Cryptanalysis of the Cai-Cusick Lattice-based Public-key Cryptosystem

Yanbin Pan and Yingpu Deng
Key Laboratory of Mathematics Mechanization
Academy of Mathematics and Systems Science,Chinese Academy of Sciences
Beijing 100190, China
{panyanbin,dengyp}@amss.ac.cn

Abstract

In 1998, Cai and Cusick proposed a lattice-based public-key cryptosystem based on the similar ideas of the Ajtai-Dwork cryptosystem, but with much less data expansion. However, they didn't give any security proof. In our paper, we present an efficient ciphertext-only attack which runs in polynomial time against the cryptosystem to recover the message, so the Cai-Cusick lattice-based public-key cryptosystem is not secure. We also present two chosen-ciphertext attacks to get a similar private key which acts as the real private key.

Keywords: lattice, Cai-Cusick Cryptosystem, Gram-Schmidt orthogonalization, ciphertext-only attack, chosen-ciphertext attack

1 Introduction

Lattices are discrete subgroups of $\mathbb{R}^n$ and have been widely used in cryptology, both in cryptanalysis and cryptography.

Since the seminal work of Ajtai [1] connecting the average-case complexity of lattice problems to their complexity in the worst case, cryptographic constructions based on lattices have drawn considerable attention. The first lattice-based cryptosystem was proposed by Ajtai and Dwork [3] with a security proof based on worst-case hardness assumptions. After their results, several lattice-based cryptosystems [7, 8, 4, 6, 10, 11, 2] have been proposed .

Lattice-based cryptosystem have many advantages: first, the computations involved are very simple and usually require only modular addition ; second, by now they resist the cryptanalysis by quantum algorithms while there already exist the efficient quantum algorithms for factoring integers and computing discrete logarithms.

Of course, the most charming things we pursue are the security based on the worst-case hardness of lattice problems and the efficiency on the speed, key size, expansion rate and so on. However, the trouble in the real life is that the lattice-based cryptosystems which are efficient have no security proofs based on the hardness of lattice problems while those which have security proofs are not efficient.

Although the Ajtai-Dwork cryptosystem has a security proof, Nguyen and Stern [9] gave a heuristic attack to show that the implementations of the Ajtai-Dwork cryptosystem would require very large keys in order to be secure, making it impractical in a real-life environment because of its key size and expansion rate.

In 1998, Cai and Cusick [4] proposed an efficient lattice-based public-key cryptosystem with much less data expansion by mixing the Ajtai-Dwork cryptosystem with a knapsack. However, they didn't give any security proof except showing that their cryptosystem could resist some potential attacks. In our paper, we present an efficient ciphertext-only attack to recover the message. However, we don't recover the private key in the attack. The probability analysis show that our attack can succeed with probability near 1 so that the cryptosystem is not secure. We also present two chosen-ciphertext attacks to get a similar private key which acts as the real private key if we have a decryption oracle working as the decryption algorithm.

As we know, it's the first cryptanalysis of the Cai-Cusick lattice-based public-key cryptosystem. Experiments show that the ciphertext-only attack indeed always succeeds to recover the message in short time, as the results of the probability analysis indicate.

The remainder of the paper is organized as follows. In section 2, we describe the Cai-Cusick lattice-based public-key cryptosystem. Section 3 presents our ciphertext-only attack to recover the message and the analysis of its succeeding probability. In section 4, we present two chosen-ciphertext attacks to recover a private key.

2 The Cai-Cusick Cryptosystem

Let us first fix some notations. $\mathbb{R}$ is the field of real numbers, $\mathbb{Z}$ is the ring of integers, $\mathbb{R}^n$ is the space of n-dimensional real vectors v, with the dot product $\langle v, u\rangle$,$v, u \in \mathbb{R}^n$ and Euclidean norm $\|v\| = \langle v, v\rangle^{1/2}$, $span(v_1, v_2, \cdots, v_m) = \{\sum_{i=1}^{m} x_i v_i | x_i \in \mathbb{R}\}$, where $v_i \in \mathbb{R}^n$. If A is a subspace of $\mathbb{R}^n$, then $A^{\perp} = \{x \in \mathbb{R}^n | \langle x, v\rangle = 0, \forall v \in A\}$. $S^{n-1} = \{x \in \mathbb{R}^n | \|x\| = 1\}$, $H_i(u) = \{x \in \mathbb{R}^n | \langle x, u\rangle = i\}$, where $i \in \mathbb{Z}^+, u \in S^{n-1}$.

We just give a simple description of the Cai-Cusick cryptosystem in this section, and see more details in [4] or [5].

2.1 Description of the Cai-Cusick Cryptosystem

Key Generation:

- Select u uniformly at random from S^{n-1} .
- Select a real number $b > 0$.
- Select $v_0, \cdots, v_m$ uniformly at random from $H_{N_0}(u), \cdots, H_{N_m}(u)$ respectively, where $m = \lfloor \frac{1}{2}n \rfloor$, $N_k > \sum_{i=0}^{k-1} N_i + b$ for $k = 1, \cdots, m$ and $N_0 > b$.
- Select randomly a permutation σ on $m+1$ letters.

