A Ciphertext-Only Attack Against the Cai-Cusick Lattice-Based Public-Key Cryptosystem

Yanbin Pan and Yingpu Deng

***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.**

***Index Terms*—Cai-Cusick cryptosystem, ciphertext-only attack, Gram-Schmidt orthogonalization, lattice.**

I. 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. Ajtai and Dwork [3] proposed the first lattice-based public-key cryptosystem whose security is based on the worst-case hardness assumptions. After their results, several lattice-based cryptosystems [8], [9], [5], [7], [11], [12], [2] have been proposed.

Lattice-based cryptosystems have many advantages: first, the computations involved are very simple and usually require only modular addition; second, by now they have resisted the cryptanalysis by quantum algorithms whereas there already exist the efficient quantum algorithms [13] for factoring integers and computing discrete logarithms. It is very significant to construct a lattice-based cryptosystem which has both the security based on the worst-case hardness and the efficiency on the speed, key size, expansion rate and so on. However, the fact is that the presented lattice-based cryptosystems which are efficient have no security proofs based on the worst-case hardness whereas most of those which have security proofs are not efficient.

Although the Ajtai-Dwork cryptosystem was thought to be secure if a particular lattice problem is difficult in the worst-case, Nguyen and Stern [10] gave a heuristic attack to show that in order to be secure, the implementations of the Ajtai-Dwork cryptosystem would require very large keys, making it impractical in a real-life environment.

Manuscript received May 12, 2008; revised September 13, 2009; accepted September 10, 2010. Date of current version February 18, 2011. This work was supported in part by the NNSF of China (No. 11071285 and No. 60821002) and in part by 973 Project (No. 2011CB302401).

The authors are with the Key Laboratory of Mathematics Mechanization, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China (e-mail: panyanbin@amss.ac.cn; dengyp@amss.ac.cn).

Communicated by A. Canteaut, Associate Editor for Complexity and Cryptography.

Digital Object Identifier 10.1109/TIT.2010.2103790

In 1998, Cai and Cusick [5] 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 this paper, we present an efficient ciphertext-only attack against the Cai-Cusick lattice-based public-key cryptosystem to recover the message. The probability analysis shows that the attack succeeds with probability very close to 1. Moreover, experimental results also show that it always succeeds to recover the message efficiently. So the Cai-Cusick cryptosystem is not secure.

As far as we know, it's the first cryptanalysis of the Cai-Cusick lattice-based public-key cryptosystem.

The remainder of the paper is organized as follows. In Section II, we give some notations and preliminaries needed. In Section III, we describe the Cai-Cusick lattice-based public-key cryptosystem and the parameter selection. In Section IV, we present our ciphertext-only attack to recover the message and give some theoretical and experimental results about the attack. Finally, we give a short conclusion in Section V.

II. Notations and Preliminaries

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

We recall the Gram-Schmidt orthogonalization process. Let $v_1,v_2,\ldots,v_m \in \mathbb{R}^n$ be linearly independent vectors. The Gram-Schmidt orthogonalization $v_1^*,v_2^*,\ldots,v_m^*$ is the orthogonal family defined as follows: v_i^* is the component of v_i orthogonal to $\mathrm{span}(v_1,v_2,\ldots,v_{i-1})$. More explicitly, the vectors v_i^* $(1 \le i \le m)$ are defined by

$$v_1^* = v_1,$$
$$v_i^* = v_i - \sum_{j=1}^{i-1} \mu_{i,j} v_j^* \quad \text{for } i > 1$$

where $\mu_{i,j} = \langle v_i, v_j^*\rangle / \langle v_j^*, v_j^*\rangle$.

Obviously, the Gram-Schmidt orthogonalization family depends on the order of the vectors, but the following property shows that v_i^* doesn't depend on the order of the vectors before it.

Property 1: For any permutation τ on $i-1$ letters, denote by $v_1^*, v_2^*, \ldots, v_i^*$ the Gram-Schmidt orthogonalization of $v_1, v_2, \ldots, v_i$, and by $v_{\tau(1)}^\dagger, v_{\tau(2)}^\dagger, \ldots, v_{\tau(i-1)}^\dagger, v_i^\dagger$ the Gram-Schmidt orthogonalization of $v_{\tau(1)}, v_{\tau(2)}, \ldots, v_{\tau(i-1)}, v_i$, then $v_i^* = v_i^\dagger$.

Proof: Since v_i can be uniquely written as $v_i = \mu + \nu$, where $\mu \in \mathrm{span}(v_1, v_2, \ldots, v_{i-1})$, $\nu \in \mathrm{span}(v_1, v_2, \ldots, v_{i-1})^\perp$, so $v_i^* = \nu = v_i^\dagger$. ∎

We will show that the Gram-Schmidt orthogonalization can be computed efficiently. To compute each $v_i^* (1 \le i \le m)$, for every j, $1 \le j \le i-1$, we need $2n$ multiplications to compute $\mu_{i,j}$, since n multiplications is needed to compute every dot product. We still need n multiplications to compute $\mu_{i,j} v_j^*$. So $(i-1) \cdot 3n$ multiplications are needed to compute each v_i^*. Hence, to complete the Gram-Schmidt orthogonalization, we need $\sum_{i=1}^{m} (i-1) \cdot 3n = \frac{3}{2} m(m-1)n$, i.e., $O(m^2 n)$ multiplications.

