Recovering Short Generators of Principal Ideals in Cyclotomic Rings

Ronald Cramer Léo Ducas
Chris Peikert Oded Regev

University of Leiden, The Netherlands

CWI, Amsterdam, The Netherlands

University of Michigan, USA

New-York University, USA

EUROCRYPT, May 2016, Vienna, Austria.

Principal ideals in cryptography

Let $\mathbb{K}$ be a numberfield (e.g. $= \mathbb{Q}(\zeta_m)$) and R its ring of integer ($R = \mathbb{Z}[\zeta_m]$).

A few cryptosystems, for example:

- Soliloquy [Campbell et al., 2014]
- FHE [Smart and Vercauteren, 2010]
- Graded encoding schemes [Garg et al., 2013, Langlois et al., 2014]

share this Key Generation procedure.

KeyGen

sk Choose a "short" $g \in R$ as a private key

pk Give a bad $\mathbb{Z}$-basis $\mathbf{B}$ of the ideal (g) as a public key (e.g. HNF).

Short generator recovery

Cryptanalysis in two steps (Key Recovery Attack)

1. Principal Ideal Problem (PIP)
   - Given a $\mathbb{Z}$-basis $\mathbf{B}$ of a principal ideal $\mathfrak{I}$,
   - Recover some generator h (i.e. $\mathfrak{I} = (h)$)

Short generator recovery

Cryptanalysis in two steps (Key Recovery Attack)

1. Principal Ideal Problem (PIP)
   - Given a $\mathbb{Z}$-basis $\mathbf{B}$ of a principal ideal $\mathfrak{I}$,
   - Recover some generator h (i.e. $\mathfrak{I} = (h)$)
2. Short Generator Problem
   - Given an arbitrary generator $h \in R$ of $\mathfrak{I}$
   - Recover g (or some g' equivalently short)

Cost of those two steps

1. Principal Ideal Problem (**PIP**)
   - sub-exponential time ($2^{\tilde{O}(n^{2/3})}$) classical algorithm [Biasse and Fieker, 2014, Biasse, 2014].
   - quantum polynomial time algorithm [Eisenträger et al., 2014, Campbell et al., 2014, Biasse and Song, 2015].
2. Short Generator Problem
   - equivalent to the **CVP** in the log-unit lattice
   - becomes a **BDD** problem in the crypto cases.
   - claimed to be easy [Campbell et al., 2014] for the m^{th}-cyclotomic ring when $m = 2^k$
   - confirmed by experiments [Schank, 2015]

This Work

We focus on step 2, and prove it can be solved in classical polynomial time for the aforementioned cryptanalytic instances, when the ring R is the ring of integers of the cyclotomic number field $K = \mathbb{Q}(\zeta_m)$ for $m = p^k$.

The Problem

Short generator recovery

Given $h \in R$, find a small generator g of the ideal (h).

Note that $g \in (h)$ is a generator iff $g = u \cdot h$ for some unit $u \in \mathbb{R}^\times$.
We need to explore the (multiplicative) unit group $R^\times$.

The Problem

Short generator recovery

Given $h \in R$, find a small generator g of the ideal (h).

Note that $g \in (h)$ is a generator iff $g = u \cdot h$ for some unit $u \in \mathbb{R}^\times$.
We need to explore the (multiplicative) unit group $R^\times$.

Translation an to additive problem

Take logarithms:

$$\mathrm{Log} : g \mapsto (\log|\sigma_1(g)|, \ldots, \log|\sigma_n(g)|) \in \mathbb{R}^n$$

where the σ_i's are the canonical embeddings $\mathbb{K} \to \mathbb{C}$.

The Unit Group and the log-unit lattice

Let $R^\times$ denotes the multiplicative group of units of R. Let

$$\Lambda = \operatorname{Log} R^\times.$$

Theorem (Dirichlet unit Theorem)

$\Lambda \subset \mathbb{R}^n$ *is a lattice (of a given rank).*

The Unit Group and the log-unit lattice

Let $R^\times$ denotes the multiplicative group of units of R. Let

$$\Lambda = \operatorname{Log} R^\times.$$

Theorem (Dirichlet unit Theorem)

$\Lambda \subset \mathbb{R}^n$ is a lattice (of a given rank).

