Short Stickelberger Class Relations and application to Ideal-SVP

Ronald Cramer Léo Ducas Benjamin Wesolowski

Leiden University, The Netherlands

CWI, Amsterdam, The Netherlands

EPFL, Lausanne, Switzerland

Spring School on Lattice-Based Cryptography
Oxford, March 2017

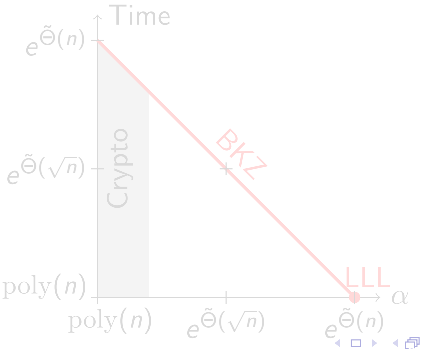
Lattice-Based Crypto

Lattice problems provides a strong fundation for Post-Quantum Crypto

Worst-case to average-case reduction [Ajtai, 1999, Regev, 2009]

$$\text{Worst-case Approx-SVP} \geq \begin{cases} \text{SIS} & \text{(Short Intreger Solution)} \\ \text{LWE} & \text{(Learning With Error)} \end{cases}$$

How hard is Approx-SVP ? Depends on the Approximation factor α.



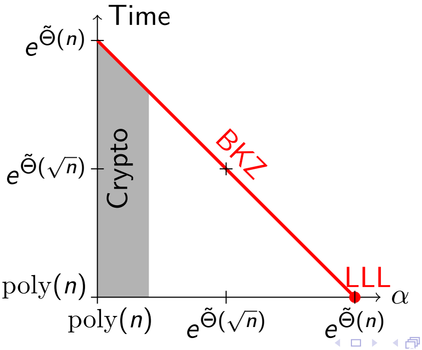
Lattice-Based Crypto

Lattice problems provides a strong fundation for Post-Quantum Crypto

Worst-case to average-case reduction [Ajtai, 1999, Regev, 2009]

$$\text{Worst-case Approx-SVP} \geq \begin{cases} \text{SIS} & \text{(Short Intreger Solution)} \\ \text{LWE} & \text{(Learning With Error)} \end{cases}$$

How hard is Approx-SVP ? Depends on the Approximation factor α.



Lattices over Rings (Ideals, Modules)

Generic lattices are cumbersome! Key-size $= \tilde{O}(n^2)$.

NTRU Cryptosystems [Hoffstein et al., 1998, Hoffstein et al., 2003]

Use the convolution ring $\mathcal{R} = R[X]/(X^p - 1)$, and module-lattices:

$$\mathcal{L}_h = \{(x, y) \in \mathcal{R}^2, \quad hx + y \equiv 0 \bmod q\}.$$

Same lattice dimension, Key-Size $= \tilde{O}(n)$. Later came variants with worst-case fundations:

wc-to-ac reduction [Micciancio, 2007, Lyubashevsky et al., 2013]

$$\text{Worst-case Approx-Ideal-SVP} \geq \begin{cases} \text{Ring-SIS} \\ \text{Ring-LWE} \end{cases}$$

Applicable for cyclotomic rings $\mathcal{R} = \mathbb{Z}[\omega_m]$ (ω_m a primitive m-th root of unity).

Denote $n = \deg \mathcal{R}$. In our cyclotomic cases: $n = \phi(m) \sim m$.

Lattices over Rings (Ideals, Modules)

Generic lattices are cumbersome! Key-size $= \tilde{O}(n^2)$.

NTRU Cryptosystems [Hoffstein et al., 1998, Hoffstein et al., 2003]

Use the convolution ring $\mathcal{R} = R[X]/(X^p - 1)$, and module-lattices:

$$\mathcal{L}_h = \{(x, y) \in \mathcal{R}^2, \quad hx + y \equiv 0 \bmod q\}.$$

Same lattice dimension, Key-Size $= \tilde{O}(n)$. Later came variants with worst-case fundations:

wc-to-ac reduction [Micciancio, 2007, Lyubashevsky et al., 2013]

$$\text{Worst-case Approx-Ideal-SVP} \geq \begin{cases} \text{Ring-SIS} \\ \text{Ring-LWE} \end{cases}$$

Applicable for cyclotomic rings $\mathcal{R} = \mathbb{Z}[\omega_m]$ (ω_m a primitive m-th root of unity).

Denote $n = \deg \mathcal{R}$. In our cyclotomic cases: $n = \phi(m) \sim m$.

Lattices over Rings (Ideals, Modules)

Generic lattices are cumbersome! Key-size $= \tilde{O}(n^2)$.

