Secure communications in quantum networks

Eleni Diamanti

LIP6, CNRS, Sorbonne Université

Paris Centre for Quantum Technologies

YQIS, Paris, France

6-8 November 2024

Quantum communication

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

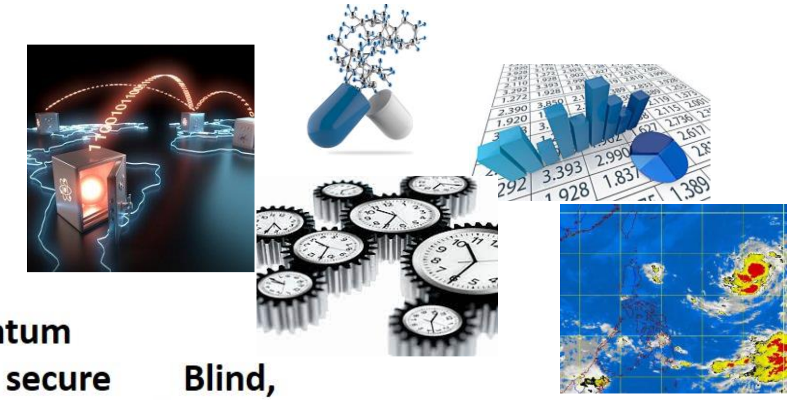
Encoding on properties of quantum states of light
Propagation in optical fibre or free-space channels
Information processing in network nodes (processors, sensors, memories)

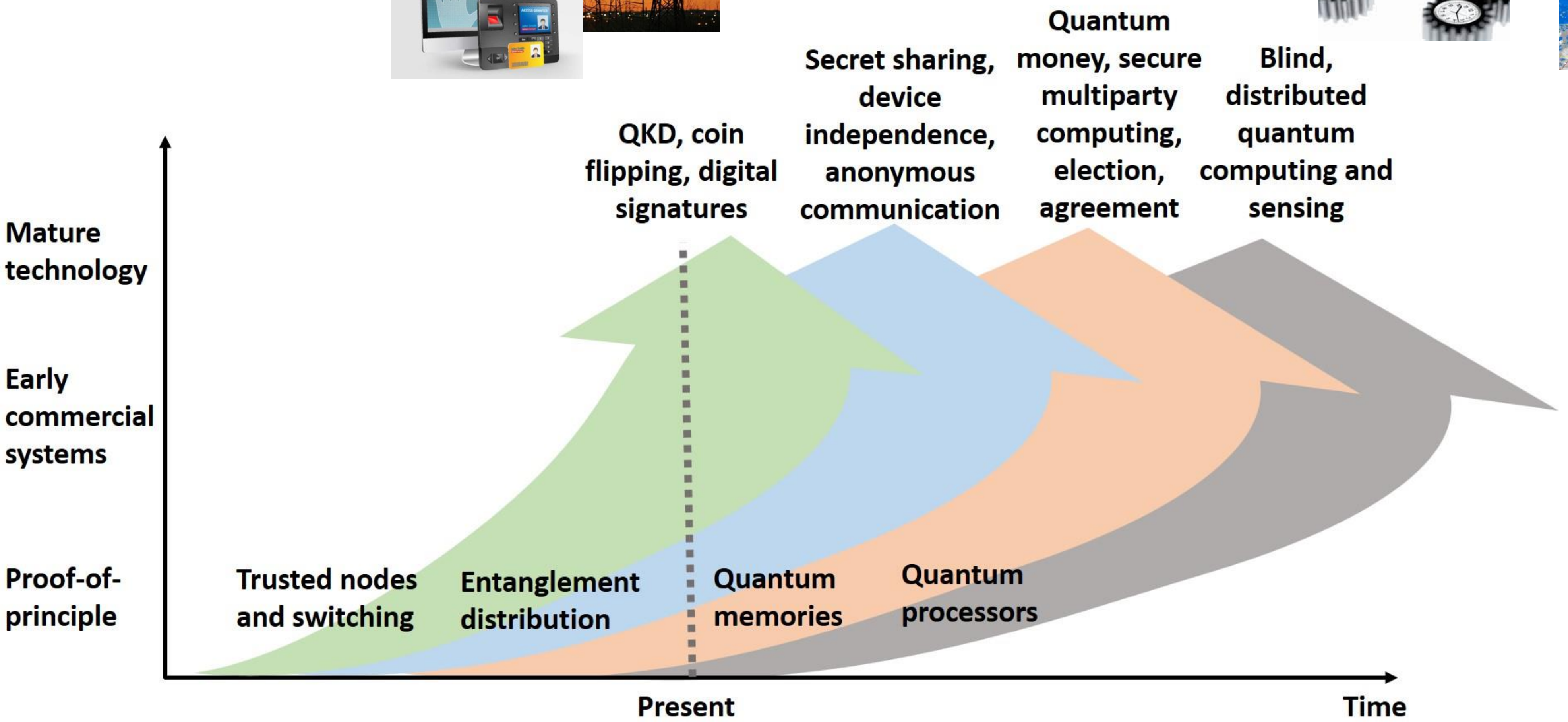
Security
Untrusted network users, devices, nodes

Efficiency
Optimal use of communication resources

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

Quantum network stages and applications



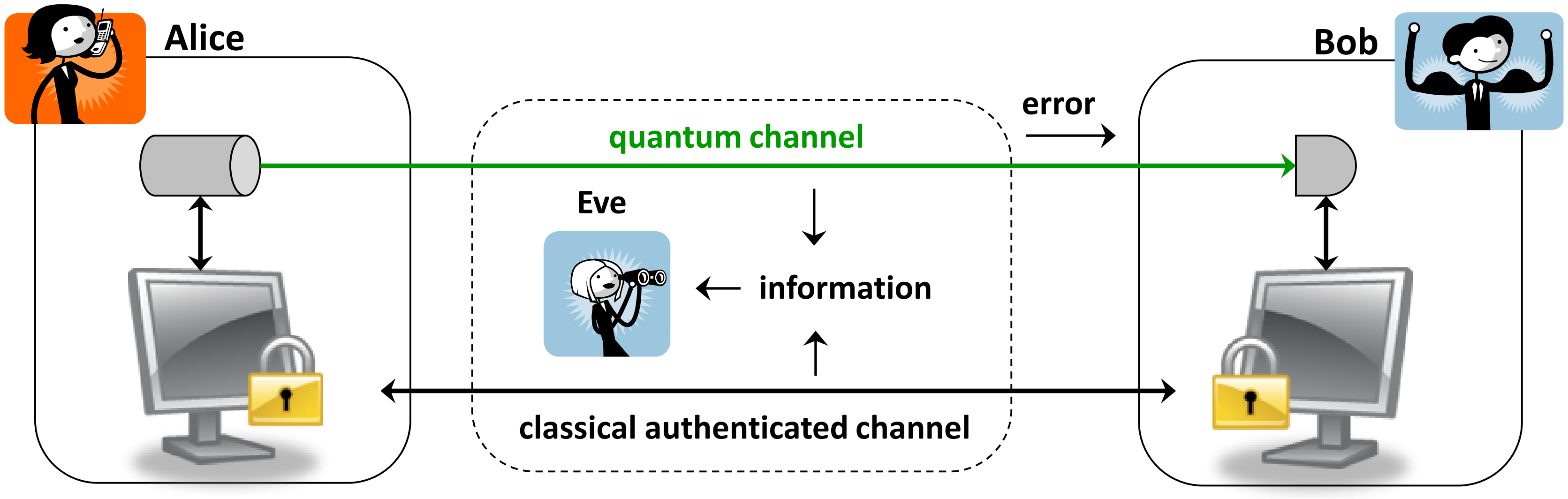


E. Agrell *et al.*, *Roadmap on Optical Communications*, J. Opt. 26, 093001 (2024)

Securing network links: quantum key distribution

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

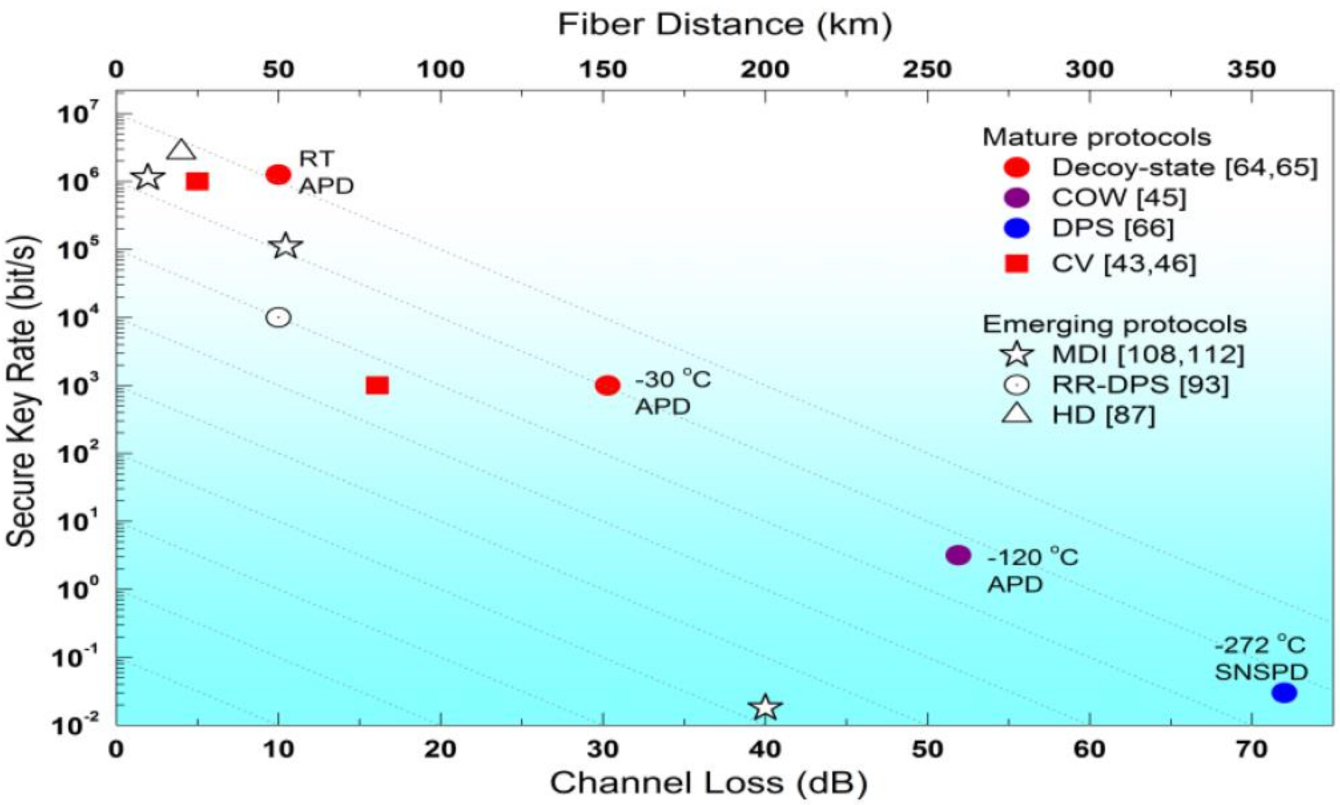
Quantum key distribution allows for exchange of sensitive data between two trusted parties with information-theoretic, long-term security guaranteed against an all-powerful eavesdropper



