# Linee Guida per Sottomettere al NIST una Proposta per Algoritmi Post-Quantum Resistant

Luca Lavazza, Università degli Studi di Brescia

Luglio - Agosto 2022




## Abstract

Fin dai primi importanti passi avanti nella teoria del quantum computing negli anni '90, con la definizione di importanti algoritmi come quello di Peter Shor e Lov Grover, è apparso chiaro che questa tecnologia apparentemente futuristica aveva la potenzialità di perturbare profondamente la crittografia e di conseguenza l'informatica tradizionale. Anni dopo, la pratica ha parzialmente raggiunto la teoria, e sono comparsi i primi veri computer quantistici: è stato quindi chiaro al NIST, National Institute of Standards and Technology, che era il momento di prepararsi alla transizione verso nuovi standard crittografici, chiamati post-quantum-resistant. È stata perciò avviata nel 2016 una competizione per la selezione e definizione di algoritmi a chiave pubblica resistenti alla tecnologia quantistica.
Quella competizione entra oggi nelle fasi finali, avviandosi alla conclusione, ma un recente articolo del NIST dichiara che una nuova competizione avrà inizio a breve.
Questo documento raggruppa le istruzioni, indicazioni e suggerimenti necessari a chi desideri partecipare con probabilità di successo alla nuova competizione, senza la necessità di recuperare diversi articoli negli annali del NIST, e dando inoltre la possibilità di approcciarsi in italiano al tema proposto.

# Indice

# 1 Introduzione [Kum] [BBD09] [BL17]

Buona parte della crittografia moderna si basa su complesse funzioni matematiche costruite in modo tale che siano semplici e poco costose da calcolare in una direzione, ma molto complesse da risolvere nella direzione inversa. La sicurezza di molti protocolli crittografici si basa proprio sul fatto che i calcolatori odierni impiegherebbero centinaia di anni per risolvere i problemi crittografici alla base di essi, indipendentemente dalla potenza di calcolo a disposizione. Tuttavia, i computer quantistici sono ormai una realtà e potenzialmente riducono di molto la complessità nel risolvere i problemi crittografici sopra menzionati.

Senza entrare nei dettagli, gli algoritmi crittografici possono essere suddivisi in due macrocategorie. Si noti che si usa la terminologia comune di Alice e Bob per identificare le parti comunicanti.

- **Algoritmi Simmetrici.**
  Alice e Bob condividono la stessa chiave, che viene utilizzata per cifrare e decifrare i dati.
  Sono algoritmi relativamente semplici rispetto alla controparte asimmetrica, tuttavia la difficoltà maggiore è nella gestione della chiave, che deve essere condivisa in modo sicuro dalle due parti prima di avviare la comunicazione cifrata.

- **Algoritmi Asimmetrici.**
  Alice e Bob hanno rispettivamente una coppia di chiavi, una privata che è mantenuta segreta, e una pubblica condivisa tra loro. Alice cifra i dati con la chiave pubblica, e Bob li decifra con la propria chiave privata.
  Alcuni dei problemi cardine su cui si basa la crittografia sono la fattorizzazione di numeri primi e il problema del logaritmo discreto.

Il quantum computing è un'applicazione di meccanismi quantistici che consentono di manipolare lo stato dei qubit in maniera controllata per eseguire degli algoritmi. I qubit sono la variante quantistica dei bit: sono rappresentati tramite la notazione Bra-Ket come $|0\rangle$ e $|1\rangle$ e hanno la particolarità di potersi trovare in stati nei quali assumono contemporaneamente il valore 0 e 1. Questo fenomeno è chiamato "superposition".
I calcolatori tradizionali in ogni momento si trovano in uno stato ben definito, che può essere descritto da una sequenza di bit, che rappresenta i dati su cui la macchina opera e il programma, una serie di direttive che manipolano questi dati.
In un computer quantistico il programma è dato da una sequenza di gates, o porte, derivanti da un insieme finito, indipendente dall'input o derivato da esso tramite algoritmi tradizionali. È nei dati che i meccanismi quantistici entrano in gioco:

- **Superposition:**
  I sistemi quantistici possono esistere in due stati contemporaneamente.

Un qubit può essere sia 0 che 1 finchè non viene osservato; a quel punto collassa ad uno dei due valori.

- **Entanglement:**
  È un fenomeno quantistico per cui intercorre una relazione tra particelle, che possono così essere descritte in riferimento le une alle altre. Misurazioni effettuate su una particella in entanglement con un'altra, influenzeranno immediatamente la seconda, indipendentemente dalla distanza spaziale tra le due.

- **Interferenza:**
  L'idea cardine del quantum computing è quella di controllare la probabilità che i qubit ricadano in uno stato piuttosto che l'altro. L'interferenza quantistica, un effetto collaterale della superposition, consente di controllare il valore di un qubit nella direzione desiderata.

Nel 1994 Peter Shor sviluppò un algoritmo quantistico in tempo polinomiale per la fattorizzazione dei numeri positivi interi. Il popolare crittosistema RSA, ad esempio, si basa proprio su questo problema, sulla difficoltà di fattorizzare un grande numero $N = pq$, dove $p$ e $q$ sono numeri primi non noti.
Si sono svolte molte ricerche ed analisi per stimare il costo dell'algoritmo di Shor, e, per esempio, una delle varianti stima che, dato $N = pq$ rappresentabile con $n$ bit, l'algoritmo di Shor impieghi $O(n^3 \log n)$ operazioni su $2n + 3$ qubit. È poi possibile, oltre ad eseguire computazioni in parallelo, ridurre il numero di operazioni a $n^{2+o(1)}$ aumentando il numero di qubit. Chiaramente la complessità del problema di fattorizzazione diventa incredibilmente minore rispetto alle centinaia d'anni di computazione richiesti dai calcolatori tradizionali, sottolineando così la debolezza dei crittosistemi odierni rispetto ai computer quantistici.
Nel 1996 Lov Grover ideò un algoritmo quantistico per la ricerca in un database non ordinato. Questo algoritmo può trovare un elemento in un database di $N$ elementi senza ordinamento con $\sqrt{N}$ ricerche.
Per quanto riguarda la crittografia, si traduce nel fatto che, ad esempio, questo algoritmo richiederebbe solamente 185 ricerche per trovare la chiave di DES con chiave a 56-bit. Pur essendo un potenziale problema, non comporta ancora un rischio per algoritmi simmetrici moderni con chiavi molto più lunghe.
La tabella seguente riassume la situazione attuale rispetto ai crittosistemi più comunemente utilizzati.

