Post Quantum Cryptography

What, Why & How

Shyam Kumar Arshid

- PQC, Hardware security, cloud security at Siemens Technology.
- Previously Cybersecurity Research work at NCIIPC (Govt. of India) and secure embedded systems development at ISRO.

www.linkedin.com/in/shyam-kumar-arshid

Definition

Cryptography designed to protect against *attacks* from ***quantum* computers**, using algorithms that can be implemented on today's ***classical* computers.**

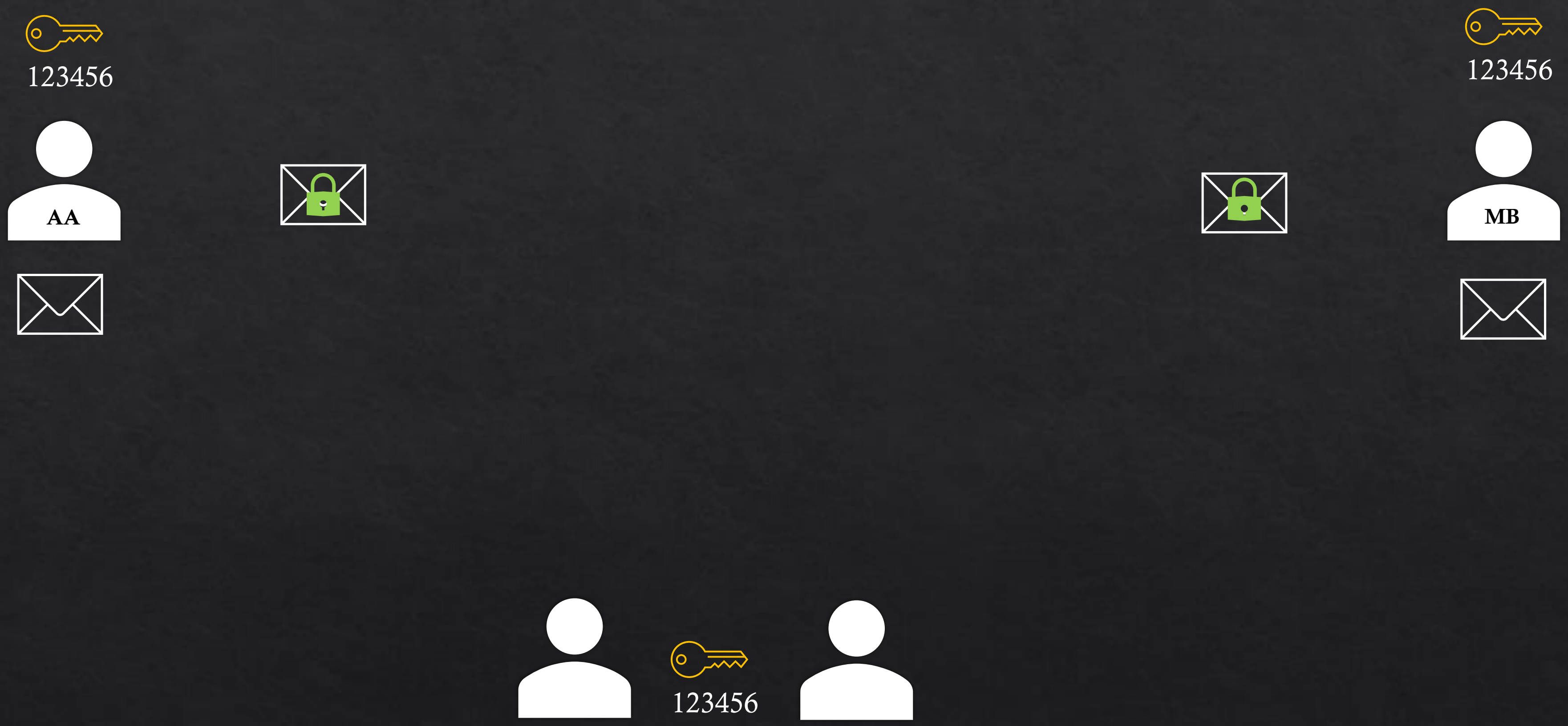
Risk

Harvest-now, decrypt-later (HNDL) or Store-now, decrypt-later (SNDL)

This makes PQC urgent *even before* a big quantum computer exists.

Forward secrecy?

