Cryptanalysis of the New CLT Multilinear Maps

Jung Hee Cheon, Changmin Lee, Hansol Ryu

Seoul National University (SNU), Republic of Korea

Abstract. Multilinear maps have many cryptographic applications. The first candidate construction of multilinear maps was proposed by Garg, Gentry, and Halevi (GGH13) in 2013, and soon afterwards, another candidate was suggested by Coron, Lepoint, and Tibouchi (CLT13) that works over the integers. However, both of these were found to be insecure in the face of a so-called zeroizing attack (HJ15, CHL$^+$15). To improve on CLT13, Coron, Lepoint, and Tibouchi proposed another candidate of new multilinear maps over the integers (CLT15).
In this paper, we describe an attack against CLT15. Our attack shares the essence of the cryptanalysis of CLT13 and exploits low level encodings of zero, as well as other public parameters. As in CHL$^+$15, this leads to finding all the secret parameters of κ-multilinear maps in polynomial time of the security parameter.

Keywords: Multilinear maps, graded encoding schemes, zeroizing attack.

1 Introduction

Multilinear maps. The cryptographic multilinear map has many applications, including non-interactive key exchange, general program obfuscation, and efficient broadcast encryption. After the first candidate construction of Garg, Gentry, and Halevi(GGH13, for short) [GGH13], it received a considerable amount of attention. Shortly afterwards, Coron, Lepoint, and Tibouchi proposed another candidate of multilinear maps (CLT13, for short) [CLT13]. It is constructed over the integers and gives the first implementation of multilinear maps [CLT13]. The most recent candidate, called GGH15, was suggested by Gentry, Gorbunov, and Halevi using a directed acyclic graph [GGH15].

Attack and revisions of CLT13. In [CLT13], it was claimed that CLT13 is robust against a zeroizing attack. Hence, CLT13 supports the Graded Decisional Diffie-Helman assumption (GDDH), subgroup membership (SubM), and decisional linear (DLIN) problems are hard in it, while GGH13 supports only the GDDH. However, Cheon, Han, Lee, Ryu, and Stehlé proposed an attack, called CHLRS, on the scheme [CHL$^+$15], which runs in polynomial time and recovers all secrets. As in the zeroizing attack of GGH13, the attack utilizes public low level encodings of zero, which allows an encoding to be generated without the secret values being known. The core of the attack is to compute several zero-testing values related to one another. Then, one can construct a matrix, the eigenvalues of which consist of the CRT component of x, which is $x \pmod{p_i}$ for some encoding x, where $p_1, \cdots, p_n$ are secret values of the scheme. Then, it reveals all the secrets of the scheme.

In response, two attempts have been made to make CLT13 secure against the CHLRS attack [GGHZ14,BWZ14]. However, both are shown to be insecure in [CGH$^+$15]. At the same time, another fix of CLT13 was proposed at Crypto15 by Coron, Lepoint, and Tibouch (CLT15, for short) [CLT15]. CLT15 is almost the same as the original scheme, except in the zero-testing parameter and procedure. To prevent zero-testing values from being obtained in CLT13, the authors did not publish the modulus x_0 and performed zero-testing in independent modulus N. They claimed that it is secure against a CHLRS attack, because a zero-testing value of an encoding x depends on the CRT components of x non-linearly.

New multilinear maps over the integers. We briefly introduce the CLT15 scheme. It is a graded encoding scheme and its level-t encoding c is an integer satisfying $c \equiv \frac{r_{it}g_i+m_i}{z^t} \pmod{p_i}$ for $1 \le i \le n$, where $p_1, \cdots, p_n$ are secret primes, $(m_1, \cdots, m_n) \in \mathbb{Z}_{g_1} \times \cdots \times \mathbb{Z}_{g_n}$ is a plaintext for secret moduli $g_1, \cdots, g_n$, and $r_{1t}, \cdots, r_{nt}$ are random noises. Then, it can be written as $\sum_{i=1}^{n}[r_{it} + m_i/g_i]_{p_i} u_{it} + a_t x_0$ for some integer a_t, where $u_{it} = \left[\frac{g_i}{z^t}\left(\frac{x_0}{p_i}\right)^{-1}\right]_{p_i} \frac{x_0}{p_i}$ for $1 \le i \le n$.

The zero-testing of level-κ encoding operates as follows. For a zero-testing parameter p_{zt} and a level-κ encoding $x = \sum_{i=1}^{n}[r_i + m_i/g_i]_{p_i} u_{i\kappa} + a x_0$, which is smaller than x_0,

$$p_{zt} \cdot x \equiv \sum_{i=1}^{n}[r_i + m_i/g_i]_{p_i} \cdot v_i + a v_0 \pmod{N},$$

where $v_i = [p_{zt} \cdot u_{i\kappa}]_N$ and $v_0 = [p_{zt} \cdot x_0]_N$. Note that v_i's are small as compared to N for all $0 \le i \le n$ and the size of a depends on that of x. Hence, the right hand side is small when all m_i's are zero. Therefore, it is used to determine whether it constitutes an encoding of zero or not.

Since $a v_0$ exceeds N for a large x, the zero-testing is effective only when the size of x is small. However, the size of the encodings is almost doubled through multiplication and is too large to allow one to obtain a correct zero-testing value. Accordingly, CLT15 publishes encodings of zero of various sizes (called ladders) to reduce the size of the encodings. The ladders are of the form $X_j = \sum_{i=1}^{n} s_{ij} u_{i\kappa} + q_j x_0$, where $0 \le j \le M$ for some integers q_j, and for small integers $s_{ij}, 1 \le i \le n, 0 \le j \le M$, and the size of X_j is about $2^j x_0$. For an encoding x larger than x_0, one can obtain x', an encoding of the same plaintext, the size of which is reduced using a ladder. Then, it can be written as $x' = x - \sum_{j=0}^{M} b_j X_j$, for some $b_0, \cdots, b_M \in \{0, 1\}$.

Proposed attack. The points of a CHLRS attack can be divided into two parts. The first is that, for a level-κ encoding of zero $x = \sum_{i=1}^{n}[\frac{r_i g_i}{z^\kappa}(\frac{x_0}{p_i})^{-1}]_{p_i} \frac{x_0}{p_i} + a x_0$,

$$[p_{zt} \cdot x]_{x_0} = \sum_{i=1}^{n} r_i \hat{v}_i,$$

where $\hat{v}_i$ is common to all the encodings in CLT13, holds over the integers. The second point is that the zero-testing value of a product of two encodings is a quadratic form of some values related to each encoding. More precisely, for two encodings $x_1 = \sum_{i=1}^{n}[\frac{r_{i1} g_i}{z^t}(\frac{x_0}{p_i})^{-1}]_{p_i} \frac{x_0}{p_i} + a_1 x_0$ and $x_2 = \sum_{i=1}^{n}[\frac{r_{i2}}{z^{\kappa-t}}(\frac{x_0}{p_i})^{-1}]_{p_i} \frac{x_0}{p_i} + a_2 x_0$, the product is $x_1 x_2 \equiv \sum_{i=1}^{n}[\frac{r_{i1} r_{i2} g_i}{z^\kappa}(\frac{x_0}{p_i})^{-1}]_{p_i} \frac{x_0}{p_i} \pmod{x_0}$. Therefore, the zero-testing value of $x_1 x_2$ is

$$[p_{zt} \cdot x_1 x_2]_{x_0} = \sum_{i=1}^{n} r_{i1} r_{i2} \hat{v}_i.$$

Let us look at CLT15 in these aspects. For a level-κ encoding of zero $x = \sum_{i=1}^{n} r_i u_{i\kappa} + ax_0$, the zero-testing value of x is written as

