Secure communications in quantum networks

Eleni Diamanti

LIP6, CNRS, Sorbonne Université

Paris Centre for Quantum Computing

Horizon 2020 Programme

Quantum Science Seminar

17 June 2021

Quantum communication networks

Photonic resources

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

Security

Untrusted network users, devices, nodes

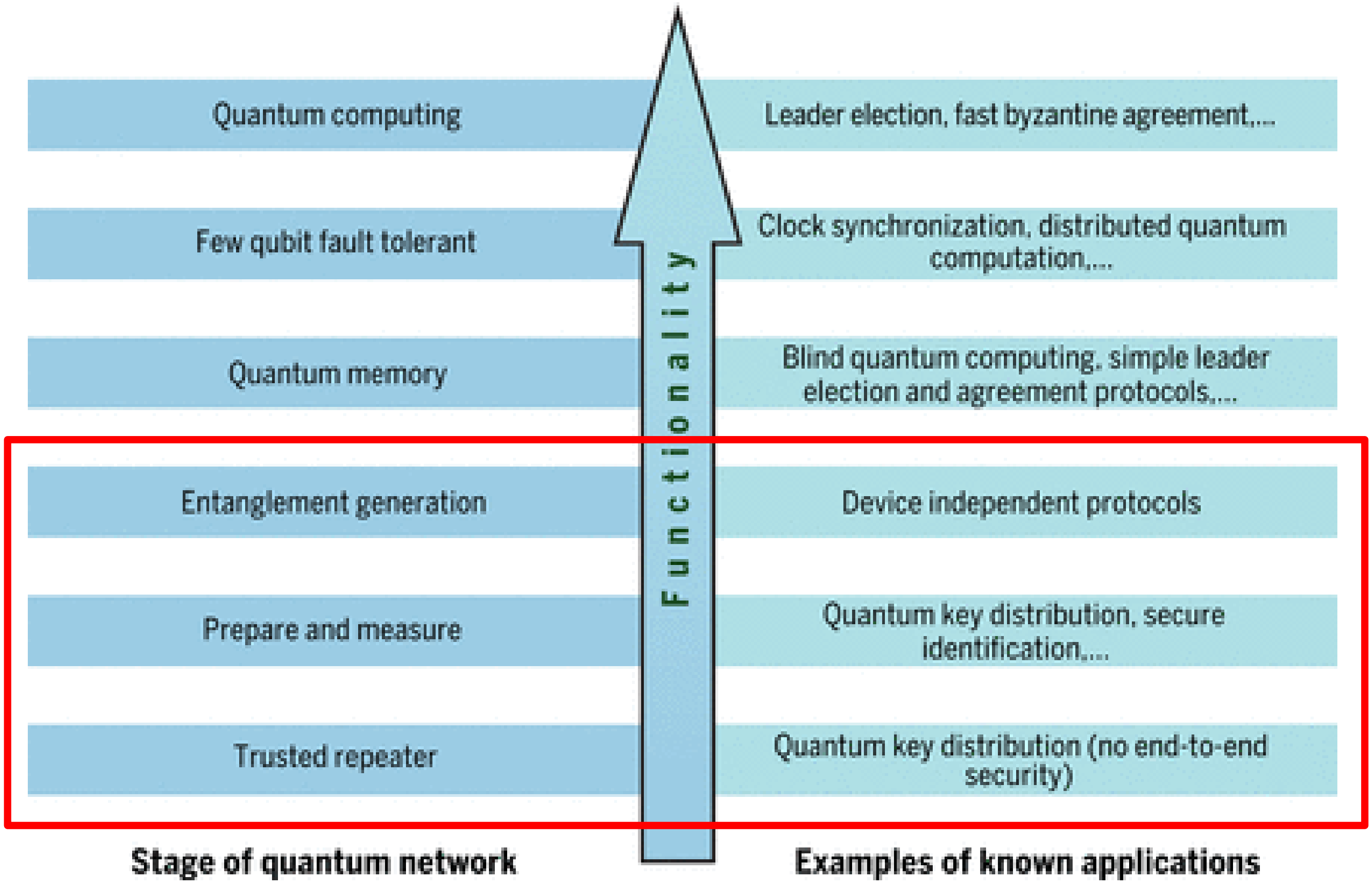
Efficiency

Optimal use of communication resources

Applications

- Exchange data
- Demonstrate quantum advantage in security and efficiency for communication, delegated and distributed computing tasks

