
black hat
MIDDLE EAST AND AFRICA
Quantum Computing, Is it breaking Encryption ?
15 – 17 NOVEMBER 2022
RIYADH FRONT EXHIBITION CENTRE
SAUDI ARABIA
Abdulrahman Al-Nimari, VP, Cybersecurity
STRATEGIC SPONSORS
GOLD SPONSORS
CO-ORGANISED BY
SPIRE
INFORMATION. SECURED.
IBM
Infoblox
Honeywell
informatech
الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز
SAUDI FEDERATION FOR CYBERSECURITY, PROGRAMMING & DRONES

Who Am I ?

- ✓ Abdulrahman Al-Nimari
- ✓ Cyber Security Advisor
- ✓ 25 Years IT & Cyber Security Experience
- ✓ Speaker : BSides, HITB, ICSC, AECT, ASC, MENA ISC, GISEC, BHME
- ✓ Awarded Arab Cybersecurity Social Network Influencer Prize 2019 - 2022
- ✓ Awarded IFSEC Global Influencers in Cyber Security 2022
- ✓ CISSP, CISM, CCISO, PMP, GCIH, GCIA, GCUX, GICSP, GREM, GSEC
- ✓ @nimari
- ✓ https://www.linkedin.com/in/alnimari/
- ✓ alnimari@gmail.com
- ✓ +966 (566) 465270

Disclaimer

"I am not in anyway an expert of Quantum Physics or Quantum Computing"

