CRITTOGRAFIA QUANTISTICA: LA SICUREZZA DEI DATI A LUNGO TERMINE NELL'ERA POST-QUANTUM

a cura di ING. M. RASO
visto da: ING. P. ROCCO, ING. M. NAVA
Commissione SICUREZZA INFORMATICA

Rischi e contromisure per contrastare l'evoluzione tecnologica dei computer quantistici

CRITTOGRAFIA QUANTISTICA: LA SICUREZZA DEI DATI A LUNGO TERMINE NELL'ERA POST-QUANTUM

a cura di ING. M. RASO
visto da: ING. P. ROCCO, ING. M. NAVA
Commissione SICUREZZA INFORMATICA

Rischi e contromisure per contrastare l'evoluzione tecnologica dei computer quantistici

È comunemente accettato che una volta che le informazioni siano state crittografate in modo sicuro, esse siano al riparo da sguardi indiscreti e da eventuali azioni di sabotaggio ancorché future. Tuttavia, la sicurezza a lungo termine offerta da molti sistemi di crittografia (noti anche come crittosistemi) è gravemente minacciata. Un nuovo tipo di computer, il computer quantistico, è stato teoricamente dimostrato in grado di rompere la maggior parte dei sistemi di crittografia di uso comune, prevedendo che tali computer siano disponibili entro i prossimi 15 anni.
Così reale è questa minaccia che lo statunitense NIST (*National Institute for Standards and Technology*) sta sollecitando proposte da tutto il mondo per valutare e infine standardizzare la crittografia nell'era *post-quantum* (*Fig. 1*). Ciò influisce direttamente sulle decisioni di acquisto di tecnologia da parte dei CISO (*Chief Information Security Officer*) e dei CTO (*Chief Technology Officer*), poiché la legislazione in tema di *privacy* in taluni paesi richiede, ad esempio, che informazioni come le cartelle cliniche siano mantenute riservate anche dopo la morte di una persona. Per tale ragione, un acquirente di prodotti di crittografia deve affrontare due scelte:

- acquistare un crittosistema che sia sicuro a lungo termine. Attualmente solo una minoranza di sistemi soddisfa questo requisito e possono essere facilmente identificati con il loro nome, crittografia "*quantum resistant*" o "*post-quantum*";
- acquistare un crittosistema che non sia sicuro a lungo termine e accettare che i dati crittografati rimangano riservati solo fino all'anno 2030 circa.

Questo articolo, infatti, vuole essere un'introduzione ai dettagli tecnici relativi ai computer quantistici e al loro impatto sulla rottura di molti dei moderni sistemi di crittografia.

Figura 1:
Workshops e Timeline del processo selettivo avviato dal NIST. Il NIST ha avviato un processo per sollecitare, valutare e standardizzare uno o più algoritmi crittografici resistenti alla potenza computazionale dei computer quantistici. Come primo passo in questo processo, il NIST ha richiesto commenti pubblici su bozze di requisiti minimi di accettabilità, requisiti di presentazione e criteri di valutazione per gli algoritmi candidati. https://csrc.nist.gov/projects/post-quantum-cryptography/workshops-and-timeline

Quale sarà la sicurezza dei dati nel lungo periodo?

La sicurezza dei dati non costituisce un elemento assoluto: dipende dal modo in cui la crittografia viene implementata e utilizzata, nonché dalle risorse dell'aggressore. Nondimeno la sicurezza dei dati degrada nel tempo! Predisporre un piano a lungo termine significa, dunque, proteggere i dati sensibili in un periodo minimo di 20-30 anni, che può essere raggiunto solo prevedendo la resistenza a potenziali attacchi nel futuro e scegliendo di conseguenza la giusta tecnologia. Ciononostante, la sicurezza dei dati a lungo termine è vista sempre più come un problema per legislatori e tecnologi. Ad esempio, la legge tedesca stabilisce infatti che i dati medici e legali restino riservati da terzi anche dopo la morte di un paziente o di un cliente. Allo stesso modo alcuni archivi di dati riservati avranno probabilmente una durata più lunga del tempo necessario ai computer quantistici per minacciare gli algoritmi crittografici convenzionali.
Inizieremo esaminando la direzione lungo la quale si stanno indirizzando le tecnologie informatiche nei prossimi decenni. In particolare, discuteremo delle minacce agli approcci crittogra-

