Quantum Computing

(and Quantum Information Science)

Presented to the

Advanced Scientific Computing Advisory Committee

by

Steve Binkley
Associate Director

April 5, 2016

Post-Moore's Law Computing: What comes after exascale?

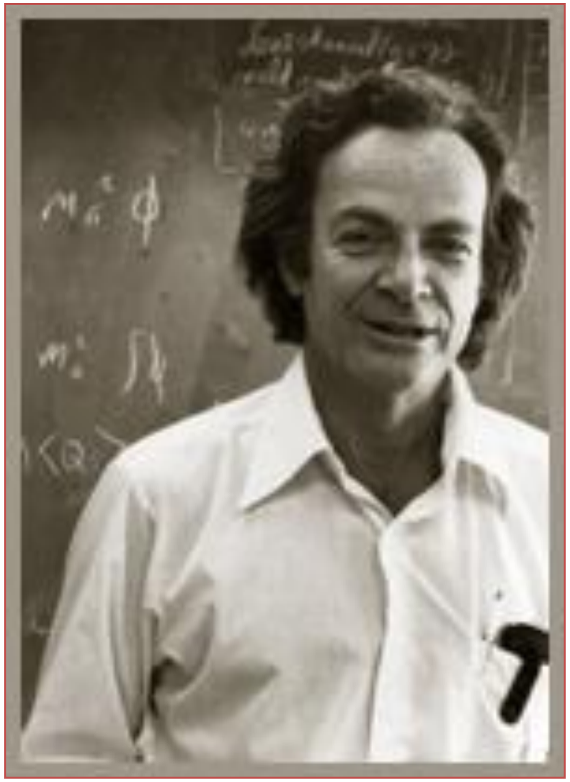
- CMOS lithographic feature sizes are approaching fundamental limits
  - Currently at 14 nm (both Intel and Nvidia)
  - 10 nm is projected for ~2016 (both Intel and Nvidia)
    - However, gate lengths may be smaller than 6 nm – corresponding gate dielectric thickness may reach a monolayer or less
  - The industry roadmap reaches beyond 10 nm (7 nm and 5 nm) but may be unattainable
    - Non-silicon extensions of CMOS, e.g., using III-V materials or nanotubes/nanowires or non-CMOS technologies, including molecular electronics, spin-based computing, single-electron devices, and graphene have been proposed
    - At scales of ~7-5 nm, quantum tunneling may become significant
  - Capital costs for tooling are increasing dramatically as feature sizes shrink
- Options:
  - Computing using superconducting technologies
  - Quantum computing/quantum information science
  - Neuromorphic computing
  - Probabilistic computing
  - ???

Considerable R&D required

Future Computing Technologies are Important to DOE

- **High-performance computing & simulation underpin DOE missions in energy, environment, and national security**
  - Historical role of computing in DOE
  - DOE/vendor synergies in deploying computing technologies
- **Future computing technologies (e.g., quantum, neuromorphic, probabilistic, etc.) hold promise for next-generation DOE mission applications**
  - Likely will augment, not replace, conventional supercomputing
  - Could open new avenues for use of computing in science (data analytics, machine learning, …)
- **New directions for applied mathematics and computer science are likely to emerge**
  - Community engagement has started and will continue
  - DOE needs to hear your views – stay tuned for further community engagement