A Quantum Computer

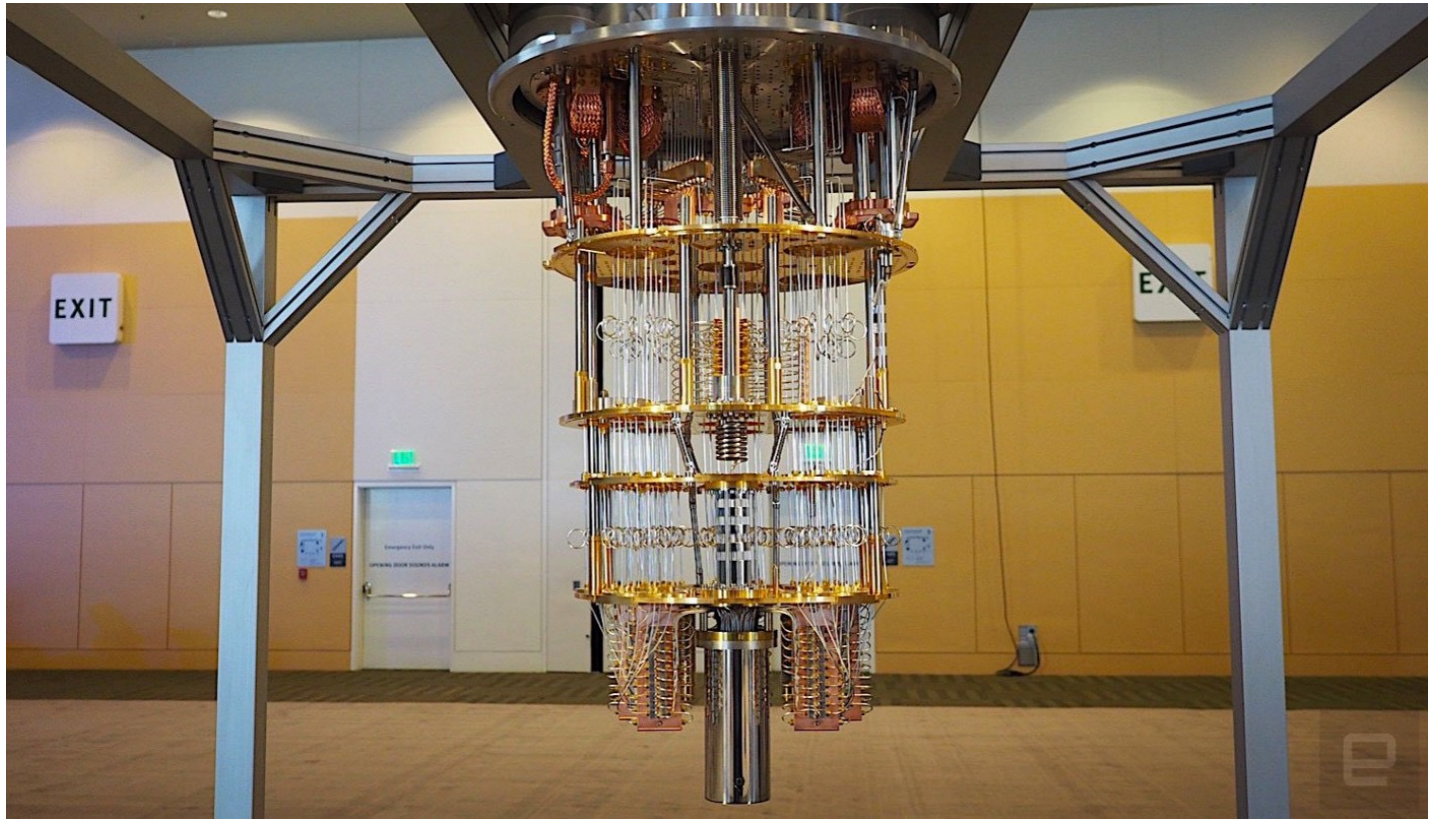
