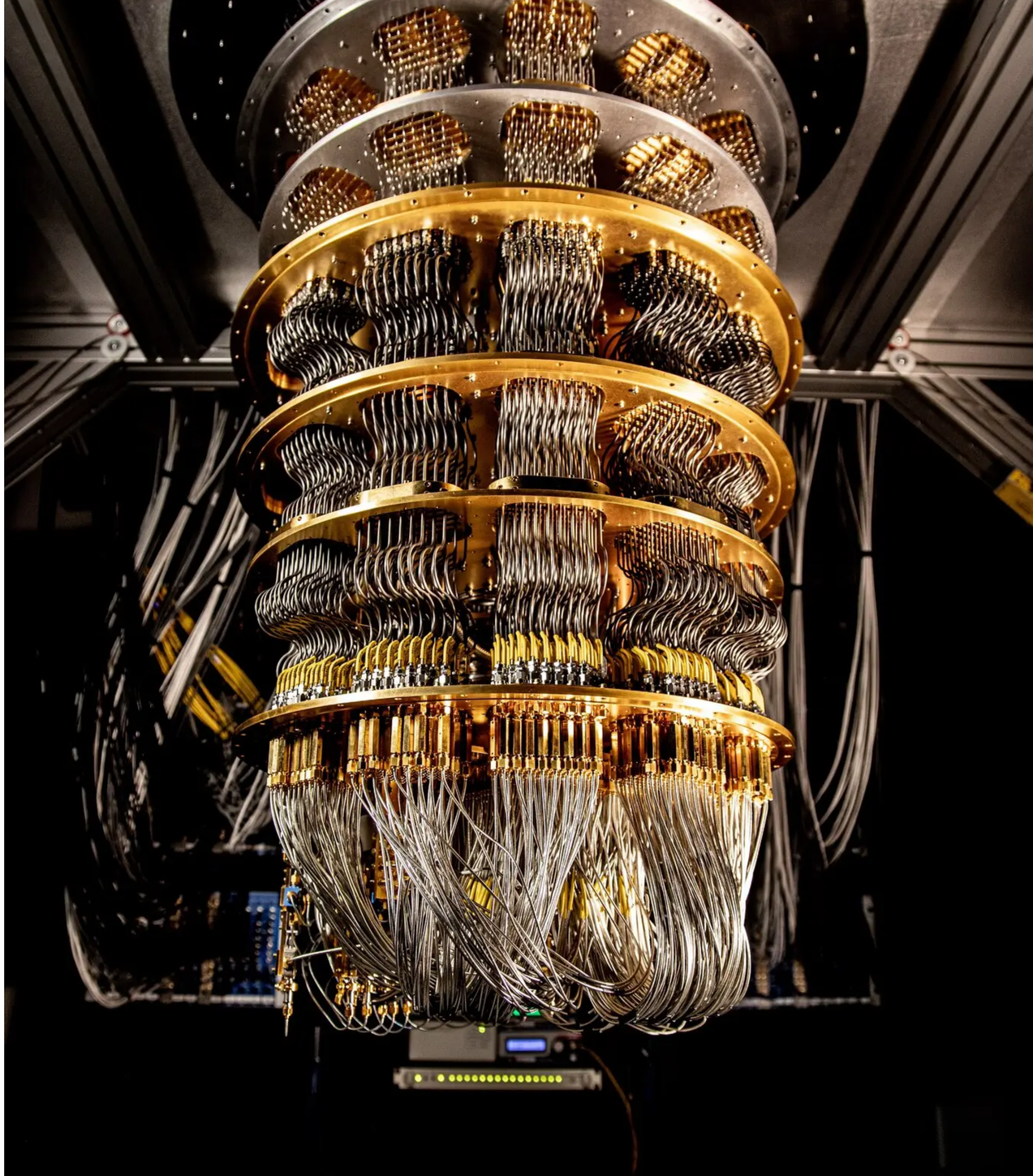
Post-Quantum Cryptography

A Practical Overview

17 53c | Ruslan Kiyanchuk – August 2025

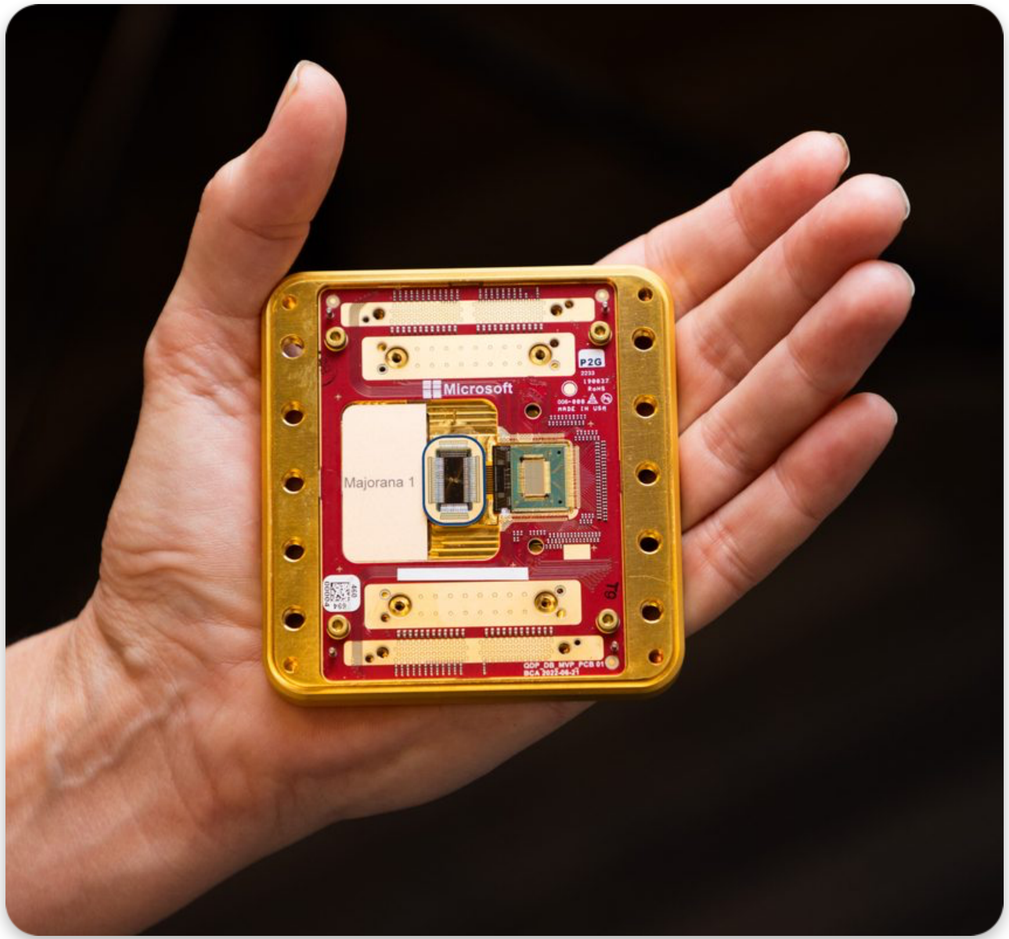


Quantum Computer

A physical computational device
that uses the principles of **quantum mechanics**

