A Digital Signature Scheme based on CVP_∞

Thomas Plantard
Willy Susilo
Khin Than Win

Centre for Computer and Information Security Research
Universiy Of Wollongong

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

Lattice Based Cryptography

Tools

- Lattice Theory
- Closest Vector Problem
- l_∞-norm

Objectives

- Digital Signature
- Efficiency and Security

Outline

1. Lattice Theory
   - Lattice
   - Inclusion
   - Closest Vector Problem
2. New Vector Reduction
   - Rectangular Matrix
   - Algorithm
3. GGH Digital Signature
   - Lattice Based Cryptography
   - GGHSign Scheme
4. Analysis and Comparison
   - Time Complexity
   - Space Complexity
   - Security
5. Conclusion

1. Lattice Theory
   - Lattice
   - Inclusion
   - Closest Vector Problem
2. New Vector Reduction
   - Rectangular Matrix
   - Algorithm
3. GGH Digital Signature
   - Lattice Based Cryptography
   - GGHSign Scheme
4. Analysis and Comparison
   - Time Complexity
   - Space Complexity
   - Security
5. Conclusion

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

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

$d = 2 \leq n = 3$

In this work

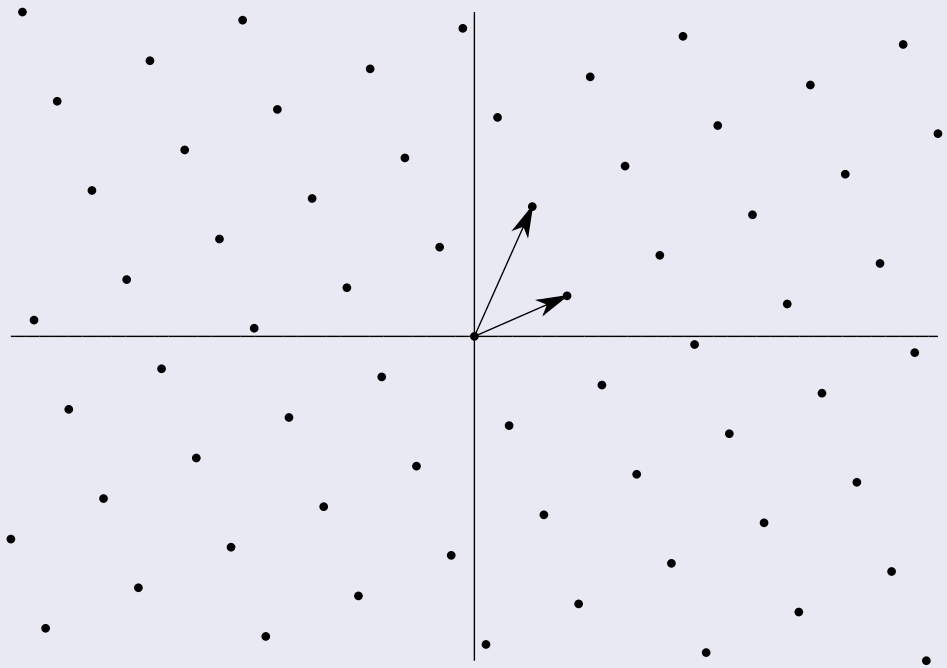
- Full-rank lattice : $d = n$
- Integer Basis: $B \in \mathbb{Z}^{n,n}$

