UNIVERSITÀ
DEGLI STUDI
DI BRESCIA

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

Corso di Laurea Magistrale
in Ingegneria Informatica

Elaborato di Sicurezza Informatica

Stato dei lavori normativi riguardanti algoritmi post quantum resistant a chiave pubblica

Docente:
Prof. Federico Cerutti

Studente:
Francesco Rossi 706086

Anno Accademico 2021/2022

Abstract

La computazione quantistica è ormai alle porte, ed è noto che renderà insicura parte della crittografia attuale. Sebbene la tempistica esatta della "minaccia" quantica non sia, e non possa essere nota con esattezza, le organizzazioni sono concentrate sulla ricerca e normazione di nuove alternative crittografiche con l'obiettivo di renderle disponibili il prima possibile. Lo scopo di questo elaborato è quello di fornire a un utente finale informazioni riguardanti lo stato attuale dei lavori di normazione degli algoritmi (classici) a chiave pubblica cosi detti quantum resistant. Inizialmente, vengono introdotti i risultati degli algoritmi quantistici di Grover e Shor in grado di mettere in difficoltà i sistemi crittografici attuali. Successivamente verranno presentati i risultati attuali dei lavori di normazione dei principali enti competenti, quali: NIST, IETF, ETSI, ISO, IEEE. Infine, verranno discussi i risultati in una chiave più ampia: di come il NIST sia l'organizzazione che sta producendo i maggiori risultati, e di come alcune fonti identifichino l'intervallo minimo più probabile 2035-2040 nel quale un computer quantistico rilevante possa essere reso disponibile.

Contents

1 Introduzione

Le tecnologie crittografiche sono utilizzate da qualsiasi governo, industria ed utente per autenticare le sorgenti, proteggere la confidenzialità e l'integrità delle informazioni che comunichiamo e manteniamo attraverso i dispositivi. Queste tecnologie includono un ampio range di protocolli, ma tutti sono basati su un numero ristretto di algoritmi crittografici. Gli algoritmi crittografici sono funzioni matematiche che trasformano i dati tramite un processo e delle variabili, alcune di esse identificate con il termine *chiavi*. Le chiavi devono rimanere segrete ai fini della sicurezza, chiunque conosce la chiave può entrare in possesso dei dati.

Tali algoritmi si dividono tra simmetrici e asimmetrici: con il termine simmetrici si identificano quegli algoritmi attraverso i quali è possibile cifrare e decifrare i dati con la stessa chiave. Con il termine asimmetrico invece si hanno 2 diverse chiavi, una pubblica ed una privata per svolgere le 2 operazioni di cifratura e decifratura separatamente. Per facilitare l'utilizzo e garantire livelli di sicurezza e prestazioni elevati gli algoritmi vengono classificati e raccolti attraverso degli *standard*. Prendendo come riferimento il Nist[1], gli standard crittografici riguardanti gli algoritmi simmetrici ed asimmetrici attualmente in uso sono presentati in figura 1: "Public key based" è la categoria che raccoglie gli standard degli algoritmi di firma digitale e "key estabilishment" cioè gli algoritmi per effettuare procedure di scambio chiavi tra le parti. La categoria "Symmetric key based" è la categoria che raccoglie gli algoritmi simmetrici e funzioni hash.

Con l'avvento della computazione quantistica questi standard non saranno più in grado di garantire lo stesso livello di sicurezza dei dati e delle comunicazioni: dalla letteratura si è già a conoscenza di 2 particolari algoritmi che sfruttando la computazione quantistica sono in grado di mettere in difficoltà gli standard attutali: l'algoritmo di Grover [2] e l'algoritmo di Shor [3].

L'algoritmo di *Grover* [2], è un algoritmo ideato da Lov Grover nel 1996 per risolvere un problema di ricerca in un database non ordinato di N elementi in un tempo di $O(N^{1/2})$. Applicando l'algoritmo di Grover nel campo crittografico, è possibile attaccare gli algoritmi simmetrici: si consideri l'algoritmo di cifratura AES (Advanced Encrytption Standard) con chiave crittografica k di lunghezza 128 bit e si assuma che un attaccante conosca alcune coppie testo in chiaro testo cifrato e che voglia trovare la chiave, a partire dal testo in chiaro si ottiene il testo cifrato corrispondente e viceversa. A oggi non si conosce un attacco nettamente migliore di una ricerca esaustiva per individuare la chiave. La ricerca esaustiva richiederebbe circa 2^{128} tentativi per ricavare k, mentre nel caso quantistico, circa 2^{64} volte con

