Agenzia per la Cybersicurezza Nazionale

CRITTOGRAFIA POST-QUANTUM E QUANTISTICA

Preparazione alla Minaccia Quantistica

LUGLIO 2024

Questo documento, elaborato dall'Agenzia per la Cybersicurezza Nazionale, contiene un'introduzione sul tema della crittografia post-quantum e quantistica come soluzione alla minaccia quantistica.
Il documento tiene in considerazione gli sviluppi e le minacce presenti al giorno della sua pubblicazione.

Versione	Data di pubblicazione	Note
1.0	**11/07/2024**	**Prima pubblicazione**

Sommario

Indice delle figure

Indice delle tabelle

1 Introduzione

L'avvento del computer quantistico ha portato con sé grandi novità nel mondo dell'informazione, permettendo di effettuare operazioni che un computer classico non può svolgere. Tuttavia, dal punto di vista della crittografia, sono stati sviluppati algoritmi quantistici che porterebbero alla compromissione dei problemi matematici su cui si basa la sicurezza di alcuni dei crittosistemi più utilizzati. Anche se al momento non sembrano esistere calcolatori quantistici con potenza computazionale e affidabilità sufficienti a perpetrare questi attacchi, la sicurezza dei cifrari a chiave pubblica risulta seriamente compromessa.

Per questo motivo, la comunità scientifica, guidata dal National Institute of Standard and Technologies (NIST) statunitense, si sta concentrando sulla ricerca di cifrari resistenti agli attacchi perpetrati dai computer quantistici, ma che possano essere implementati sui computer attuali: i cosiddetti algoritmi post-quantum.

Un'ulteriore possibilità consiste nell'avvalersi della meccanica quantistica per lo sviluppo di nuovi algoritmi di cifratura, che possano sfruttare le capacità introdotte. Si parla in questo caso di crittografia quantistica, che, al momento, trova applicazioni solo nei contesti di distribuzione delle chiavi crittografiche.

Si prevede dunque una migrazione di tutti i sistemi che utilizzano gli attuali standard di crittografia a chiave pubblica verso i nuovi algoritmi post-quantum o quantistici. Da un punto di vista organizzativo, gli Stati Uniti hanno iniziato a pianificare l'aggiornamento dei propri protocolli crittografici, pubblicando una serie di appunti e memorandum per coordinare al meglio questo cambiamento. Anche l'Unione Europea ha iniziato a occuparsi della definizione di un procedimento di transizione analogo e, allo stesso modo, anche il nostro Paese dovrà organizzare e intraprendere al più presto un procedimento per aggiornare i propri sistemi crittografici.

Questo documento intende fornire un'introduzione alla minaccia portata alla crittografia dall'avvento dei computer quantistici, illustrando le principali soluzioni ideate dalla comunità scientifica, ossia la crittografia post-quantum e la crittografia quantistica.

2 La minaccia quantum

La rivoluzione dovuta all'avvento dei computer ha cambiato il concetto di crittografia, che fino ad allora si basava unicamente sulla segretezza della chiave utilizzata per nascondere i messaggi. In aggiunta agli algoritmi classici, denominati **simmetrici** o a **chiave segreta**, vennero introdotti gli algoritmi **asimmetrici** o a **chiave pubblica** [1], la cui sicurezza è legata alla difficoltà di risoluzione di particolari problemi matematici ritenuti complicati.
Negli ultimi decenni, prima solo teoricamente e poi più concretamente, si è definito il concetto di **computer quantistico** [2], cioè una macchina i cui processi si basano sulla meccanica quantistica. Le capacità di queste nuove tecnologie sono ancora scarse per ragioni costruttive, ma il loro potenziale è molto alto. Nello specifico, i computer quantistici sono teoricamente in grado di effettuare calcoli tra stati, detti **qubit**, che corrispondono alla sovrapposizione di più stati classici, massimizzando quindi la parallelizzazione e surclassando i computer classici su alcune particolari classi di problemi. In aggiunta, sono stati ideati nuovi algoritmi implementabili solo su computer quantistici che saranno capaci di attaccare alcuni dei sistemi di crittografia più diffusi al giorno d'oggi.

2.1 Crittografia simmetrica e l'algoritmo di Grover

Gli algoritmi di cifratura simmetrica, nei quali la chiave di cifratura è uguale a quella di decifratura, sono i più veloci ed efficienti e quindi vengono comunemente utilizzati per cifrare grandi moli di dati. Tuttavia, un grosso svantaggio è la necessità di istituire un **canale sicuro** con il quale gli utenti possono scambiarsi la chiave segreta, senza correre il rischio che venga intercettata. Per questo motivo, la cifratura simmetrica non può essere l'unica adottata, soprattutto in una società digitale con miliardi di utenti, nella quale la creazione di un canale sicuro sarebbe una pratica troppo dispendiosa.
Attualmente l'algoritmo simmetrico più utilizzato è **AES** (Advanced Encryption Standard), un cifrario a blocchi riconosciuto standard dal NIST [3] e, per l'Unione Europea, dal SOG-IS (Senior Official Group Information Systems Security, un accordo di riconoscimento internazionale riguardo la sicurezza dei sistemi informativi) [4]. I migliori attacchi conosciuti, basati su crittoanalisi differenziale e lineare, restano comunque inefficienti per chiavi di grandi dimensioni (da 128 a 256 bit). Allo stesso modo, un attacco a forza bruta, cioè una ricerca esaustiva tra tutte le possibili chiavi, risulta altamente inefficiente e quindi fallimentare.
Uno dei primi algoritmi teorizzati su computer quantistico è l'algoritmo di **Grover** [5], che si pone come obiettivo la risoluzione dei problemi di ricerca di un elemento specifico all'interno di un database. A differenza degli algoritmi classici, che per un database di N dati richiedono un numero di operazioni dell'ordine di N, l'algoritmo di Grover permette

di ridurre tale numero a $\sqrt{N}$. Dal punto di vista crittografico, questo corrisponde a una velocizzazione **quadratica** di ogni algoritmo di forza bruta. Di conseguenza, al fine di mantenere invariato il livello di sicurezza attualmente ottenuto contro attacchi classici, la lunghezza delle chiavi segrete dei cifrari simmetrici deve essere semplicemente **raddoppiata**. Eccetto questa modifica, che comunque comporta un aumento dei dati da scambiare tramite canale sicuro e quindi un peggioramento delle prestazioni, gli attuali algoritmi di cifratura simmetrica risultano resistenti agli attacchi da parte di computer quantistici e non sembra perciò necessario ad ora definire un nuovo standard di crittografia simmetrica.

