# Secure communications in quantum networks

Eleni Diamanti

LIP6, CNRS, Sorbonne Université

Paris Centre for Quantum Technologies

Congrès SFP, Paris

5 July 2023

# Quantum communication



**Quantum communication is the art of transferring quantum information between distant locations**

Encoding on properties of quantum states of light
Propagation in optical fibre or free-space channels
Information processing in network nodes (processors, sensors, memories)

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

**Efficiency**
Optimal use of communication resources

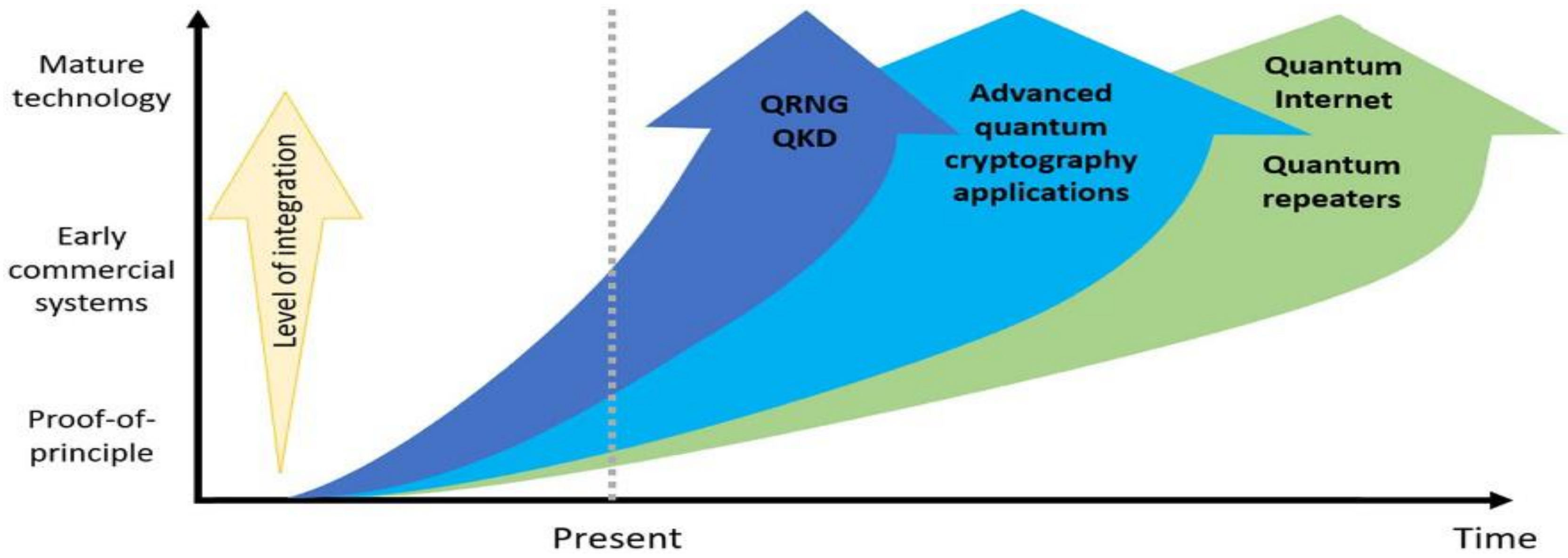
**Applications**
Demonstrate provable quantum advantage in security and efficiency for communication and information processing tasks

# Network development stages and applications



**Functionalities and applications**

| | | | |
|---|---|---|---|
| Prepare-and-measure QKD, coin flipping, oblivious transfer, position-based cryptography, digital signatures | Device-independent QKD, certification and verification, secret sharing, conference key agreement, anonymous communication | Quantum money, secure multiparty computing, leader election | Blind, delegated and distributed quantum computing, distributed quantum sensing, byzantine agreement |




| | | | |
|---|---|---|---|
| Trusted node | Entanglement | Quantum memory | Quantum processors |

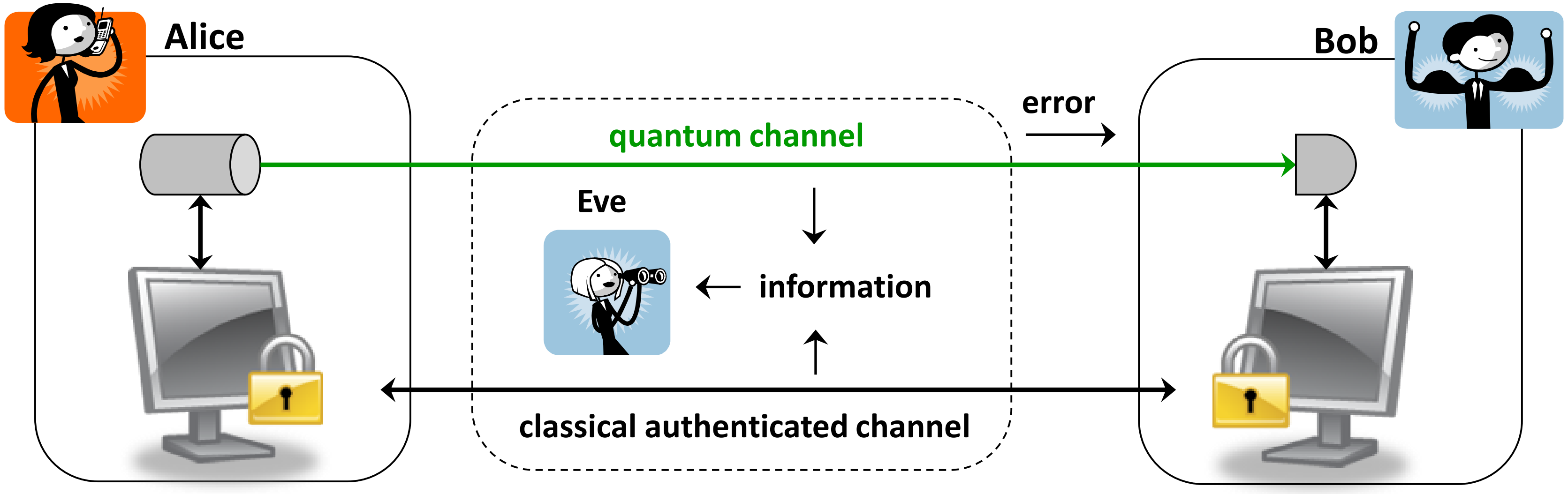
**Stages of quantum networks**

*Adapted from S. Wehner et al., Science 2018 & G. Moody et al., J. Phys. Photon. 2022*

