PAPER Special Section on Cryptography and Information Security

Faster Rotation-Based Gauss Sieve for Solving the SVP on General Ideal Lattices

Shintaro NARISADA[†a)], **Hiroki OKADA**[†], **Kazuhide FUKUSHIMA**[†], ***and*** **Shinsaku KIYOMOTO**[†], ***Members***

SUMMARY The hardness in solving the shortest vector problem (SVP) is a fundamental assumption for the security of lattice-based cryptographic algorithms. In 2010, Micciancio and Voulgaris proposed an algorithm named the Gauss Sieve, which is a fast and heuristic algorithm for solving the SVP. Schneider presented another algorithm named the Ideal Gauss Sieve in 2011, which is applicable to a special class of lattices, called ideal lattices. The Ideal Gauss Sieve speeds up the Gauss Sieve by using some properties of the ideal lattices. However, the algorithm is applicable only if the dimension of the ideal lattice n is a power of two or $n+1$ is a prime. Ishiguro et al. proposed an extension to the Ideal Gauss Sieve algorithm in 2014, which is applicable only if the prime factor of n is 2 or 3. In this paper, we first generalize the dimensions that can be applied to the ideal lattice properties to when the prime factor of n is derived from 2, p or q for two primes p and q. To the best of our knowledge, no algorithm using ideal lattice properties has been proposed so far with dimensions such as: 20, 44, 80, 84, and 92. Then we present an algorithm that speeds up the Gauss Sieve for these dimensions. Our experiments show that our proposed algorithm is 10 times faster than the original Gauss Sieve in solving an 80-dimensional SVP problem. Moreover, we propose a rotation-based Gauss Sieve that is approximately 1.5 times faster than the Ideal Gauss Sieve.

key words: *shortest vector problem, Gauss Sieve, ideal lattice, generalization*

1. Introduction

Lattice-based cryptography has attracted interest as a fundamental theory for designing candidates for quantum-resistant cryptographic algorithms. The security of lattice-based cryptographic algorithms is based on the hardness in solving the shortest vector problem (SVP). In 1998, Ajtai [1] proved that the SVP is a class of NP-hard problems. He introduced the concept of the lattice-based cryptography as well. A deterministic algorithm for solving the SVP called Enumeration was proposed [2] in 1981, and Ajtai et al. presented a probabilistic algorithm called Sieving [3] in 2001, respectively. Enumeration and Sieving are the two major algorithms for solving the SVP. Various sieving algorithms have been proposed and they have become the mainstream of algorithms for solving the SVP. In 2010, Micciancio and Voulgaris [4] proposed the Gauss Sieve (GS), which heuristically solves the SVP by recursively collecting shorter vectors. The GS was experimentally faster than the ordinary sieving algorithms and it was the first sieving algorithm to be competitive with the enumeration algorithm with regard to its computational cost. Ducas [5] proposed the SubSieve algorithm in 2018, which can reduce a few lattice dimensions by applying a technique of lattice orthogonalization. Albrecht et al. [6] proposed a new sieving implementation called *g6k*. It contains the existing sieving algorithms, and it includes some heuristic techniques for speeding-up the sieving procedure, such as optimization of the lattice basis updating process. g6k can solve the SVP with higher dimensions.

A special lattice named the Ideal Lattice contributes to reduce the computation time of cryptosystems [7], [8]. Schneider [9] presented that some types of ideal lattices are useful for reducing the computational time of the GS. He characterized these ideal lattices as the *Anti-cyclic lattice* and the *Prime cyclotomic lattice*. Then, he proposed the Ideal Gauss Sieve (IGS) by utilizing the properties of their rotation structures. The IGS is faster than the GS if the lattice dimension n is 2^a or $p-1$ for an odd prime p. Similar IGS techniques [10] enable speeding up the LLL algorithm [11], which is a lattice basis reduction algorithm. In [12], Ishiguro et al. considered a special case of ideal lattices called a *trinomial lattice*. They claimed that the rotation property of the trinomial lattice could speed up the GS only if n is 2^a3^b, in addition to the Schneider's result of 2^a or $p-1$. However, no algorithm that utilizes the ideal lattice structure has been proposed in order to reduce the computational time needed to solve the SVP with other dimensions.

1.1 Contributions

We propose a new ideal lattice structure named the *t-nomial lattice* as a generalized version of the anti-cyclic lattice, the prime cyclotomic lattice, and the trinomial lattice. Then we show that the IGS can reduce the computational time by utilizing the t-nomial lattice for dimensions $n = 2^a p^b (p-1) q^c (q-1)$ $(a, b, c \geq 0$, and p and q are odd primes s.t. $p < q)$. The equation obviously fits the previous results with dimensions $n = 2^a$, $p-1$ and 2^a3^b. Moreover, we propose an algorithm named the *rotation-based Gauss Sieve* (RGS) algorithm that leverages the rotation structure of ideal lattices to reduce the internal cost of the GS. Our experiments confirm that our proposed algorithm is 1.5 times faster than the IGS.

2. Definition

An m-dimensional vector is denoted by $\mathbf{v} = (v_0, \ldots, v_{m-1})$. For $0 \leq i \leq m-1$, the i-th element of $\mathbf{v}$ is written as $\mathbf{v}[i]$. The

Manuscript received March 16, 2020.
Manuscript revised July 1, 2020.

[†]The authors are with KDDI Research, Inc., Fujimino-shi, 356-8502 Japan.
a) E-mail: sh-narisada@kddi-research.jp

DOI: 10.1587/transfun.2020CIP0014

Euclidean norm of a vector $\mathbf{v}$ is denoted by $\|\mathbf{v}\| = \sqrt{\sum_{i=0}^{m-1} v_i^2}$. The inner product of two vectors $\mathbf{u} = (u_0, \ldots, u_{m-1})$ and $\mathbf{v} = (v_0, \ldots, v_{m-1})$ is $\langle \mathbf{u}, \mathbf{v} \rangle = \sum_{i=0}^{m-1} u_i v_i$. A matrix $\mathbf{B}$ consisting of n linearly independent m-dimensional vectors is denoted by $\mathbf{B} = (\mathbf{b}_0, \ldots, \mathbf{b}_{n-1}) \in \mathbb{R}^{m \times n}$. The *lattice* generated by a basis $\mathbf{B}$ is the set of the all linear combinations of the basis vector $\mathbf{b}_0, \ldots, \mathbf{b}_{n-1}$

$$\mathcal{L}(\mathbf{B}) = \mathcal{L}(\mathbf{b}_0, \ldots, \mathbf{b}_{n-1}) = \left\{ \sum_{i=0}^{n-1} x_i \mathbf{b}_i \middle| x_i \in \mathbb{Z} \right\}.$$

We call $\mathbf{B}$ the basis of the lattice $\mathcal{L}$. In the following, let $n = m$ and $\mathbf{b}_i \in \mathbb{Z}^n$. The determinant of a lattice generated by $\mathbf{B}$ is $\det(\mathcal{L}(\mathbf{B})) = \sqrt{\det(\mathbf{B}^T \mathbf{B})}$. We say that n is the dimension of the lattice. $\lambda_1(\mathcal{L})$ is the Euclidean norm of the shortest nonzero vector in $\mathcal{L}$. We define the SVP as follows.

Definition 1 (SVP)**.** For a lattice $\mathcal{L}(\mathbf{B})$, compute a vector $\mathbf{v} \in \mathcal{L}(\mathbf{B})$ *s.t.* $\|\mathbf{v}\| = \lambda_1(\mathcal{L}(\mathbf{B}))$.

We can estimate the length of the shortest vector in the n-dimensional lattice $\mathcal{L}(\mathbf{B})$ by the Gaussian heuristic, where $\Gamma(x)$ is a gamma function.

$$\lambda_1(\mathcal{L}(\mathbf{B})) = \frac{1}{\sqrt{\pi}} \Gamma\left(\frac{n}{2} + 1\right)^{\frac{1}{n}} \det(\mathcal{L}(\mathbf{B}))^{\frac{1}{n}}$$

An ideal I is the subgroup of the additive group of the ring $\mathbf{R} = \mathbb{Z}[x]/(g(x))$, where $g(x)$ is a monic polynomial over $\mathbb{Z}$. We make a polynomial $\mathbf{v}(x) = \sum_{i=0}^{n-1} v_i x^i \in I$ and its coefficient vector $\mathbf{v} = (v_0, \ldots, v_{n-1}) \in \mathbb{Z}$ correspond. Then, the set $\{\mathbf{v} | \mathbf{v}(x) = \sum_{i=0}^{n-1} v_i x^i \in I\}$ is a lattice. These lattices satisfy the above conditions and are called *ideal lattices*. Let the polynomial expression of a lattice vector $\mathbf{v} \in \mathcal{L}$ be $\mathbf{v}(x)$, then we write a *rotation* of the vector $\mathbf{v}(x)$ as $\mathbf{rot}(\mathbf{v}) = x\mathbf{v}(x) \bmod g(x)$. The ideal lattice is closed under the rotation operations. Namely, $\mathbf{v} \in \mathcal{L} \Rightarrow \mathbf{rot}(\mathbf{v}) \in \mathcal{L}$. We write i rotations as $\mathbf{rot}^i(\mathbf{v}) = \mathbf{rot}(\mathbf{rot}^{i-1}(\mathbf{v}))$ and $\mathbf{rot}^0(\mathbf{v}) = \mathbf{v}$.

