Practical aspects of quantum key distribution and beyond

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

Horizon 2020 Programme

QCrypt, 10-14 August 2020

Quantum communication networks

Photonic resources

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

Security

Untrusted network users, devices, nodes

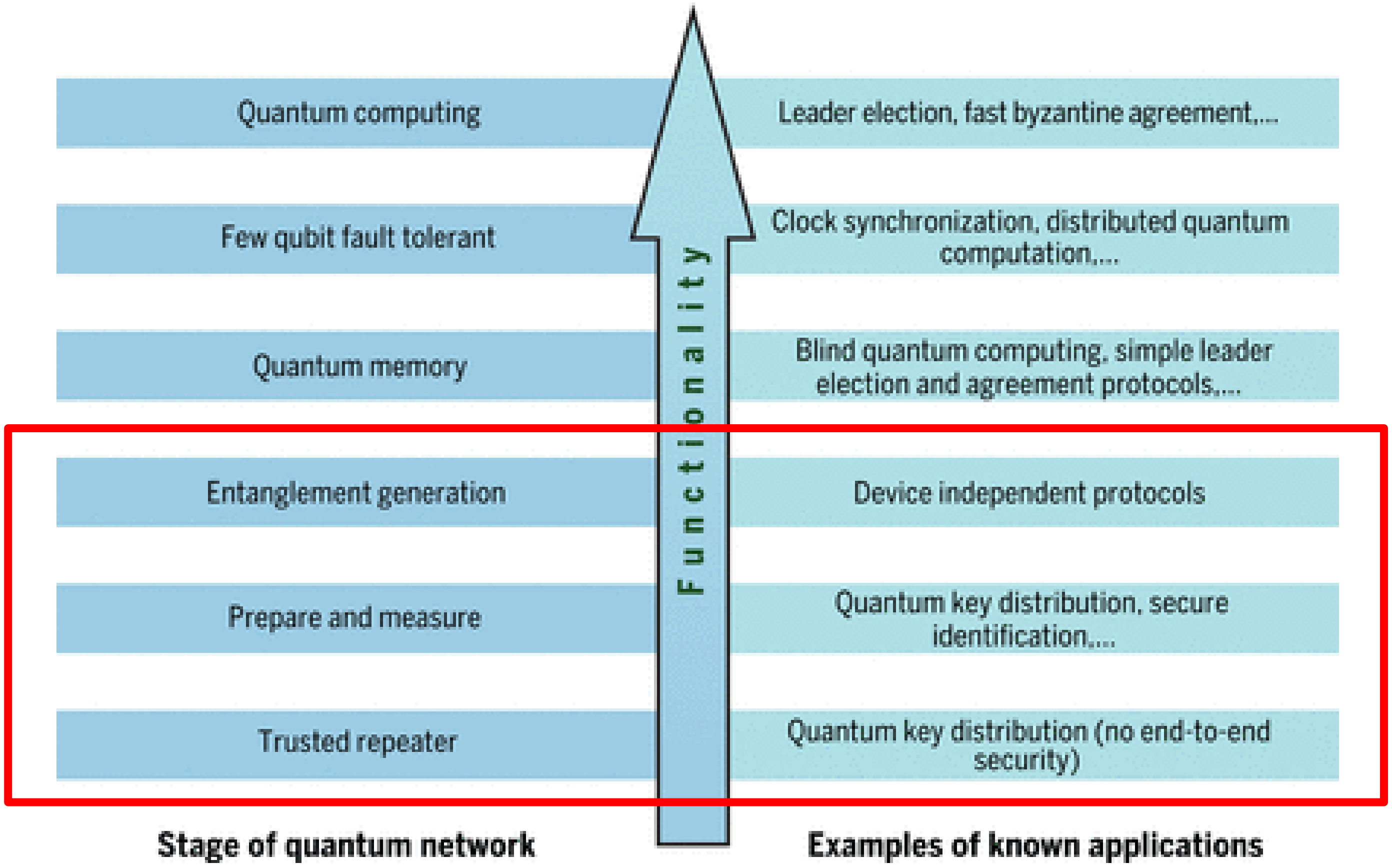
Efficiency

Optimal use of communication resources

Applications

Analysis and implementations using quantum photonics to demonstrate a provable quantum advantage in security and efficiency for communication and distributed computing tasks

Applications of quantum communication networks



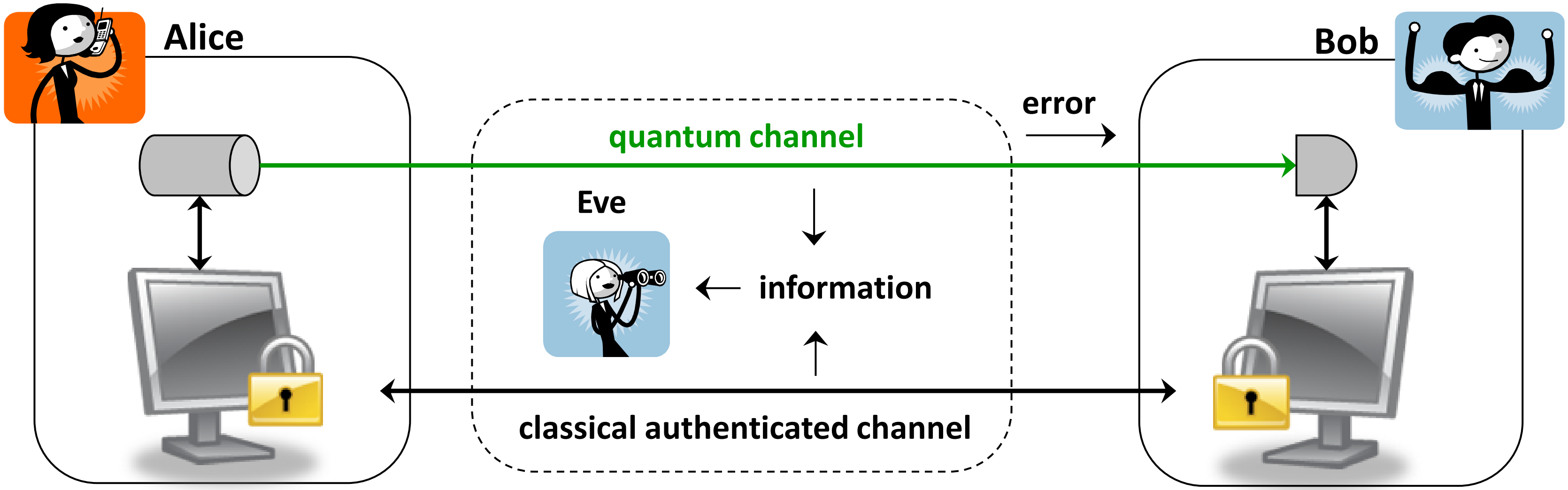
S. Wehner *et al.*, Science 2018

Outline of tutorial

1. Some reminders on QKD
2. Criteria and measures of performance of QKD systems
3. Examples of configurations and current challenges
4. Applications beyond QKD
5. Testbeds and use cases

Securing network links: QKD

Landmark application of quantum communication that has driven the field for many years



Thanks to the fundamental principles of quantum physics (no cloning theorem, superposition, entanglement & nonlocality), it is possible to detect eavesdropping on the communication link

No need for assumptions on computational power of eavesdropper → information-theoretic security (ITS)
Change of paradigm with respect to classical algorithms offering computational security

QKD and secure message exchange

QKD does not offer a stand-alone cryptographic solution for secure message exchange between two trusted parties

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:

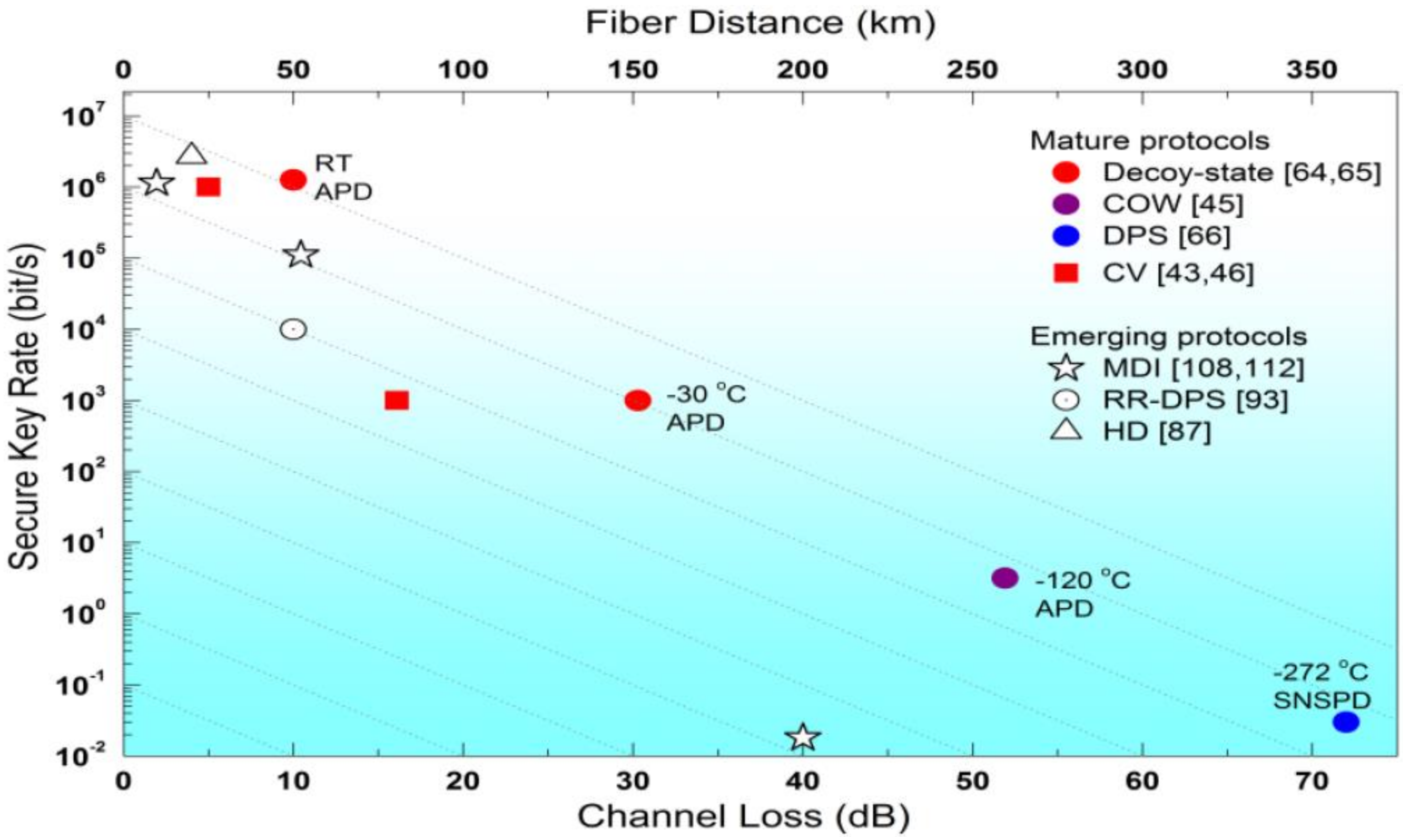
Authentication	Key agreement	Message encryption
e.g. with post-quantum or ITS digital signatures	e.g. with post-quantum or **QKD** (ITS) replacing vulnerable asymmetric algorithms	e.g. with AES or one-time pad (ITS)

No ubiquitous solution
Trade-offs between security risks and ease of implementation, depending on use case

QKD offers information-theoretic, long-term security of sensitive data, and is robust against powerful ‘Store now, Decrypt later’ attacks

QKD in practice

State-of-the-art of point-to-point fiber-optic QKD in 2016



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

A rich field with constant innovation in both theoretical protocols and practical implementations

What are relevant performance measures and interesting criteria for use cases?

Outline of tutorial

1. Some reminders on QKD
2. Criteria and measures of performance of QKD systems
3. Examples of configurations and current challenges
4. Applications beyond QKD
5. Testbeds and use cases

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 I accept prepare-and-measure schemes and trusted nodes?

Or do I need (some) untrusted nodes? Device independence?

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

Define 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

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

Complexity of classical post-processing techniques

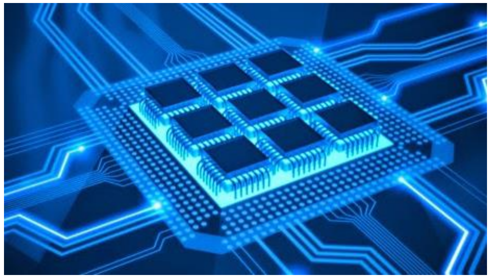
How ***cost-effective*** are the systems?

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?

Maturity and availability of components



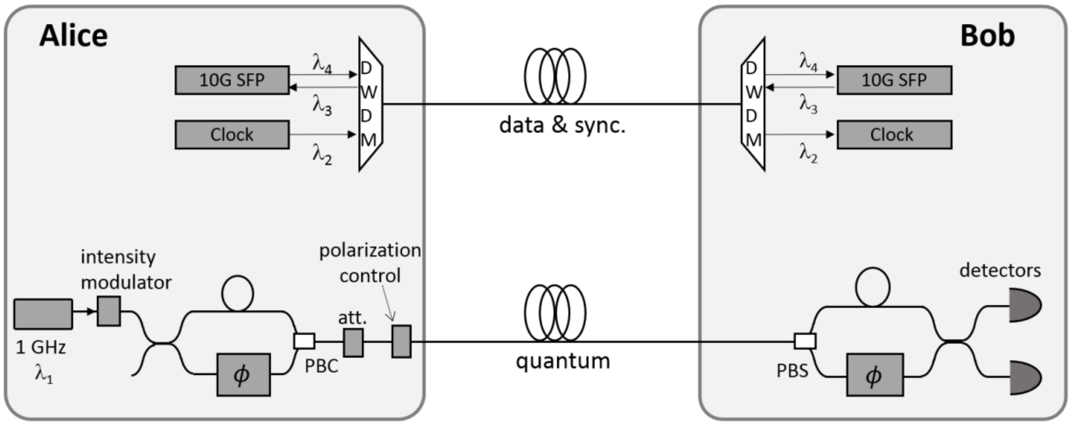
Outline of tutorial

1. Some reminders on QKD
2. Criteria and measures of performance of QKD systems
3. Examples of configurations and current challenges
4. Applications beyond QKD
5. Testbeds and use cases

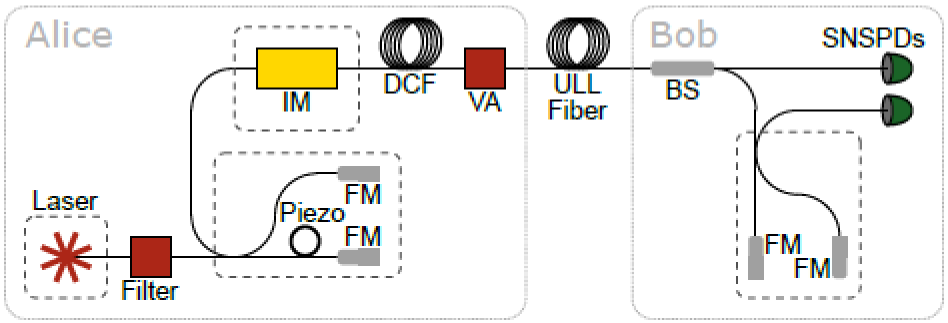
BB84 with decoy states

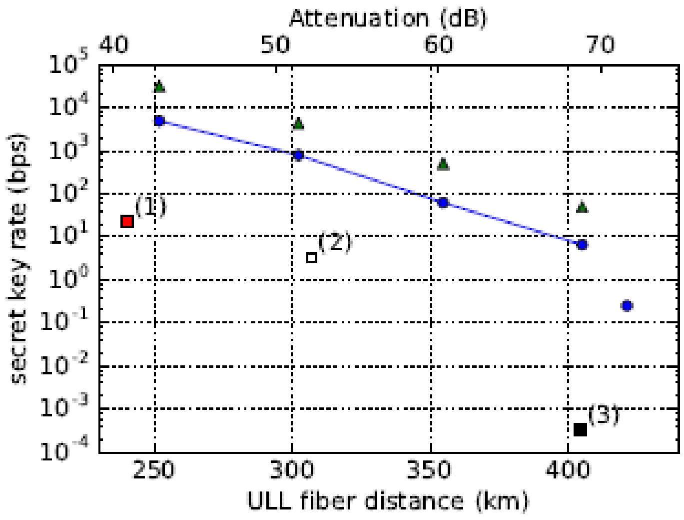
Prepare-and-measure, weak coherent pulses, single-photon detectors

