Cryptanalysis on the Multilinear Map over the Integers and its Related Problems *

Jung Hee Cheon, Kyoohyung Han, Changmin Lee, Hansol Ryu

Seoul National University (SNU), South Korea
{jhcheon, satanigh, cocomi11, sol8586}@snu.ac.kr

Damien Stehlé

ENS de Lyon, Laboratoire LIP (U. Lyon, CNRS, ENSL, INRIA, UCBL), France
damien.stehle@ens-lyon.fr

Abstract

The $\mathsf{CRT\text{-}ACD}$ problem is to find the primes $p_1, \ldots, p_n$ given polynomially many instances of $\mathsf{CRT}_{(p_1,\ldots,p_n)}(r_1, \ldots, r_n)$ for small integers $r_1, \ldots, r_n$. The $\mathsf{CRT\text{-}ACD}$ problem is regarded as a hard problem, but its hardness is not proven yet. In this paper, we analyze the $\mathsf{CRT\text{-}ACD}$ problem when given one more input $\mathsf{CRT}_{(p_1,\ldots,p_n)}(x_0/p_1, \ldots, x_0/p_n)$ for $x_0 = \prod_{i=1}^{n} p_i$ and propose a polynomial-time algorithm for this problem by using products of the instances and auxiliary input.

This algorithm yields a polynomial-time cryptanalysis of the (approximate) multilinear map of Coron, Lepoint and Tibouchi (CLT): We show that by multiplying encodings of zero with zero-testing parameters properly in the CLT scheme, one can obtain a required input of our algorithm: products of $\mathsf{CRT\text{-}ACD}$ instances and auxiliary input. This leads to a total break: all the quantities that were supposed to be kept secret can be recovered in an efficient and public manner.

We also introduce polynomial-time algorithms for the Subgroup Membership, Decision Linear, and Graded External Diffie-Hellman problems, which are used as the base problems of several cryptographic schemes constructed on multilinear maps.

Keywords: Multilinear maps, Graded encoding schemes, Decision linear problem, Subgroup membership problem, Graded external Diffie-Hellman problem.

1 Introduction

Cryptographic bilinear maps, which was made possible thanks to pairings over elliptic curves, have led to a bounty of exciting cryptographic applications. In 2002, Boneh and Silverberg [7] formalized the concept of cryptographic multilinear maps and provided two applications: a one-round multi-party key exchange protocol and a very efficient broadcast encryption scheme.

*A preliminary version of this paper appeared in the *Proceedings of EUROCRYPT 2015*, Lecture Notes in Computer Science 9056, Springer-Verlag [12].

However, these promising applications were only vague exercises as no realization of such multilinear maps was known. This had changed around ten years later as Garg, Gentry and Halevi proposed the first approximation of multilinear maps [21]. They introduced the concept of (approximate) graded encoding scheme as a variant of multilinear maps and described a candidate construction relying on ideal lattices (which we will refer to as GGH in this work). Soon after, Coron, Lepoint and Tibouchi [15] proposed another candidate construction of a graded encoding scheme relying on a variant of the approximate greatest common divisor problem, for short, CLT.

The GGH and CLT constructions share similarities as they are both derived from a homomorphic encryption scheme, Gentry's scheme [25] and the van Dijk *et al.* scheme [36], respectively. And both rely on extra public data called the zero-testing or extraction parameter, which allow them to publicly decide whether the plaintext data hidden in a given encoding is zero, as long as the encoding is not the output of a too deep homomorphic evaluation circuit.

Graded encoding schemes serve as a basis to define presumably hard problems. These problems are then used as security foundations of cryptographic constructions. A major discrepancy between GGH and CLT is that some natural problems seem easy when instantiated with the GGH graded encoding scheme and hard with CLT. Such problems are subgroup membership (SubM) and decision linear (DLIN). Briefly, SubM is to distinguish between encodings of elements of a group and encodings of elements one of its subgroup thereof whereas DLIN is to determine whether a matrix of elements is singular, given input encodings of those elements. Another similar discrepancy appears to exist between the asymmetric variants of GGH and CLT; the Graded External Decision Diffie-Hellman (GXDH) problem seems hard with CLT while it is easy for GGH. GXDH is exactly DDH for one of the components of the asymmetric graded encoding scheme. These problems have been initially used in the context of cryptographic bilinear maps [4, 5, 34].

For example, in [29], Gentry *et al.* provide a framework to prove the security of witness encryption schemes. They use computational assumptions involving graded encodings to prove the security of their witness encryption scheme. Another important application of multilinear maps is a construction of secure indistinguishability obfuscation. In [28], Gentry *et al.* provide the first construction of indistinguishability obfuscation which is secure under an instance independent computational assumption, the so-called Multilinear Subgroup Elimination Assumption. These works rely on computational assumptions involving the CLT multilinear maps that are variants of the SubM problem.

In the first public version of [21] (dated 29 Oct. 2012),[1] the GGH construction was thought to provide secure DLIN instantiation. It was soon realized that DLIN could be broken in polynomial-time. The attack consists in multiplying an encoding of some element m by an encoding of 0 and by the zero-testing parameter; this produces a small element (because the encoded value is $m \cdot 0 = 0$), which happens to be a multiple of m. This *zeroizing attack* (also called weak discrete logarithm attack) is dramatic for SubM, DLIN and GXDH. Fortunately, it does not seem useful against other problems, such as Graded Decision Diffie Hellman (GDDH) and the adaptation of DDH to the graded encoding scheme setting. As no such attack was known for CLT, the presumed hardness of the CLT instantiations of SubM, DLIN and GXDH was exploited as a security grounding for several cryptographic constructions [1–3, 6, 23, 24, 28, 29, 33, 37, 38].

Zeroizing Attack on GGH. Garg *et al.* constructed the first approximation to multilinear

[1] It can be accessed from the IACR eprint server.

maps by using graded encoding scheme and zero-testing parameter [21] which is defined on ring $R_q = \mathbb{Z}_q[X]/\langle X^n + 1\rangle$. By exploiting a zero-testing parameter, any user can decide whether two encodings encode the same value or not. More precisely, they publish a zero-testing parameter $\mathbf{p}_{zt}$ then the quantity $[\mathbf{u} \cdot \mathbf{p}_{zt}]_q$ is small if and only if u is a top encoding of zero. This property creates a weakness in the scheme in case of "zeroizing attack". When $\mathbf{u}$ is a top level encoding of zero, the zero-testing value gives an equation which holds in $R = \mathbb{Z}[X]/\langle X^n + 1\rangle$ not only in R_q. Using these equations, one can compute some fixed multiples of secrets and solve some hardness problems associated with GGH scheme (For a more detailed description, refer the reader to [21]).

Our Contributions. First, we abstract a hardness problem of the CLT scheme to CRT-ACD with auxiliary input. The CRT-ACD with auxiliary input is to find η-bit primes p_i for all $1 \le i \le n$ for given many samples in the form of $\mathsf{CRT}_{(p_1,\cdots,p_n)}(r_1, \cdots, r_n)$ which is an integer congruent to integer $|r_i| < 2^{\varepsilon}$, $x_0 = \prod_{i=1}^{n} p_i$ and $\hat{P} = \mathsf{CRT}_{(p_1,\cdots,p_n)}(x_0/p_1, \cdots, x_0/p_n)$.

Next, We describe an analysis of a CRT-ACD with auxiliary input. Moreover, we adapt the method to the CLT graded encoding scheme. It runs in polynomial-time and allows one to publicly compute all the parameters of the CLT scheme that were supposed to be kept secret.

In addition, we introduce cryptanalytic algorithms on three related problems on CLT: the SubM, DLIN, and GXDH. Since there is no known relation between the hardness of these problems and GDDH, it is worth analyzing these problems. The computational complexity is not less than that of computing the secret primes p_i. However, our approach to solving the SubM, DLIN and GXDH differs from analysis of GDDH on the CLT scheme, therefore it needs to be considered when a new multilinear map candidate is proposed. We expect it to catalyze further research of cryptanalysis and cryptographic constructions.

Impact of the Attack. The CLT candidate construction should be considered broken, unless the low-level encodings of 0 are not made public. At the moment, there does not exist any candidate multilinear map approximation for which any of SubM, DLIN and GXDH is hard. Several recent cryptographic constructions can no longer be realized. This includes all constructions from [2, 23, 24, 37], the one-round group password authenticated key exchange construction of [1] for more than 3 users, one of the two constructions of password hashing of [3], the alternative key-homomorphic pseudo random function construction from [6], and the use of the latter in [33].

Our attack heavily relies on the fact that low-level encodings of 0 are made publicly available. It is not applicable when these parameters are kept secret. They are used in applications to homomorphically re-randomize encodings so that their distributions are "canonicalize". A simple way to thwart the attack is not to make any low-level encodings of 0 public. This approach was used in [22] and [9], for example. It appears that this approach can be used to secure the construction from [38] as well.

Related and Follow-up Works. The zeroizing attack on the GGH scheme also leads to break of the GGH scheme [31]. Soon after, a third candidate construction of a variant of graded encoding schemes was proposed in [26]. Unfortunately, the scheme is also known to be insecure [19].

