CYBERSECURITY IN THE POST QUANTUM WORLD

Jennifer Cheung

March 14, 2024

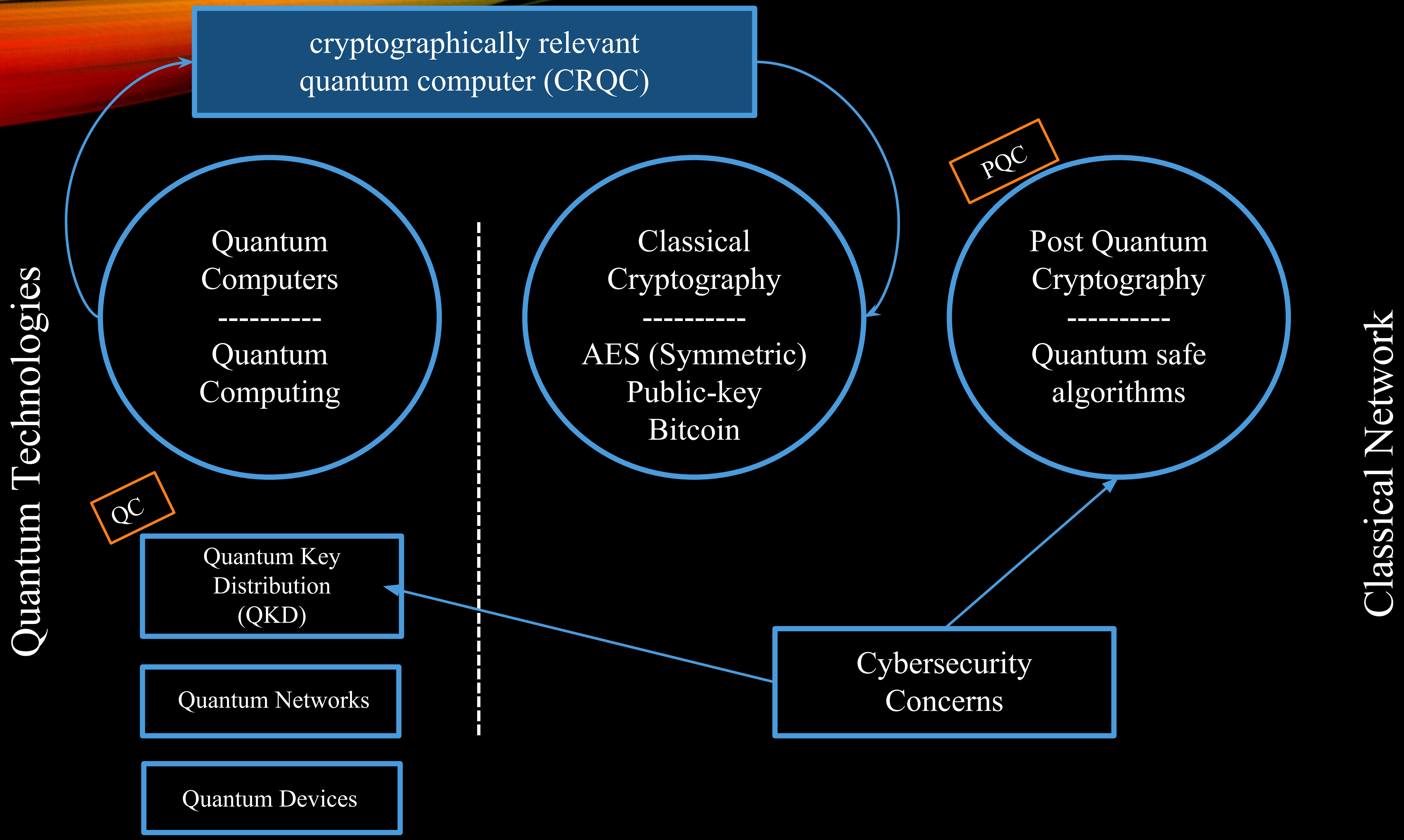
women in cybersecurity
WiCyS
SAN DIEGO AFFILIATE

WHO AM I?

MS--Applied Math (2010)

Study & Research Grant: Quantum Informatics / Cryptography (2011-2012)

Computer Science Dept Aarhus University Aarhus, Denmark


cryptographically relevant quantum computer (CRQC)
Quantum Technologies
Quantum Computers

Quantum Computing
Classical Cryptography

AES (Symmetric)
Public-key
Bitcoin
PQC
Post Quantum Cryptography

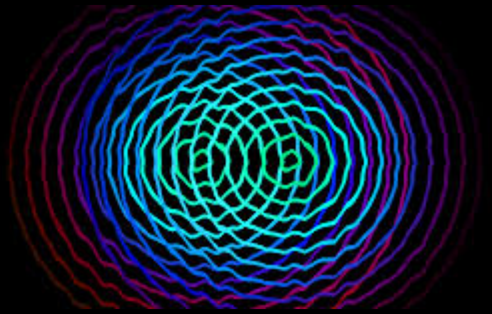
Quantum safe algorithms
Classical Network
QC
Quantum Key Distribution (QKD)
Quantum Networks
Quantum Devices
Cybersecurity Concerns

QUANTUM CRYPTOGRAPHY (QC) VS POST QUANTUM CRYPTOGRAPHY (PQC)

PQC (new standards just released from NIST:

https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022)

- has nothing to do with principles of quantum mechanics
- lattice-based or code-based (hard math problems) that there are no existing quantum algorithms to break them (yet).
- (quantum annealing mimicking quantum computing)□D-Wave?



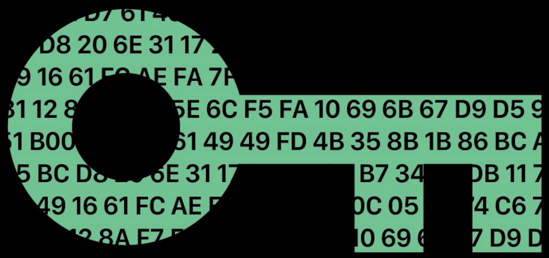
QC—best example is Quantum **Key** Distribution (QKD)

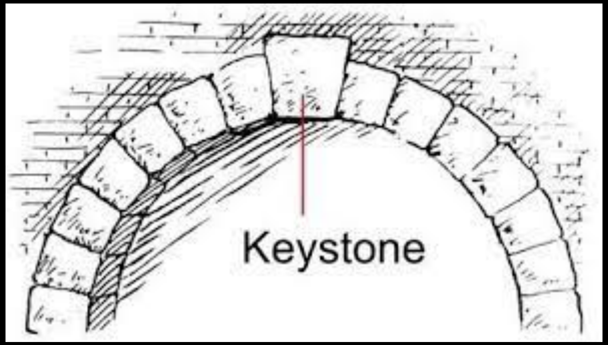
- No quantum computing /quantum Protocol
- provide **<u>provable</u>** security of information exchange
- No encryption or decryption; **<u>information becomes physical</u>** carried by photons
- Use to share private keys with symmetric key cryptography

KERCKHOFFS'S PRINCIPLE

Assume the adversaries know about the cryptosystem that you are using for secure communication. The only thing we really need to keep secret is the KEY.

KEY is the vital part of the secure communication.

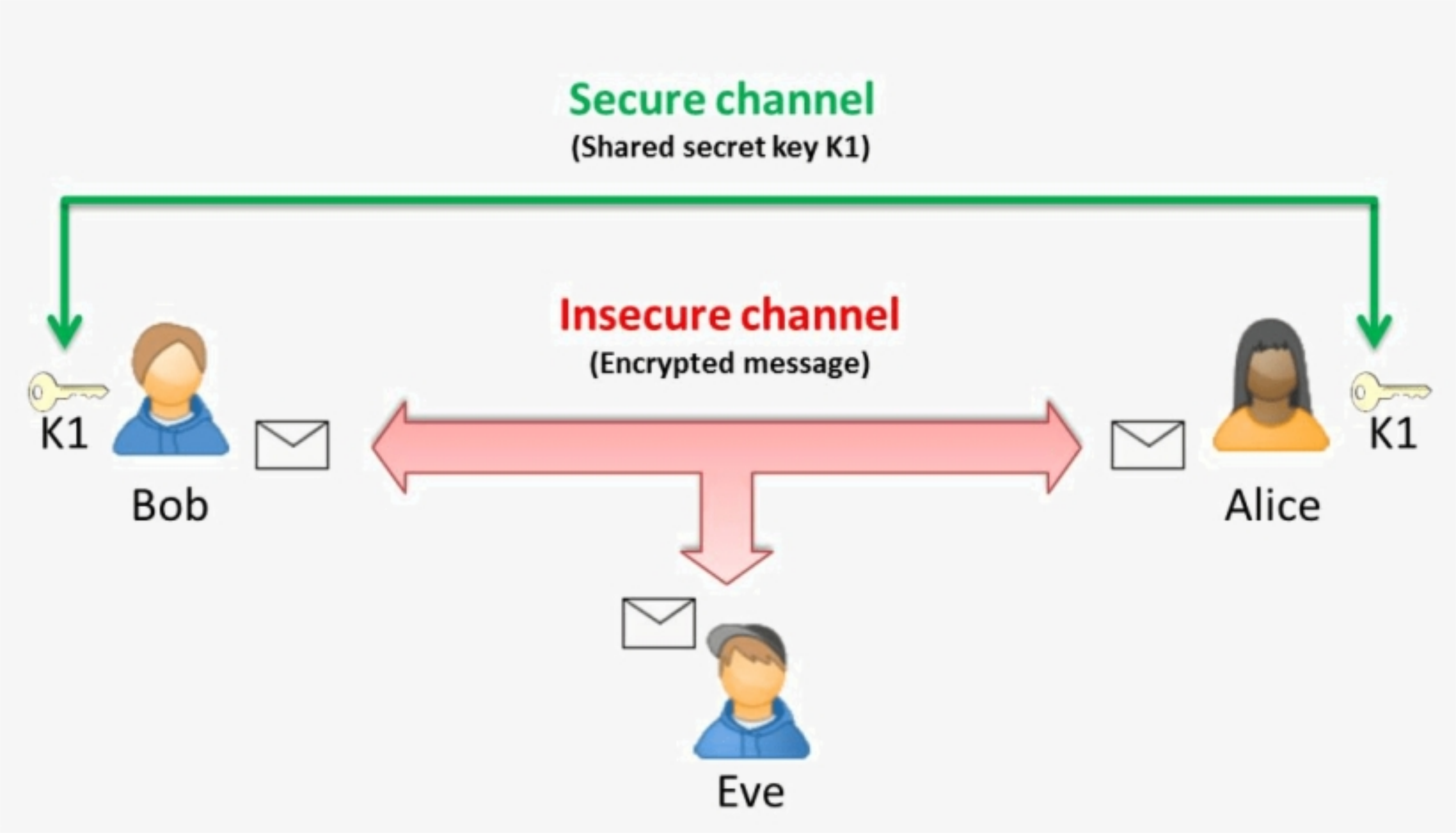




Auguste Kerckhoffs
1835 – 1903

Dutch linguist & cryptographer

SYMMETRIC KEY CRYPTOGRAPHY (PRIVATE KEY)

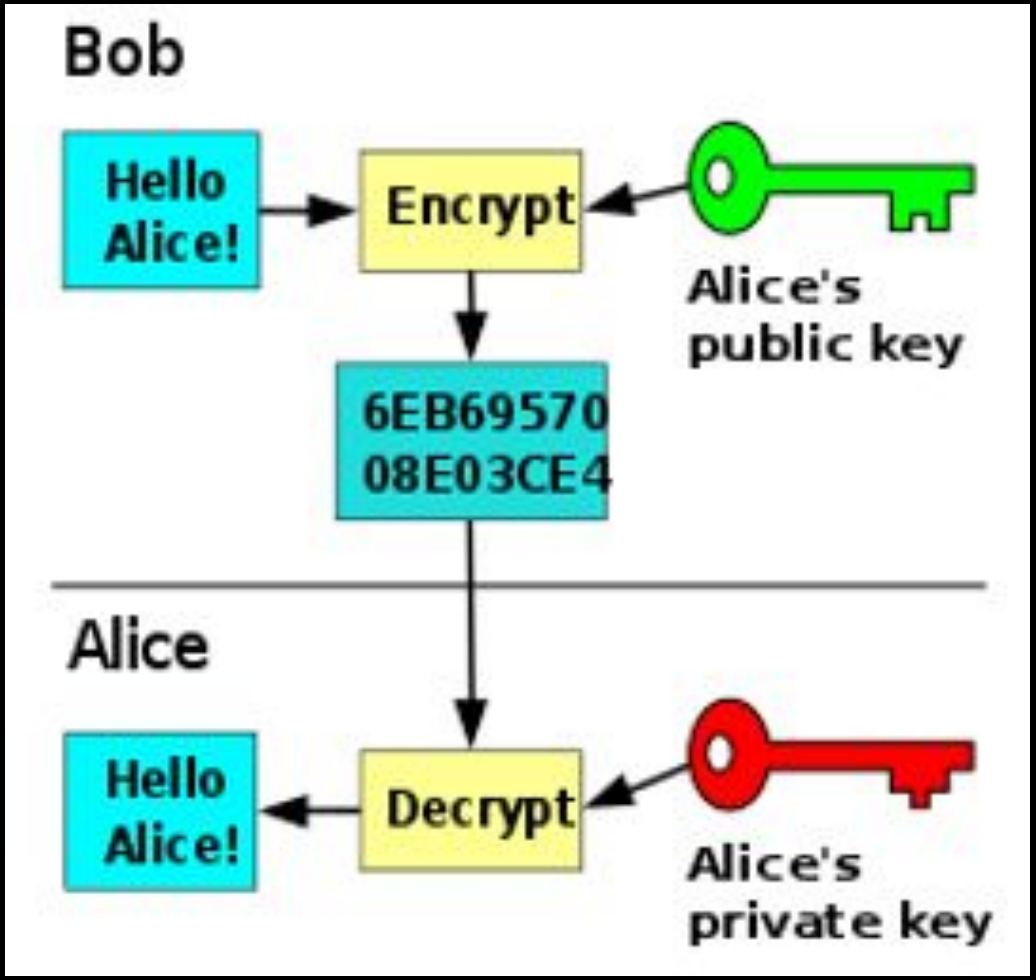


The same key must be shared between Alice and Bob.

Plaintext = x
Ciphertext = y

$e_K(x) = y$
$d_K\ (y) = d_K\ (e_K(x)) = x$

ASYMMETRIC KEY CRYPTOGRAPHY (1970'S-PUBLIC KEY)



No need to share keys.

A pair of keys,

- a private key
- a public key

are used for encryptions and decryptions.

