“Quantum Gives and Quantum Takes Away”

If computers that you build are quantum,
Then spies of all factions will want 'em.
Our codes will all fail,
And they'll read our email,
Till we've crypto that's quantum, and daunt 'em.

Jennifer and Peter Shor

To read our E-mail, how mean
of the spies and their quantum machine;
Be comforted though,
they do not yet know
how to factorize twelve or fifteen.

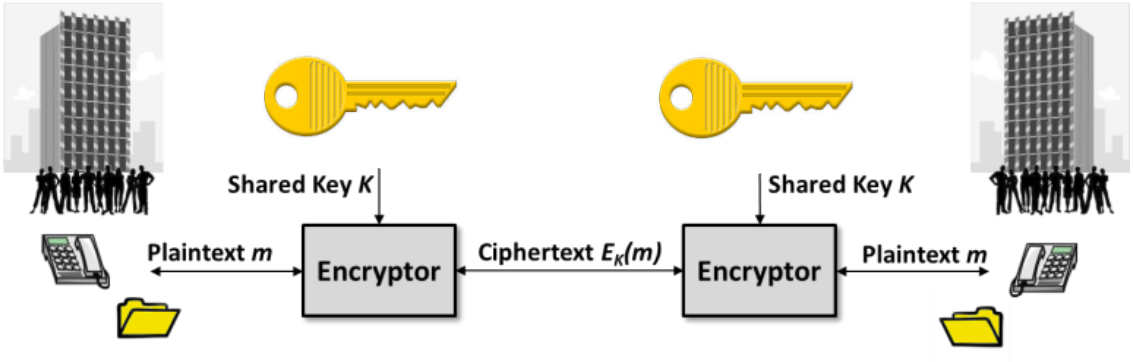
Volker Strassen (1998)

KEY DISTRIBUTION

There is a information theoretically secure way to encrypt messages.

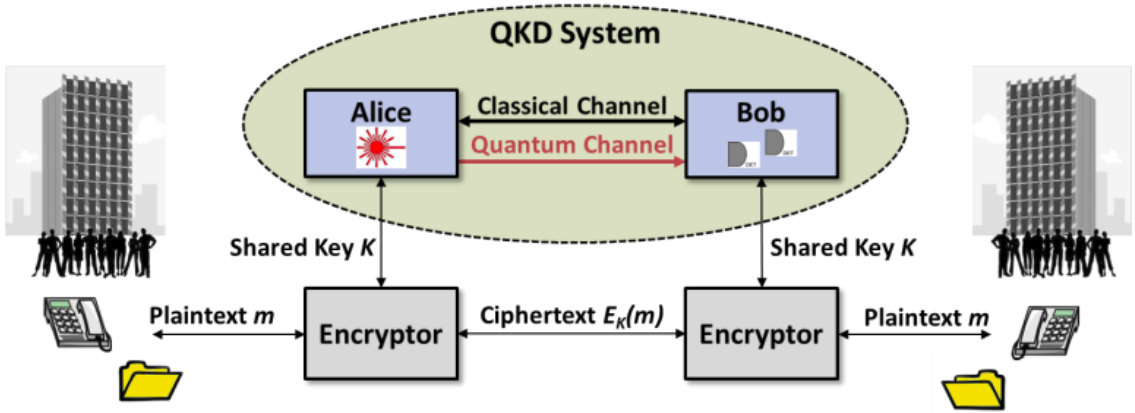
One-time pad: symmetric cipher

Prerequisite: distribution of random keys



QUANTUM KEY DISTRIBUTION

ITS method to exchange key between two partners.



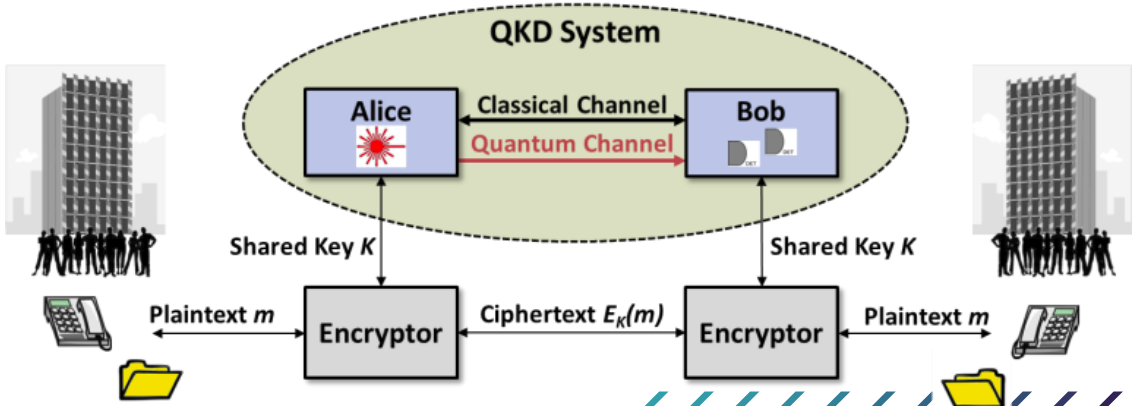
QUANTUM KEY DISTRIBUTION

Symmetric Key:

