

Quantum Cryptography Today

The **SWISS**QUANTUM testbed network

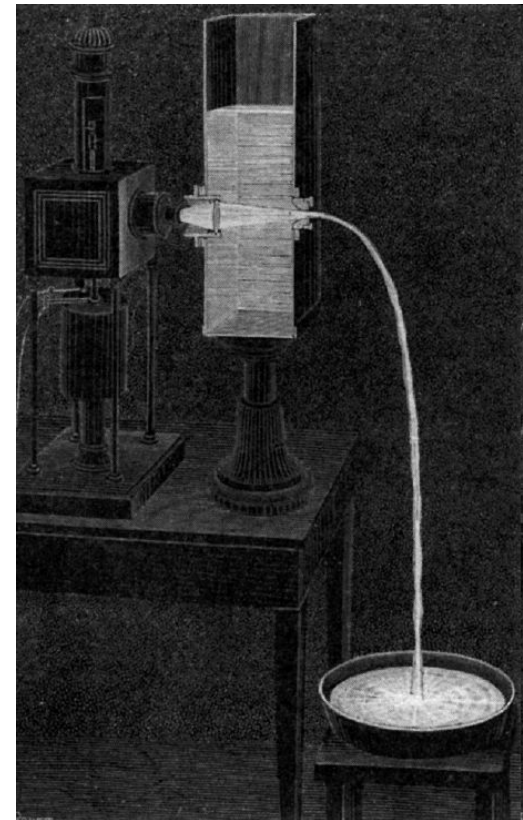
Grégoire Ribordy
ITU Telecom World 2009
October 8th, 2009



