Post Quantum Cryptography

Lattice Based Algorithms

Dylan Packer
CSci Seminar Fall 2025

Post Quantum Cryptography Lattice Based Algorithms

- Rapid development of quantum computers that are exponentially faster and stronger than what there is today.
- Data that is shared over the internet is not safe. Messages, banking, private data will be compromised
- 1994 Peter Shor proved that with a strong enough quantum computer, all current cryptography can be broken
- NIST has started developing the future of security with post quantum cryptography

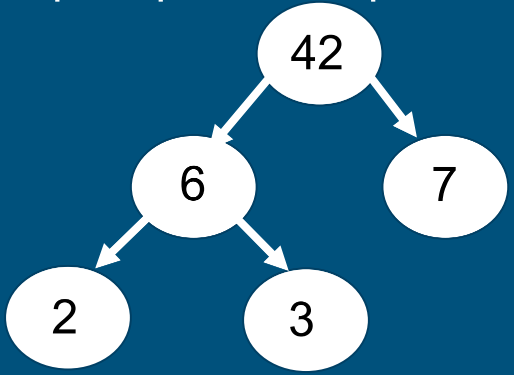
Overview

- Current algorithms
- Shor’s algorithm
- NIST
- Post Quantum Cryptography
- Lattices
- Learning With Errors
- Kyber
- SABER
- Conclusion

Current algorithms

- RSA named after Rivest–Shamir–Adleman the computer scientist who developed it
- RSA relies heavily on integer factorization
- A classical computer would take hundreds of trillions of years to break standard RSA encryption

Given a number N, the goal is to find prime numbers p1,p2,... ,pk such that N=p1✕ p2 ✕ …✕ pk



Current algorithms

- Elliptic Curve Cryptography (ECC) relies on discrete logarithm problem.
- Classic computer would take an astronomically long time to break ECC, it would take billions of years to break

$$x \text{ in } g^x \equiv h \pmod{\text{p}}$$

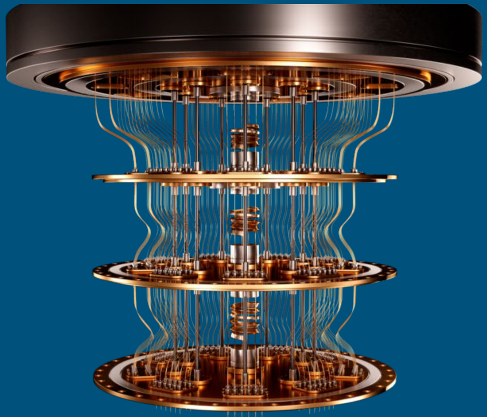
$$2^x \equiv 9 \pmod{11}$$

Current algorithms

- Major companies IBM, Google, and Microsoft are developing quantum computers
- Quantum computer and Shor’s algorithm will break current methods of encryption making them extremely less effective at protecting data

Quantum computers

- Quantum Bits (qubits) can represent 1, 0, or both at the same time this is called superposition
- Entanglement links qubits so they are mathematically correlated, allowing the computer to explore many possibilities in parallel
- Quantum parallelism



Shor’s algorithm

- Peter Shor developed an algorithm that could efficiently break the cryptographic systems used today.
- Shor’s algorithm is described as a hybrid algorithm, combining classical and quantum steps.

Pick random Integer A that A < N

Find the period R of f(x) = A^x mod N

If R is even and A^(R/2) is not -1(mod N), find the greatest common divisors of A^(R/2)± 1 and N