- QKD does not encrypt messges
- QKD produces the key
  - **secure**
  - **identical**
  - **random**
- QKD key is used in classic symmetric encryption (e.g. one-time pad, AES)

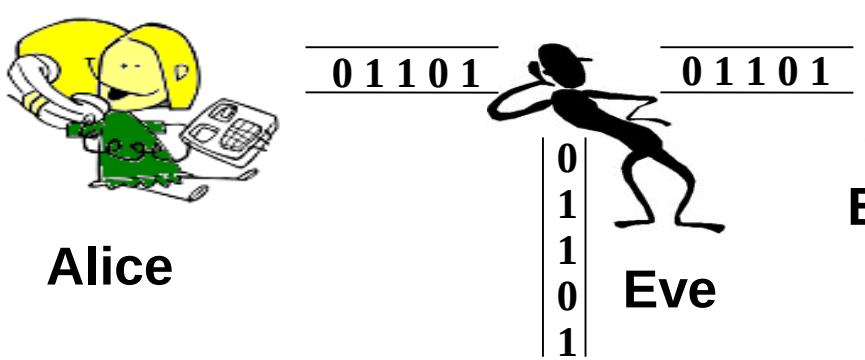
Security:

- is based on **quantum physics**
- an eavesdropper will inevitably introduce errors (Heisenberg uncertainty)
- secure against **classic attacks**
- Secure against all **quantum attacks** (incl. quantum computer)

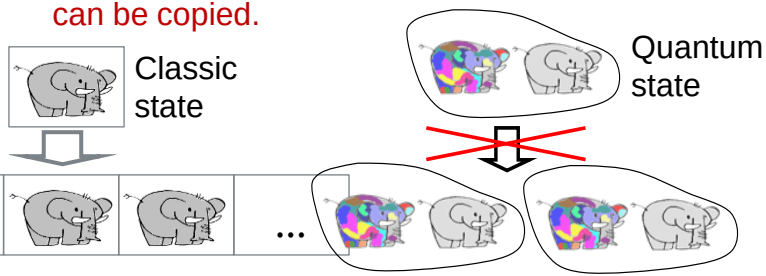


QUANTUM CHARACTERISTICS

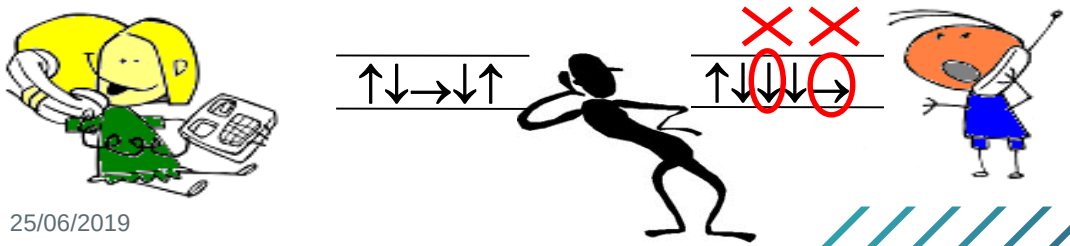
- ***No-Cloning Theorem:*** Classic information can be copied, but quantum information cannot.



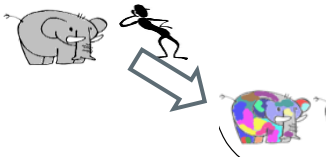
Eavesdropping on classic information goes undetected since an unknown classical state can be copied.



- ***Heisenberg's Uncertainty Principle:*** Classical states can be fully determined but quantum states cannot.



Because measurement alters quantum states, eavesdropping on quantum information can be detected.

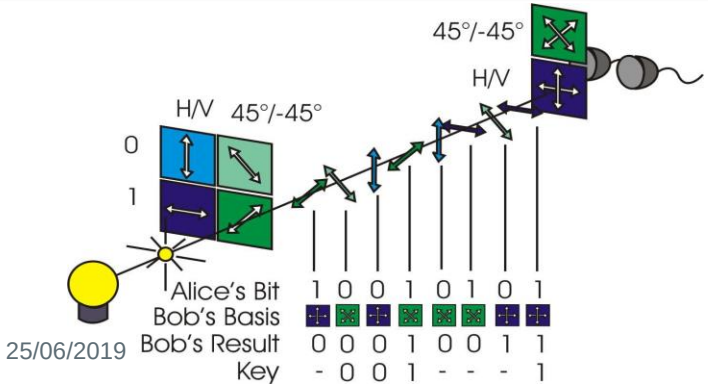


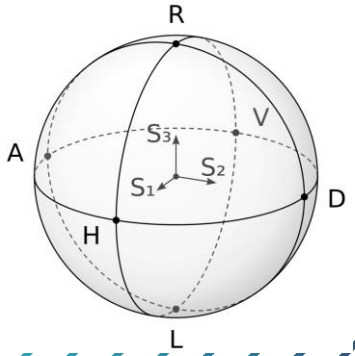
QKD PROTOCOL – STEP 1

AUSTRIAN INSTITUTE OF TECHNOLOGY

Quantum-Optics channel

- Generation of **random sequence** (e.g. Quantum Random Number Generator)
- Alice **encodes** her information in non-orthogonal quantum states (e.g. polarisation state of photons).
- Alice **transmits** the photons through a quantum channel and Bob performs **measurements** on the received photon.
- If the key is unperturbed, then QM guarantees that no one got any information about this key by eavesdropping (i.e. by measuring) the quantum communication channel.
- If, on the contrary, the key turns out to be perturbed, then A and B simply disregard it.





