Quantum Computing: An Introduction for the perplexed

Prof. Andy Stanford-Clark

Innovation Leader, IBM Research IBM Distinguished Engineer Master Inventor, Visiting Professor, FBCS IBM Quantum Ambassador leader for UK



Our mission

Bring useful quantum computing to the world Make the world quantum safe

Our mission

Bring useful quantum computing to the world Make the world quantum safe

Our modern digital world depends on public key cryptography This is now a problem

The problem with quantum computers

Shor's algorithm (1994) shows a quantum computer can factor large numbers—at least 2048 bits long (that's 617 decimal digits).

On a classical computer, this would take millions of years.

On a *cryptographically relevant quantum computer,* this would take a few hours.

Shor's algorithm breaks RSA and other public-key cryptosystems, where security is based on the difficulty of mathematical **trapdoor** functions (factoring large numbers or taking discrete logarithms).¹

Grover's algorithm (1996) theoretically affects AES, but probably won't in our lifetimes.²

1. "<u>Polynomial-Time Algorithms for Prime</u> Factorization and Discrete Logarithms on a Quantum Computer," 25 January 1996.





Peter Shor of Bell Labs and MIT delivered the 2017 Viterbi Lecture, "Capacities for Quantum Communication Channels" Photo: Ming Hsieh, Department of Electrical and Computer Engineering at the University of Southern California.

Today's classical security protocols will be obsolete tomorrow

Prime factors	2048-bit composite integer	Expected computation time
= p x q	$\begin{array}{c} 25195908475657893494027183240048398571429282126204032\\ 02777713783604366202070759555626401852588078440691829\\ 06412495150821892985591491761845028084891200728449926\\ 87392807287776735971418347270261896375014971824691165\\ 07761337985909570009733045974880842840179742910064245\\ 869187195118764121515172645432282126659875491824224\\ 33637259085141865462043576798423387184774447920739934\\ 23658482382428119816381501067481045166037730605620161\\ 967625613841436038339044149526344321901146575444541\\ 78424020924616515723350778707749817125772467962926386\\ 35637328991215483143816789988504044536402352738195137\\ 863656439212010397122822120720357 \end{array}$	The most powerful computer today: Millions of years Shor's quantum algorithm: Hours

Public key encryption • Digital signatures • Key exchange algorithms

RSA • DSA • ECC • ECDSA • DH

Journey to Quantum Safe

U.S. National Institute of Standards and Technology announced the first quantum-safe cryptography protocol standards for cybersecurity (July 2022), three of which were created by IBM in collaboration with industry and academic partners.

Purpose	Algorithm
Public-key Encryption and Key establishment Algorithms	CRYSTALS-Kyber
Digital Signature Algorithms	CRYSTALS-DILITHIUM
DSA (alternate)	Falcon
DSA (alternate)	SPHINCS+
NIST Selected Algorithms, July 5 th 2022. NIST recommended two primary algorithms to be implemented for most use cases: CRYSTALS-KYBER (key- establishment) and CRYSTALS- Dilithium (digital signatures).	National Institute of Standards and Technology U.S. Department of Commerce

US Government establishes timeline for transition to CNSA 2.0compliant algorithms

z16

First Quantum-safe platform

GSMA Telco Consortium

Support industry transition to quantumsafe cryptography



GSMA Taps IBM, Vodafone for Post-Quantum Taskforce

IBM Quantum Safe

Support client transition to quantumsafe cryptography

IBM Quantum Safe

- Understand, Prepare & Plan
- Discover & Classify Data
- Create a Crypto Inventory
- Implement with Crypto Agility





The future of computing

Hybrid Cloud Secure heterogeneous computational fabric

Mathematics + Information Today's computers and HPC

> Intelligent Applications

bits neurons qubits Biology + Information AI Systems

Intelligent Automation Automated programming and AI

Physics + Information Quantum Systems

IBM Quantum

The limit of bits

For decades we've been simplifying nature into **1**s and **0**s because that was the only way we could manage to create a useful and scalable system of computation.

