GN4-3: Quantum Key Distribution activity

Network Technology Evolution task

Xavier JEANNIN (RENATER), *task leader*
Piotr RYDLICHOWSKI (PSNC), *QKD technical leader*

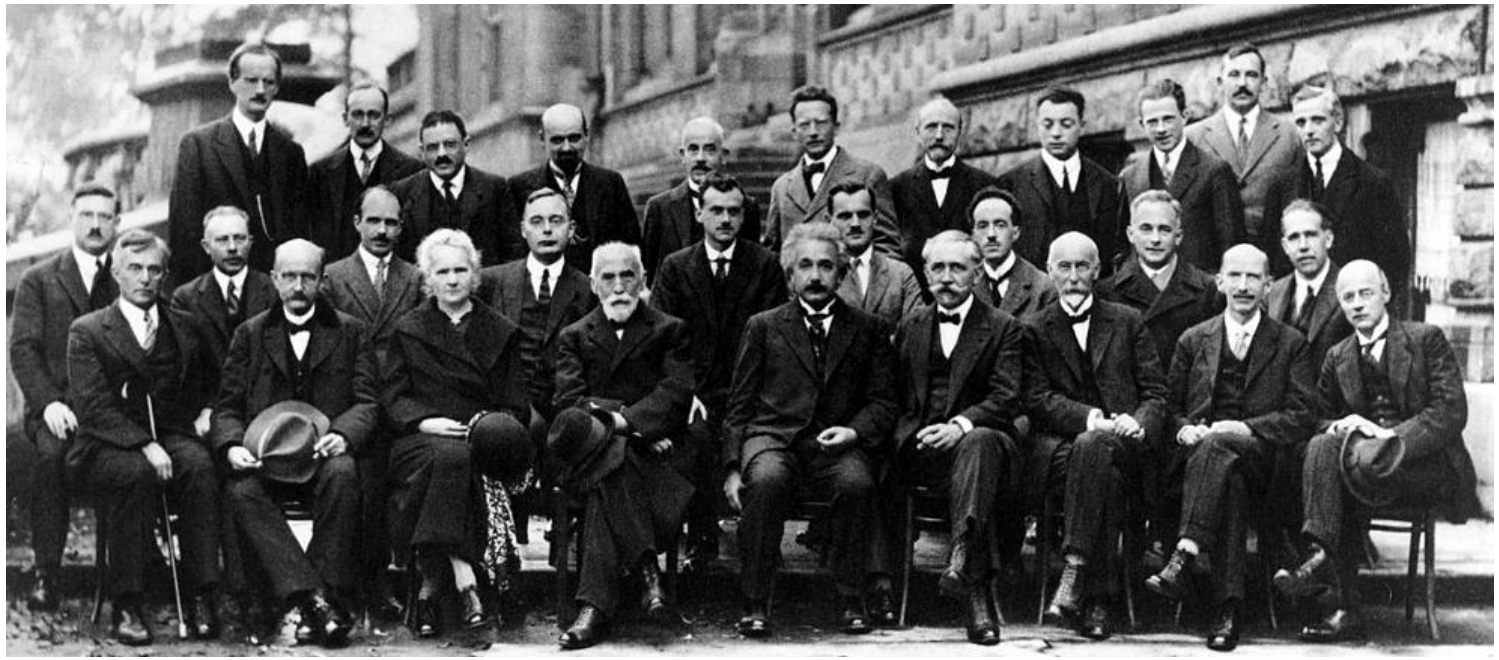
Quantum Spotlight, GA, 6 Dec. 2021

www.geant.org

quantum-discuss@lists.geant.org

Quantum, ‘the next technology revolution’?

