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 24, 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 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 encodings 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, 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 [Hal15] 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 $g \in R$, and a secret random invertible element $z \in R_q = R / qR$ are chosen during generating the public parameters of the GGH13 construction. A plaintext element $e \in R / gR$ is encoded at level-$k$ as $\left[ e / z^k \right]_q$, where $e$ is a small element in the coset $e_i = e + rg$ for some $r \in R$. 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 \( \frac{\tau}{z} \) is presented to test for zero at a level-\( \kappa \) encoding. Given a level-\( \kappa \) encoding \( u = \left[ \frac{c}{z^k} \right]_q \), one computes \( [u \cdot p_{\tau}]_q \) and checks if the norm of \( [u \cdot p_{\tau}]_q \) is smaller than \( q \) to determine whether \( u \) is zero.

Hu-Jia attack. Assume that \( \{q, y, x, i, j, \tau \} \in \mathbb{F} \) is the public parameters of the GGH13 map, where \( y = \left[ \frac{(1 + ag) / z}{q} \right], x = \left[ \frac{(a, g) / z}{q} \right], \) \( i, j \in \mathbb{F} \). Given an arbitrary level-\( k \) encoding \( u = \left[ \frac{c}{z^k} \right]_q \), one computes using zeroizing attack

\[
[v_{k,i,j}] = \left[ u \cdot x^j \cdot y^{k-j} \cdot p_{\tau} \right]_q = \left[ h(c(a)) / g^{i-j} (1 + ag)^{x-k-j} \right]_q,
\]

where \( 1 \leq k < \kappa, 1 \leq j < \kappa \) and \( k + j \leq \kappa \).

Since \( v_{k,i,j} \) is not reduced modulo \( q \), \( v_{k,i,j} \) contains a factor \( g \) when \( i < j \). As a result, one can obtain a basis of the secret element \( g \). 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 \( g_1, g_2, g_3 \in R \), and secret random invertible elements \( z_1 \in R_{q_1} = R / q_1R \). A plaintext element \( e \) in \( R / gR \) is encoded at level-\( k \) as \( \left[ \left[ \frac{c_1}{z^1} \right]_{q_1}, \left[ \frac{c_2}{z^2} \right]_{q_2}, \left[ \frac{c_3}{z^3} \right]_{q_3} \right] \), where \( c_1 \) is a small element in the coset \( e_i = e + r_i g_i \) for some \( r_i \in R \) such that \( c_1 = c_2 \) and \( c_1 = c_3 \text{ mod } g_3 \). For this three-encodings, we design new zero-testing parameters

\[
\begin{align*}
p_{zt,1} &= \left[ h_0 \cdot z_0 + z_0 \left( h_1 \cdot \left[ g_1 \right]_{q_1} \right) + h_2 \cdot \left[ g_2^{-1} \right]_{q_1} + h_3 \cdot \left[ g_3^{-1} \right]_{q_1} \right], \\
p_{zt,2} &= \left[ z_2 \left( h_0 \cdot z_0 + h_2 \cdot \left[ g_2 \right]_{q_1} \right) + q_2 \cdot \left( g_2^{-1} \right)_{q_1} \right], \\
p_{zt,3} &= \left[ z_3 \left( h_1 + h_3 \cdot g_3 \right) + q_3 \cdot \left( x \text{ mod } g_3 \right) \right],
\end{align*}
\]

where \( z_0 \in R_{q_1}, z = \left[ q_2 / q_1 \cdot \left[ z_0 / z_1 \right] \right]_{q_1} \).

Given a level-\( \kappa \) encoding \( \left[ \left[ u_1, u_2, u_3 \right] \right] \), one computes

\[
v = \left[ q_3 / q_1 \cdot \left[ u_1 \cdot p_{zt,1} \right]_{q_1} \right] - \left[ q_3 / q_2 \cdot \left[ u_2 \cdot p_{zt,2} \right]_{q_2} \right] - \left[ u_3 \cdot p_{zt,3} \right]_{q_3},
\]

and checks if the norm of \( v \) is smaller than \( q_3 \) to determine whether \( u \) is zero.

Now, using the weak-DL attack, one can no longer obtain a basis of \( g_1 \). The aim that we include \( z_0, z \) 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 $g_1$. 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 $g_1$. 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 $\{1, 2, \ldots, n\}$, and $[a]_q$ the absolute minimum residual system $[a]_q = a \mod q \in (-q/2, q/2]$. 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 column of $\mathbf{A}$ is denoted as $A_{ij}$ (or $A[i,j]$). Notation $\|\mathbf{a}\|_\infty$ (or $\|\mathbf{a}\|$ for short) denotes the infinity norm of $\mathbf{a}$. The polynomial ring $\mathbb{Z}[x]/(x^n + 1)$ is denoted by $R$, and $\mathbb{Z}_q[x]/(x^n + 1)$ by $R_q$. The elements in $R$ and $R_q$ are denoted in bold as well. Similarly, notation $[a]_q$ 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 $L \subseteq \mathbb{R}^n$ 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 $P(\mathbf{B}) = \{\mathbf{B} \mathbf{y} : \mathbf{y} \in \mathbb{R}^n, \forall i: -1/2 \leq y_i < 1/2\}$ 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 $\text{Rot}(\mathbf{g}) = (\mathbf{g}, x \mathbf{g}, \ldots, x^{n-1} \mathbf{g})$.

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

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

1. Elements $\{g_j \in G_j\}_{j=1,\ldots,\kappa}$, index $j \in [\kappa]$, and integer $a \in \mathbb{Z}_q$ hold that $e(g_{j_1}, \ldots, a \cdot g_{j_a}, \ldots, g_{j_\kappa}) = a \cdot e(g_{j_1}, \ldots, g_{j_\kappa})$.

2. Map $e$ is non-degenerate in the following sense: if elements $\{g_j \in G_j\}_{j=1,\ldots,\kappa}$ are generators of their respective groups, then $e(g_{j_1}, \ldots, g_{j_\kappa})$ is a generator of $G_\tau$.

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

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

2. Binary operations `+` and `-` exist, such that every $\alpha_1, \alpha_2$, 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 $\alpha_1, \alpha_2$, every index $j_1, j_2 \in [\kappa]$ with $j_1 + j_2 \leq \kappa$, and every $u_1 \in S_{j_1}^{(\alpha_1)}$ and $u_2 \in S_{j_2}^{(\alpha_2)}$ hold that $u_1 \times u_2 \in S_{j_1 + j_2}^{(\alpha_1 \alpha_2)}$, where $\alpha_1 \alpha_2$ is the multiplication operation in $R$ and $j_1 + j_2$ is the integer addition.

3 Our new construction

**Setting the parameters.** Let $\lambda$ be the security parameter, $\kappa$ the multilinearly level, $n$ the dimension of elements of $R$. Concrete parameters are set as $\sigma = \sqrt{n} \cdot \sigma' = n^{1.5} \cdot \sigma^* = 2^{\lambda} \cdot q_1 \cdot q_2 \cdot q_3 \geq 2^{k\kappa} \cdot n^{O(\kappa)}$, with $n > O(\kappa^2 \cdot \tau) = O(n^2)$, $\rho = O(n)$.

