Quantum Security: una nuova frontiera

Davide Calonico

d.calonico@inrim.it

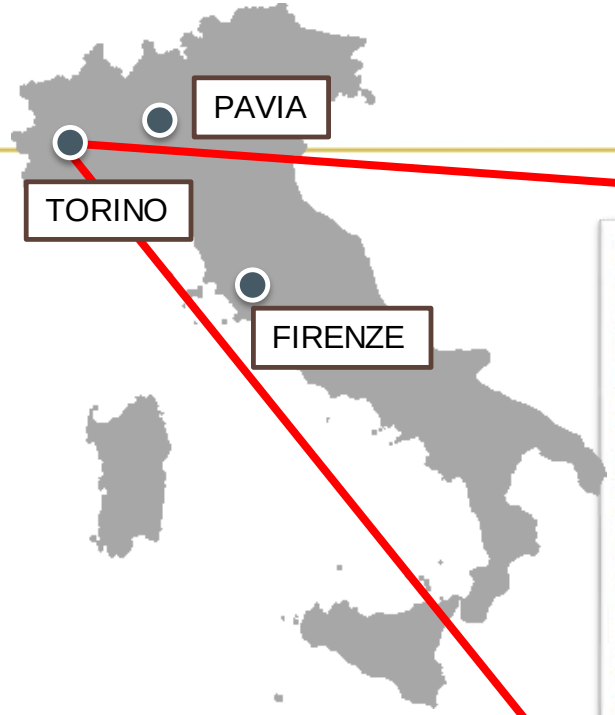
INRiM
ISTITUTO NAZIONALE
DI RICERCA METROLOGICA

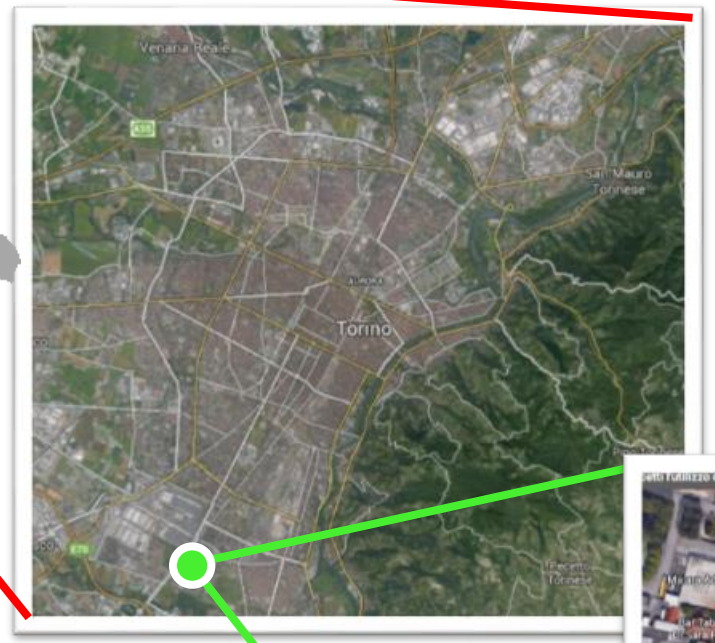
Sommario

- Quantum Security: sincronizzazione e orologi atomici
- Quantum security: QKD
- Comunicazione Quantistica / scenario nazionale ed europeo
- Conclusioni

INRiM
ISTITUTO NAZIONALE
DI RICERCA METROLOGICA

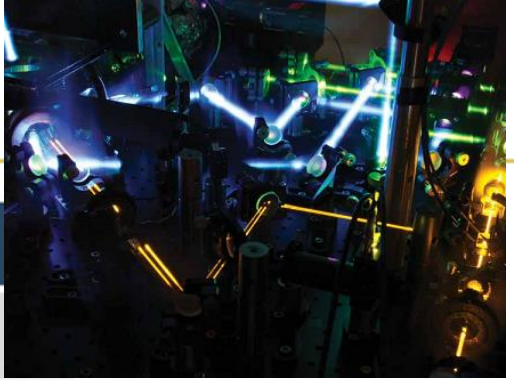
INRIM IN BREVE

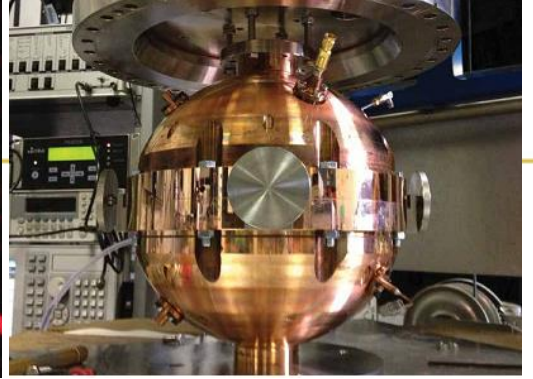
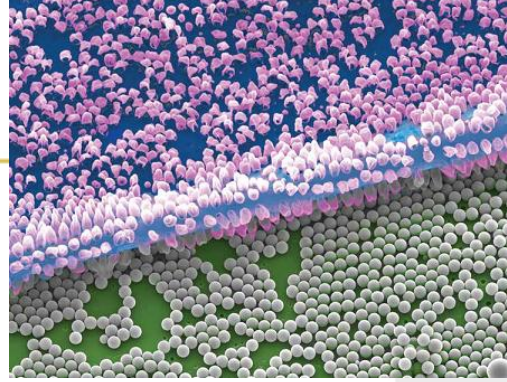




- Istituto Metrologico italiano nella Convenzione del Metro
- 250 dipendenti, 30 M€ bilancio annuale
- Campus di 120.000 m^2 campus
- 4° Istiuto Metrologico Europeo (dipendenti/bilancio)
- 5° Ente Pubblico di Ricerca in Italia (vigilato dal MUR)
- Attivo nella Scienza e Tecnologia Quantistica
- Forte legame con l'Università e con l'Industria

