Implementation of QKD protocols

Eleni Diamanti

LIP6, CNRS, Sorbonne Université

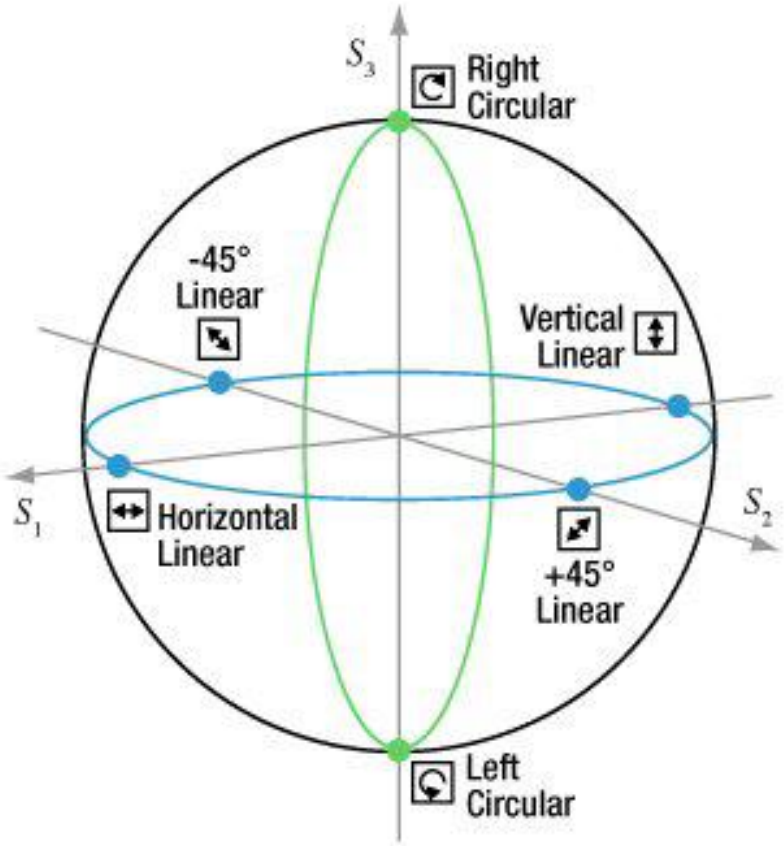
Paris Centre for Quantum Technologies

eleni.diamanti@lip6.fr

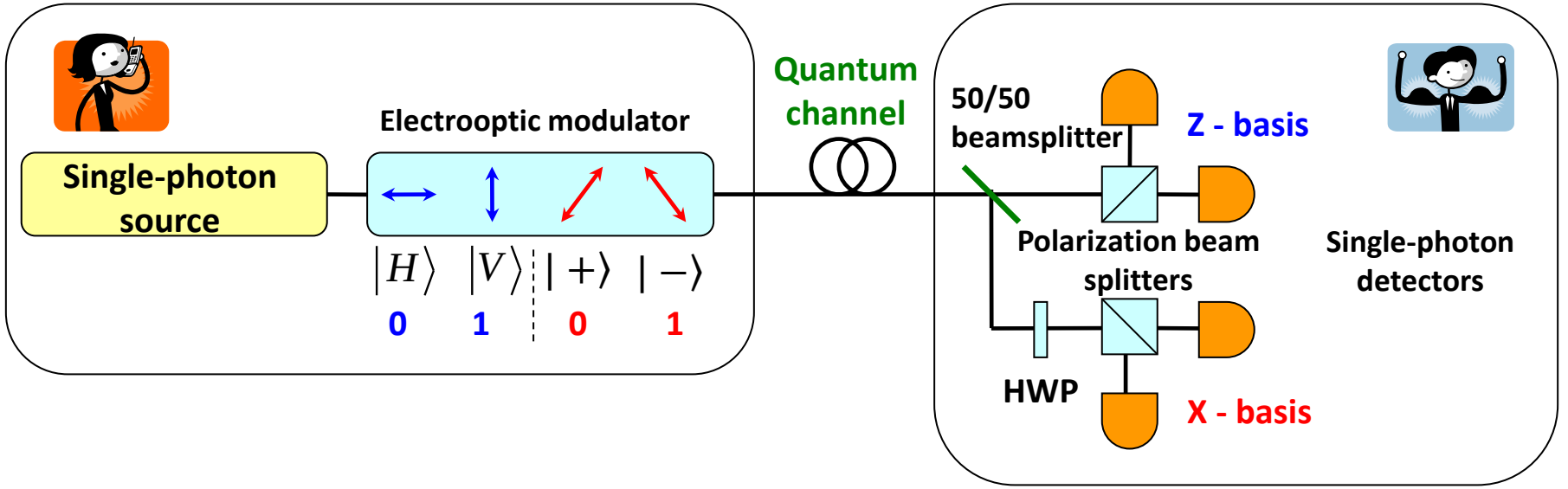
QKD Summer School

Les Diablerets, 19 August 2026

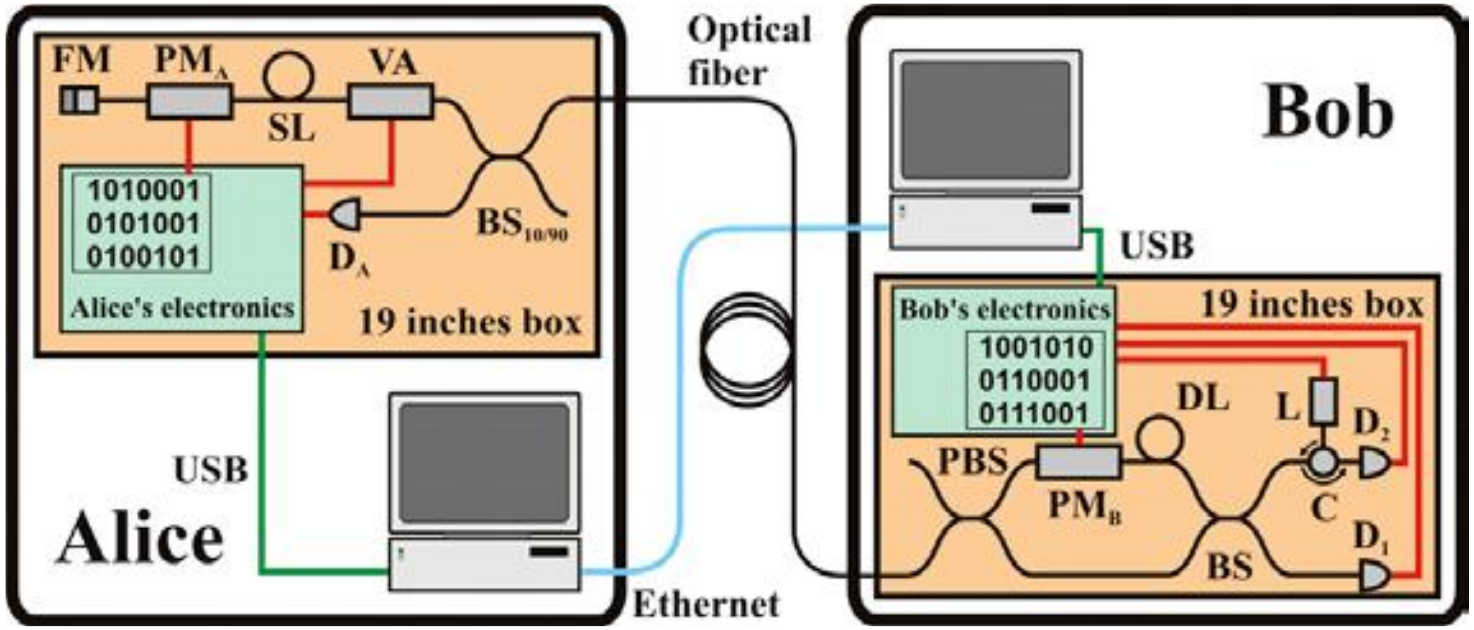
