Program Perspectives on Quantum Information

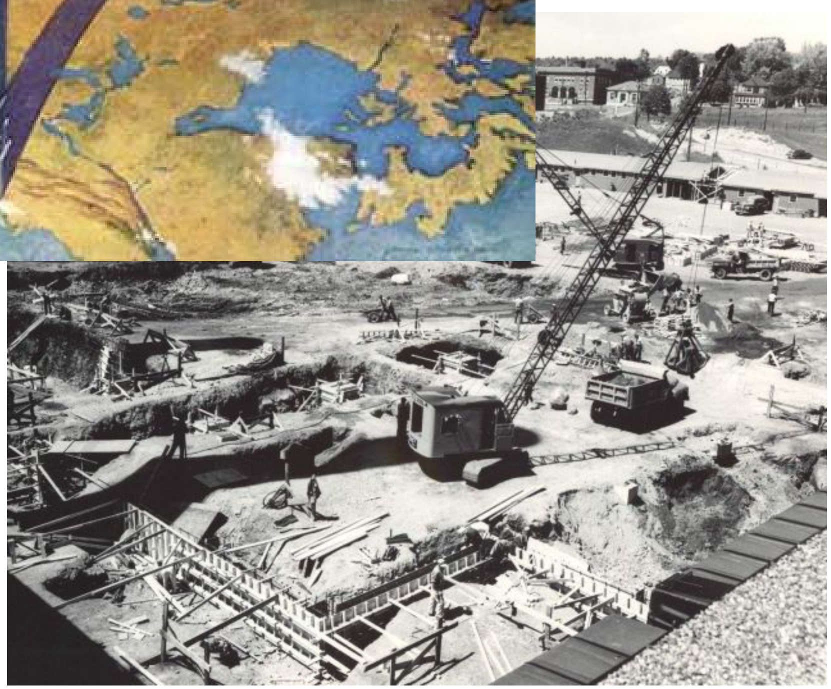
Michael Foster
National Science Foundation

Outline

- Computing & Communication Foundations
- QIS Bumper Stickers
- Quantum Computing
- Quantum Key Distribution
- Support agencies
- Where next?

Why Foundations?

