UNIVERSITÀ
POLITECNICA
DELLE MARCHE

Facoltà di Ingegneria

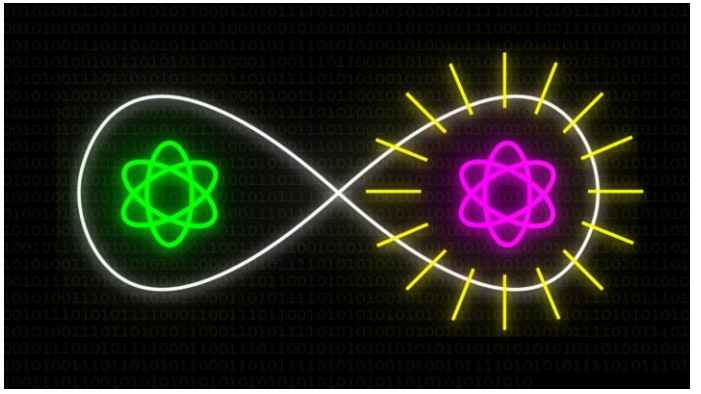
PANORAMA DELLA CRITTOGRAFIA POST-QUANTUM

Marco Baldi
Dipartimento di Ingegneria dell'Informazione

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

QUANTUM INFORMATION SCIENCE

(scienza che usa gli stati quantici di particelle subatomiche per rappresentare l'informazione)



Quantum computing

(computer che utilizza fenomeni di meccanica quantistica, come il principio di sovrapposizione e la correlazione quantistica per l'esecuzione di calcoli)

Quantum cryptography

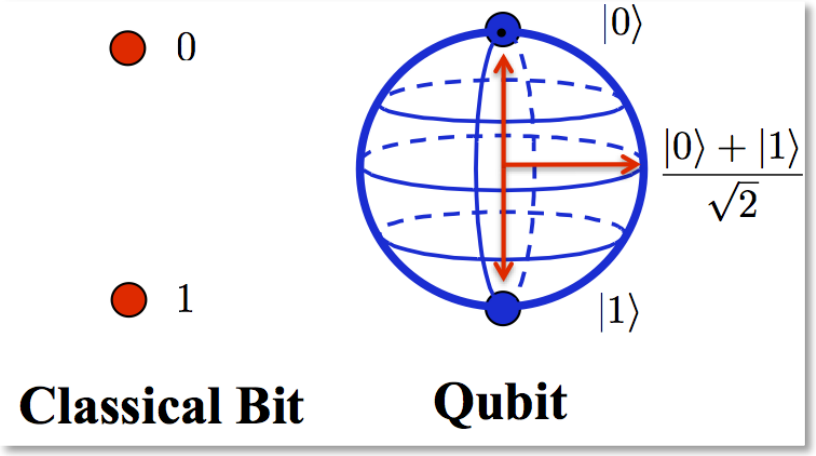
(scienza che sfrutta le proprietà della meccanica quantistica per scopi crittografici, come la quantum key distribution)

Quantum communication

(scienza che sfrutta le proprietà della meccanica quantistica per trasmettere informazione)

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*

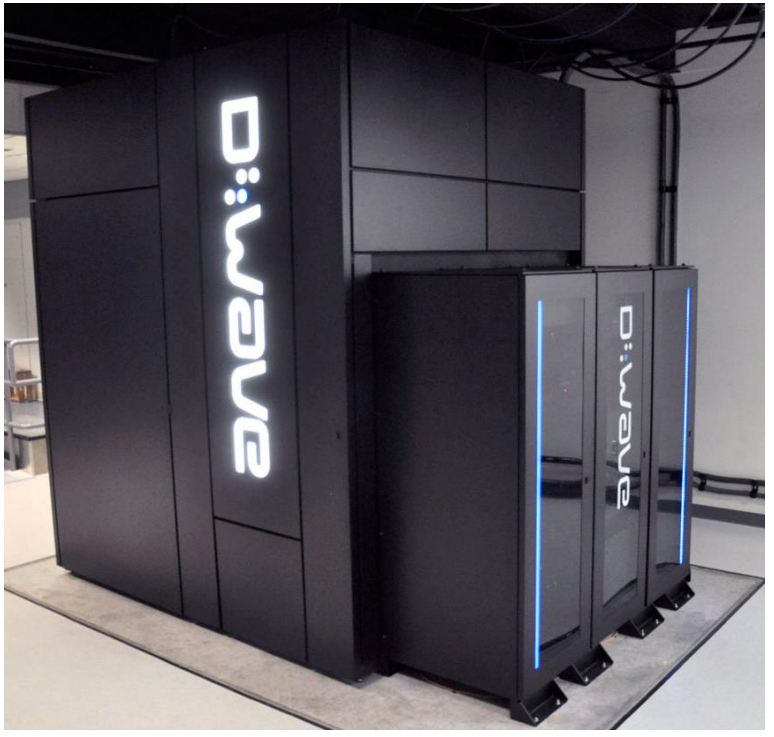
- ***Algoritmo di Grover (1996)***
  - ricerca in una lista non ordinata su quantum computer
  - in una lista lunga *N* trova un elemento in un tempo proporzionale a $\sqrt{N}$
  - su un computer classico il tempo è proporzionale a *N*

