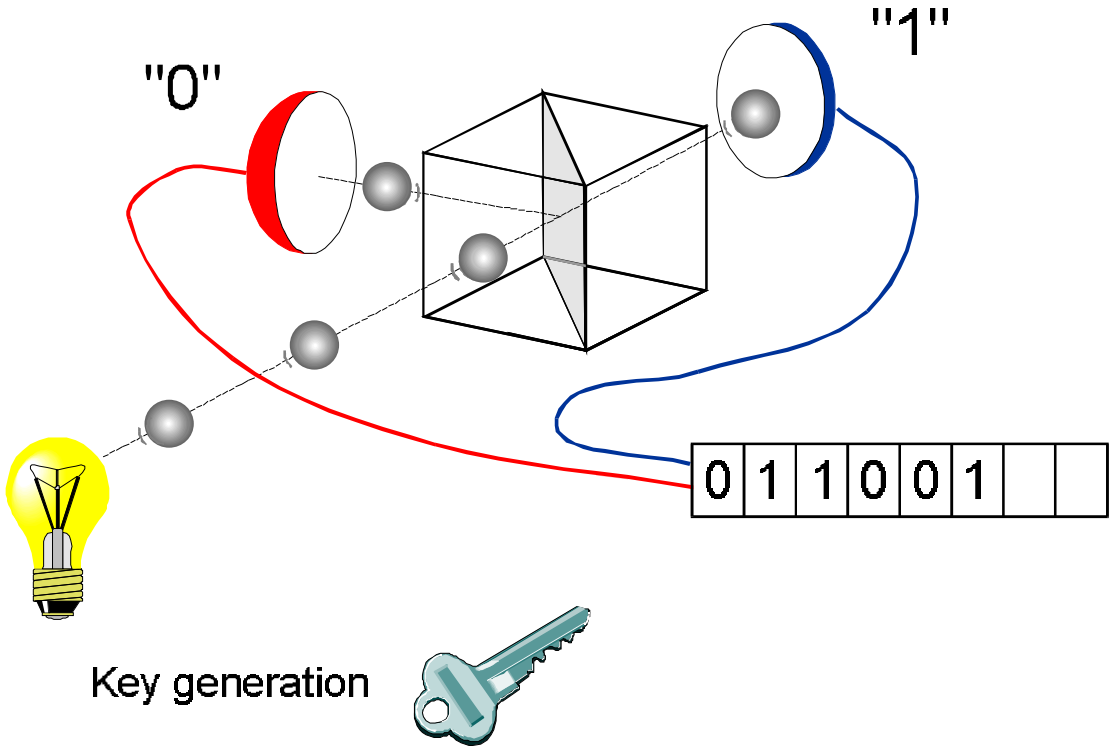
How can Quantum Cryptography contribute to cyber security

Nicolas Gisin, Hugo Zbinden
Mikael Afzelius and Rob Thew
GAP-Optique, University of Geneva

- **The Quantum Technology era has started !**
- **Quantum Random Number generators**
- **Quantum Computers and the need to move to Quantum safe cryptography**
- **Quantum Key Distribution exists today**
- **What needs to be done**

