Elaboratori Quantistici e Crittografia Post-Quantum, oggi

Author : Andrea Pasquinucci

Date : 26 Febbraio 2020

Quando si pianificano o si valutano i sistemi di sicurezza IT, è importante considerare non solo le minacce e le vulnerabilità odierne, ma anche possibili scenari futuri. Un campo abbastanza interessante che molto probabilmente influenzerà il panorama futuro della sicurezza IT è la **teoria dell'Informazione Quantistica**. La teoria dell'Informazione Quantistica può essere brevemente descritta come la disciplina che studia come le informazioni possono essere codificate in particelle elementari e cosa si può fare quando le informazioni vengono codificate in questo modo. La teoria dell'Informazione Quantistica oggi è per lo più ancora una branca della pura ricerca nella fisica fondamentale, ma ci sono alcune **sorprendenti applicazioni pratiche**.

Sin dalla fine degli anni '60, i fisici hanno studiato come usare le particelle elementari direttamente per applicazioni informatiche, partendo da come codificare bit di informazione nelle particelle elementari. L'interesse principale nasce dal fatto che le particelle elementari seguono le leggi dettate dalla teoria della Meccanica Quantistica e il loro comportamento sotto molti aspetti è molto diverso da quello di qualsiasi oggetto che affrontiamo quotidianamente. Ci sono profonde differenze tra le leggi classiche della fisica che tutti conosciamo bene, quali la dinamica di Newton, l'elettromagnetismo di Maxwell e persino la relatività di Einstein, e la fisica Quantistica. Ad esempio, di solito non è possibile misurare una particella elementare senza modificarla, il che implica anche che è impossibile farne copie esatte. Ciò è abbastanza diverso dalla nostra esperienza quotidiana con oggetti macroscopici, che possiamo misurare senza modificare e di cui possiamo fare copie identiche. È possibile sfruttare questa differenza intrinseca tra le particelle elementari ed il mondo macroscopico per fare qualcosa di veramente nuovo anche nel campo dell'informatica.

Gli elaboratori quantistici

Lo studio della teoria dell'Informazione Quantistica per lo sviluppo di elaboratori quantistici cominciò negli anni '70 (Rif. 1). In particolare all'inizio degli anni '80 un contributo importante fu dato dai fisici Manin, Benioff e Feynman che proposero l'idea che un elaboratore quantistico potesse eseguire simulazioni non possibili per i normali elaboratori classici (Rif. 2). La speranza

iniziale dei ricercatori era che un elaboratore quantistico potesse facilmente svolgere calcoli (simulazioni) di sistemi elementari complessi, quali atomi e molecole, poiché non avrebbe dovuto risolvere numericamente le equazioni della Meccanica Quantistica in quanto queste sarebbero state intrinsecamente codificate nell'elaboratore stesso. In linea di principio gli elaboratori quantistici potrebbero contribuire in maniera ancor oggi impensabile alla chimica elementare, alla farmaceutica, alla creazione di nuovi materiali ecc.

I computer quantistici si basano sull'idea di codificare il valore di un bit in una proprietà di una particella elementare. Come esempio banale e non realistico, potremmo supporre che se una particella gira in senso orario, il valore del bit è 1 e se gira in senso antiorario il valore è 0 (in realtà il valore 0 o 1 è assegnato ad una caratteristica quantistica della particella). Pertanto, invece di avere correnti e tensioni elettriche a codificare il valore del bit all'interno delle CPU, abbiamo particelle elementari, ognuna con il valore di un bit. Un bit codificato in una particella elementare viene chiamato “bit quantico”, in breve **qubit**, e le operazioni in queste CPU quantistiche vengono eseguite trasformando lo stato delle particelle elementari.[1]

Per eseguire un calcolo con un elaboratore quantistico bisogna per prima cosa preparare le particelle elementari nello stato iniziale in modo che rappresentino i numeri di partenza. Poi bisogna eseguire delle trasformazioni fisiche sulle particelle, ad esempio tramite campi magnetici o l'interazione con altre particelle, che realizzano il calcolo stesso. Infine bisogna effettuare una misura dello stato fisico finale delle particelle per ottenere il risultato numerico del calcolo. In analogia alla struttura degli elaboratori Classici, per eseguire i calcoli negli elaboratori Quantistici sono state definite teoricamente delle “porte quantistiche” (Quantum Gates) che permettono di realizzare qualunque calcolo possibile su di un elaboratore quantistico.

