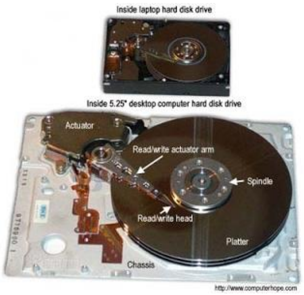
Practical challenges in quantum cryptography

Eleni Diamanti
LIP6, CNRS, Sorbonne University
Paris Centre for Quantum Computing

AtheCrypt, 23 January 2021

The quantum revolutions



Planck's quantum theory — transistor — hard disk — laser

beginning of 20th century — 1947 — 1954 — 1960

- Why doesn't the electron collapse onto the nucleus of an atom?
- Why are there thermodynamic anomalies in materials at low temperature?
- Why is light emitted at discrete colors?

Albert Einstein (1879-1955)

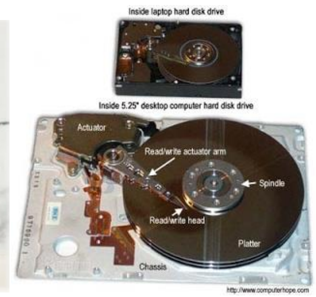
Werner Heisenberg (1901-1976)

Erwin Schrödinger (1887-1961)

The first quantum revolution

Observation and macroscopic manifestation of quantum principles

The quantum revolutions



Planck's quantum theory — transistor — hard disk — laser

beginning of 20th century — 1947 — 1954 — 1960 — end 20th / beginning 21st

Control of single quantum particles
First quantum algorithms

Richard Feynman
(1918–1988)

Serge Haroche

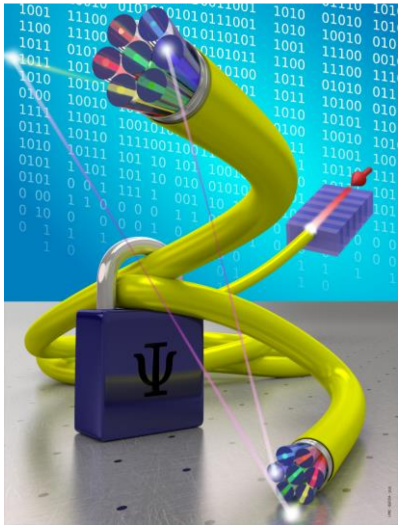
And also Alain Aspect, Charles Bennett, Gilles Brassard, Artur Ekert, Peter Shor…

The second quantum revolution

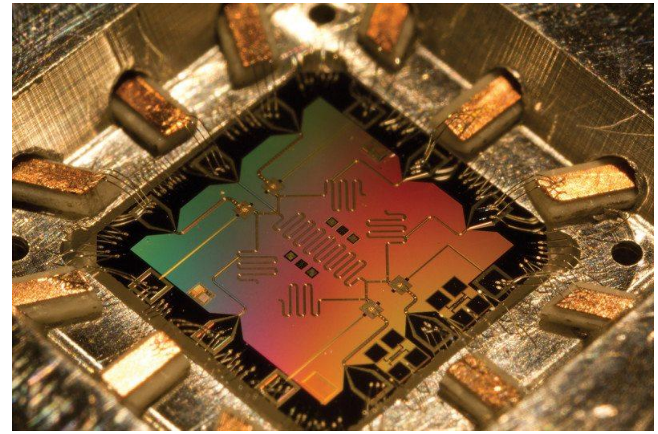
Active manipulation of single quantum particles and interaction between multiple particles for applications

Quantum technologies

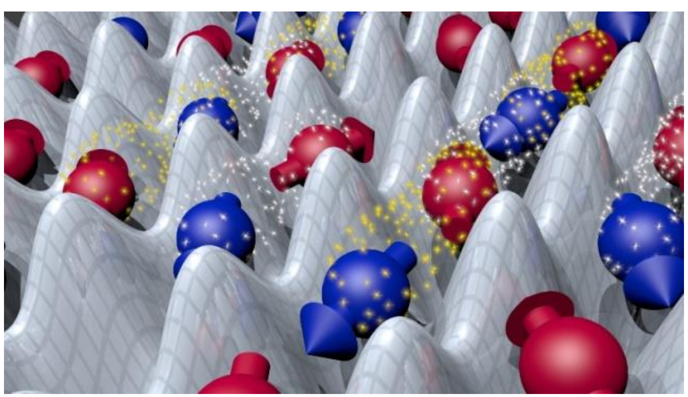
Unconditionally secure communication



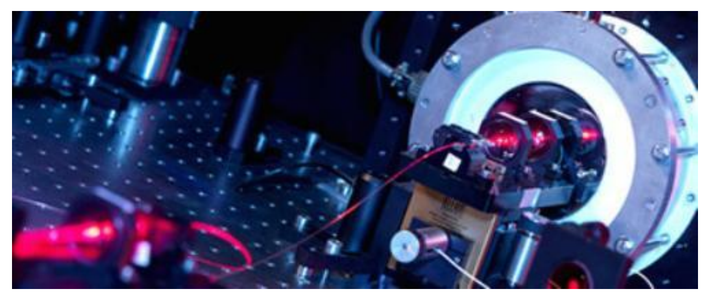
A leap in computing power



Increased understanding of complex physical systems

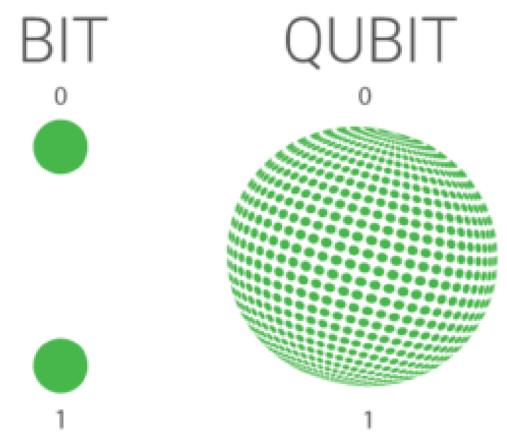


Measurement precision beyond the classical limit



Encoding quantum information

Information can be encoded on properties of **single quantum particles** which can be found in **superposition** states



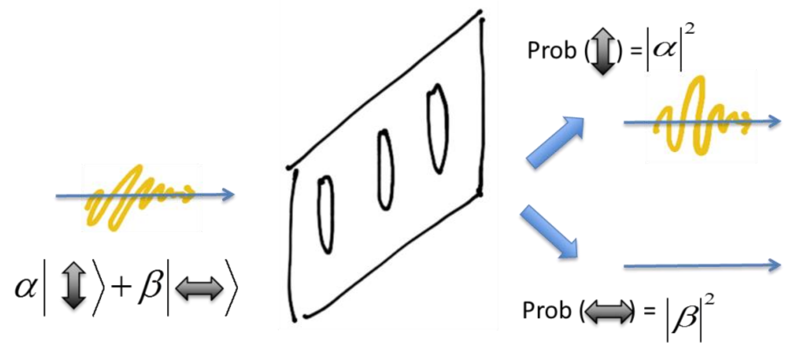
$$\alpha|0\rangle + \beta|1\rangle$$

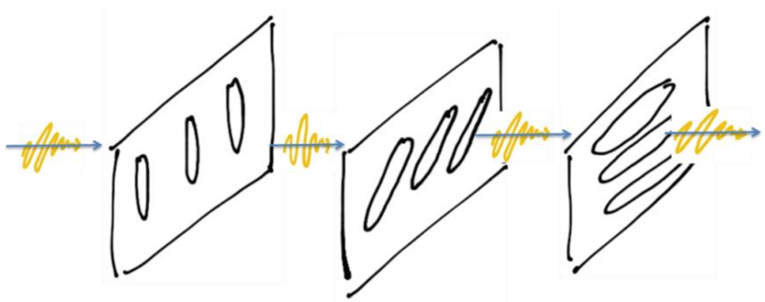
with α, β complex numbers and

$$|\alpha|^2 + |\beta|^2 = 1$$

Unknown quantum states cannot be cloned!