High Technology Readiness Level, record-breaking implementations



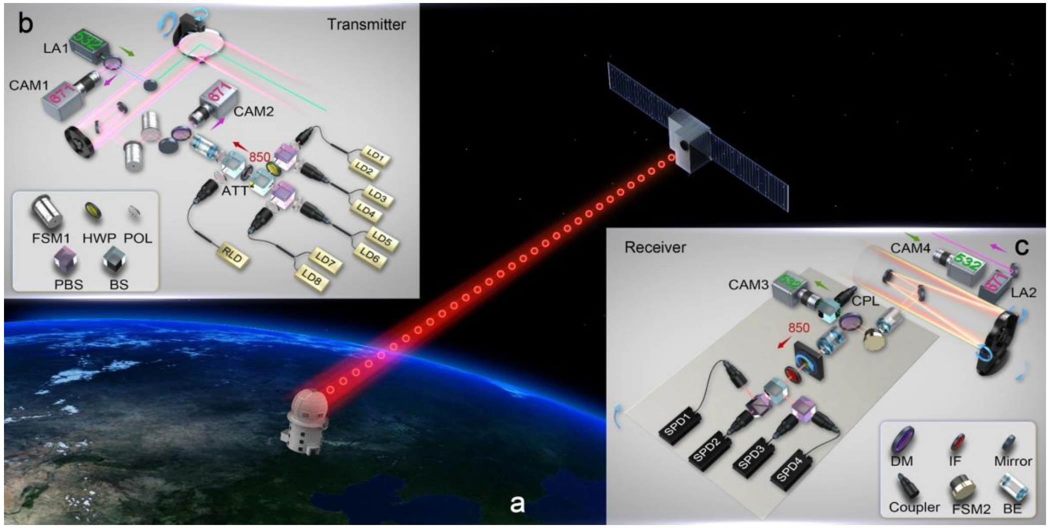
10 Mbit/s secret key rate over 2 dB, Z. Yuan *et al.*, JLT 2018



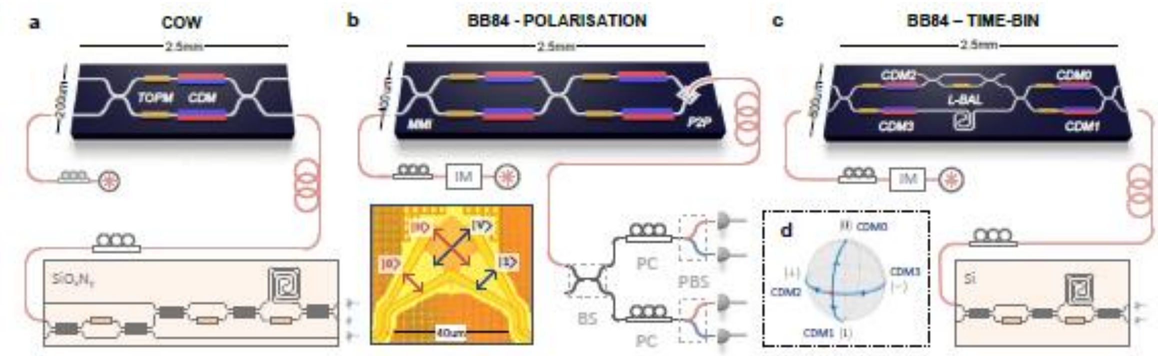


421 km, A. Boaron *et al.*, Phys. Rev. Lett. 2018

BB84 with decoy states



1200 km, S.-K. Liao *et al.*, Nature 2017



Si transmitter PIC, P. Sibson *et al.*, Optica 2016

Trusted nodes
Detector side channels
Single-photon detectors

Continuous variable QKD

Prepare-and-measure, coherent states, coherent detectors

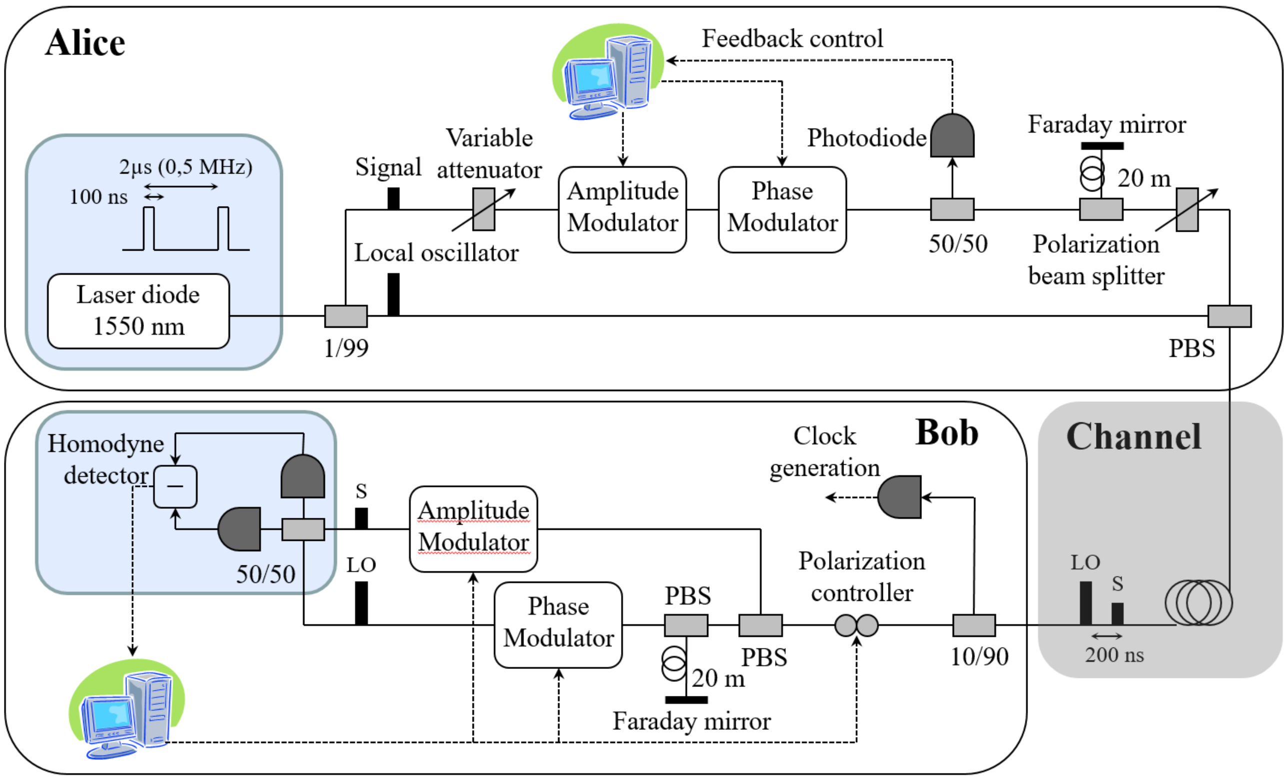
High compatibility with telecom networks, multiplexing with classical signals, high level of photonic integration

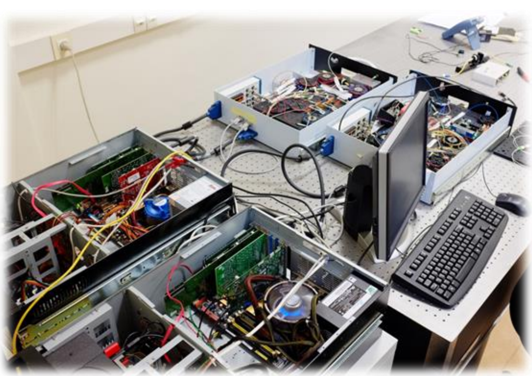
Transmitted LO

Pulsed operation

Homodyne detection

Gaussian modulation





80 km, P. Jouguet *et al.*, Nature Photon. 2013

Continuous variable QKD

Bandwidth-efficient CV-QKD

Transmitted LO

Pulsed operation

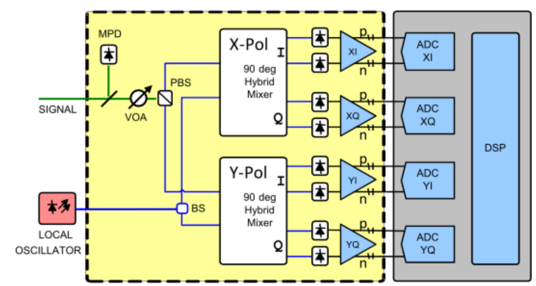
Homodyne detection

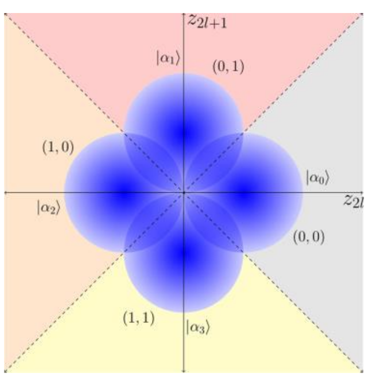
Gaussian modulation

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

CW pulse shaping techniques: optimal use of spectrum, avoid inter-symbol interference, use of pilots, challenging Digital Signal Processing, security