-

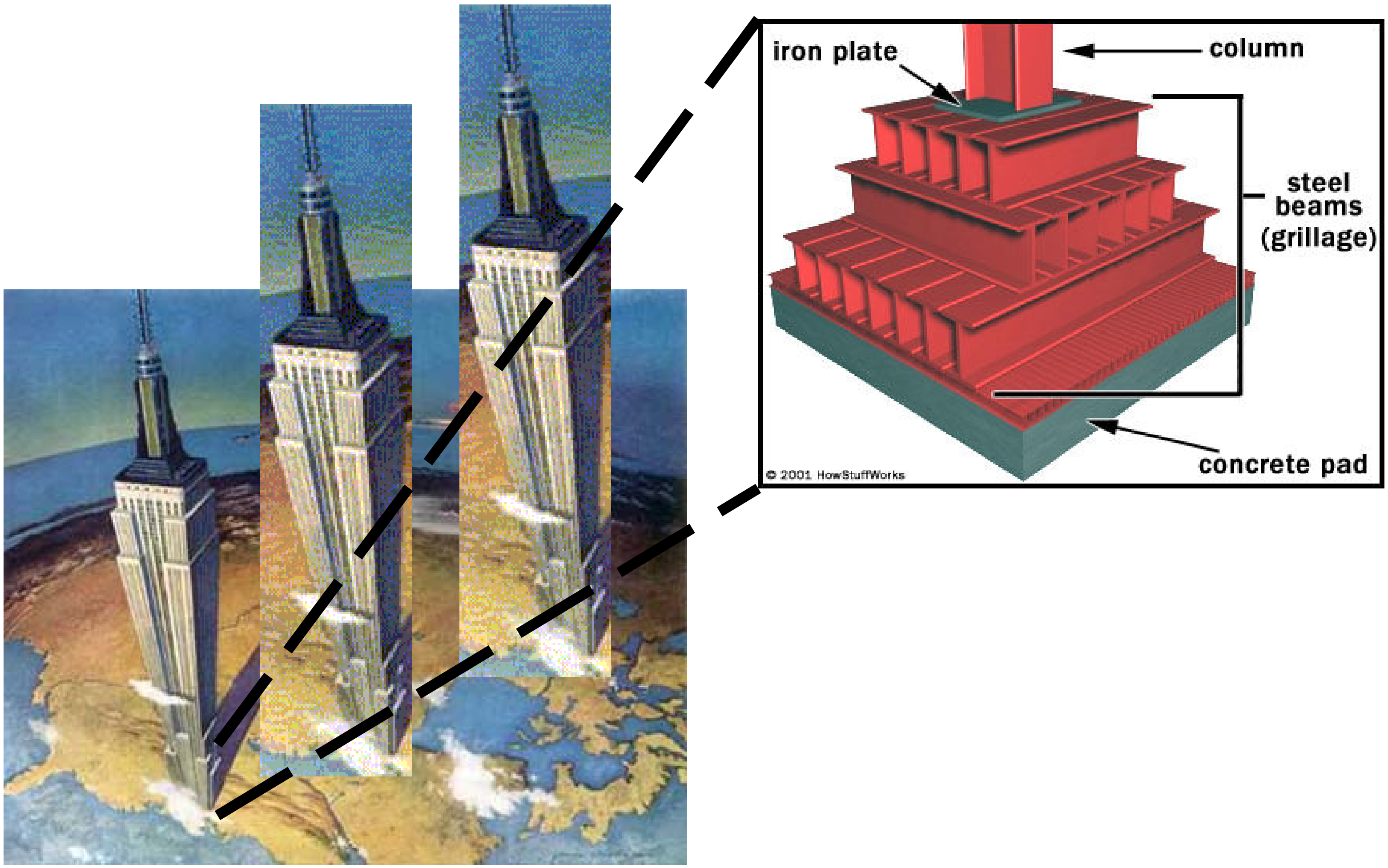


=

Foundations Everywhere

Infrastructure

Systems

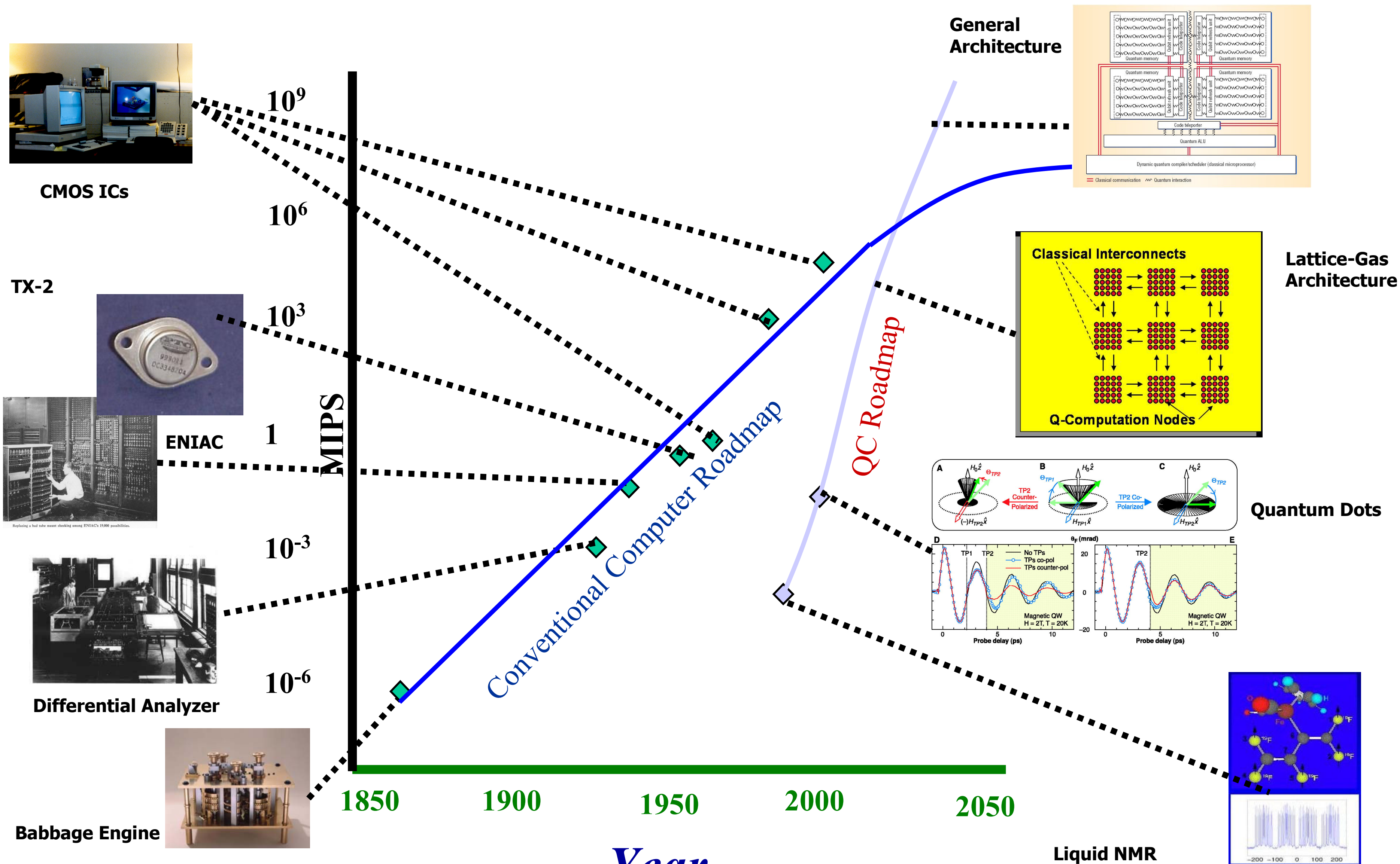


Quantum Information Bumper Stickers

- Quantum computation
  - State superposition provides parallelism
- Quantum communication
  - No cloning theorem provides unforgability
- Quantum metrology
  - Entanglement provides consistent measurement

Quantum Computation

QIP and Moore's Law



Power of Qubits

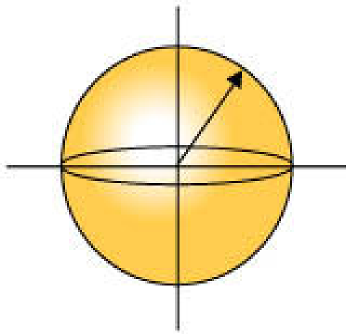
•***Qubit* = state of a quantum two-level system**

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1$$

Continuum of states!

1 classical bit has two states: 0 and 1

1 qubit has "infinitely" many states!



•***Physical realizations of qubits:***

- •photon polarization
- •electron spin
- •nuclear spin
- •pair of electron states in a trapped ion/atom
- •magnetic flux state in a Josephson junction ring
- •Cooper pair number states, etc.

Power of Qubits

- ***Multiple qubits***

  A classical 3-bit state: **001**

  A quantum 3-qubit state:

$$\alpha|000\rangle + \beta|001\rangle + \gamma|010\rangle + \delta|100\rangle + \varepsilon|011\rangle + \phi|101\rangle + \chi|110\rangle + \varphi|111\rangle$$

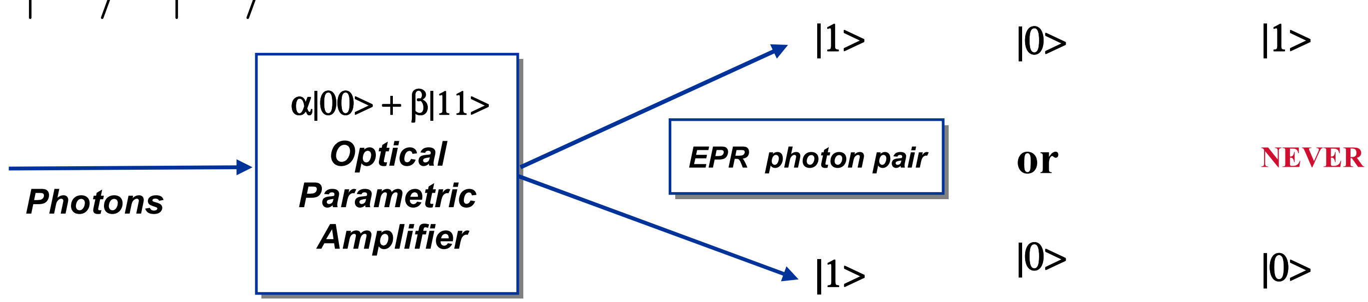
N qubits is worth 2^n classical bits!

- ***Entanglement***

$$|00\rangle + |01\rangle + |10\rangle + |11\rangle \rightarrow (|0\rangle + |1\rangle)(|0\rangle + |1\rangle)$$ ***Not entangled***

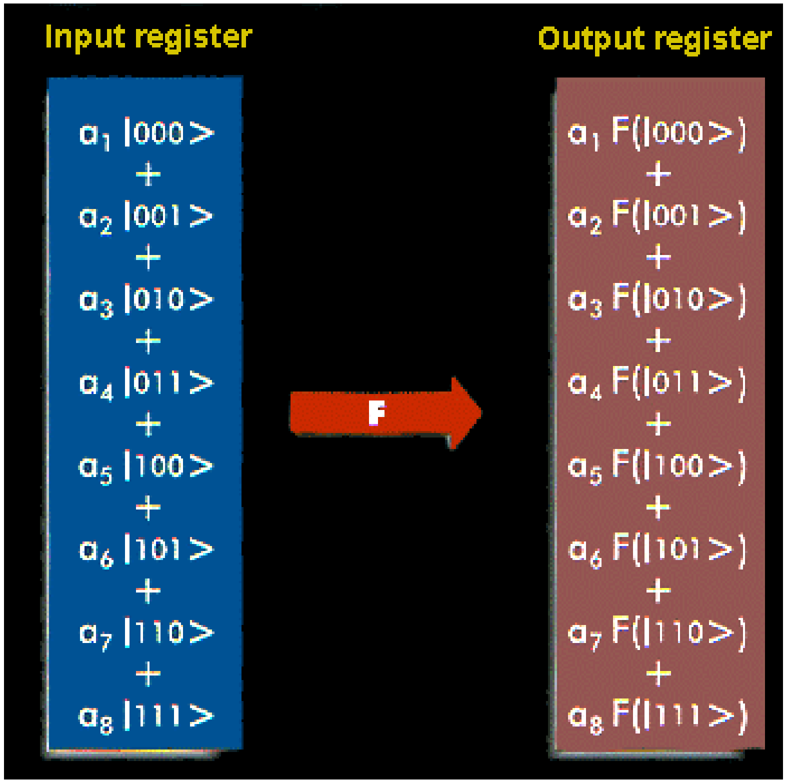
$$|00\rangle \pm |11\rangle$$
$$|01\rangle \pm |10\rangle$$

Entangled!



