Computing Generator in Cyclotomic Integer Rings

A subfield algorithm for the Principal Ideal Problem in $L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$ and application to the cryptanalysis of a FHE scheme

Jean-François Biasse[1] Thomas Espitau[2]
Pierre-Alain Fouque[3] Alexandre Gélin[2] Paul Kirchner[4]

University of South Florida, Department of Mathematics and Statistics, Tampa, USA
Sorbonne Universités, UPMC Paris 6, UMR 7606, LIP6, Paris, France
Institut Universitaire de France, Paris, France and Université de Rennes 1, France
École Normale Supérieure, Paris, France

2017/05/01

The Principal Ideal Problem

Definition

The *Principal Ideal Problem* (PIP) consists in finding a generator of an ideal, assuming it is principal.

The Principal Ideal Problem

Definition

The *Short Principal Ideal Problem* (SPIP) consists in finding a short generator of an ideal, assuming it is principal.

The Principal Ideal Problem

Definition

The *Short Principal Ideal Problem* (SPIP) consists in finding a short generator of an ideal, assuming it is principal.

- Base of several cryptographical schemes ([SV10],[GGH13])

Definition

The *Short Principal Ideal Problem* (SPIP) consists in finding a short generator of an ideal, assuming it is principal.

- Base of several cryptographical schemes ([SV10],[GGH13])
- Two distinct phases:
  1. Given the $\mathbb{Z}$-basis of the ideal $\mathfrak{a} = \langle \boldsymbol{g} \rangle$, find a — not necessarily short — generator $\boldsymbol{g'} = \boldsymbol{g} \cdot \boldsymbol{u}$ for a unit $\boldsymbol{u}$.
  2. From $\boldsymbol{g'}$, find a short generator of the ideal.

The Principal Ideal Problem

Definition

The *Short Principal Ideal Problem* (SPIP) consists in finding a short generator of an ideal, assuming it is principal.

- Base of several cryptographical schemes ([SV10],[GGH13])
- Two distinct phases:
  1. Given the $\mathbb{Z}$-basis of the ideal $\mathfrak{a} = \langle \boldsymbol{g} \rangle$, find a — not necessarily short — generator $\boldsymbol{g'} = \boldsymbol{g} \cdot \boldsymbol{u}$ for a unit $\boldsymbol{u}$.
  2. From $\boldsymbol{g'}$, find a short generator of the ideal.

Campbell, Groves, and Sheperd (2014) found a solution in polynomial time for the second point for power-of-two cyclotomic fields. Cramer, Ducas, Peikert, and Regev (2016) provided a proof and an extension to prime-power cyclotomic fields.

Key Generation:

1. Fix the security parameter $N = 2^n$.
2. Let $F(X) = X^N + 1$ be the polynomial defining the cyclotomic field $\mathbb{K} = \mathbb{Q}(\zeta_{2N})$.
3. Set $G(X) = 1 + 2 \cdot S(X)$,
   for $S(X)$ of degree $N - 1$ with coefficients in $\left[-2^{\sqrt{N}}, 2^{\sqrt{N}}\right]$,
   such that the norm $\mathcal{N}\left(\langle G(\zeta_{2N})\rangle\right)$ is prime.
4. Set $\boldsymbol{g} = G(\zeta_{2N}) \in \mathcal{O}_{\mathbb{K}}$.
5. Return the secret key $\mathsf{sk} = \boldsymbol{g}$ and the public key $\mathsf{pk} = \mathsf{HNF}(\langle \boldsymbol{g} \rangle)$.

FHE scheme – Smart and Vercauteren PKC 2010

Key Generation:

1. Fix the security parameter $N = 2^n$.
2. Let $F(X) = X^N + 1$ be the polynomial defining the cyclotomic field $\mathbb{K} = \mathbb{Q}(\zeta_{2N})$.
3. Set $G(X) = 1 + 2 \cdot S(X)$, for $S(X)$ of degree $N-1$ with coefficients in $\left[-2^{\sqrt{N}}, 2^{\sqrt{N}}\right]$, such that the norm $\mathcal{N}\left(\langle G(\zeta_{2N})\rangle\right)$ is prime.
4. Set $\boldsymbol{g} = G(\zeta_{2N}) \in \mathcal{O}_{\mathbb{K}}$.
5. Return the secret key $\mathsf{sk} = \boldsymbol{g}$ and the public key $\mathsf{pk} = \mathsf{HNF}(\langle \boldsymbol{g} \rangle)$.

