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

Yanbin Pan   Yingpu Deng

Key Laboratory of Mathematics Mechanization
Academy of Mathematics and Systems Science,Chinese Academy of Sciences

August 2008

Outline

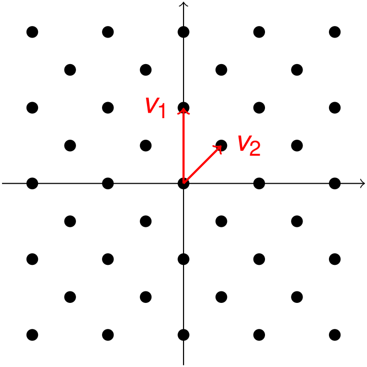
1. Introduction
    - What is Lattice?
2. The Cai-Cusick Cryptosystem
    - Description of the Cai-Cusick Cryptosystem
3. The Ciphertext-only Attack
    - Our Algorithm to Attack the Cai-Cusick Cryptosystem

What is Lattice?

For any vectors $v_1, \cdots, v_m \in \mathbb{R}^n$, the lattice spanned by them is defined as below:

Definition

$$\mathcal{L}(v_1, \cdots, v_m) = \{\sum_{i=1}^{m} a_i v_i | a_i \in \mathbb{Z}\}$$



Outline

1. Introduction
   - What is Lattice?

2. The Cai-Cusick Cryptosystem
   - Description of the Cai-Cusick Cryptosystem

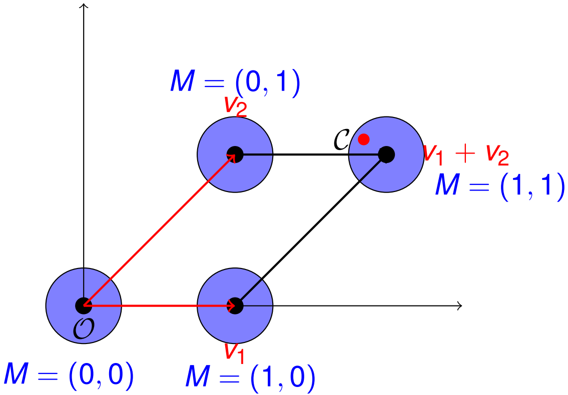
3. The Ciphertext-only Attack
   - Our Algorithm to Attack the Cai-Cusick Cryptosystem

A Glance of the Cai-Cusick Cryptosystem

- It was first proposed in SAC 1998, later in Information and Computation in 1999.
- It mixes the Ajtai-Dwork Cryptosystem and a Knapsack.
- Our analysis is the first one, to our best knowledge.

Illustration of the Encryption

Example: v_1, v_2 and the circle area are public.

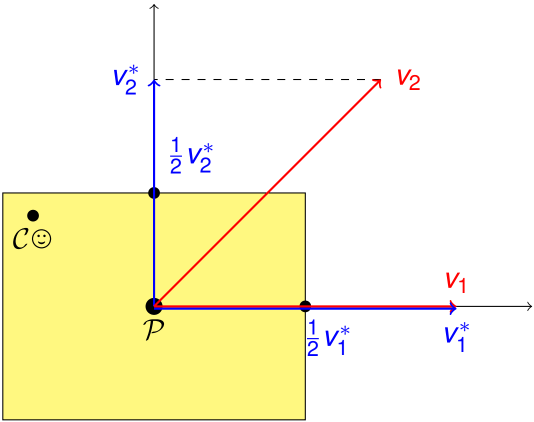


We take the decryption as solving a CVP (the Closest Vector Problem).

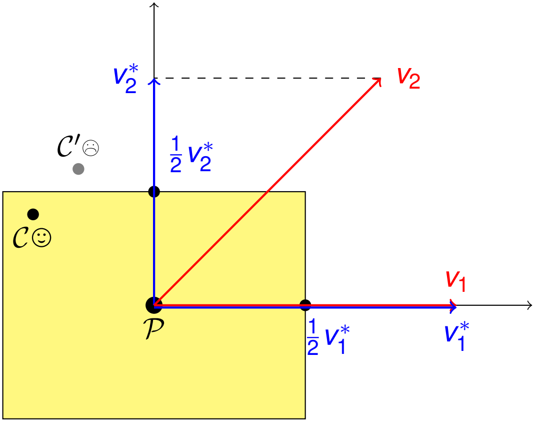
Outline

1. Introduction
   - What is Lattice?
2. The Cai-Cusick Cryptosystem
   - Description of the Cai-Cusick Cryptosystem
3. The Ciphertext-only Attack
   - Our Algorithm to Attack the Cai-Cusick Cryptosystem

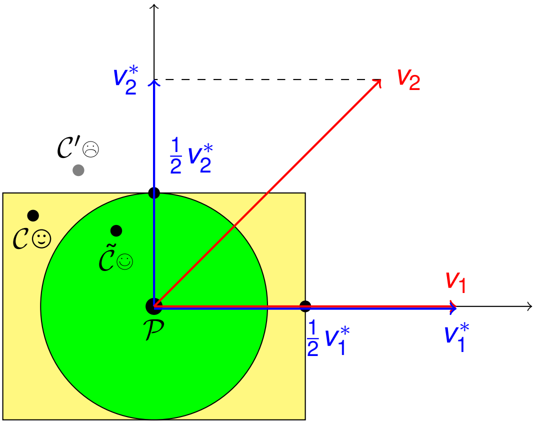
Illustration of the Algorithm



For the General Case



For the Cai-Cusick Cryptosystem


v_2^*
v_2
$\mathcal{C}'$ ☹
$\frac{1}{2}v_2^*$
$\mathcal{C}$ ☺
$\tilde{\mathcal{C}}$ ☺
v_1
$\mathcal{P}$
$\frac{1}{2}v_1^*$
v_1^*