NTRU Cryptosystems [Hoffstein et al., 1998, Hoffstein et al., 2003]

Use the convolution ring $\mathcal{R} = R[X]/(X^p - 1)$, and module-lattices:

$$\mathcal{L}_h = \{(x, y) \in \mathcal{R}^2, \quad hx + y \equiv 0 \bmod q\}.$$

Same lattice dimension, Key-Size $= \tilde{O}(n)$. Later came variants with worst-case fundations:

wc-to-ac reduction [Micciancio, 2007, Lyubashevsky et al., 2013]

$$\text{Worst-case Approx-Ideal-SVP} \geq \begin{cases} \text{Ring-SIS} \\ \text{Ring-LWE} \end{cases}$$

Applicable for cyclotomic rings $\mathcal{R} = \mathbb{Z}[\omega_m]$ (ω_m a primitive m-th root of unity).

Denote $n = \deg \mathcal{R}$. In our cyclotomic cases: $n = \phi(m) \sim m$.

Is Ideal-SVP as hard as general SVP ?

Are there other approach than lattice reduction (LLL,BKZ) ?
An algebraic approach was sketched in [Campbell et al., 2014]:

The Principal Ideal Problem (PIP)

Given a **principal ideal** $\mathfrak{h}$, recover a generator h s.t. $h\mathcal{R} = \mathfrak{h}$.

Solvable in quantum poly-time [Biasse and Song, 2016].

The Short Generator Problem (SGP)

Given a generator h, recover another **short** generator g s.t. $g\mathcal{R} = h\mathcal{R}$.

Also **solvable** in classical poly-time [Cramer et al., 2016] for $m = p^k, \mathcal{R} = \mathbb{Z}[\omega_m], \alpha = \exp(\tilde{O}(\sqrt{n}))$.

Is Ideal-SVP as hard as general SVP ?

Are there other approach than lattice reduction (LLL,BKZ) ?
An algebraic approach was sketched in [Campbell et al., 2014]:

The Principal Ideal Problem (PIP)

Given a **principal ideal** $\mathfrak{h}$, recover a generator h s.t. $h\mathcal{R} = \mathfrak{h}$.

Solvable in quantum poly-time [Biasse and Song, 2016].

The Short Generator Problem (SGP)

Given a generator h, recover another **short** generator g s.t. $g\mathcal{R} = h\mathcal{R}$.

Also **solvable** in classical poly-time [Cramer et al., 2016] for $m = p^k, \mathcal{R} = \mathbb{Z}[\omega_m], \alpha = \exp(\tilde{O}(\sqrt{n}))$.

Is Ideal-SVP as hard as general SVP ?

Are there other approach than lattice reduction (LLL,BKZ) ?
An algebraic approach was sketched in [Campbell et al., 2014]:

The Principal Ideal Problem (PIP)

Given a **principal ideal** $\mathfrak{h}$, recover a generator h s.t. $h\mathcal{R} = \mathfrak{h}$.

Solvable in quantum poly-time [Biasse and Song, 2016].

The Short Generator Problem (SGP)

Given a generator h, recover another **short** generator g s.t. $g\mathcal{R} = h\mathcal{R}$.

Also **solvable** in classical poly-time [Cramer et al., 2016] for $m = p^k, \mathcal{R} = \mathbb{Z}[\omega_m], \alpha = \exp(\tilde{O}(\sqrt{n}))$.

Are Ideal-SVP and Ring-LWE broken ?!

Not quite yet ! 3 serious obstacle remains:

(i) Restricted to **principal** ideals.

(ii) The approximation factor in **too large** to affect Crypto.

(iii) Ring-LWE $\geq$ Ideal-SVP, but **equivalence is not known**.

Approaches ?

(i) Solving the **Close Principal Multiple** problem (CPM) [**This work !**]

(ii) Considering many CPM solutions [Plausible]

(iii) Generalization of LLL to **non-euclidean** rings [Seems tough]

Are Ideal-SVP and Ring-LWE broken ?!

Not quite yet ! 3 serious obstacle remains:

(i) Restricted to **principal** ideals.

(ii) The approximation factor in **too large** to affect Crypto.

(iii) Ring-LWE $\geq$ Ideal-SVP, but **equivalence is not known**.

Approaches ?

