Multilinear Maps Using Random Matrix

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

May 15, 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 two applications of multipartite key exchange (MPKE) and witness encryption (WE) based on the hardness of 3-exact cover problem by using GGH. 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 GGH framework, 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 applications on multipartite key exchange (MPKE) and witness encryption (WE) based on the hardness of 3-exact cover problem.

Gu [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 using Gu map-1 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 GGH in three aspects. (1) We modify the zero-testing parameter of GGH by introducing random matrix. By using new zero-testing parameter, the level-1 encodings and level-0 encodings in the public parameters are separated, and cannot be directly multiplied between them. As a result, our construction thwarts the revelation of the secret parameters. (2) We transform ring elements into non-square matrix to damage the structure of ring elements and further avoid the principal ideal lattice problem. Due to this improvement, we can give encodings of zero in the public parameters. Thus, our construction supports the applications for public tools of encoding in GGH, and removes the weakness of the principal ideal lattices problem in GGH. (3) Our construction supports the membership group problem (SubM) and the decisional linear (DLIN) problem. Thus, our construction can have more applications than [GGH13].

Our second contribution is to describe two applications of MPKE and WE using our multilinear map. Since these applications are attacked by [HJ15a], they urgently require to be fixed. The construction of MPKE and WE based on our new map is same as ones using GGH.

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 $G_1,\ldots,G_\kappa,G_T$ of the same order q, a κ-multilinear map $e: G_1\times\cdots\times G_\kappa \to G_T$ has the following properties:

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

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

(2) Map e is non-degenerate in the following sense: if elements $\{g_j \in G_j\}_{j=1,\ldots,\kappa}$ 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 $k_1k_2\le n-O(\lambda)$.

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) Choose $\mathbf{g}_j\leftarrow D_{\mathbb{Z}^n,\sqrt{\sigma}}$, $\mathbf{h}_j\leftarrow D_{\mathbb{Z}^n,\sqrt{q}}$, $j\in[\![m]\!]$ in R, and set $\mathbf{g}=\prod_{j=1}^m \mathbf{g}_j$ so that $\mathbf{g}_j$'s are coprime and $\left\|\mathbf{g}_j^{-1}\right\|\le n$;

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

(4) Choose a random element $\mathbf{z}\leftarrow R_q$ so that $\mathbf{z}^{-1}\in R_q$;

(5) Choose randomly $\mathbf{T},\mathbf{S}\in\mathbb{Z}_q^{n\times n}$ so that $\mathbf{T}^{-1},\mathbf{S}^{-1}\in\mathbb{Z}_q^{n\times n}$;

(6) Choose $\mathbf{T}_1\leftarrow D_{\mathbb{Z}^{k_1\times n},\sigma}$, $\mathbf{S}_1\leftarrow D_{\mathbb{Z}^{n\times k_2},\sigma}$ and set $\mathbf{T}^*=\mathbf{T}_1\mathbf{T}^{-1}$, $\mathbf{S}^*=\mathbf{S}^{-1}\mathbf{S}_1$;

(7) For $i \in [\![\tau]\!]$, set $\mathbf{Y}_i = \left[\mathbf{T} Rot(\frac{\mathbf{a}_i \mathbf{g} + \mathbf{e}_i}{\mathbf{z}}) \mathbf{T}^{-1} \right]_q$ and $\mathbf{X}_i = \left[\mathbf{S}^{-1} Rot(\mathbf{b}_i \mathbf{g} + \mathbf{e}_i) \mathbf{S} \right]_q$;

(8) For $\delta \in [\![\rho]\!]$, choose $\mathbf{q}_\delta \leftarrow D_{\mathbb{Z}^n, \sigma'}$ in R, and set $\mathbf{Q}_\delta = \left[\mathbf{T} Rot(\frac{\mathbf{q}_\delta \mathbf{g}}{\mathbf{z}}) \mathbf{T}^{-1} \right]_q$;

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

(10) Output the public parameters $\text{par} = \left\{ q, \{\mathbf{Y}_i, \mathbf{X}_i\}_{i \in [\![\tau]\!]}, \{\mathbf{Q}_\delta\}_{\delta \in [\![\rho]\!]}, \mathbf{P}_{zt}, \mathbf{T}^*, \mathbf{S}^* \right\}$.

