

Classical Computers



Prospects for the future

- Cannot get indefinite speed increases by indefinite miniaturisation
- Can get some advantages from parallel processors (more than one computer chip working together)
- BUT: Some problems will always be difficult for classical computers
- One class of these problems involves the factoring of large numbers into prime factors



Centre for Quantum Computer Technology

Factorizing Large Numbers



- Essential for security of transactions over the internet ("RSA security"), etc
- Example:
 - 127 x 129 = ? Easy! A few minutes
 - ? X ? = 29083 Hard! Maybe an hour
 - "hardness" of factorizing large numbers is the key to internet security
- Best supercomputers today can manage a 140 digit number
- What about a 500 digit number? Forget it!

REMEMBER: Fundamentally, we do not live in a classical world! Enter the Quantum Computer



Centre for Quantum Computer Technology

The Quantum Computer



What can a quantum computer do?

- Quantum computers do the factorization problem 10⁸ times faster than conventional computers
- · Searching through long lists
- Quantum encryption for secure information exchange
- Solving chemical and biological structures
- Modelling the real (quantum) world
- How is this done?



Centre for Quantum Computer Technology

The Quantum Computer



Use quantum particles as the bits in a quantum computer!

Conventional computer memory states:

binary bits

• Quantum computer memory states:

binary *qubits*

- A quantum computer memory can occupy all possible states at the one time
- The solution to the problem appears in the final state of the computer when the state of the qubits are read out
- What can we use as qubits?

Centre for Quantum Computer Technology

Essential Quantum Mechanics



We need to get a feel for these non-classical attributes:

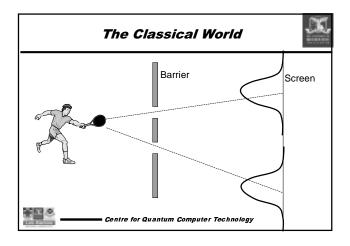
- The art of being in two places at the one time
- · Occupying two states simultaneously
- Entanglement
- "Spooky action at a distance"*

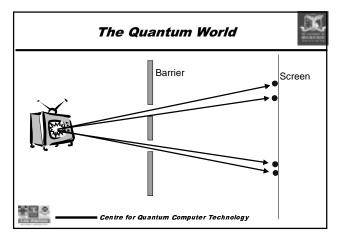
*A. Einstein

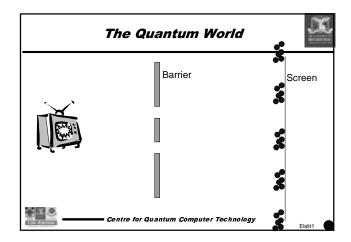


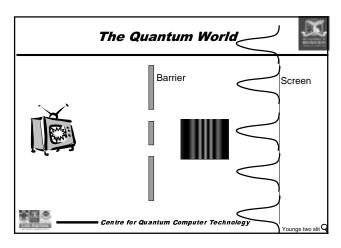
■ Centre for Quantum Computer Technology

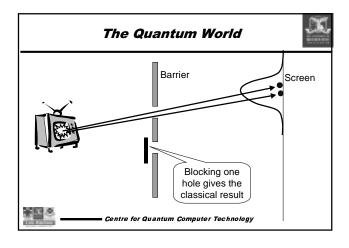
The Classical World Screen Centre for Quantum Computer Technology

