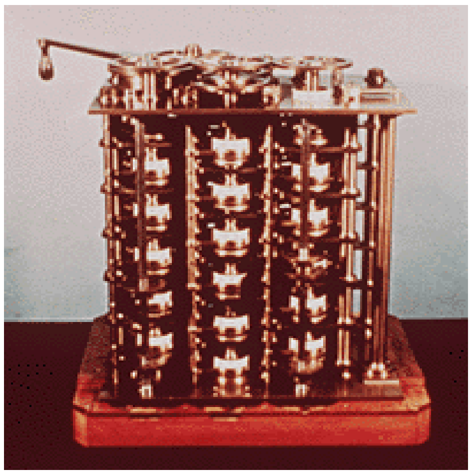
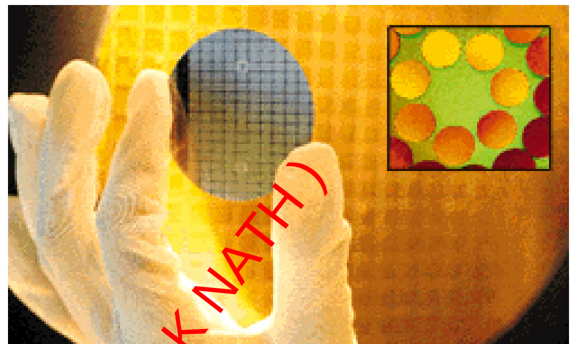
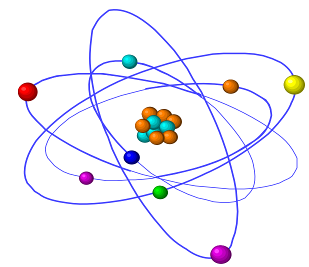
Quantum Computing

Contents

Introduction

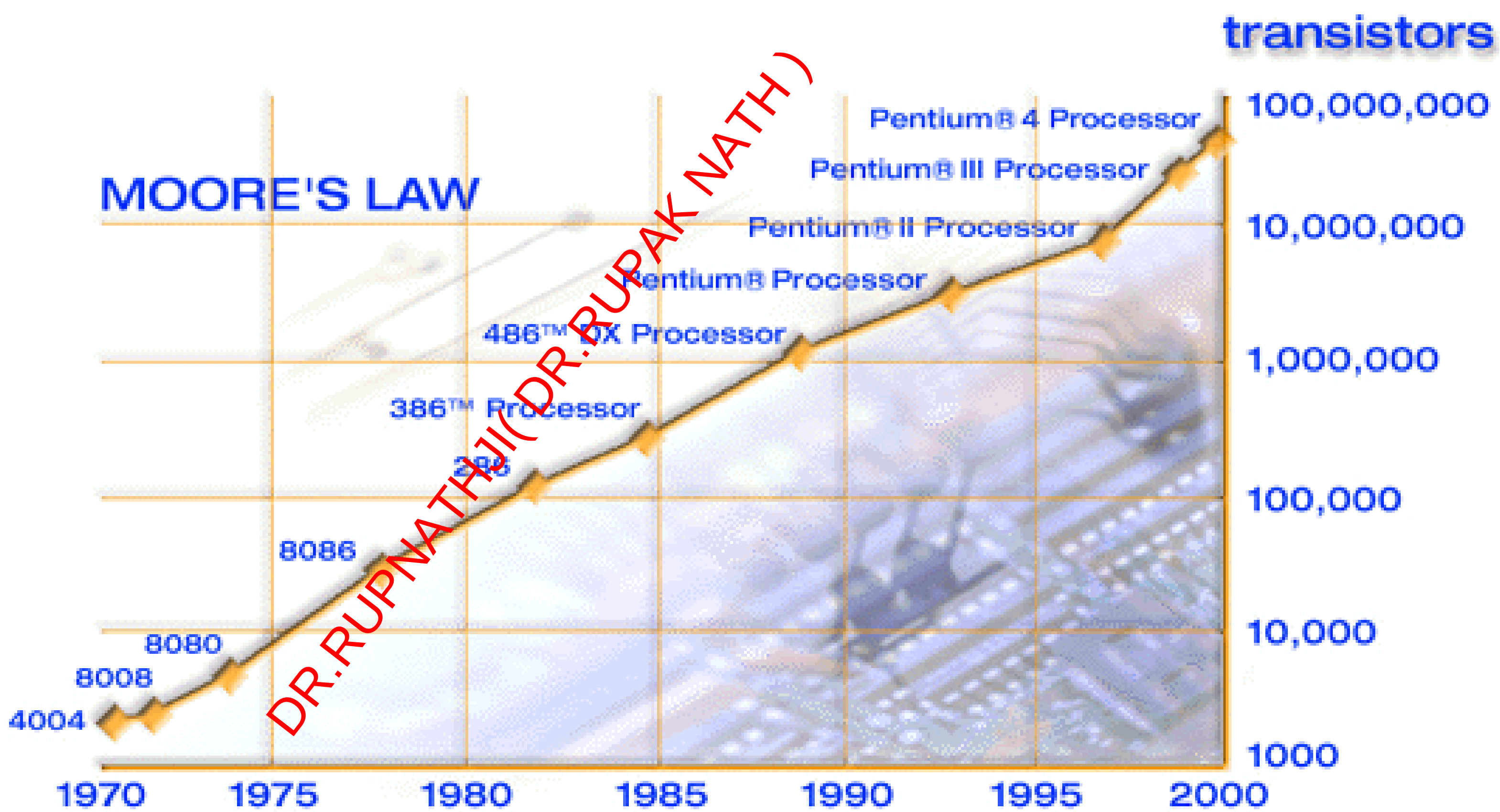






Computer technology is making devices smaller and smaller…

…reaching a point where classical physics is no longer a suitable model for the laws of physics.


