Quantum-Safe Cryptography
[M2 QMI] Syllabus

Romain Alléaume, Ludovic Perret

1 Course Description

The advent of fault-tolerant application scale (FASQ) machines would radically jeopardize the security of current public-key cryptography. Conversely, quantum communications, combined with existing classical and quantum processors, can be used to perform cryptographic tasks that cannot be achieved only with quantum means. Understanding modern cryptography, and the transition towards so-called post-quantum cryptography (PQC), and understanding quantum cryptography (QC) and its positioning and possible combination with PQC is therefore central for the future of cryptography. The objective of this course is to present the fundamentals of modern cryptography and of quantum cryptography, and to equip the students with a vision of the efforts, challenges and opportunities associated with the ongoing quantum-safe transition.

2 Prerequisites

- Linear algebra
- Information theory basics: channel, entropy, capacity, linear codes

3 Lectures

1. Introduction
    - Crypto goals and tools (security properties, primitives), OTP and perfect secrecy, symmetric and public-key cryptography (high-level);
    - How to measure and prove the security (ITS, Computational approach, reductionist approach)
    - Cryptography in a quantum world (quantum threat and impact on symmetric / asymetric crypto, intro to PQC)
    - Quantum Cryptography goals and tools (no-cloning, q money, introduction of future lectures)

2. Quantum Key Distribution Theory
    - Conjugate Coding
    - BB84 protocol and post-processing
    - QKD Security definition, BB84 Security proof
3. Quantum Key Distribution in practice
    - TD Individual Attacks on BB84
    - QKD protocols and technology, DV-QKD, CV-QKD
    - Quantum Networks
4. Hash-Based Signature Schemes
    - Security of hash functions
    - Hash data structure (Merkle Tree, Hash chains, ...)
    - One-Time Signature schemes (Lamport, Wintermitz)
    - Few-time Signature schemes (XMSS)
    - SHL-DSA
5. Design of Post-Quantum Digital Signature Schemes (DSS)
    - Overview of main hard problems (Lattice-based, code-based, multivariate-based)
    - Main approaches to design post-quantum DSS
        - Trapdoor-one way function (Falcon)
        - Zero-knowledge and Fiat-Shamir (Dilithium)
6. Design of Post-Quantum Key-Encapsulation Mechanism (KEM) and beyond
    - From PKE to KEM (FO transform)
        - Kyber
    - Advanced pq functionalities (homomorphic)
7. Modern topics in Q Cryptography
    - Secure Delegation of Quantum Computing
    - Quantum Two-Party Cryptography: from No-Go theorem to constructions in MiniQCrypt, Impagliazzo cryptographic worlds.
    - Uncloneable Quantum Cryptography
8. Quantum-Safe Networks
    - Motivation: cryptographic tools for QKD networks
    - Main initiatives
    - Hybrid schemes to secure data at rest

4 Evaluation

- Written Exam