POLITECNICO
MILANO 1863

POLIQI: MILANO QUANTUM INFRASTRUCTURE

Mario Martinelli

GTTI, Lecce Settembre 2021

Politecnico di Milano Quantum Infrastructure PoliQI

Nel **Marzo 2021** nell'ambito del PROGRAMMA DEGLI INTERVENTI PER LA RIPRESA ECONOMICA: SVILUPPO DI NUOVI ACCORDI DI COLLABORAZIONE CON LE UNIVERSITÀ PER LA RICERCA, L'INNOVAZIONE E IL TRASFERIMENTO TECNOLOGICO viene firmato un protocollo di collaborazione fra la Regione Lombardia ed il Politecnico di Milano per la costruzione di una rete di comunicazione operativa in ambito urbano per la distribuzione di chiavi quantistiche incondizionatamente sicure che rappresenti una piattaforma accessibile per il test e lo sviluppo delle future applicazioni di sicurezza.

Il progetto viene denominato POLIQI: POLItecnico di Milano Quantum Infrastructure

Politecnico di Milano Quantum Infrastructure PoliQI

- Una trasmissione di chiavi quantistiche (quantum key distribution, QKD) è sostanzialmente una applicazione delle Comunicazioni Ottiche. Si usano gli stessi ingredienti: fotoni trasmessi su canali ottici (in spazio libero o in fibra ottica).

- Al Politecnico abbiamo proposto per primi l'impiego di componenti passivi per la realizzazione di operatori quantistici (i 3 operatori di Pauli) nel 1989 e 2016.

- Al Politecnico è già attivo un Corso di Quantum Communications dal 2019.

- Come Politecnico abbiamo partecipato nel 2020 ad un progetto EIT per la costruzione e la qualifica di un nodo QKD su fibre installate (insieme a Italtel e Telefonica su fibre TOP-IX).

- Numerosi esperimenti hanno dimostrato la fattibilità di trasmissioni QKD in ambito urbano e spaziale (in Italia Padova e Firenze, in Europa Ginevra e Vienna , in USA DARPA, in Cina una trasmissione con 30 nodi, 2 spaziali per 4600 km di percorrenza). A marzo di quest'anno è partito il PON QUANCOM.

- Esistono già *almeno* 3 vendors di apparati QKD.

Article

An integrated space-to-ground quantum communication network over 4,600 kilometres

https://doi.org/10.1038/s41586-020-03093-8

Received: 1 March 2019

Accepted: 2 November 2020

Published online: 06 January 2021

Check for updates

Yu-Ao Chen[1,2]✉, Qiang Zhang[1,2], Teng-Yun Chen[1,2], Wen-Qi Cai[1,2], Sheng-Kai Liao[1,2], Jun Zhang[1,2], Kai Chen[1,2], Juan Yin[1,2], Ji-Gang Ren[1,2], Zhu Chen[1,2], Sheng-Long Han[1,2], Qing Yu[3], Ken Liang[3], Fei Zhou[4], Xiao Yuan[1,2], Mei-Sheng Zhao[1,2], Tian-Yin Wang[1,2], Xiao Jiang[1,2], Liang Zhang[2,5], Wei-Yue Liu[1,2], Yang Li[1,2], Qi Shen[1,2], Yuan Cao[1,2], Chao-Yang Lu[1,2], Rong Shu[2,5], Jian-Yu Wang[2,5], Li Li[1,2], Nai-Le Liu[1,2], Feihu Xu[1,2], Xiang-Bin Wang[4], Cheng-Zhi Peng[1,2]✉ & Jian-Wei Pan[1,2]✉

