A Practical Introduction to Quantum Computing: From Qubits to Quantum Machine Learning and Beyond

Elías F. Combarro
combarro@gmail.com

CERN openlab (Geneva, Switzerland) - University of Oviedo (Oviedo, Spain)

CERN - November/December 2020

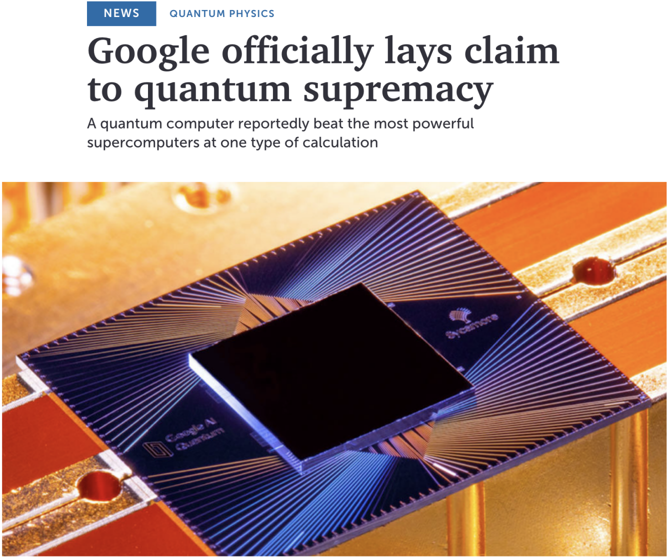
CERN openlab

Universidad de Oviedo

Part I

Introduction: quantum computing... the end of the world as we know it?

I, for one, welcome our new quantum overlords



NEWS QUANTUM PHYSICS

Google officially lays claim to quantum supremacy

A quantum computer reportedly beat the most powerful supercomputers at one type of calculation

Image credits: sciencenews.org

Philosophy of the course

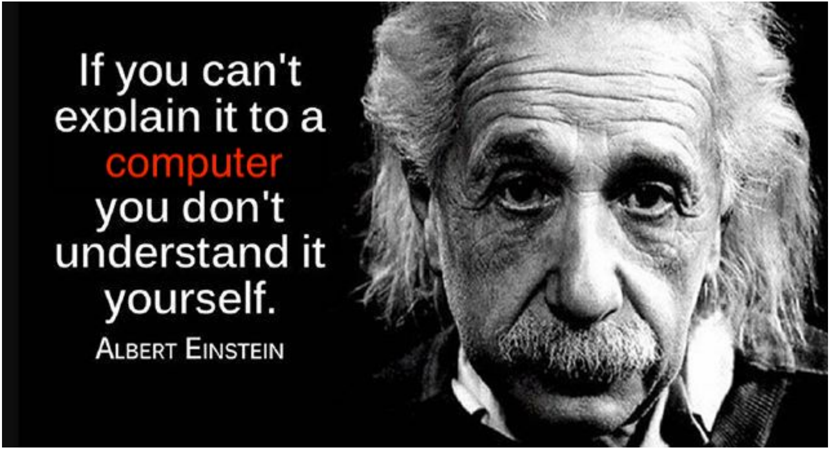


Image credits: Modified from an Instagram image by Bob MacGuffie

Tools and resources

- Jupyter Notebooks
  - Web application to create and execute notebooks that include code, images, text and formulas
  - They can be used locally (Anaconda) or in the cloud (mybinder.org, Google Colab...)
- IBM Quantum Experience
  - Free online access to quantum simulators (up to 32 qubits) and **actual quantum computers** (1, 5 and 15 qubits) with different topologies
  - Programmable with a visual interface and via different languages (python, qasm, Jupyter Notebooks)
  - Launched in May 2016
  - https://quantum-computing.ibm.com/

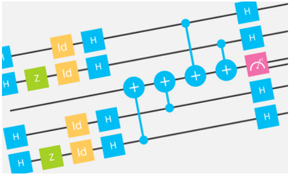


Image credits: IBM

Tools and resources (2)

- Quirk
  - Online simulator (up to 16 qubits)
  - Lots of different gates and visualization options
  - `http://algassert.com/quirk`
- D-Wave Leap
  - Access to D-Wave quantum computers
  - Ocean: python library for quantum annealing
  - Problem specific (QUBO, Ising model...)
  - `https://www.dwavesys.com/take-leap`

The shape of things to come

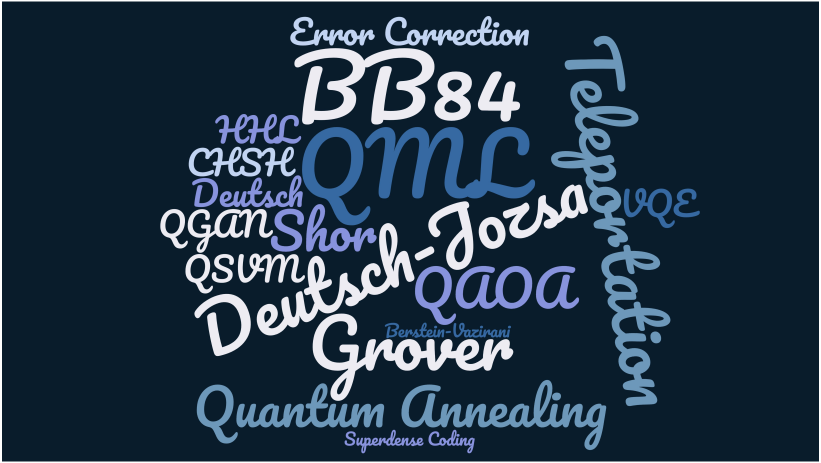


Image credits: Created with wordclouds.com

What is quantum computing?

