# Cryptography based on $CVP_\infty$

Thomas PLANTARD

Centre for Computer and Information Security Research
University Of Wollongong

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

# Lattice Based Cryptography

## Tools

- Lattice Theory
- Closest Vector Problem
- $l_\infty$-norm

## Objectives

- Digital Signature
- Cryptosystem
- Efficiency and Security

# Outline

# Lattice

## Definition of a Lattice

- All the integral combinations of $d \leq n$ linearly independent 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

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

$d = 2 \leq n = 3$

## In this work

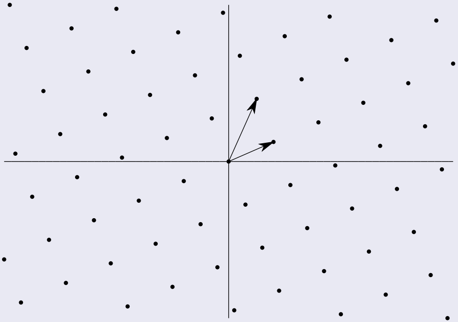
- Full-rank lattice : $d = n$
- Integer Basis: $B \in \mathbb{Z}^{n,n}$

# Example

## A lattice $\mathcal{L}$

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

## An infinity of basis

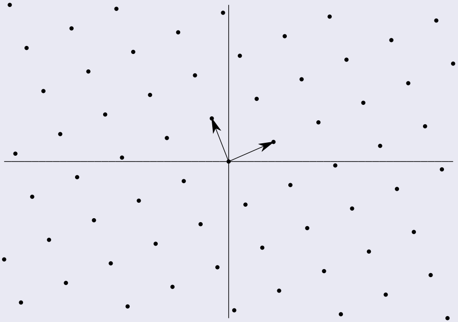


# Example

## A lattice $\mathcal{L}$

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

## An infinity of basis

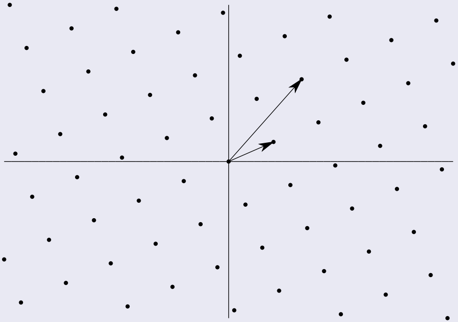


# Example

## A lattice $\mathcal{L}$

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

## An infinity of basis

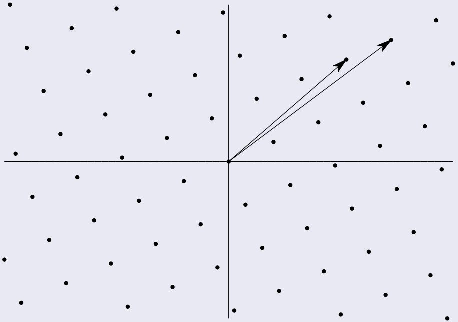


# Example

## 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



# Inclusion

## Problem: $v \stackrel{?}{\in} \mathcal{L}$

- Input: A vector $v \in \mathbb{Z}^n$
- Input: A basis $B \in \mathbb{Z}^{n,n}$ of a lattice $\mathcal{L}(B)$
- Output: YES if there exists a vector

$$\exists k \stackrel{?}{\in} \mathbb{Z}^n, kB = v$$

## Solution

- $k = vB^{-1}$, $k \stackrel{?}{\in} \mathbb{Z}^n$
- $k = vB^{-1} \bmod 1$, $k \stackrel{?}{=} 0$
- Polynomial with any basis

# Inclusion

## Example

- Input: A vector $v = (20, 20)$
- Input: A basis $\mathbf{B} = \begin{pmatrix} 8 & 5 \\ 5 & 16 \end{pmatrix}$

## Solution

- $k = vB^{-1} = (20, 20) \begin{pmatrix} \frac{16}{103} & -\frac{5}{103} \\ -\frac{5}{103} & \frac{8}{16} \end{pmatrix} = (\frac{220}{103}, \frac{60}{103})$
- $k = vB^{-1} \bmod 1 = (\frac{14}{103}, \frac{60}{103}) \neq 0$
- $(20, 20) \notin \mathcal{L}(\mathcal{B})$

