New multilinear maps from ideal lattices

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

Jul 23, 2015

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

1 Introduction

There are at present only three constructions of multilinear maps [GGH13, CLT13, GGH15]. The first candidate construction of multilinear maps is presented by Garg, Gentry, and Halevi (GGH) [GGH13]. Soon after, Coron, Lepoint, and Tibouchi [CLT13] (CLT) described a construction over the integers using same framework of GGH. Recently, Gentry, Gorbunov and Halevi [GGH15] constructed graph-induced multilinear maps from lattices.

However, the zeroizing attacks for CLT and GGH demonstrate that previous constructions require further improvement. 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 variant of the 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. Currently, an open problem is how to fix the GGH map, whilst still maintaining functionality of the original GGH.

Our results.

We first briefly recall the GGH map. The GGH map works in a polynomial ring $R=\mathbb{Z}[x]/\langle x^n+1\rangle$, where n is a positive integer. A random large integer q, a secret short ring element $\mathbf{g}\in R$, and a secret random element $\mathbf{z}_1\in R_q=R/qR$ are chosen during construction, where $\mathbf{g}$ generates a principal ideal $I=\langle\mathbf{g}\rangle\subset R$ and $\mathbf{z}$ is invertible in R_q. Elements in R/I are encoded as follows: a level-k encoding of the coset $e_I=\mathbf{e}+I$ is an element of the form $\left[\mathbf{c}/\mathbf{z}_1^k\right]_q$, where the $\mathbf{c} \in e_I$ norm is short. Encodings can both be added and multiplied if the numerator norm remains smaller than q. For a level-κ encoding $\mathbf{u} = \left[\mathbf{c}/\mathbf{z}_1^{\kappa}\right]_q$, the encoding $\mathbf{u}$ can be determined as zero by computing $\left[\mathbf{u} \cdot \mathbf{p}_{zt}\right]_q$, where $\mathbf{p}_{zt} = \left[\mathbf{h}_1 \mathbf{z}_1^{\kappa} / \mathbf{g}\right]_q$ is a zero-testing parameter. If the norm of $\left[\mathbf{u} \cdot \mathbf{p}_{zt}\right]_q$ is small, then $\mathbf{u}$ is the encoding of zero; otherwise, $\mathbf{u}$ is the encoding of non-zero.

Our main contribution is to construct a new multilinear map using ideal lattices. Our construction improves the origin GGH map in three aspects.

(1) We introduce new noise term to avoid the zeroizing attack problem of GGH. Let $\text{par}_0 = \left\{q, \mathbf{y}_1 = \left[(1+\mathbf{ag})/\mathbf{z}_1\right]_q, \mathbf{x}_{1,i} = \left[(\mathbf{a}_{1,i}\mathbf{g})/\mathbf{z}_1\right]_q, i \in [\![\tau]\!], \mathbf{p}_{zt} = \left[\mathbf{h}_1 \mathbf{z}_1^{\kappa} / \mathbf{g}\right]_q\right\}$ be the public parameters of GGH. Given arbitrary level-k encoding $\mathbf{u} = \left[\mathbf{c}/\mathbf{z}_1^k\right]_q$, one can compute $\mathbf{v}_{k,i,j} = \left[\mathbf{u} \cdot \mathbf{x}_{1,i}^j \cdot \mathbf{y}_1^{\kappa-k-j} \cdot \mathbf{p}_{zt}\right]_q = \left[\mathbf{h}_1 \cdot \mathbf{c} \cdot (\mathbf{a}_{1,i})^j \mathbf{g}^{j-1} (1+\mathbf{ag})^{\kappa-k-j}\right]_q$, where $1 \le k < \kappa, 1 \le j < \kappa$ and $k + j \le \kappa$ using so-called zeroizing attack method. It is easy to verify that $\mathbf{v}_{k,i,j}$ is not reduced modulo q. As a result, one one can compute a basis of the secret ring element $\mathbf{g}$. Using this method, Hu and Jia [HJ15a] have broken two applications of MPKE and WE based on GGH. To improve GGH and avoid the zeroizing attack, one needs to introduce new noise term for $\mathbf{v}_{k,i,j}$. If one can add a random noise to $\mathbf{v}_{k,i,j}$, then adversary cannot yield a basis of $\mathbf{g}$. We introduce a new ring element $\mathbf{f}$ in our construction to achieve this goal.

