Recovering Short Generators of Principal Ideals in Cyclotomic Rings

Ronald Cramer, Léo Ducas, Chris Peikert, Oded Regev

9 July 2015
Simons Institute Workshop on Math of Modern Crypto

Short Generators of Ideals in Cryptography

A few recent lattice-related cryptoschemes [SV10, GGH13, LSS14, CGS14] share this KeyGen:

- sk Choose a "*short*" g in some ring R (e.g., $R = \mathbb{Z}[X]/(X^n + 1)$)
- pk Output a "*bad*" $\mathbb{Z}$-basis $\mathbf{B}$ (e.g., the HNF) of the ideal gR

Short Generators of Ideals in Cryptography

A few recent lattice-related cryptoschemes [SV10, GGH13, LSS14, CGS14] share this KeyGen:

- sk Choose a "*short*" g in some ring R (e.g., $R = \mathbb{Z}[X]/(X^n + 1)$)
- pk Output a "*bad*" $\mathbb{Z}$-basis $\mathbf{B}$ (e.g., the HNF) of the ideal gR

Key recovery in two steps:

Short Generators of Ideals in Cryptography

A few recent lattice-related cryptoschemes [SV10, GGH13, LSS14, CGS14] share this KeyGen:

- sk Choose a "*short*" g in some ring R (e.g., $R = \mathbb{Z}[X]/(X^n + 1)$)
- pk Output a "*bad*" $\mathbb{Z}$-basis $\mathbf{B}$ (e.g., the HNF) of the ideal gR

Key recovery in two steps:

1. Principal Ideal Problem (**PIP**):
   - ⋆ Given a $\mathbb{Z}$-basis $\mathbf{B}$ of a principal ideal $\mathcal{I}$, recover *some* generator h (i.e., $\mathcal{I} = hR$)

Short Generators of Ideals in Cryptography

A few recent lattice-related cryptoschemes [SV10, GGH13, LSS14, CGS14] share this KeyGen:

- sk Choose a "*short*" g in some ring R (e.g., $R = \mathbb{Z}[X]/(X^n + 1)$)
- pk Output a "*bad*" $\mathbb{Z}$-basis $\mathbf{B}$ (e.g., the HNF) of the ideal gR

Key recovery in two steps:

1. Principal Ideal Problem (**PIP**):
   - ⋆ Given a $\mathbb{Z}$-basis $\mathbf{B}$ of a principal ideal $\mathcal{I}$, recover *some* generator h (i.e., $\mathcal{I} = hR$)
2. Short Generator Problem (**SGP**):
   - ⋆ Given an *arbitrary* generator h of $\mathcal{I}$, recover the *short* generator g (up to trivial equivalences)

Short Generators of Ideals in Cryptography

A few recent lattice-related cryptoschemes [SV10, GGH13, LSS14, CGS14] share this KeyGen:

- sk Choose a "*short*" g in some ring R (e.g., $R = \mathbb{Z}[X]/(X^n + 1)$)
- pk Output a "*bad*" $\mathbb{Z}$-basis $\mathbf{B}$ (e.g., the HNF) of the ideal gR

Key recovery in two steps:

1. Principal Ideal Problem (**PIP**):
   - Given a $\mathbb{Z}$-basis $\mathbf{B}$ of a principal ideal $\mathcal{I}$, recover *some* generator h (i.e., $\mathcal{I} = hR$)
2. Short Generator Problem (**SGP**):
   - Given an *arbitrary* generator h of $\mathcal{I}$, recover the *short* generator g (up to trivial equivalences)

Not obvious *a priori* that g is even uniquely defined. But any short enough element in $\mathcal{I}$ suffices to break system.

Cost of the Two Steps

1. Principal Ideal Problem (find some generator h)
   - ⋆ Subexponential $2^{\tilde{O}(n^{2/3})}$-time classical algorithm [BF14, Bia14].
   - ⋆ Major progress toward poly-time *quantum* algorithm [EHKS14, BS15, CGS14].

Cost of the Two Steps

1. Principal Ideal Problem (find some generator h)
   - ⋆ Subexponential $2^{\tilde{O}(n^{2/3})}$-time classical algorithm [BF14, Bia14].
   - ⋆ Major progress toward poly-time *quantum* algorithm [EHKS14, BS15, CGS14].

2. Short Generator Problem (find the short generator g)
   - ⋆ In general, essentially **CVP** on the *log-unit* lattice of ring . . .

Cost of the Two Steps

1. Principal Ideal Problem (find some generator h)
   - ⋆ Subexponential $2^{\tilde{O}(n^{2/3})}$-time classical algorithm [BF14, Bia14].
   - ⋆ Major progress toward poly-time *quantum* algorithm [EHKS14, BS15, CGS14].

