Quantum Computers – Is the Future Here?

Tal Mor – CS.Technion

ISCQI

Feb. 2016

128 ?? [2011 ; sold to LM]

D-Wave Two :512 ?? [2013 ; sold to NASA + Google]

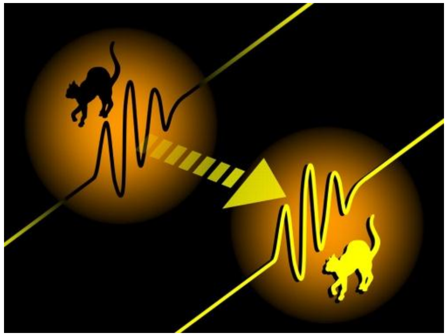
D-Wave Three: 1024 ?? [2015 ; also installed at NASA]

Goals of my talk

- Quantum information and computation – what for?
- Quantum Bits and Algorithms
- Implementations – Current Status
- "Semi-Quantum" Computing
- Conclusions

Quantum Information – what for?

- First, **quantum computers** can crack some of the strongest cryptographic systems (e.g. RSA)
- Second, they might be useful for various other things as well (simulating quantum systems etc.)
- **Quantum cryptography** provides new solutions to some cryptographic problems
- Quantum cryptography may **ALSO** become useful if (new) classical algorithms will crack RSA
- Quantum Teleportation and quantum ECC can enlarge distance for **secure** quantum communication
- Satellite quantum communication



CREDIT: Science/AAAS

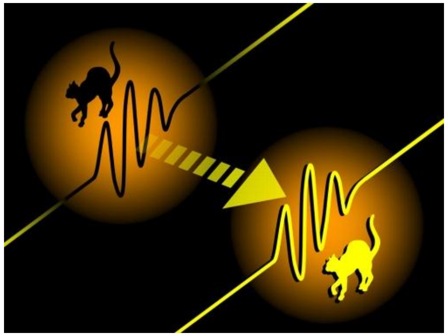
Quantum Computers – what for?

- Q**uantum computers** can **crack RSA** because they can factorize large numbers of **n** digits in polynomial time!

$$\mathbf{O(n^2 \log n)}$$

- A "classical computer will have to work "sub-exponenital time"

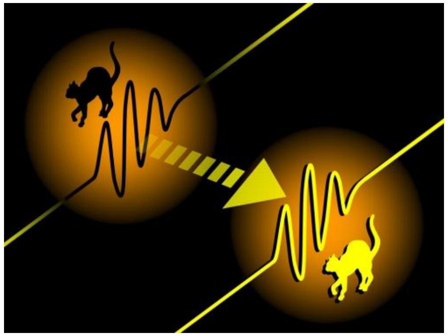
$$\mathbf{O(\exp[(n \log n)^{1/3}])}$$



CREDIT: Science/AAAS

Quantum Computers – what for? (2)

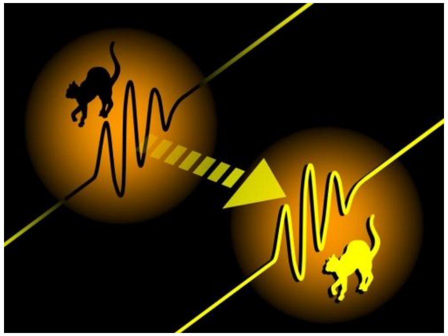
- Quantum computers might be useful for various other things as well….. Mainly - **simulating quantum systems**:
  - Fully understanding the complicated electronic structures of molecules and molecular systems
  - Predicting reaction properties and dynamics
  - Designing well controlled state preparation
  - Analyzing protein folding
  - Understanding photosynthetic systems
  - Etc. Etc. Etc.
- The **HOPE** is to have advantage already with 30-100 qubits



CREDIT: Science/AAAS

Quantum Computers – what for? (3)