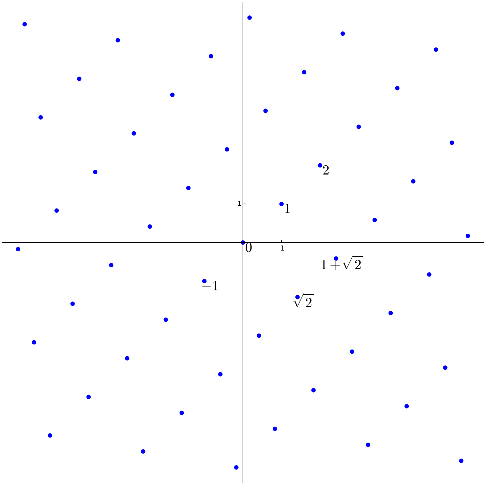
Reduction to a Close Vector Problem

Elements g is a generator of (h) if and only if

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

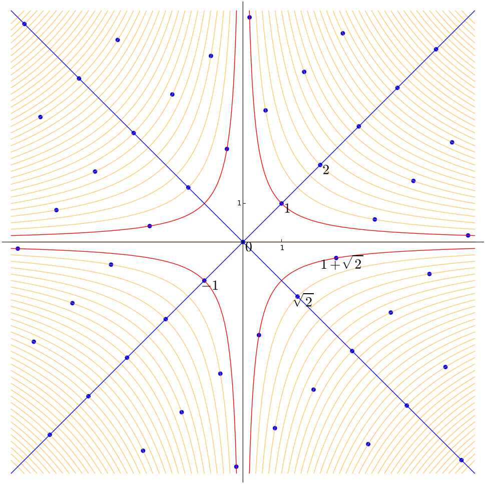
Moreover the map Log preserves some geometric information:
g is the "smallest" generator iff $\operatorname{Log} g$ is the "smallest" in $\operatorname{Log} h + \Lambda$.

Example: Embedding $\mathbb{Z}[\sqrt{2}] \hookrightarrow \mathbb{R}^2$



- 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 additions and multiplications

Example: Embedding $\mathbb{Z}[\sqrt{2}] \hookrightarrow \mathbb{R}^2$

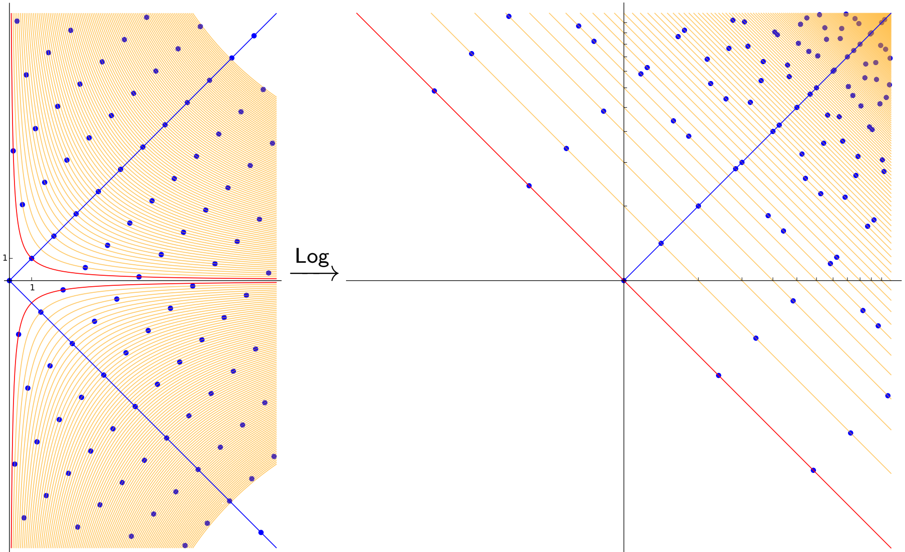


- x-axis: $\sigma_1(a + b\sqrt{2}) = a + b\sqrt{2}$
- y-axis: $\sigma_2(a + b\sqrt{2}) = a - b\sqrt{2}$
- component-wise additions and multiplications

