Quantum Foundations 5 – Quantum Technologies

Angelo Bassi

Teleportation

We now present the quantum **teleportation prot**ocol. Again, this involves two parties, Alice and Bob, who share an entangled state of two qubits. Alice also has a further qubit in a generic state $|\Psi_T\rangle$, a state that she wants to teleport to Bob, by means of **local measurements and classical communication**.

For a two qubit system, let us introduce the following states:

$$
\begin{aligned}
|\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
|\Phi^-\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\
|\Psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\
|\Psi^-\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)
\end{aligned}
\qquad \longleftrightarrow \qquad
\begin{aligned}
|00\rangle &= \frac{1}{\sqrt{2}}(|\Phi^+\rangle + |\Phi^-\rangle) \\
|01\rangle &= \frac{1}{\sqrt{2}}(|\Psi^+\rangle + |\Psi^-\rangle) \\
|10\rangle &= \frac{1}{\sqrt{2}}(|\Psi^+\rangle - |\Psi^-\rangle) \\
|11\rangle &= \frac{1}{\sqrt{2}}(|\Phi^+\rangle - |\Phi^-\rangle)
\end{aligned}
$$

Bell basis — Computational basis

Assume that the entangled state shared by Alice and Bob is $|\phi^+\rangle$. The total three-qubit state is

$$|\psi_T\rangle|\Phi^+_{AB}\rangle = (\alpha|0_T\rangle + \beta|1_T\rangle)\frac{1}{\sqrt{2}}(|0_A\rangle|0_B\rangle + |1_A\rangle|1_B\rangle)$$

The qubits whose states are labelled by A and T belong to Alice, the one labelled by B belongs to Bob.

The state ca be rewritten as follows:

$$
\begin{aligned}
|\psi_T\rangle|\Phi^+_{AB}\rangle \quad = \quad & \frac{1}{2}\left[|\Phi^+_{TA}\rangle(\alpha|0_B\rangle + \beta|1_B\rangle) + |\Phi^-_{TA}\rangle(\alpha|0_B\rangle - \beta|1_B\rangle)\right. \\
& \left. +|\Psi^+_{TA}\rangle(\alpha|1_B\rangle + \beta|0_B\rangle) + |\Psi^-_{TA}\rangle(\alpha|1_B\rangle - \beta|0_B\rangle)\right]
\end{aligned}
$$

Nothing has changed, we have simply rewritten the state in a different form, by pairing together two states of the two qubits A and T by Alice.

Now assume that **Alice performs a measurement in the Bell basis**; Then with probability 1/4 each, she will find the system in one of the four basis states and the post-measurement state will be

$$
\begin{aligned}
&|\Phi^+_{TA}\rangle(\alpha|0_B\rangle + \beta|1_B\rangle) \\
&|\Phi^-_{TA}\rangle(\alpha|0_B\rangle - \beta|1_B\rangle) \\
&|\Psi^+_{TA}\rangle(\alpha|1_B\rangle + \beta|0_B\rangle) \\
&|\Psi^-_{TA}\rangle(\alpha|1_B\rangle - \beta|0_B\rangle)
\end{aligned}
$$

We note two things. Due to the measurement, **entanglement has been moved** from the AB pair to the AT pair. Bob's qubit is now factorized. At this stage, **Bob cannot recover any piece of information**, because - as the no-signaling theorem has shown - Bob cannot even realize whether or not Alice has performed the measurement.

Given this**, Alice needs to communicate classically with Bob**, in order to tell him what to do in order to recover the state |Ψ>. The sets of orders she sends depend on the outcome of her experiment and are:

$$\begin{array}{lll} \text{Outcome:} & |\Phi^+\rangle & \text{Instruction from Alice to Bob: apply } I \\ \text{Outcome:} & |\Phi^-\rangle & \text{Instruction from Alice to Bob: apply } Z \\ \text{Outcome:} & |\Psi^+\rangle & \text{Instruction from Alice to Bob: apply } X \\ \text{Outcome:} & |\Psi^-\rangle & \text{Instruction from Alice to Bob: apply } Y = ZX \end{array}$$

with

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \sigma_z, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \sigma_x, \quad Y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = i\sigma_y$$

The teleportation protocol is achieved, and after implementing Alice's instructions, Bob's state is:

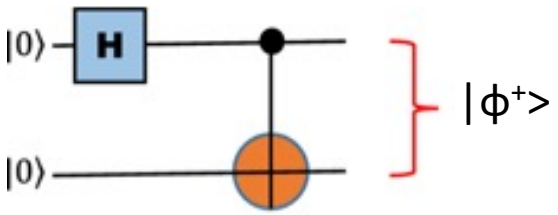
$$|\psi_B\rangle = \alpha|0_B\rangle + \beta|0_B\rangle$$

Some comments:

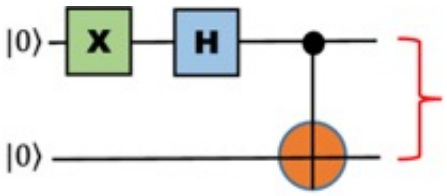
- After teleportation, Alice's initial qubit in the state |Ψ> becomes part of an entangled state. There has been no copying of the state. We will come back on this later.
- No transfer of matter or energy is involved, only the transfer of a state.
- The whole protocol is subluminal, since Alice first needs to measure and then to communicate to Bob. This is a restriction imposed by the no signaling condition (and complies with relativity)
- For every qubit teleported, Alice needs to send Bob two classical bits of information, which cannot carry complete information about the state being teleported. An eavesdropper cannot reconstruct the state |ψ> by eavesdropping the communication between Alice and Bob.