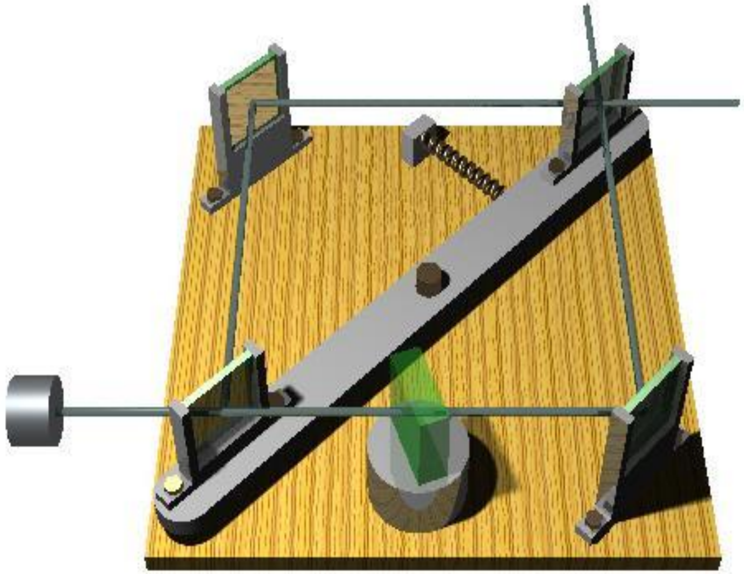
- Quantum algorithms applied onto small "quantum computers" might be useful for various QUANTUM TASKS….. Mainly - **manipulating quantum systems**:
  - Algorithmic cooling of spins, for improving MRI/MRS/NMR/ESR (that is one of my team's goals).
  - As said before: quantum ECC (error correcting codes) can much enlarge the distance for secure quantum communication



CREDIT: Science/AAAS

The Qubit

In addition to the regular values {0,1} of a bit, and a ***probability distribution*** over these values, the Quantum bit can also be in a **superposition**

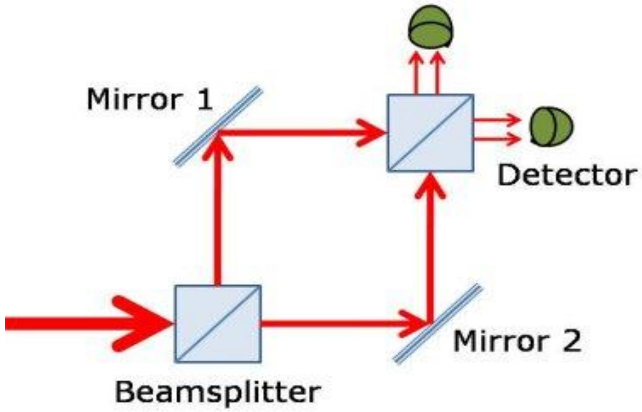


www.cqed.org/IMG/jpg/compdoublemobilemz.jpg

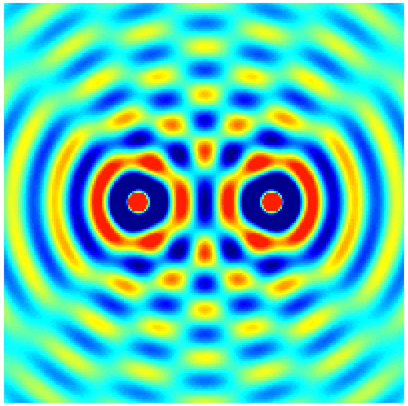
The Qubit (2)

