Reduction of Search-LWE Problem to Integer Programming Problem

Masaaki Shirase[1] [0000–0001–8993–2848]

Future University Hakodate, Japan
shirase@fun.ac.jp

Abstract. Let $(A, \boldsymbol{t})$ be an instance of the search-LWE problem, where A is a matrix and $\boldsymbol{t}$ is a vector. This paper constructs an integer programming problem as Eq.(13) using A and $\boldsymbol{t}$, and shows that it is possible to derive a solution of the instance $(A, \boldsymbol{t})$ (perhaps with high probability) using its optimal solution or its tentative solution of small norm output by an integer programming solver. In other words, the LWE-search problem can be reduced to an integer programming problem. In the reduction, only basic linear algebra and finite field calculation are required. The computational complexity of the integer programming problem obtained is still unknown.

Keywords: LWE problem · Integer programming problem · Lattice-based cryptography · Linear algebra · Finite field.

1 Introduction

Public key cryptographies have solved the long and serious key delivery problem, and have given various cryptographic protocols such as digital signatures. Currently, RSA and elliptic curve cryptography (ECC) are the most commonly used public key cryptographies. However, when large quantum computers are realized, Shor's algorithm makes RSA and ECC attackable in polynomial time. A public key cryptography that is secure against a cryptanalytic attack by a quantum computer is called a post-quantum cryptography, and lattice-based cryptography is one of the candidates.

A lattice is set of linear combinations of integer coefficients of n vectors $\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n$ that are linear independent in the vector space $\mathbb{R}^m$. There are several lattice-related problems: the shortest vector problem, the nearest vector problem, and the learning with errors (LWE) problem.

Public key cryptographies based on the hardness of these problems have been proposed. Regev proposed a public key cryptography called Regev encryption based on the hardness of the LWE problem. A version of Regev encryption based on the hardness of the module LWE problem is called CRYSTLS-Kyber. The National Institute of Standards and Technology (NIST) launched a competition for the standardization of post-quantum cryptography in 2017. Although the selection process is still ongoing, CRYSTALS-Kyber was selected in 2022 [12]. Therefore, one of the important tasks in the field of cryptography is to investigate more precisely the hardness of the (module) LWE problem.

1.1 Symbols and Notation

This paper uses the following symbols.

p : a prime
$\mathbb{R}^n$: n-dimensional (row) vector space over $\mathbb{R}$
$\mathbb{Z}^n (\subset \mathbb{R}^n)$: subset of integer components of $\mathbb{R}^n$
$\mathbb{Z}_p = \{0, 1, 2, \cdots, p-1\}$ that forms a finite field
$\mathbb{Z}_p^n$: n-dimensional (row) vector space over $\mathbb{Z}_p$
$\mathbb{Z}_p^{n\times m}$: set of $n \times m$ matrices of $\mathbb{Z}_p$ components
E_n : $n \times n$ unit matrix
$\boldsymbol{\epsilon}_i \in \mathbb{R}^n$: unit vector with nth component of 1, e.g., $\boldsymbol{\epsilon}_1 = (1, 0, 0, \cdots, 0)$, $\boldsymbol{\epsilon}_2 = (0, 1, 0, \cdots, 0)$
$N(0, \sigma^2)$: the Gaussian distribution on $\mathbb{Z}_p$ with a mean value of 0 and a standard deviation σ
$\mathbf{0}_n \in \mathbb{R}^n$: n-dimensional zero vector
$\|\boldsymbol{x}\|$: norm of $\boldsymbol{x}$
$\lfloor x \rfloor$: the result is the largest integer smaller than or equal to x

Notation of Congruence Relation Because all congruences treated in this paper are of modulo p, "$a \equiv b \pmod p$" is abbreviated to "$a \equiv b$". For vectors $\boldsymbol{v} = (v_1, v_2, \cdots, v_n)$ and $\boldsymbol{w} = (w_1, w_2, \cdots, w_n) \in \mathbb{Z}^n$, we denote $\boldsymbol{v} \equiv \boldsymbol{w}$ if $v_i \equiv w_i$ for all i. For matrices $A = (a_{i,j})$ and $B = (b_{i,j}) \in \mathbb{Z}_p^{n\times m}$, we denote $A \equiv B$ if $a_{i,j} \equiv b_{i,j}$ for all i, j.

