Solving Trapdoor Basis of Principal Ideal Lattice from Public Basis

Yupu Hu, Zhizhu Lian, and Jiangshan Chen

ISN Laboratory, Xidian University, 710071 Xi'an, China
yphu@mail.xidian.edu.cn lzz600@126.com js_chen@mnnu.edu.cn

Abstract. In this paper we present two new attacks on cryptosystems based on principal ideal lattices.
First, we show that, if there is one polynomially large entry in the transformation matrix from trapdoor basis to public basis, we can obtain the trapdoor basis with high probability. Our attack is quite simple, and rarely needs to use any lattice-reduction tools. The key point is that some class of matrices satisfies multiplication commutative law. We use multiplication commutative law to obtain a linear equation of integer variables, and find it not difficult to be solved as long as its rank is larger than half of its number of variables.
Second, we show that, if each entry of the trapdoor basis is polynomially large, we can obtain the trapdoor basis with high probability. This attack is a modified version, and we don't care whether each entry of its transformation matrix is super-polynomially large. The key point is that we can obtain many vectors of the inverse ideal, and we can reduce each of these vectors into polynomially large multiple of its generator.

Keywords: Cryptosystems based on ideal lattices, Trapdoor basis, Public basis.

1 Introduction

Cryptosystems based on lattices are important "post quantum cryptosystems". From them the most useful are those based on ideal lattices, where multiplication operation makes many novel applications possible, for example, fully homomorphic encryption (FHE) [1]. The ideal lattice has a trapdoor basis which is hidden by the user, and a public basis which is published. The transformation matrix from trapdoor basis to public basis is a unimodular matrix, that is, both itself and its inverse matrix are integer matrices. Such transformation matrix is also hidden. One security background of these cryptosystems is the hardness of Short Generator of a Principal Ideal Problem(SG-PIP), introduced in [4].

How large should the transformation matrix be to protect the trapdoor basis (That is, how large should its entries be)? Up to now there has been no clear answer to this question. The common view is that polynomially large entries of the transformation matrix seems OK, and no security weakness has been found. For the special cases of ideal lattices, Hermite normal form (HNF) is "a good choice

for the public lattice basis" (Chapter 6 of [1]), which has super-polynomially large transformation matrix. However polynomially large transformation matrix has never been negated for ideal lattices. On the other hand, it is a general case for principal ideal lattice that each entry of the trapdoor basis is polynomially large.

In this paper we show that SG-PIP is not hard under some conditions. Move detailedly we present two new attacks on cryptosystems based on principal ideal lattices.

Attack (1). We show that, if there is one polynomially large entry in the transformation matrix from trapdoor basis to public basis, we can obtain the trapdoor basis with high probability. Our attack is quite simple, and rarely needs to use any lattice-reduction tools. The key point is that some class of matrices satisfies multiplication commutative law. We use multiplication commutative law to obtain a linear equation of integer variables, and find it not difficult to be solved as long as its rank is larger than half of its number of variables.

Attack (2). We show that, if each entry of the trapdoor basis is polynomially large, we can obtain the trapdoor basis with high probability. This attack is a modified version, and we don't care whether each entry of its transformation matrix is super-polynomially large. The key point is that we can obtain many vectors of the inverse ideal, and we can reduce each of these vectors into polynomially large multiple of its generator.

2 Preliminaries

2.1 Notations and Definitions

We denote the rational numbers by $\mathbb{Q}$ and the integers by $\mathbb{Z}$. We specify that n-dimensional vectors of $\mathbb{Q}^n$ and $\mathbb{Z}^n$ are row vectors. We take $\mathbb{Q}^{n\times n}$ and $\mathbb{Z}^{n\times n}$ as $n\times n$ matrices. A matrix $\mathbf{U} \in \mathbb{Z}^{n\times n}$ is called a unimodular matrix if $\mathbf{U}^{-1} \in \mathbb{Z}^{n\times n}$. In this case the determinant of $\mathbf{U}$ is ± 1.

We consider the polynomial ring $R = \mathbb{Z}[X]/(X^n+1)$, and identify an element $\mathbf{u} \in R$ with the coefficient vector of the degree-$(n-1)$ integer polynomial that represents $\mathbf{u}$. In this way, R is identified with the integer lattice $\mathbb{Z}^n$. Addition in this ring is done component-wise in their coefficients, and multiplication is polynomial multiplication modulo the ring polynomial $X^n + 1$. Similarly, we consider the polynomial ring $\mathbb{Q}[X]/(X^n + 1)$.

For $\mathbf{x} \in R$,$\langle \mathbf{x} \rangle = \{\mathbf{x} \times \mathbf{u} : \mathbf{u} \in R\}$ is the principal ideal in R generated by $\mathbf{x}$ (alternatively, the sub-lattice of $\mathbb{Z}^n$ corresponding to this ideal).

We redefine the operation "mod q" as follows: if q is an odd, $a(\mathrm{mod}\ q)$ is within $\{-(q-1)/2, -(q-3)/2, \ldots, (q-1)/2\}$; if q is an even, $a(\mathrm{mod}\ q)$ is within $\{-q/2, -(q-2)/2, \ldots, (q-2)/2\}$.

2.2 A Class of Matrices and Its Multiplication Commutative Law

Suppose $\mathbb{X} \subset \mathbb{Q}^{n\times n}$ is a class of such matrices:

$$\begin{bmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ -a_{n-1} & a_0 & \cdots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ -a_1 & -a_2 & \cdots & a_0 \end{bmatrix},$$

where each entry $a_i \in \mathbb{Q}$.

$\{\mathbb{X}, +, \cdot\}$ is a ring. If $\mathbf{X} \in \mathbb{X}$, $\mathbf{X}^{-1} \in \mathbb{X}$. More important is that $\mathbb{X}$ satisfies multiplication commutative law, namely, for $\mathbf{A}, \mathbf{B} \in \mathbb{X}$, we have $\mathbf{A} \cdot \mathbf{B} = \mathbf{B} \cdot \mathbf{A}$. In fact $\{\mathbb{X}, +, \cdot\}$ is a ring-isomorphism of $\mathbb{Q}[X]/(X^n + 1)$.

2.3 Principal Ideal Lattice and Its {Trapdoor Basis, Public Basis}

The user randomly chooses a vector $\mathbf{b} = (b_0, b_1, \cdots, b_{n-1}) \in \mathbb{Z}^n$. Then the trapdoor basis of the ideal lattice is the matrix

$$\mathbf{B}^{Trap} = \begin{bmatrix} b_0 & b_1 & \cdots & b_{n-1} \\ -b_{n-1} & b_0 & \cdots & b_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ -b_1 & -b_2 & \cdots & b_0 \end{bmatrix} \in \mathbb{X} \cap \mathbb{Z}^{n\times n}.$$

In other words, the ideal lattice is the principal ideal $\langle \mathbf{b} \rangle$. Then the user takes a unimodular matrix $\mathbf{U} \in \mathbb{Z}^{n\times n}$, and computes the public basis

$$\mathbf{B}^{Pub} = \mathbf{U} \cdot \mathbf{B}^{Trap}.$$

He publishes $\mathbf{B}^{Pub}$ and hides $\{\mathbf{U}, \mathbf{B}^{Trap}\}$.

3 Description of Our Attack (1)

Suppose there is one polynomially large entry in $\mathbf{U}$. Our knowledge is the public basis $\mathbf{B}^{Pub}$, and we want to obtain a trapdoor basis. This trapdoor basis may not be $\mathbf{B}^{Trap}$, but it should be at least as good as or even better than $\mathbf{B}^{Trap}$, with same or smaller size.

3.1 Step 1: Obtaining a Linear Equation of the Unimodular Matrix

First, we take a matrix $\mathbf{C} \in \mathbb{X} \cap \mathbb{Z}^{n\times n}$. To make our attack successful, $\mathbf{C}$ should be sufficiently large. For example, we can take the absolute value of each entry of $\mathbf{C}$ larger than the maximum absolute value of entries of $\mathbf{B}^{Pub}$.

