Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale della difesa,
della protezione della popolazione e dello sport DDPS

**Ufficio federale della cibersicurezza UFCS**

16 maggio 2024

# Valutazione tecnologica

## Informatica quantistica e crittografia post-quantistica

## 1 Introduzione

[1]Da quando, nel 2019, la rivista scientifica *Nature* ha proclamato la supremazia quantistica, i media hanno iniziato ad occuparsi molto del tema nella sua declinazione di computer quantistici, dei pericoli e delle minacce che ne derivano per i processi crittografici attualmente utilizzati e della necessità di una crittografia sicura anche contro i computer quantistici. In alcuni casi, queste notizie hanno il potere di suscitare sentimenti di grande incertezza e timore circa l'inadeguatezza delle procedure crittografiche. In questo contesto, la presente guida si prefigge di illustrare brevemente le specificità di un computer quantistico, le relative ripercussioni sulla sicurezza di alcune procedure crittografiche, il significato del termine crittografia post-quantistica (PQC) nonché i potenziali margini di manovra a riguardo.

## 2 Computer quantistico

Mentre un computer convenzionale funziona sulla base delle leggi della fisica classica, un computer quantistico è fondato sulle leggi della meccanica quantistica ed elabora gli stati quantistici secondo i principi della meccanica quantistica, tra cui il principio di sovrapposizione o il principio di entanglement. Invece che su bit, questo computer opera su bit quantistici, noti anche come qubit (o, più raramente, qbit). Un qubit rappresenta il più semplice sistema quantistico non banale, che può assumere in linea di principio un numero infinito di stati diversi e pertanto può anche trovarsi in questi stati simultaneamente (fenomeno del «parallelismo quantistico»). Ne derivano nuove possibilità e approcci alla calcolabilità.

Grazie alla sua struttura complessa e alle sue proprietà caratteristiche, un computer quantistico è adatto soprattutto a risolvere operazioni che non possono essere espletate con i computer tradizionali o che sono troppo complessi, come ad esempio operazioni di

[1] https://www.nature.com/articles/s41586-019-1666-5

simulazione nel campo delle scienze naturali e ingegneristiche, di ottimizzazione nella logistica e nella finanza, di apprendimento automatico nel contesto dell'intelligenza artificiale, nonché la risoluzione di problemi matematici su cui si basa la sicurezza di alcune procedure crittografiche. Sebbene i computer quantistici universalmente applicabili siano ancora prevalentemente un costrutto teorico, si sta lavorando alacremente alla loro realizzazione. Il lavoro di ricerca e sviluppo non si svolge solo nelle grandi aziende tecnologiche come IBM, Google, Microsoft e Intel, ma anche nelle università, nei cosiddetti spin-off e in altre aziende di nuova costituzione. [2] Sebbene il numero di qubit che possono essere installati oggi sia ancora nell'ordine di qualche centinaio (ad esempio 433 nel caso del processore quantistico Osprey presentato da IBM nel 2022), la stessa IBM sta progettando di costruire un computer quantistico con 100 000 qubit entro il 2033. Se questo ambizioso obiettivo dovesse essere raggiunto, ci troveremmo nell'ambito del cosiddetto computer quantistico crittograficamente rilevante (CRQC). Non è ancora chiaro quanto debba essere grande un computer quantistico per essere considerato un CRQC. Il motivo di questa incertezza è che molti algoritmi quantistici utilizzano qubit a tolleranza di errore, noti anche come qubit logici. Poiché i qubit fisici attualmente utilizzati sono particolarmente soggetti a errori, un approccio alla loro correzione consiste nel combinare diversi qubit fisici in un qubit logico. Questo processo è chiamato correzione degli errori e ha conosciuto un costante miglioramento negli ultimi tempi. Un altro approccio tenta di realizzare qubit tolleranti agli errori direttamente con metodi ottici quantistici.

In ogni caso, lo sviluppo e la costruzione di un CRQC avranno una portata maggiore della supremazia quantistica proclamata nel 2019. In definitiva, il termine supremazia quantistica significa semplicemente che un computer quantistico può risolvere un problema matematico più velocemente di un supercomputer che opera in modo convenzionale. Naturalmente, il significato di questa affermazione dipende fortemente dal problema di fondo e pertanto non è universalmente valido. Analoga cautela deve essere prestata agli annunci comunicati dall'azienda D-Wave Systems[3]. Sebbene i computer commercializzati da questa azienda siano dotati di migliaia di qubit, non sono computer quantistici universalmente applicabili. [4]Piuttosto, i computer di D-Wave Systems possono essere utilizzati solo per alcuni compiti di ottimizzazione e non sembrano nemmeno essere più potenti dei computer tradizionali.

