

# Lattice-based Cryptography: An Overview

Why Lattice is the Future of  
Post-Quantum Zero-Knowledge Blockchain

Kurt Pan

The ZKPunk Organization

June 17, 2025



# Outline

- 1 What is Lattice-based Cryptography?
- 2 Why Do We Need Lattice-based Cryptography?
  - Math: The Universal Language
  - Complexity / TCS
  - Cryptanalysis: The Lattice Sword
  - Post-Quantum Security
  - Performance: Classical Meets Post-Quantum
- 3 How Does Lattice-based Cryptography Shape the Future?
- 4 Conclusion

## Section 1

What is Lattice-based Cryptography?

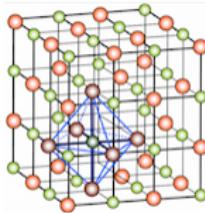
# What is a Lattice?

## Definition

A lattice is a regular grid of points in high-dimensional space.

## Intuition

Think of a 2D lattice as a chain-link fence pattern extended to hundreds of dimensions—the mathematical structure is simple, but finding optimal solutions becomes exponentially difficult as dimensions increase.



# What is a Lattice (Mathematically)?

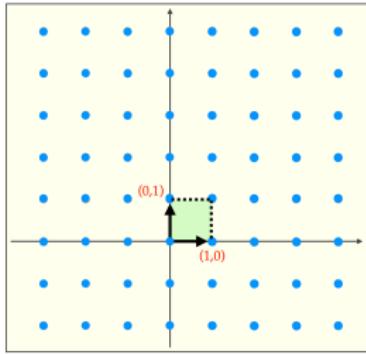
## Definition (Lattice)

A discrete additive subgroup of  $\mathbb{R}^n$

A lattice is the set of all *integer* linear combinations of (linearly independent) *basis* vectors  $\mathbf{B} = \{\mathbf{b}_1, \dots, \mathbf{b}_n\} \subset \mathbb{R}^n$  :

$$\mathcal{L} = \sum_{i=1}^n \mathbf{b}_i \cdot \mathbb{Z} = \{\mathbf{Bx} : \mathbf{x} \in \mathbb{Z}^n\}$$

The same lattice has (infinite) many bases.



# Core Hard Problems

## Shortest Vector Problem (SVP)

Given a lattice, find the shortest non-zero vector

- **Classical algorithms:** Require  $2^{0.384n}$  time—exponential even with massive computers
- **Quantum resistance:** Best quantum algorithms still need  $2^{0.312n}$  time—no polynomial speedup like factoring

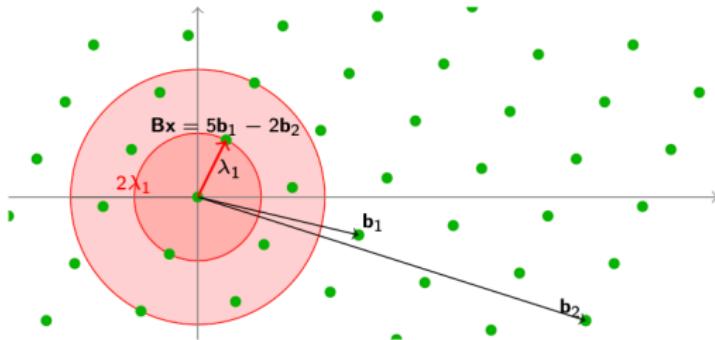
## Learning With Errors (LWE)

Solving noisy linear equations: Given samples  $(a_i, b_i)$  where  $b_i = \langle a_i, s \rangle + e_i \pmod{q}$ , recover secret  $s$  from noisy data.

# Shortest Vector Problem

## Definition (SVP $_{\gamma}$ )

Given a lattice  $\mathcal{L}(\mathbf{B})$ , find a (nonzero) lattice vector  $\mathbf{Bx}$  (with  $\mathbf{x} \in \mathbb{Z}^k$ ) of length (at most)  $\|\mathbf{Bx}\| \leq \gamma \lambda_1$



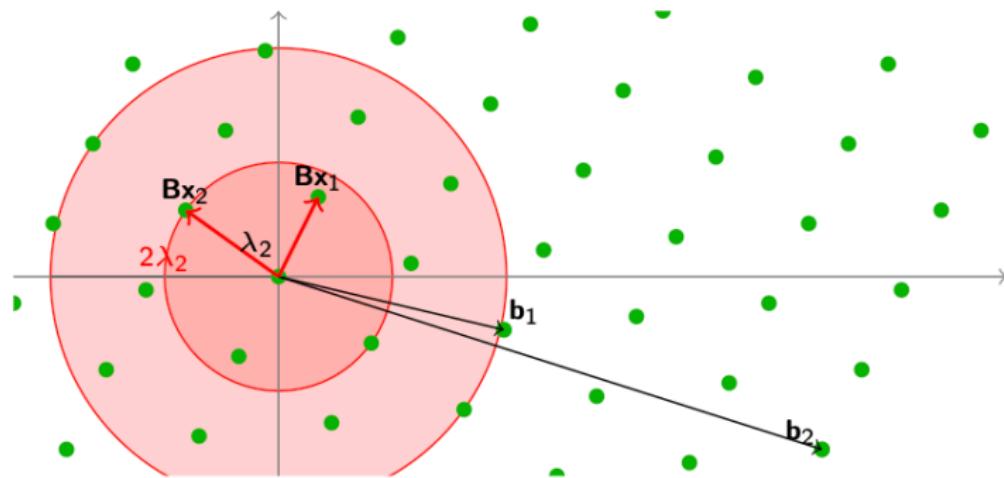
Minimum distance

$$\begin{aligned}\lambda_1 &= \min_{\mathbf{x}, \mathbf{y} \in \mathcal{L}, \mathbf{x} \neq \mathbf{y}} \|\mathbf{x} - \mathbf{y}\| \\ &= \min_{\mathbf{x} \in \mathcal{L}, \mathbf{x} \neq 0} \|\mathbf{x}\|\end{aligned}$$

# Shortest Independent Vectors Problem

## Definition ( $\text{SIVP}_\gamma$ )

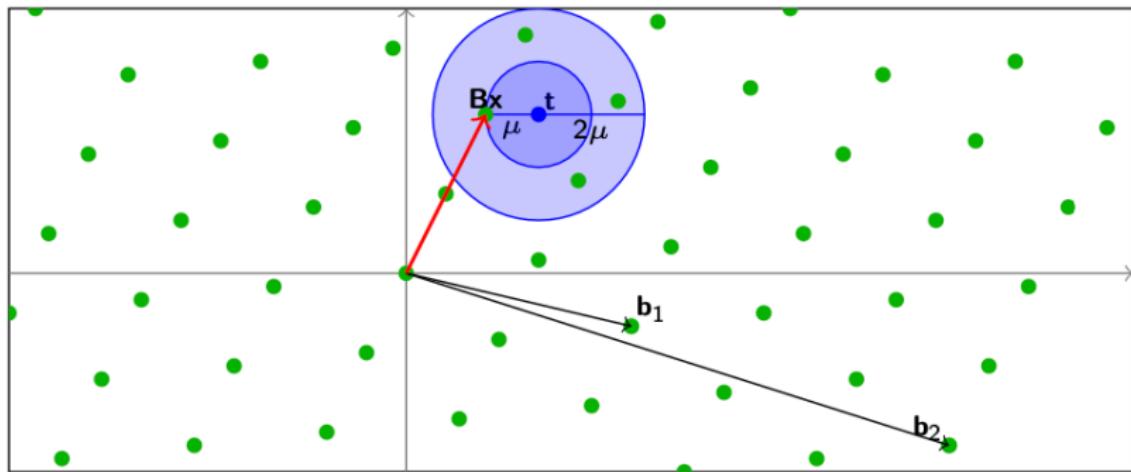
Given a lattice  $\mathcal{L}(\mathbf{B})$ , find  $n$  linearly independent lattice vectors  $\mathbf{Bx}_1, \dots, \mathbf{Bx}_n$  of length (at most)  $\max_i \|\mathbf{Bx}_i\| \leq \gamma \lambda_n$