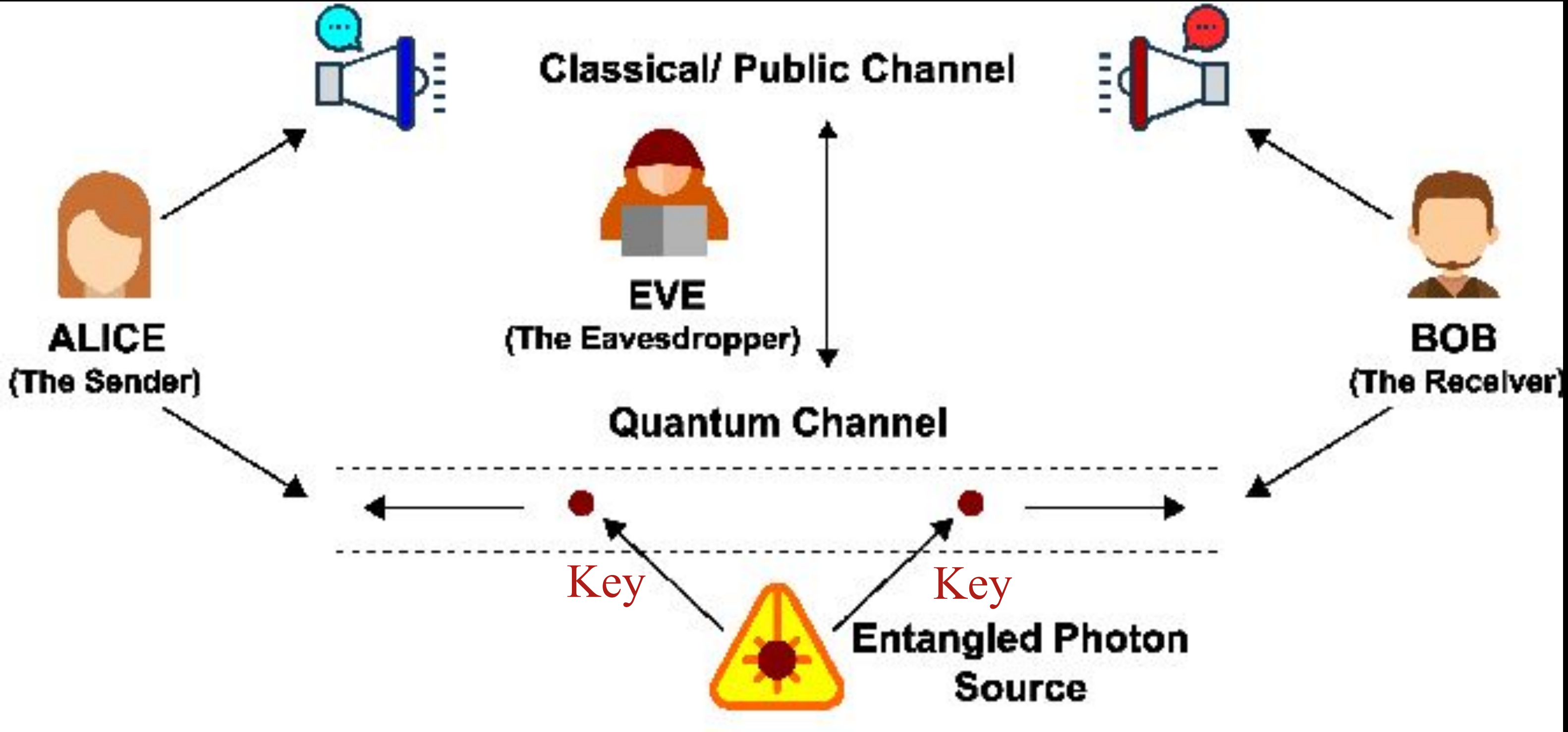
Example:

- RSA (multiplication of two prime numbers)
- ElGamal (Discrete Logarithm)

$$(a^k = b)$$

$$(log_a\, a^k = log_a\, b)$$

QUANTUM KEY DISTRIBUTION (QKD)

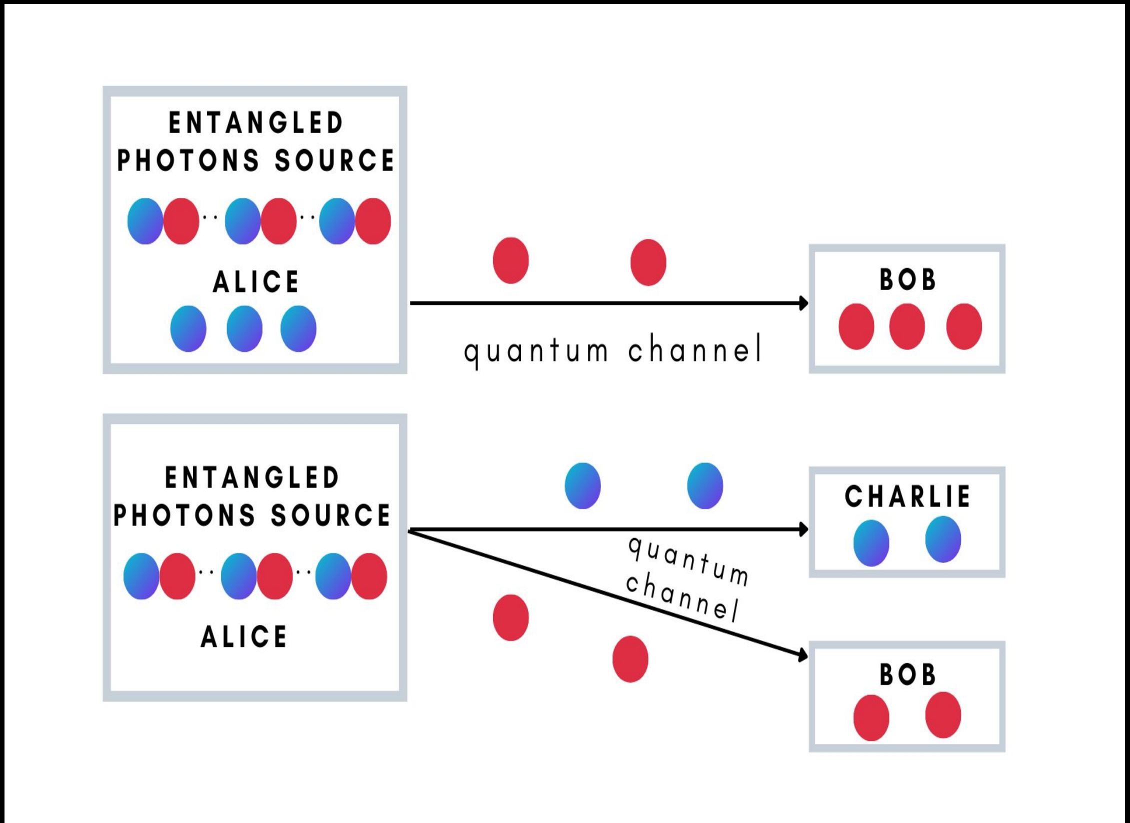


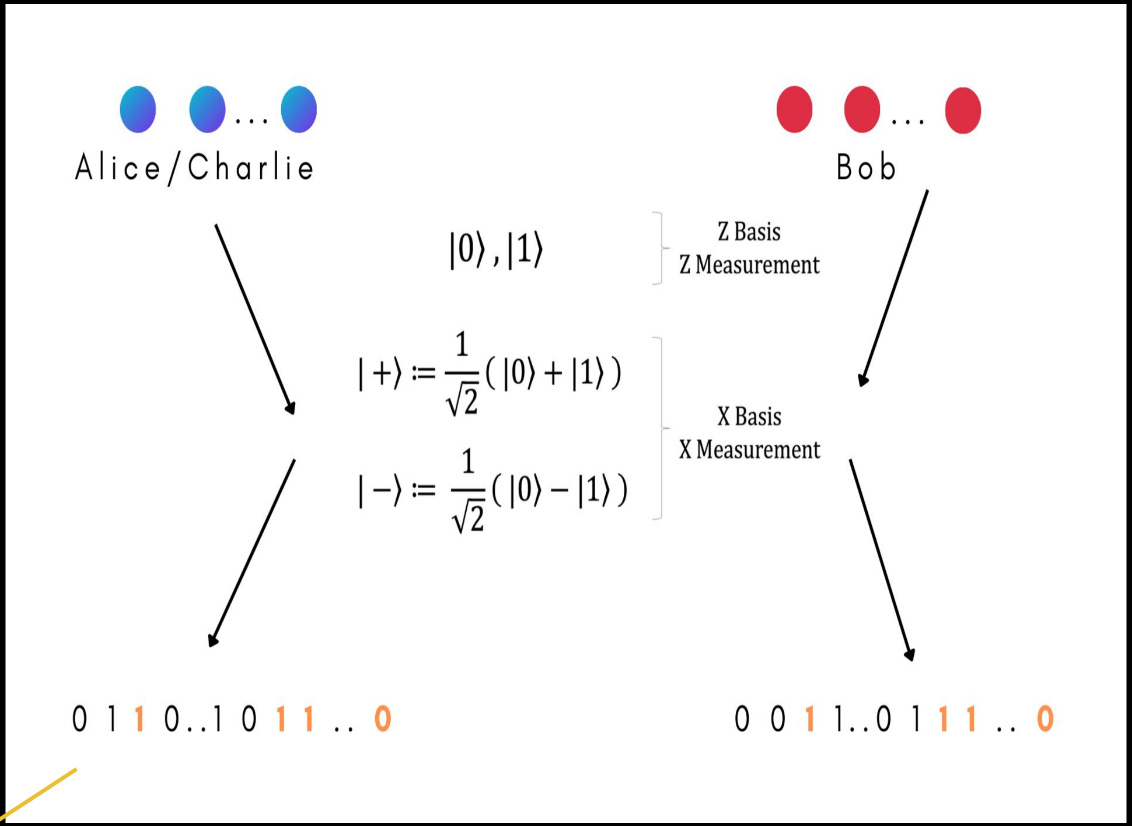
Information is carried by photons

Same key can be sent to both Alice and Bob

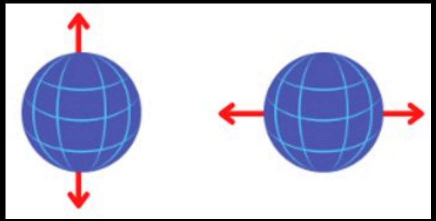
Provable security due to the quantum properties of the photons

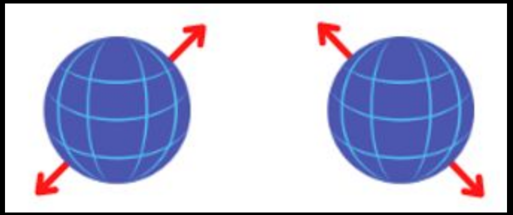
E91/EPR PAIR PROTOCOL





BB84 protocol





How about key size?

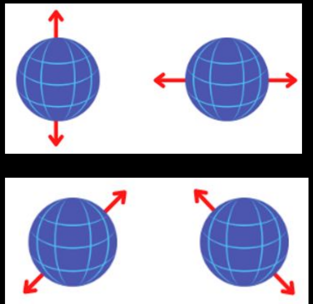
BB84 PROTOCOL

Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↘	↗	→	↗	→	→
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		1			0		1

- Alice polarized the classical bits with X- or Z-basis
- Alice sends qubits to Bob
- Bob measures them with random basis of X or Z
- Bob basis matched Alice □ shared secret key

https://en.wikipedia.org/wiki/Quantum_key_distribution

Basis	0	1
+	↑	→
×	↗	↘



NSA CONCERNS ON QKD

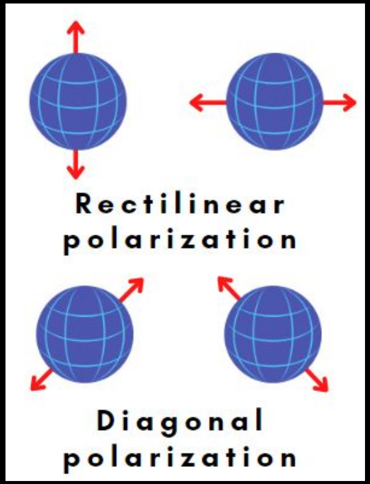
- QKD does not provide a means to **authenticate** the QKD transmission source
- Quantum key distribution is **hardware-based**, can't be implemented in software or a service on a network
- Quantum key distribution increases infrastructure **costs** and **insider threat risks**
- **Securing and validating** quantum key distribution is a significant challenge
- The sensitivity to an eavesdropper as the theoretical basis for QKD security claims also shows that **denial of service** is a significant risk for QKD

https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

QUANTUM COMPUTING VS QKD

QKD

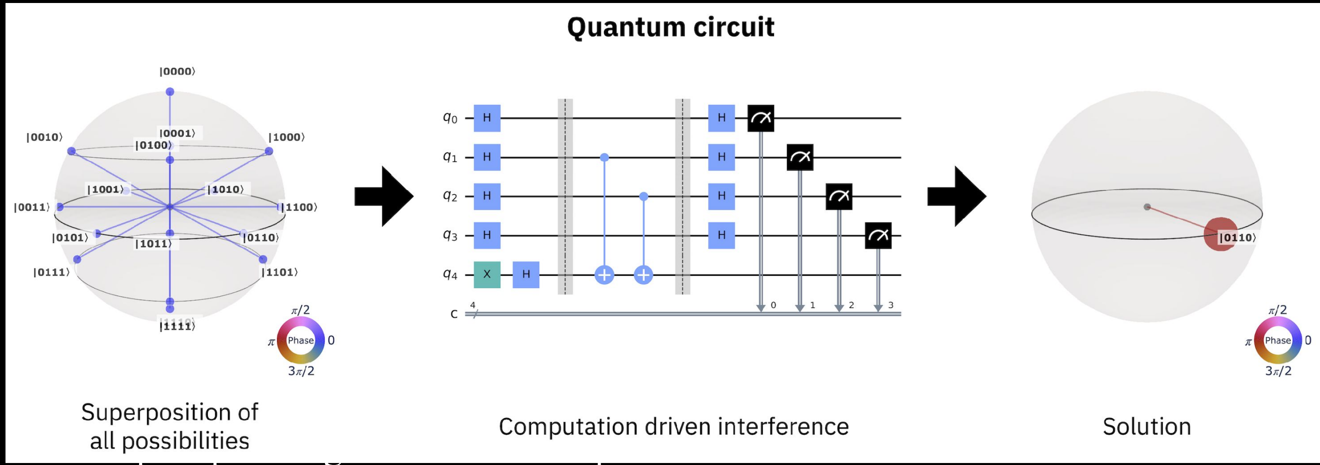
- Polarization of photons
- Measurement of the basis
- Entanglement



Basis	0	1
+	↑	→
×	↗	↘

Quantum Computing

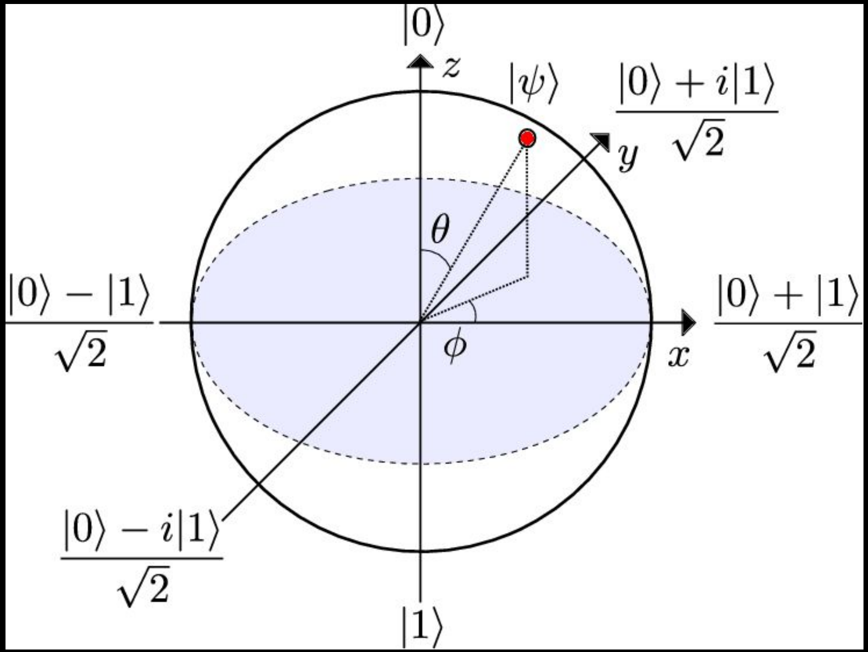
- Manipulate the qubits to perform quantum computing with quantum algorithms
- Interference / Superposition



VERY-VERY BRIEF INTRO OF QUANTUM MECHANICS (FROM A MATH VIEWPOINT)

Quantum mechanics

- *****Probabilistic model*****
- Bloch sphere in Hilbert space



$|\psi >$ -- quantum state

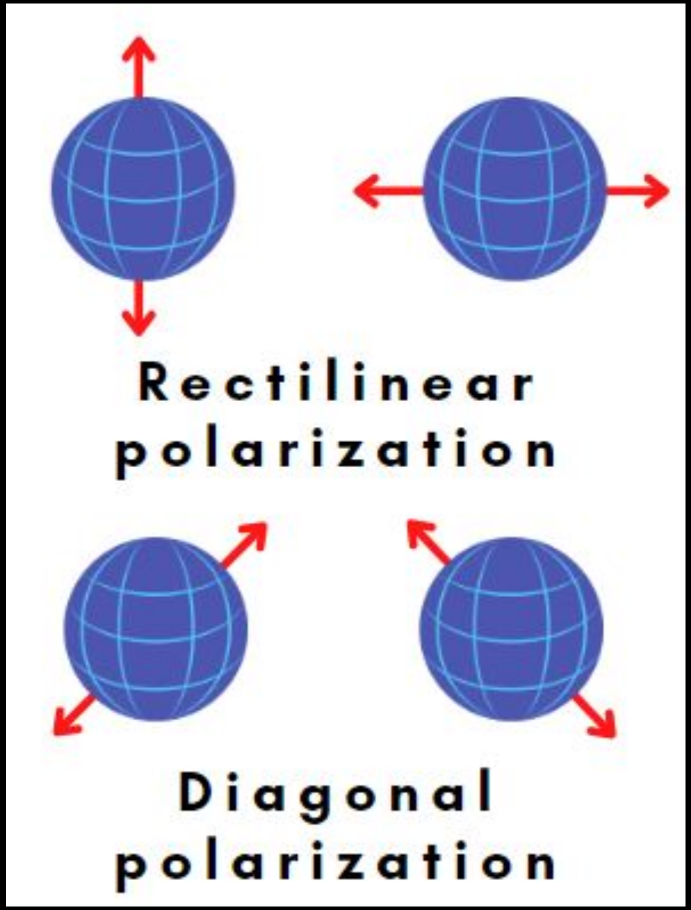
Z-basis (orthogonal)

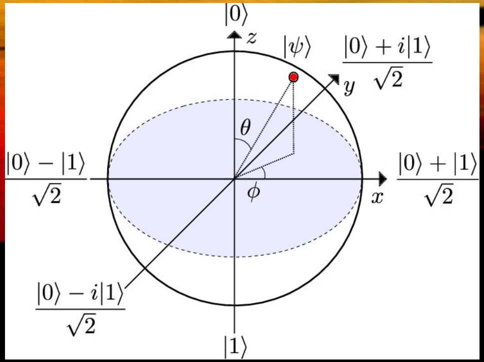
| 0> ; | 1>

X-basis (orthogonal)

$| + > = (|0 > + |1 >)/\sqrt{2}$;

$| - > = (|0 > - |1 >)/\sqrt{2}$





QUANTUM STATES AND SUPERPOSITION

A quantum state can be represented by:

$|\psi> = \alpha|0> + \beta|1>$ where $|\alpha|^2 + |\beta|^2 = 1$, α and β are complex numbers

(1 qubit superposition)

complex vector space

Superposition (unobservable states)

- Linear combinations of computational basis states

Observable states (observer effect)

- Measurement of qubit will cause the quantum state to collapse into one of the basis states: | 0> or | 1>
- No-cloning of quantum states

How about with 2 qubits?

