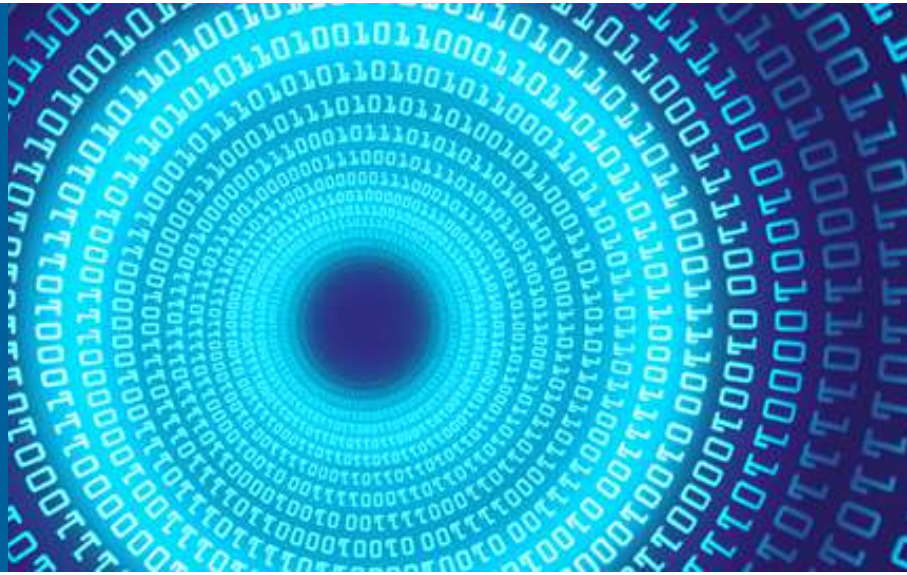
WELCOME TO THE FUTURE

Argonne NATIONAL LABORATORY

CYBERSECURITY IN A POST-QUANTUM WORLD



http://idealeague.net/wp-content/uploads/2015/03/newqubitcont.jpg

YACINE MERDJEMAK
Software Engineer, Risk & Infrastructure Science Center
Global Security Sciences
Argonne National Laboratory

Homeland Defense & Security Education Summit
March 23-24, 2017
George Mason University, Arlington, VA

WHAT'S HAPPENING…?

CYBERSECURITY

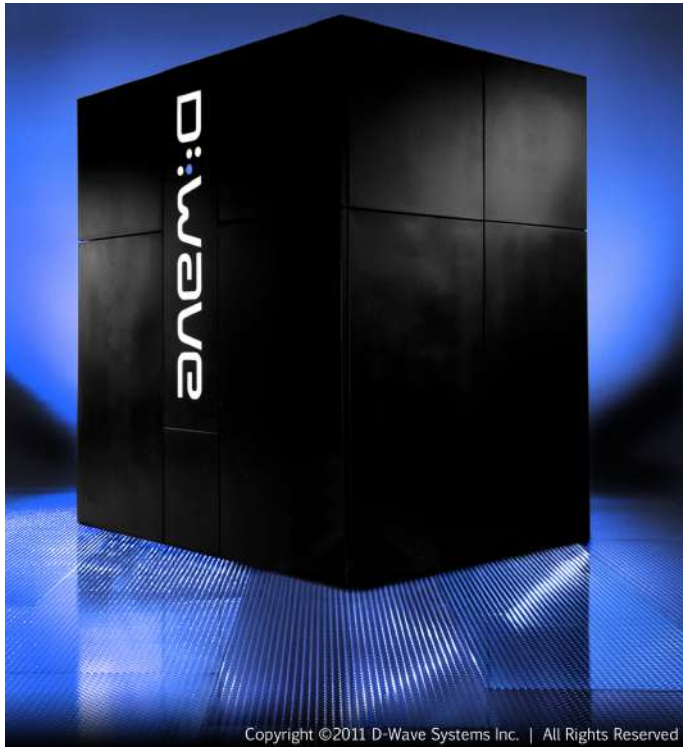
http://uwf.edu/go/cybersecurity/

WHAT'S HAPPENING...?

Quantum computing

D-Wave

- Leading quantum computing company
- Canadian based, founded in 1999
- Currently features a 2000-Qubit quantum system
- 1000 times faster than previous generation D-Wave 2X™ system
- Recently formed an independent subsidiary for the U.S Government
- Partners with NASA, Google, and Lockheed Martin



WHAT'S HAPPENING...?

Quantum computing

IBM **Q**

- Release it's 5 qubit experimental computer in the form of a cloud service (May, 2016)

QxBranch

- Based in Australia
- Q^{x}Branch currently collaborates with leading firms to develop strategies for engaging this quantum computing technology.
- Partners with Lockheed Martin

Rigetti

- Based in Berkeley, CA
- Developing cloud-deployed quantum computers

PUBLIC KEY CRYPTOGRAPHY

The eavesdropper problem

Alice
(sender)

Plaintext

Public Key

RSA Encryption Algorithm

Ciphertext

Public Key

Bob
(receiver)

Plaintext

RSA Decryption Algorithm

Ciphertext

Private Key

http://uwf.edu/go/cybersecurity/

Eve
(Eavesdropper)

Public Channel
(internet)