INRiM
ISTITUTO NAZIONALE
DI RICERCA METROLOGICA



Tre Divisioni Scientifiche

Metrologia Applicata e Ingegneria

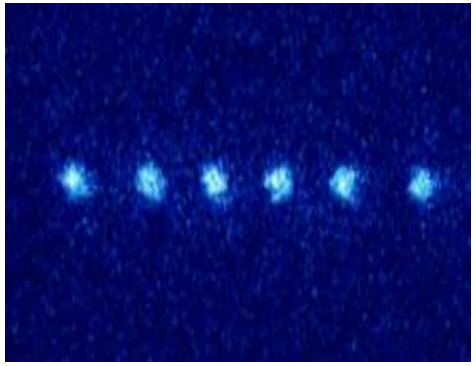
Materiali Avanzati e Scienze della Vita

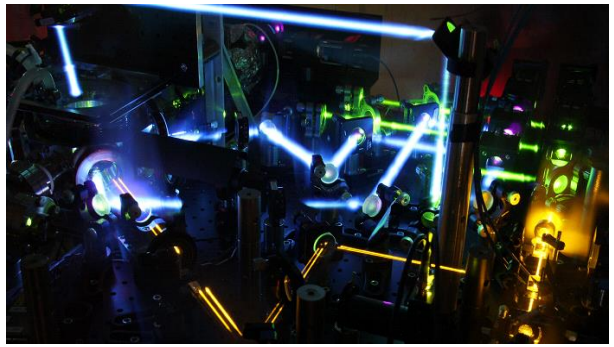
Metrologia Quantistica e Nanotecnologia

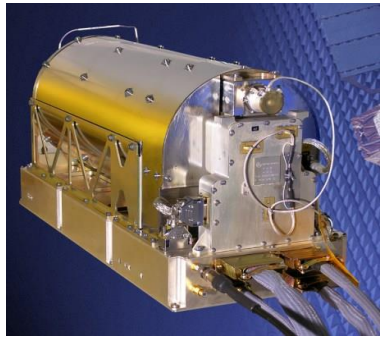
INRiM
ISTITUTO NAZIONALE
DI RICERCA METROLOGICA

