Multilinear Maps Using Random Matrix

Preliminary Report

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

July 17, 2015

Abstract. Garg, Gentry and Halevi (GGH) described the first candidate multilinear maps using ideal lattices. However, Hu and Jia presented an efficient attack on GGH map, which breaks the GGH-based applications of multipartite key exchange (MPKE) and witness encryption (WE) based on the hardness of 3-exact cover problem. We describe a new construction of multilinear map using random matrix, which supports the applications for public tools of encoding in the origin GGH, such as MPKE and WE. The security of our construction depends upon new hardness assumption. Furthermore, our construction removes the special structure of the ring element in the principal ideal lattice problem, and avoids potential attacks generated by algorithm of solving short principal ideal lattice generator.
Keywords. Multilinear maps, Ideal lattices, Multipartite Diffie-Hellman key exchange, Witness encryption, Zeroizing attack

1 Introduction

Constructing cryptographic multilinear map is a long-standing open problem [BS03]. It has many applications, such as witness encryption [GGS+13], general program obfuscation [GGH+13b, Zim15], function encryption [GGH+13b], and other applications [GGH+13a, BZ14]. Garg, Gentry, and Halevi (GGH) proposed the first candidate construction of multilinear maps from ideal lattices [GGH13]. GGHLite [LSS14] is an efficient improvement version of GGH map. Using same framework of the GGH map, Coron, Lepoint, and Tibouchi [CLT13] (CLT) presented a construction over the integers. Gentry, Gorbunov and Halevi [GGH15] constructed graph-induced multilinear maps from lattices.

The attacks for CLT and GGH demonstrate that the security of current constructions requires further deep cryptanalysis. On the one hand, Cheon, Han, Lee, Ryu, and Stehle recently broke the CLT construction using zeroizing attack introduced by Garg, Gentry, and Halevi. To fix the CLT construction, Garg, Gentry, Halevi and Zhandry [GGH+14], and Boneh, Wu and Zimmerman [BWZ14] presented two candidate fixes of multilinear maps over the integers. However, Coron, Lepoint, and Tibouchi showed that two candidate fixes of CLT can also be defeated using extensions of the Cheon et al.'s Attack [CHL+14]. By modifying zero-testing parameter, Coron, Lepoint and Tibouchi [CLT15] proposed a new construction of multilinear map over the integers. On the other hand, Hu and Jia [HJ15a] very recently presented an efficient attack on the GGH map, which breaks the GGH-based applications on multipartite key exchange (MPKE) and witness encryption (WE) based on the hardness of 3-exact cover problem. The Cheon and Lee [CL15] proposed an attack for the GGH map by computing a basis of secret ideal lattice.

Gu (Gu map-1) [Gu15] presented a construction of multilinear maps without encodings of zero, which is an improvement of GGH map. Since no encodings of zero are given in the public parameters, MPKE based on Gu map-1 [HJ15c] successfully avoids the attack in [HJ15a]. However, Gu map-1 cannot be used for the instance of witness encryption based on the hardness of 3-exact cover problem [HJ15b]. This is because there is no randomizer in Gu map-1. But the instance of WE based on the hardness of 3-exact cover problem is a strong application of multilinear map. Thus, there is a strong demand to construct scheme with randomizer.

Our results. Our main contribution is to construct a new multilinear map using random matrix. Our construction improves the GGH map in three aspects.

(1) We modify the zero-testing parameter of GGH from $\mathbf{p}_{zt} = \left[\mathbf{z}^{\kappa}\mathbf{h}/\mathbf{g}\right]_q$ to

$\mathbf{P}_{zt} = \left[\mathbf{T}Rot(\mathbf{z}^{\kappa}\mathbf{h}/\mathbf{g})\mathbf{S}\right]_q$ by using random matrix $\mathbf{T},\mathbf{S} \in \mathbb{Z}_q^{n\times n}$, where $Rot(\mathbf{r})$ is the anti-cycle matrix of $\mathbf{r}$. Since the level-1 encodings and level-0 encodings are multiplied by different matrices, they cannot be directly multiplied, and must use zero-testing matrix $\mathbf{P}_{zt}$ as intermediate element to multiply them together. As a result of using random matrix, our construction thwarts the revelation of the secret parameters.

(2) We transform the final result into a non-square matrix to damage the structure of ring elements between random matrices and further avoid the principal ideal lattice problem. Although one merely can get the final result of the form $\mathbf{V} = \left[\mathbf{T}Rot(\mathbf{r}\mathbf{g}^k)\mathbf{S}\right]_q$ with $0 \le k < \kappa$, the structure and some secret information of $\mathbf{g}$ still remain in $\mathbf{V}$. To remove this weakness, we choose another two matrics $\mathbf{T}_0 \leftarrow D_{\mathbb{Z}^{k_1\times n},\sigma}$, $\mathbf{S}_0 \leftarrow D_{\mathbb{Z}^{n\times k_2},\sigma}$ with $k_1k_2 < n$ and set $\mathbf{T}^* = \mathbf{T}_0\mathbf{T}^{-1}$, $\mathbf{S}^* = \mathbf{S}^{-1}\mathbf{S}_0$. Now, we must multiply $\mathbf{T}^*$ and $\mathbf{S}^*$ in both sides of $\mathbf{V}$ to obtain the non-reduced matrix over modulus q. That is, we get the matrix $\mathbf{V}_0 = \mathbf{T}_0Rot(\mathbf{r}\mathbf{g}^k)\mathbf{S}_0$. Notably, $\mathbf{V}_0$ is an $k_1 \times k_2$ -matrix, and does not have the structure of the ring element $\mathbf{r}\mathbf{g}^k$. However, using a variant of Cheon et al. attack, one can also obtain some secret information of $\mathbf{g}$. To avoid this problem, we use two zero-testing parameters to introduce new noise term and really destroy the structure of ring element. Owing to this reason, we can give encodings of zero in the public parameters. Thus, our construction supports the applications using GGH as public tools of encoding, and removes the weakness of the principal ideal lattices problem in GGH.

(3) By using composite-order ideal lattice, our construction can have more applications than GGH [GGH13]. Owing to destroying the structure of ring element, we conjecture that the membership group problem (SubM) and the decisional linear (DLIN) problem are hard in our construction. Thus, we can use composite-order ideal lattice in our construction to support the applications based on the SubM problem and the DLIN problem. However, in the GGH map, one can compute non-reduced ring elements over modulus q and basis of some secret ring elements. As a result, the SubM problem and the DLIN problem are easy in the GGH map.

Our second contribution is to describe the applications of MPKE and WE using our multilinear map. Since these applications are attacked by [HJ15a], fix for them is urgently required. The constructions of MPKE and WE based on our new map are same as ones using GGH. However, different from GGH, the security of our construction depends on new hard assumption.

Organization. We first recall some background in Section 2. Then we describe symmetric construction in Section 3, commutative variant and asymmetric variant in Section 4. Finally, we present two applications of MPKE and WE using our construction in Section 5, and draw conclusion in Section 6.

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 $\mathbf{A},\mathbf{B},\mathbf{C}$. Let $\mathbf{I}$ be the identity matrix. 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 $\mathbb{Z}[X]/<x^n+1>$ 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 $[\mathbf{a}]_q$ 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 $\sum_{i=1}^{n} x_i \mathbf{b}_i$ 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 $L = \left\{\mathbf{Bz} : \mathbf{z} \in Z^n\right\}$. We say that $\mathbf{B}$ spans L if $\mathbf{B}$ is a basis for L. Given a basis $\mathbf{B}$ of L, we define $P(\mathbf{B}) = \{\mathbf{Bz} \mid \mathbf{z} \in \mathbb{R}^n, \forall i : -1/2 \le z_i < 1/2\}$ as the parallelization corresponding to $\mathbf{B}$. Let $\det(\mathbf{B})$ denote the determinant of $\mathbf{B}$.

Given $\mathbf{g} \in R$, let $I = <\mathbf{g}>$ be the principal ideal 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 $\left\{g_j \in G_j\right\}_{j=1,...,\kappa}$, 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 $\left\{g_j \in G_j\right\}_{j=1,...,\kappa}$ 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 $S = \left\{S_j^{(\alpha)} \subset R : \alpha \in R, j \in [\![\kappa]\!]\right\}$ with the following properties:

(1) For every index $j \in [\![\kappa]\!]$, the sets $\left\{S_j^{(\alpha)} : \alpha \in R\right\}$ 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 Construction using random matrix

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 $\sigma = \sqrt{\lambda n}$, $\sigma' = \lambda n^{1.5}$, $\sigma^* = 2^{\lambda}$, $q \ge 2^{16\kappa\lambda} n^{O(\kappa)}$, $m = 2$, $n > \widetilde{O}(\kappa\lambda^2)$, $\tau = O(n^2)$, $\rho = O(n)$, $k_1 = O(\log n)$, $k_2 = O(\log n)$ such that $k_1 k_2 \le n - O(\lambda)$.