$$[p_{zt} \cdot x]_N = \sum_{i=1}^{n} r_i v_i + a v_0,$$

for common v_i's, similar to CLT13. Let x_1 be a level-t encoding of zero, x_2 be a level-$(\kappa - t)$ encoding, and x be a product of x_1 and x_2. Then, these can be written as $x_1 = \sum_{i=1}^{n} r_{i1} u_{it} + a_1 x_0$, $x_2 = \sum_{i=1}^{n} r_{i2} u_{i\kappa - t} + a_2 x_0$, and $x = \sum_{i=1}^{n} r_{i1} r_{i2} u_{i\kappa} + ax_0$, for some integers $a, a_1, a_2, r_{i1}, r_{i2}, 1 \le i \le n$, where a is a quadratic form of $a_1, a_2, r_{i1}, r_{i2}, 1 \le i \le n$. Since the size of x is larger than that of x_0, we need to reduce the size of x to perform zero-testing. Let x' be a size-reduced encoding of x; then, it is of the form $x' = x - \sum_{j=0}^{M} b_j X_j = \sum_{i=1}^{n} (r_{i1} r_{i2} - \sum_{j=0}^{M} b_j s_{ij}) u_{i\kappa} + (a - \sum_{j=0}^{M} b_j q_j) x_0$, for some $b_0, \cdots, b_M \in \{0, 1\}$. In this case, the zero-testing value gives

$$\begin{aligned}
[p_{zt} \cdot x']_N &= \Big[p_{zt} \cdot \big(x - \sum_{j=0}^{M} b_j X_j\big)\Big]_N \\
&= \sum_{i=1}^{n} \big(r_{i1} r_{i2} - \sum_{j=0}^{M} b_j s_{ij}\big) v_i + \big(a - \sum_{j=0}^{M} b_j q_j\big) v_0 \\
&= \sum_{i=1}^{n} \big(r_{i1} r_{i2}\big) v_i + a v_0 - \sum_{j=0}^{M} b_j \big(\sum_{i=1}^{n} s_{ij} v_i + q_j v_0\big).
\end{aligned}$$

Therefore, if one has $\sum_{i=1}^{n} s_{ij} v_i + q_j v_0$ for all j, one can compute $\sum_{i=1}^{n} (r_{i1} r_{i2}) v_i + a v_0$ and follow a CHLRS attack strategy. We define a function ψ such that the above equation is written as

$$[p_{zt} \cdot x']_N = \psi(x) - \sum_{j=0}^{M} b_j \cdot \psi(X_j). \tag{1}$$

Note that $\psi(x) = [p_{zt} \cdot x]_N$, when x is a level-κ encoding of zero smaller than x_0. Since X_j's are level-κ encodings of zero and the size of X_0 is small, one can obtain $\psi(X_0)$ by the zero-testing procedure. $\psi(X_j)$ can be obtained inductively, because the size-reduced X_j is a linear summation of $X_0, \cdots, X_{j-1}, X_j$. When one has $\psi(X_j)$ in hand, it is easy to calculate $\psi(x)$ for a level-κ encoding of 0 of arbitrary size using Equation (1).

By using $(n+1)$ level-t encodings of zero and $(n+1)$ level-$(\kappa - t)$ encodings, we constitute matrix equations that consist only of a product of matrices. As in [CHL+15], we have a matrix, the eigenvalues of which consist of the CRT components of an encoding. From these, we can recover all the secret parameters of the CLT15 scheme [CLT15]. Our attack needs only ladders and two level-0 encodings and runs in polynomial time.

Organization. In section 2, we introduce CLT15 and briefly explain the CHLRS attack. In Section 3, we examine the zero-testing process of CLT15 and give a description of our attack, splitting it into three steps. We conclude in Section 4.

2 Multilinear Maps over the Integers

Notations. We use $\mathbb{Z}_q$ to denote the ring $\mathbb{Z}/q\mathbb{Z}$. For $a, b, N \in \mathbb{Z}$, $a \equiv b \pmod{N}$ or $a \equiv_N b$ means that a is congruent to b modulo N. Additionally, we use the notation $a \pmod{N}$ or $[a]_N$ to denote the reduction of a modulo N into the interval $(-N/2, N/2]$. We denote $\mathsf{CRT}_{(p_1,p_2,\ldots,p_n)}(r_1, r_2, \ldots, r_n)$ by the unique integer in $[0, \prod_{i=1}^n p_i)$, which is congruent to $r_i \pmod{p_i}$ for all $i = 1, \cdots, n$. For short, we denote it by $\mathsf{CRT}_{(p_i)}(r_i)$.

For a finite set S, we use $s \leftarrow S$ to denote the operation of uniformly choosing an element s from S.

For an $n \times n$ square matrix $\boldsymbol{H}$, we use (h_{ij}) to represent a matrix $\boldsymbol{H}$, the (i, j) component of which is h_{ij}. Similarly, for a vector $\boldsymbol{v} \in \mathbb{R}^n$, we define $(\boldsymbol{v})_j$ as the j-th component of $\boldsymbol{v}$. Let $\boldsymbol{H}^T$ be the transpose of $\boldsymbol{H}$ and $\|\boldsymbol{H}\|_\infty$ be the $\max_i \sum_{j=1}^n |h_{ij}|$. We denote by $\mathsf{diag}(d_1, \cdots, d_n)$ the diagonal matrix with diagonal coefficients equal to $d_1, \cdots, d_n$.

2.1 CLT15 Scheme

First, we recall Coron et al.'s new multilinear maps. The scheme relies on the following parameters.

λ: the security parameter
κ: the multilinearity parameter, i.e., the proposed map is κ- linear
ρ: the bit length of the initial noise used for encodings
α: the bit length of the primes g_i
η: the bit length of the secret primes p_i
n: the number of distinct secret primes
γ: the bit length of encodings ($= n\eta$)
τ: the number of level-1 encodings of zero in public parameters
ℓ: 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-test matrix H

Coron et al. suggested setting the parameters according to the following conditions.

- $\rho = \Omega(\lambda)$: to avoid a brute force attack on the noise
- $\alpha = \lambda$: to prevent a situation where the order of message ring $\mathbb{Z}_{g_1} \times \ldots \times \mathbb{Z}_{g_n}$ has a small prime factor
- $n = \Omega(\eta\lambda)$: to thwart lattice reduction attacks
- $\ell \geq n\alpha + 2\lambda$: to apply the leftover hash lemma from [CLT15]
- $\tau \geq n(\rho + \log_2(2n)) + 2\lambda$: to apply the leftover hash lemma from [CLT15]
- $\beta = 3\lambda$: as a conservative security precaution
- $\eta \geq \rho_\kappa + 2\alpha + 2\beta + \lambda + 8$, where ρ_κ is the maximum bit size of the noise r_i of a level-κ encoding. When computing the product of κ level-1 encodings and an additional level-0 encoding, one obtains $\rho_\kappa = \kappa(2\alpha + 2\rho + \lambda + 2\log_2 n + 3) + \rho + \log_2 \ell + 1$
- $\nu = \eta - \beta - \rho_f - \lambda - 3$: to ensure correctness of zero-testing.

The constraints are the same as in [CLT13]; the condition that differs is β.

Instance generation: $(\mathsf{params}, \boldsymbol{p}_{zt}) \leftarrow \mathsf{InstGen}(1^\lambda, 1^\kappa)$. Set the scheme parameters as explained above. For $1 \le i \le n$, generate η-bit odd primes p_i and α-bit primes g_i, and compute $x_0 = \prod_{i=1}^{n} p_i$. Generate a random prime integer N of size $\gamma + 2\eta + 1$ bits. Using LLL algorithms in dimension 2, special pairs of nonzero integers $(\alpha_i, \beta_i)_{i=1}^n$ are chosen to satisfy $|\alpha_i| < 2^{\eta-1}$, $|\beta_i| < 2^{2-\eta} \cdot N$, $\beta_i \equiv \alpha_i u_i' p_i^{-1} \pmod N$, where $u_i' = \left[\frac{g_i}{z^\kappa} \left(\frac{x_0}{p_i} \right)^{-1} \right]_{p_i} \frac{x_0}{p_i}$. Finally, generate $\boldsymbol{H} = (h_{ij}) \in \mathbb{Z}^{n \times n}$ such that $\boldsymbol{H}$ is invertible and $\|\boldsymbol{H}^T\|_\infty \le 2^\beta$, $\|(\boldsymbol{H}^{-1})^T\|_\infty \le 2^\beta$ and for $1 \le i \le n$, $1 \le j \le \ell$, $m_{ij} \leftarrow [0, g_i) \cap \mathbb{Z}$. Then, define

