J. Math. Cryptol. ? (????), 1–25
DOI 10.1515/jmc-????-???

Algorithms for CRT-variant of Approximate Greatest Common Divisor Problem †

Jung Hee Cheon, Wony Cho, Minki Hhan, Minsik Kang, Jiseung Kim and Changmin Lee

Communicated by ???

Abstract. The approximate greatest common divisor problem (ACD) and its variants have been used to construct many cryptographic primitives. In particular, variants of the ACD problem based on Chinese remainder theorem (CRT) are exploited in the constructions of a batch fully homomorphic encryption to encrypt multiple messages in one ciphertext. Despite the utility of the CRT-variant scheme, the algorithms to solve its security foundation have not been studied well.

In this paper, we propose two algorithms and their experimental results for solving the variant problem. Both two algorithms take the same time complexity $2^{\tilde{O}(\frac{\gamma}{(\eta-\rho)^2})}$ up to a polynomial factor to solve the variant problem for the bit size of samples γ, secret primes η, and error bound ρ. Our algorithm gives the first parameter condition related to η and γ size. From the experimental results, we can see that our algorithms work well both in theoretical and experimental terms.

Keywords. CCK-ACD; Lattice; orthogonal lattice attack; SDA.

2010 Mathematics Subject Classification. 11Y16.

1 Introduction

The approximate greatest common divisor (ACD) problem was defined and studied by Howgrave Graham [15]. The ACD problem and its variant problems have been used to construct cryptographic schemes such as fully homomorphic encryption (FHE) and cryptographic multilinear map [4, 6, 8, 18].

† A preliminary version of this paper was submitted to the *EUROCRYPT 2018*.
The authors of Seoul National University were supported by Institute for Information & communication Technology Promotion (IITP) grant funded by the Korea government (MSIT) (No. 2016-6-00598, The mathematical structure of functional encryption and its analysis), and the ARO and DARPA under Contract No.W911NF-15-C-0227. The author of ENS de Lyon was supported by the LABEX MILYON (ANR-10-LABX-0070) of Université de Lyon, within the program "Investissements d'Avenir" (ANR-11-IDEX-0007) operated by the French National Research Agency (ANR).

In the paper [4], a variant of the ACD problem was introduced to suggest a new FHE scheme, which is called CCK-FHE scheme, over the integers. This scheme exploits Chinese remainder theorem to encrypt multiple messages in one ciphertext. Informally, for integers γ, n, η, and ρ such that $\gamma \gg n \cdot \eta$ and $\eta \gg \rho$, the γ-bit ciphertext integer b of this scheme is characterized by satisfying modulo equations $b \equiv r_i \bmod p_i$ for $1 \leq i \leq n$, where r_i's are ρ-bit integers and p_i's are η-bit fixed secret primes. We call the problem of distinguishing between ciphertexts of CCK-FHE scheme and uniform samples of γ-bit integer, when the γ-bit integer $N = \prod_{i=0}^{n} p_i$ which is the product of secret primes is given, the CCK-ACD problem.[1]

On the other hand, algorithms to directly solve the CCK-ACD problem have received a little attention. Galbraith, Gebregiyorgis and Murphy said that an algorithm to solve the CCK-ACD problem exploiting CRT structure is an open problem [12]. In fact, there have been no algorithms for solving the CCK-ACD problem so far except for the method of Chen and Nguyen [3], which depends only on ρ. Instead, to give the evidence of the security of the CCK-FHE, authors in [4] suggested a reduction from PACD to CCK-ACD.

However, while the current CCK-FHE parameters are set to be secure for the Chen and Nguyen's attack, the authors in [4] did not use the parameter settings obtained from the reduction for known PACD parameters. Therefore it is necessary to determine whether the CCK-FHE parameters satisfies the desired security even under the current conditions of η and γ. In sum, one can naturally pose the following question:

> *Is it possible to present time complexity for solving* CCK-ACD
> *by using a mathematical algorithm that depends on η and γ?*

Previous works. To solve the CCK-ACD problem, several naive methods are suggested. Their main idea is to exploit the feature of the problem that the error terms are relatively small and the product of the secret primes is given. More precisely, one can try a brute-force attack to recover a secret prime p_i from a multiple $N = \prod_{i=0}^{n} p_i$ and an sample of CCK-ACD represented by $b = p_i \cdot q_i + r_i$ for some fixed i, where an integer $r_i \in (-2^\rho, 2^\rho)$ except $i = 0$. The method is to compute the greatest common divisor between (GCD) $b - a$ and N for all integers $a \in (-2^\rho, 2^\rho)$. It would have time complexity $\tilde{O}(2^\rho)$, so ρ should be set to $\Omega(\lambda)$ for the security parameter λ. Furthermore, the methods of [CN12] and [CNT12], which were proposed as variants of exhaustive search to solve (P)ACD in $\tilde{O}(2^{\rho/2})$ time complexity, can be applied to solve the CCK-ACD problem due to the feature

[1] We describe formal definition of the CCK-ACD problem in Section 2.

mentioned previously. In addition, one can also use the factorization with the elliptic curve method to find a factor of N in $2^{\tilde{O}(\sqrt{\eta})}$ time complexity, where η is the log-size of p_i. Thus, η should be set to $\Omega(\lambda^2)$ for the security parameter λ.

As another trial to solve CCK-ACD, authors in [13] considered well-known algorithms for solving PACD such as orthogonal lattice attack method (OLA) and simultaneous Diophantine approximation (SDA) [6,11,15,18] in the context of CCK-ACD. The SDA and OLA make use of a lattice reduction algorithm for a specific lattice whose entries consist of given PACD samples and a multiple $N = \prod_{i=0}^{n} p_i$. If one can obtain a short vector from the lattice by the lattice reduction algorithm, it leads to solve the PACD problem utilizing the coordinates of the vector. Since these algorithms for (P)ACD have the time complexity depending on η and γ, one can expect an expansion of the algorithms to the CCK-ACD problem will provide answers for our main question.

However, if one constructs a lattice as similar to SDA and OLA to solve CCK-ACD, there exist several short vectors of similar length in the lattice due to the symmetry of p_i. Thus if short vector from the lattice by a lattice reduction algorithm is a short linear combination of several of these vectors, one cannot extract information about a certain prime p_i from the vector.

Independent work. Recently, Coron and Pereira [9] proposed an algorithm for solving multi-prime ACD problem which is exactly the same as the 'search' CCK-ACD problem in this paper. The main idea of the attack is also the same as our SDA-style algorithm that combines the SDA with algebraic steps from the Cheon *et al.* [5]. In this paper, we also propose another OLA-style algorithm for solving 'decisional' CCK-ACD problem using OLA with a new distinguisher determinant.

1.1 Our Work

In this paper, we propose two mathematical algorithms to solve the CCK-ACD problem by extending the OLA and SDA methods that are well-known for solving the ACD problem using lattice technique. Both algorithms take the same time complexity $2^{O\left(\frac{\gamma}{(\eta-\rho)^2}\right)}$ up to polynomial factors for the bit-size of samples γ, secret primes η and error ρ. Our algorithms are the first algorithms related to η and γ to solve the CCK-ACD problem.

Let b_j be a CCK-ACD sample of $b_j \equiv r_{ij} \bmod p_i$ for $1 \leq j \leq k$ and $0 \leq i \leq n$. Technically, the classical OLA algorithm on input b_j outputs a lattice which includes a short vector $\vec{r_i} = (r_{i1}, \ldots, r_{ik})$ for $1 \leq i \leq n$, while the algorithm on γ-bit random integers gives a random lattice. Then, the next step is to recover the short vector $\vec{r_i}$ from the lattice and p_i by computing the GCD between $b_j - r_{ji}$ and $N = \prod_{i=0}^{n} p_i$. If the last step reveals a non-trivial factor of N, we can conclude

that the b_j's are CCK-ACD samples. Unfortunately, it is a hard task to recover the vector $\vec{r}_i$ except for small n since a short vector from the lattice can be a short linear combination of several $\vec{r}_i$'s. Instead, we employ a determinant of the lattice as a new distinguisher to solve the decision CCK-ACD problem. We show that a sub-lattice of the output lattice of the classic OLA has a different-sized determinant depending on the type of inputs. Then, computing determinant enables us to avoid the obstacle to find the exact vector $\vec{r}_i$. The overall time complexity heavily depends on the cost of a lattice reduction to find a short vector.

We also propose a SDA-style algorithm to find all secret parameters in the CCK-ACD problem beyond the decision problem. It consists of two steps; find a short vector using a lattice reduction algorithm and then recover the factors $p_1, \cdots, p_n$ by employing the Cheon *et al.*'s technique [5]. More precisely, we build a lattice as similar to the SDA approach on the ACD problem, and obtain an integer of the form $\sum_{i=1}^{n} c_i \cdot N/p_i$ for some small integers c_i, which is called *dual instance*. The dual instance allows us to apply the similar method to the Choen *et al.*'s technique, which converts modulo equations into integer equations by exploiting the CRT properties of CCK-ACD samples and its relation to dual instance. The complexity of the new algorithm heavily depends on the first step, so it takes time complexity as stated above.

We provide experimental results to guarantee that our algorithms work well both in theoretical and experimental terms under the various parameters of CCK-ACD. We observe the OLA is more practical than SDA while the asymptotic complexities are the same.

Organization. In Section 2, we introduce preliminary information related to the lattice. Next, we revisit the OLA to solve the CCK-ACD problem in Section 3. Also, we extend the SDA algorithm in the context of CCK-ACD and propose the first algorithm which recovers all secret primes p_i's of the CCK-ACD problem in Section 4. In addition, we present some experimental results for our algorithms in Section 5.