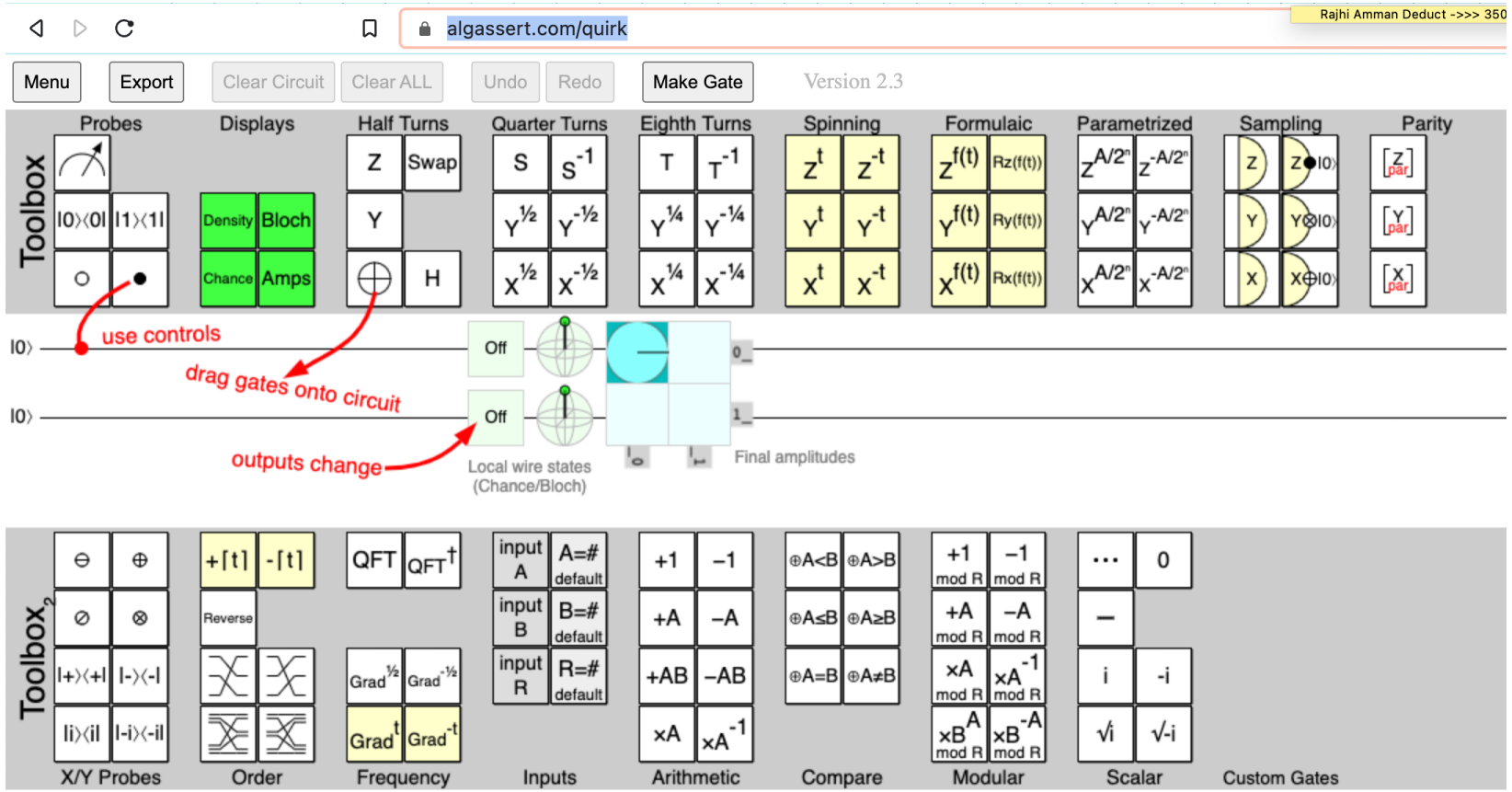