$$QBER = \frac{\text{false counts}}{\text{all counts}}$$

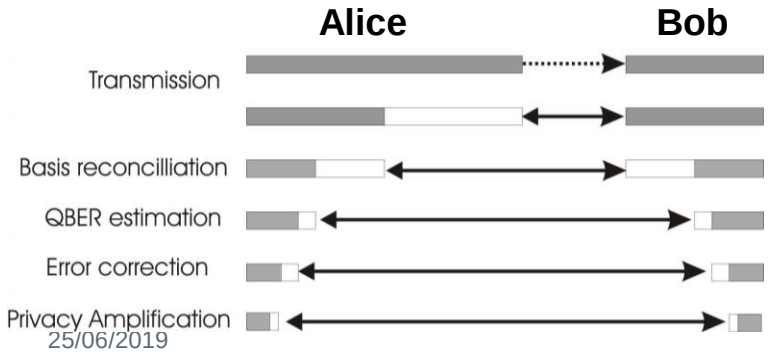
QKD PROTOCOL – STEP 2

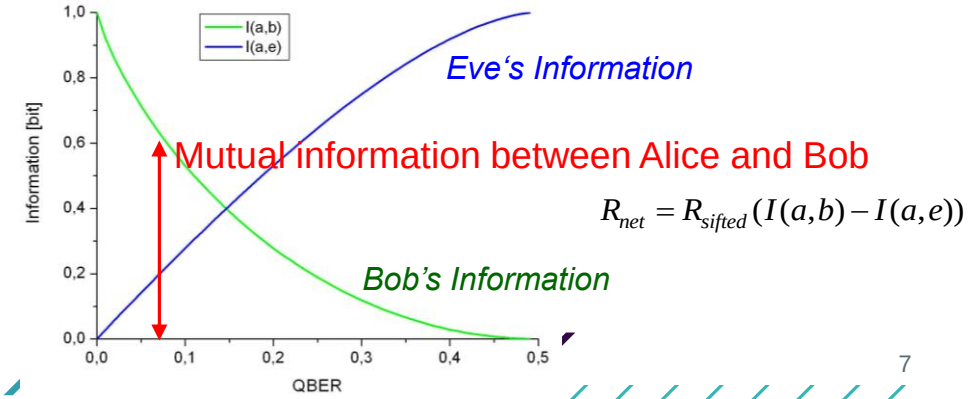
Post-Processing (**classical** channel)

QKD Post-Processing stack

- **Error Correction** (producing perfect correlation between parties‘ keys)
  - Forward Error Correction, Two-Way Reconciliation
- **Privacy Amplification**
  - generates a composable, proofably secure key
- **Authentication** (detects man-in-the-middle attacks)

Symmetric encryption with obtained QKD key using a classical protocol (classical channel)



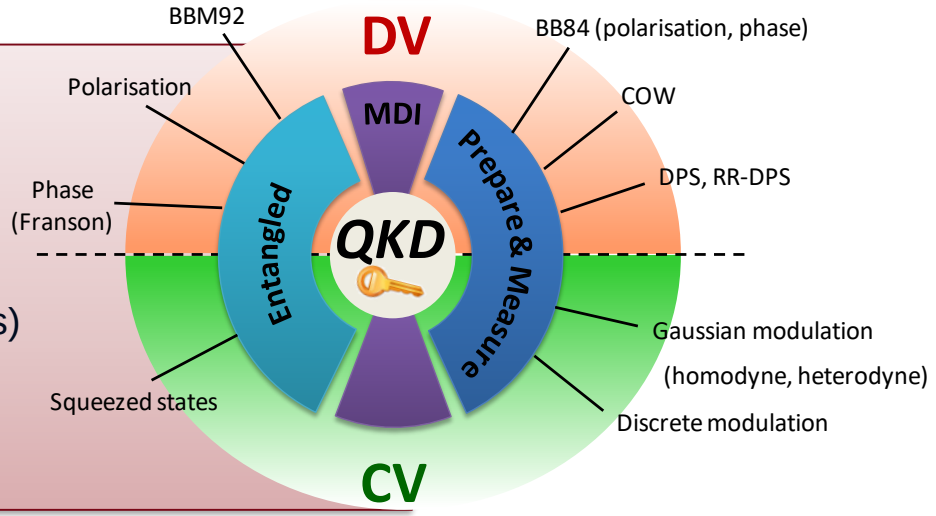


$$R_{net} = R_{sifted}(I(a,b) - I(a,e))$$

QKD FLAVOURS

Implementation

- Quantum information mostly encodeded in **polarisation** or **optical phase**
- Quantum states:
  - Entangled photons
  - Weak coherent pulses (faint laser pulses)
  - Coherent states (CV) avoiding SPADs
- Rates: kbit/s to Mbit/s, depending on distance and detector



