Multilinear Maps over the Integers Using Modulus Switching

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

Oct 08, 2015

Abstract. After CLT13 of multilinear map over the integers was broken by Cheon, Han, Lee, Ryu and Stehle using zeroizing attack, a new variant CLT15 of CLT13 was proposed by Coron, Lepoint and Tibouchi by constructing new zero-testing parameter. Very recently, CLT15 was broken independently by Cheon, Lee and Ryu, and Minaud and Fouque using an extension of Cheon et al.'s attack. To immune CLT13 against zeroizing attack, we present a new construction of multilinear map over the integers using switching modulus technique. The security of our construction depends upon new hardness assumption.
Keywords. Multilinear maps, switching modulus, zeroizing attack, MPKE

1 Introductions

Multilinear maps have many applications including one-round multipartite key exchange [GGH13, BZ14], witness encryption [GSW13a] and program obfuscation [GGH+13a]. The notion of multilinear maps, which is a generalization of bilinear maps, was first introduced by Boneh and Silverberg in 2003 [BS03]. Until 2013, the first candidate construction of multilinear maps was described over ideal lattices Garg, Gentry and Halevi [GGH13] (GGH13, for short). Then, another construction over the integers was presented by Coron, Lepoint and Tibouchi [CLT13] (CLT13, for short). The recent construction over lattices is proposed by Gentry, Gorbunov, and Halevi [GGH15].

However, current constructions of multilinear maps [GGH13, CLT13, GGH15] suffered from zeroizing attacks [GGH13, CHL+15, CGH+15, HJ15, CLR15, GGH15]. (1) The GGH13 attack. GGH13 suffered from the weak discrete logarithm attack [GGH13]. Recently, an efficient weak-DL-based attack on the GGH13, which broke GGH13-based MPKE, was presented by Hu and Jia [HJ15]. A fix of GGH13 was recently proposed by Gentry, Halevi and Lepoint [Hal15] by replacing the linear zero-testing procedure from GGH13 with a quadratic (or higher-degree) procedure. However, this new variant of GGH13 failed to immune zeroizing attack [BGH+15]. (2) The CLT13 attack. CLT13 was completely broken by Cheon, Han, Lee, Ryu and Stehle [CHL+15] using zeroizing attack introduced by the authors of GGH13. To immune zeroizing attack, two fixes of CLT13 are proposed by Garg, Gentry, Halevi and Zhandry [GGH+14], and Boneh, Wu and Zimmerman [BWZ14]. However, these two fixes [GGH+14, BWZ14] were shown to be insecure in [CGH+15] by using an extension of Cheon et al.'s attack. Designing new zero-testing parameter, a new variant of CLT13 was proposed by Coron, Lepoint and Tibouchi [CLT15] (CLT15 for short). Very recently, CLT15 was also broken independently by Cheon, Lee and Ryu [CLR15], and Minaud and Fouque [MF15].

Thus, it is still an open problem to immunize CLT13 against zeroizing attack. In this paper, we propose a new construction over the integers using switching modulus technique.

Our contribution. Our main contribution is to construct a new multilinear map over the integers, whose security depends on new hardness assumption. Our construction maintains the functionality of CLT13. We improves CLT13 in three aspects: introducing new noise term by using double-encodings, modifying zero-testing parameters, and using switching modulus technique. Moreover, owing to introducing new noise and using switching modulus, we conjecture that the membership group problem (SubM) and the decisional linear (DLIN) problem are hard in our construction.

Organization. Section 2 recalls some background. Section 3 describes our new construction using ideal lattices. Section 4 gives security analysis for our construction. Finally, Section 5 presents MPKE based on our new construction.

2 Preliminaries

2.1 Notations

We denote $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ the ring of integers, the field of rational numbers, and the field of real numbers. We take n as a positive integer and a power of 2. Notation $[\![n]\!]$ denotes the set $\{1, 2, \cdots, n\}$, and $[a]_q$ the absolute minimum residual system $[a]_q = a \bmod q \in (-q/2, q/2]$. Vectors and matrices are denoted in bold, such as $\mathbf{a}, \mathbf{b}, \mathbf{c}$ and $\mathbf{A}, \mathbf{B}, \mathbf{C}$. The j-th entry of $\mathbf{a}$ is denoted as a_j, the element of the i-th row and j-th colomn of $\mathbf{A}$ is denoted as $a_{i,j}$. Notation $\|\mathbf{a}\|_\infty$ ($\|\mathbf{a}\|$ for short) denotes the infinity norm of $\mathbf{a}$. Given a composite integer $p = \prod_{j=1}^{n} p_j$, we let $CRT(b_1, ..., b_n)$ ($CRT_{(p_j)}(b_j)$ for short) denote the unique element $b \in \mathbb{Z}_p$ such that $b = b_j \bmod p_j$. Similarly, notation $[\mathbf{a}]_q$ denotes each entry (or each coefficient) $a_i \in (-p/2, p/2]$ of $\mathbf{a}$.

2.2 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 $L = \{\mathbf{By} : \mathbf{y} \in \mathbb{Z}^n\}$. We say that $\mathbf{B}$ spans L if $\mathbf{B}$ is a basis for L. Given a basis $\mathbf{B}$ of L, we define $P(\mathbf{B}) = \{\mathbf{By} \mid \mathbf{y} \in \mathbb{R}^n, \forall i : -1/2 \le y_i < 1/2\}$ as the parallelization corresponding to $\mathbf{B}$. Let $\det(\mathbf{B})$ denote the determinant of $\mathbf{B}$.

Given $\mathbf{c} \in \mathbb{R}^n$, $\sigma > 0$, 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 $\mathbf{x} \leftarrow D_{L,\sigma}$ over the lattice.

2.3 Multilinear Maps

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

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

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

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

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

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

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

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

3 Our new construction

Setting the parameters. Let λ be the security parameter, κ the multilinearity level, ρ the bit length of the randomness used for encodings, α the bit length of the message slots, η the bit length of the secret primes, n the number of distinct secret primes, τ the number of level-1 encodings of zero in public parameters, μ the number of level-0 encodings in public parameters, ν the bit length of the image of the multilinear map, β the bit length of the entries of the zero-testing matrix, $\sigma = 2d + 1$ the dimension of encoding matrix with constant integer d.

Concrete parameters are set as $\rho = \Omega(\lambda)$, $\alpha = \lambda$, $n = \Omega(\lambda\eta)$, $\mu \ge n\alpha + 2\lambda$, $\tau \ge n(\rho + \log_2(2n)) + 2\lambda$, $\beta = \Omega(\lambda)$, $\eta \ge \rho_\kappa + \alpha + 2\beta + 2\lambda$, $\rho_\kappa = \kappa(2\alpha + 2\rho + \lambda + 2\log_2 n + 2) + \rho + \log_2 \mu + \log_2 n$, $\nu \ge \eta - \beta - \rho_\kappa - \lambda - 3$.

3.1 Construction

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

(1) For $j \in [\![n]\!]$, choose $(\eta + \rho)$-bit primes $p_{1,j}$, η-bit primes $p_{2,j}$, α-bit primes $g_{1,j}, g_{2,j}$. Let $p_t = \prod_{j=1}^{n} p_{t,j}$, and $q_{t,j} = p_t / p_{t,j}, t \in [\![2]\!]$.