- Superposition
- Entanglement
- Interference

Described by Richard Feinman in 1981



Source: Microsoft

Computer Model

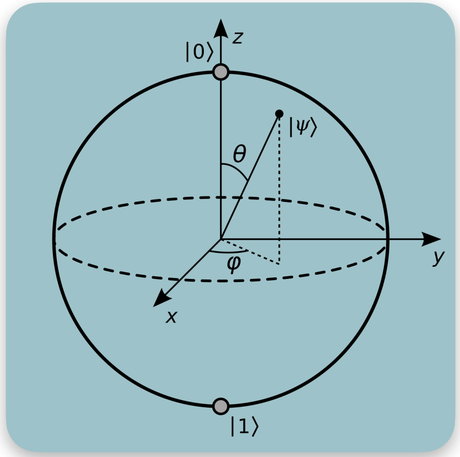
Classical: Turing Machine

Quantum: Quantum Turing Machine

Principles of Quantum Computer

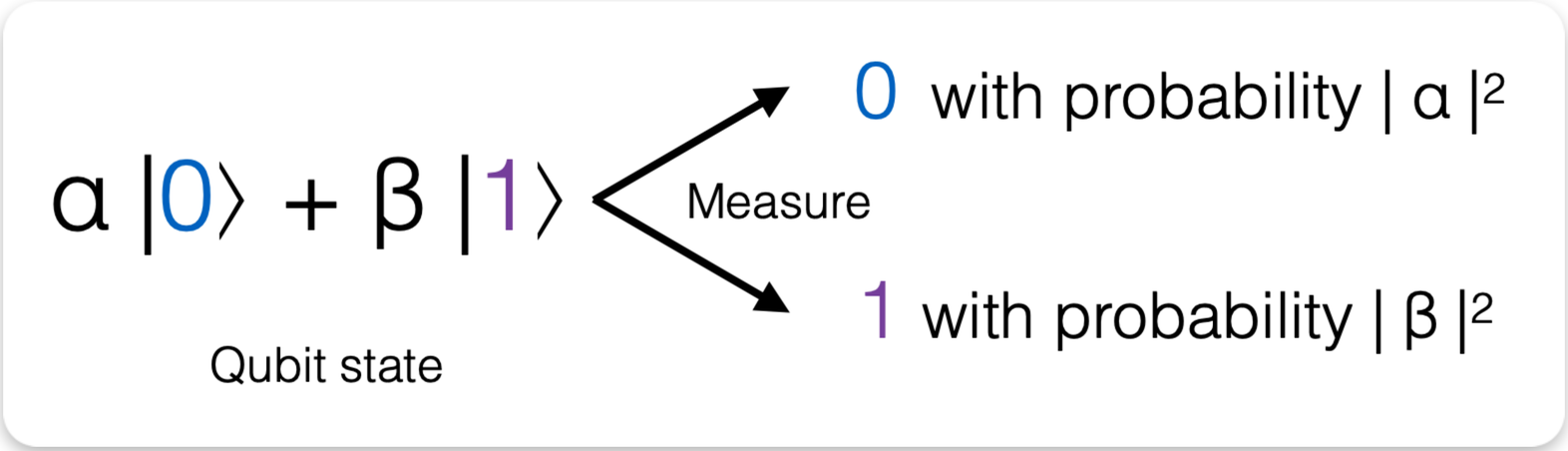
Bit

- 0 or 1



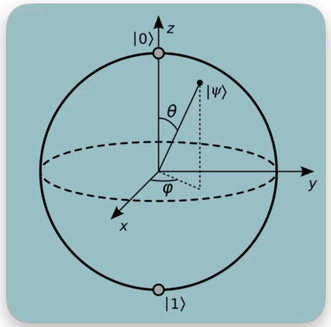
Qubit – *quantum* bit

- Exists in two states *simultaneously*,
  with a certain probability (principle of **superposition**)