Brief History of Quantum Computing



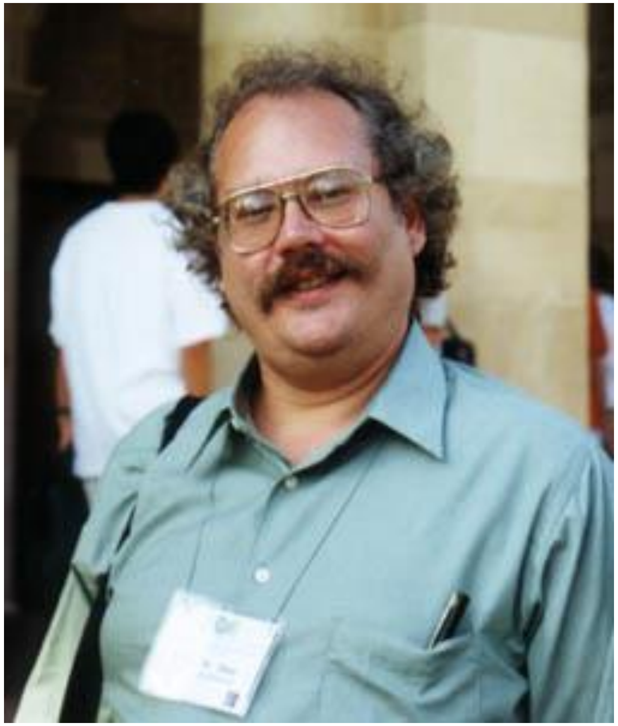
Origins trace to remarks and papers by Richard Feynman (1982):

"... and if you want to make a simulation of Nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy."[1]

---

[1] "Simulating Physics with Computers," International Journal of Theoretical Physics, VoL 21, Nos. 6/7, 1982

Shor’s Algorithm (1994)



Peter Shor (AT&T, 1994[1]):

In principle, with a quantum computer (assuming one can be built), one can factor an N-digit number in ~ N^3 steps …

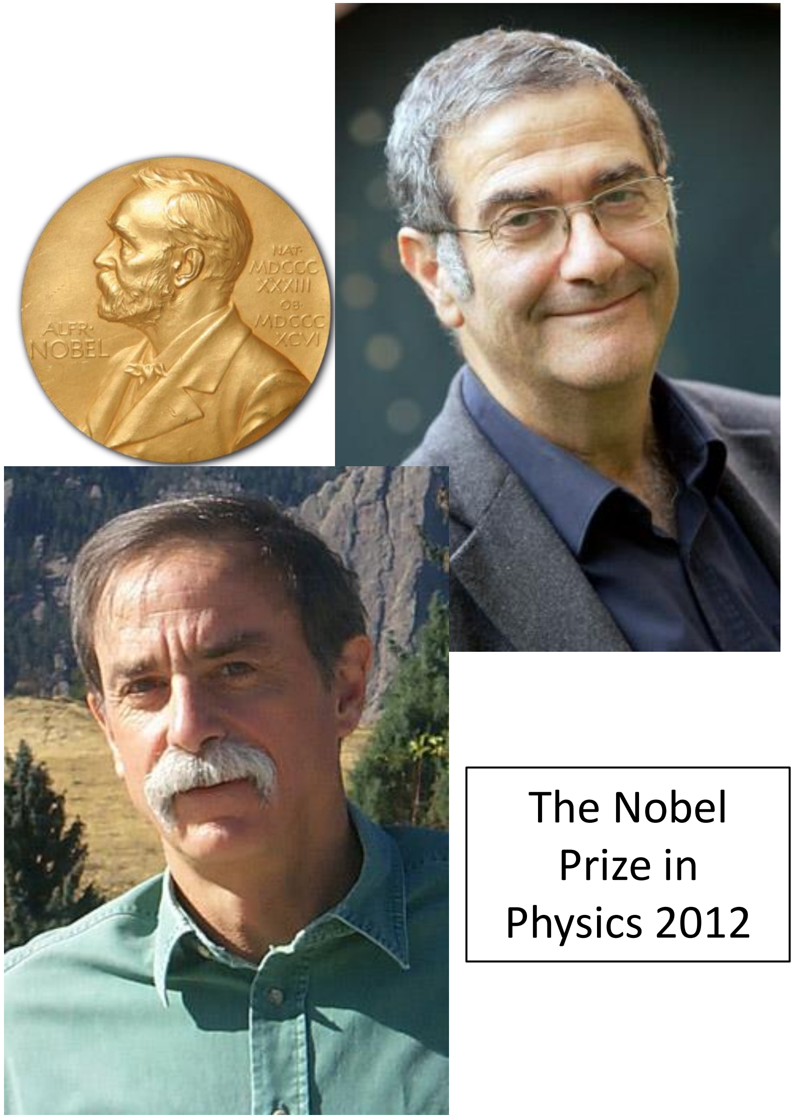
First quantum algorithm to tackle an important problem that is classically computationally hard – *i.e.,* grows exponentially in the length of an input string