(2) Choose randomly $z_t \in \mathbb{Z}_{p_t}, t \in [\![2]\!]$ such that $z_t^{-1} \in \mathbb{Z}_{p_t}$.

(3) Choose a matrix $\mathbf{\Omega} = (\omega_{i,j}) \in \mathbb{Z}^{n\times n}$ with $\omega_{i,j} \leftarrow (n2^\rho, (n+1)2^\rho) \cap \mathbb{Z}$ if $i = j$, otherwise $\omega_{i,j} \leftarrow (-2^\rho, 2^\rho) \cap \mathbb{Z}$.

(4) Generate encodings and zero-testing parameters over the integers:

(4.1) Set $y_t = CRT_{(p_{t,j})}\left(\frac{r_j g_{1,j} + 1}{z_t}\right), t \in [\![2]\!]$, where $r_j \leftarrow (-2^\rho, 2^\rho) \cap \mathbb{Z}$ for $j \in [\![n]\!]$;

(4.2) Set $x_{t,i} = CRT_{(p_{t,j})}\left(\frac{r_{i,j} g_{1,j}}{z_t}\right)$, $i \in [\![\tau]\!]$, where $\mathbf{r}_i \in \mathbb{Z}^n$ are randomly and independently chosen from the half-open parallelepiped spanned by the columns of the matrix $\mathbf{\Omega}$;

(4.3) Set $\prod_{t,i} = CRT_{(p_{t,j})}\left(\frac{\omega_{i,j} g_{1,j}}{z_t}\right)$;

(4.4) Set $w_{t,i} = CRT_{(p_{t,j})}\left(e_{i,j} g_{1,j} + a_{i,j}\right)$, $i \in [\![\mu]\!]$, where $e_{i,j} \leftarrow (-2^\rho, 2^\rho) \cap \mathbb{Z}$, $a_{i,j} \leftarrow \mathbb{Z}_{g_{1,j}}$;

(4.5) Set $p_{zt,1}=\sum_{j=1}^{n}\left(h_{0,j}z_{0,j}+z_{1,j}^{\kappa}\left(h_{1,j}\left[g_{1,j}^{-1}\right]_{p_{1,j}}+h_{2,j}\left[g_{2,j}^{-1}\right]_{p_{1,j}}\right)\right)q_{1,j} \bmod p_1$,

$p_{zt,2}=\sum_{j=1}^{n}z_{2,j}^{\kappa}\left(h_{0,j}z_{3,j}+(h_{2,j}^{'}g_{2,j}+h_{2,j})\left\lfloor\frac{p_{2,j}}{p_{1,j}}\cdot\left[g_{2,j}^{-1}\right]_{p_{1,j}}\right\rfloor\right)q_{2,j} \bmod p_2$,

where $z_{0,j}\in\mathbb{Z}_{p_{1,j}}^{*}$, $z_{1,j}=\left[z_1\right]_{p_{1,j}}$, $z_{2,j}=\left[z_2\right]_{p_{2,j}}$, $z_{3,j}=\left\lfloor\frac{p_{2,j}}{p_{1,j}}\cdot\left[\frac{z_{0,j}}{z_{1,j}^{\kappa}}\right]_{p_{1,j}}\right\rfloor$

and $h_{0,j},h_{1,j},h_{2,j},h_{2,j}^{'}\leftarrow(-2^{\beta},2^{\beta})\bigcap\mathbb{Z}$, $j\in[\![n]\!]$.

(5) Choose randomly matrices $\mathbf{T}_t\in\mathbb{Z}_{p_t}^{\sigma\times\sigma}, t\in[\![2]\!]$ such that $\mathbf{T}_t^{-1}\in\mathbb{Z}_{p_t}^{\sigma\times\sigma}$.

(6) For $t\in[\![2]\!]$, set

(6.1) $\mathbf{Y}_t=\left[\mathbf{T}_t\cdot\begin{pmatrix}y_{t,1,1}&y_{t,1,2}&\cdots&y_{t,1,\sigma}\\y_{t,2,1}&y_{t,2,2}&\cdots&y_{t,2,\sigma}\\\vdots&\vdots&&\vdots\\y_{t,\sigma,1}&y_{t,\sigma,2}&\cdots&y_{t,\sigma,\sigma}\end{pmatrix}\cdot\mathbf{T}_t^{-1}\right]_{p_t}=\left[\mathbf{T}_t\cdot\begin{pmatrix}\$&0&\cdots&0\\0&\$&\cdots&0\\\vdots&\vdots&&\vdots\\0&0&\cdots&\$\end{pmatrix}\cdot\mathbf{T}_t^{-1}\right]_{p_t}$,

where $y_{t,s,s}=\left[c_{s,s}y_t+\sum_{l=1}^{\tau}b_{s,s,l}x_{t,l}+\sum_{l=1}^{n}b_{s,s,l}^{'}\prod_{t,l}\right]_{p_t}$, $s\in[\![2d]\!]$, $y_{t,\sigma,\sigma}=y_t$, and $y_{t,s_1,s_2}=\left[\sum_{l=1}^{\tau}b_{s_1,s_2,l}x_{t,l}+\sum_{l=1}^{l}b_{s_1,s_2,l}^{'}\prod_{t,l}\right]_{p_t}$ for $s_1\neq s_2$. Here $c_{s,s},b_{s,s,l},b_{s,s,l}^{'},b_{s_1,s_2,l},b_{s_1,s_2,l}^{'}\leftarrow(-2^{\rho},2^{\rho})\bigcap\mathbb{Z}$.

(6.2) $\mathbf{X}_{t,i}=\left[\mathbf{T}_t\cdot\begin{pmatrix}x_{t,i,1,1}&x_{t,i,1,2}&\cdots&x_{t,i,1,\sigma}\\x_{t,i,2,1}&x_{t,i,2,2}&\cdots&x_{t,i,2,\sigma}\\\vdots&\vdots&&\vdots\\x_{t,i,\sigma,1}&x_{t,i,\sigma,2}&\cdots&x_{t,i,\sigma,\sigma}\end{pmatrix}\cdot\mathbf{T}_t^{-1}\right]_{p_t}=\left[\mathbf{T}_t\cdot\begin{pmatrix}0&0&\cdots&0\\0&0&\cdots&0\\\vdots&\vdots&&\vdots\\0&0&\cdots&0\end{pmatrix}\cdot\mathbf{T}_t^{-1}\right]_{p_t}$,

$i\in[\![\tau]\!]$, where $x_{t,i,s_1,s_2}=\left[\sum_{l=1}^{\tau}b_{i,s_1,s_2,l}x_{t,l}+\sum_{l=1}^{n}b_{i,s_1,s_2,l}^{'}\prod_{t,l}\right]_{p_t}$ with $b_{i,s_1,s_2,l},b_{i,s_1,s_2,l}^{'}\leftarrow(-2^{\rho},2^{\rho})\bigcap\mathbb{Z}$.

