Migrazione verso la Crittografia Post-Quantum

Servizio Certificazione e Vigilanza

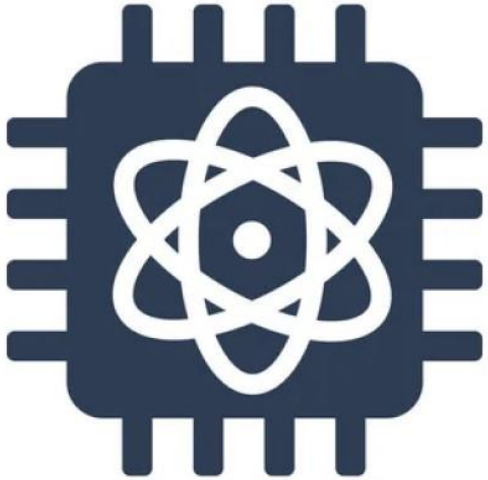
Due categorie di crittografia

Crittografia Simmetrica

La Minaccia Quantistica

Sviluppi **pratici**:
hanno ancora una **limitata** potenza computazionale

Sviluppi **teorici**:
esistono già **algoritmi** quantistici



Computer Quantistico

Progressi importanti:
surclasseranno i computer classici nell'ottimizzazione

Seria **minaccia**:
romperanno la moderna crittografia a chiave pubblica

Due categorie di crittografia

Crittografia Simmetrica

Crittografia post-quantum – In generale

Per la crittografia a chiave pubblica si sfruttano problemi con complessità **NP**:

- la risoluzione richiede tempo esponenziale
  - ➢ **funzione one-way**
- la verifica di una soluzione è polinomiale (Non-deterministic Polynomial time)
  - ➢ **decifratura efficiente**

Fattorizzazione e **logaritmo discreto** sono **NP** ma non c'è prova che siano **NP-hard**.
Un problema è **NP-hard** se ogni problema **NP** è polinomialmente riducibile ad esso.

Per la crittografia post-quantum conviene usare problemi **NP-complete**:

- sono **NP**, quindi consentono la ricostruzione del messaggio in chiaro
- sono **NP-hard**, quindi la loro risoluzione comporterebbe quella di ogni NP

Crittografia post-quantum – Reticoli

Gli algoritmi post-quantum si dividono principalmente in diverse macrocategorie.

Problemi sui reticoli

$$L = \{\sum a_i \boldsymbol{b}_i, a_i \in \mathbb{Z}\} \subset \mathbb{R}^n$$

- **SVP** (Shortest Vector Problem): trovare il più piccolo vettore non nullo in L, la cui lunghezza è $\lambda(L)$
- $\mathbf{SVP}_\gamma$ (versione approssimata): trovare un vettore di lunghezza $\gamma \cdot \lambda(L)$, se $\gamma \geq 1$ è **NP-hard**
- **LWE** (Learning With Errors): dati $\boldsymbol{B} = (\boldsymbol{b}_i)$ e $\boldsymbol{t} = \boldsymbol{B} \cdot \boldsymbol{s}$ con $\|\boldsymbol{s}\|$ piccolo, trovare $\boldsymbol{s}$ è un problema **NP-hard**

Crittografia basata sui reticoli
(PKE/KEM, firme digitali)

- Richiede **tempi** di esecuzione **ridotti**
- Utilizza chiavi di **grandezza media**
- Si basa su $\mathbf{SVP}_\gamma$ o **LWE**, cioè problemi matematici la cui **difficoltà** è stata **dimostrata teoricamente**

Crittografia post-quantum – Codici

Gli algoritmi post-quantum si dividono principalmente in diverse macrocategorie.

Problemi sui codici

$C \subset \mathbb{F}_2^n$ codice lineare

$t = \left\lfloor \frac{d-1}{2} \right\rfloor$ errori correggibili

$\boldsymbol{H} \in \mathbb{F}_2^{m,n}$ matrice di controllo di parità

$\boldsymbol{s} = \boldsymbol{H} \cdot (\boldsymbol{x} + \boldsymbol{e}) = \boldsymbol{H} \cdot \boldsymbol{e}$ sindrome di $\boldsymbol{e}$

- **MLD** (Maximum Likelihood Decoding): data la sindrome $\boldsymbol{s}$ trovare l'errore $\boldsymbol{e}$ di peso t è un problema **NP-hard**
- Hamming e rango sono i pesi più utilizzati

Crittografia basata sui codici (PKE/KEM)

- Richiede **tempi** di esecuzione **moderati**
- Utilizza chiavi di **grandezza elevata**
- Si basa su **MLD** che è un problema matematico la cui **difficoltà** è stata **dimostrata teoricamente**

Crittografia post-quantum – Hash

Gli algoritmi post-quantum si dividono principalmente in diverse macrocategorie.