A superposition state $\alpha|0\rangle + \beta|1\rangle$

Intereference (as in waves)



scienceblogs.com

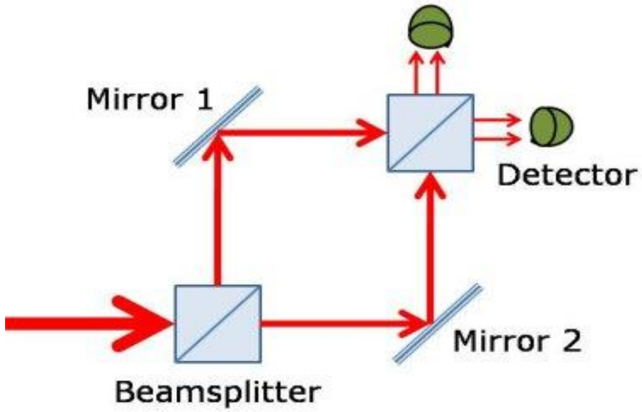


http ://upload.wikimedia.org/wikipedia/commons/2/2c/Two_sources_interference.gif

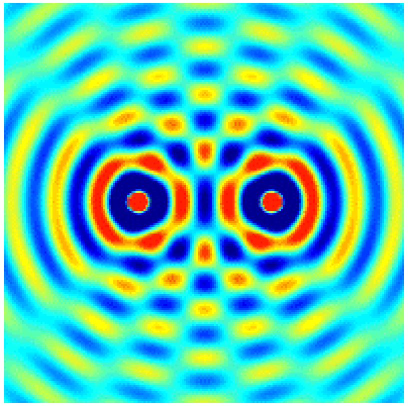
The Qubit (2)

A superposition state $\alpha|0\rangle + \beta|1\rangle$

Intereference (as in waves)



scienceblogs.com

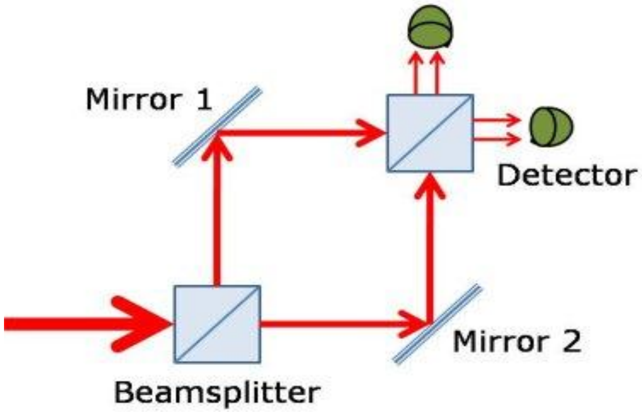


http ://upload.wikimedia.org/wikipedia/commons/2/2c/Two_sources_interference.gif

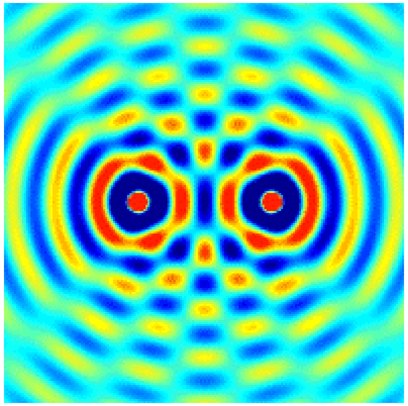
The Qubit (2)

A superposition state $\alpha|0\rangle + \beta|1\rangle$

… with $|\alpha|^2 + |\beta|^2 = 1$



scienceblogs.com

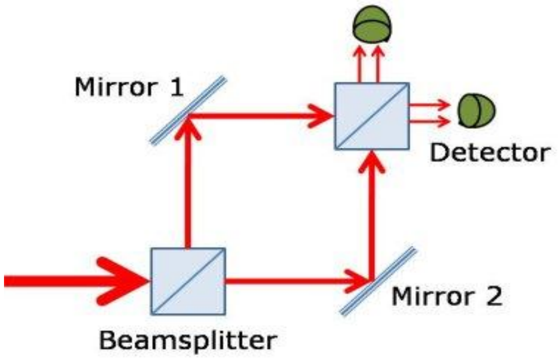


http ://upload.wikimedia.org/wikipedia/commons/2/2c/Two_sources_interference.gif

The Qubit (3)