 But the future isn't just **1**s and **0**s.

Quantum computers are the only novel hardware that changes the game

Quantum computing is not just a faster or better version of classical systems. It is an entirely new branch of computing.

Quantum computing follows the laws of nature to represent data in ways that mimic the randomness and unpredictability of the natural world.

Ultimately, GPUs and classical hardware are not built for this.



We are in the early stages of a rapidly advancing new computing technology



Computer: 1944 Quantum Computer: 2019



Superconducting qubits need to be really COLD

to 10 - 15 mK with a mixture of ³He and ⁴He

space











Quantum Particles





Quantum bits and quantum circuits



A quantum bit or **qubit** is a controllable quantum object that is the unit of information

A **quantum circuit** is a set of quantum gate operations on qubits and is the unit of computation

Quantum computing uses essential ideas from quantum mechanics



Superposition is creating a quantum state that is a combination of |0> and |1>.

Measurement is an action that forces a qubit to either |0> or |1> based on probability.

Entanglement strongly connects two or more qubits so that their quantum states are no longer independent.

Quantum gates perform the basic computational operations on qubits (think of as counterparts to classical and, +, and so on).

Interference allows us to increase the probability of getting the right answer and decrease the chance of getting the wrong one.

Entanglement: "Spooky action at a distance"

We can also combine qubits to cause a correlation of results when observed.

Is the system observed as 1 or 0?



A: 50% of the time the answer is 1 50% of the time the answer is 0
B: Gives the same random answers as qubit A

Yet we can still perform deterministic operations on the two qubits.

The power of quantum computing

Classical Computers

The potential power of a classical computer doubles every time you double the number of transistors.



Quantum Computers

The potential power of a quantum computer doubles every time you add one additional qubit.



Exponential growth

IBM Quantum

2ⁿ

n qubits – 2^{*n*} quantum state dimensions.

 $2^{10} = 1,024$

 $2^{20} = 1,048,576$

 $2^{50} = 1,125,899,906,842,624$

 $2^{65} = \overline{36,893,488,147,419,103,232}$

 $2^{127} = 170,141,183,460,469,231,731,$ 687,303,715,884,105,728

Exponential growth

275

IBM Quantum

275 qubits – more quantum state dimensions than there are atoms in the observable universe.

60,708,402,882,054,033,466,233,184,58 8,234,965,832,575,213,720,379,360,039, 119,137,804,340,758,912,662,765,568



The path to useful quantum computing

Run quantum circuits faster on quantum hardware

Chart a path to develop quantum technology (hardware + software) that runs noise-free estimators of quantum circuits faster than can be done using classical hardware alone.

Map interesting problems to quantum circuits

We need applications that can be solved only with quantum circuits that are known to be difficult to simulate. This must be done in partnership with our clients and users.

The three key metrics for measuring quantum computing performance

IBM Quantum



Scale

Measured by number of qubits which indicates the amount of information we can encode in the quantum system.



Quality

2020

32 QV

Measured by **Quantum Volume** which indicates guality of circuits and how faithfully circuits are implemented in hardware.

Need low operation errors, meaning large **Quantum Volume**

2022 433 qubits

Todav 512 QV





Speed

Measured by CLOPS (Circuit Layer **Operations Per Second)** which indicates how many circuits can run on hardware in a given time.

