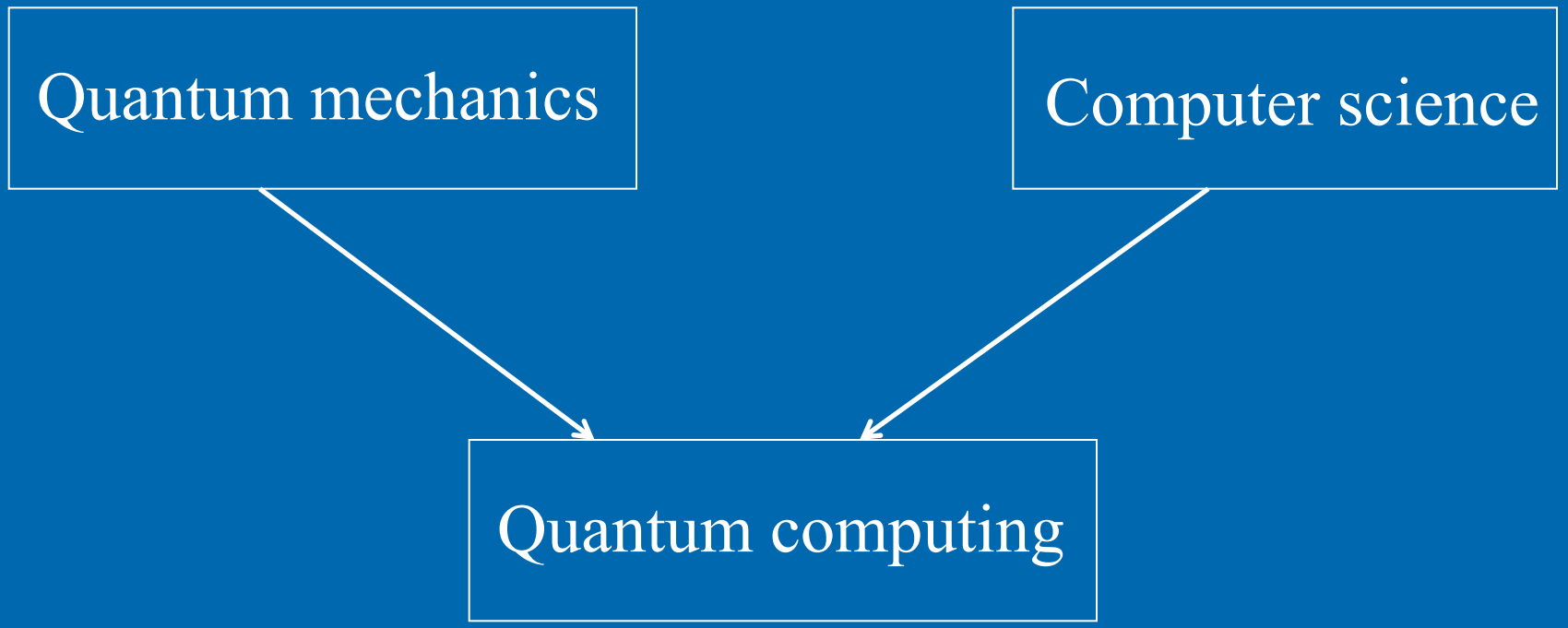
Quantum techonologies and their impact on cybersecurity

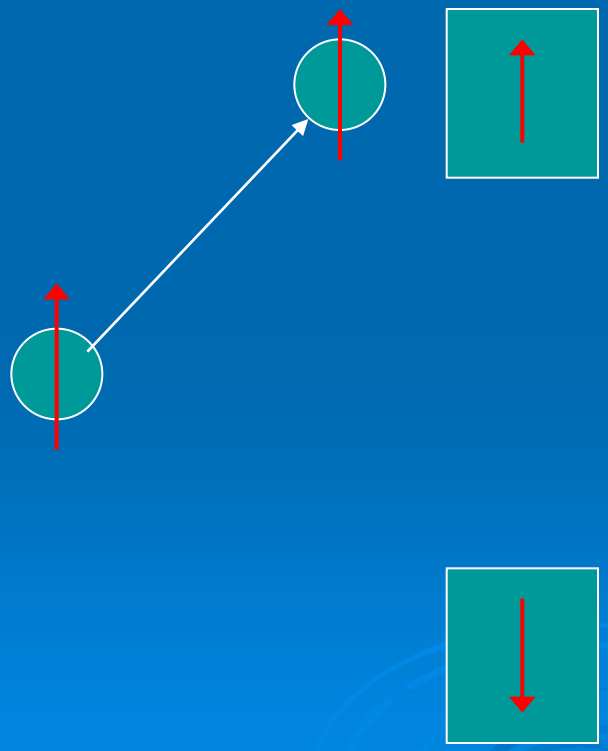
Andris Ambainis
University of Latvia



Using quantum effects for computing and communication.

