La Comunicazione - Note, Recensioni e Notizie n. 67
Anno 2023

La minaccia del quantum computing e la crittografia post-quantum: stato dell'arte e impatto su 5G

The threat of quantum computing and post-quantum cryptography: state of the art and impact on 5G

Marco Baldi♦

♦ Università Politecnica delle Marche

Sommario

L'uso della fisica quantistica per rappresentare l'informazione ci offre oggi molte nuove opportunità. Tra queste, però, c'è anche la possibilità che attaccanti dotati di strumenti quantistici possano sferrare attacchi dirompenti ai sistemi crittografici che oggi usiamo in modo pervasivo. Se da un lato i sistemi di comunicazione quantistica potrebbero rappresentare uno strumento di difesa da tali attacchi, dall'altro essi richiedono ingenti investimenti e rappresentano una soluzione soltanto parziale. La crittografia post-quantum invece non richiede dotazioni quantistiche da parte degli utenti legittimi, e offre uno strumento di difesa che può essere applicato anche a sistemi ed infrastrutture esistenti. Il presente articolo descrive tale scenario ed illustra i rischi e le necessarie contromisure che interessano le reti ed i sistemi 5G.

Abstract

The use of quantum physics to represent information nowadays offers us many new opportunities. Among them, however, is the possibility that attackers equipped with quantum devices could mount disruptive attacks on the cryptographic systems we use pervasively today. While quantum communication systems could provide a means of defense against such attacks, they require large investments and are only a partial solution. Post-quantum cryptography, instead, does not require quantum endowments for legitimate users, and offers a defense tool that can be applied also to existing systems and infrastructures.

This article describes such a scenario and illustrates the risks and necessary countermeasures concerning networks as well as 5G systems.

Keyword
Quantum information science, quantum computing, quantum key distribution, post-quantum cryptography, quantum-safe cryptography.

1 - Introduzione

Già teorizzati negli anni '80 e '90, oggi i sistemi quantistici che processano e trasmettono l'informazione stanno rapidamente diventando realtà. Da un lato i sistemi di comunicazione quantistica permettono di spingere ulteriormente avanti le capacità trasmissive dei canali di comunicazione, lasciando intuire scenari futuri in cui avremo a disposizione reti quantum ultraveloci. Dall'altro, la possibilità di usare la fisica quantistica per eseguire calcoli tramite un quantum computer permette di ideare algoritmi capaci di risolvere in poco tempo problemi di complessità insormontabile con un computer classico.

Queste nuove opportunità abilitano dirompenti scenari futuri dell'era dell'informazione, in cui però bisogna anche considerare la possibilità che tali tecnologie cadano in mani criminali, e siano sfruttate per eseguire attacchi cyber. Infatti, è stato dimostrato da tempo che un quantum computer di dimensioni sufficientemente grandi potrebbe compromettere la sicurezza di molti dei sistemi crittografici asimmetrici oggi più diffusi, minando la sicurezza dei nostri dati e delle nostre comunicazioni digitali quotidiane.

Da un lato, l'uso di comunicazioni quantistiche da parte di chi voglia difendersi da attaccanti dotati di quantum computer rappresenta una soluzione teorica, che è però affetta da limitazioni pratiche e non risolve interamente il problema. La crittografia post-quantum, invece, fornisce nuove primitive crittografiche che non necessitano di tecnologia quantistica, e possono quindi essere usate nei sistemi esistenti, fornendo protezione anche da attaccanti dotati di un computer quantistico.

Nel seguito viene illustrato lo stato dell'arte dei sistemi quantistici per l'elaborazione e la trasmissione di informazioni, descrivendo i rischi che derivano dal possibile uso di un computer quantistico per attaccare molti dei più diffusi sistemi crittografici. Viene quindi introdotta la crittografia post-quantum, descrivendone lo stato dell'arte, anche rispetto al recente processo di selezione e standardizzazione coordinato dal NIST. Infine, si analizza l'impatto di possibili attacchi quantum alle tecnologie di rete e 5G oggi più diffuse, illustrando le contromisure necessarie per ripristinare il loro livello di sicurezza.

