Quantum Cryptography in the Wild

Brief introduction on quantum information and some preliminary consequences for cybersecurity. A simple quantum key distribution algorithm.

Gate42 (http://www.gate42.org/)

We are physicists and programmers trying to gather people who are interested in quantum computing. Very big area: from academic science to engineering (hardware, software). Contemporary computer science + quantum physics.

42 is the "Answer to the Ultimate Question of Life, the Universe, and Everything"

© Deepmind

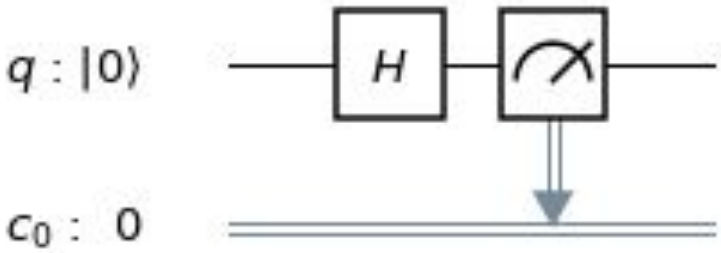
Hype on quantum computing: as for any big idea, there is a lot of hype and misunderstanding. Internet will solve all our problems, DotCom boom. AI will answer all our question. Quantum computer is exponentially fast against classic ones.
Plan: a simple example, review, QKD

Simple Random Number Generator With Photons

Polarizations:

$$|\psi\rangle = \alpha'|\uparrow\rangle + \beta'|\downarrow\rangle \qquad |\psi\rangle = \alpha|\circlearrowleft\rangle + \beta|\circlearrowright\rangle$$

$$|\circlearrowleft\rangle = |\uparrow\rangle - |\downarrow\rangle \qquad |\circlearrowright\rangle = |\uparrow\rangle + |\downarrow\rangle$$



Pseudo random generators => bad statistics, seeding problem.

Classic

Relativistic

GPS

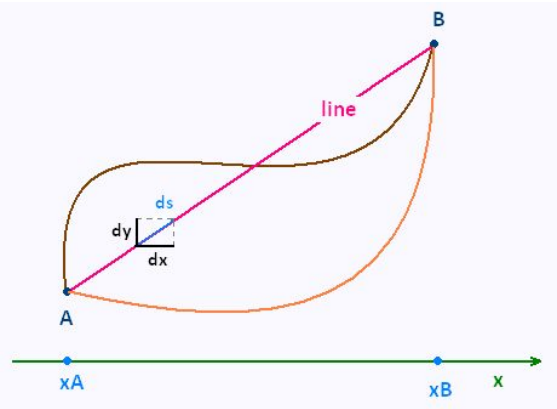
Processors

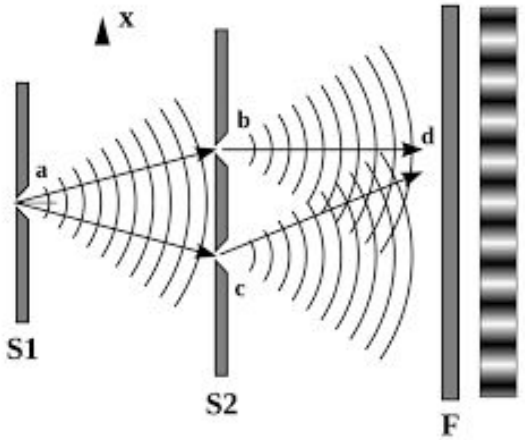
Quantum

Quantum Field Theory

10 nm technologies take into account quantum effects. But they are deemed as negative factor.

Quantum vs Classical, physics point of view





State is point in a manifold, evolution is a line.

Principle of least action.

State is vector in Hilbert space, evolution is a Unitary Transform.

Action - one trajectory, light chooses quickest path. sum of many trajectories, light == many photons and we see this probabilities as waves.
Joining two subsystems: N + M vs NxM.
Probability - we don’t know something. (not exact initial state, external noise, ...). In quantum mechanics Probability is inherent.

Quantum vs Classical, probabilities

Indicator (characteristic) function: $$\chi_A(x) = \begin{Bmatrix} 1 & if & x \in A \\ 0 & if & x \notin A \end{Bmatrix}$$

Orthogonal projectors set: $$\sum \Pi_i = I$$

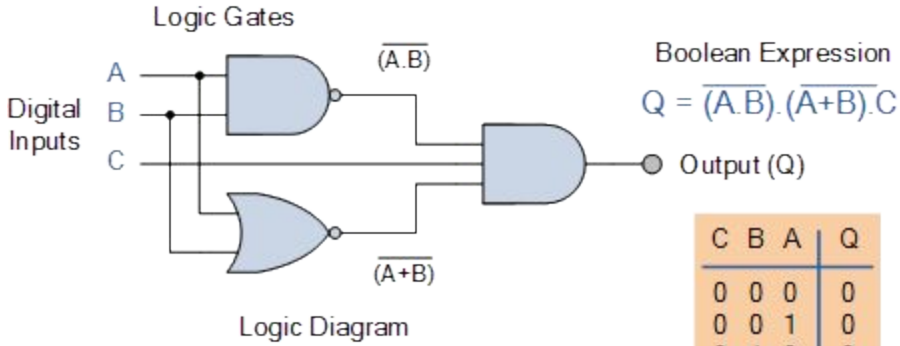
And Probability is calculated as: $$\mathrm{P(i)} = \mathrm{Tr}(\rho \Pi_i)$$

Sample space, σ-algebra, measure on it. events are represented by the lattice of projectors on a Hilbert space. The elementary outcomes are the one-dimensional projectors. C*-algebra.
Questions and answers in quantum depend on how we are asking them. In classic answer is an integral of indicator function.

Quantum vs Classical, discrete systems

Bit - {0,1}

Combinational logic



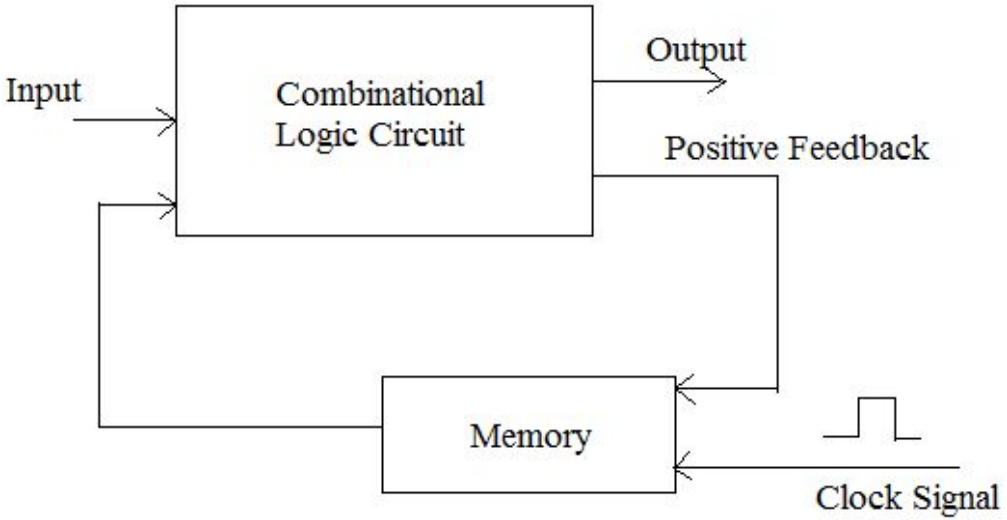
Typical Truth Table

C	B	A	Q
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	0

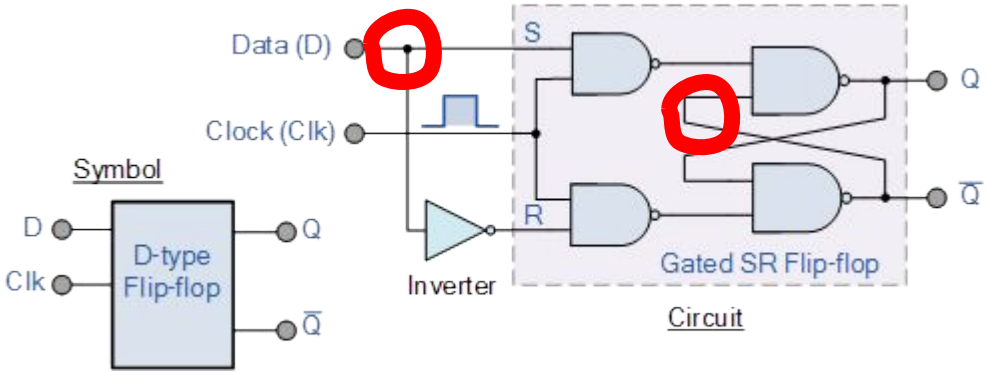
Last 50 years, we learned to describe discrete systems in bits. Combinational logic: boolean function.

Quantum vs Classical, discrete systems

Sequential logic (state Machine)



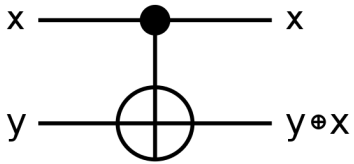
Quantum vs Classical, discrete systems

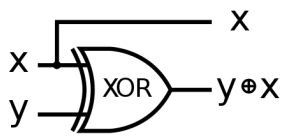


Reversible:Idea before quantum. Quantum gates should be reversible. Not a boolean function, but permutations.

Quantum vs Classical, discrete systems

Reversibles Gates. CNOT



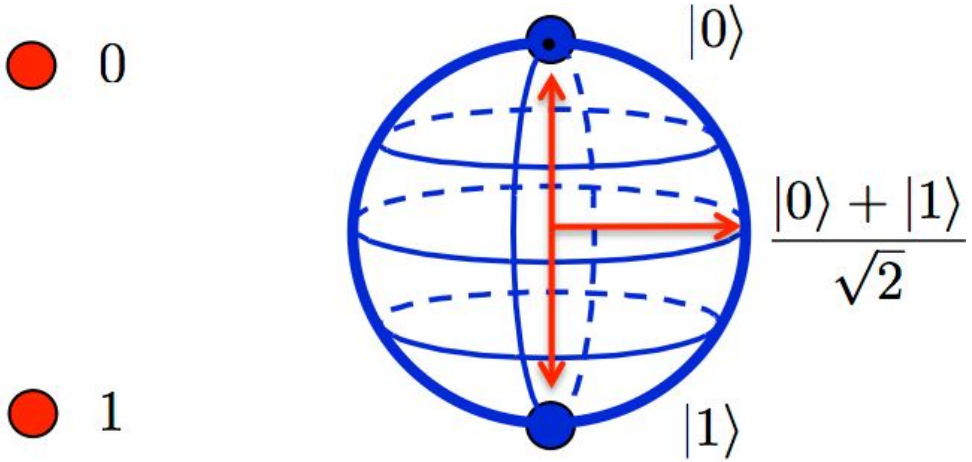


input		output	
x	y	x	y+x
|0⟩	|0⟩	|0⟩	|0⟩
|0⟩	|1⟩	|0⟩	|1⟩
|1⟩	|0⟩	|1⟩	|1⟩
|1⟩	|1⟩	|1⟩	|0⟩

input		output	
x	y	x	y+x
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Quantum vs Classical, discrete systems

Qubit - Any 2-state object. $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$



Classical Bit **Qubit**

Quantum vs Classical, discrete systems

$$|\psi\rangle = \alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle$$

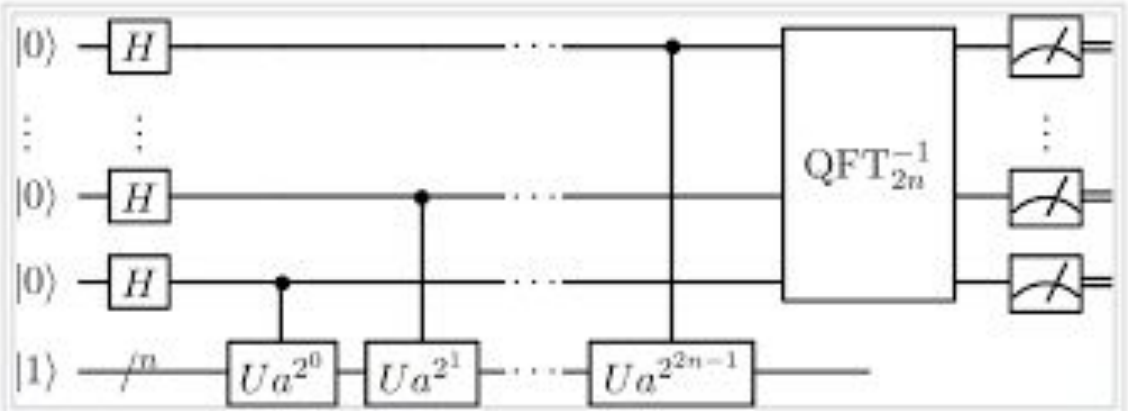
N bits encode one integer.

N qubits encode 2^N complex numbers. (superposition, entanglement)

But after computation we can ask only N questions (measurements)

Emulation QC is exponentially hard (). But no universal exponential speedup - at the end can ask only n questions.
Vulcan - BlueGene/Q: 4,300 TFlop/s, simulated 56 qubit. (2 days ~ possible 0.1 second)

A Quantum Algorithm



Quantum subroutine in Shor's algorithm.

Current Quantum Computers

DWave (quantum annealing), photonic, continuous variable.
IBM - superconducting qubits. (5 - 20 qubits are OnLine)

Qubits are unstable. 0.01~0.001 error rates.

Too much errors == classical behaviour.

Error correction - need of millions of qubits.

Controversy (2^100 ~ thermodynamics, or some other physics)

IBM - kubik rubik in big refrigerator.
Current quantum computing similar what we had for 40's (Z1, Colossus, …) debugging was not a metaphor. Error correction and fidelity. No cloning theorem.

Programming

Languages are like a DSL (setup a qubit, rotate it, mix this, measure it.)

Algorithms usually give a square root speedup (compared to classic).

Integer factorization (Shor) - sub exponential => polynomial.

As driving car with remote control.

Telecommunications & Cryptography

Threats: more computational power.

RSA - factorization of an integer is exponential. Shor’s algorithm for n bit integer needs O(2*n) logical (clean) qubits and O(n*n*n) gates. Groover - effectively divides the size of symmetric key length. Errors

No near term threat!

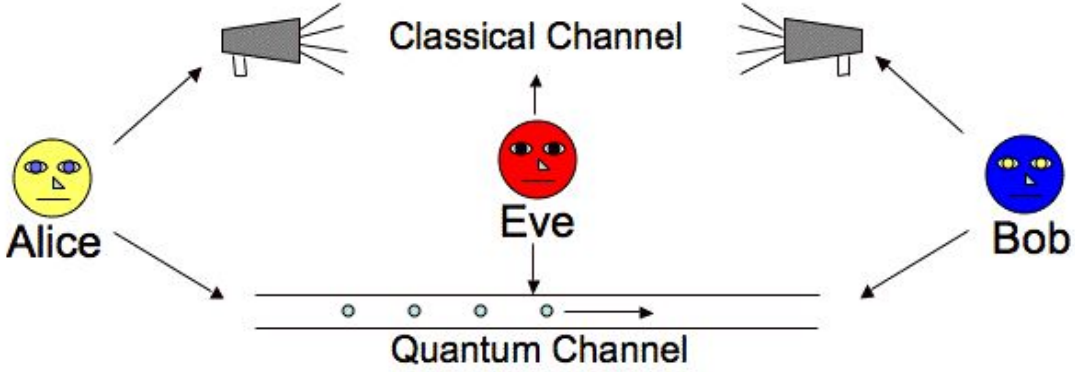
Telecommunications & Cryptography

Ideal random number generator. digital signatures, fingerprinting, authentication.

Exploiting superposition and/or entanglement.

We know how to cope with errors in telecommunications world.

Quantum key distribution: BB84 (main idea)



No cloning theorem: Eve can not intercept a qubit

Alice bits	0	1	0	1	1	1	0	1	1
Alice Base	L	C	C	L	C	L	L	L	C
Q Channel A=>B	|0>	|->	|+>	|1>	|->	|1>	|0>	|1>	|->
Bob	C	L	C	L	L	L	C	C	L
Cl Channel A => B	LCCLCLLLC								
Cl Channel B => A	CLCCLLCCL								
Basis Sifting			C	L		L			
Secret Key			0	1		1			

Classical communications to check if Eve intercepted a qubit.

But the world is not ideal. Can not distinguish Eve from channel errors. Single photon source can give 2 photons, error correction (Information reconciliation) and privacy amplification.

Telecommunications & Cryptography

ECHELON - 2001. First commercial try possibly 2004.

www.idquantique.com (Secret key rate ~3 kb/s) and www.infosecglobal.com VPN !

quantumxc.com announced QKD network in USA

Last scientific report: 1.26 Megabit/s over 50 kilometres (km) of standard optical fibre

in 2016 China launched the $100 million satellite mission named Quantum Experiments at Space Scale (QUESS) aka Micius

Chinese satellite channels: sifted key rates of ~3 kbps at ~1000 km physical separation

Idquantique: network encryption systems, quantum cryptographic systems especially designed for industry and government, a quantum random number generator, a state-of-art photon counting device, single photon source.
There are higher rates, but extremely low temperatures and in extremely well controlled lab conditions.

https://en.wikipedia.org/wiki/List_of_companies_involved_in_quantum_computing_or_communication

Quantum is not a magic bullet.
Hardware attacks. Use of physical setup impurity. (attacking photodiode). No formal proof of security.

Classic probabilistic methods dealing with classical channel.

We all have seen this.