A prova di futuro

Il percorso verso la sicurezza quantum-safe

Vanguard Report

Aprile 2022

Commissionato da

IBM

451 Research

S&P Global
Market Intelligence

L’autore

John Abbott

Principal Research Analyst, 4SIGHT

John Abbott tratta argomenti concernenti sistemi, archiviazione e infrastruttura software per 451 Research, che fa parte di S&P Global Market Intelligence. Nel corso di oltre 30 anni di carriera, è stato uno dei pionieri in materia di tecnologia specialistica in aree tematiche come Unix, supercomputer, architettura di sistema, sviluppo software e archiviazione.

Nell’ottobre 1999 Abbott, tra i co-fondatori di The 451 Group, ha condotto operazioni analitiche dalla sede di San Francisco. È stato l’autore principale di tanti report speciali di 451 Research, tra cui quelli sulla virtualizzazione dello storage e sui blade server, le prime indagini complete su entrambi i soggetti a essere state pubblicate. Più recentemente, John si è concentrato su argomenti come infrastrutture convergenti, nuove architetture di sistema e acceleratori IA e deep learning. Ha contribuito alla fondazione di 4SIGHT, il framework di 451 Research che tratta in maniera innovativa e a lungo termine le tecnologie emergenti.

Abbott ha iniziato a occuparsi del settore tecnologico nel 1984, facendo leva sulla sua precedente esperienza come autore tecnico e sul coinvolgimento diretto nell’utilizzo di mainframe, primi PC e workstation Unix. Da giornalista freelance ha collaborato con diverse riviste, tra cui Computing, Computer Weekly, The Financial Times e The Times. Nel 1987, è stato nominato redattore della newsletter settimanale Unix di ComputerWire, di Unigram.X, e in seguito è divenuto redattore del servizio quotidiano Computergram International dell’azienda, prima a Londra e successivamente a San Francisco. Ha istituito la sede di San Francisco di 451 Research e ha vissuto nella città per oltre un decennio.

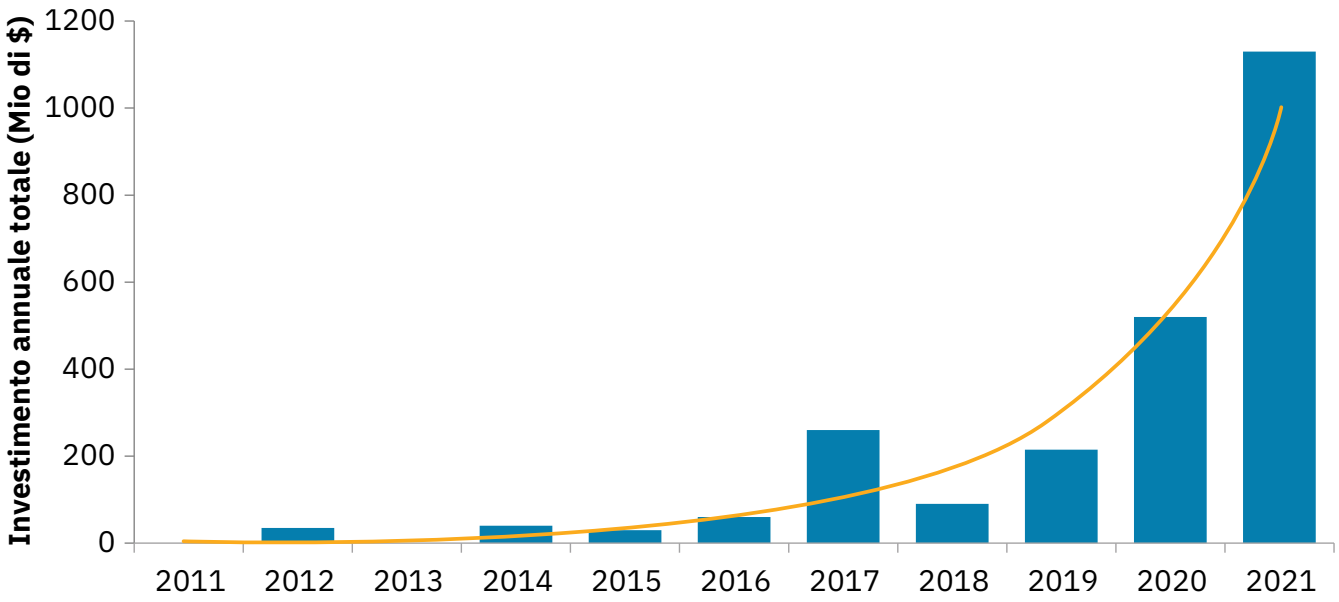
Ha studiato musica presso la University of Keele e ha conseguito un MA in Letteratura inglese moderna presso la University of London.