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

- *The effort to build "a **cryptologically useful quantum computer**" — a machine exponentially faster than classical computers — is part of a $79.7 million research program titled "Penetrating Hard Targets." Much of the work is hosted under classified contracts at a laboratory in College Park, Md.*

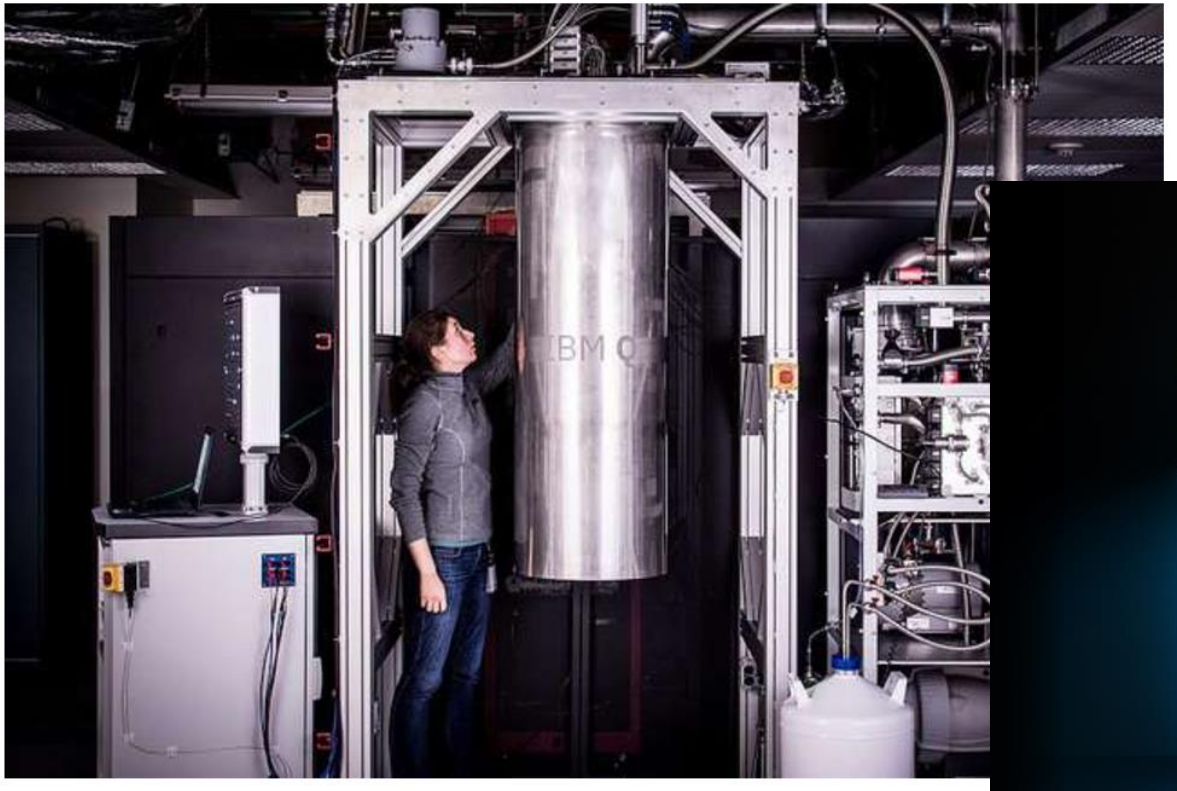
The Washington Post
2 Gennaio 2014

- *Seth Lloyd, an MIT professor of quantum mechanical engineering, said the NSA's focus is not misplaced. "The **E.U. and Switzerland** have made significant advances over the last decade and have caught up to the U.S. in quantum computing technology," he said.*