3.1 Construction

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

1. Choose primes $q_i \geq 2^{k\kappa} \cdot n^{O(\kappa)}, i \in [3]$ with $q_i > 2^{\lambda} \cdot q_2 > 2^{2\lambda} \cdot q_3$.

2. Choose $g_i \leftarrow D_{Z^{n^2}}, i \in [3]$ in $R$ so that $\|g_i\| < n^2$.

3. Choose $a_{i,0}, b_{i,0}, a_{i,j}, b_{i,j} \leftarrow D_{Z'_{n^2}}, i \in [\tau]$ in $R$.

Choose $h_{i,0}, h_{i} \leftarrow D_{Z'_{n^2}}, i \in [3]$ in $R$.

4. Choose uniformly random elements $z_0 \leftarrow R_{q_0}, z_i \leftarrow R_{q_0}, i \in [3]$ with $z_i^{-1} \in R_{q_0}$.

5. Set $e_i = (a_i g_i + 1) \mod g_i$, namely $a_i g_i + 1 = b_i g_i + e_i$ so that $\|b_i\| < n^2$.

6. Set $y_i = \left[\frac{a_i g_i + 1}{z_i}\right]_{q_i}$ and $x_{i,j} = \left[\frac{a_i g_i + 1}{z_i}\right]_{q_i}$. 
\[ y_2 = \left[ \frac{a, g_i + 1}{z_2} \right]_{q_2} \quad \text{and} \quad x_{2,j} = \left[ \frac{a, g_i}{z_2} \right]_{q_2} ; \]
\[ y_3 = \left[ \frac{b, g_i + e_i}{z_3} \right]_{q_3} \quad \text{and} \quad x_{3,j} = \left[ \frac{b, g_i + e_i}{z_3} \right]_{q_3} . \]

(7) Set \( z = \left[ \frac{q_2}{q_1} \right] \).

(8) Set \( p_{z,t,1} = \left[ h_1, t z_0 + z_t^e \left( h_1 \cdot \left[ g_1^{-1} \right]_{q_1} + h_2 \cdot \left[ g_2^{-1} \right]_{q_1} + h_3 \cdot \left[ g_3^{-1} \right]_{q_1} \right) \right]_{q_1} , \)
\[ p_{z,t,2} = \left[ z_t^e \left( h_1 + h_2, g_2 \right) g_2^{-1} \right]_{q_1} , \]
\[ p_{z,t,3} = \left[ z_t^e \left( h_1 + h_3, g_3 \right) g_3^{-1} \right]_{q_1} , \]
where \( g_2^{-1} = \left[ q_2 / q_1 \right] \cdot \left[ g_2^{-1} \right]_{q_1} \) \( g_3^{-1} = \left[ q_3 / q_1 \right] \cdot \left[ g_3^{-1} \right]_{q_1} \).

(9) Output the public parameters \( \text{par} = \left\{ \left\{ q_t, y_t, \left\{ x_{z,t} \right\}_{t \in [3]} \right\} \right\} \).

Generating level-\( k \) encoding: \( \left( u_1, u_2, u_3 \right) \leftarrow \text{Enc} \left( \text{par}, k, d \right) . \)

1. Sample \( r_i \leftarrow D_{z^{2^k}}^\ast , i \in [r] ; \)
2. Given \( d \leftarrow D_{z^{2^k}}^\ast , \) compute \( u_1 = \left[ d \cdot (y_i)^k + \sum_{i=1}^{r} r_i \cdot (x_i)^k \right]_{q_1} \), \( t \in [3] ; \)
3. Output \( \left( u_1, u_2, u_3 \right) \) as a level-\( k \) encoding of \( d . \)

Adding encodings: \( \left( u_1, u_2, u_3 \right) \leftarrow \text{Add} \left( \text{par}, k, \left( u_{1,1}, u_{2,1}, u_{3,1} \right), \ldots, \left( u_{1,s}, u_{2,s}, u_{3,s} \right) \right) \).

1. Given \( s \) level-\( k \) encodings \( \left( u_{i,1}, u_{i,2}, u_{i,3} \right) \), compute \( u_t = \left[ \sum_{i=1}^{s} u_{i,t} \right]_{q_1} , t \in [3] ; \)
2. Output a level-\( k \) encoding \( \left( u_1, u_2, u_3 \right) . \)

Multiplying encodings: \( \left( u_1, u_2, u_3 \right) \leftarrow \text{Mul} \left( \text{par}, \left( u_{1,1}, u_{2,1}, u_{3,1} \right), \ldots, \left( u_{1,k}, u_{2,k}, u_{3,k} \right) \right) . \)

1. Given \( k \) level-1 encodings \( \left( u_{i,1}, u_{i,2}, u_{i,3} \right) \), compute \( u_t = \left[ \prod_{i=1}^{k} u_{i,t} \right]_{q_1} , t \in [3] . \)
2. Output a level-\( k \) encoding \( \left( u_1, u_2, u_3 \right) . \)

Zero testing: \( \text{isZero} \left( \text{par}, \left( u_1, u_2, u_3 \right) \right) . \)

Given a level-\( \kappa \) encoding \( \left( u_1, u_2, u_3 \right) , \) to determine whether \( u_1 \) is a level-\( \kappa \) encoding of zero for \( g_1 \), we compute \( v = \left[ q_2 / q_1 \right] \cdot \left[ u_1, p_{z,t,1} \right]_{q_1} - \left[ q_2 / q_2 \right] \cdot \left[ u_2, p_{z,t,2} \right]_{q_2} - \left[ u_3, p_{z,t,3} \right]_{q_3} \) and check whether \( \| v \| \) is short:
\[ \text{isZero} \left( \text{par}, \left( u_1, u_2, u_3 \right) \right) = \begin{cases} 1 & \text{if } \| v \| < q_3^{3/4} \\
0 & \text{otherwise} \end{cases} . \]

Extraction: \( sk \leftarrow \text{Ext} \left( \text{par}, \left( u_1, u_2, u_3 \right) \right) . \)

Given a level-\( \kappa \) encoding \( \left( u_1, u_2, u_3 \right) , \) we compute
\[ v = \left[ \frac{q_3}{q_1} \cdot [u_1 \cdot p_{x,1}]_{q_1} \right] - \left[ \frac{q_3}{q_2} \cdot [u_2 \cdot p_{x,2}]_{q_2} \right] - \left[ [u_3 \cdot p_{x,3}]_{q_3} \right], \quad \text{and} \quad \eta = (\log q_3) / 4 - \lambda \text{ most-significant bits of each of the } n \text{ coefficients of } v: \]

\[ \text{Ext} (\text{par}, (u_1, u_2, u_3)) = \text{Extract}_s (\text{msbs}_s (v)). \]

**Remark 3.1** In our construction, switching modulus and using \( z_0, z \) in the zero-testing parameters are to avoid the attack in [CGH+15].

