Revisiting Orthogonal Lattice Attacks on Approximate Common Divisor Problems and their Applications

Jun Xu[1,2], Santanu Sarkar[3], and Lei Hu[1,2]

[1] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[2] Data Assurance and Communications Security Research Center, Chinese Academy of Sciences, Beijing 100093, China
[3] Indian Institute of Technology, Sardar Patel Road, Chennai 600036, India
{xujun,hulei}@iie.ac.cn,sarkar.santanu.bir@gmail.com

Abstract. In this paper, we revisit three existing types of orthogonal lattice (OL) attacks and propose optimized cases to solve approximate common divisor (ACD) problems. In order to reduce both space and time costs, we also make an improved lattice using the rounding technique. Further, we present asymptotic formulas of the time complexities on our optimizations as well as three known OL attacks. Besides, we give specific conditions that the optimized OL attacks can work and show how the attack ability depends on the blocksize β in the BKZ-β algorithm. Therefore, we put forward a method to estimate the concrete cost of solving the random ACD instances. It can be used in the choice of practical parameters in ACD problems. Finally, we give the security estimates of some ACD-based FHE constructions from the literature and also analyze the implicit factorization problem with sufficient number of samples. In the above situations, our optimized OL attack using the rounding technique performs fastest in practice.

Keywords: Fully homomorphic encryption, approximate common divisor problem, implicit factorization problem, lattice, orthogonal lattice attack, lattice reduction algorithm

1 Introduction

1.1 Background

FHE cryptosystems which allow anybody to evaluate any efficiently computable function over ciphertexts without knowing the decryption key, have significant applications in the field of cloud computation. In 2009, Gentry [29] designed the first FHE scheme by making use of hard problems on ideal lattices, which is a breakthrough work in this area. Subsequently, a wide variety of FHE schemes were put forward, which can be mainly sorted into three categories relying on the different hardness assumptions: FHE based on ideal lattices [29, 53, 54, 30],

FHE based on LWE (Learning with Errors) problems and its variants [11, 12, 31, 32, 9, 33, 10, 13, 4] and FHE based on ACD problems [56, 24, 25, 17, 23, 47, 18, 37, 7].

In 2001, Howgrave-Graham [35] first introduced the ACD problem, which contains two main versions: the general version (GACD problem) and partial version (PACD problem). For given nonnegative integers γ, η, ρ such that $\gamma > \eta > \rho$, a (γ, η, ρ)-GACD problem is defined as follows:

For a random η-bit odd number p, given polynomially (in γ, η and ρ) many samples from the set

$$\{a_i = pq_i + r_i : q_i \in \mathbb{Z} \cap (0, 2^\gamma/p), r_i \in \mathbb{Z} \cap (-2^\rho, 2^\rho)\},$$

output the approximate common divisor p.

The definition of a (γ, η, ρ)-PACD problem is almost the same as that of a (γ, η, ρ)-GACD problem, except the fact that an exact multiple (a γ-bit integer) of p is given. Apart from the GACD problem and PACD problem, the Chinese remainder theorem (CRT) version of ACD problems was also proposed to build FHE schemes [17, 23, 7] and multilinear maps [21, 22].

The computational intractability of ACD problems not only provides a sound support for constructing FHE schemes and other state-of-the-art designs but also can be used to discuss the security strength of some intractable problems. In IEEE-IT 2011, Sarkar and Maitra [49] transformed the implicit factorization problem [42] introduced by May and Ritzenhofen into the corresponding PACD problem. Moreover, a faster variant of the Guruswami-Sudan algorithm for list decoding of Reed-Solomon codes was given by Cohn and Heninger in [20] based on the idea of ACD. In EUROCRYPT 2015, Cheon and Stehlé [18] presented a reduction from LWE [48] to a quite natural decision variant of ACD. These works draw more attention towards ACD problem and show the importance of this problem.

Chronologically, the first alternative design of ACD based FHE scheme whose security is based on the hardness of ACD problems was proposed by van Dijk, Gentry, Halevi and Vaikuntanathan [56]. In this scheme, ρ is extremely small compared to η. Later, Cheon and Stehlé [18] constructed an ACD-based FHE scheme with three parameter sets, which asymptotically outperforms previously known proposals based on this problem. In these three parameter sets of (γ, η, ρ)-ACD problems, ρ is no longer extremely small compared to η.

1.2 Motivation

There may be a gap between exploited parameters of ACD-based scheme and provable parameters. Hence, many researches are conducted to analyze the exploited parameters of ACD problem to explain the security of the scheme. According to the analysis of Galbraith, Gebregiyorgis and Murphy in [27], the orthogonal lattice (OL) attack, first proposed by Nguyen and Stern [43], is the efficient method to solve ACD problems compared to the other known approaches for practical analysis.

OL attacks on ACD problems were first analyzed in [56] and later considered in [24, 36, 41, 18, 27]. For given n ACD samples $a_i = pq_i + r_i$, there are three types of OL attacks: the first one is to consider the lattice orthogonal to $(a_1, \ldots, a_n)$ and $(r_1, \ldots, r_n)$ [56]; the second one is to focus on the lattice orthogonal to $(1, -\frac{r_1}{2^\rho}, \ldots, -\frac{r_n}{2^\rho})$ [56, 18, 27]; the third one involves the lattice orthogonal to $(1, -r_1, \ldots, -r_n)$ [24, 36, 41]. In essence, these three OL attacks share the common point of finding vectors orthogonal to unknown vector $(q_1, \ldots, q_n)$ (see Section 2.3).

In fact, the OL attack, commented by Galbraith et al. [27], is the second OL attack. However, previous works, including [27], do not present the comparison of three types of OL attacks. Therefore, one does not know which one among the three OL attacks is the best. Moreover, it is worthwhile to ask what is the optimized lattice for OL attack. Furthermore, one concerns the needed time complexity for solving (γ, η, ρ)-ACD problem by using OL attacks.

1.3 Contribution

First, for given n (γ, η, ρ)-ACD samples $a_1, \ldots, a_n$, we discover new linearly independent vectors orthogonal to unknown vector $(q_1, \ldots, q_n)$ and present the optimized strategies for OL attacks. We get that the second OL attack is almost close to its first optimization. Compared to the second OL attack and its first optimization, the second optimization, using the rounding technique (e.g. [8]), approximately reduces the maximum entries of the input basis matrix from γ to $(\gamma - \rho)$ bits. Hence, the second optimization will perform faster in practice when $(\gamma - \rho)$ is relatively small.

Second, we present asymptotic formulas of the time complexities on our optimized strategies as well as three known OL attacks. By comparison, we find out that all these OL attacks have the same asymptotic time complexities when $\gamma \gg \rho$; the second OL attack and its optimizations are more advantageous than the first and third OL attacks when $(\gamma - \rho)$ is relatively small.

Third, utilizing the optimized OL attacks, we depict the expression on the root-Hermite factor δ_0 (see the definition in Section 2.2), the number n of (γ, η, ρ)-ACD samples (i.e., the involved lattice dimension) and parameters γ, η, ρ. Further, we give an estimation method of the concrete cost to solve (γ, η, ρ)-ACD instances for optimized OL attacks.

Finally, we analyze ACD problems from the FHE schemes in [56, 47, 18, 37]. Let λ refer to the security parameter. According to our estimations based on using BKZ-β and sieving to solve the SVP oracle, from the designer's point of view in order to achieve $\Omega(\lambda)$-bit security, the parameter choices in [56] are conservative for OL attacks; those in [47, 37] are optimistic for OL attacks. We present these results in Table 1. Moreover, we also point out that the (γ, η, ρ)-GACD problem with small $(\gamma - \rho)$ proposed as an open problem in [18] can be easily acquired the partial information of the approximate common divisor p by using the second OL attack as well as our OL attacks. Besides, we revisit the implicit factorization problem. In the above situations, the optimized OL attack utilizing the rounding technique is much faster in practice.

Table 1. The logarithm of asymptotic time complexities to solve (γ, η, ρ)-ACD problems by using OL attacks in Section 3, where $\lim_{\lambda\to\infty}\left(\frac{\log^2\lambda}{\log\log\lambda}/\lambda\right) = 0$

[56]	[47]	[37]
$\Omega(\lambda\log\lambda)$	$\Omega\left(\frac{\log^2\lambda}{\log\log\lambda}\right)$	$\Omega\left(\frac{\log^2\lambda}{\log\log\lambda}\right)$

1.4 Organization

In Section 2, we recall some terminologies, preliminary knowledge and known OL attacks. In Section 3, we present optimized OL attacks for solving ACD problems and give the corresponding analyses. We present the attack complexity and give comparisons with previous works in Section 4. We respectively give the cryptanalysis of ACD-based FHE schemes and the implicit factorization problem by using the existing lattice attacks and our methods in Sections 5 and 6. Section 7 concludes the paper.

2 Preliminaries

We write vectors in bold lower-case letters, e.g. $\mathbf{a}$, and matrices in bold upper-case letters, e.g. $\mathbf{A}$. We write $\langle\cdot,\cdot\rangle$ for the inner product and $\|\cdot\|$ for the l_2 Euclidean length as usual. We denote the transpose of matrix $\mathbf{A}$ as $\mathbf{A}^T$, and the logarithm to base 2 as log. We write $\lfloor r\rfloor$ for the largest integer not more than real number r.

2.1 Lattices

A rank-n lattice $\mathcal{L}$ in the m-dimensional space is spanned by n linearly independent row vectors $\mathbf{b}_1,\ldots,\mathbf{b}_n$ in $\mathbb{R}^m$,

$$\mathcal{L} = \left\{\sum_{i=1}^{n} k_i\mathbf{b}_i \mid k_i \in \mathbb{Z}\right\},$$

where $\{\mathbf{b}_1,\ldots,\mathbf{b}_n\}$ is a basis for $\mathcal{L}$ and $\mathbf{B} = [\mathbf{b}_1^T,\ldots,\mathbf{b}_n^T]^T$ is the corresponding basis matrix. The rank or dimension and determinant of $\mathcal{L}$ are respectively denoted as $\dim\mathcal{L} = n$ and $\det\mathcal{L} = \sqrt{\det(\mathbf{B}\mathbf{B}^T)}$. If $\mathbf{B}$ is a square matrix, then $\det\mathcal{L} = |\det(\mathbf{B})|$.

Definition 1 (Gram Schmidt Orthogonalization). *Given a sequence of n linearly independent vectors $\mathbf{b}_1,\ldots,\mathbf{b}_n$, the Gram Schmidt orthogonalization is the sequence of vectors $\widetilde{\mathbf{b}}_1,\ldots,\widetilde{\mathbf{b}}_n$ defined by*

$$\widetilde{\mathbf{b}}_i = \mathbf{b}_i - \sum_{j=1}^{i-1}\mu_{i,j}\widetilde{\mathbf{b}}_j$$

where $\mu_{i,j} = \langle\mathbf{b}_i,\widetilde{\mathbf{b}}_j\rangle/\langle\widetilde{\mathbf{b}}_j,\widetilde{\mathbf{b}}_j\rangle$.

For a given basis matrix $\mathbf{B}$ of $\mathcal{L}$ and the corresponding Gram Schmidt vectors $\widetilde{\mathbf{b}}_i$ for $i = 1, \ldots, n$, we have $\det \mathcal{L} = \prod_{i=1}^{n} \|\widetilde{\mathbf{b}}_i\|$.

Definition 2. *Let* $\mathbf{B}$ *be a basis and* $\widetilde{\mathbf{b}}_i$ *be its Gram Schmidt vectors and* $\mu_{i,j} = \langle \mathbf{b}_i, \widetilde{\mathbf{b}}_j \rangle / \langle \widetilde{\mathbf{b}}_j, \widetilde{\mathbf{b}}_j \rangle$*, then the basis* $\mathbf{B}$ *is size-reduced if* $|\mu_{i,j}| \leq \frac{1}{2}$ *for* $1 \leq j < i \leq n$.