Applications of quantum communication networks

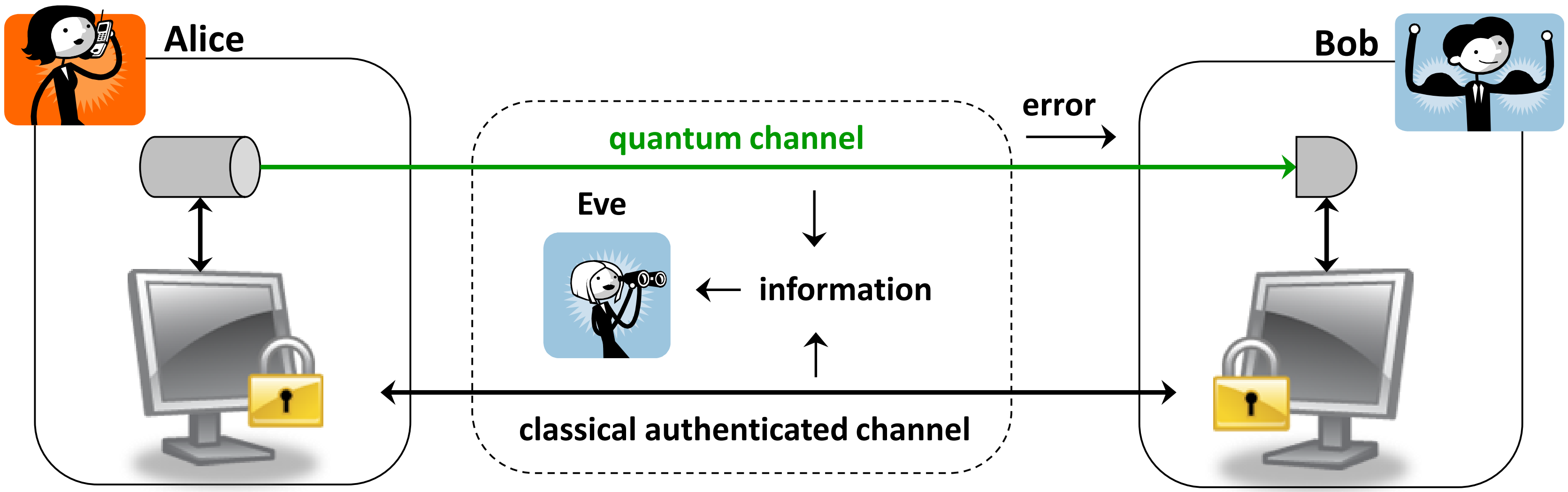


S. Wehner *et al.*, Science 2018

Securing network links: quantum key distribution

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

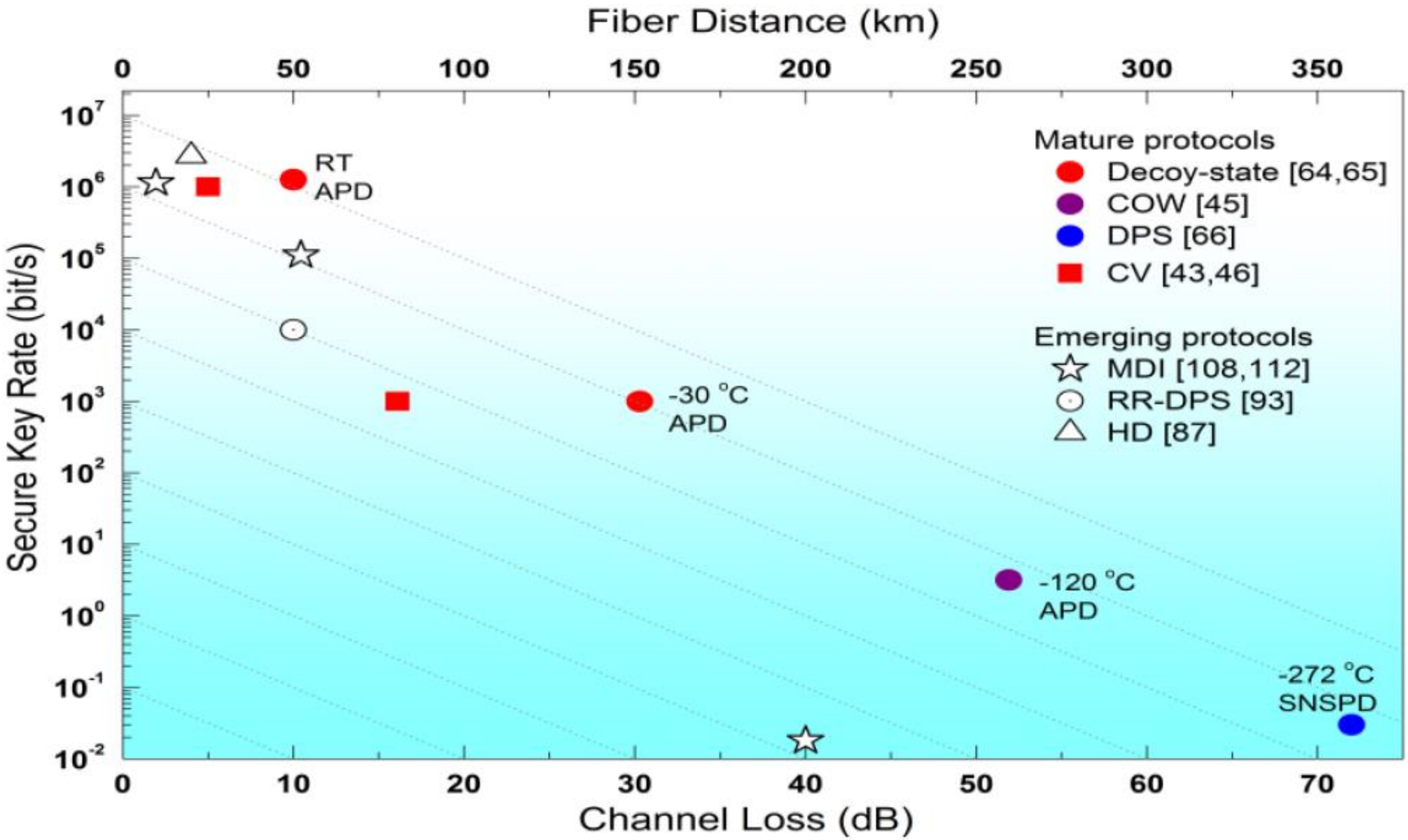
Quantum key distribution allows for exchange of sensitive data between two trusted parties with information-theoretic, long-term security guaranteed against an all-powerful eavesdropper
→ combined with suitable authentication and message encryption algorithms



Key information is encoded on photonic carriers

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

State of the art of point-to-point fiber-optic QKD



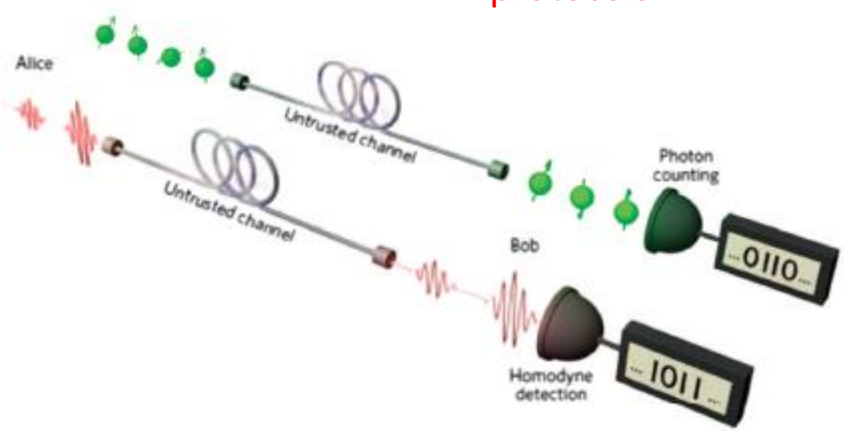
ED, H.-K. Lo, B. Qi, Z. Yuan, npj Quantum Information 2016

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

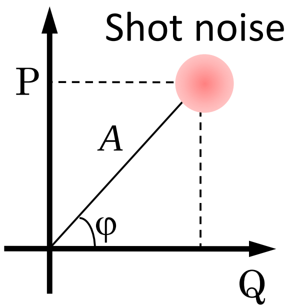
BB84, Decoy state, Coherent One Way, Differential Phase Shift, (Measurement) device independent protocols

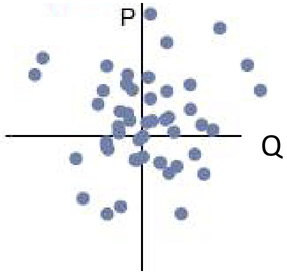
CV-QKD (one or two-way, Gaussian or discrete modulation, coherent or squeezed states, post selection), (Measurement) device independent protocols



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

Coherent state CV-QKD

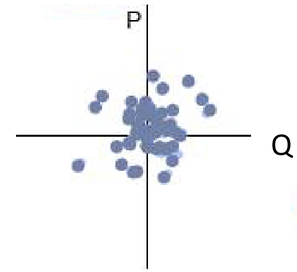




$$\{q_i \quad p_i, 1 \leq i \leq N\}$$

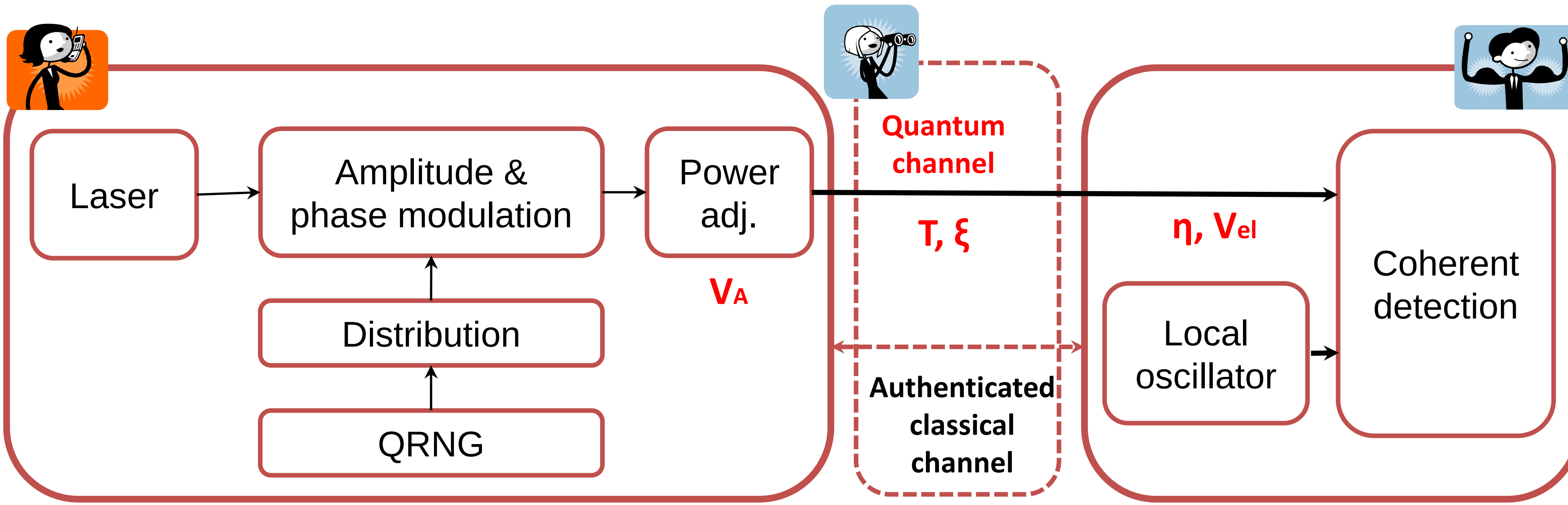
$$|\alpha\rangle_i = |q_i + ip_i\rangle$$

