STORMSHIELD

ARTICOLO DI OPINIONE

CYBERSICUREZZA E QUANTISTICA: ATTENZIONE ALLE SEMPLIFICAZIONI

Fabien Thomas
Chief Technology Officer, Stormshield

Quantum System One in IBM, Quantum AI in Google, Azure Quantum in Microsoft, Qian Shi in Baidu... Dalla fine degli anni 2010, l'informatica quantistica è diventata sempre più importante, sia in termini di protezione che di minacce alla sicurezza informatica. Perché a lungo termine questa rivoluzione informatica potrebbe infatti indebolire notevolmente i sistemi di sicurezza basati sulla crittografia, in altre parole quasi tutti... La minaccia quantistica, una nuova sfida per la cybersicurezza. A patto di comprendere bene il fenomeno ed evitare idee preconcette.

Premessa: per preservare la leggibilità di questo articolo, non descriveremo in dettaglio gli algoritmi di Grover e Shor o di tutte le sfumature dei qubit (stabili, rumorosi, ricottura E gli altri...). È in gioco anche la salute mentale dei nostri lettori.

LE PROMESSE DELLA POTENZA DI CALCOLO QUANTISTICA

Dall'informatica tradizionale al computer quantistico

L'informatica quantistica affascina, ma è anche un argomento estremamente complicato da comprendere. E, dietro la facciata, si nascondono in realtà molte incertezze, riassunte con la famosa citazione attribuita al fisico Richard Feynman: «*Penso di poter tranquillamente affermare che nessuno capisce la meccanica quantistica*». Un paradigma da tenere presente durante la lettura di questo scritto. «*Quando si tratta di quantistica, non bisogna cercare di capirla con l'intuizione,* completa **Yvan Vanhullebus**, capo tecnico di Stormshield. *Perché la nostra intuizione si basa sulle nostre esperienze passate e non è affatto addestrata ai quanti. Tanto che oggi sembra più facile spiegare cosa NON è la quantistica*... ».

«Quando si tratta di quantistica, non dovremmo cercare di capirla con l'intuizione. Perché la nostra intuizione si basa sulle nostre esperienze passate e non è affatto addestrata ai quanti. Tanto che oggi sembra più facile spiegare cosa NON è la quantistica.....»

Yvan Vanhullebus, Technical Leader di Stormshield

Un argomento complicato che affascina particolarmente il mondo della cybersicurezza, dato che **l'informatica quantistica potrebbe rivoluzionare l'informatica così come la conosciamo oggi.** Come? Grazie al "salto quantico", ovvero alla possibilità di beneficiare di una potenza di calcolo ottimizzata e poter così compiere operazioni matematiche complesse, fino ad allora impossibili. Come spiega Yvan Vanhullebus: «*il computer quantistico utilizza le proprietà della materia su scala infinitamente piccola per ottenere in pochi minuti certi calcoli che richiederebbero almeno diverse migliaia di anni con i computer più potenti di oggi*».

L'informatica quantistica è intimamente legata al concetto di una nuova unità: il bit quantistico o "qubit". Un'unità che, come spiegato nella maggior parte degli articoli, può assumere due valori (indicati con 0 o 1) ma che può anche avere entrambi i valori contemporaneamente, il che renderebbe possibile calcolare tutti i valori contemporaneamente. «***Ma in realtà non funziona così: siamo più vicini alla realtà quantistica parlando di probabilità***», come sottolinea Yvan Vanhullebus, che rimanda a un… fumetto come documento di riferimento sull'argomento: il fumetto «*The Talk*» di Scott Aaronson e Zach Weinersmith.

Le applicazioni desiderate dell'informatica quantistica

Molti soggetti si sono lanciati in una vera e propria corsa tecnologica per raggiungere la supremazia quantistica. **Ma cos'è la supremazia quantistica?** È quando un calcolo quantistico su un dato problema sarà più veloce del suo equivalente computazionale.

