Quantum communications: exploiting entanglement

Kenneth Maussang

▶ **To cite this version:**

Kenneth Maussang. Quantum communications: exploiting entanglement. Master. Quantum technologies and industry, France. 2023, pp.64. hal-04423707

HAL Id: hal-04423707
https://cel.hal.science/hal-04423707v1

Submitted on 29 Jan 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution - NonCommercial - NoDerivatives 4.0 International License

Quantum communications: exploiting entanglement

Quantum technologies and industry

Kenneth MAUSSANG

Université de Montpellier

2022 – 2023

CC BY NC ND

Quantum communications: exploiting entanglement

CC BY NC ND

Quantum communications: exploiting entanglement

CC BY NC ND

I.1. EPR paradox

Let's consider the following state

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

The measurement of the state while give 0 with a probability $P_{|0\rangle} = 1/2$ and 1 with a probability $P_{|1\rangle} = 1/2$. So, in quantum mechanics, the results of a measurement in fundamentally not deterministic: one has only a probability to obtain a given result.

I.1. EPR paradox

At the beginning of quantum mechanics theory, it was difficult for people to admit this lose of deterministic result for measurement. Albert Einstein, Boris Podolsky and Nathan Rosen (EPR) argued that the description of physical reality provided by quantum mechanics was incomplete, and there was hidden variables that are missing in the description. Such variables are not accessible to the observer of a given system.

In a 1935 paper entitled "Can Quantum-Mechanical Description of Physical Reality be Considered Complete?", they argued for the existence of "elements of reality" that were not part of quantum theory, and speculated that it should be possible to construct a theory containing them. Resolutions of the paradox have important implications for the interpretation of quantum mechanics. Their argumentation was based on a though experiment.

Quantum communications: exploiting entanglement

CC BY NC ND

I.2. EPR though experiment

In this though experiment, one considers an entangled state of two particles. Einstein, Podolsky and Rosen pointed out that, in this state, if the position (for example) of the first particle were measured, the result of measuring the position of the second particle could be predicted. They argued that no action taken on the first particle could instantaneously affect the other, since this would involve information being transmitted faster than light, which is forbidden by the theory of relativity. From this, they inferred that the second particle must have a definite value of position and of momentum prior to either being measured. It's a hidden variable theory that could heal the non-locality of quantum mechanics theory.

Quantum communications: exploiting entanglement

CC BY NC ND

I.3. Bell's theorem

In 1964, John Bell published a paper on the EPR paradox to investigate whether it was indeed possible to solve the nonlocality problem with hidden variables. One considers then a entangled state made of two spins. Then, each spin is measured on a given axis, but not necessary the same axis. Bell showed that both models (quantum and hidden variables) can reproduce the correlations between the two measurements when they are performed on the same axis or on perpendicular axes for both particles. As soon as other angles between their axes of measurement are allowed, local hidden-variable theories become unable of reproducing the quantum mechanical correlations.

This difference, expressed using inequalities known as "Bell inequalities", is in principle experimentally testable. The experiment proposed by Bell has been experimentally realized for the first time in 1982 by Alain Aspect and his team at Orsay, Paris, conducted Bell tests using calcium cascade sources.

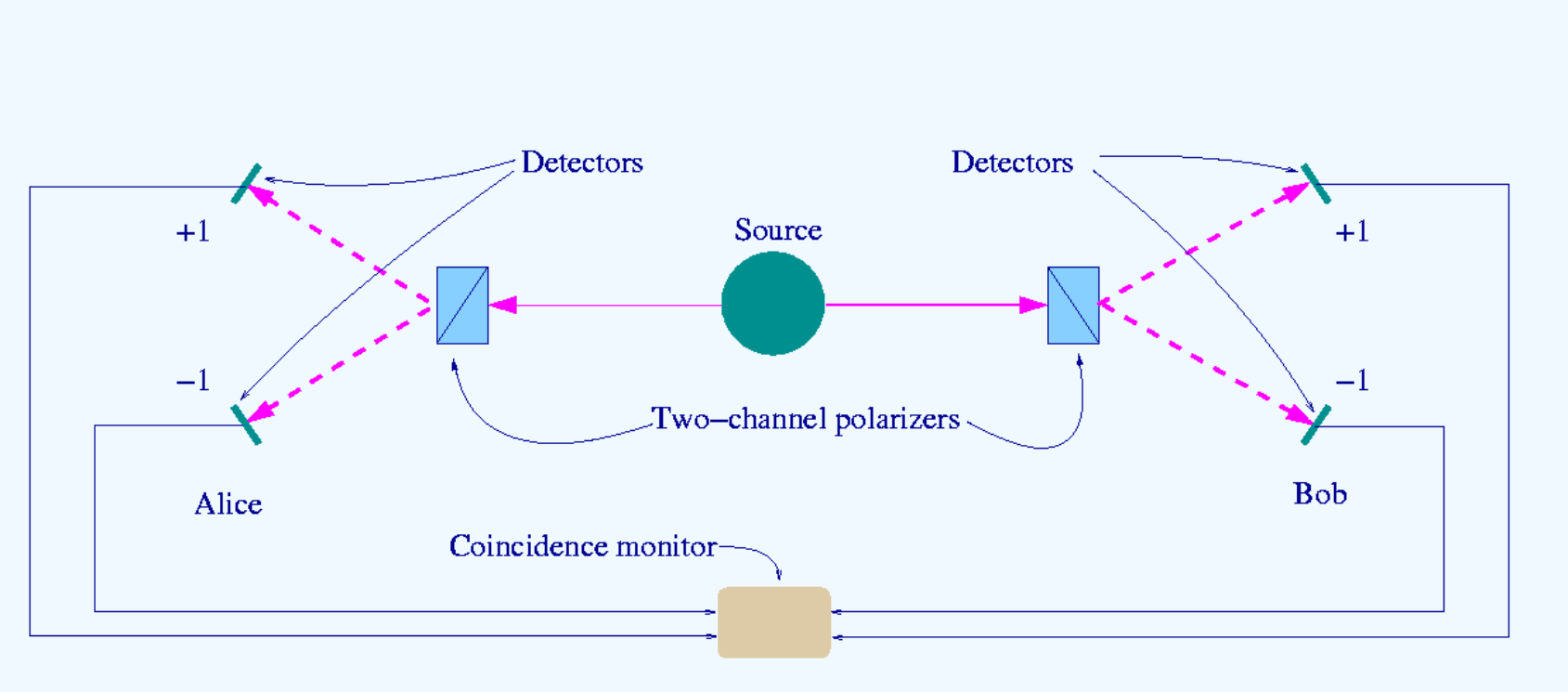
Quantum communications: exploiting entanglement