Note the role of the collapse of the wave function in the teleportation protocol, which makes it nonlocal.

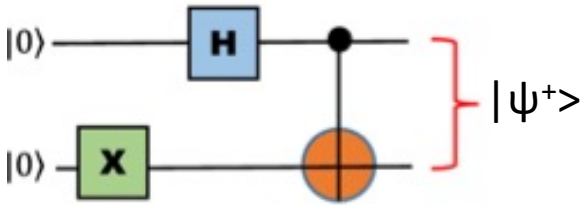
Let's see how the teleportation protocol can be implemented in a quantum computational language. The Bell states can be generated as follows:



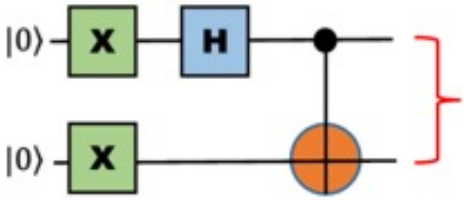
$|\phi^+\rangle$



$|\phi^-\rangle$



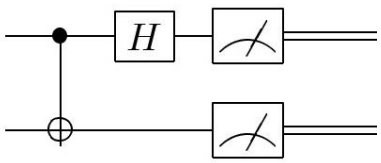
$|\psi^+\rangle$



$|\psi^-\rangle$

And they can be measured as follows

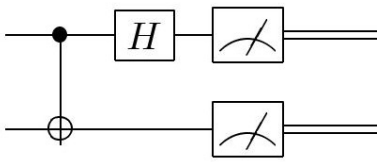
$|\phi^+\rangle$



Outcome $m_1 = 0$

Outcome $m_2 = 0$

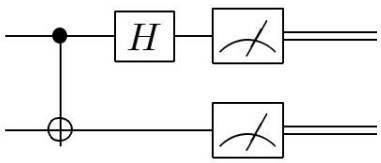
$|\phi^-\rangle$



Outcome $m_1 = 1$

Outcome $m_2 = 0$

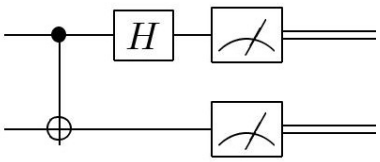
$|\psi^+\rangle$



Outcome $m_1 = 0$

Outcome $m_2 = 1$

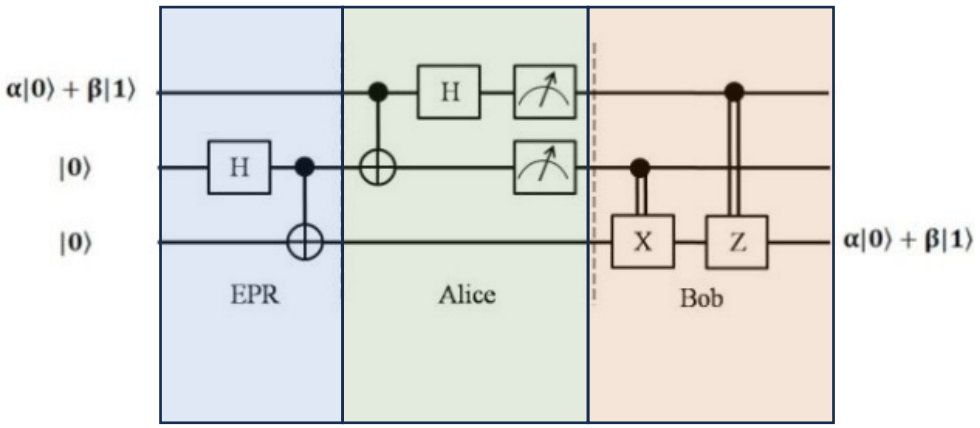
$|\psi^-\rangle$



Outcome $m_1 = 1$

Outcome $m_2 = 1$

This is called a Bell state anlayzer. The circuit for the teleportation protocol is now easy to construct