As monic polynomials, we use the cyclotomic polynomials that are used in the Ring-Learning with Errors (R-LWE) problem [13]. The m-th cyclotomic polynomial is defined as follows, where $\gcd(i, j)$ represents the greatest common divisor of two natural numbers i, j

$$\Phi_m(x) = \prod_{1 \le k \le m, \gcd(k,m)=1} \left(x - e^{2\pi i k/m}\right).$$

For instance, $\Phi_8(x) = x^4 + 1$ and $\Phi_{12}(x) = x^4 - x^2 + 1$. The degree of $\Phi_m(x)$ is $\varphi(m)$ [14], where $\varphi(m)$ is Euler's totient function.

3. Preliminaries

We describe the outline of the GS [4] and then give an overview of the IGS [9] and Ishiguro's extension [12]. We mention the following two definitions related to lattice vectors before considering the GS.

Definition 2 (Gauss-reduced)**.** Two vectors $\mathbf{u}, \mathbf{v} \in \mathcal{L}(\mathbf{B})$ are *Gauss-reduced*, where $\mathbf{u}, \mathbf{v}$ holds $\|\mathbf{u} \pm \mathbf{v}\| \ge \max(\|\mathbf{u}\|, \|\mathbf{v}\|)$.

Algorithm 1: Reduction [4]

Input: $\mathbf{u}, \mathbf{v} \in \mathcal{L}(\mathbf{B})$
Output: $\mathbf{u} \in \mathcal{L}(\mathbf{B})$
1 **if** $|2\langle \mathbf{u}, \mathbf{v} \rangle| > \|\mathbf{v}\|^2$ **then** $\mathbf{u} \leftarrow \mathbf{u} - \left\lfloor \frac{\langle \mathbf{u}, \mathbf{v} \rangle}{\|\mathbf{v}\|^2} \right\rceil \mathbf{v}$
2 **return** $\mathbf{u}$

The procedure in Algorithm 1 outputs the Gauss-reduced vectors of $\mathbf{u}$ and $\mathbf{v}$; $\mathbf{u}$ or $\mathbf{v}$ is recursively replaced by the subtraction of $\mathbf{u}$ and $\mathbf{v}$, where the vector yielded by the subtraction has a shorter norm than $\mathbf{u}$ or $\mathbf{v}$ does. This replacement is called *reduce*. Algorithm 1 details the *reduce* process. In a *collision* case in which two vectors are linearly dependent, the algorithm always outputs a zero vector.

Pairwise-reduced is a generalization of "Gauss-reduced", which is extended to a set of vectors.

Definition 3 (Pairwise-reduced)**.** For a set $A \subset \mathcal{L}(\mathbf{B})$, A is *Pairwise-reduced*, where all combinations of the vectors $\forall \mathbf{u}, \mathbf{v} \in A, \mathbf{u} \ne \mathbf{v}$ are Gauss-reduced.

3.1 Gauss Sieve

Micciancio and Voulgaris proposed two sieving algorithms named the List Sieve and GS [4]. The GS is a practical variant of the List Sieve that probabilistically solves the SVP. Algorithm 2 is related to the GS. The GS [4] extends a pairwise-reduced set of lattice vectors L until a certain number of collisions occurs. When L contains a sufficient number of lattice vectors, the shortest vector of the lattice is included in the set L with a certain probability. A new lattice vector $\mathbf{v}$ is generated by a random sampling via a sampler such as Klein's algorithm [15]. Klein's sampler generates a vector by computing within $O(n^2)$. For a fresh vector $\mathbf{v}$, the GS decreases the norm of $\mathbf{v}$ by performing the reduce function; so that $\mathbf{v}$ and all its elements of L become Gauss-reduced, and $L \cup \{\mathbf{v}\}$ is Pairwise-reduced. The GS continues the above procedures until the number of collisions c reaches $c_{\max}$. Finally, the GS outputs the shortest vector in L as a candidate of the shortest vector of the lattice $\mathcal{L}(\mathbf{B})$.

3.2 Ideal Gauss Sieve

The IGS [9] is a variant of the GS that utilizes a rotation structure of specific ideal lattices called *Anti-cyclic lattice* and *Prime cyclotomic lattice*. The anti-cyclic lattice is a lattice generated by a binomial cyclotomic polynomial $\Phi_m(x) = x^n + 1$.

Definition 4 (Anti-cyclic lattice)**.** The n-dimensional ideal lattice of the ring $\mathbf{R} = \mathbb{Z}[x]/\Phi_m(x)$ is said to be an anti-cyclic lattice, where $\Phi_m(x) = x^n + 1$ $(n = 2^{a-1}, m = 2^a, a > 0)$.

The prime cyclotomic lattice is the lattice generated by an $(n + 1)$-term cyclotomic polynomial.

Algorithm 2: Gauss Sieve [4]

Input: A basis $\mathbf{B}$ of the lattice $\mathcal{L}(\mathbf{B})$, maximal number of collisions $c_{\max}$
Output: A candidate of the shortest vector in $\mathcal{L}(\mathbf{B})$

$L \leftarrow \{\}, S \leftarrow \{\}, c \leftarrow 0$
while $c < c_{\max}$ **do**
  if $|S| = 0$ **then** $\mathbf{v} \leftarrow$ sample from $\mathcal{L}(\mathbf{B})$
  else $\mathbf{v} \leftarrow S$.pop()
  $\mathbf{v}' \leftarrow \mathbf{v}$
  for $\boldsymbol{\ell} \in L$ **do**
    $\mathbf{v} \leftarrow \text{Reduction}(\mathbf{v}, \boldsymbol{\ell})$
  if $\|\mathbf{v}\| = 0$ **then** $c \leftarrow c + 1$
  else if $\mathbf{v}' \neq \mathbf{v}$ **then** S.push($\mathbf{v}$)
  else
    for $\boldsymbol{\ell} \in L$ **do**
      $\boldsymbol{\ell}' \leftarrow \text{Reduction}(\boldsymbol{\ell}, \mathbf{v})$
      if $\boldsymbol{\ell}' \neq \boldsymbol{\ell}$ **then**
        $L \leftarrow L \setminus \{\boldsymbol{\ell}\}$
        S.push($\boldsymbol{\ell}'$)
    $L \leftarrow L \cup \{\mathbf{v}\}$
return the shortest vector in L (a candidate of the shortest vector in $\mathcal{L}(\mathbf{B})$)

Definition 5 (Prime cyclotomic lattice)**.** The n dimensional ideal lattice of the ring $\mathbf{R} = \mathbb{Z}[x]/\Phi_m(x)$ is said to be the prime cyclotomic lattice, where $\Phi_m(x) = x^n + x^{n-1} + \cdots + 1$ ($n = p - 1, m = p, p$ is a prime).

For an n-dimensional vector $\mathbf{v}$ and $0 \leq i \leq n-1$, the rotation of the anti-cyclic lattice $\mathbf{rot}(\mathbf{v})$ is

$$\mathbf{rot}(\mathbf{v})[i] = \begin{cases} -\mathbf{v}[n-1] & (i = 0) \\ \mathbf{v}[i-1] & (\text{otherwise}). \end{cases}$$

The time complexity of $\mathbf{rot}(\mathbf{v})$ for an anti-cyclic lattice is $O(1)$ when using a bidirectional list. $\mathbf{v}$ has the same Euclidean norm as $\mathbf{rot}(\mathbf{v})$. The rotation of the prime cyclotomic lattice is

$$\mathbf{rot}(\mathbf{v})[i] = \begin{cases} -\mathbf{v}[n-1] & (i = 0) \\ \mathbf{v}[i-1] - \mathbf{v}[n-1] & (\text{otherwise}). \end{cases}$$

The computational complexity of $\mathbf{rot}(\mathbf{v})$ for the prime cyclotomic lattice is $O(n)$. In general, the norm of $\mathbf{rot}(\mathbf{v})$ is different from the norm of $\mathbf{v}$, and it is not larger than $2\|\mathbf{v}\|$. Schneider applied these rotation formulae to implement the Reduction function, *i.e.*, if input of GS is an ideal lattice, Reduction in Algorithm 2 can be replaced by ReduceRot function in Algorithm 3. The ReduceRot function increases the probability of reducing the norm of $\mathbf{u}$ since $\mathbf{rot}^i(\mathbf{v})$ for all $i > 0$ is used to reduce $\mathbf{u}$ in addition to $\mathbf{v}$. The probability $\Pr[\|\mathbf{u}'\| < \|\mathbf{u}\| \mid \mathbf{u}' = \text{Reduction}(\mathbf{u}, \mathbf{rot}^i(\mathbf{v}))]$ for any i is identical to $\Pr[\|\mathbf{u}'\| < \|\mathbf{u}\| \mid \mathbf{u}' = \text{Reduction}(\mathbf{u}, \mathbf{v})]$ if input basis is the prime cyclotomic lattice and $\mathbf{rot}^i(\mathbf{v})$ is linearly independent of $\mathbf{v}$, since $\mathbf{rot}^i(\mathbf{v})$ for any i satisfies that $\|\mathbf{rot}^i(\mathbf{v})\| = \|\mathbf{v}\|$. Note that there exist two vectors $\mathbf{u}$ and $\mathbf{v}$ such that $\text{Reduction}(\mathbf{u}, \mathbf{rot}^i(\mathbf{v}))$ fails for all i. Schneider presented that both of the lattices speed up the GS in practice when dimension $n = 2^a$ and $n = p - 1$, where $a \geq 0$ and p is a prime.

