

# CYBERSECURITY IN THE POST QUANTUM WORLD

Jennifer Cheung

March 14, 2024



# WHO AM I?



MS--Applied  
Math (2010)

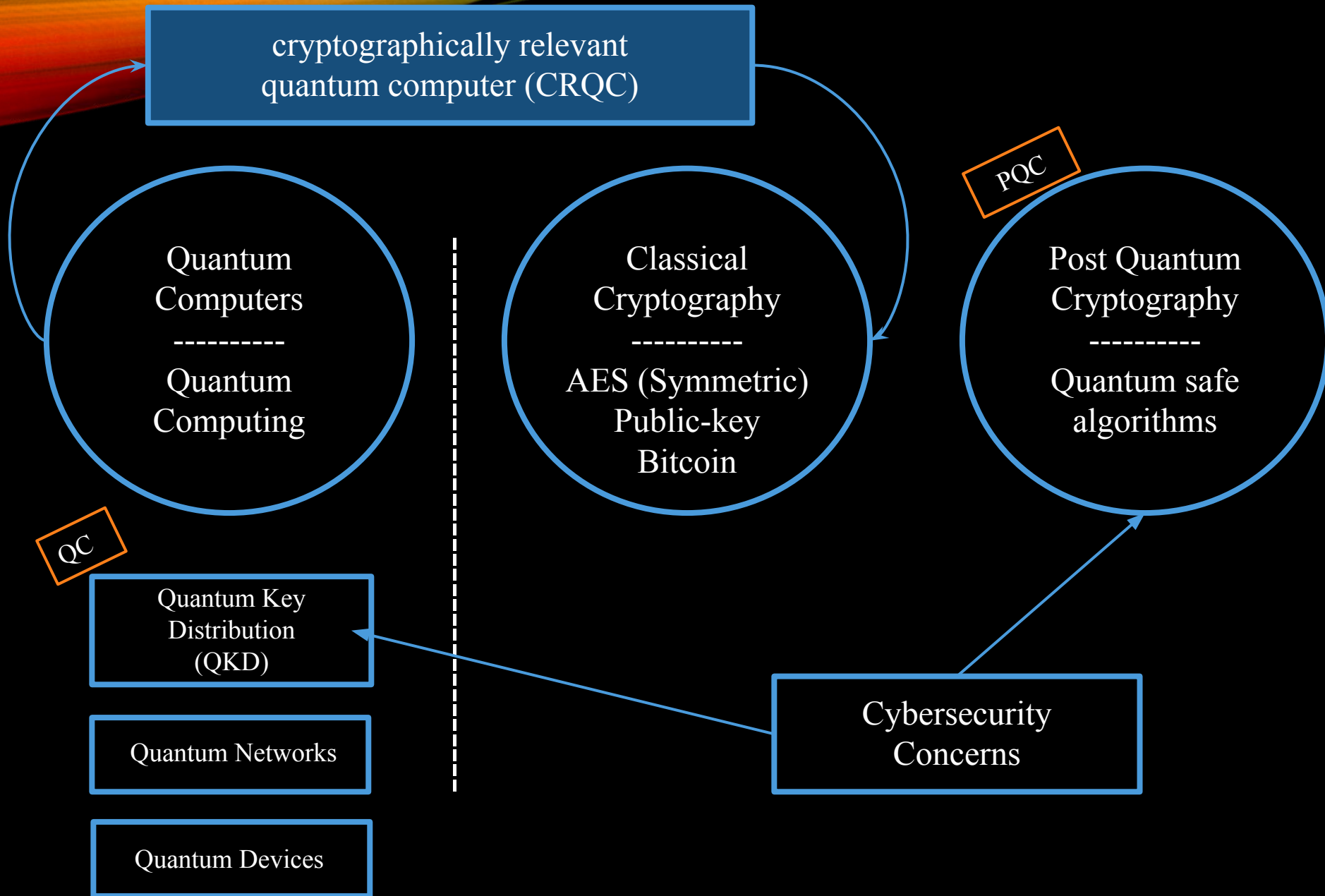


Study & Research Grant:  
Quantum Informatics /  
Cryptography  
(2011-2012)



Computer Science Dept  
Aarhus University Aarhus,  
Denmark

Quantum Technologies



Classical Network

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

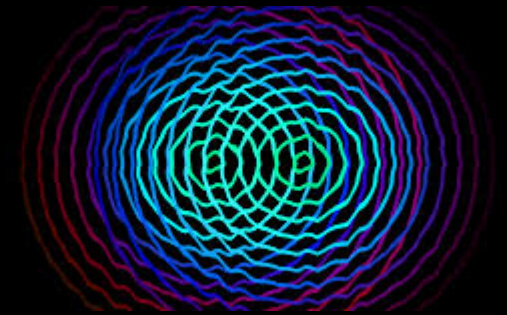
PQC (new standards just released from NIST:

<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)

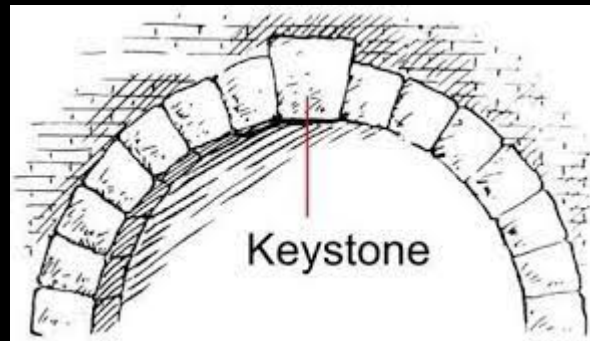
- No quantum computing /quantum Protocol
- provide **provable** security of information exchange
- No encryption or decryption; **information becomes physical** carried by photons
- Use to share private keys with symmetric key cryptography



# 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.

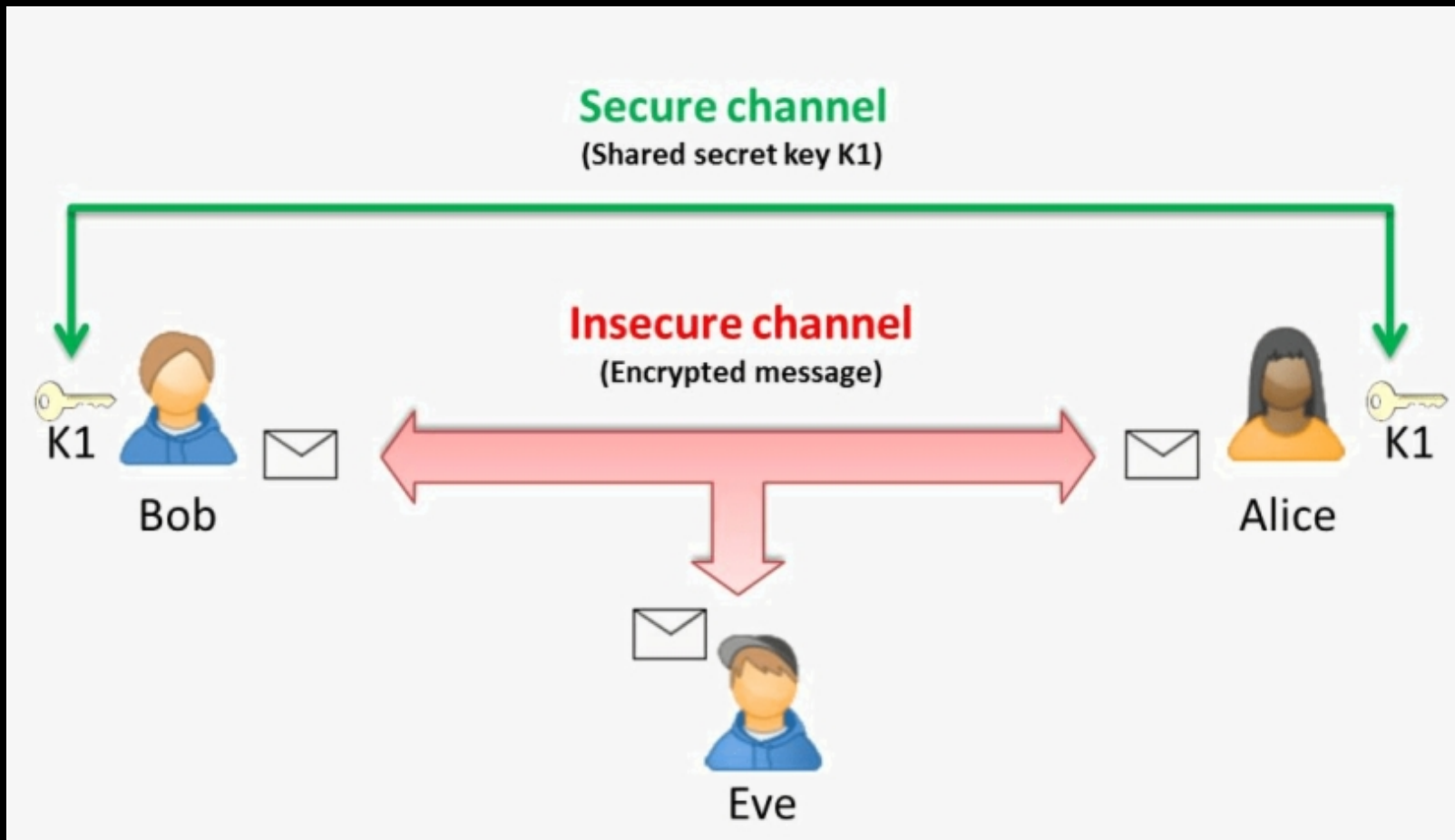
**KEY is the vital part of the secure communication.**



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.

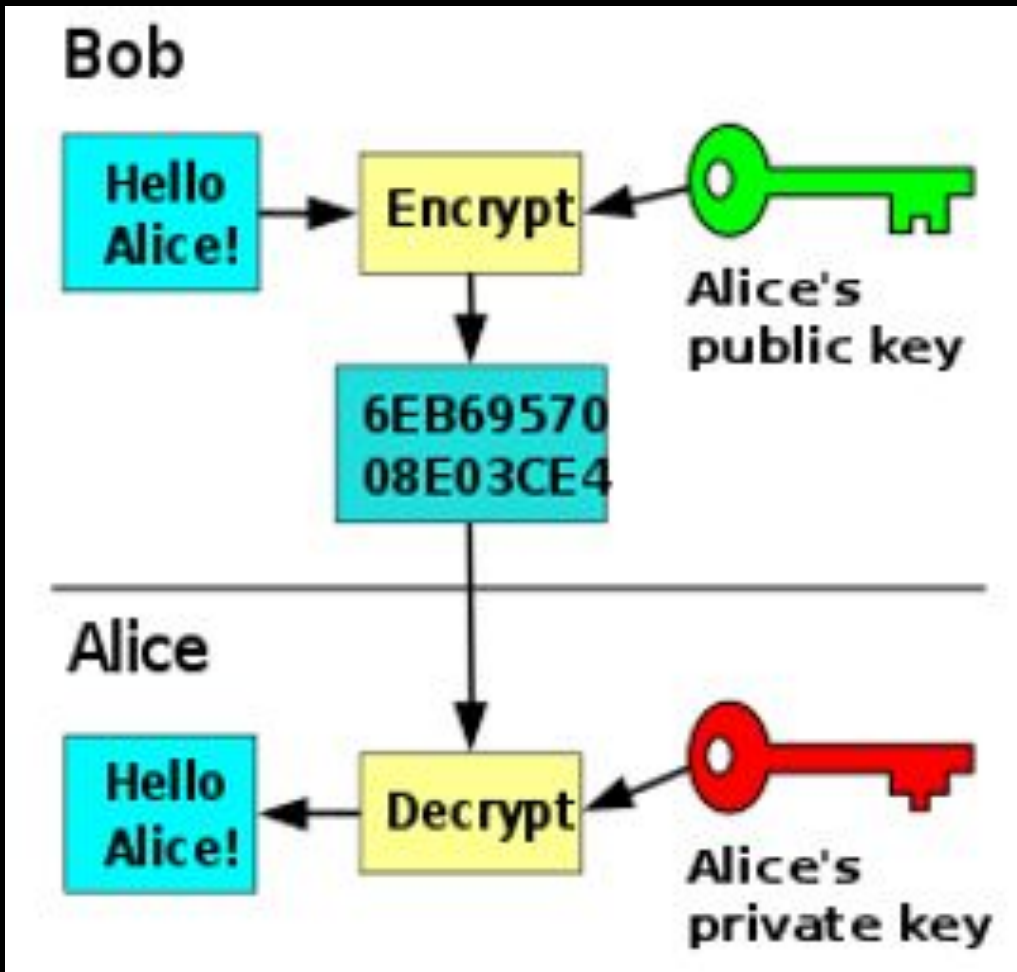
Example:

RSA (multiplication of two prime numbers)