Public Key: $v_{\sigma(0)}, \cdots, v_{\sigma(m)}$ and b.
Private Key: u and σ.
Encryption: Let $M = (a_0, a_1, \cdots, a_m)$ be the message, where $a_i \in \{0, 1\}$ and C be the ciphertext. Select r uniformly at random from $\{x \in \mathbb{R}^n | \|x\| \leq b/2\}$, and compute

$$C = \sum_{i=0}^{m} a_i v_{\sigma(i)} + r.$$

Decryption: Compute

$$\langle u, C \rangle = \sum_{i=0}^{m} a_i \langle u, v_{\sigma(i)} \rangle + \langle u, r \rangle = \sum_{i=0}^{m} a_{\sigma^{-1}(i)} N_i + \langle u, r \rangle.$$

Since $|\langle u, r \rangle| \leq \|u\|\|r\| = \|r\| \leq b/2$, so if $a_{\sigma^{-1}(m)} = 1$, then $\langle u, C \rangle \geq N_m - b/2$, otherwise, $\langle u, C \rangle \leq \sum_{i=0}^{m-1} N_i + b/2 < N_m - b/2$. Hence, we can decide whether $a_{\sigma^{-1}(m)} = 1$ by comparing $\langle u, C \rangle$ with $N_m - b/2$, i.e.

$$a_{\sigma^{-1}(m)} = \begin{cases} 1, & \text{if } \langle u, C \rangle \geq N_m - b/2; \\ 0, & \text{otherwise.} \end{cases}$$

After getting $a_{\sigma^{-1}(m)}$, substituting C by $C - a_{\sigma^{-1}(m)} N_m$, we can continue the process until all $a_{\sigma^{-1}(i)}$ are recovered. Then, using σ to recover M.

2.2 Some Remarks on the Cai-Cusick Cryptosystem

Remark 1. *Cai and Cusick [4] showed that if we did not employ the random permutation σ, there is an attack as follows:*

From the given vectors $v_0, v_1, \cdots, v_m$, we can use linear programming to find an $x \in \mathbb{R}^n$ satisfying:

$$\begin{array}{rcl} \langle x, v_0 \rangle & > & b \\ \langle x, v_1 \rangle & > & \langle x, v_0 \rangle + b \\ \vdots & \vdots & \vdots \\ \langle x, v_m \rangle & > & \langle x, \sum_{i=0}^{m-1} v_i \rangle + b \end{array}$$

Then we can use x instead of u to recover the correct message. So σ is essential to the security of the cryptosystem.

Remark 2. *Cai and Cusick [4] also gave a method to generate $v_0, v_1, \cdots, v_m$. Let B be a large integer, say $B \gg 2^n$. Choose any $b' > b$, for each i, $0 \le i \le m$, let $v_i = 2^i b' u + \sqrt{B^2 - 2^{2i} b'^2}\rho_i$, where the ρ_i's are independently and uniformly distributed on the $(n-2)$-dimensional unit sphere orthogonal to u. Note that $\|v_i\| = B$, and they showed that if the lengths of the vector v_i were not kept essentially the same, there can be statistical leakage of information.*

3 The Ciphertext-only Attack

3.1 The Principle of the Ciphertext-only Attack

As in [4], we may assume $v_{\sigma(0)}, v_{\sigma(1)}, \cdots, v_{\sigma(m)}$ are linearly independent, the Gram-Schmidt orthogonalization of $v_{\sigma(0)}, v_{\sigma(1)}, \cdots, v_{\sigma(m)}$ is defined by $v^*_{\sigma(i)} = v_{\sigma(i)} - \sum_{j=0}^{i-1} \mu_{i,j} v^*_{\sigma(j)}$, where $\mu_{i,j} = \dfrac{\langle v_{\sigma(i)}, v^*_{\sigma(j)} \rangle}{\langle v^*_{\sigma(j)}, v^*_{\sigma(j)} \rangle}$.

We get

$$(v_{\sigma(0)}, v_{\sigma(1)}, \cdots, v_{\sigma(m)}) = (v^*_{\sigma(0)}, v^*_{\sigma(1)}, \cdots, v^*_{\sigma(m)}) \begin{pmatrix} 1 & \mu_{1,0} & \cdots & \mu_{m,0} \\ 0 & 1 & \cdots & \mu_{m,1} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

So

$$\begin{aligned} C &= (v_{\sigma(0)}, v_{\sigma(1)}, \cdots, v_{\sigma(m)}) \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_m \end{pmatrix} + r, \\ &= (v^*_{\sigma(0)}, v^*_{\sigma(1)}, \cdots, v^*_{\sigma(m)}) \begin{pmatrix} 1 & \mu_{1,0} & \cdots & \mu_{m,0} \\ 0 & 1 & \cdots & \mu_{m,1} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_m \end{pmatrix} + r. \end{aligned}$$