# 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

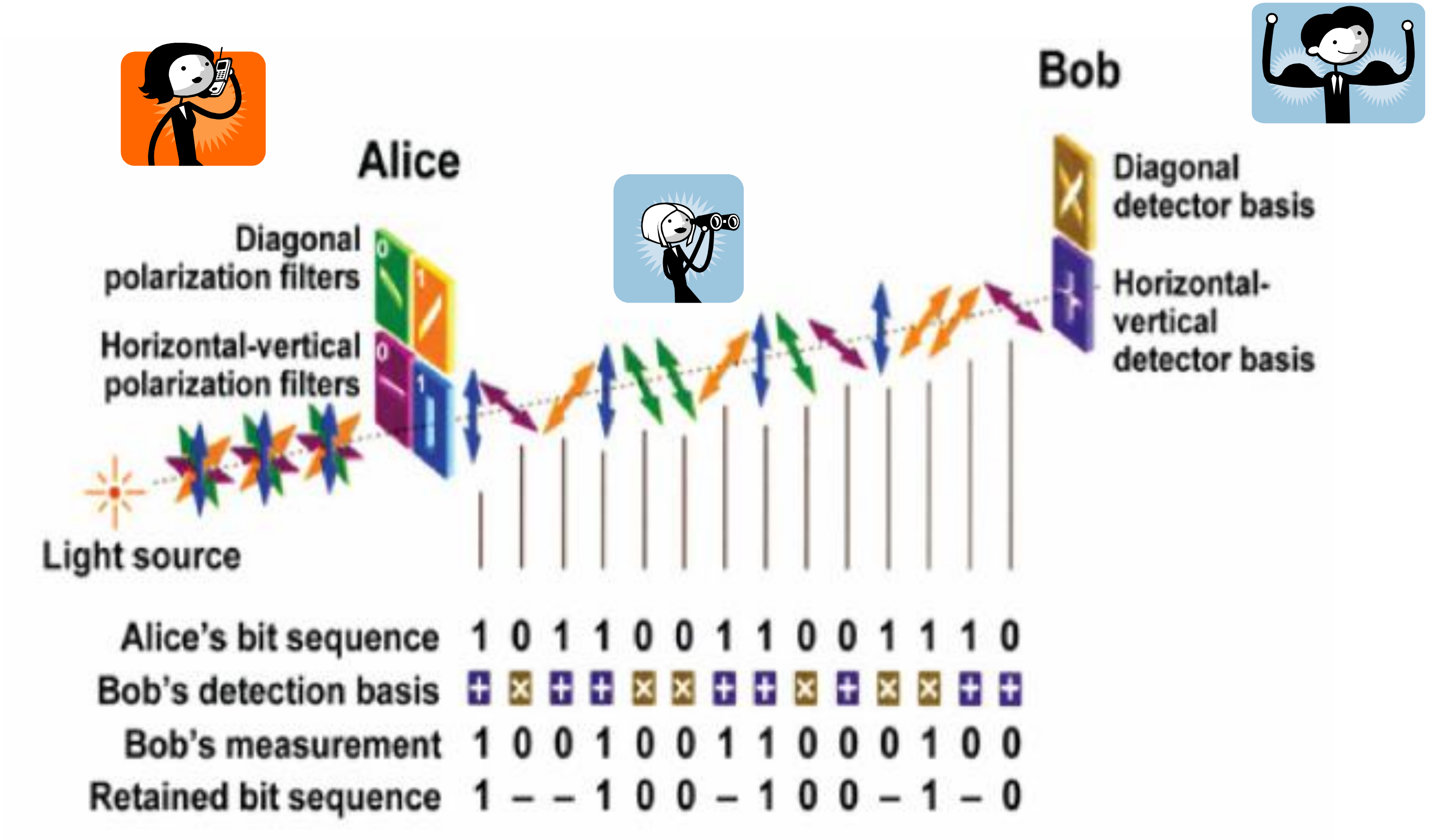



Key information is encoded on photonic carriers

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

# A single-photon QKD protocol – BB84






No cloning theorem: Eve cannot copy the states sent by Alice

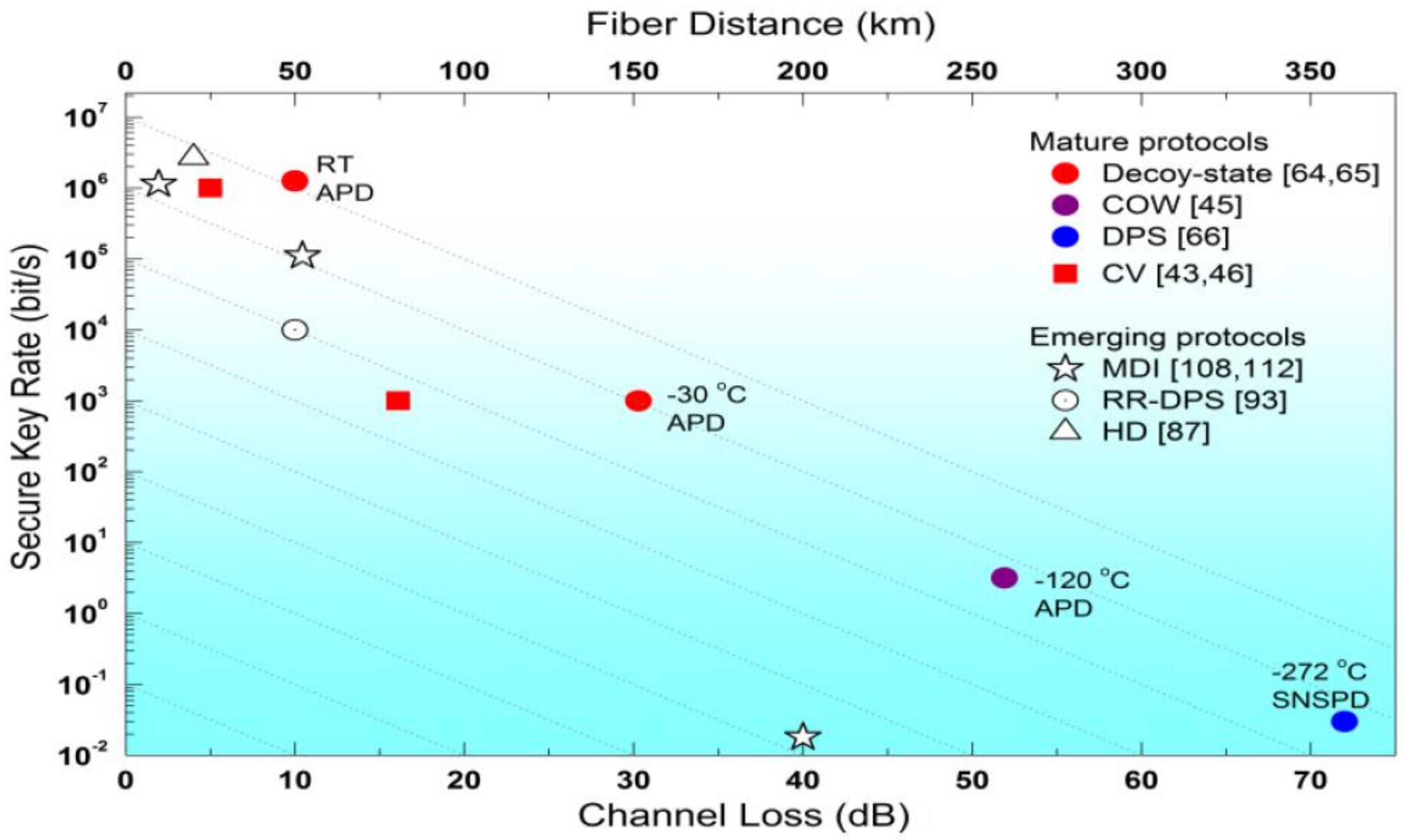
Heisenberg's uncertainty principle: Eve cannot measure in both bases

Device independence: If Alice and Bob share entangled photons less assumptions on devices

Practical security: Deviation from security proof may lead to side-channel attacks

# QKD in practice






Performance of point-to-point, prepare-and-measure fibre-optic QKD systems

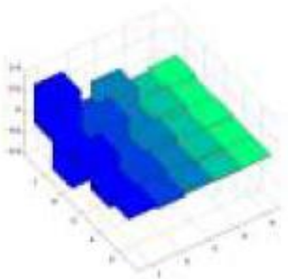
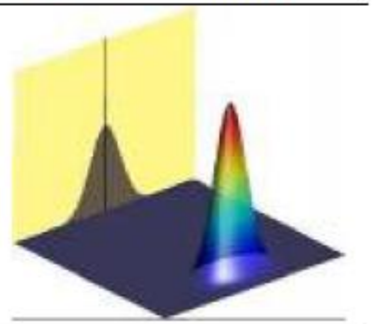
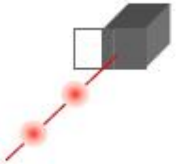
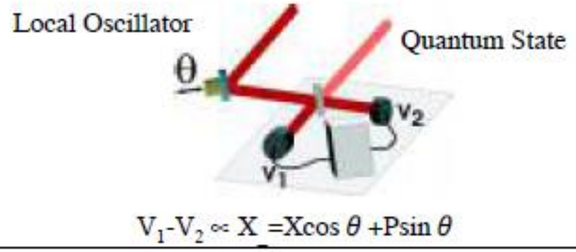
ED *et al.*, npj Quant. Info. 2016

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



| Light is : | Discrete Photons | Continuous Wave |
|---|---|---|
| We want to know : | their Number & Coherence | its Amplitude & Phase (polar)<br>its Quadratures X & P (cartesian) |
| We describe it with : | Density matrix $\rho_{n,m}$  | Wigner function W(X,P)  |
| We measure it by : | Counting: APD, VLPC, TES…  | Demodulating : Homodyne Detection  |
| « Simple » States | Fock States | Gaussian States |

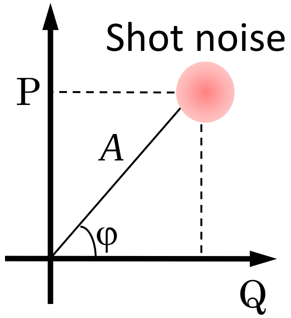
BB84, Decoy state, COW, DPS, MDI

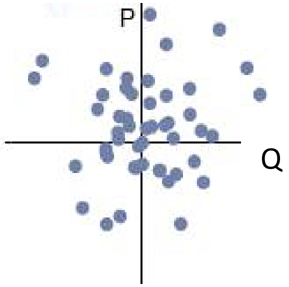
One or two-way, Gaussian or discrete modulation, coherent or squeezed states, post selection, MDI