2.2 Lattice Reduction

Lattice reduction algorithm is to output a reduced basis consisting of relatively short and nearly orthogonal vectors, which has plenty of cryptographic applications [44]. After the publication of celebrated LLL algorithm [40], a number of lattice reduction algorithms emerged, for example [51, 52, 28, 15, 46, 5]. In practice, the Block-Korkine-Zolotarev (BKZ) algorithm proposed by Schnorr and Euchner [51] has a good performance. In the BKZ algorithm, the running time and output quality depend on an input parameter–blocksize β. Hence, such an algorithm is called BKZ-β. With the increase of β, the output basis becomes much reduced but the cost significantly increases. The BKZ-β proceeds by reducing a lattice basis using an SVP oracle in a smaller dimension β. Based on [34], the number of calls to the SVP oracle remains polynomial.

Gama and Nguyen [28] identified the Hermite factor of the reduced basis as the dominant parameter in the runtime of the lattice reduction and the quality of the reduced basis. For an n-dimensional lattice $\mathcal{L}$, the Hermite factor

$$\delta_0^n = \frac{\|\mathbf{b}_1\|}{(\det \mathcal{L})^{\frac{1}{n}}},$$

where $\mathbf{b}_1$ is the first reduced basis vector of $\mathcal{L}$ and δ_0 is called as the root-Hermite factor. Chen [57] gave an expression between the root-Hermite factor δ_0 and the block size β:

$$\delta_0 = \left(\frac{\beta}{2\pi e} (\pi e)^{\frac{1}{\beta}} \right)^{\frac{1}{2(\beta-1)}}.$$

Further, we generally assume that the Geometric Series Assumption (GSA) holds for LLL and BKZ-β algorithms.

Definition 3 (Geometric Series Assumption [50]). *The Euclidean lengths of the Gram Schmidt vectors after lattice reduction satisfy*

$$\|\widetilde{\mathbf{b}}_i\| = \|\mathbf{b}_1\| \cdot \theta^{i-1} \text{ for } 0 < \theta < 1 \text{ and } i = 1, \ldots, n.$$

According to Geometric Series Assumption, $\|\mathbf{b}_1\| = \delta_0^n \cdot (\det \mathcal{L})^{\frac{1}{n}}$ and $\det \mathcal{L} = \prod_{i=1}^{n} \|\widetilde{\mathbf{b}}_i\|$, it is easy to deduce $\delta_0 = \theta^{-(n-1)/2n} > 1$.

2.3 Overview of Known OL Attacks

In this subsection, we recall the existing OL attacks, where $a_1, \ldots, a_n$ are (γ, η, ρ)-ACD samples.

The First OL Attack on ACD problems was proposed by van Dijk, Gentry, Halevi and Vaikuntanathan [56]. The involved lattice $\mathcal{L}_1(\alpha)$, first proposed by Nguyen and Stern [43], is spanned by the row vectors of the following $n \times (n+1)$ matrix

$$\begin{pmatrix} \alpha a_1 & 1 & & \\ \alpha a_2 & & 1 & \\ \vdots & & & \ddots \\ \alpha a_n & & & & 1 \end{pmatrix}$$

where $\alpha \in \mathbb{Z}$. Let $(\alpha \sum_{i=1}^{n} u_i a_i, u_1, \ldots, u_n)$ be a reduced basis vector. From the detailed analysis of [43, Theorem 4], we have $\sum_{i=1}^{n} u_i a_i = 0$ when α is sufficiently large. Since $a_i = pq_i + r_i$, we have $\sum_{i=1}^{n} u_i r_i = 0 \bmod p$. Further, one can obtain $\sum_{i=1}^{n} u_i r_i = 0$ if vector $(u_1, \ldots, u_n)$ is short enough. It implies that $(u_1, \ldots, u_n)$ is orthogonal to $(a_1, \ldots, a_n)$ and $(r_1, \ldots, r_n)$. Therefore, $(u_1, \ldots, u_n)$ is also orthogonal to $(q_1, \ldots, q_n)$.

The Second OL Attack on ACD problems also was given by van Dijk, Gentry, Halevi and Vaikuntanathan [56] and subsequently revisited in [18, 27]. The involved lattice is spanned by the row vectors of the following $n \times (n+1)$ matrix

$$\begin{pmatrix} a_1 & 2^\rho & & \\ a_2 & & 2^\rho & \\ \vdots & & & \ddots \\ a_n & & & & 2^\rho \end{pmatrix}.$$

Their core idea is to search the vector $(\sum_{i=1}^{n} u_i a_i, u_1 2^\rho, \ldots, u_n 2^\rho)$ orthogonal to $(1, -\frac{r_1}{2^\rho}, \ldots, -\frac{r_n}{2^\rho})$. Once it is found out, there is $\sum_{i=1}^{n} u_i a_i = \sum_{i=1}^{n} u_i r_i$, which leads to $\sum_{i=1}^{n} u_i q_i = 0$ since $a_i = pq_i + r_i$, i.e. $(u_1, \ldots, u_n)$ is orthogonal to $(q_1, \ldots, q_n)$.

The Third OL Attack on ACD problems was presented in [24, 36, 41]. Essentially, the corresponding lattice is generated by the row vectors of the $n \times n$ matrix

$$\begin{pmatrix} 1 & & & a_1 \\ & \ddots & & \vdots \\ & & 1 & a_{n-1} \\ & & & a_n \end{pmatrix}.$$

The strategy is to find the vector $(u_1, \ldots, u_{n-1}, \sum_{i=1}^{n} u_i a_i)$, which is orthogonal to $(-r_1, \ldots, -r_n, 1)$. That is, $\sum_{i=1}^{n} u_i a_i = \sum_{i=1}^{n} u_i r_i$, which implies that $\sum_{i=1}^{n} u_i q_i = 0$, i.e. $(u_1, \ldots, u_n)$ is orthogonal to $(q_1, \ldots, q_n)$.

Hence, it is easy to see that the common point of existing OL attacks for solving ACD problems is to find out vectors orthogonal to $(q_1, \ldots, q_n)$.

3 Optimization of OL Attacks

In this section, we first present an upper bound of the reduced vector lengths and then put forward the optimizations of OL attacks.

For (γ, η, ρ)-ACD problem with n given samples $a_i (i = 1, \cdots, n)$, there are n equations $a_i = p * q_i + r_i$ where p, q_i, r_i are unknown. Our goal is to recover common divisor p. Our approach is as follows.

- First, we design a lattice to find vectors orthogonal to unknown vector $(q_1, \cdots, q_n)$.
- Once sufficiently many such vectors are found, we can recover $(q_1, \cdots, q_n)$ by soving the corresponding linear equations.
- Then, we obtain r_i if $\eta > \rho$ as $r_i = a_i \mod q_i$.
- Finally, we get p by computing $\gcd(a_1 - r_1, \cdots, a_n - r_n)$.

3.1 Upper Bound of Lengths of Reduced Basis Vectors

Let $\mathbf{b}_i$ be the i-th BKZ-β reduced basis vector of an n-dimensional lattice $\mathcal{L}$ and $\widetilde{\mathbf{b}}_i$ be the corresponding Gram Schmidt vector. According to Definitions 1 and 2, we get that the reduced basis vectors $\mathbf{b}_i$ satisfy

$$\|\mathbf{b}_i\|^2 = \|\widetilde{\mathbf{b}}_i\|^2 + \sum_{j=1}^{i-1} \mu_{i,j}^2 \|\widetilde{\mathbf{b}}_j\|^2 \leq \|\widetilde{\mathbf{b}}_i\|^2 + \frac{1}{4} \sum_{j=1}^{i-1} \|\widetilde{\mathbf{b}}_j\|^2.$$

From Definition 3 (Geometric Series Assumption), we have

$$\|\mathbf{b}_i\|^2 \leq \left(\theta^{2i-2} + \frac{1}{4} \sum_{j=1}^{i-1} \theta^{2j-2} \right) \cdot \|\mathbf{b}_1\|^2 \leq \frac{i+3}{4} \cdot \|\mathbf{b}_1\|^2.$$

Then, based on the Hermite factor $\|\mathbf{b}_1\| = \delta_0^n \, (\det \mathcal{L})^{\frac{1}{n}}$, we obtain

$$\|\mathbf{b}_i\| \leq \frac{\sqrt{i+3}}{2} \cdot \delta_0^n (\det \mathcal{L})^{\frac{1}{n}}. \tag{1}$$

For the case of LLL, we can also get the above inequality. The similar inequality on the LLL reduced basis has been assumed in [27].

3.2 Finding Vectors Orthogonal to $(q_1, \ldots, q_n)$

For n samples of a (γ, η, ρ)-ACD problem, $a_1, \ldots, a_n$, we define a lattice $\mathcal{L}_2(\alpha)$ parameterized by α, which is spanned by the row vectors of the following $n \times (n+1)$ matrix

$$\mathbf{M}(\alpha) := \begin{pmatrix} a_1 & \alpha & & & \\ a_2 & & \alpha & & \\ \vdots & & & \ddots & \\ a_n & & & & \alpha \end{pmatrix}$$

where $0 < \alpha < 2^{\gamma}$ and $a_1, \ldots, a_n$ are γ-bit integers. It is easy to see that $L_2(\alpha)$ is a generalization of the involved lattice in the second OL attack, which corresponds to the case of $\alpha = 2^{\rho}$. We first give the following core lemma.

Lemma 1. *Given a vector* $\mathbf{v}= (\sum_{i=1}^{n} u_i a_i, \alpha u_1, \ldots, \alpha u_n)$ *in* $\mathcal{L}_2(\alpha)$*, we have*

$$|\sum_{i=1}^{n} u_i q_i| \leq \frac{\alpha + \sqrt{n}2^{\rho}}{\alpha} \cdot \frac{\|\mathbf{v}\|}{2^{\eta-1}}.$$

Proof. According to $a_i = pq_i + r_i$ for $i = 1, \ldots, n$, we have $p\sum_{i=1}^{n} u_i q_i = \sum_{i=1}^{n} u_i a_i - \sum_{i=1}^{n} u_i r_i$. Let $\mathbf{u} = (u_1, \ldots, u_n)$ and $\mathbf{r} = (r_1, \ldots, r_n)$. From the triangle inequality and the Cauchy-Schwartz inequality, we get

$$p \cdot |\sum_{i=1}^{n} u_i q_i| \leq |\sum_{i=1}^{n} u_i a_i| + \|\mathbf{r}\| \cdot \|\mathbf{u}\|.$$

Since p is an η-bit integer and $|r_i| < 2^{\rho}$ for all $1 \leq i \leq n$, we have $p \geq 2^{\eta-1}$ and $\|\mathbf{r}\| < \sqrt{n}2^{\rho}$. Further, we get

$$2^{\eta-1} \cdot |\sum_{i=1}^{n} u_i q_i| \leq |\sum_{i=1}^{n} u_i a_i| + \sqrt{n}2^{\rho}\|\mathbf{u}\|. \tag{2}$$

Note that $\mathbf{v}= (\sum_{i=1}^{n} u_i a_i, \alpha u_1, \ldots, \alpha u_n)$ and $\alpha > 0$, thus, there are $|\sum_{i=1}^{n} u_i a_i| \leq \|\mathbf{v}\|$ and $\|\mathbf{u}\| \leq \|\mathbf{v}\|/\alpha$. Plugging these two upper bounds into (2), we have

$$|\sum_{i=1}^{n} u_i q_i| \leq \frac{\alpha + \sqrt{n}2^{\rho}}{\alpha} \cdot \frac{\|\mathbf{v}\|}{2^{\eta-1}}.$$

□

Next, we consider the case that the above $\mathbf{v}$ is the reduced basis vector of $\mathcal{L}_2(\alpha)$. Based on Lemma 1, we obtain the following result.