Algorithm 3: ReduceRot [9]

Input: $\mathbf{u}, \mathbf{v} \in \mathcal{L}(\mathbf{B})$
Output: $\mathbf{u} \in \mathcal{L}(\mathbf{B})$

$\mathbf{v}' \leftarrow \mathbf{v}$
for $i \leftarrow 0, 1, \cdots, n-1$ **do**
  if $|2\langle \mathbf{u}, \mathbf{v}' \rangle| > \|\mathbf{v}'\|^2$ **then** $\mathbf{u} \leftarrow \mathbf{u} - \left\lfloor \frac{\langle \mathbf{u}, \mathbf{v}' \rangle}{\|\mathbf{v}'\|^2} \right\rceil \mathbf{v}'$
  $\mathbf{v}' \leftarrow \mathbf{rot}(\mathbf{v}')$
return $\mathbf{u}$

3.3 Ishiguro's Extension

Ishiguro et al. [12] extended the dimensions in the IGS by analyzing the property of the trinomial lattice, and proposed a method for improving the performance of the algorithm.

Definition 6 (Trinomial lattice)**.** The n-dimensional ideal lattice of the ring $\mathbf{R} = \mathbb{Z}[x]/\Phi_m(x)$ is said to be a trinomial lattice, where

$$\Phi_m(x) = \begin{cases} x^n + x^{n/2} + 1 \ (n = 2 \cdot 3^{a-1}, m = 3^a) & (1) \\ x^n - x^{n/2} + 1 \ (n = 2^a 3^{b-1}, m = 2^a 3^b) & (2) \end{cases}$$

where, $a > 0$ and $b > 0$.

They revealed that for an n-dimensional lattice $\mathbf{v}$, the rotation of the trinomial lattice is

$$\mathbf{rot}(\mathbf{v})[i] = \begin{cases} -\mathbf{v}[n-1] & (i = 0) \\ \mathbf{v}[i-1] \mp \mathbf{v}[n-1] & (i = \frac{n}{2}) \\ \mathbf{v}[i-1] & (\text{otherwise}) \end{cases}$$

where, $0 \leq i \leq n-1$. The $\mp$ operator is $-$ in the case of Eq. (1) and $+$ for Eq. (2). The computational complexity of $\mathbf{rot}(\mathbf{v})$ for the trinomial lattice is almost identical to that of the anti-cyclic lattice since the positions of $\mathbf{v}$ that need to be updated by the rotation are only $\mathbf{v}[0]$,$\mathbf{v}[\frac{n}{2} - 1]$, and $\mathbf{v}[n-1]$. However, the norm of $\mathbf{rot}(\mathbf{v})$ for the trinomial lattice is larger than that of $\mathbf{v}$ with a probability of 5/8. We consider the the difference of norm $\|\mathbf{rot}(\mathbf{v})\|^2 - \|\mathbf{v}\|^2 = \mathbf{v}[n-1]^2 + 2\mathbf{v}[\frac{n}{2} - 1]\mathbf{v}[n-1]$ (when Eq. (2)), then necessary and sufficient condition for $\Pr[\|\mathbf{rot}(\mathbf{v})\|^2 - \|\mathbf{v}\|^2 \leq 0]$ are; (i) $\mathbf{v}[\frac{n}{2} - 1]$ and $\mathbf{v}[n-1]$ have opposite signs and (ii) $|\mathbf{v}[n-1]| \leq 2|\mathbf{v}[\frac{n}{2} - 1]|$. Then we achieve $\Pr[\|\mathbf{rot}(\mathbf{v})\|^2 - \|\mathbf{v}\|^2 \leq 0] = 3/8$ since the probability of (i) is 1/2 and (ii) is 3/4 respectively. The case of Eq. (1) is the same. (see the detail in the experimental result and norm analysis in Sect. 5.) Hence, rotating $\mathbf{v}$ $n-1$ times as for the anti-cyclic lattice and prime cyclotomic lattice is not effective. Ishiguro et al. claimed that the optimal number of rotations is 12 for a trinomial lattice through experiments as well as consideration of the inverse rotation of trinomial lattices. The inverse element of x mod $\Phi_m(x)$ for the trinomial lattice is $x^{-1} = -x^{n-1} - x^{\frac{n}{2}}$ for Eq. (1) and $x^{-1} = -x^{n-1} + x^{\frac{n}{2}}$ for Eq. (2). Therefore, they presented the inverse rotation of the trinomial lattice $\mathbf{rot}^{-1}(\mathbf{v})$ as follows;

$$\mathbf{rot}^{-1}(\mathbf{v})[i] = \begin{cases} -\mathbf{v}[0] & (i = n-1) \\ \mathbf{v}[i+1] \mp \mathbf{v}[0] & (i = \frac{n}{2} - 1) \\ \mathbf{v}[i+1] & (\text{otherwise}), \end{cases}$$

Algorithm 4: ReduceInverseRot [12]

Input: $\mathbf{u}, \mathbf{v} \in \mathcal{L}(\mathbf{B})$
Output: $\mathbf{u} \in \mathcal{L}(\mathbf{B})$

$\mathbf{v}' \leftarrow \mathbf{v}$
$\mathbf{v}'' \leftarrow \mathbf{v}$
for $i \leftarrow 0, 1, \cdots, k$ **do**
  if $|2\langle \mathbf{u}, \mathbf{v}' \rangle| > \|\mathbf{v}'\|^2$ **then** $\mathbf{u} \leftarrow \mathbf{u} - \left\lfloor \frac{\langle \mathbf{u}, \mathbf{v}' \rangle}{\|\mathbf{v}'\|^2} \right\rceil \mathbf{v}'$ $\mathbf{v}' \leftarrow \mathbf{rot}(\mathbf{v}')$
for $i \leftarrow 0, 1, \cdots, k$ **do**
  if $|2\langle \mathbf{u}, \mathbf{v}'' \rangle| > \|\mathbf{v}''\|^2$ **then** $\mathbf{u} \leftarrow \mathbf{u} - \left\lfloor \frac{\langle \mathbf{u}, \mathbf{v}'' \rangle}{\|\mathbf{v}''\|^2} \right\rceil \mathbf{v}''$
  $\mathbf{v}'' \leftarrow \mathbf{rot}^{-1}(\mathbf{v}'')$
return $\mathbf{u}$

where, $0 \le i \le n-1$ and the operator $\mp$ is denoted in the same manner as for the rotation. They improved the success probability of reduction in the ReduceRot function by utilizing the inverse rotation in addition to the rotation. The improved ReduceRot function is shown in Algorithm 4. In practice, they achieved a 25-fold increase in speed of the GS when $n = 96$.

4. Proposed Algorithm

In Sect. 4.1, we first introduce a t-nomial lattice that generalizes the concepts of anti-cyclic lattice, prime cyclotomic lattice and trinomial lattice, where t is the number of terms in the cyclotomic polynomials. Then, we present the rotation and the inverse rotation of the t-nomial lattice. Rotation-based Gauss Sieve is presented in Sect. 4.2.

4.1 t-Nomial Lattice

Let m be the index of the cyclotomic polynomial $\Phi_m(x)$. We define the t-nomial lattice as follows;

Definition 7 (t-nomial lattice)**.** The n-dimensional ideal lattice of the ring $\mathbf{R} = \mathbb{Z}[x]/\Phi_m(x)$ is said to be a t-nomial lattice, where the cyclotomic polynomial $\Phi_m(x)$ has t terms.

We consider a relationship between the number of terms t and m. An index m is divided into four cases by the number of types of odd primes contained in the integer factorization of m. If the integer factorization of m contains no odd primes, then the next condition holds.

Lemma 1 ([9])**.** If $m = 2^a (a \ge 1)$, then $t = 2$.

If Lemma 1 holds, the t-nomial lattice is an anti-cyclic lattice. If the integer factorization of m contains one type of odd prime p, then cyclotomic polynomial $\Phi_m(x)$ is represented as follows.

Lemma 2 ([14], [16])**.** For an odd prime p, if $m = 2^a p^b (a \ge 0, b \ge 1)$, then $\Phi_m(x) = \sum_{i=0}^{p-1} (-1)^i x^{i 2^{a-1} p^{b-1}}$.

When $m = 2^a p^b (a \ge 0, b \ge 1)$, the number of terms t is computed from Lemma 2.

Corollary 1. For an odd prime p, if $m = 2^a p^b (a \ge 0, b \ge 1)$, then $t = p$.

Proof. From Lemma 2, $\Phi_m(x)$ is extended to $\Phi_{2^a p^b}(x) = 1 - x^{2^{a-1} p^{b-1}} + x^{2 \cdot 2^{a-1} p^{b-1}} - \cdots + x^{2^{a-1} p^{b-1}(p-1)}$. Obviously, this formula consists of p terms. □

The trinomial lattice is the case of Corollary 1. To consider the case where the integer factorization of m contains two types of odd primes, we give the following lemma;

Lemma 3. For two odd primes $p, q (p < q)$, the number of terms of $\Phi_{2^a p^b q^c}(x)$ equals to $\Phi_{pq}(x)$.

