Special Lattices in Cryptology

Combinatorial Geometry and Number Theory

Henry Bambury[1]

[1]ENS Paris, Inria

27 August 2024

Intro: New Standards in Quantum-Safe Crypto

- Shor's quantum algorithm threatens the RSA cryptosystem.
- This lead to the rise of lattice crypto (1996 $\rightarrow$ today)!

Federal Information Processing Standards Publication 203

Published: August 13, 2024
Effective: August 13, 2024

Announcing the

Module-Lattice-Based Key-Encapsulation Mechanism Standard

Figure: ML-KEM (Kyber)

Security from hard problems: SVP and CVP

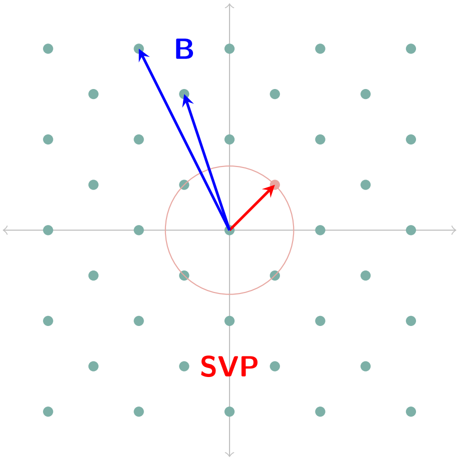
- RSA relies on the hardness of factoring.
- Lattice crypto relies on the hardness of finding short vectors in Euclidean lattices.

The Shortest Vector Problem (SVP)

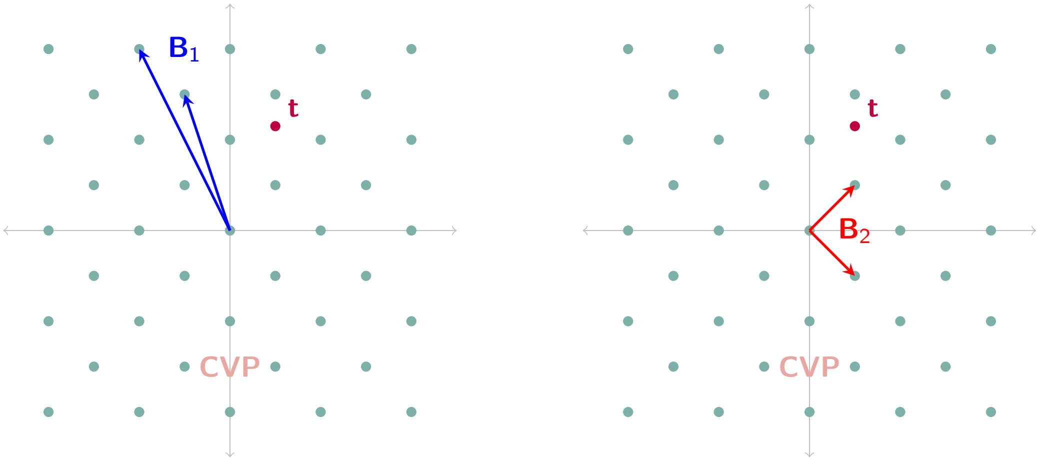
Given $\mathbf{B}$ a basis of a lattice $\Lambda \subset \mathbb{R}^n$, find a $\mathbf{v} \in \Lambda$ such that $\|\mathbf{v}\|_2 = \lambda_1(\Lambda)$.

The Closest Vector Problem (CVP)

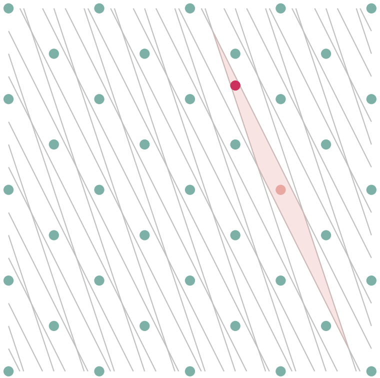
Given $\mathbf{B}$ a basis of a lattice $\Lambda \subset \mathbb{R}^n$ and a target vector $\mathbf{t} \in \mathbb{R}^n$, find a $\mathbf{v} \in \Lambda$ such that $\|\mathbf{t} - \mathbf{v}\|_2 = \text{dist}(\mathbf{t}, \Lambda)$.