[1] https://www.nist.gov/

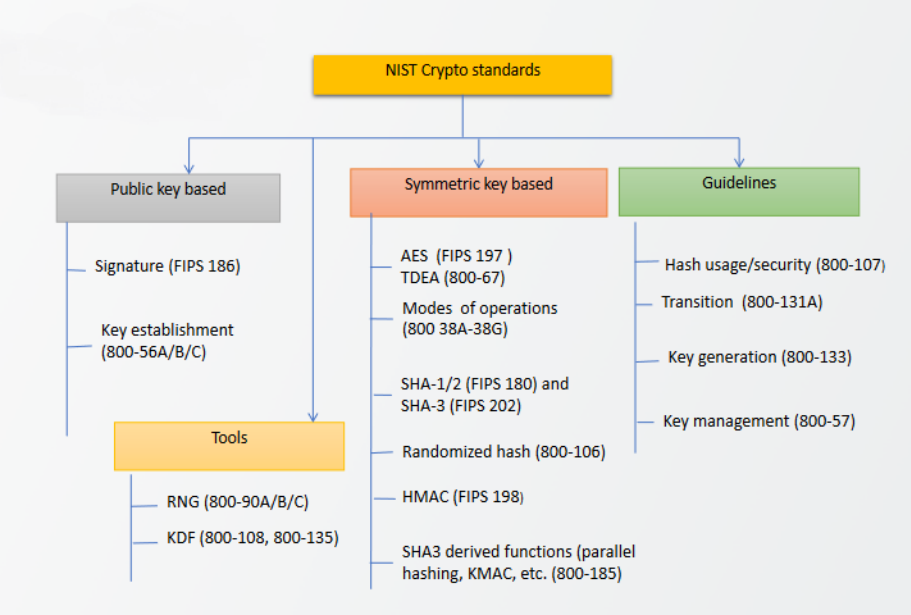

Figure 1: Standard di riferimento attuali rilasciati dal Nist, *"Public key based"* è la categoria che raccoglie gli standard target dell'algoritmo di Shor e non più sicuri in un prossimo futuro. La categoria *Symmetric key based* è la categoria di standard attaccabile dall'algoritmo di Grover, senza però comprometterne la totale sicurezza. [1] p. 3

probabilità di successo molto vicina ad 1. In generale si può affermare che l'algoritmo di Grover è in grado di "dimezzare" la sicurezza di un sistema simmetrico. Per mitigarne gli effetti è sufficiente raddoppiare la lunghezza della chiave crittografica utilizzata.

L'algoritmo di *Shor [3]* è un algoritmo ideato da Peter Shor nel 1994 per risolvere il problema della fattorizzazione dei numeri interi in numeri primi. Questo comporta un problema per l'intera crittografia a chiave pubblica: tramite l'algoritmo di Shor è possibile risolvere i problemi crittografici alla base degli algoritmi in un tempo polinomiale, o meglio, BQP (Bounded error Quantum Polynomial time): i fattori sono trovati con margine d'errore arbitrariamente piccolo in tempo polinomiale nella lunghezza dell'intero di input. Non esiste nessuna mitigazione a questo genere di attacco, l'unica soluzione è quella di abbandonare gli standard attuali in favore di standard basati su algoritmi quantum resistant, cioè famiglie di algoritmi crittografici costruiti su problemi matematici diversi, sui quali l'algoritmo di Shor non risulta efficace.

Al momento non esiste nessun computer quantistico, con sufficiente potenza di calcolo, in grado di eseguire i 2 algoritmi menzionati per attaccare gli standard crittografici attuali compromettendone la sicurezza, ma in un prossimo futuro è molto probabile che ciò accada, e sarà necessario arrivare pronti: Molti enti di normazione internazionale sono già al lavoro per identificare, analizzare e normare quelli che saranno i nuovi algoritmi alla base dei nuovi standard crittografici post quantistici. Lo stato dei lavori verrà illustrato nel paragrafo 2. Sono stati presi in considerazione come riferimento di questa indagine gli enti: NIST, ETSI, IETF, IEEE, ISO. Nel paragrafo 3 verrà discusso lo stato di questi lavori: discutendo chi sta producendo i maggiori risultati e se gli sforzi in atto sono adeguati anche in relazione alle tempistiche in cui la minaccia quantistica potrebbe diventare reale.

2 Stato dei lavori normativi

2.1 NIST

Il National Institute of Standards and Technology[2] (NIST), è un agenzia americana non regolatoria che fa parte del dipartimento del commercio. In generale la missione del Nist è quella di promuovere l'innovazione e la competitività industriale degli Stati Uniti facendo progredire la scienza, gli standard in modo da migliorare la sicurezza economica e la qualità della vita. Per quanto concerne l'ambito informatico e crittografico i tipi di risorse che deliberano vengono identificate come: *Federal Information Processing Standards* (FIPS) e *Special Publications* (SP). In ambito crittografia post quantum, il NIST ha svolto e sta svolgendo le seguenti attività:

- Nel 2016 viene pubblicato un report (NIST Interagency Report)[4], in cui il NIST condivide lo stato della computazione quantistica e della crittografia post quantum. Basandosi sull'impatto che le tecnologie quantistiche avrebbero sugli algoritmi, vengono identificate le sfide da affrontare per l'adozione di nuovi standard da parte d'industrie e governi.

- Nel dicembre 2016 viene annunciata la *"Call for Proposals"*, per partecipare a un processo di selezione per individuare i nuovi algoritmi a chiave pubblica quantum resistant, per la firma digitale, cifratura e per il meccanismo di incapsulamento (key encapsulation mechanisms). Il processo è basato su più round di selezione, su un periodo inizialmente stimato in 5-7 anni partito nel 2017 è tutt'ora in corso, nelle fasi finali. La chiamata iniziale ha fatto registrare un totale di 82 sottoscrizioni da 25 paesi: 23 schemi di firma e 59 schemi di cifratura/ key establishment, dei quali poi solo 69 rispettavano i requisiti di valutazione, tra questi, 5 sono stati ritirati. La figura 2 mostra gli schemi che hanno inizialmente preso parte al processo ufficiale di studio e selezione suddivisi per famiglie crittografiche.