Encoding - polarization



Experimental setup for polarization-encoded BB84

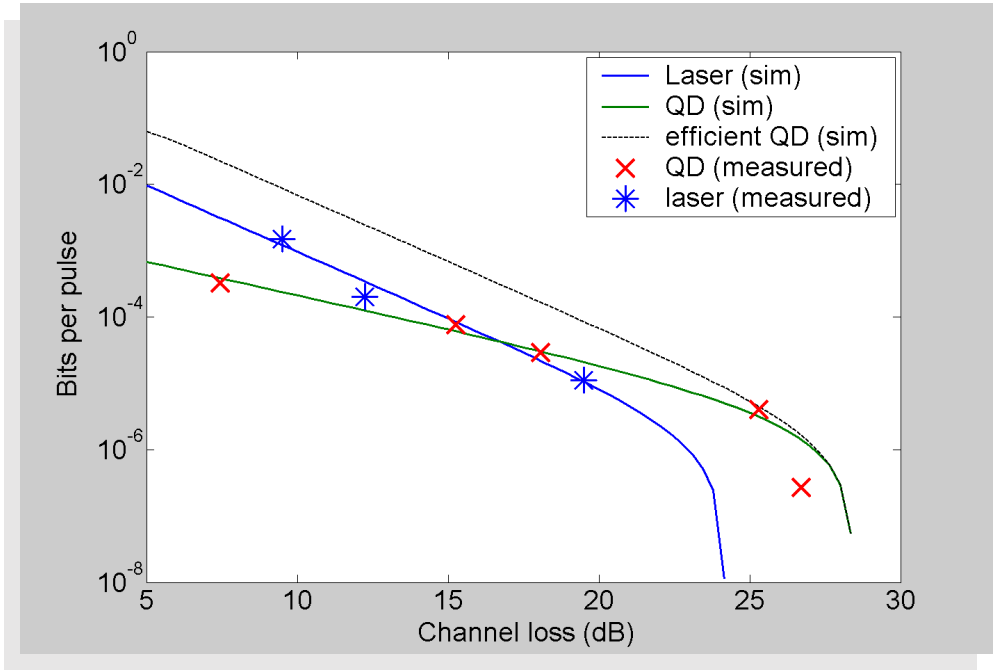


Plug and play QKD system

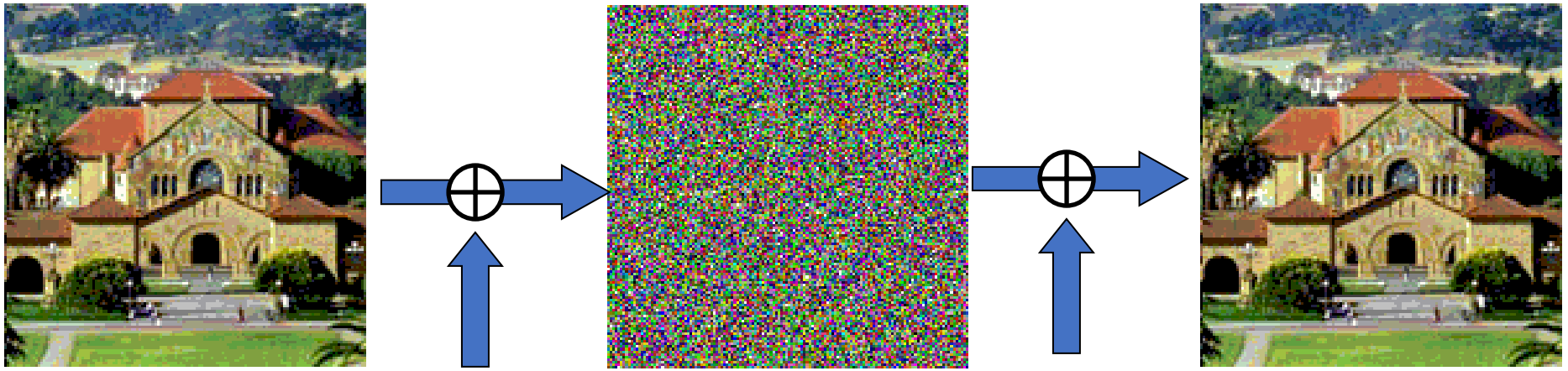


id Quantique

QKD with a quantum dot single photon source@Stanford



Many more a lot more recent experiments!