2. Short Generator Problem (find the short generator g)
   - ⋆ In general, essentially **CVP** on the *log-unit* lattice of ring ...
   - ⋆ ...but is actually a **BDD** problem in the cryptographic setting.

Cost of the Two Steps

1. Principal Ideal Problem (find some generator h)
   - ⋆ Subexponential $2^{\tilde{O}(n^{2/3})}$-time classical algorithm [BF14, Bia14].
   - ⋆ Major progress toward poly-time *quantum* algorithm [EHKS14, BS15, CGS14].

2. Short Generator Problem (find the short generator g)
   - ⋆ In general, essentially **CVP** on the *log-unit* lattice of ring ...
   - ⋆ ... but is actually a **BDD** problem in the cryptographic setting.
   - !! Claimed to be *easy* in power-of-2 cyclotomics [CGS14], and experimentally confirmed for relevant dimensions [She14, Sch15].

Cost of the Two Steps

1. Principal Ideal Problem (find some generator h)
   - ⋆ Subexponential $2^{\tilde{O}(n^{2/3})}$-time classical algorithm [BF14, Bia14].
   - ⋆ Major progress toward poly-time *quantum* algorithm [EHKS14, BS15, CGS14].

2. Short Generator Problem (find the short generator g)
   - ⋆ In general, essentially **CVP** on the *log-unit* lattice of ring ...
   - ⋆ ... but is actually a **BDD** problem in the cryptographic setting.
   - !! Claimed to be *easy* in power-of-2 cyclotomics [CGS14], and experimentally confirmed for relevant dimensions [She14, Sch15].

     But no convincing explanation why it works.

Cost of the Two Steps

1. Principal Ideal Problem (find some generator h)
   - ⋆ Subexponential $2^{\tilde{O}(n^{2/3})}$-time classical algorithm [BF14, Bia14].
   - ⋆ Major progress toward poly-time *quantum* algorithm [EHKS14, BS15, CGS14].

2. Short Generator Problem (find the short generator g)
   - ⋆ In general, essentially **CVP** on the *log-unit* lattice of ring . . .
   - ⋆ . . . but is actually a **BDD** problem in the cryptographic setting.
   - !! Claimed to be *easy* in power-of-2 cyclotomics [CGS14], and experimentally confirmed for relevant dimensions [She14, Sch15].

     But no convincing explanation why it works.

This Work: Main Theorem

In cryptographic setting, SGP can be solved in *classical polynomial time*, for any prime-power cyclotomic number ring $R = \mathbb{Z}[\zeta_{p^k}]$.

What Does This Mean for Ring-Based Crypto?

✗ The referenced works are classically weakened, and quantumly broken*.

What Does This Mean for Ring-Based Crypto?

- ✗ The referenced works are classically weakened, and quantumly broken*.
- ✔ Most ring-based crypto is unaffected, because its security is lower-bounded by harder/more general problems:

$$\text{SG-PI-SVP} \leq \text{PI-SVP} \leq \text{I-SVP} \leq \text{R-SIS/LWE} \leq \text{crypto}$$

What Does This Mean for Ring-Based Crypto?

- ✗ The referenced works are classically weakened, and quantumly broken*.
- ✔ Most ring-based crypto is unaffected, because its security is lower-bounded by harder/more general problems:

$$\text{SG-PI-SVP} \leq \text{PI-SVP} \leq \text{I-SVP} \leq \text{R-SIS/LWE} \leq \text{crypto}$$

- Attack crucially relies on ideal having "exceptionally short" generator.
  - Such ideals are extremely rare: for almost all principal ideals, the shortest generator is *vastly longer* than the shortest vector.

What Does This Mean for Ring-Based Crypto?

- ✗ The referenced works are classically weakened, and quantumly broken*.
- ✔ Most ring-based crypto is unaffected, because its security is lower-bounded by harder/more general problems:

$$\text{SG-PI-SVP} \leq \text{PI-SVP} \leq \text{I-SVP} \leq \text{R-SIS/LWE} \leq \text{crypto}$$

- ▶ Attack crucially relies on ideal having "exceptionally short" generator.
  - ⋆ Such ideals are extremely rare: for almost all principal ideals, the shortest generator is *vastly longer* than the shortest vector.

---

1. Devising hard distributions of lattice problems is very tricky: exploitable structure abounds!
2. Worst-case hardness protects us from weak instances.

