Title	Definitions	Algorithms	The dual Lattice	Attacking cryptosystems	Enc
	00000 00	00000 0000 00	000 00	00	

Shortest Vector Problem

Marios Georgiou

National Technical University of Athens

May 24, 2011

▲□▶ ▲□▶ ▲ 臣▶ ★ 臣▶ 三臣 - のへぐ

Title	Definitions •0000 00	Algorithms 00000 0000 000	The dual Lattice 000 00	Attacking cryptosystems 00	End

Contents

▲ロト ▲園 ト ▲ 臣 ト ▲ 臣 ト 一臣 - のへで

Title

Definitions Useful Definitions

The Problem

Algorithms

Main Idea-Algorithms for 1,2-dimensions Preparation for the LLL Algorithm The Algorithm

The dual Lattice

Some definitions

Gram-Schmidt lower bound property

Attacking cryptosystems

A Lattice attack on RSA

End

Title	Definitions ○●○○○ ○○	Algorithms 00000 0000 00	The dual Lattice 000 00	Attacking cryptosystems 00	End
Lattice					

▲□▶▲圖▶▲≣▶▲≣▶ ≣ のへの

Title	Definitions ○●○○○ ○○	Algorithms 00000 0000 000	The dual Lattice 000 00	Attacking cryptosystems 00	End
			Lattice		

A Lattice \mathcal{L} in \Re^n is a discrete subgroup of \Re^n which spans the real vector space \Re^n .

$$\mathcal{L} = \left\{ \sum_{i=1}^n \lambda_i \mathbf{a_i} \mid \lambda_i \in \mathbb{Z} \right\}$$

▲□▶ ▲□▶ ▲ 臣▶ ★ 臣▶ 三臣 - のへぐ

Title	Definitions 0000 00	Algorithms 00000 0000 000	The dual Lattice 000 00	Attacking cryptosystems 00	End
			1.1.1.1		

Lattice

Definition

A Lattice \mathcal{L} in \Re^n is a discrete subgroup of \Re^n which spans the real vector space \Re^n .

$$\mathcal{L} = \left\{ \sum_{i=1}^n \lambda_i \mathbf{a_i} \mid \lambda_i \in \mathbb{Z} \right\}$$

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● ● ●

 a_1, a_2, \cdots, a_n is a basis of the lattice

Title	Definitions 0000 00	Algorithms 00000 0000 000	The dual Lattice 000 00	Attacking cryptosystems 00	End
			1.1.1.1		

Lattice

Definition

A Lattice \mathcal{L} in \Re^n is a discrete subgroup of \Re^n which spans the real vector space \Re^n .

$$\mathcal{L} = \left\{ \sum_{i=1}^n \lambda_i \mathbf{a_i} \mid \lambda_i \in \mathbb{Z} \right\}$$

 a_1, a_2, \cdots, a_n is a basis of the lattice



Figure: A Lattice in \Re^2 , and the set of the set of

Title	Definitions ○○●○○ ○○	Algorithms 00000 0000 00	The dual Lattice 000 00	Attacking cryptosystems 00	End

Title	Definitions	Algorithms	The dual Lattice	Attacking cryptosystems
	00000	00000	000	00
	00	0000	00	
		00		

Theorem

Let \mathcal{L} be a n-dimensional lattice and

• A be the $n \times n$ matrix whose rows are the basis a_1, \cdots, a_n .

▲ロト ▲冊ト ▲ヨト ▲ヨト - ヨー の々ぐ

• **B** be the $n \times n$ matrix whose rows $\mathbf{b_1}, \cdots, \mathbf{b_n} \in \mathcal{L}$.

The following conditions are equivalent:

Definitions	Algorithms	The dual Lattice	
00000	00000	000	

More useful things

Theorem

Let \mathcal{L} be a n-dimensional lattice and

- A be the $n \times n$ matrix whose rows are the basis a_1, \cdots, a_n .
- **B** be the $n \times n$ matrix whose rows $\mathbf{b_1}, \cdots, \mathbf{b_n} \in \mathcal{L}$.

The following conditions are equivalent:

1.
$$\mathbf{b_1}, \cdots, \mathbf{b_n}$$
 form a basis for \mathcal{L} .

- 2. $|\det(\mathbf{A})| = |\det(\mathbf{B})|$.
- 3. there is an $n \times n$ matrix **U** such that **B** = **UA** and $|\det(\mathbf{U})| = 1$.

Definitions	Algorithms	The dual Lattice
00000	00000	000
00	0000	00

Theorem

Let \mathcal{L} be a n-dimensional lattice and

- A be the $n \times n$ matrix whose rows are the basis a_1, \cdots, a_n .
- **B** be the $n \times n$ matrix whose rows $\mathbf{b_1}, \cdots, \mathbf{b_n} \in \mathcal{L}$.

The following conditions are equivalent:

1.
$$\mathbf{b_1}, \cdots, \mathbf{b_n}$$
 form a basis for \mathcal{L} .

