# Communication in a quantum world

Eleni Diamanti
LIP6, CNRS, Sorbonne University
Paris Centre for Quantum Computing

GEANT Quantum Technologies Infoshare
20 January 2021

# The quantum revolutions





Planck's quantum theory — transistor — hard disk — laser

beginning of 20th century — 1947 — 1954 — 1960

- Why doesn't the electron collapse onto the nucleus of an atom?
- Why are there thermodynamic anomalies in materials at low temperature?
- Why is light emitted at discrete colors?

Albert Einstein (1879-1955)

Werner Heisenberg (1901-1976)

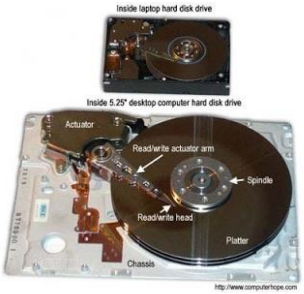
Erwin Schrödinger (1887-1961)

**The first quantum revolution**

Observation and macroscopic manifestation of quantum principles

# The quantum revolutions




Planck's quantum theory — beginning of 20th century

transistor — 1947

hard disk — 1954

laser — 1960

end 20th / beginning 21st

Control of single quantum particles
First quantum algorithms

Richard Feynman
(1918–1988)

Serge Haroche

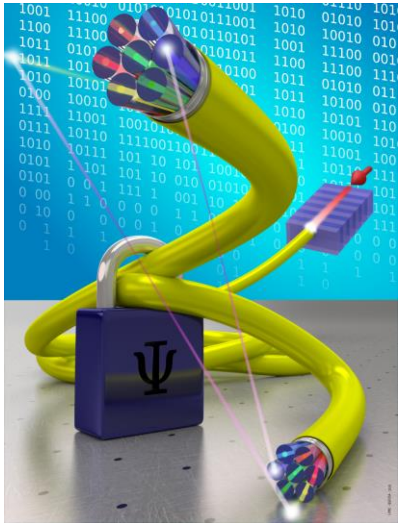
And also Alain Aspect, Charles Bennett, Gilles Brassard, Artur Ekert, Peter Shor…

**The second quantum revolution**

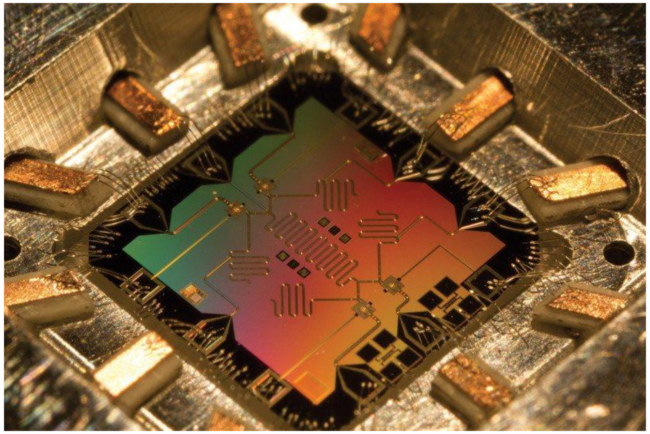
Active manipulation of single quantum particles and interaction between multiple particles for applications

