Reduction of Search-LWE Problem to Integer Programming Problem

Masaaki Shirase

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

Abstract. Let \((A, t)\) be an instance of the search-LWE problem, where \(A\) is a matrix and \(t\) is a vector. This paper constructs an integer programming problem as Eq.(13) using \(A\) and \(t\), and shows that it is possible to derive a solution of the instance \((A, t)\) (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 \(b_1, b_2, \cdots, b_n\) 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 CRYSTALS-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 of integer components of \( \mathbb{R}^n \)
- \( \mathbb{Z}_p^n = \{0, 1, 2, \cdots, p-1\} \) 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
- \( \mathbf{e}_i \in \mathbb{R}^n \): unit vector with \( i \)-th component of 1, e.g., \( \mathbf{e}_1 = (1, 0, 0, \cdots, 0) \), \( \mathbf{e}_2 = (0, 1, 0, \cdots, 0) \)
- \( N(0, \sigma^2) \): the Gaussian distribution on \( \mathbb{Z}_p \) with a mean value of 0 and a standard deviation \( \sigma \)
- \( \mathbf{0}_n \in \mathbb{R}^n \): \( n \)-dimensional zero vector
- \( \| \mathbf{x} \| \): norm of \( \mathbf{x} \)
- \( \lfloor x \rfloor \): 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 \( \mathbf{v} = (v_1, v_2, \cdots, v_n) \) and \( \mathbf{w} = (w_1, w_2, \cdots, w_n) \in \mathbb{Z}^n \), we denote \( \mathbf{v} \equiv \mathbf{w} \) 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 \( L(b_1, b_2, \cdots, b_n) \) is set of linear combinations of integer coefficients of \( n \) (row) vectors \( b_1, b_2, \cdots, b_n \in \mathbb{R}^m \) that are linear independent.

\[
L(b_1, b_2, \cdots, b_n) = \left\{ \sum_{i=1}^{n} a_i b_i \in \mathbb{R}^m : a_i \in \mathbb{Z} \right\}
\]

Let \( B \) be a matrix consisting of \( b_1, b_2, \cdots, b_n \).

\[
B = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}
\]
Then, the lattice $L(b_1, b_2, \cdots, b_n)$ is also denoted as $L(B)$.

### 2.2 Search-LWE Problem

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

$$t \equiv sA + e,$$

where the components of $e$ are chosen according to $N(0, \sigma^2)$. The $e$ is called the noise vector or the error vector. Given $(A, t)$, the problem of finding $s$ 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 $e$ is chosen according to $N(0, \sigma^2)$, Pr[$\|e\| > 2\sqrt{m}\sigma]$ < $2^{-m+1}$ is satisfied [7]. Therefore, $\|e\|$ is usually a small value. Also, from Lemma 1 of [6] or Gaussian heuristic, the probability that an instance $(A, t)$ with $\|e\| \leq 2\sqrt{m}\sigma$ 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 $(A, t)$ of the LWE problem, construct a lattice $L'$ containing the lattice $L(A)$ generated by $A$ and $t$. Then, $e \in L'$ [2]. Since $e$ 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 $(A, t)$ of the LWE problem with the relation (1), a system of noise-free nonlinear equation with $s$ as its solution can be derived. The process uses the fact that if $-t \leq e_i \leq t$ for all $e_i$'s components of $e$, then each $e_i$ is a solution of a polynomial $P(x) = x \prod_{i=1}^{n} (x + i)(x - i)$. 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 \((A, t)\) be an instance of the LWE problem for a matrix \(A \in \mathbb{Z}_p^{n \times m}\), vectors \(s \in \mathbb{Z}_p^n\), \(e \in \mathbb{Z}_m^m\), and \(t \in \mathbb{R}^m\) 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 \(e\) (perhaps with high probability) using \(A\) and \(t\). Note that the solution \(s\) of the instance is easily obtained from a subset of the set of components of \(e\) as Remark 2 given later.

