Ideal lattices in number theory and in cryptology

Jean-François Biasse

University of Waterloo

December 2014

Definition of homomorphic encryption

We assume the usual setting in cryptography

- Secret Key S_k.
- Public key P_k (or another secret key).
- Encryption function $\mathrm{Enc}(m, P_k)$.
- Decryption function $\mathrm{Dec}(c, S_k)$ such that $\mathrm{Dec}(\mathrm{Enc}(m, P_k), S_k) = m$.

Definition of homomorphic encryption

We assume the usual setting in cryptography

- Secret Key S_k.
- Public key P_k (or another secret key).
- Encryption function $\mathrm{Enc}(m, P_k)$.
- Decryption function $\mathrm{Dec}(c, S_k)$ such that $\mathrm{Dec}(\mathrm{Enc}(m, P_k), S_k) = m$.

Definition

A scheme is said to be **homomorphic** if for a function f we have

$$f(\mathrm{Enc}(m, P_k)) = \mathrm{Enc}(f(m), P_k).$$

Definition of homomorphic encryption

We assume the usual setting in cryptography

- Secret Key S_k.
- Public key P_k (or another secret key).
- Encryption function $\mathrm{Enc}(m, P_k)$.
- Decryption function $\mathrm{Dec}(c, S_k)$ such that $\mathrm{Dec}(\mathrm{Enc}(m, P_k), S_k) = m$.

Definition

A scheme is said to be **homomorphic** if for a function f we have

$$f(\mathrm{Enc}(m, P_k)) = \mathrm{Enc}(f(m), P_k).$$

- Homomorphic for f of limited complexity : somewhat homomorphic.
- Homomorphic for any f : fully homomorphic.

Motivation of homomorphic encryption

Versailles

Hospital

Far far away

Server farm

Somewhere in between

evil NSA, semi-evil GCHQ, good DGSE

Motivation of homomorphic encryption

Versailles

Hospital

Sends encrypted update

$\mathsf{Enc}(x, S_k)$

Far far away

Server farm

Somewhere in between

evil NSA, semi-evil GCHQ, good DGSE

Motivation of homomorphic encryption

Versailles

Hospital

Far far away

Server farm

Updates $c' = f(c, x)$

Somewhere in between

evil NSA, semi-evil GCHQ, good DGSE

Motivation of homomorphic encryption

Versailles

Hospital

Sends encrypted quiery

Enc($T[i], S_k$) ?

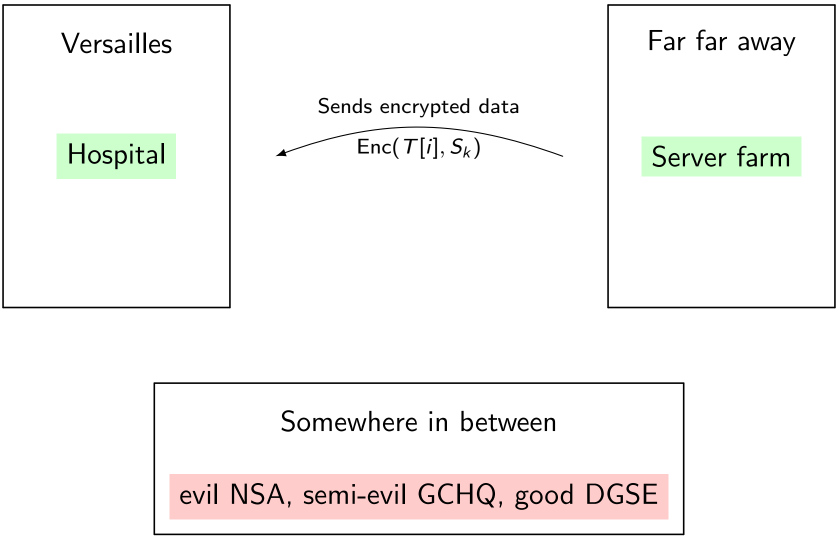
Far far away

Server farm

Somewhere in between

evil NSA, semi-evil GCHQ, good DGSE

Motivation of homomorphic encryption




Quantum Computing

Peter Shor

Polynomial time algorithms for

- Integer factoring.
- Solving the Discrete Logarithm Problem.

Hard problem 1 : (R)-LWE

Some homomorphic schemes and “quantum-resistant” cryptosystems rely on the Learning With Error assumption.

Hard problem 1 : (R)-LWE

Some homomorphic schemes and “quantum-resistant” cryptosystems rely on the Learning With Error assumption.

Encryption with (R)-LWE

Let $m \in \{0, 1\}$ be a message and s a secret.

1. Draw a and e at random.
2. Send $C = (a, a \cdot s + m + 2e)$

Hard problem 1 : (R)-LWE

Some homomorphic schemes and "quantum-resistant" cryptosystems rely on the Learning With Error assumption.

Encryption with (R)-LWE

Let $m \in \{0, 1\}$ be a message and s a secret.

1. Draw a and e at random.
2. Send $C = (a, a \cdot s + m + 2e)$

- (R)-LWE assumption : it is hard to distinguish many $(a, a \cdot s + e)$ from randomness.
- It reduces to finding short vectors in (ideal)-lattices.

Hard problem 2 : short-PIP

Some homomorphic schemes and “quantum-resistant” cryptosystems rely on the short Principal Ideal Problem assumption.

Hard problem 2 : short-PIP

Some homomorphic schemes and "quantum-resistant" cryptosystems rely on the short Principal Ideal Problem assumption.

Encryption with short-PIP

Let $m \in \{0, 1\}$ and a prime ideal $\mathfrak{p} = (g)$ where g is small and secret.

1. Draw a at random.
2. Send $C = m + 2 * a \bmod \mathfrak{p}$.

Hard problem 2 : short-PIP

Some homomorphic schemes and "quantum-resistant" cryptosystems rely on the short Principal Ideal Problem assumption.

Encryption with short-PIP

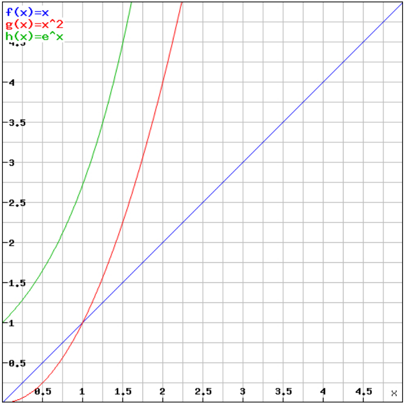
Let $m \in \{0, 1\}$ and a prime ideal $\mathfrak{p} = (g)$ where g is small and secret.

1. Draw a at random.
2. Send $C = m + 2 * a \bmod \mathfrak{p}$.

- short-PIP assumption : hard to find a short generator of an ideal $\mathfrak{p}$.
- Not sure what it reduces to, but it can be solved by solutions to the shortest vector problem.