CC BY NC ND

I.4. Bell's states and Bell's inequality

The Bell states are specific quantum states of two 2-level particles maximally entangled. Entanglement is a basis-independent result of superposition. Due to this superposition, measurement of the particle will collapse it into one of its basis states with a given probability. Because of the entanglement, measurement of one particle will assign one of two possible values to the other particle instantly, where the value assigned depends on which Bell state the two particles are in. Bell states can be generalized to represent specific quantum states of multi-particles systems, such as the GHZ state for three particles. Now one consider the case of two particles only, for example two photons which might be described by their polarization, equivalent to a two level system (two orthogonal polarizations).

I.4. Bell's states and Bell's inequality



Scheme of a "two-channel" Bell test The source S produces pairs of photons, sent in opposite directions. Each photon encounters a two-channel polariser whose orientation (a or b) can be set by the experimenter. Emerging signals from each channel are detected and coincidences counted by the coincidence monitor. `https://en.wikipedia.org/wiki/Bell's_theorem`.

I.4. Bell's states and Bell's inequality

Let labels one particle A (for Alice) and the other one B (for Bob). Each observer, Alice and Bob, might measure their photon within two different directions (not necessarily orthogonal). Let note $\hat{A}_i$ (resp. $\hat{B}_i$) the two observables associated to the measurement with the photon A (resp. B). These observables are such that they outcomes ± 1 and $\left[\hat{A}_i, \hat{B}_j\right] = 0, \forall i, j$.
Then, one defines the Clauser-Horne-Shimony-Holt (CHSH) observable $\hat{\mathcal{O}}$ such as

$$\hat{\mathcal{O}} = \hat{A}_1\hat{B}_1 + \hat{A}_1\hat{B}_2 + \hat{A}_2\hat{B}_1 - \hat{A}_2\hat{B}_2.$$

Since $\hat{A}_i^2 = \hat{B}_i^2 = \hat{\mathbb{I}}$, one obtains

$$\hat{\mathcal{O}}^2 = 4\hat{\mathbb{I}} - [A_1, A_2]\,[B_2, B_2]\,.$$

I.4. Bell's states and Bell's inequality

If

$$[A_1, A_2] = [B_2, B_2] = 0,$$

then

$$\hat{\mathcal{O}}^2 = 4\hat{\mathbb{I}}$$

such that immediately

$$\left\langle \hat{\mathcal{O}} \right\rangle \leq 2.$$

This upper bound of 2 is also the upper bound one obtains in the case of a classical hidden variable theory.

I.4. Bell's states and Bell's inequality

In the quantum case, since

$$|\left\langle \left[\hat{A}_1, \hat{A}_2\right] \right\rangle| \leq 2|\left\langle \hat{A}_1 \right\rangle| \cdot |\left\langle \hat{A}_2 \right\rangle| \leq 2.$$

Similarly,

$$|\left\langle \left[\hat{B}_1, \hat{B}_2\right] \right\rangle| \leq 2|\left\langle \hat{B}_1 \right\rangle| \cdot |\left\langle \hat{B}_2 \right\rangle| \leq 2.$$

Therefore

$$\left\langle \hat{\mathcal{O}}^2 \right\rangle \leq 4+|\langle [A_1, A_2]\,[B_2, B_2]\rangle| \leq 4+|\langle [A_1, A_2]\rangle| \cdot |\langle [B_1, B_2]\rangle| \leq 4+4.$$

I.4. Bell's states and Bell's inequality

So finally, in the quantum case, the Clauser-Horne-Shimony-Holt observable is upper-bounded by the so-called Tsirelson bound

$$\left\langle \hat{\mathcal{O}} \right\rangle \leq 2\sqrt{2}.$$

Then, if one realizes experimentally a situation such that

$$2 < \left\langle \hat{\mathcal{O}} \right\rangle \leq 2\sqrt{2},$$

Bell's inequalities are said to be violated: only quantum correlations may explain such inequality, not hidden variables theory.

The upper-bound is obtained for certain type of observables, for isntance

$$\hat{A}_1 = \hat{\sigma}_{z,A}, \quad \hat{A}_2 = \hat{\sigma}_{x,A},$$

$$\hat{B}_1 = -\frac{1}{\sqrt{2}}\left(\hat{\sigma}_{z,B} + \hat{\sigma}_{x,B}\right), \quad \hat{B}_2 = \frac{1}{\sqrt{2}}\left(\hat{\sigma}_{z,B} - \hat{\sigma}_{x,B}\right),$$

then it is easy to demonstrate that

$$\left\langle \hat{\mathcal{O}} \right\rangle = 2\sqrt{2} > 2.$$

CC BY NC ND

I.4. Bell's states and Bell's inequality

A Bell test consists in testing such inequality to insure that two particle have quantum correlations (*i.e.* not explained classically) to insure they are entangled. Classical correlation can't explain such inequality. Four specific two-qubit states with the maximal value of $2\sqrt{2}$ are designated as "Bell states". They are known as the four maximally entangled two-qubit Bell states, and they form a maximally entangled basis, known as the Bell basis, of the four-dimensional Hilbert space for two qubits:

$$|\phi+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right),$$

$$|\phi-\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right),$$

$$|\psi+\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right),$$

$$|\psi-\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right).$$

BY NC ND

Quantum communications: exploiting entanglement

CC BY NC ND

I.5. GHZ state

A Greenberger–Horne–Zeilinger state (GHZ state) is a certain type of entangled quantum state that involves $M > 2$ subsystems (particle states, or qubits).

