Cos'è la Crittografia Quantistica?

di Andrea Pasquinucci

Breve semplice guida alla comprensione di un ramo della ricerca che apre prospettive notevolissime e che vede l'Italia in prima linea. Raccontato da uno dei protagonisti

da SECOQC ai Computer Quantistici

Roma - Negli ultimi mesi si è sentito parlare molto di Crittografia Quantistica: annunci, press-realese, progetti, finanziamenti e prototipi commerciali. Verso la fine del 2003 sono comparsi sul mercato i primi due prototipi commerciali da parte di "MagiQ Technologies" (New York) e "id Quantique" (Ginevra). Inoltre altre aziende, quali NEC, Toshiba e Hewlett-Packard, stanno sviluppando propri sistemi di Crittografia Quantistica che presto appariranno sul mercato.

La Crittografia Quantistica ha già catturato l'interesse di governi, di militari ed agenzie di sicurezza, di banche ed istituzioni finanziarie.

Ad esempio, Visa International, l'azienda internazionale di carte di credito, sta sperimentando questa tecnologia ed altre banche e istituzioni finanziare hanno annunciato il loro interesse. L'Unione Europea ha finanziato il progetto SECOQC, iniziato il 1 Aprile 2004 e da alcuni indicato come il progetto "anti-echelon" europeo per lo sviluppo sia della ricerca che della implementazione tecnologica e commerciale della Crittografia Quantistica (la Press Release è disponibile sul sito quantenkryptographie.at e la descrizione del progetto sul sito www.arcs.ac.at/quanteninfo).

Il progetto ha un budget di 11,4 Milioni di euro in 4 anni, vi partecipano 41 partner in 12 paesi europei, e per l'Italia vi sono l'Università di Pavia, il CNR, la Scuola Normale Superiore di Pisa ed il Politecnico di Milano.

Ma che cosa è la Crittografia Quantistica?

Per rispondere a questa domanda conviene fare un passo indietro. Già negli anni '70 i fisici teorici si chiedevano se fosse possibile utilizzare le teorie che descrivono le particelle elementari, atomiche e sub-atomiche, cioe` la Meccanica Quantistica e la Teoria dei Campi, per realizzare direttamente qualche cosa di veramente nuovo. Infatti le leggi che regolano il mondo atomico e sub-atomico sono alquanto differenti da quelle a cui siamo abituati nella vita di tutti i giorni.

Questo le rende difficili da comprendere ma sono al contempo potenzialmente foriere di applicazioni impensabili altrimenti.

Ad esempio, quando si osserva una particella sconosciuta, si modificano sempre alcune delle sue proprietà: non e` possibile una osservazione senza una interazione e la modifica dello stato della particella sconosciuta. Ovviamente, nell'esperienza quotidiana le cose sono ben diverse: possiamo osservare quanto vogliamo un oggetto sconosciuto senza modificarlo affatto. Ed ancora, nel mondo delle particelle elementari non esiste la possibilità di una fotocopiatrice perfetta, non si possono fare copie esatte di particelle se non in particolari ed eccezionali condizioni.

Uno dei primi risultati teorici è stata l'invenzione dei Computer Quantistici. Questi sono elaboratori che funzionano seguendo la logica delle leggi della Meccanica Quantistica e quindi sono (potenzialmente) in grado di fare i conti in modo molto diverso da quello noto a tutti noi. In particolare gli elaboratori quantistici saranno in grado di risolvere alcuni difficili problemi matematici istantaneamente. Tra questi problemi vi sono quelli su cui si basano molti degli algoritmi crittografici moderni, quali ad esempio il famoso RSA.

In altre parole, se fosse possibile costruire oggi un elaboratore quantistico, questo sarebbe in grado quasi istantaneamente di ottenere da una chiave pubblica di qualunque lunghezza, la corrispondente chiave privata utilizzata dagli algoritmi Asimmetrici quali RSA. Questi algoritmi sono utilizzati oggi per l'identificazione delle parti e la creazione e scambio delle chiavi per cifrare le connessioni. Poterli "rompere" vorrebbe dire rendere del tutto insicuri smart-card, firme e certificati digitali, navigazione in internet, email cifrate ecc.ecc. Al momento comunque non siamo ancora in grado di costruire un elaboratore quantistico, e le stime più ottimistiche indicano che ci vorranno ancora 20 anni.

