J Cryptol
https://doi.org/10.1007/s00145-018-9307-y

Journal of
CRYPTOLOGY

Cryptanalysis of the CLT13 Multilinear Map*

Jung Hee Cheon · Kyoohyung Han · Changmin Lee · Hansol Ryu
Seoul National University (SNU), Seoul, South Korea
jhcheon@snu.ac.kr
satanigh@snu.ac.kr
cocomi11@snu.ac.kr
sol8586@snu.ac.kr

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

Communicated by Alon Rosen.

Received 9 May 2016 / Revised 28 September 2018

Abstract. In this paper, we describe a polynomial time cryptanalysis of the (approximate) multilinear map proposed by Coron, Lepoint, and Tibouchi in Crypto13 (CLT13). This scheme includes a zero-testing functionality that determines whether the message of a given encoding is zero or not. This functionality is useful for designing several of its applications, but it leaks unexpected values, such as linear combinations of the secret elements. By collecting the outputs of the zero-testing algorithm, we construct a matrix containing the hidden information as eigenvalues, and then recover all the secret elements of the CLT13 scheme via diagonalization of the matrix. In addition, we provide polynomial time algorithms to directly break the security assumptions of many applications based on the CLT13 scheme. These algorithms include solving subgroup membership, decision linear, and graded external Diffie–Hellman problems. These algorithms mainly rely on the computation of the determinants of the matrices and their greatest common divisor, instead of performing their diagonalization.

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

1. Introduction

Multilinear maps are very powerful tools in cryptography. Following their use in constructing two interesting applications: a one-round non-interactive multiparty key exchange protocol and a broadcast encryption scheme with short keys [7], multilinear maps

[*] A preliminary version of this paper appeared in the *Proceedings of EUROCRYPT 2015*, Lecture Notes in Computer Science 9056, Springer-Verlag [11].

Published online: 06 December 2018

have yielded many remarkable cryptographic applications. However, without the realization of multilinear maps, the promising applications would have been only ambiguous implementations. As a first breakthrough in the generation of multilinear maps, Garg, Gentry, and Halevi introduced the concept of graded encoding schemes as a variant of multilinear maps and described a candidate approximate construction (GGH13) using ideal lattices. Shortly after this, Coron, Lepoint, and Tibouchi [15] proposed another potential graded encoding scheme (CLT13) over integers. These graded encoding schemes expanded their applications such as general-purpose obfuscation, functional encryption, and others [1,3,5,6,22,24–26,30,36,37].

The security of the applications based on the graded encoding schemes relies on the presumed hardness of the problems such as the graded decision Diffie–Hellman (GDDH), subgroup membership (SubM), decision linear (DLIN), and graded external-decision Diffie–Hellman (GXDH) problems. However, it was showed that when instantiated in the GGH13 scheme with some distinct encodings termed as low-level encodings of zero, the SubM, DLIN, and GXDH problems could be solved in polynomial time by the so-called *zeroizing attack* [20, Sec. 6] (also called the weak discrete logarithm attack). Subsequently, this approach became potentially more powerful: Hu and Jia extended it and proved that the GDDH problem could also be solved in polynomial time [28].

In contrast, the CLT13 scheme was not apparently susceptible to the zeroizing attack. It was believed that the problems, including SubM, DLIN, GXDH, and GDDH, were hard problems in the CLT13 scheme. Thus, the CLT13 scheme is considered as the only candidate for implementing applications that require the presumed hardness of the problems as the security basis. Such applications include key-homomorphic pseudorandom functions and a one-round group password-based authenticated key exchange [1,3,5,6,15,22,30,36]: The widespread use of the CLT13 scheme has raised concerns about its security because its presumed hardness has not been proven for standard assumptions.

Our Contributions In this paper, we describe a polynomial time cryptanalysis of the CLT13 scheme. This algorithm employs low-level encodings of zero. Our algorithm is applicable until such encodings of zero are used for the "rerandomization procedure" in the CLT13 scheme. We then show that this algorithm allows the recovery of all the secret parameters. Using these secret parameters, we can eventually solve the SubM, DLIN, GXDH, and GDDH problems.

Apart from an indirect attack, we also provide polynomial time algorithms for analyzing three related problems in the CLT13 scheme: the SubM, DLIN, and GXDH problems. Although these polynomial time algorithms are not as efficient as the previous ones because of their computational complexity, they are of significance in that they can be directly applied to the problems.

Consequently, there is no direct construction of secure multilinear maps, for which any of the GDDH, SubM, DLIN, and GXDH problems are hard.[1] Several cryptographic applications are impacted,e.g., all the constructions of [3,22,30,36], GPAKE construc-

[1] For multilinear maps constructed by the candidate obfuscation schemes, assessing the hardness of these computational problems is an interesting open problem.

tion in [1] for more than three users, one of the two constructions of password hashing in [5], and one of the key-homomorphic PRF constructions in [6].

Technical Overview We describe two independent methods for solving the problems associated with the CLT13 scheme. The first method allows for determining all the secret elements of the CLT13 scheme, and the second one solves each problem directly. We name these two techniques as the eigenvalue technique and determinant technique, respectively, because the main part of each algorithm is the computation of the eigenvalues and determinants, respectively.

Let p_i be the secret distinct primes for $1 \le i \le n$, and x_0 equal $\prod_{i=1}^{n} p_i$. We denote $\hat{p}_i = x_0/p_i$ for each i and $\hat{P} = \sum_{i=1}^{n} \hat{p}_i$. For integer vector $\boldsymbol{r} = (r_i) \in \mathbb{Z}^n$ with $r_i \ll p_i$, a Chinese remainder encoding of $\boldsymbol{r}$ (referred as CRT-encoding) is defined as an integer, denoted by $\mathsf{CRT}_{(p_i)}(r_i) \in (x_0/2, x_0/2]$. This is congruent to integer r_i in each modulo p_i. Informally, the setting of the CLT13 scheme is reduced to the following problem: when we are given x_0, $\hat{P}$, and polynomially many CRT-encodings of the integer vectors, recover all the secret primes.

In [19], Galbraith, Gebregiyorgis, and Murphy introduced a CRT-approximate greatest common divisor problem ($\mathsf{CRT\text{-}ACD}$) problem. Herein, when given a multiple of x_0, written as $x_0 \cdot q_0$, and variants of CRT-encodings, $x_0 \cdot q_j + \mathsf{CRT}_{(p_i)}(r_{ij})$, for polynomially many $j \ge 1$, find the secret primes, for which integers q_j are sampled from some distribution. Compared to the $\mathsf{CRT\text{-}ACD}$ problem, we consider $q_0 = 1$ and $q_j = 0$ for all $j \ge 1$. In addition, integer $\hat{P}$ is given. Therefore, we call this problem as $\mathsf{CRT\text{-}ACD}$ *with an auxiliary input*.

(1) *Eigenvalue Technique* Our main technique is to construct a diagonalizable matrix in $\mathbb{Q}$ whose eigenvalues are r_i for some CRT-encoding, $\mathsf{CRT}_{(p_i)}(r_i)$. Then, by computing the greatest common divisor (gcd) between x_0 and $(\mathsf{CRT}_{(p_i)}(r_i) - r_i)$, we recover p_i.

More precisely, under the condition that the magnitude of r_i is sufficiently small, we observe that

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

The equality holds over integers. According to the Chinese remainder theorem, the product of the CRT-encodings yields a CRT-encoding in which the corresponding message vectors are multiplied componentwise. Therefore, we can extend the observation to the product of the CRT-encodings until each component of the message vector is much smaller than p_i.