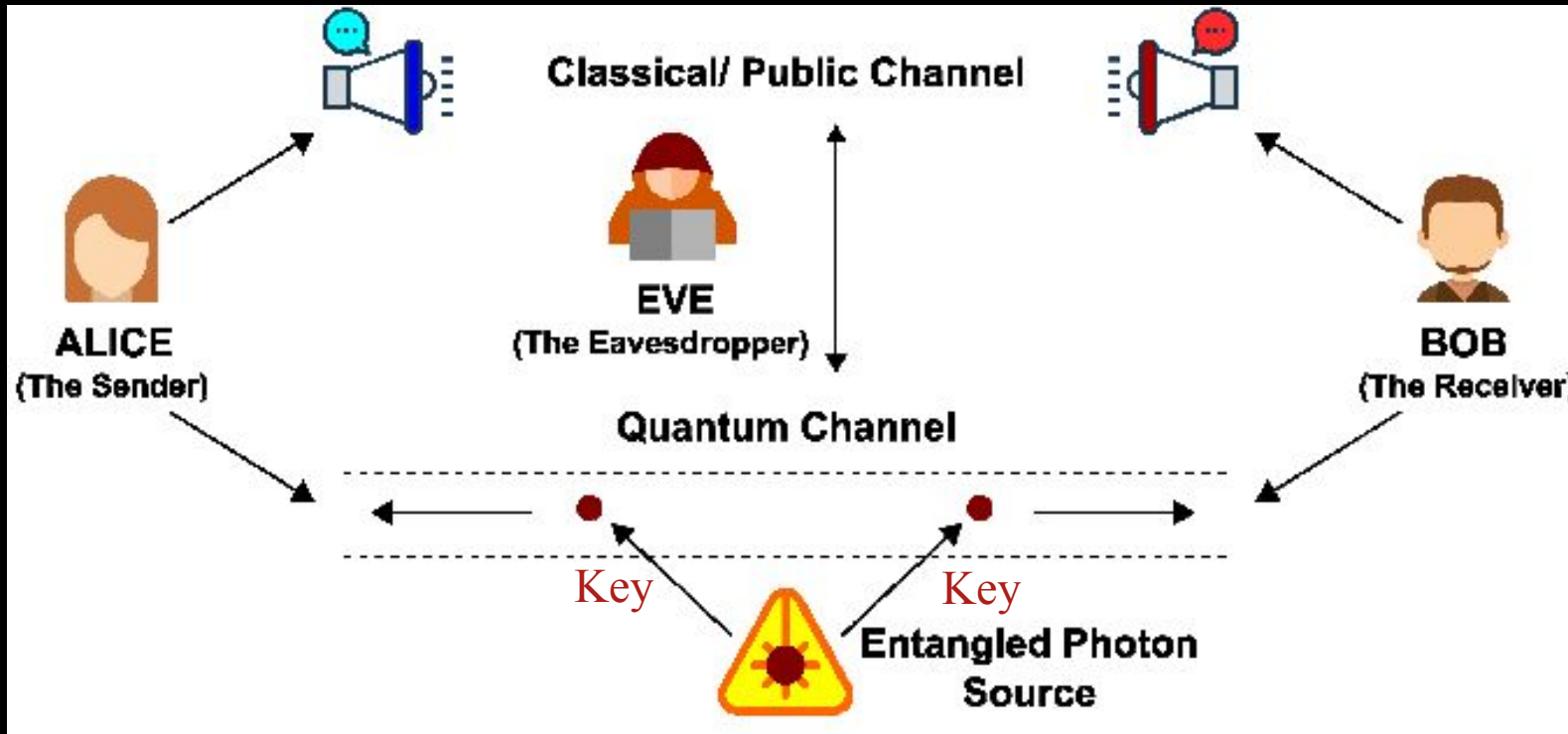
ElGamal (Discrete Logarithm)

$$(a^k = b)$$

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



# QUANTUM KEY DISTRIBUTION (QKD)



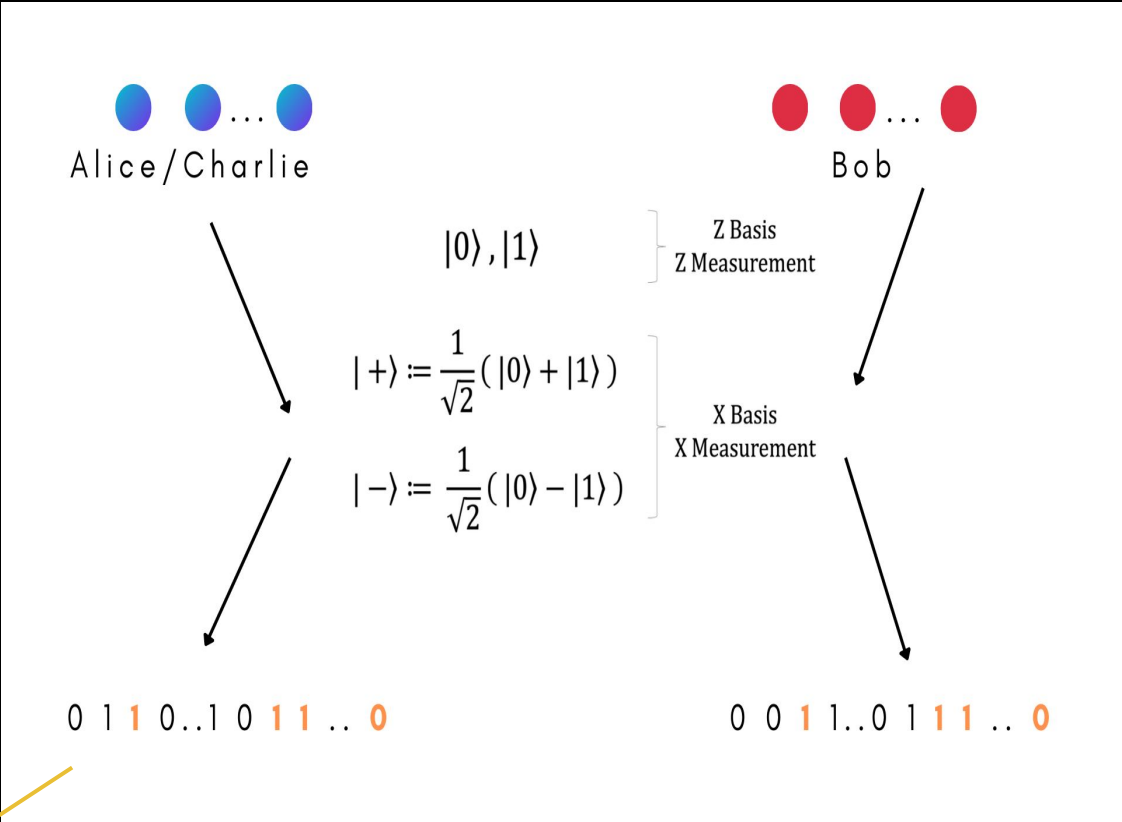
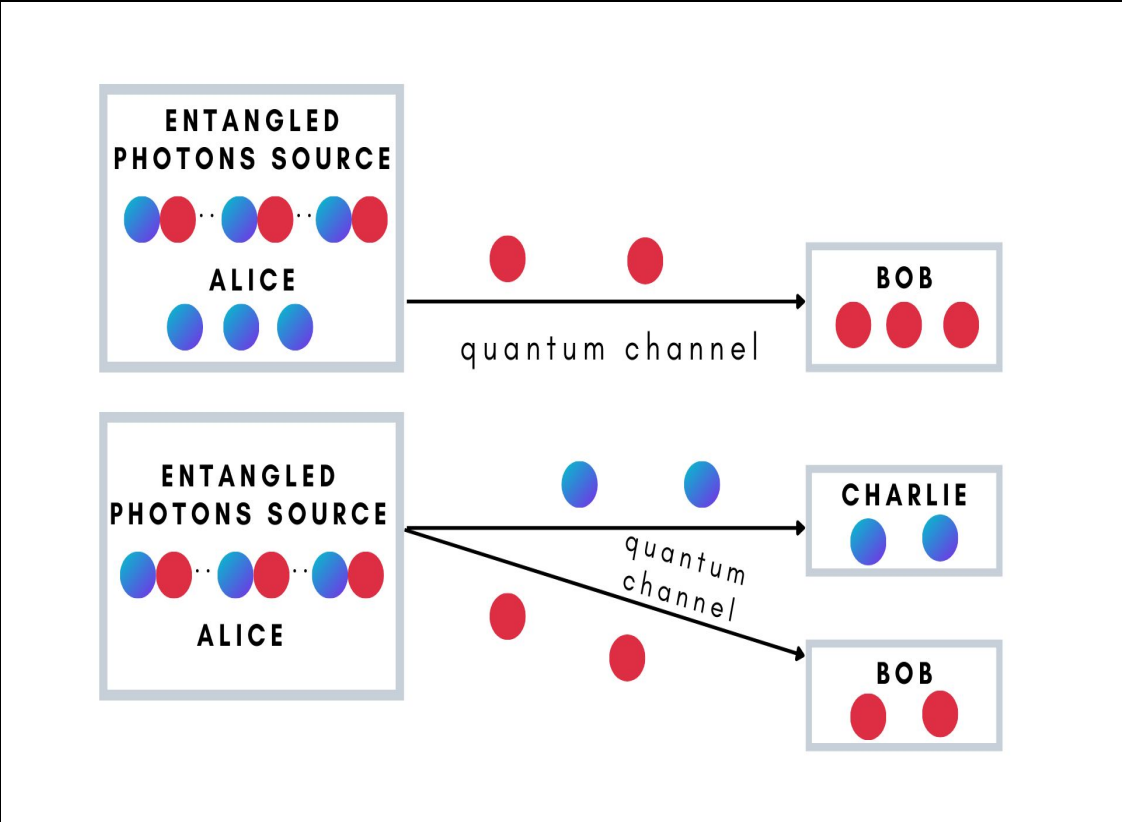
Information is carried by photons

Same key can be sent to both Alice and Bob

Provable security due to the quantum properties of the photons

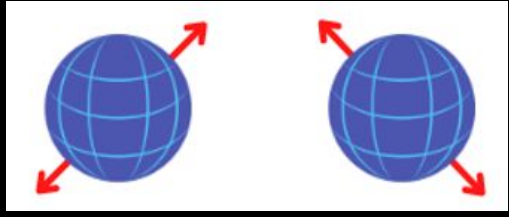
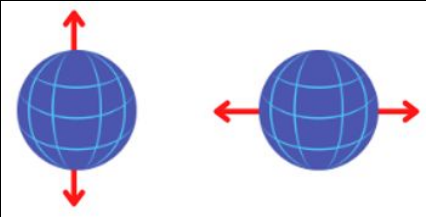


# E91/EPR PAIR PROTOCOL



How about key size?

BB84 protocol



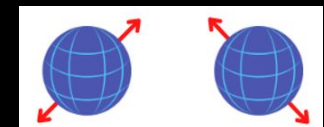
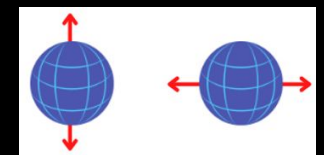
# BB84 PROTOCOL

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	↑	↗	↘	↗	→	↗	→	→
<b>PUBLIC DISCUSSION OF BASIS</b>								
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](https://en.wikipedia.org/wiki/Quantum_key_distribution)

Basis	0	1
+	↑	→
×	↗	↘



# NSA CONCERNS ON QKD

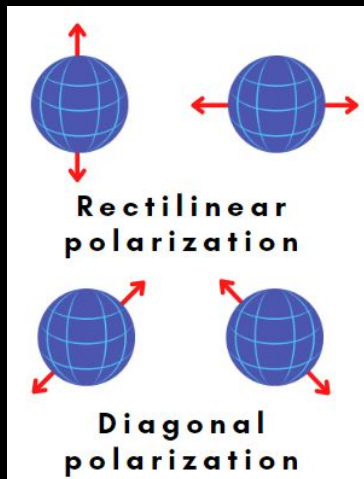
- QKD does not provide a means to **authenticate** the QKD transmission source
- Quantum key distribution is **hardware-based**, can't be implemented in software or a service on a network
- Quantum key distribution increases infrastructure **costs** and **insider threat risks**
- **Securing and validating** 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

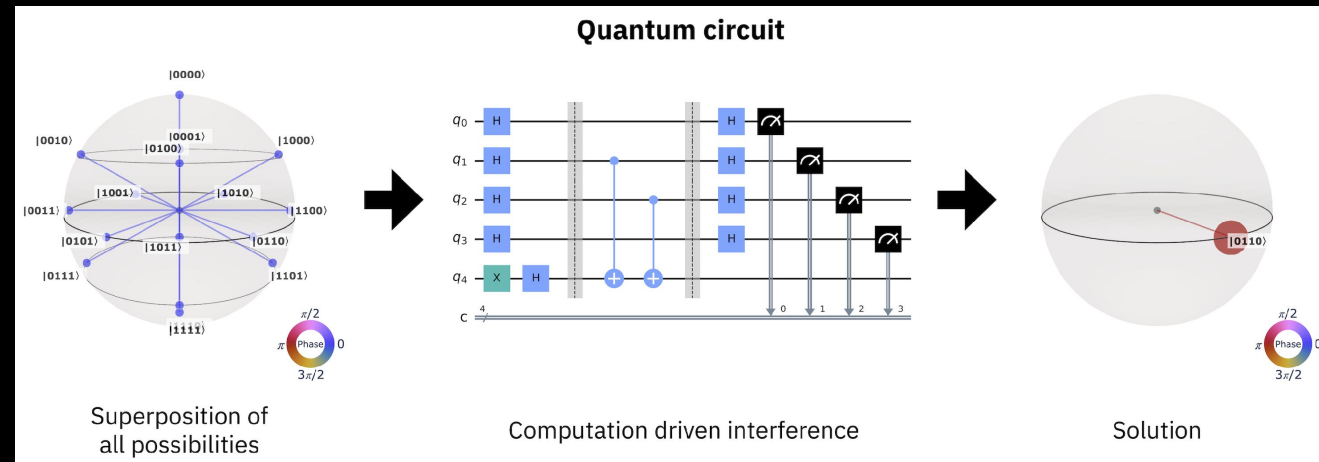
- Polarization of photons
- Measurement of the basis
- Entanglement