Generating level-t encoding: $\mathbf{U} \leftarrow \text{enc}(\text{par}, t, \mathbf{d}, \mathbf{r})$.

Given $\mathbf{d} \leftarrow D_{\mathbb{Z}^\tau, \sigma^*}$ and $\mathbf{r} \leftarrow D_{\mathbb{Z}^\rho, \sigma^*}$, then $\mathbf{U} = \left[\sum_{i=1}^{\tau} d_i \cdot (\mathbf{Y}_i)^t + \sum_{\delta=1}^{\rho} r_\delta \cdot (\mathbf{Q}_\delta)^t \right]_q$ is a level-t encoding of level-0 encoding $\mathbf{E} = \left[\sum_{i=1}^{\tau} d_i \cdot (\mathbf{X}_i)^t \right]_q$.

Adding encodings: $\mathbf{U} \leftarrow \text{add}(\text{par}, t, \mathbf{U}_1, \cdots, \mathbf{U}_k)$.

Given k level-t encodings $\mathbf{U}_l$, their sum $\mathbf{U} = \left[\sum_{l=1}^{k} \mathbf{U}_l \right]_q$ is a level-t encoding.

Multiplying encodings: $\mathbf{U} \leftarrow \text{mul}(\text{par}, 1, \mathbf{U}_1, \cdots, \mathbf{U}_k)$.

Given k level-1 encodings $\mathbf{U}_l$, their product $\mathbf{U} = \left[\prod_{l=1}^{k} \mathbf{U}_l \right]_q$ is a level-k encoding.

Zero testing: $\text{isZero}(\text{par}, \mathbf{U}, \mathbf{R})$.

Given a level-κ encoding $\mathbf{U} = \left[\mathbf{T} Rot(\frac{\mathbf{r}\mathbf{g} + \mathbf{e}}{\mathbf{z}^\kappa}) \mathbf{T}^{-1} \right]_q$ and a level-0 encoding $\mathbf{R} = \left[\sum_{i=1}^{\tau} r_i \mathbf{X}_i \right]_q$, to determine whether $\mathbf{U}$ is a level-κ encoding of zero, we compute $\mathbf{V} = \left[\mathbf{T}^* \cdot \mathbf{U} \cdot \mathbf{P}_{zt} \cdot \mathbf{R} \cdot \mathbf{S}^* \right]_q$ and check whether $\|\mathbf{V}\|$ is short:

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

Extraction: $sk \leftarrow \text{ext}(\text{par}, \mathbf{U}, \mathbf{R})$.

Given a level-κ encoding $\mathbf{U}$ and a level-0 encoding $\mathbf{R} = \left[\sum_{i=1}^{\tau} r_i \mathbf{X}_i \right]_q$, we compute $\mathbf{V} = \left[\mathbf{T}^* \cdot \mathbf{U} \cdot \mathbf{P}_{zt} \cdot \mathbf{R} \cdot \mathbf{S}^* \right]_q$, and collect $(\log q)/4 - \lambda$ most-significant bits of each of the $k_1 \times k_2$ -matrix $\mathbf{V}$:

$$\text{ext}(\text{par}, \mathbf{U}, \mathbf{R}) = \text{Extract}(\text{msb}(\left[\mathbf{T}^* \cdot \mathbf{U} \cdot \mathbf{P}_{zt} \cdot \mathbf{R} \cdot \mathbf{S}^* \right]_q)).$$

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

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

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

(2) Although we randomly choose the matrices $\mathbf{T}, \mathbf{S} \in \mathbb{Z}_q^{n \times n}$, we still use the element $\mathbf{z}$ to

control the level number of encoding.

