Quantum Computer and Cryptography

Torino, 30 november 2019
M0LECON 2019

Guglielmo Morgari
Telsy - Research Manager

Telsy

Telsy: profilo dell'azienda

Founded in 1971

Today 100% part of the TIM group

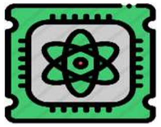
Under Golden Power

Focused on cybersecurity and cryptography

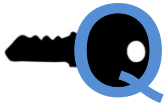
Both governmental and business markets

Strong research activity

Quantum Areas



- **Quantum Computing**



- **Quantum Cryptography**

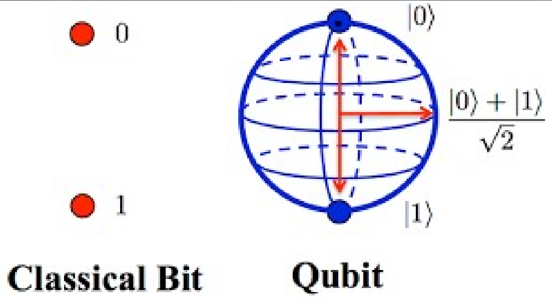
- **[Post Quantum Cryptography]**

- Quantum Communication

- Quantum Randomness

- Quantum Sensing
- …

Quantum Computer



- Theorized in 80s (Feynman, Deutsch)
- Long considered unrealizable
- No more bits (0/1) but instead **qubits**
  (superposition of states, according to the quantum model)
- If (when) realized, a quantum computer will be (much) more effective than a classical computer to solve **some** families of problems
- Impact on cryptography?

Quantum Computer

- Huge governmental investments US / China

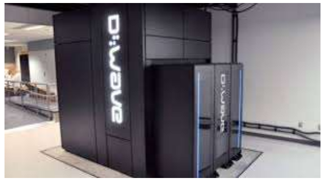
- Recently quick improvements and first prototypes

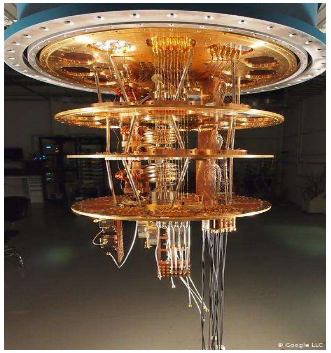
- IBM, D-Wave, Google, Microsoft
- Governments?

- Ready for the market: 2030? 2040? Never?

IBM Quantum Experience

  - Simulate quantum behavior using classical hardware (both locally and on the cloud)
  - Compare to real quantum devices in a remote environment





Quantum Computer

Two fuzzy definitions:

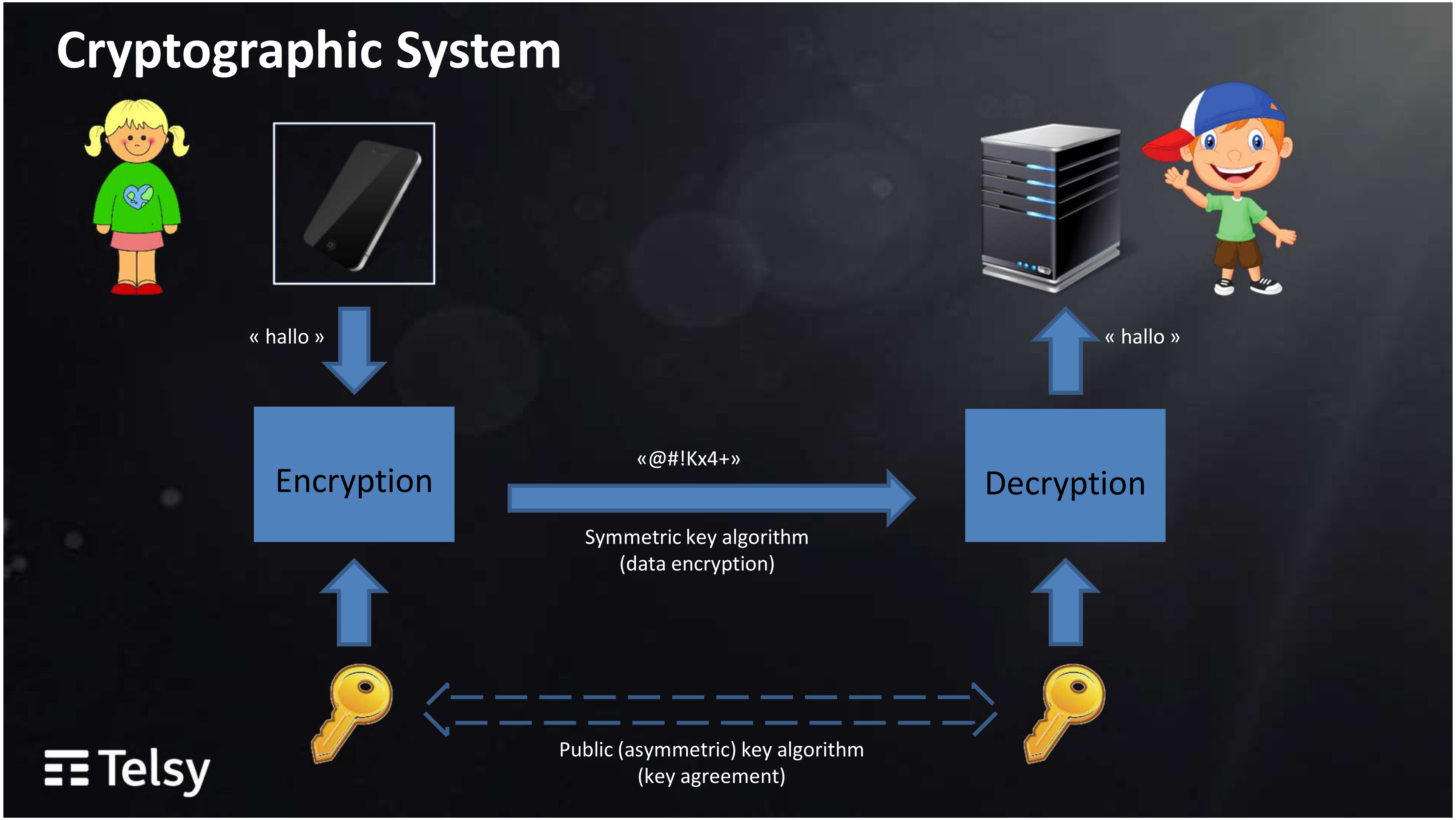
- **Quantum advantage**: when a quantum computer can solve (at least one) problem significantly **faster** than a classical computer
- **Quantum supremacy**: when a quantum computer can solve (at least one) problem that a classical computer **cannot** (practically) solve at all

September – Octobter 2019:

Dispute between Google and IBM about Google's quantum supremacy

- Google Sycamore Quantum chip took **200 secs** to solve a given specific problem
- According to Google estimations, the same task would take **10.000 years** on the currently most advanced classical computer (the IBM Summit)

- IBM claims that with an optimal configuration Summit could solve the same task in at most **2.5 days**


Cryptographic System
« hallo »
« hallo »
Encryption
«@#!Kx4+»
Decryption
Symmetric key algorithm
(data encryption)
Public (asymmetric) key algorithm
(key agreement)
Telsy

The Maths behind Public Key Cryptography

Integer Factorization Problem

- Easy: given *p*,*q* compute $n=pq$

- Hard: given *n*, find *p*,*q* such that $n=pq$

For human beings
- 521 * 547 = 284987 easy
- 282943 = ? * ? harder

For computers
- Multiplication of two numbers is always easy
- Factorization is (practically) impossible if size(n) ≥ 1024 bit

Discrete Logarithm Problem

- Easy: given a, compute $n=g^a \bmod p$

- Hard: given n, find a such that $n=g^a \bmod p$

For human beings
- 19^7 mod 191 = 143 easy
- $19^?$ mod 191 = 94 harder

For computers
- Modular exponentiation is always easy
- Discrete logarithm (practically) impossible if size(p) ≥ 1024 bit

Quantum Computer & Cryptography

Symmetric key algorithms (data encryption)