Charles Kao,
Physics Nobel Prize Laureate 2009

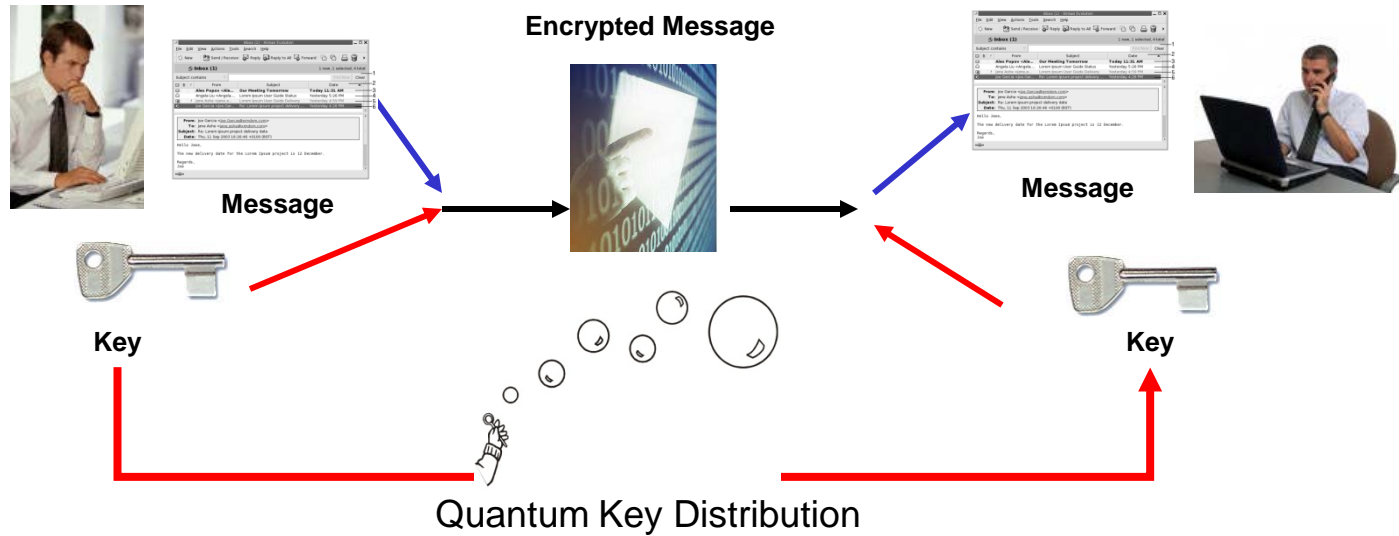


Jean-Daniel Colladon



Colladon's « Fontaine Lumineuse », 1841

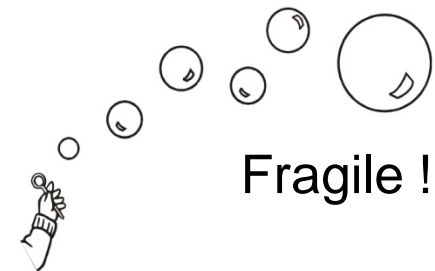
Quantum Cryptography



Classical communications



Quantum communications



An encryption system can only be secure if

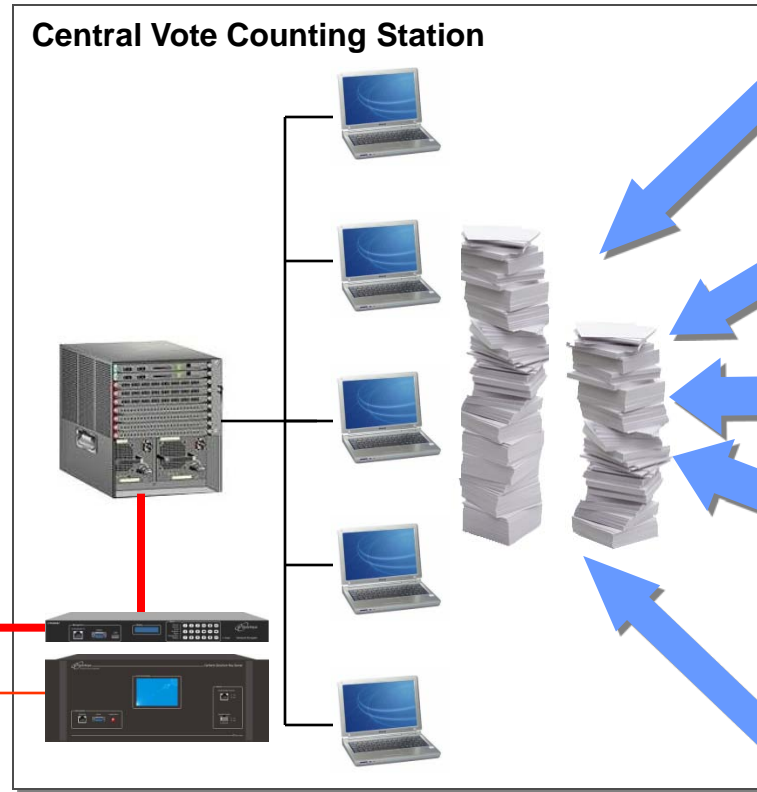
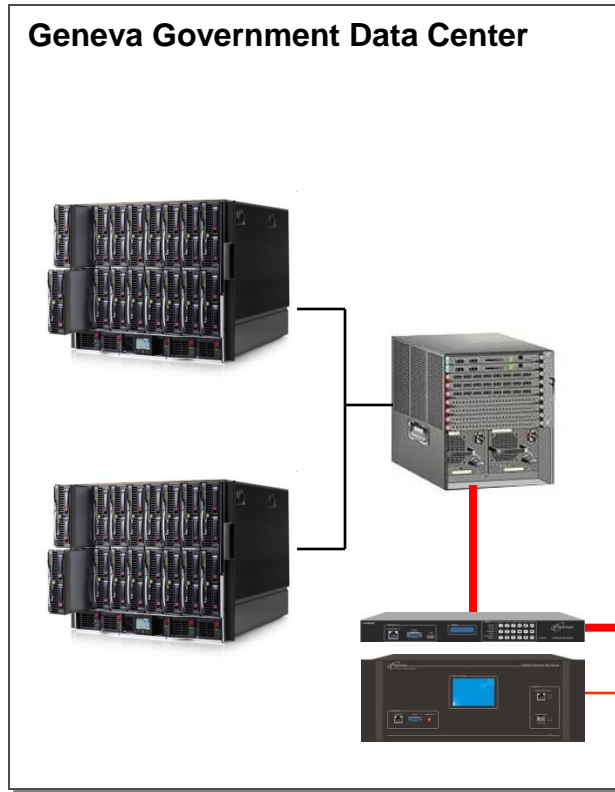
➤ It rests on sound principles