Photons are ideal carriers of quantum information
→ robust to ambient noise
→ can be transported over long distances



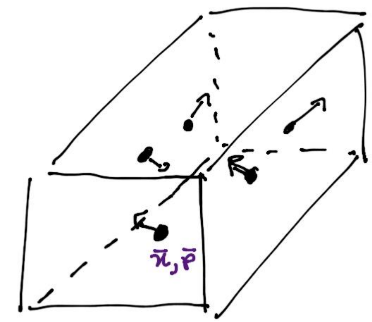


Following the probabilities according to quantum mechanics, there is a non-zero probability of photon coming out!

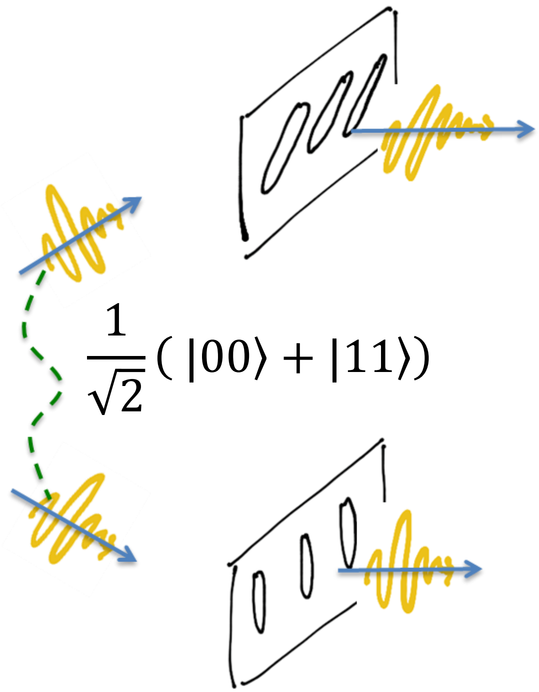
Encoding quantum information

Information can also be encoded on properties of **entangled particles** which exhibit **nonlocal correlations**

In classical physics, randomness comes from ignorance



Einstein-Podolsky-Rosen paradox: same for quantum theory?



$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Bell test: there is no **local hidden variable** model that explains quantum correlations

In quantum physics, **randomness does not come from ignorance!**

Quantum computing

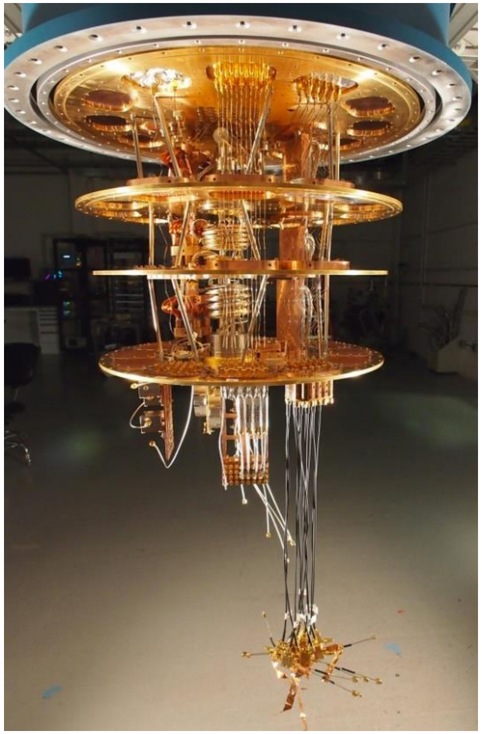
"The goal in quantum computing is to ***choreograph things*** *so that some paths leading to a wrong answer have positive amplitudes and others have negative amplitudes, so on the whole they cancel out and* ***the wrong answer is not observed****."*
Scott Aaronson

Shor algorithm (1994)
breaks RSA public-key cryptography based on factorization

Grover algorithm (1996)
Quadratic speedup for search

Harrow, Hassidim, Lloyd (2008)
Quantum machine learning

A real threat ?



IBM

Google

PsiQuantum

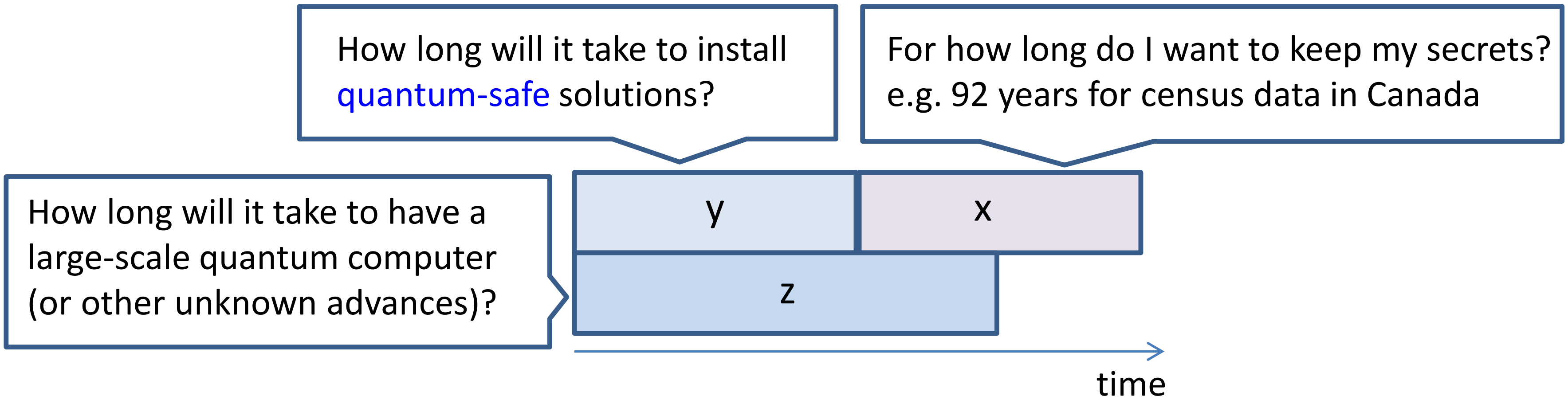
Currently 40 – 70 qubits : Noisy Intermediate-Scale Quantum (NISQ) devices

Sufficient for quantum ‘supremacy’ ?