2 Preliminaries

Notation. Throughout this paper, we use $a \leftarrow A$ to denote the operation of uniformly choosing an element a from a finite set A or generating a sample according to a distribution A. We let $\mathbb{Z}_q$ denote the set $\mathbb{Z} \cap (-q/2, q/2]$ for the positive integer q. We use the notation $[t]_p$ to denote the integer in $\mathbb{Z}_p$ congruent to t mod p. We define $\mathsf{CRT}_{(p_1,p_2,\ldots,p_n)}(r_1, r_2, \ldots, r_n)$ (or abbreviated as $\mathsf{CRT}_{(p_i)}(r_i)$) for pairwise co-prime integers $p_1, p_2, \ldots, p_n$ as the integer in $\left(-\frac{1}{2}\prod_{i=1}^{n} p_i, \frac{1}{2}\prod_{i=1}^{n} p_i\right]$ congruent to r_i in the modulus p_i for each $i \in \{1, 2, \ldots, n\}$.

We use bold letters to denote vectors or matrices and denote the set of all $m \times n$ matrices over $\mathbb{Z}$ by $\mathbb{Z}^{m\times n}$. For matrix $\mathbf{A}$, we denote the transpose of $\mathbf{A}$ by $\mathbf{A}^T$ and denote the i-th row vector of $\mathbf{A}$ by $[\mathbf{A}]_i$. When $\mathbf{A} = (a_{i,j}) \in \mathbb{Z}^{m\times n}$ is given, we define the infinite norm $\|\mathbf{A}\|_\infty$ as $\max_{1\le j\le n} \sum_{i=1}^{n} |a_{i,j}|$ and use the notation $\mathbf{A} \bmod N$ to denote the matrix $([a_{i,j}]_N) \in \mathbb{Z}^{m\times n}$. We denote by $\mathsf{diag}(a_1, \ldots, a_n)$ the diagonal matrix with diagonal coefficients $a_1, \ldots, a_n$. When $\mathbf{B}$ is an integral matrix, we define $size(\mathbf{B})$ as the logarithm of the largest entries of $\mathbf{B}$.

For a vector $\vec{v} = (v_1, \ldots, v_n)$, we define the ℓ_2-norm $\|\vec{v}\|_2$ (or abbreviated as $\|\vec{v}\|$) and ℓ_1-norm $\|\vec{v}\|_1$ as $\sqrt{\sum_{i=1}^{n} {v_i}^2}$ and $\sum_{i=1}^{n} |v_i|$, respectively.

2.1 Lattices

A lattice Λ is a discrete additive subgroup of $\mathbb{R}^n$. We call a set of linearly independent vectors $\mathbf{B} = \{\vec{b}_1, \vec{b}_2, \cdots, \vec{b}_m\} \subset \mathbb{R}^n$ a basis of a lattice Λ if Λ is the set of all $\mathbb{Z}$-linear combinations of the vectors $\vec{b}_1, \vec{b}_2, \cdots, \vec{b}_m$. We denote such lattice Λ generated by the basis $\mathbf{B}$ by $\Lambda(\mathbf{B})$. We sometimes use the notation Λ instead of $\Lambda(\mathbf{B})$. Especially, when a lattice Λ is a subset of $\mathbb{Z}^n$, it is called an integral lattice. Throughout this work, we only consider the integral lattice and regard a lattice as an integral lattice without special mention. If we regard a basis $\mathbf{B} = \{\vec{b}_1, \vec{b}_2, \cdots, \vec{b}_m\}$ of lattice Λ as a matrix whose column vectors consist of vectors $\vec{b}_i$ for $1 \le i \le m$, $\mathbf{B}$ is called a basis matrix of Λ. The rank and determinant of lattice Λ is defined as m and $\det(\Lambda) = \sqrt{\det(\mathbf{B}^T\mathbf{B})}$ for any basis matrix $\mathbf{B}$, respectively. When $n = m$, this lattice is called a full-rank lattice and $\det(\Lambda) = \det(\mathbf{B})$ holds. Throughout this paper, we denote lattice Λ whose basis vectors are $\vec{b}_1, \vec{b}_2, \cdots, \vec{b}_m$ as $\Lambda = \left\langle \vec{b}_1, \vec{b}_2, \cdots, \vec{b}_m \right\rangle$.

It is known that for a lattice $\Lambda = \Lambda(\mathbf{B}) \in \mathbb{R}^n$ with basis $\mathbf{B} = \{\vec{b}_1, \vec{b}_2, \cdots, \vec{b}_m\}$, the following holds

$$\det(\Lambda) \le \prod_{i=1}^{m} \|\vec{b}_i\|$$

In addition, when a set of column vectors $\mathbf{U} = \{\vec{u}_1, \vec{u}_2, \cdots, \vec{u}_k\} \subset \mathbb{Z}^n$ is given, we define the orthogonal lattices

$$\Lambda^{\perp}(\mathbf{U}) := \{\vec{v} \in \mathbb{Z}^n \mid \langle \vec{v}, \vec{u}_j \rangle = 0 \textit{ for all } 1 \le j \le k\}.$$

$$\Lambda_q^{\perp}(\mathbf{U}) := \{\vec{v} \in \mathbb{Z}^n \mid \langle \vec{v}, \vec{u}_j \rangle \equiv 0 \bmod q \textit{ for all } 1 \le j \le k\}.$$

Successive Minima. Let Λ be a lattice of rank n. The successive minima of Λ are $\lambda_1, \cdots, \lambda_n \in \mathbb{R}$ such that, for any $1 \le i \le n$, λ_i is minimal such that there exist i linearly independent vectors $\vec{v}_1, \ldots, \vec{v}_i \in \Lambda$ with $\|\vec{v}_j\| \le \lambda_i$ for $1 \le j \le i$.

There is a useful result, which is called the Gaussian Heuristic [1] to reduce the size of successive minima.

Gaussian Heuristic. Let Λ be a rank-n lattice. The Gaussian Heuristic states that the size of successive minima of Λ is approximately as follows.

$$\lambda_i(\Lambda) \approx \sqrt{\frac{n}{2\pi e}} \det(\Lambda)^{1/n} \quad \text{for all} \quad i \in \{1, 2, \cdots, n\}.$$

Ajtai showed that the above equation holds for a random lattice with overwhelming probability [1].

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 [16] and the BKZ algorithm [14] are well-known lattice reduction algorithms. We mainly use BKZ algorithms to find an approximately short vector of a lattice. According to [14], the block size β of the BKZ algorithm determines how short the output vector of the BKZ algorithm is. With the BKZ algorithm to the rank-n lattice Λ with basis matrix $\mathbf{B}$, we can get a short vector $\mathbf{v}$ in poly(n, $size(\mathbf{B})$) $\cdot\, \mathcal{C}_{HKZ}(\beta)$ times which satisfies the following

$$\|\vec{v}\| \leq \min\{2(\gamma_\beta)^{\frac{n-1}{2(\beta-1)}+\frac{3}{2}} \cdot (\det\Lambda)^{1/n}, 4(\gamma_\beta)^{\frac{n-1}{\beta-1}+3} \cdot \lambda_1(\Lambda)\},$$

where $\gamma_\beta \leq \beta$ is the Hermite constant of a rank-β lattice and $\mathcal{C}_{HKZ}(\beta)$ denotes the time spent to get the shortest vector of a rank-β lattice and can be regarded as $2^{O(\beta)}$.

In the case of LLL algorithm, according to [16], the LLL algorithm upon the rank-n lattice Λ with basis matrix $\mathbf{B}$ gives an LLL-reduced basis $\{\vec{b}_1, \cdots, \vec{b}_n\}$ in poly(n, $size(\mathbf{B})$) times which satisfies the following

$$\|\vec{b}_1\| \leq 2^{\frac{n-1}{4}} \cdot (\det\Lambda)^{1/n}, \ \|\vec{b}_i\| \leq 2^{\frac{n-1}{2}} \cdot \lambda_i(\Lambda) \text{ for } 1 \leq i \leq n.$$

In particular, it is known that a LLL-reduced basis $\{\vec{b}_1, \vec{b}_2, \cdots, \vec{b}_m\} \subset \mathbb{R}^n$ with $\delta = 1/4 + 1/\sqrt{2} \approx 0.957$ for a lattice Λ, the following holds

$$\|\vec{b}_j\| \leq 2^{i/4} \cdot \|\vec{b}_i^*\| \text{ for } 1 \leq j \leq i \leq m. \tag{2.1}$$

when we let $\{\vec{b}_1^*, \cdots \vec{b}_m^*\}$ be the Gram-Schmidt orthogonalization.

For convenience of calculation, throughout this paper, we use $\mathcal{A}_\delta$ to denote a lattice reduction whose output contains a short vector $\vec{v}$ with Euclidean norm less than $\delta^n \cdot \det(\Lambda)^{1/n}$ or $\delta^{2n} \cdot \lambda_1(\Lambda)$ for an n-dimensional lattice Λ instead of

$2(\gamma_\beta)^{\frac{n-1}{2(\beta-1)}+\frac{3}{2}} \cdot (\det \Lambda)^{1/n}$ or $4(\gamma_\beta)^{\frac{n-1}{\beta-1}+3} \cdot \lambda_1(\Lambda)$, respectively. In this case, the root Hermite factor δ is achieved in time $2^{O(1/\log \delta)} \cdot poly(k)$ by the BKZ algorithm with block size $\beta = \Theta(\frac{1}{\log \delta})$.

Now we given the formal definition of the CCK-ACD problem, our main concern in this paper.