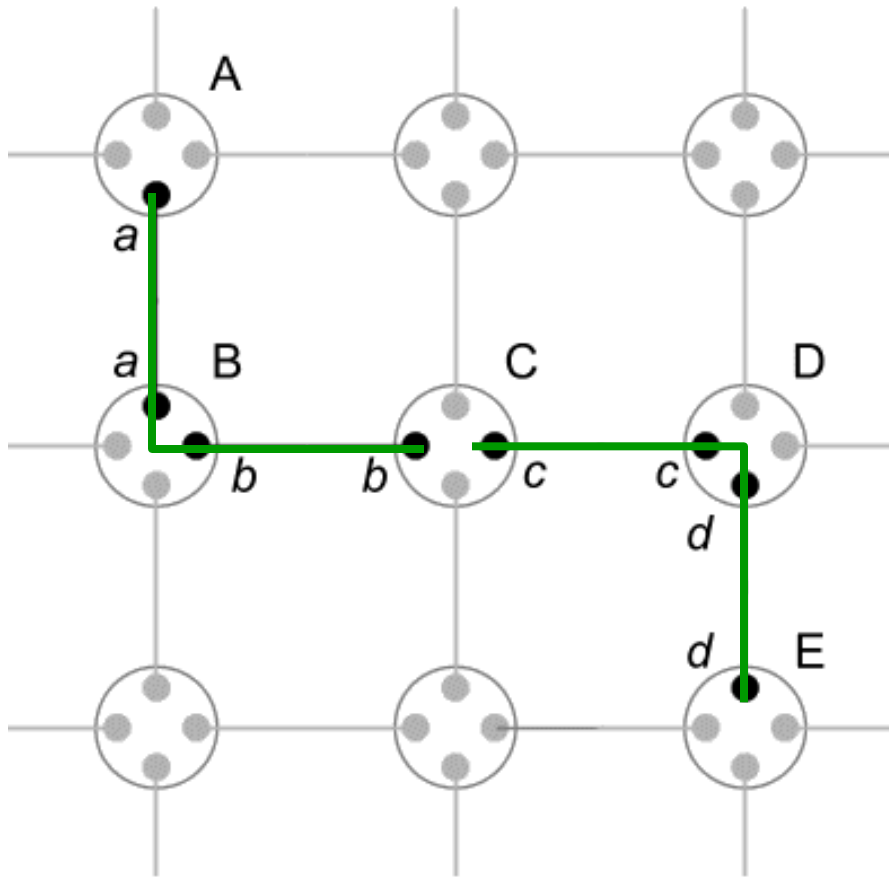
= « **Security of Principle** »

➤ It is implemented properly

= « **Security of Implementation** »

Quantum Key Distribution at Work





- Costs
- Reconfigurability
- Redundancy
- Throughput increase by aggregation
- Range extension

Quantum Key Distribution Testbed Network with the following goals

1. Long-term operation and testing of the network
2. Used with high bandwidth real traffic
3. Development of testing and management tools