La definizione di (Universal) Quantum Gates permette più facilmente di scrivere programmi ed algoritmi per elaboratori quantistici, e la creazione di ambienti di simulazione ove poter verificare la correttezza dei programmi e degli algoritmi.

Algoritmi quantistici e sicurezza informatica

Gli elaboratori quantistici sono balzati all'attenzione in particolare di chi si occupa di sicurezza informatica alla metà degli anni '90 quando Peter Shor (nel 1994) e Lov Grover (nel 1996) proposero due importanti algoritmi quantistici: il primo permette la fattorizzazione di un numero intero in tempi polinomiali, il secondo velocizza la ricerca di un valore (*“database search”*) o l'inversione numerica di una funzione. L'algoritmo di Shor è sicuramente quello più famoso in quanto permette di risolvere facilmente il problema matematico alla base di molti algoritmi di crittografia asimmetrica, o a chiave pubblica-privata, quale l'algoritmo RSA. In pratica l'avvento di elaboratori quantistici in grado di eseguire l'algoritmo di Shor renderebbe del tutto insicuro l'utilizzo di algoritmi asimmetrici quali RSA, ECC, DH [2] ecc., ovvero tutti gli algoritmi crittografici basati sui problemi matematici di fattorizzazione degli interi, dei logaritmi discreti e dei logaritmi discreti su curve ellittiche. Per l'utilizzatore verrebbe a mancare la sicurezza fornita dalla crittografia ai certificati digitali, alle firme digitali, alla cifratura con algoritmi asimmetrici, alla navigazione in Internet, in pratica alla grande maggioranza degli utilizzi quotidiani della crittografia.

L'implementazione dell'algoritmo di Grover avrebbe delle conseguenze meno catastrofiche, in quanto permette di “raddoppiare” la velocità di enumerazione delle possibili chiavi segrete di un algoritmo simmetrico quale AES. Quindi per mantenere lo stesso livello di sicurezza basterebbe utilizzare chiavi lunghe il doppio. In pratica per proteggerci oggi dall'algoritmo di Grover, invece di utilizzare AES con chiavi di 128 bit dovremmo adottare chiavi di 256 bit.

Dal punto di vista della sicurezza informatica, un aspetto molto importante è individuare quando sarà necessario sostituire gli algoritmi impattati dall'algoritmo di Shor e quando sostituire con chiavi più lunghe quelli impattati dall'algoritmo di Grover. Il primo aspetto da considerare è quando saranno realmente disponibili elaboratori quantistici in grado di eseguire questi algoritmi, esamineremo questo punto nella prossima sezione. E' fondamentale però anche valutare quanto *prima* di questo momento debbano essere implementate le contromisure (Rif. 4).

Consideriamo **due esempi:** nel primo si supponga che delle informazioni estremamente riservate siano state trasmesse a gennaio 2020 cifrate in Internet e che un attaccante abbia registrato tutto il traffico in rete. Queste informazioni devono rimanere riservate almeno per 10 anni, quindi la cifratura deve garantire la sicurezza della confidenzialità almeno sino a dicembre 2029. Se l'avvento degli elaboratori quantistici fosse prima del 2030, allora in questo scenario *già a gennaio 2020* è necessario cifrare le comunicazioni con algoritmi resistenti all'algoritmo di Shor.

Il secondo esempio riguarda la progettazione di un apparato, come ad esempio un aereo, un'automobile, un microprocessore integrato come quelli per le carte di credito o le SIM, o anche un elaboratore specializzato, che implementi in maniera *embedded* algoritmi crittografici. Nel momento in cui si sceglie quale algoritmo crittografico implementare, bisogna valutare la vita utile dell'apparato e la possibilità dell'avvento degli elaboratori quantistici entro il periodo di tale vita utile. E' da notare che apparati complessi come un aereo possono avere periodi di vita utile di 30 o più anni.