- 2. $|\det(\mathbf{A})| = |\det(\mathbf{B})|$.
- 3. there is an $n \times n$ matrix **U** such that **B** = **UA** and $|\det(\mathbf{U})| = 1$.

So the determinant of all the bases of ${\cal L}$ is invariable. ${\sf det}({\bm A})={\sf det}\,{\cal L}$

Title	Definitions	Algorithms	The dual Lattice	Attacking cryptosystems	End
	00000 00	00000	000	00	

Definition

The Eucledian norm of a vector **x** is $\|\mathbf{x}\| = \sqrt{x_1^2 + \cdots + x_n^2}$ where x_1, x_2, \cdots, x_n are the coefficients in an orthonormal system.

・ロト ・ 同 ト ・ 三 ト ・ 三 ・ うへつ

Title	Definitions	Algorithms	The dual Lattice	Attacking cryptosystems	End
	00000 00	00000	000	00	

Definition

The *Eucledian norm* of a vector **x** is $||\mathbf{x}|| = \sqrt{x_1^2 + \cdots + x_n^2}$ where x_1, x_2, \cdots, x_n are the coefficients in an orthonormal system.

▲ロト ▲母 ト ▲ 臣 ト ▲ 臣 ト ● 回 ● ● ● ●

Definition

Hadamard's inequality states that $\mathsf{det}\,\mathcal{L} \leq \|a_1\| \cdots \|a_n\|$

Title	Definitions	Algorithms	The dual Lattice	Attacking cryptosystems	End
	00000 00	00000	000 00	00	

Definition

The *Eucledian norm* of a vector **x** is $||\mathbf{x}|| = \sqrt{x_1^2 + \cdots + x_n^2}$ where x_1, x_2, \cdots, x_n are the coefficients in an orthonormal system.

Definition

Hadamard's inequality states that $\mathsf{det}\,\mathcal{L} \leq \|a_1\| \cdots \|a_n\|$

Definition

Orthogonality defect of the basis a_1, a_2, \cdots, a_n

$$\frac{\|\mathbf{a_1}\|\cdots\|\mathbf{a_n}\|}{\det \mathcal{L}}$$



The linearly independent vectors $\mathbf{b_1}, \cdots, \mathbf{b_k} \in \mathcal{L}$ are *primitive* if they can be extended to a basis of \mathcal{L} .



The linearly independent vectors $\mathbf{b_1}, \cdots, \mathbf{b_k} \in \mathcal{L}$ are *primitive* if they can be extended to a basis of \mathcal{L} .

Definition

A vector $\mathbf{a} \in \mathcal{L}$ is *shortest in its direction* if $x\mathbf{a}$ is not in \mathcal{L} for 0 < x < 1.



The linearly independent vectors $\mathbf{b_1}, \cdots, \mathbf{b_k} \in \mathcal{L}$ are *primitive* if they can be extended to a basis of \mathcal{L} .

Definition

A vector $\mathbf{a} \in \mathcal{L}$ is *shortest in its direction* if $x\mathbf{a}$ is not in \mathcal{L} for 0 < x < 1.

▲ロト ▲冊ト ▲ヨト ▲ヨト - ヨー の々ぐ

Theorem

Vector $\mathbf{a} \in \mathcal{L}$ is primitive iff \mathbf{a} is shortest in its direction.

Title	Definitions ○○○○○ ●○	Algorithms 00000 0000 000	The dual Lattice 000 00	Attacking cryptosystems 00	End

Contents

▲ロト ▲園 ト ▲ 臣 ト ▲ 臣 ト 一臣 - のへで

Title

Definitions

Useful Definitions

The Problem

Algorithms

Main Idea-Algorithms for 1,2-dimensions Preparation for the LLL Algorithm The Algorithm

The dual Lattice

Some definitions

Gram-Schmidt lower bound property

Attacking cryptosystems

A Lattice attack on RSA

End

Title	Definitions	Algorithms	The dual Lattice	Attacking cryptosystems	End
	00000	00000	000	00	

Shortest vector problem

Definition

Given a lattice \mathcal{L} , find the shortest vector, in Eucledian norm, in \mathcal{L} .



▲ロト ▲園 ト ▲ 臣 ト ▲ 臣 ト 一臣 - のへで

Title	Definitions	Algorithms	The dual Lattice	Attacking cryptosystems	End
	00000	00000	000	00	

Shortest vector problem

Definition

Given a lattice \mathcal{L} , find the shortest vector, in Eucledian norm, in \mathcal{L} .



▲ロト ▲園 ト ▲ 臣 ト ▲ 臣 ト 一臣 - のへで

Title	Definitions	Algorithms	The dual Lattice	Attacking cryptosystems	End
	00000	00000	000	00	

Shortest vector problem

Definition

Given a lattice \mathcal{L} , find the shortest vector, in Eucledian norm, in \mathcal{L} .



The shortest of the basis is not always the shortest vector.