- Require a shared secret key
- DES, AES, …

- **Grover's quantum algorithm (1996)** halves the actual security level
- **Simple solution**: to double the key length
- Grover's algorithm solves the unsorted database search problem
- Despite the Grover's quadratic speed up, as of today the problem has still **exponential** complexity, even in the quantum scenario

Public key algorithms (key agreement)

- Based on mathematical problems currently believed to be intractable through classical computers
- RSA (integer factorization)
  Diffie Hellman (Discrete Logarithm Problem)

- **Schor's quantum algorithms (1994)** completely breaks currently most used solutions (RSA, Diffie Hellman)
- **No simple solutions**
- Shor's algorithm moves Integer Factorization and Discrete Logarithm problems into the BQP (Bounded-error Quantum **Polynomial-time**) class

Telsy

Quantum Computer & Cryptography

Agosto 2015, NSA web site

Our ultimate goal is to provide cost effective security against a potential quantum computer.

[...]

We recommend [...] **to prepare for the upcoming quantum resistant algorithm transition**.

Is it a Real Problem?

- We don't know if the quantum computer will really come …
  … but we cannot afford the risk!

- The development of new technologies takes a long time
- Their standardization takes also long time
- Their deployment takes additional long time as well
- A message life can be very long

- Therefore… **yes, it is a problem**… to face as soon as possible!

- We need to define **alternatives to current public key systems**
- Two technologically distinct solutions
  - Post Quantum Cryptography (PQC)
  - Quantum Key Distribution (QKD)

Telsy

Post Quantum Cryptography

Intense research activity in the cryptographic community
New public key algorithms based on «quantum resistant» mathematical problems

A *call* has been open by NIST in **2016**, hoping to close it in **2024**

- 3 classes: encryption, key agreement, signature
- 21 December 2017: 69 proposed algorithms
- 30 January 2019: 26 still in the game

5 families are represented
- **Code-based**
- **Lattice-based**
- Multi-variate-based
- Hash-based
- Supersingular e.c. isogenies-based

Code-based and lattice-based schemes are the most studied and seem to offer higher security guarantees

NIST
National Institute of Standards and Technology

Telsy

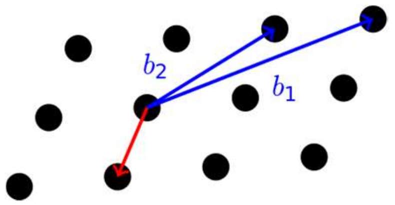
Post Quantum Cryptography

Code – based cryptography

- Relies on error correcting codes
- Based on the difficulty of decoding a general linear code
- McEliece (1978) was already quantum resistant!,
  also fast but with very long keys and thus discarded

Lattice – based cryptography

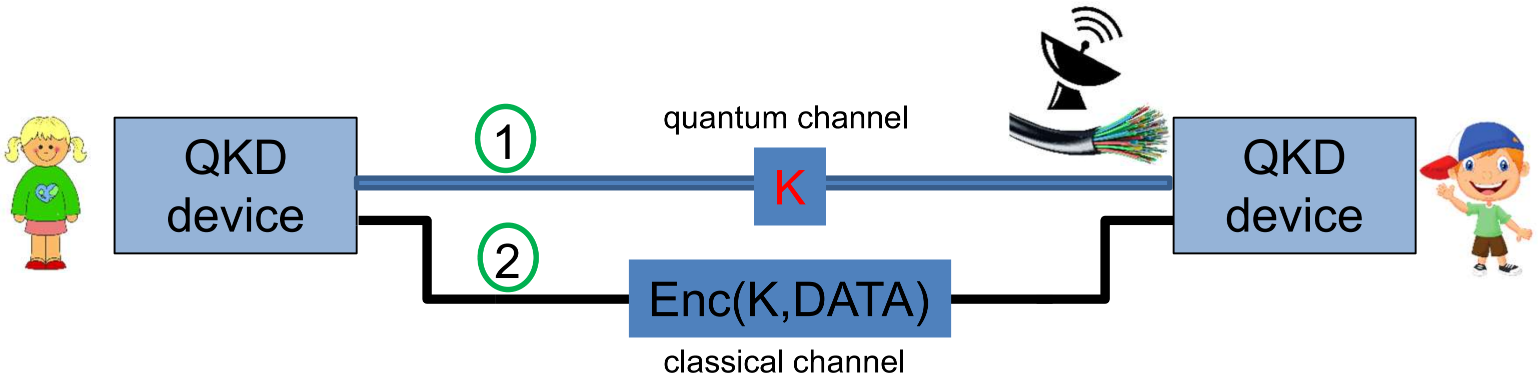
- Relies on the lattices theory
- Based on the difficulty of solving the Shortest Vector Problem in lattices
- NTRU (1996) was also quantum resistant