$$
\begin{aligned}
y &= \mathsf{CRT}_{(p_i)} \left(\frac{r_i g_i + 1}{z} \right), \\
x_j &= \mathsf{CRT}_{(p_i)} \left(\frac{r_{ij} g_i}{z} \right), \text{ for } 1 \le j \le \tau, \\
x_j' &= \mathsf{CRT}_{(p_i)} (r_{ij}' g_i + m_{ij}) \text{ for } 1 \le j \le \ell, \\
X_j^{(t)} &= \mathsf{CRT}_{(p_i)} \left(\frac{r_{ij}^{(t)} g_i}{z^t} \right) + q_j^{(t)} x_0 \text{ for } 0 \le j \le \gamma + \lfloor \log_2 \ell \rfloor, 1 \le t \le \kappa, \\
\Pi_j &= \sum_{i=1}^{n} \varpi_{ij} g_i \left[z^{-1} \left(\frac{x_0}{p_i} \right)^{-1} \right]_{p_i} \frac{x_0}{p_i} + \varpi_{n+1,j} x_0 \text{ for } 1 \le j \le n+1, \text{and} \\
(\boldsymbol{p}_{zt})_j &= \sum_{i=1}^{n} h_{ij} \alpha_i p_i^{-1} \pmod N \text{ for } 1 \le j \le n,
\end{aligned}
$$

where $r_i, r_{ij}', r_{ij}^{(t)} \leftarrow (-2^\rho, 2^\rho) \cap \mathbb{Z}$, $q_j^{(t)} \leftarrow [2^{\gamma+j-1}/x_0, 2^{\gamma+j}/x_0) \cap \mathbb{Z}$, and $\varpi_{ij} \leftarrow (-2^\rho, 2^\rho) \cap \mathbb{Z}$ if $i \ne j$, $\varpi_{ii} \leftarrow ((n+1)2^\rho, (n+2)2^\rho) \cap \mathbb{Z}$. Then, output

$$
\mathsf{params} = (n, \eta, \alpha, \rho, \beta, \tau, \ell, \mu, y, \{x_j\}_{j=1}^{\tau}, \{x_j'\}_{j=1}^{\ell}, \{X_i^{(j)}\}, \{\Pi_j\}_{j=1}^{n+1}, s) \text{ and } \boldsymbol{p}_{zt}.
$$

In this study, we used only one zero-testing parameter. Hence, hereafter, we use a notation $p_{zt} = \sum_{i=1}^{n} h_i \alpha_i p_i^{-1} \pmod N$ instead of a vector $(\boldsymbol{p}_{zt})_j$, if no confusion results.

Sampling level-0 encodings: $c \leftarrow \mathsf{samp}(\mathsf{params})$. Since the user does not know p_i, one cannot encode a vector $\boldsymbol{m} \in \mathbb{Z}_{g_1} \times \cdots \times \mathbb{Z}_{g_n}$. Hence, CLT15 provides level zero encodings $\{x_j'\}$ for sampling. A level zero encoding c is computed as a random subset sum of $\{x_j'\}$. Namely, for $1 \le j \le \ell$, sample $b_j \leftarrow \{0,1\}$ and compute $c = \sum_{j=1}^{\ell} b_j \cdot x_j'$.

Encodings at higher levels: $c_k \leftarrow \mathsf{enc}(\mathsf{params}, k, c)$. Given a level-0 encoding c, to obtain a level-1 encoding c_1 with the same plaintext as c, compute $c_1 = c \cdot y$. Since x_0 is not given, a ladder of level-1 encodings of zero $X_j^{(1)}$ is provided. Then, iteratively reduce the size of c_1 to that of $X_0^{(1)}$.

In general, to obtain a level-k encoding, compute $c_k = c \cdot y^k$ and reduce the size of c_k after each multiplication by y using ladders $\{X_j^{(i)}\}_{j=0}^{\gamma + \lfloor \log_2 \ell \rfloor}$ for levels $i = 1, \cdots, k$.

Re-randomizing level-1 encodings:[1] $c' \leftarrow \mathsf{reRand}(\mathsf{params}, c)$. For $1 \leq j \leq \tau, 1 \leq i \leq n+1$, sample $b_j \leftarrow \{0,1\}$, $b'_i \leftarrow [0, 2^{\mu}) \cap \mathbb{Z}$, with $\mu = \rho + \alpha + \lambda$. Return $c' = c + \sum_{j=1}^{\tau} b_j \cdot x_j + \sum_{i=1}^{n+1} b'_i \cdot \Pi_i$.

Adding and multiplying encodings: For two encodings, the addition and multiplication are performed in $\mathbb{Z}$. After the arithmetic, reduce the size to that of $2x_0$ using the ladder.

Zero-testing: $\mathsf{isZero}(\mathsf{params}, \boldsymbol{p}_{zt}, x) \stackrel{?}{=} 0/1$. Given a level-$\kappa$ encoding x, return 1 if $\|\boldsymbol{p}_{zt} \cdot x \pmod N\|_{\infty} < N \cdot 2^{-\nu}$, and 0 otherwise.

Extraction: $sk \leftarrow \mathsf{ext}(\mathsf{params}, \boldsymbol{p}_{zt}, c)$. Given a level-$\kappa$ encoding c, compute the most significant ν bits of $[\boldsymbol{p}_{zt} \cdot c]_N$.

2.2 CHLRS Attack

In this section, we briefly present Coron et al.'s original multilinear maps (for short, CLT13) [CLT13] and its cryptanalysis [CHL+15]. CLT13 is almost the same as the new multilinear map. The main difference between the two schemes can be divided into two parts. One is that CLT13 makes public $x_0 = \prod_{i=1}^{n} p_i$. Instead of x_0, in [CLT15] a ladder of encodings of zero at each level was published. The second is that CLT13 uses a different zero-testing vector. The zero-testing value of a level-κ encoding is a linear sum of secret value. Namely, the original zero-testing parameter p'_{zt} is defined as $\sum_{i=1}^{n} h_i [z^{\kappa} g_i^{-1}]_{p_i} \cdot \frac{x_0}{p_i} \pmod{x_0}$ for some small integer h_i. When x is a level-κ encoding, it is denoted by $\mathsf{CRT}_{(p_i)}\left(\frac{r_i g_i + m_i}{z^{\kappa}}\right) = \left[\frac{r_i g_i + m_i}{z^{\kappa}}\right]_{p_i} + q_i p_i$ for some small integer r_i and integer q_i. Hence, $[p'_{zt} \cdot x]_{x_0}$ has the form

$$\left[\sum_{i=1}^{n} h_i [r_i + m_i/g_i]_{p_i} \frac{x_0}{p_i}\right]_{x_0}.$$

If $m_i = 0$ for $1 \leq i \leq n$, its value is a linear sum of $h_i, r_i, x_0/p_i$ over $\mathbb{Z}$ not modulo x_0. Hence, it is a small integer as compared to x_0. Using this property, one can check whether x is an encoding of zero or not.

