Post Quantum Cryptography & Quantum Key Distribution

Maurizio Dècina
Professor Emeritus, Politecnico di Milano

Seminario ASTRID

Le tecnologie quantistiche: il ruolo dell'Italia nel contesto europeo

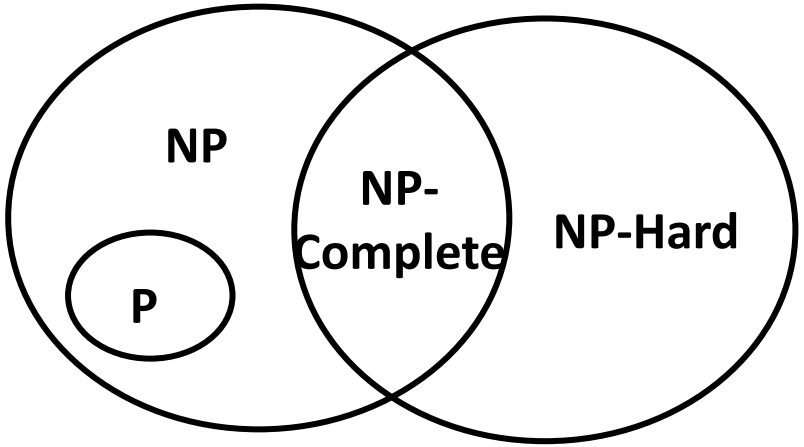
Roma, 17 Marzo, 2026

Topics

- *Today's Cryptosystems* on the Internet (asymmetric crypto: RSA, DH, ECC; symmetric crypto: AES, SHA)
- *Post Quantum Cryptography (PQC)*, 3 NIST Standards; CRISTAL-Kyber (lattice based), for key exchange, CRISTAL-Dilithium (lattice based) and SPHINCS+ (SHA based), for signatures. HQC Hamming Quasi-Cyclic (code based) is a future NIST standard for key exchange
- *Quantum Key Distribution (QKD)*, P2P quantum communication channels to transmit secure symmetric keys
- Quantum Entanglement communications
  - *Quantum Key Distribution*
  - *Quantum Repeaters*
  - *Quantum Networking/Quantum Internet*

RSA: Rivest, Shamir & Adleman - DH: Diffie & Hellman - ECC: Elliptic Curve Cryptography – AES: Advanced Encryption Algorithm -SHA: Secure Hash Algorithm - NIST: National Institute of Standards & Technology

Quantum Computing & Operations Research



P = Polynomial time Problems

NP: Non-deterministic Polynomial time Problen

Polynomial time		Exponential Time	
n	- Linear Search	2^n	- 0/1 knapsack
logn	- Binary Search	2^n	- Travelling SP
n*n	- Insertion Sort	2^n	- Sum of Subsets
n*logn	- Merge Sort	2^n	- Graph Coloring
n*n*n	- Matrix Multiplication	2^n	- Hamilton Cycle

Factorial Time - n! - Error Correcting Code

Where BQP lives in the world of complexity classes

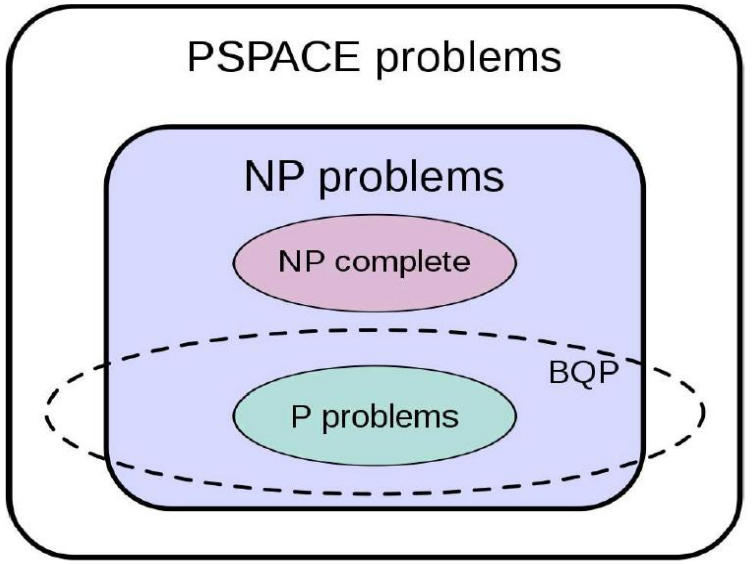


Image credits: wikipedia.org

Bounded-error Quantum Polynomial time (BQP)