POLITECNICO MILANO 1863

Mario Martinelli Incontro EXPRIVIA del 22 Aprile 2021

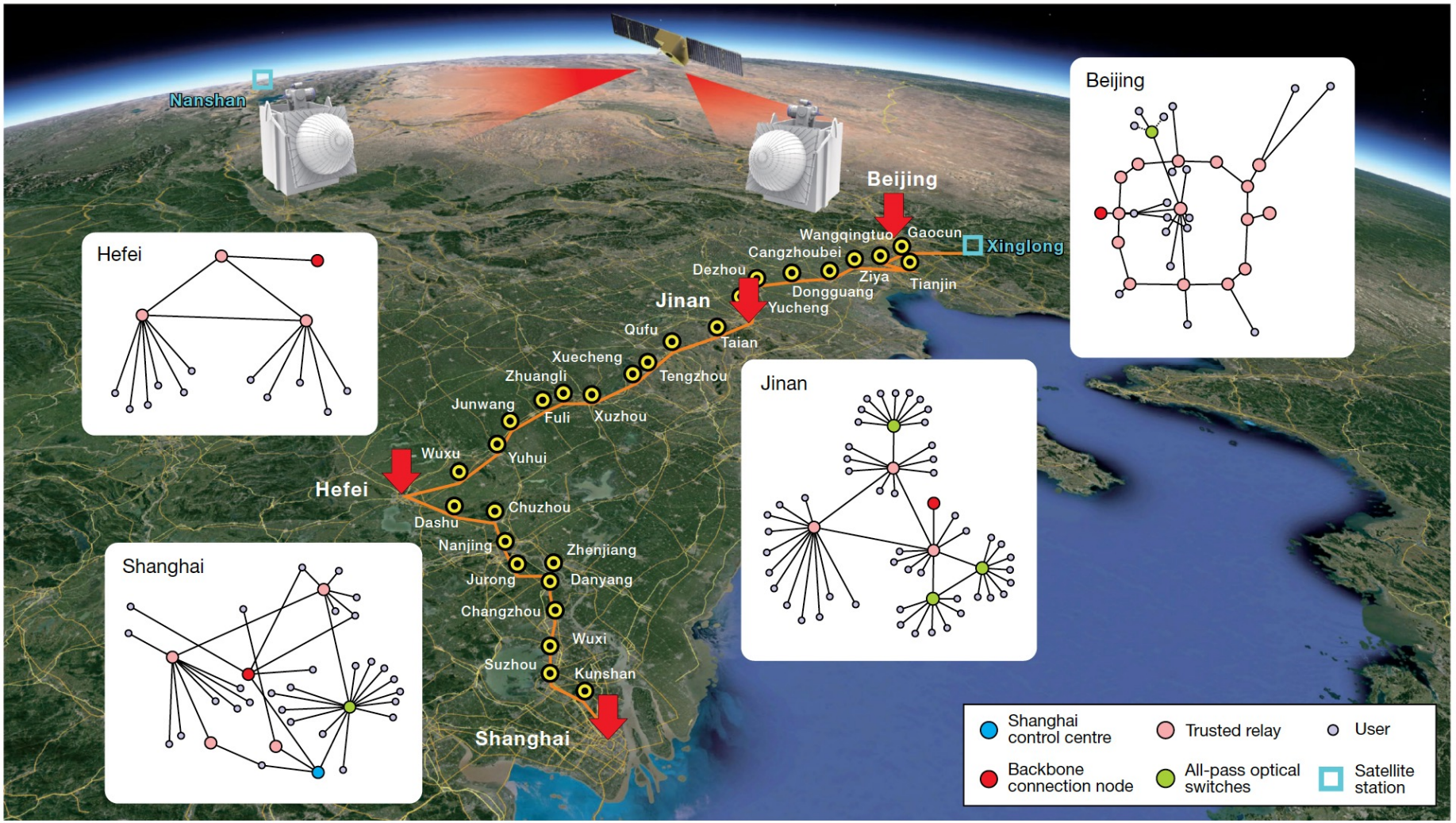
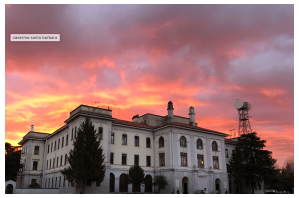


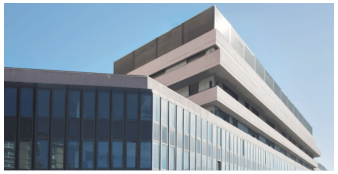
Fig. 1 | Illustration of the integrated space-to-ground quantum network. is connected by trusted relays (shown as yellow and black circles in the main

Politecnico di Milano Quantum Infrastructure PoliQI

Obiettivo primario di POLIQI **non** è quello di dimostrare la fattibilità della tecnologia punto-a-punto QKD ma di progettare e sperimentare una vera e propria **rete QKD,** cioè un sistema che permettesse lo scambio di chiavi quantistiche fra tutti i nodi della rete.
Un **secondo obiettivo**, conseguente del primo, è di verificare/investigare se i servizi abilitati dalla rete QKD siano effettivamente utili (in termini di costi/prestazioni).

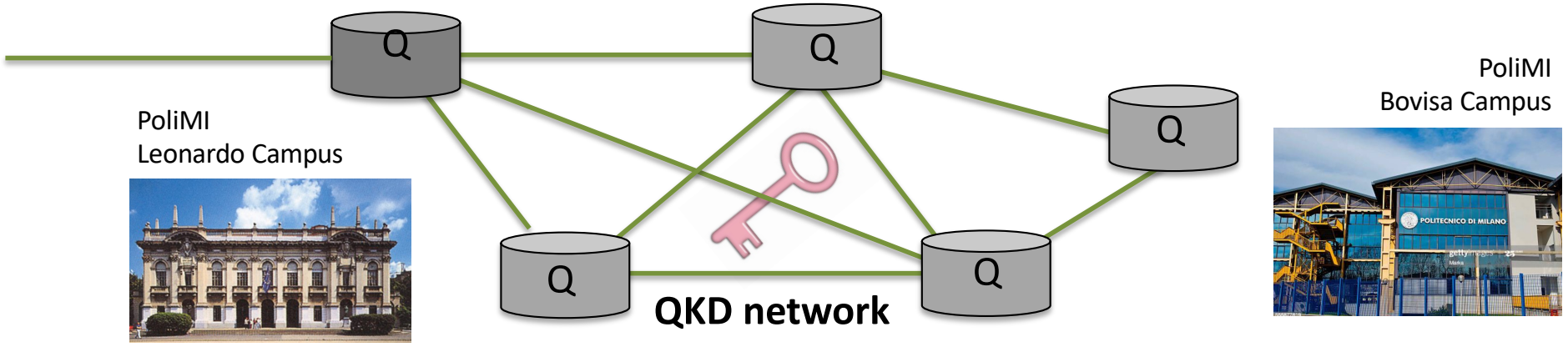
Milano
Army
Barracks





Milano
Administrative
District

Milano
Financial
District



PoliMI
Leonardo Campus

PoliMI
Bovisa Campus

Politecnico di Milano Quantum Infrastructure PoliQI

- Il protocollo usato è quello “classico” BB84 basato sulla manipolazione degli stati di polarizzazione (spin) di singoli fotoni. Gli apparati sono ETSI compliant e SDN-ready. La struttura della rete è solo simbolica: la rete effettiva verrà progettata sulla base delle interazioni che stiamo sviluppando con i vari Enti presenti sul territorio, compreso i fornitori di servizi Web;