# Quantum technologies

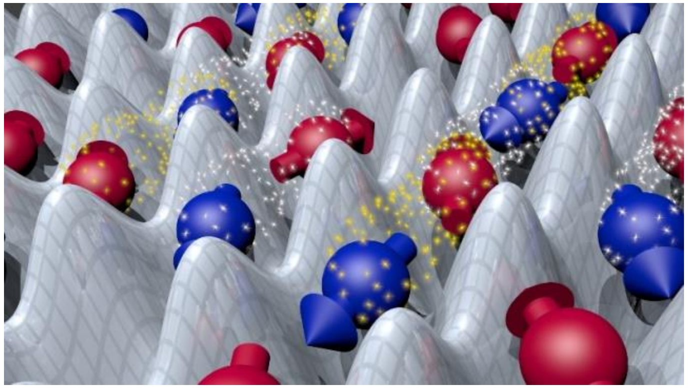
Unconditionally secure communication



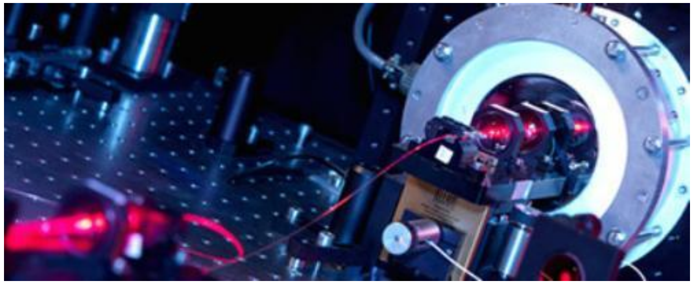
A leap in computing power



Increased understanding of complex physical systems



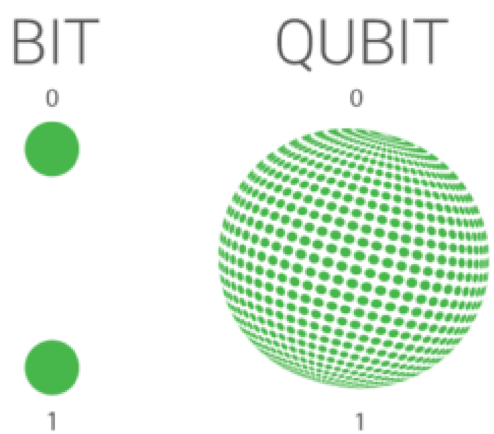
Measurement precision beyond the classical limit



# Encoding quantum information



Information can be encoded on properties of **single quantum particles** which can be found in **superposition** states

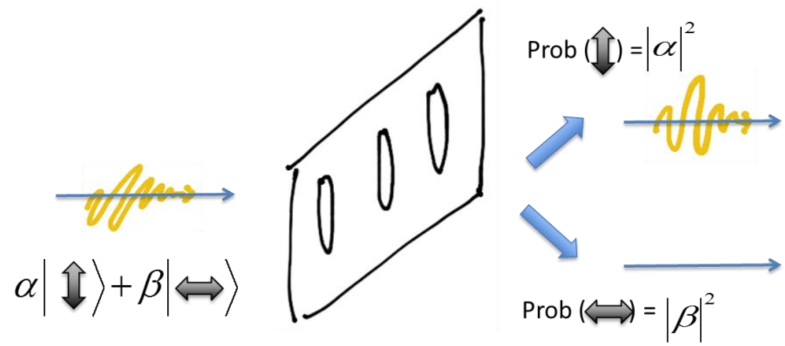


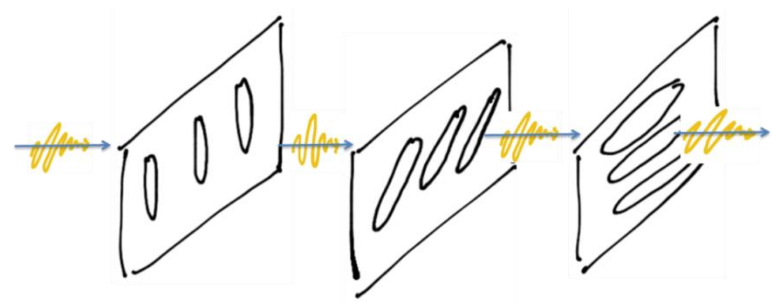

$$\alpha|0\rangle + \beta|1\rangle$$

with α, β complex numbers and

$$|\alpha|^2 + |\beta|^2 = 1$$

Photons are ideal carriers of quantum information
→ robust to ambient noise
→ can be transported over long distances



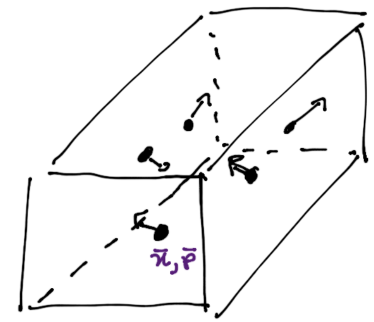



Following the probabilities according to quantum mechanics, there is a non-zero probability of photon coming out!