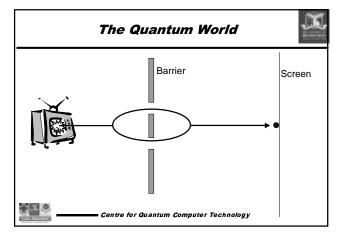




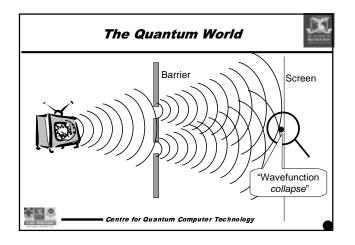


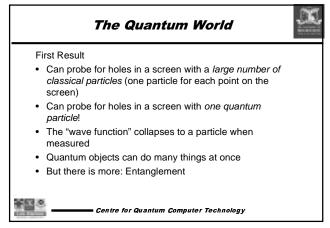


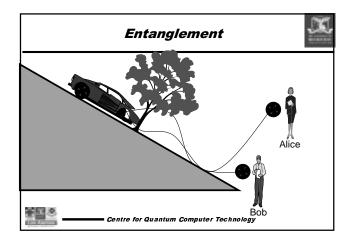


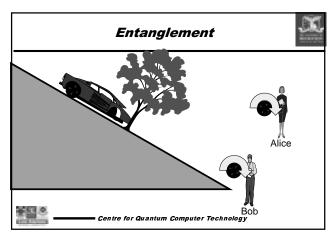


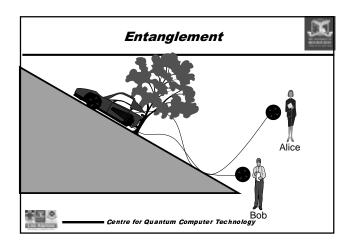
Assoc. Prof. D.N. Jamieson

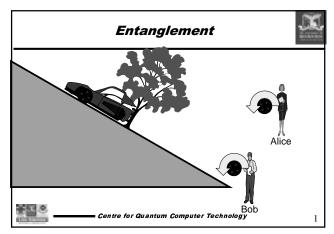




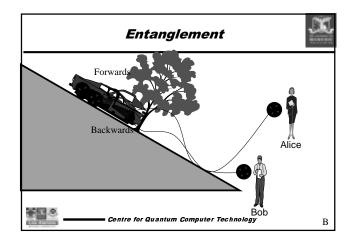


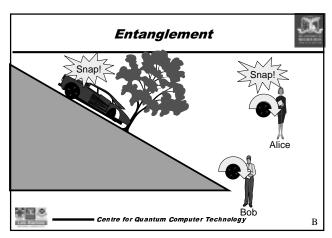


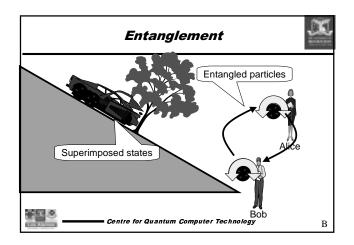


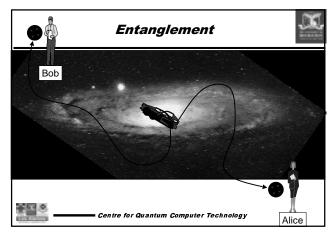


Assoc. Prof. D.N. Jamieson

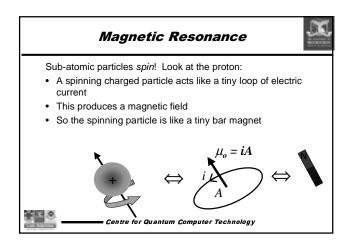




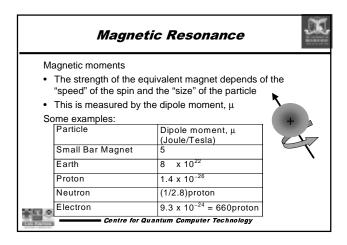


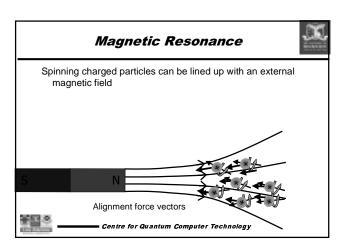


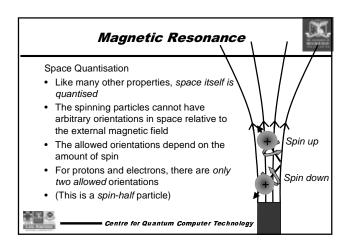
Second Result • Quantum objects can exist in two superimposed (entangled) states • This superimposed state can collapse into a definite state upon measurement • Entangled particles can be created that retain the superimposed state until measurement • But how do we use this for quantum computing?

