April 19-20, 2019
Computer History Museum
Mountain View, CA

Quantum Computing and Security Implications

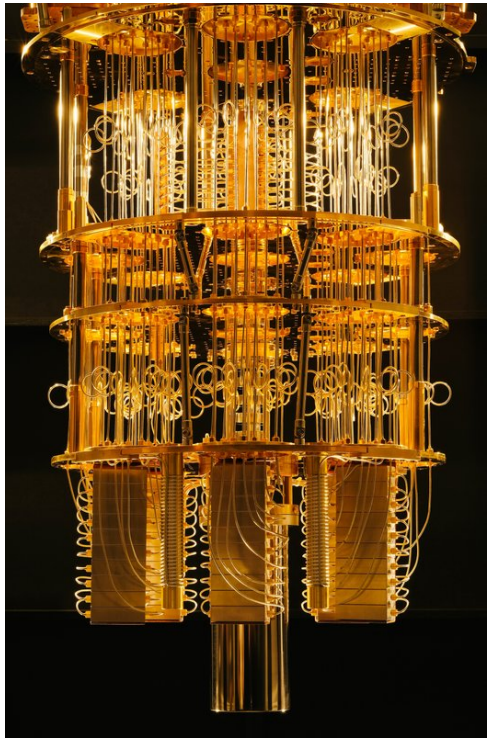
David Ott, VMware Research

Introducing ... A Quantum Computer

IBM Q System One

Announced January 2019

Source: IBM Research
https://www.research.ibm.com/ibm-q/system-one/



Source: “Is the US Lagging in the Quest for Quantum Computing?” *Scientific American*, Dec. 6, 2018.

What's In a QC?

IBM Q System One

4 Kevin (-269 C, -452.2 F)

Cryogenic Systems

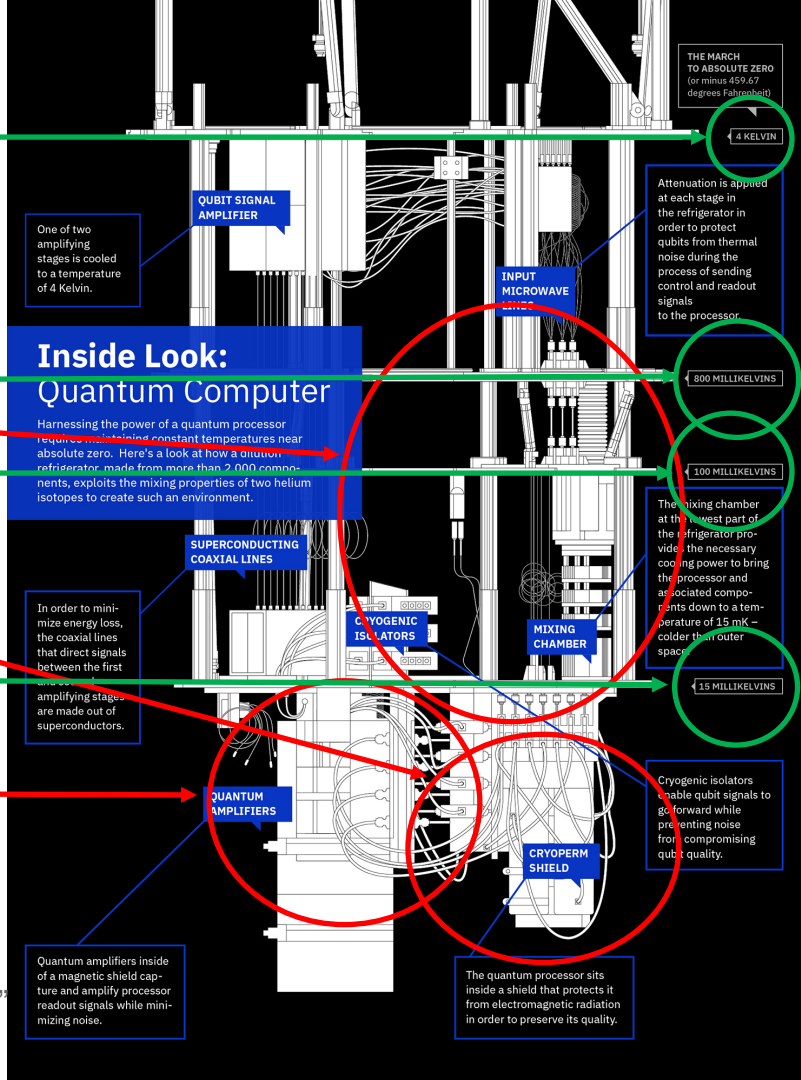
0.8 Kelvin (-272.2 C, -457.96 F)