  Nel corso dei vari round sono stati filtrati dalla lista iniziale molti algoritmi seguendo una metodologia di selezione, basata su criteri [5] che pongono come obiettivi certi livelli di sicurezza, prestazioni e usabilità. Il lavoro di studio e test degli schemi è svolto da un team interno con la partecipazione pubblica di esperti del settore, al fine di rendere il più trasparente possibile il processo di selezione. Ogni round termina con il rilascio di un report tecnico dove vengono illustrati gli algoritmi, le loro caratteristiche e le motivazioni per le quali

[2] https://www.nist.gov/

	Signatures	KEM/Encryption	Overall
Lattice-based	5	21	26
Code-based	2	17	19
Multi-variate	7	2	9
Stateless Hash or Symmetric based	3		3
Other	2	5	7
Total	**19**	**45**	**64**

Figure 2: Schemi iniziali sottoposti al NIST [1] p. 20

un algoritmo è stato scartato o selezionato per la fase successiva. Al termine dei primi 2 round sono stati rilasciati i relativi report [6][7],l'ultimo rilasciato è datato 5 luglio 2022 [8], ed è il risultato del terzo round di selezione in cui vengono annunciati i primi algoritmi che saranno standardizzati: CRYSTALS–KYBER [3] (key-establishment), CRYSTALS-Dilithium [4], FALCON [5] e SPHINCS+[6] (digital signatures), altri invece necessitano ancora di studi e sono stati rimandati ad un round successivo. Le prime bozze degli standard sono attese entro il 2024. Inoltre, nel settembre 2022 è stato rilasciato un annuncio[7] per la sottomissione di nuove proposte per i soli schemi di firma digitale, a causa delle poche alternative, con scadenza il 1 giugno 2023: l'obiettivo è quello di diversificare il porfolio di algoritmi di firma digitale, con schemi che non siano lattice-based, e per certe applicazioni con schemi che abbiano una firma corta e una verifica veloce.

- Oltre al processo di selezione in atto, il nist ha già pubblicato nell'ottobre 2020, in collaborazione con l' Internet Engineering Task Force[8] (IETF), uno standard contenente algoritmi post quantum resistant per la firma digitale: si tratta dello standard identificato come SP 800-208 [9], basato sulla famiglia di algoritmi *stateful Hash-Based*. La pubblicazione contiene 2 schemi, il *Leighton-Micali*

[3]https://pq-crystals.org/kyber/
[4]https://pq-crystals.org/dilithium/
[5]https://falcon-sign.info/
[6]https://sphincs.org/
[7]https://csrc.nist.gov/News/2022/request-additional-pqc-digital-signature-schemes
[8]https://www.ietf.org/

Signature (LMS) system [10] e l' *eXtended Merkle Signature Scheme (XMSS) [11].* La tecnologia sottostante a questi schemi è già ben compresa. In particolare, la sicurezza di uno schema HBS, è basata su delle proprietà già in uso per la sicurezza di molti algoritmi e protocolli crittografici approvati dal NIST, e non sono noti algoritmi di calcolo quantistico che rappresenterebbero una minaccia pratica nel prossimo futuro. Questi schemi non sono per l'uso generale, a causa alcuni vincoli sono più indicati per applicazioni in cui l'uso della chiave privata può essere controllato, e dove è necessario passare a uno schema di firma digitale post quantum resistant prima che il processo di standardizzazione sia completato.

Un'applicazione adatta a questo profilo è l'autenticazione degli aggiornamenti del firmware per dispositivi tipo smart devices, sensori, micro-controllori etc. Alcuni dispositivi che verranno implementati nel prossimo futuro saranno in uso per decenni. Questi dispositivi dovranno disporre di un meccanismo sicuro per la ricezione degli aggiornamenti e potrebbe non essere pratico modificare il codice per la verifica delle firme una volta che i dispositivi sono già distribuiti.

2.2 IETF-IRTF

L' Internet Engineering Task Force[9] (IETF) è una comunità internazionale aperta di designer, operatori, fornitori, e ricercatori interessati all'evoluzione di Internet, che sviluppano standard attraverso processi aperti. Il lavoro tecnico viene svolto in gruppi di lavoro, organizzati per topic attraverso varie aree di competenza. Il processo di standardizzazione segue una metodologia ben definita e documentata. In generale, l'IETF è concentrato su questioni ingegneristiche e di standardizzazione. All'interno di esso esiste un gruppo di lavoro identificato come Internet Research Task Force (IRTF) che si concentra su temi di ricerca di lungo termine inerenti all'Internet. A sua volta l'IRTF è organizzata in vari gruppi di lavoro. Il Crypto Forum Research Group (CFRG) funge da ponte tra teoria e pratica, portando nuove tecniche crittografiche alla comunità e promuovendo la comprensione dell'uso e dell'applicabilità tramite le RFC[10] informative. Dal 2016 sono stati presentati una serie di documenti classificati come "Intenret-draft" riguardanti soluzioni post-quantum safe. Alcuni sono poi evoluti in RFC e altri sono stati abbandonati. Di seguito vengono riportati i progetti attivi e a un punto più avanzato, che sono proseguiti nelle operazioni di studio e standardizzazione:

[9] https://www.ietf.org/

[10] Request for comments. Documenti contenenti specifiche tecniche e note organizzative per "l'internet". Possono poi evolversi in standard.

- **Hash-based signatures**. Sono state prodotte 2 RFC dai titoli: Leighton-Micali Hash-Based Signatures [10] datata aprile 2019 e XMSS: eXtended Merkle Signature Scheme RFC [11] datata maggio 2018. Sono le stesse RFC utilizzate dal Nist per la scrittura dei propri standard citati al punto precedente, e di conseguenza valgono le stesse considerazioni.

- **Key establishment**. E' stata rilasciata nel giugno 2020 (data dell'ultima modifica) una RFC (proposta come standard) dal titolo *Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security*[12]. Questa descrive un'estensione dell' Internet key exchange protocol IKEv2, permettendogli di essere post quantum resistant senza l'utilizzo di nuovi algoritmi, attraverso uno schema con chiave precondivisa.