ENTANGLEMENT AND BELL STATES (EPR PAIR)

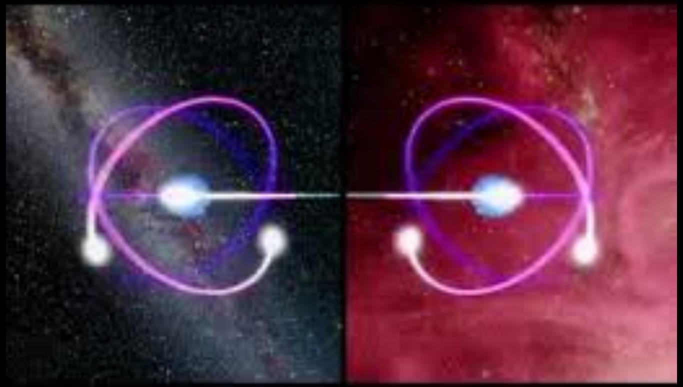
Quantum entanglement

- A pair of photons with perfect correlation as one system with one quantum state (EPR pair—Einstein, Podolsky, Rosen)
- Measuring one photon will cause the other photon collapse into the same quantum state
- Bell states – maximumly entangled states:

$$|\beta_{00}> = \frac{|00> + |11>}{\sqrt{2}} \qquad |\beta_{01}> = \frac{|01> + |10>}{\sqrt{2}}$$

$$|\beta_{10}> = \frac{|00> - |11>}{\sqrt{2}} \qquad |\beta_{11}> = \frac{|01> - |10>}{\sqrt{2}}$$

Tensor product: $|01> = |0> \otimes |1>$



QUANTUM COMPUTING--BUILDING QUANTUM CIRCUITS

HADAMARD GATES

MOST IMPORTANT GATES FOR QUANTUM CIRCUIT

Hadamard (***H***)	$H = \frac{\lvert 0\rangle + \lvert 1\rangle}{\sqrt{2}}\langle 0\rvert + \frac{\lvert 0\rangle - \lvert 1\rangle}{\sqrt{2}}\langle 1\rvert$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$	$H\lvert 0\rangle = \frac{1}{\sqrt{2}}(\lvert 0\rangle + \lvert 1\rangle)$ $H\lvert 1\rangle = \frac{1}{\sqrt{2}}(\lvert 0\rangle - \lvert 1\rangle)$	—[H]—

Dirac notation: ket $|0>$ and bra $<0|$

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} = \frac{1}{\sqrt{2}}\left(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|\right)$$

$$H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\cdot\begin{pmatrix}1\\ 0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 1\end{pmatrix} = |+\rangle$$

$$|0\rangle = \begin{bmatrix}1\\ 0\end{bmatrix} \qquad |1\rangle = \begin{bmatrix}0\\ 1\end{bmatrix}$$

Transformation:

$$H(|0\rangle) = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle =: |+\rangle$$
$$H(|1\rangle) = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle =: |-\rangle$$

classical bits → qubit with superposition

HADAMARD GATE WITH MULTIPLE QUBITS

$$H_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$H_2 = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

$$H_3 = \frac{1}{2^{3/2}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}$$

$$(H_n)_{i,j} = \frac{1}{2^{n/2}}(-1)^{i \cdot j}$$

OTHER GATES (ONE QUBIT)

Hadamard	H	$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Pauli-X	X	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y	Y	$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z	Z	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Phase	S	$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$	T	$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

$| \psi > \longrightarrow | \varphi >$

Pauli X

$|0> \longrightarrow |1>$

$|1> \longrightarrow |0>$

Pauli Y

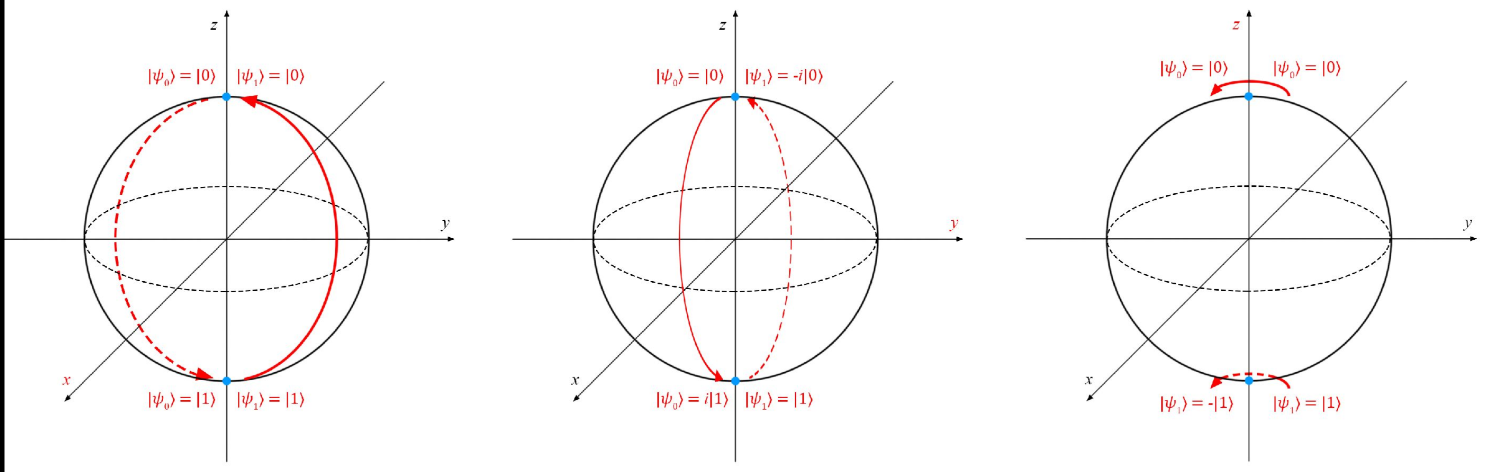
$|0> \longrightarrow i\,|1>$

$|1> \longrightarrow -i\,|0>$

Pauli Z:

$|0> \longrightarrow |0>$

$|1> \longrightarrow -|1>$



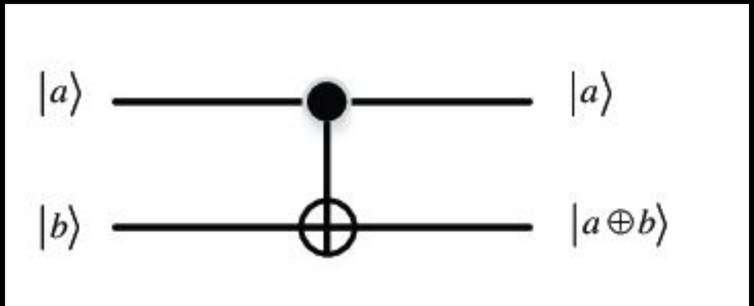
Pauli X Pauli Y Pauli Z

QUANTUM GATES FOR MULTIPLE QUBITS

CNOT gate

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

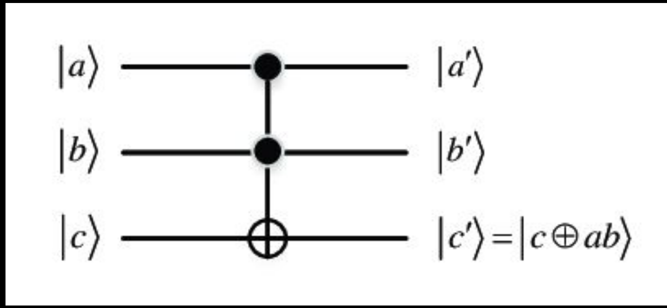
input		output	
x	y	x	y+x
$\lvert 0\rangle$	$\lvert 0\rangle$	$\lvert 0\rangle$	$\lvert 0\rangle$
$\lvert 0\rangle$	$\lvert 1\rangle$	$\lvert 0\rangle$	$\lvert 1\rangle$
$\lvert 1\rangle$	$\lvert 0\rangle$	$\lvert 1\rangle$	$\lvert 1\rangle$
$\lvert 1\rangle$	$\lvert 1\rangle$	$\lvert 1\rangle$	$\lvert 0\rangle$



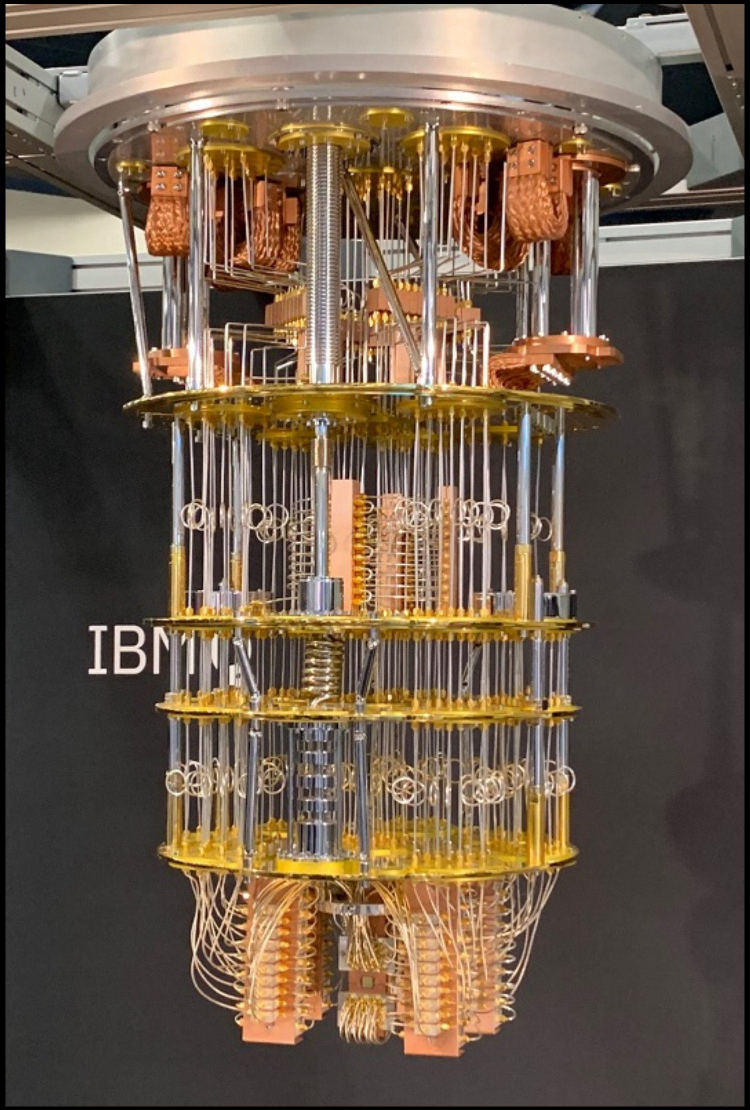
Toffoli gate

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Inputs			Ouputs		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0



IBM QUANTUM



- Up-side-down chandelier
- Super cold – 15 millikelvin
- 20-qubit commercial system in Dec 2017
- Multiple quantum systems and world wide locations with quantum computing on-site
- Nov 16, 2021 – Eagle (127-qubit quantum processor)
- 2022 – Osprey (433 qubits)
- 2023 – Condor (1,221 qubits)
- Vision for future – quantum data center

(using half of the qubits for error corrections)

IBM SYSTEM TWO

- Heron processor (133-qubit)
- Run 1800 gates within coherence times
- Lowest-error / highest-performing processor
- 2024 three coupled Heron Processors

https://www.ibm.com/quantum/summit-2023#overview

IBM QUANTUM PRICING

Open Plan	Pay-as-you-go	Premium Plan	Dedicated Service
No contract necessary	No contract necessary	Contract required	Contract required
Best for Learning quantum computing and exploring IBM quantum technology.	Best for Performing utility-scale quantum research projects and testing business use cases with flexible access.	Best for Executing a strategic quantum roadmap and developing utility-scale quantum algorithms and applications.	Best for Exploring quantum algorithms and applications with high control over your resources and data.
✓ Access to Qiskit® Runtime as a Service ✓ Access to 100+ qubit utility-scale systems	✓ Access to Qiskit Runtime as a Service ✓ Access to 100+ qubit utility-scale systems ✓ Access to IBM Quantum™ technical support	✓ Access to Qiskit Runtime as a Service ✓ Access to 100+ qubit utility-scale systems ✓ Access to IBM Quantum technical support ✓ IBM Quantum Network membership ✓ Optional access to our Quantum Accelerator offering ✓ Access to exploratory systems	✓ Access to Qiskit Runtime as a Service ✓ Access to 100+ qubit utility-scale systems ✓ Access to IBM Quantum technical support ✓ IBM Quantum Network membership ✓ Optional access to our Quantum Accelerator offering ✓ Full system capacity purchased as a service ✓ Optional system location on client site
Free Up to 10 minutes of runtime on utility-scale systems per month.	**$1.60 USD / second** Pay for what you need. Billed per second.	**Price varies** Access to additional systems & IBM quantum resources.	**Price varies** Access to an entirely dedicated quantum system, serviced and maintained for you by IBM.

