# Introduction to Quantum Computing @ SUTD

Huang Junye
Quantum Developer Advocate

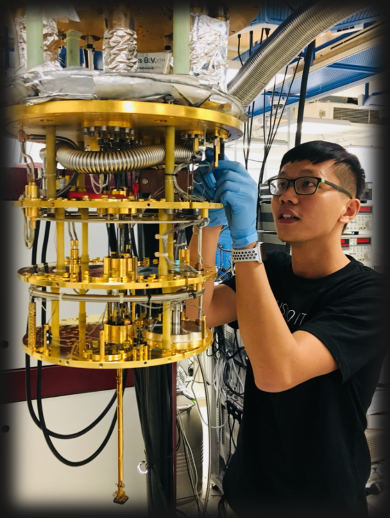


IBM **Quantum**

# Huang Junye

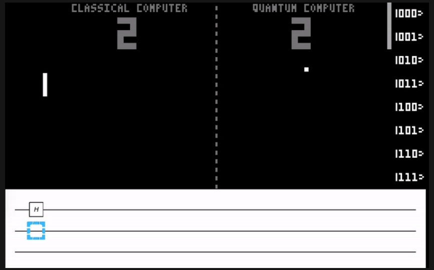
IBM **Quantum**

- Quantum developer advocate focusing on quantum education
- Leads Qiskit advocate program, supporting most active members of the Qiskit community through events, networking and mentorship.
- Led a team of 40+ for IBM Quantum Challenge 2021 for celebration of 5th anniversary of IBM Quantum and 40 years of quantum computing.
- Outstanding Accomplishment (highest level of recognition) from IBM Research for supporting Qiskit Global Summer School 2020.
- Co-creator of quantum games: QPong, QPong Arcade, QiskitBlocks, ...
- Graduate research in experimental low temperature physics at NUS




**IBM Quantum Challenge generates better solutions than challenge creators thought possible**

From May 20 to 26, 1,431 people from 76 countries participated in the IBM Quantum Challenge 2021, a celebration for 5-year anniversary of IBM Quantum and 40 years of quantum computing. Not only was the event a blast, but participants devised a more-efficient solution to one quantum computing problem than the problem's authors even thought possible.



# Agenda



| Date | Start | End | Subject |
|---|---|---|---|
| 26 Aug | 15:00 | 17:00 | Quantum Computing Lab |
| 27 Aug | 9:30 | 14:00 | Quantum Algorithms |

# Quantum Algorithms



| Start | End | Duration | Subject |
|---|---|---|---|
| 9:45 | 10:00 | 0:15 | Overview and Recap |
| 10:00 | 10:30 | 0:30 | Deutsch-Jozsa algorithm + hands-on implementations |
| 10:30 | 10:45 | 0:15 | Break |
| 10:45 | 11:20 | 0:35 | Grover’s algorithm +  + hands-on implementations |
| 11:20 | 12:00 | 0:40 | Shor’s algorithm + hands-on implementations |
| 12:00 | 13:00 | 1:00 | Lunch Break |
| 13:00 | 13:30 | 0:30 | Near-term algorithms and applications |

# Deutsch-Jozsa algorithm

# Deutsch-Jozsa Problem



$f(\{x_0, x_1, x_2, \ldots\}) \rightarrow$ 0 or 1 , where $x_n$ is 0 or 1

Determine a hidden function to be constant or balanced.

Constant example

| x | f(x) |
|---|---|
| 0 | 0 |
| 1 | 0 |
| 2 | 0 |
| 3 | 0 |

| x | f(x) |
|---|---|
| 0 | 1 |
| 1 | 1 |
| 2 | 1 |
| 3 | 1 |

Balanced example

| x | f(x) |
|---|---|
| 0 | 0 |
| 1 | 1 |
| 2 | 1 |
| 3 | 0 |

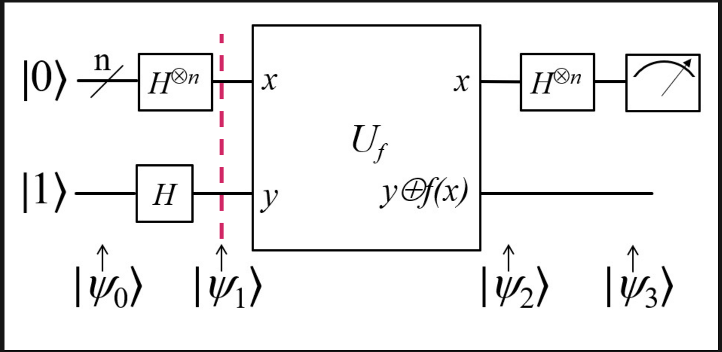
| x | f(x) |
|---|---|
| 0 | 1 |
| 1 | 0 |
| 2 | 1 |
| 3 | 0 |

Classical: $2^{n-1}+1$

Quantum: 1

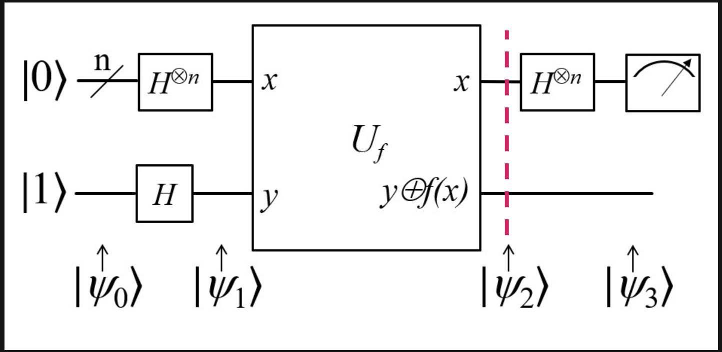
# DJ Step 1






$$\frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} |x\rangle(|0\rangle - |1\rangle)$$

# DJ Step 2

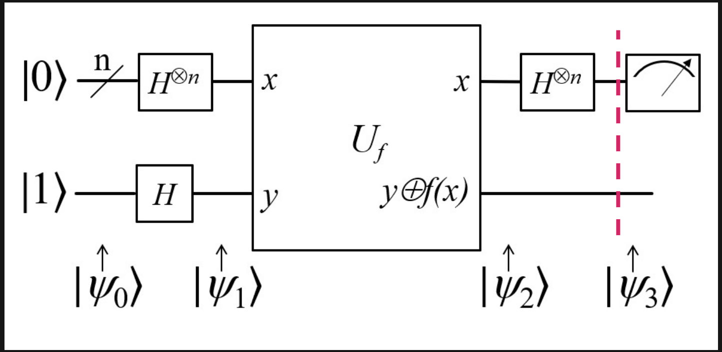



$$\frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} |x\rangle(|f(x)\rangle - |1 \oplus f(x)\rangle)$$

$$= \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle(|0\rangle - |1\rangle)$$

$$= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle$$

# DJ Step 3




$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \left[ \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle \right]$$

$$= \frac{1}{2^n} \sum_{y=0}^{2^n-1} \left[ \sum_{x=0}^{2^n-1} (-1)^{f(x)} (-1)^{x \cdot y} \right] |y\rangle$$