| **Crittografia Simmetrica** | |
|---|---|
| **Algoritmo** | **Stato Post-Quantum** |
| AES | Servono chiavi più grandi |
| SHA-2, SHA-3 | Servono output più grandi |
| **Crittografia Asimmetrica** | |
| **Algoritmo** | **Stato Post-Quantum** |
| RSA | Non più sicuro |
| ECDSA, ECDH | Non più sicuro |
| DSA | Non più sicuro |

Diverse iniziative sono state avviate per far fronte ai problemi introdotti dai computer quantistici e per standardizzare per tempo validi algoritmi Post Quantum Resistant. In particolare, l'iniziativa principale è quella che è stata proposta dal NIST nel 2016, tutt'oggi non conclusa, e che sarà trattata in questo documento. Lo scopo è quello di preparare il lettore alla presentazione di una proposta per la successiva fase di competizione che dovrebbe essere avviata a breve.

# 2 Preparazione di una Proposta

Il lettore sarà sicuramente interessato alla realizzazione di una proposta che possa venire accettata e presa in considerazione dal NIST e che, pertanto, segua con attenzione le linee guida relative ai requisiti tecnici che si procede a presentare. Sarà inoltre interessato a conoscere i parametri di valutazione delle proposte, cosicché sia possibile modellare la propria proposta in modo da soddisfare efficacemente tali parametri.
Lo scopo di questo capitolo è quello di ricapitolare e catalogare gli aspetti tecnici essenziali da osservare per partecipare con successo alla competizione.

## 2.1 Requisiti per la Sottomissione

Allo stato attuale della competizione, il NIST ha annunciato che durante l'estate 2022 pubblicherà una nuova call for proposals per algoritmi di firma digitale a chiave pubblica, che prevederà l'inoltro delle proposte nel corso del 2023 [NISc]. Alla data di stesura di questo documento, non sono disponibili aggiornamenti o dettagli più precisi da parte del NIST; si invita a tenere controllato l'hub aggregatore di notizie relative alla standardizzazione di algoritmi Post-Quantum Resistant (PQR) sul sito del NIST [NISa].
Tuttavia, si ritiene che le modalità seguiranno da vicino quelle dettagliate nel 2016 nel documento "*Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process*" [NISd], relativamente alla call for proposals originale.
Nonostante non siano al momento note le modalità concrete con cui il NIST aprirà la competizione, per offrire una prospettiva verosimile sulle possibili tempistiche che saranno adottate, si riportano le scadenze specificate nel documento sopracitato:

- Pubblicazione del documento: 20 dicembre 2016;
- Termine per la ricezione delle proposte da parte del NIST: 30 novembre 2017.
  Le proposte ricevute prima del 30 settembre 2017 hanno ricevuto una revisione di completezza da parte del NIST, avvisando gli autori delle rispettive proposte di eventuali mancanze o difetti entro il 31 ottobre 2017, così da lasciare il tempo necessario per sistemare eventuali problemi segnalati e poter ripresentare la proposta.

Il documento sopracitato specifica poi i metodi di inoltro delle proposte: queste dovranno essere consegnate su un dispositivo di memorizzazione, per mezzo di canali tradizionali di posta. Inoltre, per motivazioni legate alla proprietà intellettuale di alcune proposte, come si osserverà in un paragrafo successivo, alcune parti delle sottomissioni potranno venire inoltrate esclusivamente in forma cartacea, ovviamente sempre tramite posta tradizionale. Per privacy del destinatario, e ipotizzando che nel corso dei sei anni trascorsi dalla pubblicazione qualche dettaglio possa essere cambiato, non si riporta l'indirizzo specificato

per l'invio, che può comunque essere recuperato nel documento riportato in bibliografia.
Procedendo più nello specifico, si osserva che una proposta completa e ben formata dovrà inderogabilmente contenere i seguenti elementi, che verranno analizzati con attenzione nei rispettivi paragrafi:

- Copertina;
- Specifiche dell'algoritmo e documentazione di supporto;
- Dispositivo ottico o digitale;
- Documenti relativi alla proprietà intellettuale.

Il NIST accetta candidature sia domestiche (U.S.A.) che internazionali, tuttavia per facilitare la fase di analisi e valutazione pubbliche, richiede esplicitamente che le proposte siano in lingua inglese. Tutte le proposte in lingue differenti saranno automaticamente marchiate come incomplete.
Prima di proseguire con l'analisi di ciascuna componente di una proposta, si tiene a sottolineare che alcuni dettagli potranno essere differenti per la nuova call for proposals; tuttavia, non esistono ancora elementi certi per confermare questa ipotesi.

### 2.1.1 Copertina

La copertina di una proposta dovrà riportare le seguenti informazioni:

- Il nome del crittosistema proposto;
- I dati del candidato principale.
  In particolare:
  - Nome e cognome
  - Indirizzo e-mail
  - Numero di telefono
  - Organizzazione
  - Indirizzo postale
- Nomi di eventuali candidati aggiuntivi;
- Nomi degli inventori/sviluppatori del crittosistema;
- Se presente, nome del proprietario del crittosistema. Di norma il NIST si aspetta che sia lo stesso del candidato;
- Firma del candidato;
- Opzionalmente, contatti di backup.

### 2.1.2 Specifiche dell'algoritmo e documentazione di supporto

Ogni proposta dovrà allegare:

- **Una specifica completa per iscritto**
  Dovrà contenere tutte le operazioni matematiche, equazioni, tabelle e diagrammi necessari all'implementazione dell'algoritmo. Dovrà inoltre includere una motivazione del design, insieme ad una spiegazione relativa ad ogni importante scelta di design.
  Ogni sottomissione dovrà includere in questa sezione una raccolta di algoritmi che implementino i meccanismi crittografici che si aspira a standardizzare. In particolare, per gli algoritmi di firma digitale, dovranno essere inclusi gli algoritmi relativi ad ogni parte del crittosistema: generazione della chiave, generazione della firma e verifica della firma.
  Infine, ogni algoritmo dovrà specificare eventuali parametri modificabili (di più a riguardo nel capitolo 3.4), eventuali meccanismi di padding, la motivazione dietro all'uso di primitive approvate dal NIST o meno, e infine una spiegazione di ogni costante utilizzata al fine di eliminare i dubbi sulla presenza di backdoor.