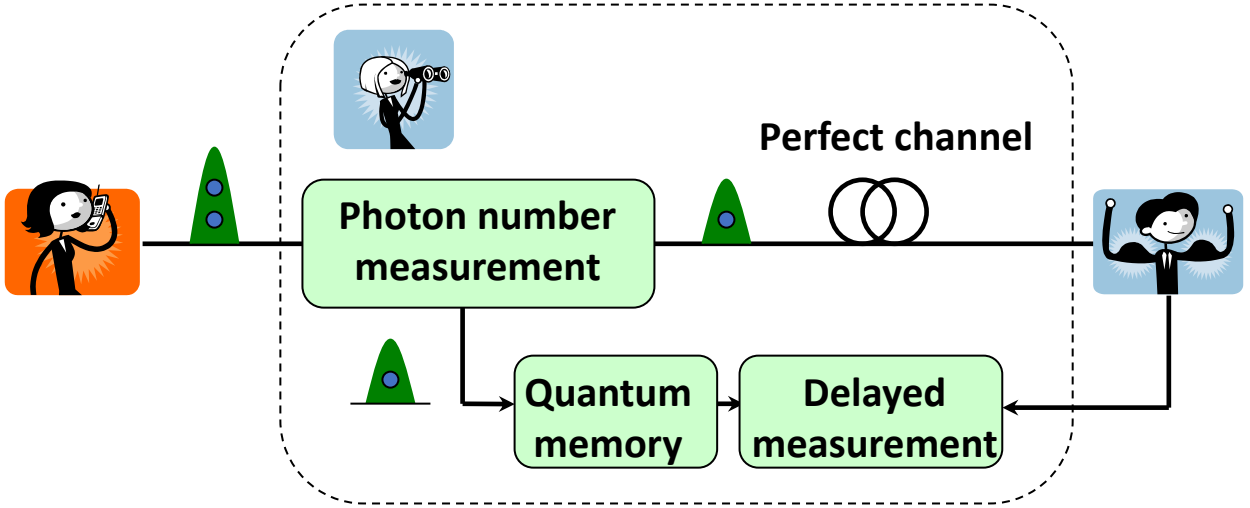
BB84 and photon number splitting (PNS) attacks

Eve performs the following attack

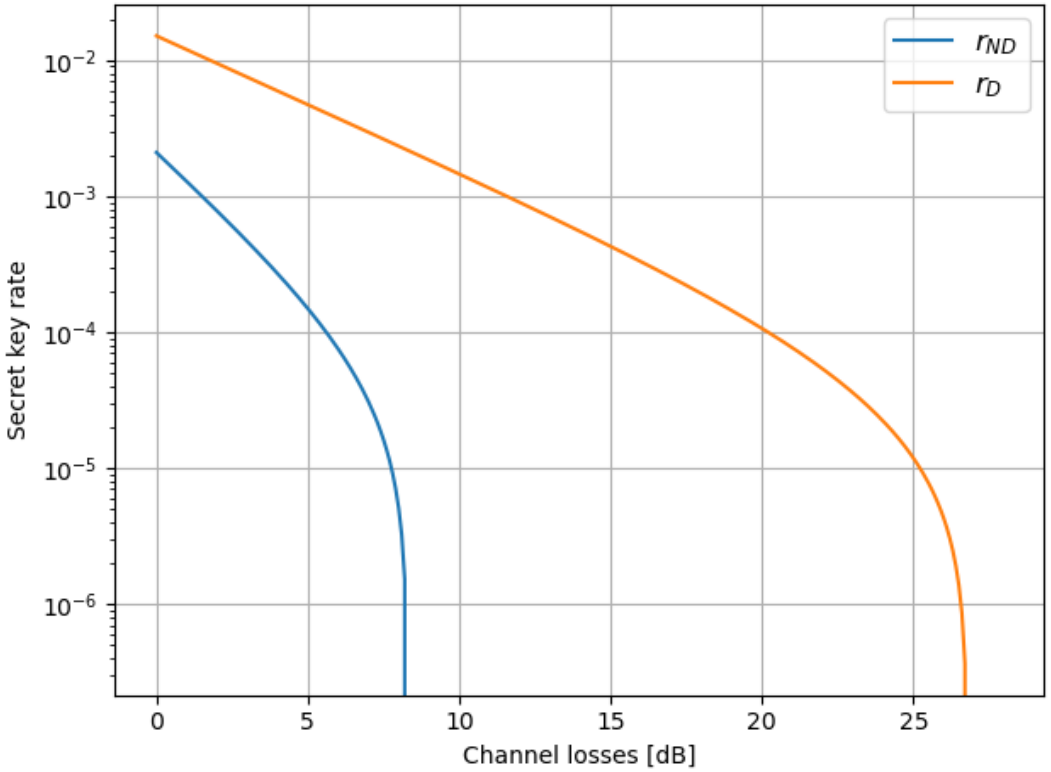
non-destructive measurement of photon number

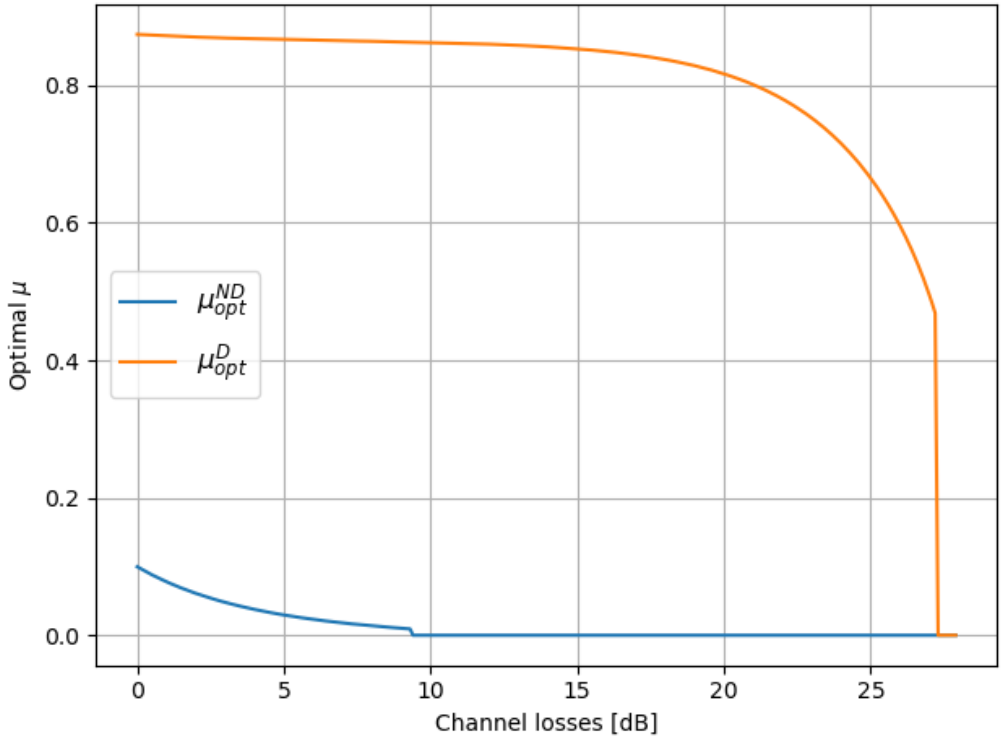
if $n \geq 2$: extract and keep one photon, perform delayed measurement