We next give some preliminaries and results used in the probability analysis in Section IV. We use the uniform distribution U on a set S, namely the Lebesgue measure on S, and denote a random variable X uniformly distributed on S by $X \in_U S$. As in [5], for clarity of presentation, we also state all results in terms of the exact Lebesgue measure, ignoring the exponentially small and insignificant errors occurring in the actual cryptographic protocols in which we use exponentially close approximations on $\mathbb{Q}$ instead of the exact values in $\mathbb{R}$.

Proposition 1: For $n \ge 2$, let $u \in \mathbb{R}^n$ be the north pole and $w \in S_+^{n-1} = \{x \in \mathbb{R}^n \mid \|x\| = 1, \langle x, u \rangle > 0\}$ be uniformly distributed on the unit (northern) hemisphere, then for $0 \le t \le 1$,

$$\mathop{\mathbf{Pr}}_{w \in_U S_+^{n-1}} [\langle u, w \rangle > t] = \int_0^{\arccos t} \frac{\sin^{n-2}\theta}{I_{n-2}} d\theta$$

where $I_{n-2} = \int_0^{\frac{\pi}{2}} \sin^{n-2}\theta d\theta$.

Proof: Since in [5], for $w \in_U S_+^{n-1}$, the density function for the value of the dot product $h = \langle w, u \rangle$ is

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

Hence

$$\begin{aligned} \mathop{\mathbf{Pr}}_{w \in_U S_+^{n-1}} [\langle u, w \rangle > t] &= \int_t^1 p_{n-1}(h) dh \\ &= \int_0^{\arccos t} \frac{\sin^{n-2}\theta}{I_{n-2}} d\theta \end{aligned}$$

where we substitute h by $\cos\theta$. ∎

Corollary 1: Let $n \ge 4$ and w be chosen uniformly at random from S^{n-1}, then for $0 < t < \frac{\sqrt{3}}{2}$,

$$\begin{aligned} \mathop{\mathbf{Pr}}_{w \in_U S^{n-1}} [|\langle w, u \rangle| > t] &= \int_0^{\arccos t} \frac{\sin^{n-2}\theta}{I_{n-2}} d\theta \\ &> 1 - \frac{4(n-2)}{\pi} t. \end{aligned}$$

Proof: By the symmetry of S^{n-1}, we have

$$\begin{aligned} \mathop{\mathbf{Pr}}_{w \in_U S^{n-1}} [|\langle w, u \rangle| > t] &= \mathop{\mathbf{Pr}}_{w \in_U S_+^{n-1}} [\langle u, w \rangle > t] \\ &= \int_0^{\arccos t} \frac{\sin^{n-2}\theta}{I_{n-2}} d\theta \\ &= 1 - \frac{\int_{\arccos t}^{\frac{\pi}{2}} \sin^{n-2}\theta d\theta}{I_{n-2}} \\ &> 1 - \frac{\frac{\pi}{2} - \arccos t}{I_{n-2}}. \end{aligned}$$

Let $\beta = \frac{\pi}{2} - \arccos t$, then $\sin\beta = t$. Since $0 < t < \frac{\sqrt{3}}{2}$, we have

$$\beta < \tan\beta = \frac{t}{\sqrt{1-t^2}} < 2t.$$

Next we show that $I_n \ge \frac{\pi}{2n}$ for $n \ge 2$. We have $I_n = \int_0^{\frac{\pi}{2}} \sin^n \theta d\theta = \frac{n-1}{n} I_{n-2}$. If n is even, then $I_n = \frac{n-1}{n}\frac{n-3}{n-2}\cdots\frac{1}{2} I_0 = \frac{1}{n}\frac{n-1}{n-2}\frac{n-3}{n-4}\cdots\frac{3}{2}\frac{\pi}{2} \ge \frac{\pi}{2n}$. If n is odd, then $I_n = \frac{n-1}{n}\frac{n-3}{n-2}\cdots\frac{2}{3} I_1 = \frac{1}{n}\frac{n-1}{n-2}\frac{n-3}{n-4}\cdots\frac{4}{3}\frac{2}{1} \ge \frac{2}{n} > \frac{\pi}{2n}$. So for $n \ge 4$,

$$I_{n-2} \ge \frac{\pi}{2(n-2)}.$$

Then the corollary follows. ∎

III. The Cai-Cusick Cryptosystem

We just give a simple description of the Cai-Cusick cryptosystem in this section and more details see [5] or [6].

A. Description of the Cai-Cusick Cryptosystem

We recall that $H_i(u) = \{x \in \mathbb{R}^n \mid \langle x, u \rangle = i\}$, where $i \in \mathbb{Z}^+$, $u \in S^{n-1}$.

Parameters: n and m.