It was first studied by Daniel Greenberger, Michael Horne and Anton Zeilinger in 1989. If each subsystem has a dimension d, the local Hilbert space is isomorphic to $\mathbb{C}^d$, then the total Hilbert space is M subsystems is $\mathcal{H} = (\mathbb{C}^d)^{\otimes M}$.

BY NC ND

I.5. GHZ state

Then, the GHZ state is expressed as

$$\begin{aligned} |\mathrm{GHZ}\rangle &= \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle \otimes \cdots \otimes |i\rangle \\ &= \frac{1}{\sqrt{d}} (|0\rangle \otimes \cdots \otimes |0\rangle + \cdots + |d-1\rangle \otimes \cdots \otimes |d-1\rangle) \end{aligned}$$

In the case of qubits ($d = 2$),

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle^{\otimes M} + |1\rangle^{\otimes M} \right).$$

I.5. GHZ state

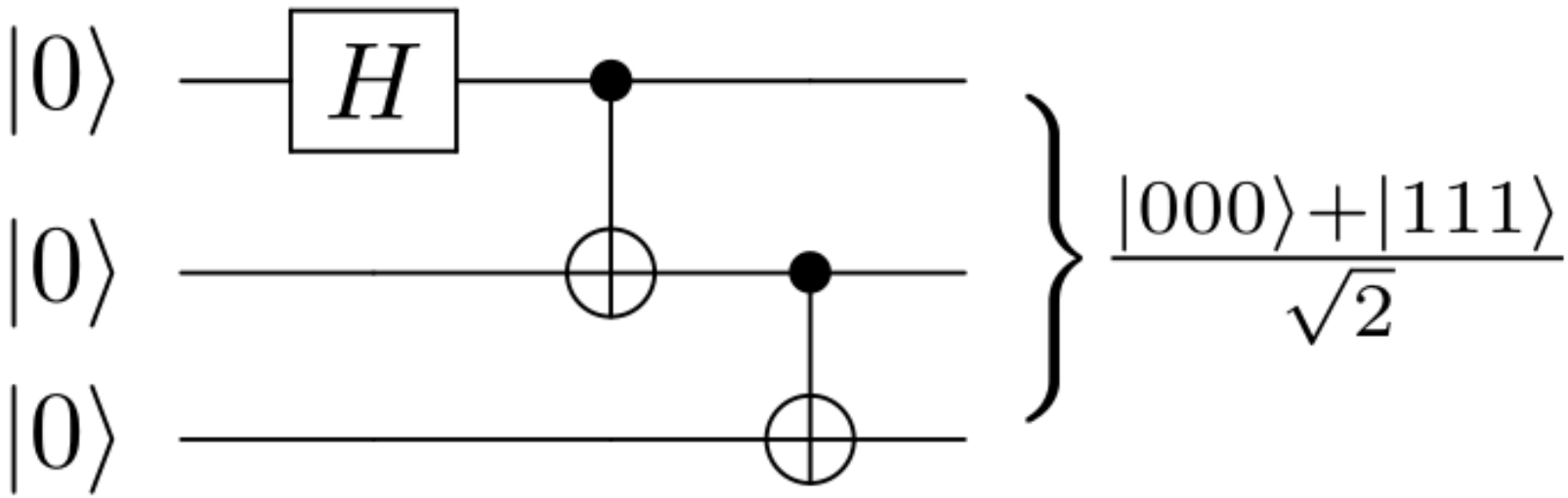
The GHZ state is a maximally entangled quantum state.

The simplest one is the 3-qubit GHZ state:

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right).$$

GHZ states are used in several protocols in quantum communication and cryptography.

I.5. GHZ state



Generation of a 3-qubits GHZ state with a quantum computer.
Extract from `https://en.wikipedia.org/wiki/Greenberger-Horne-Zeilinger_state`

Quantum communications: exploiting entanglement

CC BY NC ND

II.1. Quantum Random Number Generators

Random numbers are essential for a number of applications: encrypted data transmission (secret keys) or numerical methods rely on them (such as Monte-Carlo) for example. The random numbers have to be unpredictable and uniformly distributed.

Random Number Generators (RNG) produce sequences of random numbers.

Unpredictability refers to the fact that it is impossible to predict the next random number, even if the previous ones are known. Insuring unpredictability of a random number sequence is actually very challenging. There are three distinct types of random number generators (RNG): Pseudo-RNGs, True RNGs, and Quantum RNGs.

BY NC ND

II.1. Quantum Random Number Generators

Pseudo-RNGs are deterministic mathematical algorithms that basically "expand" a given random seed to a much longer sequence of random numbers. The random seed is supposed to be "real randomness".

The advantage of pseudo-RNGs is that they are very cheap. But they are not suited for high-quality cryptography, as a result of lack of standardization of the original seed.

II.1. Quantum Random Number Generators

In the case of True RNGs (TRNGs) and Quantum RNGs (QRNGs), random numbers are produced from the results of physical processes.

TRNGs take their random numbers from classical physical processes which are unpredictable, caused by many uncontrollable degrees of freedom (for example noise) or systems with chaotic behaviour. TRNGs based on noise in electronic circuits are very cheap and small, but the quality of the random numbers produced by TRNGs is difficult to assess. Realizing a quality TRNG is challenging and difficult to certify.

II.1. Quantum Random Number Generators

QRNGs produces random numbers from inherently indeterministic quantum processes, from the fundamental probabilistic nature of a measurement of a quantum state, providing the later is not an eigenstate of the observable used. Consequently, it is impossible to predict random numbers that are produced by QRNGs. For instance, it could be a measurement of a qubit on the following state

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

which results in 50% probability of 0 as result, and 50% probability of 1. Repeating the process, it is straightforward that one obtains a random binary number with a arbitrary number of bits. QRNGs have two major advantages: they exploit the randomness of nature which results from quantum mechanics and their implementation is relatively easy. However, it is still challenging to make a small and cheap or a really fast QRNG.

