WORKSHOP GARR 2025

NET MAKERS

Integrazione della QKD nelle fibre ottiche per le telecomunicazioni

Alice Meda

INRiM

WORLD ECONOMIC FORUM

Publications

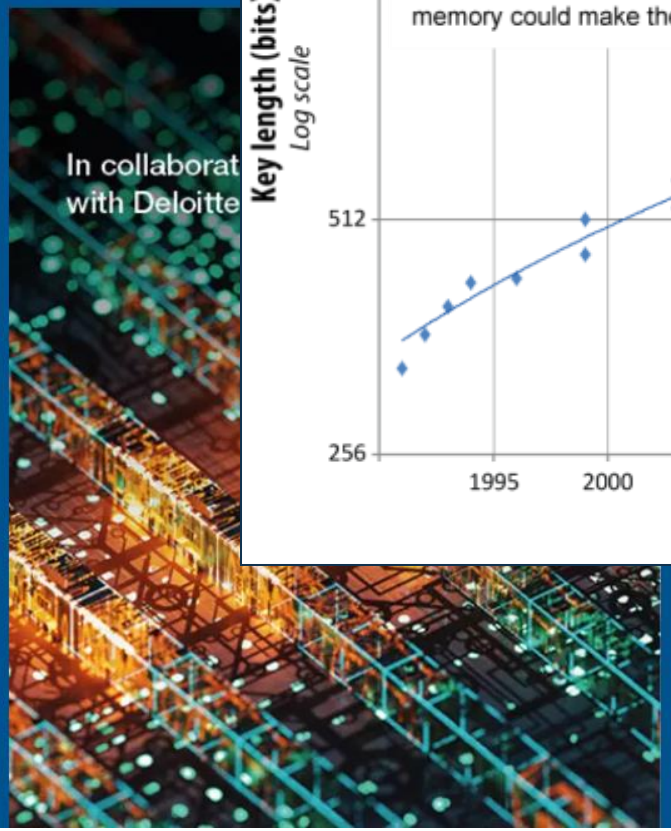
White papers

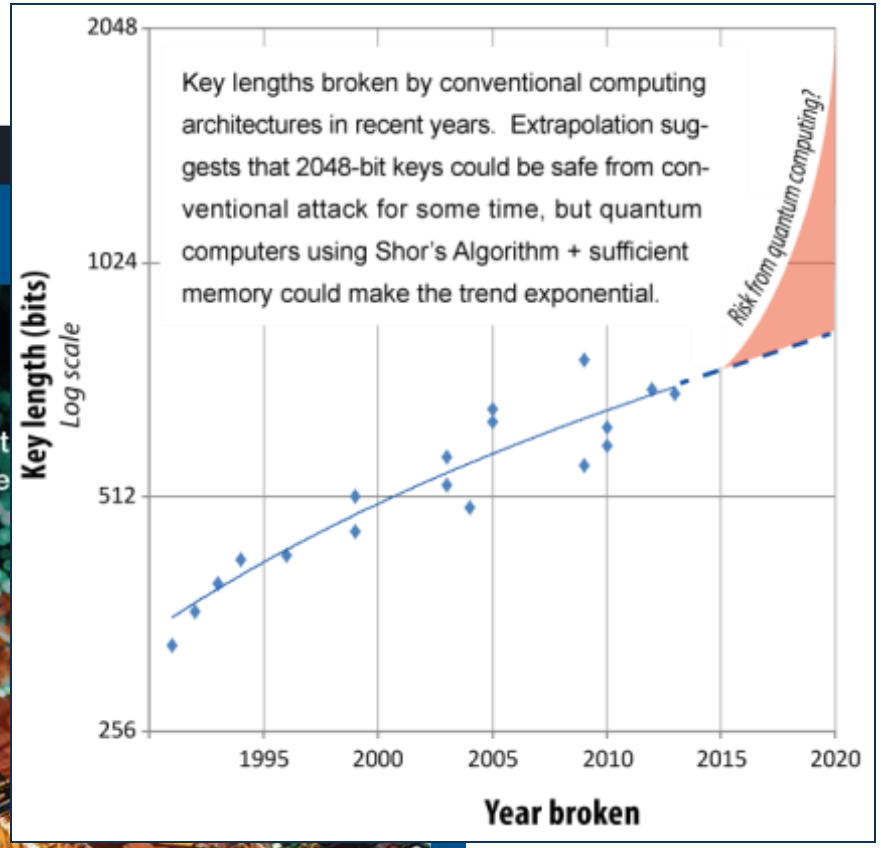
Published: 13 September 2022

Transitioning to a Quantum-Secure Economy

Download PDF

Quantum computing promises transformative simulation and modelling capabilities across a diverse range of industries. However, these advances in computational power will also introduce significant risks via the potential threat of disruption to some widely used encryption standards. While definitive timelines for both quantum computing applications and the associated quantum cybersecurity threats have not yet fully materialized, organizations must act now to evaluate their readiness to adapt to the quantum threat.





QUID QUANTUM ITALY DEPLOYMENT

EuroQCI

QU- TEST

equo

PROMISE

AQuTE PRIN 2022

QUANTUM TECHNOLOGIES

19NET02 EMN Quantum

EMPIR EURAMET

NoQTeS METROLOGY PARTNERSHIP EURAMET

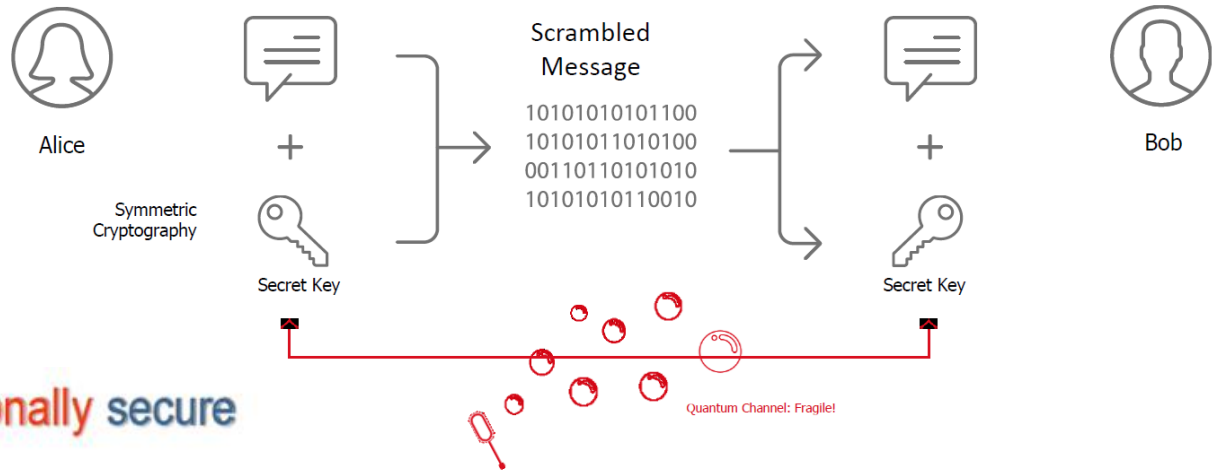
Fondazione Compagnia di San Paolo

QuteNoise

What is Quantum Key Distribution?