3.1 Construction

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

(1) Choose a prime $q \ge 2^{16\kappa\lambda} n^{O(\kappa)}$.

(2) Sample $\mathbf{g}_j \leftarrow D_{\mathbb{Z}^n,\sqrt{\sigma}}$, $\mathbf{h}_j \leftarrow D_{\mathbb{Z}^n,\sqrt{q}}$, $j \in [\![m]\!]$ in R, and set $\mathbf{g} = \prod_{j=1}^{m} \mathbf{g}_j$ so that $\mathbf{g}_j$, $j \in [\![m]\!]$ are pairwise relatively prime and $\left\|\mathbf{g}_j^{-1}\right\| \le n$.

(3) Sample $\mathbf{f} \leftarrow D_{\mathbb{Z}^n,\sqrt{\sigma}}$, $\mathbf{h} \leftarrow D_{\mathbb{Z}^n,\sqrt{q}}$ in R so that $\left\|\mathbf{f}^{-1}\right\| \le n$.

(4) For $t \in [\![2]\!]$, choose $\mathbf{a}_{t,i}, \mathbf{b}_{t,i} \leftarrow D_{\mathbb{Z}^n,\sigma'}$, $i \in [\![\tau]\!]$, and $\mathbf{q}_{t,\delta} \leftarrow D_{\mathbb{Z}^n,\sigma'}$, $\delta \in [\![\rho]\!]$ in R.

(5) Choose $\mathbf{e}_{1,i} \leftarrow D_{\mathbb{Z}^n,\sigma'}$, $i \in [\![\tau]\!]$ in R.

(6) Set $\mathbf{e}_{2,i} = (\mathbf{a}_{1,i}\mathbf{g} + \mathbf{e}_{1,i}) \bmod \mathbf{f}$, $\mathbf{v}_{2,i} = (\mathbf{q}_{1,\delta}\mathbf{g}) \bmod \mathbf{f}$, and $\mathbf{w}_{2,i} = (\mathbf{b}_{1,i}\mathbf{g} + \mathbf{e}_{1,i}) \bmod \mathbf{f}$.

That is, $\mathbf{a}_{1,i}\mathbf{g} + \mathbf{e}_{1,i} = \mathbf{r}_{1,i}\mathbf{f} + \mathbf{e}_{2,i}$, $\mathbf{q}_{1,\delta}\mathbf{g} = \mathbf{r}_{2,\delta}\mathbf{f} + \mathbf{v}_{2,\delta}$, and $\mathbf{b}_{1,i}\mathbf{g} + \mathbf{e}_{1,i} = \mathbf{r}_{3,i}\mathbf{f} + \mathbf{w}_{2,i}$.

(7) Choose a random element $\mathbf{z}_t \leftarrow R_q$ so that $\mathbf{z}_t^{-1} \in R_q$, $t \in [\![2]\!]$.

(8) Choose randomly matrices $\mathbf{T}_t, \mathbf{S}_t \in \mathbb{Z}_q^{n\times n}$ so that $\mathbf{T}_t^{-1}, \mathbf{S}_t^{-1} \in \mathbb{Z}_q^{n\times n}$, $t \in [\![2]\!]$.

(9) Choose randomly matrices $\mathbf{T}_0 \leftarrow D_{\mathbb{Z}^{k_1\times n},\sigma}$, $\mathbf{S}_0 \leftarrow D_{\mathbb{Z}^{n\times k_2},\sigma}$.

(10) For $t \in [\![2]\!]$, set $\mathbf{T}_t^* = \mathbf{T}_0\mathbf{T}_t^{-1}$, $\mathbf{S}_t^* = \mathbf{S}_t^{-1}\mathbf{S}_0$.

(11) For $i \in [\![\tau]\!]$ and $\delta \in [\![\rho]\!]$, set

$$\mathbf{Y}_{1,i} = \left[\mathbf{T}_1 Rot(\frac{\mathbf{a}_{1,i}\mathbf{g} + \mathbf{e}_{1,i}}{\mathbf{z}_1})\mathbf{T}_1^{-1}\right]_q, \quad \mathbf{Q}_{1,\delta} = \left[\mathbf{T}_1 Rot\left(\frac{\mathbf{q}_{1,\delta}\mathbf{g}}{\mathbf{z}_1}\right)\mathbf{T}_1^{-1}\right]_q, \text{ and}$$

$$\mathbf{X}_{1,i} = \left[\mathbf{S}_1^{-1} Rot(\mathbf{b}_{1,i}\mathbf{g} + \mathbf{e}_{1,i})\mathbf{S}_1\right]_q;$$

$$\mathbf{Y}_{2,i} = \left[\mathbf{T}_2 Rot(\frac{\mathbf{a}_{2,i}\mathbf{f} + \mathbf{e}_{2,i}}{\mathbf{z}_2})\mathbf{T}_2^{-1}\right]_q, \quad \mathbf{Q}_{2,\delta} = \left[\mathbf{T}_2 Rot(\frac{\mathbf{q}_{2,\delta}\mathbf{f} + \mathbf{v}_{2,\delta}}{\mathbf{z}_2})\mathbf{T}_2^{-1}\right]_q, \text{ and}$$

$$\mathbf{X}_{2,i} = \left[\mathbf{S}_2^{-1} Rot(\mathbf{b}_{2,i}\mathbf{f} + \mathbf{w}_{2,i})\mathbf{S}_2\right]_q.$$

(12) Set $\mathbf{P}_{zt,1} = \left[\mathbf{T}_1 Rot\left(\mathbf{z}_1^{\kappa}\left(\sum_{j=1}^{m}\mathbf{h}_j\mathbf{g}_j^{-1} + \mathbf{h}\mathbf{f}^{-1}\right)\right)\mathbf{S}_1\right]_q$, $\mathbf{P}_{zt,2} = \left[\mathbf{T}_2 Rot\left(\mathbf{z}_2^{\kappa}\mathbf{h}\mathbf{f}^{-1}\right)\mathbf{S}_2\right]_q$;

(13) Output the public parameters

$$\text{par} = \left\{q, \left\{\left\{\mathbf{Y}_{t,i}, \mathbf{X}_{t,i}\right\}_{i\in[\![\tau]\!]}, \left\{\mathbf{Q}_{t,\delta}\right\}_{\delta\in[\![\rho]\!]}, \mathbf{P}_{zt,t}, \mathbf{T}_t^*, \mathbf{S}_t^*\right\}_{t\in[\![2]\!]}\right\}.$$

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

Given $\mathbf{d} \leftarrow D_{\mathbb{Z}^{\tau},\sigma^*}$ and $\mathbf{r} \leftarrow D_{\mathbb{Z}^{\rho},\sigma^*}$, set $\mathbf{U}_t = \left[\sum_{i=1}^{\tau} d_i \cdot (\mathbf{Y}_{t,i})^k + \sum_{\delta=1}^{\rho} r_{\delta} \cdot (\mathbf{Q}_{t,\delta})^k\right]_q$, and $\mathbf{E}_t = \left[\sum_{i=1}^{\tau} d_i \cdot (\mathbf{X}_{t,i})^k\right]_q$ for $t \in [\![2]\!]$.

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

Given s level-k encodings $(\mathbf{U}_{1,l}, \mathbf{U}_{2,l})$, set $\mathbf{U}_t = \left[\sum_{l=1}^{s} \mathbf{U}_{t,l}\right]_q$ for $t \in [\![2]\!]$.

Multiplying encodings: $(\mathbf{U}_1, \mathbf{U}_2) \leftarrow \mathrm{Mul}\left(\mathrm{par}, k, (\mathbf{U}_{1,1}, \mathbf{U}_{2,1}), \cdots, (\mathbf{U}_{1,s}, \mathbf{U}_{2,s})\right)$.

Given k level-1 encodings $(\mathbf{U}_{1,l}, \mathbf{U}_{2,l})$, set $\mathbf{U}_t = \left[\prod_{l=1}^{k} \mathbf{U}_{t,l}\right]_q$.

Zero testing: $\mathrm{isZero}\left(\mathrm{par}, (\mathbf{U}_1, \mathbf{U}_2), \mathbf{d}\right)$.

(1) Given $\mathbf{d}$, we compute $\mathbf{E}_1 = \left[\sum_{i=1}^{\tau} d_i \cdot \mathbf{X}_{1,i}\right]_q$ and $\mathbf{E}_2 = \left[\sum_{i=1}^{\tau} d_i \cdot \mathbf{X}_{2,i}\right]_q$.