- **Una dettagliata analisi delle performance**
  Verrà inclusa una dichiarazione dell'efficienza stimata dell'algoritmo e della memoria richiesta da esso rispetto alla "NIST PQC Reference Platform". Di più su questo argomento nel capitolo dedicato alla valutazione. L'aggiunta di altre misurazioni e stime di performance su piattaforme differenti sarà a discrezione del candidato.
  In particolare, come minimo questa sezione dovrà contenere:

  - Una descrizione dettagliata della piattaforma utilizzata per realizzare le stime, cosicché queste possano essere verificate nella fase di analisi pubblica,
  - Stime intese come durata in millisecondi o cicli di clock per ciascuna operazione sulla NIST PQC Reference Platform, oltre alla dimensione degli input e output.

- **Valori per i Known Answer Tests**, da qui in poi "KAT".
  I KAT sono tuple di input che producono singoli valori di output. Un KAT ad esempio è un input formato da una tupla composta da una chiave e un testo in chiaro, che restituisce in output il relativo testo cifrato. Se un algoritmo sfrutta valori casuali, verranno fissati dei valori di riferimento per le parti randomizzate, cosicché l'algoritmo sia forzato a produrre un valore fissato in output. Saranno presentati diversi KAT per ciascun aspetto dell'algoritmo, per esempio per la generazione della chiave, la generazione della firma e la verifica della firma.
  Tutti i valori per i KAT verranno allegati elettronicamente in file separati, tramite dispositivi e metodologie illustrate nel capitolo **2.1.3**.
  Ciascun file relativo ad un KAT deve riportare le seguenti informazioni:

- Nome dell'algoritmo
- Nome del test
- Descrizione del test
- Altri parametri

Questa lista dovrà essere seguita da un insieme di tuple dove tutti i valori al loro interno sono chiaramente specificati.
Saranno inclusi insiemi di KAT per ciascuna security strength specificata nel relativo capitolo.
Ulteriori richieste da parte del NIST:

a) Se l'esecuzione di un algoritmo produce risultati intermedi informativi, dovranno essere inclusi KAT anche per questi rispetto ad ogni security strength richiesta;

b) Se sono utilizzate delle tabelle, insiemi di vettori di KAT dovranno essere inclusi per specificare gli elementi delle tabelle.

- **Una descrizione attenta dei livelli di sicurezza attesi**
  Il candidato includerà nella proposta una definizione delle security strength attese, inseme alla motivazione che giustifichi tali attese. Effettuerà queste analisi di sicurezza sulla base dei parametri che verranno specificati nel capitolo **2.3.1**, con l'invito ad essere moderati in tali considerazioni.

- **Una criptoanalisi dell'algoritmo rispetto ad attacchi noti**
  Il candidato includerà apertamente una lista di attacchi noti nei confronti dello schema, e fornirà stime di complessità di questi attacchi. Qualora esista materiale pubblicato a riguardo, questo verrà necessariamente citato si incoraggia il candidato ad allegarlo.

- **Una specifica dei vantaggi e limitazioni della proposta**
  Vantaggi e limitazioni della proposta saranno considerati rispetto alla sicurezza, a caratteristiche e vulnerabilità insolite, a funzioni extra o a tradeoff di implementazione.
  Questa specifica potrà anche considerare le difficoltà o agevolazioni di implementazione del protocollo nel mondo reale.
  Inoltre il NIST invita a considerare le possibilità di implementazione su piattaforme differenti, e a porre particolare attenzione ai casi estremi in fatto di bassa potenza di calcolo, limitazione di memoria e basso consumo energetico.

### 2.1.3 Dispositivo ottico o digitale

Tutti i materiali digitali saranno forniti al NIST in un file .zip, contenuto in un CD-ROM, DVD, o archivio USB marchiato col nome del candidato del protocollo, insieme al nome del crittosistema.
L'autore del presente documento ritiene assai verosimile che la sottomissione

delle nuove proposte potrà avvenire tramite modalità differenti, abbandonando dispositivi ormai legacy e potenzialmente rischiosi come quelli sopra citati, in favore ad esempio della condivisione nel cloud. Tuttavia, si ipotizza che la struttura del file .zip possa restare la medesima, e viene pertanto riportata in accordo col documento originale.

- **Implementazioni**
  Sono richieste due implementazioni: una di riferimento, ed una ottimizzata. Lo scopo della prima è di favorire la comprensione e dimostrare in maniera chiara il protocollo proposto e la sua implementazione; in questo caso la chiarezza conta più dell'efficacia. Nel secondo caso, al contrario, è previsto che il codice venga ottimizzato in modo da offrire le migliori prestazioni su una piattaforma di riferimento Intel x64, a discapito della comprensione del codice. In ogni caso le implementazioni saranno proposte in ANSI C, e dovranno coprire ogni sezione del protocollo.

- **KAT**
  Il file zip conterrà tutti gli elementi specificati nella relativa sezione del capitolo **2.1.2**.

- **Documentazione di supporto**
  Per facilitare la distribuzione elettronica delle proposte, sarà fornita una versione PDF di tutto il materiale scritto.

- **Struttura della directory**
  I file saranno presentati rispettando il seguente albero:

  - README
  - Reference_Implementation
  - Optimized_Implementation
  - KAT
  - Supporting_Documentation

  Il file README sarà un plain text file contenente una lista di tutti i file inclusi, con relativa breve descrizione di ciascuno.

#### 2.1.4 Documenti relativi alla proprietà intellettuale

Per rendere il presente documento più organico e meno ripetitivo, questo argomento verrà trattato in maniera approfondita nel capitolo **3.1**.
Ci si limita ad anticipare che le copie degli statement da allegare non verranno riportate in questo documento per brevità, e perché è probabile che subiscano modifiche per la nuova call for proposals. In ogni caso sono reperibili nel documento [NISd].