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ 三臣 - のへで

Title	Definitions 00000 00	Algorithms • 0000 · 000 · 000 · 000	The dual Lattice 000 00	Attacking cryptosystems 00	End

Contents

▲ロト ▲冊ト ▲ヨト ▲ヨト - ヨー の々ぐ

Title

Definitions Useful Definiti The Problem

Algorithms

Main Idea-Algorithms for 1,2-dimensions

Preparation for the LLL Algorithm The Algorithm

The dual Lattice

Some definitions

Gram-Schmidt lower bound property

Attacking cryptosystems

A Lattice attack on RSA

End

Title	Definitions 00000 00	Algorithms 0000 000 000	The dual Lattice 000 00	Attacking cryptosystems 00	End

A good strategy:





A good strategy:

1. Change the basis of the lattice (in some way) to a good one (short vectors nearly orthogonal).

▲ロト ▲冊ト ▲ヨト ▲ヨト ヨー のくで



A good strategy:

1. Change the basis of the lattice (in some way) to a good one (short vectors nearly orthogonal).

▲ロト ▲冊ト ▲ヨト ▲ヨト ヨー のくで

2. Take the shortest vector of the basis.



A good strategy:

1. Change the basis of the lattice (in some way) to a good one (short vectors nearly orthogonal).

▲ロト ▲冊ト ▲ヨト ▲ヨト - ヨー の々ぐ

2. Take the shortest vector of the basis.

We must prove that this vector is the shortest, or the shortest within some factor.



A good strategy:

1. Change the basis of the lattice (in some way) to a good one (short vectors nearly orthogonal).

▲ロト ▲冊ト ▲ヨト ▲ヨト - ヨー の々ぐ

2. Take the shortest vector of the basis.

We must prove that this vector is the shortest, or the shortest within some factor.

Step 1 is called Lattice (Basis) Reduction



A good strategy:

- 1. Change the basis of the lattice (in some way) to a good one (short vectors nearly orthogonal).
- 2. Take the shortest vector of the basis.

We must prove that this vector is the shortest, or the shortest within some factor.

Step 1 is called Lattice (Basis) Reduction



A D > A D > A D > A D >

э

SQA



Euclid's Algorithm

◆ロト ◆昼 ト ◆臣 ト ◆臣 - のへで

• Consider an 1-d lattice with basis $a \in \Re$.

Title	Definitions 00000 00	Algorithms 00€00 0000	The dual Lattice 000 00	Attacking cryptosystems	End		
	Algor	ithm for th	ne 1-dimensio	nal Lattices			
Euclid's Algorithm							

▲□▶ ▲□▶ ▲ 臣▶ ★ 臣▶ 三臣 - のへぐ

 Consider an 1-d lattice with basis a ∈ ℜ. Then the shortest vector is simply a.



- Consider an 1-d lattice with basis a ∈ ℜ. Then the shortest vector is simply a.
- Consider an 1-d lattice with basis $a, b \in \Re$.



- Consider an 1-d lattice with basis a ∈ ℜ. Then the shortest vector is simply a.
- Consider an 1-d lattice with basis a, b ∈ ℜ.
 Then the shortest vector is the smallest number expressed as an integer l.c. of a, b:



- Consider an 1-d lattice with basis a ∈ ℜ. Then the shortest vector is simply a.
- Consider an 1-d lattice with basis a, b ∈ ℜ.
 Then the shortest vector is the smallest number expressed as an integer l.c. of a, b: gcd(a, b).



- Consider an 1-d lattice with basis a ∈ ℜ. Then the shortest vector is simply a.
- Consider an 1-d lattice with basis a, b ∈ ℜ. Then the shortest vector is the smallest number expressed as an integer l.c. of a, b: gcd(a, b). Euclid's algorithm: gcd(a, b) = gcd(b, a - mb) where m is the integer closest to a/b.

itle

Algorithms

The dual Lattic

Attacking cryptosystems

Algorithm for the 2-dimensional Lattices Gauss reduced basis







The dual Lattice

▲ロト ▲冊ト ▲ヨト ▲ヨト ヨー のくで

End

Algorithm for the 2-dimensional Lattices Gauss reduced basis

How orthogonal our basis vectors have to be?





The dual Lattice

▲ロト ▲冊ト ▲ヨト ▲ヨト - ヨー の々ぐ

Algorithm for the 2-dimensional Lattices

Gauss reduced basis

How orthogonal our basis vectors have to be?

Theorem

Suppose $\mathbf{b_1}, \mathbf{b_2}$ is a basis for a 2-d \mathcal{L} and $\|\mathbf{b_1}\| \le \|\mathbf{b_2}\|$. Suppose $\theta \in (0^\circ, 180^\circ)$ the angle between the two vectors. If $60^\circ \le \theta \le 120^\circ$ then $\mathbf{b_1}$ is the shortest vector in \mathcal{L} .