(2) Given a level-κ encoding $(\mathbf{U}_1, \mathbf{U}_2)$, to determine whether $\mathbf{U}_1$ is a level-κ encoding of zero for $\mathbf{g}$, we compute an extraction encoding for $\mathbf{g}$ as follows:

$$\mathbf{V} = \left[\mathbf{T}_1^* \cdot \mathbf{U}_1 \cdot \mathbf{P}_{zt,1} \cdot \mathbf{E}_1 \cdot \mathbf{S}_1^* - \mathbf{T}_2^* \cdot \mathbf{U}_2 \cdot \mathbf{P}_{zt,2} \cdot \mathbf{E}_2 \cdot \mathbf{S}_2^*\right]_q.$$

(3) We check whether $\|\mathbf{V}\|$ is short:

$$\mathrm{isZero}\left(\mathrm{par}, (\mathbf{U}_1, \mathbf{U}_2), \mathbf{d}\right) = \begin{cases} 1 & \text{if } \|\mathbf{V}\| < q^{3/4} \\ 0 & \text{otherwise} \end{cases}.$$

Extraction: $sk \leftarrow \mathrm{Ext}\left(\mathrm{par}, (\mathbf{U}_1, \mathbf{U}_2), \mathbf{d}\right)$.

(1) Given $\mathbf{d}$, we compute $\mathbf{E}_1 = \left[\sum_{i=1}^{\tau} d_i \cdot \mathbf{X}_{1,i}\right]_q$ and $\mathbf{E}_2 = \left[\sum_{i=1}^{\tau} d_i \cdot \mathbf{X}_{2,i}\right]_q$.

(2) Given a level-κ encoding $(\mathbf{U}_1, \mathbf{U}_2)$, we compute an extraction encoding for $\mathbf{g}$ as follows:

$$\mathbf{V} = \left[\mathbf{T}_1^* \cdot \mathbf{U}_1 \cdot \mathbf{P}_{zt,1} \cdot \mathbf{E}_1 \cdot \mathbf{S}_1^* - \mathbf{T}_2^* \cdot \mathbf{U}_2 \cdot \mathbf{P}_{zt,2} \cdot \mathbf{E}_2 \cdot \mathbf{S}_2^*\right]_q.$$

(3) We collect $(\log q)/4 - \lambda$ most-significant bits of each of the $k_1 \times k_2$ -matrix $\mathbf{V}$:

$$\mathrm{Ext}\left(\mathrm{par}, (\mathbf{U}_1, \mathbf{U}_2), \mathbf{d}\right) = \mathrm{Extract}\left(\mathrm{msb}_\eta(\mathbf{V})\right).$$

Remark 3.1 (1) To generate a level-l encoding of a given plaintext, one can provide the level-l encoding and level-0 encoding in the public parameters for plaintext x^j, $j = 0, \ldots, n-1$ as follows:

$$\mathbf{Y}_{1,j} = \left[\mathbf{T}_1 Rot\left(\frac{\mathbf{a}_{1,j}\mathbf{g} + x^j}{\mathbf{z}_1}\right)\mathbf{T}_1^{-1}\right]_q \text{ and } \mathbf{X}_{1,j} = \left[\mathbf{S}_1^{-1} Rot(\mathbf{b}_{1,j}\mathbf{g} + x^j)\mathbf{S}_1\right]_q.$$

Given a plaintext $\mathbf{d} \leftarrow D_{\mathbb{Z}^n, \sigma^*}$, we can generate its level-1 encoding $\mathbf{U}_1 = \left[\sum_{j=1}^{n} d_j \mathbf{Y}_{1,j} + \sum_{\delta=1}^{\rho} r_\delta \cdot (\mathbf{Q}_{1,\delta})\right]_q$, where $\mathbf{r} \leftarrow D_{\mathbb{Z}^\rho, \sigma^*}$, and its level-0 encoding $\mathbf{E}_1 = \left[\sum_{j=1}^{n} d_j \mathbf{X}_{1,j}\right]_q$.

In this case, we need also to generate $\mathbf{Y}_{2,j}$ and $\mathbf{X}_{2,j}$ corresponding to $\mathbf{Y}_{1,j}$ and $\mathbf{X}_{1,j}$.

(2) Although we randomly choose the matrices $\mathbf{T}_t, \mathbf{S}_t \in \mathbb{Z}_q^{n \times n}$, $t \in [\![2]\!]$, we still use the element $\mathbf{z}_t$ to control the level number of encoding.

(3) The composite-order element $\mathbf{g}$ is to support the applications based on the SubM problem and the DLIN problem.

(4) Using $\mathbf{d}$ in the zero-testing and the extraction algorithm is to describe the security of our

construction and present the MPKE protocol.

(5) The level-1 encodings of zero in the public parameters are to construct an instance of witness encryption.

(6) We set $k = k_1 \times k_2 \le n - O(\lambda)$. Notably, k_1, k_2 may be set 1. Because n is the dimension of ring element, our aim is to compress n free variables of the ring element to k variables, and breakdown the structure of the ring element in the principal ideal lattice problem.

(7) One can sample $\mathbf{h}_j \leftarrow D_{\mathbb{Z}^n,\sigma^*}$ instead of $\mathbf{h}_j \leftarrow D_{\mathbb{Z}^n,\sqrt{q}}$ since $\mathbf{P}_{zt}$ cannot be squared.

(8) The number τ of level-1 encodings of non-zero in the public parameters can be set to $O(\lambda n)$ according to the result in [HJ15c].

3.2 Correctness

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

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

Proof. (1) For $\mathbf{g}$, the encoding $\mathbf{U}_1$ is a level-k encoding, and the plaintext encoded by $\mathbf{U}_1$ is identical to the plaintext encoded by $\mathbf{E}_1$.

By $(\mathbf{Y}_{1,i})^k = \left[\mathbf{T}_1 Rot(\frac{\mathbf{a}_{1,i}\mathbf{g} + \mathbf{e}_{1,i}}{\mathbf{z}_1})^k \mathbf{T}_1^{-1} \right]_q$ and $(\mathbf{Q}_{1,\delta})^k = \left[\mathbf{T}_1 Rot(\frac{\mathbf{q}_{1,\delta}\mathbf{g}}{\mathbf{z}_1})^k \mathbf{T}_1^{-1} \right]_q$, we have

$$\begin{aligned}
\mathbf{U}_1 &= \left[\sum_{i=1}^{\tau} d_i \cdot (\mathbf{Y}_{1,i})^k + \sum_{\delta=1}^{\rho} r_\delta \cdot (\mathbf{Q}_{1,\delta})^k \right]_q \\
&= \left[\mathbf{T}_1 Rot(\frac{\sum_{i=1}^{\tau} d_i \mathbf{a}'_{1,i}\mathbf{g} + \sum_{\delta=1}^{\rho} r_\delta \mathbf{q}'_{1,\delta}\mathbf{g} + \sum_{i=1}^{\tau} d_i (\mathbf{e}_{1,i})^k}{\mathbf{z}_1^k}) \mathbf{T}_1^{-1} \right]_q, \\
&= \left[\mathbf{T}_1 Rot(\frac{\mathbf{a}_1\mathbf{g} + \mathbf{e}_1}{\mathbf{z}_1^k}) \mathbf{T}_1^{-1} \right]_q
\end{aligned}$$

where $\mathbf{a}'_{1,i} = ((\mathbf{a}_{1,i}\mathbf{g} + \mathbf{e}_{1,i})^k - (\mathbf{e}_{1,i})^k)/\mathbf{g}$, $\mathbf{q}'_{1,\delta} = (\mathbf{q}_{1,\delta}\mathbf{g})^k/\mathbf{g}$, $\mathbf{a}_1 = \sum_{i=1}^{\tau} d_i \cdot \mathbf{a}'_{1,i} + \sum_{\delta=1}^{\rho} r_\delta \mathbf{q}'_{1,\delta}$, and $\mathbf{e}_1 = \sum_{i=1}^{\tau} d_i \cdot (\mathbf{e}_{1,i})^k$.

By using $(\mathbf{X}_{1,i})^k = \left[\mathbf{S}_1^{-1} Rot(\mathbf{b}_{1,i}\mathbf{g} + \mathbf{e}_{1,i})^k \mathbf{S}_1 \right]_q$, we have

$$\begin{aligned}
\mathbf{E}_1 &= \left[\sum_{i=1}^{\tau} d_i \cdot (\mathbf{X}_{1,i})^k \right]_q \\
&= \left[\mathbf{S}_1^{-1} Rot(\sum_{i=1}^{\tau} d_i \mathbf{b}'_{1,i}\mathbf{g} + \sum_{i=1}^{\tau} d_i (\mathbf{e}_{1,i})^k) \mathbf{S}_1 \right]_q, \\
&= \left[\mathbf{S}_1^{-1} Rot(\mathbf{b}_1\mathbf{g} + \mathbf{e}_1) \mathbf{S}_1 \right]_q
\end{aligned}$$

where $\mathbf{b}'_{1,i} = ((\mathbf{b}_{1,i}\mathbf{g} + \mathbf{e}_{1,i})^k - (\mathbf{e}_{1,i})^k)/\mathbf{g}$, $\mathbf{b}_1 = \sum_{i=1}^{\tau} d_i \cdot \mathbf{b}'_{1,i}$, and $\mathbf{e}_1 = \sum_{i=1}^{\tau} d_i \cdot (\mathbf{e}_{1,i})^k$.