For several CRT-encodings $\mathsf{CRT}_{(p_i)}(r_{i,j})$, let $w_{j,k}$ and $w'_{j,k}$ be integers $[\mathsf{CRT}_{(p_i)}(r_{i,j}) \cdot \mathsf{CRT}_{(p_i)}(r_{i,1}) \cdot \mathsf{CRT}_{(p_i)}(r_{i,k}) \cdot \hat{P}]_{x_0}$ and $[\mathsf{CRT}_{(p_i)}(r_{i,j}) \cdot \mathsf{CRT}_{(p_i)}(r_{i,k}) \cdot \hat{P}]_{x_0}$, respectively. Then, by spanning indices $j, k \in \{1, \dots, n\}$, we can construct matrices $\mathbf{W} = (w_{j,k})_{j,k}$ and $\mathbf{W}' = (w'_{j,k})_{j,k}$, which can be written as

$$\mathbf{W} = \mathbf{R} \cdot \mathsf{diag}(r_{i,1}) \cdot \mathbf{R}' \quad \text{and} \quad \mathbf{W}' = \mathbf{R} \cdot \mathbf{R}'$$

for $\mathbf{R} = (r_{i,j})_{i,j}$, $\mathbf{R}' = (\hat{p}_i \cdot r_{i,k})^T_{i,k}$ and diagonal matrix $\mathsf{diag}(r_{i,1})$, whose i-th diagonal entry is $r_{i,1}$. By assuming that matrices $\mathbf{R}$ and $\mathbf{R}'$ are invertible, we obtain matrix $\mathbf{Y}$ in the following form:

$$\mathbf{Y} = \mathbf{W} \cdot (\mathbf{W}')^{-1} = \mathbf{R} \cdot \mathsf{diag}(r_{i,1}) \cdot (\mathbf{R})^{-1},$$

whose eigenvalues are exactly the set, $\{r_{1,1}, \ldots, r_{n,1}\}$. Hence, we can compute the eigenvalues in polynomial time from $\mathbf{Y}$. As mentioned above, by computing $\gcd(x_0, \mathsf{CRT}_{(p_i)}(r_{i,1}) - r_{i,1})$, we can recover secret prime p_i for each i. We refer to Sect. 3 for the application of this strategy in the CLT13 scheme.

(2) *Determinant Technique* For the SubM, DLIN, and GXDH problems, the determinant technique could be directly used to analyze the problems instead of performing the eigenvalue-based analysis. For example, we consider a simplified SubM problem: given two CRT-encodings $A = \mathsf{CRT}_{(p_i)}(r_i)$ and $B = \mathsf{CRT}_{(p_i)}(r_i')$, where r_i and r_i' are ρ-bit integers much smaller than p_i. We need to distinguish whether r_i and r_i' are co-prime for all i.

Given two CRT-encodings $A = \mathsf{CRT}_{(p_i)}(r_i)$ and $B = \mathsf{CRT}_{(p_i)}(r_i')$, our goal is to construct two matrices over $\mathbb{Z}$ whose determinants are multiples of $\prod_{i=1}^n r_i$ and $\prod_{i=1}^n r_i'$, respectively. Then, one can solve this problem by computing the gcd.

More precisely, in the construction of $\mathbf{W}$, we can build two matrices $\mathbf{W}_A$ and $\mathbf{W}_B$ by replacing $\mathsf{CRT}_{(p_i)}(r_{i,1})$ with A and B, respectively. Therefore, the determinants of these matrices are $\det(\mathbf{W}_A) = \det(\mathbf{R}) \cdot \det(\mathbf{R}') \cdot \prod_{i=1}^n r_i$ and $\det(\mathbf{W}_B) = \det(\mathbf{R}) \cdot \det(\mathbf{R}') \cdot \prod_{i=1}^n r_i'$, respectively. Next, we consider the value of $\det(\mathbf{W}_A)/\gcd(\mathbf{W}_A, \mathbf{W}_B)$. If r_i and r_i' have a common factor for all i, then this term is smaller than $2^{n\cdot(\rho-1)}$. Otherwise, this value is not smaller than $2^{n\cdot(\rho-1)}$, and thus, we can solve the simplified SubM problem. This method can also be applied to the DLIN and GXDH problems. We refer to Sect. 4 for more details.

Related and Follow-up Works After the preliminary investigations of this work were published in the IACR Cryptology ePrint Archive and the proceedings of the Eurocrypt'15 conference, the attack was extended and the CLT13 scheme was transformed to prevent the attack. Our attack strongly relies on the fact that the low-level encodings of 0 are published. In [8], Boneh, Wu, and Zimmerman first extended our attack without giving the encoding of 0. Moreover, they described a modification of the CLT13 scheme to prevent the extended attack. Additionally, an independent approach to immunize the CLT13 scheme against our attack was proposed by Garg, Gentry, Halevi, and Zhandry [23].[2] Since then, Coron *et al.* [13] have extended the attack by using the so-called *orthogonal encodings*. This work showed that the two immunizations were insecure. Apart from these immunization works, a further modification of CLT13 was proposed by Coron, Lepoint, and Tibouchi in Crypto'15 [17]. They claimed that our attack and the extended attack were prevented because the modified scheme maintained underlying modulus x_0 a secret, such that the zero-testing procedure depended on the secret values nonlinearly. However, it was also shown to be insecure by Cheon, Fouque, Lee, Minaud, and Ryu in [10], who demonstrated the recovery of x_0.

Nonetheless, for the security of the general-purpose obfuscation schemes in the CLT13 scheme, one of the promising applications still remains an open problem because the schemes are neither given the encodings of zero nor are subjected to the extended attacks.

[2] After this work, Garg *et al.* [24] replaced the underlying multilinear map with a new scheme suggested by Coron, Lepoint, and Tibouchi in Crypto'15 [17].

Thereafter, Coron, Lepoint, and Tibouchi provided a new analysis result [14] that could enable one to break the polynomial time for several CLT13-based candidate obfuscations with a distinct property called input partitionability in the CLT13 scheme [2,4,21,32, 33]. However, this property of input partitionability is not typically satisfied. It was also suggested to convert any input-partitionable obfuscation scheme in the CLT13 scheme to a non-input-partitionable scheme [18]. In summary, the security of the general obfuscations in the CLT13 scheme has not yet been clarified.

Notation. We use $a \leftarrow A$ to denote the operation of uniformly choosing element a from finite set A. We define $[n] = \{1, 2, \ldots, n\}$. We let $\mathbb{Z}_q$ denote ring $\mathbb{Z}/(q\mathbb{Z})$. For pairwise co-prime integers $p_1, p_2, \ldots, p_n$ and integers $r_1, r_2, \ldots, r_n$, 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 $r_i \mod p_i$ for all $i \in [n]$. We use notation $[t]_p$ for integers t and p to denote the reduction of t modulo p in the interval $(-p/2, p/2]$.

We use lower-case bold letters to denote the vectors, whereas we use the upper-case bold letters 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 $\mathsf{diag}(a_1, \ldots, a_n)$ or $\mathsf{diag}(a_i)$ in the diagonal matrix with diagonal coefficients equal to $a_1, \ldots, a_n$.

Organization In Sect. 2, we define the CRT-ACD problem and its analysis. In Sect. 3, we recall the CLT13 scheme and adapt the analysis to it. In Sect. 4, we introduce three related problems on the CLT13 scheme and their cryptanalyses. We conclude this paper in Sect. 5.