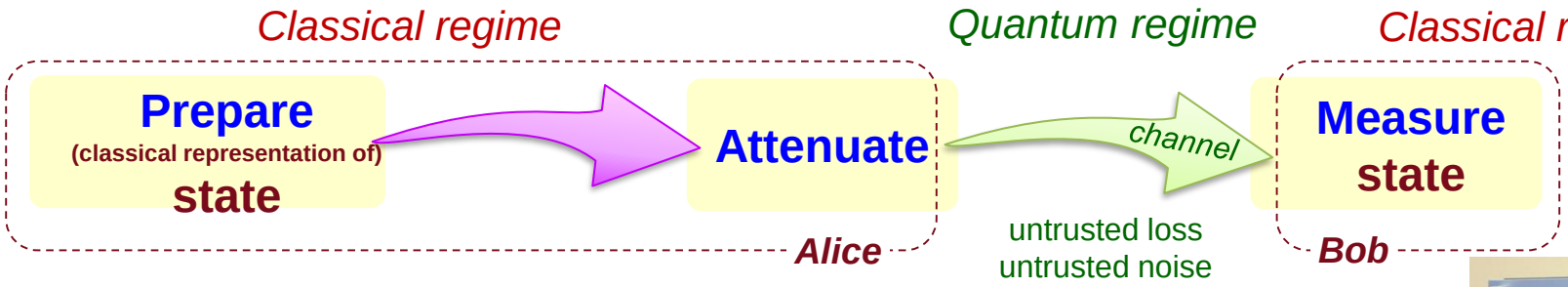
Quantum Channels

- **Optical fiber**: up to 100 km (500 km in lab)
- **Freespace** links using telescopes: meters up to 100 km
- High-altitude platforms: balloons, airplanes, drones: up to 10 km
- **Satellites:** ~ unlimited (LEO)

Use-cases and applications will demand different technological solutions

- Secure key rate
- Maximal transmission distance
- Choice of quantum channel
- Form factor
- Price (CapEx/ OpEx)

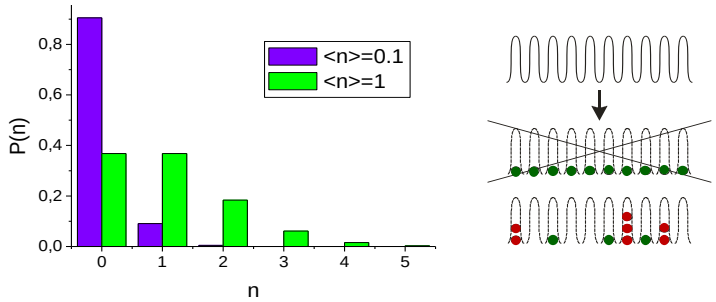
PHYSICAL IMPLEMENTATION DV-QKD



Discrete variables QKD

- Single photon source
- Phase or polarisation encoding
- Single photon detectors (InGaAs APDs)
  - Slow
  - Expensive
  - bulky

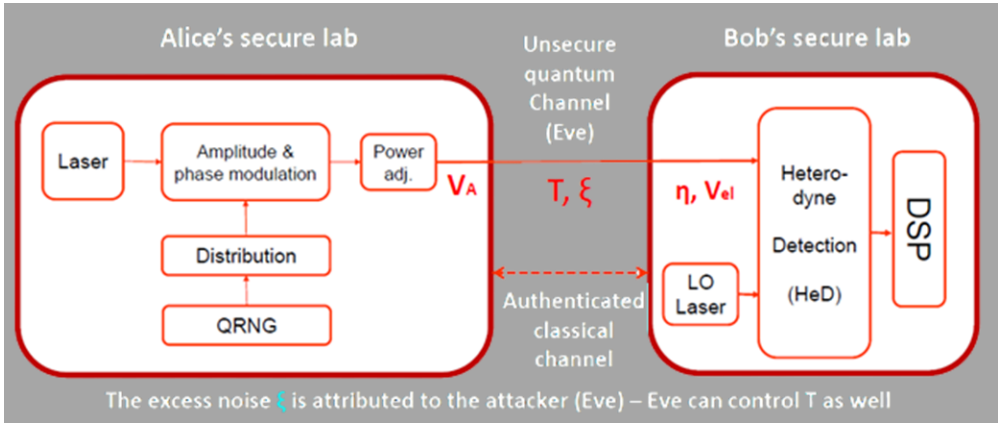
Photon number statistics of attenuated laser pulses