(2) For $\mathbf{f}$, the plaintext of $\mathbf{U}_1$ is same as the plaintext of $\mathbf{U}_2$; the plaintext in $\mathbf{E}_1$ is similar to the plaintext in $\mathbf{E}_2$.

By using $\mathbf{a}_{1,i}\mathbf{g} + \mathbf{e}_{1,i} = \mathbf{r}_{1,i}\mathbf{f} + \mathbf{e}_{2,i}$ and $\mathbf{q}_{1,\delta}\mathbf{g} = \mathbf{r}_{2,\delta}\mathbf{f} + \mathbf{v}_{2,\delta}$, we get

$$\mathbf{U}_1=\left[\sum_{i=1}^{\tau}d_i\cdot(\mathbf{Y}_{1,i})^k+\sum_{\delta=1}^{\rho}r_\delta\cdot(\mathbf{Q}_{1,\delta})^k\right]_q$$
$$=\left[\sum_{i=1}^{\tau}d_i\cdot\mathbf{T}_1Rot(\frac{\mathbf{r}_{1,i}\mathbf{f}+\mathbf{e}_{2,i}}{\mathbf{z}_1})^k\mathbf{T}_1^{-1}+\sum_{\delta=1}^{\rho}r_\delta\cdot\mathbf{T}_1Rot(\frac{\mathbf{r}_{2,\delta}\mathbf{f}+\mathbf{v}_{2,\delta}}{\mathbf{z}_1})^k\mathbf{T}_1^{-1}\right]_q$$
$$=\left[\mathbf{T}_1Rot(\frac{\sum_{i=1}^{\tau}d_i\mathbf{r}'_{1,i}\mathbf{f}+\sum_{\delta=1}^{\rho}r_\delta\mathbf{r}'_{2,\delta}\mathbf{f}+\sum_{i=1}^{\tau}d_i(\mathbf{e}_{2,i})^k+\sum_{\delta=1}^{\rho}r_\delta(\mathbf{v}_{2,\delta})^k}{\mathbf{z}_1^k})\mathbf{T}_1^{-1}\right]_q,$$
$$=\left[\mathbf{T}_1Rot(\frac{\mathbf{r}_1\mathbf{f}+\mathbf{e}_2}{\mathbf{z}_1^k})\mathbf{T}_1^{-1}\right]_q$$
where $\mathbf{r}'_{1,i}=((\mathbf{r}_{1,i}\mathbf{f}+\mathbf{e}_{2,i})^k-(\mathbf{e}_{2,i})^k)/\mathbf{f}$, $\mathbf{r}'_{2,\delta}=((\mathbf{r}_{2,\delta}\mathbf{f}+\mathbf{v}_{2,\delta})^k-(\mathbf{v}_{2,\delta})^k)/\mathbf{f}$, $\mathbf{r}_1=\sum_{i=1}^{\tau}d_i\cdot\mathbf{r}'_{1,i}+\sum_{\delta=1}^{\rho}r_\delta\mathbf{r}'_{2,\delta}$, and $\mathbf{e}_2=\sum_{i=1}^{\tau}d_i\cdot(\mathbf{e}_{2,i})^k+\sum_{\delta=1}^{\rho}r_\delta(\mathbf{v}_{2,\delta})^k$.

$$\mathbf{U}_2=\left[\sum_{i=1}^{\tau}d_i\cdot(\mathbf{Y}_{2,i})^k+\sum_{\delta=1}^{\rho}r_\delta\cdot(\mathbf{Q}_{2,\delta})^k\right]_q$$
$$=\left[\sum_{i=1}^{\tau}d_i\cdot\mathbf{T}_2Rot(\frac{\mathbf{a}_{2,i}\mathbf{f}+\mathbf{e}_{2,i}}{\mathbf{z}_2})^k\mathbf{T}_2^{-1}+\sum_{\delta=1}^{\rho}r_\delta\cdot\mathbf{T}_2Rot(\frac{\mathbf{q}_{2,\delta}\mathbf{f}+\mathbf{v}_{2,\delta}}{\mathbf{z}_2})^k\mathbf{T}_2^{-1}\right]_q,$$
$$=\left[\mathbf{T}_2Rot(\frac{\mathbf{a}_2\mathbf{f}+\mathbf{e}_2}{\mathbf{z}_2^k})\mathbf{T}_2^{-1}\right]_q$$
where $\mathbf{a}'_{2,i}=((\mathbf{a}_{2,i}\mathbf{f}+\mathbf{e}_{2,i})^k-(\mathbf{e}_{2,i})^k)/\mathbf{f}$, $\mathbf{q}'_{2,\delta}=((\mathbf{q}_{2,\delta}\mathbf{f}+\mathbf{v}_{2,\delta})^k-(\mathbf{v}_{2,\delta})^k)/\mathbf{f}$, $\mathbf{a}_2=\sum_{i=1}^{\tau}d_i\cdot\mathbf{a}'_{2,i}+\sum_{\delta=1}^{\rho}r_\delta\mathbf{q}'_{2,\delta}$, and $\mathbf{e}_2=\sum_{i=1}^{\tau}d_i\cdot(\mathbf{e}_{2,i})^k+\sum_{\delta=1}^{\rho}r_\delta(\mathbf{v}_{2,\delta})^k$.

Again using $\mathbf{b}_{1,i}\mathbf{g}+\mathbf{e}_{1,i}=\mathbf{r}_{3,i}\mathbf{f}+\mathbf{w}_{2,i}$, we obtain

$$\mathbf{E}_1=\left[\sum_{i=1}^{\tau}d_i\cdot(\mathbf{X}_{1,i})^k\right]_q$$
$$=\left[\mathbf{S}_1^{-1}Rot(\sum_{i=1}^{\tau}d_i\mathbf{r}'_{3,i}\mathbf{f}+\sum_{i=1}^{\tau}d_i(\mathbf{w}_{2,i})^k)\mathbf{S}_1\right]_q,$$
$$=\left[\mathbf{S}_1^{-1}Rot(\mathbf{r}_3\mathbf{f}+\mathbf{w}_2)\mathbf{S}_1\right]_q$$
where $\mathbf{r}'_{3,i}=((\mathbf{r}_{3,i}\mathbf{f}+\mathbf{w}_{2,i})^k-(\mathbf{w}_{2,i})^k)/\mathbf{f}$, $\mathbf{r}_3=\sum_{i=1}^{\tau}d_i\cdot\mathbf{r}'_{3,i}$, and $\mathbf{w}_2=\sum_{i=1}^{\tau}d_i\cdot(\mathbf{w}_{2,i})^k$.

$$\mathbf{E}_2=\left[\sum_{i=1}^{\tau}d_i\cdot(\mathbf{X}_{2,i})^k\right]_q$$
$$=\left[\mathbf{S}_2^{-1}Rot(\sum_{i=1}^{\tau}d_i\mathbf{b}'_{2,i}\mathbf{f}+\sum_{i=1}^{\tau}d_i(\mathbf{w}_{2,i})^k)\mathbf{S}_2\right]_q,$$
$$=\left[\mathbf{S}_2^{-1}Rot(\mathbf{b}_2\mathbf{f}+\mathbf{w}_2)\mathbf{S}_2\right]_q$$
where $\mathbf{b}'_{2,i}=((\mathbf{b}_{2,i}\mathbf{f}+\mathbf{w}_{2,i})^k-(\mathbf{w}_{2,i})^k)/\mathbf{f}$, $\mathbf{b}_2=\sum_{i=1}^{\tau}d_i\cdot\mathbf{b}'_{2,i}$, and $\mathbf{w}_2=\sum_{i=1}^{\tau}d_i\cdot(\mathbf{w}_{2,i})^k$. □

Lemma 3.4 Given s level-k encodings $(\mathbf{U}_{1,l},\mathbf{U}_{2,l}),l\in[\![s]\!]$, then $(\mathbf{U}_1,\mathbf{U}_2)$ is a level-k encoding, where $\mathbf{U}_t=\left[\sum_{l=1}^{s}\mathbf{U}_{t,l}\right]_q,t\in[\![2]\!]$.