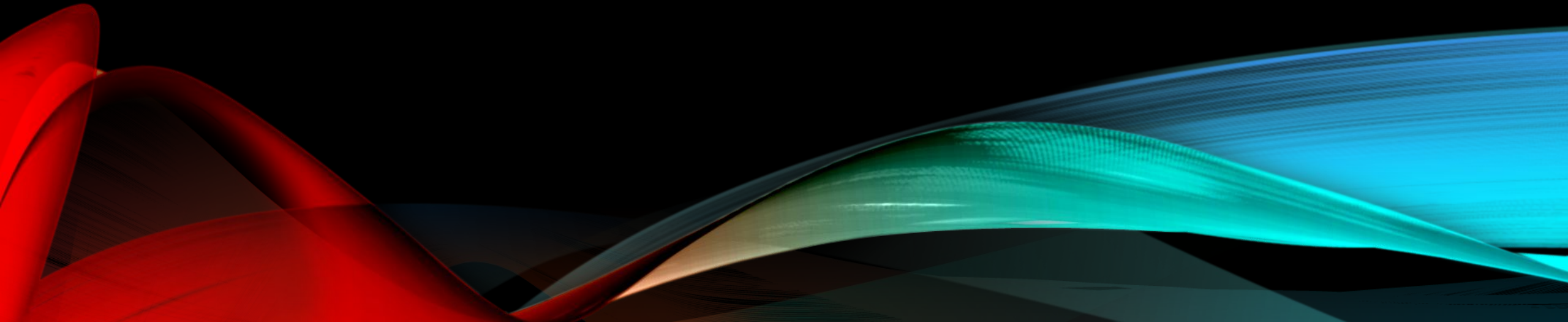
Basis	0	1
+	↑	→
×	↗	↘

## Quantum Computing

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



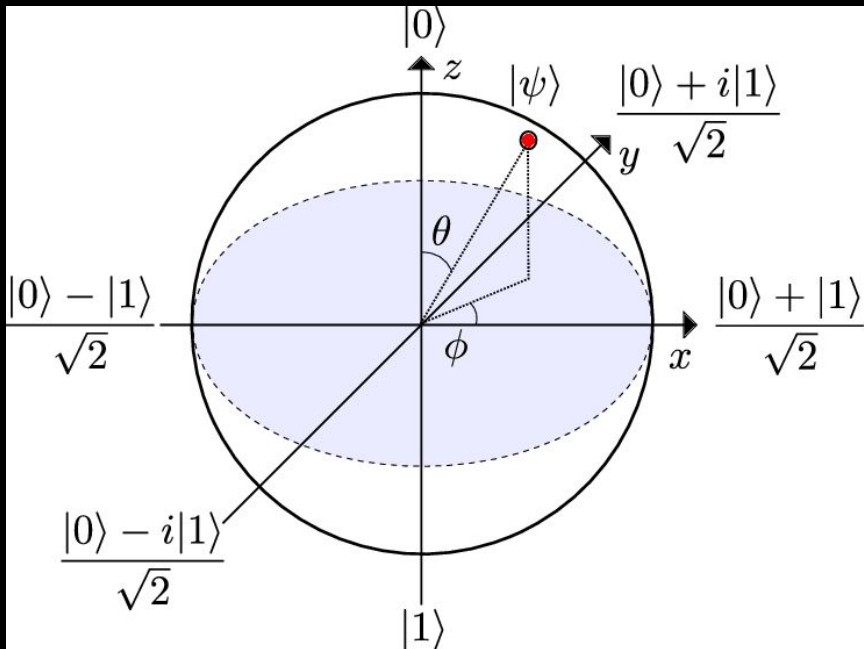
VERY-VERY BRIEF INTRO OF QUANTUM  
MECHANICS (FROM A MATH VIEWPOINT)



## Quantum mechanics

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

~~$y=f(x)$~~



$|\psi\rangle$  -- quantum state

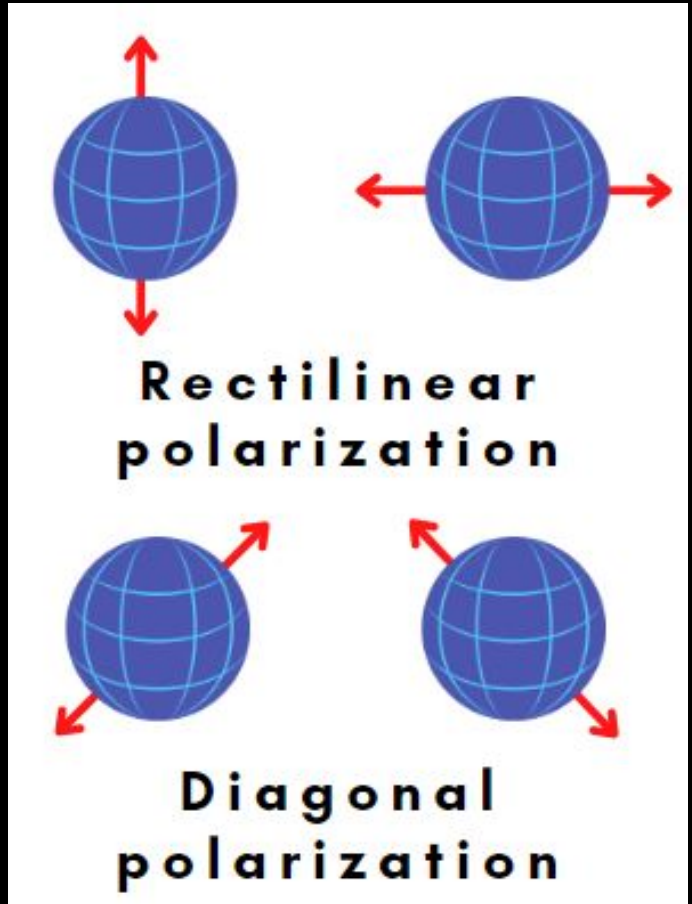
Z-basis (orthogonal)

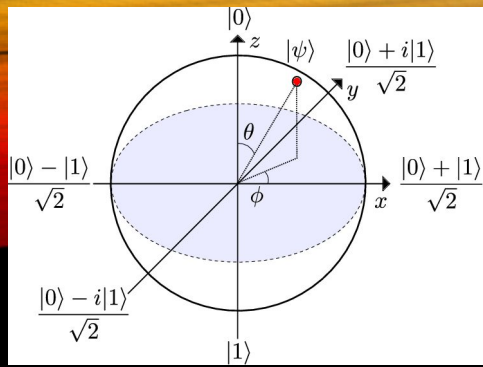
$|0\rangle$  ;  $|1\rangle$

X-basis (orthogonal)

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

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





# QUANTUM STATES AND SUPERPOSITION

A quantum state can be represented by:

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$  where  $|\alpha|^2 + |\beta|^2 = 1$ ,  $\alpha$  and  $\beta$  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:  $|0\rangle$  or  $|1\rangle$
- 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:

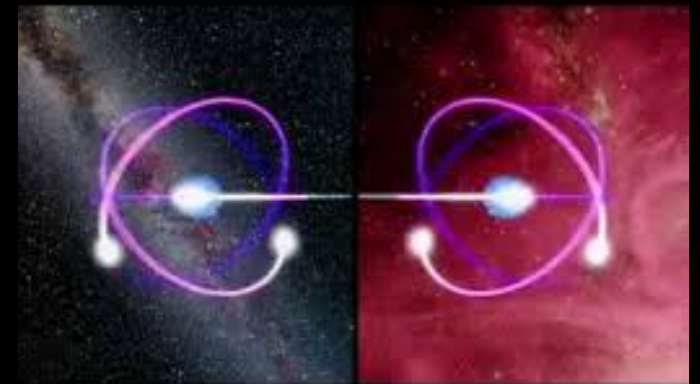
$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$|\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

$$|\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

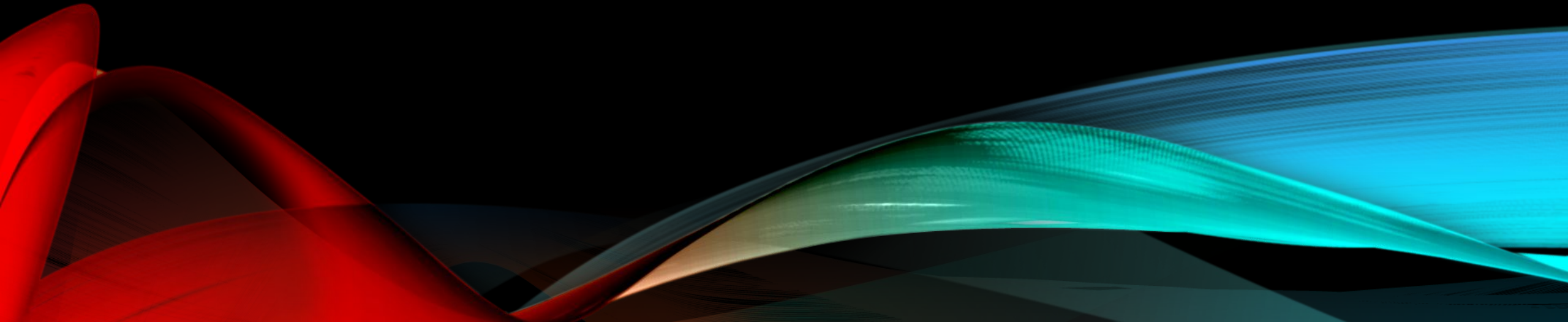
$$|\beta_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

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






QUANTUM COMPUTING--  
BUILDING QUANTUM CIRCUITS



# HADAMARD GATES

MOST IMPORTANT GATES FOR QUANTUM CIRCUIT

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

Dirac notation: ket  $|0\rangle$  and bra  $\langle 0|$

Transformation:

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

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

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

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

classical bits  $\longrightarrow$  qubit with superposition

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

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

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

$$|\psi\rangle \longrightarrow |\varphi\rangle$$

Pauli X

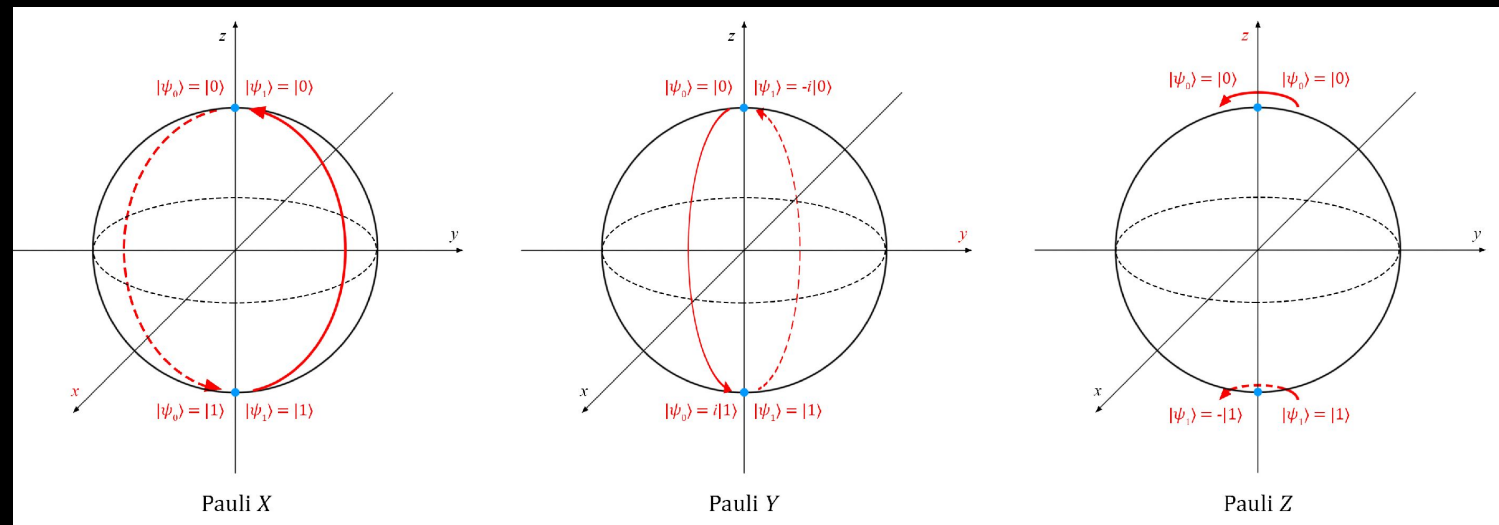
$$\begin{aligned} |0\rangle &\longrightarrow |1\rangle \\ |1\rangle &\longrightarrow |0\rangle \end{aligned}$$

Pauli Y

$$\begin{aligned} |0\rangle &\longrightarrow i|1\rangle \\ |1\rangle &\longrightarrow -i|0\rangle \end{aligned}$$

Pauli Z:

$$\begin{aligned} |0\rangle &\longrightarrow |0\rangle \\ |1\rangle &\longrightarrow -|1\rangle \end{aligned}$$



