Practical challenges in quantum cryptography

Eleni Diamanti

Laboratoire d'Informatique de Paris 6

CNRS, Sorbonne Université

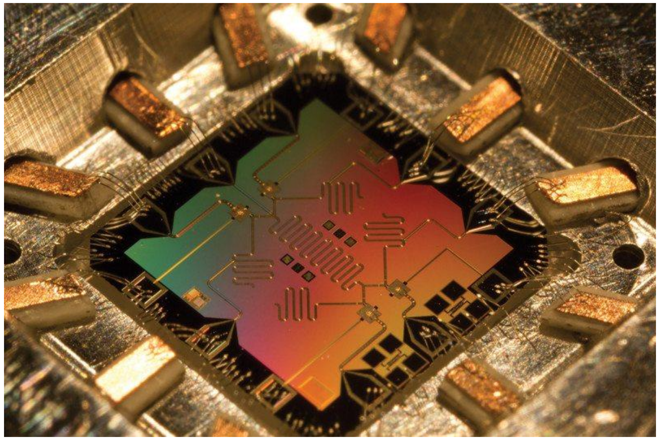
LLR Seminar, December 17, 2018

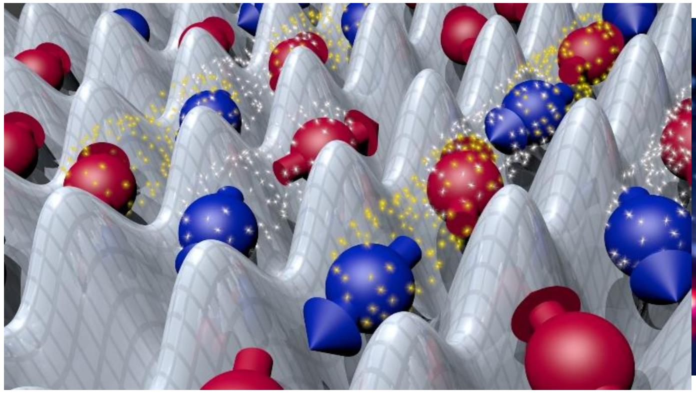
Quantum technologies

The second quantum revolution will bring technologies offering an advantage in security, communication efficiency, computational power, measurement precision and simulation of complex systems

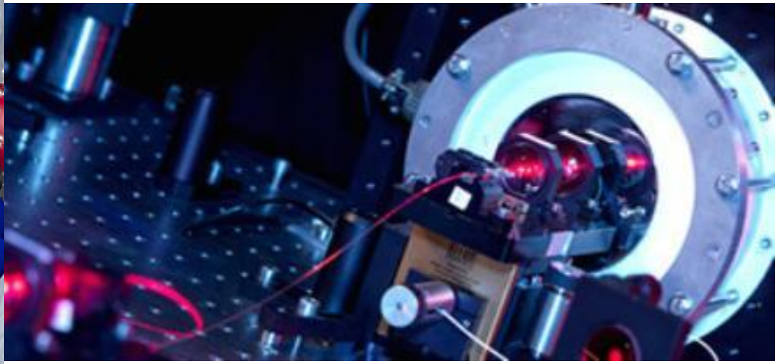
Quantum communication

Quantum computing





Quantum simulation



Quantum metrology and sensing

Quantum communication networks

Photonic resources
Encoding in single-photon or electromagnetic field properties
Propagation in optical fibre or free-space channels
Computation in network nodes (processors, memories)

Security
Untrusted network users, devices, nodes

Efficiency
Optimal use of communication resources

Applications
Realistic conditions for communication and distributed computing protocols
Implementations with provable quantum advantage in security or efficiency

Securing network links: quantum key distribution

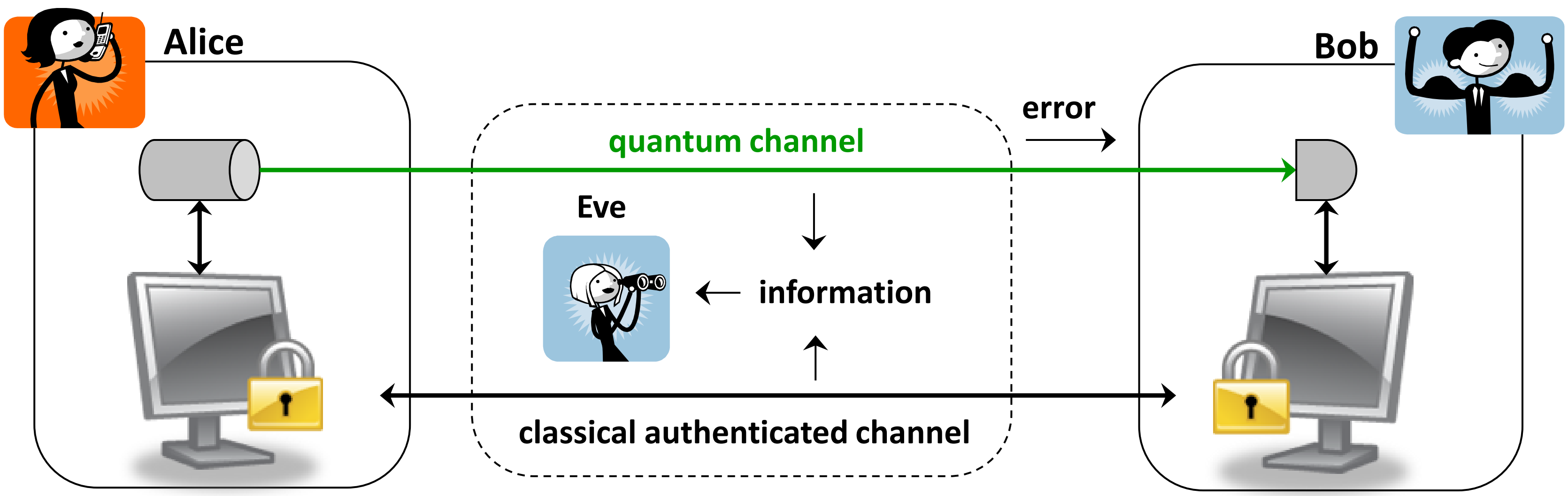
Modern cryptography

Symmetric cryptography	Security relies on secrecy of a private encryption key One-time pad gives **unconditional security** Key distribution problem!
Asymmetric (public-key) cryptography	Provides **computational security**, based on hardness of specific mathematical problems, e.g. factoring Vulnerable to future attacks, e.g. by a quantum computer
Post-quantum cryptography	Classical algorithms exploiting advanced mathematical problems, e.g. lattices, elliptical curves,… : NIST call Unknown resilience to future attacks Still provide **computational security**

Quantum key distribution provides a future-proof, unconditionally secure solution to the key distribution problem for secure message exchange between two trusted parties

Principle of quantum key distribution

QKD allows secret message exchange with information-theoretic security
→ guaranteed against an all-powerful eavesdropper

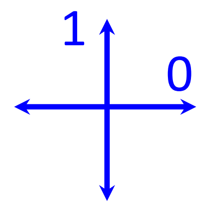


Key information is encoded in photonic carriers

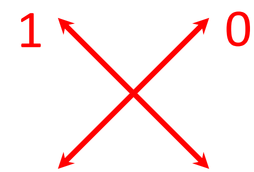
Analysis of errors due to Eve's measurements leads to secret key

The BB84 protocol

Information is encoded in the polarization of single photons using two non-orthogonal bases