(6.3) $\mathbf{W}_{t,i}=\left[\mathbf{T}_t\cdot\begin{pmatrix}w_{t,i,1,1}&w_{t,i,1,2}&\cdots&w_{t,i,1,\sigma}\\w_{t,i,2,1}&w_{t,i,2,2}&\cdots&w_{t,i,2,\sigma}\\\vdots&\vdots&&\vdots\\w_{t,i,\sigma,1}&w_{t,i,\sigma,2}&\cdots&w_{t,i,\sigma,\sigma}\end{pmatrix}\cdot\mathbf{T}_t^{-1}\right]_{p_t}=\left[\mathbf{T}_t\cdot\begin{pmatrix}\$&0&\cdots&0\\0&\$&\cdots&0\\\vdots&\vdots&&\vdots\\0&0&\cdots&\$\end{pmatrix}\cdot\mathbf{T}_t^{-1}\right]_{p_t}$,

$i\in[\![\mu]\!]$, where $w_{t,i,s_1,s_2}=\left[\sum_{l=1}^{\mu}b_{i,s_1,s_2,l}w_{t,l}\right]_{p_t}$ if $s_1=s_2$, otherwise $w_{t,i,s_1,s_2}=(e_{i,j}g_{1,j}) \bmod p_{t,j}$. Here $b_{i,s_1,s_2,l},e_{i,j}\leftarrow(-2^{\rho},2^{\rho})\bigcap\mathbb{Z}$.

(6.4) $\mathbf{q}_{zt,t}=\left(\mathbf{s}_t,\mathbf{t}_t\right)$,

where $\mathbf{s}_t=\left[\left(s_{t,1},\cdots,s_{t,\sigma}\right)\cdot\mathbf{T}_t^{-1}\right]_{p_t}=\left[\left(\underbrace{\$,...,\$}_{d},\underbrace{0,...,0}_{d},\$\right)\cdot\mathbf{T}_t^{-1}\right]_{p_t}$,

$$\mathbf{t}_t = \left[\mathbf{T}_t \cdot \left(t_{t,1}, \cdots, t_{t,\sigma}\right) \cdot p_{zt,t}\right]_{p_t} = \left[\mathbf{T}_t \cdot \left(\underbrace{0,...,0}_{d}, \underbrace{\$,...,\$}_{d}, \$\right) \cdot p_{zt,t}\right]_{p_t},$$

$s_{t,l} = CRT_{(p_{t,j})}\left(e_{1,l,j} g_{1,j} + a_{1,l,j}\right)$ for $l \in [\![d]\!] \cup \{\sigma\}$, $s_{t,l} = CRT_{(p_{t,j})}\left(e_{1,l,j} g_{1,j}\right)$ for $l \in \{d+1, \cdots, 2d\}$, and $t_{t,l} = CRT_{(p_{t,j})}\left(e_{2,l,j} g_{1,j} + a_{2,l,j}\right)$ for $l \in \{d+1, \cdots, \sigma\}$, $t_{t,l} = CRT_{(p_{t,j})}\left(e_{2,l,j} g_{1,j}\right), l \in [\![d]\!]$. Here $e_{1,l,j}, e_{2,l,j} \leftarrow (-2^{\rho}, 2^{\rho}) \cap \mathbb{Z}$, $a_{l,j} \leftarrow \mathbb{Z}_{g_{1,j}}$.

(7) Output the public parameters $\text{par} = \left\{\left\{p_t, \mathbf{Y}_t, \{\mathbf{X}_{t,i}\}_{i \in [\![\tau]\!]}, \{\mathbf{W}_{t,i}\}_{i \in [\![\mu]\!]}, \mathbf{q}_{zt,t}\right\}_{t \in [\![2]\!]}\right\}$.

Notice that "0" in $\mathbf{Y}_t, \mathbf{X}_{t,i}$ represent level-1 encoding of zero, "$\$$" level-1 encoding of random element. Similarly, "0" ,"$\$$" in $\mathbf{W}_{t,i}, \mathbf{q}_{zt,t}$ represent level-0 encoding of zero and random element. Here, the aim we write the right forms of $\mathbf{Y}_t, \mathbf{X}_{t,i}, \mathbf{W}_{t,i}, \mathbf{q}_{zt,t}$ is to easily describe our construction.

Generating level-k encoding: $\left(\mathbf{U}_1, \mathbf{U}_2\right) \leftarrow \text{Enc}\left(\text{par}, k, \mathbf{d} = (d_i) \in \{0,1\}^{\mu}\right)$.

(1) Generate a random binary vector $\mathbf{b} = (b_i) \in \{0,1\}^{\tau}$;

(2) Compute $\mathbf{U}_t = \left[(\mathbf{Y}_t)^k \cdot \sum_{i=1}^{\mu} d_i \mathbf{W}_{t,i} + \sum_{i=1}^{\tau} b_i \cdot (\mathbf{X}_{t,i})^k\right]_{p_t}, t \in [\![2]\!]$;

(3) Output a level-k encoding $\left(\mathbf{U}_1, \mathbf{U}_2\right)$.

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

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

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

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

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

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

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

Given a level-κ encoding $\left(\mathbf{U}_1, \mathbf{U}_2\right)$, to determine whether $\mathbf{U}_1$ is a level-κ encoding of zero or not, we compute $w = \left[\left\lfloor \frac{p_2}{p_1} \cdot \left[\mathbf{s}_1 \cdot \mathbf{U}_1 \cdot \mathbf{t}_1\right]_{p_1} \right\rceil - \left[\mathbf{s}_2 \cdot \mathbf{U}_2 \cdot \mathbf{t}_2\right]_{p_2}\right]_{p_2}$ and check whether w is short:

$$\text{isZero}\left(\text{par}, \left(\mathbf{U}_1, \mathbf{U}_2\right)\right) = \begin{cases} 1 & \text{if } |w| < p_2 \cdot 2^{-\nu} \\ 0 & \text{otherwise} \end{cases}.$$

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

Given a level-κ encoding $\left(\mathbf{U}_1, \mathbf{U}_2\right)$, we compute $w = \left[\left\lfloor \frac{p_2}{p_1} \cdot \left[\mathbf{s}_1 \cdot \mathbf{U}_1 \cdot \mathbf{t}_1\right]_{p_1} \right\rceil - \left[\mathbf{s}_2 \cdot \mathbf{U}_2 \cdot \mathbf{t}_2\right]_{p_2}\right]_{p_2}$, and collect ν most-significant bits of w:

$$\text{Ext}\left(\text{par}, \left(\mathbf{U}_1, \mathbf{U}_2\right)\right) = \text{Extract}_s\left(\text{msbs}_{\nu}\left(w\right)\right).$$

Remark 3.1 (1) Our construction uses double-encodings and double zero-testing parameters. (2) When $\sigma = 1$ in the above construction, our construction becomes a variant of CLT13 over the integers. The aim using $\sigma > 1$ is to thwart possible attacks since numerators in a pair of encodings are same over different modulo. (3) Using random elements $z_{0,j}, z_{3,j}$, $j \in [\![n]\!]$ in the zero-testing parameters and switching modulus are to avoid the zeroizing attack in [CGH+15].