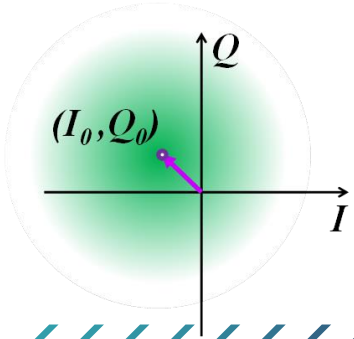
PHYSICAL IMPLEMENTATION CV-QKD

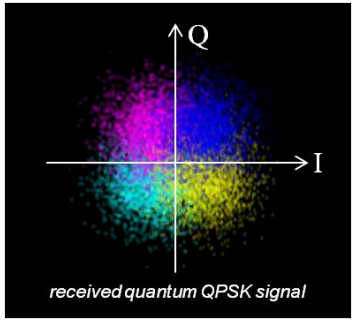
Continuous variables QKD

- Attenuated laser
- QAM encoding
- Coherent detectors
  - Chip-level integration
  - High Rate (> GHz)
  - Compatible with modern optical telecommunication
- Extensive Postprocessing
- Less robust to loss



$\Delta I \cdot \Delta Q \geq 1\text{SNU}$





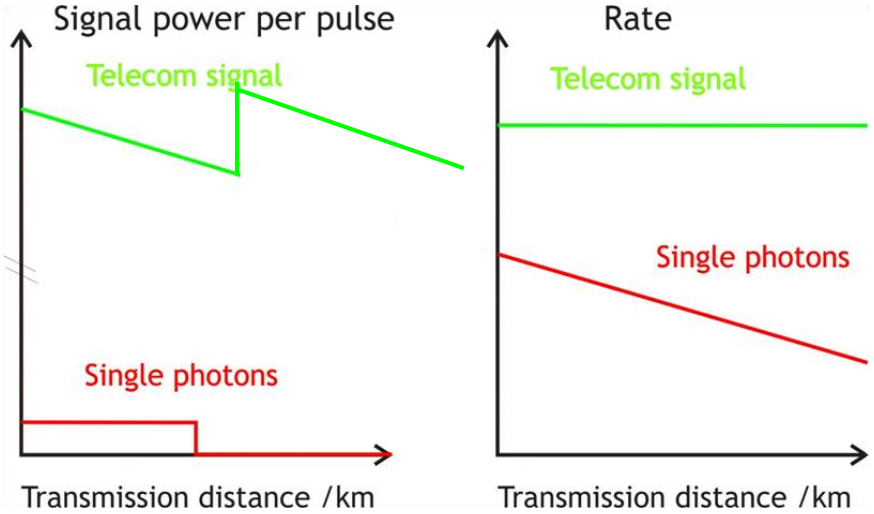
DISTANCE LIMITATIONS

Classic Signals

- Loss tolerant → re-amplify as required
- 10s to 100s of channels over a single fiber

Quantum Signals

- Loss limit at which rate drops rapidly.
- No re-amplification possible unless quantum repeater becomes available
- Very fragile: typical power of -70 dBm or less, any nearby classic channel will flood the quantum channel with noise (ASE, Raman)

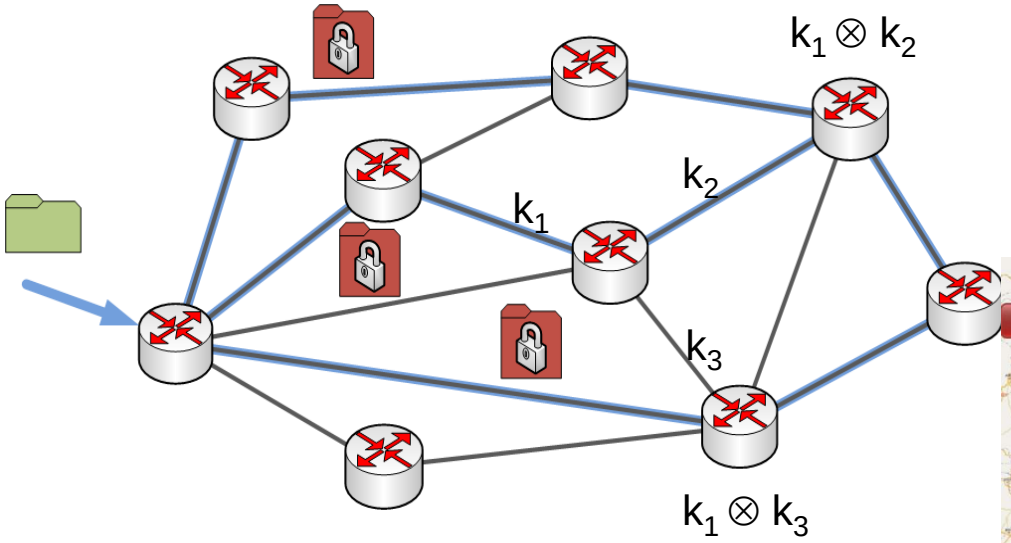


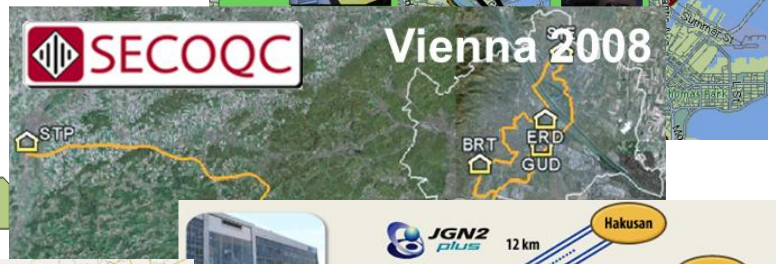
Still, we need to incorporate quantum signals in existing infrastructures – without OpEx-incurring dark fiber.