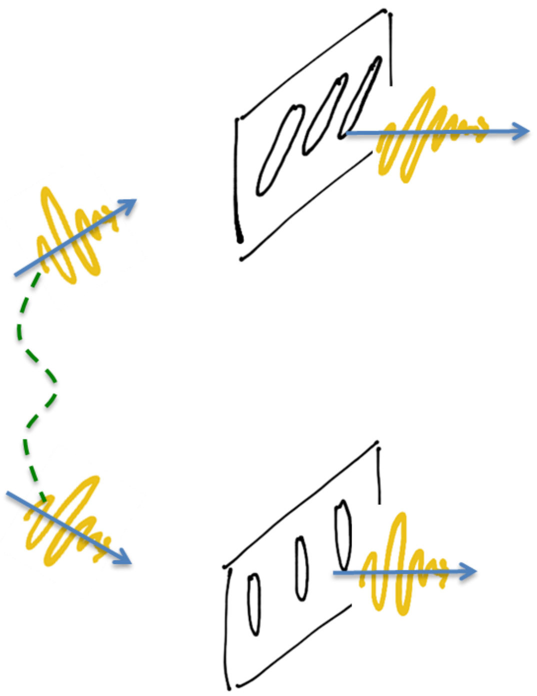
# Encoding quantum information

Information can also be encoded on properties of **entangled particles** which exhibit **nonlocal correlations**

In classical physics, randomness comes from ignorance



**Einstein-Podolsky-Rosen** paradox: same for quantum theory?



**Bell test:** there is no **local hidden variable** model that explains quantum correlations

In quantum physics, **randomness does not come from ignorance!**

# Quantum communication networks



**Photonic resources**
Encoding on properties of quantum states of light
Propagation in optical fibre or free-space channels
Computation in network nodes (processors, memories)

