf{u}_2,\mathbf{u}_3\right)\leftarrow\mathrm{Enc}\left(\mathrm{par},k,\mathbf{d}\right)$ is a level-k encoding.

Proof. We only need to show that $\mathbf{u}_1$ is a level-k encoding of $\mathbf{d}$ for the ideal lattice $\langle\mathbf{g}_1\rangle$, $\mathbf{u}_1,\mathbf{u}_2$ have same numerator, and level-k encodings $\mathbf{u}_1,\mathbf{u}_3$ encode same level-0 encoding for the ideal lattice $\langle\mathbf{g}_3\rangle$.

(1) By $\mathbf{u}_t=\left[\mathbf{d}\cdot(\mathbf{y}_t)^k+\sum_{i=1}^{\tau}\mathbf{r}_i\cdot(\mathbf{x}_{t,i})^k\right]_{q_t}$, for $t\in\{1,2\}$ we have

$$\begin{aligned}\mathbf{u}_t&=\left[\mathbf{d}\cdot(\mathbf{y}_t)^k+\sum_{i=1}^{\tau}\mathbf{r}_i\cdot(\mathbf{x}_{t,i})^k\right]_{q_t}\\&=\left[\mathbf{d}\cdot\left(\frac{\mathbf{a}_1\mathbf{g}_1+1}{\mathbf{z}_t}\right)^k+\sum_{i=1}^{\tau}\mathbf{r}_i\cdot\left(\frac{\mathbf{a}_{1,i}\mathbf{g}_1}{\mathbf{z}_t}\right)^k\right]_{q_t}\\&=\left[\frac{\mathbf{d}\cdot\left(\mathbf{a}_1\mathbf{g}_1+1\right)^k+\sum_{i=1}^{\tau}\mathbf{r}_i\cdot\left(\mathbf{a}_{1,i}\mathbf{g}_1\right)^k}{\mathbf{z}_t^k}\right]_{q_t},\\&=\left[\frac{\mathbf{a}\mathbf{g}_1+\mathbf{d}}{\mathbf{z}_t^k}\right]_{q_t}\end{aligned}$$

where $\mathbf{a}=\left(\mathbf{d}\cdot\left(\mathbf{a}_1\mathbf{g}_1+1\right)^k+\sum_{i=1}^{\tau}\mathbf{r}_i\cdot\left(\mathbf{a}_{1,i}\mathbf{g}_1\right)^k-\mathbf{d}\right)/\mathbf{g}_1$.

Thus, $\mathbf{u}_1$ is a level-k encoding of the level-0 encoding $\mathbf{d}$ for $\langle\mathbf{g}_1\rangle$, and $\mathbf{u}_1,\mathbf{u}_2$ have same numerator $\mathbf{a}\mathbf{g}_1+\mathbf{d}$.

(2) For $t\in\{1,3\}$ we have

$$\begin{aligned}\mathbf{u}_t&=\left[\mathbf{d}\cdot(\mathbf{y}_t)^k+\sum_{i=1}^{\tau}\mathbf{r}_i\cdot(\mathbf{x}_{t,i})^k\right]_{q_t}\\&=\left[\mathbf{d}\cdot\left(\frac{\mathbf{b}_t\mathbf{g}_3+\mathbf{e}_1}{\mathbf{z}_t}\right)^k+\sum_{i=1}^{\tau}\mathbf{r}_i\cdot\left(\frac{\mathbf{b}_{t,i}\mathbf{g}_3+\mathbf{e}_{1,i}}{\mathbf{z}_t}\right)^k\right]_{q_t},\\&=\left[\frac{\mathbf{c}_t\mathbf{g}_3+\mathbf{e}}{\mathbf{z}_t^k}\right]_{q_t}\end{aligned}$$

where $\mathbf{e}=\mathbf{d}\cdot\left(\mathbf{e}_1\right)^k+\sum_{i=1}^{\tau}\mathbf{r}_i\cdot\left(\mathbf{e}_{1,i}\right)^k$, $\mathbf{c}_t=\left(\mathbf{d}\cdot\left(\mathbf{b}_t\mathbf{g}_3+\mathbf{e}_1\right)^k+\sum_{i=1}^{\tau}\mathbf{r}_i\cdot\left(\mathbf{b}_{t,i}\mathbf{g}_3+\mathbf{e}_{1,i}\right)^k-\mathbf{e}\right)/\mathbf{g}_3$.

So, the level-k encodings $\mathbf{u}_1, \mathbf{u}_3$ encode same level-0 encoding for $\langle \mathbf{g}_3 \rangle$ □

Lemma 3.4 The encoding $(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3) \leftarrow \mathrm{Add}\left(\mathrm{par}, k, (\mathbf{u}_{1,1}, \mathbf{u}_{2,1}, \mathbf{u}_{3,1}), \cdots, (\mathbf{u}_{1,s}, \mathbf{u}_{2,s}, \mathbf{u}_{3,s})\right)$ is a level-k encoding.

Proof. Since for $\langle \mathbf{g}_1 \rangle$, a level-$k$ encoding $\mathbf{u}_{t,l}, t \in \{1,2\}$ has the form $\mathbf{u}_{t,l} = \left[\frac{\mathbf{r}_l \mathbf{g}_1 + \mathbf{d}_l}{\mathbf{z}_t^k} \right]_{q_t}$, then the sum is

$$\mathbf{u}_t = \left[\sum_{l=1}^{s} \mathbf{u}_{t,l} \right]_{q_t} = \left[\frac{\sum_{l=1}^{s} (\mathbf{r}_l \mathbf{g}_1 + \mathbf{d}_l)}{\mathbf{z}_t^k} \right]_{q_t} = \left[\frac{\mathbf{r}\mathbf{g}_1 + \mathbf{d}}{\mathbf{z}_t^k} \right]_{q_t},$$

where $\mathbf{r} = \sum_{l=1}^{s} \mathbf{r}_l$ and $\mathbf{d} = \sum_{l=1}^{s} \mathbf{d}_l$.

Namely, $\mathbf{u}_1$ is a level-k encoding for the ideal lattice $\langle \mathbf{g}_1 \rangle$, and $\mathbf{u}_1, \mathbf{u}_2$ have same numerator $\mathbf{r}\mathbf{g}_1 + \mathbf{d}$.

Again for $\langle \mathbf{g}_3 \rangle$, a level-$k$ encoding $\mathbf{u}_{t,l}, t \in \{1,3\}$ has the form $\mathbf{u}_{t,l} = \left[\frac{\mathbf{c}_{t,l} \mathbf{g}_3 + \mathbf{e}_l}{\mathbf{z}_t^k} \right]_{q_t}$.

Thus, we have

$$\mathbf{u}_t = \left[\sum_{l=1}^{s} \mathbf{u}_{t,l} \right]_{q_t} = \left[\frac{\sum_{l=1}^{s} (\mathbf{c}_{t,l} \mathbf{g}_3 + \mathbf{e}_l)}{\mathbf{z}_t^k} \right]_{q_t} = \left[\frac{\mathbf{c}_t \mathbf{g}_3 + \mathbf{e}}{\mathbf{z}_t^k} \right]_{q_t},$$

where $\mathbf{c}_t = \sum_{l=1}^{s} \mathbf{c}_{t,l}$ and $\mathbf{e} = \sum_{l=1}^{s} \mathbf{e}_l$.

That is, level-k encodings $\mathbf{u}_1, \mathbf{u}_3$ encode same level-0 encoding for $\langle \mathbf{g}_3 \rangle$. □

Lemma 3.5 The encoding $(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3) \leftarrow \mathrm{Mul}\left(\mathrm{par}, 1, (\mathbf{u}_{1,1}, \mathbf{u}_{2,1}, \mathbf{u}_{3,1}), \cdots, (\mathbf{u}_{1,k}, \mathbf{u}_{2,k}, \mathbf{u}_{3,k})\right)$ is a level-k encoding.

Proof. Since for $\langle \mathbf{g}_1 \rangle$, $\mathbf{u}_{t,l} = \left[\frac{\mathbf{r}_l \mathbf{g}_1 + \mathbf{d}_l}{\mathbf{z}_t} \right]_{q_t}$, $t \in \{1,2\}$, their product is:

$$\mathbf{u}_t = \left[\prod_{l=1}^{k} \mathbf{u}_{t,l} \right]_{q_t} = \left[\prod_{l=1}^{k} \frac{\mathbf{r}_l \mathbf{g}_1 + \mathbf{d}_l}{\mathbf{z}_t} \right]_{q_t} = \left[\frac{\prod_{j=1}^{k} (\mathbf{r}_l \mathbf{g}_1 + \mathbf{d}_l)}{\mathbf{z}_t^k} \right]_{q_t} = \left[\frac{\mathbf{r}\mathbf{g}_1 + \mathbf{d}}{\mathbf{z}_t^k} \right]_{q_t},$$

where $\mathbf{d} = \prod_{l=1}^{k} \mathbf{d}_l$, $\mathbf{r} = (\prod_{l=1}^{k} (\mathbf{r}_l \mathbf{g}_1 + \mathbf{d}_l) - \mathbf{d}) / \mathbf{g}_1$.

Again for $\langle \mathbf{g}_3 \rangle$, the level-$1$ encoding $\mathbf{u}_{t,l}, t \in \{1,3\}$ has the form $\mathbf{u}_{t,l} = \left[\frac{\mathbf{c}_{t,l} \mathbf{g}_3 + \mathbf{e}_l}{\mathbf{z}_t} \right]_{q_t}$.

