



UNIVERSITÀ
DEGLI STUDI
FIRENZE

ICT fest

Reti Quantistiche nel Mondo Reale: Tecnologie e Implementazioni

- Davide Bacco
- Università degli Studi di Firenze

davide.bacco@unifi.it



Agenda

- Cryptography and key distribution methods
- Quantum key distribution: protocols and state-of-the-art
- Use of QKD keys in real telecom networks
- Applications of QKD



Cryptography and key distribution methods

Cryptography

Cryptography (from ancient Greek: (kryptós) "hidden, secret" and (graphein), "to write") is **the practice and study of techniques for secure communication** in the presence of third parties called adversaries

ALICE



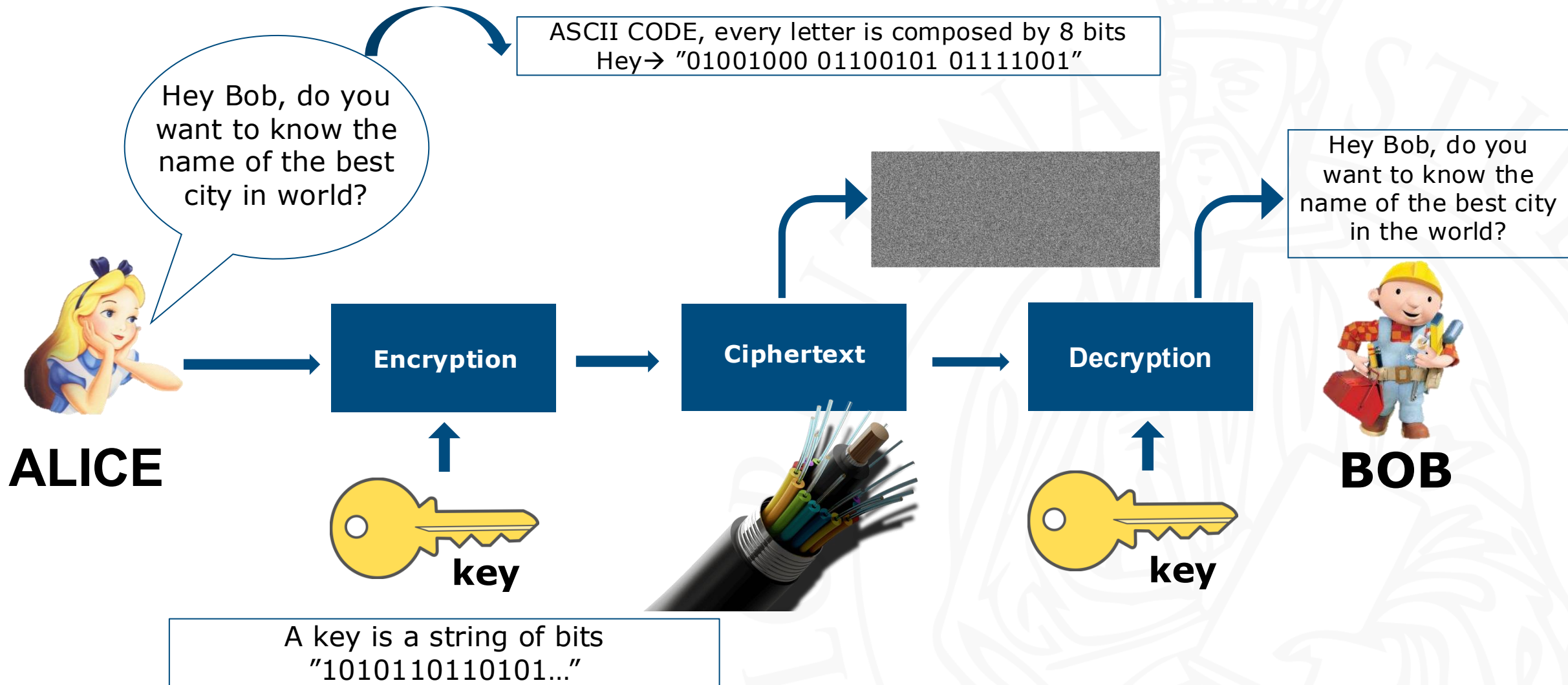
EVE



BOB

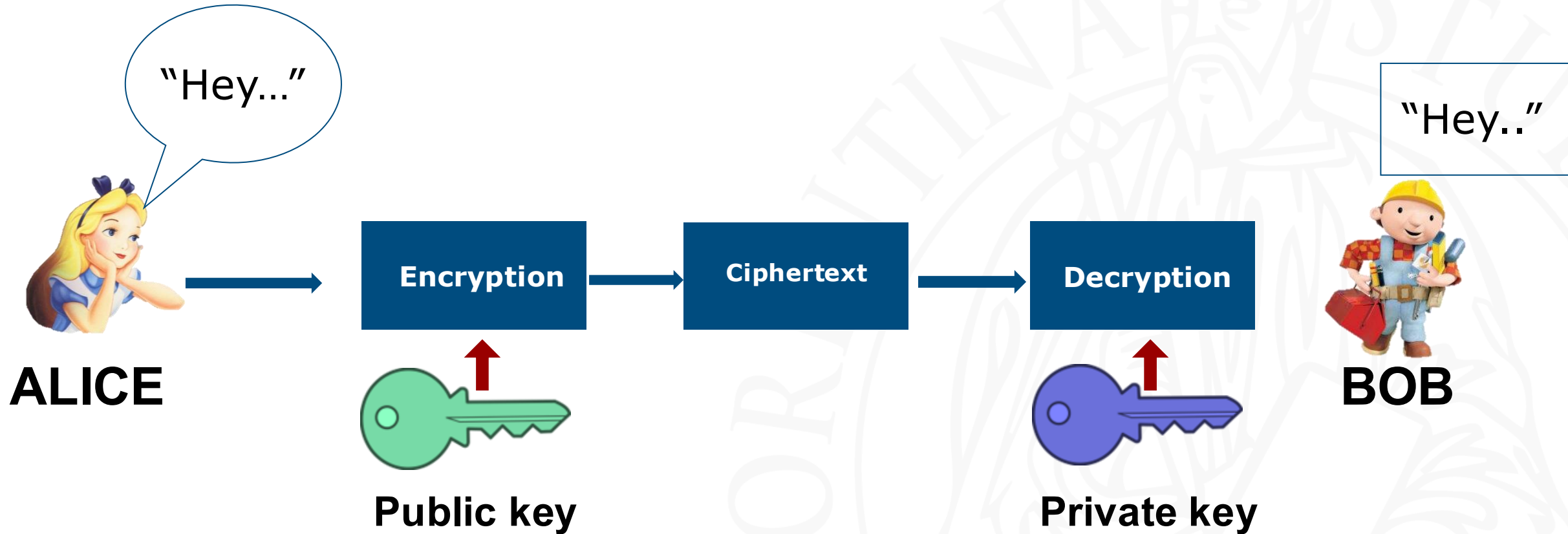


How does it work?



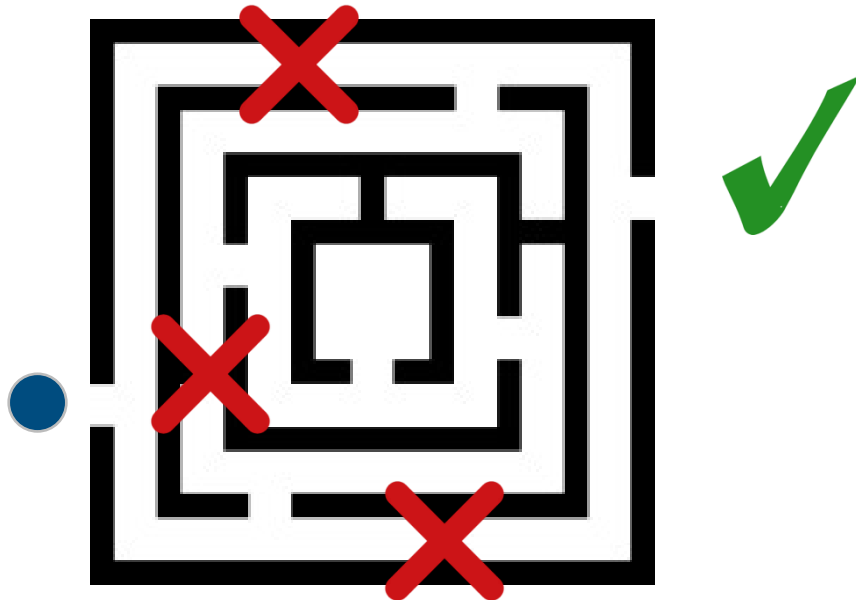
Asymmetric encryption (public and private keys)

12 x 13 = 156 easy to do, but very very difficult to guess.
The number 156 can be divided by 2,3,4,6,12,13,26,39,52,78

