

COMUNICATO STAMPA

INRiM DIMOSTRA SUL CAMPO UNA NUOVA TECNICA PER LA CRITTOGRAFIA QUANTISTICA IN FIBRA OTTICA A LUNGA DISTANZA

Uno studio INRiM, svolto su circa 200 km dell'Italian Quantum Backbone e pubblicato sulla prestigiosa rivista Nature Communications, ha dimostrato un nuovo sistema per lo scambio di chiavi crittografiche su lunghe distanze in campo reale, basato sulle tecnologie quantistiche.

■ **Torino, 20 Gennaio 2022** – In uno studio **pubblicato sulla prestigiosa rivista [Nature Communications](https://doi.org/10.1038/s41467-021-27808-1)** (doi.org/10.1038/s41467-021-27808-1), un gruppo di ricercatori dell'**Istituto Nazionale di Ricerca Metrologica (INRiM)** ha dimostrato sul campo una nuova tecnica per la crittografia quantistica in fibra ottica a lunga distanza.

La **Quantum Key Distribution (QKD)** ha provato che le leggi della fisica fondamentale permettono, attraverso lo scambio di singoli fotoni (le particelle elementari di cui la luce è composta), di scambiare chiavi di cifratura per trasmettere informazioni con un'elevata sicurezza e inviolabilità.

Il tema ormai è pienamente uscito dalla cerchia della comunità scientifica ed è oggetto di un'intensa attività istituzionale e industriale. La Commissione Europea, con l'iniziativa **"European Quantum Communication Infrastructure"** punta a integrare le tecnologie quantistiche per la crittografia all'interno di servizi specifici, entro i prossimi dieci anni, su tutto il territorio dell'Unione e INRiM è attivamente coinvolto nella progettazione di questa infrastruttura con il **progetto OQTAVO**.

Tuttavia, uno dei maggiori ostacoli allo sviluppo efficace in campo reale e su lunghe distanze di queste tecnologie è dovuto alla "fragilità" dei segnali quantistici scambiati: i fotoni possiedono infatti un'energia luminosa infinitesima e sono dunque difficili da rilevare singolarmente, a maggior ragione se si considera che, viaggiando nelle fibre ottiche con cui scambiamo informazioni, il 99% di essi viene perso nei primi 100 km; inoltre, dopo aver attraversato lunghe distanze, l'informazione trasportata da quelli che sopravvivono risulta distorta.

INRiM ha già affrontato ampiamente questi problemi in ambito metrologico e ha contribuito a sviluppare tecniche laser specifiche per ripristinare l'informazione contenuta nei segnali trasmessi. **Questi metodi sono oggi alla base dei confronti internazionali di orologi atomici.**

Ora, mettendo in sinergia l'interferometria laser coerente, le tecnologie a singolo fotone e la metrologia quantistica, **applica queste tecniche allo scambio di chiavi crittografiche quantistiche**, riducendo il numero di errori di trasmissione e aumentando la lunghezza dei messaggi. All'atto pratico, questi miglioramenti aprono alla possibilità di realizzare protocolli QKD estremamente più efficaci sfruttando **la tecnica *twin-field quantum key distribution***, la più moderna e quotata candidata per lo scambio di chiavi crittografiche su lunghe distanze.

La ricerca è stata svolta su circa 200 km dell'Italian Quantum Backbone, una rete in fibra ottica di 1800 km realizzata da INRiM, che distribuisce segnali laser di riferimento di tempo e frequenza ad alcuni fra i principali centri di ricerca del Paese ed è dedicata ad applicazioni di fisica fondamentale, sensing geofisico, e allo sviluppo di tecnologie quantistiche innovative.

Lo studio è anche il risultato di una **collaborazione con Toshiba Europe**, multinazionale tra i leader mondiali nello sviluppo e nella commercializzazione di prodotti basati sulle tecnologie quantistiche, e con il **Consorzio TOP-IX**, il provider di rete che gestisce centinaia di km di fibra ottica del Nord Italia e che ha messo a disposizione parte dell'infrastruttura per questa sperimentazione.

La sinergia fra specifiche competenze, dalla meccanica quantistica alla fisica degli orologi atomici, alla realizzazione dell'infrastruttura e alla gestione della rete, ha permesso di raggiungere un risultato di eccellenza, che consolida il ruolo dell'Italia come attore principale nella realizzazione di una infrastruttura quantistica europea.