Thus, we have

$$\mathbf{u}_t = \left[\prod_{l=1}^{k} \frac{\mathbf{c}_{t,l} \mathbf{g}_3 + \mathbf{e}_l}{\mathbf{z}_t} \right]_{q_t} = \left[\frac{\prod_{l=1}^{k} (\mathbf{c}_{t,l} \mathbf{g}_3 + \mathbf{e}_l)}{\mathbf{z}_t^k} \right]_{q_t} = \left[\frac{\mathbf{c}_t \mathbf{g}_3 + \mathbf{e}}{\mathbf{z}_t^k} \right]_{q_t},$$

where $\mathbf{e} = \prod_{l=1}^{k} \mathbf{e}_l$ and $\mathbf{c}_t = (\prod_{l=1}^{k} (\mathbf{c}_{t,l} \mathbf{g}_3 + \mathbf{e}_l) - \mathbf{e}) / \mathbf{g}_3$. □

Before proving correctness of the zero-testing algorithm, we first describe one lemma about modulus switching and three corollaries.

Lemma 3.6. Suppose that p, q are primes and $\mathbf{v} = [\mathbf{w} \cdot \mathbf{z}]_q$ with $\mathbf{z} \in R_q$ and $\|\mathbf{w}\| << p$. Then,

$$\left\lfloor \frac{p}{q}\mathbf{v} \right\rfloor = \left[\mathbf{w} \cdot \left\lfloor \frac{p}{q}\mathbf{z} \right\rfloor \right]_p + \boldsymbol{\delta} \quad \text{with} \quad \|\boldsymbol{\delta}\| < l_1(\mathbf{w}),$$

where $l_1(\mathbf{w})$ is l_1-norm of $\mathbf{w}$.

Proof. By $\mathbf{v} = [\mathbf{w} \cdot \mathbf{z}]_q = \mathbf{w} \cdot \mathbf{z} - q \cdot \mathbf{k}$, we get

$$\frac{p}{q}\mathbf{v} = \mathbf{w} \cdot \left(\frac{p}{q} \cdot \mathbf{z} \right) - p \cdot \mathbf{k},$$

$$\begin{aligned} \mathbf{w} \cdot \left(\frac{p}{q}\mathbf{z} \right) &= \mathbf{w} \cdot \left\lfloor \frac{p}{q}\mathbf{z} \right\rfloor + \mathbf{w} \cdot \left(\frac{p}{q}\mathbf{z} - \left\lfloor \frac{p}{q}\mathbf{z} \right\rfloor \right) \\ &= \mathbf{w} \cdot \left\lfloor \frac{p}{q}\mathbf{z} \right\rfloor + \mathbf{w} \cdot \boldsymbol{\varepsilon} \end{aligned},$$

where $\|\boldsymbol{\varepsilon}\| < 1$.

Therefore,

$$\begin{aligned} \left\lfloor \frac{p}{q}\mathbf{v} \right\rfloor &= \left\lfloor \frac{p}{q}[\mathbf{w} \cdot \mathbf{z}]_q \right\rfloor \\ &= \left\lfloor \mathbf{w} \cdot \left(\frac{p}{q} \cdot \mathbf{z} \right) - p \cdot \mathbf{k} \right\rfloor \\ &= \mathbf{w} \cdot \left\lfloor \frac{p}{q}\mathbf{z} \right\rfloor + \lfloor \mathbf{w} \cdot \boldsymbol{\varepsilon} \rfloor - p \cdot \mathbf{k} \\ &= \left[\mathbf{w} \cdot \left\lfloor \frac{p}{q}\mathbf{z} \right\rfloor \right]_p + p \cdot \boldsymbol{\beta} + \lfloor \mathbf{w} \cdot \boldsymbol{\varepsilon} \rfloor - p \cdot \mathbf{k} \end{aligned}.$$

By $\left\| \left\lfloor \frac{p}{q}\mathbf{v} \right\rfloor \right\| < p/2$, we have $\boldsymbol{\beta} = \mathbf{k}$ with high probability. That is, $\left\lfloor \frac{p}{q}\mathbf{v} \right\rfloor = \left[\mathbf{w} \cdot \left\lfloor \frac{p}{q}\mathbf{z} \right\rfloor \right]_{q_2} + \boldsymbol{\delta}$ with $\boldsymbol{\delta} = \lfloor \mathbf{w} \cdot \boldsymbol{\varepsilon} \rfloor$. By $\|\boldsymbol{\varepsilon}\| < 1$, we obtain $\|\boldsymbol{\delta}\| < l_1(\mathbf{w})$. □

Corollary 3.7 Suppose that p, q are primes and $\mathbf{v}_t = \left[\mathbf{w}_t \cdot \left[\mathbf{g}_t^{-1} \right]_q \right]_q, t \in [\![3]\!]$ with $\|\mathbf{w}_t\| << p$. Then,

$$\left\lfloor \frac{p}{q}\mathbf{v}_t \right\rfloor = \left[\mathbf{w}_t \cdot \left\lfloor \frac{p}{q}\left[\mathbf{g}_t^{-1} \right]_q \right\rfloor \right]_p + \boldsymbol{\delta}_t \quad \text{with} \quad \|\boldsymbol{\delta}_t\| < l_1(\mathbf{w}_t),$$

where $l_1(\mathbf{w}_t)$ is l_1-norm of $\mathbf{w}_t$.

Proof. By $\left[\mathbf{g}_t^{-1} \right]_q \in R_q$, the result is proved by directly taking $\mathbf{z} = \left[\mathbf{g}_t^{-1} \right]_q$.

Corollary 3.8 Suppose that p, q are primes and $\boldsymbol{\alpha}_t = \left[\mathbf{g}_t \cdot \left\lfloor \frac{p}{q}\left[\mathbf{g}_t^{-1} \right]_q \right\rfloor \right]_p$, $t \in [\![3]\!]$. Then $\|\boldsymbol{\alpha}_t\| < l_1(\mathbf{g}_t) + \lfloor p/q \rfloor$.

Proof. Assume that $\mathbf{v}_t = \left[\mathbf{w}_t \cdot \left[\mathbf{g}_t^{-1} \right]_q \right]_q$ with $\mathbf{w}_t = \mathbf{g}_t$. Then by Lemma 3.6, we have

$$\left\lfloor \frac{p}{q}(1,0,\cdots,0) \right\rfloor = \left\lfloor \frac{p}{q}\mathbf{v}_t \right\rfloor = \left[\mathbf{g}_t \cdot \left\lfloor \frac{p}{q}\left[\mathbf{g}_t^{-1}\right]_q \right\rfloor \right]_p + \boldsymbol{\delta}_t \text{ and } \|\boldsymbol{\delta}_t\| \le l_1(\mathbf{g}_t).$$

Thus, $\boldsymbol{\alpha}_t = \left[\mathbf{g}_t \cdot \left\lfloor \frac{p}{q}\left[\mathbf{g}_t^{-1}\right]_q \right\rfloor \right]_p = \left\lfloor \frac{p}{q}(1,0,\cdots,0) \right\rfloor - \boldsymbol{\delta}_t$ and $\|\boldsymbol{\alpha}_t\| < l_1(\mathbf{g}_t) + \lfloor p/q \rfloor$.

Corollary 3.9 Suppose that $q_t, t \in [\![3]\!]$ are primes and $\mathbf{v} = [\mathbf{w}\cdot\mathbf{z}]_{q_1}$ with $\mathbf{z} \in R_{q_1}$ such that $\|\mathbf{w}\| << q_t, t \in [\![3]\!]$. Then

$$\left\lfloor \frac{q_3}{q_2}\left\lfloor \frac{q_2}{q_1}\mathbf{v} \right\rfloor \right\rfloor = \left[\mathbf{w}\cdot \left\lfloor \frac{q_3}{q_1}\mathbf{z} \right\rfloor \right]_{q_3} + \boldsymbol{\delta} \text{ with } \|\boldsymbol{\delta}\| < \lceil q_3/q_2 \rceil + 1 + l_1(\mathbf{w}),$$

where $l_1(\mathbf{a})$ is l_1-norm of $\mathbf{a}$.

Proof. By $\left\lfloor \frac{q_2}{q_1}\mathbf{v} \right\rfloor = \frac{q_2}{q_1}\mathbf{v} - \boldsymbol{\varepsilon}_1$ with $\|\boldsymbol{\varepsilon}_1\| < 1$, we have $\frac{q_3}{q_2}\left\lfloor \frac{q_2}{q_1}\mathbf{v} \right\rfloor = \frac{q_3}{q_1}\mathbf{v} - \frac{q_3}{q_2}\boldsymbol{\varepsilon}_1$. Thus,

$$\left\lfloor \frac{q_3}{q_2}\left\lfloor \frac{q_2}{q_1}\mathbf{v} \right\rfloor \right\rfloor = \left\lfloor \frac{q_3}{q_1}\mathbf{v} \right\rfloor - \left\lfloor \frac{q_3}{q_2}\boldsymbol{\varepsilon}_1 \right\rfloor - \boldsymbol{\varepsilon}_2 \text{, with } \|\boldsymbol{\varepsilon}_2\| \le 1.$$

By Lemma 3.6, we obtain $\left\lfloor \frac{q_3}{q_1}\mathbf{v} \right\rfloor = \left[\mathbf{w}\cdot \left\lfloor \frac{q_3}{q_1}\mathbf{z} \right\rfloor \right]_p + \boldsymbol{\delta}_0$ with $\|\boldsymbol{\delta}_0\| < l_1(\mathbf{w})$.

Namely, $\left\lfloor \frac{q_3}{q_2}\left\lfloor \frac{q_2}{q_1}\mathbf{v} \right\rfloor \right\rfloor = \left[\mathbf{w}\cdot \left\lfloor \frac{q_3}{q_1}\mathbf{z} \right\rfloor \right]_p + \boldsymbol{\delta}_0 - \left\lfloor \frac{q_3}{q_2}\boldsymbol{\varepsilon}_1 \right\rfloor - \boldsymbol{\varepsilon}_2 = \left[\mathbf{w}\cdot \left\lfloor \frac{q_3}{q_1}\mathbf{z} \right\rfloor \right]_p + \boldsymbol{\delta}$,

where $\boldsymbol{\delta} = \boldsymbol{\delta}_0 - \left\lfloor \frac{q_3}{q_2}\boldsymbol{\varepsilon}_1 \right\rfloor - \boldsymbol{\varepsilon}_2$ and $\|\boldsymbol{\delta}\| < \lceil q_3/q_2 \rceil + 1 + l_1(\mathbf{w})$. □

Lemma 3.10 The zero testing $\text{isZero}(\text{par}, (\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3))$ correctly determines whether $\mathbf{u}_1$ is a level-κ encoding of zero for $\langle \mathbf{g}_1 \rangle$.