Blue: "Orthogonal" elements
Red: Units (algebraic norm 1)
Orange: "Isonorms" curves

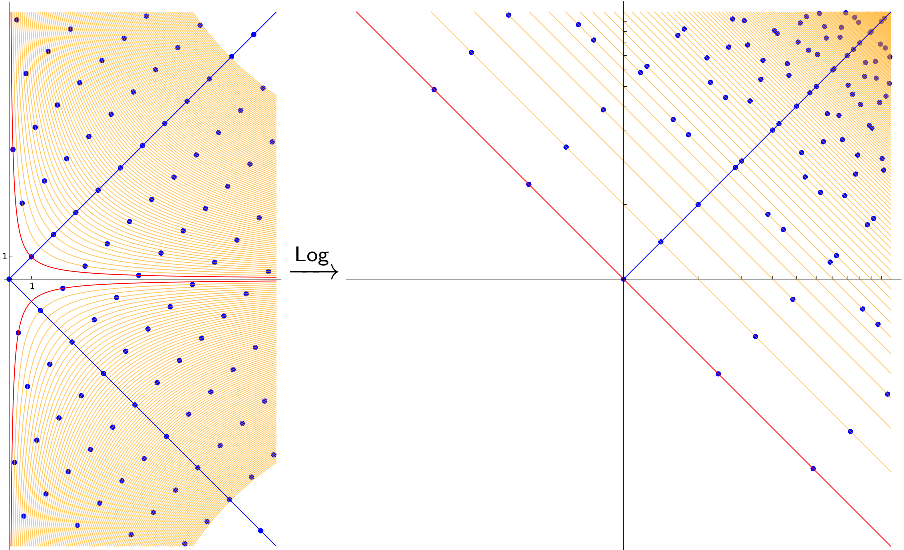
Example: Logarithmic Embedding Log $\mathbb{Z}[\sqrt{2}]$

$(\{\bullet\}, +)$ is a sub-monoid of $\mathbb{R}^2$



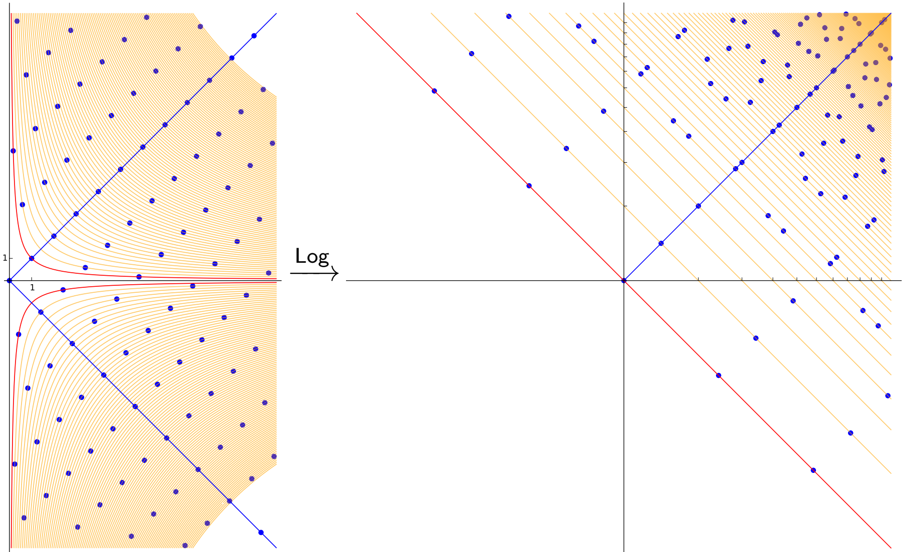
Example: Logarithmic Embedding $\operatorname{Log} \mathbb{Z}[\sqrt{2}]$