3.2 Correctness

According to the above construction, the numerators of corresponding entries of matrices in double-encodings are identical when removing outer matrices $\mathbf{T}_1, \mathbf{T}_2$. Moreover, new zero-testing parameters transform zero-testing of matrix encodings into zero-testing of the CLT13 encoding, except for using two modulo and requiring switching modulo. Given a level-k encoding $(\mathbf{U}_1, \mathbf{U}_2)$ with $\mathbf{U}_t = \mathbf{T}_t \cdot \mathbf{U}_t \cdot \mathbf{T}_t^{-1}$, since numerator of each entry in $\mathbf{U}_1', \mathbf{U}_2'$ is same over each pair of modulo, we only need to show that each entry in $\mathbf{U}_1'$ is a level-k encoding. So, by the correctness of the CLT13, it is not difficult to verify that the following Lemma 3.2-3.5 is correct.

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.

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

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

Before proving correctness of the zero-testing procedure, we first describe four lemma (Lemma 3.6-3.9) about switching modulus.

Lemma 3.6 Let $p_t = \prod_{j=1}^{n} p_{t,j}$, and $q_{t,j} = p_t / p_{t,j}$, $t \in [\![2]\!]$. Suppose that $z \in \mathbb{Z}_{p_{1,j}}$, $v = \left[w \cdot z \cdot q_{1,j} \right]_{p_1}$, $j \in [\![n]\!]$ such that $\|w\| << p_{2,j}$. Then,

$$\left\lfloor \frac{p_2}{p_1} v \right\rceil = \left[wq_{2,j} \cdot \left\lfloor \frac{p_{2,j}}{p_{1,j}} z \right\rceil \right]_{p_2} + \delta \quad \text{such that } |\delta| < wq_{2,j}.$$

Proof. By $v = \left[w \cdot z \cdot q_{1,j} \right]_{p_1} = w \cdot z \cdot q_{1,j} - p_1 \cdot k$, we have

$$\frac{p_2}{p_1} v = w \cdot q_{2,j} \cdot \frac{p_{2,j}}{p_{1,j}} z - p_2 \cdot k,$$

$$wq_{2,j} \cdot \frac{p_{2,j}}{p_{1,j}} z = wq_{2,j} \cdot \left\lfloor \frac{p_{2,j}}{p_{1,j}} z \right\rceil + wq_{2,j} \cdot \left(\frac{p_{2,j}}{p_{1,j}} z - \left\lfloor \frac{p_{2,j}}{p_{1,j}} z \right\rceil \right),$$

$$= wq_{2,j} \cdot \left\lfloor \frac{p}{q} z \right\rceil + wq_{2,j} \cdot \varepsilon$$

where $|\varepsilon| < 1$.

Thus,

$$\left\lfloor \frac{p_2}{p_1} v \right\rfloor = \left\lfloor \frac{p_2}{p_1} \left[w \cdot z \cdot q_{1,j} \right]_{p_1} \right\rfloor$$
$$= \left\lfloor wq_{2,j} \cdot \frac{p_{2,j}}{p_{1,j}} z - p_2 \cdot k \right\rfloor$$
$$= wq_{2,j} \cdot \left\lfloor \frac{p_{2,j}}{p_{1,j}} z \right\rfloor + \left\lfloor wq_{2,j} \cdot \varepsilon \right\rfloor - p_2 \cdot k$$
$$= \left[wq_{2,j} \cdot \left\lfloor \frac{p_{2,j}}{p_{1,j}} z \right\rfloor \right]_{p_2} + p_2 \cdot \beta + \left\lfloor wq_{2,j} \cdot \varepsilon \right\rfloor - p_2 \cdot k .$$

By $\left\| \left\lfloor \frac{p_2}{p_1} v \right\rfloor \right\| < p_2 / 2$, we get $\beta = k$ with high probability. That is, $\left\lfloor \frac{p_2}{p_1} v \right\rfloor = \left[wq_{2,j} \cdot \left\lfloor \frac{p_{2,j}}{p_{1,j}} z \right\rfloor \right]_{p_2} + \delta$ such that $|\delta| < wq_{2,j}$. □

Lemma 3.7 Let $p_t = \prod_{j=1}^{n} p_{t,j}$, and $q_{t,j} = p_t / p_{t,j}$, $t \in [\![2]\!]$. Suppose that $v_t = \left[w_t q_{1,j} \cdot \left[g_{t,j}^{-1} \right]_{p_{1,j}} \right]_{p_1}$, $j \in [\![n]\!]$, $t \in [\![2]\!]$ with $|w_t| << p_{2,j}$. Then,

$$\left\lfloor \frac{p_2}{p_1} v_t \right\rfloor = \left[w_t q_{2,j} \cdot \left\lfloor \frac{p_{2,j}}{p_{1,j}} \left[g_{t,j}^{-1} \right]_{p_{1,j}} \right\rfloor \right]_{p_2} + \delta_t \text{ with } |\delta_t| < w_t q_{2,j} .$$

Proof. Since $\left[g_{t,j}^{-1} \right]_{p_{1,j}} \in \mathbb{Z}_{p_{1,j}}$, the result is proved by taking $z = \left[g_{t,j}^{-1} \right]_{p_{1,j}}$ in Lemma 3.6.

Lemma 3.8 Let $p_t = \prod_{j=1}^{n} p_{t,j}$, and $q_{t,j} = p_t / p_{t,j}$, $t \in [\![2]\!]$. Suppose that $\delta_{t,j} = \left[w_{t,j} g_{t,j} q_{2,j} \cdot \left\lfloor \frac{p_{2,j}}{p_{1,j}} \left[g_{t,j}^{-1} \right]_{p_{1,j}} \right\rfloor \right]_{p_2}$, $j \in [\![n]\!]$, $t \in [\![2]\!]$ with $|w_{t,j} g_{t,j}| << p_{2,j}$. Then $|\delta_{t,j}| < w_{t,j} g_{t,j} q_{2,j} + \left\lfloor \frac{p_{2,j}}{p_{1,j}} w_{t,j} q_{2,j} \right\rfloor$.

Proof. Assume that $v_t = \left[w_t q_{1,j} \cdot \left[g_{t,j}^{-1} \right]_{p_{1,j}} \right]_{p_1}$ with $w_t = w_{t,j} g_{t,j}$. Then by Lemma 3.6, we have

$$\left\lfloor \frac{p_2}{p_1} w_{t,j} q_{1,j} \right\rfloor = \left\lfloor \frac{p_2}{p_1} v_t \right\rfloor = \left[w_{t,j} g_{t,j} q_{2,j} \cdot \left\lfloor \frac{p_{2,j}}{p_{1,j}} \left[g_{t,j}^{-1} \right]_{p_{1,j}} \right\rfloor \right]_{p_2} + \delta'_{t,j} \text{ and } |\delta'_{t,j}| < w_{t,j} g_{t,j} q_{2,j} .$$

Thus, $\delta_{t,j} = \left[w_{t,j} g_{t,j} q_{1,j} \cdot \left\lfloor \frac{p_{2,j}}{p_{1,j}} \left[g_t^{-1} \right]_q \right\rfloor \right]_p = \left\lfloor \frac{p_2}{p_1} w_{t,j} q_{1,j} \right\rfloor - \delta'_{t,j}$ and $|\delta_{t,j}| < w_{t,j} g_{t,j} q_{2,j} + \left\lfloor \frac{p_{2,j}}{p_{1,j}} w_{t,j} q_{2,j} \right\rfloor$. □

Lemma 3.9 Suppose that p_1, p_2 are integers and $p_1 < p_2$. Then

$$\left\lfloor \frac{p_2}{p_1}\left[v_1+v_2\right]_{p_1}\right\rfloor=\left\lfloor \frac{p_2}{p_1}\left[v_1\right]_{p_1}\right\rfloor+\left\lfloor \frac{p_2}{p_1}\left[v_2\right]_{p_1}\right\rfloor+\delta_1 p_2+\varepsilon_1,$$

where δ_1,ε_1 are integers, and $|\delta_1|<1$ and $|\varepsilon_1|<2$.