# Closest Vector Problem

## Definition (CVP $_{\gamma}$ )

Given a lattice  $\mathcal{L}(\mathbf{B})$  and a target point  $\mathbf{t}$ , find a lattice vector  $\mathbf{Bx}$  within distance  $\|\mathbf{Bx} - \mathbf{t}\| \leq \gamma\mu$  from the target



# Special Versions of CVP

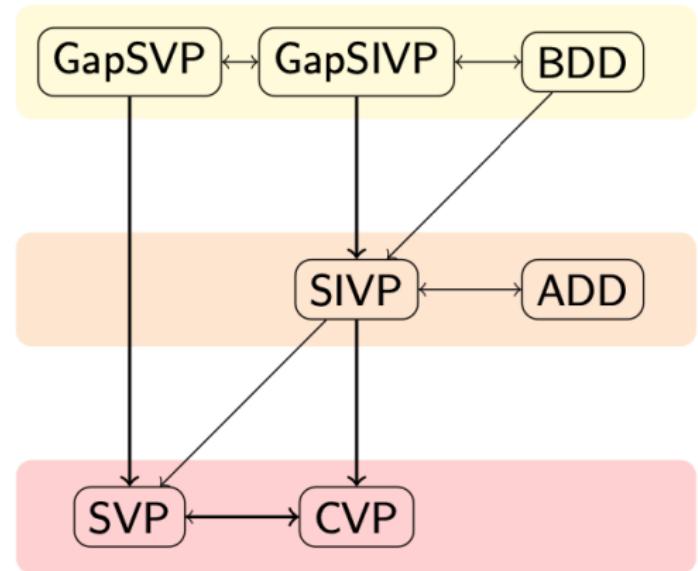
## Definition

Given  $(\mathcal{L}, \mathbf{t}, \mathbf{d})$ , with  $\mu(\mathbf{t}, \mathcal{L}) \leq \mathbf{d}$ , find a lattice point within distance  $d$  from  $\mathbf{t}$ .

- If  $d$  is arbitrary, then one can find the closest lattice vector by binary search on  $d$ .
- *Bounded Distance Decoding (BDD)*: If  $d < \lambda_1(\mathcal{L})/2$ , then there is at most one solution. Solution is the closest lattice vector.
- *Absolute Distance Decoding (ADD)*: If  $d \geq \mu(\mathcal{L})$ , then there is always at least one solution. Solution may not be closest lattice vector.

# Relations among lattice problems

- $\text{SIVP} \approx \text{ADD}$  [MG'01]
- $\text{SVP} \leq \text{CVP}$  [GMSS'99]
- $\text{SIVP} \leq \text{CVP}$  [M'08]
- $\text{BDD} \lesssim \text{SIVP}$
- $\text{CVP} \lesssim \text{SVP}$  [L'87]
- $\text{GapSVP} \approx \text{GapSIVP}$   
[LLS'91, B'93]
- $\text{GapSVP} \lesssim \text{BDD}$  [LM'09]

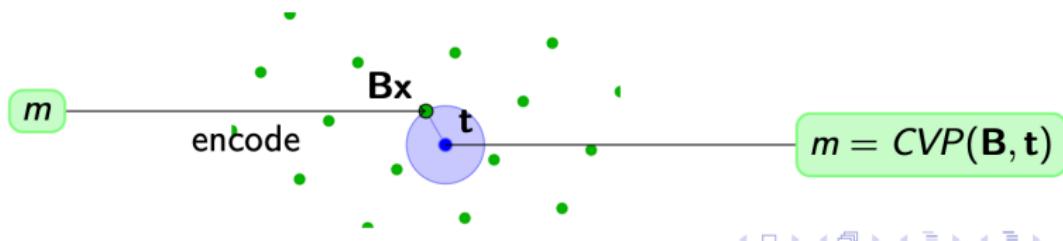


# Coding theory

## Problem: Decoding

Reliable transmission of information over noisy channels.

- Sender wants to transmit a message  $m$
- The sender encodes  $m$  as a lattice point  $\mathbf{B}x$  and transmits it over a noisy channel
- Recipient receives a perturbed lattice point  $t = \mathbf{B}x + e$ , where  $e$  is a small error vector
- Recipient recovers the original message  $m$  by finding the lattice point  $\mathbf{B}x$  closest to the target  $t$ . (CVP)



# Random lattices in Cryptography

- Cryptography typically uses (random) lattices  $\Lambda$  such that  $\Lambda \subseteq \mathbb{Z}^d$  is an integer lattice and  $q\mathbb{Z}^d \subseteq \Lambda$  is periodic modulo a small integer  $q$ .
- Cryptographic functions based on  $q$ -ary lattices involve only arithmetic modulo  $q$ .

## Definition ( $q$ -ary lattice)

$\Lambda$  is a  $q$ -ary lattice if  $q\mathbb{Z}^n \subseteq \Lambda \subseteq \mathbb{Z}^n$

Examples (for any  $\mathbf{A} \in \mathbb{Z}_q^{n \times d}$ )

- $\Lambda_q(\mathbf{A}) = \{\mathbf{x} \mid \mathbf{x} \bmod q \in \mathbf{A}^T \mathbb{Z}_q^n\} \subseteq \mathbb{Z}^d$
- $\Lambda_q^\perp(\mathbf{A}) = \{\mathbf{x} \mid \mathbf{A}\mathbf{x} = \mathbf{0} \bmod q\} \subseteq \mathbb{Z}^d$  (SIS lattice)

$$\mathcal{L}_q^\perp([\mathbf{A} \mid \mathbf{I}_n]) = \mathcal{L}\left(\left[\begin{array}{cc} -\mathbf{I}_m & \mathbf{0} \\ \mathbf{A} & q\mathbf{I}_n \end{array}\right]\right)$$

# How are they related?

$$\mathbf{A} \in \mathbb{Z}_q^{m \times k}, \mathbf{s} \in \mathbb{Z}_q^k, \mathbf{e} \in \mathcal{E}^m.$$
$$g_{\mathbf{A}}(\mathbf{s}; \mathbf{e}) = \mathbf{As} + \mathbf{e} \bmod q$$