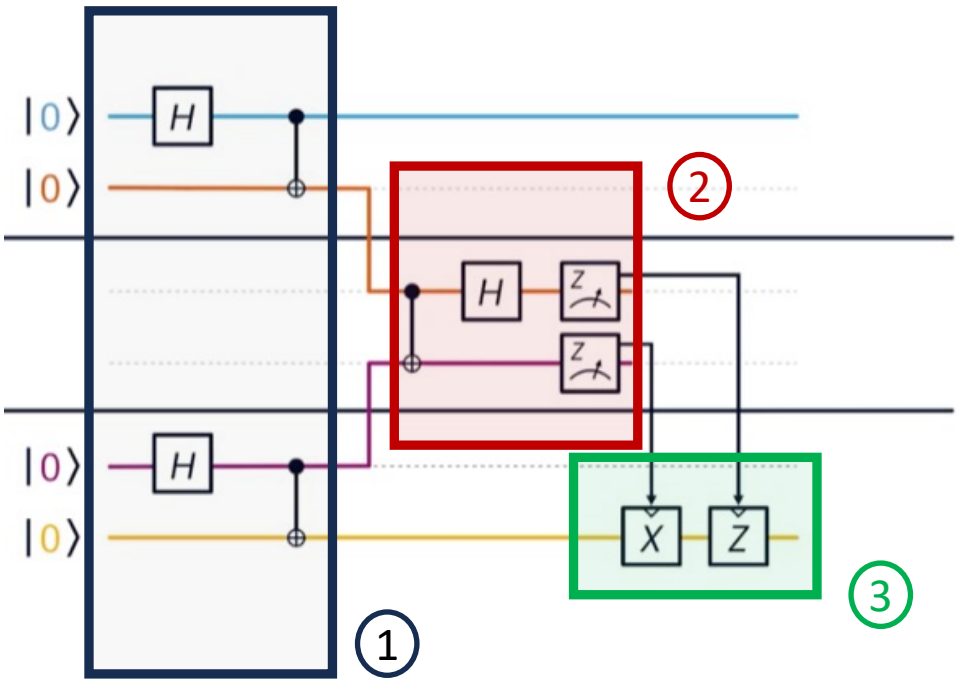
Bell state preparation

Bell state measurement

Classical communication and
Post measurement manipulation

Entanglement swapping

An important operation associated to teleportation is entanglement swapping. First we present the algorithm, then we explain its importance.



1. **Two separate Bell state are prepared**. Keeping the order from top to bottom:

$$\frac{1}{\sqrt{2}}[|00\rangle + |11\rangle]\frac{1}{\sqrt{2}}[|00\rangle + |11\rangle] = \frac{1}{2}[|00\rangle|00\rangle + |00\rangle|11\rangle + |11\rangle|00\rangle + |11\rangle|11\rangle]$$

$$= \frac{1}{2\sqrt{2}}[|0\rangle(|\Phi^+\rangle + |\Phi^-\rangle)|0\rangle + |0\rangle(|\Psi^+\rangle + |\Psi^-\rangle)|1\rangle$$
$$+|1\rangle(|\Psi^+\rangle - |\Psi^-\rangle)|0\rangle + |1\rangle(|\Phi^+\rangle - |\Phi^-\rangle)|1\rangle]$$

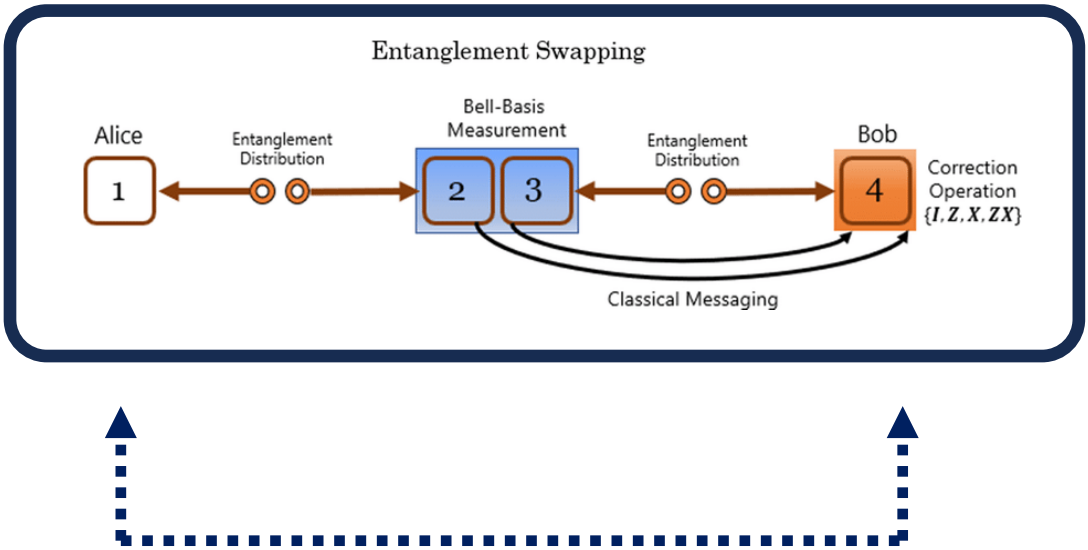
We highlight the two middle qubit in red and put them on the left

$$\frac{1}{\sqrt{2}}[|00\rangle + |11\rangle]\frac{1}{\sqrt{2}}[|00\rangle + |11\rangle] = \frac{1}{2}[|\Phi^+\rangle\Phi^+\rangle + |\Phi^-\rangle|\Phi^-\rangle + |\Psi^+\rangle\Psi^+\rangle + |\Psi^-\rangle\Psi^-\rangle]$$

2. A **Bell state analysis** of the two middle qubits is performed. There are four possible outcomes, all with the same probability 1/4. The two outer qubits will end up in an entangled state perfectly correlated to the outcome of the measurement.