2 - Quantum information science

Per meglio inquadrare l'influenza che il quantum computer sta già avendo ed avrà ancora di più in futuro sulla sicurezza dei nostri dati e delle nostre reti, è necessario definire chiaramente quali applicazioni la meccanica quantistica può avere nel mondo dell'ingegneria dell'informazione e più in dettaglio sui nostri sistemi ICT. Tale ambito scientifico è noto come **quantum information science**, ovvero la scienza dell'informazione quantistica. Ad oggi, tre sono le branche di tale scienza che hanno conosciuto maggiore sviluppo, ed iniziano ormai a trovare applicazione nei sistemi reali:

- Quantum computing
- Quantum communications
- Quantum cryptography

Esse hanno in comune il fatto di sfruttare una rappresentazione quantistica dell'informazione, seppure per scopi differenti.

Un **quantum computer** è un dispositivo capace di elaborare informazione rappresentata sotto forma di stati quantistici della materia sfruttando alcuni principi quantistici, come il principio di sovrapposizione e la correlazione quantistica (o entanglement quantistico), allo scopo di eseguire calcoli ed algoritmi per risolvere problemi computazionali.

Le **comunicazioni quantistiche** sfruttano i medesimi principi della fisica quantistica, ma non tanto per eseguire algoritmi, quanto per trasferire dati da un estremo all'altro di un canale di comunicazione. Si tratta pertanto di una applicazione diversa dal quantum computing: usare un quantum computer non implica necessariamente dover trasferire dati con comunicazioni quantistiche e viceversa.

La **crittografia quantistica** è intesa come la disciplina che punta a proteggere l'informazione rappresentata sottoforma di stati quantistici dal rischio di attacchi, quali l'esfiltrazione dei dati, l'impersonare il mittente o l'alterazione dei dati trasmessi. Ad oggi, l'esempio più rilevante di crittografia quantistica riguarda la capacità di trasmettere informazioni sotto forma di stati quantici in modo tale che esse siano teoricamente non intercettabili.

2.1 – Il Qubit

Come detto, la scienza dell'informazione quantistica sfrutta la possibilità di rappresentare informazione in un modo nuovo, basato appunto sugli stati quantistici della materia. Ciò è stato dimostrato essere possibile già negli anni '80, quando fu introdotto il concetto di qubit, come unità elementare di informazione quantistica contrapposta al bit, che invece costituisce l'unità elementare di informazione classica.

Come sappiamo, un bit classico può assumere due stati, 0 e 1, che sono mutuamente escludentisi. Un qubit ha invece la capacità, dovuta alla fisica quantistica, di assumere entrambi tali stati contemporaneamente, sfruttando un principio quantistico noto appunto come **sovrapposizione quantistica**. Tale principio consente al qubit di assumere contemporaneamente il valore 0 ed il valore 1 in uno stato di sovrapposizione quantistica, che viene riportato ad uno solo dei due stati classici per effetto di una eventuale misurazione. Fintanto che viene mantenuto lo stato di sovrapposizione, una sequenza di *n* qubit ha pertanto la possibilità di rappresentare tutte le combinazioni che potrebbero avere *n* bit classici, le quali sono ovviamente 2^n. Questo significa che sostanzialmente possiamo avere nello stesso tempo ed allo stesso posto tutti i possibili stati assunti da una variabile binaria sovrapposti in uno stato di sovrapposizione quantistica.

Oltre a tale importante principio della fisica quantistica, i qubit hanno l'ulteriore caratteristica, derivante dal **teorema di non clonazione**, di collassare nello stato classico qualora si provi a misurarli, impedendone sostanzialmente la copia. Questa proprietà è quella che sottende le soluzioni più rilevanti di crittografia quantistica, volte appunto a garantire la confidenzialità dei dati scambiati lungo un canale di comunicazione quantistica.

2.2 – Quantum key distribution

Per **distribuzione quantistica di chiave** o quantum key distribution (QKD) intendiamo tecniche finalizzate al trasferimento di una chiave segreta da una parte all'altra di un canale di comunicazione tramite una comunicazione quantistica. La prima implementazione di QKD fu proposta da Bennet e Brassard tramite il protocollo noto come BB84 [1], che codifica ogni bit della chiave segreta nello stato di polarizzazione di un singolo fotone. Poiché lo stato di polarizzazione di un singolo fotone non può essere misurato senza distruggerlo, il dato trasmesso diventa "fragile", e quindi impossibile da intercettare senza alterarlo. Successivamente, nel 1992 Bennett propose il protocollo B92 [2] come versione modificata del protocollo BB84, con la differenza fondamentale che mentre il protocollo BB84 utilizza quattro diversi stati di polarizzazione del fotone, il protocollo B92 ne utilizza soltanto due. Il protocollo alternativo proposto da Ekert, noto come E91 [3], sfrutta diversamente il principio dell'accoppiamento quantistico, facendo leva sull'impossibilità di prevedere prima della misurazione quale sarà lo stato osservato in due fotoni accoppiati. Il processo di comunicazione tramite stati accoppiati, con l'aiuto di un canale di comunicazione classico, è noto come teletrasporto quantistico ed è alla base del protocollo E91.