(2) We use two zero testing parameters to introduce new noise term. We change $\mathbf{p}_{zt}$ into $\mathbf{p}_{zt,1} = \left[\mathbf{z}_1^{\kappa}(\mathbf{h}_1/\mathbf{g} + \mathbf{h}_2/\mathbf{f})\right]_q$. The problem is how to remove encoding of non-zero element for ideal lattice $\langle \mathbf{f} \rangle$. Roughly speaking, one must generate encoding of zero for $\langle \mathbf{f} \rangle$. For this purpose, we generate some encodings $\mathbf{y}_2 = \left[(\mathbf{e} + \mathbf{b}_2\mathbf{f})/\mathbf{z}_2\right]_q, \mathbf{x}_{2,i} = \left[(\mathbf{e}_i + \mathbf{b}_{2,i}\mathbf{f})/\mathbf{z}_2\right]_q, i \in [\![\tau]\!]$ such that $\mathbf{e} = (1+\mathbf{ag}) \bmod \mathbf{f}$ and $\mathbf{e}_i = (\mathbf{a}_i\mathbf{g}) \bmod \mathbf{f}$. To obtain encoding of zero for $\langle \mathbf{f} \rangle$, we generate another zero testing parameter $\mathbf{p}_{zt,2} = \left[\mathbf{z}_2^{\kappa}(\mathbf{h}_2 + \mathbf{hf})/\mathbf{f}\right]_q$. When generating a level-k encoding $\mathbf{u}_1 = \left[\mathbf{c}_1/\mathbf{z}_1^k\right]_q$, one also generates its corresponding level-k encoding $\mathbf{u}_2 = \left[\mathbf{c}_2/\mathbf{z}_2^k\right]_q$ such that $\mathbf{c}_1 = \mathbf{c}_2 \bmod \mathbf{f}$. Hence, given a level-$\kappa$ encoding $(\mathbf{u}_1, \mathbf{u}_2)$, we can determine whether the encoding of $\mathbf{u}_1$ is zero for $\langle \mathbf{g} \rangle$ by computing $\left[\mathbf{u}_1 \cdot \mathbf{p}_{zt,1} - \mathbf{u}_2 \cdot \mathbf{p}_{zt,2}\right]_q$. Now, given arbitrary level-k encoding $(\mathbf{u}_1, \mathbf{u}_2)$, one can compute $\mathbf{v}_{k,i,j} = \left[\mathbf{u}_1 \cdot \mathbf{x}_{1,i}^j \cdot \mathbf{y}_1^{\kappa-k-j} \cdot \mathbf{p}_{zt,1} - \mathbf{u}_2 \cdot \mathbf{x}_{2,i}^j \cdot \mathbf{y}_2^{\kappa-k-j} \cdot \mathbf{p}_{zt,2}\right]_q$, where $1 \le k < \kappa$, $1 \le j < \kappa$ and $k + j \le \kappa$ using zeroizing attack method. Although $\mathbf{v}_{k,i,j}$ is not reduced modulo q, one can no longer obtain a basis of $\mathbf{g}$ using $\mathbf{v}_{k,i,j}$.

(3) Our new construction seemly supports more applications than the original GGH. Owing to adding new noise term, one can no longer yield a basis of $\mathbf{g}$. Hence, we conjecture that the membership group problem (SubM) and the decisional linear (DLIN) problem are hard in our construction. However, in the original GGH map, one can compute non-reduced ring elements over modulus q and a basis of $\mathbf{g}$. 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 new multilinear map. Since these applications are attacked by [HJ15a], fix for them is urgently required.

The MPKE and WE based on our new map are same as ones using the GGH map.

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

2 Preliminaries

2.1 Notations

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

2.2 Lattices and Ideal Lattices

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

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

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

2.3 Multilinear Maps

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

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

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

(2) Map e is non-degenerate in the following sense: if elements $\{g_j \in G_j\}_{j=1,\dots,\kappa}$ 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 New Construction

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

3.1 Construction

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

(1) Choose a prime $q \ge 2^{8\kappa\lambda} n^{O(\kappa)}$.

(2) Choose $\mathbf{g},\mathbf{f} \leftarrow D_{\mathbb{Z}^n,\sigma}$ in R so that $\left\|\mathbf{g}^{-1}\right\| < n^2$ and $\left\|\mathbf{f}^{-1}\right\| < n^2$.

(3) Choose $\mathbf{a}_{1,i}, \mathbf{b}_{2,i} \leftarrow D_{\mathbb{Z}^n,\sigma'}, i \in [\![\tau]\!]$ in R;

Choose $\mathbf{a}_1, \mathbf{b}_2 \leftarrow D_{\mathbb{Z}^n,\sigma'}$ and $\mathbf{h},\mathbf{h}_1,\mathbf{h}_2 \leftarrow D_{\mathbb{Z}^n,\sqrt{q}}$ in R.

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

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

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

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

$\mathbf{y}_2 = \left[\dfrac{\mathbf{b}_2\mathbf{f}+\mathbf{e}_1}{\mathbf{z}_2}\right]_q$ and $\mathbf{x}_{2,i} = \left[\dfrac{\mathbf{b}_{2,i}\mathbf{f}+\mathbf{e}_{1,i}}{\mathbf{z}_2}\right]_q$.

(7) Set $\mathbf{p}_{zt,1} = \left[\mathbf{z}_1^\kappa\left(\mathbf{h}_1\mathbf{g}^{-1}+\mathbf{h}_2\mathbf{f}^{-1}\right)\right]_q$, $\mathbf{p}_{zt,2} = \left[\mathbf{z}_2^\kappa(\mathbf{h}_2+\mathbf{hf})\mathbf{f}^{-1}\right]_q$.

(8) Output the public parameters $\text{par} = \left\{q, \left\{\mathbf{y}_t, \left\{\mathbf{x}_{t,i}\right\}_{i\in[\![\tau]\!]}, \mathbf{p}_{zt,t}\right\}_{t\in[\![2]\!]}\right\}$.

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

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

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

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

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

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

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

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

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

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

Zero testing: $\mathrm{isZero}(\mathrm{par},(\mathbf{u}_1,\mathbf{u}_2))$.

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 $\mathbf{v}=[\mathbf{u}_1\cdot\mathbf{p}_{zt,1}-\mathbf{u}_2\cdot\mathbf{p}_{zt,2}]_q$ and check whether $\|\mathbf{v}\|$ is short:

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

Extraction: $sk\leftarrow \mathrm{Ext}(\mathrm{par},(\mathbf{u}_1,\mathbf{u}_2))$.