Sebbene alcuni soggetti spieghino regolarmente di aver raggiunto questa supremazia quantistica, il passaggio alla vera era dell'informatica quantistica si fa ancora attendere. In questa corsa al supercomputer si sono dunque moltiplicati gli annunci di soggetti privati, come Google, IBM o Baidu ognuno dei quali ha abbondantemente riferito i propri progressi (più o meno sperimentali) in questo campo. Allora, **chi ha raggiunto la supremazia quantistica?** Non c'è consenso tra gli esperti in materia, in particolare non tutti i qubit sono uguali... Le quantità di qubit nei diversi annunci a volte possono sorprendere - perché non rappresentano sempre la stessa cosa... Già nel 2019 Google ha annunciato di aver raggiunto questa supremazia quantistica, prima dei ricercatori cinesi nel 2021 – ma in entrambi i casi i risultati sono stati contestati. Tra i 54 qubit per il processore Sycamore di Google e i 433 per il processore Osprey di IBM, la gara dei qubit è aperta e in pieno svolgimento.

I soggetti pubblici non sono da meno in questa corsa tecnologica. Negli Stati Uniti l'NSA si interessa da anni al settore quantistico (nel 2014 ha speso i suoi primi 80 milioni di dollari in un programma chiamato *Owning The Net, "Dominare la rete"*). Da parte sua, l'Europa prevede di investire almeno 4,5 miliardi di euro entro il 2027 in tecnologie quantistiche. Il governo francese, invece, a gennaio 2021 ha stanziato una somma di 1,8 miliardi di euro per le tecnologie quantistiche. «*Un budget significativo ma inferiore agli investimenti cinesi e americani,* specifica **Noël Chazotte,** Product Manager di Stormshield. *Se si considera che gli importi menzionati corrispondono a 25 miliardi di dollari per gli Stati Uniti e a 50 miliardi per la Cina, si vede che l'Europa non è sulla stessa scala...*»

«L'Europa prevede di investire almeno 4,5 miliardi di euro entro il 2027 nelle tecnologie quantistiche. Il governo francese, invece, a gennaio 2021 ha stanziato una somma di 1,8 miliardi di euro per le tecnologie quantistiche.»

Perché la posta in gioco è alta: si tratta di padroneggiare una tecnologia presentata come rivoluzionaria. Simulare il funzionamento dell'universo o il comportamento della materia a livello molecolare, trovare nuovi pianeti abitabili, prevedere meglio il tempo atmosferico, creare farmaci in grado di curare le principali patologie come il cancro o l'Alzheimer, ma anche combattere le frodi bancarie e nel complesso migliorare la sicurezza dei sistemi informativi… le applicazioni sono molteplici e riguardano numerosi settori industriali. Tuttavia, se le promesse di questo settore sono impressionanti, **l'informatica quantistica rappresenta anche una nuova minaccia per il settore della cybersicurezza.**

LE NUOVE MINACCE INTRODOTTE DALL'INFORMATICA QUANTISTICA

Una minaccia cyber... statale?

Prima di dare credito a informazioni che parlano di una minaccia quantistica cyber-criminale, la minaccia potrebbe soprattutto prendere una piega geopolitica. «*Molto chiaramente, il primo Stato a vincere la corsa per padroneggiare la tecnologia quantistica avrà la supremazia sugli altri*, spiega **Arnaud Dufournet,** Direttore Marketing di TheGreenBow. *Come le potenze nucleari, ci saranno potenze quantistiche nel mondo. Oggi la partita si gioca tra Cina e Stati Uniti. Quindi, affinché i cybercriminali non statali dispongano di quest'arma, ci vorrà ancora più tempo*». **Il computer quantistico diventerebbe quindi una nuova leva per lo spionaggio industriale e statale, persino per la destabilizzazione geopolitica?** Si sarebbe tentati di rispondere di sì, poiché la questione della sicurezza nazionale è presa molto sul serio da molti paesi. Ascoltando un raro discorso pubblico del capo dell'MI6, si scopre che i servizi segreti britannici si preoccupano dunque di vedere certi «*rogue states*", stati canaglia, posizionarsi sulla quantistica in vista di futuri conflitti.

«Molto chiaramente, il primo Stato a vincere la corsa per padroneggiare la tecnologia quantistica avrà la supremazia sugli altri. Come le potenze nucleari, ci saranno potenze quantistiche nel mondo.»