Our attack was extended in [8, 14, 27] to settings in which no low-level encoding of 0 are available. The extensions rely on low-level encodings of elements corresponding to orthogonal vectors and impact [22, 28, 29].

After our attack was published in Eurocrypt'15, the draft [23] was update to propose a candidate immunization against our attack (see [23, Se. 6]).[2] Another candidate immunization was proposed in [8]. Both immunizations have proved insecure in [16]. See also [14].

A further modification of CLT was proposed by Coron, Lepoint and Tibouchi in the proceedings of CRYPTO'15 [18]. They claimed that our attack is thwarted since the modified scheme keeps the modulus secret so that the zero-testing procedure depends on the CRT components in a non-linear way. However, it turned out to be insecure as proved by Cheon *et al.* in [11] who exploit an extension of eigenvalues and determinant techniques as in section 3 and 4.

In case of the obfuscation on CLT multilinear map, the security remained open problems because the applications is not given an encodings of zero. Recently, Coron *et al.* provide a new result [20] about it, which enables one to break the obfuscation on CLT multilinear map in polynomial-time.

Notation. We use $a \leftarrow A$ to denote the operation of uniformly choosing an element a from a finite set A. We define $[n] = \{1, 2, \ldots, n\}$. We let $\mathbb{Z}_q$ denote the ring $\mathbb{Z}/(q\mathbb{Z})$. For pairwise coprime integers $p_1, p_2, \ldots, p_n$, we define $\mathsf{CRT}_{(p_1,p_2,\ldots,p_n)}(r_1, r_2, \ldots, r_n)$ (abbreviated as $\mathsf{CRT}_{(p_i)}(r_i)$) as the unique integer in $\left(-\frac{1}{2}\prod_{i=1}^n p_i, \frac{1}{2}\prod_{i=1}^n p_i\right]$ which is congruent to $r_i \bmod p_i$ for all $i \in [n]$. We use the notation $[t]_p$ for integers t and p in order to denote the reduction of t modulo p into the interval $(-p/2, p/2]$.

We use lower-case bold letters to denote vectors whereas upper-case bold letters are employed to denote matrices. For matrix $\mathbf{S}$, we denote the transpose of $\mathbf{S}$ by $\mathbf{S}^T$. We define $\|\mathbf{S}\|_\infty = \max_i \sum_{j\in[n]} |s_{ij}|$, where s_{ij} is the (i, j) component of $\mathbf{S}$. Finally we denote by $\mathsf{diag}(a_1, \ldots, a_n)$ the diagonal matrix with diagonal coefficients equal to $a_1, \ldots, a_n$.

Organization. In Section 2, we define the CRT-ACD problem and its analysis. In Section 3, we recall the CLT multilinear maps and present our attack on this. In Section 4, we introduce three related problems on the CLT multilinear map and their cryptanalysis. We conclude this paper in Section 5.

2 CRT-ACD with auxiliary input

In this section, we introduce a CRT-ACD problem with auxiliary input and analyze the problem. The approximate greatest common divisor problem (ACD) is initially introduced by Howgrave-Graham [30]. It is a problem to find a secret prime p given many near-multiples of p. One of the promising applications of this problem is a homomorphic encryption scheme [36]. The scheme has superiority in regard to conceptual simplicity compared to other homomorphic encryption schemes based on lattice problems.

The ACD problem is naturally extended by using multiple primes rather than a single one. An instance of the problem is an integer of the form $p_i q_i + r_i$ for each prime p_i. Therefore, it can be defined by using Chinese Remainder Theorem (CRT). Now we give a precise definition of an extended ACD problem, which is called CRT-ACD problem.

Definition 1. ***(*CRT-ACD*)*** *Let $n, \eta, \varepsilon \in \mathbb{N}$, and χ_ε be a distribution over $\mathbb{Z} \cap (-2^\varepsilon, 2^\varepsilon)$. For given η bit primes $p_1, \cdots, p_n$, the sampleable* CRT-ACD *distribution $\mathcal{D}_{\chi_\varepsilon,\eta,n}(p_1, \cdots, p_n)$ is defined as*

$$\mathcal{D}_{\chi_\varepsilon,\eta,n}(p_1, \cdots, p_n) = \{\mathsf{CRT}_{(p_i)}(r_i) \mid r_i \leftarrow \chi_\varepsilon\}.$$

[2] The former version that was impacted by our attack can still be accessed from the IACR eprint server.

The CRT-ACD *problem is: For given many samples from $\mathcal{D}_{\chi_\varepsilon,\eta,n}(p_1,\cdots,p_n)$ and $x_0=\prod_{i=1}^{n} p_i$, find p_i for all i.*

Cheon *et al.* gave a batch homomorphic encryption [10] based on a stronger variant of CRT-ACD problems, where the size of p_1 is larger than other p_i's and they take r_1 from uniform distribution over $\mathbb{Z}_{p_1}$. In that case, it can be reduced to the original ACD problem.

For proper parameters, the CRT-ACD problems are regarded to be hard. In this section, however, we show that when the auxiliary input $\mathsf{CRT}_{(p_i)}(x_0/p_i)$ is given, the CRT-ACD is solved in polynomial-time of n,η,ε. Now we define a variant of CRT-ACD, as CRT-ACD problem with auxiliary input.

Definition 2. ***(*CRT-ACD *with auxiliary input)*** *Let $n,\eta,\varepsilon\in\mathbb{N}$, and χ_ε be a distribution over $\mathbb{Z}\cap(-2^\varepsilon,2^\varepsilon)$. For given η bit primes $p_1,\cdots,p_n$, define $x_0=\prod_{i=1}^n p_i$ and $\hat{p}_i=x_0/p_i$, for $1\le i\le n$. The sampleable* CRT-ACD *distribution $\mathcal{D}_{\chi_\varepsilon,\eta,n}(p_1,\cdots,p_n)$ is defined as*

$$\mathcal{D}_{\chi_\varepsilon,\eta,n}(p_1,\cdots,p_n)=\{\mathsf{CRT}_{(p_i)}(r_i)\mid r_i\leftarrow\chi_\varepsilon\}.$$

The CRT-ACD *with auxiliary input is: For given many samples from $\mathcal{D}_{\chi_\varepsilon,\eta,n}(p_1,\cdots,p_n)$, x_0 and $\hat{P}=\mathsf{CRT}_{(p_i)}(\hat{p}_i)$, to find p_i for all i.*

The auxiliary input $\hat{P}$ has a special feature which can be written as a summation of its CRT components in $\mathbb{Z}_{x_0}$. A key observation is that the equation holds over the integers when $\log n+1<\eta$. Using this property, we obtain a following lemma.

Lemma 1. *For a given $\hat{P}=\mathsf{CRT}_{(p_i)}(\hat{p}_i)$ and $a=\mathsf{CRT}_{(p_i)}(r_i)\leftarrow\mathcal{D}_{\chi_\varepsilon,\eta,n}(p_1,\cdots,p_n)$, it satisfies:*

$$a\cdot\hat{P} \bmod x_0=\mathsf{CRT}_{(p_i)}(r_i\cdot\hat{p}_i)=\sum_{i=1}^{n} r_i\cdot\hat{p}_i$$

if $\varepsilon+\log n+1<\eta$.

Proof. The first equality is correct by the definition of Chinese remainder theorem. To show that the second equality is correct, we consider the equation modulo p_i for each i. Then the left hand side is $r_i\cdot\hat{p}_i$ and the right hand side is also $r_i\cdot\hat{p}_i$, because $\hat{p}_j=0 \bmod p_i$, for $j\neq i$. Finally, the size of $\sum_{i=1}^{n} r_i\cdot\hat{p}_i$ is smaller than $n\cdot 2^\varepsilon\cdot 2^{(n-1)\cdot\eta}$ which is less than $x_0/2$. Hence, by the uniqueness of CRT, the second equality holds. □

This lemma transforms the modulus equation to an integer equation of $r_1,\cdots,r_n$ with unknown coefficients $\hat{p}_1,\cdots,\hat{p}_n$. Our goal is to recover r_i by using the integral equation.

Now we describe full details of solving the CRT-ACD with auxiliary input.

2.1 Constructing Matrix Equations over $\mathbb{Z}$

Now we show how to compute $p_1,\cdots,p_n$ when given polynomially many samples of the CRT-ACD from $\mathcal{D}_{\chi_\varepsilon,\eta,n}(p_1,\cdots,p_n)$ with $\varepsilon+\log n+1<\eta$ and the auxiliary input $\hat{P}=\mathsf{CRT}_{(p_i)}(\hat{p}_i)$. For given two instances of CRT-ACD $a=\mathsf{CRT}_{(p_i)}(a_i)$ and $b=\mathsf{CRT}_{(p_i)}(b_i)$, $ab\hat{P} \bmod x_0=$

$\sum a_i b_i \hat{p}_i \bmod x_0$. If all of a_i's and b_i's are small enough, the right hand side equals to $\sum a_i b_i \hat{p}_i$, and so it can be written as the following matrix equation over the integers:

$$ab\hat{P} \bmod x_0 = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \end{pmatrix} \begin{pmatrix} \hat{p}_1 & 0 & \cdots & 0 \\ 0 & \hat{p}_2 & \cdots & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & \cdots & \hat{p}_n \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

The matrix representations share the diagonal matrix $\mathsf{diag}(\hat{p}_1, \cdots, \hat{p}_n)$ for any $\mathsf{CRT\text{-}ACD}$ instances a and b. Hence, we can construct an $(n \times n)$-matrix which is a multiple of $\mathsf{diag}(\hat{p}_1, \cdots, \hat{p}_n)$ by arranging $ab\hat{P} \bmod x_0$ for various a and b.