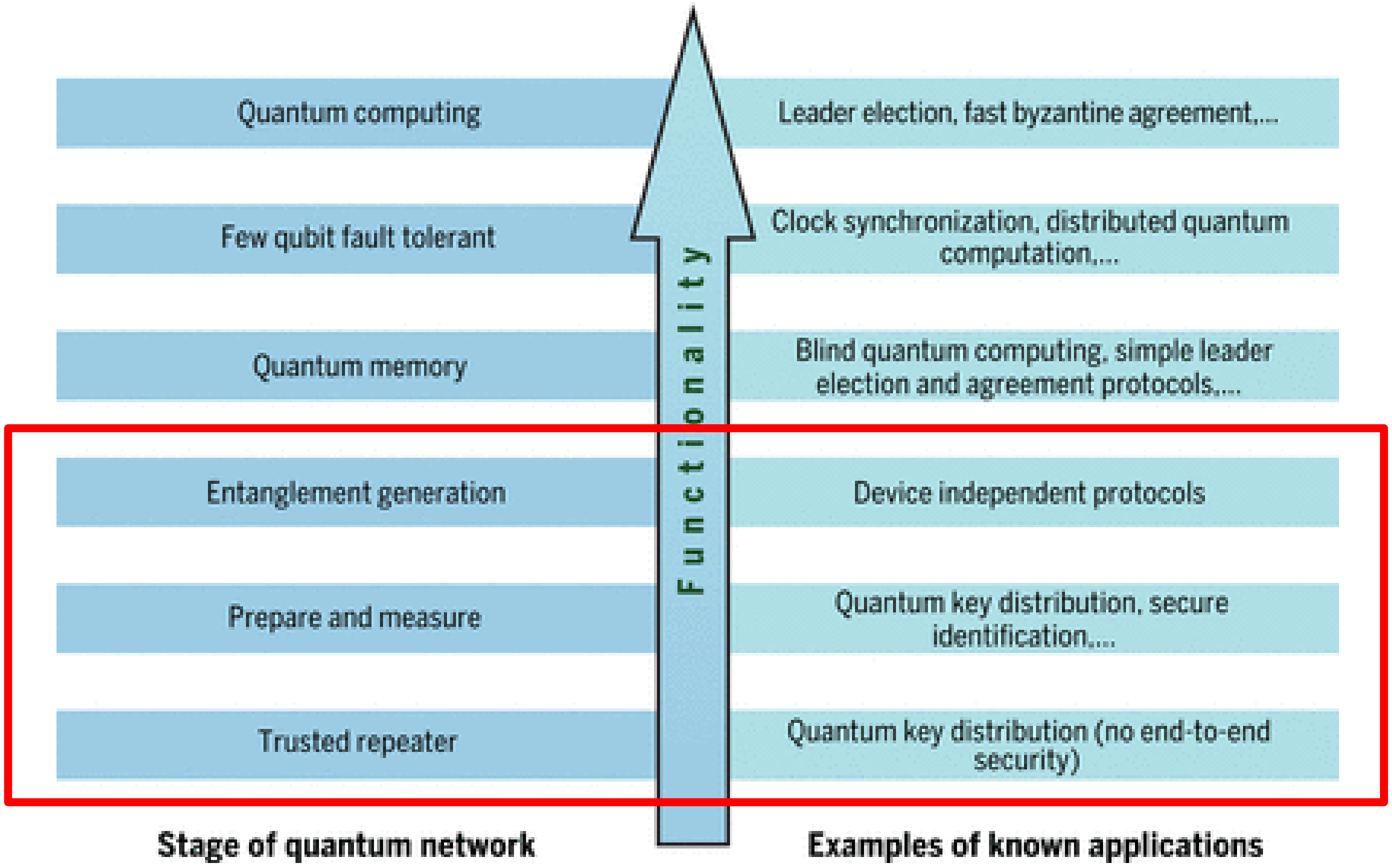
**Security**
Untrusted network users, devices, nodes

**Efficiency**
Optimal use of communication resources

**Applications**
Realistic conditions for communication and distributed computing protocols
Implementations with provable quantum advantage

