Broadcast Attacks against Lattice-based Cryptosystems

Thomas Plantard
Willy Susilo

Centre for Computer and Information Security Research
Universiy of Wollongong

http://www.uow.edu.au/~thomaspl
thomaspl@uow.edu.au

Broadcast Attack on RSA [Håstad88]

Broadcast Problem

One message m send to k recipients.

$$\forall 1 \leq i \leq k, \quad c_i \equiv m^e \pmod{N_i}$$

Attack Using CRT

If $k \geq e$ then

$$\begin{aligned} c &\equiv m^e \pmod{\prod_{i=1}^{k} N_i} \\ c &= m^e \\ c^{1/e} &= m \end{aligned}$$

Securing against Broadcast Attack

General Solution [BBM00,BPS00]

- Paddings,

$$m' = (m|h(N)).$$

- Cost in Space and Time

Do we need Paddings for ...

- ... Knapsack based cryptography?
- ... Lattice based cryptography?

Outline

1. Introduction
2. Lattice Theory
   - Lattice
   - Lattice Gap
3. Cryptosystem Concerned
   - Lattice Based Cryptography
   - Knapsack Based Cryptography
4. Intersecting Lattices
   - Theorem
   - Broadcast Attack
   - Practical Tests
5. Conclusion

Lattice Theory

Lattice

Definition of a Lattice

- All the integral conbinations of $d \leq n$ linearly independant vectors over $\mathbb{R}$

$$\mathcal{L} = \mathbb{Z}\,\mathbf{b}_1 + \cdots + \mathbb{Z}\,\mathbf{b}_d = \{\lambda_1 \mathbf{b}_1 + \cdots + \lambda_d \mathbf{b}_d \ : \ \lambda_i \in \mathbb{Z}\}$$

- d dimension.
- $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_d)$ is a *basis*.

An Example

$$\mathbf{B} = \begin{pmatrix} 5 & \frac{1}{2} & \sqrt{3} \\ \frac{3}{5} & \sqrt{2} & 1 \end{pmatrix} \tag{1}$$

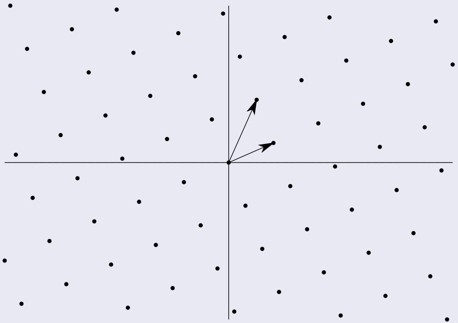
$d = 2 \leq n = 3$

Example

A lattice $\mathcal{L}$

$$\mathbf{B} = \begin{pmatrix} 8 & 5 \\ 5 & 16 \end{pmatrix} \tag{2}$$

An infinity of basis

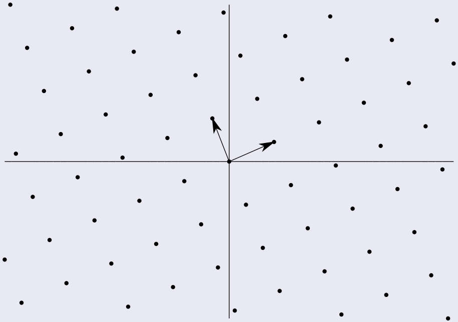


Example

A lattice $\mathcal{L}$

$$\mathbf{UB} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 8 & 5 \\ 5 & 16 \end{pmatrix} = \begin{pmatrix} 8 & 5 \\ -3 & 11 \end{pmatrix} \tag{3}$$