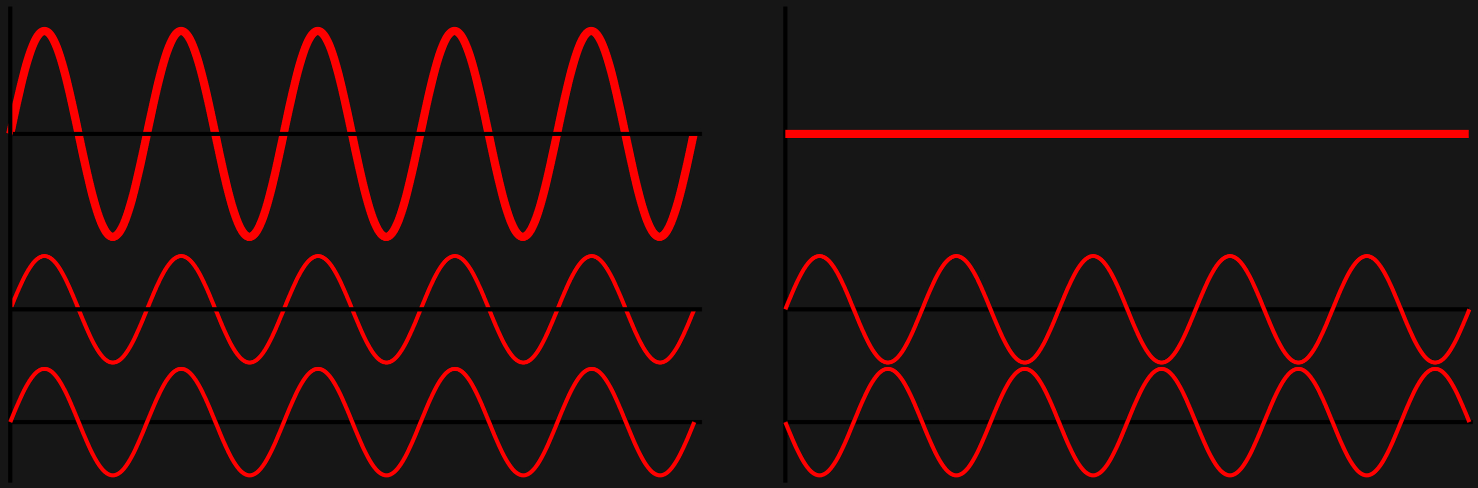
Probability of measuring $|0\rangle^{\otimes n}$ : $\left| \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \right|^2$ ➡

