Introduction to Quantum Cryptography

Tommaso Gagliardoni

Università degli Studi di Perugia

September, 12th, 2011

BunnyTN 2011, Trento, Italy

Quantum Mechanics

End of 19th century: unexpected experimental results

Quantum Mechanics: probabilistic physical theory based on an axiomatic mathematical formulation

Von Neumann axiomatization by 4 postulates (we only take into account three in this presentation). Two main consequencies in respect to our concerns:

1. quantum information cannot be copied
2. measurements destroy information

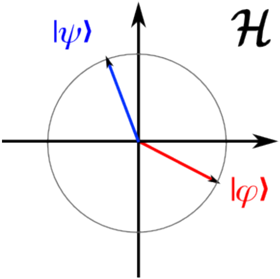
Postulate 1

Physical system $\leftrightsquigarrow$ complex separable Hilbert space $\mathcal{H}$

State of a system $\leftrightsquigarrow$ class of normalized vectors: $|\psi\rangle \in \mathcal{H}$

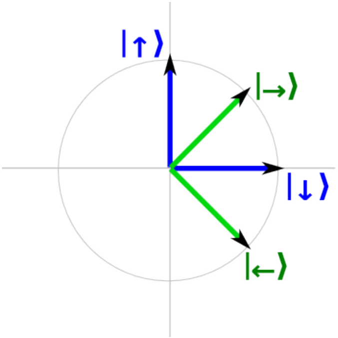
(bra-ket notation)

Most elementary physical system: qubit (space dimension: 2)



Computational bases

Different orthonormal bases can be given, e.g.:



$$|\rightarrow\rangle = \frac{1}{\sqrt{2}}\left(|\downarrow\rangle + |\uparrow\rangle\right)$$

$$|\leftarrow\rangle = \frac{1}{\sqrt{2}}\left(|\downarrow\rangle - |\uparrow\rangle\right)$$

Postulate 2

Conservation of energy: in an isolated system no energy can be created nor destroyed

The No-Cloning Theorem

Landauer's principle: erasing information has an energy cost

Information erased from the system = energy lost by the system

So: quantum information in a closed physical system cannot be erased!

No-Cloning theorem: quantum information cannot be copied

(because to copy information somewhere one must first erase other information to allocate space)

Postulate 3

Physical observable $\leftrightsquigarrow$ Hermitian operator

Possible outcomes of a measurement $\leftrightsquigarrow$ Eigenvalues of the associated observable

Measurement of an observable A on a state $|\psi\rangle$ $\leftrightsquigarrow$ Probabilistic process which causes $|\psi\rangle$ to collapse on an eigenstate of A, with probability depending on $|\psi\rangle$ and A, and produces the corresponding eigenvalue as an outcome

Computational basis in respect to a certain observable A: is an orthonormalized basis of A's eigenvectors

Example

Suppose A has eigenstates $|\uparrow\rangle$ and $|\downarrow\rangle$, with associated eigenvalues 0 and 1

$$Pr_A(0|\,|\uparrow\rangle) = 100\% \rightsquigarrow |\uparrow\rangle$$
$$Pr_A(1|\,|\uparrow\rangle) = 0\% \rightsquigarrow |\uparrow\rangle$$
$$Pr_A(0|\,|\downarrow\rangle) = 0\% \rightsquigarrow |\downarrow\rangle$$
$$Pr_A(1|\,|\downarrow\rangle) = 100\% \rightsquigarrow |\downarrow\rangle$$

recall: $|\rightarrow\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle + |\downarrow\rangle\right)$, while $|\leftarrow\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle - |\downarrow\rangle\right)$

$$Pr_A\left(0|\,|\rightarrow\rangle\right) = 50\% \rightsquigarrow |\uparrow\rangle$$
$$Pr_A\left(1|\,|\rightarrow\rangle\right) = 50\% \rightsquigarrow |\downarrow\rangle$$
$$Pr_A\left(0|\,|\leftarrow\rangle\right) = 50\% \rightsquigarrow |\uparrow\rangle$$
$$Pr_A\left(1|\,|\leftarrow\rangle\right) = 50\% \rightsquigarrow |\downarrow\rangle$$

Measurements

So: measurements can destroy information (because once a state collapses we cannot recover the previous state)

Why?

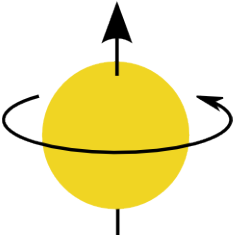
Recall that Postulate 2 claims the impossibility of erasing information for an isolated system.

Performing a measurement involves the interaction of the system with a measurement apparatus: the system is no more isolated!

To observe is to disturb!

Spin

The Spin is a quantized property of elementary particles. It is an observable, with the dimension of a magnetic angular momentum.

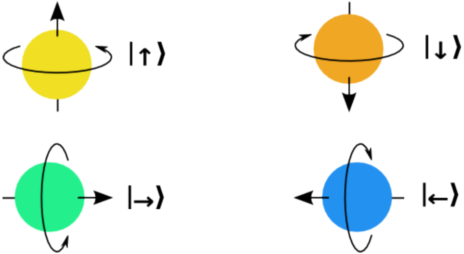


We restrict to so-called spin-$\frac{1}{2}$ particles, whose spin has only two possible values (e.g.: spin up and spin down).

Spin along different directions

Spin can be measured along different coordinate axes: each one is a different observable. These observables do not commute - this means that there is not a basis made of shared eigenvectors of the associated Hermitian operators.