In ogni caso, le tecniche di QKD consentono di trasferire da un punto all'altro di un canale di comunicazione quantistico una chiave segreta, con la garanzia teorica che nessuno possa intercettarla. Come canali di comunicazione, normalmente si usano collegamenti ottici in fibra oppure, anche se meno frequentemente, in spazio libero.

Sebbene le tecniche di QKD forniscano importanti garanzie teoriche sulla sicurezza delle chiavi scambiate, esse sono soggette a significative limitazioni, che le rendono praticamente utilizzabili soltanto in scenari molto limitati. Una sintesi delle principali limitazioni a cui sono soggette le tecniche di QKD è stata proposta dalla statunitense National Security Agency (NSA) [4], e si possono riassumere come segue.

1. La distribuzione quantistica di chiavi è solo una **soluzione parziale**. Essa consente lo scambio di una chiave segreta che va poi usata insieme ad algoritmi di cifratura simmetrica per garantire la confidenzialità dei dati scambiati in modo classico. Essa si basa sull'assunzione che la trasmissione QKD originale provenga dall'entità desiderata, ma non fornisce uno strumento per autenticare la fonte della trasmissione QKD. Pertanto, l'autenticazione del mittente richiede l'uso di strumenti crittografici asimmetrici o di chiavi pre-condivise. Dal momento che tali strumenti crittografici devono comunque essere usati parallelamente alla QKD, essi possono direttamente fornire anche le funzioni di scambio delle chiavi in modo meno costoso e più consolidato rispetto alla QKD.
2. La distribuzione quantistica di chiavi richiede **apparecchiature speciali**. La QKD richiede collegamenti in fibra dedicati o di gestire fisicamente trasmettitori quantistici per propagazione libera. Ciò non si presta ad implementazioni software e/o integrazione nei dispositivi di rete esistenti. Poiché la QKD è basata sull'hardware, essa manca anche della necessaria flessibilità richiesta dagli aggiornamenti e dalle patch di sicurezza.
3. La distribuzione quantistica di chiavi comporta elevati **costi infrastrutturali** e rischi di **minacce interne**. Le reti QKD richiedono l'uso di fornitori di tecnologia fidati, il che comporta costi aggiuntivi per strutture sicure e rischi aggiuntivi per la sicurezza derivanti da minacce interne.

4. La **sicurezza** e la **validazione** delle soluzioni per distribuzione quantistica di chiavi rappresentano una sfida aperta. La sicurezza effettiva fornita da un sistema di QKD non è la sicurezza teorica incondizionata derivante dalle leggi della fisica, ma piuttosto la sicurezza derivante da hardware e relative soluzioni ingegneristiche. L'hardware utilizzato per eseguire la QKD può introdurre delle vulnerabilità, che hanno già portato a diversi attacchi ben noti a sistemi di QKD commerciali.
5. La distribuzione quantistica di chiavi aumenta il rischio di **denial of service**. La fragilità delle trasmissioni QKD, che da un lato è alla base loro della sicurezza, è evidentemente anche un elemento critico nei confronti di attacchi volti ad interrompere il servizio.

Le considerazioni sopra esposte forniscono motivazioni oggettive per ritenere la crittografia non-quantistica ancora preferibile a soluzioni di crittografia quantistica che, sebbene affascinanti da un punto di vista teorico, lasciano molte questioni aperte relativamente ad un loro uso pratico e pervasivo.

Tuttavia, come vedremo nel seguito, la possibilità che un attaccante si doti di un quantum computer mette a rischio molti dei sistemi che utilizzano la crittografia non-quantistica oggi disponibile. Resistendo anche ad attacchi provenienti da attaccanti dotati di quantum computer, la QKD e più in generale la crittografia quantistica viene quindi spesso proposta come una soluzione per la sopravvivenza della sicurezza dei nostri sistemi ICT, nonostante le sopra elencate limitazioni.