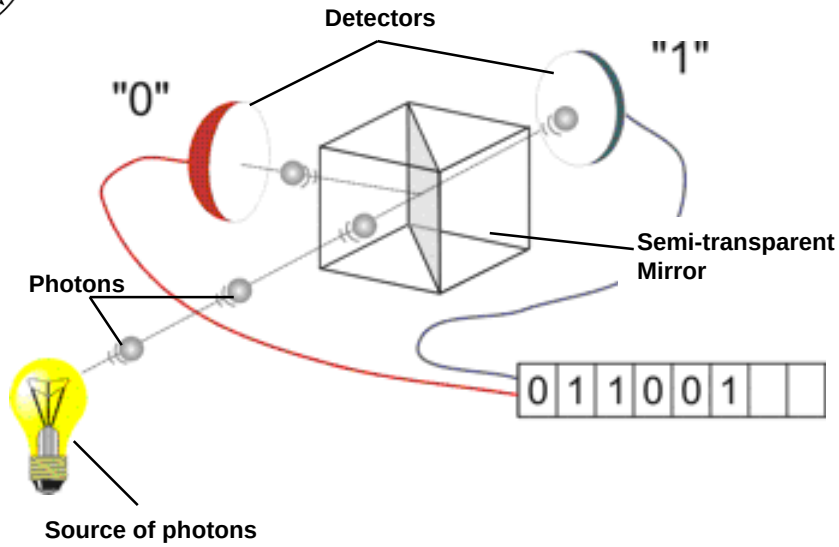
GAP Quantique

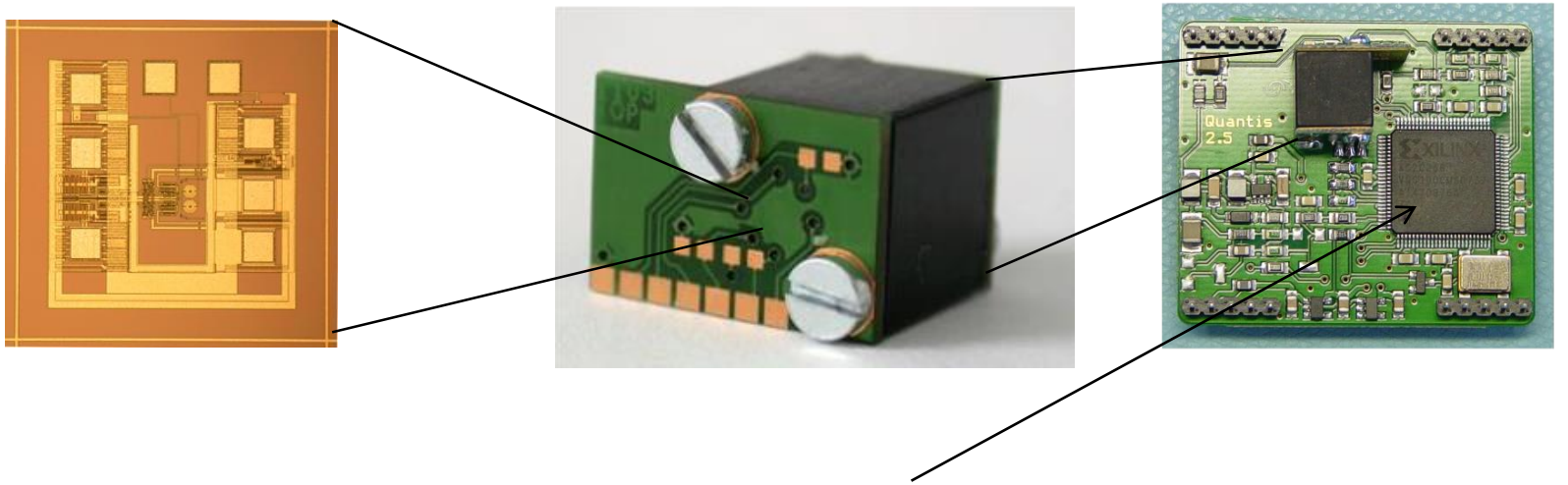
Physics of a beam-splitter



- A conceptually simple entropy source
- Only quantum physics offers fundamental randomness
- Easy to pindown the origine of the randomness
- A practical random number generator

Quantum Random Number Generator





4 Mb per second of balanced random bits

GAP Quantique

Evaluation and Certification

Non-Deterministic (Physical) RNG

Bundesamt für Sicherheit in der Informationstechnik

- PTG.1

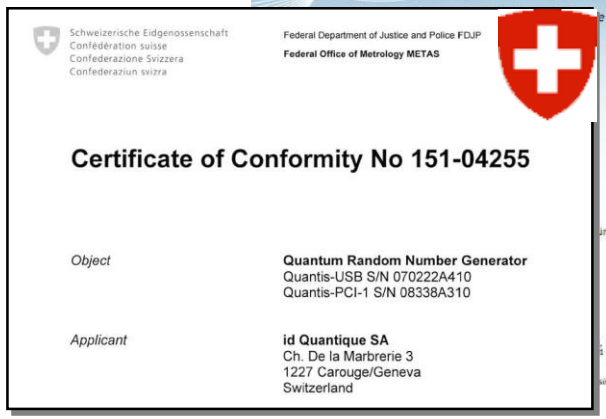
Physical RNG with internal tests that detect a total failure of the entropy source and non-tolerable statistical defects of the internal random numbers

- PTG.2

PTG.1, additionally a stochastic model of the entropy source and statistical tests of the raw random numbers

- PTG.3

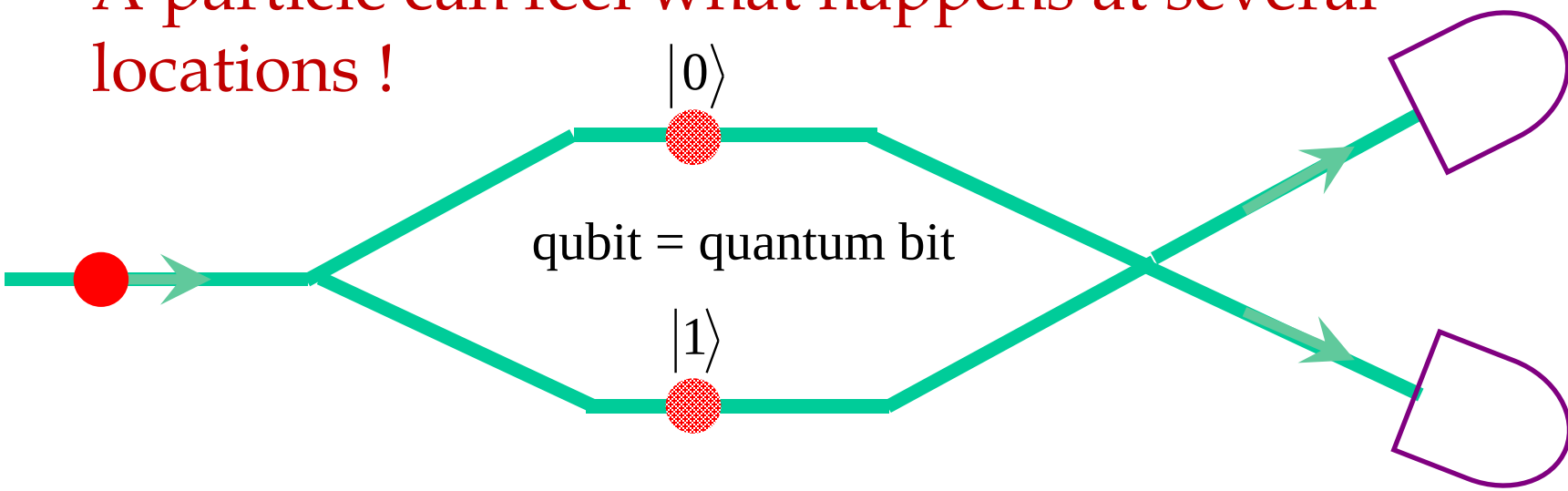
PTG.2, additionally with cryptographic post-processing (hybrid PTRNG)



GAP Quantique

Quantum mechanics (all physics you need to know)

- A particle can feel what happens at several locations !