- The **first quantum revolution** enabled inventions that followed the rules of quantum mechanics
- The **second revolution** is about controlling individual quantum systems and using the quantum principles (**no cloning theorem, superposition, entanglement & nonlocality**) to design and build new devices or systems



Auguste Piccard, Émile Henriot, Paul Ehrenfest, Édouard Herzen, Théophile de Donder, Erwin Schrödinger, Jules-Émile Verschaffelt, Wolfgang Pauli Werner Heisenberg Ralph H. Fowler, Léon Brillouin

Peter Debye, Martin Knudsen, William Lawrence Bragg, Hendrik Anthony Kramers, Paul Dirac, Arthur Compton, Louis de Broglie, Max Born, Niels Bohr ;

Irving Langmuir, Max Planck, Marie Curie, Hendrik Lorentz, Albert Einstein, Paul Langevin, Charles-Eugène Guye, Charles Thomson Rees Wilson, Owen Willans Richardson.

Quantum, ‘the next technology revolution’?

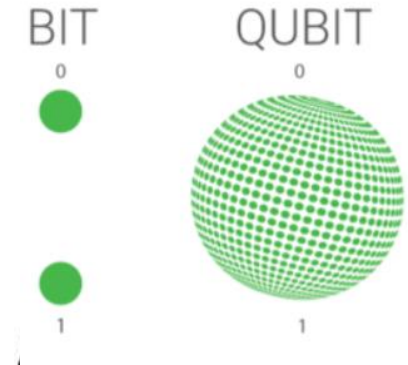
- ‘Quantum’ is receiving large amounts of funding from the EC (Quantum Flagship, European QCI) and large national programs

- ‘Quantum’ is highly likely to have a disruptive impact in many fields:
    - Quantum computing
    - Quantum communication (including quantum key distribution)
    - Quantum simulation
    - Quantum sensing

Quantum communication

- The photon is a robust quantum particle that can be used for quantum communication
- The ‘Quantum Internet’ is for now at the research stage. It will affect the future of networking, but how?
- How can the R&E network community support its users (researchers, universities) to become leaders in this area?
- How can the GN4-3/GN5 projects help the R&E network community (NRENs) to handle the emerging quantum area?
- How can NRENs get involved? What is the impact on their infrastructures?

- QKD is the first quantum communication technology that could be deployed on research networks in the foreseeable future



QKD implementation

- **QKD commercial device providers**
  - QuantumCTek (China)
  - IdQuantiqe (Swiss)
  - Toshiba QKD (Japan, UK)
  - InfiniQuant (Germany)
  - Huawei's European Research Centres

QuantumCTek

IDQuantique

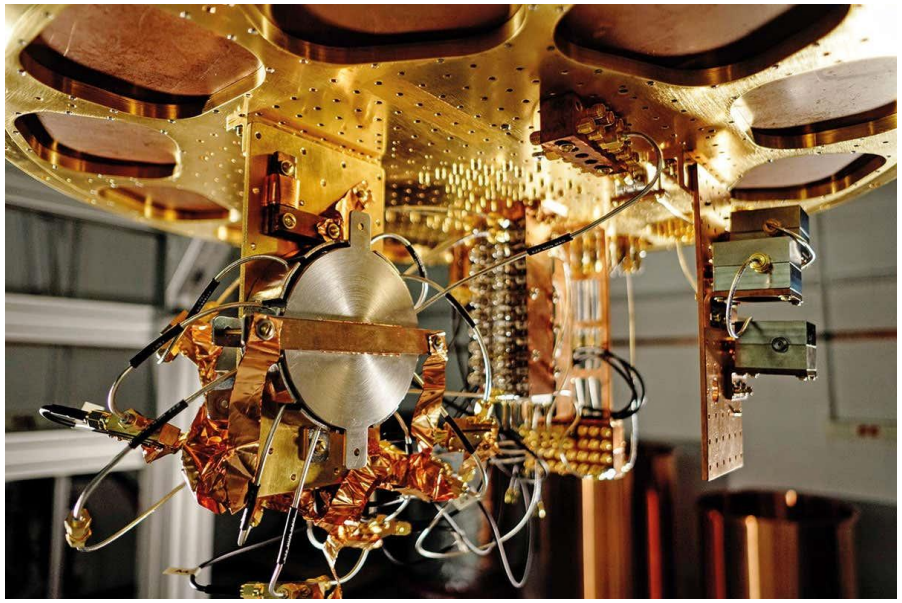
- **A first cross border**, point-to-point full QKD line was deployed between PSNC (Cieszyn) and CESNET (Ostrava - VSB – Technical University of Ostrava)
  75km – 16dB