Esiste però una nuova branca della crittografia non-quantistica, chiamata **crittografia post-quantum**, **quantum-safe** oppure **quantum-resistant**, che, pur non richiedendo il ricorso a tecnologie quantistiche da parte degli interlocutori legittimi, è capace di garantire sicurezza rispetto ad attaccanti dotati di quantum computer. È questa la soluzione verso cui la comunità internazionale si sta maggiormente orientando, e che sarà brevemente descritta nel seguito.

3 - La minaccia del quantum computer alla crittografia

Il quantum computer fu teorizzato dai fisici Feynman e Manin già all'inizio degli anni '80 [5], [6] e sostanzialmente è un computer che usa gli stati quantistici della materia per fare calcoli. Quando abbiamo un computer classico e vogliamo fare calcolare a questo computer tutti i possibili valori assunti da una data funzione $f(\cdot)$ in corrispondenza di due bit di input, non possiamo fare altro che una ricerca esaustiva, cioè provare tutte le combinazioni di input e calcolare i corrispondenti valori di output.

Se la funzione $f(\cdot)$ si presta ad una descrizione algoritmica in termini di cosiddetti **quantum gate**, ovvero unità di elaborazione elementari di un quantum computer, allora il suo input può essere formulato in termini di qubit anziché di bit classici. Ciò implica che possiamo configurare lo stato quantistico dell'input in modo tale che rappresenti contemporaneamente tutte e quattro le configurazioni di due bit. Il calcolo verrà quindi eseguito una volta sola, ma tenendo conto di tutte le possibili configurazioni dei bit di ingresso.

Ciò permette di accelerare notevolmente l'esecuzione di alcuni algoritmi, portando la loro complessità dall'essere esponenziale nella lunghezza dell'input quando eseguiti su un computer classico a diventare polinomiale nella lunghezza dell'input su di un quantum computer.

Partendo dalla formulazione teorica del quantum computer, sebbene lo stato della tecnologia non lasciasse ancora intravedere la possibilità di costruirne uno reale, già negli anni '90 alcuni fisici introdussero algoritmi capaci di risolvere su un quantum computer alcuni problemi notoriamente difficili da risolvere con i computer classici. In particolare, nel '94 **Shor** introdusse un algoritmo capace di accelerare drasticamente la fattorizzazione di numeri interi su un quantum computer [7], problema notoriamente difficile da risolvere su un computer classico. Due anni dopo, nel '96, **Grover** introdusse un altro algoritmo quantum capace di accelerare le ricerche di elementi nelle liste non ordinate di un fattore quadratico rispetto al suo equivalente eseguibile su un computer classico [8].

Entrambi tali algoritmi quantum rappresentano una minaccia alla sicurezza di molti dei sistemi crittografici asimmetrici oggi più diffusi, che per tale motivo vengono definiti **quantum-vulnerable**. Tra questi vi sono tutti gli algoritmi crittografici che basano la loro sicurezza sulla difficoltà di fattorizzare grandi numeri interi e calcolare logaritmi discreti, come RSA, Diffie-Hellmann, ElGamal, curve ellittiche e firme digitali basate sugli stessi principi (come DSA e ECDSA). Questi algoritmi crittografici sono alla base di gran parte dei nostri sistemi ICT e delle nostre reti; pertanto, oggi il quantum computer rappresenta una effettiva minaccia alla sicurezza della nostra vita digitale.

3.1 – Lo stato del quantum computer

Sebbene, dopo essere stato teorizzato negli anni '80, il quantum computer sia rimasto per molti anni solo un concetto teorico, in epoca recente esso è velocemente diventato realtà. Già dal 2010 a seguire sono diventati disponibili alcuni primi quantum computer, prodotti dall'azienda statunitense D-Wave Systems, capaci di gestire quantità di qubit piuttosto elevate (i sistemi annunciati da D-Wave Systems nel 2017 già promettevano di lavorare con 2000 qubit). Tuttavia, tali sistemi non rispondono al paradigma più generale di quantum computing, in quanto sfruttano il fenomeno quantistico del **quantum annealing**, che è meno versatile del fenomeno di **quantum superposition** che è alla base dell'idea più generale di quantum computer. Pertanto, tali primi quantum computer non sono in realtà adatti ad eseguire gli algoritmi quantum più generali, come i sopracitati algoritmi di Shor e Grover.

Proprio nel 2017, però, l'azienda IBM ha pubblicamente annunciato il proprio progetto denominato "**Q system one**", volto a sviluppare un quantum computer basato su quantum superposition capace di eseguire elaborazioni su 20 qubit.

