Quantum Nonlocality and Special Relativity

No signalling theorem

Quantum nonlocality cannot be used to send information faster than the speed of light. Actually measurements cannot send information at all

We have two systems A and B, which in general share an entangled state ρ_{AB}. They are apart from each other.

Arbitrary measurements can be performed on each of them

No signalling theorem

Alice performs a measurement of an observable Â with eigen-projectors P_n^A. The state at Bob's side changes to:

$$\rho_{AB} \;\to\; \rho'_{AB} \;=\; \sum_n \mathbf{Tr}[(P_n^A \otimes I^B)\rho_{AB}] \frac{(P_n^A \otimes I^B)\rho_{AB}(P_n^A \otimes I^B)}{\mathbf{Tr}[(P_n^A \otimes I^B)\rho_{AB}]} \;=\; \sum_n (P_n^A \otimes I^B)\rho_{AB}(P_n^A \otimes I^B)$$

Born rule

Von Neumann collapse

Then the average value of measurements Bob performs are given by:

No signalling theorem

$$\langle O^B \rangle' \;=\; \mathbf{Tr}[(I^A \otimes O^B)\rho'_{AB}] \;=\; \sum_n \mathbf{Tr}[(I^A \otimes O^B)(P_n^A \otimes I^B)\rho_{AB}(P_n^A \otimes I^B)]$$

Cyclicity of trace

$$= \sum_n \mathbf{Tr}[(I^A \otimes O^B)(P_n^A \otimes I^B)^2 \rho_{AB}]$$

Idempotent

$$= \sum_n \mathbf{Tr}[(I^A \otimes O^B)(P_n^A \otimes I^B)\rho_{AB}]$$

Linearity of trace +
Projectors sum to 1

$$= \mathbf{Tr}[(I^A \otimes O^B)\rho_{AB}] \;=\; \langle O^B \rangle$$

The value Bob gets is the same before and after Alice's measurement

No signalling theorem

Bob does not see any difference in the statistics of the outcomes of his measurements. There is no quantum operation (= unitary evolution or measurement) Alice can do, that allows her to send information to Bob.

If one looks at the reason why it is so, it ultimately rests on the fact that

$$\rho_{AB} \;\to\; \rho'_{AB} \;=\; \sum_n \underbrace{\mathrm{Tr}[(P_n^A \otimes I^B)\rho_{AB}]}_{\text{Born rule}} \underbrace{\frac{(P_n^A \otimes I^B)\rho_{AB}(P_n^A \otimes I^B)}{\mathrm{Tr}[(P_n^A \otimes I^B)\rho_{AB}]}}_{\text{Von Neumann collapse}} \;=\; \sum_n (P_n^A \otimes I^B)\rho_{AB}(P_n^A \otimes I^B)$$

In measurements, the Born rule and the von Neumann collapse are just the right recipes that avoid superluminal communication

Teleportation

The teleportation protocol begins with a quantum state or qubit $|\psi\rangle$, in Alice's possession, that she wants to convey to Bob. This qubit can be written generally, in bra–ket notation, as:

$$|\psi\rangle_C = \alpha|0\rangle_C + \beta|1\rangle_C.$$

The subscript C above is used only to distinguish this state from A and B, below.

Next, the protocol requires that Alice and Bob share a maximally entangled state. This state is fixed in advance, by mutual agreement between Alice and Bob, and can be any one of the four Bell states shown. It does not matter which one.

$$|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B),$$

$$|\Psi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B + |1\rangle_A \otimes |0\rangle_B),$$

$$|\Psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B).$$

$$|\Phi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B - |1\rangle_A \otimes |1\rangle_B),$$

In the following, assume that Alice and Bob share the state $|\Phi^+\rangle_{AB}$. Alice obtains one of the particles in the pair, with the other going to Bob. (This is implemented by preparing the particles together and shooting them to Alice and Bob from a common source.) The subscripts A and B in the entangled state refer to Alice's or Bob's particle.