An infinity of basis

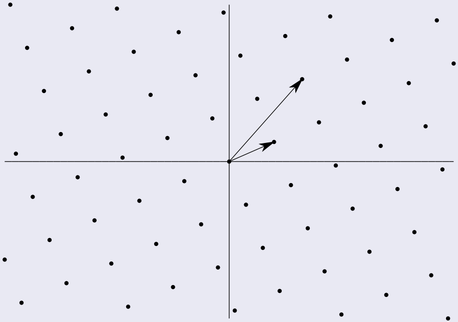


Example

A lattice $\mathcal{L}$

$$\mathbf{UB} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 8 & 5 \\ 5 & 16 \end{pmatrix} = \begin{pmatrix} 8 & 5 \\ 13 & 21 \end{pmatrix} \quad (4)$$

An infinity of basis

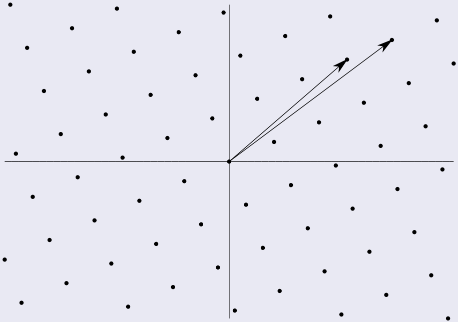


Example

A lattice $\mathcal{L}$

$$\mathbf{UB} = \begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 8 & 5 \\ 5 & 16 \end{pmatrix} = \begin{pmatrix} 29 & 31 \\ 21 & 26 \end{pmatrix} \quad (5)$$

An infinity of basis

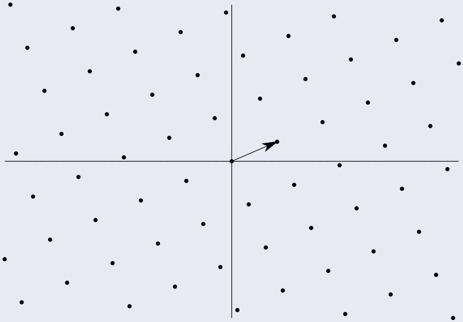


Example

The Shortest Vector and The First Minima

$$\mathbf{v} = \begin{pmatrix} 8 & 5 \end{pmatrix}, \text{ with } \lambda_1 = \sqrt{8^2 + 5^2} = 9.434 \tag{6}$$

An infinity of basis



Lattice Gap

Lattice Gap

$$\alpha(\mathcal{L}) = \frac{\lambda_2(\mathcal{L})}{\lambda_1(\mathcal{L})} = \frac{\text{Second Minima}}{\text{First Minima}}$$

Example

$$\alpha = \frac{\| \begin{pmatrix} -3 & 11 \end{pmatrix} \|}{\| \begin{pmatrix} 8 & 5 \end{pmatrix} \|} = \frac{\sqrt{3^2 + 11^2}}{\sqrt{8^2 + 5^2}} = 1.208$$

Shortest Vector Problem

- SVP on Random Lattice ($\alpha \sim 1$) NP-Hard [Ajtai98].
- SVP solvable by BKZ-20 if $\alpha > 1.07^d$.
- SVP solvable by LLL if $\alpha > 1.16^d$.
- SVP on Lattice based Cryptography $\alpha > 2$, $\alpha = O(poly(d))$.

Lattice Based Cryptography

Cryptography based on SVP

- 1996: Ajtai-Dwork (AD) first theorethical cryptosystem based on Lattice.
- 1998: Nguyen and Stern found a heuristical attack on AD.
- 1999: Improvement of Cai and Cusick.
- 2003: Improvement by Regev.

Cryptography based on CVP

- 1997: Goldreich, Goldwasser and Halevi (GGH), first efficient cryptosystem.
- 1999: Nguyen cryptanalyzed GGH.
- 2001: Improvement by Micciancio.

GGH

GGH Cryptosystem

- **Setup:** Compute a secret "good" basis G and a public "bad " basis B with
$$\mathcal{L}(G) = \mathcal{L}(B).$$
- **Encrypt:** To encrypt $m \in \mathbb{Z}^n$, compute $r \in \mathbb{Z}^n$,
$$c = m + rB.$$
- **Decrypt:** Use the good basis G to solve the CVP on c.

