Advanced Cryptography

Introduction

Christophe Petit

University of Oxford

Introduction to Cryptography

- Modern foundations : cryptography definitions, proof by reductions, (trapdoor) one-way functions
- Symmetric and public key cryptography
- Basic signature and encryption schemes ; hash functions
- Discrete logarithms and factorization problems, with some basic algorithms to solve them

This course

- Introduction to some advanced cryptography topics
  - Encryption and signature schemes based on problems different from discrete logarithms and factorization
  - Further cryptographic primitives and protocols
  - Advanced cryptanalysis techniques
- Soft introduction to cryptography research, with pointers to literature for further learning (ask me for related projects !)
- A glimpse at the breadth of (mathematical) cryptography, with cool applications of nice Mathematics areas

Tentative contents for this year

(based on your preferences and my own biases)

- Elliptic curve cryptography
- Lattice-based cryptography
- Quantum algorithms for cryptanalysis
- Isogeny-based cryptography

Bonus slides
(not covered in class)

- Basic algorithmic number theory
- Advanced discrete logarithm and factoring algorithms

Other advanced topics, a priori not covered
(ask me for references if interested)

- Zero-knowledge proofs of knowledge
- Multiparty computation
- Multivariate cryptography and algebraic attacks
- Side-channel and fault attacks
- Cryptographic hash functions from group theory
- ...

Course prerequisites

- Introduction to cryptography
- Basic algebra and number theory courses
- Basic complexity theory notions
- Knowledge of Magma or Sage
- Willingness to do some basic programming

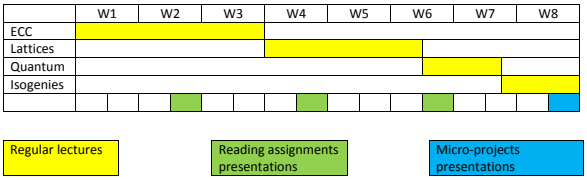
Learning methods

- Regular lectures
  - Slides will be provided (please report typos & errors)
- Group and individual learning and presentations
  - Group presentations based on reading assignments
  - Individual presentations on a chosen "micro-project" (all different, chosen from a list by week 4)
- Mini-project for the course will involve content from both regular lectures and presentations

Learning methods (2)

- Self-learning from reference books and surveys
- Self-learning by implementing your favorite algorithms (mini-project likely to include some implementation too)
- On-demand office hours

Tentative schedule



- Schedule will be re-evaluated after 3 weeks, and more topics will be added if needed (tell me about your preferences!)

My expectations

- Do all assignments and your individual micro-project
- Be committed to learning, also beyond the course
- Ask questions! don't stay behind schedule
- Be critical and give feedback
- Ask me for more literature references if needed
- Let me know your favorite extra cryptography topic in case we run ahead of schedule
- Attend our cryptography seminars (Wednesdays 3pm)

Your expectations

- Tell me about them!

Let's start !

- **Elliptic curve cryptography**
- Lattice-based cryptography
- Quantum algorithms for cryptanalysis
- Isogeny-based cryptography