# Cryptography, Quantum-safe Cryptography & Quantum Cryptography

Maurizio Dècina

*CYBERDAYS, Prato, 21 marzo 2024*

*Regione Toscana*

# Topics

- *Today's Cryptosystems* on the Internet (asymmetric crypto: RSA, DH, ECC; symmetric crypto: AES, SHA)
- *Post Quantum Cryptography*, 4 NIST Cryptosystem Candidates: Lattice, Code-based, Multivariate, and Isogeny-based,)
- *Quantum Key Distribution*, quantum communications channels to transmit secure symmetric keys
- *Quantum Teleportation*, transmission of information (qubits): no energy, matter or people tele transport
- *Quantum Cryptography*, Future Cryptosystems based on Quantum Algorithms

*Laboratory research developments*

# Public Key Cryptography

- Message: P; Message Hash: SHA(P) Secure Hash Algorithm 256 bit
- **PKI, Public Key Infrastructure & Certification Authorities**
- A generates key pair: $K_A$ & $K_A^{-1}$
- A requests a certificate from *Certification Autority* (CA) for her public Key
- **A's Digital Certificate** signed by CA: $A, K_A, \{SHA(A, K_A)\} K_{CA}^{-1}$
- **A's Digital Signature of message P**: $P, \{SHA(P)\} K_A^{-1}$
- A & B exchange their Certificates to know their Public Keys
- A can send an encrypted message P to B

  $C = \{P\}K_B$; B decodes $P = \{C\}K_B^{-1}$
- A sends a signed message P to B (or everybody who knows her public key)

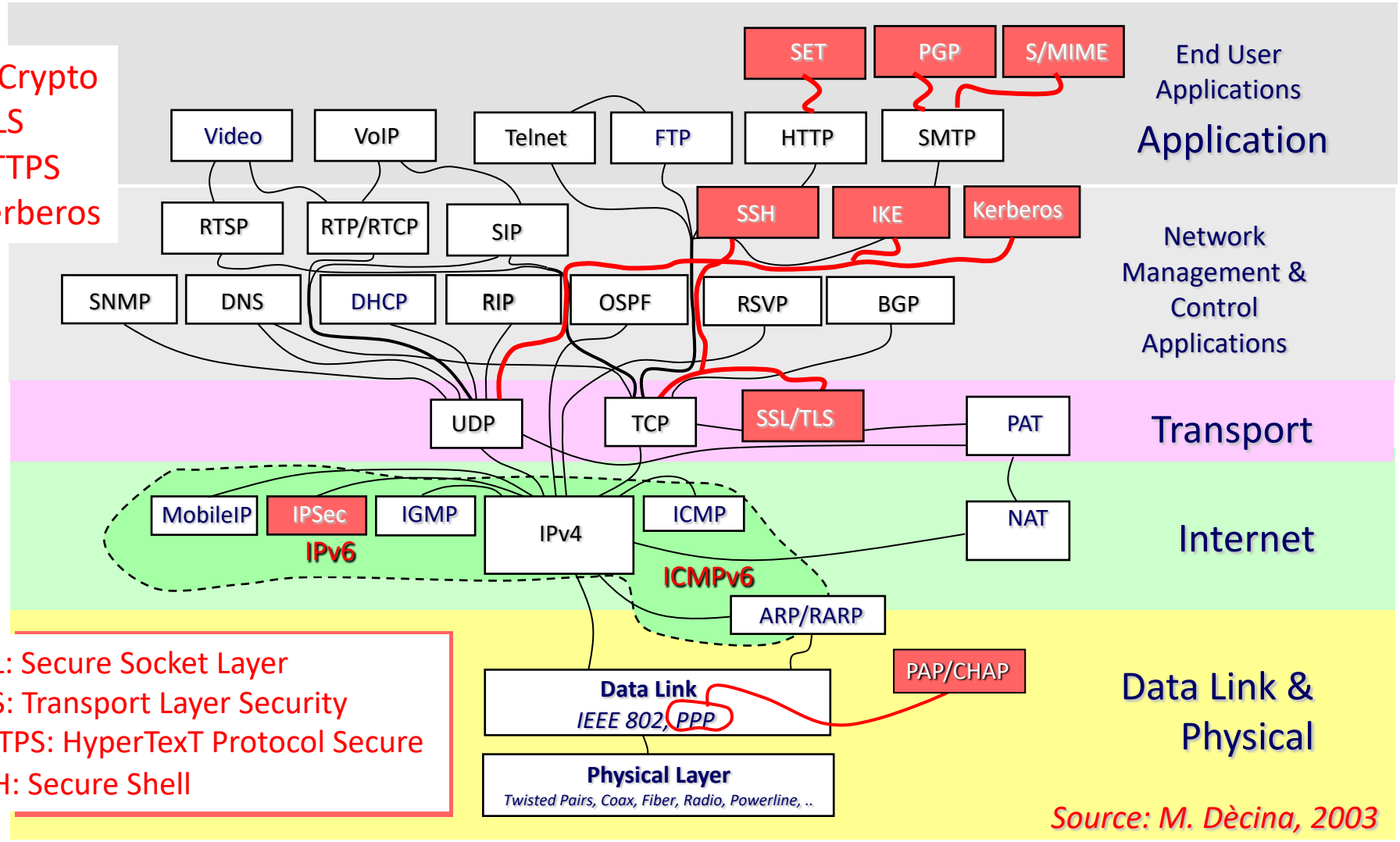
  $C = P, \{SHA(P)\}K_A^{-1}$; B decodes: $P, \{\{SHA(P)\} K_A^{-1}\}K_A = P, SHA(P)$