Second, we compute matrix $\mathbf{D} = \mathbf{B}^{Pub} \cdot \mathbf{C} \cdot (\mathbf{B}^{Pub})^{-1} \in \mathbb{Q}^{n\times n}$. By considering Multiplication Commutative Law, we have

$$\mathbf{D} = \mathbf{U} \cdot \mathbf{B}^{Trap} \cdot \mathbf{C} \cdot (\mathbf{B}^{Trap})^{-1} \cdot \mathbf{U}^{-1} = \mathbf{U} \cdot \mathbf{C} \cdot \mathbf{U}^{-1} \in \mathbb{Z}^{n\times n},$$

where $\mathbf{B}^{Trap}$ disappears, and unknown variables are only entries of $\mathbf{U}$.

Finally, we obtain a linear equation of $\mathbf{U}$:

$$\mathbf{U} \cdot \mathbf{C} - \mathbf{D} \cdot \mathbf{U} = \mathbf{O}, \tag{3.1}$$

where $\mathbf{O} \in \mathbb{Z}^{n \times n}$ is null matrix.

True value of $\mathbf{U}$ is one solution of equation (3.1), so that equation (3.1) has a reduced rank. If the rank is $n^2 - 1$, then the thing tends simple. We can search all possible values of one entry of $\mathbf{U}$, under the assumption that this entry is polynomially large. For each possible value of this entry, we obtain unique value of $\mathbf{U}$. However, we find it is almost sure that the rank of equation (3.1) is far smaller than $n^2 - 1$. To continue our attack, we need three assumptions.

3.2 Step 2: Obtaining and Solving Another Linear Equation Modular Some Integer

Assumption 1: The rank of equation (3.1) is larger than $n^2/2$.

Our experiments show that Assumption 1 can be easily satisfied. If Assumption 1 doesn't hold, we can take another matrix $\mathbf{C} \in \mathbb{X} \cap \mathbb{Z}^{n \times n}$, and compute another $\mathbf{D}$. Now suppose the rank of equation (3.1) is r, and $r > n^2/2$. We denote

$$\mathbf{U} = \begin{bmatrix} u_1 & u_2 & \cdots & u_n \\ u_{n+1} & u_{n+2} & \cdots & u_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ u_{n(n-1)+1} & u_{n(n-1)+2} & \cdots & u_{n^2} \end{bmatrix}.$$

Suppose true value of u_{n^2} is polynomially large.

First, we convert equation (3.1) into the following form:

$$(u_1, u_2, \ldots, u_r) = (u_{r+1}, u_{r+2}, \ldots, u_{n^2})\mathbf{G}, \tag{3.2}$$

where each entry of $\mathbf{G}$ is from $\mathbb{Q}$.

Second, we take g_0 as the smallest common denominator of entries of $\mathbf{G}$, and take $\mathbf{G}^{(0)} = g_0\mathbf{G}$, so that $\mathbf{G}^{(0)}$ is an integer matrix. Because $u_1, u_2, \ldots, u_r$ are integers, each entry of

$$(u_{r+1}, u_{r+2}, \ldots, u_{n^2})\mathbf{G}^{(0)}$$

must be a multiple of g_0.

Finally, we solve the linear equation modular g_0,

$$(u_{r+1}, u_{r+2}, \ldots, u_{n^2})\mathbf{G}^{(0)} \pmod{g_0} = (0, 0, \ldots, 0). \tag{3.3}$$

True value of $(u_{r+1}, u_{r+2}, \ldots, u_{n^2})$ is one solution of equation (3.3). $\mathbf{G}^{(0)}$ has $n^2 - r$ rows and r columns. We know that equation (3.3) has a reduced rank, that is, the rank is smaller than $n^2 - r$. Here we need another assumption as the follow.

Assumption 2 The rank of equation (3.3) is $n^2 - r - 1$.

According to Assumption 1, r is larger than $n^2 - r$, so it seems that Assumption 2 can be easily satisfied. By searching all possible values of u_{n^2}, we obtain all possible mod g_0 values of $(u_{r+1}, u_{r+2}, \ldots, u_{n^2})$. We need Assumption 3 as the follow.

Assumption 3 True values of $\{u_{r+1}, u_{r+2}, \ldots, u_{n^2}\}$ are all within the interval $(-g_0/2, g_0/2)$.

Assumption 3 can be easily satisfied if we take $\mathbf{C}$ sufficiently large. For example if we find g_0 larger than any entry of $\mathbf{B}^{Pub}$, then the condition is satisfied with high probability. Assumption 2 and Assumption 3 mean that, if u_{n^2} is true value, then $\{u_{r+1}, u_{r+2}, \ldots, u_{n^2-1}\}$ obtained from equation (3.3) are true values, and mod g_0 operation is not working.

3.3 Step 3: Searching a Qualified Trapdoor Basis

We search polynomially many values of u_{n^2}, and obtain corresponding values of $\{u_{r+1}, u_{r+2}, \ldots, u_{n^2-1}\}$ by solving equation (3.3), then obtain corresponding solution $\{u_1, u_2, \ldots, u_r\}$ of equation (3.2).

For each value of $(u_1, u_2, \ldots, u_{n^2})$, we make following 2 checks:

- whether $\det(\mathbf{U}) = \pm 1$, and
- whether $\mathbf{U}^{-1} \cdot \mathbf{B}^{Pub} \in \mathbb{X}$.

Whenever $(u_1, u_2, \ldots, u_{n^2})$ passes these checks, each row of $\mathbf{U}^{-1} \cdot \mathbf{B}^{Pub}$ is a generator of the principal ideal $\langle \mathbf{b} \rangle$. Finally we obtain several generators. These generators include true value of $\mathbf{b}$, and the number of these generators is polynomially large. Form them, we choose one with the smallest size, then we have obtained a qualified trapdoor basis. The cryptosystem has been broken.

A note: a principal ideal may have a lot of generators [4], but they do not affect our attack.

4 Some Details of Our Attack (1)

4.1 Shape and Rank of Coefficient-Matrix of Equation (3.1)

Denote

$$\mathbf{D} = \begin{bmatrix} d_{11} & d_{12} & \ldots & d_{1n} \\ d_{21} & d_{22} & \ldots & d_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ d_{n1} & d_{n2} & \ldots & d_{nn} \end{bmatrix},$$

and rewrite equation (3.1) into the form

$$(u_1, u_2, \ldots, u_{n^2})\mathbf{J} = (0, 0, \ldots, 0),$$

where

$$\mathbf{J} = \begin{bmatrix} d_{11} & & d_{21} & & & d_{n1} & \\ & \ddots & & \ddots & \cdots & & \ddots \\ & d_{11} & & d_{21} & & & d_{n1} \\ d_{12} & & d_{22} & & & d_{n2} & \\ & \ddots & & \ddots & \cdots & & \ddots \\ & d_{12} & & d_{22} & & & d_{n2} \\ \vdots & & \vdots & & \ddots & \vdots & \\ d_{1n} & & d_{2n} & & & d_{nn} & \\ & \ddots & & \ddots & \cdots & & \ddots \\ & d_{1n} & & d_{2n} & & & d_{nn} \end{bmatrix} - \begin{bmatrix} \mathbf{C} & & & \\ & \mathbf{C} & & \\ & & \ddots & \\ & & & \mathbf{C} \end{bmatrix}.$$

Denote

$$\mathbf{J} = \begin{bmatrix} \mathbf{J}_{11} & \mathbf{J}_{12} & \dots & \mathbf{J}_{1n} \\ \mathbf{J}_{21} & \mathbf{J}_{22} & \dots & \mathbf{J}_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{J}_{n1} & \mathbf{J}_{n2} & \dots & \mathbf{J}_{nn} \end{bmatrix},$$

where each sub-matrix $\mathbf{J}_{ij} \in \mathbb{X} \cap \mathbb{Z}^{n \times n}$.