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 continuous-variable QKD



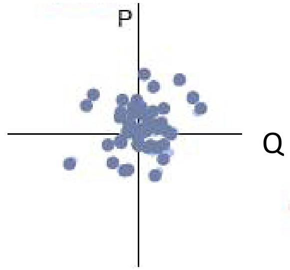



Gaussian, QPSK, QAM,…

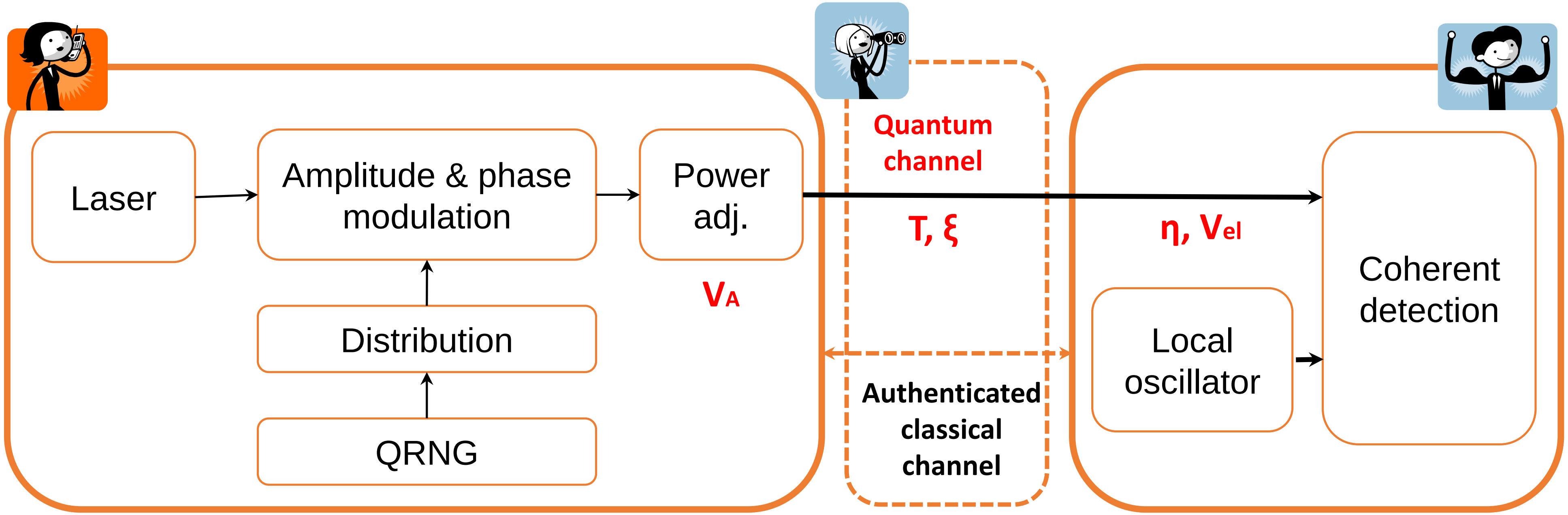
$$\{q_i \;\; p_i, 1 \leq i \leq N\}$$

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




Single (homodyne) or double (heterodyne) quadrature detection

Trusted (calibrated) noise




Composable, finite size security proof for Gaussian modulation

Adapted to arbitrary discrete constellations at asymptotic limit

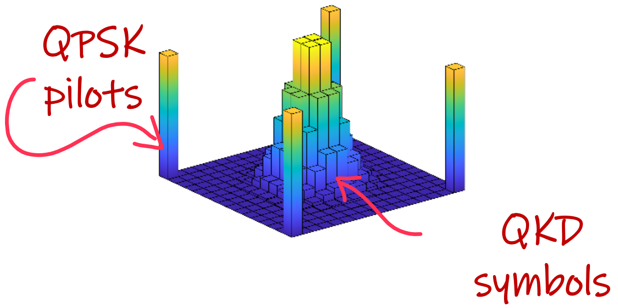
A. Leverrier, Phys. Rev. Lett. 2015, 2017

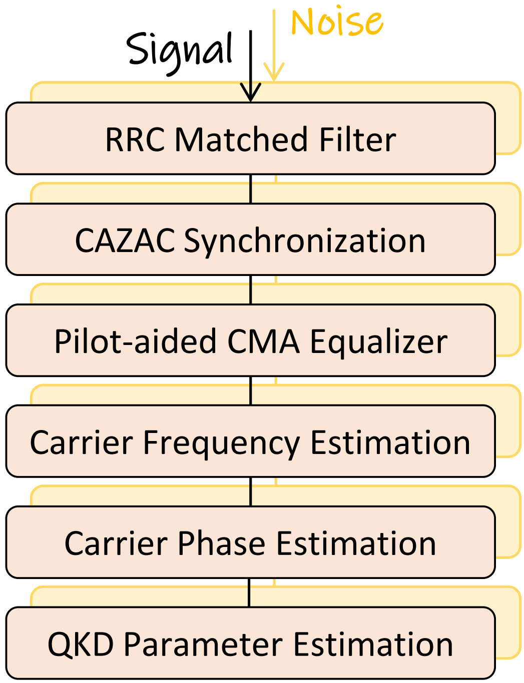
A. Denys *et al.*, Quantum 2021

# High-rate network-integrated QKD

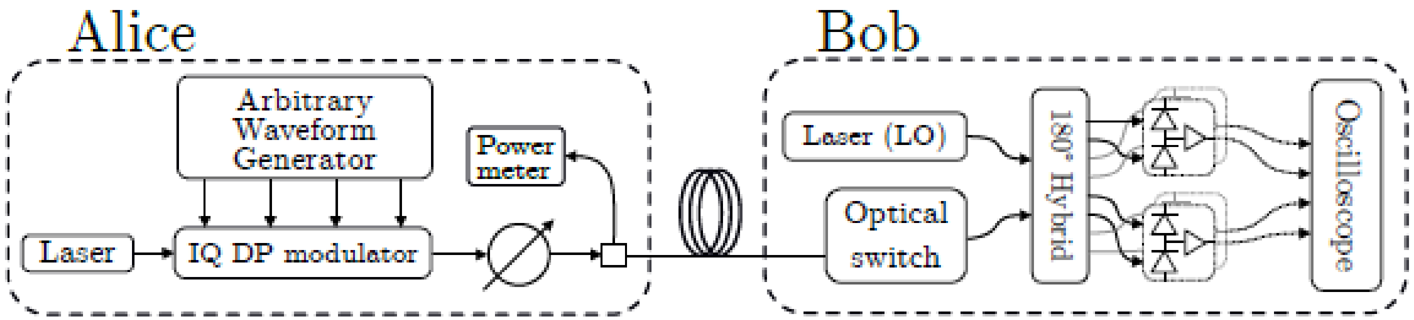


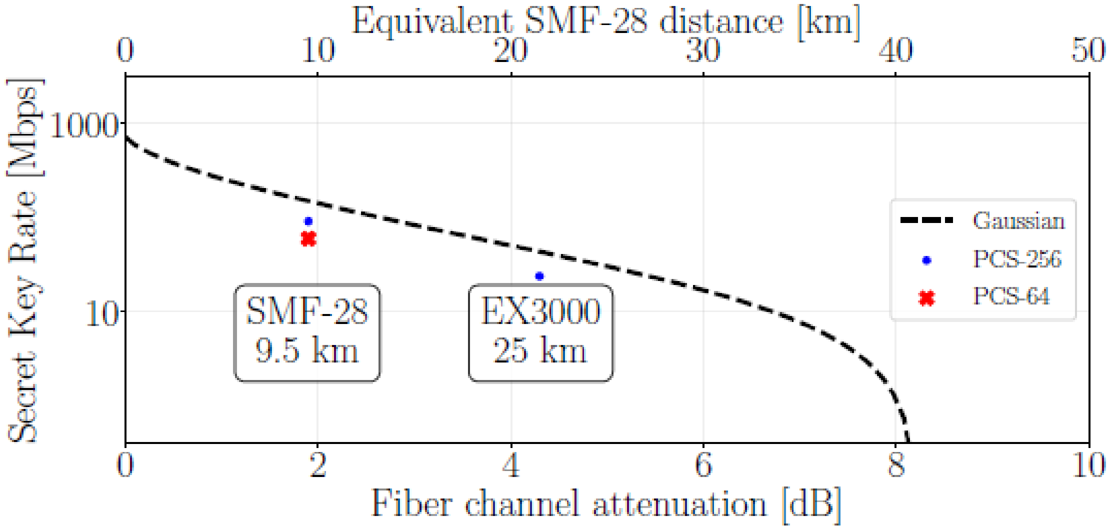
Compatibility with technology and digital signal processing techniques used in coherent telecom systems