### 3.2 Correctness

**Lemma 3.2** The algorithm InstGen\( (1^k, 1^\ell) \) runs in polynomial time.

**Lemma 3.3** The encoding \( (u_1, u_2, u_3) \leftarrow \text{Enc}(\text{par}, k, d) \) is a level-\( k \) encoding.

**Proof.** We only need to show that \( u_1 \) is a level-\( k \) encoding of \( d \) for the ideal lattice \( \langle g_i \rangle \), \( u_1, u_2 \) have same numerator, and level-\( k \) encodings \( u_1, u_3 \) encode same level-0 encoding for the ideal lattice \( \langle g_i \rangle \).

1. By \( u_t = \left[ d \cdot (y_t)^k + \sum_{i=1}^{r} r_i \cdot (x_{t,i})^k \right]_{q_t}, \) for \( t \in \{1, 2\} \) we have
   \[
   u_t = \left[ d \cdot (y_t)^k + \sum_{i=1}^{r} r_i \cdot (x_{t,i})^k \right]_{q_t},
   \]

   \[
   = \left[ d \cdot \left( a \cdot g_i + 1 \right)^k + \sum_{i=1}^{r} r_i \cdot \left( \frac{a \cdot g_i}{z_i} \right)^k \right]_{q_t},
   \]

   \[
   = \left[ \frac{d \cdot (a \cdot g_i + 1)^k + \sum_{i=1}^{r} r_i \cdot (a \cdot g_i)^k}{z_i^k} \right]_{q_t},
   \]

   \[
   = \left[ \frac{ag_i + d}{z_i^k} \right]_{q_t},
   \]

   where \( a = \left( d \cdot (a \cdot g_i + 1)^k + \sum_{i=1}^{r} r_i \cdot (a \cdot g_i)^k - d \right) / g_i. \)

   Thus, \( u_t \) is a level-\( k \) encoding of the level-0 encoding \( d \) for \( \langle g_i \rangle \), and \( u_1, u_2 \) have same numerator \( ag_i + d \).

2. For \( t \in \{1, 3\} \) we have
   \[
   u_t = \left[ d \cdot (y_t)^k + \sum_{i=1}^{r} r_i \cdot (x_{t,i})^k \right]_{q_t},
   \]

   \[
   = \left[ d \cdot \left( b \cdot g_i + e_i \right)^k + \sum_{i=1}^{r} r_i \cdot \left( \frac{b \cdot g_i + e_i}{z_i} \right)^k \right]_{q_t},
   \]

   \[
   = \left[ \frac{cg_i + e}{z_i^k} \right]_{q_t},
   \]

   where \( e = d \cdot (e_i)^k + \sum_{i=1}^{r} r_i \cdot (e_{i,j})^k \), and \( e_i = \left( d \cdot (b \cdot g_i + e_i)^k + \sum_{i=1}^{r} r_i \cdot (b \cdot g_i + e_{i,j})^k - e \right) / g_i. \)
Lemma 3.4 The encoding \( \langle g_1 \rangle \) is a level-1 encoding.

Proof. Since for \( \langle g_1 \rangle \), a level-1 encoding \( u_{i,j}, t \in \{1, 2\} \) has the form \( u_{i,j} = \left( \frac{rg_t + d_t}{z_t} \right)_{q_t} \), then the sum is
\[
\sum_{i=1}^{s} u_{i,j} = \sum_{i=1}^{s} \left( \frac{rg_t + d_t}{z_t} \right)_{q_t} = \left( \frac{rg_t + d_t}{z_t} \right)_{q_t},
\]
where \( r = \sum_{i=1}^{s} r_t \) and \( d = \sum_{i=1}^{s} d_t \).

Namely, \( u_1 \) is a level-1 encoding for the ideal lattice \( \langle g_1 \rangle \), and \( u_1, u_2 \) have same numerator \( rg_t + d_t \).

Again for \( \langle g_3 \rangle \), a level-1 encoding \( u_{i,j}, t \in \{1, 3\} \) has the form \( u_{i,j} = \left( \frac{c_tg_3 + e_t}{z_t} \right)_{q_t} \). Thus, we have
\[
\sum_{i=1}^{s} u_{i,j} = \sum_{i=1}^{s} \left( \frac{c_tg_3 + e_t}{z_t} \right)_{q_t} = \left( \frac{c_tg_3 + e_t}{z_t} \right)_{q_t},
\]
where \( c = \sum_{i=1}^{s} c_t \) and \( e = \sum_{i=1}^{s} e_t \).

That is, level-1 encodings \( u_1, u_3 \) encode same level-0 encoding for \( \langle g_3 \rangle \).

Lemma 3.5 The encoding \( \langle g_1 \rangle \) is a level-1 encoding.

Proof. Since for \( \langle g_1 \rangle \), \( u_{i,j} = \left( \frac{rg_t + d_t}{z_t} \right)_{q_t}, t \in \{1, 2\} \), their product is:
\[
u_t = \left( \prod_{i=1}^{k} u_{i,j} \right)_{q_t} = \left( \prod_{i=1}^{k} \frac{rg_t + d_t}{z_t} \right)_{q_t} = \left( \frac{rg_t + d_t}{z_t} \right)_{q_t},
\]
where \( d = \prod_{i=1}^{k} d_t, r = (\prod_{i=1}^{k} (rg_t + d_t) - d) / g_t \).

Again for \( \langle g_3 \rangle \), the level-1 encoding \( u_{i,j}, t \in \{1, 3\} \) has the form \( u_{i,j} = \left( \frac{c_tg_3 + e_t}{z_t} \right)_{q_t} \). Thus, we have
\[
u_t = \left( \prod_{i=1}^{k} c_tg_3 + e_t \right)_{q_t} = \left( \prod_{i=1}^{k} \frac{c_tg_3 + e_t}{z_t} \right)_{q_t} = \left( \frac{c_tg_3 + e_t}{z_t} \right)_{q_t},
\]
where \( e = \prod_{i=1}^{k} e_t \) and \( c = (\prod_{i=1}^{k} (c_tg_3 + e_t) - e) / g_3 \).
\[
\begin{bmatrix} \frac{p}{q} \cdot v \end{bmatrix} = \left[ w \cdot \begin{bmatrix} \frac{p}{q} \cdot z \end{bmatrix}_p \right] + \tilde{\delta} \text{ such that } \|\tilde{\delta}\| < l_i(w),
\]
where \(l_i(w)\) is \(l_i\)-norm of \(w\).

**Proof.** By \(v = [w \cdot z]_q = w \cdot z - q \cdot k\), we get

\[
\begin{align*}
\frac{p}{q} \cdot v &= w \cdot \left(\frac{p}{q} \cdot z\right) - p \cdot k, \\
w \cdot \left(\frac{p}{q} \cdot z\right) &= w \cdot \left(\frac{p}{q} \cdot z\right) + w \cdot \left(\frac{p}{q} \cdot z - \frac{p}{q} \cdot z\right), \\
&= w \cdot \left(\frac{p}{q} \cdot z\right) + w \cdot \epsilon
\end{align*}
\]

where \(\|\epsilon\| < 1\).