CRACKING THE KEY

What if ….


```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAgb9XVQ+X4+Hvj0kcgevRH3avSY2wMctUY6XWKOuiOawoSpBPFs653ndqK6+U
6VSqsjs+blf9+wBFPvPglGgNhbiM7QWYX+4tuZ8ibtZCLkoMr+smaTOZqDsr0QbfdB206glvTj0i
srW50RZ7HkPuzfjxdEdBykxQx/CnfV1pAf18UkXq16d2RE2S3zFS6HE3lgDuBjGrK4MpzIOrb05X
BVDM3zqRwJ2ZyXzSBd0i9Hke/OPw+jSrxZeWKAtWprw11CoiT5OwI0iF4qrWkTGMyBe1FfjtYXVb
3Dv91fOrRkD8fNhlsYryf0/vDZMcsr7pO8BD7yXqhN8luVHXCd/10QIDAQABAoIBACLBsw9iQfoV
yCrGFxDmrvqSvJojjpOIOG8JObl0hdyVNaXjyov9jOT/cD2Lp4Rp3eAo5qyAfdUDWYlnoz2eMiEk
Mvw7h3oLP8x9yKeQVeI4i/WENKHx5LOgRjiUcr+URaZ8KIj475aX/9L3BrwwzoP2sBfKDuG2V913
piZ7I2oYrvH8QkbHlssLY0Pn3Eh/huBTDqtdGiGPqjR2329xMUxwmmM9VQFUNrQ9TKGbpUmJtGrx
oEO06TaU0lFnWQ8rAhAGyzJRvhPplgZK3bvcyJjZotEXuuL9+76RWOKE91/ZRO4m8A1AIOEDl/rN
Hfl7k3VD3Z8IwnMR0NgK/utD4sECgYEA0HmoVKRZbo73TWuvG08iiYlq+3BvYnyNk6qBv671OEOu
6uig6jJNzZBctj2GJUn1oZhcS2Pm2IzXrgo8Rn744ZN9QBHLrS4Ztg4sBA7h1Lg1Cc67/i1FPKKF
6nGtDoaei9oz2YZ4W1n7hbZJet6YraWgTD4gIp8loU60gTisoS0CgYEAn1M7W/HzXbQFoPpCHMNO
VssOO94WqYbcrxheI2ulsYsRewRtjiUDNow+BJWISzl9R1BCqCJU3otttb9LNOxibdBwwmDSkCUT
IuPwcbQlEyVgMerAZ7o2Urh/5bkdlJIhLLErE8b60exlIxRerVb0o/sKoshRpLpxE1mzsJmwpbUC
gYEAtGzF2VNPrxZ+Q3vx1XG8k0nh0/CwBY2EPgtwNYPm6KXzKYzhTy7wFPtesb43beg/dHZXUkwI
ytvCAfcLyXs0TI4H9T4xhxUB3YUQZQa4PhCann1USBvH8z05Jvjw7ERnzOOwwg7V9UHAJC3qFDO3
8XkJbVLLHwubVqq2H6v8A5UCgYEAls1B/voYvpVZSo/1KaJWsOILO/EvBBDJKtXmrKIEN/MIfaao
R4WS7/t37ADY+1KT2H8ISHoOWIIiOoewmIwxcf177Q+V3aep4DldaVH4UZHr5fNrYAKpzkwhin9X
lztlORcMTfDlkPKum7B5GJqYfelsnLz8Qe3Sf11FLh+aSo0CgYBEGko6b+FQDmuJnIN7CzhCZnln
7TA1mjB+TmCNZPRTmbzZC0Uy7To6Tv5wHjRPUgloOb0PiRZg6rsiE/Wtx+gjchOjoBnPnGKP0/JD
oHcv8LEX/982tB0dw6FmRVJdtVd0RlB48lhMrMePwaE+l3Vg9X2SYyr5GSPuqeFwfzkXeA==
-----END RSA PRIVATE KEY-----
```


Can someone work backwards with a 2048 bit public key to decrypt a cyphertext?

2048 bit → 617 digit

Desktop computer:

470,000 times the age of the universe *

* Age of the universe ~ 13.8 billon years

QUANTUM KEY CRYPTOGRAPHY

Swiss Secure Balloting

- In 2007, elections officials in Geneva successfully used quantum cryptography to secure the network linking their ballot data entry center to the government repository where votes are stored

iStock, James Steidl

https://www.scientificamerican.com/article/swiss-test-quantum-cryptography/
http://www.cse.wustl.edu/~jain/cse571-07/ftp/ballots.pdf

WHAT'S HAPPENING...?

China's quantum satellite

- On Aug. 16, China launched a satellite into orbit with a unique feature: the ability to send information securely, not with mathematical encryption but by using the *fundamental laws of physics*.

Shutterstock

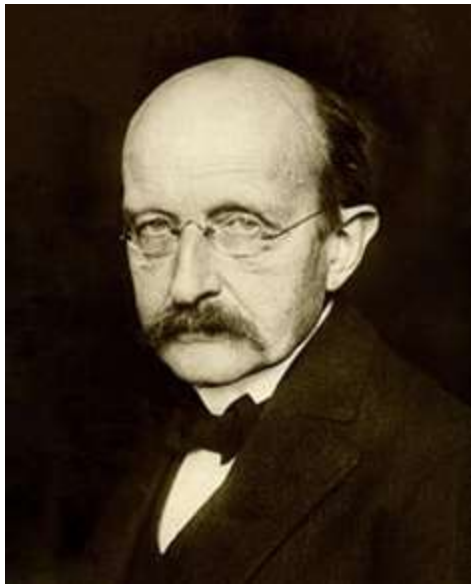
http://phys.org/news/2016-10-china-quantum-satellite-breaches.html

WHAT‘S QUANTUM PHYSICS?

