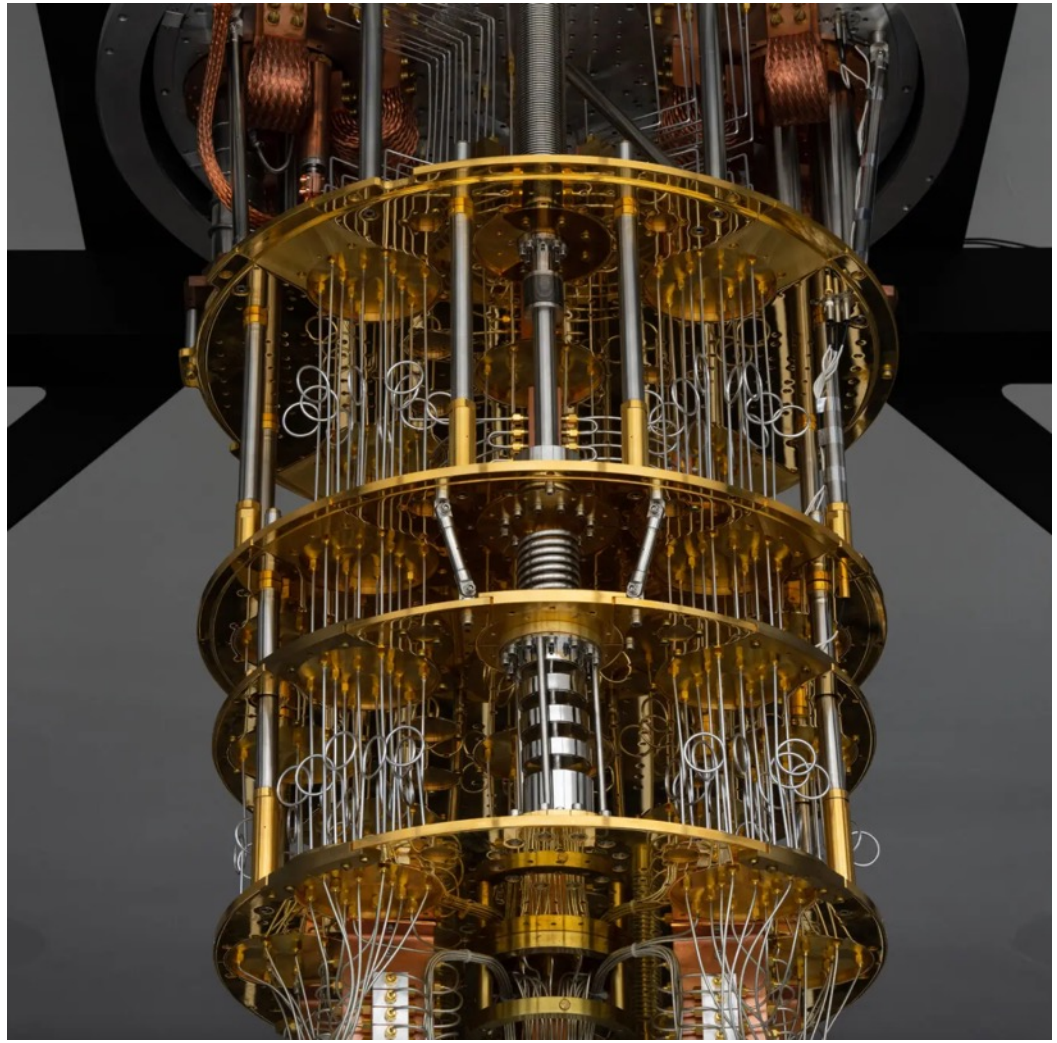
LE SFIDE DEL QUANTUM COMPUTING

Alessandro Zavatta

Banche e Sicurezza 2024 XXI edizione, 14 maggio, Milano

I computer quantistici

I computer quantistici sono in grado di rompere con discreta facilità la complessità computazionale della crittografia classica (RSA), imponendo alle organizzazioni pubbliche e private di correre ai ripari e sviluppare soluzioni di risposta efficaci.