Gaussian modulation, QPSK, QAM,…



Single (homodyne) or double (heterodyne) quadrature detection

Trusted (calibrated) noise

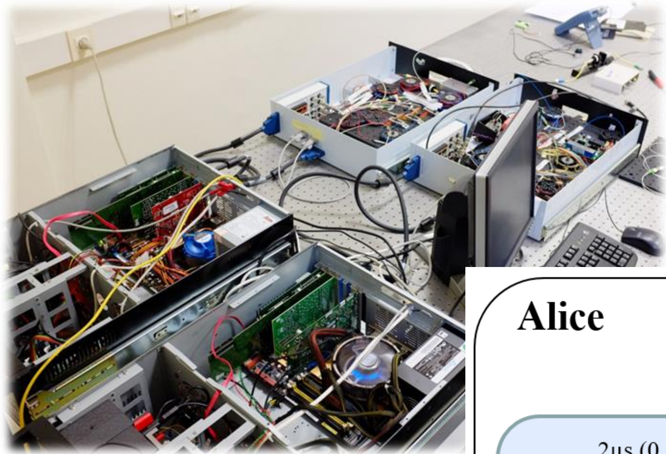


Composable, finite size security proof

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

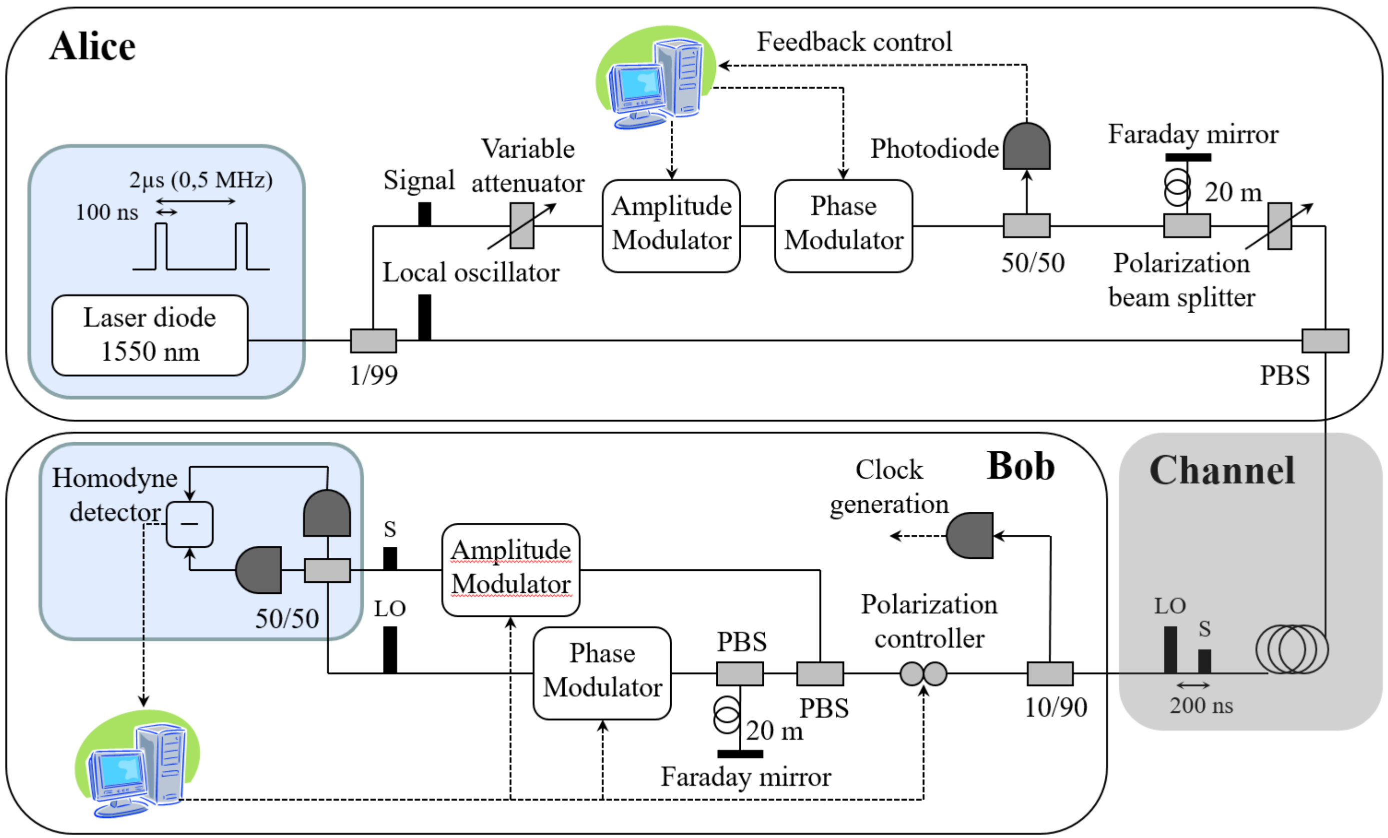
Classical post-processing: parameter estimation, error correction, privacy amplification

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

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

Transmitted LO

Pulsed operation

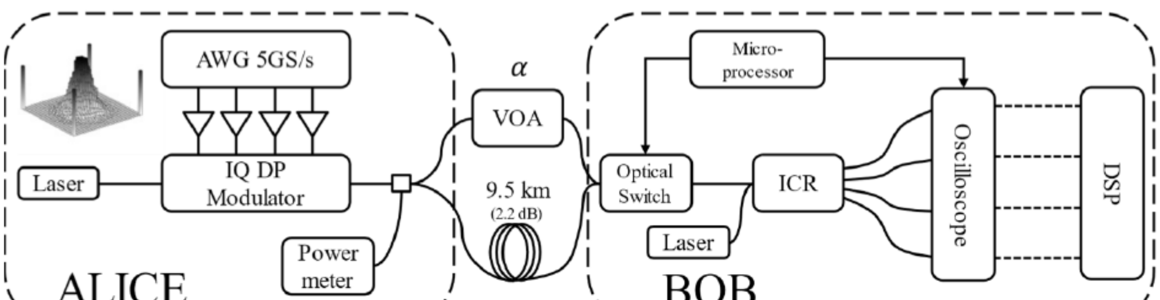
Homodyne detection

Gaussian modulation

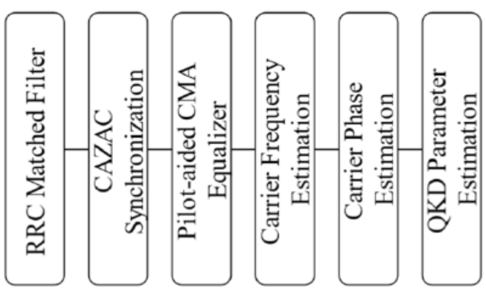
CW pulse shaping techniques: optimal use of spectrum, avoid inter-symbol interference, use of pilots, Digital Signal Processing developed for advanced coherent telecom systems

Integrated coherent receivers: shot noise limited, low noise, high bandwidth

PCS 1024-QAM, dual pol., Nyquist pulses, QPSK pilots, 400 Mbaud, 10 kHz lasers



(a)