Key Generation:

- Select u uniformly at random from S^{n-1}.
- Select a real number $b > 0$.
- Select $v_0, v_1, \ldots, v_m$ uniformly at random from $H_{N_0}(u), H_{N_1}(u), \ldots, H_{N_m}(u)$ respectively, where $m = \lfloor cn \rfloor$, for some $c < 1$, $N_k > \sum_{i=0}^{k-1} N_i + b$ for $k = 1, 2, \ldots, m$ and $N_0 > b$.
- Select randomly a permutation σ on $m+1$ letters.

Public Key: $v_{\sigma(0)}, v_{\sigma(1)}, \ldots, v_{\sigma(m)}$ and b.

Private Key: $u, N_0, N_1, \ldots, N_m$ and σ.

Encryption: Denote by $M = (a_0, a_1, \ldots, a_m)$ the message, where $a_i \in \{0, 1\}$ and C the ciphertext. To encrypt M, we first select r uniformly at random from $\{x \in \mathbb{R}^n \mid \|x\| \le b/2\}$, then compute

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

Decryption: We first compute

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

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

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

Having gotten $a_{\sigma^{-1}(m)}$, we then substitute S by $S - a_{\sigma^{-1}(m)} N_m$ and recover $a_{\sigma^{-1}(m-1)}$ similarly. It is easy to see that we can continue the process until all $a_{\sigma^{-1}(i)}$'s are recovered. Then, we use σ to recover M.

B. Parameter Selection

Cai and Cusick [5] gave some suggestions for the parameter selection to resist some potential attacks. For any parameter n, they suggested that:

- $m = \lfloor \frac{1}{2} n \rfloor$.
- b is an arbitrary positive real number.
- They suggested keeping all the lengths of the vectors $v_i (0 \le i \le m)$ essentially the same, or there could be statistical leakage of information. We denote the same length by B. However, suppose the v_i's are all roughly the same length, then m should be less than n. If $m > n$, there is a cryptanalytic attack.
- 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. In such distribution of v_i, there is no easy statistical leakage.

We denote by CC the Cai-Cusick cryptosystem generated as Cai and Cusick proposed. Next we give some notes about CC:

- Although b and b' are arbitrary positive real numbers, we suggest they not be too large. If they were too large, the public key size would be huge.
- According to Cai and Cusick's choice, $N_i = 2^i b' (i = 0, 1, \ldots, m)$.
- By the proofs in Section 4 in [5], to avoid the easy statistical leakage of information, the chosen B should satisfy $B \gg 2^m b'$, this can also be observed from $B \gg 2^n$ and b' can't be too large. So we can say $\frac{2^m b'}{B}$ is exponentially close to 0 and $\frac{b}{\sqrt{B^2 - 2^{2i} b'^2}} \le \frac{b}{\sqrt{B^2 - 2^{2m} b'^2}} = \frac{b}{B} \frac{1}{\sqrt{1 - (\frac{2^m b'}{B})^2}}$ is also exponentially close to 0 for $0 \le i \le m$.

We denote by CCG the Cai-Cusick cryptosystem with more general parameter settings generated as shown:

- $n \ge 5$ and $m + 1 < n$.
- Any real number $b > 0$ and any $N_0, N_1, \ldots, N_m$ such that $N_k > \sum_{i=0}^{k-1} N_i + b$ for $k = 1, 2, \ldots, m$ and $N_0 > b$.
- Let $v_0, v_1, \ldots, v_m$ be independent random vectors with v_i chosen uniformly from $\{x \in \mathbb{R}^n \mid \langle x, u\rangle = N_i \text{ and } \|x\| = B\}$, where we select $B \gg N_m$ to avoid the statistical leakage of information.

We also point out that $\frac{b}{\sqrt{B^2 - N_i^2}}$ $(0 \le i \le m)$ are exponentially close to 0 in CCG.

Notice that we can obtain CC from CCG by letting $m = \lfloor \frac{1}{2} n \rfloor$ and $N_i = 2^i b' (i = 0, 1, \ldots, m)$ for some $b' > b$.

IV. The Ciphertext-Only Attack

A. The Main Theorem

We first give the result about the ciphertext-only attack against CCG.

Theorem 1: For CCG, there is a ciphertext-only attack that breaks it with probability greater than $1 - \frac{4bm(n-3)}{\pi\sqrt{B^2 - N_m^2}}$ after $O(m^2 n)$ multiplications.

By "*break*," we mean given the public key and any ciphertext, one can use the attack to recover the corresponding message.

Notice that $\frac{b}{\sqrt{B^2 - N_m^2}}$ is exponentially close to 0, so the probability of success is exponentially close to 1.

Obviously, a similar result for CC follows.

Corollary 2: For CC, there is a ciphertext-only attack that breaks it with probability greater than $1 - \frac{4bm(n-3)}{\pi\sqrt{B^2 - 2^{2m} b'^2}}$ after $O(m^2 n)$ multiplications.

We next prove Theorem 1.

Proof of Theorem 1: We first describe the ciphertext-only attack as Algorithm $\mathcal{A}$:

Algorithm $\mathcal{A}$. The Ciphertext-Only Attack

Input: The public key $v_{\sigma(0)}, v_{\sigma(1)}, \ldots, v_{\sigma(m)}, b$ and any ciphertext C.