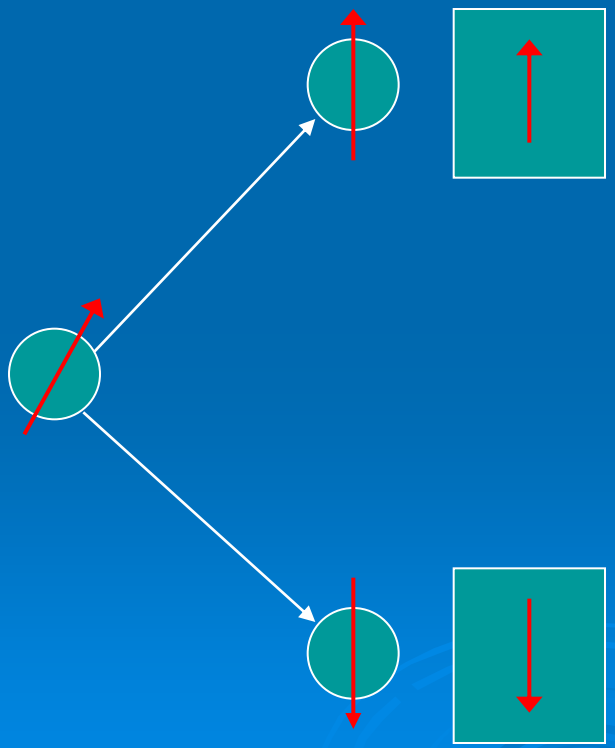
Quantum mechanics

Measuring a quantum state changes the state that is being measured.

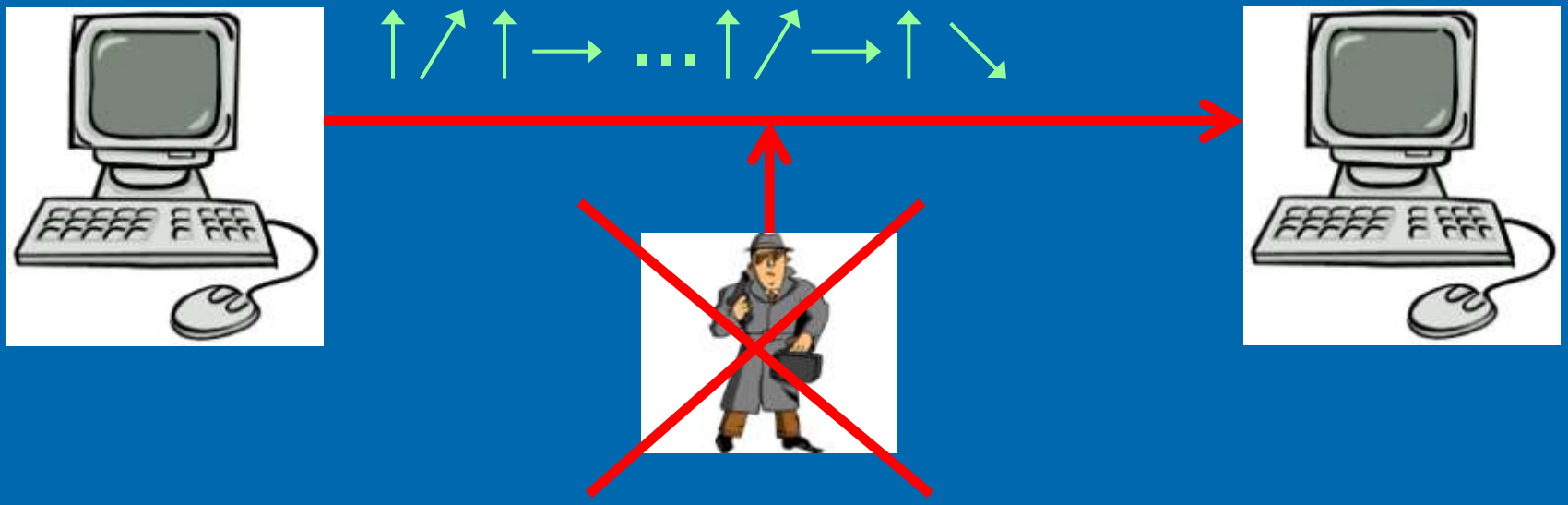


Quantum mechanics

Measuring a quantum state changes the state that is being measured.