Proof. By basic arithmetic rule, we obtain

$$\begin{aligned}\left\lfloor \frac{p_2}{p_1}\left[v_1+v_2\right]_{p_1}\right\rfloor&=\left\lfloor \frac{p_2}{p_1}\left(\left[v_1\right]_{p_1}+\left[v_2\right]_{p_1}+\delta_1 p_1\right)\right\rfloor\\&=\left\lfloor \frac{p_2}{p_1}\left(\left[v_1\right]_{p_1}+\left[v_2\right]_{p_1}\right)\right\rfloor+\delta_1 p_2\\&=\left\lfloor \frac{p_2}{p_1}\left[v_1\right]_{p_1}\right\rfloor+\left\lfloor \frac{p_2}{p_1}\left[v_2\right]_{p_1}\right\rfloor+\varepsilon_1+\delta_1 p_2\end{aligned}.$$

□

Lemma 3.10 The zero-testing procedure $\mathrm{isZero}\left(\mathrm{par},\left(\mathbf{U}_1,\mathbf{U}_2\right)\right)$ correctly determines whether $\left(\mathbf{U}_1,\mathbf{U}_2\right)$ is a level-κ encoding of zero or not.

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

$$\mathbf{U}_t=\left[\mathbf{T}_t\cdot\begin{pmatrix}u_{t,1,1}&u_{t,1,2}&\cdots&u_{t,1,\sigma}\\u_{t,2,1}&u_{t,2,2}&\cdots&u_{t,2,\sigma}\\\vdots&\vdots&&\vdots\\u_{t,\sigma,1}&u_{t,\sigma,2}&\cdots&u_{t,\sigma,\sigma}\end{pmatrix}\cdot\mathbf{T}_t^{-1}\right]_{p_t}=\left[\mathbf{T}_t\cdot\begin{pmatrix}\$&0&\cdots&0\\0&\$&\cdots&0\\\vdots&\vdots&&\vdots\\0&0&\cdots&\$\end{pmatrix}\cdot\mathbf{T}_t^{-1}\right]_{p_t}.$$

The zero-testing procedure determines whether $u_{t,\sigma,\sigma}$ is a level-κ encoding of zero.

According to the parameters setting, it is easy to obtain by arranging $w_t=\left[\mathbf{s}_t\cdot\mathbf{U}_t\cdot\mathbf{t}_t\right]_{p_t}$

$$\begin{aligned}w_t&=\left[\mathbf{s}_t\cdot\mathbf{U}_t\cdot\mathbf{t}_t\right]_{p_t}\\&=\left[\left(CRT_{(p_{t,j})}\left(\frac{r_j' g_{1,j}}{z_{t,j}^{\kappa}}\right)+s_{t,\sigma}u_{t,\sigma,\sigma}t_{t,\sigma}\right)\cdot p_{zt,t}\right]_{p_t}.\end{aligned}$$

Since $u_{t,\sigma,\sigma}=CRT_{(p_{t,j})}\left(\frac{r_{\sigma,j}g_{1,j}+d_{\sigma,j}'}{z_{t,j}^{\kappa}}\right)$, $s_{t,\sigma}=CRT_{(p_{t,j})}\left(e_{1,\sigma,j}g_{1,j}+a_{1,\sigma,j}\right)$, $t_{t,\sigma}=CRT_{(p_{t,j})}\left(e_{2,\sigma,j}g_{1,j}+a_{2,\sigma,j}\right)$, we derive the following equality:

$$\begin{aligned}w_t&=\left[\mathbf{s}_t\cdot\mathbf{U}_t\cdot\mathbf{t}_t\right]_{p_t}\\&=\left[CRT_{(p_{t,j})}\left(\frac{r_j g_{1,j}+a_{1,\sigma,j}a_{2,\sigma,j}d_{\sigma,j}'}{z_{t,j}^{\kappa}}\right)\cdot p_{zt,t}\right]_{p_t}\\&=\left[CRT_{(p_{t,j})}\left(\frac{r_j g_{1,j}+d_{\sigma,j}}{z_{t,j}^{\kappa}}\right)\cdot p_{zt,t}\right]_{p_t},\\&=\left[CRT_{(p_{t,j})}\left(\frac{c_j}{z_{t,j}^{\kappa}}\right)\cdot p_{zt,t}\right]_{p_t}\end{aligned}$$

where $c_j=r_j g_{1,j}+d_{\sigma,j}$, $d_{\sigma,j}=a_{1,\sigma,j}a_{2,\sigma,j}d_{\sigma,j}'$.

By $w=\left[\left\lfloor \frac{p_2}{p_1}\cdot w_1 \right\rfloor - w_2\right]_{p_2}$, we compute as follows:

$$\left\lfloor \frac{p_2}{p_1}\cdot w_1 \right\rfloor$$

$$=\left\lfloor \frac{p_2}{p_1}\cdot\left[CRT_{(p_{1,j})}\left(\frac{c_j}{z_{1,j}^{\kappa}}\right)\cdot p_{zt,1}\right]_{p_1}\right\rfloor$$

$$=\left\lfloor \frac{p_2}{p_1}\cdot\left[\sum_{j=1}^{n}\left(h_{0,j}c_jq_{1,j}\left[\frac{z_{0,j}}{z_{1,j}^{\kappa}}\right]_{p_{1,j}}\right)+\sum_{j=1}^{n}\left(h_{1,j}c_jq_{1,j}\left[g_{1,j}^{-1}\right]_{p_{1,j}}+h_{2,j}c_jq_{1,j}\left[g_{2,j}^{-1}\right]_{p_{1,j}}\right)\right]_{p_1}\right\rfloor$$

$$=\left\lfloor \frac{p_2}{p_1}\cdot\left[\sum_{j=1}^{n}h_{0,j}c_jq_{1,j}\left[\frac{z_{0,j}}{z_{1,j}^{\kappa}}\right]_{p_{1,j}}\right]_{p_1}\right\rfloor+\left\lfloor \frac{p_2}{p_1}\cdot\left[\sum_{j=1}^{n}h_{1,j}c_jq_{1,j}\left[g_{1,j}^{-1}\right]_{p_{1,j}}\right]_{p_1}\right\rfloor$$

$$+\left\lfloor \frac{p_2}{p_1}\cdot\left[\sum_{j=1}^{n}h_{2,j}c_jq_{1,j}\left[g_{2,j}^{-1}\right]_{p_{1,j}}\right]_{p_1}\right\rfloor+\delta_{1,1}p_2+\varepsilon_{1,1}$$

$$=\sum_{j=1}^{n}\left\lfloor \frac{p_2}{p_1}\cdot\left[h_{0,j}c_jq_{1,j}\left[\frac{z_{0,j}}{z_{1,j}^{\kappa}}\right]_{p_{1,j}}\right]_{p_1}\right\rfloor+\sum_{j=1}^{n}\left\lfloor \frac{p_2}{p_1}\cdot\left[h_{1,j}c_jq_{1,j}\left[g_{1,j}^{-1}\right]_{p_{1,j}}\right]_{p_1}\right\rfloor$$

$$+\sum_{j=1}^{n}\left\lfloor \frac{p_2}{p_1}\cdot\left[h_{2,j}c_jq_{1,j}\left[g_{2,j}^{-1}\right]_{p_{1,j}}\right]_{p_1}\right\rfloor+\delta_{1,2}p_2+\varepsilon_{1,2}+\delta_{1,1}p_2+\varepsilon_{1,1},$$

where $|\delta_{1,1}|<3$, $|\varepsilon_{1,1}|<3$ and $|\delta_{1,2}|<3n$ and $|\varepsilon_{1,2}|<3n$.