Definition 2.1. (CCK-ACD) Let γ, n, η, ρ be positive integers such that 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 distribution $\mathcal{D}_{\gamma,\eta,\rho,n}(p_i)$ is defined as

$$\mathcal{D}_{\gamma,\eta,\rho,n}(p_i) = \{T \cdot \prod_{i=1}^{n} p_i + \mathsf{CRT}_{(p_i)}(r_i) \mid T \leftarrow \mathbb{Z} \cap [2^{\gamma-1}/\prod_{i=1}^{n} p_i, 2^\gamma/\prod_{i=1}^{n} p_i),\ r_i \leftarrow \chi_\rho\}.$$

The (γ, η, ρ)-CCK-ACD problem is: For given $N = p_0 \cdot \prod_{i=1}^{n} p_i$ for uniformly chosen $p_0 \in \mathbb{Z} \cap [2^{\gamma-1}/\prod_{i=1}^{n} p_i,\ 2^\gamma/\prod_{i=1}^{n} p_i)$ and polynomially many samples from $\mathcal{D}_{\gamma,\eta,\rho,n}(p_i)$ or χ_γ, distinguish CCK-ACD samples from random samples.

In the CCK-ACD problem, we use $r_{0,j}$ to denote $b_j \bmod p_0$ for each $j \in \{1, \cdots, k\}$, where $b_j \in \mathcal{D}_{\gamma,\eta,\rho,n}(p_i)$'s are given as CCK-ACD samples. We remark that $r_{0,j}$ may not be small, unlike other $r_{i,j}$ for $i \in \{1, \cdots, n\}$.

3 OLA for the CCK-ACD Problem

In this section, we revisit the orthogonal lattice attack method (OLA) and explain how to guarantee the upper bound of the OLA proposed in [8] for the CCK-ACD problem in time $2^{O\left(\frac{\gamma}{(\eta-\rho)^2}\right)}$ using determinant of lattice.

Our orthogonal lattice attack for the CCK-ACD problem consists of two steps. The first step of our algorithm is exactly the same as the previous OLA approach for solving the ACD problem. Next we compute a determinant of the orthogonal lattice in the second step.

We find the upper bound of determinant exploiting CRT-structure of CCK-ACD samples and it can be a distinguisher of CCK-ACD and random samples. In this section, for the CCK-ACD samples, we show that the size of determinant is bounded by $2^{\frac{n+1}{4}+n(\rho+\log k)}$, where k denotes the optimized number of CCK-ACD samples, under the Gaussian Heuristic. In the case of random elements, our algorithm outputs a determinant larger than the value. From the results, we can solve the CCK-ACD problem.

Algorithm 1 `Algorithm for the CCK-ACD problem`

Input: γ-bit integer $N = \prod_{i=0}^{n} p_i$
Input: Root Hermite factor δ
Input: $\vec{b} = (b_1, b_2, \cdots, b_k)$, where $k = n + \left\lfloor \sqrt{\frac{\gamma}{2 \log \delta}} \right\rfloor$
Output: distinguish whether b_i's are sampled from $\mathcal{D}_{\gamma,\eta,\rho,n}(p_i)$ or a χ_γ.

1: Construct a lattice $\Lambda_N^{\perp}(\vec{b})$ with basis matrix $\mathbf{U} = \begin{pmatrix} N & [-b_2/b_1]_N & \cdots & [-b_k/b_1]_N \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$.
2: $\vec{u}_1, \vec{u}_2, \cdots, \vec{u}_{k-n-1} \leftarrow \mathcal{A}_\delta(\Lambda_N^{\perp}(\vec{b}))$
3: Construct an orthogonal lattice $\Lambda^{\perp}(\tilde{\mathbf{U}})$ for $\tilde{\mathbf{U}} = (\vec{u}_1 \mid \cdots \mid \vec{u}_{k-n-1})$ and its basis $\mathbf{B}$.
4: $\mathbf{B} \leftarrow$ LLL-reduced basis of $\Lambda(\mathbf{B})$ and remove the largest column vector of $\mathbf{B}$.
5: **if** $\log(\det(\Lambda(\mathbf{B}))) \leq \frac{n+1}{4} + n(\rho + \log k)$ **then**
6: **return** $\mathcal{D}_{\gamma,\eta,\rho,n}(p_i)$
7: **else**
8: **return** χ_γ.
9: **end if**

OLA for the CCK-ACD problem.

Assume that we have k CCK-ACD samples $\{b_j = \mathsf{CRT}_{(p_i)}(r_{i,j})\}_{1 \leq j \leq k}$ with $N = \prod_{i=0}^{n} p_i$, and let $\vec{b} = (b_1, \cdots, b_k)^T$, $\vec{r}_i = (r_{i,1}, \cdots, r_{i,k})^T$ for $0 \leq i \leq n$.

The first step of OLA, which is described in [8, Section 5.1], is to find the set of short vectors $\{\vec{u}_1, \cdots, \vec{u}_{k-n-1}\}$ in a k-dimensional lattice

$$\Lambda_N^{\perp}(\vec{b}) = \{\vec{u} \in \mathbb{Z}^k \mid \langle \vec{u}, \vec{b} \rangle \equiv 0 \mod N\}.$$

Since $b_j \equiv r_{i,j} \bmod N$, we observe the relations using the CRT structure

$$\begin{pmatrix} r_{0,1} & r_{1,1} & \cdots & r_{n,1} \\ r_{0,2} & r_{1,2} & \cdots & r_{n,2} \\ \vdots & \vdots & \ddots & \vdots \\ r_{0,k} & r_{1,k} & \cdots & r_{n,k} \end{pmatrix} \cdot \begin{pmatrix} (\hat{p}_0^{-1} \bmod p_0) \cdot \hat{p}_0 \\ (\hat{p}_1^{-1} \bmod p_1) \cdot \hat{p}_1 \\ \vdots \\ (\hat{p}_n^{-1} \bmod p_n) \cdot \hat{p}_n \end{pmatrix} \equiv \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_k \end{pmatrix} \mod N.$$

If a vector $\vec{u} \in \mathbb{Z}^k$ satisfies $\langle \vec{u}, \vec{r}_i \rangle = 0$ in integers for all $i = 0, \cdots, n$, then $\langle \vec{u}, \vec{b} \rangle \equiv 0 \bmod N$ because of the above relations. Thus, it holds that

$$\Lambda^{\perp}(\{\vec{r}_0, \cdots, \vec{r}_n\}) \subset \Lambda_N^{\perp}(\vec{b})$$

Moreover, we observe $\lambda_i(\Lambda_N^{\perp}(\vec{b})) \leq \lambda_i(\Lambda^{\perp}(\{\vec{r}_0, \cdots, \vec{r}_n\}))$ by the definition of successive minima for all $1 \leq i \leq k - n - 1$.

We assume the Gaussian heuristic holds on the lattice $\Lambda^{\perp}(\{\vec{r}_0, \cdots, \vec{r}_n\})$ since all components of $\vec{r}_i$ with $0 \leq i \leq n$ are uniformly chosen from each set. Therefore, it holds that

$$\log |\lambda_i(\Lambda^{\perp}(\{\vec{r}_0, \cdots, \vec{r}_n\}))| \approx \frac{\gamma - n\eta + n\rho}{k - n - 1}$$

for all $i = 1, 2, \cdots, k - n - 1$. Note that we omit the small values including $\log k$ for the convenience of writing.

To obtain such short vectors $\vec{w}_j$'s, we run a lattice reduction algorithm $\mathcal{A}_\delta$ with root Hermite factor δ on the lattice $\Lambda_N^{\perp}(\vec{b})$. By the approximate factor δ of a lattice reduction algorithm $\mathcal{A}_\delta$, the j-th output vector $\vec{w}_j$ of $\mathcal{A}_\delta$ on the lattice $\Lambda_N^{\perp}(\vec{b})$ satisfies $\|\vec{w}_j\| \leq \delta^{2k} \cdot \lambda_j(\Lambda_N^{\perp}(\vec{b}))$. Thus, for all $j = 1, 2, \cdots, k - n - 1$, $\vec{w}_j$ is bounded as follows

$$\begin{aligned}\|\vec{w}_j\| &\leq \delta^{2k} \cdot \lambda_j(\Lambda_N^{\perp}(\vec{b})) \leq \delta^{2k} \cdot \lambda_i(\Lambda^{\perp}(\{\vec{r}_0, \cdots, \vec{r}_n\})) \\ &\leq \delta^{2k} \cdot 2^{\frac{\gamma - n\eta + n\rho}{k-n-1}}.\end{aligned}$$

By the Cauchy-Schwartz inequality, it holds for $1 \leq i \leq n, 1 \leq j \leq k - n - 1$

$$\begin{aligned}|\langle \vec{w}_j, \vec{r}_i \rangle| &\leq \|\vec{w}_j\| \cdot \|\vec{r}_i\| \\ &< (\delta^{2k} \cdot 2^{\frac{\gamma - n\eta + n\rho}{k-n-1}}) \cdot (k \cdot 2^{\rho}) \\ &\approx 2^{2k \log \delta + \frac{\gamma - n\eta + n\rho}{k-n-1}} \cdot 2^{\rho}\end{aligned}$$

Since p_i's are η-bit primes, we can ensure the vector $\vec{w}_j \in \Lambda_N^{\perp}(\vec{b})$ obtained from $\mathcal{A}_\delta$ satisfies $|\langle \vec{w}_j, \vec{r}_i \rangle| < p_i/2$ under the following condition

$$2k \cdot \log \delta + \frac{\gamma - n\eta + n\rho}{k - n - 1} + \rho \leq \eta, \tag{3.1}$$

$$2(k - n - 1) \cdot \log \delta + \frac{\gamma}{k - n - 1} \leq \frac{(k-1)(\eta - \rho)}{k - n - 1} - 2(n+1) \log \delta.$$

When we choose $k - n - 1 = \sqrt{\frac{\gamma}{2 \log \delta}}$ and apply the AM-GM inequality, it is enough to satisfy $\log \delta$ as following inequality

$$2\sqrt{2\gamma \log \delta} \leq \eta - \rho.$$

Therefore, when we obtain $k \approx n + \sqrt{\frac{\gamma}{2 \log \delta}}$ CCK-ACD samples and choose δ

satisfying $\log \delta < \frac{(\eta-\rho)^2}{8\gamma} - \epsilon$ for some small ϵ, $|\langle \vec{w}_j, \vec{r}_i \rangle| \leq p_i/2$ is established for any $1 \leq i \leq n$. Thus, $\{\vec{w}_j\}_{1 \leq j \leq k-n-1}$ are the set of short vectors what we want, renamed by $\{\vec{u}_j\}_{1 \leq j \leq k-n-1}$, and the overall time complexity to compute small $\vec{w}_j$'s is $2^{O\left(\frac{\gamma}{(\eta-\rho)^2}\right)} \cdot poly(k) \approx 2^{O\left(\frac{\gamma}{(\eta-\rho)^2}\right)}$ up to polynomial factors.