Hybrid QKD and computational (post-quantum) schemes offer defense-in-depth

Authentication e.g. with pre-shared keys, post-quantum or ITS digital signatures	**Key agreement** e.g. with post-quantum or **QKD** (ITS) replacing vulnerable asymmetric algorithms	**Message encryption** e.g. with AES or one-time pad (ITS)

QKD in practice



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

ED *et al.*, npj Quantum Information 2016

Fundamental limits in rate and range
Quantum signals cannot be amplified without noise

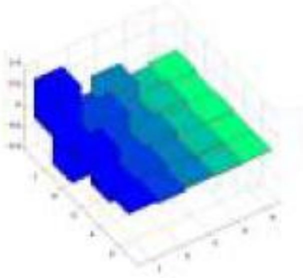
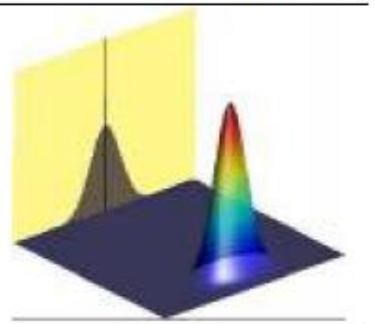
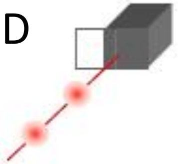
Security definition: $\frac{1}{2}\left\|\rho_{S_A S_B E} - \tau_{SS} \otimes \rho_E\right\|_1 \leq \varepsilon$ for any $\rho_{A^n B^n E}$

Device independence: If Alice and Bob share nonlocal correlations less assumptions on devices

Practical security: Deviations from security proof lead to side-channel attacks

BSI report: *Implementation attacks against QKD systems*, November 2023

Discrete and continuous variable encoding

<table>
<tr><td>Light is :</td><td>Discrete Photons</td><td>Continuous Wave</td></tr>
<tr><td>We want to know :</td><td>their Number
& Coherence</td><td>its Amplitude & Phase (polar)
its Quadratures X & P (cartesian)</td></tr>
<tr><td>We describe it with :</td><td>Density matrix $\rho_{n,m}$
</td><td>Wigner function W(X,P)
</td></tr>
<tr><td>We measure it by :</td><td>Counting:
APD, VLPC, TES…
SNSPD
</td><td>Demodulating : Homodyne Detection

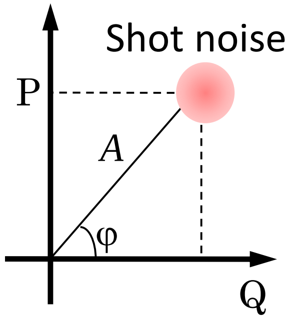

V_1-$V_2 \propto X_\theta = X\cos\theta + P\sin\theta$</td></tr>
<tr><td>« Simple » States</td><td>Fock States</td><td>Gaussian States</td></tr>
</table>

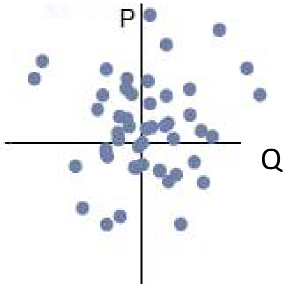
BB84, Decoy state, COW, DPS, MDI

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

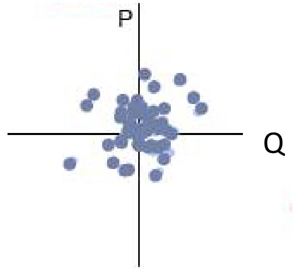




$$\{q_i \quad p_i, 1 \leq i \leq N\}$$

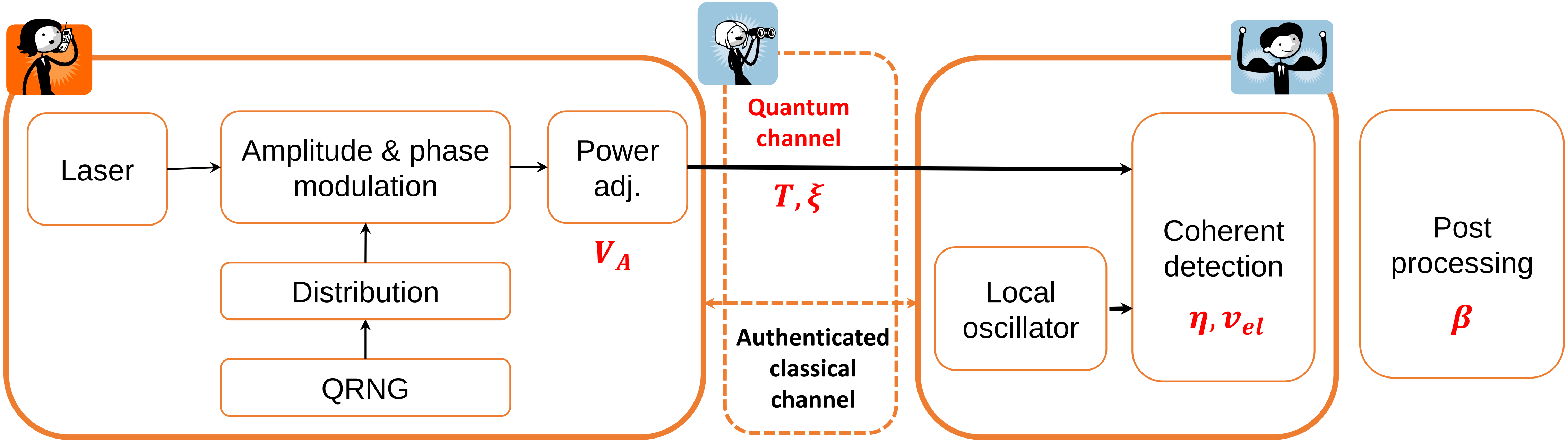
$$|\alpha\rangle_i = |q_i + ip_i\rangle$$

Gaussian, QPSK, QAM,…



Single (homodyne) or double (heterodyne) quadrature detection

Trusted (calibrated) noise

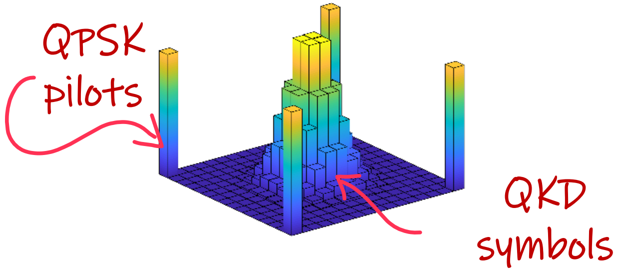


Alice and Bob perform noise variance measurements to bound the Holevo information of Eve:

$$K \; = \beta I_{AB}(V_A, T, \xi, \eta, v_{el}) - \chi_{BE}(V_A, T, \xi, \eta, v_{el})$$

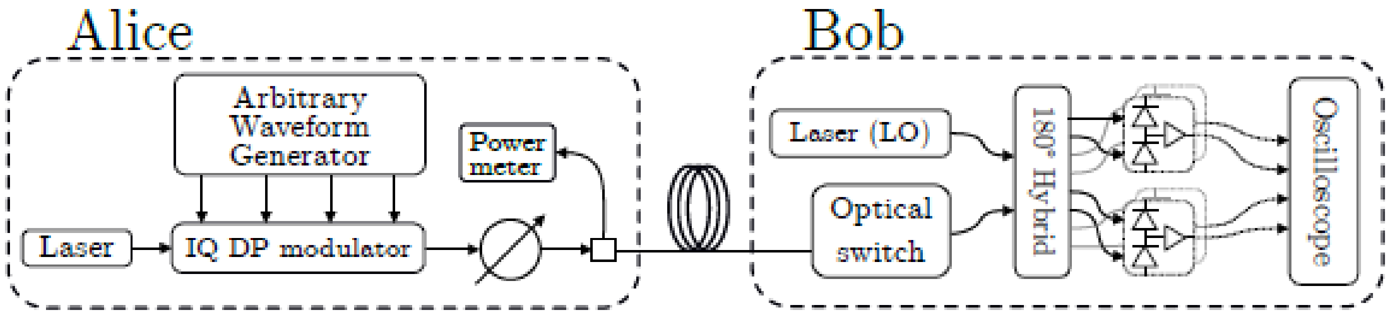
High-rate network-integrated CV-QKD

Leverage compatibility with technology and digital signal processing (DSP) techniques used in coherent telecom systems