Our goal: Recover the secret key from the public key.

Outline of the algorithm

1. Perform a reduction from the cyclotomic field to its totally real subfield, allowing to work in smaller dimension.
2. Then a $\mathfrak{q}$-descent makes the size of involved ideals decrease.
3. Collect relations and run linear algebra to construct small ideals and a generator.
4. Eventually run the derivation of the short generator from a bigger one.

Outline of the algorithm

1. Perform a reduction from the cyclotomic field to its totally real subfield, allowing to work in smaller dimension.
2. Then a $\mathfrak{q}$-descent makes the size of involved ideals decrease.
3. Collect relations and run linear algebra to construct small ideals and a generator.
4. Eventually run the derivation of the short generator from a bigger one.

All the complexities are expressed as a function of the field discriminant $\Delta_{\mathbb{Q}(\zeta_{2N})} = N^N$, for $N = 2^n$.

Outline of the algorithm

1. Perform a reduction from the cyclotomic field to its totally real subfield, allowing to work in smaller dimension.
2. Then a $\mathfrak{q}$-descent makes the size of involved ideals decrease.
3. Collect relations and run linear algebra to construct small ideals and a generator.
4. Eventually run the derivation of the short generator from a bigger one.

All the complexities are expressed as a function of the field discriminant $\Delta_{\mathbb{Q}(\zeta_{2N})} = N^N$, for $N = 2^n$. For instance,

$$L_{|\Delta_{\mathbb{K}}|}(\alpha) = 2^{N^{\alpha+o(1)}}.$$

1. Reduction to the totally real subfield

Goal: Halving the dimension of the ambient field

Gentry-Szydlo algorithm: *Polynomial complexity*

- **Input:** a $\mathbb{Z}$-basis of $\mathcal{I} = \langle \boldsymbol{u} \rangle$ and $\boldsymbol{u} \cdot \bar{\boldsymbol{u}}$
- **Output:** the generator $\boldsymbol{u}$

1. Reduction to the totally real subfield

Goal: Halving the dimension of the ambient field

Gentry-Szydlo algorithm: *Polynomial complexity*

- **Input:** a $\mathbb{Z}$-basis of $\mathcal{I} = \langle \boldsymbol{u} \rangle$ and $\boldsymbol{u} \cdot \bar{\boldsymbol{u}}$
- **Output:** the generator $\boldsymbol{u}$

Problem: no information about $\boldsymbol{g} \cdot \bar{\boldsymbol{g}}$ ($\boldsymbol{g}$ is the private key)

1. Reduction to the totally real subfield

Goal: Halving the dimension of the ambient field

Gentry-Szydlo algorithm: *Polynomial complexity*

- **Input:** a $\mathbb{Z}$-basis of $\mathcal{I} = \langle \boldsymbol{u} \rangle$ and $\boldsymbol{u} \cdot \bar{\boldsymbol{u}}$
- **Output:** the generator $\boldsymbol{u}$

Solution: we introduce $\boldsymbol{u} = \mathcal{N}(\boldsymbol{g})\boldsymbol{g}\bar{\boldsymbol{g}}^{-1}$

Goal: Halving the dimension of the ambient field

Gentry-Szydlo algorithm: *Polynomial complexity*

- **Input:** a $\mathbb{Z}$-basis of $\mathcal{I} = \langle \boldsymbol{u} \rangle$ and $\boldsymbol{u} \cdot \bar{\boldsymbol{u}}$
- **Output:** the generator $\boldsymbol{u}$

Solution: we introduce $\boldsymbol{u} = \mathcal{N}(\boldsymbol{g})\boldsymbol{g}\bar{\boldsymbol{g}}^{-1}$

$\mathbb{Z}$-basis of $\langle \boldsymbol{g} \rangle \Longrightarrow \mathbb{Z}$-basis of $\langle \boldsymbol{u} \rangle$ and $\boldsymbol{u} \cdot \bar{\boldsymbol{u}} = \mathcal{N}(\boldsymbol{g})^2$

1. Reduction to the totally real subfield

Goal: Halving the dimension of the ambient field

Gentry-Szydlo algorithm: *Polynomial complexity*

- **Input:** a $\mathbb{Z}$-basis of $\mathcal{I} = \langle \boldsymbol{u} \rangle$ and $\boldsymbol{u} \cdot \bar{\boldsymbol{u}}$
- **Output:** the generator $\boldsymbol{u}$

Solution: we introduce $\boldsymbol{u} = \mathcal{N}(\boldsymbol{g})\boldsymbol{g}\bar{\boldsymbol{g}}^{-1}$

