Comunicati stampa

Annunciati gli algoritmi sviluppati da IBM: sono i primi standard di crittografia post-quantistica al mondo

Con il rapido progresso dei computer quantistici, il National Institute of Standards and Technology (NIST) statunitense pubblica i nuovi algoritmi, tra cui quelli sviluppati da IBM, in collaborazione con partner di settore, per proteggere i dati da potenziali attacchi quantistici

3 settembre 2024 – Yorktown Heights, New York – Due algoritmi sviluppati da IBM sono stati ufficializzati all'interno dei primi tre standard mondiali di crittografia post-quantistica, pubblicati dal National Institute of Standards and Technology (NIST) del Dipartimento del Commercio degli Stati Uniti.

Gli standard includono tre algoritmi di crittografia post-quantistica: due di essi, ML-KEM (originariamente noto come CRYSTALS-Kyber) e ML-DSA (originariamente CRYSTALS-Dilithium) sono stati sviluppati da ricercatori IBM in collaborazione con diversi partner accademici e di settore. Il terzo algoritmo pubblicato, SLH-DSA (inizialmente presentato come SPHINCS+) è stato sviluppato insieme a un ricercatore che nel frattempo si è unito a IBM. Inoltre, un quarto algoritmo sviluppato da IBM, FN-DSA (inizialmente chiamato FALCON), è stato selezionato per una futura standardizzazione.

La pubblicazione ufficiale di questi algoritmi segna una pietra miliare fondamentale per far avanzare a livello mondiale la protezione dei dati criptati da attacchi informatici, che potrebbero essere perpetrati attraverso l'eccezionale potenza dei computer quantistici, che stanno rapidamente progredendo verso una crittografia sempre più rilevante. Da questo momento, i computer quantistici sfrutteranno una potenza di calcolo sufficiente a violare gli standard di crittografia su cui si basa oggi la maggior parte dei dati e delle infrastrutture del mondo.

"La missione di IBM nel campo del quantum computing è duplice: fare in modo che il quantum computing sia utile in tutto il mondo e rendere il mondo sicuro dal punto di vista quantistico. Siamo entusiasti degli incredibili progressi compiuti con gli attuali

computer quantistici, che vengono utilizzati a livello globale in tutti i settori industriali per analizzare i potenziali rischi, mentre ci avviciniamo sempre più ad ottenere sistemi completamente error-corrected", ha dichiarato **Jay Gambetta, Vice President IBM Quantum**. *"Tuttavia, siamo consapevoli che questi progressi potrebbero portare a uno sconvolgimento della sicurezza dei nostri dati e dei sistemi più sensibili. La pubblicazione da parte del NIST dei primi tre standard di crittografia post-quantistica segna un passo significativo negli sforzi per costruire un futuro sicuro per il quantum computing".*

In quanto ramo completamente nuovo dell'informatica, i computer quantistici stanno rapidamente accelerando verso sistemi utili e su larga scala, come dimostrano le tappe raggiunte da un punto di vista hardware e software, e pianificate nella Quantum Development Roadmap di IBM. Ad esempio, IBM prevede di consegnare il primo sistema quantistico*error-corrected* entro il 2029. Si prevede che questo sistema eseguirà centinaia di milioni di operazioni quantistiche per restituire risultati accurati a problemi complessi e rilevanti, attualmente inaccessibili ai computer classici. In un'ottica futura, la roadmap di IBM prevede di espandere questo sistema per eseguire fino a un miliardo di operazioni quantistiche entro il 2033. Allo scopo di raggiungere questi obiettivi, IBM ha già coinvolto esperti della sanità e delle scienze biologiche, della finanza, dello sviluppo dei materiali, della logistica e di altri settori con strutture su scala industriale per iniziare a risolvere le loro sfide più complesse e urgenti con i computer quantistici man mano che la tecnologia viene sviluppata.