*Quantum Algorithms can be based on Phase Estimation: including **Shor's algorithm**, on Amplitude Amplification including **Grover's algorithm**, and on **Quantum Walks***

Quantum Computers will break current Encryption Technologies

- When quantum computers become available, many of the actual encryption technologies (like DH, ECC & RSA protocols for digital certificates, digital signatures, etc.) can be broken. Public organizations (NIST) are standardizing post-quantum cryptography (PQC) algorithms
- According to **Schor's Quantum Algorithm**, to break the current security provided by **RSA (2048 or 4096 bits key)** it is necessary to build a quantum computer with: **~2,000 or ~4,000 logical qubits**. The corresponding number of **physical qubits depends on the error correction (QEC)** coding scheme
- For a single logical qubit using **Surface Code QEC**, ~ 1,000 physical qubits are needed, while with **Low Density Parity Check QEC**, ~ 50-100 physical qubits are needed, both targeting a 10^-3 to 10^-5 error rate

DH: Diffie & Hellman - ECC: Elliptic Curve Cryptography - RSA: Rivest, Shamir & Adleman
NIST: National Institute of Standards & Technology

IBM vs Google Quantum Computing Roadmaps

Year	IBM	Google
2016	5-qubit quantum computer (5 physical)	—
2017	IBM Q Experience (cloud access)	—
2019	53-qubit processor	Beyond Classical (Sycamore) — 54 physical
2021	127-qubit Eagle processor	—
2023	—	Scalable Quantum Error Correction ~100 physical, 1 prototype logical
2025	Heron + Quantum System Two ~1,386 physical, ~10–20 logical	Long-Lived Logical Qubit ~1,000 physical, ~1 logical
2026–2027 (est.)	—	Logical Gate Operations ~10,000 physical, ~10 logical
2028 (est.)	—	Scalable Fault-Tolerant Architecture ~100,000 physical, ~100 logical
2030 (est.)	Blue Jay FT modular system ~100,000 physical, ~100–200 logical	Fully Fault-Tolerant Quantum Computer ~1,000,000 physical, ~1,000 logical