Proof. Since the level-k encoding $\mathbf{U}_{1,l}=\left[\mathbf{T}_1Rot(\frac{\mathbf{a}'_{1,l}\mathbf{g}+\mathbf{e}'_{1,l}}{\mathbf{z}_1^k})\mathbf{T}_1^{-1}\right]_q$ for $\mathbf{g}$, then

$$\mathbf{U}_1=\left[\sum_{l=1}^{s}\mathbf{U}_{1,l}\right]_q=\left[\mathbf{T}_1 Rot(\frac{\sum_{l=1}^{s}(\mathbf{a}_{1,l}^{'}\mathbf{g}+\mathbf{e}_{1,l}^{'})}{\mathbf{z}_1^k})\mathbf{T}_1^{-1}\right]_q=\left[\mathbf{T}_1 Rot(\frac{\mathbf{a}_1\mathbf{g}+\mathbf{e}_1}{\mathbf{z}_1^k})\mathbf{T}_1^{-1}\right]_q,$$

where $\mathbf{a}_1=\sum_{l=1}^{s}\mathbf{a}_{1,l}^{'}$ and $\mathbf{e}_1=\sum_{l=1}^{s}\mathbf{e}_{1,l}^{'}$.

For $\mathbf{f}$, the level-k encoding $\mathbf{U}_{t,l}=\left[\mathbf{T}_t Rot(\frac{\mathbf{r}_{t,l}^{'}\mathbf{f}+\mathbf{e}_{2,l}^{'}}{\mathbf{z}_t^k})\mathbf{T}_t^{-1}\right]_q$, then

$$\mathbf{U}_t=\left[\sum_{l=1}^{s}\mathbf{U}_{t,l}\right]_q=\left[\mathbf{T}_t Rot(\frac{\sum_{l=1}^{s}(\mathbf{r}_{t,l}^{'}\mathbf{f}+\mathbf{e}_{2,l}^{'})}{\mathbf{z}_t^k})\mathbf{T}_t^{-1}\right]_q=\left[\mathbf{T}_t Rot(\frac{\mathbf{r}_t\mathbf{f}+\mathbf{e}_2}{\mathbf{z}_t^k})\mathbf{T}_t^{-1}\right]_q,$$

where $\mathbf{r}_t=\sum_{l=1}^{s}\mathbf{r}_{t,l}^{'}$ and $\mathbf{e}_2=\sum_{l=1}^{s}\mathbf{e}_{2,l}^{'}$. □

Lemma 3.5 Given k level-1 encodings $(\mathbf{U}_{1,l},\mathbf{U}_{2,l}), l\in[\![k]\!]$, then $(\mathbf{U}_1,\mathbf{U}_2)$ is a level-k encoding, where $\mathbf{U}_t=\left[\prod_{l=1}^{k}\mathbf{U}_{t,l}\right]_q$.

Proof. For $\mathbf{g}$, the level-1 encoding $\mathbf{U}_{1,l}=\left[\mathbf{T}_1 Rot(\frac{\mathbf{a}_{1,l}^{'}\mathbf{g}+\mathbf{e}_{1,l}^{'}}{\mathbf{z}_1})\mathbf{T}_1^{-1}\right]_q$, then

$$\mathbf{U}_1=\left[\prod_{l=1}^{k}\mathbf{U}_{1,l}\right]_q=\left[\mathbf{T}_1 Rot(\frac{\prod_{l=1}^{k}(\mathbf{a}_{1,l}^{'}\mathbf{g}+\mathbf{e}_{1,l}^{'})}{\mathbf{z}_1^k})\mathbf{T}_1^{-1}\right]_q=\left[\mathbf{T}_1 Rot(\frac{\mathbf{a}_1\mathbf{g}+\mathbf{e}_1}{\mathbf{z}_1^k})\mathbf{T}_1^{-1}\right]_q,$$

where $\mathbf{a}_1=(\prod_{l=1}^{k}(\mathbf{a}_{1,l}^{'}\mathbf{g}+\mathbf{e}_{1,l}^{'})-\prod_{l=1}^{k}\mathbf{e}_{1,l}^{'})/\mathbf{g}$ and $\mathbf{e}_1=\prod_{l=1}^{k}\mathbf{e}_{1,l}^{'}$.

For $\mathbf{f}$, the level-k encoding $\mathbf{U}_{t,l}=\left[\mathbf{T}_t Rot(\frac{\mathbf{r}_{t,l}^{'}\mathbf{f}+\mathbf{e}_{2,l}^{'}}{\mathbf{z}_t^k})\mathbf{T}_t^{-1}\right]_q$, then

$$\mathbf{U}_t=\left[\prod_{l=1}^{k}\mathbf{U}_{t,l}\right]_q=\left[\mathbf{T}_t Rot(\frac{\prod_{l=1}^{k}(\mathbf{r}_{t,l}^{'}\mathbf{f}+\mathbf{e}_{2,l}^{'})}{\mathbf{z}_t^k})\mathbf{T}_t^{-1}\right]_q=\left[\mathbf{T}_t Rot(\frac{\mathbf{r}_t\mathbf{f}+\mathbf{e}_2}{\mathbf{z}_t^k})\mathbf{T}_t^{-1}\right]_q,$$

where $\mathbf{r}_t=(\prod_{l=1}^{k}(\mathbf{r}_{1,l}^{'}\mathbf{f}+\mathbf{e}_{2,l}^{'})-\prod_{l=1}^{k}\mathbf{e}_{2,l}^{'})/\mathbf{f}$ and $\mathbf{e}_2=\prod_{l=1}^{k}\mathbf{e}_{2,l}^{'}$. □

Lemma 3.6 The zero testing $\text{isZero}(\text{par},(\mathbf{U}_1,\mathbf{U}_2),\mathbf{d})$ correctly determines whether $\mathbf{U}_1$ is a level-κ encoding of zero for $\mathbf{g}$.

Proof. Given a level-κ encoding $(\mathbf{U}_1,\mathbf{U}_2)$, then we have $\mathbf{U}_1=\left[\mathbf{T}_1 Rot(\frac{\mathbf{a}_1\mathbf{g}+\mathbf{e}_1}{\mathbf{z}_1^\kappa})\mathbf{T}_1^{-1}\right]_q$ for $\mathbf{g}$, and $\mathbf{U}_t=\left[\mathbf{T}_t Rot(\frac{\mathbf{r}_t\mathbf{f}+\mathbf{e}_2}{\mathbf{z}_t^\kappa})\mathbf{T}_t^{-1}\right]_q$ for $\mathbf{f}$ such that $\mathbf{a}_1\mathbf{g}+\mathbf{e}_1=\mathbf{r}_1\mathbf{f}+\mathbf{e}_2$.

Since $\mathbf{E}_1=\left[\sum_{i=1}^{\tau}d_i\cdot\mathbf{X}_{1,i}\right]_q$ and $\mathbf{E}_2=\left[\sum_{i=1}^{\tau}d_i\cdot\mathbf{X}_{2,i}\right]_q$, then we have $\mathbf{E}_1=\left[\mathbf{S}_1^{-1}Rot(\mathbf{a}_1^{'}\mathbf{g}+\mathbf{e}_1^{'})\mathbf{S}_1\right]_q$ for $\mathbf{g}$, and $\mathbf{E}_t=\left[\mathbf{S}_t^{-1}Rot(\mathbf{b}_t\mathbf{f}+\mathbf{w}_2)\mathbf{S}_t\right]_q$ for $\mathbf{f}$ such that $\mathbf{a}_1^{'}\mathbf{g}+\mathbf{e}_1^{'}=\mathbf{b}_1\mathbf{f}+\mathbf{w}_2$.

Thus, we get

$$\left[\mathbf{T}_1^* \cdot \mathbf{U}_1 \cdot \mathbf{P}_{zt,1} \cdot \mathbf{E}_1 \cdot \mathbf{S}_1^*\right]_q$$
$$=\left[\mathbf{T}_0\mathbf{T}_1^{-1} \cdot \mathbf{U}_1 \cdot \mathbf{P}_{zt,1} \cdot \mathbf{E}_1 \cdot \mathbf{S}_1^{-1}\mathbf{S}_0\right]_q$$
$$=\left[\mathbf{T}_0 \cdot Rot(\mathbf{a}_1\mathbf{g}+\mathbf{e}_1) \cdot Rot\left(\left(\sum_{j=1}^m \mathbf{h}_j\mathbf{g}_j^{-1} + \mathbf{hf}^{-1}\right)\right) \cdot Rot(\mathbf{a}_1^{'}\mathbf{g}+\mathbf{e}_1^{'}) \cdot \mathbf{S}_0\right]_q \quad ,$$
$$=\left[\mathbf{T}_0 \cdot Rot\left((\mathbf{a}_1\mathbf{g}+\mathbf{e}_1)\left(\sum_{j=1}^m \mathbf{h}_j\mathbf{g}_j^{-1} + \mathbf{hf}^{-1}\right)(\mathbf{a}_1^{'}\mathbf{g}+\mathbf{e}_1^{'})\right) \cdot \mathbf{S}_0\right]_q$$
$$=\left[\mathbf{T}_0 Rot\left((\mathbf{a}_1\mathbf{g}+\mathbf{e}_1)\left(\sum_{j=1}^m \mathbf{h}_j\mathbf{g}_j^{-1}\right)(\mathbf{a}_1^{'}\mathbf{g}+\mathbf{e}_1^{'}) + (\mathbf{r}_1\mathbf{f}+\mathbf{e}_2)\mathbf{hf}^{-1}(\mathbf{b}_1\mathbf{f}+\mathbf{w}_2)\right)\mathbf{S}_0\right]_q$$
$$\left[\mathbf{T}_2^* \cdot \mathbf{U}_2 \cdot \mathbf{P}_{zt,2} \cdot \mathbf{E}_2 \cdot \mathbf{S}_2^*\right]_q$$
$$=\left[\mathbf{T}_0\mathbf{T}_2^{-1} \cdot \mathbf{U}_2 \cdot \mathbf{P}_{zt,2} \cdot \mathbf{E}_2 \cdot \mathbf{S}_2^{-1}\mathbf{S}_0\right]_q \quad .$$
$$=\left[\mathbf{T}_0 \cdot Rot\left((\mathbf{r}_2\mathbf{f}+\mathbf{e}_2)\mathbf{hf}^{-1}(\mathbf{b}_2\mathbf{f}+\mathbf{w}_2)\right) \cdot \mathbf{S}_0\right]_q$$

