PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 26 - numero 5714 di Mercoledì 16 ottobre 2024

I primi algoritmi criptografici a prova di attacchi da computer quantistici

La NIST-National Institute of standards and technology ha finalmente approvato i primi algoritmi criptografici, in grado di resistere ai temibili attacchi dei computer quantistici. È così possibile mettere in sicurezza un gran numero di applicazioni.

Gli esperti aspettavano da tempo questa approvazione, che permette finalmente di utilizzare applicativi criptografici, in grado di resistere ai temibili attacchi dei computer quantistici.

Come i lettori sanno, i computer quantistici operano in modo completamente differente, rispetto ai computer attualmente in uso e sono in grado di violare gli algoritmi criptografici convenzionali in tempi brevissimi.

Gli algoritmi, che sono stati oggi annunciati, e che i lettori possono trovare meglio descritti su questo link, sono classificati come algoritmi PQC (post Quantum Cryptography) e sono già disponibili per l'uso immediato.

Sono stati approvati tre algoritmi che si spera gli esperti informatici vogliano utilizzare al più presto, in quanto recenti studi confermano come lo sviluppo dei computer quantistici crescerà in modo esponenziale in tempi brevissimi. Questo è motivo per cui, insieme alla descrizione degli algoritmi, sono state offerte anche dettagliate informazioni su come incorporare questi algoritmi in applicazioni esistenti.

La NIST è giustamente orgogliosa di questa sua attività, che conferma come gli Stati Uniti assumano un ruolo dominante, in tutto il mondo, nel campo della sicurezza informatica.

Per giungere ad individuare e approvare questi algoritmi, l'agenzia federale americana ha raccolto gli esperti di tutto il mondo, accettando indicazioni e suggerimenti provenienti da tutti i paesi.

Questi nuovi standard sono stati progettati per soddisfare a due specifiche esigenze, in cui gli algoritmi crittografici vengono tipicamente utilizzati:

- applicazioni di criptografia generale, utilizzate per proteggere lo scambio di informazioni su una rete pubblica e
- firme digitali, utilizzate per l'autentica di identità.

Attualmente la NIST sta lavorando su un quarto applicativo, FALCON, che si unisce ai precedenti, di cui offriamo ai lettori i nomi:

CRYSTALS-Kyber, CRYSTALS-Dilithium, Sphincs+.

Adalberto Biasiotti

---

www.puntosicuro.it