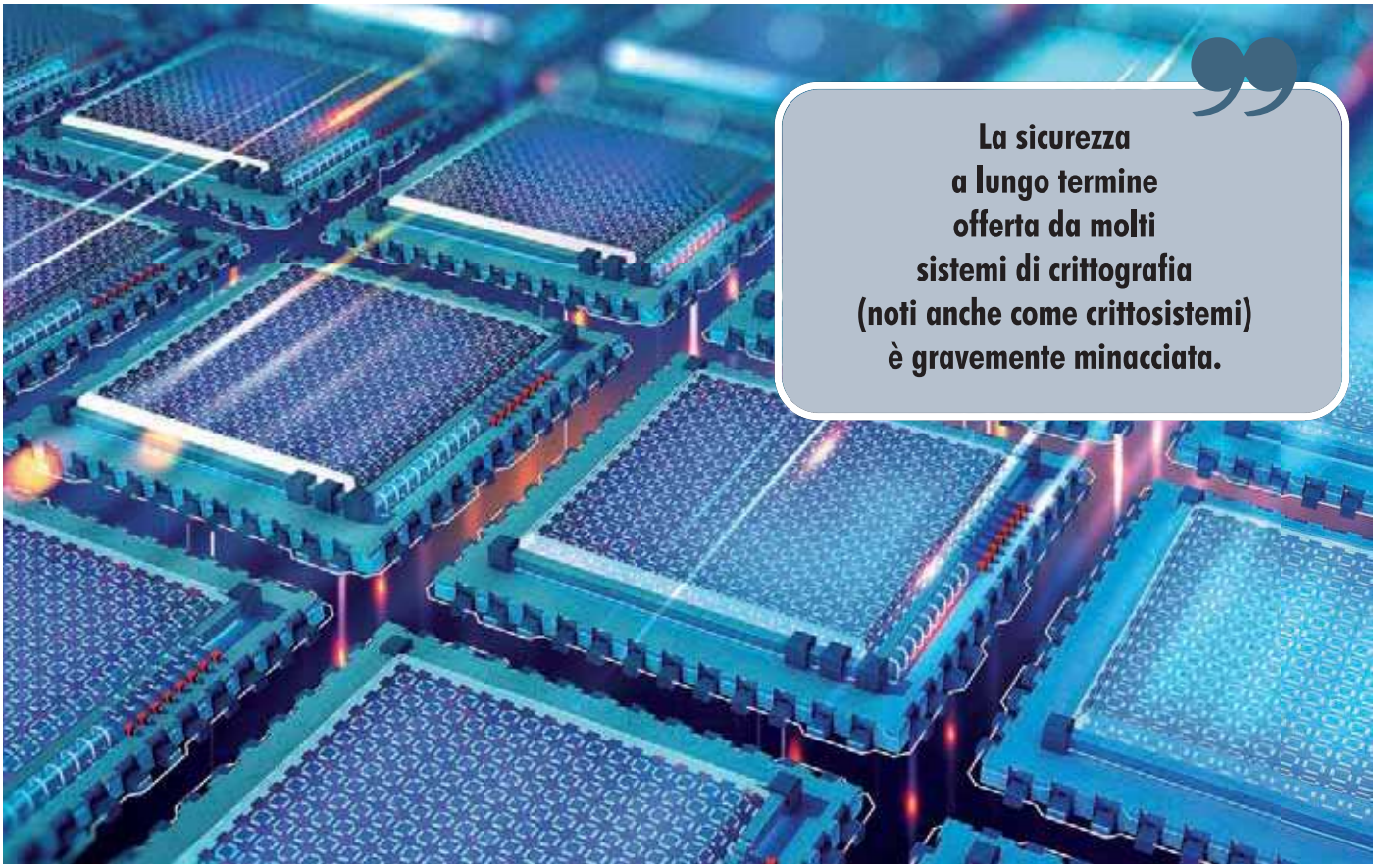
fici convenzionali e di alcuni suggerimenti su come mitigare questo rischio.