Quantum communications: exploiting entanglement

CC BY NC ND

II.2. Quantum Key Distribution

Alternative encryption scheme have been developed to exploit quantum properties for higher level and long term security. The concept of quantum key distribution (QKD) was first proposed in the 1970s but it wasn't until the 1990s that physicists started to get really interested.

Since then the progress has been remarkable and **it is the most mature quantum technology, being commercially available for over 15 years now.** Progress continues on making these systems more compact, cheaper, and capable of operating over longer distances. These are all critical steps for the uptake of these technologies by governments and industry. The main actual challenge of such QKD systems is their integration into the existing network infrastructure.

II.2. Quantum Key Distribution

QKD provides a way of distributing and sharing secret keys that are necessary for cryptographic protocols.

The security is insured from the projective nature of measurement. If a spy intercept the quantum communication, he will project the state. In other words, the observation modifies a quantum state.

The key point of secured quantum communications is the ability to detect that a quantum state has been projected prior to its arrival (meaning there was a spy on the line).

II.2. Quantum Key Distribution

Typically, information is encoded on two orthogonal states of polarizations of single photons.

The beauty that quantum physics is that if a spy tries to intercept the key generation, he will introduce detectable consequences from projective measurement and reveal themselves.

Importantly, this happens at the secret key generation, and therefore before any information is encoded or communicated!

First commercial systems of QKD appeared in the early 2000s. High rates (>Mbps) and long distances (>400km) have been demonstrated and both academic and commercial systems continue to get smaller and cheaper.

Quantum communications: exploiting entanglement

CC BY NC ND

III.1. Benefits of quantum physics for cryptography

The principle of cryptography relies on encoding a message with a key. With a mathematical operation based on this key, the message might be revealed. Otherwise, an algorithm might be sued to "crack" the message. Cryptography consists in the use of a encoding procedure complex enough (mathematically) so it takes decades of years for an algorithm to crack it with a classical computer.

Photon based systems for quantum cryptography are now commercially available (for example ID Quantique, `http://www.idquantique.com/`)

III.1. Benefits of quantum physics for cryptography

The most common algorithm used for secured transaction on internet and files encryption is the *RAS algorithm*.

RSA algorithm has been described in 1977 by Ronald Rivest, Adi Shamir and Leonard Adleman. It has been patented by MIT in 1983. The patent is in the public domain since 2000.

The RSA algorithm is asymmetric, based on the use of two *keys*. A key is an integer number of large value. The *public key* is used to encrypt and the *private* key is used to decrypt confidential data.

III.1. Benefits of quantum physics for cryptography

Let call *Alice* a person who wants to recieve confidential data or files. She creates two keys : a public and a private key. Alice makes the public key accessible. Alice's correspondent, called *Bob*, uses this key to encrypt the data he wants to send to her. The private key is reserved for Alice, and allows her to decrypt theses data. The private key can also be sued by Alice to sign a file she sends: the public key allowing anybody to verify the signature.

A prerequisite is that it is "computationally" impossible to decrypt the file using only the public key and impossible to reconstruct the private key from the public key. RSA encryption is often used to communicate a symmetric encryption key, which then allows the exchange to continue in a confidential manner. Mathematically, RSA encryption is based on the difficulty for factorizing $n = p \times q$ a large integer number as a production of two prime numbers.

III.1. Benefits of quantum physics for cryptography

- Quantum measurements are probabilistic. It is possible to generate real random number while it is not easy to have a random generator which is really random in classical computers. For example, with a state $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, then the quantity $\langle\psi|\hat{Z}|\psi\rangle$ randomly produces -1 or $+1$ as result, and it is fundamentally random.
- In classical communications, if the message is intercepted by a spy (let's call it *Eve*), then she can copy the message and transmit it to Alice or Bob. There is not way for Alice or Bob to know if the message has been intercepted or not. In quantum mechanics, if the spy intercept a quantum message, she will perform a measurement and the state will be affected (projective measurement). It is not possible to duplicate a quantum state (non-cloning theorem). Then, it is possible for Alice and Bob to know that a spy as intercept the message in the case of quantum communications.

Quantum communications: exploiting entanglement

CC BY NC ND

III.2. Non-cloning theorem

It is impossible to physically duplicate an arbitrary quantum state $|\psi\rangle$.

Remark: the non-cloning theorem considers an arbitrary state $|\psi\rangle$. Of course it is possible to duplicate pure states $|0\rangle$ or $|1\rangle$ for example with C-gates.

Demonstration:

Let assume that we have a unitry operator $\hat{U}_{\text{cloning}}$ and two quantum states $|\phi\rangle$ and $|\psi\rangle$ which $\hat{U}_{\text{cloning}}$ duplicates, *i.e.*

$$|\phi\rangle \otimes |0\rangle \overset{\hat{U}_{\text{cloning}}}{\longrightarrow} |\phi\rangle \otimes |\phi\rangle,$$

$$|\psi\rangle \otimes |0\rangle \overset{\hat{U}_{\text{cloning}}}{\longrightarrow} |\psi\rangle \otimes |\psi\rangle.$$

CC BY NC ND

III.2. Non-cloning theorem

Then,

$$\langle \phi|\psi\rangle \ = (\langle \phi|\langle 0|)\,(|\psi\rangle\,|0\rangle)\,.$$

Or, $\hat{U}_{\text{cloning}}$ is unitary

$$\hat{U}^{\dagger}_{\text{cloning}}\hat{U}_{\text{cloning}} = \hat{U}_{\text{cloning}}\hat{U}^{\dagger}_{\text{cloning}} = \mathbb{I}$$

Then

$$\begin{aligned}\langle \phi|\psi\rangle &= (\langle \phi|\langle 0|)\,\hat{U}^{\dagger}_{\text{cloning}}\hat{U}_{\text{cloning}}\,(|\psi\rangle\,|0\rangle)\\ &= (\langle \phi|\langle \phi|)\,(|\psi\rangle\,|\psi\rangle)\\ &= \langle \phi|\psi\rangle^{\,2},\end{aligned}$$

therefore

$$\langle \phi|\psi\rangle \ = \langle \phi|\psi\rangle^{\,2} \Rightarrow \langle \phi|\psi\rangle \ = 0 \text{ or } 1.$$