Corollary 1. *Let* $(\sum_{j=1}^{n} u_{ij} a_j, \alpha u_{i1}, \ldots, \alpha u_{in})$ *be the* i*-th reduced basis vector of* $\mathcal{L}_2(\alpha)$ *for* $i = 1, \ldots, n$*. Under the* GSA*, we have*

$$|u_{i1}q_1 + \cdots + u_{in}q_n| < \sqrt{i+3} \cdot \frac{\alpha + \sqrt{n}2^{\rho}}{\alpha^{\frac{1}{n}}} (n+1)^{\frac{1}{2n}} \delta_0^n 2^{\frac{\gamma}{n} - \eta}. \tag{3}$$

Further, by taking $\alpha = \frac{\sqrt{n}}{n-1}2^{\rho}$*, we get an asymptotic and optimized bound*

$$|u_{i1}q_1 + \cdots + u_{in}q_n| \leq \sqrt{(i+3)n} \cdot \delta_0^n 2^{\frac{\gamma-\rho}{n} - (\eta-\rho)}. \tag{4}$$

Proof. Under the GSA, we get (1), i.e.

$$\|(u_{i1}a_1 + \cdots + u_{in}a_n, \alpha u_{i1}, \ldots, \alpha u_{in})\| \leq \frac{\sqrt{i+3}}{2} \cdot \delta_0^n (\det \mathcal{L}_2(\alpha))^{\frac{1}{n}}$$

where $n = \dim \mathcal{L}_2(\alpha)$. Note that the determinant of $\mathcal{L}_2(\alpha)$ can be computed as $\det \mathcal{L}_2(\alpha) = \alpha^{n-1}\sqrt{\alpha^2 + a_1^2 + \cdots + a_n^2}$. Since $0 < \alpha < 2^\gamma$ and $0 < a_i < 2^\gamma$ for $i = 1, \ldots, n$, we have $\det \mathcal{L}_2(\alpha) < \sqrt{n+1}\alpha^{n-1}2^\gamma$. It implies that

$$\|(u_{i1}a_1 + \cdots + u_{in}a_n, \alpha u_{i1}, \ldots, \alpha u_{in})\| < \frac{\sqrt{i+3}}{2} \cdot (n+1)^{\frac{1}{2n}} \delta_0^n 2^{\frac{\gamma}{n}} \alpha^{\frac{n-1}{n}}.$$

From Lemma 1, we obtain the bound (3) directly, i.e.

$$|u_{i1}q_1 + \cdots + u_{in}q_n| < \sqrt{i+3} \cdot \frac{\alpha + \sqrt{n}2^\rho}{\alpha^{\frac{1}{n}}} (n+1)^{\frac{1}{2n}} \delta_0^n 2^{\frac{\gamma}{n} - \eta}.$$

Next, we minimize the upper bound of $|u_{i1}q_1 + \cdots + u_{in}q_n|$. Let $f(\alpha) = \frac{\alpha + \sqrt{n}2^\rho}{\alpha^{\frac{1}{n}}}$. As $f(\alpha)$ decreases, the upper bound becomes much tighter for fixed γ, η, ρ and n. Since the derivative of $f(\alpha)$ has the following property:

$$\begin{cases} f'(\alpha) < 0 & \text{when } 0 \le \alpha < \alpha_0, \\ f'(\alpha) = 0 & \text{when } \alpha = \alpha_0, \\ f'(\alpha) > 0 & \text{when } \alpha > \alpha_0, \end{cases}$$

where $\alpha_0 = \frac{\sqrt{n}}{n-1}2^\rho$, we have $\min\limits_{\alpha > 0} f(\alpha) = f(\alpha_0) = n\left(\frac{\sqrt{n}}{n-1}\right)^{\frac{n-1}{n}} 2^{\frac{n-1}{n}\rho}$. Plugging $f(\alpha_0)$ into (3), we get

$$|u_{i1}q_1 + \cdots + u_{in}q_n| < \sqrt{i+3} \cdot g(n) \delta_0^n 2^{\frac{\gamma-\rho}{n} - \eta + \rho},$$

where $g(n) = n\left(\frac{\sqrt{n}}{n-1}\right)^{\frac{n-1}{n}} (n+1)^{\frac{1}{2n}}$. Note that $g(n) > \sqrt{n}$ for any fixed $n \ge 2$ and $\lim_{n \to +\infty} g(n)/\sqrt{n} = 1$, the detailed analysis of which is left in Appendix A. Then we obtain an asymptotic and optimized bound (4), namely,

$$|u_{i1}q_1 + \cdots + u_{in}q_n| \le \sqrt{(i+3)n} \cdot \delta_0^n 2^{\frac{\gamma-\rho}{n} - \eta + \rho}.$$

□

Since $\mathbf{M}(\alpha)$ is a basis matrix of lattice $\mathcal{L}_2(\alpha)$ and the lattice vector

$$(\sum_{j=1}^{n} u_{ij}a_j, \alpha u_{i1}, \ldots, \alpha u_{in}) = u_{i1}\mathbf{m}_1 + \cdots + u_{in}\mathbf{m}_n,$$

where $\mathbf{m}_j$ is the j-th row vector of $\mathbf{M}(\alpha)$ for $1 \le j \le n$, we deduce that all $u_{i1}, \ldots, u_{in}$ are integers. Further, $u_{i1}q_1 + \cdots + u_{in}q_n \in \mathbb{Z}$. In order to make $u_{i1}q_1 + \cdots + u_{in}q_n = 0$, we expect that $\sqrt{(i+3)n} \cdot \delta_0^n 2^{\frac{\gamma-\rho}{n} - \eta + \rho} < 1$ based on (4). Finally, we summarize as follows.

Theorem 1. *Let* $(\sum_{j=1}^{n} u_{ij}a_j, \alpha u_{i1}, \ldots, \alpha u_{in})$ *be the* i*-th reduced basis vector of* $\mathcal{L}_2(\alpha)$ *for* $i = 1, \ldots, n$*. Take the optimized* $\alpha = \frac{\sqrt{n}}{n-1}2^{\rho}$*. Based on the* GSA*, we obtain* $u_{i1}q_1 + \cdots + u_{in}q_n = 0$ *under the condition*

$$\frac{\gamma - \rho}{n} - (\eta - \rho) + n\log\delta_0 + \log\sqrt{n(i+3)} < 0. \tag{5}$$

Remark 1. Actually, a generalization of the third OL attack also works well for our analysis. Let $\mathcal{L}_3(\alpha)$ be the lattice spanned by the row vectors of the matrix

$$\begin{pmatrix} \alpha & & & a_1 \\ & \ddots & & \vdots \\ & & \alpha & a_{n-1} \\ & & & a_n \end{pmatrix}.$$

Clearly, the corresponding lattice in the third OL attack corresponds to the case of $\alpha = 1$. For lattice $\mathcal{L}_3(\alpha)$, the optimized $\alpha = \frac{\sqrt{n^2+n}}{n-1}2^{\rho}$. Under the GSA, we can find out i linearly independent vectors orthogonal to $(q_1, \ldots, q_n)$ under the condition

$$\frac{\gamma - \rho}{n} - (\eta - \rho) + n\log\delta_0 + \log\left(n\sqrt{i+3}\right) < 0. \tag{6}$$

The detailed analysis is given in Appendix B.

3.3 Improved Lattice for OL Attack

In order to obtain more optimal space and time complexities, we reduce the entries in lattice $\mathcal{L}_2(\alpha)$ by using the rounding technique. Let $\hat{\mathcal{L}}_2(\alpha)$ be the lattice spanned by the row vectors of the following $n \times (n+1)$ matrix

$$\hat{\mathbf{M}}(\alpha) = \begin{pmatrix} \lfloor \frac{a_1}{\alpha} \rfloor & 1 & & \\ \lfloor \frac{a_2}{\alpha} \rfloor & & 1 & \\ \vdots & & & \ddots \\ \lfloor \frac{a_n}{\alpha} \rfloor & & & 1 \end{pmatrix}$$

where $\alpha > 0$. We present the following result, the corresponding proof of which is similar to that of Theorem 1. The difference is that the rounding operation is involved in $\hat{\mathcal{L}}_2(\alpha)$, which results in the difference between the optimized α in $\mathcal{L}_2(\alpha)$ and $\hat{\mathcal{L}}_2(\alpha)$.

Theorem 2. *Let* $(\sum_{j=1}^{n} u_{ij}\lfloor \frac{a_j}{\alpha} \rfloor, u_{i1}, \ldots, u_{in})$ *be the* i*-th reduced basis vector of* $\hat{\mathcal{L}}_2(\alpha)$ *for* $i = 1, \ldots, n$*. Take* $\alpha = \frac{\sqrt{n}}{(n-1)(\sqrt{n}+1)}2^{\rho}$*. Based on the* GSA*, we get* $u_{i1}q_1 + \cdots + u_{in}q_n = 0$ *under the condition (5), namely*

$$\frac{\gamma - \rho}{n} - (\eta - \rho) + n\log\delta_0 + \log\sqrt{n(i+3)} < 0.$$

3.4 Recovering $q_1, \ldots, q_n$ and p

Suppose that the desired $n-1$ linearly independent equations on $q_1, \ldots, q_n$ are obtained, like $u_{i1}q_1 + \cdots + u_{in}q_n = 0$ for $i = 1, \ldots, n-1$. Let integer $d = u_{n1}q_1 + \cdots + u_{nn}q_n$ and matrix $\mathbf{U} = (u_{ij})_{n\times n}$, then we have $\det \mathbf{U} = \pm 1$ and with an overwhelming probability $d = \pm 1$ (the unimodularity of $\mathbf{U}$ is not a probabilistic result), which are analyzed in Appendix C. Therefore, it follows that $\mathbf{U}(q_1, \ldots, q_n)^T = (0, \ldots, 0, \pm 1)^T$. Further, $(q_1, \ldots, q_n)^T = \mathbf{U}^{-1}(0, \ldots, 0, \pm 1)^T$. Since $q_1, \ldots, q_n$ are all nonnegative integers, let the last column of matrix $\mathbf{U}^{-1}$ be $(w_{1n}, \ldots, w_{nn})^T$, we have

$$(q_1, \ldots, q_n) = (|w_{1n}|, \ldots, |w_{nn}|)\,.$$

The Case of GACD. From $a_n = pq_n + r_n$, we get $\left\lfloor \frac{a_n}{q_n} \right\rfloor = p + \left\lfloor \frac{r_n}{q_n} \right\rfloor$. Note that a_n is a γ-bit integer, p is an η-bit integer, $|r_i| < 2^\rho$ and $\gamma > \eta > \rho$, we have

$$\left|\frac{r_n}{q_n}\right| < 2^{\rho-(\gamma-1-\eta)} = 2^{\eta-(\gamma-\rho-1)}.$$

If $\gamma > \eta + \rho$, we have $\left|\frac{r_n}{q_n}\right| < 1$, i.e., $\left\lfloor \frac{r_n}{q_n} \right\rfloor = 0$. Thus, we recover p due to $p = \left\lfloor \frac{a_n}{q_n} \right\rfloor$. If $\gamma \leq \eta + \rho$, we obtain that the $(\gamma - \rho - 1)$ most significant bits of p are respectively equal to those of $\left\lfloor \frac{a_n}{q_n} \right\rfloor$.

