Physical Basis of Quantum Computation and Cryptography

Manuel Calixto

Departamento de Matemática Aplicada y Estadística, Universidad Politécnica de Cartagena, Spain
Manuel.Calixto@upct.es

Abstract

QUANTUM COMPUTING *combines two of the main scientific achievements of the 20th century: Information Theory and Quantum Mechanics. Its interdisciplinary character is one of the most stimulating and appealing attributes. The new Quantum Information Theory augurs powerful machines that obey the "entangled" logic of the subatomic world.* Parallelism, entanglement, teleportation, no-cloning and quantum cryptography *are typical peculiarities of this novel way of understanding computation. In this article, we highlight and explain these fundamental ingredients that make Quantum Computing potentially powerful.*

1. Classic versus Quantum: bit versus qubit

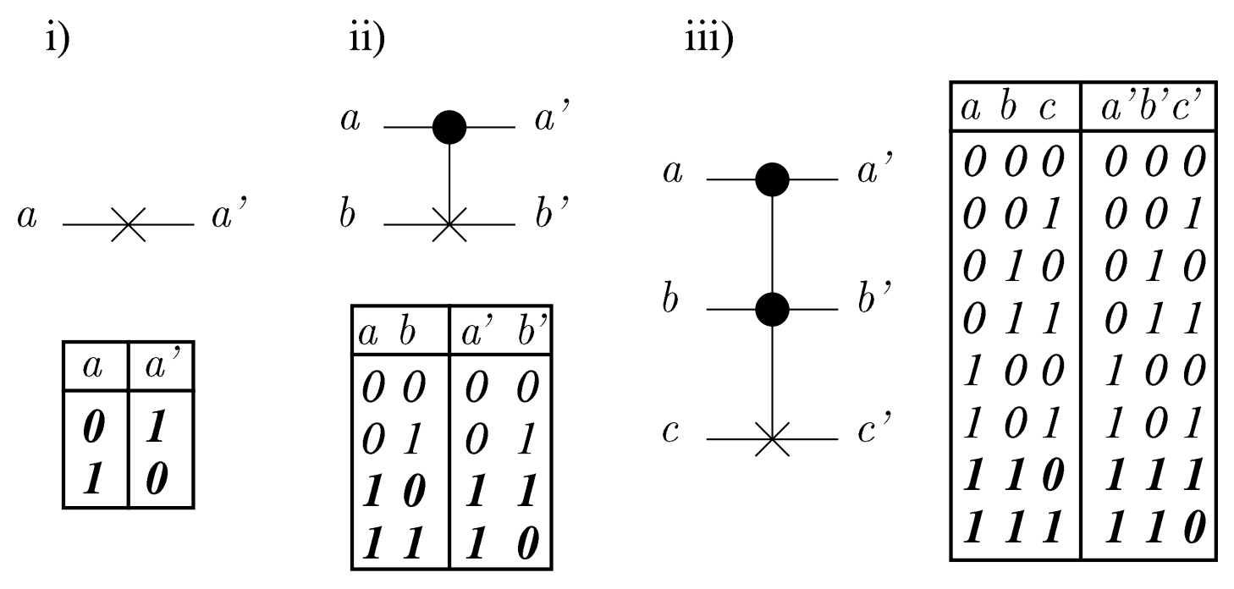
A two stable positions *classical* device can store one bit of information, e.g., the answer "yes" (1) or "no" (0) to a question.

The description of physical phenomena starts needing the Quantum Theory as the energy (or action) gap between the states $|0\rangle$ and $|1\rangle$ (in Dirac's bracket notation) becomes smaller and smaller. This happens with more probability in the subatomic world than in the macroscopic world. Quantum alternatives $|n\rangle$ whose action gap is of the order of the Planck constant $\hbar$, coexist in some sort of quantum superposition or wave function like

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle \qquad (1)$$

with complex weights c_n (probability amplitudes) fulfilling $|c_0|^2+|c_1|^2 = 1$. Thus, the wave function (1) carries an information different from the classic one, which we agree to call *qubit* (quantum bit). Physical devices that store one qubit of information are two-level quantum systems like: spin $1/2$ particles and atoms (electrons, silver atoms, etc), polarized light (photons), energy levels of some ions, etc. For example, it is possible to prepare a quantum state like (1) striking a laser beam of proper frequency and duration on some ions.