These will be non trivial factors of N

If Process fails try a different A

NIST

NIST
National Institute of
Standards and Technology

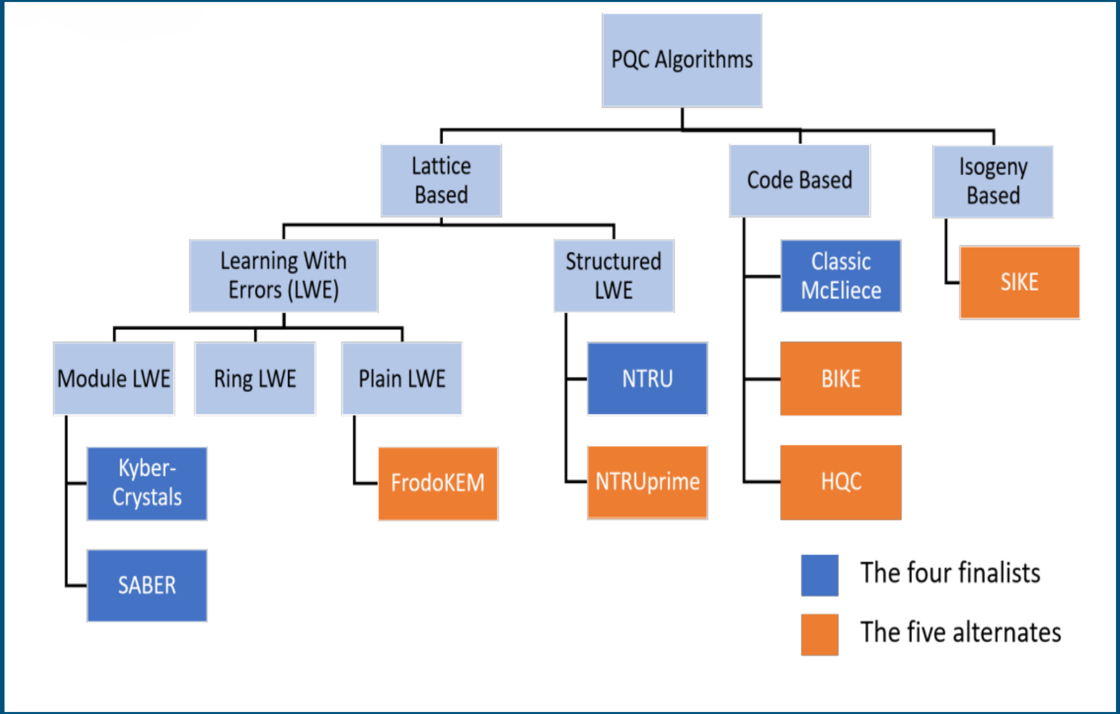
- U.S. federal agency within the Department of Commerce
- Founded on March 3, 1901, as the National Bureau of Standards. It was renamed to the National Institute of Standards and Technology in 1988
- Promotes innovation and industrial competitiveness through measurements of science, standards, and technology.

NIST process

- Identify the problem
- Call for Proposals
- Submission and Initial Evaluation
- Multi -Round Evaluation
- Selection of Finalists
- Standardization and Finalization

Post-Quantum Cryptography

- NIST finalists for PQC
- Code based
- Isogeny based
- Lattice based



PQC Algorithms

Lattice Based

Learning With Errors (LWE)