Lattice Attack, [Kannan87]

1. Compute $B' = \begin{pmatrix} B & 0 \\ c & 1 \end{pmatrix}$.
2. Find $\begin{pmatrix} m & 1 \end{pmatrix}$ shortest vector of $\mathcal{L}$.

Knapsack Based Cryptography

Knapsack based Cryptosystem [MerHel78]

- **Setup:** Create $a_1, \ldots, a_n$ with a trapdoor f for Knapsack Problem.
- **Encrypt:** To encrypt $m \in [0,1]^n$, compute

$$s = \sum_{i=1}^{n} m_i a_i.$$

- **Decrypt:** Use the trapdoor f to solve the knapsack problem.

Example

- **Setup:** Create $a = [8, 11, 15, 23]$ with f
- **Encrypt:** For $m = [0, 1, 1, 0]$ compute

$$s = 11 + 15 = 26.$$

- **Decrypt:** $f([8, 11, 15, 23], 26) = [0, 1, 1, 0]$

Security Question

Density

$$density = \frac{n}{max_{i=1}^{n} \log_2 a_i} = \frac{4}{\log_2 23} = 0.8842$$

- High Density $density > 1$, NP-Complete. [Karp72]
- Low Density $d \sim 0.9408$, solvable using LLL.

Lattice Attack [LagOdl85]

1. Compute $B = \begin{pmatrix} Id & a^T \\ 0 & s \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 8 \\ 0 & 1 & 0 & 0 & 11 \\ 0 & 0 & 1 & 0 & 15 \\ 0 & 0 & 0 & 1 & 23 \\ 0 & 0 & 0 & 0 & 26 \end{pmatrix}$
2. Find $\begin{pmatrix} m & 0 \end{pmatrix}$ shortest vector of $\mathcal{L}$. , $v = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \end{pmatrix}$

Theorem

If ...

i) v Shortest Vector of $\mathcal{L}_1$.

ii) v Shortest Vector of $\mathcal{L}_2$.

... Then ...

i) v Shortest Vector of $\mathcal{L}_1 \cap \mathcal{L}_2$.

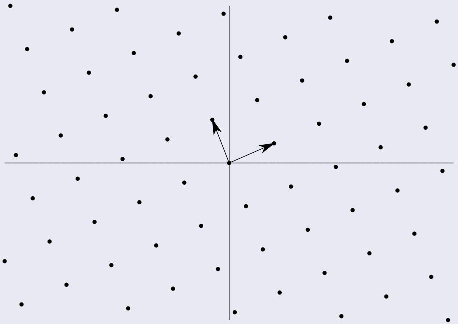
ii) Gap Bigger on $\mathcal{L}_1 \cap \mathcal{L}_2$.

Example

Basis

$$\mathbf{B_1} = \begin{pmatrix} 8 & 5 \\ 5 & 16 \end{pmatrix} \tag{7}$$

Lattice

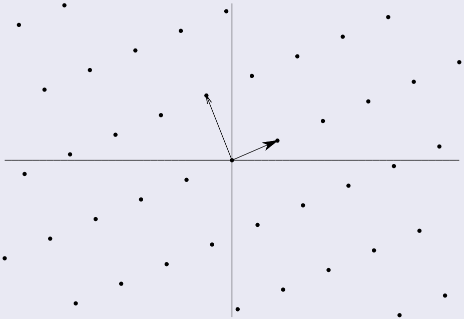


Example

Basis

$$\mathbf{B_2} = \begin{pmatrix} 8 & 5 \\ -12.5 & 11.5 \end{pmatrix} \tag{8}$$

Lattice

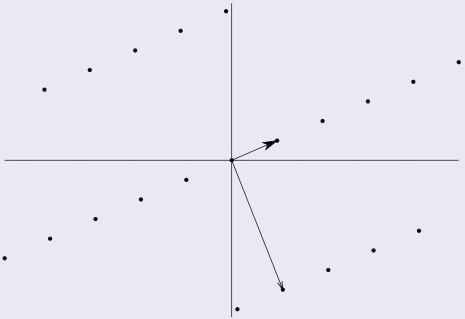


Example

Basis

$$\mathbf{B}(\mathcal{L}_1 \cap \mathcal{L}_2) = \begin{pmatrix} 8 & 5 \\ 17 & -28 \end{pmatrix} \tag{9}$$