(i) Solving the **Close Principal Multiple** problem (CPM) [**This work !**]

(ii) Considering many CPM solutions [Plausible]

(iii) Generalization of LLL to **non-euclidean** rings [Seems tough]

Our result: Ideal-SVP in poly-time for large α

This work: CPM via Stickelberger Short Class Relation

$\Rightarrow$ Ideal-SVP **solvable** in Quantum poly-time, for

$$\mathcal{R} = \mathbb{Z}[\omega_m], \quad \alpha = \exp(\tilde{O}(\sqrt{n})).$$

Better tradeoffs

Impact and limitations

- No schemes broken
- **Hardness gap** between SVP and Ideal-SVP
- New cryptanalytic tools

$\Rightarrow$ start favoring **weaker assumptions** ?
e.g. Module-LWE
[Langlois and Stehlé, 2015]

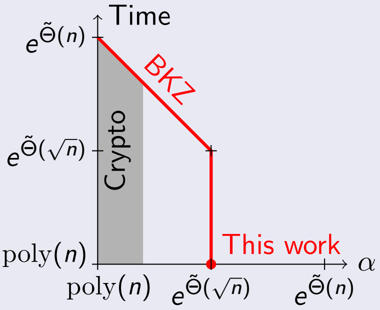
Our result: Ideal-SVP in poly-time for large α

This work: CPM via Stickelberger Short Class Relation

$\Rightarrow$ Ideal-SVP **solvable** in Quantum poly-time, for

$$\mathcal{R} = \mathbb{Z}[\omega_m], \quad \alpha = \exp(\tilde{O}(\sqrt{n})).$$

Better tradeoffs



Impact and limitations

- No schemes broken
- **Hardness gap** between SVP and Ideal-SVP
- New cryptanalytic tools

$\Rightarrow$ start favoring **weaker assumptions** ?
e.g. Module-LWE
[Langlois and Stehlé, 2015]

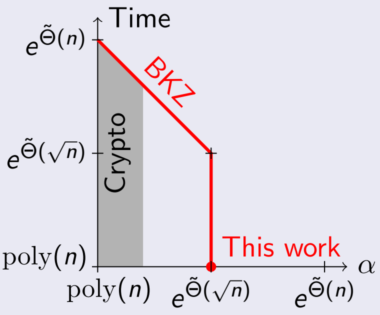
Our result: Ideal-SVP in poly-time for large α

This work: CPM via Stickelberger Short Class Relation

$\Rightarrow$ Ideal-SVP **solvable** in Quantum poly-time, for

$$\mathcal{R} = \mathbb{Z}[\omega_m], \quad \alpha = \exp(\tilde{O}(\sqrt{n})).$$

Better tradeoffs



Impact and limitations

- No schemes broken
- **Hardness gap** between SVP and Ideal-SVP
- New cryptanalytic tools

$\Rightarrow$ start favoring **weaker assumptions** ?
e.g. Module-LWE
[Langlois and Stehlé, 2015]

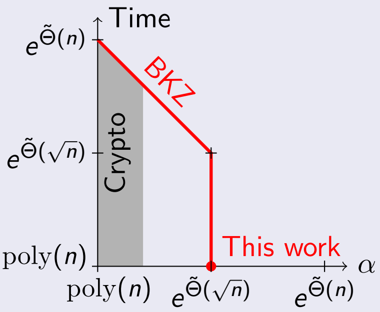
Our result: Ideal-SVP in poly-time for large α

This work: CPM via Stickelberger Short Class Relation

$\Rightarrow$ Ideal-SVP **solvable** in Quantum poly-time, for

$$\mathcal{R} = \mathbb{Z}[\omega_m], \quad \alpha = \exp(\tilde{O}(\sqrt{n})).$$

Better tradeoffs



Impact and limitations

- No schemes broken
- **Hardness gap** between SVP and Ideal-SVP
- New cryptanalytic tools

$\Rightarrow$ start favoring **weaker assumptions** ?
e.g. Module-LWE [Langlois and Stehlé, 2015]

Table of Contents

1 Introduction

2 Ideals, Principal Ideals and the Class Group

3 Solving CPM: Navigating the Class Group

4 Short Stickelberger Class Relations

5 Bibliography

Table of Contents

1 Introduction

2 Ideals, Principal Ideals and the Class Group

3 Solving CPM: Navigating the Class Group

4 Short Stickelberger Class Relations

5 Bibliography

Ideals and Principal Ideals

Cyclotomic number field: $K (= \mathbb{Q}(\omega_m))$, ring of integer $\mathcal{O}_K (= \mathbb{Z}[\omega_m])$.

Definition (Ideals)

- An **integral ideal** is a subset $\mathfrak{h} \subset \mathcal{O}_K$ closed under addition, and by multiplication by elements of $\mathcal{O}_K$,
- A **(fractional) ideal** is a subset $\mathfrak{f} \subset K$ of the form $\mathfrak{f} = \frac{1}{x}\mathfrak{h}$, where $x \in \mathbb{Z}$,
- A **principal ideal** is an ideal $\mathfrak{f}$ of the form $\mathfrak{f} = g\mathcal{O}_K$ for some $g \in K$.