Loosely speaking, the manipulation and processing of classical information comes down to swapping 0's and 1's around though logic gates (viz, NOT, AND, OR). Note that, except for NOT, classical logic gates are *irreversible*; that is, knowing the result $c = a + b$, we can not guess a and b. This loss of information leads to the well known heat dissipation of classical computers. Actually, we could make classical computation reversible, by replacing traditional logic gates by the new ones: NOT, CNOT and CCNOT, in Figure 1, the price being perhaps a waste of memory. However, Quantum Computation must be intrinsically reversible, since it is based on a *unitary* time evolution of the wave function (probability must be conserved), dictated by the Schrödinger equation.



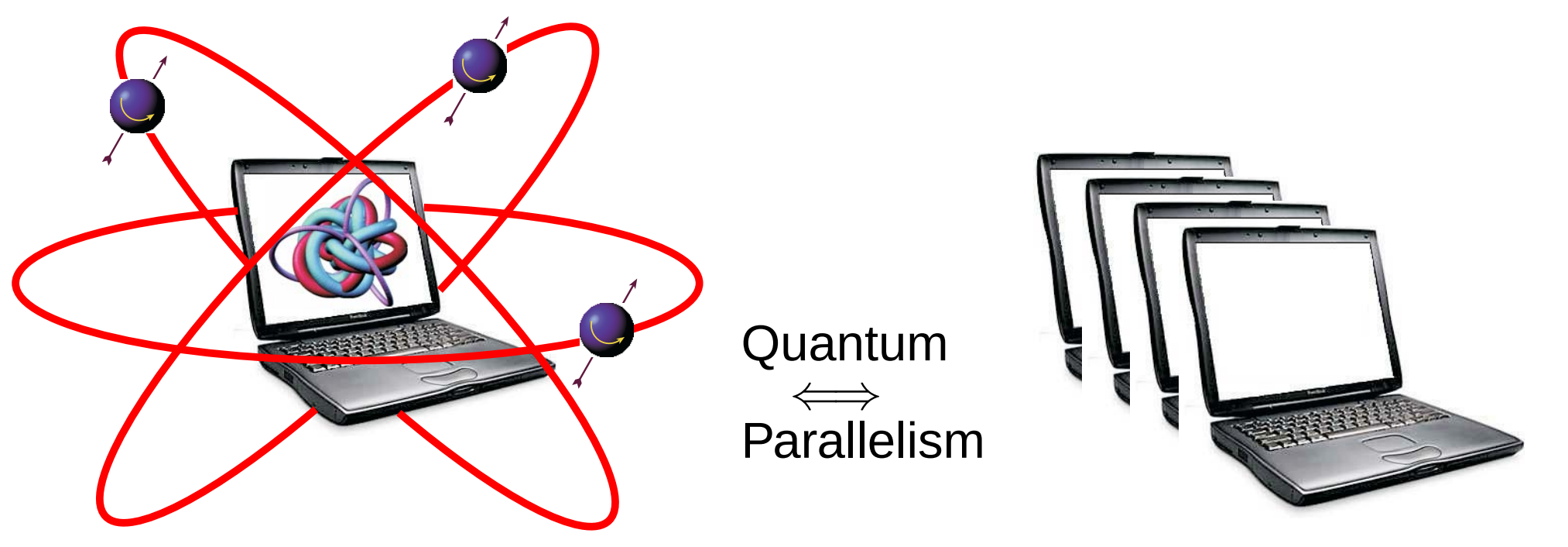
a	a'
0	1
1	0

a b	a' b'
0 0	0 0
0 1	0 1
1 0	1 1
1 1	1 0

a b c	a'b'c'
0 0 0	0 0 0
0 0 1	0 0 1
0 1 0	0 1 0
0 1 1	0 1 1
1 0 0	1 0 0
1 0 1	1 0 1
1 1 0	1 1 1
1 1 1	1 1 0

Figure 1: *Truth tables of the basic reversible gates:* NOT, CNOT *and* CCNOT *or Toffoli gates.*

2. Interference and Quantum Parallelism



Quantum Computing would not have any appeal if it wasn't that the quantum state described by the wave function (1) is not only a statistical mixture with probabilities $p_0 = |c_0|^2$ and $p_1 = |c_1|^2$ but, in addition, it incorporates two important new ingredients: *interference*, or "parallelism", and *entanglement*, or "quantum correlations" (see next section) The coexistence of quantum alternatives gives rise to interference effects that defy the common sense, like the well-known two-splits Young's experiment which highlights the particle-wave duality of the electron.