Lattice



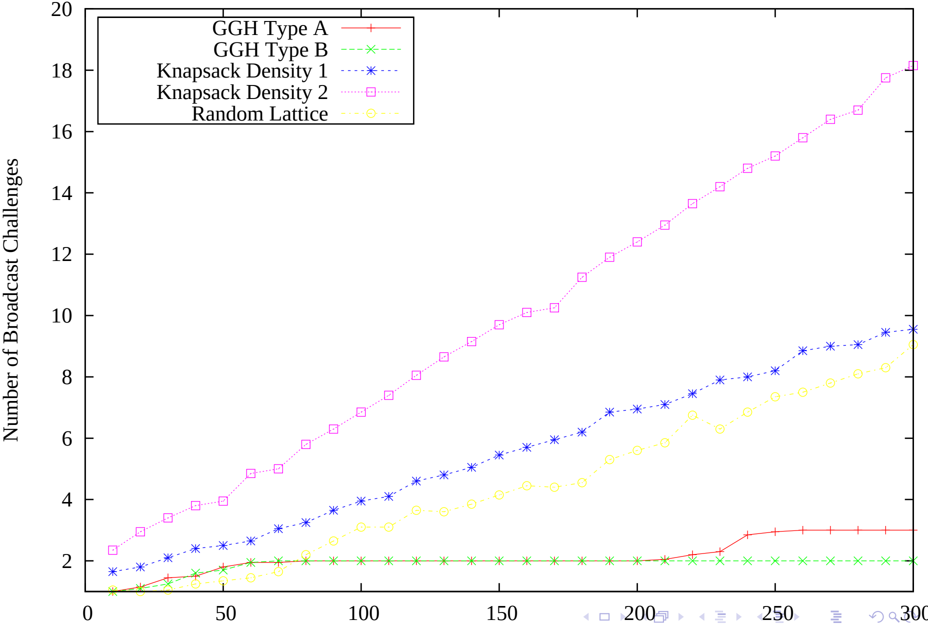
Broadcast Attack ...

...for CVP based Cryptosystem

1. Compute $B'_i = \begin{pmatrix} B_i & 0 \\ c_i & 1 \end{pmatrix}$.
2. Compute $\mathcal{L} = \bigcap_{i=1}^{k} \mathcal{L}(B'_i)$.
3. Find $\begin{pmatrix} m & 1 \end{pmatrix}$ shortest vector of $\mathcal{L}$.

... for Knapsack Cryptosystem

1. Compute $B_i = \begin{pmatrix} Id & a_i^T & 0 \\ 0 & s & 1 \end{pmatrix}$.
2. Compute $\mathcal{L} = \bigcap_{i=1}^{k} \mathcal{L}(B_i)$.
3. Find $\begin{pmatrix} m & 0 & 1 \end{pmatrix}$ shortest vector of $\mathcal{L}$.


GGH Type A
GGH Type B
Knapsack Density 1
Knapsack Density 2
Random Lattice
Number of Broadcast Challenges
0
50
100
150
200
250
300
2
4
6
8
10
12
14
16
18
20

Conclusion

Conclusion

Do we need paddings for ...

- ... Knapsack based cryptography? YES.
- ... Lattice based cryptography? YES.

Intersecting Lattices

- Nice way to modelized problems...
- ... Without loosing any information.