- Likewise one can have $|0\rangle+|1\rangle+|2\rangle+|3\rangle+\ldots+|n\rangle$
- 100 qubits can number all the particle there are in the entire universe !
- Upon a measurement one single result shows up

GAP Quantique

Quantum Computing

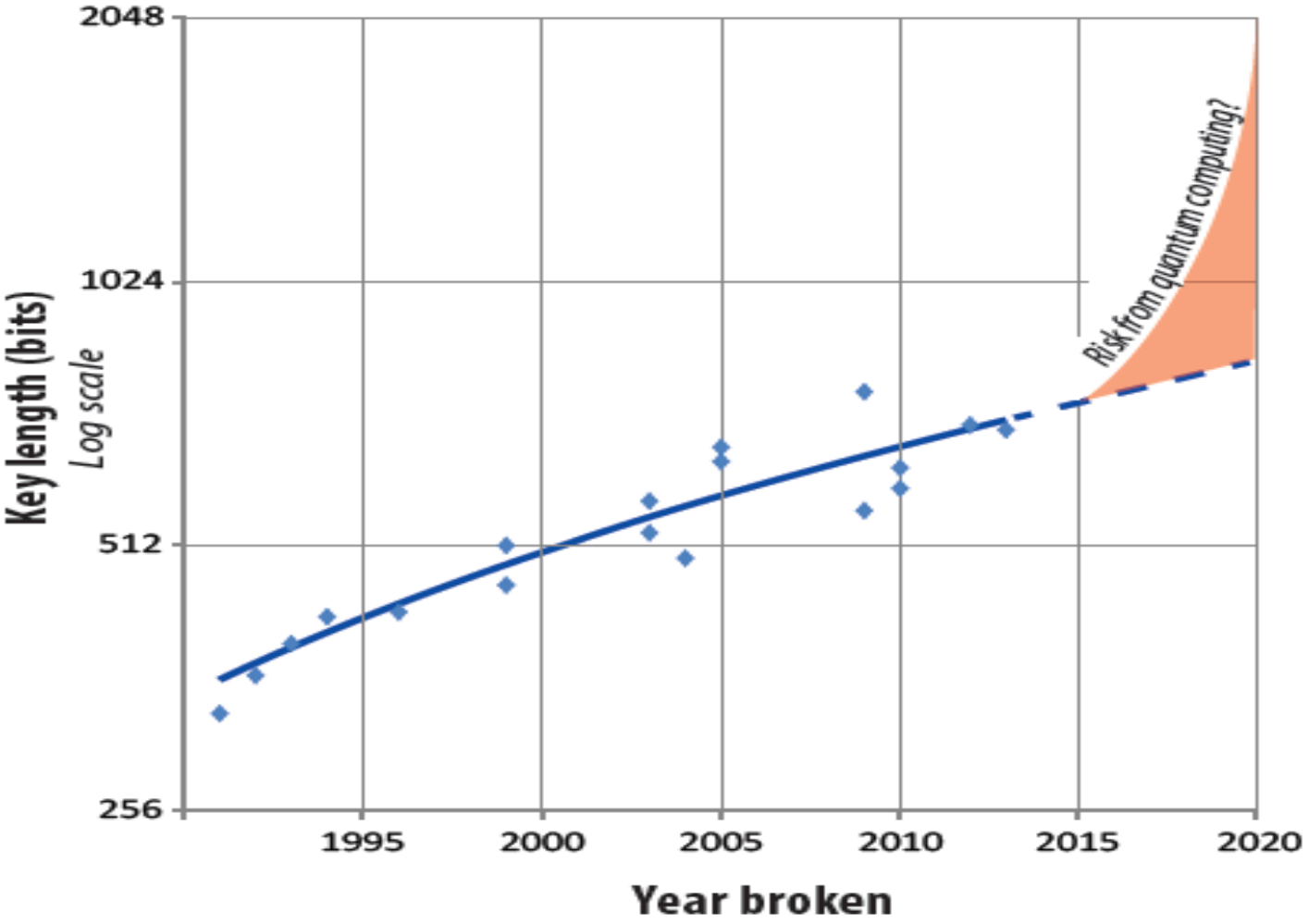
- Process information: input x $\Rightarrow$ output fct(x)
- Quantum computer:
  quantum processing of classical information
  input $|0\rangle+|1\rangle+|2\rangle+\ldots+|n\rangle \Rightarrow |fct(0)\rangle+|fct(1)\rangle+|fct(2)\rangle+\ldots+|fct(n)\rangle$
- A measurement can provide only one result
- This single result can provide information about a global property of the function fct.
- For example, the maximum value, the mean value, or information about the periodicity of the function.

Fact

- Period of a function + a bit of number theory
- $\Rightarrow$ break all of today's public key cryptographic
- i.e. allows one to decipher all encrypted messages