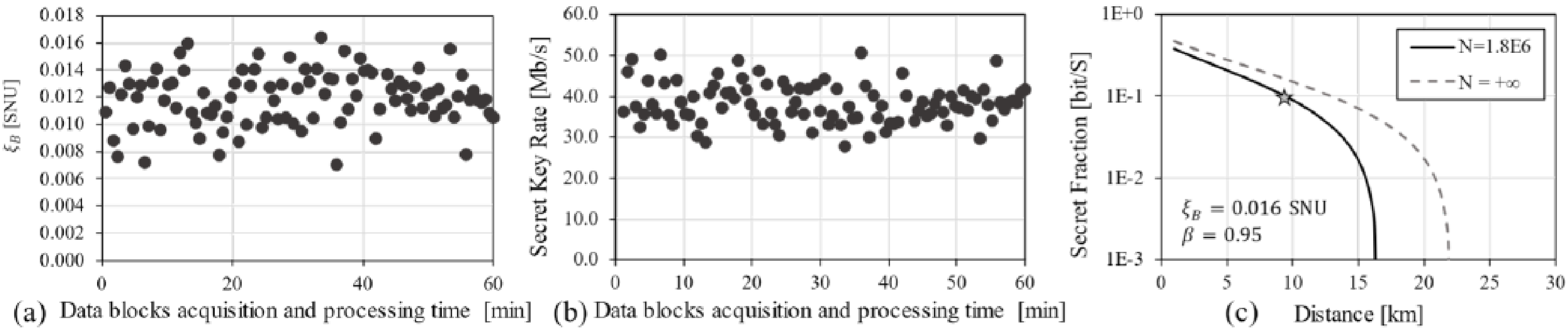


CiViQ

NOKIA Bell Labs

F. Roumestan *et al.*, OFC 2021

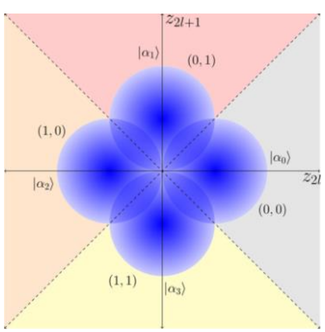
Bandwidth-efficient CV-QKD



F. Roumestan *et al.*, OFC 2021

Adapted to high secret key rates at moderate distance

Proper security analysis is crucial



Asymptotic security proof for QPSK

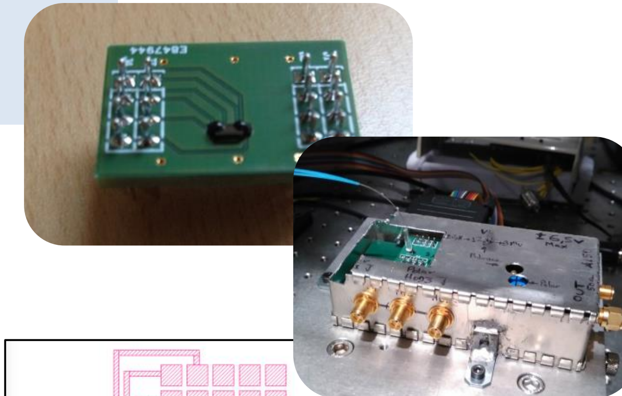
Extended to constellations of any cardinality

S. Ghorai, P. Grangier, ED, A. Leverrier, Phys. Rev. X 2019

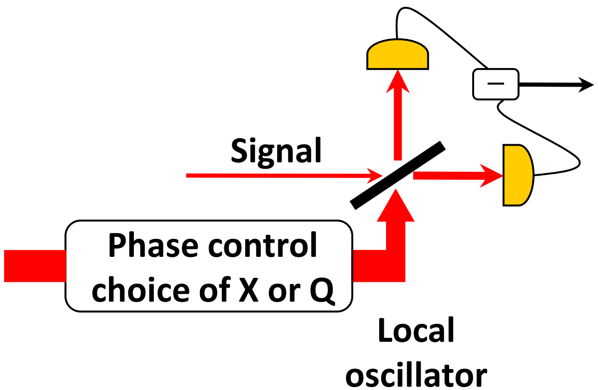
A. Denys, P. Brown, A. Leverrier, arXiv 2021

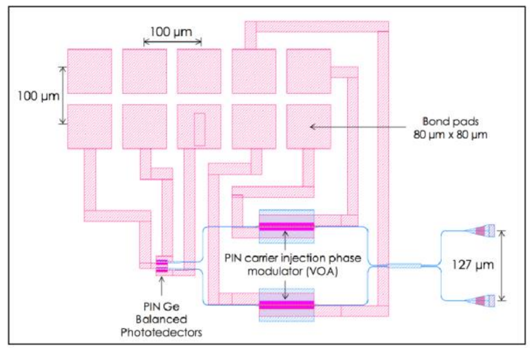
CV-QKD on chip

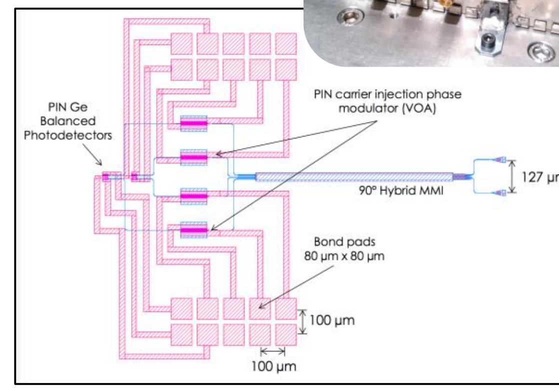
Challenge: **high cost**
Photonic integration for reduced cost and scalable solutions

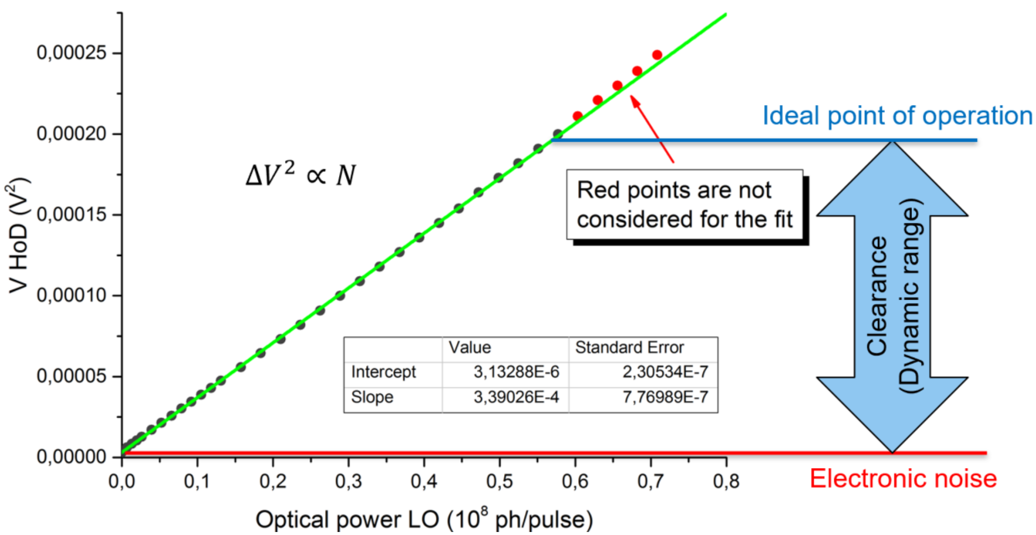


Silicon photonic chips (CEA-LETI)









