Recovering Short Generators of Principal Ideals in Cyclotomic Rings

Léo Ducas

CWI,
Amsterdam, The Netherlands

Joint work with
Ronald Cramer   Chris Peikert   Oded Regev

Conference on Mathematics of Cryptography, August 2015, UC Irvine[1]

[1] Slides revised on Sept. 7, 2015.

Recovering Short Generators for Cryptanalysis

A few cryptosystems (Fully Homomorphic Encryption [Smart and Vercauteren, 2010] and Multilinear Maps [Garg et al., 2013, Langlois et al., 2014]) share this KEYGEN:

- sk Choose a *short* g in some ring 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).

Cryptanalysis in two steps (Key Recovery Attack)

Recovering Short Generators for Cryptanalysis

A few cryptosystems (Fully Homomorphic Encryption [Smart and Vercauteren, 2010] and Multilinear Maps [Garg et al., 2013, Langlois et al., 2014]) share this KeyGen:

- sk Choose a *short* g in some ring 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).

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. $\mathfrak{I} = (h)$)

Recovering Short Generators for Cryptanalysis

A few cryptosystems (Fully Homomorphic Encryption [Smart and Vercauteren, 2010] and Multilinear Maps [Garg et al., 2013, Langlois et al., 2014]) share this $\textsc{KeyGen}$:

- sk Choose a *short* g in some ring 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).

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].
   - progress toward quantum polynomial time algorithm [Eisenträger et al., 2014, Biasse and Song, 2015b, Campbell et al., 2014, Biasse and Song, 2015a].
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] in the cyclotomic case $m = 2^k$
     - confirmed by experiments [Schank, 2015]

This Work [Cramer et al., 2015]

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 $m = p^k$.

Overview

The Logarithmic Embedding

Let K be a number field of degree n, $\sigma_1 \dots \sigma_n : K \mapsto \mathbb{C}$ be its embeddings, and let R be its ring of integers. The logarithmic Embedding is defined as

$$\begin{aligned} \mathrm{Log} : K &\to \mathbb{R}^n \\ x &\mapsto (\log|\sigma_1(x)|, \dots, \log|\sigma_n(x)|) \end{aligned}$$

It induces

- a group morphism from $(K \setminus \{0\}, \cdot)$ to $(\mathbb{R}^n, +)$
- a monoid morphism from $(R \setminus \{0\}, \cdot)$ to $(\mathbb{R}^n, +)$

The Unit Group

Let $R^\times$ denotes the multiplicative group of units of R.
Let $\Lambda = \operatorname{Log} R^\times$. By Dirichlet Unit Theorem

- the kernel of Log is the cyclic group T of roots of unity of R
- $\Lambda \subset \mathbb{R}^n$ is an lattice of rank $r + c - 1$

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

The Unit Group

Let $R^\times$ denotes the multiplicative group of units of R.
Let $\Lambda = \operatorname{Log} R^\times$. By Dirichlet Unit Theorem

- the kernel of Log is the cyclic group T of roots of unity of R
- $\Lambda \subset \mathbb{R}^n$ is an lattice of rank $r + c - 1$

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

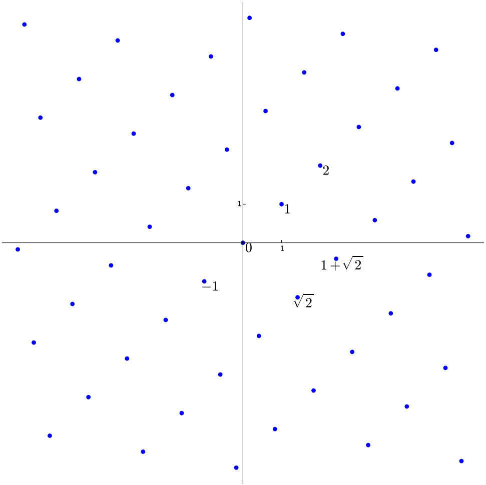
Reduction to CVP

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

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

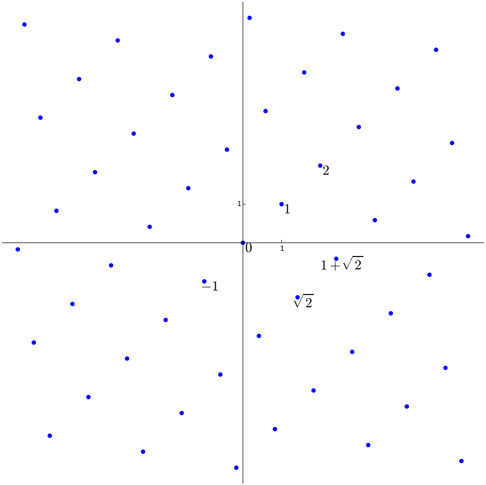
and g is the "smallest" generator iff $\operatorname{Log} u \in \Lambda$ is a vector "closest" to $\operatorname{Log} h$.