The Case of PACD. Without loss of generality, let $a_n = pq_n$, then $r_n = 0$. Therefore, after the desired $(q_1, \ldots, q_n)$ is obtained, we can directly recover $p = \frac{a_n}{q_n}$.

Remark 2. Even to recover p, it is actually enough to obtain a single relation from a lattice, if we repeat the attack: Choose $N = 2n$ samples a_i's and select an n-elements subset I from them. Then the attack gives a relation among the q_i's with $i \in I$. Repeat with new I's until we have enough such relations (Here we need to heuristically assume that there exist $N-1$ linear independence relations on N many q_i's).

4 Attack Complexity and Comparisons

In the section, we present the attack complexity and the corresponding comparisons.

4.1 Attack Complexity

The dominant calculation of OL attacks is the lattice reduction for finding $n-1$ linearly independent homogeneous equations on $q_1, \ldots, q_n$. Based on the condition (5), we expect that

$$\frac{\gamma - \rho}{n} - (\eta - \rho) + n \log \delta_0 + \log \sqrt{n^2 + 2n} < 0. \tag{7}$$

Since $\delta_0 > 1$ according to the GSA (see Section 2.2), the optimized OL attacks in Section 3 can work when

$$n > \frac{\gamma - \rho}{\eta - \rho}.$$

According to (7), we get $\log \delta_0 < \frac{(\eta-\rho)}{n} - \frac{\gamma-\rho}{n^2} - \frac{\log \sqrt{n^2+2n}}{n}$, which is equivalent to

$$\log \delta_0 < -(\gamma - \rho)\left(\frac{1}{n} - \frac{\eta - \rho}{2(\gamma - \rho)}\right)^2 + \frac{(\eta - \rho)^2}{4(\gamma - \rho)} - \frac{\log \sqrt{n^2 + 2n}}{n}.$$

When $n = 2(\gamma - \rho)/(\eta - \rho)$, the above expression is optimized as

$$\log \delta_0 < \frac{(\eta - \rho)^2}{4(\gamma - \rho)} - \frac{\eta - \rho}{2(\gamma - \rho)} - \frac{\eta - \rho}{4(\gamma - \rho)} \cdot \log\left(\left(\frac{\gamma - \rho}{\eta - \rho}\right)^2 + \frac{\gamma - \rho}{\eta - \rho}\right). \tag{8}$$

Remark 3. For the case of Remark 2, we need the condition

$$\frac{\gamma - \rho}{n} - (\eta - \rho) + n \log \delta_0 + \log \sqrt{4n} < 0, \tag{9}$$

the result of which is that we can reduce the logarithm term on n in (7), improving the attack slightly. Similar to the above analysis, taking $n = 2(\gamma - \rho)/(\eta - \rho)$, this condition is optimized as

$$\log \delta_0 < \frac{(\eta - \rho)^2}{4(\gamma - \rho)} - \frac{3(\eta - \rho)}{4(\gamma - \rho)} - \frac{\eta - \rho}{4(\gamma - \rho)} \cdot \log \frac{\gamma - \rho}{\eta - \rho}. \tag{10}$$

It is worth noting that we need to implement at least $N - 1 = 2n - 1$ attacks in Remark 2 in order to get sufficient linear independence on N many q_i's.

Based on the lemma from Albrecht, Player and Scott:

Lemma 2 ([3]). *The log of the time complexity to achieve a root-Hermite factor δ_0 with BKZ-β is*

$$\Omega\left(\frac{\log(1/\log \delta_0)}{\log \delta_0}\right)$$

if one SVP oracle costs $2^{\mathcal{O}(\beta)}$.

We give the following asymptotic complexity estimations.

Theorem 3. *The time complexity for solving (γ, η, ρ)-*ACD *instances is*

$$2^{\Omega\left(\frac{\gamma-\rho}{(\eta-\rho)^2} \log \frac{\gamma-\rho}{(\eta-\rho)^2}\right)}$$

by running BKZ-β *to achieve a root-Hermite factor δ_0 such that (8) or (10) holds if one* SVP *oracle costs $2^{\mathcal{O}(\beta)}$.*

Proof. From (8) or (10), it is easy to see that $\log \delta_0 \leq \frac{(\eta-\rho)^2}{4(\gamma-\rho)}(1 - o(1))$. Hence, $(1/\log \delta_0) \cdot \log(1/\log \delta_0) = \Omega\left(\frac{\gamma-\rho}{(\eta-\rho)^2} \log \frac{\gamma-\rho}{(\eta-\rho)^2}\right)$. □

Theorem 4. *For given* (γ, η, ρ)-ACD *instances and some sufficiently large security parameter* λ*, if the condition*

$$\gamma \geq \Omega\left(\frac{\lambda}{\log \lambda}(\eta-\rho)^2\right) + \rho$$

holds, then the time complexity for solving (γ, η, ρ)-ACD *instances is* 2^{λ} *by running* BKZ-β *if one* SVP *oracle costs* $2^{\mathcal{O}(\beta)}$*.*

Proof. According to Theorem 3, the log of the time complexity for solving (γ, η, ρ)-ACD instance is $\Omega\left(\frac{\gamma-\rho}{(\eta-\rho)^2}\log\frac{\gamma-\rho}{(\eta-\rho)^2}\right)$ by running BKZ-β if one SVP oracle costs $2^{\mathcal{O}(\beta)}$. Further, there exists some constant $\mathfrak{c} > 0$ such that

$$\Omega\left(\frac{\gamma-\rho}{(\eta-\rho)^2}\log\frac{\gamma-\rho}{(\eta-\rho)^2}\right) = \mathfrak{c}\cdot\frac{\gamma-\rho}{(\eta-\rho)^2}\log\frac{\gamma-\rho}{(\eta-\rho)^2} =: \lambda. \tag{11}$$

Let the function $f(x) = \frac{x}{\log x}$. Then $f(x)$ is continuous and monotone increasing when $x \geq e$. Moreover, $f(x) \geq \frac{e}{\log e} \approx 1.88$ for $x \geq e$. If we set $\lambda \geq e \cdot \mathfrak{c}$, then we have $\frac{\gamma-\rho}{(\eta-\rho)^2} \geq 2$ (otherwise if $\frac{\gamma-\rho}{(\eta-\rho)^2} < 2$, from $\lambda = \mathfrak{c}\cdot\frac{\gamma-\rho}{(\eta-\rho)^2}\log\frac{\gamma-\rho}{(\eta-\rho)^2}$ we obtain $\lambda < 2\cdot\mathfrak{c}$). Hence, there exists some $\lambda' > e$ such that $f(\lambda') = \frac{\lambda'}{\log\lambda'} = \frac{\gamma-\rho}{(\eta-\rho)^2}$. Then,

$$\frac{\gamma-\rho}{(\eta-\rho)^2}\log\frac{\gamma-\rho}{(\eta-\rho)^2} = f(\lambda')\log f(\lambda') = \lambda'\left(1-\frac{\log\log\lambda'}{\log\lambda'}\right) < \lambda'.$$

From $\lambda = \mathfrak{c}\cdot\frac{\gamma-\rho}{(\eta-\rho)^2}\log\frac{\gamma-\rho}{(\eta-\rho)^2}$, we deduce $\lambda' > \lambda/\mathfrak{c}$. Since that $f(x)$ is monotone increasing for $x \geq e$, we get $\frac{\gamma-\rho}{(\eta-\rho)^2} = f(\lambda') > f(\lambda/\mathfrak{c})$ which is equivalent to $\gamma > \left(\lambda/(\mathfrak{c}\log\frac{\lambda}{\mathfrak{c}})\right)\cdot(\eta-\rho)^2 + \rho$. That is, $\gamma \geq \Omega\left(\frac{\lambda}{\log\lambda}(\eta-\rho)^2\right) + \rho$. □

Finally, we analyze the concrete security estimation. For given parameters γ, η and ρ, we first compute the right hand side of the expressions (8) or (10), then determine the appropriate maximum δ_0, which corresponds to the minimal block size β according to $\delta_0 = \left(\frac{\beta}{2\pi e}(\pi e)^{\frac{1}{\beta}}\right)^{\frac{1}{2(\beta-1)}}$, and finally plug the δ_0 into the conditions (7) or (9), and derive the corresponding minimal n. Once such n, β are determined, we can estimate the cost of solving (γ, η, ρ)-ACD instances by using BKZ-β, which is estimated to $c\cdot n\cdot 2^{0.292\beta+16.4}$ clock cycles by using sieving [6, 38] for some small constant c according to [57, Figure 4.6]. Further, c takes 8 in [1, 2]. Note that the input of BKZ-β is the LLL-reduced basis. Hence, the main cost of BKZ-β is occupied by LLL for a small β. The running time of LLL (expressed in number of clock cycles) based on fplll-4.0.4 [14] is estimated to $0.00127\cdot n^{3.18}\cdot b_{\max}^{1.83}$ [41, Page 92] for the case of OL attacks on ACD problem, where $b_{\max}$ refers to the maximum bit-length of the involved lattice.

4.2 Comparisons

In this subsection, we give concrete comparisons with known attack methods.

Comparison of OL Attacks in Section 3. According to the analysis in Section 4.1, it is easy to see that OL attacks in Sections 3.2 and 3.3 have the same asymptotic time complexity. Note that the entries of input basis matrix of the OL attack in Section 3.3 are approximately reduced by ρ bits compared to that in Section 3.2. Hence, the OL attack in Section 3.3 will be faster in practical cryptanalysis. In typical scenarios, the OL attack in Section 3.3 only achieves a constant improvement of the overall attack complexity. Based on the time complexity in the paper [45], the speed-up that results from reducing the number of bits by ρ is $1-(\rho/\gamma)$. This improvement could be quite significant in practice.

Comparison with Existing OL Attacks. We present the comparisons on three known OL attacks as well as OL attacks in Section 3, the detailed analysis of which is presented in Appendix D. The corresponding conclusions are as follows: all these OL attacks for solving the (γ,η,ρ)-ACD problem have the same asymptotic time complexities when $\gamma \gg \rho$; the second OL attack and its optimizations are more advantageous than the first and third OL attacks when $(\gamma-\rho)$ is relatively small; the second OL attack is almost close to its optimizations.

For the security parameter λ, van Dijk et al. [56] gave the asymptotic condition to thwart the first and second attacks: $\gamma \geq \Omega(\lambda\eta^2)$ (see [41, Page 89]). Later, Cheon and Stehlé [18] improved the above condition into $\gamma \geq \Omega(\frac{\lambda}{\log\lambda}(\eta-\rho)^2)$. In this paper, we point out that the condition $\gamma \geq \Omega(\frac{\lambda}{\log\lambda}(\eta-\rho)^2)+\rho$ is needed to prevent the second OL attack and the optimized OL attacks in Section 3. Compared to the condition $\gamma \geq \Omega(\frac{\lambda}{\log\lambda}(\eta-\rho)^2)$ in [18], $\gamma \geq \Omega(\frac{\lambda}{\log\lambda}(\eta-\rho)^2)+\rho$ is better in the case that $(\gamma-\rho)$ is relatively small.

In [27], Galbraith et al. showed the success condition of the second OL attack based on the LLL algorithm. In this paper, we analyze the optimized OL attacks in Section 3 as well as three known OL attacks based on the BKZ-β algorithm and give the expression on ACD parameters γ,η,ρ, the number n of ACD samples and the root-Hermite factor δ_0. This expression can be used for estimating the concrete security of ACD-based schemes.

Comparison with the SDA Algorithm. The simultaneous Diophantine approximation (SDA) algorithm, proposed by Lagarias in [39], is also an efficient lattice method for solving ACD problems. Van Dijk et al. [56] and Galbraith et al. [27] pointed out that the SDA algorithm and the second OL attack for solving ACD problems have similar performances. Hence, the OL attack in Section 3.3 is the fastest since it employs the input basis matrix with smaller entries, especially when $(\gamma-\rho)$ is small. This fact is confirmed by our experiments.