As the second step, we construct an orthogonal lattice to the lattice generated by $\{\vec{u}_j\}$, instead of computing $\vec{r}_i$ directly. More precisely, let $\tilde{\mathbf{U}}$ denote a matrix $(\vec{u}_1 \,|\, \cdots \,|\, \vec{u}_{k-n-1})$ and consider the orthogonal lattice

$$\Lambda^{\perp}(\tilde{\mathbf{U}}) = \{\vec{v} \in \mathbb{Z}^k \mid \langle \vec{v}, \vec{u}_j \rangle = 0 \textit{ for all } 1 \leq j \leq k-n-1\}.$$

Due to the CRT-structure of CCK-ACD samples, $\{\vec{r}_i\}_{1 \leq i \leq n}$ are short linearly independent vectors that belong to $\Lambda^{\perp}(\tilde{\mathbf{U}})$.[2] The lattice $\Lambda^{\perp}(\tilde{\mathbf{U}}) \subset \mathbb{Z}^k$ has rank $n+1$ so there exists a basis $\mathbf{B} = \{\vec{b}_1, \cdots, \vec{b}_{n+1}\}$. We apply the LLL algorithm on the basis $\mathbf{B}$ of $\Lambda^{\perp}(\tilde{\mathbf{U}})$ to obtain $\mathbf{B}' = \{\vec{b}'_1, \cdots, \vec{b}'_{n+1}\}$, the LLL-reduced basis of $\mathbf{B}$. In this case, the required time complexity is $poly(n, size(\Lambda^{\perp}(\tilde{\mathbf{U}})))$, which is dominated by $2^{O\left(\frac{\gamma}{(\eta-\rho)^2}\right)}$.

Since $\{\vec{r}_i\}_{1 \leq i \leq n}$ are n linearly independent vectors in $\Lambda^{\perp}(\tilde{\mathbf{U}})$, there exists a vector $\vec{b}'_j$ such that $\{\vec{r}_1, \cdots, \vec{r}_n, \vec{b}'_j\}$ are $n+1$ linearly independent vectors in $\Lambda^{\perp}(\tilde{\mathbf{U}})$. Additionally, $\|\vec{r}_i\|$ is smaller than $k \cdot 2^{\rho}$ for all i, we note that $\lambda_n(\Lambda^{\perp}(\tilde{\mathbf{U}})) \leq 2^{\rho + \log k}$. Let $\tilde{B}' = \{\vec{b}'^*_1, \cdots, \vec{b}'^*_{n+1}\}$ be Gram-Schmidt basis of B'. Then we calculate the determinant of lattice Λ' spanned by $\{\vec{b}'_1, \cdots, \vec{b}'_n\}$.

$$\begin{aligned}
\det(\Lambda') = \prod_{i=1}^{n} \|\vec{b}'^*_i\| &= \frac{\prod_{i=1}^{n+1} \|\vec{b}'^*_i\|}{\|\vec{b}'^*_{n+1}\|} \\
&= \frac{\det(\Lambda^{\perp}(\tilde{\mathbf{U}}))}{\|\vec{b}'^*_{n+1}\|} \leq \frac{\|\vec{b}'_j\| \cdot \prod_{i=1}^{n} \|\vec{r}_i\|}{\|\vec{b}'^*_{n+1}\|} \\
&\leq \|\vec{b}'_j\| \cdot \prod_{i=1}^{n} \|\vec{r}_i\| \cdot \frac{2^{\frac{n+1}{4}}}{\|\vec{b}'_j\|} \text{ (By inequality (2.1))} \\
&\leq 2^{\frac{n+1}{4} + n(\rho + \log k)}
\end{aligned}$$

According to the analysis above, the log-size of determinant of the rest n column vectors after LLL algorithm is smaller than $\frac{n+1}{4} + n(\rho + \log k)$ with $k - n - 1 \approx \sqrt{\frac{\gamma}{2 \log \delta}} \approx \frac{2\gamma}{\eta - \rho}$. Then we guess that the determinant of the rest n column vectors

[2] We can assume that $\{\vec{r}_i : 1 \leq i \leq n\}$ are n linearly independent vectors because their entries are randomly chosen in χ_ρ.

after LLL algorithm is small when $\vec{b}$ is a CCK-ACD instance.

Heuristic analysis of random instance.

To analyze the size of determinant heuristically, we first assume that the logarithm of determinant of rank-n lattice is approximately $n \log B$, when each entry of a basis matrix is uniformly sampled from $[-2^B, 2^B]$. This approximation agrees the bound from Hadamard inequality, and for square matrix it is known to hold up to difference $\Theta(n \log n)$ assuming that entries are uniform [17]. In our case, $n \log n$ is negligibly small compared to other term.

- Random instances: We assume that the expected size of $\vec{u}_j$, a j-th output of the lattice reduction algorithm, are $\delta^k \cdot N^{1/k}$ for all $1 \leq j \leq k-n-1$, which agrees to the expected size of the shortest output of lattice reduction algorithm. We may suppose that these vectors are random since given instances are random. Then, the logarithm of the determinant of $\Lambda(\tilde{\mathbf{U}})$ is approximately

$$\frac{k-n-1}{k} \log N + (k-n-1)k \log \delta \approx \frac{k-n-1}{k} \cdot \gamma,$$

  since the second term is relatively small to the first term. The assumption that the basis vector of $\Lambda(\tilde{\mathbf{U}})$ is random also allows us to assume that $\det(\Lambda(\tilde{\mathbf{U}}))$ and $\det(\Lambda^{\perp}(\tilde{\mathbf{U}}))$ are the same. Then we obtain the desired result that the logarithm of determinant of $\Lambda^{\perp}(\tilde{\mathbf{U}})$ is approximately $\gamma \cdot \frac{k-n-1}{k}$. Under the same assumption, the expected size of vectors obtained as a result of the LLL algorithm are $2^{n/4} \cdot \det(\Lambda^{\perp}(\tilde{\mathbf{U}}))^{\frac{1}{n+1}}$. Then the logarithm of determinant of the matrix composed by n short vectors is approximately

$$\frac{n}{n+1} \cdot \frac{k-n-1}{k} \cdot \gamma + \frac{n^2}{4} \approx \frac{n}{n+1} \cdot \frac{k-n-1}{k} \cdot \gamma,$$

  since the second term is relatively small. The experimental result shows that this approximation roughly holds.

In summary, under Gaussian Heuristic and assumption from Hadamard inequality, we show that the logarithm of the determinant is less than $\frac{n+1}{4} + n(\rho + \log k)$ if the given instances are the CCK-ACD instances whereas it is approximately $\gamma \cdot \frac{k-n-1}{k} \cdot \frac{n}{n+1}$ for the random instances. We will see that the experimental results fit this approximation well in Section 5.

4 SDA Algorithm for the CCK-ACD problem

In this section, we first describe a lattice-based algorithm to solve the CCK-ACD problem by applying the Simultaneously Diophantine approximation (SDA) algorithm which has been served as a useful method to solve the ACD problem.

In the paper [13], Galbraith *et al.* try to apply the SDA algorithm in the context of CCK-ACD and comment that this attack is not directly applicable to the CCK-ACD problem. Reviewing this work, one can consider a column lattice Λ generated by a matrix $\mathbf{B}$

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

with given CCK-ACD samples $b_j = \mathsf{CRT}_{(p_i)}(r_{i,j})$ for each $1 \leq j \leq k$ and $N = \prod_{i=0}^{n} p_i$. It follows that the lattice contains the short vectors

$$\vec{v_i} = \hat{p}_i \cdot (1, r_{i,1}, r_{i,2}, \cdots, r_{i,k})^T.$$

for all $1 \leq i \leq n$ and these all have similar lengths. Once we compute $\hat{p}_i$ from the first entry of the vector, we can recover the prime factors $p_i = N/\hat{p}_i$. But if $\vec{u} = (u_0, u_1, \cdots, u_k) \in \Lambda$ is a short linear combination of several these vectors, *i.e.*, $\vec{u} = \sum_{i=1}^{n} e_i \cdot \vec{v_i}$, we cannot expect that $\lfloor N/u_0 \rceil$ is one of the primes of N, where $u_0 = \sum_{i=1}^{n} e_i \cdot \hat{p}_i$.