Funzioni di hash

$$h: \{0,1\}^* \rightarrow \{0,1\}^n$$

- Resistenza alla preimmagine
- Resistenza alla seconda preimmagine
- Resistenza alle collisioni

Firma effimera

Le chiavi $\left(\mathrm{sk}, h(\mathrm{sk})\right)$ si utilizzano una sola volta

Merkle tree

Ogni foglia ha l'hash di un blocco di dati e ogni nodo interno ha l'hash dei nodi figli

Crittografia basata su hash
(firme digitali)

- Richiede **tempi** di esecuzione **elevati**
- Utilizza chiavi di **grandezza ridotta**
- Si basa sulle proprietà delle hash la cui **difficoltà** è stata **ottenuta praticamente**

Crittografia post-quantum – In breve

Gli algoritmi post-quantum si dividono principalmente in diverse macrocategorie.

Crittografia basata sui reticoli

- Richiede **tempi** di esecuzione **ridotti**
- Utilizza chiavi di **grandezza media**
- Si basa su problemi matematici la cui **difficoltà** è stata **dimostrata teoricamente**

Crittografia basata sui codici

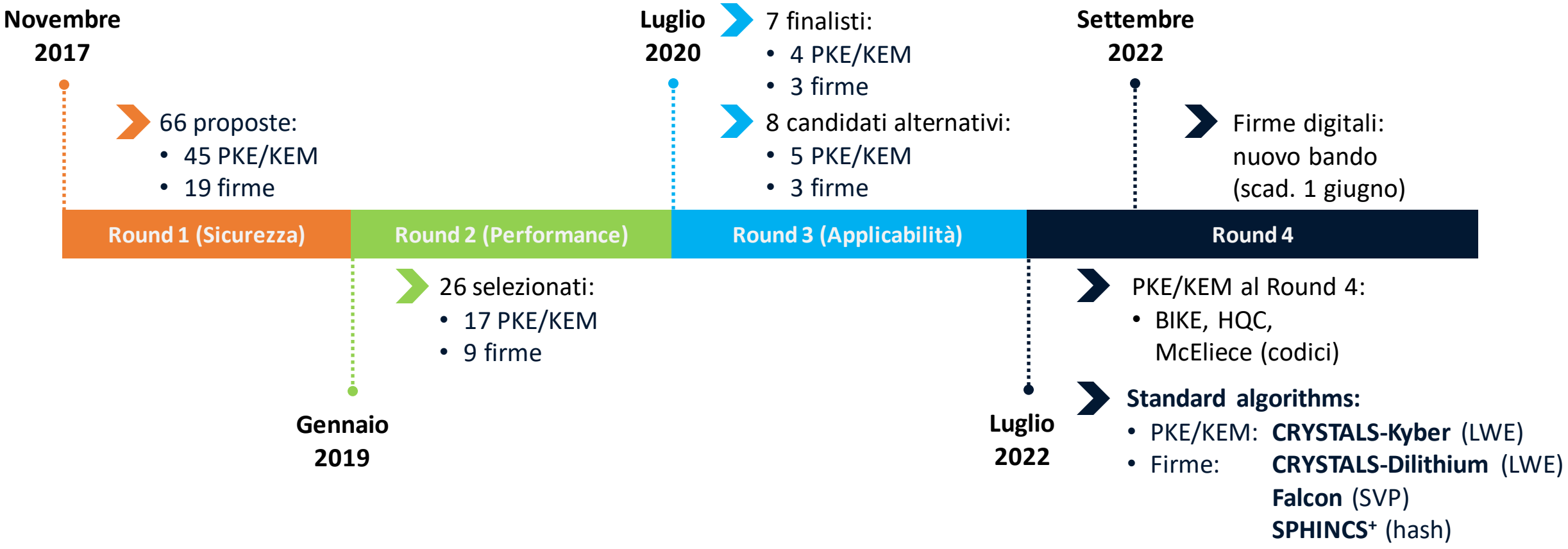
- Richiede **tempi** di esecuzione **moderati**
- Utilizza chiavi di **grandezza elevata**
- Si basa su problemi matematici la cui **difficoltà** è stata **dimostrata teoricamente**