The original CLT scheme is broken by a CHLRS attack. Its idea is as follows. If c_{jl} is a multiplication of three encodings X_j, c, and Y_l such that

$$\begin{aligned} X_j &= \mathsf{CRT}_{(p_i)}\left(\frac{r_{ij}}{z}\right) \\ c &= \mathsf{CRT}_{(p_i)}(c_i) \\ Y_l &= \mathsf{CRT}_{(p_i)}\left(\frac{r''_{il} g_i}{z^{\kappa-1}}\right) \end{aligned}$$

[1] This procedure can be adapted to higher levels $1 < k \leq \kappa$ by publishing appropriate quantities in params.

then its zero-testing value is denoted by $\sum_{i=1}^{n} h_i(r_{ij}c_ir''_{il})\dfrac{x_0}{p_i}$. By spanning $1 \le j, l \le n$, one can construct a matrix $\boldsymbol{M}_c = \boldsymbol{Y} \cdot \mathsf{diag}(\hat{v}_1, \cdots, \hat{v}_n) \cdot \mathsf{diag}(c_1, \cdots, c_n) \cdot \boldsymbol{X}$, where $\boldsymbol{X} = (r_{ij})$, $\boldsymbol{Y} = (r''_{il})^T$, and $\hat{v}_i = h_i \frac{x_0}{p_i}$. By replacing c with 1, we can also construct a matrix $\boldsymbol{M}_1 = \boldsymbol{Y} \cdot \mathsf{diag}(\hat{v}_1, \cdots, \hat{v}_n) \cdot \boldsymbol{X}$. Then, a matrix $\boldsymbol{M}_1^{-1} \cdot \boldsymbol{M}_c = \boldsymbol{X}^{-1} \cdot \mathsf{diag}(c_1, \cdots, c_n) \cdot \boldsymbol{X}$ has an eigenvalue c_i and we can obtain all of them by solving the characteristic polynomial of matrix $\boldsymbol{M}_1^{-1} \cdot \boldsymbol{M}_c$. This implies that we can recover all p_i by computing $\gcd(x_0, c - c_i)$ in polynomial time.

A CHLRS attack, however, is not directly adapted to the new CLT scheme. It keeps x_0 as a secret value, and we cannot reduce the size of $c_{jl} = X_j \cdot c \cdot Y_l$ using x_0. Instead, we reduce the size by using level-κ ladder $\{X_j^{(\kappa)}\}$. Then, the size-reduced c_{jl} can be written as

$$\sum_{i=1}^{n} \left(r_{ij}c_ir''_{il} + s_{ijl}\right) u'_i + a_{jl}x_0,$$

for some integers s_{ijl} and a_{jl}. As compared to CLT13, this has additional terms s_{ijl} and a_{jl}. Its zero-testing value in [CLT15] is represented by $\sum_{i=1}^{n} (r_{ij}c_ir''_{il} + s_{ijl})\, v_i + a_{jl}v_0$, where $v_i = [p_{zt} \cdot u'_i]_N$ and $v_0 = [p_{zt} \cdot x_0]_N$. By spanning $1 \le j, l \le n$, one can deduce matrix equations such as $\boldsymbol{M}_c = \boldsymbol{Y} \cdot \mathsf{diag}(v_1, \cdots, v_n) \cdot \mathsf{diag}(c_1, \cdots, c_n) \cdot \boldsymbol{X} + \boldsymbol{S} + \boldsymbol{A} \cdot v_0$, where $\boldsymbol{S} = (\sum_{i=1}^{n} v_i s_{ijl})$ and $\boldsymbol{A} = (a_{jl})$. Because of the $\boldsymbol{S} + \boldsymbol{A} \cdot v_0$ part, it appears difficult to extract any useful information about $\mathsf{diag}(c_1, \cdots, c_n)$.

3 A Zeroizing Attack on CLT15

3.1 Understanding the Zero-testing Procedure

Let us explain how the zero-testing operates. Let $p_{zt} = \sum_i h_i \alpha_i p_i^{-1} \mod N$, and $x = \mathsf{CRT}_{(p_i)}\left(\dfrac{r_ig_i + m_i}{z^\kappa}\right) = \sum_i \left[r_i + m_i/g_i\right]_{p_i} u'_i + ax_0$, where $u'_i = \left[\dfrac{g_i}{z^\kappa}\left(\dfrac{x_0}{p_i}\right)^{-1}\right]_{p_i} \cdot \dfrac{x_0}{p_i}$. Then,

$$p_{zt} \cdot x \equiv \sum_{i,j} h_j \left[r_i + m_i/g_i\right]_{p_i} u'_i \alpha_j p_j^{-1} + ax_0 p_{zt} \pmod{N}.$$

The zero-testing asks whether $[p_{zt} \cdot x]_N$ is much smaller than the modulus N. To identify zero, m_i's (in this case, the bit size of $\left[r_i + m_i/g_i\right]_{p_i}$ is much smaller than η), the size of $[u'_i \alpha_j p_j^{-1}]_N$ should be close to $N/2^\eta$ and $[p_{zt} \cdot ax_0]_N$ must be much smaller than N.

Let us examine the size of each term. For $i \ne j$, $[u'_i \alpha_j p_j^{-1}]_N$ is equal to $\alpha_j \dfrac{x_0}{p_ip_j}\left[\dfrac{g_i}{z^\kappa}\left(\dfrac{x_0}{p_i}\right)^{-1}\right]_{p_i}$. Therefore, it is at most a γ-bit integer, if $|\alpha_j| < p_j$. Define $\beta_i = [u'_i \alpha_i p_i^{-1}]_N$, which is expected to be a $(\gamma + \eta)$-bit integer. By the Euclidean algorithm on $u'_j[p_j^{-1}]_N$ and N, one can take β_i to be a $(\gamma + \eta)$-bit integer for an η-bit integer α_i [Sho09]. Note that $[p_{zt} \cdot ax_0]_N = \sum_i ah_i\alpha_i \frac{x_0}{p_i}$, and therefore, it is $(\gamma + \beta + \log_2 a + \log_2 n)$-bit. Let us state the result, the so-called the zero-testing lemma, more precisely.

Lemma 1 (Zero testing lemma). *Let x be a level-κ encoding of zero with $x = \sum_{i=1}^{n} r_iu'_i + ax_0, (r_1, \cdots, r_n, a \in \mathbb{Z})$. Then,*

$$[p_{zt} \cdot x]_N = \sum_{i=1}^{n} r_iv_i + av_0,$$

holds over the integers, if $|a| < 2^{2\eta-\beta-\log_2 n-1}$ *and* $|r_i| < 2^{\eta-\beta-\log_2 n-6}$ *for* $1 \le i \le n$.

Proof. By the construction of the zero-testing element, we have $p_{zt} \cdot x \equiv \sum_{i=1}^{n} r_i v_i + a v_0 \pmod N$. It is sufficient to show that the right hand side is smaller than $N/2$. For $1 \le i \le n$,

$$v_i \equiv \sum_{j=1}^{n} h_j \alpha_j p_j^{-1} u_i' \equiv h_i \beta_i + \sum_{j \neq i} h_j \alpha_j \left[\frac{g_i}{z^\kappa} \left(\frac{x_0}{p_i} \right)^{-1} \right]_{p_i} \frac{x_0}{p_i p_j} \pmod N,$$

and therefore, $|v_i| < 2^{\gamma+\eta+\beta+4}$ for $1 \le i \le n$. Moreover, $v_0 = \sum_{j=1}^{n} h_j \alpha_j \frac{x_0}{p_j}$ and $|v_0| < n 2^{\gamma+\beta-1}$. $\square$

3.2 Idea of the Attack

For a level-κ encoding of zero $x = \sum_{i=1}^{n} r_i u_i' + a x_0$ of arbitrary size, if one can compute the integer value $\sum_{i=1}^{n} r_i v_i + a v_0$, which is not reduced modulus N, then a CHLRS attack can be applied similarly. Hence, we define the function ψ such that it represents such a value and examine how to obtain the function values for a level-κ encoding of zero of arbitrary size.