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

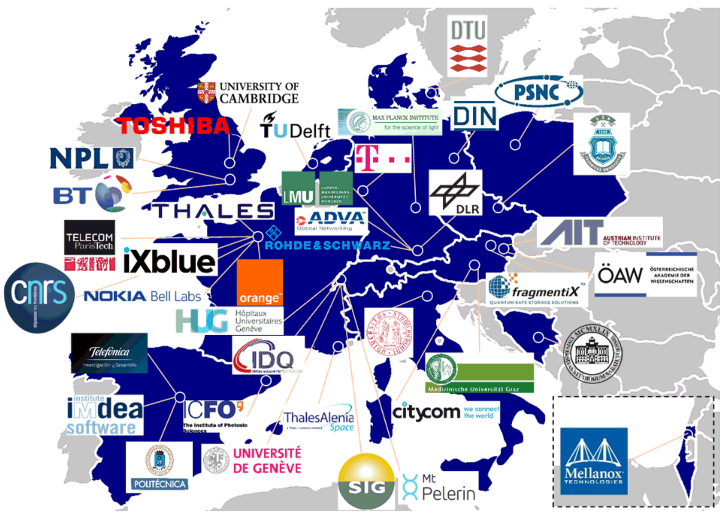
10 - 18 dB clearance

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

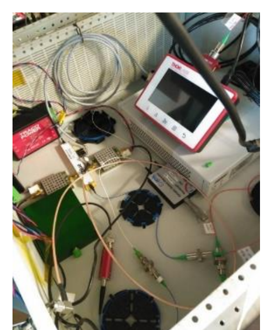


OPEN QKD

Academics, telecom operators, equipment providers, end users

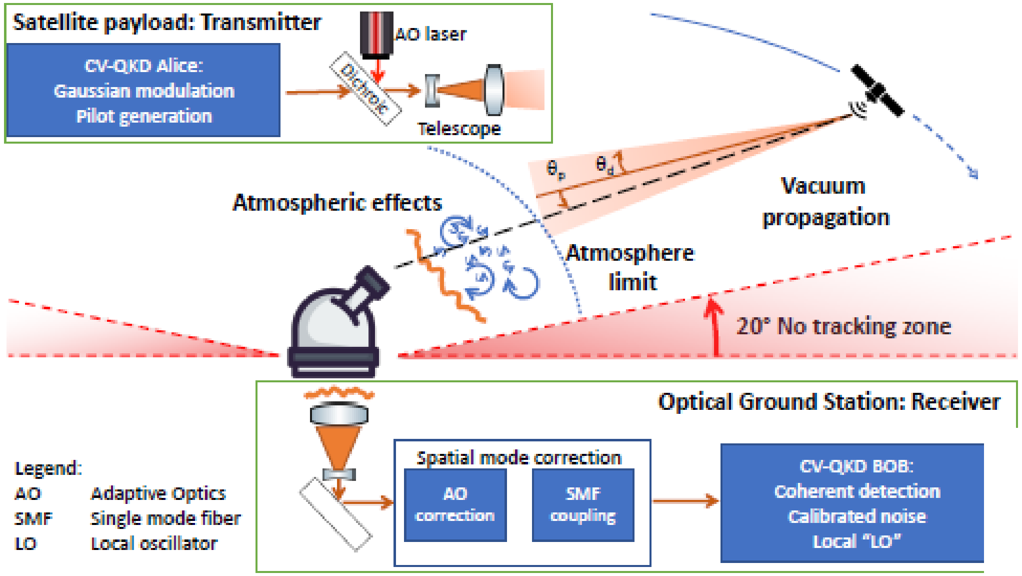
Data centres, electrical power grids, governmental communication, medical file transfer, critical infrastructure,…

High-speed FPGA solutions for prototype deployment in Paris testbed



iXblue

Feasibility of satellite-to-ground CV-QKD

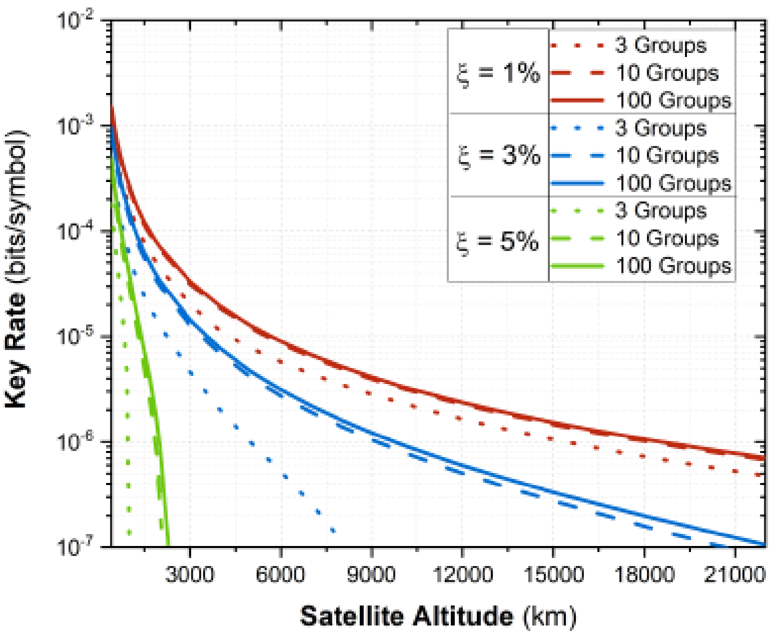


Compatible with space-certified telecom components

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

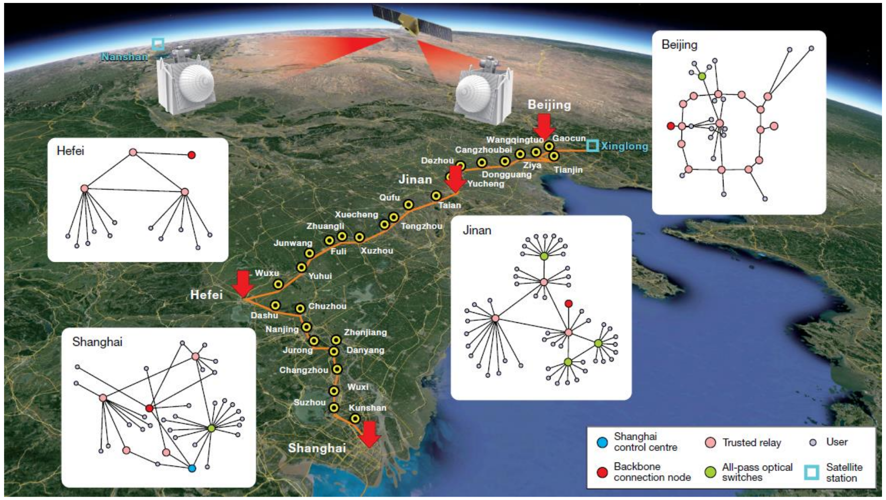
1 GHz, V_A = 1, $\beta = 0.95$, a = 0.75 m, pointing error 1 µrad, divergence angle 10 µrad, 3 dB fibre coupling loss

Agenzia Spaziale Italiana

Trusted node networks

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

Alice-R: key1, R-Bob: key2, R: key1$\oplus$key2 $\rightarrow$ Bob: key2$\oplus$(key1$\oplus$key2) = key1



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

EuroQCI program

Terrestrial and space segments

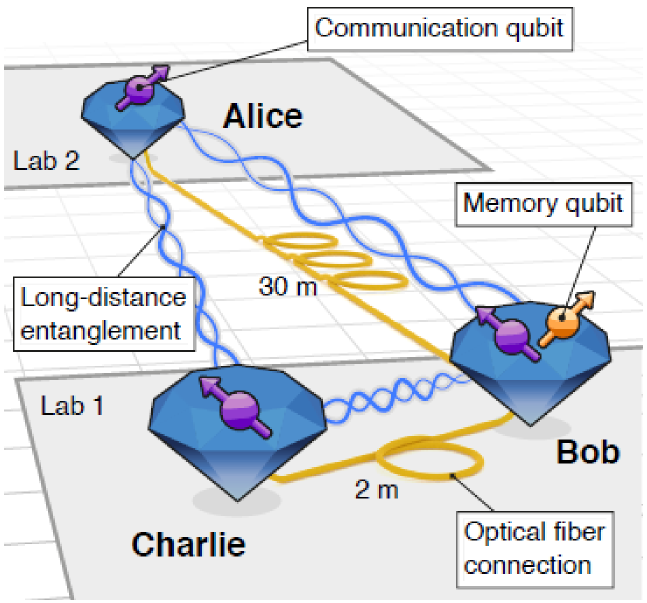
Focus on cost, range, network integration, quantum/classical coexistence, security, applications for the quantum internet, standards and certification