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



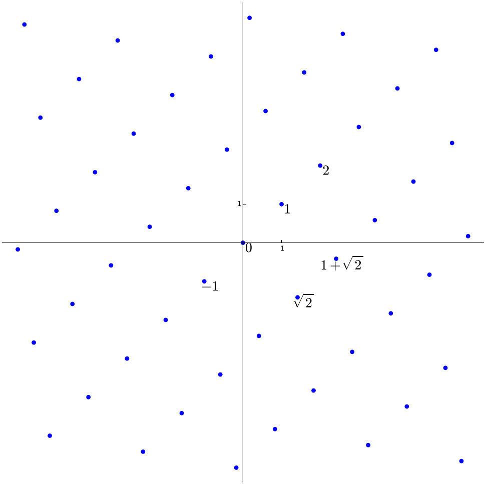
- x-axis: $a + b\sqrt{2} \mapsto a + b\sqrt{2}$
- y-axis: $a + b\sqrt{2} \mapsto a - b\sqrt{2}$

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



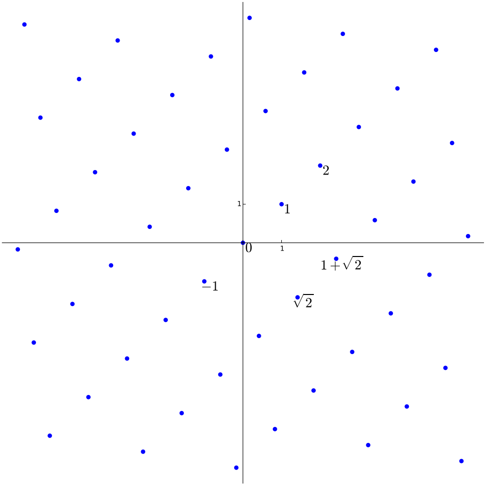
- x-axis: $a + b\sqrt{2} \mapsto a + b\sqrt{2}$
- y-axis: $a + b\sqrt{2} \mapsto a - b\sqrt{2}$

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



- x-axis: $a + b\sqrt{2} \mapsto a + b\sqrt{2}$
- y-axis: $a + b\sqrt{2} \mapsto a - b\sqrt{2}$
- component-wise multiplication

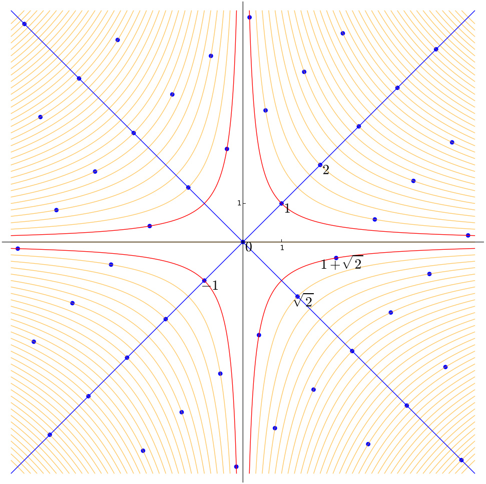
Example: Embedding $\mathbb{Z}[\sqrt{2}] \hookrightarrow \mathbb{R}^2$



- x-axis: $a + b\sqrt{2} \mapsto a + b\sqrt{2}$
- y-axis: $a + b\sqrt{2} \mapsto a - b\sqrt{2}$
- component-wise multiplication

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

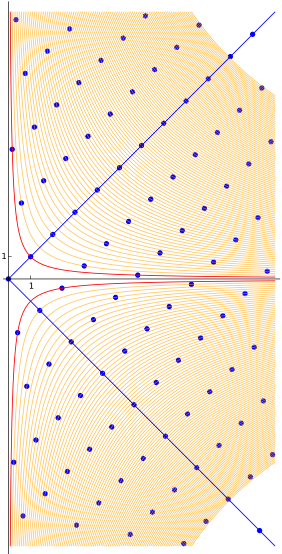
Example: Embedding $\mathbb{Z}[\sqrt{2}] \hookrightarrow \mathbb{R}^2$

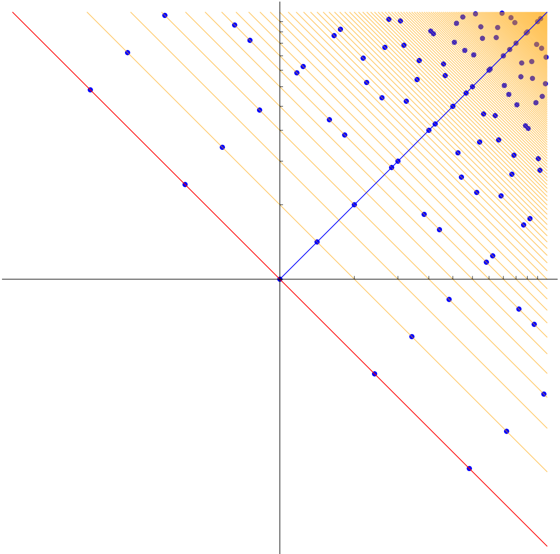


- x-axis: $a + b\sqrt{2} \mapsto a + b\sqrt{2}$
- y-axis: $a + b\sqrt{2} \mapsto a - b\sqrt{2}$
- component-wise multiplication
- Symmetries induced by
  - mult. by -1
  - conjugation $\sqrt{2} \mapsto -\sqrt{2}$

■ "Orthogonal" elements
■ Units (algebraic norm 1)
■ "Isonorms" curves

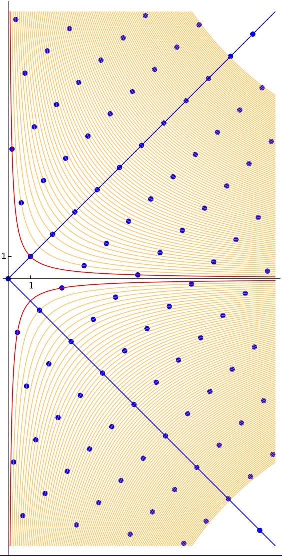
$(\{\bullet\}, +)$ is a sub-monoid of $\mathbb{R}^2$

