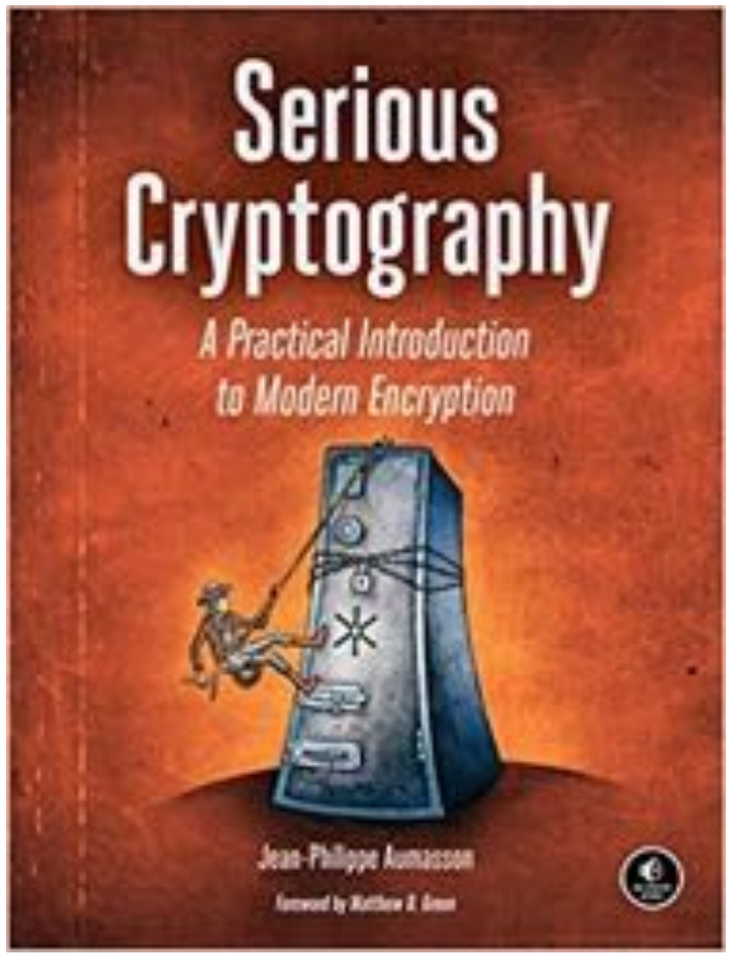
# CNIT 141

# Cryptography for Computer Networks




## 14. Quantum and Post-Quantum

**Updated 12-3-20**

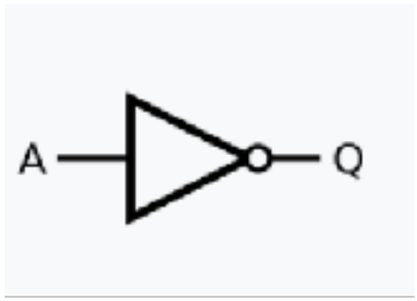
# Topics

- How Quantum Computers Work
- Quantum Speed-Up
- Whi Is It So Hard tp Build a Quantum Computer?
- Post-Quantum Cryptographic Algorithms
- How Things Can Go Wrong

# How Quantum Computers Work

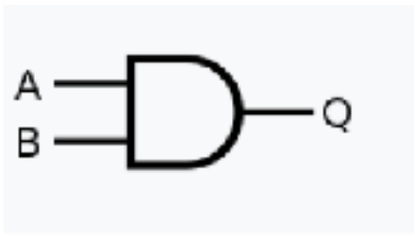
# Digital Computing
# Logic Gates

NOT



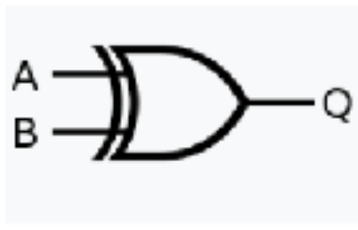

| A | Q |
|---|---|
| 0 | 1 |
| 1 | 0 |

AND




| A | B | Q |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 0 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |

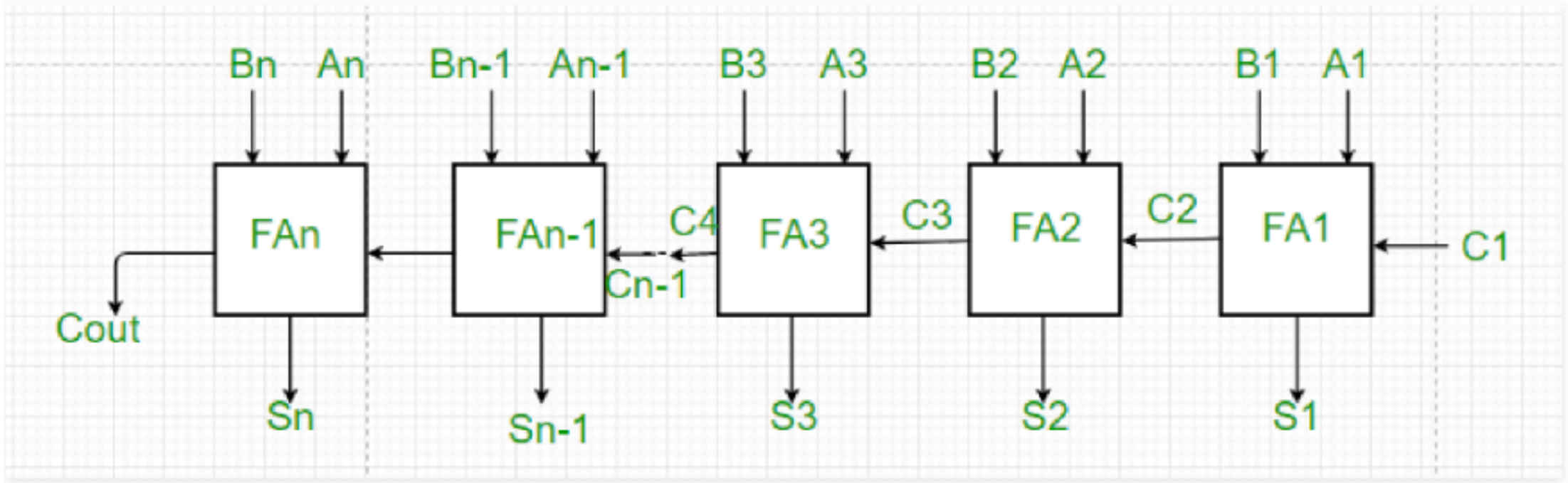
XOR




| A | B | Q |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

- From Wikibooks (link Ch 14a)