However, an instance of the form $d = \sum_{i=1}^{n} d_i \cdot \hat{p}_i$ with small d_is has a special property. More precisely, if we can ensure that d_i's are sufficiently small, the instance $d = \sum_{i=1}^{n} d_i \cdot \hat{p}_i$ enables the below modular equations to be established without modulus N due to CRT-structure of CCK-ACD samples.

$$[d \cdot b_j]_N = [\sum_{i=1}^{n} d_i \cdot b_j \cdot \hat{p}_i]_N = \sum_{i=1}^{n} d_i \cdot r_{i,j} \cdot \hat{p}_i \in \mathbb{Z}$$

$$[d \cdot b_j \cdot b_l]_N = \sum_{i=1}^{n} d_i \cdot r_{i,j} \cdot r_{i,l} \cdot \hat{p}_i \in \mathbb{Z}$$

This property plays the crucial role when solving the CCK-ACD problem and even recovering the secret primes in our algorithm. In Section 4.1, we define

a dual instance to give a standard for how small d_i's should be in an instance $d = \sum_{i=1}^{n} d_i \cdot \hat{p}_i$. Once we obtain such dual instances, we modify Cheon *et al.*'s algorithm in [5] to solve the CCK-ACD problem using the dual instances, which is the second step of our algorithm for solving the CCK-ACD problem.

The first step of our algorithm to solve the CCK-ACD problem is to obtain a dual instance. To do so, we build the $(k+1)$-dimensional lattice $\Lambda = \Lambda(\mathbf{B})$, where $\mathbf{B}$ is the same basis matrix as above. We will later show that if $\vec{v}$ is a sufficiently short vector in Λ, its first entry can be regarded as a dual instance. To understand a lattice vector $\vec{v}$ of Λ, we note that any integer d can be written as the form of $d = \sum_{i=0}^{n} d_i \cdot \hat{p}_i$ for some integers d_i's since $\gcd(\hat{p}_0, \hat{p}_1, \cdots, \hat{p}_n) = 1$. Using this property, if we denote the first entry of the vector $\vec{v}$ from Λ by $d = \sum_{i=0}^{n} d_i \cdot \hat{p}_i$, the following modular equations hold.

$$\vec{v} \equiv \begin{pmatrix} d \\ [d \cdot b_1]_N \\ [d \cdot b_2]_N \\ \vdots \\ [d \cdot b_k]_N \end{pmatrix} \equiv \begin{pmatrix} \sum_{i=0}^{n} d_i \cdot \hat{p}_i \\ \sum_{i=0}^{n} d_i \cdot r_{i,1} \cdot \hat{p}_i \\ \sum_{i=0}^{n} d_i \cdot r_{i,2} \cdot \hat{p}_i \\ \vdots \\ \sum_{i=0}^{n} d_i \cdot r_{i,k} \cdot \hat{p}_i \end{pmatrix} \pmod{N}$$

Using the above modular equation, we investigate the condition of the length of vector $\vec{v}$ which enables an instance $d = \sum_{i=0}^{n} d_i \cdot \hat{p}_i$, the first entry of $\vec{v}$, to be a dual instance in Section 4.2.

4.1 Revisiting the Algorithm of Cheon *et al.*

In this section, we revisit the Cheon *et al.*'s algorithm in [5] to solve the CCK-ACD problem. In the original paper, the authors presented an algorithm when an auxiliary input $\mathsf{CRT}_{(p_i)}(\hat{p}_i) = \sum_{i=1}^{n} \hat{p}_i$ is given.

However, in order to use an instance $d = \sum_{i=1}^{n} d_i \cdot \hat{p}_i$ in Cheon *et al.*'s algorithm, all of d_i's need not be 1. If d_i's are sufficiently small, $d = \sum_{i=1}^{n} d_i \cdot \hat{p}_i$ can also play the same role as an auxiliary input. From this, we define a dual instance for the CCK-ACD problem, which is a generalization of an auxiliary input and introduce a polynomial-time algorithm to solve the CCK-ACD problem when two dual

instances are given instead of one auxiliary input by slightly modifying Cheon *et al.*'s algorithm.

Definition 4.1 (Dual Instance). Let n, η, ρ be positive integers. For given η-bit primes $p_1, \cdots, p_n$ and $p_0 \in \mathbb{Z} \cap [2^{\gamma-1}/\prod_{i=1}^{n} p_i, 2^{\gamma}/\prod_{i=1}^{n} p_i)$ in CCK-ACD, define $N = \prod_{i=0}^{n} p_i$ and $\hat{p}_i = N/p_i$, for $0 \le i \le n$. We define a dual instance d as the integer which can be written as $d = \sum_{i=0}^{n} d_i \cdot \hat{p}_i$ for some integers d_i's satisfying $|d_i| \le p_i \cdot 2^{-2\rho - \log n - 1}$ for each $1 \le i \le n$ and $d_0 = 0$.

An algorithm to generate a dual instance when given polynomially many CCK-ACD samples will be described in Section 4.2.

For an integer $d = \sum_{i=0}^{n} d_i \cdot \hat{p}_i$ and CCK-ACD samples $b_j = \mathsf{CRT}_{(p_i)}(r_{i,j})$ and $b_l = \mathsf{CRT}_{(p_i)}(r_{i,l})$, one can check the followings

$$[d]_N \equiv \sum_{i=0}^{n} d_i \cdot \hat{p}_i \pmod{N}, \tag{4.1}$$

$$[d \cdot b_j]_N \equiv \sum_{i=0}^{n} d_i \cdot r_{i,j} \cdot \hat{p}_i \pmod{N}, \tag{4.2}$$

$$[d \cdot b_j \cdot b_l]_N \equiv \sum_{i=0}^{n} d_i \cdot r_{i,j} \cdot r_{i,l} \cdot \hat{p}_i \pmod{N}. \tag{4.3}$$

Under the condition that each size of d_i is sufficiently small for $1 \le i \le n$ and $d_0 = 0$, the above equations hold over the integers, not modulo N. In other words, for a dual instance $d = \sum_{i=1}^{n} d_i \cdot \hat{p}_i$ defined as above, the following inequalities hold

$$|d_i \cdot \hat{p}_i| = |d_i| \cdot \frac{N}{p_i} < N \cdot 2^{-2\rho - \log n - 1},$$

$$|\sum_{i=0}^{n} d_i \cdot r_{i,j} \cdot r_{i,k} \cdot \hat{p}_j| \le \sum_{i=1}^{n} |r_{i,j}| \cdot |r_{i,k}| \cdot |d_i \cdot \hat{p}_i| \le \sum_{i=1}^{n} N \cdot 2^{-\log n - 1} \le N/2.$$

Thus, we observe right sides of the three equations (4.1), (4.2) and (4.3) have the size less than $N/2$ so that those equations hold over the integer.

Now we show how to solve the CCK-ACD when given polynomially many CCK-ACD samples and two distinct dual instances $d = \sum_{i=0}^{n} d_i \cdot \hat{p}_i$ and $d' = \sum_{i=0}^{n} d'_i \cdot \hat{p}_i$. More precisely, we are $2n$ CCK-ACD samples: $b_j = \mathsf{CRT}_{(p_i)}(r_{i,j})$ and $b'_\ell =$

$\mathsf{CRT}_{(p_i)}(r'_{i,\ell})$ for $1 \le j, \ell \le n$. Then we can check the following integer equations hold.

$$[d \cdot b_j \cdot b'_\ell]_N = \sum_{i=1}^{n} d_i \cdot r_{i,j} \cdot r'_{i,\ell} \cdot \hat{p}_i \in \mathbb{Z}$$

$$[d' \cdot b_j \cdot b'_\ell]_N = \sum_{i=1}^{n} d'_i \cdot r_{i,j} \cdot r'_{i,\ell} \cdot \hat{p}_i \in \mathbb{Z}$$

We denote $w_{j,\ell}$ and $w'_{j,\ell}$ as $[d \cdot b_j \cdot b'_\ell]_N$ and $[d' \cdot b_j \cdot b'_\ell]_N$, respectively. Using the above properties, we get the following matrix equations

$$\begin{aligned} w_{j,\ell} &= \sum_{i=1}^{n} r_{i,j} \cdot (d_i \cdot \hat{p}_i) \cdot r'_{i,\ell} \\ &= \begin{pmatrix} r_{1,j} & r_{2,j} & \cdots & r_{n,j} \end{pmatrix} \begin{pmatrix} d_1 \cdot \hat{p}_1 & 0 & \cdots & 0 \\ 0 & d_2 \cdot \hat{p}_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_n \cdot \hat{p}_n \end{pmatrix} \begin{pmatrix} r'_{1,\ell} \\ r'_{2,\ell} \\ \vdots \\ r'_{n,\ell} \end{pmatrix}, \\ w'_{j,\ell} &= \sum_{i=1}^{n} r_{i,j} \cdot (d'_i \cdot \hat{p}_i) \cdot r'_{i,\ell} \\ &= \begin{pmatrix} r_{1,j} & r_{2,j} & \cdots & r_{n,j} \end{pmatrix} \begin{pmatrix} d'_1 \cdot \hat{p}_1 & 0 & \cdots & 0 \\ 0 & d'_2 \cdot \hat{p}_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d'_n \cdot \hat{p}_n \end{pmatrix} \begin{pmatrix} r'_{1,\ell} \\ r'_{2,\ell} \\ \vdots \\ r'_{n,\ell} \end{pmatrix}. \end{aligned}$$

By collecting the above values of several $1 \le j, \ell \le n$, we can construct two matrices $\mathbf{W} = (w_{j,\ell})$ and $\mathbf{W}' = (w'_{j,\ell}) \in \mathbb{Z}^{n \times n}$, which can be written as

$$\mathbf{W} = \mathbf{R}^T \cdot \mathsf{diag}(d_1 \cdot \hat{p}_1, \cdots, d_n \cdot \hat{p}_n) \cdot \mathbf{R}'$$