Sebbene tale numero di qubit sia considerato ancora insufficiente a determinare la cosiddetta **quantum supremacy**, ovvero la capacità per un quantum computer di superare un computer classico nell'esecuzione di elaborazioni (per la quale si ritiene necessario superare la soglia dei 50 qubit), esso rappresenta un primo fondamentale risultato nella corsa verso la creazione del quantum computer.

Parallelamente, nel 2017 Google annunciò che stava lavorando ad un quantum computer dotato di 72 bit, progetto che però si rivelò irrealizzabile per questioni di non controllabilità di così tanti qubit. Nondimeno, nel 2019 Google annunciò che il proprio sistema Sycamore con 53 qubit era capace di eseguire in 200 secondi un calcolo che avrebbe richiesto 10.000 anni su un computer normale. La scalabilità del numero di qubit è effettivamente il limite più significativo di tali progetti, ed un ulteriore passo in avanti è stato fatto nel 2020 con l'annuncio da parte della startup IonQ di un quantum computer a 32 qubit con bassi tassi d'errore, necessari affinché la tecnologia sia scalabile.

Da allora gli avanzamenti si sono susseguiti: nel 2020 un team dell'Università della Scienza e Tecnologia della Cina (USTC) ha sviluppato Jiuzhang, un quantum computer basato su fotoni anziché superconduttori, nel Giugno del 2021 ricercatori cinesi hanno sperimentato Zuchongzi, dotato di 56 qubit basati su superconduttori, e nell'Ottobre del 2021 Zuchongzi è stato esteso a 66 qubit. Nel frattempo, IBM ha annunciato una intensa roadmap nello sviluppo di unità di elaborazione quantistica (QPU) sempre più avanzate, fino all'annuncio del Novembre 2022 di aver completato lo sviluppo di una QPU da 433 qubit denominata Osprey, e l'annuncio di sviluppare il sistema denominato Condor con più di 1000 qubit entro il 2023.

4 - La crittografia post-quantum

Come anticipato, molti dei sistemi crittografici che oggi usiamo quotidianamente, in particolare quelli per crittografia asimmetrica, sono vulnerabili nei confronti di un potenziale attaccante dotato di un quantum computer.

Pertanto, per ristabilire adeguati livelli di sicurezza anche nei confronti di attaccanti quantum, è necessario sostituire tali algoritmi crittografici **quantum-vulnerable** con algoritmi alternativi che siano **quantum-safe** o **post-quantum**, ossia capaci di resistere anche ad attaccanti provvisti di quantum computer.

Già dal 2016 lo statunitense National Institute of Standards and Technology (NIST) ha avviato una competizione internazionale rivolta alla comunità scientifica e volta a selezionare e standardizzare algoritmi crittografici post-quantum [9]. In risposta al bando del NIST, gruppi di ricerca di tutto il mondo sono stati invitati ad inviare proposte per algoritmi crittografici post-quantum per la cifratura asimmetrica, lo scambio delle chiavi e la firma digitale.

Le proposte dei candidati sono state raccolte entro Novembre 2017, poi valutate in un primo round fino a Gennaio 2019, un secondo round fino a Luglio 2020 ed un terzo round fino a Luglio 2022, quando sono stati annunciati i primi algoritmi da standardizzare. Contemporaneamente, è stato avviato un quarto ed ultimo round ed aperto un nuovo bando, che non era inizialmente previsto, per le sole firme digitali, con scadenza a Giugno 2023.

I primi due algoritmi selezionati per la standardizzazione del NIST sono Crystals-Kyber per lo scambio di chiave e Crystals-Dilithium per la firma digitale, entrambi basati sull'algebra dei reticoli. Essi sono stati selezionati per le eccellenti prestazioni e l'elevato livello di sicurezza. Oltre ad essi, l'algoritmo Falcon, anch'esso basato sull'algebra dei reticoli, e l'algoritmo SPHINCS+, basato su funzioni hash, sono stati selezionati per le firme digitali. Gli algoritmi BIKE, Classic McEliece e HQC basati sui codici per la correzione d'errore sono invece stati ammessi ad un ulteriore round di valutazione e selezione, insieme all'algoritmo SIKE basato su isogenie supersingolari tra curve ellittiche. I primi standard sono attesi per il 2024, mentre la comunità scientifica e lo stesso NIST continua a sviluppare e valutare ulteriori soluzioni che potranno affiancare quelle che sono già in via di standardizzazione.