Toshiba QKD

Why Quantum cryptography?

- Quantum supremacy?

  https://www.newscientist.com/article/2217835-google-has-reached-quantum-supremacy-heres-what-it-should-do-next/

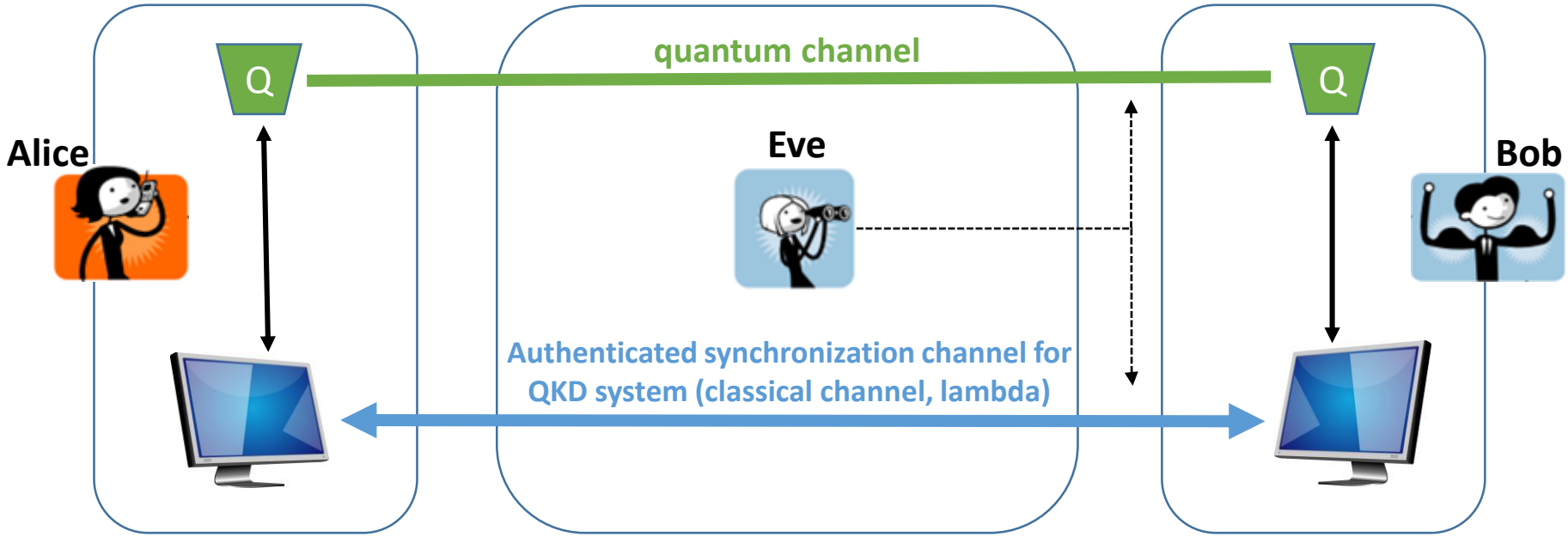


Eric Lukero/Google

- A Quantum computer is capable of cracking RSA cryptography very quickly
  - Post-quantum cryptography
  - Quantum cryptography (QKD)