Crittografia basata su funzioni di hash

- Richiede **tempi** di esecuzione **elevati**
- Utilizza chiavi di **grandezza ridotta**
- Si basa su problemi matematici la cui **difficoltà** è stata **ottenuta praticamente**

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.**



Comparazioni con i crittosistemi classici

Algoritmo	Liv. NIST	PK (bytes)	Cifrato (bytes)	Gen. Chiavi (ms)	Cifratura (ms)	Decifratura (ms)
DH (campi finiti)	0	256	256	203.92	204.08	-
ECDH	0	32	32	8.43	17.69	-
Kyber512	1	800	768	8.13	6.24	3.42
BIKE	1	1541	1573	200.62	25.97	411.31
HQC128	1	2249	4481	30.20	50.68	72.77

Dimensioni e tempi degli algoritmi di cifratura a chiave pubblica moderni e post-quantum

Algoritmo	Liv. NIST	PK (bytes)	Firma (bytes)	Gen. Chiavi (ms)	Gen. Firma (ms)	Verifica (ms)
RSA sign	0	256	256	462.85	448.25	12.50
ECDSA	0	32	32	8.43	12.31	25.19
SPHINCS+128small	1	32	7856	8674.00	66239.00	61.59
SPHINCS+128fast	1	32	17088	137.75	3361.00	190.17
Falcon512	1	897	666	1266.67	243.88	3.28
Dilithium2	2	1312	2420	12.06	25.40	9.57

Dimensioni e tempi degli algoritmi di firma digitale moderni e post-quantum

Transizione, quando?

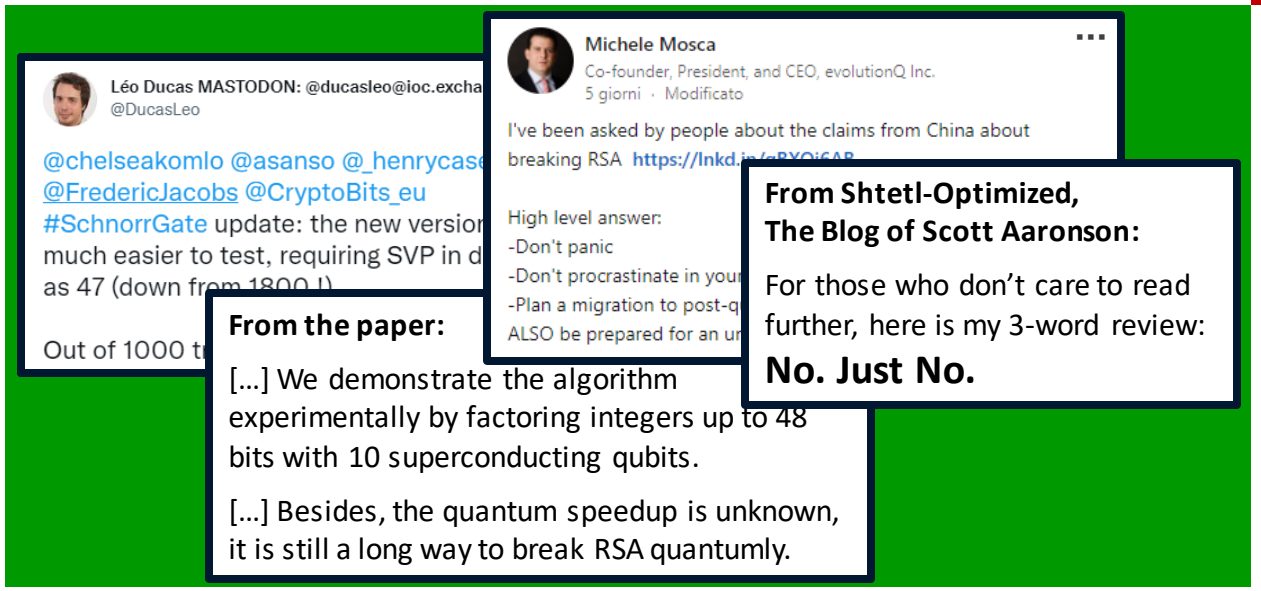
A Dicembre 2023 un team di ricercatori della Repubblica Popolare Cinese ha affermato di aver sviluppato un attacco a RSA: migliorando l'algoritmo di fattorizzazione di **Schnorr** con il **Quantum Approximate Optimization Algorithm** anche un computer quantistico attuale sarebbe sufficiente.

