Crittografia Post-Quantum

Olivieri Michele

November 26, 2025

Contents

1 Introduzione

1.1 Contesto e motivazioni

Per parlare di crittografia post-quantistica, è fondamentale comprendere il contesto in cui essa si inserisce. Come visto a lezione la crittografia classica pone le sue fondamneta su problemi computazionalmente difficili per i quali non esistono algoritmi efficienti in grado di risolverli in tempi polinomiali.

In questo contesto entrano in gioco i computer quantistici, dispositivi che sfruttano i principi della meccanica quantistica per eseguire calcoli in modo radicalmente diverso rispetto ai computer classici che quindi li rende capaci di risolvere quei problemi matematici ritenuti difficili o intrattabili per i computer convenzionali.

Tuttavia se fino ad un decennio fa sembravano non essere una minaccia, il rapido sviluppo del calcolo quantistico ha destato crescente preoccupazione riguardo alla sicurezza dei sistemi crittografici attualmente in uso.

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 probelamm della fattorizzazione e del logarimto discreto su cui di 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 storicamente 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.

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