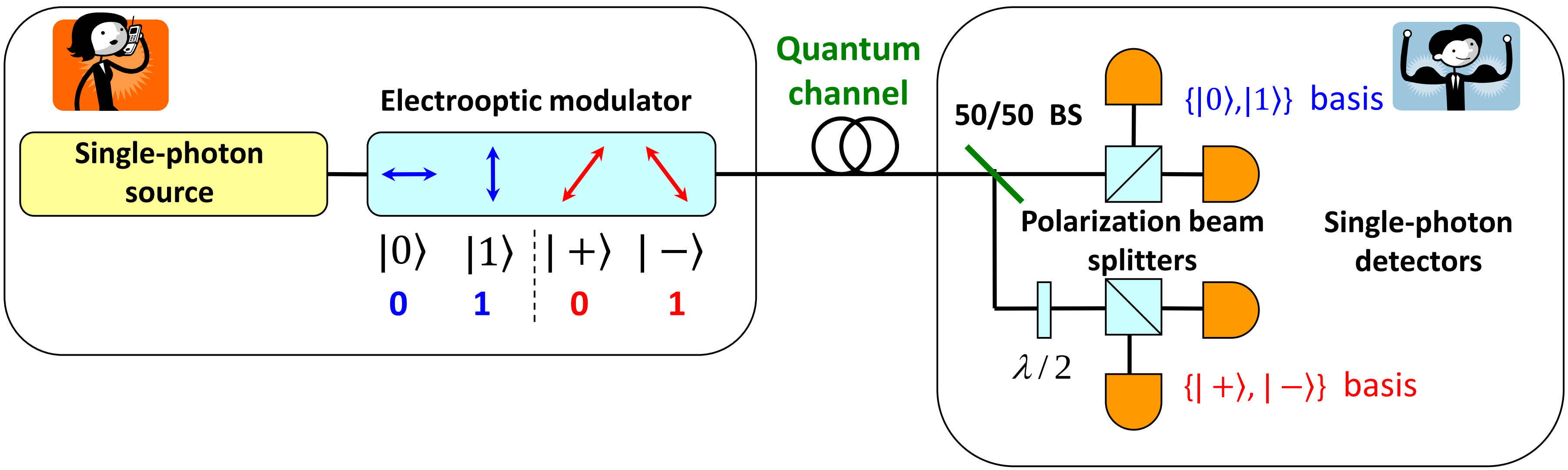


$\{|0\rangle, |1\rangle\}$ basis



$\{|+\rangle, |-\rangle\}$ basis

In practice, the system of Alice and Bob could be like this:



Remarks

- Security is obtained from the no cloning theorem for non-orthogonal states

- Entanglement-based QKD protocols derive their security from violation of a Bell inequality

  $\rightarrow$ signature of non-local correlations shared between Alice and Bob

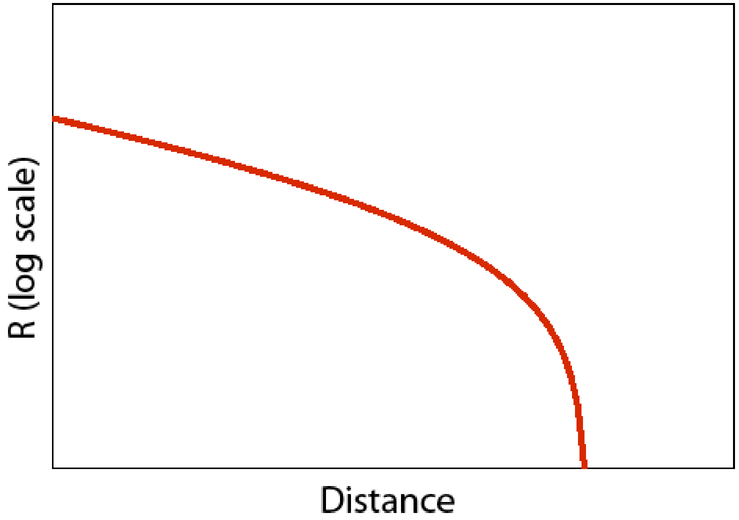
- Following the quantum transmission part of the protocol, classical post-processing algorithms are used to extract the secret key

- Security proofs take into account a range of eavesdropping attacks

  individual $\rightarrow$ collective $\rightarrow$ coherent (unconditional security)

Practical imperfections

All practical systems present imperfections: losses, errors, finite quantum efficiency and dark counts of single-photon detectors…



Using a coherent light source instead of a single-photon source opens a security loophole for BB84 and degrades performance
$\rightarrow$ photon number splitting attacks

G. Brassard, N. Lütkenhaus, T. Mor, B. Sanders, Phys. Rev. Lett. 2000

Solution: use ‘decoy’ states
Alternatively, encode information on properties of coherent states $\rightarrow$ CV-QKD

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

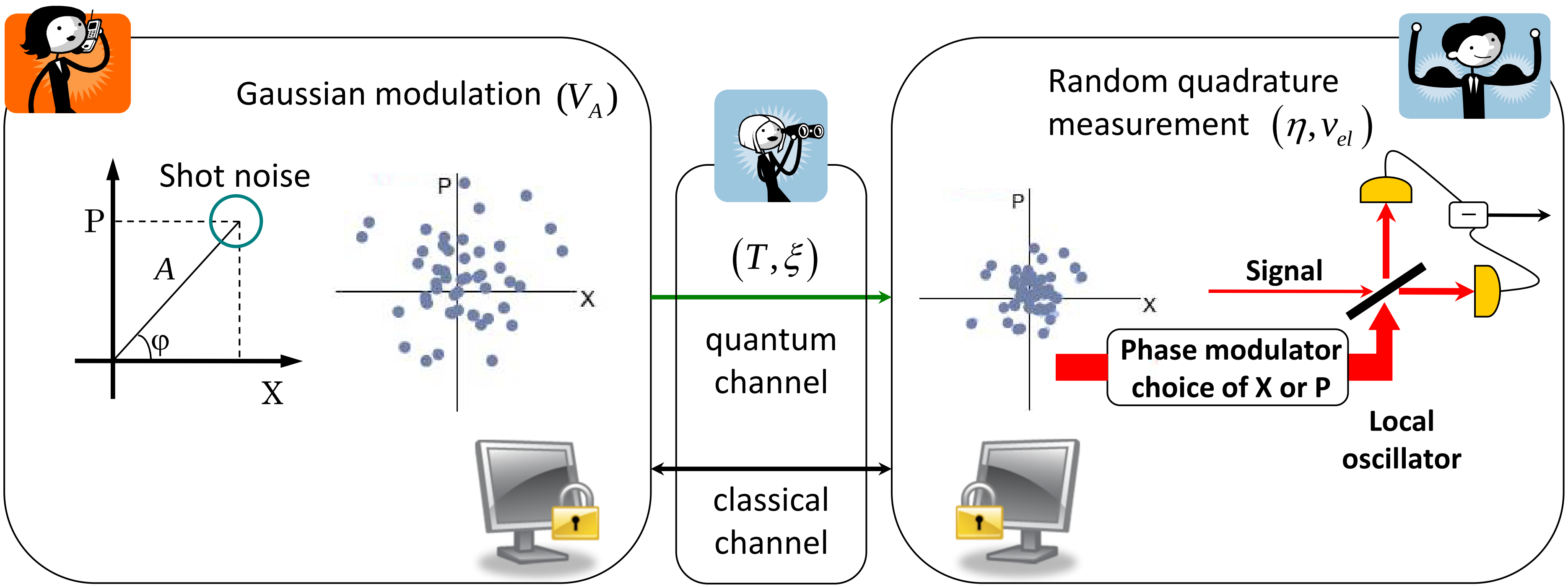
BB84, Decoy state, Coherent One Way, Differential Phase Shift, (M)DI protocols

CV-QKD (one or two-way, Gaussian or discrete modulation, coherent or squeezed states, post selection), (M)DI protocols