Hardness of a problem

We quantify it by the function Time $= f(\text{input size})$.



Subexponential complexity

Assume we want to solve a problem of input size S.

Subexponential complexity

Assume we want to solve a problem of input size S.

Subexponential function

We define the *subexponential* function by

$$L_S(a, b) = e^{b \cdot (S)^a (\log(S))^{1-a}}.$$

Subexponential complexity

Assume we want to solve a problem of input size S.

Subexponential function

We define the *subexponential* function by

$$L_S(a, b) = e^{b \cdot (S)^a (\log(S))^{1-a}}.$$

For $a \in [0, 1]$, $L_S(a, b)$ is between exponential and polynomial in S

$$L_S(0, b) = S^b,$$
$$L_S(1, b) = (e^S)^b.$$

Number fields

Let $K/\mathbb{Q}$ of degree n, $\mathcal{O}_K$ its **ring of integers**, $\sigma : K \rightarrow \mathbb{C}$ its embeddings.

$$U := \mathcal{O}_K^* = \mu \times \langle \epsilon_1 \rangle \times \cdots \times \langle \epsilon_r \rangle,$$

where $r = n_1 + n_2$ with n_1 is the number of real embeddings of K, and n_2 the paire of complex ones.

Number fields

Let $K/\mathbb{Q}$ of degree n, $\mathcal{O}_K$ its **ring of integers**, $\sigma : K \to \mathbb{C}$ its embeddings.

$$U := \mathcal{O}_K^* = \mu \times \langle \epsilon_1 \rangle \times \cdots \times \langle \epsilon_r \rangle,$$

where $r = n_1 + n_2$ with n_1 is the number of real embeddings of K, and n_2 the paire of complex ones.

The **fractional ideals** are of the form $\mathfrak{a} = \frac{1}{d} I$ where I is an ideal of $\mathcal{O}_K$.

$$\mathrm{Cl}(\mathcal{O}_K) := \{\text{Invertible fractional ideals}\}/\{\text{Principal fractional ideal}\}.$$

Number fields

Let $K/\mathbb{Q}$ of degree n, $\mathcal{O}_K$ its **ring of integers**, $\sigma : K \to \mathbb{C}$ its embeddings.

$$U := \mathcal{O}_K^* = \mu \times \langle \epsilon_1 \rangle \times \cdots \times \langle \epsilon_r \rangle,$$

where $r = n_1 + n_2$ with n_1 is the number of real embeddings of K, and n_2 the paire of complex ones.

The **fractional ideals** are of the form $\mathfrak{a} = \frac{1}{d} I$ where I is an ideal of $\mathcal{O}_K$.

$$\mathrm{Cl}(\mathcal{O}_K) := \{\text{Invertible fractional ideals}\}/\{\text{Principal fractional ideal}\}.$$

- We have $[\mathfrak{a}] = [\mathfrak{b}] \in \mathrm{Cl}(\mathcal{O}_K)$ if $\mathfrak{a} = (\alpha)\mathfrak{b}$ for some $\alpha \in K$.

Number fields

Let $K/\mathbb{Q}$ of degree n, $\mathcal{O}_K$ its **ring of integers**, $\sigma : K \to \mathbb{C}$ its embeddings.

$$U := \mathcal{O}_K^* = \mu \times \langle \epsilon_1 \rangle \times \cdots \times \langle \epsilon_r \rangle,$$

where $r = n_1 + n_2$ with n_1 is the number of real embeddings of K, and n_2 the paire of complex ones.

The **fractional ideals** are of the form $\mathfrak{a} = \frac{1}{d} I$ where I is an ideal of $\mathcal{O}_K$.

$$\mathrm{Cl}(\mathcal{O}_K) := \{\text{Invertible fractional ideals}\}/\{\text{Principal fractional ideal}\}.$$

- We have $[\mathfrak{a}] = [\mathfrak{b}] \in \mathrm{Cl}(\mathcal{O}_K)$ if $\mathfrak{a} = (\alpha)\mathfrak{b}$ for some $\alpha \in K$.
- In cryptography $K = \mathbb{Q}[X]/\Phi_N(X) = \mathbb{Q}(\xi_N)$ for $\xi_N := e^{\frac{2i\pi}{N}}$.

Computing the class group and the unit group

We assume we are given K, its n_1 real embeddings, its n_2 pairs of complex embeddings and $\mathcal{O}_K = \sum_i \mathbb{Z}\alpha_i$.

Output of the algorithm

We compute $d_1, \cdots, d_k \in \mathbb{Z}$ and $\gamma_1, \cdots, \gamma_r$ such that

- $\mathrm{Cl}(\mathcal{O}) = \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z}$.
- $U = \mu \times \langle\gamma_1\rangle \times \cdots \times \langle\gamma_r\rangle$

where $r := r_1 + r_2 - 1$ and μ is the set of roots of unity.

Computing the class group and the unit group

We assume we are given K, its n_1 real embeddings, its n_2 pairs of complex embeddings and $\mathcal{O}_K = \sum_i \mathbb{Z}\alpha_i$.

Output of the algorithm

We compute $d_1, \cdots, d_k \in \mathbb{Z}$ and $\gamma_1, \cdots, \gamma_r$ such that

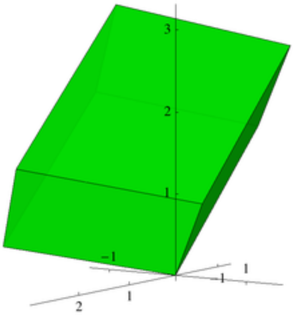
- $\mathrm{Cl}(\mathcal{O}) = \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z}$.
- $U = \mu \times \langle\gamma_1\rangle \times \cdots \times \langle\gamma_r\rangle$

where $r := r_1 + r_2 - 1$ and μ is the set of roots of unity.

We show how to use U and $\mathrm{Cl}(\mathcal{O}_K)$ to solve the PIP

$$\text{Given } \mathfrak{a}, \quad \text{find } g \text{ such that } \mathfrak{a} = (g)\mathcal{O}_K$$

Input size



Let $(\omega_i)_{i\leq n}$ the integral basis of $\mathcal{O}$ (given as input), its fundamental volume is

$$\Delta = \det \begin{pmatrix} \sigma_1(\omega_1) & \dots & \sigma_1(\omega_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\omega_1) & \dots & \sigma_n(\omega_n) \end{pmatrix}^2$$

Class group computation

Factor base

Let $\mathcal{B} = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_N\}$ be a set of ideals whose classes generate $\mathrm{Cl}(\mathcal{O})$.

We consider the surjective morphism

$$\begin{array}{ccccc} \mathbb{Z}^N & \xrightarrow{\varphi} & \mathcal{I} & \xrightarrow{\pi} & \mathrm{Cl}(\mathcal{O}) \\ (e_1, \ldots, e_N) & \longrightarrow & \prod_i \mathfrak{p}_i^{e_i} & \longrightarrow & \prod_i [\mathfrak{p}_i]^{e_i} \end{array}$$

Class group computation

Factor base

Let $\mathcal{B} = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_N\}$ be a set of ideals whose classes generate $\mathrm{Cl}(\mathcal{O})$.