Teleportation

At this point, Alice has two particles (C, the one she wants to teleport, and A, one of the entangled pair), and Bob has one particle, B. In the total system, the state of these three particles is given by

$$|\psi\rangle_C \otimes |\Phi^+\rangle_{AB} = (\alpha|0\rangle_C + \beta|1\rangle_C) \otimes \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B).$$

Alice will then make a local measurement in the Bell basis (i.e. the four Bell states) on the two particles in her possession. To make the result of her measurement clear, it is best to write the state of Alice's two qubits as superpositions of the Bell basis. This is done by using the following general identities, which are easily verified:

$$|0\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}(|\Phi^+\rangle + |\Phi^-\rangle),$$

$$|0\rangle \otimes |1\rangle = \frac{1}{\sqrt{2}}(|\Psi^+\rangle + |\Psi^-\rangle),$$

$$|1\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}(|\Psi^+\rangle - |\Psi^-\rangle),$$

$$|1\rangle \otimes |1\rangle = \frac{1}{\sqrt{2}}(|\Phi^+\rangle - |\Phi^-\rangle).$$

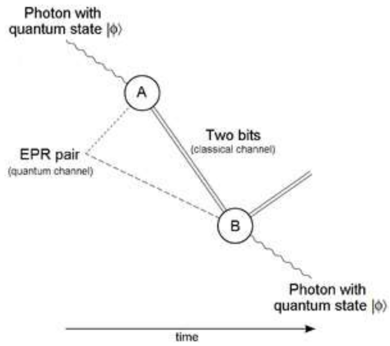


Diagram for quantum teleportation of a photon

Teleportation

One applies these identities with A and C subscripts. The total three particle state, of A, B and C together, thus becomes the following four-term superposition:

$$|\psi\rangle_C \otimes |\Phi^+\rangle_{AB} =$$
$$\frac{1}{2}\Big[|\Phi^+\rangle_{CA} \otimes (\alpha|0\rangle_B + \beta|1\rangle_B) + |\Phi^-\rangle_{CA} \otimes (\alpha|0\rangle_B - \beta|1\rangle_B)$$ [38]
$$+ |\Psi^+\rangle_{CA} \otimes (\alpha|1\rangle_B + \beta|0\rangle_B) + |\Psi^-\rangle_{CA} \otimes (\alpha|1\rangle_B - \beta|0\rangle_B)\Big].$$

The above is just a change of basis on Alice's part of the system. No operation has been performed and the three particles are still in the same total state. The actual teleportation occurs when Alice measures her two qubits A,C, in the Bell basis

$$|\Phi^+\rangle_{CA}, |\Phi^-\rangle_{CA}, |\Psi^+\rangle_{CA}, |\Psi^-\rangle_{CA}.$$

Experimentally, this measurement may be achieved via a series of laser pulses directed at the two particles. Given the above expression, evidently the result of Alice's (local) measurement is that the three-particle state would collapse to one of the following four states (with equal probability of obtaining each):

- $|\Phi^+\rangle_{CA} \otimes (\alpha|0\rangle_B + \beta|1\rangle_B)$
- $|\Phi^-\rangle_{CA} \otimes (\alpha|0\rangle_B - \beta|1\rangle_B)$
- $|\Psi^+\rangle_{CA} \otimes (\alpha|1\rangle_B + \beta|0\rangle_B)$
- $|\Psi^-\rangle_{CA} \otimes (\alpha|1\rangle_B - \beta|0\rangle_B)$

Teleportation

- $|\Phi^+\rangle_{CA} \otimes (\alpha|0\rangle_B + \beta|1\rangle_B)$
- $|\Phi^-\rangle_{CA} \otimes (\alpha|0\rangle_B - \beta|1\rangle_B)$
- $|\Psi^+\rangle_{CA} \otimes (\alpha|1\rangle_B + \beta|0\rangle_B)$
- $|\Psi^-\rangle_{CA} \otimes (\alpha|1\rangle_B - \beta|0\rangle_B)$

Alice's two particles are now entangled to each other, in one of the four Bell states, and the entanglement originally shared between Alice's and Bob's particles is now broken. Bob's particle takes on one of the four superposition states shown above. Note how Bob's qubit is now in a state that resembles the state to be teleported. The four possible states for Bob's qubit are unitary images of the state to be teleported.