Argonne NATIONAL LABORATORY

QUANTUM PHYSICS

Pioneers



Max Plank (1858-1947)

- German theoretical physicist, Nobel laureate
- Observed black-body radiation spectrum
- Discovery of Energy Quanta

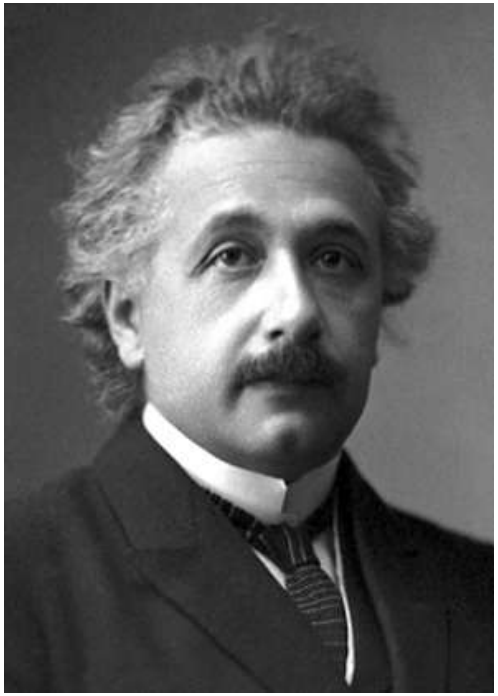
https://en.wikipedia.org/wiki/Max_Planck

$$E = h\nu$$

h: Plank Constant
ν : radiation frequency

QUANTUM PHYSICS

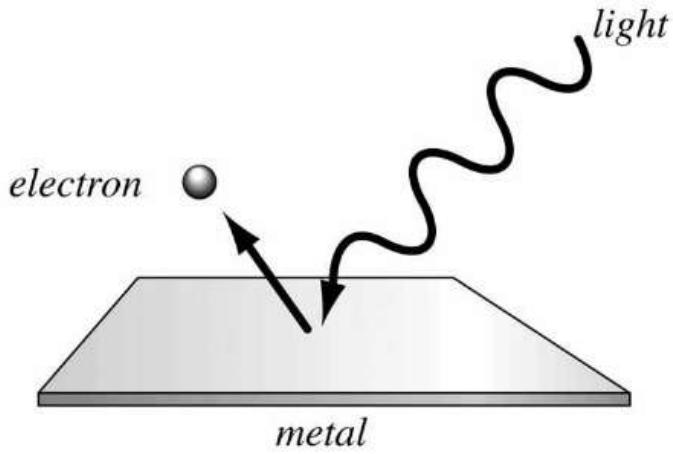
Pioneers



Einstein (1879-1955)

- German theoretical physicist, Nobel laureate
- Observed the photoelectric effect
- Discovery of Photon Particles

https://en.wikipedia.org/wiki/Albert_Einstein



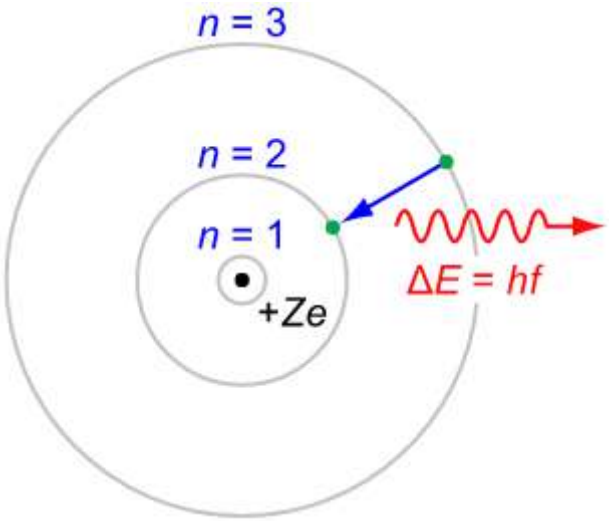
QUANTUM PHYSICS

Pioneers

Niels Bohr (1885-1962)

- Danish physicist, Nobel laureate
- Made foundational contributions to understanding atomic structure and quantum theory
- The **Bohr model** of the hydrogen atom

https://en.wikipedia.org/wiki/Niels_Bohr



QUANTUM PHYSICS

Pioneers

Erwin Schrödinger (1887-1961)

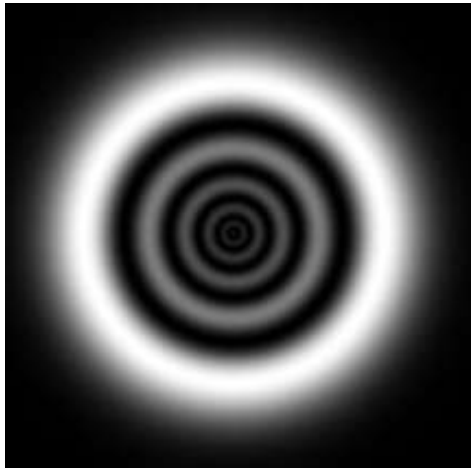
- Austrian physicist, Nobel laureate
- Developed a number of fundamental results in quantum theory and is best known for the **Schrödinger Equation**

https://en.wikipedia.org/wiki/Erwin_Schrodinger

Werner Heisenberg (1901-1976)