Power of Quantum Computation

- ***Quantum Parallelism***

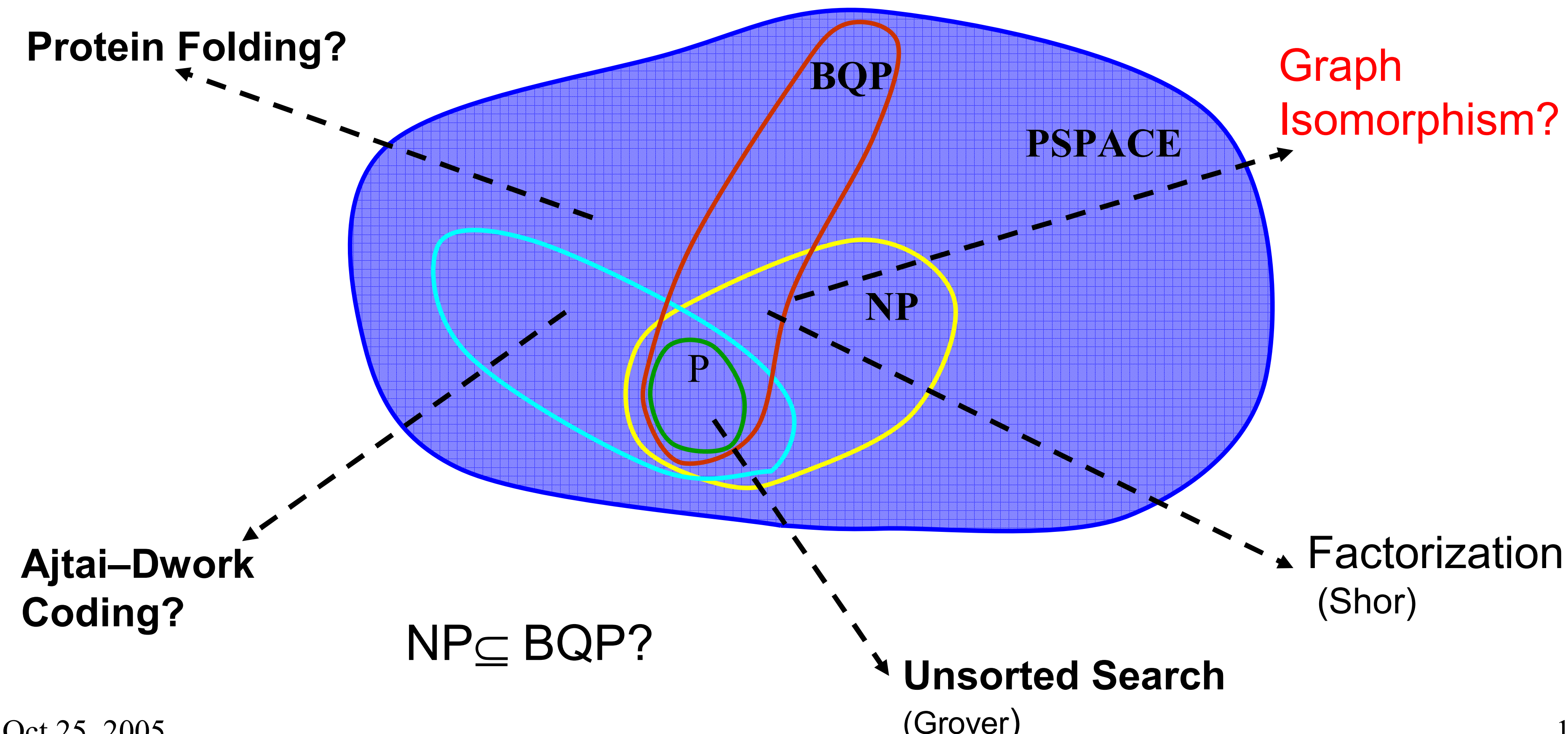


2^n values of F(x) all in one go!!

An exponential amount of computation has been achieved in the time it takes to compute the function on a single input!

Quantum Complexity

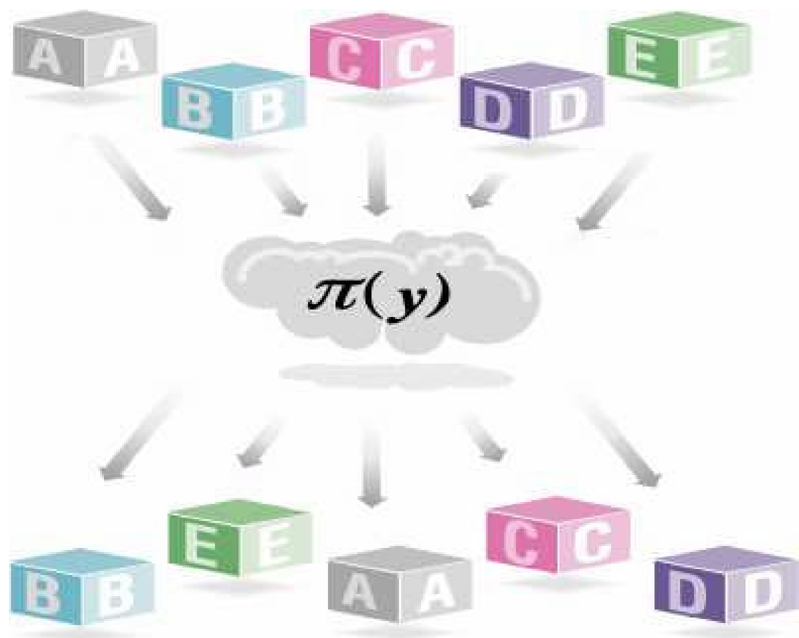
Provably Q-hard algorithms



NP⊆ BQP?

QIP: An Example Algorithm

- **Permutation Order-Finding** (Chuang *et al*, '00)
  - •Permutation π is an operation that rearranges a set of objects



•Order r of a permutation applied to element y of a set is the minimum number of times π must be applied to put y back in its original position

•Problem has wide range of applications (Cryptography)

Classical versus Quantum

Classical approach:

- *Series of trials to find the x-th permutation $\pi^x(y)$.*

- *Find equality. When $\pi^a(y) = \pi^b(y)$ then ord(π) | a-b*

- *Number of trials needed increases exponentially with the number of bits representing y*

Quantum approach:

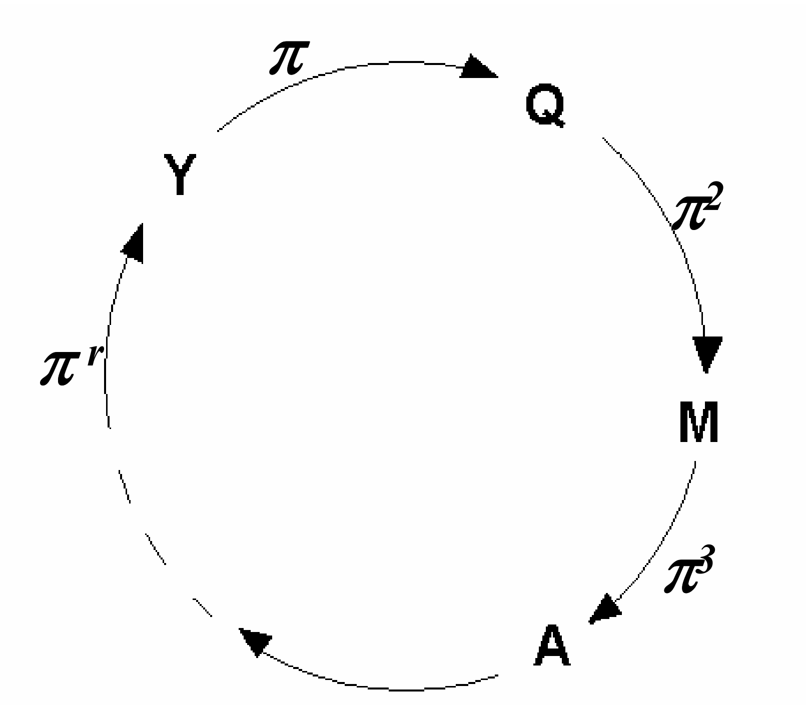
- *Order is the period of a function*
  $f_y(x) = \pi^x(y)$

- *Quantum Fourier Transform allows us to find periods of all $\pi^x(y)$ with one transform*

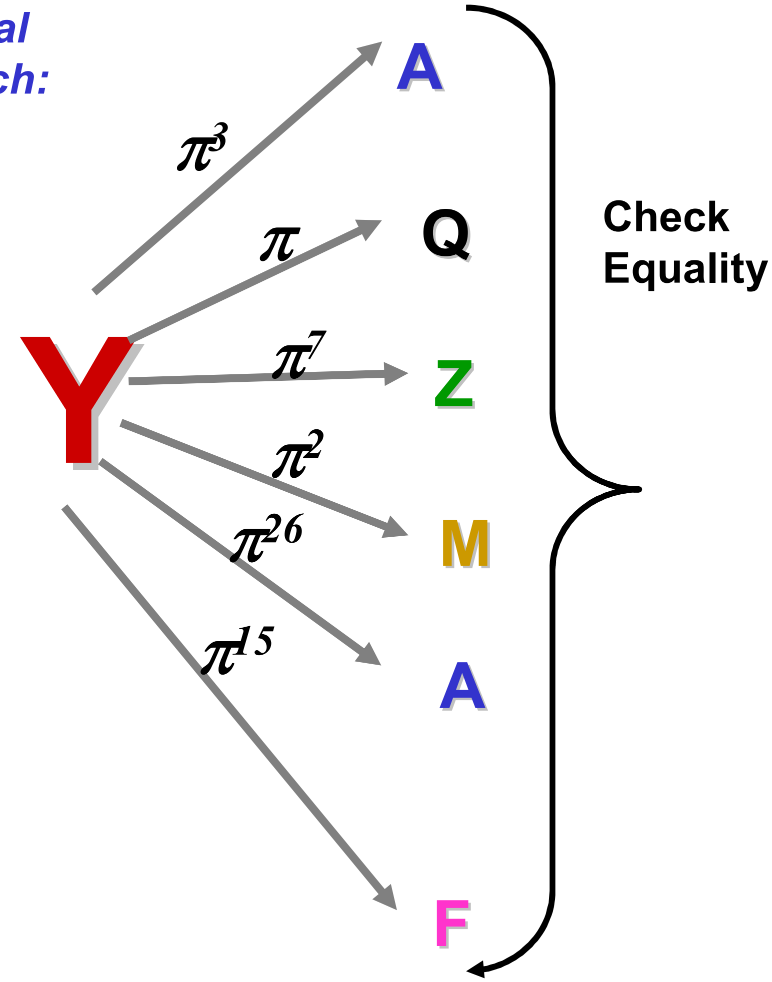
- *Exponential speedup-- Minimum number of steps proportional to bits in y*

Classical Order-Finding

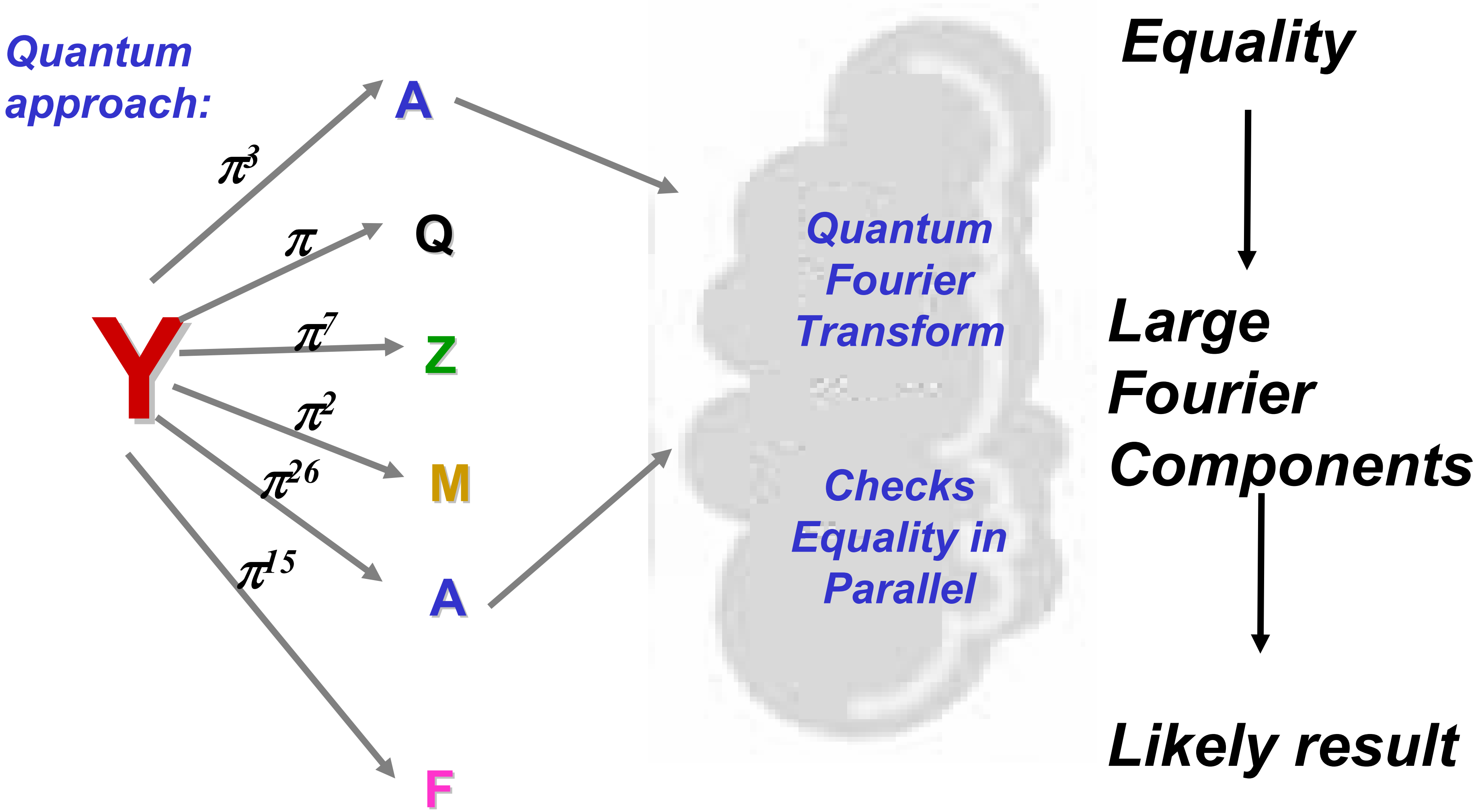
What a permutation really looks like:



Classical approach:



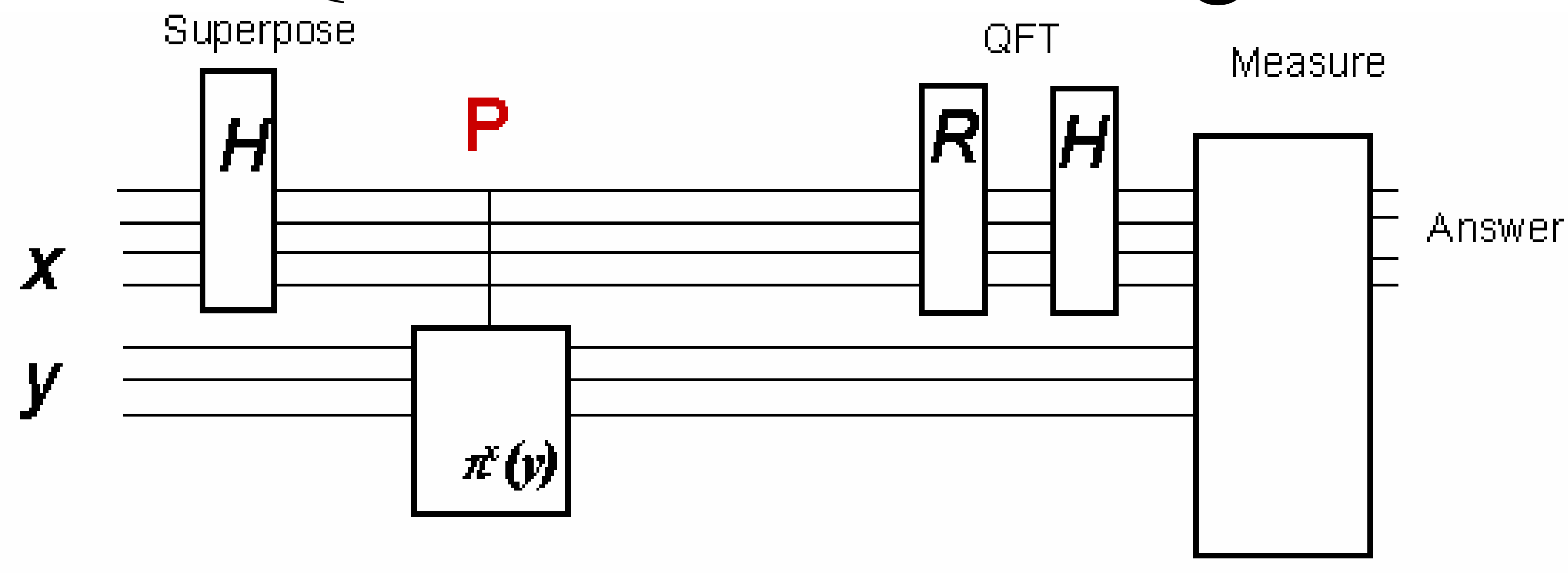
Quantum Order-Finding



Quantum Fourier Transform (QFT)

- Variant of the Discrete Fourier Transform (DFT) that can be implemented on a quantum computer
- At the heart of Factoring and Order-Finding problems
- QFT transforms state amplitudes to state amplitudes
  - NOT qubits to qubits

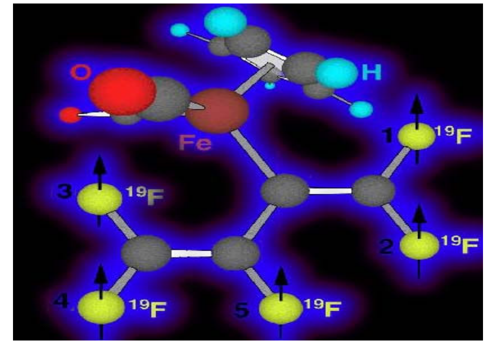
QFT in Order Finding



- States are measured according to their probability
- Many states at P produce the same $\pi^x(y)$
- QFT produces their frequency
- Probably answer reflects large number of states at P

Status of Computing

- Proof of concept factoring (2001)



Chuang et al. 4-bit Shor algorithm implementation (2001)

- Ongoing ion-trap implementation effort
- Some optical lattice efforts
- Solid-state spins moving slowly

Ion Trap Investigations

- Done (per ARDA Roadmap April 2, 2004)
  - 2-qubit operations demonstrated
  - Long decoherence times in progress
  - 3-10 qubit operations started
- Proposed (individual researchers)
  - 10-20 qubit registers
  - Architectures with 1000 circulating qubits
- Possibility
  - 20 logical qubits (2-level error correct 1000 qubits)
  - 10 bit factoring

Optical Lattices

- Done (individual researchers)
  - 110 site lattice loaded from BEC with 200 atoms/site
- Proposed (individual researchers)
  - 8000 sites with CO2 lasers proposed by Berkeley QuIST project
    - Filling factor 1/2
  - Permits 80 logical qubits
  - Permits 40 bit factoring

Architectural Roadblocks

- Classical control
  - Large feature sizes for control lines mean large computers
- Wiring and corners
  - Moving qubits leads to decoherence
- Error correction
  - More check bits than data bits
- Cumulative effect
  - May need 100,000 times longer decoherence times than required by operations alone (Balensiefer et. al, ISCA32, 2005, pp186-196).

Quantum Security

Quantum Key Distribution

- Use unforgability to detect eavesdropping
- Shared generation of secure key
- Extensive classical processing

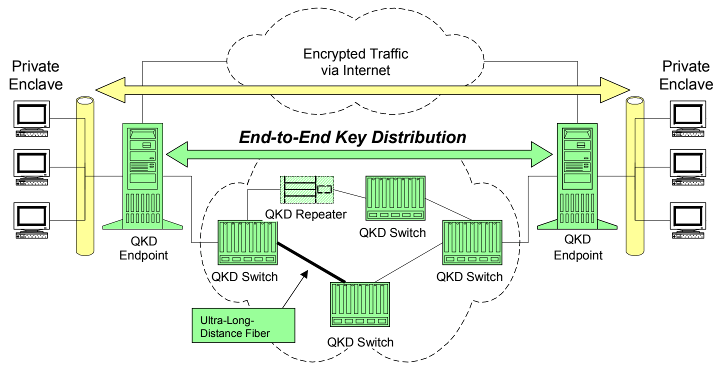
Quantum Cryptography

BB84 Protocol

Aaron VanDevender (vandvndr@uiuc.edu)

Status of Key Distribution

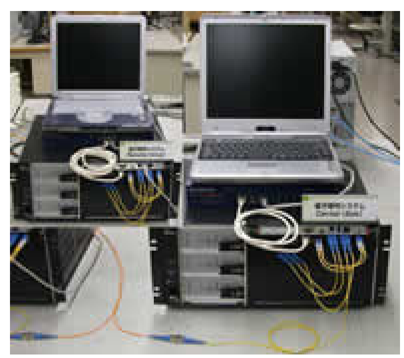
BBN-AFRL-QuIST Network Rollout June 1, 2004



NEC 2-week demonstration May 31, 2005 (AFRL-QuIST inside?)