Project Coordination



Network Design and Deployment



Testing Tools



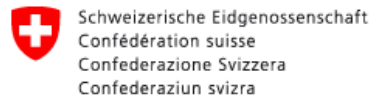
Crypto Services



Infrastructure



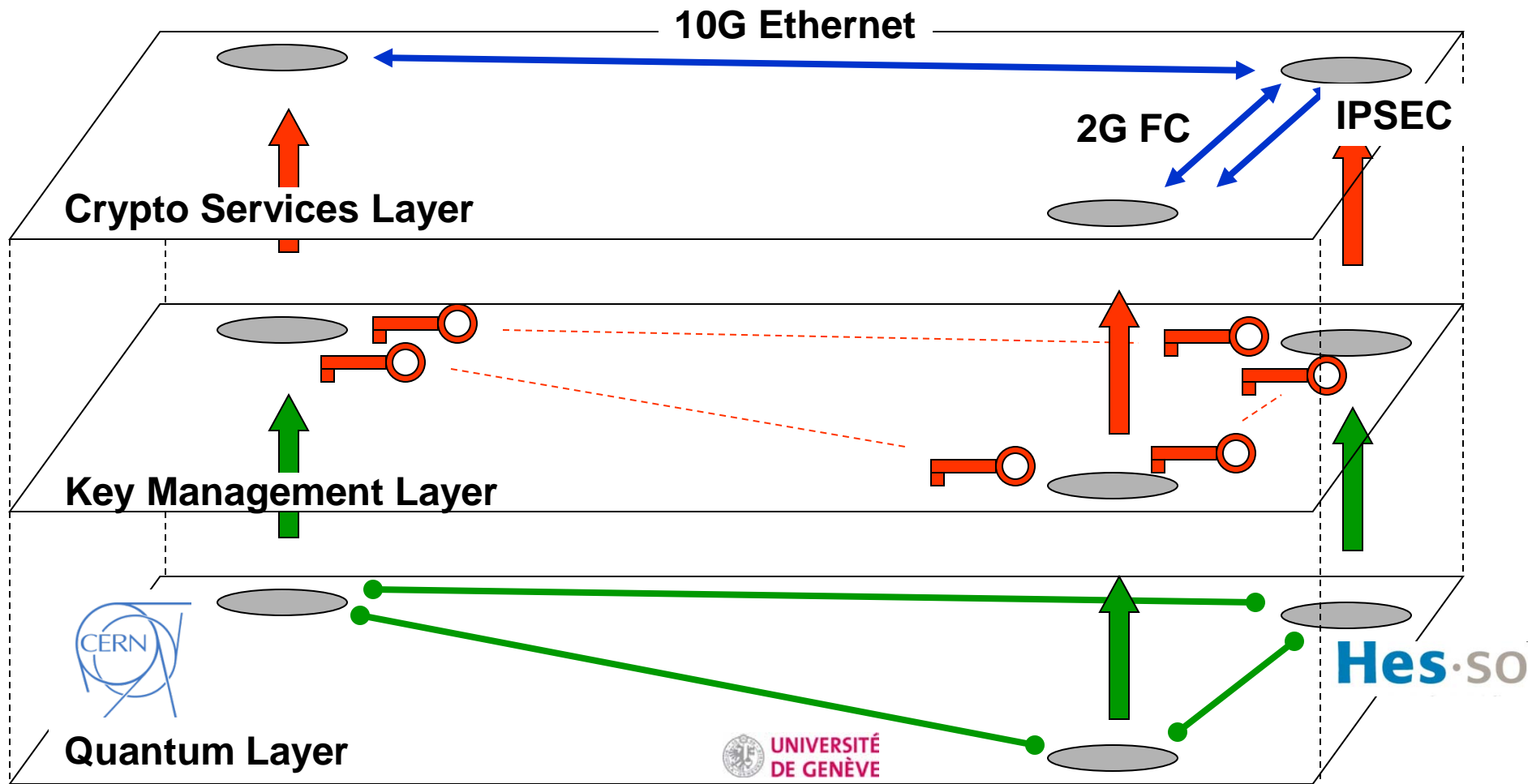
Funding



Test User









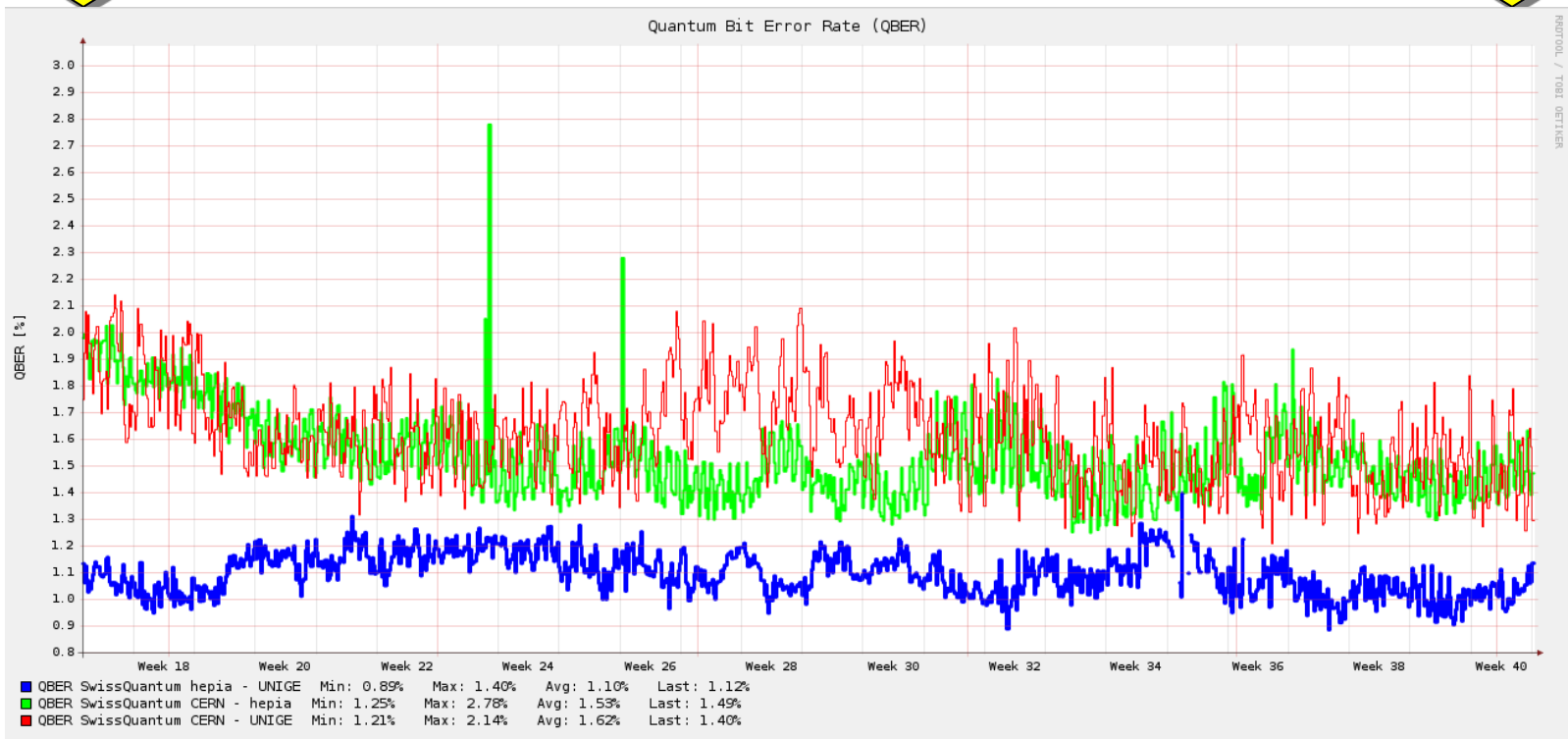
Quantum Key Server
(6 servers, 3 links)

- Provably secure key distribution
- Key rate: 1000 bps over 25km/6dB
- Standard range: 50km (100km upon request)
- Robust and reliable technology
- « Network ready » - no physicist needed
- Patent protected