Quantum computing

Quantum computing is a computing paradigm that exploits quantum mechanical properties (superposition, entanglement, interference...) of matter in order to do calculations

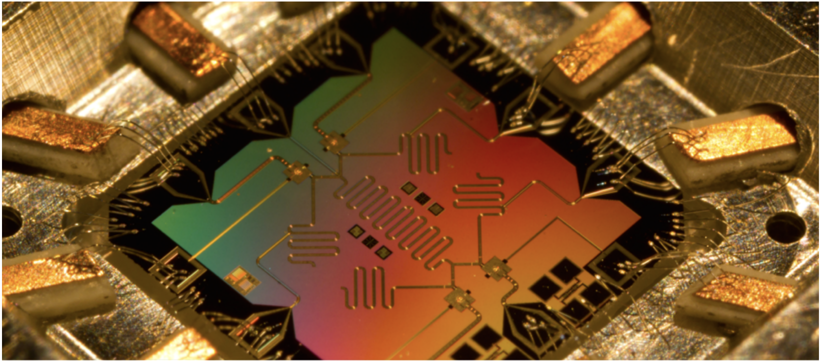


Image credits: Erik Lucero

Models of quantum computing

- There are several models of quantum computing (they're all equivalent)
  - Quantum Turing machines
  - **Quantum circuits**
  - Measurement based quantum computing (MBQC)
  - Adiabatic quantum computing
  - Topological quantum computing
- Regarding their **computational capabilities**, they are equivalent to classical models (Turing machines)

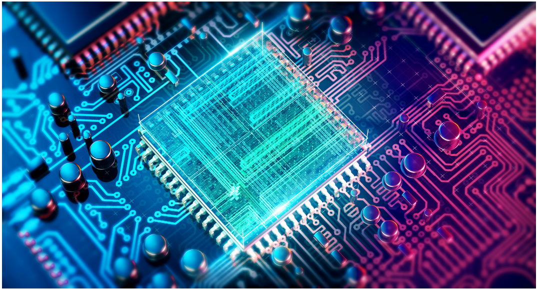


Image credits: Getty Images

Quantum and classical computational complexity

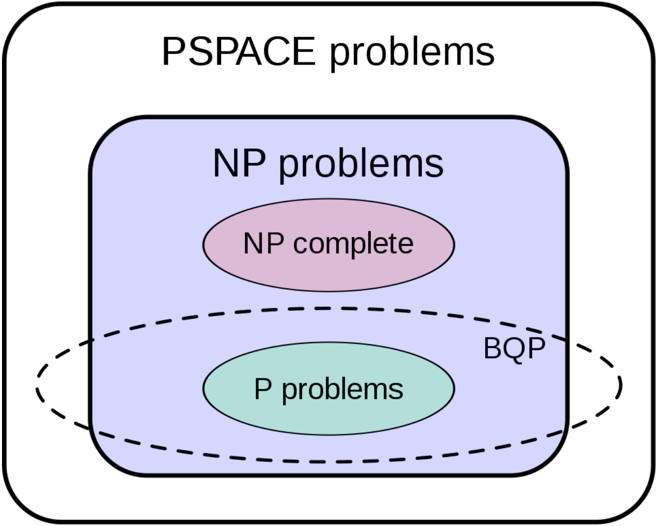
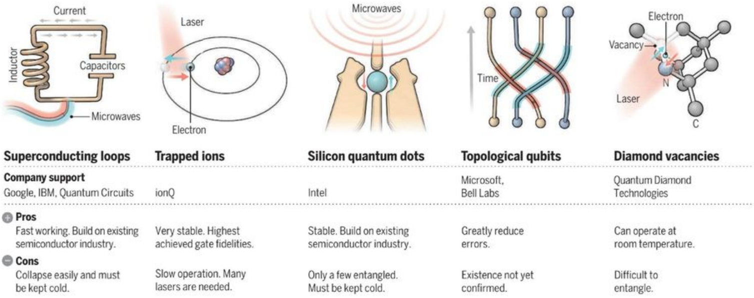


Image credits: wikipedia.org

What technologies are used to build quantum computers?



	Superconducting loops	Trapped ions	Silicon quantum dots	Topological qubits	Diamond vacancies
Company support	Google, IBM, Quantum Circuits	ionQ	Intel	Microsoft, Bell Labs	Quantum Diamond Technologies
⊕ **Pros**	Fast working. Build on existing semiconductor industry.	Very stable. Highest achieved gate fidelities.	Stable. Build on existing semiconductor industry.	Greatly reduce errors.	Can operate at room temperature.
⊖ **Cons**	Collapse easily and must be kept cold.	Slow operation. Many lasers are needed.	Only a few entangled. Must be kept cold.	Existence not yet confirmed.	Difficult to entangle.

Image credits: Graphic by C. Bickle/Science data by Gabriel Popkin

What is a quantum computer like?

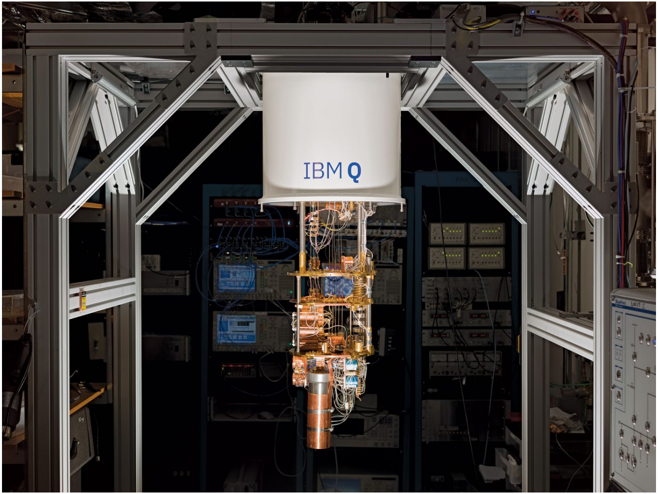
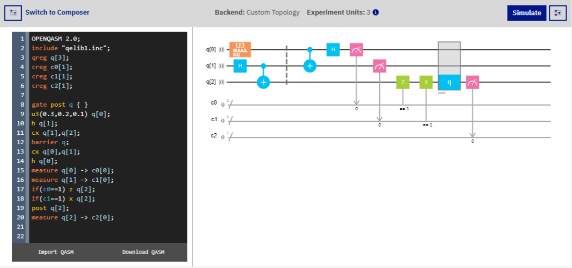


