Cryptography, hard problems and algorithmic number theory

Alice Pellet-Mary

CNRS et Université de Bordeaux

Présentation scientifique dans le cadre du DOR 2023

Public key cryptography

Cryptographic primitives

public key encryption	signature	homomorphic encryption	$\dots$

Public key cryptography

Cryptographic primitives

public key encryption | signature | homomorphic encryption | $\cdots$

error correcting codes | lattices | isogenies

factoring | discrete logarithm | $\cdots$

(Supposedly intractable) algorithmic problems

Public key cryptography

Cryptographic primitives

public key encryption

signature

homomorphic encryption

...

...

error correcting codes

lattices

isogenies

factoring

discrete logarithm

...

(Supposedly intractable) algorithmic problems

Public key cryptography

Cryptographic primitives

public key encryption

signature

homomorphic encryption

. . .

. . .

error correcting codes

lattices

isogenies

factoring

discrete logarithm

. . .

(Supposedly intractable) algorithmic problems

Today's algorithmic problem

$K = \mathbb{Q}[\sqrt{2}]$

$O_K = \mathbb{Z}[\sqrt{2}]$

Today's algorithmic problem

$K = \mathbb{Q}[\sqrt{2}]$

$O_K = \mathbb{Z}[\sqrt{2}]$

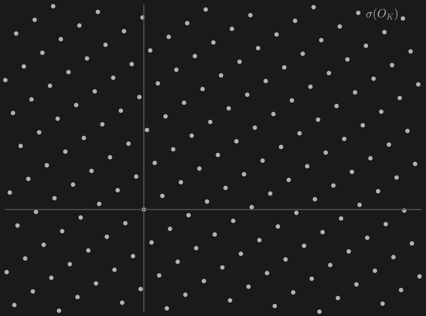
$$\begin{aligned} \sigma : \qquad & K \to \mathbb{R}^2 \\ & x_0 + x_1\sqrt{2} \mapsto (x_0 + x_1\sqrt{2}, x_0 - x_1\sqrt{2}) \end{aligned}$$

Today's algorithmic problem

$K = \mathbb{Q}[\sqrt{2}]$

$O_K = \mathbb{Z}[\sqrt{2}]$

$$\sigma : \quad K \to \mathbb{R}^2$$
$$x_0 + x_1\sqrt{2} \mapsto (x_0 + x_1\sqrt{2}, x_0 - x_1\sqrt{2})$$

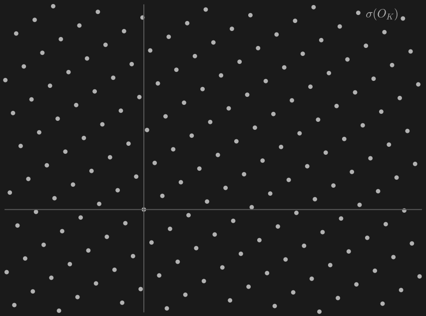


Today's algorithmic problem

$K = \mathbb{Q}[\sqrt{2}]$

$O_K = \mathbb{Z}[\sqrt{2}]$

$$\sigma : \quad K \to \mathbb{R}^2$$
$$x_0 + x_1\sqrt{2} \mapsto (x_0 + x_1\sqrt{2}, x_0 - x_1\sqrt{2})$$



Principal ideal: $\alpha O_K = \{\alpha r \mid r \in O_K\}$ (for some $\alpha \in O_K$)

Today's algorithmic problem

$K = \mathbb{Q}[\sqrt{2}]$

$O_K = \mathbb{Z}[\sqrt{2}]$

$$\sigma: \quad K \to \mathbb{R}^2$$
$$x_0 + x_1\sqrt{2} \mapsto (x_0 + x_1\sqrt{2}, x_0 - x_1\sqrt{2})$$

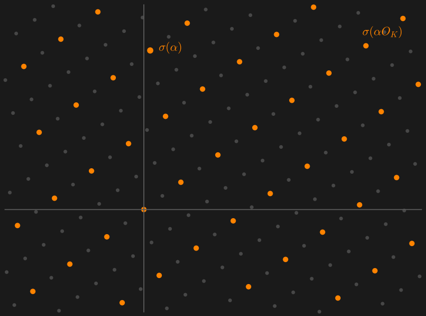
Principal ideal: $\alpha O_K = \{\alpha r \,|\, r \in O_K\}$ (for some $\alpha \in O_K$)

Today's algorithmic problem

$K = \mathbb{Q}[\sqrt{2}]$

$O_K = \mathbb{Z}[\sqrt{2}]$

$$\sigma : \quad K \to \mathbb{R}^2$$
$$x_0 + x_1\sqrt{2} \mapsto (x_0 + x_1\sqrt{2}, x_0 - x_1\sqrt{2})$$



