Course 2-12-1, Room 1002

- [Link](https://wikimpri.dptinfo.ens-cachan.fr/doku.php?id=cours:c-2-12-1)
- 12h on Lattice-based Cryptography
- 12h on Zero-Knowledge and Searchable Encryption by Brice Minaud
Lattice-based Cryptography

Phong Nguyễn

September 2022
Announcement

- Thanks to ERC funding, I offer Internship/PhD/Post-doc positions at ENS/Inria.
  - M2 internship proposals.
  - Other crypto offers at ENS: B. Minaud and D. Pointcheval.
A long time ago...
Sphere Packings
The Hexagonal Packing
Kepler’s “Conjecture”


Perrin (Nobel 1926) used the conjecture to estimate Avogadro constant.
In 2016, Viazovska et al. proved that the best sphere packings in dimensions 8 and 24 are lattice packings: $E_8$ and the Leech lattice.
Another motivation...
300 BC: Euclid’s Algorithm

- **Input**: two integers $a \geq b \geq 0$.
- **Output**: $\gcd(a, b)$.

While $b \neq 0$

- $a := a \mod b$
- Swap$(a, b)$

Return$(a)$
1773: Given \((n,a,b,c)\), Lagrange answers if \(n\) of the form \(ax^2 + bxy + cy^2\)

1850: Hermite invents an \(n\)-dimensional analogue of Lagrange's algorithm for positive definite quadratic forms.
The Ubiquity of Lattices

- Applications in computer science, statistical physics, etc.

- In mathematics
  - Algebraic number theory, Algebraic geometry, Sphere packings, etc.

Context
Context

- **Lattices** have become a buzzword in cryptography.
- Fully-Homomorphic Encryption
- Worst-case to Average-case Reductions
- Post-Quantum Cryptography

The goal of this course is to understand the applications of lattices to algorithms, complexity and cryptography.
Milestones

- **1978**: The Merkle-Hellman Cryptosystem
- **1996**: Ajtai’s SIS reduction and the first lattice cryptosystems (NTRU, Ajtai-Dwork, GGH...)
- **2005**: Regev’s LWE (Gödel Prize 2018)
- **2009**: Gentry’s fully-homomorphic encryption based on lattices.
- **2017–**: NIST’s post-quantum crypto standardization.
1994: Shor’s Breakthrough

[FOCS ’94]: A quantum computer can factor and extract discrete logarithms efficiently.

\[ N = pq \]

\[ y = g^x \]
The Quantum Menace

- 2006: creation of the Post-Quantum Cryptography conference.
- It was a small conference until...
2014: GCHQ released a quantum attack on their own lattice-based cryptosystem.

2015: NSA announced a transition to post-quantum cryptography: cryptographic algorithms resistant to quantum computers.
2018–28: €1billion for quantum technologies. Special funds in UK, France, Germany, Netherlands...

2018–23: €1billion.

Much more in China.

Google, IBM, Microsoft, Intel/TUDelft, Alibaba/CAS, etc.
In 2016, NIST announced a call for post-quantum standards:

- 5 security levels
- Public-key encryption
- Signature
Post-Quantum Candidates

- **Lattices**: TLS-prototype tested several months by Chrome/Google
- Coding theory
- Multivariate polynomials over finite fields
- Elliptic curve isogenies
The NIST Competition

- 2017: 64 Round-1 candidates: 40% lattices.
- 2022: 4 standards: 75% (3) lattices.
  - requests adoption by 2035
  - request hybrid adoption by 2025
4 NIST Standards

- KEM/encryption (1):
  - Crystals-Kyber: **El Gamal** using MLWE lattices

- Signatures (3)
  - Crystals-Dilithium: **Schnorr/Fiat-Shamir** with aborts using MLWE
  - Falcon: **Rabin/GGH-GPV** using NTRU lattices
  - Sphincs+: Hash-based

- Might still be affected by patents.
This course

- Lattices in Algorithms, Complexity and Cryptography
- Lattice Analogues of:
  - RSA: Encryption with Trapdoors
  - Diffie-Hellman key exchange
  - El Gamal: Encryption without Trapdoors
  - Rabin signatures
- Attacks
Lattice-based Cryptography
RSA cryptography uses finite (abelian) groups of hidden order, typically \( G = (\mathbb{Z}/N\mathbb{Z})^\times \) where \( N = pq \).

Because the order can be recovered in subexponential time by factoring, the group must be large: 2048 bits, 4096 bits, etc.
To speed things up, **Elliptic curve crypto** uses **smaller** groups (of known order): elliptic curves over finite fields.

- The best ECDL classical attack runs in exponential time, thus the group can be chosen much smaller than an RSA group.

- Although the group operations are more expensive, it is globally faster.
Lattice Cryptography

- To speed things up, lattice crypto instead uses larger groups with cheaper operations: an additive finite abelian group such as \( \mathbb{Z}/p\mathbb{Z} \) or \( (\mathbb{Z}/q\mathbb{Z})^n \).

- Sometimes, the best attack runs in time subexponential in the group size, yet exponential in the lattice dimension.