Image of IBM’s quantum computer.

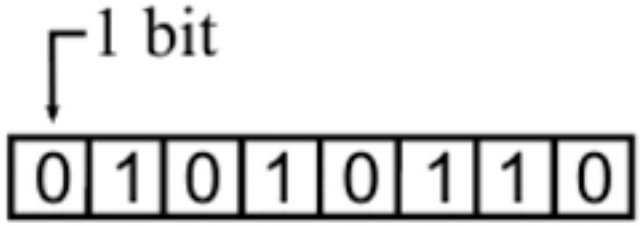
Quantum Computing Race – Investments 10.7 Billion US$ by 2024

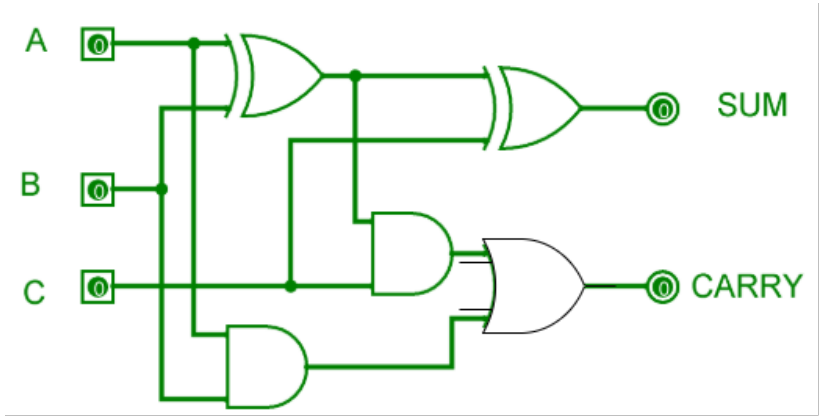
Quantum Simulator



https://algassert.com/quirk

Bits





A 065 01000001

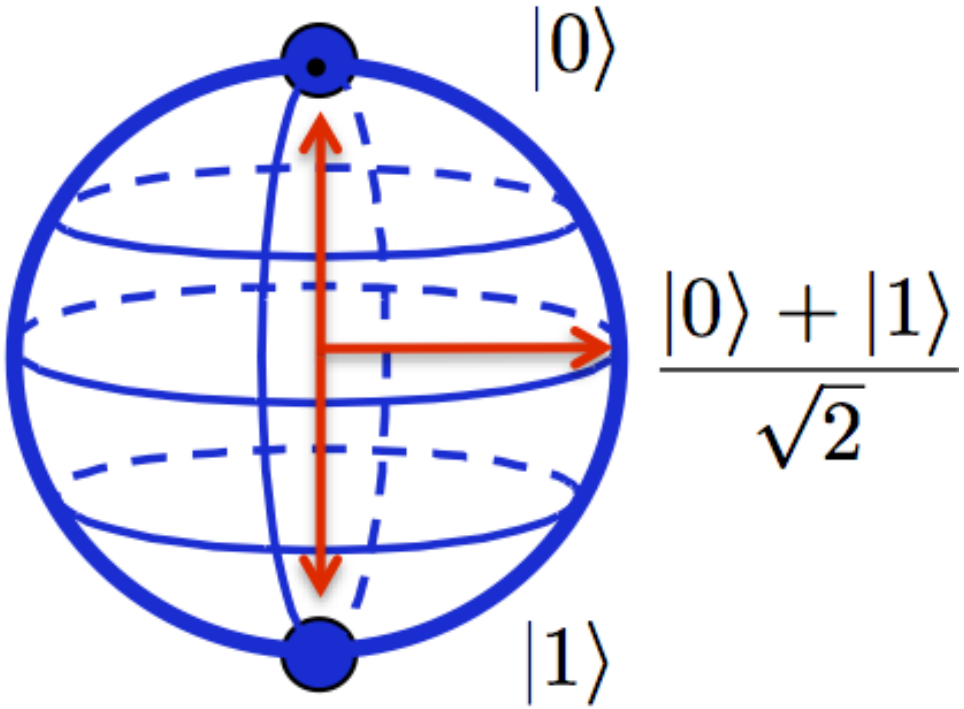
Bits vs Qubits

Bit

