On the ideal shortest vector problem over random rational primes

Qi Cheng

School of Computer Science
University of Oklahoma

Oct 2021
EuroCrypt

This is a joint work with Yanbin Pan, Jun Xu and Nick Wadleigh.

Lattice-based cryptography

- Quantum resistant.

Lattice-based cryptography

- Quantum resistant.
- Fast operation (addition and multiplication on small numbers, no exponentiation)

Lattice-based cryptography

- Quantum resistant.
- Fast operation (addition and multiplication on small numbers, no exponentiation)
- Worst case hardness

Lattice-based cryptography

- Quantum resistant.
- Fast operation (addition and multiplication on small numbers, no exponentiation)
- Worst case hardness
- Low dimensional lattice problem is easy $\rightarrow$ Key size Problem

Lattice-based cryptography

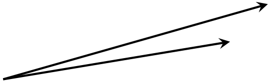
- Quantum resistant.
- Fast operation (addition and multiplication on small numbers, no exponentiation)
- Worst case hardness
- Low dimensional lattice problem is easy $\rightarrow$ Key size Problem $\rightarrow$ Ideal lattice

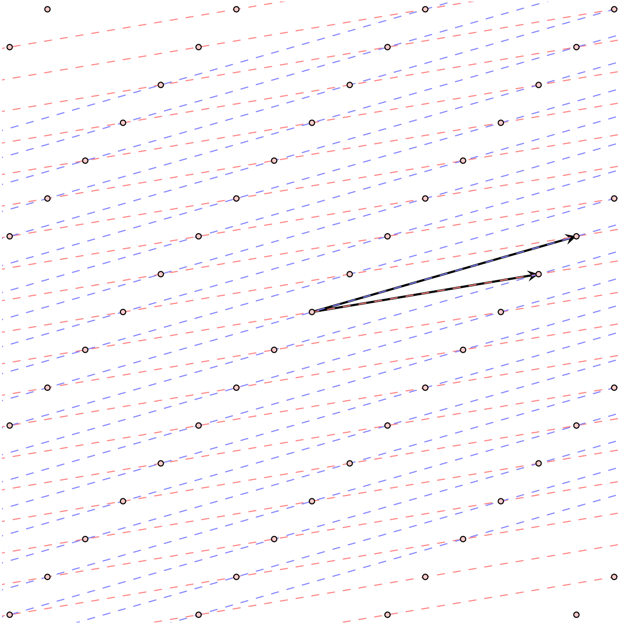
What Is a Lattice?

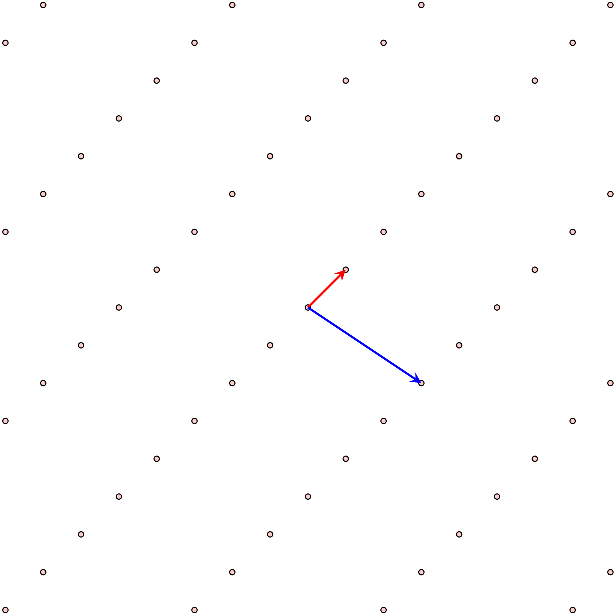
Given n linearly independent vectors $\mathrm{b_1}, \ldots, \mathrm{b_n} \in \mathbb{R}^m$ $(n \leq m)$, the lattice generated by them is the set of vectors