(3) The composite-order element $\mathbf{g}$ is to support the subgroup membership (SubM) and decisional linear (DLIN) problems.

(4) The matrix $\mathbf{R}$ 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 witness encryption scheme.

(6) We set $k = k_1 \times k_2 \le n - O(\lambda)$. In fact, k_1, k_2 can be 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 of level-1 encodings of non-zero in public parameters τ can be set to $O(\lambda n)$ according to the result in [HJ15c].

3.2 Correctness

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

Lemma 3.3 The encoding $\mathbf{U} \leftarrow \text{enc}(\text{par}, t, \mathbf{d}, \mathbf{r})$ is a level-t encoding.

Proof. Since $(\mathbf{Y}_i)^t = \left[\mathbf{T}Rot(\frac{\mathbf{a}_i\mathbf{g}+\mathbf{e}_i}{\mathbf{z}})^t\mathbf{T}^{-1}\right]_q$ and $(\mathbf{Q}_\delta)^t = \left[\mathbf{T}Rot(\frac{\mathbf{q}_\delta\mathbf{g}}{\mathbf{z}})^t\mathbf{T}^{-1}\right]_q$, we have

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

where $\mathbf{a}_i' = ((\mathbf{a}_i\mathbf{g}+\mathbf{e}_i)^t - (\mathbf{e}_i)^t)/\mathbf{g}$, $\mathbf{q}_\delta' = (\mathbf{q}_\delta\mathbf{g})^t/\mathbf{g}$, $\mathbf{a}=\sum_{i=1}^{\tau} d_i \cdot \mathbf{a}_i' + \sum_{\delta=1}^{\lambda} r_\delta\mathbf{q}_\delta'$, and $\mathbf{e}=\sum_{i=1}^{\tau} d_i \cdot (\mathbf{e}_i)^t$.

Again since $(\mathbf{X}_i)^t = \left[\mathbf{S}^{-1}Rot(\mathbf{b}_i\mathbf{g}+\mathbf{e}_i)^t\mathbf{S}\right]_q$, we have

$$\begin{aligned}\mathbf{E} &= \left[\sum_{i=1}^{\tau} d_i \cdot (\mathbf{X}_i)^t\right]_q \\ &= \left[\mathbf{S}^{-1}Rot(\sum_{i=1}^{\tau} d_i\mathbf{b}_i'\mathbf{g} + \sum_{i=1}^{\tau} d_i(\mathbf{e}_i)^t)\mathbf{S}\right]_q, \\ &= \left[\mathbf{S}^{-1}Rot(\mathbf{bg}+\mathbf{e})\mathbf{S}\right]_q\end{aligned}$$

where $\mathbf{b}_i' = ((\mathbf{b}_i\mathbf{g}+\mathbf{e}_i)^t - (\mathbf{e}_i)^t)/\mathbf{g}$, $\mathbf{b}=\sum_{i=1}^{\tau} d_i \cdot \mathbf{b}_i'$, and $\mathbf{e}=\sum_{i=1}^{\tau} d_i \cdot (\mathbf{e}_i)^t$.

Thus, $\mathbf{U}$ is a level-t encoding of the level-0 encoding $\mathbf{E}$. □

Lemma 3.4 Given k level-t encodings $\mathbf{U}_1, \cdots, \mathbf{U}_k$, their sum $\mathbf{U} = \left[\sum_{l=1}^{m} \mathbf{U}_l\right]_q$ is a level-t encoding.