2. CRT-ACD with an Auxiliary Input

In this section, we introduce and analyze the CRT-ACD problem using an auxiliary input. The approximate greatest common divisor problem (ACD) was initially introduced by Howgrave-Graham [27] as was the problem of finding secret prime p given many near-multiples of p. One of the promising applications of this problem is a homomorphic encryption scheme [35]. The scheme offers 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. Galbraith, Gebregiyorgis, and Murphy provided an informal definition of an extended ACD problem, which is called the CRT-ACD problem [19]. An instance of the problem is an integer of the form $p_i q_i + r_i$ for several primes p_i. Therefore, it can be defined by using the CRT. Cheon *et al.* provided a batch-homomorphic encryption [9] based on the CRT-ACD problem. For appropriate parameters, Galbraith *et al.* argued that “it is an open problem to give an algorithm to solve the CRT-ACD problem that exploits the CRT structure” [19].

In this section, however, we show that when some integer, called the auxiliary input, is given, the CRT-ACD problem can be solved in polynomial time. Now, we define the precise variant of the CRT-ACD we consider.

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

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

The $\mathsf{CRT\text{-}ACD}$ problem with an auxiliary input is as follows: For polynomially many given samples from $\mathcal{D}_{\chi_\varepsilon,\eta}(p_1, \dots, p_n)$, x_0 and $\hat{P} = \mathsf{CRT}_{(p_i)}(\hat{p}_i)$, the goal is to obtain p_i for all i.

Auxiliary input $\hat{P}$ needs the distinct feature that it 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 $n + \log n < \eta - 1$. Extending this property, we obtain the following lemma.

Lemma 1. *Let* $\hat{P} = \mathsf{CRT}_{(p_i)}(\hat{p}_i)$ *and* $a = \mathsf{CRT}_{(p_i)}(r_i) \leftarrow \mathcal{D}_{\chi_\varepsilon,\eta}(p_1, \dots, p_n)$. *Assume that* $\varepsilon + n + \log n + 1 < \eta$. *Then, the following holds:*

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

Proof. The first equality is clear by the definition of the CRT. To show that the second equality is correct, we consider the equation in each modulo p_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 $\hat{p}_j = 0 \mod p_i$ for $j \neq i$. Finally, the magnitude of $\sum\limits_{i=1}^{n} r_i \cdot \hat{p}_i$ is smaller than $n \cdot 2^\varepsilon \cdot 2^{(n-1)\cdot\eta}$, which is less than $2^{n\cdot(\eta-1)-1}$ under the condition, and thus, $x_0/2$. Hence, based on the uniqueness of CRT, the second equality holds. □

This lemma transforms the modulus equation to an integer equation of $r_1, \dots, r_n$ with unknown coefficients $\hat{p}_1, \dots, \hat{p}_n$.

Our algorithm for solving $\mathsf{CRT\text{-}ACD}$ with an auxiliary input consists of two steps. The first step is to construct a diagonalizable matrix in $\mathbb{Q}$, whose eigenvalues are set $\{r_i\}$ of some $\mathsf{CRT\text{-}ACD}$ sample $\mathsf{CRT}_{(p_i)}(r_i)$. The next step is to recover r_i by computing the eigenvalues. Then, by computing the common divisor of $\mathsf{CRT}_{(p_i)}(r_i) - r_i$ and x_0, we can obtain all p_i.

We now describe the complete details of solving $\mathsf{CRT\text{-}ACD}$ with an auxiliary input.

2.1. *Constructing Matrix Equations in* $\mathbb{Q}$

Suppose we are given $2n + 1$ samples from distribution $\mathcal{D}_{\chi_\varepsilon,\eta}(p_1, \dots, p_n)$ as follows:

$$a_j = \mathsf{CRT}_{(p_i)}(a_{i,j}),\ b = \mathsf{CRT}_{(p_i)}(b_i),\ c_k = \mathsf{CRT}_{(p_i)}(c_{i,k}) \text{ for } 1 \leq j, k \leq n.$$

For simplicity, we denote $w_{j,k}$ and $w'_{j,k}$ by $a_j \cdot b \cdot c_k \mod x_0$ and $a_j \cdot c_k \mod x_0$, respectively.

To adapt Lemma 1 to $w_{j,k}$ and $w'_{j,k}$ under the condition $3\varepsilon + n + \log n + 1 < \eta$, we have

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

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

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

$$\mathbf{W} = \mathbf{A}^T \cdot \mathsf{diag}(b_1\hat{p}_1, \ldots, b_n\hat{p}_n) \cdot \mathbf{C},$$
$$\mathbf{W}' = \mathbf{A}^T \cdot \mathsf{diag}(\hat{p}_1, \ldots, \hat{p}_n) \cdot \mathbf{C}$$

for $\mathbf{A}^T = (a_{i,j})$ and $\mathbf{C} = (c_{i,k}) \in \mathbb{Z}^{n\times n}$. Suppose matrices $\mathbf{A}$ and $\mathbf{C}$ are invertible in $\mathbb{Q}$. We compute $(\mathbf{W}')^{-1}$ over $\mathbb{Q}$ and the following matrix:

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

2.2. *Disclosing all the Secret Quantities*

The eigenvalues of matrix $\mathbf{V}$ discussed in Sect. 2.1 are exactly those in $B = \{b_1, \ldots, b_n\}$. Set B can be computed in polynomial time in η, n, and ε from $\mathbf{V}$ by computing the roots of the characteristic polynomial.

Prime p_i is a common factor to both $(b - b_i)$ and x_0, which have other common factors if and only if $b_j = b_i$ for some $j \in \{1, \ldots, n\}$. Hence, if b_is are distinct, we can obtain all secret integers $p_1, \ldots, p_n$.

Remark Two conditions are required for our algorithm to work appropriately. The first is that matrices $\mathbf{A}$ and $\mathbf{C}$ are invertible, and the other is that $b_i \neq b_j$ for all $1 \leq i < j \leq n$. The probability that each condition is satisfied depends on distribution χ_ε and matrix size n. Because the two conditions are independent and as they depend on different variables, our attack succeeds in obtaining the probability of the product of the two probabilities. For example, let χ_ε be a uniform distribution in $(-2^\varepsilon, 2^\varepsilon)$, and let n be asymptotically a polynomial of ε, i.e., $n = poly(\varepsilon)$. The first probability is overwhelming with respect to ε [31, Lem. 1], whereas the second probability is equal to $\frac{n!\cdot\binom{2\cdot 2^\varepsilon - 1}{n}}{(2\cdot 2^\varepsilon - 1)^n}$, where ! is the factorial operator and $\binom{2\cdot 2^\varepsilon + 1}{n}$ is the binomial coefficient. The latter probability is also overwhelming with respect to ε, where $n = poly(\varepsilon)$.

Let $f_{\mathbf{V}}$ be a characteristic polynomial of matrix $\mathbf{V}$. Because each root b_i is less than 2^ρ, we consider prime p_0 that is larger than 2^ρ and find roots x such that $f_{\mathbf{V}}(x) \bmod p_0$. This reveals the original roots of $f_{\mathbf{V}}$ in $O(M(n(\rho+\log n))\cdot(\rho+\log n)\cdot\log n)=\widetilde{\mathcal{O}}(n\cdot\rho^2)$ by Rabin's algorithm [34], where $M(t)$ is an upper bound to the number of bit operations required to multiply two t-bit numbers.

Because our attack consists of a matrix multiplication, computing a characteristic polynomial and finding the roots of the polynomial, the complexity of the first two algorithms is bounded by $\widetilde{\mathcal{O}}(n^{\omega}\cdot\log x_0)=\widetilde{\mathcal{O}}(n^{\omega}\cdot n\cdot\eta)$ and that of the last one is bounded by $\widetilde{\mathcal{O}}(n\cdot\rho^2)$ with $\omega\leq 2.38$. This implies that the overall cost is bounded by $\widetilde{\mathcal{O}}(n^{\omega+1}\cdot\eta)$, with $\omega\leq 2.38$.[3] Hence, we obtain the following result:

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

3. Application to the CLT13 Multilinear Map

We first recall the CLT13 multilinear map and then describe the attack. We refer to the original paper [15] for a complete description.