Users acquainted with Algorithm, e.g. RSA

everybody knows The CA's public key

# Internet Protocols & Security

Public Key Crypto
SSL/TLS
HTTP/HTTPS
SSH/IKE/Kerberos



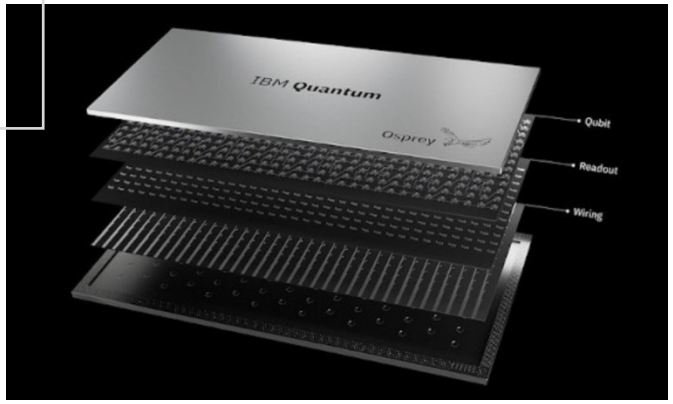

SSL: Secure Socket Layer
TLS: Transport Layer Security
HTTPS: HyperTexT Protocol Secure
SSH: Secure Shell

*Source: M. Dècina, 2003*

# Quantum Computing

*IBM 127 Qubit Eagle Computer, 2021*

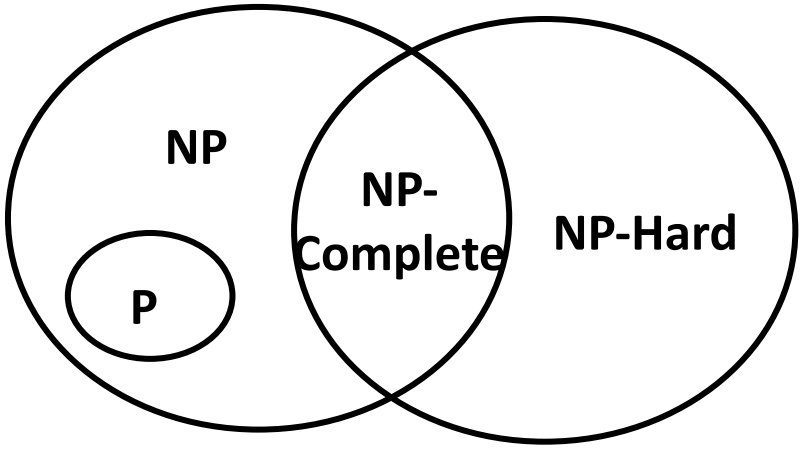
Quantum Computing




*IBM 433 Qubit Ospray Computer, 2022*

| Quantum Computing | Classic Computing |
|---|---|
| *Calculates with qubits, which can represent 0 and 1 at the same time* | *Calculates with transistors, which can represent either 0 or 1* |
| *Power increases exponentially in proportion to the number of qubits* | *Power increases in a 1:1 relationship with the number of transistors* |
| *Quantum computers have high error rates and need to be kept ultracold* | *Classical computers have low error rates and can operate at room temp* |
| *Well suited for tasks like optimization problems, data analysis, and simulations* | *Most everyday processing is best handled by classical computers* |

# Computational Complexity Theory




**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

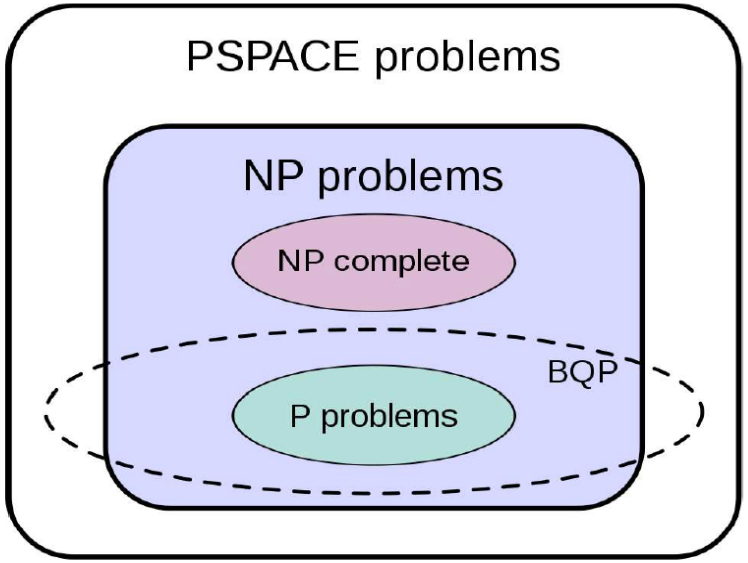



Image credits: wikipedia.org

**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 Cyber Threats to Encryption

There are two types of encryption systems currently in use: symmetric and asymmetric encryption (which is also known as public key cryptography).

## Quantum Computing poses a real threat to systems leveraging asymmetric encryption

"**Shor's algorithm**", which runs on a quantum computer, efficiently solves the integer factorization problem that offers the foundations of the public-key cryptography. This implies that, if a quantum computer is developed, today's public-key cryptography algorithms (e.g., RSA, ECDH: Elliptic Curve Diffie Hellman Key Exchange) and protocols would need to be replaced by algorithms and protocols that can offer cryptanalytic resistance against

*Examples of public-key cryptography algorithms:*
RSA, Diffie-Hellman and Elliptic Curve Cryptography

