Title: The Quantum Information Age - ISSYP Keynote Session

Date: Aug 01, 2007 09:00 AM

URL: http://pirsa.org/07080058

Abstract: The world at the size of individual atoms obeys very different laws of physics from those we are used to in the everyday world around us. Quantum mechanics rules, allowing atoms to be, in some sense, in more than one place at a time. Researchers all over the world are working to build \"quantum computers\" whose memories manipulate an inherently new type of information, \"quantum information.\"
Quantum computers have capabilities impossible for a regular computer, no matter how advanced it may be, including the ability to run new kinds of computer programs capable of rapidly solving certain problems, and to make new highly secure codes for secret communication.

Quantum Bits

We can break up regular information into "bits", either 0 or 1. Quantum information is measured in quantum bits, or "qubits," which can be in a superposition of both 0 and 1. A measurement on a qubit will produce one of the two results at random:

$a|0\rangle + b|1\rangle$ —measure→ Probability $|a|^2$ of 0; Probability $|b|^2$ of 1

We can manipulate qubits in various ways. E.g.:

$a|0\rangle + b|1\rangle$ —bit flip→ $a|1\rangle + b|0\rangle$

We can interact multiple qubits at once:

$a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ —controlled-NOT→ $a|00\rangle + b|01\rangle + c|11\rangle + d|10\rangle$

Quantum Bits

We can break up regular information into "bits", either 0 or 1. Quantum information is measured in quantum bits, or "qubits," which can be in a superposition of both 0 and 1. A measurement on a qubit will produce one of the two results at random:

$a|0\rangle + b|1\rangle$ —measure→ Probability $|a|^2$ of 0; Probability $|b|^2$ of 1

We can manipulate qubits in various ways. E.g.:

$a|0\rangle + b|1\rangle$ —bit flip→ $a|1\rangle + b|0\rangle$

We can interact multiple qubits at once:

$a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ —controlled-NOT→ $a|00\rangle + b|01\rangle + c|11\rangle + d|10\rangle$

Interference

We can also create superpositions:

$$\left\{ \begin{array}{l} |0\rangle \\ |1\rangle \end{array} \right. \xrightarrow{\text{Hadamard}} \begin{array}{l} (|0\rangle + |1\rangle)/\sqrt{2} \\ (|0\rangle - |1\rangle)/\sqrt{2} \end{array}$$

What if we attempt to create a superposition, but we already had one?

$$(|0\rangle + |1\rangle)/\sqrt{2} \xrightarrow{\text{Hadamard}} \begin{array}{l} (|0\rangle + |1\rangle)/2 + \\ (|0\rangle - |1\rangle)/2 \end{array} = |0\rangle$$

The 0 parts add together ("constructive interference")

The 1 parts cancel ("destructive interference")

What Good Is a Quantum Computer?

Quantum computers can use interference and superposition to do some things classical computers can't:

- Quickly factoring large numbers.
- Efficiently simulating quantum systems.
- Speed up exhaustive search of N items to $N^{1/2}$ tries.
- Square-root speedup to find the best chess move.
- Maybe more interesting undiscovered algorithms?

But for other problems, a quantum computer offers no speedup over a classical computer.

RSA Encryption System

RSA encryption is widely used today:

- Encryption key is a pair of large numbers (N, e) (e.g., 300 digits long)
- To encrypt a message:
  - Convert the message to numbers less than N.
  - Raise the message to the power e.
  - Divide by N and take the remainder. (Modular arithmetic)
- Decryption key d
  Derived from prime factors of N
- To decrypt a message:
  - Raise the encrypted message to the power d
  - Divide by N and take the remainder.
- Breaking RSA believed as hard as factoring N