Factoring integers with sublinear resources on a superconducting quantum processor

Bao Yan,[1,2,*] Ziqi Tan,[3,*] Shijie Wei,[4,*] Haocong Jiang,[5] Weilong Wang,[1] Hong Wang,[1] Lan Luo,[1] Qianheng Duan,[1] Yiting Liu,[1] Wenhao Shi,[1] Yangyang Fei,[1] Xiangdong Meng,[1] Yu Han,[1] Zheng Shan,[1] Jiachen Chen,[3] Xuhao Zhu,[3] Chuanyu Zhang,[3] Feitong Jin,[3] Hekang Li,[3] Chao Song,[3] Zhen Wang,[3,†] Zhi Ma,[1,‡] H. Wang,[3] and Gui-Lu Long[2,4,6,7,§]

[1]*State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China*
[2]*State Key Laboratory of Low-Dimensional Quantum Physics and Department of Physics, Tsinghua University, Beijing 100084, China*
[3]*School of Physics, ZJU-Hangzhou Global Scientific and Technological Innovation Center, Interdisciplinary Center for Quantum Information, and Zhejiang Province Key Laboratory of Quantum Technology and Device, Zhejiang University, Hangzhou 310000, China*
[4]*Beijing Academy of Quantum Information Sciences, Beijing 100193, China*
[5]*Institute of Information Technology, Information Engineering University, Zhengzhou 450001, China*
[6]*Beijing National Research Center for Information Science and Technology and School of Information Tsinghua University, Beijing 100084, China*
[7]*Frontier Science Center for Quantum Information, Beijing 100084, China*

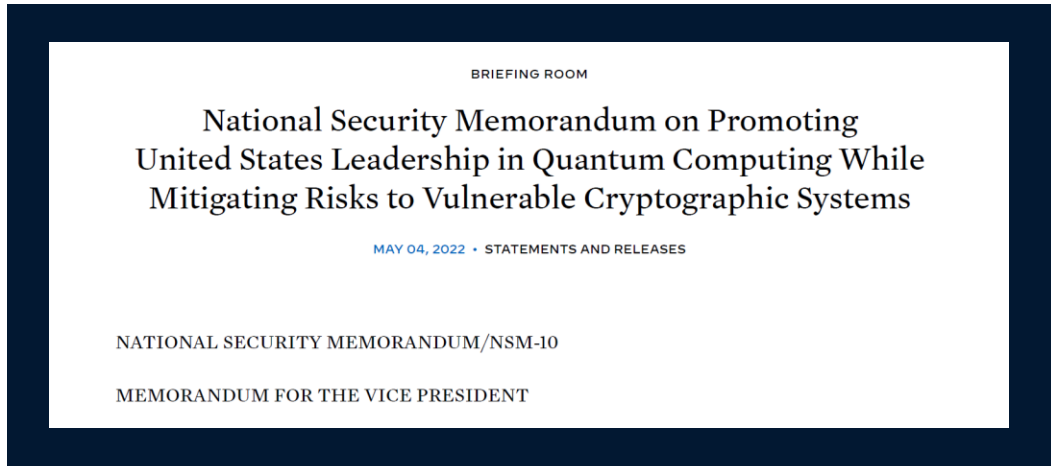
Shor's algorithm has seriously challenged information security based on public key cryptosystems. However, to break the widely used RSA-2048 scheme, one needs millions of physical qubits, which is far beyond current technical capabilities. Here, we report a universal quantum algorithm for integer factorization by combining the classical lattice reduction with a quantum approximate optimization algorithm (QAOA). The number of qubits required is $O(\log N/\log\log N)$, which is sublinear in the bit length of the integer N, making it the most qubit-saving factorization algorithm to date. We demonstrate the algorithm experimentally by factoring integers up to 48 bits with 10 superconducting qubits, the largest integer factored on a quantum device. We estimate that a quantum circuit with 372 physical qubits and a depth of thousands is necessary to challenge RSA-2048 using our algorithm. Our study shows great promise in expediting the application of current noisy quantum computers, and paves the way to factor large integers of realistic cryptographic significance.



Tuttavia, la comunità scientifica ha dichiarato che questo attacco risulta ancora **irrealizzabile**, sebbene affermazioni di questo genere siano sempre più frequenti e **non vadano sottovalutate**.