Proof. For relatively prime numbers s, t and an integer m, $\Phi_{s^m t}(x) = \Phi_{st}(x^{s^{m-1}})$ [16]. Therefore, since 2 and $p^b q^c$ are relatively prime, $\Phi_{2^a p^b q^c}(x) = \Phi_{2 p^b q^c}(x^{2^{a-1}})$. Let $y = x^{2^{a-1}}$. Then the number of terms of $\Phi_{2^a p^b q^c}(x)$ equals to $\Phi_{2 p^b q^c}(y)$. For an odd number $n > 1$, $\Phi_{2n}(x) = \Phi_n(-x)$ [14]. Since $p^b q^c$ is an odd, $\Phi_{2 p^b q^c}(y) = \Phi_{p^b q^c}(-y)$. Let $z = -y$. The number of terms of $\Phi_{2 p^b q^c}(y)$ equals to $\Phi_{p^b q^c}(z)$. Similarly, it is confirmed that the number of terms $\Phi_{2^a p^b q^c}(x)$ equals to $\Phi_{pq}(x)$. □

Carlitz [17] found that the number of terms of $\Phi_{pq}(x)$. Hence, it allows us to compute the number of terms of $\Phi_{2^a p^b q^c}(x)$ by combining [17] with Lemma 3 as follows.

Corollary 2. For an odd prime p, choose an odd prime $q > p$ where $q \equiv 1, 2, p-1, p-2 \mod p$. For $m = 2^a p^b q^c (a \ge 0, b \ge 1, c \ge 1)$ and $k = \lfloor q/p \rfloor$, the number of terms $t = 2k(p-1)+1, k(p^2-1)/2+p, 2k(p-1)+2p-3, (k+1)(p^2-1)/2-p$ for $q \equiv 1, 2, p-1, p-2 \mod p$ respectively.

For m except for the case of Corollary 1 and Corollary 2, a relationship between t and m is still unknown. In this situation, t is calculated by deriving the Φ_m.

As the next step, we consider a relationship between n and m where m is the case of Corollary 1 or Corollary 2. Then, the rotation and the inverse rotation for m are presented. We omit the case of $m = 2^a$ because it is the case of the anti-cyclic lattice itself. For a t-nomial lattice where $m = 2^a p^b$, the dimension n is computed as follows.

Lemma 4. If $m = 2^a p^b$ $(a \ge 0, b \ge 1)$, then n is,

$$n = \begin{cases} p^{b-1}(p-1) & (a = 0) \\ 2^{a-1} p^{b-1}(p-1) & (a \ge 1). \end{cases}$$

Proof. For relatively prime numbers x and y, $\varphi(xy) = \varphi(x)\varphi(y)$. For a prime p and a natural number k, $\varphi(p^k) = p^{k-1}(p-1)$. Hence, for a natural number $a \ge 1$ and $b \ge 1$, $\varphi(2^a p^b) = \varphi(2^a)\varphi(p^b) = 2^{a-1} p^{b-1}(p-1)$. Likewise, for $a = 0$, $\varphi(p^b) = p^{b-1}(p-1)$ since $m = p^b$. □

We present the rotation and the inverse rotation when $m = 2^a p^b$ from Corollary 1 and Lemma 4.

Lemma 5. For $m = 2^a p^b$, $0 \le i \le n-1$ and $1 \le \ell \le t-2$, the rotation of $\mathbf{v}$ is,

$$\mathbf{rot}(\mathbf{v})[i] = \begin{cases} -\mathbf{v}[n-1] & (i=0) \\ \mathbf{v}[i-1] \mp \mathbf{v}[n-1] & (i=\frac{\ell n}{t-1}, \ell \text{ is odd}) \\ \mathbf{v}[i-1] - \mathbf{v}[n-1] & (i=\frac{\ell n}{t-1}, \ell \text{ is even}) \\ \mathbf{v}[i-1] & (\text{otherwise}) \end{cases}$$

The operator $\mp$ is $-$ when $a = 0$; otherwise it is $+$ ($a \neq 0$). The inverse rotation $\mathbf{rot}^{-1}(\mathbf{v})$ is,

$$\mathbf{rot}^{-1}(\mathbf{v})[i] = \begin{cases} -\mathbf{v}[0] & (i=n-1) \\ \mathbf{v}[i+1] \mp \mathbf{v}[0] & (i=\frac{\ell n}{t-1}-1, \ell \text{ is odd}) \\ \mathbf{v}[i+1] - \mathbf{v}[0] & (i=\frac{\ell n}{t-1}-1, \ell \text{ is even}) \\ \mathbf{v}[i+1] & (\text{otherwise}). \end{cases}$$

The operator $\mp$ denotes the same operation as for the rotation.

Proof. We have $\Phi_{p^b}(x) = \sum_{i=0}^{p-1} x^{ip^{b-1}}$ and $\Phi_{2^a p^b}(x) = \sum_{i=0}^{p-1}(-1)^i x^{i2^{a-1}p^{b-1}}$ [14], [16]. The polynomial expression of the rotation is given by substituting the above equation in the $x\mathbf{v}(x) \bmod \Phi_m(x)$. As for the inverse rotation, we compute the inverse element x^{-1} modulo $\Phi_m(x)$. For $a = 0$, the inverse element is $x^{-1} = -\sum_{i=1}^{p-1} x^{ip^{b-1}-1}$, and for $a \neq 0$, $x^{-1} = \sum_{i=1}^{p-1}(-1)^i x^{i2^{a-1}p^{b-1}-1}$. The polynomial expression of the inverse rotation is given by substituting x^{-1} in $x^{-1}\mathbf{v}(x) \bmod \Phi_m(x)$ and by calculating the equation[†]. □

From Lemma 2, it is confirmed that the rotation/inverse rotation of the trinomial lattice is the case of a t-nomial lattice where $t = 3$.

For $m = 2^a p^b q^c$, n is obtained in the same way as in Lemma 4.

Lemma 6. If $m = 2^a p^b q^c (a \geq 0, b \geq 1, c \geq 1)$, n is,

$$n = \begin{cases} p^{b-1}(p-1)q^{c-1}(q-1) & (a=0) \\ 2^{a-1}p^{b-1}(p-1)q^{c-1}(q-1) & (a \geq 1) \end{cases}$$

When $m = 2^a p^b q^c$, the coefficients of $\Phi_m(x)$ are any of $-1, 0, 1$ [18]. The coefficients of the n-th degree and 0-th degree of $\Phi_m(x)$ are always 1. The coefficient vector $\mathbf{c}$ is defined as $\mathbf{c} = (c_1, \ldots, c_{n-1}), c_i \in \{-1, 0, 1\}, \sum_{i=1}^{n-1} |c_i| = t-2$. By using $\mathbf{c}$, the cyclic polynomial for $m = 2^a p^b q^r$ is written as $\Phi_m(x) = 1 + c_1 x + \cdots + c_{n-1}x^{n-1} + x^n$. The rotation/inverse rotation is presented as follows.

Lemma 7. For the coefficient vector $\mathbf{c}$, the rotation of the vector $\mathbf{v}$ for m that satisfies $\Phi_m(x) = 1 + c_1 x + \cdots + c_{n-1}x^{n-1} + x^n$ (including the condition of both Corollary 1 and Corollary 2) is,

$$\mathbf{rot}(\mathbf{v})[i] = \begin{cases} -\mathbf{v}[n-1] & (i=0) \\ \mathbf{v}[i-1] - c_i\mathbf{v}[n-1] & (\text{otherwise}). \end{cases}$$

The inverse rotation $\mathbf{rot}^{-1}(\mathbf{v})$ is,

$$\mathbf{rot}^{-1}(\mathbf{v})[i] = \begin{cases} -\mathbf{v}[0] & (i=n-1) \\ \mathbf{v}[i+1] - c_i\mathbf{v}[0] & (\text{otherwise}). \end{cases}$$

[†]We used `Sympy` to calculate the equation, which is a mathematical library of Python.

The rotation and inverse rotation formulae in Lemma 7 is the generalization of the formulae in Lemma 5. The actual value of $\mathbf{c}$ needs to be computed by deriving the cyclotomic polynomial $\Phi_m(x)$ for $m = 2^a p^b q^r$. From the above calculation, the rotation and the inverse rotation for the t-nomial lattice are computed.

We analyze the computational complexity of the rotation/inverse rotation of the t-nomial lattice.

Theorem 1. The computational complexity of the rotation/inverse rotation of the t-nomial lattice is $O(t)$.

Proof. From the Lemma 5 and Lemma 7, there are a total of t positions of the vectors need to be updated. For the beginning and end of the vector, delete and insert operations are performed in $O(1)$ respectively, using a bidirectional list. For each $t-2$ position, except for the positions mentioned above, the subtraction operation in the equation of the rotation is performed. In total, the rotation is performed in $O(t)$. The same applies to the inverse rotation. □

We explain concrete examples of t-nomial lattices for $t = 5$ and 7. When $m = 2^a 5^b$, the ideal lattice is a 5-nomial lattice. At this time, the rotation is $\mathbf{rot}(\mathbf{v}) = (-v_{n-1}, v_0, v_1, \cdots, v_{\frac{n}{4}-1} \mp v_{n-1}, \cdots, v_{\frac{n}{2}-1} - v_{n-1}, \cdots, v_{\frac{3n}{4}-1} \mp v_{n-1}, \cdots, v_{n-2})$. When $m = 2^a 7^b$ or $m = 2^a 3^b 5^c$, the ideal lattice is a 7-nomial lattice. For $m = 2^a 3^b 5^c$, the cyclotomic polynomial is $\Phi_{2^a 3^b 5^c}(x) = x^n \mp x^{\frac{7n}{8}} \pm x^{\frac{5n}{8}} - x^{\frac{n}{2}} \pm x^{\frac{3n}{8}} \mp x^{\frac{n}{8}} + 1$. Then, the rotation is $\mathbf{rot}(\mathbf{v}) = (-v_{n-1}, v_0, v_1, \cdots, v_{\frac{n}{8}-1} \pm v_{n-1}, \cdots, v_{\frac{3n}{8}-1} \mp v_{n-1}, \cdots, v_{\frac{n}{2}-1} + v_{n-1}, \cdots, v_{\frac{5n}{8}-1} \mp v_{n-1}, \cdots, v_{\frac{7n}{8}-1} \pm v_{n-1}, \cdots, v_{n-2})$.