## 2.2 Requisiti Minimi di Accettazione

Tutte le proposte che rispettano le regole sopra descritte verranno definite "complete" dal NIST e verrà valutato se possano essere considerati crittosistemi "proper". Una proposta "complete and proper" potrà poi accedere alla fase finale di valutazione per la standardizzazione.
I seguenti sono i requisiti minimi di accettazione perchè una proposta sia considerata proper:

- Gli algoritmi dovranno poter essere resi disponibili pubblicamente e liberamente senza impedimenti;
- Gli algoritmi non dovranno contenere elementi che si ritengono deboli rispetto ai computer quantistici;
- I sistemi di firma digitale dovranno includere necessariamente algoritmi per la generazione delle chiavi, la generazione della firma e la verifica della stessa. L'algoritmo di generazione produrrà chiavi pubbliche funzionanti. Il crittosistema dovrà supportare messaggi di lunghezza fino a $2^{63}$ bit.
  Non si riportano le specifiche relative agli algoritmi di cifratura a chiave pubblica e di KEM, in quanto non utili per la successiva call for proposals;
- La proposta includerà tutti i valori e parametri necessari a raggiungere i livelli e le proprietà di sicurezza richiesti dal NIST.

## 2.3 Criteri e Processo di Valutazione

Il NIST formerà un pannello interno di esperti, che saranno tenuti ad analizzare e valutare tutte le proposte complete and proper secondo tre parametri, che si andranno a dettagliare nei successivi paragrafi:

- Sicurezza
- Costo e Performance
- Algoritmi e Caratteristiche Implementative

Nonostante il NIST effettuerà la propria analisi, viene incoraggiata fortemente la valutazione pubblica delle proposte accettate, e la relativa pubblicazione dei risultati di tali valutazioni. Il pannello di esperti del NIST terrà in considerazione sia la propria analisi che quelle pubbliche, in modo da effettuare una decisione informata ed efficace.

### 2.3.1 Sicurezza

La sicurezza di uno schema crittografico è l'elemento più importante di valutazione e verrà misurato sulla base di molteplici parametri che si procede ad elencare e spiegare.
NIST intende standardizzare uno o più schemi di firma digitale che rispettino la proprietà accademicamente nota come EUF-CMA, acronimo che sta per "Existential Unforgeability under Chosen Message Attack" [Gre]:

1. Lo sfidante genera una coppia valida di chiavi ($p_k$, $s_k$), e inoltra $p_k$ all'attaccante.

2. L'attaccante può ora ripetutamente chiedere firme su messaggi scelti ($M_1$, $M_2$, ..., $M_q$), ricevendo in risposta le rispettive firme valide ($\sigma_1$, $\sigma_2$, ..., $\sigma_q$).

3. Alla fine dell'esperimento l'attaccante deve produrre un messaggio $M^*$ e una firma $\sigma^*$, tali che $M^* \notin (M_1, M_2, \ldots, M_q)$ e la coppia $(M^*, \sigma^*)$ sia verificata correttamente rispetto alla chiave pubblica $p_k$.
   Lo schema è considerato sicuro se non è possibile soddisfare questo requisito.

La definizione di sicurezza appena fornita va considerata come ciò che il NIST considera un attacco rilevante nei confronti dei protocolli di firma digitale. Le proposte saranno valutate sulla base di questa proprietà. Ai candidati non è richiesto di fornire una prova di sicurezza rispetto a questo attacco, ma se presente sarà sicuramente considerata.
Al fine di determinare la sicurezza dei protocolli, si assume che l'attaccante abbia accesso a non più di $2^{64}$ messaggi scelti, anche se i test potranno essere effettuati anche su più messaggi a discrezione del NIST.

Il NIST si aspetta che si incontreranno molte incertezze nella stima della sicurezza dei crittosistemi post-quantum proposti, per due motivi: la possibilità che vengano scoperti nuovi algoritmi che conducano a nuovi attacchi, e l'abilità limitata di prevedere l'evoluzione dei computer quantistici negli anni a venire.
Per far fronte a queste incertezze, il NIST propone l'approccio seguente: verrà definita una raccolta di livelli di sicurezza come guida per la valutazione, e ciascun protocollo potrà essere inizializzato con parametri differenti in modo da soddisfare più livelli. Lo scopo di questa classificazione è:

1. Facilitare la comparazione tra le prestazioni degli algoritmi considerati;

2. Consentire al NIST di fare scelte attente riguardo a quando passare a chiavi più lunghe;

3. Aiutare i candidati ad effettuare scelte attente e consistenti relative a quali primitive usare nei meccanismi di padding, o altri componenti dei loro crittosistemi;

4. Comprendere meglio i tradeoff tra sicurezza e performance di ciascuna proposta.

In accordo col secondo e terzo punto appena elencati, il NIST baserà la sua classificazione su uno spettro di livelli di sicurezza forniti da standard attuali della crittografia simmetrica, che ci si aspetta offriranno resistenza significativa anche in ambito post-quantum. In particolare, il NIST definirà una categoria separata per ciascuno dei seguenti livelli di sicurezza:

1. Ciascun attacco che supera questo livello di sicurezza deve richiedere una potenza computazionale paragonabile a, o maggiore di, quella necessaria per una ricerca di chiave su un cifrario a blocchi con una chiave di 128 bit (e.g. AES128).

2. Ciascun attacco che supera questo livello di sicurezza deve richiedere una potenza computazionale paragonabile a, o maggiore di, quella necessaria per una ricerca di collisioni su una funzione hash a 256 bit (e.g. SHA256/SHA3-256).

3. Ciascun attacco che supera questo livello di sicurezza deve richiedere una potenza computazionale paragonabile a, o maggiore di, quella necessaria per una ricerca di chiave su un cifrario a blocchi con una chiave di 192 bit (e.g. AES192)

4. Ciascun attacco che supera questo livello di sicurezza deve richiedere una potenza computazionale paragonabile a, o maggiore di, quella necessaria per una ricerca di collisioni su una funzione hash a 384 bit (e.g. SHA384/SHA3-384).