- German theoretical physicist, Nobel laureate
- One of the key pioneers of quantum mechanics, best known for the **uncertainty principle**

https://en.wikipedia.org/wiki/Werner_Heisenberg



WEIRD PHYSICS

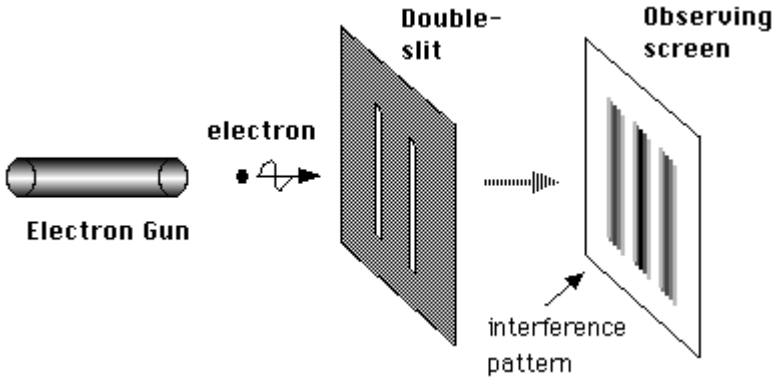
Quantum Nonlocality and Quantum Superposition

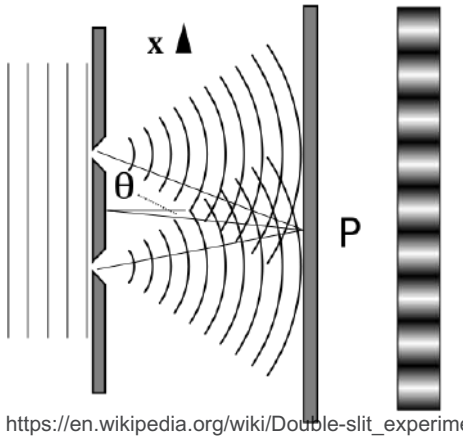
- Double slit experiment: Thomas Young (1801)
- Demonstrates that photons or particles of matter (like an electron) produce a wave pattern when two slits are used
- In the Copenhagen interpretation (1925), Bohr and Heisenberg introduced the concept that

  – ***Physical systems do not have definite properties prior to being measured***

  – ***Quantum mechanics can only predict the probabilities that measurements will produce certain results***

  – ***The act of measurement affects the system, causing the set of probabilities to reduce to only one of the possible values immediately after the measurement (known as the observer effect)***





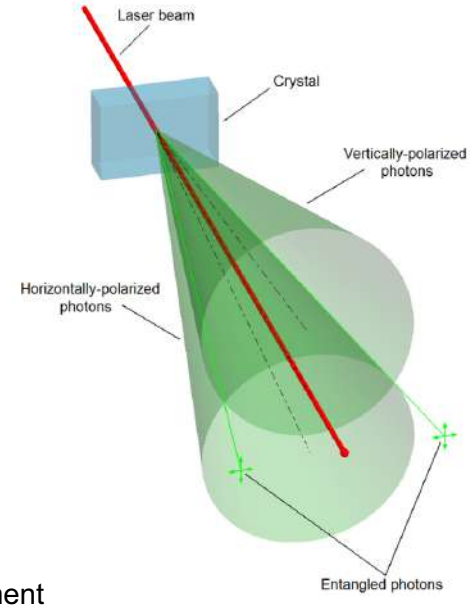
https://en.wikipedia.org/wiki/Double-slit_experiment

QUANTUM PHYSICS

Quantum Entanglement

Alain Aspect (Born 1947, Age 69)

- French physicist
- Demonstrated quantum entanglement experimentally
- Quantum entanglement occurs when two particles originate at the same point in space and time and behave as a single system