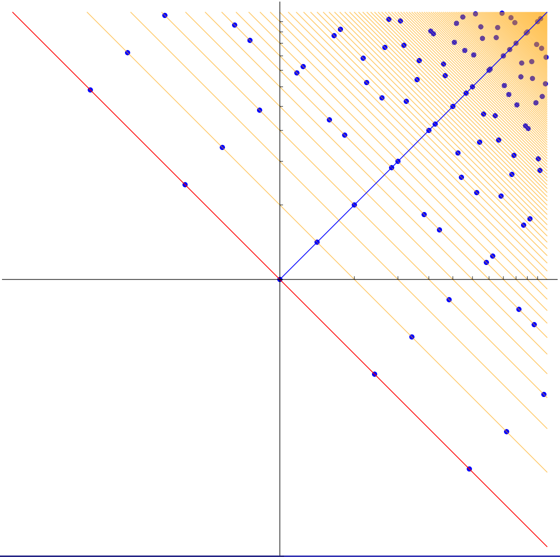




Example: Logarithmic Embedding $\text{Log}\,\mathbb{Z}[\sqrt{2}]$

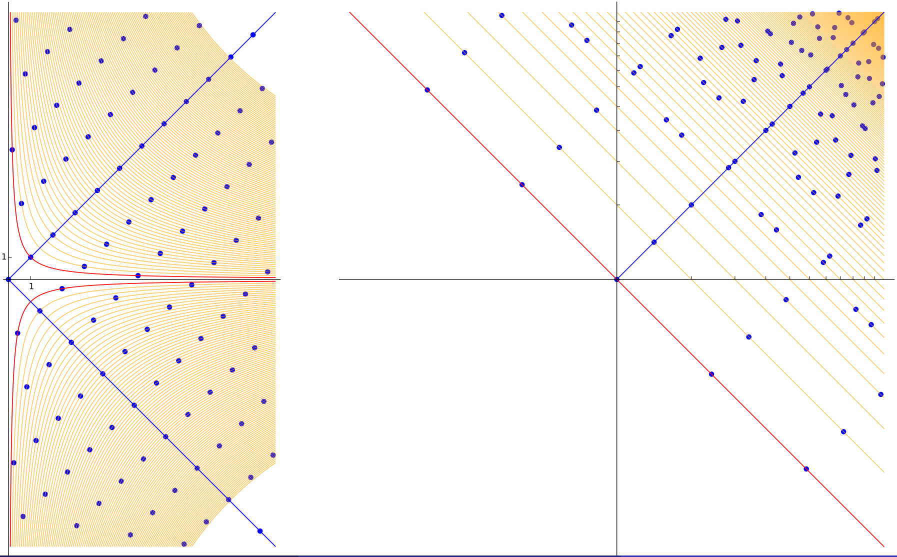
$\Lambda = (\{\bullet\}, +) \cap \diagdown$ is a lattice of $\mathbb{R}^2$, orthogonal to $(1, 1)$





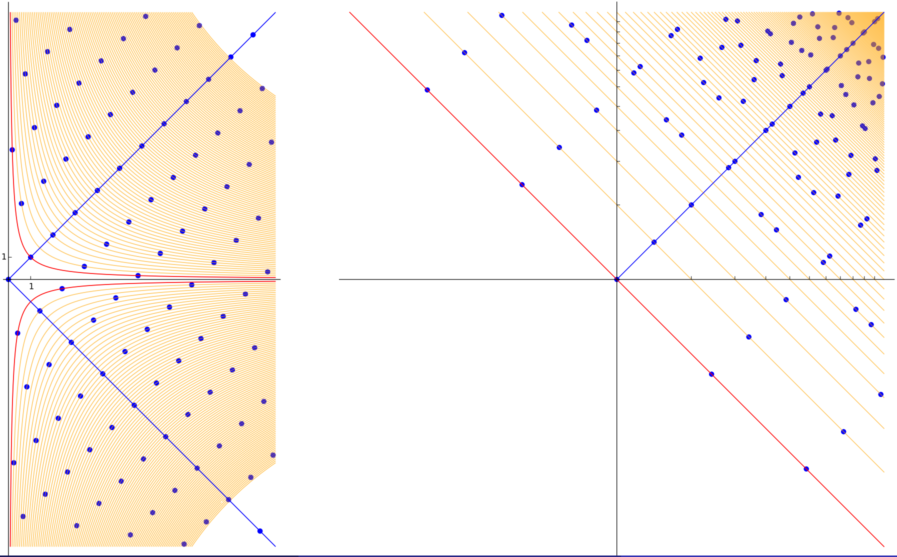
Example: Logarithmic Embedding $\operatorname{Log}\mathbb{Z}[\sqrt{2}]$

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



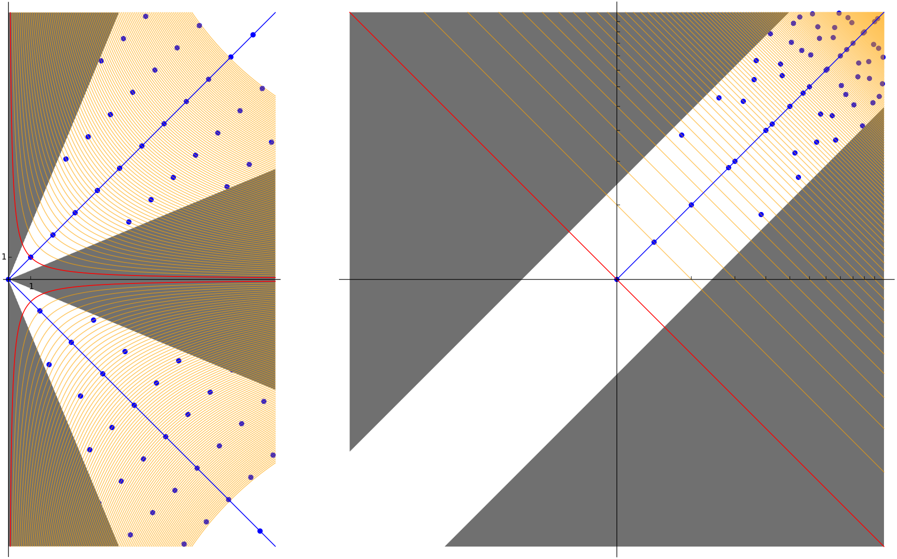
Example: Logarithmic Embedding Log $\mathbb{Z}[\sqrt{2}]$