0.1 Kevin (-272.9 C, -459.22 F)

Quantum Processor

0.015 Kevin (-272.985 C, -459.373 F)

Quantum Amplifiers



Source: IBM Research, "A look inside a quantum computer"
https://www.research.ibm.com/ibm-q/learn/what-is-ibm-q/

Qubit Technologies

Technology	Best Argument For	Best Argument Against	Companies Involved
Majorana	Fundamentally protected from errors	Hard to engineer	Microsoft
Solid-state spins (P:Si, NV centers, etc.)	Small footprint	Heterogeneous, hard to scale	Turing, CQC2T
Quantum dots	Small footprint, scalable fabrication	Connectivity	HRL, Intel
Neutral atoms	Homogeneous, long-range gates	Lack of demonstrated good 2-qubit gates	Atom Computing, Inc.
Linear optics[50]	Scalable fabrication	Lack of key components (single photon sources)	PsiCorp, Xanadu
Superconductors	Demonstrated programmability, lithographically definable	Large footprint, 10 mK	Google, IBM, Rigetti, Intel, QCI
Ions[51]	Demonstrated programmability, long coherence, homogeneous,	Microsecond gate speeds, lasers	IonQ, Honeywell

Source: "Next Steps in Quantum Computing: Computer Science's Role". CCC Workshop Report. November 2018.

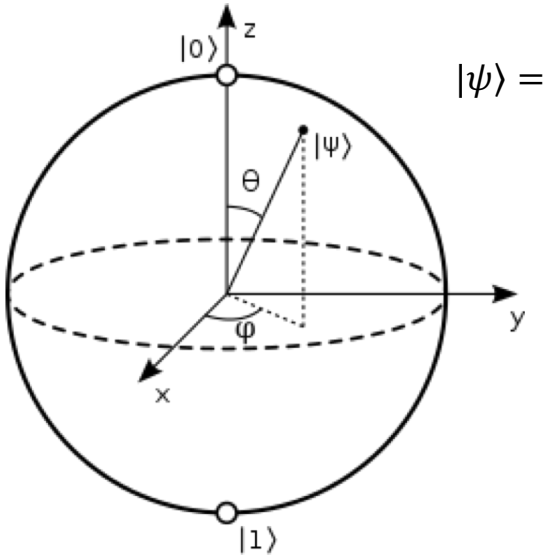
What is Quantum Computing?

Classical Computer: bits

A	B	C	Value
0	0	0	0
0	0	1	1
0	1	0	2
0	1	1	3
1	0	0	4
1	0	1	5
1	1	0	6
1	1	1	7

➔ Can simultaneously model each of the 8 states of a 3-bit classical register.