V. Scarani et al, Rev. Mod. Phys. 2009
E. Diamanti and A. Leverrier, Entropy 2015

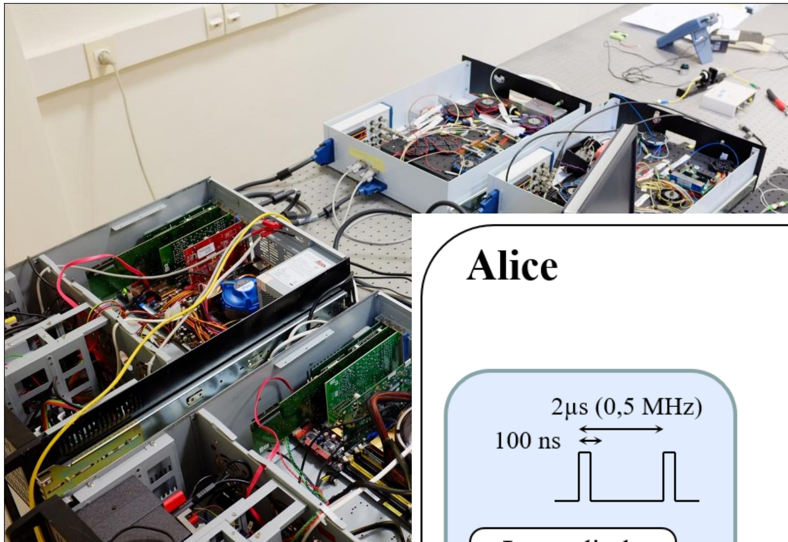
Coherent state CV-QKD

- Alice encoding: random modulation of amplitude and phase of coherent states
- Bob measurement: random choice of quadrature of each coherent state with a homodyne detection system