Some $\{\bullet\} \cap$ ╲ may be empty (e.g. no elements of Norm 3 in $\mathbb{Z}[\sqrt{2}]$)



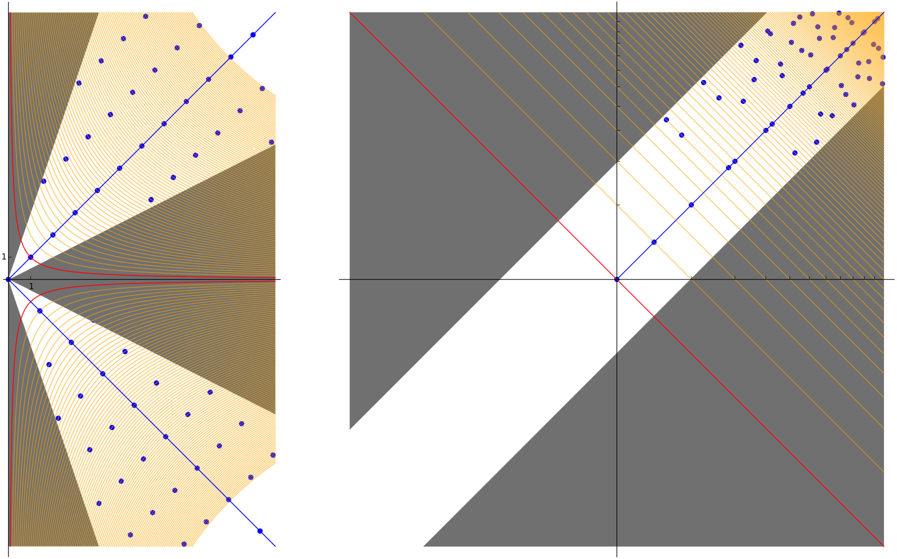
Reduction modulo $\Lambda = \operatorname{Log} \mathbb{Z}[\sqrt{2}]^\times$

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



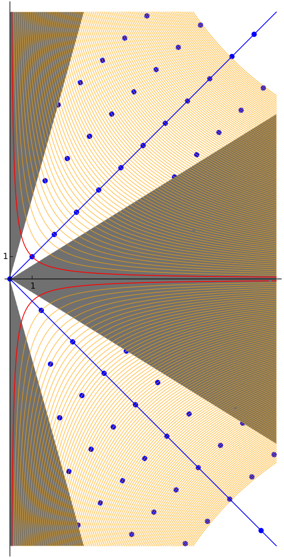
Reduction modulo $\Lambda = \operatorname{Log} \mathbb{Z}[\sqrt{2}]^{\times}$

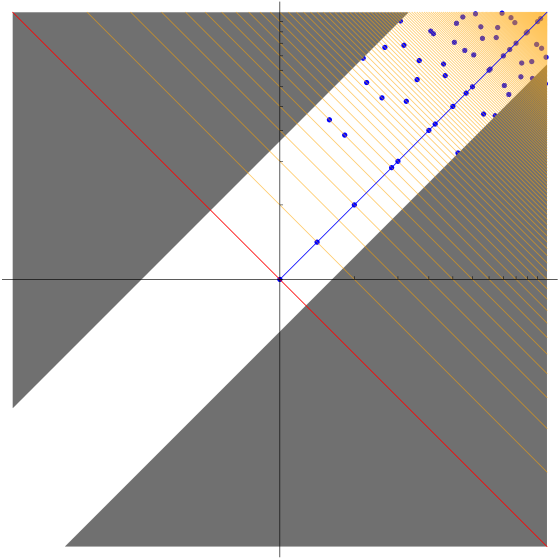
The reduction $\bmod \Lambda$ for various fundamental domains.



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

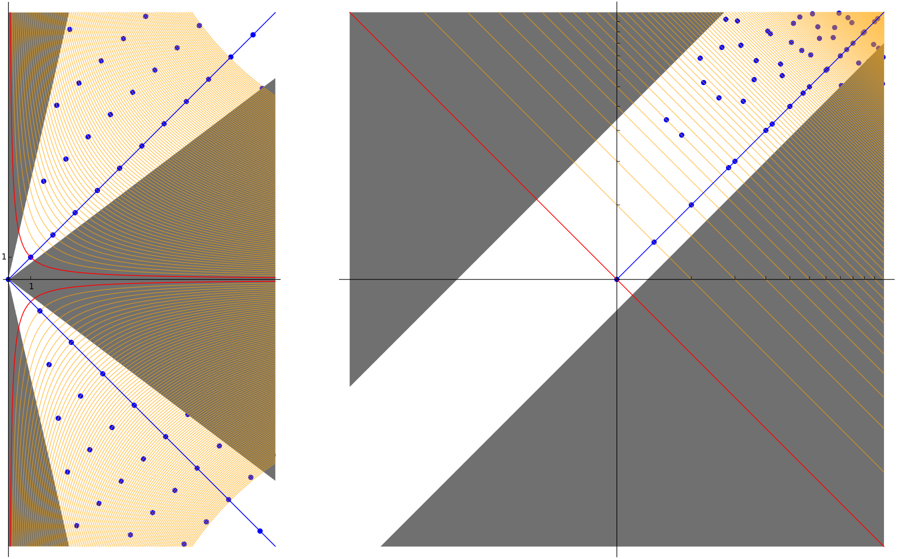
The reduction $\bmod \Lambda$ for various fundamental domains.