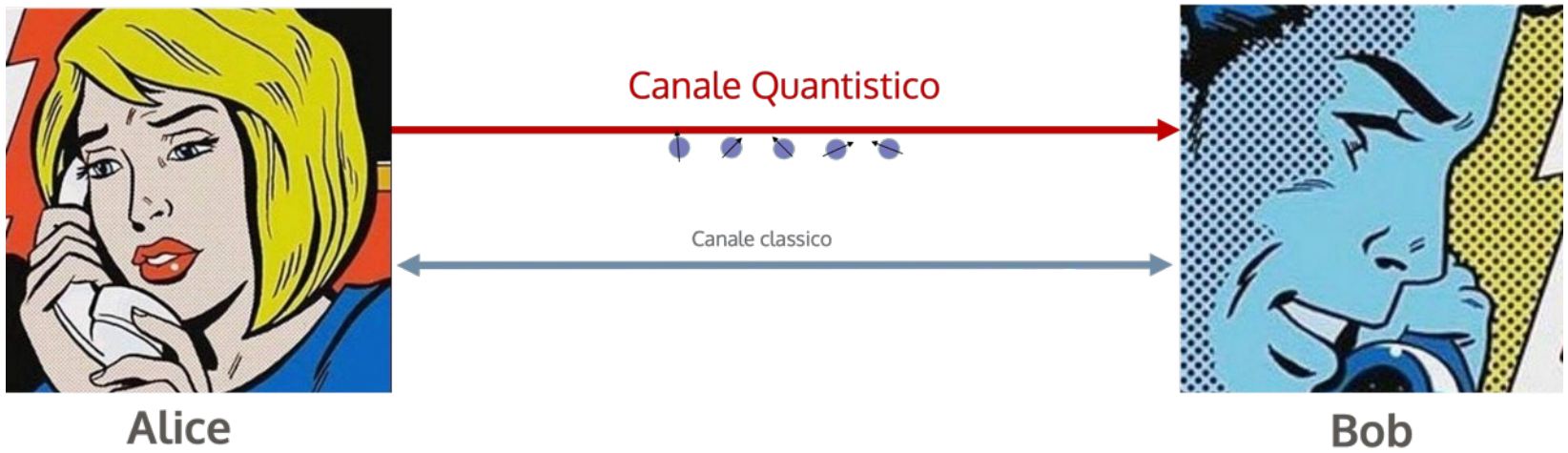


Comunicazione quantistica

La comunicazione quantistica sfrutta le stesse leggi della fisica per proteggere le comunicazioni.

Comunicazione quantistica

I fotoni vengono utilizzati per trasmettere i dati lungo cavi in fibra ottica.



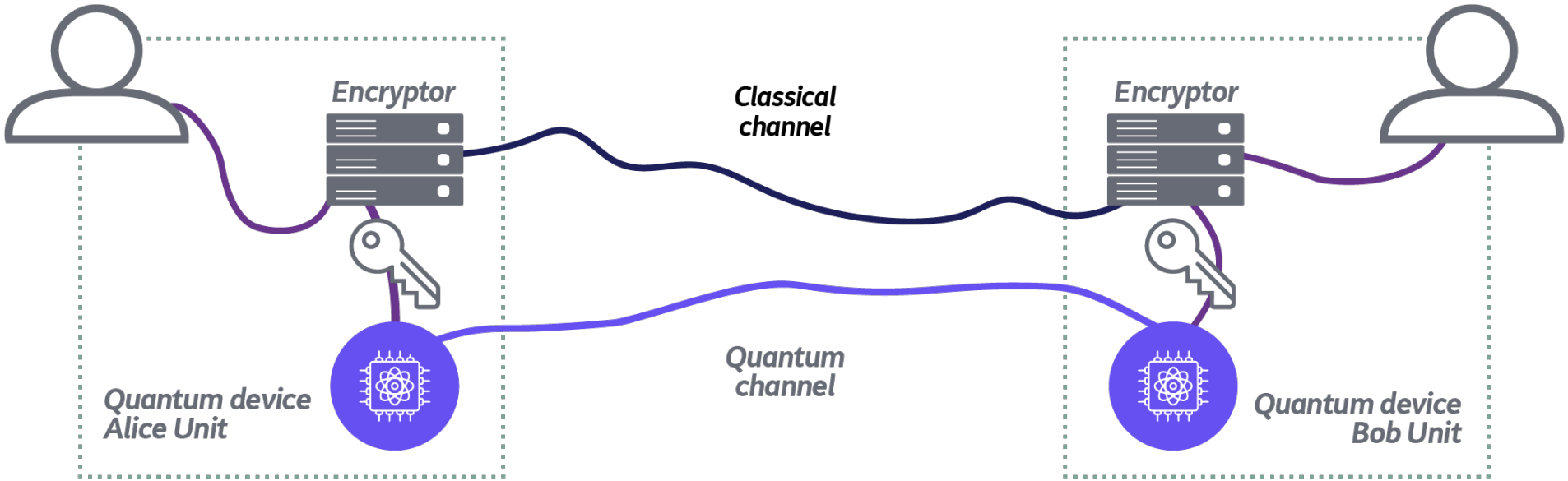
Comunicazione quantistica

Se un hacker cerca di osservare i fotoni durante il loro transito, inevitabilmente li disturberà. L'hacker non può copiare i dati trasmessi senza lasciare traccia della sua attività.