Algorithms

The dual Lattic

▲ロト ▲冊ト ▲ヨト ▲ヨト - ヨー の々ぐ

S

Algorithm for the 2-dimensional Lattices Gauss reduced basis

How orthogonal our basis vectors have to be?

Theorem

Suppose $\mathbf{b_1}, \mathbf{b_2}$ is a basis for a 2-d \mathcal{L} and $\|\mathbf{b_1}\| \le \|\mathbf{b_2}\|$. Suppose $\theta \in (0^\circ, 180^\circ)$ the angle between the two vectors. If $60^\circ \le \theta \le 120^\circ$ then $\mathbf{b_1}$ is the shortest vector in \mathcal{L} .

Let $\mu_{21}\mathbf{b_1}$ denote the projection of the vector $\mathbf{b_2}$ in the direction of the vector $\mathbf{b_1}$:



Algorithms

The dual Lattic

Attacking cryptosystem:

▲ロ ▶ ▲ 理 ▶ ▲ 国 ▶ ▲ 国 ■ ● ● ● ● ●

Algorithm for the 2-dimensional Lattices Gauss reduced basis

How orthogonal our basis vectors have to be?

Theorem

Suppose $\mathbf{b_1}, \mathbf{b_2}$ is a basis for a 2-d \mathcal{L} and $\|\mathbf{b_1}\| \le \|\mathbf{b_2}\|$. Suppose $\theta \in (0^\circ, 180^\circ)$ the angle between the two vectors. If $60^\circ \le \theta \le 120^\circ$ then $\mathbf{b_1}$ is the shortest vector in \mathcal{L} .

Let $\mu_{21}\mathbf{b_1}$ denote the projection of the vector $\mathbf{b_2}$ in the direction of the vector $\mathbf{b_1}$:

$$\mu_{21} = \frac{\|\mathbf{b_2}\| \cdot \|\mathbf{b_1}\|}{\|\mathbf{b_1}\|^2}$$





Algorithm for the 2-dimensional Lattices Gauss reduced basis

How orthogonal our basis vectors have to be?

Theorem

Suppose $\mathbf{b_1}, \mathbf{b_2}$ is a basis for a 2-d \mathcal{L} and $\|\mathbf{b_1}\| \leq \|\mathbf{b_2}\|$. Suppose $\theta \in (0^{\circ}, 180^{\circ})$ the angle between the two vectors. If $60^{\circ} < \theta < 120^{\circ}$ then **b**₁ is the shortest vector in \mathcal{L} .

Let $\mu_{21}\mathbf{b_1}$ denote the projection of the vector $\mathbf{b_2}$ in the direction of the vector **b**₁:

$$\mu_{21} = \frac{\|\mathbf{b_2}\| \cdot \|\mathbf{b_1}\|}{\|\mathbf{b_1}\|^2}$$

If $\|\mathbf{b_1}\| \leq \|\mathbf{b_2}\|$ and $|\mu_{21}| \leq 1/2$ then the basis $\mathbf{b_1}, \mathbf{b_2}$ is Gauss reduced basis.



▲ロト ▲冊ト ▲ヨト ▲ヨト - ヨー の々ぐ

Algorithm for S.V. in 2-d

 $\label{eq:constraint} \begin{array}{l} \mbox{repeat} \\ \mbox{if } \| {\bf b_1} \| > \| {\bf b_2} \| \mbox{ then} \\ \mbox{swap } {\bf b_1}, {\bf b_2} \\ \mbox{end if} \\ \mbox{$m \leftarrow \lfloor \mu_{21} \rceil$} \\ \mbox{$\bf b_2 \leftarrow {\bf b_2} - m {\bf b_1}$} \\ \mbox{until } \| {\bf b_1} \| < \| {\bf b_2} \| \\ \mbox{return } {\bf b_1} \end{array}$



Algorithm for S.V. in 2-d

 $\label{eq:constraint} \begin{array}{l} \mbox{repeat} \\ \mbox{if } \| {\bf b}_1 \| > \| {\bf b}_2 \| \mbox{ then} \\ \mbox{swap } {\bf b}_1, {\bf b}_2 \\ \mbox{end if} \\ \mbox{$m \leftarrow \lfloor \mu_{21} \rceil$} \\ \mbox{$\bf b_2 \leftarrow {\bf b}_2 - m {\bf b}_1$} \\ \mbox{until } \| {\bf b}_1 \| < \| {\bf b}_2 \| \\ \mbox{return } {\bf b}_1 \end{array}$

• Similarity with the Euclidean Algorithm

▲ロト ▲冊ト ▲ヨト ▲ヨト - ヨー の々ぐ



Algorithm for S.V. in 2-d

 $\begin{array}{l} \text{repeat} \\ \text{if } \|\mathbf{b_1}\| > \|\mathbf{b_2}\| \text{ then} \\ \text{swap } \mathbf{b_1}, \mathbf{b_2} \\ \text{end if} \\ m \leftarrow \lfloor \mu_{21} \rceil \\ \mathbf{b_2} \leftarrow \mathbf{b_2} - m \mathbf{b_1} \\ \text{until } \|\mathbf{b_1}\| < \|\mathbf{b_2}\| \\ \text{return } \mathbf{b_1} \end{array}$