III.2. Non-cloning theorem

Suppose that $\hat{U}_{\text{cloning}}$ duplicates the following state

$$|\phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle,$$

then

$$\begin{aligned} |\phi\rangle \otimes |0\rangle \overset{\hat{U}_{\text{cloning}}}{\longrightarrow} |\phi\rangle \otimes |\phi\rangle &= (\alpha\,|0\rangle + \beta\,|1\rangle)\,(\alpha\,|0\rangle + \beta\,|1\rangle)\,, \\ &= \alpha^2\,|00\rangle + \alpha\beta\,(|10\rangle + |01\rangle) + \beta^2\,|11\rangle. \end{aligned}$$

III.2. Non-cloning theorem

But now if we use $\hat{U}_{\text{cloning}}$ to clone the expansion of $|\phi\rangle$, we arrive at a different state.

$$(\alpha|0\rangle + \beta|1\rangle)|0\rangle \overset{\hat{U}_{\text{cloning}}}{\longrightarrow} \alpha|00\rangle + \beta|11\rangle.$$

In the last expression, there is no crossed terms, thus we have a contradiction. Such an unitary operator $\hat{U}_{\text{cloning}}$ does not exist. Note that it is however possible to clone a known state such as $|0\rangle$ and $|1\rangle$.

Reference : A single quantum cannot be cloned, W.K. Wootters and W.H. Zurek, *Nature*, **299** (1982).

Quantum communications: exploiting entanglement

CC BY NC ND

If it is not possible to duplicate a state, it is possible to teleport a state. Quantum teleportation is a mean to replace the state of one qubit with another. The state is "transmitted" by setting an entangled state-space of three qubits and then removing two qubits from the entanglement (via measurement). Let consider a state

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle,$$

a state to teleport, and

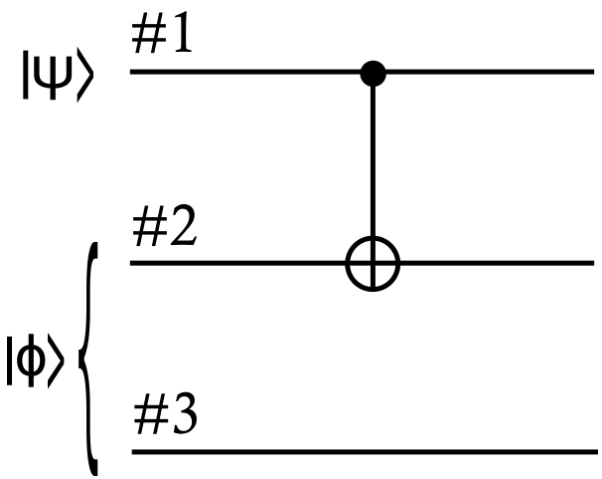
$$|\phi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right),$$

a so-called EPR state[1].

[1] An EPR state might be generated by an Hadamard gate followed by a C-NOT gate.

The state of the entire system is

$$|\psi\rangle |\phi\rangle = \frac{1}{\sqrt{2}} \left(a |0\rangle \left(|00\rangle + |11\rangle \right) + b |1\rangle \left(|00\rangle + |11\rangle \right) \right).$$



Then, applying a C-NOT control with $|\psi\rangle$ as a control qubit and the first qubit of $|\phi\rangle$ as a target qubit , one obtains the following state

$$\frac{1}{\sqrt{2}} \left(a |0\rangle \left(|00\rangle + |11\rangle \right) + b |1\rangle \left(|10\rangle + |01\rangle \right) \right).$$

Then, we apply a Hadamard gate on the qubit $|\psi\rangle$, to obtain the state $|\varphi\rangle$

$$\begin{aligned} |\varphi\rangle &= \frac{1}{\sqrt{2}}\left(\frac{a}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)\left(|00\rangle+|11\rangle\right)\right. \\ &\left.+\frac{b}{\sqrt{2}}\left(|0\rangle-|1\rangle\right)\left(|10\rangle+|01\rangle\right)\right). \end{aligned}$$

This state might be written as

$$|\varphi\rangle = \frac{1}{2}\left(|00\rangle\left(a|0\rangle + b|1\rangle\right) + |01\rangle\left(a|1\rangle + b|0\rangle\right) + |10\rangle\left(a|0\rangle - b|1\rangle\right) + |11\rangle\left(a|1\rangle - b|0\rangle\right)\right),$$

which we can shorten to

$$|\varphi\rangle = \frac{1}{2}\left(|00\rangle\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}|\psi\rangle + |01\rangle\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}|\psi\rangle + |10\rangle\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}|\psi\rangle + i|11\rangle\begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}|\psi\rangle\right)$$

CC BY NC ND

Introducing Pauli's matrix of qubit #3 ($\hat{\mathbb{I}}$,$\hat{X}$,$\hat{Y}$,$\hat{Z}$), then