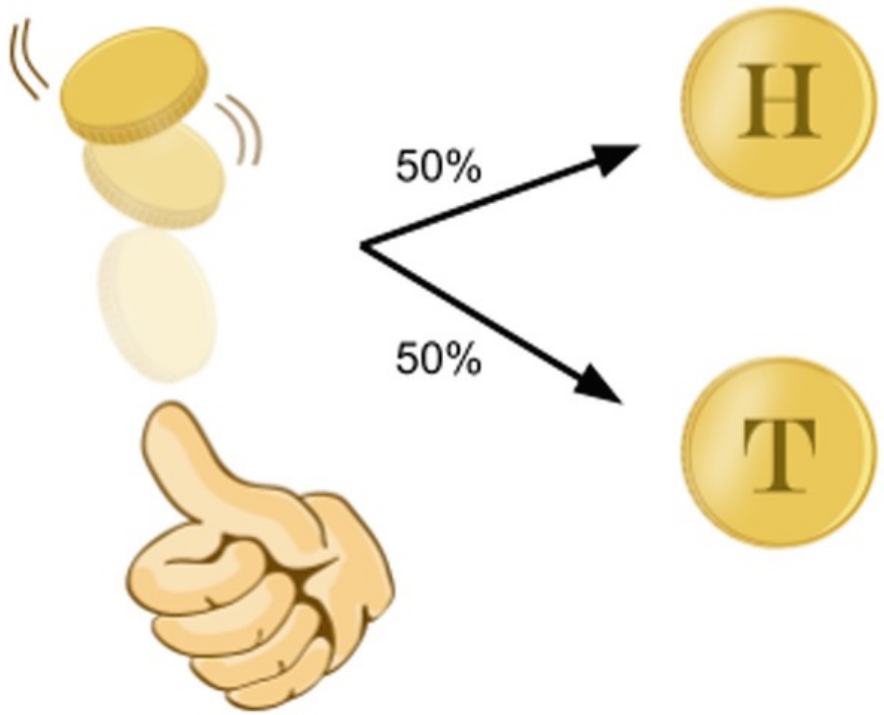
0

1

Qubit

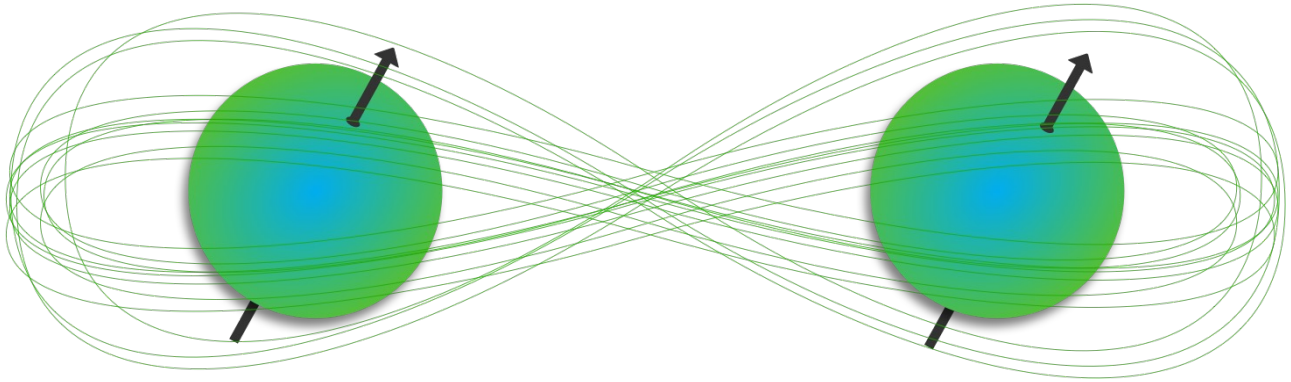


Superposition



Being in more than one state at the same time

Entanglement

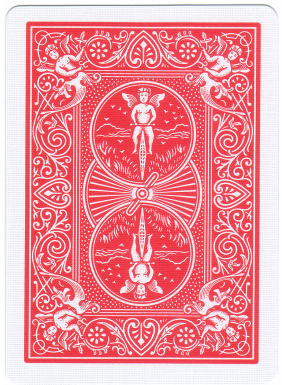
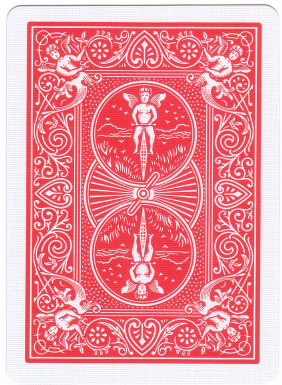
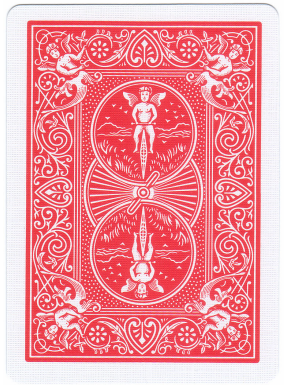
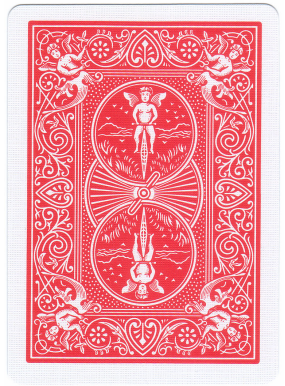