3.1 Partitioning of Matrix and Vectors

For \(A, t,\) and \(e\), define \(A_0, A_1, t_0, t_1, e_0\) and \(e_1\) as follows.

\[
A = (A_0 \ A_1),
\]
where

\[
\begin{align*}
A_0 &= n \times n \text{ matrix to the left of } A, \\
A_1 &= n \times (m - n) \text{ matrix to the right of } A.
\end{align*}
\]

\[
t = (t_0 \ t_1),
\]
where

\[
\begin{align*}
t_0 &= n \text{ dimensional vector to the left of } t, \\
t_1 &= (m - n) \text{ dimensional vector to the right of } t.
\end{align*}
\]

\[
e = (e_0 \ e_1),
\]
where

\[
\begin{align*}
e_0 &= n \text{ dimensional vector to the left of } e, \\
e_1 &= (m - n) \text{ dimensional vector to the right of } e.
\end{align*}
\]

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 \(t = (0, 1, 2, 3, 4)\), \(t_0 = (0, 1)\) and \(t_1 = (2, 3, 4)\). Then, Eq.(1) can be rewritten as

\[
t_0 \equiv sA_0 + e_0, \quad (2)
\]
\[
t_1 \equiv sA_1 + e_1. \quad (3)
\]

3.2 Maps \(\phi\) and \(\psi: \mathbb{R}^n \to \mathbb{R}^{m-n}\)

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

\[
A_0A_0^{-1} \equiv A_0^{-1}A_0 \equiv E_n. \quad (4)
\]

In fact, \(A_0^{-1}\) is the inverse matrix of \(A_0\) over finite field \(\mathbb{Z}_p\). Using \(A_0^{-1}, A_1, t_0\) and \(t_1\), define a map \(\phi: \mathbb{R}^n \to \mathbb{R}^{m-n}\) as follows.

\[
\phi : \mathbb{R}^n \to \mathbb{R}^{m-n}
\]
\[
v \mapsto vA_0^{-1}A_1 + t_1 - t_0A_0^{-1}A_1
\]

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

\[
\psi(v) = \phi(v) - \phi(0_n).
\]

The maps \(\phi\) and \(\psi\) have the following properties.

\footnote{It is equivalent to the determinant of \(A_0\) not being a multiple of \(p\).}
Proposition 1. (a) $\phi(e_0) \equiv e_1$.
(b) Assume $v_0 \in \mathbb{R}^n$ and $v_1 \in \mathbb{R}^{m-n}$ satisfies $\phi(v_0) \equiv v_1$. Let $\hat{s} \equiv (t_0 - v_0)A_0^{-1}$, then, $(t_0, t_1) = \hat{s}(A_0 A_1) + (v_0, v_1)$ holds.
(c) $\phi(0_n) = t_1 - t_0A_0^{-1}A_1$.
(d) $\psi(v) = vA_0^{-1}A_1$, that is, $\psi$ is a linear map.
(e) $\sum k_i(\phi(v_i) - \phi(0_n)) = \phi(\sum k_i v_i) - \phi(0_n)$ for $k_i \in \mathbb{Z}$.

Proof. (a) We compute $\phi(e_0) = e_0A_0^{-1}A_1 + t_1 - t_0A_0^{-1}A_1$
$\equiv (t_0 - sA_0)A_0^{-1}A_1 + t_1 - t_0A_0^{-1}A_1$ (from Eq.(2))
$= -sA_0A_0^{-1}A_1 + t_1$
$\equiv -sA_1 + t_1$ (from Eq.(4))
$\equiv e_1$. (from Eq.(3))

(b) From the definition of $\hat{s}$, we see
$\hat{s}A_0 + v_0 \equiv (t_0 - v_0)A_0^{-1}A_0 + v_0 \equiv t_0$.

In addition, from the assumption and the definition of $\phi$, we compute
$\hat{s}A_1 + v_1 \equiv (t_0 - v_0)A_0^{-1}A_1 + \phi(v_0)$
$= (t_0 - v_0)A_0^{-1}A_1 + (v_0A_0^{-1}A_1 + t_1 - t_0A_0^{-1}A_1)$
$\equiv t_1$.

(c) It is clear from the definition of $\phi$.

