Secure communications in quantum networks

Eleni Diamanti

LIP6, CNRS, Sorbonne Université

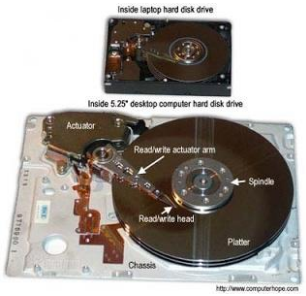
Paris Centre for Quantum Computing

Horizon 2020 Programme

ICE seminar, IP Paris

7 October 2021

The quantum revolutions



Planck's quantum theory — beginning of 20th century

transistor — 1947

hard disk — 1954

laser — 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)

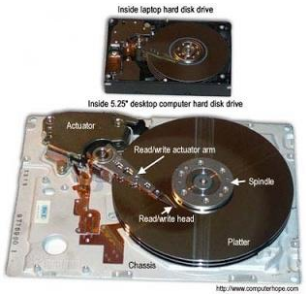
Werner Heisenberg (1901-1976)

Erwin Schrödinger (1887-1961)

The first quantum revolution

Observation and macroscopic manifestation of quantum principles

The quantum revolutions



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

beginning of 20th century — 1947 — 1954 — 1960 — end 20th / beginning 21st

Richard Feynman
(1918–1988)

Serge Haroche

Control of single quantum particles
First quantum algorithms

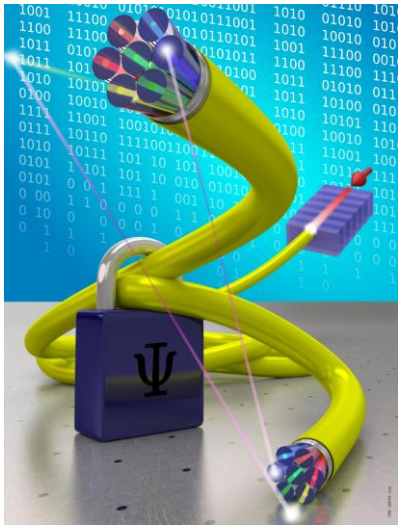
And also Alain Aspect, Charles Bennett, Gilles Brassard, Artur Ekert, Peter Shor…

The second quantum revolution

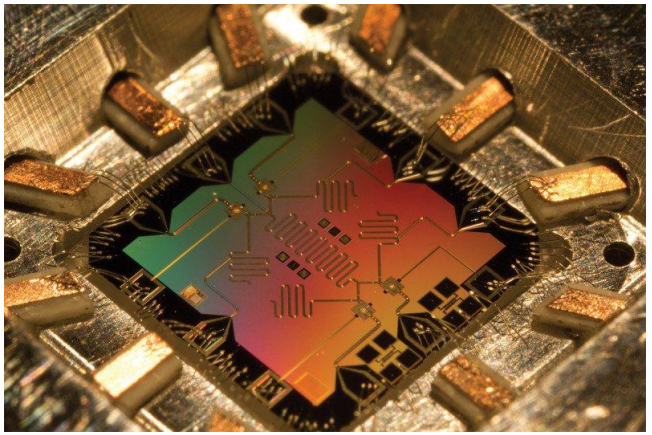
Active manipulation of single quantum particles and interaction between multiple particles for applications

Quantum technologies

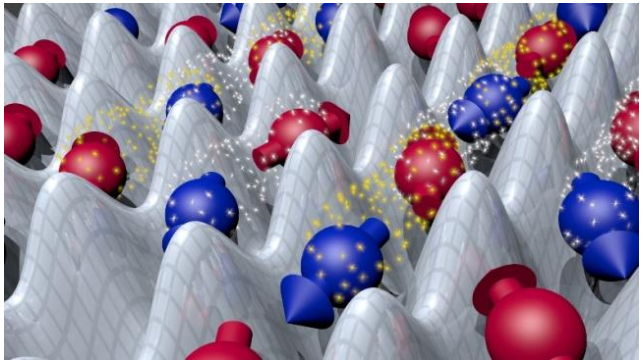
Unconditionally secure communication



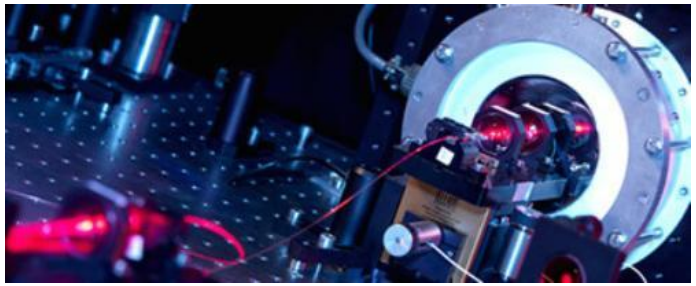
A leap in computing power



Increased understanding of complex physical systems

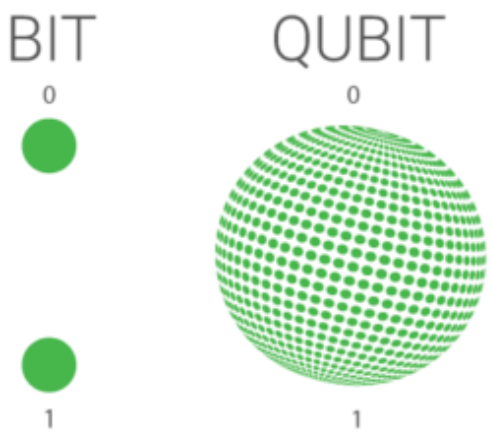


Measurement precision beyond the classical limit



Encoding quantum information

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

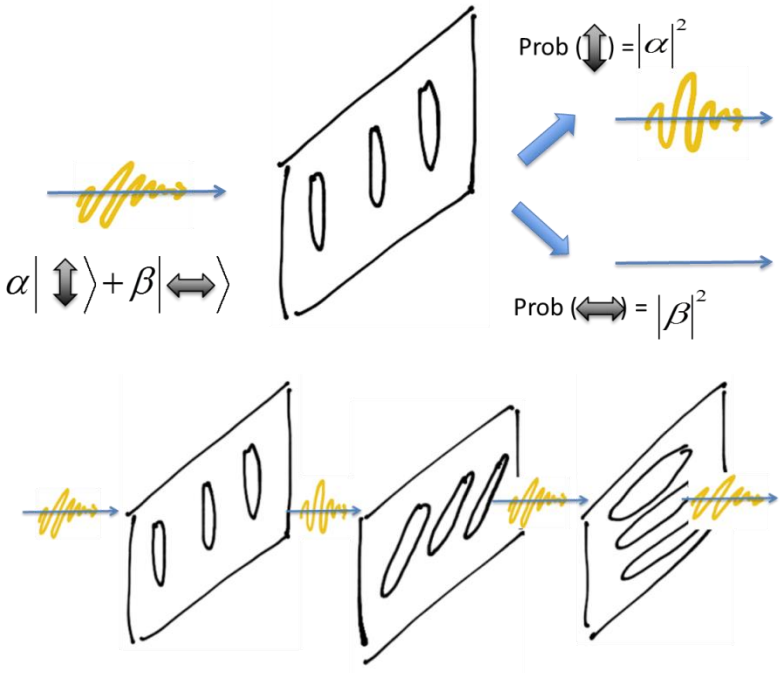


$$\alpha|0\rangle + \beta|1\rangle$$

with α, β complex numbers and

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

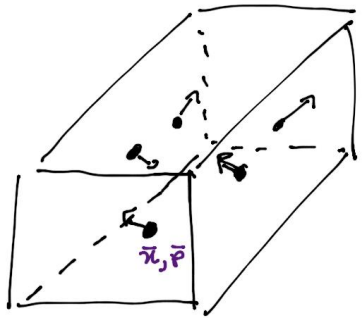
Photons are ideal carriers of quantum information
→ robust to ambient noise
→ can be transported over long distances



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

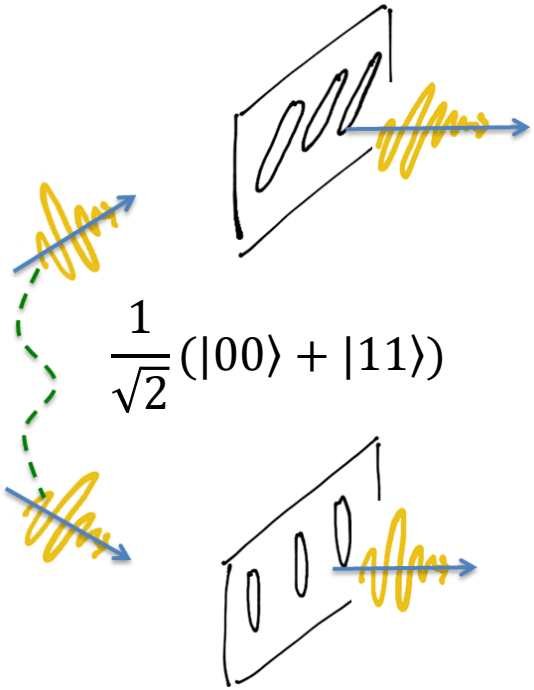
Entanglement

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



In classical physics, randomness comes from ignorance

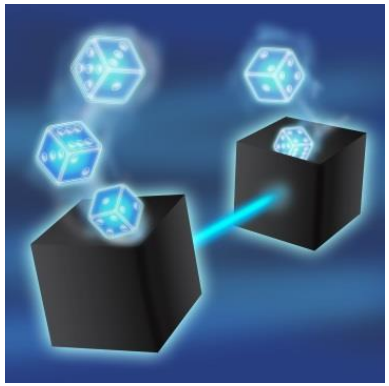
Einstein-Podolsky-Rosen paradox: same for quantum theory?



