Meccanica Quantistica, la nuova frontiera per Cybersecurity e sicurezza delle comunicazioni

intervista a Luca Ciciriello, (Torino, 1968). Fisico teorico che si occupa di calcolo e computer quantistici a livello industriale e soprattutto in ambito Cybersecurity. Autore di pubblicazioni scientifiche sulla gravità quantistica e l'innovazione tecnologica degli algoritmi quantistici in ambito Machine Learning (Quantum Machine Learning) e Security (Quantum Cryptography)

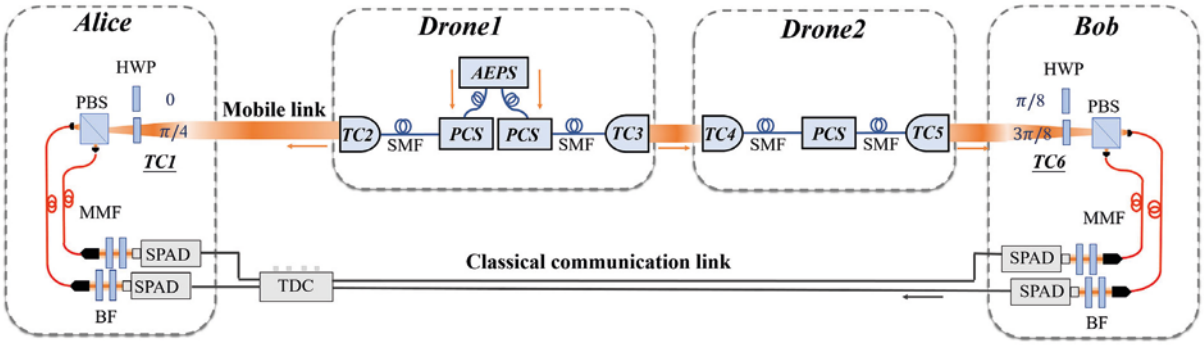
Ci può introdurre alla metodologia QKD che utilizza concetti di Meccanica Quantistica per la sicurezza delle comunicazioni?

La QKD, che sta per Quantum Key Distribution, è uno dei meccanismi per garantire la sicurezza nelle comunicazioni utilizzando concetti di Meccanica Quantistica (Quantum Cryptography). Attraverso la QKD, vengono abilitate due parti a produrre e a condividere una chiave segreta random da usare per crittare e decrittare i messaggi che vorranno scambiarsi. Il vantaggio di questa tecnica è di avere una "sicurezza intrinseca", cioè non dipendente dalla potenza di calcolo messa in campo da un eventuale attaccante. Questo ci consente sia di rilevare la presenza di una terza parte *(eavesdropper)* che tenta di ottenere informazioni sulla chiave, sia di impedire a questa terza parte l'ottenimento di tali informazioni.
La QKD è utilizzata solamente per generare e distribuire la chiave di crittatura e decrittatura, non per trasmettere alcun messaggio; la trasmissione del messaggio avverrà per i canali classici di comunicazione (LAN).

Cosa intende quando parla di "sicurezza intrinseca"?

La sicurezza intrinseca dei sistemi a trasmissione quantistica risiede in un semplice principio base che si può esplicitare in due punti: primo, l'informazione in ogni sistema fisico è finita e, secondo, si può ottenere sempre nuova informazione su un sistema fisico modificando quella esistente.
Quindi, quando acquisiamo nuova informazione su un sistema (ovvero effettuiamo una misurazione), poiché l'informazione rilevante totale non può crescere indefinitamente (primo punto), ne segue che ogni misurazione modifica in qualche modo l'informazione totale, rendendone irrilevanti alcune parti e più significative altre.
È per questo motivo che in Meccanica Quantistica, quando interagiamo con un sistema, in generale non solo acquisiamo parti di informazione su quel sistema ma, allo stesso tempo, "cancelliamo" o modifichiamo una parte dell'informazione sul sistema stesso.
Pertanto se, ad esempio, io sto trasferendo informazione da A a B, se C intercetta questa informazione (osserva il sistema eseguendo una misurazione), l'informazione trasferita cambia e il messaggio che A voleva trasferire a B e che è stato intercettato da C non è più coerente e diventa quindi inutilizzabile sia da B che da C. In termini implementativi, la chiave quantistica (un insieme di fotoni con uno stato quantizzato di polarizzazione) viene distribuita su un canale ottico che può essere una fibra, o attraverso un laser rimbalzato da una serie di specchi (rimbalzi satellitari o terrestri). La soluzione "on-the-air" (con specchi) è sempre preferibile in quanto comporta meno errori dovuti a disomogeneità ed assorbimento da parte della fibra. Per applicazioni di trasmissione di dati sensibili in condizioni di emergenza è possibile utilizzare dei droni come ripetitori del segnale laser che trasporta la chiave quantistica criptata[1]. La figura qui sotto schematizza una tipica architettura QKD con l'utilizzo di droni.