Encryption: Sharing keys



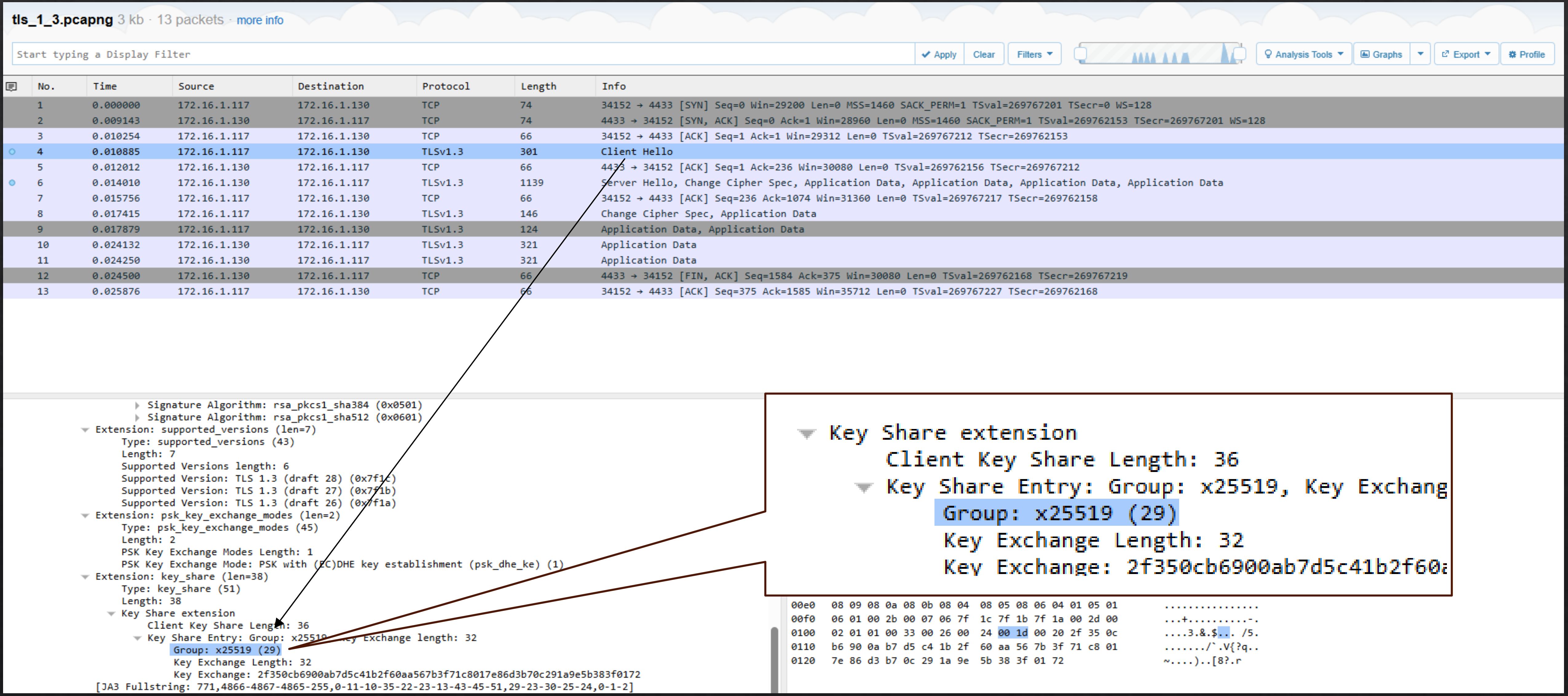
Two unknown persons share secret key physically : only secure option

Public key cryptography

given n, recover p_1, p_2 →**hard** when n is huge

easy forward, hard reverse (factoring)

TLS capture: Key Share



X25519: Elliptic Curve Diffie-Hellman key exchange

- **RSA:** "hard = factoring $n = p_1 p_2$"
- **X25519 :** "hard = discrete log on an elliptic-curve group: find $\boldsymbol{k}$ such that $\boldsymbol{Q} = \boldsymbol{kP}$"
- **The field size** (where all arithmetic happens)