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

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

No cloning theorem
Unknown quantum states cannot be cloned



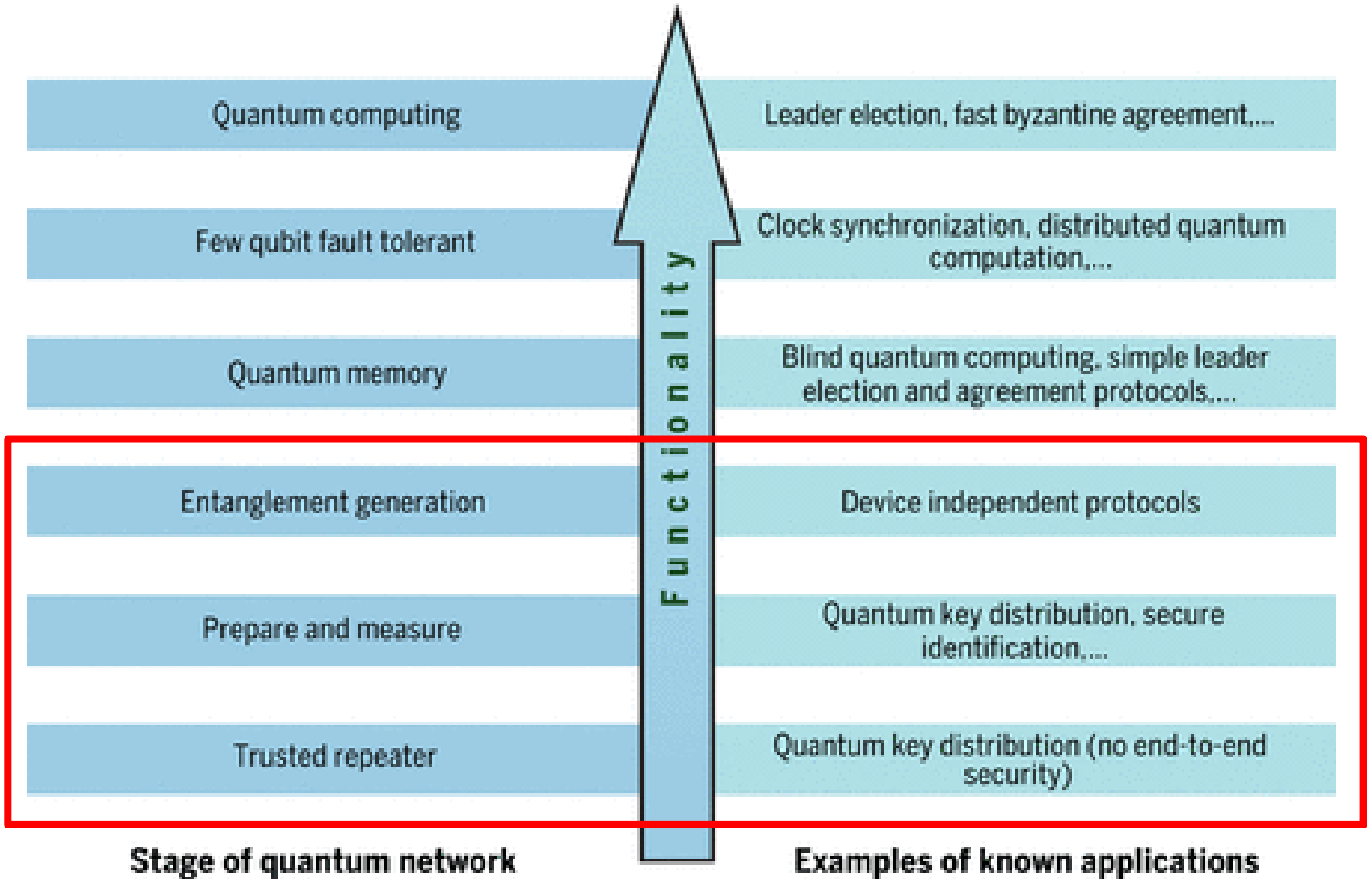
Quantum communication networks

A quantum communication network is a set of quantum systems linked together to

- exchange data
- use the fundamental properties of quantum mechanics (superposition, entanglement, measurement) in order to reinforce “classical” computer network services or to create new ones → quantum advantage in security, efficiency, computation…

The quantum systems - the nodes of the network - can be quantum processors, quantum sensors, quantum memories, or "simple" devices used to generate or measure quantum states, and are connected via optical fiber or free-space channels