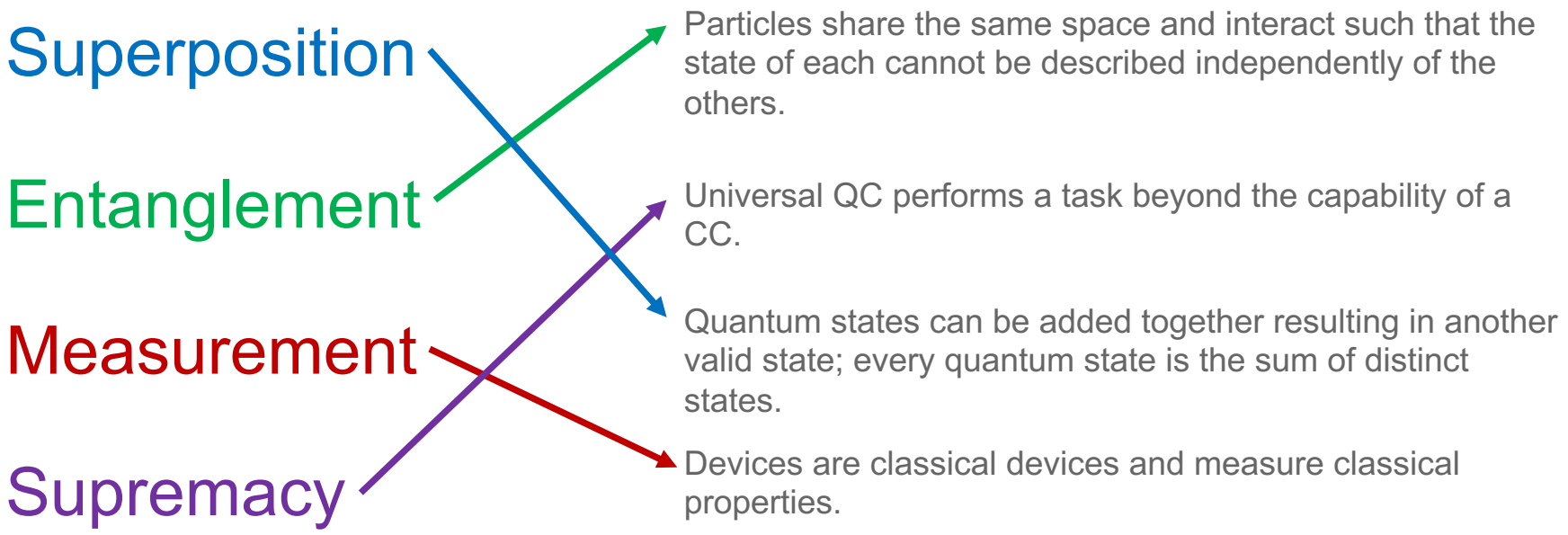
Quantum Computer: qubits



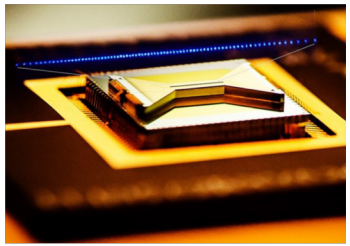
$$|\psi\rangle = a|0\rangle + b|1\rangle$$

Bloch Sphere: a geometrical representation of a two-level quantum system

QC Concepts: The Matching Game



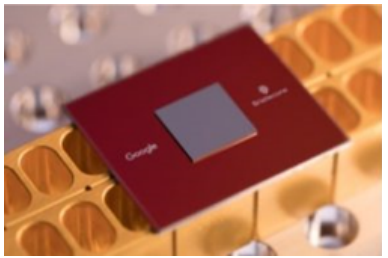
State-of-the-Art QCs



IonQ's 79-qubit trapped Ion processor.
December 2018

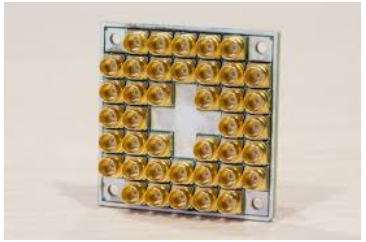
Google's 72-Qbit Bristlecone.
(March 2018)

"We are cautiously optimistic that quantum supremacy can be achieved with Bristlecone"

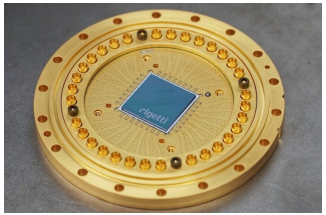


IBM Q
50 qubits
Can maintain state for 90 microsec.