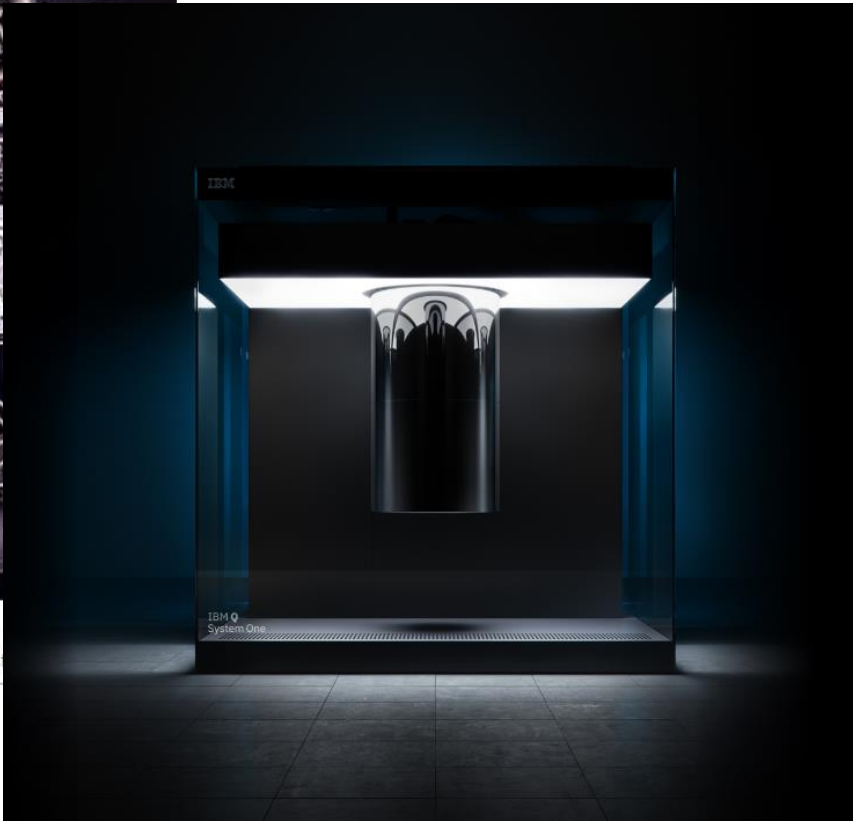
VERSO IL QUANTUM COMPUTER

IBM builds its most powerful universal quantum computing processors

May 17, 2017



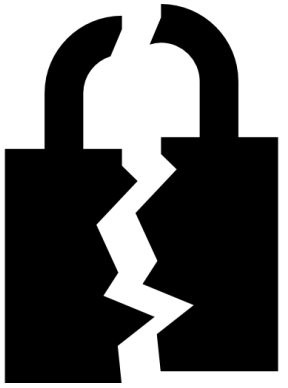
IBM Research Staff Member Katie Pooley, a Physics PhD from Harvard who recently joined IBM, pictured
Center, working on a new prototype of a commercial quantum processor, which will be the core for the firs



IBM Q

- IBM ha annunciato «***Q System One***», il primo quantum computer per scopi commerciali
- Il sistema ha ***20 qubit*** (50 qubit sono ritenuti necessari per competere con i computer classici)
- Basato su ***quantum superposition***
- Per funzionare, va mantenuto ad una temperatura bassissima ed isolato da ogni forma di rumore elettromagnetico
- Equivalente quantum dei primi computer degli anni ’50 e ’60
- Disponibili **simulatori e modelli software** per la programmazione

CRITTOGRAFIA QUANTUM-VULNERABLE



- I sistemi crittografici attualmente 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

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)

NIST PQCRYPTO TIMELINE

- ***2-3 Aprile 2015:***
  NIST Workshop on Cybersecurity in a Post-Quantum World
- ***24-26 Febbraio 2016:***
  PQCrypto 2016 – Annuncio e descrizione del bando NIST
- ***28 Aprile 2016:***
  Rilasciato il rapporto NISTIR 8105 sulla crittografia post-quantum
- ***20 Dicembre 2016:***
  Pubblicazione ufficiale del bando
- ***30 Novembre 2017:***
  Scadenza del termine per l'invio da parte dei candidati

NIST PQCRYPTO - REQUISITI

- ***Public-key encryption***: shall include algorithms for key generation, encryption, and decryption.
  - At a minimum, the scheme shall support the encryption and decryption of messages that contain symmetric keys of length at least 256 bits.

- ***Key encapsulation mechanism (KEM)***: shall include algorithms for key generation, encapsulation, and decapsulation.
  - At a minimum, the KEM functionality shall support the establishment of shared keys of length at least 256 bits.

- ***Digital signature***: shall include algorithms for key generation, signature generation and signature verification.
  - The scheme shall be capable of supporting a message size up to 2^{63} bits.