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

for $\mathbf{R} = (r_{j,i})$ and $\mathbf{R}' = (r'_{i,\ell}) \in \mathbb{Z}^{n \times n}$. By computing $(\mathbf{W}')^{-1}$ over $\mathbb{Q}$, we obtain the matrix $\mathbf{Y}$ as following form

$$\mathbf{Y} = \mathbf{W} \cdot (\mathbf{W}')^{-1} = \mathbf{R}^T \cdot \mathsf{diag}(d_1/d'_1, \cdots, d_n/d'_n) \cdot (\mathbf{R}^T)^{-1}$$

whose eigenvalues are exactly the set $\{d_1/d'_1, \cdots, d_n/d'_n\} \subset \mathbb{Q}$. We can compute

those rational eigenvalues in polynomial-time of η, n and ρ from $\mathbf{Y}$. Since the modular equations $d \equiv d_i \cdot \hat{p}_i \pmod{p_i}$ and $d' \equiv d'_i \cdot \hat{p}_i \pmod{p_i}$ hold, one can check that p_i divides $d \cdot d'_i - d' \cdot d_i$ for each i. Thus, by computing $\gcd(N, d \cdot d'_i - d' \cdot d_i)$, we can find the p_i for each $1 \leq i \leq n$. Considering the overall cost of the computations required, we obtain the following theorem.

Theorem 4.2. *(Adapted from* [5, Section 3.2]*) For given $O(n)$* CCK-ACD *samples from $\mathcal{D}_{\eta,\rho,n}(p_i)$ with $N = \prod_{i=1}^{n} p_i$ and two distinct* dual instances*, one can recover secret primes $p_1, \cdots, p_n$ in $\widetilde{O}(n^{2+\omega} \cdot \eta)$ time with $\omega \leq 2.38$ and and overwhelming probability in ρ.*

4.2 Generating a Dual Instance from SDA

In this section, we present an algorithm to generate a dual instance from polynomially many given CCK-ACD samples $b_j = \mathsf{CRT}_{(p_i)}(r_{ij})$ and $N = \prod_{i=0}^{n} p_i$.

Consider the column lattice Λ generated by the following basis matrix.

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

We confirm that any lattice vector $\vec{c} \in \Lambda$ with $\|\vec{c}\| \leq \frac{N}{2}$ can be written in the form of $([d]_N, [d \cdot b_1]_N, \cdots, [d \cdot b_k]_N)^T$, where $d = \sum_{i=0}^{n} d_i \cdot \hat{p}_i$ for some d_i's and the modular equation $[d \cdot b_j]_N \equiv \sum_{i=0}^{n} r_{i,j} \cdot [d_i]_{p_i} \cdot \hat{p}_i \pmod{N}$ holds for each j. In the next theorem, we prove that if $\vec{c} \in \Lambda$ is a sufficiently short vector for a proper integer k, and the size of each $[d_i]_{p_i}$ is small. It implies that the first entry of the vector $\vec{c}$, $\sum_{i=1}^{n} [d_i]_{p_i} \cdot \hat{p}_i$ is a dual instance.

Algorithm 2 `SDA algorithm for the CCK-ACD problem`

Input: $N = \prod_{i=0}^{n} p_i$
Input: Root Hermite factor δ_0
Input: CCK-ACD samples $b_j = \mathsf{CRT}_{(p_i)}(r_{i,j})$ for $1 \le j \le 2k$ with $k = \lfloor \sqrt{\frac{\gamma}{2 \log \delta_0}} \rceil$.
Output: prime factors p_i's of N

$m \leftarrow 0$
while $m \le 1$ **do**
  Set $\vec{b} \leftarrow (b_{1+mk}, b_{2+mk}, \cdots, b_{k+mk})$
  Construct a lattice $\Lambda = \Lambda(\mathbf{B})$ with a basis matrix $\mathbf{B} = \begin{pmatrix} 1 & 0 \\ \vec{b}^T & N \cdot \mathbf{I}_k \end{pmatrix}$
  $\vec{v} = (v_0, v_1, \cdots, v_k) \leftarrow \mathcal{A}_{\delta_0}(\Lambda)$
  if $2(k+1)\log \delta_0 + \frac{1}{k+1} \log N < \eta - \rho - \log 2\sqrt{2\pi e}$ **then**
    $d^{(m)} \leftarrow v_0$
    $m \leftarrow m + 1$
  end if
end while
Construct matrices $\mathbf{W} = ([d^{(0)} \cdot b_i \cdot b_{n+j}]_N) \in \mathbb{Z}^{n \times n}$ and $\mathbf{W}' = ([d^{(1)} \cdot b_i \cdot b_{n+j}]_N) \in \mathbb{Z}^{n \times n}$.
Calculate $(\mathbf{W}')^{-1}$ over $\mathbb{Q}$ and $\mathbf{Y} = \mathbf{W} \cdot (\mathbf{W}')^{-1} \in \mathbb{Q}^{n \times n}$
Compute eigenvalues $\{\lambda_1, \lambda_2, \cdots, \lambda_n\} \subset \mathbb{Q}$ of $\mathbf{Y}$
Compute pairs of integers $(d_i^{(0)}, d_i^{(1)})$ from $\lambda_i = \frac{d_i^{(0)}}{d_i^{(1)}}$ for $1 \le i \le n$.
$p_i \leftarrow \gcd(N, d^{(0)} \cdot d_i^{(1)} - d^{(1)} \cdot d_i^{(0)})$ for $1 \le i \le n$
return p_i's.

Theorem 4.3. *Let n, η, ρ be parameters of the* CCK-ACD *problem. When $O(\gamma/\eta)$* CCK-ACD *samples are given, one can find a* dual instance *in $2^{O\left(\frac{\gamma}{(\eta-\rho)^2}\right)}$ time up to polynomial factors.*

Proof. Suppose that $k > n$ CCK-ACD samples $b_j = \mathsf{CRT}_{(p_i)}(r_{i,j})$ and $N = \prod_{i=0}^{n} p_i$ are given. We denote $r_{0,j}$ as $[b_j]_{p_0}$. Consider the column lattice Λ generated by the following basis matrix $\mathbf{B}$

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

where b_j's are given CCK-ACD samples and $N = \prod_{i=0}^{n} p_i$. Note that any vector $\vec{v}$ in

the lattice Λ can be expressed as the following form

$$\vec{v} \equiv a_0 \cdot \hat{p}_0 \begin{pmatrix} 1 \\ r_{0,1} \\ r_{0,2} \\ \vdots \\ r_{0,k} \end{pmatrix} + a_1 \cdot \hat{p}_1 \begin{pmatrix} 1 \\ r_{1,1} \\ r_{1,2} \\ \vdots \\ r_{1,k} \end{pmatrix} + \cdots + a_n \cdot \hat{p}_n \begin{pmatrix} 1 \\ r_{n,1} \\ r_{n,2} \\ \vdots \\ r_{n,k} \end{pmatrix} \pmod{N}.$$

for some integers a_i's. We denote $\hat{p}_i \cdot (1, r_{i,1}, r_{i,2}, \cdots, r_{i,k})^T$ by $\vec{v}_i$ for each i. Then, $\vec{v}_i$'s are linearly independent and $\|\vec{v}_i\| \leq B := \sqrt{k+1} \cdot N \cdot 2^{-\eta+\rho+1}$ for all $i \neq 0$, so $\lambda_i(\Lambda) \leq B$ holds for $1 \leq i \leq n$.

We apply Gaussian Heuristic to estimate $\lambda_{n+1}(\Lambda)$ which is approximately $\sqrt{\frac{k+1}{2\pi e}} \cdot (\det \Lambda)^{\frac{1}{k+1}}$. Suppose the size of a vector $\vec{c} \in \Lambda$ obtained by the lattice reduction algorithm $\mathcal{A}_\delta$ is shorter than $\delta^{2(k+1)} \cdot \lambda_1(\Lambda) \leq \delta^{2(k+1)} \cdot B < \sqrt{\frac{k+1}{2\pi e}} \cdot (\det \Lambda)^{\frac{1}{k+1}} \approx \lambda_{n+1}(\Lambda)$. Then, we conclude $\vec{c} \in \langle \vec{v}_1, \cdots, \vec{v}_n \rangle$ and p_0 divides $\gcd(N, d)$, where d is the first entry of the vector $\vec{c}$. Hence, we require that the length of vector $\vec{c}$, the first output of the lattice reduction algorithm, is shorter than $\sqrt{\frac{k+1}{2\pi e}} \cdot (\det \Lambda)^{\frac{1}{k+1}}$. It can be written as

$$\|\vec{c}\| \leq \delta^{2(k+1)} \cdot \lambda_1(\Lambda) < \delta^{2(k+1)} \cdot B < \sqrt{\frac{k+1}{2\pi e}} \cdot (\det \Lambda)^{\frac{1}{k+1}}.$$

Taking logarithm to both sides of the inequality, we obtain as follows:

$$2(k+1)\log\delta + \log N - \eta + \rho + 1 \leq \frac{k}{k+1}\log N - \frac{1}{2}\log 2\pi e$$

$$2(k+1)\log\delta + \frac{1}{k+1}\log N < \eta - \rho - \log 2\sqrt{2\pi e} \tag{4.4}$$

In particular, when applying the AM-GM inequality for the left side of (4.4), we obtain the following inequality

$$2\sqrt{2\log\delta \cdot \log N} \leq \eta - \rho - O(1)$$

where equality holds if and only if $(k+1)^2 \approx \frac{\gamma}{2\log\delta}$ and $\gamma \cdot \log\delta \approx \frac{(\eta-\rho)^2}{8}$.

