

What, Why & How

Post Quantum Cryptography



Shyam Kumar Arshid

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

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.

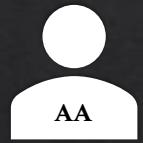


Forward secrecy?

Encryption: Sharing keys



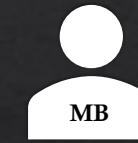
123456



AA



123456

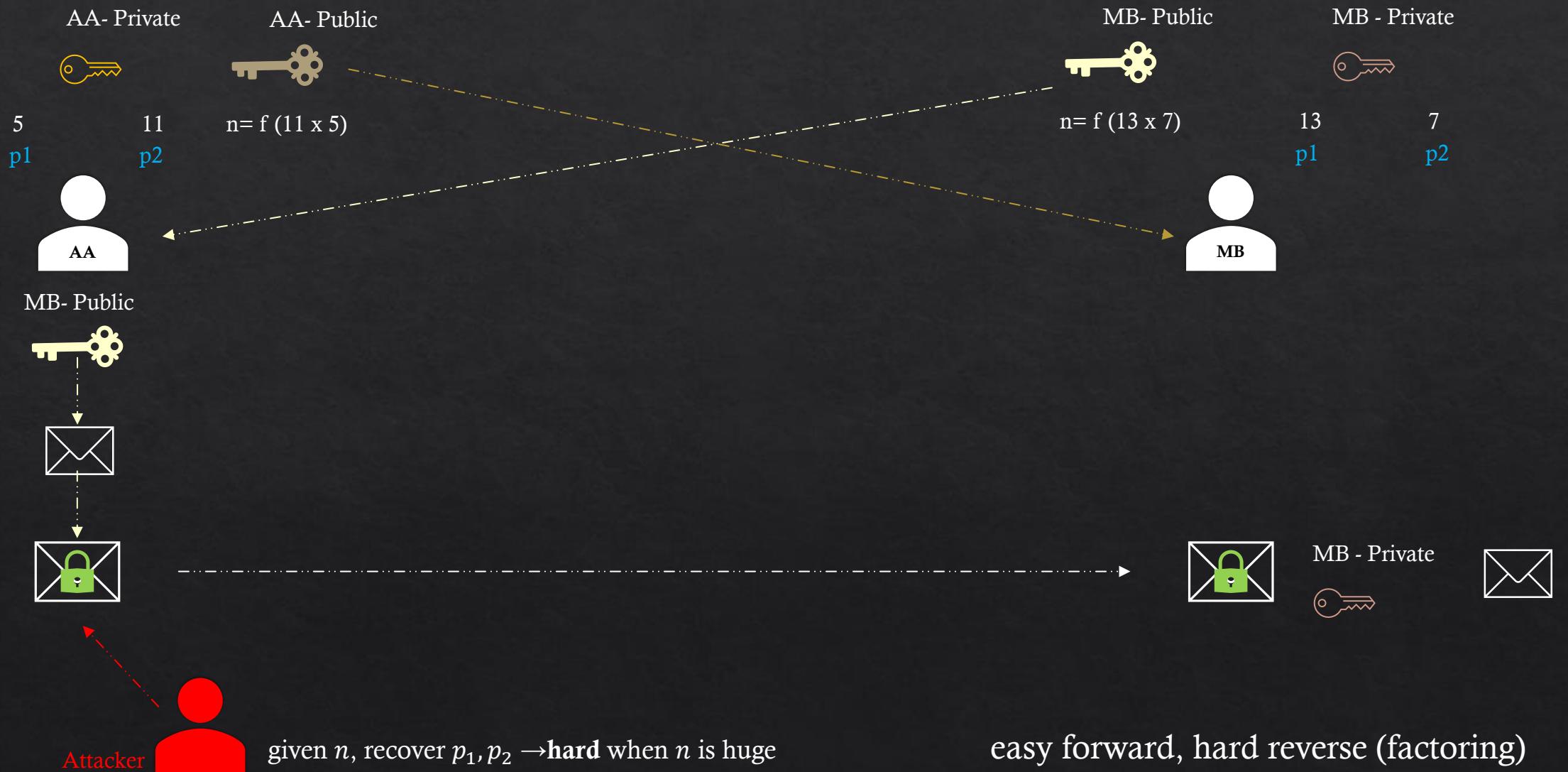


MB



Two unknown persons share secret key physically : only secure option

Public key cryptography



TLS capture: Key Share

tls_1_3.pcapng 3 kb · 13 packets · [more info](#)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.1.117	172.16.1.130	TCP	74	34152 → 4433 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=269767201 TSecr=0 WS=128
2	0.009143	172.16.1.130	172.16.1.117	TCP	74	4433 → 34152 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=269762153 TSecr=269767201 WS=128
3	0.010254	172.16.1.117	172.16.1.130	TCP	66	34152 → 4433 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=269767212 TSecr=269762153
4	0.010885	172.16.1.117	172.16.1.130	TLSv1.3	301	Client Hello
5	0.012012	172.16.1.130	172.16.1.117	TCP	66	4433 → 34152 [ACK] Seq=1 Ack=236 Win=30080 Len=0 TSval=269762156 TSecr=269767212
6	0.014010	172.16.1.130	172.16.1.117	TLSv1.3	1139	Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Application Data
7	0.015756	172.16.1.117	172.16.1.130	TCP	66	34152 → 4433 [ACK] Seq=236 Ack=1074 Win=31360 Len=0 TSval=269767217 TSecr=269762158
8	0.017415	172.16.1.117	172.16.1.130	TLSv1.3	146	Change Cipher Spec, Application Data
9	0.017879	172.16.1.117	172.16.1.130	TLSv1.3	124	Application Data, Application Data