Proof. For a level-κ encoding $(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)$, without loss of generality, we assume

$$\mathbf{u}_1 = \left[\frac{\mathbf{r}_1\mathbf{g}_1 + \mathbf{d}_1}{\mathbf{z}_1^\kappa} \right]_{q_1} = \left[\frac{\mathbf{r}_2\mathbf{g}_2 + \mathbf{d}_2}{\mathbf{z}_1^\kappa} \right]_{q_1} = \left[\frac{\mathbf{r}_3\mathbf{g}_3 + \mathbf{d}_3}{\mathbf{z}_1^\kappa} \right]_{q_1},$$

$$\mathbf{u}_2 = \left[\frac{\mathbf{r}_2\mathbf{g}_2 + \mathbf{d}_2}{\mathbf{z}_2^\kappa} \right]_{q_2},$$

$$\mathbf{u}_3 = \left[\frac{\mathbf{r}_4\mathbf{g}_3 + \mathbf{d}_3}{\mathbf{z}_3^\kappa} \right]_{q_3}.$$

It is not difficult to verify that the norms of $\mathbf{r}_2, \mathbf{r}_3$ are all small. This is because the norm of $\mathbf{r}_1\mathbf{g}_1 + \mathbf{d}_1$ is small and $\mathbf{g}_t, t \in [\![3]\!]$ are satisfied to $\|\mathbf{g}_t^{-1}\| < n^2$.

By $\mathbf{v} = \left[\left\lfloor \frac{q_3}{q_1}\cdot[\mathbf{u}_1\cdot\mathbf{p}_{zt,1}]_{q_1} \right\rfloor - \left\lfloor \frac{q_3}{q_2}\cdot[\mathbf{u}_2\cdot\mathbf{p}_{zt,2}]_{q_2} \right\rfloor - [\mathbf{u}_3\cdot\mathbf{p}_{zt,3}]_{q_3} \right]_{q_3} = [\mathbf{v}_1 - \mathbf{v}_2 - \mathbf{v}_3]_{q_3}$, we compute $\mathbf{v}_t, t \in [\![3]\!]$ as follows:

$$\mathbf{v}_1 = \left\lfloor \frac{q_3}{q_1} \cdot \left[\mathbf{u}_1 \cdot \mathbf{p}_{zt,1} \right]_{q_1} \right\rceil$$

$$= \left\lfloor \frac{q_3}{q_1} \cdot \left(\left[\mathbf{h}_{1,0} (\mathbf{r}_2 \mathbf{g}_2 + \mathbf{d}_2) \frac{\mathbf{z}_0}{\mathbf{z}_1^{\kappa}} \right]_{q_1} + \sum_{t=1}^{3} \left[\mathbf{h}_t (\mathbf{r}_t \mathbf{g}_t + \mathbf{d}_t) \cdot \left[\mathbf{g}_t^{-1} \right]_{q_1} \right]_{q_1} + \mathbf{c}_1 q_1 \right) \right\rceil ,$$

$$= \left[\mathbf{h}_{1,0} (\mathbf{r}_2 \mathbf{g}_2 + \mathbf{d}_2) \left\lfloor \frac{q_3}{q_1} \frac{\mathbf{z}_0}{\mathbf{z}_1^{\kappa}} \right\rceil \right]_{q_3} + \sum_{t=1}^{3} \left(\left[\mathbf{h}_t (\mathbf{r}_t \mathbf{g}_t + \mathbf{d}_t) \cdot \left\lfloor \frac{q_3}{q_1} \left[\mathbf{g}_t^{-1} \right]_{q_1} \right\rceil \right]_{q_3} \right) + \boldsymbol{\delta}_1 + \mathbf{c}_1 q_3$$

where $\|\mathbf{c}_1\| < 4$, $\boldsymbol{\delta}_1 = \boldsymbol{\delta}_{1,0} + \sum_{t=1}^{3} \boldsymbol{\delta}_{1,t}$ such that $\|\boldsymbol{\delta}_{1,0}\| \le l_1 \left(\mathbf{h}_{1,0} (\mathbf{r}_2 \mathbf{g}_2 + \mathbf{d}_2) \right)$ and $\|\boldsymbol{\delta}_{1,t}\| \le l_1 \left(\mathbf{h}_t (\mathbf{r}_t \mathbf{g}_t + \mathbf{d}_t) \right), t \in [\![3]\!]$.

$$\mathbf{v}_2 = \left\lfloor \frac{q_3}{q_2} \cdot \left[\mathbf{u}_2 \cdot \mathbf{p}_{zt,2} \right]_{q_2} \right\rceil$$

$$= \left\lfloor \frac{q_3}{q_2} \cdot \left(\left[\mathbf{h}_{1,0} (\mathbf{r}_2 \mathbf{g}_2 + \mathbf{d}_2) \mathbf{z} \right]_{q_2} + \left[(\mathbf{h}_2 + \mathbf{h}_{2,0} \mathbf{g}_2)(\mathbf{r}_2 \mathbf{g}_2 + \mathbf{d}_2) \mathbf{g}_{2,q_2}^{-1} \right]_{q_2} + \mathbf{c}_2 q_2 \right) \right\rceil ,$$

where $\|\mathbf{c}_2\| < 2$.

By Corollary 3.9 and $\mathbf{z} = \left\lfloor \frac{q_2}{q_1} \left[\frac{\mathbf{z}_0}{\mathbf{z}_1^{\kappa}} \right]_{q_1} \right\rceil$, $\mathbf{g}_{2,q_2}^{-1} = \left\lfloor (q_2 / q_1) \cdot \left[\mathbf{g}_2^{-1} \right]_{q_1}) \right\rceil$, we obtain

$$\mathbf{v}_2 = \left[\mathbf{h}_{1,0} (\mathbf{r}_2 \mathbf{g}_2 + \mathbf{d}_2) \left\lfloor \frac{q_3}{q_1} \left[\frac{\mathbf{z}_0}{\mathbf{z}_1^{\kappa}} \right]_{q_1} \right\rceil \right]_{q_3} + \left[(\mathbf{h}_2 + \mathbf{h}_{2,0} \mathbf{g}_2)(\mathbf{r}_2 \mathbf{g}_2 + \mathbf{d}_2) \left\lfloor \frac{q_3}{q_1} \left[\mathbf{g}_2^{-1} \right]_{q_1} \right\rceil \right]_{q_3} + \boldsymbol{\delta}_2 + \mathbf{c}_2 q_3 ,$$

where $\boldsymbol{\delta}_2 = \boldsymbol{\delta}_{2,0} + \boldsymbol{\delta}_{2,1}$ such that $\|\boldsymbol{\delta}_{2,0}\| \le l_1 \left(\mathbf{h}_{1,0} (\mathbf{r}_2 \mathbf{g}_2 + \mathbf{d}_2) \right) + 2 < n^2 q_3^{5/8}$ and $\|\boldsymbol{\delta}_{2,1}\| \le l_1 \left((\mathbf{h}_2 + \mathbf{h}_{2,0} \mathbf{g}_2)(\mathbf{r}_2 \mathbf{g}_2 + \mathbf{d}_2) \right) + 2 < n^2 q_3^{5/8}$.

$$\mathbf{v}_3 = \left[\mathbf{u}_3 \cdot \mathbf{p}_{zt,3} \right]_{q_3} = \left[(\mathbf{h}_3 + \mathbf{h}_{3,0} \mathbf{g}_3)(\mathbf{r}_4 \mathbf{g}_3 + \mathbf{d}_3) \left\lfloor \frac{q_3}{q_1} \left[\mathbf{g}_t^{-1} \right]_{q_1} \right\rceil \right]_{q_3} .$$

Thus, we have

$$\mathbf{v} = \left[\mathbf{v}_1 - \mathbf{v}_2 - \mathbf{v}_3 \right]_{q_3}$$

$$= \left[\mathbf{h}_1 \mathbf{d}_1 \cdot \left\lfloor \frac{q_3}{q_1} \left[\mathbf{g}_1^{-1} \right]_{q_1} \right\rceil + \mathbf{h}_1 \mathbf{r}_1' \boldsymbol{\alpha}_1 - \mathbf{h}_{2,0} \mathbf{r}_2' \boldsymbol{\alpha}_2 + (\mathbf{h}_3 \mathbf{r}_3' - \mathbf{h}_{3,0} \mathbf{r}_4') \boldsymbol{\alpha}_3 + \boldsymbol{\delta}_1 - \boldsymbol{\delta}_2 \right]_{q_3} ,$$

$$= \left[\mathbf{h}_1 \mathbf{d}_1 \cdot \left\lfloor \frac{q_3}{q_1} \left[\mathbf{g}_1^{-1} \right]_{q_1} \right\rceil + \boldsymbol{\delta} \right]_{q_3}$$

where $\boldsymbol{\alpha}_t = \left[\mathbf{g}_t \cdot \left\lfloor \frac{q_3}{q_1} \left[\mathbf{g}_t^{-1} \right]_{q_1} \right\rceil \right]_{q_3}$, $t \in [\![3]\!]$, $\mathbf{r}_1' = \mathbf{r}_1$, $\mathbf{r}_2' = \mathbf{r}_2 \mathbf{g}_2 + \mathbf{d}_2$, $\mathbf{r}_3' = \mathbf{r}_3 - \mathbf{c}_3$, $\mathbf{r}_4' = \mathbf{r}_4 \mathbf{g}_3 + \mathbf{d}_3$, and $\boldsymbol{\delta} = \mathbf{h}_1 \mathbf{r}_1' \boldsymbol{\alpha}_1 - \mathbf{h}_{2,0} \mathbf{r}_2' \boldsymbol{\alpha}_2 + (\mathbf{h}_3 \mathbf{r}_3' - \mathbf{h}_{3,0} \mathbf{r}_4') \boldsymbol{\alpha}_3 + \boldsymbol{\delta}_1 - \boldsymbol{\delta}_2$.