Lemma 1. *Suppose n is a power of 2. Then the rank of equation (3.1) is multiple of n. Therefore the rank is at most $n^2 - n$.*

Lemma 1 is clear. By considering that $\{\mathbb{X}, +, \cdot\}$ is a field in this case, we can use Gauss Elimination over $\mathbb{X}$ rather than over real numbers.

4.2 Our Experiments

If we take $\mathbf{C} = a\mathbf{I}$ as the multiple of the unit matrix, equation (3.1) has the rank 0. Of course there are many other cases in which the ranks of equation (3.1) are non-larger than $n^2/2$. But our experiments show that, with very high probability, equation (3.1) has the rank $n^2 - n$. Appendix presents 25 examples, for $n = 3, 4, 5, 6, 7$ respectively.

5 Description of Our Attack (2)

5.1 Our observation and Preparation

Suppose each entry of $\mathbf{b}$ is polynomially large, Then we arbitrarily choose n vectors $\{\mathbf{t}^{(1)}, \mathbf{t}^{(2)}, \dots, \mathbf{t}^{(n)}\}$ from $\langle \mathbf{b}^{-1} \rangle$ (we know it is an easy task [3]).

We take (mod 1) operation as follows:

$$\{\mathbf{t}^{(1)}, \mathbf{t}^{(2)}, \dots, \mathbf{t}^{(n)}\} (\text{mod } 1) = \{\mathbf{t}^{*(1)}, \mathbf{t}^{*(2)}, \dots, \mathbf{t}^{*(n)}\}$$

We know that $\{\mathbf{t}^{*(1)}, \mathbf{t}^{*(2)}, \ldots, \mathbf{t}^{*(n)}\}$ are still vectors of $\langle \mathbf{b}^{-1} \rangle$, and that each entry of each vector from $\{\mathbf{t}^{*(1)}, \mathbf{t}^{*(2)}, \ldots, \mathbf{t}^{*(n)}\}$ is within the interval $[-0.5, 0.5)$.

Suppose $\mathbf{t}^{*(i)} = \mathbf{u}^{*(i)} \times \mathbf{b}^{-1}$, where $\mathbf{u}^{*(i)} \in \mathbb{Z}^n$, $i = 1, 2, \ldots, n$. Then $\mathbf{u}^{*(i)} = \mathbf{t}^{*(i)} \times \mathbf{b}$, and

$$\| \mathbf{u}^{*(i)} \| \leq \sqrt{n} \| \mathbf{t}^{*(i)} \| \cdot \| \mathbf{b} \| \leq \frac{n}{2} \| \mathbf{b} \| .$$

This inequality means that, for $i = 1, 2, \ldots, n$, each entry of $\mathbf{u}^{*(i)}$ is at most polynomially large.

Take the first row $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ of matrix $\mathbf{B}^{Pub}$. We know that

$$(\alpha_1, \alpha_2, \ldots, \alpha_n) = (u_1, u_2, \ldots, u_n) \times \mathbf{b},$$

where $(u_1, u_2, \ldots, u_n) \in \mathbb{Z}^n$ is the first row of $\mathbf{U}$.

Take the matrix

$$\mathbf{B}^{*Pub} = \begin{bmatrix} (\alpha_1, \alpha_2, \ldots, \alpha_n) \times \mathbf{t}^{*(1)} \\ (\alpha_1, \alpha_2, \ldots, \alpha_n) \times \mathbf{t}^{*(2)} \\ \vdots \\ (\alpha_1, \alpha_2, \ldots, \alpha_n) \times \mathbf{t}^{*(n)} \end{bmatrix},$$

then

$$\mathbf{B}^{*Pub} = \begin{bmatrix} \mathbf{u}^{*(1)} \\ \mathbf{u}^{*(2)} \\ \vdots \\ \mathbf{u}^{*(n)} \end{bmatrix} \cdot \begin{bmatrix} u_1 & u_2 & \cdots & u_n \\ -u_n & u_1 & \cdots & u_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ -u_2 & -u_3 & \cdots & u_1 \end{bmatrix}.$$

We denote

$$\mathbf{U}^* = \begin{bmatrix} \mathbf{u}^{*(1)} \\ \mathbf{u}^{*(2)} \\ \vdots \\ \mathbf{u}^{*(n)} \end{bmatrix}, \quad \mathbf{B}^{*Trap} = \begin{bmatrix} u_1 & u_2 & \cdots & u_n \\ -u_n & u_1 & \cdots & u_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ -u_2 & -u_3 & \cdots & u_1 \end{bmatrix}.$$

therefore we have

$$\mathbf{B}^{*Pub} = \mathbf{U}^* \cdot \mathbf{B}^{*Trap},$$

where $\mathbf{B}^{*Trap} \in \mathbb{X} \cap \mathbb{Z}^{n \times n}$. $\mathbf{B}^{*Pub}$ is public, while $\{\mathbf{U}^*, \mathbf{B}^{*Trap}\}$ are hidden. The relation of $\{\mathbf{B}^{*Pub}, \mathbf{U}^*, \mathbf{B}^{*Trap}\}$ is somewhat like the relation of $\{\mathbf{B}^{Pub}, \mathbf{U}, \mathbf{B}^{Trap}\}$, so that a similar attack can be easily constructed. In fact $\{\mathbf{B}^{*Pub}, \mathbf{U}^*, \mathbf{B}^{*Trap}\}$ are quite suitable for our attack, because each entry of $\mathbf{U}^*$ is at most polynomially large. There is one difference that $\mathbf{U}^*$ is not a unimodular matrix, so that we need a modified version of checking procedure.

5.2 Procedure of Our Attack (2)

We take $\mathbf{C}^* \in \mathbb{X} \cap \mathbb{Z}^{n \times n}$, where $\mathbf{C}^*$ should be sufficiently large. Then we compute $\mathbf{D}^* = \mathbf{B}^{*Pub} \cdot \mathbf{C}^* \cdot (\mathbf{B}^{*Pub})^{-1} \in \mathbb{Q}^{n \times n}$ ($\mathbf{D}^* \notin \mathbb{Z}^{n \times n}$), and by considering

Multiplication Commutative Law, we have $\mathbf{D}^* = \mathbf{U}^* \cdot \mathbf{C}^* \cdot \mathbf{U}^{*-1}$. Then we obtain a linear equation of $\mathbf{U}^*$:

$$\mathbf{U}^* \cdot \mathbf{C}^* - \mathbf{D}^* \cdot \mathbf{U}^* = \mathbf{O}. \tag{5.1}$$

True value of $\mathbf{U}^*$ is one solution of equation (5.1), so that equation (5.1) has a reduced rank. Suppose the rank of equation (5.1) is r, and $r > n^2/2$. We denote

$$\mathbf{U}^* = \begin{bmatrix} u_1^* & u_2^* & \cdots & u_n^* \\ u_{n+1}^* & u_{n+2}^* & \cdots & u_{2n}^* \\ \vdots & \vdots & \ddots & \vdots \\ u_{n(n-1)+1}^* & u_{n(n-1)+2}^* & \cdots & u_{n^2}^* \end{bmatrix}.$$