Thus, we have

$$\mathbf{V} = \left[\mathbf{T}_1^* \cdot \mathbf{U}_1 \cdot \mathbf{P}_{zt,1} \cdot \mathbf{E}_1 \cdot \mathbf{S}_1^* - \mathbf{T}_2^* \cdot \mathbf{U}_2 \cdot \mathbf{P}_{zt,2} \cdot \mathbf{E}_2 \cdot \mathbf{S}_2^*\right]_q$$
$$= \left[\mathbf{T}_0 \cdot Rot\left((\mathbf{a}_1\mathbf{g}+\mathbf{e}_1)\left(\sum_{j=1}^m \mathbf{h}_j\mathbf{g}_j^{-1}\right)(\mathbf{a}_1^{'}\mathbf{g}+\mathbf{e}_1^{'}) + \mathbf{rh}\right) \cdot \mathbf{S}_0\right]_q ,$$

where $\mathbf{r} = \mathbf{r}_1\mathbf{b}_1\mathbf{f} + \mathbf{r}_1\mathbf{w}_2 + \mathbf{b}_1\mathbf{e}_2 - \mathbf{r}_2\mathbf{b}_2\mathbf{f} - \mathbf{r}_2\mathbf{w}_2 - \mathbf{b}_2\mathbf{e}_2$.

If $\mathbf{U}_1$ is a level-κ encoding of zero for $\mathbf{g}$, namely $\mathbf{e}_1 = 0 \bmod \mathbf{g}_j$. Since $\mathbf{g}_j$'s are coprime, we get $\mathbf{e}_1 = 0$. Thus, we have

$$\mathbf{V} = \left[\mathbf{T}_0 \cdot Rot\left((\mathbf{a}_1\mathbf{g}+\mathbf{e}_1)\left(\sum_{j=1}^m \mathbf{h}_j\mathbf{g}_j^{-1}\right)(\mathbf{a}_1^{'}\mathbf{g}+\mathbf{e}_1^{'}) + \mathbf{rh}\right) \cdot \mathbf{S}_0\right]_q$$
$$= \left[\mathbf{T}_0 \cdot Rot\left(\mathbf{a}_1\mathbf{g}\left(\sum_{j=1}^m \mathbf{h}_j\mathbf{g}_j^{-1}\right)(\mathbf{a}_1^{'}\mathbf{g}+\mathbf{e}_1^{'}) + \mathbf{rh}\right) \cdot \mathbf{S}_0\right]_q \quad .$$
$$= \left[\mathbf{T}_0 \cdot Rot\left(\mathbf{a}_1\left(\sum_{j=1}^m \mathbf{h}_j \cdot \mathbf{g}/\mathbf{g}_j\right)(\mathbf{a}_1^{'}\mathbf{g}+\mathbf{e}_1^{'}) + \mathbf{rh}\right) \cdot \mathbf{S}_0\right]_q$$

For our choice of parameter, $\|\mathbf{a}_1\| \le q^{1/8}$, $\|\mathbf{a}_1^{'}\mathbf{g}+\mathbf{e}_1^{'}\| \le n^{O(1)}$, $\|\mathbf{r}\| \le q^{1/8}$ and $\|\mathbf{T}_0\|_\infty = \|\mathbf{S}_0\|_\infty \le \sqrt{n}\sigma$. Moreover, $\mathbf{V}$ is not reduced modulo q, that is $[\mathbf{V}]_q = \mathbf{V}$. Hence,

$$\|\mathbf{V}\| = \left\|\left[\mathbf{T}_0 \cdot Rot\left(\mathbf{a}_1\left(\sum_{j=1}^m \mathbf{h}_j \cdot \mathbf{g}/\mathbf{g}_j\right)(\mathbf{a}_1^{'}\mathbf{g}+\mathbf{e}_1^{'}) + \mathbf{rh}\right) \cdot \mathbf{S}_0\right]_q\right\|$$
$$= \left\|\mathbf{T}_0 \cdot Rot\left(\mathbf{a}_1\left(\sum_{j=1}^m \mathbf{h}_j \cdot \mathbf{g}/\mathbf{g}_j\right)(\mathbf{a}_1^{'}\mathbf{g}+\mathbf{e}_1^{'}) + \mathbf{rh}\right) \cdot \mathbf{S}_0\right\|$$
$$\le 2n^3 \cdot \|\mathbf{T}_0\| \left\|Rot(\mathbf{a}_1 \sum_{j=1}^m \mathbf{h}_j \cdot \mathbf{g}/\mathbf{g}_j)\right\| \left\|Rot(\mathbf{a}_1^{'}\mathbf{g}+\mathbf{e}_1^{'})\right\| \|\mathbf{S}_0\|$$
$$= 2n^4 \cdot \sqrt{n}\sigma \|Rot(\mathbf{a}_1)\| \left\|Rot(\sum_{j=1}^m \mathbf{h}_j \cdot \mathbf{g}/\mathbf{g}_j)\right\| \cdot n^{O(1)} \cdot \sqrt{n}\sigma .$$
$$= 2n^{O(1)}\sigma^2 \cdot q^{1/8} \cdot m \cdot \left\|Rot(\mathbf{h}_j \cdot \mathbf{g}/\mathbf{g}_j)\right\|$$
$$= n^{O(1)}\sigma^2 \cdot q^{1/8} \cdot poly(n) \cdot q^{1/2} \cdot poly(n)$$
$$< q^{3/4}$$

If $\mathbf{U}_1$ is a level-κ encoding of of non-zero element for $\mathbf{g}$, namely, $\mathbf{e}_1 \ne 0 \bmod \mathbf{g}_j$ for at least one $j \in [\![m]\!]$. Thus,

$$\mathbf{V} = \left[\mathbf{T}_0 \cdot Rot\left((\mathbf{a}_1\mathbf{g}+\mathbf{e}_1)\left(\sum_{j=1}^{m}\mathbf{h}_j\mathbf{g}_j^{-1}\right)(\mathbf{a}_1^{'}\mathbf{g}+\mathbf{e}_1^{'})+\mathbf{r}\mathbf{h}\right)\cdot\mathbf{S}_0\right]_q$$

$$= \left[\mathbf{T}_0 Rot\left(\mathbf{a}_1(\mathbf{a}_1^{'}\mathbf{g}+\mathbf{e}_1^{'})\sum_{j=1}^{m}\mathbf{h}_j\cdot\mathbf{g}/\mathbf{g}_j+\mathbf{r}\mathbf{h}\right)\mathbf{S}_0+\mathbf{T}_0 Rot\left(\sum_{j=1}^{m}\frac{\mathbf{h}_j\mathbf{e}_1(\mathbf{a}_1^{'}\mathbf{g}+\mathbf{e}_1^{'})}{\mathbf{g}_j}\right)\mathbf{S}_0\right]_q .$$

Since $\left\|\left[\mathbf{T}_0 Rot\left(\sum_{j=1}^{m}\frac{\mathbf{h}_j\mathbf{e}_1(\mathbf{a}_1^{'}\mathbf{g}+\mathbf{e}_1^{'})}{\mathbf{g}_j}\right)\mathbf{S}_0\right]_q\right\| \approx q$ by Lemma 4 in [GGH13] , and $\left\|\left[\mathbf{T}_0 Rot\left(\mathbf{a}_1(\mathbf{a}_1^{'}\mathbf{g}+\mathbf{e}_1^{'})\sum_{j=1}^{m}\mathbf{h}_j\cdot\mathbf{g}/\mathbf{g}_j+\mathbf{r}\mathbf{h}\right)\mathbf{S}_0\right]_q\right\| < q^{3/4}$ from the above. That is, $\|\mathbf{V}\| \approx q$. □