Cryptography is the art of rendering a message unintelligible to **any unauthorized** party

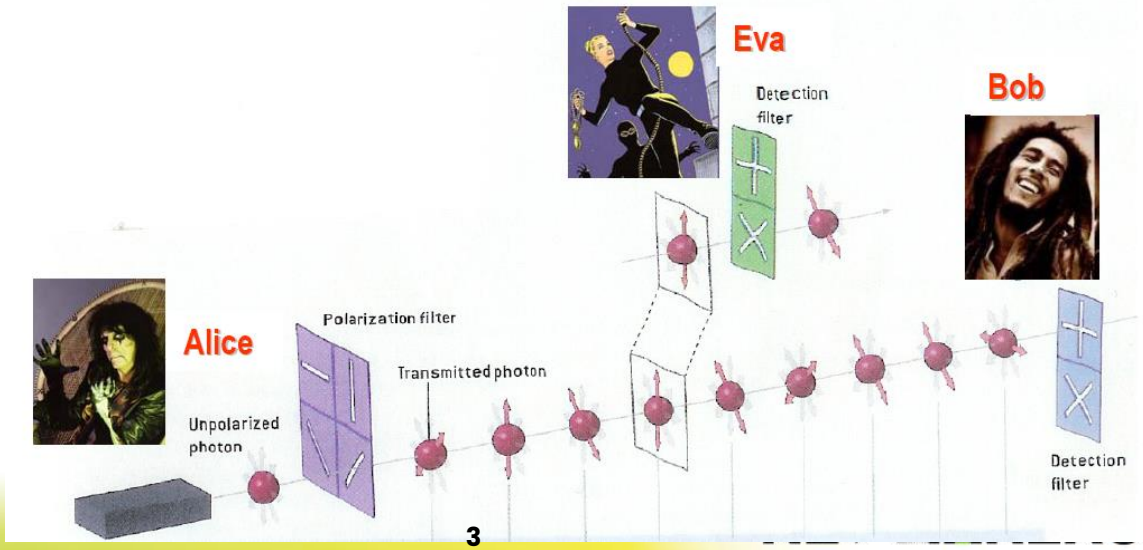
An algorithm -a Cipher- combines the message with some additional information –the Key- producing a cyphertext. The system is secure if the cyphertext can be unlocked only by the Key



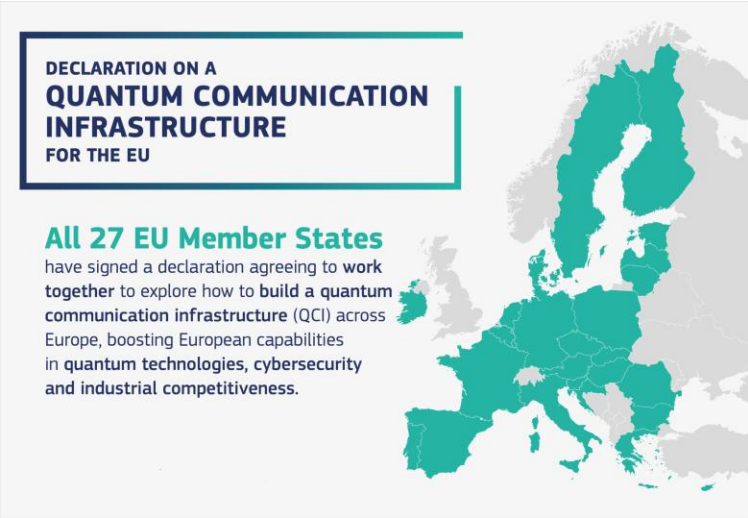
Quantum Cryptography (QKD) is able to distributed unconditionally secure Keys by means of single quantum systems

QM does not prevent eavesdropping, it only allows the detection of the presence of an eavesdropper, as this presence induces differences in the generated Keys. Unconditional secure Keys are established once Alice and Bob constantly monitor the security of the quantum communication channel

Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↘	↗	→	↗	→	→
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		1			0		1



European Quantum Communication Infrastructure



EuroQCI

EuroQCI: European Commission initiative, working with all 27 EU Member States and the European Space Agency (ESA), to design, develop and deploy a quantum communication infrastructure

EuroQCI space segment
Distribution of quantum-secured encryption keys on a global scale

EuroQCI terrestrial segment
Federation of national terrestrial QCI networks with cross borders connections