Se da una parte il processo di selezione del NIST ha già prodotto una rosa di soluzioni crittografiche quantum-safe adatte a subentrare a quelle quantum-vulnerable ed iniziare a proteggere presto i nostri sistemi ICT anche da attaccanti provvisti di quantum computer, dall'altra esso è stato disseminato di imprevisti. Ad esempio, il sistema di firma digitale basato su equazioni multivariate Rainbow, che a Luglio 2020 è stato ammesso al terzo round dopo una lunga analisi, è stato attaccato a Febbraio 2022. Ancora più sorprendentemente, il candidato SIKE, che era stato ammesso al quarto round a Luglio 2022, è stato attaccato poche settimane dopo.

Un altro limite del processo di standardizzazione del NIST è stato l'incapacità di offrire una rosa sufficientemente variegata di soluzioni per la realizzazione di firme digitali. Solo sistemi basati sull'algebra dei reticoli o su funzioni hash sono rimasti a valle del processo di selezione, e questo ha spinto il NIST ad aprire una nuova gara a cui la comunità scientifica sta nuovamente partecipando. La lista dei candidati presentati in risposta a tale nuova gara sarà presto resa pubblica, ma sono sicuramente state presentate numerose proposte di nuovi sistemi di firma digitale post-quantum capaci di superare i principali limiti di quelli esistenti. Tra questi, vi sono i sistemi LESS [10] e CROSS [11], sviluppati da gruppi di lavoro che includono ricercatori italiani.

5 – Impatto su reti e sistemi 5G

La necessità di avere presto a disposizione algoritmi crittografici post-quantum sicuri ed efficienti è evidenziata dal fatto che algoritmi crittografici quantum-vulnerable sono purtroppo oggi presenti in gran parte dei dispositivi e dei sistemi ICT di uso quotidiano.

5.1 – Protocolli di rete

Un primo esempio è il protocollo SSL/TLS, che serve a rendere sicure le comunicazioni Internet basate sui ben noti protocolli TCP e UDP. Oggi usiamo TLS ogni volta che usiamo Internet, quando il nostro browser stabilisce una connessione autenticata e confidenziale (indicata solitamente con un lucchetto verde) verso un qualunque server, dal banking online alla semplice navigazione per scopi informativi. Il protocollo SSL/TLS è nato molti anni fa, nel '94, ed è stato poi standardizzato da IETF fino all'attuale versione TLS 1.3, oggi considerata lo stato dell'arte. All'interno del protocollo TLS la crittografia si usa pesantemente, e lo si fa ogni volta che si stabilisce una nuova connessione. Allo scopo, i due interlocutori devono negoziare un insieme di algoritmi crittografici (noto come **cipher suite**) che utilizzeranno per ottenere autenticazione e confidenzialità delle loro comunicazioni. Tali algoritmi crittografici servono innanzitutto per effettuare uno scambio iniziale (handshake) di materiale crittografico su un canale non ancora protetto, e per questo si fa uso della crittografia asimmetrica e delle firme digitali. Terminata tale fase, i due terminali hanno a disposizione una o più chiavi segrete simmetriche condivise, che possono usare per applicare un metodo di cifratura simmetrica ai dati che desiderano scambiarsi in modo confidenziale. Quello seguente è un esempio tipico di cipher suite TLS:

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

In tal caso, si utilizza uno scambio di chiave iniziale tramite il protocollo di Diffie-Hellmann basato su curve ellittiche (ECDHE), con autenticazione basata su firma digitale RSA. La cifratura asimmetrica avviene poi tramite l'algoritmo AES in modalità Galois Counter Mode, che offre anche autenticazione dei dati, mentre l'integrità è fornita dalla funzione hash SHA256.

Un eventuale attaccante provvisto di un quantum computer potrebbe sfruttare l'algoritmo di Grover per accelerare di un fattore quadratico l'analisi esaustiva delle chiavi segrete di AES e la ricerca di collisioni nella funzione hash SHA256. Ciò si può fronteggiare senza il bisogno di abbandonare tali algoritmi, ma semplicemente aumentando a circa il doppio la lunghezza delle chiavi segrete e degli hash digest. Però, l'attaccante provvisto di quantum computer potrebbe utilizzare l'algoritmo di Shor per recuperare in tempi ragionevoli le chiavi private a partire dalle corrispondenti chiavi pubbliche usate in ECDHE e RSA. Pertanto, tali algoritmi devono necessariamente essere sostituiti con delle alternative **quantum-safe**.