If $\mathbf{u}_1$ is a level-κ encoding of zero for $\langle \mathbf{g}_1 \rangle$, namely $\mathbf{d}_1 = 0$. Thus, we have

$$\mathbf{v} = \left[\mathbf{v}_1 - \mathbf{v}_2 - \mathbf{v}_3\right]_{q_3} = \left[\boldsymbol{\delta}\right]_{q_3}.$$

For our choice of parameter, we know $\left\|\mathbf{r}_t^{'}\right\| < q_3^{1/8}$, and $\left\|\mathbf{h}_1\right\| < n^2 q_3^{1/2}$, $\left\|\mathbf{h}_3\right\| < n^2 q_3^{1/2}$, $\left\|\mathbf{h}_{2,0}\right\| < n^2 q_3^{1/2}$, $\left\|\mathbf{h}_{3,0}\right\| < n^2 q_3^{1/2}$. By Corollary 3.8, $\left\|\boldsymbol{\alpha}_t\right\| < n^2, t \in [\![3]\!]$.

Thus, $\mathbf{v}$ is not reduced modulo q_3. That is,

$$\begin{aligned}\|\mathbf{v}\| = \|\boldsymbol{\delta}\| &= \left\|\mathbf{h}_1\mathbf{r}_1^{'}\boldsymbol{\alpha}_1 - \mathbf{h}_{2,0}\mathbf{r}_2^{'}\boldsymbol{\alpha}_2 + (\mathbf{h}_3\mathbf{r}_3^{'} - \mathbf{h}_{3,0}\mathbf{r}_4^{'})\boldsymbol{\alpha}_3 + \boldsymbol{\delta}_1 - \boldsymbol{\delta}_2\right\| \\ &\le n^{O(1)} \cdot q_2^{1/2} \cdot q_2^{1/8} \\ &< q^{3/4}\end{aligned}.$$

If $\mathbf{u}_1$ is a level-κ encoding of non-zero element for $\langle \mathbf{g}_1 \rangle$, namely $\mathbf{d}_1 \ne 0 \bmod \mathbf{g}_1$. By Lemma 4 in [GGH13], $\left[\mathbf{h}_1\mathbf{d}_1 \cdot \left\lfloor \frac{q_3}{q_1}\left[\mathbf{g}_1^{-1}\right]_{q_1} \right\rceil\right]_{q_3} \ge q_3^{1-\varepsilon}$ with high probability, where ε is an arbitrary small positive constant.

Thus, we obtain

$$\begin{aligned}\|\mathbf{v}\| &= \left\|\left[\mathbf{h}_1\mathbf{d}_1 \cdot \left\lfloor \frac{q_3}{q_1}\left[\mathbf{g}_1^{-1}\right]_{q_1} \right\rceil + \boldsymbol{\delta}\right]_{q_3}\right\| \\ &\ge \left\|\left[\mathbf{h}_1\mathbf{d}_1 \cdot \left\lfloor \frac{q_3}{q_1}\left[\mathbf{g}_1^{-1}\right]_{q_1} \right\rceil\right]_{q_3}\right\| - \|\boldsymbol{\delta}\|, \\ &\ge q_3^{1-\varepsilon} - q_3^{3/4} \\ &> q_3^{1-\varepsilon'}\end{aligned}$$

where ε' is a small positive constant. □

Lemma 3.11 Given two level-κ encodings $\left(\mathbf{u}_{1,1}, \mathbf{u}_{2,1}, \mathbf{u}_{3,1}\right)$, $\left(\mathbf{u}_{1,2}, \mathbf{u}_{2,2}, \mathbf{u}_{3,2}\right)$, suppose that $\mathbf{u}_{1,1}, \mathbf{u}_{1,2}$ encode same plaintext for $\langle \mathbf{g}_1 \rangle$, then

$$\mathrm{Ext}\left(\mathrm{par}, \left(\mathbf{u}_{1,1}, \mathbf{u}_{2,1}, \mathbf{u}_{3,1}\right)\right) = \mathrm{Ext}\left(\mathrm{par}, \left(\mathbf{u}_{1,2}, \mathbf{u}_{2,2}, \mathbf{u}_{3,2}\right)\right).$$

Proof. Let $\mathbf{u}_{1,s} = \left[\frac{\mathbf{r}_{1,s}\mathbf{g}_1 + \mathbf{d}}{\mathbf{z}_1^{\kappa}}\right]_{q_1}$, $s \in [\![2]\!]$. By Lemma 3.10, we have

$$\mathbf{v}^{(s)} = \left[\mathbf{h}_1\mathbf{d} \cdot \left\lfloor \frac{q_3}{q_1}\left[\mathbf{g}_1^{-1}\right]_{q_1} \right\rceil + \boldsymbol{\delta}^{(s)}\right]_{q_3},$$

where $\left\|\boldsymbol{\delta}^{(s)}\right\| \le q_3^{3/4}$ and $\left[\mathbf{h}_1\mathbf{d} \cdot \left\lfloor \frac{q_3}{q_1}\left[\mathbf{g}_1^{-1}\right]_{q_1} \right\rceil\right]_{q_3} \approx q_3$ with high probability.

Thus $\mathbf{v}^{(1)} \approx \mathbf{v}^{(2)}$ when $\mathbf{d} \ne 0 \bmod \mathbf{g}_1$. □

3.3 Hardness assumption

Consider the following security experiment:

(1) $\mathrm{par} \leftarrow \mathrm{InstGen}(1^{\lambda}, 1^{\kappa})$

(2) For $l = 0$ to κ:

Sample $\mathbf{d}_l \leftarrow D_{\mathbb{Z}^n,\sigma'}$, $\mathbf{r}_{l,i} \leftarrow D_{\mathbb{Z}^n,\sigma^*}$;

Generate level-1 encoding $\mathbf{u}_{t,l} = \left[\mathbf{d}_l \mathbf{y}_t + \sum_{i=1}^{\tau} \mathbf{r}_{l,i} \mathbf{x}_{t,i}\right]_{q_t}, t \in [\![3]\!]$.

(3) Set $\mathbf{u}_t = \left[\prod_{l=1}^{\kappa} \mathbf{u}_{t,l}\right]_{q_t}, t \in [\![3]\!]$.

(4) Set $\mathbf{v}_C = \mathbf{v}_D = \mathrm{Ext}\left(\mathrm{par}, \left(\left[\mathbf{d}_0 \mathbf{u}_{1,1}\right]_{q_1}, \left[\mathbf{d}_0 \mathbf{u}_{2,1}\right]_{q_2}, \left[\mathbf{d}_0 \mathbf{u}_{3,1}\right]_{q_3}\right)\right)$.

(5) Sample $\mathbf{r}_0 \leftarrow D_{\mathbb{Z}^n,\sigma'}$ and set $\mathbf{v}_R = \mathrm{Ext}\left(\mathrm{par}, \left(\left[\mathbf{r}_0 \mathbf{u}_{1,1}\right]_{q_1}, \left[\mathbf{r}_0 \mathbf{u}_{2,1}\right]_{q_2}, \left[\mathbf{r}_0 \mathbf{u}_{3,1}\right]_{q_3}\right)\right)$.

Definition 3.12 (ext-GCDH/ext-GDDH). According to the security experiment, the ext-GCDH and ext-GDDH are defined as follows:

Level-κ extraction CDH (ext-GCDH): Given $\left\{\mathrm{par}, \left(\mathbf{u}_{1,1}, \mathbf{u}_{2,1}, \mathbf{u}_{3,1}\right), \cdots, \left(\mathbf{u}_{1,\kappa}, \mathbf{u}_{2,\kappa}, \mathbf{u}_{3,\kappa}\right)\right\}$, output a level-$\kappa$ extraction encoding $\mathbf{w} \in R_{q_2}$ such that $\left\|\left[\mathbf{v}_C - \mathbf{w}\right]_{q_2}\right\|_\infty \le q_2^{3/4}$.

Level-κ extraction DDH (ext-GDDH): Given $\left\{\mathrm{par}, \left(\mathbf{u}_{1,1}, \mathbf{u}_{2,1}, \mathbf{u}_{3,1}\right), \cdots, \left(\mathbf{u}_{1,\kappa}, \mathbf{u}_{2,\kappa}, \mathbf{u}_{3,\kappa}\right), \mathbf{v}\right\}$, distinguish between $D_{ext-GDDH} = \left\{\mathrm{par}, \left(\mathbf{u}_{1,1}, \mathbf{u}_{2,1}, \mathbf{u}_{3,1}\right), \cdots, \left(\mathbf{u}_{1,\kappa}, \mathbf{u}_{2,\kappa}, \mathbf{u}_{3,\kappa}\right), \mathbf{v}_D\right\}$ and $D_{ext-RAND} = \left\{\mathrm{par}, \left(\mathbf{u}_{1,1}, \mathbf{u}_{2,1}, \mathbf{u}_{3,1}\right), \cdots, \left(\mathbf{u}_{1,\kappa}, \mathbf{u}_{2,\kappa}, \mathbf{u}_{3,\kappa}\right), \mathbf{v}_R\right\}$.

