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 foundation for Post-Quantum Crypto

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

Worst-case Approx-SVP $\geq \{ \begin{array}{l} \text{SIS (Short Integer Solution)} \\ \text{LWE (Learning With Error)} \end{array}$

How hard is Approx-SVP? Depends on the Approximation factor $\alpha$. 

![Diagram](image-url)
Lattice-Based Crypto

Lattice problems provides a strong foundation for Post-Quantum Crypto

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

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

How hard is Approx-SVP? Depends on the Approximation factor $\alpha$.

How hard is Approx-SVP? Depends on the Approximation factor $\alpha$. The hardness depends on the Approximation factor $\alpha$. For a given $\alpha$, the problem becomes tractable if $\alpha$ is sufficiently small, but remains intractable if $\alpha$ is too large. The relationship between the approximation factor and the hardness of the problem is often captured by a trade-off curve, which shows the scaling of time and space requirements as a function of $\alpha$. For instance, as $\alpha$ increases, the time required to solve the problem might decrease, but at the cost of increased space requirements. This trade-off is illustrated by the diagram, which shows the asymptotic scaling of time and space as functions of $\alpha$.
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 $R = R[X]/(X^p - 1)$, and module-lattices:

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

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]

Worst-case Approx-Ideal-SVP $\geq \left\{\begin{array}{l} \text{Ring-SIS} \\ \text{Ring-LWE} \end{array}\right.$

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

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

Cramer, D., Wesolowski (Leiden, CWI, EPFL)  Stickelberger V.S. Ideal-SVP
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:

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

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]

Worst-case Approx-Ideal-SVP $\geq \{\text{Ring-SIS}, \text{Ring-LWE}\}$

Applicable for cyclotomic rings $\mathcal{R} = \mathbb{Z}[\omega_m]$ ($\omega_m$ 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:

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

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]

Worst-case Approx-Ideal-SVP $\geq$ \{ Ring-SIS, Ring-LWE \}

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

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

Cramer, D., Wesolowski (Leiden, CWI, EPFL) Stickelberger V.S. Ideal-SVP
Is Ideal-SVP as hard as general SVP?

Are there other approaches 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 \( m = p^k, \mathcal{R} = \mathbb{Z}[\omega_m], \alpha = \exp(O(\sqrt{n})) \).
Is Ideal-SVP as hard as general SVP?

Are there other approaches 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 approaches 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. $hR = \mathfrak{h}$.

**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. $gR = hR$.

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

**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**

<table>
<thead>
<tr>
<th>Time</th>
<th>Crypto</th>
</tr>
</thead>
<tbody>
<tr>
<td>$e^{\tilde{O}(n)}$</td>
<td>$e^{\tilde{O}(\sqrt{n})}$</td>
</tr>
</tbody>
</table>

**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 $\alpha$

This work: CPM via Stickelberger Short Class Relation

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

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

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 $\alpha$

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 $\alpha$

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
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 $\mathfrak{a} \subset \mathcal{O}_K$ 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 $\mathfrak{f} = \frac{1}{x} \mathfrak{a}$, 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.
Ideals can be multiplied, and remain ideals:

\[ ab = \left\{ \sum_{\text{finite}} a_i b_i, \quad a_i \in a, b_i \in b \right\}. \]

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** \(\text{Cl}_K = \mathcal{F}_K/\mathcal{P}_K\).

The class of a ideal \(a \in \mathcal{F}_K\) is denoted \([a] \in \text{Cl}_K\).

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

\(^1\)with neutral element \(\mathcal{O}_K\).
Class Group

Ideals can be multiplied, and remain ideals:

\[ a b = \left\{ \sum_{\text{finite}} a_i b_i, \ a_i \in a, b_i \in b \right\} . \]

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 \( \text{Cl}_K = \mathcal{F}_K / \mathcal{P}_K \).

The class of a ideal \( a \in \mathcal{F}_K \) is denoted \( [a] \in \text{Cl}_K \).