Probabilistic constellation shaped 64 and 256-QAM, dual pol., Nyquist pulses, 50% QPSK pilots, 400 Mbaud, 10 kHz linewidth




With 256-QAM, secret key rate

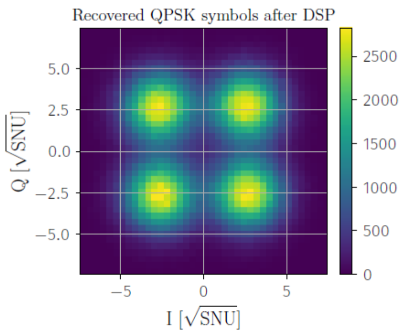
92 Mbit/s @ 9.5 km
24 Mbit/s @ 25 km

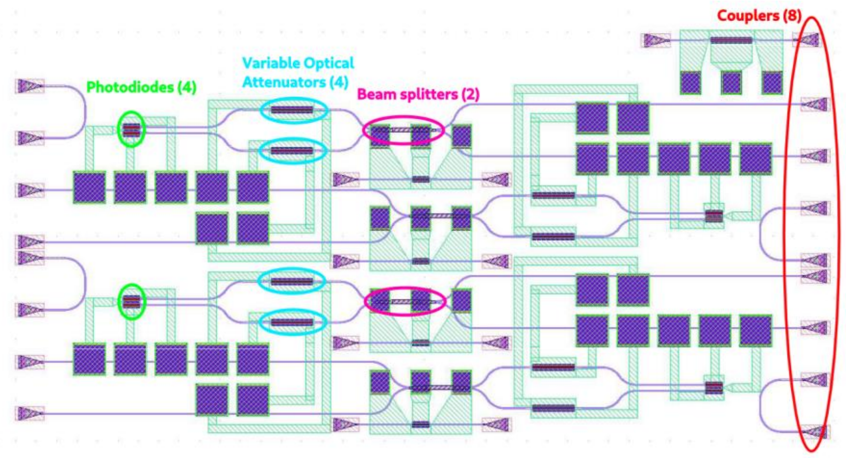
F. Roumestan *et al.*, OFC & ECOC 2021, 2022, arXiv 2207.11702

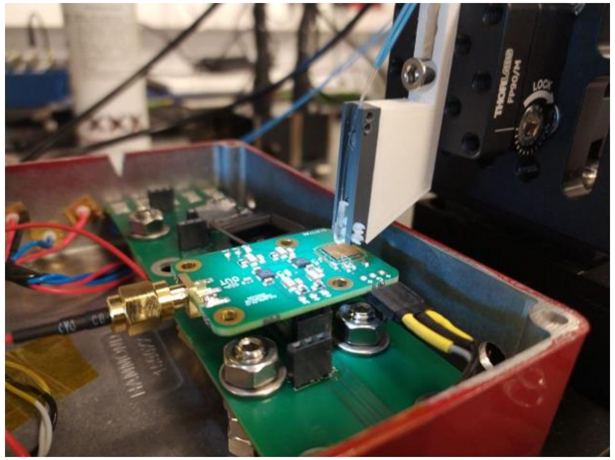
NOKIA Bell Labs

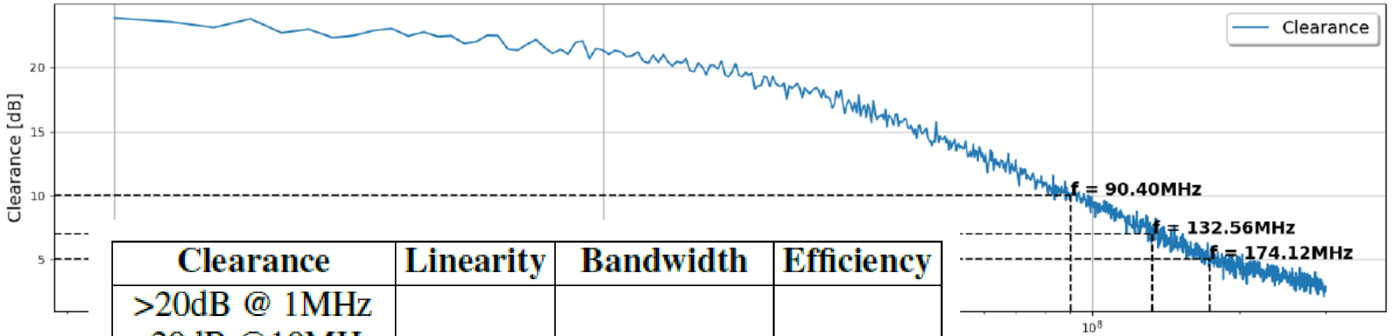
# Photonic-integrated QKD

Si receiver photonic chips from C2N and CEA-LETI
InP transmitter chips from HHI-Fraunhofer

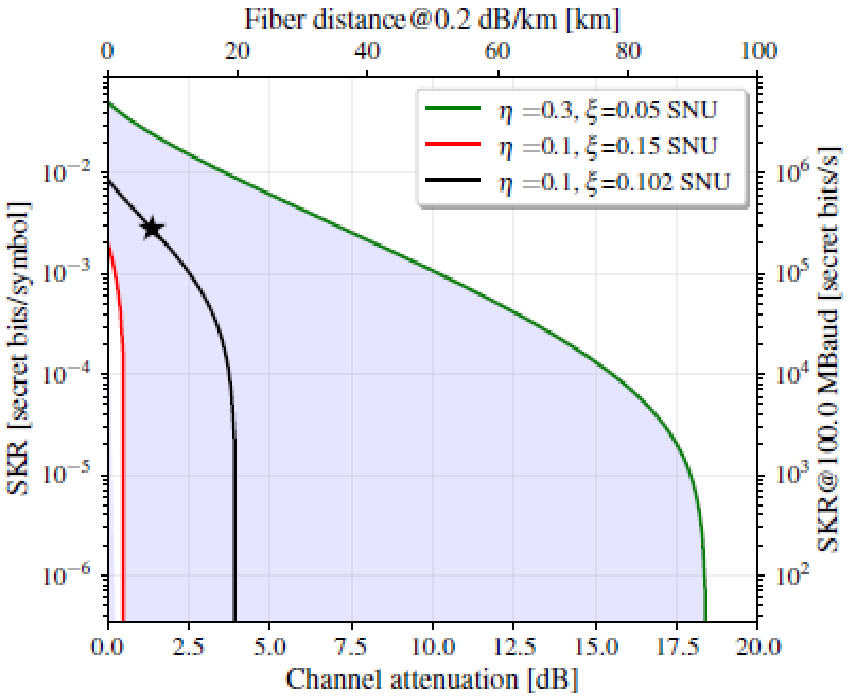





| Clearance | Linearity | Bandwidth | Efficiency |
|---|---|---|---|
| >20dB @ 1MHz<br>>20dB @10MHz<br>>10dB @100MHz<br>>5dB @200MHz | 97-99 % | 200-250 MHz | 18-28 % |



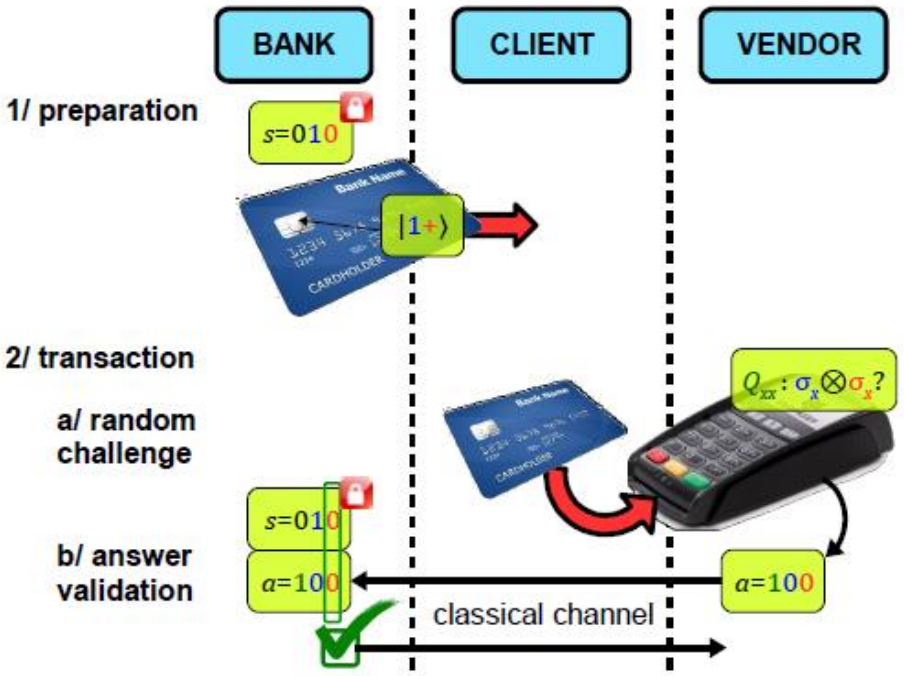

Si-PIC CV-QKD receiver platform

Y. Piétri *et al.*, OFC 2023

# Quantum advantage for advanced protocols



Key distribution is central primitive in the trusted two-party security model
In other configurations many more functionalities



