Post quantum cryptography

- A big picture of cryptographic algorithms
- The quantum threats
- What is quantum-key distribution and what is post-quantum cryptography
- Why we need to care post-quantum cryptography now
- The status of NIST’s project on post-quantum cryptography
- Candidates of post-quantum cryptography (lattice, hash, isogeny, etc.)

Fully homomorphic encryption

- What is fully homomorphic encryption (FHE)
- Partially homomorphic encryption
    - Multiplicative homomorphic encryption, RSA
    - Additive homomorphic encryption, Paillier
- Somewhat homomorphic encryption from lattice
- Bootstrapping
- 4 Generations of FHE
- Applications of FHE