A New Algorithm for the CRT-ACD Problem

No Author Given

No Institute Given

Abstract. The CRT-ACD problem is defined as follows: Let a CRT-ACD instance be an integer congruent to a ρ-bit integer modulo each η-bit prime p_j. For given polynomially many CRT-ACD instances and a known integer $N = \prod_{j=1}^{n} p_j$, find a prime integer p_j.

Recently, Cheon *et al.* suggested a polynomial time algorithm to recover all secret parameters of the CLT13 multilinear map by introducing a technique to solve the CRT-ACD problem when given $\sum_{j=1}^{n} d_j \cdot (N/p_j)$ with sufficiently small d_j's which is so called a *dual CRT-ACD* instance. However, it is not applicable to the case that a dual instance $\sum_{j=1}^{n} d_j \cdot (N/p_j)$ is not provided or cannot be easily computed as in the CLT13 multilinear map without low level encodings of zero, whose cryptanalysis remains as an open problem for years.

In this paper, we present an algorithm to solve the CRT-ACD problem. Our algorithm takes polynomial time in n and η using LLL algorithm under the condition $n \leq \eta - 4\rho - O(\log n)$ assuming Gaussian Heuristics. Furthermore, when using BKZ algorithm with block size β instead of LLL, it can be solved in $2^{O(\beta)}$ if $n \leq \frac{\beta-1}{2\log\beta}(\eta - 4\rho - O(\log n))$.

As a consequence, our algorithm reveals a factor of base modulus of the CLT13 multilinear map without low level encodings of zero in subexponential time when $n = (\eta - 6\rho) \cdot O(\lambda^{1-\epsilon})$ for any $\epsilon > 0$, where λ is the security parameter. In other words, we suggest the first guideline to set n for the CLT multilinear map for indistinguishability obfuscator as $n = \Omega(\eta\lambda)$, which agrees to suggested parameters of CLT13 with low level encodings of zero.

Keywords: CRT-ACD; Dual Instance; Cryptanalysis; Multilinear maps

1 Introduction

For given positive integers n, η and ρ, let $\{p_j\}_{1\leq j\leq n}$ be unknown η-bit primes and $\{r_j\}_{1\leq j\leq n}$ be ρ-bit integers. An integer in $\left(-\frac{1}{2}\prod_{j=1}^{n} p_j, \frac{1}{2}\prod_{j=1}^{n} p_j\right]$ congruent to r_j in the modulo each p_j is called a CRT-ACD instance and denoted by $\mathsf{CRT}_{(p_j)}(r_j)$. The CRT-ACD problem is to find a prime integer p_j for some $1 \leq j \leq n$ given polynomially many CRT-ACD instances.

The CRT-ACD problem was first proposed by Cheon *et al.* [6] to make a batch fully homomorphic encryption scheme over integers. Later, Coron *et al.* suggested a candidate of multilinear map, called the CLT13 multilinear map, using a variant of the CRT-ACD problem [10]. Recently, CLT13 multilinear map is used as a base of indistinguishability obfuscation and its numerous applications. [1, 3–5, 8, 9, 15–18, 21, 22, 24–26].

In 2015, Cheon *et al.* prove that the CLT13 multilinear map scheme can be solved in polynomial time when low level encodings of zero are given. They first compute so called a *dual CRT-ACD* instance $\sum_{j=1}^{n} d_j \cdot (N/p_j)$ for small d_j by multiplying the zerotesting parameter, low level encodings of zero and other parameters. [7]. However, for the CLT13 multilinear map without low level encodings of zero, there is no known efficient algorithm.

Our Contribution. In this work, we propose a novel algorithm to solve the CRT-ACD problem. The algorithm first generates *dual CRT-ACD* instances, and then exploits them to solve CRT-ACD by combining with the previous work. Under the Gaussian Heuristics, our algorithm generates dual instances by using LLL algorithm in polynomial time of n and η under the condition $n \leq \eta - 4\rho - O(\log n)$. When using BKZ algorithm with a block size β, one can solve the problem in the time complexity $2^{O(\beta)}$ under $n \leq \frac{\beta-1}{2\log\beta}(\eta - 4\rho - O(\log n))$. Our algorithm can be applied to the CLT13 multilinear map without low level encodings of zero. Indeed, one can recover the all secret parameters of the CLT13 multilinear map without using low level encodings of zero under the condition $n \leq \eta - 6\rho - O(\log n)$. On employing BKZ algorithm as above, we can cryptanalyze it in $2^{O(\beta)}$ time under the condition $n \leq \frac{\beta-1}{2\log\beta}(\eta - 6\rho - O(\log n))$. Hence, n has to be set as $(\eta - 6\rho) \cdot \Omega(\lambda)$ which matches the condition of CLT13 multilinear map with low level encodings of zero. Finally, we provide experimental results to support our CRT-ACD analysis.

Idea of the Attack. We briefly sketch how to generate a dual CRT-ACD instance, $\sum_{j=1}^{n} d_j \cdot N/p_j$, from only CRT-ACD instances. We observe that any element in $\mathbb{Z}_N$ can be written as a summation $A = \sum_{j=1}^{n} a_j \cdot \hat{p}_j$ for some integer $a_j's$, where $\hat{p}_j = N/p_j$. By multiplying it to given CRT-ACD instances $b_i = \mathsf{CRT}_{(p_j)}(r_{j,i})$, we obtain elements of the form $[\sum\limits_{j=1}^{n} r_{j,i} \cdot a_j \cdot \hat{p}_j]_N$. When the size of a_j is small enough for all $j's$, the quantity equals to $\sum\limits_{j=1}^{n} r_{j,i} \cdot a_j \cdot \hat{p}_j$ which is also small.

To exploit this property, consider the column lattice $\mathcal{L}$ generated by the following $(k+1) \times (k+1)$ matrix $\mathbf{B}$:

$$\mathbf{B} = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ b_1 & N & 0 & \cdots & 0 \\ b_2 & 0 & N & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b_k & 0 & 0 & \cdots & N \end{pmatrix}.$$

From the fact that $[A \cdot b_j]_N$ is small, $(A, [A \cdot b_1]_N, \cdots, [A \cdot b_k]_N)$ becomes a short vector in a lattice $\mathcal{L}$.

One can use a lattice reduction algorithm such as LLL or BKZ algorithm [19, 23] to find such a vector $([d = \sum_{j=1}^{n} d_j \cdot \hat{p}_j]_N, [d \cdot b_1]_N, \cdots, [d \cdot b_k]_N) \in \mathcal{L}$. We want to show that d is a dual $\mathsf{CRT\text{-}ACD}$ instance. In order to guarantee this, first, we express $[d \cdot b_i]_N$ as a linear combination of $[d_j \cdot \hat{p}_j]_N$ and $r_{j,i}$. *i.e.*, $[d \cdot b_i]_N = \sum_{j=1}^{n} d_j \cdot \hat{p}_j \cdot r_{j,i}$. Then, on utilizing many $\mathsf{CRT\text{-}ACD}$ instances b_i, one can generate a vector $\mathbf{c} = ([d]_N, [d \cdot b_1]_N, \cdots, [d \cdot b_k]_N)$ with $d = \sum_{j=1}^{n} d_j \cdot \hat{p}_j$. Then,

$$\tilde{\mathbf{c}} \equiv \mathbf{d} \cdot \hat{\mathbf{P}} \cdot \mathbf{R} \mod N,$$

where $\mathbf{d} = (d_1, \cdots, d_n)$, $\hat{\mathbf{P}} = \mathsf{diag}(\hat{p}_1, \ldots, \hat{p}_n)$ and $\mathbf{R} = (r_{j,i})$ is a $n \times k$ matrix. Assume that we can find a matrix $\mathbf{R}^*$ such that $\tilde{\mathbf{c}} \cdot \mathbf{R}^* \equiv \mathbf{d} \cdot \hat{\mathbf{P}} \mod N$ and $\|\mathbf{R}^*\|_\infty$ is small. By the lattice reduction algorithm, one can calculate an upper bound of $\|\tilde{\mathbf{c}}\|_2$, we can restrict the size of $d_j \cdot \hat{p}_j$. So, we can ensure that d is a dual $\mathsf{CRT\text{-}ACD}$ instance with overwhelming probability when $n \leq \eta - 6\rho - O(\log n)$. The more details are described in Section 3.1 and 3.3.