In particular, ideals are lattices.

We denote $\mathcal{F}_K$ the set of fractional ideal,
and $\mathcal{P}_K$ the set of principal ideals.

Class Group

Ideals can be multiplied, and remain ideals:

$$\mathfrak{a}\mathfrak{b} = \left\{ \sum_{\text{finite}} a_i b_i, \quad a_i \in \mathfrak{a}, b_i \in \mathfrak{b} \right\}.$$

The product of two principal ideals remains principal:

$$(a\mathcal{O}_K)(b\mathcal{O}_K) = (ab)\mathcal{O}_K.$$

$\mathcal{F}_K$ form an **abelian group**[1], $\mathcal{P}_K$ is a **subgroup** of it.

Definition (Class Group)

Their quotient form the **class group** $\mathrm{Cl}_K = \mathcal{F}_K / \mathcal{P}_K$.
The class of a ideal $\mathfrak{a} \in \mathcal{F}_K$ is denoted $[\mathfrak{a}] \in \mathrm{Cl}_K$.

An ideal $\mathfrak{a}$ is principal iff $[\mathfrak{a}] = [\mathcal{O}_K]$.

[1] with neutral element $\mathcal{O}_K$

Class Group

Ideals can be multiplied, and remain ideals:

$$\mathfrak{a}\mathfrak{b} = \left\{ \sum_{\text{finite}} a_i b_i, \quad a_i \in \mathfrak{a}, b_i \in \mathfrak{b} \right\}.$$

The product of two principal ideals remains principal:

$$(a\mathcal{O}_K)(b\mathcal{O}_K) = (ab)\mathcal{O}_K.$$

$\mathcal{F}_K$ form an **abelian group**[1], $\mathcal{P}_K$ is a **subgroup** of it.

Definition (Class Group)

Their quotient form the **class group** $\mathrm{Cl}_K = \mathcal{F}_K / \mathcal{P}_K$.
The class of a ideal $\mathfrak{a} \in \mathcal{F}_K$ is denoted $[\mathfrak{a}] \in \mathrm{Cl}_K$.

An ideal $\mathfrak{a}$ is principal iff $[\mathfrak{a}] = [\mathcal{O}_K]$.

[1] with neutral element $\mathcal{O}_K$

Table of Contents

1 Introduction

2 Ideals, Principal Ideals and the Class Group

3 Solving CPM: Navigating the Class Group

4 Short Stickelberger Class Relations

5 Bibliography

From CPM to Ideal-SVP

Definition (The Close Principal Multiple problem)

- Given an ideal $\mathfrak{a}$, and an factor F
- Find a **small integral** ideal $\mathfrak{b}$ such that $[\mathfrak{a}\mathfrak{b}] = [\mathcal{O}_K]$ and $N\mathfrak{b} \leq F$

Note: Smallness with respect to the Algebraic Norm N of $\mathfrak{b}$,
(essentially the **volume** of $\mathfrak{b}$ as a lattice).

- Solve CPM, and apply the previous results (PIP-SGP) to $\mathfrak{a}\mathfrak{b}$
- This will give a generator g of $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a}$ (so $g \in \mathfrak{a}$) of length

$$L = N(\mathfrak{a}\mathfrak{b})^{1/n} \cdot \exp(\tilde{O}(\sqrt{n}))$$

- This Ideal-SVP solution has an approx factor of

$$\alpha \approx L/N(\mathfrak{a}) = F^{1/n} \cdot \exp(\tilde{O}(\sqrt{n}))$$

CPM with $F = \exp(\tilde{O}(n^{3/2}))$ $\Rightarrow$ Ideal-SVP with $\alpha = \exp(\tilde{O}(\sqrt{n}))$

From CPM to Ideal-SVP

Definition (The Close Principal Multiple problem)

- Given an ideal $\mathfrak{a}$, and an factor F
- Find a **small integral** ideal $\mathfrak{b}$ such that $[\mathfrak{a}\mathfrak{b}] = [\mathcal{O}_K]$ and $N\mathfrak{b} \leq F$

Note: Smallness with respect to the Algebraic Norm N of $\mathfrak{b}$, (essentially the **volume** of $\mathfrak{b}$ as a lattice).