Proof. Since the level-t encoding $\mathbf{U}_l$ has the form $\mathbf{U}_l = \left[\mathbf{T}Rot(\frac{\mathbf{r}_l'\mathbf{g}+\mathbf{e}_l'}{\mathbf{z}^t})\mathbf{T}^{-1}\right]_q$, their sum

$$\mathbf{U}=\left[\sum_{l=1}^{m}\mathbf{U}_l\right]_q=\left[\mathbf{T}Rot(\frac{\sum_{l=1}^{m}(\mathbf{r}_l^{'}\mathbf{g}+\mathbf{e}_l^{'})}{\mathbf{z}^t})\mathbf{T}^{-1}\right]_q=\left[\mathbf{T}Rot(\frac{\mathbf{rg}+\mathbf{e}}{\mathbf{z}^t})\mathbf{T}^{-1}\right]_q$$ is a level- t encoding, where $\mathbf{r}=\sum_{l=1}^{m}\mathbf{r}_l^{'}$ and $\mathbf{e}=\sum_{l=1}^{m}\mathbf{e}_l^{'}$. □

Lemma 3.5 Given k level-1 encodings $\mathbf{U}_l$, their product $\mathbf{U}=\left[\prod_{l=1}^{k}\mathbf{U}_l\right]_q$ is a level-k encoding.

Proof. Since the level-1 encoding $\mathbf{U}_l=\left[\mathbf{T}Rot(\frac{\mathbf{r}_l^{'}\mathbf{g}+\mathbf{e}_l^{'}}{\mathbf{z}})\mathbf{T}^{-1}\right]_q$, the product of k level-1 encodings is:

$$\begin{aligned}\mathbf{U}&=\left[\prod_{l=1}^{k}\mathbf{U}_l\right]_q\\&=\left[\prod_{l=1}^{k}\mathbf{T}Rot(\frac{\mathbf{r}_l^{'}\mathbf{g}+\mathbf{e}_l^{'}}{\mathbf{z}})\mathbf{T}^{-1}\right]_q\\&=\left[\mathbf{T}Rot(\frac{\prod_{j=1}^{k}(\mathbf{r}_l^{'}\mathbf{g}+\mathbf{e}_l^{'})}{\mathbf{z}^k})\mathbf{T}^{-1}\right]_q,\\&=\left[\mathbf{T}Rot(\frac{\mathbf{rg}+\mathbf{e}}{\mathbf{z}^k})\mathbf{T}^{-1}\right]_q\end{aligned}$$

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

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

Proof. Given a level- κ encoding $\mathbf{U}=\left[\mathbf{T}Rot(\frac{\mathbf{rg}+\mathbf{e}}{\mathbf{z}^{\kappa}})\mathbf{T}^{-1}\right]_q$ and a level- 0 encoding $\mathbf{R}=\left[\sum_{i=1}^{\tau}r_i\mathbf{X}_i\right]_q$, we compute $\mathbf{V}=\left[\mathbf{T}^*\cdot\mathbf{U}\cdot\mathbf{P}_{zt}\cdot\mathbf{R}\cdot\mathbf{S}^*\right]_q$ and check whether $\|\mathbf{V}\|$ is short:

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

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

$$\begin{aligned}\mathbf{V}&=\left[\mathbf{T}^*\cdot\mathbf{U}\cdot\mathbf{P}_{zt}\cdot\mathbf{R}\cdot\mathbf{S}^*\right]_q\\&=\left[\mathbf{T}_1Rot(\frac{\mathbf{rg}+\mathbf{r}'\mathbf{g}}{\mathbf{z}^{\kappa}})\mathbf{T}^{-1}\cdot\mathbf{T}Rot(\mathbf{z}^{\kappa}\sum_{j=1}^{m}\mathbf{h}_j\mathbf{g}_j^{-1})\mathbf{S}\cdot(\sum_{i=1}^{\tau}r_i\mathbf{X}_i)\cdot\mathbf{S}^*\right]_q\\&=\left[\mathbf{T}_1Rot((\mathbf{rg}+\mathbf{r}'\mathbf{g})(\sum_{j=1}^{m}\mathbf{h}_j\mathbf{g}_j^{-1})(\sum_{i=1}^{\tau}r_i\mathbf{b}_i\mathbf{g}+r_i\mathbf{e}_i))\mathbf{S}_1\right]_q\\&=\left[\mathbf{T}_1Rot((\mathbf{r}+\mathbf{r}')(\sum_{j=1}^{m}\mathbf{h}_j\cdot\mathbf{g}/\mathbf{g}_j)(\mathbf{b}'\mathbf{g}+\mathbf{e}'))\mathbf{S}_1\right]_q\end{aligned}.$$