Quali elaboratori quantistici oggi? E domani?

Sin dai primi anni 2000 l'interesse agli elaboratori quantistici si è in parte spostato dall'accademia alle aziende, sia per la speranza di fare un investimento economicamente vantaggioso, sia per la necessità di grandi finanziamenti disponibili solo a grandi aziende. Ad oggi i principali laboratori nei quali sono sviluppati gli elaboratori quantistici sono quelli di Google, Microsoft, Intel, IBM ecc. Se da un lato le grandi aziende hanno le risorse principalmente economiche per procedere con la ricerca e lo sviluppo delle tecnologie necessarie per costruire un elaboratore quantistico, d'altra parte per ovvie necessità di business, le informazioni sull'andamento degli sviluppi sono meno dettagliate. È comunque possibile fare un punto approssimativo partendo dalla *road-map* stabilita da un gruppo di esperti convocati dalla ARDA (*Advanced Research and Development Activity*, un'agenzia di finanziamento della comunità di intelligence degli Stati Uniti) agli inizi degli anni 2000 (Rif. 5). Secondo questa road-map entro il 2012 sarebbe stato costruito un elaboratore quantistico con circa 50 qubit che avrebbe permesso di eseguire una semplice istanza di un algoritmo quantistico rilevante. Sino a settembre 2019 non era stata fornita alcuna evidenza definitiva che

questo traguardo fosse stato raggiunto, anche se ad esempio Intel stava lavorando ad un elaboratore quantistico con 49 qubit, IBM con 53 e Google con 54 e 72 (si veda anche Rif. 7).

Ad ottobre 2019 Google ha annunciato (Rif. 6) di aver raggiunto la “Quantum Supremacy” ovvero di essere stato in grado di eseguire un calcolo sul proprio elaboratore quantistico a 54 qubit in 200 secondi con un algoritmo quantistico mentre il corrispondente algoritmo classico avrebbe impiegato probabilmente almeno 10.000 anni sugli elaboratori Classici più potenti oggi esistenti. Simili risultati sono stati annunciati anche da IBM. Possiamo dire quindi che con 7 anni di ritardo è stato raggiunto il traguardo della *road-map*.

Uno tra i principali motivi della difficoltà nella costruzione degli elaboratori quantistici risiede nei fenomeni usualmente denominati con il termine di “Decoerenza”. L'idea di base è abbastanza semplice: come già descritto, gli elementi costitutivi di un elaboratore quantistico sono delle particelle elementari che al contempo

1. non devono interagire con qualunque altra particella o campo che potrebbe modificare il loro stato e quindi introdurre errori (in pratica cambiare il valore dei qubit);
2. devono interagire unicamente con le particelle e i campi necessari ad eseguire l'algoritmo e solo nel momento di esecuzione.

Per oggetti macroscopici, le leggi della meccanica classica garantiscono che è possibile separare e tenere separati due oggetti, mentre le leggi della meccanica quantistica garantiscono solo che si possono preparare particelle elementari, ad esempio a temperature prossime allo zero assoluto, in modo che la probabilità di interazioni sia molto bassa, ma non nulla. Perciò in un elaboratore quantistico è necessario implementare degli appositi algoritmi quantistici di correzione degli errori, che però a loro volta richiedono l'introduzione di ulteriori qubit per essere eseguiti.

Quanti qubit sono necessari per eseguire su dati reali l'algoritmo di Shor[3] e altri algoritmi quantistici rilevanti? Non vi è una risposta precisa anche perché molto dipende dalla tecnologia adottata, dagli algoritmi di correzione degli errori ecc. Le stime più ottimiste indicano alcune decine di migliaia di qubit, ma i più ritengono che saranno necessari decine di milioni - se non miliardi - di qubit fisici, ovvero particelle elementari (Rif. 8).

Sarà possibile costruire un vero elaboratore quantistico di queste dimensioni? E nel caso, quando?