Arnaud Dufournet, Responsabile marketing TheGreenBow

Questa minaccia latente, o l'uso malevolo della quantistica, consiste nell'attacco alle chiavi di crittografia asimmetrica. Porterebbe al collasso di tutti i sistemi informativi che si basano sulla crittografia ed è anche chiamata «apocalisse quantistica»', espressione tratta da un articolo della BBC ampiamente diffuso. Di cosa si tratta? Dal punto di vista aziendale, immaginate che la sicurezza dei vostri sistemi informativi non sia più garantita dall'oggi al domani. Una prospettiva molto reale secondo **Ilyas Khan** della società *Quantinuum* e **Harri Owen** della società *Post Quantum,* intervistati dalla stessa *BBC*: «*Tutto ciò che facciamo oggi su Internet, dagli acquisti online alle operazioni bancarie, è crittografato. Ma una volta che un computer quantistico funzionante sarà in grado di decifrare queste chiavi, potrebbe creare la possibilità di svuotare conti bancari o portafogli di criptovalute, oltre a far crollare i sistemi di difesa nazionale*».

Una minaccia informatica già presente

Ma qual è la natura delle nuove vulnerabilità causate dall'avvento dell'era quantistica? Riguardano quasi esclusivamente la sicurezza delle infrastrutture crittografiche, potenzialmente minate dalla potenza di calcolo quantistico che potrebbe abbattere gli attuali sistemi di crittografia asimmetrica (RSA, ECC, ecc.). Le possibili conseguenze sono l'usurpazione dell'identità dei server o di altre entità coinvolte negli scambi elettronici e/o nella decrittazione dei dati. **Fino a rendere possibile la violazione di una chiave RSA-2048 in meno di 24 ore?** Questa era la domanda posta nel «*Quantum Threat*

Timeline Report» nel 2021, con una proiezione sui prossimi 30 anni. Tra una proiezione a 5 anni e una proiezione a 30 anni, le visioni pessimistiche passano addirittura dal 2% a... l'80%. Alla fine di dicembre 2022, un team di ricercatori universitari cinesi ha annunciato in una pubblicazione di essere riuscito a decifrare l'algoritmo RSA-2048 utilizzando una macchina quantistica. Ma tale comunicazione pubblica solleva interrogativi: vero progresso tecnologico o monito per i Paesi occidentali? La questione rimane aperta.

Ma questi attacchi futuri possono essere preparati sui dati di oggi: nel suo parere dell'aprile 2022, l'agenzia francese ANSSI evoca infatti **il caso di cyberattacchi retroattivi chiamati *store now, decrypt later attack*** (memorizza adesso, decifra l'attacco più tardi). Da altri chiamato anche «*hackera ora, decifra più tardi*», «*raccogli ora, decifra più tardi*', «*cattura ora, decifra più tardi*»..., la tecnica consiste nel registrare oggi un numero molto elevato di dati e comunicazioni crittografati con l'obiettivo di decifrarli in seguito, una volta padroneggiata la tecnologia quantistica. «*Gli Stati Uniti hanno già visto questo tipo di attacco a dati di lunga durata, che possono riguardare le loro infrastrutture, i dati militari*», indica Arnaud Dufournet. Prima di pianificare: «*Nel settore bancario sarà sempre interessante disporre di dati sulle condizioni e sugli importi di alcune operazioni strategiche. Nel settore della difesa, le informazioni sui sottomarini saranno valide per decenni. Ma anche nel settore dell'energia, dell'automobile, dei segreti industriali... C'è già un urgente bisogno di proteggersi perché gli Stati iniziano a memorizzare i dati in attesa di poterli decifrare». «Anche nel settore medico francese si pone la questione, completa Yvan Vanhullebus, poiché la legge prevede che una struttura sanitaria (pubblica o privata) possa conservare le cartelle cliniche per 20 anni. In sicurezza, ovviamente*».

«Nel suo parere dell'aprile 2022, l'ANSSI evoca così il caso di cyberattacchi retroattivi denominati '»store now, decypt later attack» (memorizza adesso, decifra l'attacco più tardi). La tecnica consiste nel registrare oggi un numero molto elevato di dati e comunicazioni crittografati con l'obiettivo di decifrarli in seguito, a volte anni dopo, una volta che la tecnologia quantistica è stata padroneggiata.»

Infine, anche le criptovalute, incluso il tanto pubblicizzato Bitcoin, potrebbero vedere la loro infrastruttura corrotta, contrariamente alla loro reputazione di tecnologia non falsificabile. Secondo dei ricercatori dell'Università del Sussex nel Regno Unito, una macchina quantistica con 13 milioni di qubit potrebbe hackerare la blockchain del Bitcoin in sole 24 ore. Sarebbe quindi possibile dirottare le transazioni e svuotare i portafogli digitali delle attività. Altre ricerche sono meno allarmiste, spiegando che ci vorranno ancora uno o due decenni prima di raggiungere questo potere. Allo stato attuale, l'hacking della rete Bitcoin da parte di una macchina quantistica rimane quindi teorico.