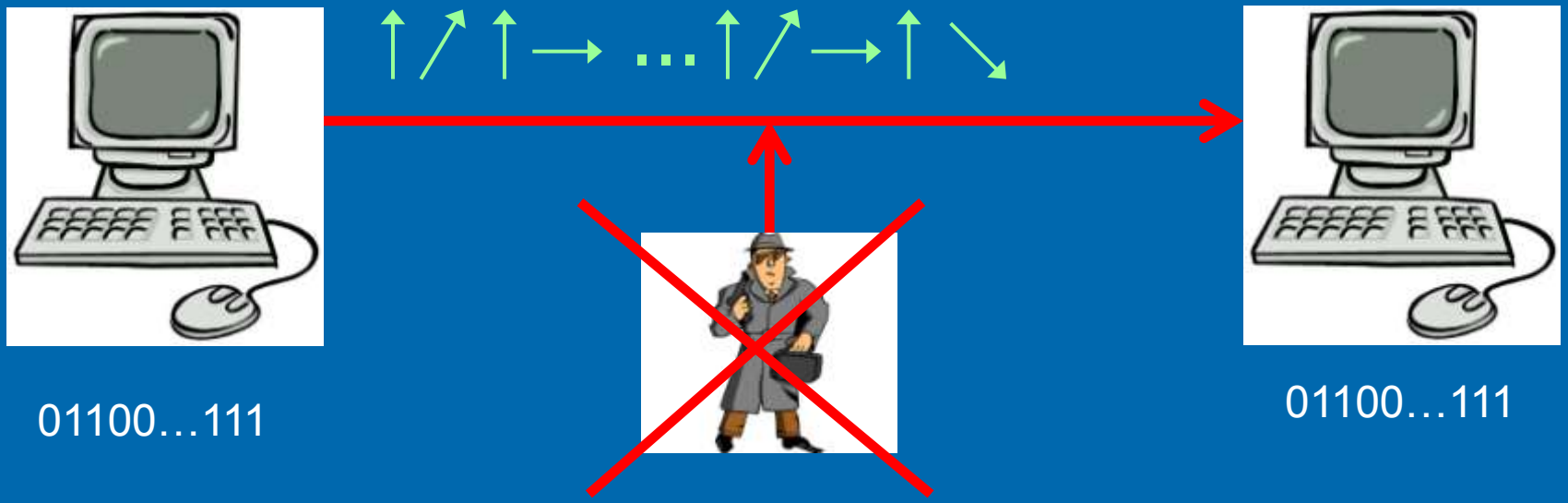


Quantum key distribution



- One side transmits a sequence of polarized photons.
- Some photons used to check for eavesdropping.