  Curve25519 uses prime : p= $\mathbf{2^{255} - 19}$
- How many points / how big the search space is : $\mathbf{2^{252}}$
- Private key is essentially choosing a scalar in a space around 2^{252}
- **Attacker's goal :** given P(base point) and Q(public key), find k
- **Brute force:** try $k = 1,2,3,$ ...until $kP = Q$ $(\ldots\mathbf{2^{252}})$
- Best known generic attack still needs ~$\mathbf{2^{126}}$ **tries**

Number of operations/tries

850705917302346158658436518579420528 64

Try = one group-step in best generic attack (≈ point add/double)

Most powerful classical supercomputer: EL Capitan

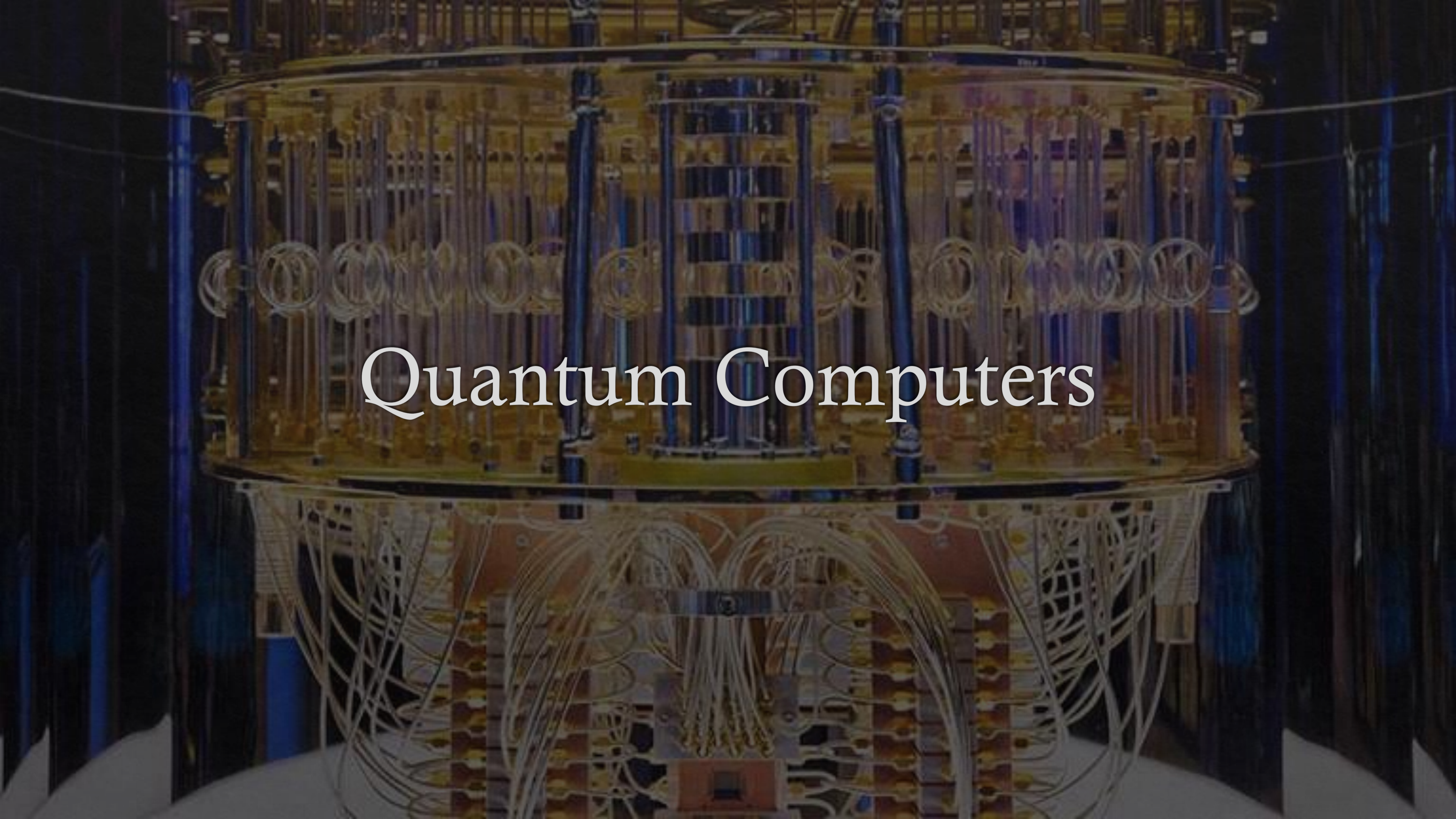
$\sim 2.8 \times 10^{18}$ ops/sec

$\approx$ 500k laptops

Time required to break ECC

- 9.5×10^{11} years using El Capitan

$\approx$ 1 trillion years



Quantum Computers

Fundamental changes with a quantum computer

Use of **quantum physics** to access new computational abilities.