$\mathbb{Z}$-basis of $\langle \boldsymbol{g} \rangle \Longrightarrow \mathbb{Z}$-basis of $\langle \boldsymbol{u} \rangle$ and $\boldsymbol{u} \cdot \bar{\boldsymbol{u}} = \mathcal{N}(\boldsymbol{g})^2$

In the end, we get $\boldsymbol{g} \cdot \bar{\boldsymbol{g}}^{-1}$ and a $\mathbb{Z}$-basis of $\mathcal{I}^+ = \langle \boldsymbol{g} + \bar{\boldsymbol{g}} \rangle \subset \mathbb{Q}(\zeta + \zeta^{-1})$

1. Reduction to the totally real subfield

Goal: Halving the dimension of the ambient field

Gentry-Szydlo algorithm: *Polynomial complexity*

- **Input:** a $\mathbb{Z}$-basis of $\mathcal{I} = \langle \boldsymbol{u} \rangle$ and $\boldsymbol{u} \cdot \bar{\boldsymbol{u}}$
- **Output:** the generator $\boldsymbol{u}$

Solution: we introduce $\boldsymbol{u} = \mathcal{N}(\boldsymbol{g})\boldsymbol{g}\bar{\boldsymbol{g}}^{-1}$

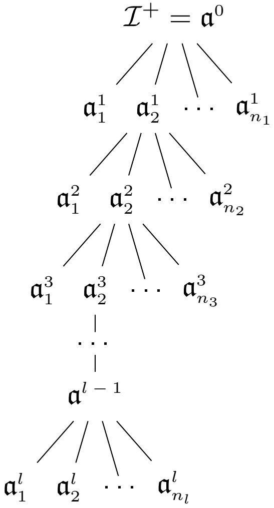
$\mathbb{Z}$-basis of $\langle \boldsymbol{g} \rangle \implies \mathbb{Z}$-basis of $\langle \boldsymbol{u} \rangle$ and $\boldsymbol{u} \cdot \bar{\boldsymbol{u}} = \mathcal{N}(\boldsymbol{g})^2$

In the end, we get $\boldsymbol{g} \cdot \bar{\boldsymbol{g}}^{-1}$ and a $\mathbb{Z}$-basis of $\mathcal{I}^+ = \langle \boldsymbol{g} + \bar{\boldsymbol{g}} \rangle \subset \mathbb{Q}(\zeta + \zeta^{-1})$

Once we have a generator for $\mathcal{I}^+$, we get one for $\mathcal{I}$ by multiplying by

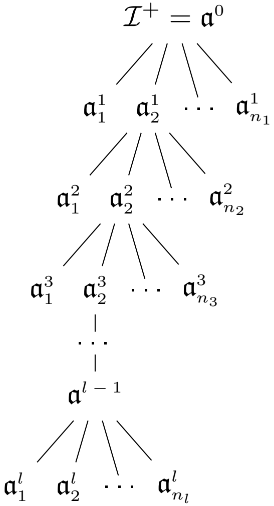
$$\frac{1}{1 + \bar{\boldsymbol{g}} \cdot \boldsymbol{g}^{-1}}$$

2. The $\mathfrak{q}$-descent



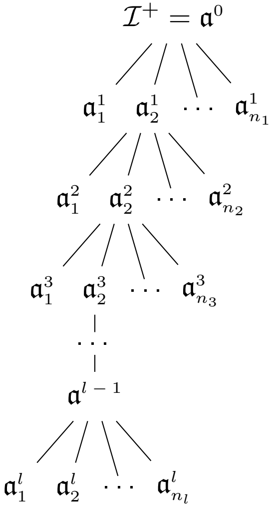
Input ideal – Norm arbitrary large

2. The $\mathfrak{q}$-descent



Input ideal – Norm arbitrary large

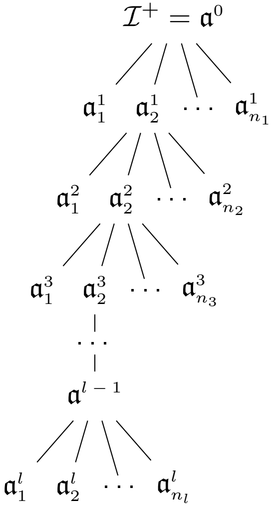
Initial reduction – Norm: $L_{|\Delta_{\mathbb{K}}|}\left(\frac{3}{2}\right)$