Applications of quantum communication networks

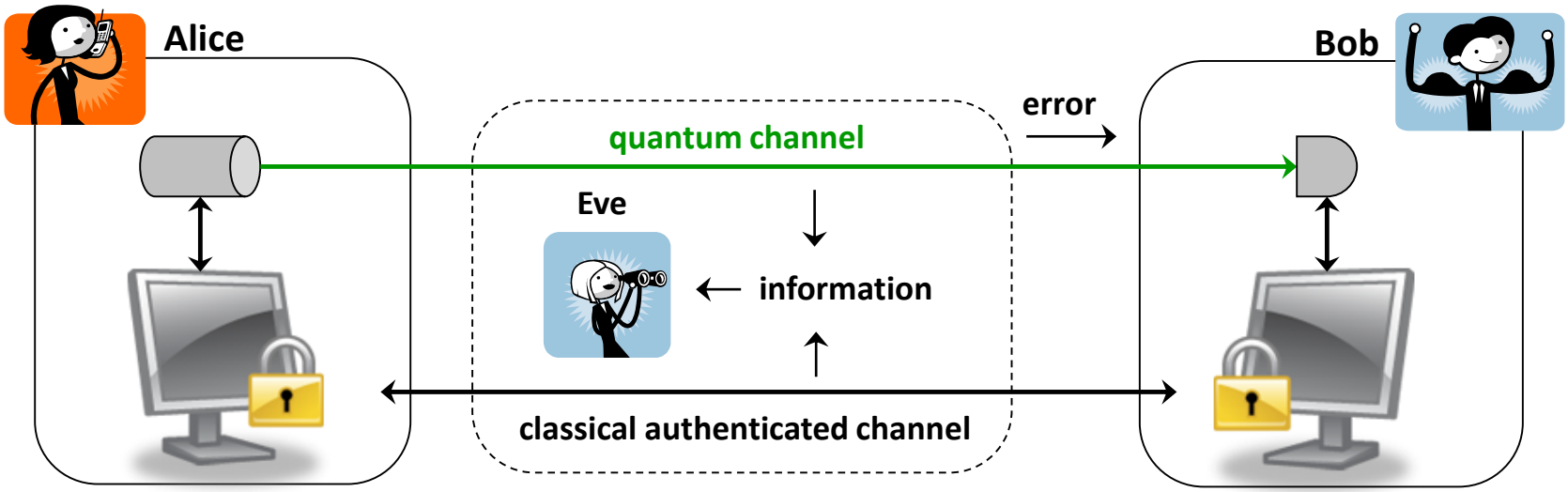


S. Wehner *et al.*, Science 2018

Securing network links: quantum key distribution

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

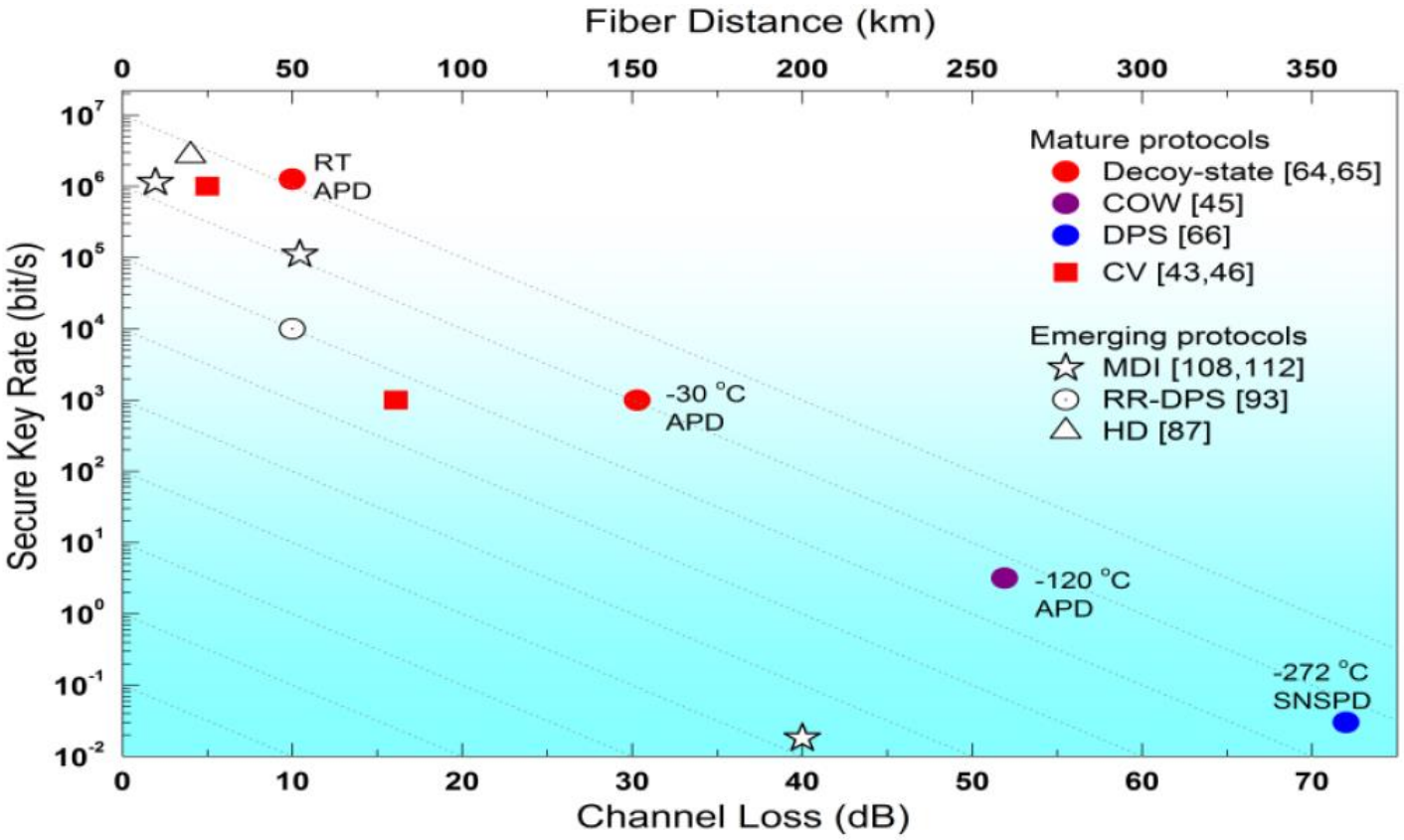
Quantum key distribution allows for exchange of sensitive data between two trusted parties with information-theoretic, long-term security guaranteed against an all-powerful eavesdropper
→ combined with suitable authentication and message encryption algorithms



Key information is encoded on photonic carriers

Analysis of errors due to Eve's perturbation leads to extraction of secret key

QKD performance



Performance of point-to-point fibre-optic QKD systems

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

Several protocols for the same functionality, fundamental limits in rate and range

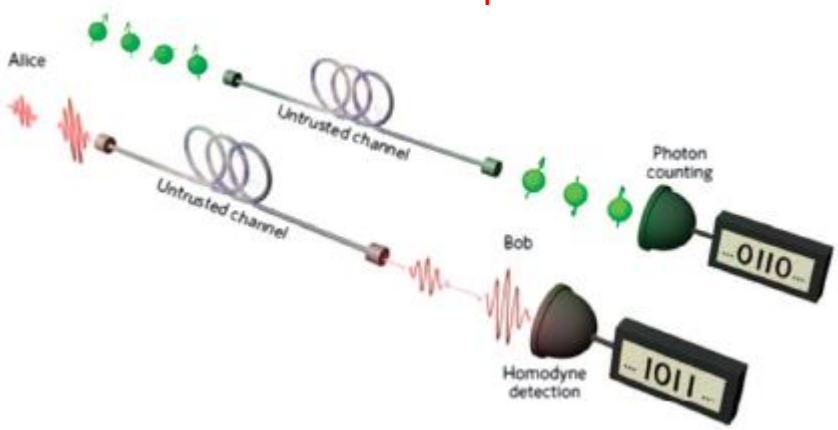
Security: $\frac{1}{2}\left\|\rho_{S_A S_B E} - \tau_{SS} \otimes \rho_E\right\|_1 \leq \varepsilon$ for any $\rho_{A^n B^n E}$

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

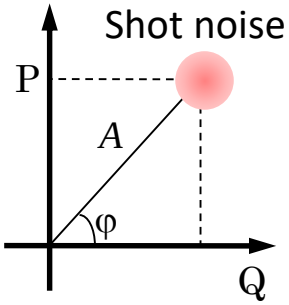
BB84, Decoy state, Coherent One Way, Differential Phase Shift, (Measurement) device independent protocols

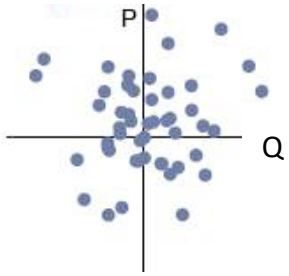
CV-QKD (one or two-way, Gaussian or discrete modulation, coherent or squeezed states, post selection), (Measurement) device independent protocols



V. Scarani *et al.*, Rev. Mod. Phys. 2009
ED and A. Leverrier, Entropy 2015
F. Xu *et al.*, Rev. Mod. Phys. 2020
S. Pirandola *et al.*, Adv. Opt. Phot. 2020

Coherent state CV-QKD

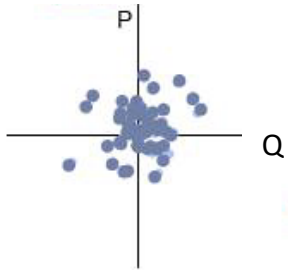




$$\{q_i \quad p_i, 1 \leq i \leq N\}$$

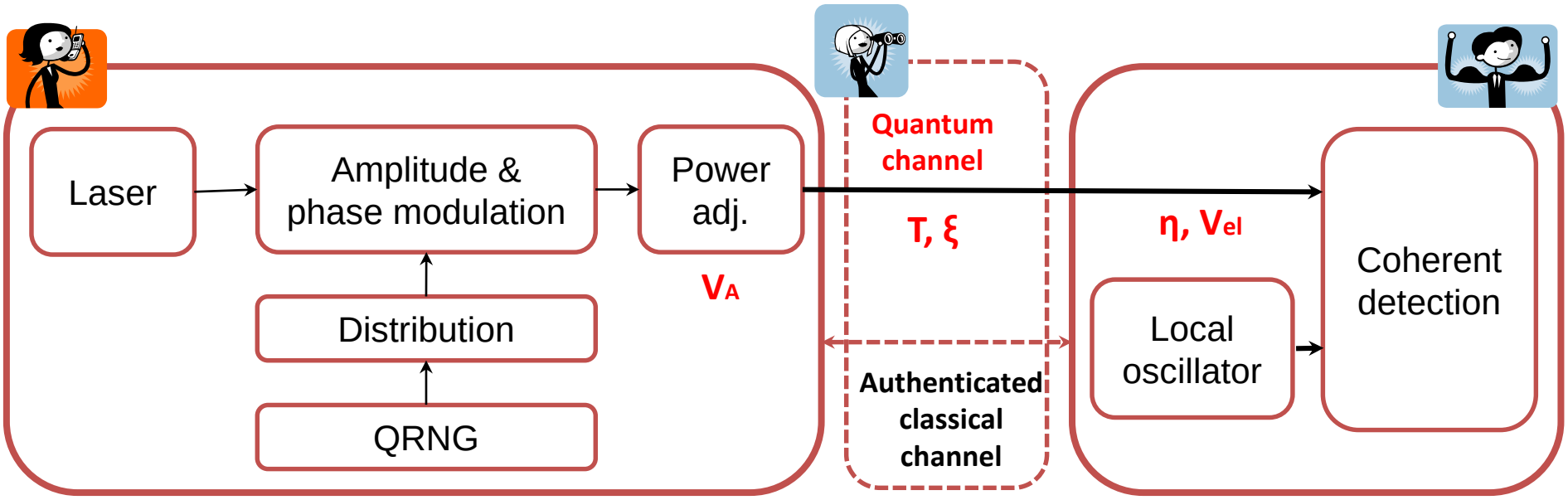
$$|\alpha\rangle_i = |q_i + ip_i\rangle$$