Piattaforme di Metrologia Avanzata con atomi e fotoni

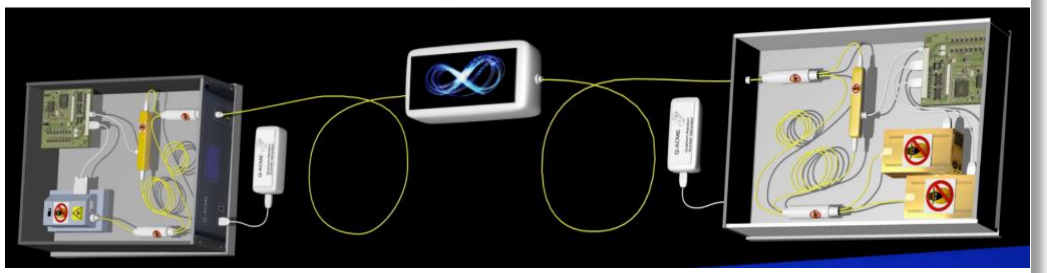
QT e atomi

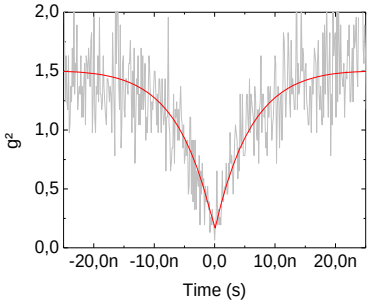


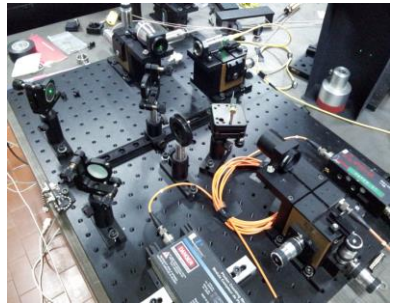


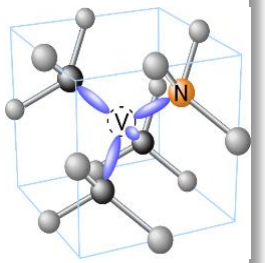


QT a singolo fotone









Quantum Metrology e Sicurezza: Sincronizzazione

Quantum Metrology e Sicurezza: Comunicazione

INRiM
ISTITUTO NAZIONALE
DI RICERCA METROLOGICA

Piemonte Quantum Enabling Technology: il nuovo laboratorio QTech

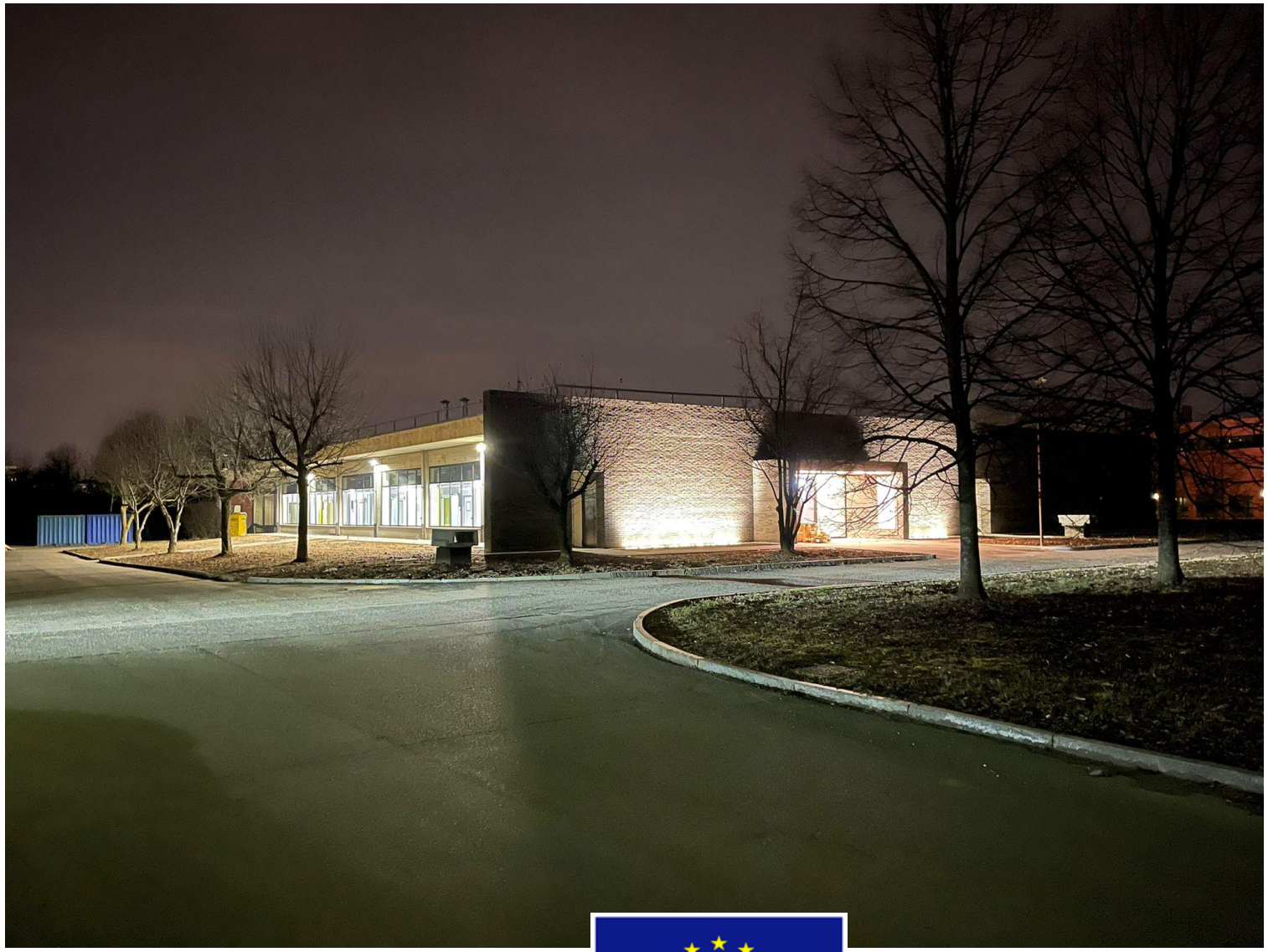
PIQUET
PIEMONTE QUANTUM ENABLING TECHNOLOGY

REGIONE PIEMONTE

INRiM
ISTITUTO NAZIONALE
DI RICERCA METROLOGICA

Politecnico di Torino

UNIVERSITÀ
DEGLI STUDI
DI TORINO



POR Piemonte
FESR 2014/2020

PIQUET: MISSIONE

RICERCA DI FRONTIERA E RI NETWORK

KNOWLEDGE TRANSFER

FORMAZIONE

PiQuET nuovo laboratorio (500 m2 di camera pulita) abilita nuove linee di ricerca nell'area dei dispostitivi con un'infrastruttura integrata, che mette insieme **metrologia, nanofabbricazione e tecnologia quantistica**, in un ambiente di metrologi, professionalità stem e **partner industriali**.

PIQUET
PIEMONTE QUANTUM ENABLING TECHNOLOGY

It-fab
The Italian Network for Micro and Nano Fabrication

INRiM
ISTITUTO NAZIONALE DI RICERCA METROLOGICA

Italian Quantum Backbone: tecnologie quantistiche in campo

Infrastruttura di Ricerca con 1850 km di fibra ottica dedicata a

- **Distribuzione del Tempo**
- **Tecnologie Quantistiche**
- **QKD**
- Radioastronomia
- Sismologia
- Fisica Fondamentale
- Spazio – Galileo

Realizzata e gestita da INRIM

Aperta a gruppi di ricerca nazionali/internazionali

Q-Tech TRL da 2 fino a 5/6 + servizi tempo e frequenza

Collabora con 7 Centri di Ricerca (CNR / INAF / ASI) e con 6 Partner Industriali

(Thales Alenia Space Italy / Telespazio/ Lenardo/ Consorzio GARR / Consortium Top-IX / Telsy /OpenFiber)

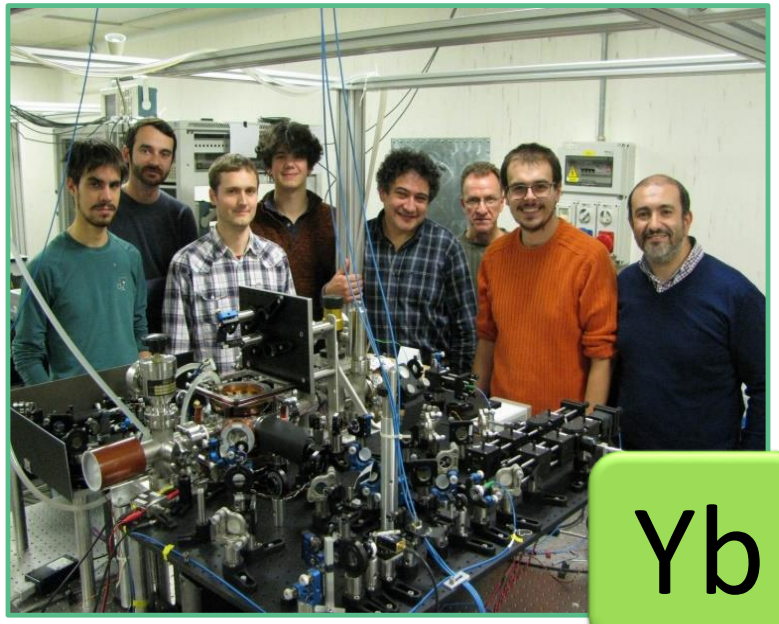
INRiM
ISTITUTO NAZIONALE
DI RICERCA METROLOGICA

INRIM 2022: campioni quantistici di frequenza

- Realizzano lo standard di tempo italiano e internazionale UTC nella Convenzione del Metro
- Accuratezza e Stabilità
- Applicazioni in Scienze fondamentali e Industria