When the size of x is small, by the zero-testing lemma, $[p_{zt} \cdot x]_N$ gives the integer value $\sum_{i=1}^{n} r_i v_i + a v_0$. However, if the size of x is large, the zero-testing lemma does not hold and one cannot compute the integer value directly. To reach the goal, we use the ladder $X_j^{(\kappa)} = \sum_{i=1}^{n} r_{ij}^{(\kappa)} u_i' + a_j^{(\kappa)}$. Let x be a level-κ encoding of zero. Then, we can compute the size-reduced encoding x' using the ladder and obtain the quantity

$$\begin{aligned}
[p_{zt} \cdot x']_N &= \Big[p_{zt} \cdot \Big(x - \sum_{j=0}^{\gamma+\lfloor \log_2 \ell \rfloor} b_j X_j^{(\kappa)} \Big) \Big]_N \\
&= \sum_{i=1}^{n} \Big(r_i - \sum_{j=0}^{\gamma+\lfloor \log_2 \ell \rfloor} b_j r_{ij}^{(\kappa)} \Big) v_i + \Big(a - \sum_{j=0}^{\gamma+\lfloor \log_2 \ell \rfloor} b_j a_j^{(\kappa)} \Big) v_0 \\
&= \sum_{i=1}^{n} r_i v_i + a v_0 - \sum_{j=0}^{\gamma+\lfloor \log_2 \ell \rfloor} b_j \Big(\sum_{i=1}^{n} r_{ij}^{(\kappa)} v_i + a_j^{(\kappa)} v_0 \Big).
\end{aligned}$$

Therefore, if one can compute $\sum_{i=1}^{n} r_{ij}^{(\kappa)} v_i + a_j^{(\kappa)} v_0$ from $X_j^{(\kappa)}$, one can easily obtain $\sum_{i=1}^{n} r_i v_i + a v_0$.

To compute $\sum_{i=1}^{n} r_{ij}^{(\kappa)} v_i + a_j^{(\kappa)} v_0$ for all $j \in \{0, \cdots, \gamma + \lfloor \log_2 \ell \rfloor\}$, we use an induction on j. When $j = 0$, $[p_{zt} \cdot X_0^{(\kappa)}]_N$ gives $\sum_{i=1}^{n} r_{i0}^{(\kappa)} v_i + a_0^{(\kappa)} v_0$, by the zero-testing lemma. Suppose we have $\sum_{i=1}^{n} r_{ij}^{(\kappa)} v_i + a_j^{(\kappa)} v_0$ for $j \in \{0, \cdots, t-1\}$; then, $[p_{zt} \cdot X_t]_N = \sum_{i=1}^{n} r_{it}^{(\kappa)} v_i + a_t^{(\kappa)} v_0 - \sum_{j=0}^{t-1} b_j (\sum_{i=1}^{n} r_{ij}^{(\kappa)} v_i + a_j^{(\kappa)} v_0)$ for computable $b_i \in \{0, 1\}$, where X_t is a size-reduced encoding of $X_t^{(\kappa)}$ using $\{X_0^{(\kappa)}, \cdots, X_{t-1}^{(\kappa)}\}$. Since we know the latter terms, we can also compute $\sum_{i=1}^{n} r_{it}^{(\kappa)} v_i + a_t^{(\kappa)} v_0$. This idea can be extended to any level ladder.

Now, we give a precise description of function ψ.

$$\begin{aligned}\psi : \mathbb{Z} &\to \mathbb{Z}\\ x &\mapsto \sum_{i=1}^{n}\Big[x\cdot\frac{z^\kappa}{g_i}\Big]_{p_i} v_i + \frac{x-\sum_{i=1}^{n}[x\cdot\frac{z^\kappa}{g_i}]_{p_i}u_i'}{x_0}v_0,\end{aligned}$$

where $v_i = [p_{zt}\cdot u_i']_N (1\le i\le n)$ and $v_0 = [p_{zt}\cdot x_0]_N$. Note that $x \equiv \sum_{i=1}^{n}[x\cdot\frac{z^\kappa}{g_i}]_{p_i}u_i' \pmod{p_j}$ for $1\le j\le n$. Hence, the value multiplied by v_0 is an integer and the function is well-defined.

Proposition 1. *Let x be an integer such that $x \equiv \frac{r_i\cdot g_i}{z^\kappa} \pmod{p_i}$ for $1\le i\le n$. If $|r_i| < p_i/2$ for each i, then x can be uniquely expressed as $\sum_{i=1}^{n} r_i u_i' + a x_0$ for some integer a, and $\psi(x) = \sum_{i=1}^{n} r_i v_i + a v_0$.*

Proof. We can see that $x\equiv \sum_{i=1}^{n} r_i u_i' \pmod{p_j}$ for each j and thus there exists an integer a such that $x = \sum_{i=1}^{n} r_i u_i' + a x_0$. For uniqueness, suppose x can be written as $x = \sum_{i=1}^{n} r_i' u_i' + a' x_0$ for integers $r_1',\cdots,r_n',a'$ with $|r_i'| < p_i/2$. Then, $x\equiv r_i'[\frac{g_i}{z^\kappa}\big(\frac{x_0}{p_i}\big)^{-1}]_{p_i} \equiv \frac{r_i' g_i}{z^\kappa} \pmod{p_i}$, which implies $r_i \equiv r_i' \pmod{p_i}$. Since $|r_i - r_i'| < p_i$, we have $r_i' = r_i$ for each i and therefore $a' = a$, which proves the uniqueness. □

Proposition 2. *Let $x_1,\cdots,x_m$ be level-κ encodings of zero such that $x_j \equiv \dfrac{r_{ij}g_i}{z^\kappa} \pmod{p_i}$ and $|r_{ij}| < p_i/2$ for all $1\le i\le n$, $1\le j\le m$. Then, the equality*

$$\psi\Big(\sum_{j=1}^{m} x_j\Big) = \sum_{j=1}^{m}\psi(x_j),$$

holds if $\Big|\sum_{j=1}^{m} r_{ij}\Big| < \dfrac{p_i}{2}$*, for all $1\le i\le n$.*

Proof. From Proposition 1, each x_j can be uniquely written as $x_j = \sum_{i=1}^{n} r_{ij}u_i' + a_j x_0$ for some integer a_j, and $\psi(x_j) = \sum_{i=1}^{n} r_{ij}v_i + a_j v_0$. Then,

$$\begin{aligned}\sum_{j=1}^{m}\psi(x_j) &= \sum_{i=1}^{n}\Big(\sum_{j=1}^{m} r_{ij}\Big)\cdot v_i + \Big(\sum_{j=1}^{m} a_j\Big)\cdot v_0\\ &= \psi\Big(\Big(\sum_{j=1}^{m} r_{ij}\Big)\cdot u_i' + \Big(\sum_{j=1}^{m} a_j\Big)\cdot x_0\Big) = \psi\Big(\sum_{j=1}^{m} x_j\Big),\end{aligned}$$

where the source of the second equality is Proposition 1, since $\big|\sum_{j=1}^{m} r_{ij}\big| < p_i/2$. □

Our strategy to attack CLT15 is similar to that in [CHL+15]. The goal is to construct a matrix equation over $\mathbb{Q}$ by computing the ψ values of several products of level-$0,1$, and $(\kappa-1)$ encodings, fixed on level-0 encoding. We proceed using the following three steps.

(Step 1) Compute the ψ-value of level-κ ladder
(Step 2) Compute the ψ-value of level-κ encodings of large size
(Step 3) Construct matrix equations over $\mathbb{Q}$.

Using the matrix equations in **Step 3**, we have a matrix, the eigenvalues of which are residue modulo p_i of level-0 encoding. From this, we deduce a secret modulus p_i.

3.3 Computing the ψ-value of $\boldsymbol{X_j^{(\kappa)}}$

To apply the zero-testing lemma to a level-κ encoding of zero $x = \sum_{i=1}^n r_i u_i' + a x_0$, the size of r_i and a has to be bounded by some fixed values. By the parameter setting, η is larger than the maximum bit size of the noise r_i of a level-κ encoding obtained from the multiplication of lower level encodings. Hence, we need to reduce the size of x so that a satisfies the zero testing lemma.