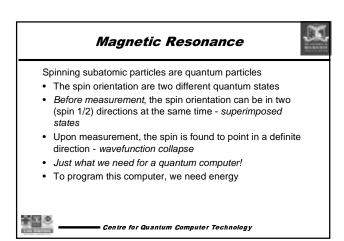


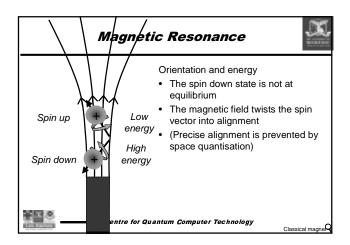
Assoc. Prof. D.N. Jamieson

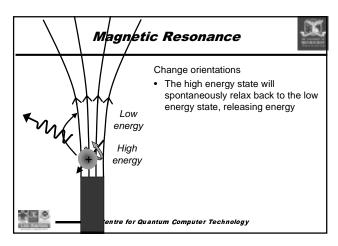


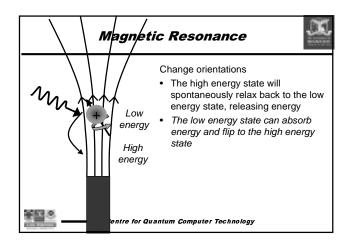


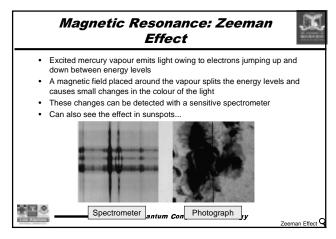


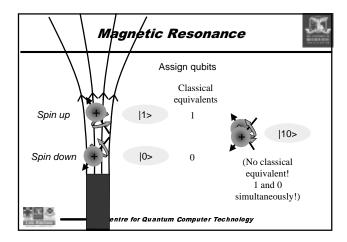


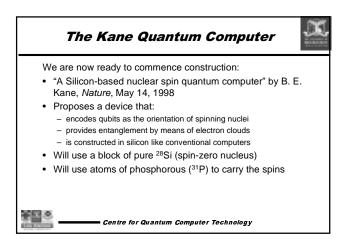


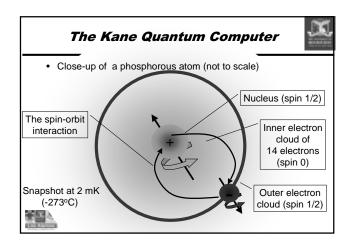


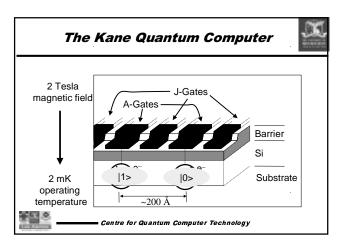


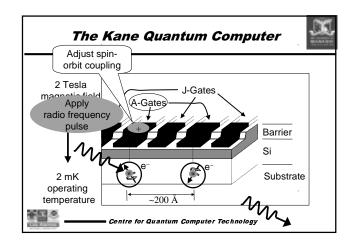


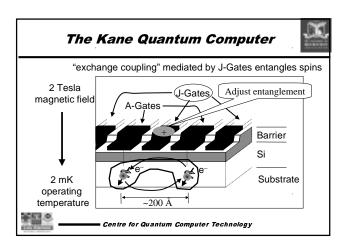


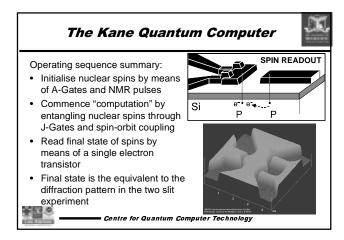


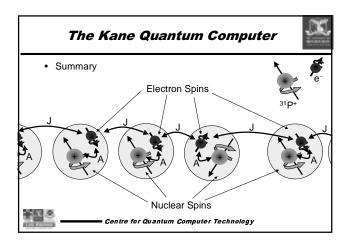


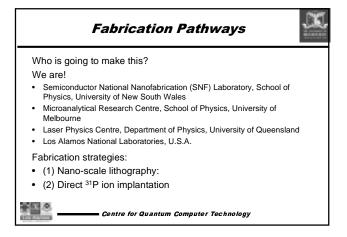


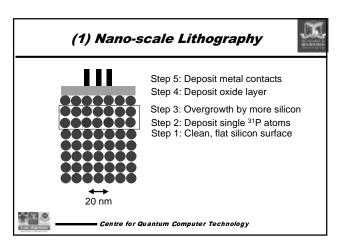


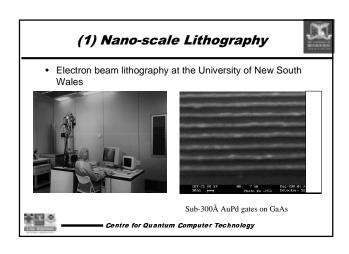


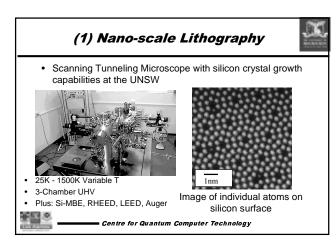


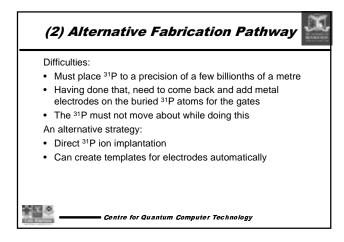