Seamless synchronization of quantum and classical circuits increases execution rate

2020	Today	2022
200 (Inferred)	1.4K CLOPS	10K CLOPS

High coherence, high reliability, lower cost

2021

127 qubits

2020 65 qubits

IBM Quantum © 2022 IBM Corporation

Quantum volume



Quality Coherence Improved control **New architectures**

Tunable Coupling Architecture for Fixed-Frequency Transmon Superconducting Qubits J. Stehlik,^{1,*} D. M. Zajac[®],^{1,*} D. L. Underwood[®],¹ T. Phung² J. Blair,¹ S. Carnevale,¹ D. Klaus,¹ G. A. Keefe,¹

PHYSICAL REVIEW LETTERS 127, 080505 (2021)

PHYSICAL REVIEW APPLIED 6, 064007 (2016)

Universal Gate for Fixed-Frequency Qubits via a Tunable Bus

David C. McKay,^{1,*} Stefan Filipp,² Antonio Mezzacapo,¹ Easwar Magesan,¹ Jerry M. Chow,¹ and Jay M. Gambetta¹
¹IBM T.J. Watton Research Center, Yorkhown Heights, New York 10598, USA ²IBM Research Carlos, 8803 Ruschlikon, Switzerland

(Received 26 April 2016; revised manuscript received 18 August 2016; published 12 December 2016)

A challenge for constructing large circuits of superconducting qubits is to balance addressability, observed, and coupling strength. High coherence can be attained by building circuits from fixedfrequency qubits; however, leading techniques cannot couple qubits that are far detuned. Here, we even a large detunings. By parametrically oscillating the bus at the qubit-qubit detuning we enable a resonant exchange (XX + T) interaction. We use this interaction to implement a 183-ns two-qubit size between qubits separated in frequency by 854 MHz, with a measured average fidelity of 0.9823(4) from interleaved randomized benchmarking. This gate may be an enabling technology for surface-code circuits and for analog quantum simulation.

DOI: 10.1103/PhysRevApplied.6.064007

Development Roadmap

	2016-2019 🛛	2020 🥥	2021 🛛	2022 👁	2023 🛛	2024	2025	2026	2027	2028	2029	2033+
	Run quantum circuits on the IBM Quantum Platform	Release multi- dimensional roadmap publicly with initial aim focused on scaling	Enhancing quantum execution speed by 100x with Qiskit Runtime	Bring dynamic circuits to unlock more computations	Enhancing quantum execution speed by 5x with quantum serverless and Execution modes	Improving quantum circuit quality and speed to allow 5K gates with parametric circuits	Enhancing quantum execution speed and parallelization with partitioning and quantum modularity	Improving quantum circuit quality to allow 7.5K gates	Improving quantum circuit quality to allow 10K gates	Improving quantum circuit quality to allow 15K gates	Improving quantum circuit quality to allow 100M gates	Beyond 2033, quantum- centric supercomputers will include 1000's of logical qubits unlocking the full power of quantum computing
Data Scientist						Platform						
						Code assistant 🛛 🕲	Functions	Mapping Collection	Specific Libraries			General purpose QC libraries
Researchers					Middleware							
					Quantum 🔗 Serverless	Transpiler Service 🔌	Resource Management	Circuit Knitting x P	Intelligent Orchestration			Circuit libraries
Quantum Physicist			Qiskit Runtime									
T TYOIGIC	IBM Quantum Experience	0	QASM3 🥥	Dynamic circuits 🤗	Execution Modes 🛛 🥏	Heron (5K) 🕲	Flamingo (5K)	Flamingo (7.5K)	Flamingo (10K)	Flamingo (15K)		
	Early Ø Canary Albatross Penguin Prototype 5 qubits 16 qubits 20 qubits 53 qubits	Falcon Benchmarking 27 qubits	Ø	Eagle Benchmarking 127 qubits	3	Error Mitigation 5k gates 133 qubits Classical modular	Error Mitigation 5k gates 156 qubits Quantum modular	Error Mitigation 7.5k gates 156 qubits Quantum modular	Error Mitigation 10k gates 156 qubits Quantum modular	Error Mitigation 15k gates 156 qubits Quantum modular	Error correction 100M gates 200 qubits Error corrected modularity	Error correction 1B gates 2000 qubits Error corrected modularity