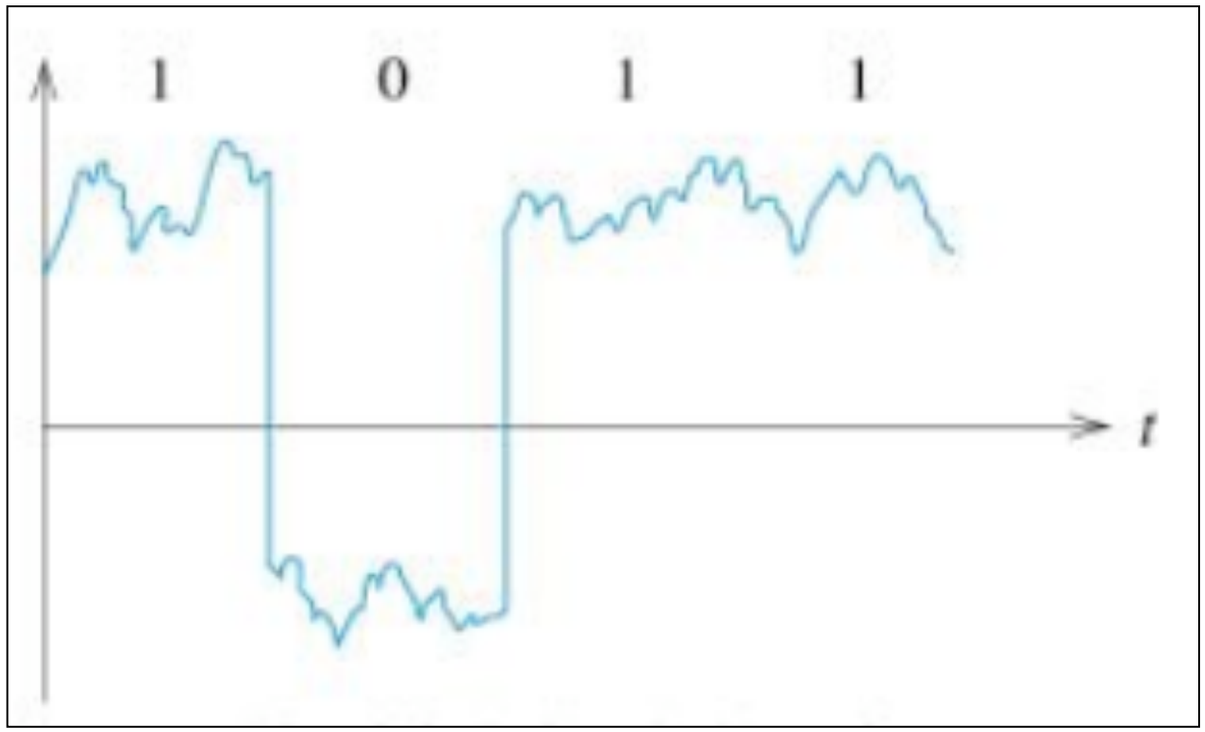
# Digital Adder




- From geeksforgeeks.com (link Ch 14b)

# Analog to Digital

- Real devices are **analog**
- Digital circuits minimize time spent in the "forbidden zone"

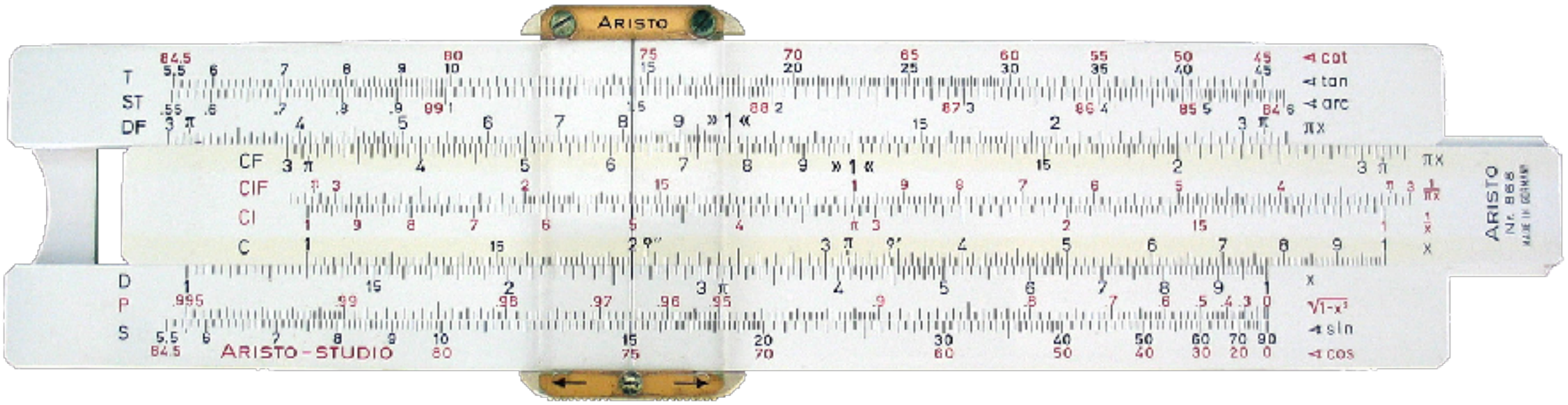



- ***Error correction*** is needed
  - From Wikipedia (link Ch 14c)

# Analog Computing

- The Antikythera mechanism, dating between 150 and 100 BC, was an early analog computer.
- From Wikipedia (link Ch 14d)