3.1. *Candidate Multilinear Map Over the Integers*

The CLT13 scheme requires the following parameters:

λ: the security parameter
κ: the multilinearity parameter
ρ: the bit length of the randomness used for the encodings
α: the bit length of the message slots
η: the bit length of 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. suggested setting the parameters such that the following conditions were satisfied:

- $\rho=\Omega(\lambda)$: to avoid a brute force attack (see also [29] 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 $\mathbb{Z}_{g_i}$.
- $n=\Omega(\eta\cdot\lambda)$: to prevent the lattice reduction attacks [15, Sec. 5].
- $\ell\geq n\cdot\alpha+2\lambda$: to be able to apply the leftover hash lemma from [15, Lem. 1].

[3] If the determinant of neither $\mathbf{A}$ or $\mathbf{C}$ is not a multiple of p_0, the same result can be obtained by performing the procedure of Sect. 2.1 modulo p_0. In this case, the total complexity becomes $\widetilde{\mathcal{O}}(n^{\omega}\cdot\rho)$ [16].

- $\tau \geq n \cdot (\rho + \log_2(2n)) + 2\lambda$: to apply the leftover hash lemma from [15, Sec. 4].
- $\beta = \Omega(\lambda)$: to avoid the so-called gcd attack [29].
- $\eta \geq \rho_\kappa + \alpha + 2\beta + \lambda + 8$, where ρ_κ is the maximum bit size of the level-κ encoding of random r_i. 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 the zero-test correctness.

Instance generation $(\mathsf{params}, \mathbf{p}_{zt}) \leftarrow \mathsf{InstGen}(\mathbf{1}^\lambda, \mathbf{1}^\kappa)$. We set the scheme parameters as explained above. For $i \in [n]$, we 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 $\Pi = (\pi_{ij})_{i,j} \in \mathbb{Z}^{n \times n}$ 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 $i \in [n]$, we generate $\mathbf{r}_i \in \mathbb{Z}^n$ by choosing randomly and independently in the half-open parallelepiped spanned by the columns of matrix Π and denote by r_{ij} the j-th component of $\mathbf{r}_i$. Generate $\mathbf{H} = (h_{ij})_{i,j} \in \mathbb{Z}^{n \times n}$, $\mathbf{A} = (a_{ij})_{i,j} \in \mathbb{Z}^{n \times \ell}$ such that $\mathbf{H}$ is invertible and $\|\mathbf{H}^T\|_\infty \leq 2^\beta$, $\|(\mathbf{H}^{-1})^T\|_\infty \leq 2^\beta$ for $i \in [n]$, $j \in [\ell]$, m $a_{ij} \leftarrow [0, g_i)$.[4] Then, define:

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

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.

Sampling level-zero encodings $c \leftarrow \mathsf{samp}(\mathsf{params})$. For $1 \leq j \leq \ell$, sample $b_j \leftarrow \{0, 1\}$ and compute $c = \left[\sum_{j=1}^{\ell} b_j \cdot x'_j\right]_{x_0}$. Note that the message of an encoding sampled from this procedure is unknown.

Encodings at level-1 $c' \leftarrow \mathsf{enc}(\mathsf{params}, c)$. Given a level-zero encoding c, compute a level-1 encoding of the same message by computing $c' = [c \cdot y]_{x_0}$.

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 $c' = \left[c + \sum_{j \in [\tau]} b_j \cdot x_j + \sum_{i \in [n]} b'_i \cdot \Pi_i\right]_{x_0}$. Note that this is the only procedure in the CLT13 scheme that uses x_j's.[5]

[4] Matrix $\mathbf{H}$ is generated in a specific approach. We refer to the original paper [15].

[5] This procedure can be adapted to higher levels $1 < k \leq \kappa$ by publishing the 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* $\mathsf{isZero}(\mathsf{params}, \mathbf{p}_{zt}, u_\kappa) \overset{?}{=} 0/1$. Given a level-$\kappa$ encoding c, return 1 if $\|[\mathbf{p}_{zt} \cdot c]_{x_0}\|_\infty < x_0 \cdot 2^{-\nu}$, and 0 otherwise.

Coron et al. also described a variant in which only one such zero-testing parameter, $\mathbf{p}_{zt}$ was given rather than n of them (see [15, Se. 6]). In [26, App. B.3], Gentry, Lewko, and Waters described an asymmetric version of the construction, which we briefly recall in Sect. 4. Our attack can also be adapted to these variants.

3.2. *Zeroizing Attack on CLT13*

In this section, we adapt the analysis of CRT-ACD with an auxiliary input to the CLT13 scheme. The instances of the problem and CLT13 scheme are quite similar. The encodings of the CLT13 resemble the instances of the problem, except for secret constant z. Zero-testing parameters $(\mathbf{p}_{zt})_j$ are also similar to auxiliary input $\hat{P}$, except for constant $[z^\kappa/\mathsf{CRT}_{(p_i)}(g_i)]_{x_0}$. Therefore, we only consider the zero-testing value of the encodings of zero, such that the constant is canceled.

More precisely, let a be a top-level encoding of zero, written as $a = \mathsf{CRT}_{(p_i)}(r_i g_i / z^\kappa)$. Hereafter, because we use only one zero-testing parameter, without the loss of generality, we denote $(\mathbf{p}_{zt})_1$ as p_{zt}. Similar to Lemma 1, we have

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

until the last quantity has a magnitude smaller than $x_0/2$. Under the zero-testing conditions, it is typically true for the valid top-level encodings of zero. Next, by replacing a with κ-level encodings of zero $\pi_u \cdot x_1' \cdot \pi_v \cdot y^{\kappa-2}$ or $\pi_u \cdot \pi_v \cdot y^{\kappa-2}$ for $1 \le u, v \le n$ in the above equation, we have:

$$\begin{aligned} w_{uv} &= \Pi_u \cdot x_1' \cdot \Pi_v \cdot y^{\kappa-2} \cdot p_{zt} \bmod x_0 \\ &= \sum_{i=1}^{n} \hat{p}_i \cdot h_i \cdot g_i \cdot \pi_{iu} \cdot (r_i g_i + 1)^{\kappa-2} \cdot x_{i1}' \cdot \pi_{iv} \\ &= \sum_{i=1}^{n} \pi_{iu} \cdot x_{i1}' \cdot h_i' \cdot \pi_{iv}, \text{ and} \\ w_{uv}' &= \Pi_u \cdot \Pi_v \cdot y^{\kappa-2} \cdot p_{zt} \bmod x_0 = \sum_{i=1}^{n} \hat{p}_i \cdot h_i \cdot g_i \cdot \pi_{iu} \cdot (r_i g_i + 1)^{\kappa-2} \cdot \pi_{iv} \\ &= \sum_{i=1}^{n} \pi_{iu} \cdot h_i' \cdot \pi_{iv}, \end{aligned}$$

where $h_i' = \hat{p}_i \cdot h_i \cdot g_i \cdot (r_i g_i + 1)^{\kappa-2}$. By spanning $1 \le u, v \le n$, we obtain the following matrices $\mathbf{W}$ and $\mathbf{W}'$:

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

for $\Pi = (\pi_{ik})_{i,k}$. As in Sect. 2.2, we can recover $\{x'_{11}, \ldots, x'_{n1}\}$ by computing the eigenvalues of $\mathbf{W} \cdot \mathbf{W}'^{-1}$. Hence, we can compute all secret p_i by computing $\gcd(x'_1 - x'_{i1}, x_0)$.