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



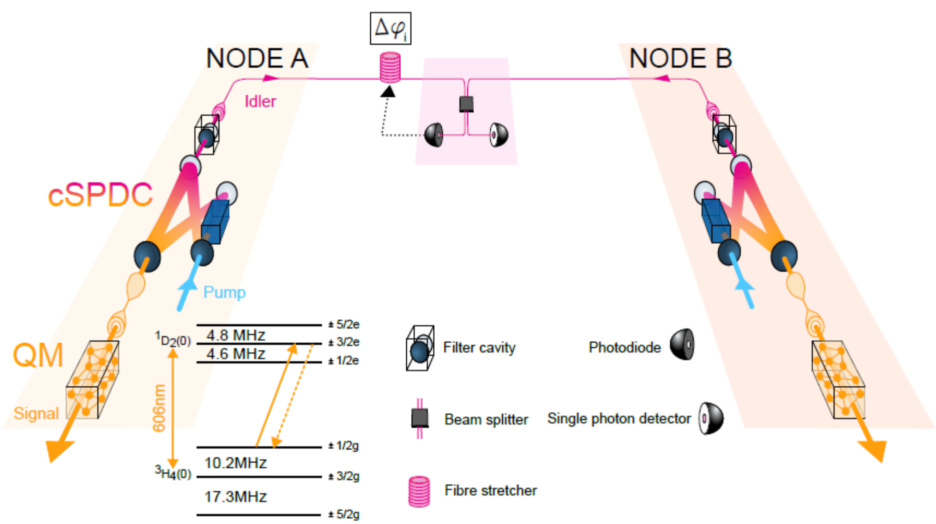
TU Delft, M. Pompili *et al.*, Science 2021

Challenges

Storage time and efficiency

Entanglement generation rates

Limited range



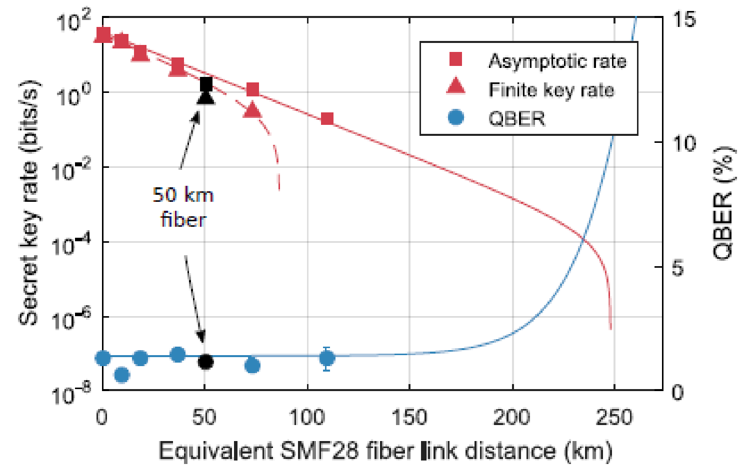
ICFO, D. Lago-Rivera *et al.*, Nature 2021

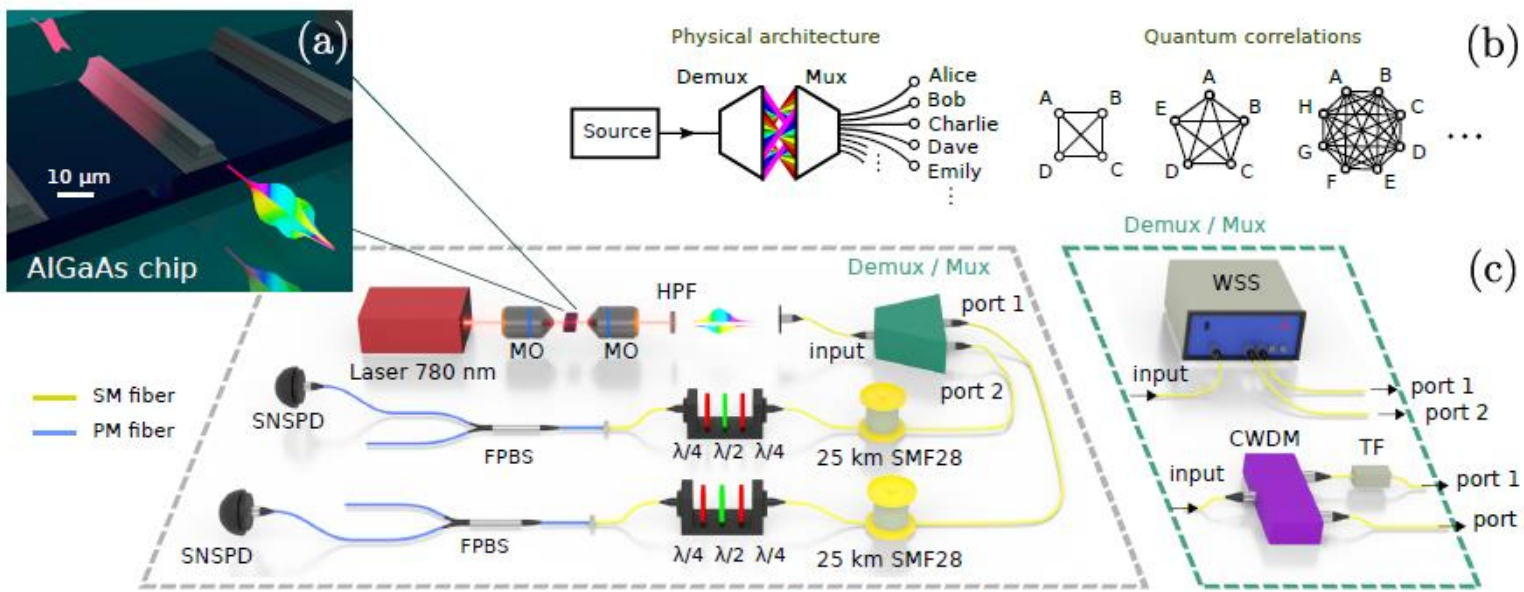
Near-term quantum network applications

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

Flexible entanglement distribution network for secure communication with a broadband source