Let us consider a ladder of level-κ encodings of zero $\{X_j^{(\kappa)}\}$. This is provided to reduce the size of encodings to that of $2x_0$. More precisely, given a level-κ encoding of zero x of size smaller than $2^{2\gamma+\lfloor \log_2 \ell \rfloor}$, one can compute $x' = x - \sum_{j=0}^{\gamma'} b_j X_j^{(\kappa)}$ for $\gamma' = \gamma + \lfloor \log_2 \ell \rfloor$, which is an encoding of the same plaintext; its size is smaller than $2x_0$. As noted in [CLT15], the sizes of $X_j^{(\kappa)}$ are increasing and differ by only one bit, and therefore, $b_j \in \{0,1\}$, which implies the noise grows additively. We can reduce a to an integer much smaller than $2^{2\eta-\beta-1}/n$ so that the zero testing lemma can be applied. We denote such x' as $[x]_{\boldsymbol{X}^{(\kappa)}}$. More generally, we use the notation

$$[x]_{\boldsymbol{X}^{(t)}} := [\cdots[[x]_{X_{\gamma'}^{(t)}}]_{X_{\gamma'-1}^{(t)}} \cdots]_{X_0^{(t)}} \qquad \text{for } \boldsymbol{X}^{(t)} = (X_0^{(t)}, X_1^{(t)}, \ldots, X_{\gamma'}^{(t)}), 1 \le t \le \kappa.$$

Note that, if x satisfies the condition in Lemma 1, i.e., it is an encoding of zero of small size, then $\psi(x)$ is exactly the same as $[p_{zt} \cdot x]_N$. However, if the size of x is large, it is congruent only to $[p_{zt} \cdot x]_N$ modulo N. Now, we show how to compute the integer value $\psi(x)$ for an encoding x of zero, although x does not satisfy the condition in Lemma 1.

First, we adapt the size reduction process to a level-κ ladder itself. We can compute binary b_{ij} for each i, j, satisfying

$$\begin{aligned}
[X_0^{(\kappa)}]_{\boldsymbol{X}^{(\kappa)}} &= X_0^{(\kappa)} \\
[X_1^{(\kappa)}]_{\boldsymbol{X}^{(\kappa)}} &= X_1^{(\kappa)} - b_{10} \cdot X_0^{(\kappa)} \\
[X_2^{(\kappa)}]_{\boldsymbol{X}^{(\kappa)}} &= X_2^{(\kappa)} - \sum_{k=0}^{1} b_{2k} \cdot X_k^{(\kappa)} \\
&\vdots \\
[X_j^{(\kappa)}]_{\boldsymbol{X}^{(\kappa)}} &= X_j^{(\kappa)} - \sum_{k=0}^{j-1} b_{jk} \cdot X_k^{(\kappa)}.
\end{aligned}$$

Each $[X_j^{(\kappa)}]_{\boldsymbol{X}^{(\kappa)}}$ is an encoding of zero at level κ and therefore can be written as $[X_j^{(\kappa)}]_{\boldsymbol{X}^{(\kappa)}} = \sum_{i=1}^n r'_{ij} u_i' + a_j' x_0$ for some integers r'_{ij} and a'_j. Moreover, its bit size is at most γ and therefore a'_j is small enough to satisfy the condition in Lemma 1. Therefore,

$$\psi([X_j^{(\kappa)}]_{\boldsymbol{X}^{(\kappa)}}) = [p_{zt} \cdot [X_j^{(\kappa)}]_{\boldsymbol{X}^{(\kappa)}}]_N = \sum_{i=1}^n r'_{ij} v_i + a'_j v_0.$$

If we write $X_j^{(\kappa)} = \sum_{i=1}^n r_{ij} u_i' + a_j x_0$ for some integer $r_{1j}, \ldots, r_{nj}, a_j$, we have $r'_{ij} = r_{ij} - \sum_{k=0}^{j-1} b_{jk} r_{ik}$ for each i and $a'_j = a_j - \sum_{k=0}^{j-1} b_{jk} a_k$, since all the coefficients of u_i' are sufficiently smaller than p_i for each i. Therefore,

$$\sum_{i=1}^{n} r_{ij}' v_i + a_j' v_0 = \sum_{i=1}^{n} r_{ij} v_i + a_j v_0 - \sum_{k=0}^{j-1} b_{jk} \Big(\sum_{i=1}^{n} r_{ik} v_i + a_k v_0 \Big)$$

holds over the integers. Hence, we have the following inductive equations for $0 \leq j \leq \gamma'$.

$$\psi(X_j^{(\kappa)}) = \Big[p_{zt} \cdot [X_j^{(\kappa)}]_{\boldsymbol{X}^{(\kappa)}} \Big]_N + \sum_{k=0}^{j-1} b_{jk} \cdot \psi\Big(X_k^{(\kappa)} \Big),$$

which gives all $\psi(X_0^{(\kappa)}), \psi(X_1^{(\kappa)}), \ldots, \psi(X_{\gamma'}^{(\kappa)})$, inductively. The computation consists of $(\gamma' + 1)$ zero testing and $O(\gamma^2)$-times comparisons and subtractions of $(\gamma + \gamma')$-bit integers, and therefore, the total computation cost is $\widetilde{O}(\gamma^2)$ by using fast Fourier transform. Hence, we obtain the following lemma.

Lemma 2. *Given the public parameters of the CLT15 scheme, one can compute*

$$\psi(X_j^{(\kappa)}) = \Big[p_{zt} \cdot [X_j^{(\kappa)}]_{\boldsymbol{X}^{(\kappa)}} \Big]_N + \sum_{k=0}^{j-1} b_{jk} \cdot \psi\left(X_k^{(\kappa)} \right)$$

in $\widetilde{O}(\gamma^2)$ bit computations.

3.4 Computing the ψ-value of Level-κ Encodings of Large Size

Using the ψ values of the κ-level ladder, we can compute the ψ value of any κ-level encoding of zero, the bit size of which is between γ and $\gamma + \gamma'$.

Lemma 3. *Let x be a level-κ encoding of zero, $x = \mathsf{CRT}_{(p_i)}\left(\frac{r_i g_i}{z^\kappa}\right) + q x_0 = \sum_{i=1}^{n} r_i u_i' + a x_0$ for some integer $r_1, \ldots, r_n, a$ satisfying $|r_i| < 2^{\eta - \beta - \log_2 n - 7}$ for each i and $|a| < 2^{\gamma'}$. Given the public parameters of the CLT15 scheme, one can compute the value $\psi(x) = \sum_{i=1}^{n} r_i v_i + a v_0$ in $\widetilde{O}(\gamma^2)$ bit computations.*

Proof. Let x be a level-κ encoding of zero satisfying the above conditions. As in Section 3.3, we can find binary b_j's satisfying $[x]_{\boldsymbol{X}^{(\kappa)}} = x - \sum_{j=0}^{\gamma'} b_j \cdot X_j^{(\kappa)}$. Then, we have

$$\psi(x) = \psi([x]_{\boldsymbol{X}^{(\kappa)}}) + \sum_{j=0}^{\gamma'} b_j \cdot \psi(X_j^{(\kappa)}).$$

Since $[x]_{\boldsymbol{X}^{(\kappa)}}$ is a κ-level encoding of zero of at most γ-bit and the size of noise is bounded by $(\eta - \beta - \log_2 n - 6)$-bit, we can compute the value $\psi([x]_{\boldsymbol{X}^{(\kappa)}})$ via the zero testing procedure. Finally, the ψ values of the κ-level ladder and $\psi([x]_{\boldsymbol{X}^{(\kappa)}})$ give the value $\psi(x)$. The source of the complexity is Lemma 2. ☐

We apply Lemma 3 to obtain the ψ value of a κ-level encoding of zero that is a product of two encodings of $(\gamma + \gamma')$-bit size.

Lemma 4. *Let X be a level-1 encoding and Y a level-$(\kappa - 1)$ encoding of zero of bit size at most $\gamma + \gamma'$. Then, one can compute $\psi(XY)$ in $\widetilde{O}(\gamma^3)$ bit computations.*

Proof. We apply Lemma 3 to a product of two γ-bit encodings. From $[X_1^{(1)}]_{\boldsymbol{X}^{(1)}} = X_1^{(1)} - b\cdot X_0^{(1)}$ for some $b\in\{0,1\}$, we find $\psi(X_1^{(1)}\cdot X_0^{(\kappa-1)}) = \psi([X_1^{(1)}]_{\boldsymbol{X}^{(1)}}\cdot X_0^{(\kappa-1)}) + b\cdot \psi(X_0^{(1)}\cdot X_0^{(\kappa-1)})$, since $[X_1^{(1)}]_{\boldsymbol{X}^{(1)}}$ is γ-bit. Thus, we can obtain inductively all $\psi(X_j^{(1)}\cdot X_k^{(\kappa-1)})$ for each j,k from $\psi(X_{l_j}^{(1)}\cdot X_{l_k}^{(\kappa-1)}),\ 0\le l_j\le j, 0\le l_k\le k, (l_j,l_k)\neq(j,k)$.