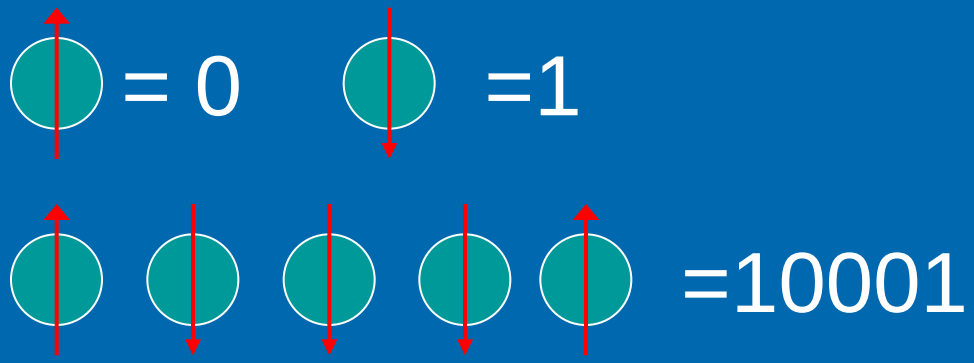
Quantum key distribution



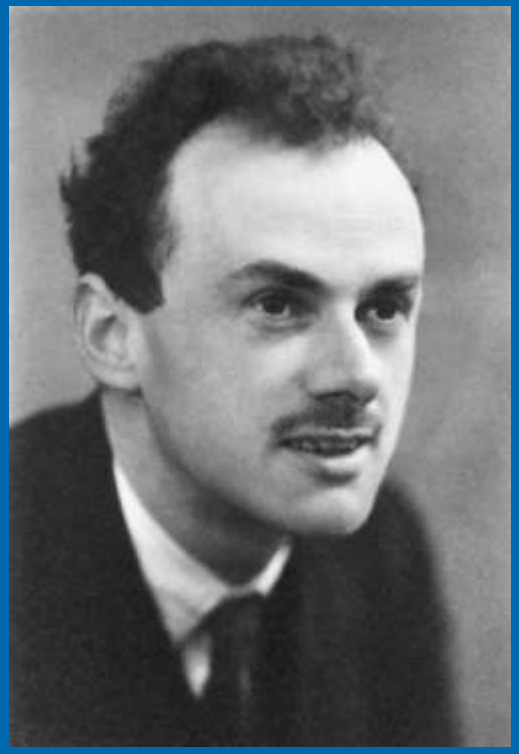
- The remaining photons are used for secret key.
- Two parties can communicate securely.

Quantum computing

- Encode 0 and 1 into quantum states:



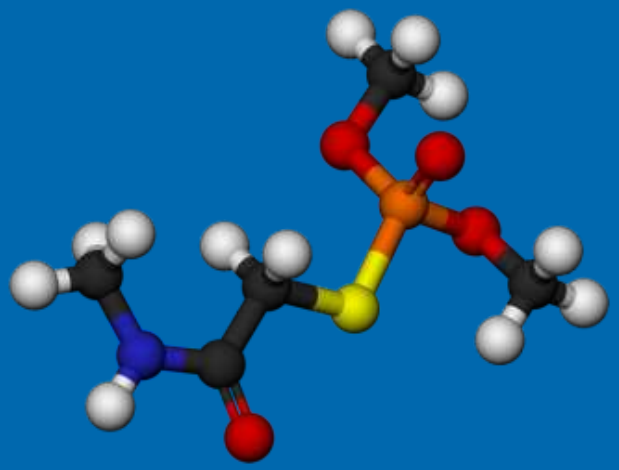
- Can be much faster than conventional computing.



Paul Dirac, 1929

The underlying physical laws ... for a large part of physics and the whole chemistry are thus completely known and the difficulty is only that the exact application of these laws leads to equations much too complicated to be soluble.

Quantum chemistry



$$H|\Psi\rangle = E|\Psi\rangle$$

Schrodinger's equation

10% of supercomputer time is quantum chemistry calculations

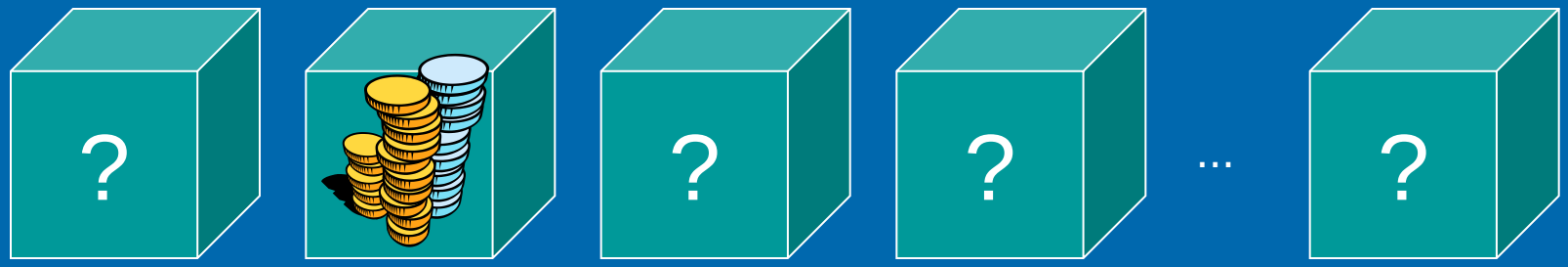
Factoring

- 6231540623 = 93599 * 66577.
- Given 6231540623, find factors?

Shor, 1994: quantum computers can factor large numbers efficiently.

Security of public key cryptography depends on factoring being difficult.

Quantum search



- N objects;
- Find an object with a certain property.

Grover, 1996: $O(\sqrt{N})$ quantum steps.

Who has the number 67033706?

