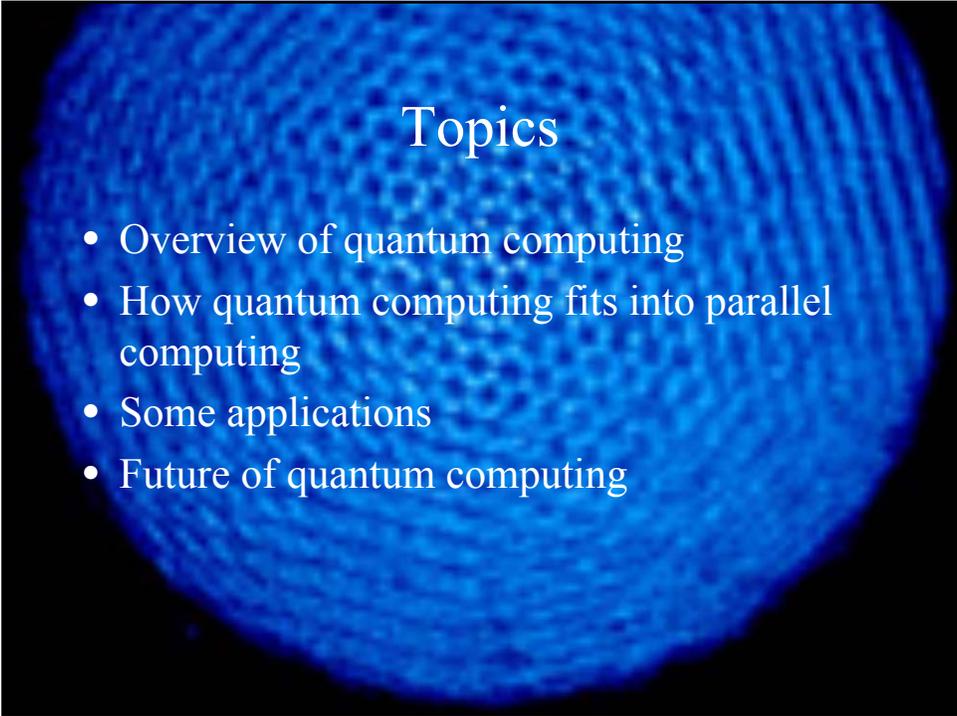
A circular pattern of blue concentric rings, resembling a fingerprint or a ripple in water, set against a black background. The pattern is centered and fills most of the frame.

Quantum Computing

Takahisa Sakurai

A circular pattern of blue concentric rings, resembling a fingerprint or a ripple in water, set against a black background. The pattern is centered and fills most of the frame.

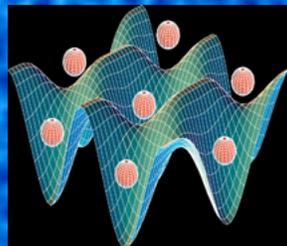
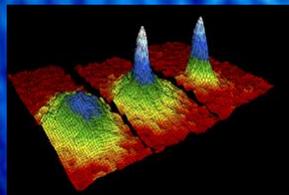
Topics