Organization. In Section 2, we introduce preliminary information related to the $\mathsf{CRT\text{-}ACD}$ problem and explain a previous algorithm to solve the $\mathsf{CRT\text{-}ACD}$ problem with a dual $\mathsf{CRT\text{-}ACD}$ instance, briefly. Also we describe how to obtain a dual instance for the $\mathsf{CRT\text{-}ACD}$ problem and a variant of the $\mathsf{CRT\text{-}ACD}$ problem throughout the Section 3. In addition, we present some experimental results in Section 4. Finally, summary of our work and remained problem are presented in Section 5, as a conclusion.

2 Preliminaries

Notation. Throughout this paper, we use the notation $a \leftarrow \mathcal{D}$ to denote the choice of an element a according to the distribution of $\mathcal{D}$. For integers t and $p > 0$, we let $[t]_p$ denote the integer in $(-p/2, p/2]$ satisfying $[t]_p \equiv t \mod p$. In general, we define $\mathsf{CRT}_{(p_1, p_2, \ldots, p_n)}(r_1, r_2, \ldots, r_n)$ (or abbreviated as $\mathsf{CRT}_{(p_j)}(r_j)$) for distinct primes $p_1, p_2, \ldots, p_n$ as the integer in $\left(-\frac{1}{2}\prod_{j=1}^{n} p_j, \frac{1}{2}\prod_{j=1}^{n} p_j\right]$ congruent to r_j in the modulus p_j for all $j \in \{1, 2, \cdots, n\}$. We use bold letters to denote vectors or matrices. We denote the set of all $m \times n$ matrices by $M_{m \times n}(\mathbb{Z})$. For any matrix $\mathbf{A}$, we denote the transpose of $\mathbf{A}$ by $\mathbf{A}^T$. We let $[\mathbf{A}]_j$ denote the j-th row vector of $\mathbf{A}$. The logarithm of the maximal absolute values of all entries is denoted $size(\mathbf{A})$. When $a_{i,j}$ is the (i,j)-entry of the $n \times m$ matrix $\mathbf{A}$, we define the infinite norm $\|\mathbf{A}\|_\infty$ as $\max_{1 \leq j \leq m} \sum_{i=1}^{n} |a_{i,j}|$. We denoted by $\mathsf{diag}(a_1, \ldots, a_n)$ the diagonal matrix with diagonal coefficients $a_1, \ldots, a_n$. $\mathbf{A} \mod N$ for an integer N denote the matrix whose (i,j)-entry is $[a_{i,j}]_N$. For a vector $\mathbf{v} = (v_1, \cdots, v_n)$, we define the ℓ_2-norm $\|\mathbf{v}\|_2$ and ℓ_1-norm $\|\mathbf{v}\|_1$ as $\sqrt{\sum_{j=1}^{n} {v_j}^2}$ and $\sum_{j=1}^{n} |v_j|$, respectively.

2.1 Lattice

In this subsection, we introduce some backgrounds about lattices.

Lattice A lattice $\mathcal{L} \subset \mathbb{R}^n$ is the set of all integer linear combinations of basis vectors $\mathbf{b}_1, \mathbf{b}_2, \cdots, \mathbf{b}_n \in \mathbb{R}^n$, *i.e.*, $\mathcal{L} = \{\ \sum_{j=1}^{n} z_j \mathbf{b}_j \mid z_j \in \mathbb{Z} \ \ \forall j\ \}$.

Successive Minima Let $\mathcal{L}$ be a lattice of rank n. Then the successive minima $\lambda_1, \cdots, \lambda_n \in \mathbb{R}^+$ of $\mathcal{L}$ are defined as follows: for any $1 \le j \le n$, λ_j is the minimum such that there exist j linearly independent vectors in $\mathcal{L}$ whose size is not exceeding λ_j. We use $\lambda_j(\mathcal{L})$ to denote the j-th successive minimum of the lattice $\mathcal{L}$.

In relation to the successive minima, there is an useful result to restrict them, which is called the Gaussian Heuristic [2].

Gaussian Heuristic Let $\mathcal{L}$ be an n-rank lattice. The size of successive minima of $\mathcal{L}$ is asymptotically as follows:

$$\lambda_j(\mathcal{L}) \sim \sqrt{\frac{n}{2\pi e}} \det(\mathcal{L})^{1/n} \quad \text{for all} \quad j \in \{1, 2, \cdots, n\}$$

Ajtai showed that the above equation is valid for a random lattice with overwhelming probability [2].

Finding a short vector of a lattice is essential in our attack. There are some algorithms to find a short vector of a lattice, called lattice reduction algorithms.

Lattice Reduction Algorithm The LLL algorithm and the BKZ algorithm, introduced in [12, 19], are typical lattice reduction algorithms. We mainly use these algorithms to find an approximately short vector of a lattice. According to [12], the LLL algorithm upon the n-rank lattice $\mathcal{L}$ with basis matrix $\mathbf{B}$ gives a short vector $\mathbf{v}$, which satisfies the following:

$$\|\mathbf{v}\|_2 \le \min\{2^{\frac{n-1}{4}} \cdot (\det \mathcal{L})^{\frac{1}{n}}, 2^{\frac{n-1}{2}} \cdot (\lambda_1(\mathcal{L}))\}.$$

We denote the time complexity of the LLL algorithm as $T_L(n, size(\mathbf{B}))$, which is a polynomial function on inputs.

In case of the BKZ algorithm, according to [19], the block size β of the BKZ algorithm determines how short the output of the BKZ algorithm is. With the BKZ algorithm to the n-rank lattice $\mathcal{L}$ with basis $\mathbf{B}$, we can get a short vector $\mathbf{v}$ in $poly(n, size(\mathbf{B})) \cdot C_{HKZ}(\beta)$ time which satisfies the following:

$$\|\mathbf{v}\|_2 \le \min\{2 \cdot \gamma_\beta^{\frac{n-1}{2(\beta-1)}+\frac{3}{2}} \cdot (\det \mathcal{L})^{\frac{1}{n}}, 4 \cdot \gamma_\beta^{\frac{n-1}{\beta-1}+3} \cdot (\lambda_1(\mathcal{L}))\}$$

where γ_β is the Hermite constant of rank β not exceeding β, and $C_{HKZ}(\beta)$ denotes the time spent to get the shortest vector of β-dimensional lattice and can be regarded as $2^{O(\beta)}$.

2.2 Cryptanalysis on the CRT-ACD with Dual Instances

The Approximate Common Divisor problem (ACD), initially introduced by Howgrave-Graham [20], is a problem to find a prime p for given many instances which are nearly multiples of p. With multiple primes rather than a single one, one can extend the ACD problem by setting an instance of the problem as the form $p_j \cdot q_j + r_j$ for each prime p_j. In this case, it is able to define the instance with Chinese Remainder Theorem (CRT), which is named as the CRT-ACD problem. Cheon *et al.* described an analysis of the CRT-ACD problem with a dual instance [7]. In this section, we introduce briefly how they analyze it.

Definition 1. (CRT-ACD) *Let n, η, ρ be positive integers and χ_ρ be an uniform distribution over $\mathbb{Z} \cap (-2^\rho, 2^\rho)$. For given η-bit primes $p_1, \cdots, p_n$, the sampleable* CRT-ACD *distribution $\mathcal{D}_{\chi_\rho,\eta,n}(p_1, \cdots, p_n)$ is defined as*

$$\mathcal{D}_{\chi_\rho,\eta,n}(p_1, \cdots, p_n) = \{\mathsf{CRT}_{(p_j)}(r_j) \mid r_j \leftarrow \chi_\rho\},$$

where $\mathsf{CRT}_{(p_j)}(r_j)$ is the integer in $\left(-\frac{1}{2}\prod_{j=1}^n p_j, \frac{1}{2}\prod_{j=1}^n p_j\right]$ congruent to r_j in the modulus p_j for all $j \in \{1, 2, \cdots, n\}$. The CRT-ACD *problem is: for given polynomially many samples from $\mathcal{D}_{\chi_\rho,\eta,n}(p_1, \cdots, p_n)$ and $N = \prod\limits_{j=1}^{n} p_j$, find a nontrivial factor of N.*

Definition 2. (Dual CRT-ACD Instance[1]) *Let n, η, ρ be positive integers. For given η bit primes $p_1, \cdots, p_n$, define $N = \prod_{j=1}^n p_j$ and $\hat{p}_j = N/p_j$, for $1 \le j \le n$. We define $(n, \eta, \rho, (\epsilon_j)_j)$-*Dual CRT-ACD Instance *as an integer of the form $\mathsf{CRT}_{(p_j)}(a_j \cdot \hat{p}_j)$ with $|d_j| \le \epsilon_j$ for all j's.*

For proper parameters, the CRT-ACD problems are regarded to be hard. However, it is known that one can solve the CRT-ACD problem in polynomial time of n, η and ρ when $(n, \eta, \rho, (\epsilon_j)_j)$-Dual CRT-ACD Instances are given. Now we define the CRT-ACD problem with an $(n, \eta, \rho, (\epsilon_j)_j)$-Dual CRT-ACD Instance (CRT-ACDwDI) by importing Definition 1 and introduce briefly about Cheon *et al.*'s method to solve it.