April 20th

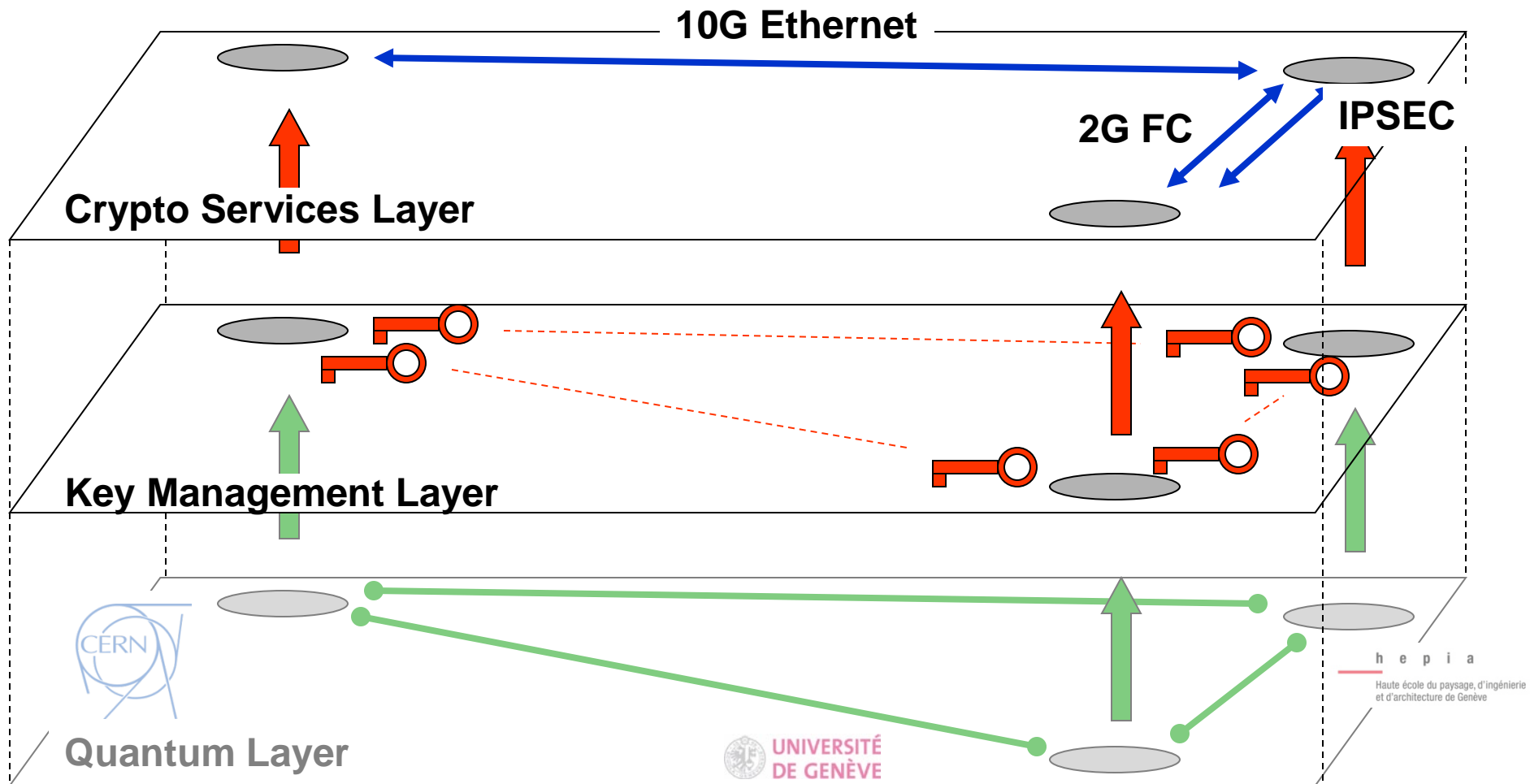


October 8th

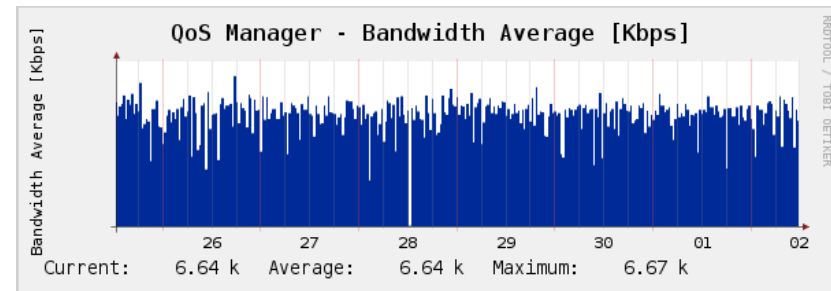
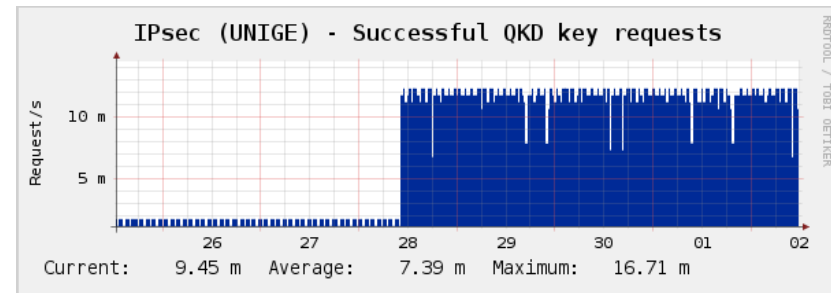