Example

A lattice $\mathcal{L}$

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

An infinity of basis

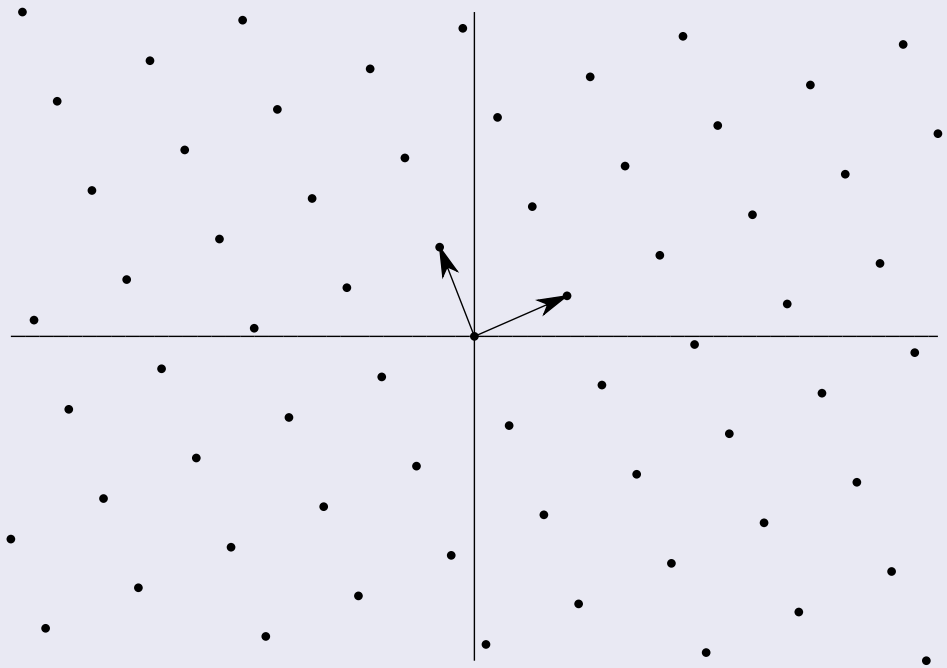


Example

A lattice $\mathcal{L}$

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

An infinity of basis

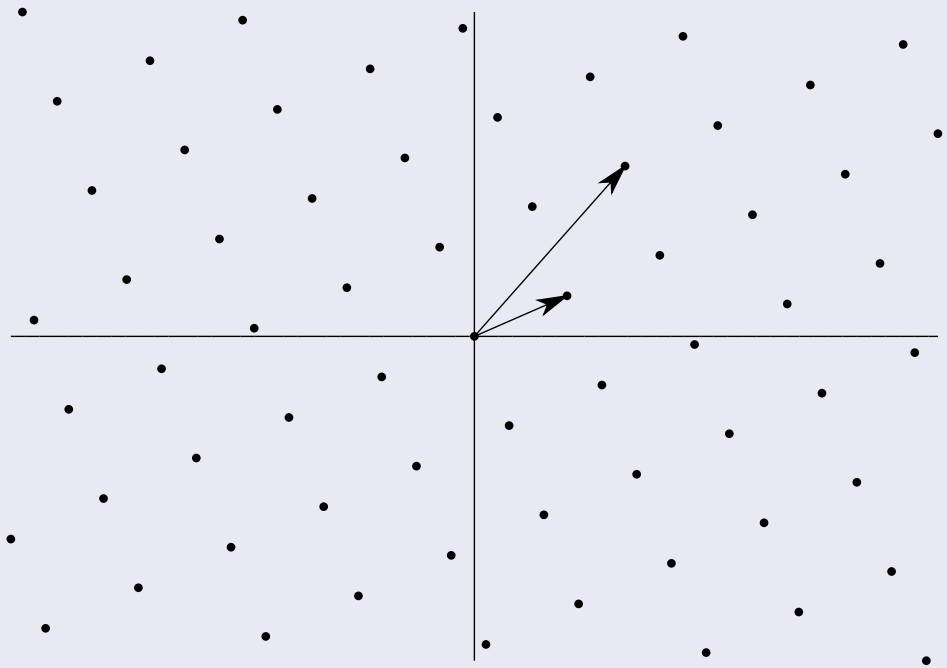


Example

A lattice $\mathcal{L}$

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

An infinity of basis

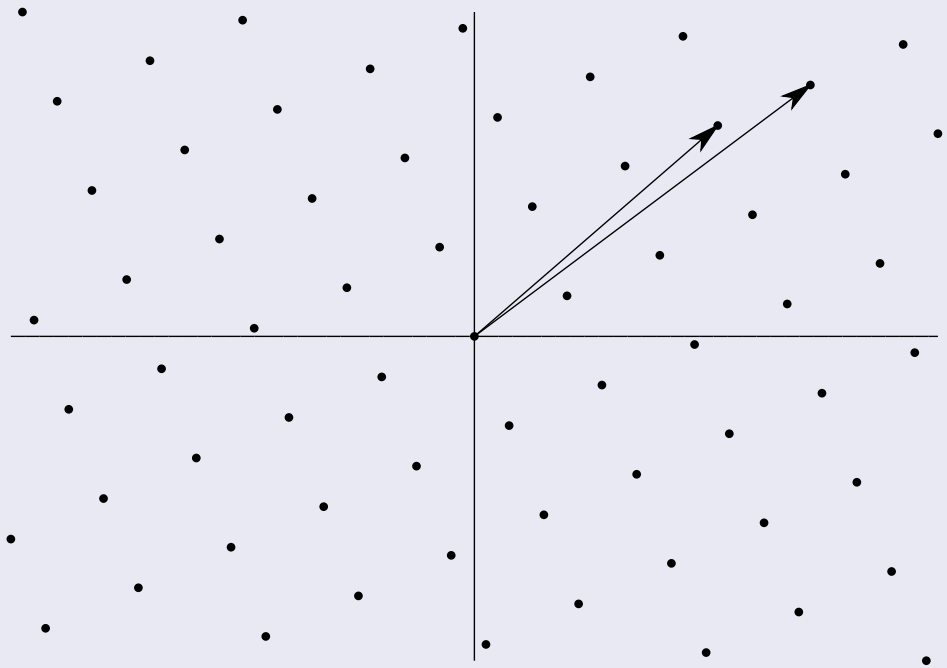


Example

A lattice $\mathcal{L}$

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

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.

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

Complexity

- NP-Hard under any norm (EmdeBoas'81) with Precomputation (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)