We consider the surjective morphism

$$\begin{array}{ccccc} \mathbb{Z}^N & \xrightarrow{\varphi} & \mathcal{I} & \xrightarrow{\pi} & \mathrm{Cl}(\mathcal{O}) \\ (e_1, \ldots, e_N) & \longrightarrow & \prod_i \mathfrak{p}_i^{e_i} & \longrightarrow & \prod_i [\mathfrak{p}_i]^{e_i} \end{array}$$

We use the property that the class group satisfies

$$\mathrm{Cl}(\mathcal{O}) \simeq \mathbb{Z}^N / \ker(\pi \circ \varphi).$$

Class group computation

Factor base

Let $\mathcal{B} = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_N\}$ be a set of ideals whose classes generate $\mathrm{Cl}(\mathcal{O})$.

We consider the surjective morphism

$$\begin{array}{ccccc} \mathbb{Z}^N & \xrightarrow{\varphi} & \mathcal{I} & \xrightarrow{\pi} & \mathrm{Cl}(\mathcal{O}) \\ (e_1, \ldots, e_N) & \longrightarrow & \prod_i \mathfrak{p}_i^{e_i} & \longrightarrow & \prod_i [\mathfrak{p}_i]^{e_i} \end{array}$$

We use the property that the class group satisfies

$$\mathrm{Cl}(\mathcal{O}) \simeq \mathbb{Z}^N / \ker(\pi \circ \varphi).$$

We therefore deduce $\mathrm{Cl}(\mathcal{O})$ from the lattice of the $(e_1, \cdots, e_N)$ such that

$$\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_N^{e_N} = (\alpha) = 1 \in \mathrm{Cl}(\mathcal{O}) \text{ for some } \alpha \in \mathcal{O}.$$

From relations to the unit group

Let $M \in \mathbb{Z}^{N \times N'}$ be a relation matrix. That is,

$$\forall i, \mathfrak{p}_1^{m_{i,1}} \cdots \mathfrak{p}_N^{m_{i,N}} = (\alpha_i) = 1 \in \mathrm{Cl}(\mathcal{O}).$$

From relations to the unit group

Let $M \in \mathbb{Z}^{N\times N'}$ be a relation matrix. That is,

$$\forall i, \mathfrak{p}_1^{m_{i,1}} \cdots \mathfrak{p}_N^{m_{i,N}} = (\alpha_i) = 1 \in \mathrm{Cl}(\mathcal{O}).$$

Property

Let $X = (x_1, \cdots, x'_N)$ be such that $XM = 0$. Then,

$$\beta_X := \alpha_1^{x_1} \cdots \alpha_N^{x'_N} \text{ is a unit}$$

From relations to the unit group

Let $M \in \mathbb{Z}^{N \times N'}$ be a relation matrix. That is,

$$\forall i, \mathfrak{p}_1^{m_{i,1}} \cdots \mathfrak{p}_N^{m_{i,N}} = (\alpha_i) = 1 \in \mathrm{Cl}(\mathcal{O}).$$

Property

Let $X = (x_1, \cdots, x'_N)$ be such that $XM = 0$. Then,

$$\beta_X := \alpha_1^{x_1} \cdots \alpha_N^{x'_N} \text{ is a unit}$$

(since $(\beta_X) = \mathfrak{p}_1^{\sum_i x_i m_{i,1}} \cdots \mathfrak{p}_N^{\sum_i x_i m_{i,N}} = \mathfrak{p}_1^0 \cdots \mathfrak{p}_N^0 = (1)$.)

From relations to the unit group

Let $M \in \mathbb{Z}^{N \times N'}$ be a relation matrix. That is,

$$\forall i, \mathfrak{p}_1^{m_{i,1}} \cdots \mathfrak{p}_N^{m_{i,N}} = (\alpha_i) = 1 \in \mathrm{Cl}(\mathcal{O}).$$

Property

Let $X = (x_1, \cdots, x'_N)$ be such that $XM = 0$. Then,

$$\beta_X := \alpha_1^{x_1} \cdots \alpha_N^{x'_N} \text{ is a unit}$$

(since $(\beta_X) = \mathfrak{p}_1^{\sum_i x_i m_{i,1}} \cdots \mathfrak{p}_N^{\sum_i x_i m_{i,N}} = \mathfrak{p}_1^0 \cdots \mathfrak{p}_N^0 = (1)$.)

We use the following strategy

- We derive units from elements in $\ker(M)$.
- We construct a minimal generating set for U by induction.

From relations to a generator of $\mathfrak{a}$

Assume the rows of $M \in \mathbb{Z}^{l \times k}$ generate all the relations of the form

$$\mathfrak{p}_1^{x_1} \cdots \mathfrak{p}_k^{x_k} = (\alpha) = 1 \in \mathrm{Cl}(\mathcal{O}_K).$$

From relations to a generator of $\mathfrak{a}$

Assume the rows of $M \in \mathbb{Z}^{l \times k}$ generate all the relations of the form

$$\mathfrak{p}_1^{x_1} \cdots \mathfrak{p}_k^{x_k} = (\alpha) = 1 \in \mathrm{Cl}(\mathcal{O}_K).$$

Algorithm for solving PIP

- Find $X = (x_1, \cdots, x_k)$ and α such that $\mathfrak{a} = (\beta)\mathfrak{p}_1^{x_1} \cdots \mathfrak{p}_k^{x_k}$.

From relations to a generator of $\mathfrak{a}$

Assume the rows of $M \in \mathbb{Z}^{l \times k}$ generate all the relations of the form

$$\mathfrak{p}_1^{x_1} \cdots \mathfrak{p}_k^{x_k} = (\alpha) = 1 \in \mathrm{Cl}(\mathcal{O}_K).$$

Algorithm for solving PIP

- Find $X = (x_1, \cdots, x_k)$ and α such that $\mathfrak{a} = (\beta)\mathfrak{p}_1^{x_1} \cdots \mathfrak{p}_k^{x_k}$.
- As $\mathfrak{a}$ is principal, so is $\mathfrak{a}_1^{x_1} \cdots \mathfrak{p}_k^{x_k}$.

From relations to a generator of $\mathfrak{a}$

Assume the rows of $M \in \mathbb{Z}^{l\times k}$ generate all the relations of the form

$$\mathfrak{p}_1^{x_1}\cdots\mathfrak{p}_k^{x_k} = (\alpha) = 1 \in \mathrm{Cl}(\mathcal{O}_K).$$

Algorithm for solving PIP

- Find $X = (x_1, \cdots, x_k)$ and α such that $\mathfrak{a} = (\beta)\mathfrak{p}_1^{x_1}\cdots\mathfrak{p}_k^{x_k}$.
- As $\mathfrak{a}$ is principal, so is $\mathfrak{a}_1^{x_1}\cdots\mathfrak{p}_k^{x_k}$.
- Solve the system $YM = X$.