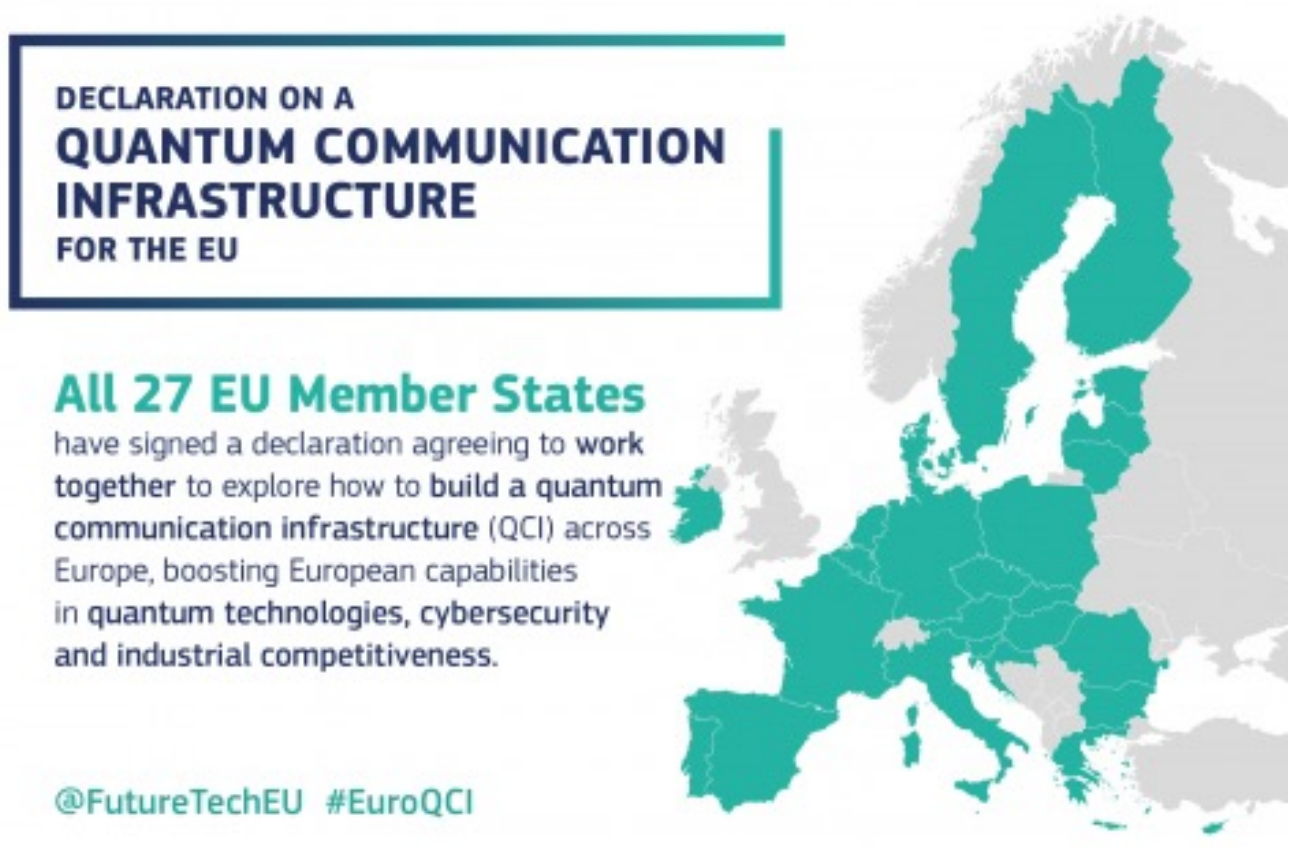
Quantum Key Distribution - QKD

QKD è un protocollo quantistico per la generazione di chiavi crittografiche simmetriche per comunicazioni ultrasicure, che consente a due (o più) utenti comunicanti di produrre e condividere una chiave segreta casuale nota solo a loro, che possono utilizzare per crittografare e decrittografare i propri messaggi.

Una proprietà unica di QKD è la capacità degli utenti comunicanti di rilevare la presenza di terzi che tentano di ottenere informazioni chiave.



EuroQCI – European Quantum Communication Infrastructure

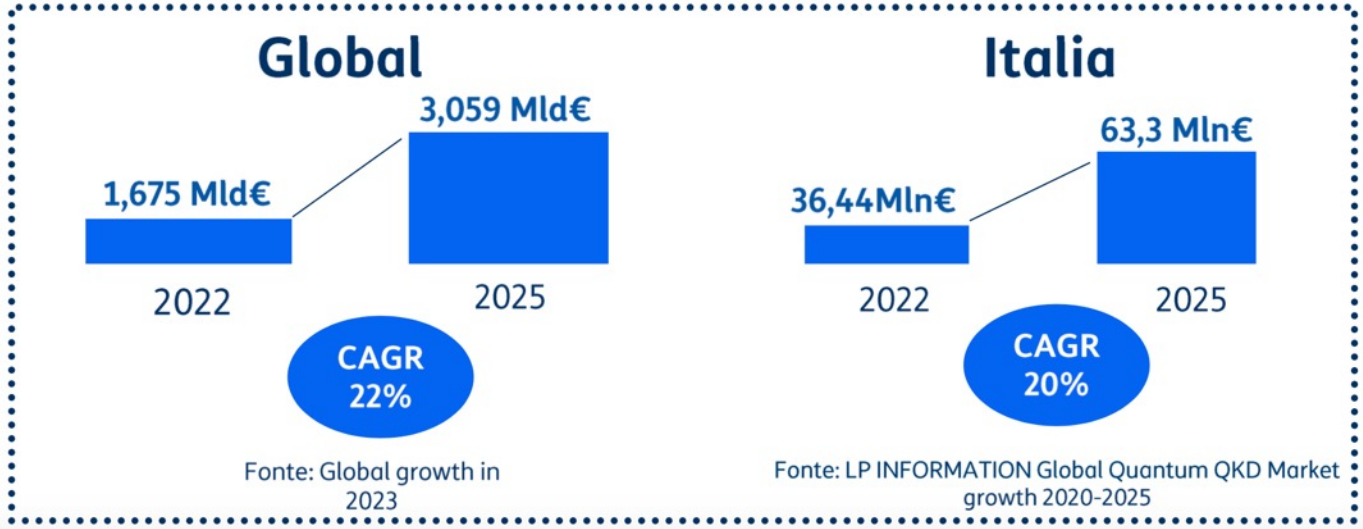


European Commission

Infrastruttura di distribuzione di chiavi quantistiche (QKD) **European Quantum Communication Infrastructure (EuroQCI)**, l'iniziativa lanciata nel 2019 dalla Commissione e dai 27EU che prevede la costruzione di un'infrastruttura di comunicazione quantistica sicura che copra tutta l'area UE, compresi i territori d'oltremare.