transistors
MOORE'S LAW
Pentium® 4 Processor
Pentium® III Processor
Pentium® II Processor
Pentium® Processor
486™ DX Processor
386™ Processor
286
8086
8080
8008
4004
100,000,000
10,000,000
1,000,000
100,000
10,000
1000
1970
1975
1980
1985
1990
1995
2000

Physics and Computation

- Information is stored in a physical medium, and manipulated by physical processes.
- The laws of physics dictate the capabilities of any information processing device.
- Designs of "classical" computers are implicitly based in the the *classical* framework for physics
- Classical physics is known to be incomplete… and has been replaced by a more powerful framework: *quantum mechanics*.

The nineteenth century was known as the machine age, the twentieth century will go down in history as the information age. I believe the twenty-first century will be the quantum age. Paul Davies, Professor Natural Philosophy – Australian Centre for Astrobiology

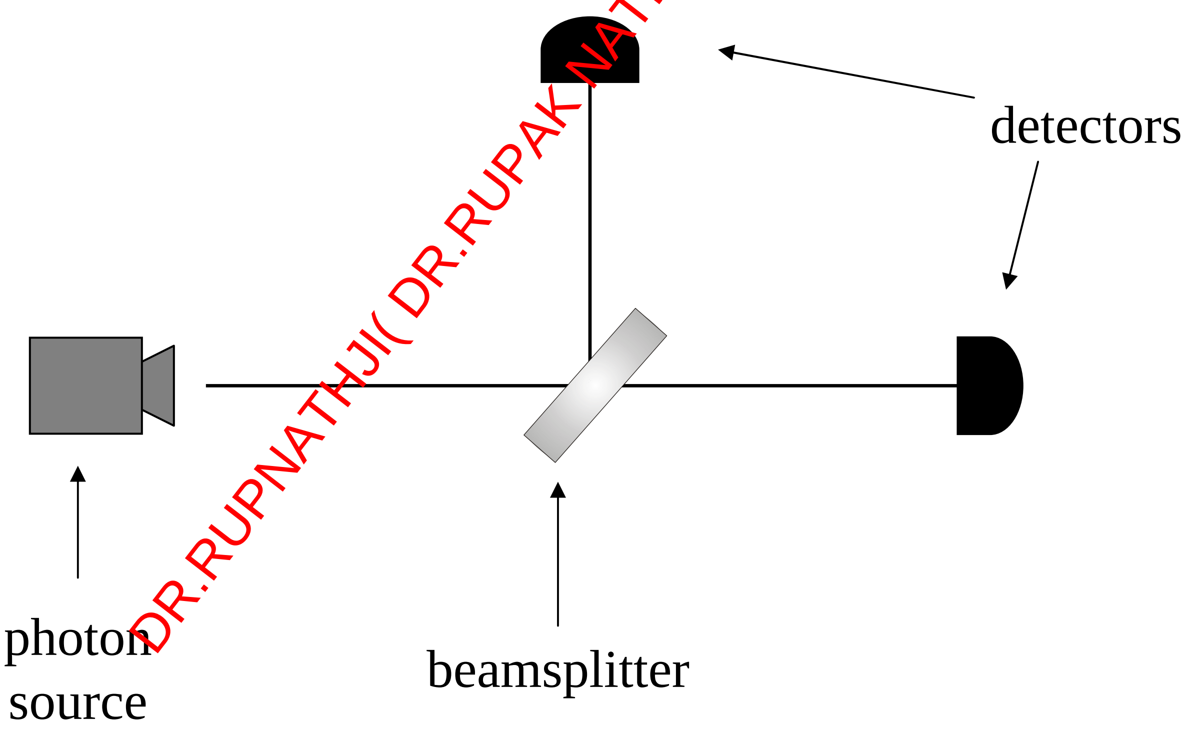
The design of devices on such a small scale will *require* engineers to control quantum mechanical effects.

Allowing computers to take advantage of quantum mechanical behaviour allows us to do *more* than just increasingly many microscopic components onto a silicon chip…