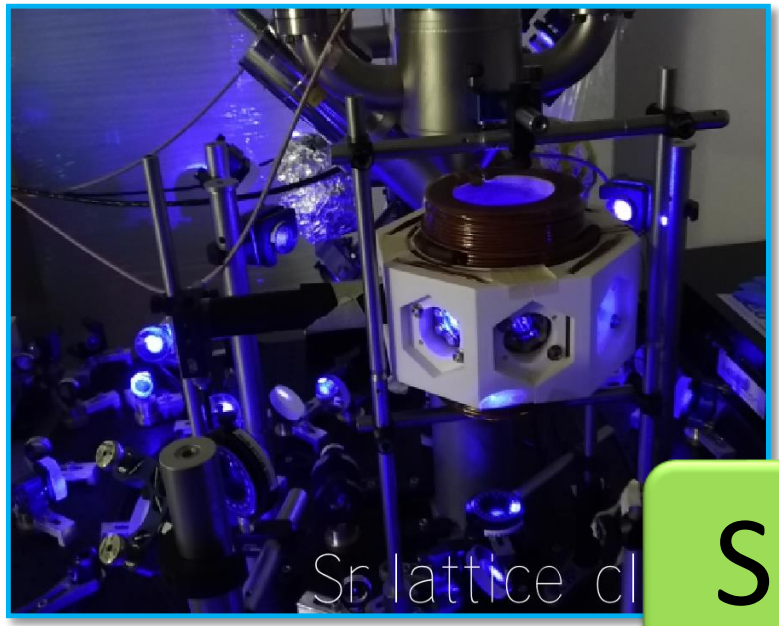
Cs

F. Levi, et al., Metrologia (2014)



Yb

M. Pizzocaro, et al., Nat Phys (2021)



Sr

M. Barbiero, et al., Phys Rev D (2020)

INRiM
ISTITUTO NAZIONALE
DI RICERCA METROLOGICA

Sistema di Navigazione Satellitare Galileo: Sincronizzazione con UTC

- Galileo ha bisogno di sincronizzarsi con lo standard internazionale di tempo UTC
- A Torino gli orologi atomici di INRIM generano una realizzazione di UTC, UTC(IT)
- Con Italian Quantum Backbone INRIM trasferisce UTC al teleporto dove ha sede centro di tempo di Galileo in Italia
- **Accuratezza, Resilienza, Aumento della Sicurezza**

INRiM
ISTITUTO NAZIONALE
DI RICERCA METROLOGICA

Sistema di Navigazione Satellitare Galileo: Sincronizzazione con UTC

INRIM Collega tramite IQB siti di

ASI, Leonardo

Thales Alenia Space e Telespazio

Legati al progetto Galileo

White Rabbit Precison Time for Industry (2018- 2021)

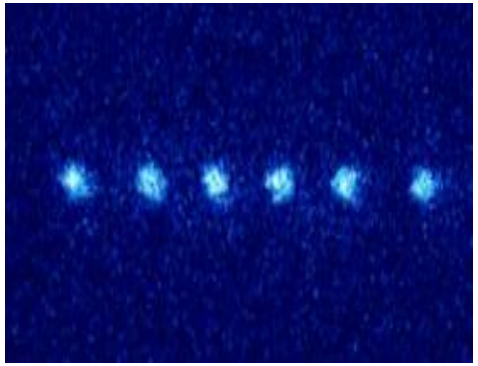
The EMPIR initiative is co-funded by the European Union's Horizon 2020 research and innovation programme and the EMPIR Participating States

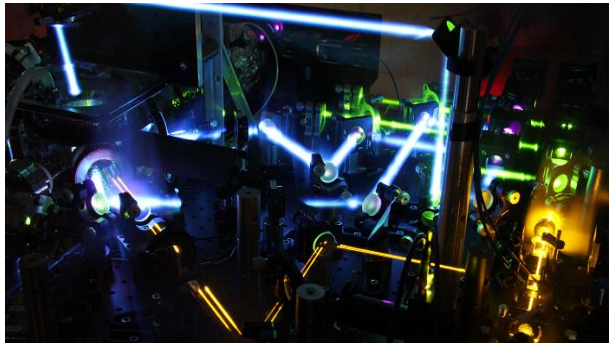
Ricerca sul protocollo White Rabbit -PTP per metrologiua primaria e per l'industria
(Tecniche di taratura / Resilienza e Ridondanza / Prestazioni migliorate / dimostrazioni in campo reale)

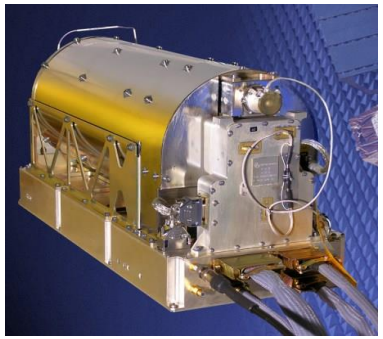
11 partners, Coordinazione: D. Calonico, INRIM