Key Deadlines & Compliance Risks

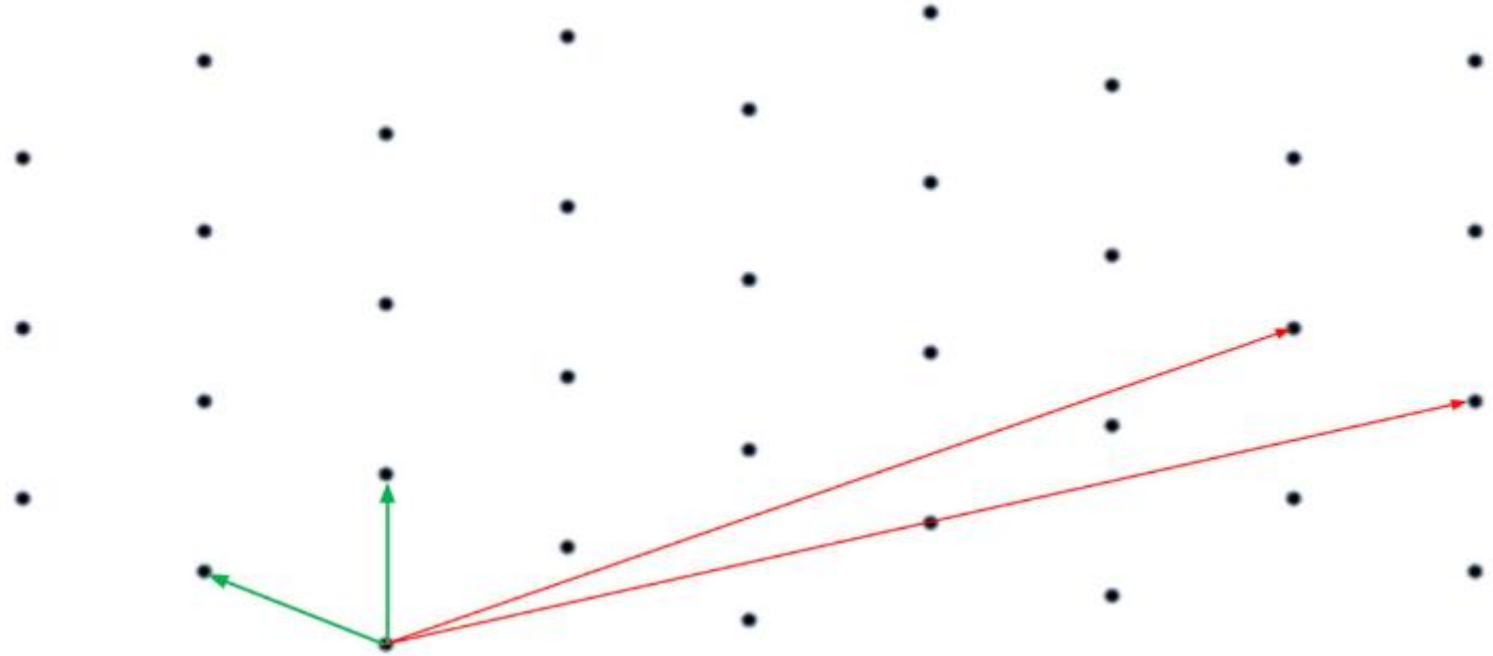
- By 2030: NIST will deprecate all **112-bit security algorithms**, requiring organisations to transition to quantum-resistant encryption
- By 2035: Quantum-vulnerable cryptography will be disallowed, meaning organisations must adopt new standards or risk compliance failures
- USA Government Mandates: The Cybersecurity and Infrastructure Security Agency (CISA) has already issued Binding Operational Directive 23-02, requiring federal vendors to begin their post-quantum transition
- EU Regulations: The European Union is advocating for algorithm agility, urging businesses to integrate multiple cryptographic methods to future-proof their security

Five NIST PQC Standard Algorithms

- **CRYSTALS-Kyber**: **FIPS 203**. This algorithm is designed **for generating encryption keys**, and for creating secure transactions on the Internet. It's part of the CRYSTALS (**Cryptographic Suite for Algebraic Lattices**) package, which is based on the hardness of certain problems in **lattice-based cryptography**
- **CRYSTALS-Dilithium**: **FIPS 204.** This is another part of the CRYSTALS package and is designed **to protect the digital signatures** we use when signing documents remotely. Digital signatures are a crucial part of ensuring the integrity and authenticity of digital documents
- **SPHINCS+**: **FIPS 205**. This is a stateless **hash-based signature scheme**, also designed for digital signatures. Hash-based signatures are particularly interesting because they're resistant to quantum attacks, making them a good choice for post-quantum cryptography
- **FALCON**: This stands for **Fast-Fourier Lattice-based Compact Signatures over NTRU**, it's designed for digital signatures, as an alternative to CRYSTALS- Dilitium and SPHINCS+
- **HQC (Hamming Quasi-Cyclic)** is a **code-based key encapsulation mechanism** that derives its security from the hardness of decoding random linear error-correcting codes— quasi-cyclic codes—with comparatively larger ciphertexts and keys, as an alternative to CDRYSTALS-Kyber

Source: NIST 2025

Lattice-based Cryptosystems



A lattice can be understood as a regular grid of points in space. The points on the lattice are chosen systematically from an object called its basis, which describes the lattice by explaining how you move between lattice points. Consider **the green basis as a 'good' basis and the red as a 'bad' one**. This is the idea used in Lattice-based cryptosystems: a **bad basis is used as a public key**, and a **good basis as the private key**. The bad basis's description of the lattice will be complicated enough to hide the message, and only the receiver can solve the problem quickly, as this requires knowledge of the good basis