- Hence, a quantum computer will render today's public key cryptography obsolete

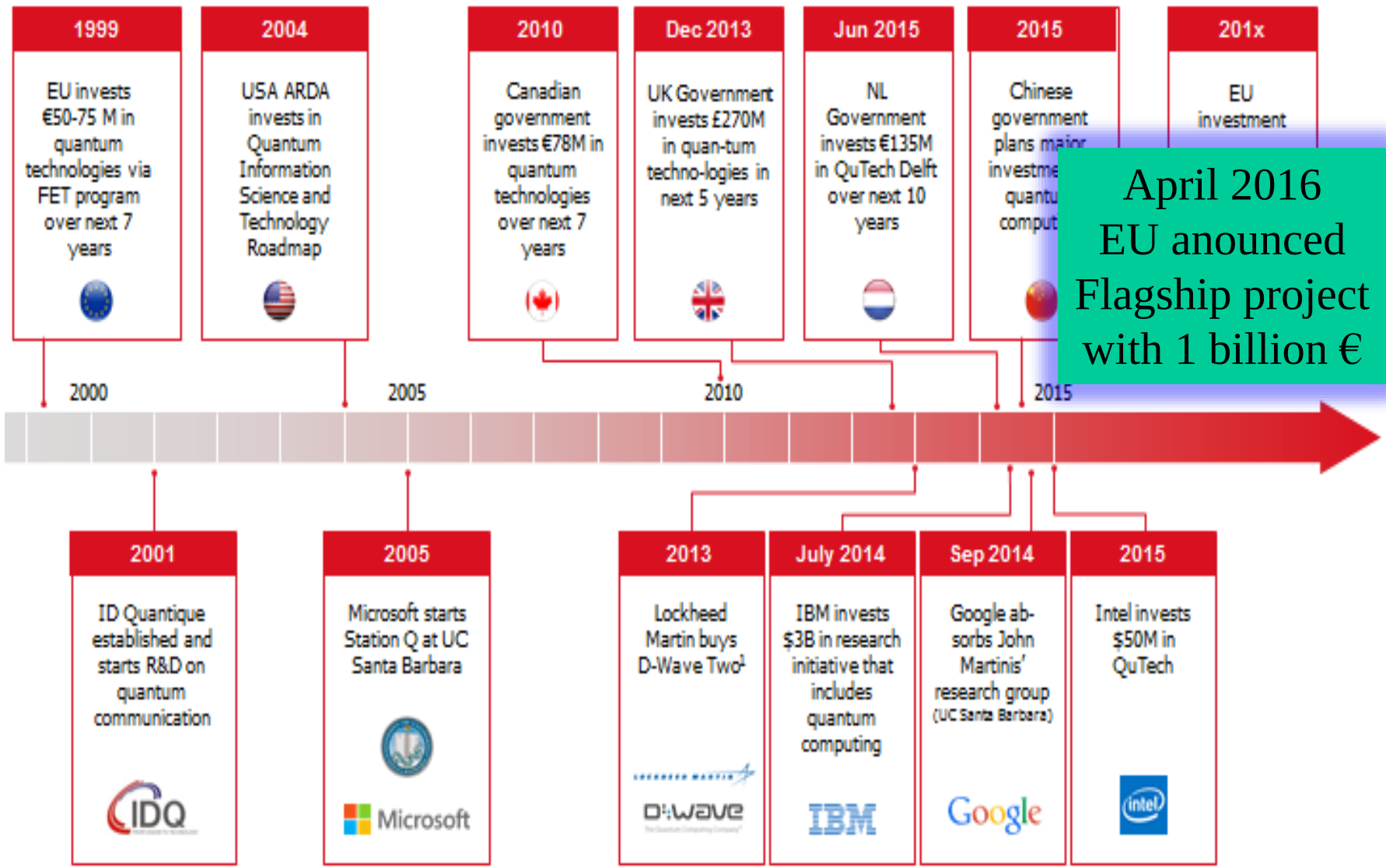
Quantum Computers effect on RSA



https://downloads.cloudsecurityalliance.org/initiatives/qss/What_is_Quantum_Safe_Security_position_paper.pdf

GAP Quantique

When shall we have Quantum Computers ?