# Applications of quantum communication networks





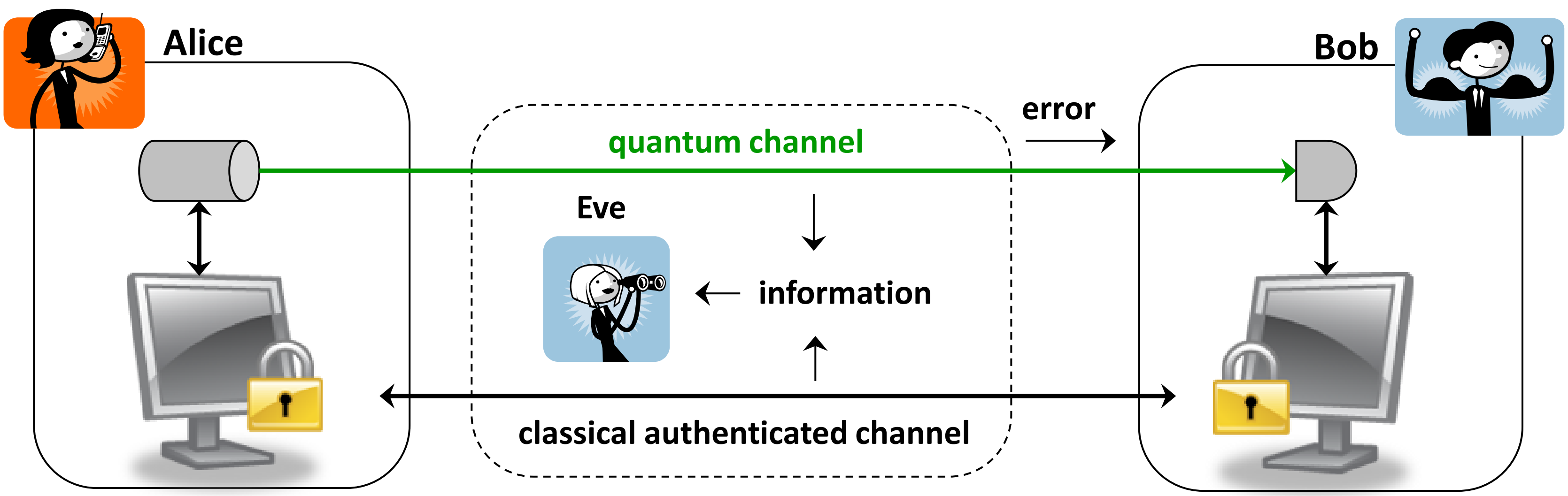

S. Wehner *et al.*, Science 2018

# Securing network links: quantum key distribution



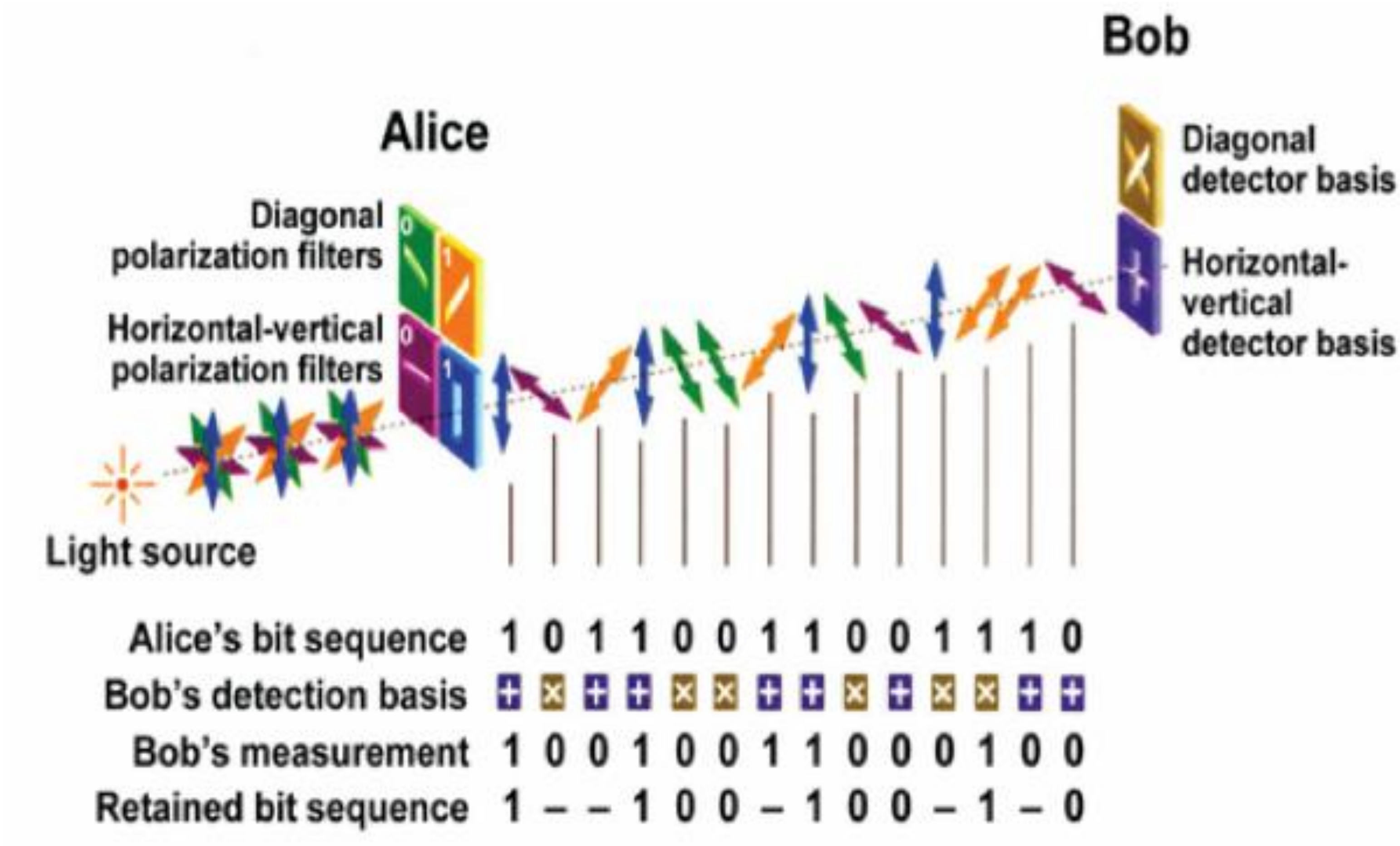
Modern cryptography relies on assumptions on the computational power of an eavesdropper → symmetric, asymmetric, post-quantum cryptography