2.2 Crittografia asimmetrica e l'algoritmo di Shor

L'introduzione della crittografia asimmetrica o a chiave pubblica è dovuta a Whitfield Diffie e Martin Hellman [1], i quali proposero un metodo per lo scambio di un segreto attraverso un canale insicuro tramite l'utilizzo di parametri pubblici. Data una particolare struttura algebrica, chiamata gruppo ciclico definito da un parametro pubblico g (il generatore del gruppo) e, dato il valore g^a, il loro crittosistema si basa sulla difficoltà di trovare l'esponente a. Questo problema è estremamente complesso da risolvere con i mezzi attuali ed è chiamato problema del **logaritmo discreto**. Il protocollo di **Diffie-Hellman** (DH) è tuttora largamente utilizzato, specialmente nelle varianti che sfruttano **Curve Ellittiche** (ECDH), ma anche nelle varianti sui **Campi Finiti** (FFDH) [6]. Un altro importante contesto di applicazione del logaritmo discreto è la firma digitale: lo standard **DSA** (Digital Signature Algorithm), definito sui gruppi moltiplicativi dei campi finiti, e la versione con curve ellittiche **ECDSA** [7] basano la loro sicurezza sulla difficoltà del logaritmo discreto.

Una seconda tipologia di crittosistemi a chiave pubblica fonda la propria sicurezza sulla difficoltà della **fattorizzazione** dei numeri interi nei loro fattori primi. L'algoritmo di questo tipo più famoso e utilizzato è **RSA** [8], acronimo derivante dai cognomi dei creatori Ron Rivest, Adi Shamir e Leonard Adleman, il quale consente di cifrare efficientemente un messaggio o può essere sfruttato per ottenere un algoritmo per la firma digitale [6].

Dato che questi algoritmi si basano sulla difficoltà di risoluzione di diversi problemi matematici, la loro sicurezza viene misurata in base a un confronto con quella di AES, per cui si ottengono le dimensioni delle chiavi descritte in Tabella 1. Da notare come le chiavi di AES siano le più piccole, poiché non esistono attacchi significativamente più efficienti di quello a forza bruta. Invece, per quanto riguarda gli algoritmi a chiave pubblica, è possibile utilizzare attacchi più specializzati, dipendenti dal problema matematico sottostante. Di conseguenza, in questi casi, è necessario che le chiavi siano di lunghezza maggiore per fornire un livello di sicurezza equivalente a quello di AES.

Oltre a richiedere chiavi più grandi, gli algoritmi asimmetrici sono più lenti rispetto a quelli simmetrici, ma hanno il grande vantaggio di non necessitare di un canale sicuro per condividere un segreto. Di conseguenza, la pratica più comune consiste nell'utilizzarli per firme digitali di documenti e scambi di chiavi segrete da adottare in seguito per cifrature simmetriche.

Tuttavia, tutti gli algoritmi a chiave pubblica in uso al giorno d'oggi sono minacciati dai computer quantistici: quando saranno sufficientemente potenti e affidabili, si potrà sfruttare l'algoritmo di **Shor** [9], che permette di risolvere in modo efficiente sia il problema del logaritmo discreto che quello della fattorizzazione di interi.

I computer quantistici esistenti non sono in grado di risolvere i problemi degli algoritmi a chiave pubblica utilizzati al momento, ma è necessario prepararsi all'eventualità che questi possano costituire una **minaccia reale** entro qualche decennio.

AES	Curve Ellittiche	Campi Finiti	RSA
128	256	3072	3072
192	384	7680	7680
256	512	15360	15360

Tabella 1 - Lunghezza delle chiavi in bit a parità di sicurezza classica [10]

3 Crittografia post-quantum

Al fine di preservare l'utilizzo della crittografia asimmetrica, la comunità scientifica ha iniziato a cercare alternative ai crittosistemi attuali che siano resistenti anche ad attacchi quantistici, dando origine alla crittografia **post-quantum**. L'alta priorità è dovuta sia alla difficile prevedibilità dello sviluppo delle tecnologie quantistiche, sia al cosiddetto scenario **harvest now, decrypt later**, cioè al rischio che un attaccante intercetti ora dati cifrati con algoritmi asimmetrici classici e li memorizzi, per poi decifrarli in futuro, quando avrà a disposizione un computer quantistico dotato di sufficiente potenza computazionale. Ad esempio, nello scambio di chiavi simmetriche utilizzate per cifrare dati estremamente sensibili, è necessario che queste siano mantenute sicure per decenni e uno scenario come quello descritto sarebbe estremamente pericoloso.
In generale, rispetto alla crittografia classica, i cifrari post-quantum presentano un incremento delle dimensioni dei parametri pubblici e della dimensione di cifrati o firme, oppure un aumento significativo dei tempi di esecuzione. Il trade-off tra queste due caratteristiche è un aspetto fondamentale nella **migrazione** dai cifrari attuali a quelli post-quantum, da tenere in considerazione per non incappare in colli di bottiglia dovuti a limiti di memoria e per non rallentare eccessivamente i sistemi e i protocolli che richiedono molte cifrature o firme.

3.1 Tipologie di algoritmi post-quantum

La sicurezza degli algoritmi post-quantum si basa su problemi matematici congetturati sicuri anche contro attacchi perpetrati da computer quantistici. Generalmente, si tratta di problemi di nuova introduzione o poco studiati dal punto di vista delle applicazioni crittografiche. Per questo motivo, è difficile fornire delle stime sulla longevità dei nuovi algoritmi e si richiede un tempo di valutazione che possa variare in base alla tipologia di problema adottato. Di seguito si introducono e descrivono brevemente le tipologie più comuni al momento.

3.1.1 Reticoli e Learning With Errors (LWE)

Un **reticolo** è una struttura algebrica, definita come un sottogruppo discreto di uno spazio vettoriale reale n-dimensionale. In altri termini, può essere visto come un insieme di punti regolarmente distribuiti all'interno di uno spazio di dimensione n, tra i quali è possibile effettuare un'operazione di somma che restituisce un altro punto del reticolo. Un esempio nel piano, cioè uno spazio 2-dimensionale, è rappresentato in Figura 1.
Uno dei problemi matematici sul quale si basa la sicurezza degli algoritmi post-quantum è lo **Shortest Vector Problem** (SVP): dato un reticolo, trovare il suo punto non nullo più vicino all'origine dello spazio.

Nonostante il problema risulti semplice per dimensioni piccole, come in Figura 1, attualmente non esistono algoritmi efficienti in grado di risolvere il problema al crescere della dimensione n.
Un secondo problema utile per la crittografia post-quantum, collegato alla teoria dei reticoli, è il **Learning With Errors** (LWE): dati una matrice A, un vettore b qualsiasi e un vettore e piccolo corrispondente a un **errore** e considerando il sistema di equazioni lineari modulari perturbato definito come $A \cdot x + e = b$, il problema è trovare un vettore soluzione x che soddisfi il sistema. Nonostante nella formulazione di questo problema non sia prevista direttamente la definizione di un reticolo, è possibile ricondurre LWE ad altri problemi definiti sui reticoli, tra cui una variante di SVP.
Un terzo problema alla base di alcuni algoritmi crittografici post-quantum, molto simile a LWE, è il problema della **Short Integer Solution** (SIS): considerati una matrice A e il sistema di equazioni lineari modulari dato da $A \cdot x = 0$, trovare un vettore x "corto" che risolve il sistema, dove la nozione di lunghezza di un vettore è definita a partire da una metrica indotta. Anche in questo caso, ci si può ricondurre a un problema che è una variante di SVP.
Questi problemi hanno diverse varianti a seconda della struttura algebrica sulla quale sono definiti gli elementi del reticolo: se si considera l'anello R dei polinomi a coefficienti su un campo finito si parla di **RLWE** e **RSIS** (dall'inglese Ring), se invece si considera l'insieme delle matrici con coefficienti definiti nello stesso anello R, chiamato in algebra modulo, si parla di **MLWE** e **MSIS**.
In un paragone con le altre famiglie di algoritmi post-quantum, gli algoritmi basati su reticoli presentano ottime prestazioni e una dimensione media di chiavi e cifrati/firme. Inoltre, alcuni algoritmi basati sui reticoli, come **NTRU** [11], vengono studiati da più di 20 anni per cui la loro sicurezza è generalmente consolidata. Per questi motivi, sono tra i sistemi più presenti in letteratura [12].