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

- Euclidian 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

$$\|v\|_\infty = \max_{i=0}^{n-1} |v_i|$$

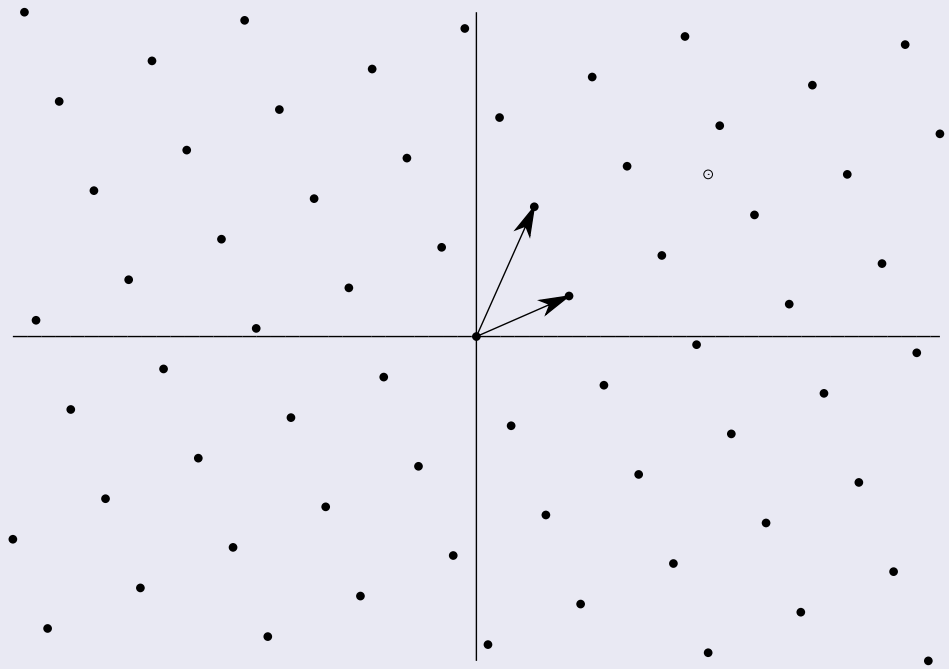
Vector Reduction

An Example

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

A Vector: $(20, 20)$

Closest Vector Problem



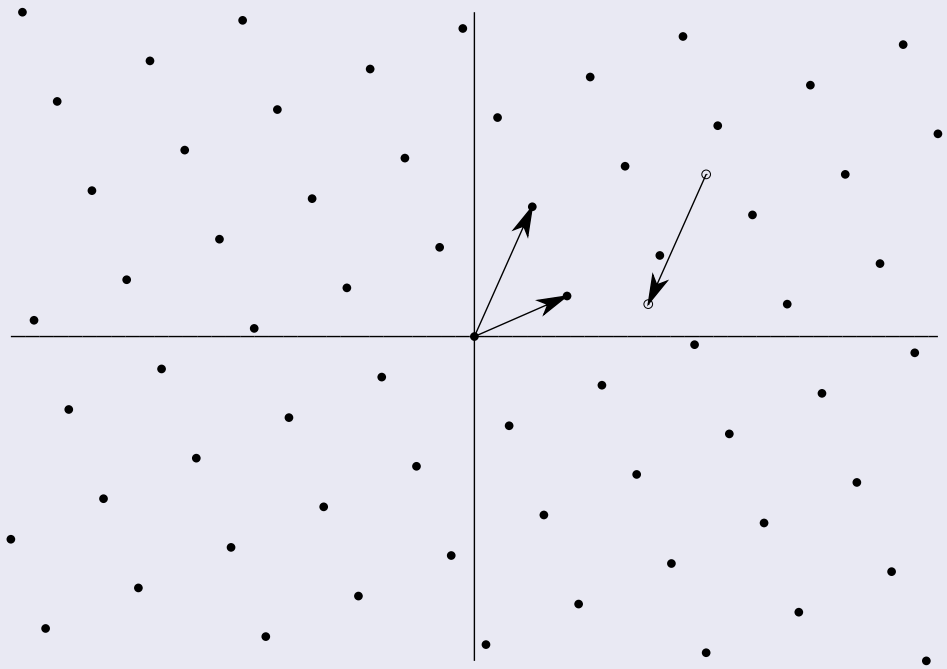
Vector Reduction

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



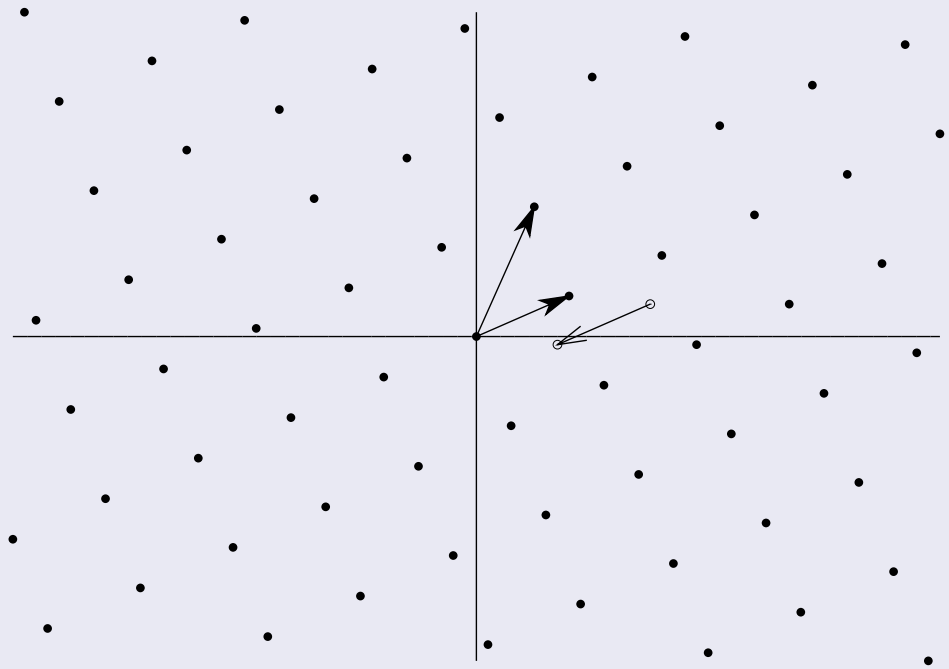
Vector Reduction

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



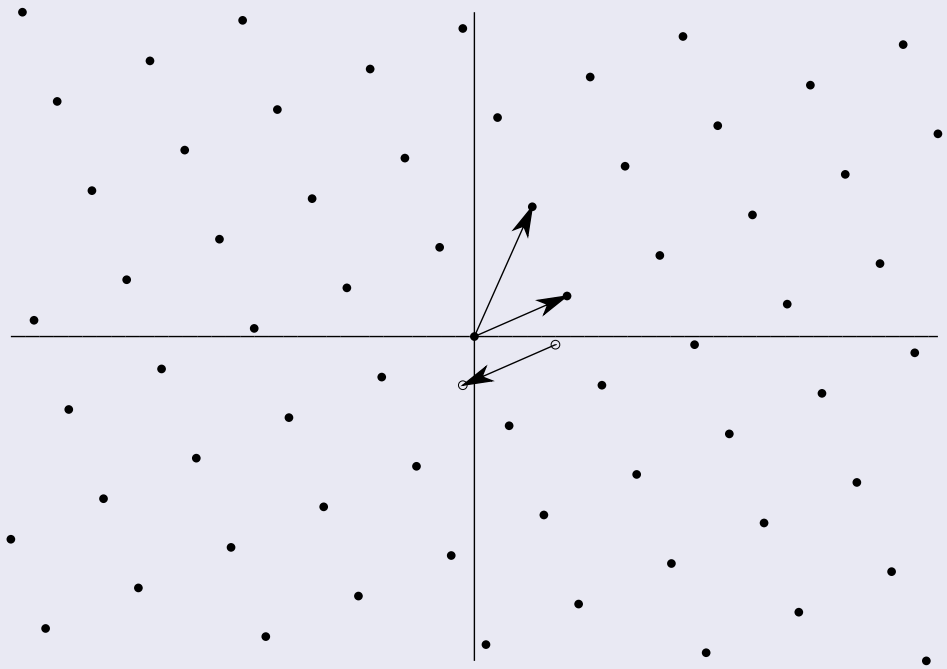
Vector Reduction

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



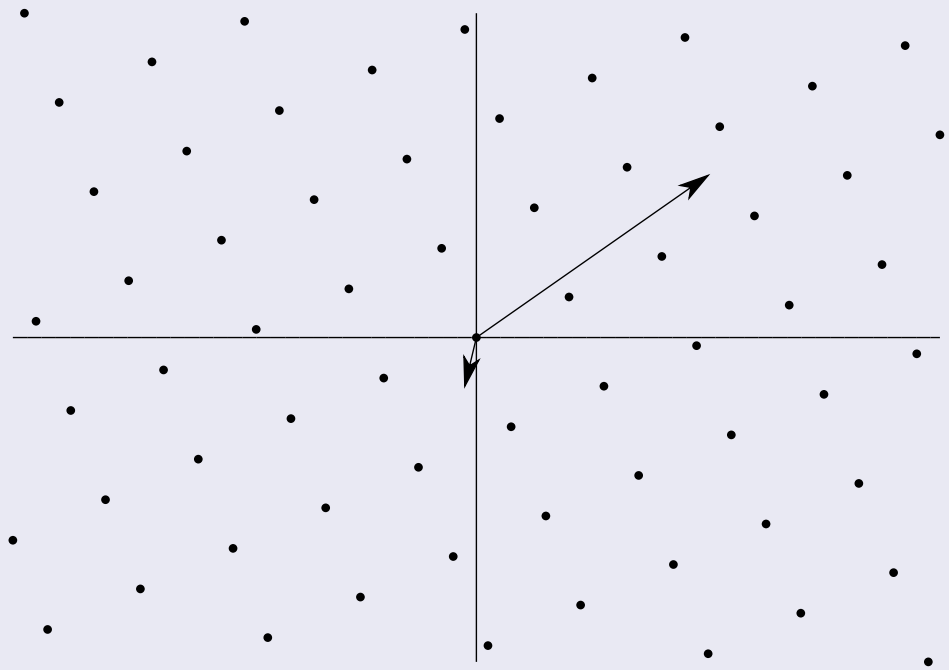
Vector Reduction

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

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

New Vector Reduction

1. Lattice Theory
   - Lattice
   - Inclusion
   - Closest Vector Problem
2. New Vector Reduction
   - Rectangular Matrix
   - Algorithm
3. GGH Digital Signature
   - Lattice Based Cryptography
   - GGHSign Scheme
4. Analysis and Comparison
   - Time Complexity
   - Space Complexity
   - Security
5. Conclusion

Rectangular Matrix

Rectangular Basis

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

Concequence

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

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. $w \leftarrow w - \lceil k \rfloor B$

Conjecture

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

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

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

GGH Digital Signature

1. Lattice Theory
   - Lattice
   - Inclusion
   - Closest Vector Problem
2. New Vector Reduction
   - Rectangular Matrix
   - Algorithm
3. GGH Digital Signature
   - Lattice Based Cryptography
   - GGHSign Scheme
4. Analysis and Comparison
   - Time Complexity
   - Space Complexity
   - Security
5. Conclusion

Cryptography based on CVP

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

GGHSign Cryptanalyzis

- Gentry and Szydlo: first leaked in in 2002.
- Szydlo: theorithical attack in 2003.
- Nguyen and Regev: Cryptanalysis of GGHSign in 2006.