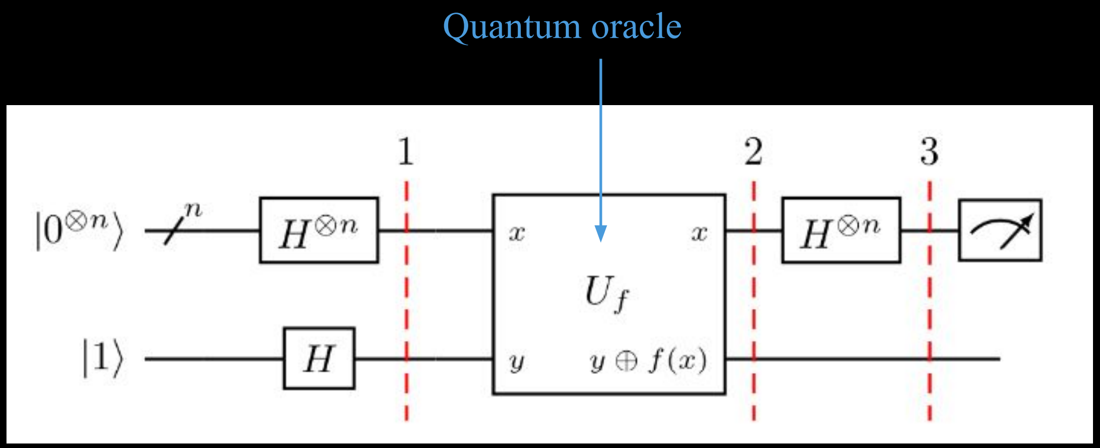
Free
Up to 10 minutes of runtime on utility-scale systems per month

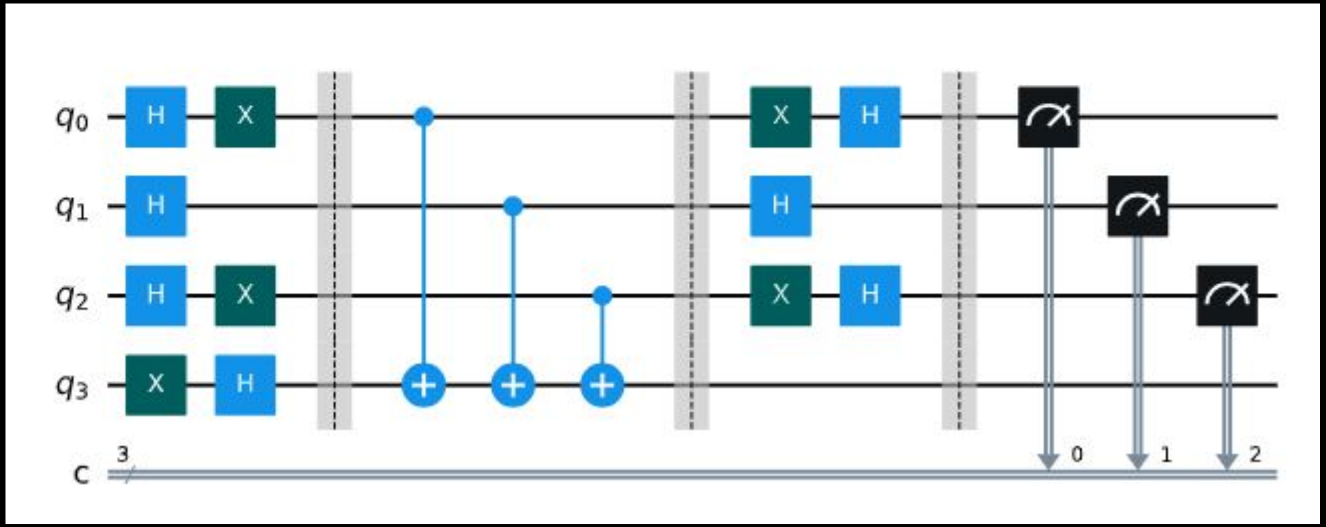
$1.60 USD / Second
Pay for what you need . Billed Per Second

QUANTUM ALGORITHMS-- PERFORMING BETTER THAN CLASSICAL ALGORITHMS

Deutsch-Jozsa algorithm (The oracle / search algorithm on specific problem)

- Generic circuit for the Deutsch-Jozsa algorithm
- https://learn.qiskit.org/course/ch-algorithms/deutsch-jozsa-algorithm

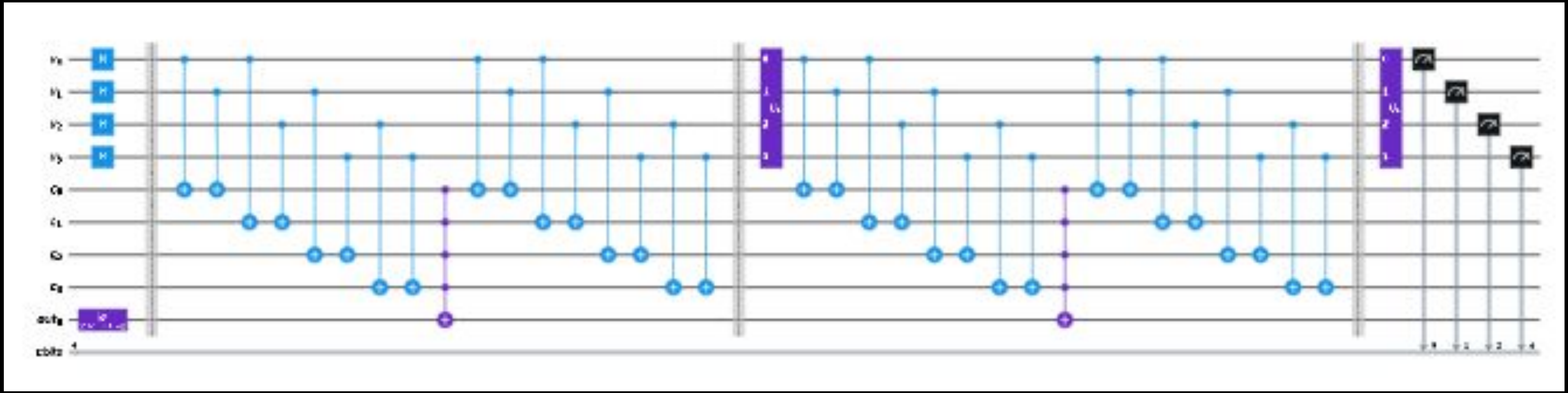




QUANTUM ALGORITHMS-- BREAKING CRYPTO BY SEARCHING THE KEY

IBMQ Qiskit implementation:

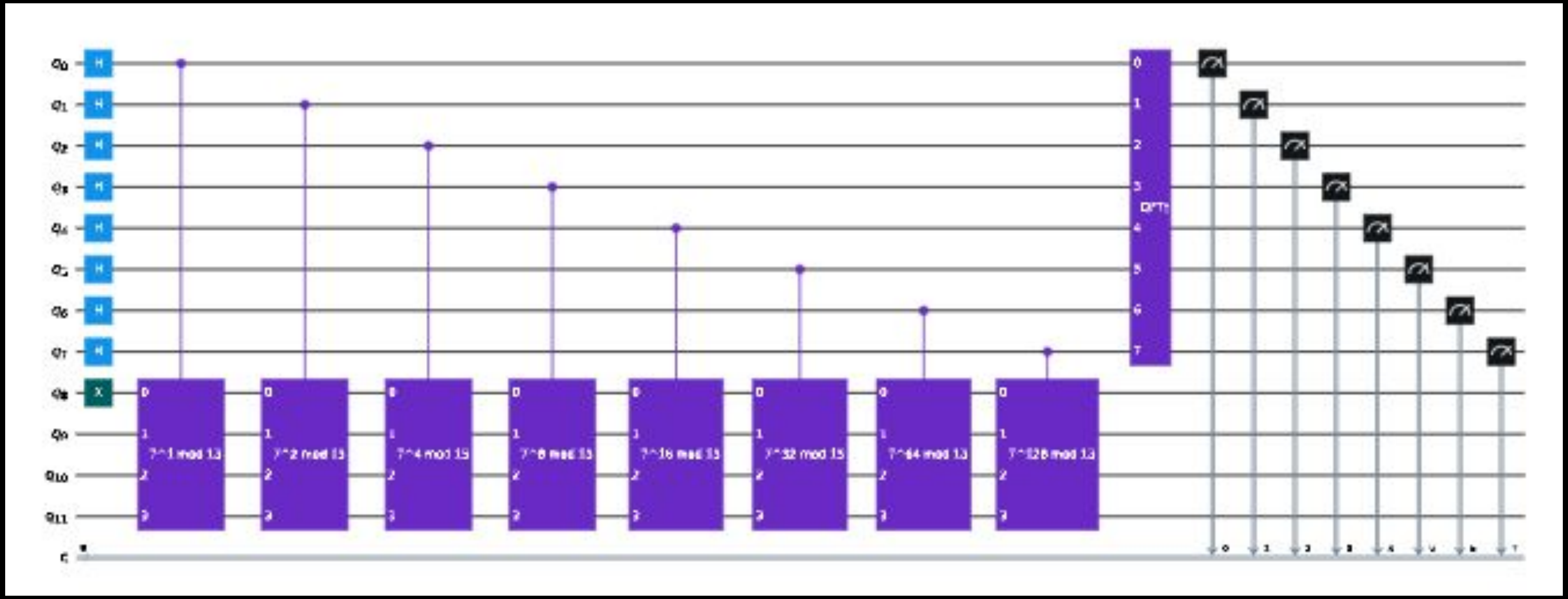
- Grover’s Algorithm unstructured Search problems
- https://learn.qiskit.org/course/ch-algorithms/grovers-algorithm



QUANTUM ALGORITHMS--
BREAKING PUBLIC KEY CRYPTO

IBMQ Qiskit implementation:

- Shor's Algorithm Factoring integers in polynomial time (two primes-RSA)
- https://learn.qiskit.org/course/ch-algorithms/shors-algorithm



MORE QUANTUM ALGORITHMS

Other quantum algorithms on IBMQ Qiskit ready for implementation:

- Simon’s Algorithm (exponential speed-up for factoring)
- Quantum Walk Search (classical Markov Chain-graph theory)
- QKD

Quantum attacks on AES (theoretically):

- Simon’s Algorithm
- Quantum Square
- Quantum DS-MITM (man in the middle attack)

Ref: Quantum Security Analysis of AES: https://eprint.iacr.org/2019/272.pdf

QUANTUM LIMITATION

- The more qubits, the faster/better the computation?? NOT REALLY
- High error rate (25%); need error correction
- Superconductor as quantum processors ; hardware limitation
- Super cold temperature (Ion-trap can operate at room temperature)

- In general, quadruple computation speed up only
- Accessibility to quantum processors/network

NIST PQC STANDARD— NOT YET HAVE ONE

Selected algorithms in 2022 and round 4 submission:

- Public-key encryption and key-establishment algorithms
  - CRYSTALS-KYBER
  - BIKE
  - Classic McEliece
  - HQC
- Digital Signature Algorithms
  - CRYSTALS-DILITHIUM
  - FALCON
  - SPHINCS+

August 24, 2023 — Comments Requested on Three Draft FIPS for Post-Quantum Cryptography

- Draft FIPS 203, *Module-Lattice-Based Key-Encapsulation Mechanism Standard*
- Draft FIPS 204, *Module-Lattice-Based Digital Signature Standard*
- Draft FIPS 205, *Stateless Hash-Based Digital Signature Standard*

https://csrc.nist.gov/projects/post-quantum-cryptography

REALITY VS MYTHS
WHAT IS ACTUALLY OUT THERE RIGHT NOW?

AWS--AMAZON BRAKET

- "fully managed quantum computing service…speed up scientific research and software development for quantum computing."

Gate-based superconducting processors

Superconducting qubits are built with superconducting electric circuits operating at cryogenic temperature. Amazon Braket provides access to quantum hardware based on superconducting qubits from Rigetti.

rigetti

OQC

Learn more about Rigetti gate-based superconducting processors »

Learn more about OQC gate-based superconducting processors »

Gate-based ion-trap processors

Trapped-ion quantum computers implement qubits using electronic states of charged atoms called ions. The ions are confined and suspended in free space using electromagnetic fields. Amazon Braket provides access to ion-trap quantum computers from IonQ.

IONQ

Learn more about gate-based ion-trap processors »

Neutral atom-based quantum processors

Rydberg atom-based quantum computers take advantage of long-range van der Waals interactions between neutral atoms arranged in one, two or three-dimensional arrays that can be addressed to simulate quantum systems of interest, beyond the capabilities of current classical computers. Amazon Braket provides access to Rydberg atom-based quantum computers from QuEra Computing.

|QuEra>
COMPUTING INC.

Learn more about QuEra Rydberg atom-based processors »

https://aws.amazon.com/braket/

AWS BRAKET PRICE

Quantum Computers (on-demand)

Hardware Provider	QPU family	Per-task price	Per-shot price
IonQ	Harmony	$0.30000	$0.01000
IonQ	Aria	$0.30000	$0.03000
OQC	Lucy	$0.30000	$0.00035
QuEra	Aquila	$0.30000	$0.01000
Rigetti	Aspen-M	$0.30000	$0.00035

Hardware Provider	QPU family	Per-hour rate
IonQ	Aria	$7,000.00
QuEra	Aquila	$2,500.00
Rigetti	Aspen-M-3	$3,000.00

EPB QUANTUM NETWORK—CHATTANOOGA, TN

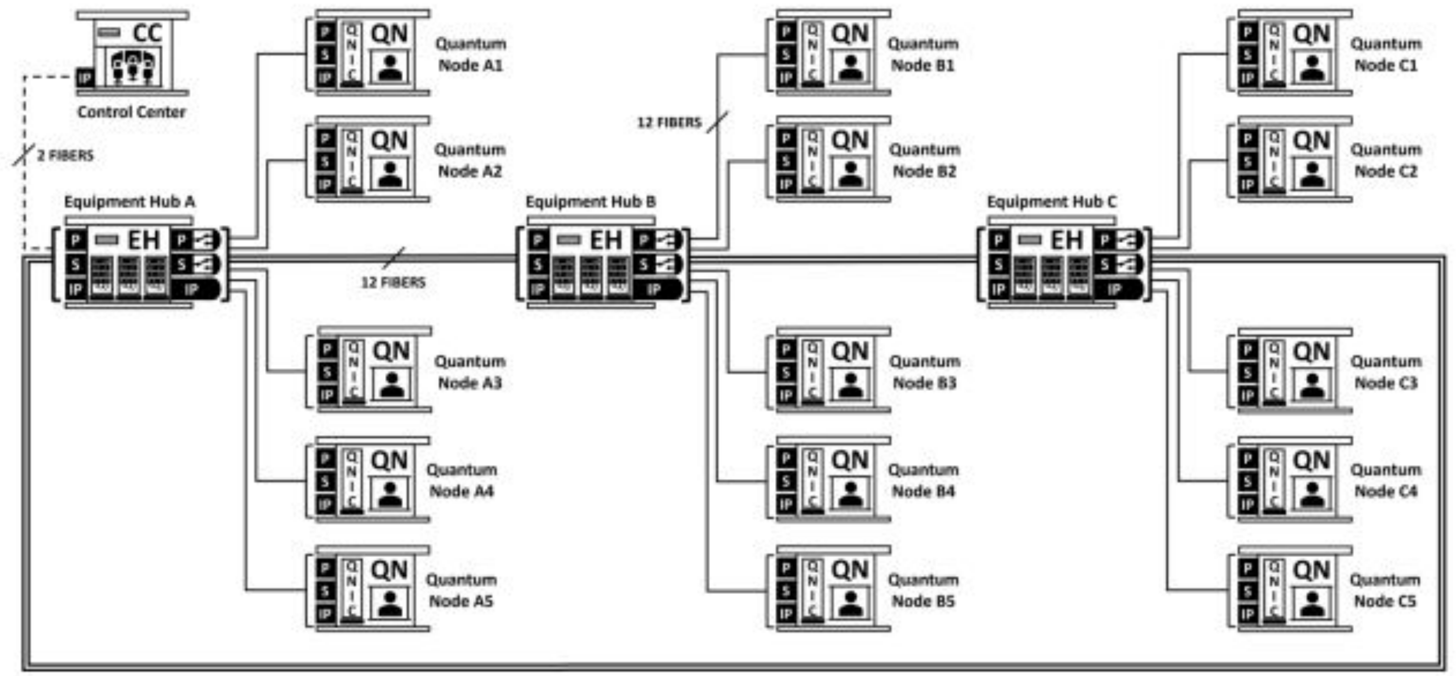
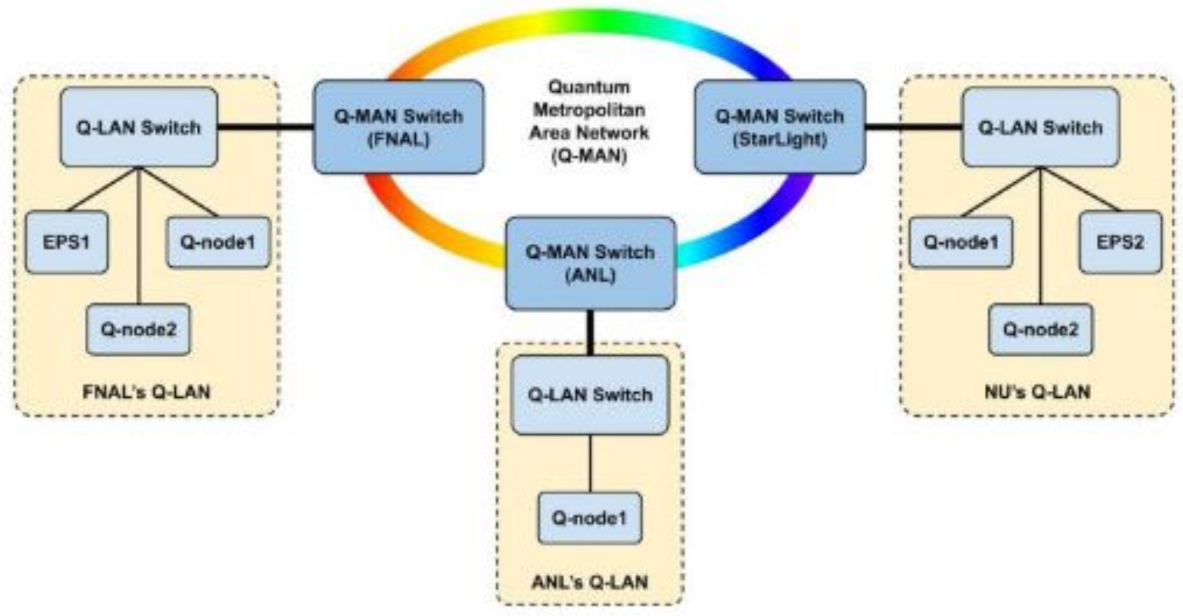


