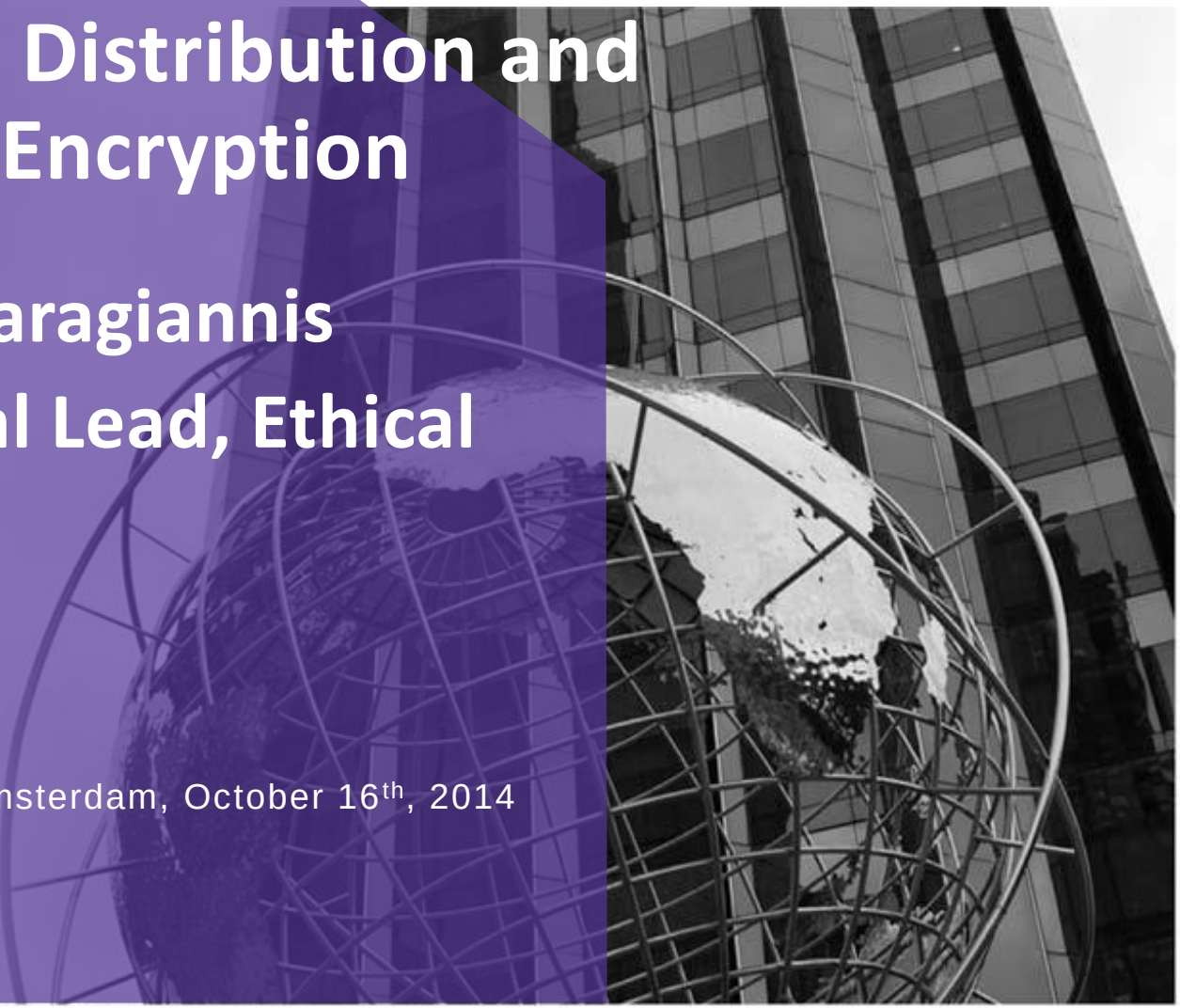
Quantum Key Distribution and the Future of Encryption

Konstantinos Karagiannis

Global Technical Lead, Ethical Hacking

BT Security



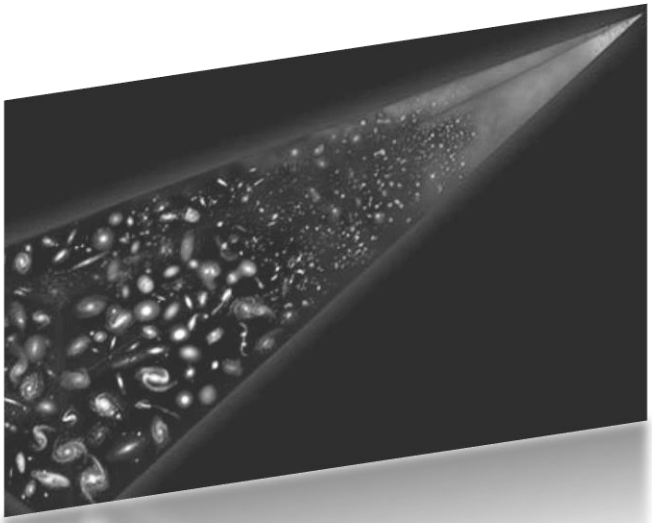
Amsterdam, October 16th, 2014

Understanding QM?