Tuttavia, l'avvento di computer quantistici più potenti potrebbe comportare dei rischi per gli attuali protocolli di sicurezza informatica. Con l'aumento dei livelli di velocità e delle capacità di correzione degli errori, è probabile che essi comprendano anche la capacità di rompere gli schemi crittografici più utilizzati oggi, come l'RSA, che da tempo protegge i dati globali. Partendo da un lavoro iniziato diversi decenni fa, il team di IBM, composto dai più importanti esperti di crittografia del mondo, continua a guidare il settore nello sviluppo di algoritmi per la protezione dei dati contro le minacce future, che sono in grado di sostituire gli attuali schemi di crittografia.

Gli standard appena pubblicati dal NIST sono progettati per salvaguardare i dati scambiati attraverso le reti pubbliche e per le firme digitali per l'autenticazione delle identità. Grazie alla loro ufficializzazione, costituiranno lo standard per i governi e i settori industriali in tutto il mondo per iniziare ad adottare strategie di sicurezza informatica post-quantistica.

Nel 2016, il NIST ha chiesto ai crittografi di tutto il mondo di sviluppare e presentare nuovi schemi crittografici, sicuri dal punto di vista quantistico, da prendere in considerazione per una futura standardizzazione. Nel 2022, tra le 69 proposte selezionate per la revisione, sono stati scelti quattro algoritmi di crittografia per un'ulteriore valutazione: CRYSTALS-Kyber, CRYSTALS-Dilithium, Falcon e SPHINCS+.

Oltre a proseguire le ricerche per la pubblicazione di Falcon come quarto standard ufficiale, il NIST sta continuando a identificare e valutare altri algoritmi per diversificare il suo toolkit di algoritmi di crittografia post-quantistica, tra cui diversi altri sviluppati da ricercatori IBM. I crittografi IBM sono tra i pionieri dell'espansione di questi strumenti, come, ad esempio, i tre

schemi di firma digitale recentemente presentati, che sono già stati selezionati per essere presi in considerazione dal NIST e sono in fase di valutazione iniziale.

Nella sua mission di rendere il mondo sicuro dal punto di vista quantistico, IBM continua a esplorare come la crittografia post-quantistica possa essere integrata in molti dei suoi prodotti, tra cui IBM z16 e IBM Cloud. Nel 2023, l'azienda ha presentato la roadmap IBM Quantum Safe, un percorso suddiviso in tre fasi per tracciare le tappe verso una tecnologia quantum-safe sempre più avanzata, definita dalle fasi di scoperta, osservazione e trasformazione. Oltre a questa roadmap, l'azienda ha presentato anche la tecnologia IBM Quantum Safe e gli IBM Quantum Safe Transformation Services per supportare i clienti nel loro percorso verso la sicurezza quantistica. Queste tecnologie includono l'introduzione della Cryptography Bill of Materials (CBOM), un nuovo standard per acquisire e scambiare informazioni sulle risorse crittografiche nel software e nei sistemi.

Per ulteriori informazioni sulla tecnologia e sui servizi IBM Quantum Safe: https://www.ibm.com/quantum/quantum-safe

Per saperne di più leggi il blog: https://research.ibm.com/blog/nist-pqc-standards

IBM

IBM è un'azienda leader a livello mondiale nel settore del cloud ibrido, dell'AI e dei servizi alle imprese e opera con le imprese di oltre 175 Paesi aiutandole a capitalizzare sugli insight dei loro dati, a semplificare i processi aziendali, a ridurre i costi e a ottenere un vantaggio competitivo nei loro settori d'industria. Quasi 4.000 enti governativi e aziende in aree infrastrutturali critiche come quelle dei servizi finanziari, delle telecomunicazioni e sanità si basano sulla piattaforma cloud ibrida di IBM e su Red Hat OpenShift per realizzare la loro trasformazione digitale in modo rapido, efficiente e sicuro. Le innovazioni di IBM nell'ambito dell'AI, del quantum computing, delle soluzioni cloud specifiche per settore d'industria e nei servizi sono offerte con opzioni open e flessibili. Tutto questo è supportato dal ben noto impegno di IBM per la trasparenza, la responsabilità, l'inclusività e il servizio. Per maggiori informazioni, visitate il sito www.ibm.com.

LinkedIn: IBM

Contatti:
Morgana Stell - *External Relations Leader, IBM Italia*

email: morgana.stell@it.ibm.com
mobile: 335 7693528