Introduzione

Il miglior modo per descrivere, oggi, l'informatica quantistica è un investimento ad alto rischio e ad alto rendimento. Che un computer quantistico universale e funzionale sia attualmente realizzabile è tutt'altro che garantito. Ma i laboratori di ricerca (e sempre più aziende private nel settore tecnologico) stanno portandosi giorno per giorno sempre più all'avanguardia nell'innovazione e nella scienza. Ne potrebbero derivare enormi vantaggi, in grado di risolvere i problemi che attualmente limitano le capacità dei (classici) supercomputer. Per questo, venditori e utenti si lanciano volentieri in una tecnologia che è potenzialmente dirompente. Secondo i dati di S&P Capital IP Pro (figura 1), negli ultimi dieci anni sono stati investiti 2,4 miliardi di dollari in startup quantistiche. Il 2021 ha registrato un'importante crescita di interesse, con 1,1 miliardi di dollari investiti in aziende quantistiche. Questi dati, per di più, non includono i grossi investimenti di aziende IT affermate, tra cui IBM, Amazon, Google e Honeywell.

Ma se da un lato le opportunità sono grandi, dall'altro sussistono alcune non trascurabili perplessità. La più concreta delle quali è probabilmente quella delle minacce alle attuali prassi di sicurezza. Con l'informatica quantistica, alcuni malintenzionati potrebbero falsificare le firme digitali e decifrare gli attuali livelli di crittografia e codifica, inclusa l'infrastruttura a chiave pubblica profondamente radicata nei sistemi IT di tutto il mondo. Ancora più preoccupante è il fatto che i dati codificati e attualmente protetti possano essere archiviati, per poi essere decodificati una volta che l'informatica quantistica si sarà effettivamente sviluppata. Non si può differire la risoluzione di un tale problema. Più aspettiamo, più i dati che creiamo sono a rischio.

Figura 1: Investimenti in startup di informatica quantistica



Fonte: S&P Capital IQ Pro

L'approccio di 451 Reseach

Non è possibile prevedere esattamente quando i computer quantistici capaci di elaborare l'algoritmo di Shor saranno abbastanza diffusi da poter finire in mano ai malintenzionati. Finora, nessun produttore IT ha fornito un'ipotesi su quando l'informatica quantistica supererà significativamente le prestazioni dei computer tradizionali. Ma i rapidi passi in avanti compiuti negli ultimi cinque anni dalla tecnologia e i notevoli investimenti attuali suggeriscono che ciò dovrebbe avvenire entro la fine del decennio. A quel punto, tutti i dati attualmente protetti da algoritmi a chiave pubblica saranno a rischio di esposizione. Per gli enti governativi che si occupano di difesa e intelligence, nonché per i fornitori di servizi cloud e sistemi i cui clienti appartengono a settori regolamentati, il rischio è già troppo alto per essere ignorato. Nonostante i falsi allarmi del passato (si pensi a Y2K, quando una scorciatoia di programmazione largamente utilizzata minacciò di creare scompiglio nel passaggio dall'anno 1999 al 2000) e l'incertezza del futuro, una cosa è chiara: il pericolo proveniente dagli attacchi informatici rappresenta oggi un grosso problema, e la tipologia delle minacce e la vulnerabilità dei sistemi sono in costante evoluzione. Le policy di sicurezza vanno continuamente riviste e aggiornate, e le tecnologie crittografiche quantum-safe, insieme all'implementazione di agilità e inventari crittografici, costituiscono oggi elementi importanti.