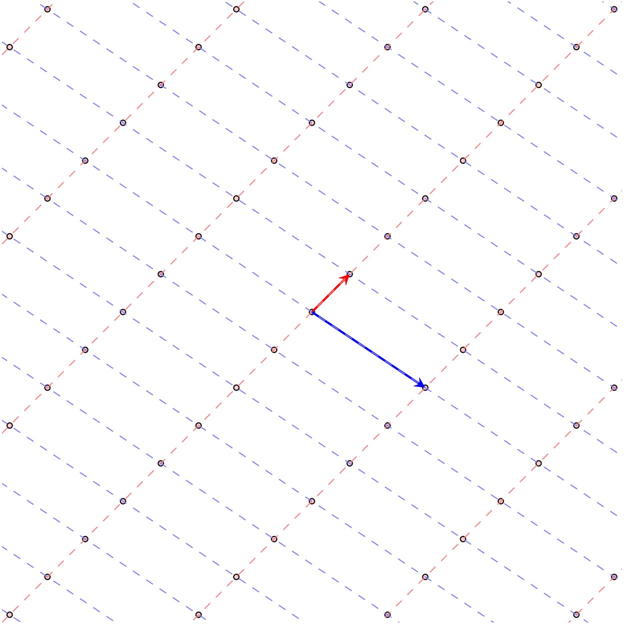
$$L(\mathrm{b_1}, \ldots, \mathrm{b_n}) = \{\sum_{i=1}^{n} x_i \mathrm{b_i} : x_i \in \mathbb{Z}\}$$

The vectors $\mathrm{b_1}, \ldots, \mathrm{b_n}$ form a basis of the lattice.









The shortest vector

- Hermite bound: $\sqrt{n}det(L)^{1/n}$ (uniform)
- On average has length $(1+o(1))\sqrt{\frac{n}{2e\pi}}det(L)^{1/n}$ (Gauss Heuristic)
- Must have length less than $(1+o(1))\sqrt{\frac{2n}{e\pi}}det(L)^{1/n}$. (The Minkowski Convex Body Theorem)

The shortest vector

- Hermite bound: $\sqrt{n} det(L)^{1/n}$ (uniform)
- On average has length $(1 + o(1))\sqrt{\frac{n}{2e\pi}} det(L)^{1/n}$ (Gauss Heuristic)
- Must have length less than $(1 + o(1))\sqrt{\frac{2n}{e\pi}} det(L)^{1/n}$. (The Minkowski Convex Body Theorem)
- SVP, approx-SVP, Hermite-SVP: find vectors of length $\leq \lambda_1, \gamma\lambda_1$ and $\gamma det(L)^{1/n}$ respectively.

Number Rings

- A number field over $\mathbf{Q}$: $L = \mathbf{Q}[x]/(x^N + \cdots)$
- The ring of integers O_L is a free $\mathbf{Z}$-module. If monogenic, then $\alpha \in O_L$ may be chosen so that

$$O_L = \mathbf{Z} + \alpha\mathbf{Z} + \alpha^2\mathbf{Z} + ... + \alpha^{N-1}\mathbf{Z}$$

Canonical embeddings

A number field $\mathbb{K}$ of degree N over $\mathbf{Q}$ has exactly N embeddings into $\mathbb{C}$: $\sigma_1, \sigma_2, \cdots, \sigma_N$. The *canonical embedding* $\Sigma_{\mathbb{K}}$ sends $\mathbb{K}$ to $\mathbb{C}^N$:

$$\Sigma_{\mathbb{K}} : \mathbb{K} \to \mathbb{C}^N, \quad a \mapsto (\sigma_1(a), \sigma_2(a), \cdots, \sigma_N(a)).$$

The image of $\Sigma_{\mathbb{K}}$ falls into a subspace in $\mathbb{C}^N$, which is isomorphic to $\mathbf{R}^N$ as an inner product space.
Example $Q[x]/(x^4 + 1)$:
$1 \to (1, 1, 1, 1) \in \mathbb{C}^4$ or $(\sqrt{2}, 0, \sqrt{2}, 0) \in \mathbf{R}^4$.
$1 + x \to (1 + \zeta_8, 1 + \zeta_8^7, 1 + \zeta_8^3, 1 + \zeta_8^5)$ or
$(\sqrt{2}Re(1 + \zeta_8), \sqrt{2}Im(1 + \zeta_8), \sqrt{2}Re(1 + \zeta_8^3), \sqrt{2}Im(1 + \zeta_8^3) \in \mathbf{R}^4$.