Definition 3. (CRT-ACDwDI) *Let n, η, ρ be positive integers. For given η bit primes $p_1, \cdots, p_n$, define $N = \prod_{j=1}^n p_j$ and $\hat{p}_j = N/p_j$, for $1 \le j \le n$.*
*The $(n, \eta, \rho, (\epsilon_j)_j)$-*CRT-ACDwDI *problem is: for given polynomially many samples from $\mathcal{D}_{\chi_\rho,\eta,n}(p_1, \cdots, p_n)$, N and an $(n, \eta, \rho, (\epsilon_j)_j)$-*Dual CRT-ACD Instance*, find a prime factor p_i.*

When $\sum\limits_{j=1}^{n} \hat{p}_j$ is less than $N/2$, one can see that for the dual instance $\hat{P} = \mathsf{CRT}_{(p_j)}(\hat{p}_j)$, $\hat{P} = \sum\limits_{j=1}^{n} \hat{p}_j$ holds. We state the following lemma described in [7] that works on a similar principle.

[1] In [7], $\hat{P} = \mathsf{CRT}_{(p_j)}(\hat{p}_j)$ was introduced as an auxiliary input. In this paper, we generalize this to an $(n, \eta, \rho, (\epsilon_j)_j)$-Dual CRT-ACD Instance.

Lemma 1. *(Adapted from [7], Section 3.1) For a given* $\hat{P} = \mathsf{CRT}_{(p_j)}(\hat{p}_j)$ *and* $r = \mathsf{CRT}_{(p_j)}(r_j) \leftarrow \mathcal{D}_{\chi_\rho,\eta,n}(p_1,\cdots,p_n)$*, it satisfies:*

$$[r \cdot \hat{P}]_N = \mathsf{CRT}_{(p_j)}(r_j \cdot \hat{p}_j) = \sum_{j=1}^{n} r_j \cdot \hat{p}_j$$

if $\log n < \eta - \rho - 2$.

Proof. The first equality is obvious due to the definition of the Chinese remainder theorem. To show that the second equality is correct, consider the equation modulo p_i for each j. Then the left hand side is $r_j \cdot \hat{p}_j$ and the right hand side is also $r_j \cdot \hat{p}_j$, because $\hat{p}_i \equiv 0 \bmod p_j$ holds for $i \neq j$. Finally, we can get the following inequalities:

$$|\sum_{j=1}^{n} r_j \cdot \hat{p}_j| \leq \sum_{j=1}^{n} |r_j| \cdot \frac{N}{p_j} \leq n \cdot 2^\rho \cdot \frac{N}{2^{\eta-1}} = N \cdot 2^{-\eta+\rho+\log n+1}$$

We can check that $N \cdot 2^{-\eta+\rho+\log n+1}$ is less than $N/2$ under the condition $\log n < \eta - \rho - 2$. Hence, by the uniqueness of CRT, the second equality holds. □

The main idea of Cheon *et al.*'s algorithm to solve the $\mathsf{CRT\text{-}ACD}$ problem with $\hat{P} = \mathsf{CRT}_{(p_j)}(\hat{p}_j)$ is to use this lemma to transform the modulus equation to an integer equation of $r_1, \cdots, r_n$ with unknown coefficients $\hat{p}_1, \cdots, \hat{p}_n$. By restoring r_j's from those integer equations, one can compute all p_j's and obtain the following:

Theorem 1. *(Adapted from [7], Section 3.2) Let* χ_ρ *be the uniform distribution over* $(-2^\rho, 2^\rho) \cap \mathbb{Z}$*. When* n, η *and* ρ *satisfy* $\log n < \eta - 3\rho - 2$ *and given* $O(n)$ $\mathsf{CRT\text{-}ACD}$ *samples from* $\mathcal{D}_{\chi_\rho,\eta,n}(p_1,\cdots,p_n)$ *with* $N = \prod_{j=1}^{n} p_j$ *and* $\hat{P} = \mathsf{CRT}_{(p_j)}(\hat{p}_j)$*, one can recover every secret primes* $p_1, \cdots, p_n$ *in time* $\widetilde{\mathcal{O}}(n^{2+\omega} \cdot \eta)$ *with* $\omega \leq 2.38$ *and overwhelming probability to* ρ*.*

Remark. Generally, with the same argument above, the $(n, \eta, \rho, (\epsilon_j)_j)$-$\mathsf{CRT\text{-}ACDwDI}$ problem can be solved with the $(n, \eta, \rho, (\epsilon_j)_j)$-$\mathsf{Dual\ CRT\text{-}ACD\ Instance}$ of the form $\hat{P} = \mathsf{CRT}_{(p_j)}(d_j \cdot \hat{p}_j)$ for $\epsilon_j \cdot \hat{p}_j \leq N \cdot 2^{-2\rho-\log n-1}$ since the following still holds:

$$[b_u \cdot b_v \cdot \hat{P}]_N = \sum_{j=1}^{n} d_j \cdot r_{j,u} \cdot r_{j,v} \cdot \hat{p}_j \quad \text{for } \mathsf{CRT\text{-}ACD} \text{ instances } b_u, b_v.$$

In the algorithm of Cheon *et al.*, since the equality $[b_u \cdot b_v \cdot b_w \cdot \hat{P}]_N = \sum_{j=1}^{n} d_j \cdot r_{j,u} \cdot r_{j,v} \cdot r_{j,w} \cdot \hat{p}_j$ has to be satisfied, the required condition for ϵ_j is $\epsilon_j \leq N \cdot 2^{-3\rho-\log n-1}/\hat{p}_j$ for each j. However, we will show in Section 3.1 that by using two different $(n, \eta, \rho, (\epsilon_j)_j)$-$\mathsf{Dual\ CRT\text{-}ACD\ Instances}$, it suffices to satisfy

$[b_u \cdot b_v \cdot \hat{P}]_N = \sum_{j=1}^{n} d_j \cdot r_{j,u} \cdot r_{j,v} \cdot \hat{p}_j$ for each $(n, \eta, \rho, (\epsilon_j)_j)$-Dual CRT-ACD Instances $\hat{P}$. Therefore, we let the $(n, \eta, \rho, (\epsilon_j)_j)$-Dual CRT-ACD Instance and $(n, \eta, \rho, (\epsilon_j)_j)$-CRT-ACDwDI abbreviate as the dual instance and CRT-ACDwDI respectively when ϵ_j is less than $N \cdot 2^{-2\rho - \log n - 1}/\hat{p}_j$.

3 Main algorithm for the CRT-ACD problem

We describe how to obtain a dual CRT-ACD instance in Section 3.1. Then, we explain how to solve the CRT-ACD problem by using the obtained dual instance in Section 3.2. Also, we define a new problem, the Scaled CRT-ACD problem and describe how to solve the problem. In Section 3.4, we describe how the algorithm for Scaled CRT-ACD is applied to CLT13 multilinear map.

3.1 Generating a dual instance for the CRT-ACD problem

In this section, we prove that it is able to generate a dual instance from CRT-ACD instances. Consider the column lattice $\mathcal{L}$ whose basis matrix is as follows:

$$\mathbf{B} = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ b_1 & N & 0 & \cdots & 0 \\ b_2 & 0 & N & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b_k & 0 & 0 & \cdots & N \end{pmatrix}.$$

where b_i's are the given CRT-ACD instances.

The vector $\mathbf{c}$ in $\mathcal{L}$ with $\|\mathbf{c}\|_2 \leq N/2$ can be written as the form of $([A]_N, [A \cdot b_1]_N, \cdots, [A \cdot b_k]_N)^T$, where $A = \sum_{j=1}^{n} a_j \cdot \hat{p}_j$ for some a_j's. If A is a proper dual instance so that each $[A \cdot b_i]_N$ is sufficiently small, $\mathbf{c}$ would be a short vector in $\mathcal{L}$. Hence, we use the lattice reduction algorithm upon the lattice $\mathcal{L}$ to find a dual instance. Indeed, we can obtain a dual instance A under the condition described in the following theorem.