If f(x) is constant: p = 1

If f(x) is balanced: p = 0

# How does it work? Interference!





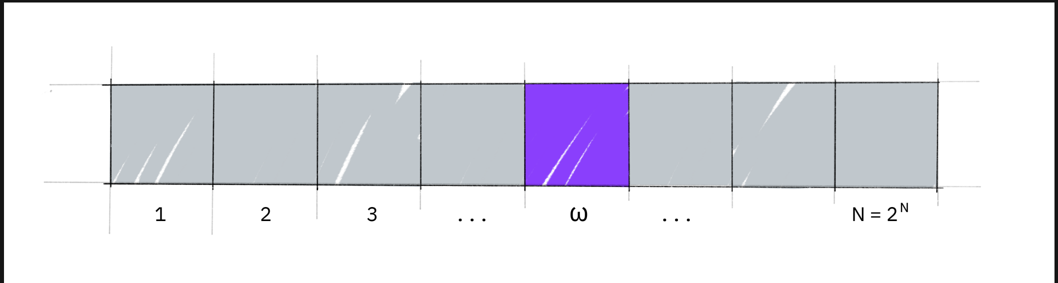
Constant

Balanced

# Grover’s algorithm

# Unstructured search problem

IBM **Quantum**

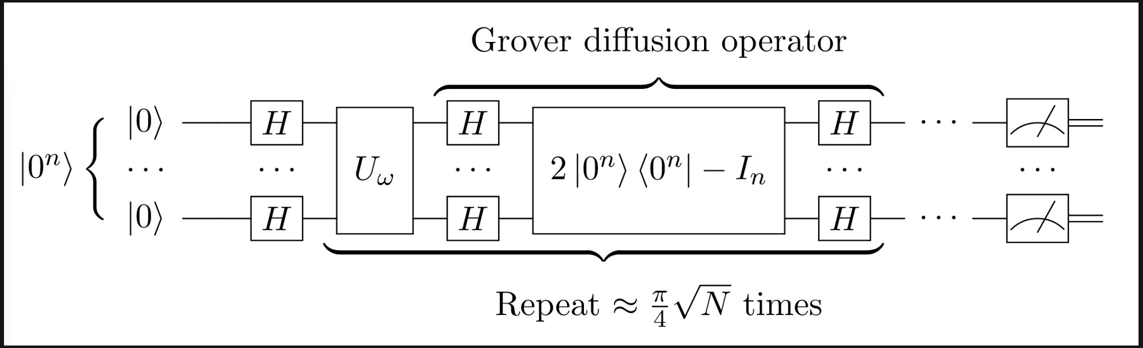



Search for an element in an unstructured data base

Classical: $O(N)$

Quantum: $O(\sqrt{N})$

# Grover’s algorithm

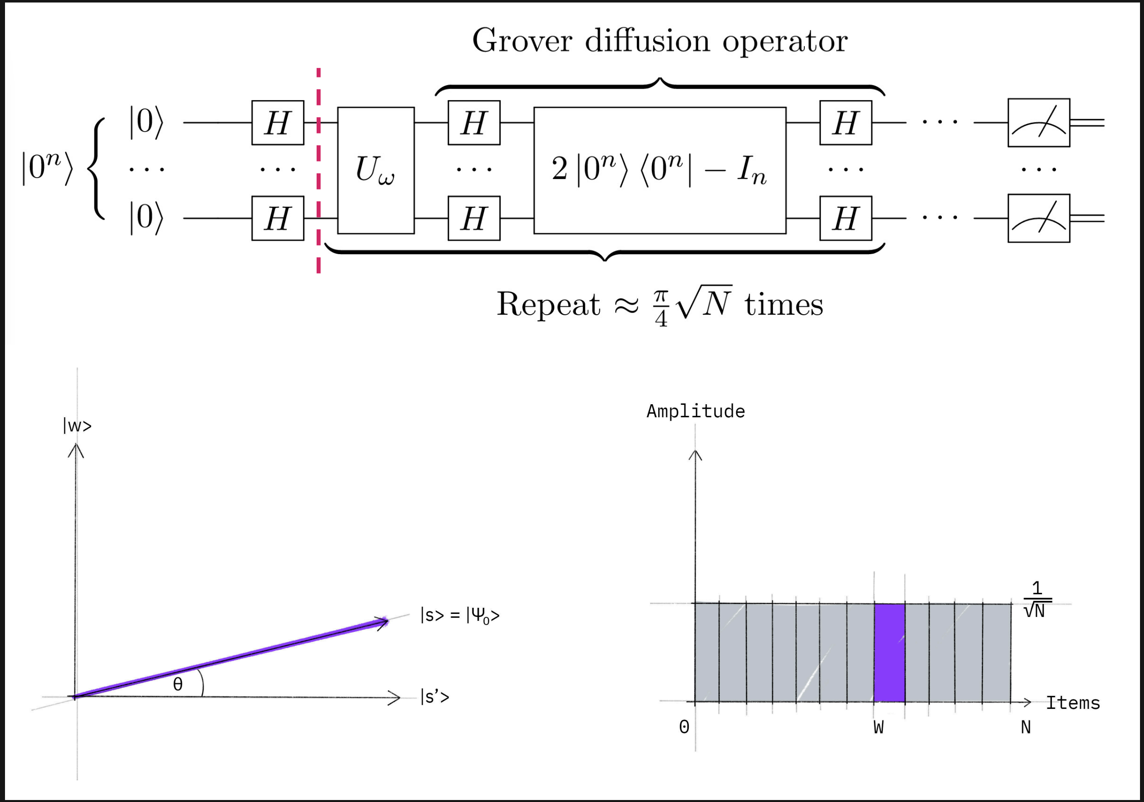



Algorithm:

1. Initialize the system to the uniform superposition over all states
2. Apply oracle $U_w$
3. Apply diffusion operator
4. Repeat step 2 & 3
5. Measure