Piattaforme di Metrologia Avanzata con atomi e fotoni

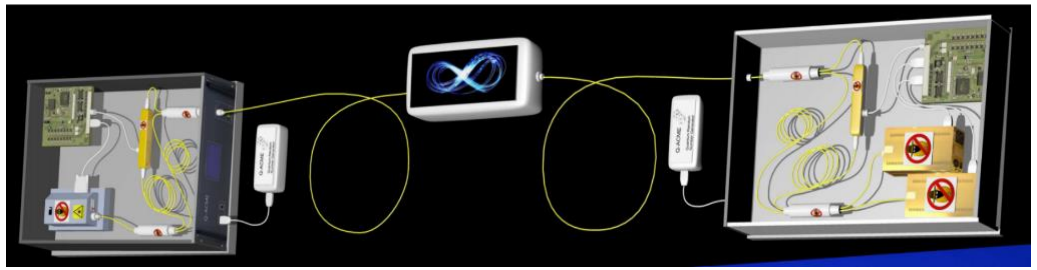
QT e atomi

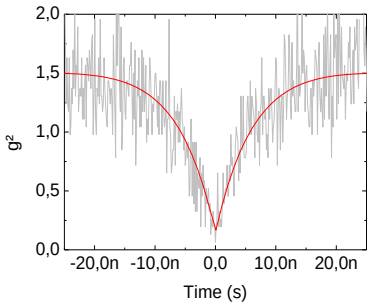


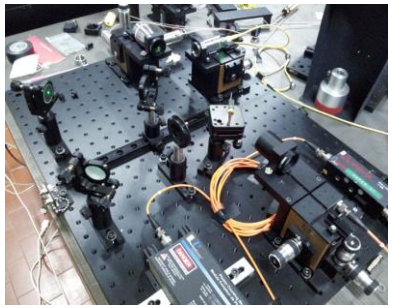


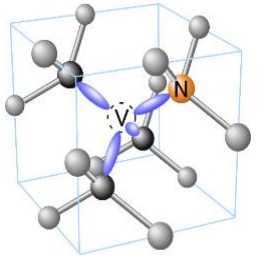


QT a singolo fotone









INRiM
ISTITUTO NAZIONALE
DI RICERCA METROLOGICA

CRITTOGRAFIA CLASSICA

Crittografia: insieme di tecniche per rendere un messaggio **non comprensibile/intelligibile** a persone non autorizzate a leggerlo, garantendo così il requisito di **confidenzialità o riservatezza** tipico della sicurezza informatica.

La crittografia si basa su un **algoritmo** e su una **chiave crittografica**

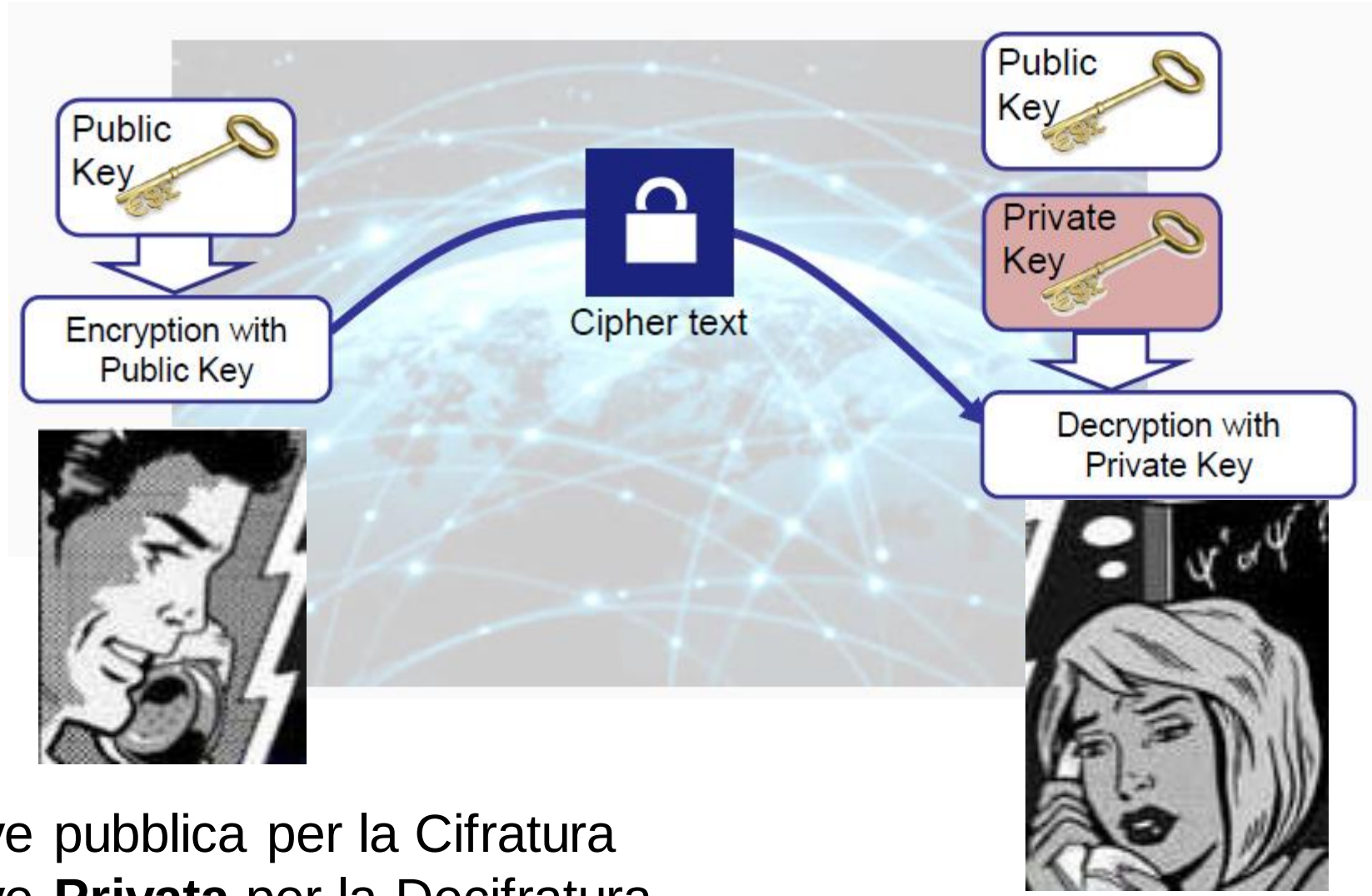
Tecniche Crittografiche Moderne:

Crittografia Asimmetrica o a **Chiave Pubblica** (Public-Key)
(ad es. RSA-Rivest, Shamir, Adleman)

Crittografia Simmetrica
(ad es. AES-Advanced Encryption Standard)

INRiM ISTITUTO NAZIONALE DI RICERCA METROLOGICA

CRITTOGRAFIA A CHIAVE PUBBLICA



Chiave pubblica per la Cifratura
Chiave **Privata** per la Decifratura

CRITTOGRAFIA SIMMETRICA

Crittografia Simmetrica (o a Chiave PRIVATA)

- Sicurezza assoluta
  (one-time-pad: *dimostrato da Shannon nel 1947*)
- Poco pratica: Alice e Bob devono avere una nuova **chiave privata comune** per ogni comunicazione
- Problema di distribuzione della **chiave privata**: è necessario avere un canale/corriere sicuro/fidato