Image credits: IBM

The Sounds of IBM: IBM Q

Programming a quantum computer

- Different frameworks and programming languages:
  - qasm
  - Qiskit (IBM)
  - Cirq (Google)
  - Forest/pyqil (Rigetti)
  - Q# (Microsoft)
  - Ocean (D-Wave)
  - ...
- Most of them for quantum circuit specification



```
OPENQASM 2.0;
include "qelib1.inc";
qreg q[3];
creg c0[1];
creg c1[1];
creg c2[1];

gate post q { }
u3(0.3,0.2,0.1) q[0];
h q[1];
cx q[1],q[2];
barrier q;
cx q[0],q[1];
h q[0];
measure q[0] -> c0[0];
measure q[1] -> c1[0];
if(c0==1) z q[2];
if(c1==1) x q[2];
post q[2];
measure q[2] -> c2[0];


```

Image credits: IBM

What are the elements of a quantum circuit?

- Every computation has three elements: data, operations and results
- In quantum circuits:
  - Data = **qubits**
  - Operations = **quantum gates** (unitary transformations)
  - Results = **measurements**

Image credits: Adobe Stock

Part II

One-qubit systems: one qubit to rule them all

What is a qubit?

- A classical bit can take two different values (0 or 1). It is discrete.
- A qubit can “take” **infinitely** many different values. It is continuous.
- Qubits live in a **Hilbert vector space** with a basis of two elements that we denote $|0\rangle$ y $|1\rangle$.
- A generic qubit is in a **superposition**

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

where α and β are **complex numbers** such that

$$|\alpha|^2 + |\beta|^2 = 1$$

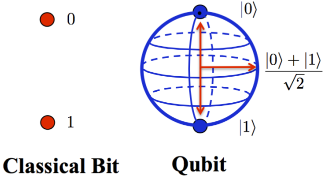


Image credits: https://prateekvjoshi.com/

Measuring a qubit

- The way to know the value of a qubit is to perform a measurement. However
  - The result of the measurement is random
  - When we measure, we only obtain one (classical) bit of information
- If we measure the state $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ we get 0 with probability $|\alpha|^2$ and 1 with probability $|\beta|^2$.
- Moreover, the new state after the measurement will be $|0\rangle$ or $|1\rangle$ depending of the result we have obtained (wavefunction colapse)
- We cannot perform several independent measurements of $|\psi\rangle$ because we cannot copy the state (**no-cloning theorem**)

HOW'S YOUR QUANTUM COMPUTER PROTOTYPE COMING ALONG?
GREAT!
Dilbert.com DilbertCartoonist@gmail.com
THE PROJECT EXISTS IN A SIMULTANEOUS STATE OF BEING BOTH TOTALLY SUCCESSFUL AND NOT EVEN STARTED.
4-17-12 ©2012 Scott Adams, Inc./Dist. by Universal Uclick
CAN I OBSERVE IT?
THAT'S A TRICKY QUESTION.

What are quantum gates?

- Quantum mechanics tells us that the evolution of an isolated state is given by the Schrödinger equation

$$H(t)|\psi(t)\rangle = i\hbar\frac{\partial}{\partial t}|\psi(t)\rangle$$

- In the case of quantum circuits, this implies that the operations that can be carried out are given by unitary matrices. That is, matrices U of complex numbers verifying

$$UU^\dagger = U^\dagger U = I$$

  where $U^\dagger$ is the conjugate transpose of U.
- Each such matrix is a possible quantum gate in a quantum circuit

Reversible computation

- As a consequence, all the operations have an inverse: **reversible computing**
- Every gate has the same number of inputs and outputs
- We cannot directly implement some classical gates such as *or*, *and*, *nand*, *xor*...
- But we can simulate any classical computation with small overhead
- Theoretically, we could compute without wasting energy (Landauer's principle, 1961)

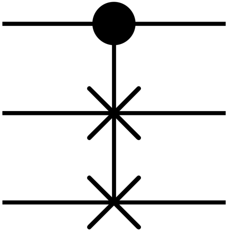


Image credits: wikipedia.org

One-qubit gates

- When we have just one qubit $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, we usually represent it as a column vector $\begin{pmatrix}\alpha \\ \beta\end{pmatrix}$
- Then, a one-qubit gate can be identified with a matrix $U = \begin{pmatrix}a & b \\ c & d\end{pmatrix}$ that satisfies

$$\begin{pmatrix}a & b \\ c & d\end{pmatrix}\begin{pmatrix}\overline{a} & \overline{c} \\ \overline{b} & \overline{d}\end{pmatrix} = \begin{pmatrix}1 & 0 \\ 0 & 1\end{pmatrix}$$

where $\overline{a}, \overline{b}, \overline{c}, \overline{d}$ are the conjugates of complex numbers a, b, c, d.