1.2 Contribution of This Paper

This paper shows that the search-LWE problem can be reduced to an integer programming problem. This process requires only basic linear algebra and finite field calculations. The applicability of the proposed method to the module LWE problem is a subject for future work.

2 Preliminary

2.1 Lattice

A lattice $L(\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n)$ is set of linear combinations of integer coefficients of n (row) vectors $\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n \in \mathbb{R}^m$ that are linear independent.

$$L(\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n) = \left\{ \sum_{i=1}^{n} a_i \boldsymbol{b}_i \in \mathbb{R}^m : a_i \in \mathbb{Z} \right\}$$

Let B be a matrix consisting of $\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n$.

$$B = \begin{pmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \\ \vdots \\ \boldsymbol{b}_n \end{pmatrix}$$

Then, the lattice $L(\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n)$ is also denoted as $L(B)$.

2.2 Search-LWE Problem

Assume that $A \in \mathbb{Z}_p^{n \times m}$ $(n < m)$, $\boldsymbol{s} \in \mathbb{Z}_p^n$, $\boldsymbol{e} \in \mathbb{Z}^m$, and $\boldsymbol{t} \in \mathbb{Z}_p^m$ satisfy

$$\boldsymbol{t} \equiv \boldsymbol{s}A + \boldsymbol{e}, \tag{1}$$

where the components of $\boldsymbol{e}$ are chosen according to $N(0, \sigma^2)$. The $\boldsymbol{e}$ is called the noise vector or the error vector. Given $(A, \boldsymbol{t})$, the problem of finding $\boldsymbol{s}$ is called the *search-LWE problem*. Although there is also a decision-LWE problem, this paper deals only with the search-LWE problem, and henceforth the search-LWE problem is referred to as the LWE problem.

Remark 1. When each component of $\boldsymbol{e}$ is chosen according to $N(0, \sigma)$, $\Pr[\|\boldsymbol{e}\| > 2\sqrt{m}\sigma] < 2^{-m+1}$ is satisfied [7]. Therefore, $\|\boldsymbol{e}\|$ is usually a small value. Also, from Lemma 1 of [6] or Gaussian heuristic, the probability that an instance $(A, \boldsymbol{t})$ with $\|\boldsymbol{e}\| \le 2\sqrt{m}\sigma$ has two solutions are negligibly small.

2.3 Existing Methods for Solving the LWE Problem

We briefly introduce representative methods to solve the LWE problem.

Reduction to the Bounded Distance Decoding (BDD) Problem The LWE problem is reduced to the BDD problem, and the BBD problem is solved using Babai's nearest-neighbor plane algorithm [4] or its improvements [10, 11].

Reduction to the Shortest Vector Problem For an instance $(A, \boldsymbol{t})$ of the LWE problem, construct a lattice L' containing the lattice $L(A)$ generated by A and $\boldsymbol{t}$. Then, $\boldsymbol{e} \in L'$ [2]. Since $\boldsymbol{e}$ is usually the shortest vector on L', we may search the shortest vector on L' using a basis reduction algorithm such as the LLL algorithm [9].

Application of the BKW Algorithm The BKW algorithm was originally proposed to solve the learning parity problem with noise [5]. The BKW algorithm can be used to solve the LWE problem.

Reduction to System of Nonlinear Equations Arora and Ge [3] showed that for an instance $(A, \boldsymbol{t})$ of the LWE problem with the relation (1), a system of noise-free nonlinear equation with $\boldsymbol{s}$ as its solution can be derived. The process uses the fact that if $-t \le e_i \le t$ for all e_is of components of $\boldsymbol{e}$, then each e_i is a solution of a polynomial $P(x) = x \prod_{i=1}^{t} (x + i)(x - i)$. The system can be solved using linearization techniques. The Gröbner basis can also be used to solve it [1].

Reduction to the Maximum Independent Set (MIS) Problem It was shown that the LWE problem can be reduced to the MIS problem in graph theory [8].

