

LATTICE-BASED CRYPTOGRAPHY

PHONG NGUYEN

<http://www.di.ens.fr/~pnguyen>

September 2026



**A LONG TIME
AGO...**



SPHERE PACKINGS



THE HEXAGONAL PACKING



KEPLER'S "CONJECTURE"

- Kepler's Conjecture

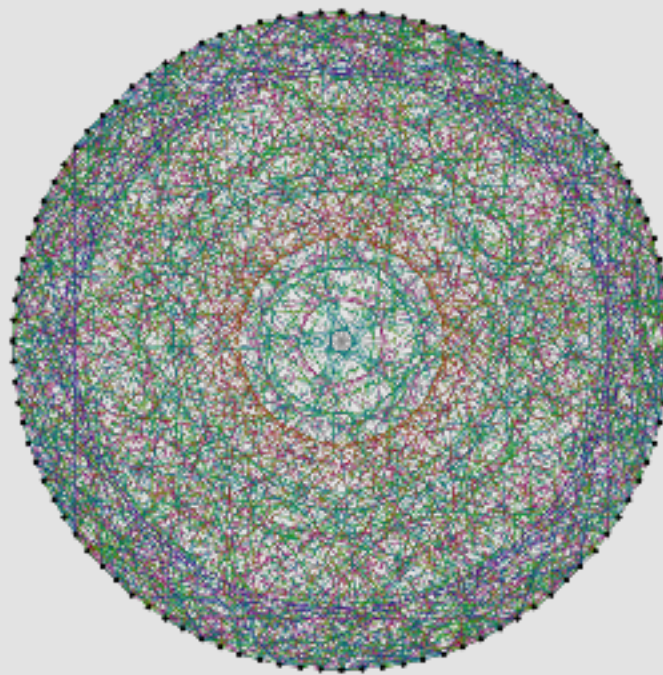


- « proved » by Hales (1998, 2005, 2014).



HIGHER DIMENSIONS

- 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.



Maryna Viazovska

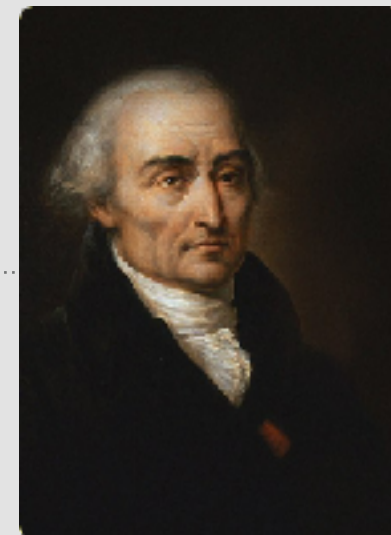
ANOTHER MOTIVATION...

300 BC: EUCLID'S ALGORITHM

- **Input:** two integers $a \geq b \geq 0$.
- **Output:** $\gcd(a, b)$.
- While $b \neq 0$
 - $a := a \bmod b$
 - Swap(a, b)
- Return(a)

GENERALIZATIONS

- 1773: Given (n,a,b,c) , Lagrange answers if n of the form $ax^2+bx+cy^2$
- 1850: Hermite invents an n -dimensional analogue of Lagrange's algorithm for positive definite quadratic forms.



Joseph-Louis Lagrange

Extraits de lettres de M. Ch. Hermite à M. Jacobi sur différents objets de la théorie des nombres.

Première lettre.

Près de deux années se sont écoulées, sans que j'aie encore répondu à la lettre pleine de bonté, que Vous m'avez fait l'honneur* de m'écrire*). Aujourd'hui, je viens Vous supplier de me pardonner ma longue négligence, et Vous exprimer toute la joie, que j'ai ressentie en me voyant une place dans le recueil de Vos oeuvres. Depuis long-temps éloigné du travail, j'ai été bien touché d'un tel témoignage de Votre bienveillance; permettez-moi, Monsieur, de croire qu'elle ne m'abandonnera pas; elle me devient encore en quelque sorte d'un plus grand prix, en me sentant, après un long intervalle ramené de nouveau à l'étude, sur la voie de quelques unes de vos pensées.