# Grover Step 1



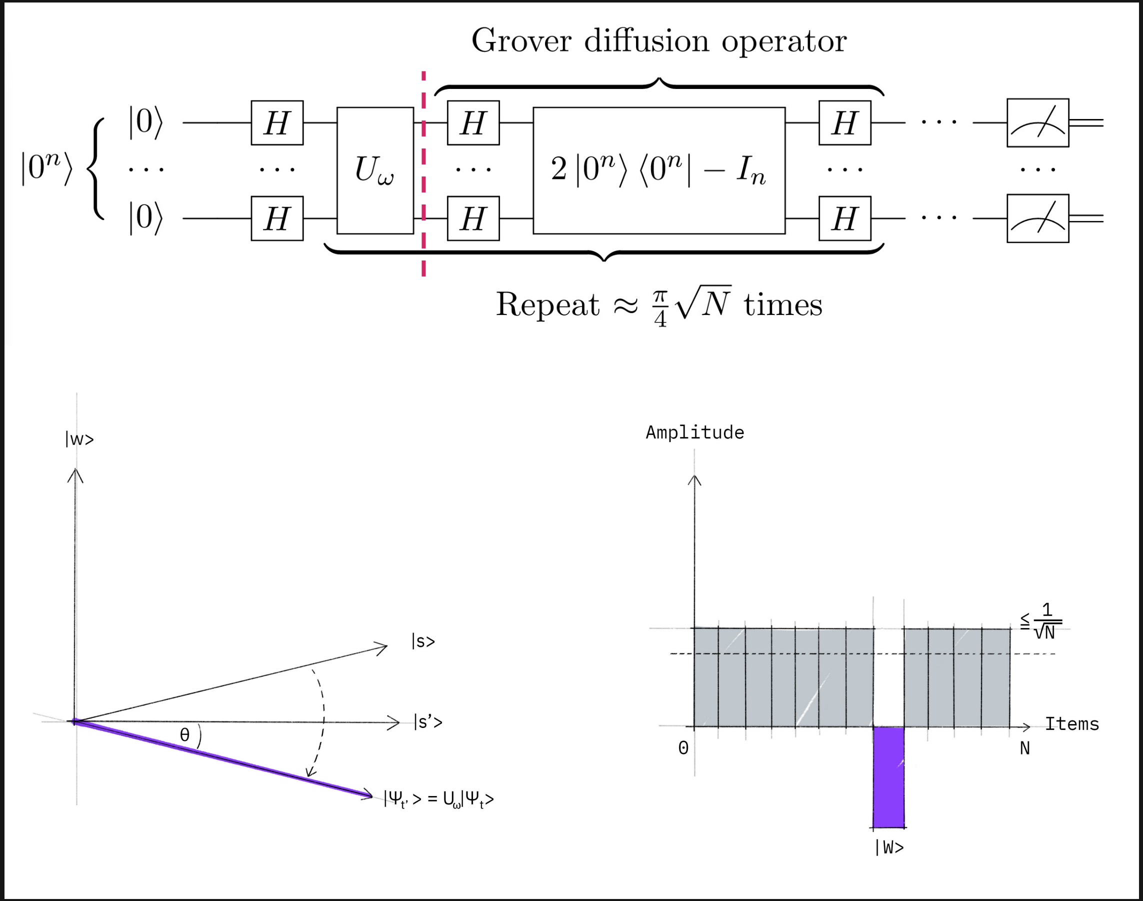



Step 1: Initialize the system to the uniform superposition over all states

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

# Grover Step 2



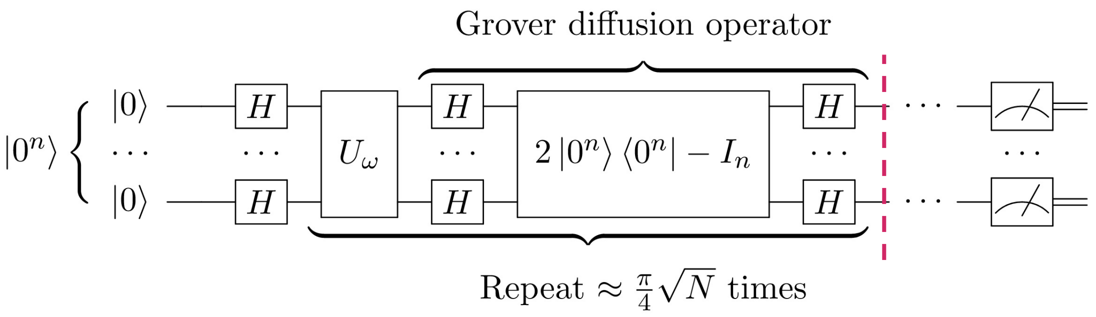


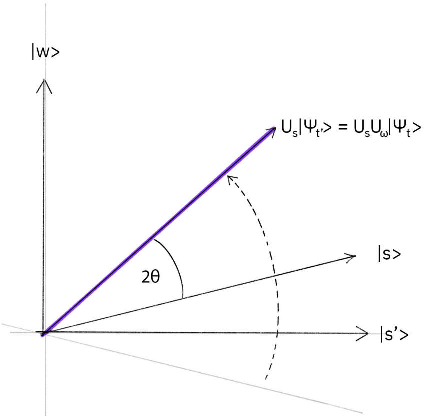

Step 2: Apply oracle $U_w$

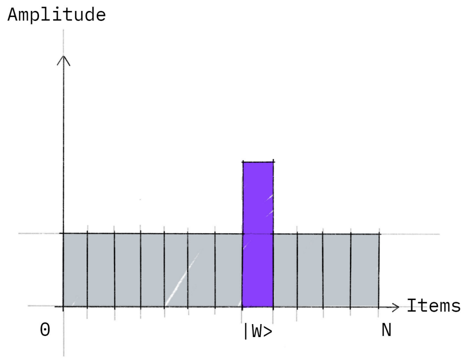
$$U_f|x\rangle = (-1)^{f(x)}|x\rangle$$

# Grover Step 3






Step 2: Apply diffuser $U_s$

$$U_s = 2|s\rangle\langle s| - 1$$

$$U_sU_w|x\rangle$$

Repeat r times

$$(U_sU_w)^r|x\rangle$$

# Shor’s algorithm

# RSA encryption



- Widely used and assumed to be safe
- In 1994, Peter Shor proposed an algorithm which showed exponential speedup compared to the best-known classical algorithm
- Ignited the field

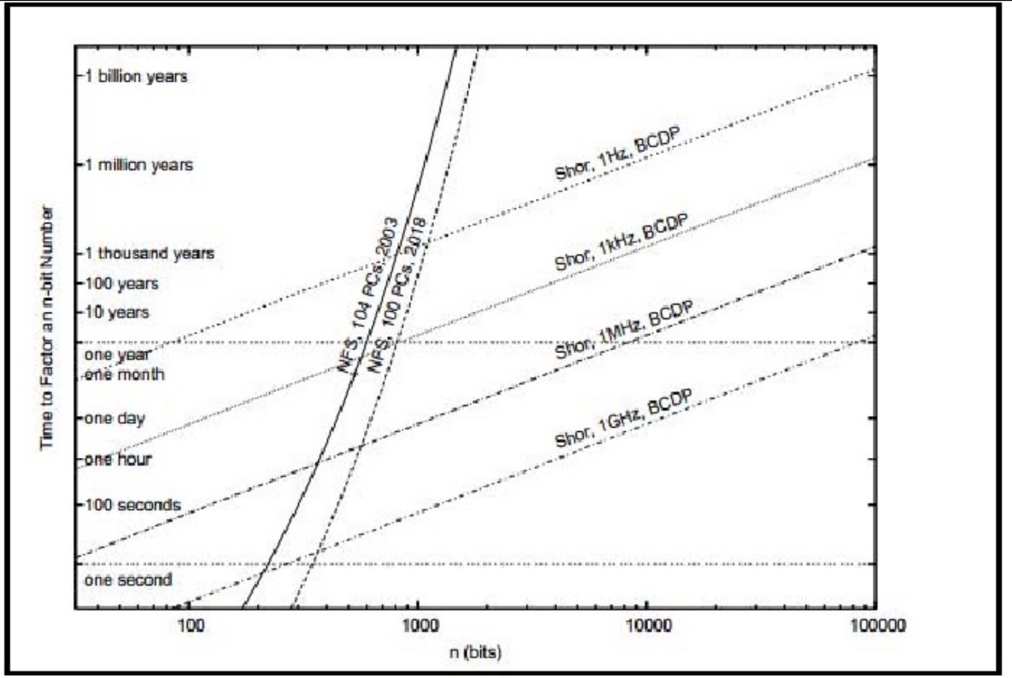



Fig. 1. Scaling of general number field sieve (GNFS) on classical computers and Shor's algorithm for factoring on a quantum computer, using BCDP modular exponentiation with various clock rates [14].

S. M. Hamdi, S. T. Zuhori, F. Mahmud and B. Pal, "A Compare between Shor's quantum factoring algorithm and General Number Field Sieve," *2014 International Conference on Electrical Engineering and Information & Communication Technology*, 2014, pp. 1-6, doi: 10.1109/ICEEICT.2014.6919115.

# How to crack RSA?



1. Find prime factors g1, g2 for N such that $g_1 \times g_2 = N$
2. Same as finding

$$\begin{aligned} x^2 &\equiv 1 (\mathrm{mod}\ N) \\ (x+1)(x-1) &\equiv 0 (\mathrm{mod}\ N) \end{aligned} \qquad \begin{aligned} gcd(x+1, N) &= g_1 \\ gcd(x-1, N) &= g_2 \end{aligned}$$

3. How to find x? => pick a random number x in the range [0, N-1], find r such that

$$\begin{aligned} &x^0 \\ &x^1 \\ &\ldots \\ &x^r \equiv 1 (\mathrm{mod}\ N) \end{aligned} \qquad \begin{aligned} &(x^{r/2})^2 \equiv 1 (\mathrm{mod} N) \\ &gcd(x^{r/2}+1) \\ &gcd(x^{r/2}-1) \end{aligned}$$

4. How to find r? => period finding => quantum Fourier transform

# Modular arithmetic



examples

$$3 \equiv 24 (\bmod 21)$$
$$14 \equiv 35 (\bmod 21)$$
$$1 \equiv -20 (\bmod 21)$$