(d) We compute
$\psi(v) = \phi(v) - \phi(0_n)$
$= (vA_0^{-1}A_1 + t_1 - t_0A_0^{-1}A_1) - (t_1 - t_0A_0^{-1}A_1)$ (from (c))
$= vA_0^{-1}A_1$.

(e) From the linearity of $\psi$, we compute
$\text{Left side} = \sum k_i(\phi(v_i) - \phi(0_n))$
$= \sum k_i \psi(v_i)$
$= \psi(\sum k_i v_i)$
$= \phi(\sum k_i v_i) - \phi(0_n)$
$= \text{Right side}$.

Remark 2. Given an instance $(A, t)$ of the LWE problem, set $A_0, t_0, \text{ and } e_0$ as in Sect.3.1. Assume $A_0$ is regular on $\mathbb{Z}_p$. Then, we have
$s \equiv (t_0 - e_0)A_0^{-1}$
from Eq.(2). Thus, it is sufficient to obtain $e_0$ to solve the instance.
3.3 Construction of the Integer Programming Problem

If \( e = (e_1, e_2, \cdots, e_m) \) (\( e_i \in \mathbb{Z} \)), we can write \( e_0 \) and \( e_1 \) as

\[
\begin{align*}
\begin{cases}
e_0 &= (e_1, e_2, \cdots, e_n), \\
e_1 &= (e_{n+1}, e_{n+2}, \cdots, e_m).
\end{cases}
\end{align*}
\] (5)

In addition, we can write \( e_0 \) as

\[
\begin{align*}
e_0 &= e_1 e_1 + e_2 e_2 + \cdots + e_n e_n 
\end{align*}
\] (6)

with each unit vector \( e_i \).

For \( i = 1, 2, \cdots, n \), let \( w_i \) be

\[
w_i = \phi(e_i) - \phi(0_n) = \psi(e_i) \in \mathbb{R}^{m-n},
\] (7)

and the components of \( w_i \) be

\[
w_i = (w_{i,1}, w_{i,2}, \cdots, w_{i,m-n}) \quad (w_{i,j} \in \mathbb{Z}_p).
\] (8)

Furthermore, let

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

Then, we compute

\[
e_1 \equiv \phi(e_0) \quad \text{(from Proposition 1 (a))}
\]

\[
= \phi(e_1 e_1 + e_2 e_2 + \cdots + e_n e_n) \quad \text{(from Eq.(6))}
\]

\[
= \sum_{i=1}^{n} (e_i \phi(e_i) - \phi(0_n)) + \phi(0_n) \quad \text{(from Proposition 1 (e))}
\]

\[
= e_1 w_1 + e_2 w_2 + \cdots + e_n w_n + \phi(0_n). \quad \text{(from Eq.(7))}
\]

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

\[
e_{n+i} \equiv w_{1,i} e_1 + w_{2,i} e_2 + \cdots + w_{n,i} e_n + u_i
\] (10)

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

\[
\begin{align*}
w_{1,1} x_1 &+ w_{2,1} x_2 + \cdots + w_{n,1} x_n + u_1 = x_{n+1} \\
w_{1,2} x_1 &+ w_{2,2} x_2 + \cdots + w_{n,2} x_n + u_2 = x_{n+2} \\
&\vdots \\
w_{1,m-n} x_1 &+ w_{2,m-n} x_2 + \cdots + w_{n,m-n} x_n + u_{m-n} = x_m
\end{align*}
\] (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

\[
m \quad \text{(number of variables)} > m - n \quad \text{(number of equations)}.
\]
Then, let’s modify this system into an integer programming problem. The congruence equation (10) can be made into an integer equation

\[ w_{1,i}e_1 + w_{2,i}e_2 + \cdots + w_{n,i}e_n - e_{n+i} + pf_i = -u_i \]  

(12)

using some \( f_i \in \mathbb{Z} \).