64 and 256 probabilistically constellation shaped (PCS) QAM, dual pol., Nyquist pulses, time-multiplexed pilots, 400 Mbaud

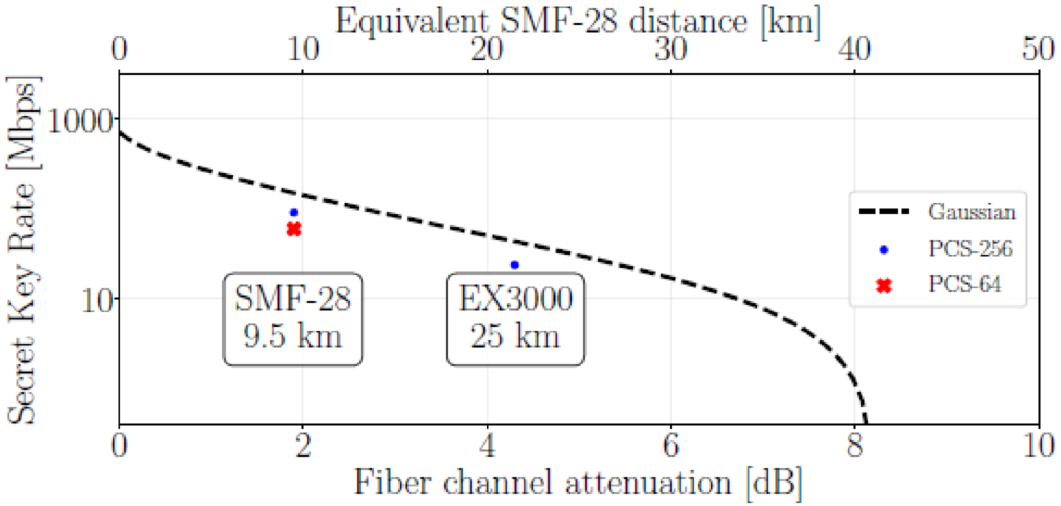
Security proof for arbitrary constellations with worst-case estimators



With 256-QAM, secret key rate

92 Mbit/s @ 10 km
24 Mbit/s @ 25 km

NOKIA Bell Labs



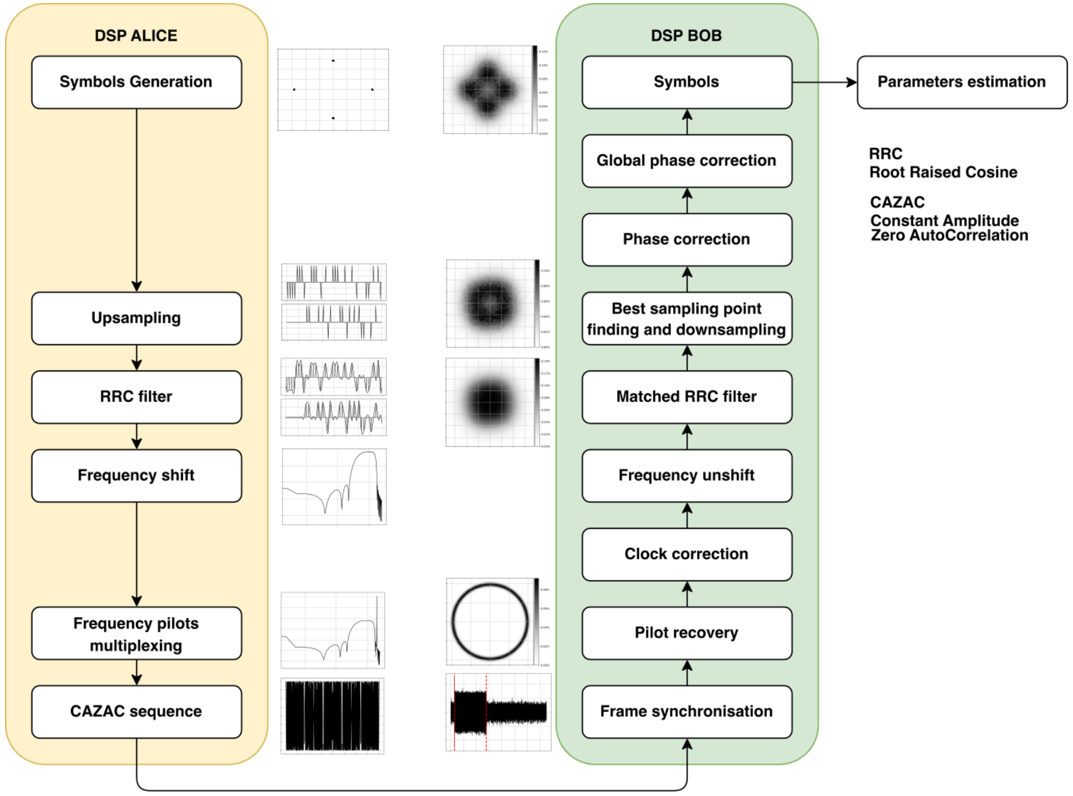
F. Roumestan *et al*., *Shaped constellation CV-QKD: concepts, methods and experimental validation*, J. Lightwave Technol. 2024

QOSST: an open-source modular software for CV-QKD

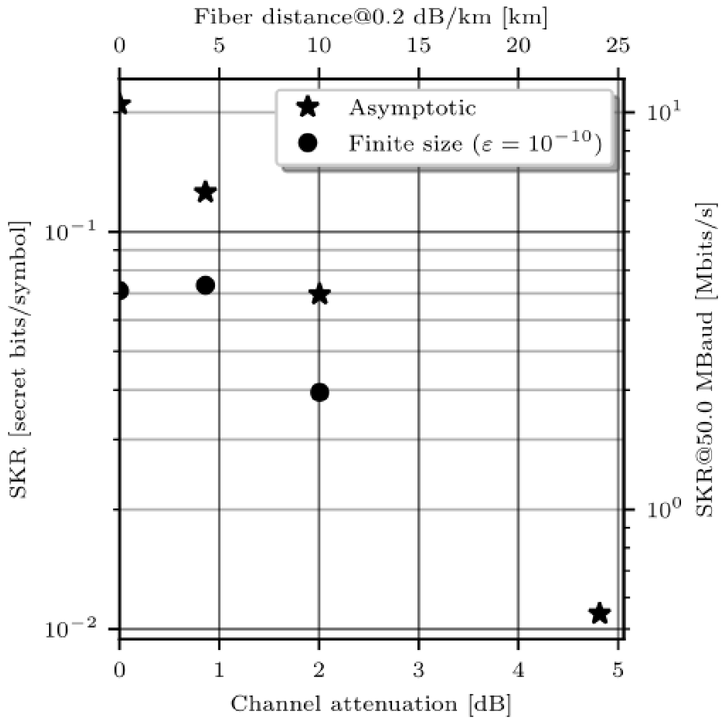
Full Python open-source software suite called QOSST (Quantum Open Software for Secure Transmissions)

Operates with built-in optimization over more than 10 DSP parameters, and calibration of Tx and Rx

DSP includes pulse shaping, synchronization, phase and frequency recovery steps

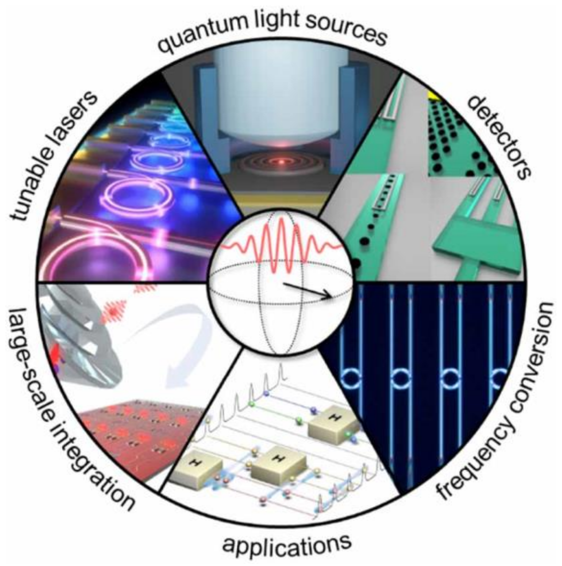


Benchmarked with setup using frequency multiplexed pilots, Gaussian modulation, 100 Mbaud, RF heterodyne detection



Y. Piétri *et al.*, *QOSST: A highly modular open-source platform for experimental CV-QKD*, arXiv:2404.18637

Photonic integration



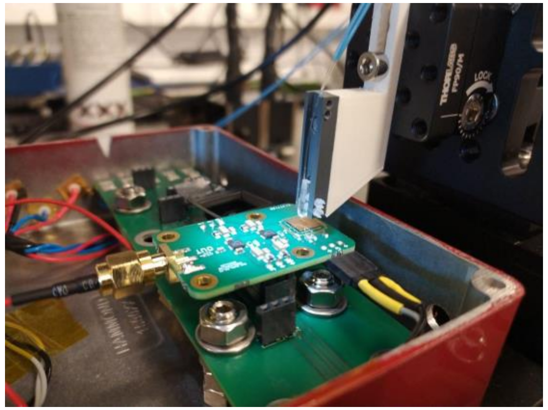
Photonic integration offers scalability, reproducibility, interconnectivity, reliability, reduced cost and physical footprint