3.4 Optimization

Our above construction with three-encodings can become double-encodings. As far as I know, one cannot obtain useful information from the same numerators of encodings in different modulo. Namely, one can generate the public parameters $\mathrm{par} = \left\{\left\{q_t, \mathbf{y}_t, \left\{\mathbf{x}_{t,i}\right\}_{i \in [\![\tau]\!]}, \mathbf{p}_{zt,t}\right\}_{t \in [\![2]\!]}\right\}$, where $\mathbf{y}_1 = \left[\frac{\mathbf{a}_1 \mathbf{g}_1 + 1}{\mathbf{z}_1}\right]_{q_1}$, $\mathbf{x}_{1,i} = \left[\frac{\mathbf{a}_{1,i} \mathbf{g}_1}{\mathbf{z}_1}\right]_{q_1}$, $\mathbf{y}_2 = \left[\frac{\mathbf{a}_1 \mathbf{g}_1 + 1}{\mathbf{z}_2}\right]_{q_2}$, $\mathbf{x}_{2,i} = \left[\frac{\mathbf{a}_{1,i} \mathbf{g}_1}{\mathbf{z}_2}\right]_{q_2}$, and $\mathbf{p}_{zt,1} = \left[\mathbf{h}_{1,0} \mathbf{z}_0 + \mathbf{z}_1^{\kappa}\left(\mathbf{h}_1 \cdot \left[\mathbf{g}_1^{-1}\right]_{q_1} + \mathbf{h}_2 \cdot \left[\mathbf{g}_2^{-1}\right]_{q_1}\right)\right]_{q_1}$, $\mathbf{p}_{zt,2} = \left[\mathbf{z}_2^{\kappa}\left(\mathbf{h}_{1,0} \mathbf{z} + (\mathbf{h}_2 + \mathbf{h}_{2,0} \mathbf{g}_2) \mathbf{g}_{2,q_2}^{-1}\right)\right]_{q_2}$.

4 Security analysis

In essence, the weak-DL attack [GGH13] is to compute a basis of secret element $\mathbf{g}_1$. So, we give easily computable some quantities in our construction, and analyze possible attacks using these quantities.

4.1 Easily computable quantities

The encodings $\mathbf{y}_1, \mathbf{x}_{1,i}$ in the public parameters are same as that of GGH13 for the ideal lattice $\langle \mathbf{g}_1 \rangle$. However, the zero testing parameter $\mathbf{p}_{zt,1}$, which is different from that of GGH13, is changed into $\mathbf{p}_{zt,1} = \left[\mathbf{h}_{1,0} \mathbf{z}_0 + \mathbf{z}_1^{\kappa}\left(\mathbf{h}_1 \cdot \left[\mathbf{g}_1^{-1}\right]_{q_1} + \mathbf{h}_2 \cdot \left[\mathbf{g}_2^{-1}\right]_{q_1} + \mathbf{h}_3 \cdot \left[\mathbf{g}_3^{-1}\right]_{q_1}\right)\right]_{q_1}$. As a result, the encodings $\mathbf{x}_{1,i}$ of zero for $\langle \mathbf{g}_1 \rangle$ are not any more encoding of zero for $\langle \mathbf{g}_2 \rangle, \langle \mathbf{g}_3 \rangle$. Moreover, we increase new random element $\mathbf{z}_0 \in R_{q_1}$. On the one hand, although the non-zero plaintexts encoded by $\mathbf{y}_1, \mathbf{x}_{1,i}$ are one-to-one corresponding to ones encoded by $\mathbf{y}_3, \mathbf{x}_{3,i}$ for $\langle \mathbf{g}_3 \rangle$, they cannot be subtracted to obtain encoding of zero for $\langle \mathbf{g}_3 \rangle$. This is because: (1) $\mathbf{z}_1$ using as level number of encoding is not equal to $\mathbf{z}_3$; (2) the modulo q_1 in the first type encodings is different from q_3 in the third type encodings. Thus, to remove the non-zero level-0 encodings in $\mathbf{y}_1, \mathbf{x}_{1,i}$ for $\langle \mathbf{g}_3 \rangle$, one must switch from q_1 to q_3 and use zero testing parameter $\mathbf{p}_{zt,3}$. On the other hand, the numerators in $\mathbf{y}_1, \mathbf{x}_{1,i}$ are same as ones in $\mathbf{y}_2, \mathbf{x}_{2,i}$, one can not get useful information from them. Because they have different modulo and random elements using encoding level. Thus, one can only get easily computable quantities in the following form.

Given a level-k encoding $(\mathbf{u}_1', \mathbf{u}_2', \mathbf{u}_3')$ with $1 \le k < \kappa$, we can compute using par to get

$$\mathbf{v} = \left[\left\lfloor \frac{q_3}{q_1} \cdot \left[\mathbf{u}_1 \cdot \mathbf{p}_{zt,1} \right]_{q_1} \right\rceil - \left\lfloor \frac{q_3}{q_2} \cdot \left[\mathbf{u}_2 \cdot \mathbf{p}_{zt,2} \right]_{q_2} \right\rceil - \left[\mathbf{u}_3 \cdot \mathbf{p}_{zt,3} \right]_{q_3} \right]_{q_3},$$

where $\mathbf{u}_t = \mathbf{u}_t' \cdot (\mathbf{x}_{t,i})^j \cdot (\mathbf{y}_t)^{\kappa-k-j}, t \in [\![3]\!]$.

It is easy to see that $\mathbf{v}$ is not reduced modulo q_3. However, switching modulus destroys the structure of the ring element in $\left[\mathbf{u}_1 \cdot (\mathbf{x}_{1,i})^j \cdot (\mathbf{y}_1)^{\kappa-k-j} \cdot \mathbf{p}_{zt,1} \right]_{q_1}$. As a result, the attacks using basis of secret element [HJ15, CL15] are not applicable for our construction.

The SubM problem. The subgroup membership problem is seemly hard for our construction. Let $\mathbf{g}_1 = \mathbf{g}_{1,1}\mathbf{g}_{1,2}$. Given a level-$1$ encoding $(\mathbf{u}_1, \mathbf{u}_2)$ with $\mathbf{u}_1 = \left[\frac{\mathbf{w}}{\mathbf{z}_1} \right]_{q_1}$, determine if $\mathbf{w} \in \langle \mathbf{g}_{1,1} \rangle$. Using $\mathbf{v}$, one cannot decide whether $\mathbf{v}$ belongs to $\langle \mathbf{g}_{1,1} \rangle$ regardless of $\mathbf{w} \in \langle \mathbf{g}_{1,1} \rangle$. This is again the result destroying structure of ring element.

The DLIN problem. The decision linear problem is also seemly hard for our construction. For a matrix of $\mathbf{A} = (\mathbf{a}_{i,j}) \in R^{w \times w}$, all encoded at level-$k$, $1 \le k < \kappa$ form a matrix $\mathbf{T}$, the DLIN problem is to distinguish between rank w and rank $w-1$ for $\mathbf{A}$. Based on the similar reason above, one cannot compute the rank of $\mathbf{A}$ in our encoding scheme.

4.2 Hu-Jia Attack

In this section, we show that the Hu-Jia attack [HJ15a] does not work for our construction.

4.2.1 Hu-Jia Attack Description

Their attack includes three steps. The first step generates an equivalent level-0 encoding for a level-1 encoding; the second step computes an equivalent level-0 encoding for the product of several level-0 encodings; the final step transforms an equivalent product level-0 encoding into the shared secret key of MPKE by the modified encoding/decoding.

By analysis, the first step is the key of the Hu-Jia attack. We describe the concrete details of the first step as follows:

(1) Let $\text{par}_0 = \left\{ q, \mathbf{y} = \left[(1+\mathbf{ag})/\mathbf{z} \right]_q, \mathbf{x}_i = \left[(\mathbf{a}_i\mathbf{g})/\mathbf{z} \right]_q, i \in [\![2]\!], \mathbf{p}_{zt} = \left[(\mathbf{hz}^{\kappa})/\mathbf{g} \right]_q \right\}$ be the public parameters of the GGH map. We generate special decodings $\left\{ \mathbf{y}^{(1)}, \mathbf{x}^{(i)}, i = 1, 2 \right\}$, where

$$\mathbf{y}^{(1)} = \left[\mathbf{p}_{zt} \mathbf{y}^{\kappa-1} \mathbf{x}_1 \right]_q = \mathbf{h}(1+\mathbf{ag})^{\kappa-1}\mathbf{a}_1,$$

$$\mathbf{x}^{(i)} = \left[\mathbf{p}_{zt}\mathbf{y}^{\kappa-2}\mathbf{x}_i\mathbf{x}_1\right]_q = \mathbf{h}(1+\mathbf{ag})^{\kappa-2}(\mathbf{a}_i\mathbf{g})\mathbf{a}_1,\ i=1,2.$$

Notice that $\mathbf{y}^{(1)}, \mathbf{x}^{(i)}$ are not reduced modulo q.

(2) Given a level-1 encoding $\mathbf{u}$, we have $\mathbf{u} = \left[\mathbf{dy} + \mathbf{r}_1\mathbf{x}_1 + \mathbf{r}_2\mathbf{x}_2\right]_q$, where $\mathbf{d}$ is secret level-0 encoding, and $\mathbf{r}_1, \mathbf{r}_2$ random noise elements.

Compute special decoding

$$\mathbf{v} = \left[\mathbf{p}_{zt}\mathbf{u}\mathbf{y}^{\kappa-2}\mathbf{x}_1\right]_q = \mathbf{dy}^{(1)} + \mathbf{r}_1\mathbf{x}^{(1)} + \mathbf{r}_2\mathbf{x}^{(2)}.$$

Since $\mathbf{v}$ is not reduced modulo q, then compute

$$\mathbf{v} \bmod \mathbf{y}^{(1)} = (\mathbf{r}_1\mathbf{x}^{(1)} \bmod \mathbf{y}^{(1)} + \mathbf{r}_2\mathbf{x}^{(2)} \bmod \mathbf{y}^{(1)}) \bmod \mathbf{y}^{(1)}.$$

(3) Given $\mathbf{v} \bmod \mathbf{y}^{(1)}$ and $\left\{\mathbf{x}^{(1)} \bmod \mathbf{y}^{(1)}, \mathbf{x}^{(2)} \bmod \mathbf{y}^{(1)}\right\}$, we get $\mathbf{v}' = \mathbf{v} \bmod \mathbf{y}^{(1)} \in \left\langle \mathbf{x}^{(1)}, \mathbf{x}^{(2)} \right\rangle$ such that $(\mathbf{v} - \mathbf{v}') \bmod \mathbf{y}^{(1)} = 0$. Let $\mathbf{v}' = \mathbf{r}_1'\mathbf{x}^{(1)} + \mathbf{r}_2'\mathbf{x}^{(2)}$.