Module LWE

Kyber-Crystals

SABER

Ring LWE

Plain LWE

FrodoKEM

Structured LWE

NTRU

NTRUprime

Code Based

Classic McEliece

BIKE

HQC

Isogeny Based

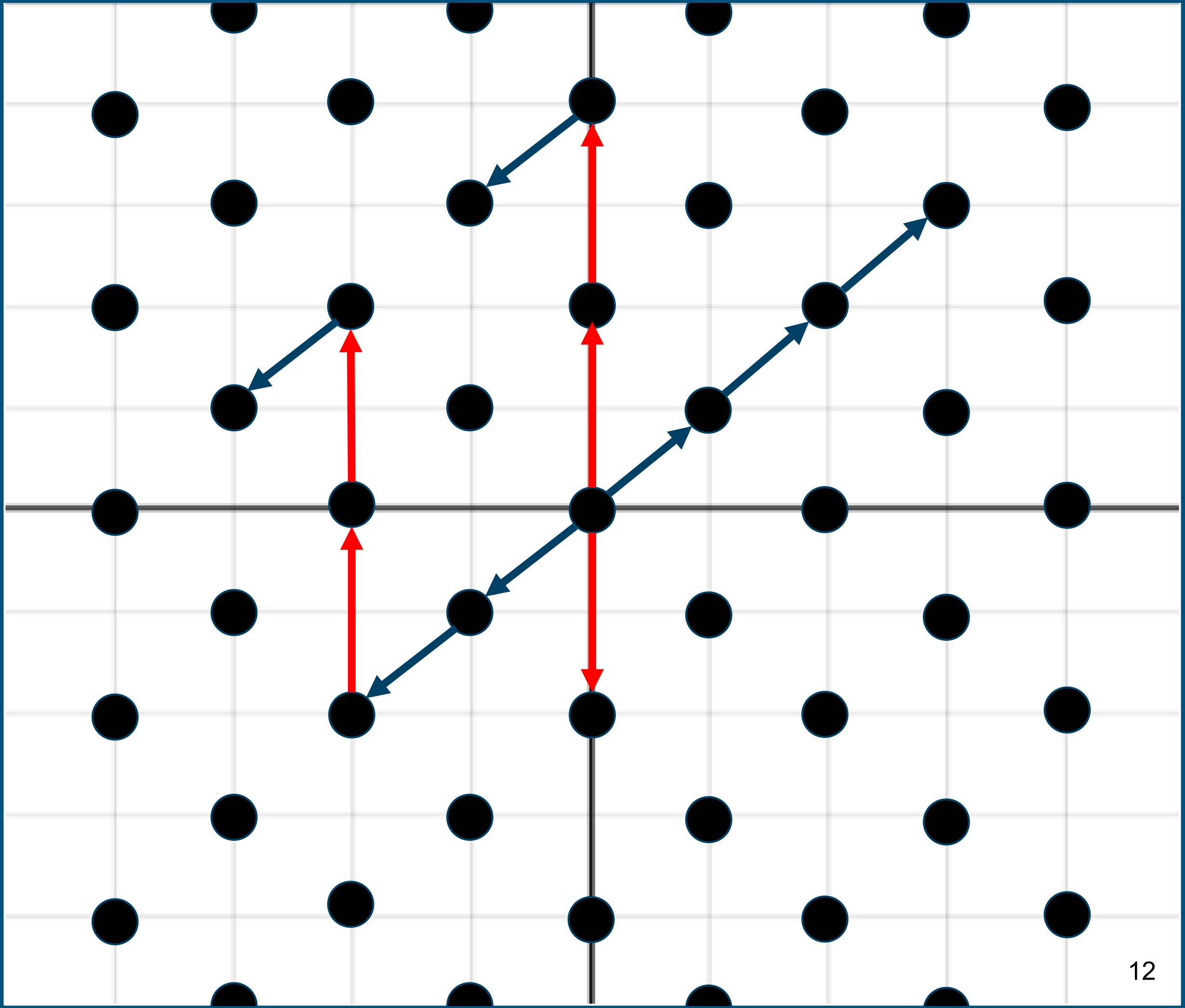
SIKE