Output: The corresponding message $M = (a_0, a_1, \ldots, a_m)$ or "Failure."

1: Compute the Gram-Schmidt orthogonalization vectors $v^*_{\sigma(0)}, v^*_{\sigma(1)}, \ldots, v^*_{\sigma(m)}$.
2: If $\min_{0 \le i \le m} \|v^*_{\sigma(i)}\| \le b$, output "Failure" and halt, else do 3 – 8.
3: $i := m$.
4: **Repeat**
5: Compute $a_i := \lceil \frac{\langle v^*_{\sigma(i)}, C\rangle}{\|v^*_{\sigma(i)}\|^2} \rfloor$.
6: $C := C - a_i v_{\sigma(i)}$, $i := i - 1$.
7: **Until** $i < 0$.
8: **Return** $(a_0, a_1, \ldots, a_m)$.

COMPUTATIONAL COMPLEXITY: We need $O(m^2 n)$ multiplications to compute the Gram-Schmidt orthogonalization of $v_{\sigma(0)}, v_{\sigma(1)}, \ldots, v_{\sigma(m)}$. Since $O(n)$ multiplications is needed to recover every a_i, we can recover the whole message after $O(mn)$ multiplications. So Algorithm $\mathcal{A}$ can be done after $O(m^2 n)$ multiplications.

For fixed public key, we can precompute all $v^*_{\sigma(i)}$ and $\|v^*_{\sigma(i)}\|^2$ for $0 \le i \le m$ after $O(m^2 n)$ multiplications, then for any ciphertext, the main computation left to us is to compute $(m+1)$ dot products, which just costs $O(mn)$ multiplications. Hence, Algorithm $\mathcal{A}$ is very efficient.

CORRECTNESS: If Algorithm $\mathcal{A}$ outputs a message $(a'_0, a'_1, \ldots, a'_m)$, we will prove that it does be the corresponding message.

Since Algorithm $\mathcal{A}$ outputs a message, then $\min_{0 \le i \le m} \|v^*_{\sigma(i)}\| > b$.

By the Gram-Schmidt orthogonalization process, we have $v^*_{\sigma(i)} = v_{\sigma(i)} - \sum_{j=0}^{i-1} \mu_{i,j} v^*_{\sigma(j)}$ where $\mu_{i,j} = \frac{\langle v_{\sigma(i)}, v^*_{\sigma(j)} \rangle}{\langle v^*_{\sigma(j)}, v^*_{\sigma(j)} \rangle}$. Hence

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

So

$$C = \left(v_{\sigma(0)}, v_{\sigma(1)}, \ldots, v_{\sigma(m)}\right) \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_m \end{pmatrix} + r$$

$$= \left(v^*_{\sigma(0)}, v^*_{\sigma(1)}, \ldots, v^*_{\sigma(m)}\right) \begin{pmatrix} 1 & \mu_{1,0} & \cdots & \mu_{m,0} \\ 0 & 1 & \cdots & \mu_{m,1} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \times \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_m \end{pmatrix} + r$$

where $(a_0, a_1, \ldots, a_m)$ is the correct corresponding message we want to recover and r is the random vector selected in encryption satisfying $\|r\| \le b/2$.

Notice that $r = \sum_{i=0}^{m} r_i v^*_{\sigma(i)} + \omega$, where $r_i \in \mathbb{R}$ and $\omega \in \operatorname{span}(v^*_{\sigma(0)}, v^*_{\sigma(1)}, \ldots, v^*_{\sigma(m)})^{\perp}$, then

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

Since $|r_m| \|v^*_{\sigma(m)}\| \le \|r\| \le b/2$ and $\|v^*_{\sigma(m)}\| \ge \min_{0 \le i \le m} \|v^*_{\sigma(i)}\| > b$, then

$$|r_m| \le \frac{b}{2\left\|v^*_{\sigma(m)}\right\|} < 1/2.$$

Moreover, it can also be concluded that $|r_i| < 1/2$ for $0 \le i \le m$.

Since

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

i.e.

$$\frac{\left\langle v^*_{\sigma(m)}, C \right\rangle}{\left\|v^*_{\sigma(m)}\right\|^2} = a_m + r_m \quad \text{and} |r_m| < 1/2$$

we have

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

By the process of Algorithm $\mathcal{A}$, we get $a'_m = a_m$. Since $|r_i| < 1/2$ holds for $0 \le i \le m$, we can use the same method to prove $a'_i = a_i$ for $0 \le i \le m-1$. So Algorithm $\mathcal{A}$ does recover the correct message.