Scenari post-quantum e quantum-safe

La questione è la seguente: l'attuale generazione degli algoritmi più diffusi si basa su problemi matematici di elevata difficoltà, troppo complessi perché i computer tradizionali riescano a violarli. Gli stessi problemi, però, possono essere facilmente risolti da un computer quantistico che sia sufficientemente potente: e questo si sa già dal 1994, cioè da quando il matematico americano Peter Shor ideò l'algoritmo in tempo polinomiale, oggi noto come algoritmo di Shor. Il primo computer quantistico fu costruito tre anni dopo. Nell'ultimo decennio si è assistito a un considerevole sviluppo degli algoritmi quantum-safe. Ma la conversione dai sistemi di crittografia a chiave pubblica, oggi ampiamente utilizzati dalle amministrazioni e nell'industria, a un nuovo sistema di algoritmi potrebbe richiedere decenni.

Ecco perché negli Stati Uniti organizzazioni come il National Institute of Standards and Technology (NIST) e il Department of Homeland Security hanno lavorato sia sul processo di standardizzazione degli algoritmi, sia alla formulazione di raccomandazioni per preparare le aziende alla transizione verso una crittografia post-quantistica. Da quel lavoro, a gennaio è scaturita una relazione della Casa Bianca che imponeva ai servizi di difesa e di intelligence del governo di avviare la transizione.

Violare un numero intero composto da 2.048 bit (trovando i fattori primi) coi computer più potenti oggi a disposizione richiederebbe milioni di anni. Con un computer quantistico una simile operazione potrebbe teoricamente essere portata a termine in alcune ore. Gli attuali schemi di chiavi pubbliche violati dall'algoritmo di Shor includono il venerando algoritmo RSA (ormai vecchio di 45 anni, ma ancora utilizzato per quasi tutte le transazioni su Internet) e il Data Security Standard, il crittosistema Paillier, l'algoritmo di firma digitale della curva ellittica, la curva ellittica Diffie-Hellman e il sistema di cifratura ElGamal. Il problema che stiamo affrontando interessa un lungo elenco di standard stabiliti da NIST, ISO/IEC, ETSI e IETF, il che significa che è il problema è di portata internazionale: sono stati violati anche l'algoritmo di firma digitale SM2 e lo standard nazionale di crittografia SM9 cinesi.

Il processo di standardizzazione NIST, avviato nel 2016 con un bando che invitava a presentare proposte, ha individuato un nuovo set di soluzioni post-quantum. Raggruppate per varietà di approccio (crittografia basata sui reticoli, multivariata, di hash, o basata su codice), queste soluzioni includono CRYSTALS-Kyber, metodo di incapsulamento chiave (KEM, key encapsulation mechanism) basato sui reticoli, McEliece (KEM basato su codice) e Falcon (basato sui reticoli), oltre a schemi di firma post-quantistica Rainbow (multivariata). Dopo la terza fase della gara, appena completata, questi e altri candidati selezionati si stanno muovendo verso la standardizzazione. La quarta fase, che include l'individuazione di algoritmi alternativi e un bando per ulteriori schemi di firma digitale, inizia quest'anno e terminerà entro la fine del 2024.