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

\(^1\)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 \( \alpha \), and a factor \( F \)
- Find a **small integral** ideal \( \beta \) such that \([\alpha \beta] = [\mathcal{O}_K]\) and \( N\beta \leq F \)

**Note:** Smallness with respect to the Algebraic Norm \( N \) of \( \beta \),
(essentially the volume of \( \beta \) as a lattice).

- Solve CPM, and apply the previous results (PIP-SGP) to \( \alpha \beta \)
- This will give a generator \( g \) of \( \alpha \beta \subset \alpha \) (so \( g \in \alpha \)) of length

\[
L = N(\alpha \beta)^{1/n} \cdot \exp(\tilde{O}(\sqrt{n}))
\]

- This Ideal-SVP solution has an approx factor of

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

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

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

- Solve CPM, and apply the previous results (PIP-SGP) to $ab$
- This will give a generator $g$ of $ab \subset a$ (so $g \in a$) of length
  \[
  L = N(ab)^{1/n} \cdot \exp(\tilde{O}(\sqrt{n}))
  \]
- This Ideal-SVP solution has an approx factor of
  \[\alpha \approx \frac{L}{N(a)} = F^{1/n} \cdot \exp(\tilde{O}(\sqrt{n}))\]

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 \( \alpha \), and an factor \( F \)
- Find a small integral ideal \( b \) such that \([\alpha b] = [\mathcal{O}_K]\) and \( N b \leq F \)

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

- Solve CPM, and apply the previous results (PIP-SGP) to \( \alpha b \)
- This will give a generator \( g \) of \( \alpha b \subset \alpha \) (so \( g \in \alpha \)) of length 
  \[ L = N(\alpha b)^{1/n} \cdot \exp(\tilde{O}(\sqrt{n})) \]
- This Ideal-SVP solution has an approx factor of 
  \[ \alpha \approx L/N(\alpha) = F^{1/n} \cdot \exp(\tilde{O}(\sqrt{n})) \]

CPM with \( F = \exp(\tilde{O}(n^{3/2})) \) ⇒ Ideal-SVP with \( \alpha = \exp(\tilde{O}(\sqrt{n})) \)
Choose a **factor basis** \( \mathcal{B} \) of integral ideals and search \( b \) of the form:

\[
b = \prod_{p \in \mathcal{B}} p^{e_p}.
\]

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

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

\[
\prod_{p \in \mathcal{B}} [p^{e_p}] = [a^{-1}].
\]

This finds a \( b \) such that \([ab] = [\mathcal{O}_K]\), yet:

- \( b \) may not be integral (negative exponents, yet easy to solve)
- \( N b \approx \exp(\|\vec{e}\|_1) \) may be huge (unbounded \( \vec{e} \), want \( \|\vec{e}\|_1 = \tilde{O}(n^{3/2}) \)).
Choose a factor basis $\mathcal{B}$ of integral ideals and search $b$ of the form:

$$b = \prod_{p \in \mathcal{B}} p^{e_p}.$$  

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

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

$$\prod_{p \in \mathcal{B}} [p^{e_p}] = [a^{-1}].$$

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

- $b$ may not be integral (negative exponents, yet easy to solve)
- $Nb \approx \exp(\|\vec{e}\|_1)$ may be huge (unbounded $\vec{e}$, want $\|\vec{e}\|_1 = \tilde{O}(n^{3/2})$).
Choose a **factor basis** $\mathcal{B}$ of integral ideals and search $b$ of the form:

$$b = \prod_{p \in \mathcal{B}} p^{e_p}.$$

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

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

$$\prod_{p \in \mathcal{B}} [p^{e_p}] = [a^{-1}].$$

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

- $b$ may not be integral (negative exponents, yet easy to solve)
- $Nb \approx \exp(\|\vec{e}\|_1)$ 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 $g \rightarrow ga$ 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 $[a]$ to $[\mathcal{O}_K]$ in Cayley-Graph($\Cl, \mathcal{B}$).