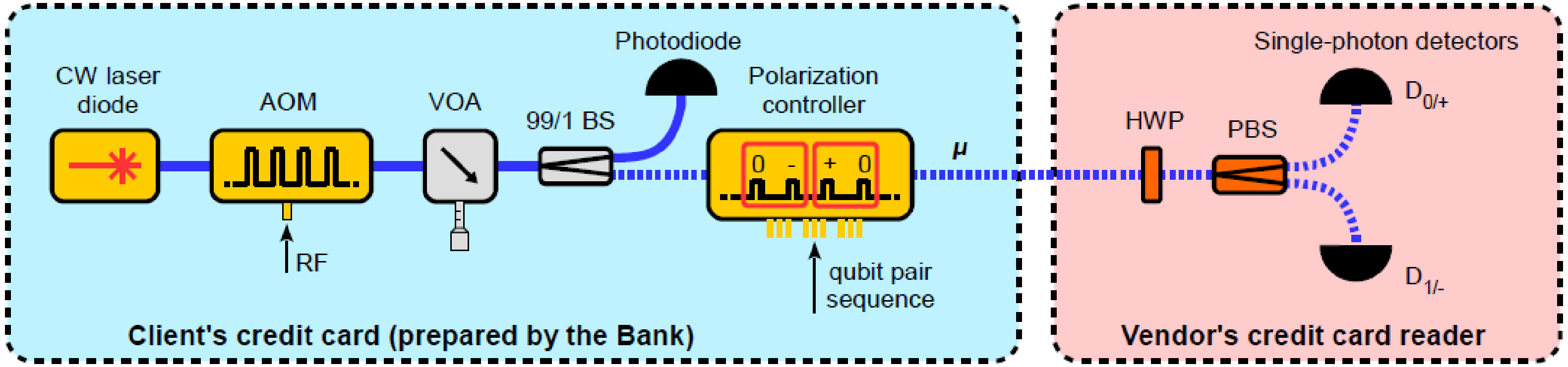

Unforgeable quantum money

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

But needs quantum verification and is not robust to imperfections
Was considered impossible to implement

New protocol with classical verification and 'BB84' states
Based on challenge questions

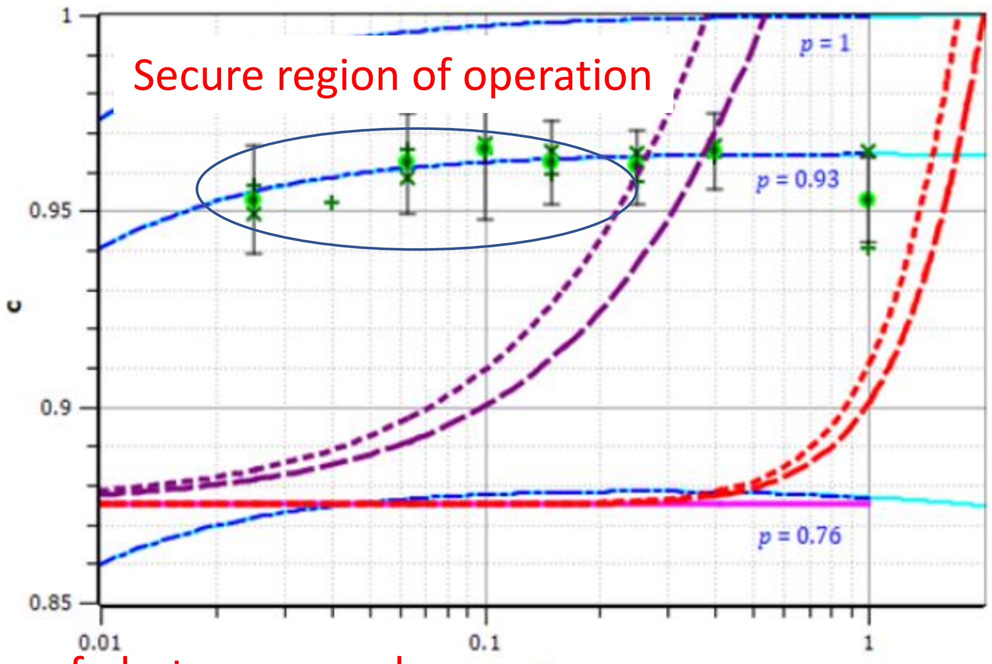
$$S_{pair} = \{|0,+\rangle, |0,-\rangle, |1,+\rangle, |1,-\rangle, |+,0\rangle, |+,1\rangle, |-,0\rangle, |-,1\rangle\}$$



# Unforgeable quantum money



Probability of answering the bank's challenge correctly →




Average number of photons per pulse →

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

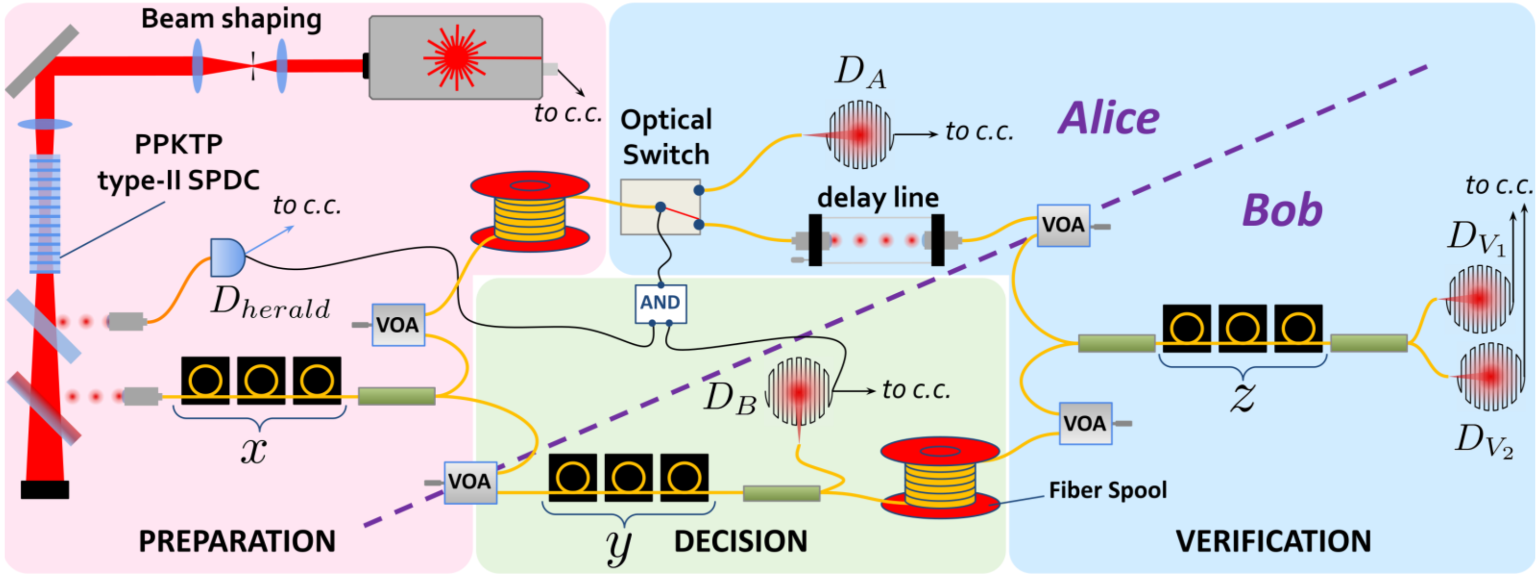
M. Bozzio *et al.*, npj Quant. Info. 2018 & Phys. Rev. A 2019; H. Mamann *et al.*, in prep. (with quantum storage)