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

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



Decoding with the RoundOff algorithm

The simplest algorithm [Babai, 1986] to reduce modulo a lattice

RoundOff$(\mathbf{B}, \mathbf{t})$, $\mathbf{B}$ a $\mathbb{Z}$-basis of Λ

$\mathbf{v} = \mathbf{B} \cdot \lfloor (\mathbf{B}^\vee)^\top \cdot \mathbf{t} \rceil$
$\mathbf{e} = \mathbf{t} - \mathbf{v}$
return $(\mathbf{t}, \mathbf{e})$ where $\mathbf{t} \in \mathbf{B}$

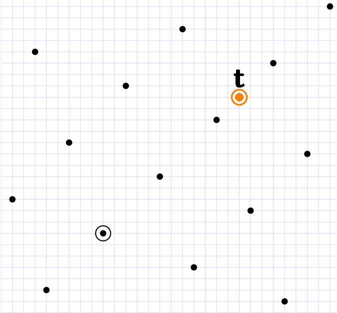
Used as a *d*ecoding algorithm, its correctness is characterized by the error $\mathbf{e}$ and the *dual basis* $\mathbf{B}^\vee$.

Fact(Correctness of RoundOff)

let $\mathbf{t} = \mathbf{v} + \mathbf{e}$ 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

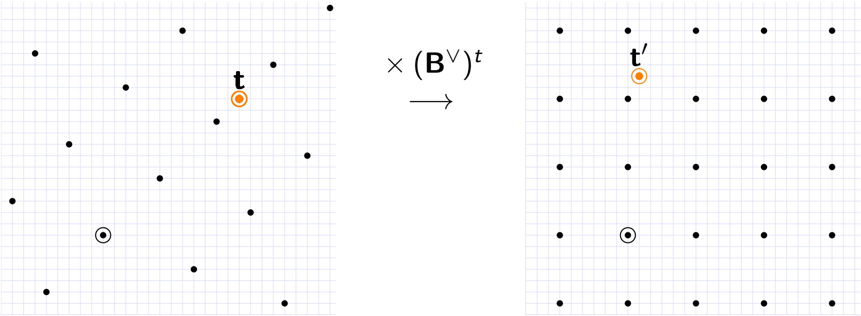
$$\text{RoundOff}(\mathbf{B}, \mathbf{t}) = (\mathbf{v}, \mathbf{e}).$$

RoundOff in pictures



RoundOff algorithm:

RoundOff in pictures

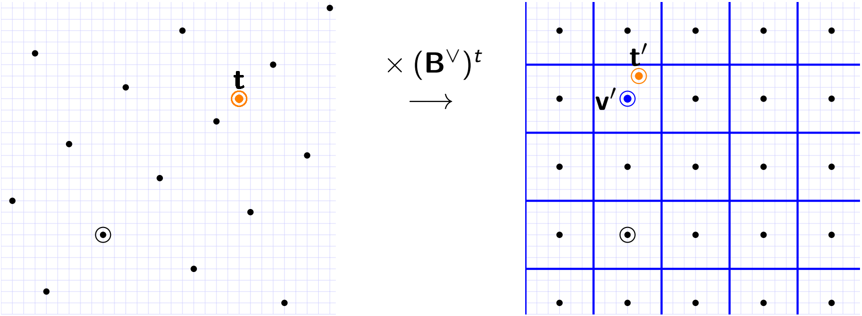


RoundOff algorithm:

1. use basis **B** to switch to the lattice $\mathbb{Z}^n$ $(\times(\mathbf{B}^\vee)^t)$

$$\mathbf{t}' = (\mathbf{B}^\vee)^t \cdot \mathbf{t};$$

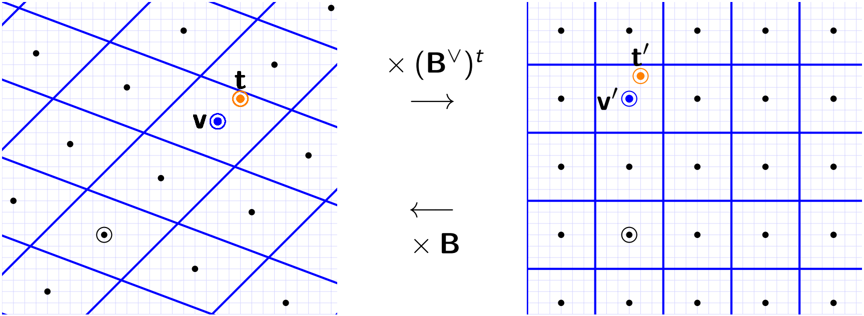
RoundOff in pictures



RoundOff algorithm:

1. use basis $\mathbf{B}$ to switch to the lattice $\mathbb{Z}^n$ $(\times(\mathbf{B}^\vee)^t)$
2. Round each coordinate

$$\mathbf{t}' = (\mathbf{B}^\vee)^t \cdot \mathbf{t}; \quad \mathbf{v}' = \lfloor \mathbf{t}' \rceil;$$