3.1.2 Codici a correzione di errori

In seguito alla ricezione di un messaggio è fondamentale poter capire se sono avvenuti degli errori e riuscire a correggerli. I **codici a correzione di errori** sono uno strumento adatto a tale scopo e vengono impiegati in applicazioni comuni come lettori CD o codici QR, oltre a essere alla base di alcuni algoritmi post-quantum. In particolare, un codice introduce ridondanza nel messaggio così che si possa ricostruire la versione originale in caso di errori. Un esempio è raffigurato nella Figura 2 che descrive come inviando un singolo bit ripetuto tre volte sia possibile ricostruirlo senza ambiguità nel caso avvenga un solo errore.
Più in generale, un codice è definito a partire da una matrice di **controllo di parità** (o parity-check) H che permette di capire se un messaggio x contiene errori semplicemente calcolando il vettore $s = H \cdot x$, detto **sindrome**. Se s è nullo, allora non sono avvenuti errori, altrimenti è possibile riconoscere le variazioni nella parola del codice trasmessa e

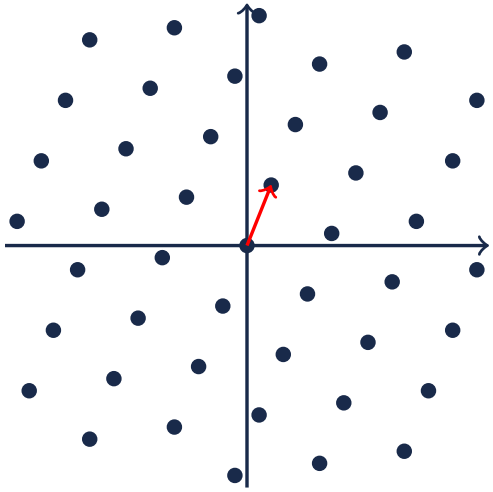

Figura 1 - Reticolo 2-dimensionale con vettore di lunghezza minima in rosso

ricostruire il messaggio originale, supponendo che non siano avvenuti più errori di quelli rilevabili e correggibili dal codice in uso. Generalmente, questa ricostruzione non è efficiente, ma per alcuni codici può essere velocizzata grazie alla conoscenza di alcuni dati aggiuntivi.
Dal punto di vista della creazione di un algoritmo crittografico, si può cifrare un messaggio aggiungendo un errore che solamente chi conosce i dati aggiuntivi può correggere rapidamente. Il problema alla base della sicurezza di questa tipologia di algoritmi viene chiamato **Syndrome Decoding Problem** (SDP).
Confrontando gli algoritmi basati su codici con le altre famiglie, i tempi di computazione sono moderati ma la dimensione delle chiavi è enorme. Tuttavia, il primo algoritmo basato su codici, il cifrario **McEliece**, risale al 1978 [13], per cui si tratta della famiglia di algoritmi post-quantum più datata e quindi più studiata, il che la rende particolarmente affidabile. Per questi motivi, gli algoritmi basati su codici sono tenuti in considerazione ancora oggi, soprattutto per quelle applicazioni che richiedono alta sicurezza, poche cifrature e non hanno particolari vincoli di memoria.

3.1.3 Funzioni di hash

Gli algoritmi post-quantum basati su **funzioni di hash** utilizzano queste primitive crittografiche come strumento alla base della propria sicurezza. Le funzioni di hash crittografiche devono resistere a determinate proprietà per essere considerate sicure. In particolare, devono essere resistenti al calcolo della preimmagine, della seconda preimmagine e delle collisioni. Si rimanda al documento della serie **Linee Guida Funzioni Crittografiche** dedicato alle funzioni di hash per la definizione di queste proprietà e delle funzioni di hash considerate sicure.
Al fine di ottenere cifrari e firme post-quantum, si sfrutta l'applicazione ricorsiva di funzioni di hash per costruire una struttura ramificata chiamata **albero di Merkle** [14]. La sicurezza del sistema risultante si basa sul fatto che le funzioni di hash, come il resto della crittografia simmetrica, non vengono minacciate dall'algoritmo di Shor e che, se la funzione di hash è sicura, allora anche l'algoritmo crittografico risultante è sicuro.
I primi esempi di firme basate su funzioni di hash risalgono alla fine degli anni '70 a opera di Ralph Merkle [15], quindi questa tecnologia è abbastanza matura. Una criticità comune a molti degli algoritmi di questa famiglia è la necessità di generare molte chiavi diverse in quanto ognuna può essere utilizzata per firmare una singola volta, e si rende quindi necessario tenere traccia di quali chiavi sono già state utilizzate. Nonostante le singole chiavi siano piccole, la dimensione totale è particolarmente grande. Le caratteristiche descritte ne permettono l'applicazione a scenari in cui la generazione e conservazione di molte chiavi non influisce sull'operatività del sistema.

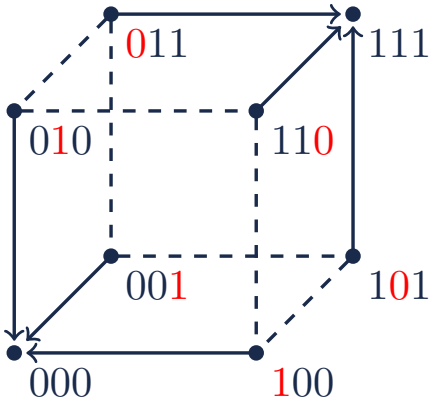

Figura 2 - Codice per correggere un errore su un singolo bit

3.1.4 Zero-Knowledge Proof (ZKP)

Le **dimostrazioni a conoscenza nulla** o **Zero-Knowledge Proof** (ZKP) sono protocolli crittografici che consentono a un utente, chiamato **prover**, di dimostrare di essere a conoscenza di un segreto rispondendo a una serie di domande poste da un altro utente, chiamato **verifier**, senza però far trapelare alcuna informazione sul segreto. Come per le funzioni di hash, questi schemi crittografici possono essere sfruttati per ottenere algoritmi di firma post-quantum. In particolare, si può applicare una tecnica introdotta da Amos Fiat e Adi Shamir [16] che consente di trasformare una procedura come una ZKP in una firma digitale.