Therefore,

\[
\begin{align*}
\begin{bmatrix} \frac{p}{q} \cdot v \end{bmatrix} &= \begin{bmatrix} \frac{p}{q} \cdot [w \cdot z]_q \end{bmatrix} \\
&= \left[ w \cdot \left(\frac{p}{q} \cdot z\right) - p \cdot k \right] \\
&= \left[ w \cdot \left(\frac{p}{q} \cdot z\right) \right] + \left[ w \cdot \epsilon \right] - p \cdot k \\
&= \left[ w \cdot \left(\frac{p}{q} \cdot z\right) \right] + p \cdot \beta + \left[ w \cdot \epsilon \right] - p \cdot k
\end{align*}
\]

By \(\left\| \frac{p}{q} \cdot v \right\| < p / 2\), we have \(\beta = k\) with high probability. That is,

\[
\begin{bmatrix} \frac{p}{q} \cdot v \end{bmatrix} = \left[ w \cdot \left(\frac{p}{q} \cdot z\right) \right] + \tilde{\delta} \text{ such that } \tilde{\delta} = \left[ w \cdot \epsilon \right]. \text{By } \|\epsilon\| < 1, \text{ we obtain } \|\tilde{\delta}\| < l_i(w). \quad \square
\]

**Corollary 3.7** Suppose that \(p, q\) are primes and \(v_i = [w_i \cdot \left(\frac{g^{-1}}{q} \right)_q, t \in [3]\) with \(\|w_i\| \ll p\). Then,

\[
\begin{bmatrix} \frac{p}{q} \cdot v_i \end{bmatrix} = \left[ w_i \cdot \left(\frac{p}{q} \cdot \frac{g^{-1}}{q} \right)_q \right] + \tilde{\delta}_i \text{ with } \|\tilde{\delta}_i\| < l_i(w_i),
\]

where \(l_i(w_i)\) is \(l_i\)-norm of \(w_i\).

**Proof.** By \(\left[ \frac{g^{-1}}{q} \right]_{q'} \in R_q\), the result is proved by directly taking \(z = \left[ \frac{g^{-1}}{q} \right]_{q'}\) in Lemma 3.6.

**Corollary 3.8** Suppose that \(p, q\) are primes and \(a_i = \left[ g_i \cdot \left(\frac{p}{q} \cdot \frac{g^{-1}}{q} \right)_q \right]_p, t \in [3]\). Then

\[
\|a_i\| \leq l_i(g_i) + \left\lfloor \frac{p}{q} \right\rfloor.
\]

**Proof.** Assume that \(v_i = [w_i \cdot \left(\frac{g^{-1}}{q} \right)_q\) with \(w_i = g_i\). Then by Lemma 3.6, we have
\[
\left[ \frac{P}{q} (1,0,\ldots,0) \right] = \left[ \frac{P}{q} \mathbf{v} \right] = \left[ g_r, \left[ \frac{P}{q} \mathbf{g}_r^{-1} \right]_q \right]_p + \delta_r \quad \text{and} \quad \| \delta_r \| \leq l_1(\mathbf{g}_r).
\]

Thus, \( \alpha_r = \left[ g_r, \left[ \frac{P}{q} \mathbf{g}_r^{-1} \right]_q \right]_p \) and \( \alpha_r < l_1(\mathbf{g}_r) + \left[ \frac{P}{q} \right] \). □

**Corollary 3.9** Suppose that \( q_t, t \in [3] \) are primes and \( \mathbf{v} = [\mathbf{w} \cdot \mathbf{z}] \) with \( \mathbf{z} \in R_{q_t} \) such that \( \| \mathbf{w} \| << q_t, t \in [3] \). Then
\[
\left[ \frac{q_3}{q_2}, \frac{q_2}{q_1} \mathbf{v} \right] = \left[ \mathbf{w} \cdot \left[ \frac{q_3}{q_1} \mathbf{z} \right] \right]_p + \delta \quad \text{with} \quad \| \delta \| < l_1(\mathbf{w}) + \left[ \frac{q_3}{q_2} \right] + 1,
\]
where \( l_1(\mathbf{w}) \) is \( l_1 \)-norm of \( \mathbf{w} \).

**Proof.** By \( \left[ \frac{q_3}{q_2}, \frac{q_2}{q_1} \mathbf{v} \right] = \frac{q_3}{q_2} \mathbf{v} - \epsilon_1 \) with \( \| \epsilon_1 \| < 1 \), we have \( \frac{q_3}{q_2} \mathbf{v} = \frac{q_3}{q_2} \mathbf{v} - \frac{q_3}{q_2} \epsilon_1 \). Thus,
\[
\left[ \frac{q_3}{q_2}, \frac{q_2}{q_1} \mathbf{v} \right] = \left[ \frac{q_3}{q_1} \mathbf{v} \right] - \left[ \frac{q_3}{q_2} \epsilon_1 \right] - \epsilon_2 \quad \text{with} \quad \| \epsilon_2 \| < 1.
\]

By Lemma 3.6, we obtain \( \left[ \frac{q_3}{q_1} \mathbf{v} \right] = \left[ \mathbf{w} \cdot \left[ \frac{q_3}{q_1} \mathbf{z} \right] \right]_p + \delta_0 \) with \( \| \delta_0 \| < l_1(\mathbf{w}) \).

Namely,
\[
\left[ \frac{q_3}{q_2}, \frac{q_2}{q_1} \mathbf{v} \right] = \left[ \mathbf{w} \cdot \left[ \frac{q_3}{q_1} \mathbf{z} \right] \right]_p + \delta_0 - \left[ \frac{q_3}{q_2} \epsilon_1 \right] - \epsilon_2 = \left[ \mathbf{w} \cdot \left[ \frac{q_3}{q_1} \mathbf{z} \right] \right] + \delta,
\]
where \( \delta = \delta_0 - \left[ \frac{q_3}{q_2} \epsilon_1 \right] - \epsilon_2 \) and \( \| \delta \| < l_1(\mathbf{w}) + \left[ \frac{q_3}{q_2} \right] + 1 \). □

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

**Proof.** For a level-\( \kappa \) encoding \( (\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3) \), without loss of generality, we assume
\[
\mathbf{u}_1 = \frac{[r_1 \mathbf{g}_r + d_1]}{z_1^t} \quad \mathbf{u}_2 = \frac{[r_2 \mathbf{g}_r + d_2]}{z_2^t} \quad \mathbf{u}_3 = \frac{[r_3 \mathbf{g}_r + d_3]}{z_3^t}.
\]

It is not difficult to verify that the norms of \( r_1, r_3 \) are all small. This is because the norm of \( r_1 \mathbf{g}_r + d_1 \) is small and \( \mathbf{g}_r, t \in [3] \) are satisfied to \( \| \mathbf{g}_r \| \) < \( n^2 \).