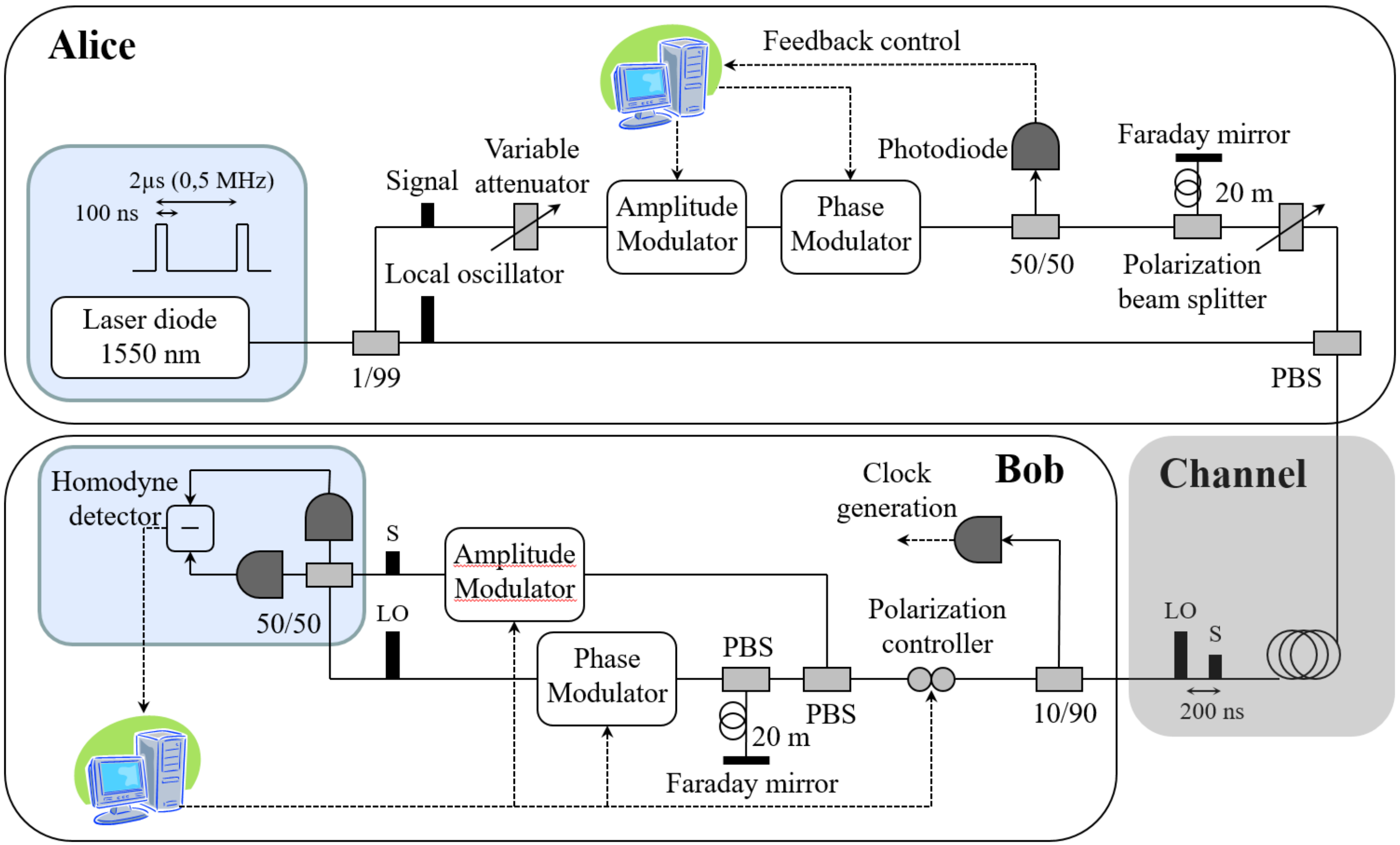


F. Grosshans et al, Nature 2003

System and main progress

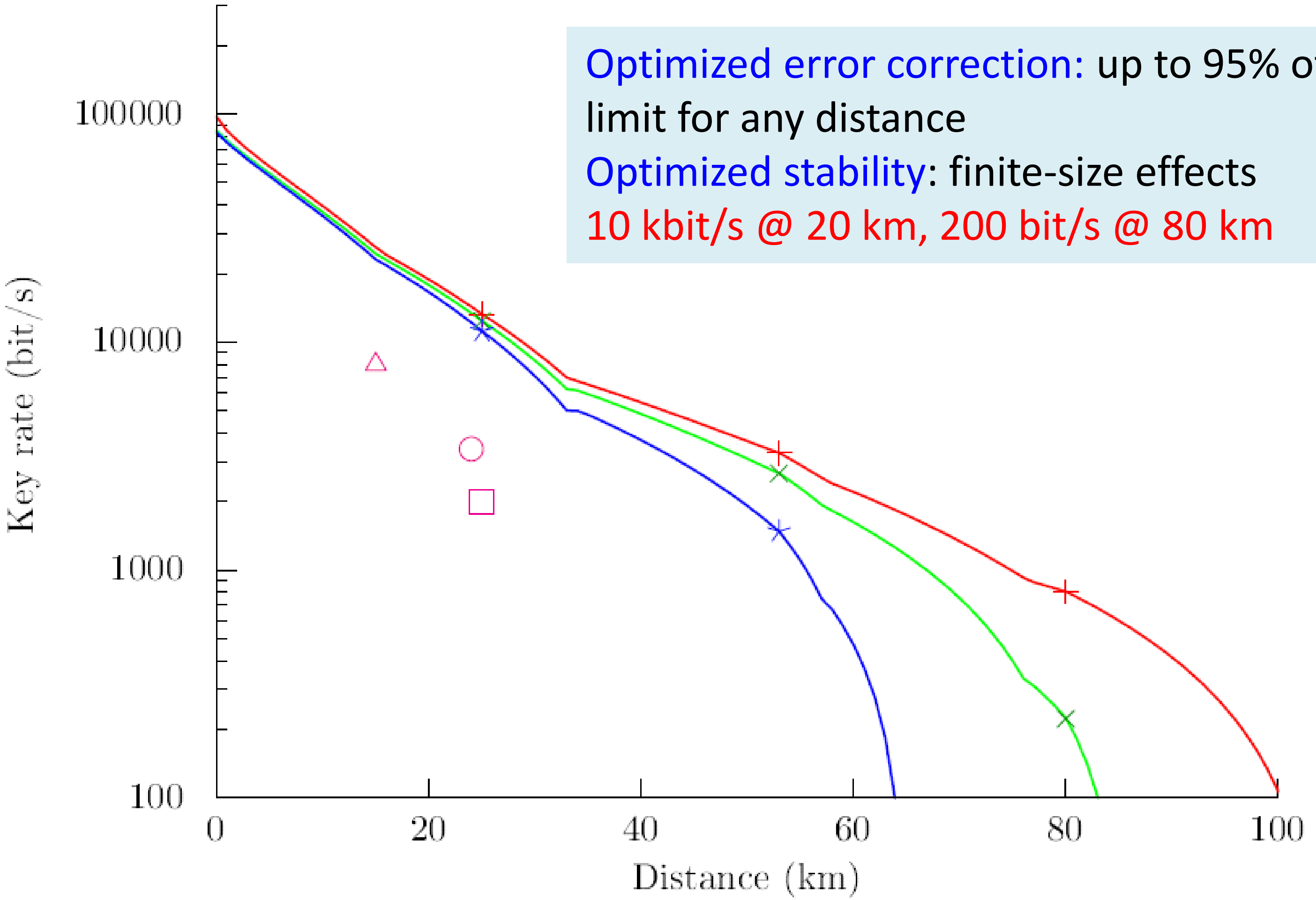


No single-photon detection
Only standard telecom components



SECOQC QKD network – S. Fossier et al, New J. Phys. 2009
Field test with classical encryption – P. Jouguet et al, Opt. Express 2012
Side channel attack analysis – P. Jouguet et al, Phys. Rev. A 2012, 2013

Long-distance CV-QKD



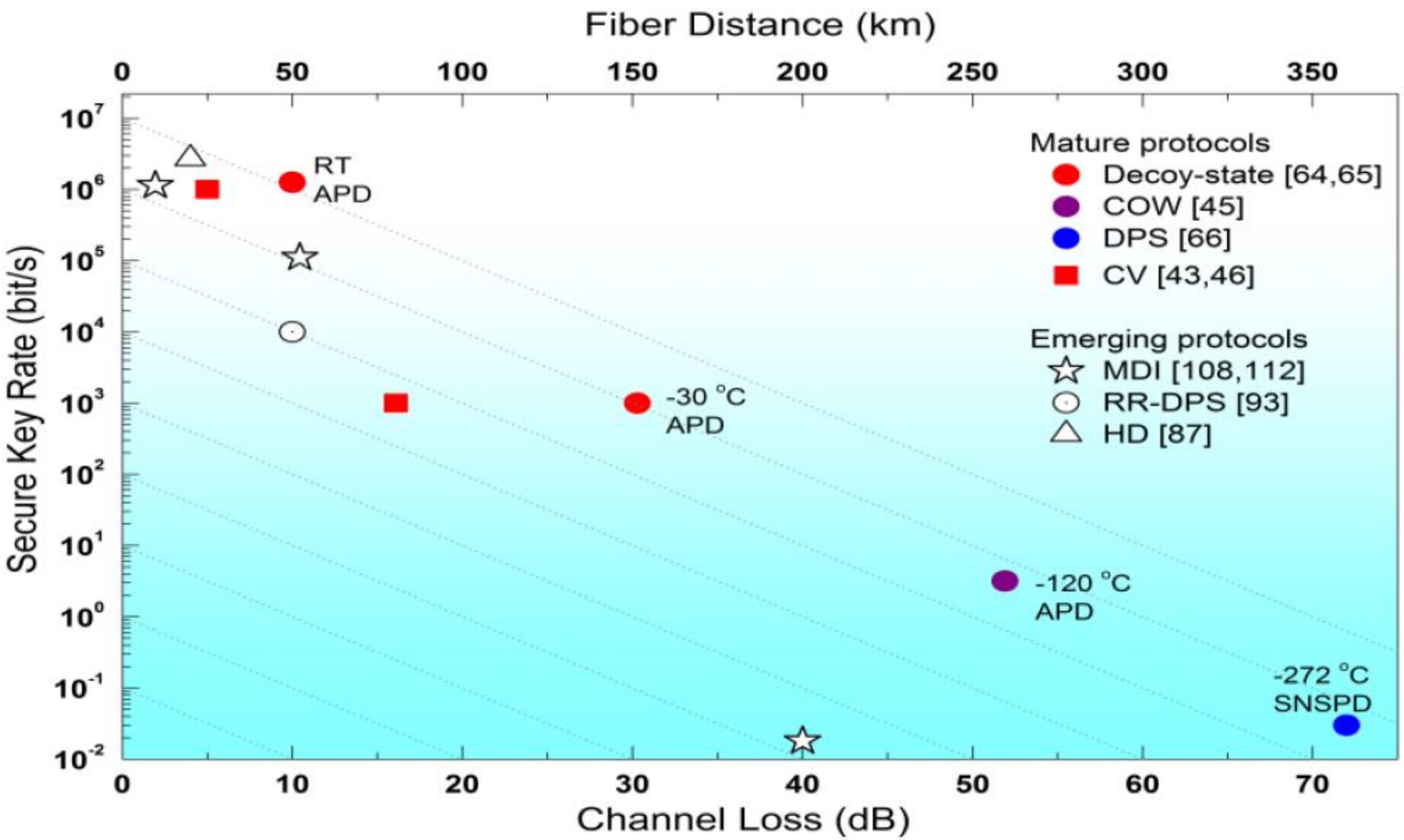
Optimized error correction: up to 95% of Shannon's limit for any distance

Optimized stability: finite-size effects

10 kbit/s @ 20 km, 200 bit/s @ 80 km

P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, E. Diamanti, Nature Photon. 2013

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



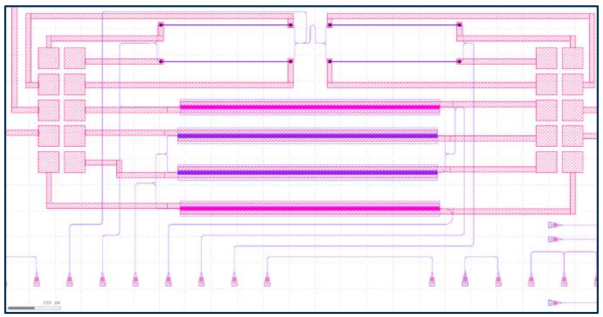
E. Diamanti, H.-K. Lo, B. Qi, Z. Yuan, npj Quantum Information 2016

Addressing practical challenges in QKD

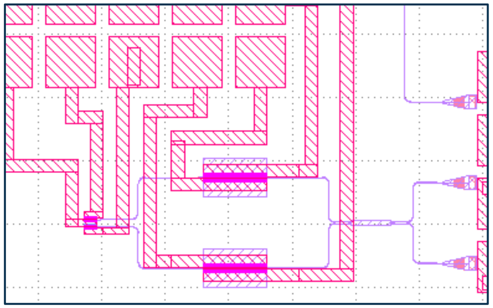
High cost

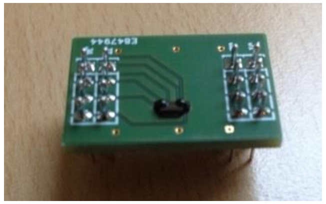
Photonic integration for reduced cost and scalable solutions