# Vector Reduction

## Problem

- Input: A vector $v \in \mathbb{Z}^n$
- Input: A basis $B \in \mathbb{Z}^{n,n}$ of a lattice $\mathcal{L}(B)$
- Output: A vector $w \equiv v \pmod{\mathcal{L}}$ with $\|w\|$ minimal.

$$w = v + kB \quad k \in \mathbb{Z}^n \text{ with } \|w\| \text{ minimal}$$

## Equivalence

- $u \equiv v \pmod{\mathcal{L}(B)}$
- $(u - v) \in \mathcal{L}(B)$
- $k \in \mathbb{Z}^n, \quad u = v + kB$

## Reduction

- $u = v \bmod \mathcal{L}(B)$
- $\nexists w \equiv v \pmod{\mathcal{L}(B)}, \quad \|w\| < \|u\|$

# Norms

## $l_p$-Norm

- $l_p$-norm $\|v\|_p$ of a vector $v$

$$\|v\|_p = \left( \sum_{i=0}^{n-1} |v_i|^p \right)^{1/p}$$

## Used Norm

- Euclidean Norm $\|v\|_2$ of a vector $v$: $\|v\|_2 = \sqrt{\sum_{i=0}^{n-1} (v_i)^2}$
- Infinity Norm $\|v\|_\infty$ of a vector $v$: $\|v\|_\infty = \max_{i=0}^{n-1} |v_i|$

## Complexity

- NP-Hard under any norm (EmdeBoas'81) with Preprocessing (Regev and Rosen '06)
- $O(n^{\frac{n}{2}})$ deterministic (Kannan'83, Hanrot and Stehle'07)
- $O(2 + \frac{1}{\epsilon})^n$ probabilistic (Blomer and Naewe'07)