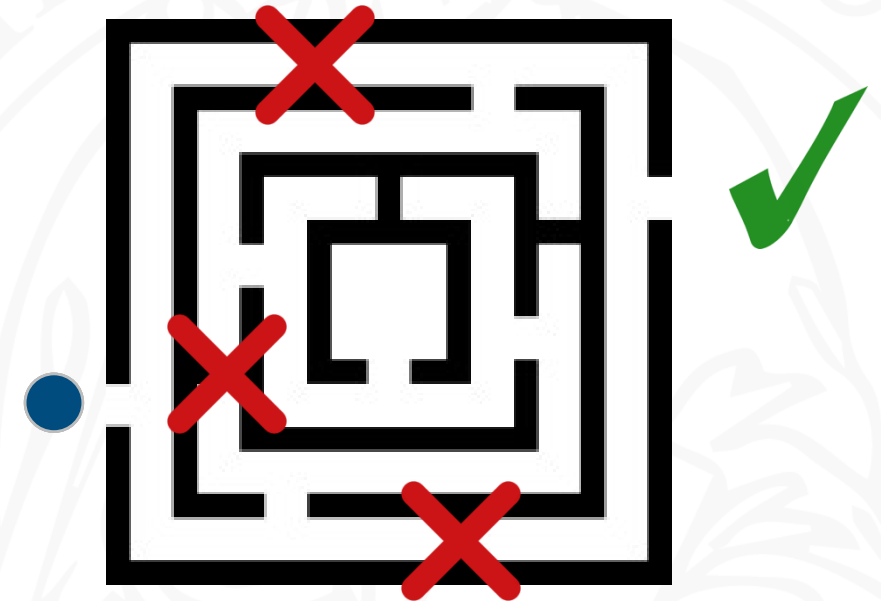


So everything is fine? The powers of quantum computer

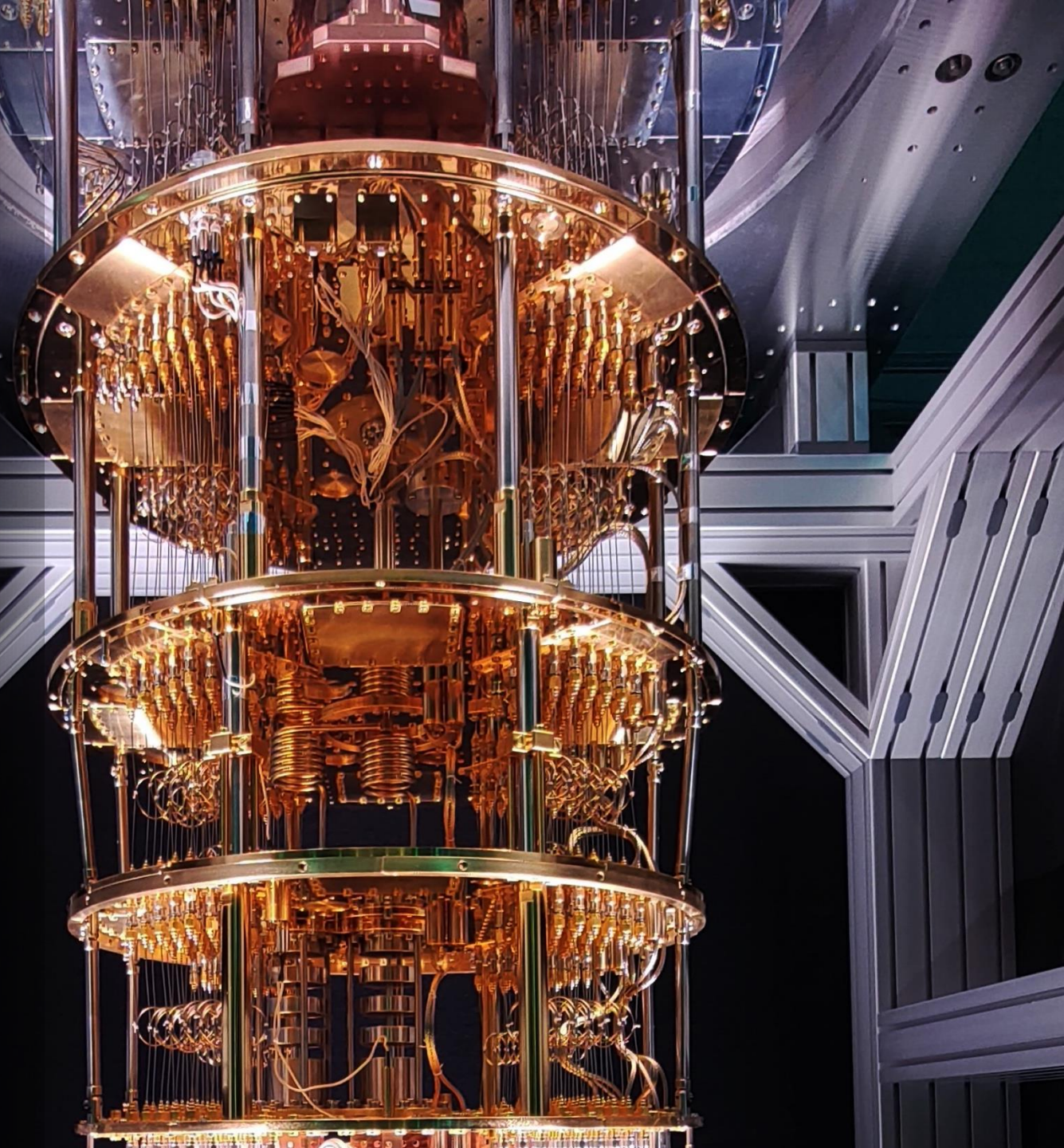
Classical physics



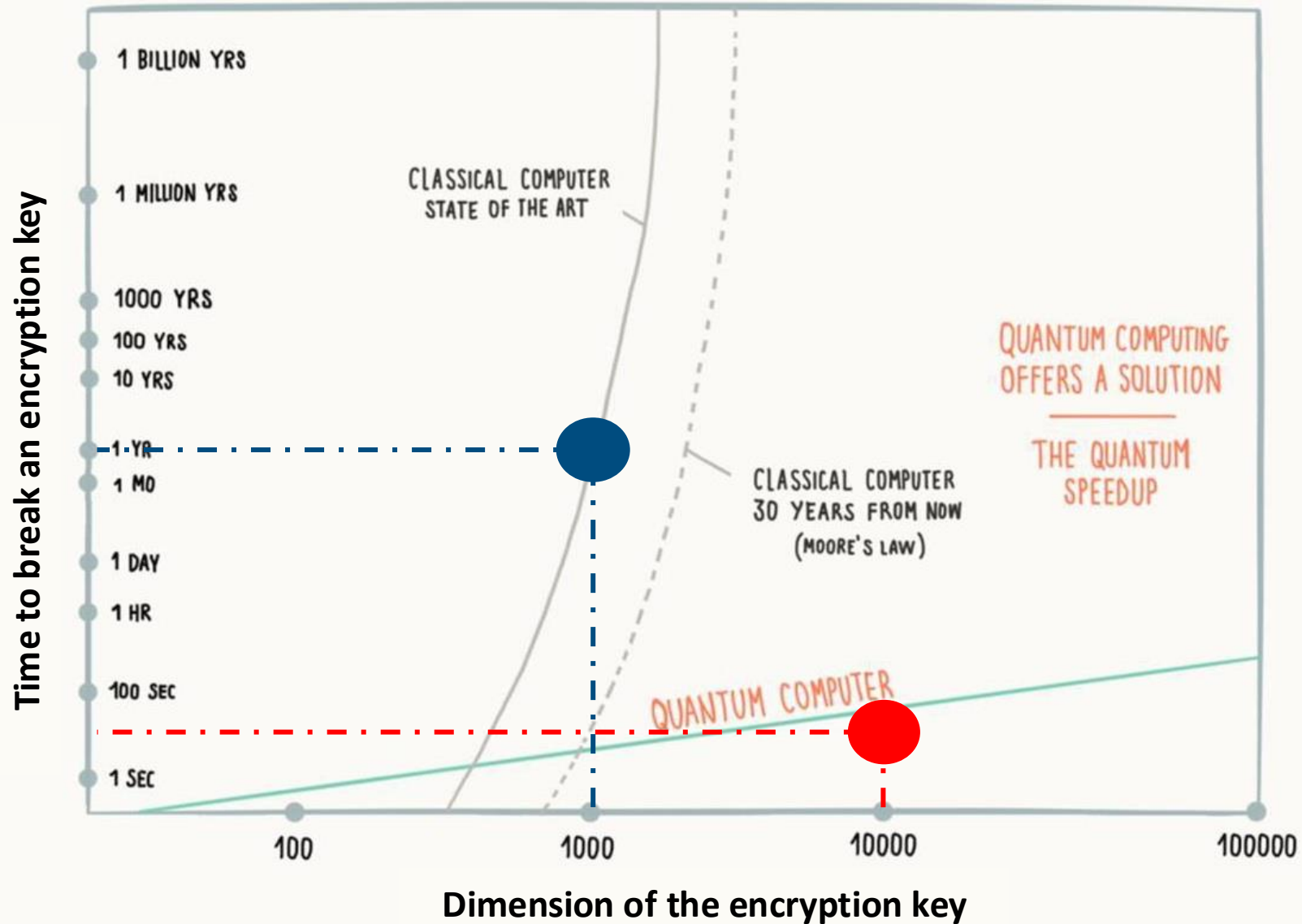
Quantum physics



Quantum computer



Quantum computer and cryptography

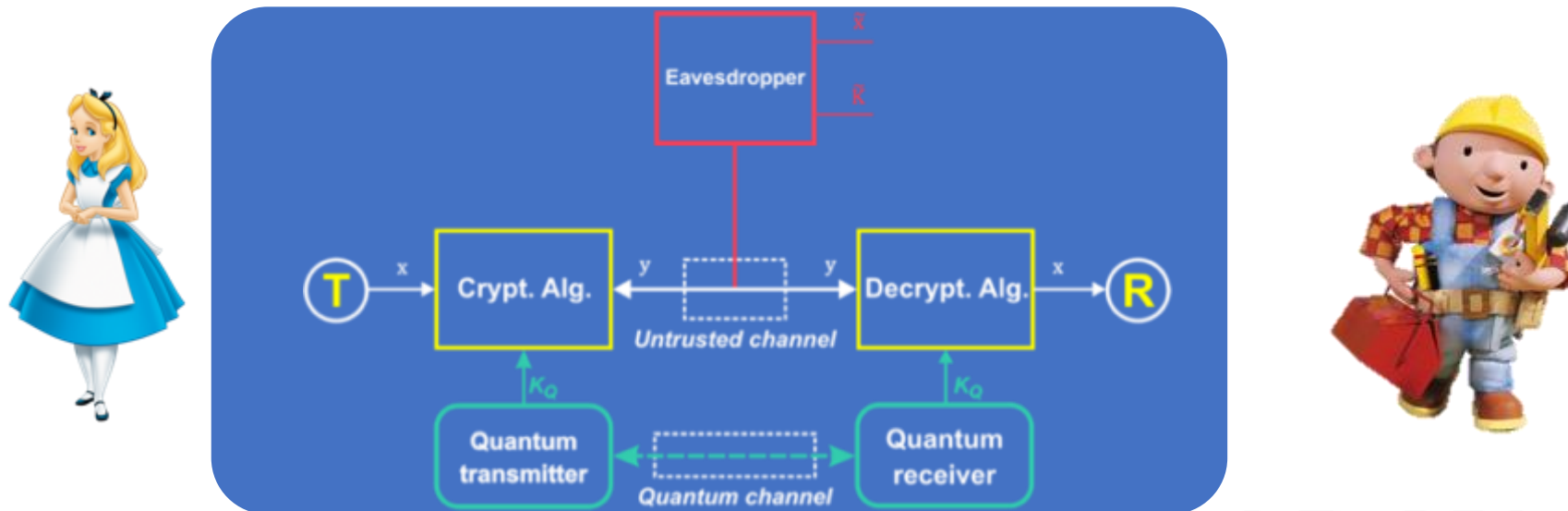




Quantum key distribution: protocols and state-of-the-art

Quantum key distribution

- exploit quantum mechanics laws for establishing symmetric secure keys
- single photons/weak coherent pulses transmission for create quantum keys and classical channel for send encrypted messages
- unique ability to detect eavesdropping in real time in the quantum channel



V. Scarani, et al., Reviews of Modern Physics, 81(3) (2009)

The building block: photon polarization

A photon can be polarized in one direction → it represents a bit (0 or 1)