I primi algoritmi di ZKP non risultano resistenti agli attacchi quantistici, ma negli ultimi anni sono stati sviluppati protocolli basati su codici o su primitive simmetriche, come le funzioni di hash, che risultano quindi post-quantum. Inoltre, le metodologie come quella di Fiat-Shamir sono state introdotte negli anni '80 e si tratta quindi di una tecnologia consolidata, considerata sicura se implementata correttamente. Tuttavia, a causa della quantità di informazioni necessarie per provare la conoscenza del segreto, le dimensioni delle firme risultano molto più grandi in confronto a quelle delle altre famiglie.

3.1.5 Isogenie su curve ellittiche

Come osservato precedentemente, la crittografia classica basata su curve ellittiche sfrutta la difficoltà di risoluzione del problema del logaritmo discreto su curve ellittiche e quindi anch'essa è minacciata dall'algoritmo di Shor. Tuttavia, tra le famiglie di crittosistemi post-quantum ne esiste una la cui sicurezza si basa sulle curve ellittiche ma che sfrutta un problema differente. Se si considerano particolari famiglie di curve ellittiche, dette **supersingolari**, è possibile definire delle trasformazioni tra di esse, dette **isogenie**. Date due curve supersingolari è difficile ricostruire un percorso all'interno del grafo costituito da tutte le isogenie che le collegano. Questo problema, chiamato **isogeny path problem**, è stato introdotto da Luca De Feo, David Jao e Jérôme Plût nel 2014 [17] e quindi è uno dei più recenti tra quelli alla base degli algoritmi post-quantum. Dal punto di vista delle dimensioni, gli algoritmi basati sulle isogenie hanno chiavi tra le più piccole di tutte le famiglie post-quantum, ma i tempi di computazione sono molto alti. Inoltre, essendo un problema di recente introduzione, la sua sicurezza non è stata ancora consolidata. Ne è un esempio uno dei primi sistemi di scambio di chiave basato su isogenie, chiamato **SIKE** [18]: nonostante sembrasse un valido candidato per la standardizzazione, è stato attaccato con successo nel 2022 [19] utilizzando un computer classico e di conseguenza è stato ritirato. Questo risultato è specifico per SIKE e quindi non intacca i problemi alla base della crittografia sulle isogenie.

Recentemente, sono stati proposti nuovi algoritmi di firma digitale basati sulle isogenie, che al momento sono ancora al vaglio degli esperti.

3.1.6 Sistemi di equazioni polinomiali multivariati

Un famoso problema matematico considerato difficile è la risoluzione dei sistemi di equazioni polinomiali **multivariati** definiti su campi finiti. Al momento, questo problema non sembra essere minacciato dall'avvento dei computer quantistici ed è stato quindi utilizzato per la definizione di alcuni algoritmi di firma digitale. Infatti, se una firma di un dato messaggio corrisponde a una soluzione del sistema multivariato e il messaggio ai suoi termini noti, allora chi è a conoscenza di tale firma riesce a verificare rapidamente che essa consente la risoluzione del sistema e di conseguenza rappresenta una firma valida per il messaggio. L'obiettivo degli schemi di questo tipo è quindi rendere semplice per il mittente risolvere il sistema, costruendo una cosiddetta **trapdoor**, in modo che sia molto difficile per chiunque non sia in possesso di tutti i parametri trovare una soluzione del sistema.

Le prime idee di schemi crittografici basati su questo problema risalgono agli anni '80 [20], ma solamente alla fine degli anni '90 sono stati raggiunti sviluppi concreti su questo argomento [21]. Va tuttavia segnalato che l'algoritmo **Rainbow** [22], uno dei candidati a diventare nuovo standard di firma post-quantum, è stato attaccato con successo [23] da un computer classico e dichiarato quindi non idoneo a essere standardizzato. Questo attacco non inficia la sicurezza di tutti gli algoritmi sui sistemi multivariati, ma occorre porre particolare attenzione in fase di creazione di un cifrario di questo tipo. Rispetto alle altre famiglie di algoritmi post-quantum, quelli basati su sistemi multivariati hanno chiavi di grandi dimensioni ma firme ridotte, mentre le prestazioni sono nella media.

3.1.7 MPC-in-the-Head

Una delle più moderne famiglie di crittosistemi post-quantum basa la propria sicurezza sulla tecnica di crittografia classica chiamata **Multi-Party Computation** (MPC). Questi protocolli consentono a un gruppo di utenti, ognuno a conoscenza di un proprio segreto personale, di ricavare un segreto condiviso tra tutti i partecipanti qualora un numero sufficiente di essi sia concorde nel recuperarlo, facendo in modo che non sia possibile ricavare informazioni sui dati personali dei singoli utenti.
Come già visto per i sistemi basati su ZKP, l'idea alla base è quella di sfruttare un protocollo che prevede la conoscenza di un segreto senza svelarlo o utilizzarlo, ma in questo caso nessuna delle parti può utilizzare il proprio segreto per accedere al segreto comune se non in cooperazione con gli altri partecipanti.
La famiglia di sistemi crittografici post-quantum è stata chiamata **MPC-in-the-Head**, in quanto l'utente con il segreto parte da uno schema MPC dal quale costruisce un protocollo ZKP. A questo punto, la sicurezza del sistema si riconduce a quella della ZKP, che a sua volta si riconduce a problemi su codici o funzioni di hash. Tuttavia, gli algoritmi della famiglia MPC-in-the-Head sono molto giovani essendo stati introdotti nel 2007 [24], e quindi necessitano ancora molto studio da parte della comunità scientifica per confermarne l'affidabilità. Al momento sono molte le proposte di sistemi che sfruttano questa struttura, anche per via dell'adattabilità a piccoli dispositivi dovuta ai bassi requisiti computazionali. Dal punto di vista della dimensione dei dati, le firme sono grandi mentre le chiavi sono tra le più piccole rispetto alle altre alternative.

3.2 Processo di standardizzazione NIST

La spinta più importante alla crittografia post-quantum è sicuramente arrivata dal processo indetto dal NIST statunitense per la **standardizzazione** di algoritmi post-quantum. Questa competizione pubblica, iniziata nel 2016 [25], ha raccolto e studiato le principali alternative presenti al fine di selezionare dei crittosistemi a chiave pubblica resistenti ad attacchi quantistici, suddivisi in Key Encapsulation Mechanisms (KEM) e firme digitali.
Nel 2022, dopo 3 round di selezione, sono stati annunciati i primi quattro standard [26]: un algoritmo KEM, chiamato **CRYSTALS-Kyber**, e tre algoritmi per la firma digitale, **CRYSTALS-Dilithium**, **SPHINCS+**, **Falcon**. Ad agosto 2023 sono state pubblicate le prime tre bozze degli standard chiamati, rispettivamente, **ML-KEM** [27], **ML-DSA** [28] e **SLH-DSA** [29]. Questi documenti sono in fase di revisione in seguito a un periodo di ricezione di commenti da parte della comunità scientifica e le versioni conclusive dovrebbero essere finalizzate entro l'estate 2024. Il documento per Falcon [30] è ancora in elaborazione, la prima bozza verrà pubblicata nell'autunno 2024.
Altri quattro algoritmi KEM sono passati a un ulteriore quarto round di valutazione: **BIKE**, **Classic McEliece**, **HQC** e **SIKE**. Come menzionato precedentemente, l'algoritmo basato sulle isogenie SIKE è stato attaccato e quindi gli stessi autori del cifrario lo hanno ritirato dalla competizione. Gli altri algoritmi sono ancora in corso di valutazione da parte della comunità scientifica. La conclusione di questo round di valutazione avverrà nell'autunno 2024 con la selezione di uno o più algoritmi da affiancare allo standard ML-KEM.
Al momento, quasi tutte le firme selezionate rientrano nella famiglia degli algoritmi basati sui reticoli. Per questa ragione, il NIST ha lanciato una **seconda competizione** nel 2022 [31], con l'obiettivo di raccogliere nuove proposte di firme digitali post-quantum. La scadenza per la presentazione dei crittosistemi era il 30 giugno 2023 e sono pervenute 40 proposte che, attualmente, si trovano al primo round di valutazione. Alcune di queste sono state attaccate e dichiarate insicure, mentre altre hanno ricevuto aggiornamenti da parte dei proponenti: per avere una maggiore certezza della sicurezza di questi algoritmi sarà necessario attendere che il loro studio sia più maturo. La conclusione del primo round di valutazione dovrebbe avvenire nell'estate 2024.