## Theorem (R'05)

*The function  $g_{\mathbf{A}}(\mathbf{s}, \mathbf{e})$  is hard to invert on the average, assuming SIVP is hard to approximate in the worst-case.*

## LWE and q-ary lattices

- If  $\mathbf{e} = \mathbf{0}$ , then  $\mathbf{As} + \mathbf{e} = \mathbf{As} \in \Lambda(\mathbf{A}^t)$
- Same as CVP in random  $q$ -ary lattice  $\Lambda(\mathbf{A}^t)$  with random target  $\mathbf{t} = \mathbf{As} + \mathbf{e}$
- Usually  $\mathbf{e}$  is shorter than  $\frac{1}{2}\lambda_1(\Lambda(\mathbf{A}^T))$ , and  $\mathbf{e}$  is uniquely determined
- TAKE AWAY:
- LWE  $\equiv$  Approximate BDD (Bounded Distance Decoding)

# (M)SIS Problem

## Definition

Let  $n, m, \beta \in \mathbb{N}$ . The Module Short Integer Solution problem M-SIS <sub>$n, m, \beta$</sub>  over  $\mathcal{R}_q$  is defined as follows.

Given  $\mathbf{A} \xleftarrow{\$} \mathcal{R}_q^{n \times m}$ , find an  $\vec{z} \in \mathcal{R}_q^m$  such that  $\mathbf{A}\vec{z} = \vec{0}$  and  $0 < \|\vec{z}\|_2 \leq \beta$ .

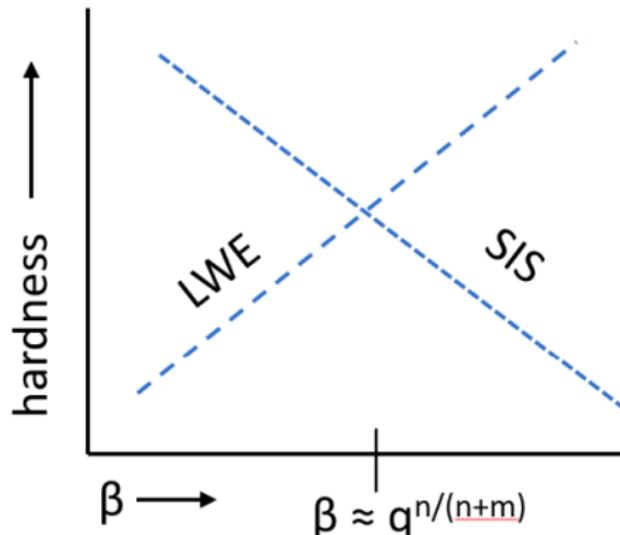
$$\begin{array}{c|c|c} A & z & = \\ \hline n \times m & m \times 1 & n \times 1 \\ & & 0 \pmod{q} \end{array}$$

# SIS (lattice formulation)

## Definition (SVP in SIS lattice)

Given  $A \in_R \mathbb{Z}_q^{n \times m}$ , find a nonzero  $z \in [-B, B]^m$  in the SIS lattice

$$L_A^\perp = L(C) \text{ where } C = \begin{bmatrix} qI_n & -\bar{A} \\ 0 & I_{m-n} \end{bmatrix}.$$



# SIS application: Collision-resistant hash function (Ajtai)

## Definition (Ajtai Hash)

Select  $A \in_R \mathbb{Z}_q^{n \times m}$ , where  $m > n \log q$ .

Define  $H_A : \{0, 1\}^m \longrightarrow \mathbb{Z}_q^n$  by  $H_A(z) = Az \pmod{q}$ .

## Compression.

Since  $m > n \log q$ , we have  $2^m > q^n$ . □

## Collision resistance.

Suppose that one can efficiently find  $z_1, z_2 \in \{0, 1\}^m$  with  $z_1 \neq z_2$  and  $H_A(z_1) = H_A(z_2)$ . Then  $Az_1 = Az_2 \pmod{q}$ , whence  $Az = 0 \pmod{q}$  where  $z = z_1 - z_2$ . Since  $z \neq 0$  and  $z \in [-1, 1]^m$ ,  $z$  is an SIS solution (with  $B = 1$ ) which has been efficiently found. □

# NTRU: Nth-degree TRUncated polynomial ring

- The NTRU cryptosystem is parameterized by a certain polynomial ring  $R = \mathbb{Z}[X]/(f(X))$ , e.g.,  $f(X) = X^n - 1$  for a prime  $n$  or  $f(X) = X^n + 1$  for an  $n$  that is a power of two, and a sufficiently large odd modulus  $q$  that defines the quotient ring  $R_q = R/qR$ .
- The public key is  $h = 2g \cdot s^{-1} \in R_q$  for two "short" polynomials  $g, s \in R$ , i.e., ones having relatively small integer coefficients, where the secret key  $s$  is also chosen to be invertible modulo both  $q$  and two.
- Can define SVP/CVP in NTRU lattice



Paper 2025/1129

## Lattice-based Obfuscation from NTRU and Equivocal LWE

Valerio Cini Bocconi University

Russell W. F. Lai Aalto University

Ivy K. Y. Woo Aalto University

### Abstract

Indistinguishability obfuscation (iO) turns a program unintelligible without altering its functionality and is a powerful cryptographic primitive that captures the power of most known primitives. Recent breakthroughs have successfully constructed iO from well-founded computational assumptions, yet these constructions are unfortunately insecure against quantum adversaries. In the search of post-quantum secure iO, a line of research investigates constructions from fully homomorphic encryption (FHE) and tailored decryption hint release mechanisms. Proposals in this line mainly differ in their designs of decryption hints, yet all known attempts either cannot be proven from a self-contained computational assumption, or are based on novel lattice assumptions which are subsequently cryptanalysed.

In this work, we propose a new plausibly post-quantum secure construction of iO by designing a new mechanism for releasing decryption hints. Unlike prior attempts, our decryption hints follow a public Gaussian distribution subject to decryption correctness constraints and are therefore in a sense as random as they could be. To generate such hints efficiently, we develop a general-purpose tool called primal lattice trapdoors, which allow sampling trapdoored matrices whose Learning with Errors (LWE) secret can be equivocated. We prove the security of our primal lattice trapdoors construction from the NTRU assumption. The security of the iO construction is then argued, along with other standard lattice assumptions, via a new Equivocal LWE assumption, for which we provide evidence for plausibility and identify potential targets for further cryptanalysis.

**Note:** An extended abstract of this work is published at CRYPTO'25. This is the full version, containing proofs in the appendix.

### Metadata

#### Available format(s)

PDF

#### Category

Public-key cryptography

#### Publication info

A major revision of an IACR publication in CRYPTO 2025

#### Keywords

obfuscation lattice cryptography NTRU  
Equivocal LWE

#### Contact author(s)

valerio.cini @ unibocconi.it  
russell.lai @ aalto.fi  
ivy.woo @ aalto.fi

#### History

2025-06-17: approved

2025-06-15: received

[See all versions](#)

#### Short URL

<https://ia.cr/2025/1129>



## Worst-case to Average-case Reduction

Breaking LWE on average requires solving SVP in the worst case on any lattice. This theoretical guarantee is rare in practical cryptography and provides exceptional confidence in security.