# 3 Presentazione del problema

Come suggerisce il nome, un CRQC può essere utilizzato per risolvere i problemi matematici che formano la base di sicurezza per alcune procedure crittografiche. In particolare, si tratta di crittosistemi asimmetrici basati sul problema della fattorizzazione dei grandi numeri, come l'algoritmo RSA, o sul problema del logaritmo discreto, come il metodo di scambio di chiavi Diffie-Hellman, DSA e i crittosistemi basati sulle curve ellittiche. Già nel 1994, Peter W. Shor ha dimostrato come un computer quantistico o CRQC sufficientemente potente possa essere utilizzato per risolvere questi problemi matematici e quindi compromettere i crittosistemi basati su questi problemi [1]. A differenza dei computer convenzionali, gli algoritmi di Shor operanti su un computer quantistico hanno solo un tempo di esecuzione polinomiale e sono quindi efficienti in termini di teoria della complessità.

Poiché i sistemi crittografici asimmetrici interessati dagli algoritmi di Shor sono oggi in uso quasi ovunque, la costruzione di un CRQC avrebbe un grave impatto sulla loro sicurezza.

---

[2] https://www.ibm.com/quantum/blog/100k-qubit-supercomputer

[3] https://www.dwavesys.com

[4] https://dl.acm.org/doi/10.1145/3459606

In questo contesto viene talvolta utilizzato il termine «Q-Day», ovvero il momento in cui i CRQC verranno effettivamente realizzati e diventeranno quindi possibili vettori di attacchi.

Per risolvere i problemi di rilevanza crittografica, gli algoritmi quantistici richiedono almeno un numero di qubit logici che cresce linearmente con la lunghezza dei bit delle chiavi corrispondenti. Nel caso di algoritmi RSA, si tratta in genere di alcune migliaia. Grazie ai metodi di correzione degli errori oggi disponibili, il numero di qubit fisici necessari è un multiplo di tale cifra. Tuttavia, se IBM riuscisse a realizzare la sua visione, il computer quantistico previsto per il 2033 (con i suoi 100 000 qubit) rappresenterà un problema per molti crittosistemi asimmetrici.

Sebbene in linea di principio un computer quantistico possa essere utilizzato anche per violare la crittografia simmetrica, gli effetti sulla sicurezza delle procedure corrispondenti sono meno gravi. Nel 1996, Lov K. Grover ha proposto un algoritmo con il quale lo sforzo di una ricerca completa di una chiave lunga n bit può essere ridotto da $2^{2n}$ a $2^{n/2}$. Sebbene ciò significhi che anche i generatori pseudocasuali, i codici di autenticazione dei messaggi e la crittografia simmetrica sono vulnerabili in linea di principio, questa vulnerabilità può essere compensata con relativa facilità raddoppiando la lunghezza della chiave. La sicurezza della crittografia simmetrica è quindi solo marginalmente influenzata dall'esistenza di un CRQC. Inoltre, l'algoritmo di Grover è ottimale, quindi non è soggetto a ulteriore miglioramento.

Anche se un CRQC non può essere costruito oggi, il problema è che la raccolta di dati criptati su larga scala può avvenire già nel presente al fine di decifrarli con un CRQC una volta che sarà disponibile in futuro. La possibile esistenza di attacchi HNDL («Harvest Now, Decrypt Later») è il motivo principale nella prospettiva odierna per cui è necessario trovare al più presto approcci praticabili e soluzioni idonee.

# 4 Possibili soluzioni

Alla luce delle importanti attività di ricerca e sviluppo con cui le aziende tecnologiche citate stanno portando avanti la costruzione di computer quantistici universali, nonché della possibilità di attacchi HNDL, è opportuno riflettere su come costruire crittosistemi resistenti ai computer quantistici. Questa sottoarea della crittografia è nota come PQK e sta guadagnando un crescente interesse. PQK si riferisce alla crittografia asimmetrica. [5] La crittografia simmetrica non necessita praticamente interventi perché, come già detto, tutti i sistemi di crittografia in uso oggi possono continuare a essere utilizzati se la lunghezza della chiave viene raddoppiata. Questo raddoppiamento compensa le implicazioni dell'algoritmo di Grover, vale a dire che la sicurezza risultante rimane più o meno la stessa. In concreto, ciò significa per esempio passare a utilizzare una chiave AES-256 invece di AES-128. Gli svantaggi nell'uso pratico, semmai esistenti, sono molto modesti (in particolare, il rendimento durante la crittografia e la decrittografia non dipende in modo significativo dalla lunghezza della chiave).