Action of a one-qubit gate

- A state $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ is transformed into

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} a\alpha + b\beta \\ c\alpha + d\beta \end{pmatrix}$$

  that is, into the state $|\psi\rangle = (a\alpha + b\beta) |0\rangle + (c\alpha + d\beta) |1\rangle$
- Since U is unitary, it holds that

$$|(a\alpha + b\beta)|^2 + |(c\alpha + d\beta)|^2 = 1$$

The *X* or *NOT* gate

- The *X* gate is defined by the (unitary) matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

- Its action (in quantum circuit notation) is

$$|0\rangle \;\; -\!\boxed{X}\!- \;\; |1\rangle$$

$$|1\rangle \;\; -\!\boxed{X}\!- \;\; |0\rangle$$

that is, it acts like the classical *NOT* gate

- On a general qubit its action is

$$\alpha\,|0\rangle + \beta\,|1\rangle \;\; -\!\boxed{X}\!- \;\; \beta\,|0\rangle + \alpha\,|1\rangle$$

The Z gate

- The Z gate is defined by the (unitary) matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- Its action is

$$|0\rangle \quad -\!\!\boxed{Z}\!\!- \quad |0\rangle$$

$$|1\rangle \quad -\!\!\boxed{Z}\!\!- \quad -|1\rangle$$

The *H* or Hadamard gate

- The *H* or Hadamard gate is defined by the (unitary) matrix

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$$

- Its action is

$$|0\rangle \;-\!\boxed{H}\!-\; \frac{|0\rangle+|1\rangle}{\sqrt{2}}$$

$$|1\rangle \;-\!\boxed{H}\!-\; \frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

- We usually denote

$$|+\rangle := \frac{|0\rangle+|1\rangle}{\sqrt{2}}$$

and

$$|-\rangle := \frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

Other important gates

- Y gate

$$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

- S gate

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{pmatrix}$$

- T gate

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$$

- The gates X, Y and Z are also called, together with the identity, the Pauli gates. An alternative notation is σ_X, σ_Y, σ_Z.

The Bloch sphere

- A common way of representing the state of a qubit is by means of a point in the surface of the Bloch sphere
- If $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ with $|\alpha|^2 + |\beta|^2 = 1$ we can find angles γ, δ, θ such that
$$\alpha = e^{i\gamma}\cos\frac{\theta}{2}$$
$$\beta = e^{i\delta}\sin\frac{\theta}{2}$$
- Since an overall phase is physically irrelevant, we can rewrite
$$|\psi\rangle = \cos\frac{\theta}{2}\,|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}\,|1\rangle$$
with $0 \le \theta \le \pi$ and $0 \le \varphi < 2\pi$.

The Bloch sphere (2)

- From $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$ we can obtain spherical coordinates for a point in $\mathbb{R}^3$

$$(\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta)$$

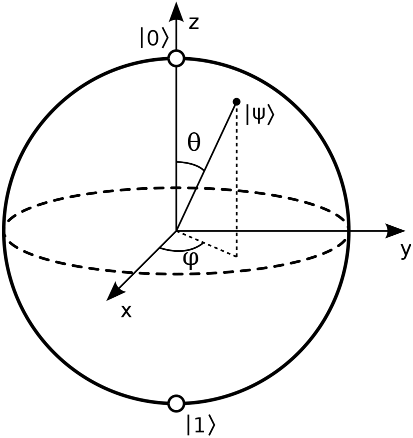


Image credits: wikipedia.org

Rotation gates

- We can define the following rotation gates

$$R_X(\theta) = e^{-i\frac{\theta}{2}X} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}X = \begin{pmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$$

$$R_Y(\theta) = e^{-i\frac{\theta}{2}Y} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Y = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$$

$$R_Z(\theta) = e^{-i\frac{\theta}{2}Z} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Z = \begin{pmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

- Notice that $R_X(\pi) \equiv X$, $R_Y(\pi) \equiv Y$, $R_Z(\pi) \equiv Z$, $R_Z(\frac{\pi}{2}) \equiv S$, $R_Z(\frac{\pi}{4}) \equiv T$

Using rotation gates to generate one-qubit gates

- For any one-qubit gate U there exist a unit vector $r = (r_x, r_y, r_z)$ and an angle θ such that

$$U \equiv e^{-i\frac{\theta}{2}r\cdot\sigma} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}(r_xX + r_yY + r_zZ)$$

- For instance, choosing $\theta = \pi$ and $r = (\frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}})$ we can see that

$$H \equiv e^{-i\frac{\theta}{2}r\cdot\sigma} = -i\frac{1}{\sqrt{2}}(X + Z)$$

- Additionally, it can also be proved that there exist angles α, β and γ such that

$$U \equiv R_Z(\alpha)R_Y(\beta)R_Z(\gamma)$$

Inner product, Dirac's notation and Bloch sphere

- The inner product of two states $|\psi_1\rangle = \alpha_1 |0\rangle + \beta_1 |1\rangle$ and $|\psi_2\rangle = \alpha_2 |0\rangle + \beta_2 |1\rangle$ is given by

$$\langle\psi_1|\psi_2\rangle = \left(\overline{\alpha_1}\;\overline{\beta_1}\right)\begin{pmatrix}\alpha_2\\ \beta_2\end{pmatrix} = \overline{\alpha_1}\alpha_2 + \overline{\beta_1}\beta_2$$

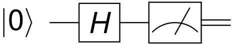
- Notice that $\langle 0|0\rangle = \langle 1|1\rangle = 1$ and $\langle 0|1\rangle = \langle 1|0\rangle = 0$
- This allows us to compute

$$\begin{aligned}\langle\psi_1|\psi_2\rangle &= \left(\overline{\alpha_1}\langle 0| + \overline{\beta_1}\langle 1|\right)\left(\alpha_2|0\rangle + \beta_2|1\rangle\right)\\ &= \overline{\alpha_1}\alpha_2\langle 0|0\rangle + \overline{\alpha_1}\beta_2\langle 0|1\rangle + \overline{\beta_1}\alpha_2\langle 1|0\rangle + \overline{\beta_1}\beta_2\langle 1|1\rangle\\ &= \overline{\alpha_1}\alpha_2 + \overline{\beta_1}\beta_2\end{aligned}$$

- Orthogonal states are antipodal on the Bloch sphere

Hello, quantum world!

- Our very first quantum circuit!



- After applying the H gate the qubit state is

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

- When we measure, we obtain 0 or 1, each with 50% probability: we have a circuit that generates perfectly uniform random bits!