if not : block the signal and pretend a vacuum state



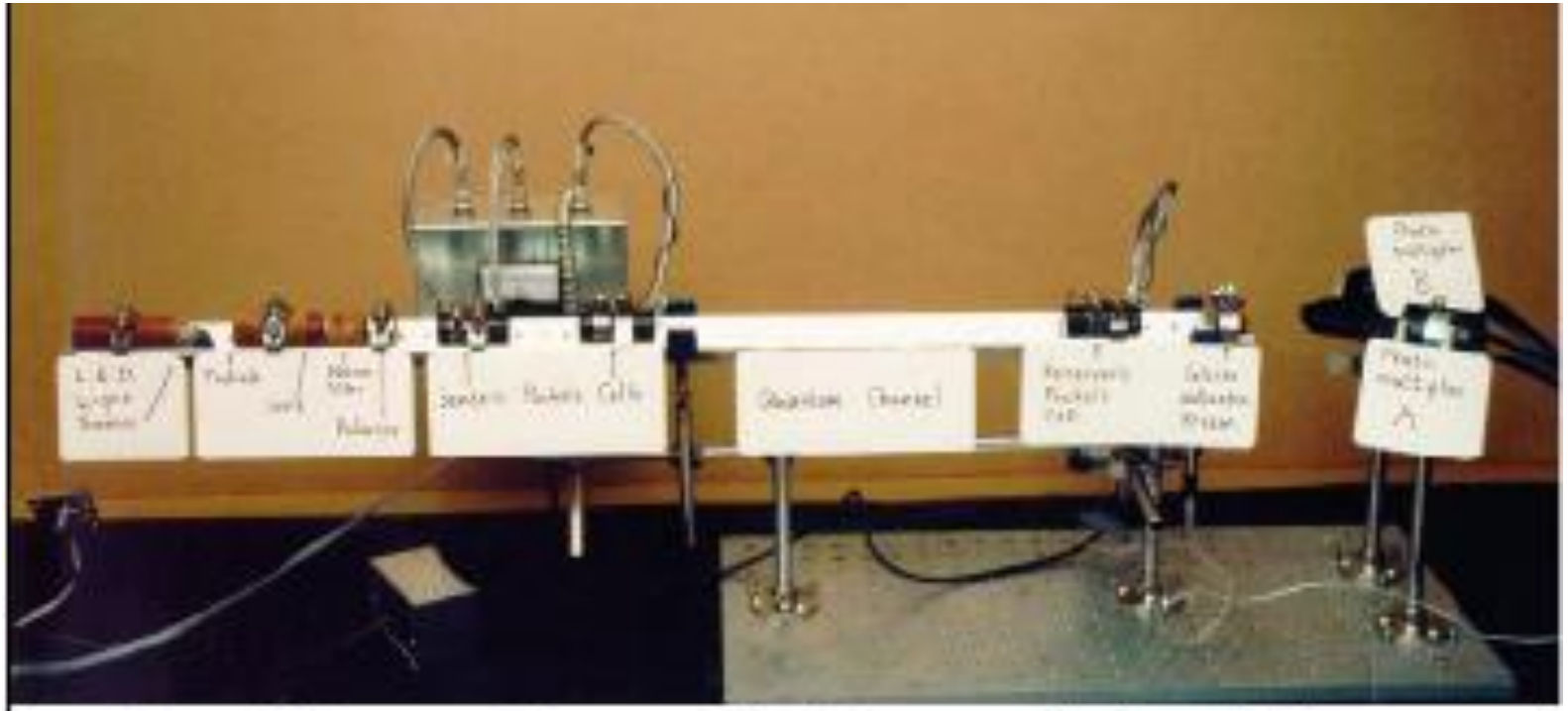
Performance of decoy state protocol





Credits: Matteo Schiavon, Yoann Piétri

The first system



Original Quantum Cryptographic Apparatus built in 1989 transmitted information secretly over a distance of about 30 cm.

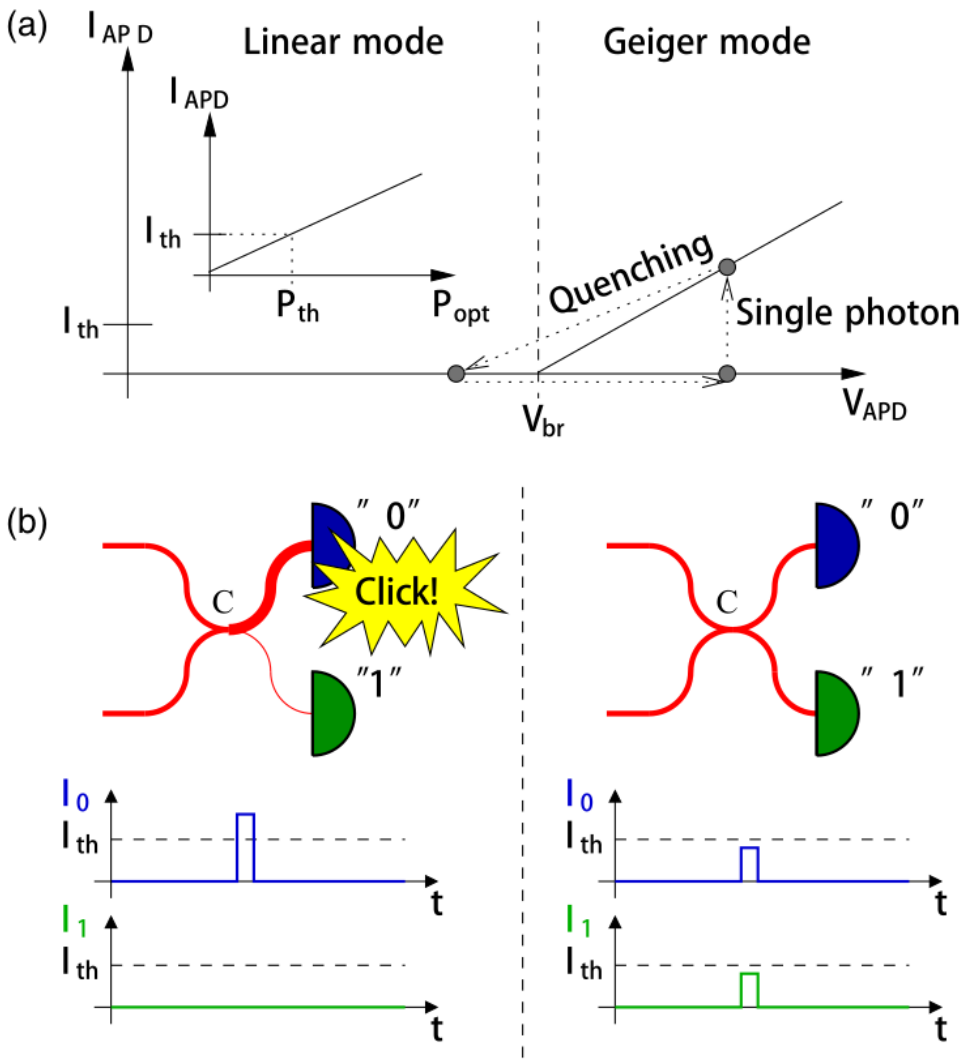
Sender's side produces very faint green light pulses of 4 different polarizations.