Rectilinear basis +

bit 0 → horizontal

bit 1 ↑ vertical

Diagonal basis ×

bit 0 ↗ 45°

bit 1 ↘ 135°

Quantum physics as the foundation of future cryptography



Uses photons

Each photon carries a bit through its polarization



Random bases

Sender and receiver choose bases independently



Detectable spy

Heisenberg guarantees every interception leaves traces



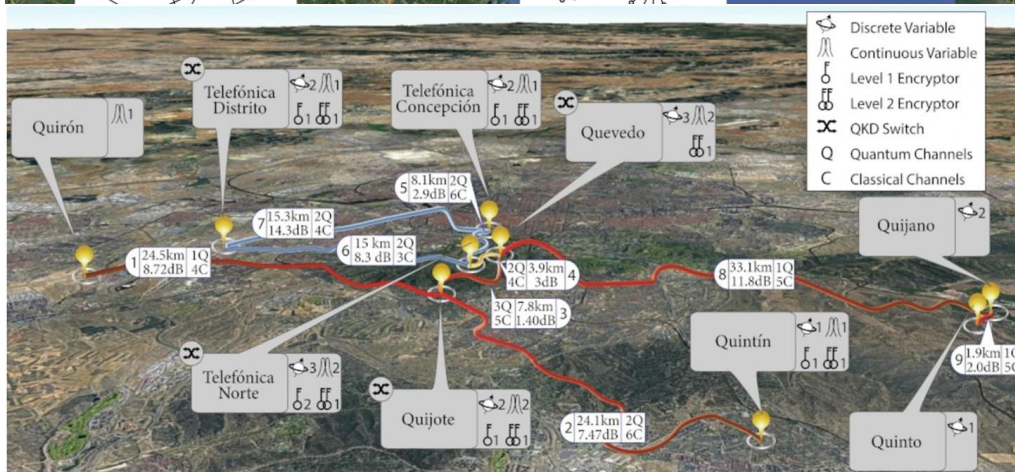
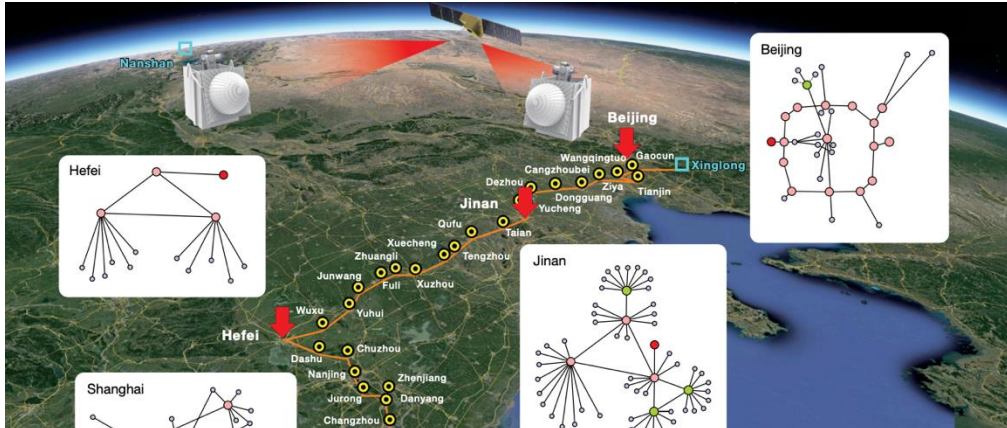
Secure key