Thus, when we choose δ satisfying $\log\delta < \frac{(\eta-\rho)^2}{8\gamma} - \epsilon$ for some small ϵ and $k \approx \frac{2\gamma}{\eta-\rho} = O(\frac{\gamma}{\eta})$, we can conclude that output vector $\vec{c}$ of $\mathcal{A}_\delta$ can be written as

$\vec{c} = \sum_{i=1}^{n} d_i \cdot \vec{v}_i$ for some d_i's. If we denote the first entry of $\vec{c}$ as d, the vector $\vec{c}$ is the form of $(d, [d \cdot b_1]_N, \cdots, [d \cdot b_k]_N)^T$. Then $d = \sum_{i=1}^{n} d_i \cdot \hat{p}_i$ and $[d \cdot b_j]_N = \sum_{i=1}^{n} r_{i,j} \cdot d_i \cdot \hat{p}_i$ hold for each j. In this case, d is a multiple of p_0 so that one can recover the factor p_0 by computing $\gcd(d, N)$. Since the root Hermite factor δ is achieved in time $\mathrm{poly}(k) \cdot 2^{O(\beta)}$ times by the BKZ algorithm with $\beta = \Theta(1/\log \delta)$, we conclude that one can recover the factor p_0 in $2^{O\left(\frac{\gamma}{(\eta-\rho)^2}\right)}$ time up to polynomial factors using the BKZ algorithm with $\beta \approx O\left(\frac{\gamma}{(\eta-\rho)^2}\right)$.

Next, we propose the condition for terms d_i's to be sufficiently bounded so that it can be regarded as a dual instance. We denote $\vec{\tilde{c}}$ as k-dimensional vector which can be obtained by removing the first coordinate of $\vec{c}$ (*i.e.* $\vec{\tilde{c}} = ([d \cdot b_1]_N, \cdots, [d \cdot b_k]_N)^T$). Using the property $[d \cdot b_j]_N = \sum_{i=1}^{n} r_{i,j} \cdot d_i \cdot \hat{p}_i$ for each j, $\vec{\tilde{c}}$ can be decomposed as follows:

$$\begin{aligned} \vec{\tilde{c}} &= (d_1 \cdot \hat{p}_1, \cdots, d_n \cdot \hat{p}_n) \cdot \begin{pmatrix} r_{1,1} & r_{1,2} & \cdots & r_{1,k} \\ r_{2,1} & r_{2,2} & \cdots & r_{2,k} \\ \vdots & \vdots & \ddots & \vdots \\ r_{n,1} & r_{n,2} & \cdots & r_{n,k} \end{pmatrix} \\ &= \mathbf{d} \cdot \hat{\mathbf{P}} \cdot \mathbf{R}, \end{aligned}$$

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

We will show later that there is a right inverse $\mathbf{R}^* \in \mathbb{Z}^{k \times n}$ such that $\mathbf{R} \cdot \mathbf{R}^* = \mathbf{I}_n$, where $\mathbf{I}_n$ is the $n \times n$ identity matrix. Then, for each i, $|d_i \cdot \hat{p}_i|$ can be bounded as follows

$$|d_i \cdot \hat{p}_i| \leq \|\mathbf{d} \cdot \hat{\mathbf{P}}\|_\infty = \|\tilde{\mathbf{c}} \cdot \mathbf{R}^*\|_\infty \leq \|\tilde{\mathbf{c}}\| \cdot \|\mathbf{R}^*\|_\infty.$$

If there is a matrix $\mathbf{R}^*$ which satisfies $\|\vec{c}\| \cdot \|\mathbf{R}^*\|_\infty \leq N \cdot 2^{-2\rho - \log n - 1}$, it implies that each d_i is smaller than $N \cdot 2^{-2\rho - \log n - 1}/\hat{p}_i$. Thus, under the above condition, the integer $d = \sum_{i=1}^{n} d_i \cdot \hat{p}_i$, the first entry of output vector $\vec{c}$, can be regarded as a dual instance.

Thus, it is enough to show the existence of matrix $\mathbf{R}^*$ which ensures that the size of $\|\vec{c}\| \cdot \|\mathbf{R}^*\|_\infty$ is less than $N \cdot 2^{-2\rho - \log n - 1}$ with $\|\mathbf{c}\| \leq \delta^{2(k+1)} \cdot \sqrt{k+1} \cdot N \cdot 2^{-\eta+\rho+1}$ to obtain a dual instance by using the lattice reduction algorithm.

Construction of $\mathbf{R}^*$. Now, we construct the right inverse matrix $\mathbf{R}^*$ and estimate the size of $\|\mathbf{R}^*\|_\infty$ using Babai's nearest plane algorithm [2] and Gaussian Heuristic assumption.

More precisely, let q_1 be a prime integer, which is independent from $\prod_{i=1}^{n} p_i$, and $\vec{z}_1 \in \mathbb{Z}^k$ be any vector with $\mathbf{R} \cdot \vec{z}_1 \equiv \vec{e}_1 \pmod{q_1}$, where $\vec{e}_1$ is a n-dimensional standard vector. Consider a full rank lattice $\Lambda_1 = \{\vec{x} \in \mathbb{Z}^k : \mathbf{R} \cdot \vec{x} \equiv \vec{0} \pmod{q_1}\}$ whose determinant is q_1^n and the set of linearly independent vectors $\{\vec{x}_i\}_{1 \le i \le k} \subset \mathbb{Z}^k$ such that $\|\vec{x}_i\| \le \lambda_k(\Lambda_1)$ for each i. We accept Gaussian heuristic to estimate $\lambda_k(\Lambda_1) \approx \sqrt{\frac{k}{2\pi e}} \cdot \det(\Lambda_1)^{1/k} = \sqrt{\frac{k}{2\pi e}} \cdot {q_1}^{n/k}$ so that we can bound $\|\vec{x}_i\| \le \sqrt{\frac{k}{2\pi e}} \cdot {q_1}^{n/k}$ for each i.

Using the Babai's nearest plane algorithm on vector $\vec{z}$, we obtain the vector $\sum_{i=1}^{k} u_i \cdot \vec{x}_i$ so that $\|\vec{z} - \sum_{i=1}^{k} u_i \cdot \vec{x}_i\| \le \sqrt{\frac{1}{4}\sum_{i=1}^{k} \|\vec{x}_i^*\|^2}$ holds, where each $\vec{x}_i^*$ is Gram-Schmidt vector of $\vec{x}_i$. We denote $\vec{z}_1'$ as $\vec{z}_1 - \sum_{i=1}^{k} u_i \cdot \vec{x}_i$ and we obtain the following:

$$\|\vec{z}_1'\| = \|\vec{z}_1 - \sum_{i=1}^{k} u_i \cdot \vec{x}_i\| \le \sqrt{\frac{1}{4}\sum_{i=1}^{k} \|\vec{x}_i^*\|^2} \le \frac{1}{2}\sqrt{\sum_{i=1}^{k} \|\vec{x}_i\|^2} \le \frac{k}{2} \cdot {q_1}^{n/k}.$$

For the modular equation

$$0 \equiv \mathbf{R} \cdot \vec{z}_1' - \vec{e}_1 \equiv \left([\mathbf{R}]_1 \cdot \vec{z}_1' - 1, [\mathbf{R}]_2 \cdot \vec{z}_1', \cdots, [\mathbf{R}]_n \cdot \vec{z}_1'\right)^T \pmod{q_1},$$

if $|[\mathbf{R}]_i \cdot \vec{z}_1'| \le \|[\mathbf{R}]_i\| \cdot \|\vec{z}_1'\| \le \sqrt{k} \cdot 2^\rho \cdot \frac{k}{2} \cdot {q_1}^{\frac{n}{k}}$ is less than $\frac{1}{2}q_1$ for all i (*i.e.* $q_1 > (k^{\frac{3}{2}} \cdot 2^\rho)^{\frac{k}{k-n}}$), the equation $\mathbf{R} \cdot \vec{z}_1' = \vec{e}_1$ holds over the integers.

By setting the size of prime q_1 to be similar to $(k^{\frac{3}{2}} \cdot 2^\rho)^{\frac{k}{k-n}}$, we can conclude that there exists a vector $\vec{z}_1'$ which satisfies the equation $\mathbf{R} \cdot \vec{z}_1' = \vec{e}_1$ and the following condition

$$\|\vec{z}_1'\|_1 \le \sqrt{k} \cdot \|\vec{z}_1'\|_2 \le \frac{1}{2} \cdot k^{\frac{3}{2}} \cdot {q_1}^{\frac{n}{k}} \approx \frac{1}{2} \cdot k^{\frac{3k}{2(k-n)}} \cdot 2^{\frac{n}{k-n}\rho}.$$

Similarly, we can also apply it to other $\vec{z}_i$'s to construct $\mathbf{R}^* = (\vec{z}_1', \cdots, \vec{z}_k')$ with

the vectors $\vec{z}_i'$ satisfying $\mathbf{R} \cdot \vec{z}_i' = \vec{e}_i$, so we can bound $\|\mathbf{R}^*\|_\infty$ as follows

$$\|\mathbf{R}^*\|_\infty = \max_{1 \le i \le k} \|\vec{z}_i'\|_1 \le \frac{1}{2} \cdot k^{\frac{3k}{2(k-n)}} \cdot 2^{\frac{n}{k-n}\rho}.$$