- Il bit rate target è 10 kbit/s ma potrebbe arrivare a 100 kbit/s ed oltre con l’impiego di ricevitori a superconduttore (criogenici). I ricevitori criogenici sono un opzione del progetto previsti a budget. La distanza di scambio Tx/Rx prevista è dell’ordine di 25 km ma distanze maggiori sono possibili (sino a 50 km) in funzione del bit-rate accettato, uso di ricevitori criogenici, ecc.

- Il canale di comunicazione impiega fibre monomodo standard della rete di comunicazione ottica urbana. Le fibre verranno noleggiate (con contratti di IRU) da principali operatori operanti sull’area di Milano (che saranno pure coinvolti nella sperimentazione). Lo scambio di chiavi sperimenterà due opzioni: intera occupazione della risorsa di fibra (opzione 1) o condivisione con canali in terza finestra);

Politecnico di Milano Quantum Infrastructure PoliQI

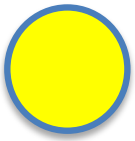
Coerentemente con il principale obiettivo della iniziativa POLIQI, la rete sarà sviluppata in funzione della abilitazione di servizi.

In particolare al momento si potranno abilitare **tre servizi**:

- Trasporto cifrato ad alta capacità sul layer OTN da uno o più più Nodi-Clienti verso uno o più Nodi-Server.
- Comunicazioni cifrate sul layer IP Nodo-Nodo
- Sviluppo di applicativi over-layers del tipo e-Procurement, Block-chain, ecc., fra tutti i 5+ Nodi della rete.

Aggiornamenti a questi servizi sono sempre *previsti e possibili* essendo il Progetto multi-partners e in continua evoluzione ed avendo una autonoma capacità di realizzazione degli apparati quantistici.

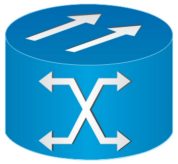
Politecnico di Milano Quantum Infrastructure PoliQI



QKD Node

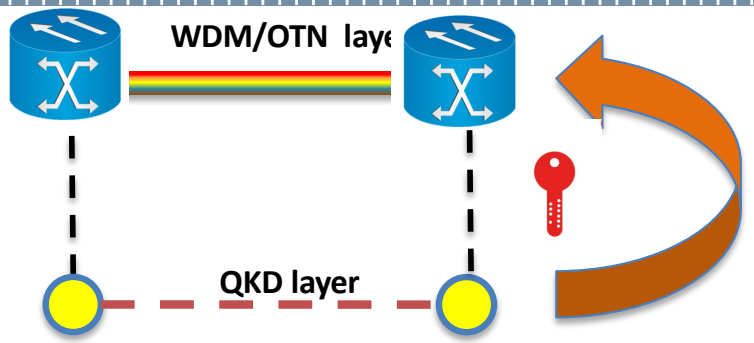
La chiave generata nel Layer QKD ha una lunghezza variabile (e.g. 256 bit) ed una cadenza variabile (e.g. 10 kb/s)

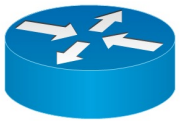
Politecnico di Milano Quantum Infrastructure PoliQI



Optical transport

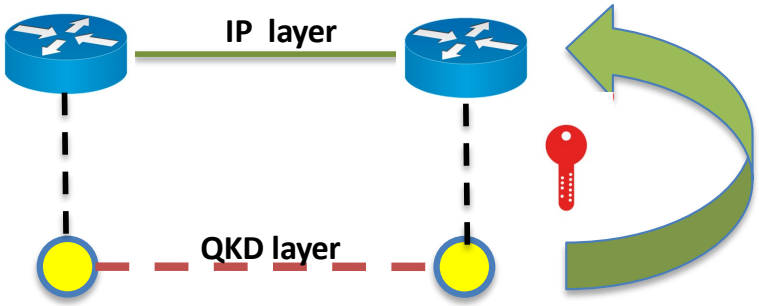
La chiave generata nel Layer QKD viene usata per cifrare la trama OTN (e.g. AES 256) e quindi garantire un trasporto ad alto bit-rate (e.g. 100 Gb/s)