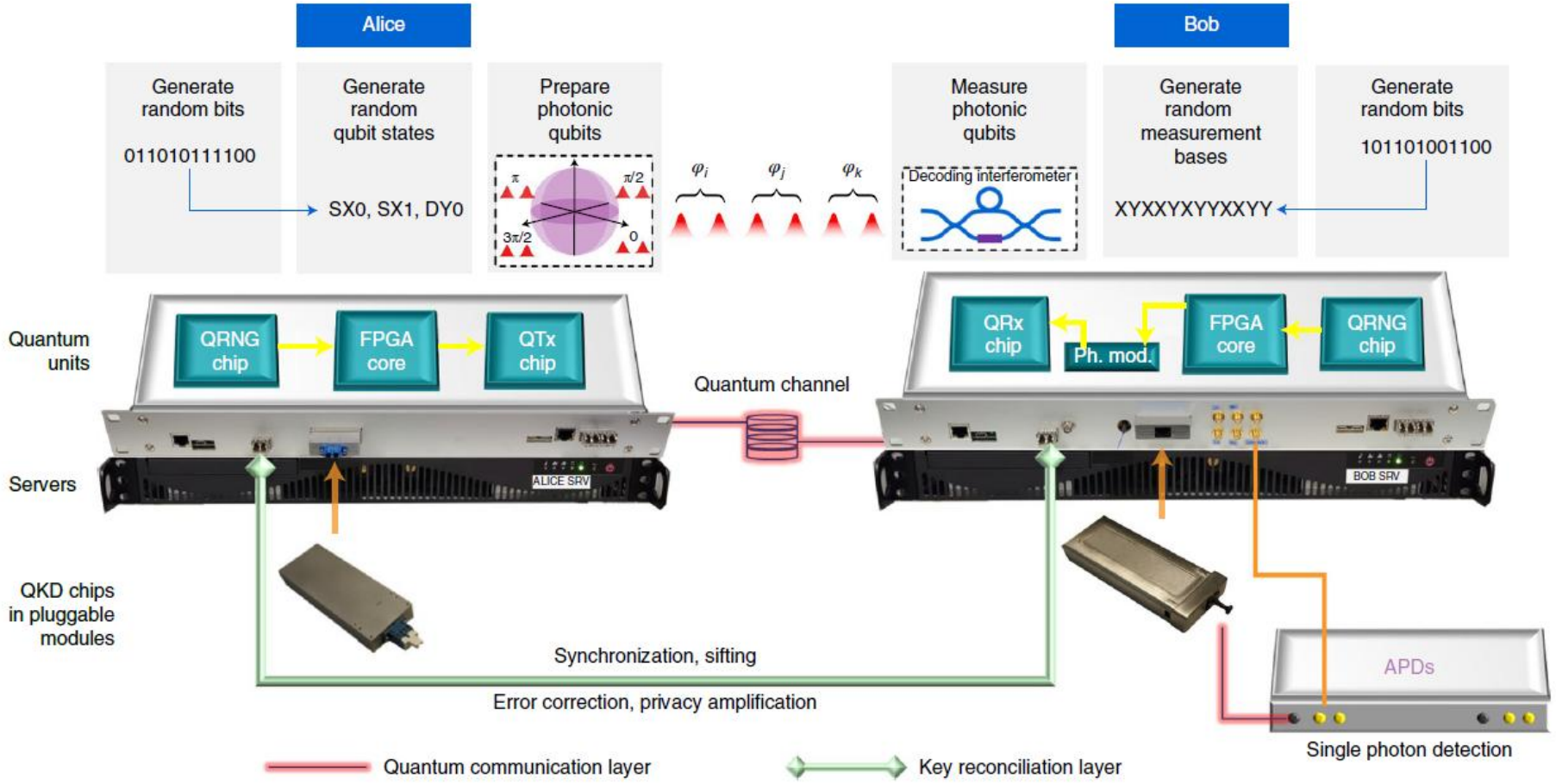
5 PQC NIST Standards

Source: NIST 2025

Algorithm	NIST Standard	Category	Mathematical Basis	Role
ML-KEM	FIPS 203	Key Encapsulation	Lattice (MLWE)	Main PQ key exchange
ML-DSA	FIPS 204	Digital Signature	Lattice (MLWE)	Default PQ signature
SLH-DSA	FIPS 205	Digital Signature	Hash-based	Conservative alternative
FALCON	(Draft / future FIPS)	Key Encapsulation	Lattice- NTRU	Conservative alternative
HQC	(Draft / future FIPS)	Key Encapsulation	Code-based	Backup / diversity

