A presentation to
the IEEE Society of East Tennessee
on 17 November 2009

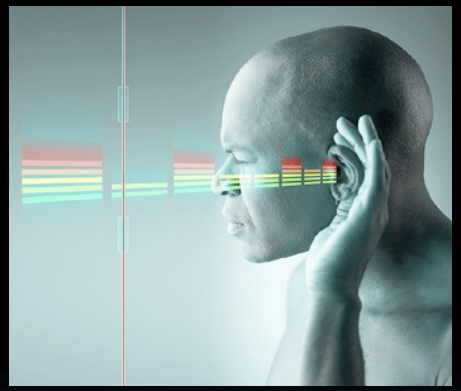
Travis S. Humble
Oak Ridge National Laboratory

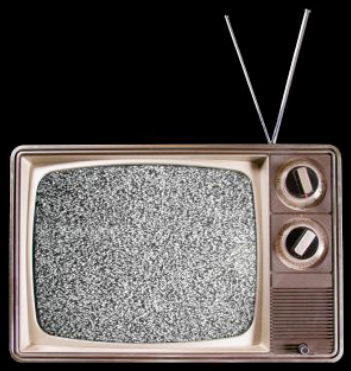
QUANTUM INFORMATION

Information is Physical

- Landauer's Principle

  Information is always encoded into mass and energy





Information processing is a physical transformation

Rolf Landauer (1927-1999), physicist

Information is Theoretical

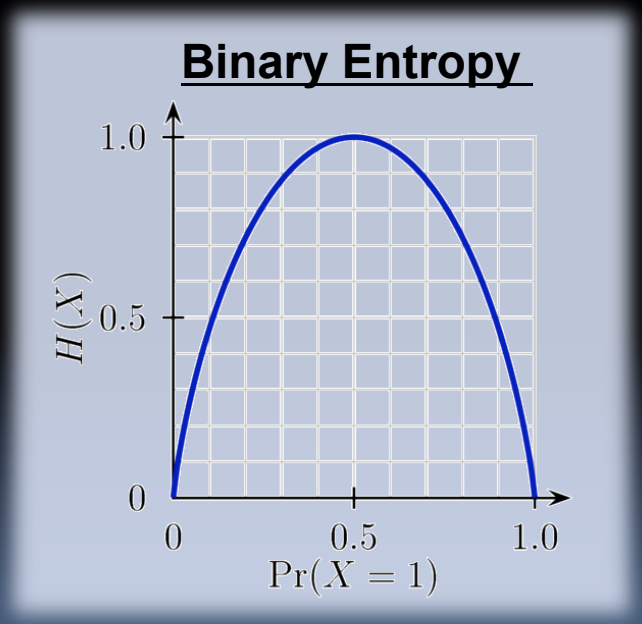
- Shannon's Theory

  Information can be mathematically quantified

  Size
  bit = binary digit (0 or 1)
  byte = 8 bits
  kilobyte = 1024 bytes

  Compression
  JPEG vs PNG

  Communication
  Cryptography
  Sensing

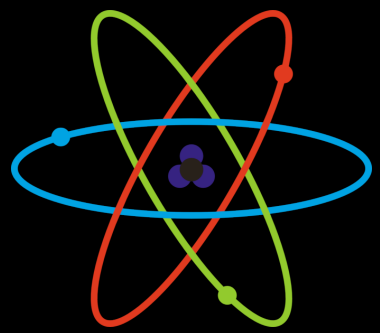


Claude Shannon (1916-2001), electrical engineer

It is Bit

- Wheeler

  "…all things physical are information-theoretic…"



Different information theories arise from different physics.

John Archibald Wheeler (1911-2008), physicist

A Tale of Two Theories

- Classical Information

  Encoded into a classical physical system, e.g., light, electricity, bulk matter

  Discrete logical values (bits) of 0 and 1

  Multiple bits are separable strings of bits.

  01001001 01000101 01000101 01000101

  I E E E

A Tale of Two Theories

- Quantum Information

  Encoded into a quantum physical system, e.g., photon, electron, atom

  Discrete logical basis of 0 and 1 provides for a continuum of possible logical values, e.g., 0 + 1 and 0 – 1

  Multiple qubits need not *be in separable states*

  00 11 00 + 11 00 – 11

QI FUNDAMENTALS

A qubit is a quantum bit

- a logical superposition state

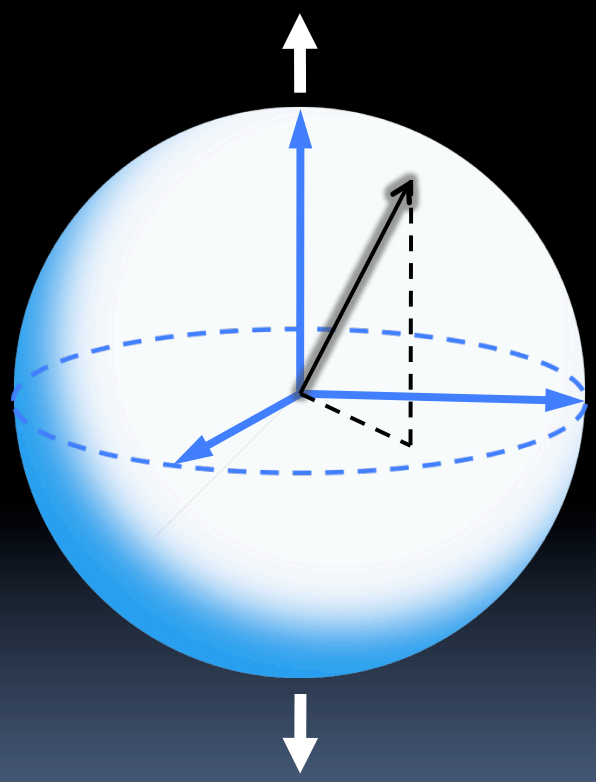
$$\psi = a\downarrow + b\uparrow$$

$$|a|^2 + |b|^2 = 1$$

- the quantum state of a quantum physical system

- a unit vector in Hilbert space, map onto the Bloch sphere

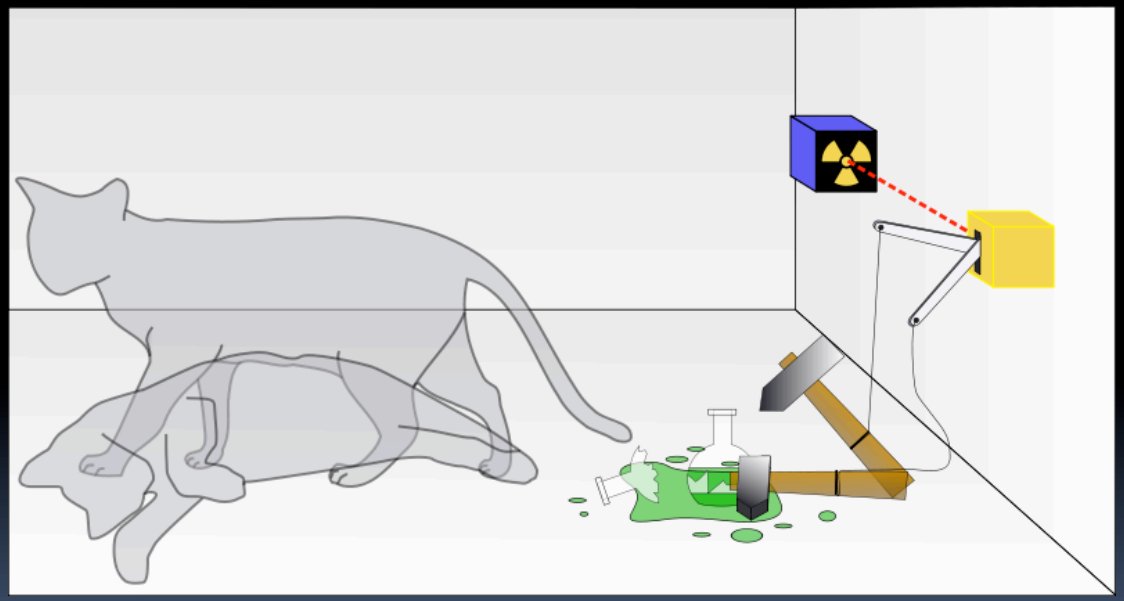
The Bloch Sphere



$a = \cos\theta \quad b = e^{i\phi}\sin\theta$

Schrödinger's Cat Paradox

A cat is killed when a vial of poison is triggered by the radioactive decay of an atom. However, the quantum state of the atom is a superposition of its stable and decayed forms, i.e., a qubit. Question: Is the cat alive or dead?



Erwin Schrödinger (1887-1961), physicist

Measuring a Quantum Universe

- The quantum state is not a physical observable; it is a statistical property of a quantum system.
- Measurements change the quantum state; these changes are irreversible.
- Measurement results are classical information that describe the statics of the quantum system.
- Each qubit reduces to one classical bit (Holevo Bound).

Entanglement

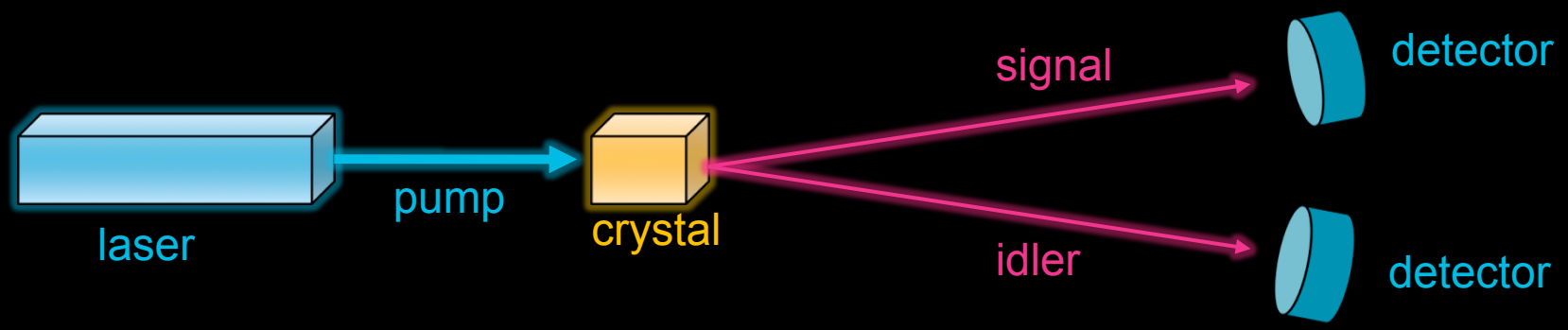
- a superposition of multiple logical states

$$\phi = a \downarrow\downarrow + b \uparrow\uparrow$$

- When particle one is $\downarrow$, then particle two is $\downarrow$
- Yet which one you get is completely random
- Bell's Theorem tests local hidden variable theories

Example of Entanglement

- *Spontaneous Parametric Down Conversion*
  one photon decays into a polarization entangled pair

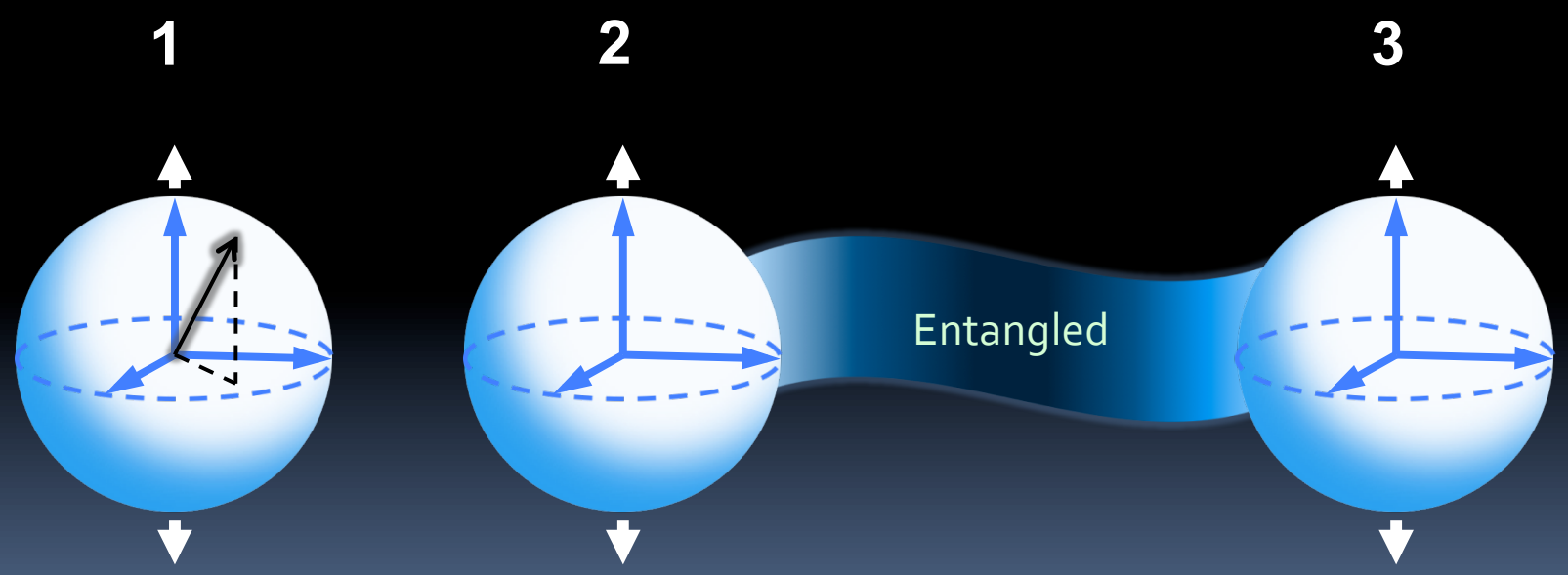


$$\phi \sim (h_s h_i + v_s v_i)$$

- Polarization correlations confirm Bell's theorem

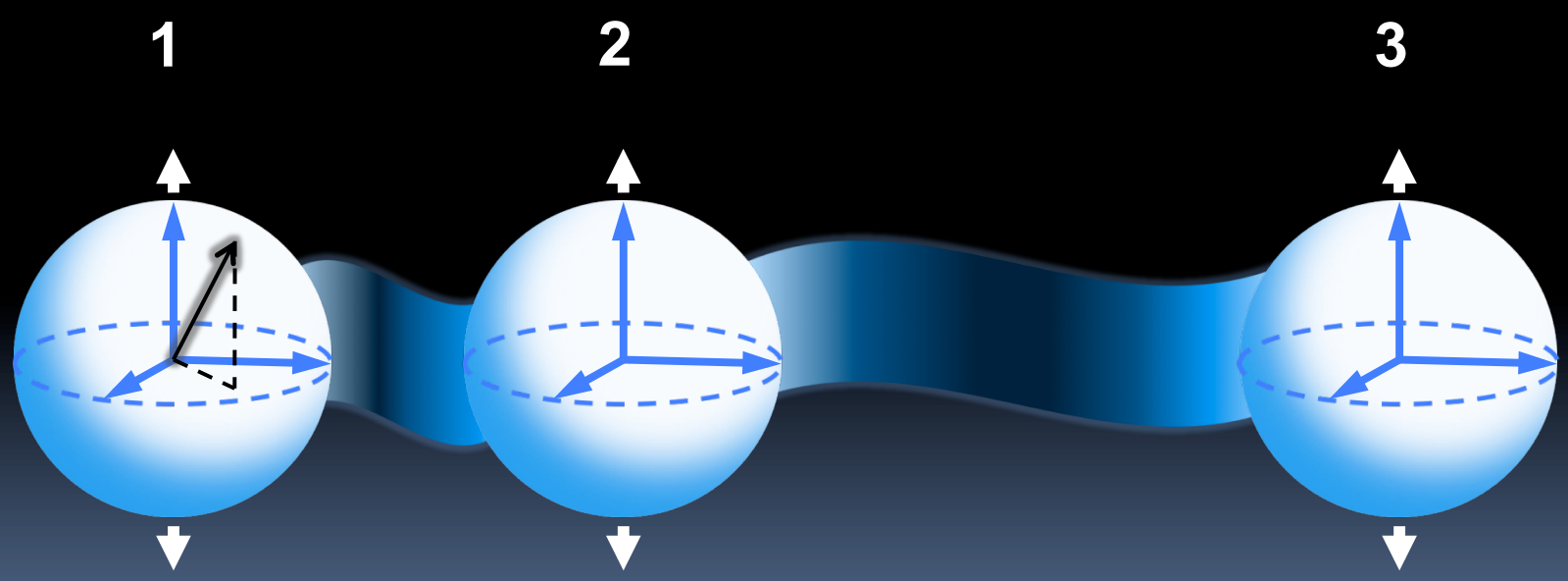
Quantum Teleportation

- Use entanglement to transfer a qubit from one particle to another, without the particles touching.



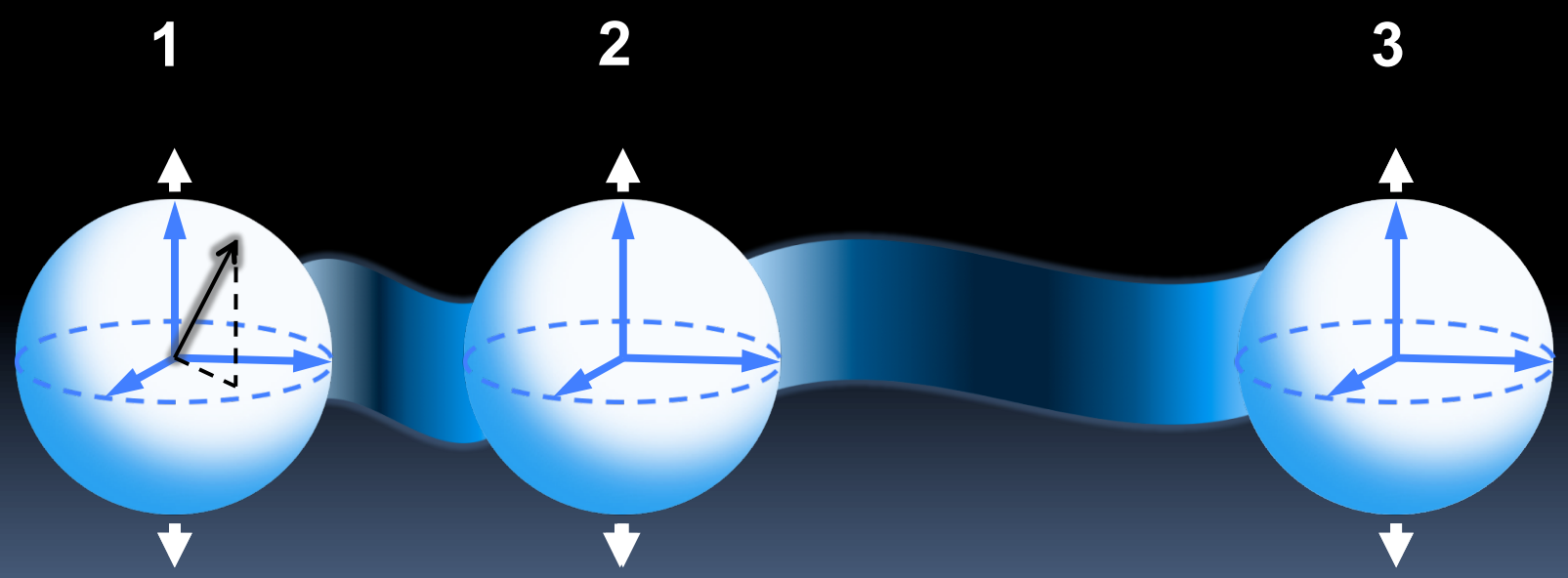
Quantum Teleportation

- Entangle particles 1 and 2



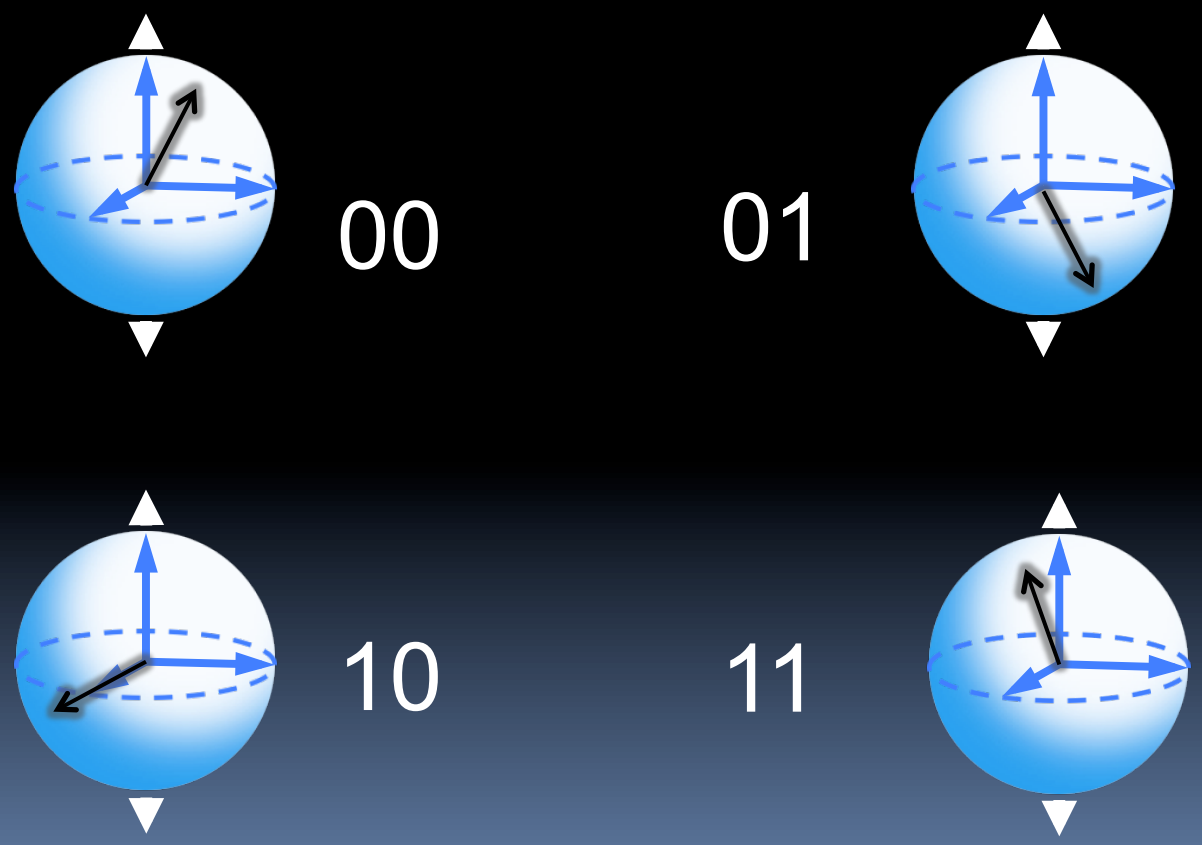
Quantum Teleportation

- Measure particles 1 and 2
- Generate classical information, e.g., 00



Quantum Teleportation

- The measurement reports the teleported state.



QI APPLICATIONS

Quantum Computing

- *Entanglement as computational parallelism*
  Deutsch (1985)

- A classical computation operating on *n* bits can be in one of 2^n possible logical states.

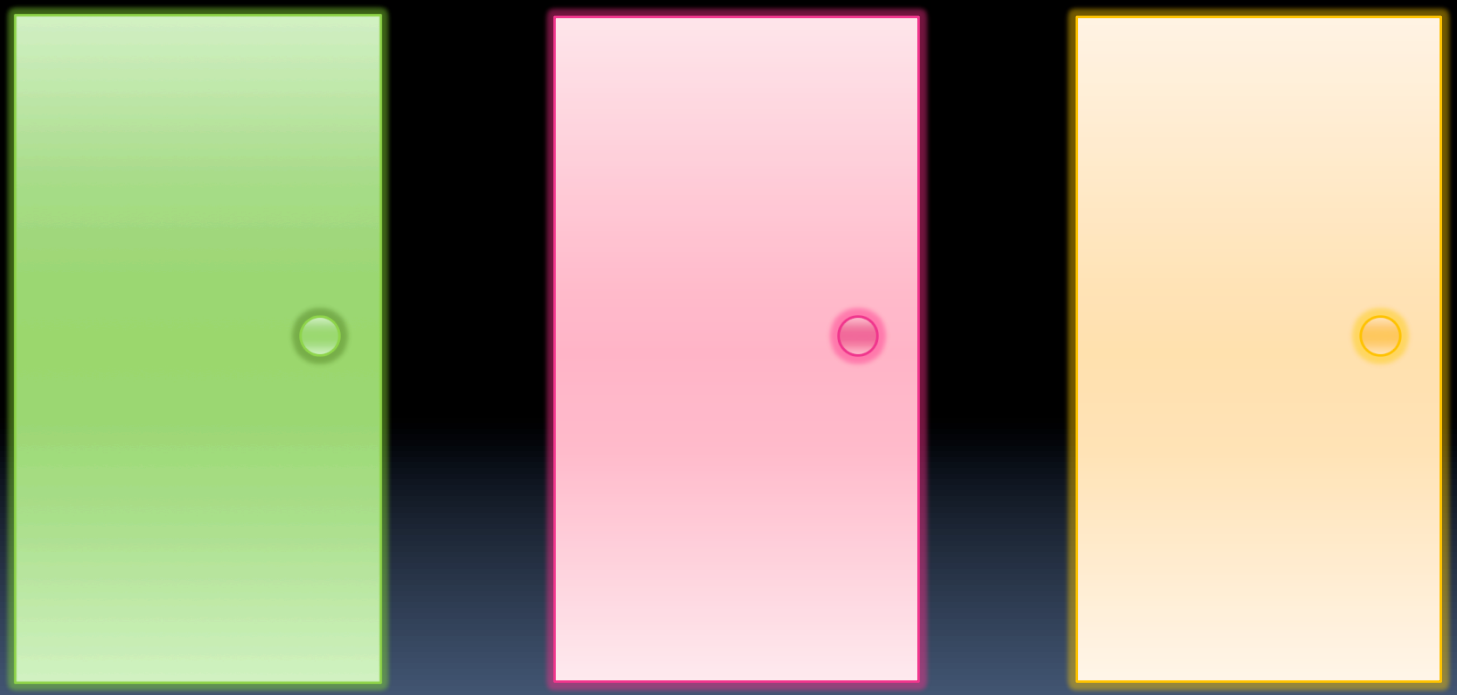
  000, 001, 010, 011, 100, 101, 110, 111

- A quantum computation operating on *n* qubits can be in all 2^n logical states *simultaneously*.

  000 + 001 + 010 + 011 + 100 + 101 + 110 + 111

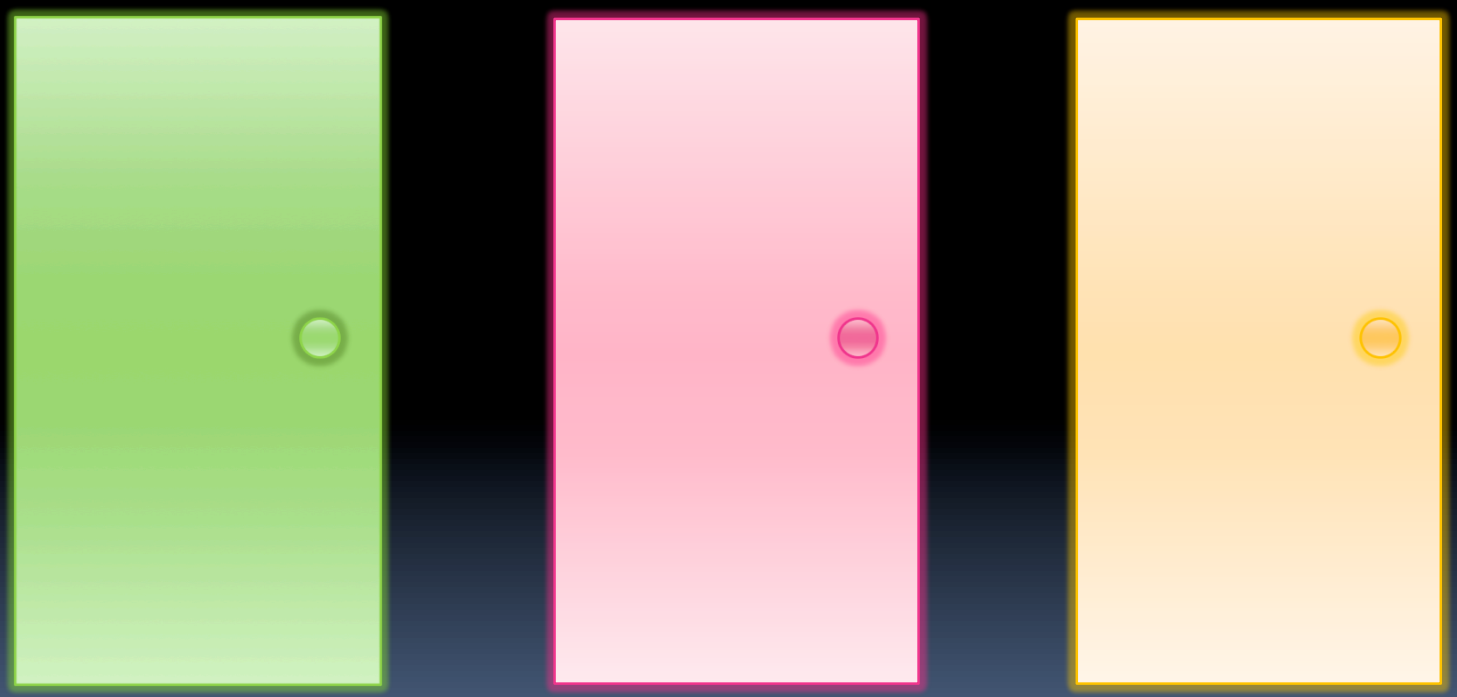
Quantum Computing

- Which door to choose?



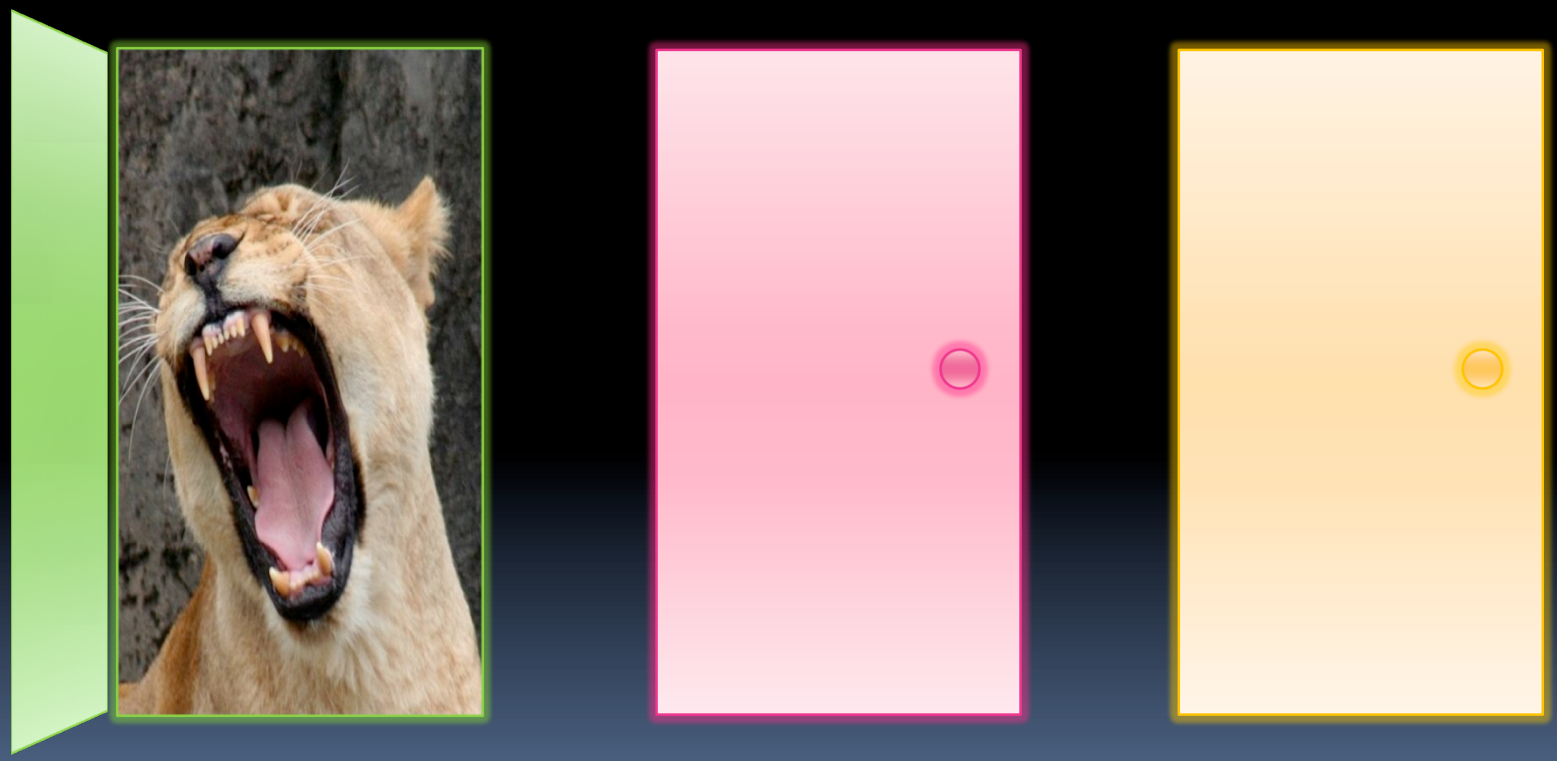
Quantum Computing

- A classical method samples each individually…



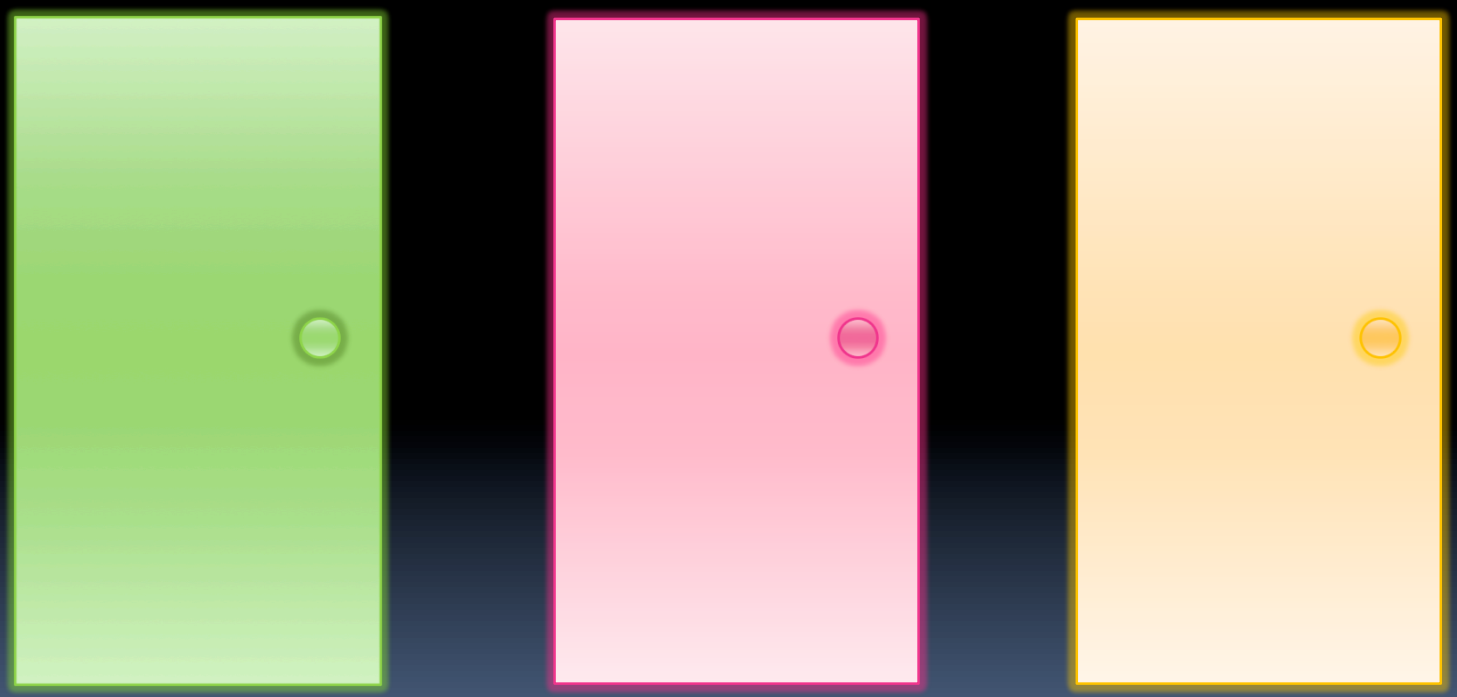
Quantum Computing

- A classical method samples each individually…



Quantum Computing

- A classical method samples each individually…

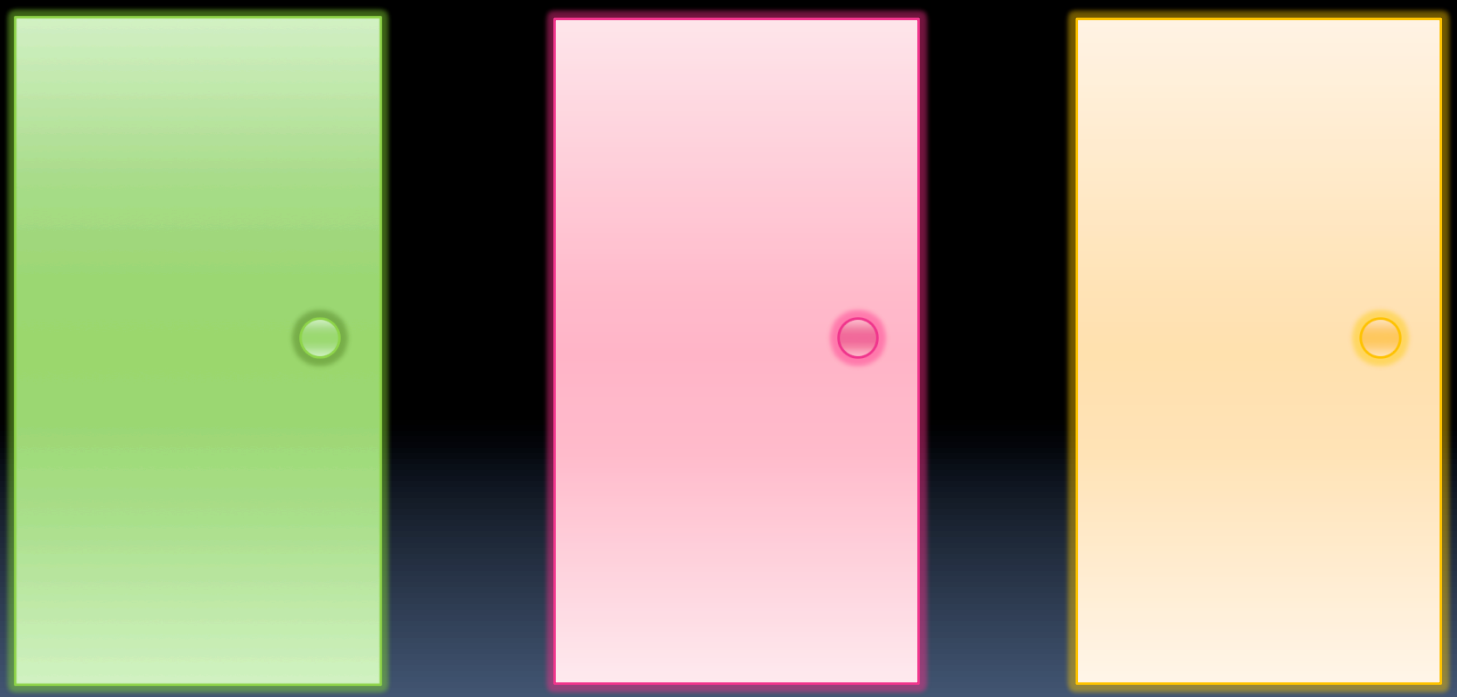


Quantum Computing

- A classical method samples each individually…

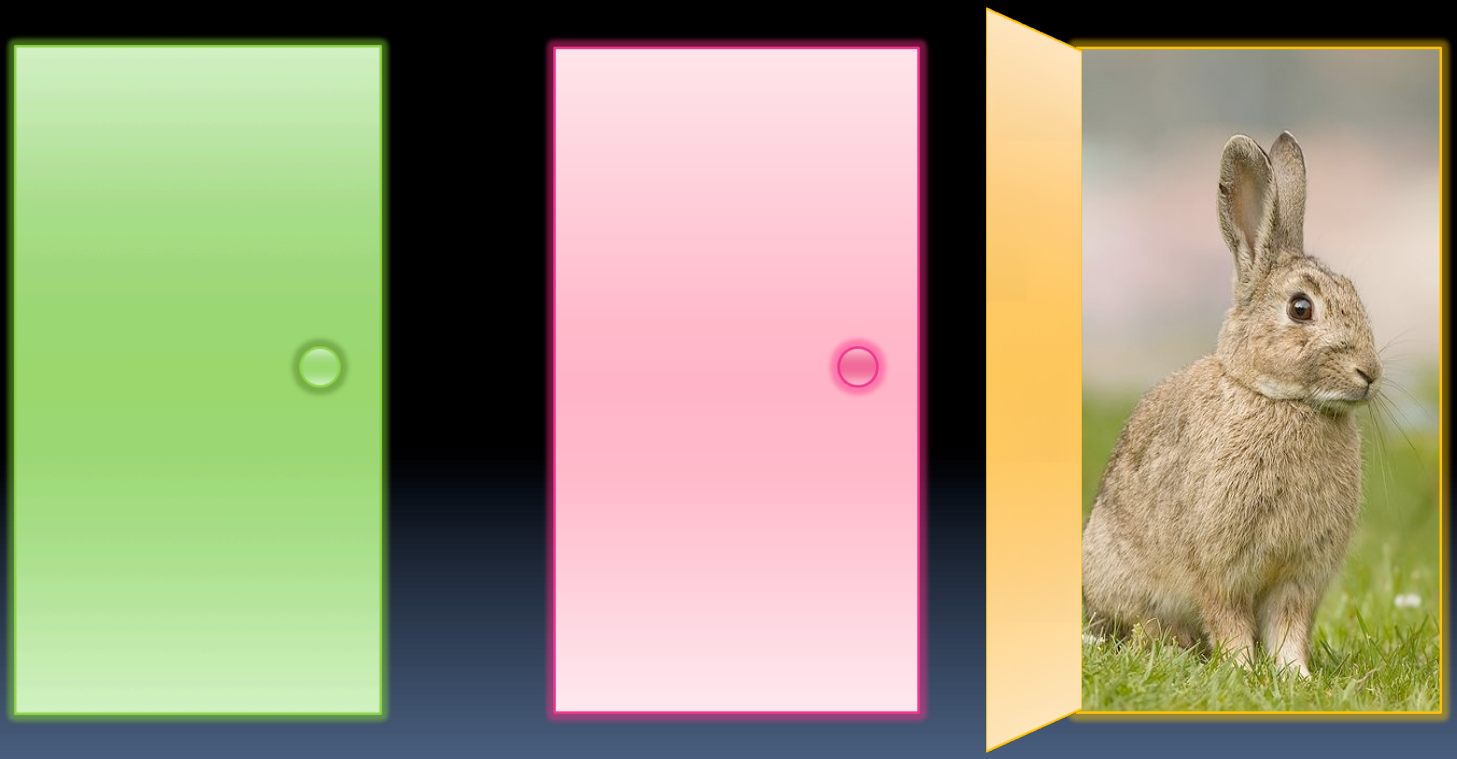
Quantum Computing

- A classical method samples each individually…



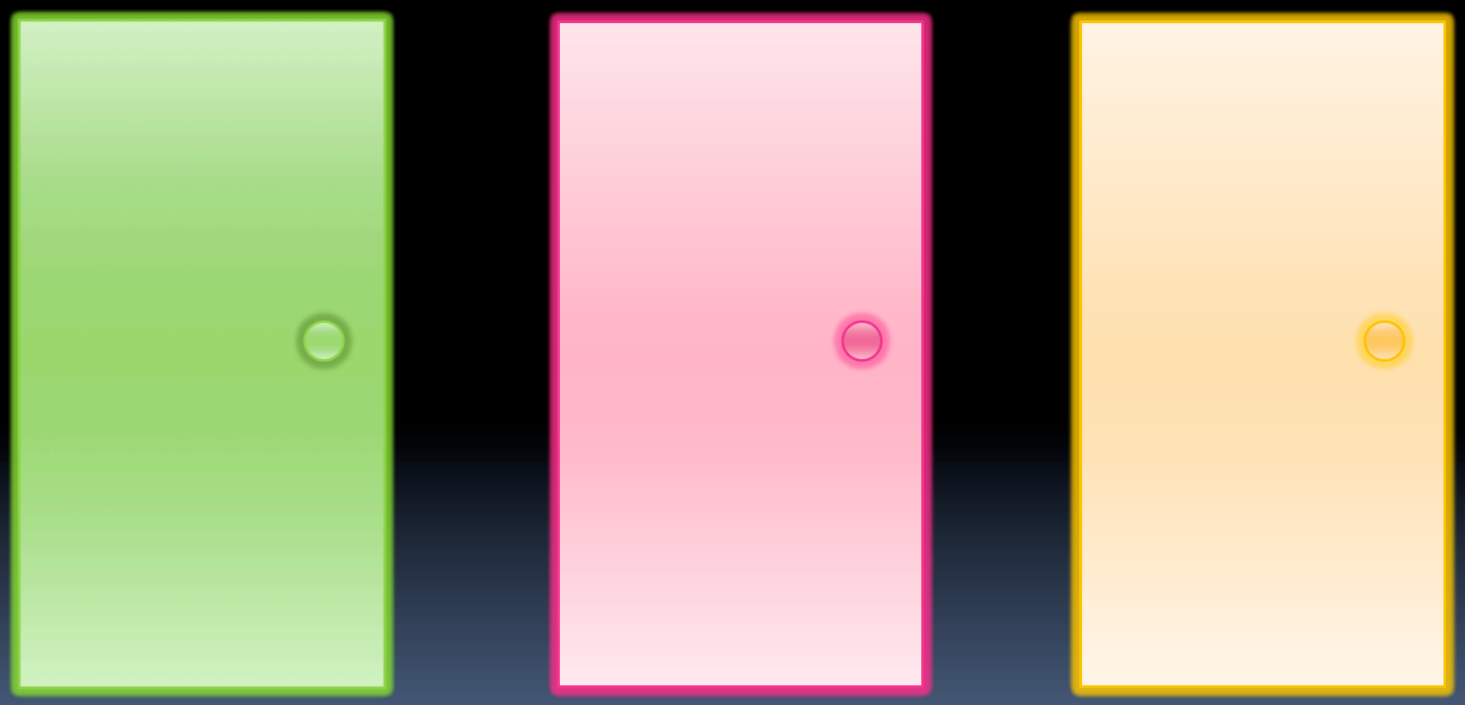
Quantum Computing

- A classical method samples each individually…



Quantum Computing

- A quantum method samples simultaneously



- Selecting a door corresponds to the measurement.

Quantum Computing Recipes

- A quantum algorithm must sample all the possibilities *and choose the right one*.

- There are a few known quantum algorithms
  - Grover's for database searches $O(N^{1/2})$
  - Deutsch-Josza's for balanced functions $O(1)$
  - Shor's for factorizing numbers* $O((\log N)^3)$

**Shor's factorization algorithm provides an exponential speed up and breaks public-key encryption security.*

Building a Quantum Computer

- Basic Research Challenges
  - Generating Qubits and Entanglement

    Many physical system are being considered

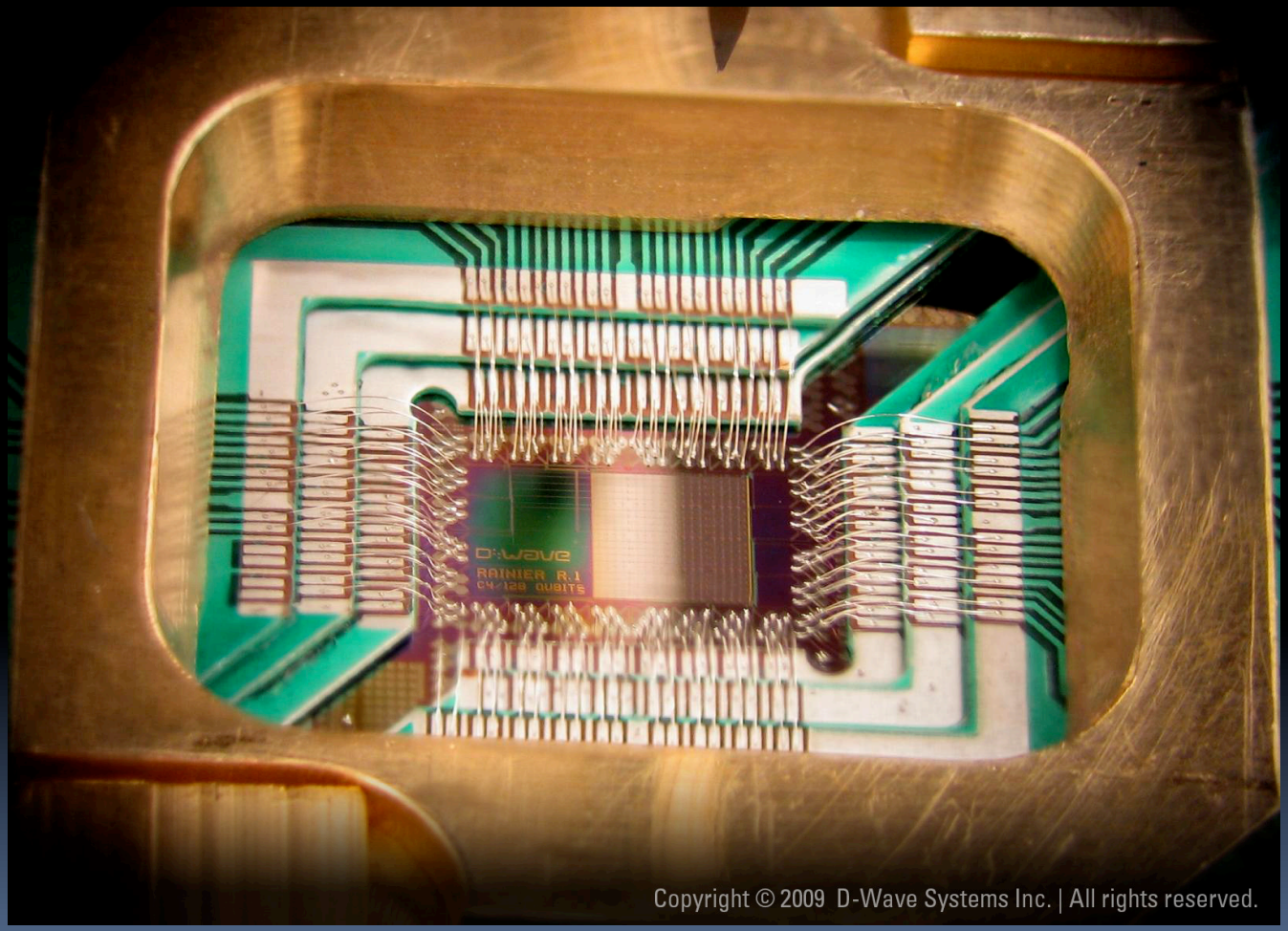
    Several different computational approaches taken
  - Quantum Error Correction

    Remove errors before computation is contaminated
  - Fault tolerance

    Computation needs to be resilient to errors, at some level
  - Scalability

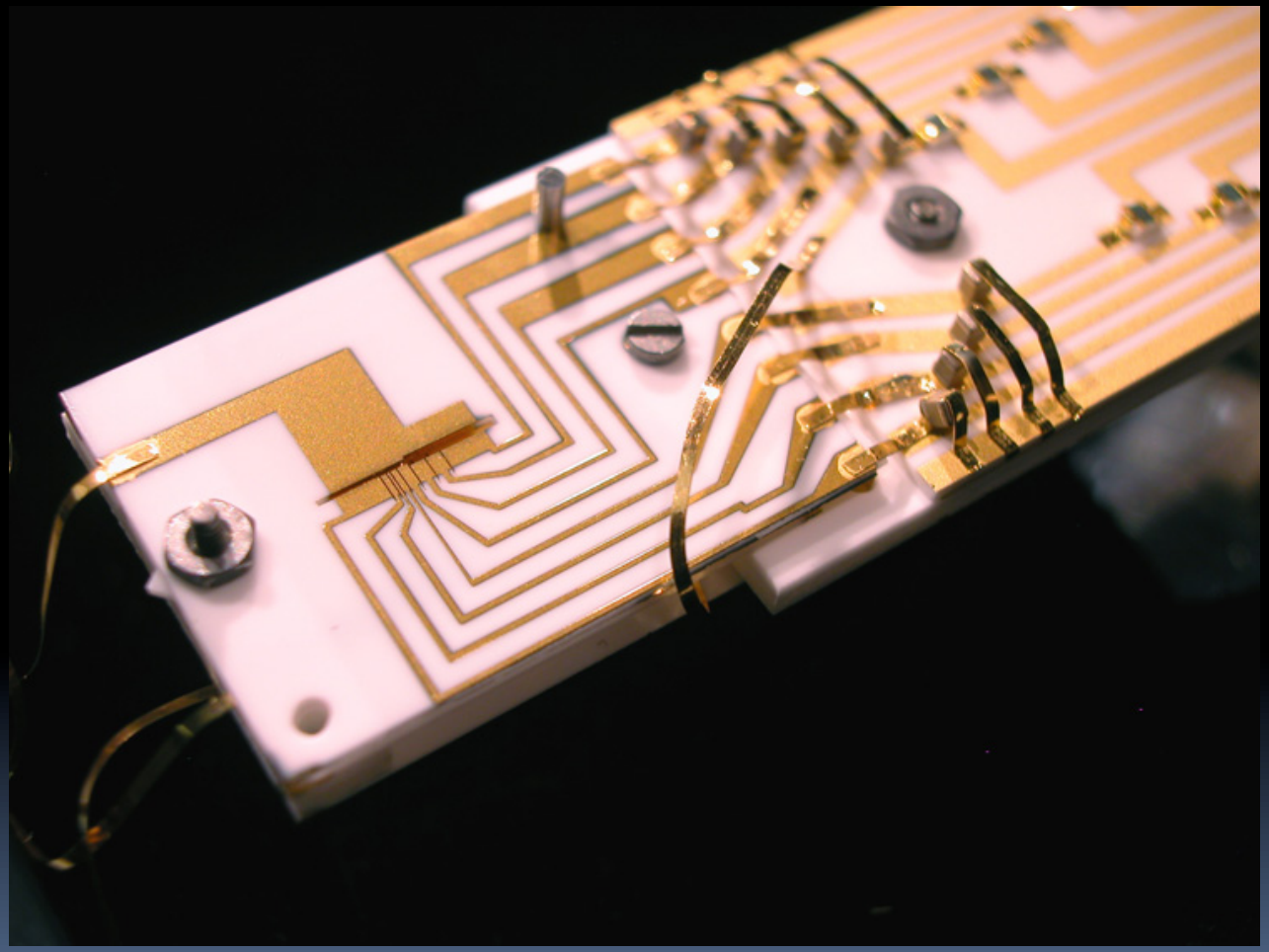
    Physical systems must scale to millions of entangled qubits

Building a Quantum Computer



128-qubit adiabatic quantum computer chip produced by D-Wave Systems

Building a Quantum Computer



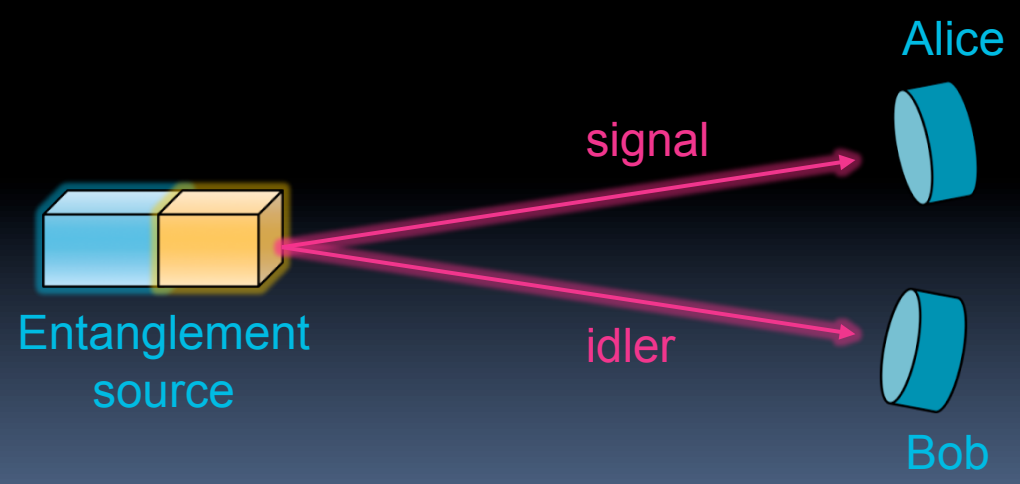
Ion trap chip composed of seven chargeable zones produced by NIST

Building a Quantum Computer

Linear optical waveguide for channeling photons, schematic of the device produced by University of Bristol (UK)

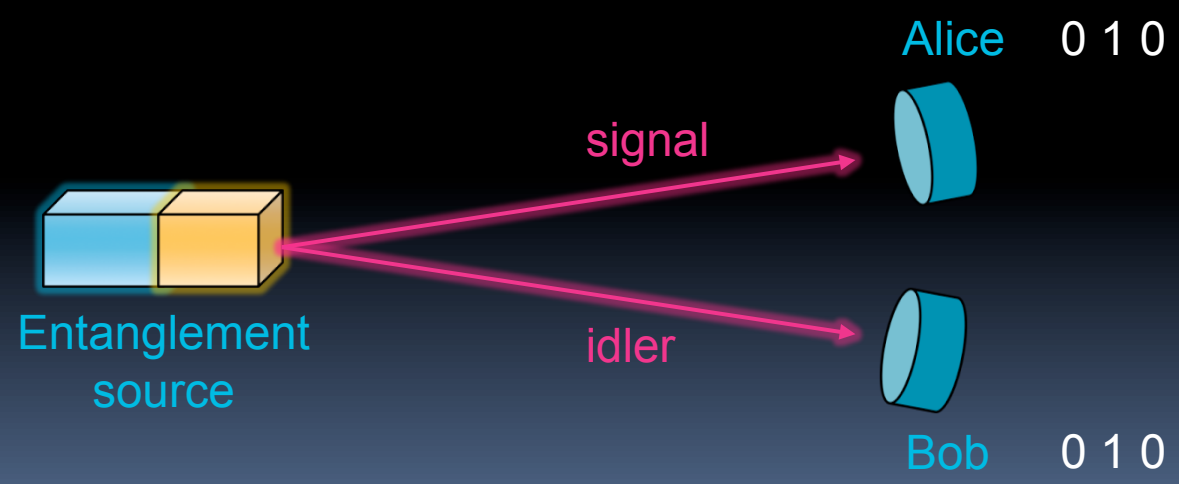
Quantum Key Distribution

- QKD uses quantum information to establish secure communication, e.g., Alice and Bob
- Usually done with entangled photons



Quantum Key Distribution

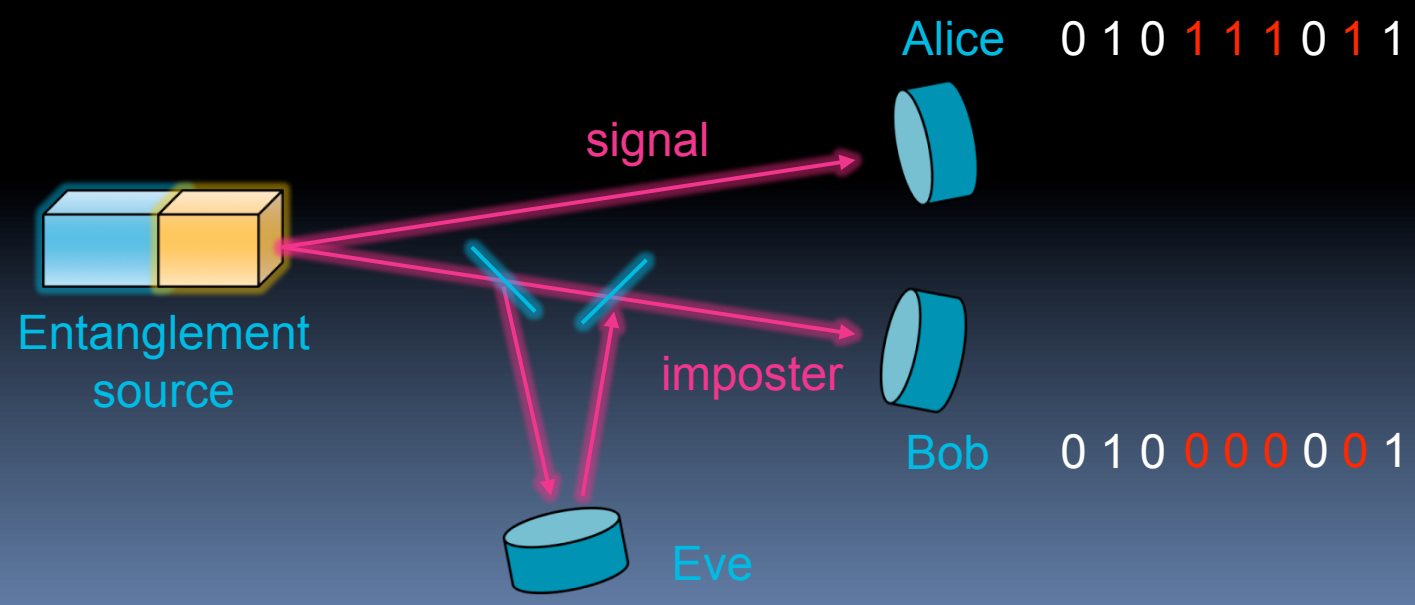
- Correlated measurement outcomes provide a raw cryptographic key
- Secret key acts as a one-time pad*



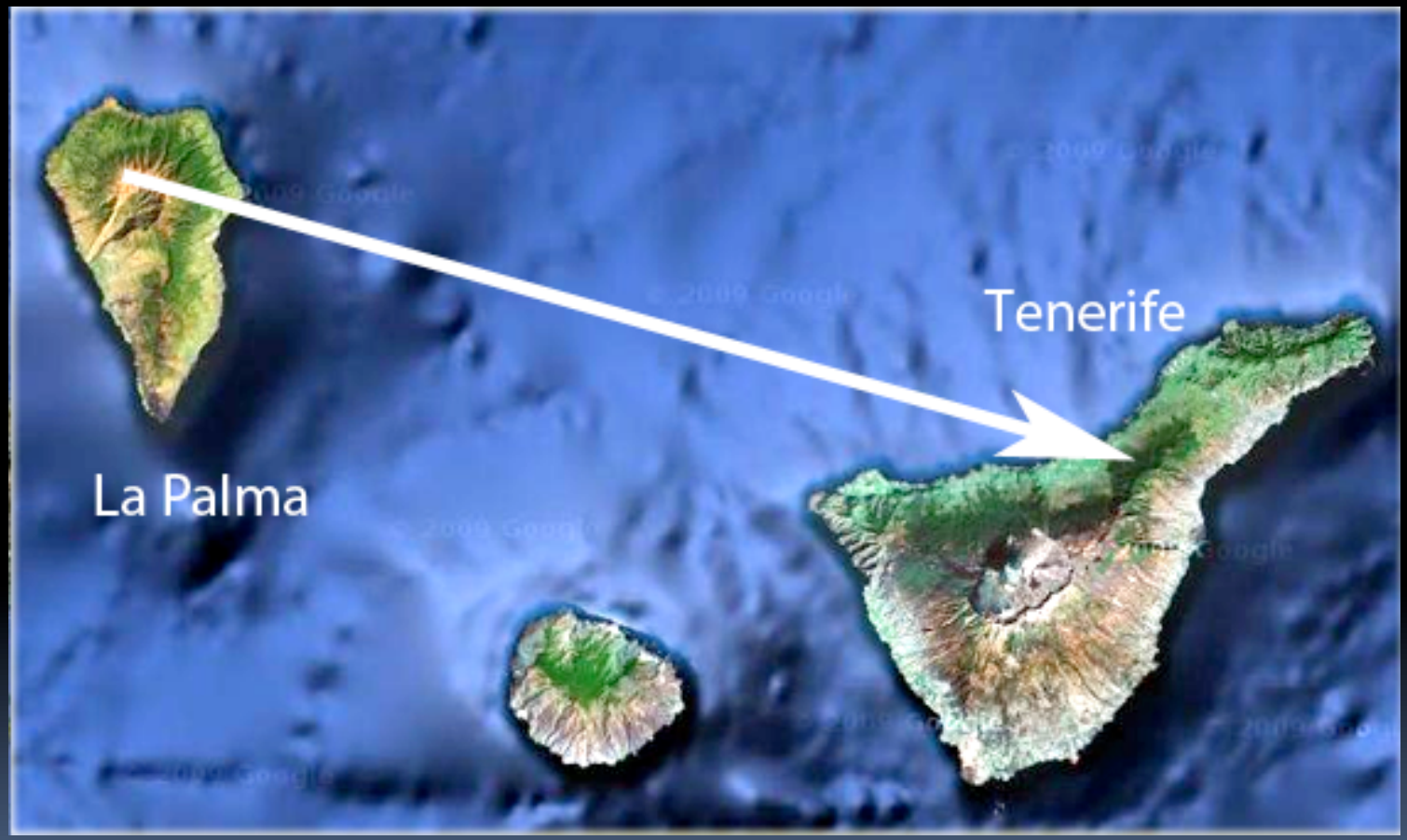
*Shannon proved this method provides perfect secrecy

Quantum Key Distribution

- Entanglement reveals eavesdroppers; Eve's interaction destroys correlations
- Alice and Bob calculate bit error rate

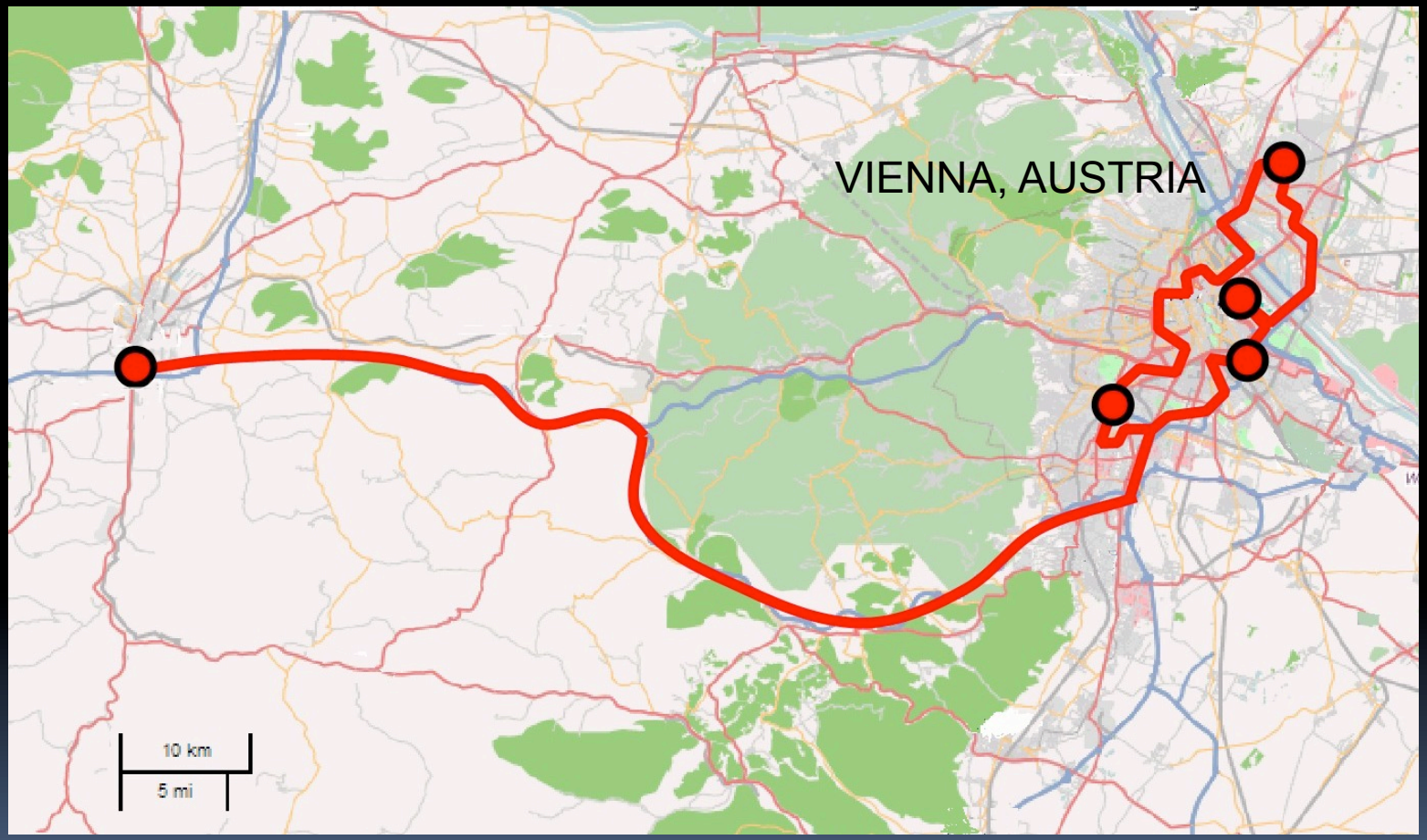


Quantum Key Distribution



144- km free-space QKD over the Canary Islands, 1.8 bit/s performed by European consortium

Quantum Key Distribution



Fiber-ring network in Vienna support QKD base stations, performed by SECOQC consortium

OUTLOOK

Development Support

- Major Investors
  - Governments – basic and applied science
  - Industry – applied encryption, computation, sensing
  - Interest is driven by revolutionary capabilities

- Quantum Information Technology Market
  - Mostly QKD and supporting technologies

    MagiQ, idQuantique, SmartQuantum, Quintessence

    Sources, Detectors, Materials, etc.
  - Multiple Industry R&D efforts known:

    D-Wave, Microsoft, HP, MagiQ, idQuantique, etc.

Technical Challenges

- Breakthroughs in scalability are required
  - *Current state of the art requires a lot of qubits*
  - *Source and detectors need much better efficiencies*
  - *Fast, feed-forward control circuitry emerging*
- More and better quantum algorithms
  - *Wide-spread relevance to maintain interest*
  - *Quantum simulation has a lot of generic potential*
  - *Programming the Universe*

Thank You

Travis S. Humble
Oak Ridge National Laboratory

QUANTUM INFORMATION