Orders of magnitude more required for fault-tolerant universal quantum computing

Towards quantum-safe communications

Courtesy of Michele Mosca, IQC Waterloo



If x + y > z, then secrets will be revealed
If y > z, cyber security is compromised with no quick fix

Roadmap

→ Find classical cryptographic techniques robust against *known* quantum attacks

→ Establish efficiency and security bottlenecks due to *future* progress

→ Design quantum cryptographic protocols to address them for long-term security

→ Develop practical quantum cryptographic systems

ED and E. Kashefi, Best of both worlds, Nature Phys. 2017

Quantum-safe cryptography

Post-quantum cryptography: conventional cryptography with no need for quantum technologies
→ **Believed/hoped** to be secure against future quantum computing attacks
→ Relatively easy to implement

+

Quantum cryptography: requires quantum technologies
→ **Known** to be secure against quantum attacks (no computational assumptions)
→ More accessible than a quantum computer but still costly to implement

Quantum Key Distribution provides a future-proof, information theoretically secure (ITS) solution to the key distribution problem for secure message exchange between two trusted parties, and is robust against powerful ‘Store now, Decrypt later’ attacks

QKD and secure message exchange

QKD does not offer a stand-alone cryptographic solution for this task

The key agreement (or key establishment, exchange, amplification, negotiation,…) protocol needs to be combined with authentication and message encryption algorithms

Many possible scenarios, combining classical (including post-quantum) and quantum solutions:

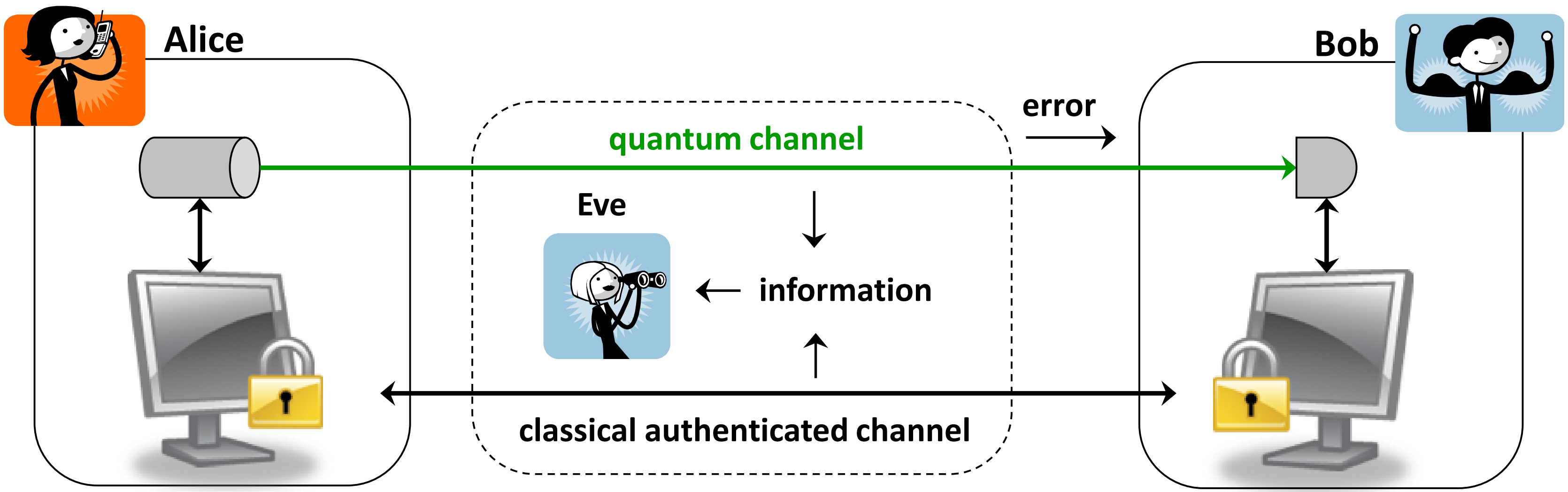
Authentication	Key agreement	Message encryption
e.g. with post-quantum or ITS digital signatures	e.g. with post-quantum or **QKD** (ITS) replacing vulnerable asymmetric algorithms	e.g. with AES or one-time pad (ITS)

No ubiquitous solution

Trade-offs between security risks and ease of implementation, depending on use case

Principle of quantum key distribution

A quantum key distribution (QKD) system includes
a quantum channel used for the transmission of qubits
an authenticated classical channel used for testing perturbations in the transmission and key processing procedures