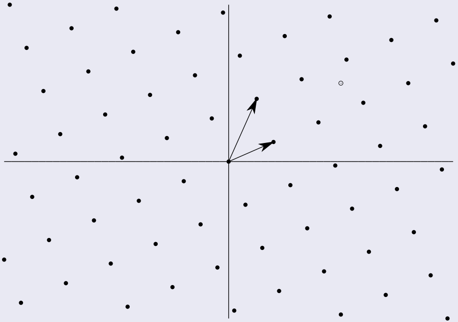
# Vector Reduction

## An Example

$$\mathbf{B} = \begin{pmatrix} 8 & 5 \\ 5 & 16 \end{pmatrix} \tag{6}$$

A Vector: $(20, 20)$

## Closest Vector Problem

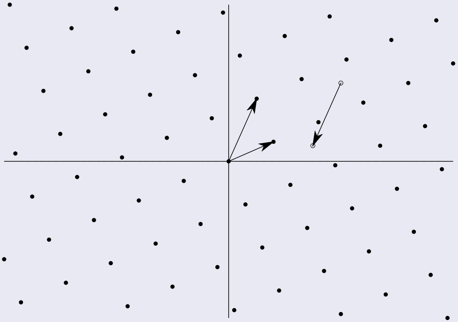


## An Example

$$\mathbf{B} = \begin{pmatrix} 8 & 5 \\ 5 & 16 \end{pmatrix} \tag{6}$$

A Vector: $(20, 20) \equiv (20, 20) - (5, 16) = (15, 4)$

## Closest Vector Problem

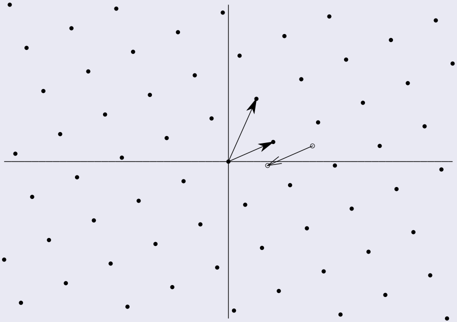


## An Example

$$\mathbf{B} = \begin{pmatrix} 8 & 5 \\ 5 & 16 \end{pmatrix} \tag{6}$$

A Vector: $(20, 20) \equiv (15, 4) - (8, 5) = (7, -1)$

## Closest Vector Problem



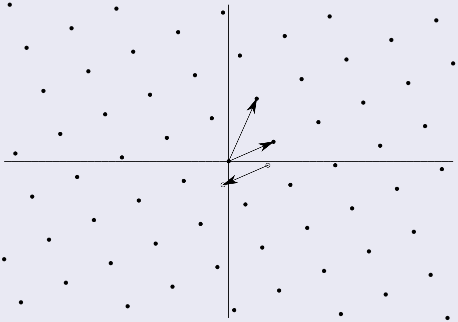
# Vector Reduction

## An Example

$$\mathbf{B} = \begin{pmatrix} 8 & 5 \\ 5 & 16 \end{pmatrix} \tag{6}$$

A Vector: $(20, 20) \equiv (7, -1) - (8, 5) = (-1, -6)$

## Closest Vector Problem

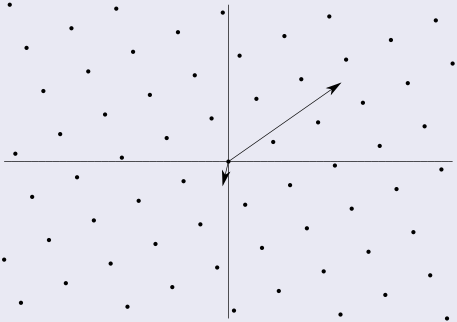


## An Example

$$\mathbf{B} = \begin{pmatrix} 8 & 5 \\ 5 & 16 \end{pmatrix} \tag{6}$$

A Vector: $(20, 20) \equiv (-1, -6) \pmod{\mathcal{L}}$

## Closest Vector Problem



## Closest Vector Problem

### A Solution: Babai's Round-Off

1. $k = vB^{-1}$
2. $w = v - \lceil k \rfloor B$

### A good Approximation of CVP

- Polynomial Time
- Quality depends on $B$
- Babai's use a LLL-reduction of $B$ (Lenstra,Lenstra and Lovasz'82)

# Closest Vector Problem

## Example

- Input: A vector $v = (20, 20)$
- Input: A basis $\mathbf{B} = \begin{pmatrix} 8 & 5 \\ 5 & 16 \end{pmatrix}$

## A Solution

- $k = vB^{-1} = (20, 20) \begin{pmatrix} \frac{16}{103} & -\frac{5}{103} \\ -\frac{5}{103} & \frac{8}{16} \end{pmatrix} = (\frac{220}{103}, \frac{60}{103})$
- $w = \lceil k \rfloor B = (20, 20) - (2, 1) \begin{pmatrix} 8 & 5 \\ 5 & 16 \end{pmatrix} = (20, 20) - (21, 26)$
- $(20, 20) \equiv (-1, -6)$

## NP-Hard Problems around CVP

### CVPP: Closest Vector Problem with Preprocessing.

- Preprocessing on $B$.
- Input: $w$
- Output: $v = w \bmod \mathcal{L}(B)$

### Covering Radius

- Input: $B$
- Output: $\nu(B) = \min_{\forall w} \|w \bmod \mathcal{L}(B)\| \leq \nu(B)$

### GDD: Garanteed Decoding Distance.

- Input: $w, B$
- Output: $v \equiv w \pmod{\mathcal{L}(B)}$ with $\|v\| \leq \nu(B)$

# New Vector Reduction

# Rectangular Matrix

## Rectangular Basis

- A Basis $B = D - M$
- $D$ dominant diagonal matrix
- $M$ noise matrix $M_{i,j}$ small

## Consequence

- $k = vB^{-1}$
- $k = v(D - M)^{-1}$
- $k = vD^{-1}(1 - MD^{-1})^{-1}$
- $k = vD^{-1} \quad (1 + MD^{-1} + (MD^{-1})^2 + (MD^{-1})^3 + \dots)$

## Spectral Radius of a matrix $A$, $\rho(A)$

- Theorem: $1 + A + A^2 + A^3 + \dots$ converge if $\rho(A) < 1$.
- $|\lambda_0| \leq |\lambda_1| \leq \cdots \leq |\lambda_{n-1}| \leq \rho(A)$
- $\rho(A) \leq \|A\| \quad \forall \|.\|$