- Solve CPM, and apply the previous results (PIP-SGP) to $\mathfrak{a}\mathfrak{b}$
- This will give a generator g of $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a}$ (so $g \in \mathfrak{a}$) of length

$$L = N(\mathfrak{a}\mathfrak{b})^{1/n} \cdot \exp(\tilde{O}(\sqrt{n}))$$

- This Ideal-SVP solution has an approx factor of

$$\alpha \approx L/N(\mathfrak{a}) = F^{1/n} \cdot \exp(\tilde{O}(\sqrt{n}))$$

CPM with $F = \exp(\tilde{O}(n^{3/2}))$ $\Rightarrow$ Ideal-SVP with $\alpha = \exp(\tilde{O}(\sqrt{n}))$

From CPM to Ideal-SVP

Definition (The Close Principal Multiple problem)

- Given an ideal $\mathfrak{a}$, and an factor F
- Find a **small integral** ideal $\mathfrak{b}$ such that $[\mathfrak{a}\mathfrak{b}] = [\mathcal{O}_K]$ and $N\mathfrak{b} \leq F$

Note: Smallness with respect to the Algebraic Norm N of $\mathfrak{b}$,
(essentially the **volume** of $\mathfrak{b}$ as a lattice).

- Solve CPM, and apply the previous results (PIP-SGP) to $\mathfrak{a}\mathfrak{b}$
- This will give a generator g of $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a}$ (so $g \in \mathfrak{a}$) of length

$$L = N(\mathfrak{a}\mathfrak{b})^{1/n} \cdot \exp(\tilde{O}(\sqrt{n}))$$

- This Ideal-SVP solution has an approx factor of

$$\alpha \approx L/N(\mathfrak{a}) = F^{1/n} \cdot \exp(\tilde{O}(\sqrt{n}))$$

CPM with $F = \exp(\tilde{O}(n^{3/2})) \quad \Rightarrow \quad$ Ideal-SVP with $\alpha = \exp(\tilde{O}(\sqrt{n}))$

Factor Basis, Class-Group Discrete-Log

Choose a **factor basis** $\mathfrak{B}$ of integral ideals and search $\mathfrak{b}$ of the form:

$$\mathfrak{b} = \prod_{\mathfrak{p} \in \mathfrak{B}} \mathfrak{p}^{e_\mathfrak{p}}.$$

Theorem (Quantum Cl-DL, Corollary of [Biasse and Song, 2016])

Assume $\mathfrak{B}$ generates the class-group. Given $\mathfrak{a}$ and $\mathfrak{B}$, one can find in quantum polynomial time a vector $\vec{e} \in \mathbb{Z}^{\mathfrak{B}}$ such that:

$$\prod_{\mathfrak{p} \in \mathfrak{B}} \left[\mathfrak{p}^{e_\mathfrak{p}}\right] = \left[\mathfrak{a}^{-1}\right].$$

This finds a $\mathfrak{b}$ such that $[\mathfrak{a}\mathfrak{b}] = [\mathcal{O}_K]$, yet:

- $\mathfrak{b}$ may not be integral (negative exponents, yet easy to solve)
- $N\mathfrak{b} \approx \exp(\|\vec{e}\|_1)$ may be huge (unbounded $\vec{e}$, want $\|\vec{e}\|_1 = \tilde{O}(n^{3/2})$).

Factor Basis, Class-Group Discrete-Log

Choose a **factor basis** $\mathfrak{B}$ of integral ideals and search $\mathfrak{b}$ of the form:

$$\mathfrak{b} = \prod_{\mathfrak{p} \in \mathfrak{B}} \mathfrak{p}^{e_\mathfrak{p}}.$$

Theorem (Quantum Cl-DL, Corollary of [Biasse and Song, 2016])

Assume $\mathfrak{B}$ generates the class-group. Given $\mathfrak{a}$ and $\mathfrak{B}$, one can find in quantum polynomial time a vector $\vec{e} \in \mathbb{Z}^{\mathfrak{B}}$ such that:

$$\prod_{\mathfrak{p} \in \mathfrak{B}} \left[\mathfrak{p}^{e_\mathfrak{p}}\right] = \left[\mathfrak{a}^{-1}\right].$$

This finds a $\mathfrak{b}$ such that $[\mathfrak{a}\mathfrak{b}] = [\mathcal{O}_K]$, yet:

- $\mathfrak{b}$ may not be integral (negative exponents, yet easy to solve)
- $N\mathfrak{b} \approx \exp(\|\vec{e}\|_1)$ may be huge (unbounded $\vec{e}$, want $\|\vec{e}\|_1 = \tilde{O}(n^{3/2})$).