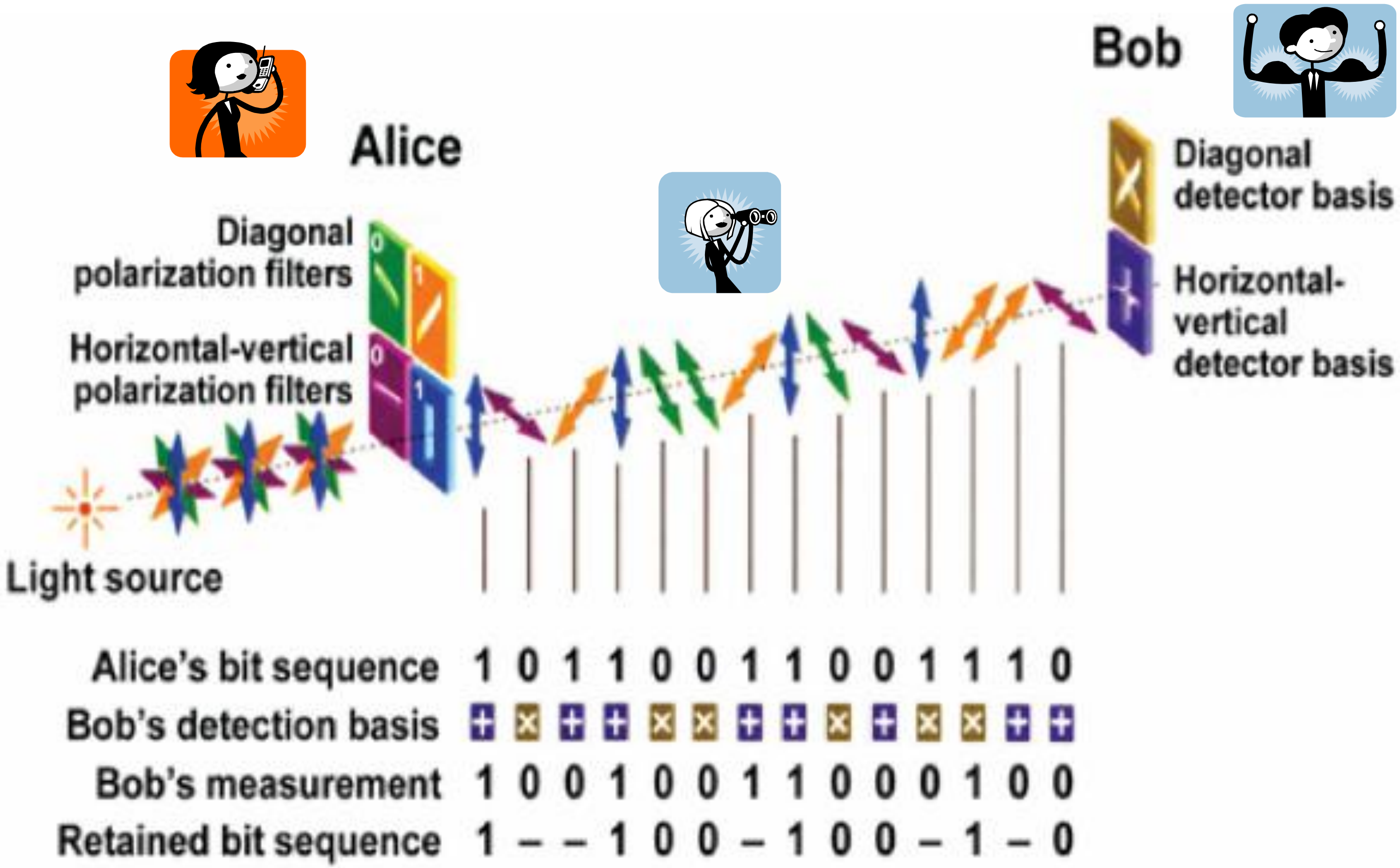


Eve's measurement inevitably introduces perturbations that lead to detectable errors
→ the analysis of these errors allows the generation of the secret key

During the quantum transmission, the key is obtained using

either a given set of non-orthogonal quantum states of **single photons**
or a given set of measurements performed on **entangled photons**

A single-photon QKD protocol – BB84

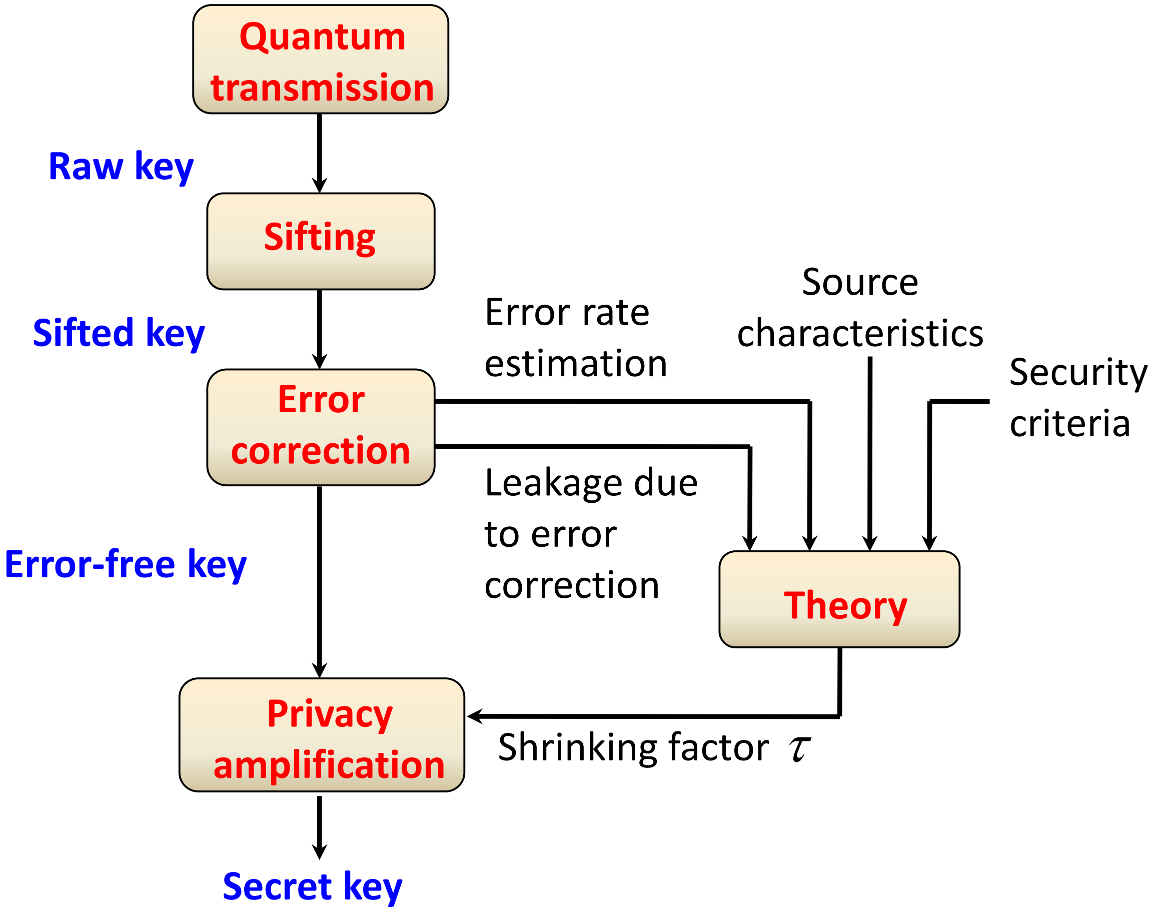


No cloning theorem: Eve cannot copy the states sent by Alice

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

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

A full QKD algorithm



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

Encompasses notions of composability, finite-size effects, generality of attacks

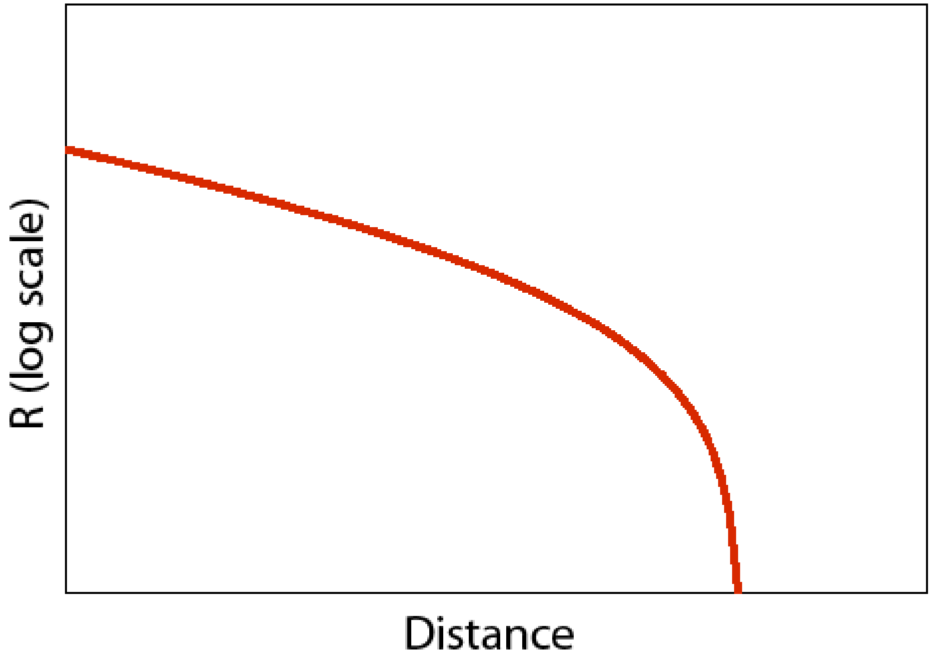
Secret key rate in practice

All practical QKD systems have imperfections

Losses (transmission channel, imperfect components)

Characteristics of light sources (true single photons or weak coherent states?) and single-photon detectors (finite quantum efficiency and dark counts)

