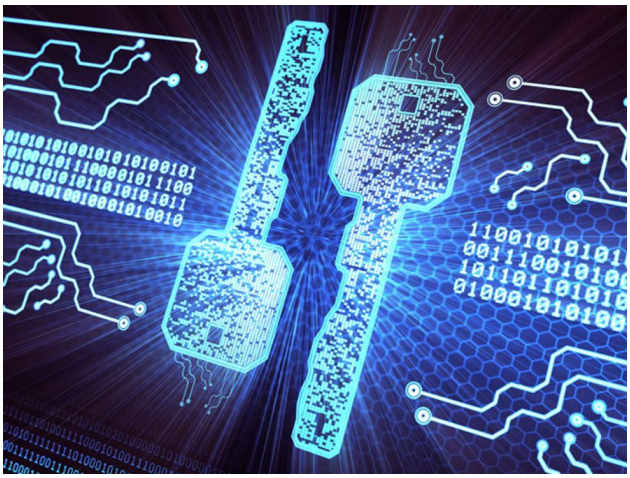
Crittografia quantistica e vita quotidiana:
un legame sorprendente

Mauro Orlandini

INAF/OAS Bologna

Fin dagli albori della civiltà, l'essere umano ha sentito il bisogno di nascondere e proteggere le proprie informazioni. Dai messaggi nascosti sotto la cera delle tavolette di Erodoto ai cifrari militari dell'antica Roma, passando per le ingegnose invenzioni rinascimentali, la storia della crittografia accompagna da sempre quella dell'umanità. È una storia fatta di segreti, di astuzie e di sfide, in cui ogni soluzione ha generato nuove domande e ogni codice ha attirato la curiosità di chi voleva violarlo.



Nei secoli, la crittografia ha conosciuto una trasformazione radicale: da semplice gioco di sostituzioni e trasposizioni è diventata una scienza vera e propria, fondata su basi matematiche sempre più sofisticate. Dalla scitala spartana ai cifrari polialfabetici, fino ai moderni algoritmi a chiave pubblica, il filo conduttore è sempre lo stesso: garantire che un messaggio possa giungere integro solo al destinatario scelto, impedendo a chiunque altro di comprenderlo. Ma se la storia ci ha insegnato che nessun codice è eterno, oggi siamo di fronte a un salto concettuale senza precedenti.

Con l'avvento della meccanica quantistica, la crittografia non si affida più alla difficoltà di un calcolo, ma alle leggi stesse della natura. Un singolo fotone, irripetibile e fragile, può diventare il custode di un bit di informazione. Qualsiasi tentativo di intercettarlo o copiarlo lo altera in modo irreversibile, lasciando tracce indelebili del passaggio dell'intruso. Per la prima volta, la sicurezza non si fonda più su ipotesi matematiche o sulla limitata potenza dei computer, ma su principi fisici che nessun progresso tecnologico potrà mai aggirare.

Questa rivoluzione ha implicazioni che vanno ben oltre il mondo della ricerca. Se la crittografia classica rischia di essere infranta dai computer quantistici del futuro, la crittografia quantistica promette comunicazioni inviolabili, sicure per definizione. Già oggi, esperimenti in fibra ottica e collegamenti satellitari mostrano che questo scenario non appartiene soltanto alla fantascienza: reti quantistiche per la distribuzione sicura delle chiavi sono già in fase di sperimentazione e aprono la strada a una nuova infrastruttura globale della sicurezza.

La conferenza invita a intraprendere un viaggio che unisce memoria e innovazione: dalla curiosità degli antichi al rigore dei matematici moderni, fino al sorprendente linguaggio della fisica quantistica. È un cammino che attraversa epoche diverse ma conserva lo stesso interrogativo: come custodire ciò che è prezioso, come garantire fiducia tra le persone e tra le società.