Agenda

1. Introduction
2. Log-Unit Lattice
3. Attack and Proof Outline

(Logarithmic) Embedding

Let $K \cong \mathbb{Q}[X]/f(X)$ be a number field of degree n and let $\sigma_i \colon K \mapsto \mathbb{C}$ be its n complex embeddings. The *canonical embedding* is

$$\begin{aligned} \sigma \colon K &\to \mathbb{C}^n \\ x &\mapsto (\sigma_1(x), \ldots, \sigma_n(x)). \end{aligned}$$

The *logarithmic embedding* is

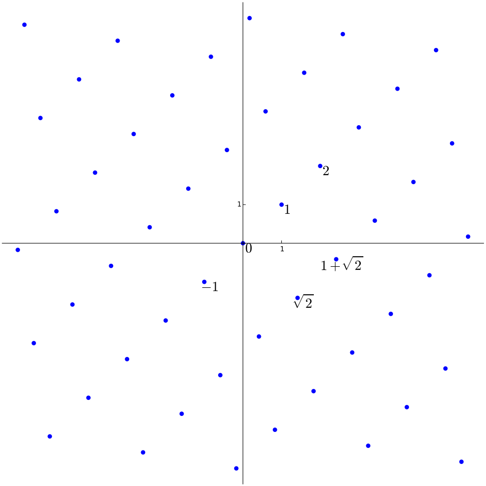
$$\begin{aligned} \mathrm{Log} \colon K \setminus \{0\} &\to \mathbb{R}^n \\ x &\mapsto (\log|\sigma_1(x)|, \ldots, \log|\sigma_n(x)|). \end{aligned}$$

It is a group homomorphism from $(K \setminus \{0\}, \times)$ to $(\mathbb{R}^n, +)$.

Example: Power-of-2 Cyclotomics

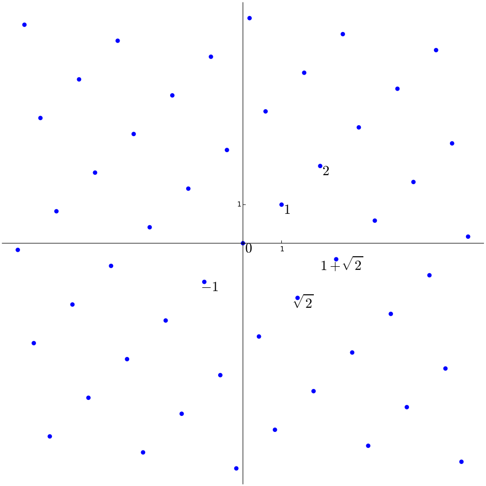
- $K \cong \mathbb{Q}[X]/(X^n + 1)$ for $n = 2^k$.
- $\sigma_i(X) = \omega^{2i-1}$, where $\omega = \exp(\pi\sqrt{-1}/n)$.
- $\mathrm{Log}(X^j) = \vec{0}$ and $\mathrm{Log}(1 - X) =$ [whiteboard]

Example: Embedding $\sigma(\mathbb{Z}[\sqrt{2}]) \subset \mathbb{R}^2$



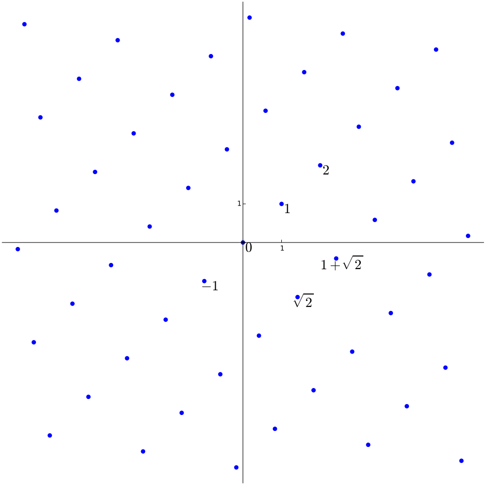
- x-axis: $\sigma_1(a+b\sqrt{2}) = a+b\sqrt{2}$
- y-axis: $\sigma_2(a+b\sqrt{2}) = a-b\sqrt{2}$

Example: Embedding $\sigma(\mathbb{Z}[\sqrt{2}]) \subset \mathbb{R}^2$



- x-axis: $\sigma_1(a + b\sqrt{2}) = a + b\sqrt{2}$
- y-axis: $\sigma_2(a + b\sqrt{2}) = a - b\sqrt{2}$
- component-wise multiplication

