Introduction to Quantum Computing
Day 2 - Quantum Communication and Cryptography

Mengoni Riccardo, PhD

24 June 2021

CINECA QUANTUM COMPUTING LAB

Content

- **Recap of QM**

- **Quantum Communication**
  - Quantum Teleportation
  - Superdense Coding

- **Quantum Cryptography**
  - Quantum Key Distribution

Recap of QM

Tensor Product

$$|\phi\rangle \otimes |\psi\rangle = \begin{pmatrix} \phi_1 \begin{pmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_n \end{pmatrix} \\ \phi_2 \begin{pmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_n \end{pmatrix} \\ \vdots \\ \phi_n \begin{pmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_n \end{pmatrix} \end{pmatrix}$$

Dimension = n^2

Compact form:

$$|\psi\rangle \otimes |\phi\rangle = |\psi\rangle\,|\phi\rangle = |\psi\,\phi\rangle$$

Postulates of Quantum Computing (1)

Quantumly

To a closed quantum system is associated a space of states *H* which is a Hilbert space. The pure state of the system is then represented by a unit norm vector on such Hilbert space.

The unit of quantum information is the quantum bit a.k.a. Qubit

State of a qubit:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

Postulates of Quantum Computing (1)

Space of states: $\mathcal{H} \simeq \mathbb{C}^2$

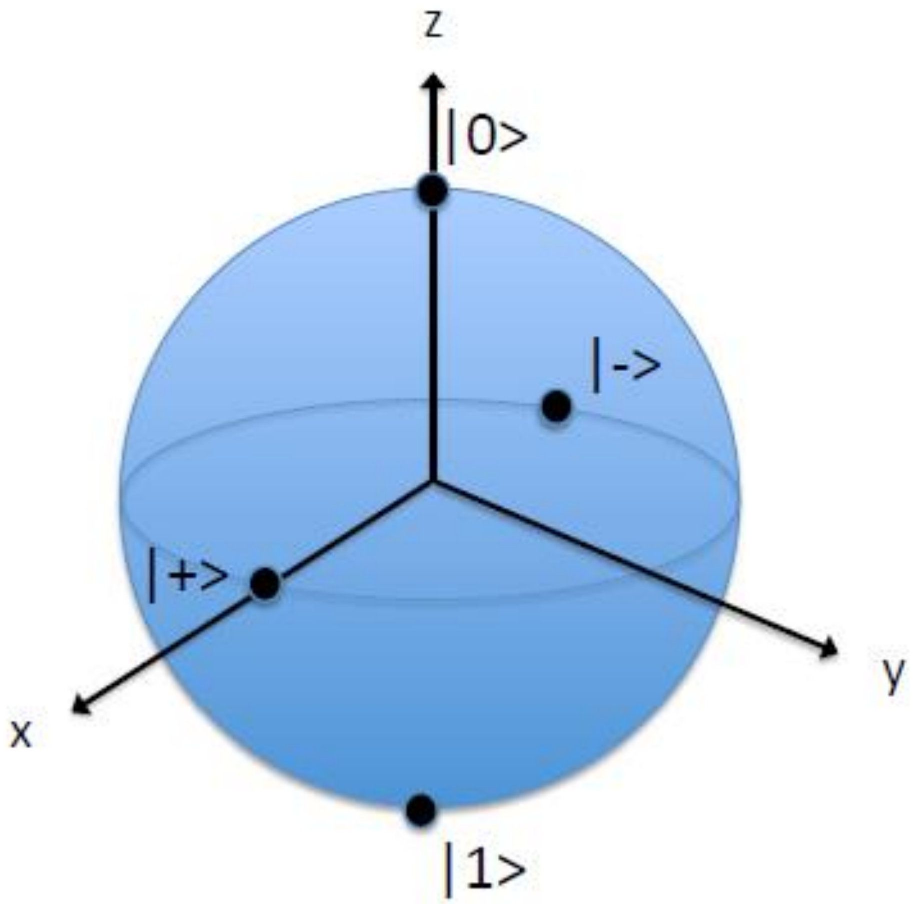
State of a qubit:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

$$\alpha, \beta \in \mathbb{C} \qquad |\alpha|^2 + |\beta|^2 = 1$$

Canonical basis: $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \ |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Other basis: $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$