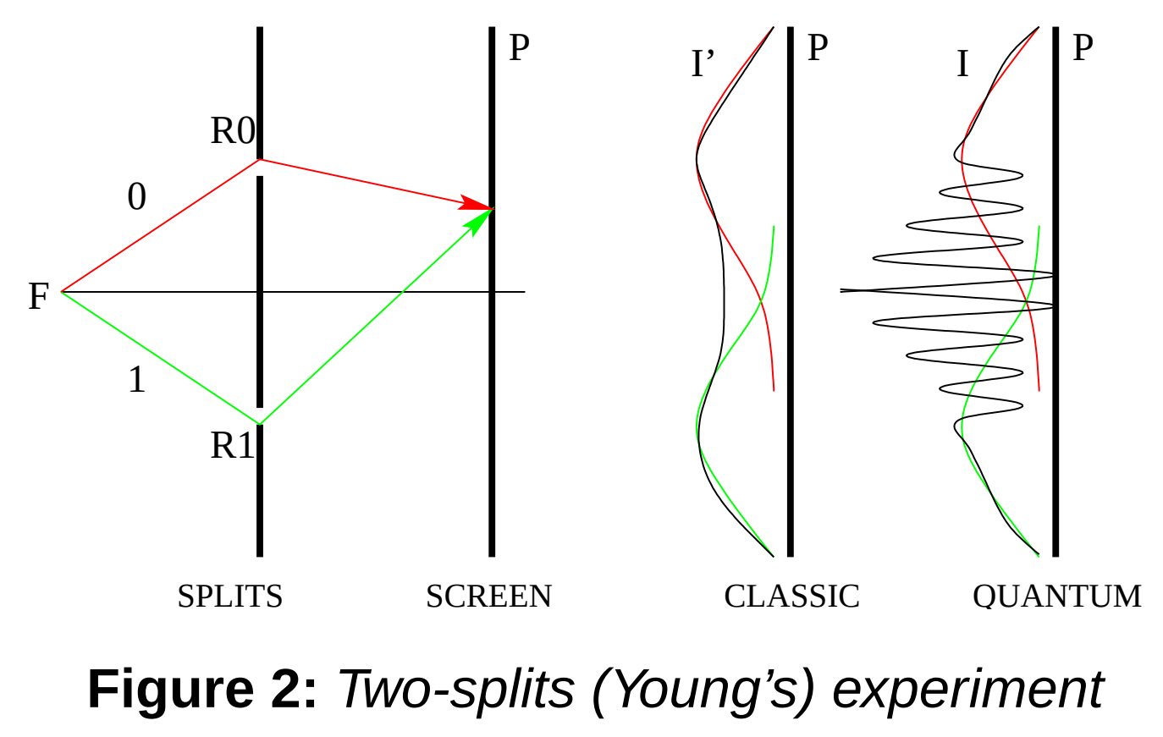


Figure 2: *Two-splits (Young's) experiment*

The interference between the two electron's path (namely 0 and 1) gives rise to a resulting intensity (quantum case) $I \propto |c_0+c_1|^2 \neq |c_0|^2+|c_1|^2 \propto I'$ different from just adding up the intensities through each split (classical case).

Note that, with two qubits, we can prepare a register in a quantum superposition of $2^2 = 4$ numbers from 0 up to 3 (we ignore normalization, for simplicity):

$$|\psi\rangle = |a\rangle\,|b\rangle = (|0\rangle+|1\rangle)\otimes(|0\rangle+|1\rangle) = |00\rangle+|01\rangle+|10\rangle+|11\rangle = \sum_{x=0}^{3}|x\rangle. \qquad (2)$$

This can be the spin state ($|\downarrow\rangle \equiv |0\rangle\,, |\uparrow\rangle \equiv |1\rangle$) of carbon (a) and hydrogen (b) nucleus in a chloroform molecule CHCl$_3$. This "toy quantum computer" can implement the CNOT (controlled not) gate in Figure 1, by placing the molecule in an external magnetic field and acting on it with radiowave pulses that flip the spin of the nucleus. Actually, only when the spin of the carbon points in the direction of the external magnetic field (i.e., $|\uparrow\rangle = |1\rangle$), it is possible to flip the spin of the hydrogen. That is, the carbon is the "control" and the hydrogen acts as a XOR gate (see Figure 1). It is proved that, assembling (two-qubit) CNOT and arbitrary one-qubit unitary (quantum) gates is enough to design any classical algorithm like: addition, multiplication, etc (classically, they are the CNOT and CCNOT gates that constitute a universal set).