The result of Alice's Bell measurement tells her which of the above four states the system is in. She can now send her result to Bob through a classical channel. Two classical bits can communicate which of the four results she obtained.

Teleportation

After Bob receives the message from Alice, he will know which of the four states his particle is in. Using this information, he performs a unitary operation on his particle to transform it to the desired state $\alpha|0\rangle_B + \beta|1\rangle_B$:

- If Alice indicates her result is $|\Phi^+\rangle_{CA}$, Bob knows his qubit is already in the desired state and does nothing. This amounts to the trivial unitary operation, the identity operator.
- If the message indicates $|\Phi^-\rangle_{CA}$, Bob would send his qubit through the unitary quantum gate given by the Pauli matrix

$$\sigma_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

to recover the state.

- If Alice's message corresponds to $|\Psi^+\rangle_{CA}$, Bob applies the gate

$$\sigma_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

to his qubit.

- Finally, for the remaining case, the appropriate gate is given by

$$\sigma_3\sigma_1 = -\sigma_1\sigma_3 = i\sigma_2 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

Teleportation is thus achieved. The above-mentioned three gates correspond to rotations of π radians (180°) about appropriate axes (X, Y and Z) in the Bloch sphere picture of a qubit.

Teleportation

Some remarks:

- After this operation, Bob's qubit will take on the state $|\psi\rangle_B = \alpha|0\rangle_B + \beta|1\rangle_B$, and Alice's qubit becomes an (undefined) part of an entangled state. Teleportation does not result in the copying of qubits, and hence is consistent with the no cloning theorem.
- There is no transfer of matter or energy involved. Alice's particle has not been physically moved to Bob; only its state has been transferred. The term "teleportation", coined by Bennett, Brassard, Crépeau, Jozsa, Peres and Wootters, reflects the indistinguishability of quantum mechanical particles.
- For every qubit teleported, Alice needs to send Bob two classical bits of information. These two classical bits do not carry complete information about the qubit being teleported. If an eavesdropper intercepts the two bits, she may know exactly what Bob needs to do in order to recover the desired state. However, this information is useless if she cannot interact with the entangled particle in Bob's possession.

Role of the collapse of the wave function in the process
Role of classical communication (teleportation protocol is subluminal)

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 basis 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.

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

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

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

2. Bob amplifies the signal:

$$|\uparrow\rangle \to |\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\rangle$$
$$|\downarrow\rangle \to |\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\rangle$$

in case Alice makes $\uparrow / \downarrow$ measurements.

$$|+\rangle \to |+++++++++\rangle$$
$$|-\rangle \to |---------\rangle$$

in case Alice makes +/- measurements.

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

3. Bob divides the states in two subsets. For half of them he performs a $\uparrow / \downarrow$ measurement; for the other half he performs a +/- measurement.

In case Alice made $\uparrow / \downarrow$ measurements:

$|\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\rangle$

$|\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\rangle$

Half to $\uparrow / \downarrow$: 100% $|\uparrow\rangle$ or 100% $|\downarrow\rangle$

Half to $+/-$: 50% $|+\rangle$ and 50% $|-\rangle$

In case Alice made $+/-$ measurements:

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

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

Half to $\uparrow / \downarrow$: 50% $|\uparrow\rangle$ and 50% $|\downarrow\rangle$

Half to $+/-$: 100% $|+\rangle$ or 100% $|-\rangle$

Bob can understand what Alice measured. Faster than light

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:

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

The No Cloning Theorem

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 ont possible to copy arbitrary non-orthogonal states. This violates the unitarity of quantum evolutions.