More precisely, we are given $2n+1$ number of samples from the distribution $\mathcal{D}_{\chi_\varepsilon, \eta, n}$ as following:

$$a_i = \mathsf{CRT}_{(p_k)}(a_{k,i}), b = \mathsf{CRT}_{(p_k)}(b_k), c_j = \mathsf{CRT}_{(p_k)}(c_{k,j}) \text{ for } 1 \le i, j \le n.$$

To adapt Lemma 1 to $a_i b c_j \bmod x_0$, we assume that the parameters of the problem satisfy the condition: $3\varepsilon + \log n + 1 < \eta$. Then compute the following values by multiplying the samples:

$$w_{i,j} = a_i \cdot b \cdot c_j \cdot \hat{P} \bmod x_0 = \sum_{k=1}^{n} a_{k,i} \cdot b_k \hat{p}_k \cdot c_{k,j} \text{ for } 1 \le i, j \le n,$$

$$w'_{i,j} = a_i \cdot c_j \cdot \hat{P} \bmod x_0 = \sum_{k=1}^{n} a_{k,i} \cdot \hat{p}_k \cdot c_{k.j} \text{ for } 1 \le i, j \le n.$$

They can be written as the the following matrix form:

$$w_{i,j} = \sum_{i=1}^{n} a_i \cdot \hat{p}_i b_i \cdot c_i = \begin{pmatrix} a_{1,i} & a_{2,i} & \cdots & a_{n,i} \end{pmatrix} \begin{pmatrix} b_1\hat{p}_1 & 0 & \cdots & 0 \\ 0 & b_2\hat{p}_2 & \cdots & 0 \\ 0 & 0 & \vdots & 0 \\ 0 & 0 & \cdots & b_n\hat{p}_n \end{pmatrix} \begin{pmatrix} c_{1,j} \\ c_{2,j} \\ \vdots \\ c_{n,j} \end{pmatrix}$$

$$w'_{i,j} = \sum_{i=1}^{n} a_i \cdot \hat{p}_i \cdot c_i = \begin{pmatrix} a_{1,i} & a_{2,i} & \cdots & a_{n,i} \end{pmatrix} \begin{pmatrix} \hat{p}_1 & 0 & \cdots & 0 \\ 0 & \hat{p}_2 & \cdots & 0 \\ 0 & 0 & \vdots & 0 \\ 0 & 0 & \cdots & \hat{p}_n \end{pmatrix} \begin{pmatrix} c_{1,j} \\ c_{2,j} \\ \vdots \\ c_{n,j} \end{pmatrix}$$

By collecting these values, we can construct two matrices $\mathbf{W} = (w_{i,j})$ and $\mathbf{W'} = (w'_{i,j}) \in M_{n \times n}(\mathbb{Z})$, which can be written as

$$\mathbf{W} = \mathbf{A}^T \cdot \mathsf{diag}(b_1\hat{p_1}, \cdots, b_n\hat{p_n}) \cdot \mathbf{C},$$

$$\mathbf{W'} = \mathbf{A}^T \cdot \mathsf{diag}(\hat{p_1}, \cdots, \hat{p_n}) \cdot \mathbf{C}$$

for $\mathbf{A}^T = (a_{k,i})$ and $\mathbf{C} = (c_{k,j}) \in M_{n \times n}(\mathbb{Z})$.

2.2 Disclosing all the Secret Quantities

Suppose $\mathbf{A}$ and $\mathbf{C}$ are invertible matrices over $\mathbb{Q}$. We compute $(\mathbf{W}')^{-1}$ over $\mathbb{Q}$ and the following matrix:

$$\mathbf{V} = \mathbf{W} \cdot (\mathbf{W}')^{-1} = \mathbf{A}^T \cdot \mathsf{diag}(b_1, \cdots, b_n) \cdot (\mathbf{A}^T)^{-1}.$$

Here the eigenvalues of the matrix $\mathbf{V}$ are exactly the set $B = \{b_1, \cdots, b_n\}$.

The set B can be computed in polynomial-time of η, n, and ε from $\mathbf{V}$ (e.g., by factoring the characteristic polynomial over $\mathbb{Z}$). The prime p_i is a common factor of both $(b - b_i)$ and x_0, and they have other common factor if and only if $b_j = b_i$ for some $j \in \{1, \cdots, n\}$. Hence if b_i's are distinct , we can get all secret integers $p_1, \cdots, p_n$.

$$\{\mathsf{GCD}(b - \beta, x_0) \mid \beta \in B\} = \{p_i \mid 1 \le i \le n\}.$$

Remark. The probability prob_1 that matrix $\mathbf{A}$ and $\mathbf{C}$ are invertible matrices depends on the distribution χ_ε. The probability prob_2 that $b_i \ne b_j$ for all $1 \le i < j \le n$ also depends on the distribution χ_ε. Our attack succeeds with probability of $\mathsf{prob}_1 \cdot \mathsf{prob}_2$. For example, this probability is overwhelming with respect to ε when χ_ε is uniform distribution over $(-2^\varepsilon, 2^\varepsilon)$. Since our attack consists of a matrix multiplication, computing a characteristic polynomial and finding roots of the polynomial, the overall cost is bounded by $\widetilde{\mathcal{O}}(n^{2+\omega} \cdot \eta)$, with $\omega \le 2.38$. Hence, we obtain the following result:

Theorem 1. *Let U_ε be the uniform distribution over $(-2^\varepsilon, 2^\varepsilon) \cap \mathbb{Z}$. When $\varepsilon + \log n + 1 < \eta$ and given $O(n)$ $\mathsf{CRT\text{-}ACD}$ samples from $\mathcal{D}_{U_\varepsilon,\eta,n}(p_1, \cdots, p_n)$ with $x_0 = \prod_{i=1}^{n} p_i$, and $\hat{P} = \mathsf{CRT}_{(p_i)}(\hat{p}_i)$, one can recover every secret primes $p_1, \cdots, p_n$ in time $\widetilde{\mathcal{O}}(n^{2+\omega} \cdot \eta)$ with $\omega \le 2.38$ and overwhelming probability to ε.*

3 Application to CLT multilinear maps

3.1 A Candidate Multilinear Map over the Integers

First, we briefly recall the Coron *et al.* construction. We refer to the original paper [15] for a complete description. The scheme relies on the following parameters.

λ: the security parameter

κ: the multilinearity parameter

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 p_i

n: the number of distinct secret primes

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.* suggests to set the parameters so that the following conditions are met:

- $\rho = \Omega(\lambda)$: to avoid brute force attack (see also [32] for a constant factor improvement).
- $\alpha = \lambda$: so that the ring of messages $\mathbb{Z}_{g_1} \times \ldots \times \mathbb{Z}_{g_n}$ does not contain a small subring $\mathbb{Z}_{g_i}$.[3]
- $n = \Omega(\eta \cdot \lambda)$: to thwart lattice reduction attacks.
- $\ell \geq n \cdot \alpha + 2\lambda$: to be able to apply the leftover hash lemma from [15, Le. 1].
- $\tau \geq n \cdot (\rho + \log_2(2n)) + 2\lambda$: to apply leftover hash lemma from [15, Se. 4].
- $\beta = \Omega(\lambda)$: to avoid the so-called gcd attack.
- $\eta \geq \rho_\kappa + \alpha + 2\beta + \lambda + 8$, where ρ_κ is the maximum bit size of the random r_i's a level-κ encoding. When computing the product of κ level-1 encodings and an additional level-0 encoding, one obtains $\rho_\kappa = \kappa \cdot (2\alpha + 2\rho + \lambda + 2\log_2 n + 2) + \rho + \log_2 \ell + 1$.
- $\nu = \eta - \beta - \rho_f - \lambda - 3$: to ensure zero-test correctness.