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: $m \in \{0,1\}^* \rightarrow v \in \mathbb{Z}^n$

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

Verify:

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

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

GGHSign Security

Security

1. "bad basis" $\overset{Difficult}{\longrightarrow}$ "good basis"
   "good basis" $\overset{Easy}{\longrightarrow}$ "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.

Question

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

Setup

a) Choose an integer n.

b) Compute a randomly integer matrix $M \in \{-1, 0, 1\}^{n,n}$.

c) Compute $b = \lfloor 2\rho(M) + 1 \rfloor$.

d) Compute the Hermite Normal Form H of the basis $bId - M$.

e) Public Key is (b, H) and the secret key is M.

Sign

To sign a message $m \in \{0,1\}^*$

a) $v = h(m) \in \mathbb{Z}^n$ with

$$\begin{array}{rccc} h: & m & \rightarrow & v \\ : & \{0,1\}^* & \rightarrow & \left\{x \in \mathbb{Z}^n, \quad \|x\|_\infty < b^2\right\} \end{array}$$

b) $v \leftarrow w \bmod D - M$

c) Using new Algorithm, compute w, which is a reduced vector of v.

d) The signature on m is w.

Verify

To verify a message-signature pair, (m, w), one does the following.

a) Check if $\|w\|_\infty < b$.

b) Compute the vector $h(m) \in \mathbb{Z}^n$.

c) Check if the vector $h(m) - w$ is in the lattice of basis H.

Analysis and Comparison

1. Lattice Theory
   - Lattice
   - Inclusion
   - Closest Vector Problem
2. New Vector Reduction
   - Rectangular Matrix
   - Algorithm
3. GGH Digital Signature
   - Lattice Based Cryptography
   - GGHSign Scheme
4. Analysis and Comparison
   - Time Complexity
   - Space Complexity
   - Security
5. Conclusion