RoundOff algorithm:

1. use basis $\mathbf{B}$ to switch to the lattice $\mathbb{Z}^n$ $(\times(\mathbf{B}^\vee)^t)$
2. Round each coordinate
3. Switch back to the lattice L $(\times\mathbf{B})$

$$\mathbf{t}' = (\mathbf{B}^\vee)^t \cdot \mathbf{t}; \quad \mathbf{v}' = \lfloor \mathbf{t}' \rceil; \quad \mathbf{v} = \mathbf{B} \cdot \mathbf{v}'$$

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[2]) 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

[2] 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[2]) 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 [CDPR15]

2. Estimate $\|\mathbf{b}_j^\vee\|$ precisely using analytic tools [Washington, 1997, Littlewood, 1924]
3. Bound $\mathbf{e}$ using theory of sub-exponential random variables [Vershynin, 2012]

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

Overview

Cyclotomic units

We fix the number field $K = \mathbb{Q}(\zeta_m)$ where $m = p^k$ for some prime p. Set

$$z_j = 1 - \zeta^j \quad \text{and } b_j = z_j / z_1 \text{ for all } j \text{ coprimes with } m.$$

The b_j are units, and the group C generated by

$$\zeta, \quad b_j \quad \text{for } j = 2, \ldots m/2, j \text{ coprime with } m$$

is known as the group of *cyclotomic units*.

[3] One just need the index $[R^\times : C] = h^+(m)$ to be small.

Cyclotomic units

We fix the number field $K = \mathbb{Q}(\zeta_m)$ where $m = p^k$ for some prime p. Set

$$z_j = 1 - \zeta^j \quad \text{and } b_j = z_j / z_1 \text{ for all } j \text{ coprimes with } m.$$

The b_j are units, and the group C generated by

$$\zeta, \quad b_j \quad \text{for } j = 2, \ldots m/2, j \text{ coprime with } m$$

is known as the group of *cyclotomic units*.

Simplification 1 (Weber's Class Number Problem)

We assume[3] that $R^\times = C$. It is conjectured to be true for $m = 2^k$.

[3] One just need the index $[R^\times : C] = h^+(m)$ to be small.

Cyclotomic units

We fix the number field $K = \mathbb{Q}(\zeta_m)$ where $m = p^k$ for some prime p. Set

$$z_j = 1 - \zeta^j \quad \text{and } b_j = z_j / z_1 \text{ for all } j \text{ coprimes with } m.$$

The b_j are units, and the group C generated by

$$\zeta, \quad b_j \quad \text{for } j = 2, \dots m/2, j \text{ coprime with } m$$

is known as the group of *cyclotomic units*.

Simplification 1 (Weber's Class Number Problem)

We assume[3] that $R^\times = C$. It is conjectured to be true for $m = 2^k$.

Simplification 2 (for this talk)

We study the dual matrix $\mathbf{Z}^\vee$, where $\mathbf{z}_j = \operatorname{Log} z_j$.
It can be proved to close to $\mathbf{B}^\vee$ where $\mathbf{b}_j = \mathbf{z}_j - \mathbf{z}_1$.

[3]One just need the index $[R^\times : C] = h^+(m)$ to be small.

The matrix **Z**

The field K admits exactly $\varphi(m)/2$ pairs of conjugate complex embeddings

$$\sigma_i = \overline{\sigma_{-i}}, \text{ where } \sigma_i : \zeta \mapsto \omega^i \text{ is defined for all } i \in \mathbb{Z}_m^\times.$$

where $\omega = \exp(2\imath\pi/m) \in \mathbb{C}$ is a primitive root of unity.

The matrix **Z**

The field K admits exactly $\varphi(m)/2$ pairs of conjugate complex embeddings

$$\sigma_i = \overline{\sigma_{-i}}, \text{ where } \sigma_i : \zeta \mapsto \omega^i \text{ is defined for all } i \in \mathbb{Z}_m^\times.$$

where $\omega = \exp(2\imath\pi/m) \in \mathbb{C}$ is a primitive root of unity.

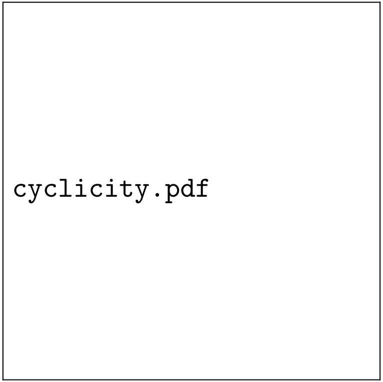


Figure : Naïve Indexing ($i = 1, 3, 5, \dots$)

The field K admits exactly $\varphi(m)/2$ pairs of conjugate complex embeddings

$$\sigma_i = \overline{\sigma_{-i}}, \text{ where } \sigma_i : \zeta \mapsto \omega^i \text{ is defined for all } i \in \mathbb{Z}_m^\times.$$

where $\omega = \exp(2\imath\pi/m) \in \mathbb{C}$ is a primitive root of unity.

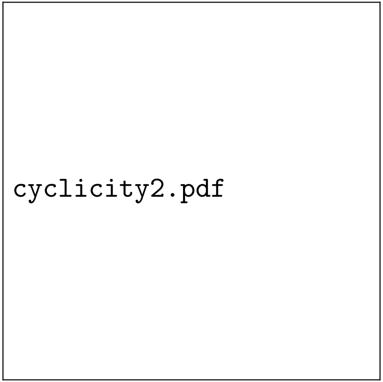


Figure : Multiplicative Indexing ($i = 3^0, 3^1, 3^2, \ldots$)

Dual of a Circulant Basis

Notice that $\mathbf{Z}_{ij} = \log|\sigma_j(1-\zeta^i)| = \log|1-\omega^{ij}|$:
the matrix $\mathbf{Z}$ is G-circulant for the cyclic group $G = \mathbb{Z}_m^\times / \pm 1$.

