CYBERSECURITY 4.0

Il futuro della sicurezza informatica è ora

Torino | giovedì 3 marzo 2022

Quantum Security: dalla fase sperimentale agli scenari futuri

L'esperienza del CSI Piemonte e di Top-IX

Leonardo Camiciotti
TOP-IX

Pier Paolo Gruero
CSI Piemonte

Consorzio non-profit

top-ix
WE DO CONNECTIONS

MISSION

IX Gestisce e sviluppa l'Internet Exchange per il Nord-ovest Italia

DP Promuove e supporta progetti di innovazione e network intensive

COMPUTING, DATA AND NETWORK INFRASTRUCTURE

KNOWLEDGE, SKILLS, TRAINING-TO-JOB

INNOVATION

IMPACT

Il progetto

Febbraio 2021

TOP- IX e CSI hanno avviato una sperimentazione **(primo caso italiano su rete in esercizio)** allo scopo di individuare i requisiti e definire le modalità di inserimento sulla rete dell'IX regionale della tecnologia **QKD** da installare agli estremi di un link in fibra ottica.

Gli apparati sono stati messi a disposizione da Italtel e Politecnico di Milano.

top-ix
WE DO CONNECTIONS

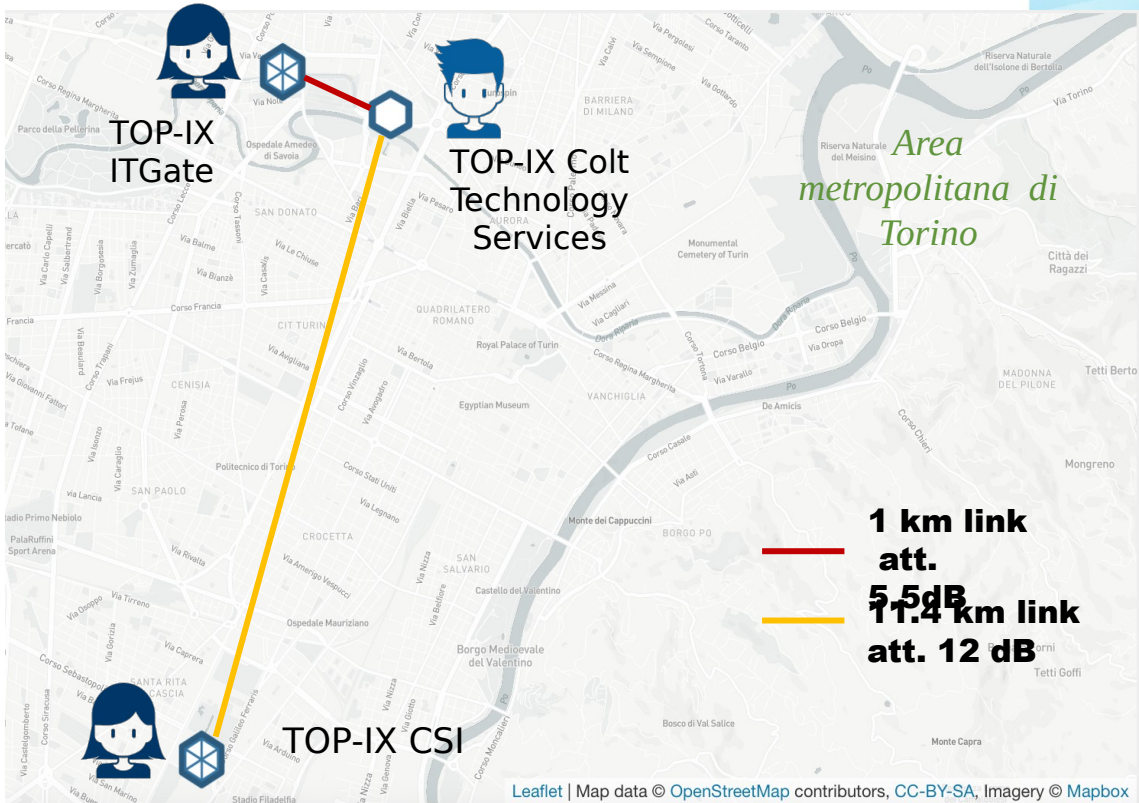
CSI
your digital partner