By Lemma 3.6-3.7, we have

$$\left\lfloor \frac{p_2}{p_1}\cdot\left[h_{0,j}c_jq_{1,j}\left[\frac{z_{0,j}}{z_{1,j}^{\kappa}}\right]_{p_{1,j}}\right]_{p_1}\right\rfloor=\left[h_{0,j}c_jq_{2,j}\left\lfloor \frac{p_{2,j}}{p_{1,j}}\cdot\left[\frac{z_{0,j}}{z_{1,j}^{\kappa}}\right]_{p_{1,j}}\right\rfloor\right]_{p_2}+\delta_{1,j}^{'},$$

$$\left\lfloor \frac{p_2}{p_1}\cdot\left[h_{1,j}c_jq_{1,j}\left[g_{1,j}^{-1}\right]_{p_{1,j}}\right]_{p_1}\right\rfloor=\left[h_{1,j}c_jq_{2,j}\left\lfloor \frac{p_{2,j}}{p_{1,j}}\cdot\left[g_{1,j}^{-1}\right]_{p_{1,j}}\right\rfloor\right]_{p_2}+\delta_{2,j}^{'},$$

$$\left\lfloor \frac{p_2}{p_1}\cdot\left[h_{2,j}c_jq_{1,j}\left[g_{2,j}^{-1}\right]_{p_{1,j}}\right]_{p_1}\right\rfloor=\left[h_{2,j}c_jq_{2,j}\left\lfloor \frac{p_{2,j}}{p_{1,j}}\cdot\left[g_{2,j}^{-1}\right]_{p_{1,j}}\right\rfloor\right]_{p_2}+\delta_{3,j}^{'}.$$

Namely,

$$\left\lfloor \frac{p_2}{p_1}\cdot w_1 \right\rfloor$$

$$= \sum_{j=1}^{n}\left[h_{0,j}c_j q_{2,j}\left\lfloor \frac{p_{2,j}}{p_{1,j}}\cdot\left[\frac{z_{0,j}}{z_{1,j}^{\kappa}}\right]_{p_{1,j}}\right\rfloor\right]_{p_2} + \sum_{j=1}^{n}\left[h_{1,j}c_j q_{2,j}\left\lfloor \frac{p_{2,j}}{p_{1,j}}\cdot\left[g_{1,j}^{-1}\right]_{p_{1,j}}\right\rfloor\right]_{p_2},$$

$$+ \sum_{j=1}^{n}\left[h_{2,j}c_j q_{2,j}\left\lfloor \frac{p_{2,j}}{p_{1,j}}\cdot\left[g_{2,j}^{-1}\right]_{p_{1,j}}\right\rfloor\right]_{p_2} + \delta' \bmod p_2$$

where $\delta' = \varepsilon_{1,2} + \varepsilon_{1,1} + \sum_{j=1}^{n}(\delta_{1,j}^{'} + \delta_{2,j}^{'} + \delta_{3,j}^{'})$.

$$w_2 = \left[CRT_{(p_{t,j})}\left(\frac{c_j}{z_{2,j}^{\kappa}}\right)\cdot p_{zt,2}\right]_{p_2}$$

$$= \left[\sum_{j=1}^{n}\left(h_{0,j}c_j z_{3,j} + c_j(h_{2,j}^{'}g_{2,j} + h_{2,j})\left\lfloor \frac{p_{2,j}}{p_{1,j}}\cdot\left[g_{2,j}^{-1}\right]_{p_{1,j}}\right\rfloor\right) q_{2,j}\right]_{p_2}.$$

Thus,

$$w = \left[\left\lfloor \frac{p_2}{p_1}\cdot w_1\right\rfloor - w_2\right]_{p_2}$$

$$= \sum_{j=1}^{n}\left[h_{1,j}c_j q_{2,j}\left\lfloor \frac{p_{2,j}}{p_{1,j}}\cdot\left[g_{1,j}^{-1}\right]_{p_{1,j}}\right\rfloor\right]_{p_2} + \delta,$$

where $\delta = \sum_{j=1}^{n}\left(h_{2,j}^{'}c_j q_{2,j} g_{2,j}\left\lfloor \frac{p_{2,j}}{p_{1,j}}\cdot\left[g_{2,j}^{-1}\right]_{p_{1,j}}\right\rfloor\right) + \delta'$.

By Lemma 3.8, $\delta = \sum_{j=1}^{n}\left(h_{2,j}^{'}c_j q_{2,j} g_{2,j}\left\lfloor \frac{p_{2,j}}{p_{1,j}}\cdot\left[g_{2,j}^{-1}\right]_{p_{1,j}}\right\rfloor\right) + \delta' = \sum_{j=1}^{n}\delta_{2,j}^{''} + \delta'$ such that

$\delta_{2,j}^{''} < h_{2,j}^{'}c_j q_{2,j} g_{2,j} + \left\lfloor \frac{p_{2,j}}{p_{1,j}} h_{2,j}^{'}c_j q_{2,j}\right\rfloor < |p_2|/2^{\nu+2\lambda}$.

According to the parameters setting, it is easy to verify that $|\delta| < |p_2|/2^{\nu+\lambda}$.

If $u_{t,\sigma,\sigma}$ is a level-κ encoding of zero, namely $d_{\sigma,j}^{'} = 0$, $c_j = r_j g_{1,j}$, $j \in [\![n]\!]$. So

$$w = \left[\left\lfloor \frac{p_2}{p_1}\cdot w_1\right\rfloor - w_2\right]_{p_2}$$

$$= \sum_{j=1}^{n}\left[h_{1,j}r_j g_{1,j} q_{2,j}\left\lfloor \frac{p_{2,j}}{p_{1,j}}\cdot\left[g_{1,j}^{-1}\right]_{p_{1,j}}\right\rfloor\right]_{p_2} + \delta,$$

$$= \sum_{j=1}^{n}\delta_{1,j}^{''} + \delta$$

where $|\delta_{1,j}^{''}| < h_{1,j}r_j g_{1,j} q_{2,j} + \left\lfloor \frac{p_{2,j}}{p_{1,j}} h_{1,j}r_j q_{2,j}\right\rfloor < |p_2|/2^{\nu+\lambda}$.

Thus, $|w| = \left|\sum_{j=1}^{n} \delta_{1,j}^{''} + \delta\right| < n \cdot |p_2| / 2^{\nu+2\lambda} + |p_2| / 2^{\nu+\lambda} < |p_2| / 2^{\nu}$.