Telsy

Quantum Key Distribution

- The key is encoded in photons sent on an optical channel (fiber or free space)
- It cannot be intercepted thanks to **the Heisenberg indeterminacy principle**
- Coupled with a non secured classic channel, where the key is used in a traditional manner



- Main advantage: **security is unconditional**, since it is based on quantum mechanics principles
- However:
    - Implementations introduce errors
    - Authentication problem must be solved otherwise
    - As distance increases, trusted nodes are required

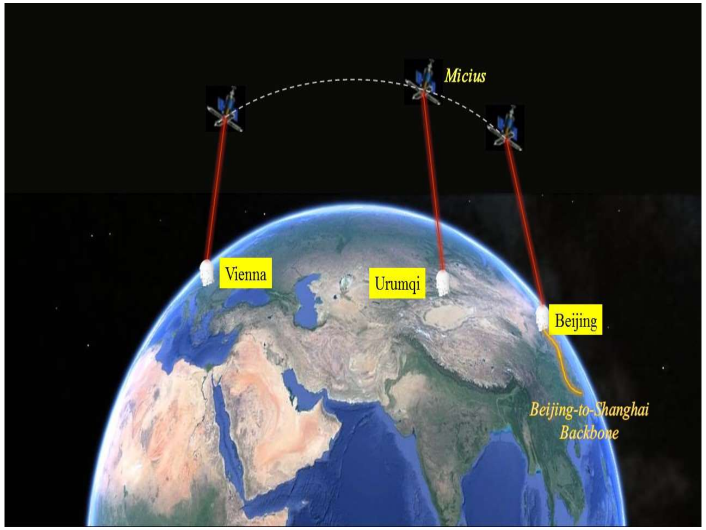
Telsy

Fiber vs Free Space QKD

- Higher technology level
- Requires infrastructure
- Compatible with standard fibers

Source: INRiM

- No infrastructure requirements
- Cover wider areas
- Less mature technology



Source: Chinese Academy of Sciences

Telsy

QKD in the World

QKD manufacturers

IDQ	ID Quantique
SK telecom	SK telecom
MagiQ Technologies	MagiQ
Quintessence Labs Data Uncompromised	Quintessence Labs
国盾量子 QuantumCTek	Quantum CTek

Europe research

Many national projects

Remarkable UE fundings

HORIZON 2020
- H2020

QUANTUM FLAGSHIP
- EU Quantum Flagship (2018-2028, 1 billion €)

Bucharest, 13 June 2019 **Digital Assembly**

7 Member states signed a declaration agreeing to study, develop and deploy a **Quantum Communication Infrastructure** (QCI) within the next 10 years

Telsy – Ongoing Research and Collaborations

Post Quantum Cryptography

Telsy

Quantum Key Distribution

Telsy

INRiM ISTITUTO NAZIONALE DI RICERCA METROLOGICA

LEONARDO

Consiglio Nazionale delle Ricerche

MPD

TELESPAZIO

Telsy

Conclusions

- Quantum computing is a real threat for information security
- It is necessary to develop countermeasures as soon as possible
- It may be late
- PQC e QKD are two solutions
  - ✓ both with pros and cons
  - ✓ complementary (each one better suited for specific scenarios)
  - ✓ can even coexist for very high security applications
  - ✓ much research and development are still required
  - ✓ significant effort at national and international level

Thank you

guglielmo.morgari@telsy.it

Telsy