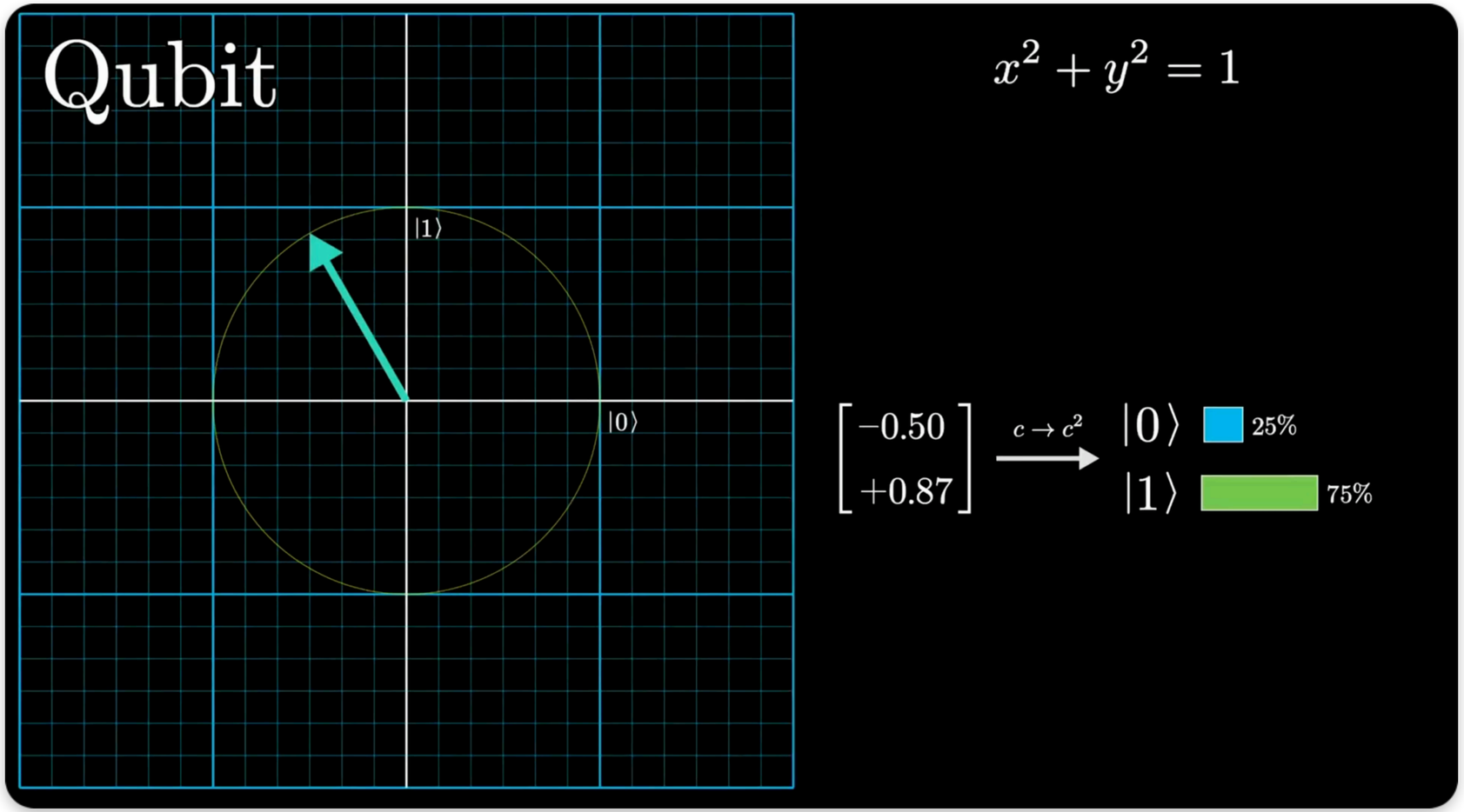


Principles of Quantum Computer

Bit vs Qubit

	Bit	Qubit
State	0/1	
What you observe	0/1	0/1

Principles of Quantum Computer



Source: 3Blue1Brown

Principles of Quantum Computer

Quantum computations

Classic n-bit register

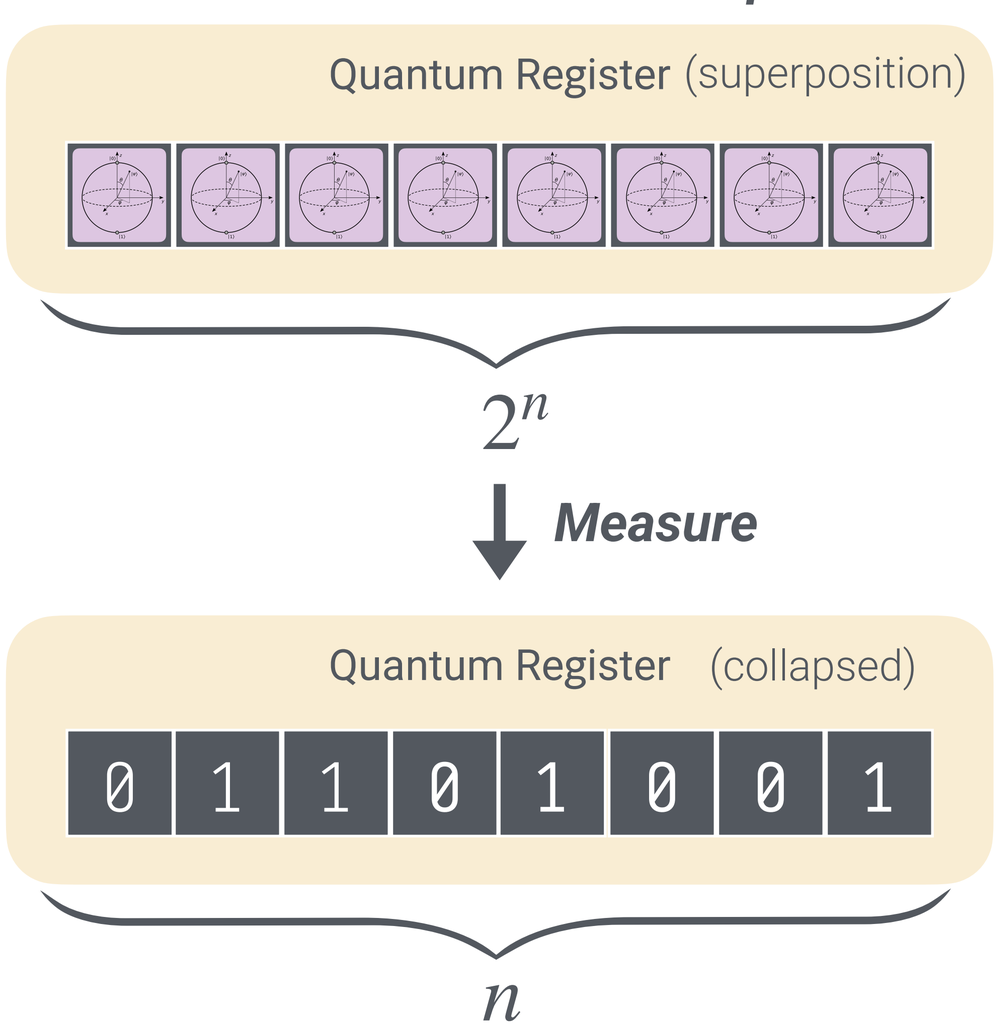
- Holds single n-bit state
- To explore all possible states of n-bit register:
  - 2^n registers
  - Perform 2^n operations over n-bit register