Charles Hermite

THE UBIQUITY OF LATTICES

- Applications in computer science, statistical physics, etc.
- In mathematics:
 - Algebraic number theory, Algebraic geometry, Sphere packings, etc.
 - Fields medals: G. Margulis (1978), E. Lindenstrauss and S. Smirnov (2010), M. Bhargava (2014), A. Venkatesh (2018), M. Viazovska (2022).

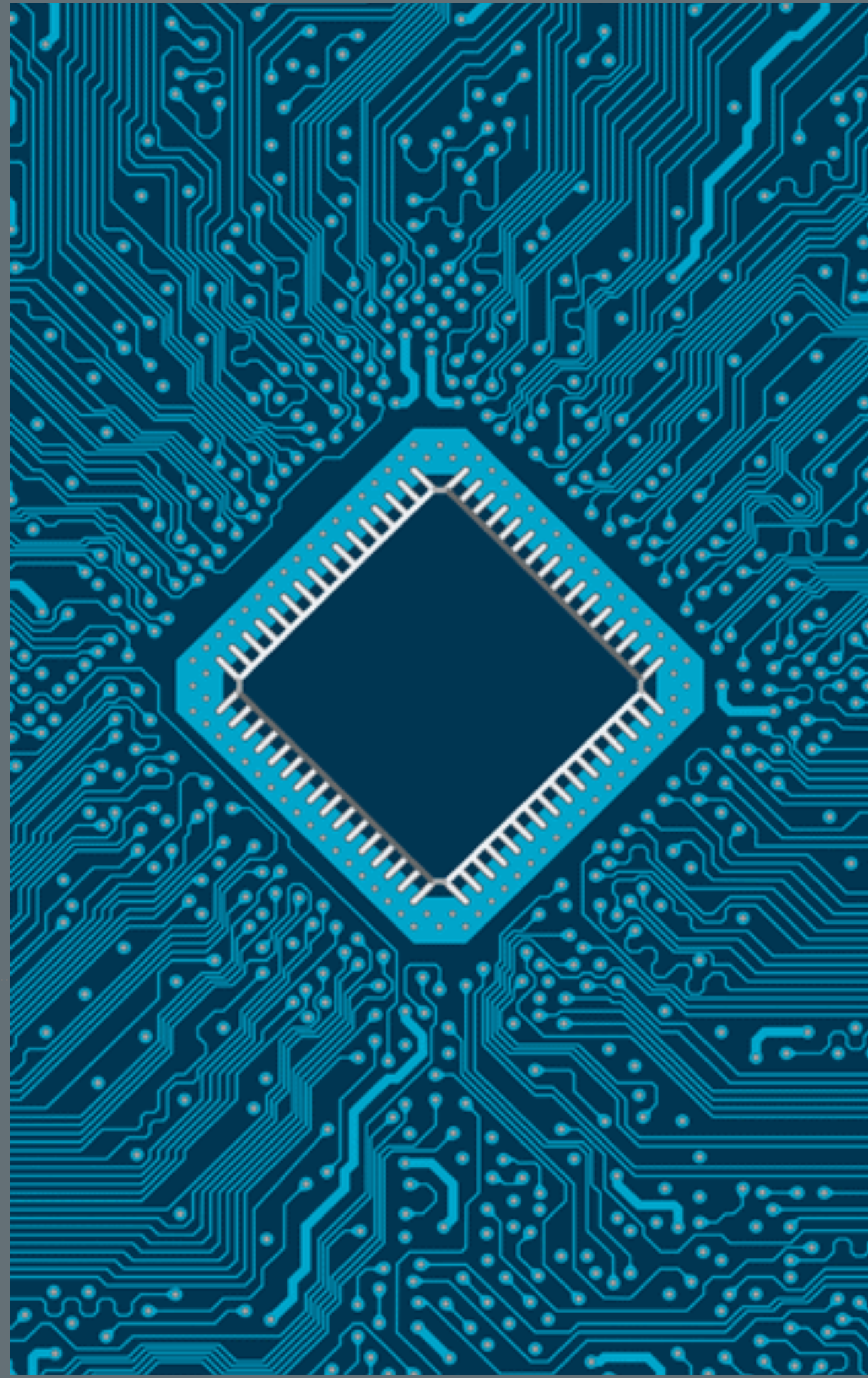


Akshay Venkatesh



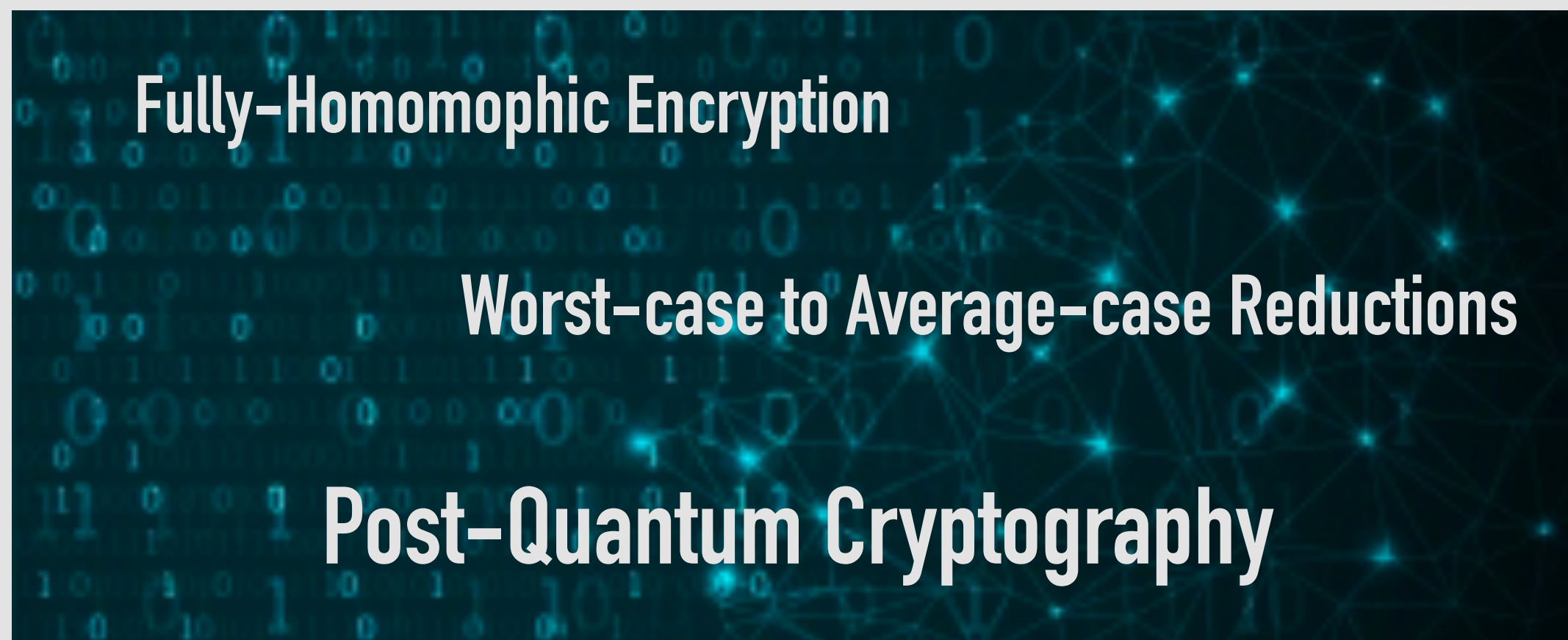
Maryna Viazovska

CONTEXT



CONTEXT

- **Lattices** have become mainstream in cryptography.