Time Complexity

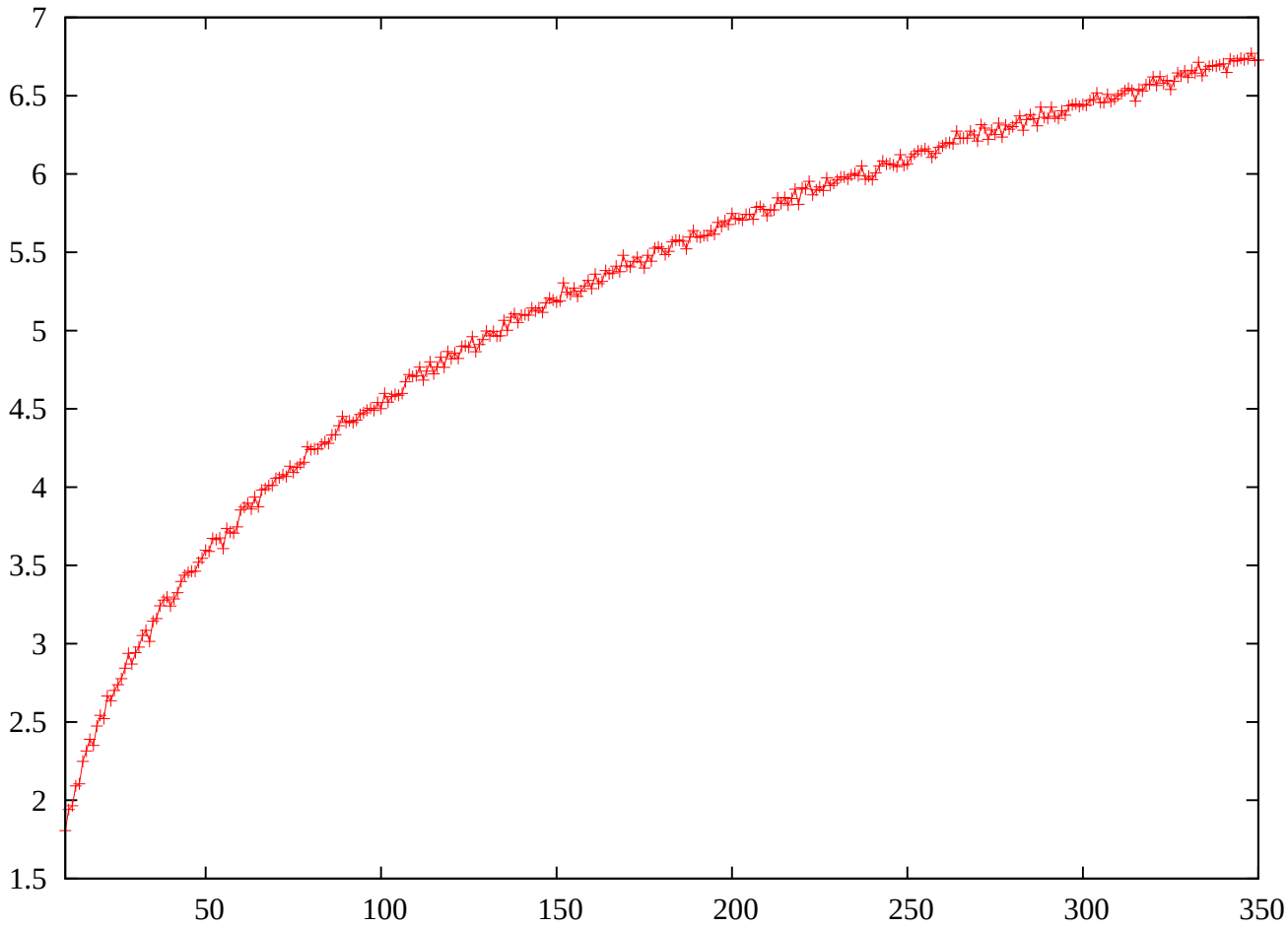


Figure: Average number of loops used to reduce a message vector to a signature vector.