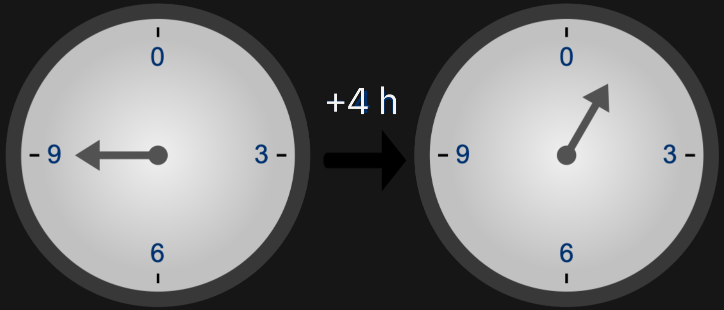
addition

$$24 + 35 (\bmod 21)$$
$$\equiv 3 + 14 (\bmod 21)$$
$$\equiv 17 (\bmod 21)$$

multiplication

$$24 \times 30 (\bmod 21)$$
$$\equiv 3 \times 9 (\bmod 21)$$
$$\equiv 27 (\bmod 21)$$
$$\equiv 6 (\bmod 21)$$

Hours in a clock is modular 12



# Greatest common divisor

The largest positive integer that divides each of the integers

Examples

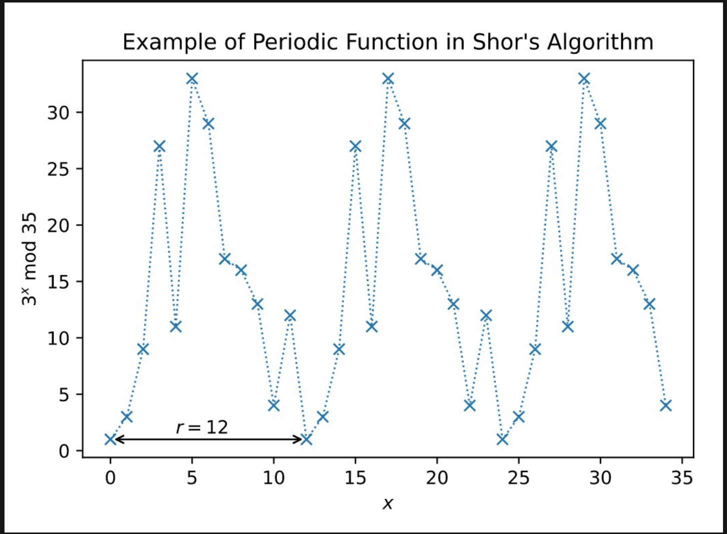
- gcd(8,12) = 4
- gcd(54,24)=6

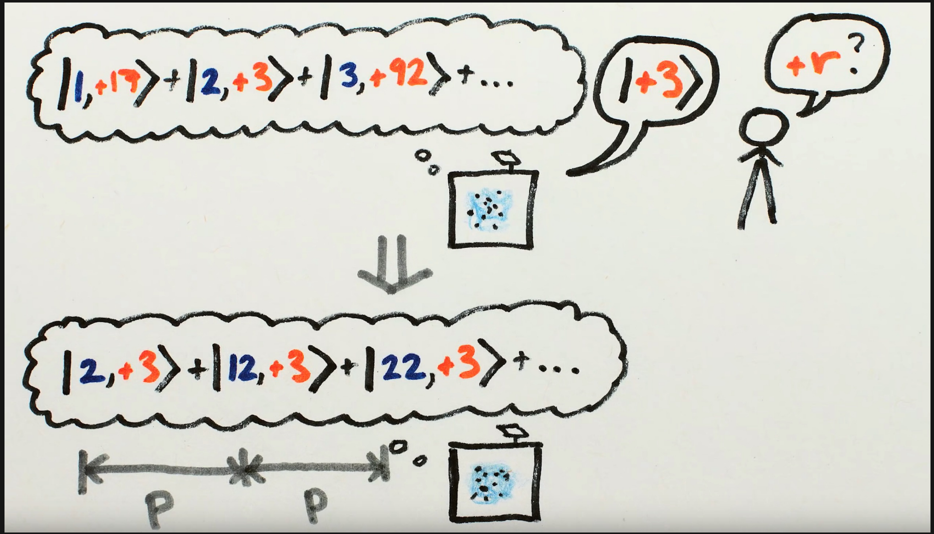
2000-year-old efficient classical algorithm for finding gcd:
Euclidean algorithm

# Period finding using QFT



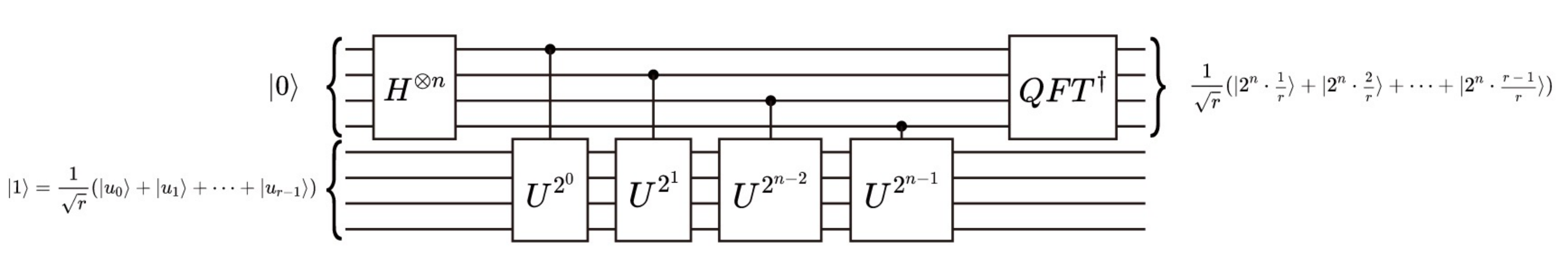
This is the crust of Shor's algorithm



# Shor’s algorithm





# Near-term algorithms & applications

# Potential Use Cases for Quantum Computing

| | Chemicals and Petroleum | Distribution and Logistics | Financial Services | Health Care and Life Sciences | Manufacturing |
|---|---|---|---|---|---|
| ● Chemical Simulation | Chemical product design<br>Surfactants, Catalysts | | | Drug Discovery<br>Protein Structure Predictions | Materials Discovery<br>Quantum Chemistry |
| ■ Scenario Simulation | | Disruption Management | Derivatives Pricing<br>Investment Risk Analysis | Disease Risk Predictions | |
| ▲ Optimization | Feedstock To Product<br>Oil Shipping / Trucking<br>Refining Processes | Distribution Supply Chain<br>Network Optimization<br>Vehicle Routing | Portfolio Management<br>Transaction Settlement | Medical/Drug Supply Chain | Fabrication Optimization<br>Manufacturing Supply Chain<br>Process Planning |
| ◆ AI/ML | Drilling Locations<br>Seismic imaging | Consumer Offer Recommender<br>Freight Forecasting<br>Irregular Behaviors (ops) | Finance Offer Recommender<br>Credit/Asset Scoring<br>Irregular Behaviors (fraud) | Accelerated Diagnosis<br>Genomic Analysis<br>Clinical Trial Enhancements | Quality Control<br>Structural Design & Fluid Dynamics |