2.3 ETSI

L' European Telecommunications Standards Institute [11] (ETSI), è un organizzazione di standardizzazione europea (ESO),che si occupa di telecomunicazioni, broadcasting e altre reti e servizi di comunicazione elettronici. Ha un ruolo speciale in Europa, attraverso il supporto ai regolamenti e alla legislazione europea attraverso la creazione di standard europei armonizzati. Inizialmente, l'ETSI è stato fondato per scopi europei, ma a oggi gli standard emessi sono riconosciuti in tutto il mondo. Produce un'alta varietà di standard, specifiche e report, per soddisfare obiettivi diversi. Le pubblicazioni vengono catalogate come: *ETSI Standard (ES), European Standard (EN), ETSI Guide (EG), ETSI Technical Specification* e *ETSI Technical Report (TR)*. In ambito della crittografia post quantum le attività di interesse da riportare sono le seguenti:

- Rilascio nel 2015 di un whitepaper con il titolo: *"Quantum Safe Cryptography and Security: An Introduction, Benefits, Enablers and Challenges" [13]*, discute le implicazioni in ambito di sicurezza che la computazione quantistica comporta, introduce le sfide da affrontare e la necessità di nuovi algoritmi, riportando le principali famiglie di crittosistemi: code-based, lattice-based, hash-based e multivariate-based discutendone la sicurezza e le performance.

- Nel 2015 viene creato il *Quantum-Safe Cryptography (QSC) working group*, l'obiettivo è quello di produrre una serie di raccomandazioni riguardanti primitive crittografiche e protocolli quantum safe, a livello implementativo e prestazionale, prendendo in considerazione sia lo stato attuale della ricerca sulla crittografia

[11] https://www.etsi.org/

accademica che la ricerca sugli algoritmi quantistici inerenti ai requisiti industriali per l'implementazione nel mondo reale. Tali attività non includono lo sviluppo di primitive crittografiche. All'interno del gruppo vengono svolti molti studi in ambito quantistico, i più significativi per la ricerca sono i seguenti:

- **Quantum-safe algorithmic framework (2017)**

  [14] Il report fornisce una panoramica sulla comprensione e sulle pratiche nel mondo accademico e industriale riguardanti la crittografia quantum safe. Si concentra sull'identificazione e sulla valutazione delle primitive crittografiche quantum safe, usate poi per la creazione di protocolli come ad esempio per l'autenticazione o lo scambio chiavi. Fornisce inoltre un framework di valutazione basata su una serie di criteri, ed introduce una discussione preliminare sulle dimensioni delle chiavi.

- **Case Studies and Deployment Scenarios (2017)**

  [15] La ricerca presenta una serie di casi d'uso reali per l'implementazione della crittografia quantum safe. In particolare, vengono prese in esame alcune applicazioni tipiche in cui le primitive crittografiche sono oggi utilizzate, mettendo in evidenza alcuni punti critici, evidenziando le funzionalità che potrebbero richiedere modifiche per adattarsi alla crittografia post quantum (a chiave pubblica).

- **Quantum-safe key exchanges (2017)**

  [16] Il report confronta una serie di proposte riguardanti il quantum-safe key exchange prese dalla letteratura. Viene fornita una panoramica per ogni metodo presentato, fornendo una lista di parametri e prestazioni dei test condotti. Infine, vengono fatte considerazioni di sicurezza e di implementazione.

- **Quantum-Safe Signatures (2021)**

  [17] Il documento fornisce una descrizione tecnica sugli schemi per firma digitale sottomessi al terzo round di selezione dei nuovi algoritmi post quantum indetta dal NIST.

- **Quantum-Safe Public-Key Encryption and Key Encapsulation (2021)**

  [18] Il documento fornisce una descrizione tecnica su schemi di "Public-Key Encryption (PKE)" e "Key Encapsulation Mechanisms (KEMs)" sottomessi al terzo round di selezione del processo di standardizzazione post quantum del NIST.

2.4 ISO

L'International Organization for Standardization [12] (ISO), è la più grande organizzazione internazionale per lo sviluppo di standard (SDO), con l' adesione di 167 organismi nazionali di normazione. L'ISO ha pubblicato oltre 21.000 Standard Internazionali e documenti correlati, in buona parte dei settori. I lavori sono organizzati, sulla base di organi tecnici, gerarchicamente in Comitati Tecnici (TC), Sottocomitati (SC) e Gruppi di Lavoro (WG). Nell'area della tecnologia dell'informazione, l'ISO e l'International Electrotechnical Commission (IEC), hanno creato un comitato tecnico congiunto, *ISO/IEC JTC 1 Information Technology*.

ISO/IEC JTC 1 /SC27 è una sottosezione incaricata di sviluppare standard per la protezione delle informazioni e per le Tecnologie dell'informazione e della comunicazione (ICT). Questo include metodi generici, tecniche e linee guida per affrontare gli aspetti di sicurezza e privacy. Più nello specifico nel 2015, il gruppo di lavoro WG2 che tratta "crittografia e altri meccanismi di sicurezza" è stato incaricato di svolgere un periodo di studio nell'area della crittografia post quantum, in preparazione alle attività di standardizzazione vere e proprie.

Il risultato degli studi preliminari viene pubblicato ufficialmente nel 2020: attraverso 6 documenti[13], vengono presentate le caratteristiche a livello teoretico, delle famiglie crittografiche "quantum resistant": hash-based, lattice-based, code-based, multivariate-based, isogeny-based.

[12] https://www.iso.org/home.html

[13] www.din.de/en/meta/jtc1sc27/downloads

2.5 IEEE

L'Institute of Electrical and Electronics Engineers[14] (IEEE) è un' organizzazione mondiale, formata da oltre 400.000 scienziati, professionisti e tecnici provenienti da oltre 170 paesi dedicata al progresso dell'innovazione e del miglioramento tecnologico a beneficio dell'umanità. IEEE sviluppa e contribuisce nella costruzione di tecnologie globali. In qualità di sviluppatore leader di standard di settore in un'ampia gamma di tecnologie, IEEE SA (Standard Association) guida la funzionalità, le capacità, la sicurezza e l'interoperabilità di prodotti e servizi, trasformando il modo in cui le persone vivono, lavorano e comunicano. Al momento si contano all'attivo più di 2100 standard e progetti in sviluppo.