Dual of a Circulant Basis

Notice that $\mathbf{Z}_{ij} = \log |\sigma_j(1-\zeta^i)| = \log |1-\omega^{ij}|$:
the matrix $\mathbf{Z}$ is G-circulant for the cyclic group $G = \mathbb{Z}_m^\times / \pm 1$.

Fact

If $\mathbf{M}$ is a non-singular, G-circulant matrix, then

- *its eigenvalues are given by* $\lambda_\chi = \sum_{g \in G} \overline{\chi(g)} \cdot \mathbf{M}_{1,g}$
  where $\chi \in \widehat{G}$ *is a character* $G \to \mathbb{C}$
- *All the vectors of* $\mathbf{M}^\vee$ *have the same norm* $\|\mathbf{m}_i^\vee\|^2 = \sum_{\chi \in \widehat{G}} |\lambda_\chi|^{-2}$

Note: The characters of G can be extended to even Dirichlet characters mod m: $\chi : \mathbb{Z} \to \mathbb{C}$, by setting $\chi(a) = 0$ if $\gcd(a, m) > 1$.

Computing the Eigenvalues

We wish to give a lower bound on $|\lambda_\chi|$ where

$$\lambda_\chi = \sum_{a \in G} \overline{\chi(a)} \cdot \log |1 - \omega^a|.$$

Computing the Eigenvalues

We wish to give a lower bound on $|\lambda_\chi|$ where

$$\lambda_\chi = \sum_{a \in G} \overline{\chi(a)} \cdot \log |1 - \omega^a|.$$

Why not stop here ?

This formula is pretty easy to evaluate numerically: at this point we can already check RoundOff's correctness numerically up to $m = 10^6$ or more.

Computing the Eigenvalues

We wish to give a lower bound on $|\lambda_\chi|$ where

$$\lambda_\chi = \sum_{a \in G} \overline{\chi(a)} \cdot \log |1 - \omega^a|.$$

Why not stop here ?

This formula is pretty easy to evaluate numerically: at this point we can already check RoundOff's correctness numerically up to $m = 10^6$ or more.

Something cute to be learned !

The equations looks not very algebraic (log ?), yet appears quite naturally... Surely mathematicians knows how to deal with this.

Indeed, computation of the volume of that basis appears in [Washington, 1997].

Computing the Eigenvalues

We wish to give a lower bound on $|\lambda_\chi|$ where

$$\lambda_\chi = \sum_{a \in G} \overline{\chi(a)} \cdot \log|1 - \omega^a|.$$

We develop using the Taylor series

$$\log|1 - x| = -\sum_{k \geq 1} x^k / k$$

Computing the Eigenvalues

We wish to give a lower bound on $|\lambda_\chi|$ where

$$\lambda_\chi = \sum_{a \in G} \overline{\chi(a)} \cdot \log |1 - \omega^a|.$$

We develop using the Taylor series

$$\log |1 - x| = -\sum_{k \geq 1} x^k / k$$

and obtain

$$-\lambda_\chi = \sum_{a \in G} \sum_{k \geq 1} \overline{\chi(a)} \cdot \frac{\omega^{ka}}{k}.$$

Computing the Eigenvalues (continued)

We were trying to lower bound $|\lambda_\chi|$ where

$$-\lambda_\chi = \sum_{k \geq 1} \frac{1}{k} \cdot \sum_{a \in G} \overline{\chi(a)} \cdot \omega^{ka}.$$

Computing the Eigenvalues (continued)

We were trying to lower bound $|\lambda_\chi|$ where

$$-\lambda_\chi = \sum_{k\geq 1} \frac{1}{k} \cdot \sum_{a\in G} \overline{\chi(a)} \cdot \omega^{ka}.$$

Fact (Separability of Gauss Sums)

If χ is a primitive Dirichlet character mod m *then*

$$\sum_{a\in\mathbb{Z}_m^\times} \overline{\chi(a)} \cdot \omega^{ka} = \chi(k) \cdot G(\chi) \quad \textit{where } |G(\chi)| = \sqrt{m}.$$

Computing the Eigenvalues (continued)

We were trying to lower bound $|\lambda_\chi|$ where

$$-\lambda_\chi = \sum_{k \geq 1} \frac{1}{k} \cdot \sum_{a \in G} \overline{\chi(a)} \cdot \omega^{ka}.$$

Fact (Separability of Gauss Sums)

If χ is a primitive Dirichlet character mod m *then*

$$\sum_{a \in \mathbb{Z}_m^\times} \overline{\chi(a)} \cdot \omega^{ka} = \chi(k) \cdot G(\chi) \quad \text{where } |G(\chi)| = \sqrt{m}.$$

For this talk, let's ignore non-primitive characters. We rewrite

$$|\lambda_\chi| = \sqrt{\frac{m}{2}} \cdot \left| \sum_{k \geq 1} \frac{\chi(k)}{k} \right|.$$

The Analytical Hammer

We were trying to lower bound $\left|\lambda_\chi\right| = \sqrt{\frac{m}{2}} \cdot \left|\sum_{k\geq 1} \frac{\chi(k)}{k}\right|$.
One recognizes a Dirichlet L-series

$$L(s, \chi) = \sum \frac{\chi(k)}{k^s}.$$

The Analytical Hammer

We were trying to lower bound $\left|\lambda_\chi\right| = \sqrt{\frac{m}{2}} \cdot \left|\sum_{k\geq 1} \frac{\chi(k)}{k}\right|$.
One recognizes a Dirichlet L-series

$$L(s,\chi) = \sum \frac{\chi(k)}{k^s}.$$

Theorem ([Littlewood, 1924, Youness et al., 2013])

Under the Generalized Riemann Hypothesis, for any primitive Dirichlet character χ mod m it holds that

$$1/\ell(m) \leq |L(1,\chi)| \leq \ell(m) \quad \textit{where } \ell(m) = C \ln\ln m$$

for some universal constant $C > 0$.