3. Through classical communication of the result, the Bell state is changed into $|\phi^+\rangle$.

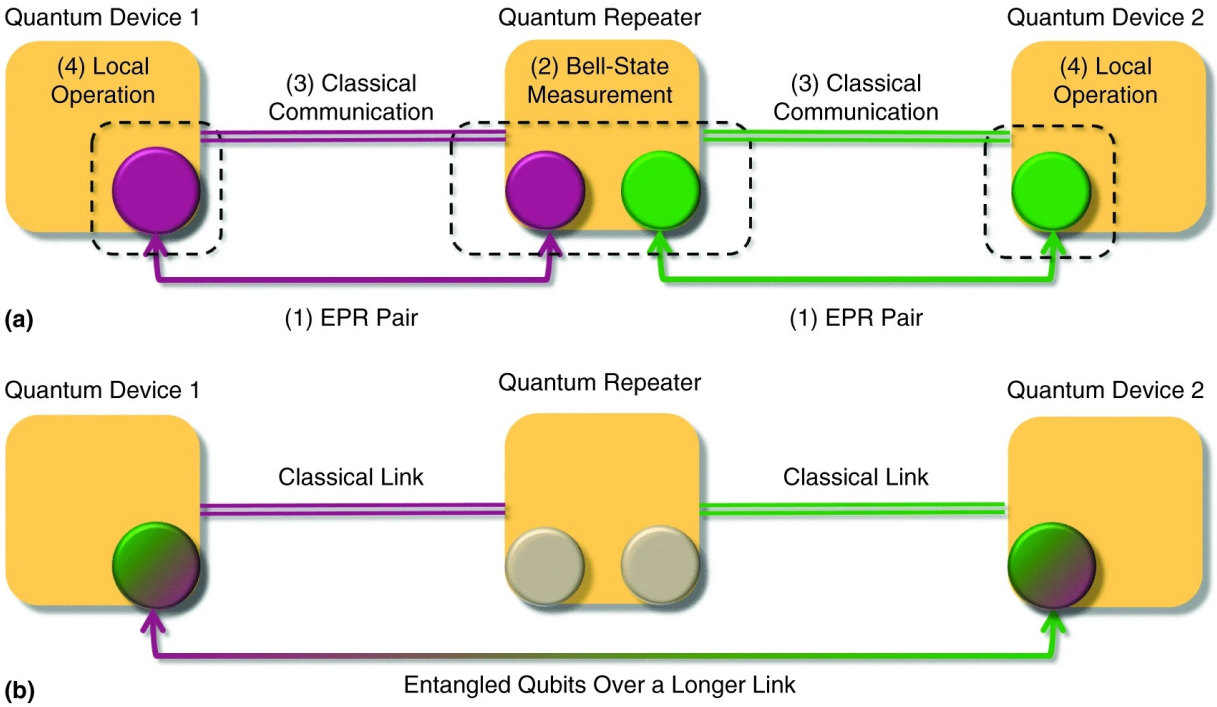
What we have realized is **entanglement swapping**



Now the two are entangled

This forms the basis of the working of a **quantum repeater**

A quantum repeater, as a classical repeater, is meant **to increase the distance** for two parties to share entangled state. Entangled states traveling foe example along optical fibbers, are subject to losses. Currently, maximum distances of hundreds of kilometres can be reached. Quantum repeaters can overcome such losses.



FLASH—A superluminal communicator based upon a new kind of measurement

As usual, there are **Alice and Bob** sharing a **singlet state** and perform distant spin measurements, as in a standard Bell setup.

The bases we will consider are $|\uparrow\rangle$, $|\downarrow\rangle$ and $|+\rangle$, $|-\rangle$.

The FLASH protocol goes as follows.

1. **Alice performs measurements** in one of the two basis indicated above. Bob will receive the opposite state.

↑/↓ measurements. Alices obtains 50% $|\uparrow\rangle$ and 50% $|\downarrow\rangle$. The states Bob receives are 50% $|\downarrow\rangle$ and 50% $|\uparrow\rangle$, respectively.

+/- measurements. Alices obtains 50% $|+\rangle$ and 50% $|-\rangle$. The states Bob receives are 50% $|-\rangle$ and 50% $|+\rangle$, respectively.

2. **Bob amplifies the signal**:

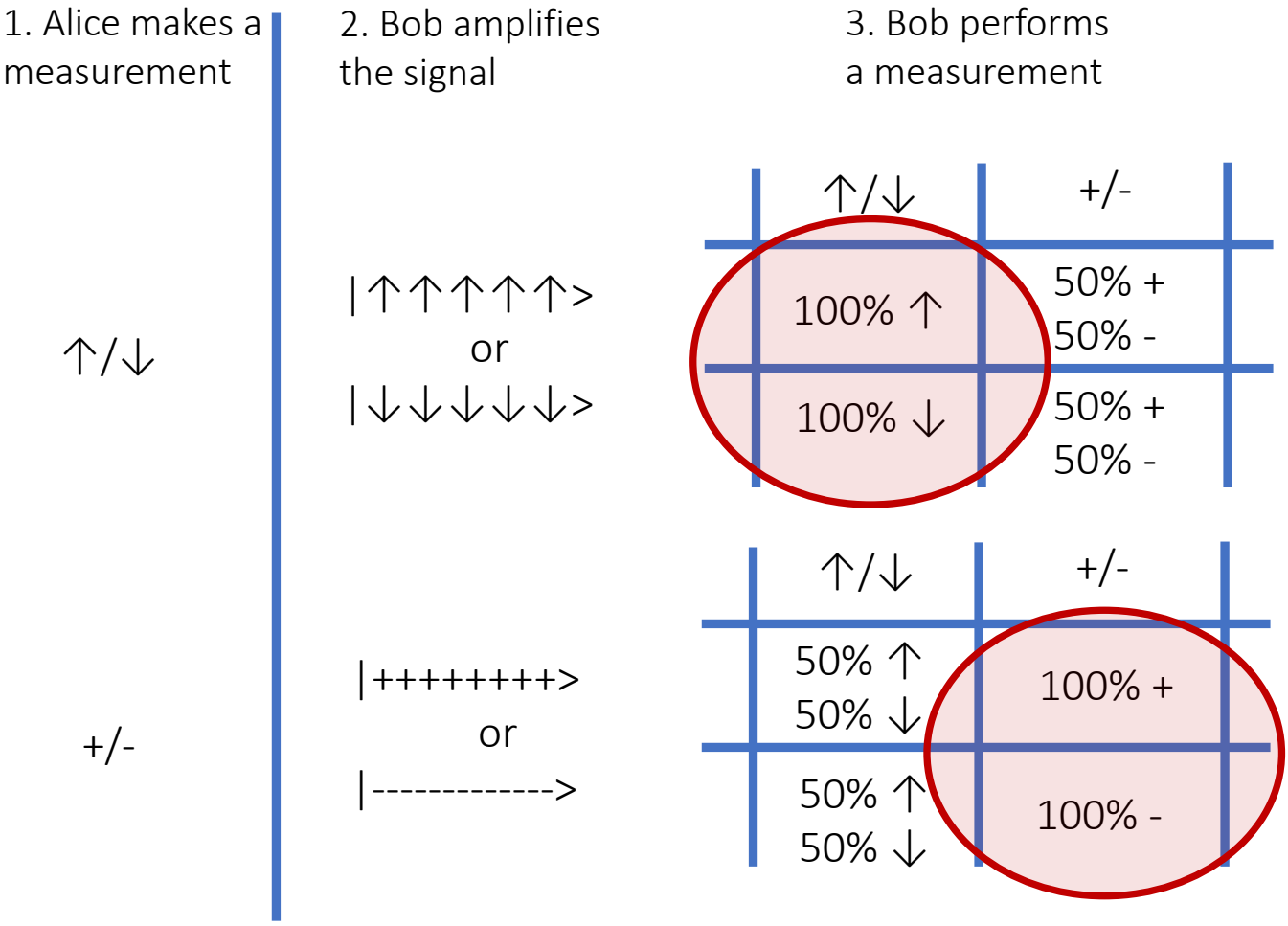
$|\uparrow\rangle \Rightarrow |\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\rangle$
$|\downarrow\rangle \Rightarrow |\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\rangle$

in case Alice makes ↑/↓ measurements.

$|+\rangle \Rightarrow |++++++++++++++++++++\rangle$
$|-\rangle \Rightarrow |--------------------------------\rangle$

in case Alice makes +/- measurements.

3. **Bob divides the states in two subsets**. For half of them he performs a ↑/↓ measurement; for the other half he performs a +/- measurement.



The statistics in the two cases is different. Bon can recover from a distance the type of measurement Alice performed. This forms the basis for a superluminal communication protocol.

The no-cloning theorem

The theorem says that it is not possible to clone an arbitrary quantum state.