5. Ciascun attacco che supera questo livello di sicurezza deve richiedere una potenza computazionale paragonabile a, o maggiore di, quella necessaria per una ricerca di chiave su un cifrario a blocchi con una chiave di 256 bit (e.g. AES256).

Affinchè una proposta soddisfi uno dei precedenti livelli, è necessario che un eventuale attacco richieda le stesse risorse computazionali dell'attacco relativo al livello target.
Come guida preliminare per i candidati, il NIST suggerisce un approccio dove gli attacchi quantistici sono ristretti ad un tempo di esecuzione fissato, altrimenti detto "circuit depth". Questo parametro è chiamato MAXDEPTH. Questa restrizione è motivata dal fatto che è complicato eseguire computazioni seriali estremamente lunghe in ambito quantistico. Possibili valori per MAXDEPTH sono:

- Da $2^{40}$ porte logiche: il numero approssimativo di porte logiche correnti,
- A $2^{64}$ porte logiche: il numero approssimativo di porte logiche raggiungibili in un futuro prossimo,
- Fino a $2^{96}$ porte logiche: il numero approssimativo di porte logiche che qubit di scala atomica con tempi di propagazione pari alla velocità della luce potrebbero effettuare in un millennio.

La seguente tabella compara la difficoltà degli attacchi ad algoritmi tradizionali con dei valori di circuit depth equivalenti:

| | |
|---|---|
| AES128 | $2^{170}$/MAXDEPTH quantum gate o $2^{143}$ gate classici |
| SHA3-256 | $2^{146}$ gate classici |
| AES192 | $2^{233}$/MAXDEPTH quantum gate o $2^{207}$ gate classici |
| SHA3-384 | $2^{210}$ gate classici |
| AES256 | $2^{298}$/MAXDEPTH quantum gate o $2^{272}$ gate classici |
| SHA3-512 | $2^{274}$ gate classici |

È utile sottolineare che questi livelli di sicurezza forniscono più sicurezza quantistica di quanto inizialmente si possa pensare. Per esempio, 1., 3. e 5. sono definiti in termini di cifrari a blocchi, che possono essere rotti sfruttando l'algoritmo di Grover, con uno speedup quantistico quadratico. Ma l'algoritmo di Grover richiede una lunga computazione seriale, che è difficile da implementare nella pratica. In uno scenario realistico è necessario eseguire molteplici piccole istanze dell'algoritmo in parallelo, che comporta uno speedup decisamente meno preoccupante.
Infine, per attacchi che sfruttano una combinazione di computazione tradizionale e quantistica, si potrebbe usare una metrica di costo che definisce i gate quantistici come diversi ordini di grandezza più costosi di quelli classici.
Il NIST richiede ai partecipanti di definire una stima preliminare di sicurezza dei propri protocolli in accordo con quanto appena espresso, per ciascun paramento che verrà considerato per la standardizzazione.
Non viene invece richiesto di presentare insiemi di parametri distinti per ciascun livello sopracitato: si assume che gli insiemi di parametri per un dato livello soddisfino automaticamente anche i livelli inferiori. È però possibile presentare più insiemi di parametri per uno stesso livello, così da dimostrare diversi comportamenti del protocollo in relazione al tradeoff prestazioni-sicurezza.
Il NIST raccomanda ai candidati di concentrarsi sulle prime categorie, in quanto verosimilmente sufficienti a garantire la sicurezza per un lungo periodo, ma di fornire almeno un insieme di parametri per i livelli 4. e 5..
Altre proprietà desiderabili sono la perfect forward secrecy, la resisitenza ad attacchi side-channel e la resistenza all'uso improprio (ad esempio malfunzionamenti, errori nel codice, problemi di implementazione, ecc...).

Poiché la crittografia a chiave pubblica è basata su concetti matematici spesso delicati da usare al meglio, è estremamente importante che le strutture matematiche di fondo siano ben comprese, così da assicurare la fiducia nella sicurezza del crittosistema. Per questo motivo, il NIST preferirà schemi semplici ad alternative più complicate. Allo stesso modo, schemi i cui principi di design possono essere ricondotti a teorie approfonditamente ricercate saranno preferiti a schemi basati su teorie più nuove, o sistemate spesso per prevenire di volta in volta delle debolezze identificate dalla ricerca.
NIST considererà anche la chiarezza della documentazione allegata come un punto a favore.

### 2.3.2 Costo

Siccome il costo dei crittosistemi a chiave pubblica può essere misurato su diverse dimensioni, il NIST continuerà a ricercare indicazioni pubbliche su quali metriche e applicazioni siano le più importanti.
Gli schemi saranno valutati sulla base della dimensione delle chiavi pubbliche e delle firme che producono. Queste sono considerazioni importanti per applicazioni con bandwidth limitata, o in protocolli Internet con dimensioni limitate dei pacchetti.
Gli schemi saranno valutati anche sulla base dell'efficienza computazionale della chiave pubblica (verifica della firma) e di quella privata (firma).
Infine, verrà anche valutata l'efficienza computazionale del processo di generazione della chiave.

### 2.3.3 Algoritmi e Caratteristiche Implementative

Verranno considerati tre parametri:

- **Flessibilità:**
  Assunte delle buone prestazioni e sicurezza, si preferiranno gli schemi più flessibili, ovvero quelli che andranno incontro alle necessità di più casi d'uso.
  Alcuni esempi di flessibilità:
  - Lo schema può essere modificato per aggiungere funzionalità o aumentare la sicurezza;
  - È semplice modificare i parametri dello schema per raggiungere nuovi livelli di sicurezza e/o prestazioni;
  - L'algoritmo può essere implementato efficientemente e in modo sicuro su una grande varietà di piattaforme;
  - L'implementazione dell'algoritmo può essere parallelizzata per ottenere prestazioni migliori;
  - Lo schema può essere incorporato in protocolli ed applicazioni esistenti, con meno modifiche possibili.
- **Semplicità:**
  Lo schema proposto sarà valutato sulla base della semplicità ed eleganza del suo design.
- **Adozione:**
  Fattori che prevengano l'adozione diffusa dell'algoritmo avranno un impatto negativo sulla valutazione. Tra queste si ricordano in particolare i problemi legati alla proprietà intellettuale.