4.2 Rotation-Based Gauss Sieve

The RGS is a variant of the IGS that reduces the computational complexity of the preprocessing of the ReduceRot function of the IGS. We propose the ImprovedReduceRot function in Algorithm 5 as a replacement for the ReduceRot function. In the previous algorithm (Algorithm 3, 4), ReduceRot (ReduceInverseRot) function needs to copy $\mathbf{v}$ to $\mathbf{v}'$ (Line 1 in Algorithm 3, 4) to prevent $\mathbf{v}$ itself to be changed due to the rotation $\mathbf{v} \leftarrow \mathbf{rot}(\mathbf{v})$. The rotation for $\mathbf{v}$ may break the pairwise-reduced relationship between $\mathbf{v}$ and the list L if $\mathbf{v}$ changes since the input vector $\mathbf{v}$ is pairwise-reduced to L in the GS algorithm.

In contrast, the ImprovedReduceRot function can rotate $\mathbf{v}$ itself and no preprocessing for $\mathbf{v}$ is required. We consider the period of rotation to explain the algorithm.

Theorem 2. For a cyclotomic polynomial $\Phi_m(x)$, the period of rotation is m. Namely, $\mathbf{rot}^m(\mathbf{v}) = \mathbf{v}$.

Proof. By transposing the recurrence relation given by the definition of the cyclotomic polynomial $\Phi_m(x) = \frac{x^m-1}{\prod_{d|m,d\neq m}\Phi_d(x)}$, we obtain $x^m = \Phi_m(x)\prod_{d|m,d\neq m}\Phi_d(x) + 1$. Hence, $x^m \equiv 1 \mod \Phi_m(x)$. Namely, $\mathbf{rot}^m(\mathbf{v}) = x^m\mathbf{v}(x) \equiv \mathbf{v}(x) \bmod \Phi_m(x) = \mathbf{v}$. Let i be a divisor of m satisfies $i < m$, then, $x^i - 1 = \Phi_i(x)\prod_{d|i,d\neq i}\Phi_d(x)$. $x^i - 1$ is not divisible by

$\Phi_m(x)$ since $\Phi_m(x)$ is a divisor of $x^m - 1$ and is not a divisor of $x^k - 1$ for any $k < m$. Thus, $\Phi_i(x) \prod_{d|i, d\neq i} \Phi_d(x)$ is also not divisible by $\Phi_m(x)$ and $x^i \not\equiv 1 \mod \Phi_m(x)$ for $i < m$. □

From Theorem 2, the original vector $\mathbf{v}$ is obtained by rotating it until reaching the period of $\mathbf{v}$. In the ImprovedReduceRot function, $\mathbf{v}$ is rotated (inversely) toward a closer period of $\mathbf{v}$ after k rotations and reductions (Line 4 in Algorithm 5). The process between Line 6 and Line 10 is to apply the reduction for the inverse direction. The purpose of rotations in Line 6 and Line 10 is to initialize the rotated vector $\mathbf{v}$ to the non-rotated state. Namely, $\mathbf{v} \leftarrow \mathbf{rot}^{-k}(\mathbf{rot}^k(\mathbf{v}))$ in Line 6 and $\mathbf{v} \leftarrow \mathbf{rot}^k(\mathbf{rot}^{-k}(\mathbf{v}))$ in Line 10. The optimal value of k depends on m and t. The analysis of k is described in Sect. 5. If m is even, the following equation holds.

Corollary 3. If m is even, $\mathbf{rot}^{\frac{m}{2}}(\mathbf{v}) = -\mathbf{v}$.

Proof. Let $m = 2m'$. From $\Phi_{2m'}(x) = \frac{x^{2m'}-1}{\prod_{d|2m', d\neq 2m'} \Phi_d(x)}$ and $x^{2m'} - 1 = (x^{m'} + 1)(x^{m'} - 1)$, $x^{m'} = \frac{\Phi_{2m'}(x) \prod_{d|2m', d\neq 2m'} \Phi_d(x)}{x^{m'}-1} - 1$. Since $\prod_{d|2m', d\neq 2m'} \Phi_d(x)$ is divisible by $x^{m'} - 1$ then $x^{m'} \equiv -1 \mod \Phi_m(x)$. Thus, $\mathbf{rot}^{m'}(\mathbf{v}) = -\mathbf{v}$. □

If $\mathbf{v}$ and L are pairwise-reduced, then $-\mathbf{v}$ and L are pairwise-reduced. Thus, we use $m/2$ as the maximal number of rotation when m is even.

We evaluate the difference in the computational complexity between the copy operation in Algorithm 3 and that required to rotate $\mathbf{rot}^k(\mathbf{v})$ to $\mathbf{v}$ in Algorithm 5. The complexity of the former is $O(n)$, while that of the latter is $O(\min(k, m - k)t)$. In Sect. 5, it is claimed that $\min(k, m - k)$ is a *constant*. The complexity of the rotation is $O(t)$. Since $t \leq n - 1$, the time complexity required by the ImprovedReduceRot function is smaller than that of the ReduceRot function. In the GS, the reduce function is repeatedly called until the shortest vector is found. Thus, the overall computational time can be reduced by replacing the ReduceRot function with the ImprovedReduceRot function. The experimental results of the RGS are presented in the next section.

5. Experiments and Analysis

We compute the optimal number of rotations k for a t-nomial lattice with various values of t and then analyze k by comparing the norm of $\mathbf{v}$ with that of $\mathbf{rot}(\mathbf{v})$. Furthermore, we measure the performance of our method and existing methods for SVPs in ideal lattices. Our implementation is based on the `gsieve` library released by Voulgaris [19]. We implemented our algorithm in C++. All experiments were performed on iMac (8GB of memory and Intel Core i5 3GHz CPU).

First, we computed the optimal number of rotations k for each t. In the experiments, we measured the average runtime needed to solve the Ideal Lattice Challenge[†] for 10 executions. For each executions, we generated an input basis randomly. We omitted the inverse rotation direction for the sake of simplicity. Figure 1 shows the results for $t = 2, 3, 5$ and 7. Figure 2 shows the result for various t where the dimension n is fixed in near 40. The runtime was minimized

[†]https://www.latticechallenge.org/ideallattice-challenge/

Algorithm 5: ImprovedReduceRot

Input: $\mathbf{u}, \mathbf{v} \in \mathcal{L}(\mathbf{B})$, number of rotations k
Output: $\mathbf{u} \in \mathcal{L}(\mathbf{B})$

1 **for** $i \leftarrow 0, \cdots, k$ **do**
2 **if** $|2\langle \mathbf{u}, \mathbf{v}\rangle| > \|\mathbf{v}\|^2$ **then** $\mathbf{u} \leftarrow \mathbf{u} - \left\lfloor \frac{\langle \mathbf{u}, \mathbf{v}\rangle}{\|\mathbf{v}\|^2} \right\rceil \mathbf{v}$
3 $\mathbf{v} \leftarrow \mathbf{rot}(\mathbf{v})$
4 **if** $k \geq m - k$ **then** $\mathbf{v} \leftarrow \mathbf{rot}^{m-k}(\mathbf{v})$
5 **else**
6 $\mathbf{v} \leftarrow \mathbf{rot}^{-k}(\mathbf{v})$
7 **for** $i \leftarrow 1, \cdots, k$ **do**
8 **if** $|2\langle \mathbf{u}, \mathbf{v}\rangle| > \|\mathbf{v}\|^2$ **then** $\mathbf{u} \leftarrow \mathbf{u} - \left\lfloor \frac{\langle \mathbf{u}, \mathbf{v}\rangle}{\|\mathbf{v}\|^2} \right\rceil \mathbf{v}$
9 $\mathbf{v} \leftarrow \mathbf{rot}^{-1}(\mathbf{v})$
10 $\mathbf{v} \leftarrow \mathbf{rot}^k(\mathbf{v})$
11 **return u**

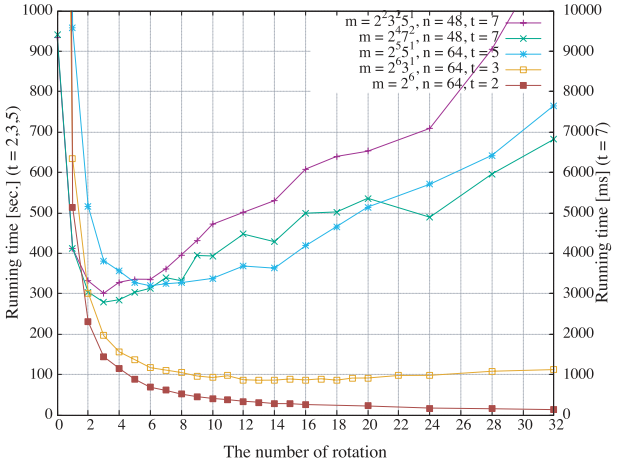

Fig. 1 Runtime of solving Ideal SVP for $t = 2, 3, 5$ and 7.