Mercato globale potenziale della quantum security

- **Record di investimenti nell'economia globale in tecnologie di Quantum Security.**
  Necessità di sviluppare da subito competenze e adottare soluzioni QKD in risposta alle minacce
- **Il mercato della QKD a livello Globale è stimato pari a 4,718 Mld € nel 2028.**
  L'Italia sarà uno dei Paesi a maggiore crescita e il 4° in EU per dimensione



Fonte: Global growth in 2023

Fonte: LP INFORMATION Global Quantum QKD Market growth 2020-2025

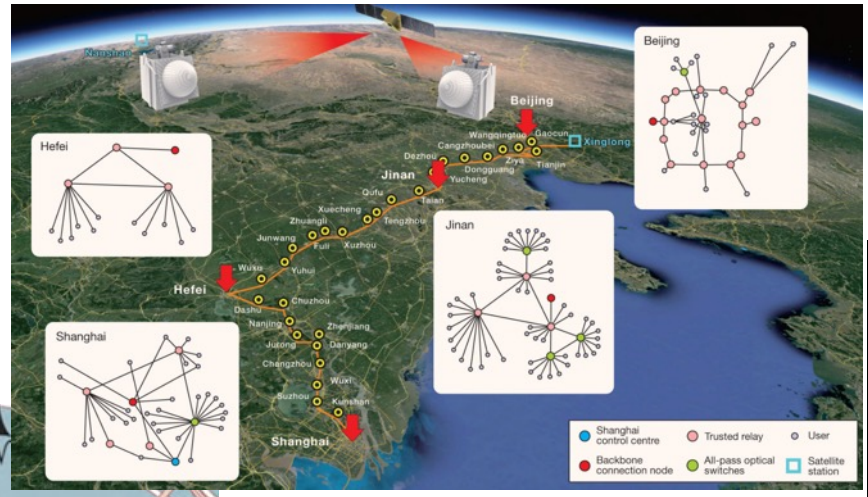
Applicazione nei diversi contesti e prospettive future

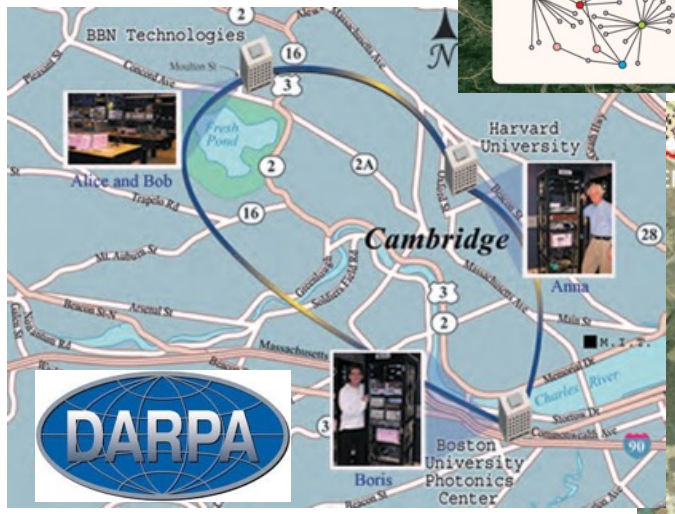
QKD – Stato dell'arte

I sistemi QKD sono pronti per essere installati in ambienti reali per un uso in ambito cripto.

QKD Metropolitan Networks:

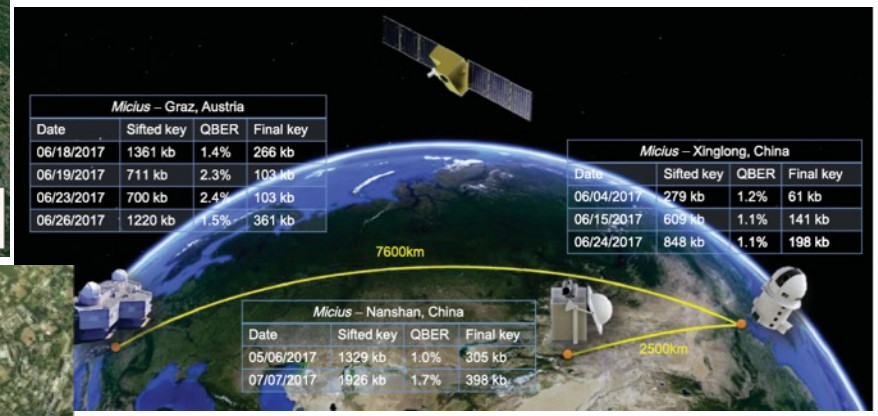
- DARPA, Boston (USA)
- *SECOQC,* Vienna (Austria)
- Geneva (Switzerland)
- Durban (South Africa)
- China
- Japan
- UK





QKD space connections:

- Da satellite a terra
- Da satellite a più stazioni di terra



Demo QKD nell'ambito del G20

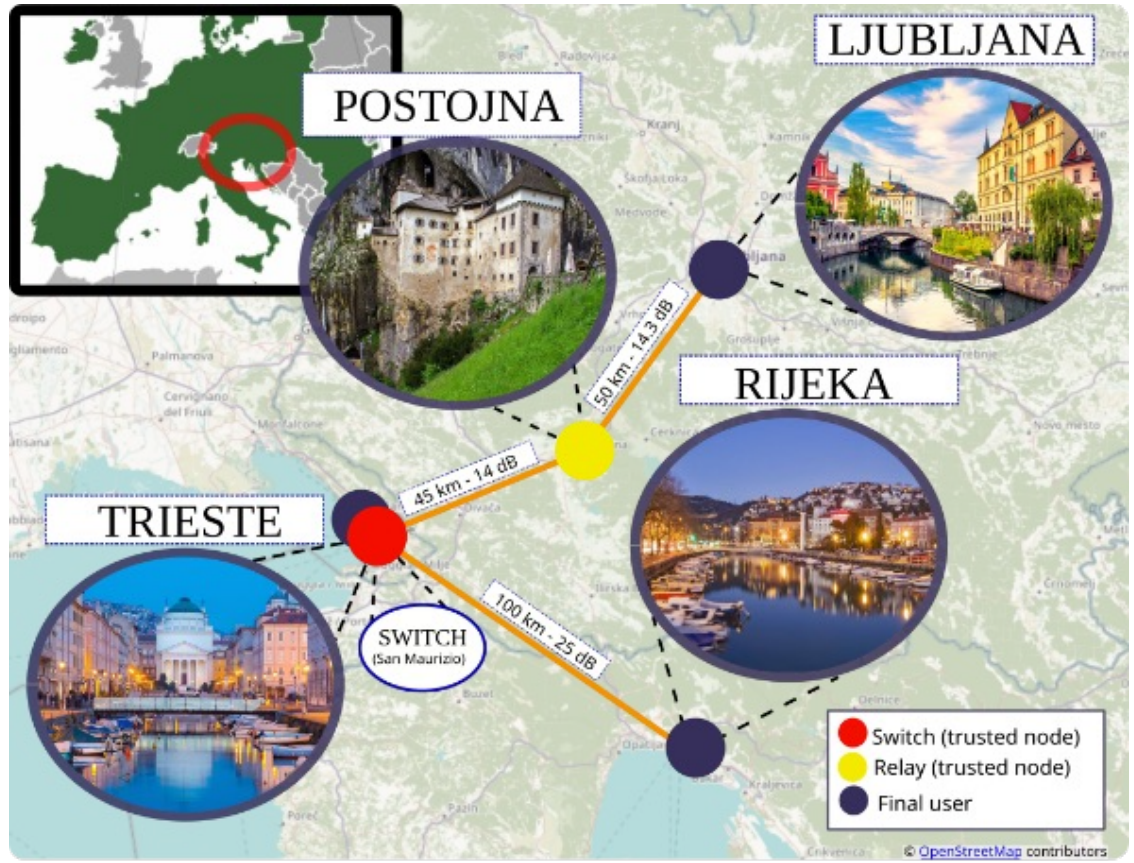
UNIVERSITÀ DEGLI STUDI DI TRIESTE

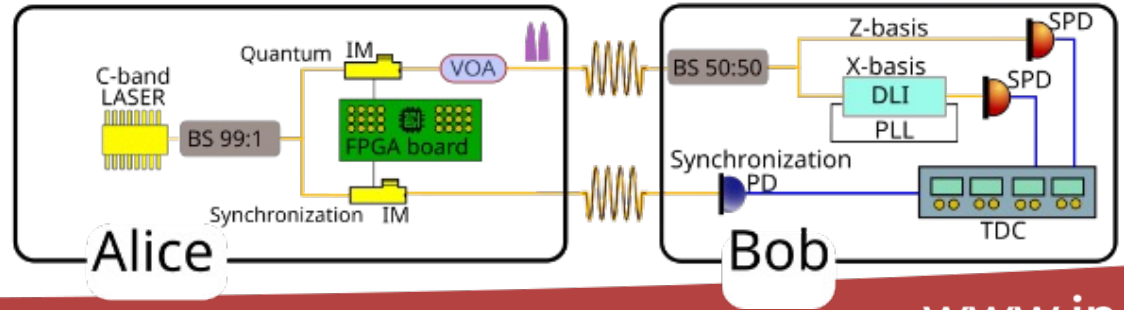
Quantum Telecommunications Italy

Prima comunicazione quantistica tra tre Paesi Europei – Italia, Slovenia and Croazia:

- Trieste – Postojna – Ljubljana (50 km + 50 km, 14 + 14.3 dB)
- Trieste – Rijeka (100 km, 25dB)