In order to process more complex quantum information, it is promising to use lineal ion traps, where the coupling between electron and vibrational degrees of freedom allows (in principle) the implementation of operations in a multi-qubit register by absorbtion and emission of photons and phonons.

In a four-qubits quantum computer, the application of the unitary operation $U_\oplus$ that implements the adding algorithm modulo 4 between the state (2) and a second one like $|\psi'\rangle = |x'\rangle$, with $x' = 0, \ldots, 3$, gives an output of the form:

$$|\psi\rangle\,|\psi'\rangle = \sum_{x=0}^{3}|x\rangle|x'\rangle \xrightarrow{U_\oplus} \sum_{x=0}^{3}|x\rangle|x\oplus x'\rangle. \qquad (3)$$

That is, we have *simultaneously* computed the addition $x \oplus x'$ for four different values of of x, equivalent to four four-bits classical computers working in parallel. This feature is called *quantum parallelism*.

However, we can only measure or "amplify" one of the four answers of the output $\sum_{x=0}^{3}|x\oplus x'\rangle \xrightarrow{\text{measure}} |x_0\oplus x'\rangle$. Let us see that it is not exactly superposition or parallelism what makes powerful quantum computation, but it is *quantum entanglement* or correlation between answers.

3. Entanglement: EPR paradox

There are physical situations in which (quantum) particle pairs (or higher groupings) are created as if the state of one member would "instantaneously" determine or influence the state of the other, though they were hundreds of kilometres apart. It is not exactly like having couples of loaded dice that always offer the same face, but much more "intriguing". For example, spin positron-electron entangled pairs $|EP\rangle = |\uparrow\rangle_e|\downarrow\rangle_p - |\downarrow\rangle_e|\uparrow\rangle_p$ are created in the decay of spin cero neutral particles; also pairs of photons with orthogonal polarizations (V means vertical and H horizontal) $|VH\rangle = |\updownarrow\rangle_1|\leftrightarrow\rangle_2 - |\leftrightarrow\rangle_1|\updownarrow\rangle_2$ are created by striking laser pulses on certain non-linear crystals. These are just particular examples (the so called "singlet states"), but more general situations are also possible.