Computer classici e quantistici

I computer "classici" sono i computer che già conosciamo ed usiamo. Formalmente noti come calcolatori elettronici digitali binari, essi operano rappresentando le informazioni come sequenze di 0 e 1 ("cifre binarie" o "*bit*"), elaborandole con dispositivi basati sulla fisica degli elettroni ("calcolatori elettronici"). Ogni *bit* può contenere uno dei due valori: 0 o 1 e non ci sono valori intermedi. I calcolatori elettronici eseguono algoritmi su questi *bit* utilizzando semplici operazioni logiche (AND, OR, NOT, etc.) per ottenere risultati utili.
Nei primi anni '80 fu proposta una nuova classe di dispositivi di calcolo che utilizzava *bit* quantistici ("*qubit*") anziché *bit*. A differenza dei *bit*, i *qubit* possono trovarsi in una combinazione di stati, quindi mantenere una sovrapposizione di stati 0 e 1 in qualsiasi momento (*Fig. 2*). All'aumentare del numero di *qubit*, aumenta anche il numero di stati detenuti dall'insieme di *qubit*. I *qubit* vengono elaborati utilizzando computer quantistici i quali eseguono algoritmi che utilizzano *gate* quantici, ossia blocchi di costruzioni logiche che operano su tutti gli stati possibili di un insieme di *qubit*, simultaneamente. Una volta completato il calcolo quantistico, l'*output* viene misurato, e ciò fa collassare la sovrapposizione multipla di stati in un singolo stato classico. I computer quantistici con molti *qubit* sono teoricamente in grado di funzionare molto più velocemente di qualsiasi computer classico. Tuttavia, i computer quantistici non sostituiranno i computer classici: entrambi hanno i loro punti di forza e di debolezza.

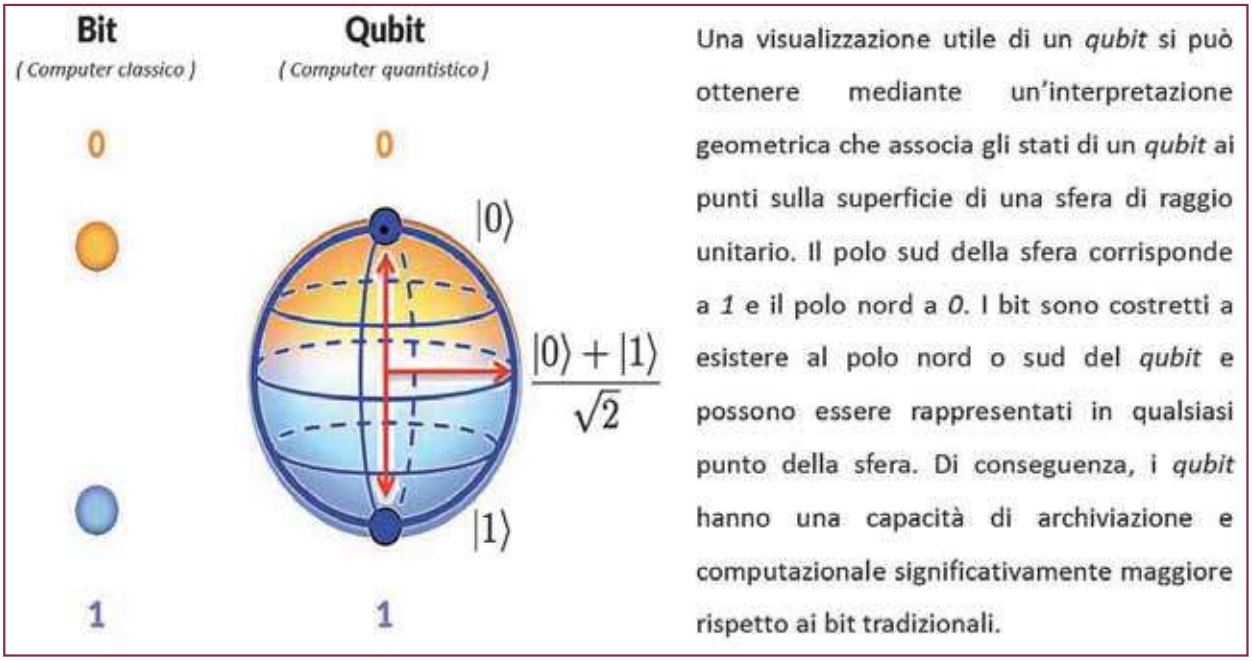
Algoritmi

Un algoritmo è una sequenza ordinata e finita di passi elementari (operazioni o istruzioni) che con-



La sicurezza a lungo termine offerta da molti sistemi di crittografia (noti anche come crittosistemi) è gravemente minacciata.