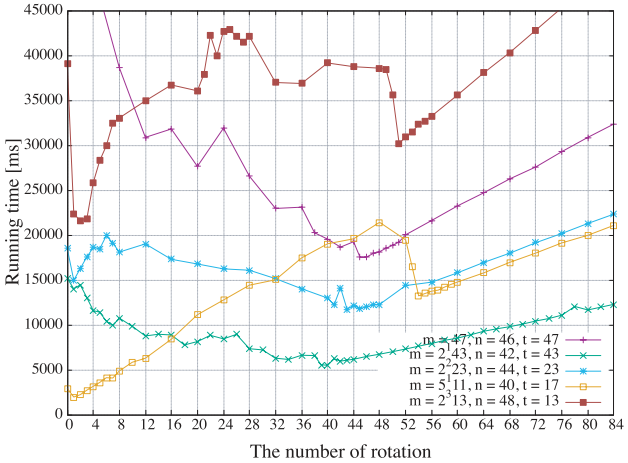

Fig. 2 Runtime of solving Ideal SVP for $n \approx 40$.

when $n = m/2$ for $t = 2$, The optimal $k = 13$, which is similar to the result of Ishiguro et al., where $t = 3$, as well as $k - 6$ at $t = 5$ and $k = 3$ at $t = 7$. Thus, the number of rotations k decreases as t increases.

From Fig. 2, two local minima of the runtime exist depending on m and t. When $m = p$ or $2p$, where p is an odd prime, the runtime is minimum when k is p. To analyze the result, we show the non-recursive expression of the i-times rotation and inverse rotation for $m = p, 2p$.

Proposition 1. For $m = p$, an integer i and $0 \le j \le n-1$, $\mathbf{rot}^i(\mathbf{v})$ is,

$$\mathbf{rot}^i(\mathbf{v})[j] = \mathbf{v}[x] - \mathbf{v}[y], \tag{3}$$

where, $x = (-i + j) \bmod p, y = (-i - 1) \bmod p$ and $\mathbf{v}[n] = \mathbf{v}[p-1] = 0$.

Proof. We show Eq. (3) by the mathematical induction. For $i = 0$, $\mathbf{rot}^0(\mathbf{v})[j] = \mathbf{v}[j] - \mathbf{v}[p-1] = \mathbf{v}[j]$. We assume that Eq. (3) is correct for a certain i. From Lemma 5, $\mathbf{rot}(\mathbf{rot}^i(\mathbf{v})[j]) = \mathbf{rot}^i(\mathbf{v})[j-1] - \mathbf{rot}^i(\mathbf{v})[n-1]$ for $j > 0$. From

$$\mathbf{rot}^i(\mathbf{v})[j-1] = \mathbf{v}[(-i + j - 1) \bmod p] - \mathbf{v}[y]$$

and

$$\mathbf{rot}^i(\mathbf{v})[n-1] = \mathbf{v}[(-i - 2) \bmod p] - \mathbf{v}[y],$$

we get

$$\begin{aligned}\mathbf{rot}^{i+1}(\mathbf{v})[j] = \ & \mathbf{v}[-((i+1) + j) \bmod p] \\ & -\mathbf{v}[-((i+1) - 1) \bmod p].\end{aligned}$$

The case for $j = 0$ is trivial. The same can be said for $\mathbf{rot}^{-1}$. □

Proposition 2. For $m = 2p$, $\mathbf{rot}^i(\mathbf{v})$ is,

$$\mathbf{rot}^i(\mathbf{v})[j] = \begin{cases} -\mathbf{v}[x] + (-1)^{j+1}\mathbf{v}[y] & (i_1 > j, i_2 < p) \\ \mathbf{v}[x] + (-1)^{j+1}\mathbf{v}[y] & (i_1 \le j, i_2 < p) \\ \mathbf{v}[x] + (-1)^{j}\mathbf{v}[y] & (i_1 > j, i_2 \ge p) \\ -\mathbf{v}[x] + (-1)^{j}\mathbf{v}[y] & (i_1 \le j, i_2 \ge p), \end{cases}$$

where, $x = (-i + j) \bmod p$, $y = (-i - 1) \bmod p$. $i_1 = i \bmod p, i_2 = i \bmod 2p$ and $0 \le i_1 < p, 0 \le i_2 < 2p$.

Proof. We can show the proposition in the same manner as Proposition 1. □

From Proposition 1, 2 no correlation exists between the number of rotations i and the norm since i only appears as the index of $\mathbf{v}$ in the formulae. Thus even if the number of rotations i increases, the norm does not increase significantly. Therefore, the runtime is minimized when k is the period p. For $m \ne p, 2p$, the runtime is minimized when k is small or when k is the period of m. The following two reasons are considered:

Reason 1 The norm changes as the number of rotations varies.

Reason 2 The norm has a period of m or $m/2$.

We consider the subtraction between a rotated vector and an original vector for Reason 1. The coefficients of $\Phi_m(x)$ are restricted to be chosen from $\{0, 1\}$ for the simplicity, but the following discussion can be extended to the case of $\{-1, 0, 1\}$. The subtraction between the norm is,

$$\|\mathbf{rot}(\mathbf{v})\|^2 - \|\mathbf{v}\|^2 = (t-2)v_{n-1}^2 - 2v_{n-1}\sum_{l=1}^{t-2} v_{i_l}. \tag{4}$$

Where the number of terms is t, the dimension is n and $0 \le i_1 < i_2 < \cdots < i_l < n-1$. If $\|\mathbf{rot}(\mathbf{v})\| \le \|\mathbf{v}\|$, then the probability that a reduction using $\mathbf{rot}(\mathbf{v})$ succeeds is greater than that when using $\mathbf{v}$. This proposition is derived from the following observation.

Observation 1. For any $0 \le r_1 < r_2 \le 2$, $\Pr[\|\mathbf{u}'\| \le \|\mathbf{u}\| \mid \mathbf{u}' = \mathrm{Reduction}(\mathbf{u}, \mathbf{v_1})] > \Pr[\|\mathbf{u}'\| \le \|\mathbf{u}\| \mid \mathbf{u}' = \mathrm{Reduction}(\mathbf{u}, \mathbf{v_2})]$, where $\|\mathbf{v_1}\| = r_1\|\mathbf{u}\|$ and $\|\mathbf{v_2}\| = r_2\|\mathbf{u}\|$.

We conducted an experiment to show the observation. The result is in Fig. 3. In the experiment, we generate an n-dimensional random vector $\mathbf{u}$ normalized to $\|\mathbf{u}\| = 1$ (we assume the type of a vector is floating point). Then we generate a random vector $\mathbf{v}$ satisfies $\|\mathbf{v}\| = r\|\mathbf{u}\|$ for a certain r. We counted the number of successful reductions of $\mathbf{u}$ and $\mathbf{v}$ for 10^4 iterations. We varied r and n for $0 \le r \le 2$ and $n = 5, 10, 20, 100, 200, 1000$. From Fig. 3, the success probability increases with decreasing r and the larger the dimension n, the smaller the probability.

For further concrete analysis, we evaluated Observation 1 for $\mathbf{rot}(\mathbf{v})$. The results are in Figs. 4, 5 and 6. In the experiments, we generate two random vectors $\mathbf{u}$ and $\mathbf{v}$ satisfy $\|\mathbf{u}\| = \|\mathbf{v}\| = 1$. We counted the number of success reductions of $\mathrm{Reduction}(\mathbf{u}, \mathbf{rot}(\mathbf{v}))$ for each ratio $r = \|\mathbf{rot}(\mathbf{v})\|$ out of 10^6 operations. From the results, it was confirmed that the success probability increases as the r decreases. Whereas, the number of success reductions is

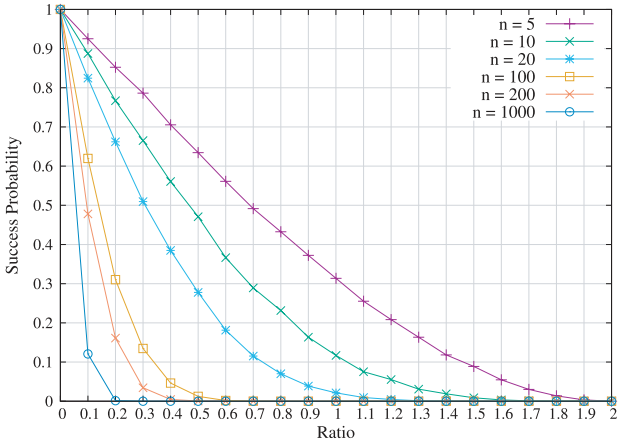

Fig. 3 The success probability $\Pr[\|\mathbf{u}'\| \le \|\mathbf{u}\| \mid \mathbf{u}' = \mathrm{Reduction}(\mathbf{u}, \mathbf{v})]$, where $\|\mathbf{v}\| = r\|\mathbf{u}\|$ for the ratio $0 \le r \le 2$.