Principles of Quantum Computer

Quantum computations

Quantum n-qubit register

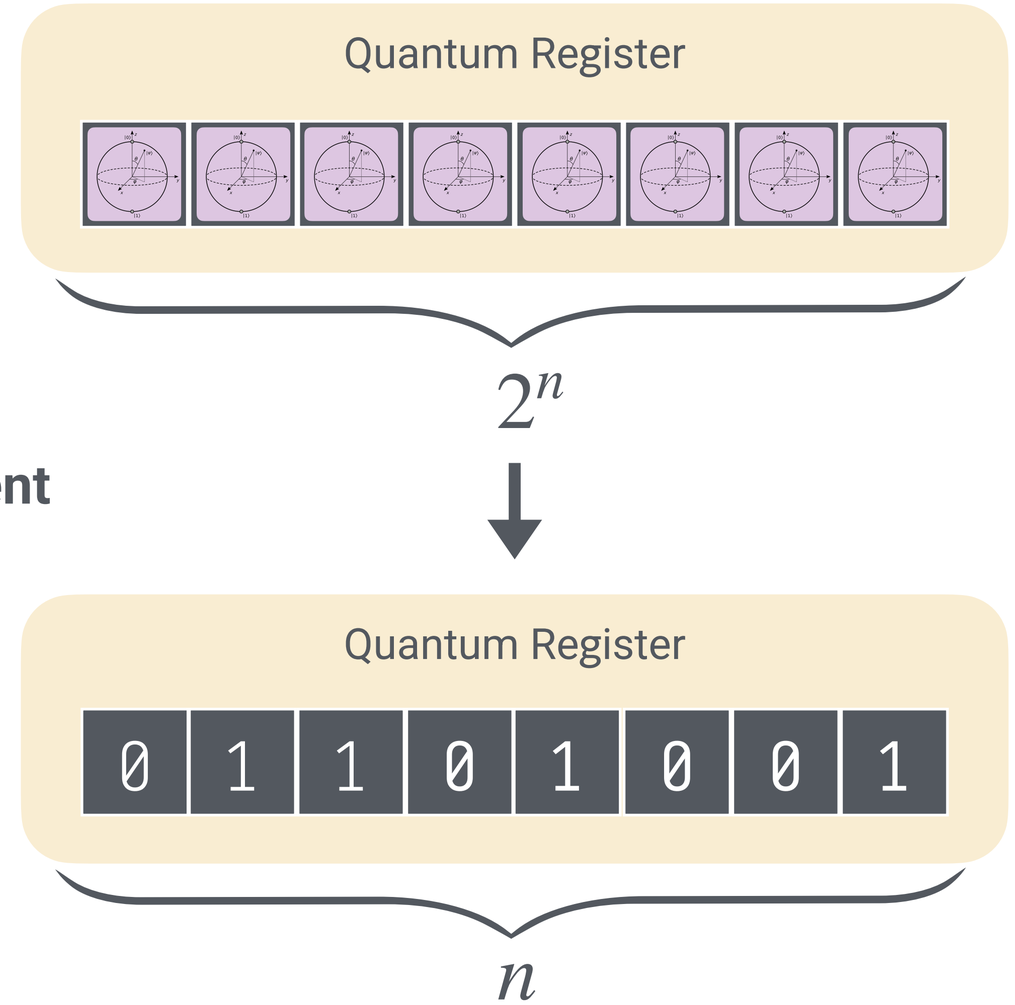
- Can hold 2^n states **simultaneously**.
- **Quantum computations are not parallel**
- Function $f : \{0,1\}^n \rightarrow \{0,1\}^n$ over n-qubit register is computed over [superposition] of **all** 2^n states.
- Results are obtained upon **measuring** the state.
- At the time of measurement, the register state **collapses** into a single value according to ***probability distribution.***



Quantum algorithms

Goal of quantum algorithms:

To exploit **quantum phenomena** in such a way that,
the **most probable state** of the qubits **upon measurement**
corresponds to a correct **solution**.



Grover's algorithm

(1996)

- Quantum algorithm for **unstructured search**
- Enables efficient search among N possible values of $F(x) \rightarrow h$ in $\sqrt{N}$ operations

What does it mean?

Proved to be the best possible algorithm

- `AES-128` $\Rightarrow 2^{128}$ ops required to break
  - $F(x) \rightarrow$ `AES-128`: key retrieval for $2^{n/2} = 2^{128/2} = 2^{64}$ ops
  - Cryptographic strength drops from **128** to **64** bits
- `SHA-256` $\Rightarrow$ pre-image recovery: $2^n = 2^{256}$
  - $F(x) \rightarrow$ `SHA-256`: preimage recovery for $2^{n/2} = 2^{128}$
  - pre-image resistance drops from **256** to **128** bits

Symmetric cryptography

- Key sizes <256 become weak

Shor's algorithm

(1994)

- Effectively solves number **factorization**
- Extends to solve **discrete logarithm problem**

What does it mean?

Asymmetric cryptography based on **trap functions**

- **RSA**
  - Factorization of $n = p \cdot q$
- **Finite Field Diffie-Hellman** (FFDH)
  - Discrete Logarithm Problem (DLP): $Y = g^x \mod p$
- **Elliptic Curve Diffie-Hellman** (ECDH)
  - ECDLP: $Y = x \cdot G$

Asymmetric cryptography

Broken:

- RSA
- Diffie-Hellman
  - FFDHE, X25519, X448...
- Elliptic Curve Digital Signatures
  - ECDSA, EdDSA, Ed25519, Schnorr signatures, BLS...

And all protocols using them:

- TLS, SSH, WireGuard, Signal..., CAs, software signatures, update channels, ...
- **Harvest Now Decrypt Later** attacks

Quantum Threat

Algorithm	Key length	Security Level Conventional Computer		Security Level Quantum Computer	
RSA-1024	1024 bits	80 bits	BROKEN	0 bits	BROKEN
RSA-2048	2048 bits	112 bits	VIABLE	0 bits	
ECC-256	256 bits	128 bits		0 bits	
ECC-384	384 bits	256 bits		0 bits	
AES-128	128 bits	128 bits		64 bits	
AES-256	256 bits	256 bits		128 bits	VIABLE

State of Quantum Computers

What quantum computers do we have?

1998: **2** qubits

2017: **50** qubits (IBM)

2019: **53** qubits (Google)

2021: **127** qubits (IBM)

2022: **433** qubits (IBM)

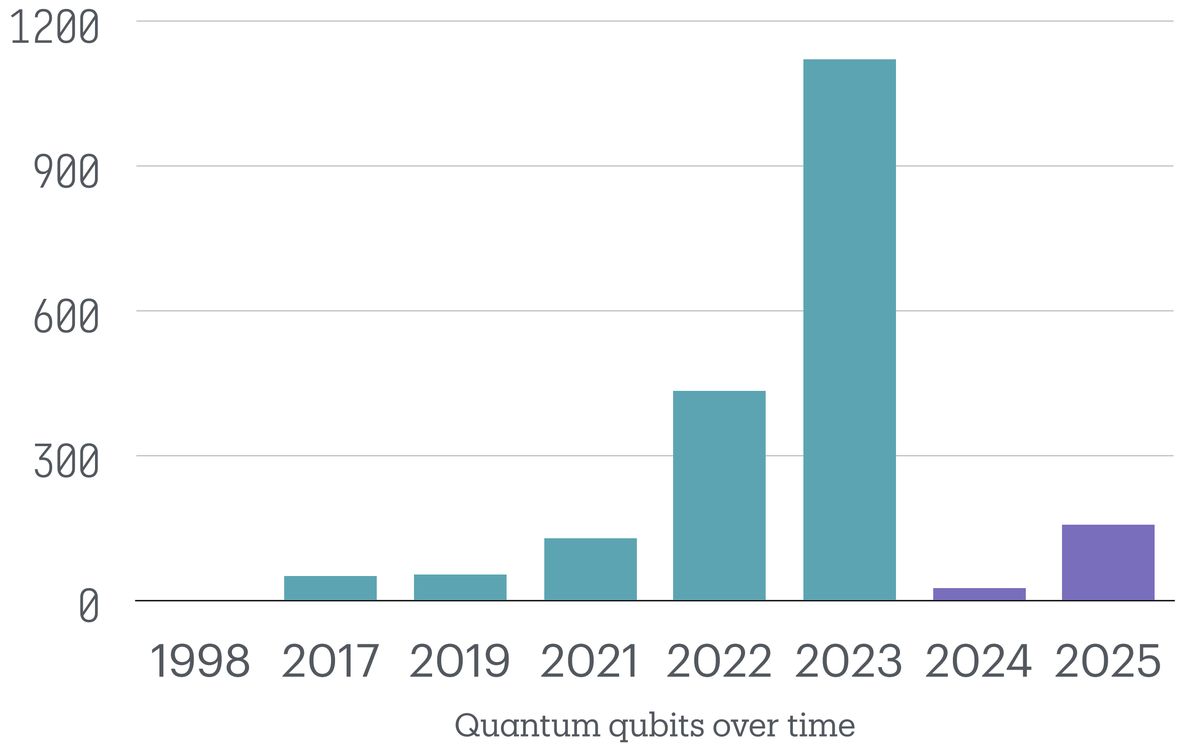
2023: **1121** qubits (IBM Condor)