Quantum key distribution provides a future-proof, information theoretically secure solution to the key distribution problem for secure message exchange between two trusted parties




Thanks to the fundamental principles of quantum physics (no cloning theorem, superposition, entanglement & nonlocality), it is possible to detect eavesdropping on the communication link

# The BB84 protocol




Eve cannot copy the states sent by Alice → no-cloning theorem
She cannot measure the state in both bases → errors!
If Alice and Bob share entangled photons less assumptions on devices

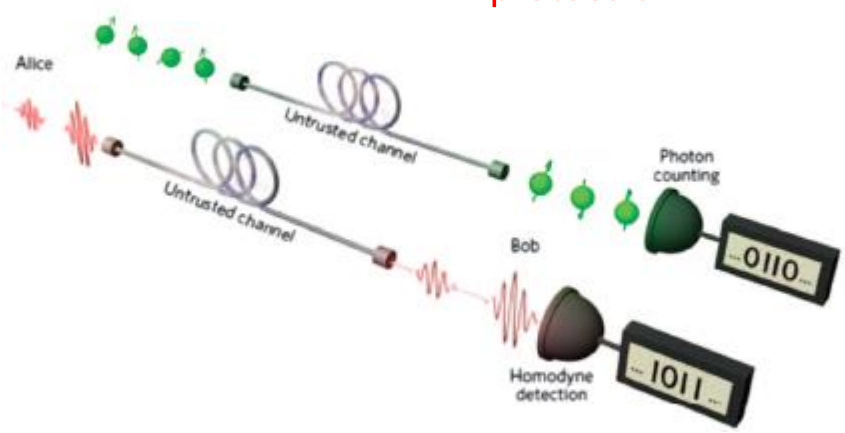
# Discrete and continuous variable QKD



| | Discrete variables | Continuous variables |
|---|---|---|
| Key encoding | Photon polarization, phase, time arrival | Electromagnetic field quadratures |
| Detection | Single-photon | Coherent (homodyne/heterodyne) |
| Post processing | Key readily available | Complex error correction |
| Security | General attacks, finite-size, side channels | General attacks, finite-size, side channels |

BB84, Decoy state, Coherent One Way, Differential Phase Shift, (Measurement) device independent protocols

CV-QKD (one or two-way, Gaussian or discrete modulation, coherent or squeezed states, post selection), (Measurement) device independent protocols