We can write $r = \sum_{i=0}^{m} r_i v^*_{\sigma(i)} + \omega$, where $r_i \in \mathbb{R}$ and $\omega \in span(v^*_{\sigma(0)}, v^*_{\sigma(1)}, \cdots, v^*_{\sigma(m)})^{\perp}$, then

$$\|r\| = \sqrt{\sum_{i=0}^{m} r_i^2 \|v^*_{\sigma(i)}\|^2 + \|\omega\|^2} \geq |r_m| \|v^*_{\sigma(m)}\|.$$

Moreover, we have

$$\langle v^*_{\sigma(m)}, C \rangle = a_m \|v^*_{\sigma(m)}\|^2 + r_m \|v^*_{\sigma(m)}\|^2$$

i.e.

$$\frac{\langle v^*_{\sigma(m)}, C \rangle}{\|v^*_{\sigma(m)}\|^2} = a_m + r_m.$$

Since $|r_m| \|v^*_{\sigma(m)}\| \leq \|r\| \leq b/2$, then $|r_m| \leq \dfrac{b}{2\|v^*_{\sigma(m)}\|}$. If $\|v^*_{\sigma(m)}\| > b$, then $|r_m| < 1/2$, we will have

$$a_m = \begin{cases} 1, & \text{if } \dfrac{\langle v^*_{\sigma(m)}, C \rangle}{\|v^*_{\sigma(m)}\|^2} \in (\dfrac{1}{2}, \dfrac{3}{2}) \ ; \\ 0, & \text{if } \dfrac{\langle v^*_{\sigma(m)}, C \rangle}{\|v^*_{\sigma(m)}\|^2} \in (-\dfrac{1}{2}, \dfrac{1}{2}). \end{cases}$$

If we have recovered a_m, substituting C by $C - a_m v_{\sigma(m)}$, and use the same method to recover a_{m-1}. The process can be continued until all a_i are recovered if $\|v^*_{\sigma(i)}\| > b$ stands for all $i \in \{0, 1, \cdots, m\}$.

It remains to show that $\|v^*_{\sigma(i)}\| > b$. Next, we prove that with probability very near 1, $\|v^*_{\sigma(i)}\| > b$ for all $i \in \{0, 1, \cdots, m\}$.

3.2 Probability Analysis

First, we prove some lemmas and always suppose $i \leq m = \lfloor \frac{1}{2}n \rfloor$.

Lemma 1. *Let $w \in S_+^{n-1} = \{x \in \mathbb{R}^n | \|x\| = 1, \langle x, u \rangle > 0\}$ be uniformly distributed on the unit (northern) hemisphere. Let u be the north pole. Then*

$$\boldsymbol{Pr}[\langle u, w \rangle > t] = \int_0^{\arccos(t)} \frac{\sin^{n-2}(\theta)}{I_{n-2}} d\theta$$

where $0 \leq t \leq 1$, and $I_{n-2} = \int_0^{\frac{\pi}{2}} \sin^{n-2}(\theta) d\theta$.

Proof. Since in [4], for $w \in S_+^{n-1}$, the density function for the value of the dot product $h = \langle w, u \rangle$ is

$$p_{n-1}(h) = (\sqrt{1-h^2})^{n-3}/I_{n-2}.$$

Hence

$$\mathbf{Pr}[\langle u, w \rangle > t] = \int_t^1 p_{n-1}(h) dh = \int_0^{\arccos(t)} \frac{\sin^{n-2}(\theta)}{I_{n-2}} d\theta$$

when we take $h = \cos(\theta)$. □

Corollary 1. *Choose w uniformly at random from S^{n-1}, then*

$$\boldsymbol{Pr}[|\langle w, u \rangle| > t] = \boldsymbol{Pr}[\langle w, u \rangle > t] = \int_0^{\arccos(t)} \frac{\sin^{n-2}(\theta)}{I_{n-2}} d\theta.$$

Corollary 2. *If t is small enough, we have*

$$\int_0^{\arccos(t)} \frac{\sin^{n-2}(\theta)}{I_{n-2}} d\theta > 1 - \frac{t}{I_{n-2}} \approx 1 - \frac{t\sqrt{2(n-2)}}{\sqrt{\pi}}.$$

Proof. We have

$$\int_0^{\arccos(t)} \frac{\sin^{n-2}(\theta)}{I_{n-2}} d\theta = 1 - \frac{\int_{\arccos(t)}^{\frac{\pi}{2}} \sin^{n-2}(\theta) d\theta}{I_{n-2}} > 1 - \frac{\frac{\pi}{2} - \arccos(t)}{I_{n-2}}.$$