2024: **24** logical qubits (Microsoft)

2024: **105** logical qubits (Google Willow)

2024: **156** logical qubits (IBM)

- IBM plans **2000** logical qubits after 2033+



Quantum qubits over time

State of Quantum Computers

What quantum computers do we need?

Cryptographically Relevant Quantum Computer

Quantum computer powerful enough to run cryptanalysis of modern cryptographic algorithms

	Circuit depth	Logical qubits	Serial overhead	Parallel overhead	Ref.
k	D_{AES}	W_{AES}	$D_{\mathrm{AES}}W_{\mathrm{AES}}$	$D^2_{\mathrm{AES}}W_{\mathrm{AES}}$	
	110,799	984	$2^{26.7}$	$2^{43.5}$	[13]
	1,090	2,896	$2^{21.6}$	$2^{31.7}$	[15]
128	**731**	**3,428**	$\mathbf{2^{21.3}}$	$\mathbf{2^{30.8}}$	[15]
	667	4,708	$2^{21.6}$	$2^{31.0}$	[15]

Qubits requirement for Grover's algorithm (2024)

How to factor 2048 bit RSA integers with less than a million noisy qubits

(~4000 logical qubits)

Craig Gidney

Google Quantum AI, Santa Barbara, California 93117, USA

June 9, 2025

Qubits requirement for Shor's algorithm (2025)

- Largest number factored **using Shore's algorithm**: $21 = 3 \times 7$

- *Quantum annealing* computers (D-Wave) are specialized for *optimization problems*
  - Cannot run Shore's algorithm
  - Factoring algorithms using *quantum optimization* approach **do not scale** to RSA-size numbers.

Solution?

Create **new** cryptographic algorithms for **classical computers**, that have **no efficient quantum algorithms** for cryptanalysis

Quantum vs **Post-Quantum** Crypto

Quantum Cryptography

- Utilizes quantum mechanics for enabling security properties
  - Quantum Key Distribution
- Requires quantum machinery for operation
- Not suitable for classical computers and networks
- Not practical

Post-Quantum Cryptography (PQC)

- Designed for **classical computers**
- **Resistant** to attacks using **quantum computations** (we don't know efficient quantum algorithms to break them)

Post-Quantum Cryptography

Categories of algorithms

Lattice-based

Hash-based

Code-based

Multivariate schemes

Isogenies

Post-Quantum Cryptography

Families of algorithms categorized by math aparatus

- **Lattice**-based

  Based on hardness of **shortest vector problem** in high-dimensional algebraic lattices.

- **Hash**-based

  Hardness of reverting hash (finding pre-image), combining key pairs using Merkle trees.

- **Code**-based

  Hardness of decoding a random linear error-correcting code.

- **Multivariate schemes**

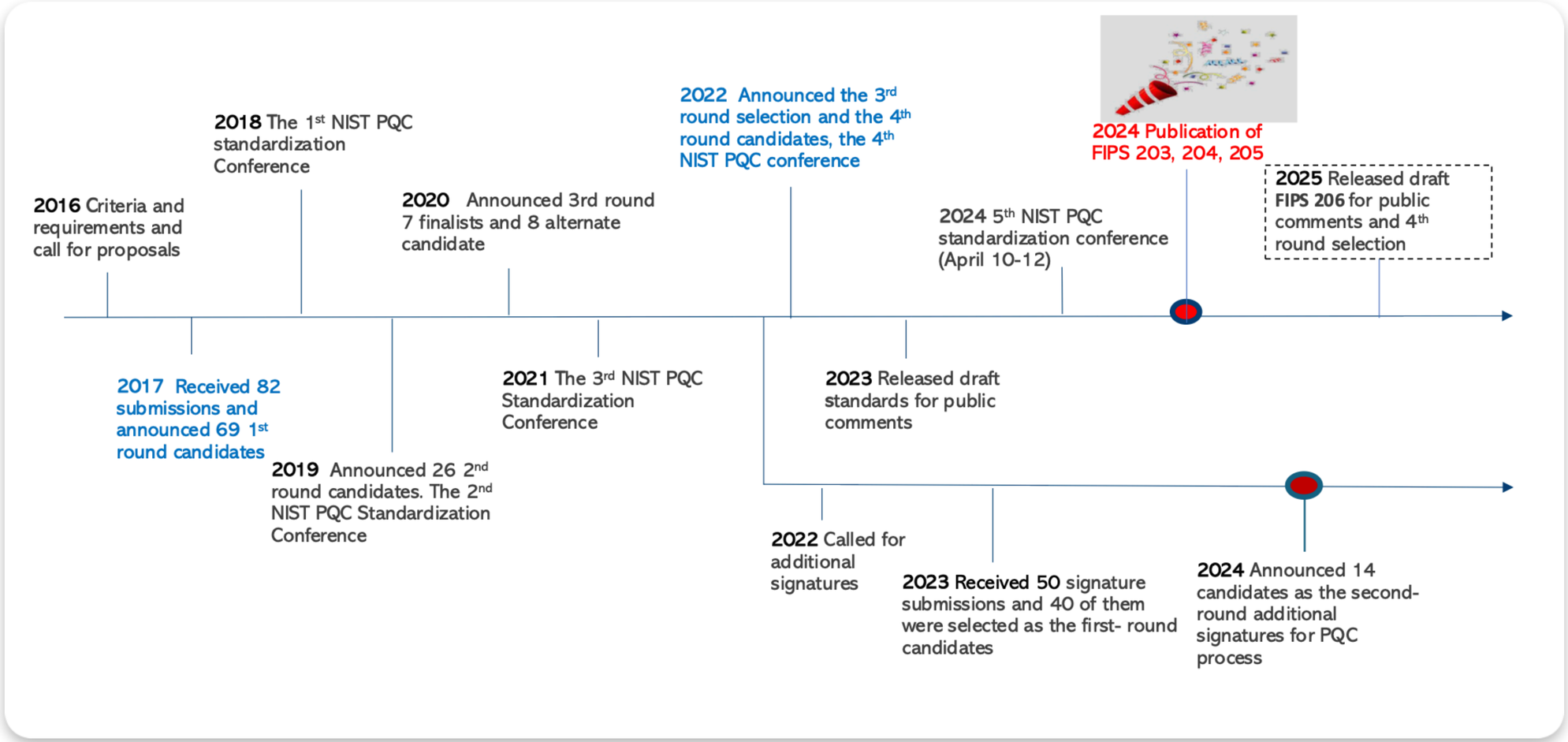
  Hardness of solving systems of nonlinear multivariate quadratic equations.