ID Quantique Turnkey System

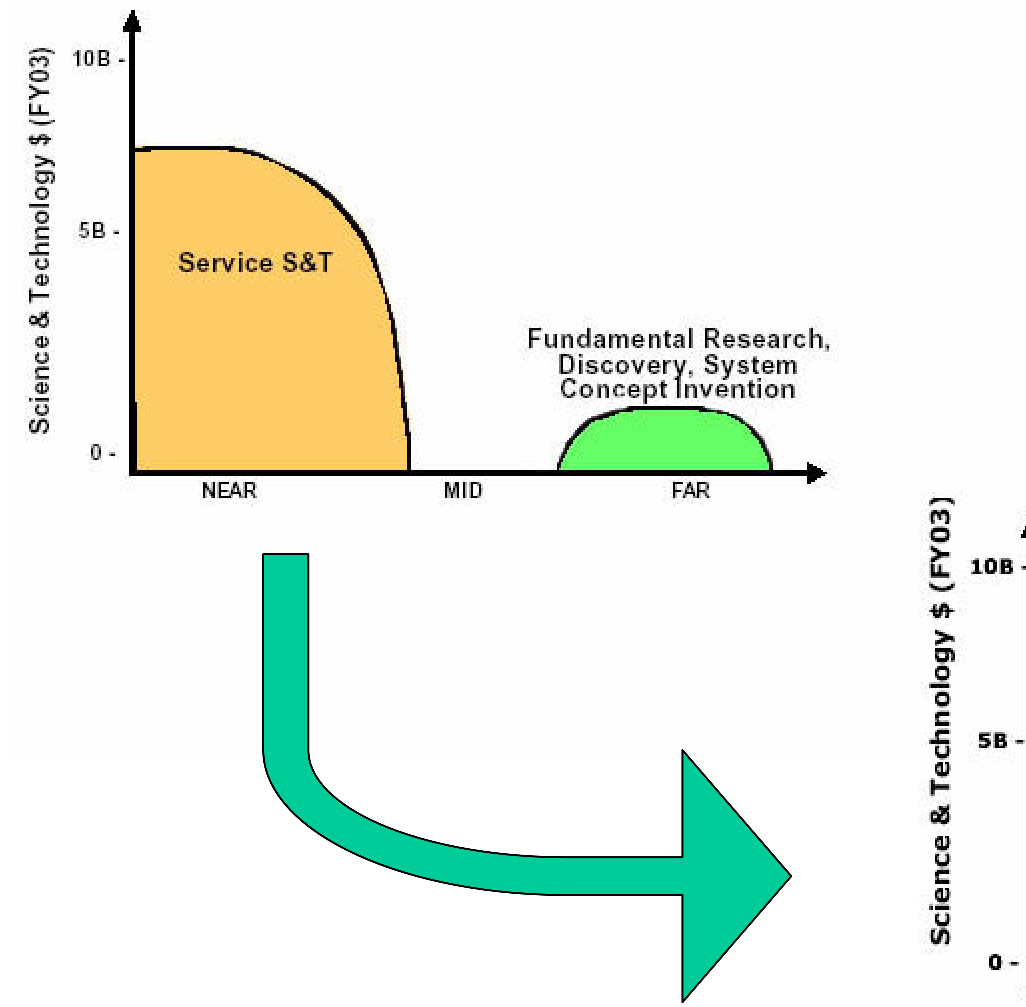
Available throughout Switzerland June 05