Theorem 2. *Let n, η, ρ be parameters of* CRT-ACD*. When $2n$* CRT-ACD *instances are given, we can find a dual instance for given* CRT-ACD *instances under the condition $n \leq \eta - 4\rho - \frac{9}{2}\log n - 1$ in $T_L(n, n \cdot \eta)$ time with the LLL algorithm. In other words, it is able to reduce* CRT-ACD *to* CRT-ACDwDI.

Proof. Assume there are $k(\geq n)$ number of CRT-ACD instances $b_i = \mathsf{CRT}_{(p_j)}(r_{j,i})$. Let $\mathbf{c} = (c_0, c_1, \cdots, c_k)^T$ be a vector in $\mathcal{L}$. Then, $\mathbf{c}$ has the following form:

$$\mathbf{c} = ([d]_N, [d \cdot b_1]_N, \cdots, [d \cdot b_k]_N)^T \quad \text{with} \quad d = \sum_{j=1}^{n} d_j \cdot \hat{p}_j.$$

Let $\tilde{\mathbf{c}}$ be the vector $(c_1, \cdots, c_k)$. Since $c_i \equiv \sum_{j=1}^{n} r_{j,i} \cdot d_j \cdot \hat{p}_j \bmod N$ holds for each i, $\tilde{\mathbf{c}}$ can be decomposed as follows:

$$\tilde{\mathbf{c}} \equiv \mathbf{d} \cdot \hat{\mathbf{P}} \cdot \mathbf{R} \mod N,$$

where $\mathbf{d} = (d_1, \cdots, d_n),\ \hat{\mathbf{P}} = \mathsf{diag}(\hat{p}_1, \ldots, \hat{p}_n),$ and $\mathbf{R} = (r_{j,i}) \in M_{n\times k}(\mathbb{Z})$.

For the matrix $\mathbf{R}$, suppose we obtain a right inverse $\mathbf{R}^* \in M_{k\times n}(\mathbb{Z})$ so that the followings hold:

$$\mathbf{R} \cdot \mathbf{R}^* = \mathbf{I}_n \quad \text{and} \quad \mathbf{d} \cdot \hat{\mathbf{P}} \cdot \mathbf{R} \cdot \mathbf{R}^* = (d_1 \cdot \hat{p}_1, d_2 \cdot \hat{p}_2, \cdots, d_n \cdot \hat{p}_n).$$

where $\mathbf{I}_n$ is the $n \times n$ identity matrix. Then, we can restrict the size of $d_i \cdot \hat{p}_i$'s as follows:

$$\|\mathbf{d} \cdot \hat{\mathbf{P}} \cdot \mathbf{R} \cdot \mathbf{R}^* \bmod N\|_\infty = \|\tilde{\mathbf{c}} \cdot \mathbf{R}^* \bmod N\|_\infty \le \|\tilde{\mathbf{c}} \cdot \mathbf{R}^*\|_\infty \le \|\tilde{\mathbf{c}}\|_2 \cdot \|\mathbf{R}^*\|_\infty.$$

Our goal is to find proper $\tilde{\mathbf{c}}$ and $\mathbf{R}^*$ which satisfy $\|\tilde{\mathbf{c}}\|_2 \cdot \|\mathbf{R}^*\|_\infty \le N \cdot 2^{-2\rho - \log n - 1}$. If so, it implies the follows:

$$\|\mathbf{d} \cdot \hat{\mathbf{P}} \cdot \mathbf{R} \cdot \mathbf{R}^* \bmod N\|_\infty \le N \cdot 2^{-2\rho - \log n - 1},$$

$$\textit{i.e.,} \quad |[d_j \cdot \hat{p}_j]_N| = |[d_j]_{p_j}| \cdot \hat{p}_j \le N \cdot 2^{-2\rho - \log n - 1} \text{ for each } j.$$

From the above condition, $[d]_N = [\sum_{j=1}^{n} d_j \cdot \hat{p}_j]_N = \sum_{j=1}^{n} [d_j]_{p_j} \cdot \hat{p}_j$ holds and it would be the dual instance for $\mathsf{CRT\text{-}ACD}$. Therefore, $c_0 = [d]_N$ is exactly $\sum_{j=1}^{n} [d_j]_{p_j} \cdot \hat{p}_j$ with $|[d_j]_{p_j}| \le N \cdot 2^{-2\rho - \log n - 1}/\hat{p}_j$ and we can regard c_0 as a dual instance of $\mathsf{CRT\text{-}ACD}$.

From now on, we let k be $2n$ for simplicity. We describe the value of k for the optimal condition to find a dual instance in Appendix.

Construction of $\mathbf{R}^*$ We can construct the matrix $\mathbf{R}^*$ and estimate the size of $\|\mathbf{R}^*\|_\infty$ using Babai's nearest algorithm and Gaussian heuristic assumption. More precisely, let q be a prime integer and $\mathbf{v}_1$ be any vector with $\mathbf{R} \cdot \mathbf{v}_1 \equiv \mathbf{e}_1 \bmod q$, where $\mathbf{e}_1$ is a standard vector. Consider a lattice $\mathit{\Lambda} = \{\mathbf{x} \in \mathbb{Z}^{2n} : \mathbf{R} \cdot \mathbf{x} \equiv \mathbf{0} \bmod q\}$ and its basis $\{\mathbf{x}_i\}_{1\le i\le 2n} \subset \mathbb{Z}^{2n}$ such that $\|x_i\|_2 = \lambda_i(\mathit{\Lambda})$ for each i. Since the rank of $\mathit{\Lambda}$ is $2n$ and its determinant is q^n, we can estimate the size of each $\|x_i\|_2$ similar to $\sqrt{\frac{n}{\pi e}} \cdot q^{1/2}$ accepting Gaussian heuristic assumption.

Next, we get the vector ${\mathbf{v}_1}' = \mathbf{v}_1 + \sum_{i=1}^{2n} u_i \mathbf{x}_i$ through the Babai's nearest plane algorithm so that $\|\mathbf{v}_1 + \sum_{i=1}^{2n} u_i \mathbf{x}_i\|_2 \le \sqrt{\frac{1}{4} \sum_{i=1}^{2n} \|\mathbf{x}_i^*\|_2^2}$ holds, where each $\mathbf{x}_i^*$

is Gram-Schmidt vector of x_i. Then we obtain the equality $\mathbf{R} \cdot \mathbf{v_1}' \equiv \mathbf{e_1} \bmod q$. Hence, by using the Cauchy-Schwarz inequality and $\|\mathbf{x}_i^*\|_2 \leq \|\mathbf{x}_i\|_2$, we can get the follows:

$$\|\mathbf{v}_1{}'\|_2 = \|\mathbf{v}_1 + \sum_{i=1}^{2n} u_i \mathbf{x}_i\|_2 \leq \sqrt{\frac{1}{4}\sum_{i=1}^{2n}\|\mathbf{x}_i^*\|_2^2} \leq \frac{n}{\sqrt{2\pi e}} \cdot q^{1/2} \text{ and}$$

$$\|\mathbf{v}_1{}'\|_1 \leq \sqrt{2n} \cdot \|\mathbf{v}_1'\|_2 \leq n\sqrt{\frac{n}{\pi e}} \cdot q^{1/2}.$$

If $|[\mathbf{R}]_i \cdot \mathbf{v}_1{}'| \leq \|[\mathbf{R}]_i\|_2 \cdot \|\mathbf{v}_1{}'\|_2 \leq \sqrt{2n} \cdot 2^\rho \cdot \dfrac{n}{\sqrt{2\pi e}} \cdot q^{1/2}$ is less than $\frac{q}{2}$ for each i, then we can obtain the following equation over integers:

$$\mathbf{R} \cdot \mathbf{v}_1{}' = \mathbf{e}_1.$$

Therefore, setting the size of $q^{\frac{1}{2}}$ similar to $\dfrac{2}{\sqrt{\pi e}} \cdot n^{\frac{3}{2}} \cdot 2^\rho$, we can conclude that the size of $\|\mathbf{v}_1{}'\|_1$ is bounded by $\dfrac{2}{\pi e} \cdot n^3 \cdot 2^\rho$. We can also apply it to other $\mathbf{v}_i$'s and we can construct $\mathbf{R}^* = (\mathbf{v}_1{}', \cdots, \mathbf{v}_{2n}{}')$ so that $\|\mathbf{R}^*\|_\infty = \max_{1\leq i \leq n} \|\mathbf{v}_i{}'\|_1 \leq \dfrac{2}{\pi e} \cdot n^3 \cdot 2^\rho$ holds. Hence, we can obtain as follows:

$$\|\tilde{\mathbf{c}}\|_2 \cdot \|\mathbf{R}^*\|_\infty \leq \frac{2}{\pi e} \cdot n^3 \cdot 2^\rho \cdot \|\tilde{\mathbf{c}}\|_2.$$