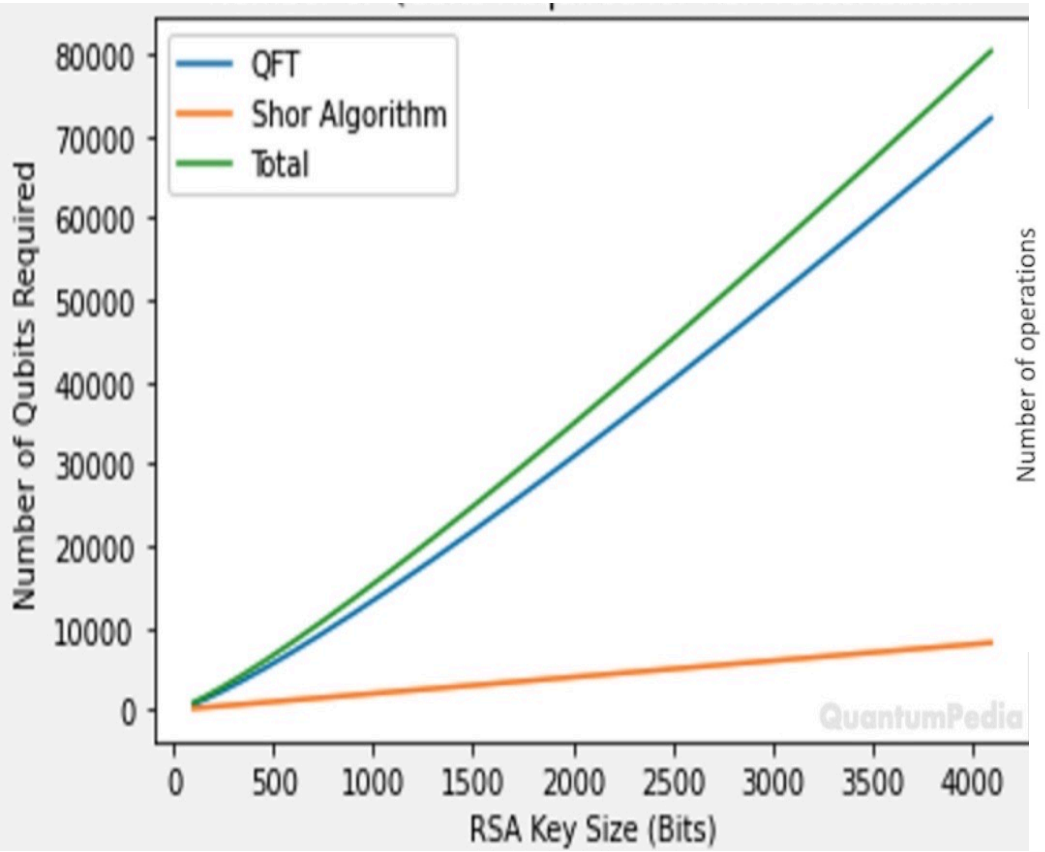
## Symmetric cryptography is also affected by Quantum Computing, but significantly less

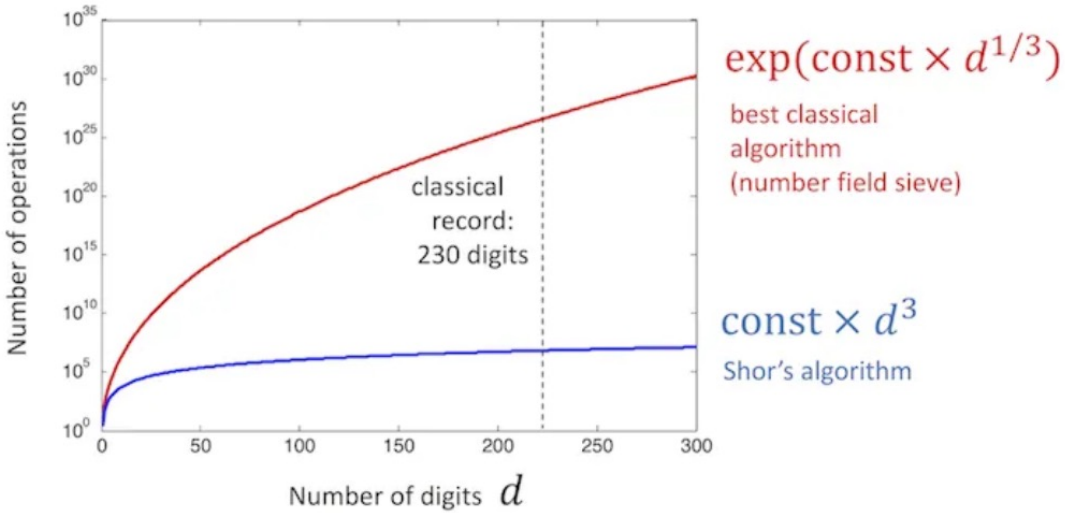
No quantum computer is known to break the security properties of these classes of algorithms, however performing a "Grover's Search" using a quantum computer halves their security level.
This means that breaking AES-128 takes 264 quantum operations, while current attacks take 2128 steps.
While this is a change, it can be managed quite easily by doubling the key sizes, e.g., by deploying AES-256