---

[1] Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, Nov. 20--22, 1994

Early Progress on Quantum Computing (1994-1995)

- Dec. 1994: Cirac and Zoller propose the first controlled-NOT (2-qubit) gate for trapped ions
- 1995: Serge Haroche suggests that QC will not work since one cannot correct quantum errors (no-cloning theorem)
- 1995: Shor and Steane propose quantum error correction
- 1995: Chris Monroe and David Wineland realize the first 2-qubit quantum logic gate based on the proposal of Cirac and Zoller



The Nobel
Prize in
Physics 2012

Satisfying the “Five DiVincenzo Criteria”[1]

The challenge:

1. **Scalable** physical system with **well characterized** qubits
2. The ability to initialize the state of the qubits
3. **Long coherence times** relative to gate operation time
4. A universal set of quantum gates
5. A qubit-specific measurement capability

---

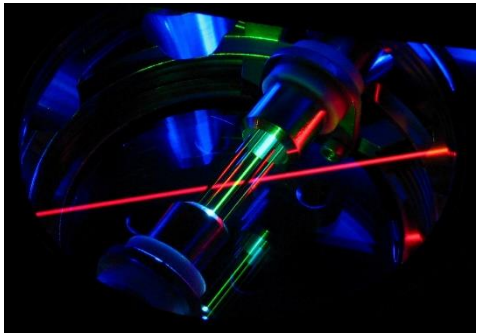
[1] "The Physical Implementation of Quantum Computation," Fortschritte der Physik, Volume 48, Issue 9-11, p.771-783 (2000)

Many proposed qubits

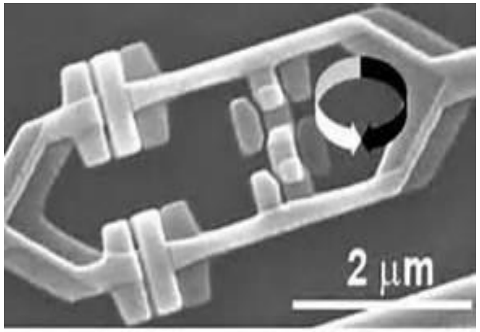
1. Cold atoms or ions in traps
2. Nuclear spins-NMR (considered limited)
3. Photon based qubits (polarization)
4. Superconductivity based qubits
    - RF squid
    - Charge
    - Phase
5. Semiconducting based qubits
    - Electrons bound to impurities in Silicon
    - Quantum Dots containing one electron
6. Electrons on Liquid ^{4}He surface
7. Topological qubits
8. …