## Structured Variants for Efficiency

- **Ring-LWE:** Operations over polynomial rings reduce complexity from  $O(n^2)$  to  $O(n \log n)$  (by using NTT)
- **Module-LWE:** Balances Ring-LWE efficiency with LWE security—used in NIST standards

# NIST Standardized Algorithms

## Lattice-based Algorithms Won

3 of 4 NIST standardized post-quantum algorithms are lattice-based:

- **ML-KEM (Kyber)**: Key Encapsulation Mechanism
- **ML-DSA (Dilithium)**: Digital Signature Algorithm
- **FN-DSA (FALCON)**: Compact Digital Signatures

## Why Lattice Won

- **Versatility**: Only post-quantum approach supporting full cryptographic functionality
- **Performance**: Recent advances achieve competitive efficiency with classical systems
- **Security**: Strong theoretical foundations with worst-case hardness

## Section 2

Why Do We Need Lattice-based Cryptography?



vitalik.eth ✅  
@VitalikButerin

∅ ...

The last week of Ethereum state tree research be like...



10:48 AM · Jul 28, 2024 · 356.4K Views

453

368

2.3K

144





Nico  
@nico\_mnbl

...

anyone else felt this after listening to the episode?

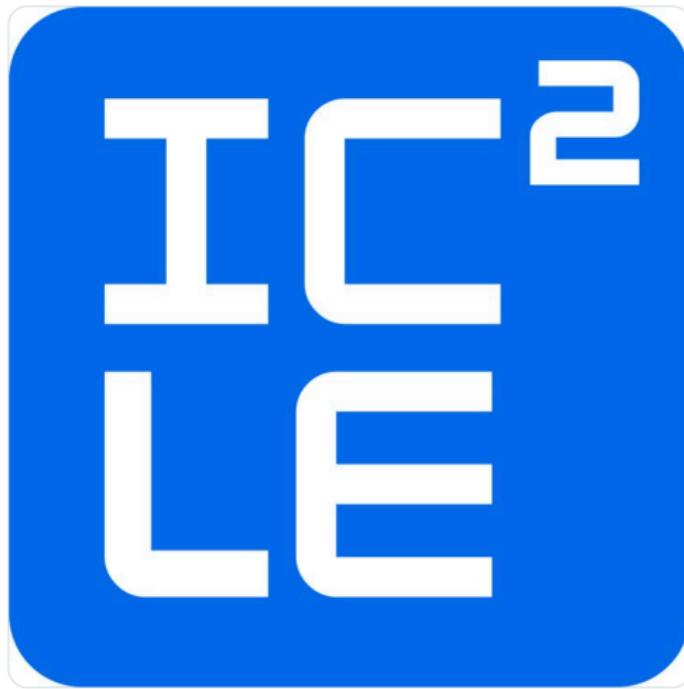


7:53 PM · Nov 28, 2024 · 5,731 Views

Omer Shlomovits   
@OmerShlomovits

🔗 ...

ICICLE v4 will introduce Lattice based cryptography. ETA is one month from now. We will first support lattice based ZK (LaBRADOR, Greyhound, LatticeFold family). Next accelerated PQC, PIR, all the way to FHE. If you are interested in early access, influence features and API design, please get in touch asap. Thank you!



7:57 PM · May 9, 2025 · 4,472 Views



## Subsection 1

Math: The Universal Language

# The Mathematical Foundation

## The Grand Unification

"Starting from linear algebra, probability theory, and abstract algebra, there is only one thing that can connect quantum computing, machine learning, computational complexity, cryptography, zero-knowledge proofs, blockchain, information theory, coding theory, Galois theory, group theory, module theory, algebraic number theory, and algebraic geometry together: **lattices**."

## From Algebra to Geometry

Lattice-based cryptography represents a paradigm shift: it adds **geometric structure** to algebraic cryptography, creating a bridge between discrete and continuous mathematics.

## Core Mathematical Objects

- **Vector Spaces:** Linear combinations and spans
- **Lattices:** Discrete subgroups of  $\mathbb{R}^n$
- **Ideals:** Connecting to algebraic number theory
- **Modules:** Generalizations over rings (not just fields)

## The Geometric Insight

While RSA relies on number-theoretic properties and ECC on algebraic curves, lattices embed cryptographic hardness in **geometric problems** in high-dimensional spaces.

# Connecting All Fields

## Information Theory

- Error-correcting codes
- Channel capacity
- Noisy channel theorem

## Quantum Computing

- Quantum states as vectors
- Entanglement geometry
- Measurement bases

## Machine Learning

- Dimension reduction
- Principal components
- Optimization landscapes

## Number Theory

- Algebraic integers
- Class field theory
- Galois theory

# From a recent LBC paper

## 2.1 Number Theory

A **number field**  $K = \mathbb{Q}(\zeta)$  of degree  $N$  is a finite field extension of the rationals  $\mathbb{Q}$  obtained by adjoining an algebraic number  $\zeta$ . We denote its **ring of integers** by  $R$ . We call  $K$  a  $\nu$ -th **cyclotomic number field** if  $\zeta$  is a  $\nu$ -th **primitive root of unity**. Its degree is given by  $N = \varphi(\nu)$ , where  $\varphi$  is Euler's totient function.