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



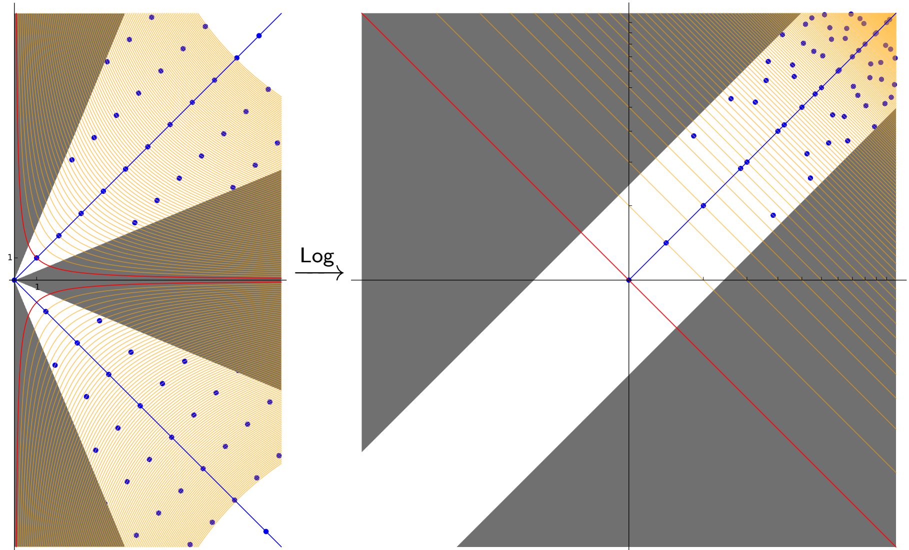
Example: Logarithmic Embedding $\mathrm{Log}\,\mathbb{Z}[\sqrt{2}]$

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



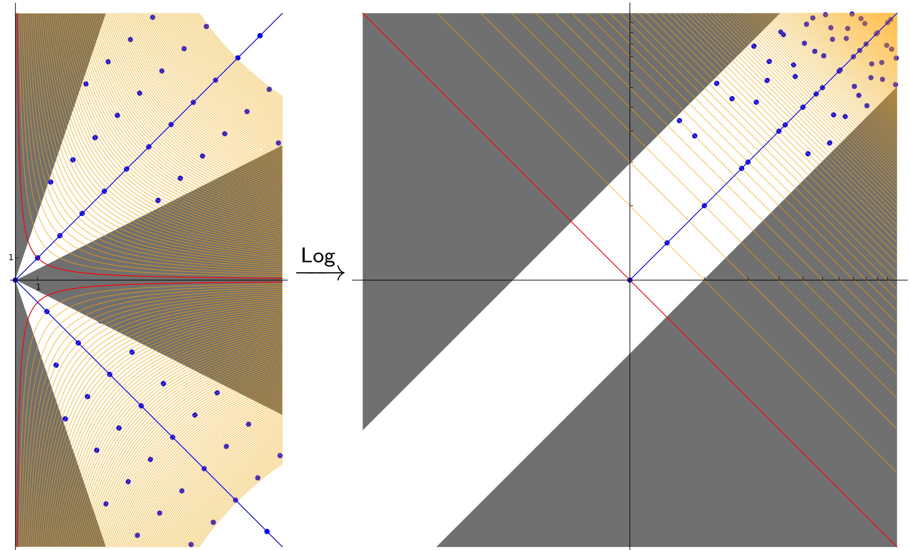
Reduction modulo $\Lambda = \operatorname{Log} \mathbb{Z}[\sqrt{2}]^\times$

The reduction $\bmod \Lambda$ for various fundamental domains.



