Quantum Computing and Cryptography

David Gessel

1.0 Introduction

2.0 Classical computing, basic definition

3.0 Basic principles of Quantum Mechanics

4.0 Basic principles of Quantum Computing

5.0 Applications: Cryptography, Cryptoanlysis

6.0 Practical Implementations

7.0 Conclusion

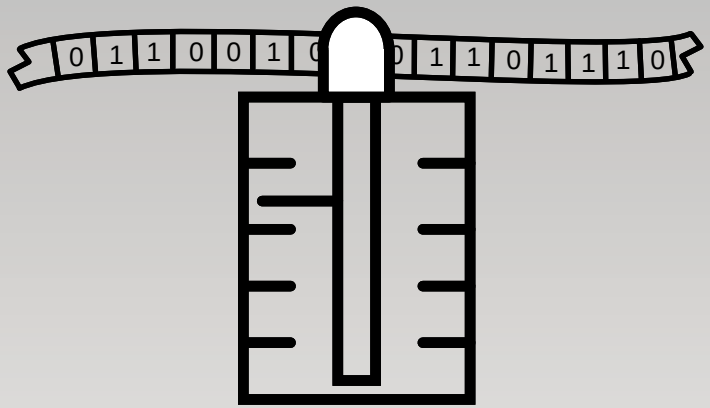
2.0 Classical Computing

2.1 Turing Machines

2.2 Dimensions: Clock, Complexity, Parallel

2.3 P, nP, Hard Problems, and Intractability

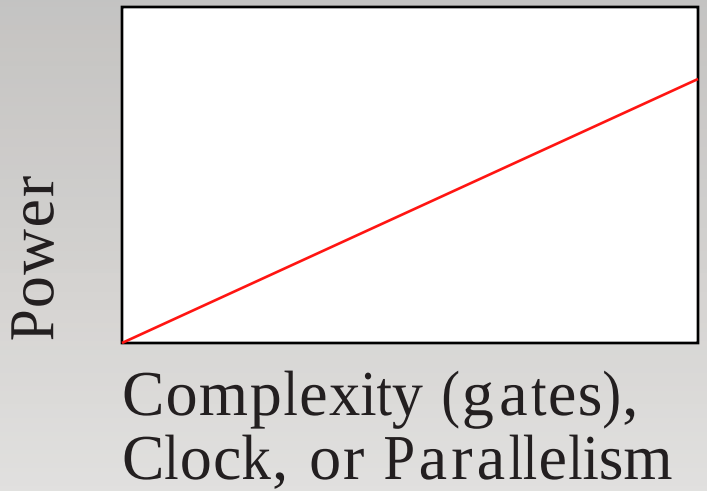
2.1 Turing Machines



Reads one bit at a time from the tape, depending on the internal state, writes a new bit on the tape

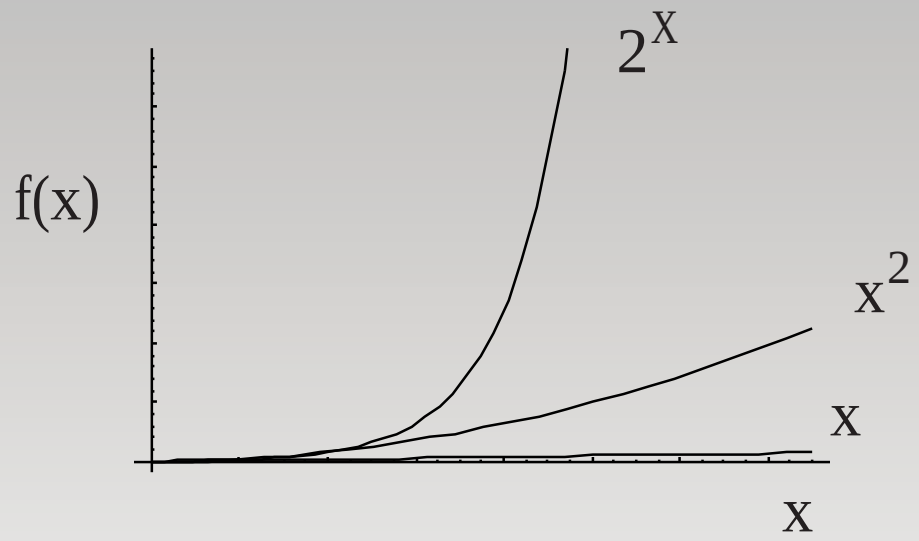
Church's Thesis: Any computable function can be computed on a Turing machine. (Approx 1930)

2.2 Complexity of Classical Systems



The complexity of classical systems is increasing exponentially such that $P = 2^{(t/1.5)}$

2.3 P, nP



Multiplication is polynomial (P)
Factorization is exponential (nP)*

*(not proven)

3.0 The Basics of Quantum Mechanics

3.1 Uncertainty and Heizenberg

3.2 Spin, Polarization

3.3 Two Slit Experiment

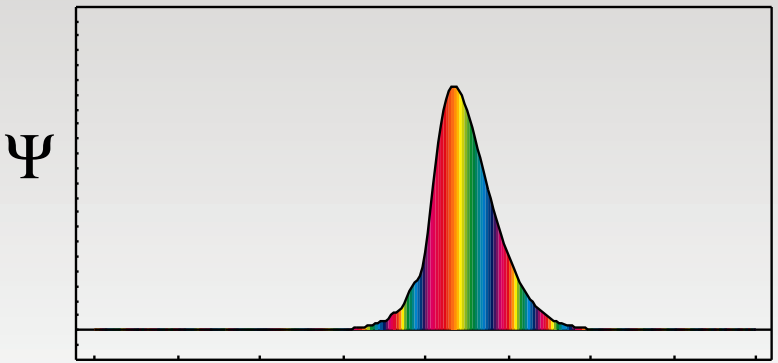
3.4 Quantum Interference

3.5 Spooky Action at a Distance

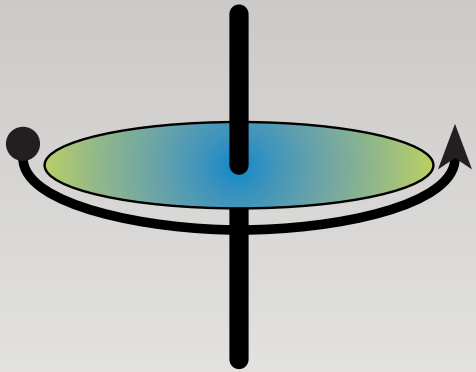
3.1 Uncertainty, Ψ

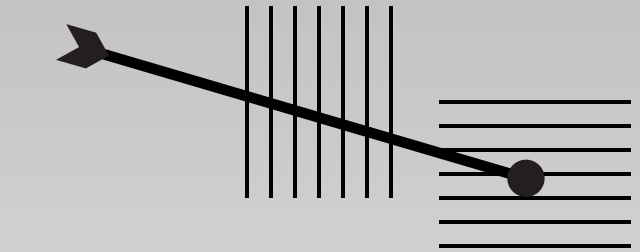
$$\Delta p \Delta x \; ‘ \; h$$

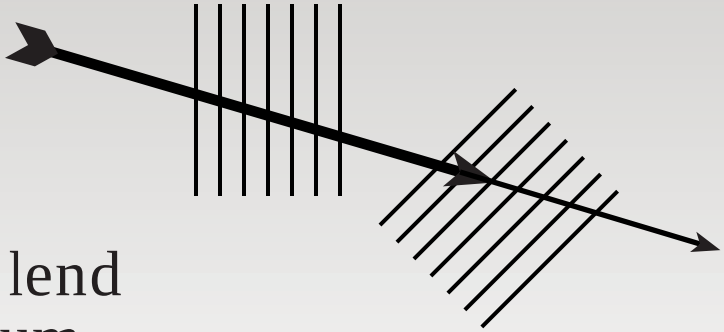
p = momentum
x = position
Planck's constant, h = 6 x10 $^{-27}$ gm cm 2 /sec



3.2 Spin and Polarization

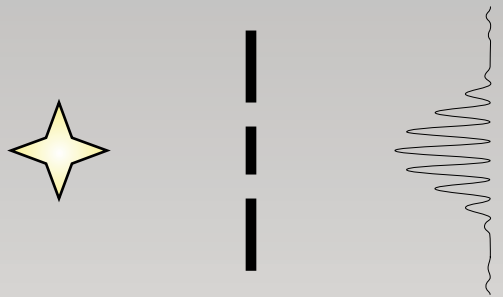






Observables which lend themselves to quantum experimentation.

3.3 Two Slit Experiment



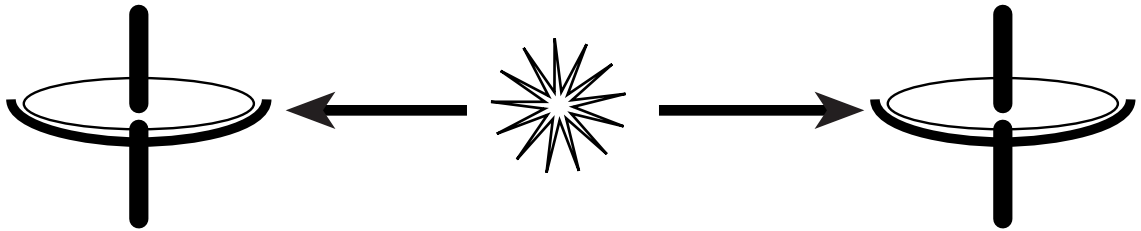
Interference is observed even one photon at a time.

3.4 Quantum Interference

Detector 2 sees no Photons, defying classical expectations

Blocking one path restores 50/50 detection, even a photon at a time.

3.5 Spooky Action at a Distance (EPR)



Particles are entangled until measurement. Measuring one defines the spin of the other, no matter how far apart.

(Einstein, Podolsky, and Rosen - 1935)

4.0 The Basics of Quantum Computing

4.1 What is a Quantum Computer

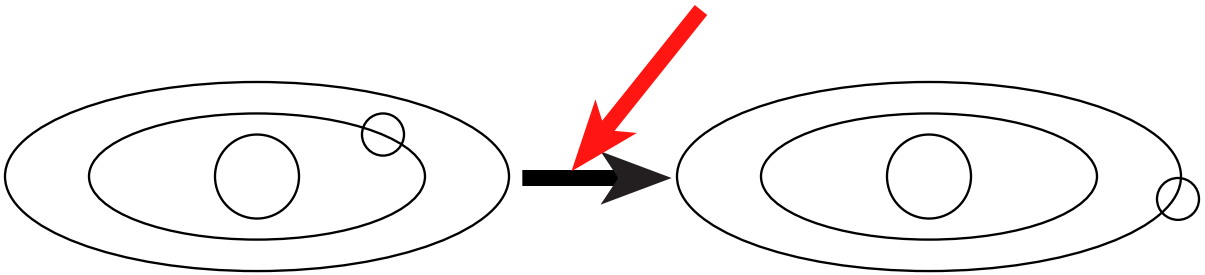
4.2 Qubits

4.3 Entangled Registers

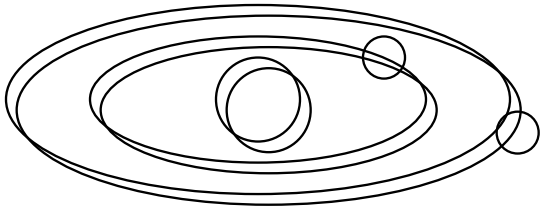
4.4 CNOT Gate

4.1 What is a Quantum Computer

Feynman, 1982: proposed a computer based on quantum interactions.
Deutsch, 1985: showed that Feynman's computer can, in principle, model any physical process exactly.



4.2 Qubits

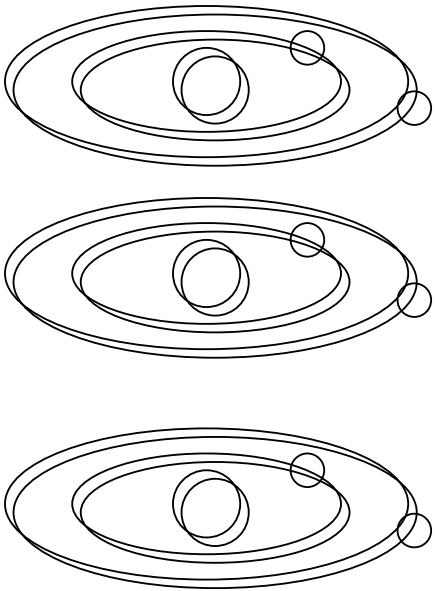


A qubit is a particle set into a superposition of states, both 1 and 0.

Each entangled state pair represents a dimension for the system of qubits

$\{|0^{>}, |1^{>}\}$

4.3 Entangled Registers



$P = 2^n$

P = power

n = number of qubits

3 qubits = 2^3

$a_1|000\rangle$

$a_2|001\rangle$

$a_3|010\rangle$

$a_4|011\rangle$

$a_5|100\rangle$

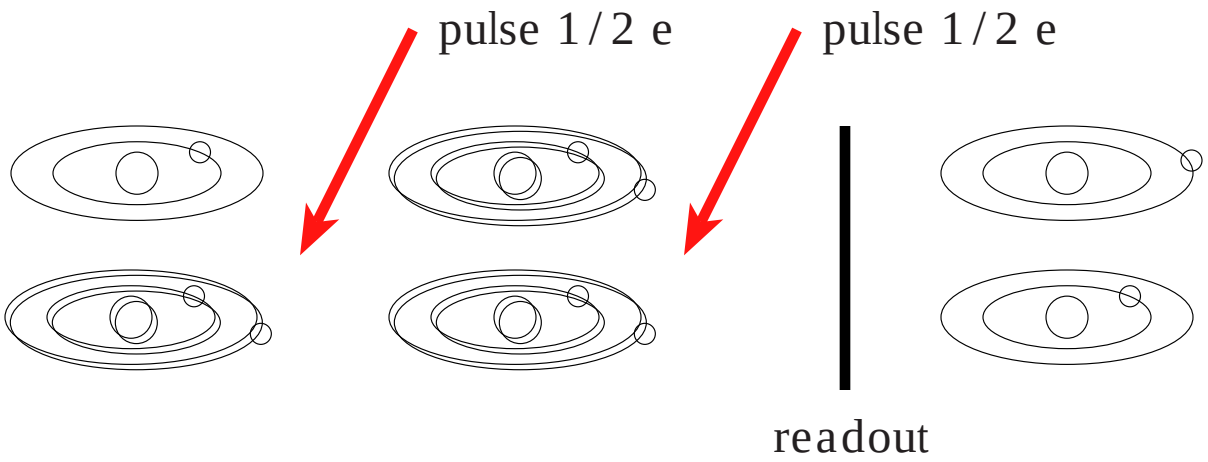
$a_6|101\rangle$

$a_7|110\rangle$

$a_8|111\rangle$

4.4 The CNOT Gate

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



5.0 Applications: Cryptography & Cryptoanalysis

5.1 Factorization

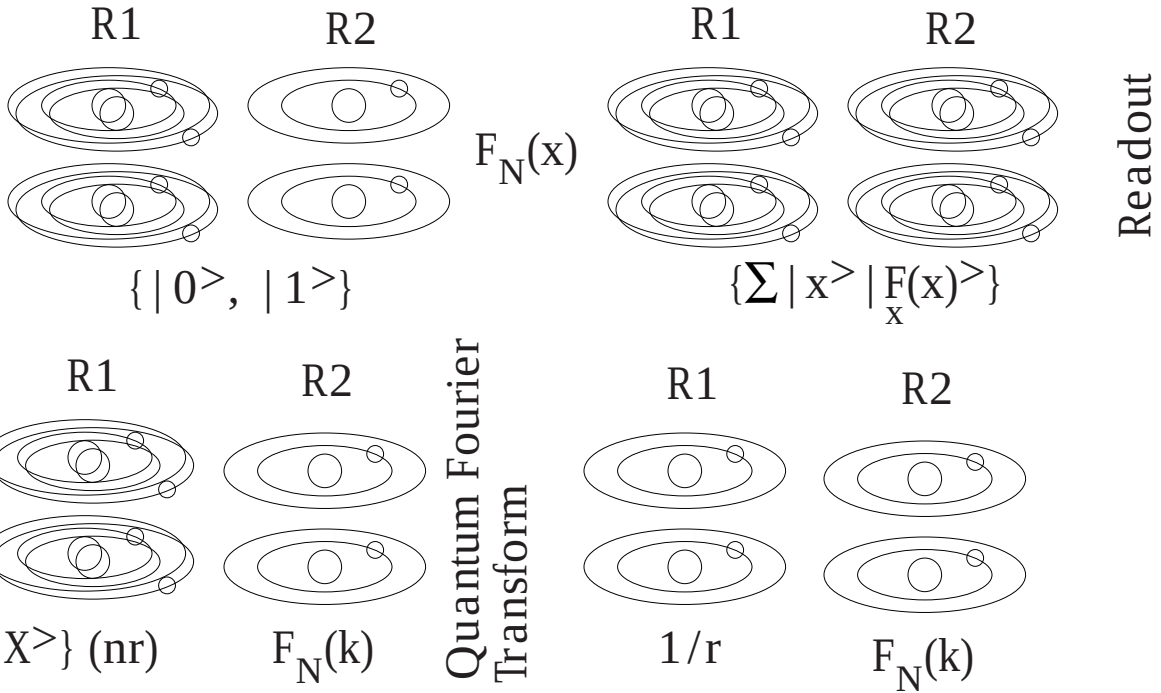
5.2 Sieve Function

5.3 Key Distribution

5.1 Factorization - Shor's Algorithm

$F_N(x) = a^x \bmod N$ - Yields data in period r.

The factors of N are greatest common divisor of N and $a^{r/2} \pm 1$.

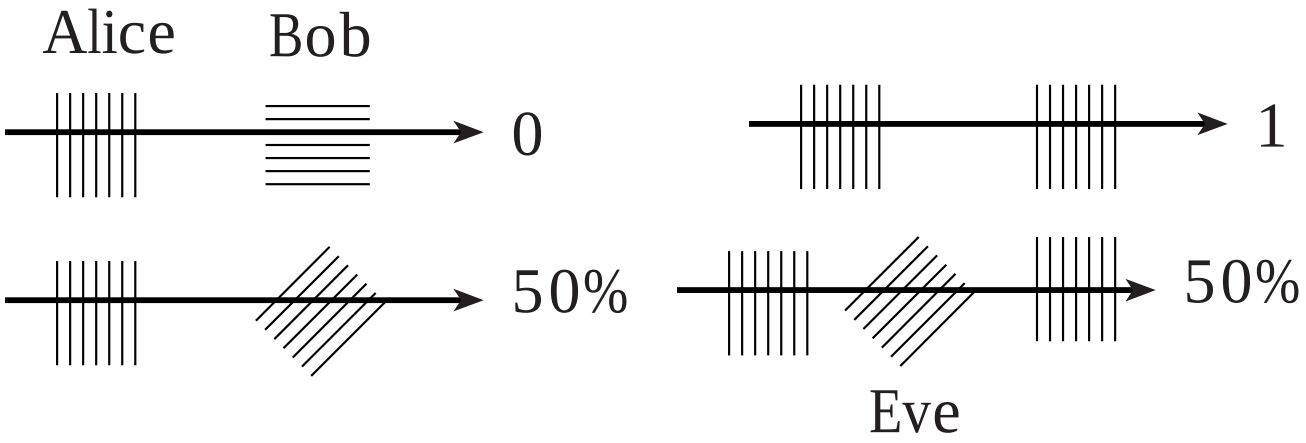


5.1 Sieve Function - Grover's Search Algorithm

Classical Search of N items takes N/2 steps
Quantum search - by applying search tests to all values in the register simultaneously - takes on average $\sqrt{N}/2$ steps.

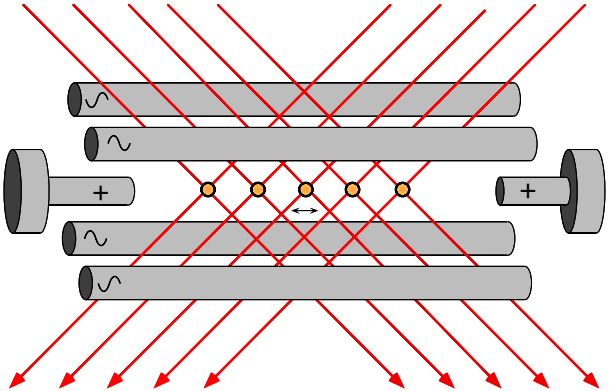
Application is finding, for example DES keys by brute force by searching the key space.
Classical DES crack, 1000 years E6 keys/sec
Grover's algorithm would take 4 minutes

5.3 Quantum Key Distribution



Alice Sends With	+	x	+	+	x	x	+	+	x	x	+	+	x
Alice Sends to Bob	|	/	|	-	/	\	|	-	\	\	-	|	/
Bob measures with	+	x	x	+	+	x	+	x	x	+	x	+	x
Bob's Results:	|	/	/	-	|	\	|	\	\	-	\	|	/
Valid Data	|	/		-		\	|		\			|	/
Translated to Key	1	0		0		1	1		1			1	0

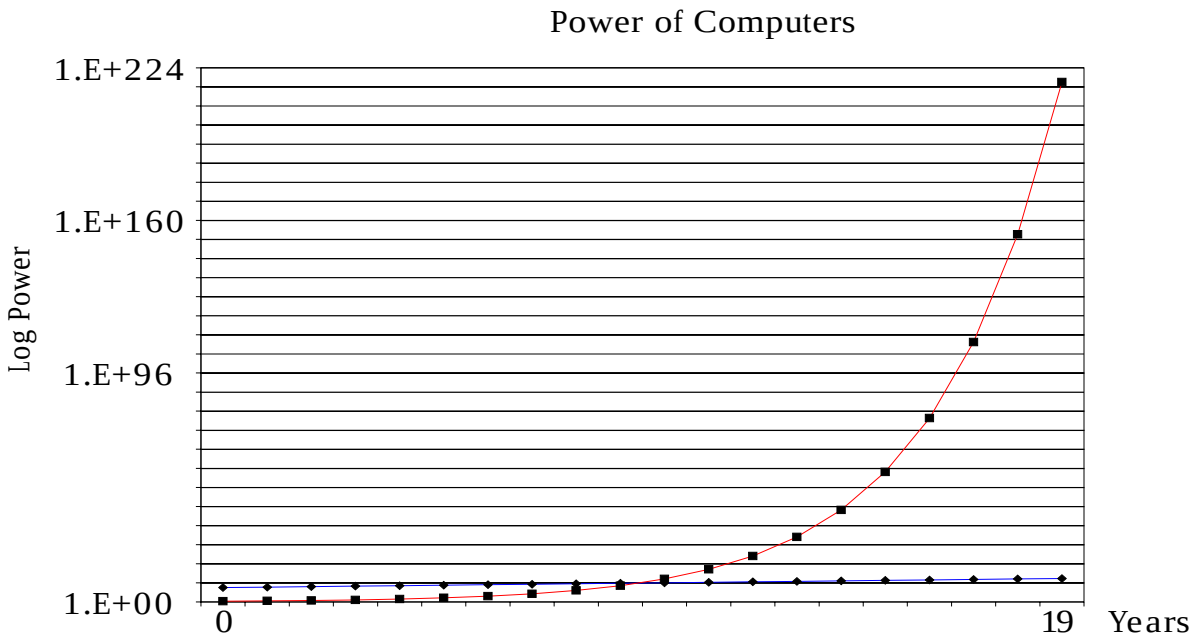
6.0 Practical Implementations



Ion Trap Computer

NMR Computer

7.0 Conclusion



Classical: $P = 2^{(y/1.5)}$ Quantum: $P = 2^{2^{(y/2)}}$