Fig. 6. **Bohr-IV Quantum Network Architecture:** Equipment Hubs are connected in a ring topology with five client Quantum Nodes connected to every Equipment Hub in a hub-and-spoke topology. This hybrid ring/spoke architecture is scaled by adding additional Equipment Hubs, which in turn adds additional Quantum Nodes.

https://arxiv.org/ftp/arxiv/papers/2211/2211.14871.pdf

IEQNET (ILLINOIS-EXPRESS QUANTUM NETWORK) METROPOLITAN TESTBED

- Research on architecture for a metropolitan-scale network
- Led by Fermilab (Dept of Energy)

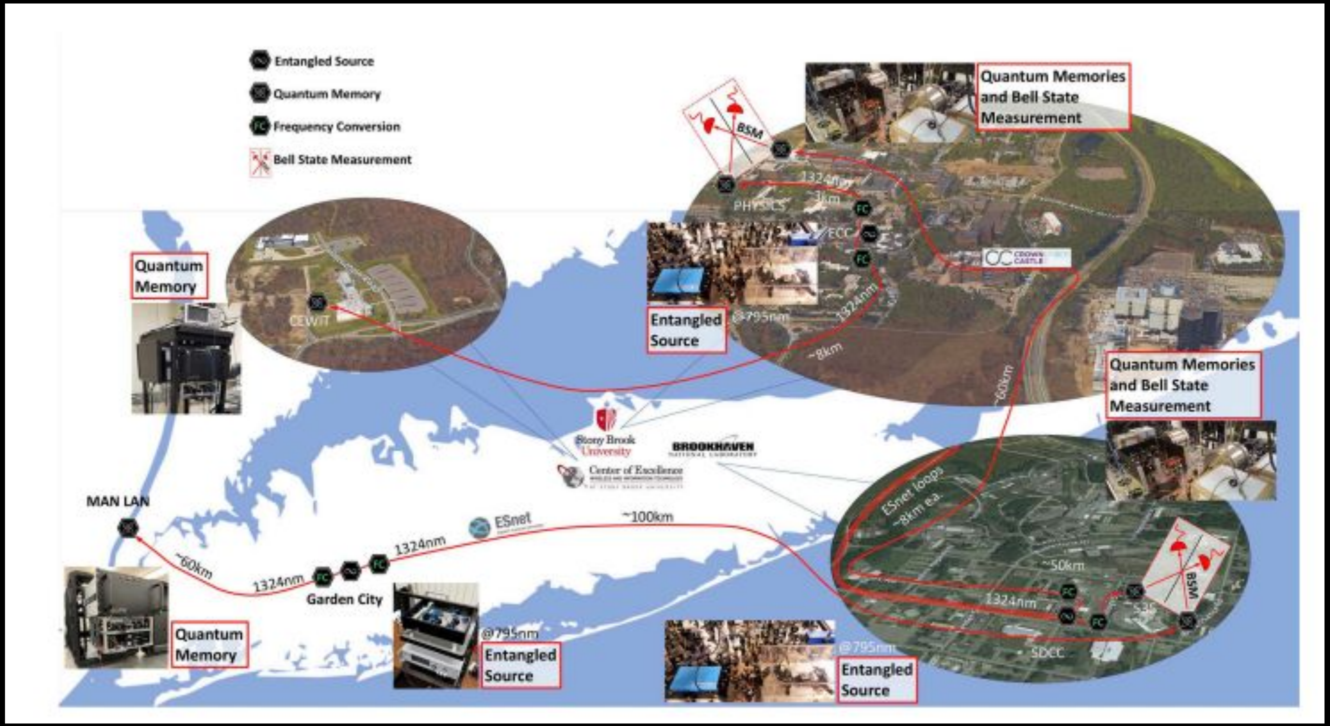


IEQNET metropolitan testbed

https://ieqnet.fnal.gov/

QUANTUM MEMORY NETWORK—LONG ISLAND, NY

- Brookhaven National Lab (BNL)+
- Stony Brook U (SBU)+
- DOE Energy Sciences Network (ESnet)
- Goal is to build a Q-LAN / Entanglement swapping



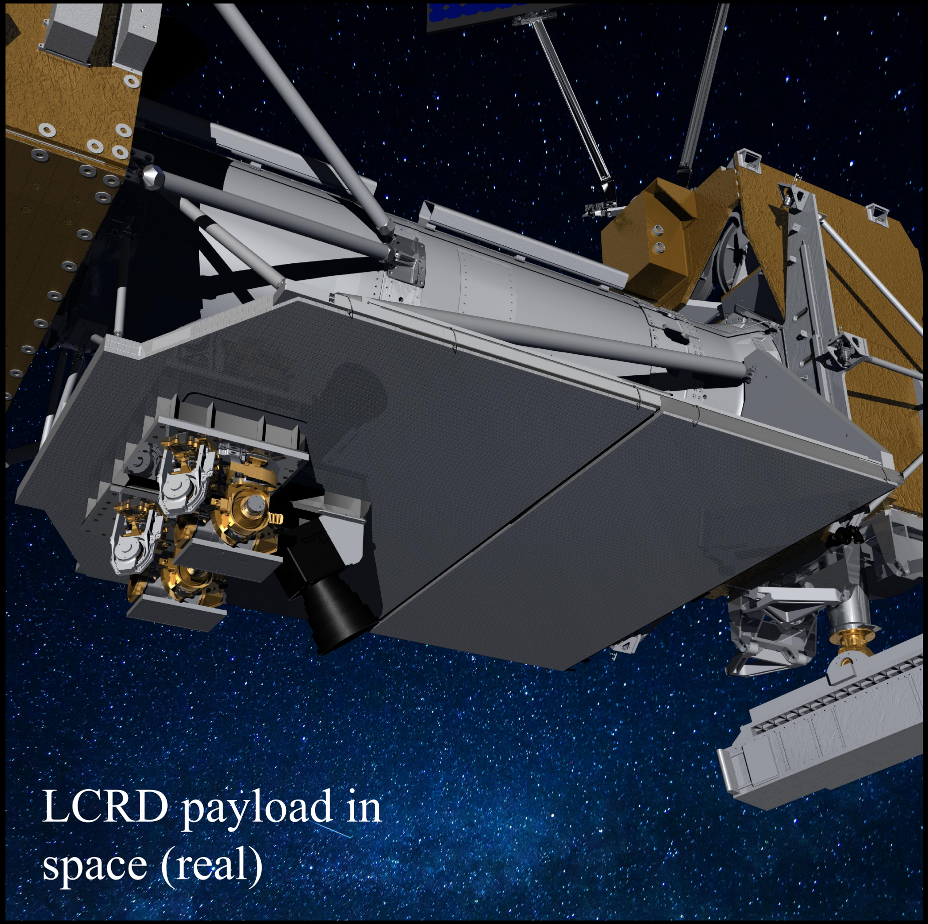
Vision for quantum internet
NOT REAL!

https://www.osti.gov/servlets/purl/1638794

NASA--LCRD
MISSION CENTER @ LAS CRUCES, NM

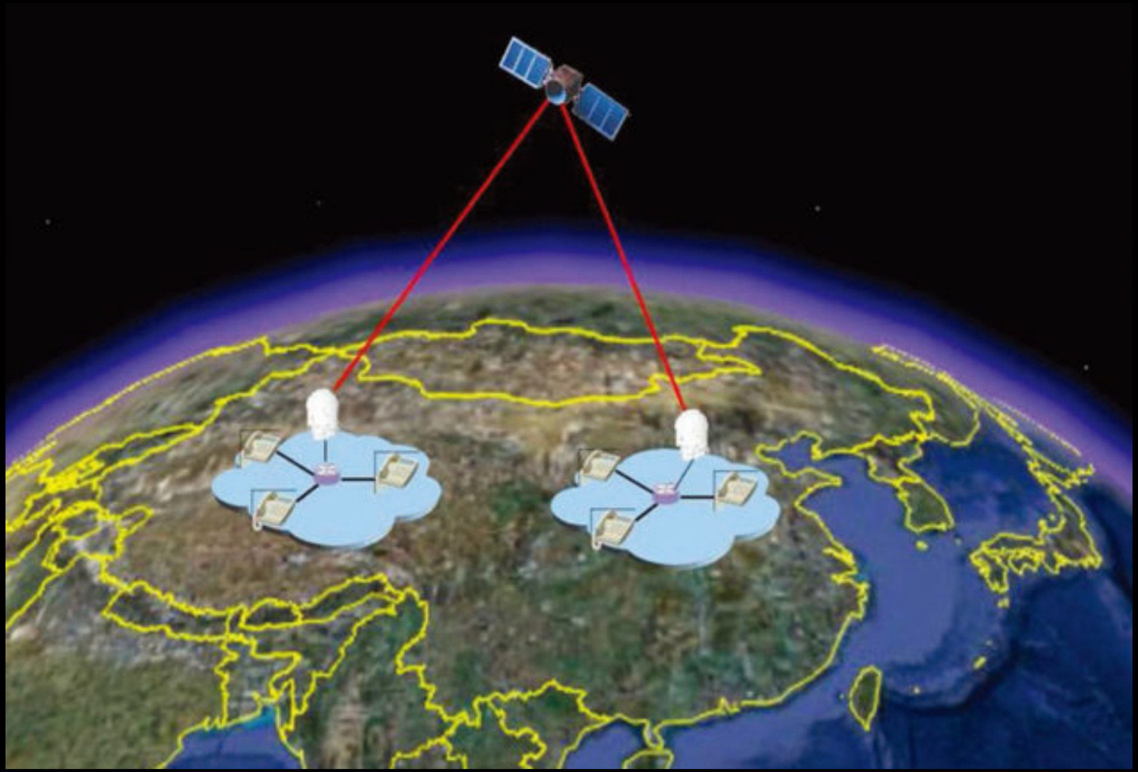
- LCRD--Laser Communications relay Demonstration
- Optical communications testbed in space
- Launched Dec 7, 2021

https://www.nasa.gov/mission_pages/tdm/lcrd/index.html



LCRD payload in space (real)

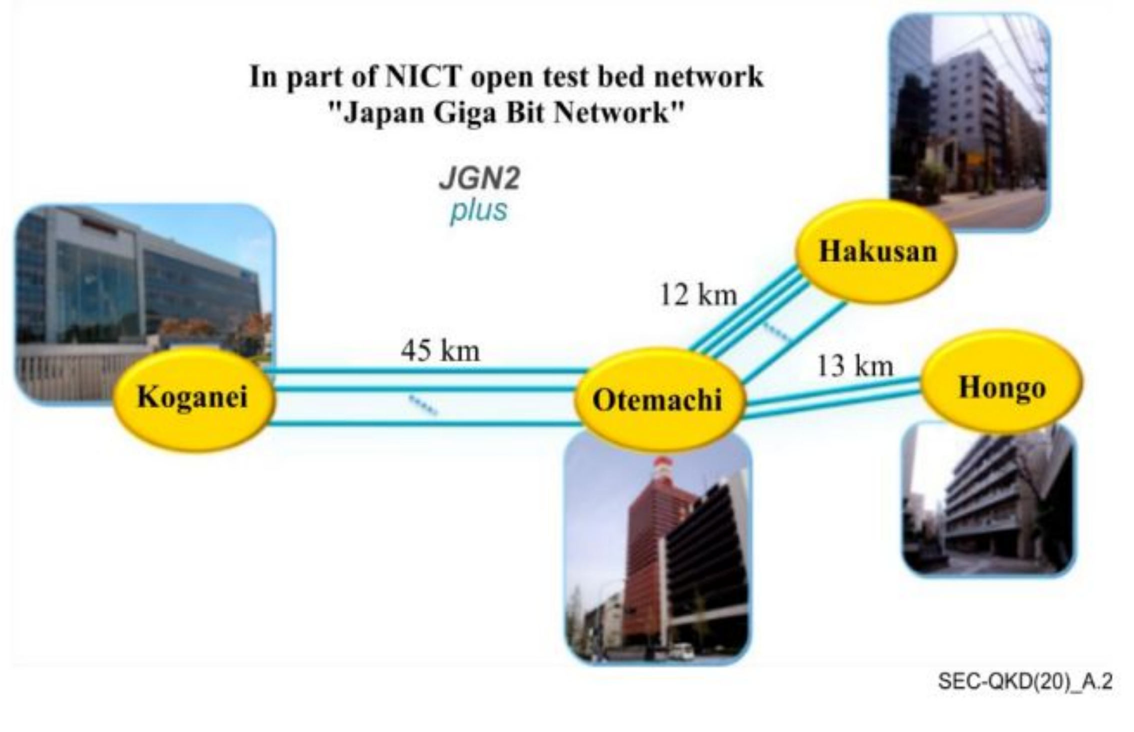
MICIUS—QUANTUM SATELLITE (CHINA)



- Launched 2016
- Satellite altitude– 500 km
- Two ground stations, Nanshan and Delingha, 1,120 km apart
- From a Chinese research project called QUESS—Quantum Experiments at Space Scale

QKD IMPLEMENTATION

- Tokyo QKD network



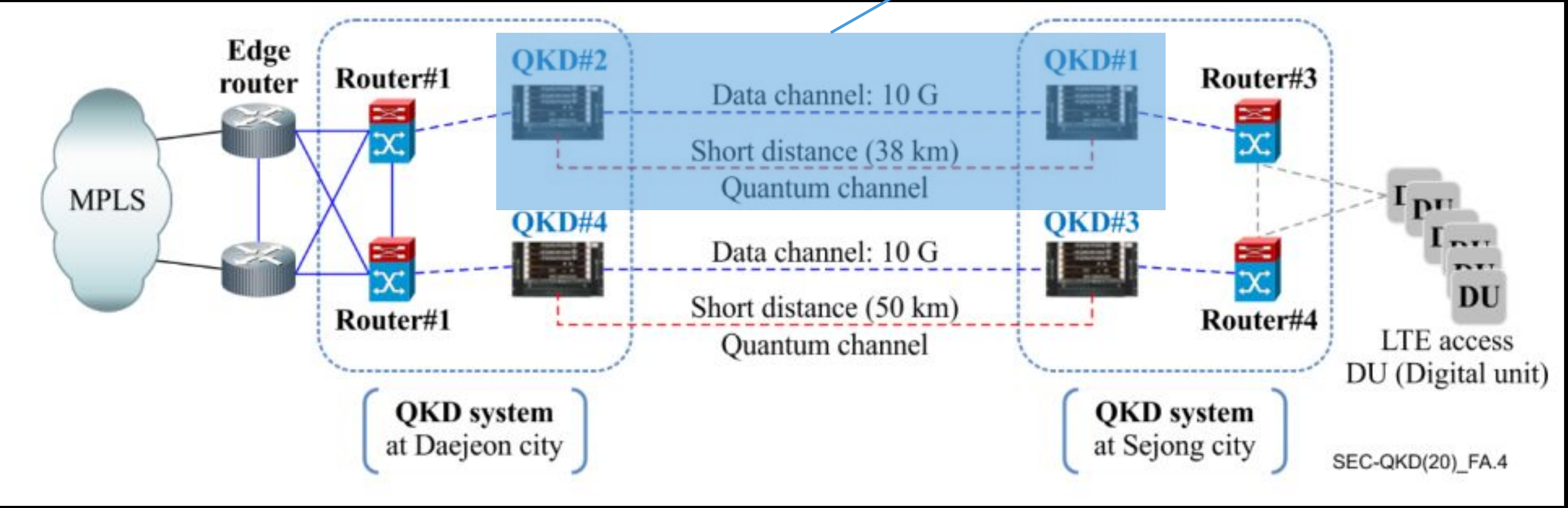
- Distance biggest obstacle
- Free space propagation
- Error rates and correcting
- No standards for quantum communication
- No nationwide quantum network yet
- Quantum layer Integrated with classical systems HOW ??
- Has its own set of vulnerabilities