*Examples of symmetric cryptography algorithms:*
AES and HMAC-SHA2

# Qubits required for RSA Factorization

QFT: Quantum Fourier Transform



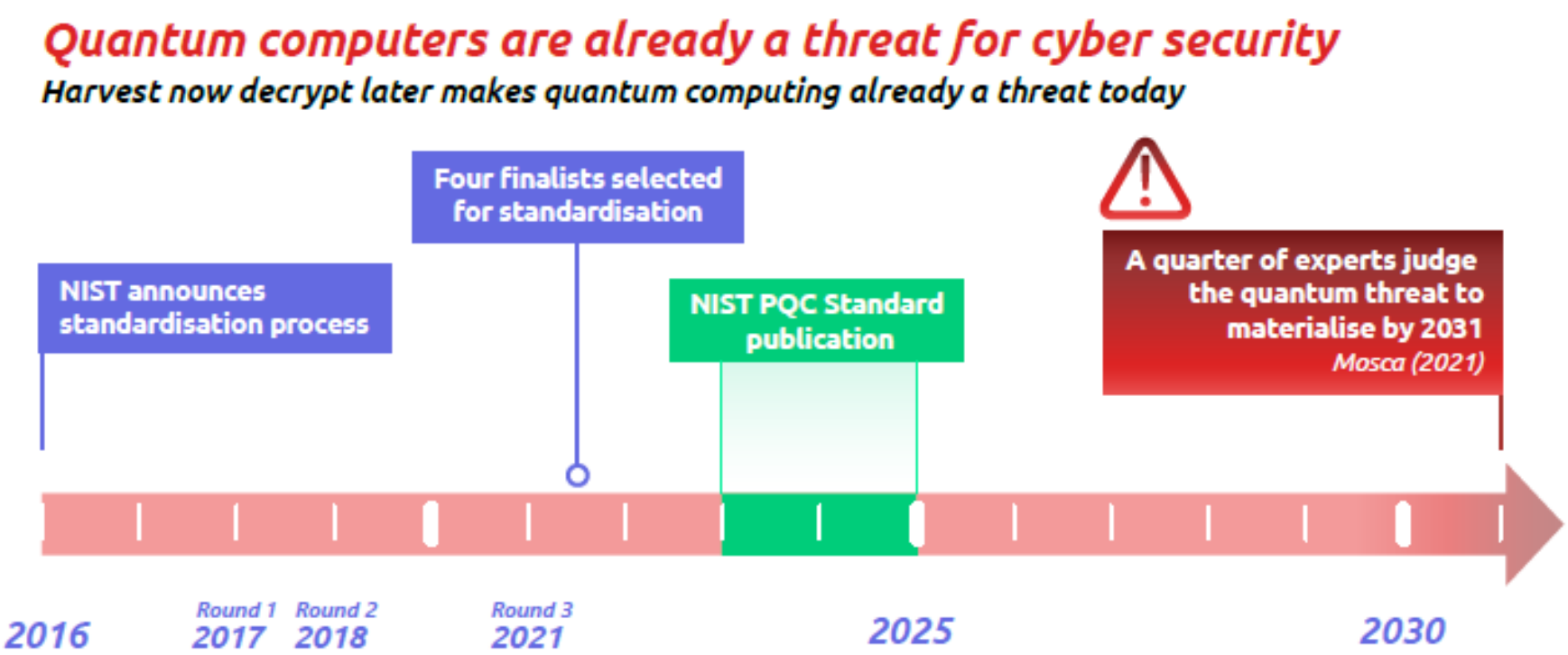




*Source: MR. Asif, 2021*

*Source: QuantumPedia, 2021,*

# Quantum Threats to Financial Data

NIST - National Institute of Standards and Technology




While current quantum computers do not pose any threat, **data stored or transmitted today are exposed to "harvest now, decrypt later" attacks by a future quantum computer**.

The **long-term sensitivity of financial data** means that the potential future existence of a quantum computer effectively renders today's systems insecure.

*https://www.netmeister.org/blog/pqc-2024-01.html*

*https://www.ibm.com/quantum/blog/ibm-quantum-roadmap*

# Four NIST PQC Standard Algorithms

- **CRYSTALS-Kyber**: 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**: 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+**: 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**. Like the others, it's also designed for digital signatures. A draft standard for FALCON will be released in about a year, which will provide more details about its implementation