By \( \mathbf{v} = \left[ \frac{q_3}{q_1} \mathbf{u}_1 \cdot p_{z_1}, \mathbf{u}_2 \cdot p_{z_2}, \mathbf{u}_3 \cdot p_{z_3} \right]_q \), we compute \( \mathbf{v}_t, t \in [3] \) as follows:
\[ v_1 = \left[ \frac{q_1}{q_0} \left[ u_1 \cdot p_{x_1} \right] \right] = \left[ \frac{q_1}{q_0} \left[ h_{1,0} (r_2, g_2 + d_2) \frac{z_0}{z_1} \right] + \sum_{i=1}^{3} \left[ h_i (r_i, g_i + d_i) \cdot \left[ g_i^{-1} \right] \right] + c_i q_1 \right] , \]

\[ v_2 = \left[ \frac{q_2}{q_1} \left[ u_2 \cdot p_{x_2} \right] \right] = \left[ \frac{q_2}{q_1} \left[ h_{1,0} (r_2, g_2 + d_2) \frac{z_0}{z_1} \right] + \sum_{i=1}^{3} \left[ h_i (r_i, g_i + d_i) \cdot \left[ g_i^{-1} \right] \right] + \delta_1 + c_i q_3 \right] , \]

where \( \| c_i \| < 4 \), \( \delta_1 = \delta_{1,0} + \sum_{i=1}^{3} \delta_{1,i} \) such that \( \| \delta_{1,0} \| \leq l_1 \left( h_{1,0} (r_2, g_2 + d_2) \right) \) and \( \| \delta_{1,i} \| \leq l_1 \left( h_i (r_i, g_i + d_i) \right), \) \( t \in [3] \).

By Corollary 3.9 and \( z = \left[ \frac{q_2}{q_1} \left[ z_0 \right] \right], \) \( g_{2,1}^{-1} = \left[ \left( q_2 / q_1 \right) \cdot \left[ g_2^{-1} \right] \right] \), we obtain

\[ v_2 = \left[ h_{1,0} (r_2, g_2 + d_2) \frac{z_0}{z_1} \right] + \sum_{i=1}^{3} \left[ h_i (r_i, g_i + d_i) \cdot \left[ g_i^{-1} \right] \right] + \delta_2 + c_2 q_3 \]

where \( \delta_2 = \delta_{2,0} + \delta_{2,1} \) such that \( \| \delta_{2,0} \| \leq l_1 \left( h_{1,0} (r_2, g_2 + d_2) \right) + 2 < n^2 q_0^{5/8} \) and \( \| \delta_{2,1} \| \leq l_1 \left( h_2 + h_2,0 g_2 \right) (r_2, g_2 + d_2) + 2 < n^2 q_0^{5/8} \).

\[ v_3 = \left[ u_3 \cdot p_{x_3} \right] = \left[ \left( h_3 + h_3,0 g_3 \right) (r_3, g_3 + d_3) \cdot \left[ \frac{q_3}{q_1} \left[ g_3^{-1} \right] \right] \right] , \]

Thus, we have

\[ v = \left[ v_1 - v_2 - v_3 \right] = \left[ h_1 r_1 + \frac{q_1}{q_0} \left[ g_1^{-1} \right] + h_1 r_1 a_1 \left( h_2,0,0 r_2,0 a_2 \right) + (h_3,0 r_3 - h_3,0 r_3) a_3 + \delta_1 - \delta_2 \right] , \]

\[ = \left[ h_1 r_1 + \frac{q_1}{q_0} \left[ g_1^{-1} \right] + \delta \right] , \]

where \( a_i = \left[ g_i \cdot \frac{q_i}{q_1} \left[ g_i^{-1} \right] \right], \) \( t \in [3], r_1 = r_1^r, r_2 = r_2, g_2 + d_2, r_3 = r_3 - c_1, r_4 = r_4 g_3 + d_3, \)

and \( \delta = h_1 r_1 a_1 - h_2,0 r_2 a_2 + (h_3,0 r_3 - h_3,0 r_3) a_3 + \delta_1 - \delta_2. \)
If $\mathbf{u}_1$ is a level-$\kappa$ encoding of zero for $\langle \mathbf{g}_1 \rangle$, namely $\mathbf{d}_1 = 0$. Thus, we have

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

For our choice of parameter, we know $\|\mathbf{r}\| < q_3^{1/8}$, and $\|\mathbf{h}_i\| < n^2 q_3^{1/2}$, $\|\mathbf{h}_{2,0}\| < n^2 q_3^{1/2}$, $\|\mathbf{h}_{3,0}\| < n^2 q_3^{1/2}$. By Corollary 3.8, $\|\mathbf{a}\| < n^2, i \in [3]$.

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

$$\|\mathbf{v}\| = \|\mathbf{r}\| = \|\mathbf{h}_1 \mathbf{r}_1 \mathbf{a}_1 - \mathbf{h}_2 \mathbf{r}_2 \mathbf{a}_2 + (\mathbf{h}_3 \mathbf{r}_3' - \mathbf{h}_3 \mathbf{r}_4' \mathbf{a}_3 + \mathbf{\delta}_1 - \mathbf{\delta}_2\|$$

$$\leq n^{O(1)} \cdot q_3^{1/2} \cdot q_3^{1/8}$$

$$< q_3^{3/4}.$$  

If $\mathbf{u}_1$ is a level-$\kappa$ encoding of non-zero element for $\langle \mathbf{g}_1 \rangle$, namely $\mathbf{d}_1 \neq 0 \bmod \mathbf{g}_1$. By Lemma 4 in [GGH13],

$$\|\mathbf{h}_1 \mathbf{d}_1 \cdot \left[ \frac{q_3}{q_1} \left[ \mathbf{g}_1^{-1} \right]_{q_1} \right]_{q_3} \| \geq q_3^{1-\varepsilon'}$$

with high probability, where $\varepsilon'$ is an arbitrary small positive constant.

Thus, we obtain

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

$$\geq \|\mathbf{h}_1 \mathbf{d}_1 \cdot \left[ \frac{q_3}{q_1} \left[ \mathbf{g}_1^{-1} \right]_{q_1} \right]_{q_3} - \|\mathbf{\delta}\|$$

$$\geq q_3^{1-\varepsilon'} - q_3^{3/4}$$

$$> q_3^{1-\varepsilon'}$$

where $\varepsilon'$ is a small positive constant. \hfill \square

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

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

**Proof.** Without loss of generality, assume that $\mathbf{u}_{1,2} = \left[ \frac{r, s + \mathbf{d}_1}{z_1} \right]_{q_1}$, $s \in [2]$. Similar as the procedure of Lemma 10, we have

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

By Lemma 3.10, we get $\|\mathbf{\delta}^{(s)}\| \leq q_3^{3/4}$ and with high probability

$$\left[ \mathbf{h}_1 \mathbf{d}_1 \cdot \left[ \frac{q_3}{q_1} \left[ \mathbf{g}_1^{-1} \right]_{q_1} \right] \right] \approx q_3$$

when $\mathbf{d}_1 \neq 0 \bmod \mathbf{g}_1$. Thus $\eta = (\log q_3) / 4 - \lambda$ most-significant bits of each of the $n$ coefficients of $\mathbf{v}^{(1)}$ are equal to that of $\mathbf{v}^{(2)}$. \hfill \square
3.3 Hardness assumption

Consider the following security experiment:

1. \( \text{par} \leftarrow \text{InstGen}(1, \lambda) \)
2. For \( l = 0 \) to \( \kappa \):
   - Sample \( d_l \leftarrow D_{2^l \cdot \sigma} \), \( r_{i,j} \leftarrow D_{2^l \cdot \sigma} \); 
   - Generate level-1 encoding \( u_{i,j} = \left[ d_l y_i + \sum_{i=1}^l r_{i,j} x_{i,j} \right]_{q_l} \), \( t \in [3] \).
3. Set \( u_{i,j} = \prod_{i=1}^l u_{i,j} \), \( t \in [3] \).
4. Set \( v_C = v_D = \text{Ext}(\text{par}, \left[ d_l u_{1,1}, d_l u_{2,1}, d_l u_{3,1} \right]) \).
5. Sample \( r_0 \leftarrow D_{2^l \cdot \sigma} \), and set \( v_R = \text{Ext}(\text{par}, \left[ r_0 u_{1,1}, r_0 u_{2,1}, r_0 u_{3,1} \right]) \).