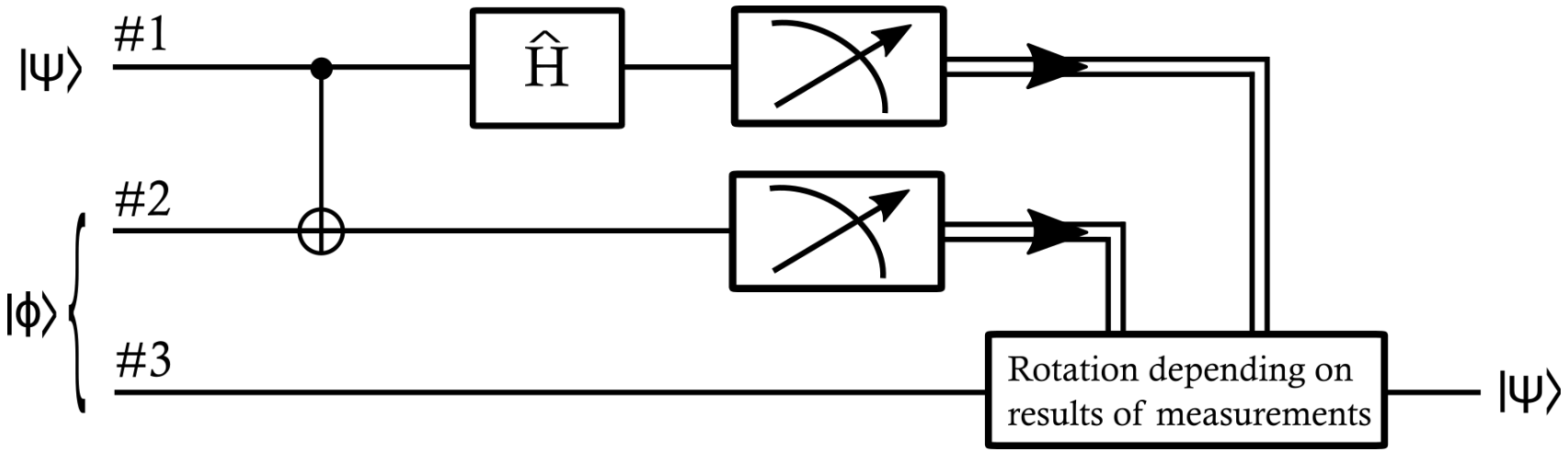
$$|\varphi\rangle = \frac{1}{2}\left(|00\rangle\hat{\mathbb{I}}\,|\psi\rangle + |01\rangle\hat{X}\,|\psi\rangle + |10\rangle\hat{Z}\,|\psi\rangle + i\,|11\rangle\hat{Y}\,|\psi\rangle\right),$$

and alternatively

$$|\varphi\rangle = \frac{1}{2}\left(|00\rangle\hat{\mathbb{I}}\,|\psi\rangle + |01\rangle\hat{X}\,|\psi\rangle + |10\rangle\hat{Z}\,|\psi\rangle + |11\rangle\hat{X}\hat{Z}\,|\psi\rangle\right).$$

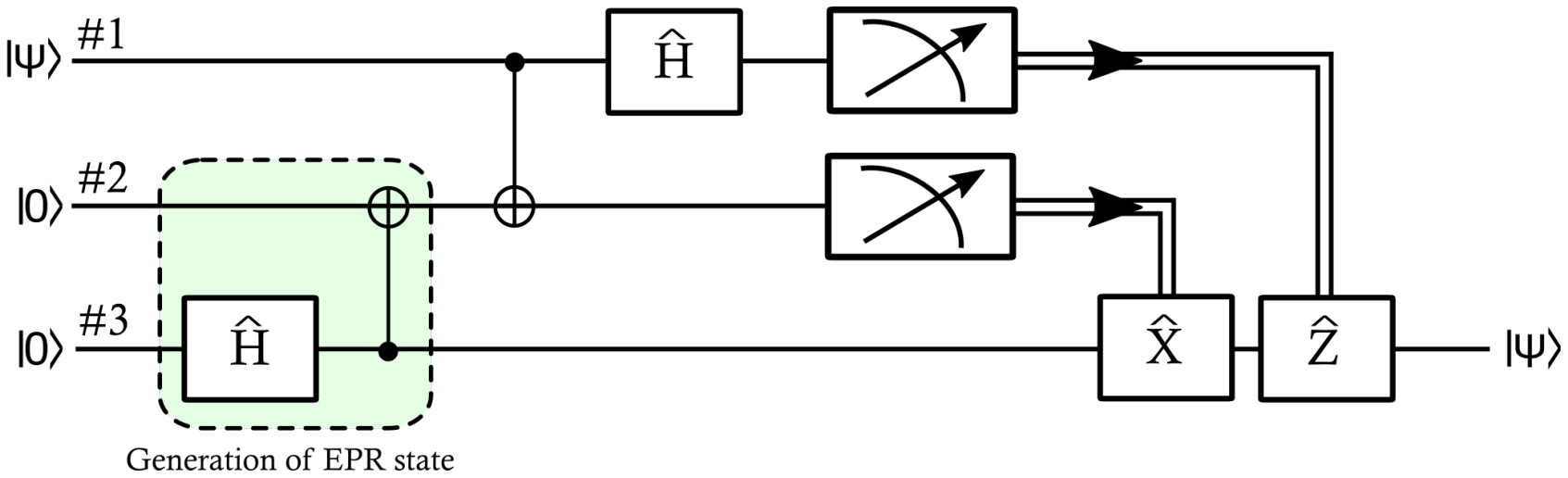
For each term, the two qubits state of qubits #1 and #2 is different in each term. This result implies that we can measure the first and second qubits to obtain two classical bits which tell us what unitary operation was applied on the third qubit. Then, we can subsequently "fix up" the third qubit once we know the classical outcome of the measurement of the first two qubits.

This fix-up is fairly straightforward,either applying nothing, $\hat{X}$, $\hat{Z}$ or $\hat{Z}\hat{X}$ (reminder: $\hat{X}^2 = \hat{Y}^2 = \hat{Z}^2 = \hat{\mathbb{I}}$).

