Crittografia post-quantum e quantistica la cybersicurezza nazionale nell'era dei computer quantistici

Roma, 23.05.2025

SERVIZIO CRITTOGRAFIA – DIVISIONE ALGORITMI E APPLICAZIONI CRITTOGRAFICHE

Agenda

- Crittografia e Quantum computing
- Minaccia quantistica
- Contromisure
- Transizione quantum-safe

Due categorie di crittografia

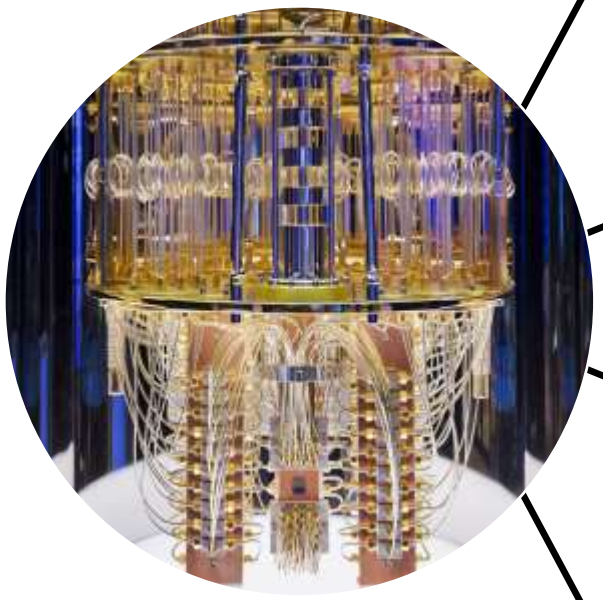
Crittografia Simmetrica

- **Una sola chiave:**
  sia per cifrare,
  che per decifrare
- **Veloce**, adatta a cifrare
  grandi quantità di dati
- Richiedono **un canale sicuro** per condividere la chiave
- Alcuni algoritmi:
  AES (Advanced Encryption Standard),
  E0 (Bluetooth),
  A5/3 (GSM)
- Esempi: cifratura di comunicazioni (dati *in-transit*) o storage (dati *at-rest*)

Crittografia a Chiave Pubblica

- **Due chiavi**:
  una per cifrare (pubblica)
  e una per decifrare (privata)
- Lenta, adatta a processare piccole quantità di dati
- **Nessuna comunicazione** precedente necessaria tra le parti
- Alcuni algoritmi:
  RSA (Rivest-Shamir-Adleman),
  DSA (Digital Signature Algorithm),
  Diffie-Hellman
- Esempi: firma digitale,
  scambio sicuro di chiavi simmetriche

La computazione quantistica



Qubit

- Generalizzazione **quantistica** del bit classico
- Assume un valore che è simultaneamente 0 e 1

Progresso

- Alte prestazioni nell'analisi di big data
- Risoluzione dei problemi di **ottimizzazione**

Algoritmi

- Sono già stati **teorizzati** algoritmi quantistici
- Si sta lavorando alla loro implementazione

Sviluppo

- Problemi ingegneristici nella realizzazione
- **Scalabilità** dei computer e **affidabilità** dei qubit

La minaccia quantistica

Crittografia Simmetrica

- L'algoritmo quantistico di **Grover** risolve efficientemente il problema della ricerca di un elemento in un database
- In crittografia, **dimezza** la sicurezza della chiave contro gli attacchi a forza bruta
- Per evitare problemi di sicurezza è sufficiente **raddoppiare** la lunghezza della chiave

Crittografia a Chiave Pubblica

- L'algoritmo quantistico di **Shor** risolve efficientemente un problema matematico molto difficile da risolvere con gli strumenti classici
- In crittografia, rompe due problemi alla base di molti algoritmi: **fattorizzazione** (RSA) e **logaritmo discreto** (DH, ECC)
- Servono nuovi algoritmi che siano resistenti agli attacchi quantistici, **post-quantum** o **quantistici**

Contromisure: crittografia quantistica

Idea

- Sfruttare i **principi quantistici** per comunicazioni sicure
- Quantum Key Distribution (**QKD**)
- In caso di **intercettazione** la chiave viene scartata

Realizzazione

- **Fibra ottica**, canali **satellitari**
- Servono **ripetitori** per il segnale che perde potenza

Problematiche

- **Costi** di realizzazione rete quantistica
- **Sicurezza** nodi ripetitori
- Necessità di un **canale classico sicuro**

Contromisure: crittografia *post-quantum*

Gli algoritmi post-quantum sono sistemi **classici** che si basano su nuove costruzioni matematiche ritenute **sicure** contro attacchi classici e quantistici