Since $(\hat{p}_1, r_{1,1} \cdot \hat{p}_1, \cdots, r_{1,2n} \cdot \hat{p}_1)^T$ is in $\mathcal{L}$, the size of $\lambda_1(\mathcal{L})$ does not exceed the previous vector's size. Thus, we get the inequality as follows:

$$\lambda_1(\mathcal{L}) \leq \sqrt{2n+1} \cdot N \cdot 2^{-\eta+\rho+1}.$$

Taking $\mathbf{c}$ as a short vector in $\mathcal{L}$ with the LLL algorithm, we can bound $\|\mathbf{c}\|_2$ as described in section 2.1. As a result, the below inequality is valid:

$$\begin{aligned}\|\tilde{\mathbf{c}}\|_2 \cdot \|\mathbf{R}^*\|_\infty \leq \|\mathbf{c}\|_2 \cdot \|\mathbf{R}^*\|_\infty &\leq (2^n \cdot \lambda_1(\mathcal{L})) \cdot \frac{2}{\pi e} \cdot n^3 \cdot 2^\rho \\ &\leq 2^n\sqrt{2n+1} \cdot N \cdot 2^{-\eta+\rho+1} \cdot \frac{2}{\pi e} \cdot n^3 \cdot 2^\rho.\end{aligned}$$

We can regard c_0 as a dual instance of CRT-ACD when $|d_i \cdot \hat{p}_i| \leq N \cdot 2^{-2\rho - \log n - 1}$. The following inequality is required:

$$\begin{aligned}\|\tilde{\mathbf{c}}\|_2 \cdot \|\mathbf{R}^*\|_\infty &\leq 2^n\sqrt{2n+1} \cdot N \cdot 2^{-\eta+\rho+1} \cdot \frac{2}{\pi e} \cdot n^3 \cdot 2^\rho \\ &\leq N \cdot 2^{-2\rho - \log n - 1}.\end{aligned}$$

In summary, the required condition for parameters to find a dual instance by using the LLL algorithm is as follows:

$$n \leq \eta - 4\rho - \frac{9}{2}\log n - 1.$$

Therefore, the first entry of the vector $\mathbf{c} \in \mathcal{L}$ obtained by the LLL algorithm under the above condition is the dual instance that we want.

$\square$

Remark. If we use the BKZ algorithm with a block size β instead of the LLL algorithm for the CRT-ACD problem, the upper bound of a vector $\mathbf{c}$ from the lattice $\mathcal{L}$ would be as follows:

$$\|\mathbf{c}\| \leq 4 \cdot \beta^{\frac{2n}{\beta-1}+3} \cdot \sqrt{2n+1} \cdot N \cdot 2^{-\eta+2\rho+1}.$$

Therefore, under the condition $n \leq \dfrac{\beta-1}{2\log\beta} \cdot \left(\eta - 4\rho - \dfrac{9}{2}\log n - 3\log\beta - 3\right)$, we can obtain a dual instance for CRT-ACD in $poly(n,\eta) \cdot 2^{O(\beta)}$ time.

3.2 Solving the CRT-ACD Problem

Now we introduce our algorithm, which is referred from [7], to solve the CRT-ACD problem using dual instances. For two different dual instances $d = \sum_{j=1}^{n} d_j \cdot \hat{p}_j$ and $d' = \sum_{j=1}^{n} d_j{}' \cdot \hat{p}_j$ obtained in the above procedure, we have already checked the followings:

$$[d \cdot b_u \cdot b_v]_N = \sum_{j=1}^{n} r_{j,u} \cdot (d_j \cdot \hat{p}_j) \cdot r_{j,v} \text{ and } [d' \cdot b_u \cdot b_w]_N = \sum_{j=1}^{n} r_{j,u} \cdot (d_j{}' \cdot \hat{p}_j) \cdot r_{j,v}.$$

By using above properties, we can solve the CRT-ACD problem with two dual instance d and d'. Suppose that $2n$ CRT-ACD instances are given as follows:

$$b_i = \mathsf{CRT}_{(p_k)}(r_{k,i}),\ b_j{}' = \mathsf{CRT}_{(p_k)}(r_{k,j}{}') \quad \text{for } 1 \leq i,j \leq n.$$

We denote $w_{i,j}$ and $w_{i,j}{}'$ as $[b_i \cdot b_j{}' \cdot d]_N$ and $[b_i \cdot b_j{}' \cdot d']_N$, respectively. Then, we get the following matrix equations:

$$\begin{aligned}
w_{i,j} &= \sum_{k=1}^{n} r_{k,i} \cdot (d_k \cdot \hat{p}_k) \cdot r_{k,j}{}' \\
&= \begin{pmatrix} r_{1,i} \; r_{2,i} \cdots r_{n,i} \end{pmatrix} \begin{pmatrix} d_1 \cdot \hat{p}_1 & 0 & \cdots & 0 \\ 0 & d_2 \cdot \hat{p}_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_n \cdot \hat{p}_n \end{pmatrix} \begin{pmatrix} r_{1,j}{}' \\ r_{2,j}{}' \\ \vdots \\ r_{n,j}{}' \end{pmatrix},
\end{aligned}$$

$$\begin{aligned}
w_{i,j}{}' &= \sum_{k=1}^{n} r_{k,i} \cdot (d_k{}' \cdot \hat{p}_k) \cdot r_{k,j}{}' \\
&= \begin{pmatrix} r_{1,i} \; r_{2,i} \cdots r_{n,i} \end{pmatrix} \begin{pmatrix} d_1{}' \cdot \hat{p}_1 & 0 & \cdots & 0 \\ 0 & d_2{}' \cdot \hat{p}_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_n{}' \cdot \hat{p}_n \end{pmatrix} \begin{pmatrix} r_{1,j}{}' \\ r_{2,j}{}' \\ \vdots \\ r_{n,j}{}' \end{pmatrix}.
\end{aligned}$$

By collecting the above values of i, j, we can construct two matrices $\mathbf{W} = (w_{i,j})$ and $\mathbf{W}' = (w_{i,j}{}') \in M_{n\times n}(\mathbb{Z})$. Computing $(\mathbf{W}')^{-1}$ over $\mathbb{Q}$, we obtain the matrix $\mathbf{Y} = \mathbf{W} \cdot (\mathbf{W}')^{-1}$ whose eigenvalues are $\dfrac{d_1}{d_1{}'}, \cdots, \dfrac{d_n}{d_n{}'}$. We can compute those rational eigenvalues in polynomial-time of η, n and ρ from $\mathbf{Y}$ and we obtain d_j, $d_j{}'$ for each j. Since the congruence $d \equiv d_j \cdot \hat{p}_j \bmod p_j$ and $d' \equiv d_j{}' \cdot \hat{p}_j \bmod p_j$ holds, $d \cdot (d')^{-1} \equiv d_j \cdot (d_j{}')^{-1} \bmod p_j$ is satisfied and we can check that p_j divides $d \cdot d_j{}' - d' \cdot d_j$ for each j. Thus, by computing $\gcd(N, d \cdot d_j{}' - d' \cdot d_j)$, we can find p_j for all j's.

Corollary 1. *Let n, η, ρ be parameters of* CRT-ACD*. When $O(n)$* CRT-ACD *instances are given, We can solve* CRT-ACD *under the asymptotic condition $n \le \eta - 4\rho - \frac{9}{2}\log n - 1$ in $\max\{T_L(n, n\cdot\eta), \widetilde{\mathcal{O}}(n^{2+\omega}\cdot\eta)\}$ time with the LLL algorithm, where ω is a constant less than 2.38.*

3.3 The Scaled CRT-ACD Problem

We introduce a variant of the CRT-ACD problem, the Scaled CRT-ACD (SCRT-ACD) problem. We give a precise definition of the problem as follows.