*Source: NIST 2023*

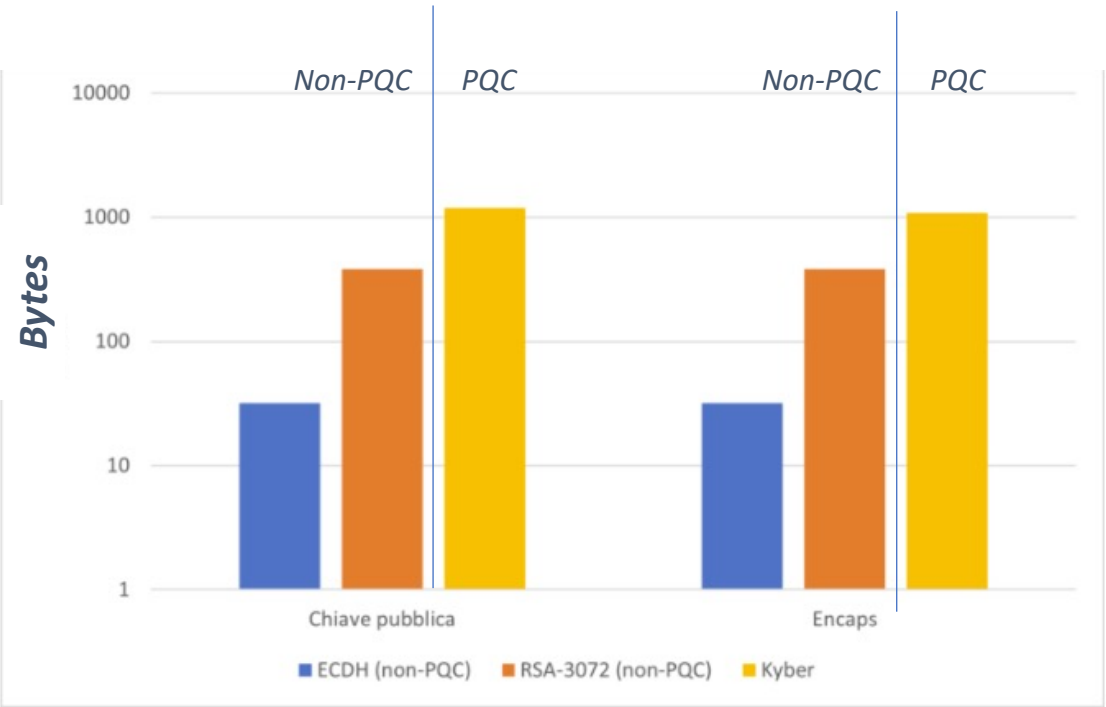
# Key Encapsulation Mechanism for PQC

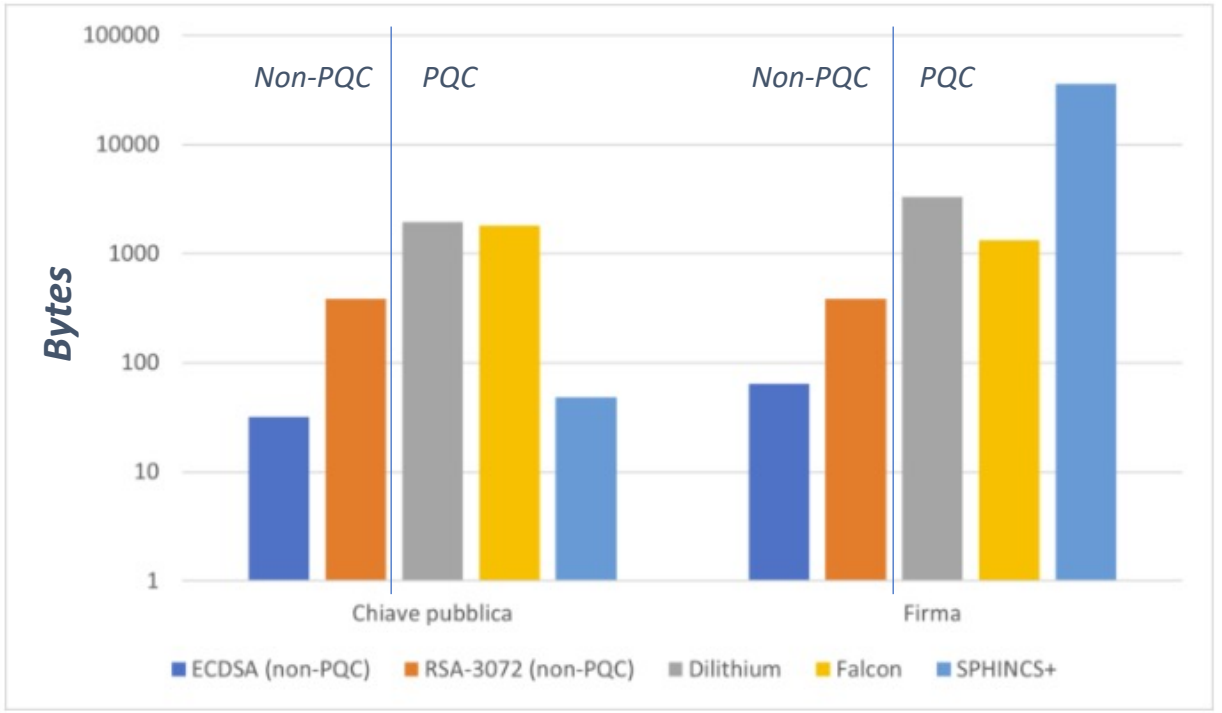
| KEM Algorithm | Generate Key | Encapsulation | Decapsulations | Public Key Size | Encapsulation Size |
|---|---|---|---|---|---|
| NTRU (lattice-based PQC) | 0.048ms | 0.0073ms | 0.012ms | 699B | 699B |
| Kyber (lattice-based PQC) | 0.0070ms | 0.011ms | 0.0084ms | 800B | 768B |
| SABER (lattice-based PQC) | 0.012ms | 0.016ms | 0.016ms | 672B | 736B |
| Classic McEliece (code-based PQC) | 14ms | 0.011ms | 0.036ms | 261120B | 128B |
| SIKE (isogeny-based PQC) CRACKED | 3.0ms | 4.4ms | 3.3ms | 197B | 236B |
| ECDH (X25519) (non-PQC) | 0.038ms | 0.044ms | 0.044ms | 32B | 32B |
| ECDH (P-256) (non-PQC) | 0.074ms | 0.18ms | 0.18ms | 32B | 32B |
| RSA-3072 (non-PQC) | 400ms | 0.027ms | 2.6ms | 384B | 384B |

*ECDH: Elliptic Curve Diffie Hellman Key Exchange*

*Source: Ericsson Review, 2021*

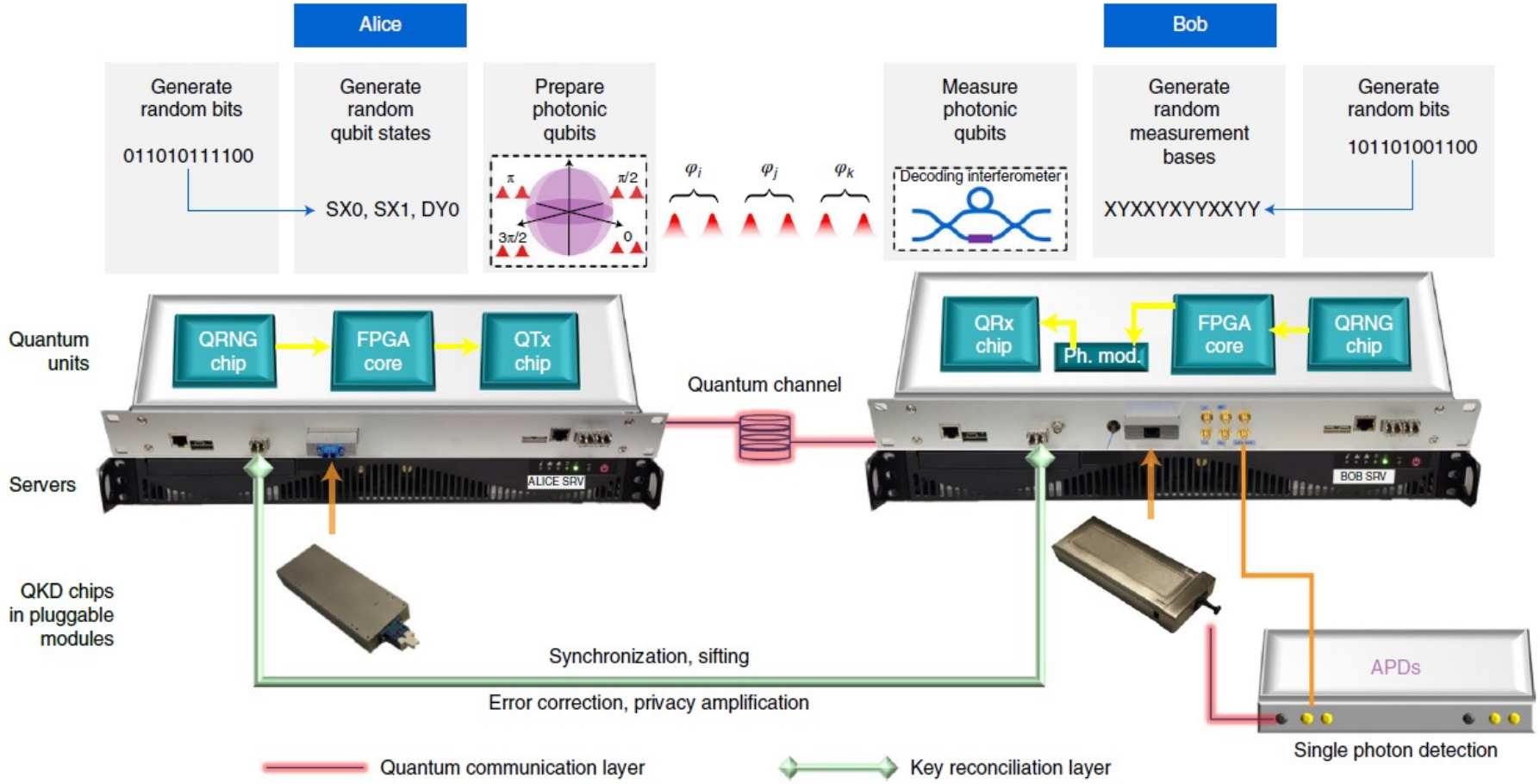
# Increase of Key & Ciphertext/Signature Sizes