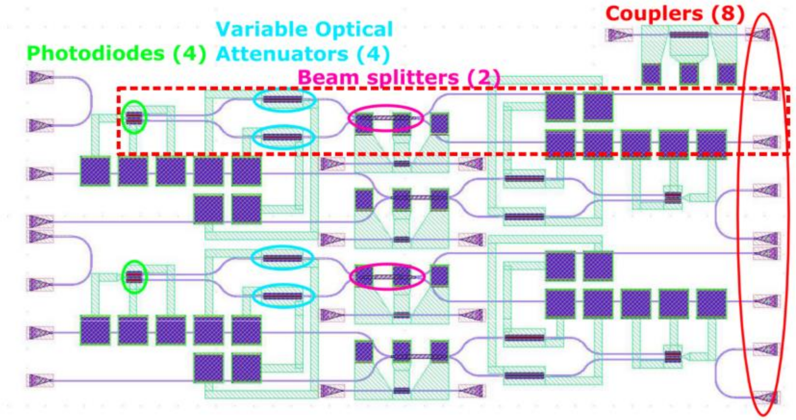
G. Moody *et al.*, *2022 Roadmap on Integrated Quantum Photonics*
J. Phys. Photon. 4, 012501 (2022)

CV-QKD well suited for PIC-based systems

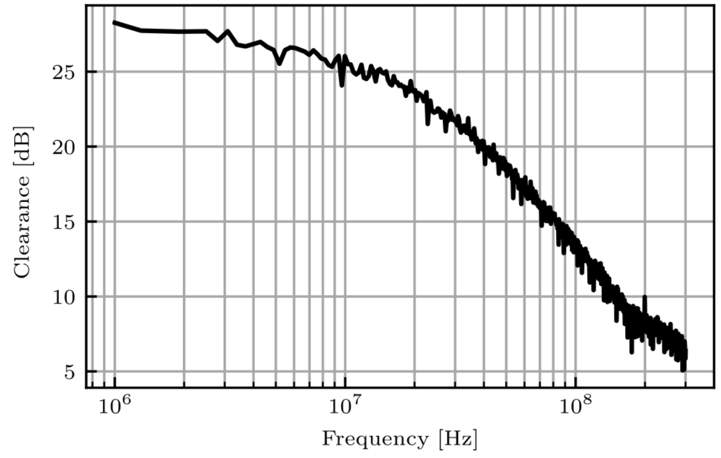
Si receiver chips designed with **CNRS/C2N** and fabricated by **CEA-LETI** on a SiGe process

Low transmission losses, high fibre-to-chip coupling efficiency, mature microfabrication techniques (but laser integration challenging)





Characterization and performance

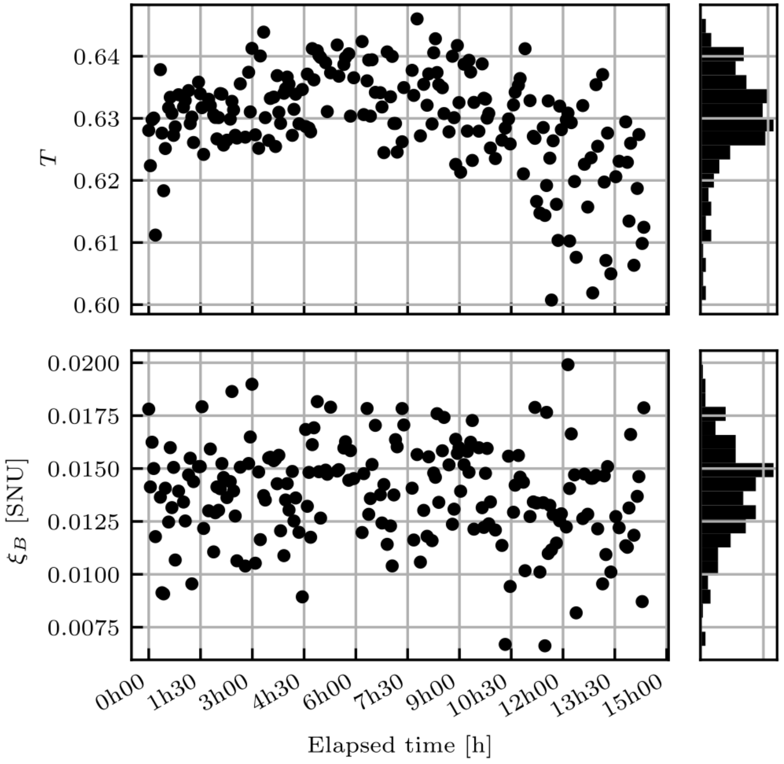


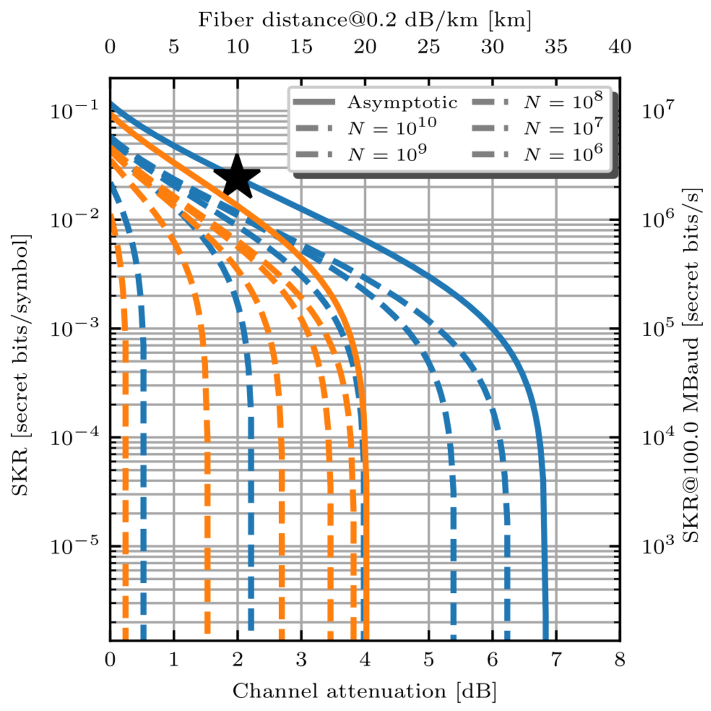
14 dB clearance @ 100 MHz, excellent linearity, $\eta \sim 16 - 17\%$

Benchmarked with QOSST

Asymptotic secret key rate with Gaussian modulation
2.4 Mbit/s @ 10 km, 220 kbit/s @ 23 km

Y. Piétri *et al.*, *Experimental demonstration of CV-QKD with a silicon photonics integrated receiver*, arXiv:2311.03978, to appear in Optica Quantum





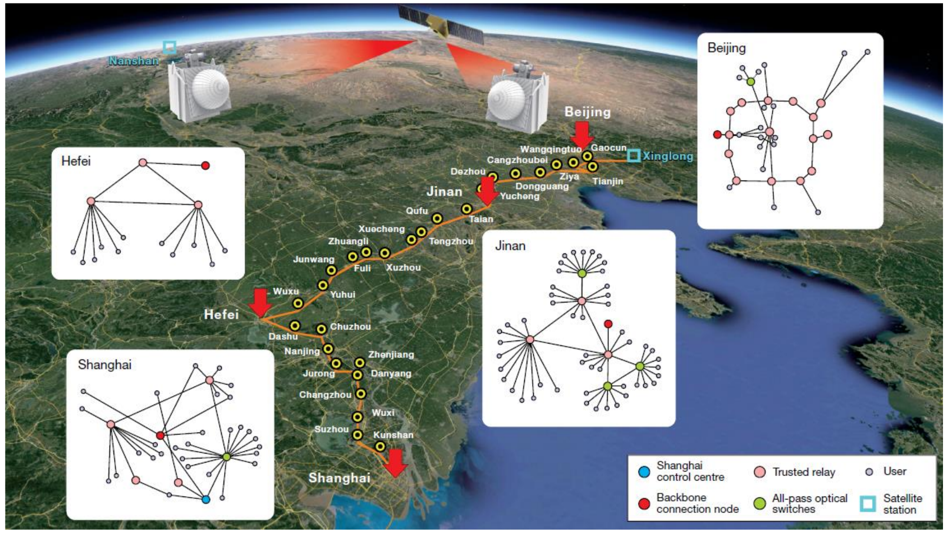
Next step: full integration

InP-PIC CV-QKD Tx, with **ICFO** and **HHI**
J. Aldama *et al.*, OFC 2023

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



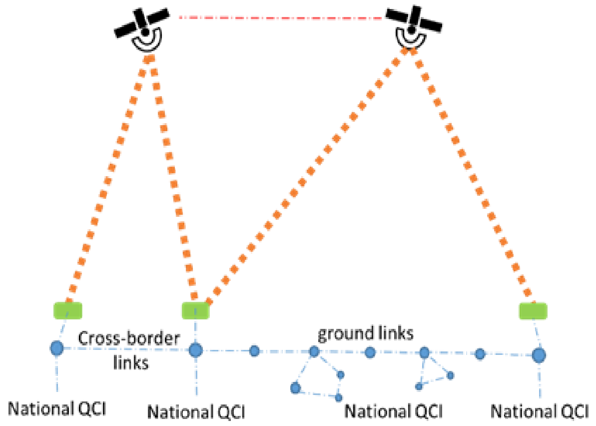
Y.-A. Chen *et al.*, Nature 2021

Mesh type networks with point-to-point links with trusted nodes

SECOQC QKD network, 2008
Swiss Quantum Network, 2011
Tokyo QKD network, 2015

China integrated terrestrial-satellite network
South Korea governmental network
Singapore NQSN+ network

