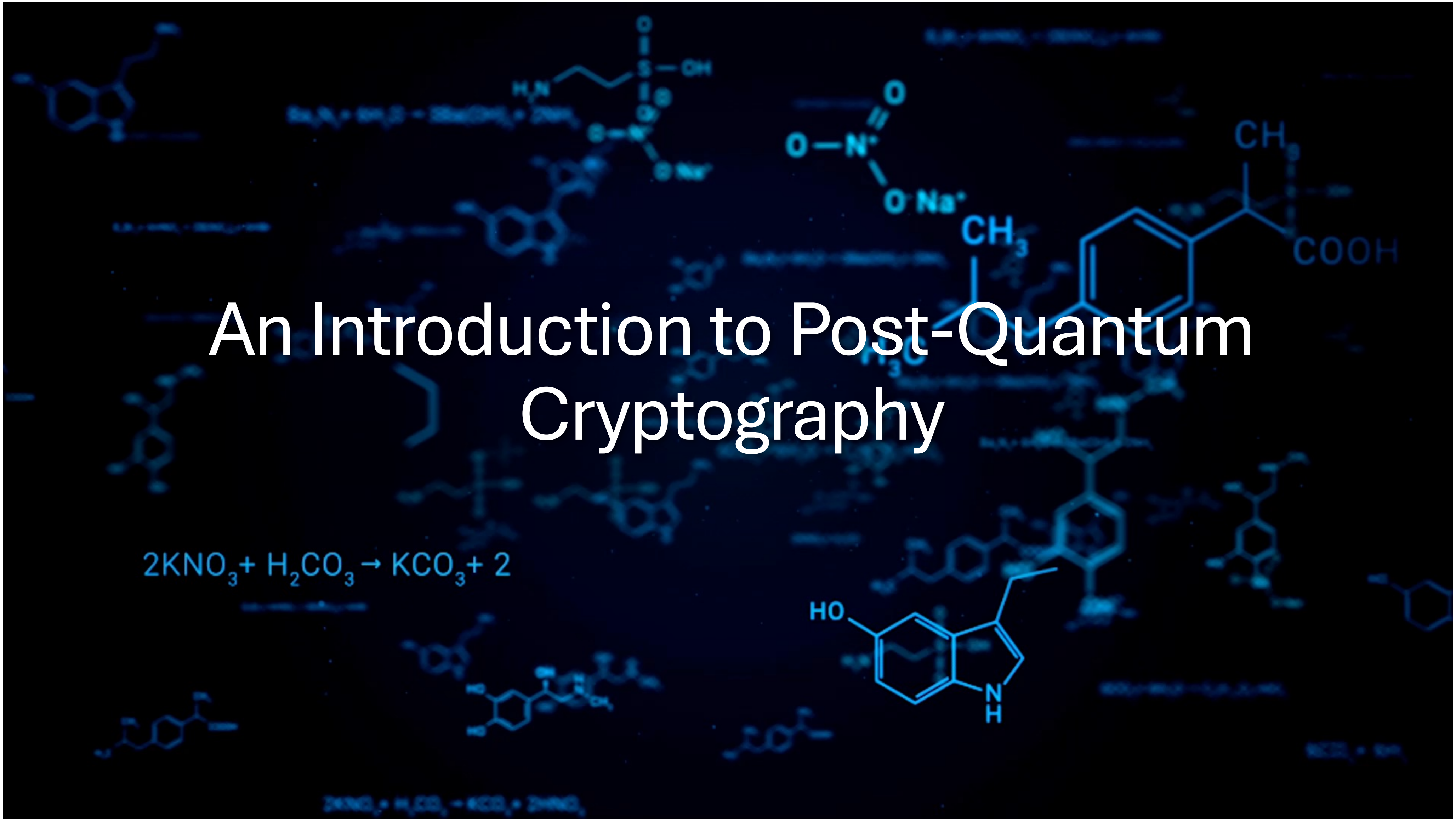
An Introduction to Post-Quantum Cryptography
2KNO3+ H2CO3 → KCO3+ 2
HO
NH
CH3
COOH
O—N+
O Na+

Objective of this lecture

- Not for math understanding and theoretical depth.
- But for future implementation and application of QPC in your professional works and research.