Usual computer: N = 1,000,000 steps

Quantum computer: $\sqrt{N}$ = 1000

Quantum cryptography in practice

Commercially available systems

Id Quantique

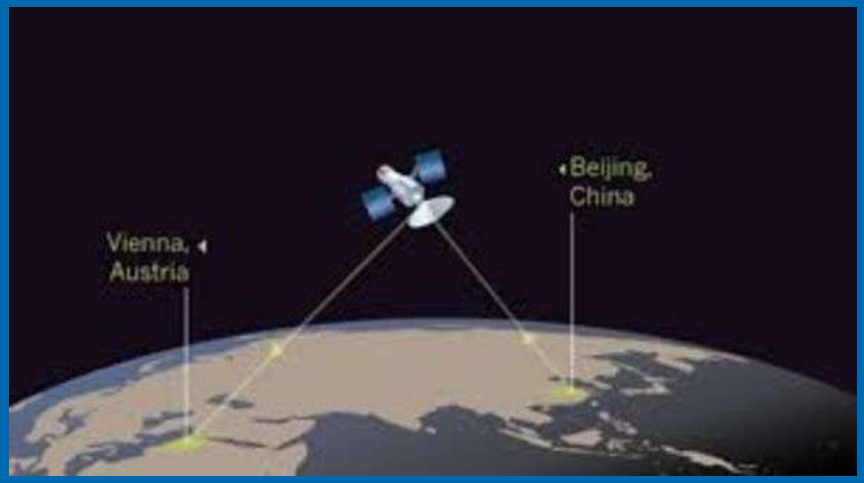
Toshiba

- Quantum communication over optical cable.
- 1Mb/s over 20km distance.
- 10 kb/s over 100km distance.

QKD deployments

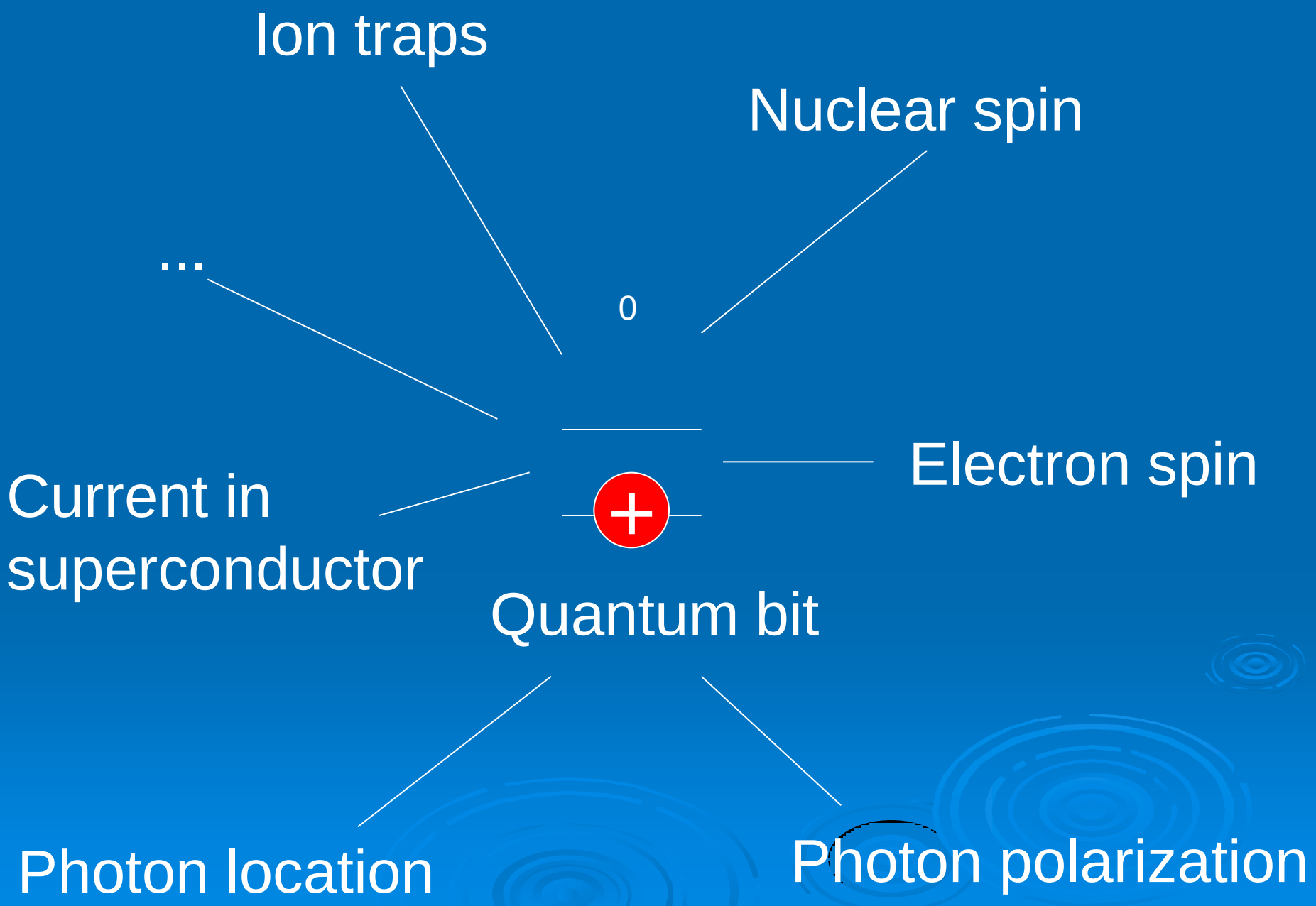
- DARPA-funded quantum network in Boston area, 2003.
- First commercial deployment, Siemens, 2010, between data centres in Netherlands.

