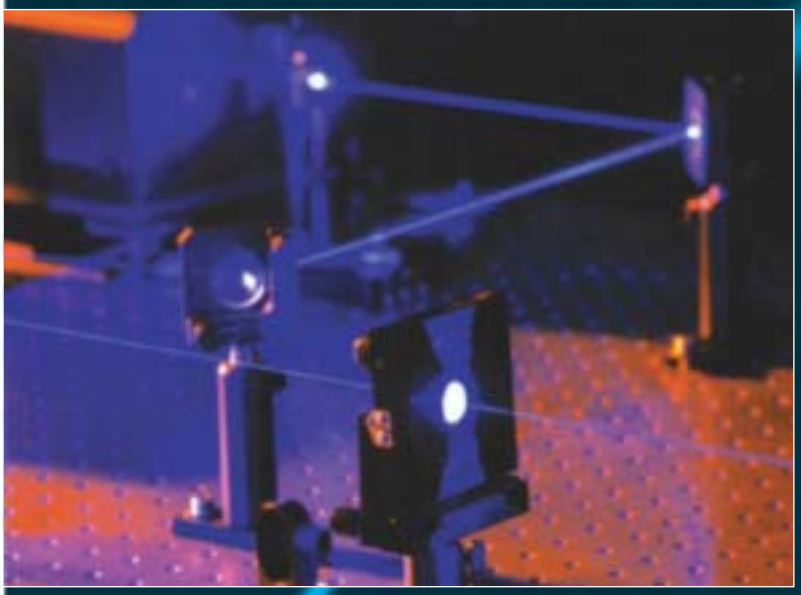

L'Elaborazione
Quantistica
dell'Informazione
ELSAG

L’elaborazione quantistica dell’informazione



L’elaborazione quantistica dell’informazione

L’elaborazione quantistica dell’informazione è un’area di ricerca in rapida evoluzione che abbraccia numerose discipline: comunicazioni, calcolo, teoria e tecnologie dell’informazione, ottica, nanotecnologie, metrologia. Questo campo, in cui numerosi gruppi di studio sono attivi in tutto il mondo, ha un potenziale d’impatto rivoluzionario sull’intero settore dell’Information Technology.

Tutti i dispositivi e i processi tecnologici che l’uomo ha realizzato per la vita di ogni giorno sono basati su effetti fisici, dalla costruzione dei primi utensili di pietra fino alle più recenti applicazioni dell’ingegneria genetica.

Con la fine della terza decade del ventesimo secolo è nata una nuova fisica, necessaria a spiegare i fenomeni che caratterizzano il mondo microscopico; si è verificata una vera e propria rivoluzione quantistica, che ha cambiato il linguaggio della scienza modellando il comportamento del mondo microscopico attraverso le leggi della meccanica quantistica. Solo in anni recenti, però, si è cominciato a pensare di riferirsi ai fenomeni del mondo quantistico per creare dispositivi utili all’uomo: tipicamente, dispositivi per il trattamento dell’informazione. Si è infatti capito che i fenomeni quantistici sono più ricchi di quelli descritti dalla fisica classica poiché, attingendo ad essi, si può creare una tecnologia in grado di risolvere problemi irrisolvibili con le tecnologie odierne (classiche).

Siamo ora nel mezzo di una seconda rivoluzione quantistica, la quale sfrutta le leggi di natura emerse nella prima rivoluzione per creare una nuova ingegneria e una nuova tecnologia quantistica che permetterà di progettare, controllare e ingegnerizzare dispositivi quantistici per il trattamento dell’informazione. Gli obiettivi finali sono la creazione di una crittografia inviolabile per legge di natura, lo sviluppo di una nuova metrologia con un’accuratezza superiore di vari ordini di grandezza rispetto alla metrologia classica e la realizzazione concreta e d’interesse industriale di un “calcolatore quantistico” potenzialmente capace di risolvere, in frazioni di secondo, problemi di calcolo la cui soluzione con i più potenti calcolatori odierni richiederebbe in linea di principio un numero di anni con decine di zeri. Nella storia della tecnologia, il maggiore impulso alla realizzazione di strumenti di calcolo sempre più potenti è scaturito dalla necessità di risolvere i problemi del mondo delle comunicazioni. Non sorprende, quindi, che anche in campo quantistico la ricerca della soluzione dei problemi di sicurezza nelle comunicazioni possa alimentare la capacità di produrre una tecnologia di calcolo perfezionata. Una prima applicazione concreta è possibile nell’ambito della crittografia.