Figura 2: Tappe verso un quantum-safe maturo

Fonte: 451 Research

Il percorso verso una crittografia quantum-safe

Quali azioni dovrebbero intraprendere ora le aziende al fine di gettare le basi per l'integrazione di una crittografia quantum-safe nelle proprie architetture di sicurezza dei dati nei prossimi dieci anni? Il primo passo, già in corso, è partecipare al processo di standardizzazione. Per ogni azienda che sia interessata a prevenire le autenticazioni fraudolente, proteggere l'integrità delle codifiche ed evitare la compromissione della firma digitale, è importante agire per garantire che i propri requisiti siano in linea con quanto previsto dall'elenco approvato di algoritmi, processori e strumenti definitivi. Nonostante gli ottimi progressi da parte degli organi di standardizzazione, bisogna continuare a lavorare: saranno necessari più algoritmi. Inoltre, per raggiungere la sicurezza quantistica sono necessarie le seguenti fasi di maturità.

- **Rilevamento e classificazione dati.** Realizzazione di un inventario di dati critici. Quale ha maggior valore? Dove sono posizionati i dati? Quali sono i requisiti di conformità? Comprendere ciò è fondamentale perché molte aziende non sono consapevoli di ciò di cui sono in possesso e di quanto valga. E senza questa consapevolezza, non sono in grado di individuare i propri punti deboli. Devono creare e gestire un inventario di dati con proprietà definite.
- **Inventario crittografico.** Un inventario crittografico descrive dove e quanto sia vulnerabile la crittografia a chiave pubblica in uso e contiene dettagli come certificati, protocolli di cifratura, algoritmi e dimensioni delle chiavi. L'inventario deve essere gestito per coprire l'intero ciclo di vita di certificati e chiavi crittografiche.
- **Agilità crittografica.** All'interno dei propri programmi e processi di transizione, le aziende devono considerare l'agilità crittografica, in modo da potersi adeguare senza traumi all'evoluzione tecnologica e ai cambiamenti situazionali. Devono progettare e integrare procedure che aggiornino o sostituiscano l'attuale generazione di procedure crittografiche, testandone quindi l'efficacia, più facilmente entro tempi ben definiti.
- **Quantum-safe (crittografia post quantistica).** Le aziende devono implementare nuovi algoritmi, consapevoli del potenziale impatto della crittografia quantum-safe sulle proprie attività.

Le aziende differiscono le une dalle altre e non tutte saranno nelle condizioni (o avranno la mentalità) per modificare tutto, per esempio a causa dei costi o dei problemi di gestione del ciclo di vita. Ma investire nella capacità di aggiornare o sostituire i protocolli di sicurezza è fondamentale, sia a breve che a lungo termine. Poiché strettamente correlata all'infrastruttura del sistema, conseguire l'agilità crittografica richiederà la collaborazione di progettisti di sistemi, sviluppatori di applicazioni ed esperti di sicurezza. Al momento si registra una carenza di strumenti in grado di favorire tale processo.

Le aziende useranno una varietà di fattori per dare priorità all'adozione della crittografia quantum-safe: il valore dei beni protetti; la vulnerabilità di ciò che deve essere protetto (per es., archivi di chiavi e password); quali sistemi collegati potrebbero risultare interessati (per es., condivisione delle informazioni con soggetti esterni, come gli enti governativi); il modo in cui i dati devono essere protetti. Durante il lungo periodo di transizione, saranno necessari schemi ibridi che combinino algoritmi classici e quantum-safe.

Implementazione, motivazione e driver

I grandi fornitori di sistemi e servizi cloud le cui apparecchiature e infrastrutture ospitano carichi di lavoro aziendali mission-critical non possono permettersi il lusso di attendere il completamento degli standard di crittografia quantum-safe. I fornitori stanno lavorando su questo problema da diversi anni e hanno contribuito alla scelta di algoritmi e protocolli che sono seri candidati ad entrare nell'elenco degli standard nel 2024. Un certo numero di servizi di gestione delle chiavi basati su cloud già supporta gli algoritmi della seconda e della terza fase. I clienti cominciano a utilizzare questi servizi per misurare il potenziale impatto sulle performance delle loro applicazioni di un probabile sovraccarico sull'utilizzo della larghezza di banda e sulla latenza, e per mitigare i probabili errori di connessione ai layer dei proxy Transport Level Security. Ma tutti concordano che, poiché gli standard e la tecnologia evolvono, la transizione ai sistemi di sicurezza quantum-safe richiederà un percorso che durerà anni, e che questo percorso inizia proteggendo l'infrastruttura IT.