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

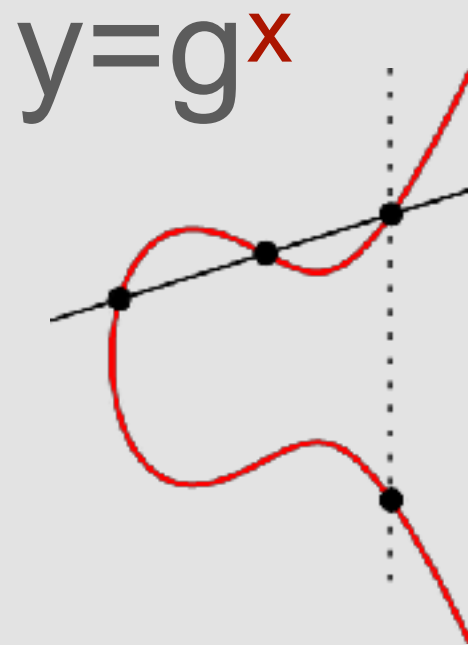
MILESTONES

- **1978**: The Merkle-Hellman Cryptosystem
- **1982**: **First use of lattices in crypto**: breaking Merkle-Hellman.
- **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.
- **2017-2022**: NIST's post-quantum crypto standardization.

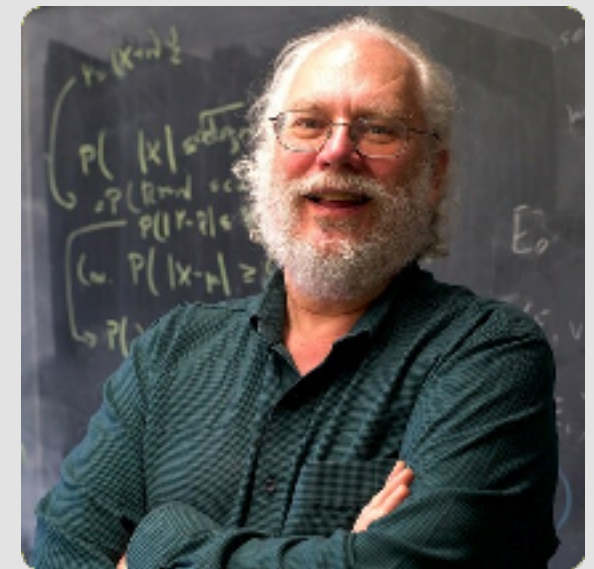
1994: SHOR'S BREAKTHROUGH

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

$$N=pq$$



RSA



Peter Shor

THE QUANTUM MENACE

- 2006: creation of the [Post-Quantum Cryptography](#) conference.



- It was a small conference until...



THE QUANTUM MENACE

- **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.



THE QUANTUM WAVE

- 2018-28:  €1billion for quantum technologies.
- 2018-23:  €1billion.
- Much more in China.



THE NIST COMPETITION

- 2016: NIST announced a call for **post-quantum standards**.



- 5 security levels
- Public-key encryption
- Signature

POST-QUANTUM CANDIDATES

- Lattices
- Coding theory
- Multivariate polynomials over finite fields
- Elliptic curve isogenies

Many changes over the summer



POST-QUANTUM
CRYPTOGRAPHY

THE NIST COMPETITION

- 2017: 64 Round-1 candidates: 40% lattices
 - 2022: 4 standards: 75% (3) lattices
-
- NSA requests adoption by 2030
 - EU request hybrid adoption by 2030 for critical cases



5 NIST STANDARDS (2 PUBLISHED IN 2024)

- KEM / encryption (1):
 - **Crystals-Kyber**: El Gamal using MLWE lattices
 - HQC based on quasi-cyclic codes
- Signatures (3)
 - **Crystals-Dilithium**: Schnorr / Fiat-Shamir with aborts using MLWE
 - **Falcon**: Rabin / GGH-GPV using NTRU lattices
 - **Sphincs+**: Hash-based