Space Complexity

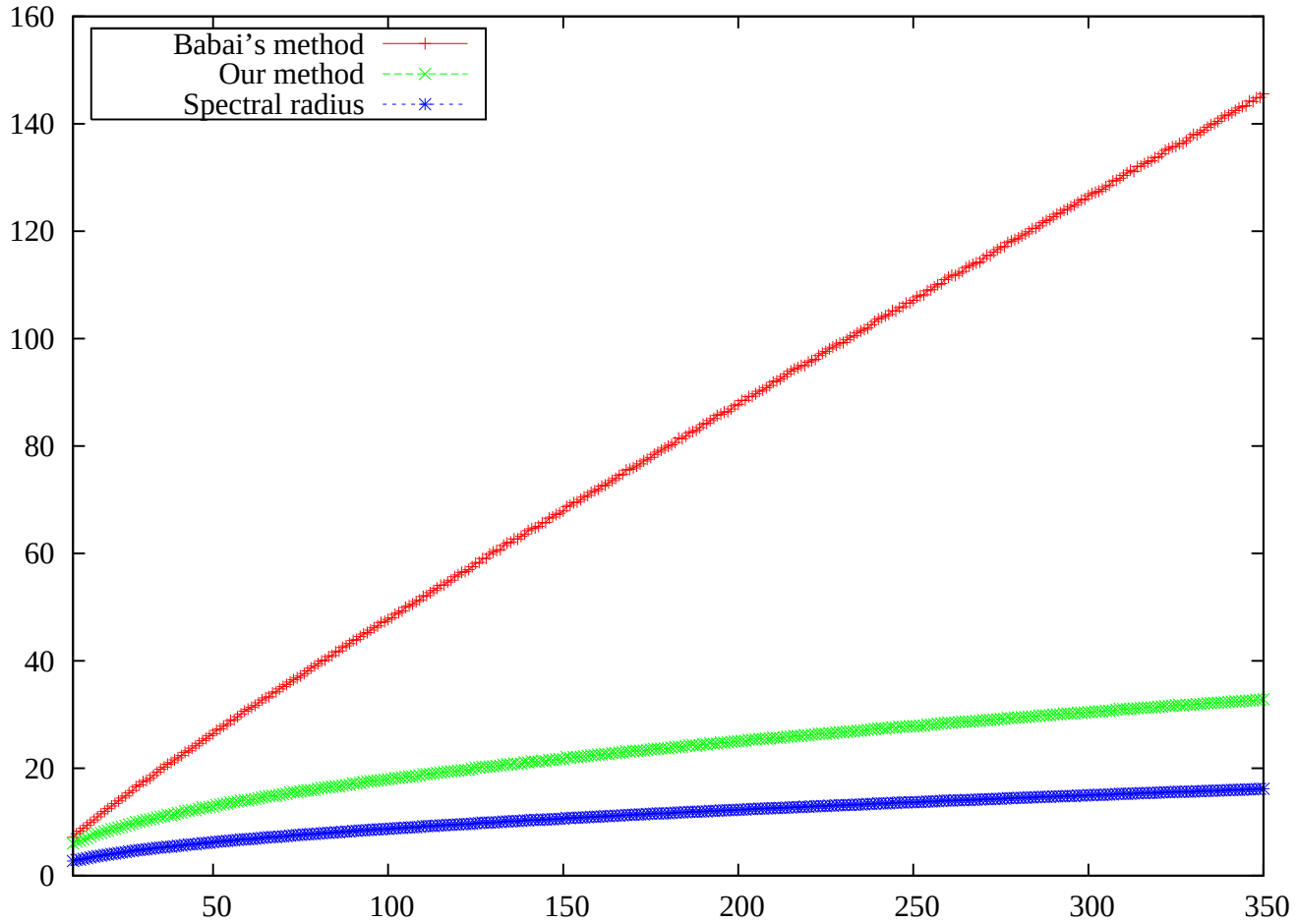


Figure: Average l_∞-norm of signature-vector using different reduction method.

Security

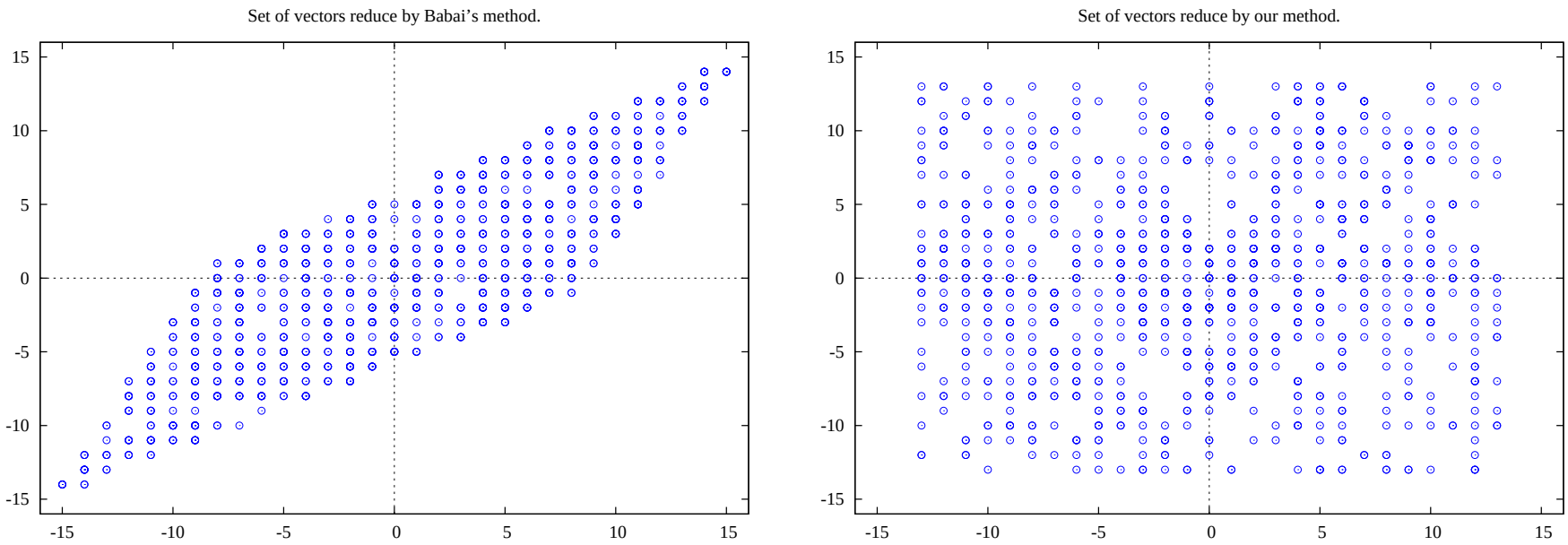


Figure: Signature-message on $\mathbb{R}^2$ for Babai's reduction and our reduction.

Conclusion

Improvement of GGHSign

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

Open Questions

1. $\rho(MD^{-1}) < \frac{1}{2}$
2. Formula for the average number of loops
3. Security Proof