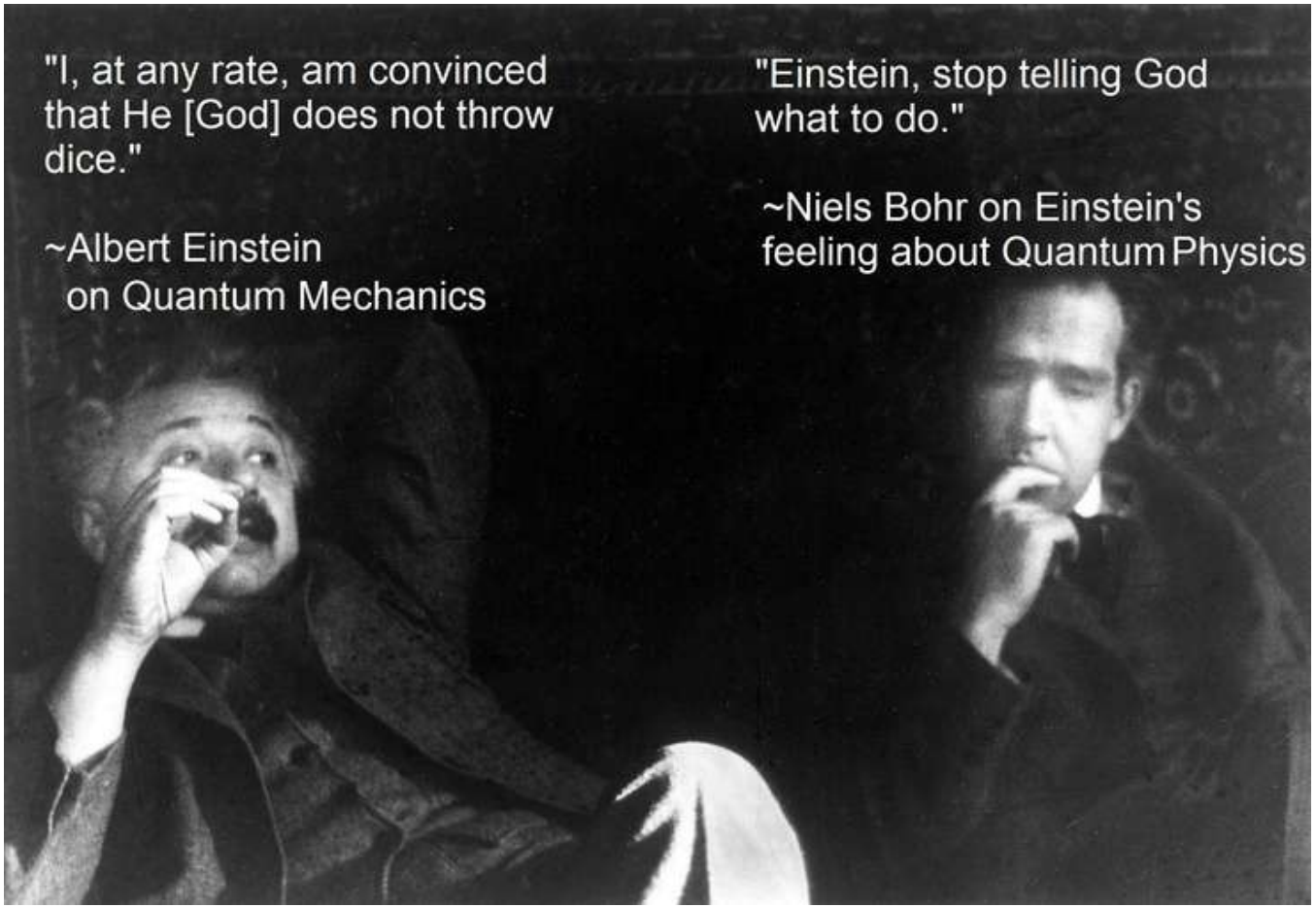


https://en.wikipedia.org/wiki/Alain_Aspect

https://en.wikipedia.org/wiki/Quantum_entanglement

WEIRD PHYSICS

“Spooky action at a distance”

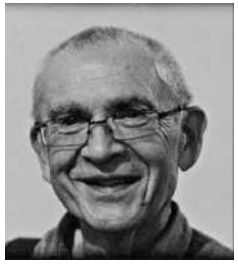


https://www.pinterest.com/pin/451767406340954025/

WHAT'S A QUANTUM COMPUTER?

QUANTUM COMPUTING

Pioneers



Yuri Manin, Mathematician

- 1980: First to proposes the idea quantum computer

https://arxiv.org/pdf/quant-ph/0005003.pdf

Paul Benioff, Argonne Scientist

- 1980: Described quantum mechanical models of computers

http://link.springer.com/article/10.1007%2FBF01011339

Richard Feynman (1918-1988), Physicist

- 1981: Presented a logical quantum computer model
- Demonstrated the impossibility to conduct the simulation of a quantum system with the use of a classic computer
- Demonstrated that the traditional approach to computer development would never lead to a revolution

https://pdfs.semanticscholar.org/75df/806e432f706b25ca35adb57d3a1a59ec9e22.pdf

QUANTUM COMPUTING

CLASSICAL COMPUTER

Uses Transistors

Type of switch:

On = 1

Off = 0

Binary language

Logic gates = grouping of transistors

Allows computations based on man-made programs

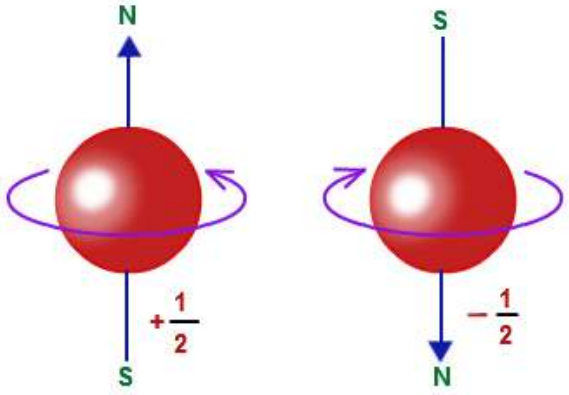
QUANTUM COMPUTING

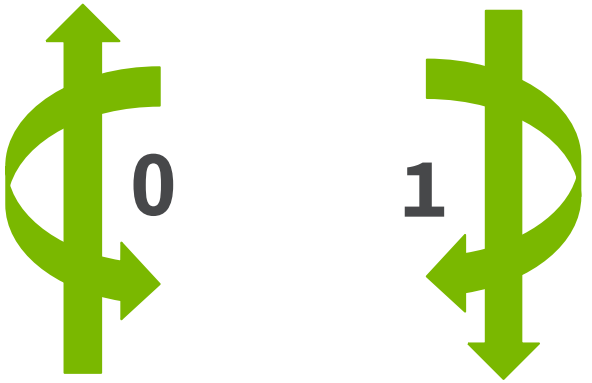
Quantum Superposition

QUANTUM COMPUTER

Quantum state of an elementary particle such as an electron

Example of state: Spin (Magnetic Orientation)





http://1.bp.blogspot.com/-Thtz1MHS-xU/V0CuCxD3IOI/AAAAAAAAEdk/GcB690jxvEw0qxRTTpTeTIJUJ-8LNvLNACK4B/s1600/spin-quantum-number.png

