Solving Trapdoor Basis of Ideal Lattice from Public Basis

Yupu Hu and Zhizhu Lian

ISN Laboratory, Xidian University, 710071 Xi'an, China
yphu@mail.xidian.edu.cn lzz600@126.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. The key point is that some class of matrices satisfies multiplication commutative law.

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

1 Introduction

Cryptosystems based on lattices are important cryptosystems, and most useful are those based on ideal lattices. The lattice has a trapdoor basis which is hidden. 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 is the transformation matrix ? For ordinary lattice, the common view is that the transformation matrix can be polynomially large without security worry. For ideal lattice, the common view is that the transformation matrix " had better supper-polynomially large", and a good type is Hermite Normal Form (HNF). However, there is no conclusion what kind of danger is if the transformation matrix is 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. The key point is that some class of matrices satisfies multiplication commutative law.

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).

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 $\mathbf{a} = (a_0, a_1, \cdots, a_{n-1}) \in \mathbb{Z}^n$, where each entry of $\mathbf{a}$ is polynomially large. 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 $\langle \mathbf{a} \rangle$. 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 $\mathbf{B}^{Trap}$.

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

$$\mathbf{B}^{Pub}\mathbf{X} = (\mathbf{U}\mathbf{X})\mathbf{B}^{Trap},$$

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

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

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

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

$$\mathbf{U}\mathbf{X} - \mathbf{Y}\mathbf{U} = \mathbf{0}. \tag{3.1}$$

Of course such linear equation is of 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 $\mathbf{U}$. For this corresponding value of $\mathbf{U}$, we make following 3 checks:

- whether $\det(\mathbf{U}) = \pm 1$,
- whether $\mathbf{U}^{-1}\mathbf{B}^{Pub} \in \mathbb{X}$,
- whether each entry of $\mathbf{U}^{-1}\mathbf{B}^{Pub}$ is polynomially large.

Whenever it passes the check, we can take $\mathbf{U}^{-1}\mathbf{B}^{Pub}$ as a trapdoor basis. The cryptosystem has been broken, although it is possible that $\mathbf{U}^{-1}\mathbf{B}^{Pub} \neq \mathbf{B}^{Trap}$.

However, we find it is almost sure that the rank of the above linear equation is $n^2 - n$ (we will explain the reason later). So we must use another method to obtain $\mathbf{U}$.

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

Suppose the rank of equation (3.1) is $n^2 - n$. 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 u_{n^2} is polynomially large.

First, we convert the linear equation into the following form:

$$\begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_{n(n-1)} \end{bmatrix} = \mathbf{V} \begin{bmatrix} u_{n(n-1)+1} \\ u_{n(n-1)+2} \\ \vdots \\ u_{n^2} \end{bmatrix},$$

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

Second, we take v_0 as the smallest common denominator of entries of $\mathbf{V}$, and take $\mathbf{V}^{(0)} = v_0\mathbf{V}$, so that $\mathbf{V}^{(0)}$ is an integer matrix. Because $u_1, u_2, \ldots, u_{n(n-1)}$ are integers, each entry of

$$\mathbf{V}^{(0)} \begin{bmatrix} u_{n(n-1)+1} \\ u_{n(n-1)+2} \\ \vdots \\ u_{n^2} \end{bmatrix}$$

must be a multiple of v_0.

Finally, we solve the linear equation modular v_0,

$$\mathbf{V}^{(0)} \begin{bmatrix} u_{n(n-1)+1} \\ u_{n(n-1)+2} \\ \vdots \\ u_{n^2} \end{bmatrix} \bmod v_0 = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}. \tag{3.2}$$

$\mathbf{V}^{(0)}$ has $n(n-1)$ rows and n columns, so that it is almost sure that the rank of this equation is $n-1$. By searching all possible values of u_{n^2}, we obtain all possible mod v_0 values of $(u_{n(n-1)+1}, u_{n(n-1)+2}, \ldots, u_{n^2})$. Here we need a condition: when u_{n^2} takes true value, corresponding mod v_0 value of $(u_{n(n-1)+1}, u_{n(n-1)+2}, \ldots, u_{n^2})$ is respectively true value of $u_{n(n-1)+1}, u_{n(n-1)+2}, \ldots, u_{n^2}$. In other words, true values of $\{u_{n(n-1)+1}, u_{n(n-1)+2}, \ldots, u_{n^2}\}$ are all within the interval $[-v_0/2, v_0/2)$. This can be easily satisfied if we take $\mathbf{X}$ sufficiently large. For example if we find v_0 larger than any entry of $\mathbf{B}^{Pub}$, then the condition is satisfied with large probability.

3.3 Step 3: Solving the Former Linear Equation

For each possible solution $\{u_{n(n-1)+1}, u_{n(n-1)+2}, \ldots, u_{n^2}\}$ of equation (3.2), we can obtain corresponding solution $u_1, u_2, \ldots, u_{n^2}$ of equation (3.1). Then we make above 3 checks. Whenever it passes the check, we can take $\mathbf{U}^{-1}\mathbf{B}^{Pub}$ as a trapdoor basis. The cryptosystem has been broken.