  (NSA concerns)
- Need a framework to deploy securely

SOUTH KOREA QKD DEPLOYMENT

Commercially available

Data channel is the classical channel



QUBITEKK

HTTPS://QUBITEKK.COM/PRODUCTS/

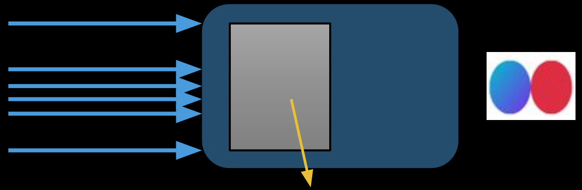
Polarization Entangled Photon Source

QKD devices

0 1 1 0..1 0 1 1 .. 0

0 0 1 1..0 1 1 1 .. 0

0 1 1 0..1 0 1 1 .. 0



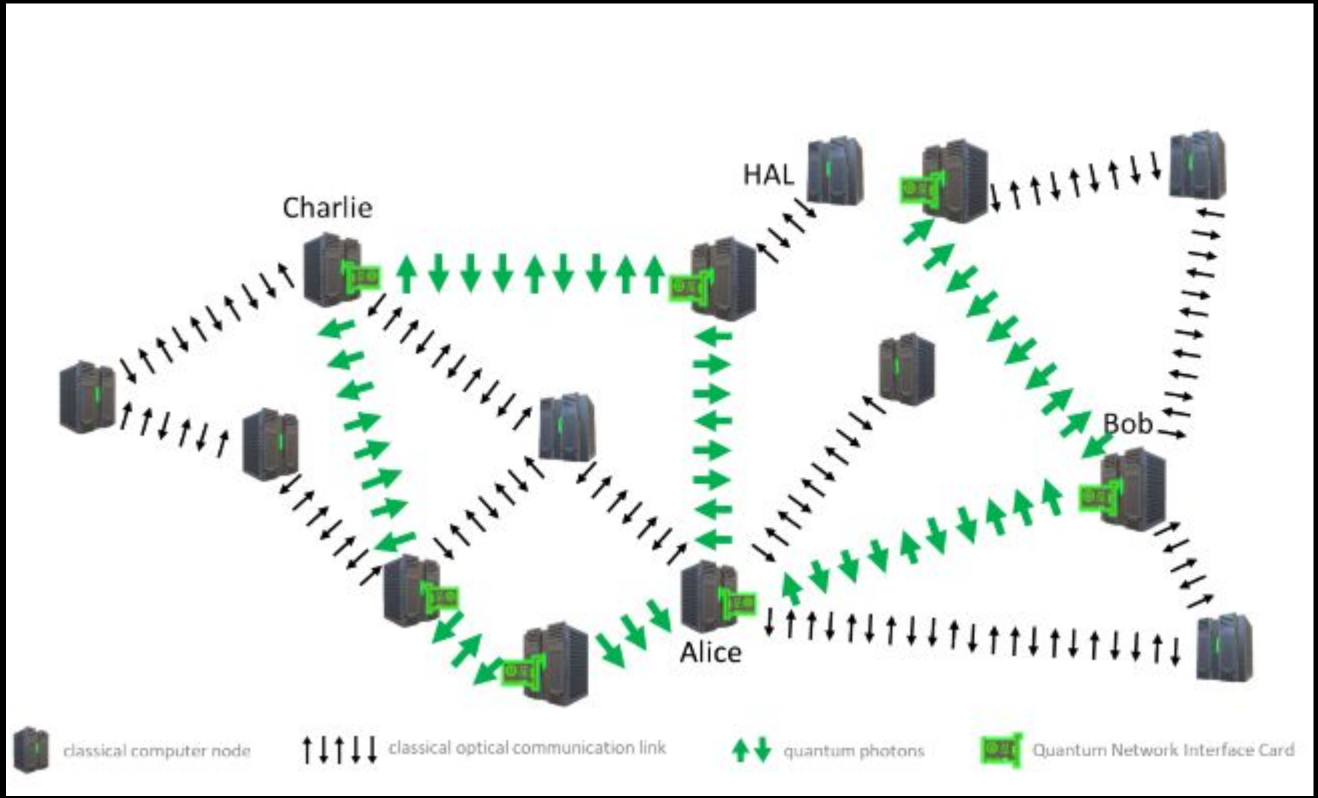
Special crystal

More than 10,000 pairs of entangled photons

Timing is extremely important

THE FUTURE? — DARPA PROGRAM QUANET

- Could this be the future?
- Quantum-Augmented Network (QuANET)
- A Network Security Revolution Enhanced By Quantum Communication



Topology with quantum and classical links

https://sam.gov/opp/60917f7ea74845bf8f6aaa1382813f86/view

REFERENCE AND ARTICLES

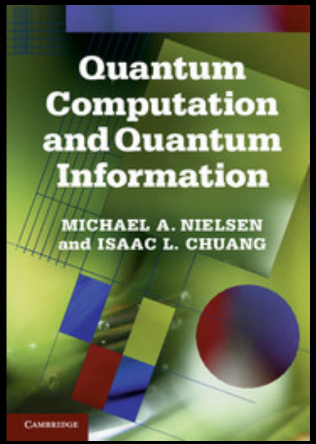
Quantum Computation and Quantum Information, Michael Nielsen and Isaac Chuang, Cambridge University, 2000.

International Telecommunication Union Technical Report, March 2020

- https://www.standict.eu/sites/default/files/2022-01/T-TUT-QKD-2020-1-PDF-E.pdf

From Long-distance Entanglement to building a nationwide quantum internet, US Dept of Energy, July 2020

- https://www.osti.gov/servlets/purl/1638794



Thank you !!

BACK UP SLIDES PART 1-
IBMQ LAB

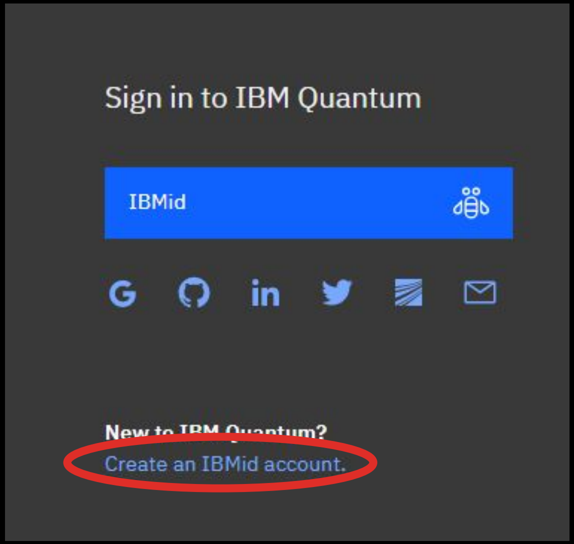
IBM QUANTUM INTRO TO QISKIT

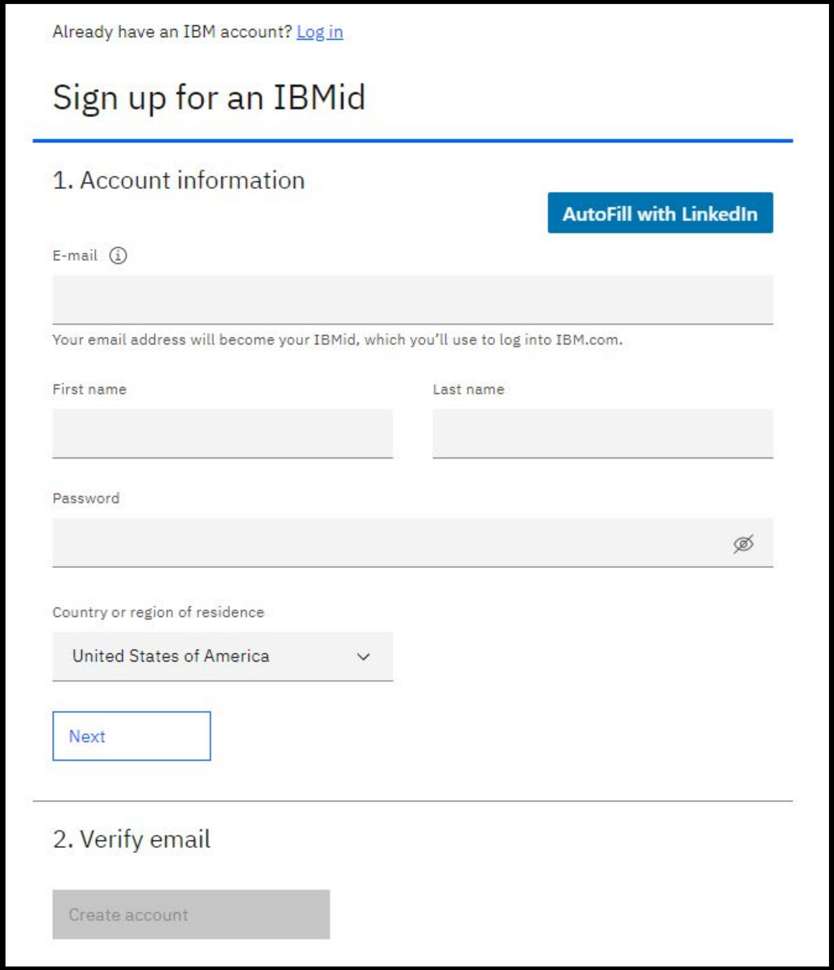
QISKIT

Open source platform-Qiskit:

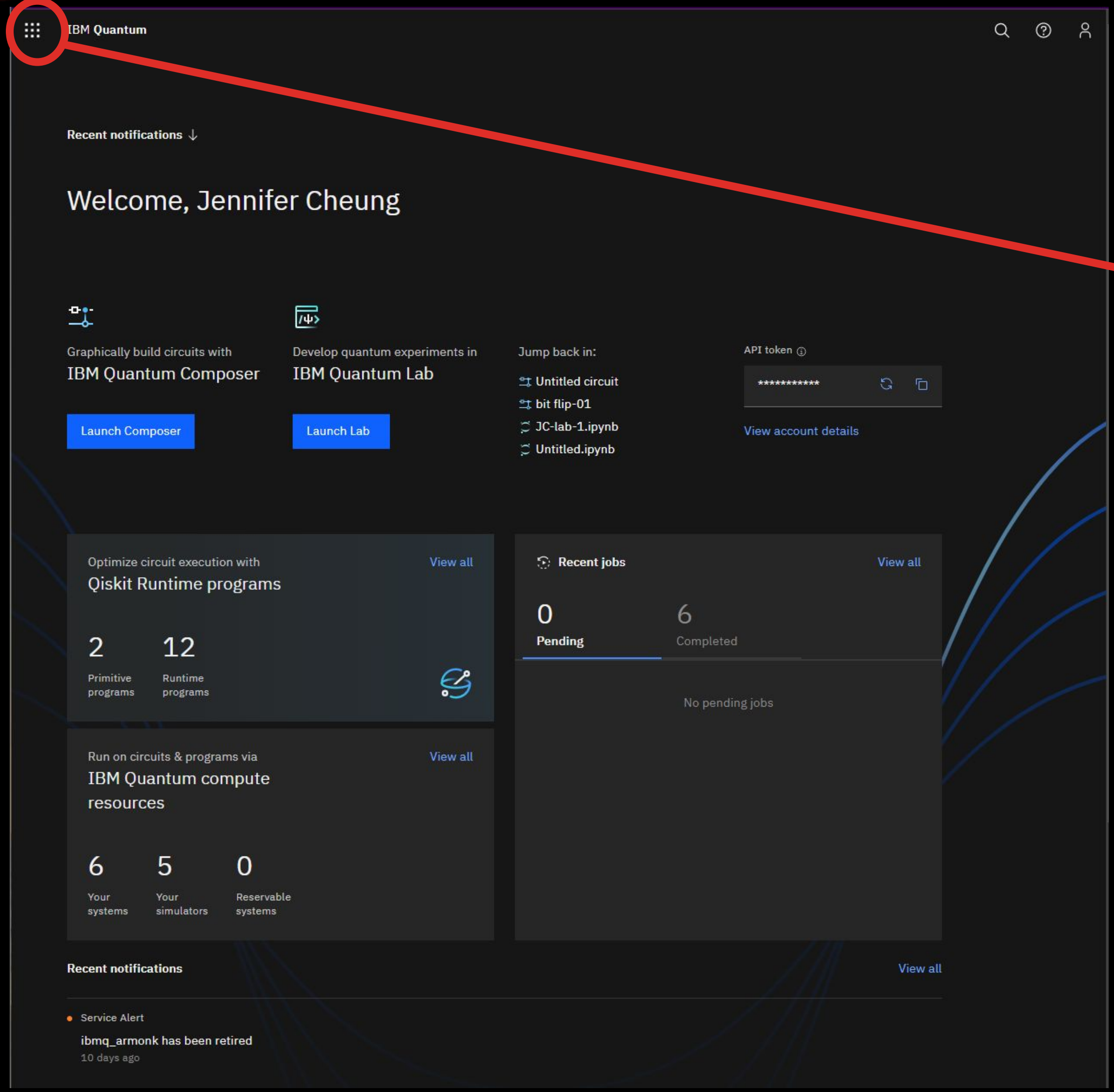
https://quantum-computing.ibm.com/

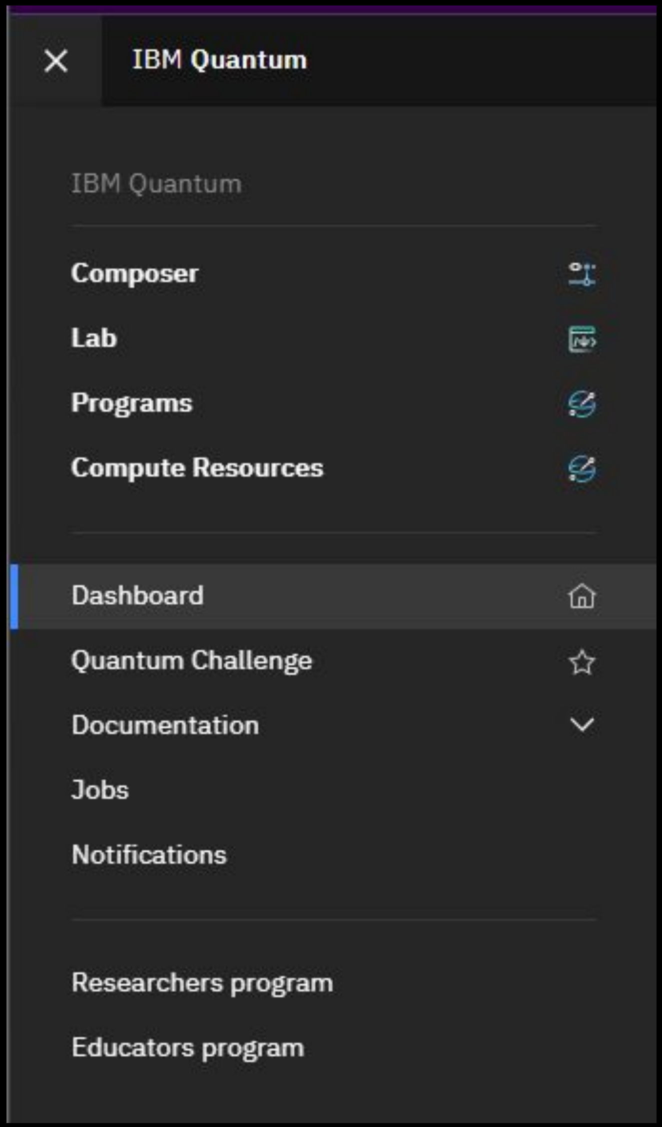
Create an IBMid account:



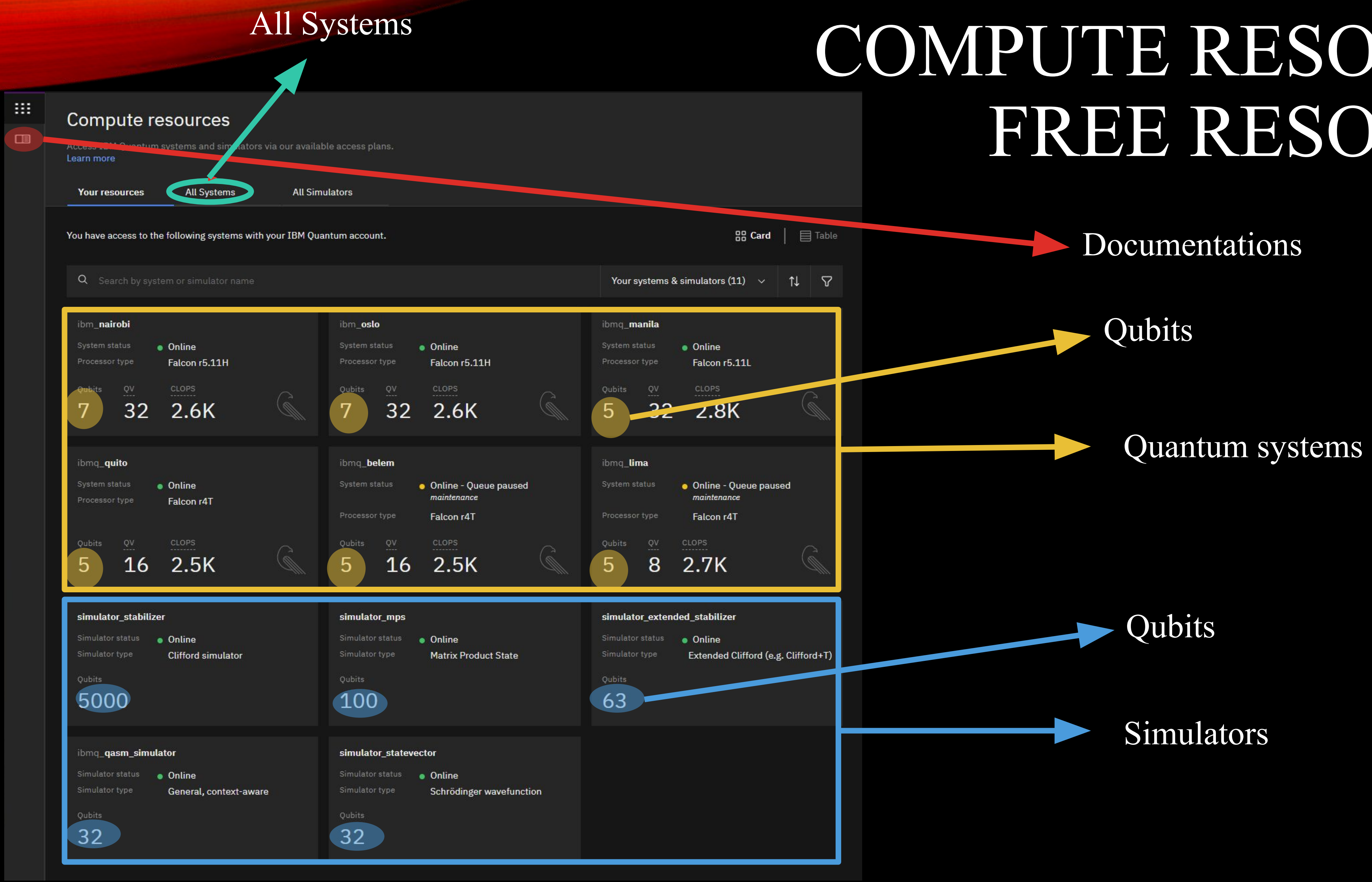


DASHBOARD


IBM Quantum
Recent notifications
Welcome, Jennifer Cheung
Graphically build circuits with
IBM Quantum Composer
Launch Composer
Develop quantum experiments in
IBM Quantum Lab
Launch Lab
Jump back in:
Untitled circuit
bit flip-01
JC-lab-1.ipynb
Untitled.ipynb
API token
View account details
Optimize circuit execution with
Qiskit Runtime programs
View all
2
Primitive programs
12
Runtime programs
Recent jobs
View all
0
Pending
6
Completed
No pending jobs
Run on circuits & programs via
IBM Quantum compute resources
View all
6
Your systems
5
Your simulators
0
Reservable systems
Recent notifications
View all
Service Alert
ibmq_armonk has been retired
10 days ago


IBM Quantum
IBM Quantum
Composer
Lab
Programs
Compute Resources
Dashboard
Quantum Challenge
Documentation
Jobs
Notifications
Researchers program
Educators program

COMPUTE RESOURCES FREE RESOURCES



QUANTUM PROCESSORS
ALL SYSTEMS

Your resources | **All Systems** | All Simulators

New pay-as-you-go access to 27 qubit systems on IBM Cloud Learn more

Card | **Table**

Search by system name

ame	Qubits	QV	CLOPS	Status	Total pending jobs	Processor type	Plan
ibm_peekskill Exploratory	27	1	-	Online	0	Falcon r8	premium
ibmq_guadalupe	16	32	2.4K	Online	0	Falcon r4P	premium
ibm_perth	7	32	2.9K	Online	11	Falcon r5.11H	premium
ibm_lagos	7	32	2.7K	Online	84	Falcon r5.11H	premium
m_nairobi	7	32	2.6K	Online	19	Falcon r5.11H	open
m_oslo	7	32	2.6K	Online	11	Falcon r5.11H	open
ibmq_jakarta	7	16	2.4K	Online	3	Falcon r5.11H	premium
mq_manila	5	32	2.8K	Online	11	Falcon r5.11L	open
mq_quito	5	16	2.5K	Online	9	Falcon r4T	open
mq_belem	5	16	2.5K	Online - Queue paused	46	Falcon r4T	open