Consequently, we need $\mathbf{W}'$ and $\mathbf{W}$ to be invertible. We argue that this case has a high probability. We prove it for $\mathbf{W}$. Note first that x'_{i1} and h'_i are all nonzero, with overwhelming probability (if the integers are zero, $w_{j,k}$ is a multiple of p_i, and thus, one can recover the factor via $\gcd(x_0, w_{j,k})$). However, matrix Π is invertible by design [15, Fact 1].

Because our algorithm consists of computing an inverse matrix and eigenvalues, the total cost is bounded by $\widetilde{\mathcal{O}}((n^\omega \log x_0)) = \widetilde{\mathcal{O}}(\kappa^{\omega+2}\lambda^{2\omega+3})$, with $\omega \leq 2.38$.

After we know all the p_i, we have $x_j/y = r_{ij}g_i/(r_i g_i + 1) \bmod p_i$. As the numerator and denominator are coprimes and very small compared to p_i, they can be recovered by the rational reconstruction algorithm. Hence, we obtain $(r_{ij}g_i)$ for all j. The gcd of all the $(r_{ij}g_i)$ yields g_i. Thus, we can also recover all the r_{ij} and r_i. 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. Hence, $z \bmod x_0$. h_{ij} can then be recovered along with r'_{ij} and a_{ij}.

4. Subgroup Membership, Decision Linear, and Graded External Diffie–Hellman Problems

We start by defining the SubM, DLIN, and GXDH problems associated with the CLT13 scheme. We then describe how to solve these problems in polynomial time. The attack procedure consists of two steps. First, in Sect. 4.1, we discuss how to recover $\prod_i g_i$, which is an order of the message space. This is a common procedure for solving the SubM and DLIN problems. Next, in Sects. 4.2, 4.3 and 4.4, we present the value for solving the SubM, DLIN, and GXDH problems.

We recall primes $\{g_i\}$ described in Sect. 3.1. Let $G = \mathbb{Z}_{g_1} \times \ldots \times \mathbb{Z}_{g_n}$ and its subgroup $G' = \{0\} \times \mathbb{Z}_{g_2} \times \ldots \times \mathbb{Z}_{g_n}$. We let $\mathsf{enc}_1(m)$ denote a level-1 encoding of $m = (m_1, \ldots, m_n) \in G$ generated by the procedure in Sect. 3.1. Then, it can be written as $\mathsf{CRT}_{(p_i)}(\frac{r_i \cdot g_i + m_i}{z})$ for some integer r_i. For integers $L > 0$, we let $\mathsf{Rk}_j(G^{L\times L})$ denote the set of $L \times L$ matrices over G of rank j. Here, we define rank of matrix $(m^{(u,v)})_{u,v} \in G^{L\times L}$ as the maximum of the ranks of matrices $(m_i^{(u,v)})_{u,v}$, where $m_i^{(u,v)}$ is the i-th entry of $m^{(u,v)} \in G$. Then, the SubM and DLIN problems are defined as follows.

Definition 2. *(Subgroup Membership Problem)* Let I, λ, and κ generate params, $\mathbf{p}_{zt}$. $\{\mathsf{enc}_1(m'_i) : i \in [I]\}$, where the m'_is are uniformly and independently sampled in strict subgroup G' of G. Given params, $\mathbf{p}_{zt}$, $\{\mathsf{enc}_1(m'_i) : i \in [I]\}$, and $\mathbf{M} = \mathsf{enc}_1(m)$, It is determined whether m is sampled uniformly in G' or G.

Definition 3. (*L-Decisional Linear Problem*) Given λ and κ, params and $\mathbf{p}_{zt}$ are generated using $\mathsf{InstGen}$. Define $N = \prod_i g_i$. Given params and $\mathbf{p}_{zt}$, the goal is to distinguish between the distributions.

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

In the constructions in [1], the authors considered the following particular case of the L-DLIN problem. The problem was defined for 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 $a_1, \ldots, a_L, b_1, \ldots, b_L \in G$. Given an encoding of $\mathsf{enc}_1(m)$, the goal was to distinguish whether m was uniformly sampled from G or $m = b_1 + \ldots + b_L$. This can be restated as a distinct case of Definition 3, as it requests to assess whether the matrix below is full rank.

$$\begin{pmatrix} a_1 b_1 & a_1 & 0 & \ldots & 0 \\ a_2 b_2 & 0 & a_2 & \ldots & 0 \\ & & \vdots & & \\ a_L b_L & 0 & 0 & \ldots & a_L \\ m & 1 & 1 & \ldots & 1 \end{pmatrix}$$

Next, to describe the GXDH problem, we briefly recall the asymmetric multilinear map variant of CLT13 [26, App. B.3].

Instance generation $(\mathsf{params}, \mathbf{p}_{zt}) \leftarrow \mathsf{InstGen}(1^\lambda, 1^\kappa)$. The parameter settings of $p_i, g_i, x_0, \{x'_j\}$, and H are as in the original scheme. Let $\Pi^{(t)} = (\pi_{ij}^{(t)})_{i,j} \in \mathbb{Z}^{n\times n}$ with $\pi_{ij}^{(t)} \leftarrow (n2^\rho, (n+1)2^\rho) \cap \mathbb{Z}$ if $i = j$, otherwise $\pi_{ij}^{(t)} \leftarrow (-2^\rho, 2^\rho) \cap \mathbb{Z}$ for $t \in [\kappa]$. For $1 \le t \le \kappa$, z_t is uniformly sampled in $\mathbb{Z}_{x_0}$. Then define, for all $1 \le t \le \kappa$:

$$y^{(t)} = \mathsf{CRT}_{(p_i)}\left(\frac{r_i^{(t)} \cdot g_i + 1}{z_t}\right), \text{ where } r_i^{(t)} \leftarrow (-2^\rho, 2^\rho) \cap \mathbb{Z}, \text{ for } 1 \le i \le n,$$

$$x_j^{(t)} = \mathsf{CRT}_{(p_i)}\left(\frac{r_{ij}^{(t)} \cdot g_i}{z_t}\right), \text{ for } 1 \le j \le \tau,$$

$$\Pi_j^{(t)} = \mathsf{CRT}_{(p_i)}\left(\frac{\pi_{ij}^{(t)} \cdot g_i}{z}\right) \text{ for } j \in [n].$$

Further, we define:

$$(\mathbf{p}_{zt})_j = \sum_{i=1}^{n} h_{ij} \cdot \left(\prod_{1\le t\le\kappa} z_t \cdot g_i^{-1} \bmod p_i\right) \cdot \hat{p}_i \bmod x_0, \text{ for } 1 \le j \le n.$$

Output $\mathsf{params} = (n, \eta, \alpha, \rho, \beta, \tau, \ell, \nu, \{y^{(t)}\}, \{x_j^{(t)}\}, \{x'_j\}, \{\Pi_j^{(t)}\}, s)$ and $\mathbf{p}_{zt}$. From now on, we use $\mathsf{enc}_t(m)$ to denote encoding $\mathsf{CRT}_{(p_i)}(\frac{r_i \cdot g_i + m_i}{z_t})$. We now define the GXDH problem in the CLT13 scheme.

Definition 4. *(Graded External DDH Problem)* Given λ and κ, params and $\mathbf{p}_{zt}$ are generated 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 any integer $t \in [\kappa]$, 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 the 2-DLIN problems by distinguishing the following distributions:

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

Throughout this section, as in Sect. 3.2, we only use one zero-testing parameter; we denote $(\mathbf{p}_{zt})_1$ as p_{zt}.