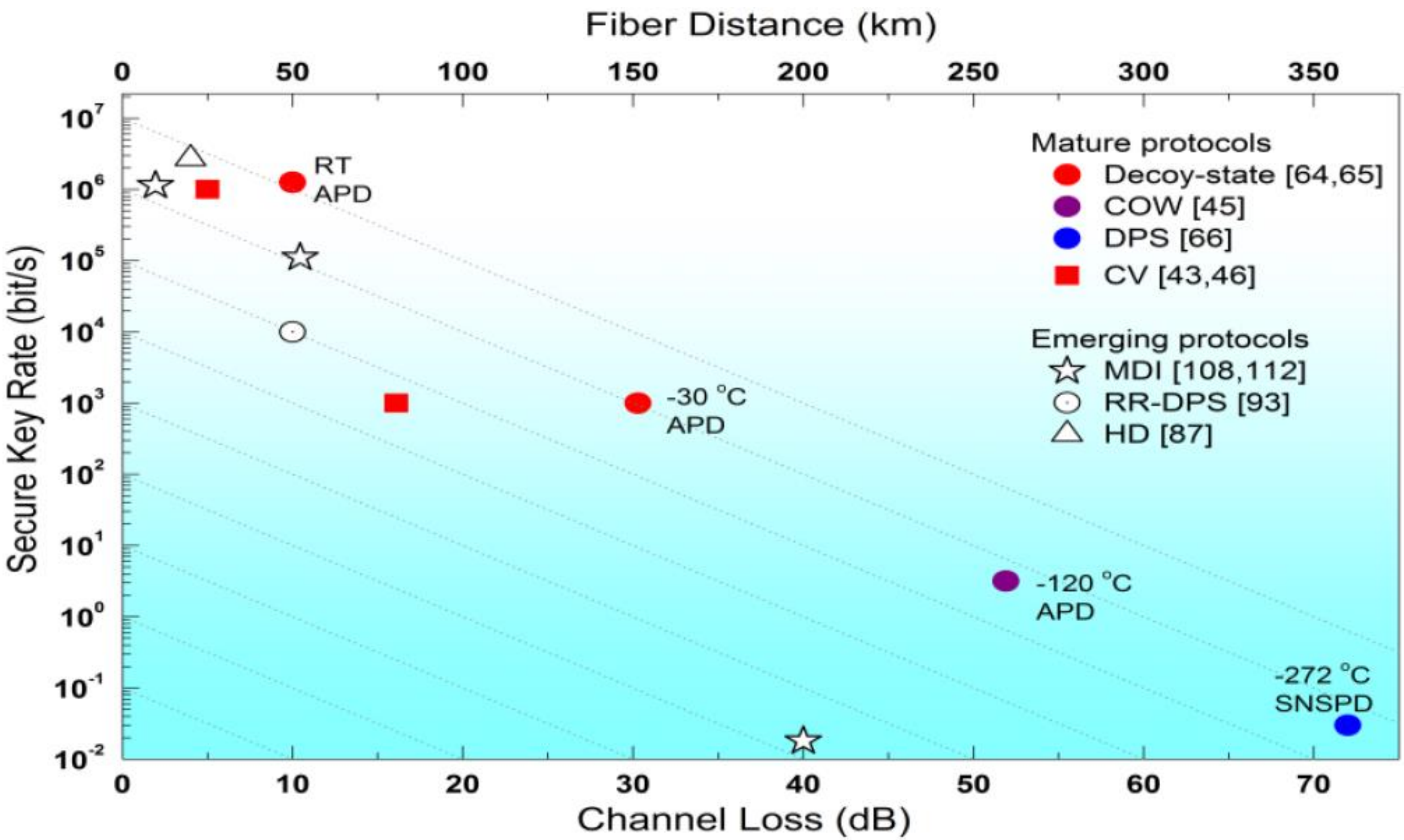
Crucial for performance



Linear part: the rate drops as a given power of the channel attenuation

Exponential part: the rate drops abruptly and goes to zero due to the growing contribution of the detector dark counts

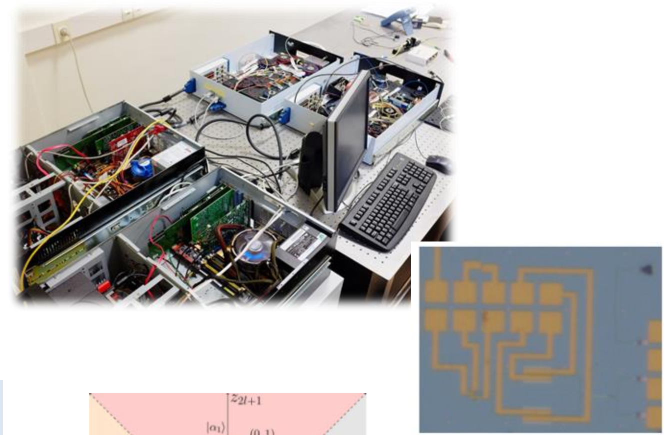
State of the art of point-to-point fiber-optic QKD



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

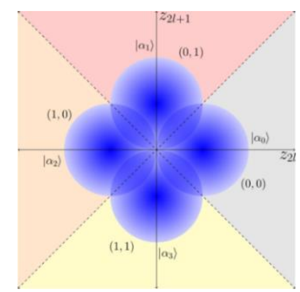
Current practical challenges

High cost
Photonic integration for reduced cost and scalable solutions



L.Trigo Vidarte *et al.*, QCrypt 2018

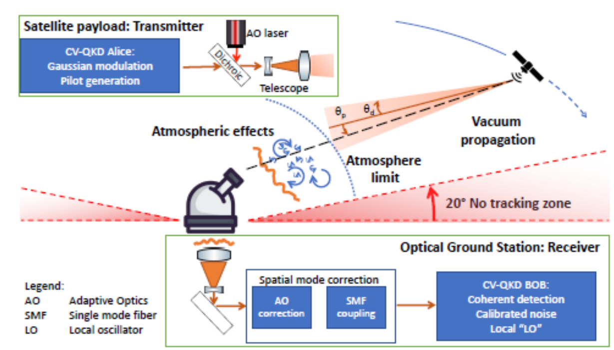
Lack of network integration
Operation in optical telecom systems to improve compatibility with conventional architectures and reduce deployment cost



S. Ghorai *et al.*, Phys. Rev. X 2019

Absence of standards and certification
Parallel efforts in relevant bodies, crucial for interoperability and market adoption