Let $\beta = \frac{\pi}{2} - \arccos(t)$, then $\sin(\beta) = t$. Since t is small enough, so $\beta \approx \sin(\beta) = t$, and we know $I_n \approx \sqrt{\frac{\pi}{2n}}$ in [4], the corollary follows. □

Theorem 1. *Given $v_0, v_1, \cdots, v_{i-1}$, choose v_i uniformly at random from $\{x \in \mathbb{R}^n | \|x\| = L\}$, where $L \gg b$, then*

$$\boldsymbol{Pr}[\|v_i^*\| > b] > 1 - \frac{b\sqrt{2(n-2)}}{L\sqrt{\pi}}.$$

Proof. Given $v_0, v_1, \cdots, v_{i-1}$, we can get the corresponding Gram-Schmidt orthogonalization $v_0^*, v_1^*, \cdots, v_{i-1}^*$, and choose a normal orthogonal basis $u_i, u_{i+1}, \cdots, u_{n-1}$ of $span(v_0^*, v_1^*, \cdots, v_{i-1}^*)^\perp$. For any $v_i \in \{x \in \mathbb{R}^n | \|x\| = L\}$, v_i can be written as

$$v_i = t_0 v_0^* + \cdots + t_{i-1} v_{i-1}^* + t_i u_i + \cdots + t_{n-1} u_{n-1}.$$

Then

$$v_i^* = t_i u_i + \cdots + t_{n-1} u_{n-1}.$$

so $\|v_i^*\| \geq |t_{n-1}| \|u_{n-1}\| = |t_{n-1}| = |\langle v_i, u_{n-1} \rangle| = L|\langle \frac{1}{L} v_i, u_{n-1} \rangle|$. Since $L \gg b$,

$$\mathbf{Pr}[\|v_i^*\| > b] \geq \mathbf{Pr}[|\langle \frac{1}{L} v_i, u_{n-1} \rangle| > \frac{b}{L}] > 1 - \frac{b\sqrt{2(n-2)}}{L\sqrt{\pi}}$$

by Corollary 1 and Corollary 2. Notice that $1 - \frac{b\sqrt{2(n-2)}}{L\sqrt{\pi}}$ is very near 1. □

Lemma 2. *For any permutation τ on i letters, denote $v_0^*, v_1^*, \cdots, v_i^*$ the Gram-Schmidt orthogonalization of $v_0, v_1, \cdots, v_i$, and $v_{\tau(0)}^\dagger, \cdots, v_{\tau(i-1)}^\dagger, v_i^\dagger$ the Gram-Schmidt orthogonalization of $v_{\tau(0)}, \cdots, v_{\tau(i-1)}, v_i$, then $v_i^* = v_i^\dagger$.*

Proof. Since v_i can be uniquely written as $v_i = \mu + \nu$, where $\mu \in span(v_0, \cdots, v_{i-1}), \nu \in span(v_0, \cdots, v_{i-1})^\perp$, so $v_i^* = \nu = v_i^\dagger$. □

As Cai and Cusick proposed, we choose $v_0, \cdots, v_m$ uniformly at random from $H_{N_0}(u), \cdots, H_{N_m}(u)$ respectively, and $N_k > \sum_{i=0}^{k-1} N_i + b$ for $k = 1, \cdots, m$ and $N_0 > b$, with $\|v_k\| = B \gg 2^n$. Moreover, v_k can be uniquely written as

$$v_k = N_k u + \sqrt{B^2 - N_k^2}\rho_k \tag{1}$$

where $\langle u, \rho_k \rangle = 0$ and $\|\rho_k\| = 1$. Let $\eta_k = \sqrt{B^2 - N_k^2}\rho_k$, we denote $\eta_0^*, \eta_1^*, \cdots, \eta_i^*$ the Gram-Schmidt orthogonalization of $\eta_0, \eta_1, \cdots, \eta_i$. Let $v_0^*, v_1^*, \cdots, v_i^*$ be the Gram-Schmidt orthogonalization of $v_0, v_1, \cdots, v_i$, and $u^\dagger, v_0^\dagger, v_1^\dagger, \cdots, v_i^\dagger$ be the Gram-Schmidt orthogonalization of $u, v_0, v_1, \cdots, v_i$, we have:

Lemma 3. $\|v_i^*\| \geq \|v_i^\dagger\| = \|\eta_i^*\|$.

Proof. If we denote $v_0^\ddagger, v_1^\ddagger, \cdots, v_{i-1}^\ddagger, u^\ddagger, v_i^\ddagger$ the Gram-Schmidt orthogonalization of $v_0, v_1, \cdots, v_{i-1}, u, v_i$, then obviously we have $\|v_i^*\| \geq \|v_i^\ddagger\|$. By Lemma 2, $\|v_i^\ddagger\| = \|v_i^\dagger\|$, so $\|v_i^*\| \geq \|v_i^\dagger\|$.