10	0.024132	172.16.1.130	172.16.1.117	TLSv1.3	321	Application Data
11	0.024250	172.16.1.130	172.16.1.117	TLSv1.3	321	Application Data
12	0.024500	172.16.1.130	172.16.1.117	TCP	66	4433 → 34152 [FIN, ACK] Seq=1584 Ack=375 Win=30080 Len=0 TSval=269762168 TSecr=269767219
13	0.025876	172.16.1.117	172.16.1.130	TCP	66	34152 → 4433 [ACK] Seq=375 Ack=1585 Win=35712 Len=0 TSval=269767227 TSecr=269762168

► Signature Algorithm: rsa_pkcs1_sha384 (0x0501)
► Signature Algorithm: rsa_pkcs1_sha512 (0x0601)
▼ Extension: supported_versions (len=7)
 Type: supported_versions (43)
 Length: 7
 Supported Versions length: 6
 Supported Version: TLS 1.3 (draft 28) (0x7f1c)
 Supported Version: TLS 1.3 (draft 27) (0x7f1b)
 Supported Version: TLS 1.3 (draft 26) (0x7f1a)
▼ Extension: psk_key_exchange_modes (len=2)
 Type: psk_key_exchange_modes (45)
 Length: 2
 PSK Key Exchange Modes Length: 1
 PSK Key Exchange Mode: PSK with (EC)DHE key establishment (psk_dhe_ke) (1)
▼ Extension: key_share (len=38)
 Type: key_share (51)
 Length: 38
 ▼ Key Share extension
 Client Key Share Length: 36
 ▼ Key Share Entry: Group: x25519, Key Exchange length: 32
 Group: x25519 (29)
 Key Exchange Length: 32
 Key Exchange: 2f350cb6900ab7d5c41b2f60...
 [JAX Fullstring: 771,4866-4867-4865-255,0-11-10-35-22-23-13-43-45-51,29-23-30-25-24,0-1-2]

▼ Key Share extension
 Client Key Share Length: 36
 ▼ Key Share Entry: Group: x25519, Key Exchange length: 32
 Group: x25519 (29)
 Key Exchange Length: 32
 Key Exchange: 2f350cb6900ab7d5c41b2f60...
 [JAX Fullstring: 771,4866-4867-4865-255,0-11-10-35-22-23-13-43-45-51,29-23-30-25-24,0-1-2]