Items per page: 10 | 11-20 of 21 items | 2 of 3 pages

ibm_ithaca Exploratory

System status: Online

Processor type: Hummingbird r3

Qubits: 65

ibm_washington Exploratory

System status: Online - Queue paused *maintenance*

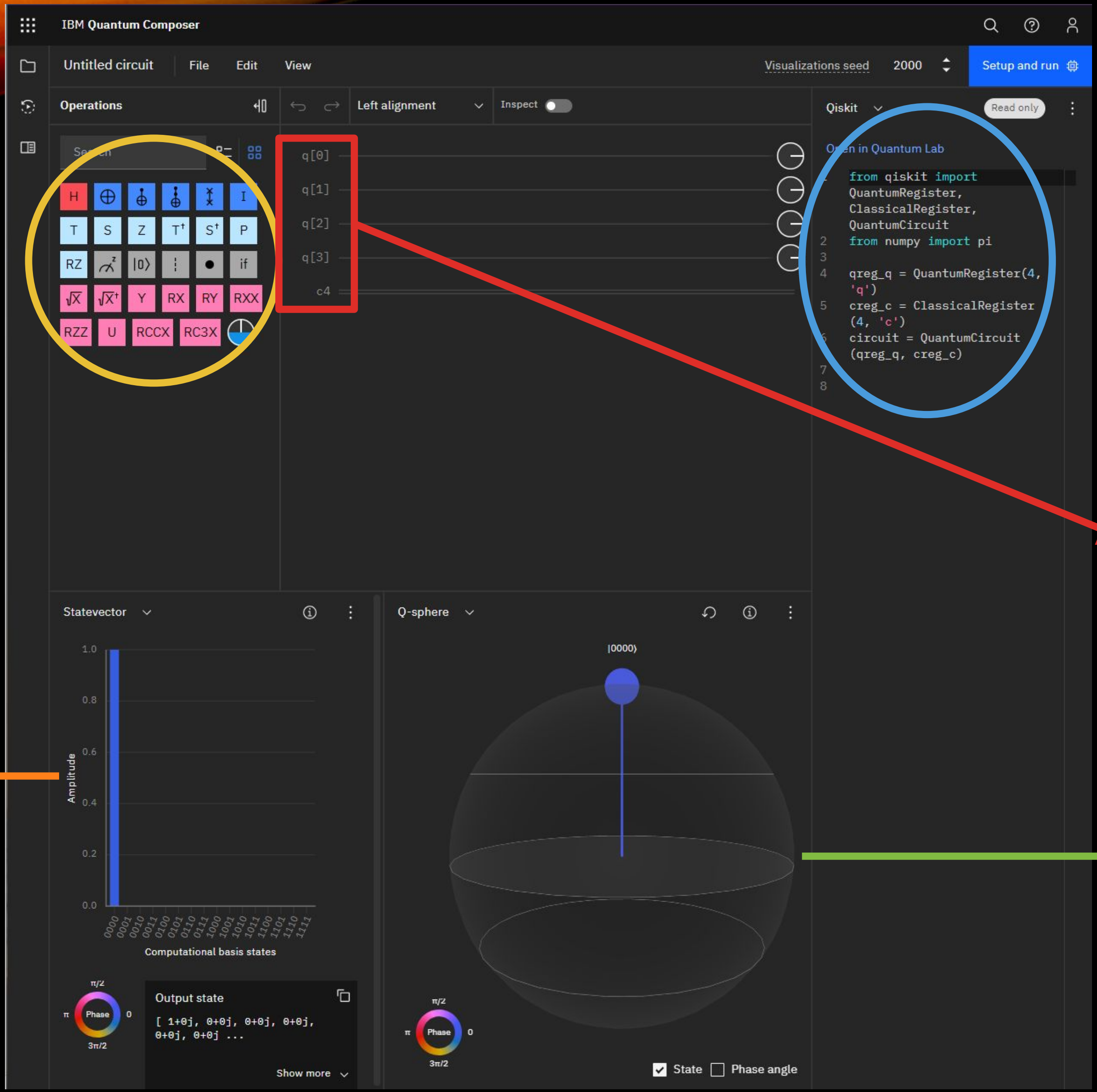
Processor type: Eagle r1

Qubits: 127 | QV: 64 | CLOPS: 850

COMPOSER

Quantum gates

Python 3.0 code

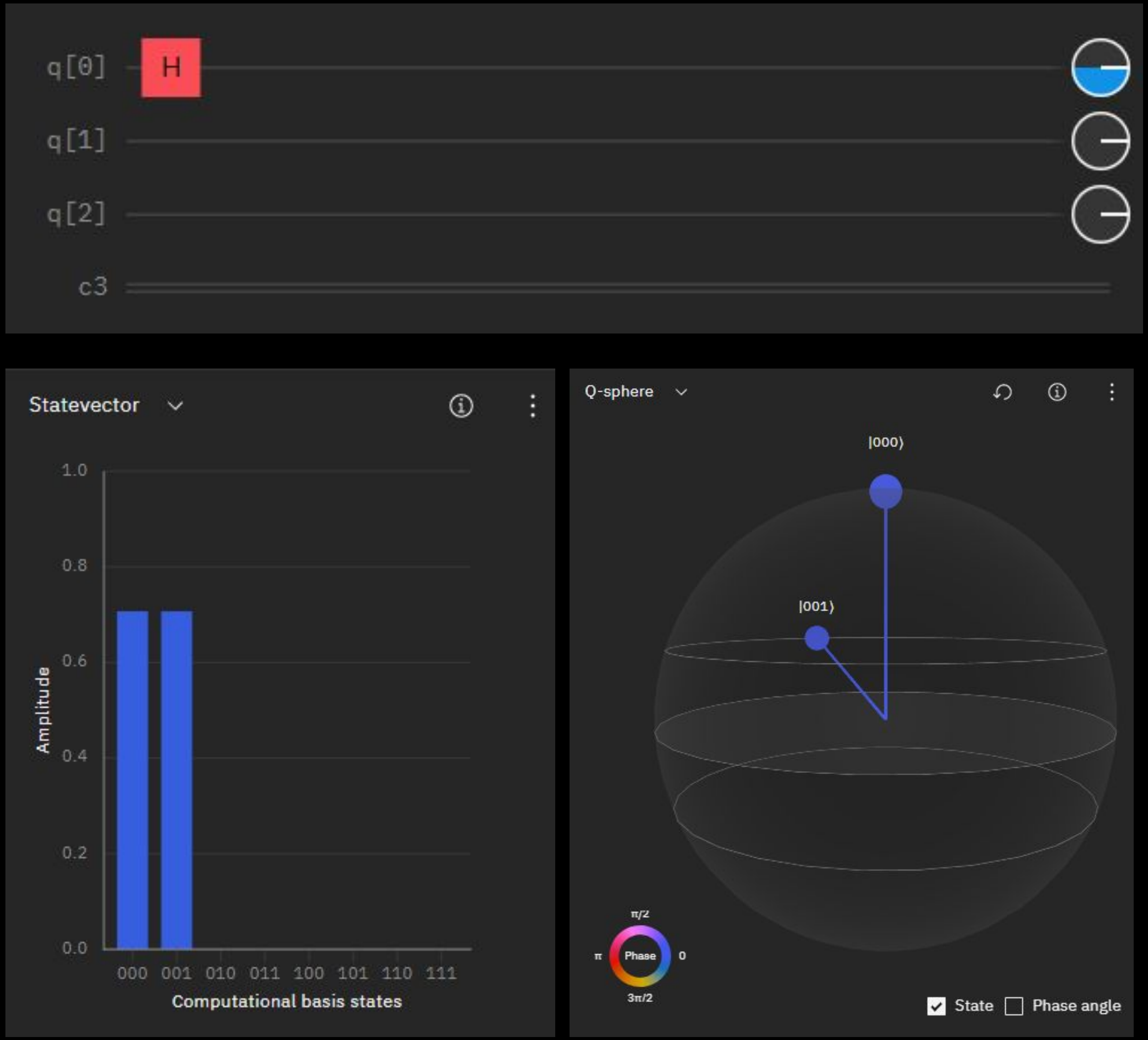


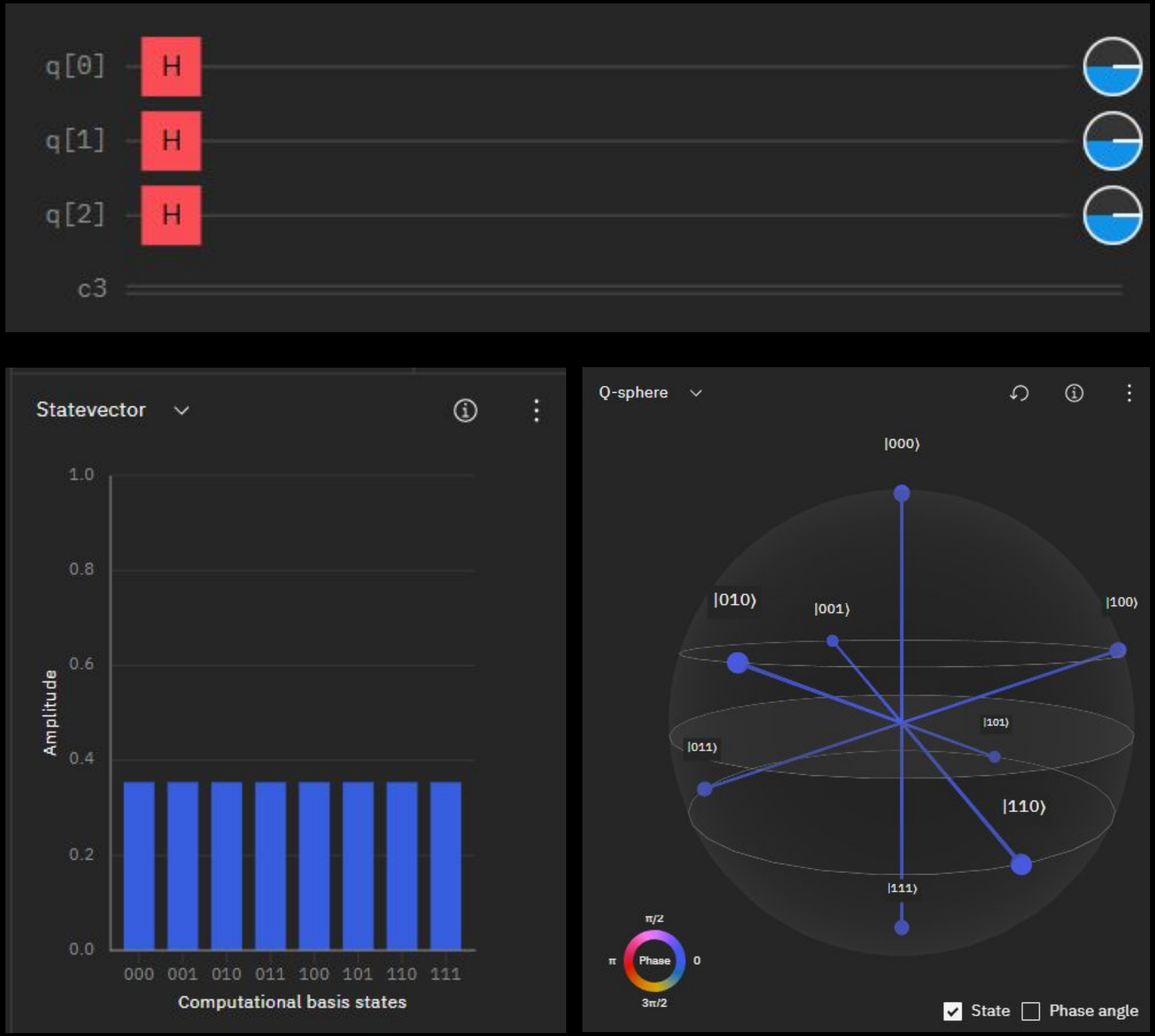
Number of qubits

Probabilities

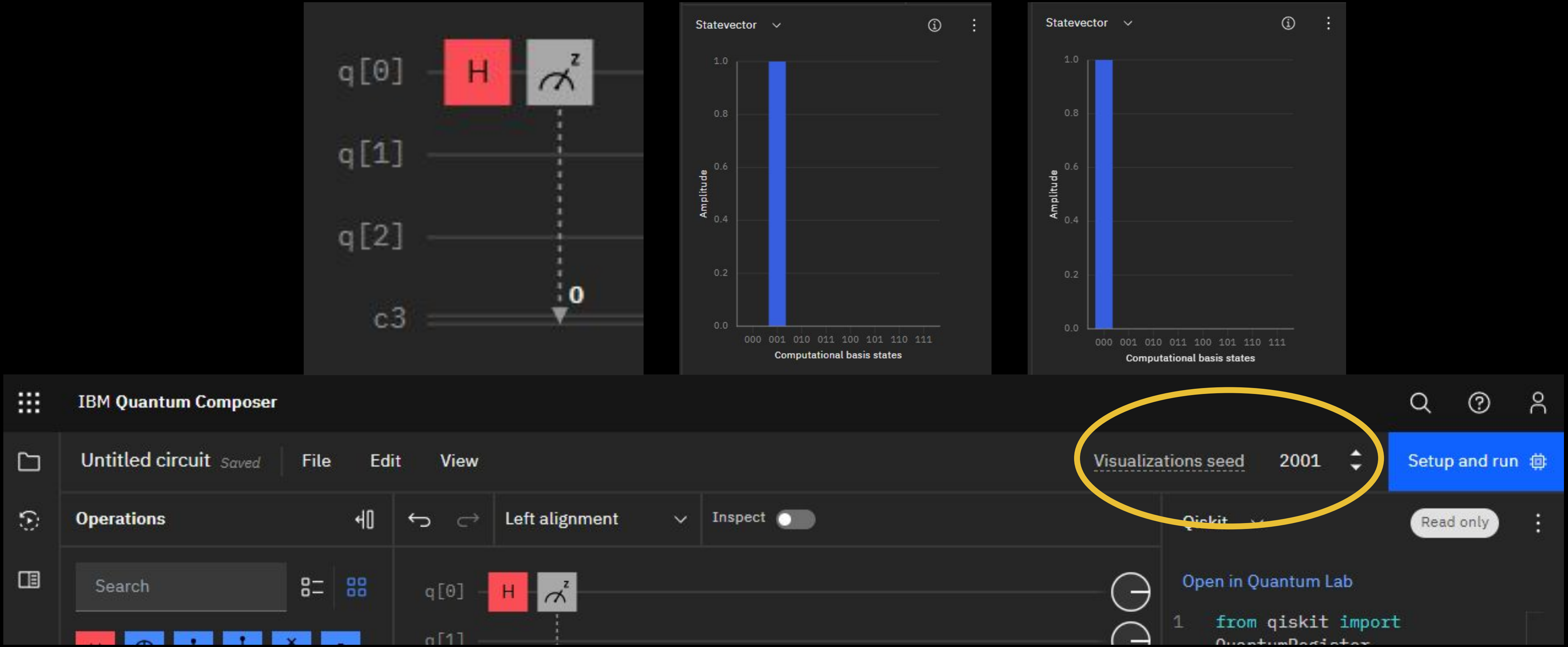
Bloch sphere

EXAMPLE--3 QUBITS

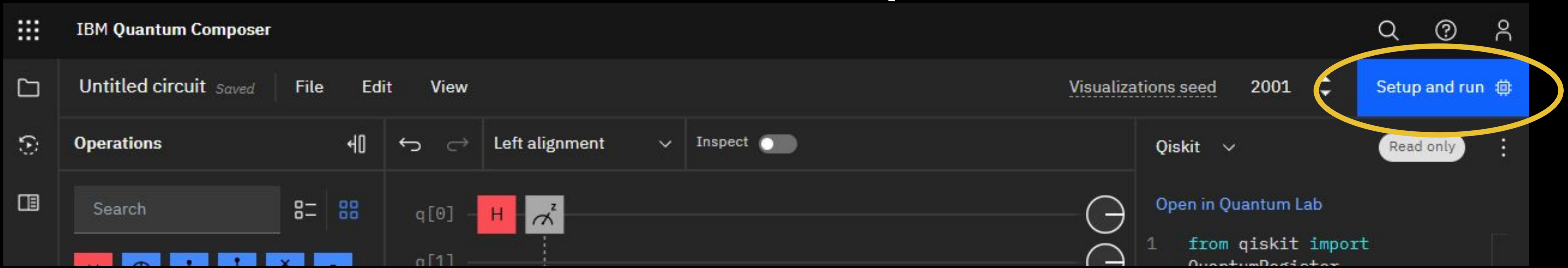


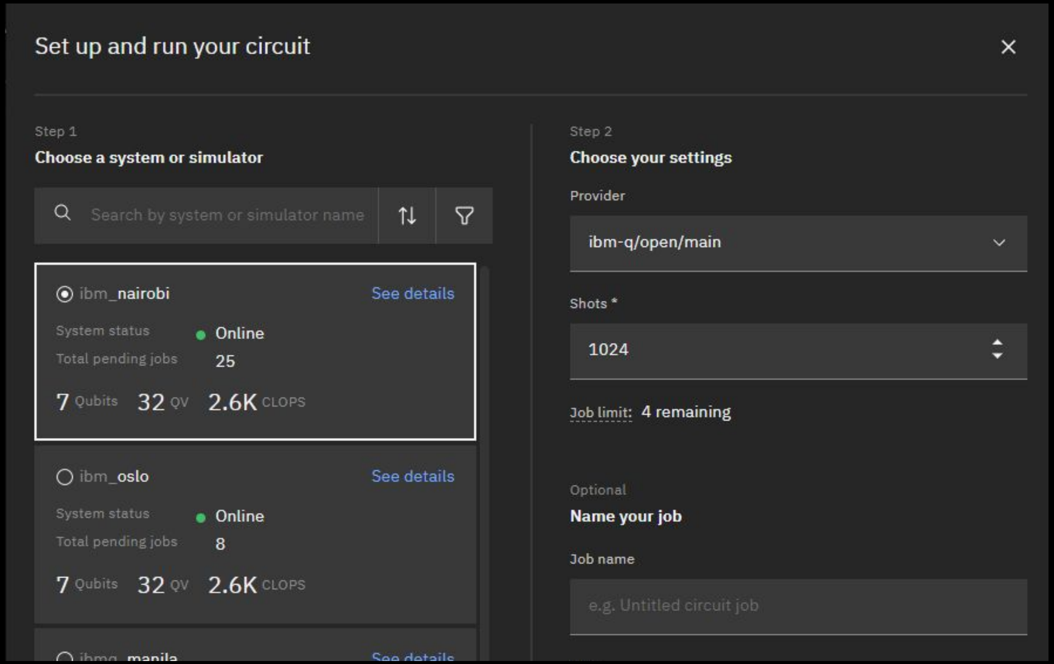


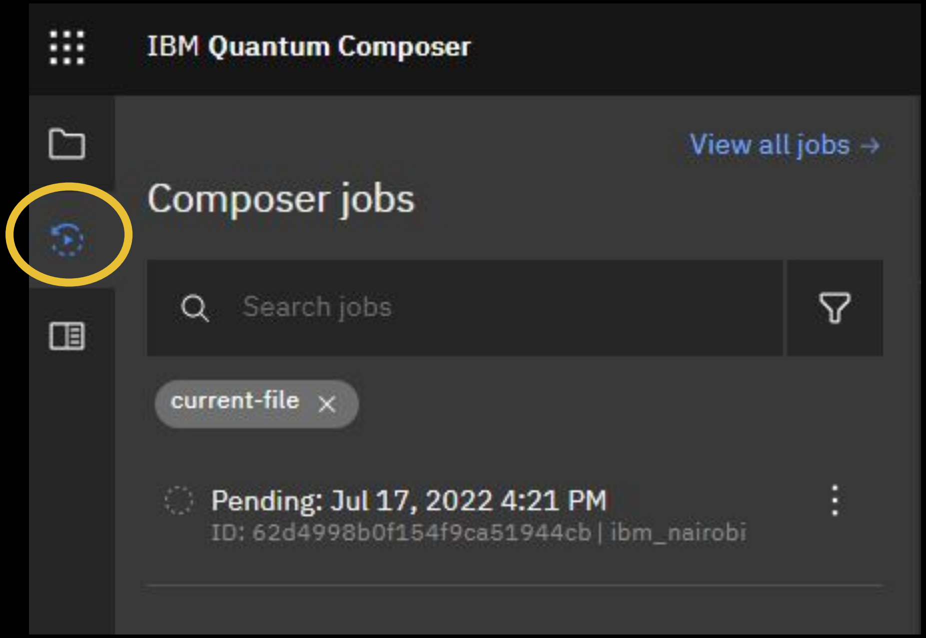
MEASUREMENT



RUNNING THE QUANTUM CIRCUIT







PYTHON CODE

Qiskit Read only

Open in Quantum Lab

```
1  from qiskit import QuantumRegister, ClassicalRegister, QuantumCircuit
2  from numpy import pi
3
4  qreg_q = QuantumRegister(4, 'q')
5  creg_c = ClassicalRegister(4, 'c')
6  circuit = QuantumCircuit(qreg_q, creg_c)
7
8  circuit.h(qreg_q[0])
9  circuit.h(qreg_q[1])
10 circuit.h(qreg_q[2])
11 circuit.cx(qreg_q[0], qreg_q[1])
12 circuit.ccx(qreg_q[1], qreg_q[2], qreg_q[3])
13 circuit.measure(qreg_q[2], creg_c[2])
```

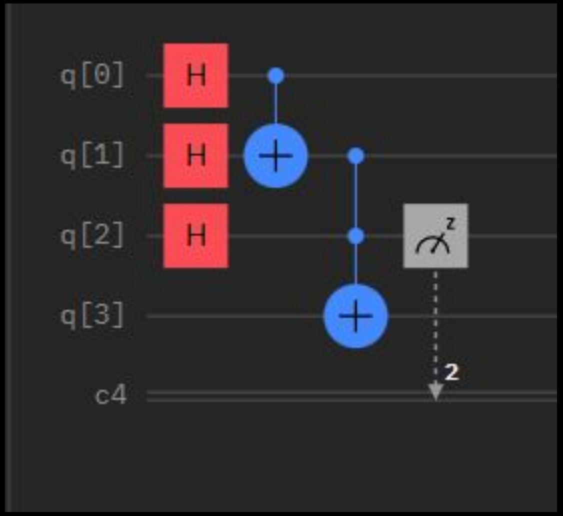
1 and 2
Loading packages

4 = set the size of the circuit, building the circuit with 4 qubits
5 = measurement, classical bits
6 = name of this circuit

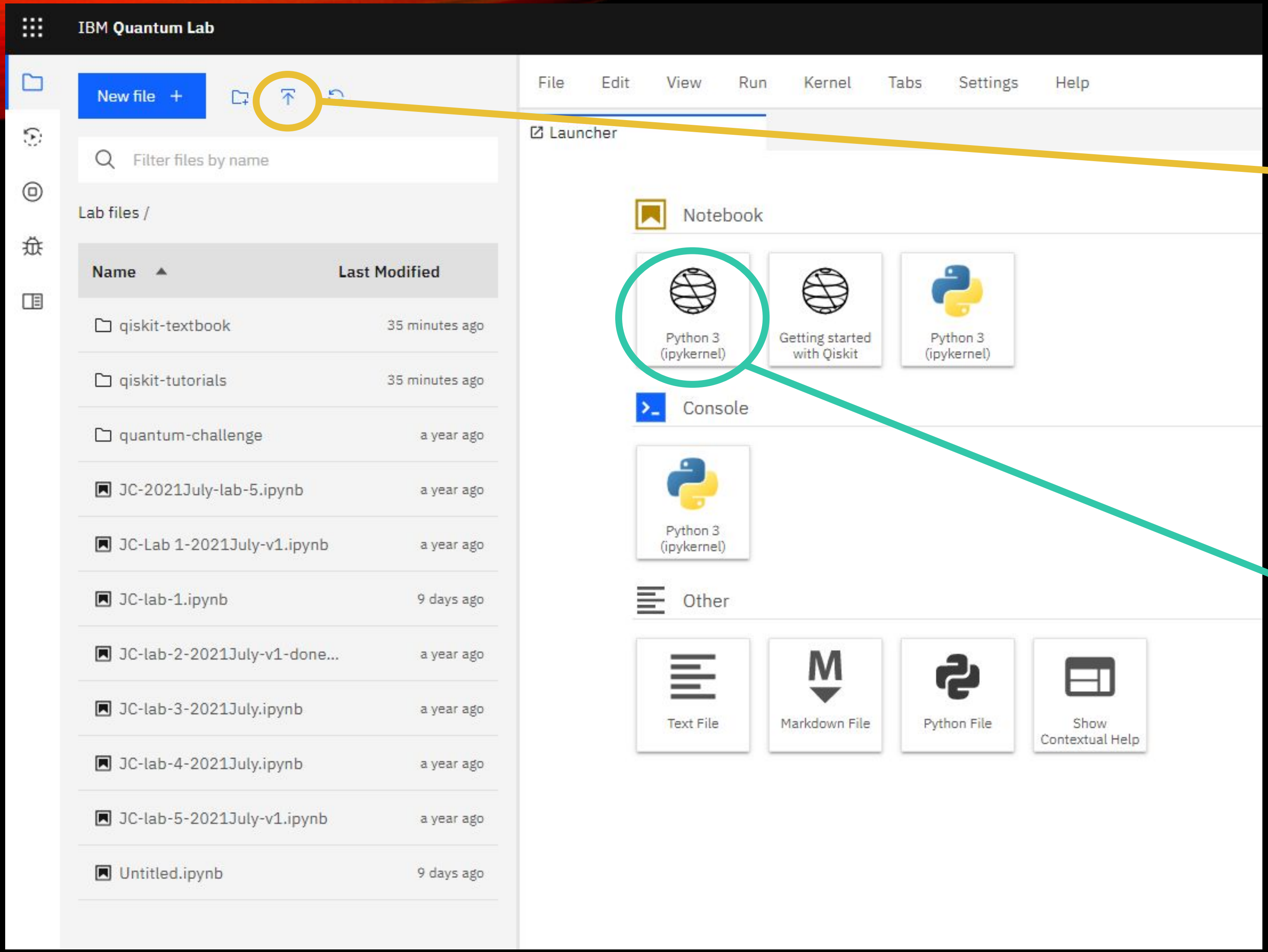
8-10 = apply Hadamard transformation to 3 of the 4 qubits

11 = CNOT gate; q[0] as input bit and q[1] as target bit
12 = Toffoli gate; q[1] and q[2] as input bits and q[3] as target bit

13 = measure q[2] and register on c[2]



LAB



Upload notebooks