- Similarity with the Euclidean Algorithm
- Terminates in a finite amount of time

▲ロト ▲冊ト ▲ヨト ▲ヨト - ヨー の々ぐ



Algorithm for S.V. in 2-d

 $\label{eq:constraint} \begin{array}{l} \mbox{repeat} \\ \mbox{if } \| {\bf b}_1 \| > \| {\bf b}_2 \| \mbox{ then} \\ \mbox{swap } {\bf b}_1, {\bf b}_2 \\ \mbox{end if} \\ \mbox{$m \leftarrow \lfloor \mu_{21} \rceil$} \\ \mbox{$\bf b_2 \leftarrow {\bf b}_2 - m {\bf b}_1$} \\ \mbox{until } \| {\bf b}_1 \| < \| {\bf b}_2 \| \\ \mbox{return } {\bf b}_1 \end{array}$

- Similarity with the Euclidean Algorithm
- Terminates in a finite amount of time
- Polynomial complexity

◆□▶ ◆□▶ ◆注▶ ◆注▶ □注 − ���?

Title	Definitions 00000 00	Algorithms 0000 000 000	The dual Lattice 000 00	Attacking cryptosystems	End

Contents

▲ロト ▲園 ト ▲ 臣 ト ▲ 臣 ト 一臣 - のへで

Title

Definitions Useful Definiti The Problem

Algorithms

Main Idea-Algorithms for 1,2-dimensions Preparation for the LLL Algorithm

The Algorithm

The dual Lattice

Some definitions

Gram-Schmidt lower bound property

Attacking cryptosystems

A Lattice attack on RSA

End

Title	Definitions	Algorithms	The dual Lattice	Attacking cryptosystems	End
	00000	00000	000	00	
	00	0000	00		
		00			

Gram-Schmidt orthogonalization

Let $b_1 \cdots b_n$ the basis of \mathcal{L} .





Gram-Schmidt orthogonalization

Let $\mathbf{b_1} \cdots \mathbf{b_n}$ the basis of \mathcal{L} . The *Gram-Schmidt orthogonalization* of this basis is: $\mathbf{b_1^*} \cdots \mathbf{b_n^*}$ and is given by the following iterative formula:

$$\begin{aligned} \mathbf{b_1^*} &= \mathbf{b_1} \\ \mathbf{b_i^*} &= \mathbf{b_i} - \sum_{j=1}^{i-1} \frac{\mathbf{b_i b_j^*}}{\|\mathbf{b_j^*}\|^2} \mathbf{b_j^*} \end{aligned}$$

▲ロト ▲冊ト ▲ヨト ▲ヨト - ヨー の々ぐ



Gram-Schmidt orthogonalization

Let $\mathbf{b_1} \cdots \mathbf{b_n}$ the basis of \mathcal{L} . The *Gram-Schmidt orthogonalization* of this basis is: $\mathbf{b_1^*} \cdots \mathbf{b_n^*}$ and is given by the following iterative formula:

$$\mathbf{b_1^*} = \mathbf{b_1}$$
 $\mathbf{b_i^*} = \mathbf{b_i} - \sum_{j=1}^{i-1} rac{\mathbf{b_i b_j^*}}{\|\mathbf{b_j^*}\|^2} \mathbf{b_j^*}$

Define

$$\mu_{ij} = \frac{\mathbf{b}_i \mathbf{b}_j^*}{\|\mathbf{b}_j^*\|^2}$$

and $\mu_{ii} = 1$. Then

$$\mathbf{b_i} = \sum_{j=1}^{i-1} \mu_{ij} \mathbf{b_j^*}$$

▲ロ ▶ ▲ 理 ▶ ▲ 国 ▶ ▲ 国 ■ ● ● ● ● ●

Title	Definitions	Algorithms	The dual Lattice	Attacking cryptosystems	End
	00000		000	00	

Lower bounding OPT



・ロト ・ 四ト ・ ヨト ・ ヨト

E

590

 $b_I = b_I^*$

Title	Definitions	Algorithms	The dual Lattice	Attacking cryptosystems	End
	00000	00000	000	00	

Lower bounding OPT



If OPT is the length of the shortest vector in the lattice then:

$$OPT \geq min\{\|\mathbf{b}_1^*\|, \cdots, \|\mathbf{b}_n^*\|\}$$

・ロト ・ 語 ・ ・ 語 ・ ・ 語 ・ ・ の へ ()



<□▶ <□▶ < □▶ < □▶ < □▶ = □ の < ⊙

The basis $\mathbf{b_1}, \cdots, \mathbf{b_n}$ is LLL reduced if for $1 \le i \le n-1$:



▲ロ ▶ ▲ 理 ▶ ▲ 国 ▶ ▲ 国 ■ ● ● ● ● ●

The basis $\mathbf{b_1}, \cdots, \mathbf{b_n}$ is LLL reduced if for $1 \le i \le n-1$:

- $|\mu_{ij}| \leq \frac{1}{2}$ for $1 \leq i < j \leq n$ and
- $\|\mathbf{b}_{\mathbf{i}}^*\|^2 \le \frac{4}{3} \|\mathbf{b}_{\mathbf{i+1}}^* + \mu_{i+1,i} \mathbf{b}_{\mathbf{i}}^*\|^2$



The basis $\mathbf{b_1}, \cdots, \mathbf{b_n}$ is LLL reduced if for $1 \le i \le n-1$:

- $|\mu_{ij}| \leq \frac{1}{2}$ for $1 \leq i < j \leq n$ and
- $\|\mathbf{b}_{\mathbf{i}}^*\|^2 \le \frac{4}{3} \|\mathbf{b}_{\mathbf{i+1}}^* + \mu_{i+1,i} \mathbf{b}_{\mathbf{i}}^*\|^2$

An LLL Reduced Basis is reasonably orthogonal:

$$\frac{\|\mathbf{b_1}\|\cdots\|\mathbf{b_n}\|}{\det\mathcal{L}} \leq 2^{\frac{n(n-1)}{2}}$$

▲ロ ▶ ▲ 理 ▶ ▲ 国 ▶ ▲ 国 ■ ● ● ● ● ●



The basis $\mathbf{b_1}, \cdots, \mathbf{b_n}$ is LLL reduced if for $1 \le i \le n-1$:

- $|\mu_{ij}| \leq \frac{1}{2}$ for $1 \leq i < j \leq n$ and
- $\|\mathbf{b}_{\mathbf{i}}^*\|^2 \leq \frac{4}{3} \|\mathbf{b}_{\mathbf{i+1}}^* + \mu_{\mathbf{i+1},\mathbf{i}}\mathbf{b}_{\mathbf{i}}^*\|^2$

An LLL Reduced Basis is reasonably orthogonal:

$$\frac{\|\mathbf{b_1}\|\cdots\|\mathbf{b_n}\|}{\det \mathcal{L}} \leq 2^{\frac{n(n-1)}{2}}$$

In an LLL Reduced Basis we have that:

$$\|\mathbf{b_1}\| \le 2^{\frac{n-1}{2}} OPT$$

▲ロト ▲冊ト ▲ヨト ▲ヨト - ヨー の々ぐ



The basis $\mathbf{b_1}, \cdots, \mathbf{b_n}$ is LLL reduced if for $1 \le i \le n-1$:

- $|\mu_{ij}| \leq \frac{1}{2}$ for $1 \leq i < j \leq n$ and
- $\|\mathbf{b}_{\mathbf{i}}^*\|^2 \le \frac{4}{3} \|\mathbf{b}_{\mathbf{i+1}}^* + \mu_{i+1,i} \mathbf{b}_{\mathbf{i}}^*\|^2$

An LLL Reduced Basis is reasonably orthogonal:

$$\frac{\|\mathbf{b_1}\|\cdots\|\mathbf{b_n}\|}{\det\mathcal{L}} \leq 2^{\frac{n(n-1)}{2}}$$

In an LLL Reduced Basis we have that:

$$\|\mathbf{b_1}\| \le 2^{\frac{n-1}{2}} OPT$$

▲ロ ▶ ▲ 理 ▶ ▲ 国 ▶ ▲ 国 ■ ● ● ● ● ●

So we want an algorithm which turns an arbitrary basis into an LLL reduced in polynomial time in n.

Title	Definitions 00000 00	Algorithms	The dual Lattice 000 00	Attacking cryptosystems 00	End

Contents

▲ロト ▲園 ト ▲ 臣 ト ▲ 臣 ト 一臣 - のへで

Title

Definitions Useful Def

The Problem

Algorithms

Main Idea-Algorithms for 1,2-dimensions Preparation for the LLL Algorithm

The Algorithm

The dual Lattice

Some definitions

Gram-Schmidt lower bound property

Attacking cryptosystems

A Lattice attack on RSA

End

Title	Definitions	Algorithms	The dual Lattice	Attacking cryptosystems	End
	00000	00000	000	00	

Shortest vector Algorithm

▲ロ ▶ ▲ 理 ▶ ▲ 国 ▶ ▲ 国 ■ ● ● ● ● ●

LLL
$$(\mathbf{B} = \mathbf{b}_1, \cdots, \mathbf{b}_n)$$

 $\mathbf{B} \leftarrow SizeReduce(\mathbf{B})$
while $\exists i$ violating $\|\mathbf{b}_i^*\|^2 \leq \frac{4}{3} \|\mathbf{b}_{i+1}^* + \mu_{i+1,i}\mathbf{b}_i^*\|^2$ do
swap $\mathbf{b}_i, \mathbf{b}_{i+1}$
update μ_{hk} and \mathbf{b}_k^* for all h, k
 $\mathbf{B} \leftarrow SizeReduce(\mathbf{B})$
end while
return \mathbf{b}_1