Let us consider a unitary operator U such that:

$$U|\psi\rangle \otimes |s\rangle \;\rightarrow\; |\psi\rangle \otimes |\psi\rangle \quad \forall \psi \in \mathscr{H}$$

The state ψ has been duplicated. In particular we have, for two given states:

$$U|\psi_1\rangle \otimes |s\rangle \;\rightarrow\; |\psi_1\rangle \otimes |\psi_1\rangle$$
$$U|\psi_2\rangle \otimes |s\rangle \;\rightarrow\; |\psi_2\rangle \otimes |\psi_2\rangle$$

Then:

$$\langle\psi_1|\psi_2\rangle = \langle\psi_1| \otimes \langle s|s\rangle \otimes |\psi_2\rangle = \langle\psi_1| \otimes \langle s|U^\dagger U|s\rangle \otimes |\psi_2\rangle = \langle\psi_1|\psi_2\rangle^2$$

So we have the equation: $x^2 = x$, whose solution is x = 0,1. This means that the two states ψ_1 and ψ_2 are either the same or orthogonal to each other.

The conclusion is that it is possible to copy orthogonal states, but it is not possible to copy arbitrary non-orthogonal states. This violates the unitarity of quantum evolutions.

Why FLASH does not work

Suppose the machine does the following

$$|\uparrow\rangle \rightarrow |\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\rangle$$
$$|\downarrow\rangle \rightarrow |\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\rangle$$

Then by linearity

$$|+\rangle = \frac{1}{\sqrt{2}}[|\uparrow\rangle + |\downarrow\rangle] \rightarrow \frac{1}{\sqrt{2}}[|\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\rangle + |\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\rangle]$$

$$|-\rangle = \frac{1}{\sqrt{2}}[|\uparrow\rangle - |\downarrow\rangle] \rightarrow \frac{1}{\sqrt{2}}[|\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\rangle - |\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\rangle]$$

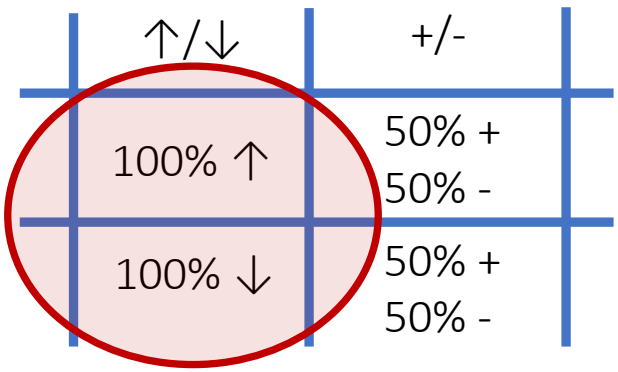
The suppose Alice prepared in the ↑ / ↓ so that Bob's machine generates

$$|\uparrow\rangle \rightarrow |\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\rangle$$
$$|\downarrow\rangle \rightarrow |\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\rangle$$

Bob divides the set un two subsets. For half of them he performs a ↑ / ↓ measurement; for the other half he performs a +/- measurement.

The statistics is

$|\uparrow\uparrow\uparrow\uparrow\uparrow\rangle$
or
$|\downarrow\downarrow\downarrow\downarrow\downarrow\rangle$



The suppose Alice prepared in the +/− so that Bob's machine generates

$$|+\rangle = \frac{1}{\sqrt{2}}[|\uparrow\rangle + |\downarrow\rangle] \rightarrow \frac{1}{\sqrt{2}}[|\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\rangle + |\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\rangle]$$

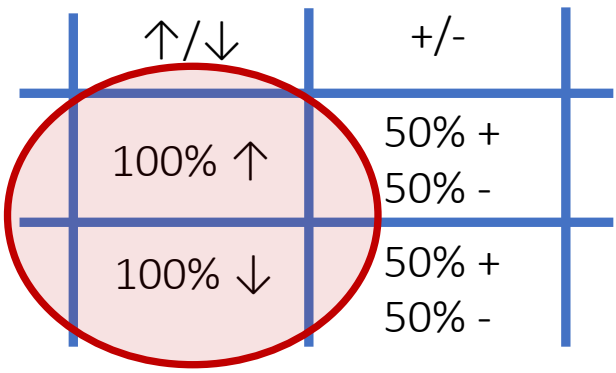
$$|-\rangle = \frac{1}{\sqrt{2}}[|\uparrow\rangle - |\downarrow\rangle] \rightarrow \frac{1}{\sqrt{2}}[|\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\rangle - |\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\rangle]$$

The statistics is

$$\frac{1}{\sqrt{2}}[|\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\rangle + |\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\rangle]$$

or

$$\frac{1}{\sqrt{2}}[|\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\rangle - |\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\rangle]$$



The two statistics are equivalent: **Bob cannot distinguish the two cases**

Exercise: Repeat the calculation assuming that Bob's machine does the following

$$|+\rangle \rightarrow |++++++++++\rangle$$

$$|-\rangle \rightarrow |----------\rangle$$

Secure communication

Classical cryptography can be divided into two major branches; **secret or symmetric key cryptography** and **public key cryptography,** which is also known as **asymmetric cryptography**.