TIM SPARKLE





Società spin-Off del CNR

Quantum Telecommunications Italy

CNR-INO
ISTITUTO NAZIONALE DI OTTICA
CONSIGLIO NAZIONALE DELLE RICERCHE

Overview

Numbers

Founded in 2020

35 Team Members

4 Business divisions

5+ Financed projects

equo

QUID
QUANTUM ITALY DEPLOYMENT

Strategic Partnership

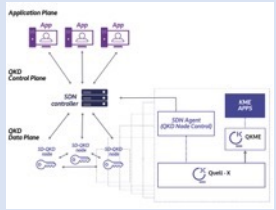
Telsy — Classical encryption provider

TIM — Telecom Operator

Products

Quell-X
Quantum Key Distribution

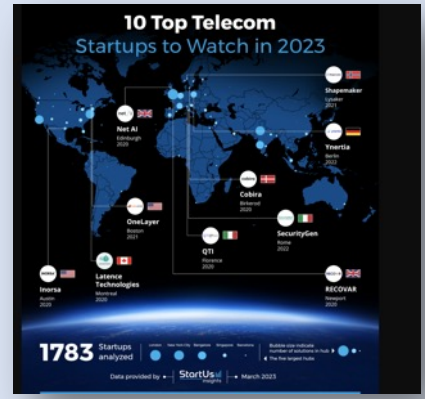
QKME
Key Management Entity



QSDN
Software Defined Network

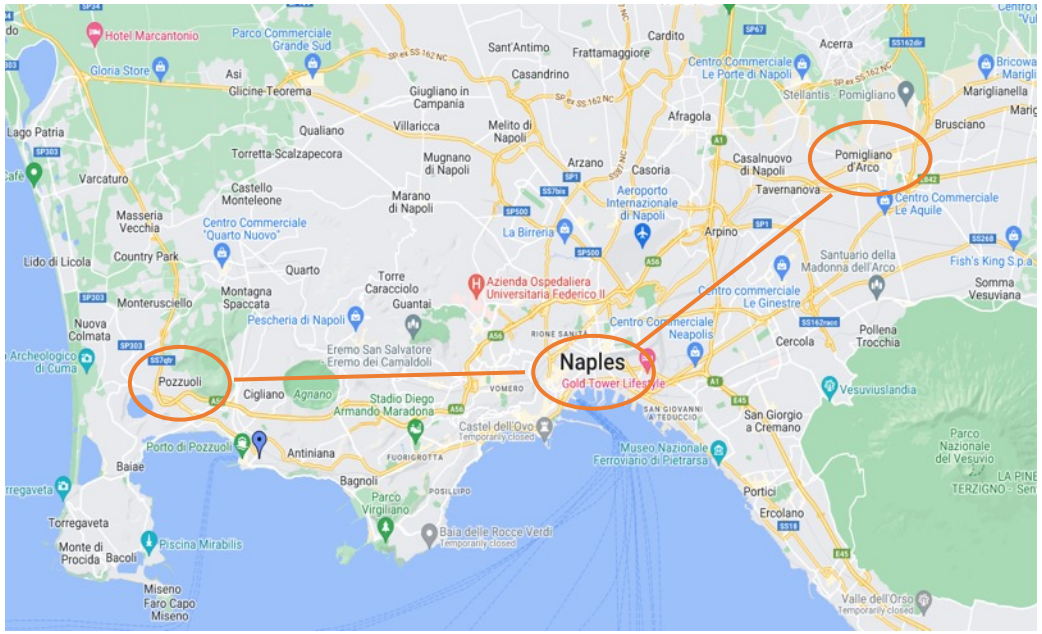
Highlights

- QKD in real world networks
- Interoperability with devices by third parties
- Multiple markets (civil, military, international)



La prima QMAN italiana a Napoli

- Inaugurazione il 25 gennaio 2024 a Napoli
- Progetto promosso Ministero delle Imprese e del Made in Italy (MiMiT)
- QMAN permanente aperta a implementazioni, test e use-case

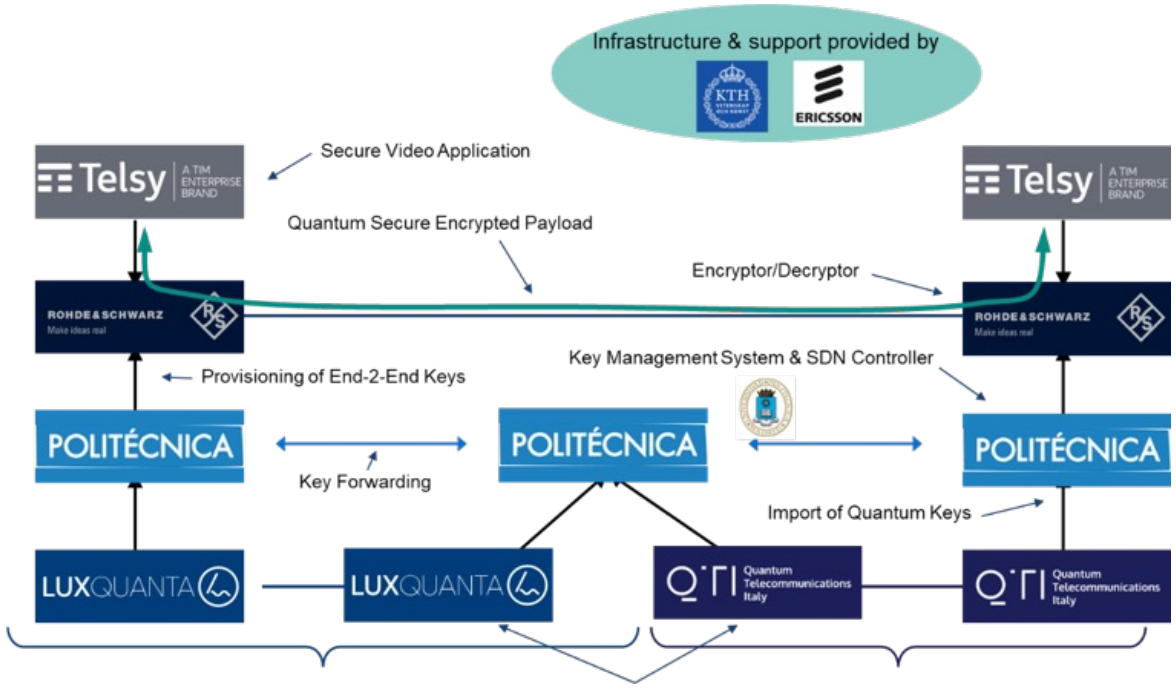


Demo QKD durante la Digital Assembly 2023

- Ospitata dalla Commissione europea e dalla Presidenza svedese del Consiglio dell'UE a Stoccolma
- Mini EuroQCI - interoperabilità tra diversi fornitori dei 27 paesi dell'UE