Given a level-κ encoding $(\mathbf{u}_1,\mathbf{u}_2)$, we compute $\mathbf{v}=[\mathbf{u}_1\cdot\mathbf{p}_{zt,1}-\mathbf{u}_2\cdot\mathbf{p}_{zt,2}]_q$, and collect $\eta=(\log q)/4-\lambda$ most-significant bits of each of the n coefficients of $\mathbf{v}$:

$$\mathrm{Ext}(\mathrm{par},(\mathbf{u}_1,\mathbf{u}_2))=\mathrm{Extract}_s\left(\mathrm{msbs}_\eta\left([\mathbf{u}_1\cdot\mathbf{p}_{zt,1}-\mathbf{u}_2\cdot\mathbf{p}_{zt,2}]_q\right)\right).$$

Remark 3.1 (1) One can only use one zero-testing parameter to introduce new noise term. We briefly describe this variant as follows. After running steps (1)-(7) of $\mathrm{InstGen}(1^\lambda,1^\kappa)$, one first generates a pair of special encoding $(\mathbf{p}_1,\mathbf{p}_2)$ with $\mathbf{p}_1=\left[\frac{\mathbf{m}_1\mathbf{fg}+1}{\mathbf{z}\cdot\mathbf{z}_2^\kappa}\right]_q$ and $\mathbf{p}_2=\left[\frac{\mathbf{m}_2\mathbf{gn}}{\mathbf{z}\cdot\mathbf{z}_1^\kappa}\right]_q$ such that $\mathbf{m}_2\mathbf{gn}=1\bmod\mathbf{f}$, where $\mathbf{m}_1,\mathbf{m}_2\leftarrow D_{\mathbb{Z}^n,\sigma'}$, and an invertible random element $\mathbf{z}\leftarrow R_q$. To obtain $\mathbf{n}$ over R, one computes $\mathbf{m}_2\mathbf{g}=\mathbf{rf}+\mathbf{k}$, and solves an inverse element $\mathbf{n}$ of $\mathbf{k}$ for $\mathbf{f}$ so that $\mathbf{n}\cdot\mathbf{k}=1\bmod\mathbf{f}$ and $\|\mathbf{n}\|\le\|\mathbf{f}\|$. Then, one sets $\mathbf{p}_{zt}=\mathbf{z}\cdot\mathbf{z}_2^\kappa\cdot\mathbf{p}_{zt,1}=\left[\mathbf{z}\cdot\mathbf{z}_1^\kappa\cdot\mathbf{z}_2^\kappa\left(\mathbf{h}_1\mathbf{g}^{-1}+\mathbf{h}_2\mathbf{f}^{-1}\right)\right]_q$. Finally, one outputs the public parameters $\mathrm{par}=\left\{q,\left\{\mathbf{y}_t,\{\mathbf{x}_{t,i}\}_{i\in[\![\tau]\!]},\mathbf{p}_t\right\}_{t\in[\![2]\!]},\mathbf{p}_{zt}\right\}$. Now, given a level-$\kappa$ encoding $(\mathbf{u}_1,\mathbf{u}_2)$, one computes $\mathbf{v}=[(\mathbf{u}_1\cdot\mathbf{p}_1-\mathbf{u}_2\cdot\mathbf{p}_2)\cdot\mathbf{p}_{zt}]_q$ and check whether $\|\mathbf{v}\|<q^{3/4}$. It is easy to verify that this variant construction is correct and avoids the zeroizing attack problem of GGH. We observe that this variant in some sense is also a modification of the zero-immunizing transformation described by Boneh, Wu, and Zimmerman [BWZ14]. However, the difference between our variant and their transformation is from method introducing new noise term. In fact, to add new noise, our variant mainly modifies zero testing parameter, whereas their transformation adds new factor for modulo.

(2) We can also improve the CLT map [CLT13] using the methods of our construction.

(3) The level-1 encoding $\mathbf{y}_1 = \left[\frac{\mathbf{b}_1\mathbf{g}+1}{\mathbf{z}_1}\right]_q$ can be set to $\mathbf{y}_1' = \left[\frac{\mathbf{b}_1\mathbf{g}+\mathbf{e}_1}{\mathbf{z}_1}\right]_q$. Of course, in this case, we take $\mathbf{e}_2 = (\mathbf{b}_1\mathbf{g}+\mathbf{e}_1) \bmod \mathbf{f}$.

(4) The zero testing parameter $\mathbf{p}_{zt,2} = \left[\mathbf{z}_2^{\kappa}(\mathbf{h}_2+\mathbf{hf})\mathbf{f}^{-1}\right]_q$ can be set to $\mathbf{p}_{zt,2}' = \left[\mathbf{z}_2^{\kappa}\mathbf{h}_2\mathbf{f}^{-1}\right]_q$. Here our aim is to further damage the relationship between $\mathbf{p}_{zt,1}$ and $\mathbf{p}_{zt,2}$.

3.2 Correctness

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

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

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

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

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

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

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

(2) Similarly, for $\langle \mathbf{f} \rangle$ we have

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

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

The level-k encodings $\mathbf{u}_1,\mathbf{u}_2$ encode same level-0 encoding for $\langle \mathbf{f} \rangle$ □

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

encoding.

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

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

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

Namely, $\mathbf{u}_1$ is a level-k encoding for $\langle \mathbf{g} \rangle$.

Again for $\mathbf{f}$, the level-k encoding $\mathbf{u}_{t,l}$ has the form $\mathbf{u}_{t,l} = \left[\frac{\mathbf{c}_{t,l} \mathbf{f} + \mathbf{e}_l}{\mathbf{z}_t^k} \right]_q$. Thus, we have

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

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

That is, level-k encodings $\mathbf{u}_1, \mathbf{u}_2$ encode same level-0 encoding for $\langle \mathbf{f} \rangle$. □

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

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

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

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

Again for $\langle \mathbf{f} \rangle$, the level-$1$ encoding $\mathbf{u}_{t,l}$ has the form $\mathbf{u}_{t,l} = \left[\frac{\mathbf{c}_{t,l} \mathbf{f} + \mathbf{e}_l}{\mathbf{z}_t} \right]_q$. Thus, we have

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

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

Lemma 3.6 The zero testing $\mathrm{isZero}\left(\mathrm{par}, (\mathbf{u}_1, \mathbf{u}_2)\right)$ correctly determines whether $\mathbf{u}_1$ is a level-κ encoding of zero for $\langle \mathbf{g} \rangle$.