13kb/sec sifted key over 16km commercial access optical network

Support Agencies

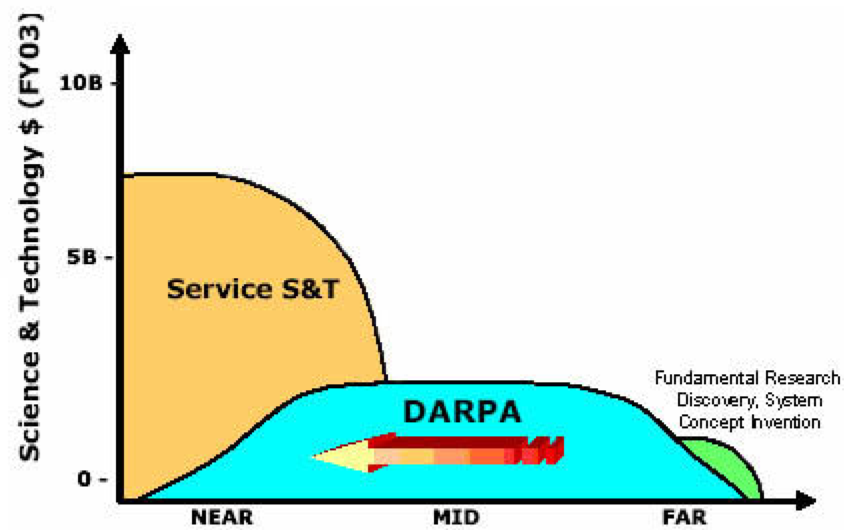
DARPA Mission



Focused strategic thrusts

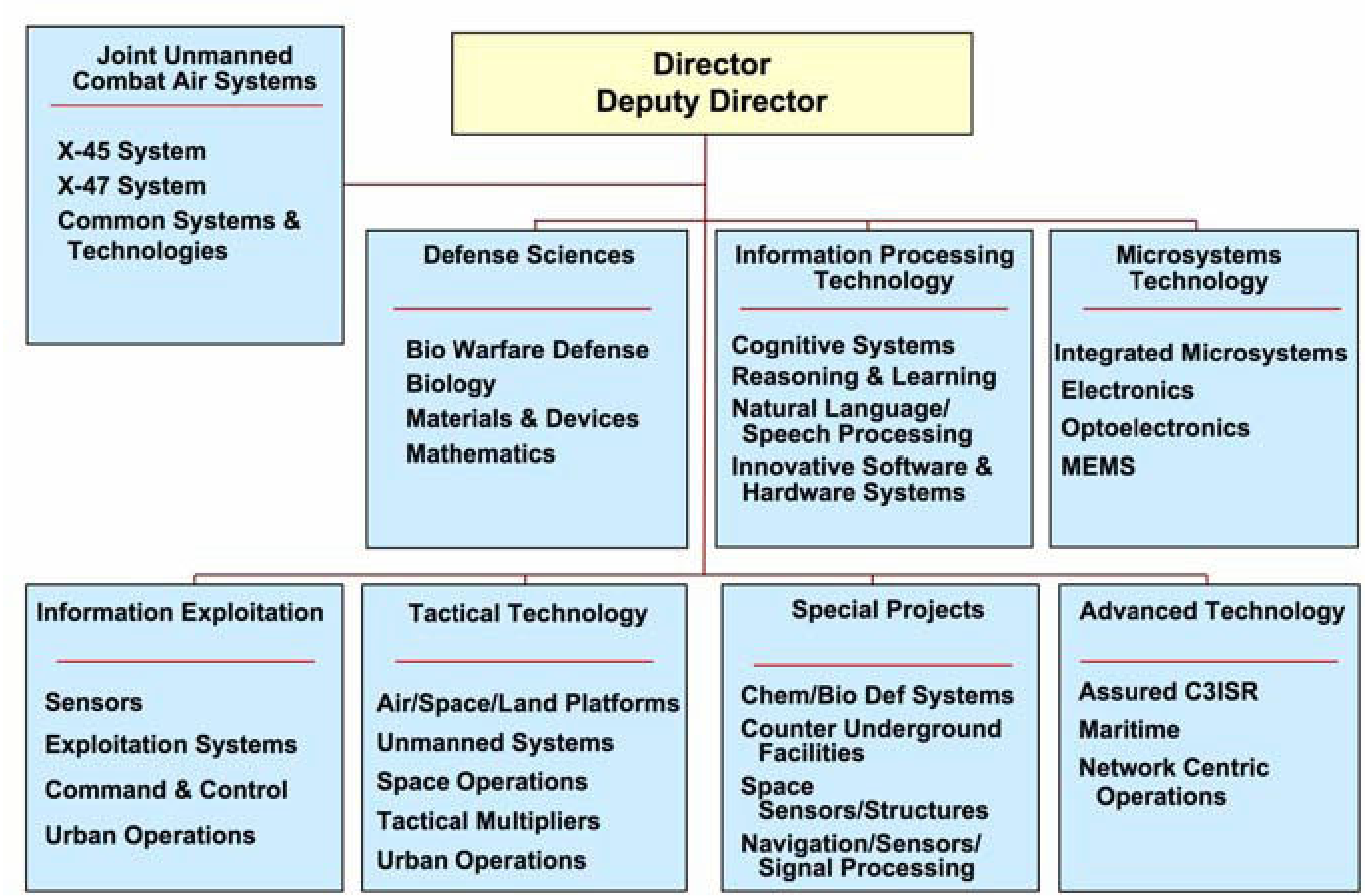
Specific programs

Emphasize transition



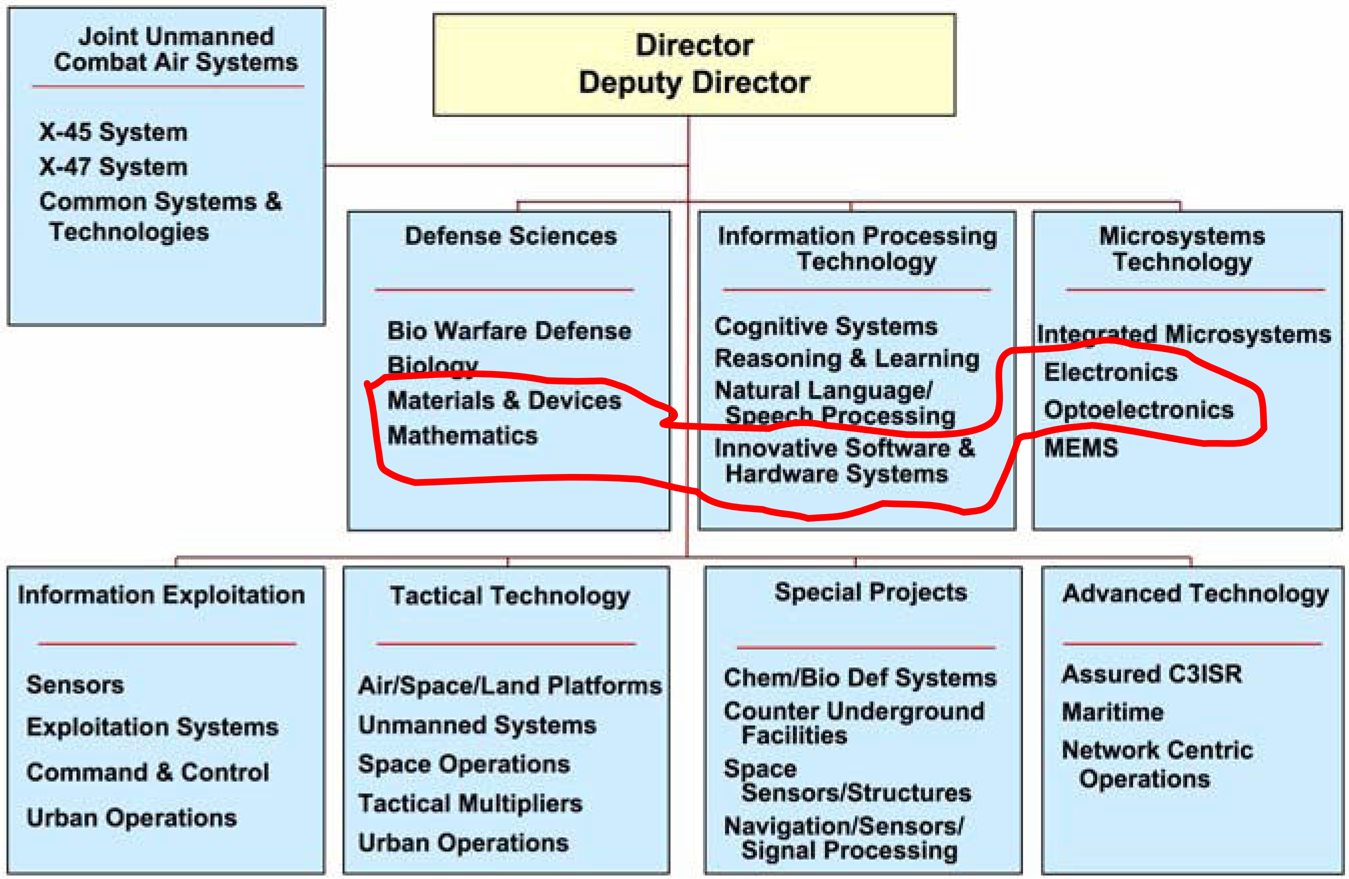
Source: Bridging the Gap February 2005

DARPA Organization



Source: Bridging the Gap February 2005

QIP in DARPA Organization



Source: Bridging the Gap February 2005

NSF Mission

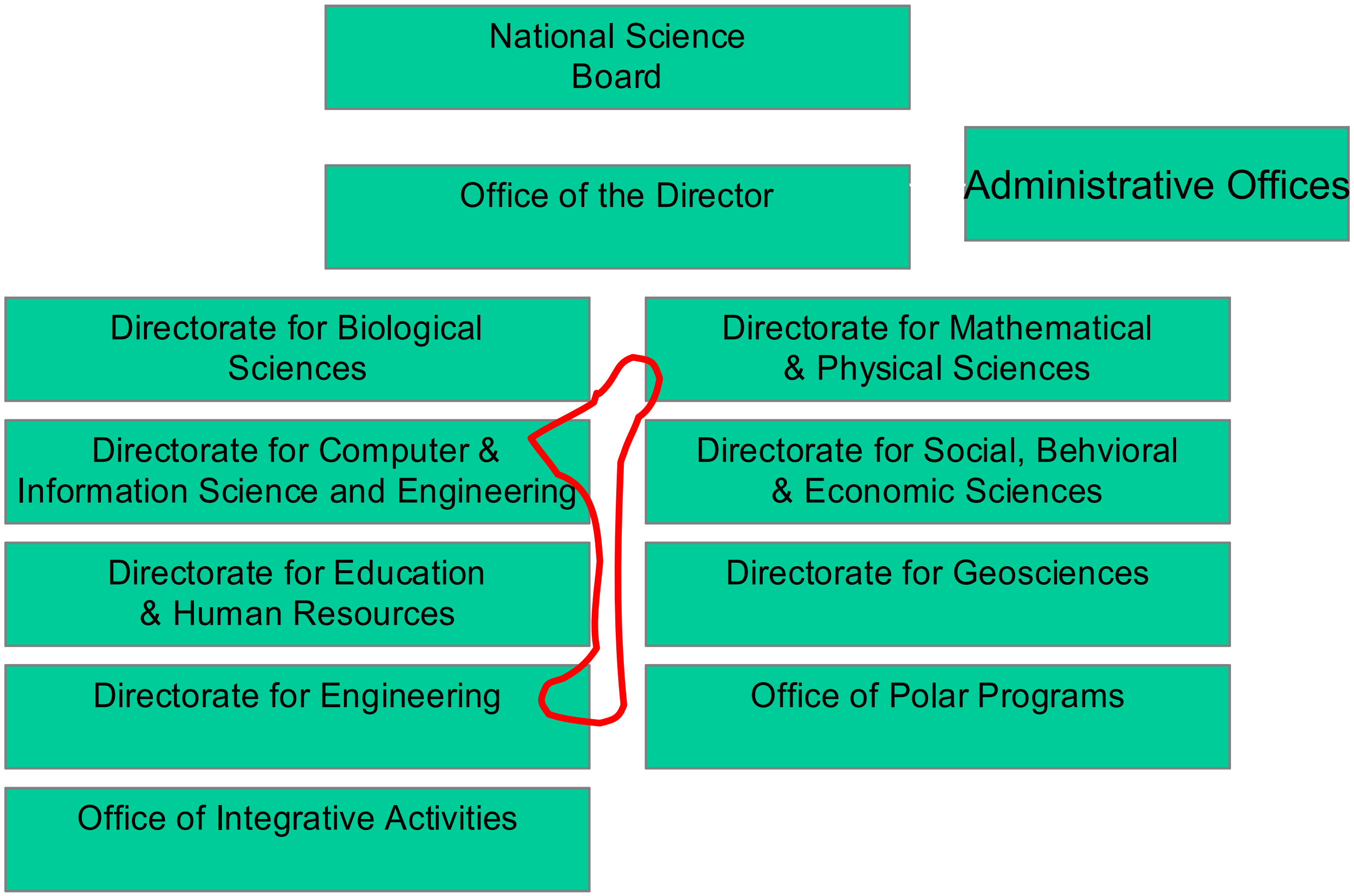
National Science Foundation Act of 1950 (Public Law 810507):

- To promote the progress of science;
- to advance the national health, prosperity, and welfare;
- to secure the national defense;
- and for other purposes.

NSF Organization

- National Science Board
- Office of the Director
- Administrative Offices
- Directorate for Biological Sciences
- Directorate for Computer & Information Science and Engineering
- Directorate for Education & Human Resources
- Directorate for Engineering
- Office of Integrative Activities
- Directorate for Mathematical & Physical Sciences
- Directorate for Social, Behvioral & Economic Sciences
- Directorate for Geosciences
- Office of Polar Programs

QIP in NSF Organization



CISE Mission

CISE has three goals:

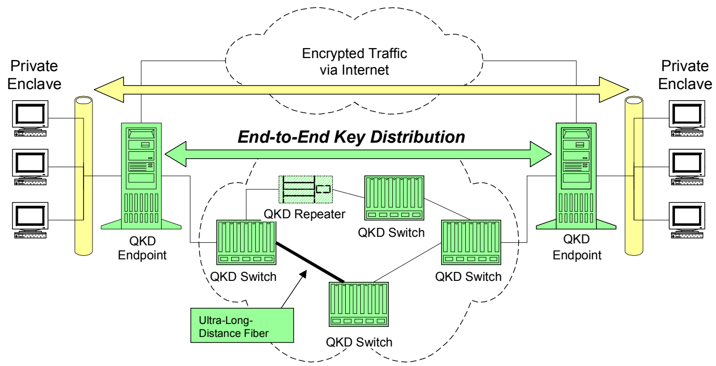
- to enable the United States to remain competitive in computing, communications, and information science and engineering;
- to promote understanding of the principles and uses of advanced computing, communications, and information systems in service to society; and
- to contribute to universal, transparent, and affordable participation in an information-based society.

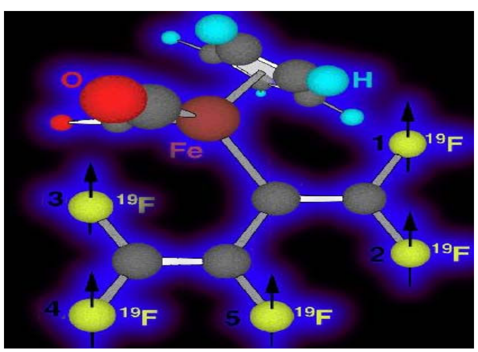
Desired Project Characteristics

- DARPA – Fast Results
  - Military need
  - Technical challenges and plan for meeting them
  - Transition plan
- NSF – Sustained Effort
  - Asks fundamental questions
  - Maintains U.S. competitiveness
  - Societal need
  - Broad participation

DARPA Program Highlights

QuIST Network Rollout June 1, 2004





Chuang et al. 4-bit Shor algorithm implementation (2001)

NSF Program Highlights

Institute for Quantum Information at Caltech