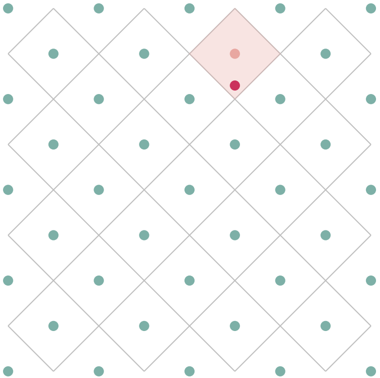


Security from hard problems: CVP (1)



Security from hard problems: CVP (2)





Security from hard problems: SVP and CVP

- In dim 2, a generalised version of Euclid's gcd algorithm is sufficient.
- Lattices in cryptographic schemes have dim ≈ 1000.
- "On average" in such dimensions, solving SVP is hard.
- But... crypto uses special classes of lattices $\rightarrow$ weaker security guarantees.

How to solve CVP:

- First reduce the lattice using LLL or stronger variants of this algorithm.
- Then conclude with clever rounding.

Lattice reduction is everywhere: factoring polynomials, breaking cryptography, finding linear relations, solving quadratic equations, computing class groups, disproving conjectures, representing ideals on a computer, ...

Lattices from ideals in number fields

- K a number field with signature (r_1, r_2) and discriminant Δ_K.
- $\mathcal{O}_K$ its ring of integers.
- Minkowski embedding sends ideals $\mathcal{I} \subseteq \mathcal{O}_K$ to lattices in $K \otimes \mathbb{R}$ (equipped with inner product $(x, y) \mapsto \mathrm{Tr}(x\overline{y})$).

Minkowski embedding:

$$\begin{array}{cccc} \sigma : & K & \to & K \otimes \mathbb{R} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \\ & \alpha & \mapsto & (\sigma_1(\alpha), \ldots, \sigma_{r_1+r_2}(\alpha)) \end{array}$$

Norm $\leftrightarrow$ Volume:

$$\mathrm{covol}(\sigma(\mathcal{I})) = N(\mathcal{I})\sqrt{|\Delta_K|}$$

Lemma (short vectors are somewhat large)

$$\sqrt{n}N(\mathcal{I})^{1/n} \leq \lambda_1(\sigma(\mathcal{I})) \leq \sqrt{|\Delta_K|}^{1/n}\sqrt{n}N(\mathcal{I})^{1/n}.$$

Ideal lattices: definition and examples

Definition

An **ideal lattice** is a lattice $\sigma(\mathcal{I}) \subset K \otimes \mathbb{R}$ where $\mathcal{I}$ is an $\mathcal{O}_K$-ideal, and $K \otimes \mathbb{R}$ is equipped with inner product $(x, y) \mapsto \mathrm{Tr}(\alpha x \overline{y})$, where $\alpha \in \mathrm{GL}_1(K \otimes \mathbb{R})$ and $\alpha = \overline{\alpha}$.

- Ideal lattices are *Hermitian line bundles* $(\mathcal{I}, \alpha)$.
- Many well-known lattices:
  - for $K = \mathbb{Q}(\sqrt{-3})$ and $(\mathcal{O}_K, 1)$ we get the hexagonal lattice.
  - many others also come from cyclotomic fields (E_8, Leech,...).

Nice property: full-rank lattices Λ such that $\mathcal{O}_K \cdot \Lambda \subseteq \Lambda$.

Ideal lattices: why are they useful?

- Widely used in cryptology since 2010.
- Bases can be stored much more efficiently.

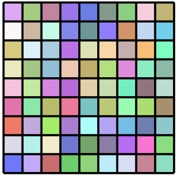


Figure: Random lattice basis

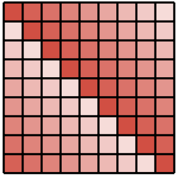


Figure: Structured lattice basis

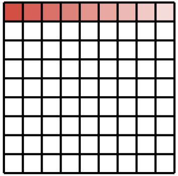


Figure: Storage gain!