L'*IEEE P1363* è un gruppo dedicato a progetti di standardizzazione per algoritmi a chiave pubblica tradizionali. Riguardo l'ambito post-quantum, nel 2008 viene pubblicata una specifica identificata come *IEEE 1363.1-2008* [19], basata sulla crittografia lattice-based. Vengono presentate specifiche tecniche sulla crittografia a chiave pubblica costruite su "hard problems over lattices", incluse primitive per key establishment, cifratura, autenticazione e firma digitale. Lo schema specificato in questo standard è il *NTRU*[15]. Lo standard è stato disattivato nel 2019, e a oggi non si registra nessuna attività di standardizzazione aggiuntiva.

[14] https://www.ieee.org/
[15] https://ntru.org/

3 Discussione

Sulla base della ricerca effettuata emergono alcune evidenze riguardo ai lavori di normazione in corso: come già introdotto nel paragrafo 1, l'unica soluzione efficace al "problema quantistico" è quella della ricerca di nuovi algoritmi quantum safe. Alcune già esistono, ma hanno un livello di applicabilità limitato, come lo standard SP 800-208 [9] pubblicato dal nist (basato su RFC del IETF), o come nel caso dello standard *IEEE 1363.1-2008[19]* già considerato deprecato nel 2019. Gli altri enti menzionati, ETSI e ISO, hanno rilasciato esclusivamente report di tipo investigativo e informativo, mantenendo un atteggiamento di attesa dei risultati del nist.

L' ente che sta compiendo il maggior sforzo per affrontare la minaccia quantistica in termini di crittografia classica è il NIST. Questo è evidente dal fatto che è l'unico ente impegnato nella ricerca di nuovi algoritmi, e senza questi non è possibile procedere nella attività di normazione. Dai risultati di questo lavoro dipenderanno tutti gli standard delle altre organizzazioni. Questo pone il NIST come l'ente trainante del settore. Va notato come esso sia un organo nazionale USA ma, di fatto, ha un'ampia influenza su tutte le altre organizzazioni, ponendolo come ente di riferimento internazionale. La cosa non è nuova: è lo stesso ente che ha standardizzato algoritmi quali AES[16] e le famiglie SHA[17], e questi algoritmi sono poi diventati un punto di riferimento per qualsiasi infrastruttura e applicazione. Da questo punto di vista le altre organizzazioni, specialmente le controparti europee, rimangono a guardare lasciando la competenza di questo tipo di ricerche al NIST (seppure i processi sono aperti e pubblici, sono comunque indetti e supervisionati dal NIST, che ha sempre l'ultima parola). L'approccio può essere vantaggioso perché avendo un unico ente che ricerca nuovi algoritmi è poi più facile concordarne il loro utilizzo nelle applicazioni e nei protocolli. Dall'altro lato mette gli USA in una posizione di dominio nel settore. Uno dei tentativi più noti di sviluppare un algoritmo "europeo" risale al 1992 all'interno del programma RACE[18] (Research and Development in Advanced Communications Technologies in Europe). Dal programma uscì una funzione hash nota oggi come RIPEMD[19]. Seppur standardizzato è meno diffuso delle alternative americane. Ci furono anche altri tentativi, di minore importanza, ma agli algoritmi proposti sono sempre stati preferiti quelli americani. Alla luce anche di questi episodi, è dunque sensata la posizione delle altre organizzazioni di mantenere un atteggiamento di at-

[16]Advanced Encryption Standard, algoritmo di cifratura a blocchi a chiave simmetrica.

[17]Secure Hash Algorithm, funzioni crittografiche di hash.

[18]Un programma europeo atto allo studio dell'espansione delle comunicazioni ad alta banda e dei servizi annessi.

[19]https://homes.esat.kuleuven.be/ bosselae/ripemd160.html

tesa nei confronti del NIST, piuttosto che iniziare ricerche simili.

E' interessante riportare che anche la Cina ha svolto un processo di standardizzazione simile a quello del NIST (un processo interno, riservato ai soli ricercatori cinesi in questo caso) indetto e gestito dalla *Chinese Association for Cryptologic Research (CACR)*: il processo ha avuto inizio nel 2019, con la durata di un solo anno. Alcuni degli algoritmi sottomessi sono poi stati decretati vincitori [20][21]. Il loro utilizzo molto probabilmente sarà limitato al solo territorio cinese, con la possibilità di essere standardizzati da un organo internazionale come l'ISO [22]. Il materiale riguardante la competizione è limitato e disponibile sono in lingua cinese, e non se ne trova traccia in nessun report di enti occidentali. Infine, l'intenzione ultima è quella di svolgere una seconda competizione aperta a tutti i paesi [23].

Un'altra cosa che si può notare è che intorno al 2015 si è avuto un incremento negli studi relativi ad algoritmi post quantum resistant, e questo può essere legato a vari motivi: il primo è senza dubbio legato all'interessamento da parte del NIST, che essendo l'ente dominante ha amplificato l'attenzione sull'argomento in generale, anche con l'apertura della competizione. Il secondo riguarda il fatto che un computer quantistico con potenza rilevante potesse essere reso disponibile da li ai prossimi anni. Un incremento dell'interessamento del settore e degli studi è senz'altro un punto a favore del processo innovativo in atto, considerando l'esistenza di una minaccia quantistica vicina che si dovrebbe manifestare nei prossimi anni. Il NIST ha lanciato la sua competizione solo nel 2017, e ad essa sono stati sottoposti una serie di algoritmi che si possono raggruppare in varie "famiglie" di appartenenza come mostrava la figura 2 nel paragrafo 2.1. Tra di esse solo 2 venivano da un livello di conoscenza già ampiamente noto, *lattice-based* e *hash-based*. Questo è anche dimostrato dal fatto che algoritmi provenienti da queste 2 famiglie fossero già stati standardizzati in qualche forma. Le restanti famiglie presentano elementi di novità non banali per i quali è necessario uno studio approfondito e un costo in termini di tempo non trascurabile per comprenderne a pieno le implementazioni. Proprio per questo, il NIST, anche attraverso i vari report [6][7][8], ha più volte espresso preferenza alla famiglia *lattice-based*, escludendo alcuni algoritmi appartenenti a famiglie diverse pur essendo promettenti, a causa dei troppi elementi di novità che si tradurrebbero in una minaccia alla sicurezza stessa. Nonostante questo, verranno selezionati comunque altri algoritmi appartenenti a famiglie diverse (che soddisfano comunque gli alti requisiti di sicurezza e performance), in modo da diversificare le soluzioni a disposizione tenendo conto dei vari casi d'uso più adatti agli schemi.