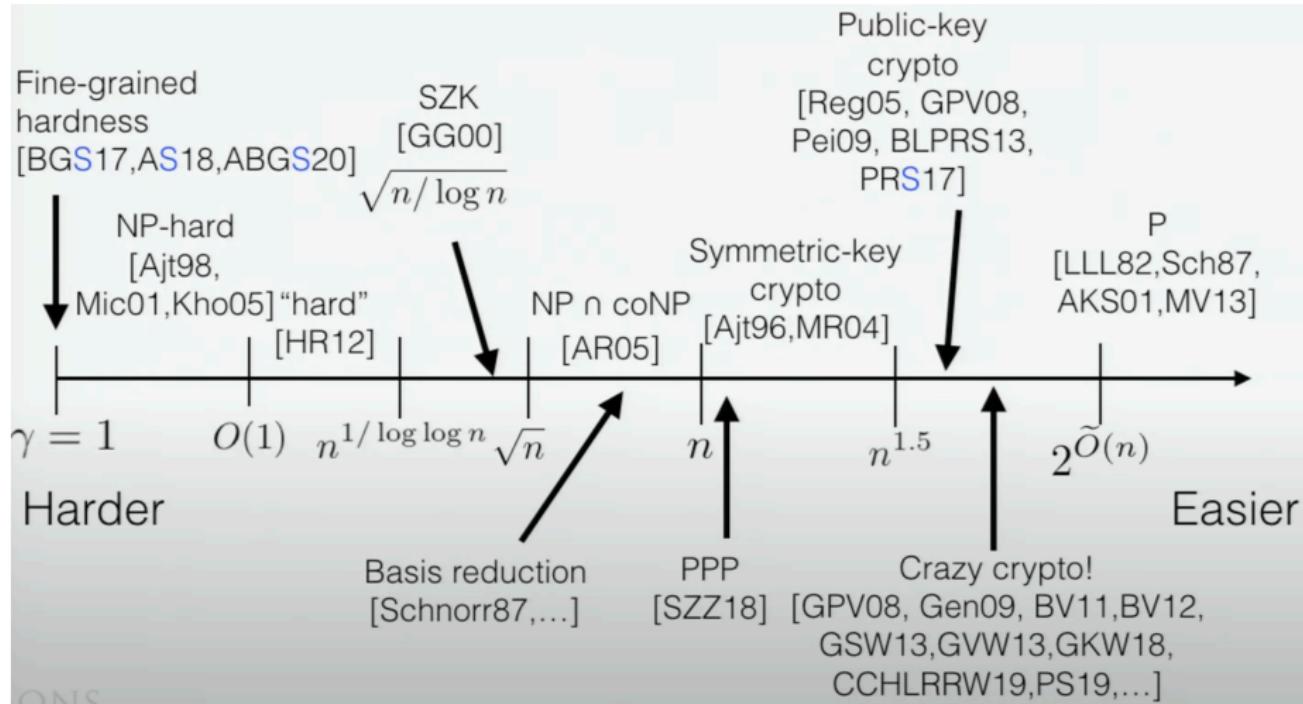
We can identify  $K = \mathbb{Q}[X]/\langle \Phi(X) \rangle$ , where  $\Phi(X)$  is the **minimal polynomial** of  $\zeta$ . Every element  $x \in K$  can then be written with respect to the basis  $\{1, \zeta, \dots, \zeta^{N-1}\}$ , thus  $x = \sum_{i=0}^{N-1} x_i \zeta^i$  with  $x_i \in \mathbb{Q}$ . The isomorphism  $\tau: K \rightarrow \mathbb{Q}^N$  which maps  $x$  to its coefficient vector  $\tau(x) = (x_0, \dots, x_{N-1})^T$  is called the **coefficient embedding**. By associating the norm of an element  $x$  in  $K$  with the norm of its corresponding  $\tau(x) \in \mathbb{Q}^N$ , it is possible to **equip  $K$  with a geometry**. For a positive integer  $\eta$ , we define  $S_\eta = \tau^{-1}(\{-\eta, \dots, \eta\}^N) = \{y \in R \mid \|\tau(y)\|_\infty \leq \eta\}$ , which corresponds to the set of polynomials in  $R$  with coefficients in  $\{-\eta, \dots, \eta\}$ .

Another way of equipping  $K$  with a geometry is the **canonical embedding**. More precisely, for a number field  $K$  of degree  $N$ , let  $\theta_1, \dots, \theta_N$  denote the embeddings of  $K$  into  $\mathbb{C}$ . The canonical embedding  $\theta: K \rightarrow \mathbb{C}^N$  is mapping  $x \in K$  to  $\theta(x) := (\theta_1(x), \dots, \theta_N(x))^T$ . It also helps us define the **discriminant of the number field  $K$**  as  $\Delta_K = |\det(\theta_i(r_j))_{i,j}|^2$  for any basis  $(r_j)$  of  $R$ .

## Subsection 2

Complexity / TCS

# Lattice and Complexity



# Worst-Case to Average-Case Reductions

## The Holy Grail of Cryptography

Most cryptographic assumptions rely on **average-case hardness** of problems, but lattice problems provide something unprecedented: reductions from **worst-case** to **average-case** hardness.

## Why This Matters

- **RSA:** Breaking *some* instances might be easy
- **Lattices:** Breaking *random* instances requires solving *all* instances
- **Confidence:** Unprecedented theoretical guarantee: Provable Cryptography directly from  $\mathcal{NP}$ -hard problem.

# NP-Hard Based Cryptography

## The Lattice Advantage

Unlike factoring (not known to be NP-complete), lattice problems like SVP are:

- **NP-hard** in the worst case
- **Hard for quantum computers** (no exponential speedup)
- **Well-studied** with 40+ years of research

## Approximation Hierarchy

Even **approximating** SVP within polynomial factors remains exponentially hard, providing a rich hierarchy of computational assumptions.

# Impagliazzo's Five Worlds

Algorithmica → Heuristica → Pessiland → Minicrypt →  
**Cryptomania**

Lattices enable us to approach the final frontier: **Obfustopia**

## Known Achievements

- **FHE**: Fully Homomorphic Encryption
- **ABE**: Attribute-Based Encryption
- **Functional Encryption**
- **Witness Encryption**

## Holy Grail

- **Post-Quantum iO**: Indistinguishability Obfuscation
- **Cryptographic completeness**
- **All cryptographic primitives**

# Lattice-Based Post-Quantum iO from Circular Security with Random Opening Assumption

(Part II: zeroizing attacks against private-coin evasive LWE assumptions)

Yao-Ching Hsieh\*

Aayush Jain<sup>†</sup>

Huijia Lin<sup>‡</sup>

## Abstract

Indistinguishability obfuscation (iO) stands out as a powerful cryptographic primitive but remains notoriously difficult to realize under simple-to-state, post-quantum assumptions. Recent works have proposed lattice-inspired iO constructions backed by new “LWE-with-hints” assumptions, which posit that certain distributions of LWE samples retain security despite auxiliary information. However, subsequent cryptanalysis has revealed structural vulnerabilities in these assumptions, leaving us without any post-quantum iO candidates supported by simple, unbroken assumptions.

# Obfustopia Still, Simple to design!

- One-Way Functions
- Public Key Encryption
- Hardness of Finding Nash
- Short Signature
- Trapdoor Permutation
- Identity-Based Encryption
- Attribute-Based Encryption
- Fully Homomorphic Encryption \*
- Multiparty Computation
- (Non-Interactive) Zero-Knowledge
- Two-Round MPC
- Hardness of finding Nash