Definition 4. *(**Scaled CRT-ACD**) Let n, η, ρ be positive integers. For given η bit primes $p_1, \cdots, p_n$ and unknown $c \in \mathbf{Z}_N$, $k+1$ number of modified CRT-ACD instances are given as follows:*

$$c \leftarrow \mathbb{Z}_N;\ \textit{sampled from an uniform distribution over } \mathbb{Z}_N.$$

$$c \cdot b_i \textit{ with } b_i = \mathit{CRT}_{(p_j)}(r_{j,i}) \leftarrow \mathcal{D}_{\chi_\rho,\eta,n}(p_1, \cdots, p_n) \textit{ for } 0 \le i \le k$$

The Scaled CRT-ACD *problem is: for given such modified samples of CRT-ACD and $N = \prod_{i=1}^{n} p_i$, find a nontrivial factor of N.*

Since the size of c is unknown, the algorithm described in section 3.1 is not directly applicable to the SCRT-ACD problem. Instead, by using divisions in modulus N, one can get the new quantities:

$$b_i{}' = [(c \cdot b_i) \cdot (c \cdot b_0)^{-1}]_N.$$

In this case, $b_i{}' \equiv b_i \cdot b_0^{-1} \equiv r_{j,i} \cdot r_{j,0}^{-1} \bmod p_j$ holds for each j.

For the new samples $b_i{}'$'s, we would apply the method similar to the Section 3.1 and 3.2. More precisely, we consider a new quantity as the following form:

$$d = \sum_{j=1}^{n} d_j \cdot r_{j,0}{}^2 \cdot \hat{p}_j.$$

Then, d plays the same role as a dual instance in the $\mathsf{CRT\text{-}ACD}$ problem due to the following properties:

$$[d \cdot {b_i}']_N \equiv \sum_{j=1}^{n} d_j \cdot r_{j,0} \cdot r_{j,i} \cdot \hat{p}_j \bmod N,$$
$$[d \cdot {b_u}' \cdot {b_v}']_N \equiv \sum_{j=1}^{n} d_j \cdot r_{j,u} \cdot r_{j,v} \cdot \hat{p}_j \bmod N,$$
$$[d \cdot {b_i}'^2]_N \equiv \sum_{j=1}^{n} d_j \cdot {r_{j,i}}^2 \cdot \hat{p}_j \bmod N.$$

Thus, we define a instance having the above properties as a dual instance for $\mathsf{SCRT\text{-}ACD}$. To obtain a such dual instance, we consider a lattice $\mathcal{L}'$ whose basis matrix is as follows:

$$\mathbf{B}' = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ {b_1}'^2 & N & 0 & \cdots & 0 \\ {b_2}'^2 & 0 & N & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ {b_k}'^2 & 0 & 0 & \cdots & N \end{pmatrix}.$$

Let $\mathbf{c}' = ([d]_N, [d \cdot {b_1}']_N, \cdots, [d \cdot {b_k}']_N)^T$; the vector from $\mathcal{L}'$ with $d = \sum_{j=1}^{n} d_j \cdot {r_{j,0}}^2 \cdot \hat{p}_j$ and let $\tilde{\mathbf{c}}' = ([d \cdot {b_1}']_N, \cdots, [d \cdot {b_k}']_N)$. Then, we can write as follows:

$$\tilde{\mathbf{c}}' \equiv \mathbf{d} \cdot \hat{\mathbf{P}} \cdot \mathbf{R}' \mod N,$$

where $\mathbf{d}$=$(d_1, \cdots, d_n)$, $\hat{\mathbf{P}} = \mathsf{diag}(\hat{p}_1, \cdots, \hat{p}_n)$, and $\mathbf{R}' = ({r_{j,i}}^2) \in M_{n \times k}(\mathbb{Z})$.

Using the same method in section 3.1, we can construct a right inverse $(\mathbf{R}')^*$ $\in M_{k \times n}(\mathbb{Z})$ satisfying $\mathbf{R}' \cdot (\mathbf{R}')^* = \mathbf{I}_n$. Then, the following holds:

$$\begin{aligned} \|\mathbf{d} \cdot \hat{\mathbf{P}} \cdot \mathbf{R}' \cdot (\mathbf{R}')^* \bmod N\|_\infty &= \|\tilde{\mathbf{c}}' \cdot (\mathbf{R}')^* \bmod N\|_\infty \\ &\le \|\tilde{\mathbf{c}}' \cdot (\mathbf{R}')^*\|_\infty \le \|\tilde{\mathbf{c}}'\|_\infty \cdot \|(\mathbf{R}')^*\|_\infty \\ &\le \|\mathbf{c}'\|_2 \cdot \|(\mathbf{R}')^*\|_\infty. \end{aligned}$$

We also let k be $2n$ for simplicity. For each entry of $({r_{j,i}}^2) \in \mathbf{R}'$, $|{r_{j,i}}^2| \le 2^{2\rho}$ holds. Hence, $\|(\mathbf{R}')^*\|_\infty \le \frac{2}{\pi e} \cdot n^3 \cdot 2^{2\rho}$ holds as the same reason in section 3.1.

Similar to the section 3.1, we take $\mathbf{c}'$ as a short vector from the lattice $\mathcal{L}'$ so that it satisfies the follows:

$$\|\mathbf{d} \cdot \hat{\mathbf{P}} \cdot \mathbf{R}' \cdot (\mathbf{R}')^* \bmod N\|_\infty \le N \cdot 2^{-2\rho - \log n - 1},$$

$$i.e., \quad |d_j \cdot \hat{p}_j \pmod N| = |[d_j]_{p_j}| \cdot \hat{p}_j \le N \cdot 2^{-2\rho - \log n - 1} \text{ for each } j.$$

From the above condition, $[d]_N = [\sum_{j=1}^{n} d_j \cdot {r_{j,0}}^2 \cdot \hat{p}_j]_N = \sum_{j=1}^{n} [d_j]_{p_j} \cdot {r_{j,0}}^2 \cdot \hat{p}_j$ holds and it would be the dual instance for the SCRT-ACD since

$$[d \cdot {b_u}' \cdot {b_v}']_N = [\sum_{j=1}^{n} d_j \cdot r_{j,u} \cdot r_{j,v} \cdot \hat{p}_j]_N = \sum_{j=1}^{n} [d_j]_{p_j} \cdot r_{j,u} \cdot r_{j,v} \cdot \hat{p}_j$$

$$\text{with} \quad |\sum_{j=1}^{n} [d_j]_{p_j} \cdot r_{j,u} \cdot r_{j,v} \cdot \hat{p}_j| \le N/2.$$

Since $\lambda_1(\mathcal{L}') \le \sqrt{2n+1} \cdot N \cdot 2^{-\eta+2\rho+1}$ holds (note that $\mathbf{v} = ({r_{1,0}}^2 \cdot \hat{p}_1, {r_{1,1}}^2 \cdot \hat{p}_1, \cdots, {r_{1,2n}}^2 \cdot \hat{p}_1)^T \in \mathcal{L}'$), the upper bound of the vector $\mathbf{c}'$ obtained from $\mathcal{L}$ by the LLL algorithm is as follows:

$$\|\mathbf{c}'\| \le 2^n \cdot \sqrt{2n+1} \cdot N \cdot 2^{-\eta+2\rho+1}.$$

Therefore, the condition for the parameters to find the dual instance is as follows:

$$\begin{aligned} &\|\mathbf{d} \cdot \hat{\mathbf{P}} \cdot \mathbf{R}' \cdot (\mathbf{R}')^* \bmod N\|_\infty \le \|\mathbf{c}'\|_2 \cdot \|(\mathbf{R}')^*\|_\infty \\ \le &\frac{2}{\pi e} \cdot n^3 \cdot 2^{2\rho} \cdot 2^n \cdot \sqrt{2n+1} \cdot N \cdot 2^{-\eta+2\rho+1} \\ \le &N \cdot 2^{-2\rho-\log n-1}. \end{aligned}$$

By summarizing the above inequality, one can get the following inequality:

$$n \le \eta - 6\rho - \frac{9}{2}\log n - 1.$$

If the above condition holds, we can obtain a dual instance for the SCRT-ACD problem by the LLL algorithm in $poly(n, \eta)$ time when $2n$ number of instances are given.

