UNIVERSITÀ
POLITECNICA
DELLE MARCHE

—

Facoltà di Ingegneria

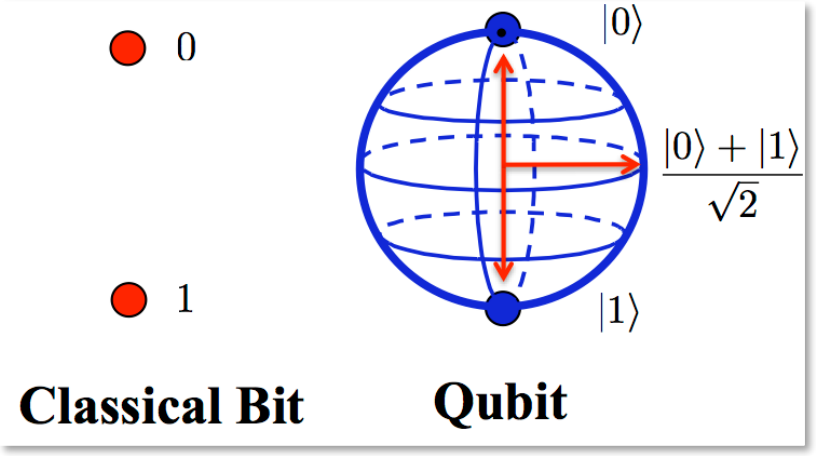
CRITTOGRAFIA POST-QUANTUM E PQCIFRIS

Marco Baldi
Dipartimento di Ingegneria dell'Informazione

m.baldi@univpm.it
www.univpm.it/marco.baldi

IL QUANTUM COMPUTER

- Teorizzato da ***Richard Feynman*** e ***Yuri Manin*** all'inizio degli anni 80

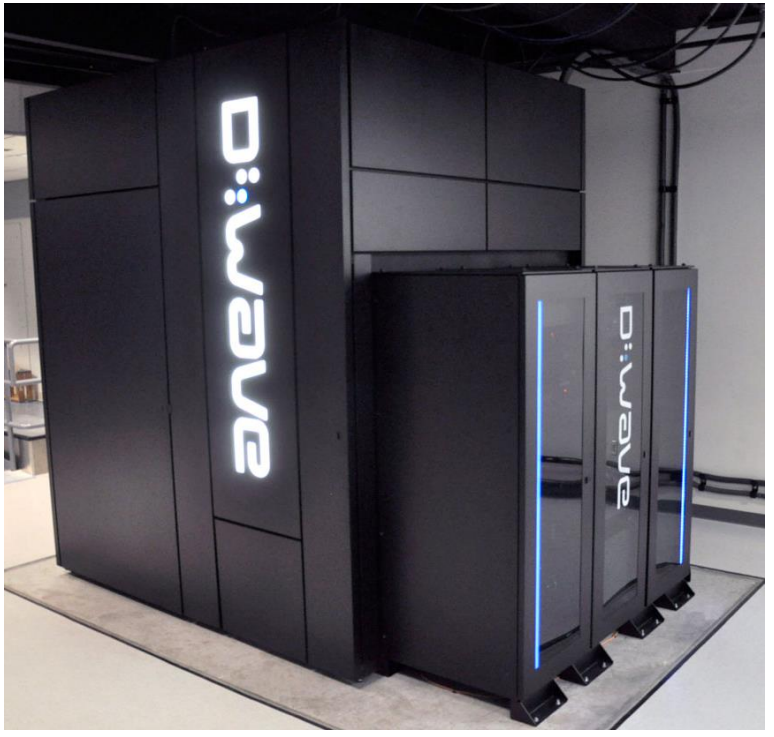


- ***Algoritmo di Shor (1994)***
  - fattorizzazione di numeri interi su quantum computer
  - dato un intero *N*, lo fattorizza in un tempo polinomiale in log *N*
  - su un computer classico il tempo è esponenziale in *N*

- ***Algoritmo di Grover (1996)***
  - ricerca in una lista non ordinata su quantum computer
  - in una lista lunga *N* trova un elemento in un tempo proporzionale a $\sqrt{N}$
  - su un computer classico il tempo è proporzionale a *N*