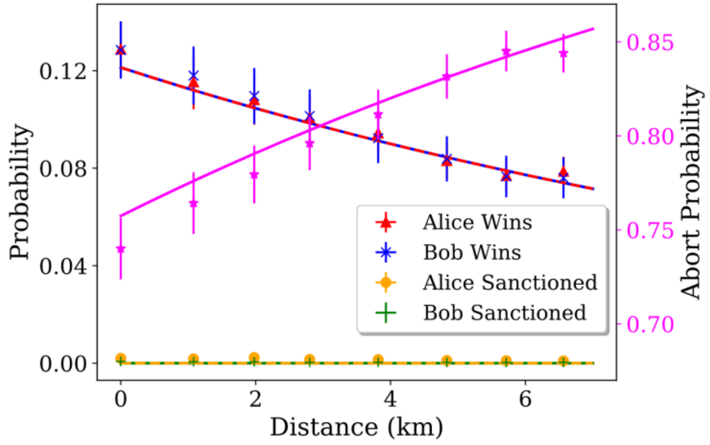
# Quantum weak coin flipping

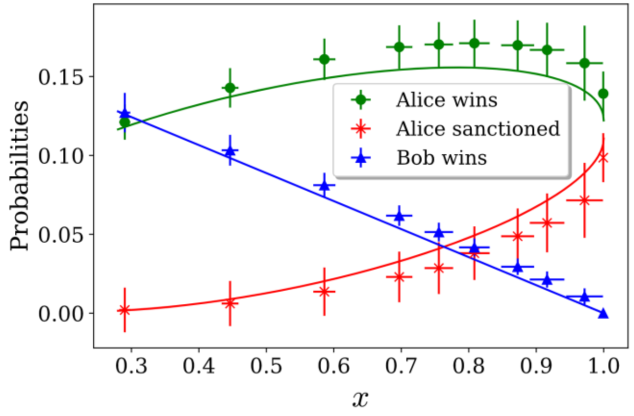
Allows two distrustful parties to agree on a random bit, whose value should not be biased

Classical → computational assumptions, quantum → information-theoretic security but fundamental lower bound on bias

In principle arbitrarily close to zero for weak protocol, where Alice and Bob have a preferred outcome




Photon number entanglement with heralded single photons, conditional verification step

Quantum advantage in the form of cheat sensitivity maintained over a few kilometres

S. Neves *et al.*, Nature Commun. 2023

# Multipartite entanglement verification and applications



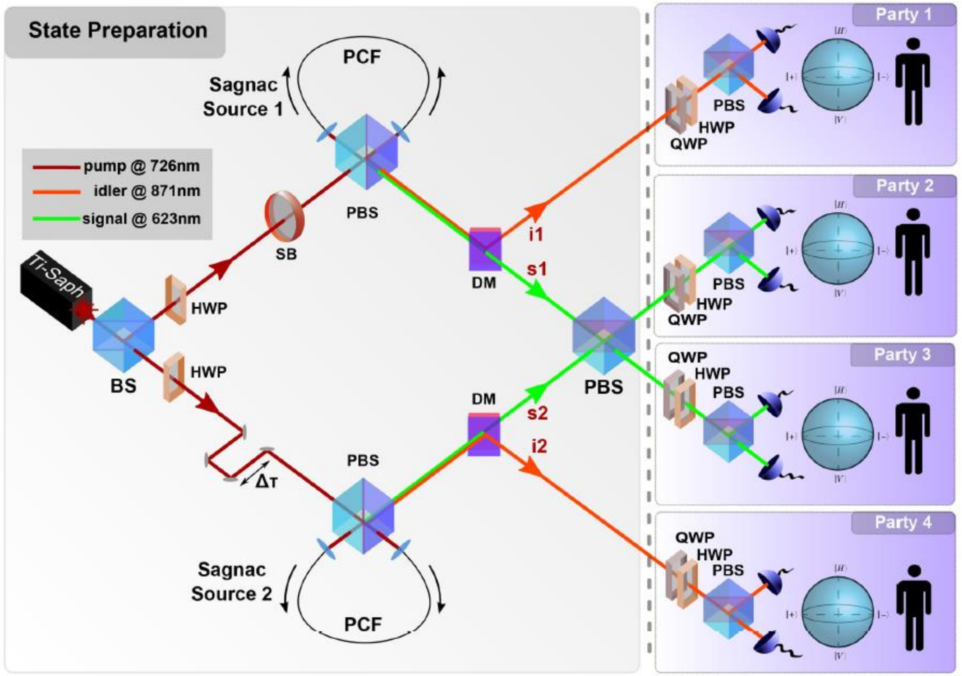
Proof-of-principle verification of multipartite entanglement in the presence of dishonest parties

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

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle|0\rangle + |1\rangle|1\rangle|1\rangle)$$

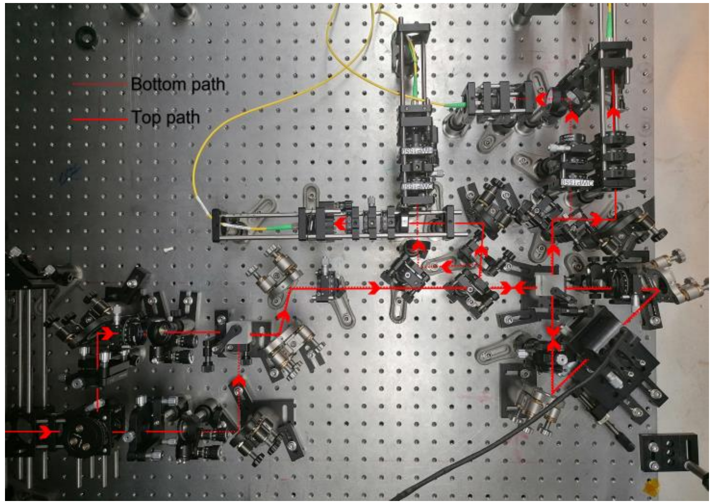
Requires very high performance resources