QUANTUM COMPUTING

CLASSICAL COMPUTER

- Classical bit

0

or

1

QUANTUM COMPUTER

- Quantum bit: Qubit
- Superposition
- Incredible possibilities!

QUANTUM COMPUTING

Let's do the math….

CLASSIC COMPUTER

2 bit:

Operation is repeated separately for each combinations of 0 and 1

00

10

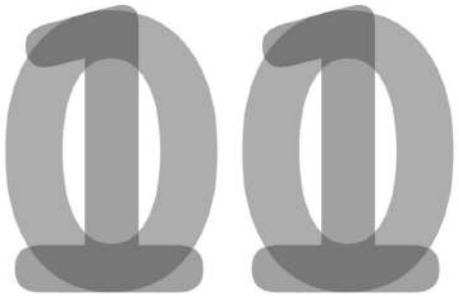
01

11

QUANTUM COMPUTER

2 qubit:

Operation is performed only once for all combinations of 0 and 1



QUANTUM COMPUTING

Let's do the math….

CLASSIC COMPUTER

3 bit:

000 or 001 or …… or 111 → 1 state per operation

4 bit:

0000 or 0001 or …… or 1111 → 1 state per operation

…….

300 bit:

00…0 or 00…1 or ….. or 11…1 → 1 state per operation

QUANTUM COMPUTING

Let's do the math….

CLASSICAL COMPUTER	QUANTUM COMPUTER
Joining classical processors:	Joining quantum processors:
One operation at a time → (OR)	Superposition → (AND)
N states	2^N states
N_1N_2 states	$2^{N_1N_2}$ states
Multiplication	Exponential growth

QUANTUM COMPUTING

Let's do the math….

QUANTUM COMPUTER

3 qubit:

000 and 001 and ….. and 111 → 2^3 = 8 states per operation

4 qubit:

0000 and ….. and 1111 → 2^4 = 16 states per operation

…….

300 qubit:

00…0 and ….. and 11…1 → $2^{300} = 2x10^{90}$ states per operation

More particles than in the observable universe!

CRACKING THE KEY

What if ….