Instance generation: $(\mathsf{params}, \mathbf{p_{zt}}) \leftarrow \mathsf{InstGen}(\mathbf{1}^\lambda, \mathbf{1}^\kappa)$. Set the scheme parameters as explained above. For $i \in [n]$, generate η-bit primes p_i, α-bit primes g_i, and compute $x_0 = \prod_{i \in [n]} p_i$. Sample $z \leftarrow \mathbb{Z}_{x_0}$. Let $\Pi = (\pi_{ij}) \in \mathbb{Z}^{n \times n}$ with $\pi_{ij} \leftarrow (n2^\rho, (n+1)2^\rho) \cap \mathbb{Z}$ if $i = j$, otherwise $\pi_{ij} \leftarrow (-2^\rho, 2^\rho) \cap \mathbb{Z}$. For $i \in [n]$, generate $\mathbf{r_i} \in \mathbb{Z}^\mathbf{n}$ by choosing randomly and independently in the half-open parallelepiped spanned by the columns of the matrix Π and denote by r_{ij} the j-th component of $\mathbf{r_i}$. Generate $\mathbf{H} = (h_{ij}) \in \mathbb{Z}^{n \times n}, \mathbf{A} = (a_{ij}) \in \mathbb{Z}^{n \times \ell}$ such that $\mathbf{H}$ is invertible and $\|\mathbf{H}^T\|_\infty \leq 2^\beta$, $\|(\mathbf{H}^{-1})^T\|_\infty \leq 2^\beta$ for $i \in [n]$, $j \in [\ell]$, $a_{ij} \leftarrow [0, g_i)$. Then define:

$$\begin{aligned}
y &= \mathsf{CRT}_{(p_i)}\left(\frac{r_i g_i + 1}{z}\right), \text{ where } r_i \leftarrow (-2^\rho, 2^\rho) \cap \mathbb{Z} \text{ for } i \in [n], \\
x_j &= \mathsf{CRT}_{(p_i)}\left(\frac{r_{ij} g_i}{z}\right) \text{ for } j \in [\tau], \\
\Pi_j &= \mathsf{CRT}_{(p_i)}\left(\frac{\pi_{ij} g_i}{z}\right) \text{ for } j \in [n], \\
x'_j &= \mathsf{CRT}_{(p_i)}(x'_{ij}), \text{ where } x'_{ij} = r'_{ij} g_i + a_{ij} \text{ and } r'_{ij} \leftarrow (-2^\rho, 2^\rho) \cap \mathbb{Z} \text{ for } i \in [n], j \in [\ell], \\
(\mathbf{p}_{zt})_j &= \left[\sum_{i=1}^n \left[h_{ij} \cdot z^\kappa \cdot g_i^{-1}\right]_{p_i} \cdot \prod_{i' \neq i} p_{i'}\right]_{x_0} \text{ for } j \in [n].
\end{aligned}$$

Output $\mathsf{params} = (n, \eta, \alpha, \rho, \beta, \tau, \ell, \nu, y, \{x_j\}, \{x'_j\}, \{\Pi_j\}, s)$ and $\mathbf{p}_{zt}$. Here s is a seed for a strong randomness extractor, which is used for an "Extraction" procedure. We do not recall the latter as it is not necessary to describe our attack.

Re-randomizing level-1 encodings: $c' \leftarrow \mathsf{reRand}(\mathsf{params}, c)$. For $j \in [\tau], i \in [n]$, sample $b_j \leftarrow \{0, 1\}$, $b'_i \leftarrow [0, 2^\mu) \cap \mathbb{Z}$, with $\mu = \rho + \alpha + \lambda$. Return $c' = [c + \sum_{j \in [\tau]} b_j \cdot x_j + \sum_{i \in [n]} b'_i \cdot \Pi_i]_{x_0}$. Note that this is the only procedure in the CLT multilinear map that uses the x_j's.[4]

[3] In fact, it seems that making the primes g_i public may not lead to any specific attack [17].

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

Adding and multiplying encodings: $\mathsf{Add}(c_1, c_2){=}[c_1 + c_2]_{x_0}$ and $\mathsf{Mul}(c_1, c_2){=}[c_1 \cdot c_2]_{x_0}$.

Zero-testing: $\mathsf{isZero}(\mathsf{params}, \mathbf{p}_{zt}, u_\kappa) \stackrel{?}{=} 0/1$. Given a level-$\kappa$ encoding c, return 1 if $\|[\mathbf{p}_{zt} \cdot c]_{x_0}\|_\infty < x_0 \cdot 2^{-\nu}$, and return 0 otherwise.

Coron *et al.* also describes a variant where only one such $(\mathbf{p}_{zt})_j$ is given out, rather than n of them (see [15, Se. 6]). Our attack requires only one $(\mathbf{p}_{zt})_j$. In [29, App. B.3], Gentry *et al.* describes a variant of the construction above that aims at generalizing asymmetric cryptographic bilinear maps, which we briefly introduce in Section 4. Our attack can be adapted to that variant.

3.2 A zeroizing attack on CLT

In this section, we adapt the analysis of $\mathsf{CRT\text{-}ACD}$ with auxiliary input to CLT multilinear maps. The instances of the problem and the CLT multilinear map are quite similar. The encodings of CLT resemble the instances of the problem except the secret constant z. The zero-testing parameters $(\mathbf{p}_{zt})_j$ also has a similar structure with $\hat{P}$ but contains coefficients with large size about p_i. However, when we restrict zero-testing to encodings of 0, it behaves similar to Lemma 1.

More precisely, let a be a top-level encoding of 0 and write $a = \mathsf{CRT}_{(p_i)}(r_i g_i / z^\kappa)$. Hereafter since we use only one zero-testing parameter, without loss of generality, we denote $(\mathbf{p}_{zt})_1$ as $\mathbf{p}_{zt}$. As similar in Lemma 1,

$$\mathbf{p}_{zt} \cdot a \bmod x_0 = \mathsf{CRT}_{p_i}(\hat{p}_i h_i r_i) = \sum_{i=1}^{n} \hat{p}_i h_i r_i$$

as long as the last quantity is smaller than $x_0/2$. By zero-testing conditions, it is always true for valid top level encodings of zero. Next, by replacing a by valid κ level encodings of zero $x'_j \cdot x'_1 \cdot x_k \cdot y^{k-1}$ or $x'_j \cdot x_k \cdot y^{k-1}$ for $1 \le j,k \le n$ in the above equation, for $1 \le j,k \le n$, we have:

$$\begin{aligned} w_{jk} &= x'_j \cdot x'_1 \cdot x_k \cdot y^{\kappa-1} \cdot \mathbf{p}_{zt} \bmod x_0 = \sum_{i=1}^{n} \hat{p}_i \cdot h_i \cdot x'_{ij} \cdot (r_i g_i + 1)^{\kappa-1} \cdot x'_{i1} \cdot r_{ik} \\ &= \sum_{i=1}^{n} x'_{ij} \cdot x'_{i1} \cdot h'_i \cdot r_{ik}, \text{ and} \\ w'_{jk} &= x'_j \cdot x_k \cdot y^{\kappa-1} \cdot \mathbf{p}_{zt} \bmod x_0 = \sum_{i=1}^{n} \hat{p}_i \cdot h_i \cdot x'_{ij} \cdot (r_i g_i + 1)^{\kappa-1} \cdot r_{ik} \\ &= \sum_{i=1}^{n} x'_{ij} \cdot h'_i \cdot r_{ik}, \end{aligned}$$

where $h'_i = \hat{p}_i \cdot h_i \cdot (r_i g_i + 1)^{\kappa-1}$. By spanning $1 \le i,j \le n$, we obtain the matrix $\mathbf{W}$ and $\mathbf{W}'$:

$$\mathbf{W} = \mathbf{X}'^T \cdot \mathsf{diag}(x'_{11} \cdot h'_1, \cdots, x'_{n1} \cdot h'_n) \cdot \mathbf{R},$$

$$\mathbf{W}' = \mathbf{X}'^T \cdot \mathsf{diag}(h'_1, \cdots, h'_n) \cdot \mathbf{R},$$

for $\mathbf{X}'^T = (x'_{ij})$ and $R = (r_{ik})$. By applying the same method in the section 2, we can recover $\{x_{11}, \cdots, x_{n1}\}$ by computing the eigenvalues of $\mathbf{W} \cdot \mathbf{W}'^{-1}$. Hence we can compute all secret p_i by computing $\mathsf{GCD}(x'_1 - x_{i1}, x_0)$.

Consequently, we need $\mathbf{W}'$ and $\mathbf{W}$ to be invertible. We argue that this is the case here. We prove it for $\mathbf{W}$. Note first that the x'_{i1}'s and the h'_i's are all non-zero, with overwhelming probability. Note that by design, the matrix $(r_{ij})_{i\in[n],j\in[\tau]}$ has rank n (see [15, Section. 4]). The same holds for the matrix $(x'_{ij})_{i\in[n],j\in[\ell]}$ (see [15, Lemma. 1]). As we can compute the rank of a $\mathbf{W} \in \mathbb{Z}^{t\times t}$ obtained by using an $\mathbf{X}' \in \mathbb{Z}^{t\times n}$ and an $\mathbf{R} \in \mathbb{Z}^{n\times t}$ obtained by respectively using a t-subset of the x'_j's and a t-subset of the x_j's. Without loss of generality we may assume that our $\mathbf{X}', \mathbf{R} \in \mathbb{Z}^{\mathbf{n}\times\mathbf{n}}$ are non-singular. The cost of finding such a pair $(\mathbf{X}', \mathbf{R})$ is bounded as $\widetilde{\mathcal{O}}((\tau+\ell)\cdot(n^\omega \log x_0)) = \widetilde{\mathcal{O}}(\kappa^{\omega+3}\lambda^{2\omega+6})$, with $\omega \le 2.38$ (assuming all parameters are set smallest possible so that the bounds of Subsection 3.1 hold). Here we used the fact that the rank of a matrix $\mathbf{A} \in \mathbb{Z}^{n\times n}$ may be computed in time $\widetilde{\mathcal{O}}(n^\omega \log \|\mathbf{A}\|_\infty)$ (see [35]). This dominates the overall cost of the attack.