Gaussian modulation, QPSK, QAM,…



Single (homodyne) or double (heterodyne) quadrature detection

Trusted (calibrated) noise

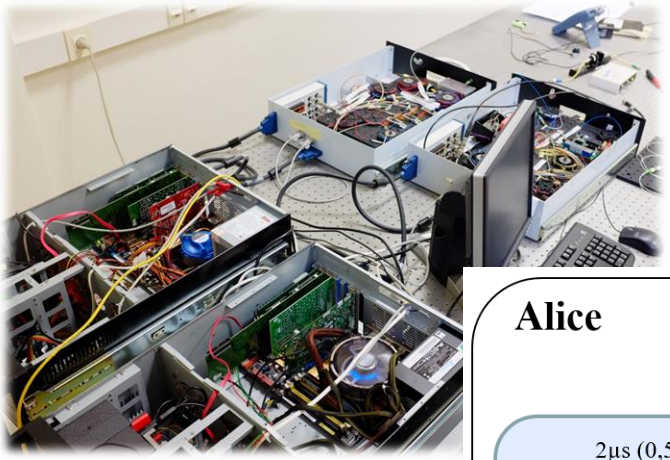


Composable, finite size security proof

A. Leverrier, Phys. Rev. Lett. 2015, 2017

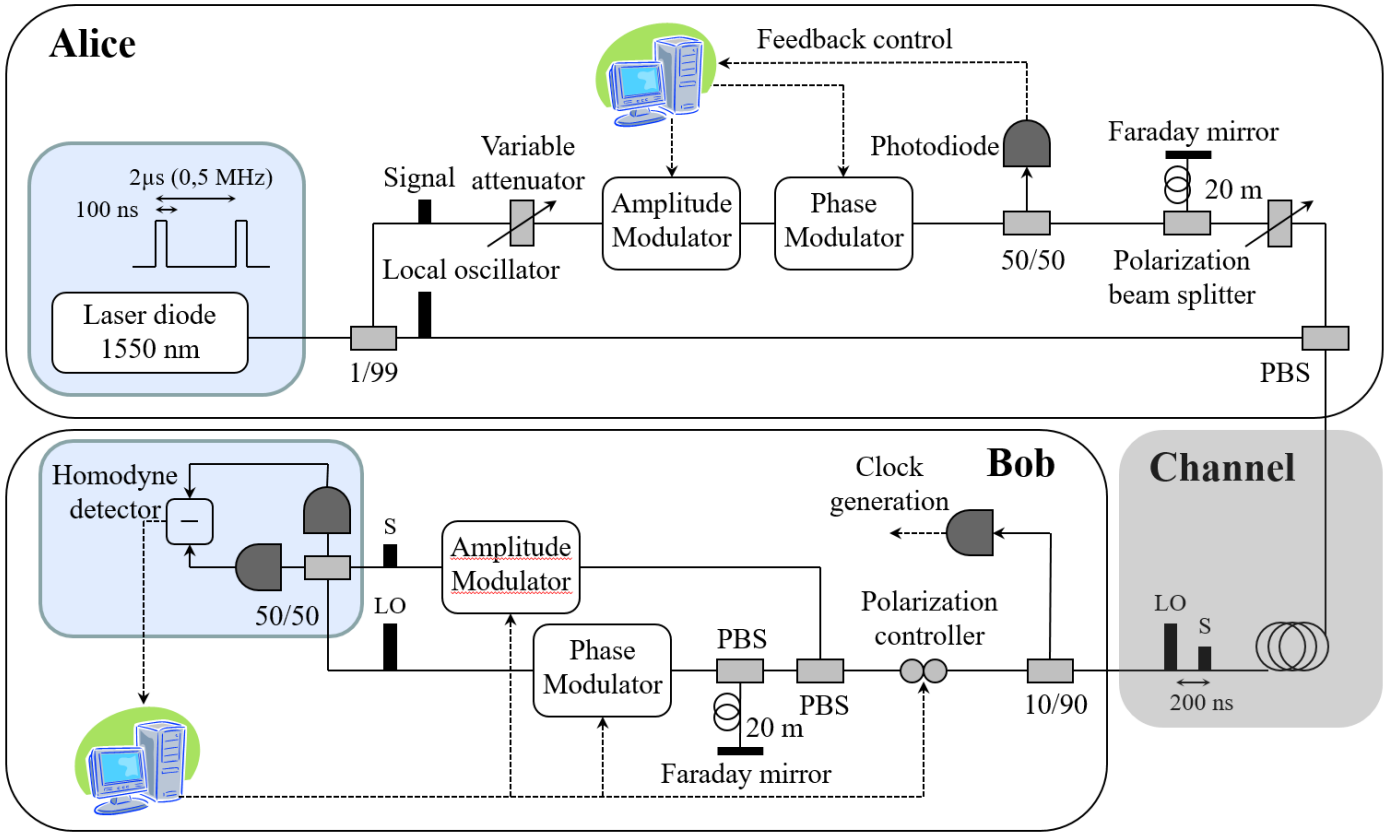
Classical post-processing: parameter estimation, error correction, privacy amplification

Experimental system



No single-photon detection
Only standard telecom components

Transmitted LO
Pulsed operation
Homodyne detection
Gaussian modulation



Long-distance operation with optimized error correction and stability

P. Jouguet *et al.*, Nature Photon. 2013

Bandwidth-efficient CV-QKD

Challenge: **lack of network integration**
Operation in coherent optical telecom systems to improve compatibility with conventional architectures and reduce deployment cost

Transmitted LO

Pulsed operation

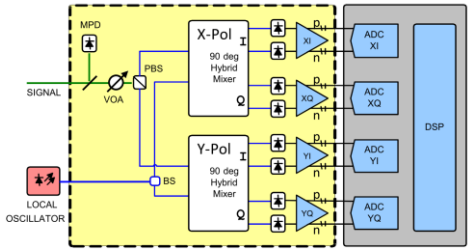
Homodyne detection

Gaussian modulation

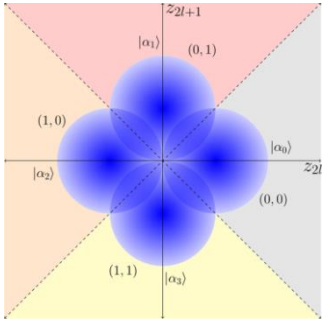
Local LO: no related side channels, no LO intensity limitation, no multiplexing, constraints in laser linewidth

CW pulse shaping techniques: optimal use of spectrum, avoid inter-symbol interference, use of pilots, optimal Digital Signal Processing used for signal recovery

Amplified balanced photodiodes or Integrated coherent receivers (ICR): shot noise limited, low noise, high bandwidth



Proper security analysis is crucial!



Asymptotic security proof for QPSK

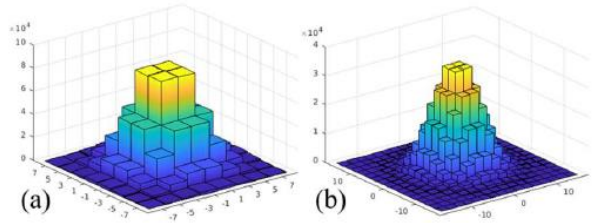
Extended to constellations of any cardinality

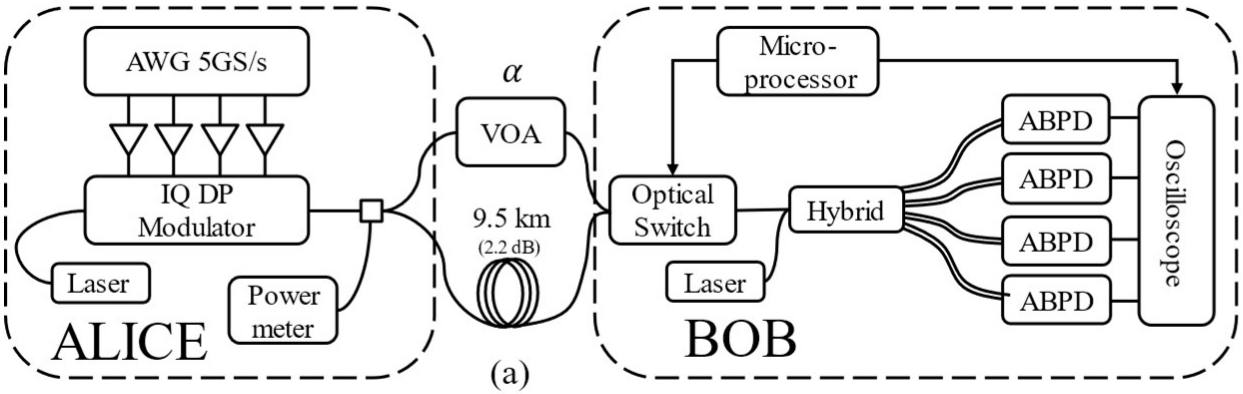
S. Ghorai, P. Grangier, ED, A. Leverrier, Phys. Rev. X 2019
A. Denys, P. Brown, A. Leverrier, Quantum 2021

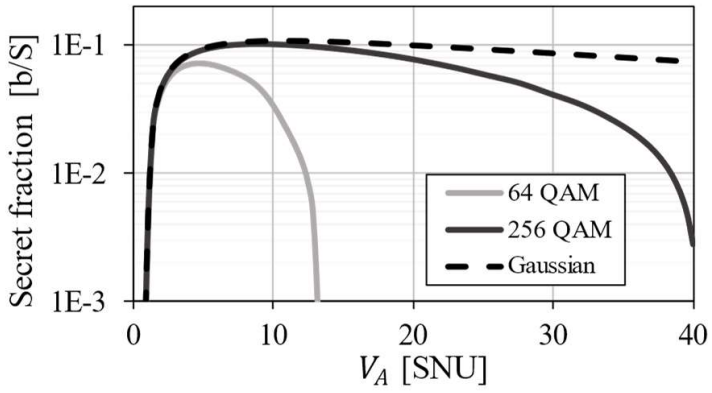
Bandwidth-efficient CV-QKD

PCS 64 and 256-QAM, dual pol., Nyquist pulses, 50% QPSK pilots, 600 Mbaud, 10 kHz linewidth lasers