QUID: Quantum Italy Deployment

2023-2025

QUID

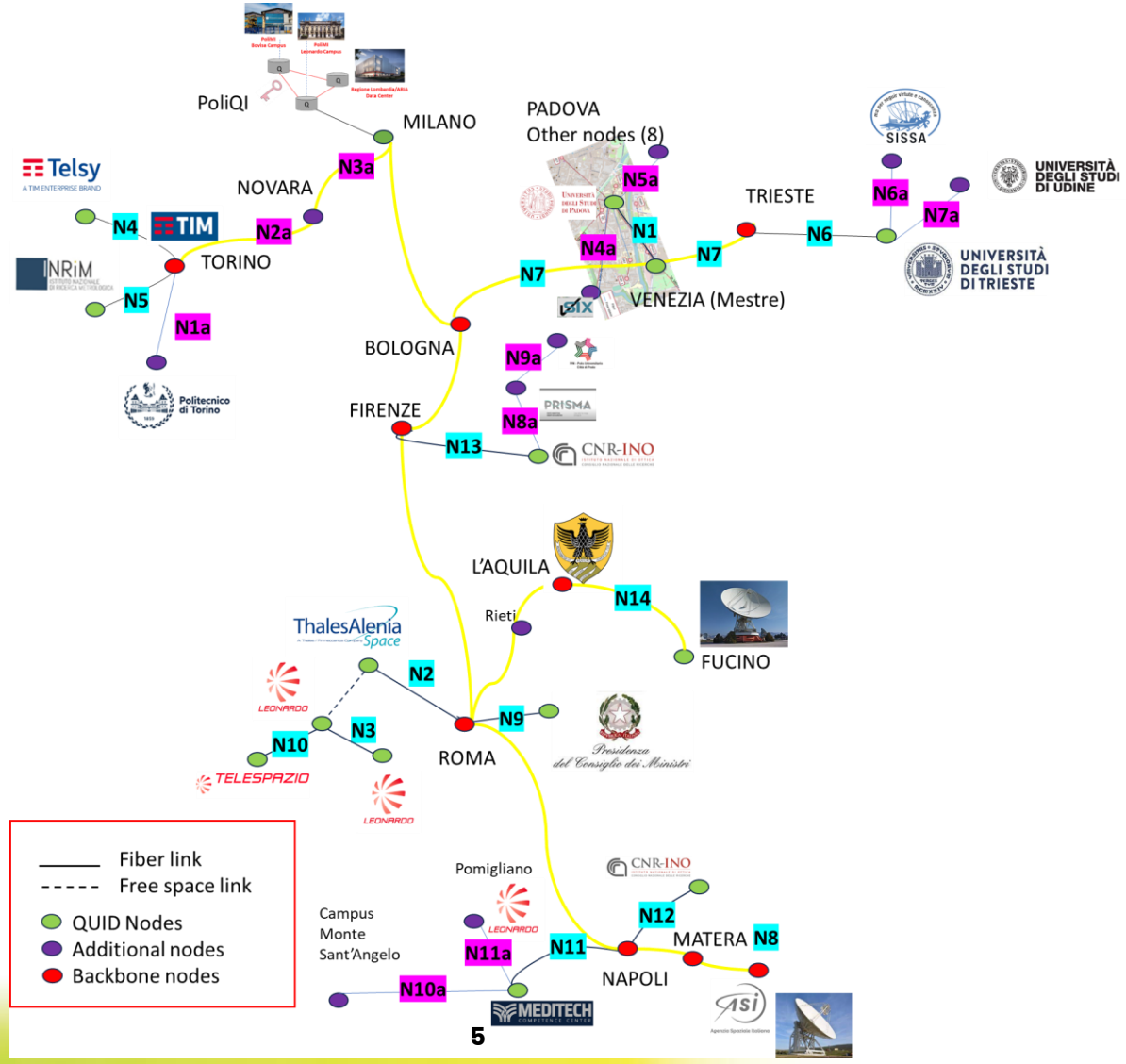
QUANTUM ITALY DEPLOYMENT

INRiM Istituto Nazionale di Ricerca Metrologica · LEONARDO · cohaerentia Fiber Optic Sensors For Smart Diagnostics · TELESPAZIO a LEONARDO and THALES company · Q.TI Quantum Telecommunications Italy · Telsy · ThinkQUANTUM · ASI Agenzia Spaziale Italiana · ThalesAlenia Space a Thales / Leonardo company · top-ix WE DO CONNECTIONS · Consiglio Nazionale delle Ricerche · TIM

Università Padova · Politecnico Milano · Università Napoli · Università Sapienza · Università Aquila · Università Trieste

- Deploy advanced national quantum systems and networks for testing quantum communication technologies and for integrating them with existing communication networks
- Use these quantum systems and networks for developing and testing use cases

- Quantum Metropolitan Area Networks (QMAN), >14 points in 9 towns: Turin, Milan, Bologna, Padua, Trieste, Florence, Rome, Naples, Matera.



Italian Quantum Backbone

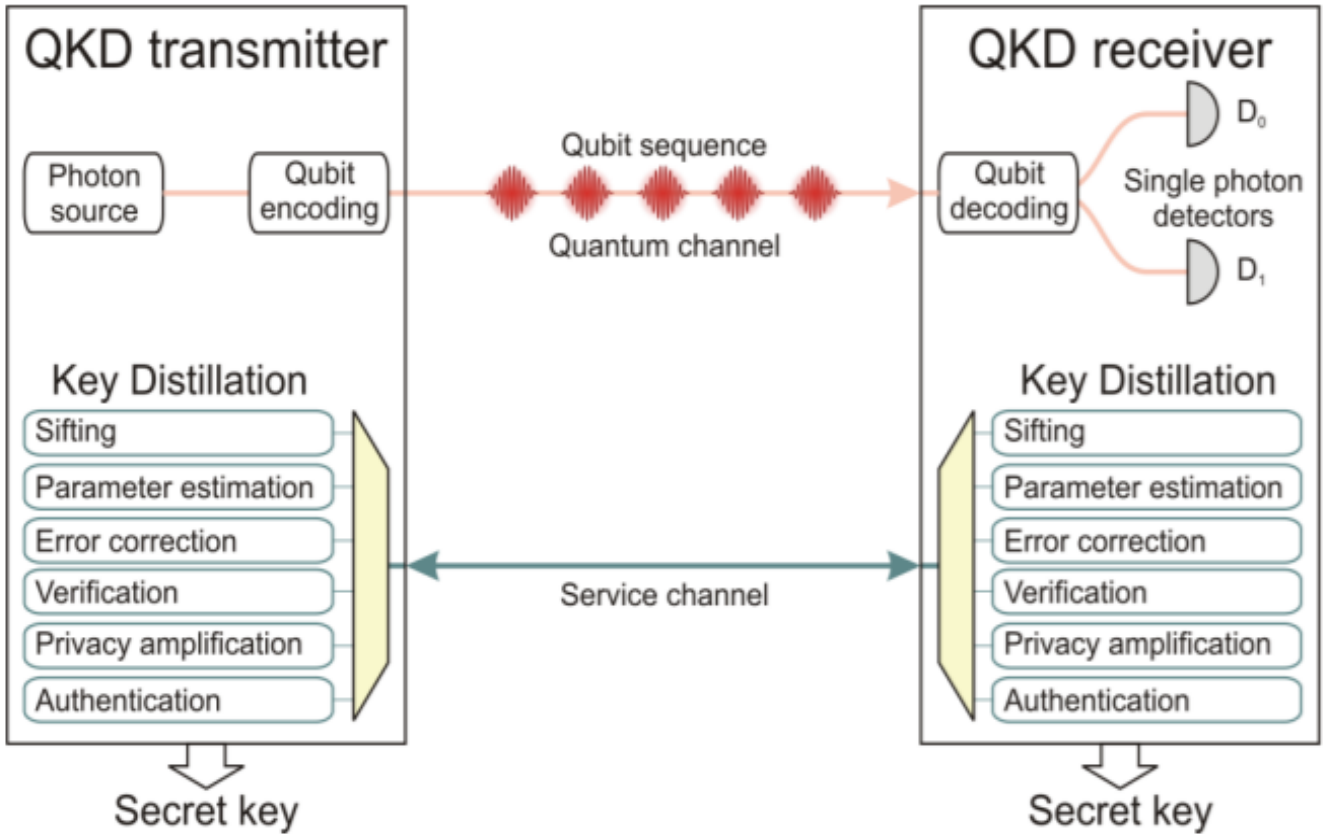
- 1800 km of dedicated optical fiber
- QUID: Long range QKD / 7 Q-MAN / 9 Use Case / 18 partners
- 6 nodes for ultrastable laser delivery
- Precise **time and frequency** references at all points of presence across Italy (VLBI Geodesy, Aerospace-Galileo)
- A testbed for **quantum physics** experiments and **distributed fiber sensing**
- WR-PTP for several public/private sub-ns time distribution
- Two fibers: one with data, one dark

https://www.inrim.it/en/research/infrastructures/italian-quantum-backbone

Real world QKD

The actual implementations of the QKD protocols belong to a number of broad technological realization classes: DV, CV, entanglement based, DI, MDI, Twin-Field.

