

Quantum Computing: gli effetti collaterali per la sicurezza



Sempre più spesso ricorre la tematica riguardante la nuova generazione di computer, i “Quantum Computer” che di giorno in giorno comincia a suscitare sempre più interesse vista la direzione presa dal mondo digitale dove la protezione del dato è in cima alla lista delle priorità. Protezione che oggi viene assicurata dalla crittografia mediante i protocolli di firma, di cifratura e di scambio delle chiavi. Già, ma questa stessa crittografia pare non essere resistente ad un eventuale attacco perpetrato tramite un computer quantistico e questo allarma non poco tutto l'intero mondo dell'Information Technology.

Ma allo stesso tempo è proprio il continuo sviluppo della tecnologia quantum computing a trainare la ricerca verso una nuova crittografia, una crittografia del futuro denominata “Post-Quantistica” capace di reggere ad ogni tipo di attacco portato dai computer quantistici, assicurando così tutte quelle modalità e tecnologie di protezione fondate sulla crittografia e di cui Internet ne è il massimo fruitore.

E' IBM a trainare la tecnologia Quantum, ma sia Microsoft che Google non stanno certo a guardare, visto i cospicui investimenti stanziati per realizzare un quantum computer alla portata di tutti comparabile al computer odierno di tipo binario. La spinta trainante arriva da quei settori ingegneristici dello studio dei materiali ma anche dal settore chimico e da quello farmaceutico che sono alla costante ricerca di soluzioni computazionali che allo stato attuale risultano ancora impossibili attraverso l'utilizzo della tecnologia offerta dai computer di oggi.

Accanto a questa spinta si manifestano gli effetti collaterali che potrebbero scatenarsi a fronte della risoluzione degli enigmi matematici basati sulle più diffuse primitive di crittografia. La potenza di calcolo sprigionata dai computer quantistici è tale da far saltare gli attuali sistemi crittografici mettendo a serio rischio tutti i nostri preziosi dati. Infatti, questi algoritmi crittografici utilizzati da moltissime applicazioni forniscono una robustezza rassicurante per i computer binari di oggi che, per decifrare e risolvere una cifratura del dato, necessitano di uno spazio temporale calcolato nell'ordine di migliaia di anni. Ma cosa accadrebbe se avessimo a disposizione un Quantum Computer? Semplice, in solo poche ore potremmo "sventrare" ogni tipo di crittografia attuata nel contesto odierno.

Ecco perché cresce l'interesse e la preoccupazione verso questa nuova generazione di computer che, è bene dirlo, per ora sono stati costruiti solo per scopi di laboratorio, quindi non ancora pronti su vasta scala. Ma sono gli stessi esperti sviluppatori del Quantum Computer a considerare il 2031 come l'anno di svolta in cui la presenza dei computer quantistici sarà così importante da poter essere in grado di violare uno degli algoritmi più utilizzati fino ad ora, l'algoritmo RSA-2048. Basta ricordare quanto questo algoritmo venga largamente utilizzato con i protocolli di sicurezza SSL e TLS che assicurano la protezione delle comunicazioni sulle reti, Internet compresa. Ad esempio, proviamo a pensare a tutte quelle transazioni economiche realizzate oggi online tramite carte bancarie di ogni tipo e protette con RSA. Ebbene se avessimo a portata un Quantum Computer basta un attimo a mettere a soqquadro l'intero sistema con un conseguente ed inestimabile danno economico.

Cosa fare quindi? Per fortuna c'è già chi si è posto il problema sviluppando la futura crittografia "post-quantistica" capace di utilizzare delle primitive crittografiche in grado di risolvere problemi matematici molto più complessi rispetto

a quelli determinati dal Quantum Computer, quindi resistenti per altrettante migliaia di anni di calcolo prima di poter essere risolte anche dai computer quantistici. Questo consente di ripristinare una certa gerarchia computazionale che vede i computer di qualsiasi natura, sempre un passo indietro rispetto alla complessità delle operazioni matematiche utilizzate per la sicurezza crittografica.

E come sempre, in campo crittografico, è il NIST a mettere ordine ad un possibile utilizzo di queste nuove primitive post-quantistiche, mediante la formulazione di nuovi standard che verranno rilasciati entro il 2024 e che saranno capaci di determinare e classificare gli algoritmi di firma e di cifratura con chiave pubblica o asimmetrica, dove viene usata la coppia di chiavi (pubblica + privata), la prima per cifrare e verificare la veridicità della firma digitale, mentre la seconda viene utilizzata per decifrare il dato o per firmarlo.

Abbiamo parlato di chiavi, e sono proprio loro a creare una seconda problematica non certo meno importante della prima, in quanto queste chiavi devono essere scambiate o distribuite tra le controparti che necessitano di comunicare. Ma anche qui c'è già chi se ne sta prendendo cura: la Quantum Key Distribution

Con la Quantum Key Distribution sia il mittente che il destinatario del messaggio possono generare e scambiare contestualmente una stringa randomica fatta di 0 e 1 evitando che un possibile attacco esterno possa individuare il contenuto della stringa mentre questa viene scambiata. Si tratta del concetto basilare con cui lavora la sicurezza crittografica, e cioè della capacità di generare le chiavi in maniera random, in modo che i digit componenti della stringa binaria (0 e 1) da cui si estrae poi la chiave risultino uniformemente distribuiti tra loro. Ed è su questo concetto che si sviluppano gli eventi quantistici, randomici per loro natura, ed utilizzati dalla Quantum Key Distribution per la generazione e distribuzione delle chiavi private. Si tratta di un metodo alternativo, non computazionale, dove sicurezza e

veridicità della stringa generata in modalità randomica sono determinate proprio dalla fisica quantistica.

Ma attenzione a non commettere l'errore di contrapporre la soluzione di scambio delle chiavi della Quantum Key Distribution con le soluzioni adottate con la crittografia classica. Si tratta di soluzioni differenti adottabili a seconda del tipo di applicazione. Ad esempio, mentre la crittografia classica può continuare ad essere utilizzata per lo scambio delle chiavi da utilizzare per le applicazioni più comuni, la Quantum Key Distribution può essere adottata per tutte quelle applicazioni che richiedono un elevato livello di sicurezza protratto nel lungo termine, come le comunicazioni strategiche militari o servizi segreti, che non possono certo essere compromesse dai mutamenti tecnologici nè tantomeno dipendere dal potere computazionale di elaboratori di nuova generazione.

Ad ogni modo...ci siamo! Siamo proprio sulla soglia di un cambiamento radicale del mondo digitale, guidato dallo sviluppo del computer quantistico che spinge fortemente sull'acceleratore del progresso, obbligando esperti di crittografia e fisici quantistici a sviluppare nuovi protocolli per la firma, la cifratura e lo scambio delle chiavi, ad alta immunità, capaci di resistere a tutti i tentativi di attacco portati dal futuro Quantum Computer.

Articolo a cura di **Luigi Perrone**

<https://www.ictsecuritymagazine.com/articoli/quantum-computing-gli-effetti-collaterali-per-la-sicurezza/>