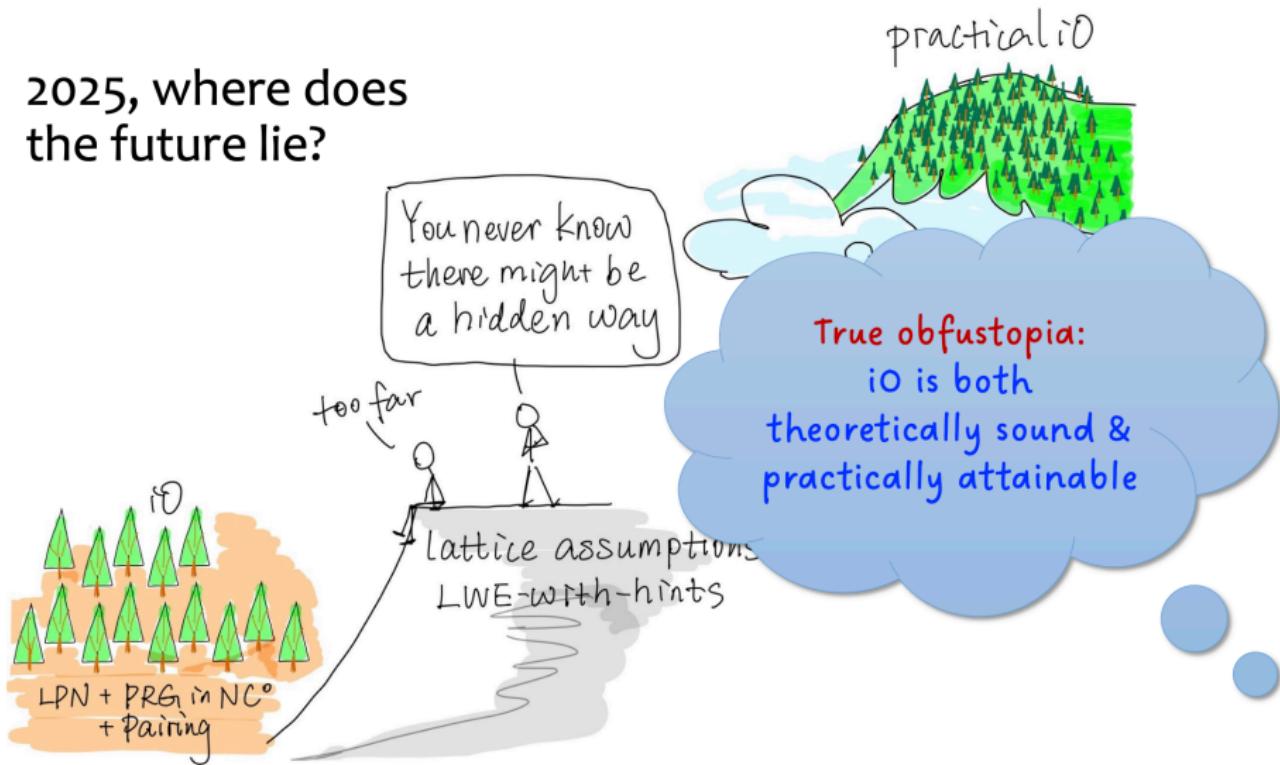
iO +  
minimal hardness  
 $NP \not\subseteq \text{ioBPP}$

↓

Most  
Crypto

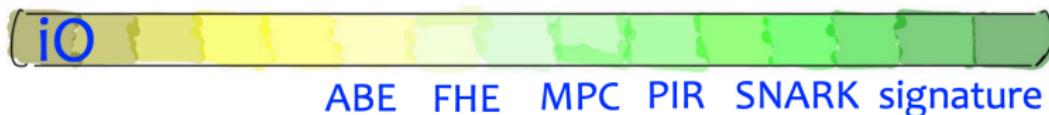
- Functional Encryption
- Witness Encryption
- (Doubly) Deniable Encryption
- Secret Sharing for NP
- Correlation Intractable Hash
- SNARG for NP in the standard model
- Multi-Party Non-Interactive Key Exchange
- OWF with poly hard core bits
- Succinct Garbled RAM
- Multilinear Map
- Constant Round Concurrent ZK
- Publicly verifiable quantum money

# 2025, where does the future lie?



# Theoretical

# Practical



“Minimal” assumptions for iO?

*Less number of assumptions?  
Remove PRG in NC<sup>0</sup>?*

More efficient constructions?

*Efficient FE/xiO-to-iO transformation?*

Post-quantum Security?

*iO from LWE or not?*

Practical iO

~~ambitious or naïve?~~

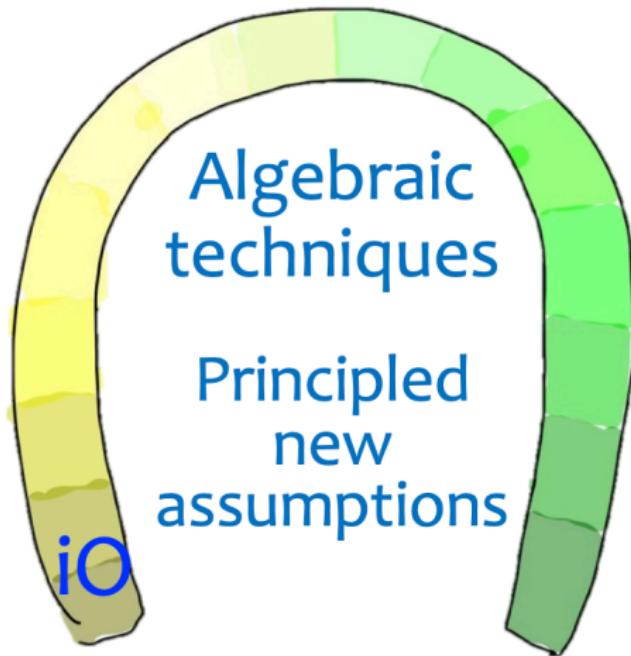
1. A worthy subject to study!
2. Great things always come out of ambitious pursuits.
3. Efficiency is a work of progress

# Opportunity of our time

Direct algebraic constructions

Close to direct algebraic: xiO, FE

Bounty: Efficient xiO/FE to iO



Theoretical

Practical

### Subsection 3

## Cryptanalysis: The Lattice Sword

# Lattice Reduction as a Weapon

## The Double-Edged Nature

Lattice reduction algorithms (LLL, BKZ) are both:

- **Cryptanalytic tools** that break classical schemes
- **Hardness assumptions** for lattice-based schemes

## Attacking Classical Cryptography

- **RSA**: Small private exponents, related keys
- **DSA**: Biased nonces, side-channel analysis
- **Knapsack**: Complete breaks of early schemes
- **NTRU**: Cryptanalysis informing parameter selection

# The LLL Algorithm Legacy

## Lenstra-Lenstra-Lovász (1982)

The LLL algorithm revolutionized both:

- **Number theory:** Polynomial-time lattice reduction
- **Cryptanalysis:** Breaking many "provably secure" schemes
- **Cryptography:** Enabling lattice-based constructions

## Modern Evolution: BKZ and Beyond

- **BKZ** (Block Korkine-Zolotarev): Stronger reduction
- **Sieving algorithms:** Exponential but more effective
- **Quantum variants:** Still exponential complexity