Point-to-point (P2P) DV QKD and Twin-Field QKD are, to date, the most documented protocols by standardization bodies.



Two units physically separated at opposite ends of a pair of communication channels, a quantum and a service channel.

In the classical channel optical signals for clock synchronization/recovery and distillation of data are transmitted.

ETSI World Class Standards

[ETSI-WP8] ETSI White Paper No. 8 Quantum Safe Cryptography and Security An introduction, benefits, enablers and challenges

Single photon detectors

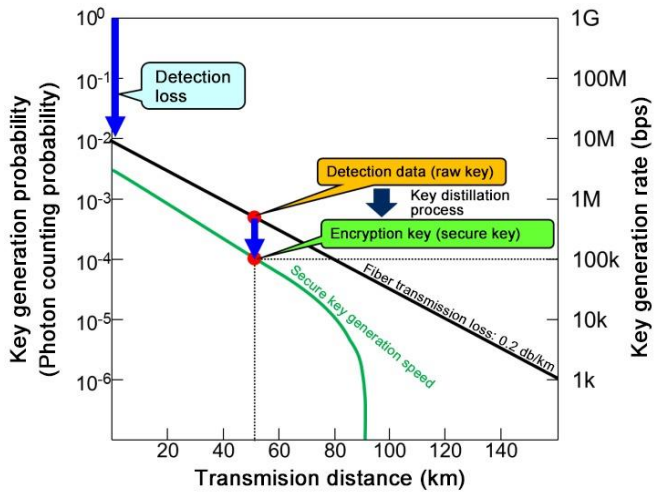
ID210 Free-running NFAD

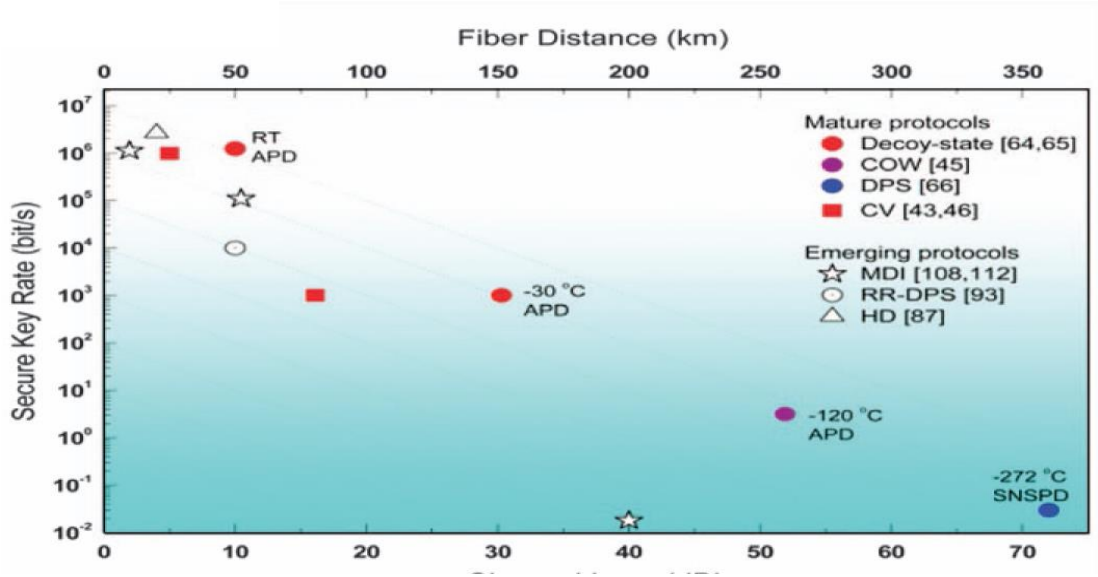
ID220 Gated and Free-running Module

ID230 Ultra-Low noise NFAD

ID281 SNSPD

Real-World channel requirements



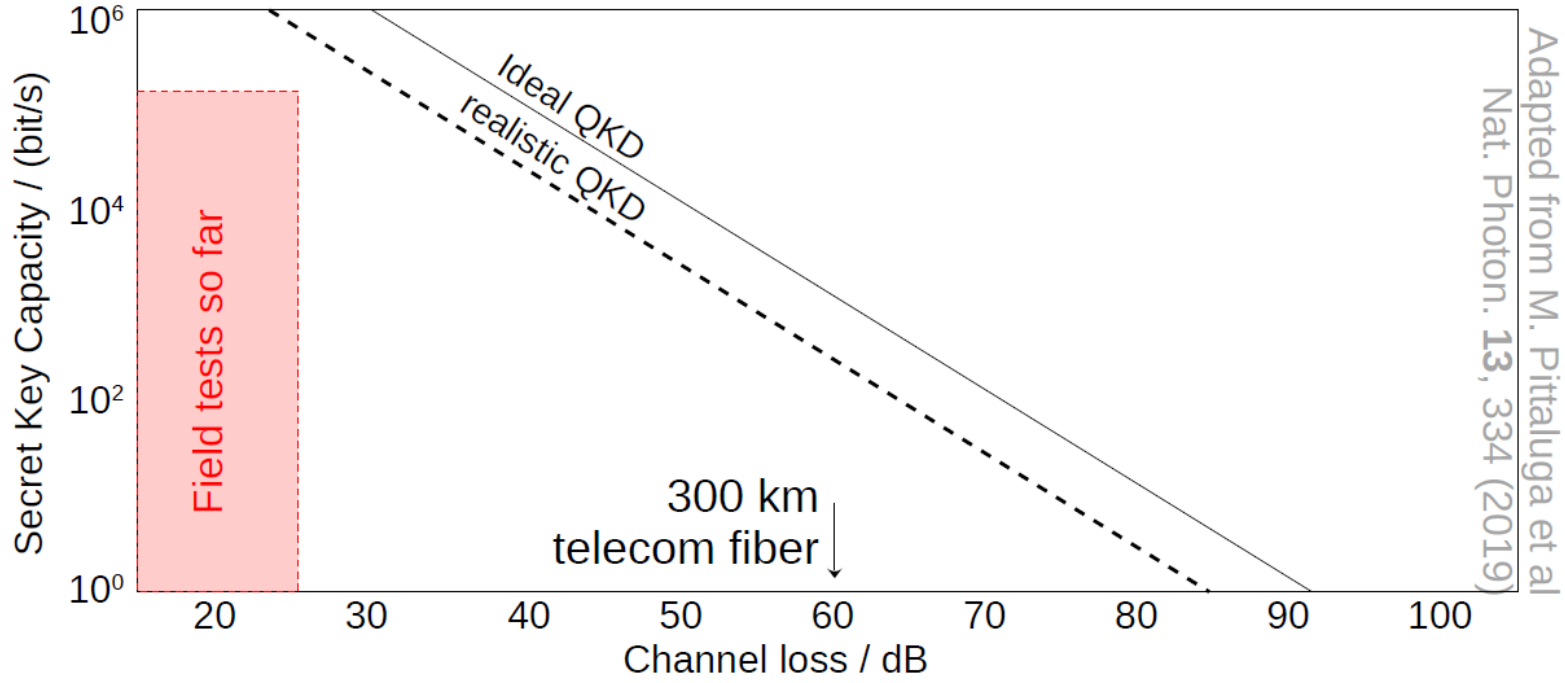


Open Access | Published: 26 April 2017

Fundamental limits of repeaterless quantum communications

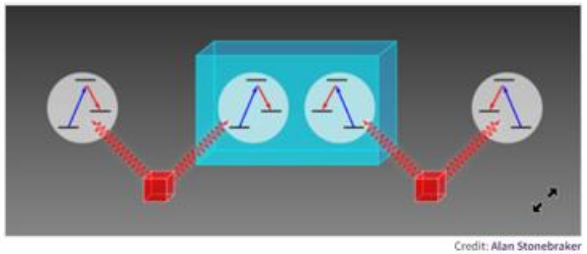
Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani & Leonardo Banchi