# Vector Reduction

## Input

- Input: A vector $v \in \mathbb{Z}^n$
- Input: A basis $B = (D - M) \in \mathbb{Z}^{n,n}$ of a lattice $\mathcal{L}(B)$
- Output: A vector $w \equiv v \bmod \mathcal{L}$ with $\|wD^{-1}\|_\infty < 1$

## Algorithm

1. $w \leftarrow v$
2. until $\|wD^{-1}\|_\infty < 1$
   1. $k \leftarrow wD^{-1}$
   2. $w \leftarrow w - \lceil k \rfloor B$

# Spectral Radius

## Theorems

- Ending:

$$\frac{\|1 - MD^{-1}\|_\infty}{1 - \|MD^{-1}\|_\infty} < 1$$

- Unicity:

$$\frac{\|v\|}{\lambda_1(D)} + \frac{\nu(D)}{\lambda_1(D)} + \|MD^{-1}\| < 1 \quad \forall \|.\|$$

- If parameters polynomial on $n \Rightarrow$ number of loops $O(\log(n))$.

## Conjecture

- Ending: $\rho(MD^{-1}) < \frac{1}{2}$

## Spectral Radius of a matrix $A$, $\rho(A)$

- $\forall \|.\|$

$$\lim_{k\to\infty} \|A^k\| = \rho(A)^k$$

- $\forall \|.\|$

$$\rho(A) \leq \|A\|$$

# Number of loops with $\rho < \frac{1}{2}$

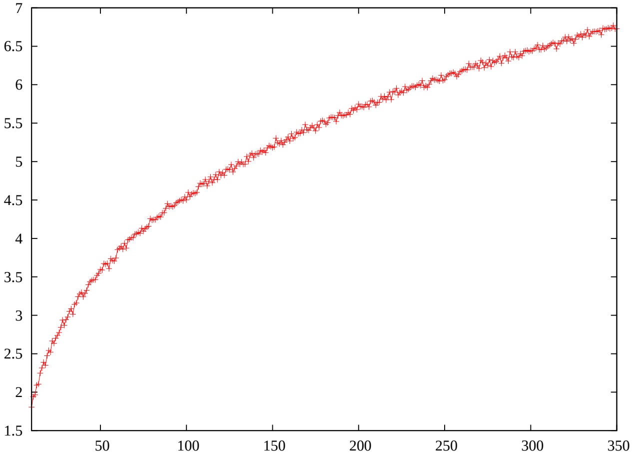



Figure: Average number of loops used to reduce a message vector to a signature vector.

## An example

### Input

- A vector $v = (22, 14)$ and a basis $B = D - M$

$$D = \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}, \quad M = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 6 & -1 \\ -1 & 4 \end{pmatrix} \tag{7}$$

### Algorithm

1. $w \leftarrow (22, 14)$
2. $k \leftarrow wD^{-1} = [\frac{22}{5}, \frac{14}{5}]$
3. $w \leftarrow w - \lceil k \rfloor B$

   $w = [22, 14] - [4, 3] \begin{pmatrix} 6 & -1 \\ -1 & 4 \end{pmatrix} = (22, 14) - (21, 8) = (1, 6)$
4. $k \leftarrow wD^{-1} = [\frac{1}{5}, \frac{6}{5}]$
5. $w \leftarrow w - \lceil k \rfloor B$

   $w = [1, 6] - [0, 1] \begin{pmatrix} 6 & -1 \\ -1 & 4 \end{pmatrix} = (1, 6) - (-1, 4) = (2, 2)$

### Output

$w = (2, 2) \equiv (22, 14) \pmod{\mathcal{L}}$

## Cryptography based on SVP

- 1997. Ajtai-Dwork first theoretical cryptosystem based on Lattice Theory.
- 1998. Nguyen and Stern: heuristic attack on AD.
- 1999. Improvement of Cai and Cusick
- 2003. Improvement by Regev.

## Cryptography based on CVP

- 1997. Goldreich, Goldwasser and Halevi: first efficient cryptosystem:GGH and GGHSign.
- 1999. GGH cryptanalyzed by Nguyen.
- 2001. GGH Improved By Micciancio, with some open questions.