EuroQCI



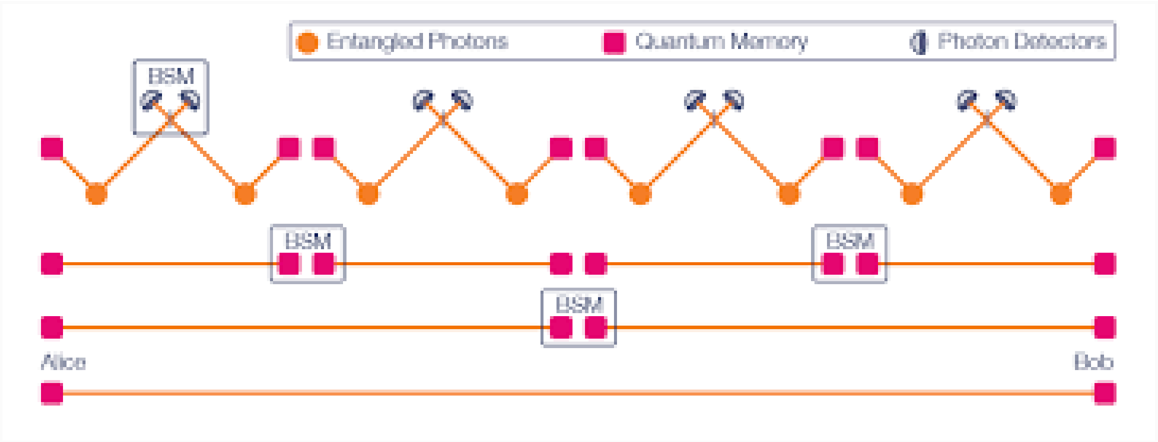
If the distance between Alice and Bob exceeds the range of the system:

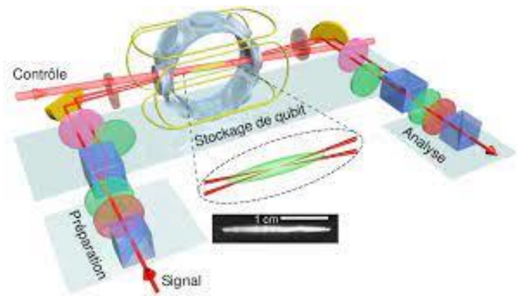
Alice-R: key1, R-Bob: key2, R: key1⊕key2 → Bob: key2⊕(key1⊕key2) = key1

Towards quantum repeaters

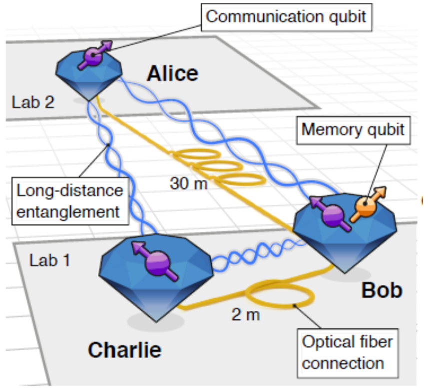
Create efficiently end-to-end entangled resources with quantum repeaters and quantum memories

Fundamental for interconnecting devices via teleportation over long distances, **alleviate need for trust in intermediate nodes**

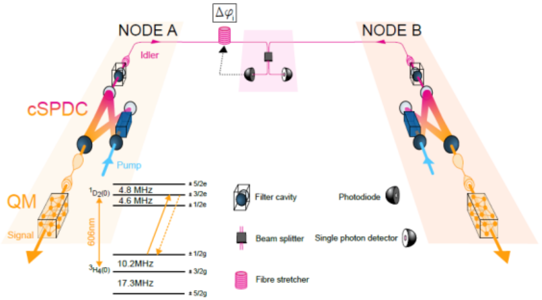




M. Cao, F. Hoffet *et al.*, Optica 2020



M. Pompili *et al.*, Science 2021



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

Technological challenges despite significant progress

→ trade-offs in critical benchmarks (efficiency, storage time), entanglement rate, range,…

→ development of network architecture for the quantum internet

Target performance with multiplexing techniques: **repeater link with 50 bit/s over 50 km, >97% fidelity**

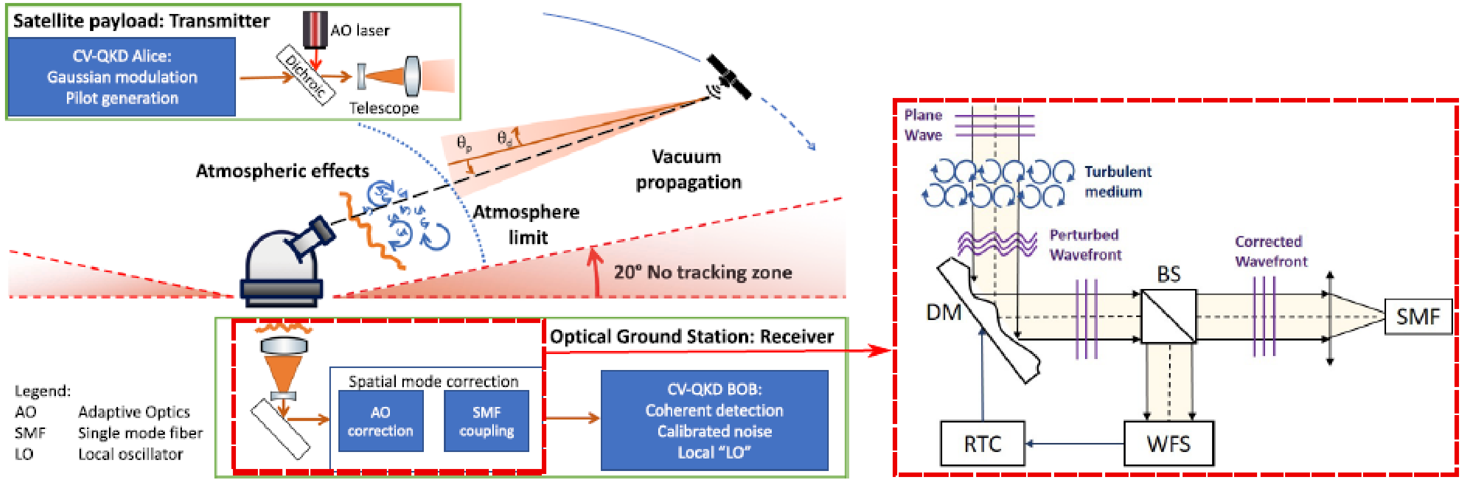
Full network stack for target use cases in server-client scenario

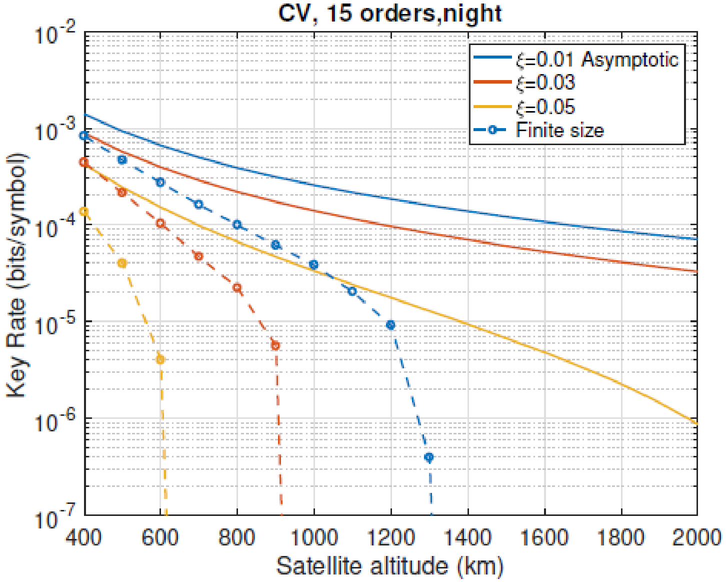
QIA QUANTUM INTERNET ALLIANCE

Towards 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

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

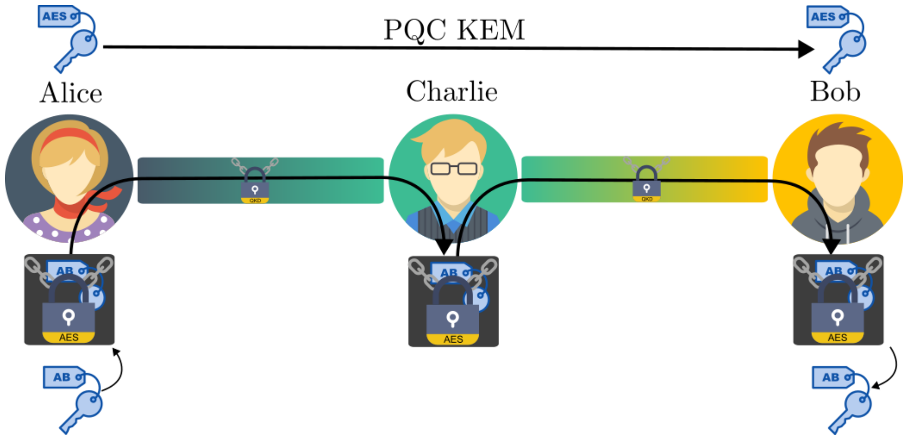
Refined analysis of fibre coupling with adaptive optic system → correcting up to 15 orders optimal for both CV and DV-QKD, for LEO at almost all conditions

