Quantum computing, l’evoluzione da bit a qubit

La sicurezza e gli algoritmi usati per crittografia e la lunghezza di password sono basati sull’attuale tecnologia Hardware che abbiamo a disposizione. Mettere una chiave lunga e complessa per entrare nel nostro sistema operativo o sui siti è considerato abbastanza sicuro poiché un attaccante avrebbe bisogno di molto tempo con l’attuale potenza di calcolo disponibile per decrittografare la password e vedere le informazioni. Per crittografia si intente, come ricorda **Wikipedia**, la branca che tratta le “scritture nascoste”, i metodi per rendere un messaggio “offuscato”, in modo da non essere comprensibile a persone non autorizzate a leggerlo.

La regola considerata come modus-operandi che tutti i consulenti di sicurezza informatica al momento usano è incentivare/obbligare l’utente a inserire caratteri particolari, maiuscole, minuscole e numeri per aumentare la complessità che la password non venga scoperta. Un esempio potrebbe essere una password su crittografia simmetrica da 2 caratteri, per scoprirla il Pc deve fare tutte le combinazioni finché non trova la giusta password, ma all’aumentare dei caratteri, esempio 10, le interazioni e combinazioni aumentano elevando così anche il tempo per trovare una chiave. Un computer per trovare password lunghissime comincia a impiegare mesi, anni,..ecc. I recenti sistemi con schede video in parallelo che sfruttano il sistema **Nivida-CUDA**, per decrittografare informazioni crittografate, hanno aumentato di molto la potenza di calcolo. Potenza usata sia per simulazioni da parte di ricercatori ma anche per scoprire dati crittografati raccolti da un potenziale cracker.

I computer che ci circondano ai giorni d’oggi usano i Binary Digit (bit), i due segnali che permettono di memorizzare i dati 0-1 un byte raccoglie 8 bit. Nella storia dei pc i bit hanno assunto diversi ruoli come nei transistor aperto-chiuso o porzioni di disco fisso meccanico, materiale magnetizzato in un verso o nell’altro. Il codice binario è alla base di tutti i computer. I bit vengono raggruppati in 32-64 bit per memorizzare porzioni più grandi di informazioni massime che il computer riesce a gestire. I computer possono volgere attraverso le porte logiche lavori della logica booleana come not, and, or, nand, xnor, nor e xor. I computer quantistici usano i qubit invece di bit, mentre sui pc attuali gli stati sono spento o acceso quindi 1 o 0 nei qubit possiamo avere una sovrapposizione coerente di stati. Questa sovrapposizione indica che è sia in uno stato sia nell’altro rispetto alla logica che conosciamo binaria. Questo stato permette al computer quantistico di avere molta più potenza di calcolo rispetto al sistema classico. Le porte logiche sono 9 nei Pc quantistici. Queste condizioni sono alla base della potenza di calcolo nella *Quantum computing*. L’algoritmo è una sequenza di azioni per ottenere un risultato, Wikipedia suggerisce, procedimento che risolve un determinato problema attraverso un numero finito di passi elementari, chiari e non ambigui, in tempo ragionevole. Nella struttura di un computer classico, anche se avesse molte Cpu in parallelo, molta Ram e frequenza di clock alta, la workstation dovrebbe usare un algoritmo che dato un input, seguendo delle regole per decrittografare, otterrebbe un risultato valido in tempi ragionevoli calcolati nella vita di un uomo. Ogni problema viene risolto con un algoritmo adatto per avere il risultato nel modo più veloce.

Nella sicurezza informatica per scoprire le password viene usato il metodo brute-force o dizionario. Mentre nella prima il tempo è elevato perché va a provare tutte le combinazioni, mentre il secondo, dato un dizionario pronto prova meno

interazioni per trovare la chiave, se contenuta nel dizionario.

Gli algoritmi si suddividono in efficienti e non efficienti. I primi se la sua complessità è di ordine polinomiale, esempio 2xN, o una qualche potenza mentre i secondi se la sua complessità è di ordine superpolinomiale ovvero 2 alla N. I computer quantistici sfruttano algoritmi quantistici diversi dai classici ovvero cercare più soluzioni contemporaneamente sfruttando la sovrapposizione di stati. I più famosi sono due algoritmi di **Grover** e di **Shor**. Se dovessimo trovare una password dentro a un file contenente 1000 parole quindi mille prove, il pc classico dovrebbe fare tutte le prove mentre il pc quantistico con l'algoritmo di Grover impiegherebbe la radice quadrata del numero da esaminare. L'algoritmo di **Peter Shor** lavora invece la fattorizzazione di numeri con più di 100 cifre. Se per trovare una password o decrittografare una sessione *sniffata* di un traffico dati di qualche comunicazione con i Pc tradizionali, che usano algoritmi classici si

impiegherebbe un certo tempo mentre con i Pc quantistici molto meno della metà. Complessi calcoli necessitano di molto tempo di elaborazione che codificano i due stati descritti, i computer quantistici sono in via di sviluppo e non vi è ancora uno standard definito. Aziende, come **IBM**, **Google**, **Intel**, e università come MIT e Harvard stanno sviluppando computer quantistici, questo porta a dover nel futuro prossimo, partendo già da ora, rivisitare la nostra sicurezza, nel modo di concepire la security IT e nel modo di proteggere le nostre comunicazioni.

The post Quantum computing, l’evoluzione da bit a qubit appeared first on Key4biz.

https://www.key4biz.it/quantum-computing-levoluzione-da-bit-a-qubit/233878/