After we know all the p_i's, we have $x_j/y = r_{ij}g_i/(r_ig_i+1) \bmod p_i$. As the numerator and denominator are coprime and very small compared to p_i, they can be recovered by the rational reconstruction algorithm. We hence obtain $(r_{ij}g_i)$'s for all j. The gcd of all the $(r_{ij}g_i)$'s reveals g_i. As a result, we can also recover all the r_{ij}'s and r_i's. As $x_1 = r_{i1}g_i/z \bmod p_i$ and the numerator is known, we can recover $z \bmod p_i$ for all i, and hence $z \bmod x_0$. The h_{ij}'s can then be recovered as well, so can the r'_{ij}'s and a_{ij}'s.

4 The Subgroup Membership, Decision Linear and Graded External Diffie-Hellman Problems

We start by defining the SubM, DLIN and GXDH problems associated with the CLT multilinear map. We then describe how to solve these problems in polynomial-time. The attack procedure consists of two steps. First, in Section 4.1, we show how to recover $\prod_i g_i$. It is a common procedure for solving the SubM and DLIN. Next, in Sections 4.2 and 4.3, we use that quantity to recognize valid instances of the SubM and DLIN. In Section 4.4, we introduce a method to solve the GXDH.

Let $G = \mathbb{Z}_{g_1} \times \ldots \times \mathbb{Z}_{g_n}$ and G_i be the subgroup of order g_i obtained by making the components of the other $\mathbb{Z}_{g_j}$'s to be zero. For index set $I \subseteq [n]$, we denote $G_I = \prod_{i\in I} G_i$. We let $\mathsf{enc}_1(m)$ denote a properly generated level-1 encoding of $m \in G$. For integers $L, N > 0$, we let $\mathsf{Rk}_i(\mathbb{Z}_N^{L\times L})$ denote the set of $L \times L$ matrices over $\mathbb{Z}_N$ of rank i. If N is a product of primes, we define the rank of a matrix as the maximum of the ranks of the matrices obtained by reduction modulo all the prime divisors of N.

Definition 3. ***(The Subgroup Membership Problem)*** *SubM is as follows. Given λ and κ, generate* params *and* $\mathbf{p_{zt}}$ *using* InstGen *and* $\{\mathsf{enc}_1(g_i) : i \in [\ell]\}$ *where the g_i's are uniformly and independently sampled in a strict subgroup G_I of G, with ℓ sufficiently large so that the g_i's generate G_I with overwhelming probability. Given* params, $\mathbf{p}_{zt}$, $\{\mathsf{enc}_1(g_i) : i \in [\ell]\}$ *and* $u = \mathsf{enc}_1(m)$, *determine whether m is sampled uniformly in G_I or in G.*

Definition 4. ***(L-Decisional Linear Problem)*** *L-DLIN is as follows. Given λ and κ, generate* params *and* $\mathbf{p}_{zt}$ *using* InstGen. *Define $N = \prod_i g_i$. Given* params *and* $\mathbf{p}_{zt}$, *the goal is to distinguish between the distributions*

$$\{(\mathsf{enc}_1(m^{(i,j)}))_{i,j}\}_{(m^{(i,j)})_{i,j}\leftarrow\mathsf{Rk}_{L-1}(\mathbb{Z}_N^{L\times L})} \quad \text{and} \quad \{(\mathsf{enc}_1(\tilde{m}^{(i,j)}))_{i,j}\}_{(\tilde{m}^{(i,j)})_{i,j}\leftarrow\mathsf{Rk}_{L}(\mathbb{Z}_N^{L\times L})}.$$

In one of the constructions of [1], the authors rely on the following particular case. The problem is as follows. The algorithm is given params and $\mathbf{p}_{zt}$ as well as $\{\mathsf{enc}_1(a_i)\}_{i\in[L]}$ and $\{\mathsf{enc}_1(a_i b_i)\}_{i\in[L]}$ for some uniform and independent $a_1,\ldots,a_L,b_1,\ldots,b_L \in G$. It is also given $\mathsf{enc}_1(m)$, and it has to assess whether m is uniformly and independently sampled in G or whether $m = b_1+\ldots+b_L$. This can be restated as a special case of Definition 4, by noting that it requests to assess whether the matrix just below is full-rank.

$$\begin{pmatrix} a_1b_1 & a_1 & 0 & \ldots & 0 \\ a_2b_2 & 0 & a_2 & \ldots & 0 \\ & \vdots & & & \\ a_Lb_L & 0 & 0 & \ldots & a_L \\ m & 1 & 1 & \ldots & 1 \end{pmatrix}$$

We recall asymmetric multilinear maps and the associated GXDH problem. By applying the attacks described above, we can solve GXDH in polynomial-time.

Instance generation: $(\mathsf{params}, \mathbf{p}_{zt}) \leftarrow \mathsf{InstGen}(1^\lambda, 1^\kappa)$. The setting of the parameters p_i, g_i, $x_0, \{x'_j\}, \Pi$ and H are as in the original scheme. For $1 \le t \le \kappa$, sample z_t uniformly in $\mathbb{Z}_{x_0}$. Then define, for all $1 \le t \le \kappa$:

$$\begin{aligned} y^{(t)} &= \mathsf{CRT}_{(p_i)}\left(\frac{r_i^{(t)}\cdot g_i + 1}{z_t}\right), \text{ where } r_i^{(t)} \leftarrow (-2^\rho, 2^\rho)\cap\mathbb{Z}, \text{ for } 1 \le i \le n, \\ x_j^{(t)} &= \mathsf{CRT}_{(p_i)}\left(\frac{r_{ij}^{(t)}\cdot g_i}{z_t}\right), \text{ for } 1 \le j \le \tau. \end{aligned}$$

Further, we define:

$$(\mathbf{p}_{zt})_j = \sum_{i=1}^{n} h_{ij}\cdot\Big(\prod_{1\le t\le\kappa} z_t\cdot g_i^{-1} \bmod p_i\Big)\cdot\prod_{i'\ne i} p_{i'} \bmod x_0, \text{ for } 1\le j\le n.$$

Output $\mathsf{params} = (n,\eta,\alpha,\rho,\beta,\tau,\ell,\nu,\{y^{(t)}\},\{x_j^{(t)}\},\{x'_j\},\{\Pi_j\},s)$ and $\mathbf{p}_{zt}$. From now on, we let $\mathsf{enc}_t(m)$ denote $\mathsf{CRT}_{(p_i)}(\frac{m_i+s_i\cdot g_i}{z_t})$.

Since, as same as in section 3.2, we only use one zero-testing parameter, we denote $(\mathbf{p}_{zt})_1$ as $\mathbf{p}_{zt}$. We now define the CLT variant of the GXDH problem.

Definition 5. ***(Graded External DDH Problem)*** *GXDH is as follows. Given λ and κ, generate* params *and* $\mathbf{p}_{zt}$ *using* $\mathsf{InstGen}$. *Given* params, $\mathbf{p}_{zt}$ *and* $\mathsf{enc}_t(a), \mathsf{enc}_t(b)$ *and* $\mathsf{enc}_t(c)$ *with $a, b \leftarrow G$ and for a given $t \in [\kappa]$, the goal is to decide whether $c = a\cdot b$ or c is uniformly and independently sampled in G.*

This can be regarded as a variant of 2-DLIN problems by distinguishing the following distributions

$$\left\{\begin{pmatrix} \mathsf{enc}_t(c) & \mathsf{enc}_t(a) \\ \mathsf{enc}_t(b) & \mathsf{enc}_t(1)\end{pmatrix}\right\} \quad\text{and}\quad \left\{\begin{pmatrix} \mathsf{enc}_t(ab) & \mathsf{enc}_t(a) \\ \mathsf{enc}_t(b) & \mathsf{enc}_t(1)\end{pmatrix}\right\}, \text{where } c \leftarrow G.$$