Entanglment is the Interaction and Connection of Two Particles

Cards Game – Find the Queen





Exponential

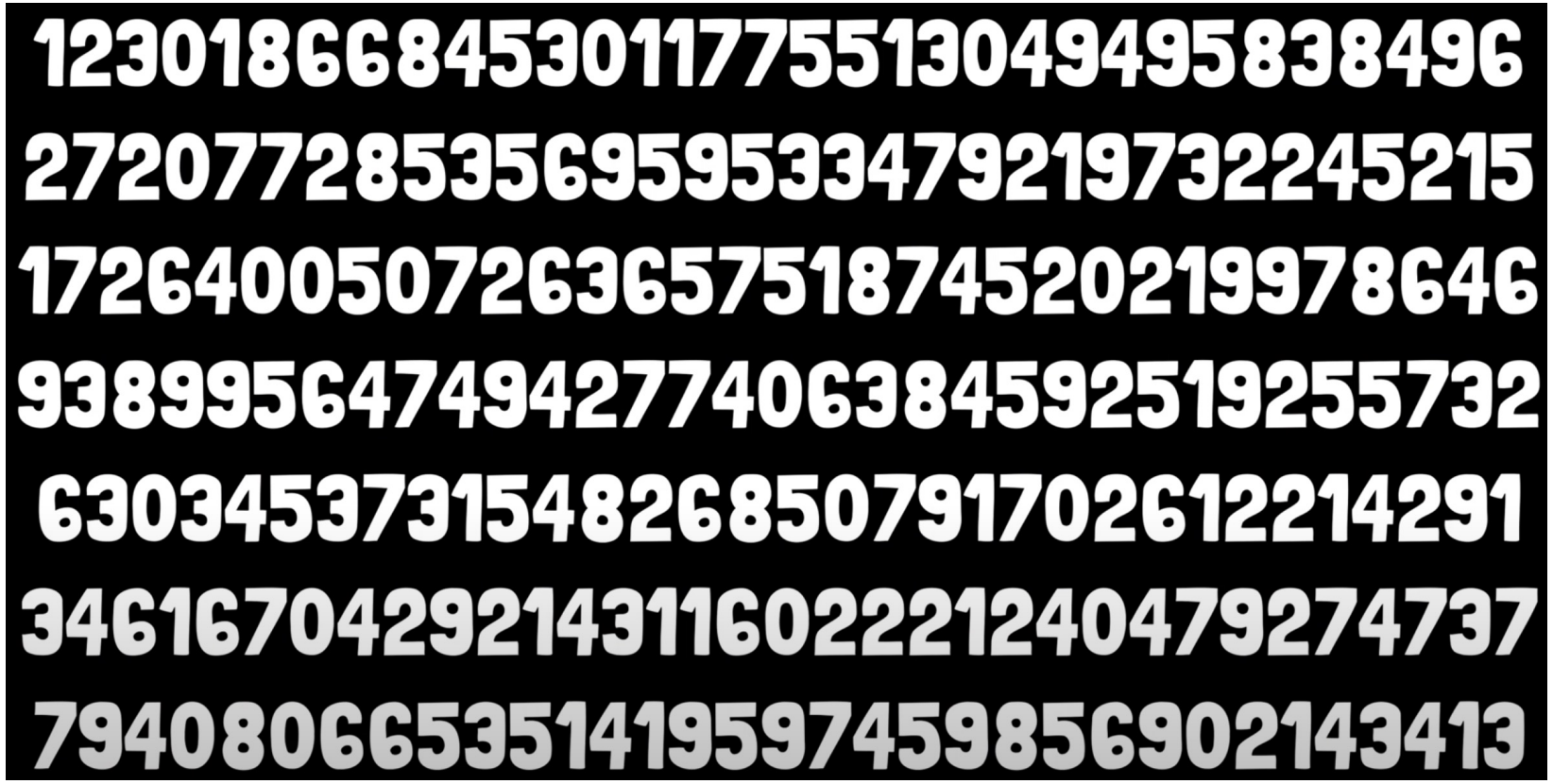
Factoring a Number into Primes

$$M = p * q$$

$$15 = 3 * 5$$

M = Large Integer
p = Prime Number
q = Prime Number

Factoring a Number into Primes



Factoring a Number into Primes

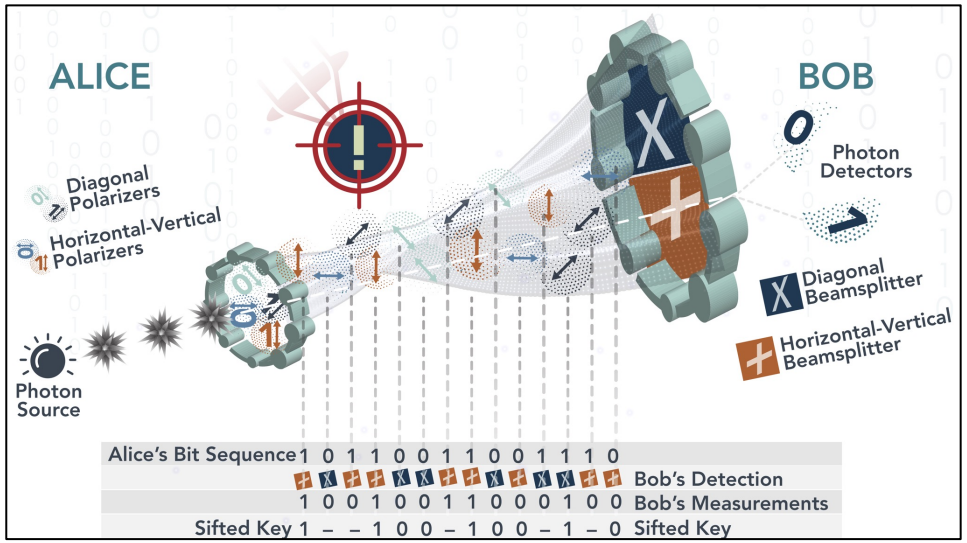
Classical Computer: 28,000,000,000,000,000,000,000 years

Quantum Computer: 100 seconds

Factoring requires **millions** of fault tolerant, **error corrected** Qubits which are decades away from us

Post Quantum Cryptography Algorithms

- ✓ CRYSTALS-Kyber
- ✓ CRYSTALS-Dilithium
- ✓ FALCON
- ✓ SPHINCS+



https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

Some Quantum Use Cases

- ✓ Artificial Intelligence & Machine Learning
- ✓ Pharmaceutical
- ✓ Chemistry
- ✓ …

Myths About Quantum Computing

- ✓ Quantum Computing will mean the end of normal computing
- ✓ Quantum Computing can run programming codes similar to classical computers
- ✓ Quantum Computing will destroy cybersecurity.
- ✓ Quantum Computing will be commercially available in 15 years.

Thank You