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

**Level-\( \kappa \)** extraction CDH (ext-GCDH): Given \( \left\{ \text{par}, \left( u_{1,1}, u_{2,1}, u_{3,1} \right), \ldots, \left( u_{1,k}, u_{2,k}, u_{3,k} \right) \right\} \), output a level-\( \kappa \) extraction encoding \( w \in R_{q_l} \) such that \( \left\| v_C - w \right\|_{q_l} \leq q_1^{3/4} \).

**Level-\( \kappa \)** extraction DDH (ext-GDDH): Given \( \left\{ \text{par}, \left( u_{1,1}, u_{2,1}, u_{3,1} \right), \ldots, \left( u_{1,k}, u_{2,k}, u_{3,k} \right), v \right\} \), distinguish between \( D_{\text{ext-GDDH}} = \left\{ \text{par}, \left( u_{1,1}, u_{2,1}, u_{3,1} \right), \ldots, \left( u_{1,k}, u_{2,k}, u_{3,k} \right), v_D \right\} \) and \( D_{\text{ext-RAND}} = \left\{ \text{par}, \left( u_{1,1}, u_{2,1}, u_{3,1} \right), \ldots, \left( u_{1,k}, u_{2,k}, u_{3,k} \right), v_R \right\} \).

In this paper, we assume that the ext-GCDH/ext-GDDH is hard.

3.4 Optimization

Our construction above using three-encodings can be improved to a double-encodings scheme. As far as I know, one cannot obtain useful information from the same numerators of encodings in different module. Namely, one can generate the public parameters

\[
\text{par} = \left\{ q_l, y_l, \left\{ x_{i,j} \right\}_{i \in [3]}, \left\{ p_{z,y} \right\}_{i \in [2]} \right\}, \quad \text{where} \quad y_1 = \left[ \frac{a_1 g_i + 1}{z_1} \right]_{q_l}, \quad x_{i,j} = \left[ \frac{a_{i,j} g_i}{z_1} \right]_{q_l},
\]

\[
y_2 = \left[ \frac{a_2 g_i + 1}{z_2} \right]_{q_l}, \quad x_{i,j} = \left[ \frac{a_{i,j} g_i}{z_2} \right]_{q_l}, \quad \text{and} \quad p_{z,y} = \left[ h_{i,z} z_0 + z_i^\kappa \left( h_i g_i^{-1}_{q_l} + h_2 g_i^{-1}_{q_l} \right) \right]_{q_l},
\]

\[
p_{z,y} = \left[ z_2^\kappa \left( h_{i,z} z_0 + h_2 g_2^{-1}_{q_l} \right) \right]_{q_l}.
\]

It is easy to verify that this variant with double-encodings is correct.

4 Cryptanalysis

In essence, the weak-DL attack [GGH13] is to compute a basis of the secret element \( g_i \) in the scheme. So, we give easily computable some quantities in our construction, and analyze possible attacks using these quantities.
4.1 Easily computable quantities

The encodings \( y_1, x_{1,i} \) in the public parameters are same as that of GGH13 for the ideal lattice \( \langle g_i \rangle \). However, the zero testing parameter \( z_{t_0} \), which is different from that of GGH13, is changed into

\[
\left( 1 + 1 + 1 \right) \left( 1 + 1 + 1 \right) = \frac{1}{q_0} \left( 1 + 1 + 1 \right) \left( 1 + 1 + 1 \right).
\]

As a result, the encodings \( x_{1,i} \) of zero for \( \langle g_i \rangle \) are not any more encoding of zero for \( \langle g_2 \rangle, \langle g_3 \rangle \). Moreover, we increase new random element \( z_{t_0} \in R_{q_0} \). On the one hand, although the non-zero plaintexts encoded by \( y_1, x_{1,i} \) are one-to-one corresponding to ones encoded by \( y_3, x_{3,i} \) for \( \langle g_3 \rangle \), they cannot be subtracted to obtain encoding of zero for \( \langle g_3 \rangle \). This is because: (1) \( z_{t_0} \) using as level number of encoding is not equal to \( z_{t_3} \); (2) the modulus \( q_1 \) 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 \( y_1, x_{1,i} \) for \( \langle g_3 \rangle \), one must switch from modulus \( q_1 \) to \( q_3 \) and use zero testing parameter \( p_{z,t,i} \). On the other hand, the numerators in \( y_1, x_{1,i} \) are same as ones in \( y_2, x_{2,j} \), 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 \( \left( u_{1}, u_{2}, u_{3} \right) \) with \( 1 \leq k < \kappa \), we can compute using \( \text{par} \) to get

\[
v = \left[ \frac{y_1}{q_1} \left( u_1 \cdot p_{z,t,1} \right) - \frac{y_2}{q_2} \left( u_2 \cdot p_{z,t,2} \right) - \frac{y_3}{q_3} \left( u_3 \cdot p_{z,t,3} \right) \right],
\]

where \( u_t = u_i \cdot (x_{1,t})^t \cdot (y_1)^{\kappa-k-t} \), \( t \in [3] \).

It is easy to see that \( v \) is not reduced modulo \( q_3 \). However, switching modulus destroys the structure of the ring element in \( \left[ u_1 \cdot (x_{1,t})^t \cdot (y_1)^{\kappa-k-t} \cdot p_{z,t,1} \right] \). 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 \( g_i = g_{i,1} g_{i,2} \). Given a level-1 encoding \( \left( u_1, u_2, u_3 \right) \) with \( u_i = \left[ \frac{w}{z_{t_i}} \right] \), determine if \( w \in \langle g_{i,1} \rangle \). Using \( v \), one cannot decide whether \( v \) belongs to \( \langle g_{i,1} \rangle \) regardless of \( w \in \langle g_{i,1} \rangle \). 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 \( A = (a_{i,j}) \in R^{m \times m} \), all encoded at level- \( k \), \( 1 \leq k < \kappa \) form a matrix \( T \), the DLIN problem is to distinguish between rank \( m \) and rank \( m-1 \) for \( A \). Based on the similar reason above, one cannot compute the rank of \( A \) 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 adaptively describe the concrete details of the first step as follows:

1. Let $\{q, y = [(1 + ag_i)/z], x_i = [(a, g_i)/z], i \in [2], p_{z_i} = [(hz^k)/g_i]_{q_i}\}$ be the public parameters of the GGH map. We generate special decodings $\{y^{(i)}, x^{(i)}, i = 1, 2\}$, where

$$y^{(1)} = \left[p_{z_1}y^{(1)}x^i_{x} \right]_{q_1} = h(1 + ag_i)\cdot a_i,$$

$$x^{(1)} = \left[p_{z_2}y^{(0)}x^i_{x} \right]_{q_2} = h(1 + ag_i)\cdot a_i, \quad i = 1, 2.$$

Notice that $y^{(1)}, x^{(1)}$ are not reduced modulo $q_i$.

