Solving Trapdoor Basis of 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 a new attack on cryptosystems based on ideal lattices. We show that, if there is one polynomially large entry in the transformation matrix from trapdoor basis to public basis, then 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.
By a modified attacking procedure, we break Gentry09 fully homomorphic encryption (FHE), although each entry of its transformation matrix is super-polynomially large. The key point is that the scheme publishes many vectors of the inverse ideal, and we can reduce each vector into polynomially large multiple of its generator. Such modified attacking procedure has a natural corollary: if we can obtain enough vectors of the inverse ideal, then we can obtain the trapdoor basis with high probability, no matter whether each entry of the transformation matrix is super-polynomially large.

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

1 Introduction

Cryptosystems based on lattices are important 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 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. 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 case 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 it is questionable whether each entry of this transformation matrix is super-polynomially large.

In this paper we present a new attack on cryptosystems based on ideal lattices. We show that, if there is only one polynomially large entry in the transformation matrix from trapdoor basis to public basis, then 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 (rather than of real number variables), and find it not difficult to be solved as long as its rank is larger than half of its number of variables.

By a modified attacking procedure, we break Gentry 09 FHE, although each entry of its transformation matrix is super-polynomially large. The key point is that, besides the public basis, the scheme leaks additional information, that is, it publishes many vectors of the inverse ideal. We can reduce each of these vectors into polynomially large multiple of its generator. Such modified attacking procedure has a natural corollary: if we can obtain enough vectors of the inverse ideal, then we can obtain the trapdoor basis with high probability, no matter whether each entry of the transformation matrix is super-polynomially large.

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, $a(\text{mod } q)$ is within $\{-(q-1)/2, -(q-3)/2, \ldots, (q-1)/2\}$; if q is an even, $a(\text{mod } q)$ 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 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

Now 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

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

Finally, we obtain a linear equation of **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 **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 **U**, under the assumption that this entry is polynomially large. For each possible value of this entry, we obtain unique value of **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 $n^2/2$.

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 **G** is from $\mathbb{Q}$.

Second, we take g_0 as the smallest common denominator of entries of **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: Solving the Former Linear Equation

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 [2], but they do not affect our attack.

4 Some Details of Our Attack

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

Lemma 1. Take $\mathbf{H} \in \mathbb{X}$.

(1) Suppose n is an even number. Then $\det(\mathbf{H}) = 0$ if and only if $\mathbf{H} = \mathbf{O}$. In other words, $\mathbb{X}$ is a field.

(2) Suppose n is an odd number. If $\det(\mathbf{H}) = 0$ and $\mathbf{H} \neq \mathbf{O}$, then $\mathbf{H} = \mathbf{H}^{(0)} \cdot \mathbf{H}^{(1)}$, where $\mathbf{H}^{(0)}$ takes one of the following two shapes:

$$\mathbf{H}^{(0)} = \begin{bmatrix} 1 & 1 & & & \\ & 1 & 1 & & \\ & & \ddots & \ddots & \\ & & & 1 & 1 \\ -1 & & & & 1 \end{bmatrix}, \quad \text{or}$$

$$\mathbf{H}^{(0)} = \begin{bmatrix} 1 & -1 & 1 & \ldots & -1 & 1 \\ -1 & 1 & -1 & \ldots & 1 & -1 \\ 1 & -1 & 1 & \ldots & -1 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ -1 & 1 & -1 & \ldots & 1 & -1 \\ 1 & -1 & 1 & \ldots & -1 & 1 \end{bmatrix}.$$

Lemma 1 is clear by considering decomposition of the polynomial X^n+1 over rational numbers (rather than over real numbers).

Denote

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

and rewrite equation (3.1) into the form

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

where

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

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 2. If n is an even number, the rank of equation (3.1) is multiple of n, therefore it is not larger than $n^2 - n$.

Lemma 2 is clear. Because $\mathbb{X}$ is a field for even n, we can make Gaussian elimination over $\mathbb{X}$ (rather than over $\mathbb{Q}$).

(To be continued)

5 Breaking Gentry09 FHE

5.1 About Gentry09 FHE

We don't repeat the whole scheme of Gentry09 FHE, only state those parameters related to our attack. $\{\mathbf{b}, \mathbf{B}^{Trap}, \mathbf{U}, \mathbf{B}^{Pub}\}$ are as described above, there is only one restriction that each entry of $\mathbf{B}^{Trap}$ (that is, each entry of $\mathbf{b}$) is polynomially large to make the scheme simple. Moreover, γ vectors of $\langle \mathbf{b}^{-1} \rangle$ are published to construct simplified decryption circuit, where $\gamma > n$. We call these vectors $\{\mathbf{t}^{(1)}, \mathbf{t}^{(2)}, \ldots, \mathbf{t}^{(\gamma)}\}$. We know that $\mathbf{t}^{(i)} \in \mathbb{Q}^n$, $i = 1, 2, \ldots, \gamma$.

5.2 Our Observations

We take (mod 1) operation as follows:

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

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

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

5.3 Modified Attack to Break Gentry09 FHE

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. Gentry09 FHE is broken.

6 A Natural Corollary

Suppose that, beside the public basis, we are given n vectors of the inverse ideal. Then we can reduce each vector into polynomially large multiple of its generator. After that we can obtain the trapdoor basis with high probability, no matter whether each entry of the transformation matrix is super-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)