00e0	08 09 08 0a 08 0b 08 04	08 05 08 06 04 01 05 01
00f0	06 01 00 2b 00 07 06 7f	1c 7f 1b 7f 1a 00 2d 00	...+.....
0100	02 01 01 00 33 00 26 00	24 00 1d 00 20 2f 35 0c	...3.&,\$.. /5.
0110	b6 90 0a b7 d5 c4 1b 2f	60 aa 56 7b 3f 71 c8 01/.V{?q..
0120	7e 86 d3 b7 0c 29 1a 9e	5b 38 3f 01 72	~....)...[8?.r

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 k such that $Q = kP$ ”
- ❖ **The field size** (where all arithmetic happens)

Curve25519 uses prime : $p = 2^{255} - 19$

- ❖ How many points / how big the search space is : 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 $k = 1, 2, 3, \dots$ until $kP = Q$ ($\dots 2^{252}$)
- ❖ Best known generic attack still needs $\sim 2^{126}$ tries



Number of operations/tries

85070591730234615

86584365185794205

2864

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

Most powerful classical supercomputer: EL Capitan



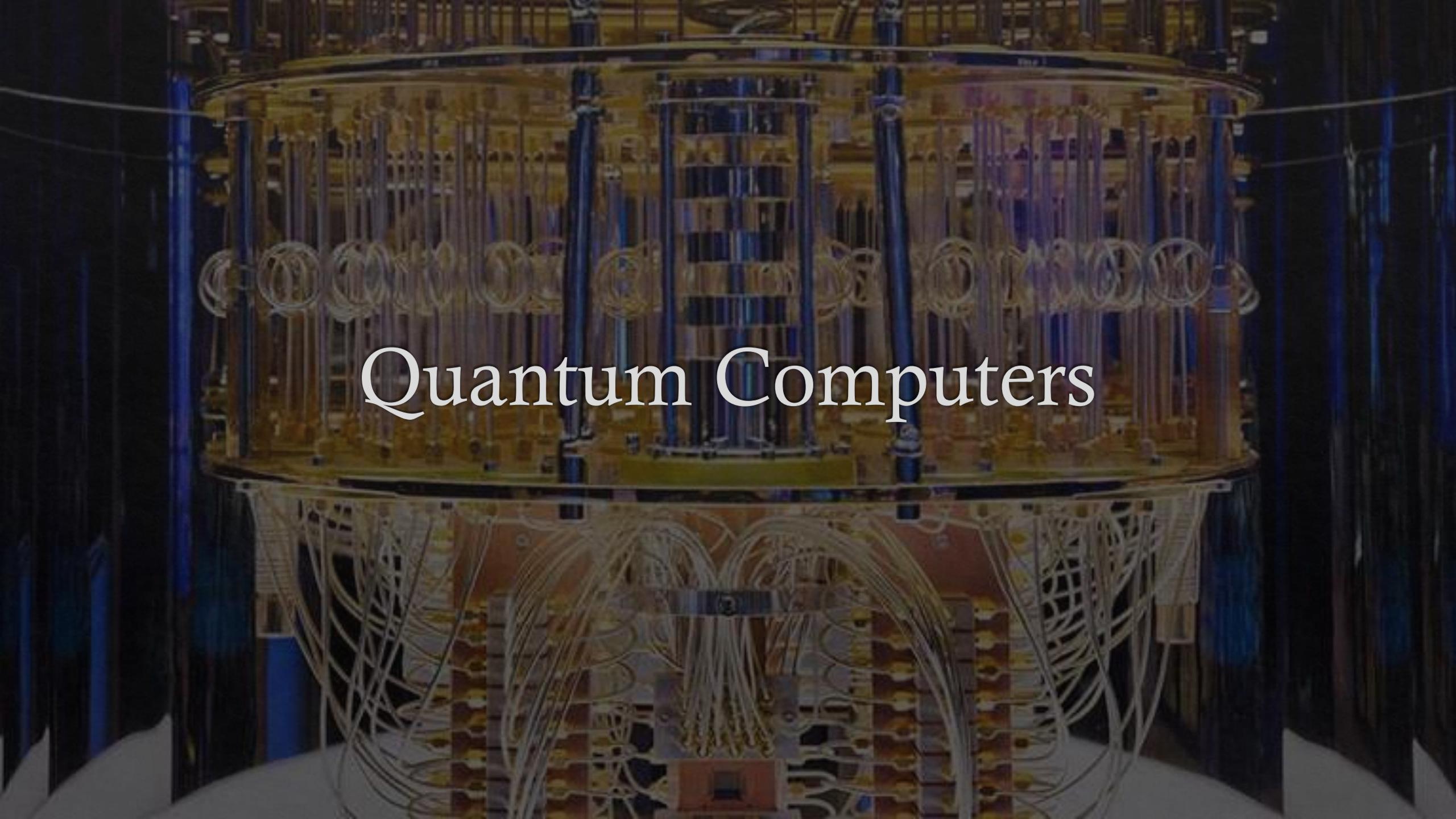
$\sim 2.8 \times 10^{18}$ ops/sec

\approx 500k laptops

Time required to break ECC

- ◆ 9.5×10^{11} years using El Capitan

\approx 1 trillion years

A photograph of a large-scale quantum computing system. The central component is a large, cylindrical vacuum chamber with a complex internal structure. Numerous optical fibers and cables are visible, many of which are color-coded (blue, orange, red) and bundled together. The system is housed in a dark, industrial-looking enclosure with various ports and equipment visible around the perimeter.

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.

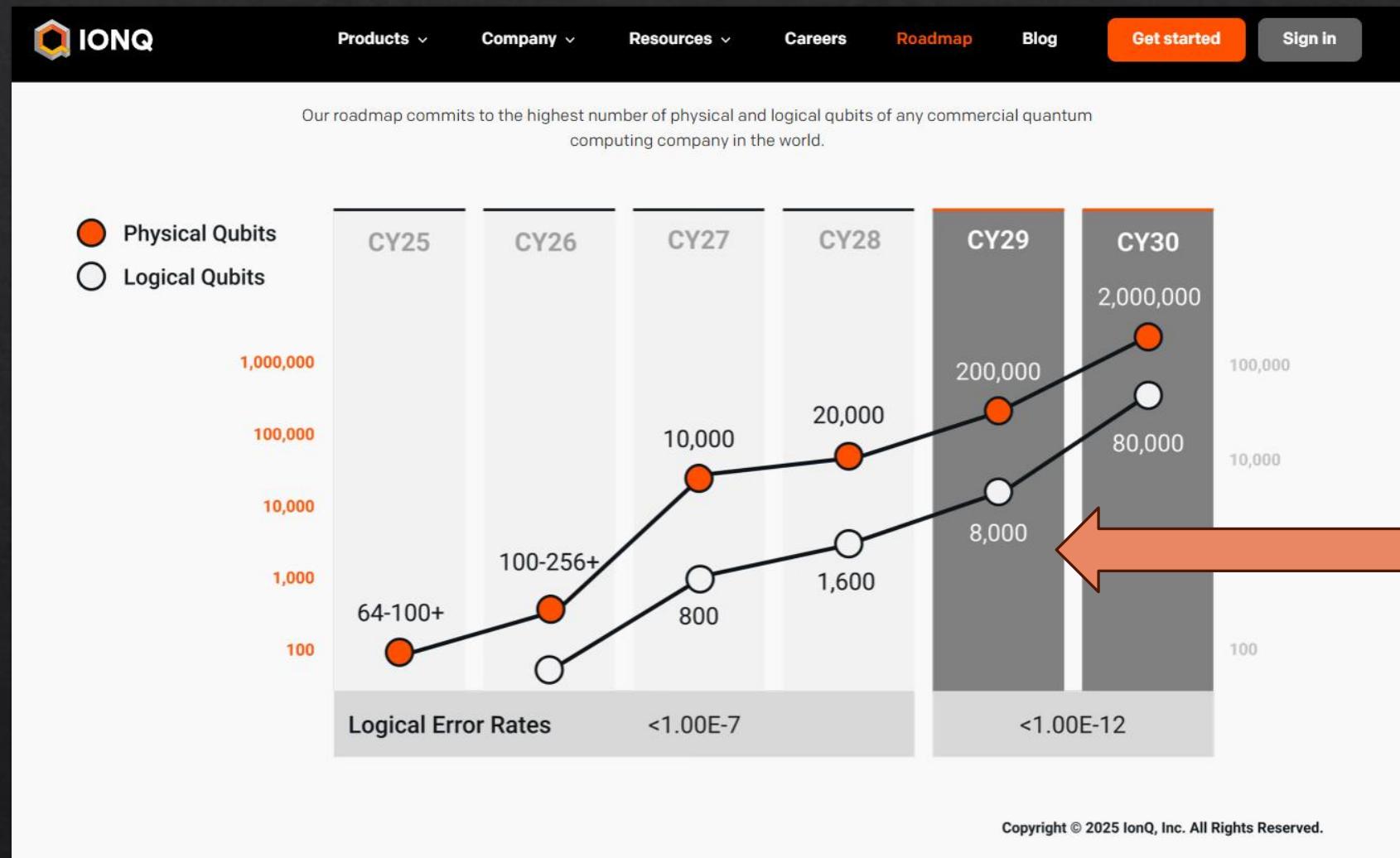
Shor's algorithm, solves **discrete logs** efficiently on a fault-tolerant quantum computer.