## GGHSign Cryptanalyzis

- 2002: first leaked found by Gentry and Szydlo.
- 2003: theoretical attack by Szydlo.
- 2006: Cryptanalysis of GGHSign by Nguyen and Regev.
- 2006. Crypto question Regev

# GGHSign

## Setup:

i) Compute a secret "good" basis $G$.

ii) Compute a public "bad " basis $B$ with

$$\mathcal{L}(G) = \mathcal{L}(B).$$

## Sign:

i) Hash: $m \in \{0,1\}^* \to v \in \mathbb{Z}^n$

ii) Signature: $w = v \bmod \mathcal{L}(G)$.

## Verify:

i) Hash: $m \in \{0,1\}^* \to v \in \mathbb{Z}^n$

ii) Check: $w - v \in \mathcal{L}(B)$

# GGH

## Setup:

i) Compute a secret “good” basis $G$.

ii) Compute a public “bad ” basis $B$ with

$$\mathcal{L}(G) = \mathcal{L}(B).$$

## Encrypt:

i) Add lattice noise: $c = m + kB$ with $k \in \mathbb{Z}^n$ random.

## Decrypt:

i) Reduce: $w = v \bmod \mathcal{L}(G)$.

## Security

1. "bad basis" $\xrightarrow{\textit{Difficult}}$ "good basis"
   "good basis" $\xrightarrow{\textit{Easy}}$ "bad basis"
2. A good vector reduction with a "good basis": Easy.
   A good vector reduction with a "bad basis": Difficult.
3. Inclusion with any basis: Easy.
4. Add a random lattice point: Easy.

## Question

- How to choose a "good" basis?
- How to choose a "bad" basis?
- How to use a good basis to have a good vector reduction?

# Analysis and Comparison

# How to choose a "good" basis?

## GGH

Rectangular Matrix

$$G = \lfloor \sqrt{n} + 1 \rfloor Id - [-4, 4]^{n,n}$$

## Micciancio

LLL-reduced basis

$$G = [-n, n]^{n,n}$$

## Us

- Signature: $G = D - M$ such $\rho(MD^{-1}) < \frac{1}{2}$

$$\left\lceil \frac{4}{3}\sqrt{n} \right\rceil Id - [-1, 1]^{n,n}$$

- Encryption: $G = D - M$ such $\|MD^{-1}\|_\infty < \frac{1}{4}$

$$4nId - [-1, 1]^{n,n}$$

# How to choose a “bad” basis?

## GGH

$B = \prod U_i G$

$$U_i \in \left\{ \begin{pmatrix} 1 & * & * & * & * \\ & 1 & * & * & * \\ & & 1 & * & * \\ & & & 1 & * \\ & & & & 1 \end{pmatrix}, \begin{pmatrix} 1 & & & & \\ * & 1 & & & \\ * & * & 1 & & \\ * & * & * & 1 & \\ * & * & * & * & 1 \end{pmatrix}, \begin{pmatrix} 1 & & & & \\ & 1 & & & \\ * & * & 1 & * & * \\ & & & 1 & \\ & & & & 1 \end{pmatrix}, \begin{pmatrix} 1 & & * & & \\ & 1 & * & & \\ & & 1 & & \\ & & * & 1 & \\ & & * & & 1 \end{pmatrix} \right\}$$

## Micciancio

Hermite Normal Form of $G$

$$B = \begin{pmatrix} * & & & & \\ * & * & & & \\ * & * & * & & \\ * & * & * & * & \\ * & * & * & * & * \end{pmatrix} \text{ with } * \geq 0$$

# How to choose a “bad” basis?

## Us

- Signature: Optimal HNF

$$H = \begin{pmatrix} * & & & & \\ * & 1 & & & \\ * & & 1 & & \\ * & & & 1 & \\ * & & & & 1 \end{pmatrix}$$

- Encryption: $B = \prod U_i G$.

$$U_i \in \left\{ \begin{pmatrix} 1 & & & & \\ & 1 & & & \\ * & * & 1 & * & * \\ & & & 1 & \\ & & & & 1 \end{pmatrix}, \begin{pmatrix} 1 & & * & & \\ & 1 & * & & \\ & & 1 & & \\ & & * & 1 & \\ & & * & & 1 \end{pmatrix} \right\}$$

# How to use a good basis to have a good vector reduction?

## GGH

- Babai's Round-off.
- $\|m\|_\infty < \frac{1}{2\|G^{-1}\|_\infty}$ and exact arithmetic for No Decryption Error

## Micciancio

- Babai Nearest Plane.
- More exact but slower.