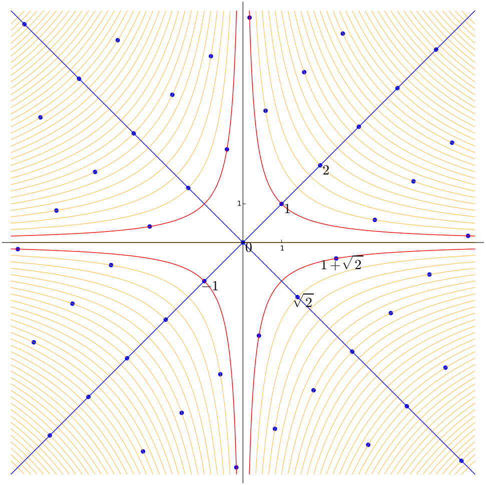
Example: Embedding $\sigma(\mathbb{Z}[\sqrt{2}]) \subset \mathbb{R}^2$



- x-axis: $\sigma_1(a+b\sqrt{2}) = a+b\sqrt{2}$
- y-axis: $\sigma_2(a+b\sqrt{2}) = a-b\sqrt{2}$
- component-wise multiplication

- Symmetries induced by
  - mult. by $-1, \sqrt{2}$
  - conjugation $\sqrt{2} \mapsto -\sqrt{2}$

Example: Embedding $\sigma(\mathbb{Z}[\sqrt{2}]) \subset \mathbb{R}^2$



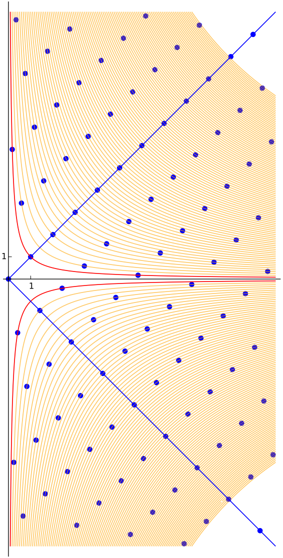
- x-axis: $\sigma_1(a + b\sqrt{2}) = a + b\sqrt{2}$
- y-axis: $\sigma_2(a + b\sqrt{2}) = a - b\sqrt{2}$
- component-wise multiplication

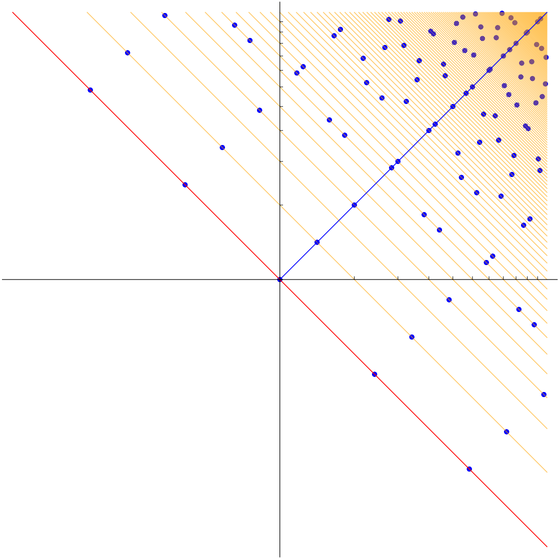
- Symmetries induced by
  - mult. by $-1, \sqrt{2}$
  - conjugation $\sqrt{2} \mapsto -\sqrt{2}$

- "Orthogonal" elements
- Units (algebraic norm 1)
- "Isonorms"

Example: Logarithmic Embedding $\operatorname{Log} \mathbb{Z}[\sqrt{2}]$

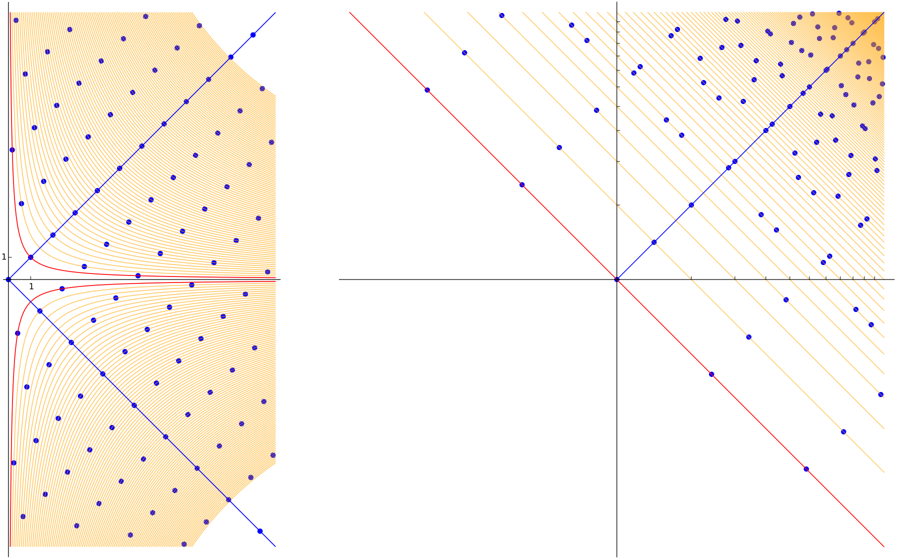
$\Lambda = \{\bullet\} \cap \diagdown$ is a rank-1 lattice of $\mathbb{R}^2$, orthogonal to $(1, 1)$