### 2.3.4 Processo di Valutazione

L'analisi del NIST includerà come minimo:

- Controllo di correttezza:
  I valori KAT inclusi nella proposta verranno utilizzati per verificare la correttezza delle implementazioni di riferimento e ottimizzate.

- Test di efficienza:
  Utilizzando le versioni ottimizzate, il NIST intende effettuare diversi test relativi alle prestazioni degli schemi.

- Altri test:
  Il NIST si riserva la libertà di effettuare eventuali altri test che potrà ritenere necessari.

I test sopracitati verranno eseguiti sulla *NIST PQC Reference Platform*, un calcolatore Intel x64 che esegue Windows o Linux e che supporta il compilatore GCC. Tuttavia, il NIST prevede di testare i protocolli anche su altre piattaforme, come per esempio processori a 8 bit.

# 3 Indicazioni e Linee Guida

Questa sezione raccoglie una serie di considerazioni personali, indicazioni e suggerimenti relativi a questioni importanti e delicate che potrebbero trasformarsi in un ostacolo per la standardizzazione di una proposta.
In particolare, si osserveranno i seguenti quattro punti:

1. Questioni legate alla proprietà intellettuale e alla promozione delle proposte.
2. Proposta di design semplici e chiari.
3. Tradeoff tra costo e sicurezza in fase d'implementazione. Definizione dell'obiettivo del protocollo: general purpose o specializzato?
4. Scelta e motivazione dei parametri previsti dagli algoritmi.

La sezione corrente verrà accompagnata da esempi notevoli di algoritmi che hanno partecipato al processo di standardizzazione.

## 3.1 Proprietà Intellettuale e Promozione [NISd]

Sin dal primo documento risalente al 2016, il NIST ha sempre posto particolare attenzione al tema della proprietà intellettuale, in quanto possibile causa di impedimenti in fase di valutazione e rallentamenti in un'eventuale fase futura di implementazione. Lo scopo del NIST è infatti quello di rendere ciascuna proposta libera e disponibile a livello mondiale sia per la valutazione che l'eventuale uso futuro.
Data la natura e il tipo di utilizzo degli algoritmi crittografici, l'obiettivo del NIST rispetto alla standardizzazione di algoritmi post-quantum resistant è quello di identificare protocolli tecnicamente robusti e favorirne la diffusione e adozione. Il NIST non si oppone in principio ad algoritmi o implementazioni che necessitino di una richiesta di brevetto laddove ci siano motivazioni tecniche valide a giustificare questo approccio, tuttavia durante la valutazione terrà presente ogni possibile fattore che possa ostacolare l'adozione diffusa del protocollo in questione.
NIST ha osservato che la disponibilità royalty-free dei crittosistemi e delle loro implementazioni ha favorito l'adozione degli standard crittografici nel passato. Per questa ragione, il NIST crede che sia estremamente importante che il processo di standardizzazione produca protocolli implementabili liberamente ove necessari. Come parte dello sforzo di valutazione, il NIST considererà le assicurazioni date dai candidati e dai proprietari dei brevetti negli statement allegati alle proposte. Preferirà protocolli nei quali la presenza di una licenza non comporti compensazioni monetarie, che presentino termini d'utilizzo ragionevoli, e che siano palesemente privi di ingiuste discriminazioni.
In particolare, ai candidati è richiesto di allegare, ove applicabili, tre statement relativi alla questione della proprietà intellettuale:

- Statement generale da parte di ogni candidato,
- Statement del proprietario del brevetto,
- Statement del proprietario delle implementazioni di riferimento e/o ottimizzate.

Data la complessità legale relativa alle leggi degli Stati Uniti d'America, che esula dallo scopo di questo documento, per prendere visione dei sopracitati statement si rimanda al documento [NISd], e ad un'eventuale consulenza esperta e professionale in caso di dubbi o complessità in fase di compilazione.

La seguente citazione è tratta dal documento "Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process" [NISb], ed è un buon esempio per sottolineare la preferenza del NIST verso protocolli slegati da brevetti e potenziali problemi di proprietà intellettuale:

*"NIST sees structured lattice-based schemes as very promising. As NTRU is such a scheme but based on a different security assumption than RLWE or MLWE, it provides some diversity to the collection of finalists. While NTRU has a small performance gap in comparison to KYBER and SABER,* ***its longer history was an important factor in NIST's decision to select NTRU as a finalist. Due to its longer history, NTRU has less risk of unexpected intellectual property claims.*** *NIST expects that, at most, only one of these candidates—KYBER, SABER, or NTRU—will be standardized at the end of the third round. In the event that new cryptanalytic or intellectual property issues threaten the future of KYBER and SABER, NTRU would be seen as a more appealing finalist."*

Tuttavia, va precisato che alla conclusione del terzo round KYBER è stato comunque selezionato per la standardizzazione grazie alle prestazioni molto migliori rispetto ai protocolli concorrenti.

## 3.2 Design Chiari e Semplici

Il NIST ribadisce spesso nei suoi documenti relativi al processo di standardizzazione la preferenza nei confronti di protocolli dal design semplice, chiaro e ben compreso. Sono diversi i motivi per cui accade questo:

- **Sicurezza rispetto ad errori involontari**
  Nel caso il protocollo matematico di base o il design fossero particolarmente complicati, inevitabilmente l'implementatore si troverebbe nella condizione di aver a che fare con un compito per forza di cose complicato, che potrebbe condurlo ad inserire inconsapevolmente errori nel codice. Se non scoperti in tempo, questi potrebbero rivelarsi catastrofici in termini di sicurezza, ed allargare la base d'attacco per possibili attaccanti.

Nonostante la semplicità non garantisca automaticamente la correttezza dell'implementazione, l'invito è di scegliere basi e design semplici che rendano i programmatori meno proni ad errori inconsapevoli.