Made of quantum bits (qubits) instead of bits.

Qubits can be in a superposition, or a complex combination, of both 0 and 1.

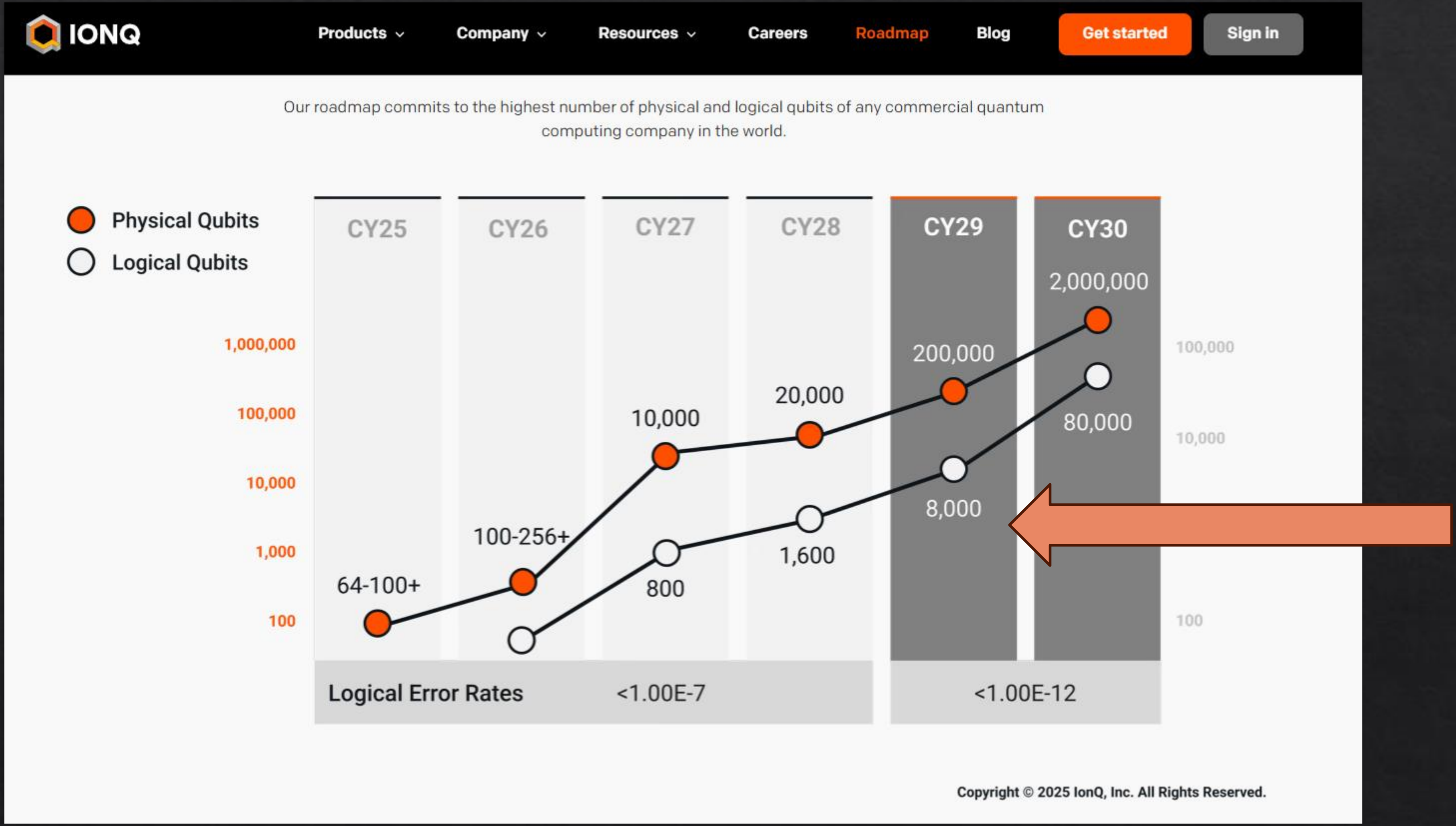
Shor’s algorithm, solves **discrete logs** efficiently on a fault-tolerant quantum computer.