Nature Communications 8, Article number: 15043 (2017) | Cite this article

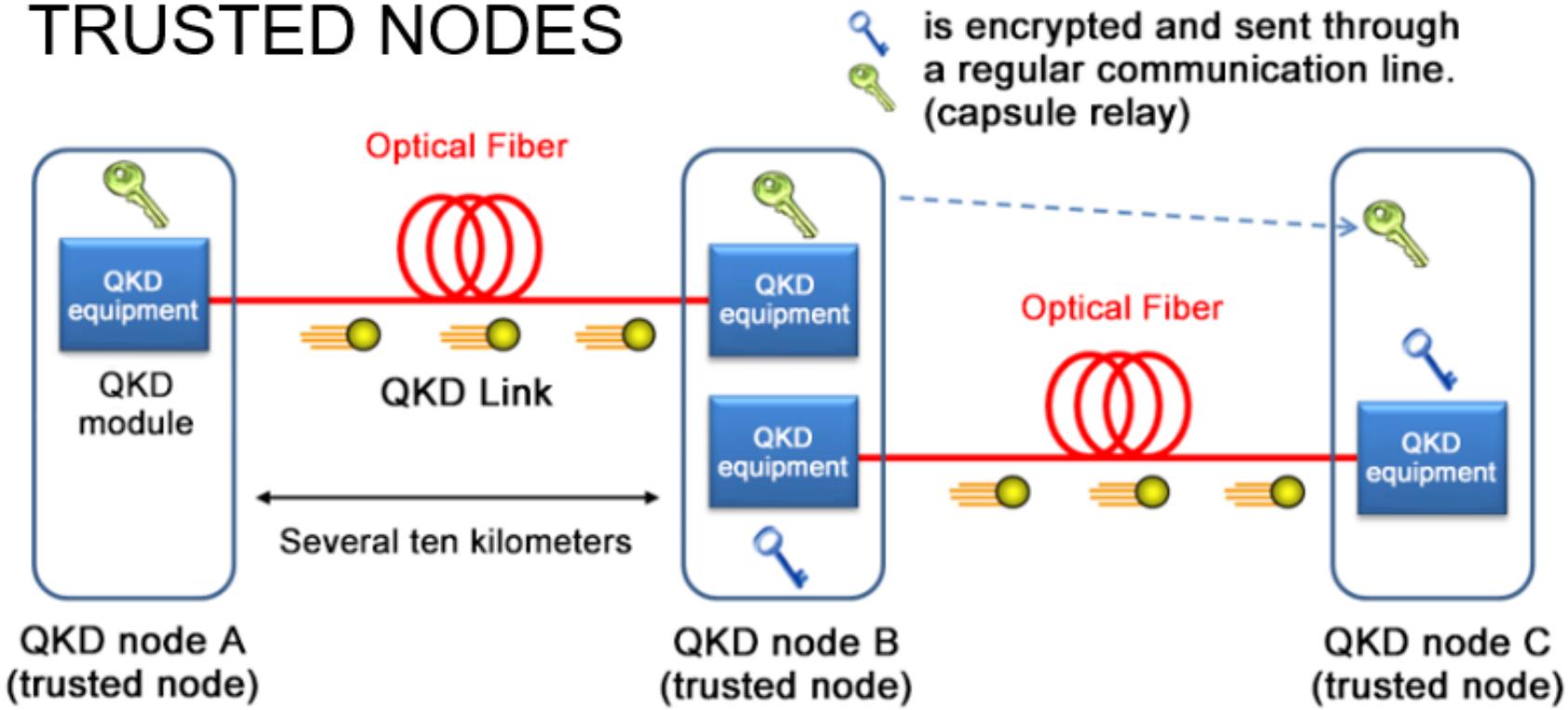


OPTICAL AMPLIFIERS

QUANTUM REPEATERS



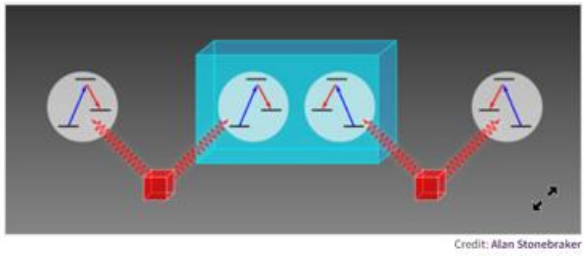
TRUSTED NODES



No Cloning Theorem

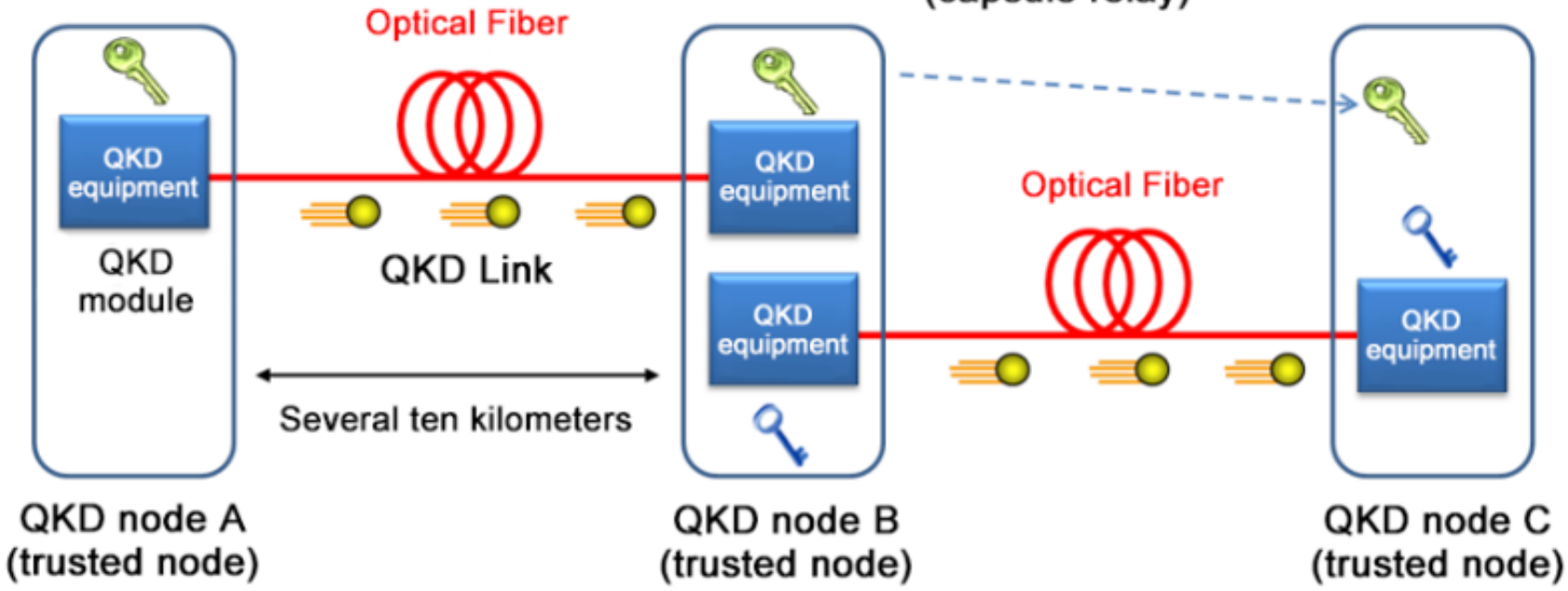