Materials for Quantum Computing

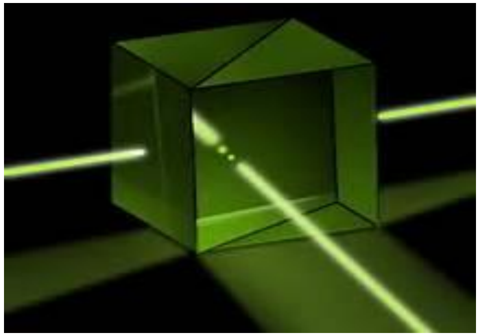
Ion traps



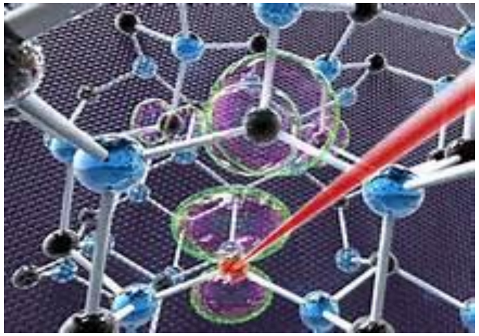
Super-conductors



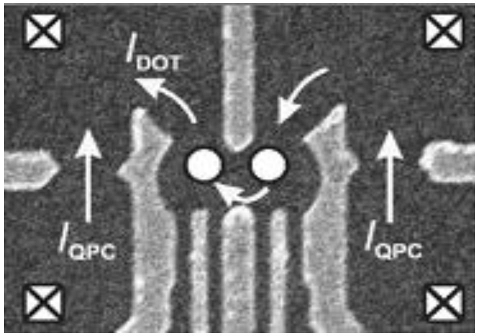
Linear optics



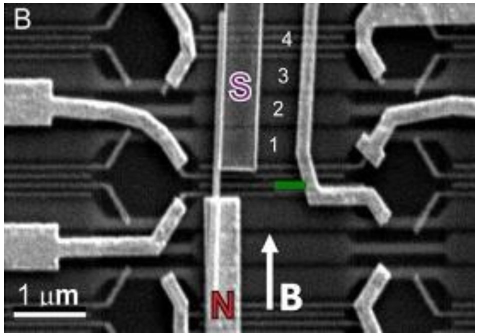
NV centers



Quantum dots



Topological



Quantum Computing is Multidisciplinary

- **Practical quantum computers require new technologies**
  - New materials for quantum devices, and fabrication capabilities
  - qubit manipulation, error correction
  - Software
  - Large-scale cryogenics
  - Ultrapure materials
  - Quantum controls
  - System integration
  - …
- **Spans multiple disciplines**
  - Computer science, applied mathematics, networking, information science
  - Materials sciences (new materials)
  - Quantum engineering
  - High-energy physics (advances in quantum theory)

Impacts of Quantum Computing

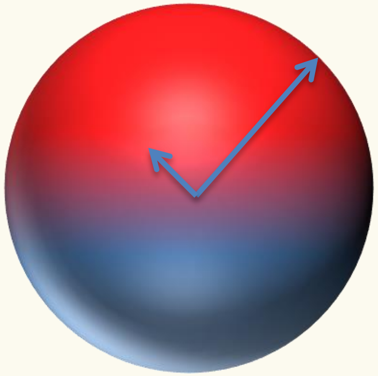
- ***National and economic security:***
  - Quantum computers could break all present-day public key encryption systems
  - Quantum encryption not susceptible to computational attack
- ***Physical sciences:***
  - Quantum simulations: materials design, pharmaceutical design, chemical processes, etc. – any problem that involves quantum mechanics
  - Broad non-computing impacts in new sensor and detector technologies:
    - Diamond NV (nitrogen-vacancy) centers are leading to previously unimaginable magnetic imaging systems
    - Chip-scale atomic clocks – precision timekeeping
    - Exquisitely sensitive magnetometers, accelerometers, gravimeters
    - Fundamentally new detectors and sensors in physical sciences, based on superposition, entanglement, and squeezing

Quantum Computing

🔴 1 = on

🔵 0 = off

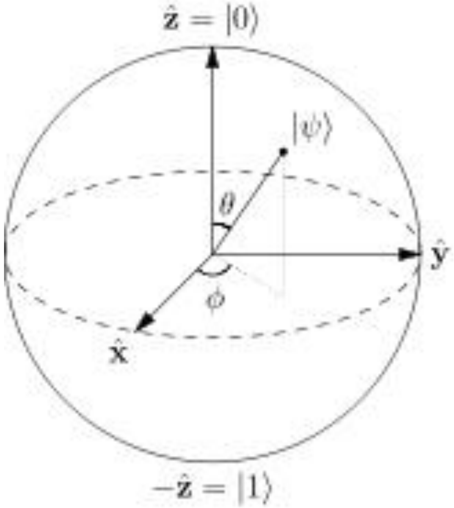
Classical “bits”