Comparison with Multivariate Polynomial Approach. The first analysis of ACD problems was given by Howgrave-Graham by using Coppersmith's technique [35]. Then, Cohn and Heninger generalized their works to the multi-

variate setting by using many samples [19], which is known as the multivariate polynomial approach. Later, Takayasu and Kunihiro further improved the result of Cohn and Heninger by taking into account the sizes of error terms r_i [55]. The multivariate polynomial approach was also considered in [41, 27]. However, the common drawback of these works is that the dimensions and entries of the involved lattices are quite large, which affects the speed of the algorithm.

In [27], Galbraith et al. pointed out that the multivariate polynomial approach is not better than the second OL attack for practical cryptanalysis. Hence, the OL attacks in Sections 3.2 and 3.3 have more advantageous than the multivariate polynomial approach.

Comparison with the Chen-Nguyen Method. Chen and Nguyen proposed a clever exhaustive search method on error terms r_i through certain polynomials [16]. Their method only needs two samples and the corresponding time complexity is $\mathcal{O}(2^{\frac{3\rho}{2}}\gamma)$ for (γ, η, ρ)-GACD problems. With the same parameters that were given in the FHE scheme [24], their attack method is faster than the multivariate polynomial approach in [19]. Later, the Chen-Nguyen attack was revisited in [25, 41]. However, such algorithms become futile as ρ increases.

Based on the analysis in [27], the Chen-Nguyen Method and its variant [16, 25] are important for ACD problems from early FHE schemes, but are less related for Cheon-Stehlé ACD problems [18]. In this paper, we get that the asymptotic time complexity to solve (γ, η, ρ)-ACD problems is $2^{\Omega\left(\frac{\gamma-\rho}{(\eta-\rho)^2}\log\frac{\gamma-\rho}{(\eta-\rho)^2}\right)}$ for the case of optimized OL attacks. Hence, these attacks are more suitable for solving (γ, η, ρ)-ACD problems where ρ is no longer extremely smaller than η.

Comparison with Pre-processing Technique. In [27], Galbraith et al. utilized the similar idea of BKW algorithm and proposed a pre-processing technique to reduce the size of the ACD samples so that the lattice attacks are applicable to them.

Their iterative algorithm is as follows: For given n ACD samples $a_1, \ldots, a_n$, one first generate m random sums $S_1, \ldots, S_m$ of d elements of $\{a_1, \ldots, a_n\}$, i.e., $S_k = \sum_{i=1}^{d} a_{k_i}$ where $k = 1, \ldots, m$, then sorts S_k to obtain the order statistics $S_{(k)}$, further computes $m-1$ neighbouring differences $S_{(k+1)} - S_{(k)}$ and stores $\frac{m}{2}$ middle neighbouring differences as the input of next iteration. The corresponding analysis shows that the average size of the resulting samples after i iterations is $(\frac{4\sqrt{d}}{m})^i 2^{\gamma-1}$. Moreover, the total number of iterations is less than η, otherwise the error terms in ACD samples become too large to determine p. Hence, if one intends to reduce the size of samples to η bits approximately for the (γ, η, ρ)-ACD problem, then one should set $\eta \approx i\log_2(\frac{4\sqrt{d}}{m}) + \gamma - 1$. Plugging the optimal $i \approx \eta$ into this relation, one can deduce that the involved m is close to $2^{\frac{\gamma}{\eta}}$. However, such an m is so large for the (γ, η, ρ)-ACD problem in [25] that this technique is not practical in this situation.

The aim of both the technique of pre-processing and the approach in Section 3.3 is to reduce the entries of the lattices that are processed, even though the ideas are different. Note that the method of pre-processing the ACD samples is

implemented before the lattice attacks perform and our strategy in Section 3.3 is to improve the OL attacks. Hence, one may be able to try to use this preprocessing technique and then carry out the approach in Section 3.3 to solve the ACD problems. In this paper, we do not consider employing the preprocessing method before OL attacks. We will try it in the future work.

5 Cryptanalysis of ACD-based FHE Schemes

In this section, we analyze ACD problems in the FHE schemes [56, 47, 18, 37].

The DGHV Scheme was proposed by van Dijk, Gentry, Halevi and Vaikuntanathan [56], which is the first ACD-based FHE scheme. The authors set parameters in [56, Section 3] as follows:

$$\rho = \lambda, \eta = \Theta(\lambda^2 \log^2 \lambda), \gamma = \Omega(\lambda^5 \log^4 \lambda).$$

According to Theorem 3 in Section 4.1 and (19) in Appendix D, the asymptotic time complexity for solving (γ, η, ρ)-ACD instances are summarized as Table 2.

Table 2. The log of the time complexities with the parameters in the DGHV scheme.

First OL	Second OL	Third OL	OL Attacks in Section 3
$\Omega(\lambda \log \lambda)$	$\Omega(\lambda \log \lambda)$	$\Omega(\lambda \log \lambda)$	$\Omega(\lambda \log \lambda)$

According to Table 2, we get that such parameters are conservative to get $\Omega(\lambda)$-bit security for the case of OL attacks. Further, according to Theorem 4, one can use $\gamma = \Omega(\frac{\lambda}{\log \lambda}\eta^2)$ instead of $\gamma = \Omega(\lambda\eta^2)$ in order to achieve λ-bit security.

The Nuida-Kurosawa Scheme was given by Nuida and Kurosawa [47]. This is an ACD-based FHE scheme for non-binary message spaces. The authors set

$$\rho = \Theta(\lambda \log\log\log \lambda), \eta = \Theta(\lambda^2 \log\log \lambda), \gamma = \Theta(\lambda^4 \log^2 \lambda).$$

Based on Theorem 3 in Section 4.1 and (19) in Appendix D, we present the corresponding asymptotic time complexities in Table 3.

Table 3. The log of the time complexities with the parameters in the Nuida-Kurosawa scheme.

First OL	Second OL	Third OL	OL Attacks in Section 3
$\Omega\left(\frac{\log^2 \lambda}{\log\log \lambda}\right)$	$\Omega\left(\frac{\log^2 \lambda}{\log\log \lambda}\right)$	$\Omega\left(\frac{\log^2 \lambda}{\log\log \lambda}\right)$	$\Omega\left(\frac{\log^2 \lambda}{\log\log \lambda}\right)$

Note that $\lim_{\lambda\to\infty}\left(\frac{\log^2\lambda}{\log\log\lambda}/\lambda\right) = 0$. Hence, the above parameter choices are optimistic to achieve $\Omega(\lambda)$-bit security for the case of OL attacks. Furthermore, based on Theorem 4, one can take $\gamma = \Theta(\frac{\lambda^5(\log\log\lambda)^2}{\log\lambda})$ instead of $\gamma = \Theta(\lambda^4\log^2\lambda)$ for obtaining λ-bit security.

The Kim-Tibouchi Scheme was put forward by Kim and Tibouchi in [37]. This is based on the Nuida-Kurosawa Scheme. The authors studied the dependence of the message size Q and gave the following parameters:

$$\rho = \Theta(\lambda\log\log\log\lambda), \eta = \Theta(Q^3\lambda^2\log\log\lambda), \gamma = \Theta(Q^6\lambda^4\log^2\lambda).$$

Similar to the analysis of the Nuida-Kurosawa Scheme, we give the corresponding asymptotic time complexities in Table 4. It is easy to see that such Q does not effect the asymptotic time complexities of OL attacks compared to the case of the Nuida-Kurosawa Scheme. Therefore, the corresponding parameter choices are also optimistic to achieve $\Omega(\lambda)$-bit security for the case of OL attacks.

Table 4. The log of the time complexities with the parameters in the Kim-Tibouchi scheme.

First OL	Second OL	Third OL	OL Attacks in Section 3
$\Omega\left(\frac{\log^2\lambda}{\log\log\lambda}\right)$	$\Omega\left(\frac{\log^2\lambda}{\log\log\lambda}\right)$	$\Omega\left(\frac{\log^2\lambda}{\log\log\lambda}\right)$	$\Omega\left(\frac{\log^2\lambda}{\log\log\lambda}\right)$

The Cheon-Stehlé Scheme was designed by Cheon and Stehlé [18] based on (γ,η,ρ)-ACD problems with $\eta-\rho = L\log\lambda$ where $L > 0$ is chosen to provide the desired functionality. Because this scheme is relatively slow compared to those based on Ring-LWE, the variant with truncated ciphertexts were proposed in [18, Section 5] in order to accelerate. The authors point out a guess attack as follows: Given a (γ,η,ρ)-ACD sample $a_i = pq_i + r_i$, one first guesses the $(\gamma-\eta)$ bits of q_i and then compute $\lfloor\frac{a_i}{q_i}\rceil = p + \lfloor\frac{r_i}{q_i}\rceil$. Since $\frac{r_i}{q_i} < 2^{\rho-(\gamma-\rho)}$, one can obtain the $(\gamma-\rho)$ most significant bits of approximate common divisor p from a (γ,η,ρ)-GACD sample, which is significant from the view of security. To prevent the above attack, one can set $\lambda = (\gamma-\eta)$. Note that $\eta-\rho = L\log\lambda$, one gets $\gamma-\rho = (\gamma-\eta)+(\eta-\rho) = \lambda + L\log\lambda$, which raised the question of taking GACD instances with small $(\gamma-\rho)$. The authors put forward the following open problem in [18, Section 1].

If $\gamma-\rho \approx \lambda+\Omega(\log\lambda)$ turns out to be safe, then the ciphertext bit-sizes of the variant scheme based on truncation can be made quite small.

In fact, the authors do not explicitly give the parameter set of this variant scheme. According to the analysis in [18], the relation $\gamma \geq \Omega(\frac{\lambda}{\log\lambda}(\eta-\rho)^2)$ should be satisfied in order to prevent from lattice-based attacks. Hence, one

can take the following parameter set

$$\left\{(\gamma,\eta,\rho) \mid \gamma=\Omega(L^2\lambda\log\lambda),\eta=\gamma-\lambda,\rho=\eta-L\log\lambda\right\} \tag{12}$$

According to Theorem 3 in Section 4.1 and (19) in Appendix D, we get the asymptotic time complexities to obtain the $(\gamma-\rho)$ most significant bits of p about Parameter Set (12) for OL attacks. We present the corresponding result in Table 5. It is easy to see that the second OL attack and OL attacks in Section 3 have more advantages.

Table 5. The log of the time complexities with Parameter Set (12).

Guess Attack [18]	First OL	Second OL	Third OL	OL Attacks in Section 3
λ	$\Omega(\lambda)$	$\Omega(\frac{\lambda}{\log\lambda})$	$\Omega(\lambda)$	$\Omega(\frac{\lambda}{\log\lambda})$

6 Cryptanalysis of the Implicit Factorization Problem

In this section, we give the corresponding comparisons for solving the implicit factorization problem [42], which was first introduced in PKC 2009 by May and Ritzenhofen. This problem is stated as follows:

Suppose n γ-bit integers $a_i = x_i y_i$ are given for $i = 1,\ldots,n$, where $x_1,\ldots,x_n$ are η-bit primes and $y_1,\ldots,y_n$ are $(\gamma-\eta)$-bit primes. Given that certain portions of the bit pattern in $x_1, x_2, \ldots, x_n$ are common, the question is under what condition it is possible to factor $a_1,\ldots,a_n$ efficiently.