 #IBMQ

# Near-term algorithms and applications



Textbook algorithms are too stringent

Near term computers are noisy

Need shorter circuits

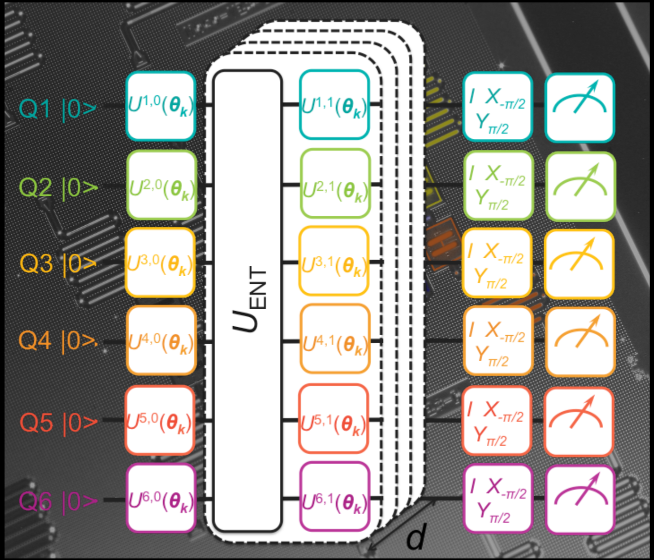
Quantum-classical hybrid algorithms

- Variational quantum eigensolver (VQE)
- Quantum approximate optimization algorithm (QAOA)

# Variational Quantum Eigensolver (VQE)

$$H = \sum_\alpha h_\alpha \sigma(\alpha)$$

Map problem onto Paulis




Prepare guess state $|\psi_G(\vec{\theta})\rangle$

Measure its energy

$$E(\vec{\theta}) = \sum_\alpha h_\alpha \langle \psi_G(\vec{\theta})|\sigma_\alpha|\psi_G(\vec{\theta})\rangle$$

$E(\vec{\theta})$

$\vec{\theta}$

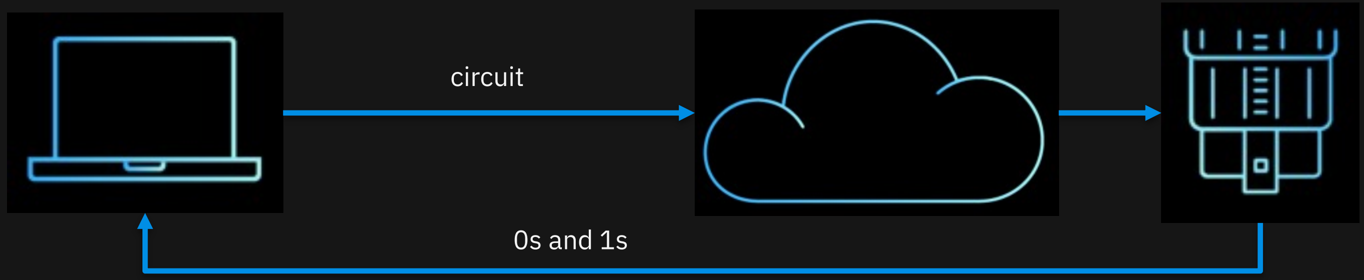
Use classical optimizer

Nat. Commun 5, 4213 (2014)
Nature **549**, 242-246 (2017)

# Qiskit Runtime (Dynamic circuit)



A static circuit is run sequentially with the result returned to the user.



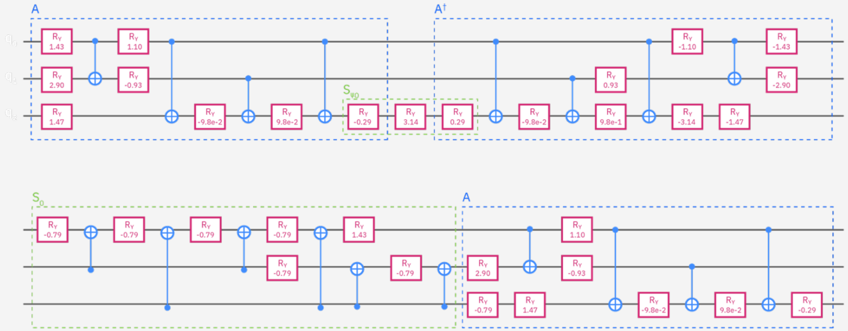

A dynamic circuit can measure qubits mid-circuit and change the flow of processing.

# JP Morgan Chase

## Quantum Computing for the Financial Services Industry

Recently, JPMC and IBM used Quantum Amplitude Estimation, a Monte Carlo-like sampling algorithm, to compute European option pricing, pricing path depend options, showing a quadratic speed-up versus a classical Monte Carlo approach.

European derivative pricing circuit

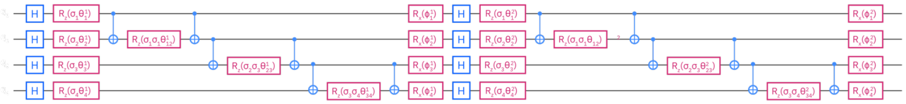


# Daimler

## Quantum Computing for Materials Discovery and Manufacturing Optimization

Daimler and IBM have recently published a series of papers demonstrating progress toward using quantum computers to model material systems including Lithium-sulfur that are relevant to advancing the performance of batteries. The teams have also demonstrated applications in manufacturing defect analysis and product recommendation.

Energy of binary crystalline materials circuit.