IL NECESSARIO ADEGUAMENTO DEI PRODOTTI PER LA SICUREZZA

Una transizione graduale alla crittografia post-quantistica

Il futuro annientamento degli attuali algoritmi di protezione dei dati di fronte all'informatica quantistica segnerà il tramonto della crittografia? «*Se tutto il settore non reagisce in modo concertato, sì*», osserva Yvan Vanhullebus. Prima di precisare questa idea di un'obsolescenza programmata dei sistemi di crittografia: «*non esiste una vera alternativa, gli algoritmi, i protocolli e i sistemi dovranno evolversi*». Un'evoluzione che prevede lo sviluppo di algoritmi matematici in grado di resistere agli attacchi classici e ai futuri attacchi quantistici. Come alcuni algoritmi di cifratura simmetrica: se l'algoritmo AES128 è considerato «rotto» da un futuro computer quantistico, l'AES256 è considerato indebolito ma comunque abbastanza resistente. Negli Stati Uniti, questa prospettiva di sicurezza nazionale è presa molto sul serio. Nel 2015 il fisico canadese Michele Mosca ha presentato i risultati delle sue ricerche sulla quantistica e ha introdotto contemporaneamente il teorema che avrebbe portato il suo nome: il teorema di Mosca. Cercando di rispondere alla domanda «quando dovremmo preoccuparci della quantistica?», teorizzò così quello che sarebbe diventato uno dei precetti della quantistica. Se la somma del tempo in cui i dati crittografati devono rimanere al sicuro (X) e il tempo necessario per riattrezzare l'infrastruttura esistente con una soluzione di sicurezza quantistica su larga scala (Y) è maggiore del tempo necessario per costruire un computer quantistico su larga scala o qualsiasi altro progresso rilevante (Z), allora c'è qualcosa di cui preoccuparsi. Il NIST (Istituto nazionale di standard e tecnologia) americano nel 2016 ha lanciato un concorso sulla creazione di algoritmi post-quantistici. Un gruppo di quattro primi vincitori, e i loro algoritmi sono stati annunciati sei anni dopo, nell'estate del 2022, dopo diversi cicli di test e analisi su tutti i candidati. Un secondo gruppo di altri quattro algoritmi è ancora allo studio. Parallelamente, il direttore della cybersicurezza della NSA, Rob Joyce, ha spiegato contestualmente che l'agenzia aveva già classificato i propri algoritmi, sviluppati internamente.

Di fatto, **tutti coloro che si occupano di sicurezza informatica devono ormai accelerare la propria transizione verso un mondo post-quantistico.** Stanno emergendo diversi assi. Da un lato, la crittografia post-quantistica, che mira a studiare nuovi problemi matematici alla base dei protocolli di crittografia, in modo da renderli più resistenti agli attacchi che la nascita dei grandi computer quantistici renderebbe possibili. Dall'altra la crittografia quantistica, che modifica il supporto fisico delle informazioni affidandosi a nuove tecnologie quantistiche. La crittografia post-quantistica, per l'ANSSI, è «*il modo più promettente per difendersi dalla minaccia quantistica*». Tuttavia, la posizione dell'agenzia francese è più cauta rispetto alla sua controparte americana della NSA, che sta spingendo per la rapida adozione delle tecnologie post-quantistiche. In un parere completo sulla migrazione alla crittografia post-quantistica, pubblicato sul suo sito nell'aprile 2022, l'agenzia francese consiglia ai produttori di passare gradualmente agli algoritmi post-quantistici. Un meccanismo ibrido che ha quindi il vantaggio di combinare

«*i calcoli di un algoritmo a chiave pubblica pre-quantistico riconosciuto e di un ulteriore algoritmo post-quantistico*» e di «*beneficiare sia della forte garanzia sulla resistenza del primo contro gli aggressori classici sia della presunta resistenza del secondo contro gli aggressori quantistici*». E gli editori, dovranno anch'essi cambiare i propri protocolli di crittografia per conformarsi alle crittografie post-quantistiche? Per Noël Chazotte, questa transizione dovrà avvenire, ma rimane una grande incognita: quale programma di implementazione? E con quali algoritmi? «*Su questo tema non si può che andare nella direzione dell'ANSSI: il settore non è ancora maturo. Ed è impossibile prevedere come si comporteranno gli algoritmi post-quantistici tra cinque anni., osserva. L'algoritmo SIKE è stato, ad esempio, per molto tempo una vera promessa su questo tema della quantistica, prima che fosse rivelata la sua vulnerabilità a un attacco classico nell'estate del 2022 dai ricercatori belgi...*».

