PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 27 - numero 5795 di Lunedì 24 febbraio 2025

I computer quantistici: un aiuto ed una minaccia

Continuando nell'analisi dei documenti messi a disposizione dall'agenzia per la cybersicurezza nazionale, passiamo ad esaminare un documento, che mette in evidenza i rischi legati alla crescente disponibilità di computer quantistici.

I computer quantistici rappresentano una nuova frontiera dell'elaborazione informatica, che offre potenzialità di calcolo estremamente elevate, grazie al fatto che questi computer invece che su bit, operano su qubit.

Questa potenza di calcolo può essere utilizzata sia per sviluppare algoritmi crittografici estremamente sofisticati, sia per cercare di violare algoritmi criptografici, realizzati con tecniche meno avanzate.

È proprio a questo esame che è dedicato questo nuovo manuale della ACN, che desideriamo brevemente illustrare ai nostri lettori.

In vista dell'ancora ridotta diffusione di computer quantistici, appare evidente che la stragrande maggioranza degli algoritmi crittografici correntemente utilizzati viene sviluppata facendo riferimento a computer tradizionali. Ove tuttavia una nazione ostile, oppure un'organizzazione criminosa con elevate professionalità, riesca a impadronirsi di un computer quantistico, lo stesso può essere usato per violare gli algoritmi crittografici correntemente utilizzati.

Per questo motivo, la comunità scientifica, guidata dal National istitute of standard and technologies ? NIST ha già sviluppato un programma, che mira a mettere a punto sistemi crittografici resistenti agli attacchi da parte di computer quantistici, ma che possono essere anche implementati su computer tradizionali.

In attesa quindi di avere a disposizione computer quantistici, che possano sviluppare algoritmi crittografici quantistici, occorre mettere a punto tecniche di miglioramento del livello di protezione degli attuali algoritmi criptografici.

Anche l'unione europea si è allineata su questa strada, dando indicazioni per la messa a punto di un procedimento, che permetta di aggiornare gli attuali sistemi crittografici, che proteggono la stragrande maggioranza delle transazioni critiche, sviluppate da amministrazioni pubbliche e private.

Questa guida inizia descrivendo brevemente gli applicativi di crittografia simmetrica e di crittografia asimmetrica.

Passa successivamente ad analizzare le modalità con cui potrebbero essere sviluppati applicativi crittografici, in grado di resistere ad attacchi con computer quantistici.

Un ampio spazio è destinato alla illustrazione di quanto già viene fatto negli Stati Uniti dalla NIST, che rappresenta sicuramente una punta di lancia in questi studi.

Viene anche analizzata la posizione dell'Asia e dell'unione europea, giungendo a conclusioni, per la verità non molto tranquillizzanti.

Ad esempio, i nuovi algoritmi di tipo post quantum sono decisamente più lenti dei precedenti, oppure richiedono una memoria maggiore per le operazioni di calcolo. Occorre quindi avere a disposizione computer tradizionali con caratteristiche tecniche decisamente più avanzate.

L'agenzia per la cybersicurezza nazionale ha già avviato un programma di transizione verso queste nuove tecnologie ed ecco il motivo per cui questo manuale rappresenta un prezioso documento di aggiornamento per tutti coloro che sono coinvolti nell'impegnativo compito di proteggere i dati da attacchi sofisticati.

Agenzia per la Cybersicurezza Nazionale ? Crittografia Post-Quantum e Quantistica - Preparazione alla Minaccia Quantistica.

Adalberto Biasiotti