From relations to a generator of $\mathfrak{a}$

Assume the rows of $M \in \mathbb{Z}^{l \times k}$ generate all the relations of the form

$$\mathfrak{p}_1^{x_1} \cdots \mathfrak{p}_k^{x_k} = (\alpha) = 1 \in \mathrm{Cl}(\mathcal{O}_K).$$

Algorithm for solving PIP

- Find $X = (x_1, \cdots, x_k)$ and α such that $\mathfrak{a} = (\beta)\mathfrak{p}_1^{x_1} \cdots \mathfrak{p}_k^{x_k}$.
- As $\mathfrak{a}$ is principal, so is $\mathfrak{a}_1^{x_1} \cdots \mathfrak{p}_k^{x_k}$.
- Solve the system $YM = X$.
- Then $\mathfrak{a} = (g)$ with $g = \beta\alpha_1^{y_1} \cdots \alpha_l^{y_l}$.

From relations to a generator of $\mathfrak{a}$

Assume the rows of $M \in \mathbb{Z}^{l \times k}$ generate all the relations of the form

$$\mathfrak{p}_1^{x_1} \cdots \mathfrak{p}_k^{x_k} = (\alpha) = 1 \in \mathrm{Cl}(\mathcal{O}_K).$$

Algorithm for solving PIP

- Find $X = (x_1, \cdots, x_k)$ and α such that $\mathfrak{a} = (\beta)\mathfrak{p}_1^{x_1} \cdots \mathfrak{p}_k^{x_k}$.
- As $\mathfrak{a}$ is principal, so is $\mathfrak{a}_1^{x_1} \cdots \mathfrak{p}_k^{x_k}$.
- Solve the system $YM = X$.
- Then $\mathfrak{a} = (g)$ with $g = \beta\alpha_1^{y_1} \cdots \alpha_l^{y_l}$.

Problem : most likely g is not short.

Short generators of ideals

Let $\mathfrak{a} \subseteq \mathcal{O}$ a principal ideal and $U = \mu \times \langle \varepsilon_1 \rangle \times \cdots \times \langle \varepsilon_r \rangle$ the unit group.

- We know how to compute generators for U and a generator of $\mathfrak{a}$.
- We want a small generator of $\mathfrak{a}$.

Short generators of ideals

Let $\mathfrak{a} \subseteq \mathcal{O}$ a principal ideal and $U = \mu \times \langle \varepsilon_1 \rangle \times \cdots \times \langle \varepsilon_r \rangle$ the unit group.

- We know how to compute generators for U and a generator of $\mathfrak{a}$.
- We want a small generator of $\mathfrak{a}$.

Assume we find $\alpha \in \mathcal{O}$ such that $\mathfrak{a} = (\alpha)$, then

$$\forall (e_1, \cdots, e_r) \in \mathbb{Z}^r,\ \mathfrak{a} = (\varepsilon_1^{e_1}, \cdots, \varepsilon_r^{e_r} \alpha).$$

Short generators of ideals

Let $\mathfrak{a} \subseteq \mathcal{O}$ a principal ideal and $U = \mu \times \langle \varepsilon_1 \rangle \times \cdots \times \langle \varepsilon_r \rangle$ the unit group.

- We know how to compute generators for U and a generator of $\mathfrak{a}$.
- We want a small generator of $\mathfrak{a}$.

Assume we find $\alpha \in \mathcal{O}$ such that $\mathfrak{a} = (\alpha)$, then

$$\forall (e_1, \cdots, e_r) \in \mathbb{Z}^r, \ \mathfrak{a} = (\varepsilon_1^{e_1}, \cdots, \varepsilon_r^{e_r} \alpha).$$

When $r = 1$, then we find $e \in \mathbb{Z}$ such that $\log|\alpha| - e \log|\varepsilon|$ has the desired size

Short generators of ideals

Let $\mathfrak{a} \subseteq \mathcal{O}$ a principal ideal and $U = \mu \times \langle \varepsilon_1 \rangle \times \cdots \times \langle \varepsilon_r \rangle$ the unit group.

- We know how to compute generators for U and a generator of $\mathfrak{a}$.
- We want a small generator of $\mathfrak{a}$.

Assume we find $\alpha \in \mathcal{O}$ such that $\mathfrak{a} = (\alpha)$, then

$$\forall (e_1, \cdots, e_r) \in \mathbb{Z}^r,\ \mathfrak{a} = (\varepsilon_1^{e_1}, \cdots, \varepsilon_r^{e_r} \alpha).$$

When $r = 1$, then we find $e \in \mathbb{Z}$ such that $\log |\alpha| - e \log |\varepsilon|$ has the desired size.

- Let $\mathrm{Log}(x) := (\log |x|_1, \cdots, \log |x|_r) \in \mathbb{R}^r$.
- We want $\| \mathrm{Log}(\alpha) + \sum_i e_i \mathrm{Log}(\varepsilon_i) \|_2$ small.

In arbitrary dimension, we want to solve the closest vector problem.

Complexity result

The complexity is expressed with respect to the input size $\log|\Delta|$.

Complexity result

The complexity is expressed with respect to the input size $\log|\Delta|$.

Buchmann 90

Subexponential complexity for computing

- Ideal class group/Unit group.
- Solutions to the PIP

In classes of **fixed degree** number fields.

Complexity result

The complexity is expressed with respect to the input size $\log|\Delta|$.

Buchmann 90

Subexponential complexity for computing

- Ideal class group/Unit group.
- Solutions to the PIP

In classes of **fixed degree** number fields.

B. - Fieker 14

Subexponential complexity for computing

- Ideal class group/Unit group.
- Solutions to the PIP

In arbitrary classes of number fields.


Quantum Computing

Finding the periods of a function

A lot of quantum algorithms rely on finding the period of a function

$$f : \mathbb{R}^m \longrightarrow \{\text{Quantum states}\}.$$

Finding the periods of a function

A lot of quantum algorithms rely on finding the period of a function

$$f : \mathbb{R}^m \longrightarrow \{\text{Quantum states}\}.$$

Hidden Subgroup Problem (HSP)

We look for a discret subgroup $G \subseteq \mathbb{R}^m$ such that there is f satisfying

- $f(x+g) = f(x)$ for all $g \in G$.
- f is efficiently computable classically.
- Other metric properties we don't want to talk about.

Finding the periods of a function

A lot of quantum algorithms rely on finding the period of a function

$$f : \mathbb{R}^m \longrightarrow \{\text{Quantum states}\}.$$

Hidden Subgroup Problem (HSP)

We look for a discret subgroup $G \subseteq \mathbb{R}^m$ such that there is f satisfying

- $f(x+g) = f(x)$ for all $g \in G$.
- f is efficiently computable classically.
- Other metric properties we don't want to talk about.