QKD via satellites

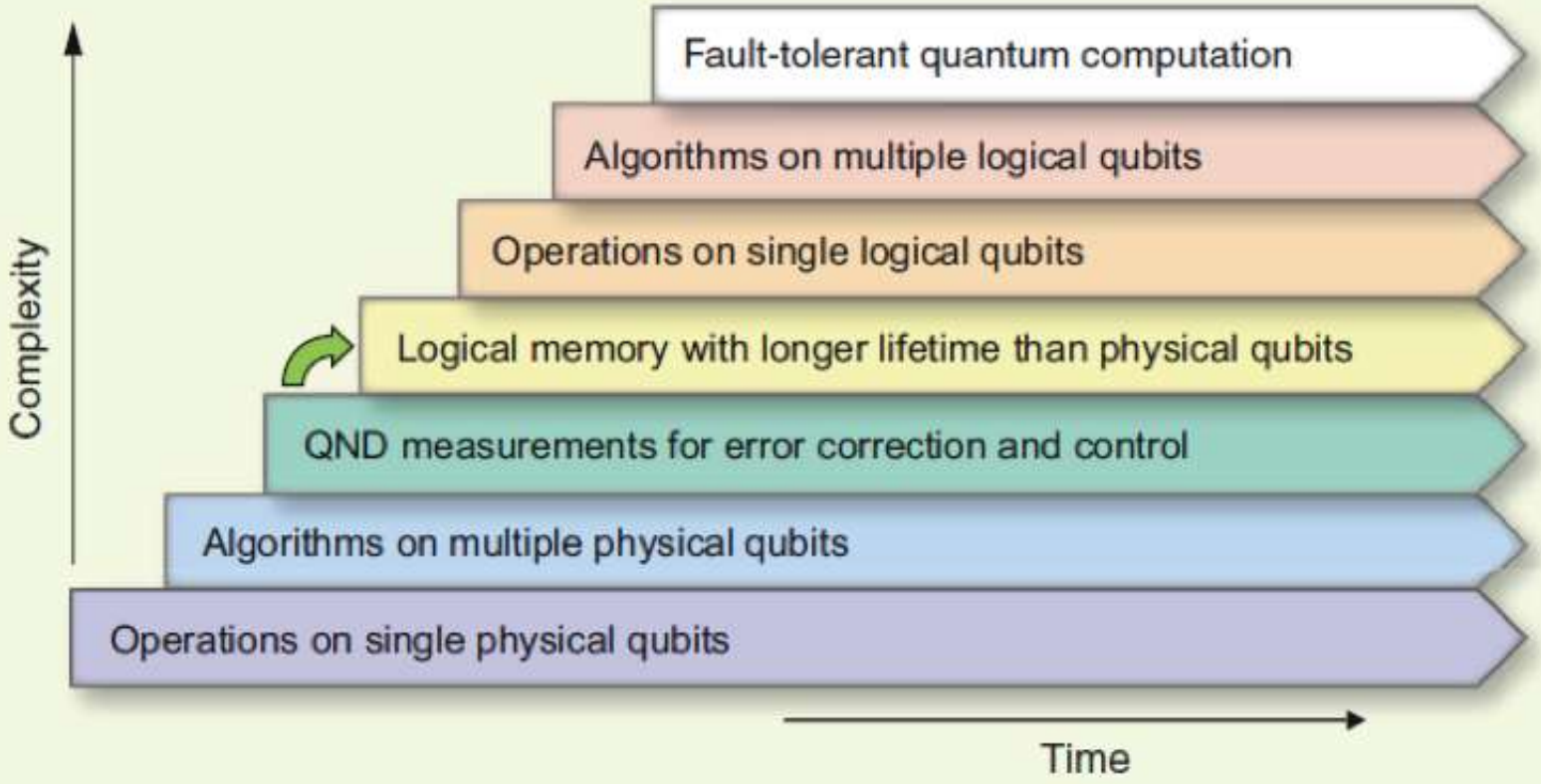


- Quantum Space Satelllite (China), launched August 2016.
- Plan for Beijing-Vienna QKD experiment.

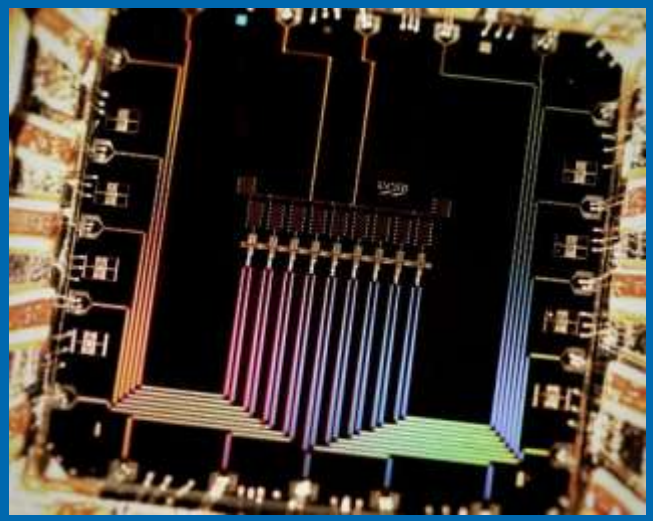
Building a quantum computer


Ion traps
Nuclear spin
...
0
Electron spin
Current in superconductor
Quantum bit
Photon location
Photon polarization

Schoelkopf's milestones (2012)



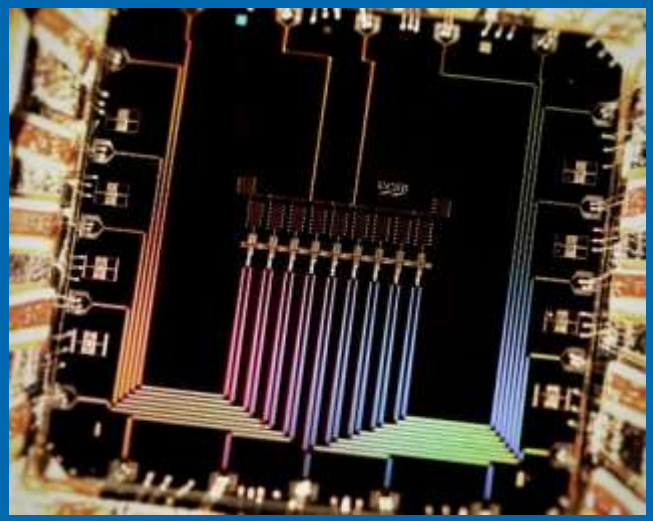
Superconductors



9 quantum bits (Martinis group, UC Santa Barbara)

- Materials that conduct electricity with no resistance.
- Electric current = quantum state.
- 0 = current in one direction, 1 = current in the other direction.

Superconducting qubits



9 quantum bits (Martinis group, UC Santa Barbara)

- Quantum gates with precision 99.4%-99.92%.
- Can be microfabricated using integrated circuit techniques.
- Possibility of mass manufacturing.