(4) Compute $\mathbf{d}^{(0)} = (\mathbf{v} - \mathbf{v}')/\mathbf{y}^{(1)}$ over $\mathbb{k} = \mathbb{R}[x]/\left\langle x^n + 1\right\rangle$ such that the quotient $\mathbf{d}^{(0)} \in R$. By arranging, we obtain

$$\begin{aligned}\mathbf{d}^{(0)} &= (\mathbf{v} - \mathbf{v}')/\mathbf{y}^{(1)} \\ &= \mathbf{d} + ((\mathbf{r}_1 - \mathbf{r}_1')\mathbf{a}_1 + (\mathbf{r}_2 - \mathbf{r}_2')\mathbf{a}_2)\mathbf{g}/(1+\mathbf{ag})\end{aligned}.$$

Again since $\mathbf{g}$ and $1+\mathbf{ag}$ are co-prime, we get $\mathbf{d} - \mathbf{d}^{(0)} \in \left\langle \mathbf{g} \right\rangle$. Thus, $\mathbf{d}^{(0)}$ is an equivalent level-0 encoding of $\mathbf{d}$. Although $\left\|\mathbf{d}^{(0)}\right\|$ is not small, Hu and Jia [HJ15a] controlled the size of $\mathbf{d}^{(0)}$ by using $\mathbf{x}^{(i)} \in \left\langle \mathbf{g} \right\rangle$.

4.2.2 Non-applicabiltiy of Hu-Jia Attack

(1) Let $\mathrm{par} = \left\{ \left\{ q_t, \mathbf{y}_t, \left\{\mathbf{x}_{t,i}\right\}_{i\in[\![\tau]\!]}, \mathbf{p}_{zt,t} \right\}_{t\in[\![3]\!]} \right\}$ be the public parameters of our construction. Similarly, we generate special decodings $S = \left\{ \mathbf{y}^{(1)}, \left\{\mathbf{x}^{(i)}\right\}_{i\in[\![\tau]\!]} \right\}$ as follows:

$$\mathbf{y}^{(1)} = \left[\left\lfloor \frac{q_3}{q_1} \cdot \left[\mathbf{u}_1 \cdot \mathbf{p}_{zt,1}\right]_{q_1} \right\rceil - \left\lfloor \frac{q_3}{q_2} \cdot \left[\mathbf{u}_2 \cdot \mathbf{p}_{zt,2}\right]_{q_2} \right\rceil - \left[\mathbf{u}_3 \cdot \mathbf{p}_{zt,3}\right]_{q_3} \right]_{q_3},$$

where $\mathbf{u}_t = \mathbf{x}_{t,1} \cdot (\mathbf{y}_t)^{\kappa-1},\ t \in [\![3]\!]$.

$$\mathbf{x}^{(i)} = \left[\left\lfloor \frac{q_3}{q_1} \cdot \left[\mathbf{u}_1 \cdot \mathbf{p}_{zt,1}\right]_{q_1} \right\rceil - \left\lfloor \frac{q_3}{q_2} \cdot \left[\mathbf{u}_2 \cdot \mathbf{p}_{zt,2}\right]_{q_2} \right\rceil - \left[\mathbf{u}_3 \cdot \mathbf{p}_{zt,3}\right]_{q_3} \right]_{q_3},$$

where $\mathbf{u}_t = \mathbf{x}_{t,i}\mathbf{x}_{t,1} \cdot (\mathbf{y}_t)^{\kappa-2},\ t \in [\![3]\!]$.

Notice that $\mathbf{y}^{(1)}, \mathbf{x}^{(i)}$ are not reduced modulo q_3.

(2) Given a level-1 encoding $(\mathbf{u}_1', \mathbf{u}_2', \mathbf{u}_3')$ with $\mathbf{u}_t' = \left[\mathbf{d} \cdot \mathbf{y}_t + \sum_{i=1}^{\tau} \mathbf{r}_i \cdot \mathbf{x}_{t,i}\right]_q, t \in [\![3]\!]$, we compute special decoding

$$\mathbf{v} = \left[\left\lfloor \frac{q_3}{q_1} \cdot \left[\mathbf{u}_1 \cdot \mathbf{p}_{zt,1}\right]_{q_1} \right\rceil - \left\lfloor \frac{q_3}{q_2} \cdot \left[\mathbf{u}_2 \cdot \mathbf{p}_{zt,2}\right]_{q_2} \right\rceil - \left[\mathbf{u}_3 \cdot \mathbf{p}_{zt,3}\right]_{q_3} \right]_{q_3} \neq \mathbf{d} \cdot \mathbf{y}^{(1)} + \sum_{i=1}^{\tau} \mathbf{r}_i \cdot \mathbf{x}^{(i)},$$

where $\mathbf{u}_t = \mathbf{u}_t'\mathbf{x}_{t,1} \cdot (\mathbf{y}_t)^{\kappa-2},\ t \in [\![3]\!]$.

Although $\mathbf{v}$ is not reduced modulo q_3, one cannot find an equivalent level-0 encoding encoded by $\left(\mathbf{u}_1^{'}, \mathbf{u}_2^{'}, \mathbf{u}_3^{'}\right)$ using the Hu-Jia method. Because $\mathbf{x}^{(i)} \notin \langle \mathbf{g}_1 \rangle$ and the probability that $\mathbf{y}^{(1)}, \mathbf{x}^{(i)}$ are co-prime is almost 1. Namely, $\mathbf{y}^{(1)}, \mathbf{x}^{(i)}$ have not common factor. This is different from the case of the original GGH described by Hu and Jia [HJ15a]. Moreover, one cannot efficiently solve $\mathbf{d}, \mathbf{r}_i$ given $\mathbf{y}^{(1)}, \mathbf{x}^{(i)}, \mathbf{v}$. This is because $\mathbf{v} \neq \mathbf{d} \cdot \mathbf{y}^{(1)} + \sum_{i=1}^{\tau} \mathbf{r}_i \cdot \mathbf{x}^{(i)}$.

In fact, we observe that one cannot also find $\mathbf{d}, \mathbf{r}_i$ even if $\mathbf{y}^{(1)}, \mathbf{x}^{(i)}, \mathbf{v}$ are not rounded when computing them. Because using $\mathbf{g}_2, \mathbf{g}_3$ increase new random noise and remove a factor of $\mathbf{g}_1$.

Thus, one cannot find an equivalent level-0 encoding encoded by $\left(\mathbf{u}_1^{'}, \mathbf{u}_2^{'}, \mathbf{u}_3^{'}\right)$. Namely, the Hu-Jia attack is prevented in our construction.

4.3 Cheon-Lee Attack

The Cheon-Lee attack [CL15] for the GGH13 map consists of three steps. The first step is find a basis of secret ideal lattice $\langle \mathbf{g}_1 \rangle$. The second step is to find the shortest vector of $\langle \mathbf{g}_1 \rangle$ using HNF. The third step is to apply a lattice reduction algorithm on reduced dimension to solve the GDDH on the GGH13 map.

However, one cannot yield a basis of $\langle \mathbf{g}_1 \rangle$ using the public parameters in our construction. Thus, The Cheon-Lee attack does not work in our construction.

4.4 Coron et al. attack

For the attack of CLT [CHL+14], Coron et al. extended this attack method to encodings more than a single monomial to get a zero [CGH+15]. The key of the extension attack in [CGH+15] is that one can write in the matrix form over the rational for non-reduced quantities.

To demonstrate effect of $\mathbf{z}_0, \mathbf{z}$ in $\mathbf{p}_{zt,1}, \mathbf{p}_{zt,2}$, we generate a basis of $\mathbf{g}_1$ using the attack in [CGH+15] when $\mathbf{z}_0 = \mathbf{z} = 0$.

By Corollary 3.8, we have $\boldsymbol{\alpha}_t = \left[\mathbf{g}_t \cdot \mathbf{g}_{t,q_t}^{-1}\right]_{q_t}$ and $\|\boldsymbol{\alpha}_t\| < l_1(\mathbf{g}_t) + \lfloor q_t / q_1 \rfloor = l_1(\mathbf{g}_t)$ for $t \in \{2,3\}$. So, $\boldsymbol{\alpha}_t$ is not reduced modulo q_t.

Given an arbitrary level-k encoding $\left(\mathbf{u}_1^{'}, \mathbf{u}_2^{'}, \mathbf{u}_3^{'}\right)$, one computes using zeroizing attack

$$\mathbf{v}_{k,i,j} = \left[\frac{q_3}{q_1} \cdot \left[\mathbf{u}_1 \cdot \mathbf{p}_{zt,1}\right]_{q_1} - \frac{q_3}{q_2} \cdot \left[\mathbf{u}_2 \cdot \mathbf{p}_{zt,2}\right]_{q_2} - \left[\mathbf{u}_3 \cdot \mathbf{p}_{zt,3}\right]_{q_3}\right]_{q_3},$$

where $\mathbf{u}_t = \mathbf{u}_t^{'} \cdot \mathbf{x}_{t,i}^{j} \cdot \mathbf{y}_t^{\kappa-k-j}, t \in [\![3]\!]$ with $j \geq 1$.

Note that $\frac{q_3}{q_1} \cdot \left[\mathbf{u}_1 \cdot \mathbf{p}_{zt,1}\right]_{q_1}$ and $\frac{q_3}{q_2} \cdot \left[\mathbf{u}_2 \cdot \mathbf{p}_{zt,2}\right]_{q_2}$ in $\mathbf{v}_{k,i,j}$ are not rounded to integers.