- **Isogenies**

  Hardness of finding special mappings between elliptic curves (isogenies).

PQC Standardization

Initiated by the National Institute of Standards and Technology (NIST) in 2016



Source: NIST PQC: The Road Ahead

PQC Algorithms Standards

- **FIPS-203: ML-KEM** (CRYSTALS-Kyber)
  Module-Lattice based Key Encapsulation Mechanism

- **FIPS-204: ML-DSA** (CRYSTALS-Dilithium)
  Module-Lattice based Digital Signature Algorithm

- **FIPS-205: SLH-DSA** (SPHINCS+)
  Stateless Hash-Based Digital Signature Algorithm

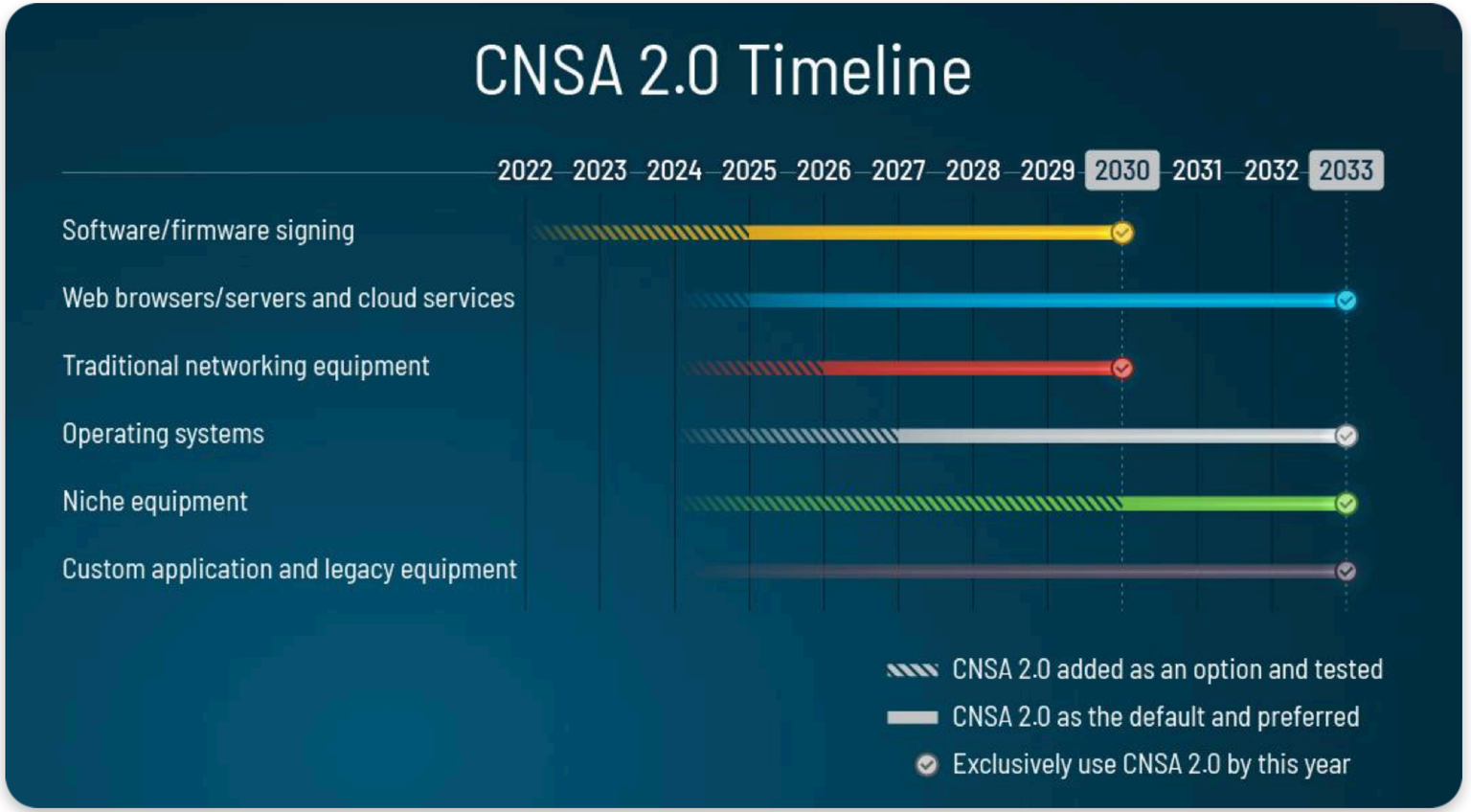
- **FIPS-206** [Draft]: **FN-DSA** (Falcon)
  Fast Fourier lattice-based compact signatures over NTRU

- **FIPS-???:** [Selected] (HQC)
  Code-based public key encryption scheme

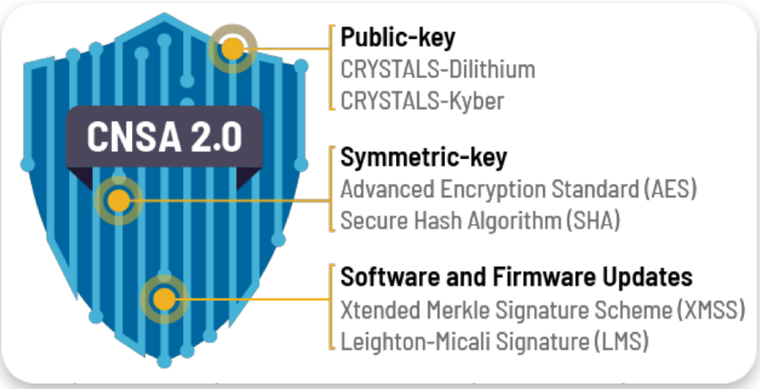
- **NIST SP 800-208: LMS, XMSS**
  Stateful hash-based digital signature algorithms; approved in 2020 for *software signing*.