Outside of crypto: the idea that lattices with nice symmetries have *large* shortest vectors was used by Venkatesh to prove high dimensional lattice packing lower bounds.

Ideal lattices in cyclotomic fields: (quantum) weakness [CDPR16]

Question

Given a basis for a (principal) $\mathcal{O}_K$-ideal $\mathcal{I}$, can one recover a *short* generator of $\mathcal{I}$?

Ideal lattices in cyclotomic fields: (quantum) weakness [CDPR16]

Question

Given a basis for a (principal) $\mathcal{O}_K$-ideal $\mathcal{I}$, can one recover a *short* generator of $\mathcal{I}$?

Log embedding: For $\alpha \in K^\times$,

$$\mathrm{Log}(\alpha) = (\ln|\sigma(\alpha)|)_\sigma \in \mathbb{R}^n.$$

Unit attack (principal case):

1. Start with a principal ideal $\mathcal{I}$;
2. Find a generator g of $\mathcal{I}$;
3. In $\Lambda := \mathrm{Log}(\mathcal{O}_K^\times)$, find a vector $\mathrm{Log}(u) \in \Lambda$ close to $\mathrm{Log}(g)$;
4. Output $g' := g/u$.

Ideal lattices in cyclotomic fields: (quantum) weakness [CDPR16]

Question

Given a basis for a (principal) $\mathcal{O}_K$-ideal $\mathcal{I}$, can one recover a *short* generator of $\mathcal{I}$?

- Step 2: easy with a **quantum computer**.
- Step 3: requires a short basis of (a sublattice of) Λ. It can be constructed in cyclotomic fields.

Log embedding: For $\alpha \in K^\times$,

$$\mathrm{Log}(\alpha) = (\ln|\sigma(\alpha)|)_\sigma \in \mathbb{R}^n.$$

Unit attack (principal case):

1. Start with a principal ideal $\mathcal{I}$;
2. Find a generator g of $\mathcal{I}$;
3. In $\Lambda := \mathrm{Log}(\mathcal{O}_K^\times)$, find a vector $\mathrm{Log}(u) \in \Lambda$ close to $\mathrm{Log}(g)$;
4. Output $g' := g/u$.

Ideal lattices in cyclotomic fields: (quantum) weakness [CDPR16]

Question

Given a basis for a (principal) $\mathcal{O}_K$-ideal $\mathcal{I}$, can one recover a *short* generator of $\mathcal{I}$?

- Step 2: easy with a **quantum computer**.
- Step 3: requires a short basis of (a sublattice of) Λ. It can be constructed in cyclotomic fields.

Log embedding: For $\alpha \in K^\times$,

$$\mathrm{Log}(\alpha) = (\ln|\sigma(\alpha)|)_\sigma \in \mathbb{R}^n.$$

Unit attack (principal case):

1. Start with a principal ideal $\mathcal{I}$;
2. Find a generator g of $\mathcal{I}$;
3. In $\Lambda := \mathrm{Log}(\mathcal{O}_K^\times)$, find a vector $\mathrm{Log}(u) \in \Lambda$ close to $\mathrm{Log}(g)$;
4. Output $g' := g/u$.

What about non-principal ideals or other number fields? The problem then reduces to decoding a single "Log-S-unit" lattice.

Module lattices

Definition

A **module lattice** of rank t is a pair (M, g) where $g \in \mathrm{GL}_t(K \otimes \mathbb{R})$ and $M \subseteq K^t$ is a (full-rank) finitely generated $\mathcal{O}_K$-module.

- Widely used in crypto since 2015.
- No magic improvement towards solving SVP.

Ideal lattices are rank-1 module lattices.

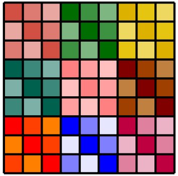


Figure: Structured lattice basis

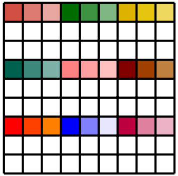


Figure: Storage gain!

Which number field(s) should we pick?