QKD PoC su rete dell'IX regionale

Infrastruttura

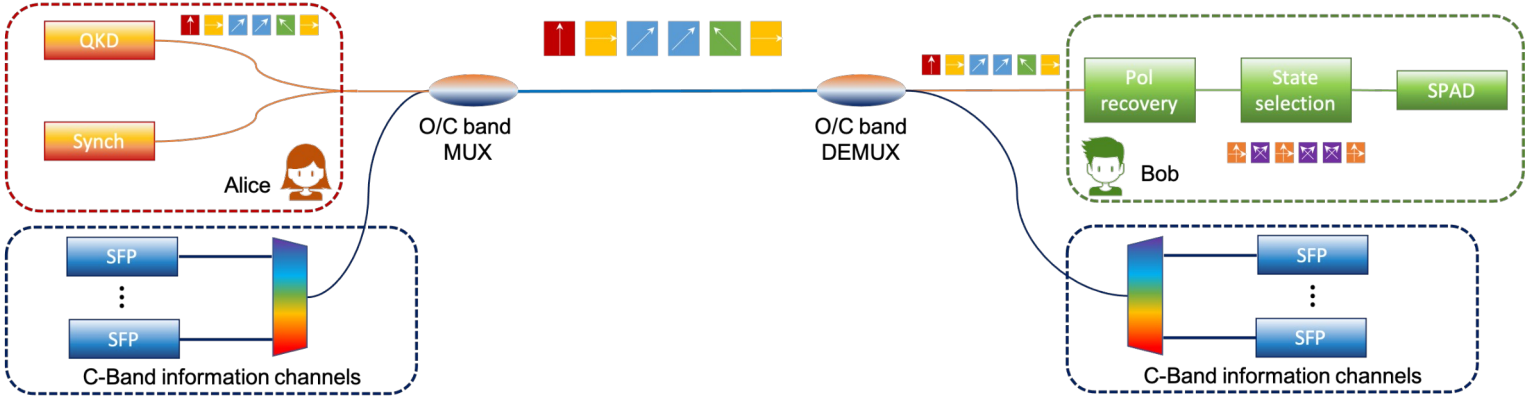
Sono stati individuati due percorsi idonei:

- **ITGATE-COLT: link breve** ideale per la verifica del funzionamento
- **CSI-COLT: link di maggiore interesse** per il fine-tuning di apparati e verifica delle prestazioni

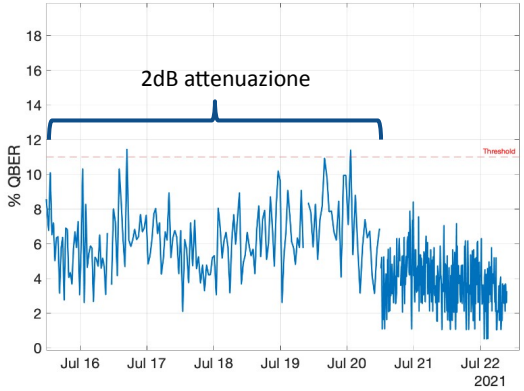


QKD PoC su rete dell'IX regionale

Prestazioni CSI-COLT



- Link DWDM attivi (2x 10Gb/s) con inserimento del segnale QKD @ 1310nm
- Soglia validazione chiave: QBER = 11%
- Perdita di 12dB: media QBER = 4%
- Perdita di 14dB: media QBER = 6%
- QBER: Quantum Bit Error Rate



I principi fondamentali

QKD si basa su alcuni principi fondamentali della meccanica quantistica, in particolare sul **principio di indeterminazione di Heisenberg** e sul **non-cloning theorem**.

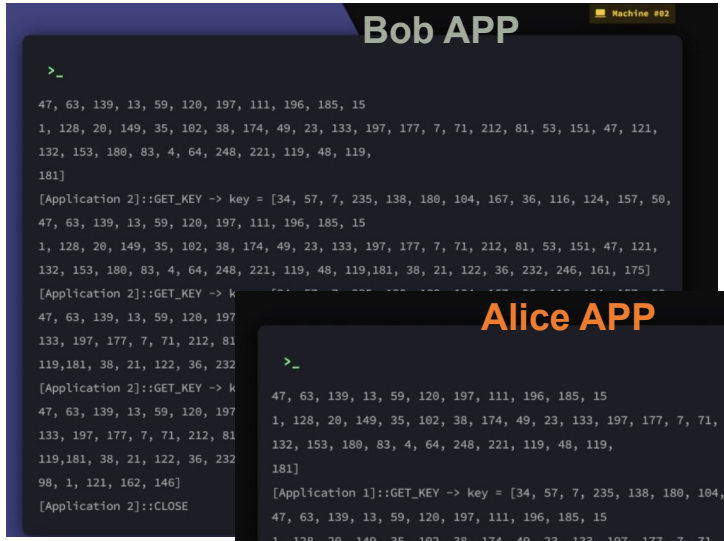
Mediante **proprietà quantistiche legate al fotone** (polarizzazione o fase) è possibile generare e distribuire chiavi simmetriche. Non si sfrutta quindi un principio matematico.