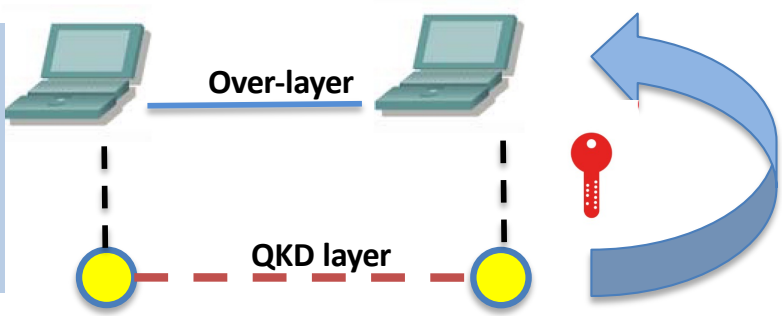
Router

La chiave generata nel Layer QKD viene usata per cifrare i pacchetti IP e quindi garantire un trasporto sicuro a livello IP

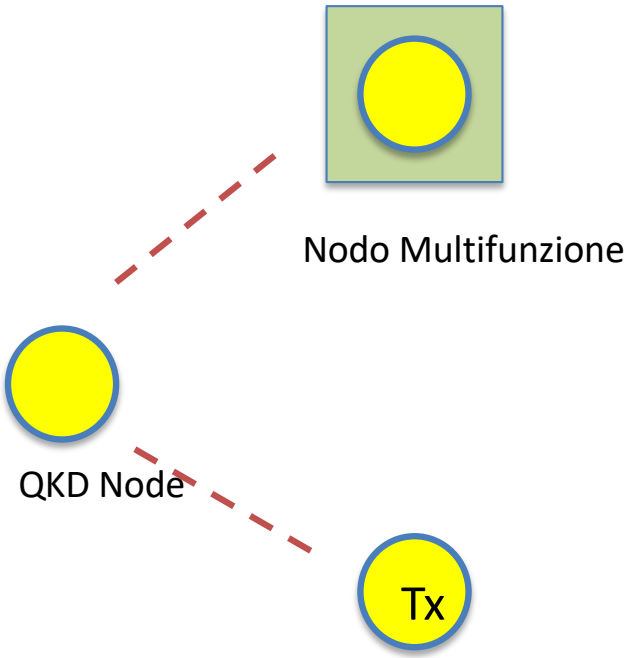


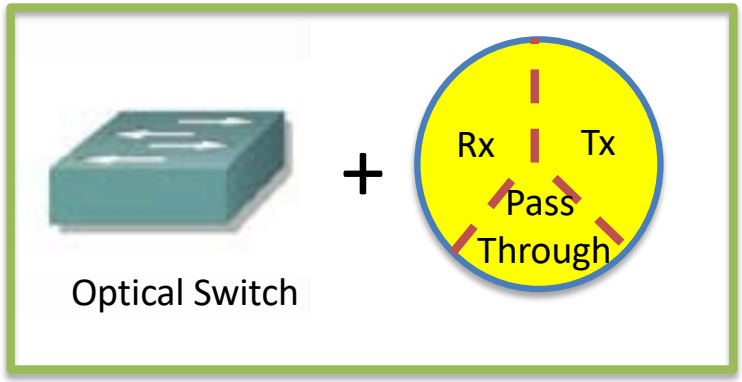
Application device

La chiave generata nel Layer QKD viene usata per applicazioni in cui sia vitale la sicurezza delle transizioni (e.g block-chain, e.procurement, etc)