Quantum-Computing and the Security Challenge

- Quantum computers threaten RSA, ECC, and DH schemes (Shor’s and Grover’s algorithms). Once large-scale quantum computers are built, they will be capable of breaking most existing public-key cryptosystems.
- This poses a serious threat to the confidentiality and integrity of Internet communications.

$O(n)$

$O(\sqrt{n})$

PKI — (1) Encryption —
(2) Digital Signature
(3) DH
(4) Certificate

Post-Quantum Cryptography (PQC)

- **Goal:** Develop cryptographic systems secure against both **quantum and classical attacks**.
- Must **interoperate with existing protocols and networks** to ensure a smooth transition. mathematic hardness
- Be executable on **all devices** (e.g. classical computers, mobile phone, sensors). This is the difference between PQC and the separate field of quantum cryptography. quantum mechanic. QKD / Q random generator
- PQC is a **proactive defense**—anticipating quantum capabilities before they arrive.

PQC algorithms families

candidate

Family	Core Math Idea	Example Algorithms	Analogy / Teaching Aid
Lattice-based	Hardness of finding short vectors in high-dimensional lattices	Kyber, Dilithium, NTRU	“Finding the shortest straw in a 1000D haystack”
Code-based	Error correction in random linear codes	Classic McEliece	“Guessing errors in noisy messages”
Multivariate	Solving nonlinear polynomial equations	Rainbow, GeMSS	“Jigsaw puzzles of equations”
Hash-based	Security from hash preimage resistance	SPHINCS+	“Digital signatures built purely from hashes”
Isogeny-based	Structure of elliptic curves and their mappings	SIKE (broken in 2022)	“Paths between geometric shapes”

NIST

NIST PQC Standards

- PQC algorithms that NIST has finalized for standardization (as of Aug. 2024) include:
  - **FIPS 203 ML-KEM:** Module-Lattice-Based Key-Encapsulation Mechanism Standard - Derived from CRYSTALS-Kyber
  - **FIPS 204 ML-DSA:** Module-Lattice-Based Digital Signature Standard - Derived from CRYSTALS-Dilithium
  - **FIPS 205 SLH-DSA:** Stateless Hash-Based Digital Signature Standard - Derived from SPHINCS+

Lattice-Based Post Quantum Cryptography

- A **lattice** is a regular grid of points in multi-dimensional space, defined by integer combinations of **basis vectors** (linear independent, no need orthogonal). $C = A \cdot S$ $x_1 \cdot a_1 + x_2 \cdot a_2 + \cdots + x_k a_k = 0$

Rank(A) = k
$$L = \{s_1\mathbf{a}_1 + s_2\mathbf{a}_2 + \cdots + s_k\mathbf{a}_k \mid s_i \in Z\}$$
$x_1 = 0,\ x_2 = 0,\ \cdots\ x_k = 0$

- Core Hard Problems (hard for both classical and quantum computers)
  - **Shortest Vector Problem (SVP):**
    Find the shortest nonzero vector in a lattice — extremely hard in high dimensions.
  - **Closest Vector Problem (CVP):**
    Given a random point, find the closest lattice point — also very hard.
  - **Learning With Errors (LWE) / Ring-LWE Problem:**
    Recover a hidden vector from noisy linear equations — believed to be hard even for quantum computers.
  - Most modern lattice-based cryptosystems are built on LWE or Ring-LWE.
    NIST

The Learning With Errors (LWE) Problem

LWE can be thought of as a *"noisy system of linear equations"* that's hard to solve.

Suppose you are given a set of linear equations:

Given (A, b) $\Rightarrow$ s

$Ax = b$

$$\mathbf{A}\mathbf{s} = \mathbf{b} \pmod{q}$$

$x = A^{-1} \cdot b$

If there's no noise, solving for s (the secret vector) is easy – just linear algebra.

But in LWE, we add small random noise to each equation:

$\rightarrow$ sk

LWE $\rightarrow$ pk $\rightarrow$ $$\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \pmod{q}$$

$\rightarrow$ private

Where A is known matrix (public), s is secret vector (unknown), e is small random "error" vector (noise), q is a modulus (a large prime or power of 2)

- Given, only (A, b), it becomes computationally infeasible to recover s – NP-hard
- While LWE is secure, it's **computationally heavy** — operations on large matrices and vectors are expensive.

