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, 6 aprile 2020

DALL'UNIVERSITÀ DI PADOVA UN INNOVATIVO SISTEMA DI CRITTOGRAFIA QUANTISTICA PER UNA COMUNICAZIONE A PROVA DI HACKER

I ricercatori di QuantumFuture mettono a punto un nuovo sistema basato sullo scambio di qubit

Al giorno d'oggi, la nostra vita, sia privata che lavorativa, è contrassegnata da una sempre più incessante presenza digitale. Basti pensare che ognuno di noi, quotidianamente, naviga sui social network, invia e-mail e sfrutta i servizi di internet banking. Tutto ciò è caratterizzato da un flusso continuo e costante di informazioni che vengono condivise tra gli utenti, i quali, anche inconsapevolmente, mettono in pericolo i propri dati personali. Per queste ragioni sono necessarie maggiori garanzie sul fronte della cyber security, a tutela, in primis, dei dati sensibili.

Le comunicazioni quantistiche possono rivoluzionare il settore della cyber security in quanto offrono un sistema di crittografia impossibile da violare che è basato sullo scambio di "quantum bit" (o qubit). La QKD (o distribuzione quantistica di chiave) infatti permette di creare una chiave di cifratura condivisa e sicura tra due utenti. La chiave è creata codificando i qubit nella polarizzazione di singoli fotoni scambiati tra essi. La sicurezza è basata sui principi della meccanica quantistica, dato che assicurano che nessun altro utente possa avere informazioni sulla chiave.

I recenti sviluppi tecnologici potrebbero rendere obsoleti gli schemi crittografici attualmente usati alla base della sicurezza informatica. Il "Quantum Advantage" recentemente raggiunta da Google ne è un chiaro esempio. Per questo motivo è cruciale rendere concreti ed efficaci i metodi per affrontare questa sfida della cyber security.

Il gruppo QuantumFuture del Dipartimento di Ingegneria dell'Informazione dell'Università di Padova lavora da anni in questa direzione, sviluppando sistemi di crittografia che sfruttano le leggi della meccanica quantistica per garantire livelli di sicurezza non raggiungibili con le risorse classiche.

In una nuova ricerca, coordinata dai Professori Giuseppe Vallone e Paolo Villoresi del gruppo QuantumFuture, pubblicata nella prestigiosa rivista «Optica» della Optical Society of America [Optica 7, 284 (2020)], è stato sviluppato e testato un innovativo sistema di QKD. Questo sistema è basato sul POGNAC, un modulatore di polarizzazione interamente sviluppato in QuantumFuture, e per il quale è stata depositata la richiesta di brevetto.

«L'innovativo sistema di QKD, sviluppato in un progetto del gruppo di ricerca QuantumFuture vanta almeno due punti di forza – **spiega il prof.**

Giuseppe Vallone -. Il primo è la sua semplicità, il sistema è stato infatti progettato per minimizzare il numero di componenti richiesti. Tale riduzione di hardware ha motivato lo sviluppo di metodi efficienti per garantire la funzionalità ed alti livelli di sicurezza richiesti dalla QKD. Un esempio in tal senso è la sincronizzazione tra trasmettitore e ricevitore. Infatti, il sistema sfrutta l'algoritmo *Qubits4Sync*, sempre di invenzione del gruppo QuantumFuture e basato esclusivamente sullo scambio di qubits, per ottenere una sincronia al picosecondo. Questo rappresenta una notevole semplificazione, basti pensare che altri sistemi di QKD precedentemente sviluppati richiedono ricevitori GPS o sistemi di comunicazione laser aggiuntivi per ottenere tale risultato, rendendo questa tecnologia quantistica più adatta ad affiancare i sistemi di comunicazione classica al giorno d'oggi usati nelle dorsali in fibra ottica.

Il secondo punto di forza del sistema di QKD sta nella capacità di trasmettere informazione quantistica con un bassissimo tasso di errore. In particolare, grazie al POGNAC è possibile preparare gli stati quantistici con la precisione più alta finora raggiunta. Questo traguardo è stato conseguito grazie al design del sistema che lo ha reso robusto e stabile.»

«Gli ottimi risultati ottenuti dal nostro gruppo dimostrano che vi sono le capacità e le competenze richieste per sviluppare questi sistemi tecnologici anche in un contesto commerciale che potrebbe essere d'importanza strategica a livello nazionale – **dice il dott. Costantino Agnesi, tra i primi firmatari dello studio, con Marco Avesani e Luca Calderaro** -. Infatti, verrebbe garantita la sicurezza dei sistemi informatici italiani, avvalendosi di dispositivi totalmente progettati e fabbricati in Italia. Abbiamo cominciato a tracciare un sentiero in questa direzione, sviluppando il sistema di QKD da noi ideato per delle dimostrazioni nella nostra rete di Ateneo.»

Questi risultati permetterebbero all'Università di Padova di assumere ruoli di rilevanza nelle cooperazioni internazionali, come il progetto OpenQKD, che a livello europeo sta predisponendo dei *testbed*, o dimostratori sul campo, per potenziare applicazioni delle comunicazioni sicure con le tecnologie quantistiche in settori cruciali, come i dati medici, le transazioni finanziarie e le comunicazioni intergovernative.

«Questo schema si profila di interesse anche per l'ambito delle comunicazioni satellitari, che negli ultimi anni vedono un forte sviluppo internazionale della parte quantistica– **sottolinea il prof. Paolo Villoresi**, che ha dato avvio al gruppo QuantumFuture nel 2003 proprio su questo tema - Infatti, in questo settore, la nostra società sta attingendo sempre più risorse che vanno utilizzate quotidianamente, come nella navigazione con GPS o Galileo, la rete dati o le trasmissioni TV e telefoniche. Le tecnologie quantistiche si possono applicare anche in questo contesto, e il gruppo QuantumFuture ha compiuto le prime dimostrazioni con dei sistemi passivi in orbita. Recentemente l'Agenzia Spaziale Italiana ha avviato un progetto per una dimostrazione mediante un satellite dedicato, che svilupperà ulteriormente le potenzialità di questa nuova tecnologia.»