3 Proposed Method

Let $(A, \boldsymbol{t})$ be an instance of the LWE problem for a matrix $A \in \mathbb{Z}_p^{n\times m}$, vectors $\boldsymbol{s} \in \mathbb{Z}_p^n$, $\boldsymbol{e} \in \mathbb{Z}^m$, and $\boldsymbol{t} \in \mathbb{R}^m$ satisfying Eq.(1). In this section, we construct an integer programming problem such that the optimal solution or a tentative solution with small norm output by an integer programming (IP) solver is equal to $\boldsymbol{e}$ (perhaps with high probability) using A and $\boldsymbol{t}$. Note that the solution $\boldsymbol{s}$ of the instance is easily obtained from a subset of the set of components of $\boldsymbol{e}$ as Remark 2 given later.

3.1 Partitioning of Matrix and Vectors

For $A, \boldsymbol{t}$, and $\boldsymbol{e}$, define $A_0, A_1, \boldsymbol{t}_0, \boldsymbol{t}_1, \boldsymbol{e}_0$ and $\boldsymbol{e}_1$ as follows.

$$A = (A_0\ A_1),\quad \text{where} \begin{cases} A_0 = n \times n \text{ matrix to the left of } A, \\ A_1 = n \times (m-n) \text{ matrix to the right of } A. \end{cases}$$

$$\boldsymbol{t} = (\boldsymbol{t}_0\ \boldsymbol{t}_1),\quad \text{where} \begin{cases} \boldsymbol{t}_0 = n \text{ dimensional vector to the left of } \boldsymbol{t}, \\ \boldsymbol{t}_1 = (m-n) \text{ dimensional vector to the right of } \boldsymbol{t}. \end{cases}$$

$$\boldsymbol{e} = (\boldsymbol{e}_0\ \boldsymbol{e}_1),\quad \text{where} \begin{cases} \boldsymbol{e}_0 = n \text{ dimensional vector to the left of } \boldsymbol{e}, \\ \boldsymbol{e}_1 = (m-n) \text{ dimensional vector to the right of } \boldsymbol{e}. \end{cases}$$

For example, for $A = \begin{pmatrix} 0\ 1\ 2\ 3\ 4 \\ 5\ 6\ 7\ 8\ 9 \end{pmatrix}$, $A_0 = \begin{pmatrix} 0\ 1 \\ 5\ 6 \end{pmatrix}$ and $A_1 = \begin{pmatrix} 2\ 3\ 4 \\ 7\ 8\ 9 \end{pmatrix}$. For $\boldsymbol{t} = (0, 1, 2, 3, 4)$, $\boldsymbol{t}_0 = (0, 1)$ and $\boldsymbol{t}_1 = (2, 3, 4)$. Then, Eq.(1) can be rewritten as

$$\boldsymbol{t}_0 \equiv \boldsymbol{s}A_0 + \boldsymbol{e}_0, \tag{2}$$

$$\boldsymbol{t}_1 \equiv \boldsymbol{s}A_1 + \boldsymbol{e}_1. \tag{3}$$

3.2 Maps ϕ and $\psi : \mathbb{R}^n \to \mathbb{R}^{m-n}$

Assume that $A_0 \in \mathbb{Z}_p^{n\times n}$ is regular over $\mathbb{Z}_p$ [1]. Then, there exists $A_0^{-1} \in \mathbb{Z}_p^{n\times n}$ satisfying

$$A_0 A_0^{-1} \equiv A_0^{-1} A_0 \equiv E_n. \tag{4}$$

In fact, A_0^{-1} is the inverse matrix of A_0 over finite field $\mathbb{Z}_p$. Using $A_0^{-1}, A_1, \boldsymbol{t}_0$ and $\boldsymbol{t}_1$, define a map $\phi : \mathbb{R}^n \to \mathbb{R}^{m-n}$ as follows.

$$\begin{aligned} \phi : \mathbb{R}^n &\to \mathbb{R}^{m-n} \\ \boldsymbol{v} &\mapsto \boldsymbol{v}A_0^{-1}A_1 + \boldsymbol{t}_1 - \boldsymbol{t}_0 A_0^{-1} A_1 \end{aligned}$$

Furthermore, define another map $\psi : \mathbb{R}^n \to \mathbb{R}^{m-n}$ as

$$\psi(\boldsymbol{v}) = \phi(\boldsymbol{v}) - \phi(\boldsymbol{0}_n).$$

The maps ϕ and ψ have the following properties.