Theorem 3. *Let n, η, ρ be parameters of the* SCRT-ACD *problem. When $2n$* SCRT-ACD *instances are given, we can find a dual instance for the* SCRT-ACD *problem under the condition $n \le \eta - 6\rho - \frac{9}{2}\log n - 1$ in $T_L(n, n \cdot \eta)$ time by using the LLL algorithm.*

For such dual instances $d = \sum_{j=1}^{n} d_j \cdot {r_{j,0}}^2 \cdot \hat{p}_j$ and $d' = \sum_{j=1}^{n} {d_j}' \cdot {r_{j,0}}^2 \cdot \hat{p}_j$, we can check the followings:

$$[d \cdot {b_u}' \cdot {b_v}']_N = \sum_{j=1}^{n} r_{j,u} \cdot (d_j \cdot \hat{p}_j) \cdot r_{j,v},$$

$$[d' \cdot {b_u}' \cdot {b_w}']_N = \sum_{j=1}^{n} r_{j,u} \cdot ({d_j}' \cdot \hat{p}_j) \cdot r_{j,v}.$$

With the same method in section 3.1, we can compute $\dfrac{d_1}{{d_1}'}, \cdots, \dfrac{d_n}{{d_n}'}$ in polynomial time of η, n and ρ and we obtain d_j, ${d_j}'$ for each j. Since the congruence $d \equiv d_j \cdot {r_{j,0}}^2 \cdot \hat{p}_j \bmod p_j$ and $d' \equiv {d_j}' \cdot {r_{j,0}}^2 \cdot \hat{p}_j \bmod p_j$ holds, $d \cdot (d')^{-1} \equiv d_j \cdot ({d_j}')^{-1} \bmod p_j$ is also satisfied in this case. Thus, we can find p_j for all j's by computing $\gcd(N, d \cdot {d_j}' - d' \cdot d_j)$ and obtain the following corollary.

Corollary 2. *Let n, η, ρ be parameters of the* SCRT-ACD *problem. If the condition about parameters; $n \le \eta - 6\rho - \dfrac{9}{2}\log n - 1$ holds, we can solve the* SCRT-ACD *in $\max\{T_L(n, n\cdot\eta), \widetilde{\mathcal{O}}(n^{2+\omega}\cdot\eta)\}$ time by using the LLL algorithm, where ω is a constant less than* 2.38*.*

Remark. Using the the BKZ algorithm instead of the LLL algorithm for the SCRT-ACD problem, one can solve the SCRT-ACD problem under the condition $n \le \dfrac{2\log\beta}{\beta - 1}\left(\eta - 6\rho - \frac{9}{2}\log n - 3\log\beta - 3\right)$ in $poly(n,\eta)\cdot 2^{O(\beta)}$ time, where β is the block size of the BKZ algorithm.

3.4 Application to the CLT13 multilinear map

In this section, we present a cryptanalysis of CLT13 multilinear map without low level encodings of zero, which is employed in indistinguishability obfuscation procedure such as [14]. In fact, encodings are the instances of SCRT-ACD. Now we describe a portion of CLT13 to explain our results.

The secret parameters of CLT13 consist of n η-bit primes p_j's, n ρ-bit integers r_j's and n α-bit primes g_j's. For the public parameter $N = \prod_{j=1}^{n} p_j$, another secret parameter z is randomly chosen from $\mathbb{Z}_N$. A level-1 encoding c of a vector $\mathbf{m} = (m_i) \in \mathbb{Z}^n$ is an integer of the form as follows:

$$c = \mathsf{CRT}_{(p_j)}\left((r_j \cdot g_j + m_j)/z\right).$$

Note that the fixed integer l satisfies $|r_j \cdot g_j + m_j| \le l \cdot 2^{\rho+\alpha}$ for each j.

In the paper [10], the parameters ρ and α are set to satisfy as $\rho = \Omega(\lambda)$ and $\alpha = \lambda$, where λ is the proposed security parameter in CLT13. In particular, when level-0 encodings are given, the authors claim that the parameter n should match the condition $n = \eta \cdot \omega(\log\lambda)$ to resist against the thwart lattice-based attacks. While, if the encodings are not published, there has not been suggested conditions with respect to n.

However, applying the algorithm in section 3.3 to the level-1 encodings c's, one can obtain the condition about n. It coincides with the condition when level-0 encodings are given. In other words, the parameter setting for n does not rely on the existence of level-0 encodings. More precisely, we can regard a level-1 encoding $c = \mathsf{CRT}_{(p_j)}(d_j/z)$ as an instance for the SCRT-ACD problem, where $d_j = r_j \cdot g_j + m_j$ with $|d_j| \le l \cdot 2^{\rho+\alpha}$. By using the algorithm for SCRT-ACD with $2n$ level-1 encodings $c_i = \mathsf{CRT}_{(p_j)}(d_{j,i}/z)$ in Section 3.3, we can recover the primes p_j's under the following condition:

$$4n + 2 \leq \frac{\eta - 6(\log l + \rho + \alpha) - \frac{9}{2}\log n - 1}{\log \delta},$$

where δ is the root Hermite factor of the lattice reduction algorithm that we use. Utilizing the above condition, we estimate that 8 out of 12 parameters suggested in [10, Section 6.4] is insecure by our attack using the BKZ algorithm with block size 20, importing the root Hermite factor experimented in [13].

According to [10], the vector $\mathbf{m}$ can be recovered if one can find all p_j's. Thus, all of parameters, which are kept to be secret in the CLT13 multilinear map, can be revealed by our algorithm in sub-exponential time with respect to λ if the condition $n = (\eta - 6\rho) \cdot O(\lambda^{1-\epsilon})$ holds for any $\epsilon > 0$. It is the first analysis of the CLT13 without low level encodings of zero.

4 Experiments and Results

We performed experiments of the proposed algorithms with concrete parameters. All experiments were performed on a single Intel Core i5 running at 2.1GHz processor and 16GB memory with fplll algorithm [11]. Our algorithm consists of two steps. The first step is to construct dual instances and the second step is to factor N with dual instances. In most of the our experiments, we could factor N with only the first step by finding the great common divisor of the dual instance and N. To avoid running LLL on a lattice with too large dimension, we set $n = 50$ and $k = 2n$. The $\rho_{\max}$ value corresponding to η is the maximum ρ value on which the experiment succeeded. The following table shows the results of our experiments for CRT-ACD and SCRT-ACD.

CRT-ACD	η	$\rho_{\max}$	time	SCRT-ACD	η	$\rho_{\max}$	time
Our result	150	70	5m	Our result	150	20	10m
	300	110	1h		300	45	1h
	450	190	2h		450	70	1.7h
	600	300	3.1h		600	90	3.4h
	750	370	4.1h		750	110	4.6h
	900	450	6.2h		900	145	6h
	1500	700	10h		1500	245	15.5h

According to experimental results, our algorithm for CRT-ACD and SCRT-ACD found a dual instance much better than our expectation when n is small. More precisely, in our experiments, the asymptotic condition of n improved from $\eta - 5\rho$ to $\eta - \frac{5}{2}\rho$ in CRT-ACD and from $\eta - 9\rho$ to $\eta - 6\rho$ in SCRT-ACD.

In most of the our experiments, we could factorize N when the first step is only conducted, and we found all of $p_j's$ in the second step. We guess that these results might be occurred that the approximate factor is too small in our experimental condition. When n is large, it is expected that we may not be able to factor N using the first step alone.

5 Conclusion

We presented the algorithm to solve the CRT-ACD problem. We described how to obtain dual instances for CRT-ACD, which implies that CRT-ACD can be reduced to CRT-ACDwDI. Using the BKZ algorithm with the block size β, we showed that dual instances can be obtained under the condition $n \leq \frac{\beta-1}{2\log\beta}(\eta-4\rho-O(\log n))$. It is the first approach to solve the CRT-ACD problem and it would provide the required condition about parameters to resist against the above algorithms.

As an application, we can use our algorithms to solve the SCRT-ACD problem. By using the BKZ algorithm with the block size β, its new dual instances can be generated under the condition $n \leq \frac{\beta-1}{2\log\beta}(\eta - 6\rho - O(\log n))$ in $poly(n, \eta) \cdot 2^{O(\beta)}$ time. With that condition, we can reveal the secret p_j's for CLT13 multilinear map using the algorithm for SCRT-ACD. It implies that n should be set as $(\eta - 6\rho) \cdot \Omega(\lambda)$ which agrees with the conditions of CLT13 multilinear map with low level encodings of zero in [10].