There exists a quantum algorithm to solve the HSP in polynomial time.

Reducing factorization to HSP

Suppose we want to factor $N = pq$. Let a coprime with N and

$$r \in \mathbb{Z}_{>0}, a^r = 0 \bmod N,\ a^{r-1} \neq 0 \bmod N.$$

Reducing factorization to HSP

Suppose we want to factor $N = pq$. Let a coprime with N and

$$r \in \mathbb{Z}_{>0}, a^r = 0 \bmod N, \ a^{r-1} \neq 0 \bmod N.$$

Then if r is even we have $(a^{r/2} - 1)(a^{r/2} + 1) = 0 \bmod N$ which yields p of q with probability $1/4$.

Reducing factorization to HSP

Suppose we want to factor $N = pq$. Let a coprime with N and

$$r \in \mathbb{Z}_{>0}, a^r = 0 \bmod N, \; a^{r-1} \neq 0 \bmod N.$$

Then if r is even we have $(a^{r/2} - 1)(a^{r/2} + 1) = 0 \bmod N$ which yields p of q with probability $1/4$.

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{f} & \mathbb{Z}/N\mathbb{Z} \\ x & \longrightarrow & a^x \bmod N \end{array}$$

- We have $f(x+g) = f(x)$ for all $x \in \mathbb{Z}$, $g \in r\mathbb{Z} \subseteq \mathbb{Z}$.
- A solution to the HSP with f yields r.

Reducing factorization to HSP

Suppose we want to factor $N = pq$. Let a coprime with N and

$$r \in \mathbb{Z}_{>0}, a^r = 0 \bmod N, \ a^{r-1} \neq 0 \bmod N.$$

Then if r is even we have $(a^{r/2} - 1)(a^{r/2} + 1) = 0 \bmod N$ which yields p of q with probability $1/4$.

$$\begin{aligned} \mathbb{Z} & \xrightarrow{\quad f \quad} \quad \mathbb{Z}/N\mathbb{Z} \\ x & \xrightarrow{\qquad} a^x \bmod N \end{aligned}$$

- We have $f(x+g) = f(x)$ for all $x \in \mathbb{Z}$, $g \in r\mathbb{Z} \subseteq \mathbb{Z}$.
- A solution to the HSP with f yields r.

The function f "hides" the subgroup $G = r\mathbb{Z} \subseteq \mathbb{Z}$.

Reducing the discrete logarithm problem to HSP

Let $a, b \in G$ such that $b = a^x$. The discrete logarithm problem consists of finding x.

Reducing the discrete logarithm problem to HSP

Let $a, b \in G$ such that $b = a^x$. The discrete logarithm problem consists of finding x.

$$\begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \xrightarrow{\quad f \quad} & G \\ (u, v) & \longrightarrow & a^u b^v \end{array}$$

Reducing the discrete logarithm problem to HSP

Let $a, b \in G$ such that $b = a^x$. The discrete logarithm problem consists of finding x.

$$\begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \xrightarrow{\quad f \quad} & G \\ (u, v) & \longrightarrow & a^u b^v \end{array}$$

- The function f "hides" the subgroup $G = \mathbb{Z} \times (x\mathbb{Z}) \subseteq \mathbb{Z} \times \mathbb{Z}$.
- Finding x reduces to solving the HSP with f.

Reducing the ideal class group and unit group to HSP

Assume we have a well defined function

$$\begin{array}{ccccc} \mathbb{Z}^N & \xrightarrow{\varphi} & \mathcal{I} & \xrightarrow{\pi} & \mathrm{Cl}(\mathcal{O}) \\ (e_1, \ldots, e_N) & \longrightarrow & \prod_i \mathfrak{p}_i^{e_i} & \longrightarrow & \prod_i [\mathfrak{p}_i]^{e_i} \end{array}$$

Reducing the ideal class group and unit group to HSP

Assume we have a well defined function

$$\begin{array}{ccccc} \mathbb{Z}^N & \xrightarrow{\varphi} & \mathcal{I} & \xrightarrow{\pi} & \mathrm{Cl}(\mathcal{O}) \\ (e_1, \ldots, e_N) & \longrightarrow & \prod_i \mathfrak{p}_i^{e_i} & \longrightarrow & \prod_i [\mathfrak{p}_i]^{e_i} \end{array}$$

- We saw how to derive $\mathrm{Cl}(\mathcal{O}_K)$ and $U = \mathcal{O}_K^*$ from $\ker(\pi \circ \varphi)$.

Reducing the ideal class group and unit group to HSP

Assume we have a well defined function

$$\begin{array}{ccccc} \mathbb{Z}^N & \xrightarrow{\varphi} & \mathcal{I} & \xrightarrow{\pi} & \mathrm{Cl}(\mathcal{O}) \\ (e_1, \ldots, e_N) & \longrightarrow & \prod_i \mathfrak{p}_i^{e_i} & \longrightarrow & \prod_i [\mathfrak{p}_i]^{e_i} \end{array}$$

- We saw how to derive $\mathrm{Cl}(\mathcal{O}_K)$ and $U = \mathcal{O}_K^*$ from $\ker(\pi \circ \varphi)$.
- We can derive $\ker(\pi \circ \varphi) \subseteq \mathbb{Z}^N$ from a solution to the HSP.

Reducing the ideal class group and unit group to HSP

Assume we have a well defined function

$$\begin{array}{ccccc} \mathbb{Z}^N & \xrightarrow{\varphi} & \mathcal{I} & \xrightarrow{\pi} & \mathrm{Cl}(\mathcal{O}) \\ (e_1, \ldots, e_N) & \longrightarrow & \prod_i \mathfrak{p}_i^{e_i} & \longrightarrow & \prod_i [\mathfrak{p}_i]^{e_i} \end{array}$$

- We saw how to derive $\mathrm{Cl}(\mathcal{O}_K)$ and $U = \mathcal{O}_K^*$ from $\ker(\pi \circ \varphi)$.
- We can derive $\ker(\pi \circ \varphi) \subseteq \mathbb{Z}^N$ from a solution to the HSP.

Remark

- We have a well-defined function only when the degree is fixed.
- We can derive solutions to the PIP easily.

Reducing the unit group to HSP (large degree)

We have n_1 real embeddings and n_2 complex embeddings of K.

- We have the natural inclusion $K \hookrightarrow \mathbb{R}^{n_1} \times \mathbb{C}^{n_2}$.

Reducing the unit group to HSP (large degree)

We have n_1 real embeddings and n_2 complex embeddings of K.

- We have the natural inclusion $K \hookrightarrow \mathbb{R}^{n_1} \times \mathbb{C}^{n_2}$.
- It follows that $K \hookrightarrow \mathbb{R}^{n_1+n_2} \times \mathbb{Z}_2^{n_1} \times (\mathbb{R}/\mathbb{Z})^{n_2}$.