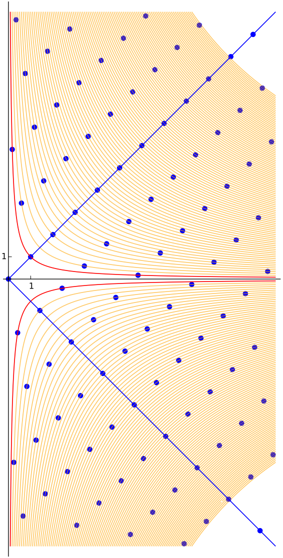
Example: Logarithmic Embedding $\operatorname{Log}\mathbb{Z}[\sqrt{2}]$

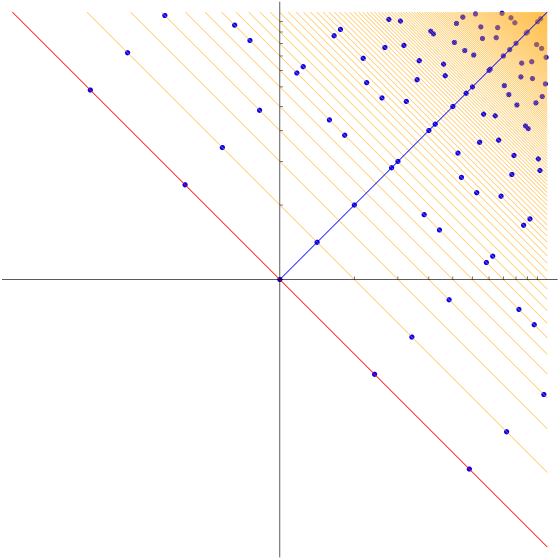
$\{\bullet\} \cap$ ╲ are finite # shifted copies of Λ



Example: Logarithmic Embedding $\operatorname{Log} \mathbb{Z}[\sqrt{2}]$

Some $\{\bullet\} \cap$ ╲ may be empty (e.g., no elements of norm 3)





Unit Group and the Log-Unit Lattice

Let $R^\times$ denote the mult. group of units of R, and $\Lambda = \operatorname{Log} R^\times \subset \mathbb{R}^n$.

Unit Group and the Log-Unit Lattice

Let $R^\times$ denote the mult. group of units of R, and $\Lambda = \operatorname{Log} R^\times \subset \mathbb{R}^n$.

Dirichlet's Unit Theorem:

- the kernel of Log is the cyclic group of roots of unity in R, and
- $\Lambda \subset \mathbb{R}^n$ is a lattice of rank $r + c - 1$, orthogonal to $\vec{1}$

  (where K has r real embeddings and $2c$ complex embeddings)

Unit Group and the Log-Unit Lattice

Let $R^\times$ denote the mult. group of units of R, and $\Lambda = \operatorname{Log} R^\times \subset \mathbb{R}^n$.

Dirichlet's Unit Theorem:

- the kernel of Log is the cyclic group of roots of unity in R, and
- $\Lambda \subset \mathbb{R}^n$ is a lattice of rank $r + c - 1$, orthogonal to $\vec{1}$

  (where K has r real embeddings and $2c$ complex embeddings)

Short Generators via CVP

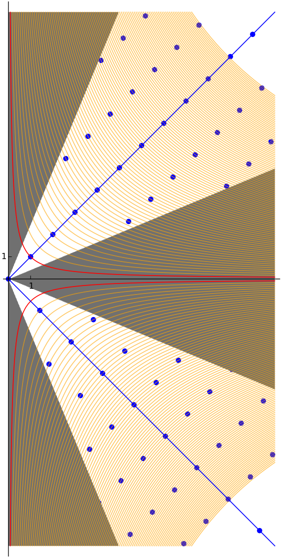
Elements $g, h \in R$ generate the same ideal if and only if $g = h \cdot u$ for some unit $u \in R^\times$, i.e.,