$$|Y\rangle = a|0\rangle + b|1\rangle$$

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

Quantum “qubits”: state superposition



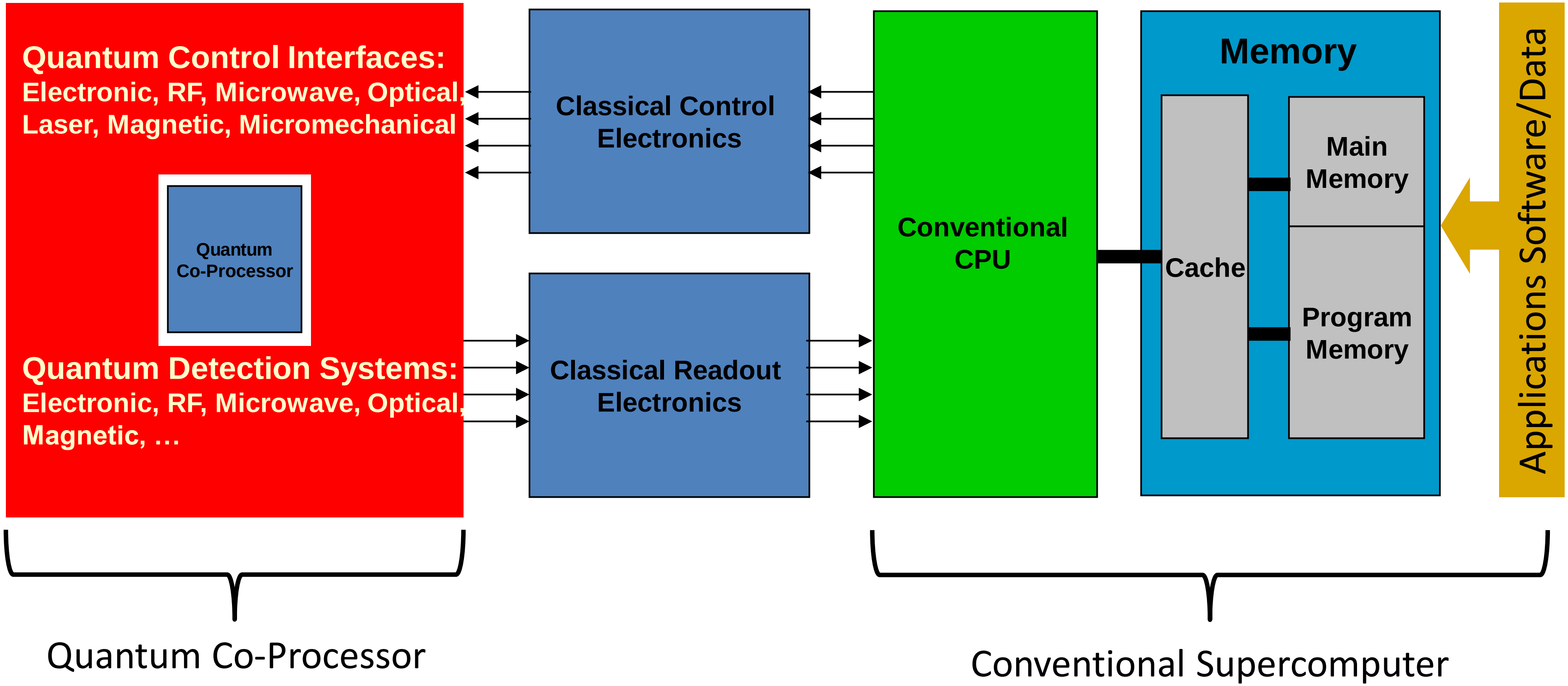
Classical vs. Quantum Computing*

Classical	Quantum
Basic unit: **bit** = 0 or 1	Basic unit: **qubit** = unit vector α|0> + β|1>
Computing: **logical** operation	Computing: **unitary** operation
Description: **truth table**	Description: **unitary matrix**
Direction: most gates run only **forward**	Direction: most gates **reversible**
Copying: independent copies are easy	Copying: independent copies **impossible**
Noise: manageable with minimal ECC	Noise: difficult to overcome
Input/Output: linear	Input: linear, Output: probabilistic
Storage: n bits store single value from 0 to 2^n-1	Storage: n bits can hold **2^n** values
Computation:	Computation:
An n-bit ALU: one operation/cycle	An n-qubit ALU: **2^n** operations/cycle