Factor Basis, Class-Group Discrete-Log

Choose a **factor basis** $\mathfrak{B}$ of integral ideals and search $\mathfrak{b}$ of the form:

$$\mathfrak{b} = \prod_{\mathfrak{p} \in \mathfrak{B}} \mathfrak{p}^{e_\mathfrak{p}}.$$

Theorem (Quantum Cl-DL, Corollary of [Biasse and Song, 2016])

Assume $\mathfrak{B}$ generates the class-group. Given $\mathfrak{a}$ and $\mathfrak{B}$, one can find in quantum polynomial time a vector $\vec{e} \in \mathbb{Z}^{\mathfrak{B}}$ such that:

$$\prod_{\mathfrak{p} \in \mathfrak{B}} \left[\mathfrak{p}^{e_\mathfrak{p}}\right] = \left[\mathfrak{a}^{-1}\right].$$

This finds a $\mathfrak{b}$ such that $[\mathfrak{a}\mathfrak{b}] = [\mathcal{O}_K]$, yet:

- $\mathfrak{b}$ may not be integral (negative exponents, yet easy to solve)
- $N\mathfrak{b} \approx \exp(\|\vec{e}\|_1)$ may be huge (unbounded $\vec{e}$, want $\|\vec{e}\|_1 = \tilde{O}(n^{3/2})$).

Navigating the Class-Group

Cayley-Graph(G, A):

- A node for any element $g \in G$
- An arrow $g \xrightarrow{a} ga$ for any $g \in G$, $a \in A$

Figure: Cayley-Graph$((\mathbb{Z}/5\mathbb{Z}, +)$,$\{1$,$2\})$

Rephrased Goal for CPM

Find a **short** path from $[\mathfrak{a}]$ to $[\mathcal{O}_K]$ in Cayley-Graph$(\mathrm{Cl}, \mathfrak{B})$.

- Using a few well chosen ideals in $\mathfrak{B}$, Cayley-Graph$(\mathrm{Cl}, \mathfrak{B})$ is an **expander Graph** [Jetchev and Wesolowski, 2015]: very short path exists.
- Finding such short path generically too costly: $|\mathrm{Cl}| > \exp(n)$

A lattice problem

Cl is **abelian** and **finite**, so $\mathrm{Cl} = \mathbb{Z}^{\mathfrak{B}}/\Lambda$ for some lattice Λ:

$$\Lambda = \left\{ \vec{e} \in \mathbb{Z}^{\mathfrak{B}}, \quad s.t. \prod [\mathfrak{p}_{\mathfrak{p}}^{e}] = [\mathcal{O}_K] \right\}$$

i.e. the (full-rank) **lattice of class-relations** in base $\mathfrak{B}$.

Figure: $(\mathbb{Z}/5\mathbb{Z}, +) = \mathbb{Z}^{\{1,2\}}/\Lambda$

Rephrased Goal for CPM: CVP in Λ

Find a **short** path from $t \in \mathbb{Z}^{\mathfrak{B}}$ to any lattice point $v \in \Lambda$.

In general: very hard. But for good Λ, with a good basis, can be easy.

Why should we know anything special about Λ ?

A lattice problem

Cl is **abelian** and **finite**, so $\mathrm{Cl} = \mathbb{Z}^{\mathfrak{B}}/\Lambda$ for some lattice Λ:

$$\Lambda = \left\{ \vec{e} \in \mathbb{Z}^{\mathfrak{B}}, \quad s.t. \prod [\mathfrak{p}_{\mathfrak{p}}^{e}] = [\mathcal{O}_K] \right\}$$

i.e. the (full-rank) **lattice of class-relations** in base $\mathfrak{B}$.

Figure: $(\mathbb{Z}/5\mathbb{Z}, +) = \mathbb{Z}^{\{1,2\}}/\Lambda$

Rephrased Goal for CPM: CVP in Λ

Find a **short** path from $t \in \mathbb{Z}^{\mathfrak{B}}$ to any lattice point $v \in \Lambda$.

In general: very hard. But for good Λ, with a good basis, can be easy.

Why should we know anything special about Λ ?

Example

Figure: Cayley-Graph$(\mathbb{Z}/5\mathbb{Z}, \{1, 2\}) \quad \simeq \quad \mathbb{Z}^{\{1,2\}}/\Lambda$

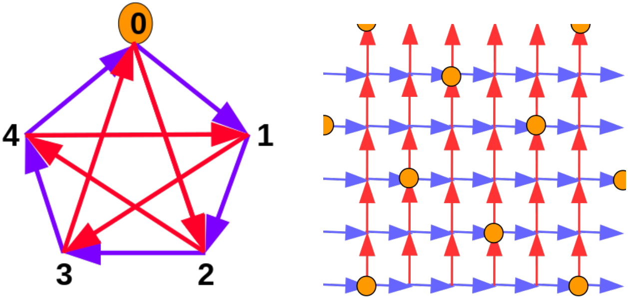


Table of Contents

1 Introduction

2 Ideals, Principal Ideals and the Class Group

3 Solving CPM: Navigating the Class Group

4 Short Stickelberger Class Relations

5 Bibliography

More than just a lattice

Let G denote the Galois group, it acts on ideals and therefore on classes:

$$[\mathfrak{a}]^{\sigma} = [\sigma(\mathfrak{a})].$$

Consider the **group-ring** $\mathbb{Z}[G]$ (formal sums on G), extend the G-action:

$$[\mathfrak{a}]^{e} = \prod_{\sigma \in G} [\sigma(\mathfrak{a})]^{e_\sigma} \qquad \text{where } e = \sum e_\sigma \sigma.$$