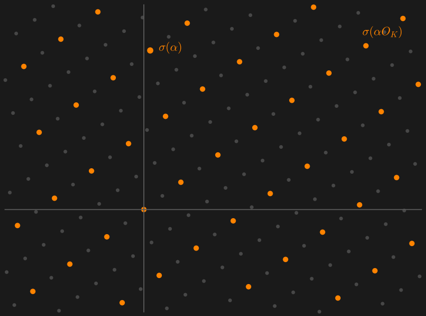
Principal ideal: $\alpha O_K = \{\alpha r \mid r \in O_K\}$ (for some $\alpha \in O_K$)

Today's algorithmic problem

$K = \mathbb{Q}[\sqrt{2}]$

$O_K = \mathbb{Z}[\sqrt{2}]$

$$\sigma : \quad K \to \mathbb{R}^2$$
$$x_0 + x_1\sqrt{2} \mapsto (x_0 + x_1\sqrt{2}, x_0 - x_1\sqrt{2})$$



Principal ideal: $\alpha O_K = \{\alpha r \mid r \in O_K\}$ (for some $\alpha \in O_K$)

ideal-Shortest Vector Problem (ideal-SVP): given α, find $\alpha r \in \alpha O_K$ such that $\|\sigma(\alpha r)\|_2$ is as small as possible (and $\neq 0$)

Short vectors in lattices

ideal-SVP is a special case of the

Shortest Vector Problem (SVP): given a lattice L, find $\vec{v} \in L$ such that $\|\vec{v}\|_2$ is as small as possible (and $\neq 0$)

ideal-SVP is a special case of the

Shortest Vector Problem (SVP): given a lattice L, find $\vec{v} \in L$ such that $\|\vec{v}\|_2$ is as small as possible (and $\neq 0$)

- Famous problem, well studied

Short vectors in lattices

ideal-SVP is a special case of the

Shortest Vector Problem (SVP): given a lattice L, find $\vec{v} \in L$ such that $\|\vec{v}\|_2$ is as small as possible (and $\neq 0$)

- Famous problem, well studied
- Known algorithms scale badly (exponentially) with the dimension n
  - $\rightsquigarrow$ $n = 2$ ☺ (by hand)
  - $\rightsquigarrow$ $n \approx 60$ ☺ (personal laptop)
  - $\rightsquigarrow$ $n = 180$ 😐 (super computer)
  - $\rightsquigarrow$ $n \approx 700$ ☹ (cryptography)

Short vectors in lattices

ideal-SVP is a special case of the

Shortest Vector Problem (SVP): given a lattice L, find $\vec{v} \in L$ such that $\|\vec{v}\|_2$ is as small as possible (and $\neq 0$)

- Famous problem, well studied
- Known algorithms scale badly (exponentially) with the dimension n
  - $\rightsquigarrow$ $n = 2$ ☺ (by hand)
  - $\rightsquigarrow$ $n \approx 60$ ☺ (personal laptop)
  - $\rightsquigarrow$ $n = 180$ 😐 (super computer)
  - $\rightsquigarrow$ $n \approx 700$ ☹ (cryptography)
- Can we exploit the algebraic structure in ideal-SVP?

Short vectors in lattices

ideal-SVP is a special case of the

Shortest Vector Problem (SVP): given a lattice L, find $\vec{v} \in L$ such that $\|\vec{v}\|_2$ is as small as possible (and $\neq 0$)

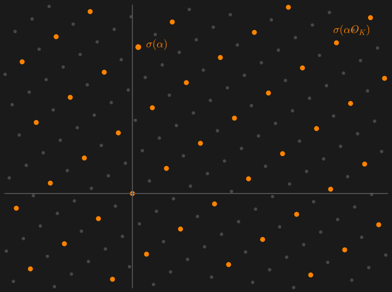
- Famous problem, well studied
- Known algorithms scale badly (exponentially) with the dimension n
  - $\rightsquigarrow$ $n = 2$ ☺ (by hand)
  - $\rightsquigarrow$ $n \approx 60$ ☺ (personal laptop)
  - $\rightsquigarrow$ $n = 180$ 😐 (super computer)
  - $\rightsquigarrow$ $n \approx 700$ ☹ (cryptography)
- Can we exploit the algebraic structure in ideal-SVP?

Remark: there are families of nice lattices in which SVP is easy

Exploiting the algebraic structure

$K = \mathbb{Q}[\sqrt{2}] \quad O_K = \mathbb{Z}[\sqrt{2}] \quad \sigma : x_0 + x_1\sqrt{2} \mapsto (x_0 + x_1\sqrt{2}, x_0 - x_1\sqrt{2})$

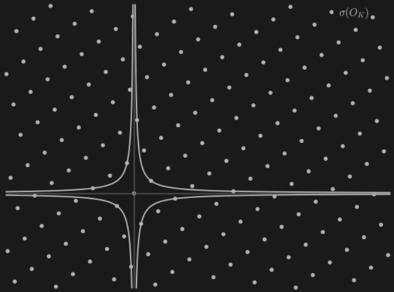
Objective: find a short element in $\alpha O_K = \{\alpha r \mid r \in O_K\}$



Exploiting the algebraic structure

$K = \mathbb{Q}[\sqrt{2}] \quad O_K = \mathbb{Z}[\sqrt{2}] \quad \sigma : x_0 + x_1\sqrt{2} \mapsto (x_0 + x_1\sqrt{2}, x_0 - x_1\sqrt{2})$