Limited loss tolerance




Application to anonymous message transmission and electronic voting

Verification phase guarantees anonymity and privacy

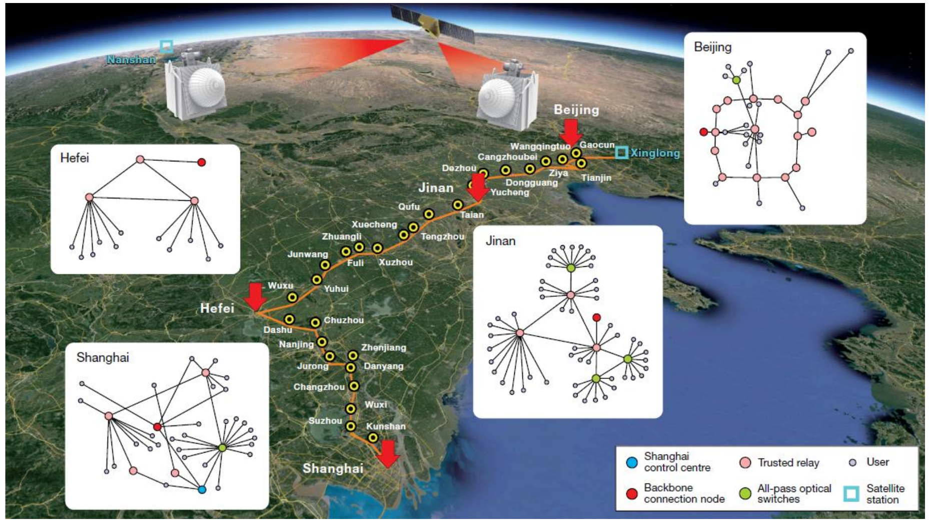



A. Unnikrishnan *et al.*, Phys. Rev. Lett. 2019
F. Centrone *et al.*, Phys. Rev. Applied 2022

# Long-distance networks

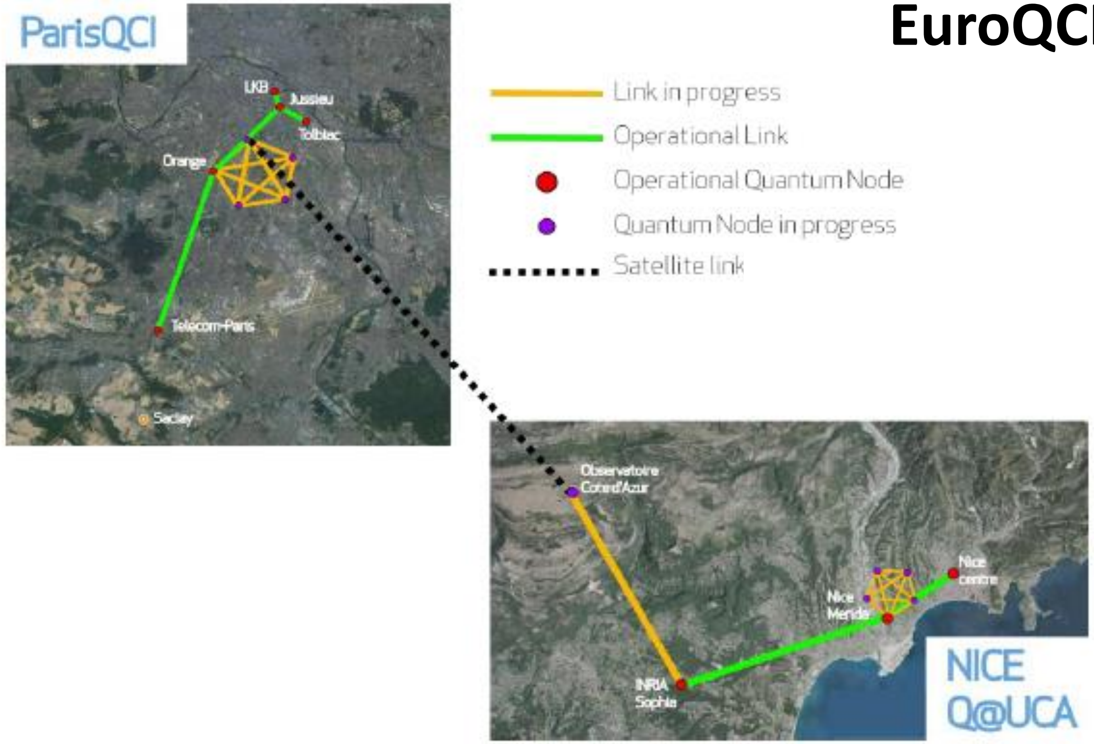
To counter inherent range limitation due to optical fiber loss → terrestrial and satellite-based networks

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




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

## EuroQCI




Trusted node networks

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

For end-to-end security, routing of entanglement with quantum repeaters and memories

Data centre storage and interconnection, protection and resilience of critical infrastructures, governmental communications, finance, telecom operators, medical file transfer

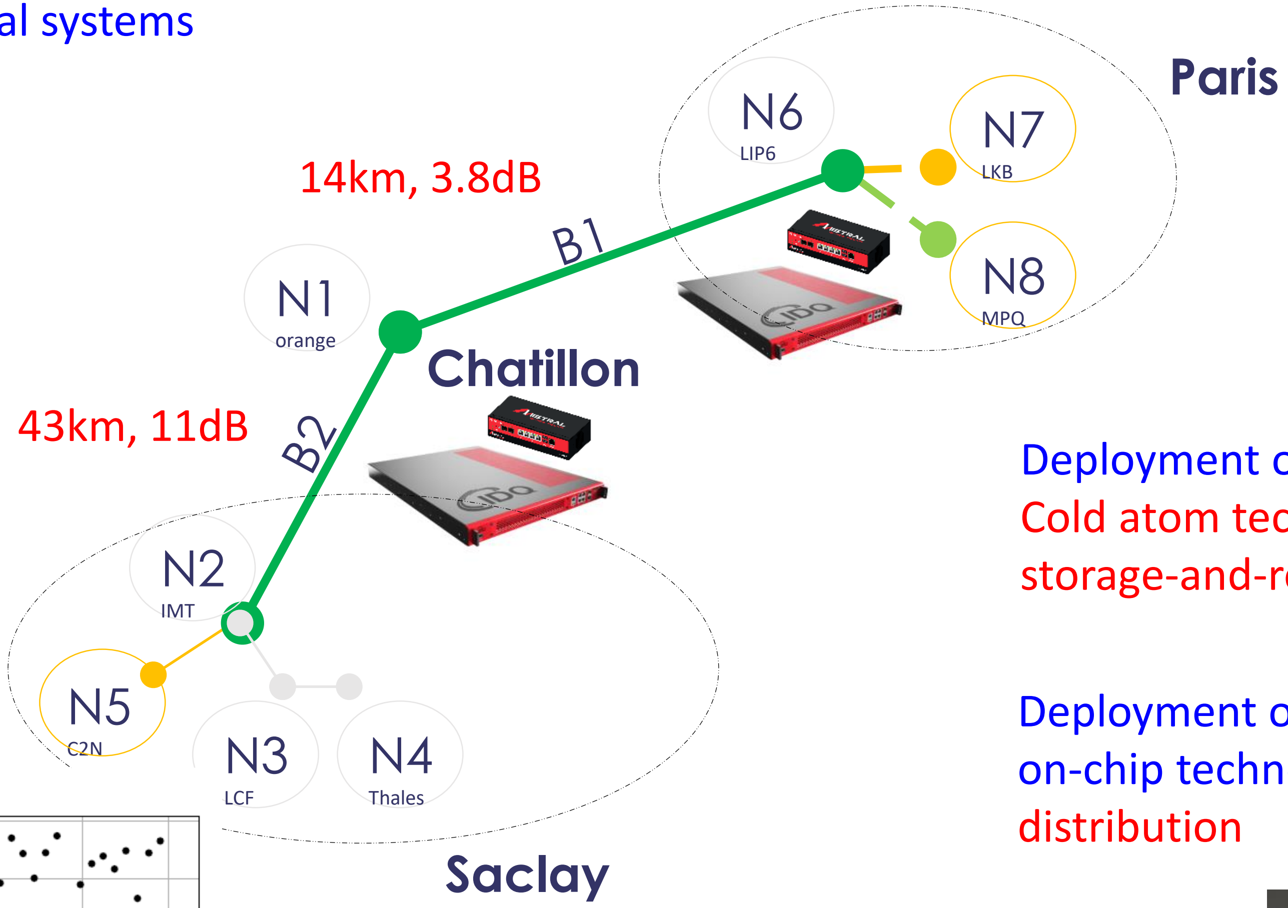
# Paris testbed deployment

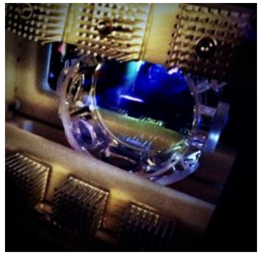


Benchmarking with commercial systems

IDQ XGR QKD systems

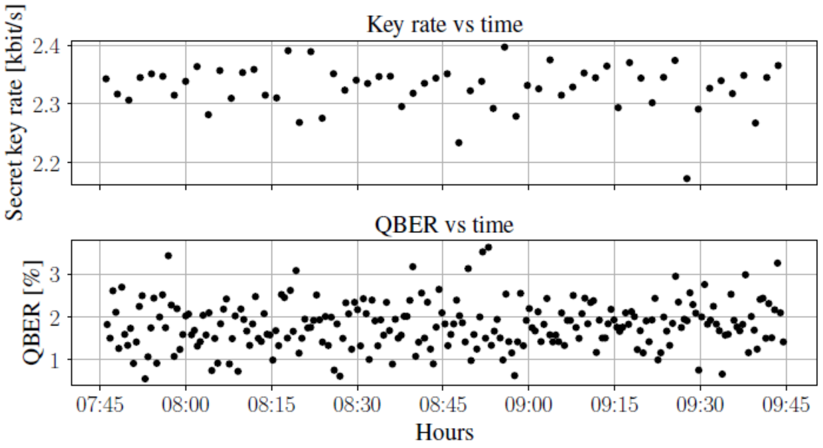
Thales Mistral encryptors



Deployment of quantum memory-based link

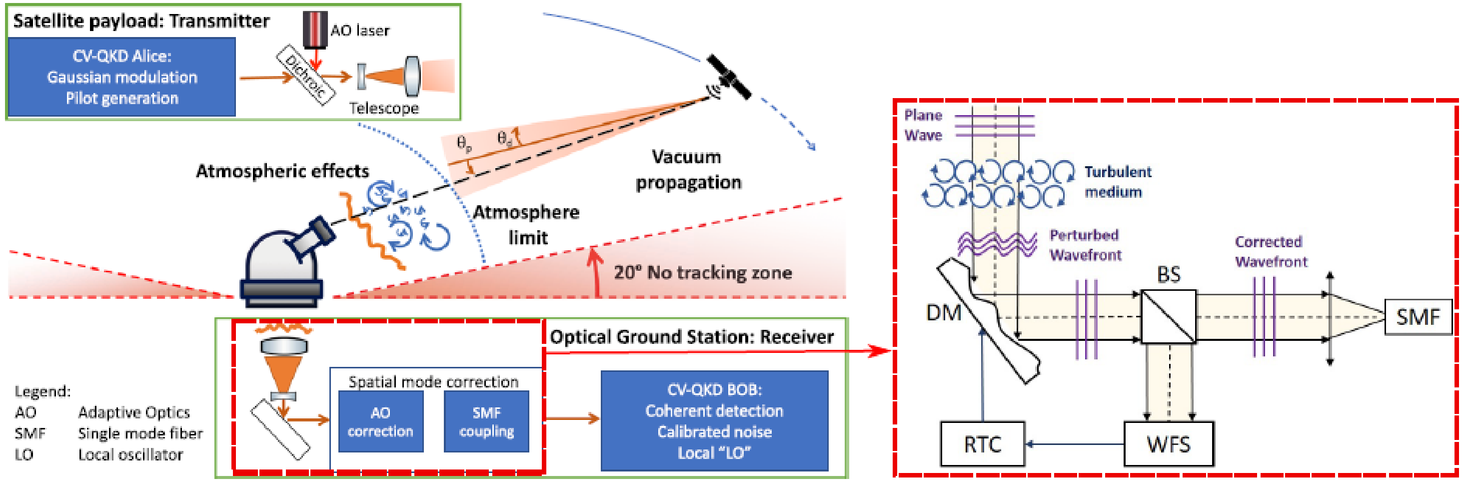
Cold atom technology with record high storage-and-retrieval efficiency