L'obiettivo del PQK è quindi quello di costruire metodi e crittosistemi asimmetrici che si basano su problemi matematici riconosciuti come difficili, praticamente irrisolvibili anche con i computer quantistici, ma che possono essere implementati in modo efficiente. [6]Il National Institute of Standards and Technology (NIST) statunitense organizza dal 2017 un concorso di portata internazionale e ha annunciato i primi quattro vincitori per la crittografia

[5] Naturalmente, questo raddoppiamento è utile e necessario solo fino a una certa lunghezza della chiave. A partire da 256 bit, tale raddoppiamento risulta comunque non necessario.

[6] https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

asimmetrica e il trasporto delle chiavi (KEM[7]) nonché per le firme digitali nel 2022. Gli standard basati su questi algoritmi sono attualmente in fase di sviluppo e di finalizzazione da parte del NIST. Si tratta di FIPS 203 per ML-KEM e FIPS 204 per ML-DSA. Le basi sono gli algoritmi a griglia CRYSTALS-Kyber e CRYSTALS-Dilithium. L'algoritmo SPHINCS+, basato su funzioni di hash, costituisce la base del FIPS 205 SLH-DSA. L'algoritmo di firma FALCON, anch'esso basato su griglie, sarà standardizzato in un secondo momento. Per i KEM, il concorso sta entrando in una nuova fase con diversi algoritmi basati su codici. Infine, il NIST ha lanciato un secondo concorso per le firme digitali nel 2023. Al momento non è quindi chiaro se e quando altri processi entreranno in gioco come possibili standard. Oltre al NIST, anche altre organizzazioni come l'Internet Engineering Task Force (IETF), l'European Telecommunications Standards Institute (ETSI) e l'International Organization for Standardisation (ISO) stanno lavorando alla standardizzazione degli algoritmi PQK.

Dal punto di vista odierno, sarebbe sbagliato sostituire tutti i metodi asimmetrici attualmente utilizzati con metodi PQK, perché solo il futuro mostrerà quanto siano realmente sicuri (molti metodi e algoritmi PQK si basano su idee crittografiche ancora relativamente nuove e non ancora pienamente comprese). Invece, integrare e complementare queste procedure rappresenta un approccio ragionevole e conveniente. In questo contesto si parla anche di processi «ibridi» o di cosiddetti «combinatori ibridi». Ad esempio, i servizi di messaggeria con crittografia end-to-end Signal e iMessage combinano il metodo convenzionale di scambio di chiavi Diffie-Hellman basato su curve ellittiche con Kyber, e in futuro si prevedono approcci ibridi anche nel settore delle firme digitali e dei relativi certificati.

La crittografia quantistica (o l'accordo a chiave quantistica, che è la principale e di fatto unica applicazione della crittografia quantistica) e i generatori casuali quantistici non sono esplicitamente soluzioni possibili per i problemi discussi in questa breve guida. Entrambe le tecnologie sono tematicamente correlate e possono essere utilizzate anche nel contesto di prodotti commerciali. [8][9] Tuttavia, la crittografia quantistica è irta di problemi pratici, tanto che né la National Security Agency (NSA) statunitense né un consorzio di quattro autorità europee ne promuovono l'uso. Poiché i generatori casuali quantistici sono inoltre solo una delle tante opzioni tecniche di implementazione dei generatori casuali, non esiste quasi nessun valore aggiunto derivante dal loro uso ipoteticamente obbligatorio.

# 5 Raccomandazioni e ulteriori passi

La costruzione di un CRQC rappresenta una grande sfida dal punto di vista tecnico e non è quindi imminente. Tuttavia, la possibilità di attacchi HNDL ad ampio raggio rende l'uso di PQK una scelta ovvia. [10] In questo caso è opportuno un approccio cauto e ponderato. La rapida diffusione di soluzioni o approcci a breve termine e possibilmente affrettati avrebbe un impatto piuttosto negativo sulla sicurezza, anche se ciò potrebbe in prima analisi

---

[7] L'abbreviazione KEM sta per «Key Encapsulation Mechanism». Si riferisce a un meccanismo che consente di inviare in modo sicuro una chiave crittografica a un destinatario. La chiave da trasportare viene scelta a caso e impacchettata (o «incapsulata») con la chiave pubblica del destinatario affinché possa essere nuovamente spacchettata solo con la corrispondente chiave privata. Sarebbe necessario un metodo di scambio di chiavi simile a Diffie-Hellman (anch'esso non interattivo), ma tale metodo non è ancora disponibile. I KEM sono quindi utilizzati come sostituti.