La crittografia quantistica

Ai primordi della crittografia, la sicurezza di un cifrario dipendeva dalla segretezza di tutta la procedura di cifratura e decifratura. Nella crittografia moderna, queste due operazioni sono di pubblico dominio: la sicurezza è legata alla segretezza della chiave utilizzata per cifrare il messaggio.

Claude Shannon, lo scienziato statunitense considerato il padre della comunicazione digitale, ha dimostrato che un messaggio può essere reso inviolabile da qualunque spia applicando metodi come il cosiddetto "blocco usa-e-getta" (*"one time pad"*), in cui la chiave è lunga quanto il messaggio, è del tutto casuale e viene usata una sola volta. Per poter utilizzare il *one time pad*, occorre innanzi tutto produrre chiavi segrete realmente casuali e rinnovarle con frequenza elevata. Anche la sicurezza di questo metodo dipende poi dalla sicurezza relativa alla distribuzione e alla conservazione delle chiavi: il problema consiste quindi nel come "distribuire" in sicurezza le chiavi ai due (o più) interlocutori. La meccanica quantistica consente di risolvere tale problema, in quanto è possibile distribuire coppie di chiavi identiche in modo assolutamente sicuro, garantendo nel contempo la perfetta casualità della sequenza di bit che le compongono.

La crittografia quantistica è una nuova tecnologia che permette la generazione e la distribuzione di chiavi crittografiche tra vari utenti che intendano comunicare in modo segreto. Non è un nuovo criptosistema ma, più propriamente, un sistema di distribuzione di chiavi assolutamente sicuro.

I vantaggi della crittografia quantistica rispetto a quella classica sono essenzialmente due:

- La distribuzione della chiave quantistica avviene contemporaneamente alla sua generazione. Due utenti che dispongano di un canale "quantistico" con tutta la componentistica necessaria e di un canale pubblico (linea telefonica, rete LAN, Internet) possono generare e condividere le chiavi per i loro messaggi segreti senza alcuna necessità di incontrarsi preventivamente per scambiarsele.
- La sicurezza della chiave quantistica è intrinsecamente assoluta, a differenza delle chiavi di tipo classico in cui il livello di sicurezza dipende essenzialmente dalla complessità computazionale di alcune procedure di calcolo quali, ad esempio, la fattorizzazione di grandi numeri. Le chiavi crittografiche classiche sono intrinsecamente sempre più vulnerabili per i continui progressi sia teorici (algoritmi di decifrazione) che tecnologici (potenza di calcolo): in un prossimo futuro, le prime realizzazioni sperimentali di computer quantistici potrebbero violare in tempi brevissimi qualunque chiave classica, per quanto lunga. Gli utenti che ricorrono a chiavi crittografiche quantistiche, invece, sono in grado di accertare direttamente se vi siano stati tentativi d'intercettare la chiave durante la sua generazione, e quindi possono decidere se utilizzarla o meno.

Un sistema di crittografia quantistica in forma prototipale è stato realizzato da Elsag – azienda leader nell'Information Technology italiana, da lungo tempo attiva in ricerche nel campo del quantum information processing – che fin dal 2001 ha istituito un Laboratorio di ottica quantistica presso la propria sede di Genova.

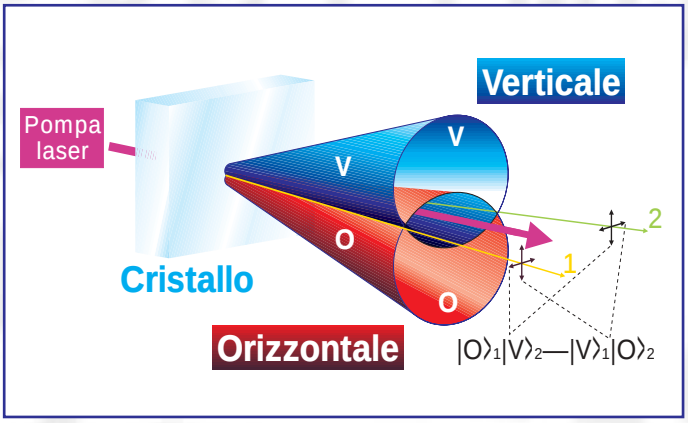
Fotoni "entangled"

Il sistema sviluppato presso Elsag appartiene alla cosiddetta "seconda generazione" della crittografia quantistica, in cui le chiavi per una coppia di utenti vengono generate a partire da sequenze di coppie di fotoni entangled in polarizzazione.