PROBABILITY OF SUCCESS: We first give the lemma we need, and we will prove it in Section IV-B:

Lemma 1: Let n, m, u, b be the same as in CCG and let $v_0, v_1, \ldots, v_m$ be independent random vectors with v_i chosen uniformly from $\{x \in \mathbb{R}^n \mid \langle x, u \rangle = N_i \text{and } \|x\| = B\}$, where $N_i > 0$ and $\min_{0 \le i \le m} \sqrt{B^2 - N_i^2} \gg b$. Let $L = \min_{0 \le i \le m} \sqrt{B^2 - N_i^2}$, then

i) $v_0, v_1, \ldots, v_m$ are linearly independent with probability 1.

ii) For any permutation σ on $m+1$ letters, the Gram-Schmidt orthogonalization $v^*_{\sigma(0)}, v^*_{\sigma(1)}, \ldots, v^*_{\sigma(m)}$ satisfies

$$\mathbf{Pr}\left[\min_{0 \le i \le m} \left\|v^*_{\sigma(i)}\right\| > b\right] > 1 - \frac{4bm(n-3)}{\pi L}.$$

Denote by $\mathcal{B}$ the event that $v_{\sigma(0)}, v_{\sigma(1)}, \ldots, v_{\sigma(m)}$ are linearly independent. By Lemma 1, we have $\mathbf{Pr}[\mathcal{B}] = 1$ and $\mathbf{Pr}[\min_{0 \le i \le m} \|v^*_{\sigma(i)}\| > b \mid \mathcal{B}] > 1 - \frac{4bm(n-3)}{\pi \sqrt{B^2 - N_m^2}}$. So it can be easily concluded that

$$\begin{aligned} \mathbf{Pr}[\mathcal{A} \text{ succeeds}] &= \mathbf{Pr}\left[\mathcal{B} \text{ and } \min_{0 \le i \le m} \left\|v^*_{\sigma(i)}\right\| > b\right] \\ &= \mathbf{Pr}\left[\min_{0 \le i \le m} \left\|v^*_{\sigma(i)}\right\| > b \mid \mathcal{B}\right] \cdot \mathbf{Pr}[\mathcal{B}] \\ &= \mathbf{Pr}\left[\min_{0 \le i \le m} \left\|v^*_{\sigma(i)}\right\| > b \mid \mathcal{B}\right] \\ &> 1 - \frac{4bm(n-3)}{\pi \sqrt{B^2 - N_m^2}}. \end{aligned}$$

■

Remark 1: We can also use some strategies to improve Algorithm $\mathcal{A}$. First, if $\min_{0 \le i \le m} \|v^*_{\sigma(i)}\| \le b$, we can randomly choose another order of $v_{\sigma(0)}, v_{\sigma(1)}, \ldots, v_{\sigma(m)}$ to compute the corresponding Gram-Schmidt orthogonalization, since the Gram-Schmidt orthogonalization family depends on the order of the vectors. Second, if we finally still have $\|v^*_{\sigma(i)}\| \le b$ for $i \in I \subset \{0, 1, \ldots, m\}$, we can try to decrypt every possible value of $C - \sum_{i \in I} a_i v_{\sigma(i)}$ by Algorithm $\mathcal{A}$ with input $v_{\sigma(i)}$ where $i \notin I$. If for some $(a_0, a_1, \ldots, a_m) \in \{0,1\}^{m+1}$, $\|C - \sum_{i=0}^{m} a_i v_{\sigma(i)}\| \le b/2$, then $(a_0, a_1, \ldots, a_m)$ is the correct message. Notice that in the worst case, we have to try $2^{|I|}$ possible values of $C - \sum_{i \in I} a_i v_{\sigma(i)}$, which may make the algorithm not polynomial time. However, it may be more efficient than the exhaustive search.

Remark 2: As we see, the success probability of the attack is exponentially close to 1 if $\frac{b}{\sqrt{B^2 - N_m^2}}$ is exponentially close to 0. We show the condition that $\frac{b}{\sqrt{B^2 - N_m^2}}$ is exponentially close to 0 can be satisfied easily. Since in CCG, $[b, N_0, N_1, \ldots, N_m]$ is a superincreasing sequence, we can prove that $N_i > 2^i b (0 \le i \le m)$ by induction. If the chosen B satisfies $B \ge N_m + b$, then $\frac{b}{\sqrt{B^2 - N_m^2}} = \frac{b}{\sqrt{(B + N_m)(B - N_m)}} \le \frac{b}{\sqrt{2 N_m b}} < \frac{b}{2^{\frac{m+1}{2}} b} = 2^{-\frac{m+1}{2}}$, which is exponentially close to 0.

Even when B is exponentially close to N_m, although in this case, $\frac{1}{B}v_m$ may be a good approximation to the private key u and some statistical information may help attack the cryptosystem, we can also adjust our algorithm to attack the cryptosystem. For every i, $0 \leq i \leq m$, we try to decrypt $C - a_i v_{\sigma(i)}$ for each $a_i \in \{0,1\}$ using Algorithm $\mathcal{A}$ with the input $v_{\sigma(0)}, \ldots, v_{\sigma(i-1)}, v_{\sigma(i+1)}, \ldots, v_{\sigma(m)}$. Then we use the method in Remark 1 to decide if we get the correct message. Notice that for i satisfying $\sigma(i) = m$, the probability of success depends on the probability of $\min_{\substack{0 \leq k \leq m \\ k \neq i}} \|v^*_{\sigma(k)}\| > b$ which is greater than $1 - \frac{4bm(n-3)}{\pi\sqrt{B^2 - N^2_{m-1}}}$. By the fact $B \geq N_m > N_{m-1} + b$, we have $\frac{b}{\sqrt{B^2 - N^2_{m-1}}} = \frac{b}{\sqrt{(B+N_{m-1})(B-N_{m-1})}} \leq \frac{b}{\sqrt{2N_{m-1}b}} < \frac{b}{2^{\frac{m}{2}}b} = 2^{-\frac{m}{2}}$, which is exponentially close to 0.