3.3 Le tecniche di ibridazione post-quantum

I problemi alla base degli algoritmi post-quantum sono relativamente nuovi nel mondo della crittografia. Per questo e per agevolare una transizione sicura dagli algoritmi classici a quelli post-quantum, sono stati ideati dei **crittosistemi post-quantum ibridi**, che uniscono l'utilizzo di un cifrario classico e a quello di uno post-quantum. I due algoritmi possono essere combinati in diversi modi, dando vita a diversi metodi di ibridazione.
Queste tecniche permettono di beneficiare della sicurezza di

entrambi i cifrari, risultando quindi utili nella prima fase di dismissione degli algoritmi classici per consentire alla comunità scientifica di continuare ad analizzare più a fondo i nuovi cifrari post-quantum proteggendo, allo stesso tempo, i dati da possibili attacchi, anche quantistici. In questo caso, se un computer quantistico dovesse rompere l'algoritmo di crittografia classica, allora il sistema rimarrebbe sicuro perché protetto dall'algoritmo post-quantum; viceversa, se comparisse un attacco in grado di rompere l'algoritmo post-quantum, allora il sistema manterrebbe la sicurezza dell'algoritmo di cifratura classico. Considerando inoltre che gli algoritmi post-quantum solitamente hanno prestazioni molto peggiori rispetto a quelli classici, il costo aggiuntivo nell'adoperare una tecnica ibrida invece del solo algoritmo post-quantum è trascurabile e sicuramente ragionevole. Dal punto di vista tecnico, le specifiche ETSI [32] propongono di applicare una **Key Derivation Function** (KDF) a un valore segreto per generare una coppia di chiavi per l'algoritmo post-quantum e una coppia per l'algoritmo classico. Una volta generate le corrispondenti cifrature/firme, queste possono essere combinate in modi diversi e il destinatario si occuperà di decifrarle singolarmente utilizzando le chiavi appropriate. Nelle specifiche vengono descritti due schemi per lo scambio di chiavi ibride, **Concatenate KDF** e **Cascade KDF**, che sono stati proposti per l'utilizzo con i sistemi post-quantum.

4 La crittografia quantistica

Prima dell'avvento della crittografia post-quantum, la meccanica quantistica era già stata coinvolta nella definizione di nuovi algoritmi crittografici, dando vita alla cosiddetta **crittografia quantistica**. Questa branca sfrutta i principi intrinseci della meccanica quantistica, come il principio di indeterminazione di Heisenberg, per garantire la sicurezza di sistemi crittografici dedicati.

L'applicazione più conosciuta e diffusa degli algoritmi crittografici quantistici riguarda i metodi di **distribuzione della chiave** o **Quantum Key Distribution** (QKD). Il primo algoritmo di questo tipo fu ideato nel 1984 ed è conosciuto come **BB84** [33]. Questi metodi crittografici utilizzano un cavo di fibra ottica o canali satellitari per inviare dati codificati come fotoni polarizzati. La loro sicurezza è garantita dal fatto che, grazie ai principi della fisica quantistica, cercare di ottenere illecitamente i dati in fase di scambio modifica immediatamente e irreparabilmente gli stati quantistici a essi associati e quindi ogni intrusione malevola può essere rilevata dai legittimi interlocutori.

Pur garantendo una sicurezza certificata dalla validità di comprovate leggi fisiche, la crittografia quantistica presenta varie problematiche:

- per resistere ad attacchi del tipo man-in-the-middle, il segreto inviato tramite QKD deve essere autenticato, e questa pratica utilizza a sua volta un segreto condiviso inizialmente. Trovare una soluzione non classica che consenta di scambiarsi efficientemente questo segreto è ancora un problema aperto;
- per questioni tecniche, la massima distanza supportata ad oggi da questa tecnologia è dell'ordine del centinaio di chilometri. Per permettere la comunicazione a distanze maggiori, è necessario inserire lungo la linea dei ripetitori classici [34], con il vincolo che siano fidati (trusted nodes), oppure utilizzare dei ripetitori quantistici [35], la cui tecnologia non è ancora abbastanza matura per un'implementazione su larga scala;
- i fotoni, anche in transito, possono essere soggetti a cambi di polarizzazione per cause esterne. Questo aumenta le possibilità di errore nella trasmissione del messaggio;
- i costi per l'installazione delle infrastrutture necessarie sono molto elevati;
- al momento, le applicazioni sono limitate alla distribuzione della chiave, mentre in molti altri contesti, come ad esempio la firma qualificata o la posta certificata, non esiste ancora una soluzione quantistica.

5 La transizione a livello internazionale

A livello internazionale, molti stati hanno iniziato a intraprendere delle azioni in risposta alla minaccia quantistica.

5.1 La strategia statunitense

Negli USA, oltre al processo di standardizzazione del NIST, il 4 maggio 2022 il Presidente Biden ha rilasciato un memorandum [36] per la vicepresidente, alcuni capi dei dipartimenti e i direttori delle più importanti Agenzie statali, nel quale si ribadisce la centralità degli Stati Uniti nella transizione dagli algoritmi crittografici classici a quelli post-quantum. In questo documento, il Presidente espone la strategia e una lista di linee guida che dovranno essere seguite dalle varie Agenzie per il passaggio ai nuovi algoritmi. Con il termine Agenzia si intende, in questo caso, ogni dipartimento esecutivo, dipartimento militare, corporazione governativa, corporazione controllata dal Governo e ogni ramo operativo del governo.
In risposta a quanto stabilito da questo appunto presidenziale, l'ufficio per la gestione e il bilancio (OMB) ha redatto un memorandum il 18 novembre 2022 [37] in cui affronta in maniera dettagliata alcuni dei punti di sua competenza per guidare la transizione verso gli algoritmi post-quantum. Entro il 4 maggio 2023, a un anno dall'appunto del Presidente, tutte le Agenzie hanno dovuto inviare all'OMB un inventario dei sistemi e degli asset contenenti sistemi crittografici vulnerabili agli attacchi quantistici. A maggio 2024 è stato inoltre stilato un secondo inventario riguardante le previsioni sui costi per la transizione dei sistemi crittografici interessati.
A conclusione e validazione di questo procedimento, il Governo statunitense ha approvato in data 21 dicembre 2022 la Public Law 117-260 contenente il "Quantum Computing Cybersecurity Preparedness Act" [38], nel quale vengono ribaditi e resi effettivi gli appunti precedenti, ribadendo l'importanza e l'urgenza di attivare le procedure di migrazione agli algoritmi post-quantum, con l'obiettivo di terminarla entro il 2035.