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



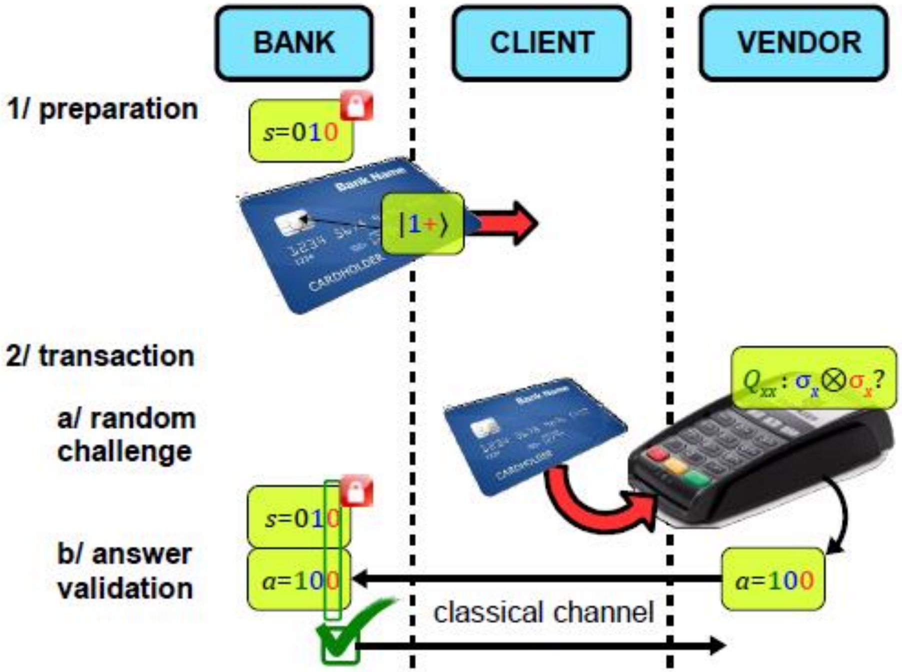


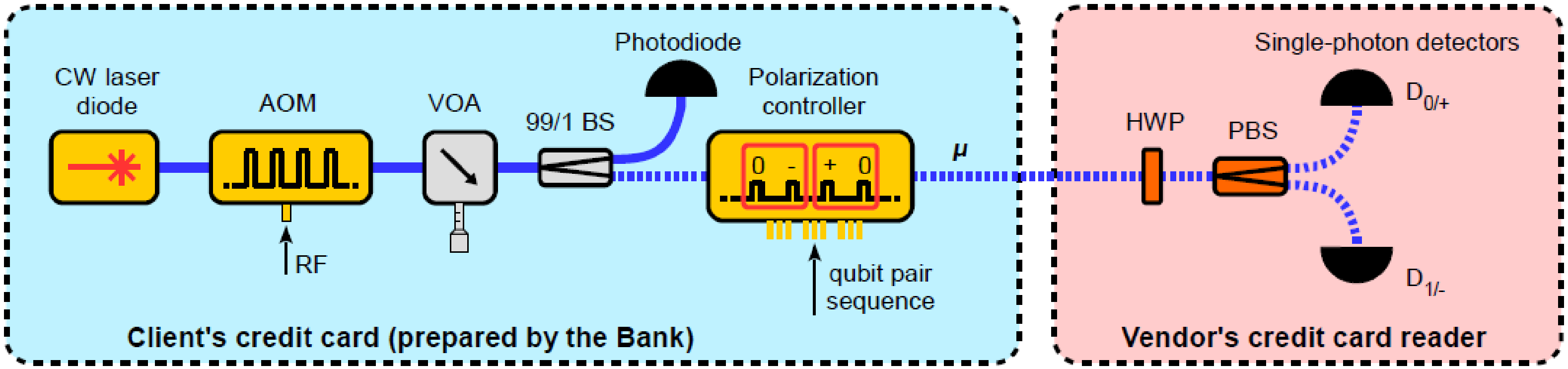
Unforgeable quantum money

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

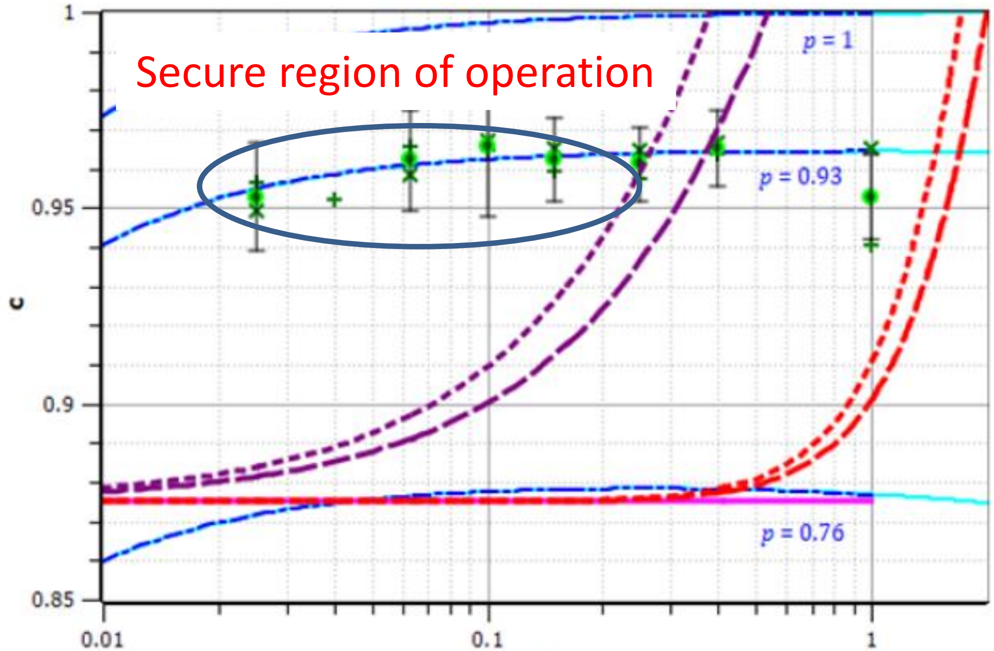
New protocol with classical verification and BB84-type states
Based on challenge questions





Unforgeable quantum money

Probability of answering the bank's challenge correctly →



Average number of photons per pulse → μ

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

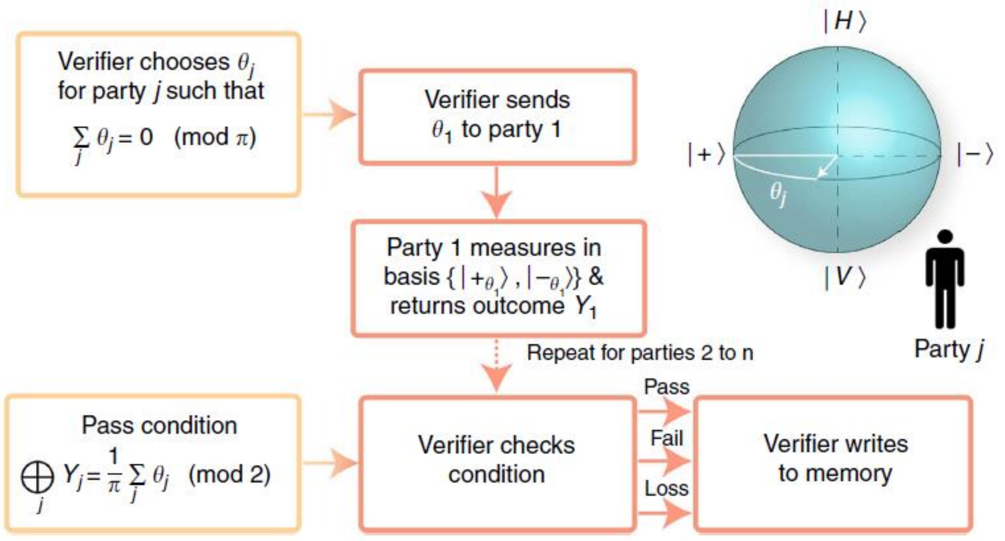
General security framework for weak coherent states and anticipating quantum memory
→ minimize losses and errors for both trusted and untrusted terminal

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

Entanglement verification

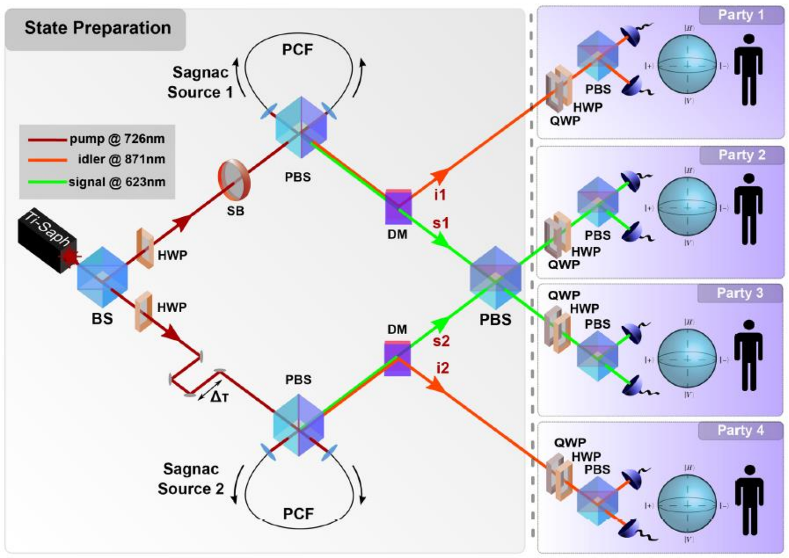
Proof-of-principle verification of multipartite entanglement in the presence of dishonest parties