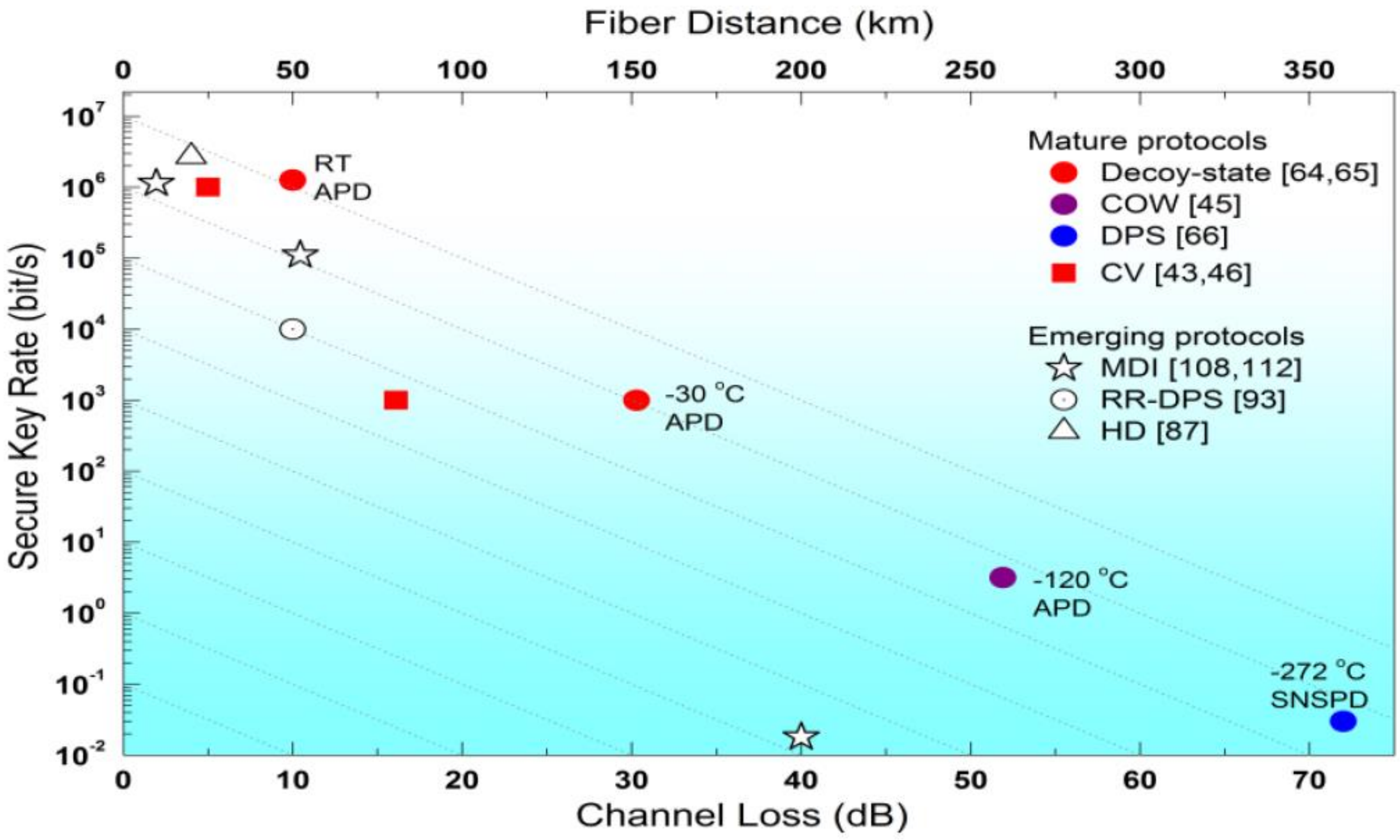



V. Scarani et al, Rev. Mod. Phys. 2009
ED and A. Leverrier, Entropy 2015

# QKD in practice



State-of-the-art of point-to-point, prepare-and-measure fiber-optic QKD in 2016



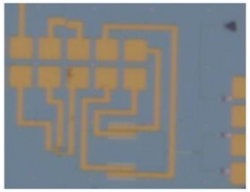

ED, H.-K. Lo, B. Qi, Z. Yuan, npj Quantum Info. 2016

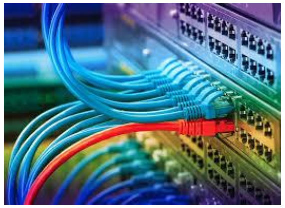
A rich field with constant innovation in both theoretical protocols and practical implementations