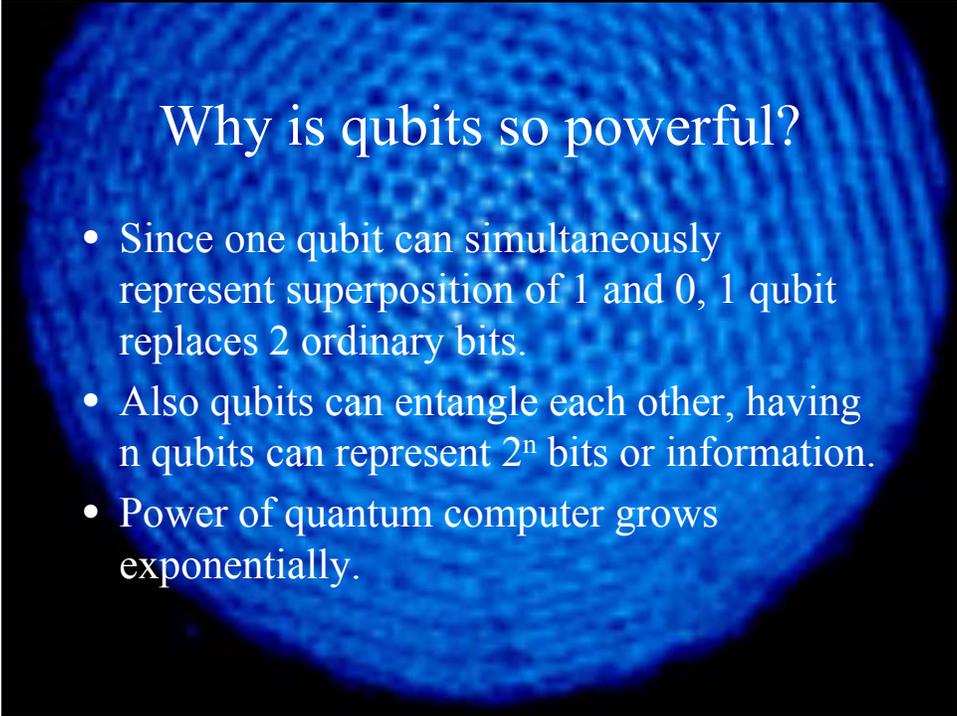
- Overview of quantum computing
- How quantum computing fits into parallel computing
- Some applications
- Future of quantum computing

What is quantum system

- Qubits (quantum bits)
 - Unlike ordinary bit, qubit can exist simultaneously in a *superposition* of both 1 and 0
 - Qubits are physically separated but they can be *entangled* or fate of one qubit ties to other qubit
 - Qubit is implemented by trapping atom into optical lattice, or superconducting circuit

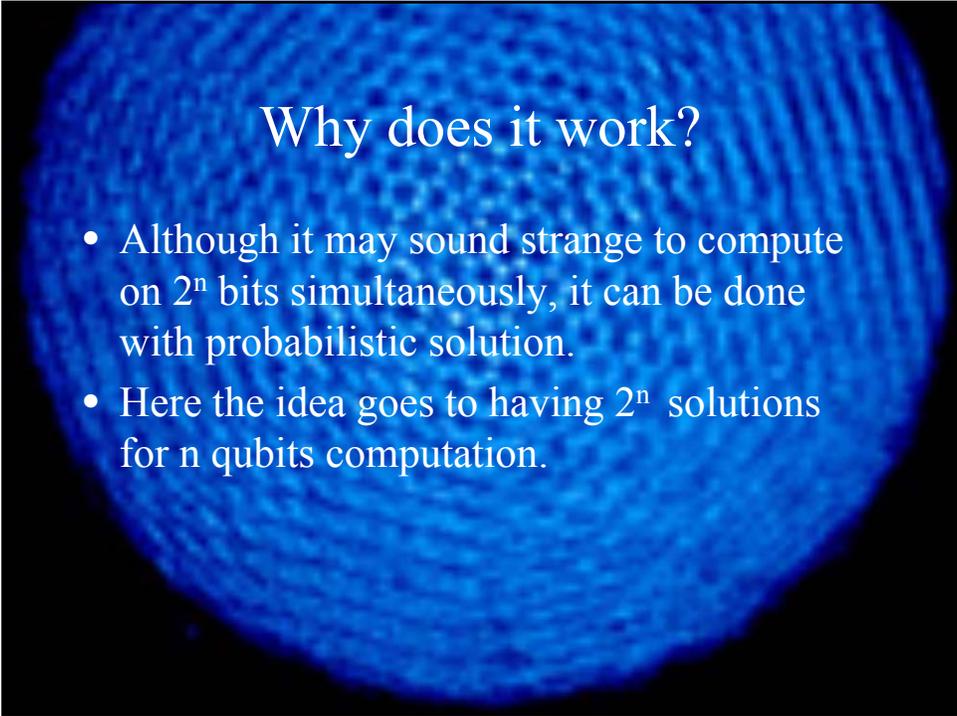
Some images





Why is qubits so powerful?

- Since one qubit can simultaneously represent superposition of 1 and 0, 1 qubit replaces 2 ordinary bits.
- Also qubits can entangle each other, having n qubits can represent 2^n bits or information.
- Power of quantum computer grows exponentially.