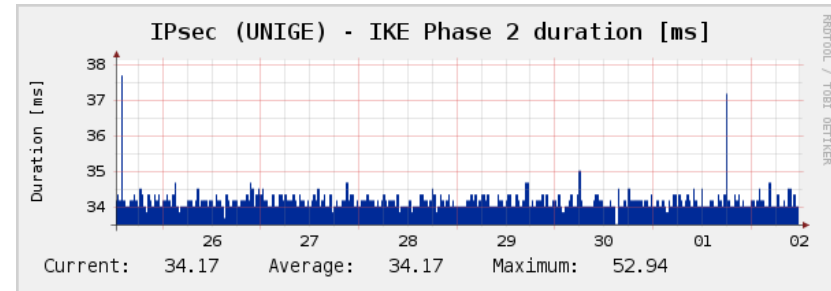


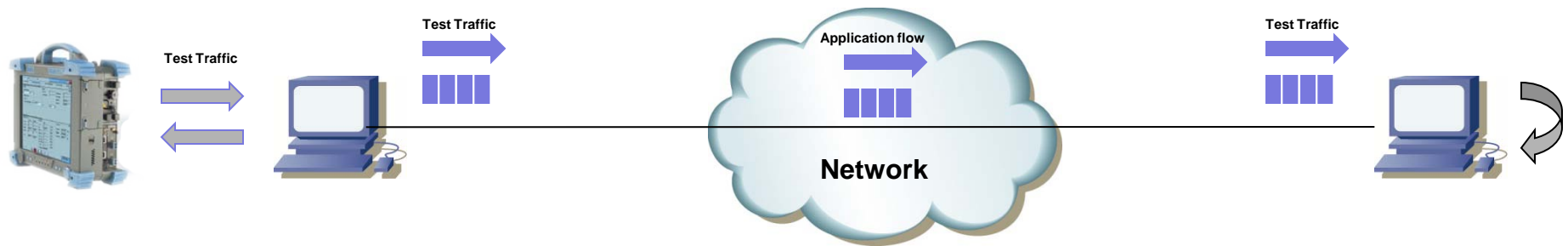
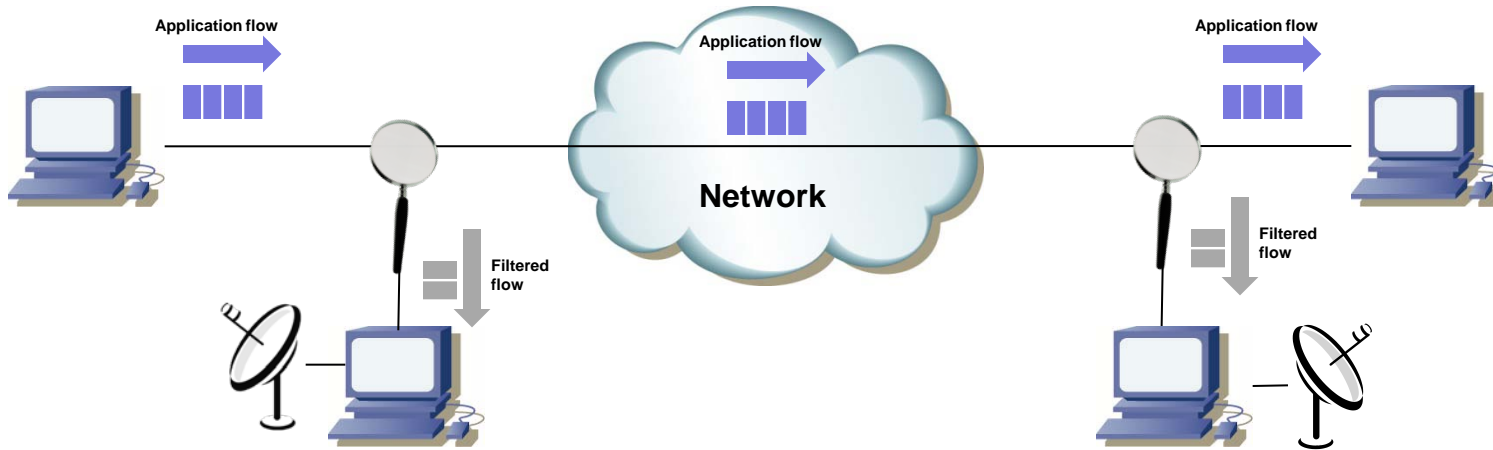
www.swissquantum.com