Our main strategy to solve the three related problems in the CLT13 scheme is as follows: For a given level-1 encoding $\mathsf{enc}_1(m) = \mathsf{CRT}_{(p_i)}(r_i \cdot g_i + m_i)$ (or $\mathsf{enc}_t(m)$ of the asymmetric multilinear map), we first suggest an approach for constructing integral matrix $\mathbf{W}_m \in \mathbb{Z}^{n\times n}$, such that $\mathbf{W}_m = \mathbf{X} \cdot \mathsf{diag}(r_1 \cdot g_1 + m_1, \ldots, r_n \cdot g_n + m_n) \cdot \mathbf{R}$ for some invertible matrices $\mathbf{X}$ and $\mathbf{R} \in \mathbb{Z}^{n\times n}$. Then, by using matrix $\mathbf{W}_m$, we construct a matrix whose determinant is related to an order of the message space, $\prod_i g_i$. Hence, by computing the determinant of the matrix, we can solve each problem.

More precisely, the related problems can be seen as follows:

SubM: Given encoding $\mathsf{enc}_1(m)$, it is determined whether $m \leftarrow G'$ or not.

L-DLIN: Given $L \times L$ matrix of level-1 encodings of $(m^{(i,j)})_{i,j}$, we determine whether the message matrix is of full rank or not.

GXDH: Given a 2×2 matrix of level-1 encodings of $\begin{pmatrix} c & a \\ b & 1 \end{pmatrix}$, we determine whether the matrix is of full rank or not.

In the case of the SubM problem, if m is sampled from G', the value of $\det(\mathbf{W}_m)$ has a non-trivial factor of $\prod g_i$. Otherwise, the value does not have a common factor. In the case of the L-DLIN problem, the determinant of $(\mathbf{W}_{m^{(i,j)}})_{i,j}$ is a multiple of $\prod_i g_i$ if middle term matrix $\mathbf{M}$ does not have a full rank. In other cases, the determinant of $\mathbf{M}$ is not a multiple of $\prod_i g_i$ with a high probability. In the case of the GXDH problem, we can apply the same argument as for the DLIN problem. Hence, if one can recover the $\prod g_i$, one can solve the related problems.

Remark. The important difference between the cryptanalysis of these related problems and that of the CLT13 scheme is the form of the middle matrix of $\mathbf{W}$. The previous attack discussed in Sect. 3.2 is based on the fact that the middle matrix is diagonal. For example, in [8], the authors chose the middle matrix as a block diagonal matrix.[6] However, the attack on the related problems in this section does not depend on it.

[6] Subsequently, it was also showed to be insecure by the extended attack of Coron et al. [13].

4.1. *Computing $\prod_i g_i$ from the CLT13 Instances*

Here, we are given params and one zero-testing parameter p_{zt}, as described in Sect. 3.1. Let us consider $w_{uv}:=\left[\Pi_u \cdot y \cdot \Pi_v \cdot y^{\kappa-3} \cdot p_{zt}\right]_{x_0}$, $w_{uv}^{(i)}:=\left[\Pi_u \cdot \Pi_i \cdot \Pi_v \cdot y^{\kappa-3} \cdot p_{zt}\right]_{x_0}$, where $\Pi_j = \mathsf{CRT}_{(p_i)}(\pi_{ij} \cdot g_i/z)$, and $y = \mathsf{CRT}_{(p_i)}((r_i \cdot g_i + 1)/z)$. Our concept of obtaining $\prod_i g_i$ is that determinant of matrix $(w_{uv}^{(i)})_{u,v}$ is typically a multiple of $\prod_i g_i$. To this end, we deal with the following matrices.

$$\begin{aligned}\mathbf{W}_y &= (w_{uv})_{u,v} = \Pi^T \cdot \mathsf{diag}(r_1 \cdot g_1 + 1, \ldots, r_n \cdot g_n + 1) \cdot \Pi'.\\ \mathbf{W}_i &= (w_{uv}^{(i)})_{u,v} = \Pi^T \cdot \mathsf{diag}(\pi_{i1} \cdot g_1, \ldots, \pi_{in} \cdot g_n) \cdot \Pi',\end{aligned}$$

where $\Pi = (\pi_{ij})_{i,j}$, $\Pi' = (h_i \cdot g_i \cdot (r_i \cdot g_i + 1)^{\kappa-3} \cdot \pi_{ik})_{i,k}$. Because $\mathbf{W}_y$ is not a multiple of $\prod_i g_i$, we can obtain multiple $\prod_i g_i$ by taking a ratio of the gcd's of the determinants of The appropriate subsets of $\{\mathbf{W}_1, \ldots, \mathbf{W}_\tau, \mathbf{W}_y\}$:

$$\begin{aligned}&\frac{\gcd(\det \mathbf{W}_1, \ldots, \det \mathbf{W}_n)}{\gcd(\det \mathbf{W}_1, \ldots, \det \mathbf{W}_n, \det \mathbf{W}_y)}\\ &\quad= \frac{\gcd(\prod_i \pi_{i1}, \ldots, \prod_i \pi_{i\tau})}{\gcd(\prod_i \pi_{i1} g_i, \ldots, \prod_i \pi_{i\tau} g_i, \prod_i (r_i g_i + 1))} \cdot \prod_i g_i\\ &\quad= \Delta \cdot \prod_i g_i,\end{aligned}$$

for some integer Δ. We expect that Δ consists of only small factors because it is a common divisor of many random variables. Based on the setting, variables $\prod_i r_{ij}$ are the products of r_{ij} sampled from each uniform distribution. Here, we assume that the probability that a multiple of p is sampled according to a uniform distribution is $\leq 1/p$. Under this assumption, integer Δ is ($2n$-)smooth (i.e., all its divisors are $\leq 2n$) with probability ≥ 0.9, as we explain below. More general results can be found in [12].

Lemma 2. (Heuristic). *Let π_{ij} be an integer described in Sect. 3.1 for $i, j \in [n]$ with $n/(1 + \log n) > s$ for some positive integer s. Then, $\gcd(\prod_i \pi_{i1}, \ldots, \prod_i \pi_{im})$ is ($2n$-)smooth with probability $\geq \zeta(s)^{-1}$, where $\zeta(\cdot)$ is the Riemann zeta function. The probability is ≥ 0.9 when $s \geq 4$.*

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

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

Here, the first inequality comes from $(n/p)^n < 1/p^s$ for $n/(1+\log n) > s$ and $p > 2n$. More precisely, we have $n > s + s\log n > s + s\log n/(\log p/n) = s \log p/(\log p/n)$.

This implies the previous inequality. 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, integer Δ is $(2n)$-smooth with probability > 0.9. We eliminate it by exhaustive division by all the integers, i.e., $\leq 2n$. This costs $\widetilde{\mathcal{O}}(n \log x_0) = \widetilde{\mathcal{O}}(\kappa^3\lambda^5)$ bit operations. This is dominated by the cost of the operations described in Sect. 3.2, which is $\widetilde{\mathcal{O}}(\kappa^{\omega+2}\lambda^{2\omega+3})$.

4.2. *Solving the SubM Problem Over the CLT13*

We explain how to solve the SubM problem using the result of the previous section. As mentioned in Sect. 4.1, we consider $w_{u,v} = \left[\Pi_u \cdot \mathsf{enc}_1(m) \cdot \Pi_v \cdot y^{\kappa-3} \cdot \mathbf{p}_{zt}\right]_{x_0}$ and a matrix $\mathbf{W} = (w_{u,v})_{u,v}$, where $\mathsf{enc}_1(m)$ is a level-1 encoding, $[\mathsf{CRT}_{(p_i)}(r_i \cdot g_i' + m_i)/z]_{x_0}$, which we need to distinguish. Then, matrix $\mathbf{W}$ can be written as

$$\mathbf{W} = \Pi^T \cdot \mathsf{diag}(r_1 \cdot g_1' + m_1, \ldots, r_n \cdot g_n' + m_n) \cdot \Pi',$$

where $\Pi^T = (\pi_{ij})_{i,j}$, $\Pi' = (h_i \cdot g_i \cdot (r_i \cdot g_i + 1)^{\kappa-3} \cdot r_{ik})_{i,k}$. The attack only consists of computing $\gcd(\det \mathbf{W}, \prod_i g_i)$.