Politecnico di Milano Quantum Infrastructure PoliQI

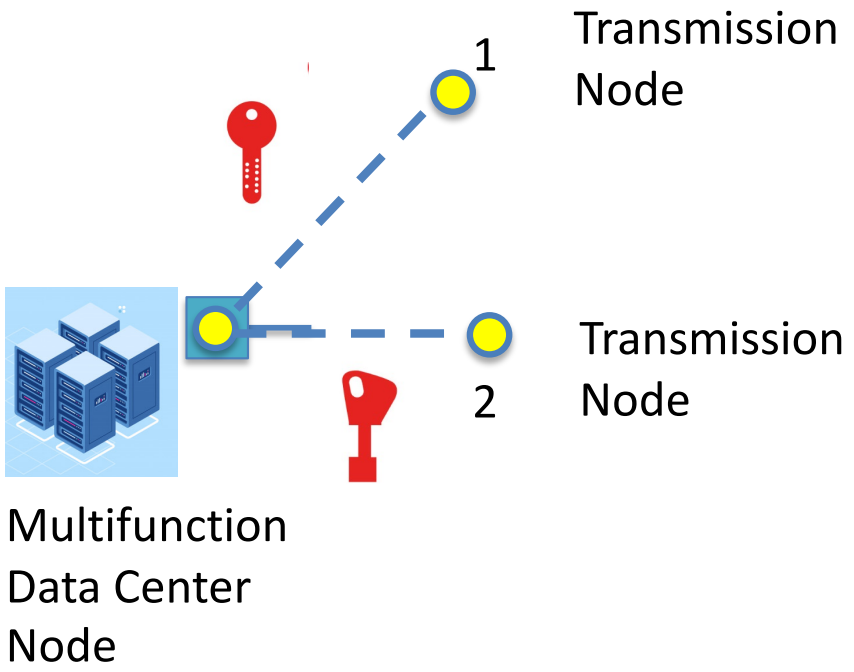


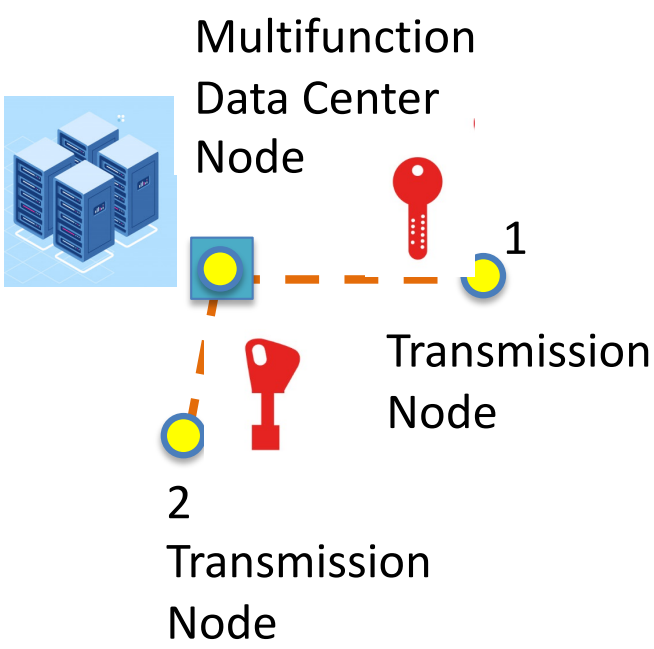


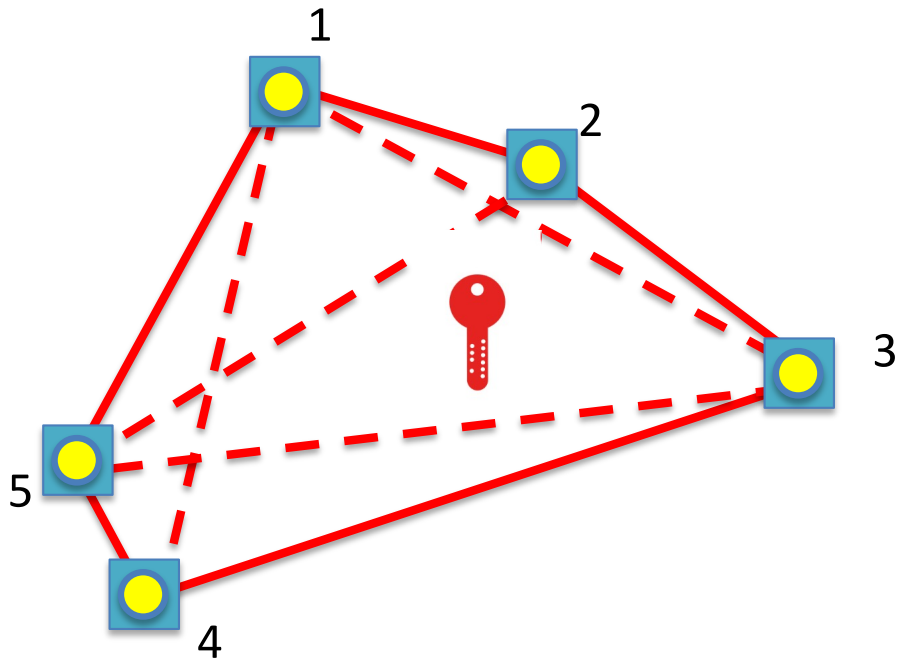
Il Nodo QKD può essere un nodo Multifunzionale oppure un semplice Nodo Trasmittente o Ricevente

La concezione della rete e dei nodi è stata coperta da due brevetti del POLITECNICO depositati in data 15 marzo e 26 Maggio 2021