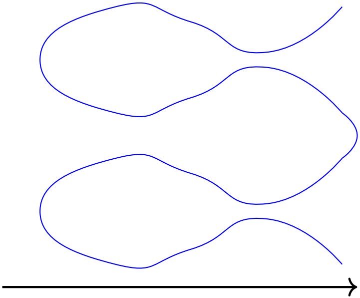
Coefficient Embedding

The *coefficient embedding,* is most commonly used in cryptographic constructions. If monogenic, map $\beta = a_0 + a_1\alpha + ... + a_{N-1}\alpha^{N-1}$ to its coefficient vector, $C(\beta) := (a_0, a_1, ..., a_{N-1})$.
Example $Q[x]/(x^4+1)$: $1 \to (1,0,0,0) \in \mathbf{Z}^4$.
$1 + 2x \to (1,2,0,0) \in \mathbf{Z}^4$

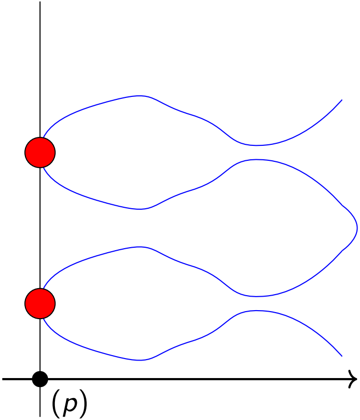
Ideal Lattices

	If $K = Q[x]/(x^N + 1)$
Principle ideal	$\mathbf{Z}(a_0, a_1, \cdots, a_{N-1})$
$g(x)O_K$	$+\mathbf{Z}(-a_{N-1}, a_0, \cdots, a_{N-2})$
	$\cdots$
	$+\mathbf{Z}(-a_1, -a_2, \cdots, a_0)$
General ideal	$+\mathbf{Z}(M, 0, \cdots, 0)$
$MO_K + g(x)O_K$	$+\mathbf{Z}(0, M, \cdots, 0)$
	$\cdots$
	$+\mathbf{Z}(0, 0, \cdots, M)$
Prime ideal	
$pO_K + g(x)O_K$	
Over $F_p, g(x)$ *is irreducible*	*and divides* $x^N + 1$ *over* F_p

Arithmetic Curves and Primes Ideals

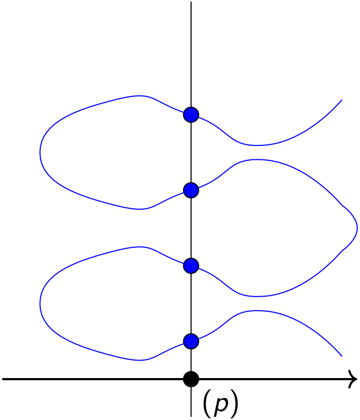


Arithmetic Curves and Primes Ideals



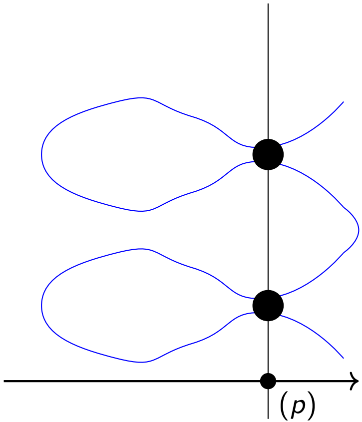
$(p) = P_1^2 P_2^2$

Arithmetic Curves and Primes Ideals



$$(p) = P_1 P_2 P_3 P_4$$

Arithmetic Curves and Primes Ideals



$$(p) = P_1 P_2$$

Decomposition groups

Let G be the Galois group of $\mathbb{L}$ over $\mathbb{Q}$. The decomposition group, D, and decomposition field, $\mathbb{K}$, for $\mathfrak{p}_1$ are defined as:

$$D := \{\sigma \in G : \sigma(\mathfrak{p}_1) = \mathfrak{p}_1\},$$

$$\mathbb{K} := \{x \in \mathbb{L} : \forall \sigma \in D, \sigma(x) = x\}.$$

- If p unramified, then D is isomorphic to $Gal((O_L/\mathfrak{p}_1)/F_p)$
- If $\mathfrak{p}_1 = (p, x^{N/g} + \cdots)$, then the degree of $\mathbb{K}$ over $\mathbb{Q}$ is g, and $det(\mathfrak{p}_1 \cap K) = p$.

A diagram

$$\begin{tikzcd}
\mathfrak{p} & \subset & O_{\mathbb{L}} & \subset & \mathbb{L} \arrow[r, "\Sigma_{\mathbb{L}}"] & \mathbb{C}^N \\
\mathfrak{c} \arrow[u, dash] & \subset & O_{\mathbb{K}} \arrow[u, dash] & \subset & \mathbb{K} \arrow[u, dash] \arrow[r, "\Sigma_{\mathbb{K}}"] & \mathbb{C}^g \arrow[u, "\beta"] \\
(p) \arrow[u, dash] & \subset & \mathbf{Z} \arrow[u, dash] & \subset & \mathbf{Q} \arrow[u, dash] & \subset & \mathbb{C} \arrow[u]
\end{tikzcd}$$

Here β is (up to permutation) just the linear embedding given by repeating each coordinate N/g times.

