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 chenjiangshan008@hotmail.com

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 non-negligible probability. The key point is that some class of matrices satisfies multiplication commutative law. We use multiplication commutative law to obtain a linear equation over integers, and find it not difficult to be solved as long as its rank is larger than half of its number of variables.

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 supper-polynomially large transformation matrix. However it is questionable whether each entry of the transformation matrix is supper-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 non-negligible probability. Our attack is quite simple, the key point is that some class of matrices satisfies multiplication commutative law. We use multiplication commutative law to obtain a linear equation over integers (rather than in real numbers), and find it not difficult to be solved as long as its rank is larger than half of its number of variables.

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.

For $\mathbf{x}\in R$,$\langle\mathbf{x}\rangle=\{\mathbf{x}\cdot\mathbf{u}:\mathbf{u}\in R\}$ 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 $\mathbb{X}\subset\mathbb{Z}^{n\times n}$ 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 $a_{i,j}\in\mathbb{Z}$. $\mathbb{X}$ satisfies multiplication commutative law, namely, for $\mathbf{A},\mathbf{B}\in\mathbb{X}$, we have $\mathbf{AB}=\mathbf{BA}$.

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 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

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

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

3 A Brief Description of Our Attack

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

Now our knowledge is $\mathbf{B}^{Pub}$, and we want to obtain $\mathbf{B}^{Trap}$.

First, we take a matrix $\mathbf{C} \in \mathbb{X}$, and compute the product $\mathbf{B}^{Pub}\mathbf{C}$. By considering Multiplication Commutative Law, we have

$$\mathbf{B}^{Pub}\mathbf{C} = (\mathbf{UC})\mathbf{B}^{Trap},$$

although we don't know $\mathbf{U}$ and $\mathbf{B}^{Trap}$.

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

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

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

$$\mathbf{UC} - \mathbf{DU} = \mathbf{O}, \tag{3.1}$$

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

Of course such linear equation 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 $n^2/2$.

Suppose the rank of equation (3.1) is r, and r is larger than $n^2/2$. 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 $u_1, u_2, \ldots, u_{n(n-1)}$ are integers, each entry of

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

must be a multiple of v_0.

Finally, we solve the linear equation modular g_0,

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

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 large 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 $\mathbf{U}^{-1}\mathbf{B}^{Pub} \in \mathbb{X}$.

Whenever $(u_1, u_2, \ldots, u_{n^2})$ passes these checks, each row of $\mathbf{U}^{-1}\mathbf{B}^{Pub}$ is a generator of the principal ideal $\langle \mathbf{b} \rangle$. Finally we obtain several generators. These generators include $\mathbf{b}$, 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: it is an open problem how many generators does a principal ideal have [2], but it does not affect our attack.

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)