Reducing the unit group to HSP (large degree)

We have n_1 real embeddings and n_2 complex embeddings of K.

- We have the natural inclusion $K \hookrightarrow \mathbb{R}^{n_1} \times \mathbb{C}^{n_2}$.
- It follows that $K \hookrightarrow \mathbb{R}^{n_1+n_2} \times \mathbb{Z}_2^{n_1} \times (\mathbb{R}/\mathbb{Z})^{n_2}$.
- Units satisfy $U \hookrightarrow \underbrace{\mathbb{R}^{n_1+n_2-1} \times \mathbb{Z}_2^{n_1} \times (\mathbb{R}/\mathbb{Z})^{n_2}}_{G}$ since $|\mathcal{N}(x)| = 1$.

Reducing the unit group to HSP (large degree)

We have n_1 real embeddings and n_2 complex embeddings of K.

- We have the natural inclusion $K \hookrightarrow \mathbb{R}^{n_1} \times \mathbb{C}^{n_2}$.
- It follows that $K \hookrightarrow \mathbb{R}^{n_1+n_2} \times \mathbb{Z}_2^{n_1} \times (\mathbb{R}/\mathbb{Z})^{n_2}$.
- Units satisfy $U \hookrightarrow \underbrace{\mathbb{R}^{n_1+n_2-1} \times \mathbb{Z}_2^{n_1} \times (\mathbb{R}/\mathbb{Z})^{n_2}}_{G}$ since $|\mathcal{N}(x)| = 1$.

$$\begin{array}{ccccc} G & \xrightarrow{\varphi} & \text{lattices of } \mathbb{R}^{n_1} \times \mathbb{C}^{n_2} & \xrightarrow{\pi} & \text{Quantum states} \\ x & \longrightarrow & x \cdot \mathcal{O}_K & \longrightarrow & |x \cdot \mathcal{O}_K\rangle \end{array}$$

Reducing the unit group to HSP (large degree)

We have n_1 real embeddings and n_2 complex embeddings of K.

- We have the natural inclusion $K \hookrightarrow \mathbb{R}^{n_1} \times \mathbb{C}^{n_2}$.
- It follows that $K \hookrightarrow \mathbb{R}^{n_1+n_2} \times \mathbb{Z}_2^{n_1} \times (\mathbb{R}/\mathbb{Z})^{n_2}$.
- Units satisfy $U \hookrightarrow \underbrace{\mathbb{R}^{n_1+n_2-1} \times \mathbb{Z}_2^{n_1} \times (\mathbb{R}/\mathbb{Z})^{n_2}}_{G}$ since $|\mathcal{N}(x)| = 1$.

$$\begin{array}{ccccc} G & \xrightarrow{\varphi} & \text{lattices of } \mathbb{R}^{n_1} \times \mathbb{C}^{n_2} & \xrightarrow{\pi} & \text{Quantum states} \\ x & \longrightarrow & x \cdot \mathcal{O}_K & \longrightarrow & |x \cdot \mathcal{O}_K\rangle \end{array}$$

Eisenträger-Hallgren-Kitaev-Song 14

- $\pi \circ \varphi$ “hides” the unit goup U.

Reducing the unit group to HSP (large degree)

We have n_1 real embeddings and n_2 complex embeddings of K.

- We have the natural inclusion $K \hookrightarrow \mathbb{R}^{n_1} \times \mathbb{C}^{n_2}$.
- It follows that $K \hookrightarrow \mathbb{R}^{n_1+n_2} \times \mathbb{Z}_2^{n_1} \times (\mathbb{R}/\mathbb{Z})^{n_2}$.
- Units satisfy $U \hookrightarrow \underbrace{\mathbb{R}^{n_1+n_2-1} \times \mathbb{Z}_2^{n_1} \times (\mathbb{R}/\mathbb{Z})^{n_2}}_{G}$ since $|\mathcal{N}(x)| = 1$.

$$\begin{array}{ccccc} G & \xrightarrow{\varphi} & \text{lattices of } \mathbb{R}^{n_1} \times \mathbb{C}^{n_2} & \xrightarrow{\pi} & \text{Quantum states} \\ x & \longrightarrow & x \cdot \mathcal{O}_K & \longrightarrow & |x \cdot \mathcal{O}_K\rangle \end{array}$$

Eisenträger-Hallgren-Kitaev-Song 14

- $\pi \circ \varphi$ “hides” the unit goup U.
- $\pi \circ \varphi$ satisfies the “HSP properties”.

The S-unit group

The algorithm of Eisenträger-Hallgren-Kitaev-Song only computes the unit group.

- The ideal class group is required to certify the result.

The S-unit group

The algorithm of Eisenträger-Hallgren-Kitaev-Song only computes the unit group.

- The ideal class group is required to certify the result.
- The principal ideal problem (PIP) is relevant in cryptography.

The S-unit group

The algorithm of Eisenträger-Hallgren-Kitaev-Song only computes the unit group.

- The ideal class group is required to certify the result.
- The principal ideal problem (PIP) is relevant in cryptography.

S-units

Let S be a set of prime ideals of $\mathcal{O}_K$, an S-unit is an $x \in K$ satisfying

$$\exists (e_1, .., e_{|S|}) \in \mathbb{Z}^{|S|},\ x \cdot \mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_{|S|}^{e_{|S|}}.$$

The S-unit group

The algorithm of Eisenträger-Hallgren-Kitaev-Song only computes the unit group.

- The ideal class group is required to certify the result.
- The principal ideal problem (PIP) is relevant in cryptography.

S-units

Let S be a set of prime ideals of $\mathcal{O}_K$, an S-unit is an $x \in K$ satisfying

$$\exists (e_1, .., e_{|S|}) \in \mathbb{Z}^{|S|},\ x \cdot \mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_{|S|}^{e_{|S|}}.$$

The S-units are a group U_S of rank $r + |S|$ where r is the rank of U.

The S-unit group

The algorithm of Eisenträger-Hallgren-Kitaev-Song only computes the unit group.

- The ideal class group is required to certify the result.
- The principal ideal problem (PIP) is relevant in cryptography.

S-units

Let S be a set of prime ideals of $\mathcal{O}_K$, an S-unit is an $x \in K$ satisfying

$$\exists (e_1, .., e_{|S|}) \in \mathbb{Z}^{|S|},\ x \cdot \mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_{|S|}^{e_{|S|}}.$$

The S-units are a group U_S of rank $r + |S|$ where r is the rank of U.

- We reduce the computation of U_S to the HSP.

The S-unit group

The algorithm of Eisenträger-Hallgren-Kitaev-Song only computes the unit group.

- The ideal class group is required to certify the result.
- The principal ideal problem (PIP) is relevant in cryptography.