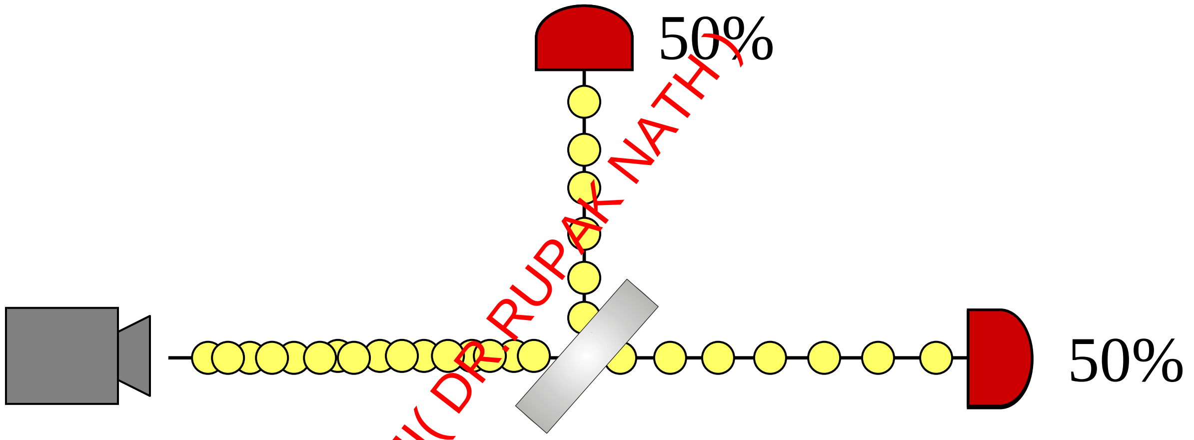
… it gives us a whole new framework in which information can be processed in *fundamentally new ways.*

A simple experiment in optics

…consider a setup involving a photon source,
a half-silvered mirror (beamsplitter),
and a pair of photon detectors.



Now consider what happens when we fire a single photon into the device…

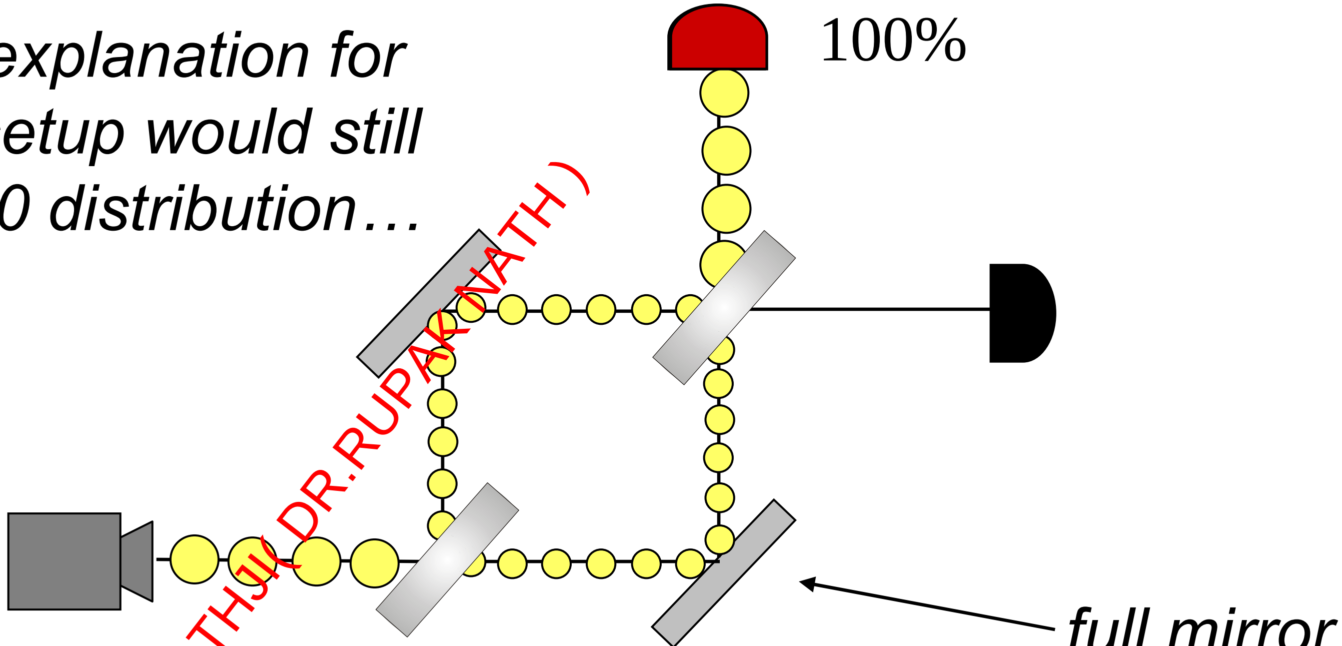


Simplest explanation: beam-splitter acts as a classical coin-flip, randomly sending each photon one way or the other.

The "weirdness" of quantum mechanics…

… consider a modification of the experiment…

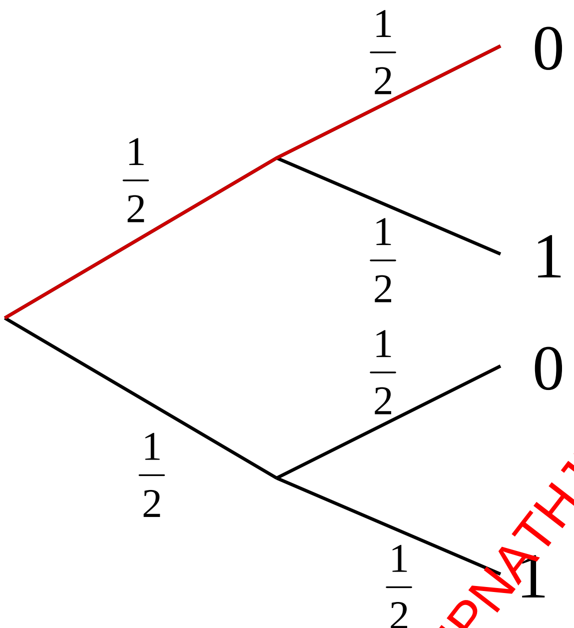
The simplest explanation for the modified setup would still predict a 50-50 distribution…



The simplest explanation is wrong!