F. Roumestan *et al.*, ECOC 2021





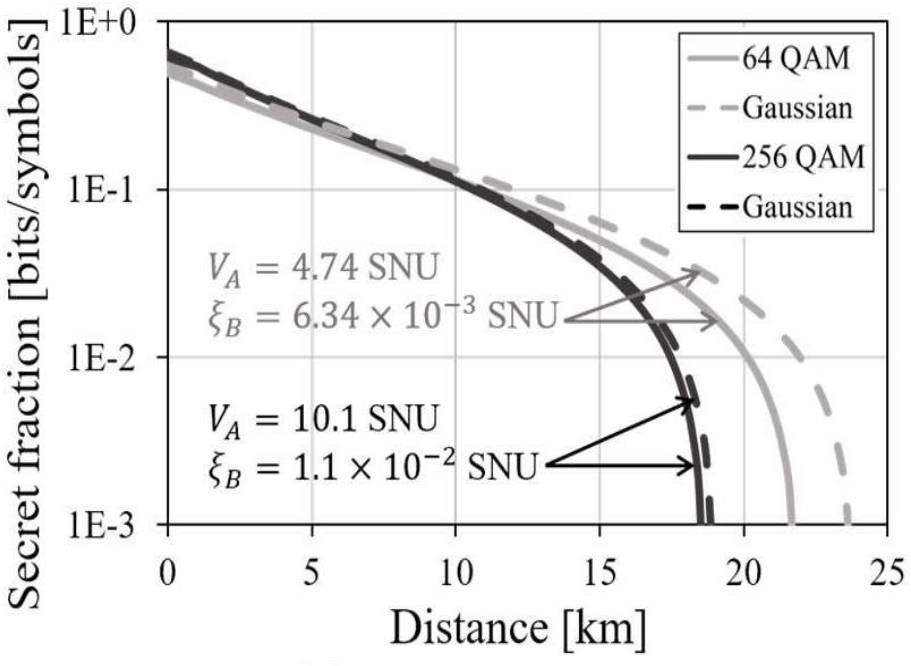


- RRC Matched Filter
- CAZAC Synchronization
- Pilot-aided CMA Equalizer
- Carrier Frequency Estimation
- Carrier Phase Estimation
- QKD Parameter Estimation

CiViQ

NOKIA Bell Labs

Bandwidth-efficient CV-QKD



Secret key rate higher than
65 Mbit/s at 10 km

Adapted to high secret key rates at moderate distance

Next steps:

Further optimization (pilots, DSP, stability) for smaller excess noise, longer distance

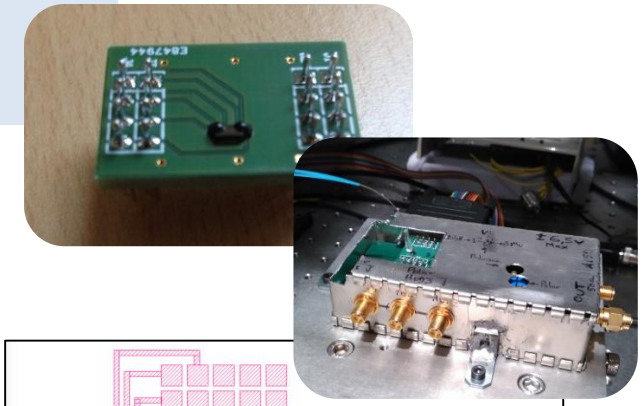
Implementation of data reconciliation

Full security proof with finite-size effects

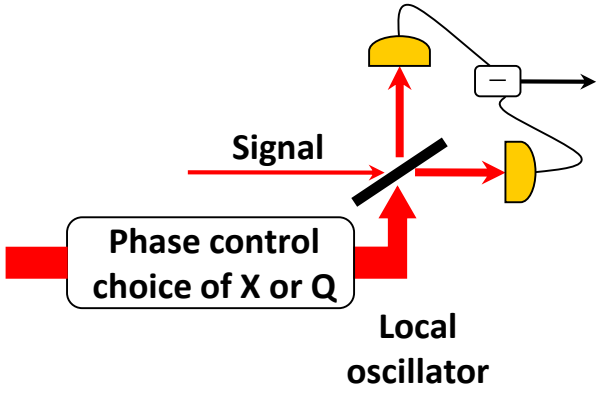
CV-QKD on chip

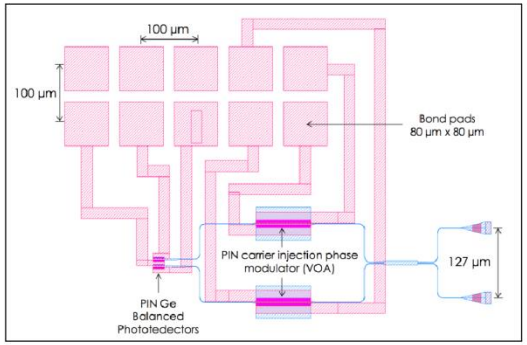
Challenge: **high cost**

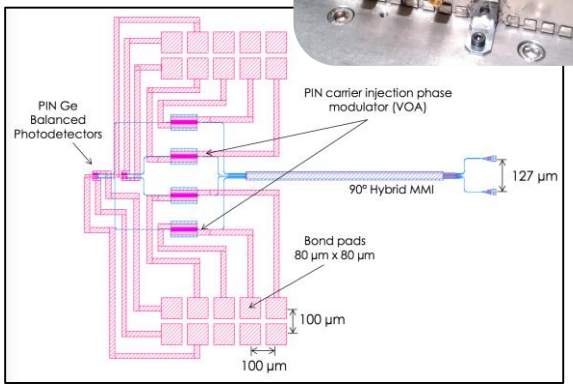
Photonic integration for reduced cost and scalable solutions

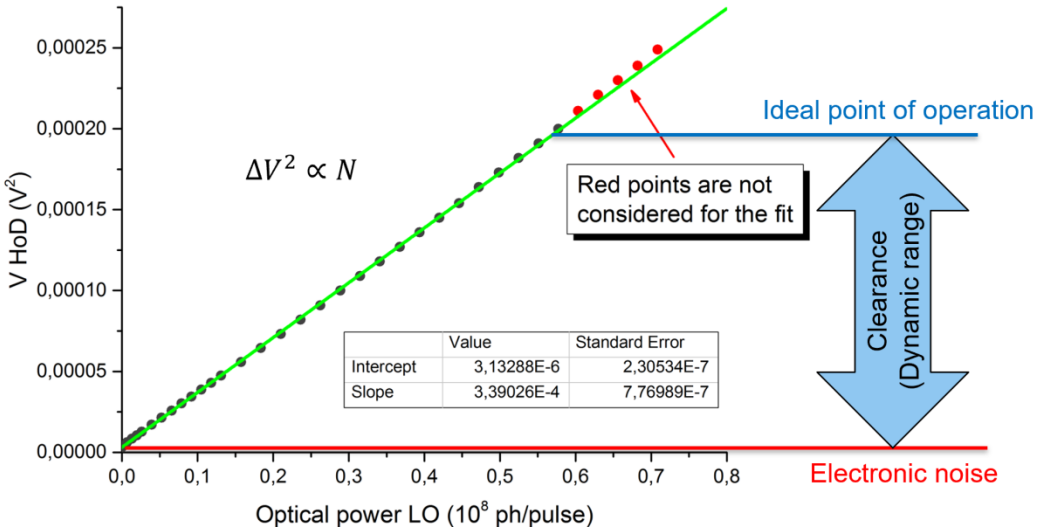


Silicon photonic chips (CEA-LETI)









Shot-noise limited silicon-integrated homodyne detection for CV-QKD

10 - 18 dB clearance

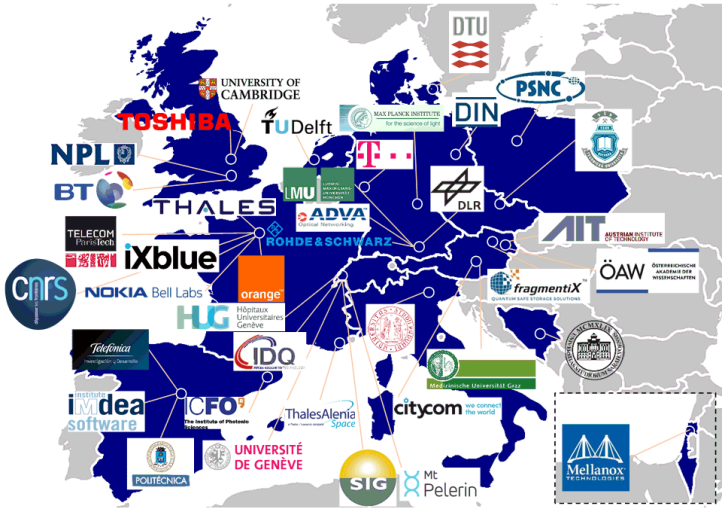
Next step: operation with on-chip Tx

L. Trigo Vidarte *et al.*, QCrypt 2018

QKD networks

Challenge: **inherent range limitation due to optical fiber loss**
QKD networks and Satellite communications

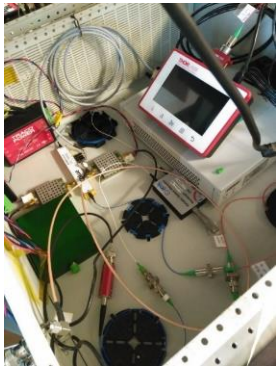
Practical testbed deployment is crucial for interoperability, maturity, network integration aspects and topology, use case benchmarking, standardization of interfaces