April 2016
EU anounced
Flagship project
with 1 billion €

GAP Quantique

Change in Technology

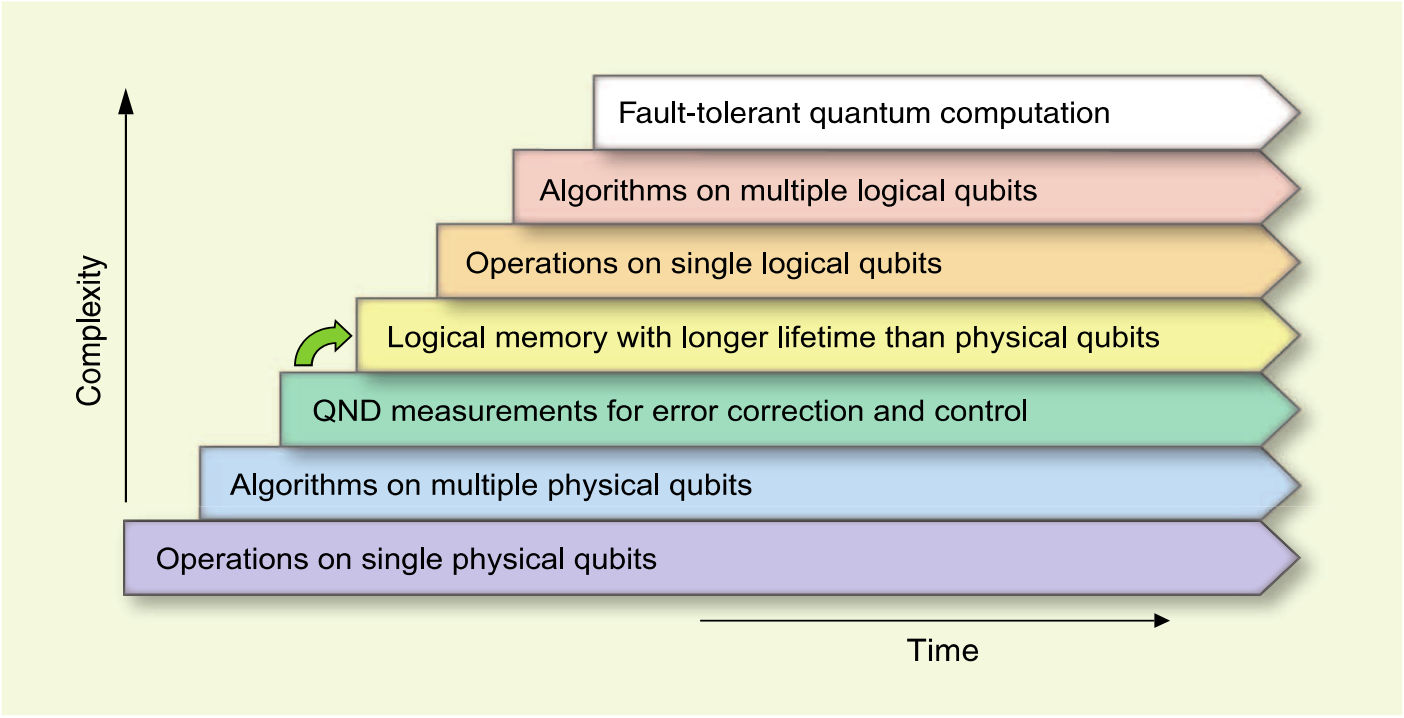


Fig. 1. Seven stages in the development of quantum information processing. Each advancement requires mastery of the preceding stages, but each also represents a continuing task that must be perfected in parallel with the others. Superconducting qubits are the only solid-state implementation at the third stage, and they now aim at reaching the fourth stage (green arrow). In the domain of atomic physics and quantum optics, the third stage had been previously attained by trapped ions and by Rydberg atoms. No implementation has yet reached the fourth stage, where a logical qubit can be stored, via error correction, for a time substantially longer than the decoherence time of its physical qubit components.

Change in perception

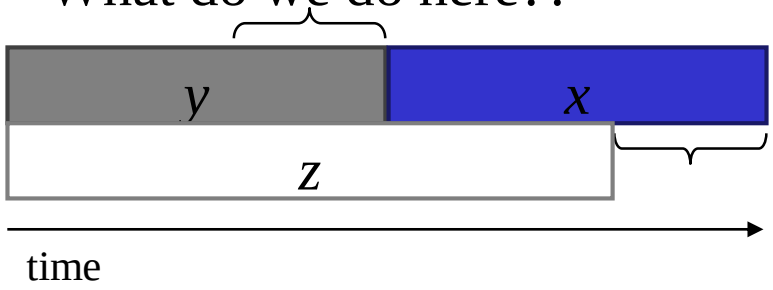
How soon do we need to worry?

Depends on:

- How long do you need encryption to be secure? (*x* years)
- How much time will it take to re-tool the existing infrastructure with large-scale quantum-safe solution? (*y* years)
- How long will it take for a large-scale quantum computer to be built (or for any other relevant advance? (*z* years)

Theorem 1: If $x + y > z$, then worry.

What do we do here??



GAP Quantique

Quantum Safe Crypto

- Post-Quantum Crypto
  = Complexity-based classical algorithms resistant to known Q attacks

+ not much change for the security experts.

- again a wild bet on the unknown.

- vulnerable backwards.

- QKD
  = Physics-based, proven resistant do Q attacks

+ provable security.

+ backward security.

- expensive.

- big change of infrastructure and mentality.

- Likely that each will find some applications, the real question is about the size of each market.
- Each needs true random bits.

GAP Quantique

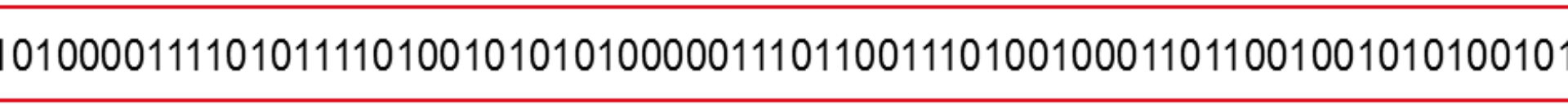
Example of Quantum Safe crypto.

OSI Model

Application	⟷	Application
Presentation	⟷	Presentation
Session	⟷	Session
Transport	⟷	Transport
Network	⟷	Network
DataLink	⟷	DataLink
Physical	⟷	Physical