La soluzione e il BB84

La Crittografia Quantistica, nata un paio di anni prima degli elaboratori quantistici, offre però una, per il momento parziale, soluzione ai possibili problemi che avverranno all'arrivo degli elaboratori quantistici. La Crittografia Quantistica permette di creare e scambiare chiavi segrete da utilizzare poi per cifrare le comunicazioni, pertanto un nome più appropriato è "Quantum Key Distribution".

I sistemi attuali di Crittografia Quantistica si basano sul codificare un bit informatico in una proprietà di un singolo fotone, che è il costituente fondamentale della luce e delle radiazioni elettromagnetiche. Come abbiamo già detto, la Meccanica Quantistica garantisce che se un fotone è intercettato da un attaccante nel suo tragitto tra le due parti che stanno generando la chiave segreta, alcune delle sue proprietà vengono modificate e l'attacco può essere perciò rilevato. In altre parole la Meccanica Quantistica garantisce l'individuazione di qualunque tentativo di attacco al processo di generazione e scambio della chiave.

Descriviamo brevemente ora il primo e principale protocollo della Crittografia Quantistica, il "BB84" dai nomi di Bennett e Brassard che lo proposero nel 1984. In questo protocollo un bit viene codificato in una particolare polarizzazione di un fotone a scelta fra quattro fissate. Due polarizzazioni vengono interpretate come il valore 0, le altre due come il valore 1.

Supponiamo che Alice e Bob vogliano utilizzare il BB84 per creare una chiave segreta. Alice sceglie a caso una delle 4 polarizzazioni, crea un fotone così polarizzato e lo invia a Bob, e ripete questa operazione per ogni bit della chiave che si vuole creare.

Bob riceve il fotone ma non sa quale polarizzazione ha scelto Alice, e deve effettuare una misura sul fotone per scoprirlo. La particolare scelta delle 4 polarizzazioni lo obbliga a scegliere fra due diverse misure non compatibili, una misura gli permette di scoprire due delle polarizzazioni, l'altra misura le altre due polarizzazioni. Se Bob sceglie la misura sbagliata rispetto alla polarizzazione usata da Alice, il risultato della misura è casuale, ovvero 0 od 1 a caso. Il punto fondamentale per la sicurezza è che anche Eve si trova nella stessa situazione di Bob: se Eve intercetta dei fotoni deve scegliere tra le due misure possibili e se sceglie quella sbagliata ottiene un risultato casuale.

Alla fine dell'invio dei fotoni, Alice e Bob scartano tutti i fotoni/bit per i quali Bob ha scelto la

misura sbagliata. A questo punto Alice e Bob hanno creato e si sono scambiati una chiave segreta casuale detta "sifted key". Come fanno a essere sicuri che Eve non l'ha intercettata?

La risposta è semplice, anche se la dimostrazione è un po' complicata e richiede l'intervento dei principi primi della Meccanica Quantistica.

Se Eve ha in qualche modo intercettato i fotoni nel loro tragitto tra Alice e Bob, grazie alle leggi della Meccanica Quantistica ed alla particolare preparazione delle quattro polarizzazioni e delle due misure possibili, li ha per forza modificati. Infatti come abbiamo detto, le fotocopiatrici perfette non esistono in Meccanica Quantistica. Se Eve ha intercettato e modificato dei fotoni, le misure di Bob avranno degli errori rispetto alle polarizzazioni inviate da Alice. Quindi, in teoria, se la sifted key di Bob è diversa da quella di Alice, vuol dire che Eve ha intercettato i fotoni e che la chiave non è sicura poiché Eve è a conoscenza di almeno parte di essa.

Purtroppo le cose non sono così facili. Infatti gli strumenti non sono perfetti e vi sono sempre degli errori, fotoni persi o che non sono rilevati correttamente. Questi sono i cosiddetti "errori sperimentali" e sono sempre presenti. Sembrerebbe quindi che siamo giunti ad un punto morto: vi sono sempre errori, ma se ci sono errori vuol dire che Eve ha intercettato la chiave poiché è molto difficile distinguere con sicurezza tra errori sperimentali ed errori dovuti ad Eve.

La soluzione a questo apparente insolubile problema, è in realtà relativamente semplice. Prima di tutto si assume che tutti gli errori siano sempre dovuti a Eve. Poi Alice e Bob debbono applicare alla sifted key due ulteriori fasi del protocollo.

La prima si chiama "Reconciliation" od "Error Correction" e permette ad Alice e Bob di eliminare tutti gli errori nella sifted key di Bob ed al contempo stimare la percentuale di errori trovati. Se questa percentuale è inferiore all'11%, allora si può passare alla fase seguente detta "Privacy Amplification".

In questa fase la chiave segreta viene modificata secondo una procedura tale che l'informazione che nel caso Eve ha sulla chiave segreta viene ridotta praticamente a zero.

Questo è possibile perché se Eve ha introdotto errori solo per al più l'11%, vuol dire che la sua conoscenza della sifted key è sufficientemente ridotta, conosce pochi bit della chiave, e quindi modificando appropriatamente la chiave segreta Alice e Bob possono eliminare i bit a conoscenza di Eve.

Queste ultime due fasi possono essere realizzate anche pubblicamente poichè le informazioni scambiate tra Alice e Bob non aiutano Eve a fare lo stesso. Bisogna inoltre notare che in queste due fasi la lunghezza della chiave viene ridotta. A seconda delle procedure utilizzate la chiave segreta finale può anche essere lunga solo 1/8 del numero di fotoni inizialmente inviato da Alice.

Una volta in possesso della chiave segreta, e con la garanzia data dalla meccanica quantistica che Eve non ne e` a conoscenza, Alice e Bob la possono usare per cifrare un messaggio e scambiarselo. Il motivo per cui la Crittografia Quantistica cosi` formulata non puo` essere usata per scambiarsi direttamente messaggi è che la presenza di Eve viene rilevata solo DOPO aver concluso l'invio dei fotoni, nella fase della Error Correction.

L'alternativa

La Crittografia Quantistica è quindi un'alternativa all'uso dei protocolli a Chiave Pubblica, quali ad esempio RSA, per generare e scambiare le chiavi segrete. La differenza principale tra i protocolli a Chiave Pubblica e la Crittografia Quantistica è che quest'ultima non teme attacchi basati sulla potenza di calcolo degli elaboratori o sugli sviluppi di tecniche matematiche che permettono già oggi di rompere sistemi a Chiave Pubblica che adottano chiavi pubbliche/private troppo corte.

D'altra parte, la Crittografia Quantistica richiede oggi l'uso di singoli fotoni, e non è facile creare e rilevare singoli fotoni con le tecnologie odierne anche se lo sviluppo in questo campo è molto rapido.

Inoltre è necessario avere a disposizione un'unica fibra ottica, il che limita la distanza di applicazione, ad oggi il massimo raggiunto è 150 chilometri.

Anche in questo caso le tecniche sono in rapido sviluppo, e si prevede che fra qualche anno saranno disponibili altre implementazioni della Crittografia Quantistica, anche via satellite, con la possibilità di copertura dell'intero globo terrestre.

Infine, oltre al BB84 altri protocolli sono stati proposti ed implementati, ma in ogni caso le leggi fisiche su cui si basano sono le stesse e le loro logiche sono molto simili a quella del BB84 anche se vengono sfruttate differenti proprietà dei fotoni e/o procedure leggermente diverse.

Ulteriori informazioni e link sulla Crittografia Quantistica si possono trovare sul sito ucci.it/.

Andrea Pasquinucci

http://www.ucci.it/

Libero Professionista in Sicurezza Informatica, PhD in Fisica Teorica, esperto di crittografia, di sicurezza delle reti e dei sistemi operativi. Membro del Comitato Tecnico-Scientifico CLUSIT, insegna presso l'Università degli Studi di Milano.

Andrea Pasquinucci e collaboratori si occupano di Crittografia Quantistica a livello di ricerca universitaria sin dal 1997 e partecipano tramite l'Università di Pavia al progetto SECOQC.