OPTICAL AMPLIFIERS

QUANTUM REPEATERS



TRUSTED NODES

is encrypted and sent through a regular communication line. (capsule relay)



No Cloning Theorem

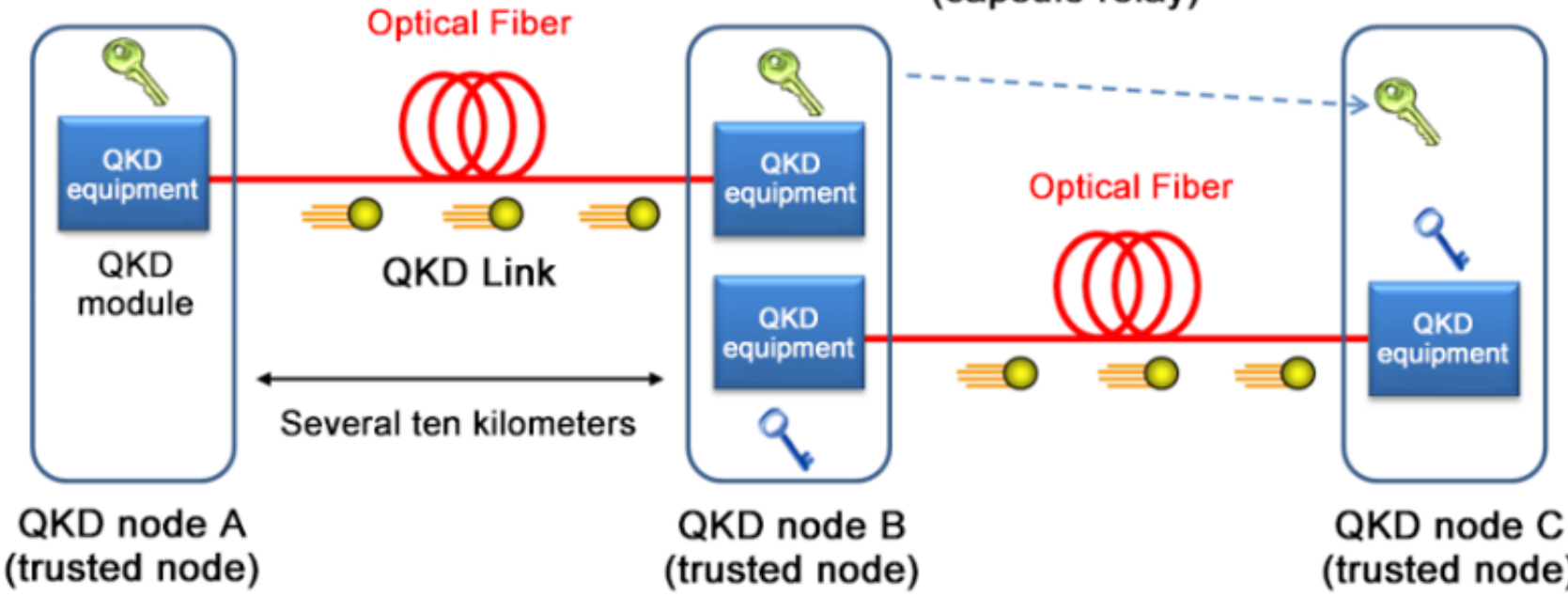
OPTICAL AMPLIFIERS

Not applicable (yet)