Quantum Key Distribution

- According to physics theory, quantum cryptography is unbreakable
- Only the key is exchanged through the ‘quantum’ channel. A classical lambda between the 2 points is needed mainly to exchange synchronisation information (could be multiplexed)
- The data is then encrypted thanks to a classical computer and transmitted over a classical network (Internet)



With the courtesy of Eleni Diamanti, CNRS

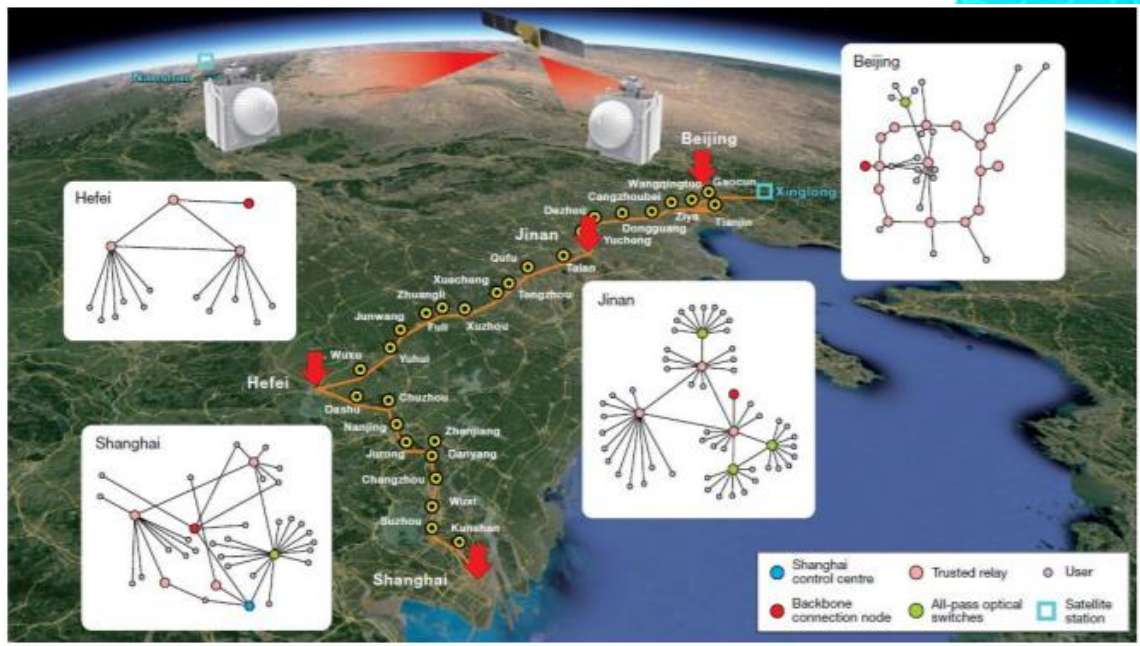
- Thanks to the fundamental principles of quantum physics (no cloning theorem, superposition, entanglement & nonlocality), **it is possible to detect eavesdropping on the communication link**

Quantum Key Distribution

- The first quantum channel solution was based on dedicated fibre (1 strand of the fibre pair) but now multiplexing solutions of the classical (data) and quantum channel is emerging
  - But the reach of the signal is limited to the weaker signal, i.e. the quantum signal
- The current generation of devices that use fibres is limited to a single hop less than 24dB (approximatively 100km, or 300km with twin field technology)

- This limitation can be overcome thanks to a trusted node architecture that allows extending the span of QKD transmission. This architecture relies on the physical security of such trusted nodes, which must be assured in order to in turn assure the security of the quantum exchange.
- Another option is to use space-based QKD – ongoing projects by ESA

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



QKD, GN4-3 - WP6 approach

- **WP6 QKD sub-task**
  - Lead by Piotr Rydlichowski (PSNC)
  - NRENs involved: CESNET, DFN, GÉANT, GRNET, KIFU, PSNC, RENATER, RiċerkaNet,
  - Email list and contact: https://lists.geant.org/sympa/info/quantum-discuss