Innovation Roadmap

Hardware Innovation Early Canary Bubins Albatross Prototype Souths Falcon Demonstrate scaling with JO routing with Demonstrate scaling with MUW and TSV Osprey Enabling scaling with MUW and TSV Condor Falmingo Demonstrate scaling with molodal coupler Kookaburra Demonstrate scaling with molodal coupler Demonstrate scaling with molodal coupler	Software Innovation	IBM © Quantum Experience	Qiskit Circuit and operator API with compilation to multiple targets	Application modules Modules for domain specific application and algorithm workflows	Qiskit Runtime Performance and abstract through Primitives	Serverless Demostrate concepts of quantum centric- supercomputing	AI enhanced quantum Prototype demonstrations of AI enhanced circuit transpilation	Resource management System partitioning to enable parallel execution	Scalable circuit knitting Circuit partitioning with classical reconstruction at HPC scale	Error correction decoder Demonstration of a quantum system with real-time error correction decoder		
 Executed by IBM On target 	Hardware Innovation	Early Canary Penguin 5 qubits 20 qubits Albatross Prototype 16 qubits 53 qubits	Falcon Demonstrate scaling with J/O routing with Bump bonds	Hummingbird Demonstrate scaling with multiplexing readout	Eagle Demonstrate scaling with MLW and TSV	Osprey Enabling scaling with high density signal delivery	Condor Single system scaling and fridge capacity	Flamingo Demonstrate scaling with modular connectors	Kookaburra Demonstrate scaling with nonlocal c-coupler	Demonstrate path to improved quality with logical memory	Cockatoo Demonstrate path to improved quality with logical communication	Starling Demonstrate path to improved quality with logical gates
	 Executed by If On target 	ВМ					Heron Architecture based on tunable- couplers	Crossbill 🔌 m- coupler				

IBM Quantum

Condor

Pushing the limits of scale & yield

1,121 Superconducting qubits

50% Increase in qubit density

1 mile +

Of flex cabling



Introducing

Heron

133 qubit systems

Tunable coupler architecture

ibm_montecarlo



	ibm_sherbrooke Eagle	ibm_montecarlo (Heron)
Gate Error (best system)	0.6-0.7%	0.3% - Best ~ 0.1%
Crosstalk	High (qubit-qubit collisions)	Almost zero!
Gate time	500-600ns	90-100ns



New error correction codes and system modularity

C-coupler enables long-range on-chip connections for high-rate LDPC codes

L-coupler enables joining multiple logical memories to create large-scale systems

M-coupler enables joining multiple short-range chip-to-chip connections



The path to useful quantum computing

Run quantum circuits faster on quantum hardware

Chart a path to develop quantum technology (hardware + software) that runs noise-free estimators of quantum circuits faster than can be done using classical hardware alone.

Map interesting problems to quantum circuits

We need applications that can be solved only with quantum circuits that are known to be difficult to simulate. This must be done in partnership with our clients and users.

Structure of a typical workload

IBM Quantum



Real workloads are not purely quantum, but rather require interaction between quantum and classical compute resources.

Quantum applications span three general areas

Simulating Quantum Systems

Artificial Intelligence

Optimization / Monte Carlo



Quantum chemistry Material science High energy physics



Better model training Pattern recognition Fraud detection



Portfolio optimization Risk analysis Loans & credit scoring Monte Carlo-like applications

Quantum applications span three general areas

Simulating Quantum Systems		tum Systems	Artificial Intelligence	Optimization / Monte Carlo				
Improved I materi	battery als	Accelerated Diagnos	sis Fraud detection	Irregular Operations	Freight Forecasting			
lanufacturir identifica	ng defect ation	Chemical product design	Options pricing	Product Portfolio Optimization Process	Fabrication Optimization			
Semicond materi	luctor als	Catalyst discovery Chemical process	Investment Risk Analysis	Planning Quality Control	Manufacturing Supply Chain			
Chemical p predict Drug Disc	roperty ion overy	optimization High energy physic	Portfolio Management S Transaction Settlement	Vehicle Routing Raw materials shipping	Fluid Dynamics			
Protein Str Predicti Disease Predicti	ructure ons Risk	Transaction classification Product	Finance Offer Recommender Credit/Asset Scoring Airline Scheduling	Refining Processes Seismic imaging Disruption Management	and many more			

IBM Quantum

Connecting industry clients with quantum computing use cases



Wells Fargo

- Wells Fargo + IBM Quantum have published more than 10 quantum research papers in recent years.
- These papers explore new kinds of algorithms and new ways of thinking about problems in the financial services industry.
- Research focus on training quantum systems to mimic the probability distributions seen in the real world, then use that system for predictive modeling.