In order to use the our algorithm for CRT-ACD, a condition $\eta > 4\rho$ is essential. So, there is a remained problem to analysis the CRT-ACD problem whose condition of parameters is given by $\eta \approx 4\rho$.

References

1. M. Abdalla, F. Benhamouda, and D. Pointcheval. Disjunctions for hash proof systems: New constructions and applications. In *EUROCRYPT (2)*, pages 69–100, 2015.
2. M. Ajtai. Generating random lattices according to the invariant distribution. draft, 2006.
3. N. Attrapadung. Fully secure and succinct attribute based encryption for circuits from multi-linear maps. *IACR Cryptology ePrint Archive*, 2014:772, 2014.
4. F. Benhamouda and D. Pointcheval. Verifier-based password-authenticated key exchange: New models and constructions. *IACR Cryptology ePrint Archive*, 2013:833, 2013.
5. D. Boneh, K. Lewi, H. Montgomery, and A. Raghunathan. Key homomorphic PRFs and their applications. In *Proc. of CRYPTO*, pages 410–428. Springer, 2013.
6. 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.
7. 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.
8. J. H. Cheon, M. Kim, and M. Kim. Search-and-compute on encrypted data. In *International Conference on Financial Cryptography and Data Security*, pages 142–159. Springer, 2015.
9. J. H. Cheon, M. Kim, and K. Lauter. Homomorphic computation of edit distance. In *International Conference on Financial Cryptography and Data Security*, pages 194–212. Springer, 2015.
10. J. Coron, T. Lepoint, and M. Tibouchi. Practical multilinear maps over the integers. In *Advances in Cryptology - CRYPTO 2013*, pages 476–493, 2013.

11. T. F. development team. fplll, a lattice reduction library. Available at https://github.com/fplll/fplll, 2016.
12. S. D. Galbraith. *Mathematics of public key cryptography.* Cambridge University Press, 2012.
13. N. Gama and P. Nguyen. Predicting lattice reduction. *Advances in Cryptology–EUROCRYPT 2008*, pages 31–51, 2008.
14. S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai, and B. Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. *SIAM Journal on Computing*, 45(3):882–929, 2016.
15. S. Garg, C. Gentry, S. Halevi, and M. Zhandry. Fully secure attribute based encryption from multilinear maps. Cryptology ePrint Archive, Report 2014/622, 2014.
16. S. Garg, C. Gentry, S. Halevi, and M. Zhandry. Fully secure functional encryption without obfuscation. Cryptology ePrint Archive, Report 2014/666, 2014.
17. 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.
18. C. Gentry, A. B. Lewko, and B. Waters. Witness encryption from instance independent assumptions. In *Advances in Cryptology - CRYPTO 2014*, pages 426–443, 2014.
19. X. P. Guillaume Hanrot and D. Stehle. Terminating bkz. 2011.
20. N. Howgrave-Graham. Approximate integer common divisors. pages 51–66, 2001.
21. D. Huang, D. Zhao, L. Wei, Z. Wang, and Y. Du. Modeling and analysis in marine big data: advances and challenges. *Mathematical Problems in Engineering*, 2015, 2015.
22. K. Lewi, H. W. Montgomery, and A. Raghunathan. Improved constructions of PRFs secure against related-key attacks. In *Proc. of ACNS*, volume 8479 of *LNCS*, pages 44–61. Springer, 2014.
23. P. Q. Nguyen and D. Stehlé. An lll algorithm with quadratic complexity. *SIAM J. Comput*, 39(3):874–903, 2009.
24. J. Tang, Y. Cui, Q. Li, K. Ren, J. Liu, and R. Buyya. Ensuring security and privacy preservation for cloud data services. *ACM Computing Surveys (CSUR)*, 49(1):13, 2016.
25. M. Zhandry. Adaptively secure broadcast encryption with small system parameters. *IACR Cryptology ePrint Archive*, 2014.
26. J. Zimmerman. How to obfuscate programs directly. In *Advances in Cryptology - EUROCRYPT 2015*, pages 439–467, 2015.

A Optimizing the condition of section 3.1

For the general k, the lattice $\Lambda = \{\mathbf{x} \in \mathbb{Z}^k : \mathbf{R} \cdot \mathbf{x} \equiv \mathbf{0} \bmod q\}$ has the rank k and its determinant is q^n. Using the same method in section 3.1, we obtain the following condition of $\|\mathbf{R}^*\|_\infty$ as follows:

$$\|\mathbf{R}^*\|_\infty \leq \frac{k^{\frac{3}{2}}}{2\sqrt{2\pi e}} \cdot \left(\frac{2^\rho}{\sqrt{2\pi e}}\right)^{\frac{n}{k-n}} \cdot k^{\frac{3n}{2(k-n)}}.$$

Also, obtaining the vector $\mathbf{c} \in \mathcal{L}$ by the BKZ algorithm with the block size β, the $\|\mathbf{c}\|_2$ is bounded as follows:

$$\|\mathbf{c}\|_2 \leq 4 \cdot \beta^{\frac{k}{\beta-1}+3} \cdot \sqrt{k+1} \cdot 2^{-\eta+\rho+1}.$$

Summarizing the inequality $\|\mathbf{c}\|_2 \cdot \|\mathbf{R}^*\|_\infty \leq N \cdot 2^{-2\rho-\log n-1}$ with above conditions, we obtain the inequality as follows:

$$\frac{\log\beta}{\beta-1}\cdot k+\frac{4k-n}{2(k-n)}\cdot\log k+\rho\cdot\frac{n}{k-n}-\frac{2k}{k-n}\leq\eta-3\rho-\log n-3\log\beta-3.5.$$

We can rewrite the above inequality asymptotically as follows:

$$\frac{\log\beta}{\beta-1}\cdot(k-n)+\rho\cdot\frac{n}{k-n}\leq\eta-3\rho-\frac{\log\beta}{\beta-1}\cdot n.$$

The left hand side is smallest when $(k-n)^2 = n\rho\cdot\frac{\beta-1}{\log\beta}$ holds. Thus, by substituting $n+\sqrt{n\rho\cdot\frac{\beta-1}{\log\beta}}$ for k, we obtain the asymptotic condition of finding a dual instance for CRT-ACD with the BKZ algorithm as follows:

$$\frac{\log\beta}{\beta-1}\cdot n+\sqrt{n\rho\cdot\frac{\log\beta}{\beta-1}}\leq\eta-3\rho-O\left(\sqrt{\frac{n}{\rho}}\cdot\log\left(n+\sqrt{\rho n}\right)\right).$$

B Optimizing the condition of section 3.3

In the case of SCRT-ACD, using the same method from above, $\|(\mathbf{R}')^*\|_\infty$ and $\|\mathbf{c}'\|_2$ are bounded as follows:

$$\|(\mathbf{R}')^*\|_\infty\leq\frac{k^{\frac{3}{2}}}{2\sqrt{2\pi e}}\cdot\left(\frac{2^{2\rho}}{\sqrt{2\pi e}}\right)^{\frac{n}{k-n}}\cdot k^{\frac{3n}{2(k-n)}}.$$

$$\|\mathbf{c}'\|_2\leq 4\cdot\beta^{\frac{k}{\beta-1}+3}\cdot\sqrt{k+1}\cdot 2^{-\eta+2\rho+1}.$$

where β is the block size of the BKZ algorithm.

Summarizing the inequality $\|\mathbf{c}'\|_2 \cdot \|(\mathbf{R}')^*\|_\infty \leq N \cdot 2^{-2\rho-\log n-1}$ by using above conditions, we obtain the inequality as follows:

$$\frac{\log\beta}{\beta-1}\cdot k+\frac{4k-n}{2(k-n)}\cdot\log k+2\rho\cdot\frac{n}{k-n}-\frac{2k}{k-n}\leq\eta-4\rho-\log n-3\log\beta-3.5.$$

In this case, substituting $n+\sqrt{2n\rho\cdot\frac{\beta-1}{\log\beta}}$ for k, we obtain the asymptotic condition of finding a dual instance for the SCRT-ACD problem with the BKZ algorithm as follows:

$$\frac{\log\beta}{\beta-1}\cdot n+\sqrt{2n\rho\cdot\frac{\log\beta}{\beta-1}}\leq\eta-4\rho-O\left(\sqrt{\frac{n}{\rho}}\cdot\log\left(n+\sqrt{\rho n}\right)\right).$$