Proof. Given a level-κ encoding $(\mathbf{u}_1, \mathbf{u}_2)$, we compute $\mathbf{v} = \left[\mathbf{u}_1 \cdot \mathbf{p}_{zt,1} - \mathbf{u}_2 \cdot \mathbf{p}_{zt,2} \right]_q$ and check whether $\|\mathbf{v}\|$ is short:

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

If $\mathbf{u}_1$ is a level-κ encoding of zero for $\langle \mathbf{g} \rangle$, namely $\mathbf{u}_1 = \left[\dfrac{\mathbf{rg}}{\mathbf{z}_1^\kappa}\right]_q$. Since $\mathbf{u}_t = \left[\dfrac{\mathbf{c}_t\mathbf{f}+\mathbf{e}}{\mathbf{z}_t^\kappa}\right]_q$ for any level-κ encoding $(\mathbf{u}_1, \mathbf{u}_2)$. Thus, we have

$$\begin{aligned}
\mathbf{v} &= \left[\mathbf{u}_1 \cdot \mathbf{p}_{zt,1} - \mathbf{u}_2 \cdot \mathbf{p}_{zt,2}\right]_q \\
&= \left[\mathbf{u}_1 \cdot \mathbf{z}_1^\kappa \left(\mathbf{h}_1\mathbf{g}^{-1} + \mathbf{h}_2\mathbf{f}^{-1}\right) - \mathbf{u}_2 \cdot \mathbf{z}_2^\kappa (\mathbf{h}_2 + \mathbf{hf})\mathbf{f}^{-1}\right]_q \\
&= \left[\mathbf{u}_1 \cdot \mathbf{z}_1^\kappa \mathbf{h}_1\mathbf{g}^{-1} + \mathbf{u}_1 \cdot \mathbf{z}_1^\kappa \mathbf{h}_2\mathbf{f}^{-1} - \mathbf{u}_2 \cdot \mathbf{z}_2^\kappa (\mathbf{h}_2 + \mathbf{hf})\mathbf{f}^{-1}\right]_q \\
&= \left[\frac{\mathbf{rg}}{\mathbf{z}_1^\kappa} \cdot \mathbf{z}_1^\kappa \mathbf{h}_1\mathbf{g}^{-1} + \frac{\mathbf{c}_1\mathbf{f}+\mathbf{e}}{\mathbf{z}_1^\kappa} \cdot \mathbf{z}_1^\kappa \mathbf{h}_2\mathbf{f}^{-1} - \frac{\mathbf{c}_2\mathbf{f}+\mathbf{e}}{\mathbf{z}_2^\kappa} \cdot \mathbf{z}_2^\kappa (\mathbf{h}_2 + \mathbf{hf})\mathbf{f}^{-1}\right]_q . \\
&= \left[\mathbf{rgh}_1\mathbf{g}^{-1} + (\mathbf{c}_1\mathbf{f}+\mathbf{e})\mathbf{h}_2\mathbf{f}^{-1} - (\mathbf{c}_2\mathbf{f}+\mathbf{e})(\mathbf{h}_2 + \mathbf{hf})\mathbf{f}^{-1}\right]_q \\
&= \left[\mathbf{rh}_1 + \mathbf{c}_1\mathbf{h}_2 - \mathbf{c}_2\mathbf{h}_2 - (\mathbf{c}_2\mathbf{f}+\mathbf{e})\mathbf{h}\right]_q
\end{aligned}$$

For our choice of parameter, $\|\mathbf{r}\| < q^{1/8}$, $\|\mathbf{c}_1\| < q^{1/8}$, $\|\mathbf{c}_2\| < q^{1/8}$, $\|\mathbf{c}_2\mathbf{f}+\mathbf{e}\| < q^{1/8}$, and $\|\mathbf{h}\| < n^{O(1)}q^{1/2}, \|\mathbf{h}_1\| < n^{O(1)}q^{1/2}, \|\mathbf{h}_2\| < n^{O(1)}q^{1/2}$. Moreover, $\mathbf{v}$ is not reduced modulo q, that is $[\mathbf{v}]_q = \mathbf{v}$. Hence,

$$\begin{aligned}
\|\mathbf{v}\| &= \left\|\left[\mathbf{rh}_1 + \mathbf{c}_1\mathbf{h}_2 - \mathbf{c}_2\mathbf{h}_2 - (\mathbf{c}_2\mathbf{f}+\mathbf{e})\mathbf{h}\right]_q\right\| \\
&= \left\|\mathbf{rh}_1 + \mathbf{c}_1\mathbf{h}_2 - \mathbf{c}_2\mathbf{h}_2 - (\mathbf{c}_2\mathbf{f}+\mathbf{e})\mathbf{h}\right\| \\
&\le \|\mathbf{rh}_1\| + \|\mathbf{c}_1\mathbf{h}_2\| + \|\mathbf{c}_2\mathbf{h}_2\| + \|(\mathbf{c}_2\mathbf{f}+\mathbf{e})\mathbf{h}\|. \\
&= 4n^{O(1)} \cdot q^{1/8} \cdot n^{O(1)} \cdot q^{1/2} \\
&< q^{3/4}
\end{aligned}$$