- Assume $\mathfrak{B} = \{\mathfrak{p}^{\sigma}, \sigma \in G\}$
- G acts on $\mathfrak{B}$, and so it acts on $\mathbb{Z}^{\mathfrak{B}}$ by permuting coordinates
- the lattice $\Lambda \subset \mathbb{Z}^{\mathfrak{B}}$ is **invariant** by the action of G !

i.e. Λ admits G as a group of **symmetries**

Λ is more than just a lattice: it is a $\mathbb{Z}[G]$-**module**

More than just a lattice

Let G denote the Galois group, it acts on ideals and therefore on classes:

$$[\mathfrak{a}]^\sigma = [\sigma(\mathfrak{a})].$$

Consider the **group-ring** $\mathbb{Z}[G]$ (formal sums on G), extend the G-action:

$$[\mathfrak{a}]^e = \prod_{\sigma \in G} [\sigma(\mathfrak{a})]^{e_\sigma} \qquad \text{where } e = \sum e_\sigma \sigma.$$

- Assume $\mathfrak{B} = \{\mathfrak{p}^\sigma, \sigma \in G\}$
- G acts on $\mathfrak{B}$, and so it acts on $\mathbb{Z}^{\mathfrak{B}}$ by permuting coordinates
- the lattice $\Lambda \subset \mathbb{Z}^{\mathfrak{B}}$ is **invariant** by the action of G !

i.e. Λ admits G as a group of **symmetries**

Λ is more than just a lattice: it is a $\mathbb{Z}[G]$-**module**

More than just a lattice

Let G denote the Galois group, it acts on ideals and therefore on classes:

$$[\mathfrak{a}]^\sigma = [\sigma(\mathfrak{a})].$$

Consider the **group-ring** $\mathbb{Z}[G]$ (formal sums on G), extend the G-action:

$$[\mathfrak{a}]^e = \prod_{\sigma \in G} [\sigma(\mathfrak{a})]^{e_\sigma} \qquad \text{where } e = \sum e_\sigma \sigma.$$

- Assume $\mathfrak{B} = \{\mathfrak{p}^\sigma, \sigma \in G\}$
- G acts on $\mathfrak{B}$, and so it acts on $\mathbb{Z}^{\mathfrak{B}}$ by permuting coordinates
- the lattice $\Lambda \subset \mathbb{Z}^{\mathfrak{B}}$ is **invariant** by the action of G !

i.e. Λ admits G as a group of **symmetries**

Λ is more than just a lattice: it is a $\mathbb{Z}[G]$-**module**

More than just a lattice

Let G denote the Galois group, it acts on ideals and therefore on classes:

$$[\mathfrak{a}]^\sigma = [\sigma(\mathfrak{a})].$$

Consider the **group-ring** $\mathbb{Z}[G]$ (formal sums on G), extend the G-action:

$$[\mathfrak{a}]^e = \prod_{\sigma \in G} [\sigma(\mathfrak{a})]^{e_\sigma} \qquad \text{where } e = \sum e_\sigma \sigma.$$

- Assume $\mathfrak{B} = \{\mathfrak{p}^\sigma, \sigma \in G\}$
- G acts on $\mathfrak{B}$, and so it acts on $\mathbb{Z}^{\mathfrak{B}}$ by permuting coordinates
- the lattice $\Lambda \subset \mathbb{Z}^{\mathfrak{B}}$ is **invariant** by the action of G !

i.e. Λ admits G as a group of **symmetries**

Λ is more than just a lattice: it is a $\mathbb{Z}[G]$-**module**

Stickelberger's Theorem

In fact, we know much more about Λ !

Definition (The Stickelberger ideal)

The **Stickelberger element** $\theta \in \mathbb{Q}[G]$ is defined as

$$\theta = \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^*} \left(\frac{a}{m} \bmod 1 \right) \sigma_a^{-1} \qquad \text{where } G \ni \sigma_a : \omega \mapsto \omega^a.$$

The **Stickelberger ideal** is defined as $S = \mathbb{Z}[G] \cap \theta\mathbb{Z}[G]$.