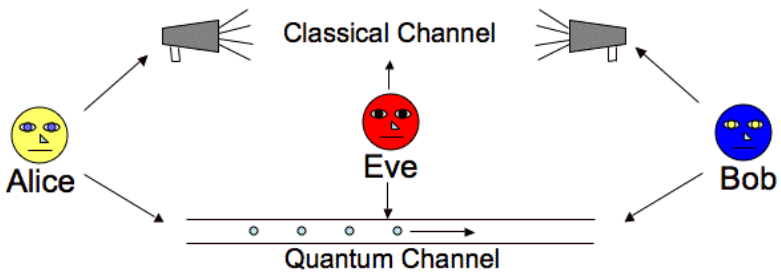
Secret key cryptography represents the most traditional form of cryptography in which two parties both encrypt and decrypt their messages using the **same shared secret key**. While some secret key schemes, such as one-time pads, are **perfectly secure** against an attacker with arbitrary computational power, they have the **major practical disadvantage** that before two parties can communicate securely they must somehow establish a secret key.

In order to establish a secret key over an insecure channel, **key distribution schemes** based on public key cryptography, such as Diffie-Hellman, are typically employed.

In contrast to secret key cryptography, a shared secret key does not need to be established prior to communication in **public key cryptography**. Instead **each party has a private key**, which remains secret, **and a public key**, which they may distribute freely. If one party, say Alice, wants to send a message to another party, Bob, **she would encrypt her message with Bob's public key after which only Bob could decrypt the message using his private key**. While there is no need for key exchange, the security of public key cryptography algorithms are currently all based on the **unproven assumption of the difficulty of certain problems** such as integer factorization or the discrete logarithm problem. This means that **public key cryptography algorithms are potentially vulnerable** to improvements in computational power or the discovery of efficient algorithms to solve their underlying problems. Indeed algorithms have already been proposed to perform both integer factorization and solve the discrete logarithm problem in polynomial time on a quantum computer.

QKD – Quantum Key Distribution

The basic model for Quantum Key Distribution (QKD) protocols involves two parties, referred to as Alice and Bob, wishing to exchange a key both with access to a classical public communication channel and a quantum communication channel. This is shown in the figure.



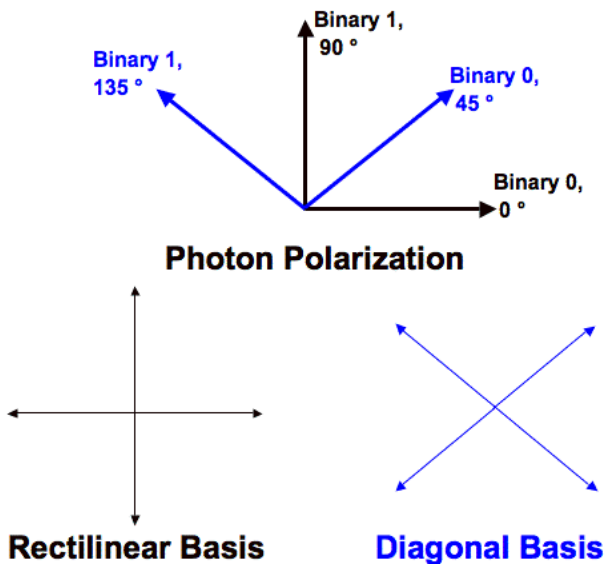
An eavesdropper, called Eve, is assumed to have access to both channels and no assumptions are made about the resources at her disposal. With this basic model established, we describe in layman's terms the necessary quantum principles needed to understand the QKD protocols.

QKD – The BB84 protocol

The Figure shows how a bit can be encoded in the polarization state of a photon in BB84.

We define a binary 0 as a polarization of 0 degrees in the rectilinear bases or 45 degrees in the diagonal bases. Similarly a binary 1 can be 90 degrees in the rectilinear bases or 135 in diagonal bases.

Thus a bit can be represented by polarizing the photon in either one of two bases.



The protocol is (a variation of) the following

1. Alice begins by choosing a random string of bits.

2. For each bit, Alice will randomly choose a basis, rectilinear or diagonal, to use to encode the bit.

3. She will transmit a photon for each bit with the corresponding polarization, as just described, to Bob.

4. Bob also chooses a random basis.

5. For every photon Bob receives, he will measure the photon's polarization in the chosen basis. If, for a particular photon, Bob chose the same basis as Alice, then in principle, Bob should measure the same polarization and thus he can correctly infer the bit that Alice intended to send.

6. Bob will notify Alice over any insecure channel what basis he used to measure each photon. Alice will report back to Bob whether he chose the correct basis for each photon.

7. Alice and Bob will discard the bits corresponding to the photons which Bob measured with a different basis. On the average, only half of the photons have to be disregarded. Provided no errors occurred or no one manipulated the photons, Bob and Alice should now both have an identical string of bits which is called a sifted key.