Ring-LWE (R-LWE) — The Optimized Version

Ring-LWE is a **more efficient variant** that replaces vectors and matrices with **polynomials**.

$$b = a(x) \cdot s(x) + e(x) \pmod{q, f(x)}$$

Where a(x), s(x), e(x) are polynomials with small integer coefficients.
f(x) is a fixed modulus polynomial (e.g. x^n + 1).

- All operations are polynomial arithmetic, which can be computed efficiently using fast Fourier transforms (FFT).
- Application: 1. CRYSTALS-Kyber (encryption/ key exchange)
  2. CRYSTALS-Dilithium (digital signature)

Polynomial Ring with a Modulus: Used in Kyber

$f(x)$

$q = 4$

$1 \quad 2 \quad 3 \quad 4 \quad 5 \bmod q$

1

🔍 Why reduce by $x^n + 1$?

Because:

- it forces polynomial degrees to stay < n
- multiplication "wraps around" (cyclic structure)
- enables very fast multiplication using **Number Theoretic Transform (NTT)** (a finite-field FFT)

$$
x^n + 1 \overline{\smash{)}\, x^n + 3x}
$$

$$
x^n + 1
$$

$$
3x - 1
$$

Example:

$$
x^n \equiv -1 \pmod{x^n + 1}
$$

So:

$$
x^n + 3x \equiv -1 + 3x
$$

CRYSTALS-Kyber Cryptography

1 1 0 1 1 1

$x^5 + x^4 + 0x^3 + x^2 + x + 1$

- Let $R_q = \mathbb{Z}_q[X]/(X^{256}+1)$ be a ring

KGen
1. Choose matrix A from $R_q^{k \times k}$ — random number
2. Choose short vectors $\mathsf{sk} = s$ and e from R_q^k
3. Compute $t = As + e$, and set $\mathsf{pk} = (t, A)$

pk

(pk, m)

Enc(pk, m)
1. Choose short r, e_1 from R_q^k and e_2 from R_q^k

mod q, $f(x)$.

2. Set $u = A^T r + e_1$ and $v = t^T \cdot r + e_2 + m$ (x)
3. Return $c = (u, v)$

message

Dec(sk, c) Compute $w = v - s^T \cdot u$ and return w

sk

CRYSTALS-Kyber, Martin Strand, Nov. 2023,
https://www.uio.no/studier/emner/matnat/its/TEK4500/h23/lectures/lecture-14---crystals-kyber-(guest-lecture-martin-strand).pdf

Correctness

$b = Ax + e$

$$
\begin{aligned}
\underbrace{v - s^T \cdot u}_{} &= \overbrace{t^T + e_2 + m}^{v} - s^T\,\overbrace{\left(A^T r + e_1\right)}^{u} \\
&= \underbrace{(As + e)}_{t}{}^T r + e_2 + m - (As)^T r - s^T \cdot e_1 \\
&= \cancel{(As)^T r} - \cancel{(As)^T r} + e^T \cdot r + e_2 - s^T e_1 + m \\
&= \underbrace{m}_{m} + \underbrace{(small)}_{\bmod q}
\end{aligned}
$$

$\Rightarrow [0, q/2] \bmod q$

u

0

Performance on Digital Signature

- The performance of PQC algorithms is so poor that their practical deployment often encounters resistance from vendors.
- Transition challenges:
  - Larger key sizes, slower performance
  - Integration into TLS, VPNs, IoT devices
- However, growing security demands compel continued exploration and development of these algorithms.
  - Harvest-Now-Decrypt-Later