- The two arms meet - there is an interference
- This is so due to Linearity of quantum mechanics
- $|0\rangle \rightarrow |+\rangle = (1/\sqrt{2})\,|0\rangle + (1/\sqrt{2})\,|1\rangle$

  $|1\rangle \rightarrow |-\rangle = (1/\sqrt{2})\,|0\rangle - (1/\sqrt{2})\,|1\rangle$



- We get

$|+\rangle = (1/\sqrt{2})\,|0\rangle + (1/\sqrt{2})\,|1\rangle \rightarrow$

$(1/\sqrt{2})\,[(1/\sqrt{2})\,|0\rangle + (1/\sqrt{2})\,|1\rangle] + (1/\sqrt{2})\,[(1/\sqrt{2})\,|0\rangle - (1/\sqrt{2})\,|1\rangle]$

$= |0\rangle$ **"Constructive/Destructive Interference"**

Two Qubits - Entanglement

$$\alpha|00\rangle + \beta|11\rangle$$

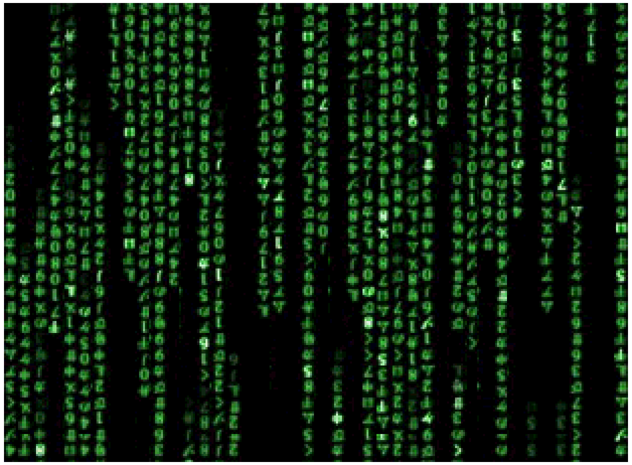
brusselsjournal.com

n Qubits – parallel computing

- Prepare a superposition over 2^n states
- Run your algorithm in parallel …
- Interference enhances the probability of the desired solution
- Peter Shor factorized large numbers (in principle) using Shor's algorithm!
- Several other problems in NP were also solved
- Current quantum architectures reach 13-14 qubits (NMR, ion trap); far from being practical…

Will quantum computers factorize large numbers?

- If ‘yes’ – this is a revolution in Computer Science
- If ‘never’ – this is a revolution in Physics
- So let’s assume it will… but maybe not so soon!
- Can we predict when?

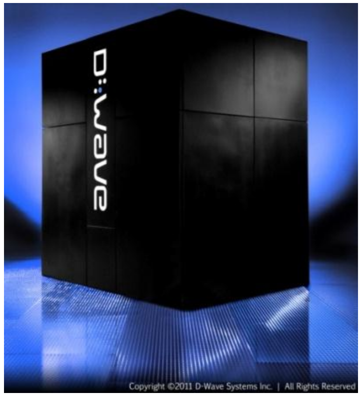


Implementations

1. Ion trap (qubit is the ground-state vs excited-state of an electron attached to an ion; “many” ions in one trap)
2. NMR (qubit is the spin of a nuclei on a molecule; “many” spins on a molecule)
3. Josephson-Junction qubits (magnetic flux)
4. Optical qubits (photons)