Input ideal – Norm arbitrary large

Initial reduction – $L_{|\Delta_{\mathbb{K}}|}(1)$-smooth

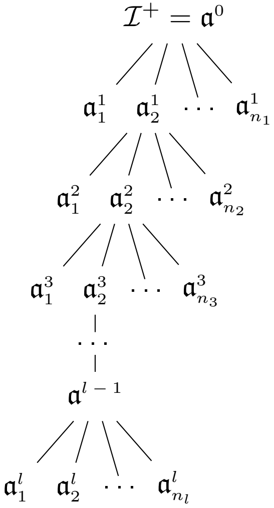
2. The $\mathfrak{q}$-descent



Input ideal – Norm arbitrary large

Initial reduction – $L_{|\Delta_{\mathbb{K}}|}(1)$-smooth

First step – Norm: $L_{|\Delta_{\mathbb{K}}|}\left(\frac{5}{4}\right)$

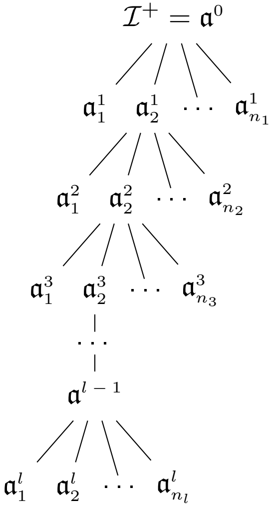


Input ideal – Norm arbitrary large

Initial reduction – $L_{|\Delta_{\mathbb{K}}|}(1)$-smooth

First step – $L_{|\Delta_{\mathbb{K}}|}\left(\frac{3}{4}\right)$-smooth

2. The $\mathfrak{q}$-descent

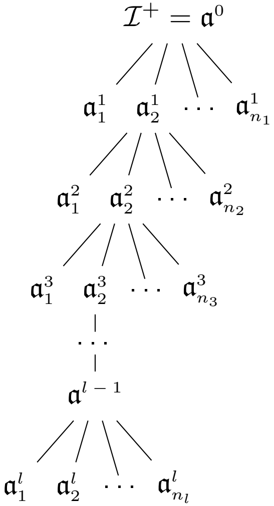


Input ideal – Norm arbitrary large

Initial reduction – $L_{|\Delta_{\mathbb{K}}|}(1)$-smooth

First step – $L_{|\Delta_{\mathbb{K}}|}\left(\frac{3}{4}\right)$-smooth

Second step – Norm: $L_{|\Delta_{\mathbb{K}}|}\left(\frac{9}{8}\right)$



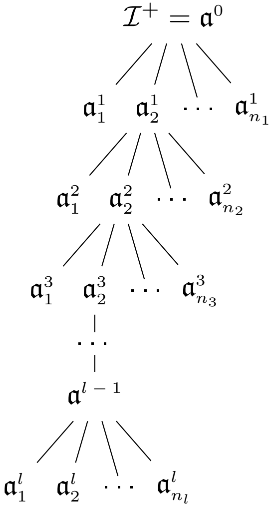
Input ideal – Norm arbitrary large

Initial reduction – $L_{|\Delta_{\mathbb{K}}|}(1)$-smooth

First step – $L_{|\Delta_{\mathbb{K}}|}\left(\frac{3}{4}\right)$-smooth

Second step – $L_{|\Delta_{\mathbb{K}}|}\left(\frac{5}{8}\right)$-smooth

2. The $\mathfrak{q}$-descent



Input ideal – Norm arbitrary large

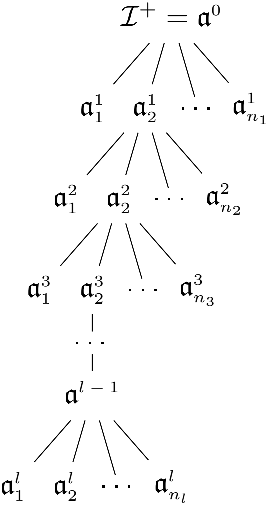
Initial reduction – $L_{|\Delta_{\mathbb{K}}|}(1)$-smooth