Regulations: USA

The Commercial National Security Algorithm Suite (CNSA) 2.0



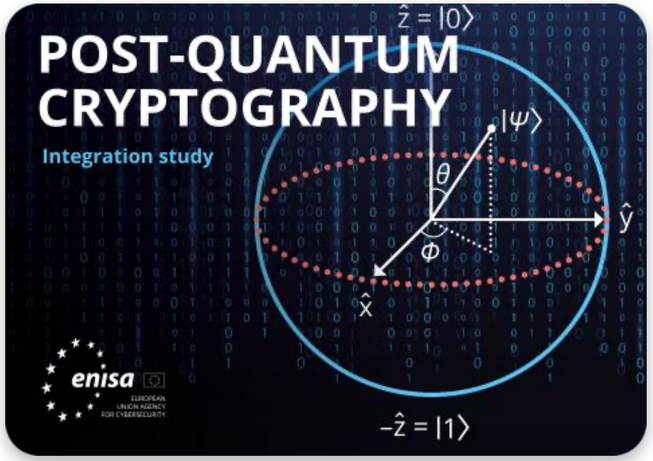
Source: NSA Cybersecurity Advisory



- Announced by NSA in 2022
- Deprioritized in 2025 by Executive Order 14306

Regulations: EU

- 2024-11: **A joint statement from partners from 18 EU member states**
  - Member states should **start transition** to PQC by the end of **2026**
  - Transition **critical infrastructure**: ASAP, no later than the end of **2030**



Source: ENISA

Regulations: EU

- 2025-06: **Coordinated Implementation Roadmap**
  - By 2026
    - **Roadmaps** for transition established by all Member States.
    - Transition & pilots of **medium-** to **high-risk** use cases initiated.
  - By 2030
    - Transition of **high-risk** use cases **completed**.
    - Quantum-safe **software** and **firmware** upgrades enabled **by default.**
  - By 2035
    - Transition of **medium-risk** use cases **completed**.
    - Transition of **low-risk** use cases **completed** as much as feasible.

Regulations: United Kingdom

- 2025-03: **Timelines for migration to PQC** by **National Cyber Security Center**
  - By 2028:
    - Full descovery and migration plan
  - By 2031:
    - Migrate high-priority properties
  - By 2035:
    - Complete migration to PQC of all systems
- Endorses NIST standards

Properties of PQC algorithms

Key Encapsulation

Parameter Set	Private Key (Decapsulation)	Public Key (Encapsulation)	Ciphertext	Shared Secret	Cycles (enc/dec)
X25519	32 B	32 B	—	32 B	125K/125K
RSA-2048	1 700 B	256 B	256 B	32 B	—
ML-KEM-512	1 632 B	800 B	768 B	32 B	45K/59K
ML-KEM-768	2 400 B	1 184 B	1 088 B	32 B	68K/82K
ML-KEM-1024	3 168 B	1 568 B	1 568 B	32 B	97K/115K
HQC-128	2 305 B	2 249 B	4 433 B	64 B	419K/833K
HQC-192	4 586 B	4 522 B	8 978 B	64 B	946K/1.66M
HQC-256	7 317 B	7 245 B	14 421 B	64 B	1.83M/3.34M

Sources: Latacora, NIST

Properties of PQC algorithms

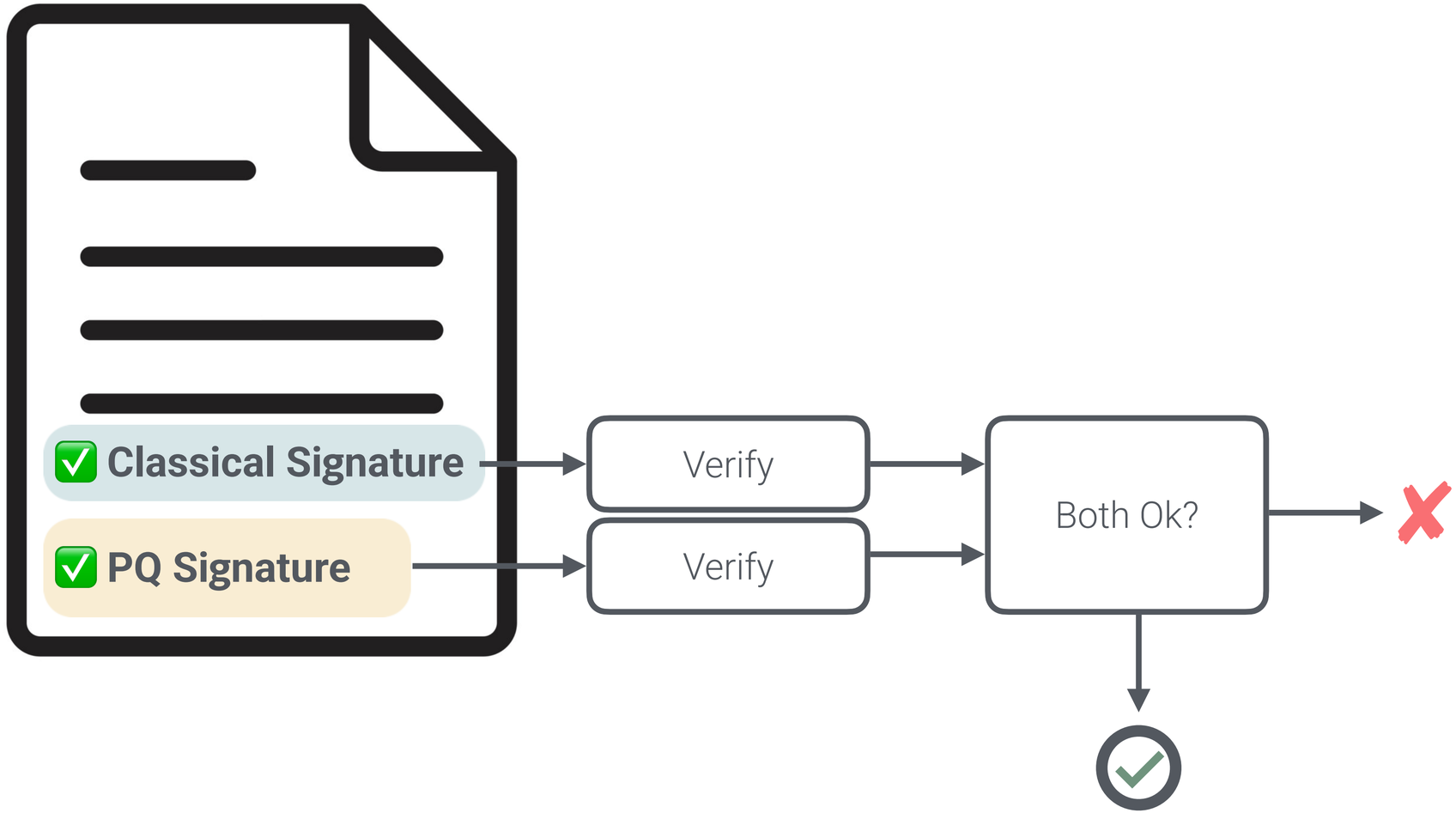
Signatures

Parameter Set	Private Key	Public Key	Signature Size	Cycles (sign/verify)
Ed25519	32 B	32 B	64 B	42K/130K
RSA-3072	384 B	387 B	384 B	—
ML-DSA-44	2 528 B	1 312 B	2 420 B	333K/118K
ML-DSA-65	4 000 B	1 952 B	3 293 B	529K/179K
ML-DSA-87	4 864 B	2 592 B	4 595 B	642k/279K
Falcon-512	1 281 B	897 B	690 B	1M/80K
Falcon-1024	2 305 B	1 793 B	1 280 B	2M/160K
SLH-DSA SHA2-128s	64 B	32 B	7 856 B	—
SLH-DSA SHA2-256f	128 B	64 B	49 856 B	51M/1.4M