Time required to break ECC-256 with quantum computer

- Using a QC with 50 million Toffoli gates (~6,000 logical qubits)

$\approx$ 10 minutes

Roadmaps target early 2030s+



Post-Quantum Cryptography algorithms (NIST)

- **NIST** finalized the first **PQC** standards (Aug 13, 2024) : resist quantum attacks, runs on classical computers.
  - **ML-KEM (key establishment)** → replaces **(EC)DHE / RSA key transport**
  - **ML-DSA (signatures)** → replaces **RSA / ECDSA**
  - **SLH-DSA (hash-based signatures)** → alternative to **RSA / ECDSA**

ML-KEM

- **ML-KEM (FIPS 203)** is a module-lattice KEM.
- Depends on hardness of **Module Learning With Errors (Module-LWE / MLWE)**: you see "almost-linear equations," but with **small random noise** added, and you must recover the secret.

> **"ECC hides the secret as a scalar on a curve; ML-KEM hides it as a noisy point in a high-dimensional lattice."**

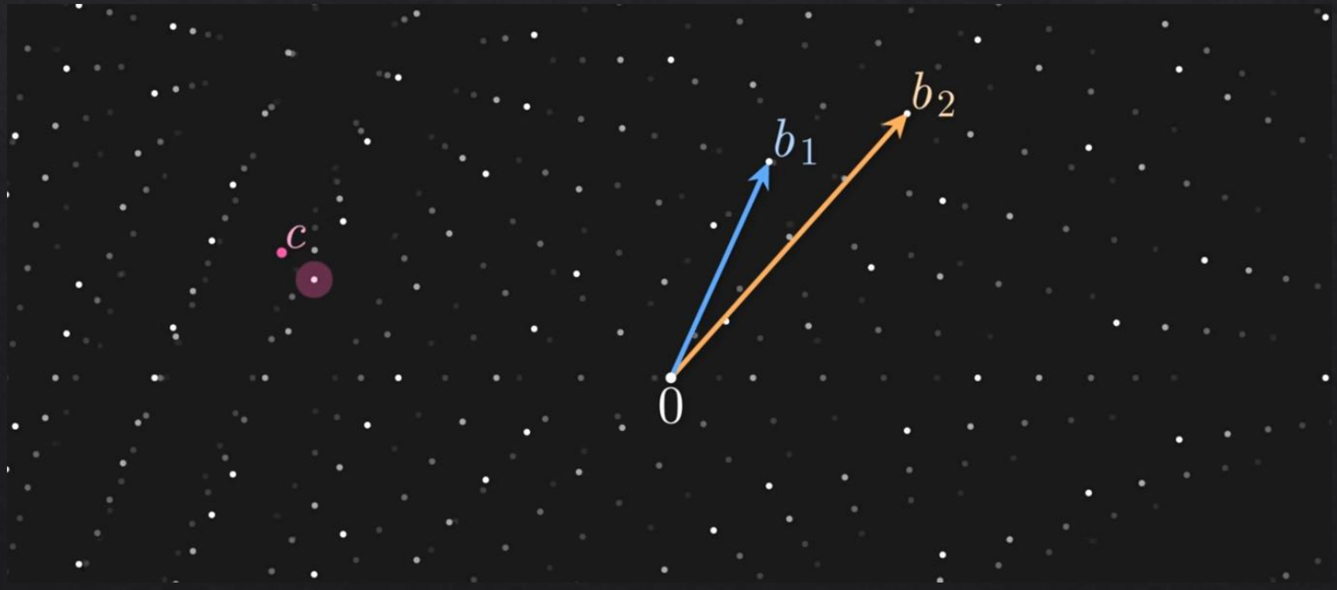


Image source: Veritasium

ECC vs ML-KEM

- ECC/RSA have a clean **periodic** structure under the hood; quantum Fourier analysis can 'read out' that period.