B. Proof of Lemma 1

It remains to prove Lemma 1.

Proof of Lemma 1: We denote by $\mathcal{D}$ the subspace orthogonal to u in $\mathbb{R}^n$, then $\dim(\mathcal{D}) = n - 1$. Let $S_{\mathcal{D}} = \{x \in \mathcal{D} \mid \|x\| = 1\}$.

Since $v_0, v_1, \ldots, v_m$ are independent random vectors with v_i chosen uniformly from $\{x \in \mathbb{R}^n \mid \langle x, u\rangle = N_i \text{ and } \|x\| = B\}$, every v_i can be uniquely written as

$$v_i = N_i u + \sqrt{B^2 - N_i^2}\rho_i$$

where $\rho_i \in S_{\mathcal{D}}$. Obviously, choosing v_i uniformly from $\{x \in \mathbb{R}^n \mid \langle x, u\rangle = N_i \text{ and } \|x\| = B\}$ is equivalent to choosing ρ_i uniformly at random from $S_{\mathcal{D}}$.

Proof of i): For $0 \leq i \leq m-1$, given $v_0, \ldots, v_i$, denote by $\mathcal{D}'$ the subspace orthogonal to u in $\operatorname{span}(u, v_0, \ldots, v_i)$. Notice that $\mathcal{D}'$ is a subspace of $\mathcal{D}$ and $\dim(\mathcal{D}') = i + 1 \leq m < n - 1$, then when we independently choose v_{i+1}, we have

$$\begin{aligned}
&\mathbf{Pr}[v_{i+1} \in \operatorname{span}(v_0, \ldots, v_i)] \\
&\quad \leq \mathbf{Pr}[v_{i+1} \in \operatorname{span}(u, v_0, \ldots, v_i)] \\
&\quad = \mathop{\mathbf{Pr}}_{\rho_{i+1} \in_U S_{\mathcal{D}}}[\rho_{i+1} \in \operatorname{span}(u, v_0, \ldots, v_i)] \\
&\quad = \mathop{\mathbf{Pr}}_{\rho_{i+1} \in_U S_{\mathcal{D}}}[\rho_{i+1} \in \mathcal{D}'] \\
&\quad = 0.
\end{aligned}$$

This yields that $v_0, v_1, \ldots, v_m$ are linearly independent with probability 1.

Proof of ii): For clarity of presentation, we assume $\sigma = id$. The proof is same for the case $\sigma \neq id$, since the following proof doesn't depend on the order of N_i's at all.

Let $v_0^*, v_1^*, \ldots, v_m^*$ be the Gram-Schmidt orthogonalization of $v_0, v_1, \ldots, v_m$. Let $\eta_i = \sqrt{B^2 - N_i^2}\rho_i$, it can be also concluded that $\eta_0, \eta_1, \ldots, \eta_m$ are linearly independent with probability 1. So we denote by $\eta_0^*, \eta_1^*, \ldots, \eta_m^*$ the Gram-Schmidt orthogonalization of $\eta_0, \eta_1, \ldots, \eta_m$.

First we show that for $0 \leq i \leq m$,

$$\|v_i^*\| \geq \|\eta_i^*\|. \tag{1}$$

Denote by $u^\dagger, v_0^\dagger, v_1^\dagger, \cdots, v_i^\dagger$ the Gram-Schmidt orthogonalization of $u, v_0, v_1, \ldots, v_i$ and by $v_0^\ddagger, v_1^\ddagger, \ldots, v_{i-1}^\ddagger, u^\ddagger, v_i^\ddagger$ the Gram-Schmidt orthogonalization of $v_0, v_1, \ldots, v_{i-1}, u, v_i$, then obviously we have $\|v_i^*\| \geq \|v_i^\ddagger\|$. By Property 1, $\|v_i^\ddagger\| = \|v_i^\dagger\|$, so $\|v_i^*\| \geq \|v_i^\dagger\|$.

We then 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 $j \leq k$, 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 (1) follows.

Next, we show that for $1 \leq i \leq m$

$$\mathbf{Pr}\left[\|\eta_i^*\| > b\right] > 1 - \frac{4b(n-3)}{\pi\sqrt{B^2 - N_i^2}}. \tag{2}$$

Given $\eta_0, \eta_1, \ldots, \eta_{i-1}$ for $1 \leq i \leq m$, we can compute the corresponding Gram-Schmidt orthogonalization $\eta_0^*, \eta_1^*, \ldots, \eta_{i-1}^*$. Notice that $\eta_0, \eta_1, \ldots, \eta_{i-1}$ are vectors in $\mathcal{D}$ and $\dim(\operatorname{span}(\eta_0, \eta_1, \ldots, \eta_{i-1})) = i \leq m < n - 1$. So we can choose a normal orthogonal basis $u_i, \ldots, u_{n-2}$ of the subspace orthogonal to $\operatorname{span}(\eta_0, \eta_1, \ldots, \eta_{i-1})$ in $\mathcal{D}$. When we independently choose v_i, η_i can be written as $\eta_i = t_0\eta_0^* + t_1\eta_1^* + \cdots + t_{i-1}\eta_{i-1}^* + t_i u_i + \cdots + t_{n-2}u_{n-2}$.