OPEN QKD

Academics, telecom operators, equipment providers, end users

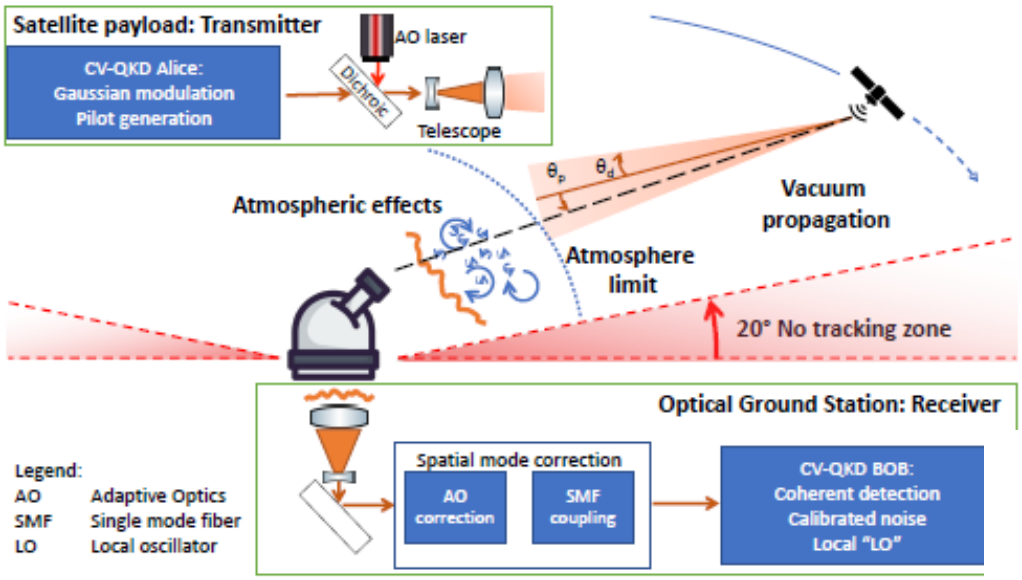
Data centres, electrical power grids, governmental communication, medical file transfer, critical infrastructure,…



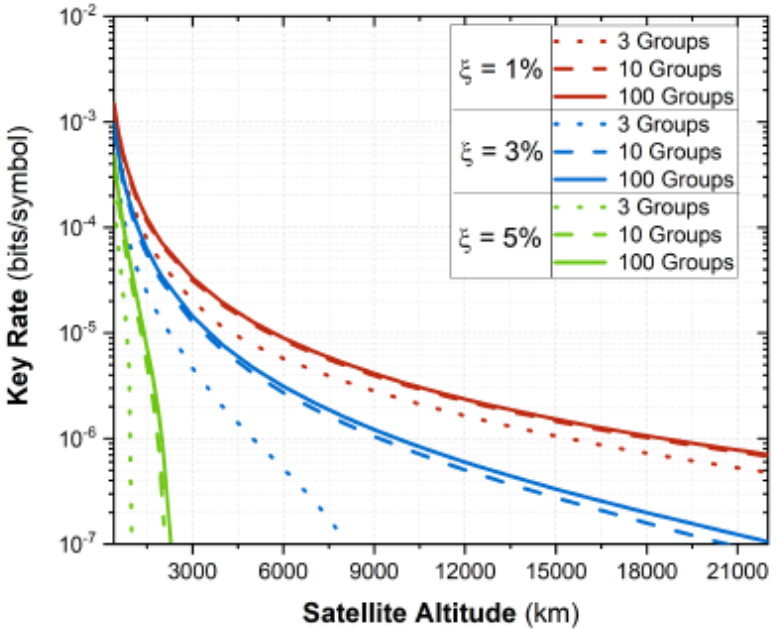
High-speed solutions based on RFSoC technology
for prototype deployment in Paris testbed

iXblue

Feasibility of satellite-to-ground CV-QKD



Compatible with space-certified telecom components



Security analysis for a fluctuating channel

Fading introduces an additional noise source

To reduce its variance division of data according to transmission efficiency

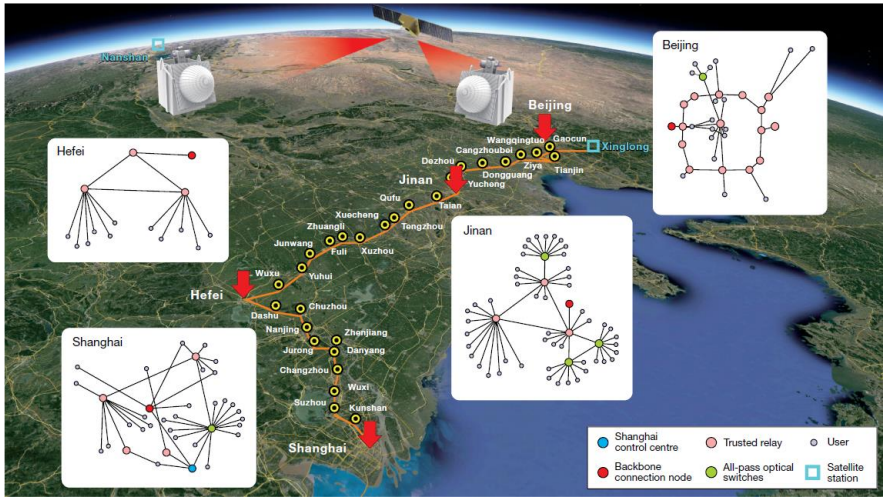
D. Dequal *et al.*, npj Quant. Info. 2021

1 GHz, $V_A = 1$, $\beta = 0.95$, a = 0.75 m, pointing error 1 µrad, divergence angle 10 µrad, 3 dB fibre coupling loss

Trusted node networks

If the distance between Alice and Bob exceeds the range of the system:

Alice-R: key1, R-Bob: key2, R: key1⊕key2 → Bob: key2⊕(key1⊕key2) = key1



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

EuroQCI program

Terrestrial and space segments

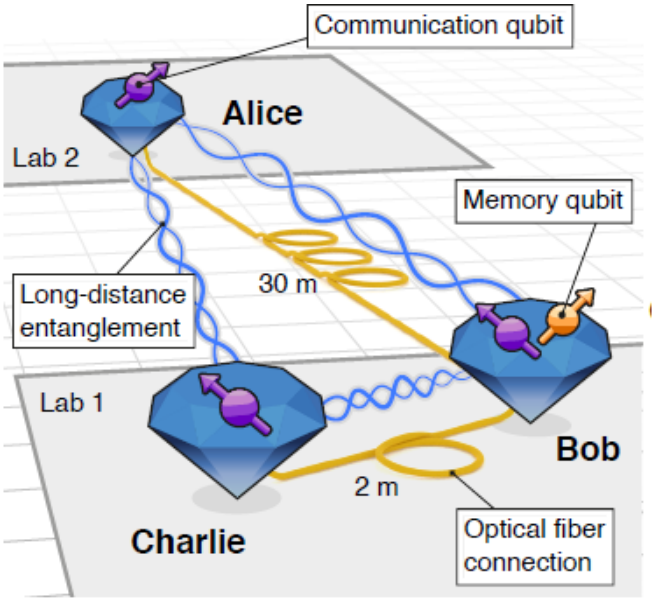
Focus on cost, range, network integration, quantum/classical coexistence, security, standards and certification, applications for the quantum internet

Reducing trust requirements : quantum repeaters

From trusted nodes to end-to-end security

Entanglement distribution alleviates the need for trust in the nodes but quantum channels are lossy and noisy

Quantum repeaters and processing nodes, quantum memories



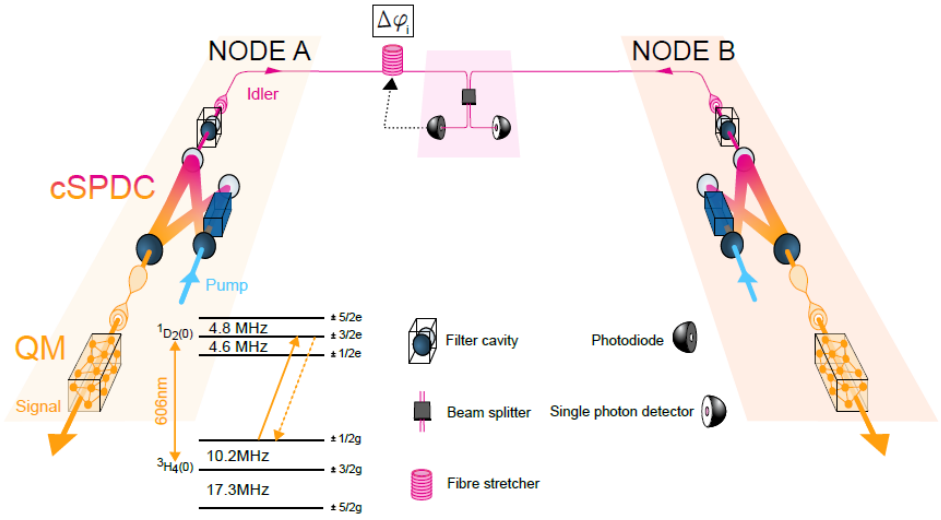
TU Delft, M. Pompili *et al.*, Science 2021