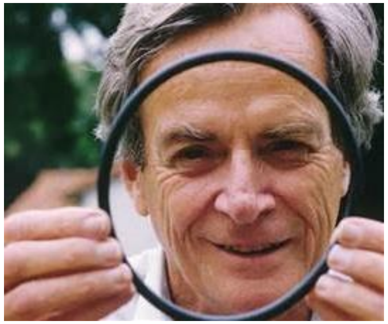
*Svore, Microsoft Corporation, 2015

Notional Quantum Computer

- Would more closely resemble a massive computer-controlled quantum physics experiment than a classical computing engine
- Would have a large external classical control computer that will drive a quantum core



DOE-Relevant Quantum Computing Applications

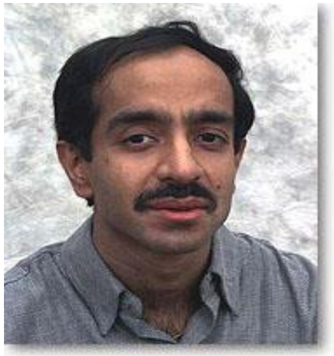


FEYNMAN QUANTUM SIMULATION: 1982

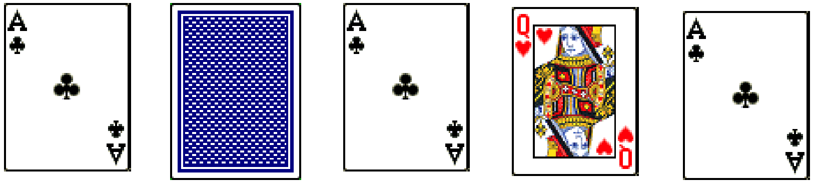
- Simulate physical systems in a quantum mechanical device
- Exponential speedups

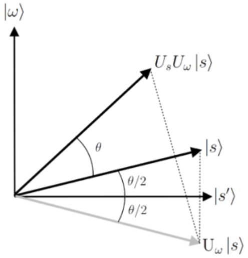
LLOYD, et al., LINEAR EQUATIONS SOLVER: 2010