Then

$$\eta_i^* = t_i u_i + \cdots + t_{n-2}u_{n-2}.$$

So $\|\eta_i^*\| \geq |t_{n-2}|\|u_{n-2}\| = |t_{n-2}| = |\langle \eta_i, u_{n-2}\rangle| = \sqrt{B^2 - N_i^2}|\langle \rho_i, u_{n-2}\rangle|$. Since $\sqrt{B^2 - N_i^2} \geq L \gg b$, by Corollary 1

$$\begin{aligned}
\mathbf{Pr}\left[\|\eta_i^*\| > b\right] &\geq \mathop{\mathbf{Pr}}_{\rho_i \in_U S_{\mathcal{D}}}\left[|\langle \rho_i, u_{n-2}\rangle| > \frac{b}{\sqrt{B^2 - N_i^2}}\right] \\
&> 1 - \frac{4b(n-3)}{\pi\sqrt{B^2 - N_i^2}}.
\end{aligned}$$

So (2) follows.

Combining (1) and (2), we have that for $1 \leq i \leq m$,

$$\mathbf{Pr}\left[\|v_i^*\| > b\right] > 1 - \frac{4b(n-3)}{\pi\sqrt{B^2 - N_i^2}} \geq 1 - \frac{4b(n-3)}{\pi L}.$$

Notice that $\mathbf{Pr}[\|v_0^*\| > b] = \mathbf{Pr}[\|v_0\| > b] = 1$. So we have

$$\begin{aligned}
&\mathbf{Pr}\left[\min_{0 \leq i \leq m}\|v_i^*\| \leq b\right] \\
&\quad = \mathbf{Pr}\left[\|v_0^*\| \leq b \text{ or } \|v_1^*\| \leq b \text{ or } \cdots \text{or } \|v_m^*\| \leq b\right] \\
&\quad = \mathbf{Pr}\left[\|v_1^*\| \leq b \text{ or } \cdots \text{or } \|v_m^*\| \leq b\right] \\
&\quad \leq \sum_{j=1}^{m}\mathbf{Pr}[\|v_j^*\| \leq b] \\
&\quad < \frac{4mb(n-3)}{\pi L}.
\end{aligned}$$

TABLE I
PROBABILITY OF SUCCESS

n	m	Probability of $\min_{0\le i\le m}\|v^*_{\sigma(i)}\| > b$
100	25	100%
	50	100%
	75	100%
300	75	100%
	150	100%
	225	100%
500	125	100%
	250	100%
	375	100%

Thus we have

$$\mathbf{Pr}\left[\min_{0\le i\le m}\|v_i^*\| > b\right] > 1 - \frac{4mb(n-3)}{\pi L}.$$

■

Remark 3: By the proof, we can see that the probability of success depends on the distribution of $\|\eta_i^*\|$, or equivalently, the distribution of $\|\rho_i^*\|$, since $\|\eta_i^*\| = \sqrt{B^2 - N_i^2}\|\rho_i^*\|$. In fact, although the lower bound (2) is enough for our proof, we must point out that the probability of $\|\rho_i^*\| > \frac{b}{\sqrt{B^2-N_i^2}}$ in CCG or CC can be computed precisely since $\|\rho_i^*\|$ is beta distributed by the result in [4]. This observation also allows us to generalize the attack to many other possible distributions for ρ_i satisfying that $\mathbf{Pr}[\|\rho_i^*\| > \frac{b}{\sqrt{B^2-N_i^2}}]$ is large enough.

C. Experimental Results

We implemented the attack on an AMD Athlon(tm) 64 Processor 2800+1.81 GHz PC using Shoup's NTL library version 5.4.1 [14]. Since the probability of success of the attack depends on the probability of $\min_{0\le i\le m}\|v^*_{\sigma(i)}\| > b$, we tested the probability of $\min_{0\le i\le m}\|v^*_{\sigma(i)}\| > b$ for $n = 100, 300, 500$. For every n, we let $m = \frac{n}{4}, \frac{n}{2}, \frac{3n}{4}$ respectively.

For CC, 50 random instances were tested for every n and m. In every instance,

- b was selected randomly in $(0, 2^5)$,
- b' was selected randomly in $[2^5, 2^{10}]$,
- B was set to be 2^n,
- $v_i = 2^i b' u + \sqrt{B^2 - 2^{2i}b'^2}\rho_i (0 \le i \le m)$,
- σ was selected randomly.

In Table I, we list the probability of $\min_{0\le i\le m}\|v^*_{\sigma(i)}\| > b$ in our experiments.