First, we follow the idea about transforming the implicit factorization problem into the ACD problem in [49]. Suppose that η-bit integers $x_1,\ldots,x_n$ share τ MSBs for larger values of n. We write $x_1 - x_i = z_i$ for $i = 1,\ldots,n$ where $|z_i| < 2^{\eta-\delta}$. Further, we have $a_i = x_i y_i = (x_1 - z_i)y_i$. Let $p = x_1$, $q_i = y_i$ and $r_i = -y_i z_i$ for all $1 \le i \le n$. We rearrange the above equations and get

$$a_i = pq_i + r_i \text{ for } i = 1,\ldots,n \tag{13}$$

Note that $a_1,\ldots,a_n$ are γ-bit integers, p is a η-bit integer, $r_1 = 0$ and $|r_i| = |y_i z_i| \le 2^{(\gamma-\eta)+(\eta-\tau)} = 2^{\gamma-\tau}$. Therefore, the system (13) can be regarded as a $(\gamma,\eta,\gamma-\tau)$-PACD problem, of which n samples are given. Once (13) is solved, since $p = x_1$, we can factor a_1. Moreover, we can also recover $r_i = a_i \bmod p$ if $\gamma - \tau < \eta$ (i.e. $\tau > \gamma - \eta$). Further, we factor a_i $(2 \le i \le n)$ by computing $\gcd(a_i, r_i)$, which implies that the implicit factorization problem is solved.

Next, we utilize the attack in Section 3.3 and the second OL attack to solve (13). According to the required condition (7), we get that the $(\gamma,\eta,\gamma-\tau)$-PACD problem can be solved when $\frac{\tau}{n} + (\gamma - \eta - \tau) + n\log\delta_0 + \log\sqrt{n^2+n} \le 0$. Since we focus on the number of shared bits in the implicit factorization problem, we

simplify the above condition as $\frac{\tau}{n} + (\gamma - \eta - \tau) < 0$, which implies that the number δ of shared MSBs in $p_1, \ldots, p_n$ should satisfy $\tau > \frac{n}{n-1}(\gamma - \eta)$.

Finally, let us compare our work with previous results in [26, 49]. For the case of [26], the number of shared MSBs should not be less than $\frac{n}{n-1}(\gamma-\eta)+6$ for $n \geq 3$. For the situation of [49], the number of shared bits is greater than $\frac{n}{n-1}(\gamma-\eta)$, which is obtained by solving (13) according to the SDA algorithm. It is easy to see that our theoretical result and the work of [49] are almost the same and slightly better than the result of [26].

Experimental Results. The experiments are implemented in the Sage 7.4 on Linux Ubuntu 16.04 on a laptop with Intel(R) Xeon(R) CPU E5-2670 v3 @ 2.30GHz, 3 GB RAM and 3 MB Cache. We respectively use the method in Section 3.3, the second OL attack and the method of [49] based on the LLL algorithm to solve the implicit factorization problem.[4] In the experiments, the desired $(q_1, \ldots, q_n)$ can be recovered successfully. Further, the implicit factorization problem is solved. We give the concrete comparisons in Table 6. It is clear that the attack in Section 3.3 is the most efficient in practice.

Table 6. Cryptanalysis of the implicit factorization problem instances by the attack in Section 3.3, the second OL attack and the work in [49] based on the LLL algorithm.

γ (bit-size of a_i)	η, $\gamma - \eta$ (bit-size of x_i, y_i)	τ (shared MSBs)	n (exp.)	Section 3.3 (seconds)	Second OL (seconds)	[49] (seconds)
1024	774, 250	264	42	0.094	0.531	1.516
	724, 300	314	61	< 1	< 1	1.39
	674, 350	364	88	< 1	1.42	5.57
	624, 400	414	95	1.26	2.0	7.15
	574, 450	464	101	1.73	2.48	9.69
	524, 500	514	108	2.14	3.44	13.27
2048	1398, 650	668	84	3.92	9.18	14.76
	1348, 700	718	99	2.81	6.37	23.41
	1298, 750	768	129	5.98	13.59	54.46
	1248, 800	816	141	7.79	17.24	73.36
	1198, 850	867	146	9.22	21.08	86.48
	1148, 900	919	150	11.80	23.88	100.85

7 Conclusion

In this paper, orthogonal lattice attacks for solving ACD problems were revisited, the optimized OL attacks were proposed, and the theoretical proofs as well as the informative experimental results were presented to support our analyses.

[4] According to the experimental results in [49], the method in [49] is much faster than that in [26] for larger values of n. Thus, we omit the corresponding experiments in [26].

Then, we used the optimized OL attacks and the existing methods to analyze the security estimates of some ACD problems from FHE schemes. Moreover, we also utilized these methods to solve the implicit factorization problem. In our optimized OL attack using the rounding operation, the entries of the involved lattice are reduced so that it becomes the fastest and the most efficient till date in practice.

References

1. Martin R. Albrecht. On dual lattice attacks against small-secret LWE and parameter choices in helib and SEAL. In *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part II*, pages 103–129, 2017.
2. Martin R. Albrecht, Florian Göpfert, Fernando Virdia, and Thomas Wunderer. Revisiting the expected cost of solving uSVP and applications to LWE. In *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part I*, pages 297–322, 2017.
3. Martin R. Albrecht, Rachel Player, and Sam Scott. On the concrete hardness of learning with errors. *J. Mathematical Cryptology*, 9(3):169–203, 2015.
4. Jacob Alperin-Sheriff and Chris Peikert. Faster bootstrapping with polynomial error. In Juan A. Garay and Rosario Gennaro, editors, *Advances in Cryptology – CRYPTO 2014*, volume 8616 of *Lecture Notes in Computer Science*, pages 297–314. Springer Berlin Heidelberg, 2014.
5. Yoshinori Aono, Yuntao Wang, Takuya Hayashi, and Tsuyoshi Takagi. Improved progressive BKZ algorithms and their precise cost estimation by sharp simulator. In *Proceedings of the 35th Annual International Conference on Advances in Cryptology — EUROCRYPT 2016 - Volume 9665*, pages 789–819, New York, NY, USA, 2016. Springer-Verlag New York, Inc.
6. Anja Becker, Léo Ducas, Nicolas Gama, and Thijs Laarhoven. New directions in nearest neighbor searching with applications to lattice sieving. In *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2016, Arlington, VA, USA, January 10-12, 2016*, pages 10–24, 2016.
7. Daniel Benarroch, Zvika Brakerski, and Tancrède Lepoint. FHE over the integers: Decomposed and batched in the post-quantum regime. In *Public-Key Cryptography - PKC 2017 - 20th IACR International Conference on Practice and Theory in Public-Key Cryptography, Amsterdam, The Netherlands, March 28-31, 2017, Proceedings, Part II*, pages 271–301, 2017.
8. Jingguo Bi, Jean-Sébastien Coron, Jean-Charles Faugère, Phong Q. Nguyen, Guénaël Renault, and Rina Zeitoun. Rounding and chaining LLL: finding faster small roots of univariate polynomial congruences. In *Public-Key Cryptography - PKC 2014 - 17th International Conference on Practice and Theory in Public-Key Cryptography, Buenos Aires, Argentina, March 26-28, 2014. Proceedings*, pages 185–202, 2014.
9. Zvika Brakerski. Fully homomorphic encryption without modulus switching from classical GapSVP. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology – CRYPTO 2012*, volume 7417 of *Lecture Notes in Computer Science*, pages 868–886. Springer Berlin Heidelberg, 2012.

10. Zvika Brakerski, Craig Gentry, and Shai Halevi. Packed ciphertexts in LWE-based homomorphic encryption. In Kaoru Kurosawa and Goichiro Hanaoka, editors, *Public-Key Cryptography – PKC 2013*, volume 7778 of *Lecture Notes in Computer Science*, pages 1–13. Springer Berlin Heidelberg, 2013.
11. Zvika Brakerski and Vinod Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. In *Proceedings of the 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science*, FOCS '11, pages 97–106, Washington, DC, USA, 2011. IEEE Computer Society.
12. Zvika Brakerski and Vinod Vaikuntanathan. Fully homomorphic encryption from Ring-LWE and security for key dependent messages. In Phillip Rogaway, editor, *Advances in Cryptology – CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 505–524. Springer Berlin Heidelberg, 2011.
13. Zvika Brakerski and Vinod Vaikuntanathan. Lattice-based FHE as secure as PKE. In *Proceedings of the 5th Conference on Innovations in Theoretical Computer Science*, ITCS '14, pages 1–12, New York, NY, USA, 2014. ACM.
14. David Cadé, Xavier Pujol, , and Damien Stehlé. fplll, 4.0.4 edition, 2013.
15. Yuanmi Chen and Phong Q. Nguyen. BKZ 2.0: Better lattice security estimates. In *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*, pages 1–20, 2011.
16. Yuanmi Chen and Phong Q. Nguyen. Faster algorithms for approximate common divisors: Breaking fully-homomorphic-encryption challenges over the integers. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology – EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 502–519. Springer Berlin Heidelberg, 2012.
17. JungHee Cheon, Jean-Sbastien Coron, Jinsu Kim, MoonSung Lee, Tancrde Lepoint, Mehdi Tibouchi, and Aaram Yun. Batch fully homomorphic encryption over the integers. In Thomas Johansson and Phong Q. Nguyen, editors, *Advances in Cryptology – EUROCRYPT 2013*, volume 7881 of *Lecture Notes in Computer Science*, pages 315–335. Springer Berlin Heidelberg, 2013.
18. JungHee Cheon and Damien Stehlé. Fully homomorphic encryption over the integers revisited. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology – EUROCRYPT 2015*, volume 9056 of *Lecture Notes in Computer Science*, pages 513–536. Springer Berlin Heidelberg, 2015.
19. Henry Cohn and Nadia Heninger. Approximate common divisors via lattices. *The Open Book Series*, 1(1):271–293, 2013.
20. Henry Cohn and Nadia Heninger. Ideal forms of Coppersmith's theorem and Guruswami-Sudan list decoding. *Adv. in Math. of Comm.*, 9(3):311–339, 2015.
21. Jean-Sébastien Coron, Tancrède Lepoint, and Mehdi Tibouchi. Practical multilinear maps over the integers. In *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I*, pages 476–493, 2013.
22. Jean-Sébastien Coron, Tancrède Lepoint, and Mehdi Tibouchi. New multilinear maps over the integers. In *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I*, pages 267–286, 2015.
23. Jean-Sbastien Coron, Tancrde Lepoint, and Mehdi Tibouchi. Scale-invariant fully homomorphic encryption over the integers. In Hugo Krawczyk, editor, *Public-Key Cryptography – PKC 2014*, volume 8383 of *Lecture Notes in Computer Science*, pages 311–328. Springer Berlin Heidelberg, 2014.