If $\mathbf{u}_1$ is a level-κ encoding of non-zero element for $\langle \mathbf{g} \rangle$. Namely $\mathbf{u}_1 = \left[\dfrac{\mathbf{rg}+\mathbf{d}}{\mathbf{z}_1^\kappa}\right]_q$ with $\mathbf{d} \neq 0 \bmod \mathbf{g}$ and $\|\mathbf{d}\| \le \|\mathbf{g}\|$. Thus,

$$\begin{aligned}
\mathbf{v} &= \left[\mathbf{u}_1 \cdot \mathbf{p}_{zt,1} - \mathbf{u}_2 \cdot \mathbf{p}_{zt,2}\right]_q \\
&= \left[\mathbf{u}_1 \cdot \mathbf{z}_1^\kappa \left(\mathbf{h}_1\mathbf{g}^{-1} + \mathbf{h}_2\mathbf{f}^{-1}\right) - \mathbf{u}_2 \cdot \mathbf{z}_2^\kappa (\mathbf{h}_2 + \mathbf{hf})\mathbf{f}^{-1}\right]_q \\
&= \left[\mathbf{u}_1 \cdot \mathbf{z}_1^\kappa \mathbf{h}_1\mathbf{g}^{-1} + \mathbf{u}_1 \cdot \mathbf{z}_1^\kappa \mathbf{h}_2\mathbf{f}^{-1} - \mathbf{u}_2 \cdot \mathbf{z}_2^\kappa (\mathbf{h}_2 + \mathbf{hf})\mathbf{f}^{-1}\right]_q \\
&= \left[\frac{\mathbf{rg}+\mathbf{d}}{\mathbf{z}_1^\kappa} \cdot \mathbf{z}_1^\kappa \mathbf{h}_1\mathbf{g}^{-1} + \frac{\mathbf{c}_1\mathbf{f}+\mathbf{e}}{\mathbf{z}_1^\kappa} \cdot \mathbf{z}_1^\kappa \mathbf{h}_2\mathbf{f}^{-1} - \frac{\mathbf{c}_2\mathbf{f}+\mathbf{e}}{\mathbf{z}_2^\kappa} \cdot \mathbf{z}_2^\kappa (\mathbf{h}_2 + \mathbf{hf})\mathbf{f}^{-1}\right]_q . \\
&= \left[(\mathbf{rg}+\mathbf{d})\mathbf{h}_1\mathbf{g}^{-1} + (\mathbf{c}_1\mathbf{f}+\mathbf{e})\mathbf{h}_2\mathbf{f}^{-1} - (\mathbf{c}_2\mathbf{f}+\mathbf{e})(\mathbf{h}_2 + \mathbf{hf})\mathbf{f}^{-1}\right]_q \\
&= \left[\mathbf{dh}_1\mathbf{g}^{-1} + \mathbf{rh}_1 + \mathbf{c}_1\mathbf{h}_2 - \mathbf{c}_2\mathbf{h}_2 - (\mathbf{c}_2\mathbf{f}+\mathbf{e})\mathbf{h}\right]_q
\end{aligned}$$

By Lemma 4 in [GGH13], $\left\|\left[\mathbf{dh}_1\mathbf{g}^{-1}\right]_q\right\| \approx q$. Thus we have $\|\mathbf{v}\| \approx q$. □

Lemma 3.7 Given two level-κ encodings $(\mathbf{u}_{1,1}, \mathbf{u}_{2,1}), (\mathbf{u}_{1,2}, \mathbf{u}_{2,2})$, suppose that $\mathbf{u}_{1,1}, \mathbf{u}_{1,2}$ encode same plaintext, then

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

Proof. Let $\mathbf{u}_{1,s}=\left[\frac{\mathbf{r}_s\mathbf{g}+\mathbf{d}}{\mathbf{z}_1^{\kappa}}\right]_q=\left[\frac{\mathbf{c}_{1,s}\mathbf{f}+\mathbf{e}_s}{\mathbf{z}_1^{\kappa}}\right]_q$, $s\in[\![2]\!]$ so that $\|\mathbf{r}_s\mathbf{g}+\mathbf{d}\|\le q^{1/8}$, and $\mathbf{u}_{2,s}=\left[\frac{\mathbf{c}_{2,s}\mathbf{f}+\mathbf{e}_s}{\mathbf{z}_2^{\kappa}}\right]_q$, $s\in[\![2]\!]$. Thus, we have

$$\begin{aligned}\mathbf{v}_s &=\left[\mathbf{u}_{1,s}\cdot\mathbf{p}_{zt,1}-\mathbf{u}_{2,s}\cdot\mathbf{p}_{zt,2}\right]_q\\ &=\left[\mathbf{u}_{1,s}\cdot\mathbf{z}_1^{\kappa}\left(\mathbf{h}_1\mathbf{g}^{-1}+\mathbf{h}_2\mathbf{f}^{-1}\right)-\mathbf{u}_{2,s}\cdot\mathbf{z}_2^{\kappa}(\mathbf{h}_2+\mathbf{h}\mathbf{f})\mathbf{f}^{-1}\right]_q\\ &=\left[\mathbf{u}_{1,s}\cdot\mathbf{z}_1^{\kappa}\mathbf{h}_1\mathbf{g}^{-1}+\mathbf{u}_{1,s}\cdot\mathbf{z}_1^{\kappa}\mathbf{h}_2\mathbf{f}^{-1}-\mathbf{u}_{2,s}\cdot\mathbf{z}_2^{\kappa}(\mathbf{h}_2+\mathbf{h}\mathbf{f})\mathbf{f}^{-1}\right]_q\\ &=\left[\frac{\mathbf{r}_s\mathbf{g}+\mathbf{d}}{\mathbf{z}_1^{\kappa}}\cdot\mathbf{z}_1^{\kappa}\mathbf{h}_1\mathbf{g}^{-1}+\frac{\mathbf{c}_{1,s}\mathbf{f}+\mathbf{e}_s}{\mathbf{z}_1^{\kappa}}\cdot\mathbf{z}_1^{\kappa}\mathbf{h}_2\mathbf{f}^{-1}-\frac{\mathbf{c}_{2,s}\mathbf{f}+\mathbf{e}_s}{\mathbf{z}_2^{\kappa}}\cdot\mathbf{z}_2^{\kappa}(\mathbf{h}_2+\mathbf{h}\mathbf{f})\mathbf{f}^{-1}\right]_q\\ &=\left[(\mathbf{r}_s\mathbf{g}+\mathbf{d})\mathbf{h}_1\mathbf{g}^{-1}+(\mathbf{c}_{1,s}\mathbf{f}+\mathbf{e}_s)\mathbf{h}_2\mathbf{f}^{-1}-(\mathbf{c}_{2,s}\mathbf{f}+\mathbf{e}_s)(\mathbf{h}_2+\mathbf{h}\mathbf{f})\mathbf{f}^{-1}\right]_q\\ &=\left[\mathbf{d}\mathbf{h}_1\mathbf{g}^{-1}+\mathbf{r}_s\mathbf{h}_1+\mathbf{c}_{1,s}\mathbf{h}_2-\mathbf{c}_{2,s}\mathbf{h}_2-(\mathbf{c}_{2,s}\mathbf{f}+\mathbf{e}_s)\mathbf{h}\right]_q\end{aligned}$$

For our parameter setting, $\left\|\left[\mathbf{r}_s\mathbf{h}_1+\mathbf{c}_{1,s}\mathbf{h}_2-\mathbf{c}_{2,s}\mathbf{h}_2-(\mathbf{c}_{2,s}\mathbf{f}+\mathbf{e}_s)\mathbf{h}\right]_q\right\|<q^{3/4}$. By Lemma 4 in [GGH13], $\left\|\left[\mathbf{d}\mathbf{h}_1\mathbf{g}^{-1}\right]_q\right\|\approx q$ when $\mathbf{d}\ne 0 \bmod \mathbf{g}$. 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 $\mathbf{d}_l\leftarrow D_{\mathbb{Z}^n,\sigma'}$, $\mathbf{r}_{l,i}\leftarrow D_{\mathbb{Z}^n,\sigma^*}$;

Generate level-1 encoding $\mathbf{u}_{t,l}=\left[\mathbf{d}_l\mathbf{y}_t+\sum_{i=1}^{\tau}\mathbf{r}_{l,i}\mathbf{x}_{t,i}\right]_q$, $t\in[\![2]\!]$.

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

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

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

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 $\left\{\mathrm{par},\left(\mathbf{u}_{1,1},\mathbf{u}_{2,1}\right),\cdots,\left(\mathbf{u}_{1,\kappa},\mathbf{u}_{2,\kappa}\right)\right\}$, output a level-$\kappa$ extraction encoding $\mathbf{w}\in R_q$ such that $\left\|\left[\mathbf{v}_C-\mathbf{w}\right]_q\right\|_\infty\le q^{3/4}$.

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

3.4 Cryptanalysis

In this section, we give easily computable some quantities in our construction, and analyze possible attacks using these quantities.

3.4.1 Easily computable quantities

The encodings $\mathbf{y}_1, \mathbf{x}_{1,i}$ in the public parameters are same as that of GGH for the ideal lattice $\langle \mathbf{g} \rangle$. However, the zero testing parameter $\mathbf{p}_{zt,1}$, which is different from one of GGH, includes $\mathbf{z}_1^{\kappa} \mathbf{h}_2 \mathbf{f}^{-1}$. As a result, the encodings $\mathbf{x}_{1,i}$ of zero for $\langle \mathbf{g} \rangle$ are not any more encoding of zero for $\langle \mathbf{f} \rangle$. Although the non-zero plaintexts encoded by $\mathbf{y}_1, \mathbf{x}_{1,i}$ are one-to-one corresponding to ones encoded by $\mathbf{y}_2, \mathbf{x}_{2,i}$ for $\langle \mathbf{f} \rangle$, respectively, they cannot be subtracted to obtain encoding of zero for $\langle \mathbf{f} \rangle$. This is because that random element $\mathbf{z}_1$ using as level number of encoding is not equal to $\mathbf{z}_2$. That is, one must use zero testing parameter $\mathbf{p}_{zt,2}$ to remove the non-zero level-0 encodings in $\mathbf{y}_1, \mathbf{x}_{1,i}$. Thus, one can only get easily computable quantities in the following form.

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

$$\mathbf{v} = \left[\mathbf{u}_1 \cdot (\mathbf{x}_{1,i})^j \cdot (\mathbf{y}_1)^{\kappa-k-j} \cdot \mathbf{p}_{zt,1} - \mathbf{u}_2 \cdot (\mathbf{x}_{2,i})^j \cdot (\mathbf{y}_2)^{\kappa-k-j} \cdot \mathbf{p}_{zt,2} \right]_q.$$