If $u_{t,\sigma,\sigma}$ is a level-κ encoding of non-zero element, namely $d_{\sigma,j}^{'} \neq 0 \bmod g_{1,j}$ for at least one $j \in [\![n]\!]$. By Lemma 4 in [GGH13], $\left|\left[h_{1,j} d_{\sigma,j}^{'} q_{2,j} \left\lfloor \frac{p_{2,j}}{p_{1,j}} \cdot \left[g_{1,j}^{-1}\right]_{p_{1,j}} \right\rfloor\right]_{p_2}\right| \geq p_2^{1-\varepsilon}$ with high probability, where ε is an arbitrary small positive constant.

Thus, with high probability

$$
\begin{aligned}
|w| &= \left|\left[\left\lfloor \frac{p_2}{p_1} \cdot w_1 \right\rfloor - w_2\right]_{p_2}\right| \\
&= \left|\left[\sum_{j=1}^{n} \left[h_{1,j}(r_j g_{1,j} + d_{\sigma,j}^{'}) q_{2,j} \left\lfloor \frac{p_{2,j}}{p_{1,j}} \cdot \left[g_{1,j}^{-1}\right]_{p_{1,j}} \right\rfloor\right]_{p_2} + \delta\right]_{p_2}\right| \\
&= \left|\sum_{j=1}^{n} \left[h_{1,j} d_{\sigma,j}^{'} q_{2,j} \left\lfloor \frac{p_{2,j}}{p_{1,j}} \cdot \left[g_{1,j}^{-1}\right]_{p_{1,j}} \right\rfloor\right]_{p_2} + \left[\sum_{j=1}^{n} \delta_{1,j}^{''} + \delta\right]_{p_2}\right|, \\
&> p_2^{1-\varepsilon} - p_2 / 2^{\nu} \\
&> p_2^{1-\varepsilon'}
\end{aligned}
$$

where ε' is a small positive constant. □

Lemma 3.11 Given two level-κ encodings $\left(\mathbf{U}_{1,1}, \mathbf{U}_{2,1}\right), \left(\mathbf{U}_{1,2}, \mathbf{U}_{2,2}\right)$, suppose that $\mathbf{U}_{1,1}, \mathbf{U}_{1,2}$ encode same plaintext for all $g_{1,j}, j \in [\![n]\!]$, 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. Without loss of generality, assume that $u_{t,\sigma,\sigma,s} = CRT_{(p_{t,j})}\left(\frac{r_{\sigma,j,s} g_{1,j} + d_{\sigma,j}^{'}}{z_{t,j}^{\kappa}}\right), s \in [\![2]\!]$.

Similar to the procedure of Lemma 3.10, we have

$$w^{(s)} = \left[\sum_{j=1}^{n} \left[h_{1,j} d_{\sigma,j}^{'} q_{2,j} \left\lfloor \frac{p_{2,j}}{p_{1,j}} \cdot \left[g_{1,j}^{-1}\right]_{p_{1,j}} \right\rfloor\right]_{p_2} + \delta^{(s)}\right]_{p_2}.$$

By Lemma 3.10, we get $\left|\delta^{(s)}\right| < p_2 / 2^{\nu}$ and with high probability $\left|\sum_{j=1}^{n} \left[h_{1,j} d_{\sigma,j}^{'} q_{2,j} \left\lfloor \frac{p_{2,j}}{p_{1,j}} \cdot \left[g_{1,j}^{-1}\right]_{p_{1,j}} \right\rfloor\right]_{p_2}\right| \approx p_2$ when $d_{\sigma,j}^{'} \neq 0 \bmod g_{1,j}$ for at least one $j \in [\![n]\!]$.

Thus ν most-significant bits of $w^{(1)}$ are equal to that of $w^{(2)}$. □

3.3 Hardness assumption

Consider the following security experiment:

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

(2) For $l = 0$ to κ:

Sample $\mathbf{d}_l \leftarrow \{0,1\}^{\mu}$, $\mathbf{b}_l \leftarrow \{0,1\}^{\tau}$;

Generate level-1 encoding $\mathbf{U}_{t,l} = \left[\mathbf{Y}_t \cdot \sum_{i=1}^{\mu} d_{l,i} \mathbf{W}_{t,i} + \sum_{i=1}^{\tau} b_{l,i} \cdot \mathbf{X}_{t,i} \right]_{p_t}, t \in [\![2]\!]$.

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

(4) Set $w_C = w_D = \mathrm{Ext}\left(\mathrm{par}, \left(\left[\mathbf{U}_1 \sum_{i=1}^{\mu} d_{0,i} \mathbf{W}_{1,i} \right]_{p_1}, \left[\mathbf{U}_2 \sum_{i=1}^{\mu} d_{0,i} \mathbf{W}_{2,i} \right]_{p_2} \right) \right)$.

(5) Set $w_R = \mathrm{Ext}\left(\mathrm{par}, \left(\left[\mathbf{U}_1 \sum_{i=1}^{\mu} r_{0,i} \mathbf{W}_{1,i} \right]_{p_1}, \left[\mathbf{U}_2 \sum_{i=1}^{\mu} r_{0,i} \mathbf{W}_{2,i} \right]_{p_2} \right) \right)$ with $\mathbf{r}_0 \leftarrow \{0,1\}^{\mu}$.

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

Level-κ extraction CDH (ext-GCDH): Given $\left\{ \mathrm{par}, \left(\mathbf{U}_{1,0}, \mathbf{U}_{2,0} \right), \cdots, \left(\mathbf{U}_{1,\kappa}, \mathbf{U}_{2,\kappa} \right) \right\}$, output a level-$\kappa$ extraction encoding $w \in \mathbb{Z}_{p_2}$ such that $\left| [v_C - w]_{p_2} \right| < p_2 / 2^{\nu}$.

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

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

4 Cryptanalysis

Using zeroizing attacks, CHL+15, CLR15 [CHL+15, CLR15] have completely broken the CLT13 and CLT15 schemes. The successful key of the CHL+15 and CLR15 attacks is to build the equations over the rational by easily computable quantities for CLT13 and CLT15. In this section, we first give easily computable some quantities in our construction, then analyze that the CHL+15, CLR15 attacks do not work for our construction using these quantities.

4.1 Easily computable quantities

Since the public parameters in our construction include encodings of zero, one can similarly compute some quantities that are not reduced over modulo. However, we construct new zero-testing parameters under different modulo and introduce random elements $z_{0,j} \in \mathbb{Z}_{p_{1,j}}$ and $z_{3,j} \in \mathbb{Z}_{p_{2,j}}$, $j \in [\![n]\!]$. As a result, one can not get useful information from these non-reduced quantities. In the following, we give some easily computable quantities.

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

$$w = \left[\left\lfloor \frac{p_2}{p_1} \cdot \left[\mathbf{s}_1 \cdot \mathbf{U}_1 \cdot \mathbf{t}_1 \right]_{p_1} \right\rfloor - \left[\mathbf{s}_2 \cdot \mathbf{U}_2 \cdot \mathbf{t}_2 \right]_{p_2} \right]_{p_2},$$

where $\mathbf{U}_t = \mathbf{U}_t^{'} \cdot (\mathbf{X}_{t,i})^{l} \cdot (\mathbf{Y}_t)^{\kappa - k - l}, t \in [\![2]\!]$.

