LA GIORNATA

La scelta di Conte

di Laura Pertici

ASCOLTA

La comunicazione quantistica e un mondo a prova di hacker
di Angelo Bassi

(ansa)

Come trasmettere una chiave a due interlocutori senza che altri ne

vengano in possesso?

04 LUGLIO 2022 ALLE 23:59

3 MINUTI DI LETTURA

È in corso un intenso dibattito tra i crittografi per trovare nuove soluzioni contro il numero crescente di attacchi informatici. Un problema rilevante è che nessuna comunicazione è veramente sicura, a meno che non venga realizzata tramite quella che, in linguaggio tecnico, viene chiamata crittografia simmetrica, la quale prevede che il mittente e il destinatario, e solo loro, possiedano due copie esatte della chiave utilizzata per criptare e decrittare il messaggio. Ma come fare per trasmettere la chiave ai due interlocutori senza che, nel mentre, altri ne vengano in possesso? I metodi classici per garantire ciò sono molto costosi, e per questo sono utilizzati solamente in circostanze speciali, quali in ambito diplomatico e militare.

La comunicazione quantistica, invece, permette di generare e trasmettere le due copie della chiave in modo completamente sicuro, e per questo si sta imponendo all'attenzione dei governi. La Cina, ad esempio, da alcuni anni possiede una rete quantistica funzionante, utilizzata per usi governativi, commerciali e presumibilmente anche militari. Anche l'Italia concorre allo sviluppo di questa tecnologia con due importanti iniziative: la prima è la costituzione di un consorzio di università e imprese del settore, coordinate dall'Inrim (Istituto nazionale di Ricerca metrologica) di Torino, volto allo sviluppo di una rete nazionale di comunicazione quantistica su fibra ottica; la seconda iniziativa, coordinata da Thales Alenia Space, è finalizzata a sviluppare le tecnologie quantistiche nello Spazio, tra cui anche la comunicazione.

Tecnologia quantistica, la corsa cinese e il nostro futuro

di Angelo Bassi
15 Dicembre 2021

Nel frattempo, la maggior parte delle comunicazioni cifrate nel mondo è realizzata tramite quella che viene chiamata crittografia asimmetrica, in cui mittente e destinatario hanno ciascuno una coppia diversa di chiavi: una chiave della coppia è privata, non condivisa con nessuno, nemmeno tra di loro, mentre l'altra è di pubblico dominio. In questo caso il mittente utilizza la chiave pubblica del destinatario per cifrare il messaggio, che viene comunicato senza curarsi che possa essere intercettato, perché solo il destinatario, l'unico che possiede la chiave privata collegata alla sua chiave pubblica utilizzata dal mittente, è in grado di decrittare il messaggio.

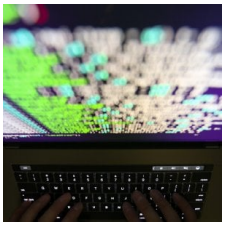
La crittografia asimmetrica ha l'enorme vantaggio di evitare il problema della condivisione di un'unica chiave crittografica, e ciò l'ha resa di gran lunga la più popolare per garantire la sicurezza delle telecomunicazioni; in questo caso, infatti, solo le chiavi per criptare i messaggi sono pubbliche, mentre quelle per decrittare - ciò che serve a un hacker per violare la cifratura - sono private e non vengono divulgate.

C'è tuttavia una potenziale vulnerabilità: è in linea di principio possibile per un hacker ricostruire la chiave privata a partire dalla chiave pubblica, e quindi decrittare il messaggio, perché le due chiavi sono legate da una precisa relazione matematica. Tuttavia, questo processo di ricostruzione richiede un'enorme potenza di calcolo e anche il più potente super-computer classico esistente impiegherebbe un tempo lunghissimo per compiere l'operazione.

La crittografia a chiave pubblica si basa quindi sull'impossibilità pratica (non teorica) di violare la sicurezza del protocollo di crittografia, e per decenni le sue fortune si sono basate su questa ipotesi. Ma nel 1994 Peter Shor sorprese il mondo dimostrando che un computer quantistico è in grado di compiere la stessa operazione in maniera veloce, compromettendo così la gran parte degli attuali sistemi di comunicazione sicura.

La sfida dei supercomputer

di Angelo Bassi
18 Novembre 2021



Per prevenire il problema, si stanno esplorando due strade. La prima prende il nome di crittografia post-quantum: si tratta di nuovi algoritmi classici per generare coppie di chiavi da utilizzare nella crittografia asimmetrica, che non possono essere violati da un computer quantistico.

Questa strada ha il vantaggio di non richiedere un ripensamento radicale delle architetture di comunicazione esistenti, ma ha lo stesso limite degli schemi crittografici che si vuole

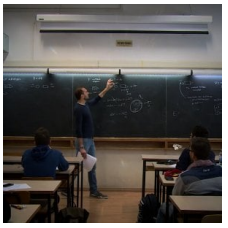
rimpiazzare: non c'è la certezza che un giorno qualcuno non trovi un modo intelligente per violare anche i nuovi protocolli.

E questo è già successo. Nel 2016, il prestigioso Nist (National Istituite for Standard and Technology) americano ha avviato una competizione internazionale per creare un nuovo standard di comunicazione sicura post-quantum; il processo di selezione ha portato nel 2020 all'individuazione di tre schemi crittografici, tra i quali poi scegliere il nuovo standard. Tuttavia, all'inizio di quest'anno un ricercatore dell'Ibm è riuscito a violare uno dei tre sistemi finalisti, riproponendo così la questione della loro effettiva sicurezza.

Oltre i confini della fisica

di Gianluca Di Feo (coordinamento editoriale e testo). Coordinamento multimediale di Laura Pertici. Foto di Mattia Balsamini. Produzione Gedi Visual

20 Ottobre 2021



L'altra strada consiste nell'implementare la crittografia simmetrica tramite la comunicazione quantistica. Come anticipato, questa tecnologia ha l'enorme vantaggio di essere in grado di generare a distanza due copie della stessa chiave, in modo intrinsecamente sicuro: si può cioè dimostrare che, se implementata correttamente, qualunque tentativo di attacco esterno durante il processo di generazione delle chiavi può essere rivelato e quindi neutralizzato. Il prezzo da pagare è un (inizialmente costoso) ripensamento degli attuali sistemi classici di comunicazione, che vanno sostituiti con nuovi sistemi quantistici. Potrebbe valerne la pena.

Angelo Bassi è professore di Fisica all'Università degli Studi di Trieste

Argomenti

scienza | meccanica quantistica | tecnologia | fisica | hacker

LEGGI I COMMENTI