Esiste effettivamente una bozza di standard IETF che introduce la possibilità di eseguire uno scambio di chiavi ibrido in TLS 1.3 [12]. Ciò significa usare algoritmi multipli di scambio di chiave, per poi combinare i vari risultati con l'obiettivo di fornire sicurezza anche se tutti tranne uno degli algoritmi componenti fossero compromessi[1].

In una situazione analoga ci si trova quando consideriamo protocolli per comunicazioni Internet sicure che lavorano a livello 3 della pila protocollare ISO/OSI, come IPsec che si usa nelle applicazioni VPN.

Anche in questo caso, un protocollo di handshaking iniziale (ad esempio, IKEv2) deve essere usato per effettuare uno scambio iniziale di materiale crittografico su un canale non ancora sicuro. A tale scopo, anche IKEv2 normalmente usa il protocollo di Diffie-Hellmann, che è quantum-vulnerable, e va sostituito con un'alternativa **quantum-safe**. Invece, per la successiva trasmissione di dati confidenziali ed autenticati si fa ricorso nuovamente agli algoritmi AES e SHA2, che possono essere usati anche in presenza di attaccanti provvisti di quantum computer, a condizione di aumentare la lunghezza di chiavi segrete e digest.

Esistono progetti che mirano ad estendere il protocollo IKEv2 per supportare l'uso di crittografia post-quantum, però essi non produrranno risultati nel breve termine in attesa del rilascio degli standard NIST.

[1] Ciò consente di introdurre algoritmi di scambio di chiave post-quantum in TLS, affiancandoli agli attuali algoritmi quantum-vulnerable, per avviare una transizione progressiva verso l'uso di cipher suite post-quantum.

Per far fronte temporaneamente al problema, è stata invece proposta una estensione di IKEv2 che introduce l'uso di chiavi pre-condivise [13]; quindi, sostanzialmente abbandona temporaneamente la crittografia asimmetrica e usa quella simmetrica al suo posto, richiedendo chiavi pre-condivise manualmente. Una tale soluzione è chiaramente applicabile se si usano un numero limitato di terminali, ma diventa rapidamente inapplicabile su reti che comprendono molti terminali.

5.2 – Sistemi 5G

I sistemi e le reti 5G derivano dalle precedenti generazioni di reti radiomobili, ma rispetto ad esse introducono una forte componente di astrazione e virtualizzazione basata sul software e su soluzioni mutuate dall'architettura di Internet. In particolare, il paradigma del **Software Defined Networking** (SDN) caratteristico del 5G sfrutta una architettura basata su tre livelli:

- Application plane, che include le applicazioni SDN
- Control plane, dedicato ai controllori SDN
- Data plane, che contiene i nodi SDN

Le comunicazioni tra questi tre piani operativi utilizzano comuni protocolli Internet, ed in particolare sfruttano i sopracitati protocolli TLS e IPsec per ottenere confidenzialità ed autenticazione. Pertanto, valgono in questo ambito le medesime considerazioni riportate nella precedente sezione per quanto riguarda l'esposizione ad attacchi basati su quantum computer e l'adozione di algoritmi crittografici **quantum-safe**.

Un ulteriore aspetto dell'architettura 5G che si espone al rischio di attacchi basati su quantum computer riguarda la possibilità di accesso degli utenti tramite reti non-3GPP. Nelle reti 5G esiste infatti la funzione N3IWF (non-3GPP Inter-Working Function) che consente l'accesso alla rete 5G anche ad utenti provenienti da reti di accesso (RAN) diverse dalla rete di accesso 5G (come ad esempio le reti wireless). Il N3IWF deve fornire una connessione sicura per il dispositivo dell'utente e lo fa utilizzando IPsec per la comunicazione tra il dispositivo dell'utente ed il N3IWF.

Pertanto, anche in questo caso, è necessaria l'adozione di strumenti crittografici **quantum-safe** per proteggere la rete di accesso 5G da attacchi basati su quantum computer.