Strategia di transizione degli Stati Uniti

- Il **4 Maggio 2022**, il Presidente degli USA Joe Biden ha pubblicato un memorandum per la migrazione alla crittografia post-quantum
- Il **18 Novembre 2022**, esce la lista di algoritmi compromessi dal quantum



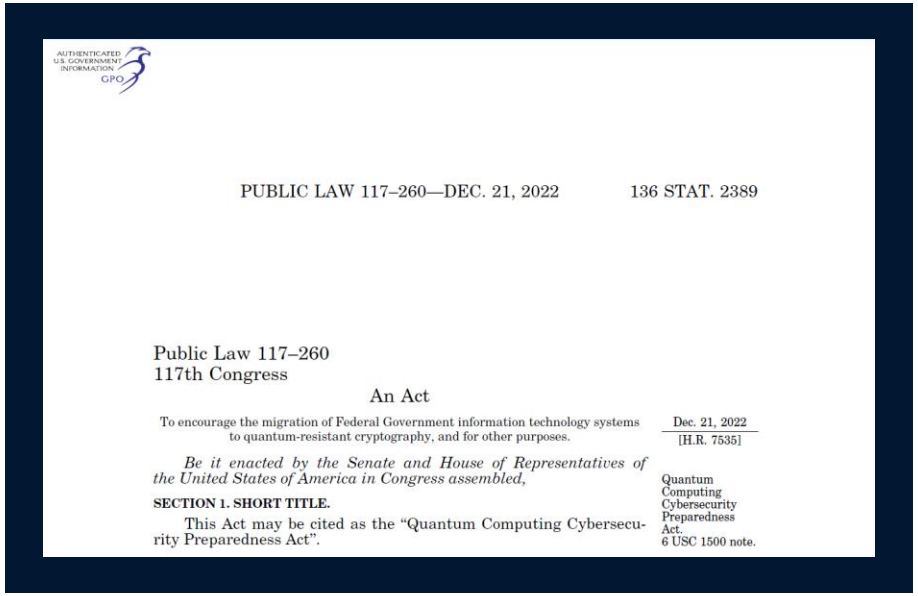
BRIEFING ROOM

National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

MAY 04, 2022 • STATEMENTS AND RELEASES

NATIONAL SECURITY MEMORANDUM/NSM-10

MEMORANDUM FOR THE VICE PRESIDENT



AUTHENTICATED U.S. GOVERNMENT INFORMATION GPO

PUBLIC LAW 117–260—DEC. 21, 2022 136 STAT. 2389

Public Law 117–260
117th Congress

An Act

To encourage the migration of Federal Government information technology systems to quantum-resistant cryptography, and for other purposes.

Dec. 21, 2022
[H.R. 7535]

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

Quantum Computing Cybersecurity Preparedness Act.
6 USC 1500 note.

SECTION 1. SHORT TITLE.

This Act may be cited as the "Quantum Computing Cybersecurity Preparedness Act".

- Il **21 Dicembre 2022**, il Senato ha approvato il "**Quantum Computing Cybersecurity Preparedness Act**" in cui venivano resi effettivi gli atti pubblicati in precedenza, ribadendo l'importanza e l'urgenza di attivare le procedure di migrazione verso algoritmi post-quantum

Strategia di transizione in Europa

- **ENISA** (European Union Agency for Cybersecurity)
  "Post-Quantum Cryptography - Integration study"
  (ottobre 2022)
- **Horizon Europe Framework Programme**
  "Transition towards Quantum-Resistant Cryptography"
  (scad. novembre 2022)

- **NCSC** (National Cyber Security Center)
  "Preparing for Quantum-Safe Cryptography" (novembre 2020)
- **BSI** (Bundesamt für Sicherheit in der Informationstechnik)
  "Migration to Post Quantum Cryptography" (maggio 2021)
- **ANSSI** (Agence Nationale de la Sécurité des Systèmes d'Information)
  "Views on the Post-Quantum Cryptography transition" (marzo 2022)
- **AIVD** (Algemene Inlichtingen- en Veiligheidsdienst)
  "The PQC Migration Handbook" (marzo 2023)

La tabella di marcia per l'Italia

Analizzare e identificare

Infrastrutture, attività, e tecnologie che usano sistemi vulnerabili ad attacchi quantistici

1

Valutare

L'importanza delle informazioni cifrate

2

Sostituire gradualmente

Vecchi metodi con nuovi algoritmi post-quantum

3

Entro il 2035

Strategia intrapresa

Gennaio 2023: ACN coordina l'avvio di un gruppo di lavoro per la transizione alla crittografia post-quantum in Italia

Q3 2023: coinvolgimento del mondo accademico nel gruppo di lavoro

Prossimi passi: elaborazione di un piano di transizione nazionale di concerto con gli organismi competenti