Hence, we can obtain the upper bound of $\|\vec{c}\| \cdot \|\mathbf{R}^*\|_\infty$ as follows

$$\|\vec{c}\| \cdot \|\mathbf{R}^*\|_\infty \le \delta'^{2(k+1)} \cdot \sqrt{k+1} \cdot N \cdot 2^{-\eta+\rho+1} \cdot \frac{1}{2} \cdot k^{\frac{3k}{2(k-n)}} \cdot 2^{\frac{n}{k-n}\rho}.$$

We remind that the size of $\|\vec{c}\| \cdot \|\mathbf{R}^*\|_\infty$ needs to be less than $N \cdot 2^{-2\rho - \log n - 1}$. Therefore the following inequality should be satisfied

$$\delta^{2(k+1)} \cdot \sqrt{k+1} \cdot N \cdot 2^{-\eta+\rho} \cdot k^{\frac{3k}{2(k-n)}} \cdot 2^{\frac{n}{k-n}\rho} \le N \cdot 2^{-2\rho - \log n - 1}$$

Taking logarithm to both sides of the inequality, we obtain as follows

$$2(k+1)\log\delta \le \eta - 3\rho - \frac{n}{k-n}\rho - \frac{3k}{2(k-n)}\log k - \log(2n\sqrt{k+1}) \quad (4.5)$$

Since we set $k \approx \frac{2\gamma}{\eta-\rho} > 2n$, the condition $\frac{k}{k-n} = O(1)$ holds so we can rewrite the above equality and obtain the following condition for n, k, η, and ρ

$$2(k+1)\log\delta \le \eta - 3\rho - \frac{n}{k-n}\rho - O(\log k).$$

The left side of the above inequality $2(k+1)\log\delta$ is approximated as $\frac{4\gamma}{\eta-\rho} \cdot \frac{(\eta-\rho)^2}{8\gamma} \approx \frac{\eta-\rho}{2}$ so that the equality holds with our optimized parameters $k \approx \frac{2\gamma}{\eta-\rho}$ and $\log\delta < \frac{(\eta-\rho)^2}{8\gamma} - \epsilon$ for the condition (4.4). Thus we can conclude that when we use the lattice reduction $\mathcal{A}_\delta$ with $\log\delta < \frac{(\eta-\rho)^2}{8\gamma} - \epsilon$ for some small $\epsilon > 0$ and about $\frac{2\gamma}{\eta-\rho}$ CCK-ACD samples to construct the lattice Λ, the conditions (4.4) and (4.5) are satisfied. In other words, we can obtain a dual instance from the first entry of output vector in $2^{O\left(\frac{\gamma}{(\eta-\rho)^2}\right)}$ time up to polynomial factors. □

Remark 1. The time $2^{O\left(\frac{\gamma}{(\eta-\rho)^2}\right)}$ up to polynomial factors required for the above algorithm does not depend on the number of secret primes n and bit-length of the multiple of n secret primes $n \cdot \eta$ but depends on the bit-length of CCK-ACD samples γ.

5 Experiments

In this section, we provide the experimental results of OLA, SDA for the CCK-ACD problem. All experiments were implemented on a single Intel Core i5 running at 2.1GHz processor and 16GB memory.

We remark that we use a few simplifications for the experiments to run our algorithm; we run fplll algorithm [10] instead of BKZ algorithm. For efficient experiment, we choose the number of samples, k, to satisfy the required conditions for attack instead of the asymptotic optimum.

OLA									
CCK-ACD									
Experimental parameters						Experimental Det		Expected Det	
n	k	η	ρ	$\gamma/10^4$	time(min)	CCK-ACD	Random	CCK-ACD	Random
20	65	1500	500	6	3	10022	38707	10000	38682
30	90	1000	100	8	14	3040	50804	3000	50753
40	120	600	120	5.4	21	5661	34785	5600	34683
50	150	1000	300	10	128	15085	64871	15000	64706
80	150	400	70	4.7	36	5727	21530	5600	21354
80	240	400	100	6.7	615	8162	44239	8000	43840
90	270	200	40	3.8	490	3790	25433	3600	24916
100	240	400	50	8	790	5199	46306	5000	45875
*10	320	988	26	29	14600	284	254770	260	254574
**10	325	988	80	29	15540	824	254813	800	254713

Table 1. Experiments about OLA on the CCK-ACD problem. Random means that we do the OLA with random instances whose size is $\gamma-$bits. Parameters* is the toy parameters in [7] with $\lambda = 42$ and our attack cost is 2^{47}. Parameters** is increasing the size of ρ to withstand the GCD attack in [3], although our attack cost is almost the same.

According to our experiments in Table 1, from various parameters, we can see that the determinant of the orthogonal lattice is very similar to our prediction. Thus, our several assumptions of OLA are reasonable for CCK-ACD and random instances. Especially, in actual use of parameters, the difference of determinant between CCK-ACD and random is more pronounced because n and ρ are set considerably smaller than γ.

Experimental results of OLA say that our expectation of the condition for OLA is very accurate. OLA works well even when the ρ is quite large as long as the condition (3.1) is satisfied.

We also experimented with a toy parameter in [7]. OLA is slower than conventional attacks, GCD attack in [3], in toy parameters. Since conventional attacks,

the GCD algorithms, in [3] is $\tilde{O}(2^{\rho/2})$ polynomial-time operation, they depend a lot on the size of ρ unlike OLA. If ρ is larger than current parameters, then OLA can be the faster than other direct algorithms for the CCK-ACD problem.

When the number of secret primes, n, is small, OLA can even find the exact some $\vec{r}_i$ through LLL algorithm on $\Lambda^{\perp}(\tilde{\mathbf{U}})$. But if n is more than 100, the outputs of the LLL algorithm are linear combinations of $\vec{r}_i$'s with a high probability. For the above reason, we find it difficult to get an exact $\vec{r}_i$ when n is large.

SDA					
CCK-ACD					
n	k	η	ρ	$\gamma/10^4$	time(min)
20	60	1500	500	6	59
30	90	1000	100	8	550
40	120	600	120	5.4	692
50	150	1000	300	10	3650
80	150	400	70	4.7	760
80	240	400	100	6.7	9300
90	270	200	40	3.8	5900
100	300	120	10	2.5	8870
100	250	400	50	8	13950

Table 2. Experiments about SDA on the CCK-ACD problem.

In Table 2, we can see SDA experimental results on the CCK-ACD problem. According to our results, we have confirmed that experimental results of SDA are better than we expected, even in parameters that do not satisfy our condition. In SDA, we can not only distinguish them from a uniform distibution but also find the factor of N and recover the secret primes.

In the CCK-ACD problem, OLA is much faster than SDA like the ACD problem. It is not surprising considering the size of the determinant of lattice applying lattice reduction algorithm.

References

[1] M. Ajtai, *Generating random lattices according to the invariant distribution. draft*, 2006.

[2] L. Babai, On Lovász'lattice reduction and the nearest lattice point problem, *Combinatorica* **6** (1986), 1–13.

[3] Y. Chen and P. Q. Nguyen, Faster algorithms for approximate common divisors: Breaking fully-homomorphic-encryption challenges over the integers, in: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, pp. 502–519, 2012.

[4] 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*, Springer, pp. 315–335, 2013.

[5] J. H. Cheon, K. Han, C. Lee, H. Ryu and D. Stehlé, Cryptanalysis of the multilinear map over the integers, in: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, pp. 3–12, 2015.

[6] J. H. Cheon and D. Stehlé, Fully homomorphic encryption over the integers revisited, in: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, pp. 513–536, 2015.

[7] J. S. Coron, T. Lepoint and M. Tibouchi, Batch Fully Homomorphic Encryption over the Integers, *IACR Cryptology ePrint Archive* **2013** (2013), 36.

[8] J. S. Coron, T. Lepoint and M. Tibouchi, Practical multilinear maps over the integers, in: *Annual Cryptology Conference*, Springer, pp. 476–493, 2013.

[9] J. S. Coron and H. V. Pereira, *On Kilian's Randomization of Multilinear Map Encodings*, Cryptology ePrint Archive, Report 2018/1129, 2018, `https://eprint.iacr.org/2018/1129`.

[10] The FPLLL development team, *fplll, a lattice reduction library*, Available at `https://github.com/fplll/fplll`, 2016.

[11] J. Ding and C. Tao, A New Algorithm for Solving the Approximate Common Divisor Problem and Cryptanalysis of the FHE based on GACD., *IACR Cryptology ePrint Archive* **2014** (2014), 42.

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

[13] S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai and B. Waters, Candidate indistinguishability obfuscation and functional encryption for all circuits, *SIAM J. Comput.* **45** (2016), 882–929.

[14] G. Hanrot, X. Pujol and D. Stehlé, Terminating BKZ., *IACR Cryptology ePrint Archive* **2011** (2011), 198.

[15] N. Howgrave-Graham, Approximate integer common divisors, in: *Cryptography and lattices*, pp. 51–66, Springer, 2001.

[16] A. K. Lenstra, H. W. Lenstra and L. Lovász, Factoring polynomials with rational coefficients, *Math. Ann.* **261** (1982), 515–534.

[17] H. H. Nguyen and V. Vu, Random matrices: Law of the determinant, *Ann. Probability* **42** (2014), 146–167.

[18] M. Van Dijk, C. Gentry, S. Halevi and V. Vaikuntanathan, Fully homomorphic encryption over the integers, in: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, pp. 24–43, 2010.

Received **???**.

Author information

Jung Hee Cheon, Wony Cho, Minki Hhan, Minsik Kang, Jiseung Kim, SNU, Republic of Korea.
E-mail: jungheechoen, wony0404, hhan,?,tort154@snu.ac.kr

Changmin Lee, ENS de Lyon, France.
E-mail: changmin.lee@ens-lyon.fr