Our main strategy to solve these three related problem of CLT scheme is that: For a given level-1 encoding

$$\mathbf{E} = (e_{i,j}) = \mathsf{CRT}_{(p_k)}\left(\frac{s_k^{(i,j)} g_k + m_k^{(i,j)}}{z}\right) \text{ for } 1 \le i, j \le t,$$

we can construct a matrix $\mathbf{W}_{e_{i,j}} = \mathbf{W}_{i,j}$ as similar to section 3.2 by computing $[x'_k \cdot e_{i,j} \cdot x_l \cdot y^{\kappa-2} \cdot \mathbf{p}_{zt}]_{x_0}$ for $1 \le k, l \le n$:

$$\begin{aligned}\mathbf{W}_{i,j} &= \mathbf{X}' \cdot (\mathbf{S}_{i,j}\mathbf{G} + \mathbf{M}_{i,j}) \cdot \mathsf{diag}(\tilde{h}_1, \cdots, \tilde{h}_n) \cdot \mathbf{R} \\ &= \mathbf{X}' \cdot (\mathbf{S}_{i,j}\mathbf{G} + \mathbf{M}_{i,j}) \cdot \mathbf{R}',\end{aligned}$$

for $\tilde{h}_i = h_i \cdot (r_i g_i + 1)^{\kappa-2} \cdot \hat{p}_i$, $\mathbf{S}_{i,j} = \mathsf{diag}(s_1^{(i,j)}, \cdots, s_n^{(i,j)})$ and $\mathbf{M}_{i,j} = \mathsf{diag}(m_1^{(i,j)}, \cdots, m_n^{(i,j)})$. By collecting these matrix $\mathbf{W} = (\mathbf{W}_{i,j})$ for $1 \le i, j \le t$, we can get following matrix:

$$\mathbf{W} = \mathbf{X}' \cdot \left(\begin{pmatrix} \mathbf{S}_{1,1} \cdot \mathbf{G} & \mathbf{S}_{1,2} \cdot \mathbf{G} & \dots & \mathbf{S}_{1,t} \cdot \mathbf{G} \\ \mathbf{S}_{2,1} \cdot \mathbf{G} & \mathbf{S}_{2,2} \cdot \mathbf{G} & \dots & \mathbf{S}_{2,t} \cdot \mathbf{G} \\ \vdots & & \ddots & \\ \mathbf{S}_{t,1} \cdot \mathbf{G} & \mathbf{S}_{t,2} \cdot \mathbf{G} & \dots & \mathbf{S}_{t,t} \cdot \mathbf{G} \end{pmatrix} + \begin{pmatrix} \mathbf{M}_{1,1} & \mathbf{M}_{1,2} & \dots & \mathbf{M}_{1,t} \\ \mathbf{M}_{2,1} & \mathbf{M}_{2,2} & \dots & \mathbf{M}_{2,t} \\ \vdots & & \ddots & \\ \mathbf{M}_{t,1} & \mathbf{M}_{t,2} & \dots & \mathbf{M}_{t,t} \end{pmatrix} \right) \cdot \mathbf{R}'.$$

Related problems are to distinguish problems for given matrix of encoding $\mathbf{E}$, the size of matrix is different depending on problem. Those related problems can be seen as following:

SubM: For $t = 1$ and a given $\mathbf{E}$, determine $m \leftarrow G_I$ or not.

L-DLIN: For $t = L$ and a given $\mathbf{E}$, determine $(m^{(i,j)})_{i,j} \leftarrow \mathsf{Rk}_{L-1}(\mathbb{Z}_N^{L\times L})$ or $\mathsf{Rk}_L(\mathbb{Z}_N^{L\times L})$.

GXDH: For $t = 2$ and a given $\mathbf{E}$, determine $\begin{pmatrix} c & a \\ b & 1 \end{pmatrix}$ is a full rank or not

In case of SubM, determining $\mathbf{m} = (m_i)_{1\le i\le n}$ is in G_I or not is the same as computing factors of $\mathsf{gcd}(\prod(r_i g_i + m_i), \prod g_i)$. This value can be computed from determinant of $\mathbf{W}$ and $\prod g_i$. In case of GXDH and L-DLIN, the determinant of $\mathbf{W}$ is a multiple of g_i for any i, if the middle term matrix $\mathbf{M}$ does not have a full rank. In other case, the determinant of $\mathbf{M}$ is not a multiple of g_i with a high probability. Hence, if one can recover the $\prod g_i$, one can solve the related problems.

Remark. The important difference between cryptanalysis of these related problems and the cryptanalysis of the CLT scheme is the form of the middle matrix of $\mathbf{W}$. The previous attack in Section 3 is based on the fact that the middle matrix is a diagonal matrix. For example, in [8], the authors fixed the middle matrix into block diagonal matrix form.[5] On the other hand, the attack of related problems in this section does not depend on it.

4.1 Step 1: Computing $\prod_i g_i$

The main step in the attack is to get $\prod_i g_i$ from $(\mathsf{params}, \mathbf{p}_{zt})$. It may be admissible to assume that the g_i's are public in which computing $\prod_i g_i$ is trivial. If for some reason the g_i's have to stay secret, one must set their bit-sizes as $\Omega(\lambda^2)$, so that they cannot be recovered by combining the approach described below with the elliptic curve factorization algorithm.

[5] Soon after, it is also known to be insecure by Coron *et al.*'s extended attack

Similarly, to compute w_{kl} in the Section 3.2, we compute $w_{kl} := \left[x'_k \cdot y \cdot x_l \cdot y^{\kappa-2} \cdot \mathbf{p}_{zt}\right]_{x_0}$, $w_{kl}^{(i)} := \left[x'_k \cdot x_i \cdot x_l \cdot y^{\kappa-2} \cdot \mathbf{p}_{zt}\right]_{x_0}$ and obtain a matrix

$$\begin{aligned} \mathbf{W}_y &= \mathbf{X}' \cdot \mathsf{diag}(r_1 g_1 + 1, \ldots, r_n g_n + 1) \cdot \mathbf{R}'. \\ \mathbf{W}_i &= \mathbf{X}' \cdot \mathsf{diag}(r_{i1} g_1, \ldots, r_{in} g_n) \cdot \mathbf{R}'. \end{aligned}$$

We can get a multiple of $\prod_i g_i$ by taking a ratio of gcd's of determinants of appropriate subsets of $\{\mathbf{W}_1, \ldots, \mathbf{W}_m, \mathbf{W}_y\}$:

$$\begin{aligned} \frac{\gcd(\det \mathbf{W}_1, \ldots, \det \mathbf{W}_m)}{\gcd(\det \mathbf{W}_1, \ldots, \det \mathbf{W}_m, \det \mathbf{W}_y)} &= \frac{\gcd(\prod_i r_{i1}, \ldots, \prod_i r_{im})}{\gcd(\prod_i r_{i1} g_i, \ldots, \prod_i r_{im} g_i, \prod_i (r_i g_i + 1))} \cdot \prod_i g_i \\ &= \Delta \cdot \prod_i g_i, \end{aligned}$$

for some integer Δ. We expect that Δ consists of only small factors because it is a common divisor of many random variables. These variables do not satisfy uniformity condition, because r_{ij} is chosen in a half-open parallelepiped spanned by matrix Π. However the elements of matrix Π are drawn from some interval that is independent of an arbitrary prime p. Therefore, we may (heuristically) assume that the smoothness probabilities are the same as that of the uniform case. Under this assumption, the integer Δ is $2n$-smooth (i.e., all its divisors are $\leq 2n$) with probability ≥ 0.9, as we explain below. The more general results can be found in [13].

Lemma 2 (Heuristic)**.** *Let r_{ij} be a random integer for $i \in [n], j \in [m]$ with $m \geq s \log(2n)$ for some positive integer s. Then $\gcd(\prod_i r_{i1}, \ldots, \prod_i r_{im})$ is $2n$-smooth with probability $\geq \zeta(s)^{-1}$, which is ≥ 0.9 when $s \geq 4$.*

Proof. Our heuristic assumption is that each r_{ij} is divisible by a prime $p > 2n$ with probability $\leq 1/p$, for all p's. First, we observe that for each j, the integer $\prod_i r_{ij}$ is divisible by p with probability $\leq 1 - (1 - 1/p)^n \leq n/p$. Then the probability that $\gcd(\prod_i r_{i1}, \ldots, \prod_i r_{im})$ is divisible by p is $\leq (n/p)^m$. As a result, the gcd is $2n$-smooth with probability at least

$$\prod_{p>2n} (1 - (n/p)^m) \geq \prod_{p>2n} (1 - 1/p^s) = \zeta(s)^{-1} \prod_{p \leq 2n} (1 - 1/p^s)^{-1} \geq \zeta(s)^{-1}.$$

Here the first inequality comes from $(n/p)^m \leq (n/2n)^m = (1/2)^m \leq 1/p^s$ for $m \geq s \log p$. The equality is Euler's identity for the Riemann zeta function. The latter is decreasing and $\zeta(4)^{-1} > 0.9$. This completes the proof. □

By Lemma 2, the integer Δ is $(2n)$-smooth with probability > 0.9. We eliminate it by trial division by all integers $\leq 2n$. This costs $\widetilde{\mathcal{O}}(\kappa^2 \lambda^5)$ bit operations. This is dominated by the cost of the operations described in Sections 3.2, which is $\widetilde{\mathcal{O}}(\kappa^{\omega+3} \lambda^{2\omega+6})$.

4.2 Solving the CLT SubM Problem

We compute $w_{kl} = \left[x'_k \cdot \mathsf{enc}_1(m) \cdot x_l \cdot y^{\kappa-2} \cdot \mathbf{p}_{zt}\right]_{x_0}$:

$$\mathbf{W} = \mathbf{X}' \cdot \mathsf{diag}(r_1 g_1 + x_1, \ldots, r_n g_n + x_n) \cdot \mathbf{R}',$$

with $x_i \in \mathbb{Z}_{g_i}$ for all i. The attack consists in computing $\gcd(\det \mathbf{W}, \prod_i g_i)$.