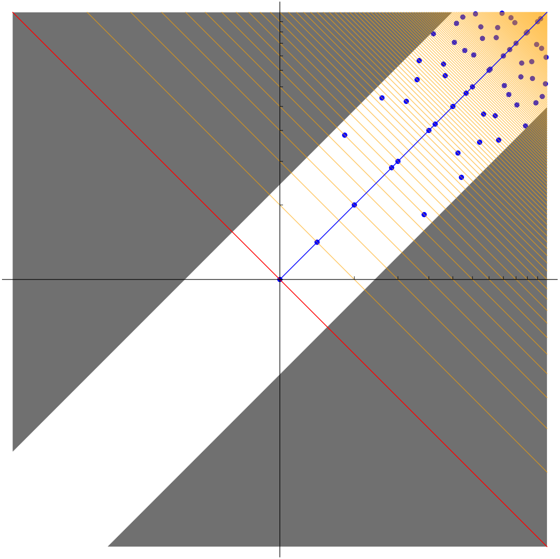
$$\operatorname{Log} g = \operatorname{Log} h + \operatorname{Log} u \in \operatorname{Log} h + \Lambda.$$

In particular, g is a "smallest" generator iff $\operatorname{Log} g$ is a "shortest" element of $\operatorname{Log} h + \Lambda$.

Decoding $\Lambda = \operatorname{Log} \mathbb{Z}[\sqrt{2}]^\times$

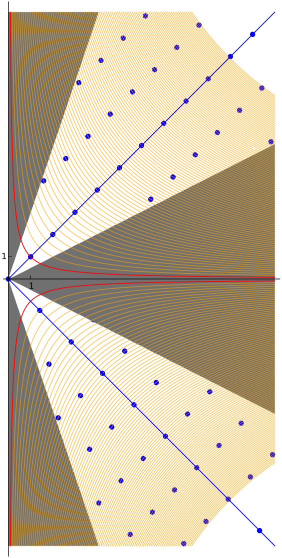
Decoding mod Λ into various fundamental domains.

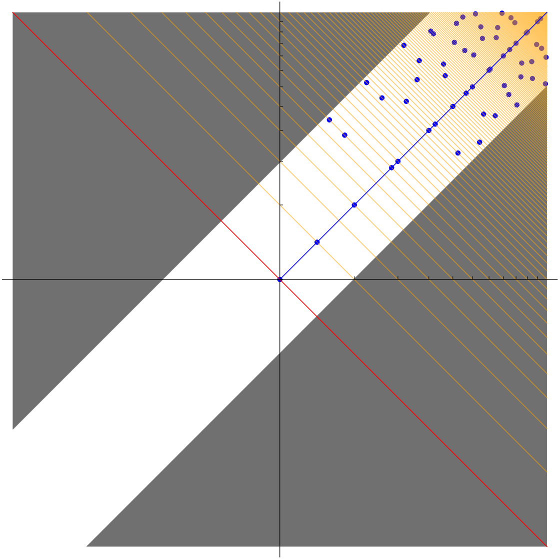




Decoding $\Lambda = \operatorname{Log} \mathbb{Z}[\sqrt{2}]^{\times}$

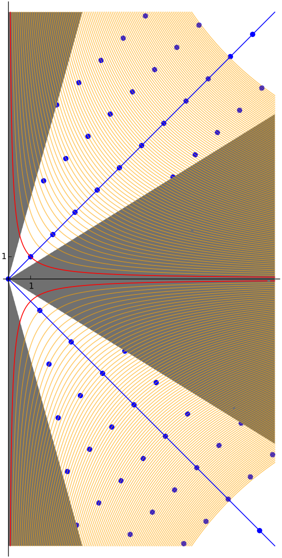
Decoding mod Λ into various fundamental domains.