Source: https://www.telsy.com/la-crittografia-post-quantum-pqc-una-soluzione-classica-alla-minaccia-quantistica/

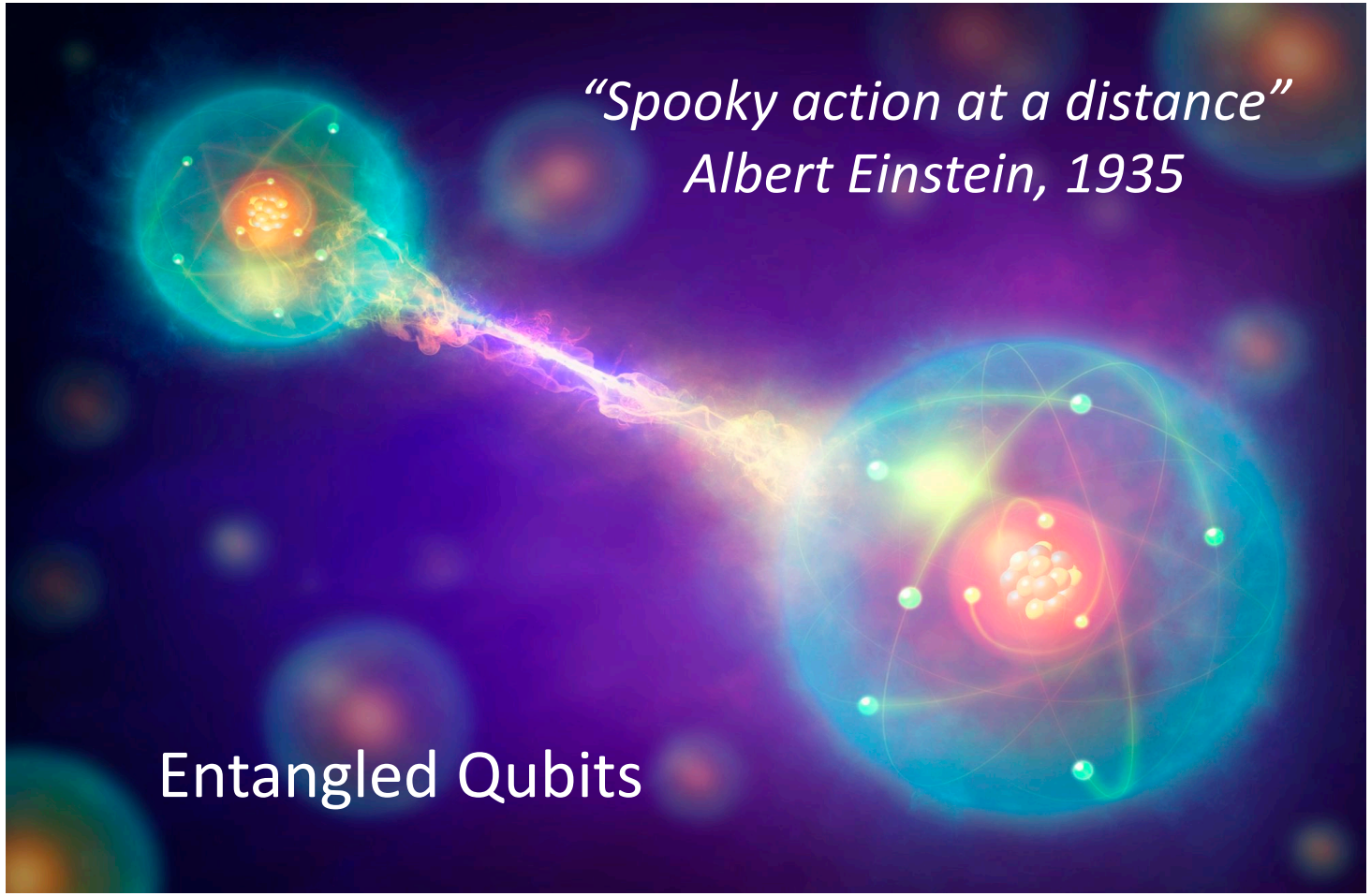
# Photonic Quantum Key Distribution




100 Gbit/s line speed data encryption. 10 km fiber distance. Long-term continuous operation of the quantum secured communication system (BB84), using feedback control, decoy and error correction