La distribuzione a chiave quantistica (QKD) per applicazioni precise

Esistono alternative alla crittografia post-quantistica, ma sono meno promettenti perché sono limitate ad applicazioni specifiche. È il caso della distribuzione a chiave quantistica (*Quantum key distribution, QKD*). Si tratta di un insieme di protocolli per distribuire una chiave di cifratura tra due interlocutori distanti, garantendo al tempo stesso la sicurezza della trasmissione grazie alle leggi della fisica quantistica e della teoria dell'informazione. Si tratta di una famiglia di metodi basati su principi fisici e non matematici come avviene per la normale crittografia. Permette a due corrispondenti di costruire «un segreto comune» (una chiave) per dialogare. La QKD è generalmente proposta per stabilire comunicazioni riservate e integre, cioè non modificabili da un aggressore. Per questo sono necessari due canali: un canale con proprietà fisiche controllate (una fibra ottica o un collegamento diretto all'aria aperta) senza alcun dispositivo che interagisca con le informazioni trasportate e un collegamento di rete convenzionale.

La QKD è quindi totalmente dipendente dalle caratteristiche fisiche dei canali che utilizza, il che rende la sua implementazione su larga scala «*complessa e costosa*» ritiene l'ANSSI. Inoltre l'agenzia francese ritiene che la distribuzione di chiavi quantistiche non costituisca «*il naturale percorso evolutivo delle comunicazioni sicure*». Il motivo: l'assenza di una linea diretta che collega due punti costringe gli utenti a negoziare le chiavi in sezioni su un percorso composto da più nodi. Tuttavia ciò richiede di avere fiducia in questi intermediari. Fatto che costituisce «*un importante passo indietro rispetto agli attuali metodi di negoziazione di chiave end-to-end*», rileva l'autorità. Questa tecnologia potrebbe quindi essere utilizzata solo per applicazioni di nicchia.

Dalla teoria all'industrializzazione

L'era dell'informatica quantistica è appena iniziata e le sfide sono già numerose. Il monitoraggio attivo, l'anticipazione, l'agilità e l'adattamento a questa nuova minaccia sono ora bussole essenziali per navigare tra l'informatica quantistica e la cybersicurezza. Da un lato, la corsa tecnologica verso il computer quantistico è complessa e costosa. Anche gli investimenti di bilancio, dell'ordine di diverse decine di miliardi di euro, rappresentano un grosso ostacolo. È complessa e costosa anche la necessità di protezioni crittografiche contro gli attacchi quantistici. Per Yvan Vanhullebus, «*se la fase teorica è già stata superata, ci sono ancora molte fasi importanti da realizzare prima di arrivare all'era dell'industrializzazione*». La standardizzazione dei primi algoritmi è stata una di queste, ma – recente com'è – ha ancora bisogno di tempo per poterne valutare realmente la solidità e la robustezza. Allo stesso tempo, sarà necessario anche produrre altri standard per il loro utilizzo in un contesto ibrido, come raccomandato dall'ANSSI. La questione si pone sin da oggi anche a livello di componenti hardware, che per loro stessa natura vivono una vera e propria inerzia. «*Questo è un argomento che abbiamo affrontato presto e molto seriamente a Stormshield, spiega Yvan Vanhullebus. Per i nostri firewall Stormshield Network Security, ad esempio, stiamo già integrando gli ultimi TPM Infineon, l'unico componente TPM sul mercato a offrire una protezione post-quantistica*».

È importante che tutti i soggetti che si occupano di cybersicurezza mettano in atto sin da ora misure per anticipare l'era dell'informatica quantistica e quella della crittografia post-quantistica. **L'obiettivo? Non essere vittime ma protagonisti di questa grande evoluzione tecnologica.** In questo contesto, l'Europa sta cercando il suo posto.