Next, we prove $v_i^\dagger = \eta_i^*$ by induction. $v_0^\dagger = v_0 - \frac{\langle v_0, u\rangle}{\langle u, u\rangle}u = \eta_0^*$. Suppose $v_j^\dagger = \eta_j^*$ holds for $j \le k$, then

$$\begin{aligned} v_{k+1}^\dagger &= v_{k+1} - \frac{\langle v_{k+1}, u\rangle}{\langle u, u\rangle}u - \sum_{j=0}^{k}\frac{\langle v_{k+1}, v_j^\dagger\rangle}{\langle v_j^\dagger, v_j^\dagger\rangle}v_j^\dagger \\ &= \eta_{k+1} - \sum_{j=0}^{k}\frac{\langle v_{k+1}, \eta_j^*\rangle}{\langle \eta_j^*, \eta_j^*\rangle}\eta_j^* \\ &= \eta_{k+1} - \sum_{j=0}^{k}\frac{\langle \eta_{k+1}, \eta_j^*\rangle}{\langle \eta_j^*, \eta_j^*\rangle}\eta_j^* \\ &= \eta_{k+1}^*. \end{aligned}$$

So the lemma follows. □

By induction we can also prove that $N_i > 2^i b$. Since $B \gg 2^n$ and $B \ge N_m$, it's reasonable to believe that $\sqrt{B^2 - N_i^2} \gg b$ for $i \in \{0, 1, \cdots, m\}$. In fact, we won't choose b too large in the real life, otherwise the entries of every v_k may be huge. Moreover, if $\frac{\sqrt{B^2 - N_m^2}}{B} = \sqrt{1 - (\frac{N_m}{B})^2}$ is too small, or equivalently, $\frac{N_m}{B}$ is too near 1, then $\frac{1}{B}v_m$ will be a good approximation to u, so we can try all the $\frac{1}{B}v_{\sigma(i)}$'s to decrypt some ciphertexts, and will easily get $\frac{1}{B}v_m$ as u to break the cryptosystem. Even when $B > \sqrt{1 + 2^{-m}}N_m$,

$$\frac{b}{\sqrt{B^2 - N_i^2}} < \frac{b}{\sqrt{(1 + 2^{-m})N_m^2 - N_m^2}} = \frac{b}{\sqrt{2^{-m}N_m^2}} < \frac{b}{\sqrt{2^{-m}2^{2m}b^2}} < \frac{1}{2^{\frac{m}{2}}}$$

is very small. So, we always suppose $\frac{b}{\sqrt{B^2 - N_i^2}}$ is small enough below.

Theorem 2. *If we choose $v_0, \cdots, v_m$ uniformly at random from $H_{N_0}(u), \cdots, H_{N_m}(u)$ respectively with $\|v_i\| = B$ for $i = 0, \cdots, m$, then*

$$\boldsymbol{Pr}[\|v_i^*\| > b] > 1 - \frac{b\sqrt{2(n-3)}}{\sqrt{B^2 - N_i^2}\sqrt{\pi}}.$$

Proof. Choosing v_i uniformly at random from $H_{N_i}(u)$ is equivalent to choosing ρ_i uniformly at random from $\{x \in \mathbb{R}^n | \langle x, u\rangle = 0, \|x\| = 1\}$ by (1). Using the similar method to prove Theorem 1, we can prove $\mathbf{Pr}[\|\eta_i^*\| > b] > 1 - \frac{b\sqrt{2(n-3)}}{\sqrt{B^2 - N_i^2}\sqrt{\pi}}$, then by Lemma 3 , the theorem follows. □

Notice that the proof of Theorem 2 just depends on the lengths N_i's but independent of the order $N_0 < N_1 < \cdots < N_m$. Hence, it still holds when we take a permutation σ:

Corollary 3. *If we choose $v_0, \cdots, v_m$ uniformly at random from $H_{N_0}(u), \cdots, H_{N_m}(u)$ respectively with $\|v_i\| = B$, for $i = 0, \cdots, m$, then for any permutation σ on $m+1$ letters we have*

$$\boldsymbol{Pr}[\|v^*_{\sigma(i)}\| > b] > 1 - \frac{b\sqrt{2(n-3)}}{\sqrt{B^2 - N^2_{\sigma(i)}}\sqrt{\pi}}.$$

Corollary 4. *If we choose $v_i = 2^i b'u + \sqrt{B^2 - 2^{2i}b'^2}\rho_i$ as Cai and Cusick proposed, and suppose $\sqrt{B^2 - 2^{2i}b'^2} \gg b$, for $i = 0, \cdots, m$, then for any permutation σ on $m+1$ letters we have*

$$\boldsymbol{Pr}[\|v^*_{\sigma(i)}\| > b] > 1 - \frac{b\sqrt{2(n-3)}}{\sqrt{B^2 - 2^{2\sigma(i)}b'^2}\sqrt{\pi}}.$$