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

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

$$\Lambda = \left\{ \bar{e} \in \mathbb{Z}^B, \text{ s.t. } \prod [p^e_p] = [\mathcal{O}_K] \right\}$$

i.e. the (full-rank) lattice of class-relations in base $B$.

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

Rephrased Goal for CPM: CVP in $\Lambda$

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

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

Why should we know anything special about $\Lambda$?
A lattice problem

Cl is **abelian** and **finite**, so \( \text{Cl} = \mathbb{Z}^B / \Lambda \) for some lattice \( \Lambda \):

\[
\Lambda = \left\{ \vec{e} \in \mathbb{Z}^B, \text{ s.t. } \prod [p_{p}] = [\mathcal{O}_K] \right\}
\]
i.e. the (full-rank) **lattice of class-relations** in base \( B \).

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

Rephrased Goal for CPM: CVP in \( \Lambda \)

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

In general: very hard. But for good \( \Lambda \), with a good basis, can be easy.

Why should we know anything special about \( \Lambda \)?
Example

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

$$[a]^\sigma = [\sigma(a)].$$

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

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

- Assume $B = \{p^\sigma, \sigma \in G\}$
- $G$ acts on $B$, and so it acts on $\mathbb{Z}^G$ by permuting coordinates
- the lattice $\Lambda \subset \mathbb{Z}^G$ is **invariant** by the action of $G$!
  i.e. $\Lambda$ admits $G$ as a group of **symmetries**

$\Lambda$ 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:

$$[a]^\sigma = [\sigma(a)].$$

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

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

- Assume $\mathcal{B} = \{p^\sigma, \sigma \in G\}$
- $G$ acts on $\mathcal{B}$, and so it acts on $\mathbb{Z}^m$ by permuting coordinates
- the lattice $\Lambda \subset \mathbb{Z}^m$ is invariant by the action of $G$!
  i.e. $\Lambda$ admits $G$ as a group of symmetries

$\Lambda$ 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:

$$[a]^\sigma = [\sigma(a)].$$

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

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

- Assume $\mathcal{B} = \{p^\sigma, \sigma \in G\}$
- $G$ acts on $\mathcal{B}$, and so it acts on $\mathbb{Z}^{\mathcal{B}}$ by permuting coordinates
- the lattice $\Lambda \subset \mathbb{Z}^{\mathcal{B}}$ is **invariant** by the action of $G$!
  i.e. $\Lambda$ admits $G$ as a group of **symmetries**

$\Lambda$ 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:

$$[a]^\sigma = [\sigma(a)].$$

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

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

- Assume $\mathcal{B} = \{ p^\sigma, \sigma \in G \}$
- $G$ acts on $\mathcal{B}$, and so it acts on $\mathbb{Z}^\mathcal{B}$ by permuting coordinates
- the lattice $\Lambda \subset \mathbb{Z}^\mathcal{B}$ is invariant by the action of $G$
  i.e. $\Lambda$ admits $G$ as a group of symmetries

$\Lambda$ is more than just a lattice: it is a $\mathbb{Z}[G]$-module
Stickelberger’s Theorem

In fact, we know much more about $\Lambda$!

**Definition (The Stickelberger ideal)**

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

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

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: $\forall e \in S, \alpha \subset K$

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

In particular, if $\mathcal{B} = \{ p^\sigma, \sigma \in G \}$, 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 can find $x \in S$ such 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:

\[ \mathcal{B} = \{ p^\sigma, \sigma \in G \} \] generates the class group.

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

Eliminating minus exponents

- Easy when \( h^+ = 1 \) : \( [a^{-1}] = [\bar{a}] \), doable when \( h^+ = \text{poly}(n) \)
  - \( h^+ \) is the size of the class group of \( K^+ \), the maximal totally real subfield of \( K \)
- \( h^+ = \text{poly}(n) \) 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 is 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 \text{Ideal-SVP}, but equivalence is not known.