2. Given a level-1 encoding $u$, we have $u = [dy + r_1x_1 + r_2x_2]_{q_3}$, where $d$ is a secret level-0 encoding, and $r_1, r_2$ random noise elements.

Compute special decoding $v = \left[p_{z_3}uy^{(2)}x^i_{x} \right]_{q_3} = dy^{(1)} + r_1x^{(1)} + r_2x^{(2)}$.

Since $v$ is not reduced modulo $q_3$, then compute $v \mod y^{(1)} = (r_1x^{(1)} \mod y^{(1)} + r_2x^{(2)} \mod y^{(1)}) \mod y^{(1)}$.

3. Given $v \mod y^{(1)}$ and $\{x^{(1)} \mod y^{(1)}, x^{(2)} \mod y^{(1)}\}$, we get $v' = v \mod y^{(1)} \in \{x^{(1)}, x^{(2)}\}$ such that $(v - v') \mod y^{(1)} = 0$. Let $v' = r_1x^{(1)} + r_2x^{(2)}$.

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

$$= d + ((r_1 - r_1)a_1 + (r_2 - r_2)a_2)g_i / (1 + ag_i).$$

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

4.2.2 Non-applicabiltiy of Hu-Jia Attack

(1) Let $\text{par} = \left\{\{q_i, y, \{x_{i,j}\}_{j=1}^3, p_{z_{i,j}}\}_{j=1}^3\right\}$ be the public parameters of our construction.

Similarly, we generate special decodings $S = \left\{y^{(i)}, \{x^{(i)}\}_{i=1}^3\right\}$ as follows:

$$y^{(1)} = \left[q_3 \cdot \left[u_{i,1} \cdot p_{z_{i,1}}\right]_{q_{i,1}} - \frac{q_3}{q_2} \cdot \left[u_{i,2} \cdot p_{z_{i,2}}\right]_{q_{i,2}} - \left[u_{i,3} \cdot p_{z_{i,3}}\right]_{q_{i,3}}\right]_{q_i},$$

where $u_{i,1} = [(y_i)^{-1} \cdot x_{i,1}]_{q_{i,1}}, \quad t \in [3].$

$$x^{(1)} = \left[q_3 \cdot \left[u_{i,1} \cdot p_{z_{i,1}}\right]_{q_{i,1}} - \frac{q_3}{q_2} \cdot \left[u_{i,2} \cdot p_{z_{i,2}}\right]_{q_{i,2}} - \left[u_{i,3} \cdot p_{z_{i,3}}\right]_{q_{i,3}}\right]_{q_i},$$

where $u_{i,1} = [(y_i)^{-1} \cdot x_{i,1}]_{q_{i,1}}, \quad t \in [3].$

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

14
(2) Given a level-1 encoding \((u_1', u_2', u_3')\) with \(u_i' = \left[ d \cdot y_i + \sum_{j=1}^{\tau} r_j \cdot x_{i,j} \right]_{q_i}, \ i \in [3]\), we compute special decoding
\[
v = \left[ \frac{g_{i,1}}{q_1} \left[ u_{1}' \cdot p_{2,1} \right]_{q_1} \right] - \left[ \frac{g_{i,2}}{q_2} \left[ u_{2}' \cdot p_{2,2} \right]_{q_2} \right] - \left[ u_{3}' \cdot p_{2,3} \right]_{q_3},
\]
where \(u_i' = (y_i)^{q_{i-2}} \cdot u_j \cdot x_{i,j}, \ i \in [3]\).

However, we observe that \(v \neq d \cdot y^{(i)} + \sum_{j=1}^{\tau} r_j \cdot x^{(i)}\). This is because the zero-testing parameters in our construction use random elements \(z_0, z\).

Although \(v\) is not reduced modulo \(q_3\), one cannot find an equivalent level-0 encoding encoded by \((u_1', u_2', u_3')\) using the Hu-Jia method. Because \(x^{(i)} \notin \langle g_i \rangle\) and the probability that \(y^{(i)}, x^{(i)}\) are co-prime is almost 1. Namely, \(y^{(i)}, x^{(i)}\) have not common factor. This is different from the case of the GGH map described by Hu and Jia [HJ15a]. Currently, we do not know how to efficiently solve \(d, r_j\) given \(y^{(i)}, x^{(i)}, v\) since \(v \neq d \cdot y^{(i)} + \sum_{j=1}^{\tau} r_j \cdot x^{(i)}\).

In fact, we observe that one cannot also find \(d, r_j\) even if \(y^{(i)}, x^{(i)}, v\) are not rounded when computing them. Because new random noise is introduced by using \(g_2, g_3, z_0, z\) and the factor \(g_1\) in \(v\) is destroyed.

Thus, one cannot find an equivalent level-0 encoding encoded by \((u_1', u_2', u_3')\). 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 \(\langle g_i \rangle\). The second step is to find the shortest vector of \(\langle g_i \rangle\) 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 \(\langle g_i \rangle\) 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 Cheon et al.’s attack [CHL+15], Coron et al. [CGH+15] extended this attack method to encodings more than a single monomial to get a zero. 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 \(z_0, z\) in \(p_{2,1}, p_{2,2}\), we generate a basis of \(g_1\) using the attack in [CGH+15] when taking \(z_0 = z = 0\).

By Corollary 3.8, we have \(a_i = \left[ g_{i,1} \cdot g_{1,1}^{-1} \right]_{q_i}\) and \(\|a_i\| < l_i(g_i) + \left\lfloor q_i / q_1 \right\rfloor\) for \(i \in \{2, 3\}\).

So, \(a_i\) is not reduced modulo \(q_j\).

Given an arbitrary level-\(k\) encoding \((u_1', u_2', u_3')\), one computes using zeroizing attack
\[
v_{k,i,j} = \left[ \frac{g_{i,1}}{q_1} \left[ u_{1}' \cdot p_{2,1} \right]_{q_1} \right] - \left[ \frac{g_{i,2}}{q_2} \left[ u_{2}' \cdot p_{2,2} \right]_{q_2} \right] - \left[ u_{3}' \cdot p_{2,3} \right]_{q_3},
\]
where \( u_t = \left[ y_t^{e-k-j} \cdot u^t \cdot x_{t,j}^i \right]_{q_t}, t \in \{ 3 \} \) with \( j \geq 1 \).

Note that \( q_j, q_1 \cdot \left[ u_1 \cdot p_{z,t,1} \right]_{q_1} \) and \( q_2, q_2 \cdot \left[ u_2 \cdot p_{z,t,2} \right]_{q_2} \) in \( v_{k,j,j} \) are not rounded to integers.

It is easy to see that \( v_{k,j,i} \) is not reduced modulo \( q_j \). Assume that \( t_k, t_q \), \( t_t, t_u \) and \( t_k, t_q \) are not rounded to integers.