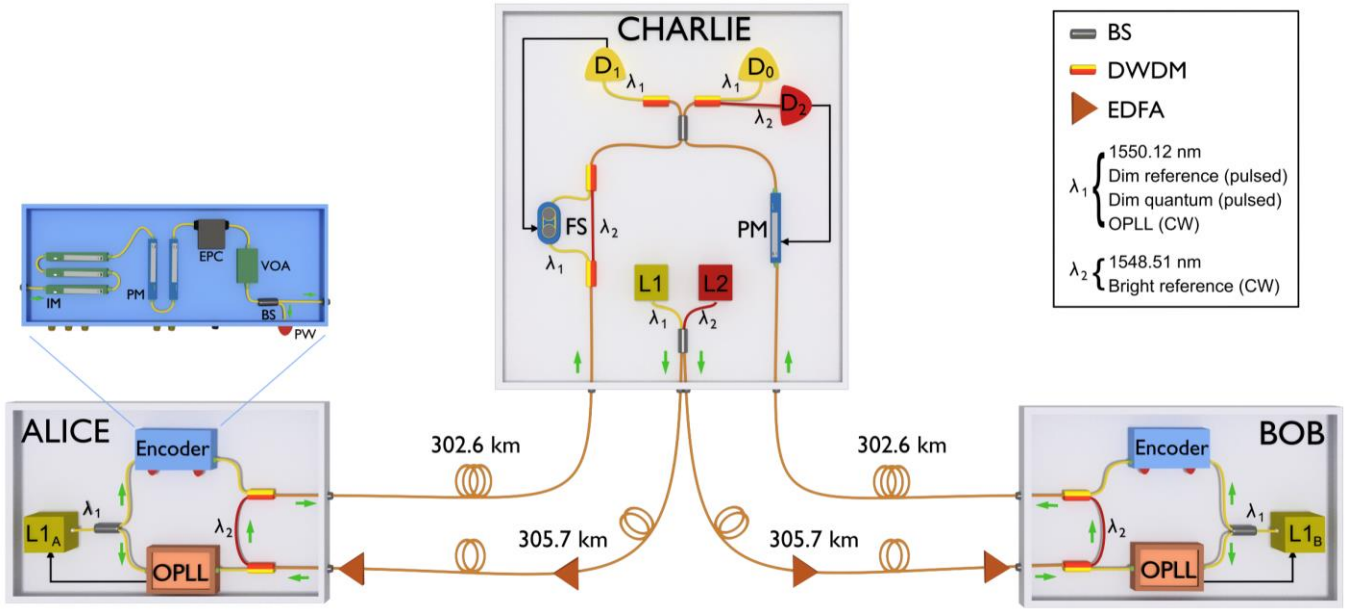
- **Objectives** :
  - Identify the R&E network community interest and needs
  - Involve GÉANT and NREN community in the QKD technology. Establish a cooperation between GÉANT community and commercial QKD vendors
  - Make the European NRENs ‘quantum aware’ and increase the ‘knowledge capital’
  - Establish a QKD testbed
  - Investigate QKD technology and quantum solutions and use cases for GÉANT