*Source: Toshiba, Nature, 2021*

# Quantum Entanglement & Teleportation



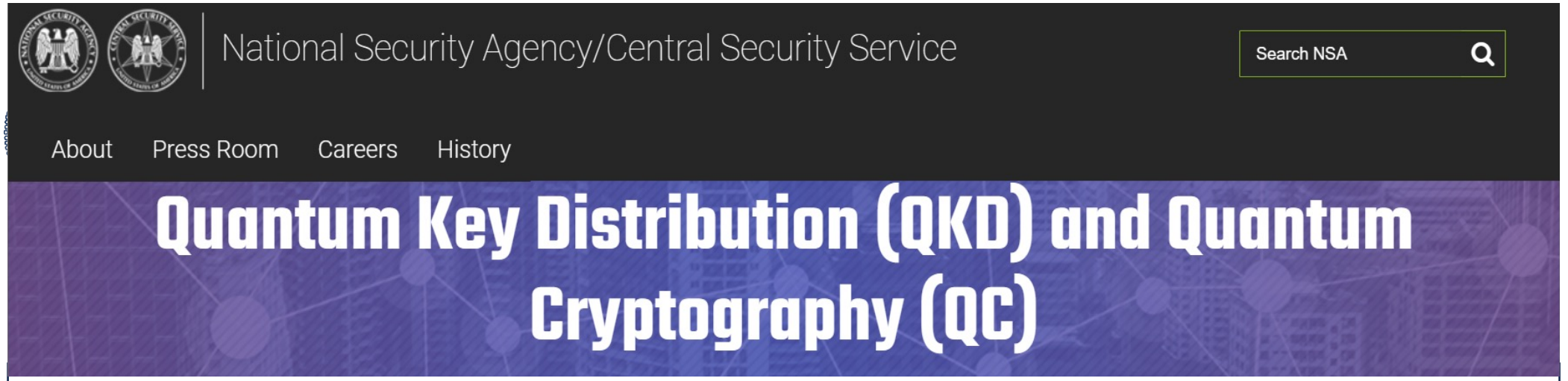

- Quantum teleportation enables the ‘‘transmission’’ of an unknown qubit without the physical transfer of the particle encoding the information
- It requires three main ingredients:

a) both source and destination share the same 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

***Quantum Teleportation refers to transmission of information, not energy, matter or people!***



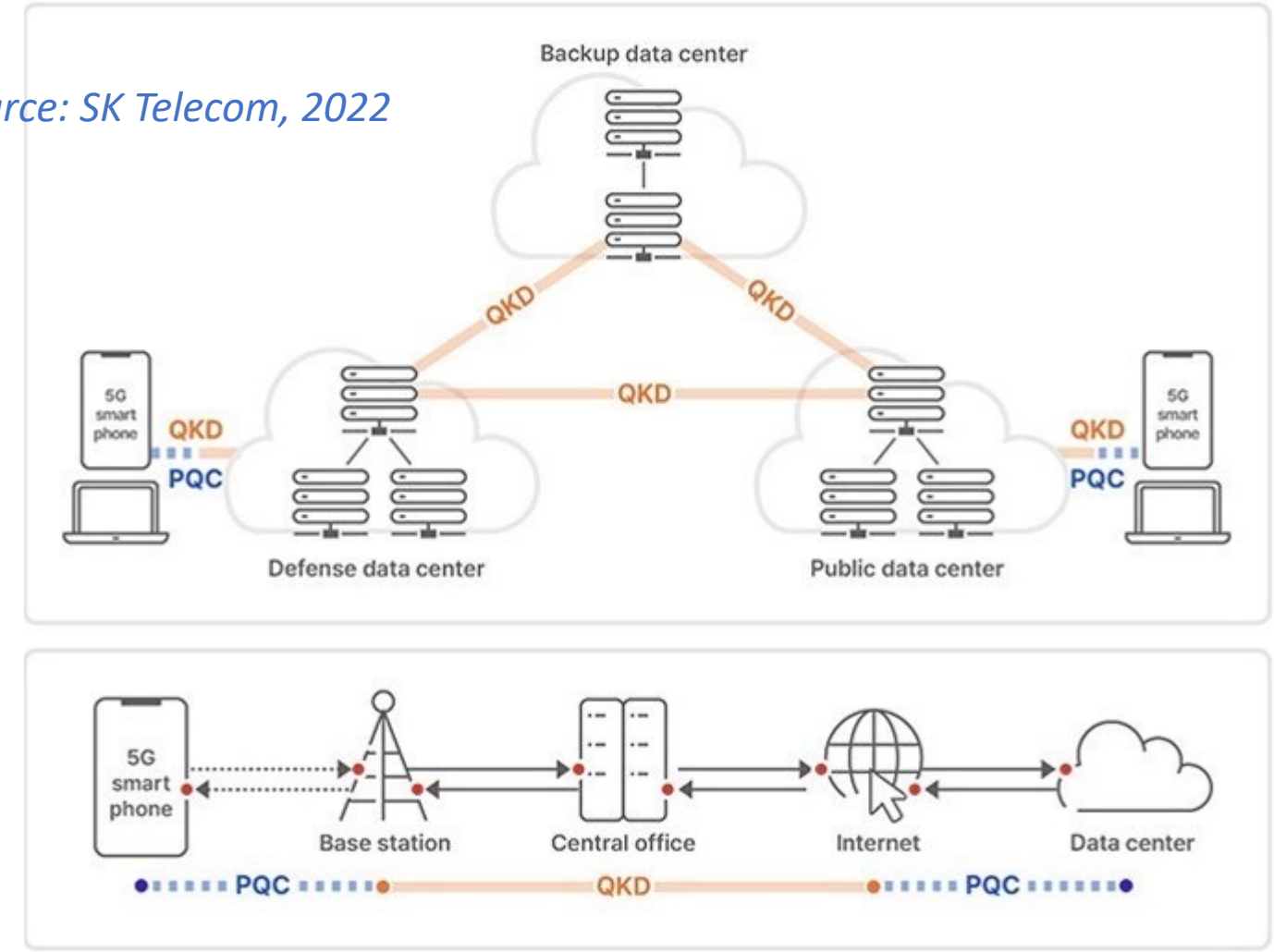

## 5 Issues on Quantum Key Distribution - Some Highlights

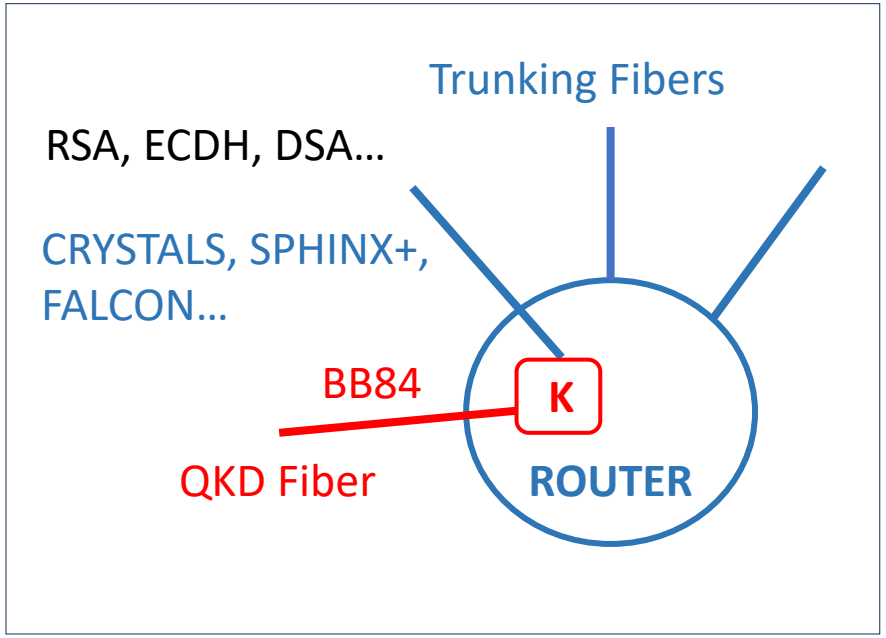
1. **QKD is only a partial solution**. QKD generates keying material for an encryption algorithm that provides confidentiality. QKD does not provide a means to authenticate the QKD transmission source**. Source authentication requires the use of** asymmetric cryptography or **preplaced keys**
2. **QKD 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