Postulates of Quantum Computing (1)

Different physical realization of qubits

Physical support	Name	Information support	$\vert 0\rangle$	$\vert 1\rangle$
Photon	Polarization encoding	Polarization of light	Horizontal	Vertical
	Number of photons	Fock state	Vacuum	Single photon state
	Time-bin encoding	Time of arrival	Early	Late
Coherent state of light	Squeezed light	Quadrature	Amplitude-squeezed state	Phase-squeezed state

Canonical Basis

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \longleftarrow |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Quantumly

The space of states of a composite system is the tensor product of the spaces of the subsystems

$$\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \dots \otimes \mathbb{C}^2$$

State of N qubits:

$$\alpha_1 |000..0\rangle + \alpha_2 |100..0\rangle + \alpha_3 |010..0\rangle + \dots \alpha_n |111..1\rangle$$

$$\alpha_i \in \mathbb{C} \qquad \sum_i |\alpha_i|^2 = 1$$

Postulates of Quantum Computing (2)

Quantum Entanglement

States that **can NOT** be written as tensor product are **entangled**

$$|\psi\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle \otimes \dots \otimes |\psi_N\rangle$$

Bell's states

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

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

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

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

Quantumly

The state change of a closed quantum system is described by a unitary operator

$$i \frac{d|\psi\rangle}{dt} = H|\psi\rangle \Rightarrow |\psi(t)\rangle = e^{-iHt}|\psi(0)\rangle$$

$$U = e^{-iHt}$$

Schrodinger Equation

Quantumly

- To **any observable** physical quantity is associated an **hermitian operator** *O*

$$O\,|o_i\rangle = o_i|o_i\rangle$$

- A **measurement** outcomes are the **possibile eigenvalues** $\{o_i\}$.
- The **probability of obtaining** o_i as a result of the measurement is

$$Pr(o_i) = |\langle\psi|o_i\rangle|^2$$

- The effect of the **measure is to change the state** $|\psi\rangle$ **into the eigenvector of** *O*

$$|\psi\rangle \rightarrow |o_i\rangle$$

Postulates of Quantum Computing (4)

Different physical realization of qubits

Physical support	Name	Information support	$\lvert 0\rangle$	$\lvert 1\rangle$
Photon	Polarization encoding	Polarization of light	Horizontal	Vertical
	Number of photons	Fock state	Vacuum	Single photon state
	Time-bin encoding	Time of arrival	Early	Late
Coherent state of light	Squeezed light	Quadrature	Amplitude-squeezed state	Phase-squeezed state

Observable quantities

$$O\,|o_i\rangle = o_i|o_i\rangle$$

Canonical Basis

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix},\ |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$\Downarrow$$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Postulates of Quantum Computing (4)

Different physical realization of qubits

Physical support	Name	Information support	$\lvert 0\rangle$	$\lvert 1\rangle$
Photon	Polarization encoding	Polarization of light	Horizontal	Vertical
	Number of photons	Fock state	Vacuum	Single photon state
	Time-bin encoding	Time of arrival	Early	Late
Coherent state of light	Squeezed light	Quadrature	Amplitude-squeezed state	Phase-squeezed state

Observable quantities

$$\boxed{\begin{array}{ll} Z|0\rangle = |0\rangle & X|+\rangle = |+\rangle \\ Z\,|1\rangle = -|1\rangle & X\,|-\rangle = -|-\rangle \end{array}}$$

Canonical Basis

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix},\ |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$\Downarrow$$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Postulates of Quantum Computing (4)

