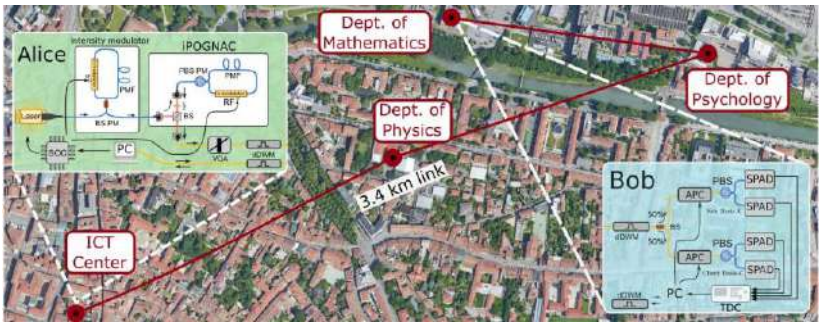
AMMINISTRAZIONE CENTRALE
AREA COMUNICAZIONE E MARKETING
SETTORE **UFFICIO STAMPA**
Via VIII febbraio, 2 – 35122 Padova
stampa@unipd.it
http://www.unipd.it/comunicati
tel. 049-8273066/3041

Padova, 10 giugno 2021

# CRITTOGRAFIA QUANTISTICA SULLE FIBRE DI PADOVA

***Testata una videochiamata protetta con un nuovo sistema di QKD sulla rete in fibra di Ateneo***

Nel numero di giugno 2021 della prestigiosa rivista dell'Optical Society of America «Optics Letters», i ricercatori del **gruppo QuantumFuture del Dipartimento di Ingegneria dell'Informazione dell'Università di Padova** hanno dimostrato la distribuzione di chiave quantistica (QKD, dall'inglese Quantum Key Distribution) per finalità istituzionali dell'Università sulla rete in fibra ottica dell'Ateneo patavino, utilizzando dei sistemi da loro sviluppati e brevettati. Questo test è un passo importante verso l'integrazione completa della sicurezza quantistica sulle reti in fibra ottica volta a implementare il salto tecnologico nella sicurezza delle comunicazioni sollecitato energicamente sia livello europeo che nazionale.




*Test in campo di QKD - I ricercatori dell'Università di Padova hanno dimostrato un sistema di QKD semplificato e l'hanno utilizzato sulla rete in fibra ottica padovana. Una mappa del centro città [©2021 Google] mostra il trasmettitore è stato posizionato al centro ICT di Ateneo, mentre il ricevitore al Dipartimento di Matematica. La chiave quantistica ha viaggiato su 3.4 km di fibra interrata. (Immagine fornita da: QuantumFuture Group, Università degli Studi di Padova)*

Infatti, la **QKD** permette di realizzare comunicazioni digitali sicure perché utilizza le proprietà quantistiche della luce per generare chiavi poi utilizzate per criptare e decriptare i dati.

«La QKD è utile in tutte le situazioni in cui la sicurezza è fondamentale. Infatti, offre sicurezza incondizionata per il processo di scambio di chiave- dice **Marco Avesani**, ricercatore dell'Università di Padova e **primo autore dell'articolo assieme a Luca Calderaro e Giulio Foletto** -. Ad esempio, può essere usata per crittografare e autenticare le comunicazioni fra gli ospedali oppure le transazioni monetarie fra le banche».


*Il trasmettitore QKD - L'intero sistema di trasmissione è chiuso in un contenitore rack standard da 19 pollici, come quelli che si trovano comunemente nelle server room. (Immagine fornita da: Luca Calderaro, Università degli Studi di Padova)*

Nell'articolo, il gruppo di ricerca guidato dai Professori Paolo Villoresi e Giuseppe Vallone presenta un sistema semplice e stabile nel tempo che può generare chiavi crittografiche quantistiche su una linea in fibra ottica standard.