# Slide Rule



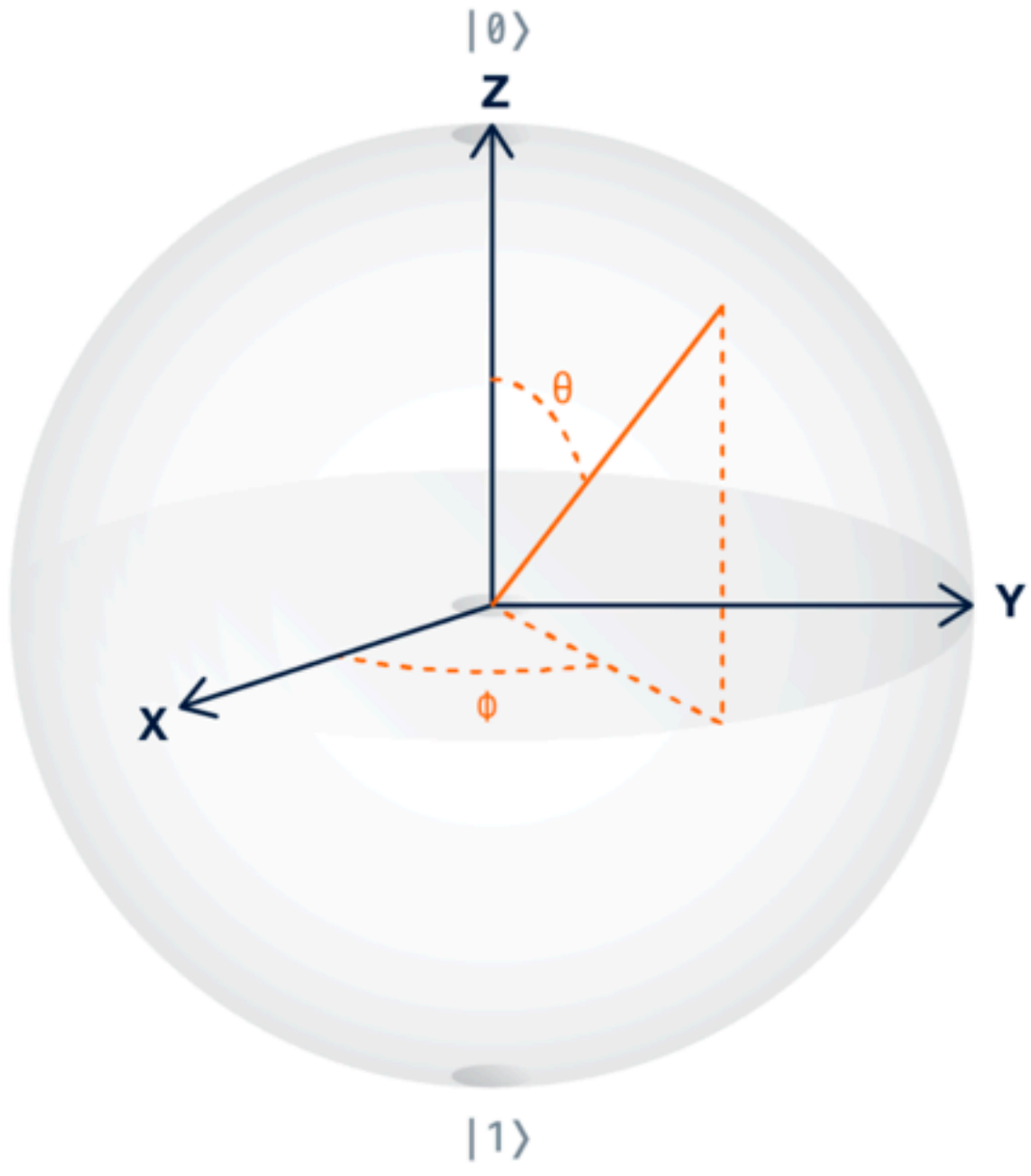

- How many bits does it process?

# Flute

- Input: white noise
- Output: clear note
- Analog Fourier transform
- How many bits does it process?

# Qubit
# Bloch Sphere

- Certain states
  **|0>** and **|1>**
  are at the top and bottom
- Uncertain or ***superposition*** states are in between
  - ***Collapses*** to **1** or **0** when ***measured***



# Range of States

- Digital computing
  - One byte has 8 bits of information
  - 256 possible states
- 8 qubits
  - Qubit might have any possible value
  - 256 complex numbers required to specify state

$$\alpha_0 |00000000\rangle + \alpha_1 |00000001\rangle + \alpha_2 |00000010\rangle + \alpha_3 |00000011\rangle + \ldots + \alpha_{255} |11111111\rangle$$

# Range of States

- Digital computing
  - ***n*** bits contains ***n*** bits of information
- ***n*** qubits
  - Contain $2^n$ complex floating-point values