Il concetto di *"entanglement"*, definito da Erwin Schrödinger come "la peculiarità della meccanica quantistica", è basato sul principio di sovrapposizione degli stati e sulla non separabilità degli stati delle parti di un sistema composto. Coppie di fotoni entangled in polarizzazione possono essere create quando un fascio laser attraversa un cristallo non-lineare come il beta borato di bario; il cristallo converte un fotone ultravioletto in due fotoni di energia più bassa (nell'infrarosso vicino), l'uno polarizzato orizzontalmente (cono rosso), l'altro polarizzato verticalmente (cono blu). I fotoni che viaggiano lungo l'intersezione dei due coni non hanno una polarizzazione definita, ma le loro polarizzazioni risultano complementari all'atto della misura.

Consideriamo due fotoni entangled in polarizzazione e pensiamo di distribuirli a due utenti, che chiameremo "Alice" e "Bob", situati ad una certa distanza dalla sorgente dei fotoni. Quando Alice esegue una misurazione sul suo fotone per sapere se è polarizzato orizzontalmente o verticalmente, ciascuno dei due risultati è ugualmente probabile.

La misurazione da parte di Bob ha la stessa probabilità, ma l'entanglement garantisce che il risultato della sua misura sia anticorrelato a quello ottenuto da Alice: se Alice vede un fotone polarizzato orizzontalmente, Bob lo vede verticale e viceversa; questo a patto che gli apparati di misura siano ruotati dello stesso angolo. Prima che venga effettuata la misurazione, i due fotoni non hanno polarizzazione propria: l'entanglement garantisce che le due misure ottenute siano opposte.



La sovrapposizione quantistica e il collasso dello stato all'atto della misura permettono quindi la generazione di sequenze di bit identiche (a meno di complementare una delle sequenze).
Le sequenze, inoltre, sono perfettamente casuali, essendo uguali le probabilità di ottenere – come risultato della misura – una polarizzazione verticale o una polarizzazione orizzontale.

Distillazione della chiave

Tuttavia, per garantire l'assoluta sicurezza non basta una sola base, ma occorre che Alice e Bob misurino con due basi di polarizzazione ciascuno. Nel protocollo più diffuso, il cosiddetto *"BB84",* le basi sono verticale/orizzontale e +45º/-45º. Grazie alla proprietà di invarianza rotazionale dello stato quantistico della coppia, l'anticorrelazione viene preservata a prescindere dalla base usata per la misura.
In effetti, Alice e Bob misurano su una o sull'altra base in maniera casuale e solo nei casi in cui le due basi scelte risultino uguali si vedrà la perfetta anticorrelazione.
Ciascun utente è pertanto equipaggiato con apparecchiature opto-elettroniche atte a rilevare singoli fotoni (*single photon avalanche diodes*), ad etichettarli temporalmente (*timestamp*) per sincronizzare la distillazione, e a scegliere casualmente una base (*beam splitter*) su cui misurare la loro polarizzazione.
Successivamente alle misure, gli utenti procedono ad uno scambio d'informazioni, di tipo classico, sulle basi utilizzate, ma ovviamente non sulle misure ottenute.
Dopo questa fase (in gergo chiamata *sifting*), è possibile ricavare la sequenza di bit condivisa dagli utenti da cui poi distillare la chiave segreta.

Sicurezza

Una spia che cerchi d'intercettare, misurare e rimandare uno dei fotoni della coppia (*intercept-resend strategy*), distrugge la correlazione intercorrente tra essi e pertanto introduce inevitabilmente degli errori nella sequenza di bit. Inoltre, un teorema della meccanica quantistica (*no-cloning theorem*) stabilisce che non si possono effettuare copie perfette di uno stato quantistico.

In pratica, i due utenti si scambiano pubblicamente un sottoinsieme delle proprie sequenze di bit che verrà poi scartato: l'eventuale presenza di una spia viene svelata da un'anomala percentuale di errori in questa sottostringa. I bit della sequenza condivisa, sopravvissuti dopo aver scartato quelli sacrificati in questa operazione, non sono mai stati rivelati pubblicamente e costituiscono la chiave segreta.