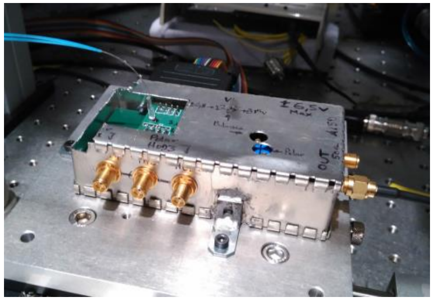
Alice

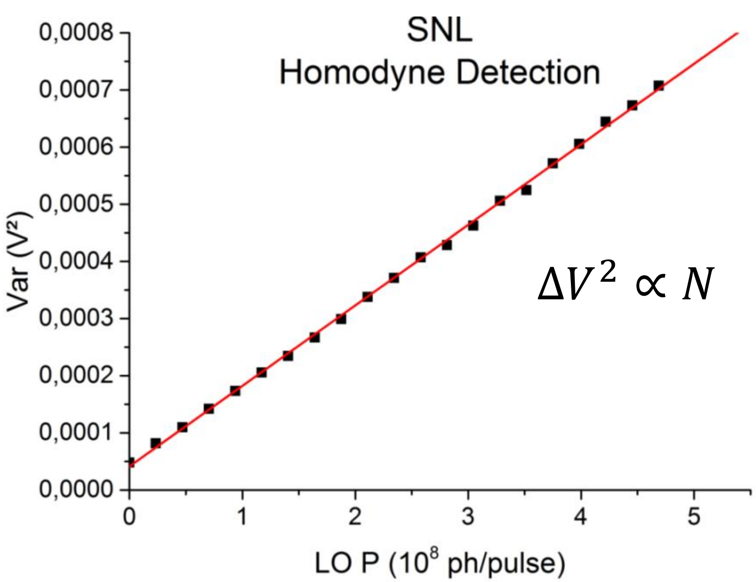


Bob









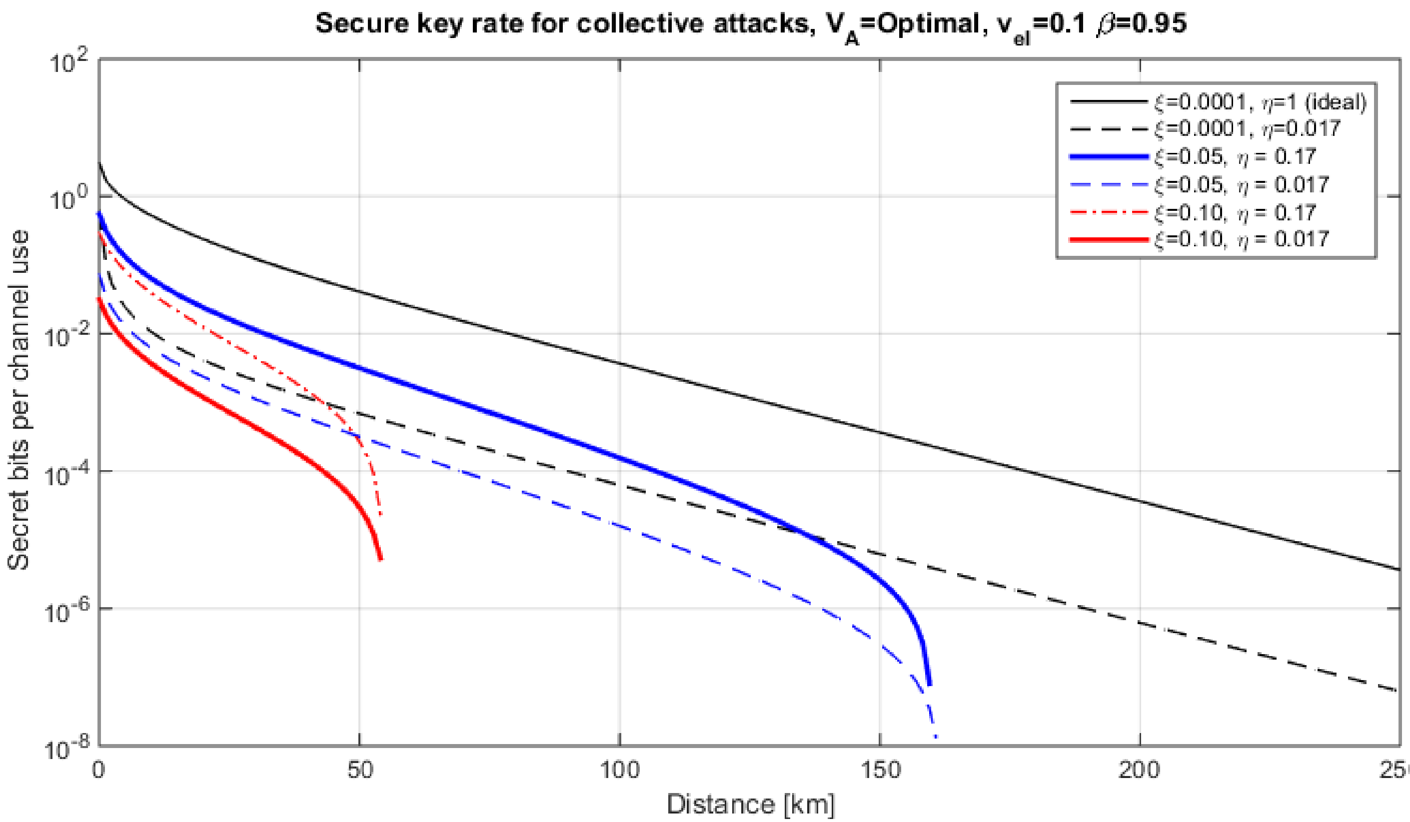
Si chips from LETI

Other chips from OPSIS, IME Foundry and Columbia University, AIM Foundry

Shot-noise limited silicon-integrated homodyne detection for CV-QKD
10 - 18 dB clearance

M. Persechino, L. Trigo Vidarte et al, QCrypt 2018

CV-QKD on chip



Secret key rate determined mainly by η and T

Maximal distance determined by ξ and reconciliation efficiency β

Ongoing characterization of Alice chip for complete integration

M. Persechino, L. Trigo Vidarte et al, QCrypt 2018

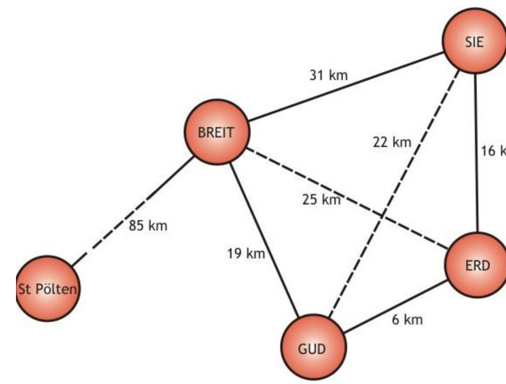
Overcoming channel losses

Going beyond point-to-point links towards secure quantum networks

Mesh trusted node networks

SECOQC QKD network, 2008
Durban South Africa network, 2010
Swiss Quantum Network, 2011
Tokyo QKD network, 2015
UK QC Hub (Cambridge)
China 2000 km, 60-node network
Planned testbed infrastructure in Europe

Currently available technology

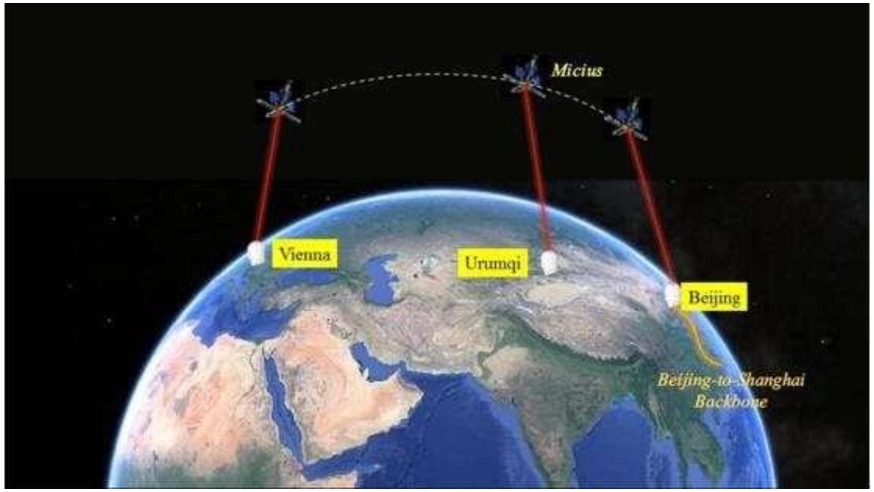


Networks with untrusted nodes

Network nodes with few-qubit processors, memories
Quantum repeaters, multiparty photonic resources

- beat direct transmission
- improve rates
- develop full network and software stack for applications