24. Jean-Sbastien Coron, Avradip Mandal, David Naccache, and Mehdi Tibouchi. Fully homomorphic encryption over the integers with shorter public keys. In Phillip Rogaway, editor, *Advances in Cryptology – CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 487–504. Springer Berlin Heidelberg, 2011.
25. Jean-Sbastien Coron, David Naccache, and Mehdi Tibouchi. Public key compression and modulus switching for fully homomorphic encryption over the integers. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology – EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 446–464. Springer Berlin Heidelberg, 2012.
26. Jean-Charles Faugère, Raphaël Marinier, and Guénaël Renault. Implicit factoring with shared most significant and middle bits. In *Proceedings of the 13th International Conference on Practice and Theory in Public Key Cryptography*, PKC'10, pages 70–87, Berlin, Heidelberg, 2010. Springer-Verlag.
27. Steven D Galbraith, Shishay W Gebregiyorgis, and Sean D Murphy. Algorithms for the approximate common divisor problem. In *Proceedings of Twelfth Algorithmic Number Theory Symposium (ANTS-XII)*, 2016.
28. Nicolas Gama and Phong Q. Nguyen. Predicting lattice reduction. In *Advances in Cryptology - EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13-17, 2008. Proceedings*, pages 31–51, 2008.
29. Craig Gentry. Fully homomorphic encryption using ideal lattices. In *Proceedings of the Forty-first Annual ACM Symposium on Theory of Computing*, STOC '09, pages 169–178, New York, NY, USA, 2009. ACM.
30. Craig Gentry and Shai Halevi. Implementing Gentry's fully-homomorphic encryption scheme. In KennethG. Paterson, editor, *Advances in Cryptology – EUROCRYPT 2011*, volume 6632 of *Lecture Notes in Computer Science*, pages 129–148. Springer Berlin Heidelberg, 2011.
31. Craig Gentry, Shai Halevi, and Nigel P. Smart. Fully homomorphic encryption with polylog overhead. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology C EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 465–482. Springer Berlin Heidelberg, 2012.
32. Craig Gentry, Shai Halevi, and Nigel P. Smart. Homomorphic evaluation of the AES circuit. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology – CRYPTO 2012*, volume 7417 of *Lecture Notes in Computer Science*, pages 850–867. Springer Berlin Heidelberg, 2012.
33. Craig Gentry, Amit Sahai, and Brent Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology – CRYPTO 2013*, volume 8042 of *Lecture Notes in Computer Science*, pages 75–92. Springer Berlin Heidelberg, 2013.
34. Guillaume Hanrot, Xavier Pujol, and Damien Stehlé. Analyzing blockwise lattice algorithms using dynamical systems. In *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*, pages 447–464, 2011.
35. Nick Howgrave-Graham. Approximate integer common divisors. In JosephH. Silverman, editor, *Cryptography and Lattices*, volume 2146 of *Lecture Notes in Computer Science*, pages 51–66. Springer Berlin Heidelberg, 2001.
36. Ding Jintai and Tao Chengdong. A new algorithm for solving the general approximate common divisors problem and cryptanalysis of the FHE based on the GACD problem. Cryptology ePrint Archive, Report 2014/042, 2014. `http://eprint.iacr.org/`.

37. Eunkyung Kim and Mehdi Tibouchi. FHE over the integers and modular arithmetic circuits. In *Cryptology and Network Security - 15th International Conference, CANS 2016, Milan, Italy, November 14-16, 2016, Proceedings*, pages 435–450, 2016.
38. Thijs Laarhoven. Sieving for shortest vectors in lattices using angular locality-sensitive hashing. In *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I*, pages 3–22, 2015.
39. J. C. Lagarias. The computational complexity of simultaneous Diophantine approximation problems. *SIAM J. Comput.*, 14(1):196–209, 1985.
40. Arjen Klaas Lenstra, Hendrik Willem Lenstra, and László Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4):515–534, 1982.
41. Tancrède Lepoint. *Design and Implementation of Lattice-Based Cryptography*. Theses, Ecole Normale Supérieure de Paris - ENS Paris, June 2014.
42. Alexander May and Maike Ritzenhofen. *Public Key Cryptography – PKC 2009: 12th International Conference on Practice and Theory in Public Key Cryptography, Irvine, CA, USA, March 18-20, 2009. Proceedings*, chapter Implicit Factoring: On Polynomial Time Factoring Given Only an Implicit Hint, pages 1–14. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.
43. Phong Q. Nguyen and Jacques Stern. Merkle-Hellman revisited: A cryptanalysis of the Qu-Vanstone cryptosystem based on group factorizations. In *Advances in Cryptology - CRYPTO '97, 17th Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 1997, Proceedings*, pages 198–212, 1997.
44. Phong Q. Nguyen and Brigitte Vallée, editors. *The LLL Algorithm - Survey and Applications*. Information Security and Cryptography. Springer, 2010.
45. Andrew Novocin, Damien Stehlé, and Gilles Villard. An LLL-reduction algorithm with quasi-linear time complexity: extended abstract. In *Proceedings of the 43rd ACM Symposium on Theory of Computing, STOC 2011, San Jose, CA, USA, 6-8 June 2011*, pages 403–412, 2011.
46. Andrew Novocin, Damien Stehlé, and Gilles Villard. An LLL-reduction algorithm with quasi-linear time complexity: Extended abstract. In *Proceedings of the Forty-third Annual ACM Symposium on Theory of Computing*, STOC '11, pages 403–412, New York, NY, USA, 2011. ACM.
47. Koji Nuida and Kaoru Kurosawa. (batch) fully homomorphic encryption over integers for non-binary message spaces. In *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I*, pages 537–555, 2015.
48. Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proceedings of the Thirty-seventh Annual ACM Symposium on Theory of Computing*, STOC '05, pages 84–93, New York, NY, USA, 2005. ACM.
49. S. Sarkar and S. Maitra. Approximate integer common divisor problem relates to implicit factorization. *IEEE Transactions on Information Theory*, 57(6):4002–4013, June 2011.
50. Claus-Peter Schnorr. Lattice reduction by random sampling and birthday methods. In *STACS 2003, 20th Annual Symposium on Theoretical Aspects of Computer Science, Berlin, Germany, February 27 - March 1, 2003, Proceedings*, pages 145–156, 2003.
51. Claus-Peter Schnorr and M. Euchner. Lattice basis reduction: Improved practical algorithms and solving subset sum problems. *Math. Program.*, 66:181–199, 1994.

52. Claus-Peter Schnorr and Horst Helmut Hörner. Attacking the Chor-Rivest cryptosystem by improved lattice reduction. In *Advances in Cryptology - EUROCRYPT '95, International Conference on the Theory and Application of Cryptographic Techniques, Saint-Malo, France, May 21-25, 1995, Proceeding*, pages 1–12, 1995.
53. N.P. Smart and F. Vercauteren. Fully homomorphic encryption with relatively small key and ciphertext sizes. In Phong Q. Nguyen and David Pointcheval, editors, *Public Key Cryptography – PKC 2010*, volume 6056 of *Lecture Notes in Computer Science*, pages 420–443. Springer Berlin Heidelberg, 2010.
54. Damien Stehlé and Ron Steinfeld. Faster fully homomorphic encryption. In Masayuki Abe, editor, *Advances in Cryptology - ASIACRYPT 2010*, volume 6477 of *Lecture Notes in Computer Science*, pages 377–394. Springer Berlin Heidelberg, 2010.
55. Atsushi Takayasu and Noboru Kunihiro. Better lattice constructions for solving multivariate linear equations modulo unknown divisors. In Colin Boyd and Leonie Simpson, editors, *Information Security and Privacy*, volume 7959 of *Lecture Notes in Computer Science*, pages 118–135. Springer Berlin Heidelberg, 2013.
56. Marten van Dijk, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan. Fully homomorphic encryption over the integers. In Henri Gilbert, editor, *Advances in Cryptology – EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 24–43. Springer Berlin Heidelberg, 2010.
57. Chen Yuanmi. *Réduction de réseau et sécurité concrète du chiffrement complètement homomorphe.* Ph.d theses, Paris 7, June 2013.

A Analysis on the function $g(n)$

According to $g(n) = n\left(\frac{\sqrt{n}}{n-1}\right)^{\frac{n-1}{n}}(n+1)^{\frac{1}{2n}}$, we have

$$\frac{g(n)}{\sqrt{n}} = \sqrt{n}\left(\frac{\sqrt{n}}{n-1}\right)^{\frac{n-1}{n}}(n+1)^{\frac{1}{2n}} = \frac{n}{n-1}\cdot(n-1)^{\frac{1}{n}}\left(\frac{n+1}{n}\right)^{\frac{1}{2n}}.$$

For any fixed $n \geq 2$, we have $(n-1)^{\frac{1}{n}} > 1$ and $\left(\frac{n+1}{n}\right)^{\frac{1}{2n}} > 1$. Hence, we get $\frac{g(n)}{\sqrt{n}} > 1$. Furthermore, since $\lim_{n\to+\infty}(n-1)^{\frac{1}{n}} = 1$ and $\lim_{n\to+\infty}\left(\frac{n+1}{n}\right)^{\frac{1}{2n}} = 1$, we obtain $\lim_{n\to+\infty} g(n)/\sqrt{n} = 1$.

B Optimization of the Third OL Attack

We first consider a generalized lattice $\mathcal{L}_3(\alpha)$. Without loss of generality, assume $a_n = \max\{a_1, \ldots, a_n\}$ and $0 < \alpha \leq a_n$. Then we give the following lemma.

Lemma 3. *Given a vector* $\mathbf{v} = (\alpha u_1, \ldots, \alpha u_{n-1}, \sum_{i=1}^{n} u_i a_i)$ *in* $\mathcal{L}_3(\alpha)$*, then*

$$|\sum_{i=1}^{n} u_i q_i| \leq \frac{\alpha + 2^{\rho}\sqrt{n^2+2n}}{\alpha}\cdot\frac{\|\mathbf{v}\|}{2^{\eta-1}}.$$

Proof. Let $\mathbf{u} = (u_1, \ldots, u_n)$, $\mathbf{r} = (r_1, \ldots, r_n)$ and $v_n = \sum_{i=1}^{n} u_i a_i$. Similar to the analysis of Lemma 1, we can also get (2), i.e.

$$2^{\eta-1} \cdot |\sum_{i=1}^{n} u_i q_i| \leq |v_n| + \sqrt{n} 2^{\rho} \cdot \|\mathbf{u}\|.$$

Then let us bound $|v_n|$ and $\|\mathbf{u}\|$. Obviously $|v_n| \leq \|\mathbf{v}\|$ and $\sqrt{u_1^2 + \cdots + u_{n-1}^2} \leq \|\mathbf{v}\|/\alpha$. From $v_n = \sum_{i=1}^{n} u_i a_i$, we have $u_n = (v_n - u_1 a_1 - \cdots - u_{n-1} a_{n-1})/a_n$. Then we get

$$\begin{aligned}
|u_n| &= \left| \frac{v_n \cdot 1 - (\alpha u_1) \cdot \frac{a_1}{\alpha} - \cdots - (\alpha u_{n-1}) \cdot \frac{a_{n-1}}{\alpha}}{a_n} \right| \\
&\leq \frac{\sqrt{1^2 + (\frac{a_1}{\alpha})^2 + \cdots + (\frac{a_{n-1}}{\alpha})^2}}{a_n} \cdot \sqrt{v_n^2 + (\alpha u_1)^2 + \cdots + (\alpha u_{n-1})^2} \\
&\qquad \text{(According to the Cauchy} - \text{Schwartz inequality)} \\
&= \sqrt{(\frac{1}{a_n})^2 + \frac{(\frac{a_1}{a_n})^2}{\alpha^2} + \cdots + \frac{(\frac{a_{n-1}}{a_n})^2}{\alpha^2}} \cdot \|\mathbf{v}\| \\
&\leq \frac{\sqrt{n}}{\alpha} \|\mathbf{v}\|. \text{ (Since } 0 < \alpha \leq a_n = \max\{a_1, \ldots, a_n\})
\end{aligned}$$

From the above inequality and $\sqrt{u_1^2 + \cdots + u_{n-1}^2} \leq \|\mathbf{v}\|/\alpha$, we deduce $\|\mathbf{u}\| = \sqrt{(u_1^2 + \cdots + u_{n-1}^2) + u_n^2} \leq \frac{\sqrt{n+1}}{\alpha} \|\mathbf{v}\|$. Plugging these two bounds of $|v_n|$ and $\|\mathbf{u}\|$ into (2), we obtain

$$|\sum_{i=1}^{n} u_i q_i| \leq \frac{\alpha + 2^{\rho}\sqrt{n^2 + n}}{\alpha} \cdot \frac{\|\mathbf{v}\|}{2^{\eta-1}}.$$

□

Based on Lemma 3, we present the following result.