Geometric Conclusion

Theorem (Cramer, D. , Peikert, Regev)

Let $m = p^k$*, and* $\mathbf{B} = \left(\mathrm{Log}(b_j)\right)_{j \in G \setminus \{1\}}$ *be the canonical basis of* $\mathrm{Log}\, C$*. Then, all the vectors of* $\mathbf{B}^\vee$ *have the same norm and, under GRH, this norm is upper bounded as follows*

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

Overview

Proof Plan (Reminder)

1. Construct a basis $\mathbf{B}$ of the unit-log lattice $\operatorname{Log} R^\times$
   - Choose the Canonical Cyclotomics Units
   $$\mathbf{b}_j = \operatorname{Log} \frac{1-\zeta^j}{1-\zeta}$$
2. Prove that the basis is "good", that is $\|\mathbf{b}_j^\vee\|$ are all small
   - Proved
   $$\left\|\mathbf{b}_j^\vee\right\|^2 \leq O\left(m^{-1} \cdot \log^3 m\right)$$
3. Prove that $\mathbf{e} = \operatorname{Log} g$ is small enough

Scaling Invariance

Lets assume the embeddings $(\sigma_i(g))$ are i.i.d. of distribution $\mathcal{D}$.

$$\mathrm{Log}\,(s \cdot \mathcal{D}^n) \simeq (1, 1, \ldots 1) \cdot \log s + \mathrm{Log}\,\mathcal{D}^n$$

Heuristic argument

Using scaling, assume that $\mathbb{E}[\operatorname{Log}\mathcal{D}^m] = \mathbf{0}$.

- Let $\mathbf{e} \leftarrow \operatorname{Log}\mathcal{D}^m$ ($\mathbf{e} = \operatorname{Log} g$)
- Each coordinate $\operatorname{Log}\mathcal{D}$ of $\mathbf{e}$ are independents, centered, of variance V
- For any $\mathbf{b}$, the variance of $\langle \mathbf{b}, \mathbf{e} \rangle$ is $V \cdot \|\mathbf{b}\|$
- By Markov Inequality, for a fixed i it should hold that

$$|\langle \mathbf{b}_i^\vee, \mathbf{e} \rangle| \leq 1/2$$

except with $o(1)$ probability (recall we've proved that $\|\mathbf{b}_i^\vee\| = o(1)$)

Conclusion from better tail bounds

The previous argument does not allows to conclude simultanously on all i's. We fill this gap using stronger tail bounds, form the theory of sub-exponential random variables [Vershynin, 2012]

Theorem (Cramer, D. , Peikert, Regev)

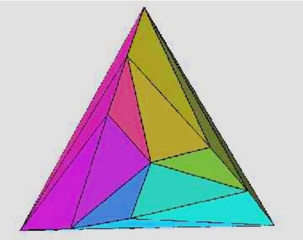
If g follows a Continuous Normal Distribution, then for $\mathbf{e} = \operatorname{Log} g$, we have $|\langle \mathbf{b}_i^\vee, \mathbf{e}\rangle| \leq 1/2$ for all i's except with negligible probability.

Corollary

If g follows a Discrete Normal Distribution of parameter $\sigma \geq poly(m)$, then for $\mathbf{e} = \operatorname{Log} g$, we have $|\langle \mathbf{b}_i^\vee, \mathbf{e}\rangle| \leq 1/2$ for all i's except with probability $1/n^{\Theta(1)}$.

Thanks

Figure : The Shintani Domain of $\mathbb{Z}[\zeta_7 + \bar{\zeta_7}]$. Credit: Paul Gunells
`http://people.math.umass.edu/~gunnells/pictures/pictures.html`



We thank Dan Bernstein, Jean-Franois Biasse, Sorina Ionica, Dimitar Jetchev, Paul Kirchner, René Schoof, Dan Shepherd and Harold M. Stark for many insightful conversations related to this work.

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. (2015a).
A note on the quantum attacks against schemes relying on the hardness of finding a short generator of an ideal in Q(z_2n̂).
http://cacr.uwaterloo.ca/techreports/2015/cacr2015-12.pdf.
Technical Report.

References II

Biasse, J.-F. and Song, F. (2015b).
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/.
In preparation.

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.

Cramer, R., Ducas, L., Peikert, C., and Regev, O. (2015).
Recovering short generators of principal ideals in cyclotomic rings.
Cryptology ePrint Archive, Report 2015/313.
http://eprint.iacr.org/.

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.

References III

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

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.

Littlewood, J. (1924).
On the zeros of the riemann zeta-function.
In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 22, pages 295–318. Cambridge Univ Press.

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.

References IV

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.

Youness, L., Xiannan, L., and Kannan, S. (2013).
Conditional bounds for the least quadratic non-residue and related problems.
http://arxiv.org/abs/1309.3595.