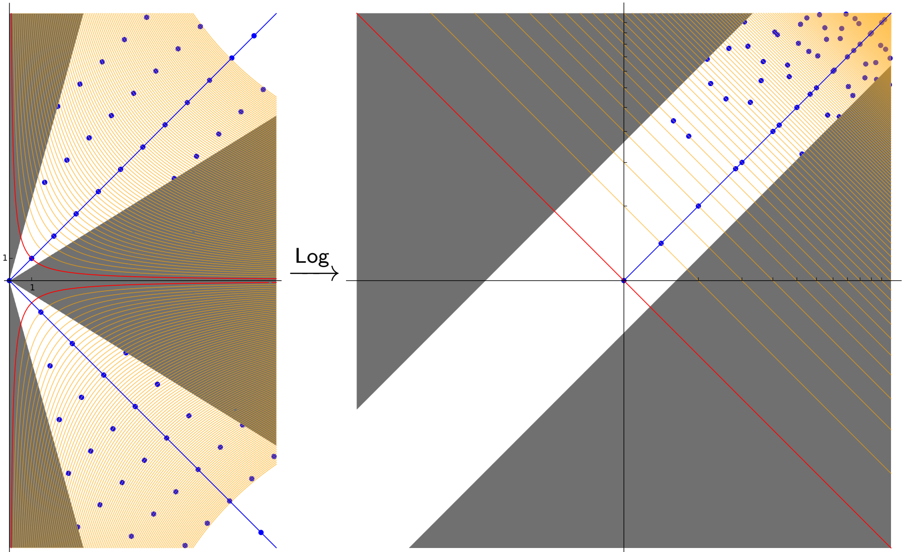
Reduction modulo $\Lambda = \operatorname{Log} \mathbb{Z}[\sqrt{2}]^{\times}$

The reduction $\bmod \Lambda$ for various fundamental domains.



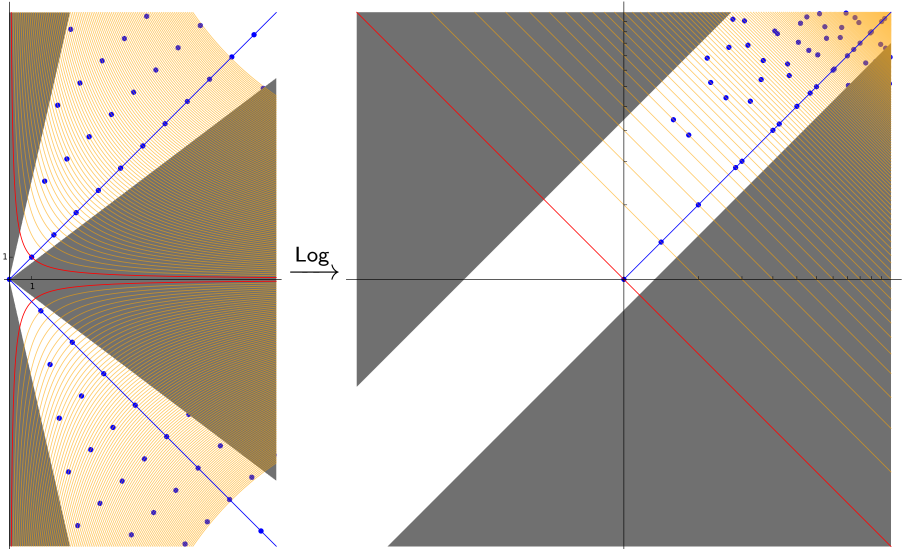
Reduction modulo $\Lambda = \operatorname{Log} \mathbb{Z}[\sqrt{2}]^{\times}$

The reduction modΛ for various fundamental domains.



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

The reduction $\bmod \Lambda$ for various fundamental domains.