# Quantum Algorithm

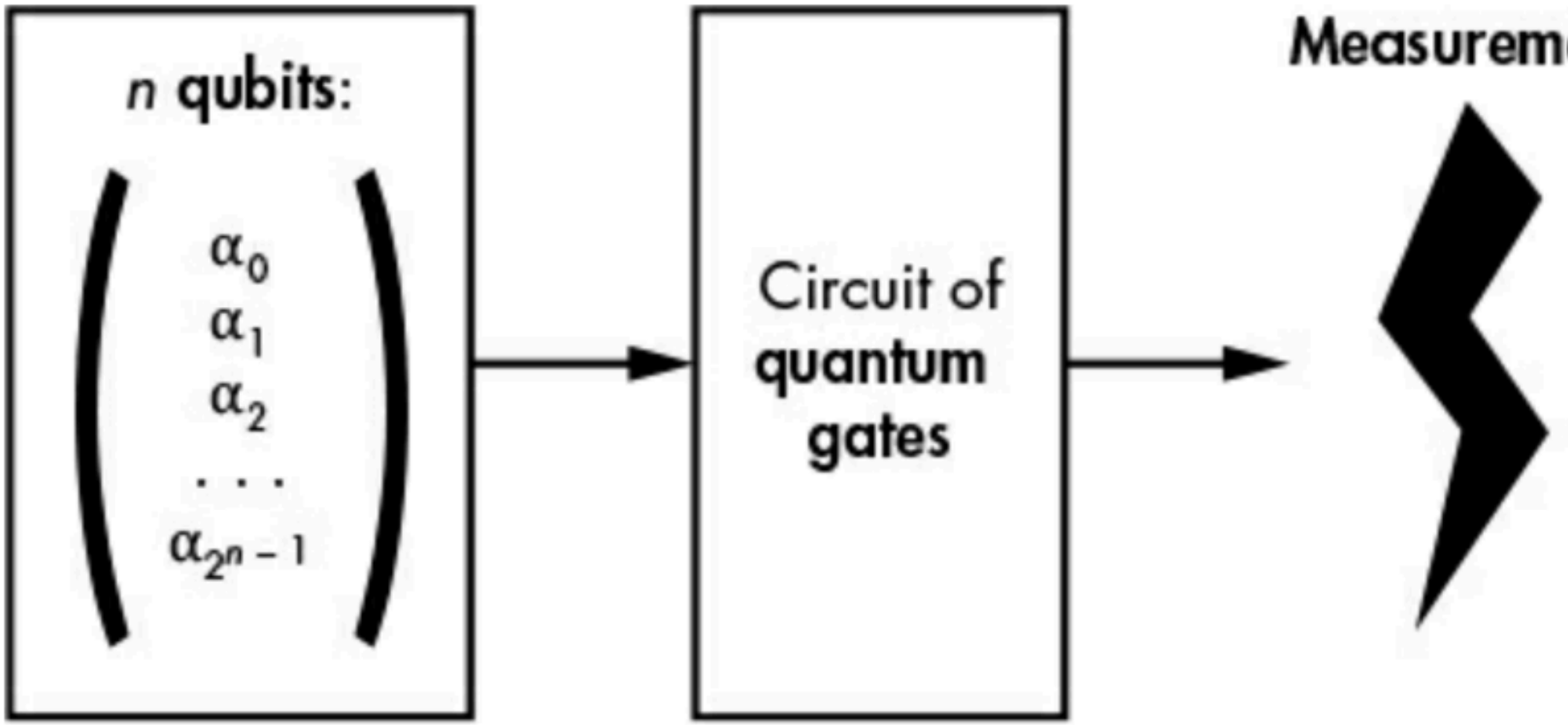



*Figure 14-3: Principle of a quantum algorithm*

# Quantum Gates


Measurement

X

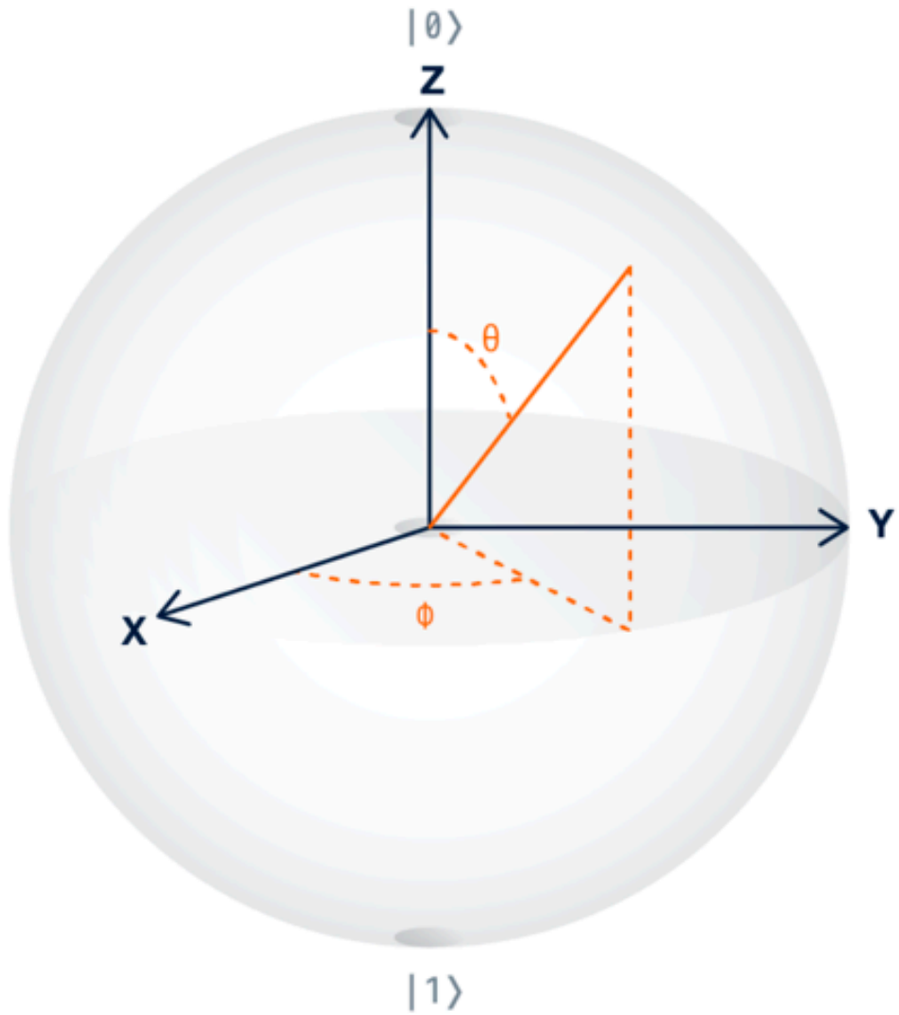
180° rotation about X axis: Bit-flip

***Hadamard gate***

H

180° rotation about X-Z axis: Bit-flip

Converts a ***certain*** state to a ***superposition*** state



# Quantum Speed-Up

# Searching a List

- Searching an unordered list of ***n*** items
- Classical computer
  - ***n*/2** operations
- Quantum computer:
  - **sqrt(*n*)** operations
  - Using Grover's algorithm

# Simon's Problem

- Similar to hash collisions
- Given a function **f**()
- Find ***m*** such that
  - For all ***x***, **y** satisfying **f**(***x***) = **f**(***y***)
  - Then $\boldsymbol{y = x \oplus m}$

# Simon's Problem

- Classical computer
  - Takes $\mathbf{2^{n/2}}$ operations
- Quantum computer
  - Takes $\boldsymbol{n}$ operations

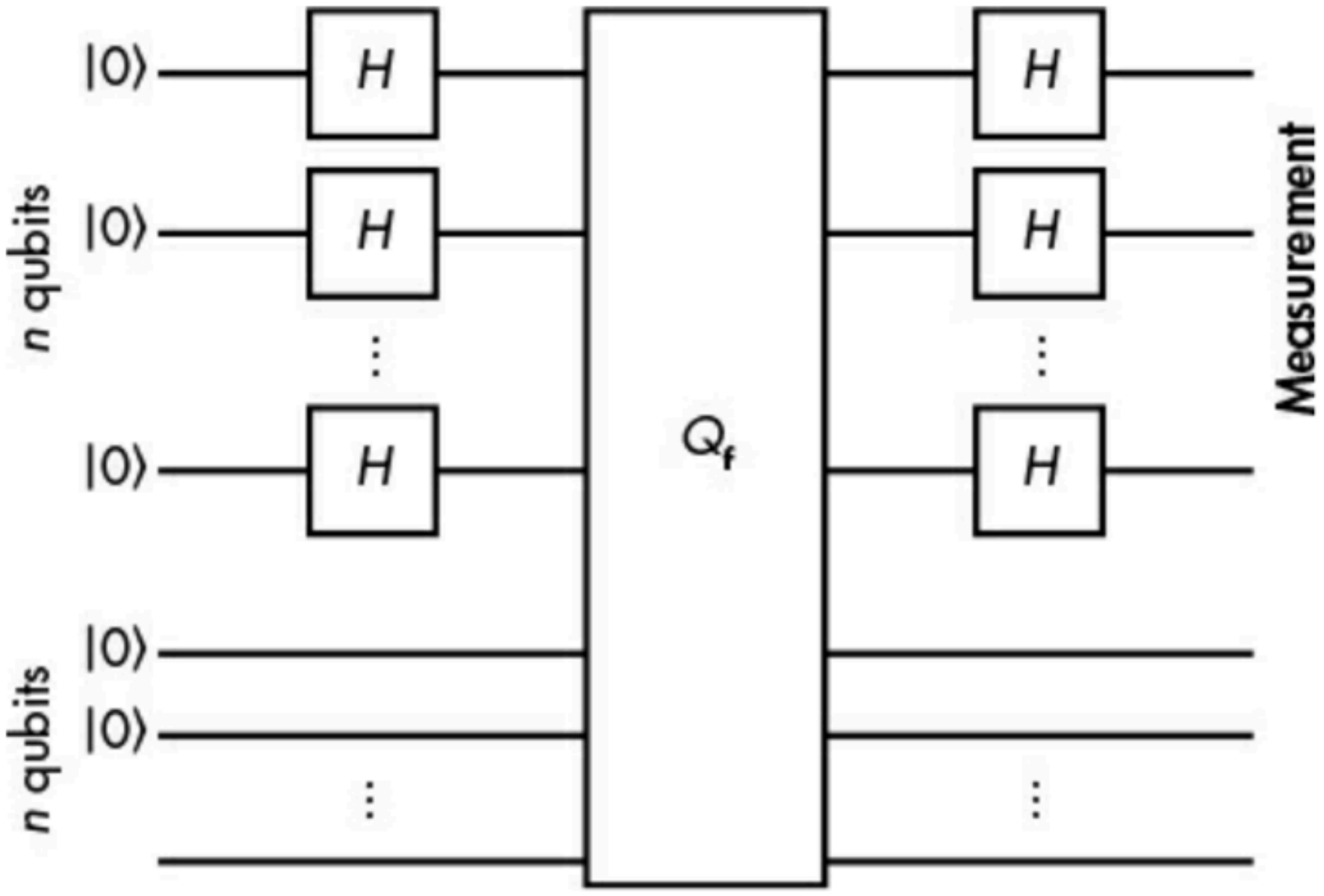



*Figure 14-4: The circuit of the quantum algorithm that solves Simon's problem efficiently*