Reticoli
- Tempi ridotti
- Dimensioni moderate

Codici
- Tempi moderati
- Dimensioni elevate

Funzioni di hash
- Tempi moderati
- Dimensioni moderate

Sistemi multivariati
- Tempi ridotti
- Dimensioni elevate

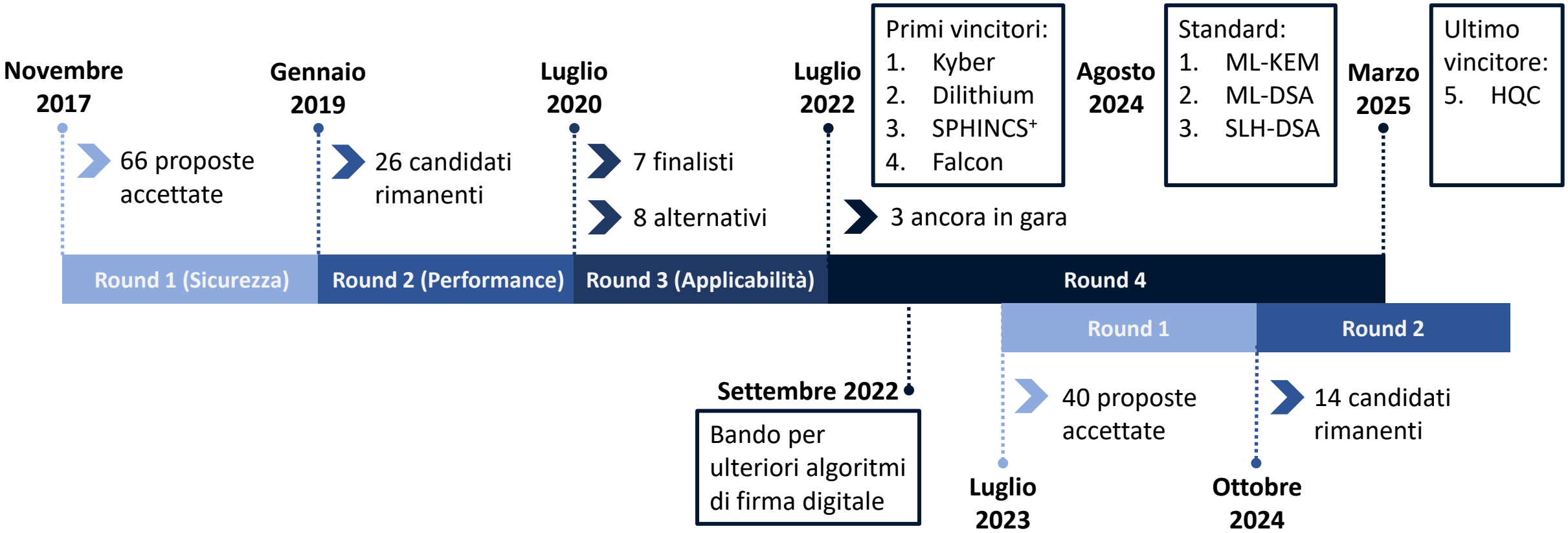
Isogenie
- Tempi elevati
- Dimensioni ridotte

MPC-in-the-Head
- Tempi moderati
- Dimensioni moderate

Perché diverse famiglie?
- Proprietà diverse per adattarsi a diversi contesti specifici
- Evitare che la sicurezza dipenda da un'unica scelta

Competizione NIST per la crittografia post-quantum

Alla conferenza **PQCrypto 2016** il NIST ha pubblicizzato una competizione per scegliere nuovi algoritmi di **cifratura a chiave pubblica** e **schemi di firma digitale.**



La transizione verso il post-quantum

Inventario

- **Identificare** e mappare i crittosistemi in uso

Priorità

- Stabilire l'ordine di **priorità** degli asset da migrare, sulla base di una **analisi del rischio**

Sostituzione

- **Avviare** la sostituzione degli algoritmi crittografici
- **Integrare** i processi standard di *vulnerability management*

Crittografia ibrida

- Combinare la sicurezza di algoritmi **classici** e **post-quantum**

Cripto agilità

- Rendere semplice la **sostituzione** dei cifrari all'interno dei sistemi

La transizione nell'Unione Europea

11 aprile 2024	**Raccomandazione** della Commissione Europea per la formazione di un gruppo di lavoro sulla crittografia post-quantum
Obiettivi	Stilare una **tabella di marcia** per la transizione coordinata tra gli Stati Membri dell'Unione Europea
Lavori in corso	Documento di **linea guida** per gli Stati Membri per la stesura delle tabelle di marcia nazionali