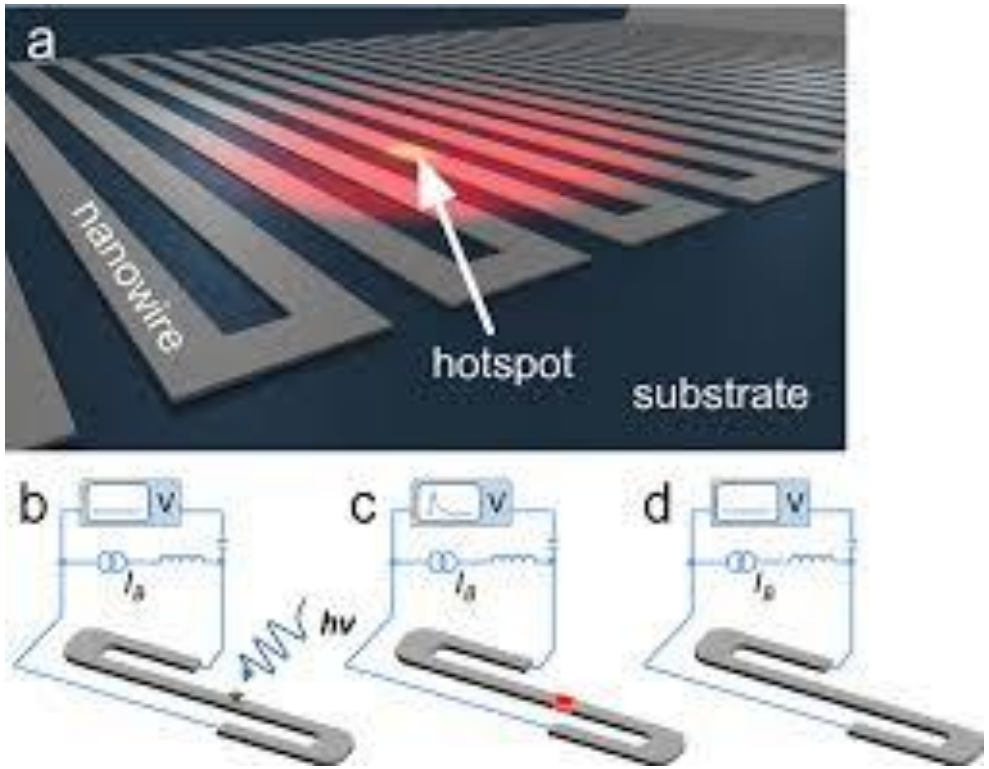
Quantum channel is an empty space about 30 cm long. There is no Eavesdropper, but if there were she would be detected.

Calcite prism separates polarizations. Photomultiplier tubes detect single photons.