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

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

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

$$
\begin{aligned}
\mathbf{V} &= \left[\mathbf{T}^*\cdot\mathbf{U}\cdot\mathbf{P}_{zt}\cdot\mathbf{R}\cdot\mathbf{S}^*\right]_q \\
&= \left[\mathbf{T}_1 Rot(\frac{\mathbf{rg}+\mathbf{e}}{\mathbf{z}^{\kappa}})\mathbf{T}^{-1}\cdot\mathbf{T}Rot(\mathbf{z}^{\kappa}\textstyle\sum_{j=1}^{m}\mathbf{h}_j\mathbf{g}_j^{-1})\mathbf{S}\cdot(\sum_{i=1}^{\tau}r_i\mathbf{X}_i)\cdot\mathbf{S}^*\right]_q \\
&= \left[\mathbf{T}_1 Rot(\mathbf{rg}+\mathbf{e})Rot(\textstyle\sum_{j=1}^{m}\mathbf{h}_j\mathbf{g}_j^{-1})Rot(\mathbf{b}'\mathbf{g}+\mathbf{e}')\mathbf{S}_1\right]_q \\
&= \left[\mathbf{T}_1 Rot(\mathbf{rg}(\mathbf{b}'\mathbf{g}+\mathbf{e}')\textstyle\sum_{j=1}^{m}\mathbf{h}_j\mathbf{g}_j^{-1})\mathbf{S}_1+\mathbf{T}_1 Rot(\sum_{j=1}^{m}\frac{\mathbf{h}_j\mathbf{e}(\mathbf{b}'\mathbf{g}+\mathbf{e}')}{\mathbf{g}_j})\mathbf{S}_1\right]_q
\end{aligned}
.
$$

By Lemma 4 in [GGH13], $\left\|\mathbf{T}_1 Rot(\sum_{j=1}^{m}\frac{\mathbf{h}_j\mathbf{e}(\mathbf{b}'\mathbf{g}+\mathbf{e}')}{\mathbf{g}_j})\mathbf{S}_1\right\|\approx q$, namely $\|\mathbf{V}\|\approx q$. □

Lemma 3.7 Suppose that two level-κ encodings $\mathbf{U}_1,\mathbf{U}_2$ encode same plaintext, then

$$\mathrm{ext}(\mathrm{par},\mathbf{U}_1,\mathbf{R})=\mathrm{ext}(\mathrm{par},\mathbf{U}_2,\mathbf{R}).$$

Proof. Assume that $\mathbf{U}_i=\left[\mathbf{T}Rot(\frac{\mathbf{r}_i\mathbf{g}+\mathbf{e}}{\mathbf{z}^{\kappa}})\mathbf{T}^{-1}\right]_q$, $i\in[\![2]\!]$, and $\mathbf{R}=\mathbf{S}^{-1}Rot(\mathbf{b}'\mathbf{g}+\mathbf{e}')\mathbf{S}$ such that $\|\mathbf{r}_i\mathbf{g}+\mathbf{e}\|\le q^{1/8}$, $\|\mathbf{b}'\mathbf{g}+\mathbf{e}'\|\le n^{O(1)}$. Thus