First step – $L_{|\Delta_{\mathbb{K}}|}\left(\frac{3}{4}\right)$-smooth

Second step – $L_{|\Delta_{\mathbb{K}}|}\left(\frac{5}{8}\right)$-smooth

Last but one step – Norm: $\approx L_{|\Delta_{\mathbb{K}}|}(1)$

2. The $\mathfrak{q}$-descent



Input ideal – Norm arbitrary large

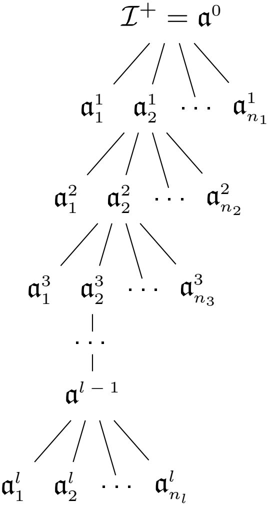
Initial reduction – $L_{|\Delta_{\mathbb{K}}|}(1)$-smooth

First step – $L_{|\Delta_{\mathbb{K}}|}\left(\frac{3}{4}\right)$-smooth

Second step – $L_{|\Delta_{\mathbb{K}}|}\left(\frac{5}{8}\right)$-smooth

Last but one step – $\approx L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$-smooth

2. The $\mathfrak{q}$-descent



Input ideal – Norm arbitrary large

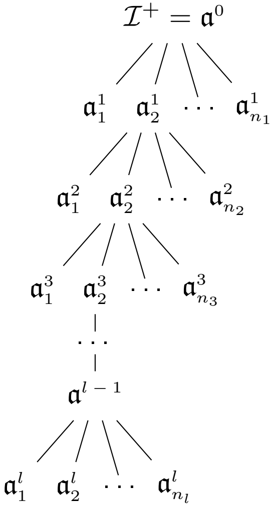
Initial reduction – $L_{|\Delta_\mathbb{K}|}(1)$-smooth

First step – $L_{|\Delta_\mathbb{K}|}\left(\frac{3}{4}\right)$-smooth

Second step – $L_{|\Delta_\mathbb{K}|}\left(\frac{5}{8}\right)$-smooth

Last but one step – $\approx L_{|\Delta_\mathbb{K}|}\left(\frac{1}{2}\right)$-smooth

Last step – Norm: $L_{|\Delta_\mathbb{K}|}(1)$



Input ideal – Norm arbitrary large

Initial reduction – $L_{|\Delta_{\mathbb{K}}|}(1)$-smooth

First step – $L_{|\Delta_{\mathbb{K}}|}\left(\frac{3}{4}\right)$-smooth

Second step – $L_{|\Delta_{\mathbb{K}}|}\left(\frac{5}{8}\right)$-smooth

Last but one step – $\approx L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$-smooth

Last step – $L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$-smooth

Input: $\mathfrak{a}$ of norm arbitrarily large

Input: $\mathfrak{a}$ of norm arbitrarily large

Tool: DBKZ-reduction with block-size $(\log |\Delta_{\mathbb{K}}|)^{\frac{1}{2}} \leq N$ on the lattice built from the canonical embedding $\mathcal{O}_{\mathbb{K}^+} \to \mathbb{R}^{\frac{N}{2}}$

Input: $\mathfrak{a}$ of norm arbitrarily large

Tool: DBKZ-reduction with block-size $(\log|\Delta_{\mathbb{K}}|)^{\frac{1}{2}} \leq N$ on the lattice built from the canonical embedding $\mathcal{O}_{\mathbb{K}^+} \to \mathbb{R}^{\frac{N}{2}}$

Output: small vector $\longleftrightarrow$ algebraic integer $\boldsymbol{v} \in \mathfrak{a}$

$\Longrightarrow$ ideal $\mathfrak{b} \subset \mathcal{O}_{\mathbb{K}^+}$ s.t. $\langle \boldsymbol{v} \rangle = \mathfrak{a} \cdot \mathfrak{b}$ and

$$\mathcal{N}(\mathfrak{b}) \leq L_{|\Delta_{\mathbb{K}}|}\left(\tfrac{3}{2}\right)$$

Input: $\mathfrak{a}$ of norm arbitrarily large

Tool: DBKZ-reduction with block-size $(\log|\Delta_{\mathbb{K}}|)^{\frac{1}{2}} \leq N$ on the lattice built from the canonical embedding $\mathcal{O}_{\mathbb{K}^+} \to \mathbb{R}^{\frac{N}{2}}$

Output: small vector $\longleftrightarrow$ algebraic integer $v \in \mathfrak{a}$

$\Longrightarrow$ ideal $\mathfrak{b} \subset \mathcal{O}_{\mathbb{K}^+}$ s.t. $\langle v \rangle = \mathfrak{a} \cdot \mathfrak{b}$ and

$$\mathcal{N}(\mathfrak{b}) \leq L_{|\Delta_{\mathbb{K}}|}\left(\tfrac{3}{2}\right)$$