La possibile tabella di marcia per l'Italia

Il ruolo di ACN

Sensibilizzare in merito alla minaccia quantistica e alle possibili soluzioni

Stabilire strumenti, metodologie e algoritmi per supportare le organizzazioni nella transizione

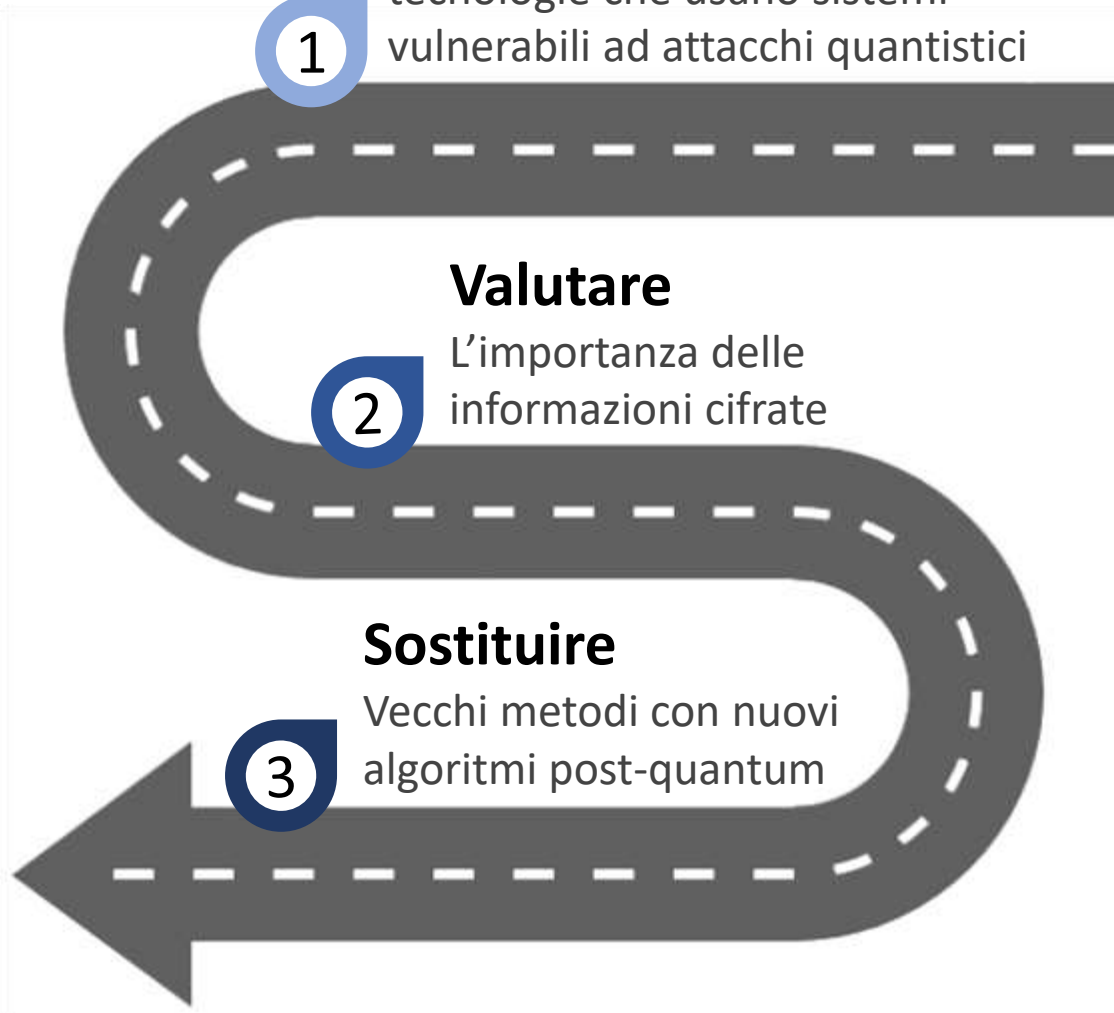
Elaborare, di concerto con gli altri stakeholder nazionali, un piano di transizione nazionale per soggetti pubblici e infrastrutture critiche

Scadenze

2026

Critici: 2030

2035



Documenti informativi di ACN

Evidenziano l'**urgenza** di avviare la **transizione** di tutti i sistemi informativi verso una crittografia **resistente** agli attacchi quantistici

In collaborazione con le principali **agenzie per la cybersicurezza europee**

Grazie


AGENZIA PER LA CYBERSICUREZZA NAZIONALE
ACN
SAPIENTIA ADIUVAT