Part III

The BB84 protocol: Alice and Bob's hotline

One-time pad: a Catch-22 situation

- Alice wants to send Bob a message m without Eve being able to learn anything about its content
- This can be achieved if Alice and Bob share in advance a string k of random bits:
  - Alice computes $x = m \oplus k$ and sends x to Bob
  - Eve cannot learn anything from x $(Pr(M = m|X = x) = Pr(M = m))$
  - But Bob can recover m by computing $x \oplus k$
- The main problem is that k has to be as long as m and cannot be reused so... how to agree on k?

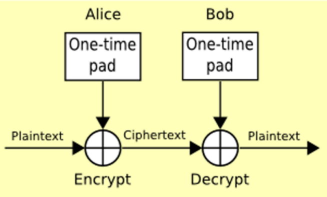
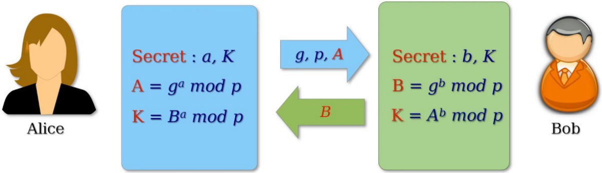


Image credits: nullprogram.com

The problem of key distribution

- Alice and Bob may share several keys for later use when they are together
- But... what if they cannot meet each other?
- There exist key distribution methods like the Diffie-Hellman protocol but...
  - They are not unconditionally secure (they usually rely on hardness assumptions)
  - In fact, DH can be broken with quantum computers!

Diffie – Hellman Key Exchange Protocol



The Security Buddy
https://www.thesecuritybuddy.com/

BB84: Alice's part

- In 1984, Charles Bennett and Gilles Brassard proposed the first protocol for quantum key distribution (QKD)
- Alice generates a (private) string of random bits
- She could even do this with a quantum computer (H gate + measure)
- Then, for each bit she randomly chooses if she encodes it in the $\{|0\rangle, |1\rangle\}$ basis or in the $\{|+\rangle, |-\rangle\}$ basis (remember that $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$)
- She can easily do this by using H and X gates (recall that $H|0\rangle = |+\rangle, H|1\rangle = |-\rangle, X|0\rangle = |1\rangle, X|1\rangle = |0\rangle$)
- Alice sends the resulting qubits to Bob (through a quantum but not necessarily secure channel)

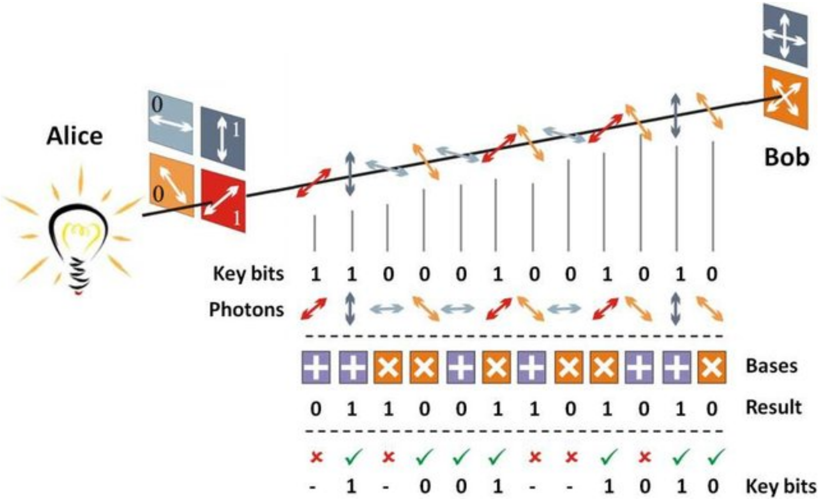
BB84: Bob's part

- Each time Bob receives a qubit, he randomly decides whether he will measure it in the $\{|0\rangle, |1\rangle\}$ basis or in the $\{|+\rangle, |-\rangle\}$ basis
- He does this by applying (or not) the H gate before measuring
- He writes down the results and the basis he used:
  - If he used $\{|0\rangle, |1\rangle\}$ he writes down 0 if he gets $|0\rangle$ and 1 if he gets $|1\rangle$
  - If he used $\{|+\rangle, |-\rangle\}$ he writes down 0 if he gets $|+\rangle$ and 1 if he gets $|-\rangle$

BB84: Alice and Bob on the phone

- After this process, Alice and Bob talk on a classical channel (authenticated but not necessarily secure)
- Bob announces the bases he has used for the measurements and Alice announces the bases she used to code the bits
- Bob does NOT announce the results of his measurements
- For those bits in which Bob measured with the same basis that Alice used for coding, he has got the bit that Alice intended to send
- The rest are discarded (they will keep about half of the bits)

BB84: The protocol in an image



Key bits	1	1	0	0	0	1	0	0	1	0	1	0
Photons	⤢	↕	↔	⤡	↔	⤢	⤡	↔	⤢	⤡	↕	⤡
Bases	+	+	×	×	+	×	+	×	×	+	+	×
Result	0	1	1	0	0	1	1	0	1	0	1	0
	✗	✓	✗	✓	✓	✓	✗	✗	✓	✗	✓	✓
Key bits	-	1	-	0	0	1	-	-	1	0	1	0

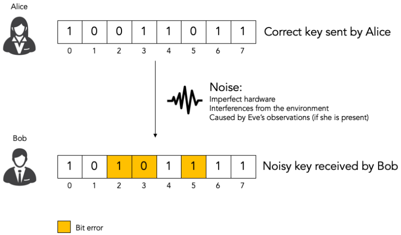
Image credits: A. Carrasco-Casado, V. Fernández, N. Denisenko

Eve tries to intercept and resend...