Let $[X]_{\boldsymbol{X}^{(1)}} = X - \sum_{j=0}^{\gamma'} b_j\cdot X_j^{(1)}$ and $[Y]_{\boldsymbol{X}^{(\kappa-1)}} = Y - \sum_{j=0}^{\gamma'} b'_j\cdot X_j^{(\kappa-1)}$. Then,

$$\begin{aligned}[X]_{\boldsymbol{X}^{(1)}}\cdot[Y]_{\boldsymbol{X}^{(\kappa-1)}} = XY &- \textstyle\sum_j b_j\cdot X_j^{(1)}\cdot Y \\ &- \textstyle\sum_j b'_j\cdot X_j^{(\kappa-1)}\cdot X + \sum_{j,k} b_j b'_k\cdot X_j^{(1)}\cdot X_k^{(\kappa-1)}.\end{aligned}$$

Note that the noise of $[[X]_{\boldsymbol{X}^{(1)}}\cdot[Y]_{\boldsymbol{X}^{(\kappa-1)}}]_{\boldsymbol{X}^{(\kappa)}}$ is bounded by $2\rho+\alpha+2\log_2(\gamma')+2$ and $\eta > \kappa(2\alpha+2\rho+\lambda+2\log_2 n+3)$, and therefore, we can adapt Proposition 2. Therefore, if we know the ψ-value of each term, we can compute the ψ-value of XY. Finally, Lemma 3 enables one to compute $\psi([X]_{\boldsymbol{X}^{(1)}}\cdot[Y]_{\boldsymbol{X}^{(\kappa-1)}})$. The second and third terms of the right hand side can be computed using $[X_j^{(1)}]_{\boldsymbol{X}^{(1)}}$, $[X_j^{(\kappa-1)}]_{\boldsymbol{X}^{(\kappa-1)}}$, and we know the ψ-value of the last one. Since we perform zero testings for $O(\gamma^2)$ encodings of zero, the complexity becomes $\widetilde{O}(\gamma^3)$. □

Note that the above Lemma can be applied to a level-t encoding X and a level-$(\kappa-t)$ encoding of zero Y. The proof is exactly the same, except for the indexes.

3.5 Constructing Matrix Equations over $\mathbb{Q}$

We reach the final stage. The following theorem is the result.

Theorem 1. *Given the public instances in [CLT15] and p_{zt}, sampled from $\mathsf{InstGen}(1^\lambda, 1^\kappa)$, one can find all the secret parameters given in [CLT15] in $\widetilde{O}(\kappa^{\omega+4}\lambda^{2\omega+6})$ bit computations with $\omega\le 2.38$.*

Proof. We construct a matrix equation by collecting several ψ-values of the product of level-0, 1 and $(\kappa-1)$ encodings. Let c, X, and Y be a level-0, 1, and $(\kappa-1)$ encoding, respectively, and additionally we assume Y is an encoding of zero. Let us express them as

$$\begin{aligned} c &= \mathsf{CRT}_{(p_i)}(c_i),\\ X &= \mathsf{CRT}_{(p_i)}\left(\frac{x_i}{z}\right) = x_i\left[z^{-1}\right]_{p_i} + q_i p_i,\\ Y &= \mathsf{CRT}_{(p_i)}\left(\frac{y_i g_i}{z^{\kappa-1}}\right) = \sum_{i=1}^n y_i\left[\frac{g_i}{z^{\kappa-1}}\left(\frac{x_0}{p_i}\right)^{-1}\right]_{p_i}\cdot\frac{x_0}{p_i} + a x_0.\end{aligned}$$

Assume that the size of each is less than $2x_0$. The product of c and X can be written as $cX = c_i x_i\left[z^{-1}\right]_{p_i} + q'_i p_i$ for some integer q'_i.

By multiplying cX and Y, we have

$$\begin{aligned} &cXY\\ &= \sum_{i=1}^n\left(c_i x_i y_i\left[z^{-1}\right]_{p_i}\left[\frac{g_i}{z^{\kappa-1}}\left(\frac{x_0}{p_i}\right)^{-1}\right]_{p_i}\cdot\frac{x_0}{p_i} + y_i\left[\frac{g_i}{z^{\kappa-1}}\left(\frac{x_0}{p_i}\right)^{-1}\right]_{p_i} q'_i x_0\right) + (cX)(ax_0)\\ &= \sum_{i=1}^n c_i x_i y_i u'_i + \sum_{i=1}^n (c_i x_i y_i s_i + y_i\theta_i q'_i)x_0 + acXx_0,\end{aligned}$$

where $\theta_i = \left[\frac{g_i}{z^{\kappa-1}}\left(\frac{x_0}{p_i}\right)^{-1}\right]_{p_i}$, $\theta_i\left[z^{-1}\right]_{p_i}\frac{x_0}{p_i} = u_i' + s_i x_0$ for some integer $s_i \in \mathbb{Z}$. Then, we can obtain $\psi(cXY) = \sum_{i=1}^n c_i x_i y_i v_i + \sum_{i=1}^n (c_i x_i y_i s_i + y_i \theta_i q_i')v_0 + acXv_0$ by Lemma 4.

By plugging $q_i' = \frac{1}{p_i}(cX - c_i x_i [z^{-1}]_{p_i})$ into the equation, we obtain

$$\begin{aligned}\psi(cXY) &= \sum_{i=1}^n y_i(v_i + s_i v_0 - \frac{\theta_i v_0}{p_i}[z^{-1}]_{p_i})c_i x_i + \sum_{i=1}^n y_i \frac{\theta_i v_0}{p_i} cX + av_0 cX \\ &= \sum_{i=1}^n y_i w_i c_i x_i + \sum_{i=1}^n y_i w_i' cX + av_0 cX,\end{aligned}$$

where $w_i = v_i + s_i v_0 - \frac{\theta_i}{p_i}[z^{-1}]_{p_i} v_0$ and $w_i' = \frac{\theta_i v_0}{p_i}$. It can be written (over $\mathbb{Q}$) as

$$\psi(cXY) = \begin{pmatrix} y_1 \; y_2 \; \cdots \; y_n \; a \end{pmatrix} \begin{pmatrix} w_1 & & & 0 & w_1' \\ & w_2 & & & w_2' \\ & & \ddots & & \vdots \\ & & & w_n & w_n' \\ 0 & & & & v_0 \end{pmatrix} \begin{pmatrix} c_1 x_1 \\ c_2 x_2 \\ \vdots \\ c_n x_n \\ cX \end{pmatrix}. \tag{2}$$

Since $p_i w_i = p_i(v_i + s_i v_0) - \theta_i\left[z^{-1}\right]_{p_i} v_0 \equiv -\theta_i\left[z^{-1}\right]_{p_i} v_0 \not\equiv 0 \pmod{p_i}$, w_i is not equal to zero. Therefore, $v_0 \prod_{i=1}^n w_i \neq 0$ and thus the matrix in Equation (2) is non singular. By applying Equation (2) to various X, Y, taking for $0 \le j, k \le n$

$$\begin{aligned} X &= [X_j^{(1)}]_{\boldsymbol{X}^{(1)}} = \mathsf{CRT}_{(p_i)}\left(\frac{x_{ij}}{z}\right), \\ Y &= [X_k^{(\kappa-1)}]_{\boldsymbol{X}^{(\kappa-1)}} = \sum_{i=1}^n y_{ik}\theta_i \frac{x_0}{p_i} + a_k x_0, \end{aligned}$$

we finally obtain the matrix equation

$$\begin{aligned}\boldsymbol{W}_c &= \begin{pmatrix} y_{10} & \cdots & y_{n0} & a_0 \\ & & & \\ & \ddots & & \vdots \\ & & & \\ y_{1n} & \cdots & y_{nn} & a_n \end{pmatrix} \begin{pmatrix} w_1 & & & 0 & w_1' \\ & w_2 & & & w_2' \\ & & \ddots & & \vdots \\ & & & w_n & w_n' \\ 0 & & & & v_0 \end{pmatrix} \begin{pmatrix} c_1 & & & 0 \\ & c_2 & & \\ & & \ddots & \\ & & & c_n & \\ 0 & & & & c \end{pmatrix} \begin{pmatrix} x_{10} & \cdots & x_{1n} \\ & & \\ & \ddots & \vdots \\ x_{n0} & & x_{nn} \\ X_0 & \cdots & X_n \end{pmatrix} \\ &= \qquad\quad \boldsymbol{Y} \qquad\qquad\qquad \boldsymbol{W} \qquad\qquad \mathsf{diag}(c_1, \cdots, c_n, c) \qquad\quad \boldsymbol{X}.\end{aligned}$$