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



Requires high performance resources

Very small loss tolerance



Application to anonymous message transmission

Verification phase guarantees anonymity

A. Unnikrishnan *et al.*, Phys. Rev. Lett. 2019

Quantum advantage in communication resources

Input **x**

Input **y**

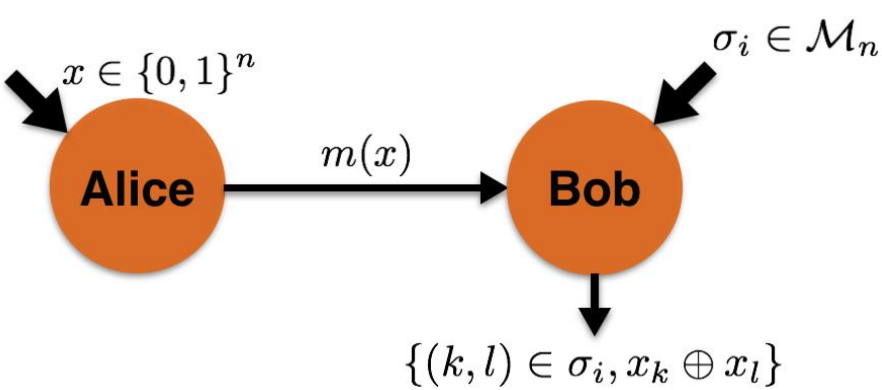
Goal: Output f(**x**,**y**)
with minimum communication

Communication complexity

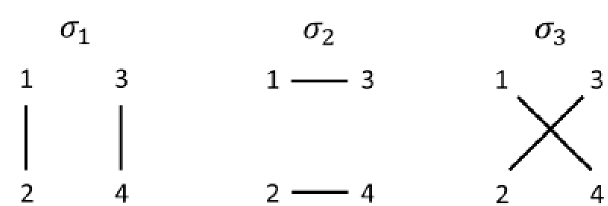
Amount of communication required for distant parties to jointly perform a distributed task

Applications in VLSI design, Data structures, Secure Computation,…

Hidden Matching



$$\mathcal{M}_4 = \{\sigma_1, \sigma_2, \sigma_3\}$$



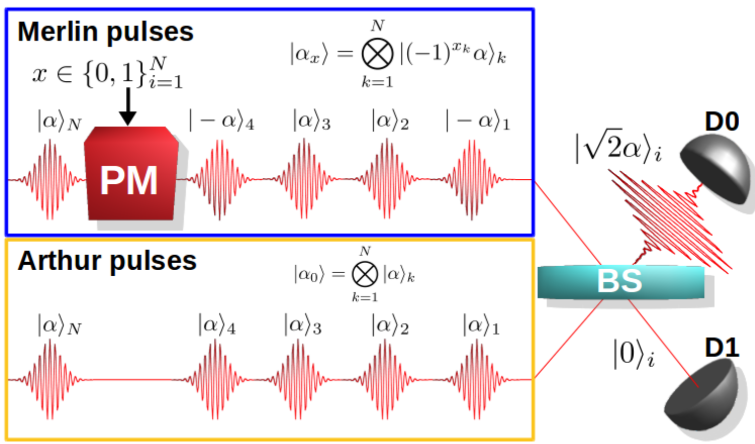
Exponential advantage $O(\sqrt{n})$ vs. $O(\log n)$

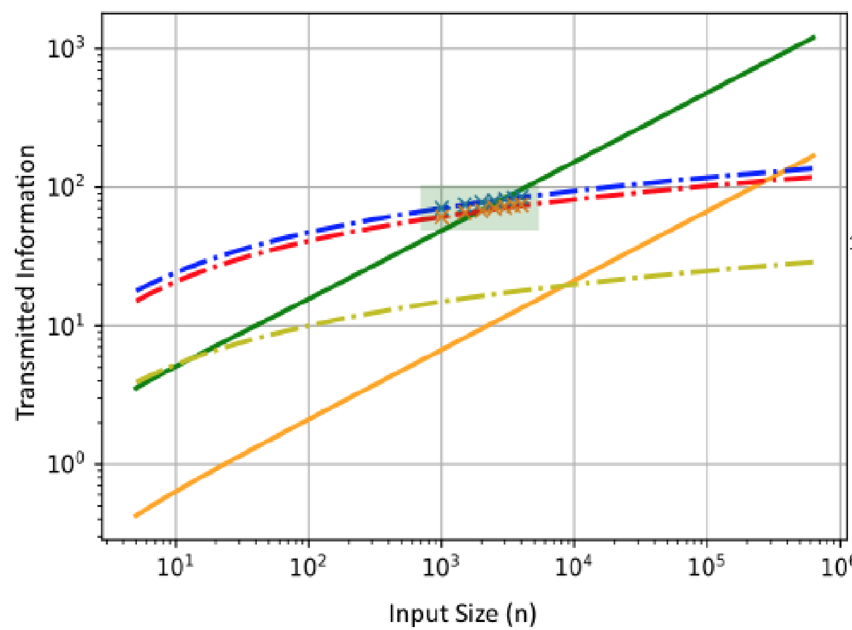
Coherent state mapping $|\phi_z\rangle = \sum_{i=1}^{n} z_i |i\rangle \longrightarrow |\alpha_z\rangle = \bigotimes_{i=1}^{n} |z_i \alpha\rangle_i$

One-to-one equivalence keeping the exponential gap but with worse communication time

Coherent state manipulation, linear optic circuits, single-photon detection

J. M. Arrazola and N. Lütkhenhaus, Phys. Rev. A 2014





Quantum advantage in one-way communication complexity for Sampling Matching

Application in efficient verification of NP-complete problem proofs with limited information

N. Kumar *et al.*, Nature Commun. 2019 & F. Centrone *et al.*, Nature Commun. 2021

Conclusion and perspectives

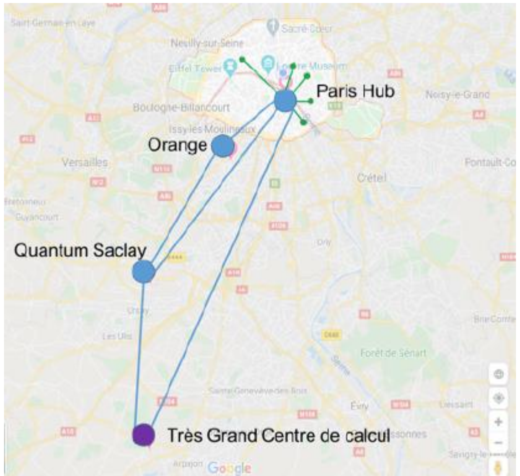
Quantum communication networks will be part of the future quantum-safe communication infrastructure

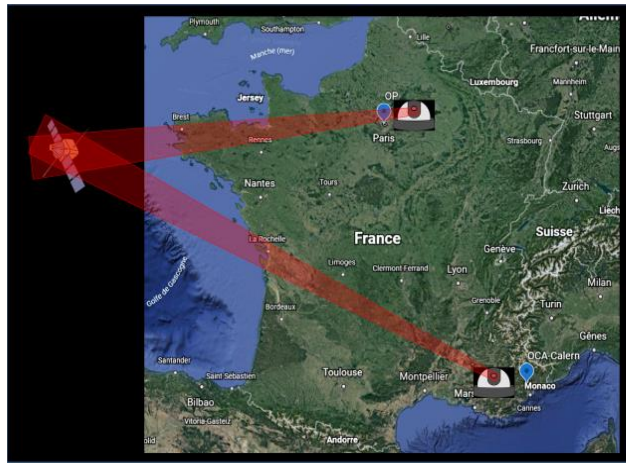
Such an infrastructure can address a range of use cases with high security requirements in multiple configurations

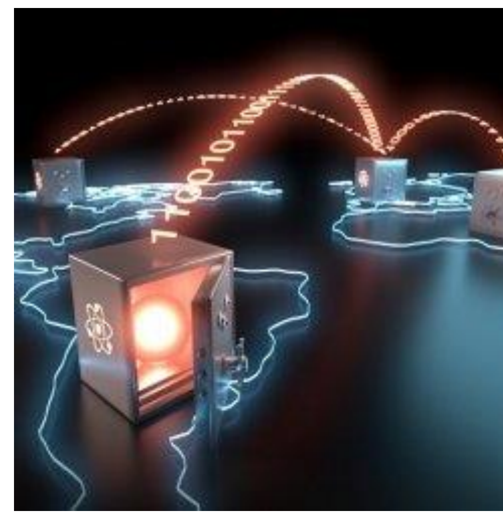
The quantum communication toolbox is rich and increasingly advanced

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