Overcoming channel losses



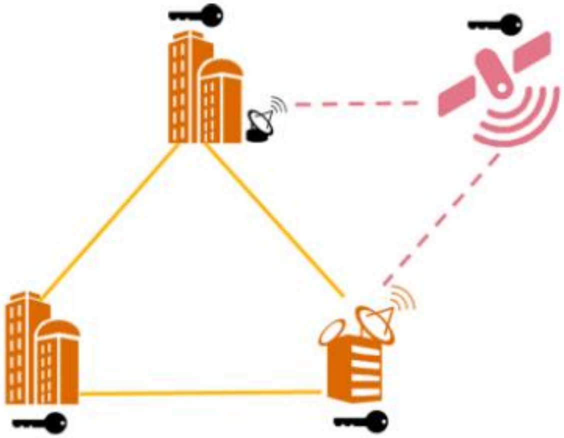
Nature & Science 2017

China's Micius satellite first to be equipped with quantum technologies

- Down-link QKD
- Up-link quantum teleportation
- Entanglement distribution
- Videoconferencing across the globe in trusted node-satellite model

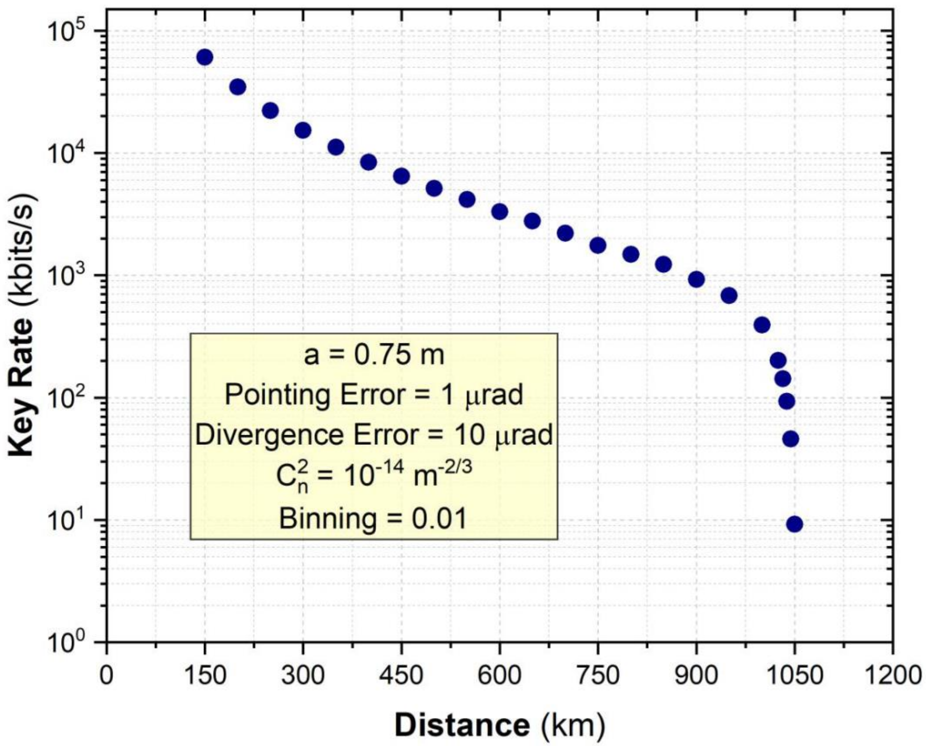
Canada, Japan, Singapore, France, UK, Germany,…
European Space-QUEST initiative: Fundamental physics and quantum communications

S. Joshi et al, New J. Phys. 2018



Long-term vision
Interconnected ground networks located anywhere on Earth, linked by satellites

Feasibility of CV-QKD in space



Preliminary results for positive secret key rate for Low Earth Orbit – ground link, including effects of pointing, beam divergence, turbulence, optical losses (binning of transmission efficiency), satellite orbit…

D. Dequal, L. Trigo Vidarte, V. Roman Rodriguez et al, 2018

Univ. Padova, Matera Laser Ranging Observatory

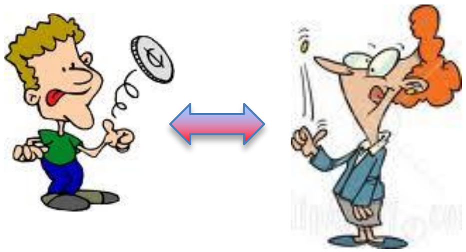
ThalesAlenia Space
a Thales / Leonardo company

Quantum advantage for other cryptographic tasks

Key distribution is central paradigm in the trusted two-party security model

In other security models many more functionalities

Playground for demonstrating quantum advantage



Bit commitment, coin flipping, oblivious transfer, digital signatures, position-based cryptography, secure identification, quantum money,…

Secret sharing, entanglement verification, authenticated teleportation, anonymous communication,…

Random number generation, communication complexity,…

Main challenges

Perfect protocols often impossible

'Expensive' resources

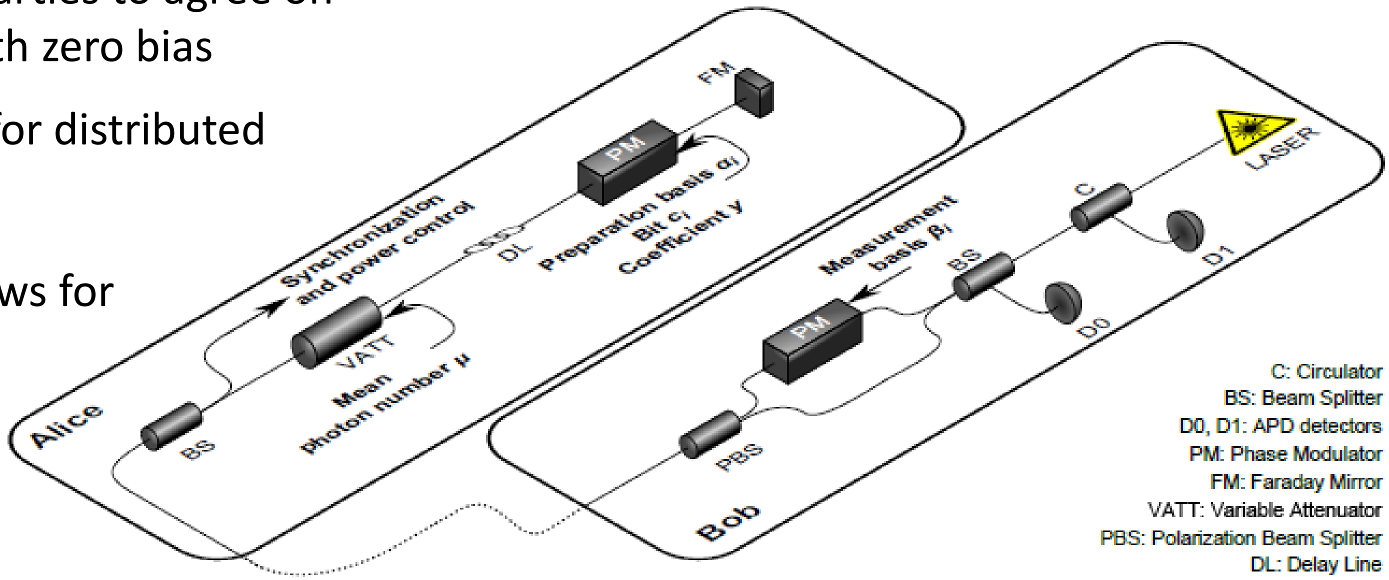
Vulnerability to experimental imperfections