# QUANTUM GATES FOR MULTIPLE QUBITS

## CNOT gate

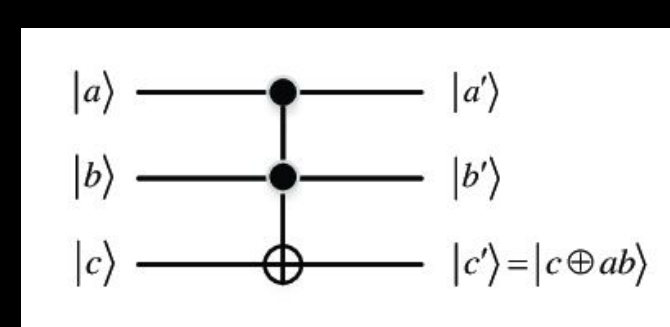
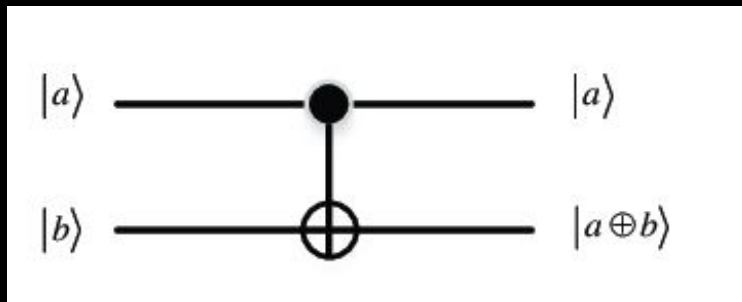
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

input		output	
x	y	x	y+x
0⟩	0⟩	0⟩	0⟩
0⟩	1⟩	0⟩	1⟩
1⟩	0⟩	1⟩	1⟩
1⟩	1⟩	1⟩	0⟩

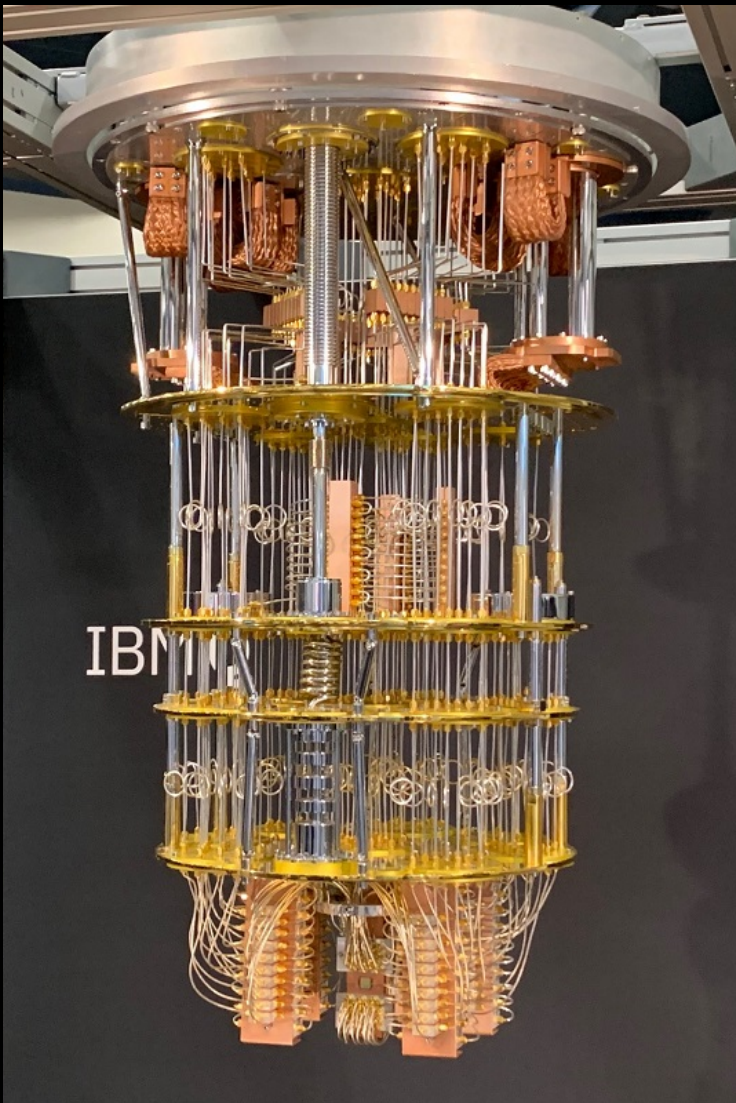
## Toffoli gate

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

Inputs			Outputs		
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
<b>Best for</b> Learning quantum computing and exploring IBM quantum technology.	<b>Best for</b> Performing utility-scale quantum research projects and testing business use cases with flexible access.	<b>Best for</b> Executing a strategic quantum roadmap and developing utility-scale quantum algorithms and applications.	<b>Best for</b> Exploring quantum algorithms and applications with high control over your resources and data.
<ul style="list-style-type: none"><li>✓ Access to Qiskit® Runtime as a Service</li><li>✓ Access to 100+ qubit utility-scale systems</li></ul>	<ul style="list-style-type: none"><li>✓ Access to Qiskit Runtime as a Service</li><li>✓ Access to 100+ qubit utility-scale systems</li><li>✓ Access to IBM Quantum™ technical support</li></ul>	<ul style="list-style-type: none"><li>✓ Access to Qiskit Runtime as a Service</li><li>✓ Access to 100+ qubit utility-scale systems</li><li>✓ Access to IBM Quantum technical support</li><li>✓ <a href="#">IBM Quantum Network</a> membership</li><li>✓ Optional access to our <a href="#">Quantum Accelerator</a> offering</li><li>✓ Access to exploratory systems</li></ul>	<ul style="list-style-type: none"><li>✓ Access to Qiskit Runtime as a Service</li><li>✓ Access to 100+ qubit utility-scale systems</li><li>✓ Access to IBM Quantum technical support</li><li>✓ <a href="#">IBM Quantum Network</a> membership</li><li>✓ Optional access to our <a href="#">Quantum Accelerator</a> offering</li><li>✓ Full system capacity purchased as a service</li><li>✓ Optional system location on client site</li></ul>
<b>Free</b> Up to 10 minutes of runtime on utility-scale systems per month.	<b>\$1.60 USD / second</b> Pay for what you need. Billed per second.	<b>Price varies</b> Access to additional systems & IBM quantum resources.	<b>Price varies</b> 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

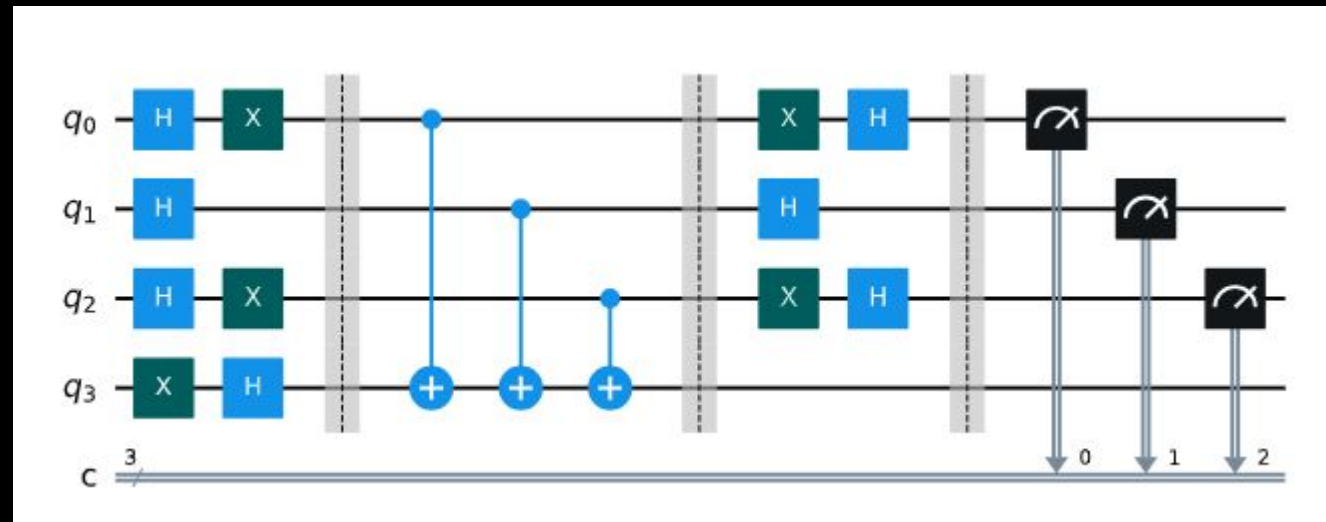
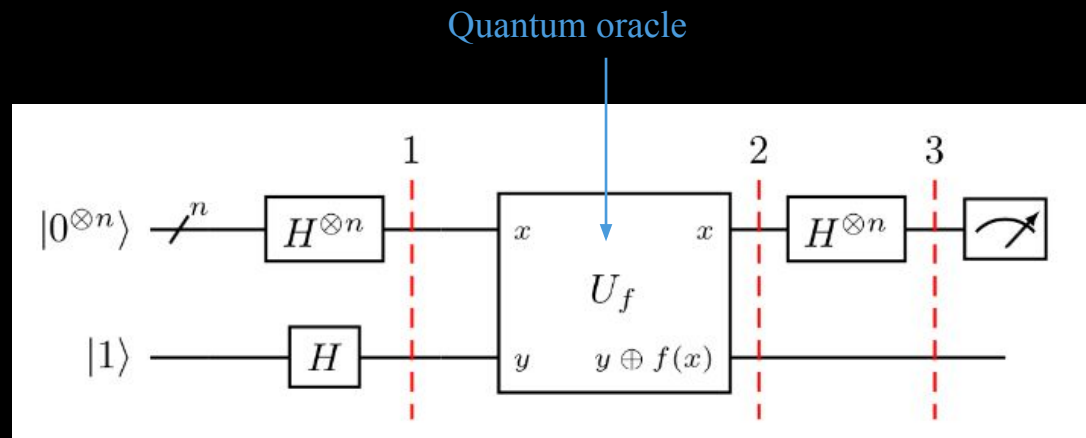
\$1.60 USD / Second  
Pay for what you need . Billed Per Second



# QUANTUM ALGORITHMS-- PERFORMING BETTER THAN CLASSICAL ALGORITHMS

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

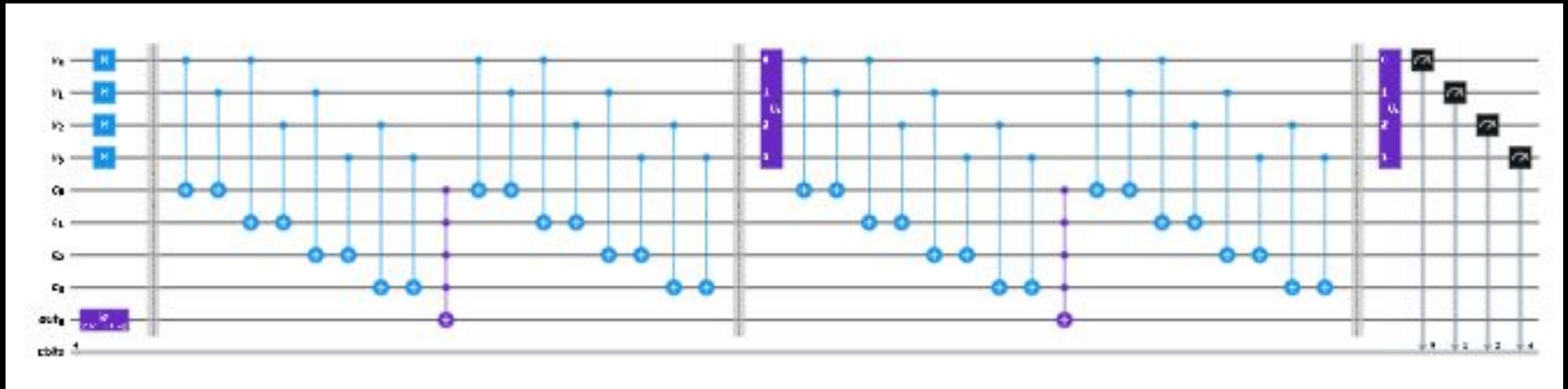
- Generic circuit for the Deutsch-Jozsa algorithm
- <https://learn.qiskit.org/course/ch-algorithms/deutsch-jozsa-algorithm>



# QUANTUM ALGORITHMS-- BREAKING CRYPTO BY SEARCHING THE KEY

IBMQ Qiskit implementation:

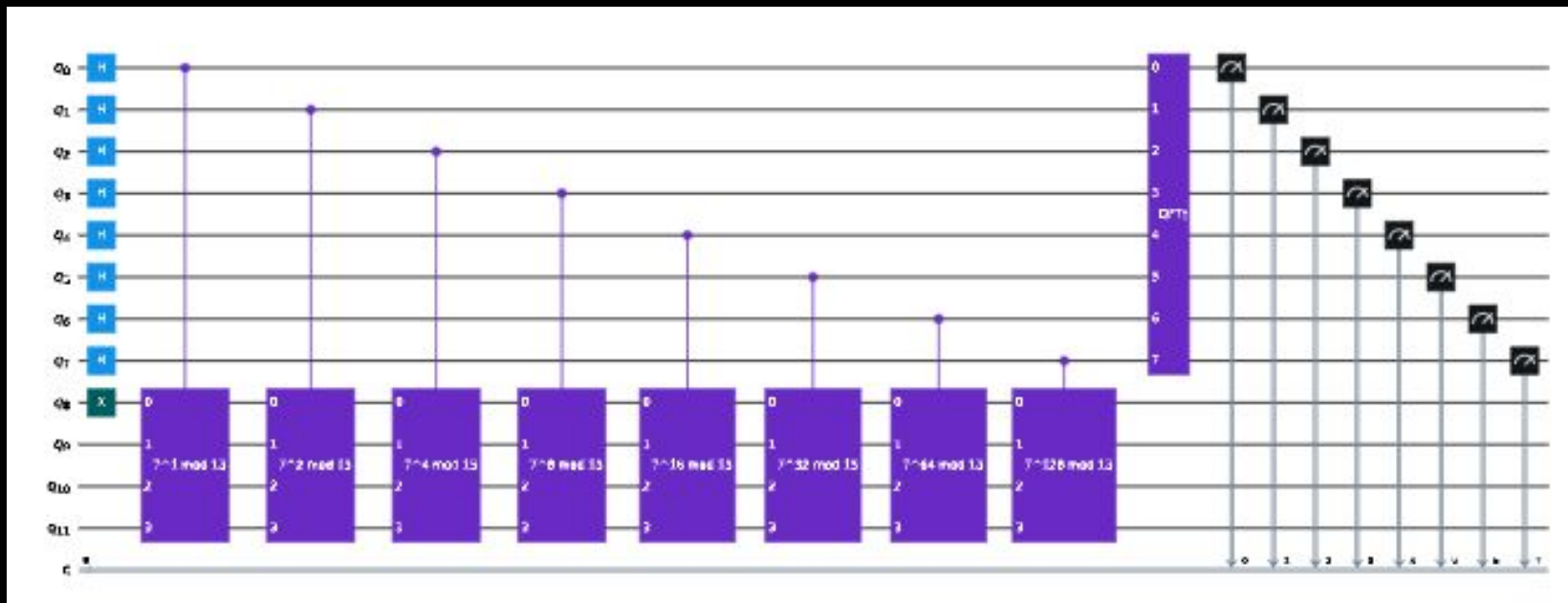
- Grover's Algorithm □ unstructured Search problems
- <https://learn.qiskit.org/course/ch-algorithms/grovers-algorithm>