[1] It is equivalent to the determinant of A_0 not being a multiple of p.

Proposition 1. *(a)* $\phi(\boldsymbol{e}_0) \equiv \boldsymbol{e}_1$.
(b) Assume $\boldsymbol{v}_0 \in \mathbb{R}^n$ *and* $\boldsymbol{v}_1 \in \mathbb{R}^{m-n}$ *satisfies* $\phi(\boldsymbol{v}_0) \equiv \boldsymbol{v}_1$. *Let* $\hat{\boldsymbol{s}} \equiv (\boldsymbol{t}_0 - \boldsymbol{v}_0)A_0^{-1}$, *then,* $(\boldsymbol{t}_0\ \boldsymbol{t}_1) = \hat{\boldsymbol{s}}(A_0\ A_1) + (\boldsymbol{v}_0\ \boldsymbol{v}_1)$ *holds.*
(c) $\phi(\boldsymbol{0}_n) = \boldsymbol{t}_1 - \boldsymbol{t}_0 A_0^{-1} A_1$.
(d) $\psi(\boldsymbol{v}) = \boldsymbol{v}A_0^{-1}A_1$, *that is,* ψ *is a linear map.*
(e) $\sum k_i(\phi(\boldsymbol{v}_i) - \phi(\boldsymbol{0}_n)) = \phi(\sum(k_i\boldsymbol{v}_i)) - \phi(\boldsymbol{0}_n)$ *for* $k_i \in \mathbb{Z}$.

Proof. (a) We compute

$$\begin{aligned}
\phi(\boldsymbol{e}_0) &= \boldsymbol{e}_0 A_0^{-1}A_1 + \boldsymbol{t}_1 - \boldsymbol{t}_0 A_0^{-1}A_1 \\
&\equiv (\boldsymbol{t}_0 - \boldsymbol{s}A_0)A_0^{-1}A_1 + \boldsymbol{t}_1 - \boldsymbol{t}_0 A_0^{-1}A_1 \quad &&\text{(from Eq.(2))} \\
&= -\boldsymbol{s}A_0A_0^{-1}A_1 + \boldsymbol{t}_1 \\
&\equiv -\boldsymbol{s}A_1 + \boldsymbol{t}_1 &&\text{(from Eq.(4))} \\
&\equiv \boldsymbol{e}_1. &&\text{(from Eq.(3))}
\end{aligned}$$

(b) From the definition of $\hat{\boldsymbol{s}}$, we see

$$\hat{\boldsymbol{s}}A_0 + \boldsymbol{v}_0 \equiv (\boldsymbol{t}_0 - \boldsymbol{v}_0)A_0^{-1}A_0 + \boldsymbol{v}_0 \equiv \boldsymbol{t}_0.$$

In addition, from the assumption and the definition of ϕ, we compute

$$\begin{aligned}
\hat{\boldsymbol{s}}A_1 + \boldsymbol{v}_1 &\equiv (\boldsymbol{t}_0 - \boldsymbol{v}_0)A_0^{-1}A_1 + \phi(\boldsymbol{v}_0) \\
&= (\boldsymbol{t}_0 - \boldsymbol{v}_0)A_0^{-1}A_1 + (\boldsymbol{v}_0A_0^{-1}A_1 + \boldsymbol{t}_1 - \boldsymbol{t}_0A_0^{-1}A_1) \\
&\equiv \boldsymbol{t}_1.
\end{aligned}$$

(c) It is clear from the definition of ϕ.
(d) We compute

$$\begin{aligned}
\psi(\boldsymbol{v}) &= \phi(\boldsymbol{v}) - \phi(\boldsymbol{0}_n) \\
&= (\boldsymbol{v}A_0^{-1}A_1 + \boldsymbol{t}_1 - \boldsymbol{t}_0A_0^{-1}A_1) - (\boldsymbol{t}_1 - \boldsymbol{t}_0A_0^{-1}A_1) \quad \text{(from (c))} \\
&= \boldsymbol{v}A_0^{-1}A_1.
\end{aligned}$$