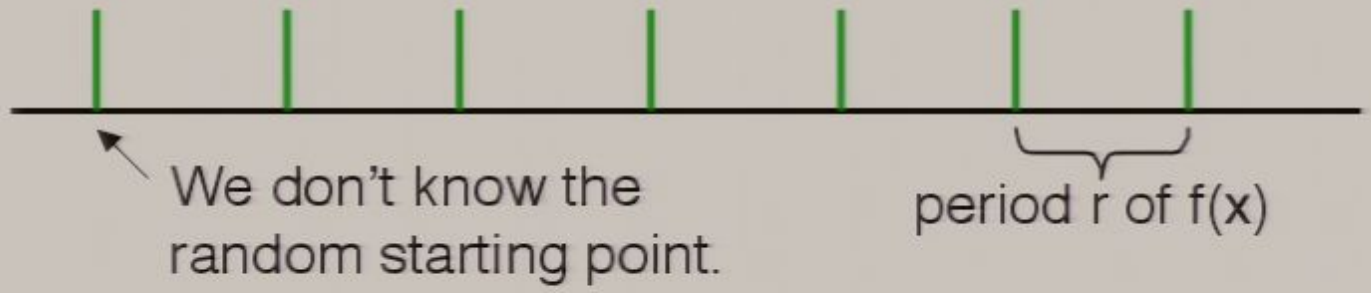
Factoring with a Quantum Computer

Find period of function $f(x) = a^x$

Factor large numbers (hard on classical computer)

Create superposition:

(over points where $f(x) = c$, c random)

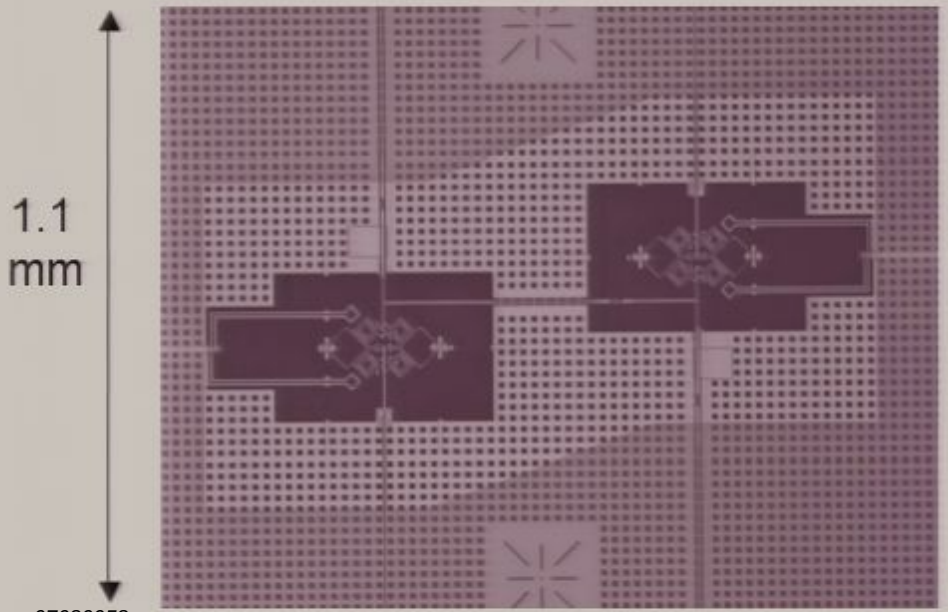


The Fourier Transform determines the period of a repeating function, so Shor's algorithm applies the Fourier transform to the superposition. Once we know the period of RSA, that tells us the value of the private key d.

How Do We Build a Quantum Computer?

Ions in an electromagnetic bottle, with an electron's energy level as the qubit. They are controlled with lasers. (Record size: 4 qubits.)

~10 microns between ions. Ion trap at NIST Boulder.



From UC Santa Barbara, in Science Magazine

Small superconducting circuits, with a current, charge location, or some other quantity as the qubit. They are controlled with voltage sources and inductors. (Record: 2 qubits.)

How Do We Build a Quantum Computer?

A molecule in an NMR machine, using nuclear spins as qubits. They are controlled using RF pulses. (Record: 12 qubits.)

The magnet for an NMR quantum computer at the University of Waterloo

And more:

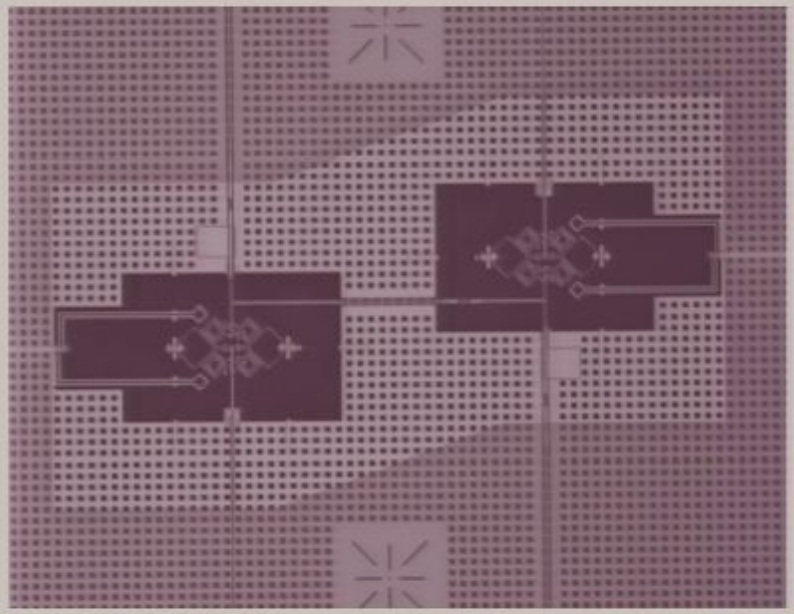
- Polarization of photons
- Atoms in an optical lattice
- Quantum dots in semiconductors
- ...

How Do We Build a Quantum Computer?

Ions in an electromagnetic bottle, with an electron's energy level as the qubit. They are controlled with lasers. (Record size: 4 qubits.)

~10 microns between ions. Ion trap at NIST Boulder.

1.1 mm



From UC Santa Barbara, in Science Magazine

Small superconducting circuits, with a current, charge location, or some other quantity as the qubit. They are controlled with voltage sources and inductors. (Record: 2 qubits.)

How Do We Build a Quantum Computer?

A molecule in an NMR machine, using nuclear spins as qubits. They are controlled using RF pulses. (Record: 12 qubits.)

The magnet for an NMR quantum computer at the University of Waterloo

And more:

- Polarization of photons
- Atoms in an optical lattice
- Quantum dots in semiconductors
- ...

Quantum Cryptography

Quantum computers can break existing codes, but they can also help make stronger codes.

In classical cryptography, the one-time pad is an unbreakable code:

Message	00001 10011 00111 10010 . . .
Key	00101 11011 10100 10100 . . .
Ciphertext	00100 01000 10011 00110 . . .

Each bit of the message is flipped or left alone, according to a new random key bit. The encrypted message looks random to someone who does not know the key.

Quantum Key Distribution: Alice

But the key in a one-time pad can only be safely used once. If Alice wants to send a long message to Bob, how can they agree on the long secret key necessary?

Answer: By sending qubits.

This is called "Quantum key distribution," or QKD.

Alice sends single particles of light ("photons"), in one of four possible quantum states:

Key bit: 0 1 Key bit: 0 1

"Z" states "X" states

vertical or horizontal polarization diagonal polarization

Quantum Key Distribution: Bob

When Bob receives a photon, he can either measure it right away (a "Z" measurement): is it 0 or 1?

Or he can shift to a superposition (the "X" measurement) to try to distinguish the two X states.

But if he guesses wrong, his measurement result is random:

$$|0\rangle + |1\rangle \xrightarrow{\text{measure}} \begin{array}{l} \text{50\% chance of 0} \\ \text{50\% chance of 1} \end{array}$$

To avoid this problem, once Bob has measured, Alice and Bob compare their choices, and only keep the bit if Bob guessed the right measurement to make.

Quantum Key Distribution: Alice

But the key in a one-time pad can only be safely used once. If Alice wants to send a long message to Bob, how can they agree on the long secret key necessary?

Answer: By sending qubits.

This is called "Quantum key distribution," or QKD.

Alice sends single particles of light ("photons"), in one of four possible quantum states:

Key bit: 0 1 Key bit: 0 1

"Z" states "X" states

vertical or horizontal polarization diagonal polarization

Quantum Key Distribution: Bob

When Bob receives a photon, he can either measure it right away (a "Z" measurement): is it 0 or 1?

Or he can shift to a superposition (the "X" measurement) to try to distinguish the two X states.

But if he guesses wrong, his measurement result is random:

$$|0\rangle + |1\rangle \xrightarrow{\text{measure}} \begin{array}{l} \text{50\% chance of 0} \\ \text{50\% chance of 1} \end{array}$$

To avoid this problem, once Bob has measured, Alice and Bob compare their choices, and only keep the bit if Bob guessed the right measurement to make.