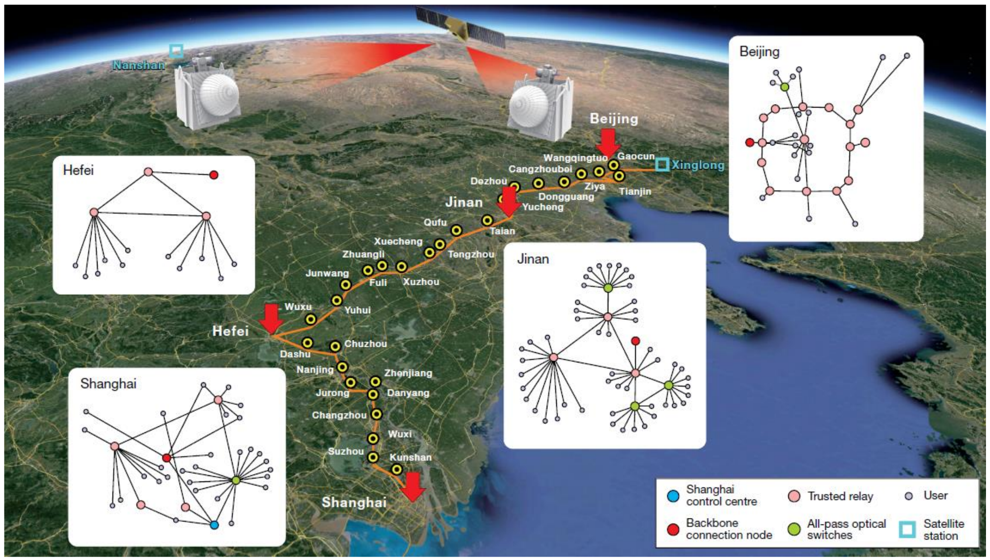
Inherent range limitation due to optical fiber loss
Quantum networks and Satellite communications



D. Dequal *et al.*, npj Quant. Info. 2021

QKD networks

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



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

OPEN QKD

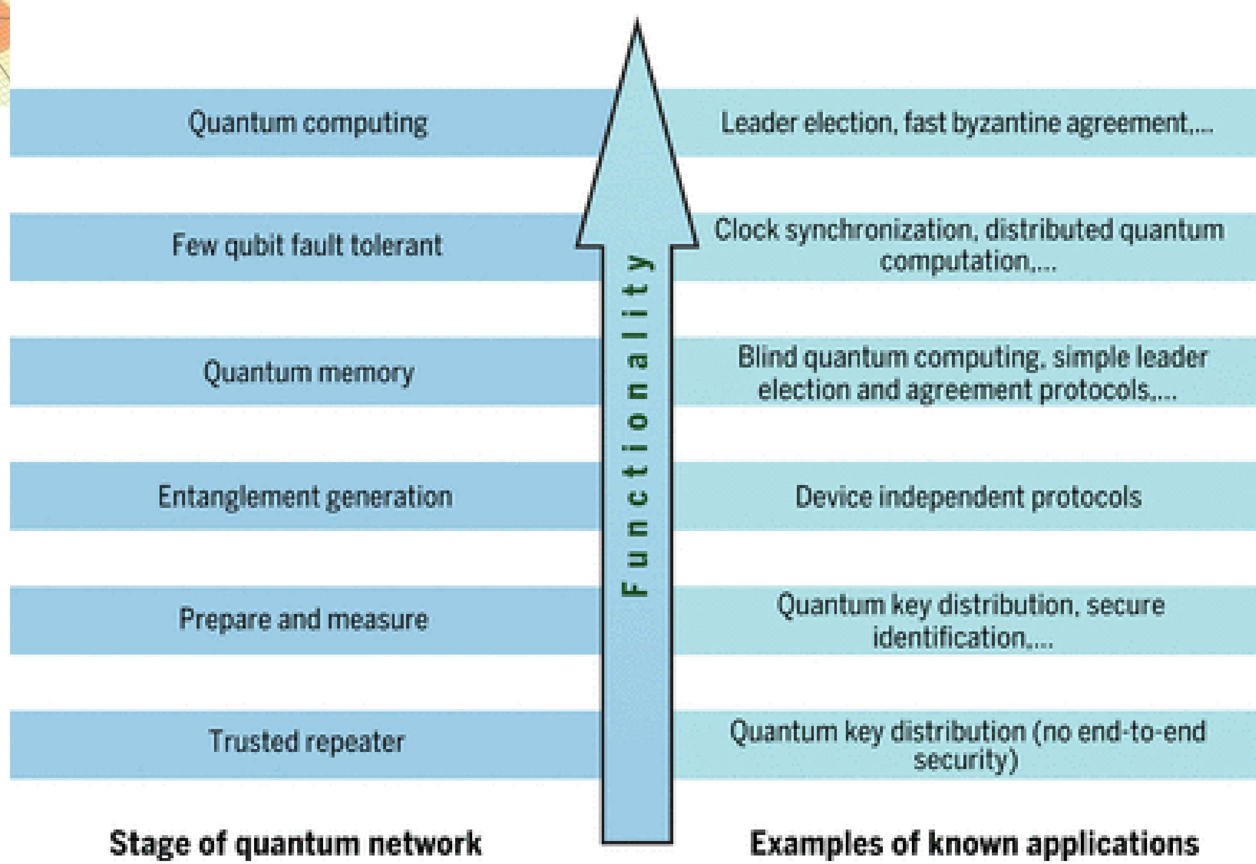
Data centres, electrical power grids, governmental communication, medical file transfer, critical infrastructure,...

From trusted nodes to end-to-end security

Quantum repeaters and processing nodes, long-term and efficient quantum storage

Applications of quantum communication networks

The goal is to demonstrate a provable quantum advantage in security and efficiency for communication, delegated and distributed computing tasks



S. Wehner *et al.*, Science 2018

Quantum advantage for advanced tasks

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

In other configurations many more functionalities
→ Framework for demonstrating quantum advantage

Secret sharing, entanglement verification, authenticated teleportation, anonymous communication

Random number generation, quantum money, communication complexity

Bit commitment, coin flipping, oblivious transfer, digital signatures, position-based cryptography

How do we make abstract protocols compatible with experiments?
→ protocols typically require inaccessible resources and are vulnerable to imperfections

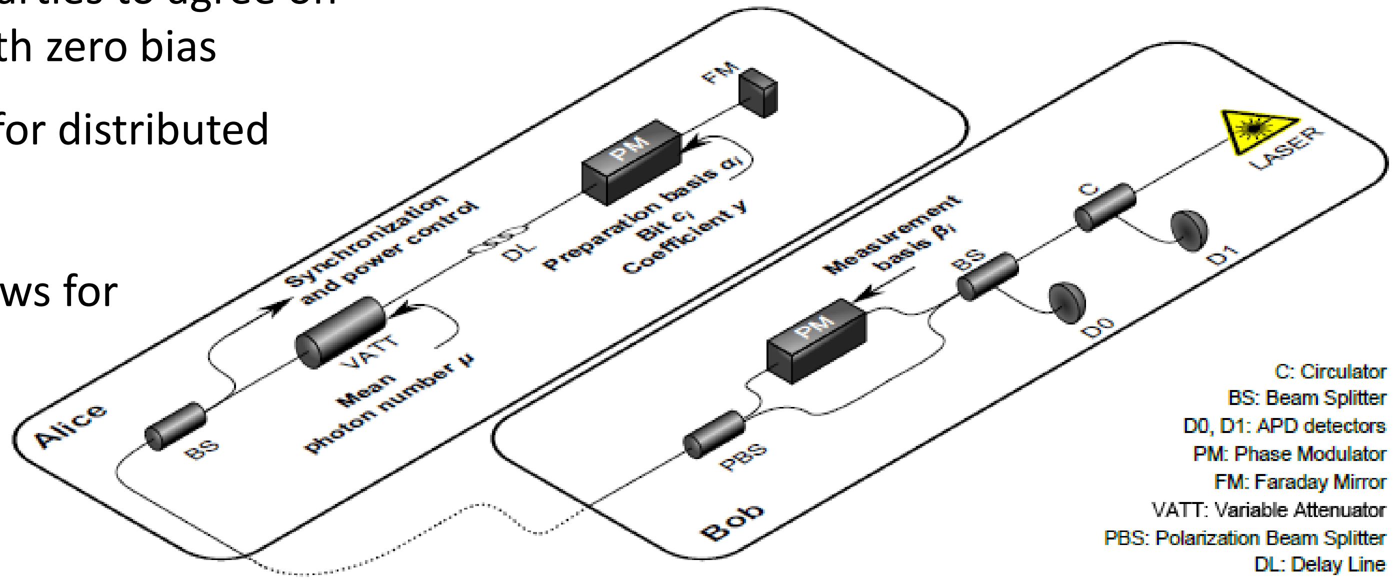
When do we claim a quantum advantage?
→ fair comparison with classical resources