## Us

- Our method with loops.
- No floating-point arithmetic.

# Time Complexity

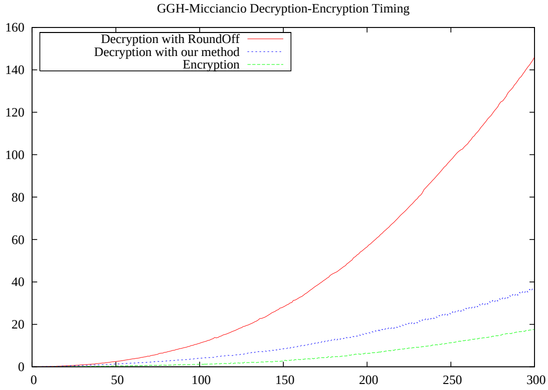



Figure: GGH-Micciancio Cryptosystem Timing in ms.

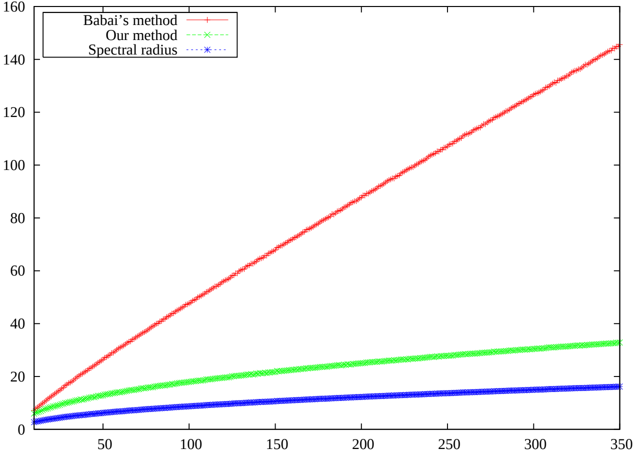



Figure: Average $l_\infty$-norm of signature-vector using different reduction method.

# Security

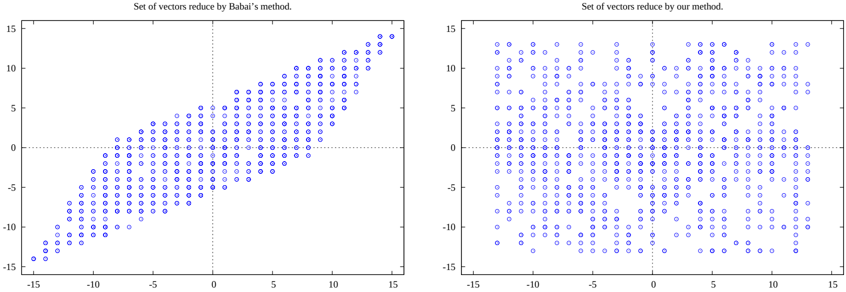



Figure: Signature-message on $\mathbb{R}^2$ for Babai's reduction and our reduction.

# New version of GGH-Micciancio's Space and Time Complexity.

## Space Complexity

| | |
|---|---|
| Secret Key Size | $O(n^2)$ |
| Public Key Size | $O(n^2 \log n)$ |
| Message Size | $O(n \log n)$ |
| Encrypted Size | $O(n \log n)$ |

## Time Complexity

| | |
|---|---|
| SetUp Time | $O(n^3 \log^2 n)$ |
| Encryption Time | $O(n^2 \log n)$ |
| Decryption Time | $O(n^2 \log^2 n)$ |

# Conclusion

## Improvement of GGHSign

1. Faster
2. Shorter Signature: $\pm$ half.
3. Not broken

## Improvement of GGH

1. Faster
2. No Decryption Error

## Open Questions

1. $\rho(MD^{-1}) < \frac{1}{2}$