(e) From the linearity of ψ, we compute

$$\begin{aligned}
\text{Left side} &= \sum k_i(\phi(\boldsymbol{v}_i) - \phi(\boldsymbol{0}_n)) \\
&= \sum k_i\psi(\boldsymbol{v}_i) \\
&= \psi\left(\sum k_i\boldsymbol{v}_i\right) \\
&= \phi\left(\sum k_i\boldsymbol{v}_i\right) - \phi(\boldsymbol{0}_n) \\
&= \text{Right side.} \quad \square
\end{aligned}$$

Remark 2. Given an instance $(A, \boldsymbol{t})$ of the LWE problem, set $A_0, \boldsymbol{t}_0$, and $\boldsymbol{e}_0$ as in Sect.3.1. Assume A_0 is regular on $\mathbb{Z}_p$. Then, we have

$$\boldsymbol{s} \equiv (\boldsymbol{t}_0 - \boldsymbol{e}_0)A_0^{-1}$$

from Eq.(2). Thus, it is sufficient to obtain $\boldsymbol{e}_0$ to solve the instance.

3.3 Construction of the Integer Programming Problem

If $\boldsymbol{e} = (e_1, e_2, \cdots, e_m)$ $(e_i \in \mathbb{Z})$, we can write $\boldsymbol{e}_0$ and $\boldsymbol{e}_1$ as

$$\begin{cases} \boldsymbol{e}_0 = (e_1, e_2, \cdots, e_n), \\ \boldsymbol{e}_1 = (e_{n+1}, e_{n+2}, \cdots, e_m). \end{cases} \tag{5}$$

In addition, we can write $\boldsymbol{e}_0$ as

$$\boldsymbol{e}_0 = e_1\boldsymbol{\epsilon}_1 + e_2\boldsymbol{\epsilon}_2 + \cdots + e_n\boldsymbol{\epsilon}_n \tag{6}$$

with each unit vector $\boldsymbol{\epsilon}_i$.

For $i = 1, 2, \cdots, n$, let $\boldsymbol{w}_i$ be

$$\boldsymbol{w}_i = \phi(\boldsymbol{\epsilon}_i) - \phi(\boldsymbol{0}_n)(= \psi(\boldsymbol{\epsilon}_i)) \in \mathbb{R}^{m-n}, \tag{7}$$

and the components of $\boldsymbol{w}_i$ be

$$\boldsymbol{w}_i = (w_{i,1}, w_{i,2}, \cdots, w_{i,m-n}) \ \ (w_{i,j} \in \mathbb{Z}_p). \tag{8}$$

Furthermore, let

$$\phi(\boldsymbol{0}_n) = (u_1, u_2, \cdots, u_{m-n}) \ \ (u_i \in \mathbb{Z}_p). \tag{9}$$

Then, we compute

$$\begin{aligned} \boldsymbol{e}_1 &\equiv \phi(\boldsymbol{e}_0) && \text{(from Proposition 1 (a))} \\ &= \phi(e_1\boldsymbol{\epsilon}_1 + e_2\boldsymbol{\epsilon}_2 + \cdots + e_n\boldsymbol{\epsilon}_n) && \text{(from Eq.(6))} \\ &= \sum_{i=1}^{n}(e_i(\phi(\boldsymbol{\epsilon}_1) - \phi(\boldsymbol{0}_n)) + \phi(\boldsymbol{0}_n) && \text{(from Proposition 1 (e))} \\ &= e_1\boldsymbol{w}_1 + e_2\boldsymbol{w}_2 + \cdots + e_n\boldsymbol{w}_n + \phi(\boldsymbol{0}_n). && \text{(from Eq.(7))} \end{aligned}$$

Then, from Eqs.(5) and (9) we see

$$e_{n+i} \equiv w_{1,i}e_1 + w_{2,i}e_2 + \cdots + w_{n,i}e_n + u_i \tag{10}$$

for $i = 1, 2, \cdots, m - n$. Therefore, the system of linear equations over $\mathbb{Z}_p$

$$\begin{cases} w_{1,1}x_1 + w_{2,1}x_2 + \cdots + w_{n,1}x_n + u_1 = x_{n+1} \\ w_{1,2}x_1 + w_{2,2}x_2 + \cdots + w_{n,2}x_n + u_2 = x_{n+2} \\ \qquad \vdots \\ w_{1,m-n}x_1 + w_{2,m-n}x_2 + \cdots + w_{n,m-n}x_n + u_{m-n} = x_m \end{cases} \tag{11}$$

with $x_1, x_2, \cdots, x_m$ as variables has a solution $(x_1, x_2, \cdots, x_m) = (e_1, e_2, \cdots, e_m)$.