The shared key is mathematically unbreakable

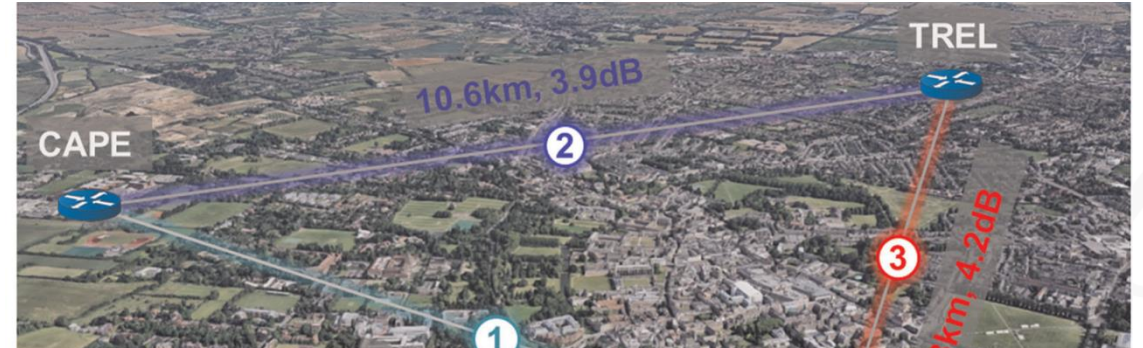


State of the art of QKD

Terrestrial link SoTA

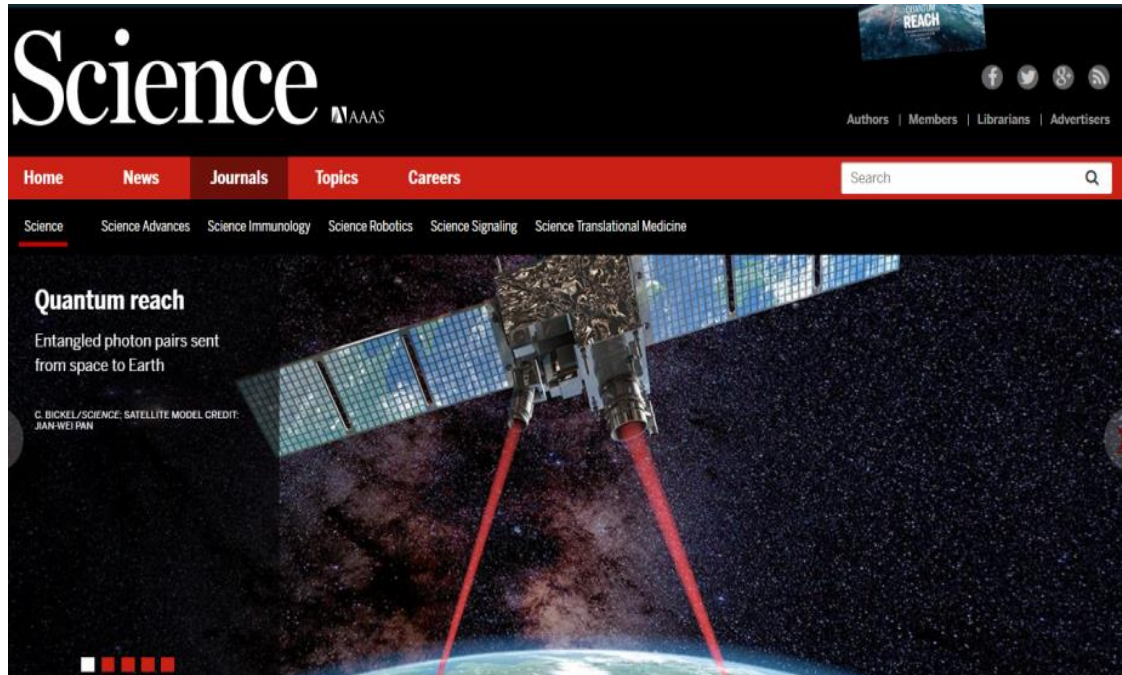


M.I. García Cid, et al., *The 16th International Conference on Availability, Reliability and Security*. 2021.

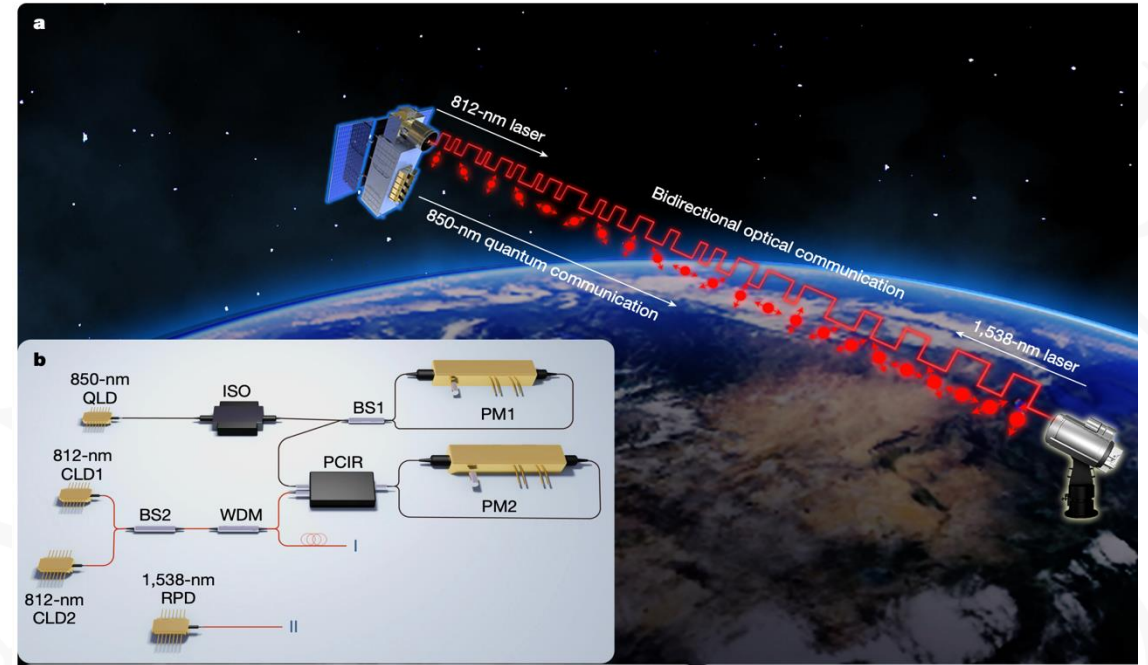


P. Horoschenkoff, et al., arXiv:2503.21186 (2025)

Satellite QCs SoTA

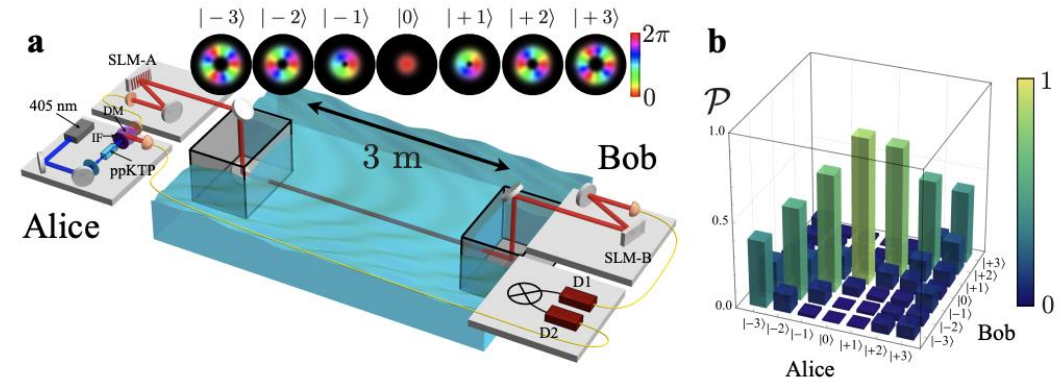
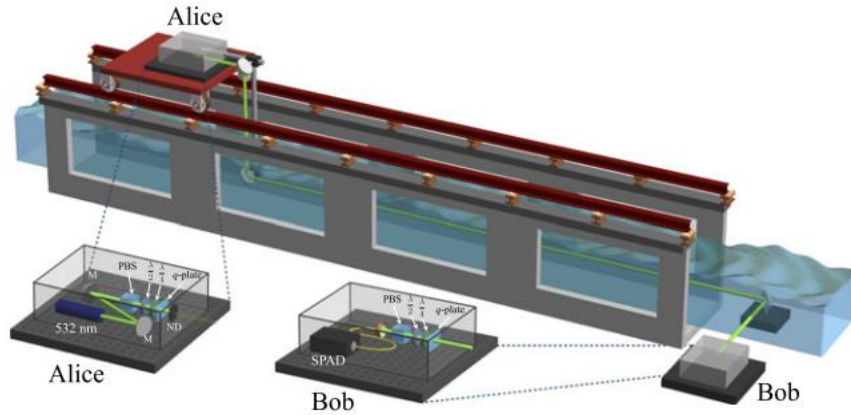