If m is uniformly sampled in G, then we expect the probability that m_i is zero for some i is at most $n/2^\alpha$, where α is $\log(g_i)$. Hence, in that case, we have $\alpha n/2^\alpha$ as an expected value of $\log(\gcd(\det \mathbf{W}, \prod_i g_i))$. For the original setting of $\alpha = \lambda$, this is negligible.

If m is uniformly sampled in G', then m_1 is zero, and we expect the probability that the others are zero is $(n-1)/2^\alpha$. Hence, in that case, we have $\log(\gcd(\det \mathbf{W}, \prod_i g_i)) \approx \alpha + \alpha(n - |I|)/2^\alpha$, which is at least larger than $\alpha - 1$. Hence, this value is distinguished from the previous one.

4.3. *Solving the DLIN Problem in CLT13*

As we have seen, we assume that $\prod_i g_i$ is known. In the DLIN problem, we are given a matrix of level-1 encodings $\mathbf{E} = (\mathsf{enc}_1(m^{(i,j)}))_{i,j}$ for $1 \leq i, j \leq L$. We write $\mathsf{enc}_1(m^{(i,j)}) = \mathsf{CRT}(\frac{r_k^{(i,j)} \cdot g_k + m_k^{(i,j)}}{z})$. Using the same method as above, we compute matrices $\mathbf{W}_{i,j} = \mathbf{X}' \cdot \mathsf{diag}(r_1^{(i,j)} \cdot g_1 + m_1^{(i,j)}, \ldots, r_n^{(i,j)} \cdot g_n + m_n^{(i,j)}) \cdot \Pi' \in \mathbb{Z}^{n \times n}$ for all $1 \leq i, j \leq L$. We define

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

Next, we evaluate the determinant of $\mathbf{W}$. It satisfies the following equation:

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

where $\mathbf{D}_{i,j} = \mathsf{diag}(r_1^{(i,j)} \cdot g_1 + m_1^{(i,j)}, \dots, r_n^{(i,j)} \cdot g_n + m_n^{(i,j)})$ for all i, j. For simplicity, let $\Delta = \det(\Pi)^L \cdot \det(\Pi')^L$, $\mathbf{Q}_k = (r_k^{(i,j)} \cdot g_k + m_k^{(i,j)})_{i,j}$, and $\mathbf{P}_k = (m_k^{(i,j)})_{i,j}$. Then, $\det \mathbf{W}$ can be written as $\Delta \cdot \prod_k \det \mathbf{Q}_k$.

To distinguish between 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 a multiple of $\prod_k g_k$. In the other case, then $\det \mathbf{P}_i = 0$ for all i. Hence, $\det \mathbf{W}$ is a multiple of $\prod_k g_k$ because $\mathbf{Q}_k$ is congruent to $\mathbf{P}_k$ in modulo g_k. The total bit-complexity of the attack is $\widetilde{\mathcal{O}}(\kappa^{\omega+2}\lambda^{2\omega+3} + L^{\omega}\kappa^2\lambda^3)$.

4.4. *Solving the GXDH Problem in CLT13*

Without the loss of generality, we assume that $t = 1$ in the GXDH problem. The first step in the attack is to obtain $\prod_i g_i$ from $(\mathsf{params}, p_{zt})$. Similar to Sect. 4.1, we compute $\mathbf{W}_{y^{(1)}}$ and $\mathbf{W}_i$ by using (params) as follows (for $1 \le i \le n$):

$$\begin{aligned} \mathbf{W}_{y^{(1)}} &= ([y^{(1)} \cdot \Pi_u^{(2)} \cdot \Pi_v^{(3)} \cdot y^{(4)} \dots y^{(\kappa)} \cdot p_{zt}]_{x_0})_{u,v} \\ &= (\Pi^{(2)})^T \cdot \mathsf{diag}(r_1^{(1)} \cdot g_1 + 1, \dots, r_n^{(1)} \cdot g_n + 1) \cdot \mathsf{diag}(h_1', \dots, h_n') \cdot \Pi^{(3)}, \\ \mathbf{W}_i &= ([\Pi_i^{(1)} \cdot \Pi_u^{(2)} \cdot \Pi_v^{(3)} \cdot y^{(4)} \dots y^{(\kappa)} \cdot p_{zt}]_{x_0})_{u,v} \\ &= (\Pi^{(2)})^T \cdot \mathsf{diag}(\pi_{i1}^{(1)} \cdot g_1, \dots, \pi_{in}^{(1)} \cdot g_n) \cdot \mathsf{diag}(h_1', \dots, h_n') \cdot \Pi^{(3)}, \end{aligned}$$

where $\Pi^{(2)} = (\pi_{ui}^{(2)})_{u,i}$, $\tilde{h}_i = h_i \cdot g_i \cdot \prod_{k=4}^{\kappa}(r_i^{(k)} \cdot g_i + 1) \cdot \hat{p}_i$, and $\Pi^{(3)} = (\pi_{iv}^{(3)})_{i,v}$.

Similar to Sect. 4.1, we obtain a multiple of $\prod_i g_i$ by taking a ratio of the gcds of the determinants of the appropriate subsets of $\{\mathbf{W}_1, \dots, \mathbf{W}_n, \mathbf{W}_{y^{(1)}}\}$:

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

for some integer Δ. By Lemma 2, integer Δ is $(2n)$-smooth with probability ≥ 0.9. We eliminate it by trial division by all the integers $\le 2n$. Thus, we can obtain $\prod_i g_i$ in complexity time $\widetilde{\mathcal{O}}(\kappa^{\omega+3}\lambda^{2\omega+6})$.

The rest is similar to the DLIN attack in Sect. 4.3. In the GXDH problem, we are given three encodings $\mathsf{enc}_1(a) = \mathsf{CRT}(\frac{r_{ak} \cdot g_k + a_k}{z_1})$, $\mathsf{enc}_1(b) = \mathsf{CRT}(\frac{r_{bk} \cdot g_k + b_k}{z_1})$, and $\mathsf{enc}_1(c) = \mathsf{CRT}(\frac{r_{ck} \cdot g_k + c_k}{z_1})$. Next, we repeat the procedure for the construction of $\mathbf{W}_{y^{(1)}}$ by replacing $y^{(1)}$ with $\mathsf{enc}_1(a)$, $\mathsf{enc}_1(b)$, and $\mathsf{enc}_1(c)$, respectively. Then, we obtain:

$$\begin{aligned} \mathbf{W}_a &= (\Pi^{(2)})^T \cdot \mathsf{diag}(r_{a1} \cdot g_1 + a_1, \dots, r_{an} \cdot g_n + a_n) \cdot \mathsf{diag}(h_1', \dots, h_n') \cdot \Pi^{(3)}, \\ \mathbf{W}_b &= (\Pi^{(2)})^T \cdot \mathsf{diag}(r_{b1} \cdot g_1 + b_1, \dots, r_{bn} \cdot g_n + b_n) \cdot \mathsf{diag}(h_1', \dots, h_n') \cdot \Pi^{(3)}, \\ \mathbf{W}_c &= (\Pi^{(2)})^T \cdot \mathsf{diag}(r_{c1} \cdot g_1 + c_1, \dots, r_{cn} \cdot g_n + c_n) \cdot \mathsf{diag}(h_1', \dots, h_n') \cdot \Pi^{(3)}. \end{aligned}$$

As the last step, we compute:

$$\mathbf{W} = \begin{pmatrix} \mathbf{W}_c & \mathbf{W}_a \\ \mathbf{W}_b & \mathbf{W}_{y^{(1)}} \end{pmatrix} \in \mathbb{Z}^{2n \times 2n} \quad \text{and}$$

$$\det \mathbf{W} = \Delta' \cdot \prod_i \Big((r_{ai} \cdot g_i + a_i) \cdot (r_{bi} \cdot g_i + b_i) - (r_{ci} \cdot g_i + c_i) \cdot (r_i^{(1)} \cdot g_i + 1) \Big),$$

where $\Delta' = \det(\Pi^{(2)})^2 \cdot \det(\Pi^{(3)})^2 \cdot (\prod_i h'_i)^2$. 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 of $\prod_i g_i$. The cost of the attack is also bounded by $\widetilde{\mathcal{O}}(\kappa^{\omega+2}\lambda^{2\omega+3})$.