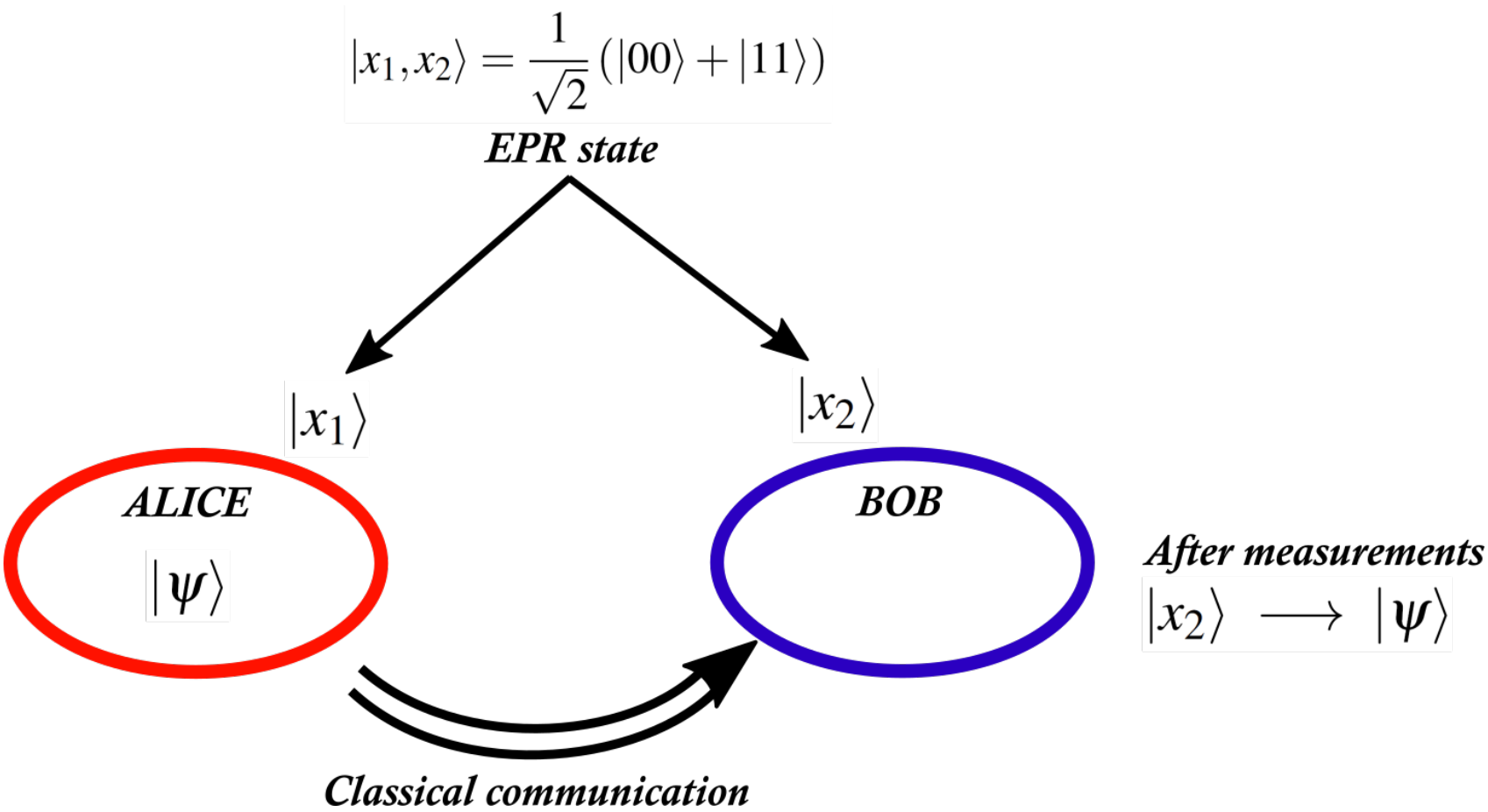


Remark: if qubit #1 is measured in state $|1\rangle$, one should apply $\hat{Z}$, nothing otherwise. If qubit #2 is measured in state $|1\rangle$, one should apply $\hat{X}$, nothing otherwise.

Implementation of quantum teleportation: complet diagram.



First, one prepares the EPR state, then it is possible to have qubit #2 and qubit #3 at different locations.



General scheme of quantum teleportation.

IV. The BB84 protocol

In 1984, the first protocol for quantum cryptography was proposed by Charles H. Bennett and Gilles Brassard, name "BB84".

Reference :
Quantum Cryptography: Public key distribution and coin tossing,
C.H. Bennett and G. Brassard, *Proc. of the IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore (1984).

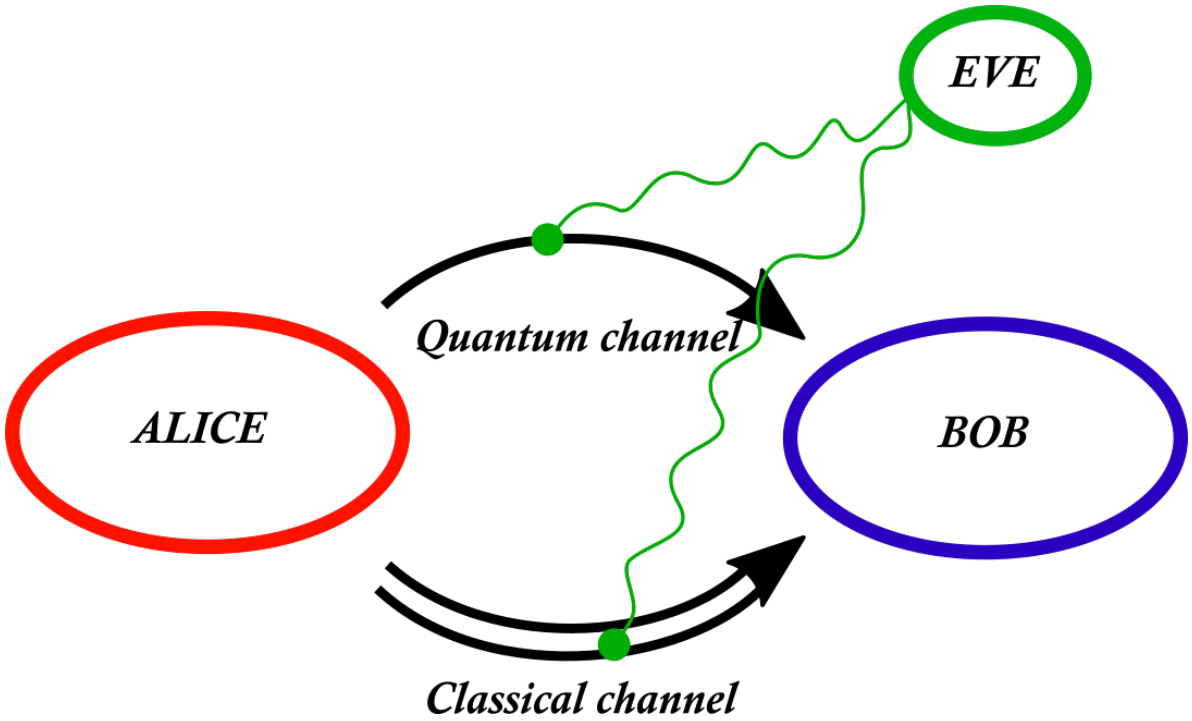
IV. The BB84 protocol

In 1984, the first protocol for quantum cryptography was proposed by Charles H. Bennett and Gilles Brassard, name "BB84".