Remark 3. *From the results above, $\|v^*_{\sigma(i)}\| > b$ holds with probability near 1, so we can use our method to attack the Cai-Cusick Cryptosystem successfully with probability near 1. In fact, if for some i, it happens that $\|v^*_{\sigma(i)}\| \leq b$, and suppose the unknown bits of the message then are $a_{k_0}, \cdots, a_{k_s}$, then we can try all k_j's where $j = 0, \cdots, s$ and $k_j \neq \sigma(i)$ to compute the Gram-Schmidt orthogonalization of $v_{k_0}, \cdots, v_{k_{j-1}}, v_{k_{j+1}} \cdots, v_{k_j}$, until we find $\|v^*_l\| > b$ for some l, then we recover a_l first. In our experiments, it happens that $\|v^*_{\sigma(i)}\| > b$ all the time.*

As we see, the main work in our attack is to compute the Gram-Schmidt orthogonalization of $v_{\sigma(0)}, v_{\sigma(1)}, \cdots, v_{\sigma(m)}$ and this can be precomputed with $O(n^3)$ multiplications. After we have done this, the main computations involved in our attack is just to compute $m+1$ dot products which just costs $O(n^2)$ multiplications.

4 Two Chosen-Ciphertext Attacks

Since σ is essential to the security of the cryptosystem, we give two chosen-ciphertext attacks to recover σ and then use linear programming to break the cryptosystem.

Assume we have a decryption oracle $\mathcal{D}$ which works as the decryption algorithm, we query $\mathcal{D}$ with a vector $C \in \mathbb{R}^n$, and will get $M = \mathcal{D}(C)$, if C is a cipher, then M is the corresponding message.

We say $v_i < v_j$ if $N_i < N_j$, or equivalently, $i < j$, so if we have gotten $v_{\sigma(i_0)} < v_{\sigma(i_1)} < \cdots < v_{\sigma(i_m)}$, then $\sigma(i_k) = k$, for $k = 0, \cdots, m$, hence we recover σ.

4.1 The Foundation of the Chosen-Ciphertext Attack

Let $P_I = [\sum_{i\in I} N_i - b/2, \sum_{i\in I} N_i + b/2] = \{x \in \mathbb{R} | \sum_{i\in I} N_i - b/2 \le x \le \sum_{i\in I} N_i + b/2\}$, where I is a subset of $\{0, 1, \cdots, m\}$, $CS = \{P_I | I \subseteq \{0, 1, \cdots, m\}\}$, $center(P_I) = \sum_{i\in I} N_i$. We say $P_I < P_J$ if $center(P_I) < center(P_J)$. So we can order all the elements in CS as below:

$$P_\emptyset < P_{I_1} < P_{I_2} < \cdots < P_{\{0,1,\cdots,m\}}.$$

We define I° for $I \neq \emptyset$ such that P_{I° is the nearest one before P_I in the sequence above, i.e. for any $P_J < P_I$, $J \neq I^\circ$, we have $P_J < P_{I^\circ}$.

The lemma below can be easily gotten:

Lemma 4. *$P_I \bigcap P_J = \emptyset$, if $I \neq J$.*

Proof. Suppose $P_I < P_J$, since $I \neq J$,

$$(\sum_{i\in J} N_i - b/2) - (\sum_{i\in I} N_i + b/2) > b - b = 0.$$

□

Let the message space $MS = \{(a_0, a_1, \cdots, a_m) | a_i \in \{0, 1\}\}$, and we define a $1-1$ map φ from CS to MS:

$$\varphi : CS \to MS$$

by $\varphi(P_I) = (a_0, a_1, \cdots, a_m)$, where

$$a_i = \begin{cases} 1, & \text{if } \sigma(i) \in I; \\ 0, & \text{otherwise.} \end{cases}$$

Notice that for any ciphertext C, the corresponding message M is decided only by $\langle u, C\rangle$, so we get our basic theorem. Before stating the theorem, we prove some lemmas first.

Lemma 5. *For any $C \in \mathbb{R}^n$, there must exist an $I \subseteq \{0, 1, \cdots, m\}$, s.t. $center(P_{I^\circ}) - b/2 \le \langle u, C\rangle < center(P_I) - b/2$, if $-b/2 \le \langle u, C\rangle < center(P_{\{0,1,\cdots,m\}}) - b/2$.*

We define $I(u, C) = I^\circ$ as in Lemma 5.

Lemma 6. *If $I = \{i\}$, then $I^\circ = \{0, 1, \cdots, i-1\}$ is the set consists of all the non-negtive integer less than i.*

Proof. For any $k \in \{i, i+1, \cdots, m\}$, $N_k \ge center(P_I)$, so $k \notin I^\circ$. For any subset $I' \subset \{0, 1, \cdots, i-1\}$, it is obvious that $P_{I'} < P_{\{0,1,\cdots,i-1\}}$, so $I^\circ = \{0, 1, \cdots, i-1\}$. □

Lemma 7. *If $|I| > 1$, and denote $max(I)$ the maximal element in I, then $max(I) = max(I^\circ)$ and $(I - \{max(I)\})^\circ = I^\circ - \{max(I)\}$.*

Proof. First, if $|I| > 1$, we prove $max(I) = max(I^\circ)$. Otherwise, if $max(I) \neq max(I^\circ)$, then $max(I) > max(I^\circ)$. Let $I' = \{max(I)\}$, then $P_{I^\circ} < P_{I'} < P_I$, contradiction.