Then we convert equation (5.1) into the following form:

$$(u_1^*, u_2^*, \ldots, u_r^*) = (u_{r+1}^*, u_{r+2}^*, \ldots, u_{n^2}^*)\mathbf{G}^*, \tag{5.2}$$

where each entry of $\mathbf{G}^*$ is from $\mathbb{Q}$. Then we take g_0^* as the smallest common denominator of entries of $\mathbf{G}^*$, and take $\mathbf{G}^{*(0)} = g_0^*\mathbf{G}^*$, so that $\mathbf{G}^{*(0)}$ is an integer matrix. Because $u_1^*, u_2^*, \ldots, u_{n(n-1)}^*$ are integers, each entry of

$$(u_{r+1}^*, u_{r+2}^*, \ldots, u_{n^2}^*)\mathbf{G}^{*(0)}$$

must be a multiple of g_0^*. Then we solve the linear equation modular g_0^*,

$$(u_{r+1}^*, u_{r+2}^*, \ldots, u_{n^2}^*)\mathbf{G}^{*(0)} \pmod{g_0^*} = (0, 0, \ldots, 0). \tag{5.3}$$

True value of $(u_{r+1}^*, u_{r+2}^*, \ldots, u_{n^2}^*)$ is one solution of equation (5.3). $\mathbf{G}^{*(0)}$ has $n^2 - r$ rows and r columns, $r > n^2 - r$. Then we assume that the rank of equation (5.3) is $n^2 - r - 1$, which can be easily satisfied. By searching all possible values of $u_{n^2}^*$ ($u_{n^2}^*$ is at most polynomially large), we obtain all possible mod g_0^* values of $(u_{r+1}^*, u_{r+2}^*, \ldots, u_{n^2}^*)$. Then we assume that true values of $\{u_{r+1}^*, u_{r+2}^*, \ldots, u_{n^2}^*\}$ are all within the interval $(-g_0^*/2, g_0^*/2)$, which is almost sure to be satisfied because each of true values of $\{u_{r+1}^*, u_{r+2}^*, \ldots, u_{n^2}^*\}$ is at most polynomially large.

For each possible value of $(u_{r+1}^*, u_{r+2}^*, \ldots, u_{n^2}^*)$, we obtain corresponding solution $\{u_1^*, u_2^*, \ldots, u_r^*\}$ of equation (5.2).

For each value of $(u_1^*, u_2^*, \ldots, u_{n^2}^*)$ (that is , for each value of $\mathbf{U}^*$), we make the following check:

• whether $\mathbf{U}^{*-1} \cdot \mathbf{B}^{*Pub} \in \mathbb{X} \cap \mathbb{Z}^{n \times n}$.

If it passes this check, we denote

$$\mathbf{U}^{*-1} \cdot \mathbf{B}^{*Pub} = \begin{bmatrix} u_1 & u_2 & \cdots & u_n \\ -u_n & u_1 & \cdots & u_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ -u_2 & -u_3 & \cdots & u_1 \end{bmatrix},$$

denote $(b_0, b_1, \ldots, b_{n-1}) = (u_1, u_2, \ldots, u_n)^{-1} \times (\alpha_1, \alpha_2, \ldots, \alpha_n)$, and check

- whether $(b_0, b_1, \ldots, b_{n-1}) \in \mathbb{Z}^n$, and
- whether

$$\mathbf{B}^{Pub} \cdot \begin{bmatrix} b_0 & b_1 & \cdots & b_{n-1} \\ -b_{n-1} & b_0 & \cdots & b_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ -b_1 & -b_2 & \cdots & b_0 \end{bmatrix}^{-1}$$

is a unimodular matrix.

If it passes these two checks, then such vector $(b_0, b_1, \ldots, b_{n-1})$ is a generator of the principal ideal. Finally we obtain several generators. These generators include true value of $\mathbf{b}$, and the number of these generators is polynomially large. Form them, we choose one with the smallest size, then we have obtained a qualified trapdoor basis.

6 Impact of Our Attacks

Our attacks greatly reduce the security background of cryptosystems based on principal ideal lattices. To resist our attacks, the system must prove that

- each entry of transformation matrix is super-polynomially large, and
- for arbitrarily chosen vector from the inverse ideal, it is negligible that some entry of multiple vector is polynomially large.

References

1. Gentry, C.: A fully homomorphic encryption scheme. PhD thesis, Stanford University, 2009. http://crypto.stanford.edu/craig.
2. Cramer R., Ducas L.,Peikert C., Regev O.: Recovering Short Generators of Principal Ideals in Cyclotomic Rings. In: Fischlin M., Coron J.-S.(eds) Eurocrypt 2016. LNCS, vol. 9666, pp 559–585. Springer, Heidelberg(2016)
3. Garg, S., Gentry, C., Halevi, S.: Candidate Multilinear Maps from Ideal Lattices. In: Johansson, T., Nguyen, P.Q. (ed.) EUROCRYPT 2013. LNCS, vol. 7881, pp. 181–184. Springer, Heidelberg (2013)
4. Cramer R., Ducas L., Peikert C., Regev O.: Recovering short generators of principal ideals in cyclotomic rings. In: Fischlin M., Coron J.-S (Ends.): EUROCRYPT 2016, Part II, LNCS 9666, pp. 559-585. Springer, Heidelberg (2016)

Appendix

Our experiments show that, with very high probability, equation (3.1) has the rank $n^2 - n$. Here we present 25 examples, for $n = 3, 4, 5, 6, 7$ respectively.

Example 1. Take $n = 3$,

$$\mathbf{U} = \begin{bmatrix} 29 & 10 & 1 \\ 11 & 11 & 2 \\ 32 & 15 & 2 \end{bmatrix}, \mathbf{C} = \begin{bmatrix} 8 & 9 & 3 \\ -3 & 8 & 9 \\ -9 & -3 & 8 \end{bmatrix} \in \mathbb{X} \cap \mathbb{Z}^{3\times 3}.$$

Then

$$\mathbf{D} = \begin{bmatrix} -21943 & -13452 & 24516 \\ -20370 & -12499 & 22758 \\ -30849 & -18918 & 34466 \end{bmatrix},$$

and we have the rank of equation (3.1) is $6 = 3^2 - 3 > 3^2/2$.

Example 2. Take $n = 3$,

$$\mathbf{U} = \begin{bmatrix} 13 & 4 & 4 \\ 14 & 5 & 4 \\ 16 & 5 & 5 \end{bmatrix}, \mathbf{C} = \begin{bmatrix} 4 & 7 & 0 \\ 0 & 4 & 7 \\ -7 & 0 & 4 \end{bmatrix} \in \mathbb{X} \cap \mathbb{Z}^{3\times 3}.$$

Then

$$\mathbf{D} = \begin{bmatrix} -962 & 63 & 728 \\ -1078 & 67 & 819 \\ -1197 & 77 & 907 \end{bmatrix},$$

and we have the rank of equation (3.1) is $6 = 3^2 - 3 > 3^2/2$.

Example 3. Take $n = 3$,

$$\mathbf{U} = \begin{bmatrix} 9 & 4 & 1 \\ 21 & 5 & 4 \\ 14 & 5 & 2 \end{bmatrix}, \mathbf{C} = \begin{bmatrix} 1 & 3 & 8 \\ -8 & 1 & 3 \\ -3 & -8 & 1 \end{bmatrix} \in \mathbb{X} \cap \mathbb{Z}^{3\times 3}.$$

Then

$$\mathbf{D} = \begin{bmatrix} 3557 & 1105 & -3946 \\ 7359 & 2294 & -8174 \\ 5269 & 1639 & -5848 \end{bmatrix},$$

and we have the rank of equation (3.1) is $6 = 3^2 - 3 > 3^2/2$.

Example 4. Take $n = 3$,

$$\mathbf{U} = \begin{bmatrix} 17 & 7 & 3 \\ 9 & 3 & 2 \\ 21 & 8 & 4 \end{bmatrix}, \mathbf{C} = \begin{bmatrix} 8 & 9 & 8 \\ -8 & 8 & 9 \\ -9 & -8 & 8 \end{bmatrix} \in \mathbb{X} \cap \mathbb{Z}^{3\times 3}.$$

Then

$$\mathbf{D} = \begin{bmatrix} 2905 & 3166 & -3706 \\ 1449 & 1590 & -1853 \\ 3502 & 3825 & -4471 \end{bmatrix},$$

and we have the rank of equation (3.1) is $6 = 3^2 - 3 > 3^2/2$.