- **Sicurezza rispetto a possibili backdoor e nuovi attacchi**
  Protocolli basati su schemi crittografici molto nuovi potrebbero non venir compresi a fondo e risultare rischiosi in due versi. Da un lato potrebbe accadere che il candidato abbia profonda e completa comprensione dello schema, approfittando di questo fatto per introdurre backdoor nella speranza che la commissione di valutazione e il pubblico analizzante non se ne accorgano, a causa della difficoltà e novità del problema su cui è strutturato il protocollo. Dall'altro, eventuali incomprensioni da parte del candidato potrebbero venir scoperte e sfruttate in futuro da attaccanti con alle spalle più ricerca sullo schema in questione.
  Il NIST predilige quindi protocolli con schemi crittografici ben documentati e analizzati.

- **Sicurezza rispetto ad attacchi legacy**
  Ovviamente risulterà immediatamente chiaro al lettore che basare il proprio protocollo su schemi deboli o noti per poter essere attaccabili, non è una scelta saggia. Allo stesso modo non è opportuno realizzare protocolli con alcuna parte debole rispetto ai computer quantistici.
  Inoltre, il NIST ha esplicitamente espresso la preferenza nei confronti di schemi che non abbiano subito numerosi o pesanti redesign come forma di patch per problemi di sicurezza scoperti nel corso del tempo.

- **Facilità di comprensione e valutazione**
  Come già espresso nei punti precedenti, un design semplice è esplicitamente preferito dal NIST rispetto ad uno più complicato. Questo ha lo scopo di agevolare la comprensione sia da parte della commissione di esperti del NIST, che del pubblico analizzante, garantendo migliori basi per una valutazione più attenta e consapevole.

- **Facilità di implementazione**
  Facendo seguito al punto precedente, è possibile ipotizzare che un protocollo dal design semplice sia anche più semplice da implementare (senza errori). Pertanto, nell'ottica futura di diffusione e standardizzazione, la semplicità è da tenere comunque e sempre presente.

Appare chiaro da quanto appena riportato, che il candidato debba puntare alla semplicità in fase di realizzazione di una proposta che abbia il potenziale di essere standardizzata.

Per fare un esempio della preferenza del NIST nei confronti della semplicità, si riporta un breve estratto dal documento "Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process" [NISb], nel quale viene esplicitamente apprezzata la maggiore semplicità di un algoritmo

rispeto al suo diretto concorrente:

*"CRYSTALS-DILITHIUM was one of three lattice-based signature schemes in the second round. The security of DILITHIUM relies on the hardness of the MLWE and module short integer solutions problems (MSIS) and follows the Fiat-Shamir with aborts technique.* ***DILITHIUM uses the same modulus and ring for all parameter sets and samples via the uniform distribution, which results in a simpler implementation than its main competitor, FALCON.*** *"*

## 3.3 Tradeoff Costo/Sicurezza e Scopo del Protocollo

In diversi frangenti è importante avere ben presente lo scopo per il quale si realizzerà il protocollo: si punta a creare una proposta estremamente sicura a discapito della velocità e del costo d'implementazione ed utilizzo? Potrebbe essere il caso ad esempio per applicazioni mediche e finanziarie. Oppure si ha in mente un'implementazione agile e poco costosa per ambienti a basso rischio e bassa potenza? Ad esempio per processori ad 8-bit o per le smart-card.
Il NIST richiede di esplicitare questo tradeoff, e se possibile presentare molteplici spettri d'utilizzo della propria proposta in fase di:

- Presentazione delle versioni di riferimento ed ottimizzata della propria proposta.
- Scelta dei parametri che potrebbero comportare implementazioni più sicure o più agili. Il NIST stesso ha comunicato che la valutazione avverrà anche fornendo parametri diversi da quelli suggeriti per verificare il comportamento del protocollo nei confronti del problema correntemente discusso.
- Definizione dei livelli di sicurezza. È utile presentare varianti che soddisfino i livelli più bassi (1-3) di sicurezza, ma che al contempo siano ben ottimizzate, insieme a versioni più sicure e più lente.

Il NIST ha fin da subito affermato che è aperto alla possibilità di standardizzare più algoritmi appartenenti alla stessa categoria, qualora questi siano specificatamente realizzati per una particolare applicazione, in modo da affiancarli a protocolli più general-purpose e cercare di soddisfare tutte le possibili necessità dei futuri utilizzatori.
La nuova call for proposals nasce proprio a tal riguardo: nel terzo report sul processo di standardizzazione [NISc], il NIST ha espresso il desiderio di ricevere nuove proposte per la firma digitale, che si concentrino su schemi con firme corte e verifiche veloci, ad esempio per l'utilizzo nel web.

## 3.4 Scelta e motivazione dei parametri

Il NIST ha più volte ribadito che la scelta e la motivazione dei parametri utilizzati è estremamente importante, in particolare per quelli modificabili.

Innanzitutto, la scelta va giustificata in merito alla motivazione per cui certi parametri sono stati scelti e utilizzati, così da poter verificare ed escludere che si tratti di valori identificati malevolmente per nascondere delle backdoor.
In secondo luogo è necessario giustificare la scelta in termini del tradeoff sicurezza-prestazioni osservato nel paragrafo precedente. In particolare, nel caso si parametri modificabili, il candidato è tenuto a specificare degli insiemi con valori concreti da far assumere ai parametri, esplicitando cosa ciascun insieme comporti in termini di sicurezza e performance. È inoltre invitato a offrire uno spettro quanto più ampio ed esaustivo di insiemi di parametri rispetto al tradeoff sopra citato.

# 4 Conclusioni

Per concludere la trattazione, si procede a delineare tre paragrafi che racchiudano il messaggio che si è voluto trasmettere e che offrano uno sguardo all'immediato futuro della competizione e al futuro della crittografia post-quantum.

## 4.1 Riepilogo delle informazioni chiave

I seguenti punti elencano i concetti presentati nei capitoli precedenti, che si ritiene essere di massima importanza per realizzare una proposta competitiva e vincente:

- Il candidato deve possedere una profonda comprensione dell'ambiente e tecnologie quantistici, e degli algoritmi che rischiano di rendere inefficace la crittografia tradizionale.
  Allo stesso modo, deve avere una profonda conoscenza delle basi matematiche e degli schemi su cui andrà a realizzare il proprio protocollo.