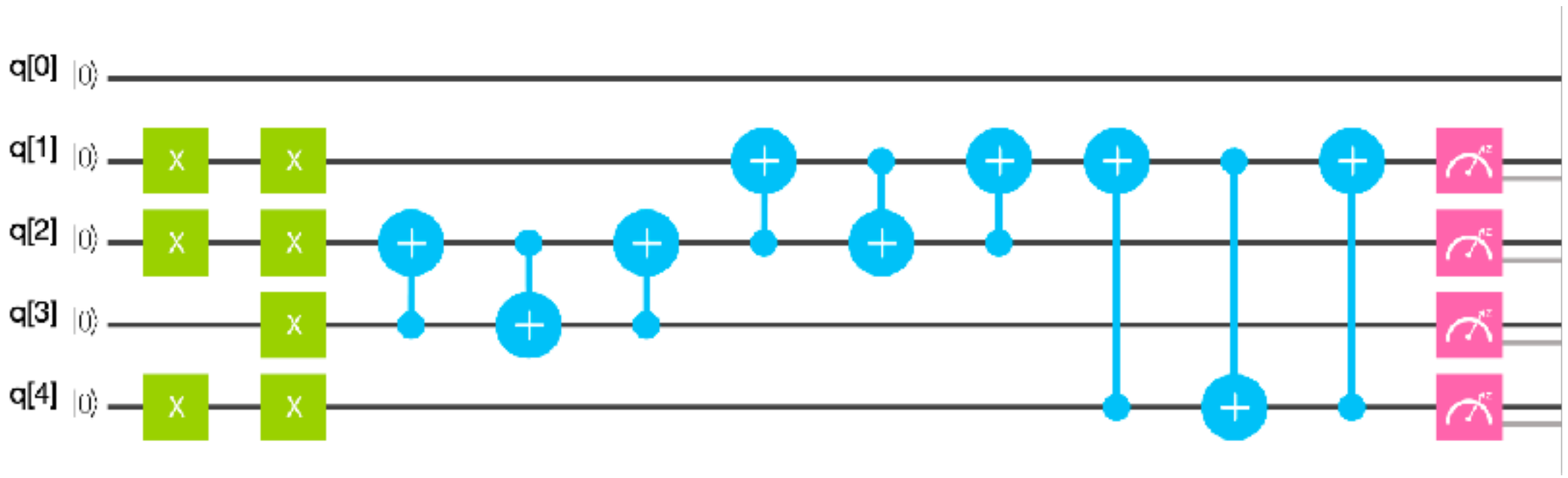
# Shor's Algorithm

- Factors numbers into prime factors
- Solves Discrete Logarithm Problem (DLP)
- And the Elliptic Curve DLP

- Breaks RSA, Diffie-Hellman, ECC
  - And all currently deployed public-key algorithms

# Shor's Algorithm

- 7 x 13 mod 15
  - Link Ch 14e

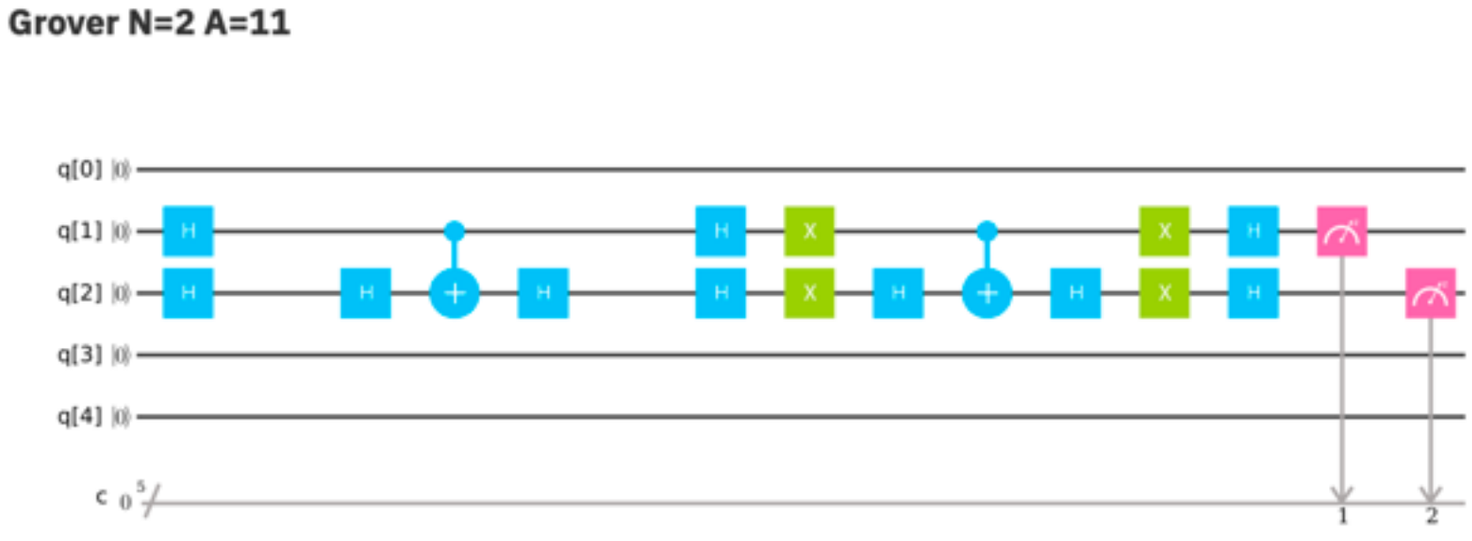


# Breaking AES-128

- Brute-force search
  - Try all $\mathbf{2^{128}}$ possible keys
  - Classical: requires $\mathbf{2^{128}/2}$ calculations
- Grover's algorithm
  - Quantum: requires $\mathbf{2^{64}}$ calculations

# Grover's Algorithm

- Can break symmetric encryption and reverse hashes
- Requires $\mathbf{2^{n/2}}$ calculations



# Double Key Length

- Even with a quantum computer, breaking AES-256 or SHA-256
  - Requires $\mathbf{2^{128}}$ calculations