J. Yin et al., *Science* 356 (1140)
J. G. Ren et al., *Nature* 549 (70)



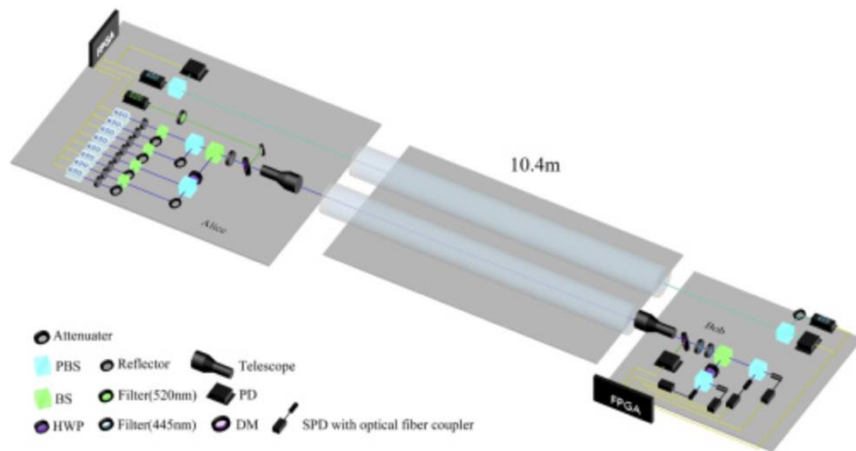
Li, Y., Cai, WQ., Ren, JG. et al. Microsatellite-based real-time quantum key distribution. *Nature* (2025)