- Number field $K \cong \mathbb{Q}[X]/(f(X))$ for some irreducible $f(X)$.
- Elements are represented as vectors of coefficients.
- We want coefficients of products of polynomials mod f to stay bounded. This is best achieved for $X^n \pm 1$.
- Conclusion: we end up using cyclotomic polynomials $X^{2^k} + 1$ and their associated cyclotomic fields.

> In standardised crypto: rank $2, 3, 4$ modules.

NTRU: In between module and symplectic lattices

In 1996, Hoffstein, Pipher and Silverman introduce the NTRU cryptosystem over a polynomial ring $\mathbb{Z}[X]/(X^n - 1)$.

- More generally, NTRU lattices are rank-2 $\mathcal{O}_K$-module lattices with basis $\begin{pmatrix} 1 & h \\ 0 & q \end{pmatrix}$, with an *unusually dense* rank-1 submodule ($q \in \mathbb{Z}_{>1}$ and $h \in \mathcal{O}_K$).

For now,

Ideal lattice SVP $\leq$ NTRU $\leq$ Rank-2 module lattice SVP

- NTRU is inherantly a *symplectic* lattice, which makes it easier to reduce.
- NTRU lattice reduction is still very much open.

Gaussian heuristic and average behaviour

Heuristic point counting

How many lattice points does my convex measurable set X contain?

$$\#(\Lambda \cap X) \approx \frac{\mathrm{vol}(X)}{\mathrm{covol}(\Lambda)}.$$

- Leads to statements like

$$\lambda_1(\Lambda) \approx \frac{\mathrm{covol}(\Lambda)^{1/n}}{\mathrm{vol}(B_2(1))^{1/n}}.$$

- True on average (Siegel/Rogers/...).
- But not always true...

Interesting questions:

- Do we have better point-counting techniques in *special* lattices?
- Is the behaviour of lattice functions fundamentally different on spaces of module/ideal lattices compared to random lattices in general?
- Can we leverage potential differences to speed up LLL-like algorithms on such lattices?

Nicer arguments for security: WC to AC reduction for ideal lattices

Worst-case to Average-case reduction: "If I can solve SVP for a random ideal lattice, then I can solve SVP for any ideal lattice".

Before anything else:

- What is a random ideal lattice?
- We fix the covolume.
- We remove isometric lattices.

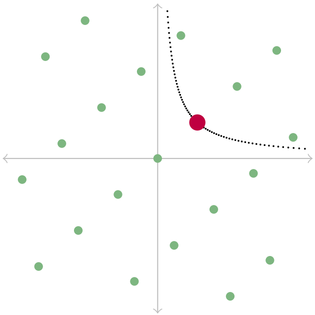


Figure: $K = \mathbb{Q}(\sqrt{2})$ (PID)

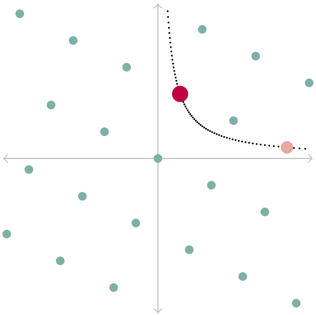


Figure: $K = \mathbb{Q}(\sqrt{2})$ (PID)

WC to AC reduction for ideal lattices [dBDPW20]

In fact we have the short exact sequence

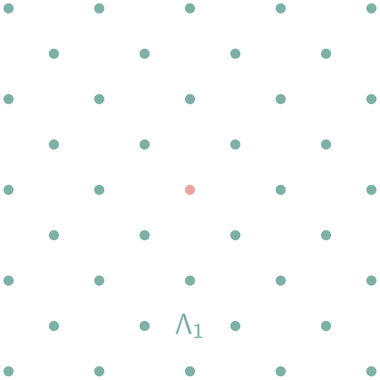
$$0 \to \mathrm{Log}(K_{\mathbb{R}})^0 / \mathrm{Log}(\mathcal{O}_K^\times) \to \underbrace{\text{Ideal Lattice Classes}_K}_{\textit{Arakelov class group } \mathrm{Pic}_K^0} \to \mathrm{Cl}_K \to 0.$$

From there:

- We have enough compactness to define *random*.
- We can define a random walk whose steps preserve the easiness of "SVP finding".
- Using Fourier analysis on $\widehat{\mathrm{Pic}_K^0}$, one can show that the walk reaches the uniform distribution fast enough.