- Imagine Eve has access to the qubits that Alice sends to Bob
- Eve could try to measure and resend the qubit to Bob
- It is imposible for Eve to distinguish the four possibilities $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ because she does not know the basis that Alice has chosen
- If Eve chooses a basis at random, she will make an error half of the time and Alice and Bob may detect it (by sharing some of the bits of the key to check that they are equal)
- Eve cannot copy the qubits and wait to check the basis that Alice and Bob have used (no cloning theorem)
- Other more complex attacks are possible, but can be shown to fail

Information reconciliation and privacy amplification

- Because of imperfections in the channel and devices or because of eavesdropping, some of the bits that Alice and Bob have may be different
- They can conduct a process of information reconciliation (for instance, with the cascade protocol)
- After this phase (or even before), some information may have leaked to Eve
- Alice and Bob can perform privacy amplification (for instance, with randomness extractors)



Alice
1 0 0 1 1 0 1 1
0 1 2 3 4 5 6 7
Correct key sent by Alice
Noise:
Imperfect hardware
Interferences from the environment
Caused by Eve's observations (if she is present)
Bob
1 0 1 0 1 1 1 1
0 1 2 3 4 5 6 7
Noisy key received by Bob
Bit error

Image credits: hikingandcoding.wordpress.com

QKD at CERN

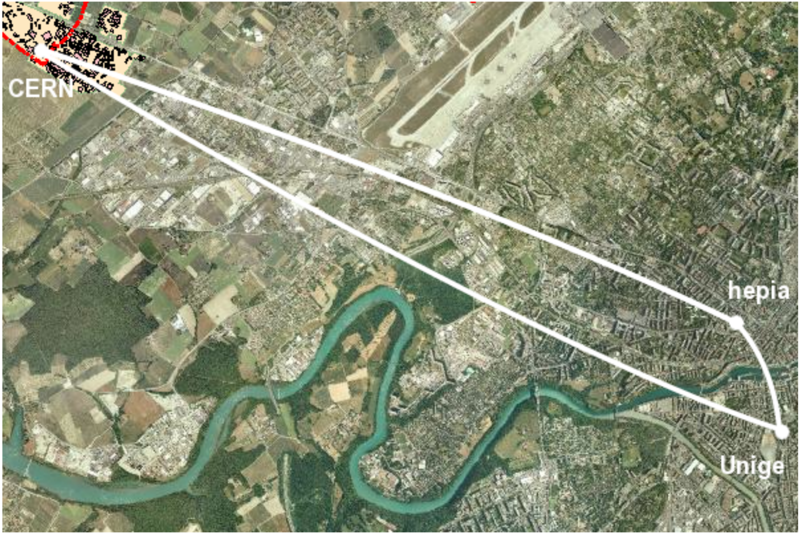


Image credits: https://arxiv.org/pdf/1203.4940.pdf

Kak's three-stage protocol

- Proposed by Kak in 2006
- It needs an authenticated quantum channel
- Suppose Alice wants to send $|x\rangle \in \{|0\rangle, |1\rangle\}$ to Bob:
  - Alice chooses θ_A at random and sends $R_Y(\theta_A)|x\rangle$ to Bob
  - Bob choose θ_B at random and sends $R_Y(\theta_B)R_Y(\theta_A)|x\rangle$ back to Alice
  - Alice applies $R_Y(-\theta_A)$ and sends

    $$R_Y(-\theta_A)R_Y(\theta_B)R_Y(\theta_A)|x\rangle = R_Y(\theta_B)|x\rangle$$

    to Bob
- Bob can now recover $|x\rangle$ by applying $R_Y(-\theta_B)$

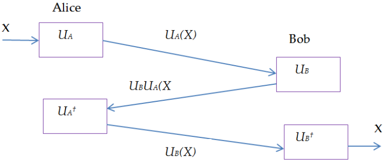


Image credits: wikipedia.org

The quantum one-time pad

- The analagous of the one-time pad with quantum operations would be to choose $a \in \{0, 1\}$ at random and encode $|x\rangle \in \{|0\rangle, |1\rangle\}$ as

$$X^a |x\rangle = |x \oplus a\rangle$$

- This cannot be extended to general qubits $|\psi\rangle$ because $X|+\rangle = |+\rangle$ and $X|-\rangle \equiv |-\rangle$
- We need to choose two bits a and b at random and encode $|\psi\rangle$ as

$$Z^b X^a |\psi\rangle$$

- Bob can now recover $|\psi\rangle$ by applying $X^a Z^b$
- It can be proved that this is unconditionally secure
- The QOTP is the basis of some blind quantum computing protocols

Other protocols that use independent qubits

- The use of independent qubits does not fully exploit the possibilities of quantum information, but there are some additional interesting applications
- For instance:
    - Other QKD protocols: B92, SARG04, Six-state protocol...
    - The concept of quantum money (Wiesner)
    - The Elitzur-Vaidman bomb tester
    - Quantum position verification
    - One-qubit classifier

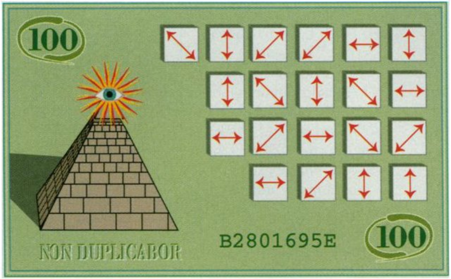


Image credits: The American Association for the Advancement of Science

Part IV

Two-qubit systems: more than the sum of their parts

Working with two qubits

- Each of the qubits can be in state $|0\rangle$ or in state $|1\rangle$
- So for two qubits we have four possibilities:

  $$|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle$$

  that we also denote

  $$|0\rangle|0\rangle, |0\rangle|1\rangle, |1\rangle|0\rangle, |1\rangle|1\rangle$$

  or

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

- Of course, we can have superpositions so a generic state is

  $$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

  where α_{xy} are complex numbers such that

  $$\sum_{x,y=0}^{1} |\alpha_{xy}|^2 = 1$$

Measuring a two-qubit system

- Suppose we have a state

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

- If we measure both qubits, we will obtain:
  - 00 with probability $|\alpha_{00}|^2$ and the new state will be $|00\rangle$
  - 01 with probability $|\alpha_{01}|^2$ and the new state will be $|01\rangle$
  - 10 with probability $|\alpha_{10}|^2$ and the new state will be $|10\rangle$
  - 11 with probability $|\alpha_{11}|^2$ and the new state will be $|11\rangle$
- It is an analogous situation to what we had with one qubit, but now with four possibilities