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

\[-t \leq e_i \leq t \quad (i = 1, 2, \ldots, m)\]

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

\[-\left\lfloor \frac{t(np - n + 1) + p - 1}{p} \right\rfloor \leq f_i \leq \left\lfloor \frac{t(np - n + 1)}{p} \right\rfloor \quad (i = 1, 2, \ldots, m - n).\]

In addition, \( \|\mathbf{e}\| \) 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 \((A, t)\) of the LWE problem, where \( A \in \mathbb{Z}_p^{n \times m} \) (\( n < m \)) and \( t \in \mathbb{R}^m \). 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), \((u_1, u_2, \ldots, u_{m-n}) = t_1 - t_0 A_0^{-1}A_1\).

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

\[
W = \begin{pmatrix}
w_1 \\
w_2 \\
\vdots \\
w_n
\end{pmatrix}
\]

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

\[
W = \begin{pmatrix}
\psi(e_1) \\
\psi(e_2) \\
\vdots \\
\psi(e_n)
\end{pmatrix} \equiv \begin{pmatrix}
e_1A_0^{-1}A_1 \\
e_2A_0^{-1}A_1 \\
\vdots \\
e_nA_0^{-1}A_1
\end{pmatrix} \equiv E_nA_0^{-1}A_1 \equiv A_0^{-1}A_1.
\]

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

\((u_1, u_2, \ldots, u_{m-n}) = \phi(\theta_n) = t_1 - t_0 A_0^{-1}A_1.\) \(\square\)

The discussion so far gives the following proposition.
Proposition 2. Suppose we are given an instance $(A, t)$ of the LWE problem satisfying Eq.(1), where $A \in \mathbb{Z}_p^{n \times m}$ ($n < m$) and $t \in \mathbb{R}^m$. Set $A_0$ and $t_0$ as in Sect.3.1. Assume $A_0$ is regular over $\mathbb{Z}_p$. 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.

\[
\begin{align*}
&\text{minimize:} \\
&\quad x_1^2 + x_2^2 + \cdots + x_m^2 \\
&\text{subject to:} \\
&\quad w_{1,1}x_1 + w_{2,1}x_2 + \cdots + w_{n,1}x_n - x_{n+1} + py_1 = -u_1 \\
&\quad w_{1,2}x_1 + w_{2,2}x_2 + \cdots + w_{n,2}x_n - x_{n+2} + py_2 = -u_2 \\
&\quad \vdots \\
&\quad w_{1,m-n}x_1 + w_{2,m-n}x_2 + \cdots + w_{n,m-n}x_n - x_n + py_{m-n} = -u_{m-n} \\
&\quad -t \leq x_i \leq t \\
&\quad -\lfloor (t(p^n - n + 1) + p^i - 1) / p \rfloor \leq f_i \leq \lfloor (t(p^n - n + 1) + p^i - 1) / p \rfloor \quad (i = 1, 2, \cdots, m - n) \\
&\quad x_i, y_j \in \mathbb{Z} \quad (i = 0, 1, \cdots, n, j = 1, 2, \cdots, m - n)
\end{align*}
\]

(13)

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

\[
\hat{s} = (t_0 - x_0)A_0^{-1}
\]

(14)

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

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

\[
t = \hat{s}A + \hat{x} \quad \text{that implies} \quad t_0 = \hat{s}A_0 + \hat{x}_0.
\]

The solution $s = (s_0, s_1)$ of the instance $(A, t)$ satisfies

\[
t = sA + e \quad \text{that implies} \quad t_0 = s_0A + e_0.
\]

If $\|\hat{x}\|$ is small enough, then $\hat{x} = e$ that implies $\hat{x}_0 = e_0$ with high probability from Remark 1. In this case, we see

\[
\hat{s}A_0 = sA_0 \\
\hat{s} \equiv sA_0A_0^{-1} \equiv s,
\]

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

Remark 3. For $t \in \mathbb{N}$ selected in Proposition 2, if $t$ is too small such that $-t \leq e_i \leq t$ 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 \( s \), while the proposed method derives an integer programming problem such that the optimal solution or a tentative solution with small norm is \( e \) 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 \((A, t)\) of the search-LWE problem with the relation \( t \equiv sA + e \pmod{p} \) such that one of its solutions is equal to \( e \) 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 \( e \) with high probability. We has been able to make a solution of the instance from \( e \). 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