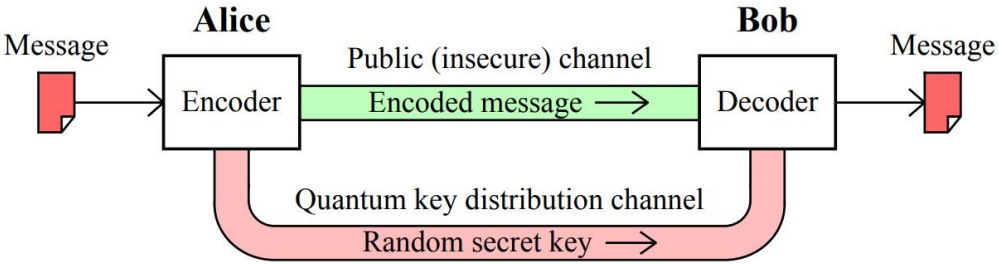
La caratteristica significativa di questa tecnologia è che **i tentativi di intercettazione possono essere rilevati**, cosa invece non possibile nelle comunicazioni convenzionali.

QKD PoC su rete dell'IX regionale

Application layer e sviluppo

- Le chiavi generate sono state utilizzate per criptare uno **scambio file tra applicativi di test installati su ambiente Cloud**.





Scenari futuri

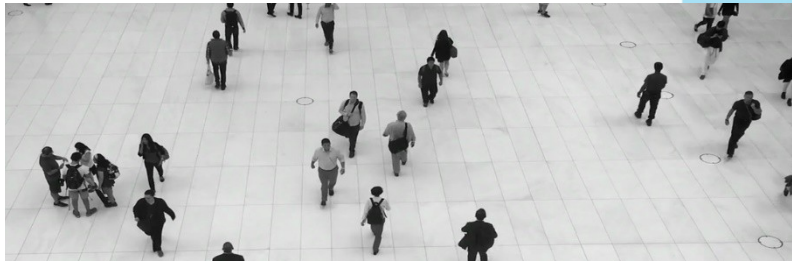
Data Spaces

aggregazioni di ecosistemi (produttivi e/o sociali) fondati su regole, strumenti e tecnologie, che permettono di condividere dati fra Enti ed Aziende e nella società civile nel pieno rispetto dei principi di sovranità, interoperabilità e fiducia.

Data Transfer Protection

Trasferimento sicuro dati «particolari» tra Data Center, tra Cloud Operator.

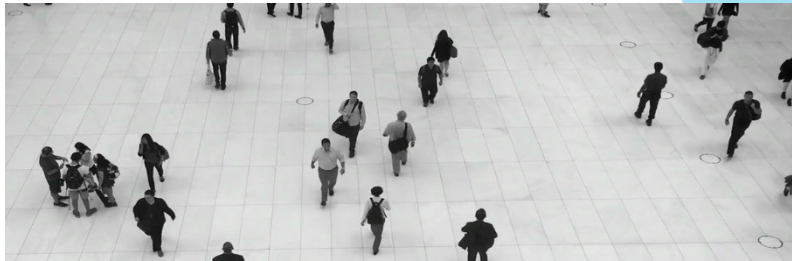
Migrazione verso il Cloud da ambienti tradizionali



Scenari futuri

Oggetti Connessi

In previsione di una maggiore diffusione di **oggetti connessi** (es. veicoli a guida autonoma, droni o robot) diventa fondamentale **l'ambito della sicurezza**. Il controllo di un veicolo a guida autonoma, ad esempio, non deve essere assunto o compromesso da un malintenzionato, tramite l'installazione di software malevolo. Ci sono iniziative in atto, ad esempio, per la valutazione della tecnologia della gestione della comunicazione intra ed extra veicolare.



REGIONE PIEMONTE

CSI your digital partner

Politecnico di Torino

FONDAZIONE links PASSION FOR INNOVATION

INRiM ISTITUTO NAZIONALE DI RICERCA METROLOGICA

top-ix

CYBERSECURITY 4.0

Il futuro della sicurezza informatica è ora

Torino | giovedì 3 marzo 2022

Grazie per l'attenzione.