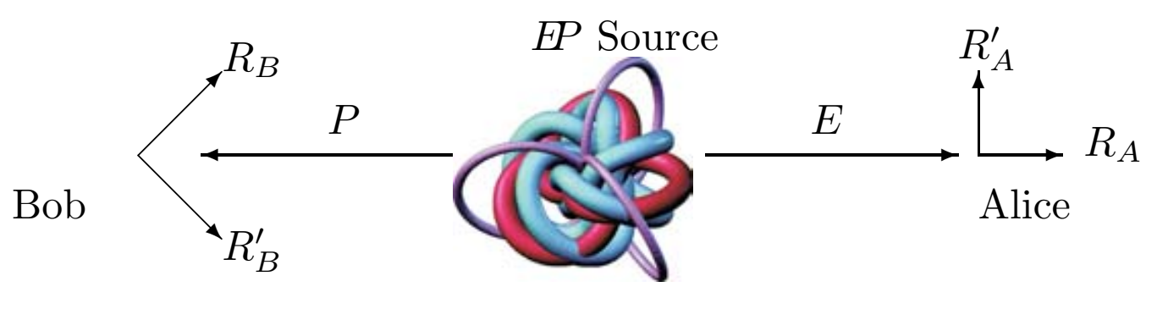


Figure 3: *Measuring entangled pairs* $|EP\rangle$

In the case of entangled spins like EP, we propose the following "gedankenexperiment" (imaginary experiment depicted in Figure 3. Alice A and Bob B are equipped each of them with magnetic fields $\vec{H}_A$ and $\vec{H}_B$, which can be oriented in the directions: $\uparrow, \rightarrow$ and $\nearrow, \searrow$, respectively, like in the Stern-Gerlach experiment for silver atoms. From the result R_A of the electron's (E) spin in the Alice's measurement (which can result in: either parallel $|\uparrow\rangle_e$ or antiparallel $|\downarrow\rangle_e$ to the external magnetic field $\vec{H}_A$), one can predict with certainty the result R_B of the positron's (P) spin in Bob's measurement, when measuring in the same direction $\vec{H}_B||\vec{H}_A$ as Alice (R_B ought to be antiparallel to R_A in this case). This would happen even if Alice and Bob were far away, so that no information exchange between them could take place before each measurement, according to Einstein's causality principle.

The insight of these experiments is that, contrary the classical (macroscopic) systems, **subatomic entities do NOT have well defined values of their properties before they are measured**; instead, all possible values must coexist in a quantum superposition like (1). This interpretation upset Albert Einstein, who once said: "Good does not play dice".

It is clear that these kind of experiences at subatomic level, utterly uncommon in the macroscopic world, could be efficiently used in a future to create really surprising situations. Let us imagine a World-Wide-Web of entangled quantum computers that cooperate performing tasks which are imposible even via satellite. Nowadays, this is just speculation, although there are actual and future applications of entanglement in the field of telecommunications. Le us see some of these implementations of entanglement.

4. Entanglement and teleportation

One of the most spectacular applications of entanglement is the possibility of transporting a quantum system from one place to another without carrying matter, but just information. Teleporting the polarization state of one photon, like $|\Psi\rangle = c_0\,|\updownarrow\rangle + c_1\,|\leftrightarrow\rangle$, is nowadays physically realizable thanks to the original idea of Bennet et al. and the Innsbruck experiment. However, there is a long way to cover before we can teleport a macroscopic (even a mesoscopic) system. Before we must fight "quantum decoherence" (qubits a fragile and sensitive to any kind of external noise).

Teleportation of one photon goes as follows (see Figure 4). A ultraviolet laser pulse strikes a Barium β-Borate crystal, creating an entangled pair of photons $(F1, F1')$ and other pair $(F2, F2')$ after reflection in a mirror $M1$. The polarizer P prepares $F2$ in the state Ψ, which joins $F1$ through a beam splitter (BS). Then Alice makes a two-qubit measure (also, "coincidence" or Bell's measure) with the photon detectors $D1, D2$. The measurement can have four different answers: $(R_{D_1}, R_{D_2}) = (1,1), (1,0), (0,1), (0,0)$. If both detectors are struck (i.e. the answer is $(1,1)$), Alice tells Bob (through a classic message) that the photon $F1'$ has "transmuted" to the state Ψ, which Bob can verify by using a beam splitter polarizer (BSP), consisting in a calcite crystal. In the other three cases, Alice can always indicate Bob the operation to rotate $F1'$ to Ψ. Thus, we need a two-bits classic message to teleport one qubit (this is some sort of *dense information coding*).