Cost: DBKZ-reduction $\Rightarrow$ Poly $(N, \log \mathcal{N}(\mathfrak{a})) \cdot L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$

Smoothness tests & Randomization

Heuristic

We assume that the probability $\mathcal{P}$ that an ideal of norm bounded by $L_{|\Delta_{\mathbb{K}}|}(a)$ is a power-product of prime ideals of norm bounded by $B = L_{|\Delta_{\mathbb{K}}|}(b)$ satisfies

$$\mathcal{P} \geq L_{|\Delta_{\mathbb{K}}|}\left(a-b\right)^{-1}.$$

Using ECM algorithm, each B-smoothness test costs $L_{|\Delta_{\mathbb{K}}|}\left(\frac{b}{2}\right)$.

Smoothness tests & Randomization

Heuristic

We assume that the probability $\mathcal{P}$ that an ideal of norm bounded by $L_{|\Delta_{\mathbb{K}}|}(a)$ is a power-product of prime ideals of norm bounded by $B = L_{|\Delta_{\mathbb{K}}|}(b)$ satisfies

$$\mathcal{P} \geq L_{|\Delta_{\mathbb{K}}|}\left(a-b\right)^{-1}.$$

Using ECM algorithm, each B-smoothness test costs $L_{|\Delta_{\mathbb{K}}|}\left(\frac{b}{2}\right)$.

Conclusion: $\mathfrak{b}$ is $L_{|\Delta_{\mathbb{K}}|}(1)$-smooth with probability $L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)^{-1}$ and one test costs $L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$.

Heuristic

We assume that the probability $\mathcal{P}$ that an ideal of norm bounded by $L_{|\Delta_{\mathbb{K}}|}(a)$ is a power-product of prime ideals of norm bounded by $B = L_{|\Delta_{\mathbb{K}}|}(b)$ satisfies

$$\mathcal{P} \geq L_{|\Delta_{\mathbb{K}}|}\left(a-b\right)^{-1}.$$

Using ECM algorithm, each B-smoothness test costs $L_{|\Delta_{\mathbb{K}}|}\left(\frac{b}{2}\right)$.

Conclusion: $\mathfrak{b}$ is $L_{|\Delta_{\mathbb{K}}|}(1)$-smooth with probability $L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)^{-1}$ and one test costs $L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$.

$\Longrightarrow$ We use $L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$ ideals $\tilde{\mathfrak{a}} = \mathfrak{a}\prod \mathfrak{p}_i^{e_i}$ for small prime ideals $\mathfrak{p}_i$ and integers e_i to be sure to derive one $\tilde{\mathfrak{b}}$ that is $L_{|\Delta_{\mathbb{K}}|}(1)$-smooth.

2.2. The $\mathfrak{q}$-descent – Subsequent steps

We cannot reduce the norm using the same lattice-reduction.

2.2. The $\mathfrak{q}$-descent – Subsequent steps

We cannot reduce the norm using the same lattice-reduction.

Solution: Cheon's trick

- Use the coefficient embedding in the basis $\left(\zeta^i + \zeta^{-i}\right)_i$
- Compute the HNF of the integral lattice
- Find a short vector in a sublattice of smaller dimension

2.2. The $\mathfrak{q}$-descent – Subsequent steps

We cannot reduce the norm using the same lattice-reduction.

Solution: Cheon's trick

- Use the coefficient embedding in the basis $\left(\zeta^i + \zeta^{-i}\right)_i$
- Compute the HNF of the integral lattice
- Find a short vector in a sublattice of smaller dimension

Input: $\mathfrak{a}$ with $\mathcal{N}(\mathfrak{a}) \leq L_{|\Delta_{\mathbb{K}}|}(\alpha)$

We cannot reduce the norm using the same lattice-reduction.

Solution: Cheon's trick

- Use the coefficient embedding in the basis $\left(\zeta^i + \zeta^{-i}\right)_i$
- Compute the HNF of the integral lattice
- Find a short vector in a sublattice of smaller dimension

Input: $\mathfrak{a}$ with $\mathcal{N}(\mathfrak{a}) \leq L_{|\Delta_{\mathbb{K}}|}(\alpha)$

Output: algebraic integer $v \in \mathfrak{a}$ and ideal $\mathfrak{b} \subset \mathcal{O}_{\mathbb{K}^+}$ s.t. $\langle v \rangle = \mathfrak{a} \cdot \mathfrak{b}$ and

$$\mathcal{N}\left(\mathfrak{b}\right) \leq L_{|\Delta_{\mathbb{K}}|}\left(\tfrac{2\alpha+3}{4}\right)$$

We cannot reduce the norm using the same lattice-reduction.