 $\begin{array}{l} \mbox{SizeReduce } (\mathbf{B} = \mathbf{b_1}, \cdots, \mathbf{b_n}) \\ \mbox{for } j = 2, \cdots, n \ \mbox{do} \\ \mbox{for } i = j - 1, \cdots, 1 \ \mbox{do} \\ \mbox{b_j} \leftarrow \mbox{b_j} - \lfloor \mu_{ji} \mbox{b_i} \end{bmatrix} \\ \mu_{jk} \leftarrow \mu_{jk} - \mu_{jj} \mbox{b_i} \mu_{ik} \ \mbox{for } k = 1, \cdots, i \\ \mbox{end for} \\ \mbox{end for} \\ \mbox{return } \ \mbox{B} \end{array}$

Title	Definitions 00000 00	Algorithms 00000 0000 00	The dual Lattice ●○○ ○○	Attacking cryptosystems 00	End

Contents

▲ロト ▲園 ト ▲ 臣 ト ▲ 臣 ト 一臣 - のへで

Title

Definitions

Useful Definitions The Problem

Algorithms

Main Idea-Algorithms for 1,2-dimensions Preparation for the LLL Algorithm The Algorithm

The dual Lattice

Some definitions

Gram-Schmidt lower bound property

Attacking cryptosystems

A Lattice attack on RSA

End

Title	Definitions	Algorithms	The dual Lattice	Attacking cryptosystems	End
	00000 00	00000 0000 00	000 00	00	

Title	Definitions	Algorithms	The dual Lattice	Attacking cryptosystems	End
	00000	00000	000	00	
	00	0000	00		

Definition

The *dual lattice* \mathcal{L}^* of the lattice \mathcal{L} is defined by:

$$\mathcal{L}^* = \{oldsymbol{v} \in \Re^n | orall oldsymbol{b} \in \mathcal{L}, oldsymbol{b} \cdot oldsymbol{v} \in \mathbb{Z} \}$$

▲□▶ ▲□▶ ▲ 臣▶ ★ 臣▶ 三臣 - のへぐ



Definition

The *dual lattice* \mathcal{L}^* of the lattice \mathcal{L} is defined by:

$$\mathcal{L}^* = \{oldsymbol{v} \in \Re^n | orall oldsymbol{b} \in \mathcal{L}, oldsymbol{b} \cdot oldsymbol{v} \in \mathbb{Z}\}$$

Theorem

Let $\mathbf{b_1} \cdots \mathbf{b_n}$ be any basis for \mathcal{L} . Then, the rows of $\mathbf{B}^{-\mathsf{T}}$ form a basis for the dual lattice \mathcal{L}^* . Furthermore, det $\mathcal{L}^* = \frac{1}{\det \mathcal{L}}$.

・ロット (四)・ (田)・ (日)・ (日)

Title	Definitions	Algorithms	The dual Lattice	Attacking cryptosystems	End
	00000	00000	000	00	
	00	0000	00		
		00			

Definition

The *dual lattice* \mathcal{L}^* of the lattice \mathcal{L} is defined by:

$$\mathcal{L}^* = \{oldsymbol{v} \in \Re^n | orall oldsymbol{b} \in \mathcal{L}, oldsymbol{b} \cdot oldsymbol{v} \in \mathbb{Z}\}$$

Theorem

Let $\mathbf{b_1} \cdots \mathbf{b_n}$ be any basis for \mathcal{L} . Then, the rows of $\mathbf{B}^{-\mathsf{T}}$ form a basis for the dual lattice \mathcal{L}^* . Furthermore, det $\mathcal{L}^* = \frac{1}{\det \mathcal{L}}$.

Definition

Let $v \in \Re^n$ be a non-zero vector. Then, v^{\perp} will denote the (n-1)-dimensional space $\{\mathbf{b} \in \Re^n | \mathbf{b} \cdot v = 0\}$

San

Title	Definitions	Algorithms	The dual Lattice	Attacking cryptosyst
	00000	00000	000	00
	00	0000	00	
		00		

Definition

A set $\mathcal{L}'\subset\mathcal{L}$ that is a lattice in its own right will be called sublattice of $\mathcal L$



▲□▶ ▲□▶ ▲ 臣▶ ★ 臣▶ 三臣 - のへぐ

Title	Definitions	Algorithms	The dual Lattice	
	00000	00000	000	
	00	0000	00	

▲ロト ▲冊ト ▲ヨト ▲ヨト - ヨー の々ぐ

End

The dual lattice \mathcal{L}^*

Definition

A set $\mathcal{L}'\subset\mathcal{L}$ that is a lattice in its own right will be called sublattice of $\mathcal L$