Example 5. Take $n = 3$,

$$\mathbf{U} = \begin{bmatrix} 7 & 21 & 4 \\ 6 & 21 & 4 \\ 8 & 26 & 5 \end{bmatrix}, \mathbf{C} = \begin{bmatrix} 7 & 1 & 2 \\ -2 & 7 & 1 \\ -1 & -2 & 7 \end{bmatrix} \in \mathbb{X} \cap \mathbb{Z}^{3\times 3}.$$

Then

$$\mathbf{D} = \begin{bmatrix} -461 & -447 & 739 \\ -446 & -415 & 701 \\ -565 & -537 & 897 \end{bmatrix},$$

and we have the rank of equation (3.1) is $6 = 3^2 - 3 > 3^2/2$.

Example 6. Take $n = 4$,

$$\mathbf{U} = \begin{bmatrix} 34 & 17 & 11 & 4 \\ 19 & 11 & 9 & 4 \\ 10 & 6 & 5 & 2 \\ 37 & 19 & 13 & 5 \end{bmatrix}, \mathbf{C} = \begin{bmatrix} 3 & 7 & 1 & 3 \\ -3 & 3 & 7 & 1 \\ -1 & -3 & 3 & 7 \\ -7 & -1 & -3 & 3 \end{bmatrix} \in \mathbb{X} \cap \mathbb{Z}^{4\times 4}.$$

Then

$$\mathbf{D} = \begin{bmatrix} 4176 & 2132 & -562 & -4780 \\ 2278 & 1216 & -374 & -2617 \\ 1168 & 628 & -196 & -1343 \\ 4526 & 2330 & -634 & -5184 \end{bmatrix},$$

and we have the rank of equation (3.1) is $12 = 4^2 - 4 > 4^2/2$.

Example 7. Take $n = 4$,

$$\mathbf{U} = \begin{bmatrix} 17 & 30 & 19 & 4 \\ 9 & 19 & 7 & 1 \\ 5 & 14 & 13 & 3 \\ 18 & 33 & 23 & 5 \end{bmatrix}, \mathbf{C} = \begin{bmatrix} 3 & 5 & 7 & 5 \\ -5 & 3 & 5 & 7 \\ -7 & -5 & 3 & 5 \\ -5 & -7 & -5 & 3 \end{bmatrix} \in \mathbb{X} \cap \mathbb{Z}^{4\times 4}.$$

Then

$$\mathbf{D} = \begin{bmatrix} -222396 & 31642 & -69942 & 213634 \\ -118822 & 16908 & -37368 & 114140 \\ -111854 & 15915 & -35174 & 107444 \\ -250546 & 35647 & -78794 & 240674 \end{bmatrix},$$

and we have the rank of equation (3.1) is $12 = 4^2 - 4 > 4^2/2$.

Example 8. Take $n = 4$,

$$\mathbf{U} = \begin{bmatrix} 20 & 19 & 5 & 2 \\ 11 & 12 & 3 & 1 \\ 7 & 9 & 5 & 4 \\ 21 & 20 & 6 & 3 \end{bmatrix}, \mathbf{C} = \begin{bmatrix} 2 & 7 & 8 & 9 \\ -9 & 2 & 7 & 8 \\ -8 & -9 & 2 & 7 \\ -7 & -8 & -9 & 2 \end{bmatrix} \in \mathbb{X} \cap \mathbb{Z}^{4\times 4}.$$

Then

$$\mathbf{D} = \begin{bmatrix} -6957 & 2180 & -1440 & 5955 \\ -3865 & 1213 & -795 & 3305 \\ -7207 & 2249 & -1565 & 6201 \\ -8537 & 2672 & -1788 & 7317 \end{bmatrix},$$

and we have the rank of equation (3.1) is $12 = 4^2 - 4 > 4^2/2$.

Example 9. Take $n = 4$,

$$\mathbf{U} = \begin{bmatrix} 9 & 12 & 20 & 4 \\ 5 & 15 & 23 & 4 \\ 3 & 8 & 16 & 3 \\ 10 & 14 & 25 & 5 \end{bmatrix}, \mathbf{C} = \begin{bmatrix} 4 & 8 & 6 & 2 \\ -2 & 4 & 8 & 6 \\ -6 & -2 & 4 & 8 \\ -8 & -6 & -2 & 4 \end{bmatrix} \in \mathbb{X} \cap \mathbb{Z}^{4\times 4}.$$

Then

$$\mathbf{D} = \begin{bmatrix} -65940 & 10324 & -32080 & 63794 \\ -74958 & 11730 & -36456 & 72516 \\ -48974 & 7662 & -23816 & 47378 \\ -80668 & 12628 & -39242 & 78042 \end{bmatrix},$$

and we have the rank of equation (3.1) is $12 = 4^2 - 4 > 4^2/2$.

Example 10. Take $n = 4$,

$$\mathbf{U} = \begin{bmatrix} 20 & 19 & 5 & 2 \\ 11 & 12 & 3 & 1 \\ 7 & 9 & 5 & 4 \\ 21 & 20 & 6 & 3 \end{bmatrix}, \mathbf{C} = \begin{bmatrix} 3 & 6 & 6 & 10 \\ -10 & 3 & 6 & 6 \\ -6 & -10 & 3 & 6 \\ -6 & -6 & -10 & 3 \end{bmatrix} \in \mathbb{X} \cap \mathbb{Z}^{4\times 4}.$$

Then

$$\mathbf{D} = \begin{bmatrix} 117 & 572 & 1872 & -788 \\ 24 & 45 & 140 & -72 \\ 34 & 232 & 753 & -306 \\ 124 & 668 & 2168 & -903 \end{bmatrix},$$

and we have the rank of equation (3.1) is $12 = 4^2 - 4 > 4^2/2$.

Example 11. Take $n = 5$,

$$\mathbf{U} = \begin{bmatrix} 31 & 35 & 15 & 11 & 3 \\ 37 & 36 & 17 & 11 & 3 \\ 22 & 26 & 16 & 11 & 4 \\ 3 & 4 & 1 & 1 & 0 \\ 33 & 38 & 18 & 13 & 4 \end{bmatrix}, \mathbf{C} = \begin{bmatrix} 4 & 1 & 2 & 7 & 7 \\ -7 & 4 & 1 & 2 & 7 \\ -7 & -7 & 4 & 1 & 2 \\ -2 & -7 & -7 & 4 & 1 \\ -1 & -2 & -7 & -7 & 4 \end{bmatrix} \in \mathbb{X} \cap \mathbb{Z}^{5\times 5}.$$

Then

$$\mathbf{D} = \begin{bmatrix} 40065 & -4856 & 11868 & -21624 & -38146 \\ 46027 & -5559 & 13665 & -24730 & -43874 \\ 31533 & -3816 & 9350 & -16992 & -30039 \\ 3853 & -469 & 1139 & -2087 & -3664 \\ 43848 & -5314 & 12989 & -23667 & -41749 \end{bmatrix},$$

and we have the rank of equation (3.1) is $20 = 5^2 - 5 > 5^2/2$.