“I think I can safely say that no one understands quantum mechanics.” –

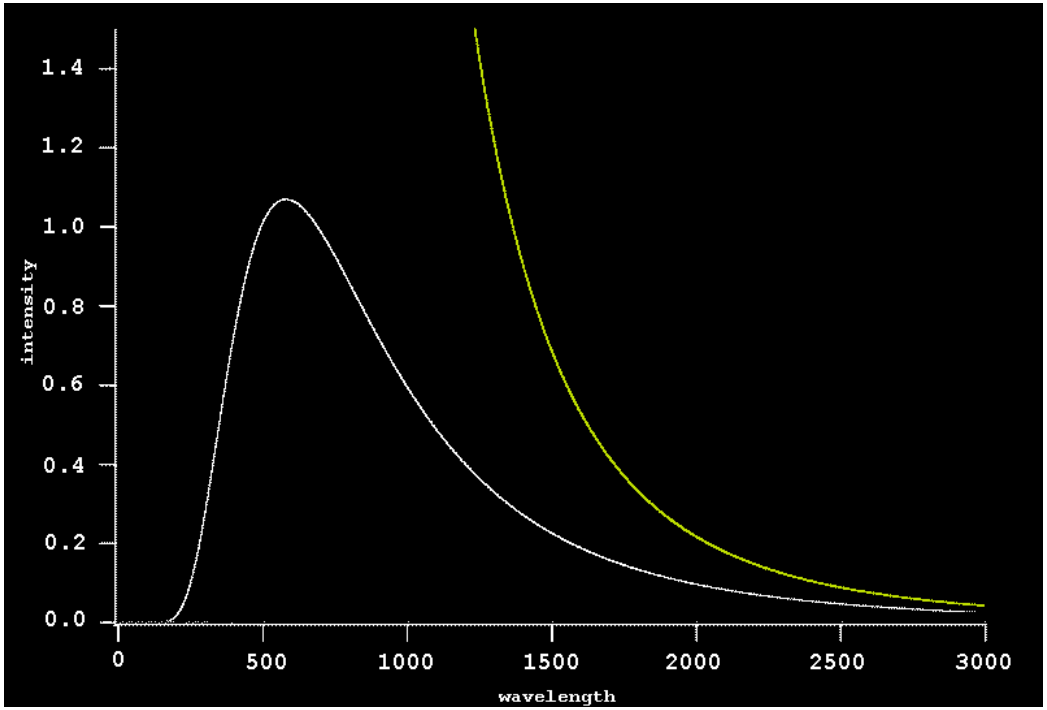
Richard Feynman

(Nobel Prize, 1965)



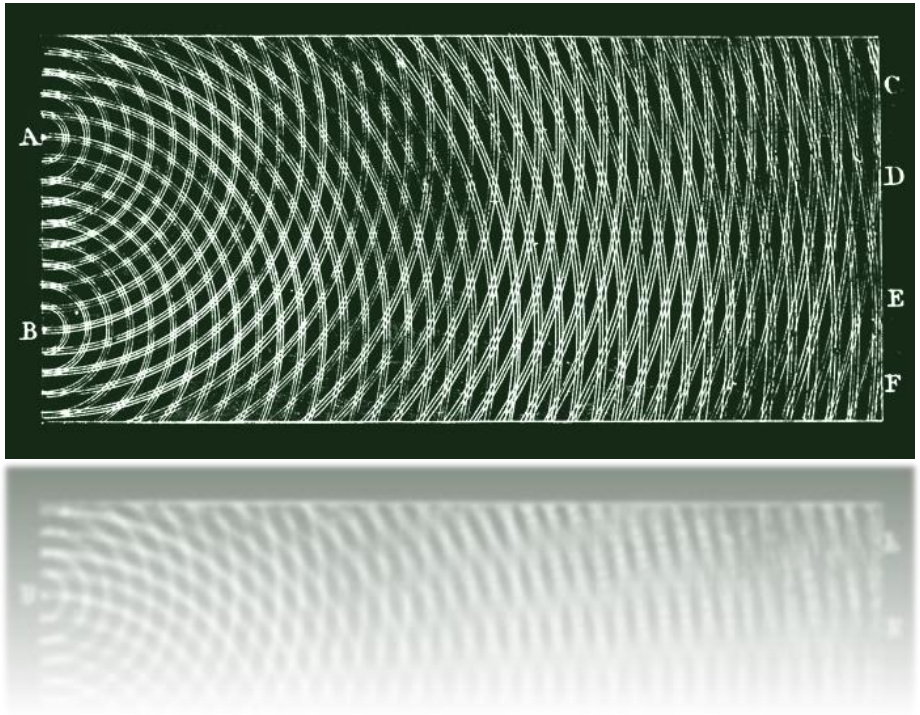
Planck Avoids Catastrophe, Gives Birth to a Field

- Science in the late 1800s—”we’ve found everything, only need better measurements”
- 1800s—blackbody radiation
- 1900—Max Planck proposes “quanta”
- *E=hf*

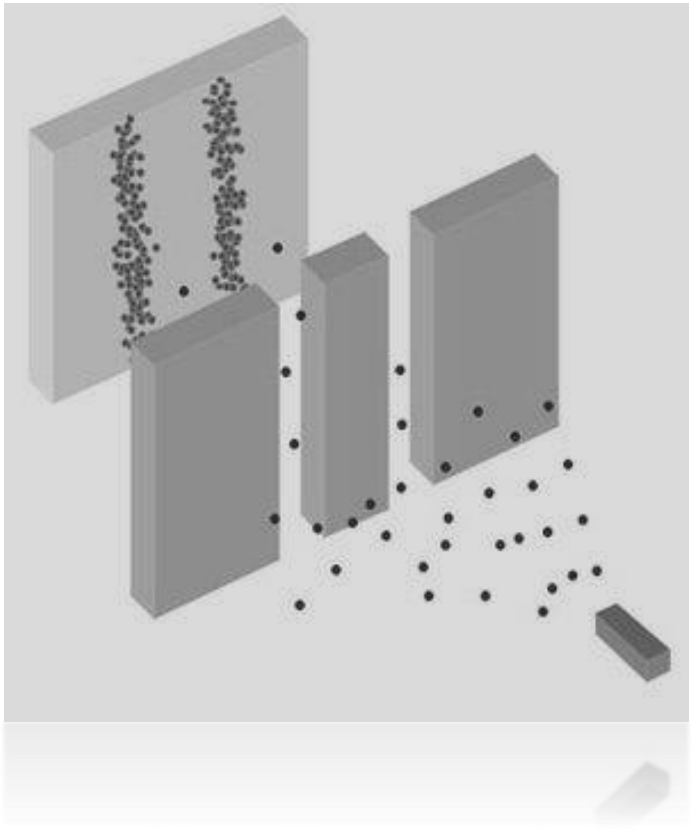


Light: Wave or Particle?