Challenges

Storage time and efficiency

Entanglement generation rates

Limited range



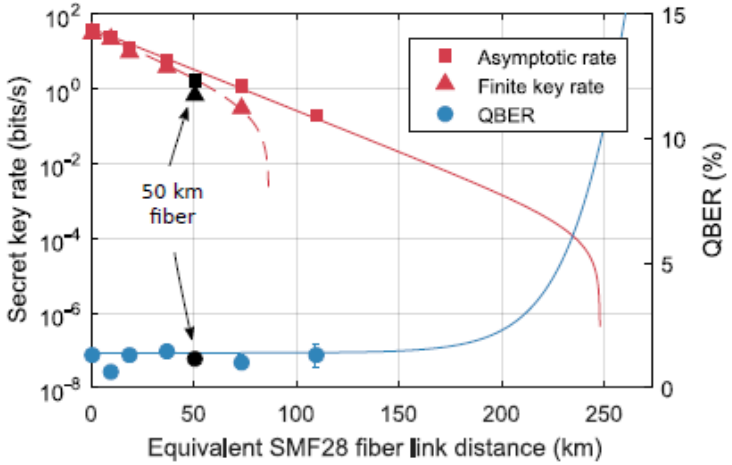
ICFO, D. Lago-Rivera *et al.*, Nature 2021

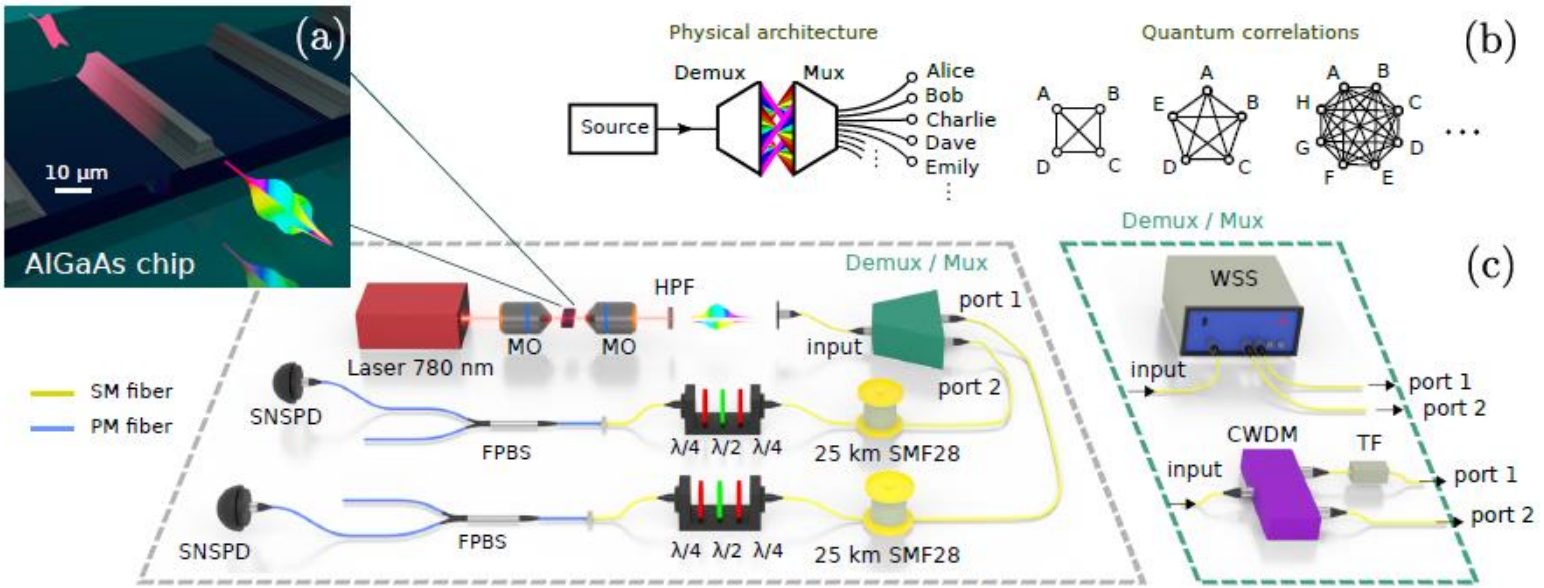
Near-term quantum network applications

Entanglement-based QKD, quantum coin flipping, unforgeable quantum money, anonymous transmission, communication complexity,…

Flexible entanglement distribution network for secure communication with a broadband AlGaAs source

F. Appas *et al.*, npj Quant. Info. 2021



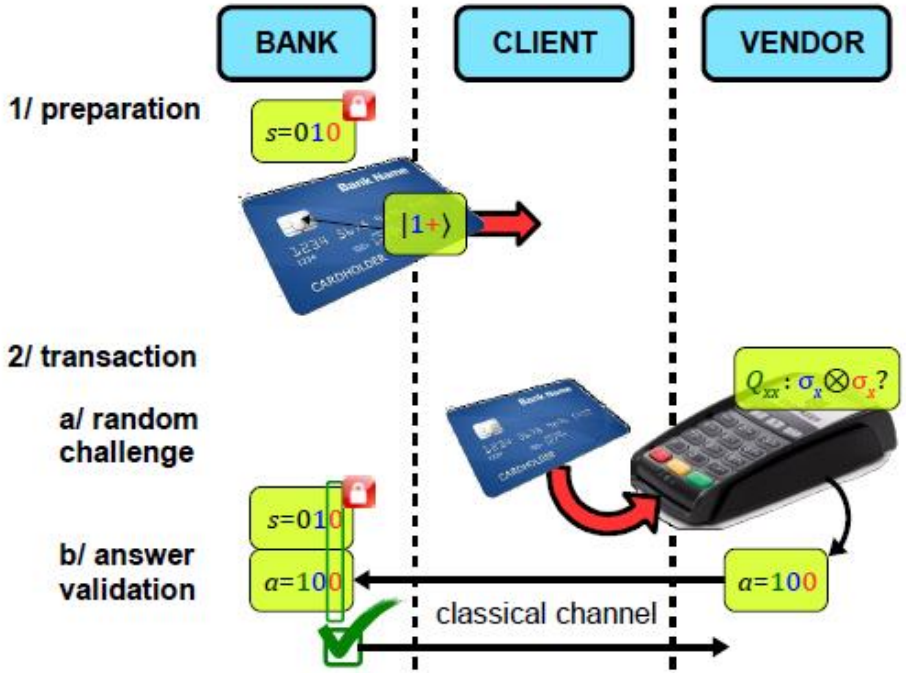


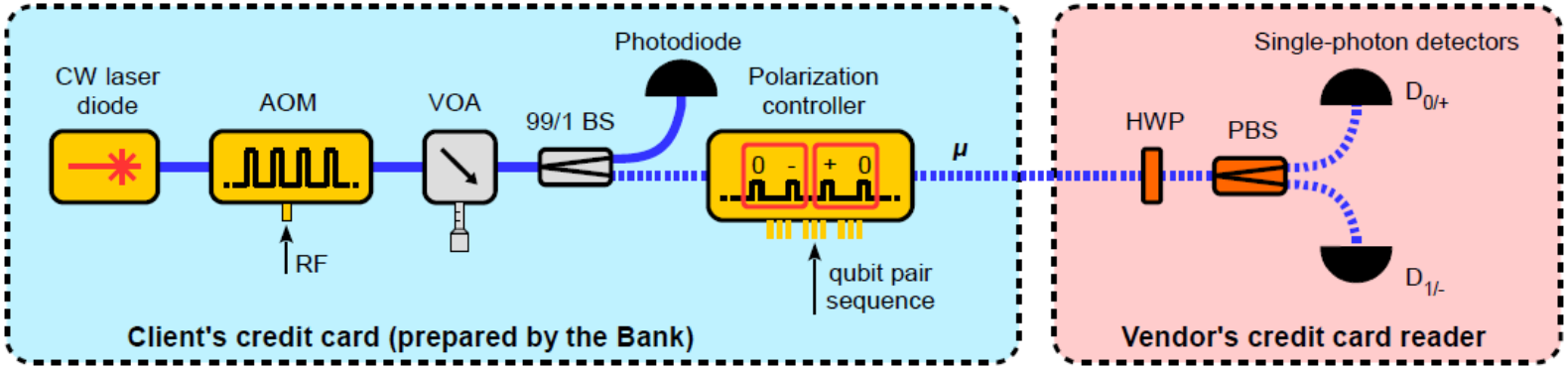
Unforgeable quantum money

Wiesner's original idea (1973) of using the uncertainty principle for security

But needs quantum verification and is not robust to imperfections
Considered hard to implement