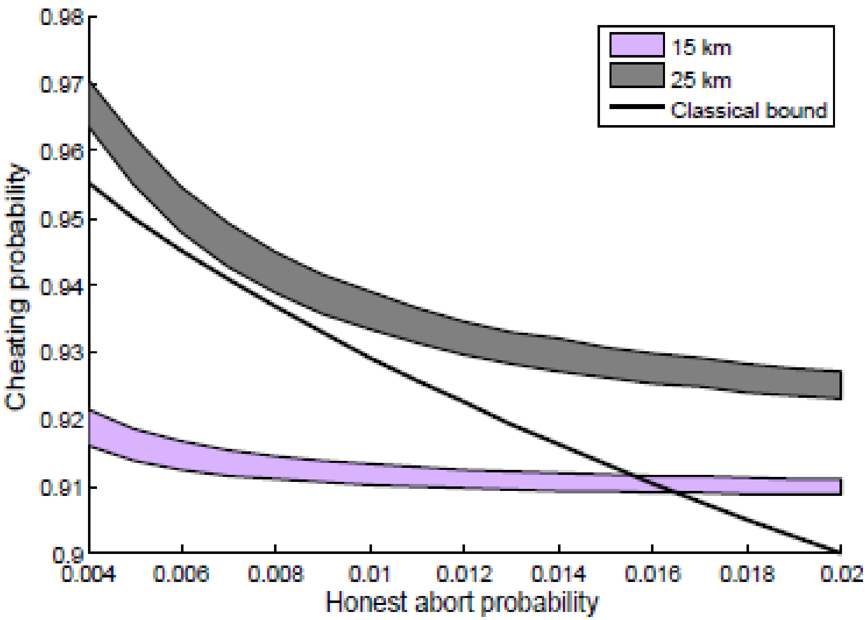
Quantum coin flipping

Allows two distrustful parties to agree on a random bit, ideally with zero bias

Fundamental primitive for distributed computing

Theoretical analysis allows for honest abort to include imperfections





DV-QKD-like plug and play system

Quantum advantage for metropolitan area distances

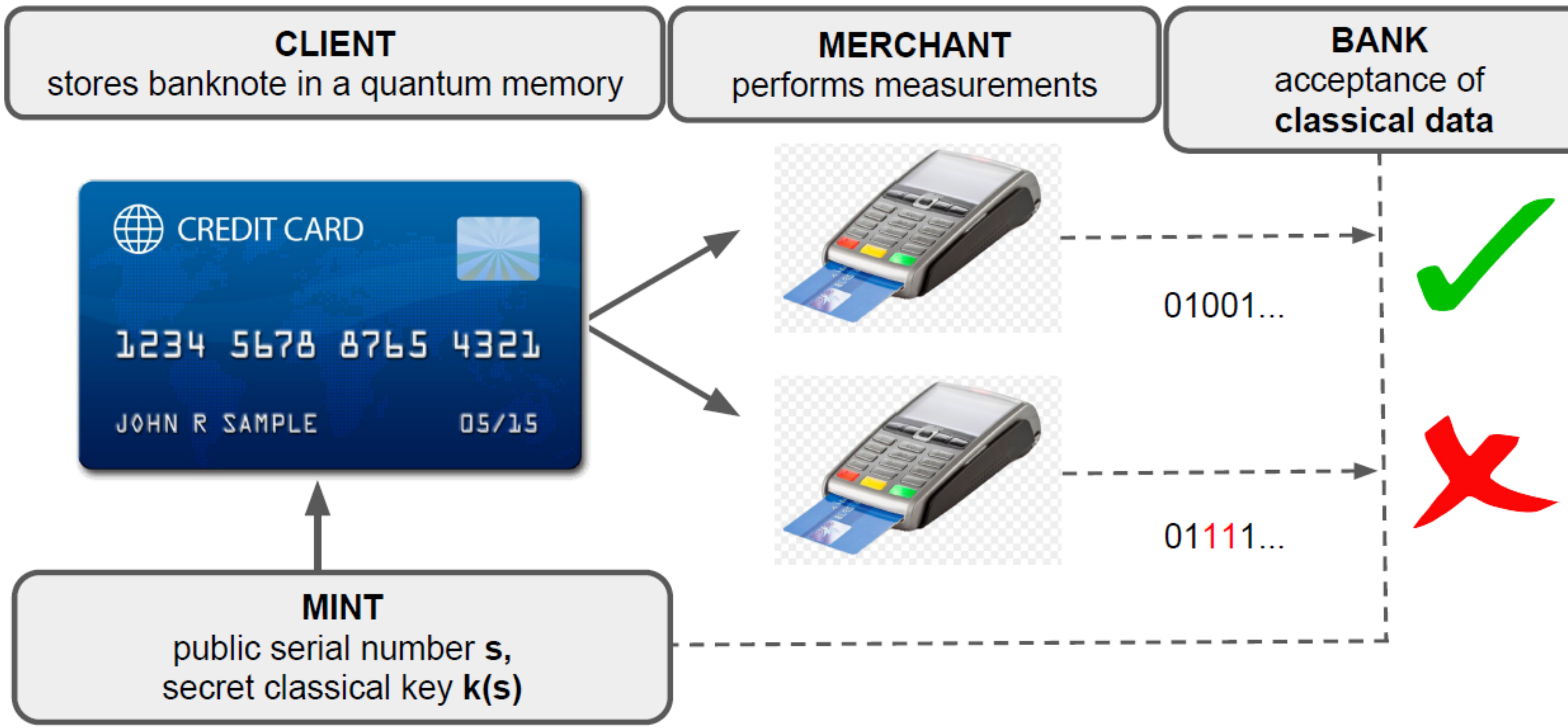
A. Pappa et al, Nature Commun. 2014

Unforgeable quantum money

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

But requires quantum verification and quantum memories
Was considered impossible to implement

