Algoritmo di Shor

Candidato: Giacomo Fantozzi* Relatore: Paola Verrucchi†

9 ottobre 2018

Tra le molte rivoluzioni scientifiche che hanno segnato il XX secolo, tre risaltano particolarmente per il loro impatto, sia pratico che concettuale: lo sviluppo dei moderni computer, e quindi dell'informatica; l'introduzione di nuove tecniche di crittografia, al seguito dello sviluppo della scienza delle comunicazioni; la nascita della meccanica quantistica. Fin dall'inizio informatica e crittografia si sono stimolate a vicenda: l'archetipo del computer moderno, il calcolatore meccanico chiamato "Colossus" ideato e costruito da Alan Turing negli anni della seconda guerra mondiale, aveva lo scopo di decifrare i codici militari tedeschi. Con il passare degli anni, il legame fra questi due campi di conoscenza si è sempre più rafforzato, al punto che non ha più senso parlare di sistemi crittografici in ambiti esterni all'informatica.
In questo contesto entra in gioco, sul finire del XX secolo, la meccanica quantistica. È di Paul Benioff e Yuri Manin, risalente al 1980, e di Richard Feynman, nel 1982, la proposta di un *computer quantistico*, ovvero un dispositivo che sfruttasse le leggi della meccanica quantistica per svolgere calcoli secondo algoritmi totalmente nuovi. Nel giro di pochi anni, diventa evidente che un tale dispositivo sarebbe in grado di riuscire in operazioni irrealizzabili in tempi brevi per un computer classico, per quanto potente, ed i primi algoritmi appositamente progettati per essere svolti da computer quantistici, detti algoritmi quantistici, vedono la luce. Risale al 1994, in particolare, l'ideazione da parte di Peter W. Shor di un algoritmo quantistico in grado di completare efficientemente la riduzione in fattori primi di un numero, operazione su cui si basa uno dei sistemi crittografici piu' noti ed utilizzati, il cosiddetto sistema RSA (Rivest–Shamir–Adleman, 1977). La sicurezza di tale metodo è garantita dall'imponente mole di calcoli necessaria a decifrare un messaggio cifrato secondo la procedura RSA, così imponente da essere difficile da manipolare anche per i più potenti computer classici, ma non per un computer quantistico in grado di realizzare l'algoritmo di Shor. Bisognerà pero' aspettare il 2001 per avere la conferma sperimentale della possibile realizzazione di un dispositivo quantistico in grado di implementare tale algoritmo. Per quanto gli attuali circuiti quantistici siano ancora in fase di sperimentazione, è diventato evidente che un futuro in cui essi saranno estensivamente utilizzati per operazioni di calcolo è una possibilità concreta.
Al fine di comprendere la portata di quanto sopra descritto, in questa tesi abbiamo prima introdotto i principi fondamentali della crittografia RSA, mettendo in evidenza il legame fra il problema della fattorizzazione in numeri primi e la sicurezza del protocollo stesso, facendo riferimento al concetto di complessità computazionale. Per meglio chiarire in che modo la realizzazione di un dispositivo quantistico può minare la sicurezza della crittografia RSA, abbiamo quindi introdotto i principali elementi della computazione quantistica (qubit e porte logiche quantistiche): in termini di tali elementi abbiamo quindi descritto le parti computazionalmente più rilevanti dell'algoritmo di Shor, ovvero le subroutine quantistiche per il calcolo della trasformata di Fourier e la stima della fase di un operatore unitario. Il dettaglio della descrizione proposta ci ha permesso infine di presentare un'applicazione semplice ma completamente esplicita dell'algoritmo di Shor, in tutti i suoi passaggi ed iterazioni.

*email: giacomo.fantozzi@stud.unifi.it
†email: mailto:verrucchi@fi.infn.it