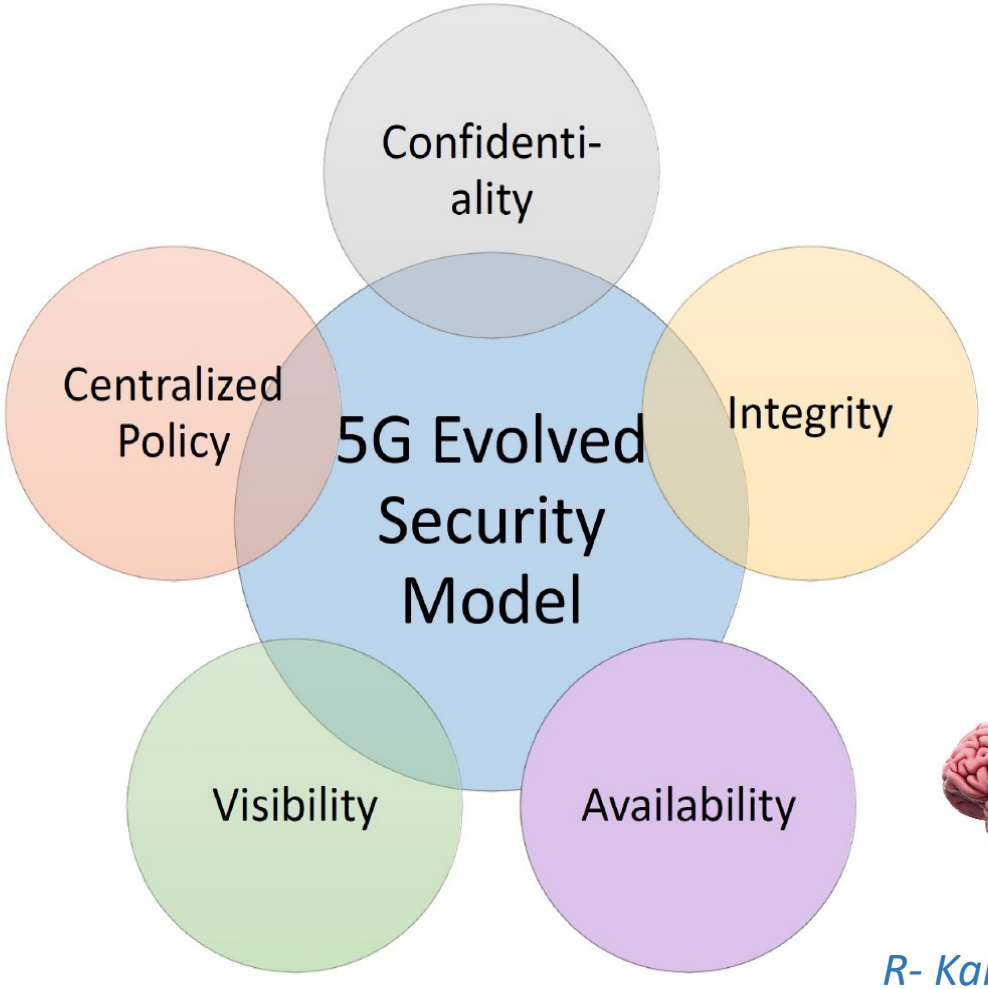
# SK Telecom's QKD & PQC Networking

*Source: SK Telecom, 2022*

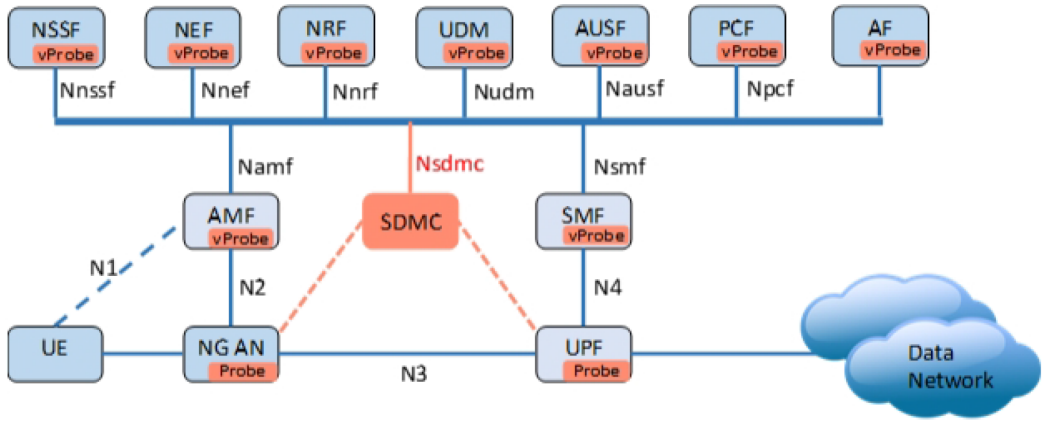


# 5G/6G Evolved Security Model




**Visibility**




Software Defined (Security) Monitoring, **SDM**

Centralized Security Policy =
**AI Security as a Service**

*R- Kahn et alii, IEEE Communications Surveys and Tutorials, 2019*