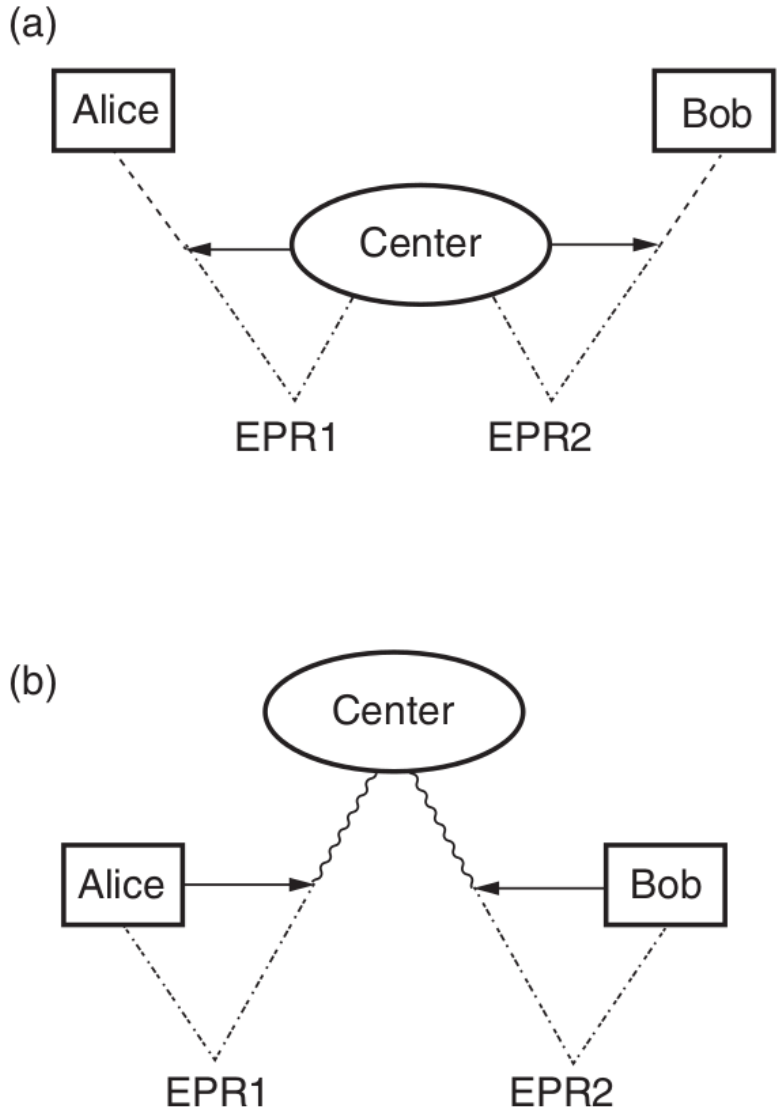
IBM-University of Montréal

Single-photon detectors

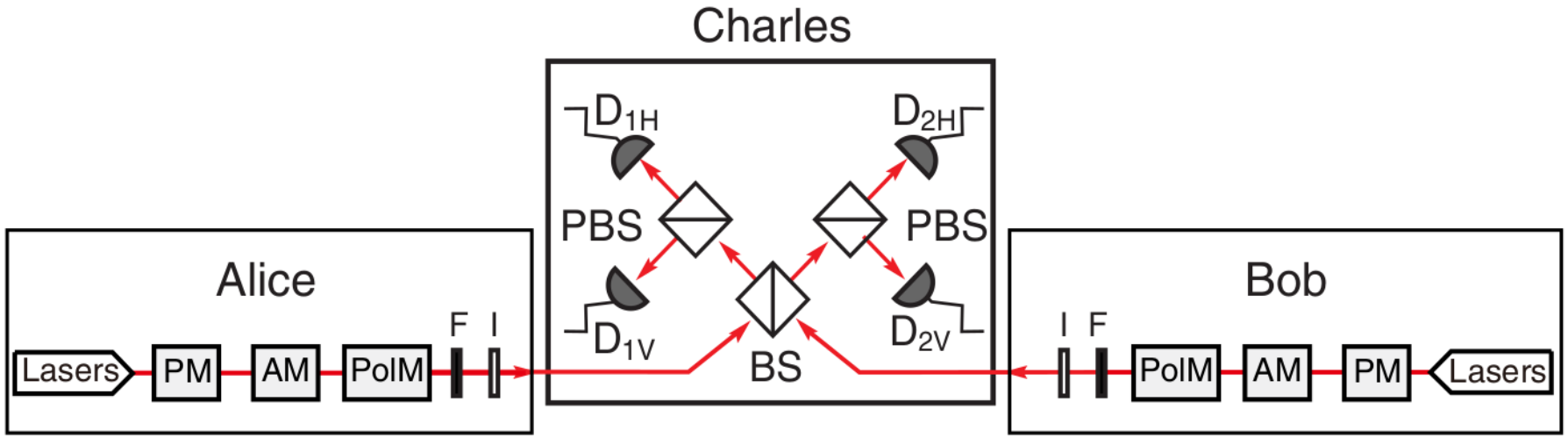




Entanglement swapping based QKD and time-reversed version

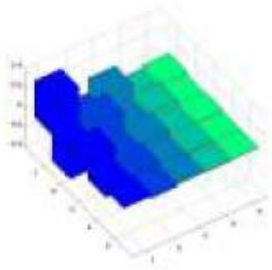
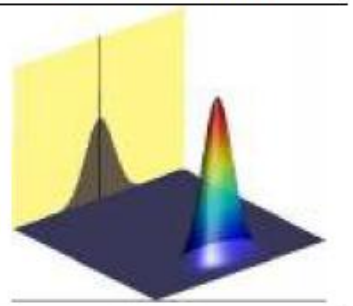
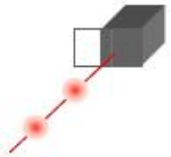
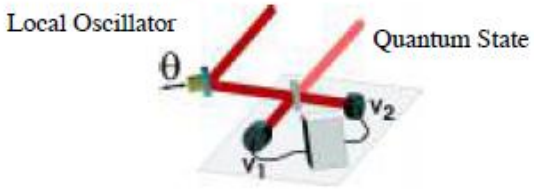


MDI scheme



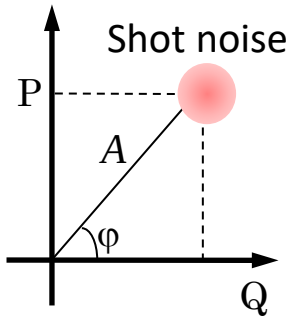
F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, Rev. Mod. Phys. 92, 025002 (2020)

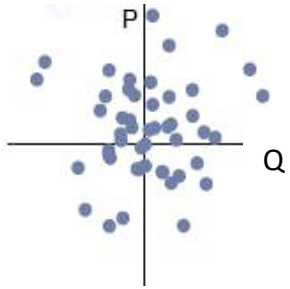
Discrete and continuous variable encoding for QKD

Light is :	Discrete Photons	Continuous Wave
We want to know :	their Number & Coherence	its Amplitude & Phase (polar) 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  $V_1 - V_2 \propto X_\theta = X\cos\theta + P\sin\theta$
« Simple » States	Fock States	Gaussian States

Post processing	Key readily available	Complex error correction
Security	General attacks, finite-size, side channels	General attacks, finite-size, side channels