If m is uniformly sampled in G, then we expect $n/2^\alpha$ of the x_i's to be zero. Hence, in that case, we have $\log\gcd(\det \mathbf{W}, \prod_i g_i) \approx \alpha n/2^\alpha$. For the original setting of $\alpha = \lambda$, this is essentially 0.

If m is uniformly sampled in G_I, then all the x_i's for $i \notin I$ are zero, and we expect $(n-|I|)/2^\alpha$ of the others to be zero. Hence, in that case, we have $\log\gcd(\det \mathbf{W}, \prod_i g_i) \approx \alpha|I| + \alpha(n-|I|)/2^\alpha$.

4.3 Solving the CLT DLIN Problem

As we have seen, we assume that $\prod_i g_i$ is known. In DLIN, we are given a matrix of level-1 encodings $\mathbf{E} = (e_{i,j})_{i,j}$. We write $e_{i,j} = (s_k^{(i,j)} g_k + m_k^{(i,j)})/z \bmod p_k$. Using the same method to above, we compute matrices $\mathbf{W}_{i,j} \in \mathbb{Z}^{n\times n}$ for all $e_{i,j}$. We define

$$\mathbf{W} = \begin{pmatrix} \mathbf{W}_{11} & \mathbf{W}_{12} & \dots & \mathbf{W}_{1L} \\ \mathbf{W}_{21} & \mathbf{W}_{22} & \dots & \mathbf{W}_{2L} \\ \vdots & & \ddots & \\ \mathbf{W}_{L1} & \mathbf{W}_{L2} & \dots & \mathbf{W}_{LL} \end{pmatrix} \in \mathbb{Z}^{nL\times nL}.$$

We compute the determinant of $\mathbf{W}$. It satisfies the following equation.

$$\det(\mathbf{W}) = \det(\mathbf{X}')^L \cdot \det(\mathbf{R}')^L \cdot \det \begin{pmatrix} \mathbf{B}_{1,1} & \mathbf{B}_{1,2} & \dots & \mathbf{B}_{1,L} \\ \mathbf{B}_{2,1} & \mathbf{B}_{2,2} & \dots & \mathbf{B}_{2,L} \\ \vdots & & \ddots & \\ \mathbf{B}_{L,1} & \mathbf{B}_{L,2} & \dots & \mathbf{B}_{L,L} \end{pmatrix},$$

where $\mathbf{B}_{i,j} = \mathsf{diag}(s_1^{(i,j)} \cdot g_1 + m_1^{(i,j)}, \cdots, s_n^{(i,j)} \cdot g_n + m_n^{(i,j)})$ for all i,j. Let $\Delta = \det(\mathbf{X}')^L \cdot \det(\mathbf{R}')^L$. We have $\det \mathbf{W} = \Delta \cdot \prod_k \det \mathbf{Q}_k$, where $\mathbf{Q}_k = (r_k^{(i,j)} \cdot g_k + m_k^{(i,j)})_{i,j}$ and it is congruent to $\mathbf{P}_k = (m_k^{(i,j)})_{(i,j)}$ in modulo g_k.

To distinguish among the instances of DLIN, we compute $\det \mathbf{W}$ and check whether it is divisible by $\prod_k g_k$. If $\mathbf{E}$ is sampled from a full rank matrix, the determinant of $\mathbf{P}_k$ is nonzero for some k. Hence $\det \mathbf{W}$ cannot be multiple of $\prod_k g_k$. In other case, then $\det \mathbf{P}_i = 0$ for all i. Hence $\det \mathbf{W}$ is a multiple of $\prod_k g_k$. The total bit-complexity of the attack is $\widetilde{\mathcal{O}}(\kappa^{\omega+3}\lambda^{2\omega+6} + \kappa^{\omega+3}L^{\omega+1}\lambda^{2\omega+5})$.

4.4 Solving the CLT GXDH Problem

In the following, we assume that $\kappa \geq 3$. Without loss of generality, we assume that $t = 1$ in the GXDH problem. The first step in the attack is to get $\prod_i g_i$ from $(\mathsf{params}, \mathbf{p}_{zt})$. Similar to Section 4.1, we compute $\mathbf{W}_{y^{(1)}}$ and the $\mathbf{W}_i$'s by using (params), as follows (for $1 \leq i \leq m$):

$$\begin{aligned} \mathbf{W}_{y^{(1)}} &= ([y^{(1)} \cdot x_k^{(2)} x_l^{(3)} \cdot y^{(4)} \dots y^{(\kappa)} \cdot \mathbf{p}_{zt}]_{x_0})_{k,l} \\ &= \mathbf{R} \cdot \mathsf{diag}(r_1^{(1)} g_1 + 1, \dots, r_n^{(1)} g_n + 1) \cdot \mathsf{diag}(h'_1, \dots, h'_n) \cdot \mathbf{R}', \\ \mathbf{W}_i &= ([x_i^{(1)} \cdot x_k^{(2)} x_l^{(3)} \cdot y^{(4)} \dots y^{(\kappa)} \cdot \mathbf{p}_{zt}]_{x_0})_{k,l} \\ &= \mathbf{R} \cdot \mathsf{diag}(r_{i1}^{(1)} g_1, \dots, r_{in}^{(1)} g_n) \cdot \mathsf{diag}(h'_1, \dots, h'_n) \cdot \mathbf{R}', \end{aligned}$$

where $\mathbf{R} = (r_{ki}^{(2)})$ and $\mathbf{R}' = (r_{il}^{(3)})$.

Similar to Section 4.1, we obtain a multiple of $\prod_i g_i$ by taking a ratio of gcd's of determinants of appropriate subsets of $\{\mathbf{W}_1, \ldots, \mathbf{W}_m, \mathbf{W}_{y^{(1)}}\}$:

$$\frac{\gcd(\det \mathbf{W}_1, \ldots, \det \mathbf{W}_m)}{\gcd(\det \mathbf{W}_1, \ldots, \det \mathbf{W}_m, \det \mathbf{W}_{y^{(1)}})} = \Delta \cdot \prod_i g_i,$$

for some integer Δ. For the same reason as before, by Lemma 2, the integer Δ is $(2n)$-smooth with probability > 0.9. We eliminate it by trial division by all integers $\leq 2n$. Thus, we can get $\prod_i g_i$ in time $\widetilde{\mathcal{O}}(\kappa^{\omega+3}\lambda^{2\omega+6})$.

Next, we instantiate with $y^{(1)} = \mathsf{enc}_1(a), \mathsf{enc}_1(b), \mathsf{enc}_1(c)$, respectively. We get:

$$\begin{aligned}
\mathbf{W}_a &= \mathbf{R} \cdot \mathsf{diag}(r_{a1}^{(1)} g_1 + a_1, \ldots, r_{an}^{(1)} g_n + a_n) \cdot \mathsf{diag}(h'_1, \ldots, h'_n) \cdot \mathbf{R}', \\
\mathbf{W}_b &= \mathbf{R} \cdot \mathsf{diag}(r_{b1}^{(1)} g_1 + b_1, \ldots, r_{bn}^{(1)} g_n + b_n) \cdot \mathsf{diag}(h'_1, \ldots, h'_n) \cdot \mathbf{R}', \\
\mathbf{W}_c &= \mathbf{R} \cdot \mathsf{diag}(r_{c1}^{(1)} g_1 + c_1, \ldots, r_{cn}^{(1)} g_n + c_n) \cdot \mathsf{diag}(h'_1, \ldots, h'_n) \cdot \mathbf{R}'.
\end{aligned}$$

Then, we can compute:

$$\begin{aligned}
\mathbf{W} &= \begin{pmatrix} \mathbf{W}_c & \mathbf{W}_a \\ \mathbf{W}_b & \mathbf{W}_{y^{(1)}} \end{pmatrix} \in \mathbb{Z}^{2n \times 2n} \quad \text{and} \\
\det \mathbf{W} &= \Delta' \cdot \Big((r_{ai}^{(1)} g_i + a_i) \cdot (r_{bi}^{(1)} g_i + b_i) - (r_{ci}^{(1)} g_i + c_i) \cdot (r_i^{(1)} g_i + 1) \Big),
\end{aligned}$$

where $\Delta' = \det(R)^2 \cdot \det(R')^2 \cdot (\prod_i h'_i)^2$. If c is equal to $a \cdot b$, then the quantity above has $\prod_i g_i$ as a large factor. If c is uniformly and independently sampled in G, then the quantity above is independent from $\prod_i g_i$. The cost of the attack is bounded by $\widetilde{\mathcal{O}}(\kappa^{\omega+3}\lambda^{2\omega+6})$.

5 Conclusion

In this paper, we propose polynomial-time attacks for CRT-ACD with auxiliary input, the CLT scheme and its related problems.

Until now, the CRT-ACD is known to be hard problems. However, if an auxiliary input $\hat{P} = \sum_{i=1}^{n} \prod_{j \neq i} p_j = \mathsf{CRT}_{(p_1, \cdots, p_n)}(\prod_{j \neq 1} p_j, \cdots, \prod_{j \neq n} p_j)$ is given, we find quadratic equations for secret parameters and construct a matrix. The matrix has eigenvalues as secret parameters and reveals them by computing characteristic polynomial of the matrix. Adapting this methods to the CLT scheme allows us to totally find every secret parameters.