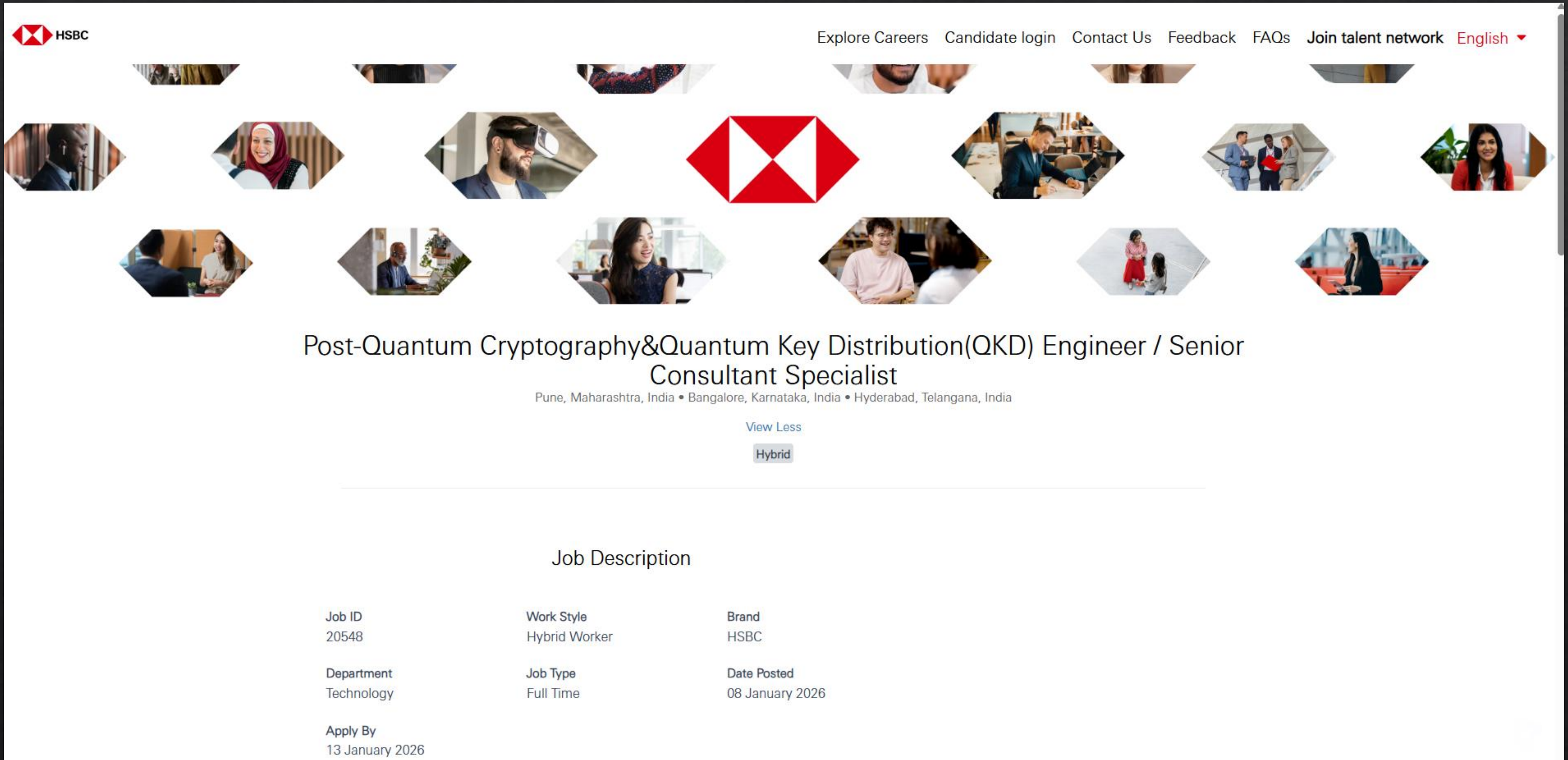
- Shor algorithm wins when the math is *perfectly structured*. LWE intentionally injects *small randomness,* so the structure is blurred.

PQC in Real World

- **Web browsing (TLS/HTTPS):** major stacks already use **hybrid key exchange** (classical X25519 + ML-KEM). Ex: Cloudfare
- **Browsers**: Chrome has been actively deploying hybrid PQ key exchange for HTTPS.
- **SSH**: OpenSSH has offered **post-quantum key agreement** by default since 9.0.
- **Messaging** apps: Signal & iMessage

PQC Job opening

This is already a hiring skill



https://portal.careers.hsbc.com/careers/job/563774608798825

Thank you