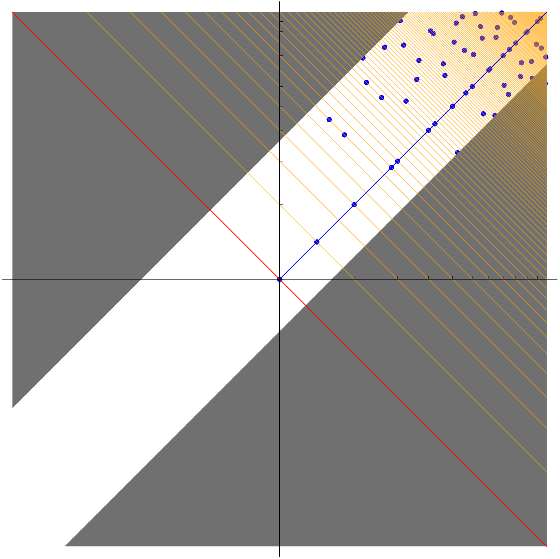




Decoding $\Lambda = \operatorname{Log} \mathbb{Z}[\sqrt{2}]^{\times}$

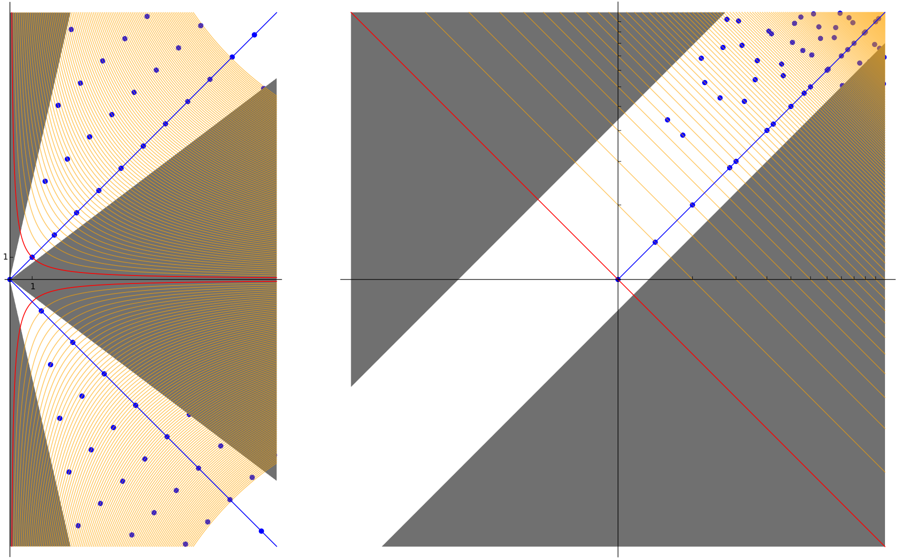
Decoding mod Λ into various fundamental domains.





Decoding $\Lambda = \operatorname{Log} \mathbb{Z}[\sqrt{2}]^\times$

Decoding mod Λ into various fundamental domains.



Round-Off Decoding

The simplest algorithm to solve CVP/BDD:

$\textsc{Round}(\mathbf{B}, \mathbf{t})$ for $\mathbf{B}$ a basis of Λ

- Return $\mathbf{B} \cdot \mathsf{frac}(\mathbf{B}^{-1} \cdot \mathbf{t})$.

Used as a decoding algorithm, its correctness is characterized by the error $\mathbf{e}$ and the *dual basis* $\mathbf{B}^\vee = \mathbf{B}^{-T}$.

Fact

Suppose $\mathbf{h} = \mathbf{u} + \mathbf{g}$ for some $\mathbf{u} \in \Lambda$. If $\langle \mathbf{b}_j^\vee, \mathbf{g} \rangle \in [-\frac{1}{2}, \frac{1}{2})$ for all j, then

$$\textsc{Round}(\mathbf{B}, \mathbf{h}) = \mathbf{g}.$$

Recovering the Short Generator: Proof Outline

1. Construct a basis $\mathbf{B}$ of the log-unit lattice $\Lambda = \operatorname{Log} R^{\times}$.
   - ⋆ For $K = \mathbb{Q}(\zeta_m)$, $m = p^k$, a canonical (almost[1]-)basis is given by

$$\mathbf{b}_j = \operatorname{Log} \frac{1-\zeta^j}{1-\zeta}, \quad 2 \le j < m/2,\ j \text{ coprime with } m.$$

[1] it only generates a sublattice of finite index h^+, which is conjectured to be small

Recovering the Short Generator: Proof Outline

1. Construct a basis $\mathbf{B}$ of the log-unit lattice $\Lambda = \operatorname{Log} R^{\times}$.
   - For $K = \mathbb{Q}(\zeta_m)$, $m = p^k$, a canonical (almost[1]-)basis is given by

$$\mathbf{b}_j = \operatorname{Log} \frac{1-\zeta^j}{1-\zeta}, \quad 2 \le j < m/2, \ j \text{ coprime with } m.$$

2. Prove that the basis $\mathbf{B}$ is "good," i.e., all $\|\mathbf{b}_j^\vee\|$ are small.

[1] it only generates a sublattice of finite index h^+, which is conjectured to be small

Recovering the Short Generator: Proof Outline

1. Construct a basis $\mathbf{B}$ of the log-unit lattice $\Lambda = \operatorname{Log} R^\times$.
   - ⋆ For $K = \mathbb{Q}(\zeta_m)$, $m = p^k$, a canonical (almost[1]-)basis is given by

$$\mathbf{b}_j = \operatorname{Log} \frac{1-\zeta^j}{1-\zeta}, \quad 2 \le j < m/2, \ j \text{ coprime with } m.$$

2. Prove that the basis $\mathbf{B}$ is "good," i.e., all $\|\mathbf{b}_j^\vee\|$ are small.
3. Prove that $\mathbf{g} = \operatorname{Log} g$ is sufficiently small when g generated as in cryptosystem, so that $\langle \mathbf{b}_j^\vee, \mathbf{g} \rangle \in [-\frac{1}{2}, \frac{1}{2})$.