# Why Is It So Hard to Build a Quantum Computer?

# Noise

- Google and IBM form Qubits are formed from ***superconducting circuits***
  - Must be cooled to extremely low temperatures
  - Only stable for a few milliseconds
- Another method uses ***ion traps***

ionq.co

IONQ

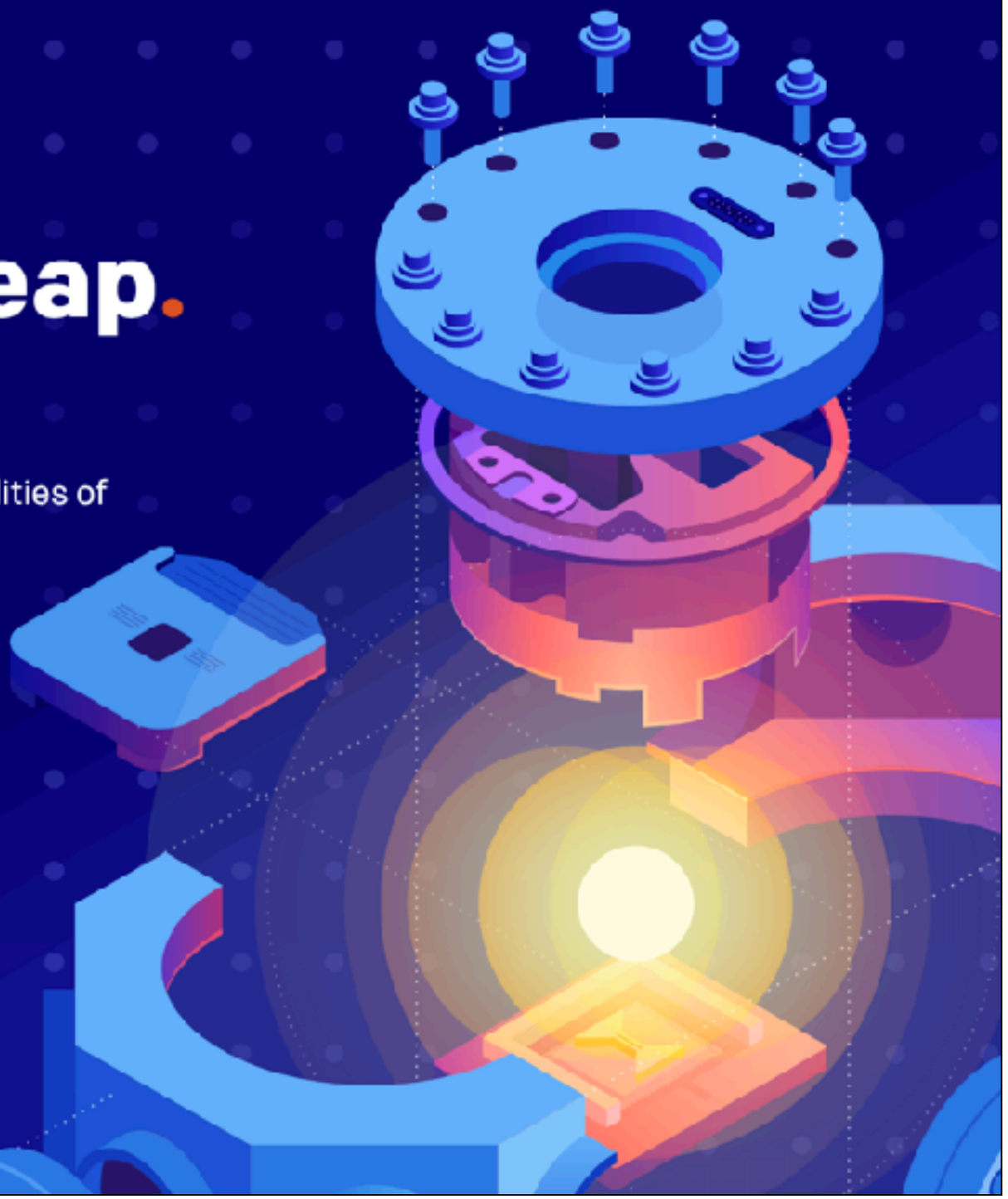
Company Resources Request Access

NEW IonQ publishes new benchmarks for quantum computation ▸

# A true quantum leap.

Introducing the first commercial trapped ion quantum computer. By manipulating individual atoms, it has the potential to one day solve problems beyond the capabilities of even the largest supercomputers.

Request Access



## The World's Most Advanced Quantum Computer

Our quantum cores use lasers pointed at individual atoms to perform longer, more sophisticated calculations with fewer errors than any quantum computer yet built. In 2019, leading companies will start investigating real-world problems in chemistry, medicine, finance, logistics, and more using our systems.

### Powerful

Program length:

**>60** two-qubit gates

what does this mean?

### Connected

Fully-connected qubits: **11**

Addressable pairs: **55**

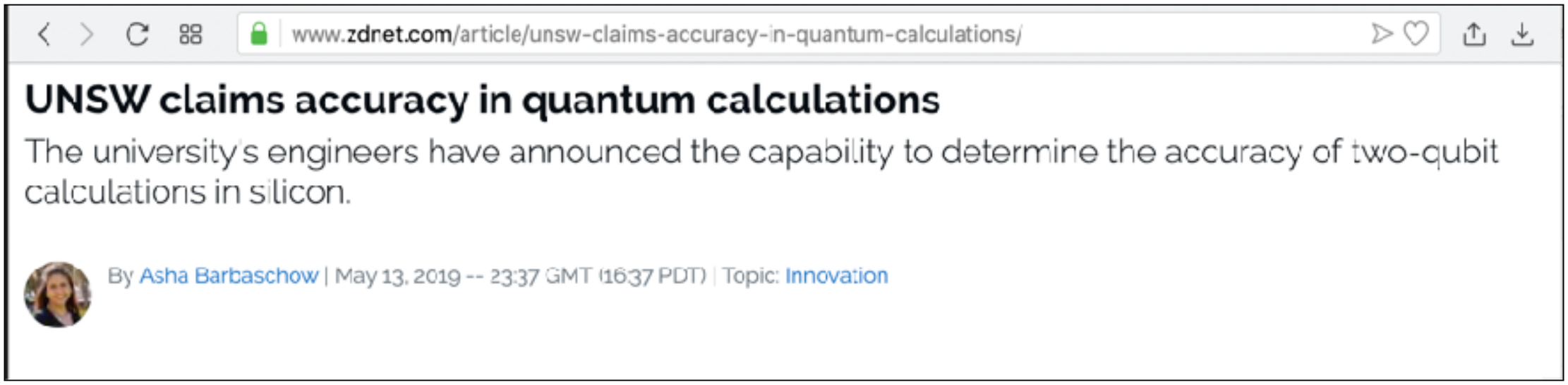
what does this mean?

### Precise

One-qubit gate error: **<0.03%**

Two-qubit gate error: **<1.0%**

what does this mean?




UNSW's approach has been to focus on making qubits out of single atoms of phosphorus or quantum dots in silicon -- the material that forms the basis of today's computer chips.

The university said that in conducting its study, the team implemented and performed Clifford-based fidelity benchmarking, which is a technique assesses qubit accuracy across all technology platforms. The benchmarking outcome resulted in an average two-qubit gate fidelity of 98%.

3 Mar 2016 | 19:03 GMT

# Quantum Computer Comes Closer to Cracking RSA Encryption

## Shor's algorithm performed in a system less than half the size experts expected

Though a functional quantum computer of the necessary size to crack RSA encryption is still far off in the future, the threat that such a computer poses still resonates among digital security experts. In January, the U.S. National Security Agency posted a FAQ on the risks.

"I think people are starting to get freaked out about it," Green says. "They still think it's anywhere from 15 to 30 years away but data can last a very long time. The good news is most of the data we had doesn't have to be kept secure for 30 years, but some of it does."