But, the system (11) doesn't have a unique solution because

$$m \text{ (number of variables)} > m - n \text{ (number of equations)}.$$

Then, let's modify this system into an integer programming problem. The congruence equation (10) can be made into an integer equation

$$w_{1,i}e_1 + w_{2,i}e_2 + \cdots + w_{n,i}e_n - e_{n+i} + pf_i = -u_i \tag{12}$$

using some $f_i \in \mathbb{Z}$.

Next consider the range of each component e_i of $\boldsymbol{e}$ and f_i. Since each e_i is chosen according to $N(0, \sigma^2)$, we can choose $t \in \mathbb{N}$ satisfying

$$-t \le e_i \le t \quad (i = 1, 2, \cdots, m)$$

with high probability. Then, $0 \le w_{i,j} \le p-1$ and Eq.(12) give the range of f_is as

$$-\left\lfloor \frac{t(np-n+1)+p-1}{p} \right\rfloor \le f_i \le \left\lfloor \frac{t(np-n+1)}{p} \right\rfloor \quad (i = 1, 2, \cdots, m-n).$$

In addition, $\|\boldsymbol{e}\|$ is sufficiently small from Remark 1.

The following lemma gives efficient computation of $w_{i,j}$ and u_i.

Lemma 1. *Suppose we are given an instance $(A, \boldsymbol{t})$ of the LWE problem, where $A \in \mathbb{Z}_p^{n\times m}$ $(n < m)$ and $\boldsymbol{t} \in \mathbb{R}^m$. Set A_0 and t_0 as in Sect.3.1. Assume A_0 is regular over $\mathbb{Z}_p$.*

(a) Define an $n \times (m-n)$ matrix W as $W = (w_{i,j})$ using $w_{i,j}$ given by Eq.(8). Then, $W \equiv A_0^{-1}A_1$.

(b) For u_i given Eq.(9), $(u_1, u_2, \cdots, u_{m-n}) = \boldsymbol{t}_1 - \boldsymbol{t}_0 A_0^{-1} A_1$.

Proof. (a) From the definition of $w_{i,j}$, we see

$$W = \begin{pmatrix} \boldsymbol{w}_1 \\ \boldsymbol{w}_2 \\ \vdots \\ \boldsymbol{w}_n \end{pmatrix}.$$

From Eq.(7), definition of ψ, and Proposition 1 (d), we compute

$$W = \begin{pmatrix} \psi(\boldsymbol{\epsilon}_1) \\ \psi(\boldsymbol{\epsilon}_2) \\ \vdots \\ \psi(\boldsymbol{\epsilon}_n) \end{pmatrix} \equiv \begin{pmatrix} \boldsymbol{\epsilon}_1 A_0^{-1} A_1 \\ \boldsymbol{\epsilon}_2 A_0^{-1} A_1 \\ \vdots \\ \boldsymbol{\epsilon}_n A_0^{-1} A_1 \end{pmatrix} \equiv E_n A_0^{-1} A_1 \equiv A_0^{-1} A_1.$$

(b) From Proposition 1 (c), we see

$$(u_1, u_2, \cdots, u_{m-n}) = \phi(\boldsymbol{0}_n) = \boldsymbol{t}_1 - \boldsymbol{t}_0 A_0^{-1} A_1. \qquad \square$$

The discussion so far gives the following proposition.