VERSO IL QUANTUM COMPUTER

- ***Ottobre 2011:***
  Primo centro accademico di quantum computing (Univ. South. California, Lockheed Martin e D-Wave Systems)



- ***Gennaio 2012:***
  D-Wave annuncia la realizzazione di un quantum computer a 84 qubit

- ***Primavera 2013:***
  Quantum computer D-Wave Two™ installato presso il centro NASA Advanced Supercomputing (NAS) del Ames Research Center
  …

- ***Gennaio 2017:***
  Annunciato D-Wave 2000Q con 2000 qubit

Sistemi che si basano su ***quantum annealing***, meno versatili di quelli basati su ***quantum superposition***

VERSO IL QUANTUM COMPUTER

- ***2017:***
  Google lavora ad un quantum computer a 72 qubit che si rivela troppo difficile da controllare.

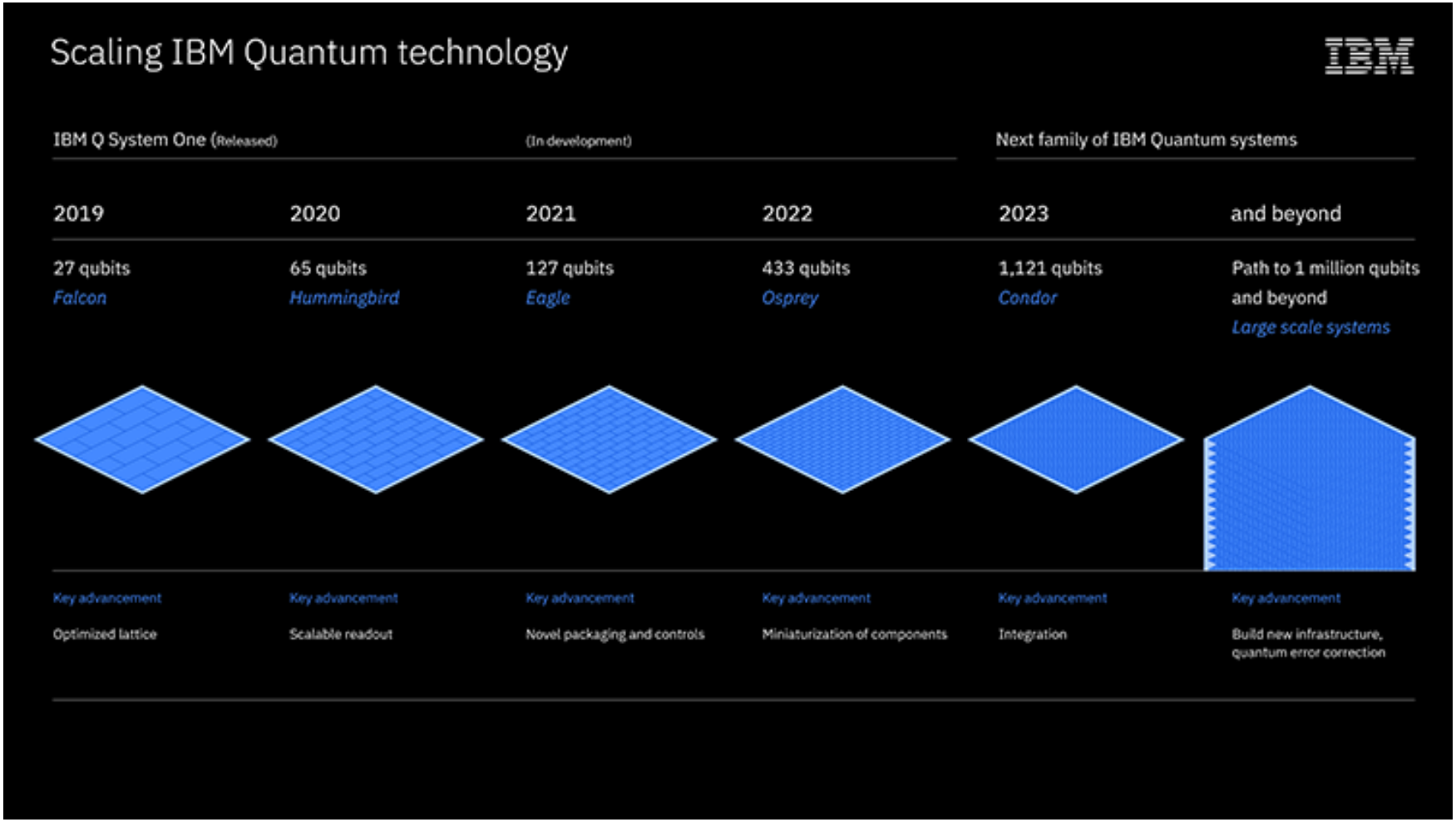
- ***Gennaio 2019:***
  IBM annuncia il suo **Q System One** con 20 qubit basati su ***quantum superposition***.