🟦 The four finalists

🟧 The five alternates

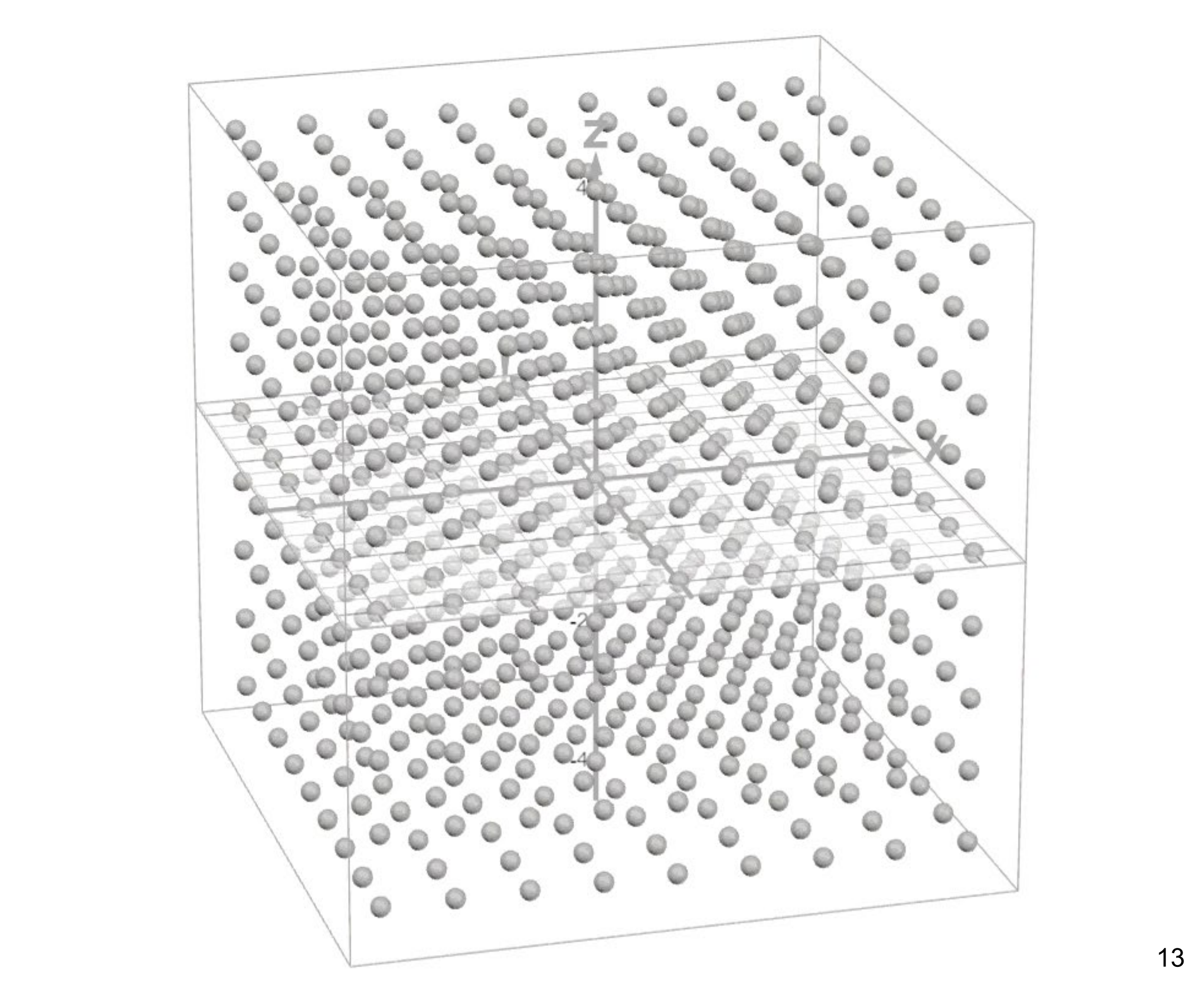
Lattices

- A lattice is a grid like structure with a repeating pattern
- The basis vectors are (0,2) and (1,1)