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



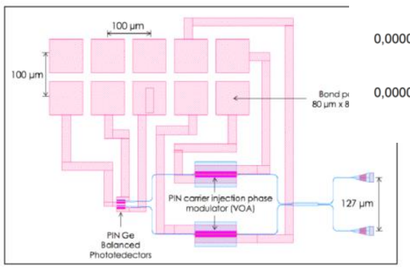


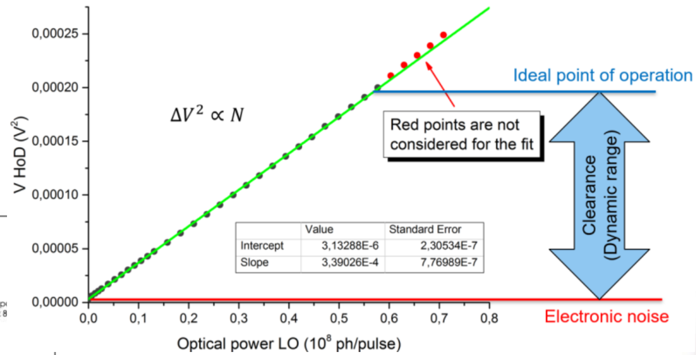
Security proof for QPSK discrete modulation

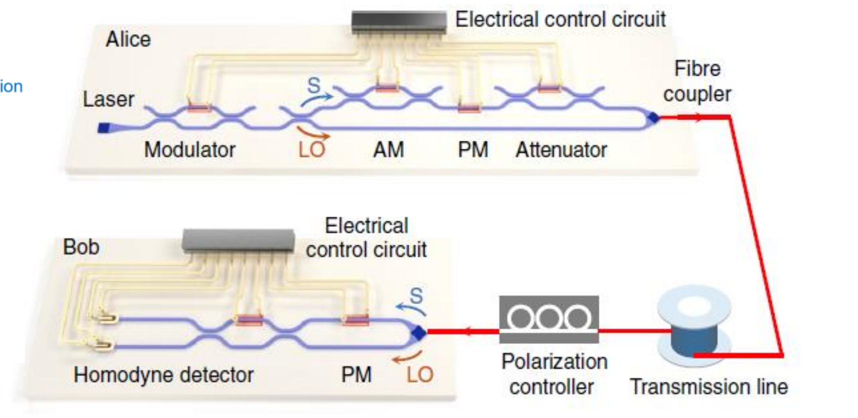
Technique may be extended to other modulations

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

Continuous variable QKD

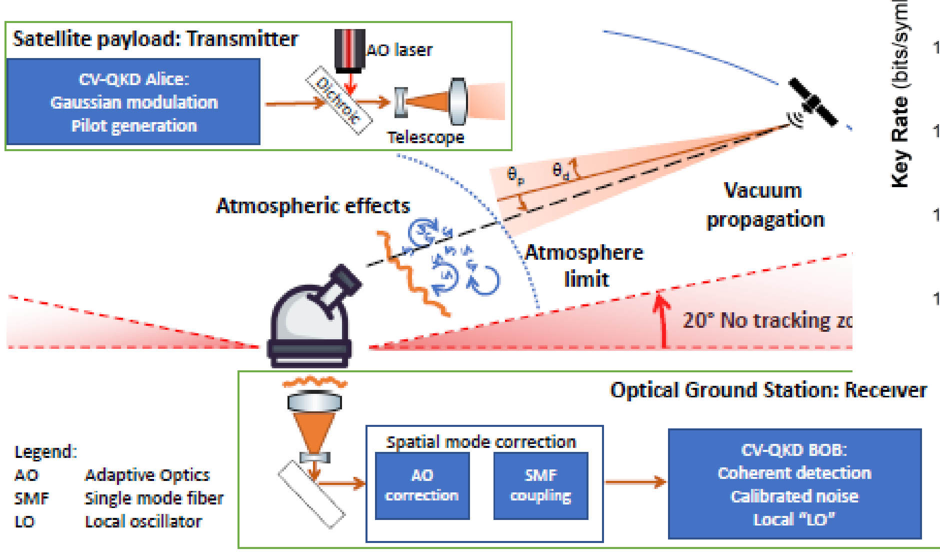


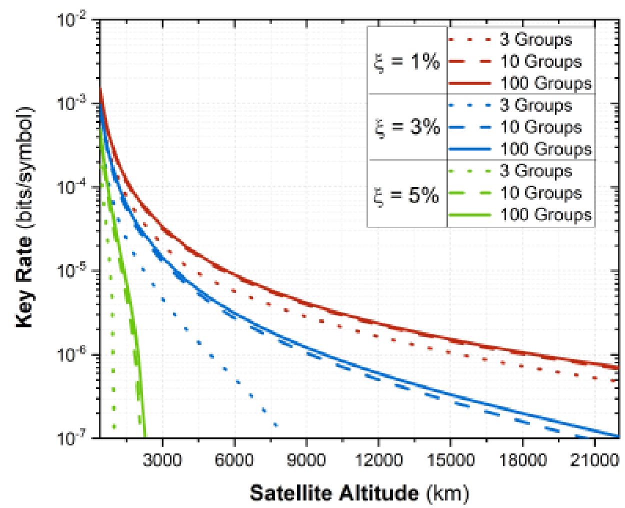




Si PIC, G. Zhang *et al.*, Nature Photon. 2019

Feasibility study, D. Dequal *et al.*, 2002.02002

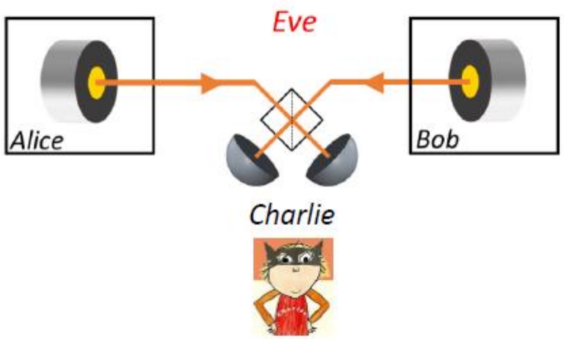


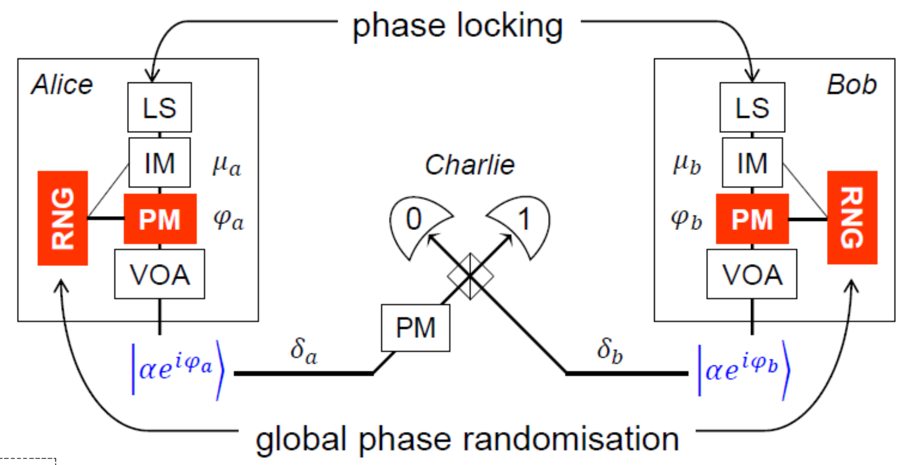


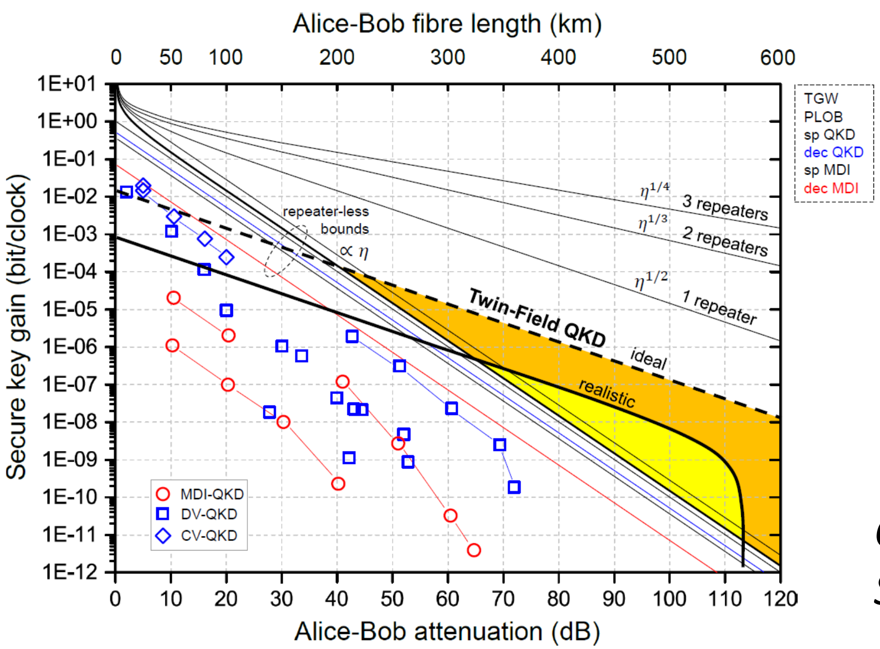
Trusted nodes
Weak loss resilience
Complex post processing