Classical probabilities…

Consider a computation tree for a simple two-step (classical) probabilistic algorithm, which makes a coin-flip at each step, and whose output is 0 or 1:



The probability of the computation following a given path is obtained by multiplying the probabilities along all branches of that path… in the example the probability the computation follows the red path is

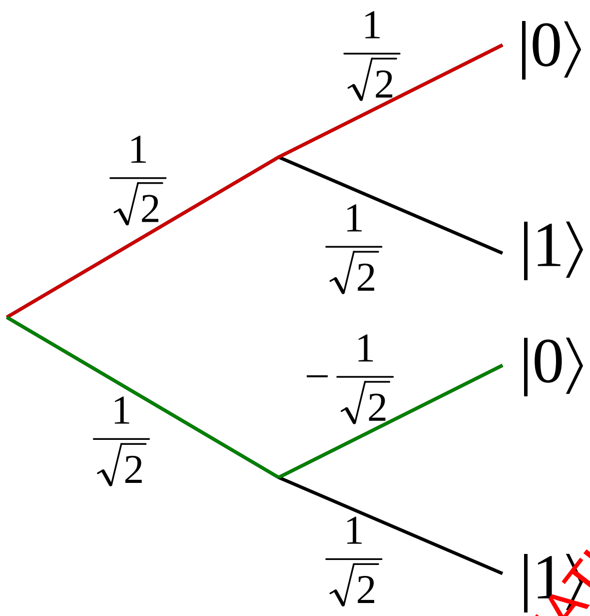
$$\frac{1}{2}\cdot\frac{1}{2}=\frac{1}{4}$$

The probability of the computation giving the answer 0 is obtained by adding the probabilities of all paths resulting in 0:

$$\frac{1}{4}+\frac{1}{4}=\frac{1}{2}$$

…vs quantum probabilities …

In quantum physics, we have probability *amplitudes,* which can have complex phase factors associated with them.



The probability *amplitude* associated with a path in the computation tree is obtained by multiplying the probability *amplitudes* on that path. In the example, the red path has amplitude 1/2, and the green path has amplitude –1/2.

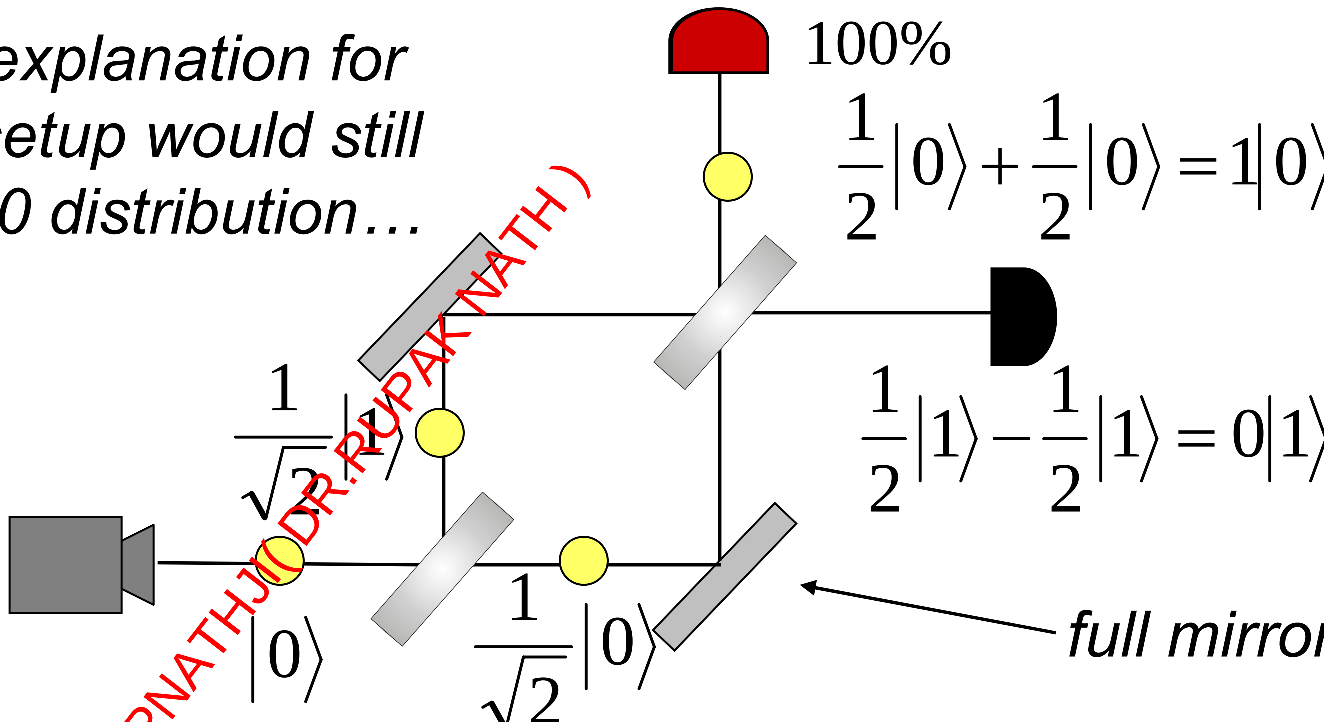
The probability amplitude for getting the answer $|0\rangle$ is obtained by adding the probability amplitudes… the phase factors can lead to cancellations! The probability of obtaining $|0\rangle$ is obtained by squaring the total probability amplitude. In the example the probability of getting $|0\rangle$ is

$$\left(\frac{1}{2}-\frac{1}{2}\right)=0$$

Explanation of experiment

… consider a modification of the experiment…

The simplest explanation for the modified setup would still predict a 50-50 distribution…