# Addressing current practical challenges

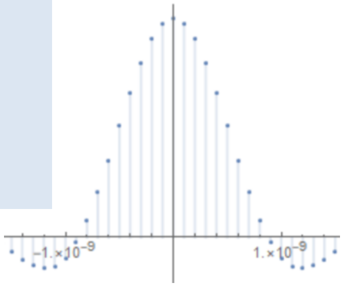


**High cost**
Photonic integration for reduced cost and scalable solutions





**Lack of network integration**
Operation in optical telecom systems to improve compatibility with conventional architectures and reduce deployment cost




**Absence of standards and certification**
Parallel efforts in relevant bodies, crucial for interoperability and market adoption

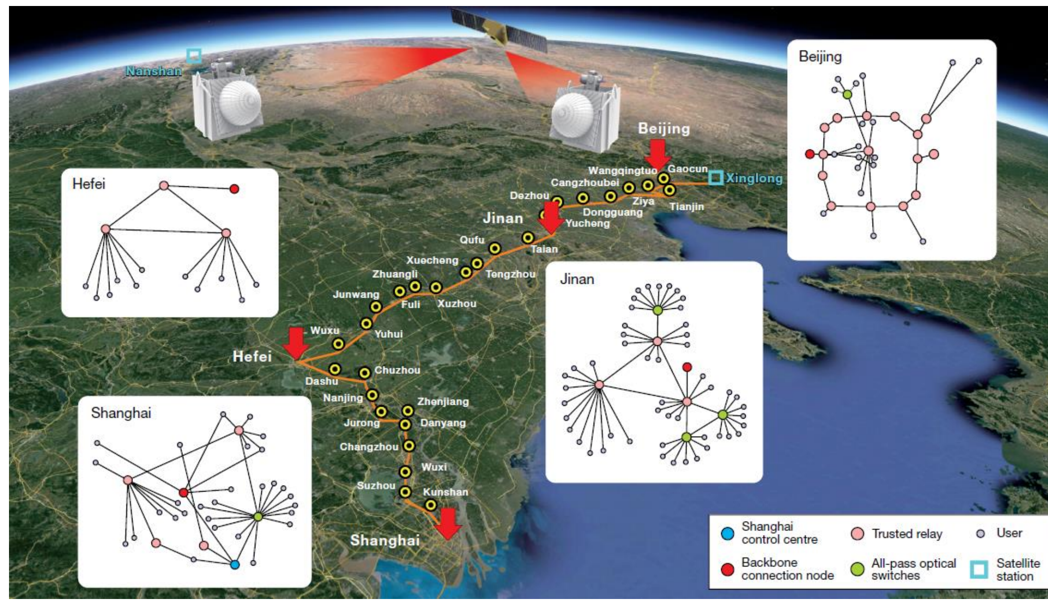

**Inherent range limitation due to optical fiber loss**
Quantum networks and Satellite communications

# Towards a Quantum Communication Infrastructure



Practical testbed deployment is crucial for
interoperability, maturity, network integration aspects and topology, use case benchmarking, standardization of interfaces

Y.-A. Chen *et al.*, Nature 2021




Trusted node networks
SECOQC QKD network, 2008
South Africa, Swiss, Tokyo,
UK QC Hub networks
China 2000 km backbone network, including satellite link

LEO Micius: downlink QKD, uplink quantum teleportation, entanglement-based QKD

Networks with untrusted nodes for end-to-end security

Quantum repeaters, long-term and efficient quantum storage beat direct transmission, improve rates, develop network and protocol stack

European Commission

esa

**EuroQCI**