S-units

Let S be a set of prime ideals of $\mathcal{O}_K$, an S-unit is an $x \in K$ satisfying

$$\exists (e_1, .., e_{|S|}) \in \mathbb{Z}^{|S|},\ x \cdot \mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_{|S|}^{e_{|S|}}.$$

The S-units are a group U_S of rank $r + |S|$ where r is the rank of U.

- We reduce the computation of U_S to the HSP.
- We reduce the class group and the PIP to the computation of U_S.

Reducing the S-unit group to HSP (large degree)

Let x an S-unit and $v_i \in \mathbb{Z}$ such that $v_i = v_{\mathfrak{p}_i}$, then

$$x \cdot \mathcal{O}_K \cdot \mathfrak{p}_1^{-v_1} \cdots \mathfrak{p}_{|S|}^{-v_{|S|}} = \mathcal{O}_K.$$

Reducing the S-unit group to HSP (large degree)

Let x an S-unit and $v_i \in \mathbb{Z}$ such that $v_i = v_{\mathfrak{p}_i}$, then

$$x \cdot \mathcal{O}_K \cdot \mathfrak{p}_1^{-v_1} \cdots \mathfrak{p}_{|S|}^{-v_{|S|}} = \mathcal{O}_K.$$

Following the same approach as before, we deduce an embedding

$$U_S \hookrightarrow \underbrace{\mathbb{R}^{n_1+n_2-1} \times \mathbb{Z}_2^{n_1} \times (\mathbb{R}/\mathbb{Z})^{n_2}}_{G} \times \mathbb{Z}^{|S|} := G'$$

Reducing the S-unit group to HSP (large degree)

Let x an S-unit and $v_i \in \mathbb{Z}$ such that $v_i = v_{\mathfrak{p}_i}$, then

$$x \cdot \mathcal{O}_K \cdot \mathfrak{p}_1^{-v_1} \cdots \mathfrak{p}_{|S|}^{-v_{|S|}} = \mathcal{O}_K.$$

Following the same approach as before, we deduce an embedding

$$U_S \hookrightarrow \underbrace{\mathbb{R}^{n_1+n_2-1} \times \mathbb{Z}_2^{n_1} \times (\mathbb{R}/\mathbb{Z})^{n_2}}_{G} \times \mathbb{Z}^{|S|} := G'$$

$$\begin{array}{ccccc} G' & \xrightarrow{\varphi} & \text{lattices of } \mathbb{R}^{n_1} \times \mathbb{C}^{n_2} & \xrightarrow{\pi} & \text{Quantum states} \\ x, (v_i) & \longrightarrow & x \cdot \mathcal{O}_K \cdot \prod_i \mathfrak{p}_i^{-v_i} & \longrightarrow & |x \cdot \mathcal{O}_K \cdot \prod_i \mathfrak{p}_i^{-v_i}\rangle \end{array}$$

Reducing the S-unit group to HSP (large degree)

Let x an S-unit and $v_i \in \mathbb{Z}$ such that $v_i = v_{\mathfrak{p}_i}$, then

$$x \cdot \mathcal{O}_K \cdot \mathfrak{p}_1^{-v_1} \cdots \mathfrak{p}_{|S|}^{-v_{|S|}} = \mathcal{O}_K .$$

Following the same approach as before, we deduce an embedding

$$U_S \hookrightarrow \underbrace{\mathbb{R}^{n_1+n_2-1} \times \mathbb{Z}_2^{n_1} \times (\mathbb{R}/\mathbb{Z})^{n_2}}_{G} \times \mathbb{Z}^{|S|} := G'$$

$$\begin{array}{ccccc} G' & \xrightarrow{\varphi} & \text{lattices of } \mathbb{R}^{n_1} \times \mathbb{C}^{n_2} & \xrightarrow{\pi} & \text{Quantum states} \\ x, (v_i) & \longrightarrow & x \cdot \mathcal{O}_K \cdot \prod_i \mathfrak{p}_i^{-v_i} & \longrightarrow & |x \cdot \mathcal{O}_K \cdot \prod_i \mathfrak{p}_i^{-v_i}\rangle \end{array}$$

B.-Song 14

- $\pi \circ \varphi$ "hides" the unit goup U.

Reducing the S-unit group to HSP (large degree)

Let x an S-unit and $v_i \in \mathbb{Z}$ such that $v_i = v_{\mathfrak{p}_i}$, then

$$x \cdot \mathcal{O}_K \cdot \mathfrak{p}_1^{-v_1} \cdots \mathfrak{p}_{|S|}^{-v_{|S|}} = \mathcal{O}_K.$$

Following the same approach as before, we deduce an embedding

$$U_S \hookrightarrow \underbrace{\mathbb{R}^{n_1+n_2-1} \times \mathbb{Z}_2^{n_1} \times (\mathbb{R}/\mathbb{Z})^{n_2}}_{G} \times \mathbb{Z}^{|S|} := G'$$

$$\begin{array}{ccccc} G' & \xrightarrow{\varphi} & \text{lattices of } \mathbb{R}^{n_1} \times \mathbb{C}^{n_2} & \xrightarrow{\pi} & \text{Quantum states} \\ x, (v_i) & \longrightarrow & x \cdot \mathcal{O}_K \cdot \prod_i \mathfrak{p}_i^{-v_i} & \longrightarrow & |x \cdot \mathcal{O}_K \cdot \prod_i \mathfrak{p}_i^{-v_i}\rangle \end{array}$$

B.-Song 14

- $\pi \circ \varphi$ “hides” the unit goup U.
- $\pi \circ \varphi$ satisfies the “HSP properties”.

Reducing the ideal class group to the S-unit group

Choice of S

Let $\{\mathfrak{p}_1, \cdots, \mathfrak{p}_N\}$ be a set of ideals whose classes generate $\mathrm{Cl}(\mathcal{O})$.

$$\text{Under GRH, } |S| \leq 12 \log^2 |\Delta|.$$

Reducing the ideal class group to the S-unit group

Choice of S

Let $\{\mathfrak{p}_1, \cdots, \mathfrak{p}_N\}$ be a set of ideals whose classes generate $\mathrm{Cl}(\mathcal{O})$.

$$\text{Under GRH, } |S| \leq 12 \log^2 |\Delta|.$$

The S-unit group gives a basis of us all the $(e_1, \cdots, e_N)$ such that

$$\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_N^{e_N} = (\alpha) = 1 \in \mathrm{Cl}(\mathcal{O}) \text{ for some } \alpha \in \mathcal{O}.$$

Reducing the ideal class group to the S-unit group

Choice of S

Let $\{\mathfrak{p}_1, \cdots, \mathfrak{p}_N\}$ be a set of ideals whose classes generate $\mathrm{Cl}(\mathcal{O})$.