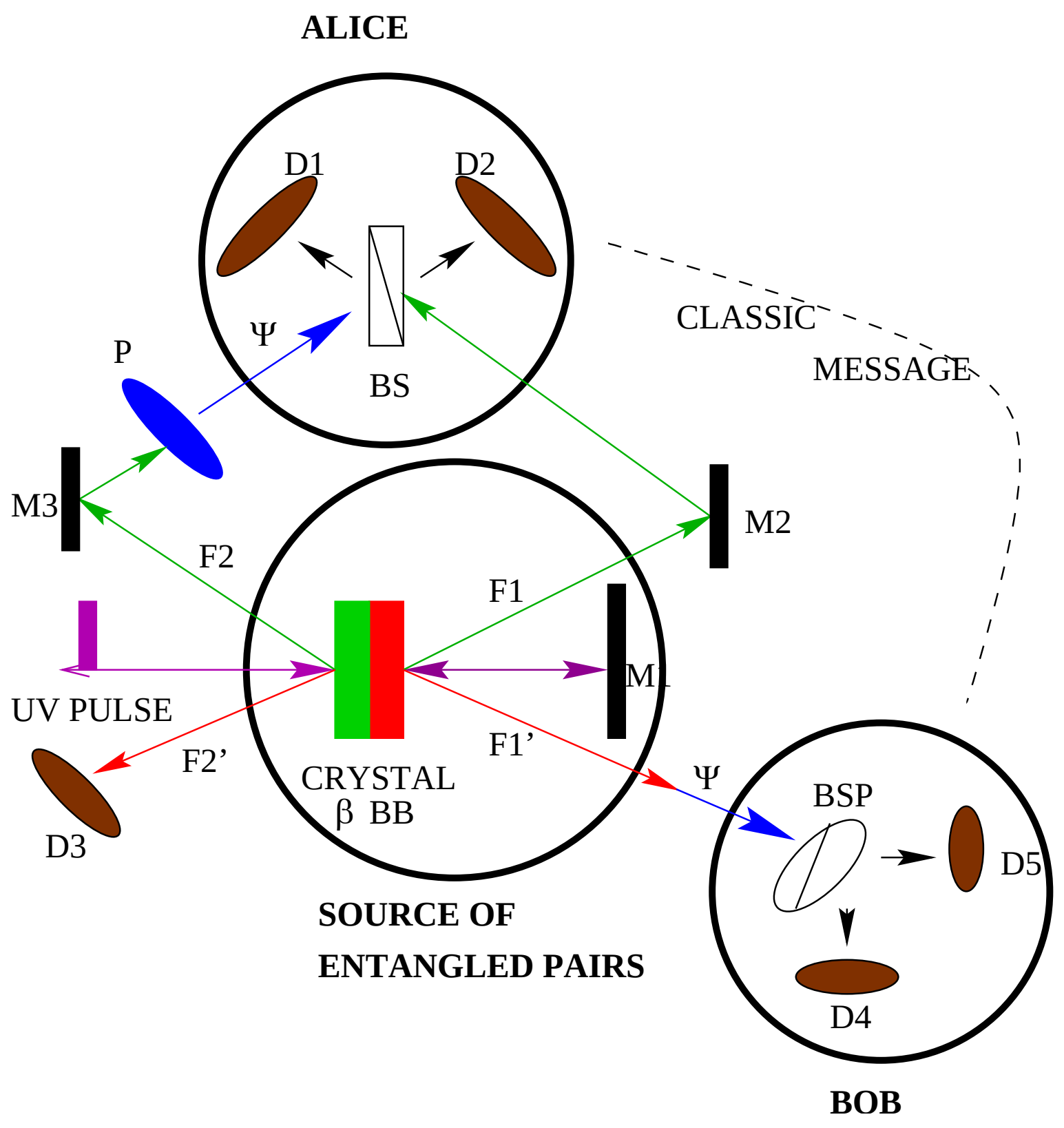


Figure 4: *Quantum teleportation of the polarization state of one photon.*

Quantum information can not be cloned (*no-cloning quantum theorem*), which can limit long-range quantum communications due to decoherence of quantum signals. However, intermediary teleporting stations can save this obstruction.

However, the impossibility of (perfectly) cloning a quantum signal has a positive side: the detection of eavesdroppers and the establishment of reliable quantum communications.