So for, e.g., two axes, we must choose two different computational bases:



Quantum Key Distribution

In Secure Key Distribution two parties want to share a common encryption key over an insecure channel, to be used for subsequent encryption of the communication.

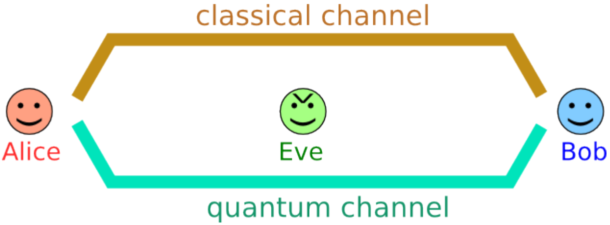
(e.g.: Diffie-Hellmann)

In Quantum Key Distribution (QKD) the goal is the same. The only difference is that in this cenario the two parties are also allowed to share quantum states.

BB84 Protocol - 1/7

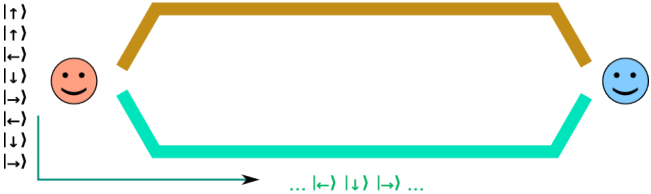
Suppose Alice wants to share a secret key with Bob. They can use both a classical channel (where classical bits are exchanged) or a quantum channel (where qubits are exchanged - e.g., single spin-$\frac{1}{2}$ particles are sent through the channel).

Both channels are insecure, and can be tampered by Eve



First of all, Alice and Bob agree on two different computational bases, e.g.: $(|\uparrow\rangle, |\downarrow\rangle)$ and $(|\leftarrow\rangle, |\rightarrow\rangle)$

Then, Alice chooses a sequence of basis elements picked at random among both bases' elements and sends them to Bob through the quantum channel



BB84 Protocol - 3/7

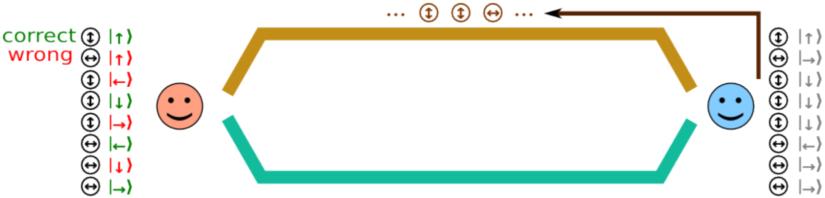
For each qubit received, Bob chooses randomly one of two different measurement instruments (each one measuring either the observable related to the first computational basis or the other one) and performs measurements of the states

(↕) instrument to perform measurements in regard to |↑⟩ and |↓⟩

(↔) instrument to perform measurements in regard to |←⟩ and |→⟩

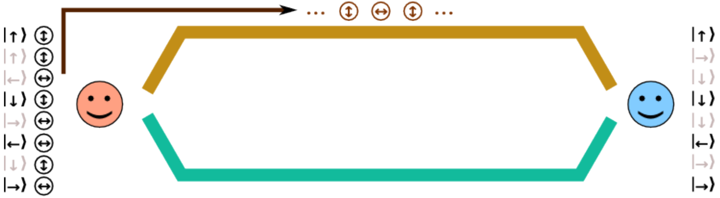
Sometimes Bob chooses the correct instrument, sometimes not, receiving a random outcome

Then, Bob communicates to Alice (using the classical channel) the sequence of instruments he has used. Alice can then infere which of the states she has sent has been observed by Bob with the right instrument (50 % on average)



BB84 Protocol - 5/7

Finally, Alice communicates to Bob (through the classical channel) the right sequence of measurement instruments that had to be used. This allows Bob to know which of the states he measurede were a random outcome, and hence have to be discarded. He and Alice now both know (about) half of the initial sequence, and so they can use this sequence as a shared key to initiate a secure communication.



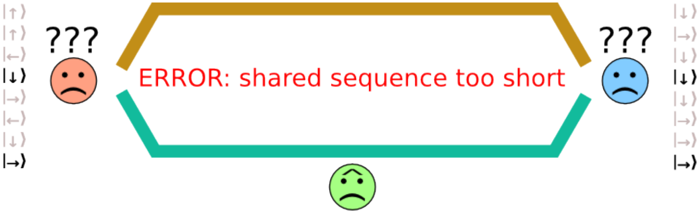
correct sequence: $|\uparrow\rangle$ $|\downarrow\rangle$ $|\leftarrow\rangle$ $|\rightarrow\rangle$

If Eve tries to eavesdrop the communication, she causes a state alteration every time she chooses a wrong measurement instrument (50 % of the times on average). So Bob receives a sequence of states that are already wrong by 50 %

Notice that Eve cannot store a copy of the eavesdropped qubit prior of observing it, because of the no-cloning theorem

BB84 Protocol - 7/7

This means that Alice and Bob will end up with just a 25 % (on average) of correctly shared values, and are then able to spot Eve's presence and abort the communication!



By increasing the number of qubits exchanged, the probability that Eve passes undetected can be made arbitrarily small

BB84 in practice

BB84 has been successfully tested (and is currently used in some high-security bank and military systems), usually using polarized photons over a fibre channel as quantum states.

BB84 is provably, unconditionally secure (as long as QM is correct)

Known attacks to the protocol relies only on implementation issues (e.g.: measurement instruments can be temporarily 'blinded' with strong laser pulses to produce wrong or noisy results)

End of this presentation

Thanks for the attention

tommaso[AT]gagliardoni[DOT]net