Nel mondo dei sistemi, i mainframe sono ancora ampiamente utilizzati, in quanto infrastruttura IT altamente disponibile e sicura per grandi banche, compagnie assicurative, telecomunicazioni, vendita al dettaglio e attività di trasporto; una posizione che hanno mantenuto per oltre mezzo secolo. Le nuovissime generazioni di mainframe saranno dotate di moduli di sicurezza hardware quantum-safe, che lavorano insieme a componenti aggiornati del sistema operativo, gestione delle chiavi API e supporto, per una suite di algoritmi capaci di resistere alla quantistica emergente. Per proteggere l'integrità del firmware di avvio sistema sarà utilizzata una tecnologia di avvio quantum-safe, con un hardware root-of-trust, mentre per lo scambio sicuro di chiavi crittografiche con i partner commerciali saranno forniti meccanismi quantum-safe attraverso le interfacce di programmazione delle applicazioni.

I provider e venditori di servizi cloud devono giocare un ruolo importante per aiutare i propri clienti nel passaggio a una crittografia quantum-safe. Le disposizioni normative di per sé non sono sufficienti, perché in genere non sono abbastanza prescrittive da fornire delle linee guida chiare alle aziende prive di grande esperienza. I fornitori già al centro dell'infrastruttura mission-critical possono semplificare il processo fornendo la protezione del sistema aziendale centrale senza ulteriori modifiche a livello di sistema per l'attivazione. Inoltre, possono fornire gli strumenti di rilevamento necessari per l'analisi delle applicazioni crittografiche. Le aziende che gestiscono dati devono fare in modo che le informazioni in loro possesso siano protette durante l'intero ciclo di vita (oggi quanto in futuro), perché i dati che oggi vengono criptati utilizzando i classici algoritmi, in futuro, potrebbero essere decodificati da un computer quantistico avanzato. Significa che, se i dati devono essere protetti per 20 anni, ci si spinge oltre il 2040. Anche gli scettici, secondo cui un'informatica quantistica funzionale è ancora molti anni di là da venire, devono sapere che, vista l'attuale velocità dell'innovazione tecnologica, a quel punto le probabilità saranno notevolmente aumentate.

Conclusioni

Il business case per l'informatica quantistica è solido: un computer quantistico del tutto efficiente consentirebbe notevoli opportunità di sviluppo in campi quali chimica, apprendimento automatico, finanza, trasporti, assistenza sanitaria e molto altro. I computer quantistici sarebbero in grado di accelerare in maniera esponenziale l'elaborazione di equazioni oggi impossibili per gli algoritmi deterministici dei computer attualmente in uso.

Il rovescio della medaglia è rappresentato dalle conseguenze che l'informatica quantistica potrebbe avere sulla già crescente minaccia alla protezioni di dati e privacy proveniente dai cyberattacchi. Con l'aumento del valore commerciale dei dati, crescono anche la scalabilità e i costi dei requisiti di protezione dei dati. E poiché il valore dei dati è duraturo nel tempo, bisogna tener conto della crescente probabilità che, in un futuro non troppo lontano, l'informatica quantistica diventi una diffusa realtà. Agire subito, piuttosto che più in là nel tempo, si tradurrebbe in un'evoluzione più sicura e controllata verso un'infrastruttura IT quantum-safe, nell'implementazione di strumenti capaci di rilevare le attuali vulnerabilità dei livelli di applicazioni, nella protezione dei sistemi di scambio chiavi tra le aziende e nella protezione continua dei segreti a lungo termine contenuti nei dati.

CONTATTI

Americhe
+1 877 863 1306
market.intelligence@spglobal.com

Europa, Medio Oriente, Africa
+44 20 7176 1234
market.intelligence@spglobal.com

Asia-Pacifico
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence