



Quantum Computing, Is it breaking Encryption ?

15 – 17 NOVEMBER 2022

RIYADH FRONT EXHIBITION CENTRE
SAUDI ARABIA

Abdulrahman Al-Nimari, VP, Cybersecurity

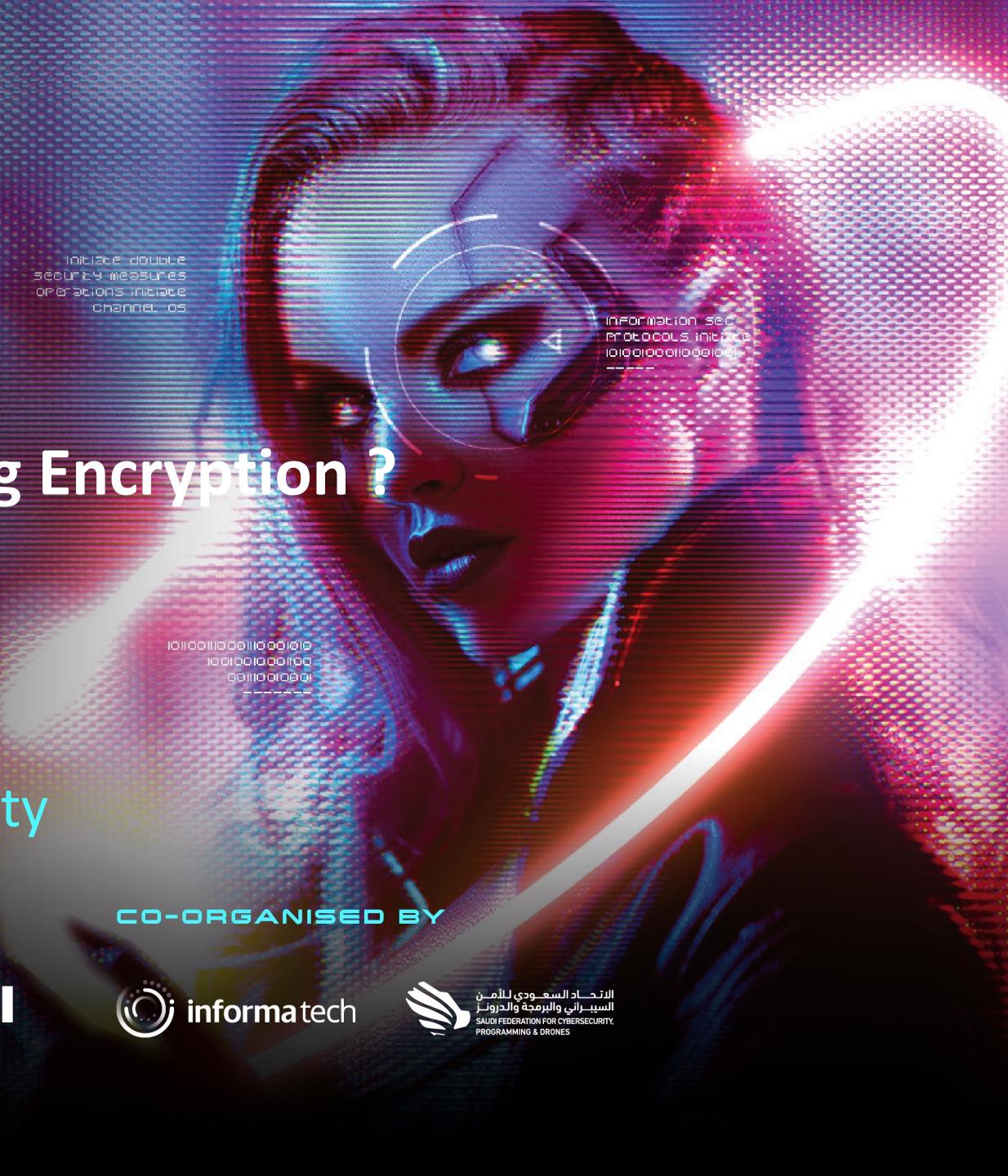
STRATEGIC SPONSORS



GOLD SPONSORS



CO-ORGANISED BY



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

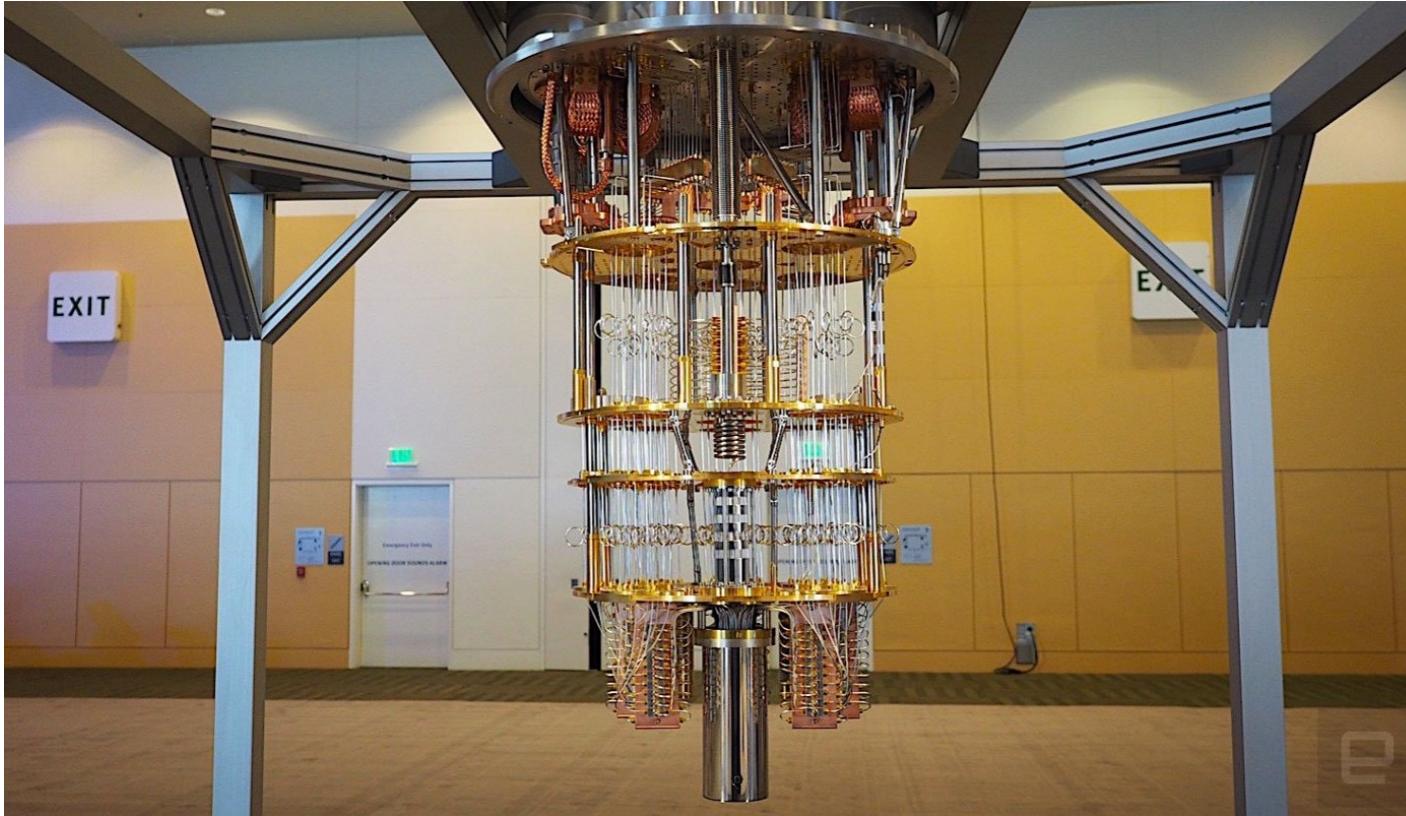


Image of IBM's quantum computer.

Quantum Computing Race – Investments 10.7 Billion US\$ by 2024



Quantum Simulator

Quantum Simulator interface showing a circuit diagram and two toolboxes.

Top Toolbox: A grid of quantum gates categorized by rotation type (Probes, Displays, Half Turns, Quarter Turns, Eighth Turns, Spinning, Formulaic, Parametrized, Sampling, Parity).

Circuit Diagram: A two-qubit circuit with controls and measurements.

- Top wire: $|0\rangle$ has controls (red arrows point to "use controls" and "drag gates onto circuit").
- Bottom wire: $|0\rangle$ has controls (red arrow points to "outputs change").
- Measurement: "Local wire states (Chance/Bloch)"
- Final amplitudes: "Off", "0", "1".

Bottom Toolbox: A grid of quantum operations categorized by type (X/Y Probes, Order, Frequency, Inputs, Arithmetic, Compare, Modular, Scalar, Custom Gates).

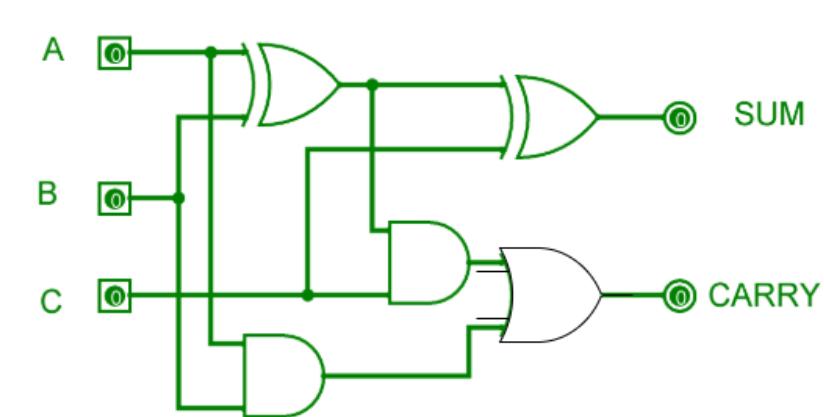
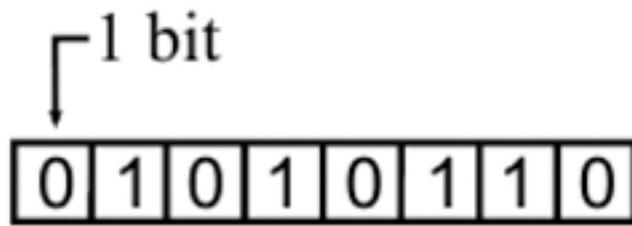
<https://algassert.com/quirk>