[1] it only generates a sublattice of finite index h^+, which is conjectured to be small

Recovering the Short Generator: Proof Outline

1. Construct a basis $\mathbf{B}$ of the log-unit lattice $\Lambda = \operatorname{Log} R^\times$.
   - ★ For $K = \mathbb{Q}(\zeta_m)$, $m = p^k$, a canonical (almost[1]-)basis is given by

$$\mathbf{b}_j = \operatorname{Log} \frac{1 - \zeta^j}{1 - \zeta}, \quad 2 \le j < m/2, \ j \text{ coprime with } m.$$

2. Prove that the basis $\mathbf{B}$ is "good," i.e., all $\|\mathbf{b}_j^\vee\|$ are small.
3. Prove that $\mathbf{g} = \operatorname{Log} g$ is sufficiently small when g generated as in cryptosystem, so that $\langle \mathbf{b}_j^\vee, \mathbf{g} \rangle \in [-\frac{1}{2}, \frac{1}{2})$.

Technical Contributions

2. Show $\|\mathbf{b}_j^\vee\| = \tilde{O}(1/\sqrt{m})$ using Gauss sums and Dirichlet L-series.
3. Bound $\langle \mathbf{b}_j^\vee, \mathbf{g} \rangle$ using theory of subexponential random variables.

[1] it only generates a sublattice of finite index h^+, which is conjectured to be small

Open Problems

(Easy?) Extend to non-prime-power cyclotomics.

Open Problems

(Easy?) Extend to non-prime-power cyclotomics.

(Not hard?) Extend to "nice" non-cyclotomic families of number fields K.

- Enough to find a "good enough" basis of $\operatorname{Log} \mathcal{O}_K^\times$ (or a dense enough sublattice).

Open Problems

(Easy?) Extend to non-prime-power cyclotomics.

(Not hard?) Extend to "nice" non-cyclotomic families of number fields K.

- Enough to find a "good enough" basis of $\operatorname{Log} \mathcal{O}_K^\times$ (or a dense enough sublattice).

(Hard.) Asymptotically bound h^+ for cyclotomics.

Open Problems

(Easy?) Extend to non-prime-power cyclotomics.

(Not hard?) Extend to "nice" non-cyclotomic families of number fields K.

- Enough to find a "good enough" basis of $\operatorname{Log} \mathcal{O}_K^\times$ (or a dense enough sublattice).

(Hard.) Asymptotically bound h^+ for cyclotomics.

Thanks!

References I

J.-F. Biasse and C. Fieker.
Subexponential class group and unit group computation in large degree number fields.
LMS Journal of Computation and Mathematics, 17:385–403, 1 2014.

Jean-François Biasse.
Subexponential time relations in the class group of large degree number fields.
Adv. Math. Commun., 8(4):407–425, 2014.

J.-F. Biasse and F. Song.
A polynomial time quantum algorithm for computing class groups and solving the principal ideal problem in arbitrary degree number fields.
http://www.lix.polytechnique.fr/Labo/Jean-Francois.Biasse/, 2015.
In preparation.

Peter Campbell, Michael Groves, and Dan Shepherd.
Soliloquy: A cautionary tale.
ETSI 2nd Quantum-Safe Crypto Workshop, 2014.
Available at http://docbox.etsi.org/Workshop/2014/201410_CRYPTO/S07_Systems_and_Attacks/S07_Groves_Annex.pdf.

Kirsten Eisenträger, Sean Hallgren, Alexei Kitaev, and Fang Song.
A quantum algorithm for computing the unit group of an arbitrary degree number field.
In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, pages 293–302. ACM, 2014.

References II

Sanjam Garg, Craig Gentry, and Shai Halevi.
Candidate multilinear maps from ideal lattices.
In *EUROCRYPT*, pages 1–17, 2013.

Adeline Langlois, Damien Stehlé, and Ron Steinfeld.
Gghlite: More efficient multilinear maps from ideal lattices.
In *Advances in Cryptology–EUROCRYPT 2014*, pages 239–256. Springer, 2014.

John Schank.
LogCvp, Pari implementation of CVP in $\log \mathbb{Z}[\zeta_{2^n}]^*$.
https://github.com/jschanck-si/logcvp, 2015.

Dan Shepherd, December 2014.
Personal communication.

Nigel P. Smart and Frederik Vercauteren.
Fully homomorphic encryption with relatively small key and ciphertext sizes.
In *Public Key Cryptography*, pages 420–443, 2010.