# QUANTUM ALGORITHMS-- BREAKING PUBLIC KEY CRYPTO

IBMQ Qiskit implementation:

- Shor's Algorithm  $\square$  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)

# 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:

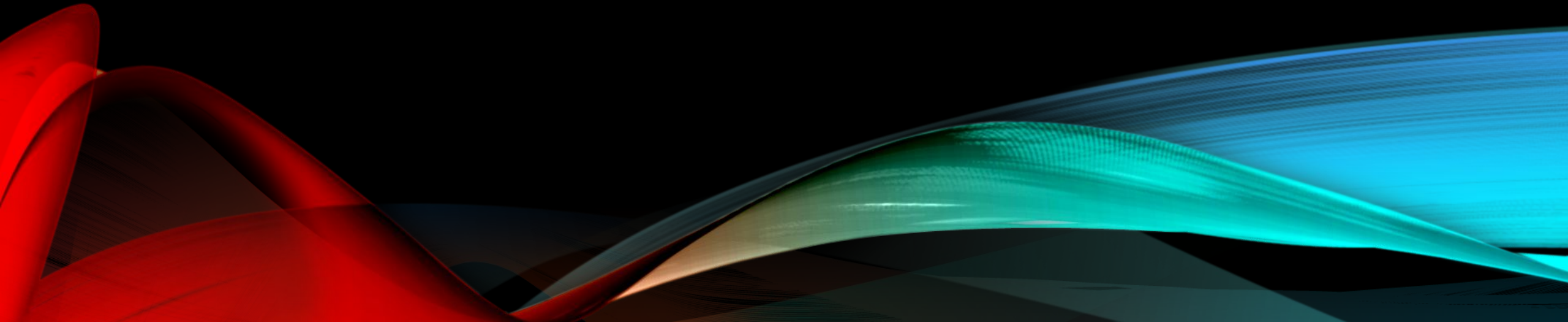
- Public-key encryption and key-establishment algorithms
  - CRYSTALS-KYBER
  - BIKE
  - Classic McEliece
  - HQC
- Digital Signature Algorithms
  - CRYSTALS-DILITHIUM
  - FALCON
  - SPHINCS+

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](#)

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 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.



[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.



[Learn more about QuEra Rydberg atom-based processors »](#)

## 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.



[Learn more about Rigetti gate-based superconducting processors](#)

»



[Learn more about OQC gate-based superconducting processors »](#)

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



# AWS BRAKET PRICE

## Quantum Computers (on-demand)

<u>Hardware Provider</u>	<u>QPU family</u>	<u>Per-task price</u>	<u>Per-shot price</u>
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

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

# EPB QUANTUM NETWORK— CHATTANOOGA, TN

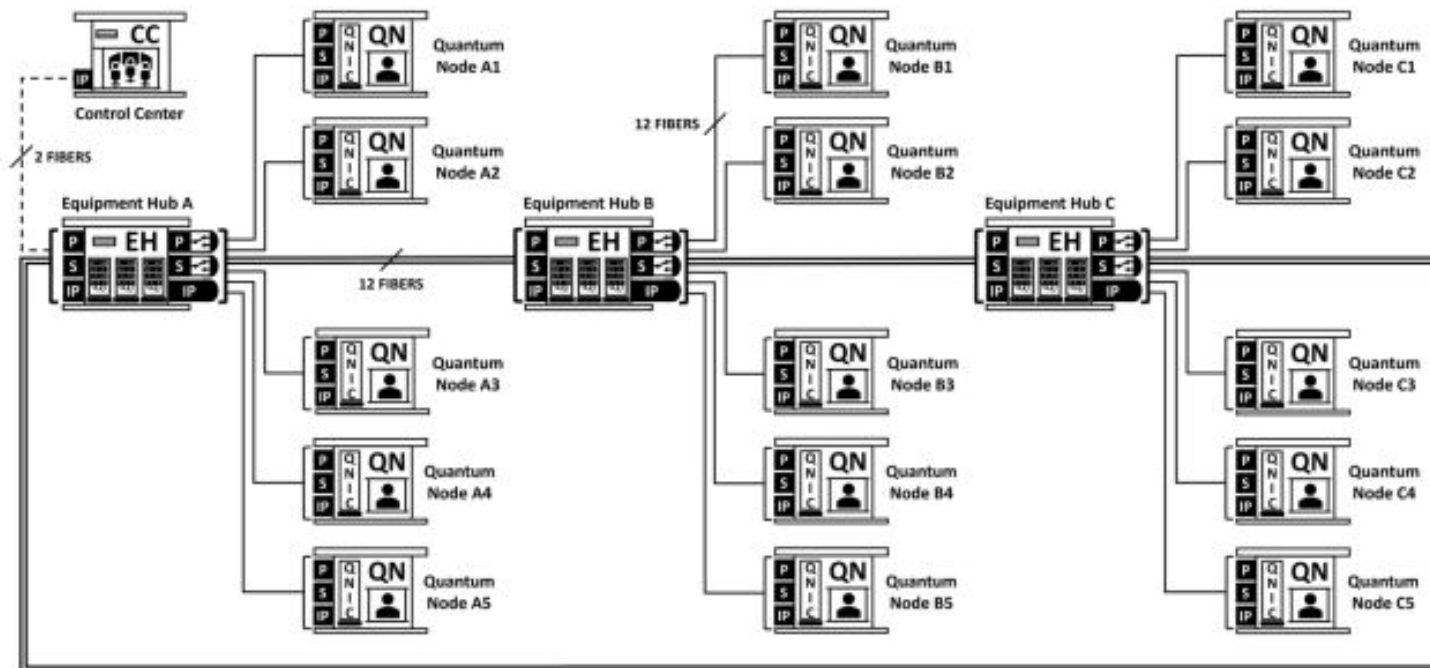
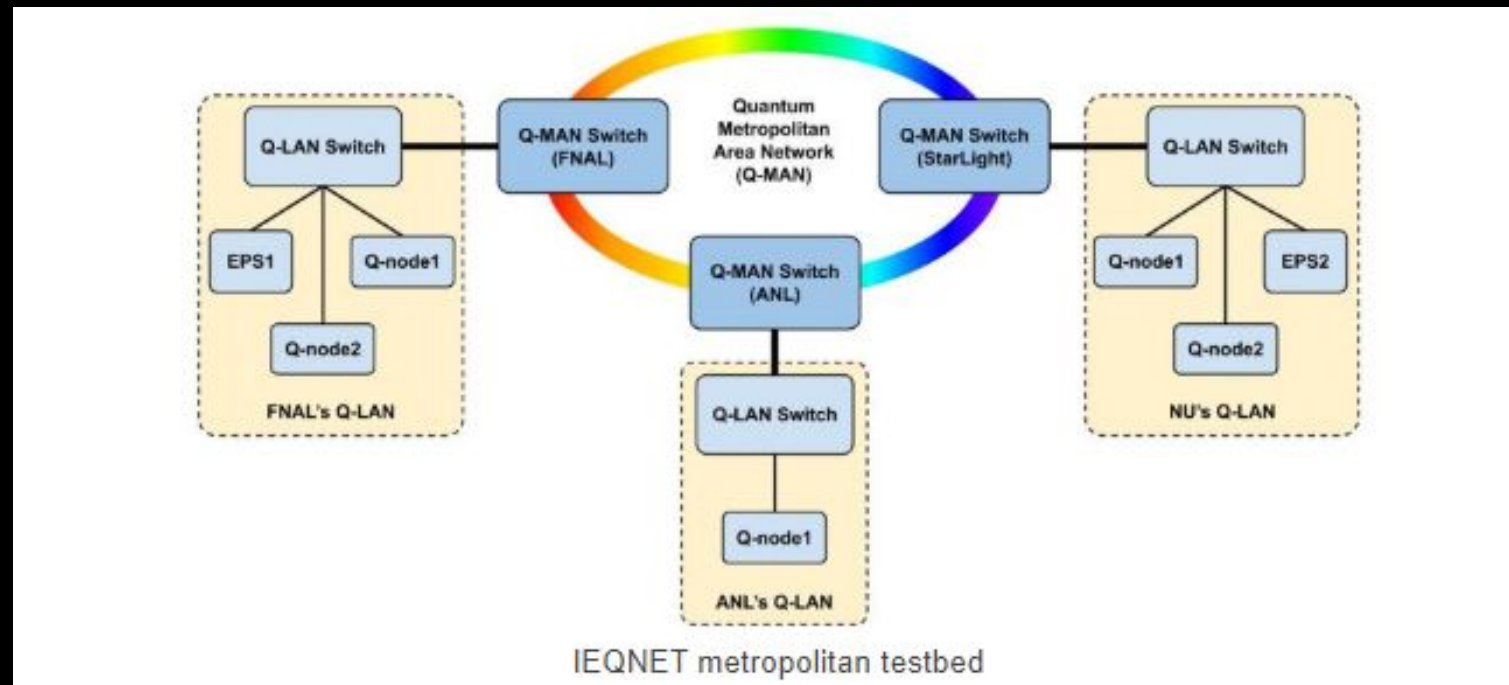


Fig. 6. **Bohr-IV Quantum Network Architecture:** Equipment Hubs are connected in a ring topology with five client Quantum Nodes connected to every Equipment Hub in a hub-and-spoke topology. This hybrid ring/spoke architecture is scaled by adding additional Equipment Hubs, which in turn adds additional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