Theorem (Stickelberger's theorem [Washington, 2012, Thm. 6.10])

The Stickelberger ideal annihilates the class group: $\forall e \in S, \mathfrak{a} \subset K$

$$[\mathfrak{a}^e] = [\mathcal{O}_K].$$

In particular, if $\mathfrak{B} = \{\mathfrak{p}^\sigma, \sigma \in G\}$*, then* $S \subset \Lambda$.

Geometry of the Stickelberger ideal

Fact

There exists an **explicit** *(efficiently computable)* **short** *basis of S, precisely it has binary coefficients.*

Corollary

Given $t \in \mathbb{Z}[G]$, one ca find $x \in S$ suh that $\|x - t\|_1 \leq n^{3/2}$.

Conclusion: back to CPM

The CPM problem can be solved with approx. factor $F = \exp(\tilde{O}(n^{3/2}))$.
QED.

Extra technicalities

Convenient simplifications/omissions made so far:

$\mathfrak{B} = \{\mathfrak{p}^\sigma, \sigma \in G\}$ generates the class group.

- can allow a few (say polylog) many different ideals and their conjugates in $\mathfrak{B}$
- Numerical computation says such $\mathfrak{B}$ it should exists [Schoof, 1998]
- Theorem+Heuristic then says we can find such $\mathfrak{B}$ efficiently

Eliminating minus exponents

- Easy when $h^+ = 1$: $[\mathfrak{a}^{-1}] = [\bar{\mathfrak{a}}]$, doable when $h^+ = \mathrm{poly}(n)$
  h^+ is the size of the class group of K^+, the maximal totally real subfield of K
- $h^+ = \mathrm{poly}(n)$ already needed for previous result [Cramer et al., 2016]
- Justified by numerical computations and heuristics [Buhler et al., 2004, Schoof, 2003]

Open questions

Obstacle toward attacks Ring-LWE

(i) Restricted to **principal** ideals.

(ii) The approximation factor in **too large** to affect Crypto.

(iii) Ring-LWE $\geq$ Ideal-SVP, but **equivalence is not known**.

Open questions

Obstacle toward attacks Ring-LWE

(i) ~~Restricted to **principal** ideals.~~

(ii) The approximation factor in **too large** to affect Crypto.

(iii) Ring-LWE $\geq$ Ideal-SVP, but **equivalence is not known**.

References I

Ajtai, M. (1999).
Generating hard instances of the short basis problem.
In *ICALP*, pages 1–9.

Biasse, J.-F. and Song, F. (2016).
Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields.
In *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 893–902. SIAM.

Buhler, J., Pomerance, C., and Robertson, L. (2004).
Heuristics for class numbers of prime-power real cyclotomic fields,.
In *High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams*, Fields Inst. Commun., pages 149–157. Amer. Math. Soc.

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`.

References II

Cramer, R., Ducas, L., Peikert, C., and Regev, O. (2016).
Recovering Short Generators of Principal Ideals in Cyclotomic Rings, pages 559–585.
Springer Berlin Heidelberg, Berlin, Heidelberg.

Hoffstein, J., Howgrave-Graham, N., Pipher, J., Silverman, J. H., and Whyte, W. (2003).
NTRUSIGN: Digital signatures using the NTRU lattice.
In *CT-RSA*, pages 122–140.

Hoffstein, J., Pipher, J., and Silverman, J. H. (1998).
NTRU: A ring-based public key cryptosystem.
In *ANTS*, pages 267–288.

Jetchev, D. and Wesolowski, B. (2015).
On graphs of isogenies of principally polarizable abelian surfaces and the discrete logarithm problem.
CoRR, abs/1506.00522.

Langlois, A. and Stehlé, D. (2015).
Worst-case to average-case reductions for module lattices.
Designs, Codes and Cryptography, 75(3):565–599.

References III

Lyubashevsky, V., Peikert, C., and Regev, O. (2013).
On ideal lattices and learning with errors over rings.
Journal of the ACM, 60(6):43:1–43:35.
Preliminary version in Eurocrypt 2010.

Micciancio, D. (2007).
Generalized compact knapsacks, cyclic lattices, and efficient one-way functions.
Computational Complexity, 16(4):365–411.
Preliminary version in FOCS 2002.

Regev, O. (2009).
On lattices, learning with errors, random linear codes, and cryptography.
J. ACM, 56(6):1–40.
Preliminary version in STOC 2005.

Schoof, R. (1998).
Minus class groups of the fields of the l-th roots of unity.
Mathematics of Computation of the American Mathematical Society, 67(223):1225–1245.

Schoof, R. (2003).
Class numbers of real cyclotomic fields of prime conductor.
Mathematics of computation, 72(242):913–937.

References IV

Washington, L. C. (2012).
Introduction to cyclotomic fields, volume 83.
Springer Science & Business Media.