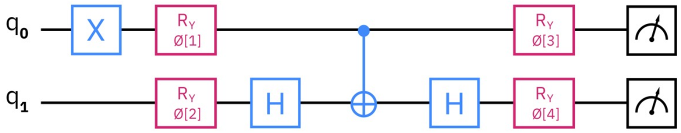


# ExxonMobil

## Quantum Computing as a Tool for Chemistry and Engineering

Working together, ExxonMobil and IBM recently demonstrated advancements in using quantum computers to accurately calculate thermodynamic observables, demonstrating how quantum can be the next generation tool for chemists and chemical engineers developing advanced energy solutions.

Accurate thermodynamic observables calculation circuit



# What are the next steps?

# Deutsch-Jozsa algorithm

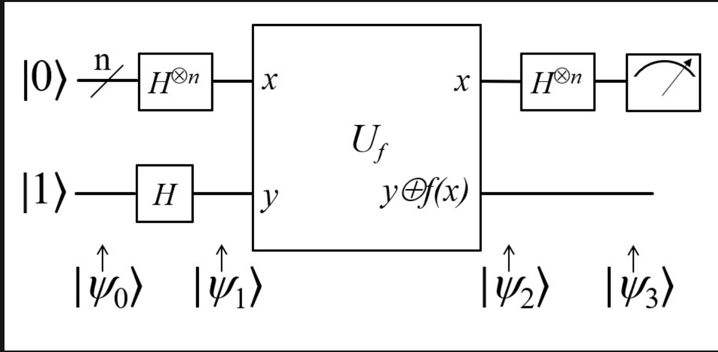


**Deutsch-Jozsa problem**

$f(\{x_0,x_1,x_2,\ldots\}) \rightarrow 0$ or 1 , where $x_n$ is 0 or 1

Determine a hidden function to be constant or balanced.

**Deutsch-Jozsa algorithm**




[Qiskit textbook chapter]

[Circuit composer demo]

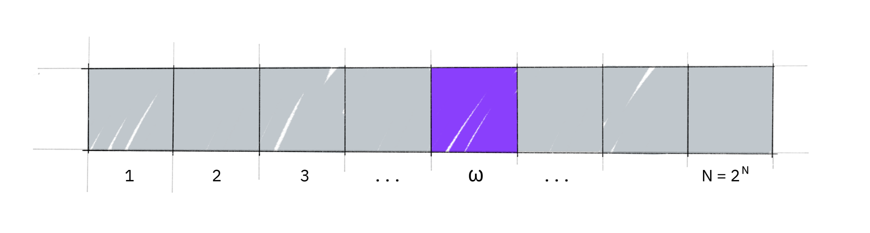
[Qiskit notebook demo]

[Qiskit GSS lecture]

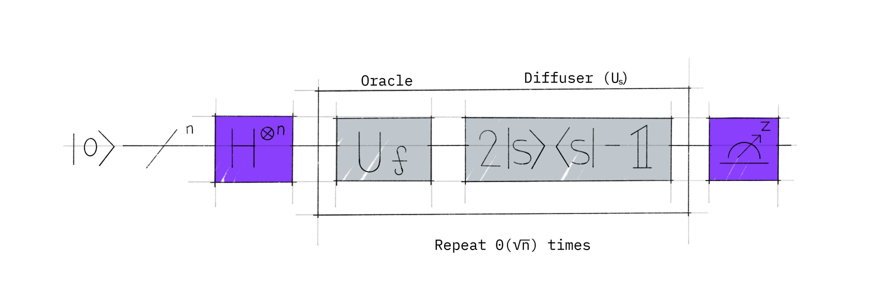
[Lecture note]

# Grover’s algorithm

## Unstructured search problem

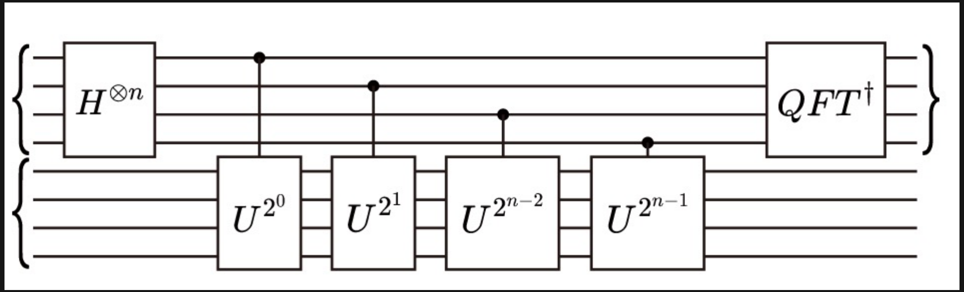



## Grover’s algorithm




- [Qiskit textbook chapter]
- [Circuit composer demo]
- [Qiskit notebook demo]
- [Qiskit GSS lecture]
- [Lecture note]

# Shor’s algorithm




- Qiskit textbook chapter
- Circuit composer demo*
- Qiskit notebook demo
- Qiskit GSS lecture
- Lecture note 1 and 2

# IBM Quantum Challenge Africa 2021

The IBM Research Lab in South Africa and Wits University have developed a quantum computing challenge showcasing how the technology can be used in the fields of medicine, finance, and logistics.

With a focus on problems relevant to Africa for African learners, students, and industry members; the challenge highlights the amazing opportunities available to grow the necessary expertise and communities on the continent.

9 September (07:00 UTC) -
20 September (23:00 UTC)

Learn more at ibm.co/ibmQuantumAfrica21

# Qiskit Developer Certification




Quantum industry’s first developer certificate

A requirement for becoming a Qiskit advocate

# IBM Quantum Resources – Self-learning



## IBM Quantum Composer and IBM Quantum Lab

Cloud applications for programming real quantum hardware and high performance simulators

## Qiskit Online Open Source Textbook

Interactive advanced text on quantum algorithms and computation based on Qiskit

## Qiskit Youtube Channel

- Coding with Qiskit Series: learn to program quantum computers with Qiskit
- Qiskit Live: livestream of public lecture series
- SuperPosition Series: explores how individuals became Qiskit developers
- 1 Minute Qiskit: Qiskit tips & tricks

## Qiskit.org

Open-source quantum computing software development

- Documentation, Tutorials, Events, Education
- Metal - quantum device design
- OpenQASM 3.0

# Qiskit on Social Networks

IBM **Quantum**

Follow @Qiskit

[Twitter]

[YouTube]

[Slack]