Figura 2:
Descrizione astratta di un qubit come vettore in uno spazio bidimensionale.
Un qualsiasi sistema fisico con almeno due livelli di energia discreti e sufficientemente separati è un candidato appropriato per rappresentare un qubit. I tre approcci più comuni per realizzare fisicamente un qubit sono quelli basati su:
– le due diverse polarizzazione di un fotone;
– l'allineamento di uno spin nucleare in un campo magnetico uniforme;
– due livelli di energia di un elettrone che orbita in un singolo atomo.



duce a un ben determinato risultato in un tempo finito. Lo scopo degli algoritmi crittografici è quello di crittografare un testo in chiaro in un testo cifrato, codificato utilizzando una chiave. Il testo cifrato può essere riconvertito in un testo in chiaro leggibile utilizzando un algoritmo di decifratura complementare, insieme alla chiave.
Un importante algoritmo quantistico è l'algoritmo di Shor, sviluppato nel 1995, che decompone un numero intero nei suoi fattori (numeri primi). Ad esempio, il numero 6344 può essere scomposto come segue: 1x2x2x2x13x61. La fattorizzazione dei numeri infatti diventa difficile man mano che l'ordine di grandezza aumenta. In precedenza, potevano essere necessari quadrilioni di anni di calcolo per fattorizzare un intero composto da centinaia di cifre su un computer classico. L'algoritmo di Shor che opera su un computer quantistico sufficientemente potente, potrebbe invece fattorizzare lo stesso numero in diversi giorni di calcolo.

Crittografia classica a chiave pubblica (o asimmetrica)

Una forma di algoritmo crittografico è quello cosiddetto della chiave pubblica, in cui due parti (tradizionalmente indicate come Alice e Bob) desiderano comunicare segretamente su un canale non sicuro. Nella crittografia a chiave pubblica, Alice e Bob creano ciascuno chiavi pubbliche e private. La chiave pubblica di Alice viene inviata a Bob e utilizzata da lui per crittografare il messaggio ad Alice, che può essere decifrato da lei solo con la sua chiave privata (che lei mantiene segreta). Allo stesso modo, la chiave pubblica di Bob viene inviata ad Alice affinché possa crittografare il messaggio indirizzato a Bob (*Fig. 3*).
Le chiavi pubbliche e private sono correlate alla fattorizzazione di grandi numeri. Migliorare l'approccio alla fattorizzazione, con l'algoritmo di Shor in esecuzione su un computer quantistico adeguatamente potente, accrescerà di certo la

probabilità di rompere un crittosistema a chiave pubblica. Questi algoritmi non sono quindi ritenuti infrangibili, poiché la loro inviolabilità diminuisce con l'aumento della capacità di calcolo dei computer quantistici (*Fig. 4*).

Crittografia classica simmetrica

Un'altra forma di algoritmo crittografico classico utilizza la crittografia simmetrica, in cui Alice e Bob condividono una singola chiave e questa viene utilizzata per tutte le operazioni di cifratura e decifratura. La chiave incapsula tutta la segretezza in questo processo e i dati possono essere decifrati solo con la chiave corretta. Non vi è alcuna segretezza incorporata nell'algoritmo, che si presume sia noto a qualsiasi potenziale aggressore. In generale, algoritmi di crittografia simmetrici come AES (*Advanced Encryption Standard*) e il suo predecessore, ora non sicuro, *DES* (*Data Encryption Standard*), non comportano la fattorizzazione di interi e l'algoritmo di *Shor* non fornisce pertanto alcun vantaggio. Tuttavia, gli algoritmi di crittografia simmetrica sono influenzati da un diverso attacco quantistico: l'algoritmo di Grover. Quest'ultimo è in grado di fornire una significativa accelerazione trovando la soluzione in un tempo medio pari alla radice quadrata del tempo impiegato da un computer classico. Ad esempio, se un computer classico ha bisogno di cercare 2 ^ 56 possibili chiavi per garantire la decodificazione della crittografia DES, un computer quantistico che esegue l'algoritmo di Grover ha solo bisogno di fare 2 ^ 28 ricerche. Questo è più facile da capire quando è rappresentato in notazione convenzionale:

- computer classico: 2^{56} ricerche = 72 057 594 037 927 936 ricerche;
- computer quantistico: 2^{28} ricerche = 268 435 456 ricerche.