- JSR + IBM are experimenting with chemical simulations to help improve the development and manufacture of photoresists.
- We've already demonstrated that we can simulate small molecules that mimic parts of the photoresist.
- We hope that simulations like these will help us realize even faster chips.



- Boeing + IBM demonstrated a way to create larger computational spaces for simulating new materials.
- The simulations that the team ran are among the most complex quantum optimizations ever run.
- Boeing hopes these simulations will let them design lighter and stronger materials so planes can fly further with less fuel.



- ExxonMobil + IBM are modeling maritime inventory routing on quantum devices.
- By analyzing different strategies for vehicle and inventory routing they're laying the foundation for constructing practical solutions for their operations.
- More efficient shipping routes could help us transport fuel more efficiently around the globe.



IBM Quantum Network

A collaborative community of discovery



IBM Quantum Network members worldwide

Consiglio Nazionale delle Ricerche -

Istituto di calcolo e reti ad alte

10bit Systems AIOTECH Inc Aalto University Agnostia Inc Aliro Ouantum Amgen Anthem Applied Quantum Computing Apply Science Argonne National Lab Arizona State University Assured Information Security ΒP Beit Bluegat Boeing Bosch **Boston University** Bowie State University Boxcat Inc. Brookhaven National Lab Bundeswehr University Munich CERN CMC Microsystems Cambridge Quantum Computing Capgemini SE Carnegie Mellon Software Engineering Institute Centrum Wiskunde & Informatica Chalmers University of Technology Classiq Clemson University **Cleveland Clinic Foundation** Cognizant ColdQuanta

ColibriTD

prestazioni **Cornell University** Credit Mutuel **DIC** Corporation Daimler Deloitte Deutsches Elektronen Synchrotron F ON ETH Zurich Entangled Networks Ltd. Entropica Labs Equal1 Erste Group Bank AG ExxonMobil Fermi National Accelerator Laboratory Fidelity Investments First Ouantum Flightprofiler Florida State University Fraunhofer Fraunhofer members **GE Global Research** General Atomics Georgia Institute of Technology Goldman Sachs HOS Ouantum Simulations HSBC Hampton University Hanyang University Harvard University Hitachi Ltd Horizon Quantum Computing Howard University III Taiwan

Indian Institute of Technology - Madras

IIT Industrial Technology Research Institute Infosys Istituto Italiano di Tecnologia JP Morgan Chase JSR Corporation JoS Quantum Johns Hopkins University **KEIO Universitv** Keysight Kipu Ouantum Korea Advanced Institute of Science and Technology Korea Quantum Computing Corporation Korea University LG Corporation Lantik SA Lawrence Berkeley National Laboratory (Berkeley Lab) Lockheed Martin Los Alamos National Laboratory Maastricht University Massachusetts Institute of Technology Max Kelsen Menten Al Miraex Mitsubishi Chemical Corporation Mitsubishi UFJ Financial Group Mizuho Bank Molecular Forecaster Inc Morehouse College Morgan State University Multiverse Computing National Institute for Nuclear Physics National Taiwan University National University of Singapore

Netherlands Organization for Applied Scientific Research Netherlands eScience Center NetraMark Corp New Mexico State University New York University Nordic Quantum Computing Group North Carolina AT State University North Carolina State University Northeastern University Northwestern University Oak Ridge National Lab Opacity Pacific Northwest National Lab Phasecraft Pohang University of Science and Technology Poznan Supercomputing and Networking Center Prairie View AM University Princeton University ProteinQure Purdue University O-Ctrl OC Ware **QEDMA Quantum Computing** Ou & Co Ouantfi Quantum MADS **Ouantum Machines Ouantum South Ouantum Technology Foundation of** Thailand OuantumNET Ouebec PINO2 Qunasys **RIKEN National Research and**