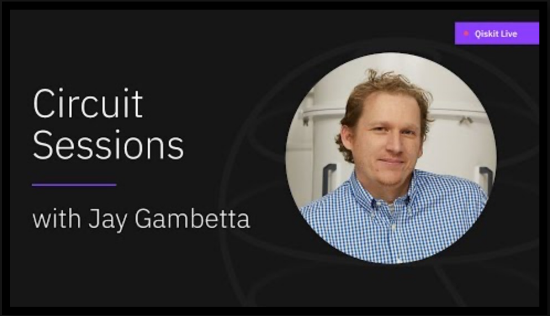
[Medium]

Coding with Qiskit


1 minute Qiskit (every Monday)


SuperPosition

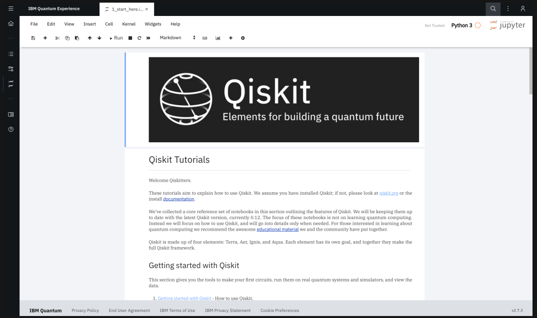

Qiskit Live (every Wednesday and Friday)



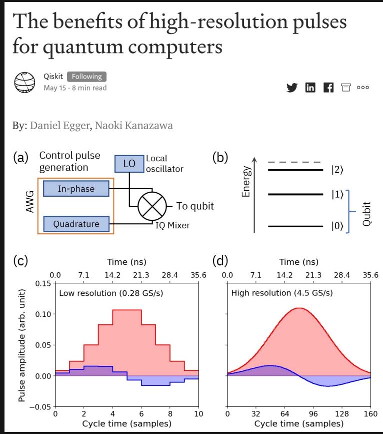

# Qiskit Learning Resources

IBM **Quantum**

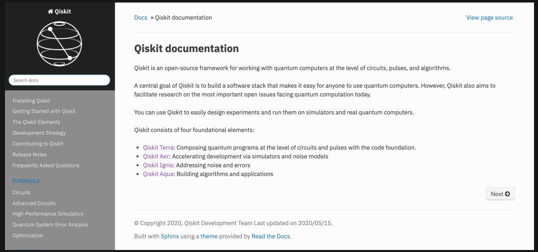

[Qiskit textbook]



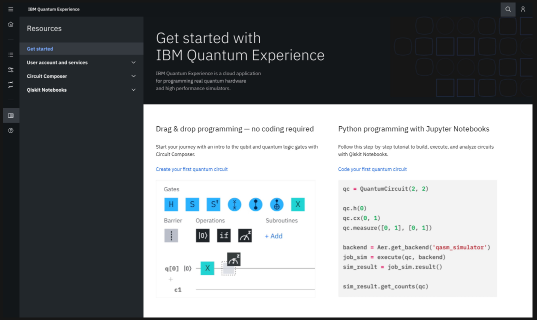

[Qiskit tutorials]



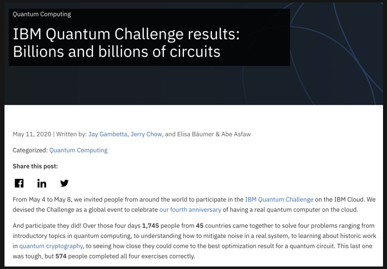

[Qiskit Medium]




[Qiskit documentation]



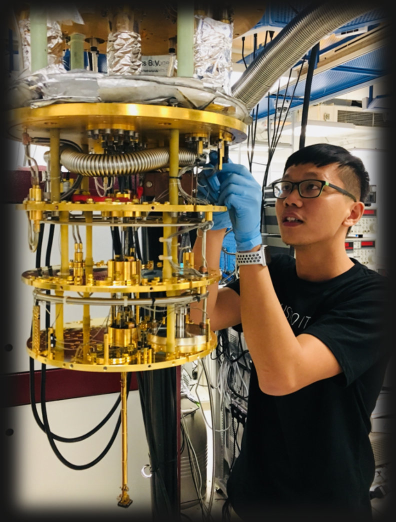

[IQX documentation]




[IBM Research Blog]

# Contacts





Huang Junye

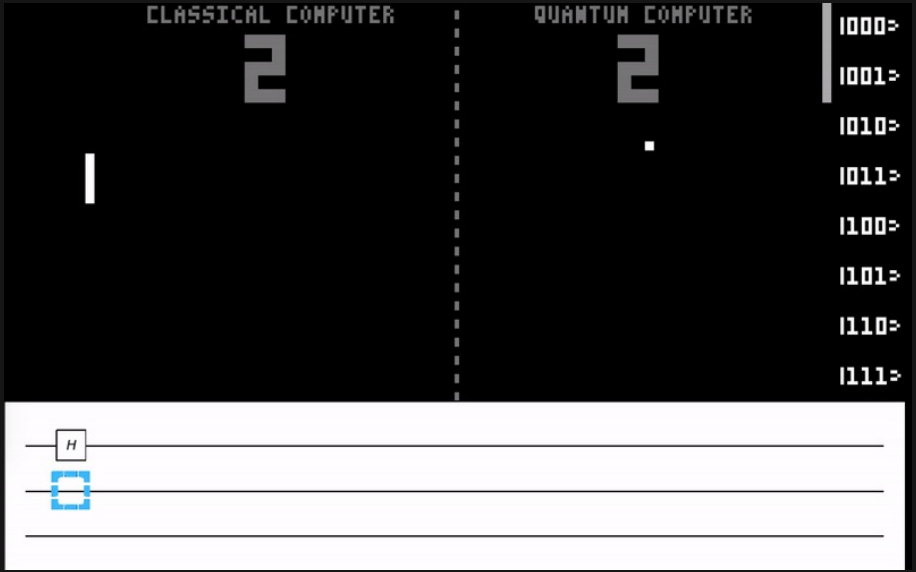
@HuangJunye

Huang Junye

@Junye

junye.huang@ibm.com

# QPong


CLASSICAL COMPUTER
2
QUANTUM COMPUTER
2
|000>
|001>
|010>
|011>
|100>
|101>
|110>
|111>
H


clockwork
1 2
|000⟩
|001⟩
|010⟩
|011⟩
|100⟩
|101⟩
|110⟩
|111⟩
H
H
WARNING
Hot plug is inhibited
320x240 PIXEL LCD SCREEN
clockwork
GameSH>
– VOL +
MENU
Shift
Select
Start

IBM **Quantum**

https://quantum-computing.ibm.com