It is easy to see that $\mathbf{v}_{k,i,j}$ is not reduced modulo q_3. Assume that $\mathbf{u}_t^{'} = \left[\mathbf{c}_t / \mathbf{z}_t^{k}\right]_{q_t}$, $\mathbf{x}_{t,i}^{j} = \left[\mathbf{b}_{t,i}^{j} / \mathbf{z}_t^{j}\right]_{q_t}$, $\mathbf{y}_t^{\kappa-k-j} = \left[\mathbf{d}_t^{\kappa-k-j} / \mathbf{z}_t^{\kappa-k-j}\right]_{q_t}$. Now, we can write $\mathbf{v}_{k,i,j}$ in matrix form:

$$\mathbf{v}_{k,i,j}=\left[\frac{q_3}{q_1}\cdot\left[\mathbf{u}_1\cdot\mathbf{p}_{zt,1}\right]_{q_1}-\frac{q_3}{q_2}\cdot\left[\mathbf{u}_2\cdot\mathbf{p}_{zt,2}\right]_{q_2}-\left[\mathbf{u}_3\cdot\mathbf{p}_{zt,3}\right]_{q_3}\right]_{q_3}$$

$$=\begin{pmatrix}\mathbf{c}_1 & \mathbf{c}_2 & \mathbf{c}_3\end{pmatrix}\begin{pmatrix}\frac{q_3}{q_1}\cdot\mathbf{b}_{1,i}^{j}\cdot\boldsymbol{\rho}_1 & & \\ & -\frac{q_3}{q_2}\cdot\mathbf{b}_{2,i}^{j}\cdot\boldsymbol{\rho}_2 & \\ & & -\mathbf{b}_{3,i}^{j}\cdot\boldsymbol{\rho}_3\end{pmatrix}\begin{pmatrix}\mathbf{d}_1^{\kappa-k-j}\\ \mathbf{d}_2^{\kappa-k-j}\\ \mathbf{d}_3^{\kappa-k-j}\end{pmatrix},$$

where $\boldsymbol{\rho}_1=\left(\frac{\mathbf{h}_1}{\mathbf{g}_1}+\frac{\mathbf{h}_2}{\mathbf{g}_2}+\frac{\mathbf{h}_3}{\mathbf{g}_3}\right)$, $\boldsymbol{\rho}_2=\frac{\mathbf{h}_2+\mathbf{h}_{2,0}\mathbf{g}_2}{\mathbf{g}_2}\boldsymbol{\alpha}_2$, $\boldsymbol{\rho}_3=\frac{\mathbf{h}_3+\mathbf{h}_{3,0}\mathbf{g}_3}{\mathbf{g}_3}\boldsymbol{\alpha}_3$.

Since $\mathbf{c}_1=\mathbf{c}_2$, $\mathbf{b}_{1,i}=\mathbf{b}_{2,i}$ and $\mathbf{d}_1=\mathbf{d}_2$, we transform $\mathbf{v}_{k,i,j}$ into the following form:

$$\mathbf{v}_{k,i,j}=\begin{pmatrix}\mathbf{c}_1 & \mathbf{c}_3\end{pmatrix}\begin{pmatrix}\mathbf{b}_{1,i}^{j}\cdot(\frac{q_3}{q_1}\cdot\boldsymbol{\rho}_1-\frac{q_3}{q_2}\cdot\boldsymbol{\rho}_2) & \\ & -\mathbf{b}_{3,i}^{j}\cdot\boldsymbol{\rho}_3\end{pmatrix}\begin{pmatrix}\mathbf{d}_1^{\kappa-k-j}\\ \mathbf{d}_3^{\kappa-k-j}\end{pmatrix}$$

By the matrix form of $\mathbf{v}_{k,i,j}$ over the rational, one can compute a basis of $\mathbf{g}_1$ by directly using the attack in [CGH+15].

However, the random ring elements $\mathbf{z}_0\in R_{q_1}$, $\mathbf{z}\in R_{q_2}$ in $\mathbf{p}_{zt,1},\mathbf{p}_{zt,2}$ cannot represent as ring elements over the rational. This is also the reason that they are used in the zero-testing parameters. Thus, our construction can thwart the extension attack in [CGH+15].

4.5 Attack for numerator of encodings

For the public parameters par, the numerators in the encodings $\mathbf{y}_1,\mathbf{x}_{1,i}$ are same as that in $\mathbf{y}_2,\mathbf{x}_{2,i}$. Since they use different modulo, one cannot directly compute between these encodings. Given two encodings $\left(\mathbf{u}_{1,s},\mathbf{u}_{2,s},\mathbf{u}_{3,s}\right), s\in[\![2]\!]$ for our construction, we can obtain the following quantities:

$$\mathbf{c}_1=\left[\frac{\mathbf{u}_{1,1}}{\mathbf{u}_{1,2}}\right]_{q_1}=\left[\frac{\mathbf{r}_1\mathbf{g}_1+\mathbf{d}_1}{\mathbf{r}_2\mathbf{g}_1+\mathbf{d}_2}\right]_{q_1},\quad \mathbf{c}_2=\left[\frac{\mathbf{u}_{2,1}}{\mathbf{u}_{2,2}}\right]_{q_2}=\left[\frac{\mathbf{r}_1\mathbf{g}_1+\mathbf{d}_1}{\mathbf{r}_2\mathbf{g}_1+\mathbf{d}_2}\right]_{q_2},$$

where $\mathbf{u}_{t,s}=\left[\frac{\mathbf{r}_s\mathbf{g}_t+\mathbf{d}_s}{\mathbf{z}_t}\right]_{q_t}, t\in[\![2]\!], s\in[\![2]\!]$.

However, one cannot find $\mathbf{r}_s\mathbf{g}_1+\mathbf{d}_s$ by using $\mathbf{c}_1,\mathbf{c}_2$. Since by Lemma 3.6, we have

$$\left\lfloor\frac{q_2}{q_1}\mathbf{c}_1\right\rceil=\left[(\mathbf{r}_1\mathbf{g}_1+\mathbf{d}_1)\cdot\left\lfloor\frac{q_2}{q_1}\left[\frac{1}{\mathbf{r}_2\mathbf{g}_1+\mathbf{d}_2}\right]_{q_1}\right\rceil\right]_{q_2}+\boldsymbol{\delta},$$

where $\|\boldsymbol{\delta}\|<l_1(\mathbf{w})$ and $\boldsymbol{\delta}\neq 0$.

Again, by $\left\lfloor\frac{q_2}{q_1}\left[\frac{1}{\mathbf{r}_2\mathbf{g}_1+\mathbf{d}_2}\right]_{q_1}\right\rceil\neq\left[\frac{1}{\mathbf{r}_2\mathbf{g}_1+\mathbf{d}_2}\right]_{q_2}$, one cannot obtain useful information from

$\left\lfloor \frac{q_2}{q_1}\mathbf{c}_1 \right\rceil$ and $\mathbf{c}_2$.

Thus, our construction cannot be attacked by using same numerators of encodings in the public parameters.

5 Applications

In the following, we describe two applications using our construction: the MPKE protocol and the instance of witness encryption.

5.1 MPKE Protocol

Setup$(1^\lambda, 1^N)$. Output $(\text{par}) \leftarrow \text{InstGen}(1^\lambda, 1^\kappa)$ as the public parameters.

Publish(par, j). The j-th party samples $\mathbf{d}_j \leftarrow D_{\mathbb{Z}^n,\sigma'}$, $\mathbf{r}_{j,i} \leftarrow D_{\mathbb{Z}^n,\sigma^*}, i \in [\![\tau]\!]$, publishes the public key $\mathbf{u}_{t,j} = \left[\mathbf{d}_j \cdot \mathbf{y}_t + \sum_{i=1}^{\tau} \mathbf{r}_{j,i} \cdot \mathbf{x}_{t,i}\right]_{q_t}, t \in [\![3]\!]$ and remains $\mathbf{d}_j$ as the secret key.

KeyGen$\left(\text{par}, j, \mathbf{d}_j, \left\{\left(\mathbf{u}_{1,k}, \mathbf{u}_{2,k}, \mathbf{u}_{3,k}\right)\right\}_{k \neq j}\right)$. The j-th party computes $\mathbf{c}_{t,j} = \left[\prod_{k \neq j} \mathbf{u}_{t,k}\right]_{q_t}$, $t \in [\![3]\!]$ and extracts the common secret key $sk = \text{Ext}\left(\text{par}, \left(\left[\mathbf{d}_j \mathbf{c}_{1,j}\right]_{q_1}, \left[\mathbf{d}_j \mathbf{c}_{2,j}\right]_{q_2}, \left[\mathbf{d}_j \mathbf{c}_{3,j}\right]_{q_3}\right)\right)$.

Theorem 5.1 Suppose the ext-GCDH/ext-GDDH defined in Section 3.3 is hard, then our construction is one round multipartite Diffie-Hellman key exchange protocol.

5.2 Witness Encryption

5.2.1 Construction

Garg, Gentry, Sahai, and Waters [GGSW13] constructed an instance of witness encryption based on the NP-complete 3-exact cover problem and the GGH13 map. However, Hu and Jia [HJ15a] have broken the GGH13-based WE. In this section, we present a new construction of WE based on our new multilinear map.

3-Exact Cover Problem [GGH13, Gol08] Given a collection Set of subsets $T_1, T_2, ..., T_\pi$ of $[\![K]\!] = \{1, 2, ..., K\}$ such that $K = 3\theta$ and $|T_i| = 3$, find a 3-exact cover of $[\![K]\!]$. For an instance of witness encryption, the public key is a collection Set and the public parameters par in our construction, the secret key is a hidden 3-exact cover of $[\![K]\!]$.

Encrypt$(1^\lambda, \text{par}, M)$**:**

(1) For $k \in [\![K]\!]$, sample $\mathbf{d}_k \leftarrow D_{Z^n,\sigma'}$, $\mathbf{r}_{k,i} \leftarrow D_{\mathbb{Z}^n,\sigma^*}$, $i \in [\![\tau]\!]$ and generate level-1 encodings $\mathbf{u}_{t,k} = \left[\mathbf{d}_k \cdot \mathbf{y}_t + \sum_{i=1}^{\tau} \mathbf{r}_{k,i} \cdot \mathbf{x}_{t,i}\right]_{q_t}, t \in [\![3]\!]$.