Different physical realization of qubits

Physical support	Name	Information support	$\vert 0\rangle$	$\vert 1\rangle$
Photon	Polarization encoding	Polarization of light	Horizontal	Vertical
	Number of photons	Fock state	Vacuum	Single photon state
	Time-bin encoding	Time of arrival	Early	Late
Coherent state of light	Squeezed light	Quadrature	Amplitude-squeezed state	Phase-squeezed state

Observable quantities

Linear Polarization Z	Circular Polarization X

Canonical Basis

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix},\ |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$\Downarrow$$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Postulates of Quantum Computing (4)

Example:

Initial qubit state

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Measurement

Outcome

Z:

$$|0\rangle \quad con \ Pr = |\alpha|^2$$

$$|1\rangle \quad con \ Pr = |\beta|^2$$

X:

$$|+\rangle \quad con \ Pr = \frac{|\alpha+\beta|^2}{2}$$

$$|-\rangle \quad con \ Pr = \frac{|\alpha-\beta|^2}{2}$$

Quantum Communication

Classical vs Quantum Channel

Classical information channel is a communication channel used to transmit classical information

Unit of classical information -> BIT $\in \{0, 1\}$

Example: transmission cables (channel) of electrical impulses (classical information)

Classical vs Quantum Channel

Quantum information channel is a communication channel that can be used to transmit quantum information

Unit of quantum information -> QUBIT

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

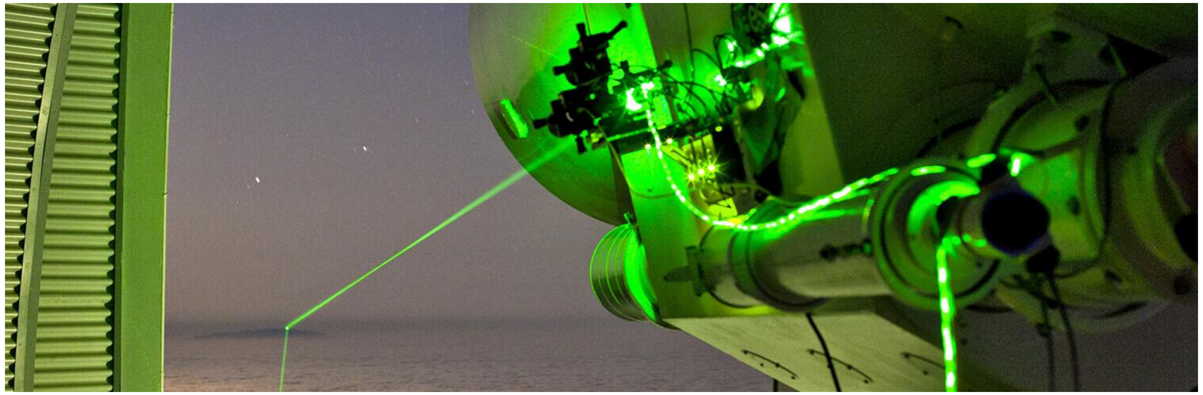
It is capable of transmitting not only base states ($|0\rangle$, $|1\rangle$) but also their quantum superimpositions (e.g. $|0\rangle + |1\rangle$).

Coherence is maintained while transmitting through the channel.

Quantum Communication

Quntum information encoded into photons

Physical support	Name	Information support	$\lvert 0 \rangle$	$\lvert 1 \rangle$
Photon	Polarization encoding	Polarization of light	Horizontal	Vertical
	Number of photons	Fock state	Vacuum	Single photon state
	Time-bin encoding	Time of arrival	Early	Late
Coherent state of light	Squeezed light	Quadrature	Amplitude-squeezed state	Phase-squeezed state