Measuring just one qubit in a two-qubit system

- If we have a state

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

  we can also measure just one qubit
- If we measure the first qubit (for the second one is analogous):
  - We will get 0 with probability $|\alpha_{00}|^2 + |\alpha_{01}|^2$
  - In that case, the new state of $|\psi\rangle$ will be

$$\frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$$

  - We will get 1 with probability $|\alpha_{10}|^2 + |\alpha_{11}|^2$
  - In that case, the new state of $|\psi\rangle$ will be

$$\frac{\alpha_{10}|10\rangle + \alpha_{11}|11\rangle}{\sqrt{|\alpha_{10}|^2 + |\alpha_{11}|^2}}$$

Two-qubit states and vector representation

- A general two-qubit quantum state is

$$|\psi\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle$$

- We can represent with the column vector

$$\begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix}$$

- We can compute inner products by noticing that

$$\langle 00|00\rangle = \langle 01|01\rangle = \langle 10|10\rangle = \langle 11|11\rangle = 1$$

$$\langle 00|01\rangle = \langle 00|10\rangle = \langle 00|11\rangle = \cdots = \langle 11|00\rangle = 0$$

- A two-qubit quantum gate is a unitary matrix U of size 4×4

Tensor product of one-qubit gates

- The simplest way of obtaining a two-qubit gate is by having a pair of one-qubit gates A and B acting on each of the qubits
- In this case, the matrix for the two-qubit gate is the tensor product $A \otimes B$
- It holds that

$$(A \otimes B)(|\psi_1\rangle \otimes |\psi_2\rangle) = (A\,|\psi_1\rangle) \otimes (B\,|\psi_2\rangle)$$

- Of course, either A or B may be the identity
- This does NOT exhaust all posible two-qubit gates

$$\begin{bmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{bmatrix} \otimes \begin{bmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{bmatrix} = \begin{bmatrix} a_{1,1} \begin{bmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{bmatrix} & a_{1,2} \begin{bmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{bmatrix} \\ a_{2,1} \begin{bmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{bmatrix} & a_{2,2} \begin{bmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{bmatrix} \end{bmatrix} = \begin{bmatrix} a_{1,1}b_{1,1} & a_{1,1}b_{1,2} & a_{1,2}b_{1,1} & a_{1,2}b_{1,2} \\ a_{1,1}b_{2,1} & a_{1,1}b_{2,2} & a_{1,2}b_{2,1} & a_{1,2}b_{2,2} \\ a_{2,1}b_{1,1} & a_{2,1}b_{1,2} & a_{2,2}b_{1,1} & a_{2,2}b_{1,2} \\ a_{2,1}b_{2,1} & a_{2,1}b_{2,2} & a_{2,2}b_{2,1} & a_{2,2}b_{2,2} \end{bmatrix}$$

Image credits: wikipedia.org

The *CNOT* gate

- The *CNOT* (or controlled-*NOT* or *cX*) gate is given by the (unitary) matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

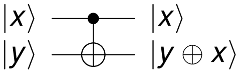
- If the first qubit is $|0\rangle$, nothing changes. If it is $|1\rangle$, we flip the second bit (and the first stays the same)
- That is:

$$|00\rangle \to |00\rangle \qquad |01\rangle \to |01\rangle$$

$$|10\rangle \to |11\rangle \qquad |11\rangle \to |10\rangle$$

Action of the *CNOT* gate

- Its action on $x, y \in \{0, 1\}$ is, then:



- This is an extremely important gate for it allows to:
  - Create entanglement (more on this soon)
  - Copy *classical* information, because:

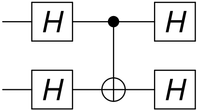
$$|00\rangle \rightarrow |00\rangle$$

$$|10\rangle \rightarrow |11\rangle$$

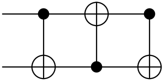
  - Construct other controlled gates

Equivalences with CNOT gates

- Sometimes, CNOT gates are not implemented between all pairs of qubits in a quantum computer
- We can use H gates to change the control and target of a CNOT gate



- We can swap states using three CNOT gates

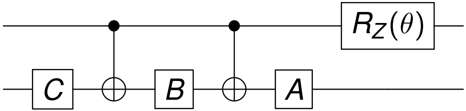


Constructing controlled gates by using the *CNOT* gate

- Any one-qubit gate U can be decomposed in the form

$$e^{i\theta} AXBXC$$

  with $ABC = I$
- Then, the circuit



  implements a U gate on the lower qubit controlled by the upper qubit

The no-cloning theorem

- There is **no** quantum gate that makes copies of an arbitrary (unknown) qubit
- The proof is easy: suppose we have a gate U such that $U\,|\psi\rangle\,|0\rangle = |\psi\rangle\,|\psi\rangle$
- Then $U\,|00\rangle = |00\rangle$ and $U\,|10\rangle = |11\rangle$ and by linearity

$$U(\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)) = \frac{1}{\sqrt{2}}(U\,|00\rangle + U\,|10\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

- But

$$\frac{|00\rangle + |10\rangle}{\sqrt{2}} = (\frac{|0\rangle + |1\rangle}{\sqrt{2}})\,|0\rangle$$

so we should have

$$U(\frac{|00\rangle + |10\rangle}{\sqrt{2}}) = \frac{(|0\rangle + |1\rangle)}{\sqrt{2}}\frac{(|0\rangle + |1\rangle)}{\sqrt{2}} \neq \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Quantum entanglement: the spooky action at a distance

- We say that a state $|\psi\rangle$ is a product state if it can be written in the form

$$|\psi\rangle = |\psi_1\rangle\,|\psi_2\rangle$$

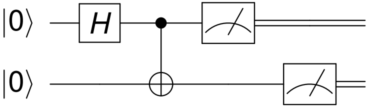
  where $|\psi_1\rangle$ and $|\psi_2\rangle$ are two states (of at least one qubit)
- An **entangled** state is a state that is not a product state
- Example of entangled states (Bell states):

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} \qquad \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

$$\frac{|01\rangle + |10\rangle}{\sqrt{2}} \qquad \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

Hello, entangled world!

- We can construct (and measure) Bell states with simple circuits



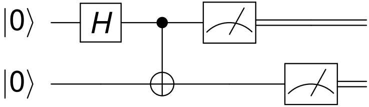
- Initially, the state of the system is $|00\rangle$
- After we apply the *H* gate, the state is

$$\frac{|00\rangle + |10\rangle}{\sqrt{2}}$$

- When we apply the *CNOT* gate, the state changes to

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Hello, entangled world!



- Before we measure the first qubit, we have the state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$
- We will get 0 or 1, each with probability $\frac{1}{2}$
- Suppose we obtain 0. Then, the new state will be $|00\rangle$
- Then, when we measure the second qubit we will obtain 0 with probability 1!
- Also, if we obtain 1 in the first qubit, in the second we will also obtain 1!

Part V

The CHSH game: Nature isn’t classical, dammit

The CHSH game

- Based in an inequality proposed in 1969 by Clauser, Horne, Shimony and Holt based on previous work by John Bell
- Alice and Bob receive bits x and y from a referee
- They have to respond with bits a and b
- They win if

$$a \oplus b = x \cdot y$$

- They can decide on a joint strategy beforehand, but they cannot communicate during the game

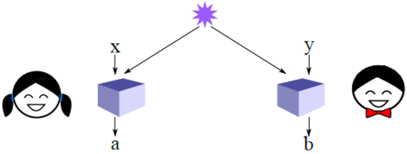
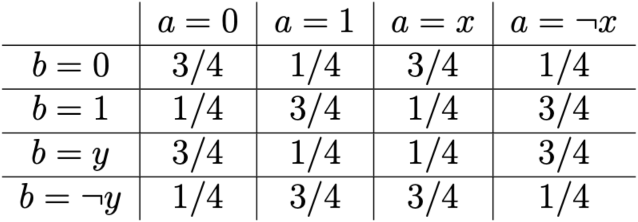


Image credits: quantumcomputing.stackexchange.com

Classical strategies for the CHSH game

- Alice and Bob can win 75% of the time if they always answer ‘0’
- No other deterministic strategy can do better
- And probabilistic strategies are convex combinations of classical strategies so they cannot improve the 75% success rate

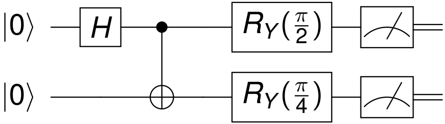


	$a = 0$	$a = 1$	$a = x$	$a = \neg x$
$b = 0$	$3/4$	$1/4$	$3/4$	$1/4$
$b = 1$	$1/4$	$3/4$	$1/4$	$3/4$
$b = y$	$3/4$	$1/4$	$1/4$	$3/4$
$b = \neg y$	$1/4$	$3/4$	$3/4$	$1/4$

Image credits: Ryan O’Donnell

Quantum strategy for the CHSH game

- Alice and Bob share a Bell pair $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ before the start of the game
- If Alice receives 0, she measures her qubit and ouputs the result
- If she receives 1, she applies $R_Y(\frac{\pi}{2})$ to her qubit and then she measures it
- If Bob receives 0, he applies $R_Y(\frac{\pi}{4})$. Else, he applies $R_Y(-\frac{\pi}{4})$.
- Then, he measures his qubit
- The probability of winning is now $\cos^2(\frac{\pi}{8}) \approx 0.85 > 0.75$



Some comments on the CHSH game

- It can be proved that $\cos^2(\frac{\pi}{8})$ is the highest possible success rate for a quantum strategy (Tsirelson's bound)
- The CHSH game can be used to rule out local realism
- Several experiments have been conducted, including:
  - Aspect et al. (1981-82)
  - Hensen et al. (2005) - Eliminate the locality and detection loopholes
- All of them agree with the predictions of quantum theory

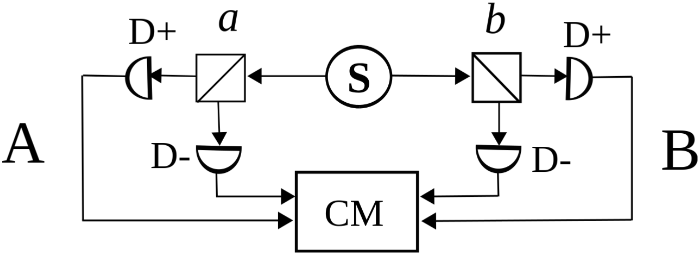


Image credits: George Stamatiou based on png file of C.Thompson

The GHZ game

- Introduced by Greenberger, Horne and Zeilinger
- A referee selects *rst* from $\{000, 011, 101, 110\}$ and sends *r* to Alice, *s* to Bob and *t* to *Charlie*
- They produce *a*, *b* and *c* and win if

$$a \oplus b \oplus c = r \vee s \vee t$$

- Classically, they can only win with 75% probability
- Quantumly, they can win every single time
  - They share the state

$$\frac{1}{2}(|000\rangle - |011\rangle - |101\rangle - |110\rangle$$

  - They apply *H* to their qubit if the receive 1
  - They measure and return the answer
- This is sometimes called “quantum pseudo-telepathy” (Brassard, Cleve, Tapp)
- Both the CHSH and the GHZ game can be used for randomness certification (and expansion)