<u>Worst-case to Average-case reduction:</u> "If I can solve SVP for a random ideal lattice, then I can solve SVP for any ideal lattice".

New problems in lattice crypto [DvW22]



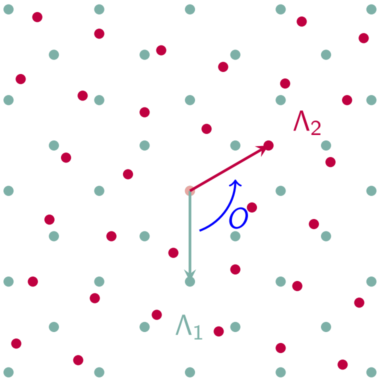
Lattice Isomorphism Problem (search)

Given two lattices $\Lambda_1, \Lambda_2 \subset \mathbb{R}^n$ such that there exists $O \in \mathcal{O}_n(\mathbb{R})$ for which $\Lambda_1 = O \cdot \Lambda_2$, recover an equivalent O.

Lattice Isomorphism Problem (decision)

Given two lattices $\Lambda_1, \Lambda_2 \subseteq \mathbb{R}^n$, decide whether $\Lambda_1 \cong \Lambda_2$ or not.

New problems in lattice crypto



$\Lambda_2 = O \cdot \Lambda_1$

Lattice Isomorphism Problem (search)

Given two lattices $\Lambda_1, \Lambda_2 \subset \mathbb{R}^n$ such that there exists $O \in \mathcal{O}_n(\mathbb{R})$ for which $\Lambda_1 = O \cdot \Lambda_2$, recover an equivalent O.

Lattice Isomorphism Problem (decision)

Given two lattices $\Lambda_1, \Lambda_2 \subseteq \mathbb{R}^n$, decide whether $\Lambda_1 \cong \Lambda_2$ or not.

How to solve Lattice Isomorphism?

Strategy for Search-LIP:

- Use lattice reduction to get a set of short vectors.
- Recover the isometry from the vector set.

The best approach is exponential in runtime and memory.

(Partial) Strategy for Distinguish-LIP:

- Find efficiently computable invariants $\mathrm{inv}(\cdot)$ that are as *fine* as possible.
- If $\mathrm{inv}(\Lambda_1) \neq \mathrm{inv}(\Lambda_2)$, then we can immediately conclude.

- We now restrict to *integral lattices*, or equivalently Gram matrices with all integer entries.

Some Invariants

- Rank: $n = \dim_{\mathbb{R}}(\mathrm{span}(\Lambda))$
- Covolume: $\mathrm{vol}(\mathbb{R}^n/\Lambda)$
- Gcd: $\gcd\{\langle \mathbf{x}, \mathbf{y} \rangle : \mathbf{x}, \mathbf{y} \in \Lambda\}$
- Equivalence over $\mathcal{R}$: does there exist $\mathbf{U} \in GL_n(\mathcal{R})$ such that $\mathbf{U}^T \mathbf{G}_1 \mathbf{U} = \mathbf{G}_2$?

Genus

The **genus** $\mathrm{gen}(\Lambda)$ is the set of lattices equivalent to Λ over $\mathbb{R}$ and all $\mathbb{Z}_p$ for prime p.

- A genus class is compatible with the Siegel Haar measure.

Interesting questions:

- Is the genus the best (computable) invariant?
- Can we have Worst-case to Average-case reductions inside a genus?
- How does this translate to the (module) structured variant of LIP?

Recap

In this overview talk we have seen...

- Special lattices from crypto:
  - Ideal lattices
  - Module lattices
  - NTRU lattices
- Some lattice problems:
  - Lattice reduction
  - SVP, CVP
  - Lattice Isomorphism
- A lot of structure from active number theory topics, sometimes hundreds of years old.

> ✓ Lattice crypto is only 10-30 years old.
>
> ✓ Very few researchers understand both worlds in depth yet those lattices are already being used by many.
>
> ✓ I hope this encourages work on better understanding of those special lattices, their average behaviour, and how to reduce them.

Thank you!