

Quantum key distribution

Giorgio Ancona – Chief Delivery Officer
Gruppo Lutech

22nd September 2026

Lutech e IonQ Italia: nasce la nuova alleanza per il Quantum

Il quantum computing supera i limiti del calcolo classico nei problemi a complessità esponenziale. La disponibilità tecnologica sta diventando una finestra strategica: **chi la usa per primo in modo industriale guadagna un vantaggio difficile da recuperare.**

NASCE L'ALLEANZA IONQ ITALIA e LUTECH

IonQ Italia porta la tecnologia a ioni trappolati — computing, networking, sicurezza e sensing. Lutech la traduce in progetti pilota e soluzioni scalabili, integrate nei sistemi cloud, AI e cybersecurity già in produzione, con delivery e governance mantenute in Italia e in Europa.



Technology provider



Service provider



Perché le tecnologie quantistiche

I computer quantistici attuali non sono un pericolo per la crittografia

«Harvest now, decrypt later»

Quantum networks

Protezione del canale di comunicazione da attacchi «man in the middle»

Quantum key distribution

Le chiavi crittografiche non vengono condivise con terzi

Progetto & Servizi

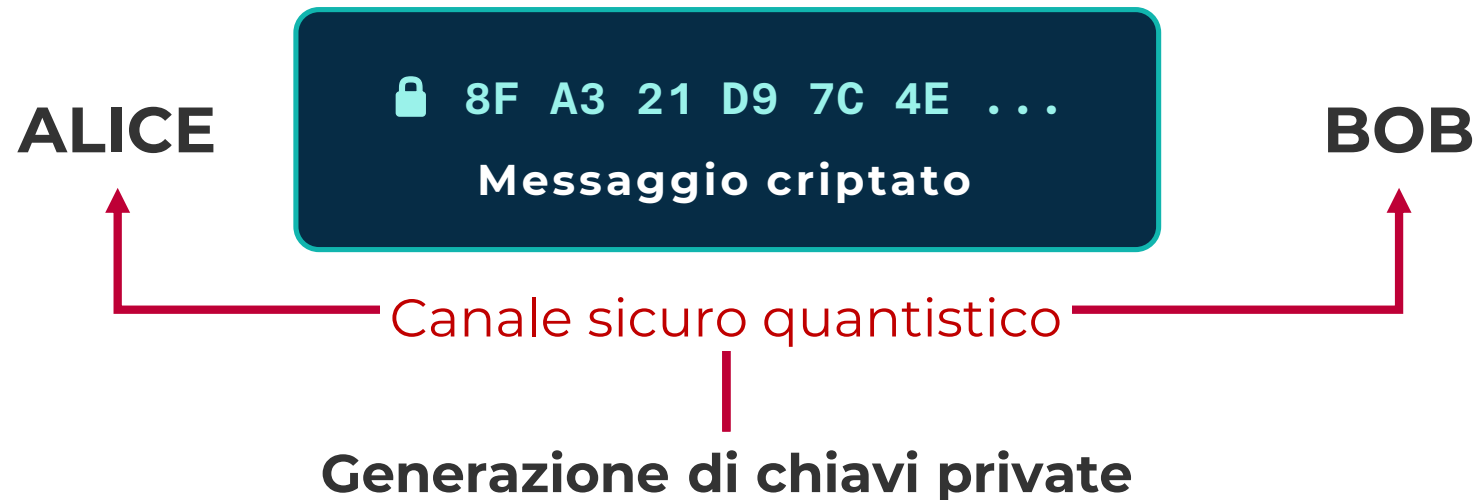
Implementazione dei modelli e integrazione della tecnologia



La soluzione quantistica

Puoi usare una crittografia quantistica molto robusta per creare chiavi migliori

Ma come si distribuiscono le chiavi private in modo sicuro?



Le linee di comunicazione quantistiche rilevano immediatamente intrusioni utilizzando stati quantici

Supportato dalla fisica, non da complessità matematiche



Idee false sulla Quantum key distribution (QKD)

La QKD ha costi Elevati

- QKD è 2 ordini di grandezza più economico rispetto al PQC
- QKD opera a livello di rete, non è necessario aggiornare i dispositivi di rete
- Non è necessaria una rete in fibra ottica separata per il canale quantum-resistant

La QKD è vulnerabile agli attacchi Denial of Service (DOS)

- Il rilevamento istantaneo di intercettazioni da parte di QKD non è particolarmente vulnerabile agli attacchi DOS
- Per montare un tale attacco, gli intercettatori dovrebbe avere accesso diretto al collegamento in fibra ottica
- L'aggressore potrebbe anche tagliare il cavo — qualsiasi tecnologia è vulnerabile al DOS

La QKD è praticabile solo su brevi distanze

- Un segmento di QKD terrestre attualmente non può superare i 175 km
- Più segmenti possono essere concatenati utilizzando nodi affidabili, ripetitori quantistici e connessioni satellitari



Qual è il miglior approccio sicuro quantisticamente?



NIST

"Alternative key exchange mechanisms are allowed , **and those who have a use case to leverage QKD can proceed to implement it.**"



'This should lead to the implementation of PQC technologies across the Union in existing government systems and critical infrastructures via **hybrid schemes that can combine PQC with existing cryptographic approaches or with QKD.**'



Monetary Authority
of Singapore

"Consider [...] monitoring ongoing developments in quantum computing for cybersecurity threats and risks that could affect financial services, and their possible **mitigation via quantum security solutions such as PQC and QKD.**"



JPMORGAN
CHASE & CO.

"We are thrilled to say that at JPMorgan Chase **we are pursuing both approaches, both quantum cryptography and QKD**, where PQC is primarily used in the application layer and QKD is delegated to work at the network layer and encrypt everything underneath."



MOODY'S

"[The new standards] were chosen because PQC methods are available today and can be expected to provide some level of resistance to quantum attacks, **but ideally future standards will be based on QKD methods.**"





www.lutech.group