Quantum mechanics and information

Any physical medium capable of representing 0 and 1 is in principle capable of storing any linear combination $\alpha_0|0\rangle + \alpha_1|1\rangle$

What does $\alpha_0|0\rangle + \alpha_1|1\rangle$ really mean??

It's a "mystery". THE mystery. We don't understand it, but we can tell you how it works. (Feynman)

Uncertainty

quantum world is irreducibly small so it's impossible to measure a quantum system without having an effect on that system as our measurement device is also quantum mechanical.

There is a trade off - the properties occur in complementary pairs (like position and momentum, or vertical spin and horizontal spin)

Entanglement

Two classical bits can be 00 or 01 or 10 or 11. We can ask the value of the first bit without affecting the second bit.

Two qubits could be in the state

$$1 / 2 \; (|01> + |10>)$$

The first qubit is neither |0> nor |1>.

It's not even a superposition of |0> and |1> because the state is not separable: the value of the first qubit is *entangled* with the value of the second.
We can't discover value of first qubit without affecting the second. Say we measure it and get 0; that means the state of the system is now |01> and therefore the second qubit is now |1>. But it wasn't |1> before; it was entangled with the first qubit.

Superposition

Superposition means a system can be in two or more of its states simultaneously. For example a single particle can be traveling along two different paths at once. This implies that the particle has wave-like properties, which can mean that the waves from the different paths can *interfere* with each other.

A superposition is not necessarily entangled. Consider

$$1 / 2 \, (|10\rangle + |11\rangle).$$

We can measure the first qubit without affecting the second.

The ability for the particle to be in a superposition is where we get the parallel nature of quantum computing