BEATING THE DISTANCE – NOW

Trusted Repeater Networks

- Key is available in classical form at nodes



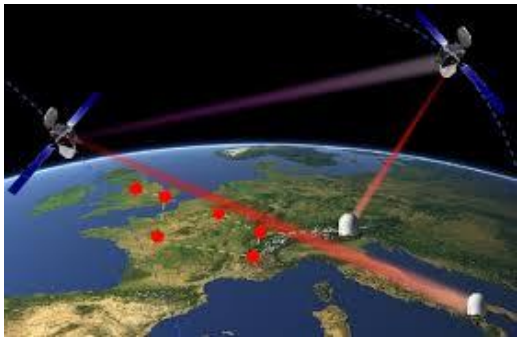


BEATING THE DISTANCE – IN FUTURE

Satellite QKD

+ • unlimited range

− • high cost
• low rate
• ground stations



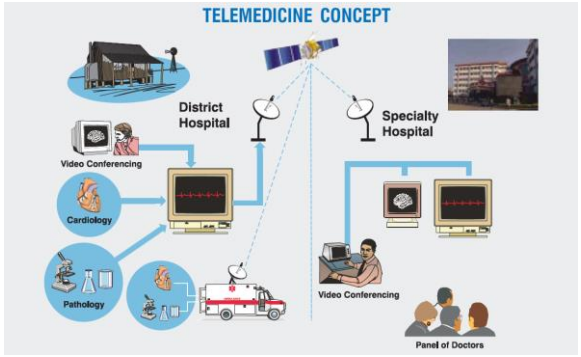
Quantum repeaters

+ • unlimited range in fibers
• no trusted nodes
• end-to-end security

− • technologically extremely challenging

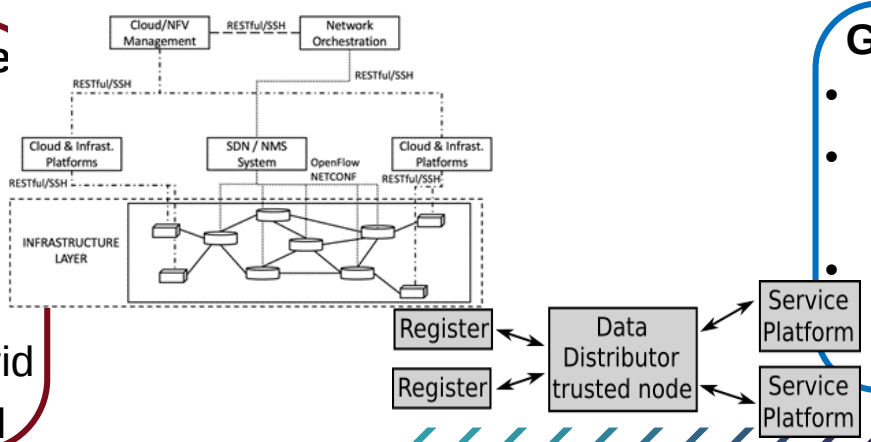
QKD USE-CASES

Data Services
- Data exchange
- Data/Cloud Centers
- High performance computing
- Long term storage



Health applications
- Storage of medical data
- Telemedicine
- Patients data
- Medical data mining

Critical infrastructure
- Telco networks
  - Control plane
  - SDQN
- Energy Grid
  - Smart meter/grid
  - Intrusion denial

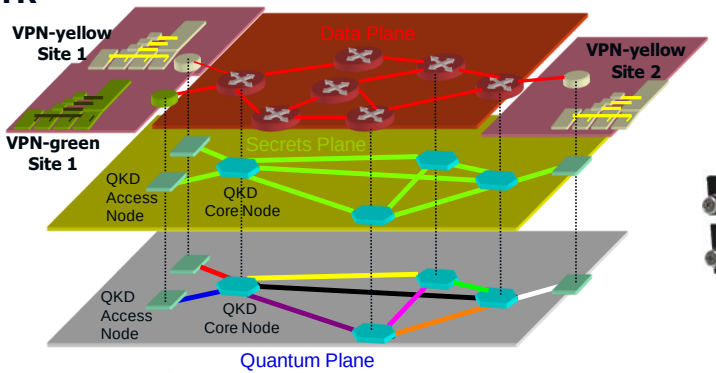


Governmental services
- e-Government
- Emergency services (database)
- High-security channels
- Financial services