Participating Projects

NQCIS weden
EUROQCI SPAIN
SEQRET
equo
QUARTER
QSN PARTNERSHIP
PETRUS
TIM GRUPPO TIM



Applicazioni

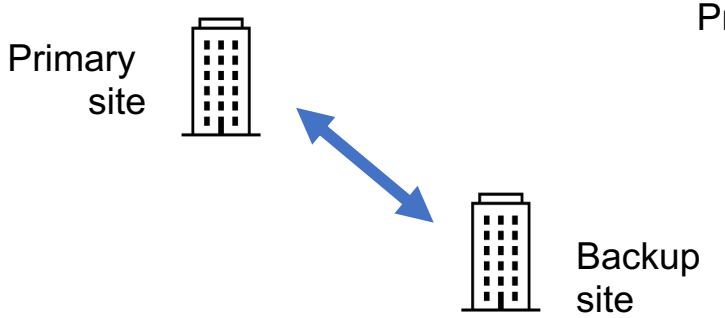
- Crypto keys distributor infrastructures
- Data center security
- Medical data protection
- National and cross-borders backbones
- Trusted nodes based long-distance key distribution
- Key distribution across advanced reconfigurable networks (star, ring, software defined networks)
- Governmental and financial data security
- Critical infrastructure security: airports, harbours, gas-distribution and power-grids distribution

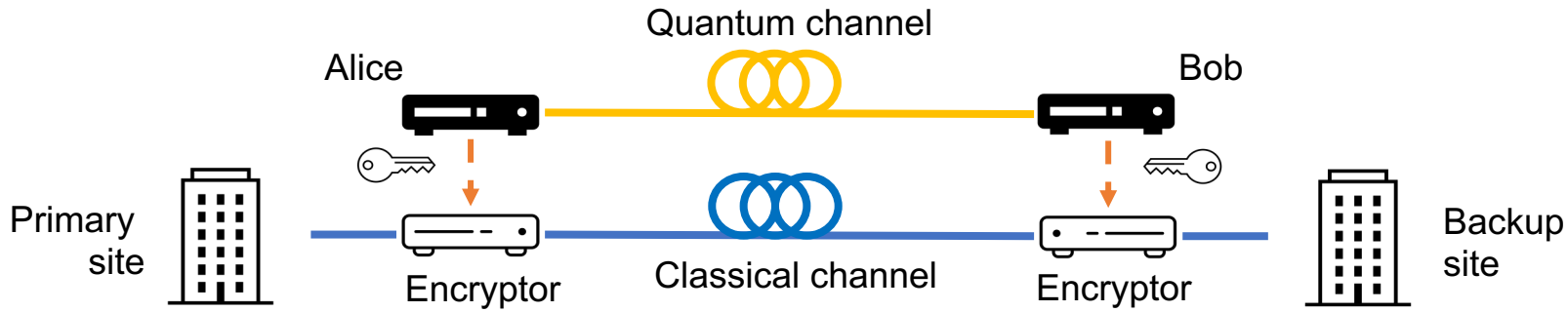
Offsite Backup / Business Continuity

Protezione dei processi e delle transazioni di backup e di altri processi di continuità operativa.

Le chiavi crittografiche vengono create e trasmesse tra il sito primario e quello secondario con un collegamento QKD e alimentate da un link encryptor che utilizza un cifrario a blocchi simmetrico per cifrare il traffico su un collegamento in fibra Ethernet.

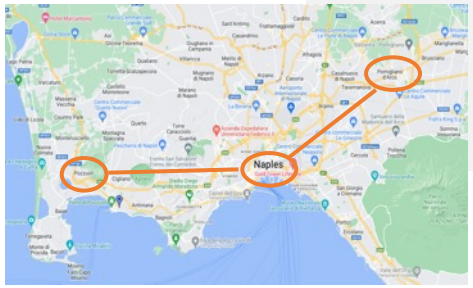
G20 in Trieste, world premiere of an "anti-hacker" quantum call





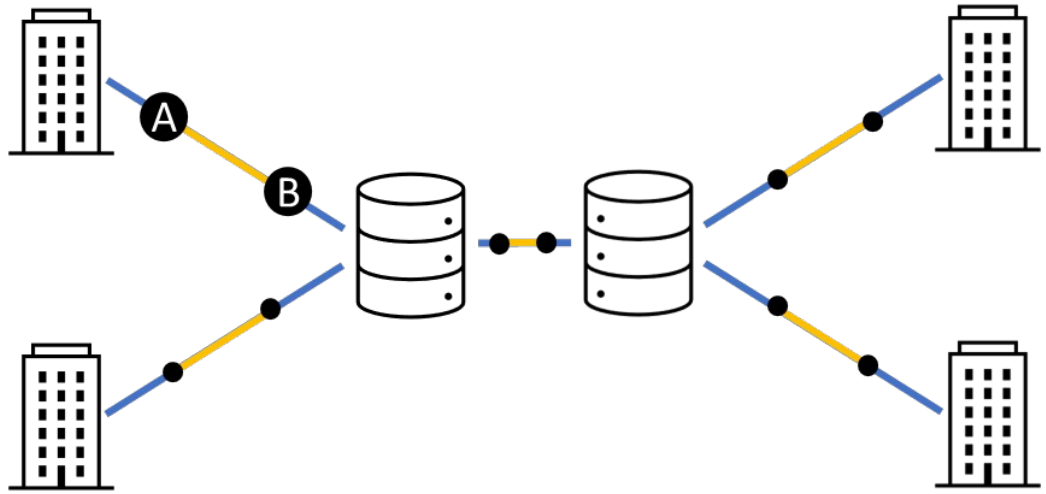
Metropolitan Area Network (MAN)