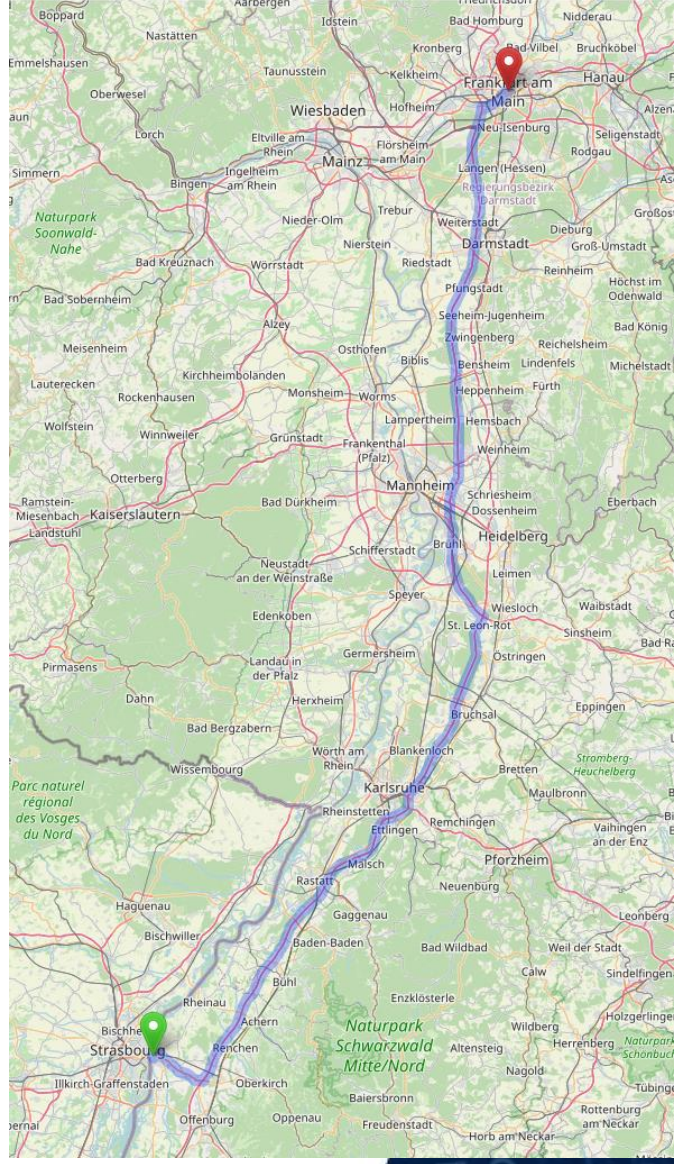
QKD, GN4-3 - WP6 work results

- A **survey** on the state of the art in NRENs has been carried out
- **Dissemination**
  - Four infoshares have been held with speakers from the EC and industry
  - White paper: ‘Quantum Technologies Status Overview’ has been distributed
  - Quantum meetings for all NRENs on the first Friday of each month
  - Materials are available on the wiki: https://wiki.geant.org/display/NETDEV/QKD
- **Technology testing**
  - Quantum simulators (QKDNETSIM for NS-3 and QUISP) installed
  - Physical testbed established
  - PoC between GÉANT PoPs with Toshiba/OpenQKD

Long-haul QKD proof-of-concept

- Between 2 GÉANT PoPs (254 Km)
- A collaboration between GN4-3 (WP6, WP7), OpenQKD and Toshiba – coordinator GÉANT
- Based on a Twin Field Solution





With the courtesy of Guy Roberts, GÉANT association

QKD, GN4-3 - WP6 future work

- **Continue dissemination**
  - Quantum meetings for all NRENs on the first Friday of each month
  - Training?

- **Technology testing**
  - Test on quantum simulators (QKDNETSIM for NS-3 and QUISP)
  - Test on the physical testbed
  - PoC demonstration between GÉANT PoPs with Toshiba/OpenQKD

- **Exploring QT solutions and use cases for GÉANT**

Summary

- Quantum is a strategic topic and the EC strongly supports a future European ‘Quantum Internet’
- GÉANT and NREN communities have the infrastructure, services and use cases to fully support quantum communication development
- GN4-3 WP6 T1 already set a close cooperation with QKD vendors and QKD testbeds as well as dissemination work toward NRENs
- The GÉANT project can play an important role in coordinating and facilitating the introduction of quantum technology to the R&E networks
    - But there is considerable work to be done in the long term to scope, fully engage, and deliver

GÉANT
Networks • Services • People

Thank you

Any questions?

quantum-discuss@lists.geant.org

www.geant.org

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).