- 1803—Thomas Young's "double slit" experiment
- 1905—Einstein shows light is made of particles
- 1909—Taylor finds wave interference patterns with even one photon at a time

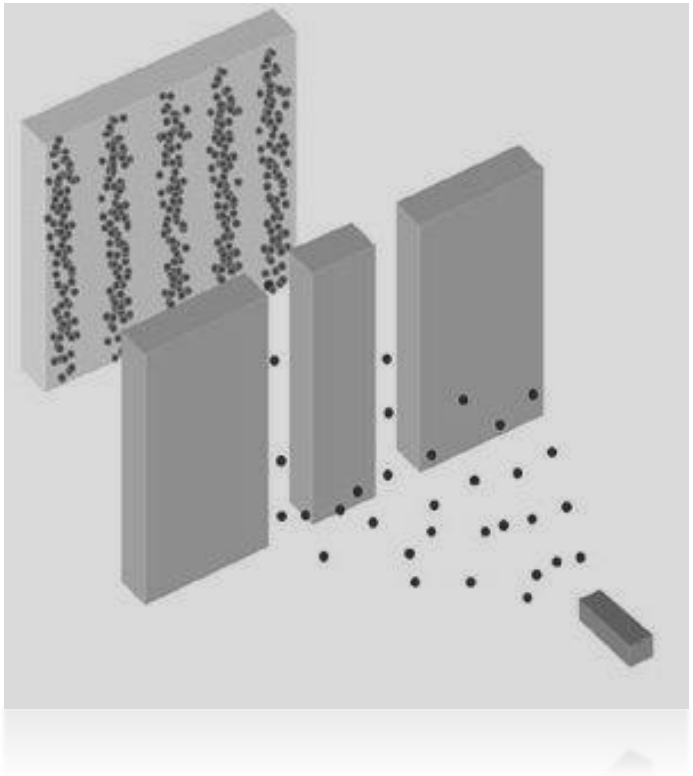


Particle-Wave Duality



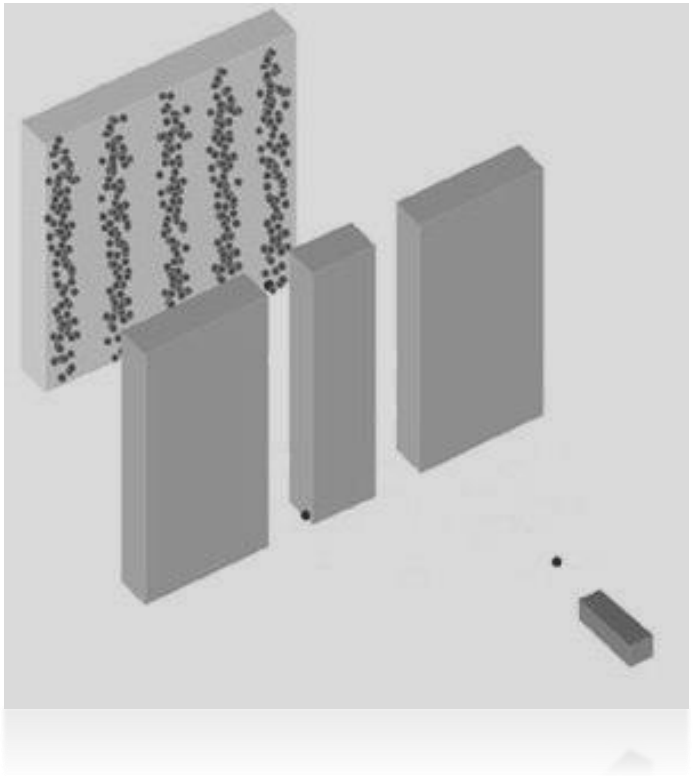
Expected particle behavior or “pooling”

Particle-Wave Duality



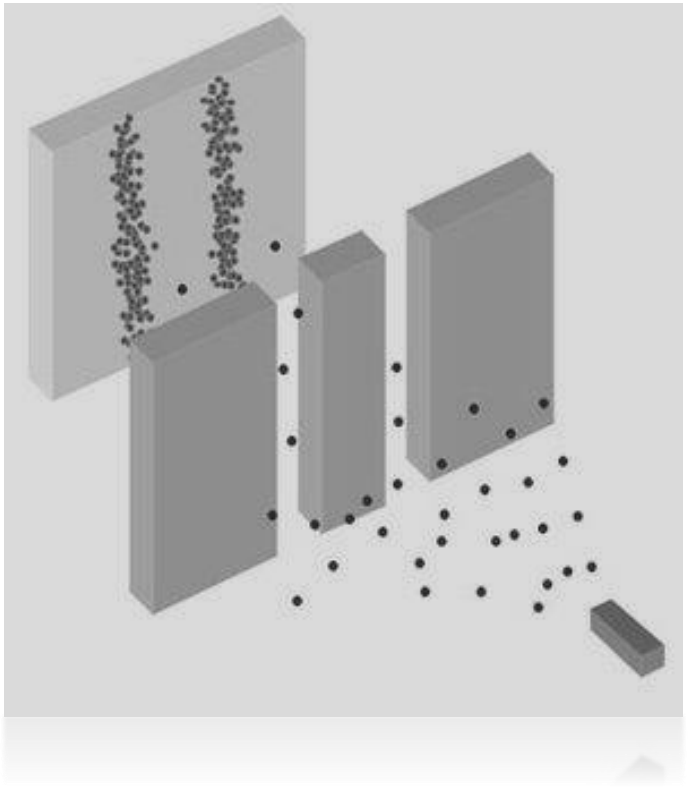
Wave pattern without observation of which slit a particle goes through

Particle-Wave Duality



As Taylor showed, even one particle at a time shows the wave pattern

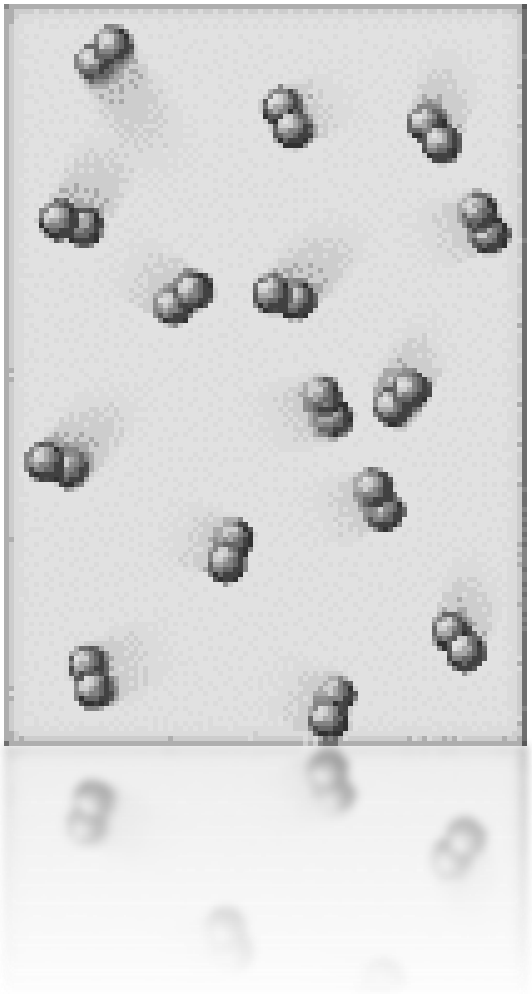
Particle-Wave Duality



Use a detector on either slit, however, and pooling appears

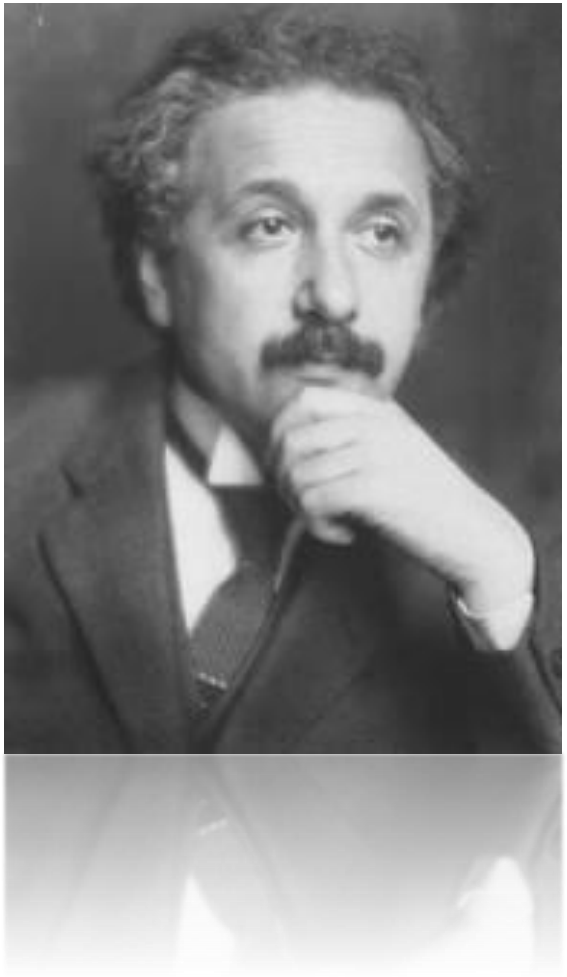
Superposition

- Observing either slit destroyed quantum superposition
- Decoherence—of critical importance in QC
- Quantum weirdness can't occur on a macro scale because universe makes "observations"



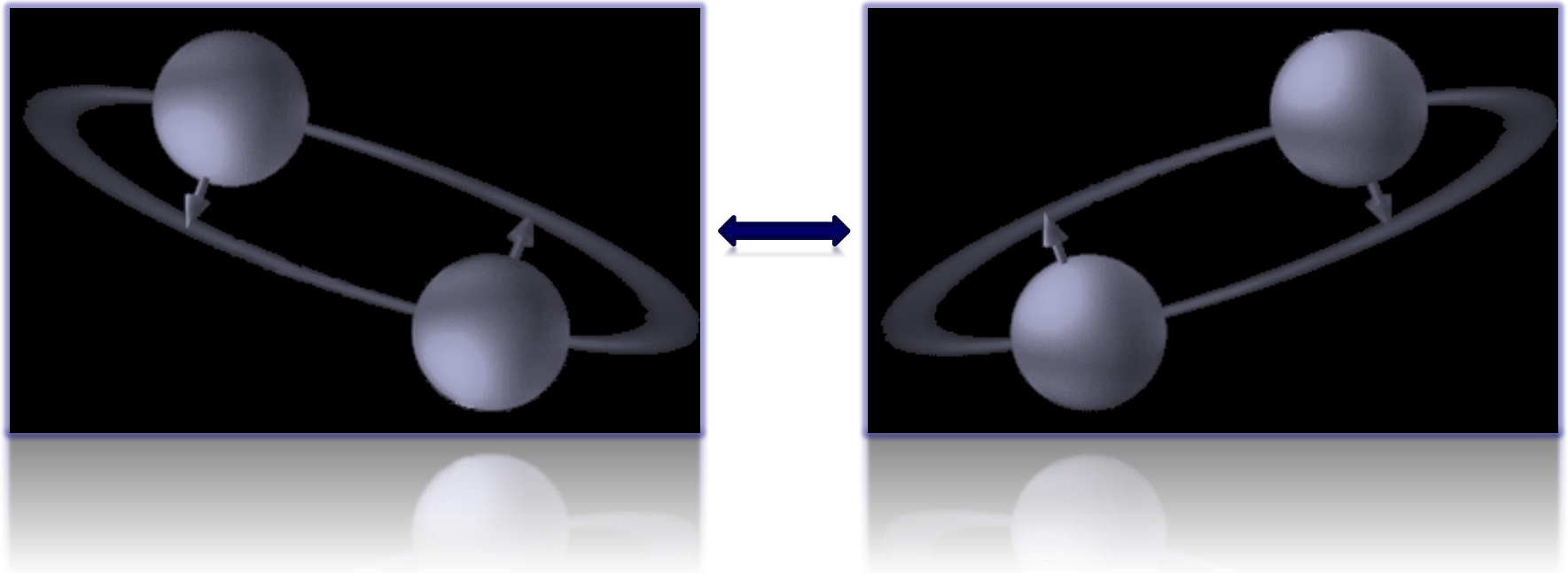
Einstein's Dilemma

- Einstein troubled by a type of superposition: entanglement
- Two of his most colorful quotes relate to it:
  - "God does not play dice with the universe."
  - "Spooky action at a distance."



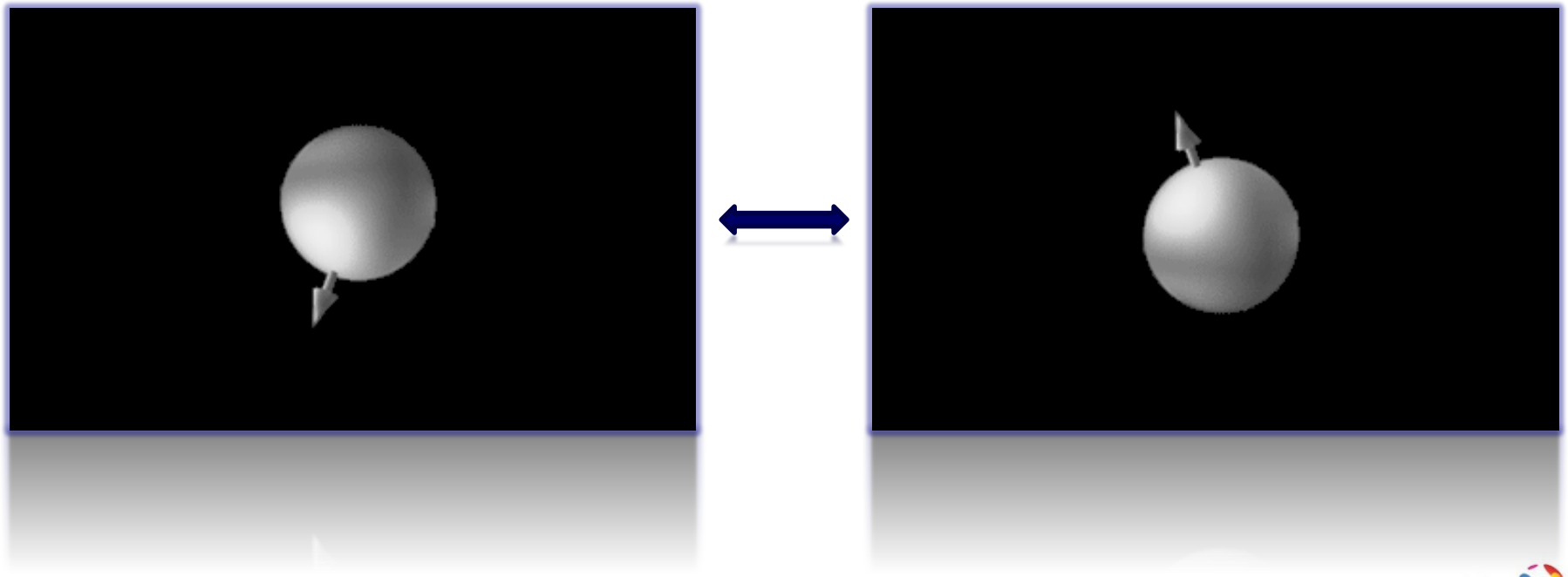
Entanglement

- Created by a quantum event, entangled particles share a quality in superposition; *say*, spin up and down
- Until measured/observed, each particle is in both states



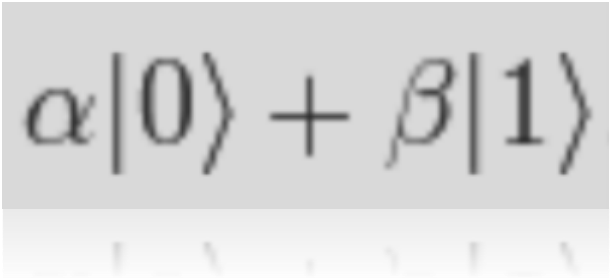
Spooky Decoherence

- Observe the spin of one particle, decoherence occurs
- If one particle is spin down, we know instantly the other is spin up
- *Instantly* could mean faster than light? Not exactly.



Enter the Qubit

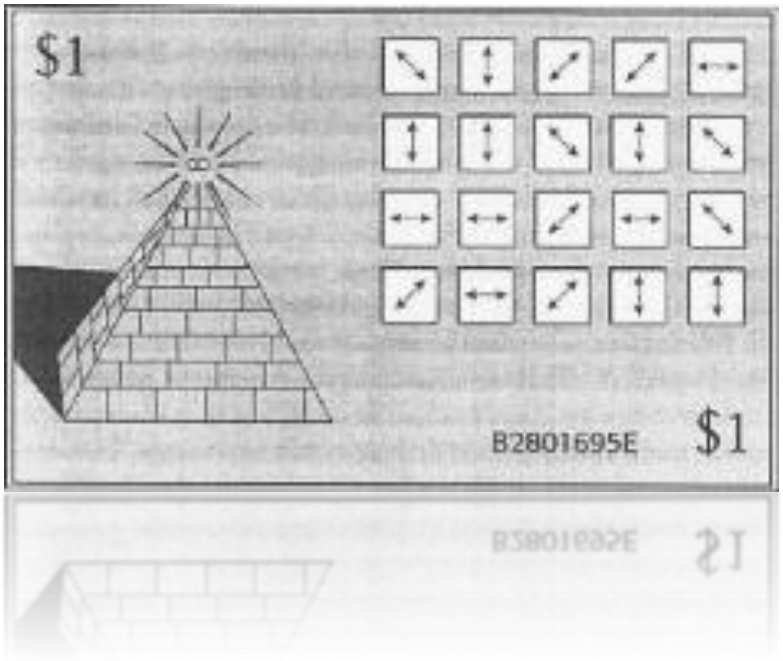
- Unlike bits, qubits can be:
  - Zero
  - One
  - Or a superposition of both (with probabilities of each)
- Qubits can perform certain functions with a percentage of effort of a classical computer



BT

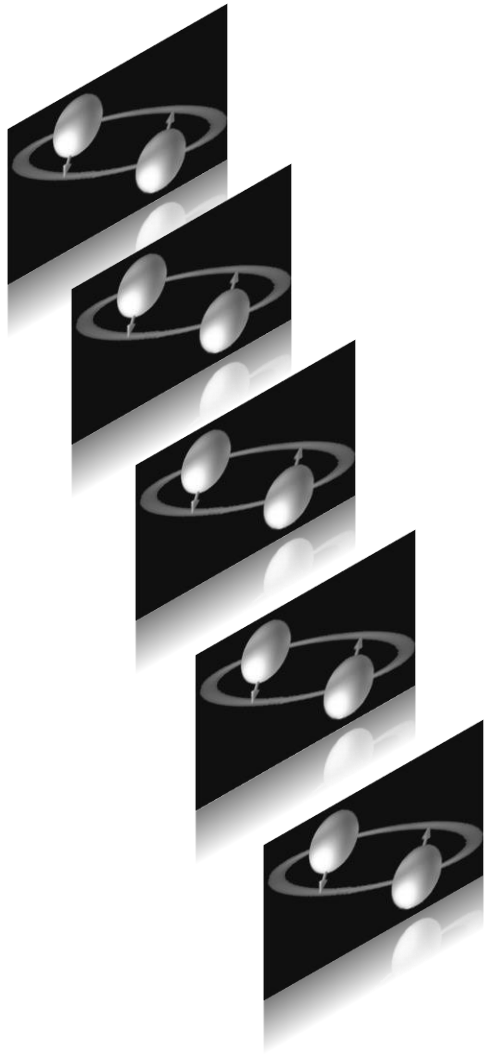
Qubits Invented for Different Purpose

- Stephen Wiesner “invented” qubits in 1969 to stop counterfeiters
- 20 photons in light traps that preserve their random polarity
- A bank could tell with a serial number if a bill was authentic
- This was an early quantum key, too (much more later)



Staying Coherent

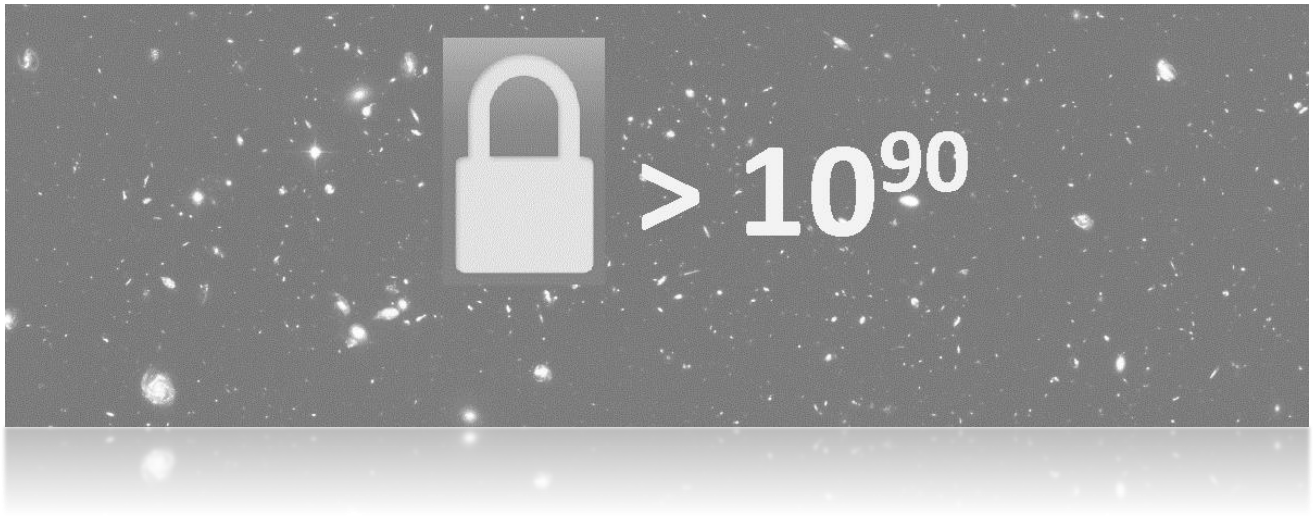
- QCs must maintain coherence in hundreds of particles via:
  - Quantum optics
  - Single atom silicon
  - “Large” artificial qubits
  - NMR
  - Discord
- 2012 Nobel Prize for this work:
  - Serge Haroche (France)
  - David Wineland (USA)



Public-Key Crypto

- PK crypto relies on a classical computer's difficulty at factoring large numbers
- Example—find factors of a 400-digit number:

  400-digit number = 200-digit number * 200-digit number

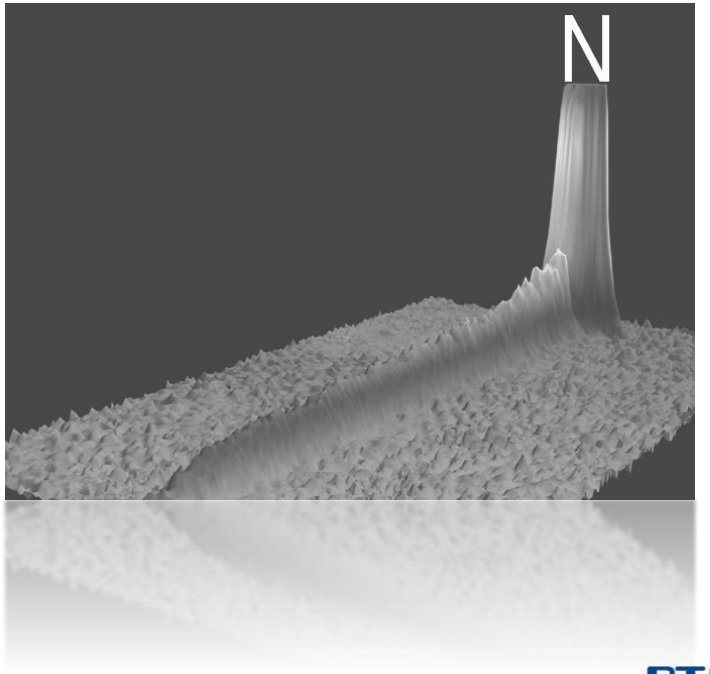


Shor's Algorithm

- 1994—Peter Shor showed a QC could find the factors of large numbers quickly
- Shor's Algorithm has likely answers interfere constructively, unlikely ones destructively
- Proven on a simple QC with four photonic qubits, showing 15=3*5

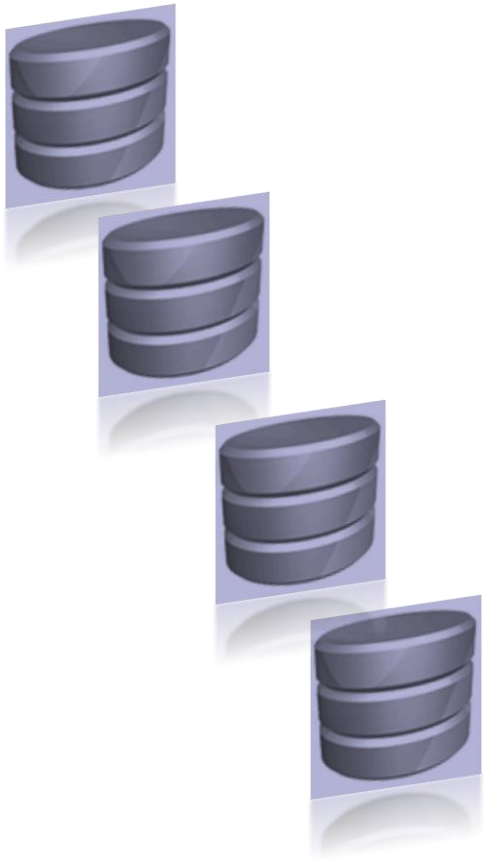
$$\Psi = \frac{1}{2^{n_1}} \sum_{i=0}^{2^{n_1}-1} |\, i >_1 \otimes |\, 0 >_2$$

$$\Psi = \frac{1}{2^{n_1}} \sum_{i=0}^{2^{n_1}-1} |\, i >_1 \otimes |\, x^i \mod N >_2$$



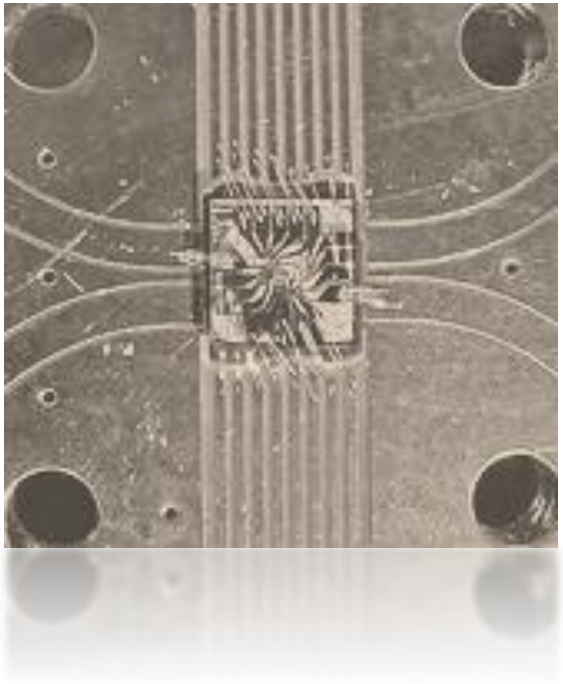
Grover's Algorithm

- Traditional database searches require *N/2* searches for N entries
- Peter Grover showed in 1996 how a QC would allow for $\sqrt{N}$ searches
- Could impact DES if encrypted file and source are available—classical computer would need to search 2^{55} keys, but quantum only 185 million



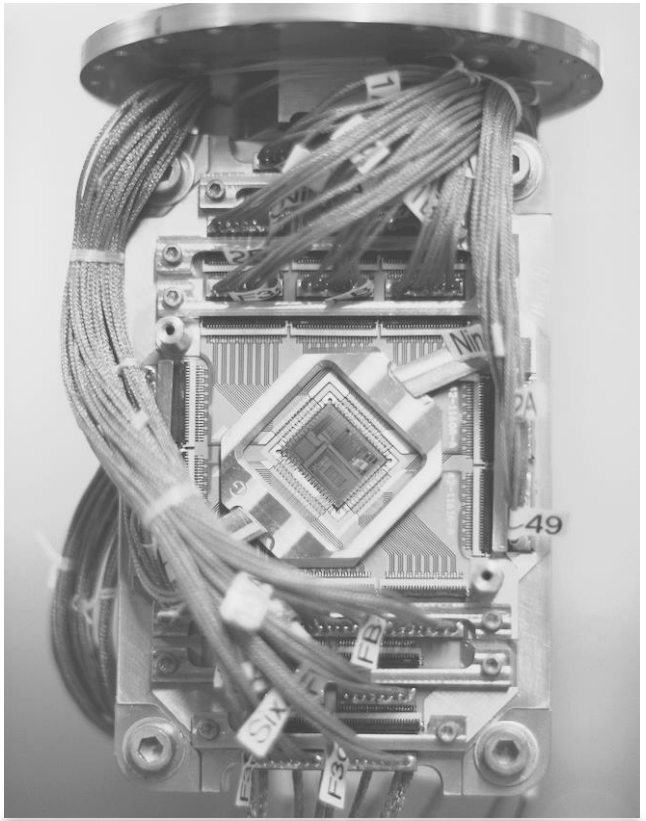
Diamond QC Proves Grover's Algorithm

- Delft University (NL) and UC Santa Barbara
- Simple QC using impurities in a 1mm x 1mm diamond chip at room temperature
- Two qubits: spin of a nitrogen atom and an electron
- A successful result of 4 database entries performed in one search, instead of classical 2
- Grover could affect scanners and AI



Google Searches for Quantum Search Capability

- Google and NASA have a 512-qubit D-Wave at their Quantum Artificial Intelligence Lab
- Google could benefit from Grover's—oddly only mention:
  - Efficient recognizers
  - Polluted data handlers
- Google now working with UC Santa Barbara to build "true" quantum computer



NSA Getting in on the Fun…

- Washington Post reported January 2
- Snowden documents cite $79.7 million research program “Penetrating Hard Targets”
- Not surprising considering EVERYONE wants one in this arms race
- Keep in mind how supercomputers got their start: Colossus (1943), Tommy Flowers, GPO


The Washington Post

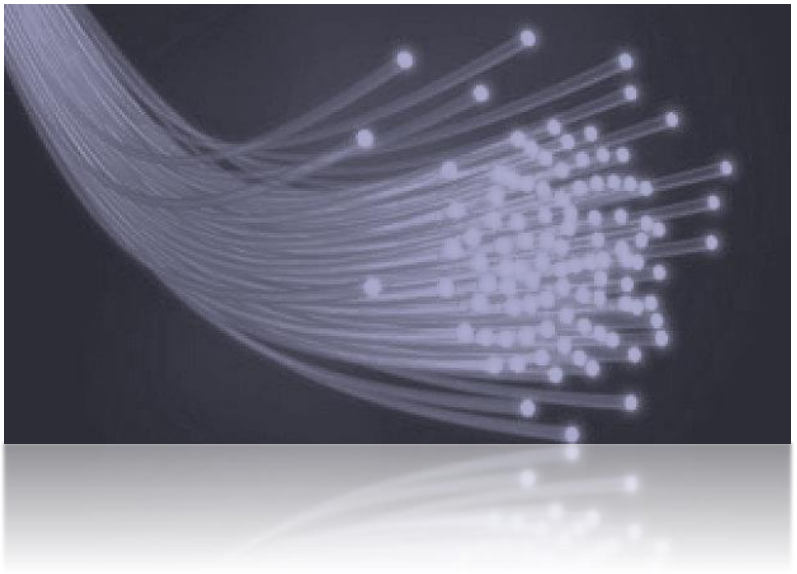
NSA seeks to build quantum computer that could crack most types of encryption

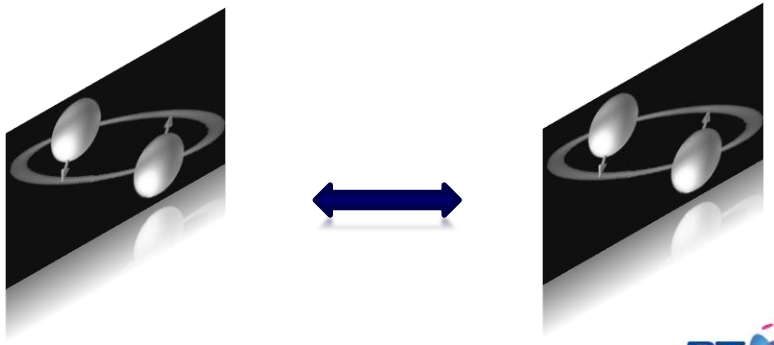
Post Quantum Encryption

- Shor's only proven to work for PK—Grover may affect DES
- The following still seem safe:
  - Code based
  - Hash based
  - Lattice based
  - Multivariate quadratic equations
  - Elliptical curve
  - One time pad (more on this in a moment)
- New quantum encryption on horizon

Quantum Keys to the Future

- Introducing QKD
- Quantum encoded keys sent via a relevant medium—e.g., photons via fiber
- One-time pad system protected by QKD
- Works today, provides hope for complete quantum systems to take over





BT Transfers Quantum Keys over Live Fiber!

- BT, Toshiba, ADVA, and NPL sent Quantum Keys over live fiber
- QKD a reality, sharing a truly secure key over a network
- Any attempt to tap signal can be detected and prevented
- Live fiber takes this into real world applications

Field trial of 10Gb/s transmission secured by QKD*

VOA= variable attenuator
Mux= multiplexer

*Thanks to Yu Rong Zhou and Andrew Lord

Thank you

konstantinos.karagiannis@bt.com
http://www.bt.com/security

Read my blogs at:

http://letstalk.globalservices.bt.com/en/security