5. Conclusion

This study exhibits a method to recover in polynomial time all the secret values in the CLT13 scheme with a low-level encoding of zero. In addition, we propose a direct algorithm to solve the problems associated with the CLT13 scheme. Consequently, several applications of the CLT13 scheme are impacted.

Because the security of the general-purpose obfuscation schemes in the CLT13 scheme has not been yet clarified, a natural line of research is to extend the range of the attackable graded encoding schemes for the application.

In addition, as a main technique for solving the CLT13 scheme, we introduce a new problem CRT-ACD with an auxiliary input. Independently, solving the CRT-ACD problem is still an open problem. Hence, studying the relation between the two problems will also be an interesting topic.

Acknowledgements

The authors would like to extend their gratitude to 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 Institute for Information & communication Technology Promotion (IITP) grant funded by the Korea government (No. 2016-6-00598, The mathematical structure of functional encryption and its analysis) and supported by the ARO and DARPA under Contract No. W911NF-15-C-0227. The author from ENS de Lyon was supported by the ERC Starting Grant ERC-2013-StG-335086-LATTAC.

References

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

[2] P.V. Ananth, D. Gupta, Y. Ishai, A. Sahai, Optimizing obfuscation: Avoiding barrington's theorem, in *Proceedings of the 2014 ACM SIGSAC* (2014), pp. 646–658

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

[4] S. Badrinarayanan, E. Miles, A. Sahai, M. Zhandry, Post-zeroizing obfuscation: New mathematical tools, and the case of evasive circuits, in *Advances in Cryptology—EUROCRYPT 2016* (2016), pp. 764–791

[5] F. Benhamouda, D. Pointcheval, Verifier-based password-authenticated key exchange: New models and constructions. *IACR Cryptol. ePrint Arch.* **2013**, 833 (2013)

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

[7] D. Boneh, A. Silverberg, Applications of multilinear forms to cryptography. *Contemp. Math. Am. Math. Soc.* **324**, 71–90 (2003)

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

[9] J.H. Cheon, J. Coron, J. Kim, M.S. Lee, T. Lepoint, M. Tibouchi, A. Yun, Batch fully homomorphic encryption over the integers, in *Advances in Cryptology—EUROCRYPT 2013* (2013), pp. 315–335

[10] J.H. Cheon, P. Fouque, C. Lee, B. Minaud, H. Ryu, Cryptanalysis of the new CLT multilinear map over the integers, in *Advances in Cryptology—EUROCRYPT 2016* (2016), pp. 509–536

[11] J.H. Cheon, K. Han, C. Lee, H. Ryu, D. Stehlé, Cryptanalysis of the multilinear map over the integers, in *Advances in Cryptology—EUROCRYPT 2015* (2015), pp. 3–12

[12] J.H. Cheon, D. Kim, Probability that the k-gcd of products of positive integers is b-friable. *J. Number Theory* **168**, 72–80 (2016)

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

[14] J. Coron, M.S. Lee, T. Lepoint, M. Tibouchi, Zeroizing attacks on indistinguishability obfuscation over CLT13, in *Public-Key Cryptography—PKC 2017* (2017), pp. 41–58

[15] J. Coron, T. Lepoint, M. Tibouchi, Practical multilinear maps over the integers, in *Advances in Cryptology—CRYPTO 2013* (2013), pp. 476–493

[16] J. Coron, T. Lepoint, M. Tibouchi, Cryptanalysis of two candidate fixes of multilinear maps over the integers. *IACR Cryptol. ePrint Arch.* **2014**, 975 (2014)

[17] J. Coron, T. Lepoint, M. Tibouchi, New multilinear maps over the integers, in *Advances in Cryptology—CRYPTO 2015* (2015), pp. 267–286

[18] R. Fernando, P.M.R. Rasmussen, A. Sahai, Preventing CLT attacks on obfuscation with linear overhead, in *Advances in Cryptology—ASIACRYPT 2017* (2017), pp. 242–271

[19] S.D. Galbraith, S.W. Gebregiyorgis, S. Murphy, Algorithms for the approximate common divisor problem. *LMS J. Comput. Math.* **19**(A), 58–72 (2016)

[20] S. Garg, C. Gentry, S. Halevi, Candidate multilinear maps from ideal lattices. in *Advances in Cryptology—EUROCRYPT 2013* (2013), pp. 1–17

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

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

[23] S. Garg, C. Gentry, S. Halevi, M. Zhandry, Fully secure functional encryption without obfuscation. *IACR Cryptology ePrint Archive* (2014)

[24] S. Garg, C. Gentry, S. Halevi, M. Zhandry. Functional encryption without obfuscation, in *Theory of Cryptography—13th International Conference, TCC 2016-A* (2016), pp. 480–511

[25] C. Gentry, A.B. Lewko, A. Sahai, B. Waters. Indistinguishability obfuscation from the multilinear subgroup elimination assumption. in *Proceedings of FOCS 2015* (2015), pp. 151–170

[26] C. Gentry, A.B. Lewko, B. Waters, Witness encryption from instance independent assumptions, in *Advances in Cryptology—CRYPTO 2014* (2014), pp. 426–443

[27] N. Howgrave-Graham, Approximate integer common divisors, in *Cryptography and Lattices, International Conference, CaLC 2001, Providence, RI, USA, March 29–30, 2001, Revised Papers* (2001), pp. 51–66

[28] Y. Hu, H. Jia, Cryptanalysis of GGH map, in *Advances in Cryptology—EUROCRYPT 2016* (2016), pp. 537–565

[29] H.T. Lee, J.H. Seo, Security analysis of multilinear maps over the integers, in *Advances in Cryptology—CRYPTO 2014* (2014), pp. 224–240

[30] K. Lewi, H.W. Montgomery, A. Raghunathan, Improved constructions of prfs secure against related-key attacks, in *Applied Cryptography and Network Security* (2014), pp. 44–61

[31] G. Martin, E.B. Wong, Almost all integer matrices have no integer eigenvalues. *Am. Math. Mon.* **116**(7), 588–597 (2009)

[32] E. Miles, A. Sahai, M. Weiss, Protecting obfuscation against arithmetic attacks. *IACR Cryptol. ePrint Arch.*, **2014**, 878 (2014)

[33] R. Pass, K. Seth, S. Telang, Indistinguishability obfuscation from semantically-secure multilinear encodings, in *Advances in Cryptology—CRYPTO 2014* (2014), pp. 500–517

[34] M.O. Rabin, Probabilistic algorithms in finite fields. *SIAM J. Comput.* **9**(2), 273–280 (1980)

[35] M. van Dijk, C. Gentry, S. Halevi, V. Vaikuntanathan, Fully homomorphic encryption over the integers, in *Advances in Cryptology—EUROCRYPT 2010* (2010), pp. 24–43

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

[37] J. Zimmerman, How to obfuscate programs directly, in *Advances in Cryptology—EUROCRYPT 2015* (2015), pp. 439–467

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.