M1 MoSIG/Info/AM: elective course
Algebraic Algorithms for Cryptology

Clément Pernet

November 14, 2024

Motivation

What is Algebraic Computing ?

The art (algorithmic, implementation, etc) of computing with objects from algebra or arithmetic:

- integers,
- polynomials,
- group or field elements, etc

Motivation

What is Algebraic Computing ?

The art (algorithmic, implementation, etc) of computing with objects from algebra or arithmetic:

- integers,
- polynomials,
- group or field elements, etc

Why do we care ?

- **Security** in crypto (often) relies on the existence of classes of **algorithmic problems** that are either difficult or easy
- Arithmetic and Algebra are excellent providers of such problems

Motivation

Get familiar with the algorithmic foundations of cryptology and related topics

- Study and design algorithms for algebra and arithmetic
- Analyse their complexity in various cost models
- Closer look at how the algorithms behave in real life (implementations, and hardware optimizations)

Content

Integer and Polynomial arithmetic

- Multiplication, GCD, exponentiaton, etc
- Towards the fastest asymptotic complexities
- Software / Hardware implementation

Content

Integer and Polynomial arithmetic

- Multiplication, GCD, exponentiaton, etc
- Towards the fastest asymptotic complexities
- Software / Hardware implementation

Finite fields

- (a bit) of mathematical context
- Their algorihtmic
- Software / Hardware implementation

Content

Integer and Polynomial arithmetic

- Multiplication, GCD, exponentiaton, etc
- Towards the fastest asymptotic complexities
- Software / Hardware implementation

Finite fields

- (a bit) of mathematical context
- Their algorihtmic
- Software / Hardware implementation

Applications

- Coding theory (algebraic error correcting codes)
- Algorithmic of asymmetric ciphers

Organisation

- 1.5h per week of CTD (mixing lecture and tutorial)
- Evaluation: homework with implementation project

Organisation

- 1.5h per week of CTD (mixing lecture and tutorial)
- Evaluation: homework with implementation project

Joint UE with Introduction to Cryptology (B. Grenet)

- Strong connection of the contents
- Highly recommended to follow the 2 options for applying in Master2 Cybersecurity
    - If you validate both UE and your M1 $\Rightarrow$ automatically admitted to M2 Cybersecurity