QUANTUM REPEATERS

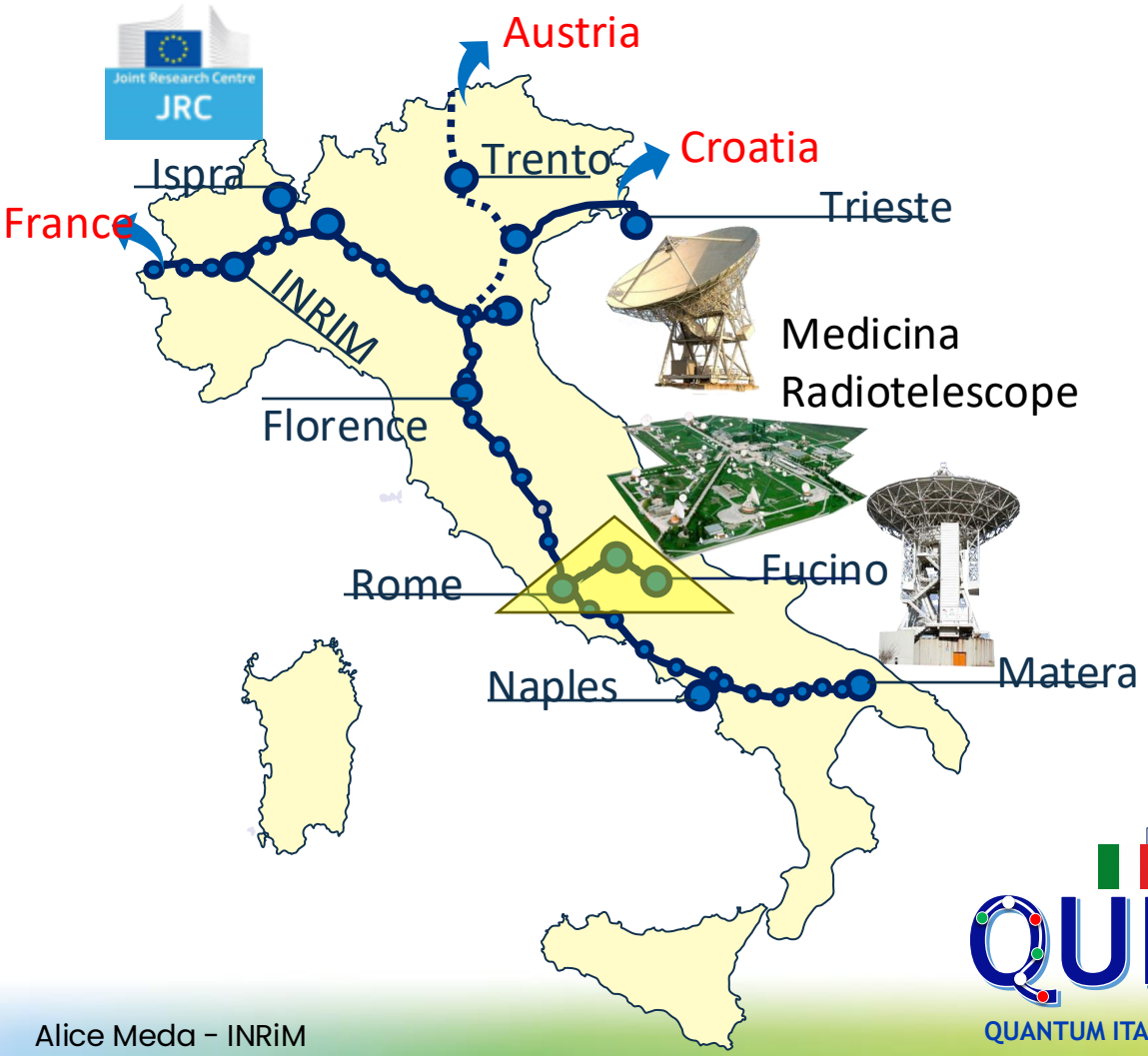
TRUSTED NODES

is encrypted and sent through a regular communication line. (capsule relay)