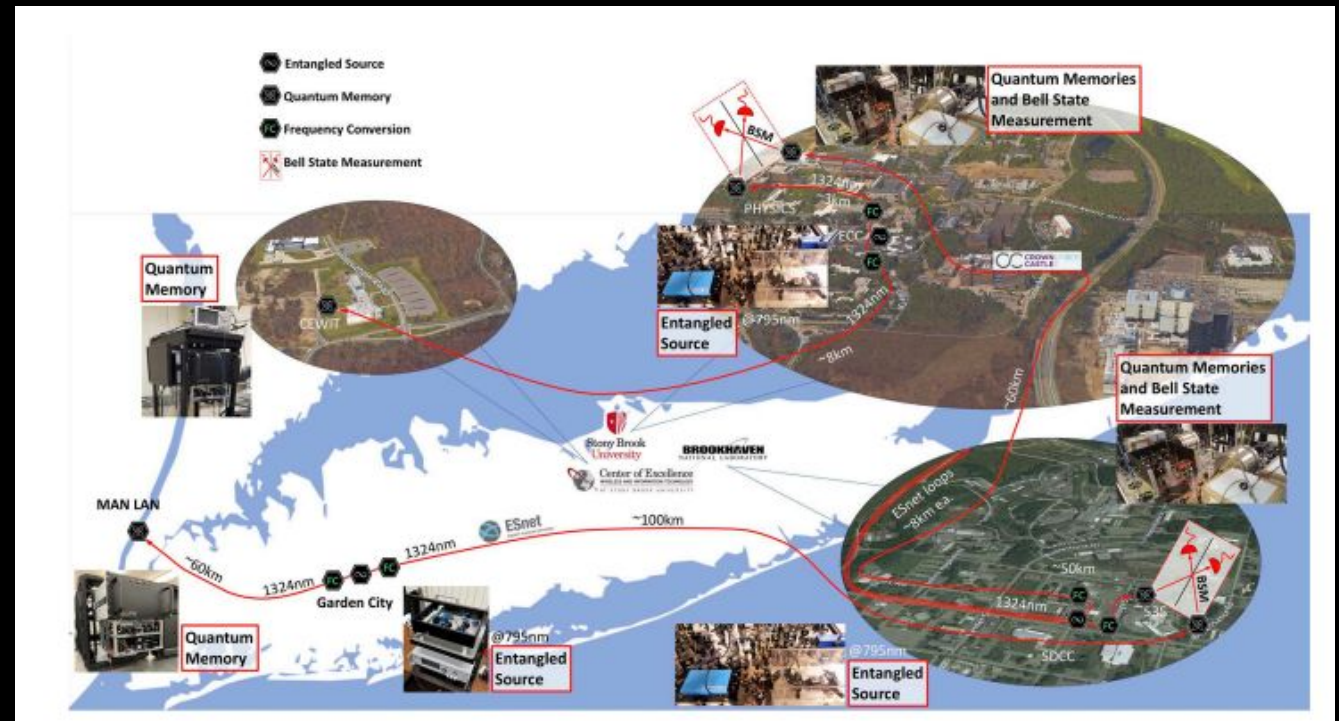
# IEQNET (ILLINOIS-EXPRESS QUANTUM NETWORK) METROPOLITAN TESTBED

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



# QUANTUM MEMORY NETWORK— LONG ISLAND, NY

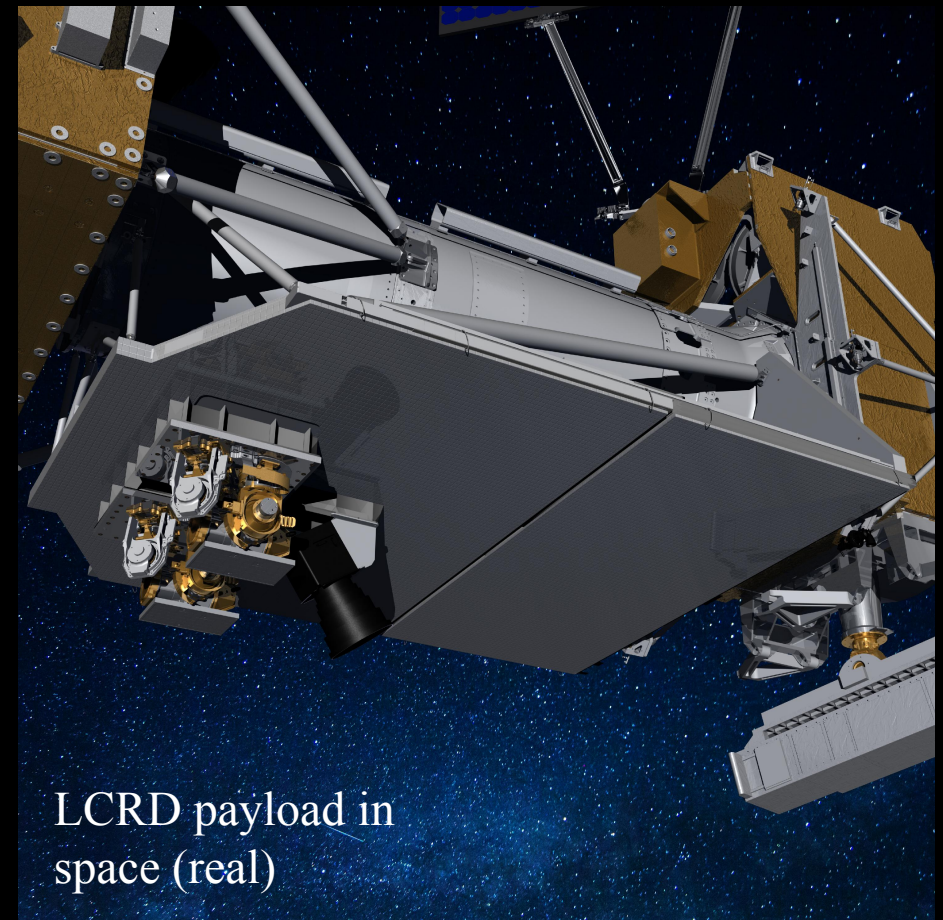
- Brookhaven National Lab (BNL)+
- Stony Brook U (SBU)+
- DOE Energy Sciences Network (ESnet)
- Goal is to build a Q-LAN / Entanglement swapping



Vision for quantum internet  
NOT REAL!

# NASA--LCRD MISSION CENTER @ LAS CRUCES, NM

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



LCRD payload in  
space (real)

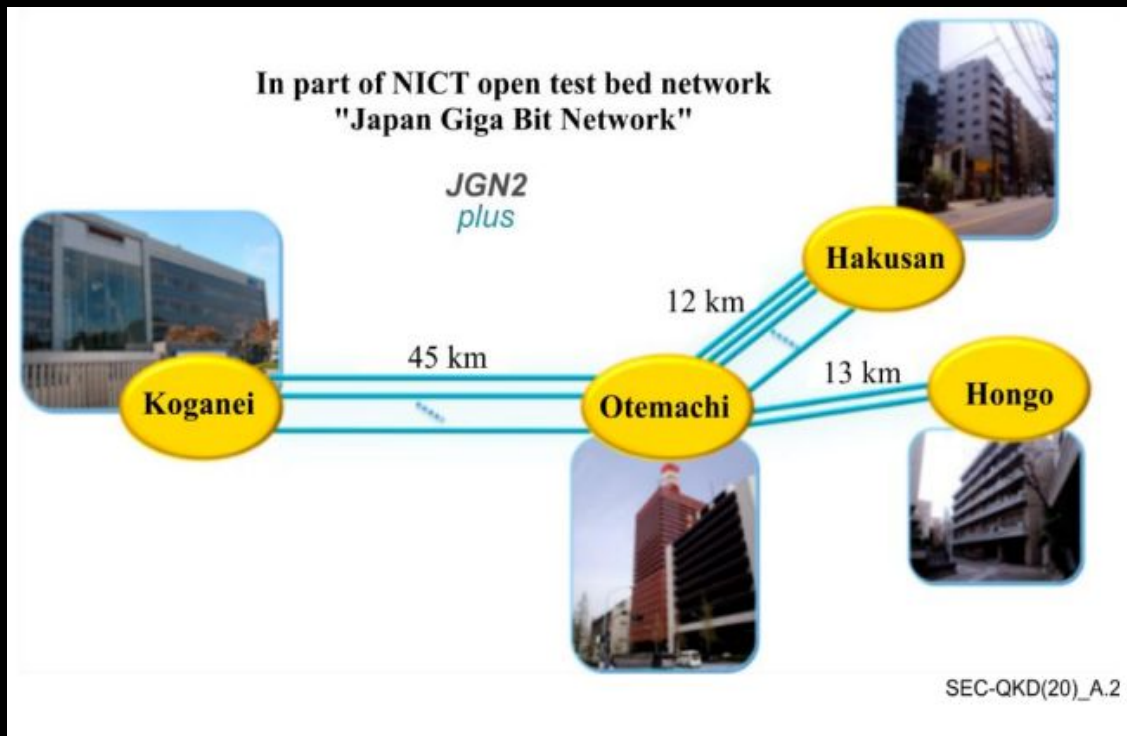
# MICIUS—QUANTUM SATELLITE (CHINA)



- 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

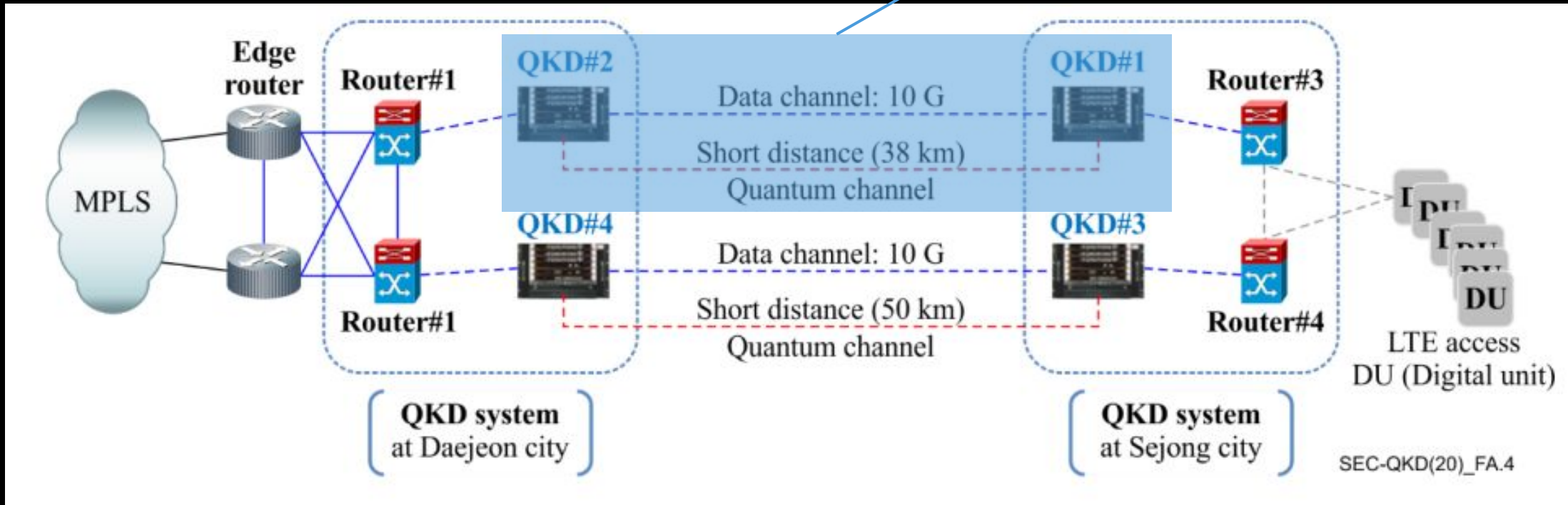


- Distance □ biggest obstacle
- Free space propagation
- Error rates and correcting
- No standards for quantum communication
- No nationwide quantum network yet
- Quantum layer Integrated with classical systems □ HOW ??
- Has its own set of vulnerabilities (NSA concerns)
- Need a framework to deploy securely

# SOUTH KOREA QKD DEPLOYMENT

Data channel is the classical channel

Commercially available



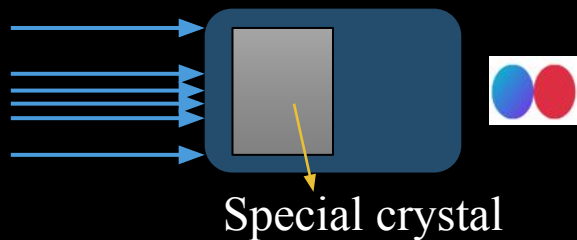


# QUBITEKK

[HTTPS://QUBITEKK.COM/PRODUCTS/](https://qubitekk.com/products/)



Polarization Entangled Photon Source



More than 10,000 pairs of entangled photons

QKD devices

Timing is extremely important

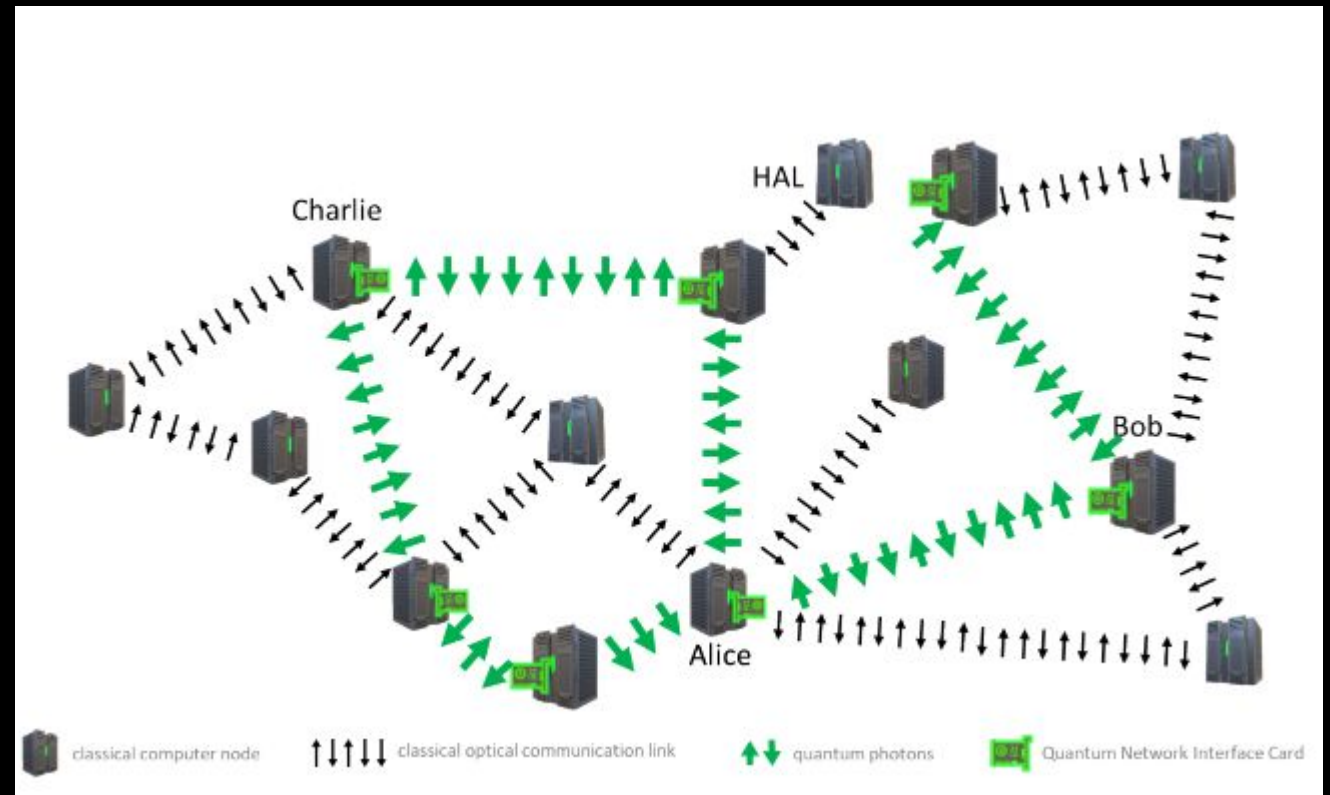
0 1 1 0 .. 1 0 1 1 .. 0

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

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

# THE FUTURE? — DARPA PROGRAM QUANET

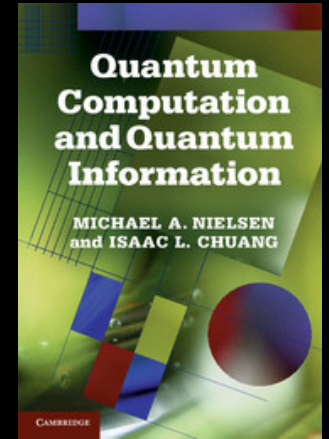
- Could this be the future?
- Quantum-Augmented Network (QuANET)
- A Network Security Revolution Enhanced By Quantum Communication



Topology with quantum and  
classical links

# 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>

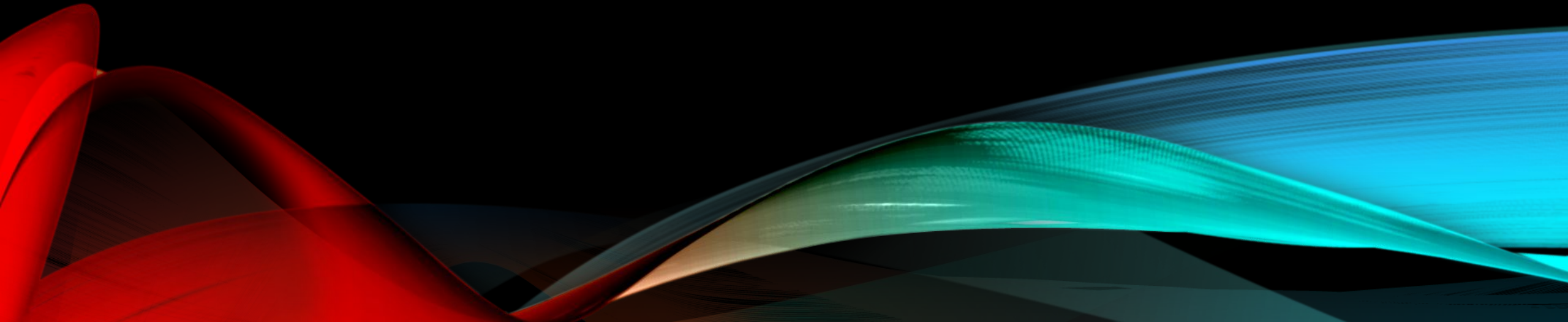
From Long-distance Entanglement to building a nationwide quantum internet, US Dept of Energy, July 2020

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



Thank you !!

