Solo un Paese che investe nella ricerca scientifica e nei propri giovani può avere un futuro

Barack Obama, 2010

La ricerca è particolarmente attiva sul fronte della sicurezza delle comunicazioni (Getty Images)

SELEX ES

Le password di luci e fotoni Così cambierà la security

di Barbara Millucci

Password fatte di luce. Tra una decina di anni, useremo telefonini e computer quantistici che funzioneranno con atomi e molecole, al posto dei processori. Diremo addio alla tecnologia al silicio, troppo lenta e costosa, per entrare nel mondo dell'infinitamente piccolo dove tutto è possibile. I nuovi pc, che seguono le leggi della fisica quantistica, al momento hanno forme bizzarre, con schermi sospesi in aria, immersi in liquidi, sottoposti a onde elettromagnetiche, incapsulati a temperature insolite. Ai bit preferiscono i qubit in grado di assumere non solo due (0-1) ma un numero infinito di stati, moltiplicando esponenzialmente l'informazione che la macchina può gestire. Con atomi e molecole come memoria, avremo potenzialità di calcolo impressionanti. Con possibilità di trasferire informazioni in modo sicuro. Perché ogni tentativo di alterare una comunicazione tramite un terzo incomodo altererebbe il messaggio trasmesso.

«La crittografia quantistica è un protocollo per scambiare e generare in assoluta sicurezza tra due utenti delle chiavi segrete tramite particelle elementari, senza sfruttare le leggi classiche della fisica», spiega Fabio Bovino, responsabile del Quantum Technologies Lab per Selex ES (gruppo Finmeccanica), specializzata in meccanica quantistica. Qui si realizzano sensori sensibilissimi, calcolatori di nuova generazione e applicazioni per telefonini in grado di generare chiavi crittografiche quantistiche. Niente a che vedere con password da ricordare. Solo fasci luminosi. Dispositivi in grado di controllare la luce, anzi dominare i fotoni per poi utilizzarli negli apparati elettronici. I telefonini del futuro funzioneranno così. Con una sicurezza infallibile, perché dettata dalle leggi della natura. Grazie a sensori di luce introdotti nei microchip degli smartphone «sono stati creati dei prototipi che useremo nella vita di tutti i giorni. La comunicazione avviene tramite uno scambio di fotoni che, a loro volta, permettono un passaggio sicuro di chiavi segrete su fibra ottica», afferma lo scienziato.

TELETRASPORTO

Il teletrasporto è realtà, non fantascienza come nei film di Star Trek. Per la prima volta una particella di luce è stata scaraventata in un cristallo a 25 km di distanza su fibra ottica. L'esperimento di un' equipe di ricercatori dell'Università di Ginevra batte il record di 6 km di teletrasporto. Si parla di trasporto dello stato quantistico del fotone, la creazione di una sua perfetta copia, senza doverlo fisicamente muovere. Una tecnica che potrebbe rendere le nostre comunicazioni sicure e impossibili da decifrare. A prova di qualsiasi hacker che usi le leggi fisiche della materia.

Ma come funzioneranno? D al bancomat, grazie a un dispositivo collegato a un'unità centrale, scaricheremo chiavi crittografiche sullo smartphone, in modalità sicura. Con questi codici di luce accederemo poi ai servizi del settore pubblico, banche, sanità, voto elettronico, shopping on line, in gran segreto e tutelando la privacy. «Solo negli ultimi tre anni, gli attacchi di cybercrime sono cresciuti del 245%, con danni quantificabili in 500 miliardi di euro. Se ne contano 1.150, di cui 39 riguardano il nostro Paese», continua Bovino. La crittografia quantistica proteggerà i nostri sistemi di sicurezza nazionale ma anche le reti energetiche, le comunicazioni, i trasporti. Non a caso, ogni Paese ha in atto progetti di tecnologia quantistica di sicurezza nazionale. Qualche esempio? «Toshiba in Inghilterra, Telefonica in Spagna, Thales in Francia, i cinesi tramite collegamenti satellitari. Nel Maryland, c'è un programma di ricerca da 80 milioni mentre l'ente governativo Battelle sta creando una rete di mille chilometri, dalla propria sede fino alla Casa Bianca. Barack Obama, accanto al telefono rosso, avrà un dispositivo per comunicare protetto dalla crittografia quantistica», continua Bovino, docente a La Sapienza di Roma. «Oggi i sistemi che esistono per la protezione dell'informazione si basano su algoritmi, più o meno complessi. Ma l'impenetrabilità di un sistema non sta nella sua trasformazione matematica, quanto nella sicurezza della chiave. Scambiando l'informazione cifrata tramite un algoritmo come lo conosciamo oggi, quel contenuto non sarà mai sicuro». Ecco un esempio: «Il numero delle chiavette per accedere al banking on line, che appare sempre diverso, è associato all'istante in cui è stato generato. E' però insicuro perché genera chiavi diverse, ma a partire da una iniziale che è sempre la stessa. Ogni nuovo codice è in qualche modo legato al precedente. La sicurezza della crittografia quantistica consiste nel fatto che ogni nuova chiave generata è statisticamente indipendente dalla precedente». La fisica quantistica permette di generare in due luoghi distanti stringhe di bit correlati, senza che nessuna copia possa essere ricostruita altrove. «Sono i cosiddetti stati quantistici entangled, cioè accoppiati: quando si agisce su uno dei due fotoni, il gemello ovunque si trovi reagirà istantaneamente».

Proteggeranno i trasporti e le reti. E nel Maryland c'è già un piano da 80 milioni

Anche Obama per comunicare avrà un telefono protetto accanto a quello «rosso»

Determinato Fabio Bovino, responsabile del Quantum Technologies Lab di Selex Es

Non dobbiamo più pensare «al mondo in termini di cose, che stanno in questo o quello stato, bensì in termini di processi, cioè passaggi da un'interazione all'altra» scrive Carlo Rovelli in *La Realtà non è come ci appare* (2014). La prima transizione di denaro tramite fotoni entangled per creare codici di comunicazione indecifrabili è stata da poco sperimentata anche dall'Università di Vienna fra il municipio e una banca. In pratica, i fotoni disturbando lo stato di uno, disturbano automaticamente anche l'altro, anche se si trovano lontanissimi tra loro. I fotoni correlati sono stati generati inviando un laser attraverso un cristallo che li ha divisi in due. Un fotone di ogni coppia correlata è stato poi inviato dalla banca al municipio su fibra ottica. Entrambi avevano a disposizione una password. Chiunque, intercettando i fotoni, secondo il principio d' indeterminazione di Heisenberg, ne avrebbe cambiato il comportamento, lasciando una traccia e allertando mittente e destinatario della presenza di un intruso. «Programmare» l'universo e renderlo sicuro non è mai stato così facile.