Sources: Latacora, NIST

Real World Use: Hybrids

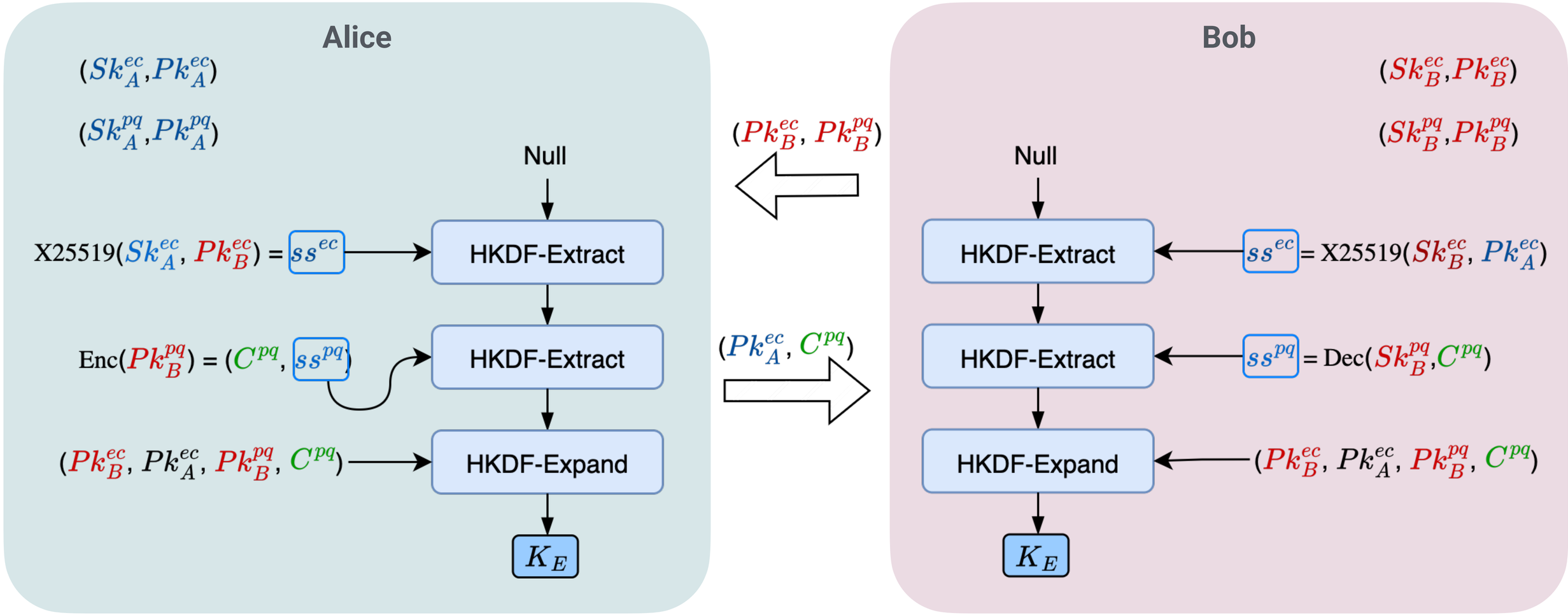
Signatures



Real World Use: Hybrids

Key Exchange

X25519MLKEM768



Adoption

Libraries

- OpenSSL 3.5 (March 2025)
  - The default TLS keyshares have been changed to offer **X25519MLKEM768** and **X25519**.
  - Support for PQC algorithms (ML-KEM, ML-DSA and SLH-DSA)
- AWS libraries s2n-tls and s2n-quic support ECDH + Kyber, use it in AWS KMS.
- BoringSSL
- WolfSSL
- Bouncy Castle Crypto package for Java
- ❌ libsodium – no PQ support, but planned in roadmap for v 1.0.x
- liboqs – open source C library for quantum-safe cryptographic algorithms

Adoption

Tools and Services

- OpenSSH (2022): supports PQ since v9.0 (check your client with `❯ ssh -Q kex`)
- Signal protocol (2023): PQXDH = `X25519+Kyber1024`
- iMessage (2024): PQ3 = EC P-256 + Kyber-1024
- JDK 24 (March 2025)
  - Added support for ML-KEM and ML-DSA
- Go v1.24: supports `X25519MLKEM768`
- Browsers Support
  - Chrome ✅, Edge ✅, Firefox ✅, Safari ❌

Adoption

- IETF Draft: ML-DSA in X.509 Certificates
- IETF Draft: Hybrid key exchange in TLS 1.3

- Open Quantum Safe

  The Linux Foundation project for Post-Quantum software implementations

  - liboqs – an open source C library for quantum-resistant cryptographic algorithms
  - prototype integrations into protocols and applications (TLS, SSH, X.509)
  - Interop test server for quantum-safe cryptography

- Cloudflare PQ Key Agreement test and PQC Support page

Resources

- YouTube: But what is quantum computing? (Grover's Algorithm) by 3Blue1Brown
- YouTube: Step inside the Google Quantum AI lab
- Google's Threat model for Post-Quantum Cryptography
- IETF Draft: Post-Quantum Cryptography for Engineers
- SoK: The Engineer’s Guide to Post-Quantum Cryptography for Embedded Devices

Learning PQC:

1. A beginner’s guide to lattice cryptography by Cloudflare
2. Enough polynomials and linear algebra to implement kyber by Filippo Valsorda
3. Cryptography course on Kyber and Dilithium by Alfred Menezes

Keep in touch!

- **LinkedIn:** rkiyanchuk
- **Bsky:** @rkiyanchuk.bskysocial
- **Mastodon:** @ruslan@infosec.exchange
- **Email:** ruslan.kiyanchuk@gmail.com
- **Signal:** rkiyanchuk.46

SLIDES LINK