Intel Tangle Lake
49 qubits
Si + quantum dots



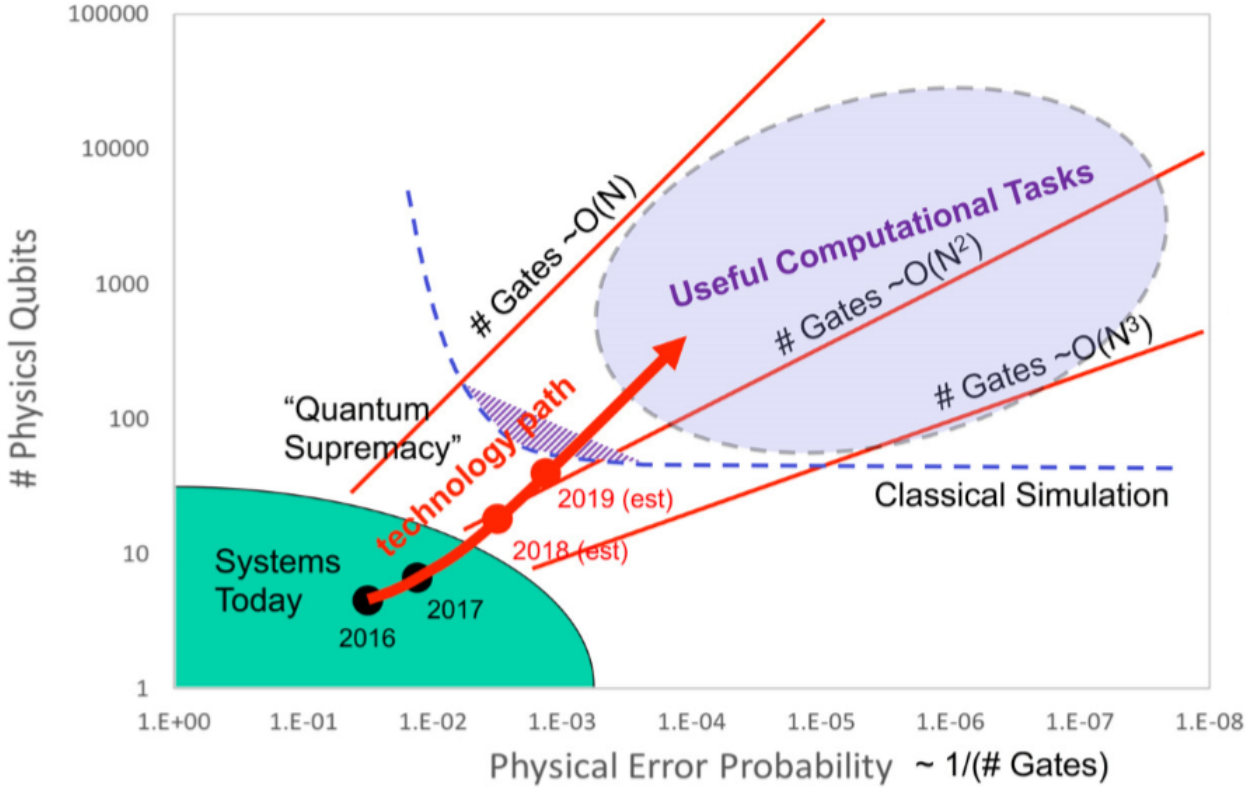
Rigetti 19Q
19 qubits
(and working on a 128-qubit system)



D-Wave 2000Q
2048 qubit
Quantum Annealer

+ Many Startups and Research Labs...

How Many Qubits Is Enough?



Source: "Next Steps in Quantum Computing: Computer Science's Role". CCC Workshop Report. November 2018.

Applications of Quantum Computing

Areas	*Technology*	*Examples*
Quantum Optimization	Hybrid quantum-classical algorithm • classical optimizer interatively alters quantum state	• graphing problems, clustering, Bayesian optimization • supply chain, logistics
Material Science, Chemistry, Medicine	Quantum simulation: • complex molecular systems using quantum entanglement	• material design • new catalysts • new pharmaceuticals
Quantum Recommendation Systems	Given approximate preference matrix and some new user preferences • find recommendation efficiently	• recommendation systems • machine learning
Quantum Deep Learning	QRAM: Quantum Random Access Memory • encoding n-element vector in log n qubits	• understanding correlations in quantum tasks • quantum probability distributions

Application: Public Key Cryptography

Shor's Algorithm (1994)

Peter Shor

Massachusetts Institute of Technology

"Quantum Algorithm"

- Runs on a quantum computer
- Solves integer factorization problem in polynomial time: O(log N)2 operations/gates

Quick summary:

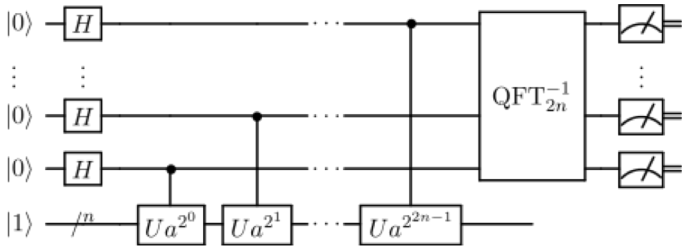
- Use CC to reduce factoring problem to finding the period of modular exponentiation function

  f(a) = x2 mod N.

- Use QC to solve period finding

  Find period r over N

Quantum Fourier Transform (QFT) applied to input register (dimension q).



Intuition: Quantum operations cause answers that are not "right" to cancel each other out.

Demonstrated by IBM using 7-qubit nuclear magnetic resonance (NMR) quantum computer in 2001. Factored 15 into 3 x 5.