- Etc…

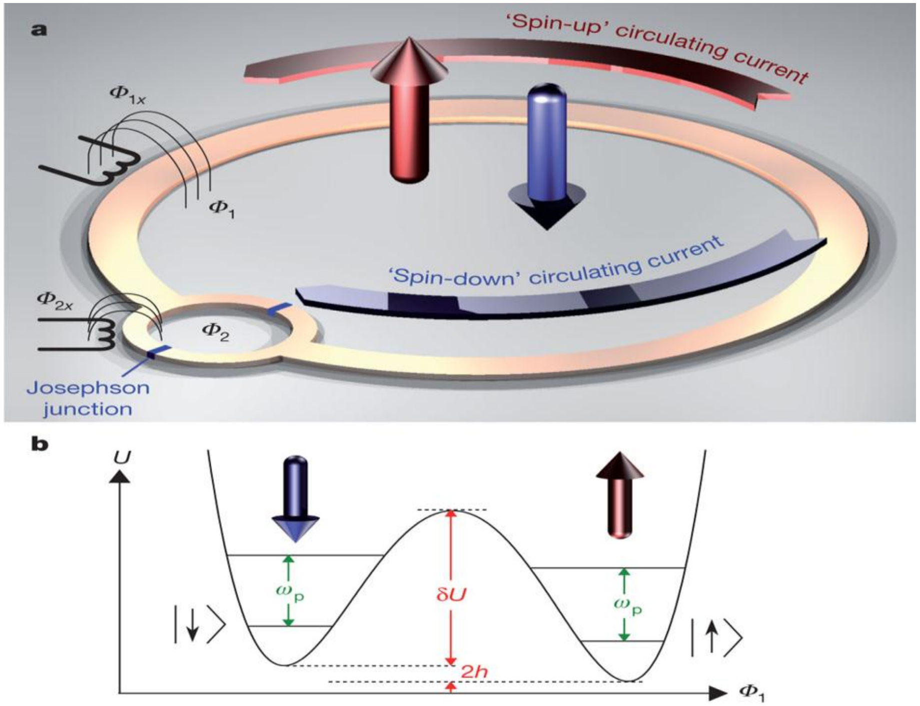
D-Wave collaborations (Wikipedia)



In 2011 ,**Lockheed Martin** signed a contract with D-Wave Systems to realize the benefits based upon a **quantum annealing processor** applied to some of Lockheed's most challenging computation problems. The contract includes the purchase of a "***128 qubit*** Quantum Computing System".

In 2013, a "*512 qubit* system" was sold to Google and NASA.

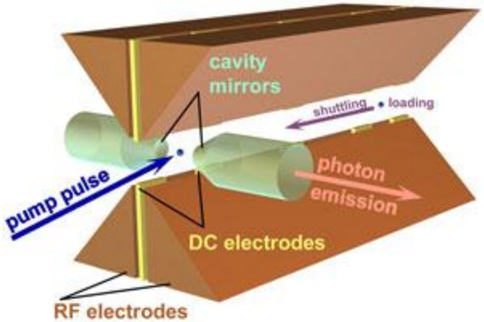
D-WAVE: Superconducting flux **qubit**



MW Johnson *et al.* ***Nature*** **473**, 194-198 (May 2011)
However, their "qubits" are **highly limited**. Similar Technology with less limited qubits reached **4-9 qubits**, no more!

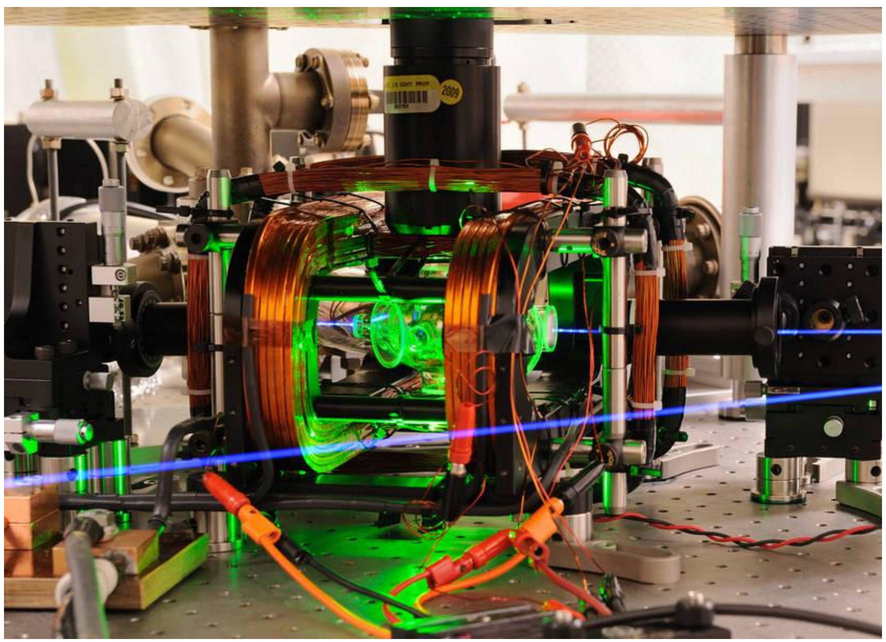
So what is the TRUTH??