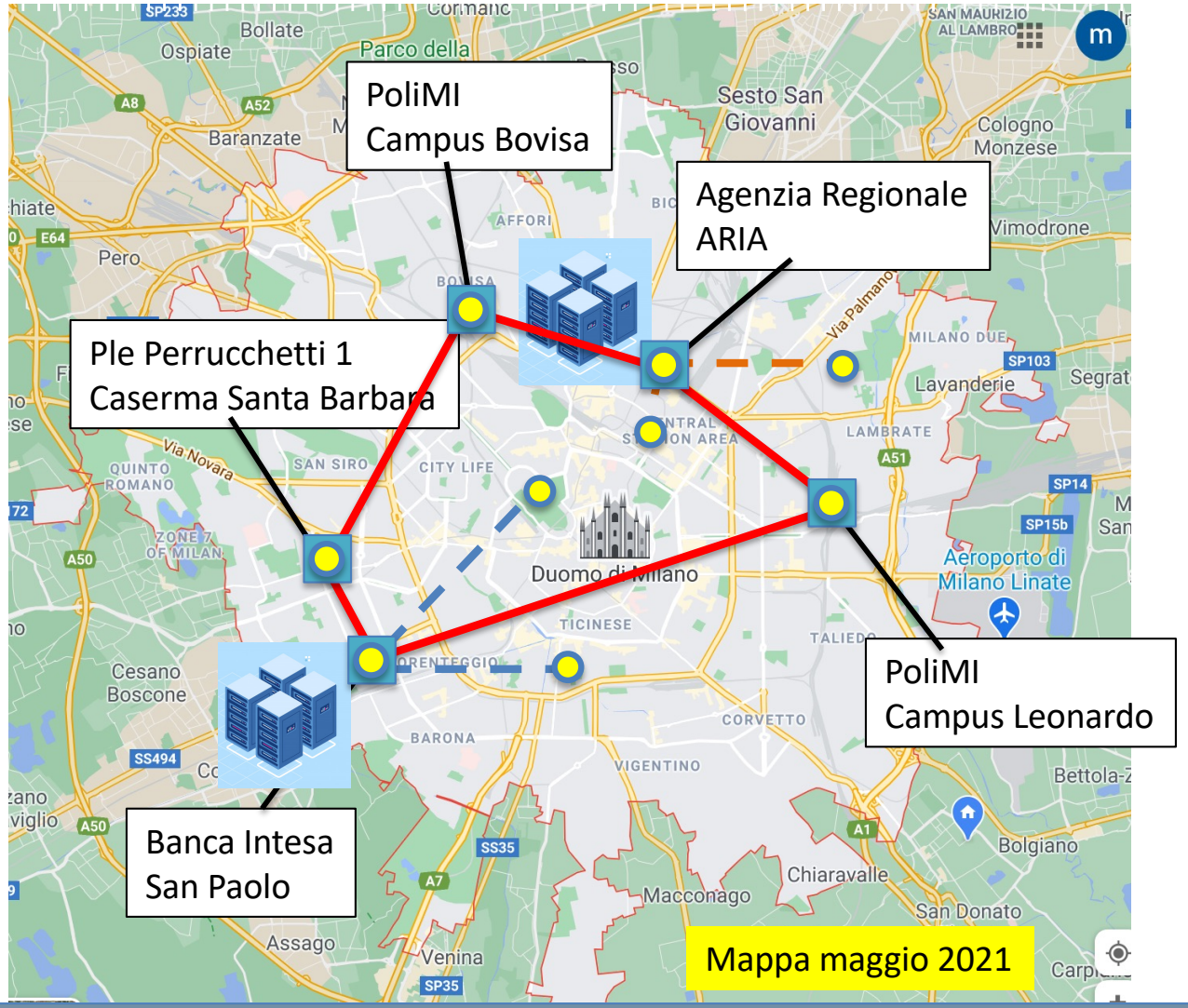
Politecnico di Milano Quantum Infrastructure PoliQI