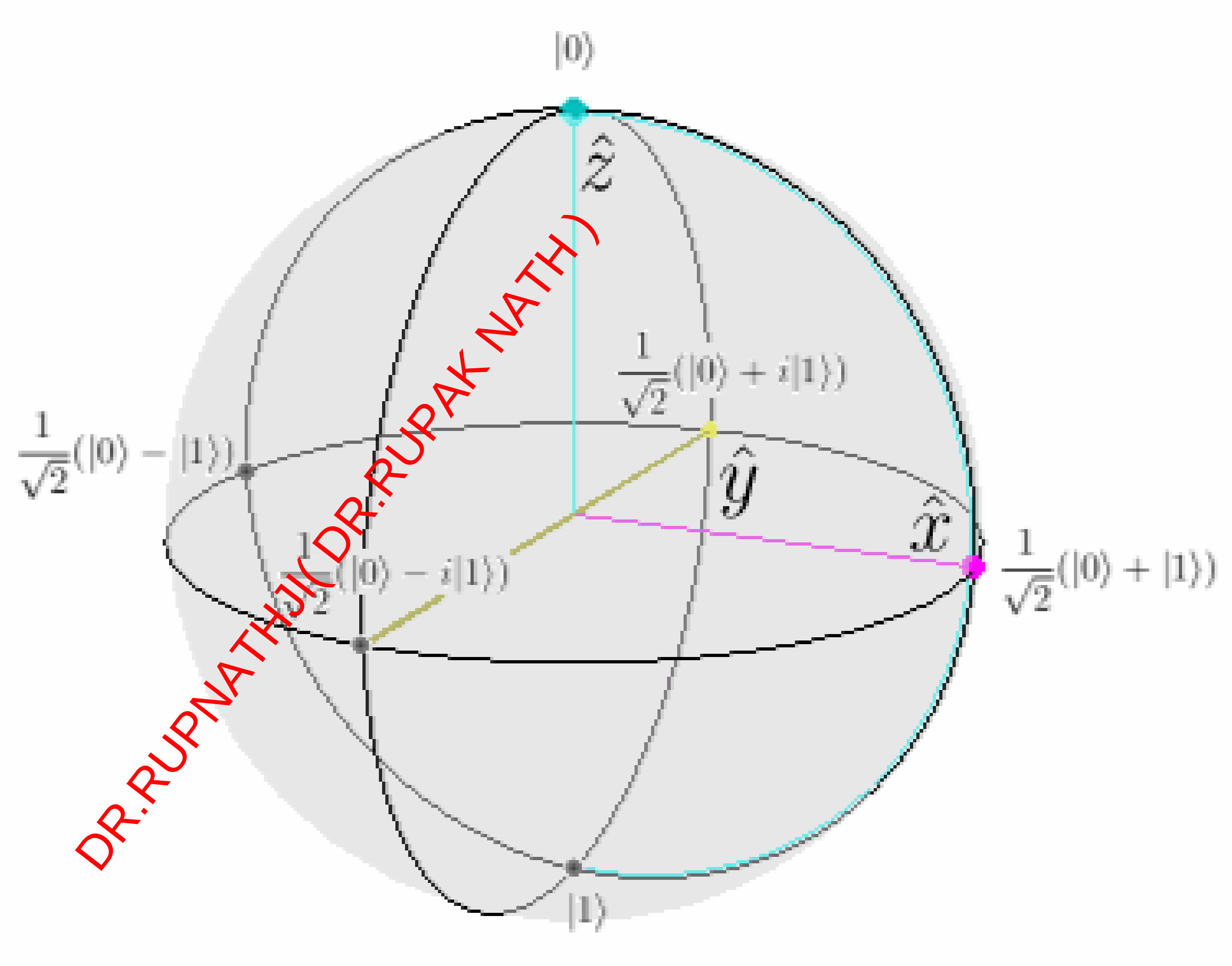
Qubit

$|0\rangle$ corresponds to $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$

$|1\rangle$ corresponds to $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$

$\alpha_0|0\rangle + \alpha_1|1\rangle$ corresponds to $\alpha_0\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \alpha_1\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$

State of a single qubit on the Bloch sphere



More than one qubit

If we concatenate two qubits

$$(\alpha_0|0\rangle + \alpha_1|1\rangle)\ (\beta_0|0\rangle + \beta_1|1\rangle)$$

we have a 2-qubit system with 4 basis states

$$|0\rangle|0\rangle = |00\rangle \quad |0\rangle|1\rangle = |01\rangle \quad |1\rangle|0\rangle = |10\rangle \quad |1\rangle|1\rangle = |11\rangle$$

and we can also describe the state as

$$\alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle$$

or by the vector

$$\begin{pmatrix} \alpha_0\beta_0 \\ \alpha_0\beta \\ \alpha_1\beta_0 \\ \alpha_1\beta_1 \end{pmatrix} = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \otimes \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix}$$

Generalization to *n* qubits

The general state of *n* qubits is $\sum_{x\in\{0,1\}^n} \alpha_x |x\rangle$

where the α_x are complex numbers satisfying the normalization constraint

$$\sum_{x\in\{0,1\}^n} |\alpha_x|^2 = 1.$$

In general we can have arbitrary superpositions

$$\alpha_{00}|0\rangle|0\rangle + \alpha_{01}|0\rangle|1\rangle + \alpha_{10}|1\rangle|0\rangle + \alpha_{11}|1\rangle|1\rangle$$

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$$

Classical vs. Quantum

Classical bits:

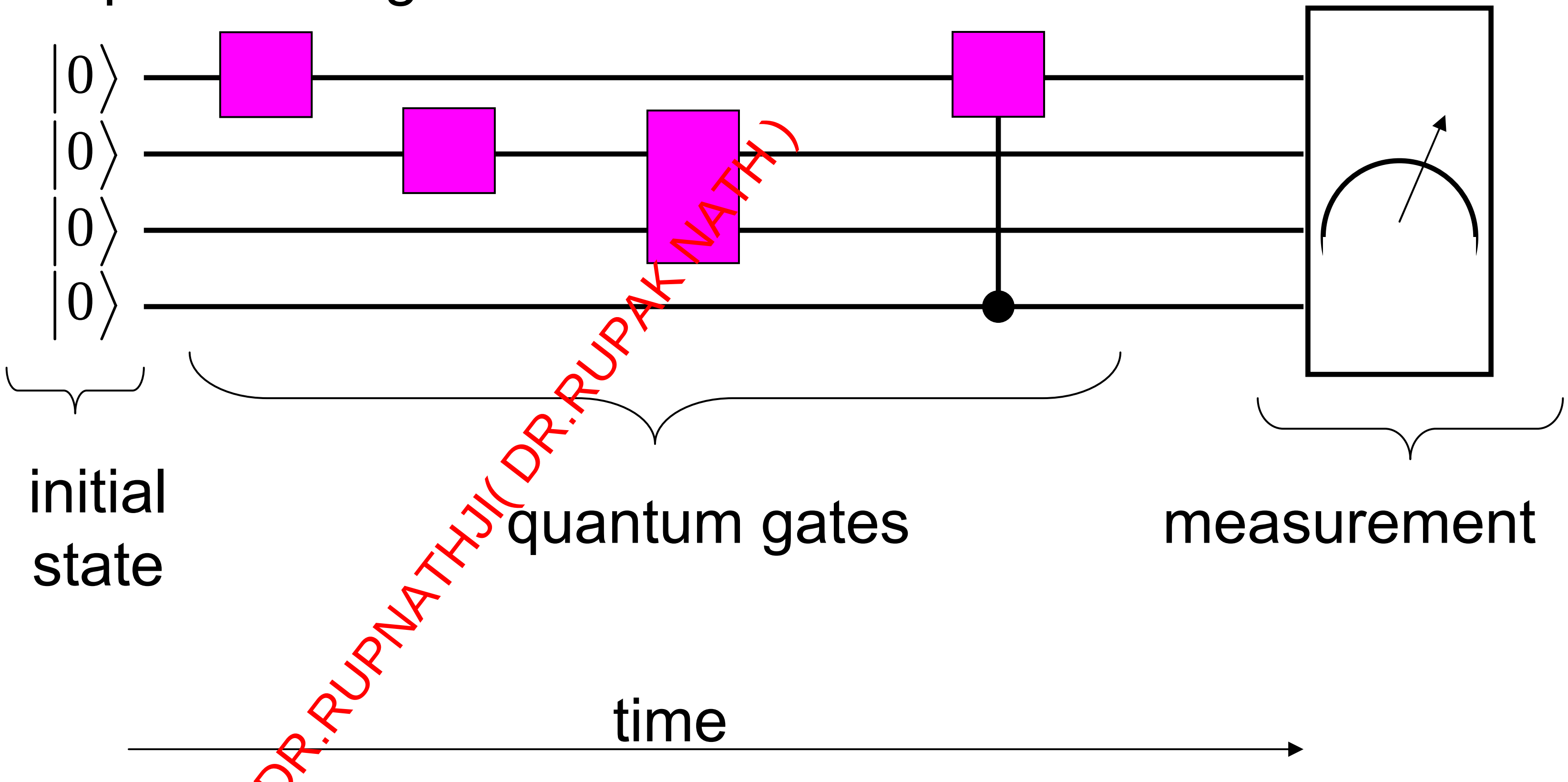
- can be measured completely,
- are not changed by measurement,
- can be copied,
- can be erased.