BACK UP SLIDES PART 1-  
IBMQ LAB



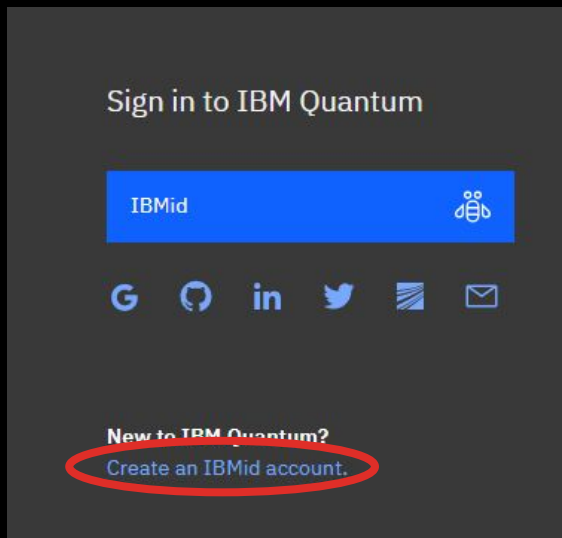


# IBM QUANTUM INTRO TO QISKIT

Open source platform-Qiskit:

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

Create an IBMid account:



Already have an IBM account? [Log in](#)

## Sign up for an IBMid

---

1. Account information AutoFill with LinkedIn

E-mail ⓘ

Your email address will become your IBMid, which you'll use to log into IBM.com.

First name

Last name

Password

Country or region of residence

United States of America ▼

---

2. Verify email

# DASHBOARD

IBM Quantum

Recent notifications ↓

Welcome, Jennifer Cheung

Graphically build circuits with IBM Quantum Composer

Develop quantum experiments in IBM Quantum Lab

Jump back in:

- Untitled circuit
- bit flip-01
- JC-lab-1.ipynb
- Untitled.ipynb

API token

View account details

Launch Composer

Launch Lab

Optimize circuit execution with Qiskit Runtime programs

2 Primitive programs

12 Runtime programs

View all

Recent jobs

0 Pending

6 Completed

No pending jobs

View all

Run on circuits & programs via IBM Quantum compute resources

6 Your systems

5 Your simulators

0 Reservable systems

View all

Recent notifications

- Service Alert
- ibmq\_armonk has been retired 10 days ago

IBM Quantum

Composer

Lab

Programs

Compute Resources

Dashboard

Quantum Challenge

Documentation

Jobs

Notifications

Researchers program

Educators program



# COMPUTE RESOURCES FREE RESOURCES

All Systems

The screenshot displays the IBM Quantum Compute Resources dashboard. At the top, there are tabs for 'Your resources', 'All Systems', and 'All Simulators'. Below this, a search bar and a dropdown menu for 'Your systems & simulators (11)' are visible. The main content area is divided into two sections: 'Quantum systems' (highlighted with a yellow box) and 'Simulators' (highlighted with a blue box). Each system or simulator card shows its name, status, processor type, and qubit count. Arrows from the text labels on the right point to specific elements in the dashboard.

System Name	Status	Processor Type	Qubits	QV	CLOPS
ibmq_nairobi	Online	Falcon r5.11H	7	32	2.6K
ibmq_oslo	Online	Falcon r5.11H	7	32	2.6K
ibmq_manila	Online	Falcon r5.11L	5	32	2.8K
ibmq_quito	Online	Falcon r4T	5	16	2.5K
ibmq_belem	Online - Queue paused maintenance	Falcon r4T	5	16	2.5K
ibmq_lima	Online - Queue paused maintenance	Falcon r4T	5	8	2.7K
simulator_stabilizer	Online	Clifford simulator	5000		
simulator_mps	Online	Matrix Product State	100		
simulator_extended_stabilizer	Online	Extended Clifford (e.g. Clifford+T)	63		
ibmq_qasm_simulator	Online	General, context-aware	32		
simulator_statevector	Online	Schrödinger wavefunction	32		

Documentations

Qubits

Quantum systems

Qubits

Simulators

# 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

Name	Qubits	QV	CLOPS	Status	Total pending jobs	Processor type	Plan
ibm_peekskill <span>Exploratory</span>	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

The screenshot displays the IBM Quantum Composer interface. At the top, the title bar reads "IBM Quantum Composer". Below it, a menu bar includes "Untitled circuit", "File", "Edit", and "View". On the right side of the top bar, there are options for "Visualizations seed" (set to 2000) and a "Setup and run" button.

The main workspace is divided into several sections:

- Operations:** A grid of quantum gates is visible. A yellow circle highlights a group of gates including H, S, Z, T, S†, P, RZ, |0⟩, and if. A red box highlights a list of qubits: q[0], q[1], q[2], q[3], and c4.
- Python 3.0 code:** A code editor on the right shows the following code:

```
from qiskit import
QuantumRegister,
ClassicalRegister,
QuantumCircuit
from numpy import pi

qreg_q = QuantumRegister(4,
'q')
creg_c = ClassicalRegister
(4, 'c')
circuit = QuantumCircuit
(qreg_q, creg_c)
```

A blue circle highlights this code block.
- Statevector:** A bar chart showing the amplitude of computational basis states. The state |0000⟩ has an amplitude of 1.0, while all other states have an amplitude of 0.0.
- Q-sphere:** A Bloch sphere visualization showing the state |0000⟩ at the top pole.

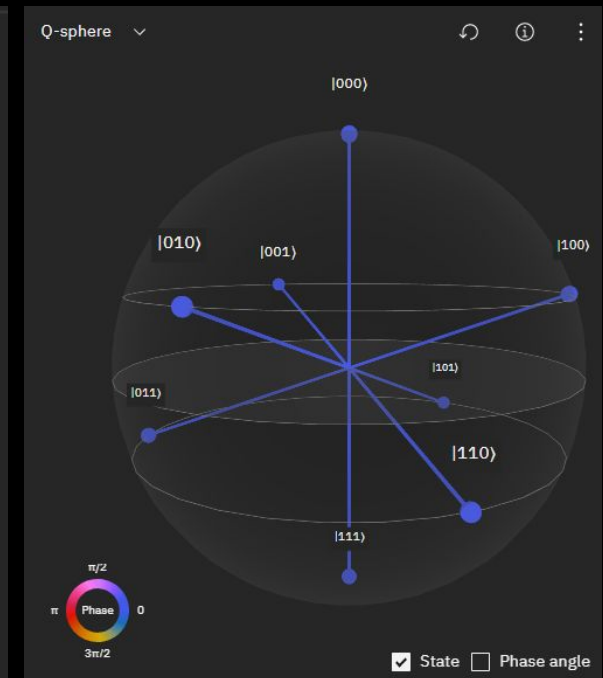
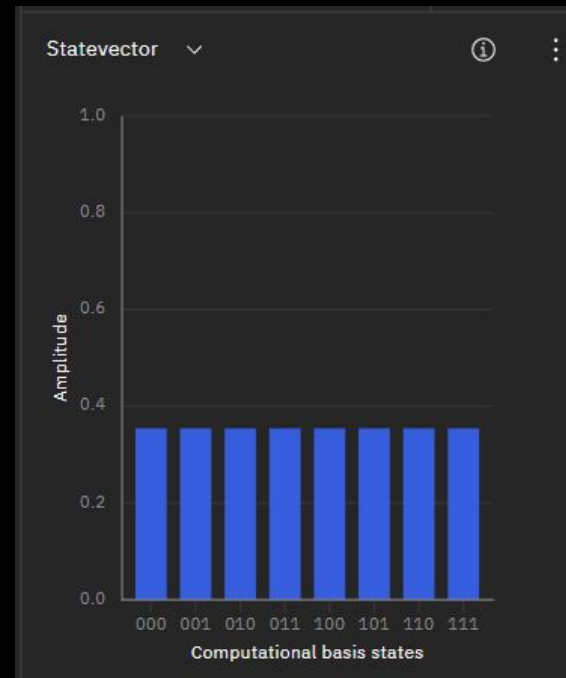
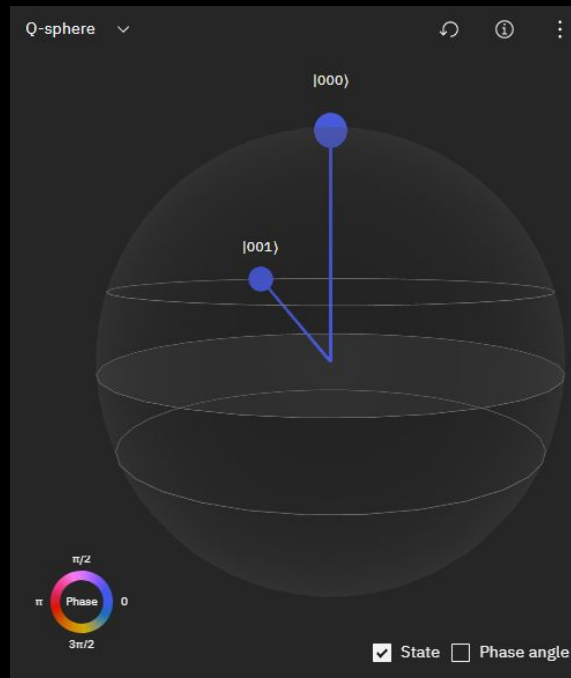
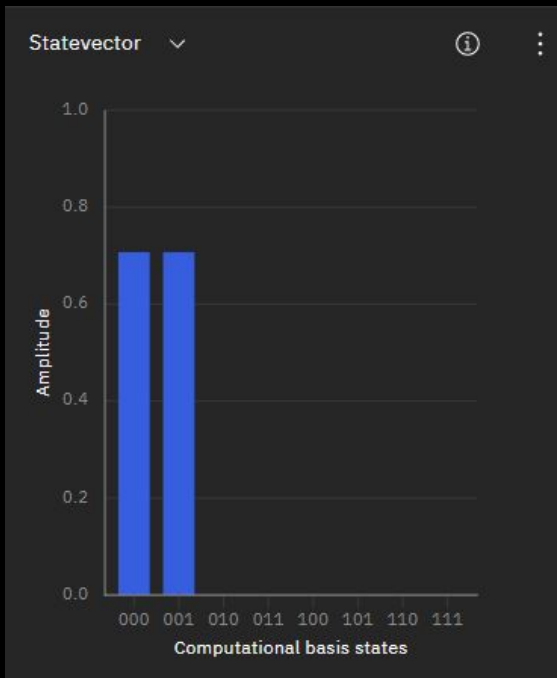
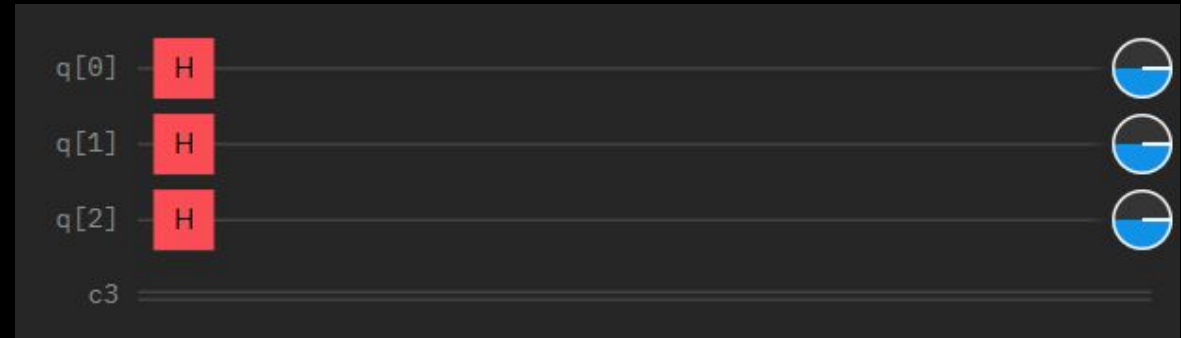
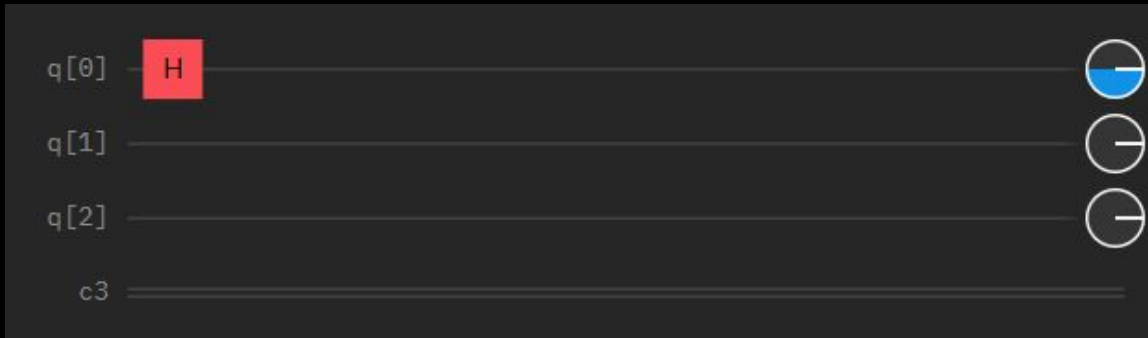
Python 3.0 code