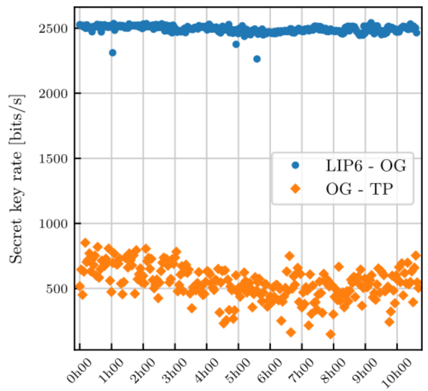
Analysis of entanglement-based scenario → trade-offs between visibility time, losses, divergence, pointing, telescope size, detector efficiency,…

D. Dequal *et al.*, npj Quant. Info. 2021, V. Marulanda Acosta *et al.*, New. J. Phys. 2024
L. de Forges de Parny *et al.*, Commun. Phys. 2023

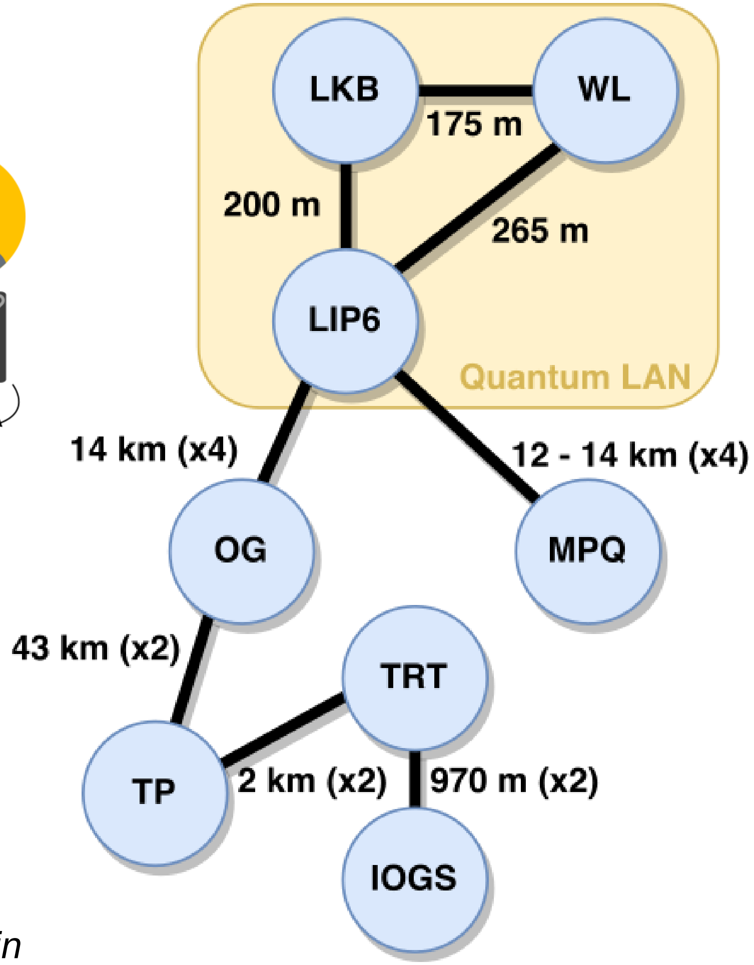
Paris testbed deployment and FranceQCI

Benchmarking with commercial systems
Efficient PQC-secured trusted-node QKD exchange





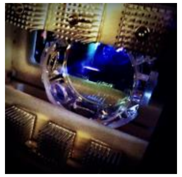
Y. Piétri *et al.*, *PQC-secured Trusted Node for QKD in a Deployed Network*, QCrypt 2024



Deployment of CV-QKD industrial prototype

Entanglement distribution with PIC-based sources

Deployment of quantum memory link
Highly-efficient neutral atom based technology

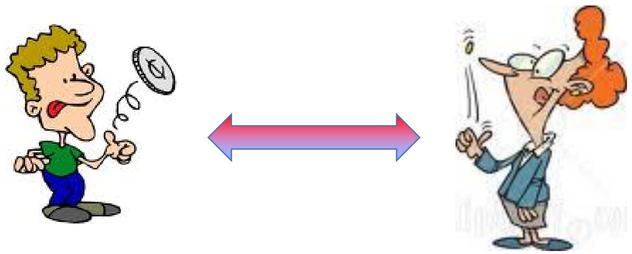


Long term secure storage with QKD

Quantum coin flipping

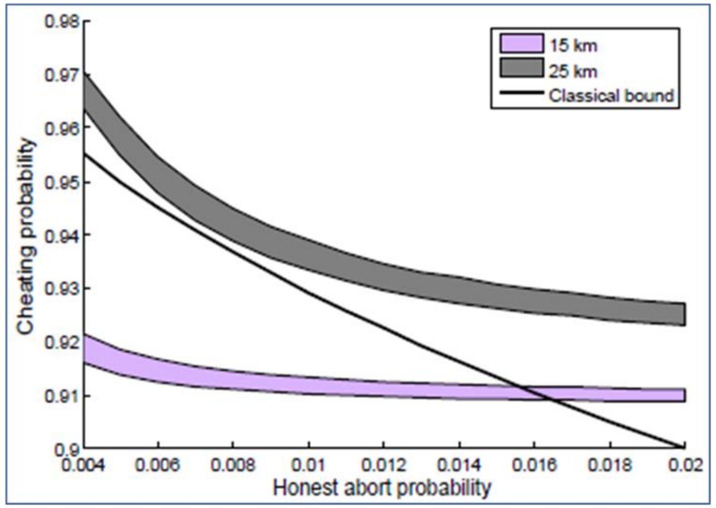
Strong coin flipping

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



$$P_B \leq \frac{1}{2} + \epsilon_B \qquad P_A \leq \frac{1}{2} + \epsilon_A$$

With classical resources $\rightarrow$ computational assumptions or trusted third party
With quantum resources $\rightarrow$ information-theoretic security but fundamental lower bound: bias $\epsilon > 0$



Theoretical analysis allows for non-zero honest abort to include imperfections

Satisfies balancing condition: $P_d^A = P_d^B$

Experimental demonstration with adapted QKD system

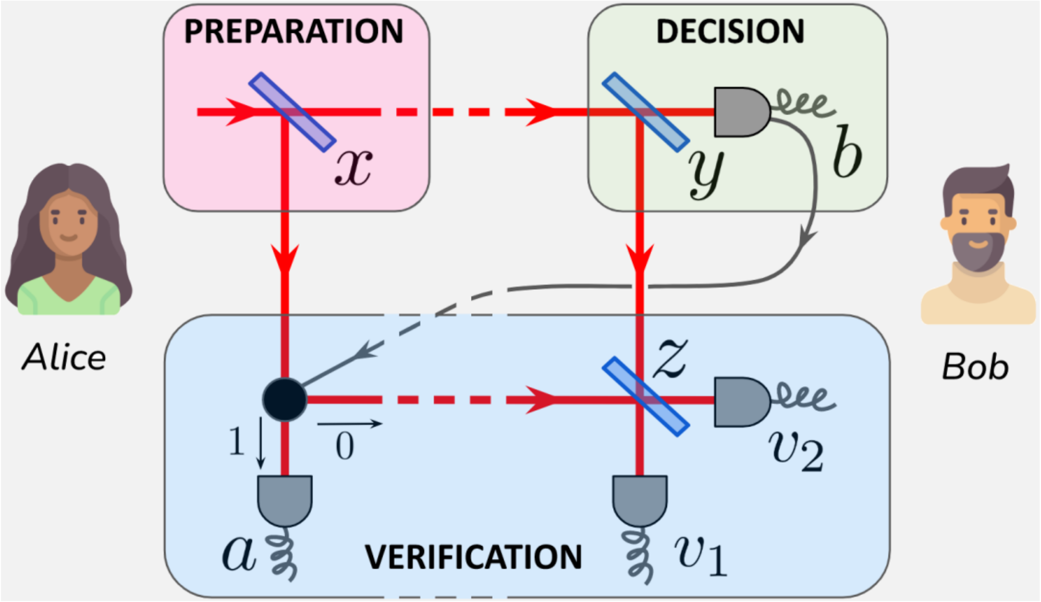
A. Pappa *et al.*, Nature Commun. 2014

Weak coin flipping

Alice and Bob have a preferred outcome, effectively designates a winner and a loser
$\rightarrow$ bias arbitrarily close to zero in principle
$\rightarrow$ allows to construct optimal quantum SCF and bit commitment schemes

Protocol for quantum WCF with a single photon

High sensitivity to loss: a party can declare loss if unhappy with the flip
Previously impractical protocols: require beyond-qubit states and generalized measurements



photon number encoding
conditional verification step

If $b = 0$,
- $v_2 = 1$: Alice is sanctioned for cheating,
- $(v_1, v_2) = (1, 0)$: Alice wins,
- $(v_1, v_2) = (0, 0)$: the protocol aborts.