MDI and Twin-Field QKD

Prepare and joint measure, weak coherent pulses, single-photon detectors
Resilience to detector side channels, compatibility with star topology (less trusted nodes), TF beats repeaterless bounds, high loss resilience







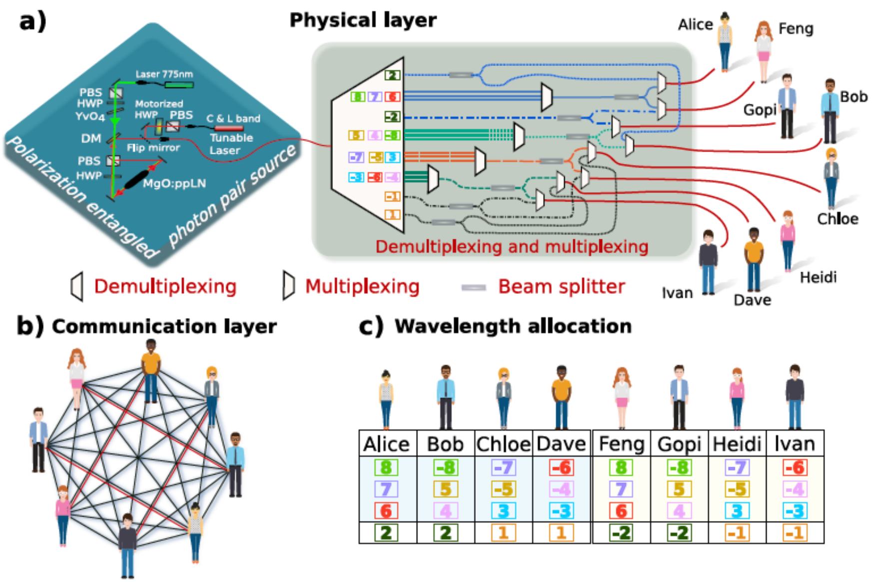
M. Lucamarini's tutorial, QCrypt 2018

Complex implementation, especially for free space
Single-photon detectors

Entanglement-based QKD

Entangled states, single-photon detectors

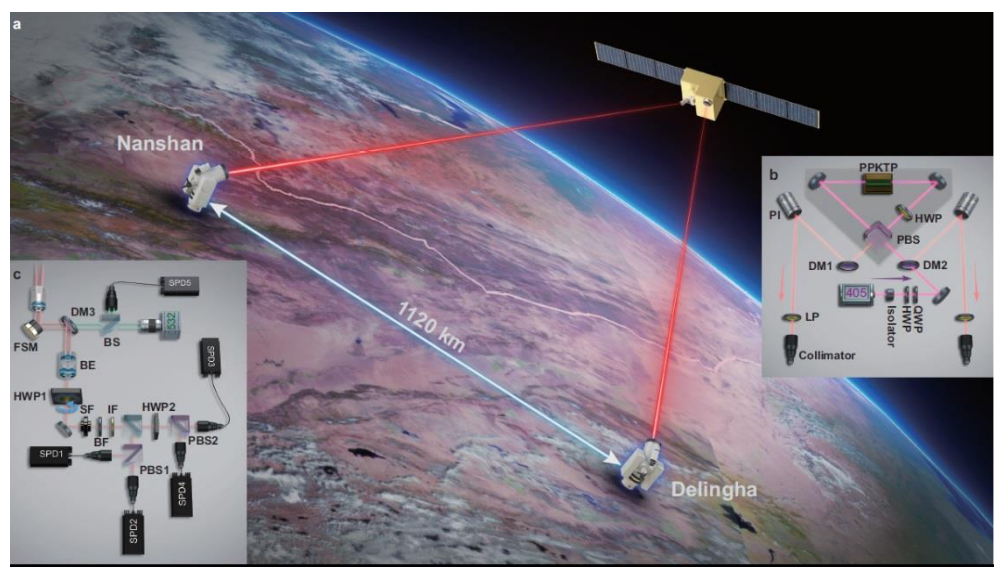
Less trusted nodes, path to device independence, high loss resilience



Alice	Bob	Chloe	Dave	Feng	Gopi	Heidi	Ivan
8	-8	-7	-6	8	-8	-7	-6
7	5	-5	-4	7	5	-5	-4
6	4	3	-3	6	4	3	-3
2	2	1	1	-2	-2	-1	-1

Fully connected graph, S. Joshi *et al.*, 1907.08229

1120 km, J. Yin *et al.*, Nature 2020



Entangled-photon source
Single-photon detectors
Detector side channels
Device independence challenging

Outline of tutorial

Quantum advantage for advanced tasks

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

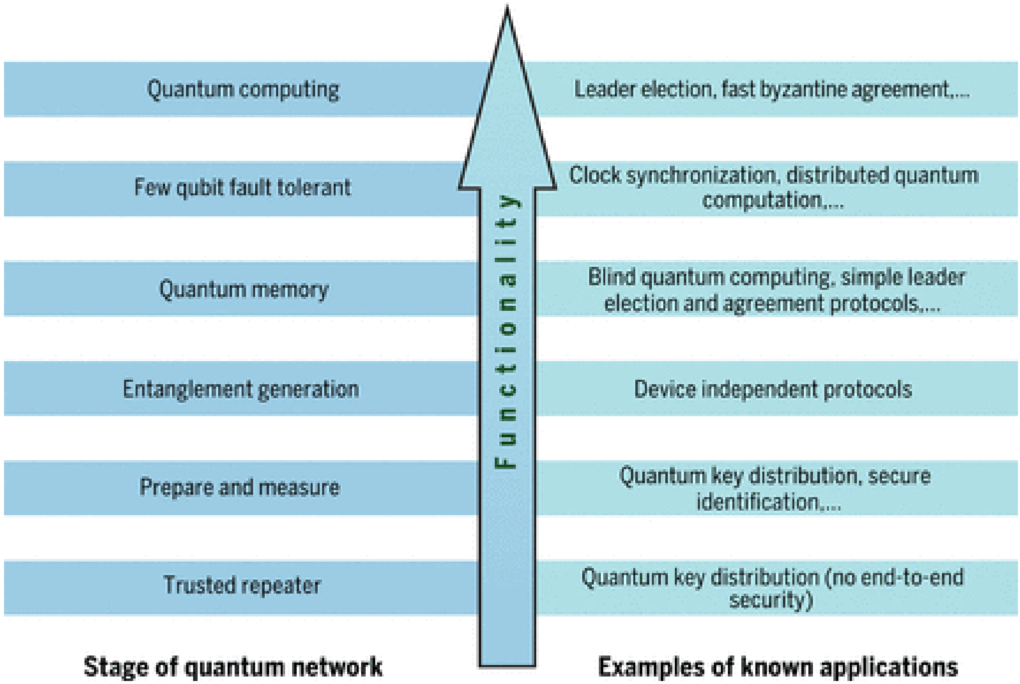
In other configurations many more functionalities
→ Framework for demonstrating quantum advantage (even without ITS)

Secret sharing, entanglement verification, authenticated teleportation, anonymous communication, conference key agreement, secure multi-party computation