$$\text{Under GRH, } |S| \leq 12 \log^2 |\Delta|.$$

The S-unit group gives a basis of us all the $(e_1, \cdots, e_N)$ such that

$$\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_N^{e_N} = (\alpha) = 1 \in \mathrm{Cl}(\mathcal{O}) \text{ for some } \alpha \in \mathcal{O}.$$

This is the kernel of the surjective morphism

$$\begin{array}{ccccc} \mathbb{Z}^N & \xrightarrow{\varphi} & \mathcal{I} & \xrightarrow{\pi} & \mathrm{Cl}(\mathcal{O}) \\ (e_1, \ldots, e_N) & \longrightarrow & \prod_i \mathfrak{p}_i^{e_i} & \longrightarrow & \prod_i [\mathfrak{p}_i]^{e_i} \end{array}$$

Reducing the ideal class group to the S-unit group

Choice of S

Let $\{\mathfrak{p}_1, \cdots, \mathfrak{p}_N\}$ be a set of ideals whose classes generate $\mathrm{Cl}(\mathcal{O})$.

$$\text{Under GRH, } |S| \leq 12 \log^2 |\Delta|.$$

The S-unit group gives a basis of us all the $(e_1, \cdots, e_N)$ such that

$$\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_N^{e_N} = (\alpha) = 1 \in \mathrm{Cl}(\mathcal{O}) \text{ for some } \alpha \in \mathcal{O}.$$

This is the kernel of the surjective morphism

$$\begin{array}{ccccc} \mathbb{Z}^N & \xrightarrow{\varphi} & \mathcal{I} & \xrightarrow{\pi} & \mathrm{Cl}(\mathcal{O}) \\ (e_1, \ldots, e_N) & \longrightarrow & \prod_i \mathfrak{p}_i^{e_i} & \longrightarrow & \prod_i [\mathfrak{p}_i]^{e_i} \end{array}$$

Which gives us $\mathrm{Cl}(\mathcal{O}) \simeq \mathbb{Z}^N / \ker(\pi \circ \varphi)$.

Reducing the PIP to the S-unit group

First step, factor input $\mathfrak{a} = \prod_j \mathfrak{q}_j$ with Shor's algorithm.

Reducing the PIP to the S-unit group

First step, factor input $\mathfrak{a} = \prod_j \mathfrak{q}_j$ with Shor's algorithm.

Choice of S

Let $(\mathfrak{p}_j)_{j \leq N}$ be ideals generating $\mathrm{Cl}(\mathcal{O}_K)$. $S := \{\mathfrak{p}_1, \cdots, \mathfrak{p}_N\} \cup \{\mathfrak{q} \mid \mathfrak{a}\}$.

Reducing the PIP to the S-unit group

First step, factor input $\mathfrak{a} = \prod_j \mathfrak{q}_j$ with Shor's algorithm.

Choice of S

Let $(\mathfrak{p}_j)_{j \leq N}$ be ideals generating $\mathrm{Cl}(\mathcal{O}_K)$. $S := \{\mathfrak{p}_1, \cdots, \mathfrak{p}_N\} \cup \{\mathfrak{q} \mid \mathfrak{a}\}$.

The S-unit group gives a matrix $(a_{i,j})$ such that

$$\mathfrak{p}_1^{a_{i,1}} \cdots \mathfrak{p}_N^{a_{i,N}} = (\alpha_i)$$

Reducing the PIP to the S-unit group

First step, factor input $\mathfrak{a} = \prod_j \mathfrak{q}_j$ with Shor's algorithm.

Choice of S

Let $(\mathfrak{p}_j)_{j \leq N}$ be ideals generating $\mathrm{Cl}(\mathcal{O}_K)$. $S := \{\mathfrak{p}_1, \cdots, \mathfrak{p}_N\} \cup \{\mathfrak{q} \mid \mathfrak{a}\}$.

The S-unit group gives a matrix $(a_{i,j})$ such that

$$\mathfrak{p}_1^{a_{i,1}} \cdots \mathfrak{p}_N^{a_{i,N}} = (\alpha_i)$$

The Hermite form of A has the shape $UA = \left(\frac{H|0}{B|I}\right)$. The matrix U gives us

$$\mathfrak{q}_i = (\beta_i)\mathfrak{p}_1^{b_{i,1}} \cdots \mathfrak{p}_N^{b_{i,N}}.$$

Reducing the PIP to the S-unit group

First step, factor input $\mathfrak{a} = \prod_j \mathfrak{q}_j$ with Shor's algorithm.

Choice of S

Let $(\mathfrak{p}_j)_{j \leq N}$ be ideals generating $\mathrm{Cl}(\mathcal{O}_K)$. $S := \{\mathfrak{p}_1, \cdots, \mathfrak{p}_N\} \cup \{\mathfrak{q} \mid \mathfrak{a}\}$.

The S-unit group gives a matrix $(a_{i,j})$ such that

$$\mathfrak{p}_1^{a_{i,1}} \cdots \mathfrak{p}_N^{a_{i,N}} = (\alpha_i)$$

The Hermite form of A has the shape $UA = \left(\frac{H|0}{B|I}\right)$. The matrix U gives us

$$\mathfrak{q}_i = (\beta_i)\mathfrak{p}_1^{b_{i,1}} \cdots \mathfrak{p}_N^{b_{i,N}}.$$

- We rewrite $\mathfrak{a}$ as a power-product of the $\mathfrak{p}_j$ given by the vector b.
- We solve the linear system $XH = b$.

The daunting question

Given $\mathfrak{a} = (g)$ in $\mathcal{O}_K$ the ring of integers of K. we know how to compute

$$g' \in \mathcal{O}_K, \quad \mathfrak{a} = (g')\mathcal{O}_K$$

- In classical subexponential time.
- In quantum polynomial time.

The daunting question

Given $\mathfrak{a} = (g)$ in $\mathcal{O}_K$ the ring of integers of K. we know how to compute

$$g' \in \mathcal{O}_K, \quad \mathfrak{a} = (g')\mathcal{O}_K$$

- In classical subexponential time.
- In quantum polynomial time.

Moreover, we know the unit group $U = \mu \times \langle \varepsilon_1 \rangle \times \langle \varepsilon_r \rangle$ and all the generators of $\mathfrak{a}$

$$\alpha = g' \cdot \varepsilon_1^{e_1} \cdots \varepsilon_r^{e_r}.$$

The daunting question

Given $\mathfrak{a} = (g)$ in $\mathcal{O}_K$ the ring of integers of K. we know how to compute

$$g' \in \mathcal{O}_K, \quad \mathfrak{a} = (g')\mathcal{O}_K$$

- In classical subexponential time.
- In quantum polynomial time.

Moreover, we know the unit group $U = \mu \times \langle \varepsilon_1 \rangle \times \langle \varepsilon_r \rangle$ and all the generators of $\mathfrak{a}$

$$\alpha = g' \cdot \varepsilon_1^{e_1} \cdots \varepsilon_r^{e_r}.$$

The daunting question : How do we find the small ones ?