1	Alice's bit	0	1	1	0	1	0	0	1
2	Alice's basis	+	+	X	+	X	X	X	+
3	Alice's polarization	↑	→	↖	↑	↖	↗	↗	→
4	Bob's basis	+	X	X	X	+	X	+	+
5	Bob's measurement	↑	↗	↖	↗	→	↗	→	→
6	Public discussion								
7	Shared Secret key	0		1			0		1

The role of Eve

Assume that Eve tries to intercept the basis. She will do that by measuring the photon's state. In this way, she will introduce an error with probability 25%

A sends bit 0 in basis +	The best Eve can do is:		Bob mesures in basis +
	50% +: outcome 0	⟶	Outcome 0
	50% x: outcome 0 or 1	⟶	50 % 0 and 50% 1

So 25% of the times Bob gets a different result from Alice, in spite they have measured in the same basis.

If now Alice and Bob publicly compare n bits (then disregarding them as key bits, since they are no longer secret) the probability of finding a disagreement is

$\mathbb{P}_D^{(n)} = 1 - (3/4)^n$ (where 3/4 is the probability that they all match)

Then for n = 72: $\mathbb{P}_D^{(n)} = 0{,}999999999$ (nine 9)

Almost immediately Alice and Bob realize that Eve tried to copy the key and abort the operation of key distribution.

In general, if there are too many errors when comparing the bits, the quantum channel in considered insecure and the protocol is aborted.

QKD – The E91 protocol

This protocol makes specific use of entanglement

1. Alice and Bob share an entangled state, specifically the state $|\phi^+\rangle$.

2. Alice makes a measurement with a direction randomly chosen between $\{0, \pi/8 , \pi/4\}$, whereas Bob makes a measurement with a direction randomly chosen between $\{-\pi/8 , 0, \pi/8\}$. They record the measurement result and broadcast the measurement basis which they used, through the classical channel.

3. Thus, Alice and Bob now know each other's choice. They divide the measurement result into two groups: one is the decoy qubits G_1 where they choose different measurement basis and another is the raw key qubits G_2 where they choose the same measurement basis.

4. The group G_1 is used to detect whether there is an eavesdropping. To detect eavesdropping, they can compute the test statistic S using the correlation coefficients between Alice's bases and Bob's, similar to that shown in the Bell test experiments. If there is an error in the value of S, which means that there is also a eavesdropper, Alice and Bob will conclude that the quantum channel is not safe, and they will interrupt this communication and start a new one.

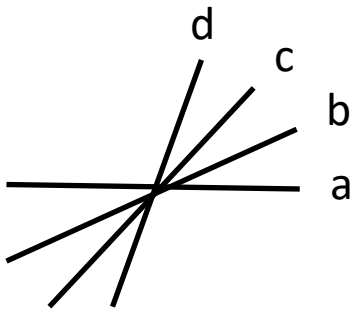
5. If the quantum channel is safe, G_2 can be used as the raw keys because Alice and Bob can receive the same measurements. Both Alice and Bob agree on that the measurement $|0\rangle$ represents the classical bit 0, while the measurement $|1\rangle$ represents the classical bit 1, and thus get their key string.

Note: The choice of direction is different from that considered before when presenting Bell's theorem, because now we are referring to photon polarization in the $|\phi^+\rangle$ state, while before we were referring to the singlet state of spins. In the present case we have

$$\mathbb{P}_{\rm QM}(++|\mathbf{a},\mathbf{b},\psi) \;=\; \mathbb{P}_{\rm QM}(--|\mathbf{a},\mathbf{b},\psi) = \frac{1}{2}\cos^2\theta$$
$$\mathbb{P}_{\rm QM}(+-|\mathbf{a},\mathbf{b},\psi) \;=\; \mathbb{P}_{\rm QM}(-+|\mathbf{a},\mathbf{b},\psi) = \frac{1}{2}\sin^2\theta$$

and

$$E_{\rm QM}(\mathbf{a},\mathbf{b}|\psi) = \cos 2\theta$$



And, for a choice of directions like in the figure

$$|E_{QM}(\mathbf{a},\mathbf{b}) - E_{QM}(\mathbf{a},\mathbf{d})| + |E_{QM}(\mathbf{c},\mathbf{b}) + E_{QM}(\mathbf{c},\mathbf{d})| =$$
$$= |\cos 2\theta_{\mathbf{a},\mathbf{b}} - \cos 2\theta_{\mathbf{a},\mathbf{d}}| + |\cos 2\theta_{\mathbf{c},\mathbf{b}} + \cos 2\theta_{\mathbf{c},\mathbf{d}}|$$
$$= |\cos 2\theta - \cos 6\theta| + 2|\cos 2\theta|$$

For θ = π/8 we have

$$|\cos 2\theta - \cos 6\theta| + 2|\cos 2\theta| = 2\sqrt{2} > 2$$

The inequality is violated.