Corollary 2. *Let $\mathbf{v}_i = (\alpha u_{i1}, \ldots, \alpha u_{i,n-1}, \sum_{j=1}^{n} u_{ij} a_j)$ be the i-th reduced basis vector of $\mathcal{L}_3(\alpha)$ where $1 \leq i \leq n$. From the* GSA*, we have*

$$|\sum_{j=1}^{n} u_{ij} q_j| \leq \sqrt{i+3} \cdot \frac{\alpha + 2^{\rho}\sqrt{n^2 + n}}{\alpha^{\frac{1}{n}}} \delta_0^n 2^{\frac{\gamma}{n} - \eta}. \tag{14}$$

Further, by choosing $\alpha = \frac{\sqrt{n^2+n}}{n-1} 2^{\rho}$, we obtain an asymptotic and optimized bound

$$|\sum_{j=1}^{n} u_{ij} q_j| \leq \sqrt{i+3} \cdot n \delta_0^n 2^{\frac{\gamma-\rho}{n} - (\eta-\rho)}. \tag{15}$$

Proof. Under the GSA, we have

$$\|\mathbf{v}_i\| \leq \frac{\sqrt{i+3}}{2} \delta_0^n \left(\det \mathcal{L}_3(\alpha)\right)^{\frac{1}{n}} \leq \frac{\sqrt{i+3}}{2} \delta_0^n 2^{\frac{\gamma}{n}} \alpha^{1-\frac{1}{n}}.$$

According to Lemma 3, we can directly deduce the bound (14). Then, let us minimize the right side of (14) by taking $\alpha = \frac{\sqrt{n^2+n}}{n-1}2^{\rho}$ and get $|\sum_{j=1}^{n} u_{ij}q_j| < \sqrt{i+3} \cdot t(n)\delta_0^n 2^{\frac{\gamma-\rho}{n}-(\eta-\rho)}$ where $t(n) = n\left(\frac{\sqrt{n^2+n}}{n-1}\right)^{1-\frac{1}{n}}$. Since $t(n) \sim n$, we get (15). □

Finally, we present the following theorem.

Theorem 5. *Let* $\mathbf{v}_i = (\alpha u_{i1}, \ldots, \alpha u_{i,n-1}, \sum_{j=1}^{n} u_{ij}a_j)$ *be the* i*-th reduced basis vector of* $\mathcal{L}_3(\alpha)$*. Take the optimized* $\alpha = \frac{\sqrt{n^2+n}}{n-1}2^{\rho}$*. From the* GSA*, we find out* $u_{i1}q_1 + \cdots + u_{in}q_n = 0$ *under the condition*

$$\frac{\gamma-\rho}{n} - (\eta-\rho) + n\log\delta_0 + \log\left(n\sqrt{i+3}\right) < 0.$$

C Analysis on $\det U = \pm 1$ and $d = \pm 1$

Here we only analyze the case of lattice $\mathcal{L}_2(\alpha)$, since that of $\hat{\mathcal{L}}_2(\alpha)$ is similar. Let $\mathbf{U} = (u_{ij})_{n\times n}$. We rewrite the system of equation

$$\begin{cases} u_{1,1}q_1 + \cdots + u_{1,n}q_n = 0 \\ \cdots \\ u_{n-1,1}q_1 + \cdots + u_{n-1,n}q_n = 0 \\ u_{n,1}q_1 + \cdots + u_{n,n}q_n = d \end{cases}$$

as

$$\mathbf{U} \cdot (q_1, \ldots, q_n)^T = (0, \ldots, 0, d)^T. \tag{16}$$

Noting that $\mathbf{M}(\alpha)$ is a basis matrix on $\mathcal{L}_2(\alpha)$ and $\mathbf{U} \cdot \mathbf{M}(\alpha)$ is the reduced basis matrix on $\mathcal{L}_2(\alpha)$. Hence, $\mathbf{U}$ is an unimodular matrix, i.e., $\mathbf{U}$ is an integer matrix and $\det \mathbf{U} = \pm 1$.

Further, the inverse matrix $\mathbf{U}^{-1}$ is also an unimodular matrix. Left multiply $\mathbf{U}^{-1}$ to both sides of (16) and get $(q_1, \ldots, q_n)^T = \mathbf{U}^{-1} \cdot (0, \ldots, 0, d)^T$. Let $(w_{1n}, \ldots, w_{nn})^T$ be the n-th column vector of $\mathbf{U}^{-1}$, we can deduce

$$(q_1, \ldots, q_n) = d \cdot (w_{1n}, \ldots, w_{nn}),$$

which implies that d is a common divisor of $q_1, \cdots, q_n$. Since integers $q_1, \cdots, q_n$ are randomly chosen from $[0, 2^{\gamma}/p)$, then $\gcd(q_1, \ldots, q_n) = 1$ holds with the asymptotic probability $1/\zeta(n)$, where $\zeta(n) = \sum_{k=1}^{\infty} 1/k^n$ is the Euler-Riemann zeta function. In other words, it is very likely to be true that $d = \pm 1$.

D Comparison of Known OL Attacks

We first give work conditions that depend on the root-Hermite factor δ_0 for existing OL attacks. Then we present the corresponding comparison.

The First OL Attack. We have the following result and proof.

Theorem 6. *Let $(\alpha \sum_{j=1}^{n} u_{ij} a_j, u_{i1}, \ldots, u_{in})$ be the i-th reduced basis vector of $\mathcal{L}_1(\alpha)$ where α is some sufficiently large integer. Based on the* GSA*, we obtain $\sum_{j=1}^{n} u_{ij} r_j = 0$ for $i = 1, \ldots, n-1$ under the condition*

$$\frac{\gamma}{n-1} - (\eta - \rho) + (n-1)\log \delta_0 + \log \sqrt{n^2 + 2n} < 0. \tag{17}$$

Proof. Let $\mathcal{L}^{\perp}$ be the lattice orthogonal to $(a_1, \ldots, a_n)$. According to [43, Theorem 4], when α is sufficiently large, $(u_{i1}, \ldots, u_{in})$ is the reduced basis vector of $\mathcal{L}^{\perp}$ for $i = 1, \ldots, n-1$. Hence, we have $\sum_{j=1}^{n} u_{ij} a_j = 0$. From $a_j = pq_j + r_j$ for all $1 \le j \le n$, we have $\sum_{j=1}^{n} u_{ij} a_j = p \sum_{j=1}^{n} u_{ij} q_j + \sum_{j=1}^{n} u_{ij} r_j$. Hence, we get $\sum_{j=1}^{n} u_{ij} r_j = 0 \bmod p$. The goal is to generate $\sum_{j=1}^{n} u_{ij} r_j = 0$ for all $1 \le i \le n-1$.

Let $\mathbf{u}_i = (u_{i1}, \ldots, u_{in})$ and $\mathbf{r} = (r_1, \ldots, r_n)$. Clearly, $\|\mathbf{r}\| < \sqrt{n} 2^{\rho}$. According to the Cauchy-Schwartz inequality, we have $|\sum_{j=1}^{n} u_{ij} r_j| \le \|\mathbf{u}_i\| \cdot \|\mathbf{r}\| \le \sqrt{n} 2^{\rho} \|\mathbf{u}_i\|$. Since $\sum_{j=1}^{n} u_{ij} r_j = 0 \bmod p$ and $p \ge 2^{\eta-1}$, we deduce $\sum_{j=1}^{n} u_{ij} r_j = 0$ under the condition $\|\mathbf{u}_i\| < \frac{2^{\eta-\rho-1}}{\sqrt{n}}$.

Note that $\mathbf{u}_i$ is the i-th reduced basis vector of $\mathcal{L}^{\perp}$. Based on $\dim \mathcal{L}^{\perp} = n-1$ and $\det \mathcal{L}^{\perp} \le \sqrt{a_1^2 + \cdots + a_n^2} < \sqrt{n} 2^{\gamma}$, we have $\|\mathbf{u}_i\| \le \frac{\sqrt{i+3}}{2} \cdot \delta_0^{n-1} n^{\frac{1}{2(n-1)}} 2^{\frac{\gamma}{n-1}}$ under the GSA. Hence, in order to get $\sum_{j=1}^{n} u_{ij} r_j = 0$ for all $1 \le i \le n-1$, we expect $\frac{\sqrt{n+2}}{2} \cdot \delta_0^{n-1} n^{\frac{1}{2(n-1)}} 2^{\frac{\gamma}{n-1}} < \frac{2^{\eta-\rho-1}}{\sqrt{n}}$. Rearranging this expression, we get $\frac{\gamma}{n-1} - (\eta - \rho) + (n-1)\log \delta_0 + \log h(n) < 0$, where $h(n) = (n^2 + 2n)^{\frac{1}{2}} n^{\frac{1}{2(n-1)}}$. Since $h(n) \sim (n^2 + 2n)^{\frac{1}{2}}$, we have the simplified condition $\frac{\gamma}{n-1} - (\eta - \rho) + (n-1)\log \delta_0 + \log \sqrt{n^2 + 2n} < 0$.

□

The Second OL Attack. In fact, the involved lattice is $\mathcal{L}_2(2^{\rho})$, which is a particular case of $\mathcal{L}_2(\alpha)$ appeared in Section 3.2. Plugging $\alpha = 2^{\rho}$ into the condition (3) and rearranging it, we get that $n-1$ linear independent vectors orthogonal to $(q_1, \ldots, q_n)$ approximately under the condition (7), i.e.

$$\frac{\gamma - \rho}{n} - (\eta - \rho) + n \log \delta_0 + \log \sqrt{n^2 + 2n} \le 0.$$

It implies that the second OL attack is almost same as the optimized situation. In other words, the second OL attack and the OL attack in Section 3.2 have similar performances.

The Third OL Attack. It is clear that the involved lattice in the third OL attack is $\mathcal{L}_3(1)$, which is a concrete case of $\mathcal{L}_3(\alpha)$ given in Remark 1 and Appendix

B. Plugging $\alpha = 1$ into the condition (14) and re-expressing it, we deduce that $n-1$ linear independent vectors orthogonal to $(q_1, \ldots, q_n)$ approximately under the condition

$$\frac{\gamma}{n} - (\eta - \rho) + n \log \delta_0 + \log \sqrt{n^3 + 3n^2 + 2n} \leq 0. \tag{18}$$

Comparison. Similar to the analysis of Theorem 3 in Section 4.1, from (17), (7) and (18), we respectively get the time complexities to solve (γ, η, ρ)-ACD instances by running BKZ-β if one SVP oracle costs $2^{\mathcal{O}(\beta)}$:

$$\begin{cases} 2^{\Omega\left(\frac{\gamma}{(\eta-\rho)^2} \log \frac{\gamma}{(\eta-\rho)^2}\right)} & \text{The First OL Attack} \\ 2^{\Omega\left(\frac{\gamma-\rho}{(\eta-\rho)^2} \log \frac{\gamma-\rho}{(\eta-\rho)^2}\right)} & \text{The Second OL Attack} \\ 2^{\Omega\left(\frac{\gamma}{(\eta-\rho)^2} \log \frac{\gamma}{(\eta-\rho)^2}\right)} & \text{The Third OL Attack} \end{cases} \tag{19}$$

Hence, the first and third OL attacks have the same asymptotic complexity; the second OL attack and OL attacks in Section 3 have the same asymptotic complexity. When $\gamma \gg \rho$, the asymptotic complexities of all these OL attacks are the same. When $(\gamma - \rho)$ is relatively small, the second OL attack and OL attacks in Section 3 are more advantageous than the first and third ones.