In ultimo, per valutare lo stato effettivo dei lavori viene da chiedersi quando un computer quantistico con potenza sufficiente per rendere obsoleti gli standard attuali possa essere disponibile. Non basta aver sviluppato gli standard per essere pronti alla

minaccia quantistica, va valutato e gestito anche il processo di transizione tra i vecchi standard e quelli aggiornati, non essendo un lasso di tempo trascurabile. Gli USA con una direttiva datata 4 maggio 2022 con il titolo *"National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems"*[24] pone una serie di obiettivi nell'ambito della computazione quantistica, uno in particolare, è dedicato alla transizione ai nuovi algoritmi identificando con il 2035 il termine ultimo per aggiornare (almeno) i sistemi ritenuti più delicati. Nel 2018, in un report [25], il National Academies of Sciences (NAS) afferma che "è del tutto inaspettato che entro il prossimo decennio venga costruito un computer quantistico in grado di compromettere RSA 2048 o analoghi sistemi crittografici a chiave pubblica basati su logaritmi discreti." In un altro report del 2021, pubblicato dal Global Risk Institute [26], viene condotto un sondaggio tra 46 esperti del settore quantistico, e nel sondaggio, tra i tanti quesiti, veniva chiesto d'indicare una stima della probabilità che un computer quantistico crittograficamente rilevante da compromettere RSA-2048 in 24 ore, fosse creato entro un periodo di tempo determinato.

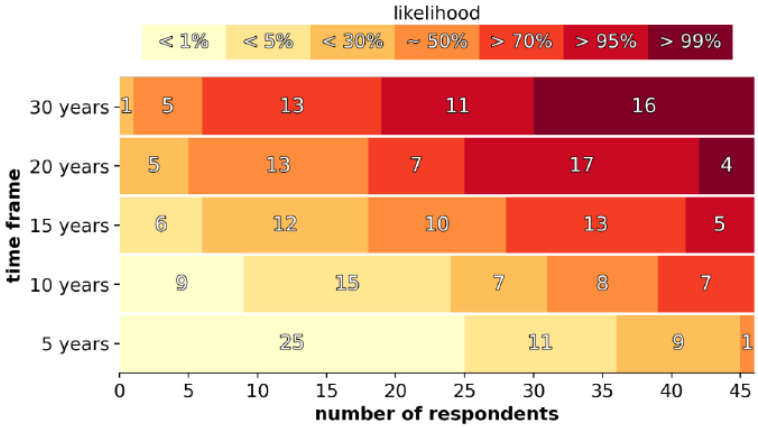

Figure 3: Risultati aggregati del sondaggio, nel quale ad un gruppo di esperti è stato chiesto una stima su quando potesse essere creato un computer quantistico in grado di compromettere RSA-2048 in 24 ore. Sull'asse x il numero degli esperti chiamati in causa, sull'asse y i timeframe oggetto della risposta sui quali è stata chiesta la stima. [26] p.24

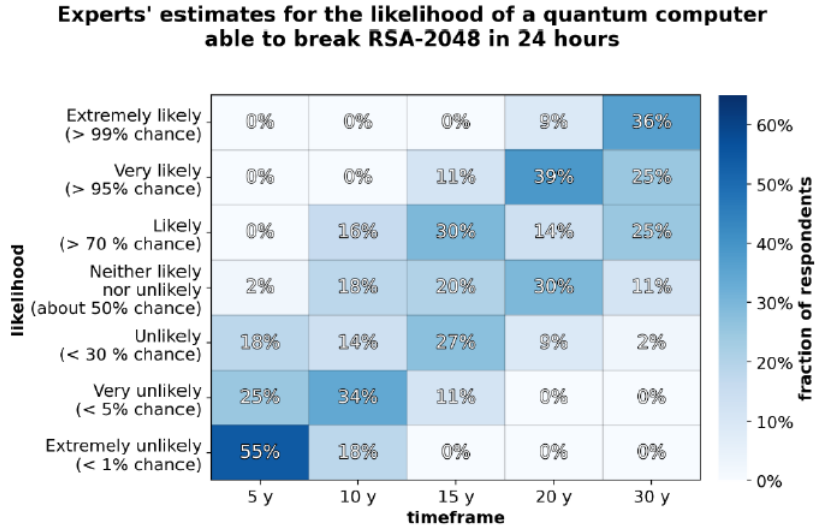

Figure 4: Risultati aggregati dello stesso sondaggio in fig. 3 in una vista diversa, rappresentante l'heatmap degli esperti che hanno assegnato una delle likelihood elencate (asse y) all'esistenza di un computer quantistico in grado di rompere RSA-2048 in meno di 24 ore, entro un certo lasso di tempo in avanti (asse x). [26] p.27

Dal sondaggio, i cui risultati sono riportati in figura 3 e 4, emergono i seguenti risultati:

- **Prossimi 5 anni**: La maggior parte concorda l'alta improbabilità dell'evento.
- **Prossimi 10 anni**: 24 su 46 intervistati ha ritenuto probabile che l'evento fosse "$< 1\%$" o "$< 5\%$", 15/46 hanno ritenuto che fosse probabile "circa il 50%" o "$> 70\%$", suggerendo che esiste una possibilità che la minaccia quantistica diventi concreta in questo lasso di tempo.
- **Prossimi 15 anni**: Più della metà (28/46) degli intervistati ha indicato "circa il 50%" probabile o più probabile, tra i quali 13 hanno indicato una probabilità "$> 70\%$" e 5 una probabilità ancora più alta "$> 95\%$". Questo lasso di tempo appare come un punto significativo, poiché il numero d'intervistati che stimano una probabilità di "circa il 50%", o più, è la maggioranza.
- **Prossimi 20 anni** : Circa il 90% (41/46) degli intervistati ha indicato "circa il 50%" o più probabile, 21/46 hanno indicato "$> 95\%$" o "$> 99\%$" probabile. Ciò indica un timeframe chiave, sostanzialmente più probabile che non, entro questo lasso di tempo.
- **Prossimi 30 anni**: Quaranta esperti su 46 hanno indicato che la minaccia quantistica ha una probabilità più del 70%, con 16/44 esperti che indicano una probabilità maggiore del 99%.

Dai dati raccolti, gli esperti sembrano andare nella direzione nella quale le tempistiche più vicine e probabili per avere un computer quantistico rilevante siano all'incirca tra il 2035-2040 (stesse tempistiche citate nel memorandum della casa bianca [24]). Prendendo queste date come riferimento e lo stato attuale dei lavori di normazione, discussi in precedenza, possiamo affermare che nel complesso i lavori sono a buon punto. Le tempistiche rimangono strette: le prime versioni degli standard sono attese dal NIST entro il 2024, e la competizione non è ancora del tutto terminata. Una volta che paesi e aziende avranno a disposizione i loro standard di riferimento, sarà necessario partire subito con il processo di migrazione da uno standard a un altro. Il processo di transizione è difficilmente stimabile e varia da infrastruttura, azienda e al tipo di dati trattati. L'ultimo processo di transizione avvenuto ha avuto una durata di circa 10 anni, per fare un esempio. Sarà molto improbabile che tutti i sistemi si adeguino per il 2035/2040, ma almeno per i servizi principali è possibile e necessario riuscirci, l'importante è che non si perda tempo.

4 Conclusioni

In questo elaborato sono stati introdotti inizialmente, i risultati degli algoritmi quantistici di Grover e Shor, i quali riescono a compromettere (al momento solo teoricamente) in tutto o in parte gli algoritmi crittografici attuali. In particolare, l'algoritmo di Shor è in grado di compromettere totalmente gli algoritmi a chiave pubblica, utilizzati per operazioni di cifratura e firma digitale, basati sulla fattorizzazione di numeri primi e sull'aritmetica modulare. Per questo, i principali enti di normazione si sono già mossi per l'aggiornamento ai nuovi standard crittografici così detti quantum resistant. Tra quelli citati (NIST, IETF, ETSI, ISO, IEEE), il NIST, grazie anche all'avvio della competizione per la ricerca dei nuovi algoritmi (classici) quantum resistant, è l'ente che ha prodotto e sta producendo i maggiori risultati e questi avranno un alto impatto su tutti gli altri enti. Gli altri enti hanno prodotto solamente materiale di studio preliminare o informativo, ad eccezione dell'IETF che ha prodotto RFC di algoritmi di firma digitale quantum resistant di limitata applicabilità, riprese anche dal NIST per la scrittura dei relativi standard . In generale, gli altri enti mantengono un atteggiamento di attesa nei confronti del NIST, prima di procedere con le pubblicazioni dei propri standard, che saranno basati proprio sui risultati del NIST. A oggi non esiste un computer abbastanza potente per eseguire un'istanza dell'algoritmo di Shor che sia in grado di compromettere i crittosistemi attuali, ma secondo fonti della casa bianca e altri ricercatori del settore è probabile che questo possa accadere almeno tra 15-20 anni. E' perciò necessario arrivare pronti a questa eventualità, almeno per dati e infrastrutture più importanti. Considerando che dovrà passare ancora qualche mese (o anno) per avere i nuovi standard completi, il tempo per effettuare la migrazione ai nuovi algoritmi non manca, ma sarà necessario partire appena possibile una volta che gli standard saranno pronti. Il processo di transizione sarà la prossima "sfida". E' un processo complicato e che richiederà del tempo, probabilmente più di quello usato nell'ultima transizione avvenuta, soprattutto vista la nuova natura degli algoritmi proposti.

References

[1] Dustin (Fed) Moody. "Let's Get Ready to Rumble- The NIST PQC "Competition"". en. In: (), p. 37.

[2] Lov K. Grover. "A fast quantum mechanical algorithm for database search". en. In: *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96*. Philadelphia, Pennsylvania, United States: ACM Press, 1996, pp. 212–219. ISBN: 978-0-89791-785-8. DOI: 10.1145/237814.237866. URL: http://portal.acm.org/citation.cfm?doid=237814.237866 (visited on 12/09/2022).

[3] Peter W. Shor. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". en. In: *SIAM J. Comput.* 26.5 (Oct. 1997). arXiv:quant-ph/9508027, pp. 1484–1509. ISSN: 0097-5397, 1095-7111. DOI: 10.1137/S0097539795293172. URL: http://arxiv.org/abs/quant-ph/9508027 (visited on 12/09/2022).

[4] Lily Chen et al. *Report on Post-Quantum Cryptography*. en. Tech. rep. NIST IR 8105. National Institute of Standards and Technology, Apr. 2016, NIST IR 8105. DOI: 10.6028/NIST.IR.8105. URL: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf (visited on 12/09/2022).

