Efficient arithmetic for cryptography and cryptanalysis

Édouard Rousseau

Math Innov day

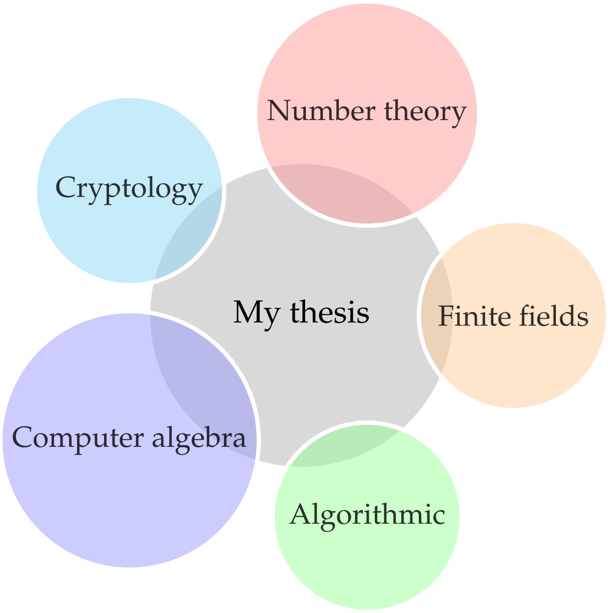
UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES

université PARIS-SACLAY

MATH INNOV

îledeFrance

TELECOM ParisTech



Number theory

Cryptology

My thesis

Finite fields

Computer algebra

Algorithmic

Some recalls

Some recalls

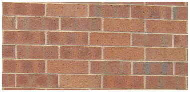
Definition (Wall)

Construction used for shelter, protection, or privacy, etc.

Some recalls

Definition (Wall)

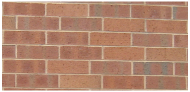
Construction used for shelter, protection, or privacy, etc.



Some recalls

Definition (Wall)

Construction used for shelter, protection, or privacy, etc.



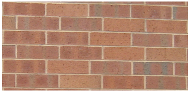
Definition (Door)

Part of a wall that can be opened to enter inside the walls.

Some recalls

Definition (Wall)

Construction used for shelter, protection, or privacy, etc.



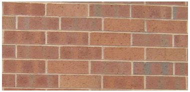
Definition (Door)

Part of a wall that can be opened to enter inside the walls.

Some recalls

Definition (Wall)

Construction used for shelter, protection, or privacy, etc.



Definition (Door)

Part of a wall that can be opened to enter inside the walls.

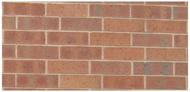
Definition (Lock and key)

Device for securing a door: a *locked* door can only be opened with the associated *key*.

Some recalls

Definition (Wall)

Construction used for shelter, protection, or privacy, etc.



Definition (Door)

Part of a wall that can be opened to enter inside the walls.

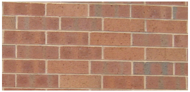
Definition (Lock and key)

Device for securing a door: a *locked* door can only be opened with the associated *key*.

Some recalls

Definition (Wall)

Construction used for shelter, protection, or privacy, etc.



Definition (Door)

Part of a wall that can be opened to enter inside the walls.

Definition (Lock and key)

Device for securing a door: a *locked* door can only be opened with the associated *key*.

Definition (Cryptology)

The art/science of building walls, doors, locks and keys for protecting informations.

ⓘ 🔒 https://www.

Goal of the thesis

= Number theory

= Algorithmically hard problems

- Goal: study the material used to craft locks and keys to better understand how to open the doors.

Goal of the thesis

= Number theory

= Algorithmically hard problems

- Goal: study the material used to craft locks and keys to better understand how to open the doors.
- Goal: (maths) study the algebraic structures used in the hard problems to better understand how to efficiently solve them.

WHAT *exactly* DID I STUDY?

- If $\ell \mid m$, then $\mathbb{F}_{p^\ell} \hookrightarrow \mathbb{F}_{p^m}$
- If $\ell \mid m \mid n$, then $\mathbb{F}_{p^\ell} \hookrightarrow \mathbb{F}_{p^m} \hookrightarrow \mathbb{F}_{p^n}$

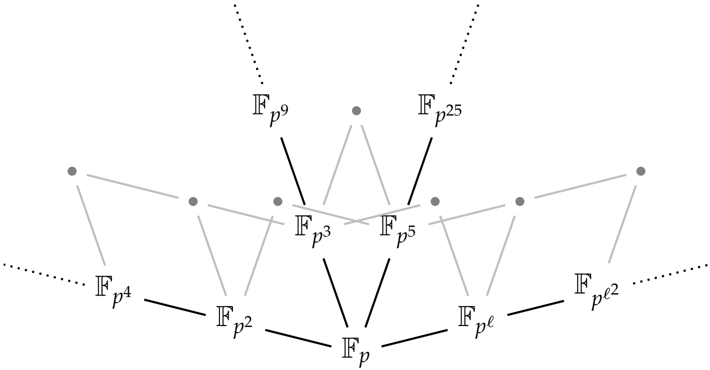
$$\begin{tikzcd}
 & G & \\
 & & F \arrow[ul, "\phi_{F\hookrightarrow G}"'] \\
E \arrow[uur, "\phi_{E\hookrightarrow G}"] \arrow[urr, "\phi_{E\hookrightarrow F}"'] & &
\end{tikzcd}$$

What *exactly* did I study?

- If $\ell \mid m$, then $\mathbb{F}_{p^\ell} \hookrightarrow \mathbb{F}_{p^m}$
- If $\ell \mid m \mid n$, then $\mathbb{F}_{p^\ell} \hookrightarrow \mathbb{F}_{p^m} \hookrightarrow \mathbb{F}_{p^n}$

$$\begin{tikzcd}
 & G & \\
 & & F \arrow[ul, "\phi_{F\hookrightarrow G}"'] \\
E \arrow[uur, "\phi_{E\hookrightarrow G}"] \arrow[urr, "\phi_{E\hookrightarrow F}"'] & &
\end{tikzcd}$$

$$\phi_{F\hookrightarrow G} \circ \phi_{E\hookrightarrow F} \overset{?}{=} \phi_{E\hookrightarrow G}$$



Thanks for your attention!