Lemma

Let $v \in \mathcal{L}^*$ be primitive. Then

- $\mathcal{L} \cap (v^{\perp})$ is an (n-1)-dimensional sublattice of \mathcal{L} .
- There is a vector $\mathbf{b} \in \mathcal{L}$ such that $\boldsymbol{v} \cdot \mathbf{b} = 1$

itle	Definitions	Algorithms	The dual Lattice	
	00000	00000	000	
	00	0000	00	

Definition

A set $\mathcal{L}'\subset\mathcal{L}$ that is a lattice in its own right will be called sublattice of $\mathcal L$

Lemma

Let $\boldsymbol{\upsilon} \in \mathcal{L}^*$ be primitive. Then

- $\mathcal{L} \cap (v^{\perp})$ is an (n-1)-dimensional sublattice of \mathcal{L} .
- There is a vector $\mathbf{b} \in \mathcal{L}$ such that $v \cdot \mathbf{b} = 1$

Lemma

We can create a basis $\mathbf{w}_n, \dots, \mathbf{w}_1$ with Gram-Schmidt orthogonalization $\left(\frac{\boldsymbol{v}_n}{\|\boldsymbol{v}_n\|^2}, \dots, \frac{\boldsymbol{v}_1}{\|\boldsymbol{v}_1\|^2}\right)$.

Title	Definitions 00000 00	Algorithms 00000 0000 000	The dual Lattice ○○○ ●○	Attacking cryptosystems 00	End

Contents

▲ロト ▲園 ト ▲ 臣 ト ▲ 臣 ト 一臣 - のへで

Title

Definitions

Useful Definitions The Problem

Algorithms

Main Idea-Algorithms for 1,2-dimensions Preparation for the LLL Algorithm The Algorithm

The dual Lattice

Some definitions

Gram-Schmidt lower bound property

Attacking cryptosystems

A Lattice attack on RSA

End

Title	Definitions	Algorithms	The dual Lattice	Attacking cryptosystems	E
	00000	00000	000	00	
		00			

Gram-Schmidt lower bound is not so bad

▲□▶ ▲□▶ ▲三▶ ▲三▶ 三回 りへぐ



The dual Lattice

Gram-Schmidt lower bound is not so bad

Minkowski's theorem

There is a vector $\mathbf{b} \in \mathcal{L}$ such that $\|\mathbf{b}\| \leq \sqrt{n} \sqrt[n]{\det \mathcal{L}}$.

▲□▶ ▲圖▶ ▲≣▶ ▲≣▶ = ● ● ●



The dual Lattice

Gram-Schmidt lower bound is not so bad

Minkowski's theorem

There is a vector $\mathbf{b} \in \mathcal{L}$ such that $\|\mathbf{b}\| \leq \sqrt{n}\sqrt[n]{\det \mathcal{L}}$.

Theorem

There is a basis for \mathcal{L} whose Gram-Schmidt lower bound is at least OPT/n.

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三回 ● のへで

Title	Definitions 00000 00	Algorithms 00000 0000 000	The dual Lattice 000 00	Attacking cryptosystems ●0	End

Contents

▲ロト ▲園 ト ▲ 臣 ト ▲ 臣 ト 一臣 - のへで

Title

Definitions

Useful Definitions The Problem

Algorithms

Main Idea-Algorithms for 1,2-dimensions Preparation for the LLL Algorithm The Algorithm

The dual Lattice

Some definitions Gram-Schmidt lower bound property

Attacking cryptosystems

A Lattice attack on RSA

End

Title	Definitions	Algorithms	The dual Lattice	Attacking cryptosystems	End
	00000	00000	000	0.	

Solving modular equations

▲□▶ ▲□▶ ▲三▶ ▲三▶ 三回 りへぐ

Title	Definitions 00000 00	Algorithms 00000 0000	The dual Lattice 000 00	Attacking cryptosystems O•	End
		00			

Solving modular equations

Lemma

If f is a polynomial modulo n and h is a polynomial having the same roots as f modulo n and has 'small' norm then all the roots of f (smaller than some value) are also roots of h over the integers.

・ロト ・ 同 ト ・ 三 ト ・ 三 ・ うへつ

Title	Definitions	Algorithms	The dual Lattice	Attacking cryptosystems	End
	00000	00000 0000 00	000 00	0•	

Solving modular equations

Lemma

If f is a polynomial modulo n and h is a polynomial having the same roots as f modulo n and has 'small' norm then all the roots of f (smaller than some value) are also roots of h over the integers.

The LLL algorithm can find such a polynomial h and then solve the equation h(x) = 0 over the integers to get small solutions.

・ロト ・ 同 ト ・ 三 ト ・ 三 ・ うへつ
Title	Definitions 00000 00	Algorithms 00000 0000 000	The dual Lattice 000 00	Attacking cryptosyste

QUESTIONS



・ロト ・ 通 ト ・ 注 ト ・ 注 ・ つ へ ()・

End