FIPS (Federal Information Processing Standard), ML (Module-Lattice), KEM (Key Encapsulation Mechanisms), DSA (Digital Signature Algorithm), MLWE (Module-Learning With Errors), SLH (Stateless Hash-based), NTRU (N-th Degree Truncated Polynomial Ring Unit), FALCON (Fast Fourier Lattice-based Compact signatures over NTRU), HQC (Hamming Quasi-Cyclic)

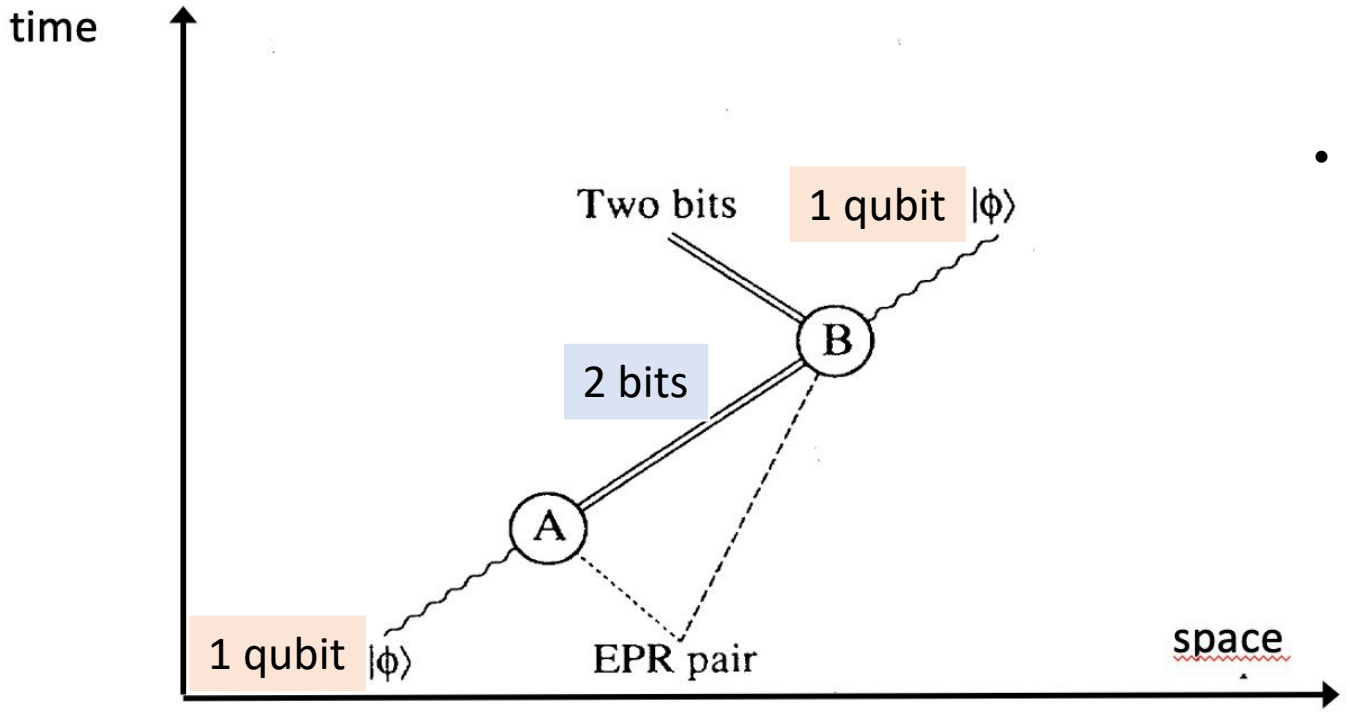
Photonic Quantum Key Distribution



100 Gbit/s line speed data encryption. 20 km fiber distance. Long-term continuous operation of the quantum secured communication system **(BB84),** using feedback control, decoy and error correction