In termini di unità di tempo, rispetto ad un attacco con tecniche di crittoanalisi, se un computer classico impiegherebbe un giorno per scardinare una chiave a 56 *bit*, il computer quantistico impiegherà solo 0,322 millisecondi. Allo stesso modo, un computer classico impiegherebbe un anno per rompere la codifica di un messaggio cifrato con un chiave a 64 *bit*, mentre un computer quantistico attuerebbe l'attacco in 7,3 millisecondi.

Dunque, per contrastare questa accelerazione quantistica, è necessario utilizzare chiavi di dimensioni maggiori. Affinché la crittografia simme-

Figura 3:
Crittografia moderna basata su chiave pubblica (asimmetrica)

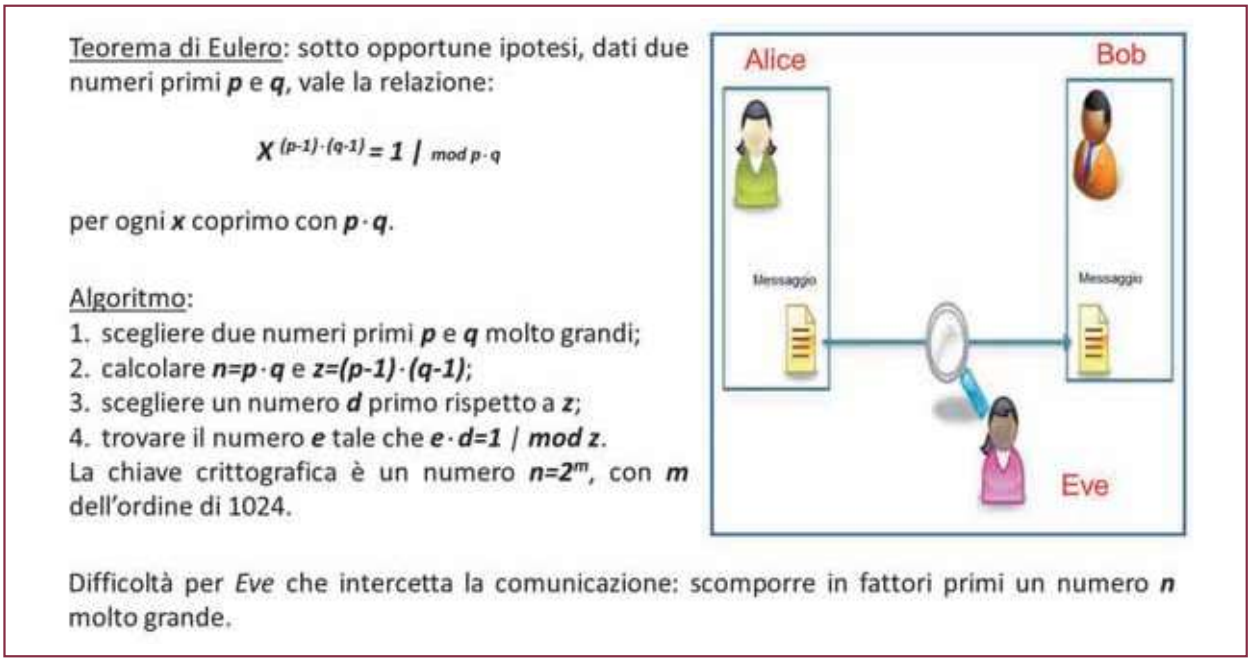


Figura 4:
Sicurezza degli algoritmi di crittografia nell'era post-quantum.