Random number generation, quantum money, communication complexity

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

Quantum protocol zoo, wiki.veriqloud.fr



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

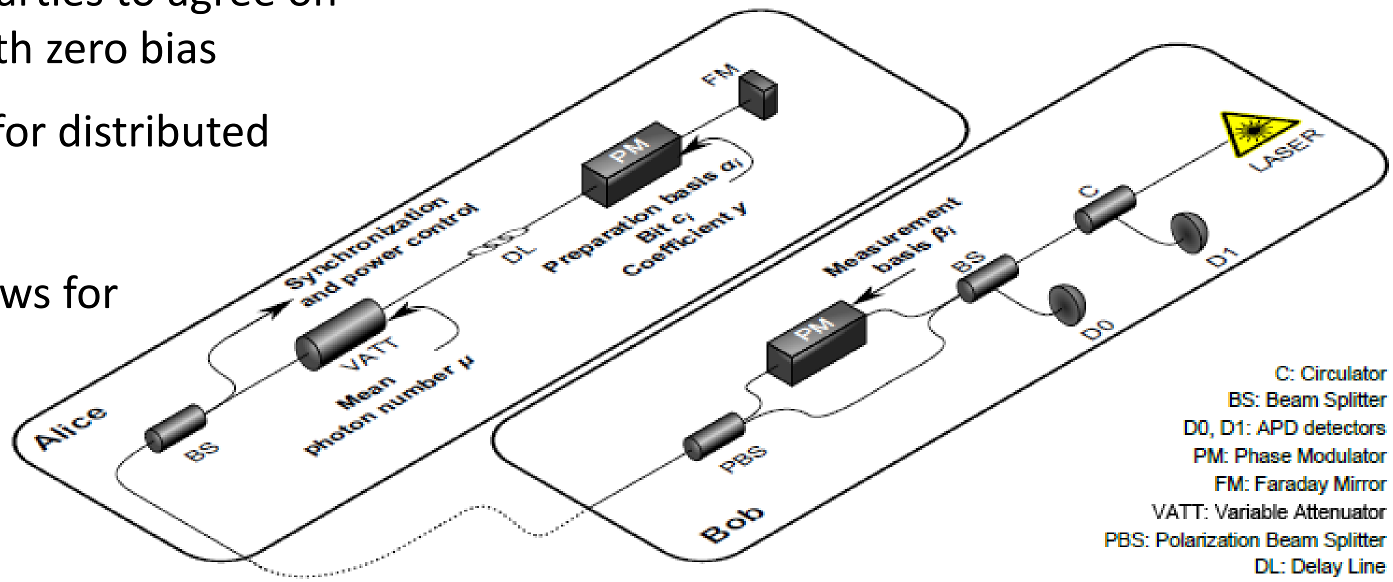
When do we claim a quantum advantage? → fair comparison with classical resources