«Tipicamente, i sistemi di QKD necessitano di un complesso apparato di stabilizzazione e componenti addizionali per la sincronizzazione - **aggiunge Avesani**. Il nostro sistema, invece, riduce notevolmente le procedure di stabilizzazione e non richiede hardware aggiuntivo per sincronizzarsi, per cui si adatta direttamente alle normali reti di comunicazione attualmente utilizzate. Inoltre, il sistema è contenuto in contenitori rack standard, che si trovano di solito nelle *server room*».

Progettare un sistema semplice da usare

Per produrre gli stati quantistici richiesti dalla QKD, i ricercatori hanno sviluppato un nuovo sistema di manipolazione della polarizzazione di singoli fotoni, chiamato iPOGNAC. Esso fornisce un riferimento di polarizzazione fisso e non richiede frequenti ricalibrazioni, una caratteristica fondamentale per le comunicazioni quantistiche in spazio libero e in particolare nel caso in cui venisse installato su satellite per QKD a lunga distanza.

«Grazie a questa nuova tecnologia, la sorgente di stati quantistici è stata subito pronta a produrre chiavi dopo il trasporto dal laboratorio al luogo del test - **dice Luca Calderaro** -. Non è stata necessaria alcuna procedura di stabilizzazione tipica di altri sistemi di QKD, che spesso richiede tempo e l'intervento umano».

*Gruppo QuantumFuture del Dipartimento di Ingegneria dell'Informazione dell'Università di Padova*

I ricercatori hanno sviluppato anche un nuovo algoritmo, chiamato Qubit4Sync, per sincronizzare i due terminali che scambiano la chiave. Invece di usare un hardware dedicato e un canale ottico addizionale, l'algoritmo è una procedura puramente software che usa gli stessi segnali ottici della QKD. Ciò rende il sistema più compatto, economico e facile da integrare con la rete ottica esistente. Per il test, i due terminali QKD sono stati portati in due edifici universitari distanti circa 3.4 km e in quartieri diversi della città. Sono stati collegati a due fibre ottiche sotterranee della rete di ateneo che hanno svolto i ruoli di canale quantistico e canale classico, necessario per il trasferimento di informazione ausiliaria.

Una videochiamata protetta dalla QKD

«Il test in campo è stato un successo - dice Giulio Foletto -. Abbiamo dimostrato che il nostro sistema semplificato può produrre chiavi alla velocità di vari kilobit al secondo e che funziona tranquillamente fuori dal laboratorio, senza intervento umano. È stato anche veloce e facile da installare».

In una dimostrazione i ricercatori hanno usato il loro sistema per proteggere una videochiamata fra il Rettore dell'Ateneo e il Direttore del Dipartimento di Matematica. Il sistema ha prestazioni comparabili con alternative di QKD commerciali in termini di velocità di produzione di chiave, ma - sottolineano gli autori sottolineano - ha meno componenti ed è più facile da integrare con la rete esistente. I ricercatori lavoreranno ancora per ridurre le dimensioni dell'apparato di ricezione e per rendere il sistema più resistente al rumore causato da altra luce che potrebbe viaggiare sulla stessa fibra del segnale quantistico. Questi sforzi per sviluppare un sistema completo e autonomo di QKD hanno dato vita a uno spin-off chiamato ThinkQuantum S.r.l., che porterà questa tecnologia sul mercato.

Link alla ricerca: https://www.osapublishing.org/ol/fulltext.cfm?uri=ol-46-12-2848&id=451747

Titolo: “*Resource-effective quantum key distribution: a field trial in Padua city center*” - «Optics Letters» - 2021

Autori: Marco Avesani, Luca Calderaro, Giulio Foletto, Costantino Agnesi, Francesco Picciariello, Francesco B. L. Santagiustina, Alessia Scriminich, Andrea Stanco, Francesco Vedovato, Mujtaba Zahidy, Giuseppe Vallone e Paolo Villoresi