In order to apply our attacks, it is important that the **Lemma 1** is established for three CRT instances. More precisely, for $A = \mathsf{CRT}_{(p_i)}(a_i)$, $B = \mathsf{CRT}_{(p_i)}(b_i)$ and $C = \mathsf{CRT}_{(p_i)}(c_i)$, if $|a_i \cdot b_i \cdot c_i| > p_i$, the product of A, B, C and $\hat{P}$ does not give a linear integer equation for a_i, b_i, c_i so it is not easy to recover p_i.

Unfortunately, it is possible only when low level encodings of zero and zero-testing parameter are given. Because some applications use the CLT scheme without the encoding of zero, the hardness of the schemes remain interesting problems. When low level encodings are not given in applications of the CLT graded encoding scheme, we only have zero-testing parameter in the form of $\hat{P} \cdot \mathsf{CRT}_{(p_i)}(\frac{z^\kappa}{g_i})$. If multiplying it with top level encoding of zero $A = \mathsf{CRT}_{(p_i)}(\frac{a_i \cdot g_i}{z^\kappa})$, it is of the form $A \cdot \hat{P} \cdot \mathsf{CRT}_{(p_i)}(\frac{z^\kappa}{g_i}) = \sum_{i=1}^{n} a_i \hat{p}_i$. However, the size of a_i is too large to multiply other level zero encodings. In other case, when A is a product of low level encodings, one can not reduce the $\mathsf{CRT}_{(p_i)}(\frac{1}{g_i})$. In many cases, the size of $\frac{1}{g_i} \bmod p_i$ is similar to that of p_i. Hence, in this case too, it is not easy to recover the secret primes p_i.

Therefore, natural proceedings of this research is to extend the range of applications of graded encoding schemes for which the encodings of zero are not needed.

Acknowledgments.

The authors would like to extend their heartfelt gratitude Michel Abdalla, Jean-Sébastien Coron, Shai Halevi, Adeline Langlois, Tancrède Lepoint, Benoît Libert, Alon Rosen, Gilles Villard and Joe Zimmerman for constructive discussions. The authors from SNU received support from the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (No. 2016XXXX). The last author from ENS de Lyon was supported by the ERC Starting Grant ERC-2013-StG-335086-LATTAC.

References

[1] M. Abdalla, F. Benhamouda, and D. Pointcheval. Disjunctions for hash proof systems: New constructions and applications. In *Advances in Cryptology - EUROCRYPT 2015*, pages 69–100, 2015.

[2] N. Attrapadung. Fully secure and succinct attribute based encryption for circuits from multi-linear maps. *IACR Cryptology ePrint Archive*, 2014.

[3] F. Benhamouda and D. Pointcheval. Verifier-based password-authenticated key exchange: New models and constructions. *IACR Cryptology ePrint Archive*, 2013.

[4] D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In *Advances in Cryptology - CRYPTO 2004*, pages 41–55, 2004.

[5] D. Boneh, E. Goh, and K. Nissim. Evaluating 2-dnf formulas on ciphertexts. In *Theory of Cryptography, Second Theory of Cryptography Conference, TCC 2005*, pages 325–341, 2005.

[6] D. Boneh, K. Lewi, H. W. Montgomery, and A. Raghunathan. Key homomorphic prfs and their applications. In *Advances in Cryptology - CRYPTO 2013*, pages 410–428, 2013.

[7] D. Boneh and A. Silverberg. Applications of multilinear forms to cryptography. *Contemporary Mathematics, American Mathematical Society*, 324:71–90, 2003.

[8] D. Boneh, D. J. Wu, and J. Zimmerman. Immunizing multilinear maps against zeroizing attacks. *IACR Cryptology ePrint Archive*, 2014.

[9] Z. Brakerski and G. N. Rothblum. Obfuscating conjunctions. In *Advances in Cryptology - CRYPTO 2013*, pages 416–434, 2013.

[10] J. H. Cheon, J.-S. Coron, J. Kim, M. S. Lee, T. Lepoint, M. Tibouchi, and A. Yun. Batch fully homomorphic encryption over the integers. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 315–335. Springer, 2013.

[11] J. H. Cheon, P. Fouque, C. Lee, B. Minaud, and H. Ryu. Cryptanalysis of the new CLT multilinear map over the integers. *IACR Cryptology ePrint Archive*, 2016.

[12] J. H. Cheon, K. Han, C. Lee, H. Ryu, and D. Stehlé. Cryptanalysis of the multilinear map over the integers. In *Advances in Cryptology - EUROCRYPT 2015*, pages 3–12, 2015.

[13] J. H. Cheon and D. Kim. Probability that the k-gcd of products of positive integers is b-smooth. *IACR Cryptology ePrint Archive*, page 334, 2016.

[14] J. Coron, C. Gentry, S. Halevi, T. Lepoint, H. K. Maji, E. Miles, M. Raykova, A. Sahai, and M. Tibouchi. Zeroizing without low-level zeroes: New MMAP attacks and their limitations. In *Advances in Cryptology - CRYPTO 2015*, pages 247–266, 2015.

[15] J. Coron, T. Lepoint, and M. Tibouchi. Practical multilinear maps over the integers. In *Advances in Cryptology - CRYPTO 2013*, pages 476–493, 2013.

[16] J. Coron, T. Lepoint, and M. Tibouchi. Cryptanalysis of two candidate fixes of multilinear maps over the integers. *IACR Cryptology ePrint Archive*, 2014.

[17] J. Coron, T. Lepoint, and M. Tibouchi. Personal communication. 2014.

[18] J. Coron, T. Lepoint, and M. Tibouchi. New multilinear maps over the integers. In *Advances in Cryptology - CRYPTO 2015*, pages 267–286, 2015.

[19] J.-S. Coron, M. S. Lee, T. Lepoint, and M. Tibouchi. Cryptanalysis of ggh15 multilinear maps. 2015.

[20] J.-S. Coron, M. S. Lee, T. Lepoint, and M. Tibouchi. Zeroizing attacks on indistinguishability obfuscation over clt13. 2016.

[21] S. Garg, C. Gentry, and S. Halevi. Candidate multilinear maps from ideal lattices. In *Advances in Cryptology - EUROCRYPT 2013*, pages 1–17, 2013.

[22] S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai, and B. Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. In *IEEE Symposium on Foundations of Computer Science, FOCS*, pages 40–49, 2013.

[23] S. Garg, C. Gentry, S. Halevi, and M. Zhandry. Fully secure attribute based encryption from multilinear maps. *IACR Cryptology ePrint Archive*, 2014.

[24] S. Garg, C. Gentry, S. Halevi, and M. Zhandry. Functional encryption without obfuscation. In *Proceedings of TCC 2016-A*, volume 9563 of *Lecture Notes in Computer Science*, pages 480–511. Springer, 2016.

[25] C. Gentry. Fully homomorphic encryption using ideal lattices. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009*, pages 169–178, 2009.

[26] C. Gentry, S. Gorbunov, and S. Halevi. Graph-induced multilinear maps from lattices, 2015.

[27] C. Gentry, S. Halevi, H. K. Maji, and A. Sahai. Zeroizing without zeroes: Cryptanalyzing multilinear maps without encodings of zero. *IACR Cryptology ePrint Archive*, 2014.

[28] C. Gentry, A. B. Lewko, A. Sahai, and B. Waters. Indistinguishability obfuscation from the multilinear subgroup elimination assumption. In *Proceedings of FOCS 2015*, pages 151–170, 2015.

[29] C. Gentry, A. B. Lewko, and B. Waters. Witness encryption from instance independent assumptions. In *Advances in Cryptology - CRYPTO 2014*, pages 426–443, 2014.

[30] N. Howgrave-Graham. Approximate integer common divisors. pages 51–66, 2001.

[31] Y. Hu and H. Jia. Cryptanalysis of GGH map. *IACR Cryptology ePrint Archive*, page 301, 2015.

[32] H. T. Lee and J. H. Seo. Security analysis of multilinear maps over the integers. In *Advances in Cryptology - CRYPTO 2014*, pages 224–240, 2014.

[33] K. Lewi, H. W. Montgomery, and A. Raghunathan. Improved constructions of prfs secure against related-key attacks. In *Applied Cryptography and Network Security*, pages 44–61, 2014.

[34] M. Scott. Authenticated ID-based key exchange and remote log-in with simple token and PIN number. *IACR Cryptology ePrint Archive*, page 164, 2002.

[35] A. Storjohann. Integer matrix rank certification. In *Symbolic and Algebraic Computation, International Symposium, ISSAC*, pages 333–340, 2009.

[36] M. van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan. Fully homomorphic encryption over the integers. In *Advances in Cryptology - EUROCRYPT 2010*, pages 24–43, 2010.

[37] M. Zhandry. Adaptively secure broadcast encryption with small system parameters. *IACR Cryptology ePrint Archive*, 2014.

[38] J. Zimmerman. How to obfuscate programs directly. In *Advances in Cryptology - EUROCRYPT 2015*, pages 439–467, 2015.