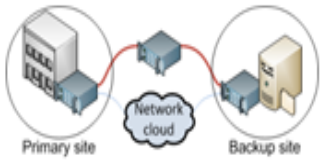
Use Quantum Resistant algorithms here

Use QKD here

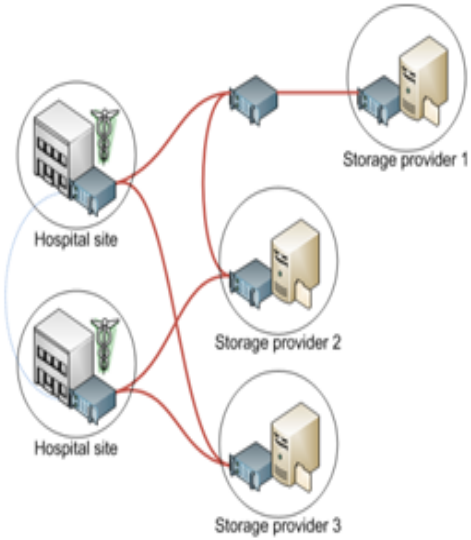


Examples of user cases

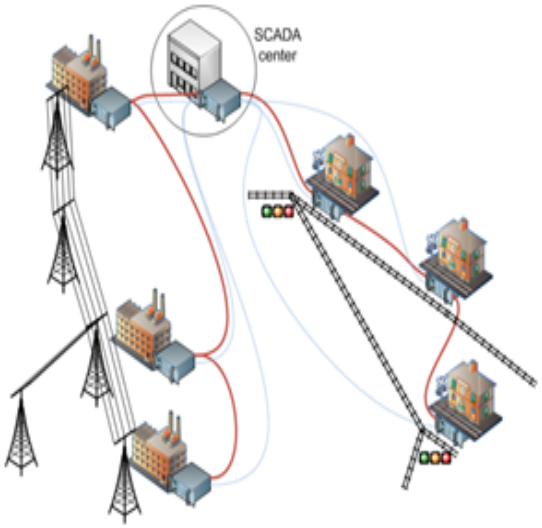
Off-site backup



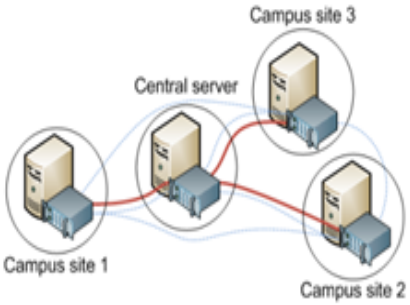
High security cloud storage



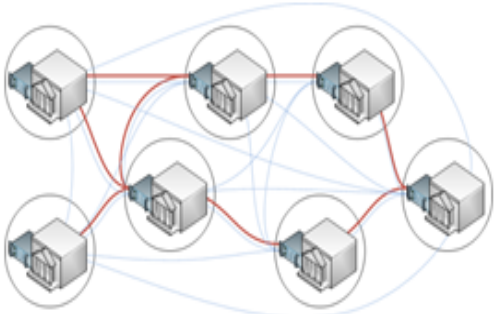
Critical infrastructure protection



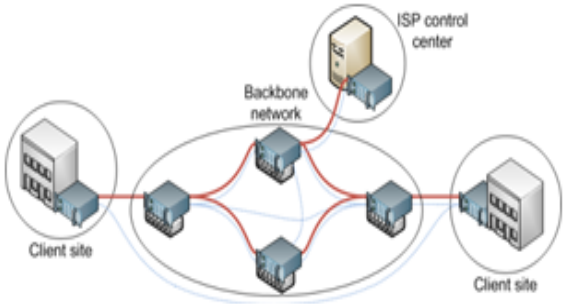
Key and signature server



High security private networks

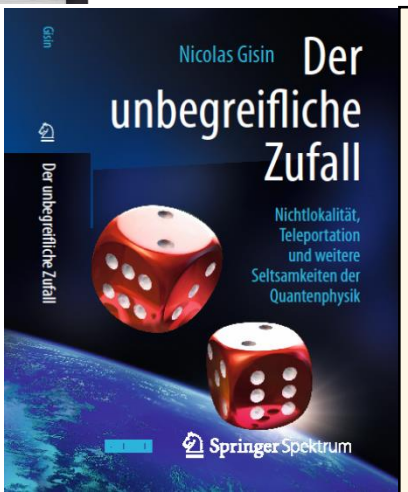


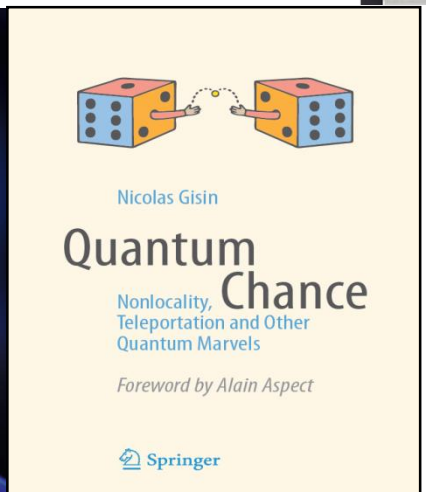
Backbone link protection



Nature Offers True Local & Nonlocal Private Randomness

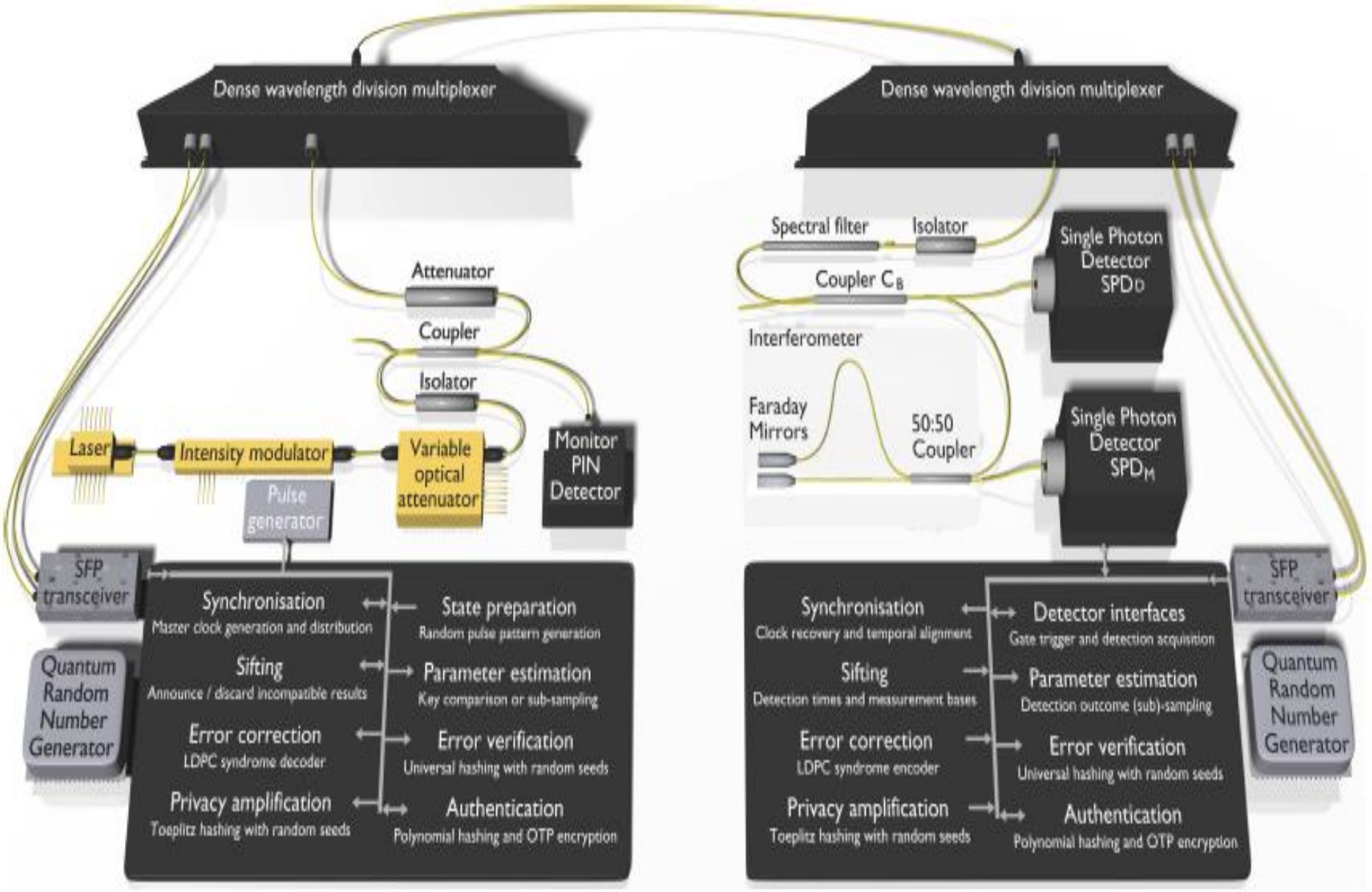
- Assume that distances really exist.
- Assume that Alice & Bob can make sure that no info leaks to the outside world
- Assume that $a \oplus b = x \cdot y$ holds with a large probability (note that this can be checked)