# Understanding Our Own Weapons

## Self-Aware Cryptography

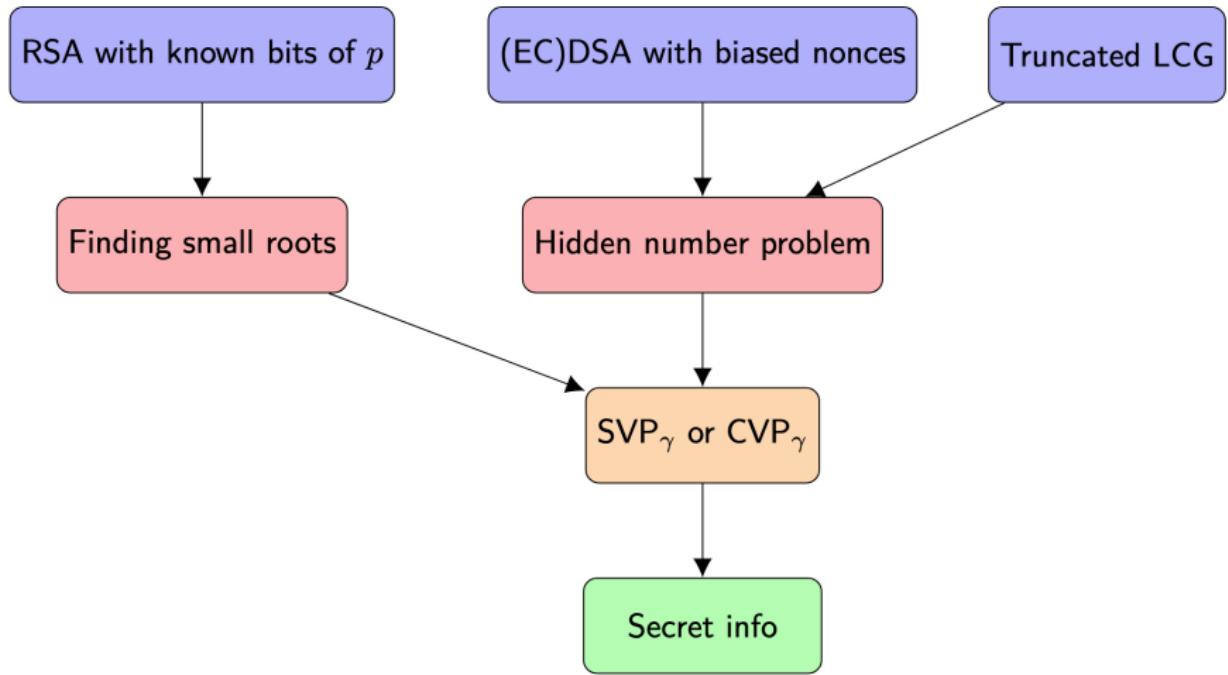
Lattice-based cryptography uniquely benefits from its own cryptanalytic tools:

- **Parameter selection** guided by reduction algorithms
- **Security estimates** based on computational costs
- **Conservative margins** accounting for future improvements

## The Virtuous Cycle

Better cryptanalysis → Stronger schemes → More confidence → Wider adoption

# Examples of lattice-based attacks



# Examples of lattice-based attacks

Lattice-based Problem	Attack	Description
Finding small roots	RSA stereotyped message	Low exponent RSA with large amount of known plaintext
	Boneh-Durfee attack	RSA with small private exponent $d < 0.292$
	Partial key exposure attack	RSA with small private exponent $d$ and known bits of $d$
Knapsack problem	ECDSA with $k = z \oplus d$	ECDSA given many signatures calculated with nonce as the message hash XOR the private key
Hidden number problem	ECDSA with biased nonces	ECDSA given many signatures calculated with biased nonces
	Bleichenbacher's PKCS#1 v1.5 padding oracle attack	PKCS#1 v1.5 given a large number of requests to a decryption padding oracle
Extended hidden number problem	ECDSA key disclosure problem	ECDSA given many signatures calculated with partially known nonces and known bits of private key

## Subsection 4

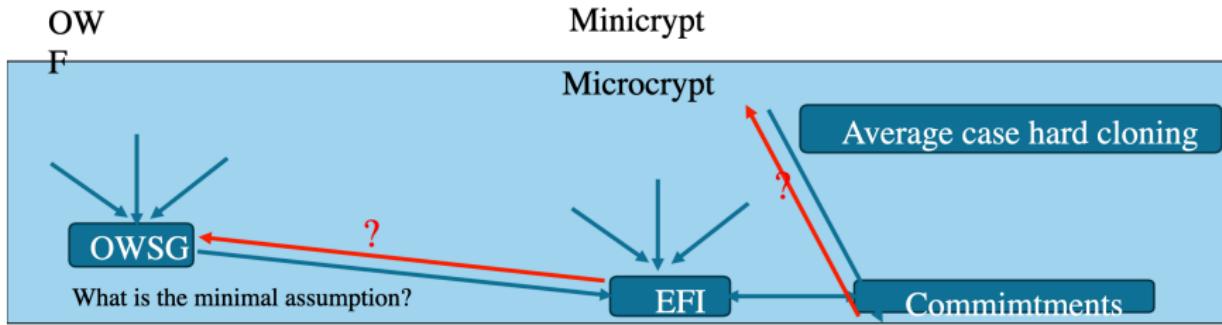
### Post-Quantum Security

# Quantum Cryptographic landscape

## Classical Crypto

Public key encryption

Cryptomania



# The Quantum Apocalypse

## Shor's Algorithm Impact

- **RSA, DSA, ECDSA:** Polynomial-time quantum attacks
- **Discrete log:** Both integer and elliptic curve variants broken
- **Timeline:** 10-20 years to cryptographically relevant quantum computers

## Grover's Algorithm

- **Symmetric crypto:** Square-root speedup (AES-128 → AES-256)
- **Hash functions:** Birthday attacks become more effective
- **Lattices:** No known exponential quantum speedup

## NIST's PQC standards

Digital Signature Algorithm Family	Parameters	Transition
ECDSA [FIPS186]	112 bits of security strength	<b>Deprecated</b> after 2030 <b>Disallowed</b> after 2035
	$\geq 128$ bits of security strength	<b>Disallowed</b> after 2035
EdDSA [FIPS186]	$\geq 128$ bits of security strength	<b>Disallowed</b> after 2035
RSA [FIPS186]	112 bits of security strength	<b>Deprecated</b> after 2030 <b>Disallowed</b> after 2035
	$\geq 128$ bits of security strength	<b>Disallowed</b> after 2035

# Quantum Resistance Comparison

Approach	Classical	Quantum	Basis	Maturity
Lattice	$2^n$	$2^n$	Geometry	High
Hash-based	$2^n$	$2^{n/2}$	OWF	High
Code-based	$2^n$	$2^n$	Coding	Medium
Multivariate	$2^n$	$2^n$	Algebra	Low
Isogeny	$2^n$	$2^n$	Curves	Broken

## The Clear Winner

Lattices provide the best combination of security, functionality, and performance.