Why does it work?

- Although it may sound strange to compute on 2^n bits simultaneously, it can be done with probabilistic solution.
- Here the idea goes to having 2^n solutions for n qubits computation.

Parallelism of quantum computing

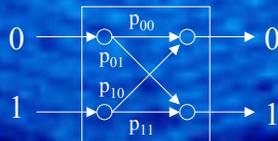
- Quantum computing has unique structure of parallelism
 - Quantum computing operate single instruction on one or more variables containing multiple values.
- Exponential speed up is not a dream !!
 - Since each computation determines 2^n possibilities, it is possible to get unimaginable speed up obtained by ordinal parallel architecture.

Basic operation of qubits

- Although qubits can be operated on quantum gates to compute, they require good understanding of physics and math.
 - The second link I have posted have detailed explanation of this material:
<http://beige.ucs.indiana.edu/B679/>

Showing that it is really parallel

- NOT operation for a qubit
 - Each arrow represents probability of transition
 - To create NOT operation, $p_{00} = p_{11} = 0$ and $p_{10} = p_{01} = 1$
 - However this operation can be done with having 0.5 probability to transition.

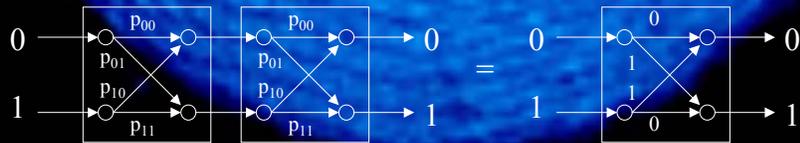


Showing that it is really parallel (cont'd)

- New concept: *probability amplitude*
 - This is idea that for some complex number c , $|c|^2$ is treated as probability.
 - So identical two submachine can be used to implement NOT without using probability or 1 or 0

Showing that it is really parallel (cont'd)

- If $p_{00} = p_{11} = 1/2$ and $p_{10} = p_{01} = 1/2$, then the following two machines produce equal outcome.
- This machine is called $\sqrt{\text{NOT}}$
- In this case math does work.



Showing that it is really parallel (cont'd)

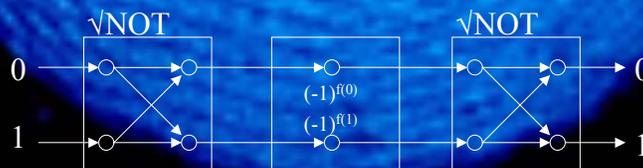
- Quantum algorithms
 - Algorithm that uses quantum computer to solve problem.
 - Although there are difference in computability classes, algorithm for classical algorithm is still algorithm for quantum computer.
 - Now let us use $\sqrt{\text{NOT}}$ machine to solve Deutsch's problem