Coherent state continuous-variable QKD

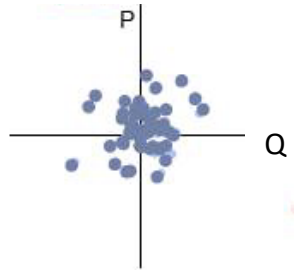




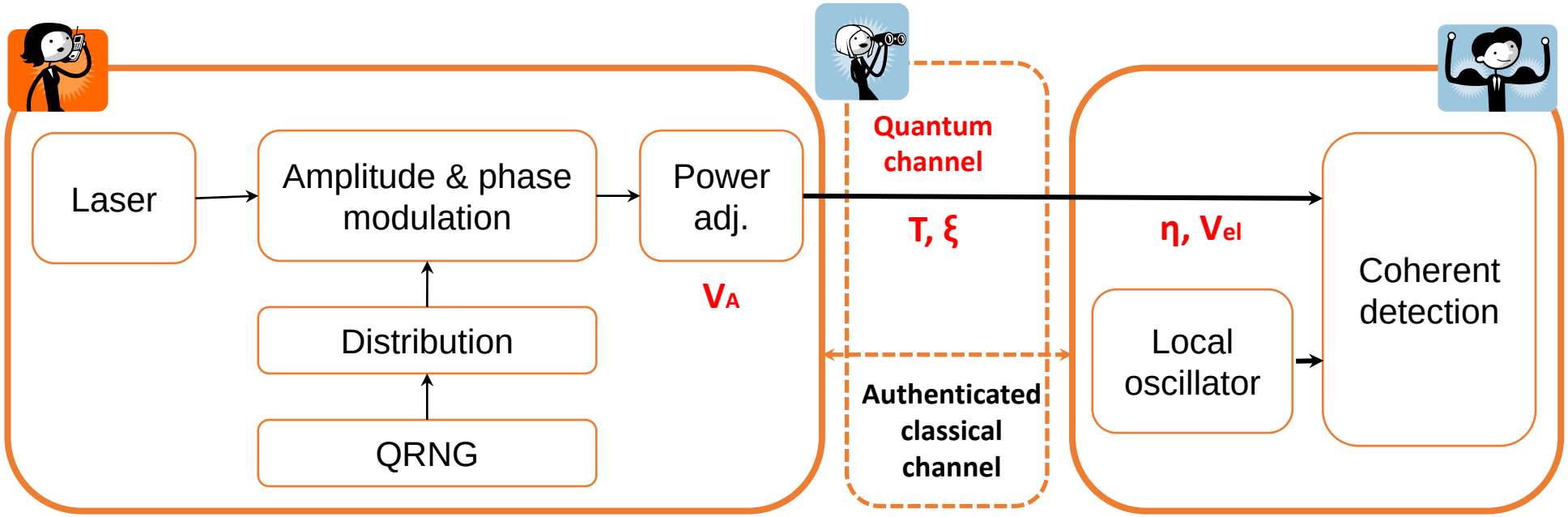
$$\{q_i \quad p_i, 1 \le i \le N\}$$

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

Gaussian, QPSK, QAM,…

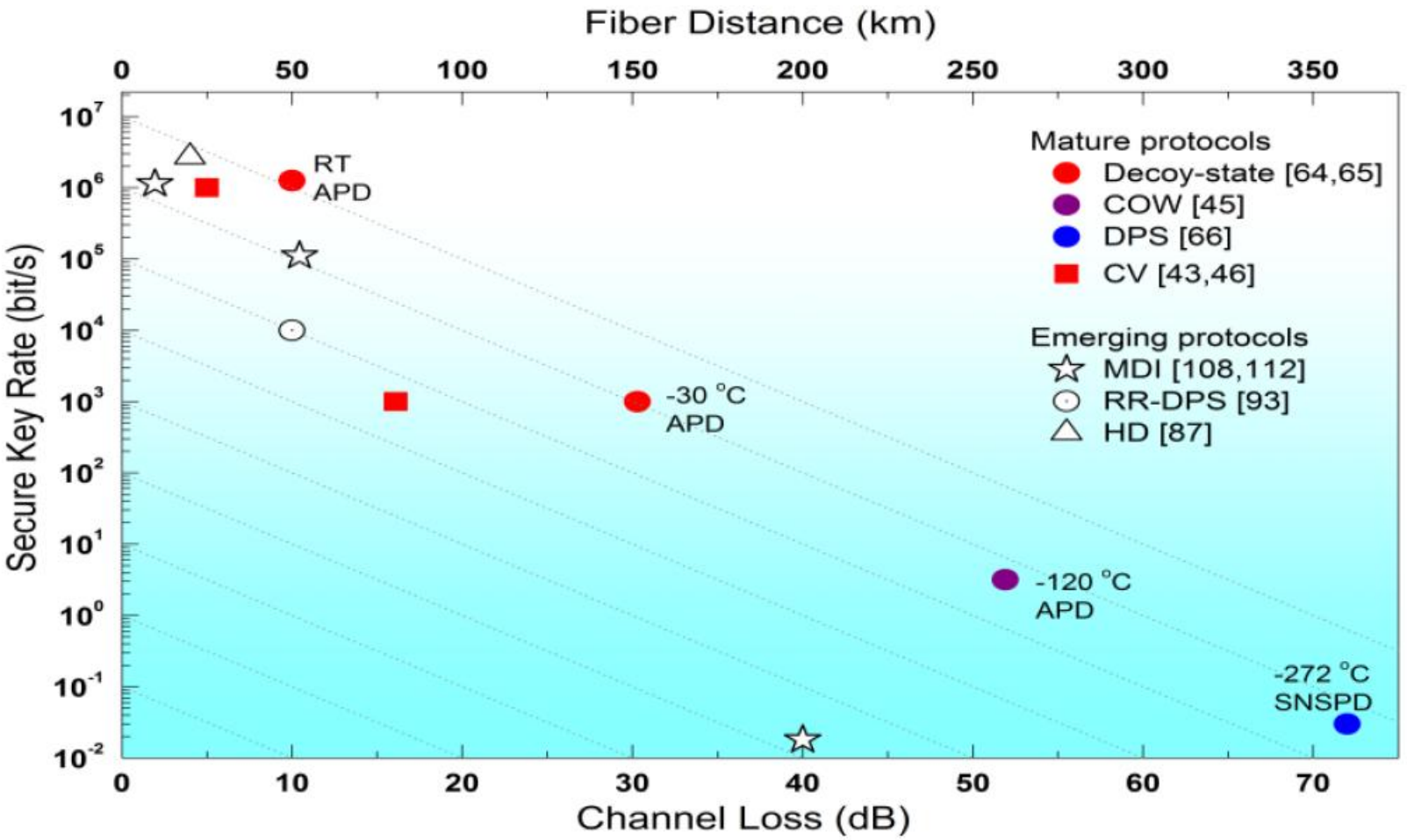


Single (homodyne) or double (heterodyne) quadrature detection



Composable, finite size security proof for Gaussian modulation
Adapted to arbitrary discrete constellations at asymptotic limit

QKD in practice



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

ED, H.-K. Lo, B. Qi, Z. Yuan, Practical challenges in quantum key distribution, npj Quantum Information 2, 16025 (2016)

Performance measures and use case criteria

At what ***distance*** can the secret key be generated?

Major difference with classical cryptographic systems: inherent limitation due to optical fiber loss

→ QKD networks and satellite communication

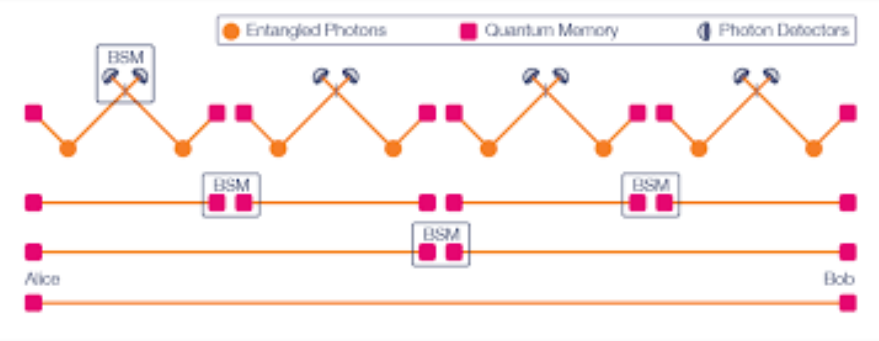
What is the right ***topology*** for the QKD network?