Cumulative operation time of 12'000 hours



- Secure integration of the Quantum Key Distribution protocol within an IPsec stack
- Throughput of up to 400 Mbps on commodity PCs running under Linux





Crypto Services - Layer 2 Encryption

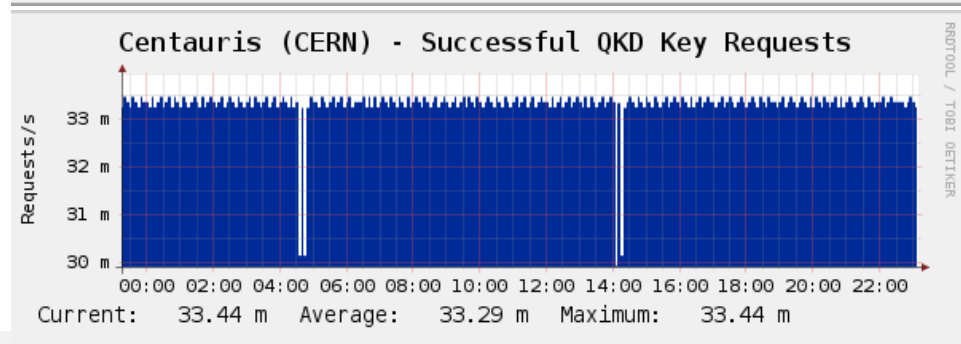
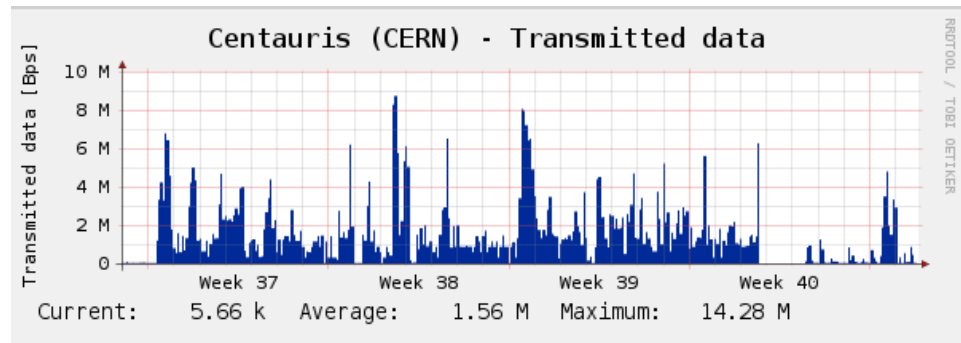


Encryption

- AES-256

Performance

- Transparent for the network
 - 100% of bandwidth available for data transmission (no encryption tax)
 - Low latency $\approx 10\mu\text{s}$





POST TENEBRAS LUX

Follow the progress of the SwissQuantum testbed on www.swissquantum.com