Crittografia Post-Quantum

Olivieri Michele

November 26, 2025

Contents

1 Introduzione

1.1 Contesto e motivazioni

Per comprendere l'importanza della crittografia post-quantistica, è fondamentale analizzare il contesto in cui essa si inserisce e le motivazioni che ne hanno guidato lo sviluppo.

La crittografia classica, come visto a lezione, pone le sue fondamenta su problemi computazionalmente difficili per i quali non esistono algoritmi efficienti in grado di risolverli in tempi polinomiali.

Tuttavia, l'emergere dei computer quantistici ha introdotto una nuova dimensione nel panorama della sicurezza informatica. Questi dispositivi sfruttano i principi della meccanica quantistica per eseguire calcoli in modo radicalmente diverso rispetto ai computer classici, rendendoli potenzialmente capaci di risolvere in tempi polinomiali quei problemi matematici che risultano intrattabili per le macchine convenzionali.

1.2 Minaccia dei computer quantistici: Perché è necessaria?

Il rapido sviluppo nel settore del calcolo quantistico, che fino a due decenni anni fa sembrava lontano dall'essere una minaccia concreta, ha destato crescente preoccupazione riguardo alla sicurezza dei sistemi attualmente in uso. La necessità di sviluppare nuovi sistemi crittografici nasce proprio dalla vulnerabilità degli algoritmi attuali di fronte a questa tecnologia emergente.

Sebbene i computer quantistici siano ancora in una fase sperimentale, i loro potenziali avanzamenti rappresentano una minaccia concreta per gli algoritmi crittografici classici su cui si basa gran parte della sicurezza informatica moderna. In particolare, algoritmi come RSA (Rivest-Shamir-Adleman), ECC (Elliptic Curve Cryptography) e DSA (Digital Signature Algorithm) potrebbero essere facilmente compromessi dall'uso di potenti computer quantistici grazie all'algoritmo di Shor, che è infatti capace di risolvere in tempi polinomiali il problema della fattorizzazione e del logaritmo discreto su cui si basano gli algoritmi citati.

Questa vulnerabilità mette a rischio non solo la riservatezza delle comunicazioni attuali, ma anche l'integrità e l'autenticità dei dati, ponendo una seria minaccia a lungo termine per la sicurezza delle infrastrutture digitali globali.

Molti scienziati ritengono che la costruzione di computer quantistici su larga scala sia ormai solo una sfida ingegneristica, con alcuni ingegneri che prevedono il loro sviluppo entro i prossimi vent'anni. Considerando che stori-

camente ci sono voluti quasi due decenni per implementare l'attuale infrastruttura crittografica, è necessario iniziare ora a preparare sistemi in grado di resistere al calcolo quantistico.

upgrade

L'algoritmo di Shor, sviluppato nel 1994, ha dimostrato teoricamente che un computer quantistico sufficientemente potente potrebbe fattorizzare grandi numeri interi e calcolare logaritmi discreti in tempo polinomiale. Questo significa che algoritmi come RSA, ECC e DSA, pilastri della sicurezza informatica moderna, potrebbero essere compromessi, mettendo a rischio non solo la riservatezza delle comunicazioni, ma anche l'integrità e l'autenticità dei dati scambiati attraverso le infrastrutture digitali globali.

Sebbene i computer quantistici siano ancora in una fase sperimentale, molti scienziati ritengono che la loro realizzazione su larga scala sia ormai solo una questione ingegneristica. Alcuni esperti prevedono che entro i prossimi vent'anni potrebbero essere disponibili computer quantistici sufficientemente potenti da violare gli schemi crittografici attualmente in uso. Considerando che l'implementazione dell'attuale infrastruttura crittografica ha richiesto quasi due decenni, risulta evidente l'urgenza di iniziare ora la transizione verso sistemi resistenti al calcolo quantistico.

1.3 Obiettivi della crittografia post-quantistica

L'obiettivo della crittografia post-quantistica è quindi sviluppare algoritmi crittografici sicuri sia contro i computer quantistici che classici, garantendo così un futuro sicuro anche in un'era dominata dai computer quantistici.

La crittografia post-quantistica non si limita a sostituire gli algoritmi vulnerabili, ma mira a costruire un'infrastruttura di sicurezza robusta e duratura, capace di adattarsi alle sfide tecnologiche future mantenendo la compatibilità con i protocolli e le reti esistenti.