Round-Off Decoding

We also need the fundamental domain to have an efficient reduction algorithm. The simplest one follows:

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

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

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 [Lenstra, 1982, Babai, 1986]

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

$$\textsc{Round}(\mathbf{B}, \mathbf{t}) = \mathbf{v}.$$

Recovering Short Generator: Proof Plan

Folklore strategy [Bernstein, 2014, Campbell et al., 2014] to recover a short generator g

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

$$\mathbf{b}_j = \operatorname{Log} \frac{1-\zeta^j}{1-\zeta}, \quad j \in \{2, \dots, m/2\}, j \text{ co-prime with } m$$

2. Prove that the basis is "good", that is $\|\mathbf{b}_j^{\vee}\|$ are all small
3. Prove that $\mathbf{e} = \operatorname{Log} g$ is small enough

[1] it only spans a super-lattice of finite index h^{+} which is conjectured to be small

Recovering Short Generator: Proof Plan

Folklore strategy [Bernstein, 2014, Campbell et al., 2014] to recover a short generator g

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

$$\mathbf{b}_j = \operatorname{Log} \frac{1-\zeta^j}{1-\zeta}, \quad j \in \{2, \ldots, m/2\}, j \text{ co-prime with } m$$

2. Prove that the basis is "good", that is $\|\mathbf{b}_j^\vee\|$ are all small
3. Prove that $\mathbf{e} = \operatorname{Log} g$ is small enough

Technical contributions

2. Estimate $\|\mathbf{b}_j^\vee\|$ precisely using analytic tools [Washington, 1997, Landau, 1927]
3. Bound $\mathbf{e}$ using theory of sub-exponential random variables [Vershynin, 2012]

[1] it only spans a super-lattice of finite index h^+ which is conjectured to be small

Geometric statement from Analytic Number Theory

Theorem ([Landau, 1927])

If χ is a non-quadratic Dirichlet character of conductor f.

$$|L(1,\chi)| \geq 1/O(\log f).$$

Geometric statement from Analytic Number Theory

Theorem ([Landau, 1927])

If χ is a non-quadratic Dirichlet character of conductor f.

$$|L(1,\chi)| \geq 1/O(\log f).$$

Theorem (Cramer, D. , Peikert, Regev)

Let $m = p^k$, and $\mathbf{B} = (\mathrm{Log}(b_j))_{j \in G \setminus \{1\}}$ be the canonical basis of $\mathrm{Log}\, C$. Then, for all j

$$\left\| \mathbf{b}_j^\vee \right\|^2 \leq O\left(m^{-1} \cdot \log^3 m\right).$$

Interpretation

The log-unit lattice $\mathrm{Log}\, R^\times$ admits a (known, efficiently computable) basis that is **almost orthogonal**: **BDD** is easy !

No Crypto from Principal Ideals

We formalized, generalized and proved a claim of [Campbell et al., 2014]:

Corollary [Cramer, D. , Peikert, Regev] (simplified)

If g follows a reasonable distribution, then given any generator h of (g), one may recover g in poly-time with probability $1 - o(1)$.

Combined with a poly-time quantum algorithm[2] of [Biasse and Song, 2015], this breaks several cryptographic proposal.

[2] Alt. a classical sub-exponential algorithm [Biasse and Fieker, 2014, Biasse, 2014].

What about the worst case ?

Theorem [Cramer, D. , Peikert, Regev]

Given a generator h of any principal ideal (h), one may find in poly-time a generator g of (h) of length

$$\|g\| \leq N(h)^{1/n} \cdot 2^{\tilde{O}(\sqrt{n})}.$$

What about the worst case ?

Theorem [Cramer, D. , Peikert, Regev]

Given a generator h of any principal ideal (h), one may find in poly-time a generator g of (h) of length

$$\|g\| \leq N(h)^{1/n} \cdot 2^{\tilde{O}(\sqrt{n})}.$$

We also show that this is nearly optimal:

Theorem [Cramer, D. , Peikert, Regev]