Quantum bits:

- can be measured partially,
- are changed by measurement,
- cannot be copied (No cloning theorem)
- cannot be erased.

Quantum circuit

A quantum circuit provides an visual representation of a quantum algorithm.



Properties of Quantum Circuits

1. They are acyclic (no loops - runs once from left to right).
2. No FANIN, as FANIN implies that the circuit is NOT reversible.
3. No FANOUT, as we can't copy a qubit's state during the computational phase because of the no-cloning theorem.

Single-qubit quantum logic gates

Pauli gates

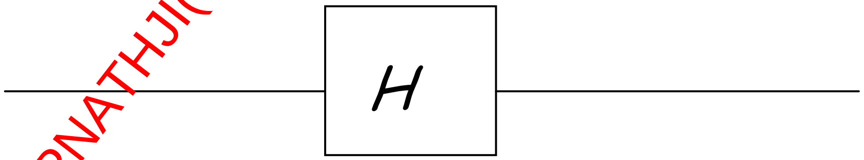
$$X=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix};\quad Y=\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix};\quad Z=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$$

NOT gate

$$|0\rangle \longrightarrow X \longrightarrow |1\rangle,$$

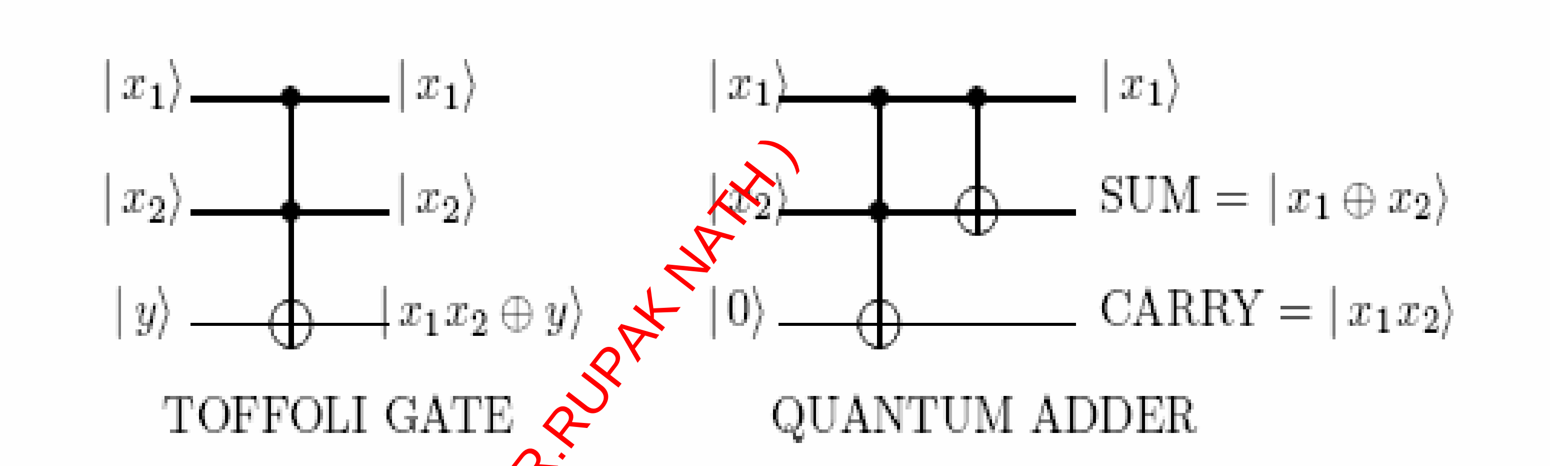
$$|1\rangle \longrightarrow X \longrightarrow |0\rangle,\quad \alpha|0\rangle+\beta|1\rangle \rightarrow X \rightarrow \beta|0\rangle+\alpha|1\rangle.$$

Hadamard gate



$$H|0\rangle=\frac{|0\rangle+|1\rangle}{\sqrt{2}};\quad H|1\rangle=\frac{|0\rangle-|1\rangle}{\sqrt{2}};\quad H=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