LIVELLI DI SICUREZZA NIST

Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for:

1) key search on a block cipher with a 128-bit key (e.g. AES128)

2) collision search on a 256-bit hash function (e.g. SHA256/ SHA3-256)

3) key search on a block cipher with a 192-bit key (e.g. AES192)

4) collision search on a 384-bit hash function (e.g. SHA384/ SHA3-384)

5) key search on a block cipher with a 256-bit key (e.g. AES 256)

NIST – CANDIDATI PRIMO ROUND

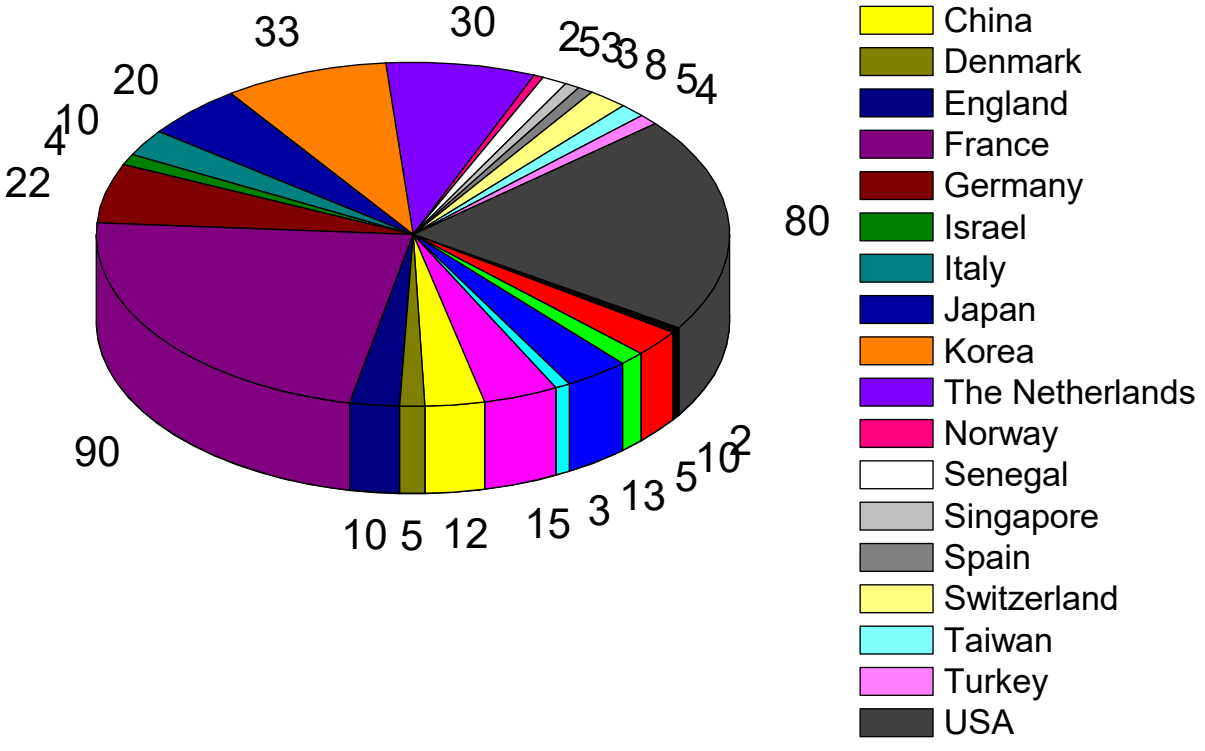
FINAL SUBMISSIONS RECEIVED

- The deadline is past – no more submissions
- 82 total submissions received
  - 23 signature schemes
  - 59 Encryption/KEM schemes

	Signatures	KEM/Encryption	Overall
Lattice-based	4	24	28
Code-based	5	19	24
Multi-variate	7	6	13
Hash-based	4		4
Other	3	10	13
Total	**23**	**59**	**82**

NIST – CANDIDATI PRIMO ROUND

263 ricercatori provenienti da
24 Paesi diversi



NIST – SECONDO ROUND

- I candidati sono stati 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 candidati ammessi al secondo round
- **26 candidati** ammessi al secondo round
- Stima di durata del secondo round: **12-18 mesi**
- **22-24 Agosto 2019**, Santa Barbara: 2nd NIST PQC Standardization Conference
- Dopo il secondo round, NIST potrà chiudere la competizione oppure iniziare un terzo round

NIST – ROUND2 KEM/PKC

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

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*
- **SIKE:** *Luca De Feo*


OH ALICE... YOU'RE THE ONE FOR ME
BUT BOB... IN A QUANTUM WORLD HOW CAN WE BE SURE?
Ψ^+ or Ψ^- ?