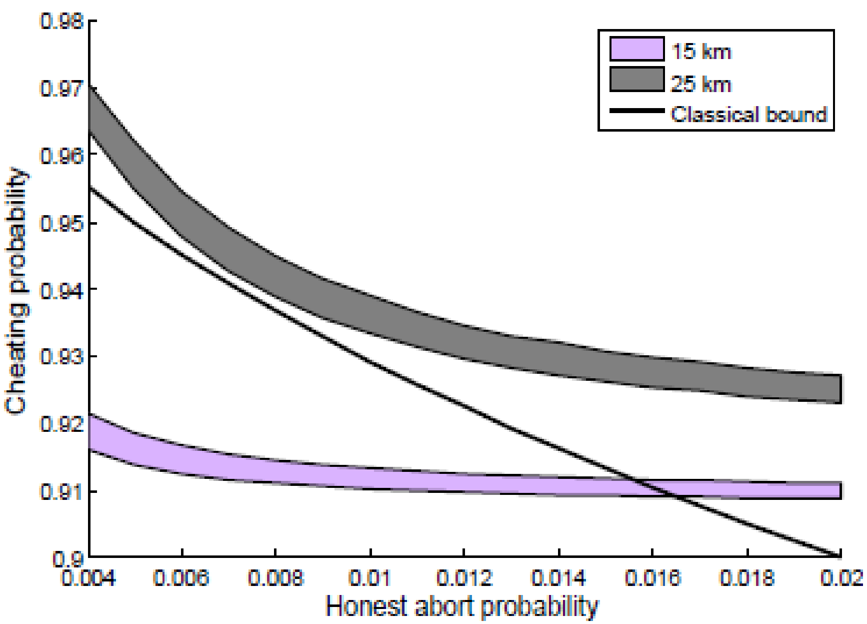
Quantum coin flipping

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





QKD-like system

Quantum advantage for metropolitan area distances

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

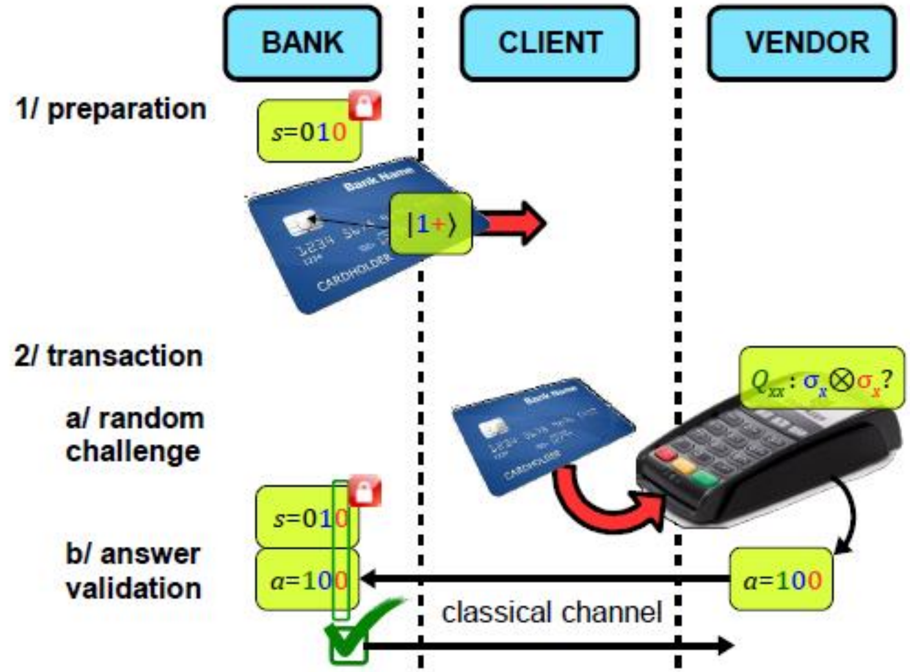
Experimental proposal for weak quantum coin flipping