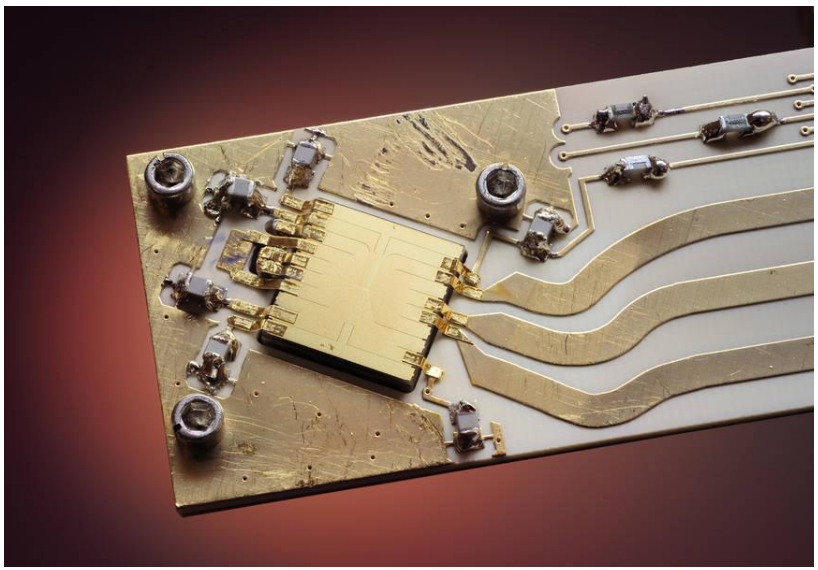
Example – ion trap



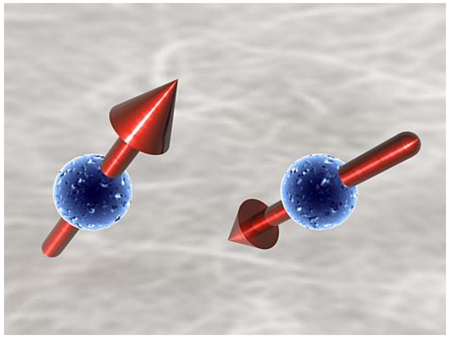
sciencedaily.com

- Reached 14 qubits
- Nobel Prize and Wolf Prize
- Still – progress is very slow



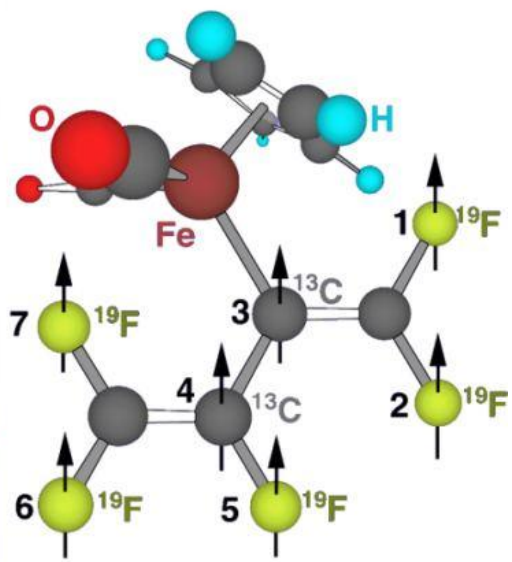


Example - NMR



- Reached 13 qubits
- Scalability problem
- Resolved via *Algorithmic Cooling*

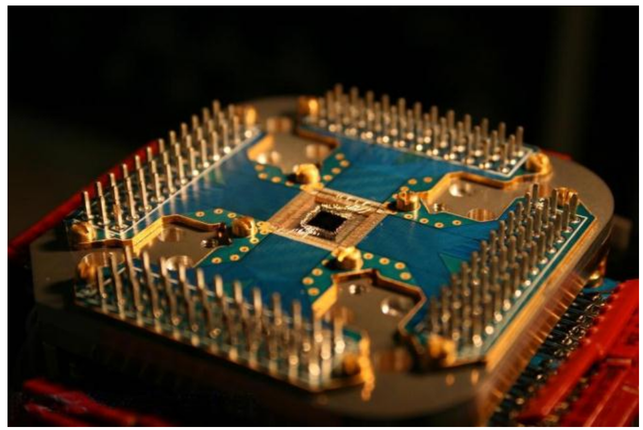
tudelft.nl

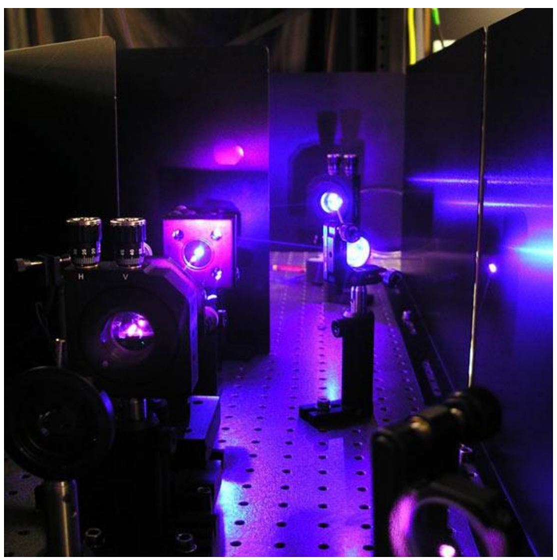


robert.nowotniak.com

Examples 3+4

- **Josephson Junctions (4-9 qubits)**





- **Q. Optics (6-7 qubits)**
- **Sufficient for some ECC**

Current status of fully-quantum computing

- Despite the Nobel prize – we have no clue when ion traps (etc.) will reach 25 qubits
- Despite of 20M $ DWAVE computers already sold – we have no clue if JJ qubits are of any good; We do know (Shin, Smith Smolin, Vazirani; 2014) that there is probably no reason to believe that the DWAVE model is **quantum**.

Limited QC Models: <u>Semi-quantum (or sub-universal-quantum) computing</u>

- D-Wave’s AQC [???] (closely related to JJ)
- One Clean Qubit * (closely related to NMR)
- Linear Optics (closely related to Q. Optics)
- Commuting quantum computation
- Various quantum simulators [???]

Limited QC Models: <u>Semi-quantum (or sub-universal-quantum) computing</u>

Five Extremely Important Questions:

- What algorithms can the <u>limited</u> models run?

[OCQ – Trace estimation; LO – boson sampling]

- Why do we believe a classical computer cannot?
- What kind of Quantumness/Entanglement is there?
- Do they scale much easier/better than full QC?
- How can we know if a machine (or a model) is classical/ quantum/ semi-quantum?

Conclusions

- Zero conclusions about the future of full QC
- Some optimism about semi-quantum computing? Maybe
- Many more questions than answers, both theoretically and experimentally

Thanks