5.2 Gli sviluppi asiatici

Nel continente asiatico vari paesi si sono mossi per provvedere alla minaccia quantistica, sia cercando di validare degli standard post-quantum propri, comunque basati sugli stessi problemi matematici utilizzati dagli algoritmi della competizione NIST, sia testando le possibilità della crittografia quantistica.
Nel 2021, la Repubblica di Corea ha istituito un gruppo di ricerca sulla crittografia post-quantum che, prendendo spunto dalla situazione americana, ha indetto una competizione per selezionare degli standard post-quantum per la cifratura a chiave pubblica e per la firma digitale. A dicembre 2023, sono stati annunciati i risultati del primo

round, che è stato superato da 8 algoritmi, 4 per ognuna delle due categorie [39].
La Chinese Association for Cryptologic Research (CACR) ha anch'essa indetto nel 2018 una competizione per la standardizzazione post-quantum [40] e ha annunciato i vincitori nel 2020 [41]: due algoritmi per la cifratura, chiamati **LAC.PKE** [42] e **Aigis-enc** [43], e uno per la firma digitale, **Aigis-sig** [43], tutti basati sul problema LWE. Allo stesso tempo, la Cina è una delle nazioni più fortemente attive nel campo della crittografia quantistica. In particolare, nel 2011 il National Space Science Center della Chinese Academy of Science ha iniziato lo "Strategic Priority Programme on Space Science" [44] che comprende tra gli obiettivi principali l'effettuare esperimenti su scala globale riguardanti i fenomeni quantistici dell'entanglement e del trasporto quantistico e lo sviluppo di una rete di comunicazione quantistica ad ampio raggio. Uno dei principali traguardi del programma è stato raggiunto dal progetto **Quantum Experiments at Space Scale** (QUESS): nel 2016 è stato lanciato in orbita il primo satellite quantistico [45], soprannominato **Micius**, che ha permesso di applicare metodi di QKD tra satellite e stazioni a terra. Nel 2021, la Cina ha annunciato di aver ottenuto la prima rete di comunicazione quantistica sfruttando fibre ottiche, ripetitori classici e due collegamenti terra-satellite [46].
La Russia ha istituito la commissione tecnica TC26 per la standardizzazione crittografica e dei meccanismi di sicurezza [47] all'interno della quale è stato creato il "Working Group 2.5 – Post-Quantum Cryptographic Mechanisms" nel 2019 [48]. Il gruppo, in collaborazione con il gruppo di aziende **Kryptonit**, ha già sviluppato numerose alternative post-quantum, molte delle quali sono simili agli algoritmi che hanno preso parte alle competizioni NIST, ma nessun algoritmo è ancora stato standardizzato al momento. Dal punto di vista della crittografia quantistica, nel 2023 la Russia ha collaborato con la rete di comunicazione quantistica cinese, effettuando una comunicazione quantistica tra due stazioni terresti a 3800 chilometri di distanza [49].

5.3 La situazione nell'Unione Europea

Per quanto riguarda la scelta degli algoritmi post-quantum da utilizzare, gli stati dell'Unione Europea intendono seguire la linea dettata dalla competizione del NIST. Questa decisione è dovuta in parte al fatto che i ricercatori europei hanno partecipato attivamente alla gara, proponendo nuovi algoritmi e fornendo commenti durante le varie fasi di valutazione; inoltre, scegliere algoritmi comuni tra vari stati europei renderebbe più semplice il processo di transizione.
Al momento, sono stati istituiti diversi gruppi di lavoro all'interno di alcuni enti europei, come l'European Union Agency For Cybersecurity (ENISA) e l'European Telecommunications Standards Institute (ETSI), ma questi si occupano principalmente della standardizzazione di una corretta implementazione degli algoritmi post-quantum.
In parallelo, la Commissione Europea ha bandito diversi concorsi per programmi come **Horizon Europe** e **Digital Europe Programme** finalizzati allo studio e gestione della transizione a sistemi crittografici resistenti ad attacchi quantistici. Tra questi si possono trovare:

- Transition towards Quantum-Resistant Cryptography (HORIZON-CL3-2022-CS-01-03);
- Post-quantum cryptography transition (HORIZON-CL3-2024-CS-01-02);
- Standardisation and awareness of the European transition to post-quantum cryptography (DIGITAL-ECCC-2024-DEPLOY-CYBER-06-STANDARDPQC);
- Roadmap for the transition of European public administrations to a post-quantum cryptography era (DIGITAL-ECCC-2024-DEPLOY-CYBER-06-TRANSITIONEUPQC);
- Deployment of Post Quantum Cryptography in systems in industrial sectors (DIGITAL-ECCC-2024-DEPLOY-CYBER-06-PQCINDUSTRY).

Inoltre, la Commissione Europea si è attivata anche nell'ambito della crittografia quantistica dirigendo i lavori di costruzione della **European Quantum Communication Infrastructure** (EuroQCI) [50], un progetto lanciato nel 2019 con l'obiettivo di instaurare entro il 2030 una rete di comunicazione quantistica che sfrutta sia fibre ottiche sia collegamenti con satelliti. La prima fase di implementazione della parte terrestre è iniziata nel 2023 con il supporto del Digital Europe Programme, mentre il lancio del primo satellite è previsto tra il 2025 e il 2026.
Il considerevole numero di iniziative dedicate alla crittografia resistente ad attacchi quantistici sottolinea l'urgenza dell'aggiornamento dei sistemi di sicurezza, sia a livello europeo che a livello nazionale. Al fine di aumentare

la consapevolezza sull'argomento e aprire la strada ai processi di transizione, le agenzie di cybersicurezza di molti stati europei hanno pubblicato report sull'argomento. Tra i documenti principali si possono trovare quelli di BSI (Germania) [51], NCSC (Regno Unito) [52], ANSSI (Francia) [53], AIVD (Olanda) [54] e CCN (Spagna) [55]. In generale, l'approccio comune prevede l'utilizzo di algoritmi riconosciuti sicuri dalla comunità scientifica, per la maggior parte risultanti dalla competizione del NIST ma tenendo in considerazione anche eventuali algoritmi scartati per troppa somiglianza con altri ritenuti più validi. Allo stesso modo, per la strategia di transizione si intende iniziare al più presto il processo di identificazione e sostituzione degli algoritmi classici, cercando di uniformare il più possibile le scelte tra i vari Paesi Europei in modo da rendere più semplici le interazioni a livello internazionale.