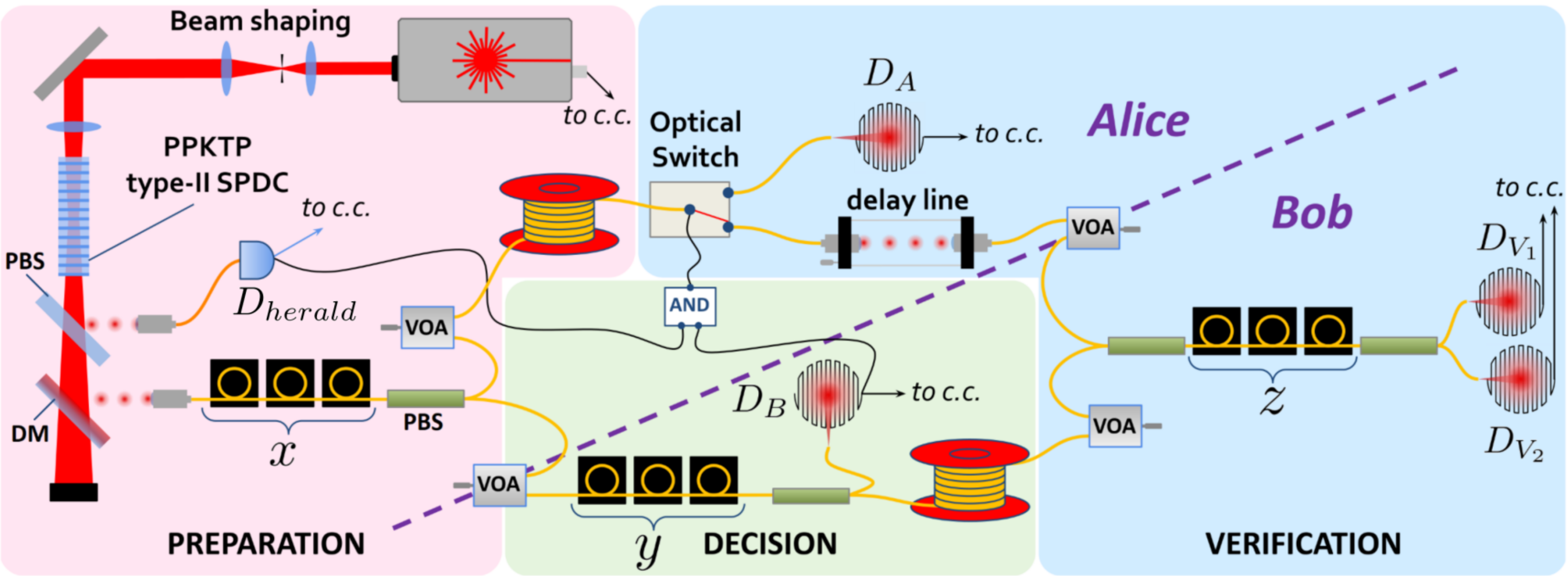
If $b = 1$,
- $a = 0$: Bob wins,
- $a = 1$: Bob is sanctioned for cheating.

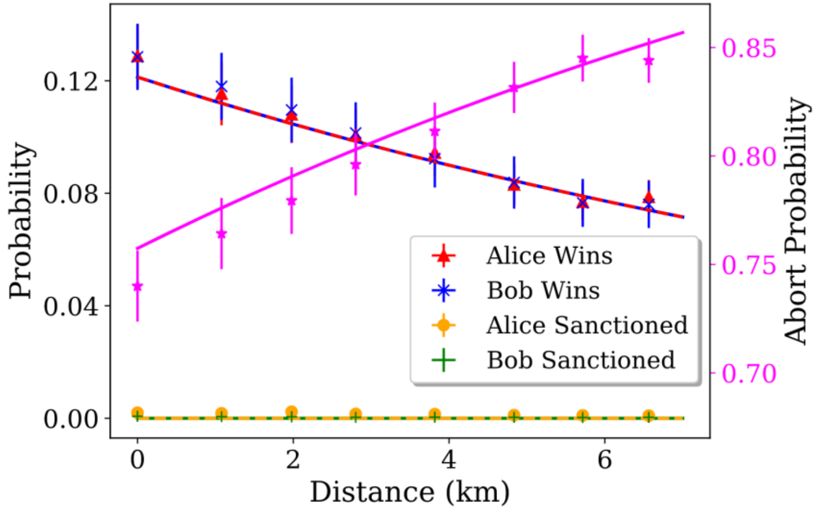
Ideal conditions for cheat sensitivity

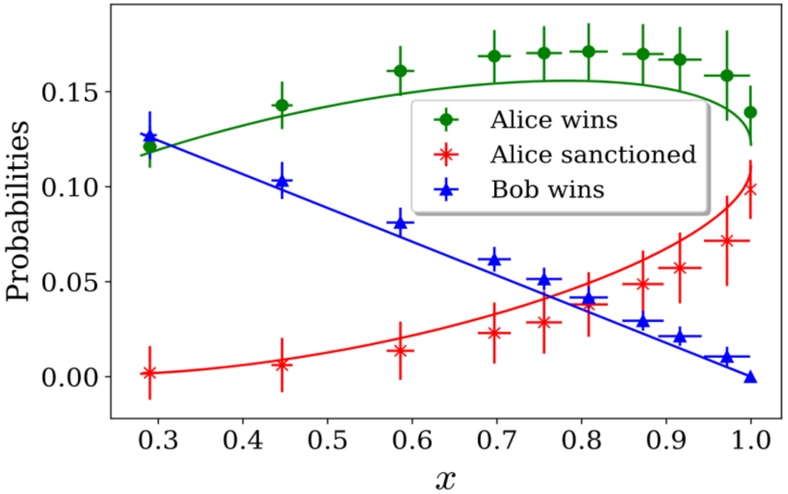
Fairness: $P_h^{A.wins} = P_h^{B.wins}$ Correctness: $P_h^{A.sanct} = P_h^{B.sanct} = 0$

S. Neves, V. Yacoub, U. Chabaud, M. Bozzio, I. Kerenidis, ED, Nature Commun. 2023

Experimental demonstration of quantum WCF







Detector performance and interferometer visibility crucial

Quantum advantage in form of cheat sensitivity maintained over a few kilometers

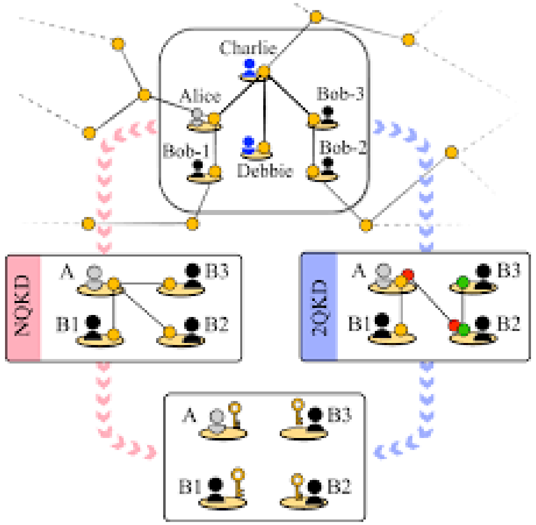
S. Neves *et al.*, Nature Commun. 2023

Certification of multipartite entangled states

The development of tools to certify the "**quantumness**" of resources ubiquitous in quantum technologies is fundamental for their use for practical applications

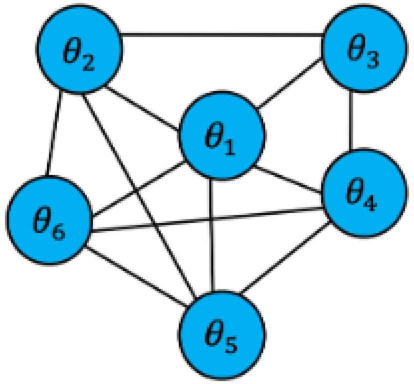
Multipartite entangled states as a resource for quantum network protocols

Conference key agreement



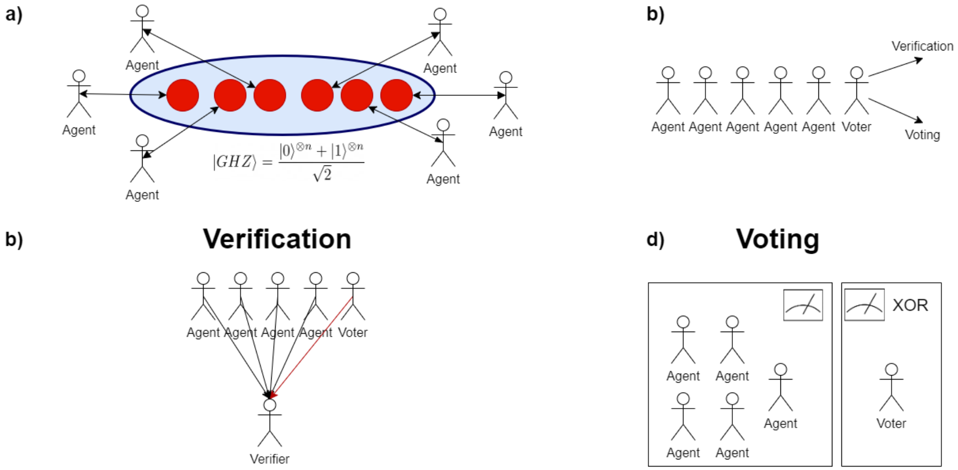
A. Pickston *et al.*, npj Quant Info. 2023

Privacy in networks of sensors



N. Shettell *et al.*, arXiv quant-ph/2207.14450

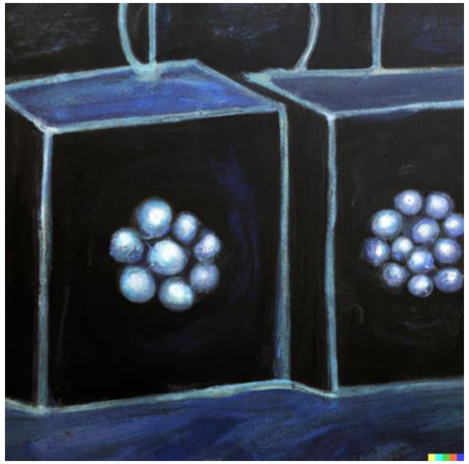
Electronic voting



F. Centrone *et al.*, Phys. Rev. Applied 2022

To guarantee the correct functioning of the protocol and hence the targeted property – privacy, security, anonymity,…
→ introduce subroutine for authentication of resources at hand

Certification of multipartite entangled states



Ideally no assumptions for certification: black box model → device independence (DI)

Violation of Bell inequality is a DI witness of entanglement
→ ***maximal*** Bell violation DI witness of ***particular*** quantum states and measurements?