Reference :
Quantum Cryptography: Public key distribution and coin tossing,
C.H. Bennett and G. Brassard, *Proc. of the IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore (1984).

IV. The BB84 protocol

The BB84 protocol uses pulses of polarized light, where each pulse contains a single photon. Alice and Bob are connected by a quantum channel, for example an optical fibre, and a classical public channel, such as a phone line or an Internet connexion.



IV. The BB84 protocol

In pratice, it is common to use the same link for both channels. In the case of polarized photons, this would be an optical fiber, differing only in the intensity of light pulses: while for the quantum channel it consists in one photon per qubit, the classical channel uses hundreds of photons per bits.

Reference : Quantum Cryptography, W. Tittel, G. Ribordy and N. Gisin, *Phys. World*, March 1998.

IV. The BB84 protocol

In order to encrypte messages, Alice and Bob need to share a secret key: that is the aim of quantum cryptography. Alice has the message and the key, she can generate an encrypted message. The problem consists in transferring the key. In order to provide a secure communication, Alice can choose between four non-orthogonal states. She has two bases with polarized photons.

The horizontal-vertical basis (noted $\bigoplus$)

- Horizontally polarized photon $|\rightarrow\rangle$,
- Vertically polarized photon $|\uparrow\rangle$,

and the diagonal basis (noted $\bigotimes$)

- $+45°$ polarized photon $|\nearrow\rangle$,
- $-45°$ polarized photon $|\nwarrow\rangle$.

IV. The BB84 protocol

To transmit information, a coding system is required. In this case and the diagonal basis (noted $\bigotimes$)

- $|\uparrow\rangle$ and $|\nwarrow\rangle$ encode for 0,
- $|\rightarrow\rangle$ and $|\nearrow\rangle$ encode for 1.

IV. The BB84 protocol

Alice chooses randomly one of the polarization state ($\bigoplus$ or $\bigotimes$) for each photon and sends the corresponding state to Bob. Then, Bob measures the incoming state in one of the two bases. If Alice and Bob use the same basis, they will get perfectly correlated results. However, every time Bob chooses a different basis than Alice, he will not get any information about the state of the photon. For example, if Alice send $|\rightarrow\rangle$ and Bob measures in the diagonal basis $\bigotimes$, he will get 50% probability of measuring $+45°$ and 50% probability of measuring $-45°$. Even if he finds out afterwards that he has chosen the wrong basis, he will not be able to determine which polarization state Alice has sent.

BB84 protocol

1. Alice chooses randomly both the basis and polarization of each photon and sends the corresponding polarization state to Bob.
2. Independently and randomly for each photon, Bob chooses one of the two bases. He either measures in the same basis than Alice and gets a perfectly correlated result or the exact opposite. If he measures in a different basis than Alice, he gets uncorrelated results. Sometimes, it also happens that Bob does not register anything because of errors on the detection or in the transmission.
3. Bob obtains a string of all received bits, also called *raw key*.
4. For each bit, Bob announces via the public channel which bases was used and which photons were registered ($\oplus$ or $\otimes$) but of course **he does not reveal which result he obtained**.

BY NC ND

BB84 protocol

4. After comparing the selected bases, Alice and Bob keep only the bits corresponding to the same basis. Because both have randomly chosen the basis, they get correlated and uncorrelated results with equal probability. Therefore, about 50% of raw key is discarded. The shorter key is called *sifted key*.
5. Alice and Bob choose randomly some of the remaining bits which they will discard later to check the error rate. There are two main reason why the error rate can differ from the expected value: technical imperfections in the setup and a potential **spy** on the transmission line. To ensure a secret key, Alice and Bob must correct the errors and they reduce Eve's knowledge of the key. The remaining string of bits is the secret key.
6. Eventually, the actual process encrypting a message can begin.

BY NC ND

The role of the spy

Eve's goal is to obtain as much valuable information as possible. The easiest way is to intercept a qubit which is transmitted from Alice to Bob. But Eve must send a qubit to Bob. Otherwise, he will tell Alice to disregard this measurement, because he did not receive the expected qubit. Consequently, Eve would not gain any useful information. In the ideal case, Eve would send a qubit in its original state. But because of the non-cloning theorem which states that creating a copy of an unknown quantum state is impossible, Eve must find another spying strategy.

BY NC ND

One of them is the intercept-resend strategy. In this case, Eve uses the same equipment than Bob, but just like him, she can't know in which basis Alice has measured the qubit ($\oplus$ or $\otimes$). She has no other choice but to choose the basis randomly. In 50% of the cases, Eve will guess the correct basis and resend a qubit in the correct state to Bob. Consequently, Eve's intervention will not be noticed by tge legitimate users. Howevern in the remaining cases, Eve will use the wrong basis as she has no information about Alice's choice. This intervention will be discovered, in half of the cases, by Alice and Bob as they get uncorrelated results. With the help of the intercept-resend strategy, Eve will get 50% information but Alice and Bob will obtain 25% error rate in their sifted key, which reveals the presence of Eve.

BY NC ND

IV. The BB84 protocol

What if Eve applies this strategy to only a fraction of measurements?
For example, with only 10% of the measurements collected by Eve, only 2.5% error rate is expected, while Eve information will be 5%. In order to appeal against such an attack, Alice and Bob use classical algorithms, first to correct the errors, and then to reduce Eve's knowledge of the final key. This process is called **privacy amplification**.

Reference : Quantum Cryptography, N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, *Rev. Mod. Phys.*, **74**, 145-195 (2002).