La chiave "quantistica" può essere utilizzata dagli utenti che l'hanno distillata in vari scenari applicativi: in pratica, nell'ambito di qualunque applicazione che richieda comunicazioni sicure e con qualsiasi algoritmo di cifratura a chiave segreta.

Prestazioni e prospettive

Nel Laboratorio di ottica quantistica Elsag è stato realizzato un sistema crittografico quantistico basato su fotoni entangled, funzionante su distanze dell'ordine dei km con prestazioni prolungate dell'ordine dei kbit di chiave netta al secondo.

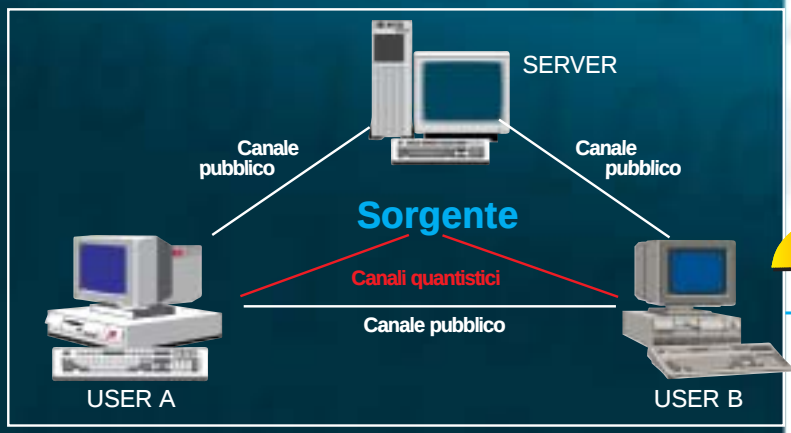
Il sistema è composto da un server e da due user unit collegate al server con canali quantistici in fibra ottica. L'architettura software del sistema è costituita da una serie di componenti configurabili, distribuiti su una rete di computer su Local Area Network. Gli utenti possono utilizzare il sistema attraverso interfacce grafiche user-friendly.

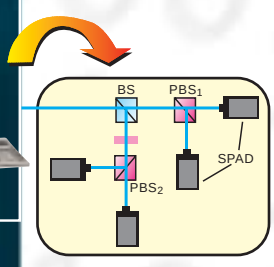
Una libreria software ottimizzata realizza con elevata efficienza il protocollo BB84 e tutte le procedure (classiche) necessarie per la distillazione completa della chiave, tra cui la correzione d'errore e l'autenticazione degli utenti. Il sistema mette a disposizione degli utenti anche altre funzionalità, tra cui il monitoraggio dei dati provenienti dal canale quantistico. In fase operativa, inoltre, il sistema si rivela dotato di grande robustezza.

L'ottimizzazione delle tecniche di generazione dell'entanglement e delle procedure di accoppiamento in fibra ci permette di produrre un elevato numero di coppie entangled di elevata purezza (565 coppie / [milliwatt x mm di cristallo x secondo]). Nel sistema Elsag l'alto grado di efficienza ha reso possibile una sostanziale riduzione dei costi e della dimensione della sorgente di fotoni entangled. È stata inoltre messa a punto e brevettata un'originale procedura di sincronizzazione tra i due utenti.

Il prototipo del Laboratorio si sta via via compattando, divenendo, nello stesso tempo, sempre più potente. Gli sviluppi in corso sono volti principalmente alla miniaturizzazione della sorgente e dei dispositivi di ricezione e misura dei fotoni, nonché all'estensione delle dimensioni della rete di utenti. L'architettura del sistema è intrinsecamente orientata alla gestione di più unità utente, grazie a scelte progettuali che la rendono assai flessibile e agevolano la sua espansione, non solo nel numero di unità, ma anche dal punto di vista geografico (Local and Metropolitan Area Network).

L'adozione di nuove tecnologie e nuovi materiali nonché il passaggio a lunghezze d'onda tipiche delle telecomunicazioni (1.55µm) consentiranno la realizzazione di un sistema per la distribuzione di chiavi su distanze dell'ordine delle centinaia di km e bit rates superiori al megahertz.





Una Società Finmeccanica

Via Puccini, 2 - 16154 Genova
Tel. +39 01065821 - Fax +39 0106582898 - E-mail: quantum@elsag.it
www.elsag.it