Quantum Key Distribution: Eve

An eavesdropper Eve wants to learn the key bits too, but she faces the same problem as Bob: she does not know which measurement to make.

If Bob makes the correct measurement, his result is supposed to agree with the bit Alice sent.

If Eve guesses wrong, Eve's measurement might introduce an error into Bob's result:

$$|0\rangle \xrightarrow{\text{Eve}} |0\rangle + |1\rangle \xrightarrow{\text{Bob}} \begin{matrix} 50\%: 0 \\ 50\%: 1 \end{matrix}$$

Alice and Bob can compare a few of their bits to look for errors and detect Eve!

QKD: Full Protocol

- Alice chooses random sequence of bits and X/Z
- Alice sends corresponding qubits to Bob
- Alice and Bob:
  - Compare X/Z values.
  - Discard bits where Bob chose wrong.
  - Compare bit values on a test subset.
  - Abort if error rate is too high.
  - Use an error-correcting code to fix remaining bits (there will always be some errors, even without Eve).
  - Privacy amplification: Mix up remaining bits to eliminate any little bits of information Eve might have.

Alice and Bob either end up with a secret shared key, or detect Eve's attempt at eavesdropping.

Moving Qubits Around

If we use photons as qubits, as in QKD, moving them is easy, but computing is very hard.

If we use atoms as qubits, as in many types of quantum computer, computing is not quite as hard, but now moving them is also hard.

A solution: Quantum Teleportation

Quantum teleportation splits up the task of quantum communication into two parts:

- Quantum part: Alice & Bob create a specific quantum state shared between them.
- Communication part: Alice sends classical bits to Bob.

Entangled State

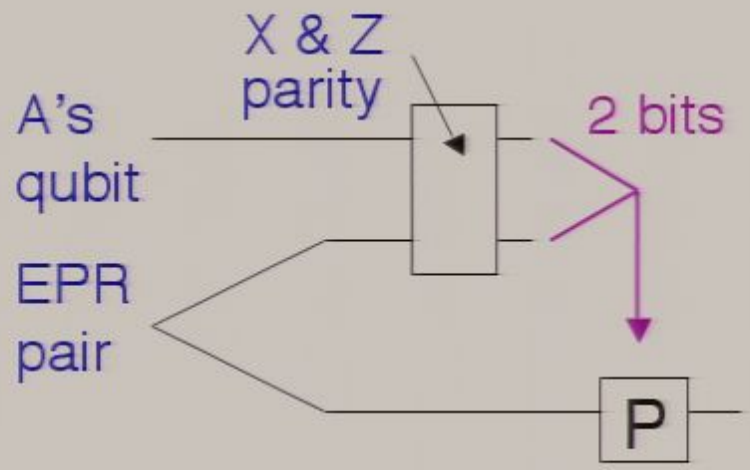
In quantum mechanics, there are incompatible pairs of measurements. For instance, the X and Z measurements from before cannot both be done on the same qubit. This means Alice cannot measure everything about the qubit she wishes to teleport.

However, if we only ask if the X measurements on two qubits give the same or different answers (the "X parity" measurement), that is compatible with the Z parity measurement.

It is possible to create a state (an "EPR pair") that will always give the answer "same" to both the X parity and Z parity measurements. An EPR pair is an example of an entangled state, and has strange non-classical properties.

Quantum Teleportation

In quantum teleportation, Alice and Bob first create an EPR pair, and each takes one of the two qubits.



Then Alice asks if the qubit she wishes to teleport is the same or different from her half of the EPR pair for both X and Z (i.e., she does the X and Z parity measurements).

She sends the result to Bob, who corrects his state appropriately:

X or Z parity	A's qubit & A's EPR	A's and B's EPR	A's qubit & B's EPR
same	same	same	same
different	same	same	different

Teleporting Large Objects

Teleporting a single qubit requires sending 2 bits of information. Teleporting 10^{27} qubits thus requires 2×10^{27} bits, which would take 60 billion years over a 1 Gps line.

In any case, for most large objects, the exact quantum state is unimportant, so quantum teleportation has little to do with science-fiction style teleportation.

Quantum Information

You now have a taste of how quantum information differs from classical information:

- Quantum algorithms
- Quantum computers
- Quantum cryptography

There are others:

- Quantum error correction
- Quantum communication complexity
- And more, including many yet to be discovered.