- ***Ottobre 2019:***
  Google annuncia che il suo sistema **Sycamore** con 53 qubit è capace di eseguire in 200 secondi un calcolo che richiederebbe 10’000 anni se eseguito sul più potente supercomputer del mondo.

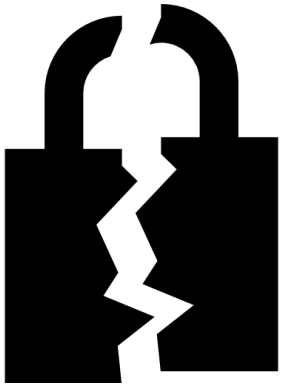
- ***Ottobre 2020:***
  La startup **IonQ** annuncia il lancio di un quantum computer a 32 qubit con bassi tassi d’errore, necessari affinché la tecnologia sia scalabile.

VERSO IL QUANTUM COMPUTER

- ***…2023:***
  IBM prevede di sviluppare il sistema **Quantum Condor** con più di 1000 qubit



CRITTOGRAFIA QUANTUM-VULNERABLE



- I sistemi crittografici asimmetrici più diffusi si basano su problemi matematici risolvibili con l'algoritmo di **Shor**:
  - ***RSA***

    (crittosistema a chiave pubblica basato su fattorizzazione di numeri interi, usato in SSL/TLS, online banking, ATM,…)
  - ***ElGamal***

    (crittosistema a chiave pubblica basato su logaritmo discreto, usato in SSL/TLS,…)
  - ***Diffie-Hellman***

    (protocollo di scambio di chiave basato su logaritmo discreto, usato in SSL/TLS, NFC/contactless,…)
  - ***ECC, DSA, ECDSA,…***

CRITTOGRAFIA POST-QUANTUM

- ***Sistemi asimmetrici:***
  - Basati su reticoli
  - Basati su codici
  - Basati su polinomi multivariati
  - Basati su funzioni hash
  - Altri (isogenie…)

- ***Sistemi simmetrici:***
  - Sistemi di cifratura simmetrica (AES…)
  - Funzioni hash (SHA…)

  Ancora utilizzabili purché si tenga conto dell'algoritmo di ***Grover***

NIST PQCRYPTO PROJECT

Nel 2016 Il ***NIST*** ha avviato un processo per lo sviluppo e la standardizzazione di uno o più algoritmi crittografici a chiave pubblica aggiuntivi per arricchire:

- La raccomandazione ***FIPS 186-4*** (Digital Signature Standard - DSS)
- La pubblicazione speciale ***SP 800-56A Rev 2*** (sistemi di key establishment basati su logaritmo discreto)
- La pubblicazione speciale ***SP 800-56B*** (sistemi di key establishment basati sulla fattorizzazione di interi)

UNIVERSITÀ POLITECNICA DELLE MARCHE

NIST – ROUND 1 E 2

- **20 Novembre 2017**: scadenza per l'invio dei candidati
- ***69 candidati*** ammessi, analizzati per oltre un anno dal NIST e dalla comunità internazionale
- Nel primo round il criterio principale di valutazione è stata la **sicurezza**
- **30 Gennaio 2019**: annuncio dei ***26 candidati*** ammessi al secondo round
- Durata del secondo round: **18 mesi**
- **22-24 Agosto 2019**, Santa Barbara: 2nd NIST PQC Standardization Conference