If $(I - \{max(I)\})^\circ \neq I^\circ - \{max(I)\}$, then $P_{I^\circ - \{max(I)\}} < P_{(I-\{max(I)\})^\circ}$, since $P_{I^\circ - \{max(I)\}} < P_{I-\{max(I)\}}$. So,

$$P_{(I^\circ - \{max(I)\}) \bigcup \{max(I)\}} < P_{(I-\{max(I)\})^\circ \bigcup \{max(I)\}} < P_{(I-\{max(I)\}) \bigcup \{max(I)\}} = P_I$$

i.e.

$$P_{I^\circ} < P_{(I-\{max(I)\})^\circ \bigcup \{max(I)\}} < P_I$$

contradiction. □

By Lemma 6 and Lemma 7, we can easily get our theorem below:

Theorem 3. *For any $C \in \mathbb{R}^n$, we have*

$$\mathcal{D}(C) = \begin{cases} (0, 0, \cdots, 0), & \text{if } \langle u, C\rangle < N_0 - b/2; \\ \varphi(P_{I(u,C)}), & \text{if } -b/2 \leq \langle u, C\rangle < center(P_{\{0,1,\cdots,m\}}) - b/2; \\ (1, 1, \cdots, 1), & \text{if } \langle u, C\rangle \geq center(P_{\{0,1,\cdots,m\}}) - b/2. \end{cases}$$

4.2 The First Chosen-Ciphertext Attack

We claim that

Lemma 8. *if $\{\sigma(i)\} \bigcup \{\sigma(j)\} \neq \{0, 1\}, i \neq j$, then*

$$\mathcal{D}(v_{\sigma(i)} - v_{\sigma(j)}) = \begin{cases} (0, 0, \cdots, 0), & \text{if } v_{\sigma(i)} < v_{\sigma(j)}; \\ (a_0, a_1, \cdots, a_m), & \exists i \in \{0, 1, \cdots, m\}, s.t. a_i = 1, \text{ otherwise.} \end{cases}$$

Proof. By Theorem 3, if $v_{\sigma(i)} < v_{\sigma(j)}$, then $\langle u, v_{\sigma(i)} - v_{\sigma(j)}\rangle < 0$, so we get $(0, 0, \cdots, 0)$. If $v_{\sigma(j)} < v_{\sigma(i)}$ and $\{\sigma(i)\} \bigcup \{\sigma(j)\} \neq \{0, 1\}$, $\langle u, v_{\sigma(i)} - v_{\sigma(j)}\rangle = N_{\sigma(i)} - N_{\sigma(j)} > \sum_{k=0, k\neq\sigma(j)}^{\sigma(i)-1} N_k + b > N_0$, so we can get the message $(a_0, a_1, \cdots, a_m)$, satisfying there exists i s.t. $a_i = 1$. □

The First Chosen-Ciphertext Attack: For all $\frac{m(m+1)}{2}$ pairs $v_{\sigma(i)}, v_{\sigma(j)}$, if $\mathcal{D}(v_{\sigma(i)} - v_{\sigma(j)}) = (0, 0, \cdots, 0)$, we suppose $v_{\sigma(i)} < v_{\sigma(j)}$, and $v_{\sigma(j)} < v_{\sigma(i)}$, otherwise. After having done this, we get $v_{\sigma(i_0)}, v_{\sigma(i_1)}, \cdots, v_{\sigma(i_m)}$ and hope that $v_{\sigma(i_0)} < v_{\sigma(i_1)} <$

$\cdots < v_{\sigma(i_m)}$. According to Lemma 8, we know that $\sigma(i_j) = j, j > 1$. It remains to decide if $v_{\sigma(i_0)} < v_{\sigma(i_1)}$. Assume $v_{\sigma(i_0)} < v_{\sigma(i_1)}$, we can get σ' and u' as private key, choose message $(a_0, a_1, \cdots, a_m)$, where $a_{i_0} = 1$ and the others are 0, let C be the corresponding ciphertext. If we can get the correct message using σ' and u', then $v_{\sigma(i_0)} < v_{\sigma(i_1)}$, else $v_{\sigma(i_1)} < v_{\sigma(i_0)}$.