# Post-Quantum Cryptographic Algorithms

# A Different Hard Problem

- Can't be based on the Discrete Logarithm Problem
- Four types
  - Code-Based
  - Lattice-Based
  - Multivariate
  - Hash-Based

# Code-Based

- Based on ***error-correcting codes***
- First one: ***McEliece*** developed in 1978
  - Still unbroken
- Can be used for encryption and signatures
- Public key is 100 KB in size

# Error-Correcting Code

- You want to send a three-bit message **010**
  - Over a noisy channel
- One method: send every bit three times
  - **000111000**
- If a single bit is wrong, the other two will outvote it
  - But if two errors occur the system fails

# Linear Codes

- Word contains ***n*** bits
  - Treat it as a vector ***v***
  - Multiply the word by a matrix ***G***
  - To form code word ***w = vG***
- Can correct multi-bit errors

# McEleice Encryption

- ***G*** is a secret combination of three matrices
  - ***G = ABC***
- Encryption is ***w = vG + e***
  - ***e*** is a random error bit
  - ***G*** is the pubic key
  - ***A B C*** are the private keys

# McEleice Encryption

- Relies on the hardness of decoding a linear code with insufficient information
- Known to be NP-complete
- Beyond the reach of quantum computers

# Lattice-Based

- A ***Lattice*** is a set of points with a periodic structure

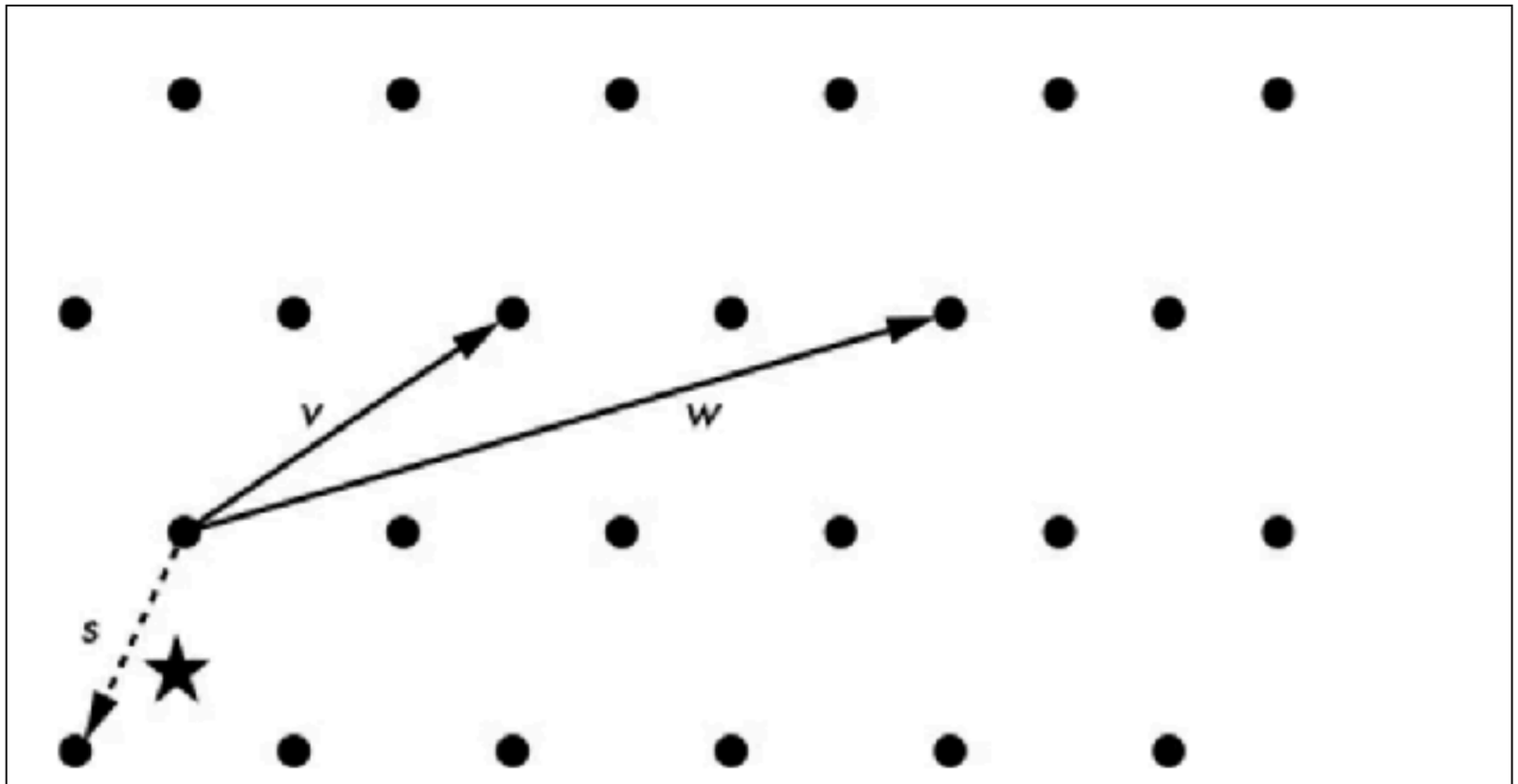



*Figure 14-5: Points of a two-dimensional lattice, where* v *and* w *are basis vectors of the lattice, and* s *is the closest vector to the star-shaped point*