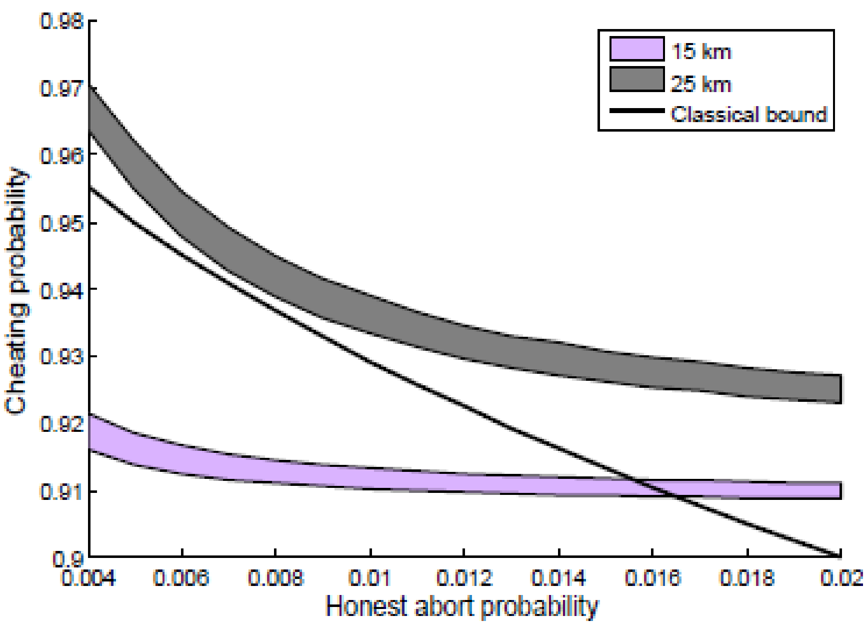
Quantum coin flipping

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





DV-QKD-like plug and play system

Quantum advantage for metropolitan area distances

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

Experimental proposal for weak quantum coin flipping

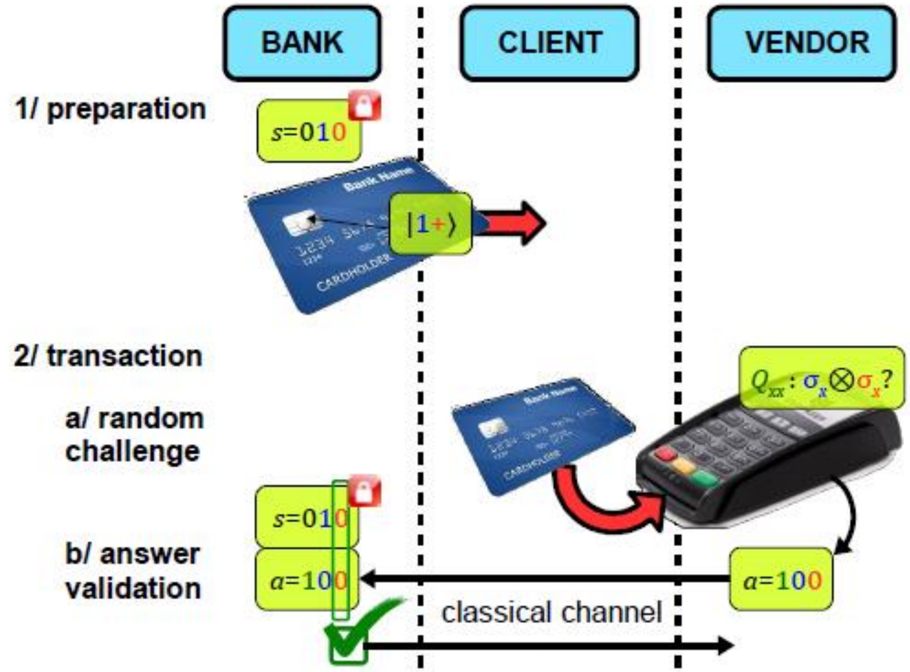
M. Bozzio *et al.*, 2002.09005

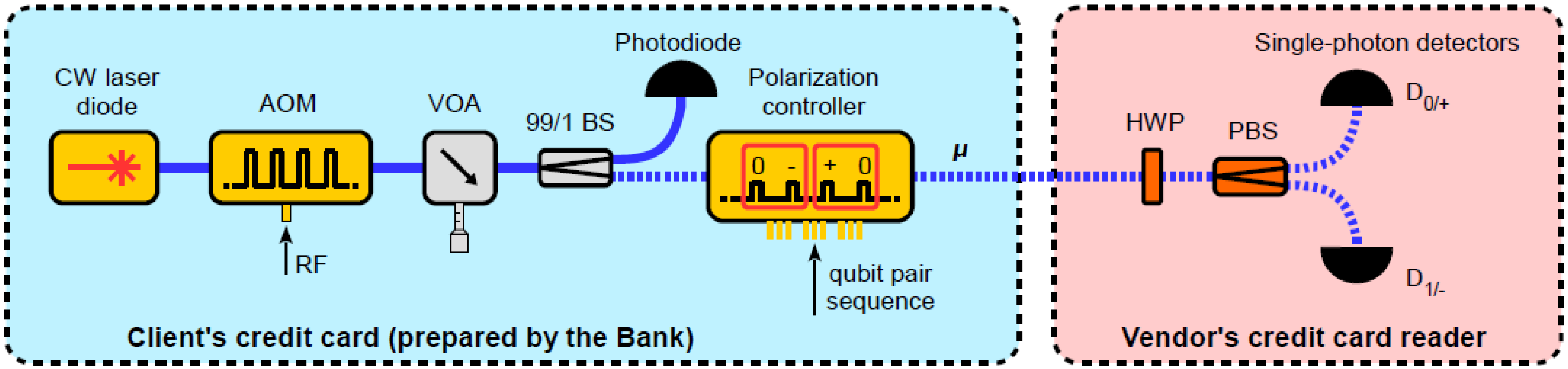
Unforgeable quantum money

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

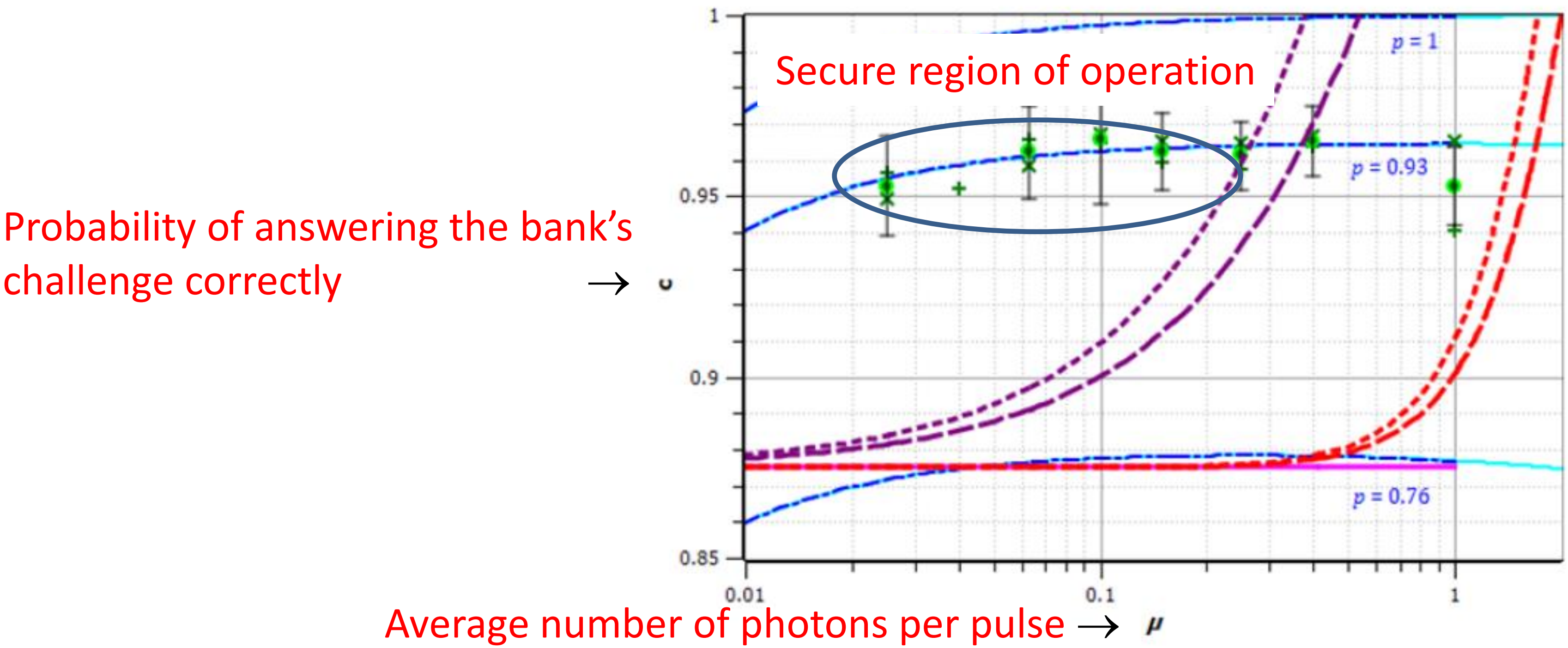
But needs quantum verification and is not robust to imperfections
Considered hard to implement

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





Unforgeable quantum money



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

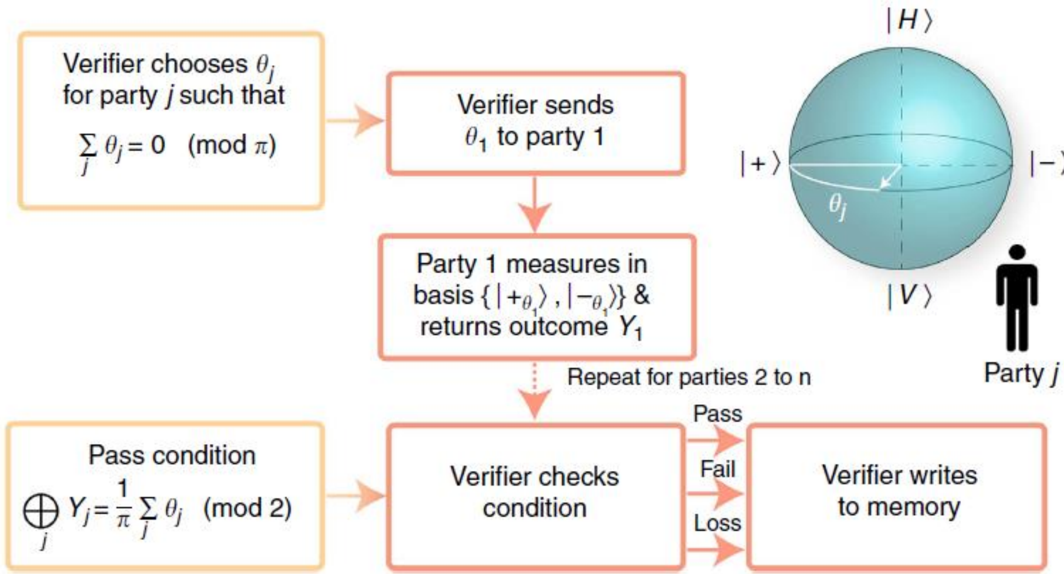
General security framework for weak coherent states and anticipating quantum memory
→ minimize losses and errors using SDP techniques for both trusted and untrusted terminal