Lemma 3.7 Given two level-κ encodings $(\mathbf{U}_1,\mathbf{U}_2)$ and $(\mathbf{W}_1,\mathbf{W}_2)$, suppose that $\mathbf{U}_1,\mathbf{W}_1$ encode same plaintext for $\mathbf{g}$, then

$$\mathrm{Ext}\left(\mathrm{par},(\mathbf{U}_1,\mathbf{U}_2),\mathbf{d}\right)=\mathrm{Ext}\left(\mathrm{par},(\mathbf{W}_1,\mathbf{W}_2),\mathbf{d}\right).$$

Proof. Assume that $\mathbf{U}_1 = \left[\mathbf{T}_1 Rot\left(\frac{\mathbf{a}_1\mathbf{g}+\mathbf{e}_1}{\mathbf{z}_1^{\kappa}}\right)\mathbf{T}_1^{-1}\right]_q$ and $\mathbf{W}_1 = \left[\mathbf{T}_1 Rot\left(\frac{\mathbf{a}_2\mathbf{g}+\mathbf{e}_1}{\mathbf{z}_1^{\kappa}}\right)\mathbf{T}_1^{-1}\right]_q$. Then

$$\mathbf{V}_1 = \left[\mathbf{T}_1^{*}\cdot\mathbf{U}_1\cdot\mathbf{P}_{zt,1}\cdot\mathbf{E}_1\cdot\mathbf{S}_1^{*}-\mathbf{T}_2^{*}\cdot\mathbf{U}_2\cdot\mathbf{P}_{zt,2}\cdot\mathbf{E}_2\cdot\mathbf{S}_2^{*}\right]_q$$

$$= \left[\mathbf{T}_0 \cdot Rot\left((\mathbf{a}_1\mathbf{g}+\mathbf{e}_1)\left(\sum_{j=1}^{m}\mathbf{h}_j\mathbf{g}_j^{-1}\right)(\mathbf{a}_1^{'}\mathbf{g}+\mathbf{e}_1^{'})+\mathbf{r}_1\mathbf{h}\right)\cdot\mathbf{S}_0\right]_q ,$$

$$= \left[\mathbf{T}_0 Rot\left(\mathbf{a}_1(\mathbf{a}_1^{'}\mathbf{g}+\mathbf{e}_1^{'})\sum_{j=1}^{m}\mathbf{h}_j\cdot\mathbf{g}/\mathbf{g}_j+\mathbf{r}_1\mathbf{h}\right)\mathbf{S}_0+\mathbf{T}_0 Rot\left(\sum_{j=1}^{m}\frac{\mathbf{h}_j\mathbf{e}_1(\mathbf{a}_1^{'}\mathbf{g}+\mathbf{e}_1^{'})}{\mathbf{g}_j}\right)\mathbf{S}_0\right]_q$$

$$\mathbf{V}_2 = \left[\mathbf{T}_1^{*}\cdot\mathbf{W}_1\cdot\mathbf{P}_{zt,1}\cdot\mathbf{E}_1\cdot\mathbf{S}_1^{*}-\mathbf{T}_2^{*}\cdot\mathbf{W}_2\cdot\mathbf{P}_{zt,2}\cdot\mathbf{E}_2\cdot\mathbf{S}_2^{*}\right]_q$$

$$= \left[\mathbf{T}_0 \cdot Rot\left((\mathbf{a}_2\mathbf{g}+\mathbf{e}_1)\left(\sum_{j=1}^{m}\mathbf{h}_j\mathbf{g}_j^{-1}\right)(\mathbf{a}_1^{'}\mathbf{g}+\mathbf{e}_1^{'})+\mathbf{r}_2\mathbf{h}\right)\cdot\mathbf{S}_0\right]_q .$$

$$= \left[\mathbf{T}_0 Rot\left(\mathbf{a}_2(\mathbf{a}_1^{'}\mathbf{g}+\mathbf{e}_1^{'})\sum_{j=1}^{m}\mathbf{h}_j\cdot\mathbf{g}/\mathbf{g}_j+\mathbf{r}_2\mathbf{h}\right)\mathbf{S}_0+\mathbf{T}_0 Rot\left(\sum_{j=1}^{m}\frac{\mathbf{h}_j\mathbf{e}_1(\mathbf{a}_1^{'}\mathbf{g}+\mathbf{e}_1^{'})}{\mathbf{g}_j}\right)\mathbf{S}_0\right]_q$$

For our parameter setting, $\left\|\left[\mathbf{T}_0 Rot\left(\mathbf{a}_t(\mathbf{a}_1^{'}\mathbf{g}+\mathbf{e}_1^{'})\sum_{j=1}^{m}\mathbf{h}_j\cdot\mathbf{g}/\mathbf{g}_j+\mathbf{r}_t\mathbf{h}\right)\mathbf{S}_0\right]_q\right\| < q^{3/4}$. By Lemma 4 in [GGH13], $\left\|\left[\mathbf{T}_0 Rot\left(\sum_{j=1}^{m}\frac{\mathbf{h}_j\mathbf{e}_1(\mathbf{a}_1^{'}\mathbf{g}+\mathbf{e}_1^{'})}{\mathbf{g}_j}\right)\mathbf{S}_0\right]_q\right\| \approx q$ when $\mathbf{e}_1 \neq 0 \bmod \mathbf{g}_j$ for at least one $j \in [\![m]\!]$. Thus, the equality holds. □

3.3 Security

Consider the following security experiment:

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

(2) For $l=0$ to κ:

Sample $\mathbf{d}_l \leftarrow D_{\mathbb{Z}^\tau,\sigma^*}$, $\mathbf{r}_l \leftarrow D_{\mathbb{Z}^\rho,\sigma^*}$;

Compute level-0 encoding $\mathbf{E}_{t,l} = \left[\sum_{i=1}^{\tau} d_{l,i}\mathbf{X}_{t,i}\right]_q$, $t \in [\![2]\!]$;

Generate level-1 encoding $\mathbf{U}_{t,l} = \left[\sum_{i=1}^{\tau} d_{l,i}\mathbf{Y}_{t,i} + \sum_{\delta=1}^{\rho} r_{l,\delta}\mathbf{Q}_{t,\delta}\right]_q$, $t \in [\![2]\!]$.

(3) Set $\mathbf{U}_t = \left[\prod_{j=1}^{\kappa}\mathbf{U}_{t,j}\right]_q$, $t \in [\![2]\!]$.

(4) Set $\mathbf{V}_C = \mathbf{V}_D = \left[\mathbf{T}_1^* \cdot \mathbf{U}_1 \cdot \mathbf{P}_{zt,1} \cdot \mathbf{E}_{1,0} \cdot \mathbf{S}_1^* - \mathbf{T}_2^* \cdot \mathbf{U}_2 \cdot \mathbf{P}_{zt,2} \cdot \mathbf{E}_{2,0} \cdot \mathbf{S}_2^*\right]_q$.

(5) Set $\mathbf{V}_R = \left[\mathbf{T}_1^* \cdot \mathbf{U}_1 \cdot \mathbf{P}_{zt,1} \cdot \mathbf{R}_{1,0} \cdot \mathbf{S}_1^* - \mathbf{T}_2^* \cdot \mathbf{U}_2 \cdot \mathbf{P}_{zt,2} \cdot \mathbf{R}_{2,0} \cdot \mathbf{S}_2^*\right]_q$, where $\mathbf{R}_{t,0} = \left[\sum_{i=1}^{\tau} r_i\mathbf{X}_{t,i}\right]_q$, $t \in [\![2]\!]$ and $\mathbf{r} \leftarrow D_{\mathbb{Z}^\tau,\sigma^*}$.

Definition 3.8 (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 $\left\{\mathrm{par}, \left(\mathbf{U}_{1,0}, \mathbf{U}_{2,0}\right), \cdots, \left(\mathbf{U}_{1,\kappa}, \mathbf{U}_{2,\kappa}\right)\right\}$, output a level-$\kappa$ extraction encoding $\mathbf{W} \in \mathbb{Z}_q^{k_1 \times k_2}$ such that $\left\|\left[\mathbf{V}_C - \mathbf{W}\right]_q\right\|_\infty \le q^{3/4}$.

Level-κ extraction DDH (ext-GDDH): Given $\left\{\mathrm{par}, \left(\mathbf{U}_{1,0}, \mathbf{U}_{2,0}\right), \cdots, \left(\mathbf{U}_{1,\kappa}, \mathbf{U}_{2,\kappa}\right), \mathbf{V}\right\}$, distinguish between $D_{ext-GDDH} = \left\{\mathrm{par}, \left(\mathbf{U}_{1,0}, \mathbf{U}_{2,0}\right), \cdots, \left(\mathbf{U}_{1,\kappa}, \mathbf{U}_{2,\kappa}\right), \mathbf{V}_D\right\}$ and $D_{ext-RAND} = \left\{\mathrm{par}, \left(\mathbf{U}_{1,0}, \mathbf{U}_{2,0}\right), \cdots, \left(\mathbf{U}_{1,\kappa}, \mathbf{U}_{2,\kappa}\right), \mathbf{V}_R\right\}$.