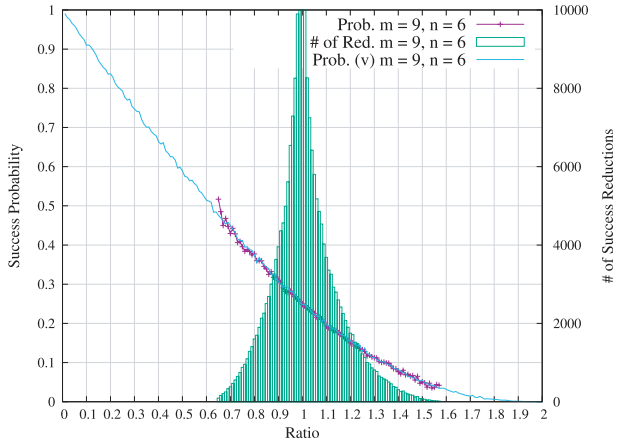

Fig. 4 The success probability and the number of success reduction of Reduction($\mathbf{u}$, $\mathbf{rot}(\mathbf{v})$) for the trinomial lattice ($n = 6$).

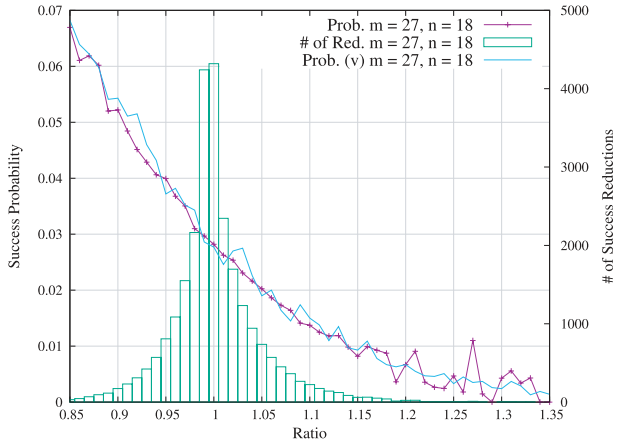

Fig. 5 The success probability and the number of success reduction of Reduction($\mathbf{u}$, $\mathbf{rot}(\mathbf{v})$) for the trinomial lattice ($n = 18$).

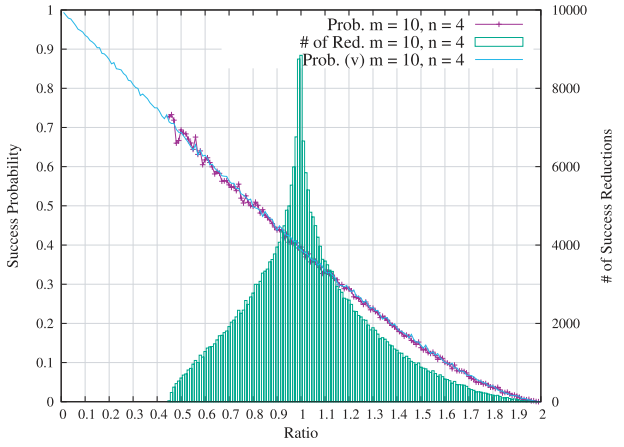

Fig. 6 The success probability and the number of success reduction of Reduction($\mathbf{u}$, $\mathbf{rot}(\mathbf{v})$) for the pentanomial lattice ($n = 4$).

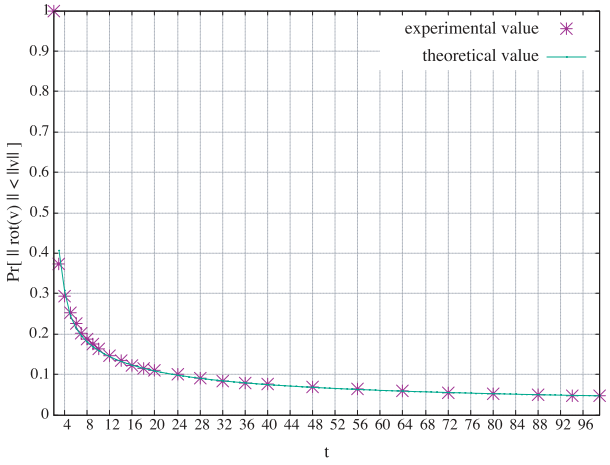

Fig. 7 Probability $\Pr[\|\mathbf{rot}(\mathbf{v})\| \le \|\mathbf{v}\|]$ for t.

distributed centered at $r = 1$. We overlay the graph corresponding to Reducton($\mathbf{u}$, $\mathbf{v}$) for each dimension in the blue line. It can be seen that the results of Reduction($\mathbf{u}$, $\mathbf{v}$) and Reduction($\mathbf{u}$, $\mathbf{rot}(\mathbf{v})$) are almost identical. Regarding to the variance of the reduction, the pentanomial lattice (Fig. 6) seems to larger than the trinomial lattice (Fig. 4) due to its rotation formula.

Now we analyze the probability $\Pr[\|\mathbf{rot}(\mathbf{v})\| \le \|\mathbf{v}\|]$ for t. From Eq. (4), the necessary and sufficient condition of $(t-2)v_{n-1}^2 - 2v_{n-1}\sum_{l=1}^{t-2} v_{i_l} < 0$ is, $v_{n-1}\sum_{l=1}^{t-2} v_{i_l} > 0$ and $|v_{n-1}| < \frac{2}{t-2}\left|\sum_{l=1}^{t-2} v_{i_l}\right|$. If each element of the vector is chosen from an uniform distribution and all elements are identically distributed, then the probability $p(t)$ that the norm of a t-nomial vector decreases by a rotation is approximated by the following equation.

Theorem 3. We assume that each element of a vector is chosen from the uniform distribution on $[-1, 1]$, then $p(t)$ is approximated by $p(t) \simeq \sqrt{\frac{3}{2(t-2)\pi}}(1 - e^{-\frac{3(t-2)}{8}}) + \frac{1}{2}\mathrm{erf}(\sqrt{\frac{3(t-2)}{2}}) - \frac{1}{2}\mathrm{erf}(\frac{1}{2}\sqrt{\frac{3(t-2)}{2}})$, where, $\mathrm{erf}(x)$ is the error function *s.t.* $\mathrm{erf}(x) = \int_0^x \frac{2}{\sqrt{\pi}} e^{-z^2} dz$.

Proof. The probability that v_{n-1} and $\sum_{l=1}^{t-2} v_{i_l}$ have the same sign is $1/2$. The expected value of each element of the vector is 0, and the variance is $\frac{t-2}{3}$. Thus, the probability density function $f(z)$ of $z = \frac{2}{t-2}\left|\sum_{l=1}^{t-2} v_{i_l}\right|$ is approximated using the central limit theorem as follows,

$$f(z) \simeq \begin{cases} 0 & z < 0 \\ 2\sqrt{\frac{3}{2\pi(t-2)}} e^{-\frac{3z^2}{2(t-2)}} & z \ge 0. \end{cases}$$

By the definition of the cumulative distribution function, $\Pr[|v_{n-1}| < z]$ is denoted as $\Pr[|v_{n-1}| < z] = \frac{2}{t-2}\int_0^{\frac{t-2}{2}} z f(z) dz + \int_{\frac{t-2}{2}}^{t-2} f(z) dz$. Finally, we obtain the above equation since $p(t) \simeq \frac{1}{2}\Pr[|v_{n-1}| < z]$. □

Figure 7 shows $p(t)$ and the experimental value of the norm decrease probability for various t. In our experiments, each element of the vector $\mathbf{v}$ was first chosen from the uniform distribution on $[-10^5, 10^5]$, then we rotated $\mathbf{v}$ and compared the norms of $\mathbf{v}$ and $\mathbf{rot}(\mathbf{v})$. We calculated the ratio at

Table 1 Runtime for solving ideal lattice SVP (in seconds). The result of this paper is represented by bold font.

m	n	t	GS	IGS	RGS1[†]	RGS2[†]
128	64	2	7,432	18	**17**	–
192	64	3	3,423	129	**113**	**73**
200	80	5	904,860	**98,581**[*]	**89,502**[*]	**52,164**[*]
240	64	7	5,127	**745**[*]	**666**[*]	**455**[*]

[*] using t-nomial lattice
[†] using ImprovedReduceRot function

which the norm decreased over 10^5 executions. Figure 7 shows that $p(t)$ approximated the experimental value almost correctly. We also confirmed that the probability of a decrease in the norm decreases as t increases. Thus, the larger the value of t is, the more easily the norm tends to increase per a rotation, and the optimal number of rotations t is considered to be small.

We generalize the discussion above from one rotation to k-fold rotations. Assume that the norm of the vector $\mathbf{v}$ increases to $c\|\mathbf{v}\|$ or decreases to $\|\mathbf{v}\|/c$ per a rotation ($c > 1$). When we rotate a vector $\mathbf{v}$ k times, an important factor of success of a reduction is that the norm $\|\mathbf{rot}^k(\mathbf{v})\|$ does not increase significantly from $\mathbf{v}$ and it stays in a certain range. Let $P_k(t)$ be the probability that $\|\mathbf{rot}^k(\mathbf{v})\|$ satisfies $\|\mathbf{v}\|/c \leq \|\mathbf{rot}^k(\mathbf{v})\| \leq c\|\mathbf{v}\|$ for k. By using $p(t)$ in Theorem 3, $P_k(t)$ is written as $P_k(t) = \binom{k}{\lceil \frac{k}{2} \rceil}\left(p(t)^{\lceil \frac{k}{2} \rceil}(1-p(t))^{\lfloor \frac{k}{2} \rfloor} + p(t)^{\lfloor \frac{k}{2} \rfloor}(1-p(t))^{\lceil \frac{k}{2} \rceil}\right)$. For a threshold τ, we compute the maximum k that satisfies $P_k(t) \geq \tau$. When $\tau = 0.3$, k is theoretically derived that is closer to the experimental value of k as follows, when $t = 3$ then $k = 15$, when $t = 5$ then $k = 5$, when $7 \leq t \leq 17$ then $k = 3$, when $18 \leq t \leq 33$ then $k = 2$, and when $34 \leq t$ then $k = 1$. At least one rotation is valid for speeding up the GS for any dimension.