Source: Toshiba, Nature, 2023

Quantum Entanglement & Teleportation



(Einstein, Podolski, & Rosen)

- Quantum teleportation enables the ‘‘transmission’’ of an unknown qubit without the physical transfer of the particle encoding the information
- It requires three main ingredients:
  a) source and destination share a pair of entangled qubits (a quantum communication channel is needed to distribute such a pair)
  b) local quantum circuit operations both at the source and the destination
  c) the transmission of two classical bits from source to destination via a conventional communication channel

Source: Charles H Bennett et alii, Physical Review Letters, 1993

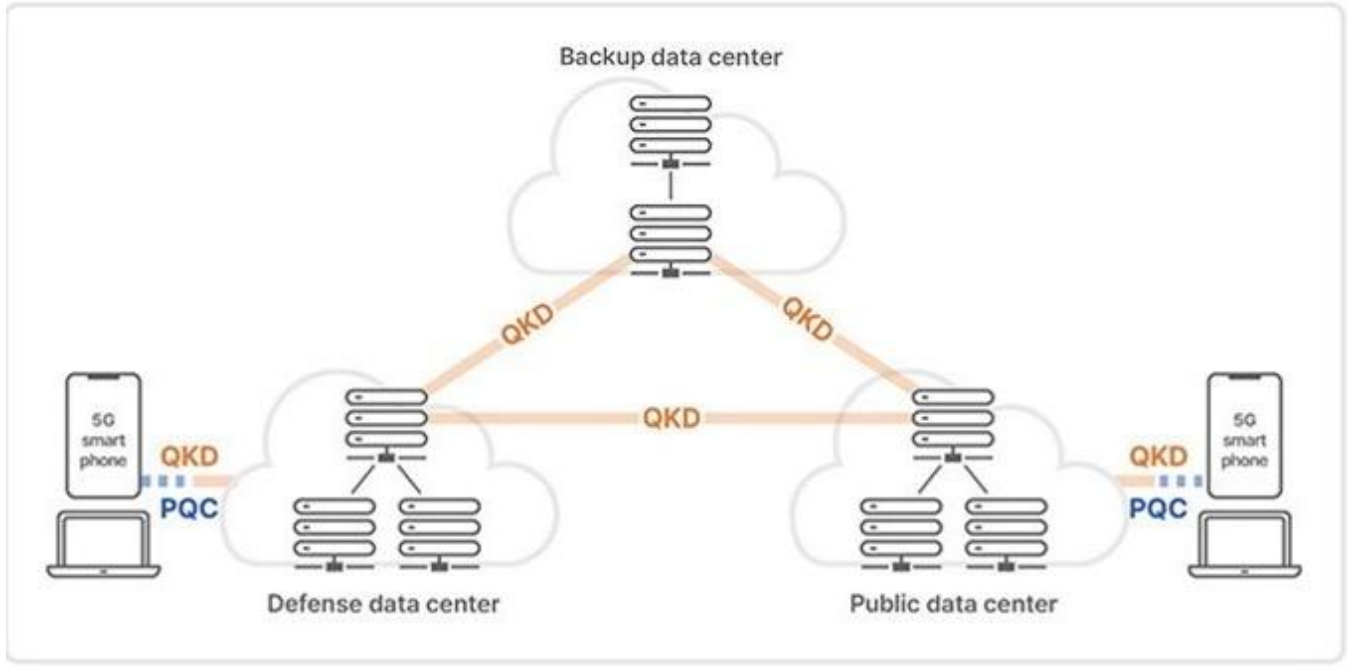
Technology Readiness Levels

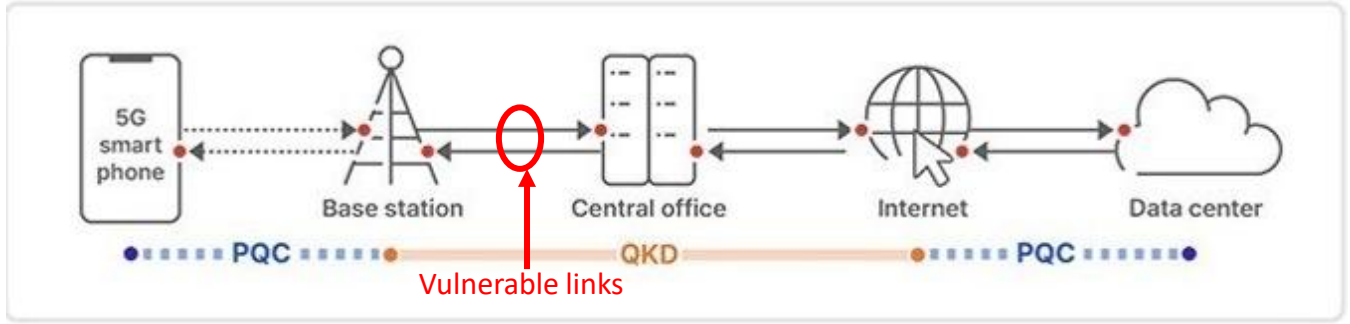
- **TRL 1 –** Basic principles observed
- **TRL 2 –** Technology concept formulated
- **TRL 3 –** Experimental proof of concept
- **TRL 4 –** Technology validated in laboratory
- **TRL 5 –** Technology validated in relevant environment
- **TRL 6 –** Technology demonstrated in relevant environment
- **TRL 7 –** System prototype demonstrated in operational environment
- **TRL 8 –** System complete and qualified
- **TRL 9 –** Actual system proven in operational environment

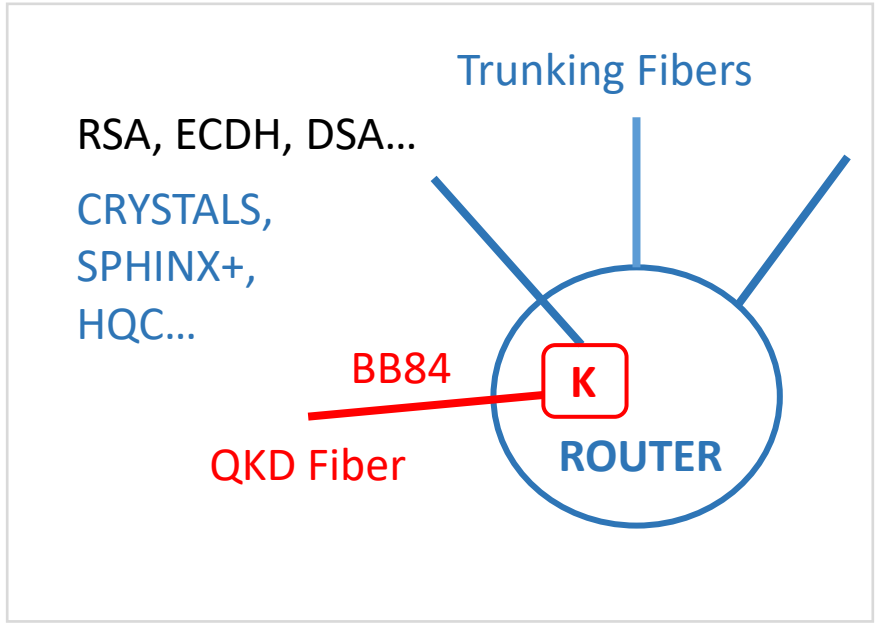
QKD & Quantum Communications Technology Readiness Levels 2026–2045