Can we accept prepare-and-measure schemes and trusted nodes?

Or do we need (some) untrusted nodes? (Semi) device independence?

Is it possible to ensure upgradability towards long-term quantum networks?

Definition of appropriate network interfaces



What is the right ***satellite orbit and payload***?

LEO/MEO/GEO satellites differ vastly in terms of geographic coverage, loss budget, requirements for pointing and tracking system, operation wavelength

When are satellite constellations or nanosatellite technologies useful?

Performance measures and use case criteria

At what ***rate*** can the secret key be generated?

Important difference with classical systems: theoretical bounds for repeaterless links

→ New protocols and multiplexing techniques

What is the ***security*** status?

Composable security proof including finite-size effects

In terms of practical security, identification of side channels and countermeasures, crucial for certification

Complexity of classical post-processing techniques

When does it make sense to integrate with Post-Quantum Cryptography?

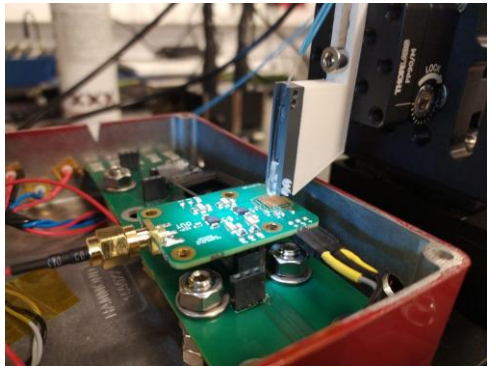
How ***cost-effective*** are the systems?

Compatibility with telecom network infrastructure → mutualized use important given the deployment cost

Dark or lit fibers

To what degree is it possible to use photonic integration circuits for scalability?

Maturity and availability of components

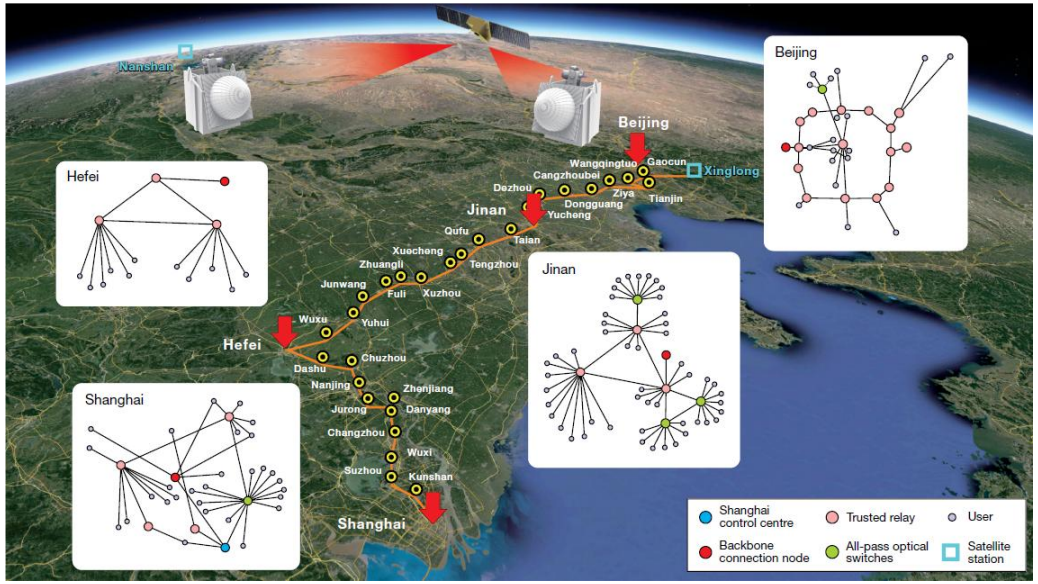


Y. Piétri et al., Optica Quantum 2024

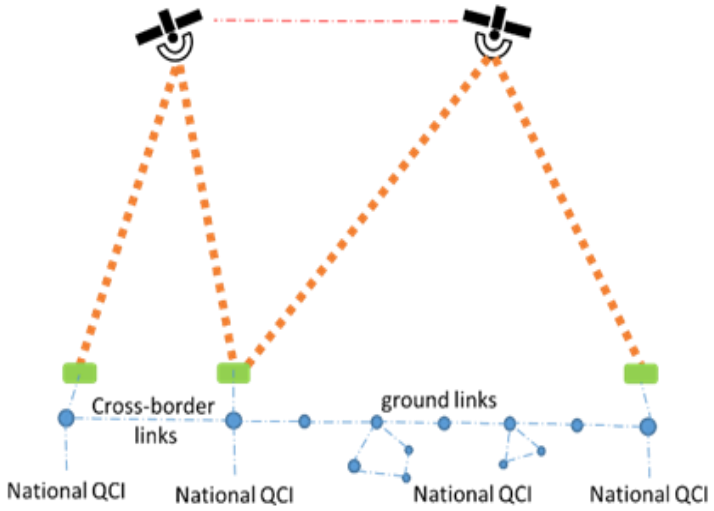
Long-distance networks

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

SECOQC QKD network, 2008
Swiss Quantum Network, 2011
Tokyo QKD network, 2015
China integrated terrestrial-satellite network



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



EuroQCI

An operational integrated satellite and terrestrial system spanning the whole EU for ultra-secure exchange of cryptographic keys

Reducing trust requirements

From trusted nodes to end-to-end security and advanced quantum networking applications

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

- if we want to send a photon successfully, trials increase exponentially with distance
- even when the photon arrives, the fidelity of the transmitted state decreases exponentially with distance…

Why can't we use amplifiers like in classical communications?
Amplification introduces noise → loss of correlations

Quantum memory and repeater technologies enable interconnecting devices over long distances

A quantum memory must have high storage-and-retrieval efficiency, high fidelity and long storage time

A quantum repeater must guarantee a good fidelity, use few resources, tolerate realistic operation and measurement errors

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

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

Quantum network stages and applications

QKD, coin flipping, digital signatures

Secret sharing, device independence, anonymous communication

Quantum money, secure multiparty computing, election, agreement

Blind, distributed quantum computing and sensing

Mature technology

Early commercial systems

Proof-of-principle

Trusted nodes and switching

Entanglement distribution

Quantum memories

Quantum processors

Present

Time