5. Quantum Cryptography

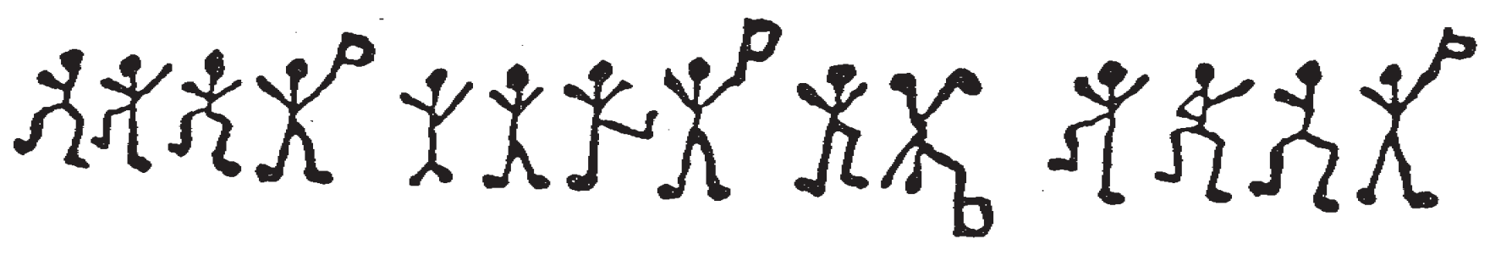


Figure 5: "COME HERE AT ONCE" *(Sherlock Holmes)*

The basic ingredients to encrypt a secret message M are: a key K (known only by the sender, Alice, and the receiver, Bob) and a cryptographic algorithm E that assigns a cryptogram $C = E_K(M)$ to M though K. The decryption process consists in applying the inverse algorithm $M = E_K^{-1}(C)$. For example, the "one-time pad" algorithm assigns a q-digits $C = \{c_1, \ldots, c_q\}$ (with $c_j = 0, \ldots 2^5 - 1$ the alphabet symbols) to $M = \{m_1, \ldots, m_q\}$ though $K = \{k_1, \ldots, k_q\}$ by using the addition $c_j = m_j \oplus k_j$ mod 32. The reliability of this simple cryptographic system is guaranteed as long as the key K is randomly generated and not used more than once. The problem is then when Alice and Bob, who are far apart, run out of keys. How to generate new keys overcoming the presence of eavesdroppers?.

5.1 Secure quantum private key distribution

One possibility is to use entangled pairs. Both can choose the direction of magnetic fields $\vec{H}$: $\uparrow$ or $\rightarrow$, at pleasure. After measuring n pairs, they broadcast the direction choice of $\vec{H}$ each time, but not the answer, which can be: $1 = \uparrow$ or $0 = \downarrow$. In average, they should coincide $n/2$ times in the direction choice, for which the answers are perfectly anti-correlated $(R_A, R_B) = (1,0) \equiv 0$ or $(R_A, R_B) = (0,1) \equiv 1$. Then Alice and Bob keep only these approximately $n/2$ (anti-)correlated answers $(R_A, R_B) = 0, 1$ and construct the key $K = 00101\ldots$ One can prove that (R_A, R_B) are indeed anti-correlated if and only if there has been no eavesdroppers tapping the quantum channel, which can be verified by sacrificing a small part of the key, for high values of n. The reliability of this key distribution algorithm lies in the fact that the observation of eavesdroppers destroys the quantum entanglement. Summarizing: unlike classical communications, *quantum communications detect the presence of eavesdroppers*. Actually, there are prototypes of tens of kilometers long.

5.2 Quantum cracking of public key cryptographic systems

Nowadays, the reliability of the RSA (Rivest, Shamir and Adleman) public key cryptographic system is based on the difficulty of integer factoring on classical computers. The protocol is the following. Alice broadcasts her key, consisting of two big integers (s, c), with $c = pq$ the product of two big prime numbers only known by her. Anyone wanting to send her an encrypted message can do it by computing $C = M^s\,(\mathrm{mod}\,c)$. In order to decrypt the message, Alice uses the formula $M = C^t\,(\mathrm{mod}\,c)$, where $t = t(s,p,q)$ can be calculated from the simple equations: $st \equiv 1\,(\mathrm{mod}\,p-1)$, $st \equiv 1\,(\mathrm{mod}\,q-1)$. Any other eavesdropper who wants to decrypt the message, firstly has to factorize $c = pq$. To make oneself an idea of the difficulty of this operation, for $c \sim 10^{50}$, and with a rough algorithm, we should make the order of $\sqrt{c} \simeq 10^{25}$ divisions. A quite good classical computer capable to perform 10^{10} divisions per second would last 10^{15} seconds in finding p and q. Knowing that the universe is about $3,8{\cdot}10^{17}$ seconds, this discourages any eavesdropper. Actually, there are more efficient algorithms that reduce the computational time, although it keeps exponentially growing with the input size anyway.

P.W. Shor designed an algorithm, to be run on a quantum computer, that factors in polinomial time $t \sim (\log c)^n$, making factoring a tractable problem in the quantum arena and threatening the security of most of business transactions. The efficiency of the algorithm lies in the quantum mechanical resources: entanglement and parallelism.

References

[1] Visit my web page:
www.dmae.upct.es/˜calixto/docencia/doctorado.htm

IWINAC-07, International Work-conference on the Interplay between Natural and Artificial Computation, 18-21 June 2007, La Manga del Mar Menor, Spain