Some student projects

Charlene Ahn, "Continuous quantum error correction via quantum feedback …"
John Cortese, "Classical communication over quantum channels"
Sumit Daftuar, "The communication cost of entanglement transformations"
Jim Harrington, "Calculating the accuracy threshold for toric codes"
Theresa Lynn, "Active feedback strategies for motion of a single atom …"
Carlos Mochon, "Computing with anyons"
Ben Rahn, "Exact and approximate performance of concatenated codes"
Federico Spedalieri, "Distinguishing separable and entangled states"
John Stockton, "Entanglement in atomic ensembles"
Ben Toner, "Communication cost of simulating quantum correlations"
Jake West, "Universal quantum computation using projective measurement"

Quantum Complexity and Polynomial Approximations of Boolean Functions

- Quantum and classical tradeoffs
- Classical simulation of quantum communication.
- Phase transition in biological signaling systems
- Education plan: theory of computation courses

CAREER Award: Yaoyun Shi at U. Michigan

Where Next for Communication?

- DARPA
  - Long range demonstrations between metronets
  - GtoA and GtoS demonstrations
  - ConOps for QKD
- NSF
  - New protocols
  - Security bounds

Where Next for Computation?

- New algorithms
  - Exponential speedups, please!
  - (Hashing outdoes unstructured search)
- New applications of existing algorithms
  - Pell's equation
  - Random walk
- Scalable architectures
  - Controllable
  - Fault tolerant
- Medium-scale implementations
  - 10's of qubits
  - Probably beyond NSF resources

The Near Future

- NSF budget is down 3% in 2005, looks flat
- DoD will need transitions beyond crypto
- New algorithms and protocols are needed for the next push
  - Scalable architectures too

The Want Ads

Program Directors Sought

- Numeric, Symbolic, Geometric computing
- Emerging Models and Technologies
- Interdisciplinary capability
  - Across cluster, division, NSF, and globally

Contact

- Vacancy announcements appear on www.nsf.gov
- Meanwhile contact

Michael Foster
Division Director
Computing & Communication Foundations
National Science Foundation
4201 Wilson Boulevard
Arlington, VA 22230
703-292-8910
mfoster@nsf.gov