In some principal ideals $\mathfrak{I}$, the shortest generator has length at least

$$\|g\| \geq N(\mathfrak{I})^{1/n} \cdot 2^{\Omega(\sqrt{m}/\log m)}.$$

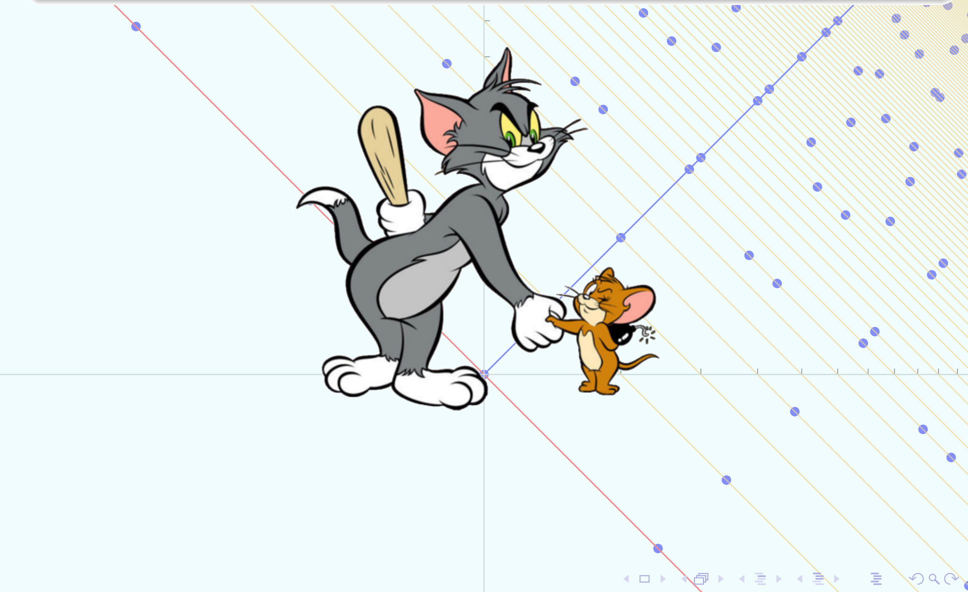
Open questions

1. Are there other classes of rings whose log-unit lattice can be studied ?
   - For cyclotomics, several happy event for the proof to go through.
   - Other rings are harder to study. Security by ignorance ?

2. Does this result has a bearing on (worst-case) non-principal ideals ?
   - Possibly: class group Caley graphs, Stickleberger's Ideal . . .
   - This approach seems limited to large approx. factors $2^{\tilde{O}(\sqrt{n})}$.

3. And on Ring-LWE ?
   - Seems much harder than 2 .
   - Would still be limited to large approx. factors $2^{\tilde{O}(\sqrt{n})}$.

Questions ?



Questions ?

Thanks for your attention !

References I

Babai, L. (1986).
On Lovász' lattice reduction and the nearest lattice point problem.
Combinatorica, 6(1):1–13.
Preliminary version in STACS 1985.

Bernstein, D. (2014).
A subfield-logarithm attack against ideal lattices.
`http://blog.cr.yp.to/20140213-ideal.html`.

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

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

Biasse, J.-F. and Song, F. (2015).
On the quantum attacks against schemes relying on the hardness of finding a short generator of an ideal in q (ζpn).

References II

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

Eisenträger, K., Hallgren, S., Kitaev, A., and Song, F. (2014).
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.

Garg, S., Gentry, C., and Halevi, S. (2013).
Candidate multilinear maps from ideal lattices.
In *EUROCRYPT*, pages 1–17.

Landau, E. (1927).
Über Dirichletsche Reihen mit komplexen Charakteren.
Journal für die reine und angewandte Mathematik, 157:26–32.

Langlois, A., Stehlé, D., and Steinfeld, R. (2014).
Gghlite: More efficient multilinear maps from ideal lattices.
In *Advances in Cryptology–EUROCRYPT 2014*, pages 239–256. Springer.

References III

Lenstra, A. K. (1982).
Lattices and factorization of polynomials over algebraic number fields.
In *Computer Algebra*, pages 32–39. Springer.

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

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

Vershynin, R. (2012).
Compressed Sensing, Theory and Applications, chapter 5, pages 210–268.
Cambridge University Press.
Available at
http://www-personal.umich.edu/~romanv/papers/non-asymptotic-rmt-plain.pdf.

Washington, L. (1997).
Introduction to Cyclotomic Fields.
Graduate Texts in Mathematics. Springer New York.