We compared the average runtime between the proposed algorithm and the existing algorithms for 10 executions. The results are displayed in Table 1. We implemented the GS, the IGS with the ReduceInverseRot function (IGS), the RGS without the inverse rotation for the reduction (RGS1), and the RGS with the inverse rotation (RGS2). The cyclotomic polynomials for each m are, $\Phi_{128}(x) = x^{64} + 1$, $\Phi_{192}(x) = x^{64} - x^{32} + 1$, $\Phi_{200}(x) = x^{80} - x^{60} + x^{40} - x^{20} + 1$ and $\Phi_{240}(x) = x^{64} + x^{56} - x^{40} - x^{32} - x^{24} + x^8 + 1$. For $t > 3$, we implemented t-nomial rotation/inverse rotation in IGS and compared the runtime with those of RGS1 and RGS2 under the same conditions. We used the optimal number of rotations k obtained in the previous experiment. For $t = 2$, since the inverse rotation is useless because we rotate a vector until reaching its period, IGS uses the ReduceRot function instead, and we omit RGS2. Table 1 shows that RGS1 is faster than GS and IGS nevertheless RGS1 did not use the inverse rotation. The main reason is that the process of copying vector $\mathbf{v}$ in IGS required much more time in practice than the rotation without it in RGS1. Moreover, RGS2 is approximately 1.5 times faster than RGS1, as the ImprovedReduceRot function enables a reduction in the vector $\mathbf{u}$ by inverse rotations without additional cost to prepare an extra vector $\mathbf{v}''$ for the inverse rotation. The function leverages the inverse rotation for the reduction more efficiently than does the ReduceInverseRot function. Table 1 also implies that the t-nomial lattice is useful for not only our algorithm, but also others such as IGS based on the GS. For the same dimension, the smaller t is, the smaller the runtime due to the cost of the rotation for t and the probability of decreasing the norm by a rotation. We presented the first time that GS could be sped up for $t > 3$.

Table 2 List size $|L|$ (# of sampled vectors) of IGS, RGS1 and RGS2. The **bold** font represents the smallest one.

m	n	t	IGS	RGS1	RGS2
128	64	2	685	685	–
192	64	3	2,932	3,796	**2,502**
200	80	5	76,931	78,460	**50,042**
240	64	7	9,594	8,972	**7,821**

The space complexity is bounded by the list size of L, in which Gauss-reduced and relatively shorter lattice vectors are contained. We measured the average list size of IGS, RGS1 and RGS2 for 10 executions. The results are showen in Table 2. When $t = 2$, no difference exists between IGS and RGS. For other values of t, RGS2 is the smallest among the algorithms. However, RGS1 is not always smaller than IGS. The main reason is that the probability of a collision is higher when one uses the inverse rotation for the reduction.

6. Conclusion

In this paper, we defined t-nomial lattices as a generalized expression of anti-cyclic lattices, prime cyclotomic lattices, and trinomial lattices. Then, we designed the rotation operation and the inverse rotation operation for t-nomial lattices by unraveling the relationship between the dimension n of the input vectors, $\Phi_m(x)$ and t, i.e., the number of terms of $\Phi_m(x)$. We applied the rotation and inverse rotation structures of t-nomial lattices to the IGS, and showed that it could reduce the computational time of the GS regardless of the dimensions. Moreover, we proposed RGS algorithm that could reduce the overhead caused by the copying of vectors in the IGS. Our experimental results suggested that the RGS was more than 1.5 times faster than the IGS.

References

[1] M. Ajtai, "The shortest vector problem in L_2 is NP-hard for randomized reductions," Proc. thirtieth annual ACM symposium on Theory of computing, pp.10–19, 1998.
[2] M. Pohst, "On the computation of lattice vectors of minimal length, successive minima and reduced bases with applications," SIGSAM Bull., vol.15, no.1, pp.37–44, 1981.
[3] M. Ajtai, R. Kumar, and D. Sivakumar, "A sieve algorithm for the shortest lattice vector problem," Proc. Thirty-third Annual ACM Symposium on Theory of Computing, STOC'01, pp.601–610, ACM, 2001.
[4] D. Micciancio and P. Voulgaris, "Faster exponential time algorithms for the shortest vector problem," Proc. Twenty-first Annual ACM-SIAM Symposium on Discrete Algorithms, SODA'10, pp.1468–1480, SIAM, 2010.
[5] L. Ducas, "Shortest vector from lattice sieving: A few dimensions

for free," Advances in Cryptology – EUROCRYPT 2018, pp.125–145, Springer, 2018.
[6] M.R. Albrecht, L. Ducas, G. Herold, E. Kirshanova, E.W. Postlethwaite, and M. Stevens, "The general sieve kernel and new records in lattice reduction," Advances in Cryptology – EUROCRYPT 2019, pp.717–746, Springer, 2019.
[7] S. Garg, C. Gentry, and S. Halevi, "Candidate multilinear maps from ideal lattices," Advances in Cryptology – EUROCRYPT 2013, pp.1–17, Springer, 2013.
[8] J. Hoffstein, J. Pipher, and J. Silverman, "NTRU: A ring-based public key cryptosystem," Algorithmic Number Theory, pp.267–288, Springer, 1998.
[9] M. Schneider, "Sieving for shortest vectors in ideal lattices," Progress in Cryptology – AFRICACRYPT 2013, pp.375–391, Springer, 2013.
[10] T. Plantard, W. Susilo, and Z. Zhang, "LLL for ideal lattices: re-evaluation of the security of Gentry–Halevi's FHE scheme," Des. Codes Cryptogr., vol.76, pp.325–344, 2015.
[11] A.K. Lenstra, H.W. Lenstra, and L. Lovász, "Factoring polynomials with rational coefficients," Math. Ann., vol.261, no.4, pp.515–534, 1982.
[12] T. Ishiguro, S. Kiyomoto, Y. Miyake, and T. Takagi, "Parallel Gauss sieve algorithm: Solving the SVP challenge over a 128-dimensional ideal lattice," Public-Key Cryptography – PKC 2014, pp.411–428, Springer, 2014.
[13] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," Advances in Cryptology – EUROCRYPT 2010, pp.1–23, Springer, 2010.
[14] H. Riesel, Prime Numbers and Computer Methods for Factorization, pp.305–308, Birchäuser, 1994.
[15] P. Klein, "Finding the closest lattice vector when it's unusually close," Proc. Eleventh Annual ACM-SIAM Symposium on Discrete Algorithms, SODA'00, pp.937–941, SIAM, 2000.
[16] T. Nagell, Introduction to Number Theory, pp.158–168, Wiley, 1951.
[17] L. Carlitz, "The number of terms in the cyclotomic polynomial $F_{pq}(x)$," The American Mathematical Monthly, vol.73, no.9, pp.979–981, 1966.
[18] A. Migotti, "Zur Theorie der Kreisteilungs-gleichung," S.-B. der Math.-Naturwiss. Class der Kaiser. Akad. Der Wiss., Wien, vol.87, pp.7–14, 1883.
[19] P. Voulgaris, "A simple implementation in C++ of Gauss Sieve," https://cseweb.ucsd.edu/˜pvoulgar/impl.html

Shintaro Narisada received his B.E. in Electrical, Information and Physics Engineering and his M.E. in Information Sciences from Tohoku University, Japan, in 2016 and 2018, respectively. He joined KDDI in 2018 and has been engaged in the research on lattice-based cryptography. He is currently an associate research engineer at the Information Security Laboratory of KDDI Research, Inc.

Hiroki Okada received his B.E. and M.E. in applied mathematics and physics from Kyoto University, Japan, in 2014 and 2016, respectively. He joined KDDI in 2016 and has been engaged in research on lattice-based cryptography and homomorphic encryption. He is currently an associate research engineer at the Information Security Laboratory of KDDI Research, Inc.

Kazuhide Fukushima received his M.E. in Information Engineering from Kyushu University, Japan, in 2004. He joined KDDI and has been engaged in the research on post-quantum cryptography, cryptographic protocols, and identification technologies. He is currently a research manager at the Information Security Laboratory of KDDI Research, Inc. He received his Doctorate in Engineering from Kyushu University in 2009. He received the IEICE Young Engineer Award in 2012. He served as the Editor of IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences from 2015 to 2017, and he is a Director, General Affairs of IEICE Engineering Science Society from 2019. He is a member of the Information Processing Society of Japan.

Shinsaku Kiyomoto received his B.E. in engineering sciences and his M.E. in Material Science from Tsukuba University, Japan, in 1998 and 2000, respectively. He joined KDD (now KDDI) and has been engaged in research on stream ciphers, cryptographic protocols, and mobile security. He is currently a senior researcher at the Information Security Laboratory of KDDI Research, Inc. He was a visiting researcher of the Information Security Group, Royal Holloway University of London from 2008 to 2009. He received his doctorate in engineering from Kyushu University in 2006. He received the IEICE Young Engineer Award in 2004 and Distinguished Contributions Awards in 2011. He is a member of IEICE and JPS.