Multiple-qubit quantum logic gates



$$|x_1, x_2\rangle\,|0\rangle \mapsto |x_1, x_2\rangle\,|x_1 \wedge x_2\rangle$$

AND Gate

$$|x_1, x_2\rangle\,|1\rangle \mapsto |x_1, x_2\rangle\,|x_1 \uparrow x_2\rangle$$

NAND Gate

Quantum Parallelism

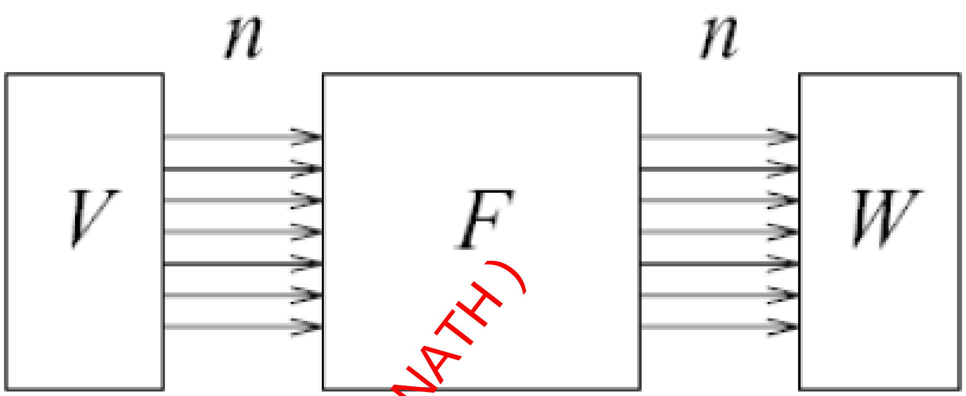
Why are quantum computers capable of solving seemingly very difficult mathematical problems?

Since quantum states can exist in exponential superposition, a computation of a function being performed on *quantum states* can process an *exponential number of possible inputs* in a single evaluation of *f* :

$$\sum_{i=0}^{2^n-1} \alpha_x |x\rangle \longrightarrow \boxed{f} \longrightarrow \sum_{i=0}^{2^n-1} \alpha_x | f(x)\rangle$$

By exploiting a phenomenon known as *quantum interference*, some *global properties* of *f* can be deduced from the output.

Quantum Computer



Takes n input qubits from register V, and producing n output qubits in register W

F computes W = √ v

V is a superposition of all integers from 0 to 2^{n}.

F calculates the square roots of all the integers in parallel. Measuring gives only one of them in W.

We need to arrange F so that the probability amplitudes of the output state strongly favor the desired output from F.

Quantum Algorithms

Integer Factorization (basis of RSA cryptography):

Given N = pq, find p and q.

Discrete logarithms (basis of DH crypto):

Given N, g and x, compute r such that $g^r \equiv x \pmod{N}$.

Computational Complexity Comparison

	Classical	Quantum
Factoring	$e^{O\left(n^{1/3}\log^{2/3} n\right)}$	$O(n) \in e^{O(\log n)}$
Elliptic Curve Discrete Logarithms	$e^{O(n)}$	$O(n) \in e^{O(\log n)}$

(in terms of number of group multiplications for n-bit inputs)

Which cryptosystems are threatened by Quantum Computers??

Information security protocols must be studied in the context of quantum information processing.

The following cryptosystems are insecure against such quantum attacks:

- *RSA (factoring)*
- *Rabin (factoring)*
- *ElGamal (discrete log, including ECC)*
- *Buchmann-Williams (principal ideal distance problem)*
- *and others…*

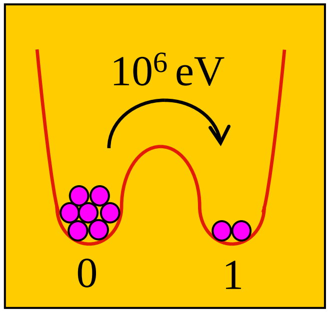
Quantum Information Security

We can exploit the eavesdropper detection that is intrinsic to quantum systems in order to derive new "unconditionally secure" information security protocols.

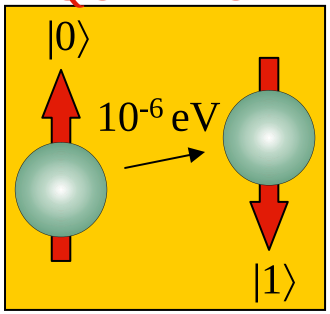
- Quantum key distribution (available now/soon)
- Quantum random number generation (available now/soon)
- Quantum money (require stable quantum memory)
- Quantum digital signatures (requires quantum computer)
- Quantum secret sharing (requires quantum computer)
- Multi-party quantum computations

Quantum Information is Fragile

CLASSICAL



QUANTUM



- low energy
  - control of operations
    - superpositions are very fragile
      - isolation from environment

Devices for Quantum Computing

- Atom traps
- Cavity QED
- Electron floating on helium
- Electron trapped by surface acoustic waves
- Ion traps
- Nuclear magnetic resonance (NMR)
- Quantum optics
- Quantum dots
- Solid state
- Spintronics
- Superconducting Josephson junctions
- and more…