NIST – ROUND2 KEM/PKC

- ***Code-based***
  - BIKE
  - Classic McEliece
  - HQC
  - LEDAcrypt
  - NTS-KEM
  - ROLLO
  - RQC
- ***Isogeny-based***
  - SIKE
- ***Lattice-based***
  - CRYSTALS-KYBER
  - FrodoKEM
  - LAC
  - NewHope
  - NTRU
  - NTRU Prime
  - Round5
  - Three Bears
  - SABER

NIST – ROUND2 FIRMA DIGITALE

- ***Lattice-based***
  CRYSTALS-DILITHIUM
  FALCON
  qTESLA
- ***Hash-based+***
  Picnic
  SPHINCS+
- ***Multivariate***
  GeMSS
  LUOV
  MQDSS
  Rainbow

NIST – ITALIANI NEL SECONDO ROUND

- **BIKE:**
  Edoardo Persichetti
- **Classic McEliece:**
  Edoardo Persichetti
- **CRYSTALS-KYBER:**
  Roberto Avanzi
- **HQC:**
  Edoardo Persichetti
- **LEDAcrypt:**
  Marco Baldi, Alessandro Barenghi, Franco Chiaraluce, Gerardo Pelosi, Paolo Santini
- **NewHope:**
  Roberto Avanzi, Emmanuela Orsini
- **SABER:**
  Andrea Basso
- **SIKE:**
  Luca De Feo
- **Picnic:**
  Claudio Orlandi

NIST – TERZO ROUND

- Annunciato il **22 Luglio 2020**

- **7 finalisti**
  - Classic McEliece
  - CRYSTALS-KYBER
  - NTRU
  - SABER

  Public-Key Encryption/KEMs
  - CRYSTALS-DILITHIUM
  - FALCON
  - Rainbow

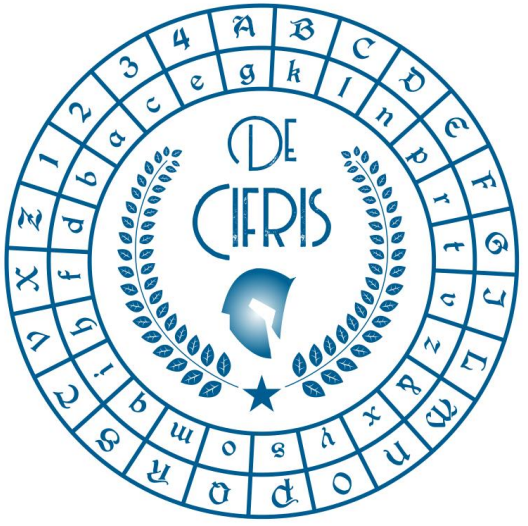
  Digital Signatures

- **8 candidati alternativi**
  - BIKE
  - FrodoKEM
  - HQC
  - NTRU Prime
  - SIKE