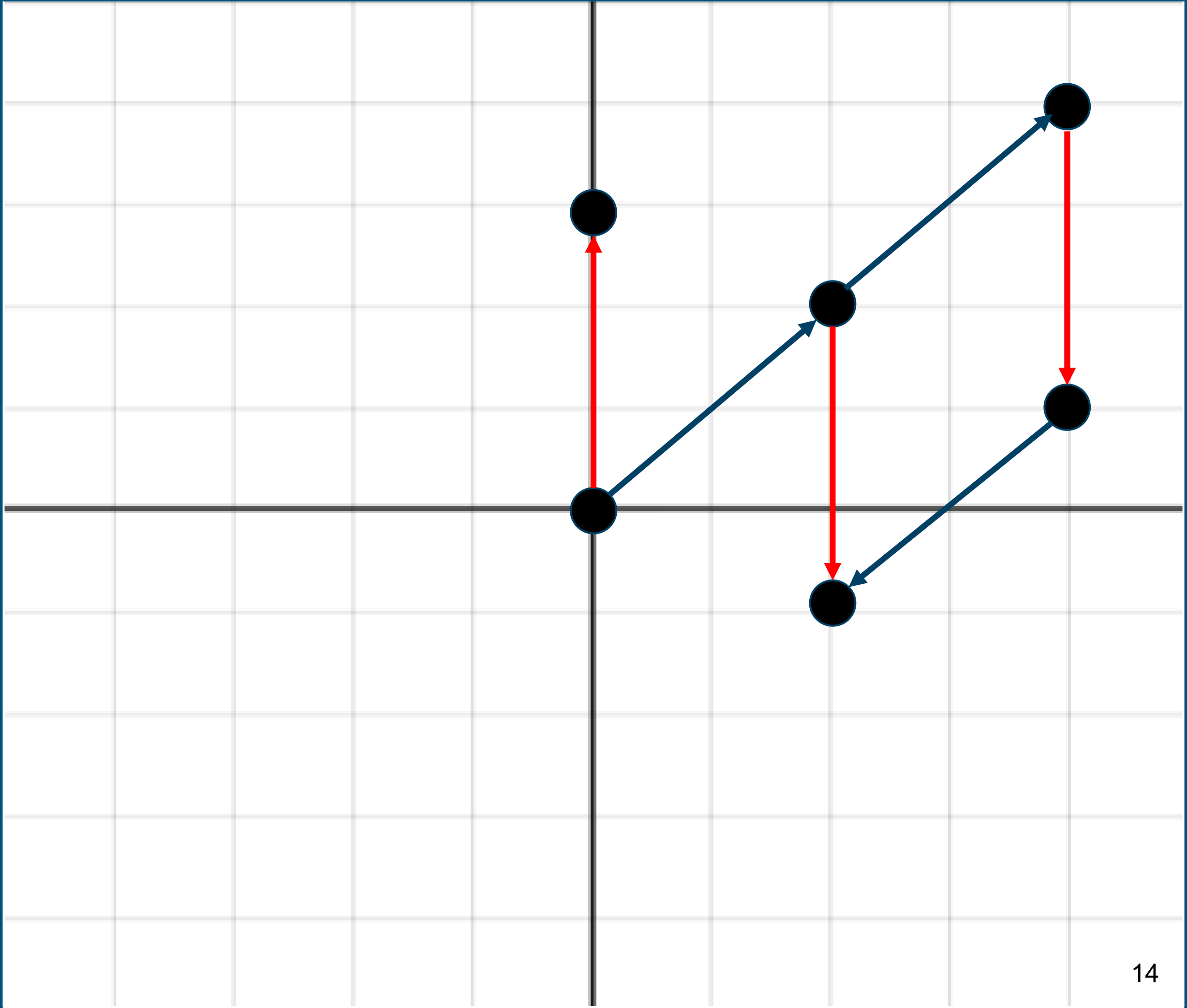
Lattices

- Each dimension adds more complexity



Lattices

- Shortest Vector Problem
- How to find the shortest vector that isn't the zero vector?



Learning with Errors

- Given a set of equations with small random errors find the hidden secret vector
- These are the subcategories of LWE: Plain LWE, Ring LWE, and Module LWE

Plain LWE

$$\begin{array}{r|l|}
77x + 7y + 28z + 23w = 2859 & -1 \\
21x + 19y + 30z + 48w = 3508 & +3 \\
4x + 24y + 33z + 38w = 3848 & -2 \\
8x + 20y + 84z + 61w = 6225 & +0
\end{array}$$

s

x= 10

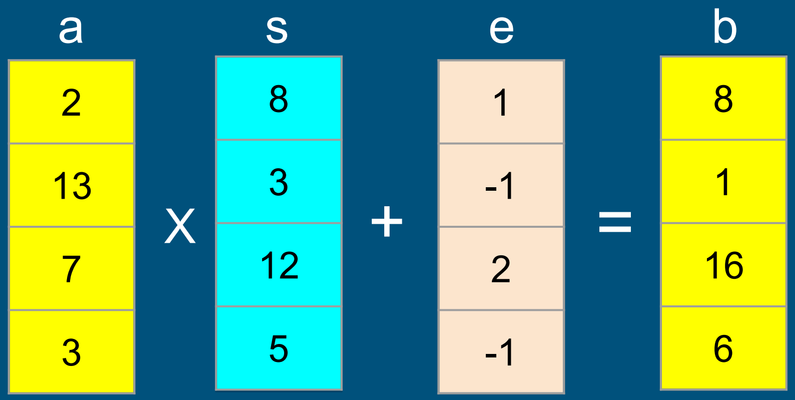
y=82

z=50

w=5

Ring Learning with Errors

- Used to build efficient and secure lattice-based cryptographic schemes
- Operates over the ring R, Let R=Zq[x]/(x^n)+1



$$\begin{array}{ccccccc} a & & s & & e & & b \\ 2 & & 8 & & 1 & & 8 \\ 13 & & 3 & & -1 & & 1 \\ 7 & X & 12 & + & 2 & = & 16 \\ 3 & & 5 & & -1 & & 6 \end{array}$$