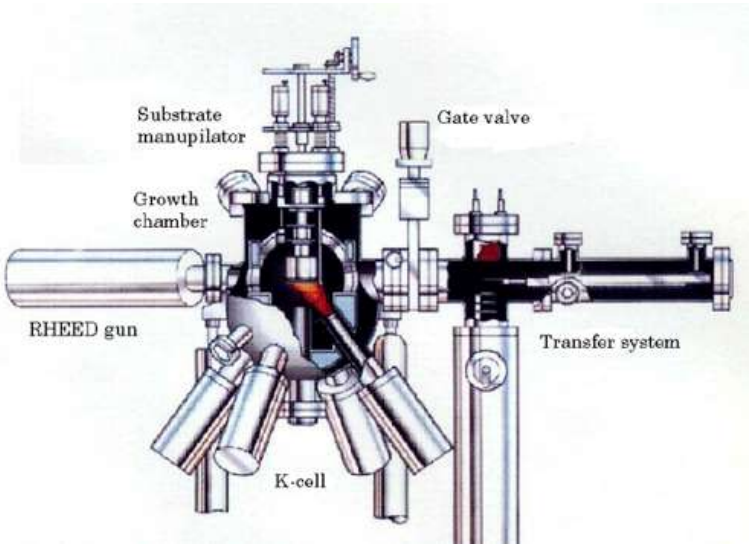
- -----BEGIN RSA PRIVATE KEY-----
- MIIEpAIBAAKCAQEAgb9XVQ+X4+Hvj0kcgevRH3avSY2wMctUY6XWKOuiOawoSpBPFs653ndqK6+U
- 6VSqsjs+blf9+wBFPvPglGgNhbiM7QWYX+4tuZ8ibtZCLkoMr+smaTOZqDsr0QbfdB206glvTj0i
- srW50RZ7HkPuzfjxdEdBykxQx/CnfV1pAf18UkXq16d2RE2S3zFS6HE3lgDuBjGrK4MpzIOrb05X
- BVDM3zqRwJ2ZyXzSBd0i9Hke/OPw+jSrxZeWKAtWprw11CoiT5OwI0iF4qrWkTGMyBe1FfjtYXVb
- 3Dv91fOrRkD8fNhlsYryf0/vDZMcsr7pO8BD7yXqhN8luVHXCd/10QIDAQABAoIBACLBsw9iQfoV
- yCrGFxDmrvqSvJojjpOIOG8JObl0hdyVNaXjyov9jOT/cD2Lp4Rp3eAo5qyAfdUDWYlnoz2eMiEk
- Mvw7h3oLP8x9yKeQVeI4i/WENKHx5LOgRjiUcr+URaZ8KIj475aX/9L3BrwwzoP2sBfKDuG2V913
- piZ7I2oYrvH8QkbHlssLY0Pn3Eh/huBTDqtdGiGPqjR2329xMUxwmmM9VQFUNrQ9TKGbpUmJtGrx
- oEO06TaU0lFnWQ8rAhAGyzJRvhPplgZK3bvcyJjZotEXuuL9+76RWOKE91/ZRO4m8A1AIOEDl/rN
- Hfl7k3VD3Z8IwnMR0NgK/utD4sECgYEA0HmoVKRZbo73TWuvG08iiYlq+3BvYnyNk6qBv671OEOu
- 6uig6jJNzZBctj2GJUn1oZhcS2Pm2IzXrgo8Rn744ZN9QBHLrS4Ztg4sBA7h1Lg1Cc67/i1FPKKF
- 6nGtDoaei9oz2YZ4W1n7hbZJet6YraWgTD4gIp8loU60gTisoS0CgYEAn1M7W/HzXbQFoPpCHMNO
- VssOO94WqYbcrxheI2ulsYsRewRtjiUDNow+BJWISzl9R1BCqCJU3otttb9LNOxibdBwwmDSkCUT
- IuPwcbQlEyVgMerAZ7o2Urh/5bkdlJIhLLErE8b60exlIxRerVb0o/sKoshRpLpxE1mzsJmwpbUC
- gYEAtGzF2VNPrxZ+Q3vx1XG8k0nh0/CwBY2EPgtwNYPm6KXzKYzhTy7wFPtesb43beg/dHZXUkwI
- ytvCAfcLyXs0TI4H9T4xhxUB3YUQZQa4PhCann1USBvH8z05Jvjw7ERnzOOwwg7V9UHAJC3qFDO3
- 8XkJbVLLHwubVqq2H6v8A5UCgYEAls1B/voYvpVZSo/1KaJWsOILO/EvBBDJKtXmrKIEN/MIfaao
- R4WS7/t37ADY+1KT2H8ISHoOWIIiOoewmIwxcf177Q+V3aep4DldaVH4UZHr5fNrYAKpzkwhin9X
- lztlORcMTfDlkPKum7B5GJqYfelsnLz8Qe3Sf11FLh+aSo0CgYBEGko6b+FQDmuJnIN7CzhCZnln
- 7TA1mjB+TmCNZPRTmbzZC0Uy7To6Tv5wHjRPUgloOb0PiRZg6rsiE/Wtx+gjchOjoBnPnGKP0/JD
- oHcv8LEX/982tB0dw6FmRVJdtVd0RlB48lhMrMePwaE+l3Vg9X2SYyr5GSPuqeFwfzkXeA==
- -----END RSA PRIVATE KEY-----

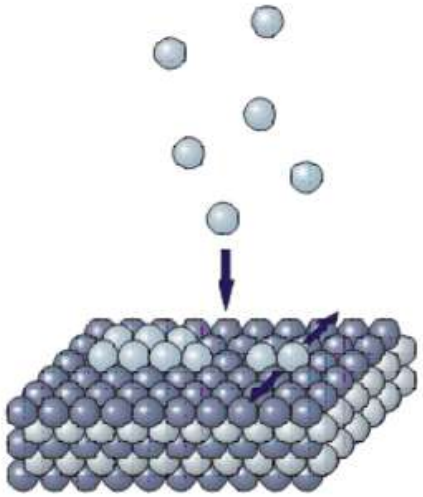
Can a 2048-bit quantum computer break it the RSA-2048 encryption key?

QUANTUM COMPUTING

Single-Atom Device

- Scientists from the University of New South Wales (2012)
- Scanning tunneling microscope (STM)
- First single-atom transistor
- Made from a single phosphorus atom embedded in a silicon crystal
- Read and write information using the spin of the electron





http://www.lps.umd.edu/MBEGroup/MBEWhatIs.htm

QUANTUM COMPUTING

Engineering Challenges

- Significant technological problems to overcome

  - Long-living Qubits for memory and communication
  - Providing separations to control decoherence due to quantum tunneling
  - Scalable implementations
  - Costs associated with cooling to absolute zero
    - 10 mK = - 460 F (100 times colder then interstellar space)
  - New quantum models of computations
  - Better quantum error-correction
  - New algorithms
    - Finding quantum algorithms that achieve a speed-up
    - Some problems do not allow for a quantum speed-up
  - Getting funding