In risposta a questa richiesta di unificazione e coordinamento delle iniziative europee, la Commissione Europea ha pubblicato una raccomandazione l'11 aprile 2024 [56], in cui si raccomanda la formazione di un sottogruppo, composto dai rappresentanti delle agenzie nazionali per la sicurezza, esperti in materia di cybersicurezza e in collaborazione con ENISA, che si occupi di coordinare la transizione verso algoritmi crittografici post-quantum. L'obiettivo di questo sottogruppo è quello di pubblicare, entro aprile 2026, una tabella di marcia per l'attuazione coordinata della crittografia post-quantum. In seguito alla pubblicazione di questo documento, i singoli Stati membri elaboreranno dei piani di transizione conformi ai principi stabiliti dal sottogruppo.

6 Conclusioni

La minaccia portata dall'avvento dei computer quantistici ai cifrari a chiave pubblica ha dato il via alla ricerca di nuove soluzioni crittografiche per sostituire gli algoritmi classici. Da una parte, il NIST sta tenendo una competizione per la ricerca di nuovi standard crittografici post-quantum, ossia in grado di resistere ad attacchi classici e quantistici. La gara, ancora in corso, ha già scelto alcuni standard per lo scambio di chiave e la firma digitale, ma altri algoritmi sono in corso di valutazione e altri ancora devono ancora essere valutati a fondo. Tuttavia, in generale, questi nuovi algoritmi sono più lenti oppure richiedono una memoria maggiore rispetto ai crittosistemi attuali. Inoltre, si prevede una prima fase di adozione ibrida durante la quale algoritmi classici e quantistici verranno utilizzati congiuntamente per garantire una sicurezza maggiore in questa situazione delicata. Un'alternativa possibile, ma che al momento sembra riscontrare più difficoltà dal punto di vista pratico in determinate applicazioni, è quella della crittografia quantistica, che sfrutta le proprietà della meccanica quantistica per scambiare informazioni cifrate in modo sicuro.

Alcuni stati e organizzazioni internazionali hanno già iniziato a occuparsi della minaccia quantistica e a programmare un processo di migrazione al post-quantum. Anche il nostro Paese sta avviando un iter di transizione e qualunque organizzazione utilizzi metodi crittografici dovrebbe prestare particolare attenzione a questo aspetto, in modo da continuare a mantenere sicuri i propri dati cifrati.

Bibliografia

[1] W. Diffie e M. E. Hellman. «New directions in cryptography». In: *IEEE Transactions on Information Theory* 22.6 (1976), pp. 644–654. DOI: 10.1109/TIT.1976.1055638.

[2] R. P. Feynman. «Simulating Physics with Computers». In: *International Journal of Theoretical Physics* 21.6 (1982), pp. 467–488. DOI: 10.1007/BF02650179.

[3] NIST. *Advanced Encryption Standard (AES)*. FIPS 197. U.S. Department of Commerce, 2023. DOI: 10.6028/NIST.FIPS.197-upd1.

[4] SOG-IS. *Agreed Cryptographic Mechanisms, Version 1.3*. 2023. URL: https://www.sogis.eu/documents/cc/crypto/obsolete/SOGIS-Agreed-Cryptographic-Mechanisms-1.3.pdf.

[5] L. K. Grover. «A fast quantum mechanical algorithm for database search». In: *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*. STOC '96. 1996, pp. 212–219. DOI: 10.1145/237814.237866.

[6] E. Barker et al. *Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography*. SP 800-56A. NIST, 2018. DOI: 10.6028/NIST.SP.800-56Ar3.

[7] NIST. *Digital Signature Standard (DSS)*. FIPS 186-5. U.S. Department of Commerce, 2023. DOI: 10.6028/NIST.FIPS.186-5.

[8] R. L. Rivest, A. Shamir e L. Adleman. «A method for obtaining digital signatures and public-key cryptosystems». In: *Communications of the ACM* 21.2 (1978), pp. 120–126. DOI: 10.1145/359340.359342.

[9] P. W. Shor. «Algorithms for quantum computation: discrete logarithms and factoring». In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700.

[10] E. Barker. *Recommendation for Key Management: Part 1 - General*. SP 800-57. NIST, 2020. DOI: doi.org/10.6028/NIST.SP.800-57pt1r5.

[11] J. Hoffstein, J. Pipher e J. H. Silverman. «NTRU: A ring-based public key cryptosystem». In: *Algorithmic Number Theory*. 1998, pp. 267–288. DOI: 10.1007/BFb0054868.

Bibliografia

[12] M. Ajtai. «Generating hard instances of lattice problems (extended abstract)». In: *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*. STOC '96. 1996, pp. 99–108. DOI: 10.1145/237814.237838.

[13] R. J. McEliece. *A Public-Key Cryptosystem Based On Algebraic Coding Theory*. DSN PR 42-44. NASA, 1978, pp. 114–116. URL: https://tda.jpl.nasa.gov/progress_report/42-44/44N.PDF.

[14] R. C. Merkle. «A Digital Signature Based on a Conventional Encryption Function». In: *Advances in Cryptology - CRYPTO '87*. Lecture Notes in Computer Science. 1988, pp. 369–378. DOI: 10.1007/3-540-48184-2_32.

[15] R. C. Merkle. *Secrecy, authentication, and public key systems*. Stanford University, 1979. URL: http://www.ralphmerkle.com/papers/Thesis1979.pdf.

[16] A. Fiat e A. Shamir. «How To Prove Yourself: Practical Solutions to Identification and Signature Problems». In: *Advances in Cryptology - CRYPTO '86*. Lecture Notes in Computer Science. 1987, pp. 186–194. DOI: 10.1007/3-540-47721-7_12.

[17] D. Jao, L. De Feo e J. Plût. «Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies». In: *Journal of Mathematical Cryptology* 8.3 (2014), pp. 209–247. DOI: 10.1515/jmc-2012-0015.

[18] C. Costello et al. *Supersingular Isogeny Key Encapsulation*. NIST submission. 2022. URL: https://csrc.nist.gov/csrc/media/Projects/post-quantum-cryptography/documents/round-4/submissions/SIKE-spec.pdf.

[19] W. Castryck e T. Decru. «An Efficient Key Recovery Attack on SIDH». In: *Advances in Cryptology - EUROCRYPT 2023*. Lecture Notes in Computer Science. 2023, pp. 423–447. DOI: 10.1007/978-3-031-30589-4_15.

[20] T. Matsumoto e H. Imai. «Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption». In: *Advances in Cryptology - EUROCRYPT '88*. Lecture Notes in Computer Science. 1988, pp. 419–453. DOI: 10.1007/3-540-45961-8_39.

[21] A. Kipnis, J. Patarin e L. Goubin. «Unbalanced Oil and Vinegar Signature Schemes». In: *Advances in Cryptology - EUROCRYPT '99*. Lecture Notes in Computer Science. 1999, pp. 206–222. DOI: 10.1007/3-540-48910-X_15.