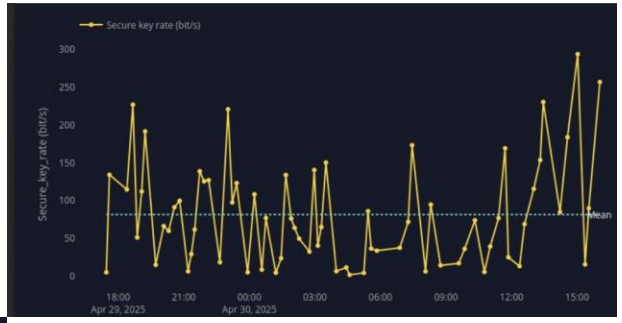


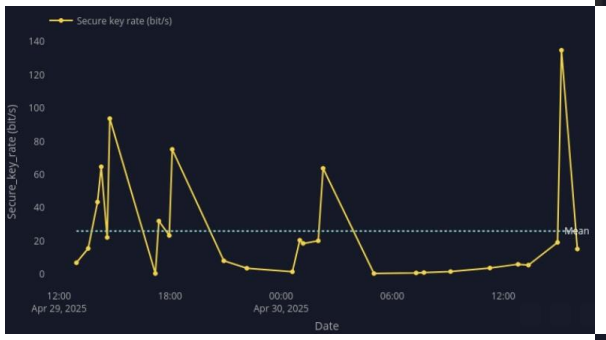
Long-Haul Transmission

TRUSTED NODE SOLUTION



ROMA – RIETI
1550 nm
LOSSES: 25 dB
BG ~ 1700 cps



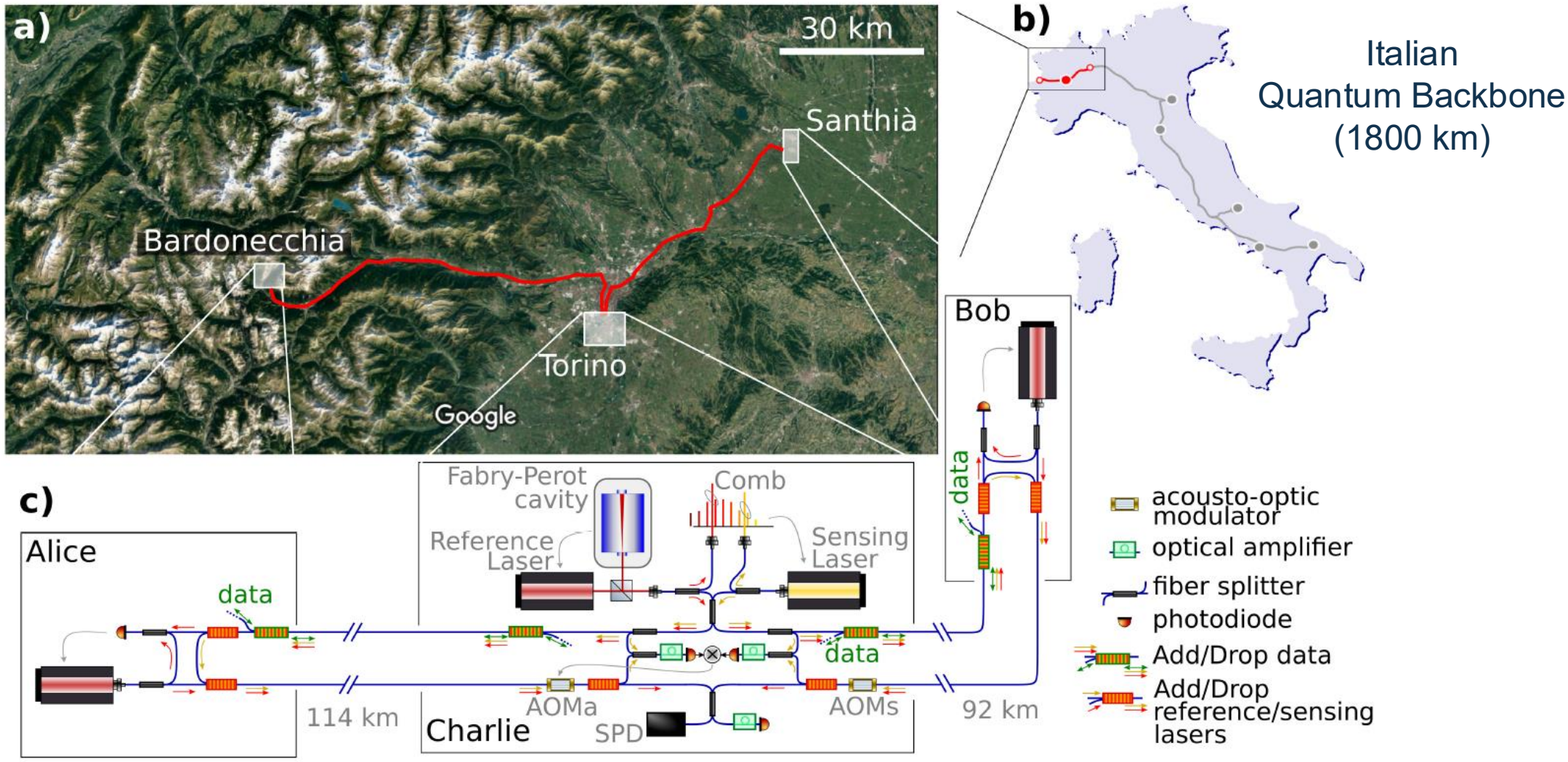


RIETI – L' AQUILA
1310 nm
LOSSES: 25 dB
BG ~ 6000 cps

L' AQUILA – FUCINO
1550 nm
LOSSES: 27 dB
BG ~ 1000 cps

QUID
QUANTUM ITALY DEPLOYMENT

Twin-Field QKD Setup



C. Clivati, A. Meda*et al.*, Nat. Commun. **13**, 157 (2022)

G. Bertaina *et al.*, Adv. Quantum Technol. **7**, 2400032 (2024)

QKD-protected time dissemination

Opportunity to protect and disseminate Time information

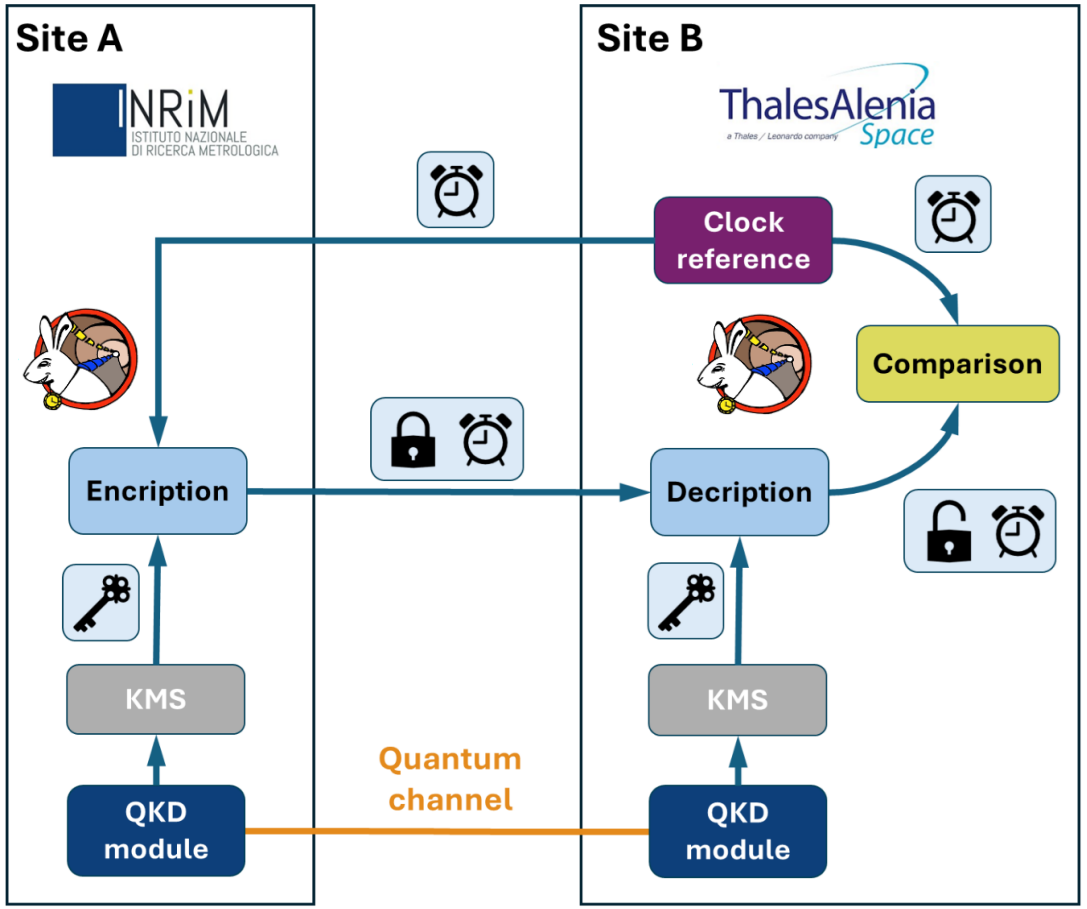
Article | Open access | Published: 18 April 2025

QKD protected fiber-based infrastructure for time dissemination

Alice Meda, Alberto Mura, Salvatore Virzì, Alessio Avella, Filippo Levi, Ivo Pietro Degiovanni, Andrea Geraldi, Mauro Valeri, Silvia Di Bartolo, Tommaso Catuogno, Mattia Verducci, Marco Genovese & Davide Calonico

Scientific Reports **15**, Article number: 13419 (2025) | Cite this article

White Rabbit COLLABORATION



QKD is used to insert random noise in the time and frequency signal.
Idea of strategic selected availability time distribution service: only accredited users that own the key would have access to the highest-precision time and frequency signals.

Grazie per l'attenzione!

per le domande: wooclap.com
codice WSGARR25

QUID QUANTUM ITALY DEPLOYMENT
EuroQCI
QU- TEST
equo
PROMISE
AQuTE PRIN 2022
QUANTUM TECHNOLOGIES
19NET02 EMN Quantum
EMPIR EURAMET
NoQTeS METROLOGY PARTNERSHIP EURAMET
Fondazione Compagnia di San Paolo
QuteNoise

WORKSHOP GARR 2025

NET MAKERS