Fondazione Compagnia di San Paolo
Quotidiano
18-09-2023
Pagina 15
Foglio 1 / 2
Il Messaggero
Tiratura: 75.729
Diffusione: 60.650

Quando saranno operativi i potentissimi calcolatori quantistici, bisognerà ripensare la sicurezza informatica. Andrea Vesco (fondazione Links): «Le macchine potranno violare qualsiasi sistema»

Password in pericolo con i supercomputer

IL CASO

Sfruttano le proprietà della meccanica quantistica per raggiungere capacità di calcolo e velocità mai viste prima. Ma le stesse caratteristiche che rendono i computer quantistici dei veri fuoriserie dell'informatica possono anche trasformarli nell'arma perfetta per aggredire sistemi bancari, infrastrutture critiche nazionali e sistemi di sicurezza. Un'arma che, nelle mani sbagliate, in un futuro non più tanto lontano potrebbe mettere in ginocchio l'intera rete internet.

Una sfida enorme per la comunità globale di crittografi che lavorano nei centri di ricerca pubblici e privati coordinati dal Nist, l'agenzia governativa americana che si occupa dello sviluppo di nuovi standard tecnologici.

I SISTEMI

Uno sforzo comune racchiuso nell'acronimo PQC, crittografia post-quantistica, ovvero il tentativo di creare sistemi di crittografia talmente sofisticati da poter resistere agli attacchi informatici lanciati dai computer quantistici. Anche l'Europa si sta muovendo. E adesso trova nella città di Torino il nuovo polo di riferimento di un progetto internazionale nato per rendere più sicura l'internet di domani. Con 200 ricercatori all'attivo, fondazione Links - ente strumentale di Compagnia di San Paolo e del Politecnico di Torino - è capofila di un consorzio che coinvolge 11 soggetti tra università e imprese da 4 diversi Paesi europei, e che ha da poco ottenuto un finanziamento triennale di cinque milioni di euro dalla Commissione Europea per il progetto QuBip, nato per sviluppare sistemi di cybersecurity capaci di resistere alla mostruosa potenza di calcolo dei computer quantistici. Per capire la portata di questa rivoluzione basta qualche numero. Per violare un sistema protetto da una password di 10 caratteri che includa anche simboli e numeri, un pc di fascia alta oggi impiega circa 500 anni. Un supercomputer, a seconda della potenza, ci riesce in qualche settimana. Ai computer quantistici basteranno una manciata di secondi. Ma quando si parla di crittografia post-quantistica la vera minaccia del futuro «non saranno più tanto gli attacchi "brute force" (che consistono nell'individuare una password provando tutte le possibili combinazioni di caratteri esistenti, ndr) ma il fatto che queste macchine saranno in grado di rompere tutti quei protocolli e algoritmi che oggi rendono sicura la comunicazione online», spiega Andrea Vesco, responsabile gruppo ricerca cybersecurity in fondazione Links.

LUCCHETTO

Primo bersaglio la cosiddetta "chiave pubblica", cioè quella crittografia che negli ultimi trent'anni è stata usata per creare canali di comunicazione sicuri con i servizi digitali e che viene identificata nel nostro browser dalla dicitura "https" e dall'icona di un lucchetto. I computer quantistici saranno in grado di rompere questa chiave in pochi secondi, intrufolarsi in una rete e leggere le password in diretta, senza bisogno di indovinarle. Insomma, in un mondo post-quantistico nessuno sarà più al sicuro. Conti bancari, caselle di posta e accessi digitali oggi blindatissimi «crolleranno sotto il peso degli attacchi portati dai computer quantistici. Dobbiamo pensare a nuove soluzioni capaci di riadattare i vecchi protocolli in vista di questa transizione, la più grande e difficile che il mondo della sicurezza mondiale abbia mai affrontato», spiega Vesco. Gli addetti ai lavori concordano sul fatto che per la piena operabilità dei computer quantistici bisognerà aspettare almeno un altro decennio, ma la ricerca nel settore intanto procede a passo spedito.

TRAGUARDI

IBM ha già raggiunto traguardi importanti nello sviluppo di hardware quantistici: viene subito in mente Osprey, il nuovo processore a 433 qubit presentato a novembre. Ma il colosso statunitense prevede di lanciare il nuovo chip Condor da 1121 qubit entro la fine dell'anno. Google insegue con il suo Sycamore, che oggi si assesta sui 70 qubit. Entrambi sono capaci di eseguire in pochi secondi dei calcoli che al Frontier di HP, il supercomputer attualmente più veloce al mondo, richiederebbero 47 anni. Con una potenza simile tra le mani, mettere in ginocchio uno smartphone sarà un gioco da ragazzi. E in effetti la vera, grande sfida della crittografia post-quantistica sarà integrare i nuovi protocolli di sicurezza anche nei dispositivi mobili e nei pc tradizionali. «Ovviamente dobbiamo poter utilizzare i device che già abbiamo – spiega Vesco – che da qui a 15 anni aumenteranno di potenza tanto da essere pronti per accogliere il nuovo standard crittografico. Solo così potremo essere davvero al sicuro».