Solution: Cheon's trick

- Use the coefficient embedding in the basis $\left(\zeta^i + \zeta^{-i}\right)_i$
- Compute the HNF of the integral lattice
- Find a short vector in a sublattice of smaller dimension

Input: $\mathfrak{a}$ with $\mathcal{N}(\mathfrak{a}) \leq L_{|\Delta_{\mathbb{K}}|}(\alpha)$

Output: algebraic integer $v \in \mathfrak{a}$ and ideal $\mathfrak{b} \subset \mathcal{O}_{\mathbb{K}^+}$ s.t. $\langle v \rangle = \mathfrak{a} \cdot \mathfrak{b}$ and

$$\mathcal{N}\left(\mathfrak{b}\right) \leq L_{|\Delta_{\mathbb{K}}|}\left(\tfrac{2\alpha+3}{4}\right) \qquad \rightsquigarrow L_{|\Delta_{\mathbb{K}}|}\left(\tfrac{2\alpha+1}{4}\right)\text{-smooth}$$

2.2. The $\mathfrak{q}$-descent – Subsequent steps

We cannot reduce the norm using the same lattice-reduction.

Solution: Cheon's trick

- Use the coefficient embedding in the basis $\left(\zeta^i + \zeta^{-i}\right)_i$
- Compute the HNF of the integral lattice
- Find a short vector in a sublattice of smaller dimension

Input: $\mathfrak{a}$ with $\mathcal{N}(\mathfrak{a}) \leq L_{|\Delta_{\mathbb{K}}|}(\alpha)$

Output: algebraic integer $\boldsymbol{v} \in \mathfrak{a}$ and ideal $\mathfrak{b} \subset \mathcal{O}_{\mathbb{K}^+}$ s.t. $\langle \boldsymbol{v} \rangle = \mathfrak{a} \cdot \mathfrak{b}$ and

$$\mathcal{N}(\mathfrak{b}) \leq L_{|\Delta_{\mathbb{K}}|}\left(\frac{2\alpha+3}{4}\right) \qquad \rightsquigarrow L_{|\Delta_{\mathbb{K}}|}\left(\frac{2\alpha+1}{4}\right)\text{-smooth}$$

Cost: $L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$ for lattice reduction & smoothness tests

After $l-1$ steps, ideals have norm below $L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}+\frac{1}{2^l}\right)$.

After $l-1$ steps, ideals have norm below $L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}+\frac{1}{2^l}\right)$.

For $l = \lceil \log_2(\log N) \rceil$, we have

$$L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}+\frac{1}{2^l}\right) \leq L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}+\frac{1}{\log N}\right) = L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right).$$

After $l-1$ steps, ideals have norm below $L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}+\frac{1}{2^l}\right)$.

For $l=\lceil \log_2(\log N) \rceil$, we have

$$L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}+\frac{1}{2^l}\right) \leq L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}+\frac{1}{\log N}\right) = L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right).$$

Conclusion:

- All ideals have norm below $L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$

After $l-1$ steps, ideals have norm below $L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}+\frac{1}{2^l}\right)$.

For $l = \lceil \log_2(\log N) \rceil$, we have

$$L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}+\frac{1}{2^l}\right) \leq L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}+\frac{1}{\log N}\right) = L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right).$$

Conclusion:

- All ideals have norm below $L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$
- They are at most $N^l \ll L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$ ideals

2.3. The $\mathfrak{q}$-descent – The final step

After $l-1$ steps, ideals have norm below $L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}+\frac{1}{2^l}\right)$.

For $l = \lceil \log_2(\log N) \rceil$, we have

$$L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}+\frac{1}{2^l}\right) \leq L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}+\frac{1}{\log N}\right) = L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right).$$

Conclusion:

- All ideals have norm below $L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$
- They are at most $N^l \ll L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$ ideals
- The total runtime of the $\mathfrak{q}$-descent is $L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$.