Le opinioni sono molto diverse: ad esempio M. Mosca, in Rif. 4, stima una possibilità del 50% che per il 2031 sia costruito e funzionante un elaboratore quantistico in grado di decifrare RSA (facendo anche ricorso a una possibile “legge di Moore” per gli elaboratori quantistici) mentre M. Dyakonov, in Rif. 8, ritiene che non sarà mai possibile far funzionare un tale elaboratore quantistico.

Crittografia post-quantum

Per i nostri scopi, possiamo dividere gli algoritmi crittografici in due grandi classi: quelli che sono

rotti dall'algoritmo di Shor e quelli che non lo sono. La principale caratteristica degli algoritmi crittografici a rischio è quella di basare la propria sicurezza su alcuni problemi matematici di difficile soluzione. Più precisamente, sono problemi matematici facili da risolvere quando alcune particolari informazioni sono note, ma difficili o in pratica impossibili da risolvere se i numeri sono grandi e se alcune particolari informazioni non sono note. Solo per dare un'idea, è possibile fare l'esempio del prodotto di due numeri primi, a cui abbiamo già accennato: se dato 15 è facile identificare 3 e 5 come i suoi fattori primi, la matematica ci insegna che dato un numero prodotto di due numeri primi di centinaia o migliaia di cifre, anche con i più potenti elaboratori Classici esistenti sono necessari almeno migliaia di anni per calcolare i due numeri primi fattore.

In generale, un algoritmo crittografico è ritenuto sicuro quando l'attacco più efficace ed efficiente è quello di provare tutte le chiavi segrete possibili. Quindi per utilizzare l'algoritmo in maniera sicura è sufficiente scegliere chiavi segrete lunghe a sufficienza (e pseudo-casuali, cioè impossibili da indovinare). In questo caso, l'avvento degli elaboratori quantistici richiede solo il raddoppio della lunghezza delle chiavi per rimanere in sicurezza rispetto all'algoritmo di Grover.

Molti algoritmi crittografici, quali quelli simmetrici come AES o di impronta come SHA256, sono basati su trasformazioni ripetute dei dati quali sostituzioni, permutazioni ed XOR. Questi algoritmi sono soggetti solo all'algoritmo di Grover. Al contrario, la quasi totalità degli algoritmi in uso a chiave pubblica-privata ed utilizzati quotidianamente per la navigazione web, le firme digitali ecc., sono basati su problemi matematici complessi ad “una via”, ovvero impossibili in pratica da invertire, e questi sono soggetti all'algoritmo di Shor che li rende del tutto insicuri.

È chiara quindi la necessità di sviluppare **nuovi algoritmi**, in particolare a chiave pubblica-privata, per sostituire quelli soggetti all'attacco di Shor. Sull'effettivo rischio di sicurezza, i crittografi non sono unanimi nel considerare realistico l'avvento degli elaboratori quantistici all'inizio degli anni 2030. Alcuni, seguendo ad esempio l'analisi di M. Dyakonov, ritengono più opportuno indirizzare gli sforzi della ricerca nel miglioramento degli algoritmi attuali quali RSA, ECC, DH ecc. piuttosto che dedicarsi allo sviluppo di nuovi algoritmi crittografici.

Altri invece ritengono assolutamente necessario sviluppare algoritmi che non siano soggetti all'attacco di Shor. Questa direzione di ricerca è chiamata **Crittografia “Post-Quantum”**, cioè che ha lo scopo di identificare e creare algoritmi crittografici che rimarranno sicuri *dopo* l'avvento degli elaboratori quantistici.

Si può far risalire l'avvio della ricerca di questi nuovi algoritmi al 2006 quando si svolse la prima conferenza PQCrypto presso la Katholieke Universiteit di Leuven in Belgio (Rif. 9). L'interesse e la necessità di sviluppare questi nuovi algoritmi è stata supportata ad esempio anche dall'Unione Europea che negli anni 2015-2018 ha fornito 3,9 M€ per il progetto PQCRYPTO (Rif. 10). Il NIST nel 2016 ha avviato un processo di selezione di nuovi algoritmi post-quantum (Rif. 11) con l'obiettivo di sostituire in pratica entro il 2030 gli algoritmi suscettibili all'attacco di Shor. Al momento è in corso il secondo round di selezione degli algoritmi candidati, è poi previsto un terzo round a partire dal 2020/2021 e la standardizzazione degli algoritmi selezionati entro il 2024. In questo modo rimarrebbero almeno 5 anni per implementare i nuovi algoritmi in tutti i sistemi IT, sia hardware che software prima dell'avvento degli elaboratori quantistici. Alla

ricerca post-quantum partecipano non solo ricercatori universitari ma anche le principali aziende informatiche a livello mondiale, a partire da Microsoft, Google[4] ecc.