			Sizes (bytes)		CPU time (lower is better)	
Family	Name variant		Public key	Signature	Signing	Verification
Elliptic curves	Ed25519	❌	32	64	0.15	1.3
Factoring	RSA 2048	❌	256	256	80	0.4
Lattices	ML-DSA 44	✅	1,312	2,420	1 (baseline)	1 (baseline)
Symmetric	SLH-DSA 128s	✅	32	7,856	14,000	40
	SLH-DSA 128f	✅	32	17,088	720	110
	LMS M4_H20_W8	✅	48	1,112	2.9 ⚠️	8.4
Lattices	Falcon 512	📝	897	666	3 ⚠️	0.7
Codebased	CROSS R-SDP(G)1 small	🤔	38	7,956	20	35
	LESS 1s	🤔	97,484	5,120	620	1800
MPC in the head	Mirath Mirith Ia fast	🤔	129	7,877	25	60
	MQOM L1-gf251-fast	🤔	59	7,850	35	85
	PERK I-fast5	🤔	240	8,030	20	40
	RYDE 128F	🤔	86	7,446	15	40
	SDitH gf251-L1-hyp	🤔	132	8,496	30	80
VOLE in the head	FAEST EM-128f	🤔	32	5,696	6	18
Lattices	HAWK 512	🤔	1,024	555	0.25	1.2
Isogeny	SQISign I	🤔	64	177	17,000	900
Multivariate	MAYO one	🤔	1,168	321	1.4	1.4
	MAYO two	🤔	5,488	180	1.7	0.8
	QR-UOV I-(31,165,60,3)	🤔	23,657	157	75	125
	SNOVA (24,5,4)	🤔	1,016	248	0.9	1.4
	SNOVA (25,8,3)	🤔	2,320	165	0.9	1.8
	SNOVA (37,17,2)	🤔	9,842	106	1	1.2
	UOV Is-pkc	🤔	66,576	96	0.3	2.3
	UOV Ip-pkc	🤔	43,576	128	0.3	0.8

traditional algorithms (❌), ✅ standardized, 📝 soon-to-be standardized, or 🤔 still candidates

https://blog.cloudflare.com/another-look-at-pq-signatures/

Industry Migration Status

- **OpenSSL** began introducing post-quantum cryptography algorithms starting with version **3.0**, providing support for schemes such as Kyber and Dilithium.
- **OpenSSH (Key Exchange)** has rapidly moved to adopt NIST-standardized Post-Quantum Key Exchange (PQC KEX) to secure remote access protocols in version 9.9. PQC
  - **The Hybrid Approach** combines a classical algorithm with a PQC algorithm for defense-in-depth:
  - Mechanism**:** mlkem768x25519-sha256
    - Classical: X25519 (Traditional ECDH) → KK
    - PQC: ML-KEM (Kyber) → E(KK)
  - In version **10.0**, this hybrid method was made the **default** key exchange mechanism.

Open-Source PQC Repository

- The **Open Quantum Safe (OQS)** project, specifically its **liboqs** library, is a core force in the open-source PQC space. It is now part of the **Linux Foundation's Post-Quantum Cryptography Alliance (PQCA)**.
- **open-quantum-safe/liboqs.** https://openquantumsafe.org/
- **liboqs** integrates various quantum-resistant **Key-Encapsulation Mechanisms (KEMs)** and **digital signature algorithms**. It supports the algorithms selected by NIST, such as **ML-KEM (Kyber)**, **ML-DSA (Dilithium)**, **SLH-DSA (SPHINCS+)**, and **Falcon**. Furthermore, it includes candidate algorithms from the NIST Fourth Round evaluation, as well as other promising schemes.

  Draft
- liboqs provides a **unified API** interface, making it easy for developers to switch between different algorithms. The project also includes a **test toolset** and **performance benchmarking** programs, along with wrappers for multiple programming languages (e.g., Java, Python, Rust, Go) and **integration solutions** for common applications like OpenSSL.

Reading Materials

- PQCrypto: post-quantum cryptography conference series. https://pqcrypto.org/conferences.html
- Chen, Lily, et al. *Report on post-quantum cryptography*. Vol. 12. Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology (NIST), https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf?ref=suddo.de
- FIPS 203–205 Documents – csrc.nist.gov
- Joseph, David, et al. "Transitioning organizations to post-quantum cryptography." *Nature* 605.7909 (2022): 237-243. https://www.nature.com/articles/s41586-022-04623-2
- A. Aydeger, etc. "Towards a Quantum-Resilient Future: Strategies for Transitioning to Post-Quantum Cryptography",2024 https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10741441

Review class & quiz 3

- Monday (Dec. 1) after Thanksgiving.
- Content: Chapter 4 (excluding PQC)
- No class on Dec. 3 (Wednesday)

- Thank you!