3. Solution for smooth ideals

Input: Bunch of prime ideals of norm below $B = L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$

3. Solution for smooth ideals

Input: Bunch of prime ideals of norm below $B = L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$

Index Calculus Method:

- Factor base: set of all prime ideals with norm below B

Input: Bunch of prime ideals of norm below $B = L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$

Index Calculus Method:

- Factor base: set of all prime ideals with norm below B
- Relation collection: construction of a full-rank matrix M

3. Solution for smooth ideals

Input: Bunch of prime ideals of norm below $B = L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$

Index Calculus Method:

- Factor base: set of all prime ideals with norm below B
- Relation collection: construction of a full-rank matrix M

  Relation: principal ideal that splits on the factor base. Test ideals generated by $\boldsymbol{v} = \sum v_i(\zeta^i + \zeta^{-i})$ for $|v_i| \leq \log|\Delta_{\mathbb{K}}|$.

3. Solution for smooth ideals

Input: Bunch of prime ideals of norm below $B = L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$

Index Calculus Method:

- Factor base: set of all prime ideals with norm below B
- Relation collection: construction of a full-rank matrix M

  Relation: principal ideal that splits on the factor base. Test ideals generated by $\boldsymbol{v} = \sum v_i(\zeta^i + \zeta^{-i})$ for $|v_i| \leq \log|\Delta_{\mathbb{K}}|$.

  Norm below $L_{|\Delta_{\mathbb{K}}|}(1) \Longrightarrow L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$-smooth ideals in $L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$.

Input: Bunch of prime ideals of norm below $B = L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$

Index Calculus Method:

- Factor base: set of all prime ideals with norm below B
- Relation collection: construction of a full-rank matrix M

$$\begin{pmatrix} \boldsymbol{v}_1 \\ \boldsymbol{v}_2 \\ \vdots \\ \boldsymbol{v}_{Q|\mathcal{B}|} \end{pmatrix} \begin{matrix} \rightarrow \\ \rightarrow \\ \vdots \\ \rightarrow \end{matrix} \begin{pmatrix} M_{1,1} & \cdots & M_{1,|\mathcal{B}|} \\ M_{2,1} & \cdots & M_{2,|\mathcal{B}|} \\ \vdots & & \vdots \\ M_{Q|\mathcal{B}|,1} & \cdots & M_{Q|\mathcal{B}|,|\mathcal{B}|} \end{pmatrix} \Longrightarrow \forall i, \langle \boldsymbol{v}_i \rangle = \prod_{j=1}^{|\mathcal{B}|} \mathfrak{p}_j^{M_{i,j}}$$

Input: Bunch of prime ideals of norm below $B = L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$

Index Calculus Method:

- Factor base: set of all prime ideals with norm below B
- Relation collection: construction of a full-rank matrix M
- A N-dimensional vector Y including all the valuations of the smooth ideals in the $\mathfrak{p}_i$

3. Solution for smooth ideals

Input: Bunch of prime ideals of norm below $B = L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$

Index Calculus Method:

- Factor base: set of all prime ideals with norm below B
- Relation collection: construction of a full-rank matrix M
- A N-dimensional vector Y including all the valuations of the smooth ideals in the $\mathfrak{p}_i$
- A solution X of $MX = Y$ provides a generator of the product of the $L_{|\Delta_{\mathbb{K}}|}\left(\frac{1}{2}\right)$-smooth ideals

Implementation results

`PARI-GP` and `fplll` for BKZ-reductions — Intel(R) Xeon(R) CPU E3-1275 v3 @ 3.50GHz with 32GB of memory

Dimension of the field: $N = 2^8 = 256$.

Implementation results

`PARI-GP` and `fplll` for BKZ-reductions — Intel(R) Xeon(R) CPU E3-1275 v3 @ 3.50GHz with 32GB of memory

Dimension of the field: $N = 2^8 = 256$.

- Gentry-Szydlo: 20h and 24GB memory

Implementation results

`PARI-GP` and `fplll` for BKZ-reductions — Intel(R) Xeon(R) CPU E3-1275 v3 @ 3.50GHz with 32GB of memory

Dimension of the field: $N = 2^8 = 256$.

- Gentry-Szydlo: 20h and 24GB memory
- BKZ-reduction: between 10 min and 4h
  (Descent reduced to only one step)

Implementation results

`PARI-GP` and `fplll` for BKZ-reductions — Intel(R) Xeon(R) CPU E3-1275 v3 @ 3.50GHz with 32GB of memory

Dimension of the field: $N = 2^8 = 256$.

- Gentry-Szydlo: 20h and 24GB memory
- BKZ-reduction: between 10 min and 4h
  (Descent reduced to only one step)

We recover $\boldsymbol{g} \cdot \zeta^i$ — and so the secret key $\boldsymbol{g}$ — in less than a day.

Thanks

Thank you