Shor's algorithm can be generalized to solve the discrete logarithm and elliptic curve discrete logarithm problems!

Implications of QC for Cryptography

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	----------	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

Source: NISTIR 8105: Report on Post-Quantum Cryptography, 2016

New Public Key Cryptography Alternatives

a.k.a., Post Quantum Cryptography

PQC: Cryptographic algorithms thought to be secure against attack by a quantum computer.

Hash-based Cryptography	Alternative for digital signatures based on one-way hash functions. Merkle Hash Trees
Code-based Cryptography	Provides asymmetric encryption based on error-correcting codes. McEliece (binary Goppa codes), RLCE
Lattice-based Cryptography	Sets of points in n-dimensional Euclidean space with strong periodicity and a large number of bases. Ring-LWE, NTRU, BLISS
Multivariate Cryptography	Alternative for digital signatures using multivariate polynomials over finite fields. Rainbow (Unbalanced Oil and Vinegar)
Supersingular Elliptic Curve Isogeny	Class of elliptic curves over a field of characteristic p > 0. Replacement for widely used Diffie-Hellman key exchange.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

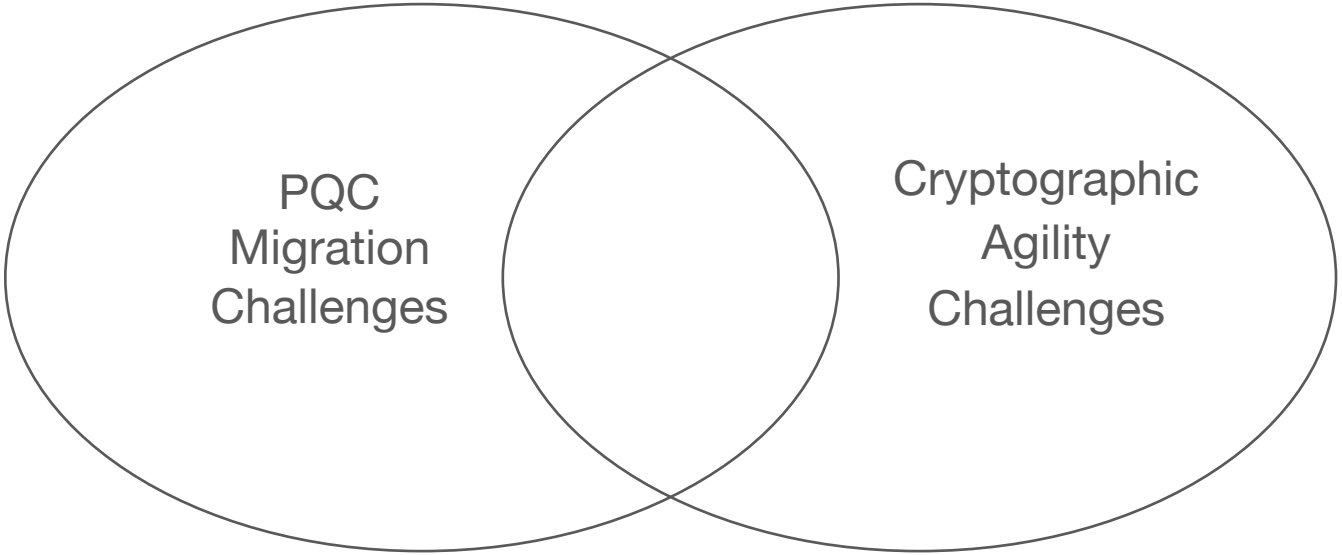
NIST
First PQC Standardization Conference
April 11-13, 2018

Fort Lauderdale, FL
69 submissions from 25 countries 400+ attendees

NIST
PQC Standardization Timeline

Aug 2016: Draft CFP submission
Dec 2016: Final requirements/criteria
Nov 2017: Deadline for submissions
Apr 2018: 1st NIST PQC Workshop
Jan 2019: 2nd Round Announcement
Aug 2019: 2nd NIST PQC Workshop
2020/2021: Selections or start 3rd Round
2022-2024: Draft standards available

Two Overlapping Challenges



What issues could benefit from academic research?

“Attaining quantum supremacy and exploring its consequences will be among the great challenges facing 21st century science.”

Professor John Preskill
Insitute for Quantum Information and Matter
California Institute of Technology


codechix
DevPulseCon


codechix
DevPulseCon