The main theorem

Theorem

Suppose $\mathbb{L}/\mathbb{Q}$ *is a finite Galois extension with degree* N*, and suppose* $\mathfrak{p}$ *is a prime ideal of* $O_{\mathbb{L}}$ *lying over an unramified rational prime* p *such that* $pO_{\mathbb{L}}$ *has* g *distinct prime ideal factors in* $O_{\mathbb{L}}$*. If* $\mathbb{K}$ *is the decomposition field of* $\mathfrak{p}$*, then a solution to Hermite-SVP with factor* γ *in the sublattice* $\mathfrak{c} = \mathfrak{p} \cap O_{\mathbb{K}}$ *under the canonical embedding of* $\mathbb{K}$ *will also be a solution to Hermite-SVP in* $\mathfrak{p}$ *with factor* $\frac{\sqrt{N/g}}{N_{\mathbb{K}}(disc(\mathbb{L}/\mathbb{K}))^{1/(2N)}} \cdot \gamma$ $(\leq \sqrt{\frac{N}{g}} \cdot \gamma)$ *under the canonical embedding of* $\mathbb{L}$*.*

Power of two cyclotomic fields

Theorem

For any prime ideal $\mathfrak{p} = (p, f(\zeta))$ in $\mathbf{Z}[\zeta]$, where p is an odd prime and $f(x)$ is some irreducible factor of $x^{2^n} + 1$ in $\mathbf{F}_p[x]$. Write

$$p = \begin{cases} 2^A \cdot m + 1, & \text{if } p \equiv 1 \pmod 4; \\ 2^A \cdot m - 1, & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

for some odd m and $A \geq 2$, and let

$$r = \begin{cases} \min\{A-1, n\}, & \text{if } p \equiv 1 \pmod 4; \\ \min\{A, n\}, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Then given an oracle that can solve SVP for 2^r-dimensional lattices, a shortest nonzero vector in $\mathfrak{p}$ can be found in $\mathrm{poly}(2^n, \log_2 p)$ time with the coefficient embedding.

Power of two cyclotomic fields

Theorem

Let $N = 2^n$*, where* n *is a positive integer. Let* $\mathfrak{p}$ *be a prime ideal in the ring* $\mathbf{Z}[x]/(x^N + 1)$*, and suppose* $\mathfrak{p}$ *contains a prime number* $p \equiv \pm 3 \pmod 8$*. Then under the coefficient embedding, the shortest vector in* $\mathfrak{p}$ *can be found in time poly*$(N, \log p)$*, and the length of the shortest vector is exactly* $\sqrt{p}$*.*

Complexity of Prime Ideals

Example $\mathbf{Z}[x]/(x^N + 1)$

p	dimension of $\mathfrak{p}_1 \cap K$
$\pm 3 \pmod 8$	2
$\pm 7 \pmod{16}$	4
$\pm 15 \pmod{32}$	8
$\pm 31 \pmod{64}$	16
$\vdots$	$\vdots$

Average case complexity

- To select a random prime ideal, one fixes a large M, uniformly randomly selects a prime number in the set

$$\{p \text{ is a prime} : p < M\},$$

  and then uniformly randomly selects a prime ideal lying over p.
- Select a prime ideal uniformly at random from the set

$$\{\mathfrak{p} \text{ prime ideal} : p \in \mathfrak{p}, p \text{ is a prime}, p < M\}.$$

- We select uniformly at random a prime ideal from the set

$$\{\mathfrak{p} \text{ prime ideal} : \mathcal{N}(\mathfrak{p}) < M\},$$

  where $\mathcal{N}(\mathfrak{p})$ is the norm of the ideal $\mathfrak{p}$.

Composite ideals

Let $N = 2^n$, where n is a positive integer. Let $\mathcal{I}$ be an ideal in the ring $\mathbf{Z}[x]/(x^N + 1)$ with prime factorization

$$\mathcal{I} = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_k.$$

If each $\mathfrak{p}_i$ contains a prime integer $\equiv \pm 3 \pmod 8$, the shortest vector in $\mathcal{I}$ can be found in time $\mathit{poly}(N, \log(\mathcal{N}(\mathcal{I})))$.

Open problems

- The length of the shortest vectors in prime ideals lying over rational primes not congruent to $\pm 3 \pmod 8$.
- The worst case hardness of prime ideal lattice SVP for power-of-two cyclotomic fields is also left open.

The end

Thank you !