INRiM
ISTITUTO NAZIONALE
DI RICERCA METROLOGICA

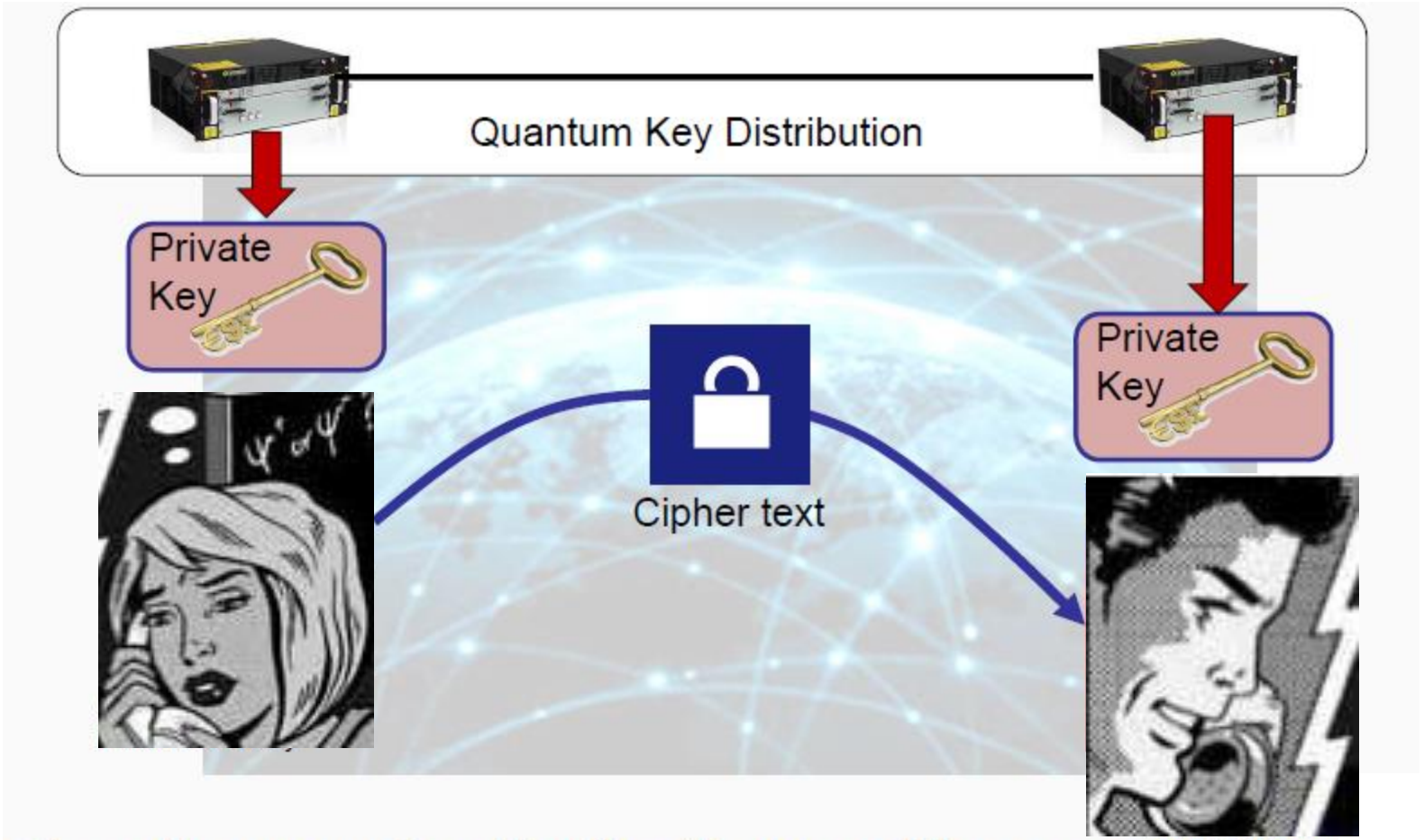
QUANTUM KEY DISTRIBUTION

Crittografia Quantistica (o Quantum Key Distribution -QKD)

- Risolve il problema di distribuzione della **chiave privata** nella crittografia simmetrica
- Genera copie di **chiavi private** identiche sfruttando fenomeni quantistici («distribuzione» di chiavi per crittografia asimmetrica)
- Distribuzione di **chiavi private** con **confidenzialità** garantita dalle **leggi della fisica**. Il **principio di indeterminazione di Heisenberg** garantisce la rivelazione di attacchi hacker al processo QKD

INRiM
ISTITUTO NAZIONALE
DI RICERCA METROLOGICA

QKD e Crittografia Simmetrica



SOLUZIONE: QKD + Crittografia Simmetrica (a chiave privata)

Sicurezza garantita dal Principio di Indeterminazione di Heisenberg a dal Teorema di Shannon (one-time-pad)