# NIST Standardization Victory

## The Results Are In

NIST Post-Quantum Cryptography Standardization (2024):

- **ML-KEM** (Kyber): Key encapsulation
- **ML-DSA** (Dilithium): Digital signatures
- **FN-DSA** (FALCON): Compact signatures
- **3 out of 4** primary standards are lattice-based

## Industry Adoption

Major deployments already underway: AWS KMS, Apple iMessage, Cloudflare, Signal Protocol

## Subsection 5

Performance: Classical Meets Post-Quantum

- Compared to other signature schemes selected for standardisation by NIST, such as Dilithium [LDK+22] and Sphincs+ [HBD+22],
- Falcon stands out for its compactness, minimising both public key and signature sizes.<sup>1</sup>

variant	keygen (ms)	keygen (RAM)	sign/s	verify/s	pub size	sig size
FALCON-512	8.64	14336	5948.1	27933.0	897	666
FALCON-1024	27.45	28672	2913.0	13650.0	1793	1280

Table 2. SLH-DSA parameter sets

	$n$	$h$	$d$	$h'$	$a$	$k$	$lg_w$	$m$	security category	pk bytes	sig bytes
SLH-DSA-SHA2-128s	16	63	7	9	12	14	4	30	1	32	7856
SLH-DSA-SHAKE-128s	16	66	22	3	6	33	4	34	1	32	17088
SLH-DSA-SHA2-128f	16	66	22	3	6	33	4	34	1	32	17088
SLH-DSA-SHA2-192s	24	63	7	9	14	17	4	39	3	48	16224
SLH-DSA-SHAKE-192s	24	63	7	9	14	17	4	39	3	48	16224
SLH-DSA-SHA2-192f	24	66	22	3	8	33	4	42	3	48	35664
SLH-DSA-SHA2-256s	32	64	8	8	14	22	4	47	5	64	29792
SLH-DSA-SHAKE-256s	32	64	8	8	14	22	4	47	5	64	29792
SLH-DSA-SHA2-256f	32	68	17	4	9	35	4	49	5	64	49856
SLH-DSA-SHAKE-256f	32	68	17	4	9	35	4	49	5	64	49856

<sup>1</sup><https://falcon-sign.info/>

# Comparison with Other Post-Quantum Approaches

Approach	Key Size	Maturity	Versatility
Hash-based	Large	High	Limited
Code-based	Very Large	Medium	Medium
Multivariate	Medium	Low	Medium
<b>Lattice-based</b>	<b>Medium</b>	<b>High</b>	<b>High</b>

# Post-Quantum Performance Landscape

Operation	ML-KEM-768	ML-DSA-65	FALCON-512
Key Gen	0.1ms	1ms	100ms
Encaps/Sign	0.1ms	2ms	5ms
Decaps/Verify	0.1ms	1ms	0.1ms
Key Size	1184 bytes	1952 bytes	897 bytes
Ciphertext/Sig	1088 bytes	3293 bytes	690 bytes

## The Verdict

Lattice schemes are **competitive** in speed, with larger but manageable sizes.

## Dan Boneh at ZKProofs (2025)

[LatticeFold] is one of the first times where a post-quantum SNARK system might actually be better than a pre-quantum SNARK system.

# Real-World Performance Analysis

## Network Impact

- **TLS handshake:** 64 bytes → 2,272 bytes (35x increase)
- **IoT devices:** Require careful parameter selection

## Computational Efficiency

- **Hardware acceleration:** Dedicated instructions emerging
- **Vectorization:** Natural fit for SIMD operations
- **Memory access:** Regular patterns enable optimization

# The Performance Evolution

## Historical Perspective

- **2000s:** Lattices were academic curiosities
- **2010s:** First practical constructions emerged
- **2020s:** Competitive with classical schemes
- **2025+:** Hardware acceleration mainstream

## Future Trajectory

As quantum computers approach, the **relative** advantage of lattice-based schemes will only increase.

- **Signal Protocol:** PQXDH implementation using Kyber
- **Cloudflare:** Widespread ML-KEM deployment
- **Algorand:** FALCON signatures in State Proofs system

## Section 3

How Does Lattice-based Cryptography Shape the Future?

# Production-Ready Tools Available Now

- **Open Quantum Safe (OQS)**: Comprehensive library with OpenSSL 3.x integration
- **Platform support**: Multi-architecture optimizations (x86\_64, ARM) with language wrappers
- **Industry integration**: AWS KMS, Google Chrome, Signal, Cloudflare, Apple iMessage already using these implementations

# Side-channel attacks Countermeasure

## Security Gotchas

Side-channel attacks are the primary practical threat—use established, tested implementations

## Best Practices

- Constant-time algorithms essential
- Hybrid deployment recommended during transition
- Hardware acceleration available
- Memory requirements manageable ( 4KB for operations)

# Recent Game-Changing Advances (Part 1)

## SLAP Framework (Eurocrypt 2024)

- First lattice-based polynomial commitment with polylogarithmic proof size and verifier time under standard Module-SIS assumptions.
- Concrete proof size: 17 MB for  $2^{20}$  constraints ( $15 \times$  smaller than previous lattice SNARKs).

## LaBRADOR and Greyhound (Crypto 23-24)

- LaBRADOR: First lattice-based recursively amortized R1CS proof system achieving  $O(\log n)$  proof size (58 KB for  $2^{20}$  constraints).
- Greyhound: First concretely efficient lattice polynomial commitment; 53 KB proofs for degree- $2^{30}$  polynomials with 3-round evaluation protocol.

# Recent Game-Changing Advances (Part 2)

## LatticeFold and LatticeFold+ (2024–2025)

- LatticeFold: First post-quantum folding scheme for R1CS and CCS over 64-bit fields—comparable performance to preceding PCP-based systems.
- LatticeFold+: Algebraic range proofs and double-commitment techniques yielding  $5\times$  faster proving and shorter proofs.

## Neo (Eurocrypt 2025)

- Lattice-based folding for CCS with “pay-per-bit” Ajtai commitments over small prime fields; concrete post-quantum security.

# Classical vs. Lattice-Based Polynomial Commitments

## KZG (Classical)

- ✓ Constant-size proofs
- ✓ Efficient verification
- ✗ Quantum-vulnerable
- ✗ Requires trusted setup

## FRI (Quantum-resistant)

- ✓ Transparent setup
- ✓ Hash-based security
- ✗ Larger proofs
- ✗ Higher communication

## Lattice-based

- ✓ Quantum resistance
- ✓ Competitive efficiency
- ✓ Transparency
- ✓ 2x smaller than FRI

# Strategic Recommendations

## For Organizations

- ① Start now with hybrid approaches:** Combine classical + lattice-based systems
- ② Focus on crypto-agility:** Design systems for easy algorithm updates
- ③ Prioritize by risk:** Long-lived systems need immediate attention
- ④ Investment in expertise:** Train teams on lattice cryptography specifics

# IBM Updated 2029 Roadmap

2026

First demonstration of quantum advantage

2029

First large-scale, fault-tolerant quantum computer

## Section 4

### Conclusion

# Why Lattice Cryptography Is Inevitable

## The Convergence of Necessity and Capability

Lattice-based cryptography uniquely provides **quantum resistance**, **practical efficiency**, and **comprehensive functionality**. The mathematical foundations are solid, the performance is competitive, and the real-world deployments prove viability.

## The Network Effect Moment

With NIST standardization complete, major platforms deploying, and quantum threats crystallizing, we're reaching the tipping point where lattice-based cryptography transitions from experimental to essential infrastructure.

# Your Next Steps

## The Question

The question isn't whether to adopt lattice-based cryptography, but how quickly you can integrate it into your systems before the quantum transition forces the change.

## Action Items

Whether you're building blockchain systems, implementing zero-knowledge proofs, or designing any long-term cryptographic infrastructure, lattice-based approaches are not just an option—they're the future-proof foundation for security in the quantum era.

# Thank You!

## Questions & Discussion

by your sincere  
**Kurt Pan**