Proposition 2. *Suppose we are given an instance $(A, \boldsymbol{t})$ of the LWE problem satisfying Eq.(1), where $A \in \mathbb{Z}_p^{n\times m}$ $(n < m)$ and $\boldsymbol{t} \in \mathbb{R}^m$. Set A_0 and $\boldsymbol{t}_0$ as in Sect.3.1. Assume A_0 is regular over $\mathbb{Z}_p$. We compute $w_{i,j}$ and u_i $(i = 0, 1, \cdots, m-n,\ j = 1, 2, \cdots, n)$ as Lemma 1, and select $t \in \mathbb{N}$. Construct the following integer programming problem with x_i, y_j as variables.*

$$\begin{cases} \textbf{minimize:} \\ \quad x_1^2 + x_2^2 + \cdots + x_m^2 \\ \textbf{subject to:} \\ \quad w_{1,1}x_1 + w_{2,1}x_2 + \cdots + w_{n,1}x_n - x_{n+1} + py_1 = -u_1 \\ \quad w_{1,2}x_1 + w_{2,2}x_2 + \cdots + w_{n,2}x_n - x_{n+2} + py_2 = -u_2 \\ \quad \vdots \\ \quad w_{1,m-n}x_1 + w_{2,m-n}x_2 + \cdots + w_{n,m-n}x_n - x_m + py_{m-n} = -u_{m-n} \\ \quad -t \le x_i \le t \\ \quad -\lfloor (t(np-n+1)+p-1)/p \rfloor \le f_i \le \lfloor (t(np-n+1)/p \rfloor \quad (i = 1, 2, \cdots, m-n) \\ \quad x_i, y_j \in \mathbb{Z} \ \ (i = 0, 1, \cdots, n,\ j = 1, 2, \cdots, m-n) \end{cases} \tag{13}$$

For the optimal solution or a tentative solution with small norm to this problem $(x_1, x_2, \cdots, x_m) = (\hat{x}_1, \hat{x}_2, \cdots, \hat{x}_m)$ output by an IP solver, set $\hat{\boldsymbol{x}}_0 = (\hat{x}_1, \hat{x}_2, \cdots, \hat{x}_n) \in \mathbb{R}^n$. Then,

$$\hat{\boldsymbol{s}} = (\boldsymbol{t}_0 - \boldsymbol{x}_0)A_0^{-1} \tag{14}$$

is a solution of the instance $(A, \boldsymbol{t})$ of the LWE problem with high probability.

Proof. Set $\hat{\boldsymbol{x}} = (\hat{x}_1, \hat{x}_2, \cdots, \hat{x}_m) \in \mathbb{R}^m$ and $\hat{\boldsymbol{x}}_1 = (\hat{x}_{n+1}, \hat{x}_{n+2}, \cdots, \hat{x}_m) \in \mathbb{R}^{m-n}$. From the discussion of Sect.3.3, $\phi(\hat{\boldsymbol{x}}_0) \equiv \hat{\boldsymbol{x}}_1$ holds. Then, from Proposition 1 (b) we see

$$\boldsymbol{t} = \hat{\boldsymbol{s}}A + \hat{\boldsymbol{x}} \text{ that implies } \boldsymbol{t}_0 = \hat{\boldsymbol{s}}A_0 + \hat{\boldsymbol{x}}_0.$$

The solution $\boldsymbol{s} = (\boldsymbol{s}_0\ \boldsymbol{s}_1)$ of the instance $(A, \boldsymbol{t})$ satisfies

$$\boldsymbol{t} = \boldsymbol{s}A + \boldsymbol{e} \text{ that implies } \boldsymbol{t}_0 = \boldsymbol{s}_0A + \boldsymbol{e}_0.$$

If $\|\hat{\boldsymbol{x}}\|$ is small enough, then $\hat{\boldsymbol{x}} = \boldsymbol{e}$ that implies $\hat{\boldsymbol{x}}_0 = \boldsymbol{e}_0$ with high probability from Remark 1. In this case, we see

$$\begin{aligned} \hat{\boldsymbol{s}}A_0 &= \boldsymbol{s}A_0 \\ \hat{\boldsymbol{s}} &\equiv sA_0A_0^{-1} \equiv s, \end{aligned}$$

and $\hat{\boldsymbol{s}} = \boldsymbol{s}$ since $\boldsymbol{s}, \hat{\boldsymbol{s}} \in \mathbb{Z}_p^n$. □

Remark 3. For $t \in \mathbb{N}$ selected in Proposition 2, if t is too small such that $-t \le e_i \le t$ is not held, perhaps an IP solver cannot output any solution. Perhaps, the bigger t is, the longer run time of the IP solver is.