Objective: find a short element in $\alpha O_K = \{\alpha r \mid r \in O_K\}$

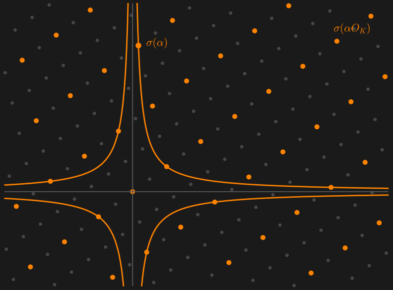


Fact 1: $O_K^\times = \{x_0 + x_1\sqrt{2} \in O_K \mid (x_0 + x_1\sqrt{2})(x_0 - x_1\sqrt{2}) = \pm 1\}$

Exploiting the algebraic structure

$K = \mathbb{Q}[\sqrt{2}] \quad O_K = \mathbb{Z}[\sqrt{2}] \quad \sigma : x_0 + x_1\sqrt{2} \mapsto (x_0 + x_1\sqrt{2}, x_0 - x_1\sqrt{2})$

Objective: find a short element in $\alpha O_K = \{\alpha r \,|\, r \in O_K\}$



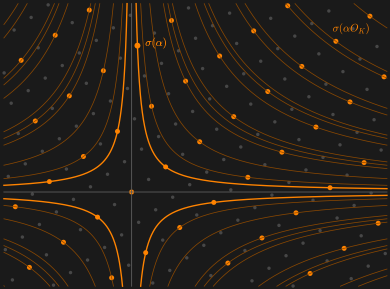
Fact 1: $O_K^\times = \{x_0 + x_1\sqrt{2} \in O_K \,|\, (x_0 + x_1\sqrt{2})(x_0 - x_1\sqrt{2}) = \pm 1\}$

Fact 2: $\alpha O_K = \beta O_K \Leftrightarrow \alpha = \beta \cdot u$ for some $u \in O_K^\times$

Exploiting the algebraic structure

$K = \mathbb{Q}[\sqrt{2}] \quad O_K = \mathbb{Z}[\sqrt{2}] \quad \sigma : x_0 + x_1\sqrt{2} \mapsto (x_0 + x_1\sqrt{2}, x_0 - x_1\sqrt{2})$

Objective: find a short element in $\alpha O_K = \{\alpha r \mid r \in O_K\}$



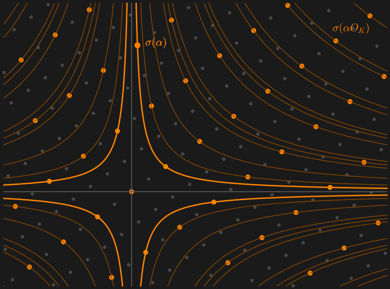
Fact 1: $O_K^\times = \{x_0 + x_1\sqrt{2} \in O_K \mid (x_0 + x_1\sqrt{2})(x_0 - x_1\sqrt{2}) = \pm 1\}$

Fact 2: $\alpha O_K = \beta O_K \Leftrightarrow \alpha = \beta \cdot u$ for some $u \in O_K^\times$

Exploiting the algebraic structure

$K = \mathbb{Q}[\sqrt{2}]$ $\quad O_K = \mathbb{Z}[\sqrt{2}]$ $\quad \sigma : x_0 + x_1\sqrt{2} \mapsto (x_0 + x_1\sqrt{2}, x_0 - x_1\sqrt{2})$

Objective: find a short element in $\alpha O_K = \{\alpha r \mid r \in O_K\}$



Idea:

- focus on finding $u \in O_K^\times$ s.t. $\|\sigma(\alpha u)\|$ is minimal

Exploiting the algebraic structure

$K = \mathbb{Q}[\sqrt{2}] \quad O_K = \mathbb{Z}[\sqrt{2}] \quad \sigma : x_0 + x_1\sqrt{2} \mapsto (x_0 + x_1\sqrt{2}, x_0 - x_1\sqrt{2})$

Objective: find a short element in $\alpha O_K = \{\alpha r \mid r \in O_K\}$

Idea:

- focus on finding $u \in O_K^\times$ s.t. $\|\sigma(\alpha u)\|$ is minimal
- take the $\log(|\cdot|)$ coordinate-wise (Log)
  - $\rightsquigarrow$ $\mathrm{Log}(\{\alpha u \mid u \in O_K^\times\}) = \mathrm{Log}(\alpha) + \mathrm{Log}(O_K^\times)$ is a shifted lattice
  - $\rightsquigarrow$ for some K, $\mathrm{Log}(O_K^\times)$ is a nice lattice (nicer than $\sigma(\alpha O_K)$)
  - $\rightsquigarrow$ use lattice algorithms here!

Summing up

Motivation: cryptography

Tools:

- algorithmic number theory
- complexity theory

Motivation: cryptography

Tools:

- algorithmic number theory
- complexity theory

Thank you