Ad oggi i ricercatori hanno proposto molti diversi algoritmi crittografici post-quantum con diversi approcci e basati su problemi matematici diversi. Una caratteristica abbastanza comune di questi algoritmi è la lunghezza delle chiavi e delle firme digitali, come si può evincere ad esempio da questa tabella (Rif. 12):

Algorithm	Type	Public Key	Private Key	Signature
NTRU Encrypt[36]	Lattice	6130 B	6743 B	
Streamlined NTRU Prime	Lattice	1232 B		
Rainbow[37]	Multivariate	124 KB	95 KB	
SPHINCS[19]	Hash Signature	1 KB	1 KB	41 KB
SPHINCS+[38]	Hash Signature	32 B	64 B	8 KB
BLISS-II	Lattice	7 KB	2 KB	5 KB
GLP-Variant GLYPH Signature[10][39]	Ring-LWE	2 KB	0.4 KB	1.8 KB
New Hope[40]	Ring-LWE	2 KB	2 KB	
Goppa-based McEliece[14]	Code-based	1 MB	11.5 KB	
Random Linear Code based encryption[41]	RLCE	115 KB	3 KB	
Quasi-cyclic MDPC-based McEliece[42]	Code-based	1232 B	2464 B	
SIDH[43]	Isogeny	751 B	48 B	
SIDH (compressed keys)[44]	Isogeny	564 B	48 B	
3072-bit Discrete Log	**not PQC**	384 B	32 B	96 B
256-bit Elliptic Curve	**not PQC**	32 B	32 B	65 B

In questa tabella sono raffigurate le lunghezze delle chiavi e delle firme digitali necessarie per ottenere una sicurezza equivalente a quella offerta oggi con chiavi simmetriche a 128 bit di alcuni algoritmi post-quantum. Per confronto le ultime due righe riportano gli stessi dati per due algoritmi attuali soggetti all'attacco di Shor. Come si vede, la maggior parte degli algoritmi utilizzano chiavi e producono firme digitali almeno mille volte più grandi degli attuali. Questo avrebbe almeno **due conseguenze:**

1. l'aumento di dati da trasferire e, quindi, del traffico in rete;
2. l'utilizzo di maggiori risorse dei computer, smartphone, IoC ecc., sia di memoria sia della CPU per l'esecuzione degli algoritmi.

Quello ancora da fare da parte dei ricercatori non è poco: oltre a creare algoritmi post-quantum

che permettano prestazioni compatibili con con i dispositivi su cui saranno utilizzati e sufficientemente simili alle prestazioni degli algoritmi in uso oggigiorno, devono verificare che questi nuovi algoritmi siano “sicuri” anche rispetto a tutti i requisiti della crittografia non quantistica. Dato che alcuni di questi algoritmi sono basati su problemi matematici alternativi a quelli utilizzati in crittografia sinora, sono necessari studi approfonditi per poter raggiungere una sufficiente certezza dell'assenza di debolezze che possano portare alla “rottura” dell'algoritmo. Sarebbe grave e probabilmente molto costoso, se dopo aver adottato ed implementato a livello mondiale un algoritmo post-quantum si scoprisse una sua falla rispetto ad attacchi effettuati con elaboratori Classici e si fosse obbligati a sostituirlo in tempi rapidi.

Un altra direzione della ricerca è quella dello sviluppo di nuovi algoritmi per elaboratori quantistici. Questo è un campo molto attivo in particolare per usi non di crittografia degli elaboratori quantistici. Sino ad ora non sono stati trovati altri algoritmi quantistici con conseguenze simili per la crittografia a quello di Shor. Visto che sono ormai passati 25 anni dalla pubblicazione dell'algoritmo di Shor e che la ricerca in questo campo è stata ed è attiva, si ritiene difficile che venga scoperto un altro algoritmo quantistico con simili conseguenze per la crittografia nel prossimo futuro.