Google Partners With UCSB To Build Quantum Processors For Artificial Intelligence

Posted Sep 2, 2014 by Frederic Lardinois (@fredericl)

Intel invests $50m in the Delft University of Technology to advance quantum computing

By Danny Palmer 03 Sep 2015 Print Send

Alibaba Places Bet on Quantum Computing, Pledges to Invest 30 Million Yuan Annually

Monica Castro | Sep 05, 2015 07:43 AM EDT

Outlook

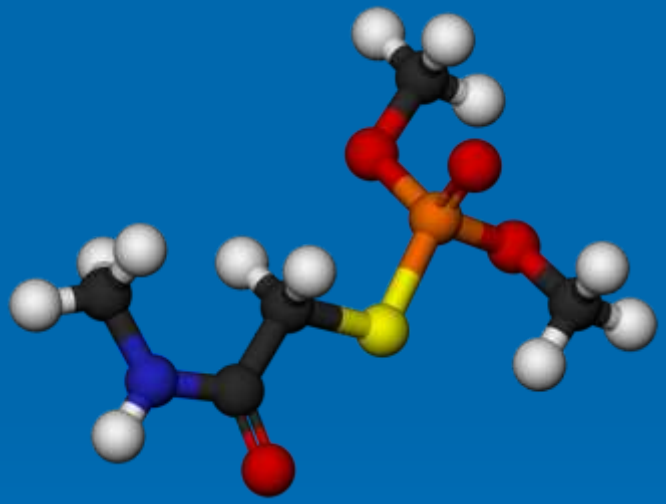
- Stage 1: quantum computer that is impossible to simulate classically.
- Stage 2: quantum computer that solves useful task.
- Stage 3: quantum computer that breaks RSA/etc.

Stage 1

- Quantum computer that is impossible to simulate classically.
- 50 quantum bits, can be noisy.
- Google: 1-2 years.

Stage 2

- Quantum computer that solves useful task.
- Most likely, quantum chemistry.



- 200-500 quantum bits, some form of error correction.

Stage 3

- Quantum computer that breaks RSA/other public key crypto.
- 4000-6000 quantum bits, good quantum error correction.

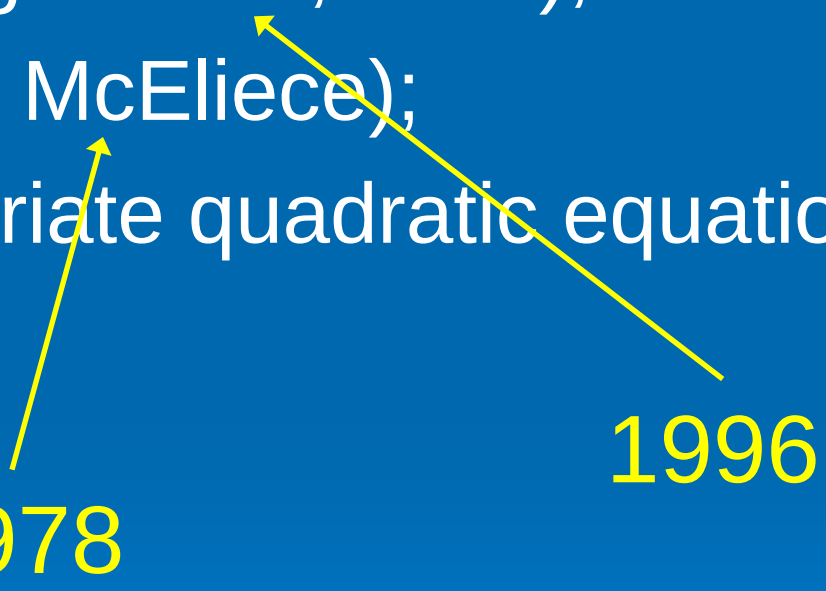
«Historically, it has taken a long time from deciding a cryptographic system is good until we actually get it out there as a disseminated standard in products on the market. It can take 10 to 20 years»

D. Moody, National Institute of Standards and Technology, USA

Post quantum cryptography

Methods for post quantum cryptography

- Lattice based (e.g. NTRU, LWE);
- Code based (e.g. McEliece);
- Based on multivariate quadratic equations (oil-and-vinegar);



Lattice/code based cryptography

- Can be based on many lattices/codes.
- Broken in some cases, looks secure in others.
- Moving to simpler lattices/codes improves efficiency, may damage security.

Soliloquy: very efficient lattice scheme by GCHQ, was discovered to be insecure

Experiments in PQ crypto

Google last week announced an experiment with post-quantum cryptography in Chrome. A small fraction of connections between Google's servers and Chrome on the desktop will use a post-quantum key-exchange algorithm in addition to the elliptic-curve key-exchange algorithm already being used.

Summary

- Substantial advances towards quantum computers/QKD devices;
- Time to think about post quantum cryptography.