La prima QMAN italiana a Napoli



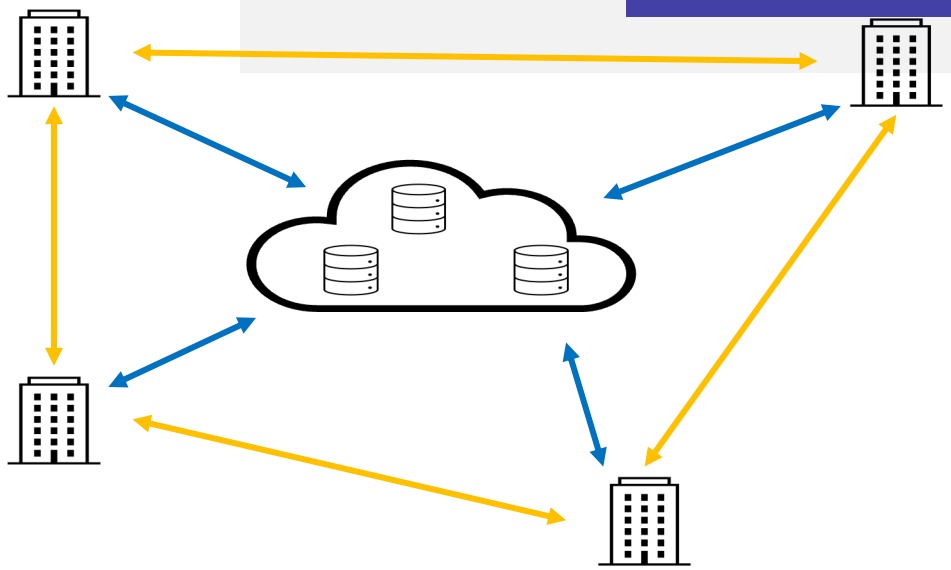
Protezione di infrastrutture e servizi nelle reti MAN aziendali.

Le chiavi crittografiche vengono create e scambiate tra le filiali dell'azienda e i data center centrali, nonché tra i data center stessi. L'azienda o l'ente governativo acquista un canale in fibra dedicato o la noleggia dal fornitore della fibra.



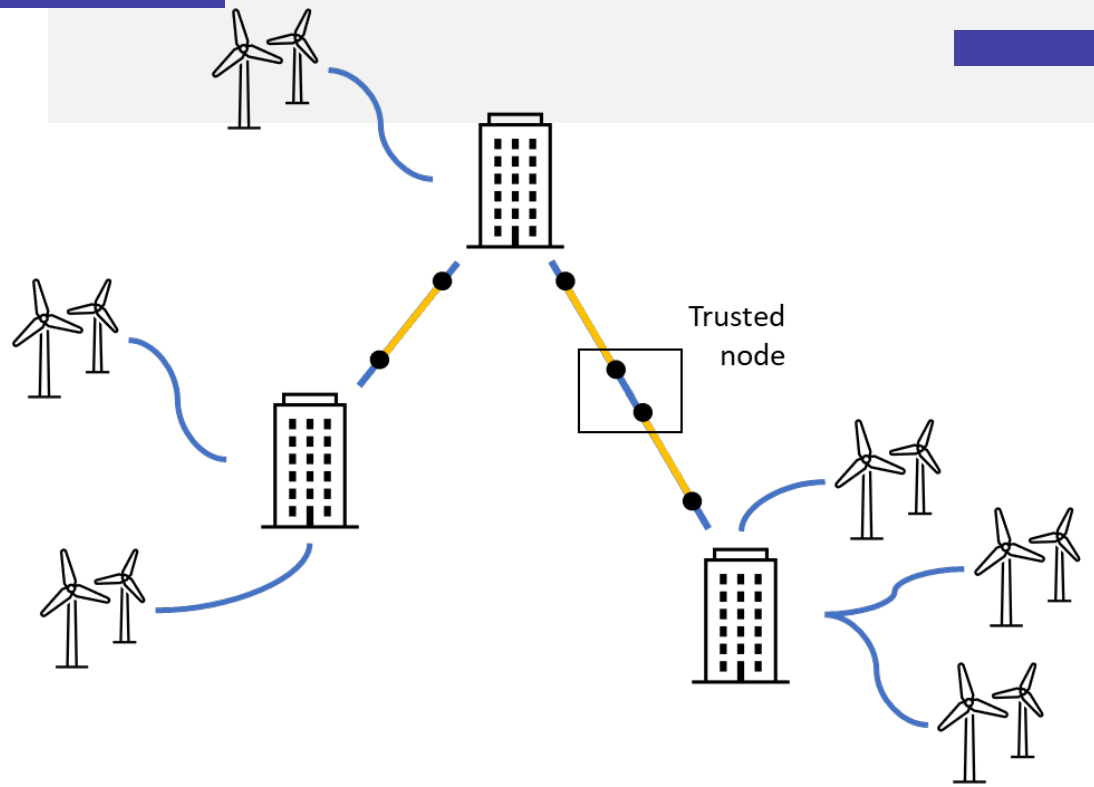
Cloud datacenters

I **data center aziendali** e istituzionali si stanno progressivamente spostando verso i **cloud pubblici** per aumentare la resilienza e la disponibilità dei dati. Tuttavia, tale attività di outsourcing dei dati comporta la necessità di crittografare i dati che viaggiano attraverso la rete.



Critical Infrastructure Control and Data Acquisition

Protezione della comunicazione in un sistema di controllo di supervisione e acquisizione dati (SCADA) di un'infrastruttura critica.



Grazie per l’attenzione