Cifrari a chiave asimmetrica	Sicurezza nell'era *post-quantum*
RSA-1024, RSA-2048, RSA-4096	Insicuro
ECC-256, ECC-521	Insicuro
Diffie-Hellman	Insicuro
Curve ellittiche Diffie-Hellman (ECDHP)	Insicuro

Cifrari a chiave simmetrica	Sicurezza nell'era *post-quantum*
3DES	Insicuro
AES-128	Insicuro
AES-256	Sicuro

trica sia considerata resistente a livello quantistico, è necessario avere una lunghezza della chiave di 256 *bit*. Un sistema di crittografia quale l'AES-256 sarà equivalente all'AES-128 in un mondo post-quantistico (cit. *Fig. 4*).

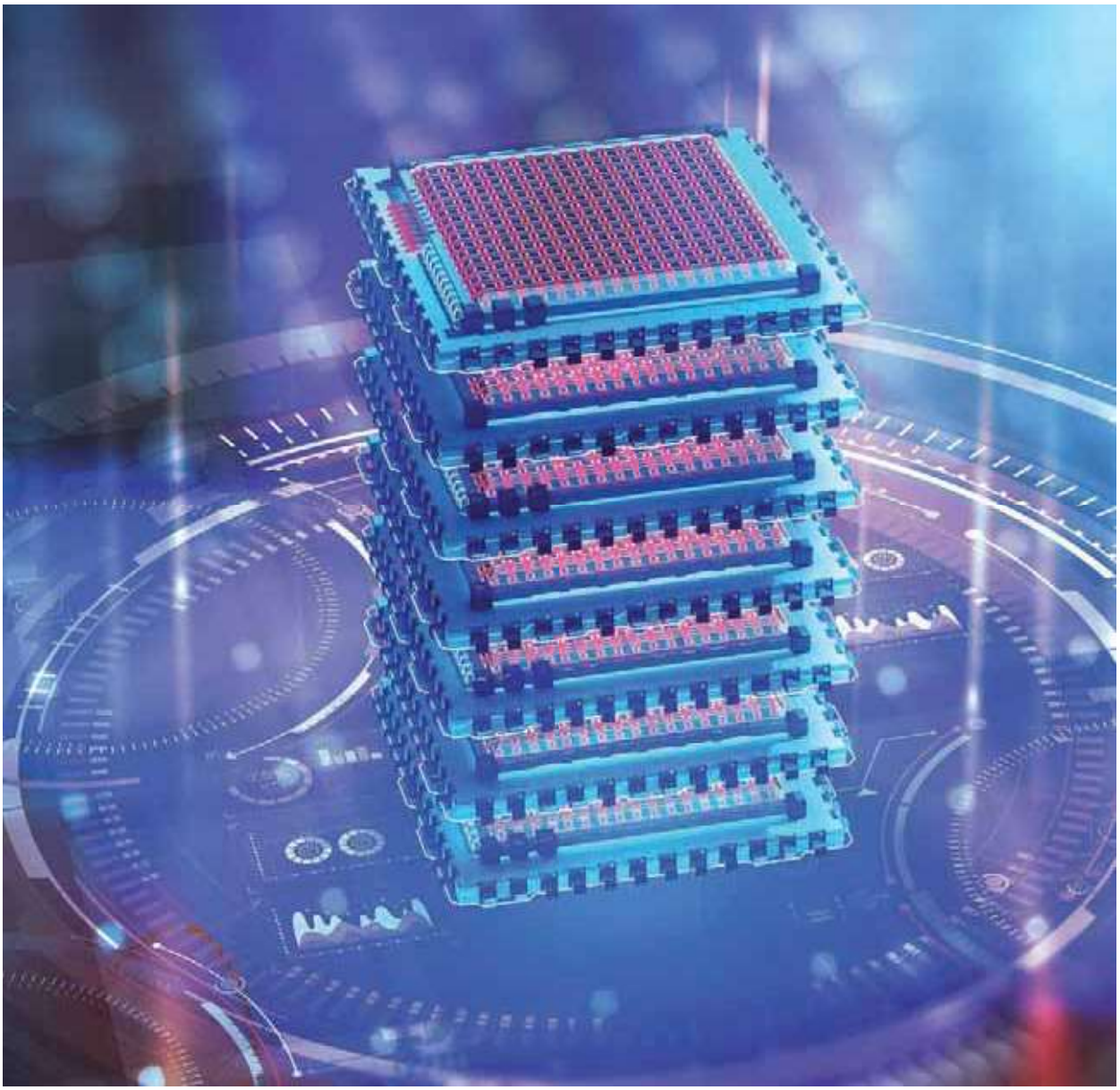
Resistenza dei crittosistemi agli attacchi quantistici

