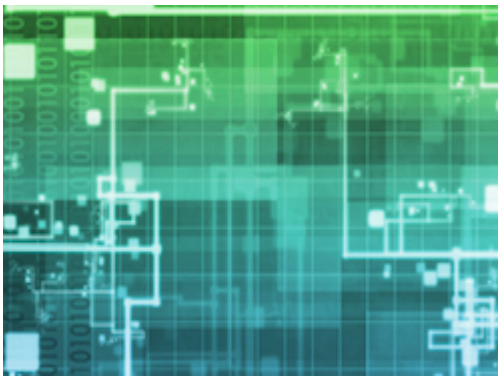
Come tenere al sicuro i dati di crittografia contro la minaccia dei futuri computer quantistici

Quando saranno disponibili i computer quantistici, un algoritmo già esistente metterà in difficoltà le attuali tecniche di crittografia considerate finora sicure. Un progetto finanziato dall'UE sta lavorando per cominciare a trovare una soluzione.



© kentoh, Shutterstock

In un articolo recentemente pubblicato sulla rivista “Nature”, i ricercatori descrivono diversi approcci per sviluppare nuove tecniche di crittografia resistenti agli attacchi quantistici. Un approccio ovvio è sviluppare nuove tecniche di crittografia che evitano di usare le tecniche attuali poiché queste potrebbero non essere altrettanto sicure in futuro.

Il problema della crittografia attuale

Al momento la nostra sicurezza online dipende in gran parte dal sistema conosciuto come RSA (Rivest-Shamir-Adleman) molto usato per la crittografia. Questo dipende dall’uso di chiavi pubbliche che consistono nel prodotto di due numeri primi. Attualmente anche i computer più potenti che abbiamo potrebbero richiedere una grande quantità di tempo per identificare i due numeri primi, un processo conosciuto come fattorizzazione: i supercomputer più potenti impiegherebbero secoli a risolvere il rompicapo.

All’altro capo dei dati crittografati c’è il destinatario del messaggio che ha una chiave privata che consiste in un numero conosciuto solo a lui e al mittente. Usando un’operazione matematica, i due numeri primi necessari per decodificare il messaggio si ottengono con la chiave privata. Se la chiave privata non è intercettata, la codifica è resistente.

Ma adesso che ci sono computer quantistici più potenti dietro l'angolo, il potere di elaborazione necessario per scoprire i numeri primi sarà disponibile, rendendo quello che finora è stato un processo molto sicuro, più vulnerabile. Questo pericolo si conosce dal 1994, quando fu pubblicato un algoritmo per computer quantistici in grado dividere una grande chiave pubblica in due numeri primi nel giro di pochi secondi o minuti.

Ricercatori identificano i primi passi verso una soluzione

Il team di PQCRYPTO (Post-Quantum CRYPTOgraphyfor long-term security) prevedono un approccio su due fronti: accanto all'idea che una soluzione attuabile potrebbe essere basata sullo sviluppo di nuove tecniche di crittografia, suggerisce anche di concentrarsi su tecniche che comportano operazioni matematiche per le quali i computer quantistici non sono efficienti.

I ricercatori sottolineano diversi limiti delle tecniche che dovranno essere sviluppate. Queste dovrebbero ispirare fiducia e non essere troppo costose da applicare e non troppo esigenti per i sistemi di calcolo. Dovrebbero anche evitare chiavi di lunghezza eccessiva. Gli autori insistono su un aspetto importante per lo sviluppo di futuri sistemi di crittografia post-quantistica: un'attenzione sollecita alla standardizzazione poiché tutte le parti dovranno usare gli stessi sistemi crittografici.

Per maggiori informazioni, consultare:
Sito web del progetto PQCRYPTO

Paesi

Paesi Bassi

Progetti correlati

HORIZON 2020

PROGETTO

Post-quantum cryptography for long-term security

PQCRYPTO

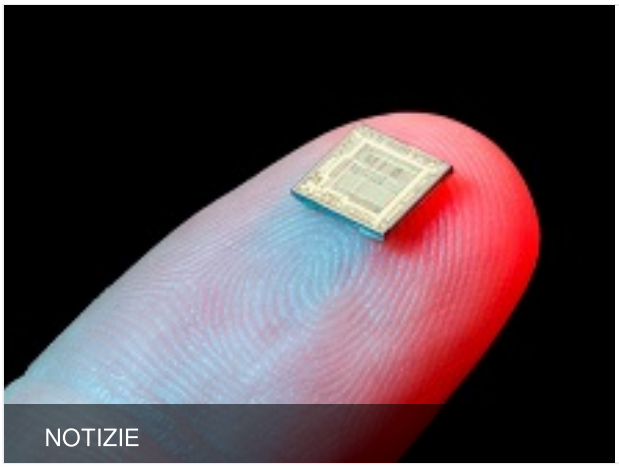
7 Settembre 2023

Articoli correlati

PROGRESSI SCIENTIFICI

È possibile prevenire gli attacchi informatici quantistici? Sì, secondo un'iniziativa dell'UE, che mostra anche come

26 Marzo 2020



PROGRESSI SCIENTIFICI

Un salto di qualità quantistico per i chip di silicio: L'accoppiamento spin-fotone è ora una realtà

27 Febbraio 2018

PROGRESSI SCIENTIFICI

I benefici degli effetti quantistici per le reti biologiche, sociali e tecnologiche

9 Febbraio 2018

PROGRESSI SCIENTIFICI

Un salto di qualità per la misurazione ultraprecisa e la codifica delle informazioni

24 Novembre 2017

NOTIZIE

Ultimo aggiornamento: 11 Ottobre 2017

Permalink: https://cordis.europa.eu/article/id/122627-securing-encryption-data-against-the-threat-of-future-quantum-computers/it