Quantum Computation: From Quantum Teleportation to the Shor's Algorithm

J. J. Ruiz-Lorenzo

Dep. Física, Universidad de Extremadura
Instituto de Computación Científica Avanzada de Extremadura (ICCAEx)
http://www.eweb.unex.es/eweb/fisteor/juan
http://landau.unex.es/iccaex/

Badajoz, March 27th 2014

Plan of the Talk

- Information and Computation:
  1. Classical
     - Bits
     - Classical Logical Gates
  2. A Brief Introduction to Quantum Physics
  3. Quantum
     - Qubits
     - Quantum Logical Gates
- Quantum Teleportation
- Cryptography:
  1. Classical
  2. Quantum
- Quantum Parallelism
- The Shor's algorithm (short!!)
- Quantum Computers (Hardware)
- Is D-Wave a Quantum Computer?
- Some Bibliography

Some Philosophy of Science

- *The theory of computation has traditionally been studied almost entirely in the abstract, as a topic of pure mathematics. This is to miss the point of it. Computers are physical objects, and computations are physical process. What computers can or cannot compute is determined by the laws of physics alone, and not by pure mathematics.*

  (David Deustch)

- *Like mathematics, computer science will be somewhat different from the other sciences, in that it deals with artificial laws that can be proved, instead of natural laws that are never known certainty.*

  (Donald Knuth)

- *The opposite of a profound truth may well be another profound truth.*

  (Niels Bohr)

Library of Congress

Classical Information: the bit

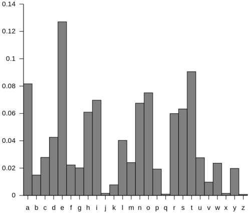
- The information is discretized.
- The elementary unit is the bit (or cbit) which can take only two values: 0/1 or yes/no.
- Any text can be coded in a binary string (e.g. using the ASCII code) and append it a parity check bit. For example "SPhinX" can be coded as:

  11100010 10100000 11010001 11010010 11011101 10110001

- Each bit can be stored physically. For example in a classical computer each bit is registered as the charge of a "macroscopic" capacitor.

Classical Information: The (1^{st}) Shannon's theorem

Alphabet. Let $A = \{a_1, \ldots, a_{|A|}\}$ a finite alphabet equipped with a probability distribution $p_A(a_i)$ ($\sum_i p_A(a_i) = 1$).



We will consider character strings $\{x\} \equiv x_1 x_2 \cdots x_n \in A^n$ originated from a memoryless source.

- Noiseless channel (binary alphabet): Typically (as $n \gg 1$) a n-string should be composed by np 1's and $n(1-p)$ 0's (they are the typical sequences), and their number is:

$$\binom{n}{np} \simeq 2^{nH(p)}$$

being

$$H(p) \equiv -p \log_2 p - (1-p) \log_2 (1-p)$$

the Shannon entropy.
For a generic alphabet:

$$H(A) \equiv -\sum_i p_i \log_2 p_i$$

So, an optimal code will be able to compress each letter in H bits asymptotically. So, we can define the redundancy of a given source A as:

$$R(A) \equiv 1 - \frac{H(A)}{\log_2 |A|}$$

Examples: Huffman codes, Morse code, writings in WhatsApp, etc.

In English we can assume $H \simeq 1.2$.
A typical sequence of n letters can be encoded with 1.2 n bits or $1.2n/\log_2 27 = 0.25n$ letters.
So, the redundancy of the English is 75%.

Note. In Statistical Mechanics,

$$P(E_i) = \exp(-\beta E_i)/Z$$

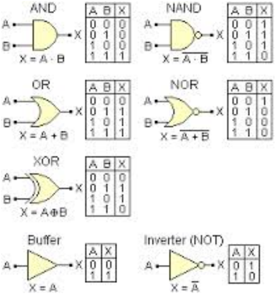
with

$$Z = \sum_i \exp(-\beta E_i)$$

then the entropy can be written as:

$$S/k_B = -\langle \log P(E_i) \rangle = -\sum_i P(E_i) \log P(E_i)$$

Classical Information: Logical Gates



A	B	X
0	0	0
0	1	0
1	0	0
1	1	1

A	B	X
0	0	1
0	1	1
1	0	1
1	1	0

A	B	X
0	0	0
0	1	1
1	0	1
1	1	1

A	B	X
0	0	1
0	1	0
1	0	0
1	1	0

A	B	X
0	0	0
0	1	1
1	0	1
1	1	0

A	X
0	0
1	1

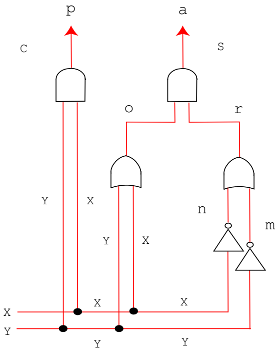
A	X
0	1
1	0

We can build all the logical gates with only NANDs and (FANOUTs) (Universal Set).

Another universal sets: {NOR}, {AND, NOT}.

Classical Information: Logical Gates

Classical circuit which sums two bits (x and y).



Quantum Physics

The state

- We will denote a quantum state as $|\phi\rangle$. For example the spin state of an electron is ($m_s = +1/2$):

$$|\phi\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

- We also define:

$$\langle\phi| = (1, 0)$$

$\langle\phi| = (|\phi\rangle^T)^*$

- And so,

$$|\phi\rangle\langle\phi| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} (1, 0) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$(\phi, \phi) = \langle\phi|\phi\rangle = (1, 0) \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 1$$

Quantum Physics

The state

- A state (e.g. a vector of $\mathbb{C}^2$) can be expanded on a given (orthonormal) basis $\{|\phi_i\rangle\}$:

$$|\Psi\rangle = \sum_i a_i |\phi_i\rangle$$

  In our example:

$$|\Psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix} = a \begin{pmatrix} 1 \\ 0 \end{pmatrix} + b \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

  with a and b being complex numbers.

- We will use states with norm (length) unit: $\langle \Psi | \Psi \rangle = 1$. So: $|a|^2 + |b|^2 = 1$.

Quantum Physics

The evolution

- The evolution of a state in Quantum Physics is Unitary: it preserves the norms of the vectors

$$|\Psi'\rangle = U|\Psi\rangle$$

In our example, U is a 2×2 complex matrix satisfying: $U^\dagger U = I$.

$$\begin{pmatrix} a' \\ b' \end{pmatrix} = \begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}$$

Notes:

1. $U^\dagger = (U^T)^*$
2. $(\Psi', \Psi') = \langle \Psi' | \Psi' \rangle = (U\Psi, U\Psi) = (U^\dagger U \Psi, \Psi) = (\Psi, \Psi) = 1$

- The state $|\Psi\rangle = \sum_i a_i|\phi_i\rangle$ has a probability $|a_j|^2$ to be in the state $|\phi_j\rangle$.
- In our example, the state $|\Psi\rangle$ has a probability $|a|^2$ to be in the state $m_s = +1/2$.
- This is the reason to work with states of unit norm (the sum of all the probabilities should be 1):

$$\langle\Psi|\Psi\rangle = \sum_i |a_i|^2 = 1$$

- If we measure and find the state $|\phi_j\rangle$, the original state "collapses" after the measurement in $|\phi_j\rangle$:

$$|\psi\rangle \xrightarrow{\text{measurement}} |\phi_i\rangle$$

Quantum Physics

The Density Matrix

- A given device can generate states $|\psi_l\rangle$ with probability p_l $(\sum_l p_l = 1)$.
- For example, one can generate electrons 50% of the time with $m_s = 1/2$ otherwise with $m_s = -1/2$.
- But this is different from

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\end{pmatrix} + \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\end{pmatrix}$$

- Mathematically we describe this device by means a density matrix (mixed states), defined as

$$\rho = \sum_l p_l |\psi_l\rangle\langle\psi_l|$$

- In the example:

$$\rho = \frac{1}{2}\begin{pmatrix}1\\0\end{pmatrix}(1,0) + \frac{1}{2}\begin{pmatrix}0\\1\end{pmatrix}(0,1) = \begin{pmatrix}\frac{1}{2} & 0\\0 & \frac{1}{2}\end{pmatrix}$$

The entanglement

- Schrödinger introduced this concept/term in the early days of the QM.
- Let us consider only two state levels (e.g. electron spin or light polarization) and two particles (#1 and #2).
- The typical example of entangled state is the EPR pair:

$$|\Psi_{12}^{(-)}\rangle = \frac{1}{\sqrt{2}}\Big(|1\rangle_1|0\rangle_2 - |0\rangle_1|1\rangle_2\Big)$$

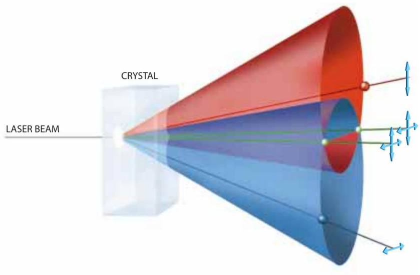
- In terms of the photon polarization: $|0\rangle = |V\rangle$ and $|1\rangle = |H\rangle$.
- In terms of the third component of the spin of the electron: $|0\rangle = |+\rangle$ and $|1\rangle = |-\rangle$.
  In both cases:

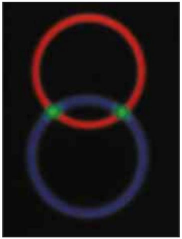
$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}\ ,\ |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$$

We can use this vector representation for all two state levels.

The entanglement

Entangled photon pairs are created when a laser beam crosses a crystal of beta barium borate.



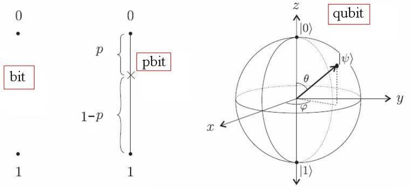


Quantum Information: the qubit

- A qubit is a two dimensional quantum system (with Hilbert space $\mathbb{C}^2$).
- In addition to the vectors $|0\rangle$ and $|1\rangle$, the systems can be in infinitely many other (pure) states given by the linear superposition:

$$\boxed{\alpha|0\rangle + \beta|1\rangle}$$

- The Hilbert space of n qubits is $\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2 = \mathbb{C}^{2^n}$.
- We can parameterize a generic ray Ψ in the so-called Bloch sphere (with angles θ, ϕ): $|\Psi\rangle = \cos(\theta/2)|0\rangle + \sin(\theta/2)\mathrm{e}^{i\phi}|1\rangle$,



$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle.$$

Quantum Information: The Schumacher's Theorem

- Now the alphabet consists in quantum states (in general non-orthogonal) and their probabilities:

$$A = \{|\phi_i\rangle, p_i\} \ , \ i = 1, \ldots, |A|$$

- We will assign to A a density matrix:

$$\rho(A) = \sum_i p_i |\phi_i\rangle\langle\phi_i|$$

- A message from the source A is composed by a sequence of quantum states $|\phi_1\rangle|\phi_2\rangle \ldots |\phi_{i_m}\rangle$, each of them generated with probability p_i.
- The associated density matrix is

$$\rho^{(n)} = \rho \otimes \cdots \otimes \rho$$

which lives in a Hilbert space of dimension $|A|^n = 2^{n \log_2 |A|}$

Quantum Information: Theorem of Schumacher

- Asymptotically ($n \gg 1$) the matrix $\rho^{(n)}$ can be compressed, with fidelity F, to another density matrix which lives in a Hilbert space of dimension:

  $$2^{nS(\rho^{(n)})}$$

  where

  $$S(\rho) = -\mathrm{Tr}(\rho \log_2 \rho)$$

  is the Von Neumann entropy.
- Using the (convex) decomposition of ρ as $\rho = \sum_i p_i |\phi_i\rangle\langle\phi_i|$ then

  $$S(\rho) \le H(I) = -\sum_i p_i \log_2 p_i$$

  (Equality holds iff all the states are pairwise orthogonal).
- For a pure state $\rho = |\phi\rangle\langle\phi|$ and $S(\rho) = 0$.

Quantum Information: Logical Gates

- A quantum logical gate acting on a group of k qubits (a quantum register) is any unitary operator in the associated Hilbert space $\mathbb{C}^{2^k}$.
- For one qubit, we can use, e.g., the identity (I), and the three Pauli matrices (denoted as $X \equiv U_{\mathrm{NOT}}$, Y and Z). We can define the Hadamard gate as $H_{\mathrm{H}} = 2^{-1/2}(X + Z)$.

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

- We can implement some logical gates via, e.g., firing a pulse laser on a two state system.

- On two qubits one of the most important gate is the controlled NOT (U_{CNOT}) or *exclusive* OR (U_{XOR}) which acts on the basis of $(\mathbb{C}^2)^2$ as:

  $$U_{\mathrm{CNOT}}|x\rangle|y\rangle = U_{\mathrm{XOR}}|x\rangle|y\rangle \equiv |x\rangle|x \oplus y\rangle$$

  where x, y are 0 or 1 and $x \oplus y = x + y \pmod 2$. The matrix representation of this gate is

  $$U_{\mathrm{CNOT}} = U_{\mathrm{XOR}} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U_{\mathrm{NOT}}$$

- Reversible computation (two qubits to two qubits)!
- We can also define Universal Quantum Gates.

Quantum Information: No cloning Theorem

[Wootters+Zurek(1982)]

- Let $U_{\rm QCM}$ be the *linear* and unitary operator that implements the quantum copier machine in the Hilbert space ($\mathcal{H}$).
- This operator satisfies $U_{\rm QCM}|\Psi\rangle_{\rm orig}|\phi_0\rangle = |\Psi\rangle_{\rm orig}|\Psi\rangle_{\rm copy}, \ \forall \Psi \in \mathcal{H}$.
- We want to copy the simplest entity, a qubit: $|\Psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$
- Linearity of $U_{\rm QCM}$ implies: $U_{\rm QCM}|\Psi\rangle|\phi_0\rangle = \alpha_0|0\rangle|0\rangle + \alpha_1|1\rangle|1\rangle$
- But using the definition of a copier: $U_{\rm QCM}|\Psi\rangle|\phi_0\rangle = |\Psi\rangle|\Psi\rangle = \alpha_0^2|0\rangle|0\rangle + \alpha_0\alpha_1|0\rangle|1\rangle + \alpha_0\alpha_1|1\rangle|0\rangle + \alpha_1^2|1\rangle|1\rangle$
- States which are, in general, different!!
- Hence, the quantum copier machine cannot exit.

Quantum Information: No cloning Theorem

- We can extend the previous proof to take into account the environment. Now $\mathcal{H} = \mathcal{H}_{\text{orig}} \otimes \mathcal{H}_{\text{copy}} \otimes \mathcal{H}_{\text{env}}$.
- By the definition of the copier machine: $U_{\text{QCM}}|\Psi\rangle_{\text{orig}}|\phi_0\rangle|E_0\rangle = |\Psi\rangle_{\text{orig}}|\Psi\rangle|E_\Psi\rangle, \ \forall \Psi \in \mathcal{H}_{\text{orig}}$.
- Let us consider two actions of the QCM: $U_{\text{QCM}}|\Psi_1\rangle|\phi_0\rangle|E_0\rangle = |\Psi_1\rangle|\Psi_1\rangle|E_{\Psi_1}\rangle\,,$ $U_{\text{QCM}}|\Psi_2\rangle|\phi_0\rangle|E_0\rangle = |\Psi_2\rangle|\Psi_2\rangle|E_{\Psi_2}\rangle\,.$
- Taking the scalar product of the two previous states and using the unitarity of U_{QCM}: $\langle\Psi_1|\Psi_2\rangle = \langle\Psi_1|\Psi_2\rangle^2\langle E_{\Psi_1}|E_{\Psi_2}\rangle\,.$
- Since all the probability amplitudes have modulus ≤ 1: either $\langle\Psi_1|\Psi_2\rangle = 1$ or it is equal to 0: hence it is impossible to copy two different and non-orthogonal states Ψ_1 and Ψ_2.
- However, a *known* state can be copied at will.

Quantum Banknotes

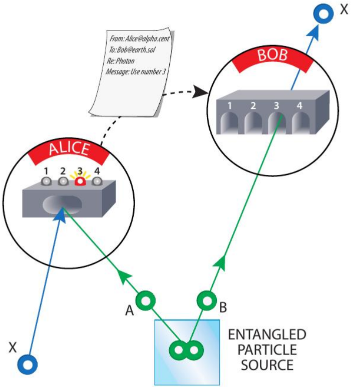
100
FEDERAL RESERVE NOTE
FF 95594731 A
$\Delta x \Delta p \geq \hbar/2$
IN QUANTUM PHYSICS WE TRUST.
$|0\rangle$ $|-\rangle$ $|+i\rangle$ $|-\rangle$ $|+i\rangle$ $|1\rangle$
$|-\rangle$ $|0\rangle$ $|1\rangle$ $|0\rangle$ $|1\rangle$ $|+i\rangle$
$|-i\rangle$ $|+\rangle$ $|+\rangle$ $|-i\rangle$ $|+\rangle$ $|1\rangle$
FF 95594731 A
ONE HUNDRED DOLLARS

Quantum Banknotes

10
10
10 EURO
10
10
10 EURO

Quantum Teleportation

- Quantum teleportation transfers only information not matter through a quantum channel. As we have seen, information can be transferred but never duplicated or cloned.
- We need a classical channel to send classical information.



From: Alice@alpha.cent
To: Bob@earth.sol
Re: Photon
Message: Use number 3

Quantum Teleportation

- We will start with three identical particles.
- The particles #2 and #3 are prepared in EPR singlet: $|\Psi^{(-)}_{23}\rangle = \frac{1}{\sqrt{2}}\Big(|1\rangle_2|0\rangle_3 - |0\rangle_2|1\rangle_3\Big)$.
- Let $|\Phi\rangle_1 = a|1\rangle_1 + b|0\rangle_1$ be the state of the particle #1 to be teletransported ($|a|^2 + |b|^2 = 1$).
- The whole state of the three particles is $|\Phi\rangle_1|\Psi^{(-)}_{23}\rangle$.
- We give particles #1 and #2 to Alice and the particle #3 to Bob.

Quantum Teleportation

- Alice will measure in the join system composed by particles #1 and #2.
- The measurement performed by Alice is made in the Bell's basis which consists in $|\Psi_{12}^{(-)}\rangle$ and

$$|\Psi_{12}^{(+)}\rangle = \frac{1}{\sqrt{2}}\Big(|1\rangle_1|0\rangle_2 + |0\rangle_1|1\rangle_2\Big)$$

$$|\Phi_{12}^{(\pm)}\rangle = \frac{1}{\sqrt{2}}\Big(|1\rangle_1|1\rangle_2 \pm |0\rangle_1|0\rangle_2\Big)$$

- The Alice's measurement consists in to detect one of the four elements of the Bell's basis $\{|\Psi_{12}^{(-)}\rangle, |\Psi_{12}^{(+)}\rangle, |\Phi_{12}^{(+)}\rangle, |\Phi_{12}^{(-)}\rangle\}$.

Quantum Teleportation

- The original state can be written using the Bell's basis as

$$
\begin{aligned}
|\Phi\rangle_1 |\Psi_{23}^{(-)}\rangle = \frac{1}{2}\Big(& |\Psi_{12}^{(-)}\rangle \left(-a|1\rangle_3 - b|0\rangle_3\right) \\
& + |\Psi_{12}^{(+)}\rangle \left(-a|1\rangle_3 + b|0\rangle_3\right) \\
& + |\Phi_{12}^{(-)}\rangle \left(b|1\rangle_3 + a|0\rangle_3\right) \\
& + |\Phi_{12}^{(+)}\rangle \left(-b|1\rangle_3 + a|0\rangle_3\right) \Big)
\end{aligned}
$$

- Some rotation matrices ($s = 1/2$):

$$R_{\hat{\boldsymbol{n}}}(\theta) = \exp(-i\frac{\theta}{2}\boldsymbol{\sigma}\hat{\boldsymbol{n}})$$

So,

$$R_x(\pi) = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}, R_y(\pi) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, R_z(\pi) = \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix}.$$

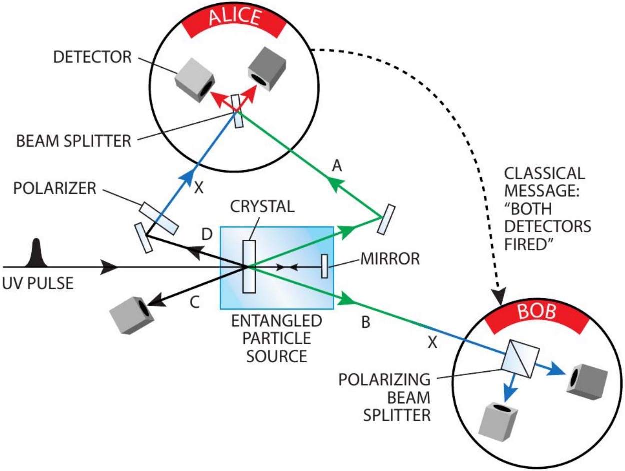
Quantum Teleportation

- Hence

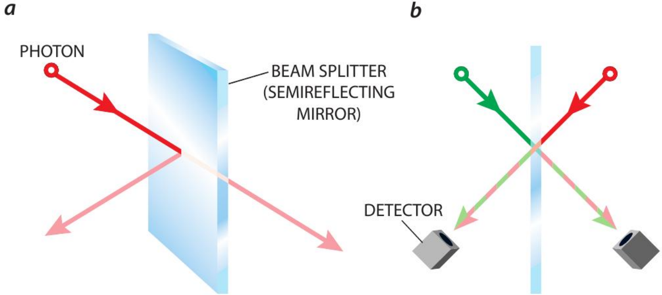
$$
\begin{aligned}
-iR_x(\pi)|\Phi\rangle &= b|1\rangle + a|0\rangle \, , \\
R_y(\pi)|\Phi\rangle &= -b|1\rangle + a|0\rangle \, , \\
-iR_z(\pi)|\Phi\rangle &= -a|1\rangle + b|0\rangle \, .
\end{aligned}
$$

- The probability of the four independent measures are the same 1/4. In addition:
  1. If Alice measures $|\Psi_{12}^{(-)}\rangle$, communicates it to Bob (classically), Bob has already the state $|\Phi\rangle$.
  2. If Alice measures $|\Psi_{12}^{(+)}\rangle$, communicates it to Bob (classically), and Bob will rotate his particle π around the axis z in order to recover $|\Phi\rangle$.
  3. If Alice measures $|\Phi_{12}^{(-)}\rangle$, communicates it to Bob (classically), Bob will rotate his particle π around the axis x in order to recover $|\Phi\rangle$.
  4. If Alice measures $|\Psi_{12}^{(+)}\rangle$, communicates it to Bob (classically), Bob will rotate his particle π around the axis y in order to recover $|\Phi\rangle$.

Quantum Teleportation



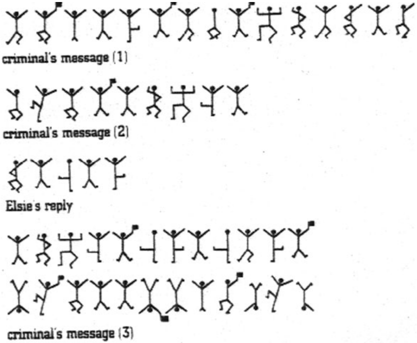
Quantum Teleportation

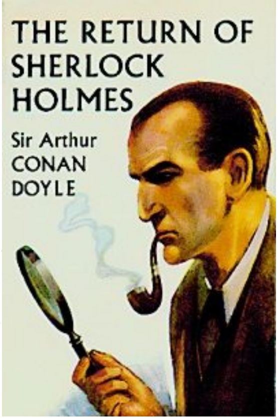


Both detectors (simultaneously) detect photons only when the polarization state of particles #1 and #2 is $|\Psi_{12}^{(-)}\rangle$. This happens with 25% of probability.

Classical Cryptography

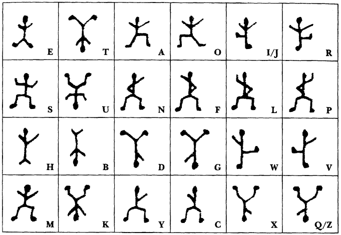
The adventure of a dancing man:





Classical Cryptography

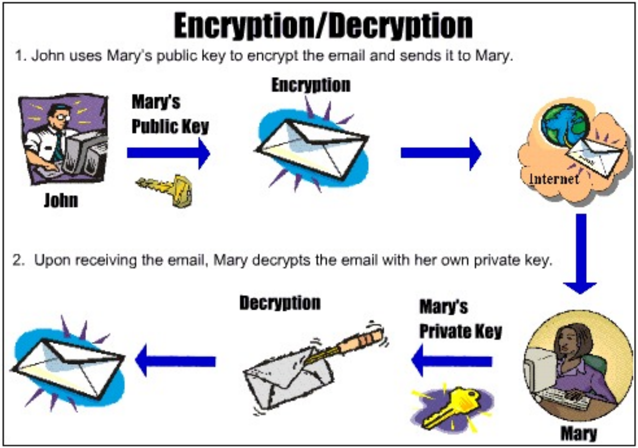
- Sherlock cracked the code by frequency analysis: it is a substitution cipher.



Classical Cryptography

- Symmetric-Key Cryptography System: The One-time Pad (or VERNAN code).
  [0 XOR 0 = 1 XOR 1 = 0, 1 XOR 0 = 0 XOR 1 = 1]
  1. We generate a string of random binary digits (Key), which is shared between the Sender and the Receiver.
  2. The Sender encodes its message as:
     Encrypted Message= Plain Message XOR Key
  3. The Receiver decodes the message as:
     Plain Message= Encrypted Message XOR Key
- Used in the *red telephone*, by Castro-Che Guevara, KGB spies,...
- Problem: Distribution of the Key. If the Key is used twice one could decode the message.

Classical Cryptography: Public Key Cryptography (RSA)

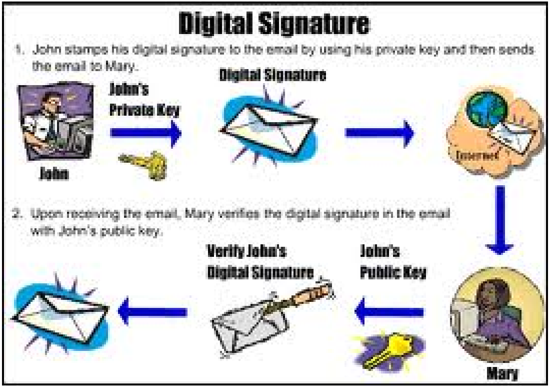


Encryption/Decryption

1. John uses Mary's public key to encrypt the email and sends it to Mary.

2. Upon receiving the email, Mary decrypts the email with her own private key.

Classical Cryptography: Public Key Cryptography (RSA)



Digital Signature

1. John stamps his digital signature to the email by using his private key and then sends the email to Mary.

2. Upon receiving the email, Mary verifies the digital signature in the email with John's public key.

Classical Cryptography: Public Key Cryptography (RSA)

- The public key consists in two numbers (N, e). N should be large and $e \in (1, \phi(N))$ with $\gcd(e, \phi(N)) = 1$. [$\phi(N)$ is the Euler totient function.]
- Alice modifies her message M using some public agreed (bijective) transformation, obtaining B ($|B| < N$) and encodes it as:

  $$C(B) \equiv B^e \pmod{N},$$

  and sends $C(B)$ to Bob, the owner of the key.
- Upon reception Bob decodes $C(B)$ using

  $$B \equiv C^d \pmod{N},$$

  where the exponent d satisfies (Bob obviously knows it)

  $$ed \equiv 1 \pmod{\phi(N)}.$$

- Note. If $N = pq$, with p and q prime numbers, then $\phi(N) = (p-1)(q-1)$, since ϕ is a multiplicative function and $\phi(p) = p - 1$, for a prime number p.

Classical Cryptography: RSA-Challenge.

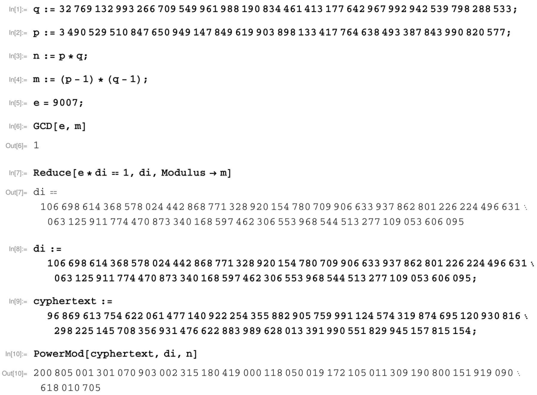
- Challenge proposed by M. Gardner in Scientific American in 1977 (with 100$ reward!).
- The encoded message:

  96869613754622061477140922254355882905759991124574319874695120930816298225145708356931476622883989628013391990551829945157815154

- It was used the following dictionary:
  $(\text{blank} \rightarrow 00, a \rightarrow 01, b \rightarrow 02, \ldots, z \rightarrow 26)$
- It was encoded using the cipher (RSA-129,9007), where RSA-129 was the number:

  114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541

Classical Cryptography: RSA-Challenge.



```
In[1]:= q := 32 769 132 993 266 709 549 961 988 190 834 461 413 177 642 967 992 942 539 798 288 533;

In[2]:= p := 3 490 529 510 847 650 949 147 849 619 903 898 133 417 764 638 493 387 843 990 820 577;

In[3]:= n := p * q;

In[4]:= m := (p - 1) * (q - 1);

In[5]:= e = 9007;

In[6]:= GCD[e, m]

Out[6]= 1

In[7]:= Reduce[e * di == 1, di, Modulus → m]

Out[7]= di ==
          106 698 614 368 578 024 442 868 771 328 920 154 780 709 906 633 937 862 801 226 224 496 631 \
           063 125 911 774 470 873 340 168 597 462 306 553 968 544 513 277 109 053 606 095

In[8]:= di :=
           106 698 614 368 578 024 442 868 771 328 920 154 780 709 906 633 937 862 801 226 224 496 631 \
            063 125 911 774 470 873 340 168 597 462 306 553 968 544 513 277 109 053 606 095;

In[9]:= cyphertext :=
           96 869 613 754 622 061 477 140 922 254 355 882 905 759 991 124 574 319 874 695 120 930 816 \
            298 225 145 708 356 931 476 622 883 989 628 013 391 990 551 829 945 157 815 154;

In[10]:= PowerMod[cyphertext, di, n]

Out[10]= 200 805 001 301 070 903 002 315 180 419 000 118 050 019 172 105 011 309 190 800 151 919 090 \
          618 010 705
```

- The original message:

  200805001301070903002315180419000118050019172105011309190800151919090618010705

- And using the dictionary:

  The magic words are squeamish ossifrage

How to break RSA

1. Eve knows the public key (N, e) and the encrypted message C.
2. Eve computes the order r of the number C:

$$C^r \equiv 1 \pmod{N}$$

3. She solves:

$$ed' \equiv 1 \pmod{r}$$

4. And finally Eve recovers the original message by computing

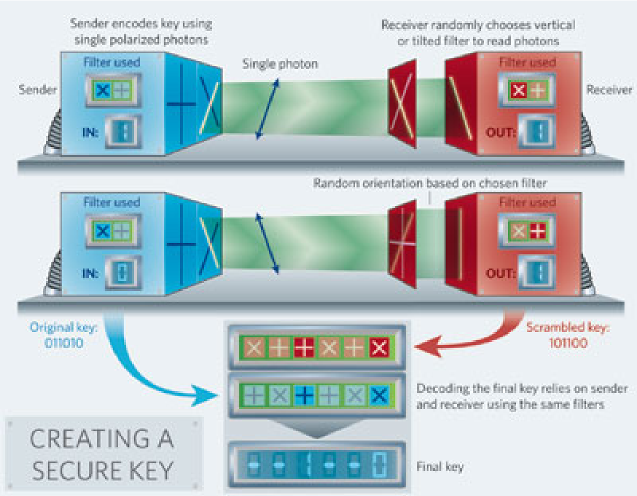
$$B \equiv C^{d'} \pmod{N}$$

Remember $C \equiv B^e \pmod{N}$.

Quantum Cryptography or better Quantum Key Distribution (QKD)

- QKD is a type of key distribution to be used in any symmetric encryption method.
- Any attempt to steal or copy a key can be detected.
- We need a classical channel and a quantum one.

Quantum Key Distribution (QKD): BB84


Sender encodes key using single polarized photons
Receiver randomly chooses vertical or tilted filter to read photons
Sender
Filter used
IN:
Single photon
Filter used
OUT:
Receiver
Random orientation based on chosen filter
Filter used
IN:
Filter used
OUT:
Original key: 011010
Scrambled key: 101100
Decoding the final key relies on sender and receiver using the same filters
Final key
CREATING A SECURE KEY

Quantum parallelism (Deutsch's problem)

- Let $f(x)$ be a function from bits to bits.
- We want to decide if this function is constant (i.e. $f(0)=f(1)$) or balanced (i.e. $f(0)\neq f(1)$).
- We define a transformation acting in two qubits:

$$U_f : |x\rangle|y\rangle \longrightarrow |x\rangle|y\oplus f(x)\rangle$$

- We define the following input state

$$|i\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

then

$$U_f|x\rangle|i\rangle = \frac{1}{\sqrt{2}}U_f|x\rangle|0\rangle - \frac{1}{\sqrt{2}}U_f|x\rangle|1\rangle$$

and

$$U_f|x\rangle|i\rangle = (-1)^{f(x)}|x\rangle|i\rangle$$

Quantum parallelism

- Now, we fix

$$|x\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$

- Hence,

$$U_f|x\rangle|i\rangle = \frac{1}{\sqrt{2}}\Big((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\Big)\,|i\rangle$$

- The next step is to project (measure) the first qubit in the basis

$$|\pm\rangle = \frac{1}{2}\left(|0\rangle \pm |1\rangle\right)$$

- Obtaining $|-\rangle$ if f is balanced and $|+\rangle$ if f is constant.

Quantum parallelism

- Now, we are interested in global properties of a function f acting on N bits [2^N possible arguments].
- $U_f : |x\rangle|0\rangle \longrightarrow |x\rangle|f(x)\rangle$. Now x is a N-qubits.
- As the input state we choose

$$|i\rangle = \left[\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)\right]^N = \frac{1}{2^N}\sum_{x=0}^{2^N-1}|x\rangle$$

- Then

$$U_f : |i\rangle|0\rangle = \frac{1}{2^N}\sum_{x=0}^{2^N-1}|x\rangle|f(x)\rangle$$

Factoring numbers in primes: The Shor's algorithm

- The computational cost of factoring (general number field sieve) a number with n decimal digits is

  $$\text{cost} = O\left[\exp\left(c(\log n)^{1/3}(\log\log n)^{2/3}\right)\right]$$

  with $c \simeq 1.9$
- The biggest factorized number is a RSA-768 (768 bits with 232 decimal digits) on 12/12/2009. It took 2000 years on a single-core AMD-Opteron running at 2.2 GHz [2 years using a citizen computing platform].
- However the cost for the Shor's algorithm is

  $$\text{cost} = O\left[(\log n)^3\right]$$

Quantum Hardware: Specifications

1. Storage.
2. Isolation. In order to avoid the decoherence problem.
3. Readout.
4. Gates.
5. Precision.

Quantum Hardware: Some Examples

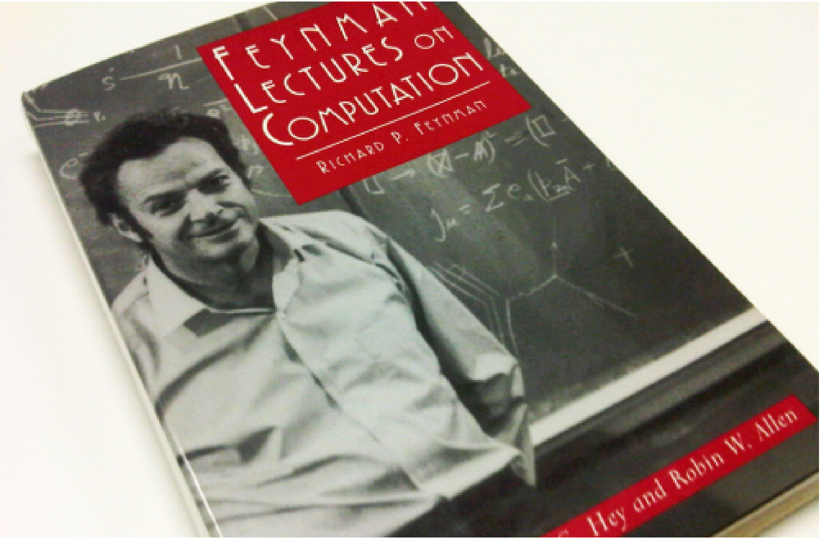
- One- and two-qubit logic gates with spin qubits.
- Ion Trap.
- Cavity QED.
- MNR. Factorizing the number 15 with 7 qubits. The record is the factorization of 21 (2012)!!
- Solid State Quantum Computers.

D-Wave

D-Wave “quantum computers” have been bought by Google, USC-Lockheed-Martin and NASA.

Some Bibliography

- A. Galindo and M. A. Martín-Delgado, *Information and computation: Classical and quantum aspects*, Reviews of Modern Physics **74**, 347 (2002).
- J. Preskill's course on Quantum Computation: `http://www.theory.caltech.edu/people/preskill/ph229/`.
- U. V. Vazirani's lecture notes: `http://www-inst.eecs.berkeley.edu/~cs191/sp12/`.
- M. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
- R. P. Feynman, *Feynman Lectures on Computation* (Addison-Wesley, Reading MA, 1996). Edited by A. Hey and R. Allen.
- D. Mermin's lecture notes: `http://www.lassp.cornell.edu/mermin/qcomp/CS483.html`. See also the book: *Quantum Computer Science: An Introduction* (Cambridge University Press, Cambridge, 2006).
- A. Zelinger, *Quantum Teleportation*. Sci. Am. April 2000.


Feynman
Lectures on
Computation
Richard P. Feynman
Hey and Robin W. Allen