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



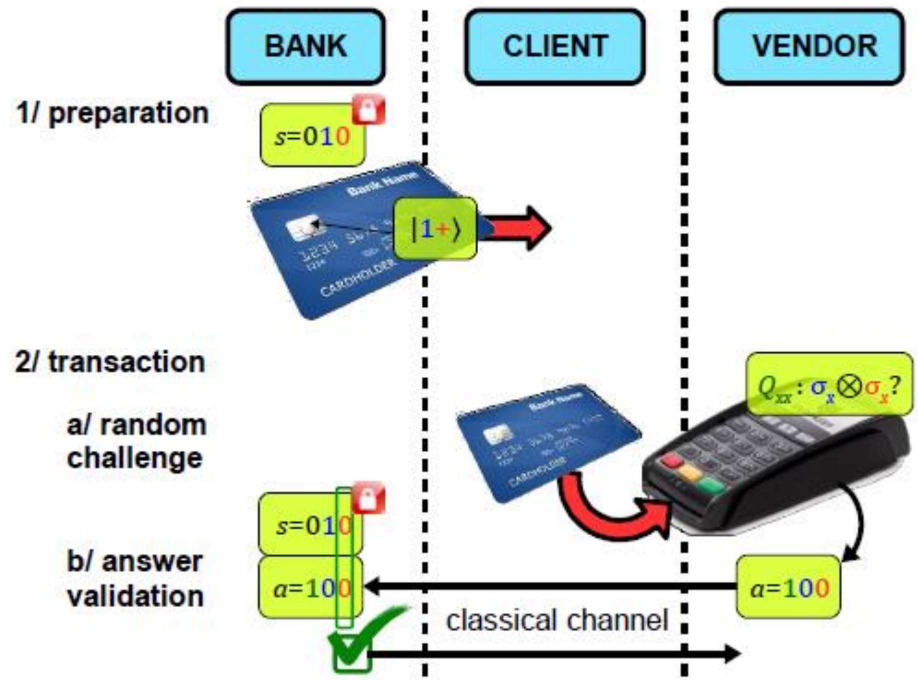
Protocol

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

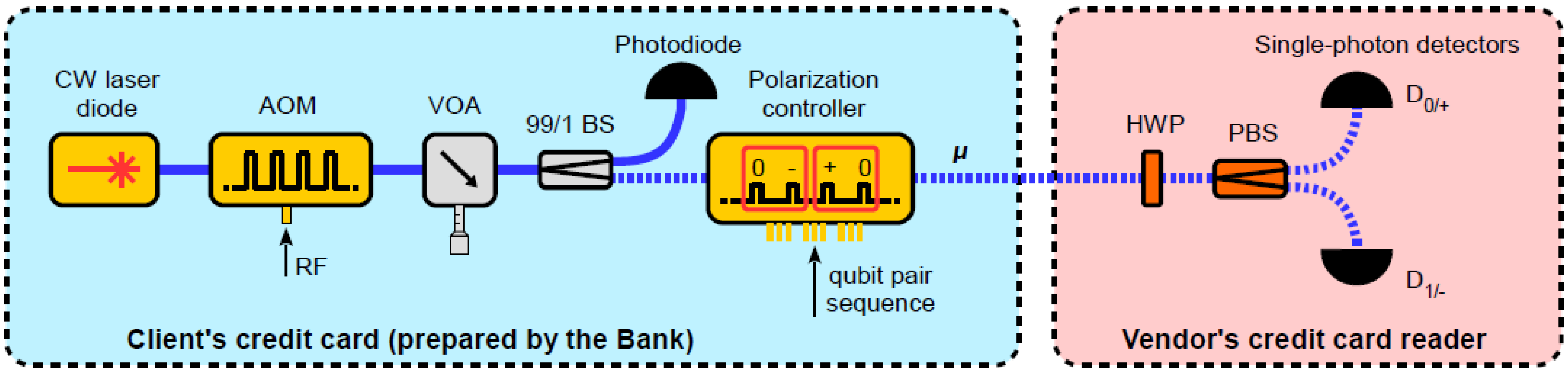
Secret classical key : 3 bits $\{b, c_0, c_1\}$, b = basis of the first qubit,
c_i = information contained in each qubit.

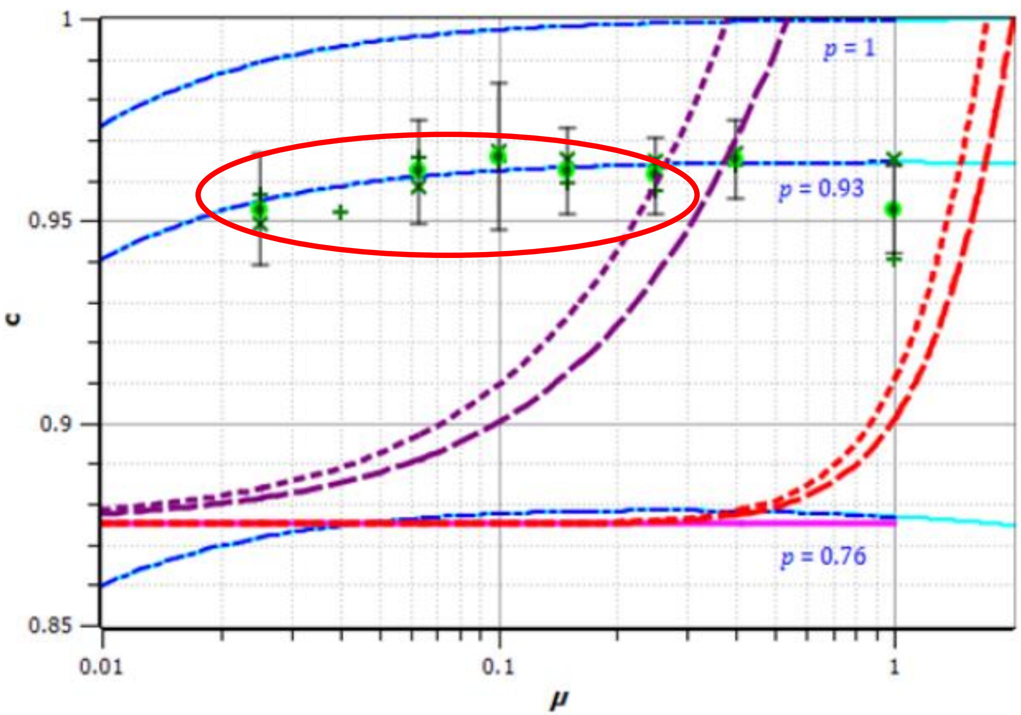
Correctness challenges (c=1, asked by the bank)
Q_{xx} : *Guess the two bits c_0 and c_1 such that the guess corresponding to the qubit prepared in the σ_x basis is correct.*
Q_{zz} : *Guess the two bits c_0 and c_1 such that the guess corresponding to the qubit prepared in the σ_z basis is correct.*

Security challenge ($\epsilon = 3/4$ = cloning probability)
Q_ϵ = *Guess the two bits c_0 and c_1.*



Experimental results





DV-QKD-like system

Security analysis for weak coherent states and anticipating quantum memory

Rigorously satisfies security condition for unforgeability → quantum advantage

Ongoing work:
Implementation with quantum memory
Untrusted terminal security analysis

M. Bozzio et al, npj Quantum Info. 2018

Perspectives

Current or near-term quantum technologies can be used to demonstrate security advantage for useful tasks

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

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

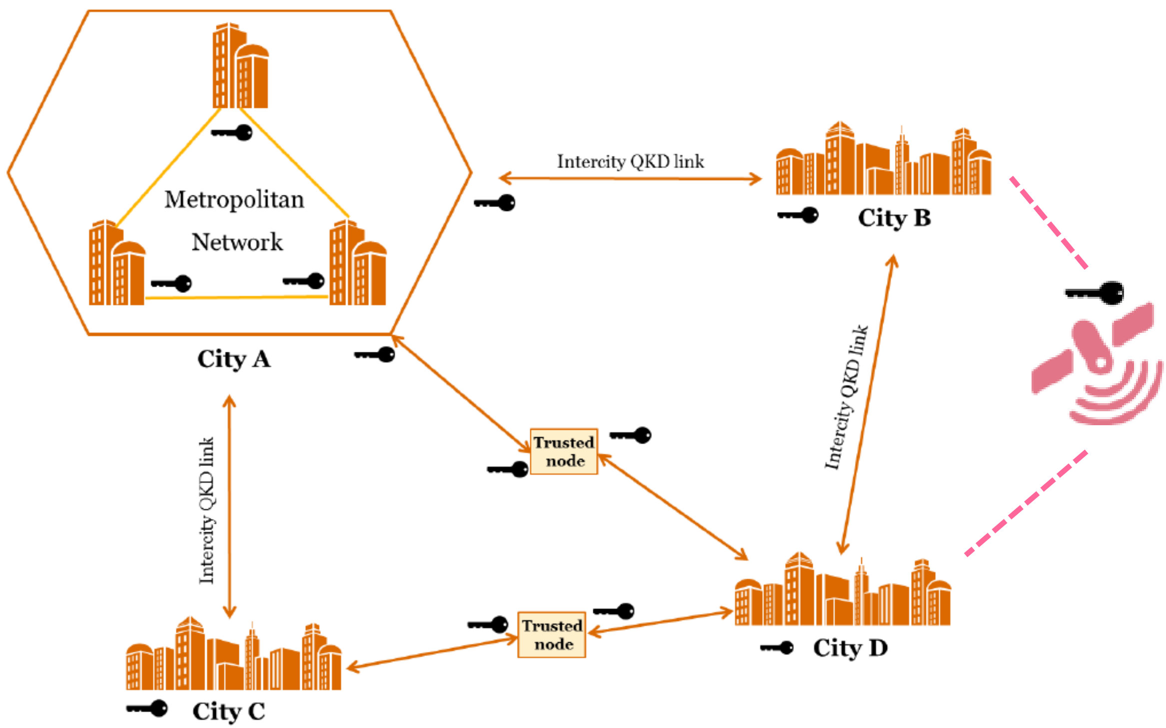
Data center interconnections

Banks, e-currency, embassies, hospitals

Telecom operator and public sector services

Critical infrastructure

…



Thank you!

Luis Trigo Vidarte

Mathieu Bozzio

Niraj Kumar

Victor Roman Rodriguez

Adeline Orieux

Mauro Persechino

Iordanis Kerenidis – Univ. Paris Diderot
Philippe Grangier – Institut d'Optique
Delphine Marris-Morini, Laurent Vivien – C2N, Univ. Paris Saclay
Daniele Dequal – Matera Observatory
Paolo Villoresi, Pino Vallone – Univ. Padova