Now, we can write \( v_{k,j,j} \) in matrix form:

\[
\begin{bmatrix}
q_1 \cdot s_{i,j} \cdot \rho_1 \\
- q_2 \cdot s_{i,j} \cdot \rho_2 \\
- s_{i,j} \cdot \rho_3
\end{bmatrix}
\]

where \( \rho_1 = \left( \frac{g_1 + h_1 + h_2}{g_1} \right), \rho_2 = \frac{h_2 + h_{2,0}}{g_2}, \rho_3 = \left( \frac{h_3 + h_{3,0}}{g_3} \right) \).

Since \( c_1 = c_2, s_{i,j} = s_{s,i} \) and \( d_1 = d_2 \), we transform \( v_{k,j,j} \) into the following form:

\[
\begin{bmatrix}
q_1 \cdot s_{i,j} \cdot \rho_1 \\
- q_2 \cdot s_{i,j} \cdot \rho_2 \\
- s_{i,j} \cdot \rho_3
\end{bmatrix}
\]

By the matrix form of \( v_{k,j,j} \) over the rational and \( s_{i,j} = b_{i,j}g_1 \), one can compute a basis of \( \langle g_1 \rangle \) by directly using the attack in [CGH+15].

However, the random ring elements \( z_{q_1} \in R_{q_1}, z_{q_2} \in R_{q_2} \) in \( p_{z,t,1} \cdot p_{z,t,2} \) 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 \( \text{par} \), the numerators in the encodings \( y_j, x_{i,j} \) are same as that in \( y_2, x_2, x_{j,2} \). Since they use different modulo, one cannot directly compute between these encodings. Given two encodings \( \left( u_{1,s}, u_{2,s}, u_{3,s} \right), s \in \{ 2 \} \) for our construction, we can obtain the following quantities:

\[
c_1 = \left[ u_{1,1} \cdot u_{1,2} \right]_{q_1} = \left[ \frac{r_1 g_1 + d_1}{r_1 g_1 + d_1} \right]_{q_1}, c_2 = \left[ u_{2,1} \cdot u_{2,2} \right]_{q_2} = \left[ \frac{r_1 g_1 + d_1}{r_1 g_1 + d_1} \right]_{q_2},
\]

where \( u_{t,s} = \left[ \frac{r_1 g_1 + d_1}{z_{q_t}} \right]_{q_t}, t \in \{ 2 \}, s \in \{ 2 \} \).

However, one cannot find \( r_1 g_1 + d_1 \) by using \( c_1, c_2 \). Since by Lemma 3.6, we have
\[
\begin{bmatrix}
q_2 \\
q_1
\end{bmatrix} c_i = \begin{bmatrix}
r_1 g_i + d_1
\end{bmatrix} \cdot \begin{bmatrix}
q_2 \\
q_1
\end{bmatrix} \begin{bmatrix}
1 \\
r_2 g_1 + d_2
\end{bmatrix} + \delta,
\]

where \( \|\delta\| < l(w) \) and \( \delta \neq 0 \).

Again, by
\[
\begin{bmatrix}
q_2 \\
q_1
\end{bmatrix} c_i \neq \begin{bmatrix}
1 \\
r_2 g_1 + d_2
\end{bmatrix},
\]

one cannot obtain useful information from
\[
\begin{bmatrix}
q_2 \\
q_1
\end{bmatrix} c_i
\]

and \( c_2 \).

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

5 Applications

Based on our new construction, we describe two applications: the one-round multipartite Diffie-Hellman key exchange protocol and witness encryption. Their security relies on the hardness assumption of the ext-GDDH.

5.1 MPKE Protocol

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

\textbf{Publish}(\text{par}, j). The \(j\)-th party samples \(d_j \leftarrow D_{\mathbb{Z}^*}, r_{j, \ell} \leftarrow D_{\mathbb{Z}^*}, i \in [\tau]\), publishes the public key \(u_{i,j} = \left[d_j \cdot y + \sum_{t=1}^{\tau} r_{j,t} \cdot x_{i,t}\right]_{q_1}, t \in [3]\) and remains \(d_j\) as the secret key.

\textbf{KeyGen}(\text{par}, j, d_j, \{u_{i,j}, u_{2,j}, u_{3,j}\})_{k_{x,j}}. The \(j\)-th party computes
\[
c_{i,j} = \prod_{k_{x,j}} u_{i,k} \quad , \quad t \in [3]
\]

and extracts the common secret key \(sk = \text{Ext}(\text{par}, [d_j c_{i,j}]_{q_1}, [d_j c_{2,j}]_{q_2}, [d_j c_{3,j}]_{q_3})\).

\textbf{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.

\textbf{3-Exact Cover Problem} [GGH13, Gol08] Given a collection \(\mathcal{S}\) of subsets \(T_1, T_2, \ldots, T_\pi\) of \([K] = \{1, 2, \ldots, K\}\) such that \(K = 3\theta\) and \(|T_\pi| = 3\), find a 3-exact cover of \([K]\). For an instance of witness encryption, the public key is a collection \(\mathcal{S}\) and the public parameters \(\text{par}\) in our construction, the secret key is a hidden 3-exact cover of \([K]\).
Encrypt($1^k$, par, $M$):

1. For $k \in \{K\}$, sample $d_k \leftarrow D_{2^\alpha_1 \sigma_1}$, $r_k \leftarrow D_{2^\alpha_2 \sigma_2}$, $i \in \{\tau\}$ and generate level-1 encodings $u_{i,k} = \left[d_k \cdot y + \sum_{i=1}^{\tau} r_{k,i} \cdot x_{i,j}\right]_{q_i}$, $t \in [3]$.

2. Compute $u_i = \left[\prod_{k=1}^{K} u_{i,k}\right]_{q_i}$, $t \in [3]$ and $sk = \text{Ext}(\text{par}, (u_1, u_2, u_3))$, and encrypt a message $M$ into ciphertext $C$.

3. For each element $T_j = \{j_1, j_2, j_3\} \in \text{Set}$, sample $r_{T_j,i} \leftarrow D_{2^\alpha_3 \sigma_3}$, $i \in \{\tau\}$, and generate a level-3 encoding $u_{i,T_j} = \left[u_{i,j_1}u_{i,j_2}u_{i,j_3} + \sum_{i=1}^{\tau} r_{T_j,i}(x_{i,j})^3\right]_{q_i}$, $t \in [3]$.

4. Output the ciphertext $C$ and all level-3 encodings $E = \{(u_{i,T_j}, u_{2,T_j}, u_{3,T_j}) | T_j \in \text{Set}\}$.

Decrypt($C, E, W$):

1. Given $C, E$ and a witness set $W$, compute $u_i = \left[\prod_{T_j \in W} u_{i,T_j}\right]_{q_i}$, $t \in [3]$.

2. Generate $sk = \text{Ext}(\text{par}, (u_1, u_2, u_3))$, 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 $u_{i,T_j} = \left[u_{i,j_1}u_{i,j_2}u_{i,j_3} + \sum_{i=1}^{\tau} r_{T_j,i}(x_{i,j})^3\right]_{q_i}$, $t \in [3]$ is a level-3 encoding in our encoding method, one cannot obtain $u_{i,T_j} = \left[u_{i,T_j}u_{i,T_j}^{-1}\right]_{q_i}$ when $T_j = T_j \cup T_k - T_j$. 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 three 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


[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.