Without loss of generality, let $\mathbf{u}_1 = \left[\frac{\mathbf{w}}{\mathbf{z}_1^k} \right]_q = \left[\frac{\mathbf{r}_1 \mathbf{g} + \mathbf{d}}{\mathbf{z}_1^k} \right]_q = \left[\frac{\mathbf{c}_1 \mathbf{f} + \mathbf{e}}{\mathbf{z}_1^k} \right]_q$ and $\mathbf{u}_2 = \left[\frac{\mathbf{c}_2 \mathbf{f} + \mathbf{e}}{\mathbf{z}_2^k} \right]_q$. Hence,

$$\begin{aligned}
\mathbf{v} &= \left[\mathbf{u}_1 \cdot (\mathbf{x}_{1,i})^j \cdot (\mathbf{y}_1)^{\kappa-k-j} \cdot \mathbf{p}_{zt,1} - \mathbf{u}_2 \cdot (\mathbf{x}_{2,i})^j \cdot (\mathbf{y}_2)^{\kappa-k-j} \cdot \mathbf{p}_{zt,2} \right]_q \\
&= \begin{bmatrix} \frac{\mathbf{w}}{\mathbf{z}_1^k} \cdot (\frac{\mathbf{a}_{1,i}\mathbf{g}}{\mathbf{z}_1})^j \cdot (\frac{\mathbf{a}_1\mathbf{g}+1}{\mathbf{z}_1})^{\kappa-k-j} \cdot \mathbf{z}_1^{\kappa} \mathbf{h}_1 \mathbf{g}^{-1} \\ + \frac{\mathbf{c}_1\mathbf{f}+\mathbf{e}}{\mathbf{z}_1^k} \cdot (\frac{\mathbf{b}_{1,i}\mathbf{f}+\mathbf{e}_{1,i}}{\mathbf{z}_1})^j \cdot (\frac{\mathbf{b}_1\mathbf{f}+\mathbf{e}_1}{\mathbf{z}_1})^{\kappa-k-j} \cdot \mathbf{z}_1^{\kappa} \mathbf{h}_2 \mathbf{f}^{-1} \\ - \frac{\mathbf{c}_2\mathbf{f}+\mathbf{e}}{\mathbf{z}_2^k} \cdot (\frac{\mathbf{b}_{2,i}\mathbf{f}+\mathbf{e}_{1,i}}{\mathbf{z}_2})^j \cdot (\frac{\mathbf{b}_2\mathbf{f}+\mathbf{e}_1}{\mathbf{z}_2})^{\kappa-k-j} \cdot \mathbf{z}_2^{\kappa} (\mathbf{h}_2 + \mathbf{hf}) \mathbf{f}^{-1} \end{bmatrix}_q \\
&= \left[\mathbf{h}_1 \mathbf{w} \mathbf{g}^{j-1} \cdot \triangle_{1,i} + \mathbf{h}_2 \cdot \triangle_{2,i} + \mathbf{h} \cdot \triangle_i \right]_q
\end{aligned}$$

It is easy to see that $\mathbf{v}$ in the above equality is not reduced modulo q.

First, one cannot yield a basis of $\mathbf{g}$ using $\mathbf{v}$ for the encoding scheme above. Since we add a new noise term $\mathbf{h}_2 \cdot \triangle_{2,i} + \mathbf{h} \cdot \triangle_i$ to $\mathbf{h}_1 \mathbf{w} \mathbf{g}^{j-1} \cdot \triangle_{1,i}$ and $\mathbf{h}_2 \cdot \triangle_{2,i} + \mathbf{h} \cdot \triangle_i$ has not the factor of $\mathbf{g}$. Hence, our construction hides the plaintext space $R / \langle \mathbf{g} \rangle$ itself. The aim we introduce $\mathbf{f}$ is to add another noise term to remove the factor of $\mathbf{g}$.

Then, the subgroup membership problem is seemly hard for our construction. Let $\mathbf{g} = \mathbf{g}_1 \mathbf{g}_2$.

Given a level-1 encoding $(\mathbf{u}_1,\mathbf{u}_2)$ with $\mathbf{u}_1=\begin{bmatrix}\frac{\mathbf{w}}{\mathbf{z}_1}\end{bmatrix}_q$, determine if $\mathbf{w}\in\langle\mathbf{g}_1\rangle$. Using $\mathbf{v}=\left[\mathbf{h}_1\mathbf{w}\mathbf{g}^{j-1}\cdot\triangle_{1,i}+\mathbf{h}_2\cdot\triangle_{2,i}+\mathbf{h}\cdot\triangle_i\right]_q$, one cannot decide whether $\mathbf{v}$ belongs to $\langle\mathbf{g}_1\rangle$ regardless of $\mathbf{w}\in\langle\mathbf{g}_1\rangle$. This is again the result adding new noise term.

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

3.4.2 Hu-Jia Attack

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

Hu-Jia Attack Description

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

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

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

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

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

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

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

Compute special decoding

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

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

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

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

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

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

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

Non-applicabiltiy of Hu-Jia Attack

(1) Let $\text{par} = \left\{ q, \left\{ \mathbf{y}_t, \left\{ \mathbf{x}_{t,i} \right\}_{i \in [\![\tau]\!]}, \mathbf{p}_{zt,t} \right\}_{t \in [\![2]\!]} \right\}$ be the public parameters of our construction. Similarly, we generate special decodings $S = \left\{ \mathbf{y}^{(1)}, \left\{ \mathbf{x}^{(i)} \right\}_{i \in [\![\tau]\!]} \right\}$ as follows:

$$\mathbf{y}^{(1)} = \left[\mathbf{x}_{1,1} \cdot (\mathbf{y}_1)^{\kappa-1} \cdot \mathbf{p}_{zt,1} - \mathbf{x}_{2,1} \cdot (\mathbf{y}_2)^{\kappa-1} \cdot \mathbf{p}_{zt,2} \right]_q = \mathbf{h}_1 \triangle_{1,0} + \mathbf{h}_2 \triangle_{2,0} + \mathbf{h} \triangle_0 ,$$

$$\mathbf{x}^{(i)} = \left[\mathbf{x}_{1,i} \mathbf{x}_{1,1} \cdot (\mathbf{y}_1)^{\kappa-2} \cdot \mathbf{p}_{zt,1} - \mathbf{x}_{2,i} \mathbf{x}_{2,1} \cdot (\mathbf{y}_2)^{\kappa-2} \cdot \mathbf{p}_{zt,2} \right]_q = \mathbf{h}_1 \mathbf{g} \triangle_{1,i} + \mathbf{h}_2 \triangle_{2,i} + \mathbf{h} \triangle_i .$$