[1] www.researchgate.net/publication/348538158_Optical-Relayed_Entanglement_Distribution_Using_Drones_as_Mobile_Nodes



E' una tecnologia già disponibile sul mercato? Quali sono gli utilizzatori attuali?

Sì, certamente, è una tecnologia consolidata e utilizzata a livello industriale. Ad oggi, ci sono almeno quattro aziende nel mondo che possono fornire un'offerta di prodotti QKD "chiavi in mano". Queste aziende sono la svizzera **ID Quantique**[2], la statunitense **MagiQ Technologies**[3], l'australiana **Quintessence Labs**[4] e la francese **SeQureNet**[5].

L'azienda svizzera è sicuramente la capostipite. È la prima, con più di dieci anni di esperienza. È nata come spin-off dell'università di Ginevra. Ha in catalogo una serie di prodotti specifici, da generatori quantistici di numeri casuali (QRNG) a piattaforme QKD vere a proprie, basate sul protocollo BB84 o COW.

Senza fare nomi, anche un paio tra i più grandi istituti bancari italiani utilizzano oggi la tecnologia QKD per le loro transazioni più delicate.

E' possibile stimare i costi da sostenere per l'impiego di QKD a livello commerciale? Quali infrastrutture e dispositivi sono necessari?

Come detto in precedenza, oltre al normale canale di trasmissione del segnale criptato, è necessario avere un canale ottico (fibra/laser-on-the-air) collegato ad un set di trasmissione e ricezione che comprende un generatore casuale di chiavi e un sistema di polarizzazione dei fotoni trasmessi.

Ad oggi, questo sistema è realizzato da schede apposite che possono risiedere all'interno delle stesse macchine usate per la trasmissione classica del segnale, oppure su macchine dedicate (collegate con le principali).

Non ho elementi per quantificare con precisione il costo di un'infrastruttura completa, ma ritengo che la maggior parte delle spese riguardino la realizzazione della seconda linea dedicata in fibra o tramite collegamento satellitare/terrestre per trasmettere la chiave criptata.

Ritiene sia applicabile a sistemi di sicurezza fisica, quali ad esempio, impianti di videosorveglianza e controllo accessi in siti sensibili?

Il CASD (Centro Alti Studi per la Difesa) e il CeMiSS (Centro Militare di Studi Strategici) stanno già studiando ed implementando sistemi di questo tipo, che riguardano principalmente tecnologie di IoT e per le comunicazioni satellitari strategiche .

In campo civile, penso che non ci siano limitazioni di sorta all'utilizzo della tecnologia QKD. Grazie alla sua versatilità di affiancamento a sistemi classici già esistenti (gli algoritmi di codifica/decodifica della chiave sono algoritmi quantistici che girano su computer classici), questa tecnologia può benissimo essere impiegata per rendere inattaccabili sistemi di videosorveglianza preesistenti di siti sensibili.

In più, come detto all'inizio, se si deve presidiare in condizioni di emergenza un sito mobile temporaneo e trasmettere dati sensibili, è possibile impiegare un ponte ottico formato da uno o più droni.

---

[2] www.idquantique.com
[3] www.magiqtech.com
[4] www.quintessencelabs.com
[5] www.cbinsights.com/company/sequrenet
[6] www.difesa.it/SMD_/CASD/IM/CeMiSS/DocumentiVis/Rcerche_da_pubblicare/Pubblicate_nel_2019/AO_SMD_06_ITA.pdf