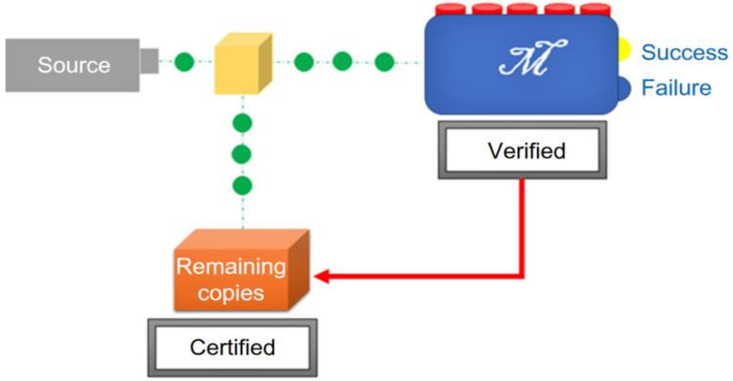
Self-testing: find the relation between the physical and an ideal reference experiment
The distance of the observed violation from the maximal one bounds the fidelity of the state

Typically, important assumptions: no losses, large sets of independently and identically distributed (IID) states, measurement of all states,…

I. Šupić and J. Bowles., Self-testing of Quantum Systems: A Review, Quantum 2020

- No trust on the measurement devices (DI scenario)
- No IID assumption (compatibility with adversarial scenarios)
- Output certified state available for use

Our contribution: few-copies, non-IID GHZ state certification



A. Gočanin *et al.*, PRX Quantum 2022

Fully device-independent scenario

Extractability: maximum fidelity over all possible isometries

Isometry

Define the goal: $\Xi(\tilde{\sigma}_c, |GHZ\rangle) = \max_{\Phi} \mathscr{F}(\Phi[\tilde{\sigma}_c], |GHZ\rangle) \geq 1 - \eta$

Fidelity

Certified State

Violation of Bell inequality

Choose a Bell inequality that self-tests the target state: $\Xi \geq s\beta + \mu$

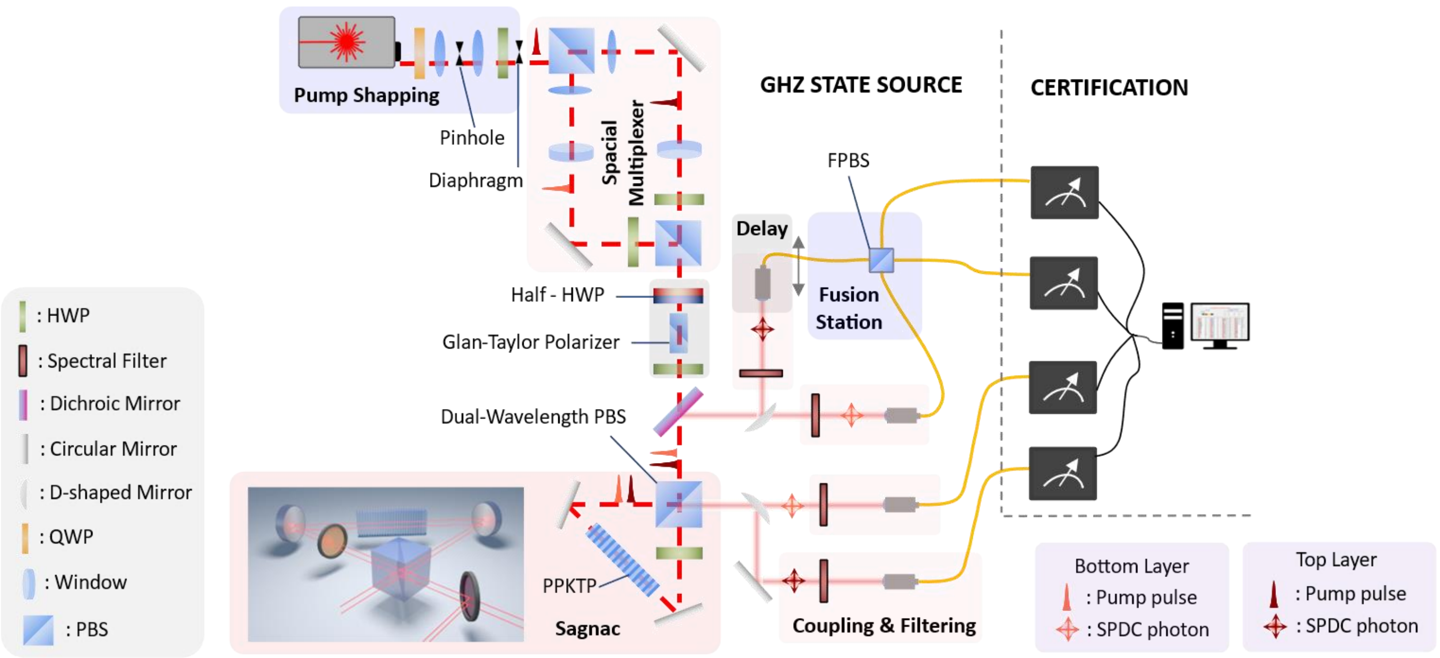
Reframe scenario as nonlocal game derived from the Bell inequality

Only the target state (up to local isometries) achieves the optimal quantum winning probability

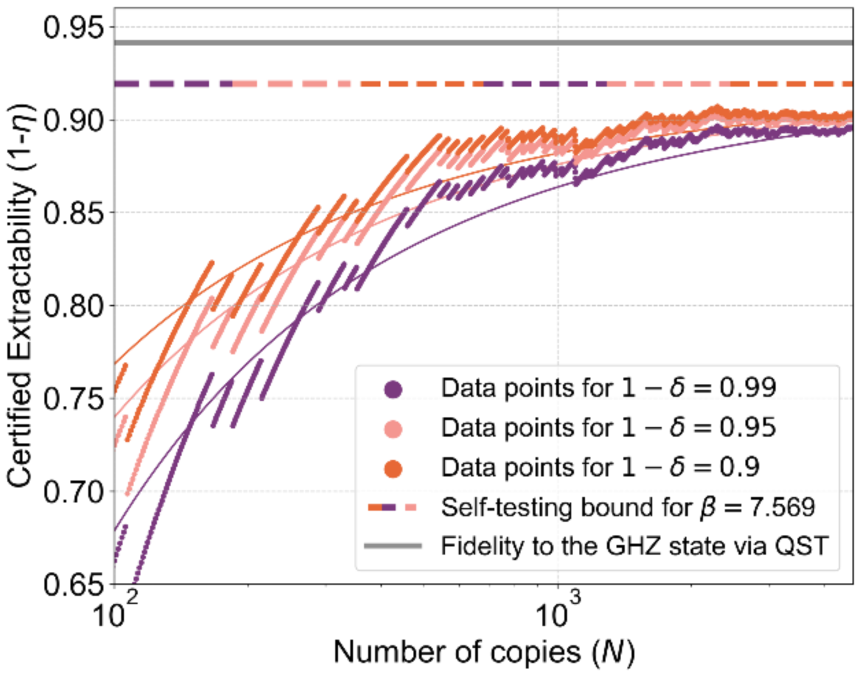
Sample efficiency

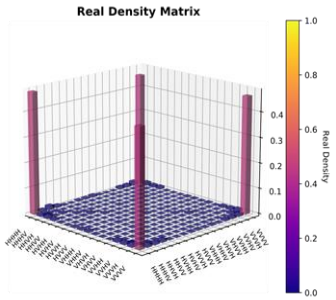
For N-1 measured copies and given a randomly selected unmeasured copy, we can infer with a confidence (1-δ) that this copy is (1-η) close to the target state

Experimental certification of a 4-party GHZ state



L. dos Santos Martins *et al.*, *Experimental sample-efficient and device-independent GHZ state certification*, arXiv:2407.13529





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

F = 94.73 % @ 1.7 Hz

Mermin-like nonlocal game

Trade-off between N and δ

Certification of $\boldsymbol{\Xi(\sigma_c, |GHZ\rangle) \geq 0.896}$ **for** $\boldsymbol{1-\delta = 0.99}$ **and** $\boldsymbol{N = 4643}$

L. dos Santos Martins *et al.*, *Realizing a compact, high-fidelity, telecom-wavelength source of mutltipartite entangled photons*, arXiv:2407.00802

Key takeaways

Significant progress in recent years

High-TRL QKD systems deployed in moderate-scale testbeds all over the world with strong security assumptions (trusted end users, mostly trusted intermediate nodes)

Milestone satellite quantum communication experiments

Low-TRL implementations of other quantum cryptographic functionalities

Low-TRL quantum memory devices and elementary repeater links

What are the next barriers to overcome for scale up and wide use in global quantum networks?

Relax security assumptions on users and nodes

Enhance performance and increase TRL while also providing agility and versatility in large-scale testbeds

Integrate with computational (post-quantum) cryptography and standard networks

Enrich functionalities with demonstrated quantum advantage

Certification and standardization across all quantum technology pillars

Thank you!

Y. Piétri, M. Schiavon, A. Rosio, V. Marulanda Acosta, L. Trigo-Vidarte, D. Fruleux, A. Rhouni, F. Roumestan, A. Ghazisaeidi, M. Huguenot, B. Gouraud, A. Leverrier, P. Grangier, T. Liège, C. Lim, J.-M. Conan, D. Dequal L. dos Santos Martins, N. Laurent-Puig, V. Yacoub, S. Neves, M. Bozzio, U. Chabaud, M. Baroni, S. Scheiner, A. Innocenzi, A. Yangüez, M. Rezig, P. Lefebvre, I. Šupić, I. Kerenidis, A. Grilo, D. Markham