GAP Quantique

QKD engine @ 625 MHz



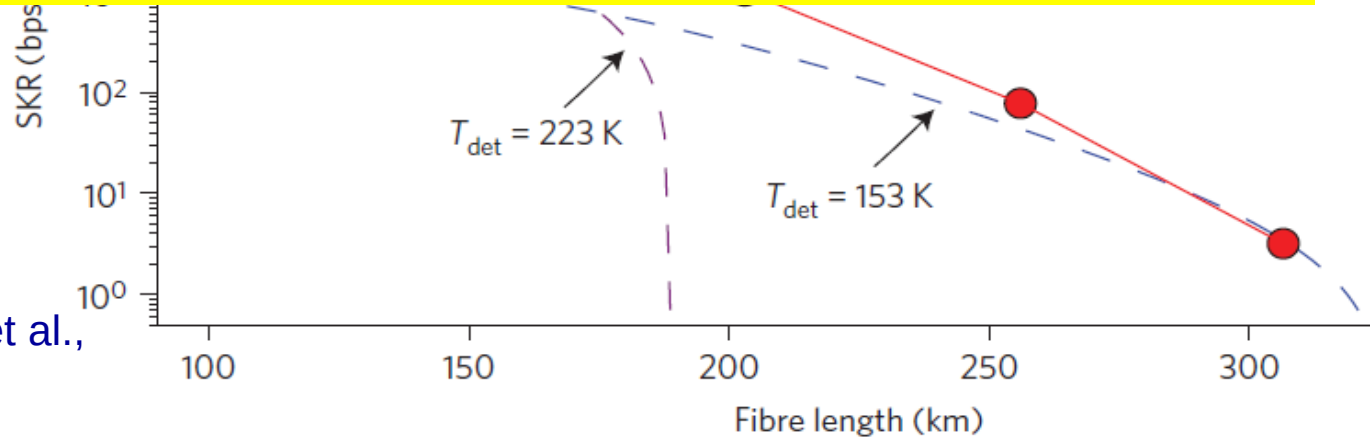
Integrated QKD Engine

- Built on the Advanced Telecommunication Computing Architecture (ATCA).
- Provides standardized mechanical, power, and data interfaces.
- Provides network services, cooling, power supplies.
- Scalable architecture, familiar to potential clients.

GAP Quantique

QKD over 307 km with real time secret key distillation and finite key analysis

- Integration into ATCA blades
- A vision of a QKD engine producing 1 Gb/s of provably secret bits is on the horizon.



B. Korzh, C. W. Lim et al.,
Nature Photonics
9, 163-168 (2015)

GAP Quantique

Example of a commercial link running continuously since 2011

Lausanne

Nyon

67 km

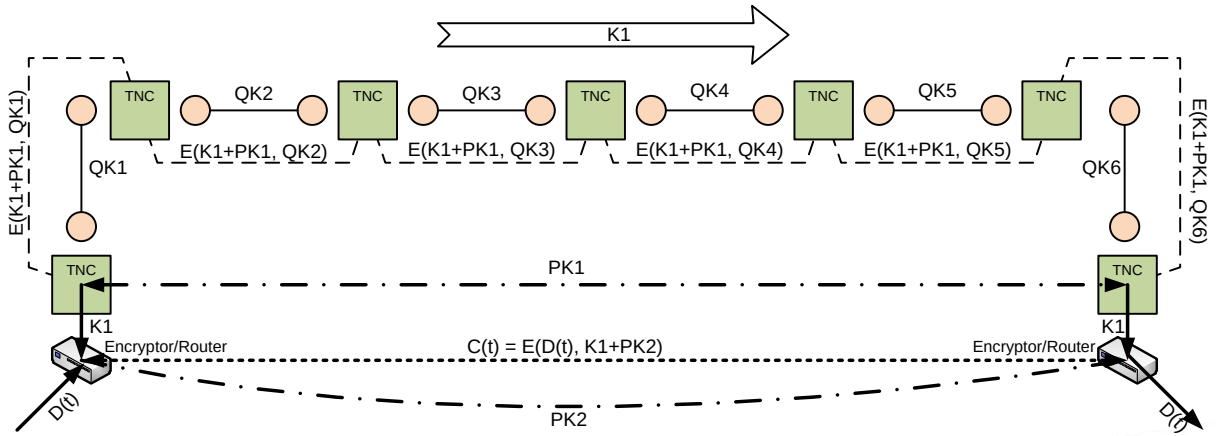
Genève

IDQ
FROM VISION TO TECHNOLOGY

Installed multiplexed quantum channel for commercial users.