- Il candidato deve rispettare attentamente tutte le scadenze, i requisiti e le metodologie di sottomissione imposte dal NIST per la candidatura del proprio protocollo. Un buono schema che non viene considerato a causa di errori di sottomissione è intrinsecamente un protocollo senza futuro.
  L'invito è quindi di tenersi costantemente aggiornati rispetto a notizie ed indicazioni ufficiali da parte del NIST [NISa].
  Si consiglia inoltre di affidarsi a consulenza legale esperta per quanto riguarda la compilazione degli statement relativi alla proprietà intellettuale. La conoscenza della lingua inglese, o una relativa consulenza, sono inoltre indispensabili.

- Il candidato dovrà in ogni momento tenere presente i criteri di valutazione e le piattaforme per cui sta sviluppando il proprio protocollo. Un buon design che offra pessime prestazioni in fase di valutazione, verrà quasi certamente scartato.

- Qualora possibile, al candidato si suggerisce di presentate una proposta libera da vincoli di proprietà intellettuale, o quantomeno di renderli il più possibile laschi. Richieste di compenso, segretezza e possibili difficoltà di distribuzione e adozione sono elementi che influiscono negativamente nella valutazione.

- La semplicità e la chiarezza, sia nel design che nella documentazione, dovrebbero essere sempre al centro dei pensieri del candidato in fase di preparazione della proposta. Il NIST valuta molto positivamente questa caratteristica.

- Il candidato dovrà tener presente nella fase di scelta dei parametri, di autovalutazione della sicurezza, e della definizione del tradeoff tra costo e sicurezza del tipo di schema che sta realizzando: general purpose o dedicato ad un utilizzo specifico?

## 4.2 Lo Stato Attuale della Competizione [NISc]

Al momento della scrittura del presente documento, si è appena concluso il terzo round del processo di standardizzazione, pertanto se ne riportano i risultati e le prospettive per il futuro.
Dopo sei anni dall'avvio della competizione, il NIST ha annunciato i primi algoritmi a chiave pubblica che verranno standardizzati:

- CRYSTALS-KYBER per il key-establishment,
- CRYSTALS-Dilithium, FALCON e SPHINCS$^+$ per la firma digitale.

Inoltre, i seguenti algoritmi per cifratura a chiave pubblica e key-establishment verranno ulteriormente analizzati durante il quarto round del processo di standardizzazione:

- BIKE,
- Classic McEliece,
- HQC,
- SIKE.

Il NIST creerà insieme ai candidati nuove bozze di standardizzazione, e cercherà opinioni sui valori dei parametri presenti nei rispettivi parametri, in particolare valori per il primo livello di sicurezza. Una volta terminata questa fase, gli standard saranno pubblicati per ricevere l'analisi pubblica, successivamente alla quale il NIST procederà alla revisione degli stessi. L'ultima fase di revisione, approvazione e diffusione avverrà immediatamente dopo: il NIST prevede di terminare il processo entro il 2024.

La novità più interessante però risiede nella decisione del NIST di divulgare nel corso dell'estate 2022 una nuova call for proposals per algoritmi di firma digitale basati su schermi di tipo non-structured lattice, e/o con firme brevi e verifiche veloci. Indicativamente il termine delle sottomissioni sarà nel 2023. Per quanto la competizione sarà molto più ristretta a quella originale, il NIST si aspetta che ci vorranno comunque anni prima che questa venga portata a termine.

## 4.3 Oltre la Competizione: Cenno al Futuro della Crittografia Post-Quantum

Seguendo l'infografica realizzata dallo U.S. Department of Homeland Security in collaborazione col NIST [Hom], si offre una breve panoramica dei prossimi step per quanto riguarda la predisposizione dei sistemi informatici alla crittografia post-quantum.

- 2021-2023: Inventario e definizione delle priorità.
  In particolare questo step si sviluppa nei sette punti seguenti:

1. Avvio di contatti con le organizzazioni di standardizzazione per essere al corrente degli sviluppi nel campo post-quantum, e iniziare a prepararsi alla transizione.
2. Inventario dei dati critici perchè siano i primi ad essere protetti dai nuovi protocolli.
3. Inventario delle tecnologie crittografiche utilizzate, per capire quali debbano essere rimpiazzate.
4. Identificazione degli standard interni per verificare che siano compatibili con i nuovi protocolli.
5. Identificazione, in particolare, dal passo 3., dei protocolli a chiave pubblica utilizzati, in quanto particolarmente vulnerabili rispetto agli algoritmi quantistici.
6. Definizione delle priorità di sostituzione in base al valore delle informazioni e/o dei sistemi interessati, sulla base degli inventari e delle identificazioni precedenti.
7. Pianificazione della transizione alla luce dei passi precedenti.

- 2024: Conclusione del processo di standardizzazione del NIST e pubblicazione dei protocolli post-quantum.
- 2024-2030: Transizione ai protocolli post-quantum.
- 2030: Potenzialmente disponibile il primo computer quantistico crittograficamente rilevante.

# Bibliografia


[BBD09] Daniel J. Bernstein, Johannes Buchmann e Erik Dahmen. *Post-Quantum Cryptography*. Berlin, Heidelberg: Springer-Verlag, 2009.

[BL17] Daniel J. Bernstein e Tanja Lange. «Post-Quantum Cryptography». In: *Nature* 549 (2017), pp. 188–194. DOI: doi:10.1038/nature23461.

[Gre] Matthew Green. *EUF-CMA and SUF-CMA*. URL: https://blog.cryptographyengineering.com/euf-cma-and-suf-cma/.

[Hom] U.S. Department of Homeland Security. *Preparing for Post-Quantum Cryptography: Infographic*. URL: https://www.dhs.gov/sites/default/files/publications/post-quantum_cryptography_infographic_october_2021_508.pdf.

[Kum] Dr. Manish Kumar. *Post-Quantum Cryptography Algorithm's Standardization and Performance Analysis*. URL: https://arxiv.org/ftp/arxiv/papers/2204/2204.02571.pdf.

[NISa] NIST. *Post-Quantum Cryptography - News and Updates*. URL: https://csrc.nist.gov/Projects/post-quantum-cryptography/news.

[NISb] NIST. *Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process*. URL: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8309.pdf. NIST IR 8309.

[NISc] NIST. *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*. URL: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413.pdf. NIST IR 8413.

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