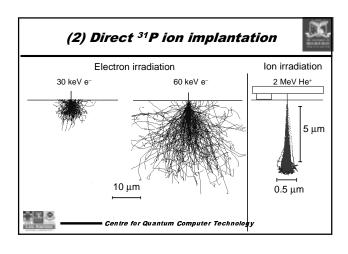


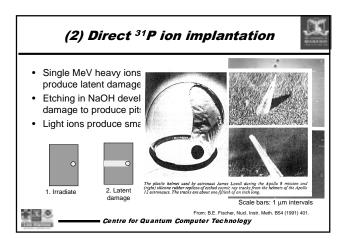


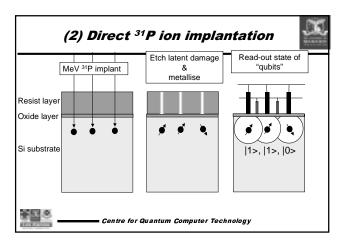


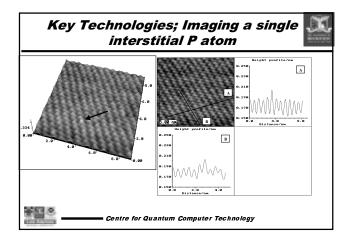


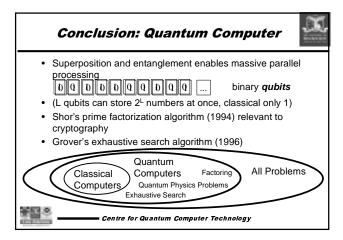












Further Reading



- Australian Centre for Quantum Computer Technology http://www.ph.unimelb.edu.au/~dnj/src/srchome.html
- Oxford quantum computer group http://www.qubit.org
- The Feynman Processor, G. Milburn, Allen & Unwin, 1998
- Quantum Technology, G. Milburn, Allen & Unwin, 1996
- The Large, the Small and the Human Mind, R. Penrose, Cambridge, 1997
- Quantum Teleportation, A. Zeilinger, Scientific American, April 2000
- Physics and the Information Revolution, J. Birnbaum, R.S. Williams, Physics Today, January 2000



Centre for Quantum Computer Technology