  Public-Key Encryption/KEMs
  - GeMSS
  - Picnic
  - SPHINCS+

  Digital Signatures

PQCIFRIS



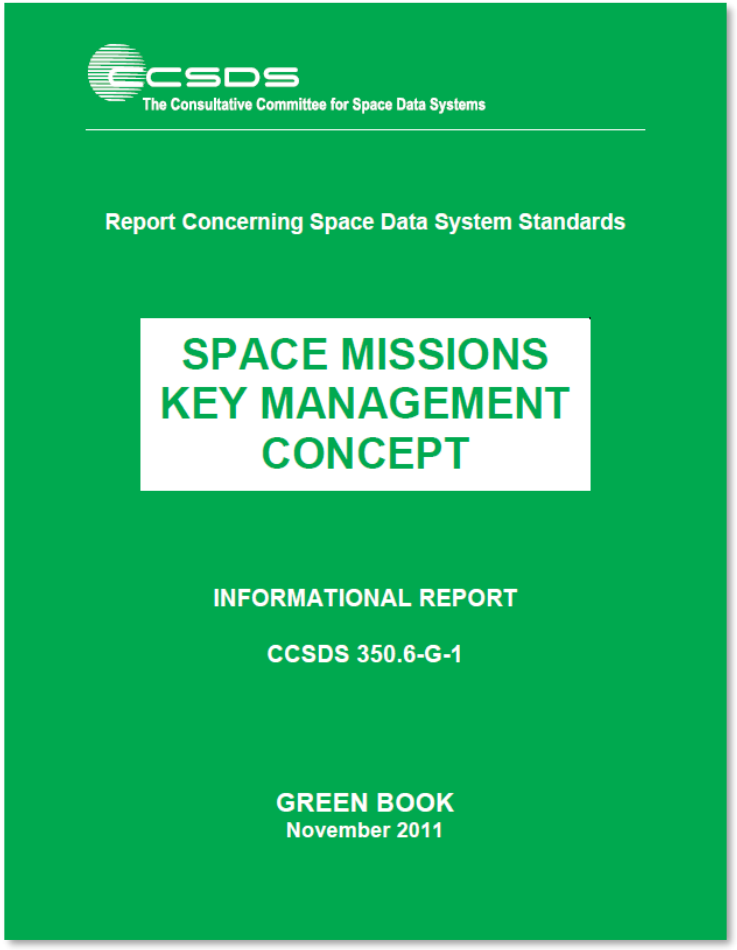
- Gruppo tematico su Crittografia Post-Quantum nell'ambito dell'iniziativa nazionale di crittografia **De Componendis Cifris**

- **40+ membri** provenienti da:
  - *Università italiane e straniere*
  - *Centri di ricerca*
  - *Aziende pubbliche e private*

- Organizzazione di incontri e seminari su Post-Quantum Crypto:
  - *8 Febbraio 2018*: sessione dedicata ad **ITASEC18**
  - *9 Maggio 2019*: evento presso **CONSOB**
  - Webinar e seminari online

PQC NELLE MISSIONI SPAZIALI?

- Diversi protocolli per comunicazioni spaziali adottano primitive crittografiche quantum-vulnerable



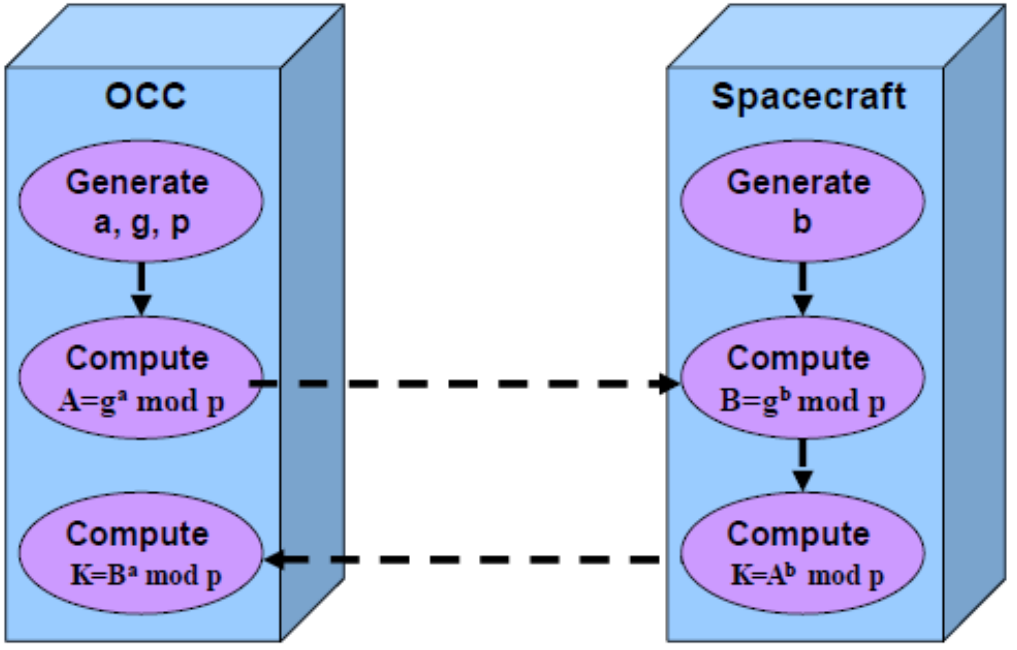


Figure 4-2: Diffie Hellman Key Exchange between OCC and Spacecraft