Number of qubits

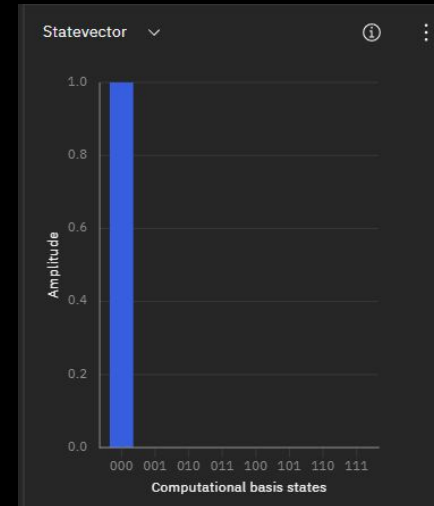
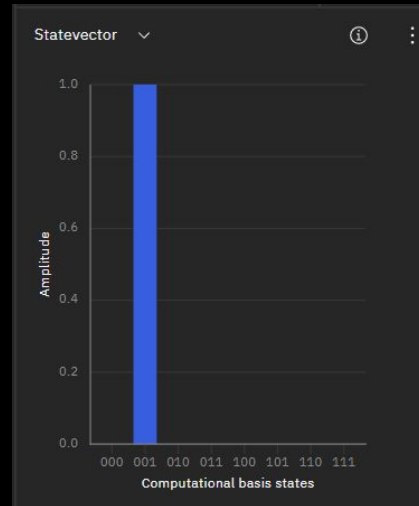
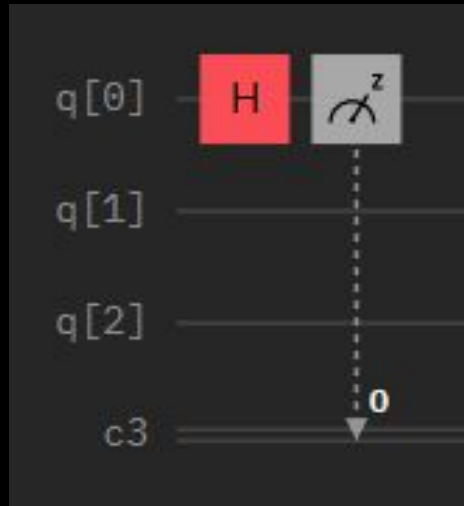
Probabilities

Bloch sphere

# EXAMPLE--3 QUBITS



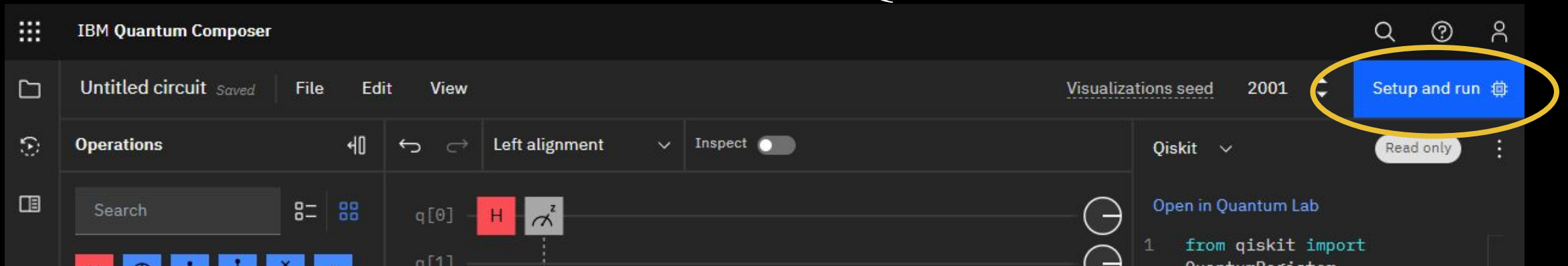
# MEASUREMENT



IBM Quantum Composer interface showing the 'Visualizations seed' dropdown menu set to 2001. The interface includes a menu bar (File, Edit, View), a toolbar with 'Operations' and 'Inspect' options, and a 'Setup and run' button. The 'Visualizations seed' dropdown is highlighted with a yellow circle.

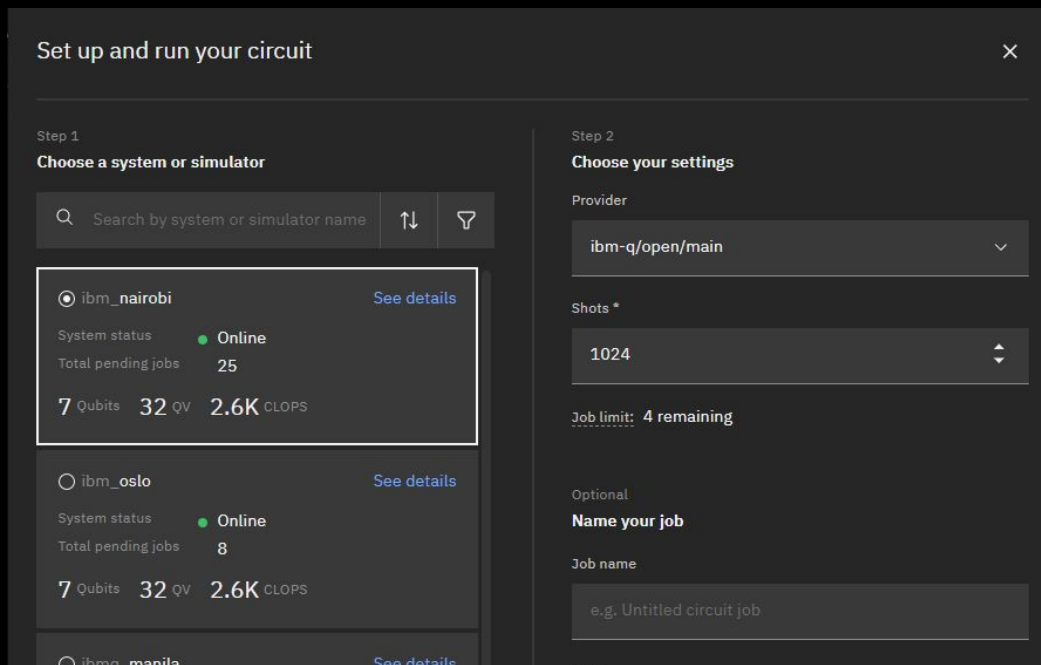
```
from qiskit import  
QuantumRegister
```

# RUNNING THE QUANTUM CIRCUIT

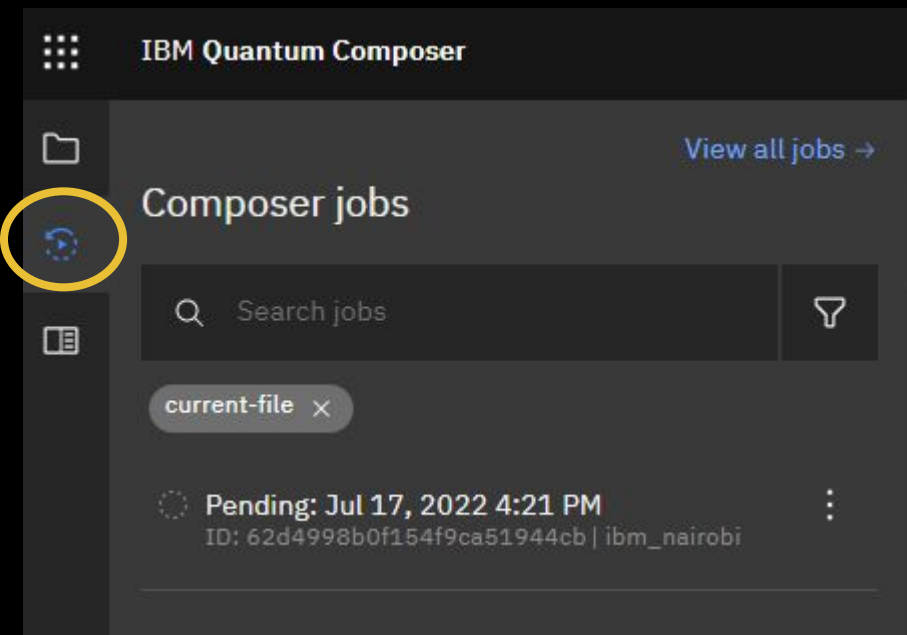


The screenshot shows the IBM Quantum Composer interface. At the top, the title bar reads "IBM Quantum Composer". Below it is a menu bar with "File", "Edit", and "View". The main workspace displays a quantum circuit with two qubits, q[0] and q[1]. Qubit q[0] has a red "H" gate and a grey "Z" gate. The right sidebar shows the "Visualizations seed" set to "2001" and a "Setup and run" button, which is highlighted with a yellow circle. Below the button are "Read only" and "Open in Quantum Lab" options. A code editor at the bottom shows the start of a Qiskit script: 

```
1 from qiskit import QuantumRegister
```



The screenshot shows the "Set up and run your circuit" dialog box. It is divided into two steps: "Step 1: Choose a system or simulator" and "Step 2: Choose your settings". In Step 1, there is a search bar and a list of providers. The provider "ibm\_nairobi" is selected and highlighted with a white box. Its details are: System status: Online (green dot), Total pending jobs: 25, 7 Qubits, 32 QV, 2.6K CLOPS. Other providers listed include ibm\_oslo and ibm\_manila. In Step 2, the "Provider" is set to "ibm-q/open/main", "Shots" is set to "1024", and "Job limit" is "4 remaining". There is also a section for "Optional: Name your job" with a text input field containing "e.g. Untitled circuit job".



The screenshot shows the IBM Quantum Composer interface with the "Composer jobs" panel open. The panel has a search bar and a filter icon. A job is listed in a "Pending" state: "Pending: Jul 17, 2022 4:21 PM" with ID "62d4998b0f154f9ca51944cb | ibm\_nairobi". A yellow circle highlights the play button icon in the top left of the jobs panel.

# 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

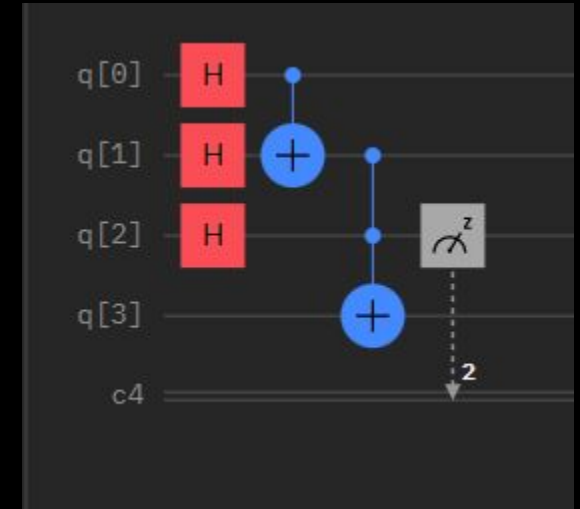
6 = name of this circuit

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

The screenshot shows the IBM Quantum Lab interface. On the left is a file browser with a table of files. The main area shows a 'Launcher' section with various options for creating new files or notebooks. A yellow circle highlights the 'Upload' icon in the top toolbar, with an arrow pointing to the text 'Upload notebooks'. A green circle highlights the 'Python 3 (ipykernel)' notebook icon in the launcher, with an arrow pointing to the code editor in the adjacent screenshot.

Name	Last Modified
qiskit-textbook	35 minutes ago
qiskit-tutorials	35 minutes ago
quantum-challenge	a year ago
JC-2021July-lab-5.ipynb	a year ago
JC-Lab 1-2021July-v1.ipynb	a year ago
JC-lab-1.ipynb	9 days ago
JC-lab-2-2021July-v1-done...	a year ago
JC-lab-3-2021July.ipynb	a year ago
JC-lab-4-2021July.ipynb	a year ago
JC-lab-5-2021July-v1.ipynb	a year ago
Untitled.ipynb	9 days ago

Launcher options:

- Notebook
  - Python 3 (ipykernel)
  - Getting started with Qiskit
  - Python 3 (ipykernel)
- Console
  - Python 3 (ipykernel)
- Other
  - Text File
  - Markdown File
  - Python File
  - Show Contextual Help

Upload notebooks

The screenshot shows the code editor in the IBM Quantum Lab. The code is as follows:

```
[1]: import numpy as np

# Importing standard Qiskit libraries
from qiskit import QuantumCircuit, transpile, Aer, IBMQ
from qiskit.tools.jupyter import *
from qiskit.visualization import *
from ibm_quantum_widgets import *
from qiskit.providers.aer import QasmSimulator

# Loading your IBM Quantum account(s)
provider = IBMQ.load_account()

<frozen importlib._bootstrap>:219: RuntimeWarning: scipy._lib.mtrandtool
ged, may indicate binary incompatibility. Expected 56 from C he

[ ]:
```