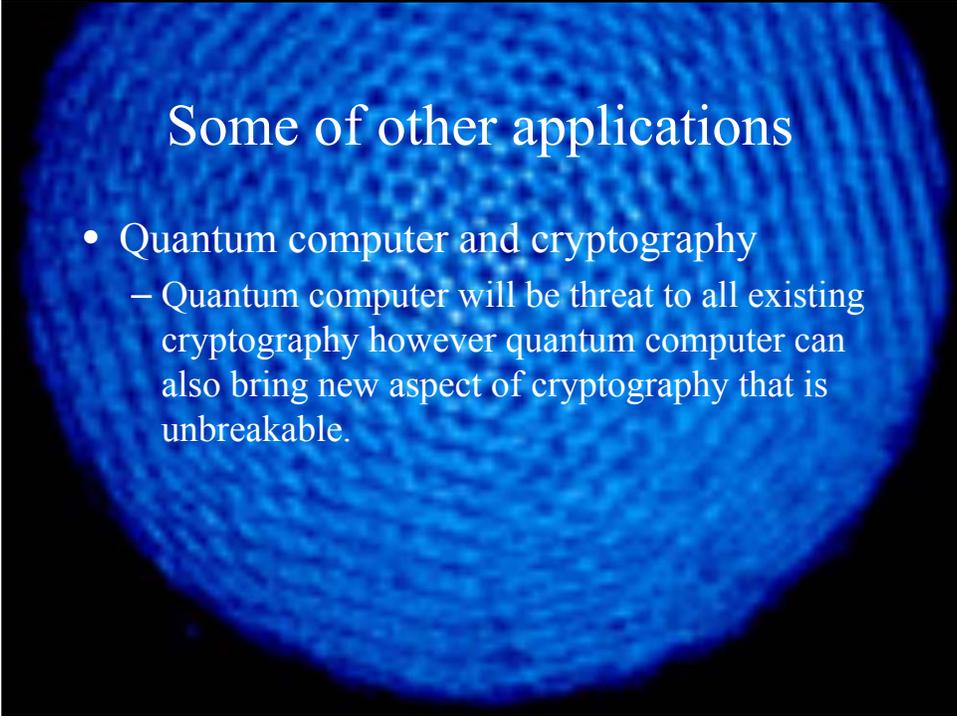
Deutsch's problem

- If you have one function f in $\Sigma = \{0,1\}$, then is it possible to determine if f is constant $\{f(0) = f(1) = 0 \text{ and } f(0) = f(1) = 1\}$ function or balanced function $\{f(0) = 0, f(1) = 0 \text{ and } f(0) = 1, f(1) = 1\}$ by evaluating function f *only once*.

Deutsch's problem (cont'd)

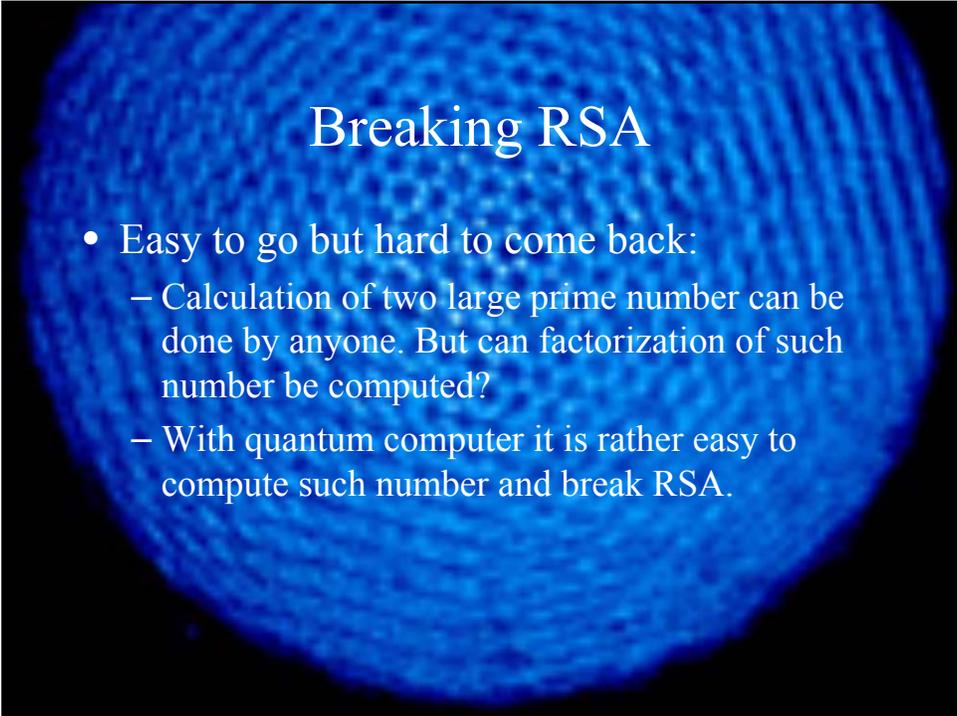
- In general, phase factor of mapping from $\{0,1\}^n$ to $\{0,1\}^m$ is $\exp(2\pi i f(x)/2^m)$ but since Deutsch's problem is $\{0,1\}^2$ to $\{0,1\}^2$ mapping, phase factor is $(-1)^{f(x)}$. So this problem can be solved by following machine:





Some of other applications

- Quantum computer and cryptography
 - Quantum computer will be threat to all existing cryptography however quantum computer can also bring new aspect of cryptography that is unbreakable.