3.4 Cryptanalysis

We first generate easily computable quantities in our construction, then analyze possible attacks using these quantities.

3.4.1 Easily computable quantities

For an arbitrary level-κ encoding $\left(\mathbf{U}_1, \mathbf{U}_2\right)$, if $\mathbf{U}_1$ is a level-κ encoding of zero for $\mathbf{g}$, then we have $\mathbf{V} = \left[\mathbf{T}_0 \cdot Rot\left(\mathbf{r}_1 \cdot \mathbf{g}^k + \mathbf{h}\mathbf{r}_2\right) \cdot \mathbf{S}_0\right]_q$, where $0 \le k < \kappa$ and $\mathbf{r}_1, \mathbf{r}_2 \in R$. Although $\mathbf{V}$ is not reduced modulo q, the noise term $\mathbf{h}\mathbf{r}_2$ prevents adversary obtaining the information of $\mathbf{g}$. Moreover, it is easy to see that $\mathbf{V}$ has been destroyed the structure of the ring element by using $\mathbf{T}_0, \mathbf{S}_0$, and does not have the property of the principal ideal lattice problem. We do not find feasible attacks by using $\mathbf{V}$ for our construction.

Other attacks (such as [HJ15a, CL15]) are described in the following full version.

3.4.2 The Subgroup Membership and Decision Linear Problems

The SubM problem. Let $R_j = R / \mathbf{g}_j R$, $G = R_1 \times \cdots \times R_m$, and $G_1 = \{0\} \times R_2 \times \cdots \times R_m$. Let $\mathbf{Z}_i$ be level-1 encodings of elements from G, and $\mathbf{Z}_i^{(1)}$ be level-1 encodings of elements from G_1. When generating encoding $\mathbf{U} \leftarrow \mathrm{enc}(\mathrm{par}, t, \mathbf{d}, \mathbf{r})$, we replace $\mathbf{Y}_i$ with $\mathbf{Z}_i$ or $\mathbf{Z}_i^{(1)}$. The subgroup membership problem is to distinguish between $\mathbf{U} \leftarrow \mathrm{enc}(\mathrm{par}, t, \mathbf{d}, \mathbf{r})$ using $\mathbf{Z}_i$ and $\mathbf{U}_1 \leftarrow \mathrm{enc}(\mathrm{par}, t, \mathbf{d}_1, \mathbf{r}_1)$ using $\mathbf{Z}_i^{(1)}$. By the above analysis, $\mathbf{V}^{(\varepsilon)}$ has erased the structure of principal ideal lattice problem. That is, one cannot distinguish between $\mathbf{U}$ and $\mathbf{U}_1$. Thus, we conjecture that the SubM problem is hard in our encoding scheme.

The DLIN problem. Given a matrix of elements $\mathbf{A}=(\mathbf{a}_{i,j})\in R^{w\times w}$ and their encodings matrix $\mathbf{T}=(\mathrm{enc}(\mathrm{par},t,\mathbf{a}_{i,j},\mathbf{r}))$, the DLIN problem is to distinguish between rank w and rank $w-1$ matrices $\mathbf{A}$. Based on same reason, we conjecture that the DLIN problem is hard in our encoding scheme.

4 Variant

We can use polynomial ring instead of integer ring $\mathbb{Z}$ for our symmetric construction to improve the efficiency of our construction. It is easy to verify that our constructions are still correct under this case.

We can adapt the above symmetric construction into asymmetric variant. This variant is same as that [GGH13], except with changing polynomial ring to matrix ring.

5 Applications

In this section, 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 $(\mathrm{par})\leftarrow \mathrm{InstGen}(1^\lambda,1^\kappa)$ as the public parameters.

Publish(par,j). The j-th party samples $\mathbf{d}_j\leftarrow D_{\mathbb{Z}^\tau,\sigma^*}$, $\mathbf{r}_j\leftarrow D_{\mathbb{Z}^\rho,\sigma^*}$, publishes the public key $\mathbf{U}_{t,j}=\left[\sum_{i=1}^{\tau}(d_{j,i}\cdot \mathbf{Y}_{t,i})+\sum_{\delta=1}^{\rho}(r_{j,\delta}\cdot \mathbf{Q}_{t,\delta})\right]_q$, $t\in[\![2]\!]$ and generates the secret key $\mathbf{d}_j$.

KeyGen$(\mathrm{par},j,\mathbf{d}_j,\{\mathbf{U}_{1,k},\mathbf{U}_{2,k}\}_{k\neq j})$. The j-th party computes $\mathbf{C}_{t,j}=\prod_{k\neq j}\mathbf{U}_{t,k}$ and extracts the common secret key $sk=\mathrm{Ext}\left(\mathrm{par},\left(\mathbf{C}_{1,j},\mathbf{C}_{2,j}\right),\mathbf{d}\right)$.

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 GGH map. However, Hu and Jia [HJ15a] have broken the GGH-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$(1^\lambda,\mathrm{par},M)$**:**

(1) For $k\in[\![K]\!]$, sample $\mathbf{d}_k\leftarrow D_{Z^\tau,\sigma}$, $\mathbf{r}_k\leftarrow D_{\mathbb{Z}^\rho,\sigma^*}$ and generate level-1 encodings

$\mathbf{U}_{t,k} = \left[\sum_{i=1}^{\tau} d_{k,i}\mathbf{Y}_{t,i} + \sum_{\delta=1}^{\rho}(r_{k,i}\cdot\mathbf{Q}_{t,\delta})\right]_q$, $t\in[\![2]\!]$.

(2) Compute $\mathbf{U}_t = \left[\prod_{k=1}^{K}\mathbf{U}_{t,k}\right]_q$, $t\in[\![2]\!]$ and $sk = \mathrm{Ext}\left(\mathrm{par},\left(\mathbf{U}_1,\mathbf{U}_2\right),\mathbf{1}\right)$, and encrypt a message M into ciphertext C, where $\mathbf{1}=(1,\ldots,1)\in\mathbb{Z}^{\tau}$.

(3) For each element $T_i=\{i_1,i_2,i_3\}$, sample $\mathbf{r}_{T_i}\leftarrow D_{\mathbb{Z}^{\rho},\sigma^*}$, and generate a level-$3$ encoding $\mathbf{U}_{t,T_i} = \left[\mathbf{U}_{t,i_1}\mathbf{U}_{t,i_2}\mathbf{U}_{t,i_3} + \sum_{\delta=1}^{\rho} r_{T_i,\delta}(\mathbf{Q}_{t,\delta})^3\right]_q$, $t\in[\![2]\!]$.

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

Decrypt(C,E,W):

(1) Given C, E and a witness set W, compute $\mathbf{U}_t = \left[\prod_{T_i\in W}\mathbf{U}_{t,T_i}\right]_q$, $t\in[\![2]\!]$.

(2) Generate $sk = \mathrm{Ext}\left(\mathrm{par},\left(\mathbf{U}_1,\mathbf{U}_2\right),\mathbf{1}\right)$, and decrypt C to a 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

The Hu-Jia attack [HJ15b] is thwarted in our new construction. Since Gu map-1 [Gu15] uses hidden randomizers, in some sense one merely can generate a deterministically level-l encoding. As a result, one can compute $\mathbf{U}_{T_i} = \left[\mathbf{U}_{T_j}\mathbf{U}_{T_k}(\mathbf{U}_{T_l})^{-1}\right]_q$ if $T_i = T_j \cup T_k - T_l$. Thus, one can generate a combined 3-exact cover, and correctly compute a secret level-K encoding. However, since $\mathbf{U}_{t,T_i} = \left[\mathbf{U}_{t,i_1}\mathbf{U}_{t,i_2}\mathbf{U}_{t,i_3} + \sum_{\delta=1}^{\rho} r_{T_i,\delta}(\mathbf{Q}_{t,\delta})^3\right]_q$ is a level-3 encoding in our new construction, one cannot obtain $\mathbf{U}_{t,T_i} = \left[\mathbf{U}_{t,T_j}\mathbf{U}_{t,T_k}(\mathbf{U}_{t,T_l})^{-1}\right]_q$ when $T_i = T_j \cup T_k - T_l$. This is because our construction uses level-1 encodings $\mathbf{Q}_{\delta}$ of zero.

6 Conclusion

In this paper, we describe a new modification of GGH, which supports the applications for public tools of encoding in GGH, such MPKE and WE. Our construction removes the special structure of the principal ideal lattice problem, and avoids potential attacks generated by algorithm of solving short principal ideal lattice generator. However, the security of our construction depends upon new hardness assumption, which cannot be reduced to classical hardness problem, such as LWE or SVP.

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.

[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.

[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.