EuroQCI: European Quantum Communication Infrastructure Initiative

Search

European Commission › Strategy › Shaping Europe's digital future › News ›

Shaping Europe's digital future

DIGIBYTE | 13 June 2019

The future is quantum: EU countries plan ultra-secure communication network

INRiM nei Board della Commissione per EuroQCI

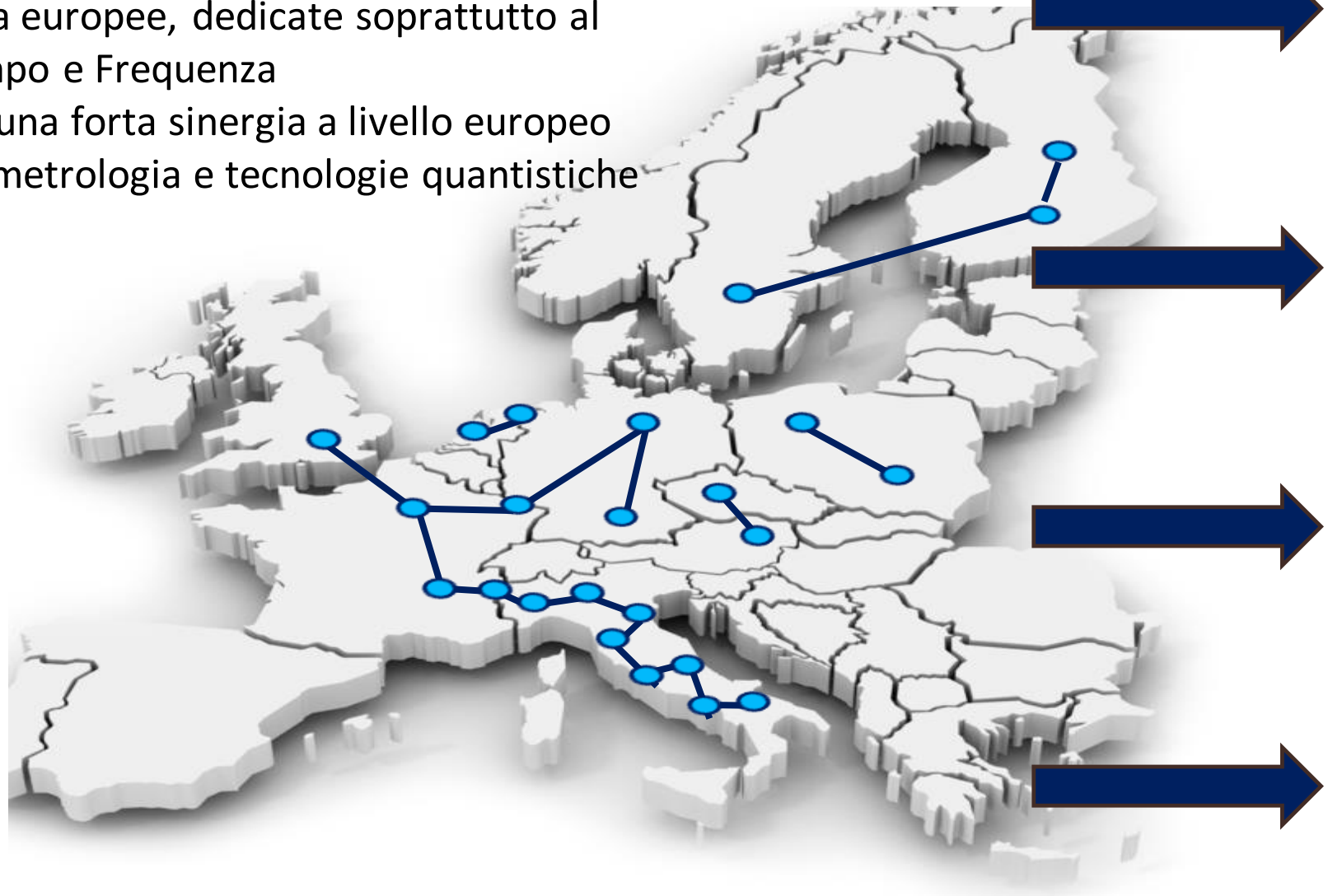
Con il progetto OQTAVO darà un contributo all'architettura dell'Infrastruttura e alla Testing&Validation Facility

AIRBUS AIRBUS CYBERSECURITY orange LEONARDO TELESPAZIO a LEONARDO and THALES company INRiM ISTITUTO NAZIONALE DI RICERCA METROLOGICA Consiglio Nazionale delle Ricerche IFC - Istituto di Fisiologia Clinica pwc &tav

INRiM ISTITUTO NAZIONALE DI RICERCA METROLOGICA

IQB , Metrologia e QT in Europa

- IQB si collega ad altre infrastrutture in fibra europee, dedicate soprattutto al Tempo e Frequenza
- C'è una forta sinergia a livello europeo tra metrologia e tecnologie quantistiche



SI

Commissione Europea

EURAMET

INRIM / European Metrology Network su Quantum Technology

Coordinatore Ivo Degiovanni, INRIM

INRIM coordina lo European Metrology Network sulle Tecnologie Quantistiche

Vision: **EMN-Q vuole essere il punto di riferimento in Europa per la metrologia in quest'area.**

Rationale

- **Allineare la metrologia continentale alle richieste industriali, alla EC Quantum Technologies Flagship,** ai programme sulle QT a livello nazionale e internazionale
- **Contribuire allo sviluppo dell QT** attraverso la ricerca e l'innovazione degli istituti metrologici
- **Contribuire alla standardizzazione e certificazione delle QT**
- **Promuovere i benefici della metrologia verso questi stakeholder.**

A oggi, EMN-Q è compost da **18 Partner in EURAMET** da 15 stati.

Quantum Communication: tecnologie italiane in campo (in progress)

Iniziative pubbliche Quantum Communication:
Regione Lombardia/ Politecnico di Milano
Regione Friuli Venezia Giulia / Università di Trieste / CNR
Regione Abruzzo / Università L'Aquila
Regione Piemonte / CSI / Top-IX / INRIM

Iniziative aziende italiane (GI):
Italtel
Leonardo
Telespazio
Thales Alenia Space
Tim
Telsy

Iniziative PMI (apparati):
Cohaerentia
QTI
Think Quantum

Iniziative Enti Pubblici di Ricerca:
ASI
CNR
INRIM

INRiM
ISTITUTO NAZIONALE
DI RICERCA METROLOGICA

INRIM - QKD in campo

1. Test Torino-Santhià Inter-MAN (100 km, -30 dB)
Fatto

2. Metropolitan Area Network a Firenze (17 km, -10 dB)
Fatto – Collaborazione CNR

3. MAN in Turin Area: in progress

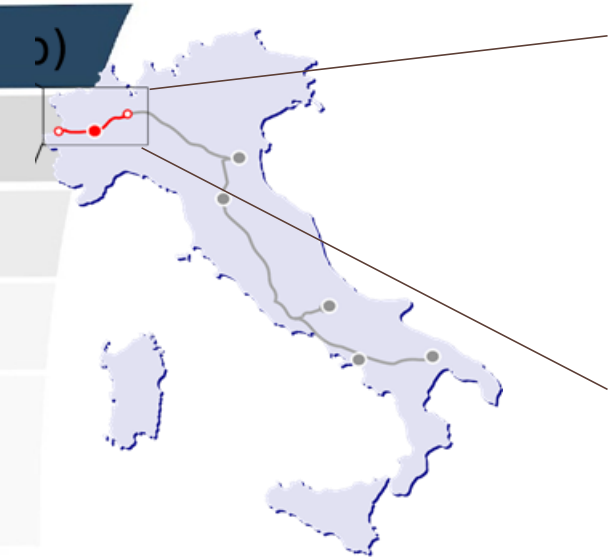
4. Interoperation Space-Ground in Matera : in progress (con ASI)