Remark 4. The proposed method and the method of Arora and Ge [3] may look similar. However, the method of Arora and Ge derives a nonlinear polynomial system whose solution is $\boldsymbol{s}$, while the proposed method derives an integer programming problem such that the optimal solution or a tentative solution with small norm is $\boldsymbol{e}$ with high probability. The derivation of the integer programming problem is obtained using by only basic linear algebra and finite field calculations.

4 Conclusion and Future Work

This paper has constructed a system of linear equations over $\mathbb{Z}_p$ given an instance $(A, \boldsymbol{t})$ of the search-LWE problem with the relation $\boldsymbol{t} \equiv \boldsymbol{s}A + \boldsymbol{e} \pmod{p}$ such that one of its solutions is equal to $\boldsymbol{e}$ but it is not unique one. Then, this paper has modified this system into an integer programming problem as Eq.(13). Its optimal solution or its tentative solution with small norm is also equal to $\boldsymbol{e}$ with high probability We has been able to make a solution of the instance from $\boldsymbol{e}$. In other words, this paper has reduced the search-LWE problem to the integer programming problem.

The computational complexity of the derived integer programming problem is still unknown. In general, integer optimization problems are NP-hard, but IP solvers are relatively good at some type of integer programming problems.

Evaluating the computational complexity of the derived integer programming problem is a future work. Another future work is to investigate the applicability of the proposed method to the module LWE problem.

References

1. Albrecht, M.R., Cid, C., Faugère, J.C., Perret, L.: Algebraic algorithms for LWE. Cryptology ePrint Archive, Paper 2014/1018 (2014), `https://eprint.iacr.org/2014/1018`
2. Albrecht, M.R., Fitzpatrick, R., Göpfert, F.: On the efficacy of solving LWE by reduction to unique-SVP. In: Information Security and Cryptology–ICISC 2013: 16th International Conference, Seoul, Korea, November 27-29, 2013, Revised Selected Papers 16. pp. 293–310. Springer (2014)
3. Arora, S., Ge, R.: New algorithms for learning in presence of errors. In: International Colloquium on Automata, Languages, and Programming. pp. 403–415. Springer (2011)
4. Babai, L.: On lovász' lattice reduction and the nearest lattice point problem. Combinatorica **6**, 1–13 (1986)
5. Blum, A., Kalai, A., Wasserman, H.: Noise-tolerant learning, the parity problem, and the statistical query model. Journal of the ACM (JACM) **50**(4), 506–519 (2003)
6. Buchmann, J., Büscher, N., Göpfert, F., Katzenbeisser, S., Krämer, J., Micciancio, D., Siim, S., van Vredendaal, C., Walter, M.: Creating cryptographic challenges using multi-party computation: The LWE challenge. In: Proceedings of the 3rd ACM International Workshop on ASIA Public-Key Cryptography. pp. 11–20 (2016)
7. Ducas, L., Durmus, A., Lepoint, T., Lyubashevsky, V.: Lattice signatures and bimodal gaussians. In: Annual Cryptology Conference. pp. 40–56. Springer (2013)
8. Kawano, Y.: A reduction from an LWE problem to maximum independent set problems. Scientific Reports **13**(1), 7130 (2023)
9. Lenstra, A.K., Lenstra, H.W., Lovász, L.: Factoring polynomials with rational coefficients. Mathematische annalen **261**(ARTICLE), 515–534 (1982)

10. Lindner, R., Peikert, C.: Better key sizes (and attacks) for LWE-based encryption. In: Topics in Cryptology–CT-RSA 2011: The Cryptographers' Track at the RSA Conference 2011, San Francisco, CA, USA, February 14-18, 2011. Proceedings. pp. 319–339. Springer (2011)
11. Liu, M., Nguyen, P.Q.: Solving BDD by enumeration: An update. In: Cryptographers' Track at the RSA Conference. pp. 293–309. Springer (2013)
12. NIST: Post-quantum cryptography, https://csrc.nist.gov/projects/post-quantum-cryptography