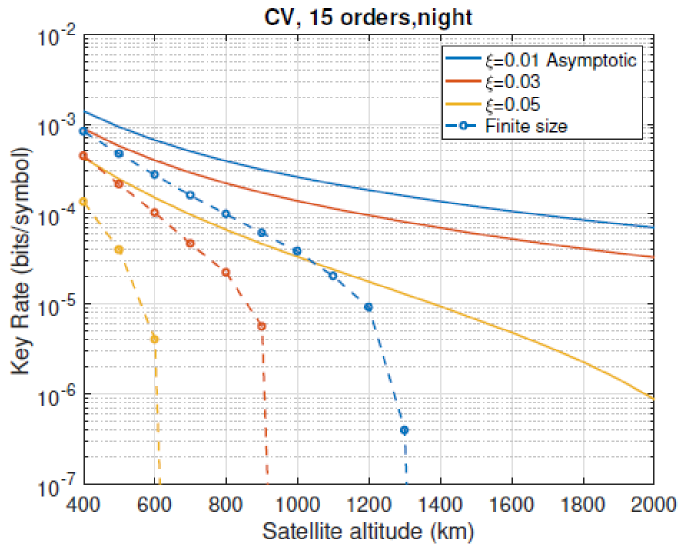

Deployment of CV-QKD integrating system-on-chip technology and of entanglement distribution

# Feasibility studies for space-based quantum networks

They alleviate the need for long chains of trusted nodes or quantum repeaters
They serve more use cases: remote, isolated or inaccessible locations
Terrestrial and space networks work together and can be fallback options




Downlink channel with turbulence
Probability distribution of transmission efficiency
Payload characteristics of Micius:
pointing error 1 μrad, divergence angle 10 μrad
Ground station characteristics of Matera Laser Ranging Observatory: telescope diameter 1.5 m



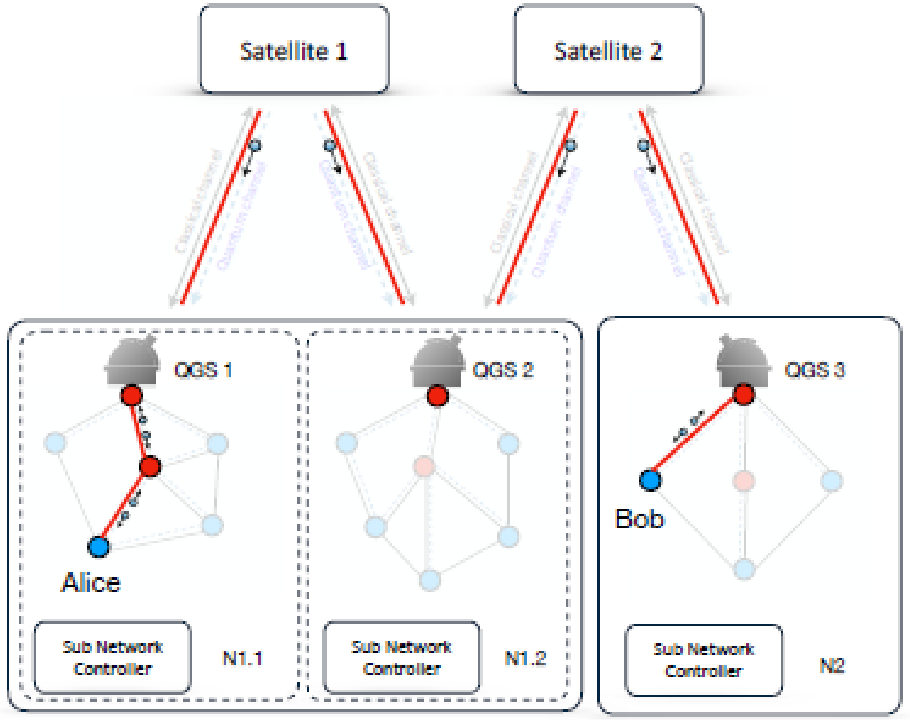

Security analysis for a fluctuating channel → fading introduces additional noise
Trade-off between binning of data to reduce variance and finite-size effects

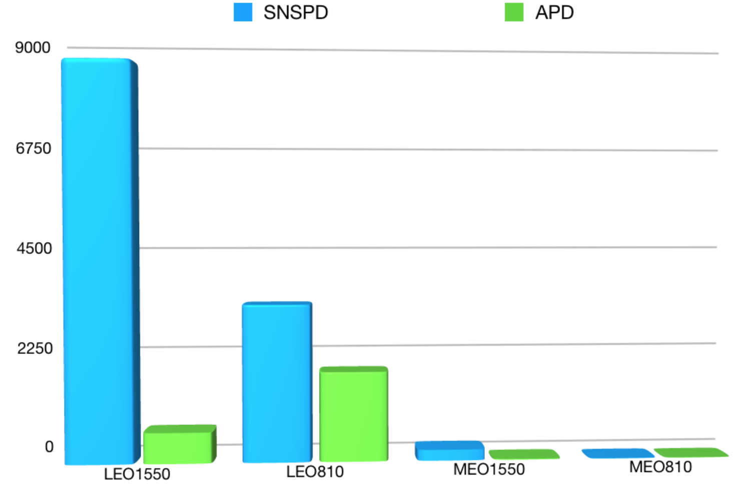
Refined analysis of fibre coupling with adaptive optic system → correcting up to 15 orders optimal for both CV and DV-QKD, for LEO at almost all conditions

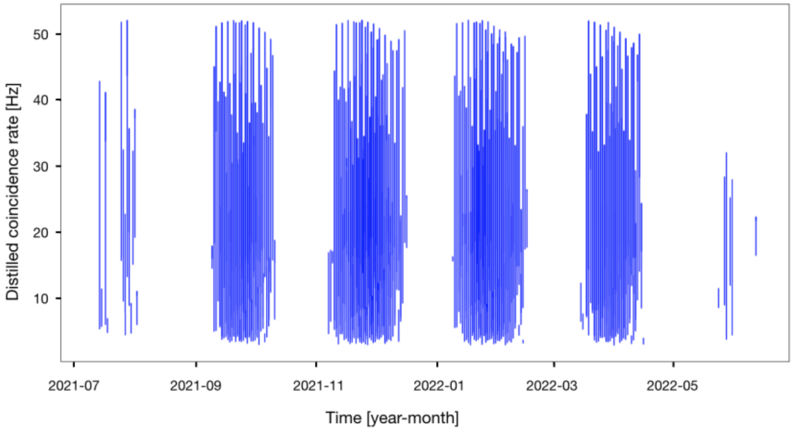
D. Dequal *et al.*, npj Quant. Info. 2021
V. Marulanda Acosta *et al.*, arXiv 2111.06747

ONERA THE FRENCH AEROSPACE LAB
Agenzia Spaziale Italiana

# Feasibility studies for space-based quantum networks




Analysis of entanglement-based scenario

Trade-offs between visibility time, losses, divergence, pointing, telescope size, atmospheric turbulence, detector efficiency,…

Importance of long simulation duration

L. de Forges de Parny *et al.*, Commun. Phys. 2023

cnes CENTRE NATIONAL D'ÉTUDES SPATIALES

ThalesAlenia Space

# 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!

Y. Piétri, M. Schiavon, L. Trigo-Vidarte, D. Fruleux, A. Rhouni, F. Roumestan, A. Ghazisaeidi,
M. Huguenot, B. Gouraud, A. Leverrier, P. Grangier
V. Marulanda Acosta, C. Lim, J.-M. Conan, D. Dequal
V. Yacoub, L. Martins, S. Neves, R. Yehia, F. Centrone, P. Lefebvre, I. Supic, D. Markham, I. Kerenidis