$$
\begin{aligned}
\mathbf{V}_i &= \left[\mathbf{T}^*\cdot\mathbf{U}_i\cdot\mathbf{P}_{zt}\cdot\mathbf{R}\cdot\mathbf{S}^*\right]_q \\
&= \left[\mathbf{T}_1 Rot(\mathbf{r}_i\mathbf{g}(\mathbf{b}'\mathbf{g}+\mathbf{e}')\textstyle\sum_{j=1}^{m}\mathbf{h}_j\mathbf{g}_j^{-1})\mathbf{S}_1+\mathbf{T}_1 Rot(\sum_{j=1}^{m}\frac{\mathbf{h}_j\mathbf{e}(\mathbf{b}'\mathbf{g}+\mathbf{e}')}{\mathbf{g}_j})\mathbf{S}_1\right]_q \\
&= \left[\left[\mathbf{T}_1 Rot(\mathbf{r}_i\mathbf{g}(\mathbf{b}'\mathbf{g}+\mathbf{e}')\textstyle\sum_{j=1}^{m}\mathbf{h}_j\mathbf{g}_j^{-1})\mathbf{S}_1\right]_q+\left[\mathbf{T}_1 Rot(\sum_{j=1}^{m}\frac{\mathbf{h}_j\mathbf{e}(\mathbf{b}'\mathbf{g}+\mathbf{e}')}{\mathbf{g}_j})\mathbf{S}_1\right]_q\right]_q
\end{aligned}
.
$$

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

3.3 Security

Consider the following security experiment:

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

(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 $\mathbf{E}_l = \left[\sum_{i=1}^{\tau} d_{l,i}\mathbf{X}_i\right]_q$;

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

(3) Set $\mathbf{U} = \left[\prod_{j=1}^{\kappa}\mathbf{U}_j\right]_q$.

(4) Set $\mathbf{V}_C = \mathbf{V}_D = \left[\mathbf{T}^* \cdot \mathbf{U} \cdot \mathbf{P}_{zt} \cdot \mathbf{E}_0 \cdot \mathbf{S}^*\right]_q$.

(5) Set $\mathbf{V}_R = \left[\mathbf{T}^* \cdot \mathbf{U} \cdot \mathbf{P}_{zt} \cdot \mathbf{R}_0 \cdot \mathbf{S}^*\right]_q$, where $\mathbf{R}_0 = \left[\sum_{i=1}^{\tau} w_i\mathbf{X}_i\right]_q$ and $\mathbf{w} \leftarrow D_{\mathbb{Z}^{\tau},\sigma^*}$.

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 $\{\text{par}, \mathbf{U}_0, \cdots, \mathbf{U}_{\kappa}\}$, output a level-$\kappa$ extraction encoding $\mathbf{W} \in \mathbb{Z}_q^{k_1 \times k_2}$ such that $\left\|\left[\mathbf{V}_C - \mathbf{W}\right]_q\right\|_{\infty} \leq q^{3/4}$.

Level-κ extraction DDH (ext-GDDH): Given $\{\text{par}, \mathbf{U}_0, \cdots, \mathbf{U}_{\kappa}, \mathbf{V}\}$, distinguish between $D_{ext-GDDH} = \{\text{par}, \mathbf{U}_0, \cdots, \mathbf{U}_{\kappa}, \mathbf{V}_D\}$ and $D_{ext-RAND} = \{\text{par}, \mathbf{U}_0, \cdots, \mathbf{U}_{\kappa}, \mathbf{V}_R\}$.

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

On the one hand, encodings $\mathbf{Y}_i, \mathbf{X}_i$ encode same element $\mathbf{e}_i$, they cannot be directly multiplied. Since they are enveloped by different matrices $\mathbf{T}, \mathbf{S}$. To multiply them, we must use $\mathbf{P}_{zt}$. On the other hand, $\mathbf{Q}_{\delta}$ are encoding of zero. However, the random matrices $\mathbf{T}, \mathbf{S}$ are over modulo q. Thus, to eliminate $\mathbf{T}, \mathbf{S}$, we must compute the following expression: $\mathbf{V} = \left[\mathbf{T}^* \cdot \mathbf{U} \cdot \mathbf{P}_{zt} \cdot \mathbf{D} \cdot \mathbf{S}^*\right]_q$, where $\mathbf{U}$ is a level-κ encoding and $\mathbf{D}$ is a level-0 encoding.