We perform the same computation on $c = 1$, which is a level-0 encoding of $\mathbf{1} = (1, 1, \cdots, 1)$, and then, it implies

$$\boldsymbol{W}_1 = \boldsymbol{Y} \cdot \boldsymbol{W} \cdot \boldsymbol{I} \cdot \boldsymbol{X}.$$

From $\boldsymbol{W}_c$ and $\boldsymbol{W}_1$, we have a matrix that is similar to $\mathsf{diag}(c_1, \cdots, c_n, c)$:

$$\boldsymbol{W}_1^{-1} \cdot \boldsymbol{W}_c = \boldsymbol{X}^{-1} \cdot \mathsf{diag}(c_1, \cdots, c_n, c) \cdot \boldsymbol{X}.$$

Then, by computing the eigenvalues of $\boldsymbol{W}_1^{-1} \cdot \boldsymbol{W}_c$, we have $c_1, \cdots, c_n$, satisfying $p_i|(c - c_i)$ for each i. Using an additional level-0 encoding c', we obtain $\boldsymbol{W}_1^{-1} \cdot \boldsymbol{W}_{c'}$, and therefore, $c'_1, \cdots, c'_n$ with $p_i|(c' - c'_i)$ for each i. Computing $\gcd(c - c_i, c' - c'_i)$ gives the secret prime p_i.

Using $p_1, \cdots, p_n$, we can recover all the remaining parameters. By the definition of y and $X_j^{(1)}$, the equation $y/[X_j^{(1)}]_{x_0} \equiv (r_i g_i + 1)/(r_{ij}^{(1)} g_i) \pmod{p_i}$ is satisfied. Since $r_i g_i + 1$ and $r_{ij}^{(1)} g_i$ are smaller than $\sqrt{p_i}$ and are co-prime, one can recover them by rational reconstruction up to the sign. Therefore, we can obtain g_i by computing the gcd of $r_{i0}^{(1)} g_i, \cdots, r_{im}^{(1)} g_i$. Moreover, using $r_{ij}^{(1)} g_i$ and $[X_j^{(1)}]_{x_0}$, we can compute $[z]_{p_i}$ for each i and therefore z. Any other parameters are computed using z, g_i, and p_i.

Our attack consists of the following arithmetics: computing $\psi(X_j^{(\kappa)})$, $\psi(X_j^{(1)} \cdot X_k^{(\kappa-1)})$, constructing a matrix $\boldsymbol{W}_c$ and $\boldsymbol{W}_1$, matrix inversing and multiplying, and computing eigenvalues and the greatest common divisor. All of these are bounded by $\widetilde{O}(\gamma^3 + n^\omega \gamma) = \widetilde{O}(\kappa^6 \lambda^9)$ bit computations with $\omega \leq 2.38$. For this algorithm to succeed, we need a property that $\boldsymbol{W}_1$ is non-singular. If we use the fact that the rank of a matrix $\boldsymbol{A} \in \mathbb{Z}^{(n+1)\times(n+1)}$ can be computed in time $\widetilde{\mathcal{O}}\left((n+1)^\omega \log \|\boldsymbol{A}\|_\infty\right)$ (see [Sto09]), we can find that $\boldsymbol{X}, \boldsymbol{Y} \cdot \boldsymbol{W} \in \mathbb{Q}^{(n+1)\times(n+1)}$ are non-singular in $\widetilde{\mathcal{O}}(2(\gamma + \log \ell)(n^\omega \log N)) = \widetilde{\mathcal{O}}(\kappa^{\omega+4} \lambda^{2\omega+6})$ by considering another subset of $\{X_0^{(1)}, \cdots, X_{\gamma'}^{(1)}\}$ with cardinality $(n+1)$ for X and also for Y. Therefore, the total complexity of our attack is $\widetilde{\mathcal{O}}(\kappa^{\omega+4} \lambda^{2\omega+6})$. $\square$

4 Conclusion

In this paper, we introduced a cryptanalysis of the new multilinear maps over the integers [CLT15]. The scheme was modified to prevent a zeroizing attack [CHL+15] on the original scheme [CLT13]. The zero-testing element is defined over the independent modulus N so that the resulting value is expressed non-linearly. $x_0 = \prod_{i=1}^n p_i$ was not published for security reasons, but we can compute all the secret primes p_i in polynomial time. Therefore, the modified scheme also is vulnerable to a zeroizing attack.

As other analyses of multilinear maps [CGH+15,CHL+15,HJ15], our analysis is based on a zeroizing attack. To construct a matrix equation, we need encodings of zero. It is worth considering analyzing multilinear maps without encodings of zero. The construction of a graded encoding scheme for which the subgroup membership and decision linear problems are hard is another open problem.

References

BWZ14. Dan Boneh, David J Wu, and Joe Zimmerman. Immunizing multilinear maps against zeroizing attacks. *IACR Cryptology ePrint Archive*, 2014:930, 2014.

CGH+15. Jean-Sébastien Coron, Craig Gentry, Shai Halevi, Tancrede Lepoint, Hemanta K Maji, Eric Miles, Mariana Raykova, Amit Sahai, and Mehdi Tibouchi. Zeroizing without low-level zeroes: New mmap attacks and their limitations. In *Advances in Cryptology–CRYPTO 2015*, pages 247–266. Springer, 2015.

CHL+15. Jung Hee Cheon, Kyoohyung Han, Changmin Lee, Hansol Ryu, and Damien Stehlé. Cryptanalysis of the multilinear map over the integers. In *Advances in Cryptology–EUROCRYPT 2015*, pages 3–12. Springer, 2015.

CLT13. Jean-Sébastien Coron, Tancrede Lepoint, and Mehdi Tibouchi. Practical multilinear maps over the integers. In *Advances in Cryptology–CRYPTO 2013*, pages 476–493. Springer, 2013.

CLT15. Jean-Sebastien Coron, Tancrede Lepoint, and Mehdi Tibouchi. New multilinear maps over the integers. In *Advances in Cryptology–CRYPTO 2015*, pages 267–286. Springer, 2015.

GGH13. Sanjam Garg, Craig Gentry, and Shai Halevi. Candidate multilinear maps from ideal lattices. In *Eurocrypt*, volume 7881, pages 1–17. Springer, 2013.

GGH15. Craig Gentry, Sergey Gorbunov, and Shai Halevi. Graph-induced multilinear maps from lattices. In *Theory of Cryptography*, pages 498–527. Springer, 2015.

GGHZ14. Sanjam Garg, Craig Gentry, Shai Halevi, and Mark Zhandry. Fully secure functional encryption without obfuscation. Technical report, Cryptology ePrint Archive, Report 2014/666, 2014.

HJ15. Yupu Hu and Huiwen Jia. Cryptanalysis of GGH map. Technical report, Cryptology ePrint Archive, Report 2015/301, 2015.

Sho09. Victor Shoup. *A Computational Introduction to Number Theory and Algebra*. Cambridge University Press, 2009.

Sto09. Arne Storjohann. Integer matrix rank certification. In *Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation*, pages 333–340. ACM, 2009.