Even setting $B = 2^m b'$ in CC, we also tested 50 instances for every n and m and still got $\min_{0\le i\le m}\|v^*_{\sigma(i)}\| > b$ for every instance. This showed that the attack performed much better than the theoretical results indicated. One reason was that the theoretical lower bound of $\mathbf{Pr}[\min_{0\le i\le m}\|v^*_{\sigma(i)}\| > b]$ we gave was usually rough.

For CCG, we also tested 50 instances for every n and m. In every instance, b was selected randomly in $(0, 2^5)$. We first selected N_0 randomly in $(2^5, 2^6)$ and generated $N_i (1 \le i \le m)$ inductively as follows: after having $N_0, N_1, \ldots, N_k$, we selected $e \in (0, 2^5)$ and let $N_{k+1} = \sum_{j=0}^{k} N_j + b + e$. B was set to be $N_m + b$, $v_i = N_i u + \sqrt{B^2 - N_i^2}\rho_i (0 \le i \le m)$ and σ was selected randomly. The probability of $\min_{0\le i\le m}\|v^*_{\sigma(i)}\| > b$ was also 100% in our experiments.

V. CONCLUSION

As we see, the Cai-Cusick lattice-based public-key cryptosystem is not secure since the ciphertext-only attack we present can efficiently recover the corresponding message. We also prove that it will succeed with probability very close to 1 and the experiments support our view very well.

ACKNOWLEDGMENT

The authors thank the anonymous referees for their suggestions on how to improve the presentation of this paper.

REFERENCES

[1] M. Ajtai, "Gennerating hard instances of lattice problems," in *Proc. 28th ACM STOC*, New York, 1996, pp. 99–108.
[2] M. Ajtai, "Representing hard lattices with $o(n \log n)$ bits," in *Proc. 37th STOC*, D. S. Johnson and U. Feige, Eds., New York, 2005, pp. 94–103, ACM.
[3] M. Ajtai and C. Dwork, "A public-key cryptosystem with worst-case/average-case equivalence," in *Proc. 29th ACM STOC*, New York, 1997, pp. 284–293.
[4] A. Akhavi, J.-F. Marckert, and A. Rouault, "On the reduction of a random basis," in *Proc. ANALCO'07 (SIAM)*, New Orleans, LA, 2007.
[5] J.-Y. Cai and T. W. Cusick, "A lattice-based public-key cryptosystem," in *Proc. SAC'98 (Lecture Notes Comput. Science)*, S. Tavares and H. Meijer, Eds., Berlin, Germany, 1999, vol. 1556, pp. 219–233.
[6] J.-Y. Cai and T. W. Cusick, "A lattice-based public-key cryptosystem," *Inf. Comput.*, vol. 151, pp. 17–31, 1999.
[7] R. Fischlin and J.-P. Seifert, "Tensor-based trapdoors for CVP and their application to public key cryptography (extended abstract)," in *Proc. IMA Conf. Cryptogr. y Coding (Lecture Notes Comput. Sci.)*, M. Walker, Ed., Berlin, Germany, 1999, vol. 1746, pp. 244–257, Springer-Verlag.
[8] O. Goldreich, S. Goldwasser, and S. Halevi, "Public-key cryptosystems from lattice reduction problems," in *Crypto'97 (Lecture Notes in Comput. Sci.)*, B. S. Kaliski, Jr., Ed. Berlin, Germany: Springer-Verlag, 1997, vol. 1294, pp. 112–131.
[9] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A ring-based public key cryptosystem," in *Proc. Algorithmic Number Theory (Lecture Notes Comput. Sci.)*, J. P. Buhler, Ed., Berlin, Germany, 1998, vol. 1423, pp. 267–288, Springer-Verlag.
[10] P. Nguyen and J. Stern, "Cryptanalysis of the Ajtai-Dwork cryptosystem," in *Crypto'98 (Lecture Notes in Computer Science)*, H. Krawczyk, Ed. Berlin, Germany: Springer-Verlag, 1998, vol. 1462, pp. 223–242.
[11] O. Regev, "New lattice-based cryptographic constructions," *J. ACM*, vol. 51, pp. 899–942, 2004.
[12] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," in *Proc. 37th STOC*, D. S. Johnson and U. Feige, Eds., New York, 2005, pp. 84–93, ACM.
[13] P. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Ann. Symp. Found. Comput. Sci.*, Santa Fe, NM, 1994, pp. 124–134, IEEE Computer Science Press.
[14] V. Shoup, NTL: A Library For Doing Number Theory Available at [Online]. Available: http://www.shoup.net/ntl/

Yanbin Pan was born in Hebei Province, China, in 1982. He received the B.S. degree in information and computation science from Nanjing University, Nanjing, China, in 2005, and the Ph.D. degree in applied mathematics from Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing, China, in 2010.

He joined the Academy of Mathematics and Systems Science, Chinese Academy of Sciences, in July 2010, where he is currently an Assistant Professor. His current research interests include algorithms and cryptography.

Yingpu Deng was born in Hunan Province, China, in 1971. He received the B.S. degree in mathematics from Wuhan University, Wuhan, China, in 1993, and the Ph.D. degree in mathematics from Peking University, Beijing, China, in 2002.

He joined Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing, in July 2004, where he is currently an Associate Professor. His current research interests include cryptography and combinatorics.