Nella prima parte di questo articolo si era valutato come **requisiti di sicurezza** forniti dalla crittografia possano durare anche per 10 o più anni. Pertanto, nel caso dell'avvento di un elaboratore quantistico nel 2030, ove necessario dovremmo già oggi utilizzare algoritmi resistenti all'attacco di Shor. Questo però non è possibile, anzi il NIST prevede che i nuovi algoritmi post-quantum saranno disponibili non prima del 2024 e completamente implementati e distribuiti per il 2030. Nell'incertezza di se - e quando - arriveranno gli elaboratori quantistici, questo ci lascia con un rischio sicuramente difficile da valutare e rispetto al quale ad oggi abbiamo poche contromisure possibili da adottare.

Riferimenti bibliografici

Rif. 1: si veda ad esempio https://en.wikipedia.org/wiki/Timeline_of_quantum_computing per una *timeline* dell'evoluzione degli elaboratori quantistici.

Rif. 2: per la nascita della teoria degli elaboratori quantistici si fa spesso riferimento alla presentazione di Richard Feynman intitolata “Quantum mechanical Hamiltonian models of discrete processes that erase their own histories: application to Turing machines” presentata alla prima conferenza in “Physics of Computation”, maggio 1981, MIT (USA).

Rif. 3: M.A. Nielsen, I.L. Chuang “Quantum Computation and Quantum Information”, Cambridge University Press, 2010.

Rif. 4: M. Mosca “Cybersecurity in an era with quantum computers: will we be ready?”, https://eprint.iacr.org/2015/1075.pdf ; si veda anche https://post-quantum-cryptography.com/#tg.

Rif. 5: Report of the Quantum Information Science and Technology Experts Panel “A Quantum Information Science and Technology Roadmap”, 2/4/2004, https://qist.lanl.gov/pdfs/qc_roadmap.pdf.

Rif. 6: F. Arute et. al (Google AI Quantum), “Quantum supremacy using a programmable superconducting processor”, Nature 574, pag. 505 (2019), https://www.nature.com/articles/s41586-019-1666-5 ; “Google's Quantum Tech Milestone Excites Scientists and Spurs Rivals”, IEEE Spectrum, https://spectrum.ieee.org/tech-talk/computing/hardware/googles-quantum-tech-milestone-excites-scientists-and-spurs-rivals.

Rif. 7: “Qubit Count”, https://quantumcomputingreport.com/scorecards/qubit-count/.

Rif. 8: M. Dyakonov “The Case Against Quantum Computing”, https://spectrum.ieee.org/computing/hardware/the-case-against-quantum-computing.

Rif. 9: Per le conferenze e workshop PQCrypto si faccia riferimento a https://www.pqcrypto.org/conferences.html.

Rif. 10: https://ec.europa.eu/digital-single-market/en/news/pqcrypto-eu-funded-project-success-story , https://pqcrypto.eu.org/.

Rif. 11: Post-Quantum Cryptography, NIST Computer Security Resource Center, https://csrc.nist.gov/projects/post-quantum-cryptography.

Rif. 12: https://en.wikipedia.org/wiki/Post-quantum_cryptography.

Note

[1] Per maggiori dettagli sulla teoria dell'Informazione Quantistica, gli elaboratori e il calcolo quantistico si fa riferimento alla letteratura specialistica quale ad esempio Rif. 3.

[2] RSA è l'acronimo di R. Rivest, A. Shamir, L. Adleman, ECC di “elliptic-curve cryptography”, DH di W. Diffie, M. Hellman.

[3] Già nel 2001 un elaboratore quantistico a 7 qubit di IBM riuscì a fattorizzare 15 in 3 * 5. Nel 2012 fu fattorizzato 21 in 7 * 3.

[4] Solo a titolo di esempio, Google ha svolto alcuni test sul campo dell'algoritmo post-quantum “New Hope” inserendolo nel suo browser Chrome.

Articolo a cura di **Andrea Pasquinucci**