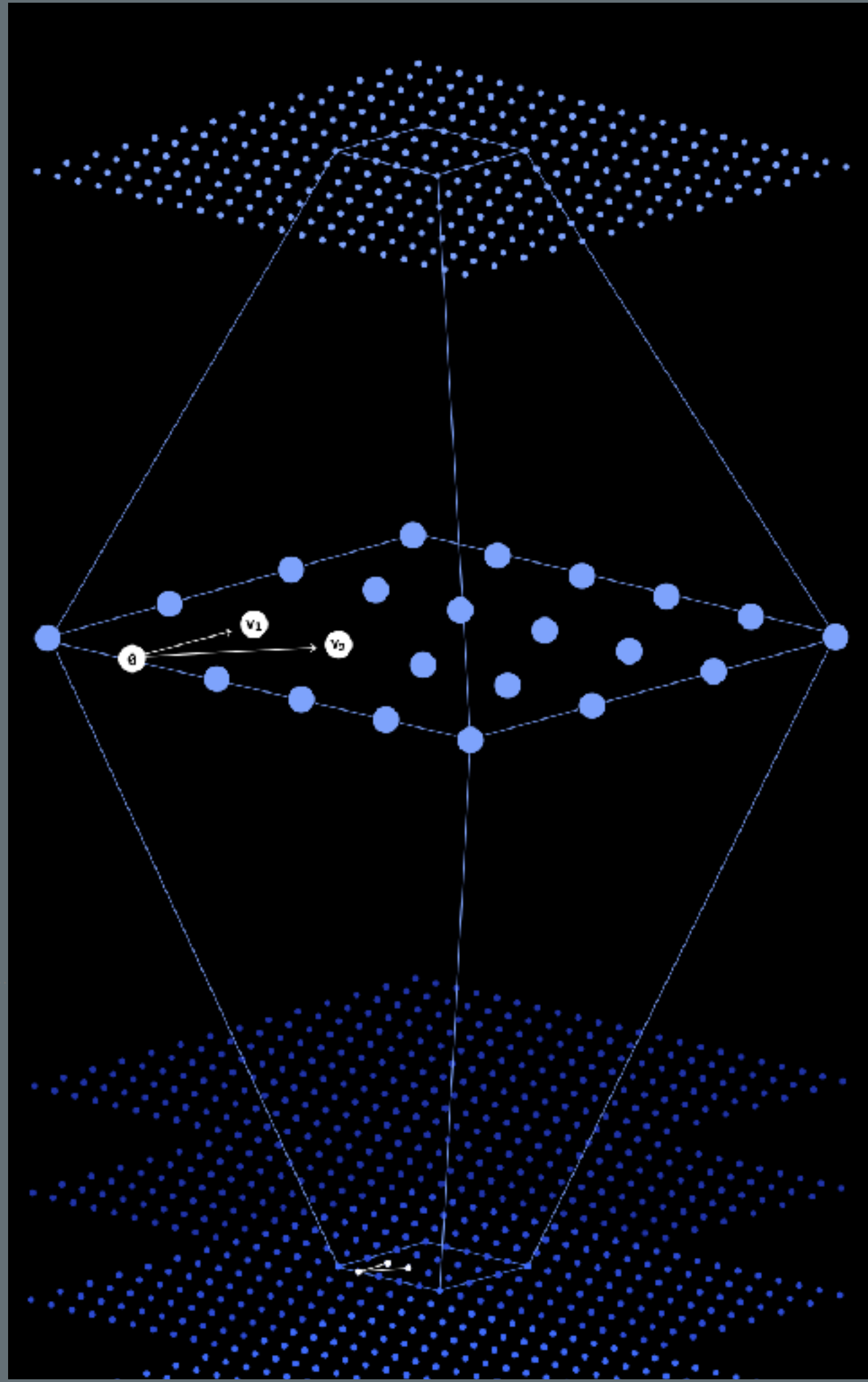


Kyber and Dilithium are already implemented in OpenSSL

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 and Schnorr signatures
- **Lattice Attacks.**
- **Homomorphic encryption**

LATTICE-BASED CRYPTOGRAPHY



CLASSICAL PUBLIC-KEY CRYPTOGRAPHY

- **RSA cryptography** uses finite (abelian) groups of hidden order, typically $G=(\mathbb{Z}/N\mathbb{Z})^\times$ where $N=\mathbf{pq}$.
- Because the order can be recovered in sub-exponential time by factoring, the group must be large: 2048 bits, 4096 bits, etc.

CLASSICAL PUBLIC-KEY CRYPTOGRAPHY

- 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** uses **larger** groups with cheaper operations: an additive finite abelian group, typically $(\mathbb{Z}/q\mathbb{Z})^n$ with small q or $(\mathbb{Z}/q\mathbb{Z})$ with a large q .
- Sometimes, the best attack runs in time sub-exponential in the group size, yet exponential in the lattice dimension.