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

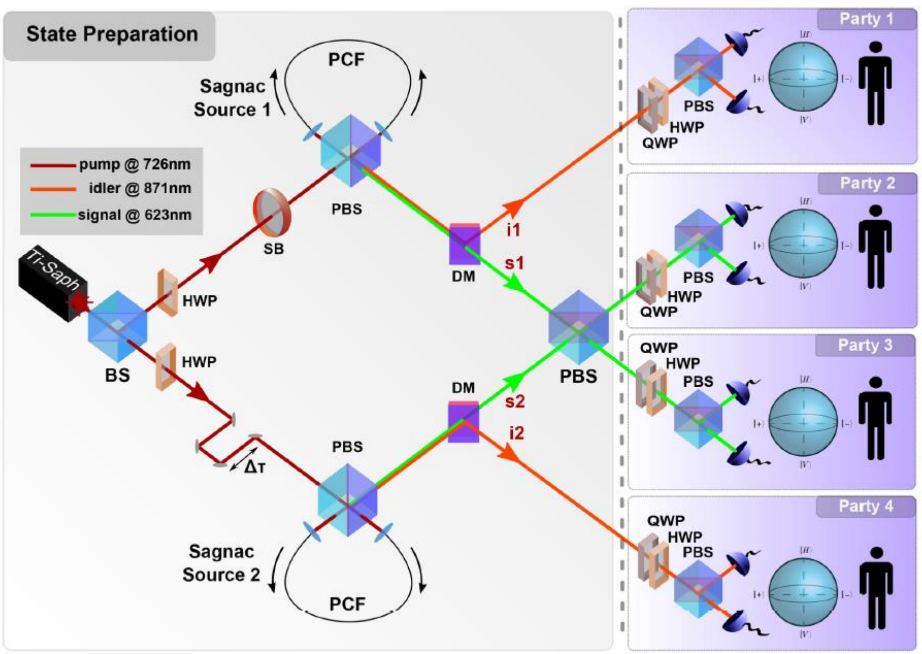
Quantum network protocols

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.*, 2004.07679

Outline of tutorial

Testbeds

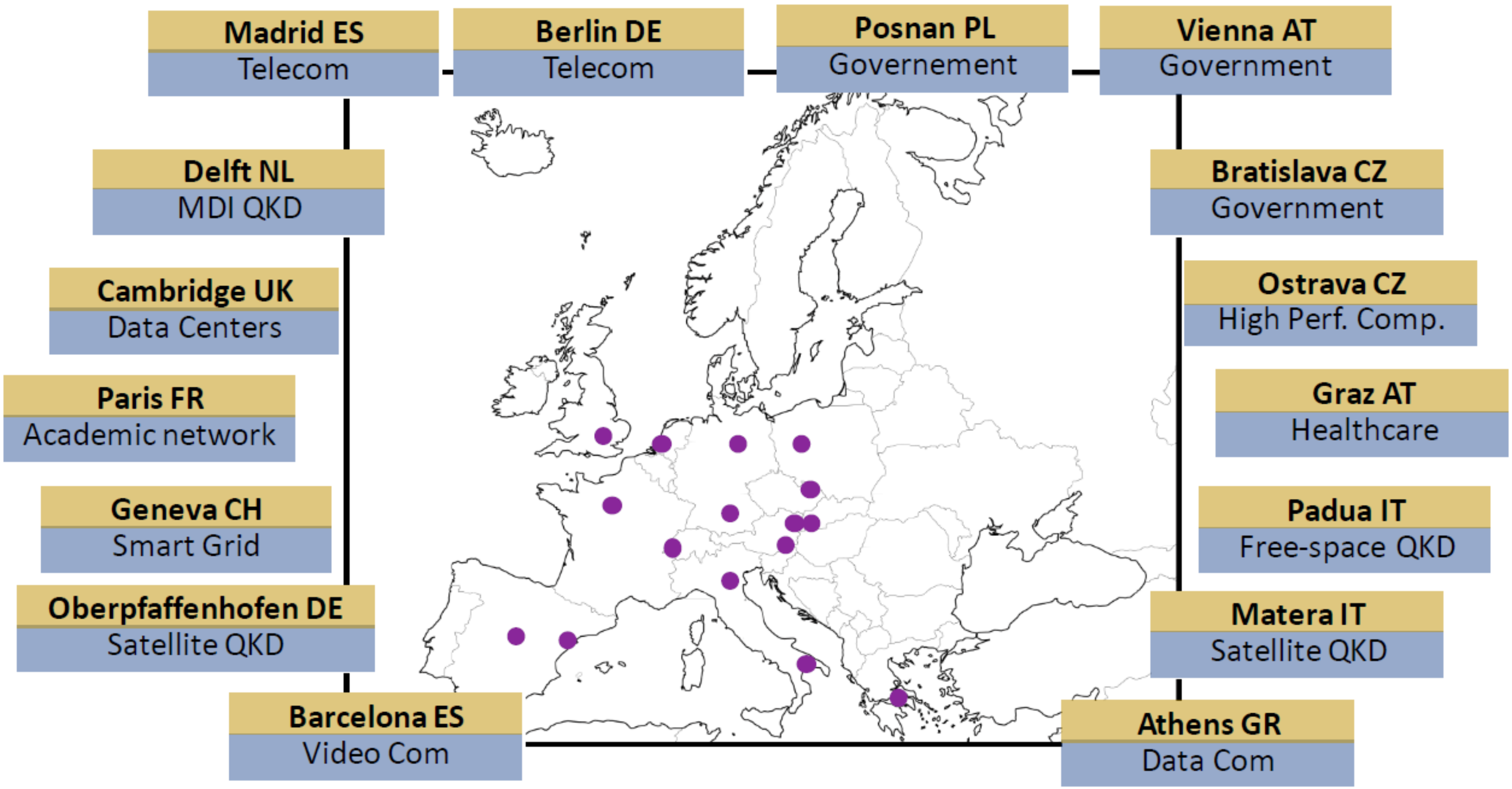
Practical testbed deployment is crucial for
interoperability, maturity, network integration aspects and topology, use case benchmarking, standardization of interfaces

SECOQC QKD network, 2008
South Africa, Swiss, Tokyo, UK QC Hub networks
China 2000 km, 32-node network, including satellite link

- Telco operators
- QKD developers
- Suppliers of classical network equipment
- Academic groups
- End users

OPEN QKD

Open European QKD network



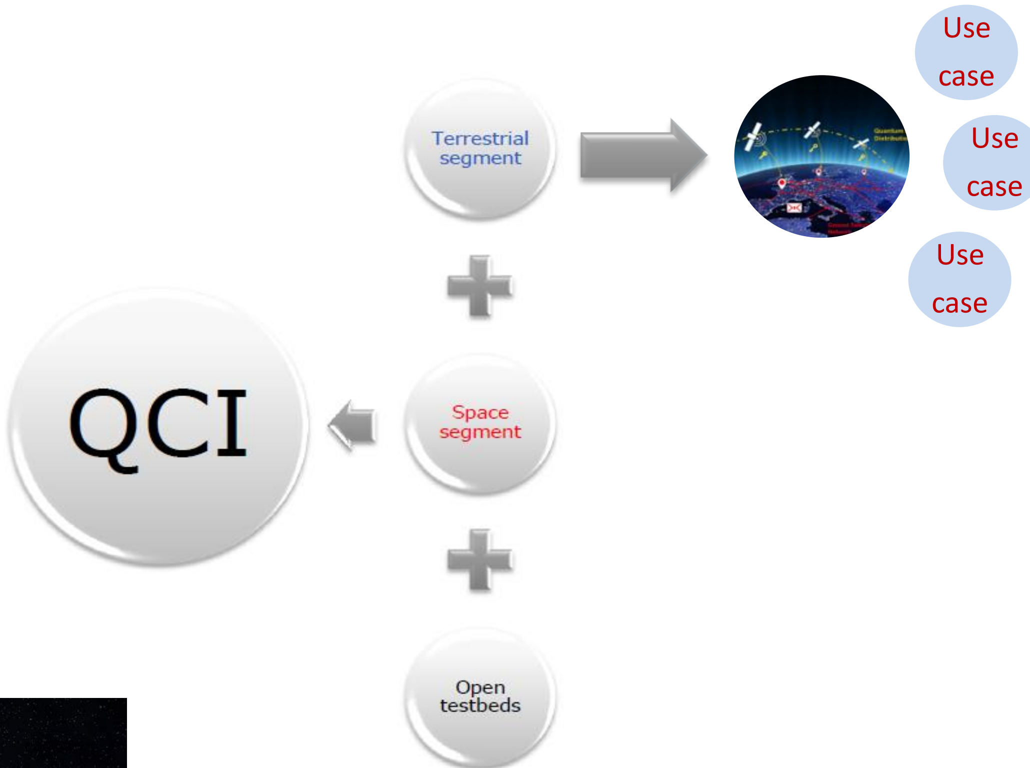
Credit: AIT

Large-scale network deployment is challenging

How many fibers are available? Dark, lit, in pairs? Too high attenuation?

Key management system in place?...

Towards a Quantum Communication Infrastructure



Terrestrial and space segments

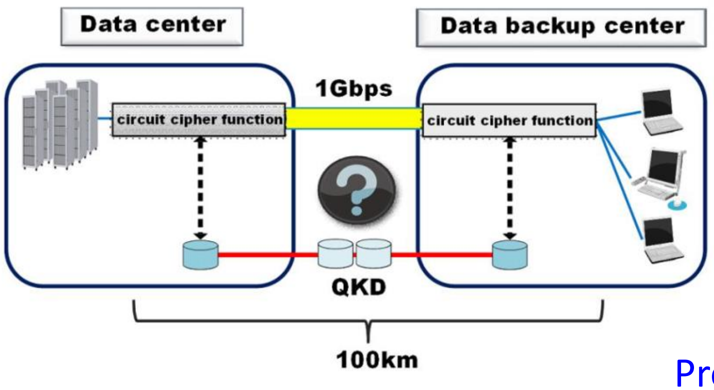
Focus on improving cost, range, network integration, quantum/classical coexistence, security, applications for the quantum internet, standards and certification

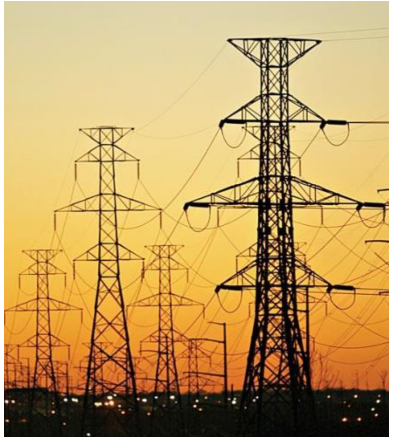
Top-down approach, driven by real use cases

Use cases

Data centre storage and interconnection

Connection between headquarters and disaster recovery centres





Protection and resilience of critical infrastructure

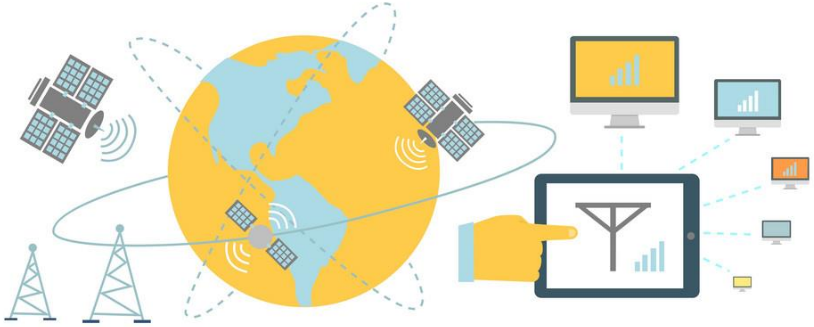
Electrical power grid command & control, water management,…

High level government communications

Software defined telecom networks

Medical file transfer

Communication between quantum processors



Conclusion

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

The quantum communication toolbox is rich and increasingly advanced

Current rapid advancements address the multiple, interlinked challenges

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

A future quantum communication infrastructure can address a range of use cases with high security requirements in configurations of interest

Thank you!