To obtain easily computable quantities, we require that $\mathbf{U}$ is a level-κ encoding of zero.

(1) By using $\mathbf{Q}_{\delta}$, we compute $\mathbf{V}^{(1)} = \left[\mathbf{T}^* \cdot (\mathbf{Q}_{\delta})^{\kappa} \cdot \mathbf{P}_{zt} \cdot \mathbf{D} \cdot \mathbf{S}^*\right]_q$;

(2) By using cross-multiplication of $\mathbf{Y}_i, \mathbf{X}_i$, we compute

$$\mathbf{V}^{(2)} = \left[\mathbf{T}^* \cdot \mathbf{Y}_t^{\kappa-1}(\mathbf{Y}_i \cdot \mathbf{P}_{zt} \cdot \mathbf{X}_j - \mathbf{Y}_j \cdot \mathbf{P}_{zt} \cdot \mathbf{X}_i) \cdot \mathbf{S}^*\right]_q;$$

(3) By using mix-multiplication of $\mathbf{Q}_{\delta}$ and $\mathbf{Y}_i, \mathbf{X}_i$, we compute

$$\mathbf{V}^{(3)} = \left[\mathbf{T}^* \cdot (\mathbf{Q}_{\delta})^k \mathbf{Y}_t^{\kappa-1-k}(\mathbf{Y}_i \cdot \mathbf{P}_{zt} \cdot \mathbf{X}_j - \mathbf{Y}_j \cdot \mathbf{P}_{zt} \cdot \mathbf{X}_i) \cdot \mathbf{S}^*\right]_q;$$

$$\mathbf{V}^{(4)} = \left[\mathbf{T}^* \cdot (\mathbf{Q}_{\delta})^k \mathbf{Y}_i^{\kappa-k} \cdot \mathbf{P}_{zt} \cdot \mathbf{X}_j \cdot \mathbf{S}^*\right]_q.$$

By our parameter setting, it is easy to see that the matrices $\mathbf{V}^{(\varepsilon)}, \varepsilon \in [\![4]\!]$ are not reduced modulo q, namely $\left[\mathbf{V}^{(\varepsilon)}\right]_q = \mathbf{V}^{(\varepsilon)}$.

After simplification, $\mathbf{V}^{(\varepsilon)}, \varepsilon \in [\![4]\!]$ have the form $\mathbf{T}_1 Rot(\mathbf{r}\cdot\mathbf{g}^k)\mathbf{S}_1$, where $0 \le k < \kappa$ and $\mathbf{r} \in R$. By $\mathbf{T}_1 \in \mathbb{Z}^{k_1 \times n}$, $\mathbf{S}_1 \in \mathbb{Z}^{n \times k_2}$, and $Rot(\mathbf{r}\cdot\mathbf{g}^k) \in \mathbb{Z}^{n\times n}$, we get $\mathbf{V}^{(\varepsilon)} \in \mathbb{Z}^{k_1 \times k_2}$. It is easy to see that $\mathbf{V}^{(\varepsilon)}$ has destroyed the structure of the ring element $\mathbf{r}\cdot\mathbf{g}^k$, and does not have the property of the principal ideal lattice problem. We do not find feasible attacks by using $\mathbf{V}^{(\varepsilon)}$ for our construction.