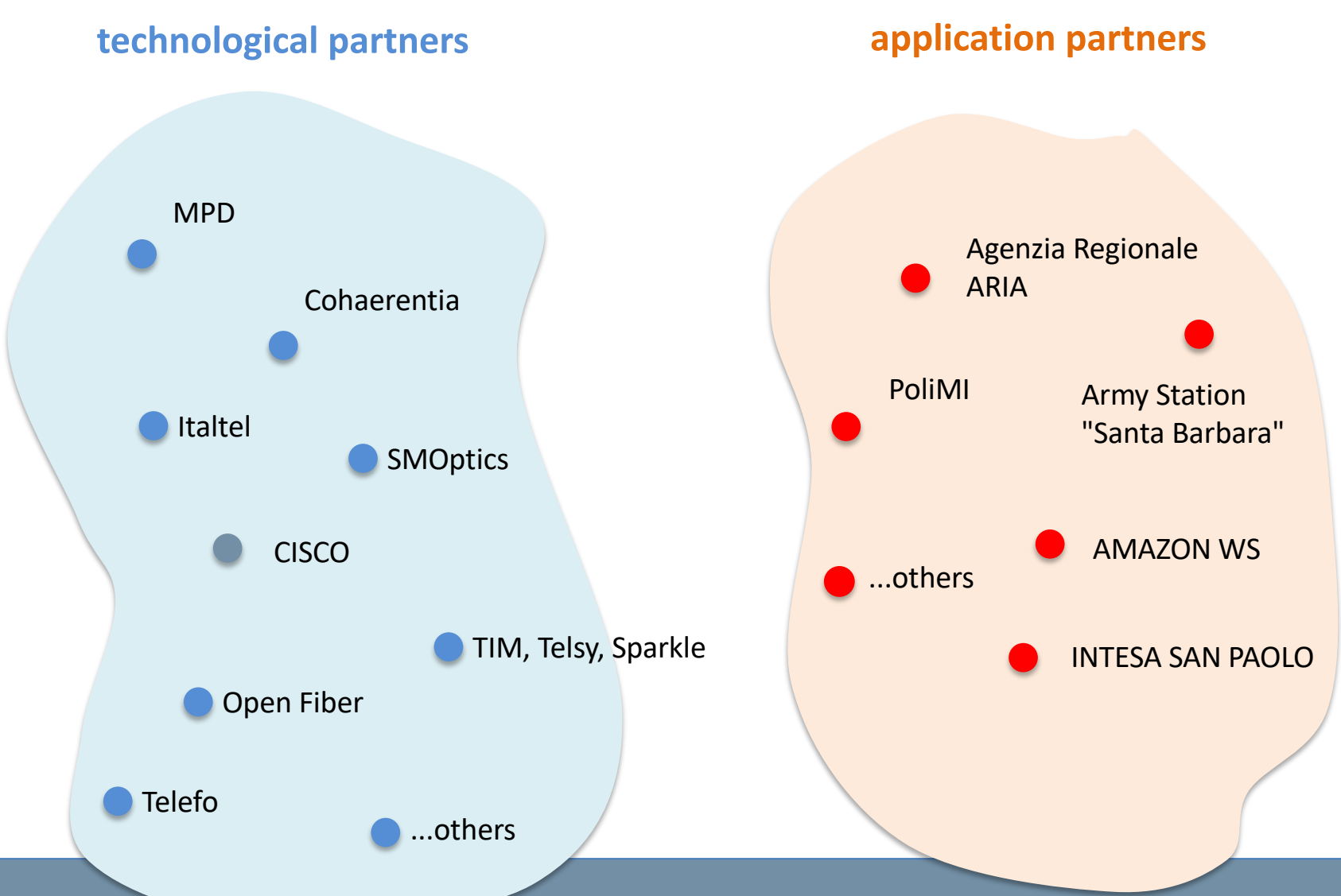



1
2
3
4
5

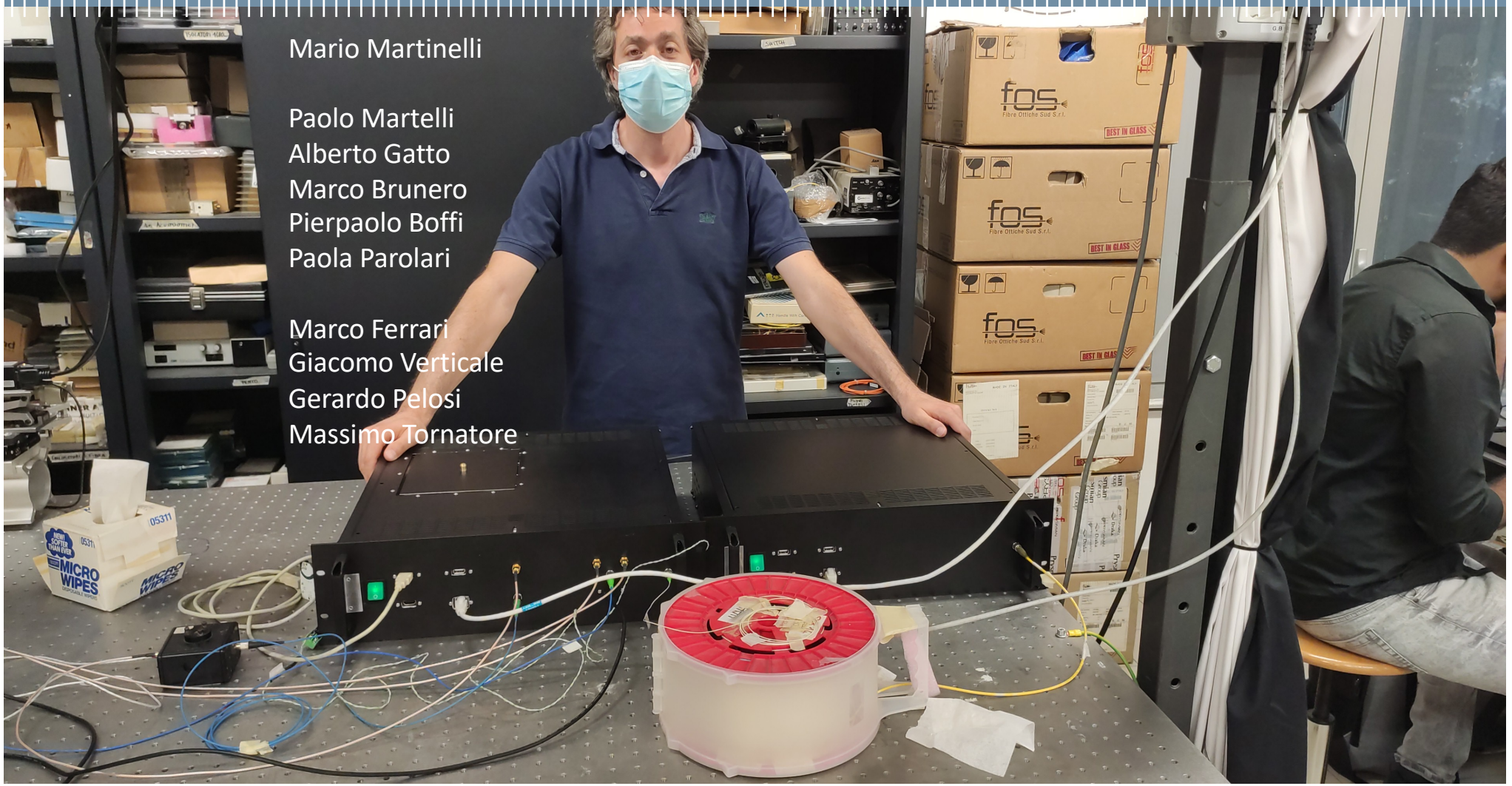
Politecnico di Milano Quantum Infrastructure PoliQI