Development Agency Rahko Saarland University Samsung Advanced Institute of Technology Sandia National Labs Science and Technology Facilities Council Daresbury Seoul National University SoftwareO Solid State AI Sonv Southern University and A&M College SpinUp AI Stanford University Stony Brook University Strangeworks Sumitomo Mitsui Trust Bank Limited Sungkvunkwan University Super Tech Labs Surf Swiss Federal Institute of Technology Lausanne System Vertrieb Alexander GmbH TNO Tech Mahindra Limited The University of Texas at Austin **Tokyo Electron Limited** Toshiba Tovota Tovota Central RD Labs Turku University Tuskegee University Ulsan National Institute of Science and Technology United States Air Force Research Lab United States Naval Postgraduate

IBM Quantum

Military University United States Naval Research Laboratory University of Amsterdam University of Basque Country University of Chicago University of Georgia University of Illinois at Urbana Champaign University of Innsbruck University of Madrid University of Melbourne University of Minho University of Montpellier University of New Mexico University of Oxford University of Sherbrooke University of South Carolina University of Southern California University of Tennessee University of Tokyo University of Washington University of Waterloo University of Witwatersrand Johannesburg University of the District of Columbia Community College Virginia Tech Wells Fargo Woodside Energy Ltd Xanadu Yokogawa Electric Corporation Yonsei University Zapata Computing Inc Zurich Instruments gBraid Co

43

back

þ

😂 Quantum Circuit

品 Dashboard

TOOLS

- E Results
- 🙄 Circuit Composer
- Ċ 🛛 Qiskit Notebooks

RESOURCES

⑦ Documentation & Support

New here? Get started with the IBM Q [×] Experience!



Qiskit Notebooks C

Create your first notebook and start using Qiskit

Create a notebook ightarrow

Circuit Composer

Explore the graphical interface for creating and testing circuits

Create a circuit \rightarrow

Your backends

These are the quantum systems and simulators that you have access to.

Got it!

🔅 online

ibmq_16_melbourne (14 qubits)

Queue: 0 runs

ibm-q/open/main

🔅 online

ibmq_5_yorktown - ibmqx2 (5 qubits)

Queue: 1 runs

ibm-q/open/main

quantum-computing.ibm.com

What builds a quantum workforce?

OPEN ACCESS

IBM is the only company to offer our real quantum computers available for public and premium access via the cloud.

OPEN SOURCE

Written in Python and maintained on GitHub, Qiskit is designed to make quantum computing software tools and frameworks available to everyone.

EDUCATION

Now is the opportunity for us all to give back and support building a diverse community of researchers, students, educators, and developers.

Open Source Textbook

community.qiskit.org/textbook





- 1. Quantum States and Qubits
- 2. Single Qubits and Multi-Qubit Gates
- 3. Quantum Algorithms
- 4. Quantum Algorithms for Applications

5. Investigating Quantum Hardware Using Qiskit

learning.quantum.ibm.com

6. Implementations of Recent Quantum Algorithms







2016 - 2023











IBM Quantum / © 2024 IBM Corporation

$2023 \rightarrow Utility$

We have entered the era of Quantum Utility.

Definition of Quantum Utility

High-fidelity quantum computation outside the reach of exact classical simulation methods

It is the first major milestone on the path to Quantum Advantage.

Useful quantum computation requires utility-scale hardware and co-designed scalable software capabilities.

This means systems larger than 100 qubits, where simulations are not a viable alternative.



If you're not using 100+ qubits, you're not doing quantum.

quantum-computing.ibm.com

IBM Quantum

@andysc

andysc@uk.ibm.com