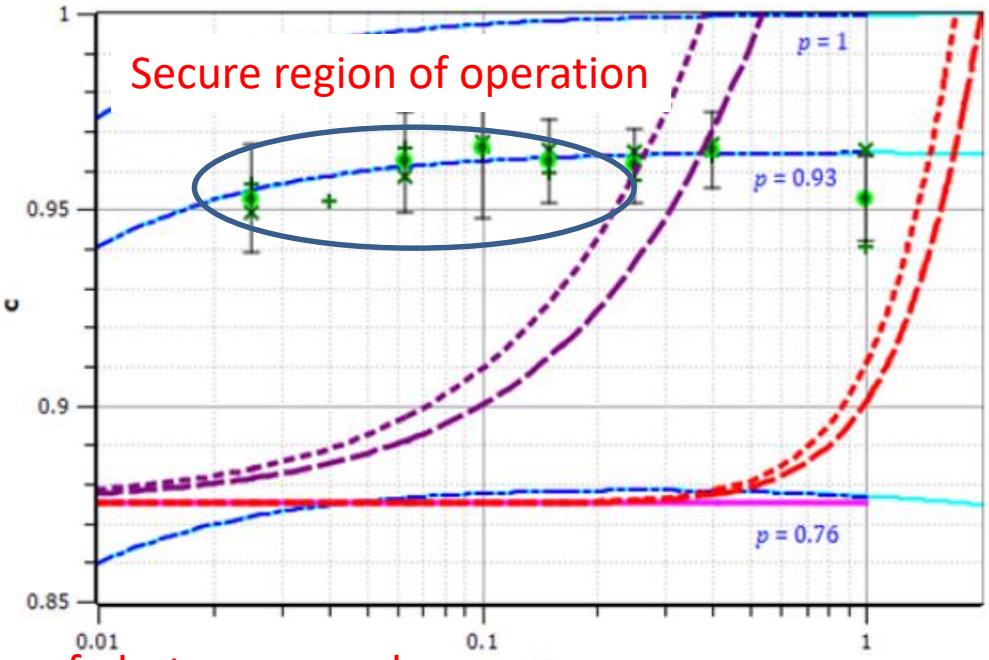
New protocol with classical verification and standard qubit states
Based on challenge questions





Unforgeable quantum money

Probability of answering the bank's challenge correctly →



Rigorously satisfies security condition for unforgeability
→ quantum advantage with trusted terminal

General security framework for weak coherent states and anticipating quantum memory
→ minimize losses and errors for both trusted and untrusted terminal

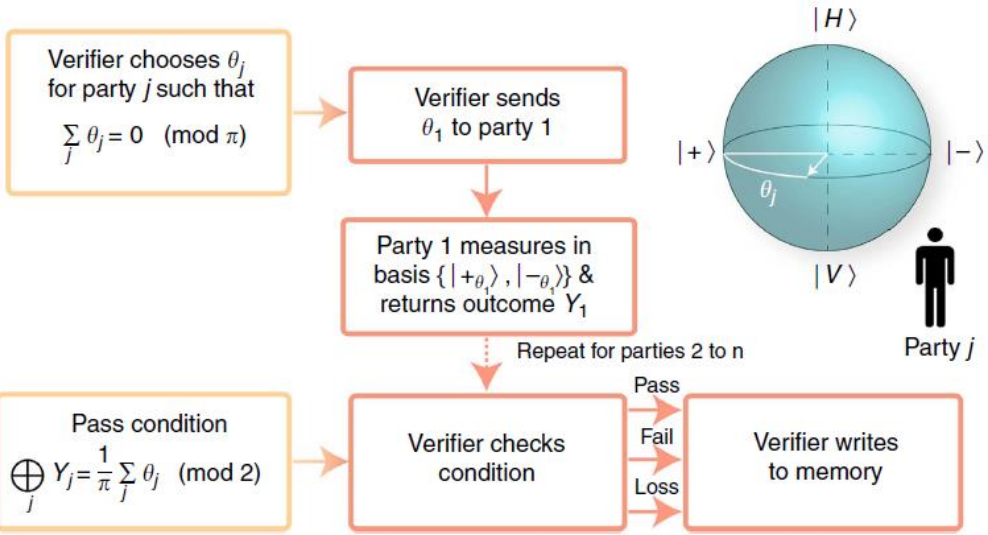
M. Bozzio *et al.*, npj Quant. Info. 2018 & Phys. Rev. A 2019

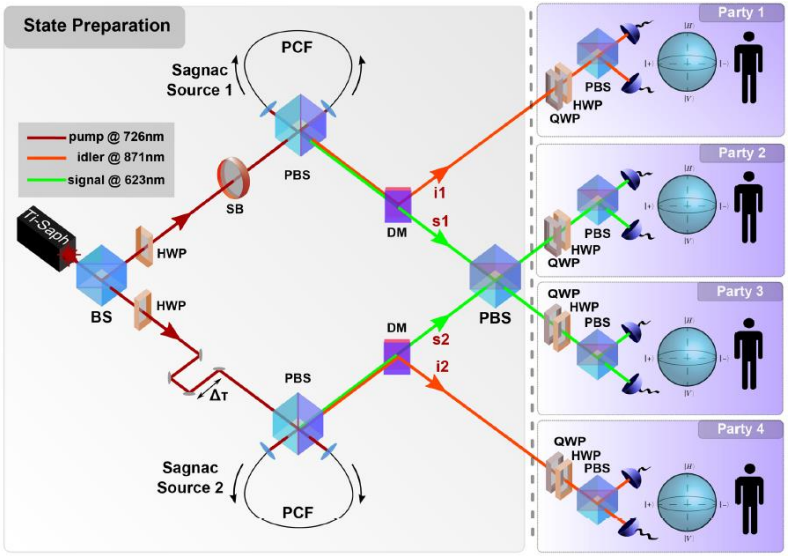
Entanglement verification

Proof-of-principle verification of multipartite entanglement in the presence of dishonest parties

W. McCutcheon *et al.*,
Nature Commun. 2016

Requires high performance resources
Very small loss tolerance





Application to anonymous message transmission and electronic voting

Verification phase guarantees anonymity and privacy

A. Unnikrishnan *et al.*, Phys. Rev. Lett. 2019
F. Centrone *et al.*, arXiv 2107.14719

Conclusion and perspectives

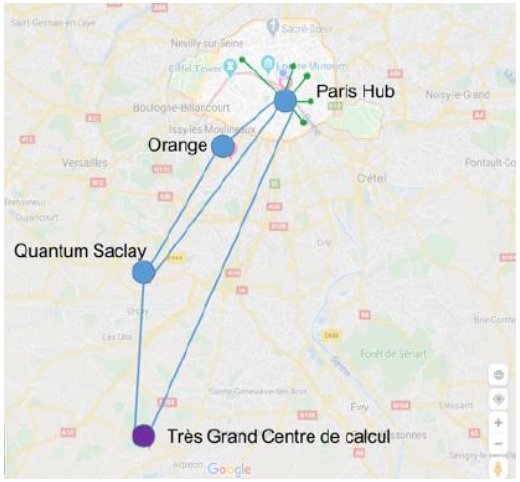
Quantum communication networks will be part of the future quantum-safe communication infrastructure

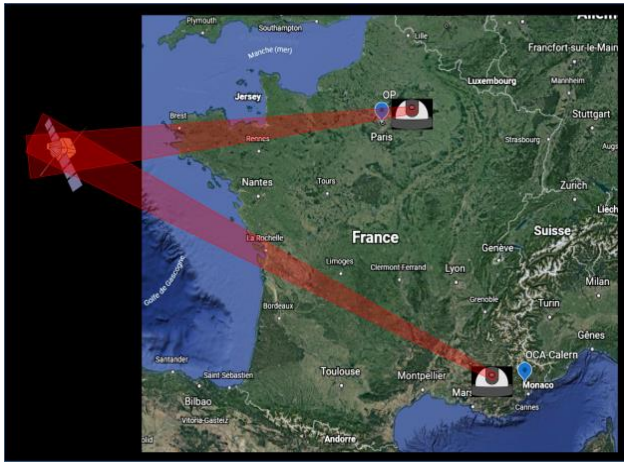
Such an infrastructure can address a range of use cases with high security requirements in multiple configurations

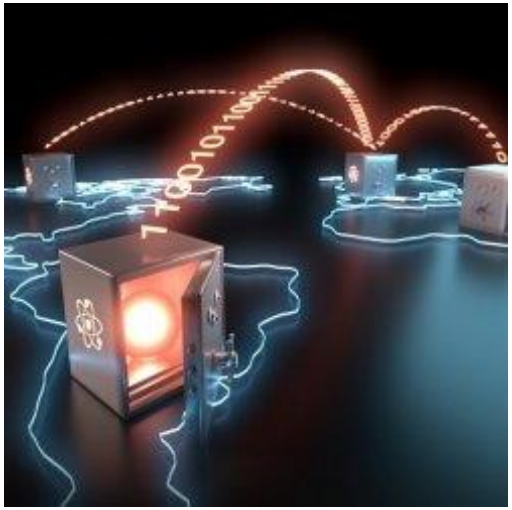
The quantum communication toolbox is rich and increasingly advanced

Quantum technologies need to integrate into standard network and cryptographic practices to materialize the global quantum network vision

Thank you!







L. Trigo-Vidarte, M. Schiavon, D. Fruleux, Y. Piétri,
V. Marulanda Acosta
F. Roumestan, A. Ghazisaeidi, B. Gouraud
A. Leverrier, P. Grangier
D. Dequal, G. Vallone, P. Villoresi
F. Appas, F. Baboux, M. Amanti, F. Boitier, S. Ducci
S. Neves, F. Centrone, V. Yacoub, R. Yehia, N. Kumar,
M. Bozzio, A. Unnikrishnan, D. Markham, I. Kerenidis