NETWORK ARCHITECTURES

QKD Backbone network

- Mesh network
- Dark/lit fiber
- Trusted repeater

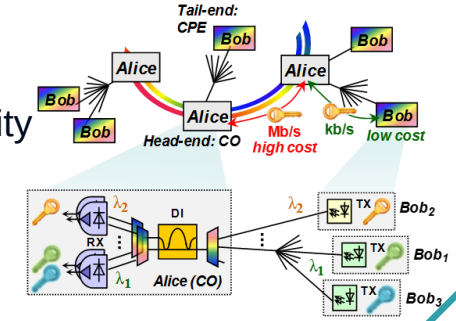


High performance QKD

- High rate
- Long range
- Coexistence
- SDN capabilities

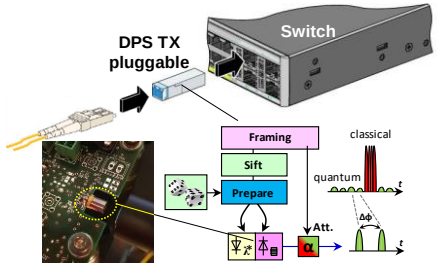
Access network

- Shared fiber
- End-user functionality
- Star network
- QIoT



Low-cost QKD

- low cost
- CapEx sharing
- small form factor
- Short distance
- Coexistence
- Low rate (multiplexing)



POST QUANTUM CRYPTOGRAPHY

- Also called **quantum safe/resistant cryptography**
  - **NOT quantum cryptography (= quantum key distribution (QKD), etc.)**

- Cryptosystems which run on classical computers, and are **considered** to be resistant to quantum attacks (no known exponential quantum speedup)
  - Based on **structured hardness** assumptions (lattice-based, super-elliptic curve, etc.)
  - (Public key) encryption schemes, signature schemes, Key-establishment (like DH), etc.
- Only proven for **known** quantum computing **algorithms**
- **No** classical **ITS** security

NIST is running a project for Post-Quantum Cryptography Standardization
  - Signatures, Encryption and Key-establishment
  - Standard in 2023-2025

INGREDIENTS FOR QUANTUM ICT

Quantum applications

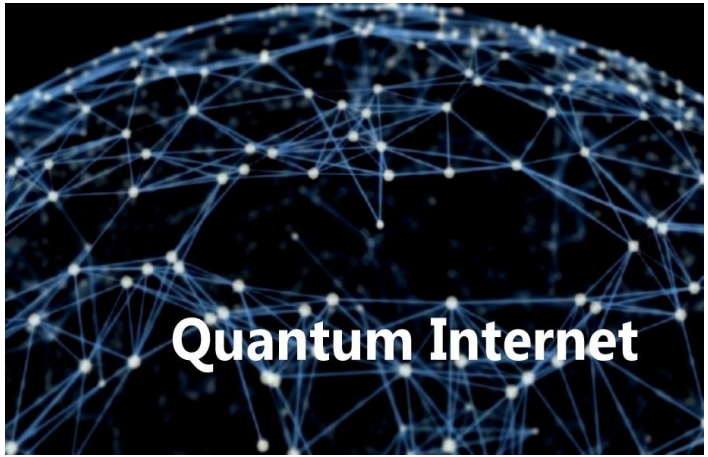
- Use-cases
- Algorithms
- Interfaces to classical ICT

Quantum devices

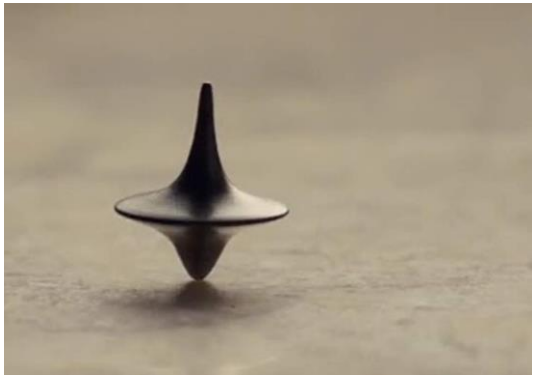
- Devices for all QKD flavours, and other primitives
- PIC based systems
- Interfaces/conversion of flying qubits
- Quantum Computer
- Quantum Sensors