M. Bozzio *et al.*, Phys. Rev. A 2020

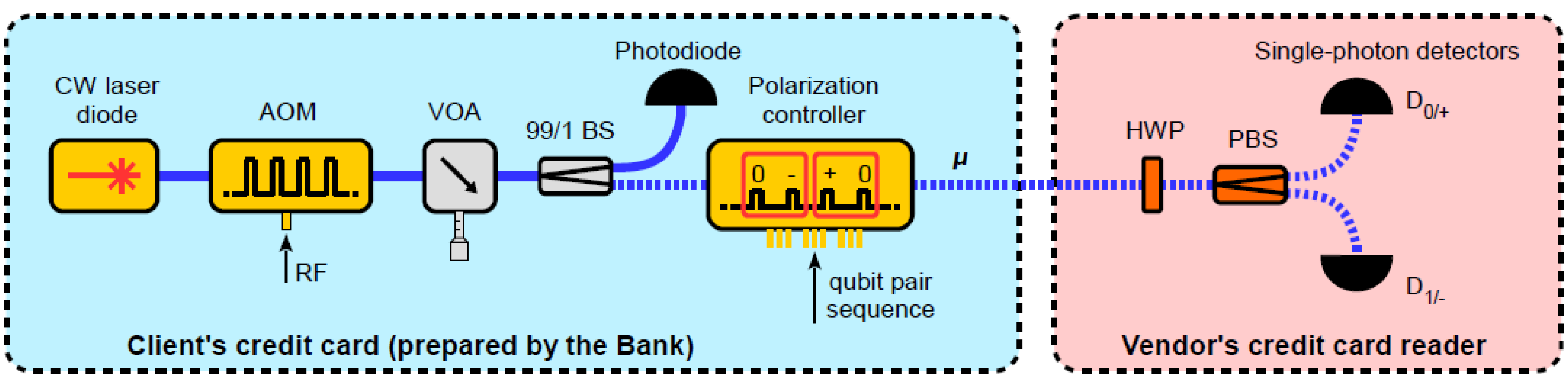
Unforgeable quantum money

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

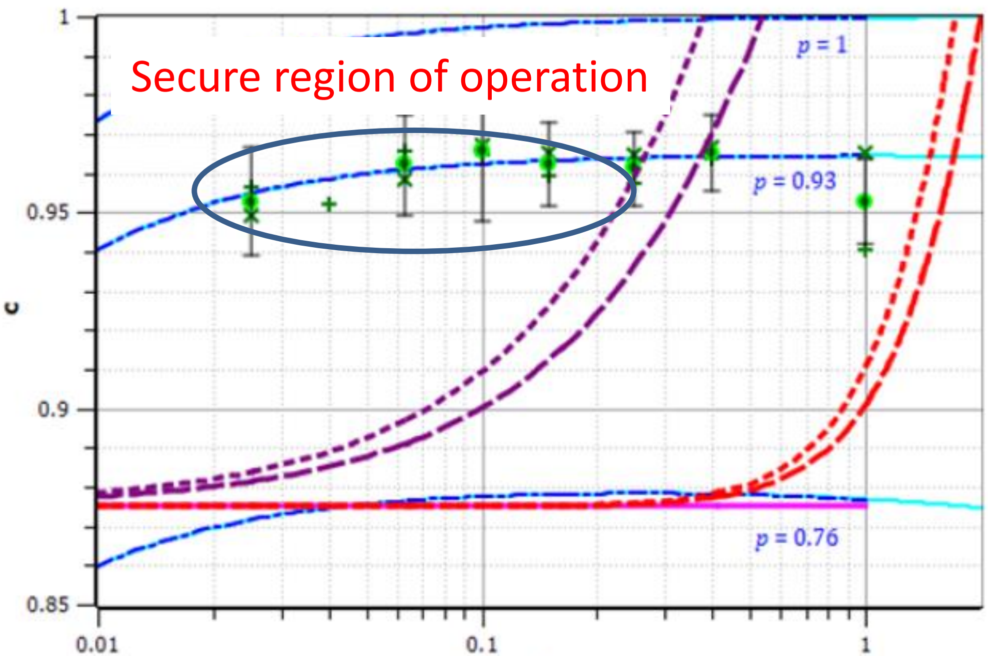


New protocol with classical verification and BB84-type states
Based on challenge questions



Unforgeable quantum money

Probability of answering the bank's challenge correctly → c



Average number of photons per pulse → μ

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

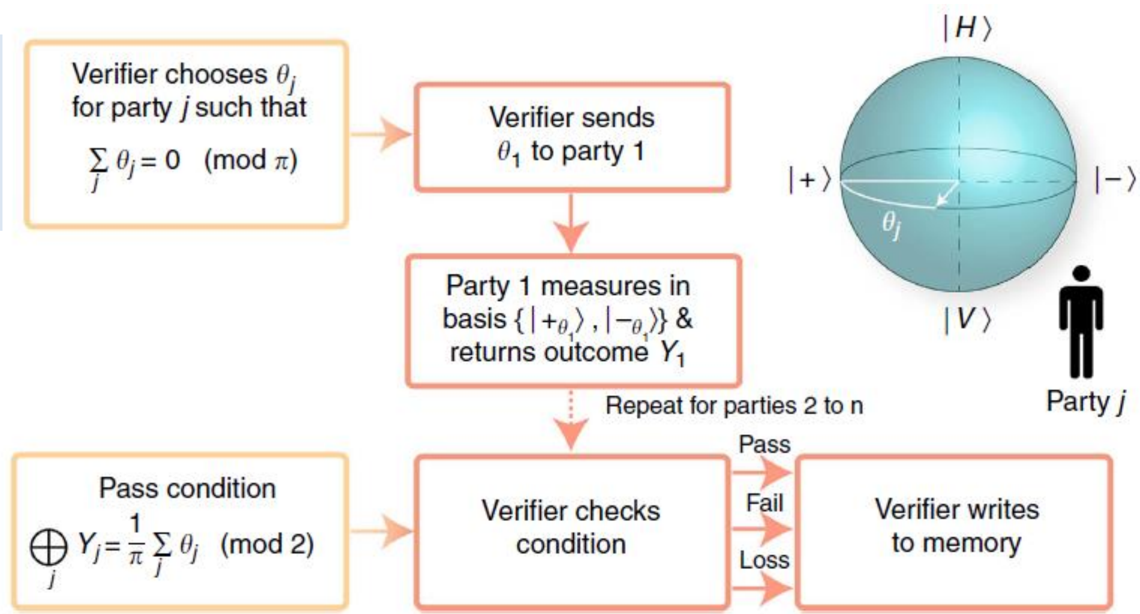
General security framework for weak coherent states and anticipating quantum memory
→ minimize losses and errors for both trusted and untrusted terminal

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

Quantum network protocols

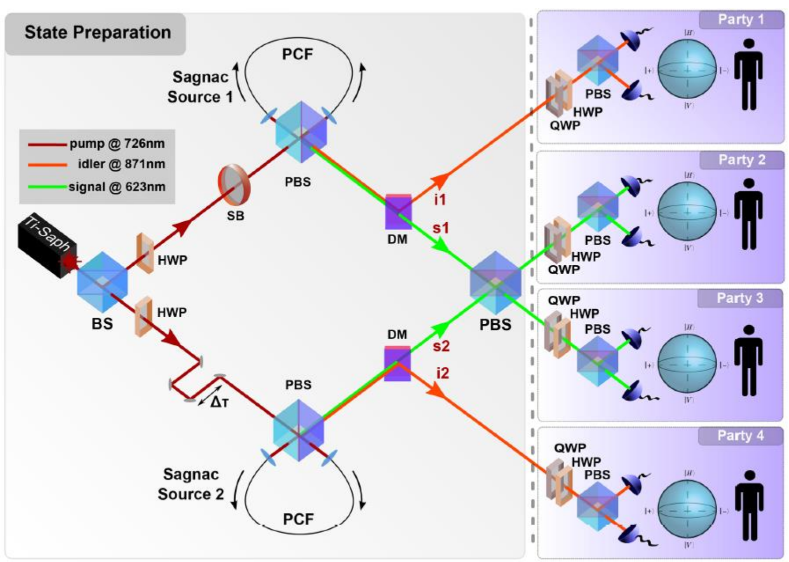
Proof-of-principle **verification of multipartite entanglement** in the presence of dishonest parties

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

Theoretical framework for **composability**

R. Yehia *et al.*, arXiv 2004.07679

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

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

The quantum communication protocol toolbox is rich and increasingly advanced

Thank you!

CV-QKD: Luis Trigo Vidarte, Damien Fruleux, Matteo Schiavon, Shouvik Ghorai, Adrien Cavaillès
Quantum money and communication complexity: Federico Centrone, Verena Yacoub, Mathieu Bozzio, Niraj Kumar
Quantum network protocols and resources: Simon Neves, Victor Roman Rodriguez, Raja Yehia, Anu Unnikrishnan

Philippe Grangier – IOGS
Anthony Leverrier – INRIA
François Roumestan, Amir Ghazisaeidi – Nokia Bell Labs France
Baptiste Gouraud - iXblue
Delphine Marris-Morini, Laurent Vivien – C2N, U. Paris Saclay
Daniele Dequal – Matera Observatory
Paolo Villoresi, Pino Vallone – U. Padova
Iordanis Kerenidis – U. Paris, PCQC
Damian Markham, Elham Kashefi, Frédéric Grosshans – LIP6