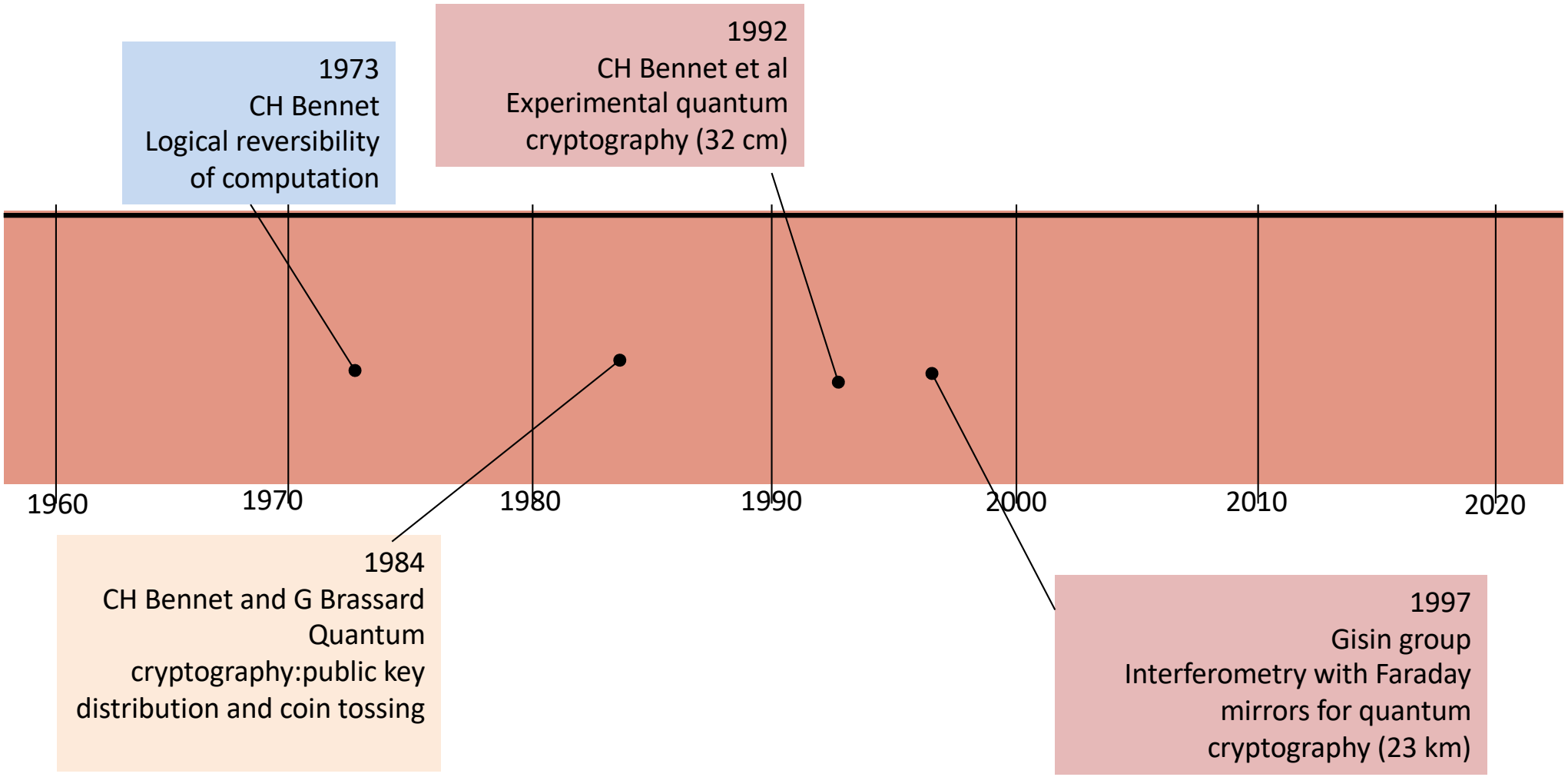
Politecnico di Milano Quantum Infrastructure PoliQI



Politecnico di Milano Quantum Infrastructure PoliQI



Politecnico di Milano Quantum Infrastructure PoliQI



Google Scholar: 9282 citations

QUANTUM CRYPTOGRAPHY: PUBLIC KEY DISTRIBUTION AND COIN TOSSING

Charles H. Bennett (IBM Research, Yorktown Heights NY 10598 USA)
Gilles Brassard (dept. IRO, Univ. de Montreal, H3C 3J7 Canada)

International Conference on Computers, Systems & Signal Processing Bangalore, India December 10-12, 1984

Google Scholar: 9282 citations

because of the random mix of rectilinear and

information over the quantum channel.

The following example illustrates the above protocol.

QUANTUM TRANSMISSION														
Alice's random bits	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Random sending bases	D	R	D	R	R	R	R	R	D	D	R	D	D	D	R
Photons Alice sends	↗	↕	↘	↔	↕	↕	↔	↔	↘	↗	↕	↘	↗	↗	↕
Random receiving bases	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R
Bits as received by Bob	1		1		1	0	0	0		1	1	1		0	1
PUBLIC DISCUSSION															
Bob reports bases of received bits	R		D		R	D	D	R		R	D	D		D	R
Alice says which bases were correct			OK		OK			OK				OK		OK	OK
Presumably shared information (if no eavesdrop)			1		1			0				1		0	1
Bob reveals some key bits at random					1									0	
Alice confirms them					OK									OK	
OUTCOME															
Remaining shared secret bits			1					0				1			1

The need for the public (non-quantum) channel

an eavesdropper ignorant of the