4.3 The Second Chosen-Ciphertext Attack

The Second Chosen-Ciphertext Attack: If we have a vector $w \in \mathbb{R}^n$ s.t. $\langle u, w\rangle = b$, then for any $k \in \{0, 1, \cdots, m\}$, $N_0 - b \leq \langle u, v_{\sigma(k)} - w\rangle \leq N_m - b$, so

$$\mathcal{D}(v_{\sigma(k)} - w) = \varphi(P_{I(u, v_{\sigma(k)} - w)}) = (a_0, a_1, \cdots, a_m).$$

Since $\sum_{i=0}^{\sigma(k)-1} N_i < \langle u, v_{\sigma(k)} - w\rangle = N_{\sigma(k)} - b < center(P_{\{\sigma(k)\}}) - \frac{b}{2}$, then $I(u, v_{\sigma(k)} - w) = \{0, 1, \cdots, \sigma(k) - 1\}$ by Lemma 6. Hence we check the a_i's, if $a_i = 1$, then $v_{\sigma(i)} < v_{\sigma(k)}$, else $v_{\sigma(k)} < v_{\sigma(i)}$.

Therefore, we can decrypt $v_{\sigma(i)} - w$ for some i's, until we get $v_{\sigma(i_0)} < v_{\sigma(i_1)} < \cdots < v_{\sigma(i_m)}$ to recover σ. Moreover, to recover σ, we only need query the oracle $\mathcal{D}$ for $\lceil \log_2(m) \rceil$ times at the best case, and $m - 1$ times at the worst case , much less than $\frac{m(m+1)}{2}$ times in the first attack.

It remains to find w. Choose randomly $v \in \{v_{\sigma(0)}, v_{\sigma(1)}, \cdots, v_{\sigma(m)}\}$, since $\langle u, v\rangle > 0$, then we try to find a real number $s > 0$ by using bisection method, s.t. $\mathcal{D}(sv) = (0, 0, \cdots, 0)$ but $\mathcal{D}((s + \epsilon)v) \neq (0, 0, \cdots, 0)$, where $\epsilon > 0$ we set first is small enough, then $\langle u, sv\rangle \approx N_0 - b/2$, let $w = \frac{b}{N_0 - b/2} sv$, then $\langle u, w\rangle \approx b$.

Remark 4. *Notice that although the vector C we choose to query the oracle $\mathcal{D}$ may not be a legal ciphertext, the oracle $\mathcal{D}$ still decrypt it. If we only have another oracle $\mathcal{D}'$ which just gives an alert when the vector C is an illegal ciphertext instead of decrypting it, we may spend more time to find a proper real number $s > 0$ by bisection method, such that sC is not only a legal ciphertext, but also meets the need as in querying $\mathcal{D}$.*

5 Conclusion

As we see, the Cai-Cusick lattice-based public-key cryptosystem is not secure. We present a ciphertext-only attack and prove that it will succeed with probability very near 1 to recover the message in short time. What's more, our experiments support our view very well. The two efficient chosen-ciphertext attacks in Section

4 show that the private key of the cryptosystem is easy to be recovered under the chosen-ciphertext attack.

References

[1] M. Ajtai: Gennerating hard instances of lattice problems. *In Proc. of 28th STOC*, pages 99-108. ACM, 1996.

[2] M. Ajtai: Representing hard lattices with $O(n \log n)$ bits. *In Proc. of 37th STOC*, pages 94-103. ACM, 2005.

[3] M. Ajtai and C. Dwork: A public-key cryptosystem with worst-case/average-case equivalence. *In Proc. of 29th STOC*, pages 284-293. ACM, 1997.

[4] J.-Y. Cai and T.W. Cusick: A lattice-based public-key cryptosystem. *In Proc. of SAC'98*, volume 1556 of *LNCS*, pages 219-233. Springer-Verlag, 1999.

[5] J.-Y. Cai and T.W. Cusick: A lattice-based public-key cryptosystem. Information and Computation, 151: 17-31, 1999.

[6] R. Fischlin and J.-P. Seifert: Tensor-based trapdoors for CVP and their application to public key cryptography(Extended Abstract). *In Proc. of IMA Conference on Cryptography and Coding*, volume 1746 of *LNCS*, pages 244-257. Springer-Verlag, 1999.

[7] O. Goldreich, S. Goldwasser, and S. Halevi: Public-key cryptosystems from lattice reduction problems. *In Proc. of Crypto'97*, volume 1294 of *LNCS*, pages 112-131. Springer-Verlag, 1997.

[8] J. Hoffstein, J. Pipher, J.H. Silverman: NTRU: A Ring-Based Public Key Cryptosystem. *In Proc. of Algorithmic Number Theory*, volume 1423 of *LNCS*, pages 267-288. Springer-Verlag, 1998.

[9] P. Nguyen and J. Stern: Cryptanalysis of the Ajtai-Dwork cryptosystem. *In Proc. of Crypto'98*, volume 1462 of *LNCS*, pages 223-242. Springer-Verlag, 1998.

[10] O. Regev: New lattice-based cryptographic constructions. J. ACM, 51(6): 899-942, 2004.

[11] O. Regev: On lattices, learning with errors, random linear codes, and cryptography. *In Proc. of 37th STOC*, pages 84-93. ACM, 2005.