Crittografia post quantistica

Cifrari asimmetrici

Esistono algoritmi polinomiali per la fattorizzazione di interi e il calcolo del logaritmo discreto su macchine quantistiche, che permettono in teoria di forzare i cifrari a chiave pubblica in uso corrente. Tuttavia l'algoritmo di Shor (fattorizzazione) su numeri da migliaia di bit richiede una macchina con migliaia di qubit e miliardi ($\mathrm{O}(n^3)$) di gate in grado di mantenere la sovrapposizione.

Si congettura che i problemi NP-hard siano difficili anche su macchine quantistiche.

Cifrari simmetrici

L'algoritmo di Grover esegue una ricerca sequenziale su un insieme non strutturato in tempo $\mathrm{O}(\sqrt{n})$ anziché $\mathrm{O}(n)$. Questo permette di ridurre i tempi di ricerca esaustiva di una chiave da $\mathrm{O}(2^n)$ a $\mathrm{O}(2^{\frac{n}{2}})$, per cui i bit di sicurezza sono dimezzati.

One-Time Pad rimane sicuro, visto che non è suscettibile ad attacchi brute-force.