It is easy to verify that w is not reduced modulo p_2. Since using $z_{0,j} \in \mathbb{Z}_{p_{1,j}}$ and $z_{3,j} \in \mathbb{Z}_{p_{2,j}}$, $j \in [\![n]\!]$, the non-reduced quantity w can no longer represent as matrix form over the rational.

4.2 Cheon et al. Attack and extension

For the Cheon et al.'s attack [CHL+15] and its extension attack [CGH+15], which include encodings more than a single monomial, the success key of the attack in [CHL+15, CGH+15] is that one can write in the matrix form over the rational for non-reduced quantities.

To demonstrate effect of $z_{0,j} \in \mathbb{Z}_{p_{1,j}}$ and $z_{3,j} \in \mathbb{Z}_{p_{2,j}}$, $j \in [\![n]\!]$ in $p_{zt,1}, p_{zt,2}$, we recovery all secret parameters using the extension attack in [CGH+15] when taking $z_{0,j} = z_{3,j} = 0$, $j \in [\![n]\!]$. For simplicity, we also set $\sigma = 1$, and $\mathbf{T}_t$, $t \in [\![2]\!]$ as identity matrix.

By Corollary 3.8, we have $\alpha_{t,j} = \left[g_{t,j} \cdot \left[g_{t,j}^{-1} \right]_{p_{1,j}} \right]_{p_{2,j}}$ and $\alpha_{t,j} < \left| g_{t,j} \right| + \lfloor p_{2,j} / p_{1,j} \rfloor$ for $t \in [\![2]\!]$. So, $\alpha_{t,j}$ is not reduced modulo $p_{2,j}$.

In the above simplified condition, given an arbitrary level-k encoding $\left(u_1^{'}, u_2^{'}\right)$, one computes using zeroizing attack

$$w = \left[\frac{p_2}{p_1} \cdot \left[u_1 \cdot p_{zt,1} \right]_{p_1} - \left[u_2 \cdot p_{zt,2} \right]_{p_2} \right]_{p_2},$$

where $u_t = u_t^{'} \cdot (x_{t,i})^l \cdot (y_t)^{\kappa - k - l}, t \in [\![2]\!]$ with $l \geq 1$.

Note that here $\frac{p_2}{p_1} \cdot \left[u_1 \cdot p_{zt,1} \right]_{p_1}$ in w is not rounded to integers. It is easy to see that w is not reduced modulo p_2.

Without loss of generality, assume that $u_t^{'} = CRT_{(p_{t,j})}(c_j / z_{t,j}^k)$, $x_{t,i}^l = CRT_{(p_{t,j})}(s_{i,j}^l / z_{t,j}^l)$, $y_{t,j}^{\kappa-k-l} = CRT_{(p_{t,j})}(d_j^{\kappa-k-l} / z_{t,j}^{\kappa-k-l})$. We can write w in matrix form:

$$\begin{aligned} w &= \left[\frac{p_2}{p_1} \cdot \left[u_1 \cdot p_{zt,1} \right]_{p_1} - \left[u_2 \cdot p_{zt,2} \right]_{p_2} \right]_{p_2} \\ &= \left(c_1, ..., c_n\right) \begin{pmatrix} s_{i,1}^l \cdot (\frac{p_{2,1}}{p_{1,1}} \cdot \rho_{1,1} - \rho_{2,1}) & & \\ & \ddots & \\ & & s_{i,n}^l \cdot (\frac{p_{2,n}}{p_{1,n}} \cdot \rho_{1,n} - \rho_{2,n}) \end{pmatrix} \begin{pmatrix} d_1^{\kappa-k-l} \\ \vdots \\ d_n^{\kappa-k-l} \end{pmatrix}, \end{aligned}$$

where $\rho_{1,j} = \left(\frac{h_{1,j}}{g_{1,j}} + \frac{h_{2,j}}{g_{2,j}} \right) q_{1,j}$, $\rho_{2,j} = \frac{h_{2,j}^{'} g_{2,j} + h_{2,j}}{g_{2,j}} \alpha_{2,j} q_{2,j}$.

Since w can be written as the matrix form over the rational, this simplified version can be broken by directly using the attack in [CGH+15].

However, using $z_{0,j} \in \mathbb{Z}_{p_{1,j}}$ and $z_{3,j} \in \mathbb{Z}_{p_{2,j}}$, $j \in [\![n]\!]$ in $p_{zt,1}, p_{zt,2}$, our construction thwart to represent w as matrix form over the rational. This is also the reason that they are used in the zero-testing parameters. Thus, the attacks in [CHL+15, CGH+15] do not work for our construction.

5 MPKE Protocol

Based on our construction, we describe a one-round multipartite Diffie-Hellman key exchange protocol. The security relies on the hardness assumption of ext-GDDH.

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

Publish(par,k). The k-th party samples $\mathbf{d}_k \in \{0,1\}^{\mu}$ and $\mathbf{r}_k \in \{0,1\}^{\tau}$, publishes the public key $\mathbf{U}_{t,k} = \left[\mathbf{Y}_t \cdot \sum_{i=1}^{\mu} d_{k,i} \mathbf{W}_{t,i} + \sum_{i=1}^{\tau} r_{k,i} \cdot \mathbf{X}_{t,i} \right]_{p_t}, t \in [\![2]\!]$ and remains $\mathbf{d}_k$ as the secret key.

KeyGen$\left(\text{par}, k, \mathbf{d}_k, \left\{\left(\mathbf{U}_{1,i}, \mathbf{U}_{2,i}\right)\right\}_{i \neq k}\right)$. The k-th party computes $\mathbf{C}_{t,k} = \left[\prod_{i \neq k} \mathbf{U}_{t,i} \right]_{p_t}, t \in [\![2]\!]$ and extracts the common secret key $sk = \text{Ext}\left(\text{par}, \left(\left[\mathbf{C}_{1,k} \sum_{i=1}^{\mu} d_{k,i} \mathbf{W}_{1,i} \right]_{p_1}, \left[\mathbf{C}_{2,k} \sum_{i=1}^{\mu} d_{k,i} \mathbf{W}_{2,i} \right]_{p_2} \right) \right)$.

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

References

[BGH+15] Z. Brakerskiy, C. Gentry, S. Halevi, T. Lepoint, A. Sahai, M. Tibouchi. Cryptanalysis of the Quadratic Zero-Testing of GGH. http://eprint.iacr.org/2015/845.

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

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

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

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

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

[CHL+15] 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.

[CLR15] J. H. Cheon, C. Lee, H. Ryu. Cryptanalysis of the New CLT Multilinear Maps. http://eprint.iacr.org/2015/934.

[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.

[Hal15] Shai Halevi. The state of cryptographic multilinear maps, 2015. Invited Talk of CRYPTO 2015.

[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.

[HJ15] Yupu Hu and Huiwen Jia. Cryptanalysis of GGH Map. http://eprint.iacr.org/2015/301.

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

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

[MF15] B. Minaud and P. Fouque. Cryptanalysis of the New Multilinear Map Over the integers, http://eprint.iacr.org/2015/941.