Underwater QCs SoTA

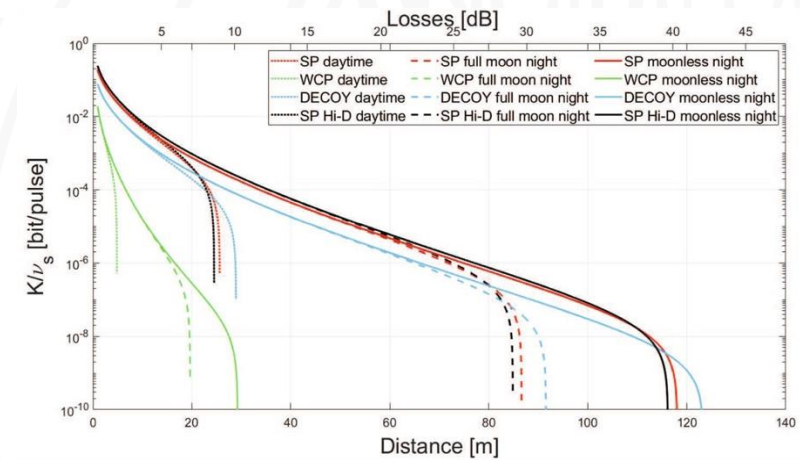


F. Hufnagel, et al., *New Journal of Physics* 22.9 (2020): 093074.

F. Bouchard, et al., *Optics express* 26.17 (2018): 22563-22573.



Y. Yu, et al., *Optics Express* 29.19 (2021): 30506-30519.

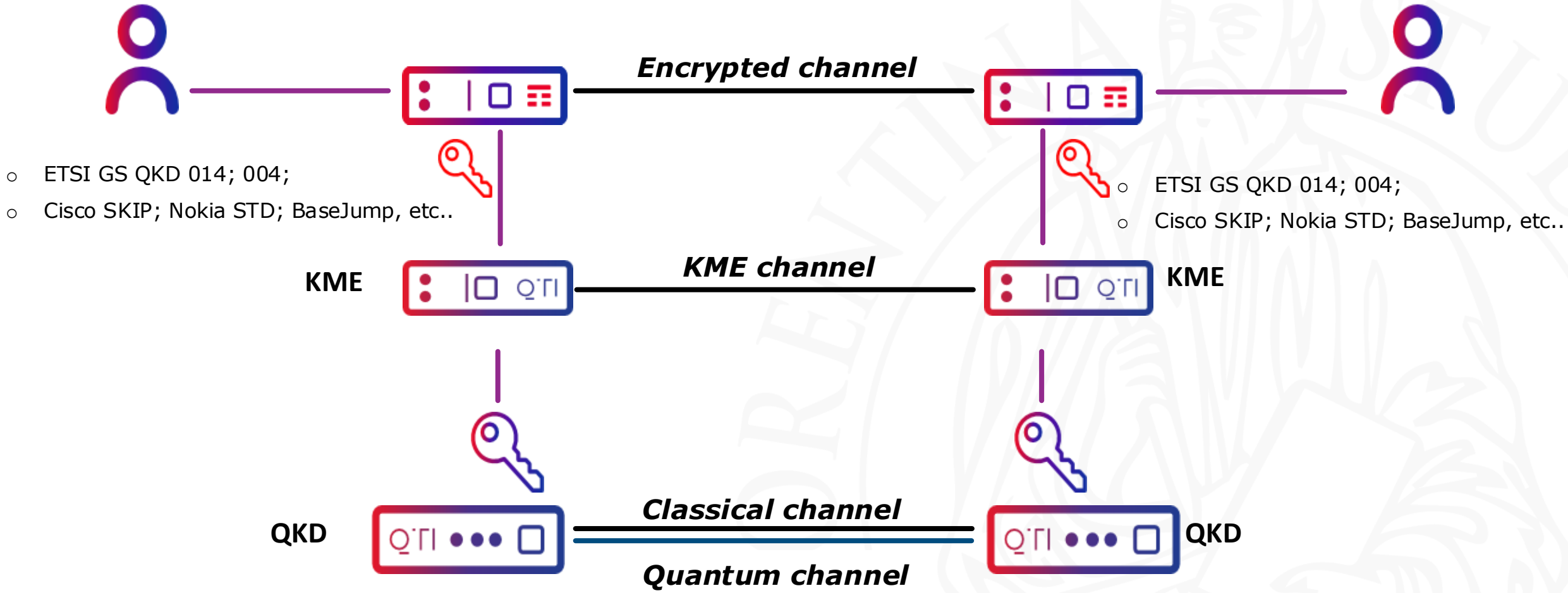


S. Tarantino, ..., D. Bacco, *Optik* 216 (2020): 164639.



Use of QKD keys, and application of QKD

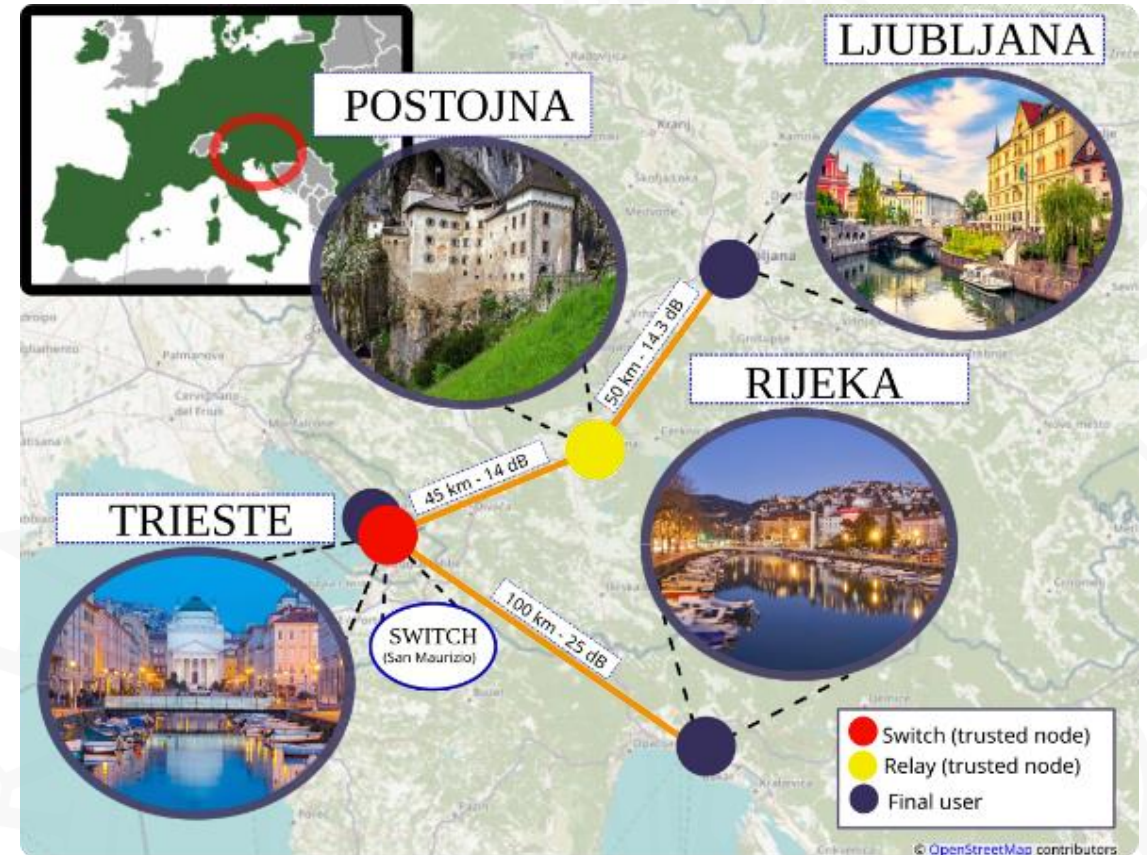
Key manager entity (KME)



The first intergovernmental quantum communication between three countries

In August 2021, QTI supported the implementation of the **intergovernmental quantum communication** during the G-20 on Digitalization.

It was the **first quantum transmission** between three countries, connecting Trieste, Ljubljana and Rijeka.



- **BB84** protocol-time bin encoding with **decoy-state** (up to **30 dB**);
- operating with **single/duplex fiber (C/O band)**

[Deploying an inter-European quantum network, D. Ribezzo et al., Advanced Quantum Technologies, 2200061, 2022]

G7 Summit 2024 Borgo Egnazia

- **13 June 2024**, Apulia
- **QKD link** between Borgo Egnazia and Fiera di Bari (~ 80Km)
- Real-world application



QKD Technology



Encryptors



Connectivity

CORRIERE DELLA SERA

Quotidiano - Dir. Resp.: Luciano Fontana
Tiratura: 182710 Diffusione: 231167 Lettori: 1750000 (DS0001186)

Sussurri & Grida

Tim, connettività per il G7

Tim fornirà servizi di connettività mobile e di sicurezza per il G7 di Borgo Egnazia.

TIM for the G7 Summit

Connectivity and cybersecurity will be the focus of the summit to be held from 13 to 15 June

<https://www.gruppotim.it/en/group/about-us/news/TIM-for-the-G7-Summit.html>

G7 ITALIA
2024



“The truth is, everyone is confused by quantum physics”
– **David Walton, Superposition**

Thank you!