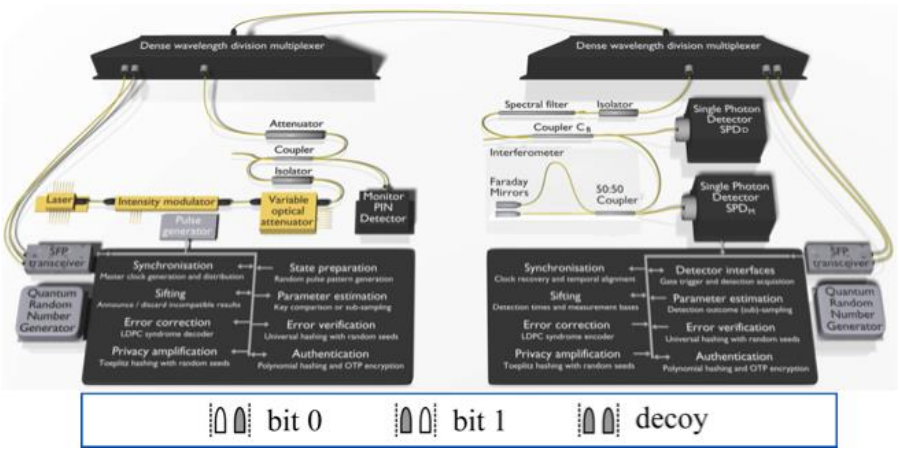
GAP Quantique

QKD Trusted Node



Keys move securely across the network in a piece-wise fashion

Coherent One-Way (COW) Protocol



Telecom-compatible architecture (ATCA)
Up to 8 quantum blades per chassis

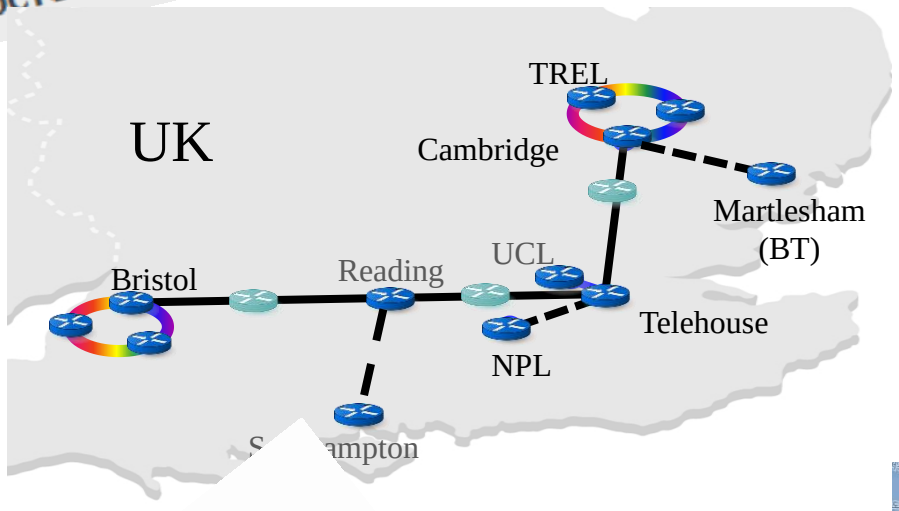
FIPS 140-2 Certification (Planned)
CC Evaluation (Planned)

GAP Quantique

3rd ETSI/IQC Workshop on Quantum-Safe Cryptography

ADD THIS TO MY CALENDAR

5-7 OCTOBER 2015



Battelle
The Business of Innovation

What does QKD achieve

1. Attacks have to be launched on the spot
   ⇒ immune to future progress
2. With only the assumption of proper implementation
   ⇒ key expansion
3. Assuming short term secure 1-way function
   ⇒ Cryptographic Key Distribution with long term security

I. QKD with one-time-pad (limited to the bit rate of QKD)
   ⇒ allows for information theoretical long term security.

II. QKD allows to change the seed key of AES very frequently
   ⇒ limited data available for cryptoanalysis and limited motivation for an adversary.

GAP Quantique

What needs to be done

- Today, physicists and cryptographers don't collaborate.

➔Forge a community of physicists and cryptographers that work together on Quantum Safe Cryptography.

➔Find out where Post-Quantum Algorithms are suitable, e.g. mobile phones, grand-public applications, most of e-commerce, etc.

➔Find out where Quantum cryptography (both QRNG & QKD) are suitable, e.g. a **Swiss Quantum Backbone** for critical infrastructures and backups of large aggregated data.

GAP Quantique

What needs to be done

- Today, physicists and cryptographers don't collaborate.

➔Forge a community of physicists and cryptographers that work together on Quantum Safe Cryptography.

➔Find out where Post-Quantum Algorithms are suitable, e.g. mobile phones, grand-public applications, most of e-c

➔Find out where QKD is suitable, e.g. a **Swiss Quantum Backbone** for critical infrastructures ar aggregated data

GAP Quantique