Module Learning with Errors

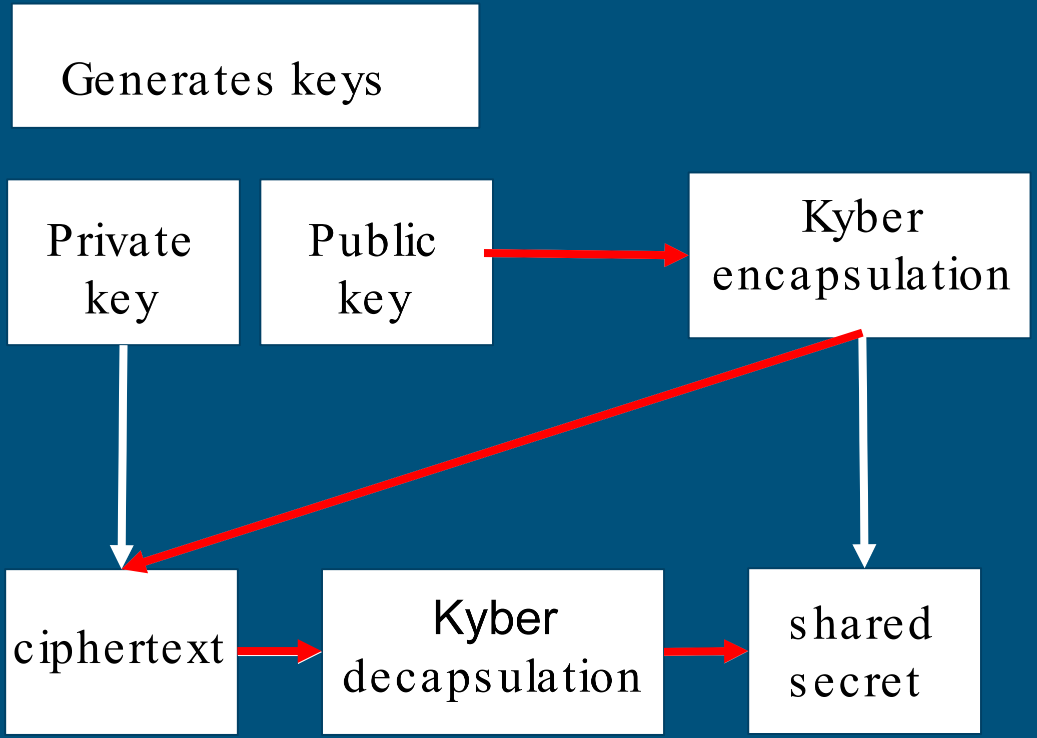
- Finding a secret module vector s given a set of "noisy" linear equations.
- equations are formed by taking inner products of known module vectors a_i with the secret s, and then adding a small, randomly distributed error e_i.

- secret vector s
- a_i are known random vectors
- e_i are small errors
- b_i is the result
- multiple equations of the form:

$$a_i * s + e_i \approx b_i \pmod{q}$$

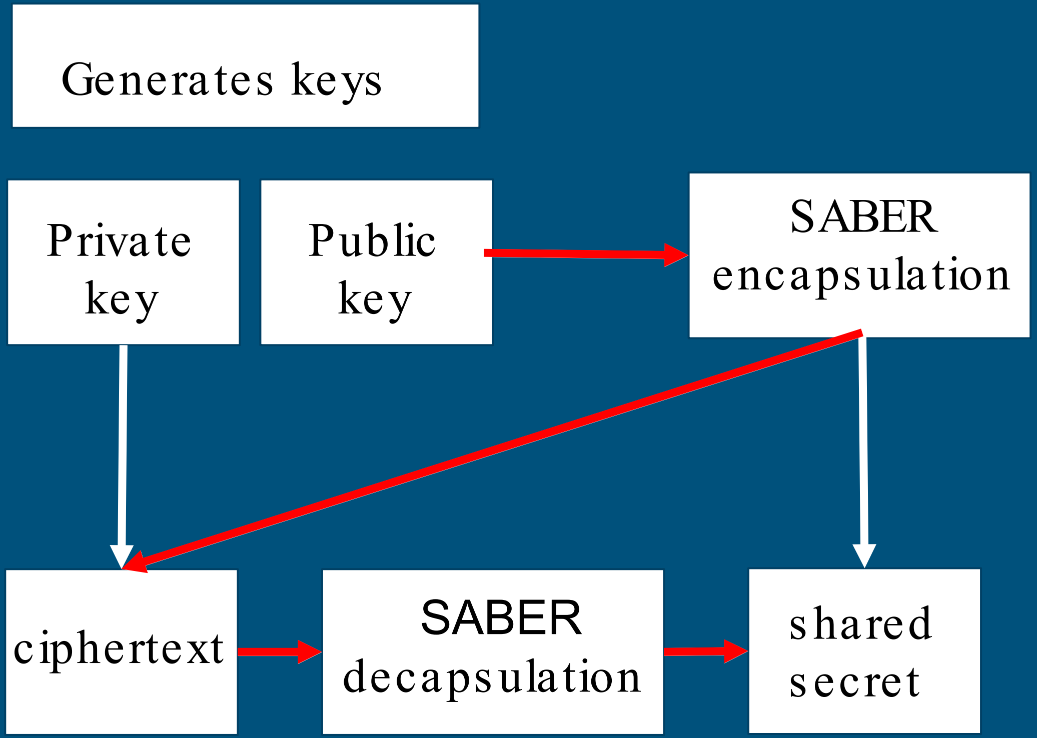
Kyber

- Encryption scheme based on module-LWE
- Built for speed and compactness
- Kyber 512, Kyber 768, Kyber 1024



SABER

- Built for simplicity and resilience
- LightSABER, SABER, FireSABER



Generates keys

Private key

Public key

SABER encapsulation

ciphertext

SABER decapsulation

shared secret

Conclusion

- Quantum computer are coming
- Shor’s algorithm proves this isn’t theory
- PQC is the solution
- Lattice based schemes like Kyber and SABER are leading the way
- The transition to PQC will take time, but the groundwork is being laid now.
- Early adoption ensures long-term security

References

M. Kumar and P. Pattnaik, "Post Quantum Cryptography(PQC) - An overview: (Invited Paper)," 2020 IEEE High Performance Extreme Computing Conference (HPEC), Waltham, MA, USA, 2020, pp. 1-9, doi: 10.1109/HPEC43674.2020.9286147. keywords: {Program processors;Quantum computing;Standardization;NIST;Computational efficiency;Quantum cryptography;Galois fields},

Wenwen Xia, Geng Wang, and Dawu Gu. 2025. Post-Quantum Backdoor for Kyber-KEM. In Selected Areas in Cryptography – SAC 2024: 31st International Conference, Montreal, QC, Canada, August 28-30, 2024, Revised Selected Papers, Part I. Springer-Verlag, Berlin, Heidelberg, 237–255. https://doi.org/10.1007/978-3-031-82852-2_11

P. Singh, A. Srivastava, D. Srivastava, Shivam, M. Verma and V. Srivastava, "An Overview of Quantum Cryptography Evolution From Classical Cryptography," 2025 International Conference on Cognitive Computing in Engineering, Communications, Sciences and Biomedical Health Informatics (IC3ECSBHI), Greater Noida, India, 2025, pp. 1-6, doi: 10.1109/IC3ECSBHI63591.2025.10990566. keywords: {Polarization;Uncertainty;Protocols;Quantum entanglement;Scalability;Qubit;Quantum key distribution;Cryptography;Quantum cryptography;Standards;BB84 protocol;Quantum cryptography;Classical cryptography;Polarization states;Photon polarization;Qubit;Quantum entanglement;Quantum Key Distribution;Sifting key.},