Breaking RSA

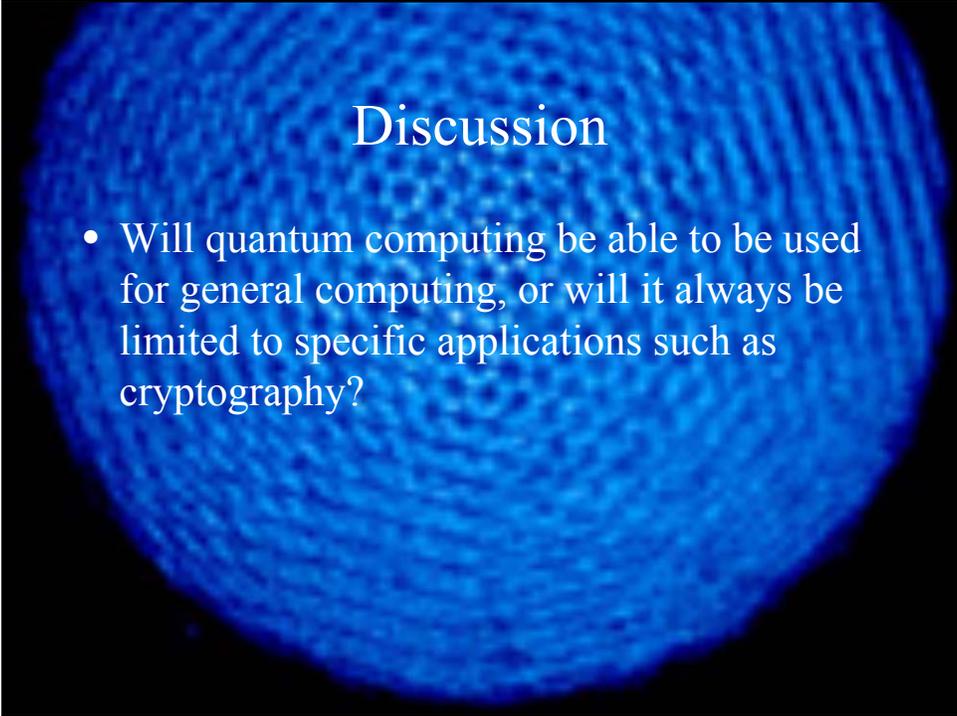
- Easy to go but hard to come back:
 - Calculation of two large prime number can be done by anyone. But can factorization of such number be computed?
 - With quantum computer it is rather easy to compute such number and break RSA.

Quantum cryptography proposal

- (A)
 - Cryptosystems with encoding based on two non-commuting observables proposed by S.Wiesner (1970), and by C.H.Bennett and G.Brassard (1984) [5].
- (B)
 - Cryptosystems with encoding built upon quantum entanglement and the Bell Theorem proposed by A.K.Ekert (1990) [6].
- (C)
 - Cryptosystems with encoding based on two non-orthogonal state vectors proposed by C.H.Bennett (1992) [7].