Anche la protezione della privacy degli utenti nelle reti 5G fa affidamento su strumenti crittografici asimmetrici. In particolare, per l'accesso alla rete l'identificativo IMSI (International Mobile Subscriber Identity) dell'utente deve essere mascherato affinché non sia trasmesso in chiaro, trattandosi di un dato personale dell'utente stesso. Per questo scopo, il 5G prevede che l'utente autentichi il proprio IMSI usando una propria chiave privata di crittografia asimmetrica basata su curve ellittiche, e poi lo cifri usando la chiave pubblica della rete di appartenenza per ottenere confidenzialità. Si ottiene così il SUCI (Subscription Concealed Identifier), che viene usato per la registrazione alla rete 5G proteggendo l'identità dell'utente. Una volta ricevuto dalla rete, esso viene decifrato usando la chiave privata della rete stessa, e ne viene verificata l'autenticità usando la chiave pubblica dell'utente. Trattandosi di un sistema crittografico asimmetrico basato su curve ellittiche, anch'esso è vulnerabile ad attacchi basati su quantum computer che sfruttino l'algoritmo di Shor; pertanto, deve essere rimpiazzato con uno alternativo che sia **quantum-safe**.

Così come per i protocolli TLS e IPsec, iniziative per la transizione di queste tecniche verso soluzioni quantum-safe iniziano a muovere i primi passi. Relativamente all'architettura 5G, 3GPP ha già iniziato a studiare l'adozione di chiavi di 256 bit nei cifrari simmetrici usati in 5G per contrastare l'algoritmo di Grover [14]. 3GPP considera invece ancora prematuro studiare l'inclusione di cifrari asimmetrici post-quantum in 5G, in quanto non sono ancora disponibili i primi standard NIST, previsti entro il 2024.

5 – Conclusioni

In conclusione, abbiamo descritto come la scienza dell'informazione quantistica promette di modificare l'attuale scenario della elaborazione e della trasmissione di dati, con particolare riferimento alle comunicazioni sicure. Abbiamo illustrato come un quantum computer rappresenti una minaccia nei confronti di gran parte della crittografia che oggi usiamo nei nostri sistemi ICT, e come l'uso di tecnologie quantistiche offra una difesa solo parziale nei confronti di tale minaccia. Abbiamo introdotto il concetto di crittografia post-quantum, e mostrato come essa invece possa aiutarci a difendere i nostri sistemi ICT da attaccanti dotati di quantum computer, senza richiedere il ricorso a tecnologie quantistiche da parte degli utenti legittimi, e potendosi integrare nelle tecnologie esistenti. Abbiamo considerato casi di studio basati sulle comunicazioni Internet sicure e sulle reti 5G, mostrando quali aggiornamenti sono necessari per mantenere il loro livello sicurezza anche in presenza di attaccanti dotati di quantum computer.

9 - Bibliografia

[1] C.H. Bennett, G. Brassard, "Quantum Cryptography: Public-Key Distribution and Coin Tossing", Proceedings of the International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984.

[2] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states" Physical review letters, 68, 3121, 1992.

[3] A. Ekert. "Quantum cryptography based on Bell's theorem." Physical review letters, 67, 1991, pp. 661-663.

[4] National Security Agency, "Quantum Key Distribution (QKD) and Quantum Cryptography (QC)", 2020, online, available: https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

[5] R. P. Feynman, "Simulating physics with computers", International Journal of Theoretical Physics, 21, 1981, pp. 467-488.

[6] Y. Manin, "Computable and Uncomputable", Sovetskoye Radio, Moscow, 128, 1980.

[7] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring", Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE Comput. Soc. Press, 1994, pp. 124-134.

[8] L. K. Grover, "A fast quantum mechanical algorithm for database search", Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing. STOC '96. Philadelphia, Pennsylvania, USA: Association for Computing Machinery, 1996, pp. 212–219.

[9] NIST Post-Quantum Cryptography project, online, available: https://csrc.nist.gov/projects/post-quantum-cryptography.

[10] LESS: Linear Equivalence Signature Scheme, online, available: https://www.less-project.com.

[11] CROSS: Codes and Restricted Objects Signature Scheme, online, available: https://cross-crypto.com.

[12] D. Stebila, S. Fluhrer, S. Gueron, "Hybrid key exchange in TLS 1.3", Network Working Group, draft-ietf-tls-hybrid-design-06, February 2023.

[13] S. Fluhrer, P. Kampanakis, D. McGrew, V. Smyslov, "Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security", Internet Engineering Task Force (IETF) RFC 8784, June 2020.

[14] 3rd Generation Partnership Project (3GPP), Technical Specification Group Services and Systems Aspects; Security aspects, "Study on the support of 256-bit algorithms for 5G", (Release 16), 3GPP TR 33.841 V16.1.0, 2019.