[5] Nist team, ed. *call-for-proposals-final*. en. Dec. 2016. URL: https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf (visited on 12/09/2022).

[6] Gorjan Alagic et al. *Status report on the first round of the NIST post-quantum cryptography standardization process*. en. Tech. rep. NIST IR 8240. Gaithersburg, MD: National Institute of Standards and Technology, Jan. 2019, NIST IR 8240. DOI: 10.6028/NIST.IR.8240. URL: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8240.pdf (visited on 12/09/2022).

[7] Dustin Moody et al. *Status report on the second round of the NIST post-quantum cryptography standardization process*. en. Tech. rep. NIST IR 8309. Gaithersburg, MD: National Institute of Standards and Technology, July 2020, NIST IR 8309. DOI: 10.6028/NIST.IR.8309. URL: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8309.pdf (visited on 12/09/2022).

[8] Dustin Moody. *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*. en. Tech. rep. NIST IR 8413-upd1. Gaithersburg, MD: National Institute of Standards and Technology, 2022, NIST IR

8413–upd1. DOI: 10.6028/NIST.IR.8413-upd1. URL: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413-upd1.pdf (visited on 12/09/2022).

[9] David A. Cooper et al. *Recommendation for Stateful Hash-Based Signature Schemes*. en. Tech. rep. National Institute of Standards and Technology, Oct. 2020. DOI: 10.6028/NIST.SP.800-208. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-208.pdf (visited on 12/09/2022).

[10] D. McGrew, M. Curcio, and S. Fluhrer. *Leighton-Micali Hash-Based Signatures*. en. Tech. rep. RFC8554. RFC Editor, Apr. 2019, RFC8554. DOI: 10.17487/RFC8554. URL: https://www.rfc-editor.org/info/rfc8554 (visited on 12/09/2022).

[11] A. Huelsing et al. *XMSS: eXtended Merkle Signature Scheme*. en. Tech. rep. RFC8391. RFC Editor, May 2018, RFC8391. DOI: 10.17487/RFC8391. URL: https://www.rfc-editor.org/info/rfc8391 (visited on 12/09/2022).

[12] S. Fluhrer et al. *Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security*. en. Tech. rep. RFC8784. RFC Editor, June 2020, RFC8784. DOI: 10.17487/RFC8784. URL: https://www.rfc-editor.org/info/rfc8784 (visited on 12/09/2022).

[13] ETSI. "Quantum Safe Cryptography and Security - An introduction, benefits, enablers and challenges - June 2015". en. In: (), p. 64.

[14] ETSI GR QSC. *Quantum-safe algorithmic framework*. Tech. rep. 2016. URL: https://www.etsi.org/deliver/etsi_gr/qsc/001_099/001/01.01.01_60/gr_qsc001v010101p.pdf (visited on 12/09/2022).

[15] ETSI GR QSC. *Quantum Safe Cryptography; Case Studies and Deployment Scenarios*. Tech. rep. 2017. URL: https://www.etsi.org/deliver/etsi_gr/qsc/001_099/003/01.01.01_60/gr_qsc003v010101p.pdf (visited on 12/09/2022).

[16] ETSI GR QSC. *Quantum-Safe Key Exchanges*. Tech. rep. Oct. 2017. URL: https://www.etsi.org/deliver/etsi_tr/103500_103599/103570/01.01.01_60/tr_103570v010101p.pdf (visited on 12/09/2022).

[17] ETSI GR QSC. *Quantum-Safe Signatures*. en. Tech. rep. Sept. 2021. URL: https://www.etsi.org/deliver/etsi_tr/103600_103699/103616/01.01.01_60/tr_103616v010101p.pdf (visited on 12/09/2022).

[18] ETSI GR QSC. *Quantum-Safe Public-Key Encryption and Key Encapsulation*. Tech. rep. Oct. 2021. URL: https://www.etsi.org/deliver/etsi_tr/103800_103899/103823/01.01.02_60/tr_103823v010102p.pdf (visited on 12/09/2022).

[19] "IEEE Standard Specification for Public Key Cryptographic Techniques Based on Hard Problems over Lattices". In: *IEEE Std 1363.1-2008* (2009), pp. 1–81. DOI: 10.1109/IEEESTD.2009.4800404.

[20] *Announcement on the Algorithm Selection Results of the National Cryptography Algorithm Design Competition*. URL: https://www.cacrnet.org.cn/site/content/854.html (visited on 12/09/2022).

[21] *Notice on Announcing the Results of the First Round of Algorithm Selection in the National Cryptography Algorithm Design Competition*. URL: https://www.cacrnet.org.cn/site/content/838.html (visited on 12/09/2022).

[22] Nancy Liu. *China, Russia to Adopt 'Slightly Different' PQC Standards From US*. en-US. Oct. 2022. URL: https://www.sdxcentral.com/articles/analysis/china-russia-to-adopt-slightly-different-pqc-standards-from-us/2022/10/ (visited on 12/09/2022).

[23] *CACR post-quantum competition*. URL: https://en.qapp.tech/help/cacr (visited on 12/09/2022).

[24] The White House. *National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems*. en-US. May 2022. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/ (visited on 12/09/2022).

[25] Committee on Technical Assessment of the Feasibility and Implications of Quantum Computing et al. *Quantum Computing: Progress and Prospects*. en. Ed. by Emily Grumbling and Mark Horowitz. Pages: 25196. Washington, D.C.: National Academies Press, Mar. 2019. ISBN: 978-0-309-47969-1. DOI: 10.17226/25196. URL: https://www.nap.edu/catalog/25196 (visited on 12/09/2022).

[26] Marco Piani and Michele Mosca. "QUANTUM THREAT TIMELINE REPORT 2021". en. In: (2021), p. 87.