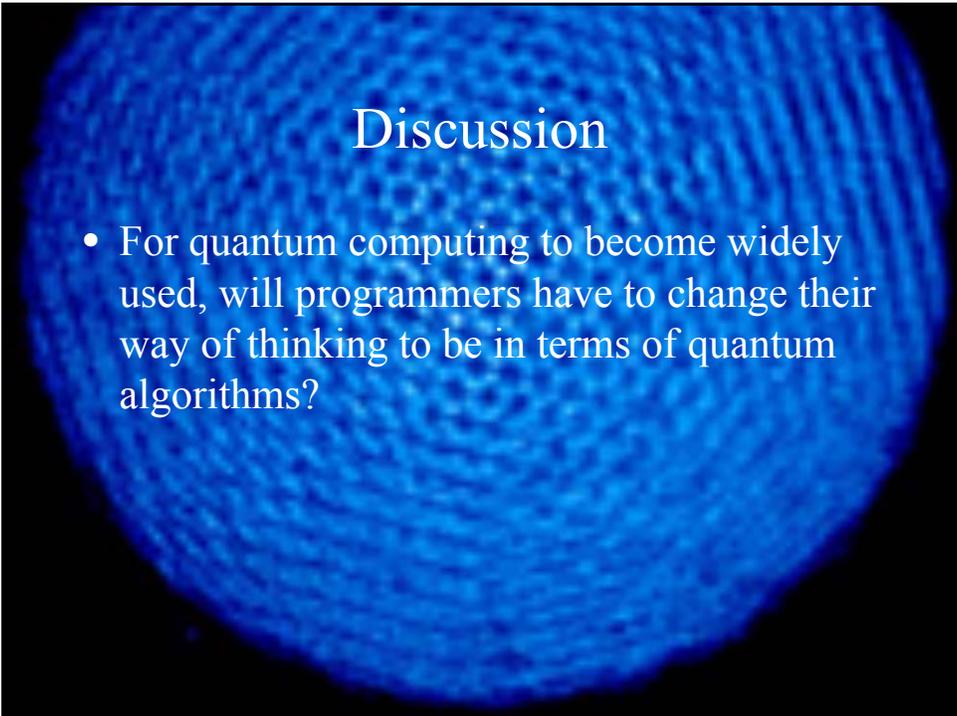
References

- Centre for Quantum Computation. Qubits.org
<http://www.qubit.org/> (particularly tutorials)
- Introduction to Quantum Computing (M743). 5 Feb 2004. Zdzislaw Meglicki
<http://beige.ucs.indiana.edu/B669/>
- NIST Research on Quantum Systems for the "Next" Information Age. 12 Feb 2003. NIST
http://www.nist.gov/public_affairs/factsheet/quantum.htm
- And all published/unpublished document/thesis posted on Qubits.org



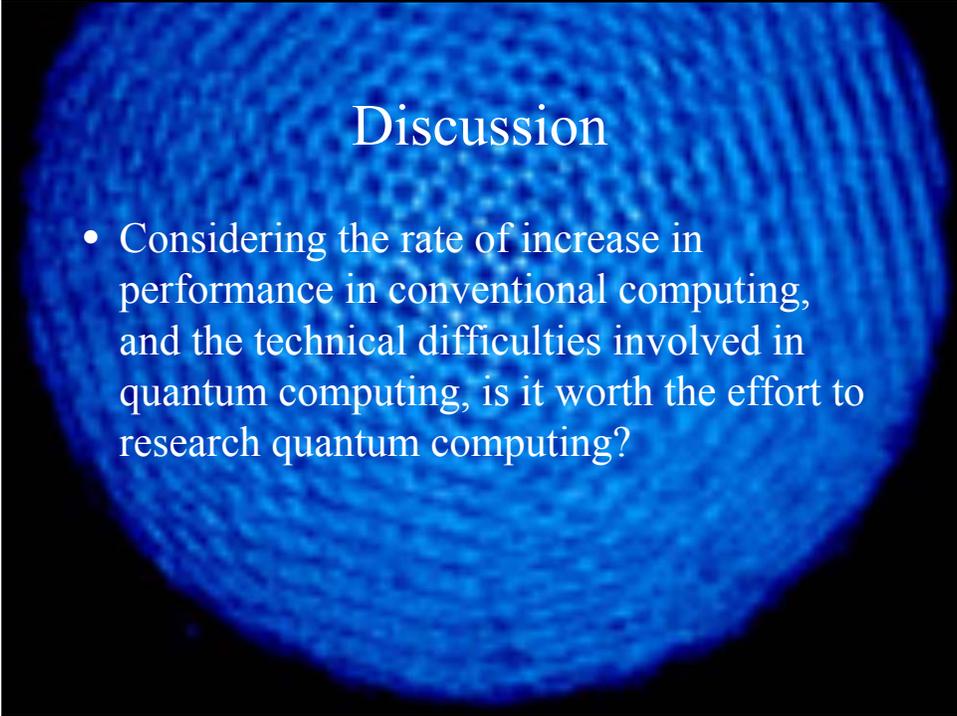
Discussion

- Will quantum computing be able to be used for general computing, or will it always be limited to specific applications such as cryptography?



Discussion

- For quantum computing to become widely used, will programmers have to change their way of thinking to be in terms of quantum algorithms?



Discussion

- Considering the rate of increase in performance in conventional computing, and the technical difficulties involved in quantum computing, is it worth the effort to research quantum computing?