Raffaele d'Ettorre

IBM STA PER LANCIARE IL NUOVO CHIP CONDOR DA 1121 QUBIT: ANCHE PER GLI SMARTPHONE LA CRITTOGRAFIA DOVRÀ ESSERE RIVOLUZIONATA

Il Messaggero

Le domande

1 PERCHÉ SONO UN PERICOLO?

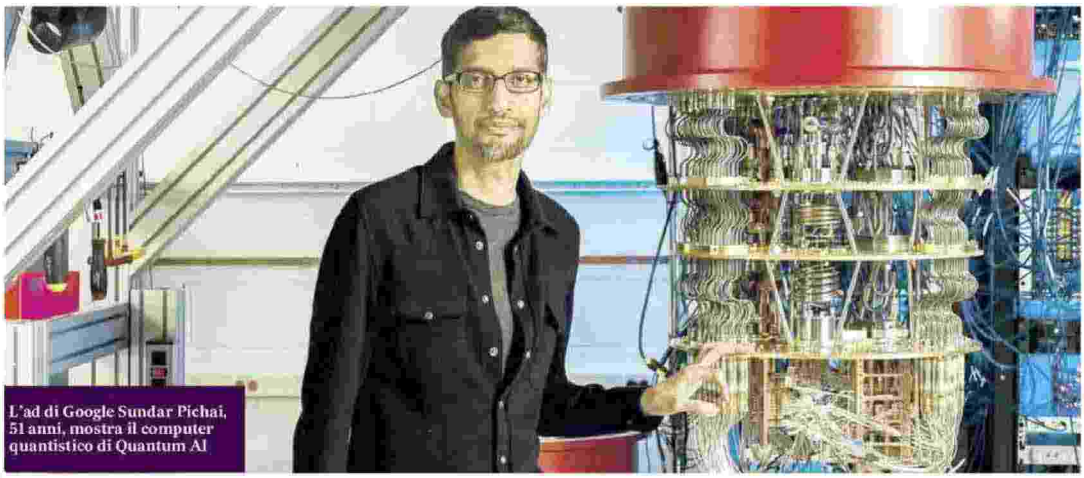
Perché in pochissimi secondi possono violare i sistemi che sono protetti dalla crittografia attualmente in uso

2 COME CI SI DIFENDE?

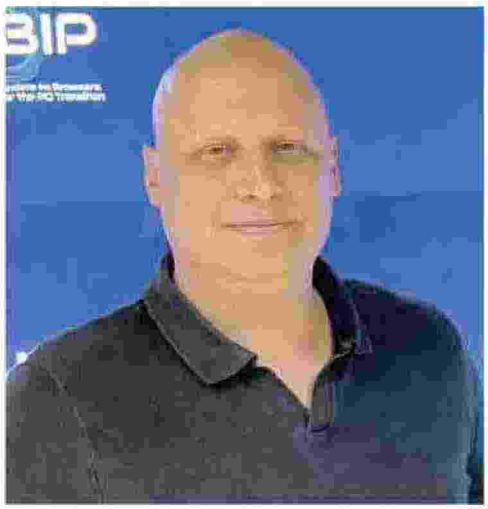
Riadattando i vecchi protocolli di sicurezza in vista della transizione. A Torino se ne sta occupando la fondazione Links

3 COME PROTEGGERE I CELLULARI?

Gli sviluppi hardware consentiranno anche ai dispositivi mobile di integrare i nuovi protocolli, mettendoli al sicuro



L'ad di Google Sundar Pichai, 51 anni, mostra il computer quantistico di Quantum AI



IBM STA PER LANCIARE IL NUOVO CHIP CONDOR DA 1121 QUBIT: ANCHE PER GLI SMARTPHONE LA CRITTOGRAFIA DOVRÀ ESSERE RIVOLUZIONATA

Qui sopra Andrea Vesco, responsabile gruppo ricerca cybersecurity in fondazione Links

vice c
Vesco
mente
essere
nuovo
Solo c
ro al si


Password in pericolo con i supercomputer