Bibliografia

[22] J. Ding e D. Schmidt. «Rainbow, a New Multivariable Polynomial Signature Scheme». In: *Applied Cryptography and Network Security*. Lecture Notes in Computer Science. 2005, pp. 164–175. DOI: 10.1007/11496137_12.

[23] W. Beullens. «Breaking Rainbow Takes a Weekend on a Laptop». In: *Advances in Cryptology - CRYPTO 2022*. Lecture Notes in Computer Science. 2022, pp. 464–479. DOI: 10.1007/978-3-031-15979-4_16.

[24] Y. Ishai et al. «Zero-knowledge from secure multiparty computation». In: *Proceedings of the Thirty-Ninth Annual ACM Symposium on Theory of Computing*. STOC '07. 2007, pp. 21–30. DOI: 10.1145/1250790.1250794.

[25] NIST. *Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process*. 2016. URL: https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf.

[26] NIST. *PQC Standardization Process: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates*. 2022. URL: https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4.

[27] NIST. *Module-Lattice-Based Key-Encapsulation Mechanism Standard*. FIPS 203. U.S. Department of Commerce, 2023. DOI: 10.6028/NIST.FIPS.203.ipd.

[28] NIST. *Module-Lattice-Based Digital Signature Standard*. FIPS 204. U.S. Department of Commerce, 2023. DOI: 10.6028/NIST.FIPS.204.ipd.

[29] NIST. *Stateless Hash-Based Digital Signature Standard*. FIPS 205. U.S. Department of Commerce, 2023. DOI: 10.6028/NIST.FIPS.205.ipd.

[30] P.-A. Fouque et al. *Supersingular Isogeny Key Encapsulation*. NIST submission. 2020. URL: https://falcon-sign.info/falcon.pdf.

[31] NIST. *Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process*. 2022. URL: https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/call-for-proposals-dig-sig-sept-2022.pdf.

Bibliografia

[32] ETSI. *CYBER; Quantum-safe Hybrid Key Exchanges, Version 1.1.1*. TS 103 744. 2020. URL: https://www.etsi.org/deliver/etsi_ts/103700_103799/103744/01.01.01_60/ts_103744v010101p.pdf.

[33] C. H. Bennett e G. Brassard. «Quantum cryptography: Public key distribution and coin tossing». In: *Theoretical Computer Science* 560 (2014), pp. 7–11. DOI: 10.1016/j.tcs.2014.05.025.

[34] L. Salvail et al. «Security of Trusted Repeater Quantum Key Distribution Networks». In: *Journal of Computer Security* 18.1 (2010), pp. 61–87. DOI: 10.3233/JCS-2010-0373.

[35] K. Azuma et al. «Quantum repeaters: From quantum networks to the quantum internet». In: *Reviews of Modern Physics* 95.4 (2023). DOI: 10.1103/revmodphys.95.045006.

[36] J. R. J. Biden. *National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems*. NSM-10. 2022. URL: https://irp.fas.org/offdocs/nsm/nsm-10.pdf.

[37] S. D. Young. *Migrating to Post-Quantum Cryptography*. M-23-02. 2022. URL: https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf.

[38] U. S. Congress. *Quantum Computing Cybersecurity Preparedness Act*. Public Law 117-260. 2022. URL: https://www.govinfo.gov/content/pkg/PLAW-117publ260/pdf/PLAW-117publ260.pdf.

[39] Korean post-quantum Cryptography. *Selected Algorithms from the KpqC Competition Round 1*. 2023. URL: https://www.kpqc.or.kr/competition.html.

[40] CACR. *Avviso per l'indizione di un concorso nazionale per la progettazione di algoritmi crittografici*. 2018. URL: https://www.cacrnet.org.cn/site/content/259.html.

[41] CACR. *Annuncio dei risultati della selezione dell'algortimo del Consorzio Nazionale di Progettazione di Algoritmi Crittografici*. 2020. URL: https://www.cacrnet.org.cn/site/content/854.html.

[42] X. Lu et al. *LAC: Practical Ring-LWE Based Public-Key Encryption with Byte-Level Modulus*. IACR Cryptology ePrint Archive. 2018. URL: https://eprint.iacr.org/2018/1009.pdf.

Bibliografia

[43] J. Zhang et al. «Tweaking the Asymmetry of Asymmetric-Key Cryptography on Lattices: KEMs and Signatures of Smaller Sizes». In: *Public-Key Cryptography - PKC 2020*. Lecture Notes in Computer Science. 2020, pp. 37–65. DOI: 10.1007/978-3-030-45388-6_2.

[44] NSSC-CAS. *Projects of Quantum Science Satellite and Dark Matter Satellite Kicked off*. 2011. URL: http://english.cssar.cas.cn/ns/NU/201112/t20111231_80542.html.

[45] NSSC-CAS. *China launches first-ever quantum communication satellite*. 2016. URL: http://english.cssar.cas.cn/ns/headline/201608/t20160818_166576.html.

[46] Y.-A. Chen et al. «An integrated space-to-ground quantum communication network over 4,600 kilometres». In: *Nature* 589 (2021), pp. 214–219. DOI: 10.1038/s41586-020-03093-8.

[47] TC26. *Technical Committee for standardization "Cryptography and security mechanisms"*. [Consultato: Giugno 2024]. URL: https://tc26.ru/en/.

[48] TADVISER. *Post-quantum cryptography*. 2023. URL: https://tadviser.com/index.php/Article:Post-quantum_cryptography.

[49] TADVISER. *Quantum cryptography/encryption*. 2023. URL: https://tadviser.com/index.php/Article:Quantum_cryptography_(encryption).

[50] Commissione Europea. *Iniziativa per l'infrastruttura europea di comunicazione quantistica (EuroQCI)*. 2024. URL: https://digital-strategy.ec.europa.eu/it/policies/european-quantum-communication-infrastructure-euroqci.

[51] BSI. *Migration zu Post-Quanten-Kryptografie*. 2020. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Post-Quanten-Kryptografie.pdf.

[52] NCSC. *Preparing for Quantum-Safe Cryptography*. 2020. URL: https://www.ncsc.gov.uk/pdfs/whitepaper/preparing-for-quantum-safe-cryptography.pdf.

Bibliografia

[53] ANSSI. *Avis de l'ANSSI sur la migration vers la cryptographie post-quantique*. 2023. URL: https://cyber.gouv.fr/publications/avis-de-lanssi-sur-la-migration-vers-la-cryptographie-post-quantique-0.

[54] AIVD. *Het PQC-migratie handboek*. 2023. URL: https://www.aivd.nl/documenten/publicaties/2023/04/04/pqc-migratie-handboek.

[55] CCN-CERT. *Recomendaciones para una transición postcuántica segura de CCN-PYTEC*. 2022. URL: https://www.ccn-cert.cni.es/es/seguridad-al-dia/novedades-ccn-cert/12234-recomendaciones-para-una-transicion-postcuantica-segura-de-ccn-pytec.html.

[56] Commissione Europea. *Raccomandazione (UE) 2024/1101 della Commissione, dell'11 aprile 2024, relativa a una tabella di marcia per l'attuazione coordinata della transizione verso la crittografia post-quantistica*. 2024. URL: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:L_202401101.