QUANTUM COMPUTING

The good stuff…

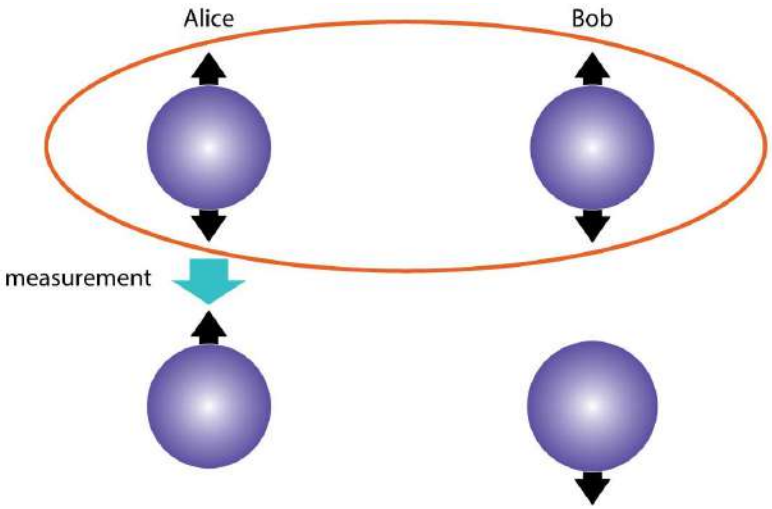
- Simulations of quantum-mechanical systems
- Speed-up simulation-driven design
- Applications in almost everything: medicine, material science, …etc
- Simulation of new catalysts that can capture carbon from the atmosphere to help solve global warming
- More powerful forms of artificial intelligence
- Solve problems where patterns cannot be seen (without data)
- Sort through unordered databases

QUANTUM CRYPTOGRAPHY

QUANTUM KEY CRYPTOGRAPHY

…using entangled photons?

- Hypothesis:
  - A quantum communication satellite sends and a pair of quantum entangled photons to Alice and Bob
  - Alice and Bob are now able to come up with a shared quantum key based on the entangled photons
  - Alice uses the key to encrypt the message and sends it to Bob on the public channel
  - Bob uses the key to decrypt the message
  - Alice and Bob will be able to detect if anyone has spied on the quantum channel used to determine the key



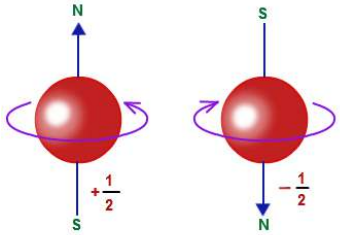
- Security is based on properties of physics rather then any mathematical method of encryption

http://www.sciencemag.org/news/2015/08/more-evidence-support-quantum-theory-s-spooky-action-distance

QUANTUM KEY CRYPTOGRAPHY

…using entangled photons?

Basis	0	1
+	↑	→
×	↗	↘



Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↘	↗	→	↗	→	→
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		1			0		1

https://en.wikipedia.org/wiki/Quantum_key_distribution

QUANTUM KEY CRYPTOGRAPHY

…using entangled photons?

Alice
(sender)

Plaintext

Encryption Algorithm

Key

Quantum State Generator

Eve (Eavesdropper)

Public Channel
(internet)

Ciphertext

Quantum Channel
(optical fiber or free space)

Bob
(receiver)

Plaintext

Decryption Algorithm

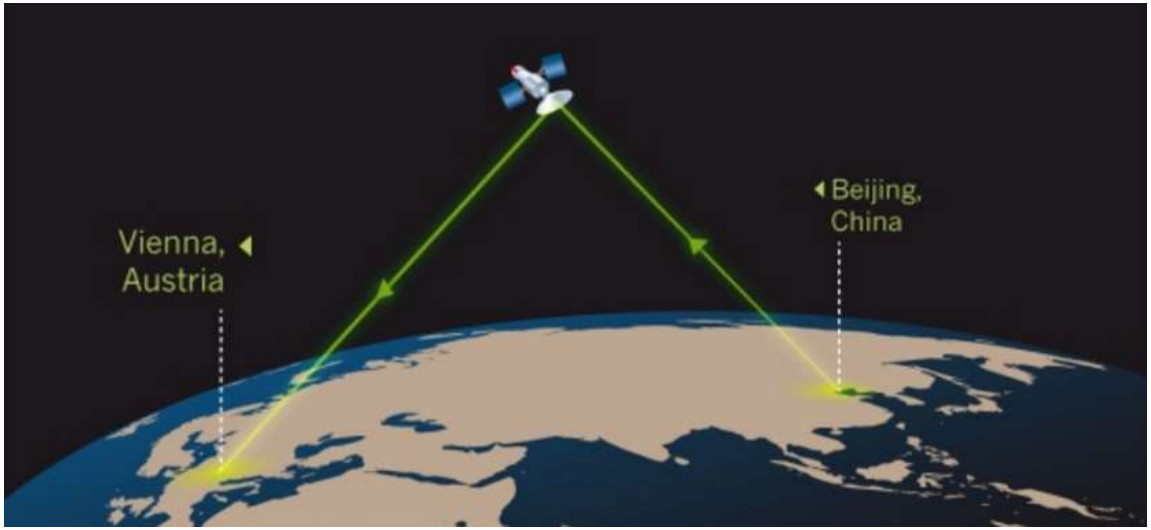
Key

Quantum State Detector

QUANTUM KEY DISTRIBUTION

- At the heart the satellite is a crystal that produces pairs of entangled photons, whose properties remain entwined however far apart they are separated. The first task will be to fire the partners in these pairs to ground-stations in Beijing and Vienna, and use them to generate a secret key.

http://www.nature.com/news/chinese-satellite-is-one-giant-step-for-the-quantum-internet-1.20329



http://www.nature.com/polopoly_fs/7.7775.1355230159!/slideshowimage/quantum%E2%80%933.jpg_gen/derivatives/landscape_592/quantum%E2%80%933.jpg

A MATTER OF TIME…?