# Closest Vector Problem (CVP)

- Problem: Combine basis vectors to find the lattice point closest to a point

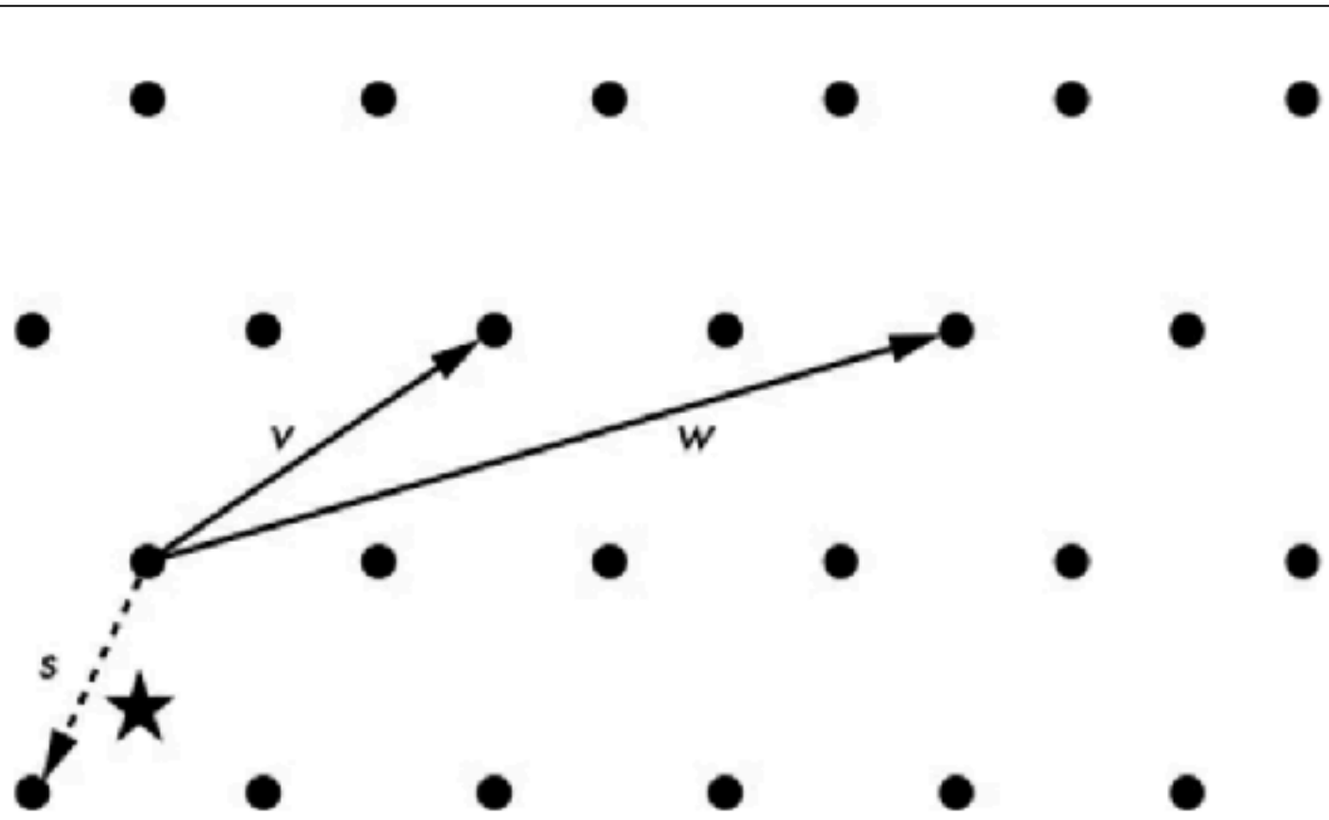



*Figure 14-5: Points of a two-dimensional lattice, where* v *and* w *are basis vectors of the lattice, and* s *is the closest vector to the star-shaped point*

# Short Integer Solution (SIS)

- ***A*** is a random matrix
- ***q*** is a prime number
  - ***b*** is a vector
- Problem: Given ***A*** and ***b***
- Find a secret vector ***s*** such that

  $$\boldsymbol{b = As \bmod q}$$

# Learning With Errors (LWE)

- Problem: Given $\boldsymbol{A}$ and $\boldsymbol{b}$
- Find a secret vector $\boldsymbol{s}$ such that

$$\boldsymbol{b} = \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e} \bmod q$$

- $\boldsymbol{e}$ is a random vector of noise

# Lattice-Based Cryptography

- These three problems are somewhat equivalent
- Believed to be hard for both classical and quantum computers
- But perhaps only in the hardest cases
- And finding approximate solutions might be easier

# Multivariate

- Four unknowns, and four random quadratic equations
- Solving this may be a hard problem

$$x_1x_2 + x_3x_4 + x_2 = 1$$

$$x_1x_3 + x_1x_4 + x_2x_3 = 12$$

$$x_1^2 + x_3^2 + x_4 = 4$$

$$x_2x_3 + x_2x_4 + x_1 + x_4 = 0$$

# Multivariate Limitations

- Actual hardness depends on the parameters
  - Number of equations
  - Size and type of numbers
  - Choosing secure parameters is hard
  - More than one multivariate scheme has been broken

# Multivariate Limitations

- Not used in major apps
  - Concerns about security
  - Often slow or requires tons of memory
- Benefit: produces short signatures

# Hash-Based

- Based on difficulty of finding hash collisions
  - Quantum computers cannot break hash functions
- Hash-based cryptographic schemes are complex

# Winternitz One-Time Signature (WOTS)

- Private key can be used only once
  - To sign one message
- Message ***M*** is a number from **0** to ***w* - 1**
  - ***w*** is a parameter of the scheme
  - ***K*** is the private key
- Signature is formed by hashing ***K*** with ***M*** rounds

  **Hash(Hash(Hash( ... Hash(*K*) ... ))**
- Public key is formed by hashing **K** with ***w*** rounds

# WOTS Limitations

- **Signatures can be forged**
  - Hash the signature of ***M*** to create the signature of ***M* + 1**

# WOTS Limitations

- **Only works for short messages**
  - If message has 8 bits, you must calculate
    - $2^8 - 1 = 255$ rounds of hashing
  - If message has 128 bits
    - $2^{128} - 1$ rounds of hashing
  - Must break long messages into several smaller ones

# WOTS Limitations

- **Only works once**
  - If a private key is used twice
  - Attacker can combine those signatures to forge other messages
  - There is no simple way to fix this problem

# Hash-Based Schemes

- State-of-the-art schemes use more complex versions of WOTS
  - With tree data structures
  - And sophisticated techniques to sign different messages with different keys
- SPHINCS is a state-of-the-art scheme
  - Signatures are dozens of KB long

# How Things Can Go Wrong

# Unclear Security Level

- Security proofs are often ***asymptotic***
  - Only true for large values of parameters
    - Such as the dimension of the lattice
- In practice, smaller values are used
- Difficult to quantify the level of security
- Attacks on new schemes, like lattices, are not well understood

# Too Late?

- Post-quantum encryption is more important than post-quantum signatures
  - Signatures can be revoked & replaced
    - Old encrypted data can be archived and broken years later
- In practice, Diffie-Hellman often uses more than the shared secret to form the session key
  - Safer against quantum computers

# Implementation Issues

- Some post-quantum encryption implementations have been optimized for speed
  - And are vulnerable to timing attacks
- Post-quantum algorithms will be less secure than older algorithms at first

NISTIR 8309

# Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process

- Began in 2016
- Plan: standard will be chosen in 2022
  - https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8309.pdf

**Table 2: Second-Round Candidates**

| | | |
|---|---|---|
| BIKE | LEDAcrypt | Rainbow |
| Classic McEliece | LUOV | ROLLO |
| CRYSTALS-DILITHIUM | MQDSS | Round5 |
| CRYSTALS-KYBER | NewHope | RQC |
| FALCON | NTRU | SABER |
| FrodoKEM | NTRU Prime | SIKE |
| GeMSS | NTS-KEM | SPHINCS+ |
| HQC | Picnic | Three Bears |
| LAC | qTESLA | |

**Table 3: Third-Round Finalists**

| Public-Key Encryption/KEMs | Digital Signatures |
|---|---|
| Classic McEliece | CRYSTALS-DILITHIUM |
| CRYSTALS-KYBER | FALCON |
| NTRU | Rainbow |
| SABER | |

**Table 4: Alternate Candidates**

| Public-Key Encryption/KEMs | Digital Signatures |
|---|---|
| BIKE | GeMSS |
| FrodoKEM | Picnic |
| HQC | SPHINCS+ |
| NTRU Prime | |
| SIKE | |


Kahoot!