5. Cavi sottomarini: Malta-Sicilia
Fatto / follow up

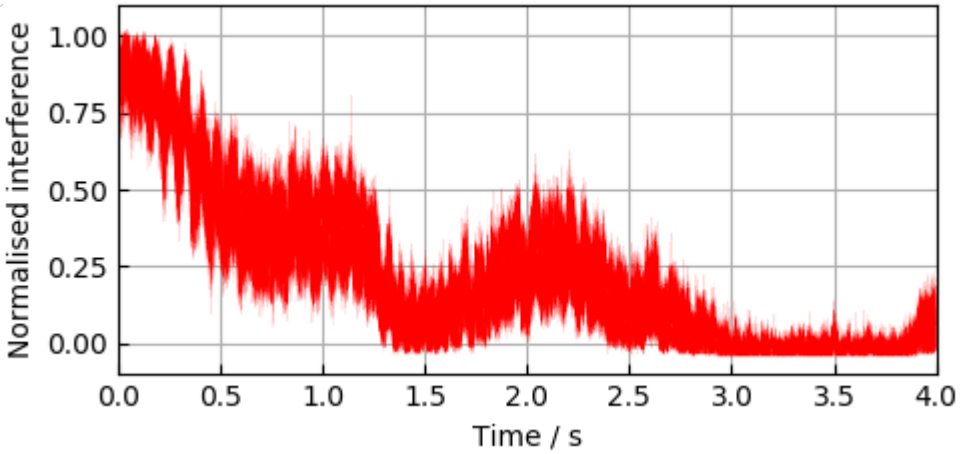
6. QKD a Lunga Distanza QKD: Trusted Node / TF-QKD (>200km)
Fatto/ follow up

INRiM
ISTITUTO NAZIONALE
DI RICERCA METROLOGICA

IQB e interferometria laser per TF-QKD



Set up reale, 200 km, 65 dB di perdita



Traccia di interferometria laser della TF-QKD

Twin-field QKD è una tecnica di QKD che permette un **aumento significativo della distanza** permessa tra Alice e Bob e **riduce il numero dei critici Trusted Nodes**

INRIM usa IQB, i propri laser ultrastabili e le tecniche di interferometria laser di uso metrologico e applica la TF-QKD (200 km, 65 dB di perdita)

Il risultato è stato un **miglioramento di 100 volte delle qualità operative della TF-QKD** (tempi di riallineamento) e **di 20 volte del QBER potenziale** dimostrando che la TDF-QKD è realizzabile in set-up reali

C. Clivati et al. , Nature Communications 13,157 (2022)

top-ix WE DO CONNECTIONS

INRiM ISTITUTO NAZIONALE DI RICERCA METROLOGICA

Standardizzazione della QKD

INRIM membro dell'**Industry Specification Group (ISG) of the European Telecommunications Standards Institute (ETSI) ISG/ETSI**
Per sviluppare la standardizzazione della QKD

INRIM membro del CEN/CLC FGQT, Focus Group sulle necessità di standardization delle Quantum Technologies.

Metrologia per la verifica della sicurezza dell'hw QKD

INRIM coordina il progetto METISQ, per lo sviluppo di misure riferite al SI per caratterizzare sistemi QKD seguendo l'elaborazione di ETSI ISG QKD.

19NRM06 MeTISQ

Metrology for Testing the Implementation Security of Quantum Key Distribution Hardware

(2020- 2024)

EMPIR
The EMPIR initiative is co-funded by the European Union's Horizon 2020 research and innovation programme and the EMPIR Participating States

Sviluppo della metrologia per caratterizzazioni a livello del singolo fotone di sistemi e apparati quantum key distribution (QKD) - trasmettitori, ricevitori, e componeneti – in cooperazione con la stadnardizzazione in ETSI.

12 partners, Coordination: M. Gramegna, INRIM

SVILUPPO DI SISTEMI E TECNOLOGIE QUANTISTICHE PER LA SICUREZZA INFORMATICA IN RETI DI COMUNICAZIONE

QUANCOM (2021- 2024)

UNIONE EUROPEA
Fondo Europeo di Sviluppo Regionale

Ministero dell'Istruzione, dell'Università e della Ricerca

PON RICERCA E INNOVAZIONE 2014 - 2020

Il Progetto QUANCOM si propone di supportare lo sviluppo e la sperimentazione di protezione incondizionata della rete IP sfruttando la crittografia quantistica.

7 partners

Consiglio Nazionale delle Ricerche

INRiM ISTITUTO NAZIONALE DI RICERCA METROLOGICA

ASI Agenzia Spaziale Italiana

UNIVERSITÀ DEGLI STUDI DI PADOVA

demetriX

MEMORY CONSULT Consulenza Aziendale

exprivia

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Progetto Cybersecurity 4.0
“Quantum Communication and Synchronization Testbed”

Prototipo di infrastruttura di comunicazione e sincronizzazione sicura basata su distribuzione quantistica delle chiavi crittografiche.

ThalesAlenia Space
a Thales / Leonardo company

TELESPAZIO
a LEONARDO and THALES company

INRiM
ISTITUTO NAZIONALE
DI RICERCA METROLOGICA

SAPIENZA
UNIVERSITÀ DI ROMA

Conclusioni

- Italia: eccellenza scientifica e industriale nelle Tecnologie Quantistiche
- INRIM e il Piemonte ne sono parte attiva (metrologia e comunicazione quantistica)
- La cybersecurity ha nel quantum un asset importante di potenziamento
- Forte interazione Pubblico - Privato
- Parte attiva della comunità quantistica europea (i.e. EuroQCI)

Grazie per l'attenzione

European Commission

EURAMET

MUR
Ministero dell'Università e della Ricerca

REGIONE PIEMONTE

INRiM
ISTITUTO NAZIONALE DI RICERCA METROLOGICA