- Applications shown for electromagnetic wave scattering
- Exponential speedups

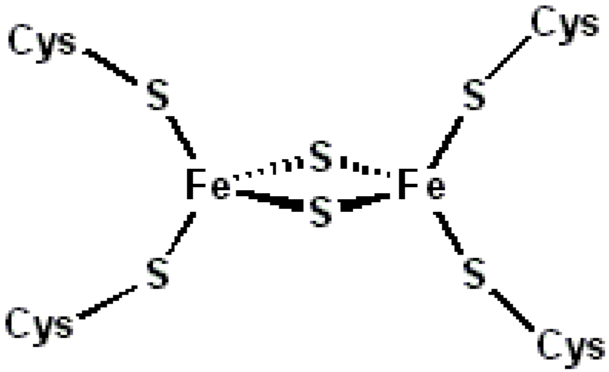


GROVER'S SEARCH ALGORITHM:1996



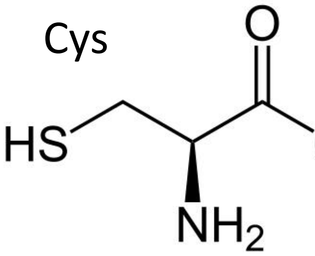


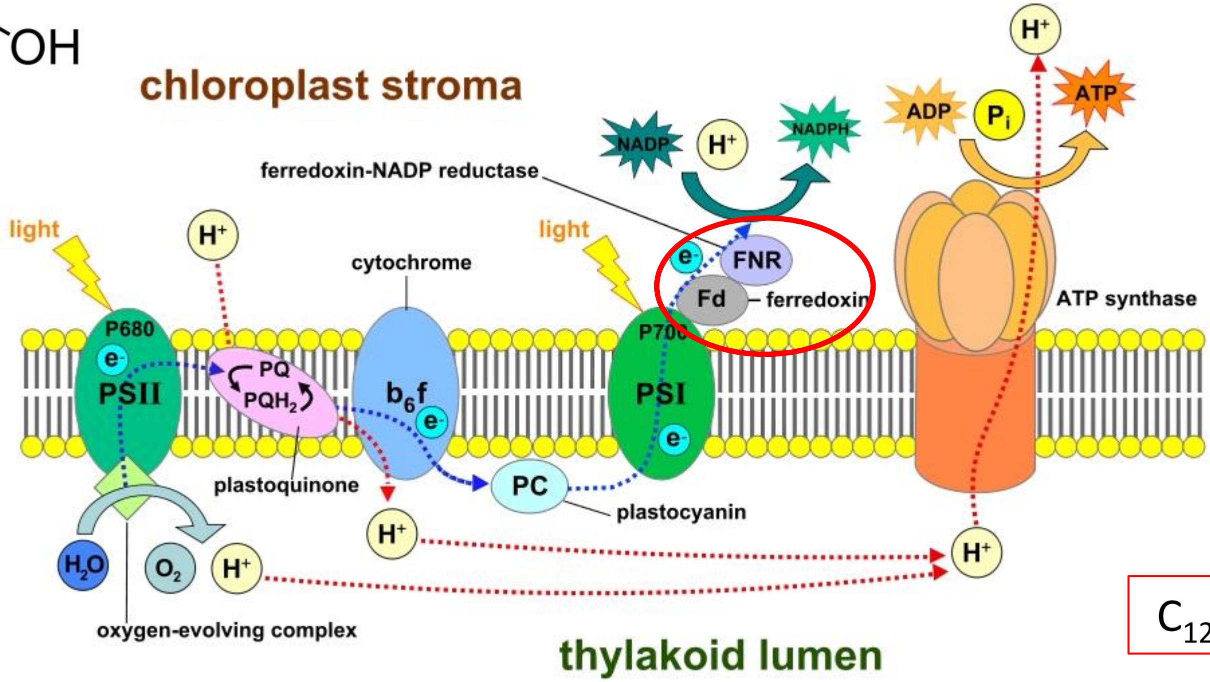
Ferredoxin (Fe_2S_2) – Key in Photosynthesis



In chloroplasts, Fe_2S_2 ferredoxins function as electron carriers in the photosynthetic electron transport chain and as electron donors to cellular proteins

Cys





$C_{12}H_{28}N_4O_8S_6Fe_2$

Quantum Chemistry Example (Ferredoxin)*

$$H = \sum_{pq} h_{pq} a_p^\dagger a_q + \frac{1}{2} \sum_{pqrs} h_{pqrs}\, a_p^\dagger a_q^\dagger a_r a_s$$

Ferredoxin (Fe_2S_2) used in many metabolic reactions including energy transport in photosynthesis

$C_{12}H_{28}N_4O_8S_6Fe_2$

- *Intractable on a classical computer*
- *Assumed quantum scaling: ~24 billion years (N^{11} scaling)*
- *First paper: ~850 thousand years to solve (N^9 scaling)* http://arxiv.org/abs/1312.1695
- *Second paper: ~30 years to solve (N^7 scaling)* http://arxiv.org/abs/1403.1539
- *Third paper: ~5 days to solve ($N^{5.5}$ scaling)* http://arxiv.org/abs/1406.4920
- *Fourth paper: ~1 hour to solve ($N^3, Z^{2.5}$ scaling)* http://arxiv.org/abs/1410.8159

<200 qubits

*Svore, Microsoft Corporation, 2015

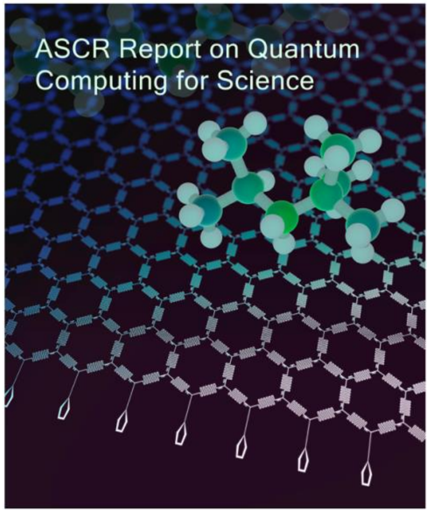
Quantum Computing Community Engagement

- Workshop on Materials Opportunities for Quantum Computing,* October 7-8, 2014, LANL
- Grand Challenges at the Intersections of QIS, Particle Physics, and Computing, December 11, 2014, joint DOE/HEP & ASCR
- NNSA Workshop on Applications of Quantum Computing, February 5-6, 2015, SNL (organized by LANL)
- DOE/ASCR Workshop on Quantum Computing in Scientific Applications, Date: February 17-18, 2015
- Workshop on Beyond Exascale: Qubits for Quantum Computing,* ORNL, August 20-21, 2015
- Round Table on “Quantum Sensors at the Intersection of Fundamental Science, Advanced Computing, and QIS,” February 25, 2016
- Also … NSF and NIST community events (2015)

**Community organized*

DOE/ASCR Workshop on Quantum Computing in Scientific Applications (Feb 17-18, 2015)

- The goal of the workshop was to assess the viability of quantum computing technologies to meet the computational requirements in support of DOE's science and energy mission and to identify the potential impact of these technologies.
- Research into quantum computing technologies is making rapid progress and it is important for the Office of Advanced Scientific Computing Research (ASCR) to understand the utilization of these new technologies for DOE-relevant applications and their impact on conventional computing systems.



http://www.csm.ornl.gov/workshops/ascrqcs2015/index.html

- The workshop explored the following topics:
  - Mission relevance: What aspects of DOE's science mission are suitable for quantum computing? What are the early tests that will demonstrate viability, or lack thereof, for the DOE's mission in fundamental and applied sciences?
  - Impact on Computing: How will quantum computing improve the properties of the computation with respect to conventional contemporary computational systems? Such attributes include, but are not limited, to performance, capacity, power, cost, generality and programmability.
  - Challenges: What are the challenges in adopting quantum computing technologies and developing the required infrastructure? What algorithm/application bottlenecks need to be solved before a quantum enabled system can be used for mission critical applications? What can ASCR do to mitigate these challenges?

Research and Evaluation Prototypes Quantum Computing: Testbeds

- **Challenge:**

  A major barrier to developing quantum computing is availability of testbed computing systems that can be used to explore algorithms and computational approaches

- **FY 2017 Objective:**

  Initiate the development of two to three testbeds, which would support ASCR, BES, and HEP-based algorithm development activities. These testbeds will not look like conventional computers – they would likely comprise approximately a six-nine qubits and likely would be based on optical or circuit-based approaches, requiring modest technical support to use.

Computational Partnerships Quantum Computing: Algorithms

- **Challenge:**

  Research community workshops have identified scientific applications that are important to DOE missions (both SC and NNSA) that can be attacked using quantum algorithms.

- **FY 2017 Objective:**

  Initiate two EFRC-sized efforts, focused on problems relevant to SC, to begin development of quantum algorithms and to evaluate efficacy of this funding modality for achieving the needed multidisciplinary integration. These EFRC-like activities would use the quantum testbeds in a co-design fashion, feeding back into the testbeds ideas for improvement.

DOE/ASCR Workshop on Quantum Computing in Scientific Applications (Feb 17-18, 2015)

Brief examples of applied mathematics opportunities identified in the report:

1. ***Linear Algebra***

   Discovery of extensions to and analogs of the Harrow, Hassidim, and Lloyd algorithm (quantum algorithms to solve Ax=B)

2. ***Integration and Summation***

   Investigating speedups that can be achieved by applying amplitude estimation or quantum walks in current state of the art classical algorithms

3. ***Optimization***

   Discovery of practical quantum algorithms for finding global extrema in physical-sciences problems, e.g., molecular dynamics and protein folding

4. ***Graph Theory***

   Discovery of new quantum algorithms that offer polynomial speedup for graph theoretic problems, including finding spanning trees, locating cliques, and deciding bipartiteness

Questions?