Quantum network

- Terrestrial fibre
- Free space
- Satellites
- Quantum repeater



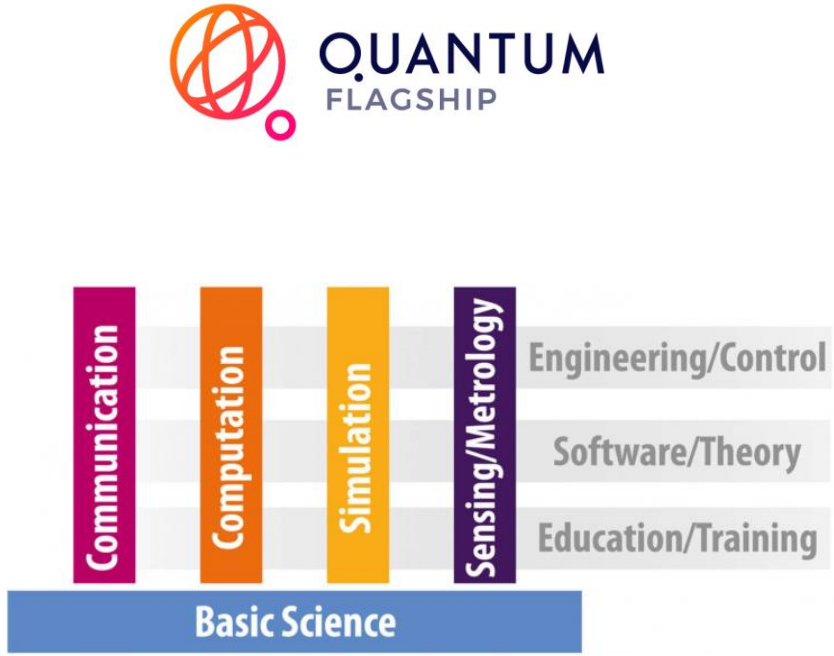
Is it all a dream ?



QT FLAGSHIP

Quantum Technology Flagship

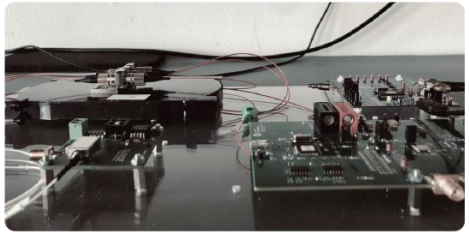
- 1 billion Euros
- 10 years duration
- Ramp-up phase (2018-2021)
- 20 projects in the QT pillars
- Focus on technological progress
- First step towards an EU Quantum Technology Ecosystem



CIVIQ

Continuous Variable Quantum Communications

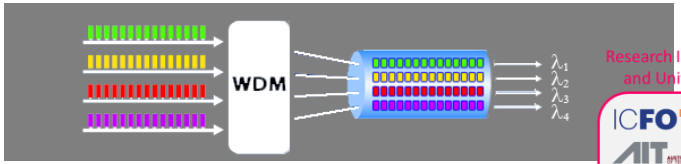
Project coordinator: ICFO, Spain



Increase TRL for CV-QKD

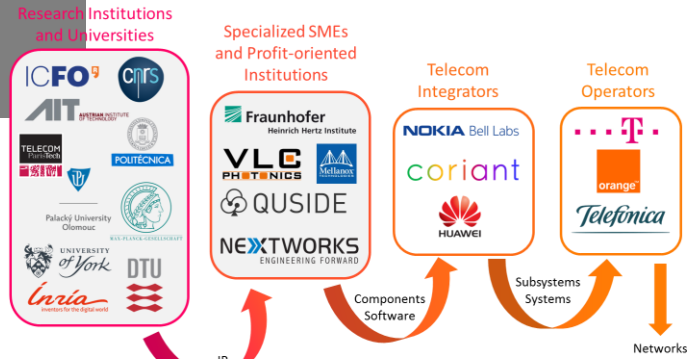
- High symbol rate
- Cost-effective scalable system design
- Photonic integration of components

Strengthened WDM Coexistence



Software define network (SDN)-interfaced systems and network

Validation over Datacom and telecom infrastuctures



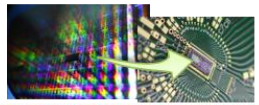
UNIQORN

AUSTRIAN INSTITUTE OF TECHNOLOGY

UNIQORN
Affordable Quantum Communication for Everyone

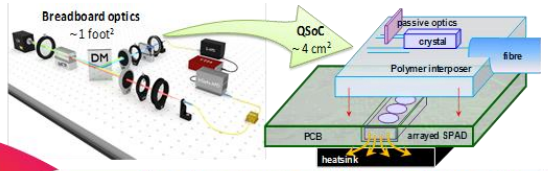
Project coordinator: AIT, Austria

- Photonic integration
- Quantum systems on chip
- Quantum applications
- Field trials in telco networks



I. Develop value-added InP, CMOS and polymer quantum-optic communication components.

Quantum Fab



II. Shoehorning breadboards into chips – Develop a quantum System-on-Chip methodology.

III. Demonstrate the power of the technological food-chain: Realize feature-rich, scalable key sub-systems for quantum comms.

IV. Deployable system performance and novel network functionalities.

Quantum App

V. Demonstration of low-cost quantum links and novel end-user quantum applications beyond QKD in lab and field.

EU QUANTUM TECHNOLOGY ECO-SYSTEM

ESA Scylight

- SeCure and Laser communication Technology
- Quantum Cryptography Technologies and initial services demonstration

QKD Testbed

- Pilot for **Pan-European** QKD network
- **Use-case** demonstrator
- **Showcase** for European Quantum Communication Technology
- **Attract** industry, suppliers, end customers, policy makers, etc.

source: www.qt.eu

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

THANK YOU!

Fabian Laudenbach & Hannes Hübel, 13th March 2019