Time required to break ECC-256 with quantum computer

- ❖ Using a QC with 50 million Toffoli gates (\sim 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.”

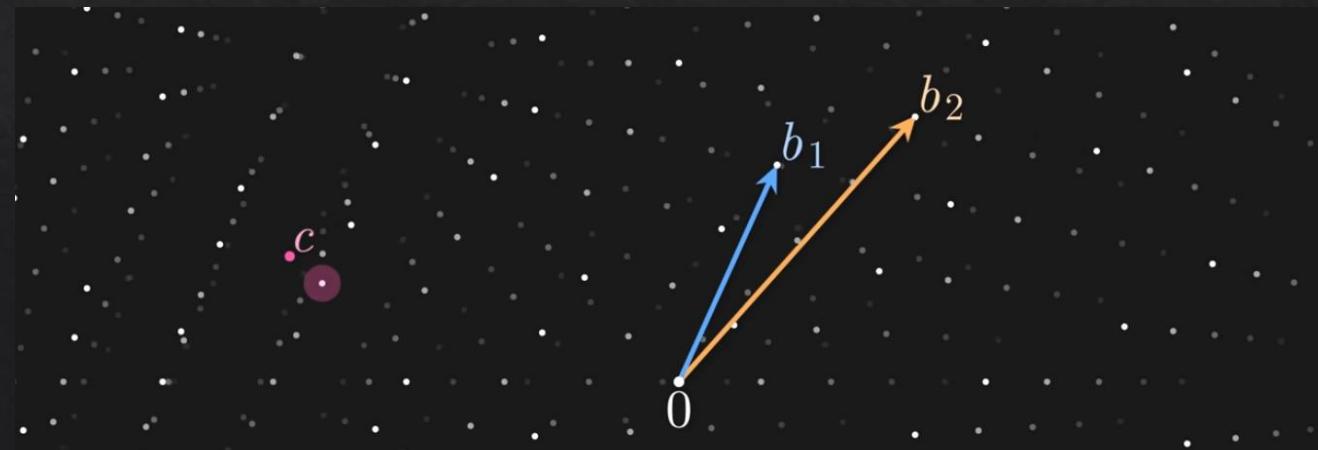


Image source: Veritasium

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: Cloudflare



- ❖ **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

HSBC

Explore Careers Candidate login Contact Us Feedback FAQs Join talent network English ▾

Post-Quantum Cryptography&Quantum Key Distribution(QKD) Engineer / Senior Consultant Specialist

Pune, Maharashtra, India • Bangalore, Karnataka, India • Hyderabad, Telangana, India

[View Less](#)

Hybrid

Job Description

Job ID 20548	Work Style Hybrid Worker	Brand HSBC
Department Technology	Job Type Full Time	Date Posted 08 January 2026

Apply By
13 January 2026

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

Thank you