(2) Compute $\mathbf{u}_t = \left[\prod_{k=1}^{K} \mathbf{u}_{t,k}\right]_{q_t}, t \in [\![3]\!]$ and $sk = \text{Ext}\left(\text{par}, \left(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3\right)\right)$, and encrypt a message M into ciphertext C.

(3) For each element $T_j = \{j_1, j_2, j_3\} \in Set$, sample $\mathbf{r}_{T_j,i} \leftarrow D_{\mathbb{Z}^n,\sigma^*}, i \in [\![\tau]\!]$, and generate a

level-3 encoding $\mathbf{u}_{t,T_j} = \left[\mathbf{u}_{t,j_1}\mathbf{u}_{t,j_2}\mathbf{u}_{t,j_3} + \sum_{i=1}^{\tau}\mathbf{r}_{T_j,i}(\mathbf{x}_{t,i})^3\right]_{q_t}, t \in [\![3]\!]$.

(4) Output the ciphertext C and all level-3 encodings $E = \left\{\left(\mathbf{u}_{1,T_j}, \mathbf{u}_{2,T_j}, \mathbf{u}_{3,T_j}\right), T_j \in Set\right\}$.

Decrypt(C, E, W):

(1) Given C, E and a witness set W, compute $\mathbf{u}_t = \left[\prod_{T_j \in W}\mathbf{u}_{t,T_j}\right]_{q_t}, t \in [\![3]\!]$.

(2) Generate $sk = \mathrm{Ext}\left(\mathrm{par}, \left(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3\right)\right)$, and decrypt C to the message M.

Similar to [GGSW13], the security of our construction depends on the hardness assumption of the Decision Graded Encoding No-Exact-Cover.

Theorem 5.2 Suppose that the Decision Graded Encoding No-Exact-Cover is hard. Then our construction is a witness encryption scheme.

5.2.2 Hu-Jia Attacks

Since $\mathbf{u}_{t,T_j} = \left[\mathbf{u}_{j_1}\mathbf{u}_{j_2}\mathbf{u}_{j_3} + \sum_{i=1}^{\tau}\mathbf{r}_{T_j,i}(\mathbf{x}_{t,i})^3\right]_{q_t}, t \in [\![3]\!]$ is a level-3 encoding in our encoding method, one cannot obtain $\mathbf{u}_{t,T_i} = \left[\mathbf{u}_{t,T_j}\mathbf{u}_{t,T_k}(\mathbf{u}_{t,T_l})^{-1}\right]_{q_t}$ when $T_i = T_j \cup T_k - T_l$. As a result, the Hu-Jia attacks [HJ15a, HJ15b] are prevented in our new construction.

6 Conclusion

In this paper, we construct a new multilinear map, which supports the applications for public tools of encoding in the GGH13 map, such as MPKE and WE. Using switching modulo and two zero testing parameters, our construction introduces new noise term to thwart zeroizing attack against the GGH13 map. As a result, our new construction not only prevents all known attacks, but also seemly supports the hardness assumption of the SubM problem and the DLIN problem.

References

[BF03] D. Boneh and M. K. Franklin. Identity-based encryption from the Weil pairing, SIAM Journal on Computing, 32(3):586–615, 2003.

[BGG+14] D. Boneh, C. Gentry, S. Gorbunov, S. Halevi, V. Nikolaenko, G. Segev, V. Vaikuntanathan, and D. Vinayagamurthy. Fully keyhomomorphic encryption, arithmetic circuit abe and compact garbled circuits. EUROCRYPT 2014, LNCS 8441, pp. 533-556.

[BR14] Z. Brakerski and G. N. Rothblum. Virtual black-box obfuscation for all circuits via generic graded encoding. TCC 2014, LNCS 8349, pp. 1-25.

[BS03] D. Boneh and A. Silverberg. Applications of multilinear forms to cryptography. Contemporary Mathematics, 324:71–90, 2003.

[BWZ14] D. Boneh, D. J. Wu, and J. Zimmerman. Immunizing multilinear maps against zeroizing attacks. http://eprint.iacr.org/2014/930.

[BZ14]D. Boneh and M. Zhandry. Multiparty key exchange, efficient traitor tracing, and more from indistinguishability obfuscation. CRYPTO 2014, LNCS 8616, pp. 480-499.

[CGH+15] J. S. Coron, C. Gentry, S. Halevi, T. Lepoint, H. K. Maji, E. Miles, M. Raykova, A. Sahai, M. Tibouchi. Zeroizing Without Low-Level Zeroes New MMAP Attacks and Their Limitations. http://eprint.iacr.org/2015/596.

[CHL+14] J. H. Cheon, K. Han, C. Lee, H. Ryu, D. Stehle. Cryptanalysis of the Multilinear Map over the Integers. http://eprint.iacr.org/2014/906.

[CL15] J. H. Cheon, C. Lee. Cryptanalysis of the multilinear map on the ideal lattices. http://eprint.iacr.org/2015/461.

[CLT13] J. S. Coron, T. Lepoint, and M. Tibouchi. Practical multilinear maps over the integers. CRYPTO 2013, LNCS 8042, pp. 476–493.

[CLT14] J. S. Coron, T. Lepoint, and M. Tibouchi. Cryptanalysis of two candidate fixes of multilinear maps over the integers. http://eprint.iacr.org/2014/975.

[CLT15] J. S. Coron, T. Lepoint, and M. Tibouchi. New Multilinear Maps over the Integers. http://eprint.iacr.org/2015/162.

[CN11] Y. Chen and P. Q. Nguyen. BKZ 2.0 Better Lattice Security Estimates, ASIACRYPT 2011, LNCS 7073, pp. 1–20.

[GG13] J. von zur Gathen, J. Gerhard. Modern computer algebra [M]. 3rd edition, Cambridge: Cambridge University Press, 2013.

[GGH13] S. Garg, C. Gentry, and S. Halevi. Candidate multilinear maps from ideal lattices. EUROCRYPT 2013, LNCS 7881, pp. 1–17.

[GGH+13a] S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai, and B. Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. FOCS 2013, pp.40-49.

[GGH+13b] S. Garg, C. Gentry, S. Halevi, A. Sahai, and B. Waters. Attribute-based encryption for circuits from multilinear maps, CRYPTO (2) 2013, LNCS 8043, 479-499.

[GGH+14] S. Garg, C. Gentry, S. Halevi, and M. Zhandry. Fully secure functional encryption without obfuscation. http://eprint.iacr.org/2014/666.

[GGH15] C. Gentry, S. Gorbunov, and S. Halevi. Graph-induced multilinear maps from lattices. TCC 2015, Part II, LNCS 9015, pp. 498–527.

[GHM+14] C. Gentry, S. Halevi, H. K. Majiy, A. Sahaiz. Zeroizing without zeroes: Cryptanalyzing multilinear maps without encodings of zero. http://eprint.iacr.org/2014/929.

[Gol08] O. Goldreich. Computational Complexity: a Conceptual Perspective. Cambridge University Press, New York, NY, USA, 1 edition, 2008.

[GSW13a] S. Garg, C. Gentry, A. Sahai, and B. Waters. Witness encryption and its applications. STOC 2013, pp. 467-476.

[GSW13b] C. Gentry, A. Sahai and B. Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. CRYPTO (1) 2013, LNCS 8042, pp. 75-92.

[Gu15] Gu Chunsheng. Multilinear Maps Using Ideal Lattices without Encodings of Zero. http://eprint.iacr.org/2015/023.

[HIL+99] J. Hastad, R. Impagliazzo, L. A. Levin, and M. Luby. A pseudorandom generator from any one-way function. SIAM Journal on Computing, 1999, 28(4):1364-1396.

[HJ15a] Yupu Hu and Huiwen Jia. Cryptanalysis of GGH Map. http://eprint.iacr.org/2015/301.

[HJ15b] Yupu Hu and Huiwen Jia. A Comment on Gu Map-1. http://eprint.iacr.org/2015/448.

[HJ15c] Yupu Hu and Huiwen Jia. An Optimization of Gu Map-1. http://eprint.iacr.org/2015/453.

[HPS98] J. Hoffstein, J. Pipher, and J. H. Silverman. NTRU: a ring based public key cryptosystem. ANTS 1998, LNCS 1423, pp. 267-288.

[Jou00] A. Joux. A one round protocol for tripartite Diffie-Hellman. ANTS 2000, LNCS 1838, pp. 385–394.

[LLL82] H.W. Lenstra, A.K. Lenstra and L. Lovasz. Factoring polynomials with rational coefficients. Mathematische Annalen, 1982, 261(4): 515–534.

[LSS14] A. Langlois, D. Stehlé, and R. Steinfeld, GGHLite: More Efficient Multilinear Maps from Ideal Lattices, EUROCRYPT 2014, LNCS 8441, 2014, pp. 239–256.

[PTT10] C. Papamanthou, R. Tamassia, and N. Triandopoulos. Optimal authenticated data structures with multilinear forms. Pairing 2010, LNCS 6487, pp. 246–264.

[Rot13] R. Rothblum. On the circular security of bit-encryption. TCC 2013, LNCS 7785, 2013, pp. 579–598.

[RS09] M. Rückert and D. Schröder. Aggregate and verifiably encrypted signatures from multilinear maps without random oracles. ISA 2009, LNCS 5576, pp. 750–759.

[Sho09] V. Shoup. NTL: A Library for doing Number Theory. http://shoup.net/ntl/, Version 5.5.2, 2009. 2009.08.14.

[Sma03] Smart, N.P. An identity based authenticated key agreement protocol based on the Weil pairing, Electronics Letters, 38(13), pp. 630-632, 2002.

[SOK00] R. Sakai, K. Ohgishi and M. Kasahara. Cryptosystems based on pairing, the 2000 Symposium on Cryptography and Information Security, Okinawa, Japan, 2000.

[SS11] D. Stehlé and R. Steinfeld. Making NTRU as secure as worst-case problems over ideal lattices, EUROCRYPT 2011, LNCS 6632, pp. 27–47.