Let $\mathbf{t}_i$ be the i-th row vector of $\mathbf{T}_1$, $\mathbf{s}_j$ be the j-th column vector of $\mathbf{S}_1$, and $\mathbf{m} = \mathbf{r}\cdot\mathbf{g}^k$. We define a function $f_{\mathbf{t},\mathbf{s}}(Rot(\mathbf{m})) = \mathbf{t}^T \cdot Rot(\mathbf{m}) \cdot \mathbf{s}$. Thus $v_{i,j}^{(\varepsilon)} = \mathbf{t}_i \cdot Rot(\mathbf{m}) \cdot \mathbf{s}_j$ is the entry of the i-th row and the j-th column of $\mathbf{V}^{(\varepsilon)}$. By arranging $\mathbf{t}^T \cdot Rot(\mathbf{m}) \cdot \mathbf{s}$, we can obtain a scalar product of $\mathbf{m}$ and $\mathbf{n}$, where $\mathbf{n}$ is determined by $\mathbf{t}$ and $\mathbf{s}$. However, we cannot find usable quantities from some $v_i = \mathbf{t}^T \cdot Rot(\mathbf{m}_i) \cdot \mathbf{s}$ when $\mathbf{t}, \mathbf{m}_i, \mathbf{s}$ are unknown.

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

$\mathbf{U}_j = \left[\sum_{i=1}^{\tau}(d_{j,i}\cdot \mathbf{Y}_i) + \sum_{i=1}^{\rho}(r_{j,i}\cdot \mathbf{Q}_i)\right]_q$ and generates the secret key $\mathbf{D}_j = \left[\sum_{i=1}^{\tau}(d_{j,i}\cdot \mathbf{X}_i)\right]_q$.

KeyGen$(\text{par}, j, \mathbf{D}_j, \{\mathbf{U}_k\}_{k\neq j})$. The j-th party computes $\mathbf{C}_j = \prod_{k\neq j}\mathbf{U}_k$ and extracts the common secret key $sk = \text{ext}(\text{par}, \mathbf{D}_j, \mathbf{C}_j) = \text{Extract}(\text{msb}(\left[\mathbf{T}^* \cdot \mathbf{C}_j \cdot \mathbf{P}_{zt} \cdot \mathbf{D}_j \cdot \mathbf{S}^*\right]_q))$.

Theorem 5.1 Suppose the ext-GCDH/ext-GDDH defined in Section 3.2 is hard, then our construction is one round multipartite Diffie-Hellman key exchange protocol.

5.2 Witness Encryption

Given an instance $inst$ of 3-exact cover problem, which includes a number K and a collection Set of subsets $T_1, T_2, ..., T_\pi \subset [\![K]\!]$, 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 $[\![K]\!]$ for $inst$.

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

(1) For $j \in [\![K]\!]$, sample $\mathbf{d}_j \leftarrow D_{Z^\tau,\sigma}$, $\mathbf{r}_j \leftarrow D_{\mathbb{Z}^\rho,\sigma^*}$ and generate level-1 encodings $\mathbf{U}_k = \left[\sum_{i=1}^{\tau} d_{k,i}\mathbf{Y}_i + \sum_{i=1}^{\rho}(r_{k,i}\cdot \mathbf{Q}_i)\right]_q$.

(2) Compute $\mathbf{U} = \left[\prod_{k=1}^{K}\mathbf{U}_k\right]_q$ and $sk = \text{Ext}(\text{par}, \mathbf{I}, \mathbf{U})$ and encrypt M into ciphertext C, where $\mathbf{I}$ is an identity matrix.

(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 $\mathbf{U}_{T_i} = \left[\mathbf{U}_{i_1}\mathbf{U}_{i_2}\mathbf{U}_{i_3} + \sum_{\delta=1}^{\rho} r_{T_i,\delta}(\mathbf{Q}_\delta)^3\right]_q$, where .

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

Decrypt$(inst, W, C, E)$:

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

(2) Generate $sk = \text{Ext}(\text{par}, \mathbf{I}, \mathbf{U})$, and decrypt C to obtain 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.

It is easy to verify that our WE construction cannot be broken by using the attack methods in [HJ15a, HJ15b].

6 Conclusion and open problem

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.

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

[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.

[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.

[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.

[HAO14] R. Hiromasa, M. Abe and T. Okamoto. Multilinear Maps on LWE. SCIS 2014, pp. 1-8.

[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.