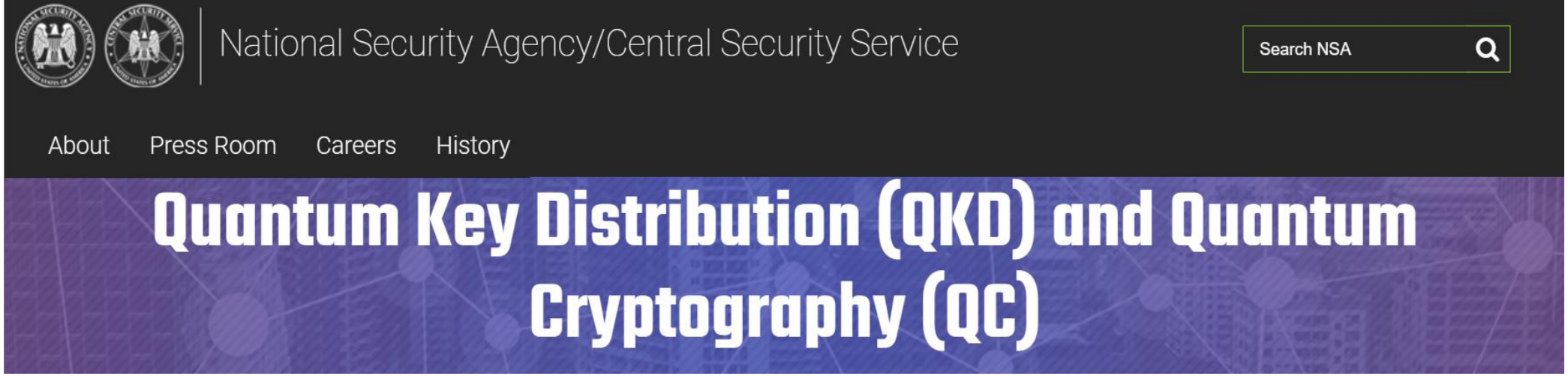
Technology	Current TRL (2026)	TRL 2035	TRL 2045	Typical Key Rate	Typical Distance	Commercial / Industrial Scenario
BB84 + Decoy	8–9	9	9	1–10 Mbit/s	50–100 km (metro fiber)	Already commercialized; integration in metropolitan networks and datacenters; first industrial generation of QKD
BBM92 (entangled)	7–8	8–9	9	0.1–1 Mbit/s	50–100 km (metro fiber)	Operational trials; use in government and finance networks; limited commercial deployment; second generation compared to BB84
MDI-QKD (entangled)	6–7	8–9	9	0.01–1 Mbit/s	50–150 km (fiber)	High detector security; metropolitan adoption post-2030; pre-commercial products
Quantum Repeater	3–4	6–7	8	N/A	>1000 km	Enabler for long-distance networks; still research + field trials; high cost; required for national and continental-scale quantum networks
Quantum Network / Internet	2–3	5–6	7–8	N/A	Multi-node testbeds	Experimental testbeds; selective government/scientific networks; depends on repeaters; not general-purpose; long-term development

SK Telecom's QKD & PQC Networking









5 Issues on Quantum Key Distribution - Some Highlights

1. **QKD is only a partial solution**. QKD generates keying material for an encryption algorithm that provides confidentiality. QKD does not provide a means to authenticate the QKD transmission source**. Source authentication requires the use of asymmetric cryptography or preplaced keys**
2. **QKD requires special purpose equipment. It cannot be implemented in software or as a service** on a network and cannot be easily integrated into existing network equipment. Since QKD is hardware-based it also **lacks flexibility for upgrades or security patches**
3. **QKD increases infrastructure costs and insider threat risks**
4. **Securing and validating QKD is a significant challenge.** The **actual security provided by a QKD system is not the theoretical unconditional security from the laws of physics**, but rather **the** more **limited security that can be achieved by hardware and engineering designs**. The **tolerance for error** in cryptographic security is many orders of magnitude smaller than in most physical engineering scenarios. The specific **hardware used to perform QKD can introduce vulnerabilities**

5. **QKD increases the risk of denial of service.** The sensitivity to an eavesdropper as the theoretical basis for QKD security claims also shows that denial of service is a significant risk for QKD