Bits

A

065

01000001



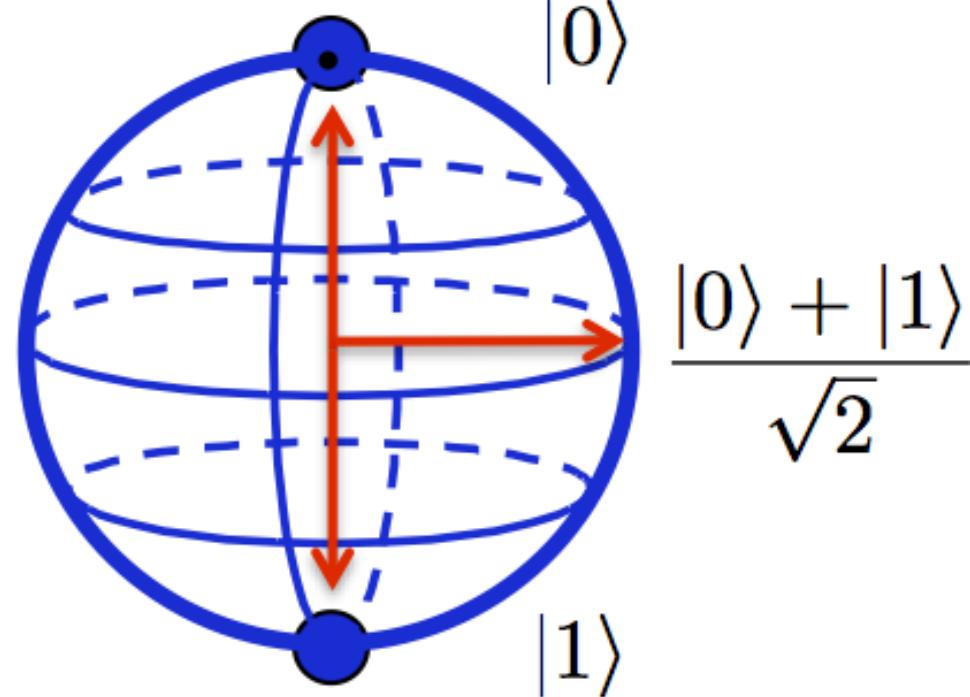
Bits vs Qubits

Bit

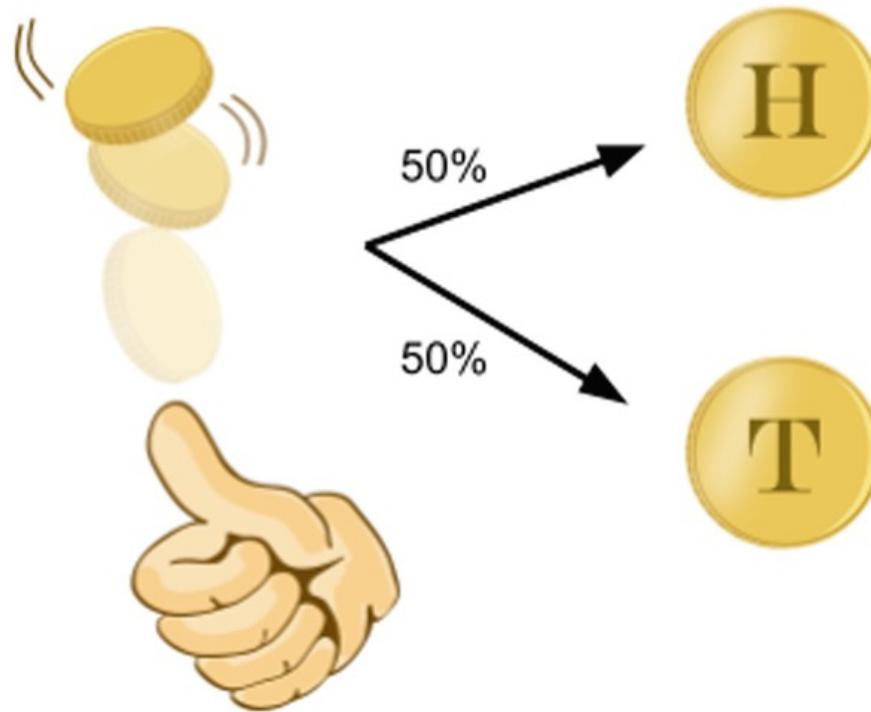
0

1

Qubit

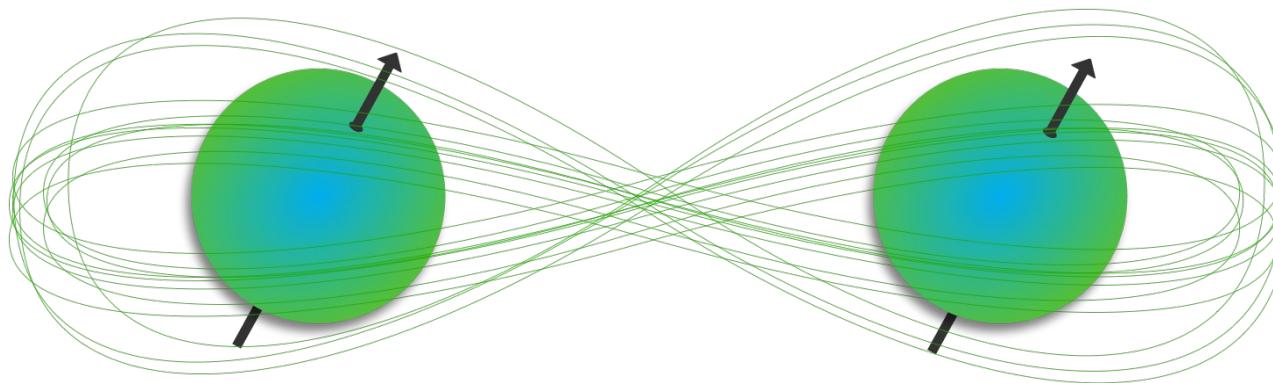


Superposition



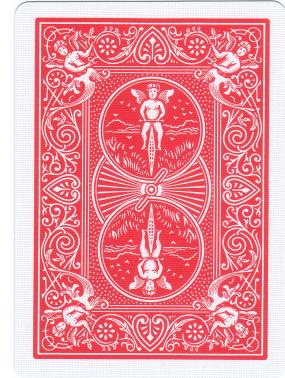
Being in more than one state at the same time

Entanglement



Entanglement 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

123018668453011775513049495838496
272077285356959533479219732245215
172640050726365751874520219978646
938995647494277406384592519255732
630345373154826850791702612214291
3461670429214311602221240479274737
794080665351419597459856902143413

Factoring a Number into Primes

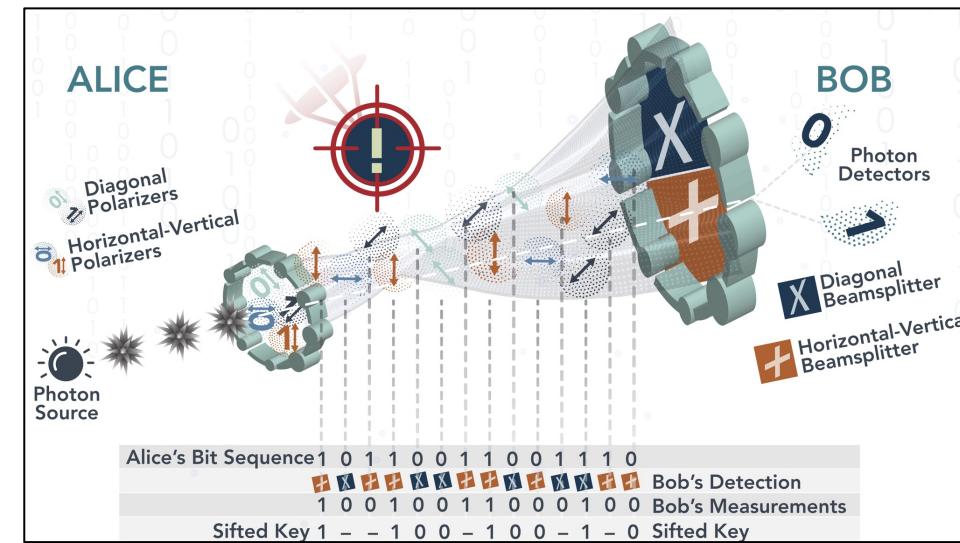
Classical Computer: 28,000,000,000,000,000,000 years

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