È quanto più evidente, quindi, che l'era *post-quantum* costituisca un cambiamento di paradigma che cambierà presto le nostre opinioni sulla sicurezza dei dati. Se vorremo mantenerne la segretezza nei prossimi decenni, cosa dovremmo fare oggi?
Fortunatamente non tutti i crittosistemi odierni sono destinati a cedere dinanzi ad un attacco quantistico. Infatti, l'algoritmo di Shor (e algoritmi simili) si dimostra efficace solo per crittosistemi basati sulla fattorizzazione di interi, tuttavia sono disponibili altri crittosistemi che si basano su basi matematiche differenti e maggiormente "sicure". Ad esempio, l'algoritmo simmetrico AES utilizza una rete di permutazioni di sostituzione per la codifica e decodifica dei dati, la cui sicurezza è leggermente indebolita dagli attacchi quantici. Per compensare questo indebolimento, è necessario semplicemente raddoppiare la lunghezza della chiave, senza modificare l'algoritmo. Ciò crea un codice sicuro e resistente all'attacco quantistico. Quindi, la selezione di un algoritmo *quantum resistant* come l'AES-256, configurato con accuratezza e attentamente integrato, si tradurrà in un sistema crittografico che sarà sicuro oggi e nei decenni.
Inoltre sono in fase di sviluppo nuovi crittosistemi resistenti agli algoritmi di crittoanalisi quantistica. Sono stati proposti diversi approcci e alcuni stanno ricevendo supporto istituzionale. Al riguardo, il NIST stima che i computer quantistici saranno in grado di decifrare l'infrastruttura a chiave pubblica esistente entro il 2029. Se questi nuovi crittosistemi post-quantistici saranno disponibili, prima che avvenga l'avvento di computer quantistici sufficientemente potenti, resta da vedere (*Fig. 5*).

Figura 5:
Ricerca e sviluppo in IBM e Google.
Google è in competizione con rivali quali IBM per dimostrare come un computer quantistico possa superare le capacità dei computer moderni. Si ritiene che, per raggiungere questo obiettivo, siano necessari circa 50 qubit e Google spera di ottenerlo quest'anno. Tuttavia, le simulazioni quantistiche nei computer comuni mostrano come siano necessari invece più di 50 qubit.

IBM Q Experience è un'iniziativa per consentire l'esperienza di programmare un *computer* quantistico. Sul sito *https://www.research.ibm.com/ibm-q/* è possibile creare programmi quantistici e farli eseguire su di un processore quantistico a 5 *qubit*.

Google ha presentato un nuovo processore quantistico da 72 *qubit* chiamato *Bristlecone*, il più grande mai costruito. L'occasione è stato il meeting dell'*American Physical Society* di *Los Angeles*.



Conclusioni

Proteggere i dati ora, nella prospettiva di un futuro post-quantistico, non è un compito semplice ed implica decisioni già in fase di progettazione dei sistemi di sicurezza. Tuttavia, abbiamo dimostrato come sia possibile condurre delle previsioni attendibili su come alcuni degli attuali sistemi crittografici diventeranno progressivamente meno sicuri, mentre altri continueranno a proteggere la nostra *privacy* e la sicurezza delle comunicazioni anche in un mondo *post-quantum*.

Bibliografia

- Holden, "*Mathematics of secrets*", Princeton University Press 2017
- Languasco, Zaccagnini, "*Manuale di crittografia*", Hoepli 2015
- Katz, Lindell, "*Introduction to modern cryptography*", 2nd edition, CRC Press 2015
- Baldoni, Ciliberto, Piacentini Cattaneo, "*Aritmetica, crittografia e codici*", Springer 2006
- Koblitz, "*A course in number theory and cryptography*", 2nd edition, Springer-Verlag 1994
- Apostol, "*Introduction to analytic number theory*", Springer-Verlag 1976