How the No-Cloning Theorem Got its Name

Asher Peres
Department of Physics,
Technion—Israel Institute of Technology,
32000 Haifa, Israel

February 1, 2008

This is the story of my own personal contribution to the no-cloning theorem, made public for the first time after more than twenty years. Early in 1981, the editor of *Foundations of Physics* asked me to be a referee for a manuscript by Nick Herbert, with title "*FLASH*—A superluminal communicator based upon a new kind of measurement." It was obvious to me that the paper could not be correct, because it violated the special theory of relativity. However I was sure this was also obvious to the author. Anyway, nothing in the argument had any relation to relativity, so that the error had to be elsewhere.

I recommended to the editor of *Foundations of Physics* that this paper be published [5]. I wrote that it was obviously wrong, but I expected that it would elicit considerable interest and that finding the error would lead to significant progress in our understanding of physics. Soon afterwards, Wootters and Zurek [1] and Dieks [2] published, almost simultaneously, their versions of the no-cloning theorem. The tantalizing title "A single quantum cannot be cloned" was contributed by John Wheeler. How the present paper got its name is another story [6].

There was another referee, GianCarlo Ghirardi, who recommended to reject Herbert's paper. His anonymous referee's report contained an argument which was a special case of the theorem in references [1, 2]. Perhaps Ghirardi thought that his objections were so obvious that they did not deserve to be published in the form of an article (he did publish them the following year [7]). Other objections were raised by Glauber [8], and then by many other authors whom I am unable to cite, because of space limitations.

With some hindsight, it is now clear that the no-cloning interdiction was implicitly used by Stephen Wiesner in his seminal paper *Conjugate Coding* which was submitted circa 1970 to IEEE Transactions on Information Theory, and promptly rejected because it was written in a jargon incomprehensible to computer scientists (this actually was a paper about physics, but it had been submitted to a computer science journal). Wiesner's work was finally published in its original form in 1983 [9] in the newsletter of ACM SIGACT (Association for Computing Machinery, Special Interest Group in Algorithms and Computation Theory). Another early article, *Unforgeable Subway Tokens* [10], also tacitly assumes that exact duplication of a quantum state is impossible. As it often happens in science, these things were well known to those who know things well.

Why FLASH does not work

Suppose the machine does the following

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

Then by linearity

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

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

Why FLASH does not work

The suppose Alice prepared in the $\uparrow / \downarrow$ so that Bob's machine generates

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

Bob divides the set un two subsets. For half of them he performs a $\uparrow / \downarrow$ measurement; for the other half he performs a +/- measurement.

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

$\Rightarrow$

Half to $\uparrow / \downarrow$: 100% $|\uparrow\rangle$ or 100% $|\downarrow\rangle$
Half to $+/-$: 50% $|+\rangle$ and 50% $|-\rangle$

Why FLASH does not work

The suppose Alice prepared in the $\uparrow / \downarrow$ so that Bob's machine generates

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

Bob divides the set un two subsets. For half of them he performs a $\uparrow / \downarrow$ measurement; for the other half he performs a +/- measurement.

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

$\Rightarrow$

Half to $\uparrow / \downarrow$: 100% $|\uparrow\rangle$ or 100% $|\downarrow\rangle$
Half to $+/-$: 50% $|+\rangle$ and 50% $|-\rangle$

Why FLASH does not work

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

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

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

Bob divides the set un two subsets. For half of them he performs a $\uparrow / \downarrow$ measurement; for the other half he performs a +/- measurement. It is evident that as soon as he performs a $\uparrow / \downarrow$ measurement on the first system, the whole state collapses to

50% $|\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\rangle$ 50% $|\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\rangle$

Therefore the same statistics as in the previous case is recovered

Why FLASH does not work

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

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

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

Cryptography

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.

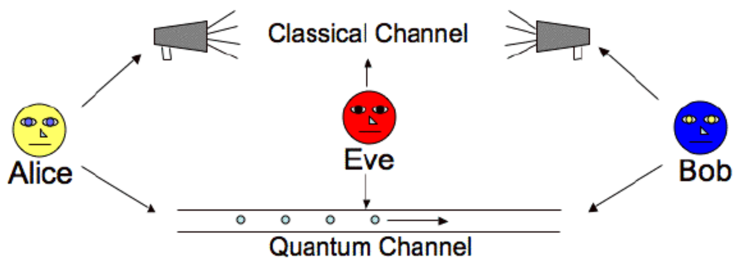
In order to establish a secret key over an insecure channel, **key distribution schemes** based on public key cryptography, such as Diffie-Hellman, are typically employed.