Example 12. Take $n = 5$,

$$\mathbf{U} = \begin{bmatrix} 34 & 24 & 11 & 7 & 1 \\ 49 & 26 & 13 & 9 & 2 \\ 32 & 17 & 11 & 15 & 4 \\ 17 & 5 & 6 & 13 & 4 \\ 37 & 24 & 12 & 10 & 2 \end{bmatrix}, \mathbf{C} = \begin{bmatrix} 1 & 3 & 2 & 2 & 2 \\ -2 & 1 & 3 & 2 & 2 \\ -2 & -2 & 1 & 3 & 2 \\ -2 & -2 & -2 & 1 & 3 \\ -3 & -2 & -2 & -2 & 1 \end{bmatrix} \in \mathbb{X} \cap \mathbb{Z}^{5\times 5}.$$

Then

$$\mathbf{D} = \begin{bmatrix} 580 & 464 & 5167 & -3499 & -4010 \\ 1441 & 622 & 6592 & -4267 & -5890 \\ 3089 & 584 & 5267 & -2862 & -6854 \\ 3229 & 396 & 2978 & -1200 & -5517 \\ 1404 & 545 & 5691 & -3638 & -5264 \end{bmatrix},$$

and we have the rank of equation (3.1) is $20 = 5^2 - 5 > 5^2/2$.

Example 13. Take $n = 5$,

$$\mathbf{U} = \begin{bmatrix} 18 & 11 & 10 & 18 & 4 \\ 27 & 24 & 10 & 11 & 2 \\ 21 & 14 & 10 & 15 & 3 \\ 6 & 3 & 3 & 5 & 1 \\ 19 & 12 & 12 & 22 & 5 \end{bmatrix}, \mathbf{C} = \begin{bmatrix} 9 & 2 & 5 & 8 & 5 \\ -5 & 9 & 2 & 5 & 8 \\ -8 & -5 & 9 & 2 & 5 \\ -5 & -8 & -5 & 9 & 2 \\ -2 & -5 & -8 & -5 & 9 \end{bmatrix} \in \mathbb{X} \cap \mathbb{Z}^{5\times 5}.$$

Then

$$\mathbf{D} = \begin{bmatrix} 18135 & -9785 & 29674 & -66832 & -14972 \\ 27442 & -14943 & 45420 & -102080 & -22729 \\ 20335 & -11026 & 33472 & -75290 & -16818 \\ 5369 & -2904 & 8809 & -19822 & -4437 \\ 20356 & -10970 & 33258 & -74933 & -16797 \end{bmatrix},$$

and we have the rank of equation (3.1) is $20 = 5^2 - 5 > 5^2/2$.

Example 14. Take $n = 5$,

$$\mathbf{U} = \begin{bmatrix} 32 & 19 & 12 & 11 & 4 \\ 38 & 25 & 19 & 15 & 5 \\ 14 & 15 & 12 & 10 & 3 \\ 3 & 4 & 3 & 3 & 1 \\ 35 & 21 & 13 & 13 & 5 \end{bmatrix}, \mathbf{C} = \begin{bmatrix} 6 & 5 & 6 & 9 & 6 \\ -6 & 6 & 5 & 6 & 9 \\ -9 & -6 & 6 & 5 & 6 \\ -6 & -9 & -6 & 6 & 5 \\ -5 & -6 & -9 & -6 & 6 \end{bmatrix} \in \mathbb{X} \cap \mathbb{Z}^{5\times 5}.$$

Then

$$\mathbf{D} = \begin{bmatrix} 23699 & 9919 & -31811 & 87736 & -27236 \\ 31125 & 13052 & -41824 & 115334 & -35790 \\ 17540 & 7343 & -23543 & 64923 & -20162 \\ 4655 & 1945 & -6242 & 17214 & -5348 \\ 26448 & 11066 & -35498 & 97904 & -30392 \end{bmatrix},$$

and we have the rank of equation (3.1) is $20 = 5^2 - 5 > 5^2/2$.

Example 15. Take $n = 5$,

$$\mathbf{U} = \begin{bmatrix} 65 & 26 & 29 & 15 & 5 \\ 45 & 15 & 17 & 8 & 2 \\ 33 & 13 & 14 & 7 & 1 \\ 11 & 8 & 8 & 5 & 2 \\ 68 & 29 & 32 & 17 & 6 \end{bmatrix}, \mathbf{C} = \begin{bmatrix} 5 & 7 & 1 & 8 & 10 \\ -10 & 5 & 7 & 1 & 8 \\ -8 & -10 & 5 & 7 & 1 \\ -1 & -8 & -10 & 5 & 7 \\ -7 & -1 & -8 & -10 & 5 \end{bmatrix} \in \mathbb{X} \cap \mathbb{Z}^{5\times 5}.$$

Then

$$\mathbf{D} = \begin{bmatrix} 59174 & -6482 & -5367 & 20898 & -53053 \\ 39048 & -4203 & -3555 & 13885 & -35066 \\ 30168 & -3328 & -2714 & 10633 & -27039 \\ 11895 & -1386 & -1064 & 4097 & -10601 \\ 62863 & -6926 & -5696 & 22150 & -56329 \end{bmatrix},$$

and we have the rank of equation (3.1) is $20 = 5^2 - 5 > 5^2/2$.

Example 16. Take $n = 6$,

$$\mathbf{U} = \begin{bmatrix} 13 & 16 & 13 & 5 & 4 & 1 \\ 11 & 14 & 4 & 2 & 5 & 1 \\ 9 & 11 & 7 & 2 & 2 & 0 \\ 11 & 17 & 9 & 5 & 7 & 2 \\ 6 & 9 & 6 & 4 & 5 & 2 \\ 15 & 19 & 16 & 7 & 6 & 2 \end{bmatrix}, \mathbf{C} = \begin{bmatrix} 0 & 4 & 1 & 5 & 5 & 4 \\ -4 & 0 & 4 & 1 & 5 & 5 \\ -5 & -4 & 0 & 4 & 1 & 5 \\ -5 & -5 & -4 & 0 & 4 & 1 \\ -1 & -5 & -5 & -4 & 0 & 4 \\ -4 & -1 & -5 & -5 & -4 & 0 \end{bmatrix} \in \mathbb{X} \cap \mathbb{Z}^{6\times 6}.$$

Then

$$\mathbf{D} = \begin{bmatrix} -6302 & 384 & 766 & 544 & -2978 & 5502 \\ -4958 & 248 & 817 & 358 & -2135 & 4210 \\ -3846 & 228 & 485 & 328 & -1799 & 3348 \\ -6712 & 347 & 1070 & 492 & -2926 & 5720 \\ -4127 & 220 & 642 & 306 & -1817 & 3526 \\ -7918 & 476 & 997 & 670 & -3710 & 6894 \end{bmatrix},$$

and we have the rank of equation (3.1) is $30 = 6^2 - 6 > 6^2/2$.

Example 17. Take $n = 6$,

$$\mathbf{U} = \begin{bmatrix} 9 & 11 & 8 & 4 & 1 & 0 \\ 12 & 10 & 10 & 9 & 4 & 3 \\ 7 & 9 & 9 & 6 & 2 & 1 \\ 10 & 7 & 12 & 11 & 5 & 2 \\ 10 & 6 & 8 & 8 & 4 & 3 \\ 12 & 13 & 10 & 6 & 2 & 1 \end{bmatrix}, \mathbf{C} = \begin{bmatrix} 7 & 5 & 7 & 8 & 6 & 5 \\ -5 & 7 & 5 & 7 & 8 & 6 \\ -6 & -5 & 7 & 5 & 7 & 8 \\ -8 & -6 & -5 & 7 & 5 & 7 \\ -7 & -8 & -6 & -5 & 7 & 5 \\ -5 & -7 & -8 & -6 & -5 & 7 \end{bmatrix} \in \mathbb{X} \cap \mathbb{Z}^{6\times 6}.$$

Then

$$\mathbf{D} = \begin{bmatrix} 32205 & 2664 & 1834 & -4910 & 11079 & -33035 \\ 39112 & 3229 & 2253 & -5990 & 13496 & -40144 \\ 30980 & 2554 & 1781 & -4736 & 10680 & -31791 \\ 39042 & 3207 & 2252 & -5980 & 13488 & -40073 \\ 29787 & 2450 & 1724 & -4570 & 10297 & -30578 \\ 40441 & 3343 & 2311 & -6174 & 13925 & -41490 \end{bmatrix},$$

and we have the rank of equation (3.1) is $30 = 6^2 - 6 > 6^2/2$.