[8] https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

[9] https://cyber.gouv.fr/en/actualites/uses-and-limits-quantum-key-distribution

[10] Adi Shamir ha dato un consiglio che descrive perfettamente la situazione alla RSA Conference 2023, nell'ambito di un panel su «Migrating to Post-Quantum Schemes»: «If you want to switch to post-quantum algorithms, walk, don't run» (https://www.rsaconference.com/library/presentation/usa/2023/Panel%20Migrating%20to%20Post-Quantum%20Schemes).

garantire una resistenza agli attacchi provenienti dai computer quantistici. La conseguente migrazione è un processo lungo, che deve essere pianificato di conseguenza sullo sfondo dell'attuale standardizzazione degli algoritmi PQK.[11]

Si sta lavorando su vari fronti per standardizzare gli algoritmi PQK e per incorporarli nei protocolli e nei prodotti di sicurezza. Tra questi sono già stati citati Signal e iMessage. [12] Anche Google ha cercato di incorporare Frodo (un algoritmo predecessore di Kyber) in TLS a metà degli anni 2010 e da allora sta lavorando a varie estensioni PQK per i suoi prodotti. Lo stesso vale per Microsoft, Cloudflare e altre aziende tecnologiche. In linea di principio, più un sistema è aperto, più risulta difficile e oneroso in termini di tempo integrarlo con il PQK. In questo senso, l'uso del PQK nei protocolli di sicurezza standardizzati per Internet (ad esempio IPsec, TLS, ...) rappresenta una sfida importante per l'IETF e i suoi gruppi di lavoro.

Tutti gli sforzi a favore del PQK servono in ultima analisi all'agilità crittografica e devono essere considerati in questo contesto. I sistemi e le applicazioni devono essere progettati e implementati in modo da poter utilizzare e supportare diverse procedure e algoritmi crittografici. Questa forma di agilità è già importante oggi e probabilmente lo diventerà ancora di più in futuro. L'agilità crittografica richiede un'architettura software progettata a tal fine. Con le implementazioni hardware, che sono tipicamente utilizzate per aumentare le prestazioni e/o i requisiti di sicurezza, le opzioni di agilità sono generalmente limitate. È sempre opportuno documentare i componenti, i processi e gli algoritmi crittografici utilizzati in un software (SBOM) o in una Cryptography Bill of Materials (CBOM). Questo tipo di inventariazione è importante indipendentemente dal tema del PQK, in un contesto di crescenti attacchi alla «supply chain».

# Abbreviazioni

| | |
|---|---|
| AES | Advanced Encryption Standard |
| UFCS | Ufficio federale della cibersicurezza |
| CBOM | Cryptography Bill of Materials |
| CRQC | Cryptographically Relevant Quantum Computer |
| DSA | Digital Signature Algorithm |
| ETSI | European Telecommunications Standards Institute |
| FIDO2 | Fast IDentity Online |
| FIPS | Federal Information Processing Standards (US) |
| HNDL | Harvest Now, Decrypt Later |
| IETF | Internet Engineering Task Force |
| IPsec | Internet Protocol Security |
| ISO | International Organization for Standardization |
| KEM | Key Encapsulation Mechanism |
| ML | Module Lattice |
| NIST | National Institute of Standards and Technology |
| NSA | National Security Agency |
| PQK | Post-Quanten-Kryptografie |
| RSA | Rivest, Shamir, Adleman |
| SBOM | Software Bill of Materials |
| SLH | Stateless Hash |
| TLS | Transport Layer Security |

[11] https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography

[12] https://bughunters.google.com/blog/5108747984306176/google-s-threat-model-for-post-quantum-cryptography

DDPS Dipartimento federale della difesa, della protezione della popolazione e dello sport

# Fonti bibliografiche

[1] Peter W. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, In: Proceedings of the 35th Annual Symposium on Foundations of Computer Science, November 1994, Santa Fe, NM, pp. 124–134

[2] Lov K. Grover, *A Fast Quantum Mechanical Algorithm for Database Search*, In: Proceedings of the 28th Annual ACM Symposium on the Theory of Computing, May 1996, pp. 212–219