Cryptography

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

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.

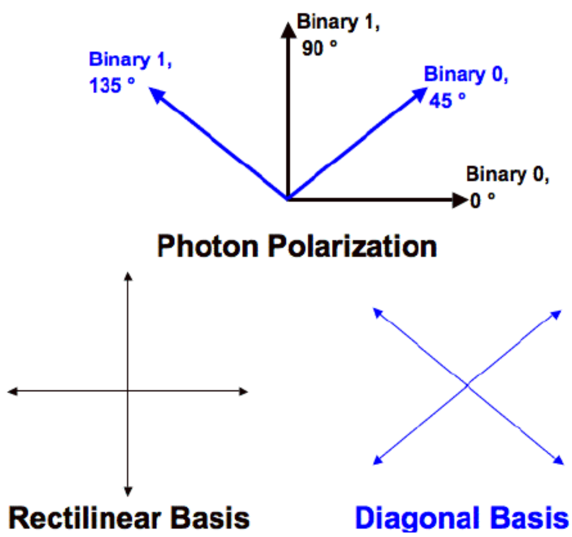


QKD - BB84

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.



QKD - BB84

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

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

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

4. For every photon Bob receives, he will measure the photon's polarization by a randomly 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. If he chose the wrong basis, his result, and thus the bit he reads, will be random.

QKD - BB84

5. 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.

6. Alice and Bob will discard the bits corresponding to the photons which Bob measured with a different basis. <u>On the average, only half of the photons have to be disregarded.</u> 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.

QKD - BB84

Alice's bit	0	1	1	0	1	0	0	1
Alice's basis	+	+	X	+	X	X	X	+
Alice's polarization	↑	→	↖	↑	↖	↗	↗	→
Bob's basis	+	X	X	X	+	X	+	+
Bob's measurement	↑	↗	↖	↗	→	↗	→	→
Public discussion								
Shared Secret key	0		1			0		1

QKD - BB84 - 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.

QKD - BB84 - Eve

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)

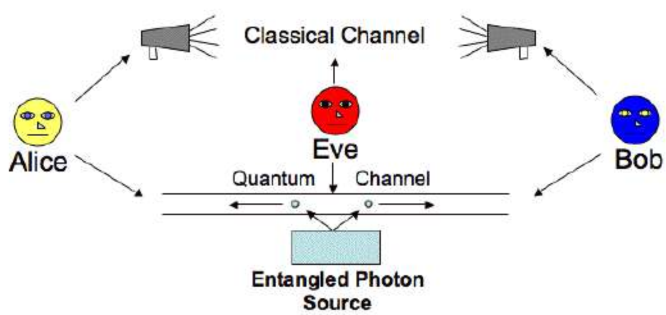
Almost immediately Alice and Bob realize that Eve tried to copy the key and abort the operation of key distribution.

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

QKD - E91

Eckert describes a channel where there is a single source that emits pairs of entangled particles, which could be polarized photons. The particles are separated and Alice and Bob each receive one particle from each pair as shown in figure 5. Alice and Bob would each choose a random bases on which to measure their received particles. As in BB84, they would discuss in the clear which bases they used for their measurements. For each measurement where Alice and Bob used the same bases, they should expect opposite results due to the principle of quantum entanglement as described earlier.

This means that if Alice and Bob both interpret their measurements as bits as before, they each have a bit string which is the binary complement of the other. Either party could invert their key and they would thus share a secret key.



QKD - E91

The presence of an eavesdropper can be detected by examining the photons for which Alice and Bob chose different bases for measurement. Alice and Bob can measure these photons in a third basis and discuss their results. With this information they can test Bell's Inequality which should not hold for entangled particles. If the inequality does hold, it would indicate that the photons were not truly entangled and thus there may be an eavesdropper present.