Example 18. Take $n = 6$,

$$\mathbf{U} = \begin{bmatrix} 19 & 11 & 17 & 18 & 7 & 2 \\ 10 & 9 & 15 & 19 & 9 & 3 \\ 6 & 5 & 10 & 13 & 6 & 2 \\ 2 & 2 & 3 & 7 & 4 & 2 \\ 2 & 3 & 5 & 9 & 5 & 2 \\ 19 & 12 & 18 & 21 & 9 & 3 \end{bmatrix}, \mathbf{C} = \begin{bmatrix} 8 & 6 & 10 & 10 & 9 & 4 \\ -4 & 8 & 6 & 10 & 10 & 9 \\ -9 & -4 & 8 & 6 & 10 & 10 \\ -10 & -9 & -4 & 8 & 6 & 10 \\ -10 & -10 & -9 & -4 & 8 & 6 \\ -6 & -10 & -10 & -9 & -4 & 8 \end{bmatrix} \in \mathbb{X} \cap \mathbb{Z}^{6\times 6}.$$

Then

$$\mathbf{D} = \begin{bmatrix} -19862 & -7180 & 9128 & -7655 & -3410 & 21907 \\ -17489 & -6293 & 8069 & -6615 & -3146 & 19260 \\ -11367 & -4096 & 5256 & -4291 & -2054 & 12517 \\ -5009 & -1802 & 2325 & -1850 & -945 & 5510 \\ -6790 & -2440 & 3148 & -2520 & -1271 & 7469 \\ -21830 & -7882 & 10042 & -8366 & -3799 & 24068 \end{bmatrix},$$

and we have the rank of equation (3.1) is $30 = 6^2 - 6 > 6^2/2$.

Example 19. Take $n = 6$,

$$\mathbf{U} = \begin{bmatrix} 14 & 17 & 3 & 11 & 8 & 2 \\ 15 & 19 & 1 & 12 & 6 & 1 \\ 10 & 14 & 2 & 9 & 5 & 1 \\ 5 & 8 & 1 & 6 & 4 & 1 \\ 4 & 9 & 2 & 8 & 7 & 2 \\ 15 & 20 & 4 & 14 & 11 & 3 \end{bmatrix}, \mathbf{C} = \begin{bmatrix} 1 & 9 & 5 & 4 & 8 & 9 \\ -9 & 1 & 9 & 5 & 4 & 8 \\ -8 & -9 & 1 & 9 & 5 & 4 \\ -4 & -8 & -9 & 1 & 9 & 5 \\ -5 & -4 & -8 & -9 & 1 & 9 \\ -9 & -5 & -4 & -8 & -9 & 1 \end{bmatrix} \in \mathbb{X} \cap \mathbb{Z}^{6\times 6}.$$

Then

$$\mathbf{D} = \begin{bmatrix} -7539 & 2048 & 458 & -5522 & -851 & 6733 \\ -7405 & 1993 & 469 & -5409 & -844 & 6617 \\ -5343 & 1414 & 313 & -3766 & -660 & 4782 \\ -3417 & 947 & 196 & -2546 & -365 & 3049 \\ -4447 & 1276 & 233 & -3414 & -430 & 3960 \\ -9205 & 2534 & 540 & -6816 & -1005 & 8215 \end{bmatrix},$$

and we have the rank of equation (3.1) is $30 = 6^2 - 6 > 6^2/2$.

Example 20. Take $n = 6$,

$$\mathbf{U} = \begin{bmatrix} 13 & 16 & 13 & 5 & 4 & 1 \\ 11 & 14 & 4 & 2 & 5 & 1 \\ 9 & 11 & 7 & 2 & 2 & 0 \\ 11 & 17 & 9 & 5 & 7 & 2 \\ 6 & 9 & 6 & 4 & 5 & 2 \\ 15 & 19 & 16 & 7 & 6 & 2 \end{bmatrix}, \mathbf{C} = \begin{bmatrix} 9 & 6 & 3 & 1 & 6 & 2 \\ -2 & 9 & 6 & 3 & 1 & 6 \\ -6 & -2 & 9 & 6 & 3 & 1 \\ -1 & -6 & -2 & 9 & 6 & 3 \\ -3 & -1 & -6 & -2 & 9 & 6 \\ -6 & -3 & -1 & -6 & -2 & 9 \end{bmatrix} \in \mathbb{X} \cap \mathbb{Z}^{6\times 6}.$$

Then

$$\mathbf{D} = \begin{bmatrix} -2478 & -179 & 913 & 1006 & -2149 & 1942 \\ -1402 & -115 & 573 & 583 & -1260 & 1086 \\ -1461 & -87 & 526 & 603 & -1250 & 1128 \\ -2083 & -109 & 683 & 840 & -1736 & 1629 \\ -1214 & -44 & 377 & 496 & -988 & 936 \\ -2905 & -191 & 1042 & 1181 & -2492 & 2269 \end{bmatrix},$$

and we have the rank of equation (3.1) is $30 = 6^2 - 6 > 6^2/2$.

Example 21. Take $n = 7$,

$$\mathbf{U} = \begin{bmatrix} 16 & 12 & 14 & 11 & 10 & 3 & 2 \\ 7 & 10 & 9 & 9 & 7 & 2 & 1 \\ 12 & 19 & 17 & 22 & 18 & 5 & 2 \\ 2 & 7 & 5 & 9 & 7 & 2 & 0 \\ 6 & 9 & 7 & 11 & 13 & 4 & 3 \\ 4 & 6 & 5 & 7 & 9 & 3 & 2 \\ 18 & 14 & 16 & 13 & 13 & 4 & 3 \end{bmatrix}, \mathbf{C} = \begin{bmatrix} 8 & 6 & 0 & 7 & 6 & 9 & 8 \\ -8 & 8 & 6 & 0 & 7 & 6 & 9 \\ -9 & -8 & 8 & 6 & 0 & 7 & 6 \\ -6 & -9 & -8 & 8 & 6 & 0 & 7 \\ -7 & -6 & -9 & -8 & 8 & 6 & 0 \\ 0 & -7 & -6 & -9 & -8 & 8 & 6 \\ -6 & 0 & -7 & -6 & -9 & -8 & 8 \end{bmatrix} \in \mathbb{X} \cap \mathbb{Z}^{7\times 7}.$$

Then

$$\mathbf{D} = \begin{bmatrix} -228589 & -9970 & -27221 & 87537 & -4386 & -86724 & 236209 \\ -135784 & -5934 & -16123 & 51925 & -2635 & -51461 & 140286 \\ -263952 & -11561 & -31339 & 100938 & -5108 & -100038 & 272704 \\ -78927 & -3470 & -9354 & 30159 & -1540 & -29886 & 81536 \\ -130604 & -5696 & -15550 & 49985 & -2496 & -49519 & 134942 \\ -90819 & -3960 & -10817 & 34766 & -1743 & -34427 & 93838 \\ -263887 & -11505 & -31429 & 101054 & -5060 & -100112 & 272682 \end{bmatrix},$$

and we have the rank of equation (3.1) is $42 = 7^2 - 7 > 7^2/2$.

Example 22. Take $n = 7$,

$$\mathbf{U} = \begin{bmatrix} 15 & 10 & 12 & 6 & 4 & 6 & 2 \\ 20 & 15 & 11 & 6 & 3 & 2 & 1 \\ 10 & 12 & 7 & 5 & 5 & 3 & 1 \\ 8 & 13 & 10 & 7 & 6 & 8 & 3 \\ 3 & 6 & 4 & 3 & 3 & 3 & 1 \\ 2 & 5 & 4 & 3 & 3 & 5 & 2 \\ 16 & 12 & 13 & 7 & 5 & 8 & 3 \end{bmatrix}, \mathbf{C} = \begin{bmatrix} 9 & 6 & 6 & 5 & 2 & 10 & 5 \\ -5 & 9 & 6 & 6 & 5 & 2 & 10 \\ -10 & -5 & 9 & 6 & 6 & 5 & 2 \\ -2 & -10 & -5 & 9 & 6 & 6 & 5 \\ -5 & -2 & -10 & -5 & 9 & 6 & 6 \\ -6 & -5 & -2 & -10 & -5 & 9 & 6 \\ -6 & -6 & -5 & -2 & -10 & -5 & 9 \end{bmatrix} \in \mathbb{X} \cap \mathbb{Z}^{7\times 7}.$$

Then

$$\mathbf{D} = \begin{bmatrix} 7904 & -771 & 4854 & 5362 & -18235 & 5423 & -9427 \\ 8793 & -971 & 5606 & 6378 & -21041 & 5765 & -10501 \\ 7746 & -740 & 4754 & 5206 & -17791 & 5340 & -9249 \\ 10339 & -868 & 6126 & 6564 & -22994 & 7361 & -12340 \\ 4506 & -384 & 2682 & 2871 & -10046 & 3200 & -5378 \\ 4777 & -338 & 2725 & 2833 & -10251 & 3533 & -5702 \\ 9785 & -892 & 5910 & 6451 & -22222 & 6836 & -11675 \end{bmatrix},$$

and we have the rank of equation (3.1) is $42 = 7^2 - 7 > 7^2/2$.

Example 23. Take $n = 7$,

$$\mathbf{U} = \begin{bmatrix} 9 & 6 & 17 & 10 & 9 & 4 & 2 \\ 9 & 6 & 19 & 9 & 6 & 3 & 1 \\ 11 & 3 & 20 & 11 & 8 & 4 & 1 \\ 4 & 4 & 8 & 7 & 7 & 2 & 2 \\ 4 & 2 & 7 & 5 & 5 & 2 & 1 \\ 1 & 0 & 3 & 1 & 1 & 1 & 0 \\ 9 & 8 & 19 & 12 & 12 & 5 & 3 \end{bmatrix}, \mathbf{C} = \begin{bmatrix} 8 & 0 & 5 & 10 & 0 & 1 & 5 \\ -5 & 8 & 0 & 5 & 10 & 0 & 1 \\ -1 & -5 & 8 & 0 & 5 & 10 & 0 \\ 0 & -1 & -5 & 8 & 0 & 5 & 10 \\ -10 & 0 & -1 & -5 & 8 & 0 & 5 \\ -5 & -10 & 0 & -1 & -5 & 8 & 0 \\ 0 & -5 & -10 & 0 & -1 & -5 & 8 \end{bmatrix} \in \mathbb{X} \cap \mathbb{Z}^{7\times 7}.$$

Then

$$\mathbf{D} = \begin{bmatrix} 2563 & -160 & -709 & 1718 & -1034 & 2692 & -2149 \\ 3500 & 73 & -1249 & 2356 & -619 & 3796 & -3246 \\ 3956 & -6 & -1314 & 2636 & -941 & 4198 & -3569 \\ 558 & -280 & 79 & 367 & -889 & 486 & -205 \\ 918 & -142 & -171 & 608 & -600 & 922 & -678 \\ 552 & 18 & -204 & 368 & -77 & 611 & -519 \\ 2192 & -320 & -438 & 1470 & -1377 & 2262 & -1644 \end{bmatrix},$$

and we have the rank of equation (3.1) is $42 = 7^2 - 7 > 7^2/2$.

Example 24. Take $n = 7$,

$$\mathbf{U} = \begin{bmatrix} 18 & 16 & 17 & 12 & 9 & 5 & 2 \\ 24 & 18 & 19 & 10 & 10 & 7 & 2 \\ 6 & 3 & 5 & 4 & 2 & 0 & 0 \\ 11 & 9 & 12 & 10 & 7 & 3 & 1 \\ 10 & 6 & 9 & 5 & 6 & 4 & 1 \\ 5 & 4 & 5 & 3 & 4 & 3 & 1 \\ 20 & 19 & 20 & 15 & 12 & 7 & 3 \end{bmatrix}, \mathbf{C} = \begin{bmatrix} 3 & 9 & 5 & 3 & 5 & 4 & 5 \\ -5 & 3 & 9 & 5 & 3 & 5 & 4 \\ -4 & -5 & 3 & 9 & 5 & 3 & 5 \\ -5 & -4 & -5 & 3 & 9 & 5 & 3 \\ -3 & -5 & -4 & -5 & 3 & 9 & 5 \\ -5 & -3 & -5 & -4 & -5 & 3 & 9 \\ -9 & -5 & -3 & -5 & -4 & -5 & 3 \end{bmatrix} \in \mathbb{X} \cap \mathbb{Z}^{7\times 7}.$$

Then

$$\mathbf{D} = \begin{bmatrix} -6458 & -864 & -3321 & -2753 & 10964 & -19179 & 8661 \\ -7659 & -1051 & -3992 & -3319 & 13152 & -22988 & 10337 \\ -1131 & -156 & -545 & -491 & 1878 & -3266 & 1514 \\ -4356 & -537 & -2171 & -1788 & 7193 & -12635 & 5754 \\ -3892 & -484 & -1973 & -1618 & 6500 & -11428 & 5167 \\ -2577 & -317 & -1317 & -1065 & 4311 & -7587 & 3418 \\ -8195 & -1071 & -4201 & -3458 & 13841 & -24248 & 10950 \end{bmatrix},$$

and we have the rank of equation (3.1) is $42 = 7^2 - 7 > 7^2/2$.

Example 25. Take $n = 7$,

$$\mathbf{U} = \begin{bmatrix} 12 & 16 & 7 & 8 & 4 & 4 & 2 \\ 9 & 19 & 10 & 12 & 5 & 9 & 3 \\ 5 & 11 & 5 & 7 & 2 & 4 & 1 \\ 3 & 9 & 5 & 8 & 2 & 7 & 2 \\ 2 & 7 & 3 & 3 & 1 & 2 & 0 \\ 2 & 4 & 3 & 5 & 2 & 5 & 2 \\ 13 & 17 & 8 & 10 & 5 & 6 & 3 \end{bmatrix}, \mathbf{C} = \begin{bmatrix} 5 & 7 & 7 & 1 & 10 & 8 & 7 \\ -7 & 5 & 7 & 7 & 1 & 10 & 8 \\ -8 & -7 & 5 & 7 & 7 & 1 & 10 \\ -10 & -8 & -7 & 5 & 7 & 7 & 1 \\ -1 & -10 & -8 & -7 & 5 & 7 & 7 \\ -7 & -1 & -10 & -8 & -7 & 5 & 7 \\ -7 & -7 & -1 & -10 & -8 & -7 & 5 \end{bmatrix} \in \mathbb{X} \cap \mathbb{Z}^{7\times 7}.$$

Then

$$\mathbf{D} = \begin{bmatrix} -19476 & 3133 & -3500 & 5468 & -1223 & -16716 & 18635 \\ -27551 & 4362 & -4936 & 7799 & -1697 & -23682 & 26386 \\ -13679 & 2161 & -2429 & 3842 & -829 & -11716 & 13093 \\ -15939 & 2475 & -2854 & 4535 & -933 & -13694 & 15283 \\ -7207 & 1159 & -1280 & 2034 & -470 & -6200 & 6891 \\ -10597 & 1631 & -1914 & 3029 & -601 & -9111 & 10173 \\ -23627 & 3765 & -4254 & 6655 & -1447 & -20280 & 22624 \end{bmatrix},$$

and we have the rank of equation (3.1) is $42 = 7^2 - 7 > 7^2/2$.