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

(2) Given a level-1 encoding $(\mathbf{u}_1, \mathbf{u}_2)$ with $\mathbf{u}_t = \left[\mathbf{d} \cdot \mathbf{y}_t + \sum_{i=1}^{\tau} \mathbf{r}_i \cdot \mathbf{x}_{t,i} \right]_q, t \in [\![2]\!]$, we compute special decoding

$$\mathbf{v} = \left[\mathbf{u}_1 \mathbf{x}_{1,1} \cdot (\mathbf{y}_1)^{\kappa-2} \cdot \mathbf{p}_{zt,1} - \mathbf{u}_2 \mathbf{x}_{2,1} \cdot (\mathbf{y}_2)^{\kappa-2} \cdot \mathbf{p}_{zt,2} \right]_q = \mathbf{d} \cdot \mathbf{y}^{(1)} + \sum_{i=1}^{\tau} \mathbf{r}_i \cdot \mathbf{x}^{(i)} .$$

It is easy to verify that $\mathbf{v}$ is not reduced modulo q. On the one hand, one cannot find an equivalent level-0 encoding encoded by $(\mathbf{u}_1, \mathbf{u}_2)$ using the Hu-Jia method. Because $\mathbf{x}^{(i)} \notin \langle \mathbf{g} \rangle$ and the probability that $\mathbf{y}^{(1)}, \mathbf{x}^{(i)}$ are co-prime is almost 1. Namely, $\mathbf{y}^{(1)}, \mathbf{x}^{(i)}$ have not common factor. This is different from the case of the original GGH computed by Hu and Jia [HJ15a].

On the other hand, one cannot efficiently solve $\mathbf{d}, \mathbf{r}_i$ given $\mathbf{y}^{(1)}, \mathbf{x}^{(i)}, \mathbf{v}$. Because computing $\mathbf{d}, \mathbf{r}_i$ are similar to solving small integer problem. However, currently there exists no efficient algorithm for small integer problem.

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

3.4.3 Cheon-Lee Attack

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

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

4 Applications

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

4.1 MPKE Protocol

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

Publish(par, j). The j-th party samples $\mathbf{d}_j \leftarrow D_{\mathbb{Z}^n, \sigma'}$, $\mathbf{r}_{j,i} \leftarrow D_{\mathbb{Z}^n, \sigma^*}, i \in [\![\tau]\!]$, publishes the public key $\mathbf{u}_{t,j} = \left[\mathbf{d}_j \cdot \mathbf{y}_t + \sum_{i=1}^{\tau} \mathbf{r}_{j,i} \cdot \mathbf{x}_{t,i} \right]_q, t \in [\![2]\!]$ and remains $\mathbf{d}_j$ as the secret key.

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

Theorem 4.1 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.

4.2 Witness Encryption

4.2.1 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 $\mathbf{d}_k \leftarrow D_{Z^n,\sigma'}$, $\mathbf{r}_{k,i} \leftarrow D_{\mathbb{Z}^n,\sigma^*}$, $i \in [\![\tau]\!]$ and generate level-1 encodings $\mathbf{u}_{t,k} = \left[\mathbf{d}_k \cdot \mathbf{y}_t + \sum_{i=1}^{\tau} \mathbf{r}_{k,i} \cdot \mathbf{x}_{t,i}\right]_q, t \in [\![2]\!]$.

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

(3) For each element $T_j = \{j_1, j_2, j_3\} \in Set$, sample $\mathbf{r}_{T_j,i} \leftarrow D_{\mathbb{Z}^n,\sigma^*}, i \in [\![\tau]\!]$, and generate a level-$3$ encoding $\mathbf{u}_{t,T_j} = \left[\mathbf{u}_{t,j_1}\mathbf{u}_{t,j_2}\mathbf{u}_{t,j_3} + \sum_{i=1}^{\tau} \mathbf{r}_{T_j,i}(\mathbf{x}_{t,i})^3\right]_q, t \in [\![2]\!]$.

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

Decrypt(C, E, W):

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

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

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

Theorem 4.2 Suppose that the Decision Graded Encoding No-Exact-Cover is hard. Then our construction is a witness encryption scheme.

4.2.2 Hu-Jia Attacks

Since $\mathbf{u}_{t,T_j} = \left[\mathbf{u}_{j_1}\mathbf{u}_{j_2}\mathbf{u}_{j_3} + \sum_{i=1}^{\tau} \mathbf{r}_{T_j,i}(\mathbf{x}_{t,i})^3\right]_q$, $t \in [\![2]\!]$ is a level-3 encoding in our encoding method, one cannot obtain $\mathbf{u}_{t,T_i} = \left[\mathbf{u}_{t,T_j}\mathbf{u}_{t,T_k}(\mathbf{u}_{t,T_l})^{-1}\right]_q$ when $T_i = T_j \bigcup T_k - T_l$. As a result, the Hu-Jia attacks [HJ15a, HJ15b] are prevented in our new construction.

5 Conclusion

In this paper, we describe a new variant of GGH, which supports the applications for public tools of encoding in the original GGH, such as MPKE and WE. Using two zero testing parameters, our construction introduces new noise term to avoid weakness of GGH. As a result, our new construction not only prevents all known attacks, but also seemly supports the hardness assumption of the SubM problem and the DLIN problem.

References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[GGH15] C. Gentry, S. Gorbunov, and S. Halevi. Graph-induced multilinear maps from lattices.

TCC 2015, Part II, LNCS 9015, pp. 498–527.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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