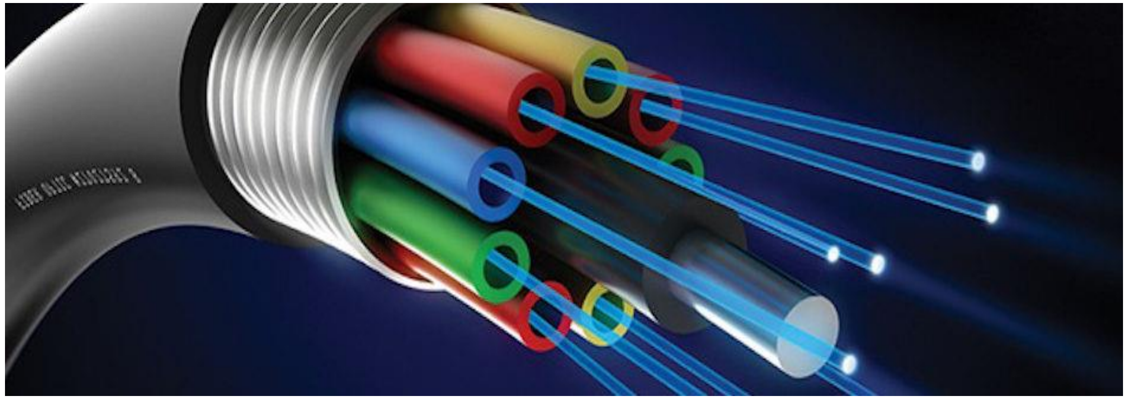
Quantum Channel:

Free-space

Quantum Communication

Quntum information encoded into photons

Physical support	Name	Information support	$\|0\rangle$	$\|1\rangle$
Photon	Polarization encoding	Polarization of light	Horizontal	Vertical
	Number of photons	Fock state	Vacuum	Single photon state
	Time-bin encoding	Time of arrival	Early	Late
Coherent state of light	Squeezed light	Quadrature	Amplitude-squeezed state	Phase-squeezed state

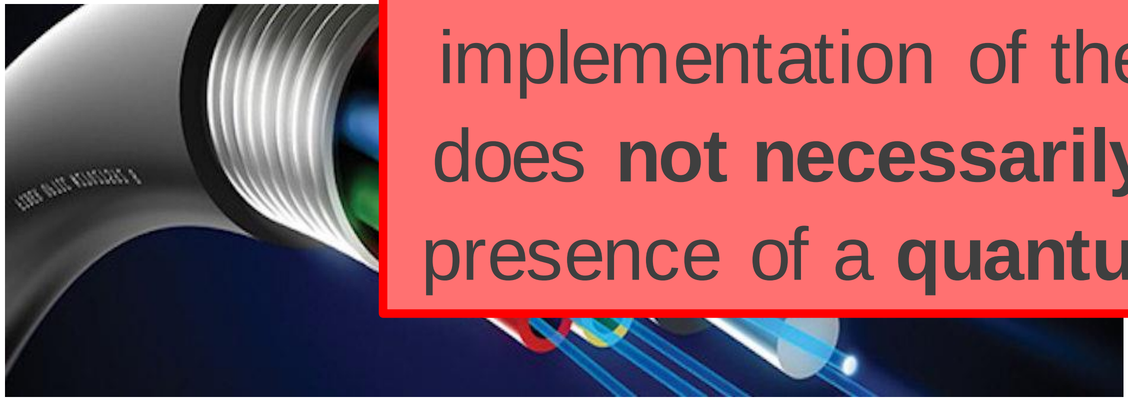


Quantum Channel:

Optical fiber

Quantum Communication

Physical support			$\|1\rangle$
Photon	Polarization e		Vertical
	Number of ph		Single photon state
	Time-bin enc		Late
Coherent state of light	Squeezed ligh		Phase-squeezed state



annel:

ber

The realization of quantum communication protocols is already possible today thanks to **specialized devices** capable of **measuring qubits**. Therefore, the implementation of these protocols does **not necessarily require** the presence of a **quantum computer**

No-Cloning Theorem

Given the postulates of quantum mechanics, **it not possible to copy exactly (cloning) an unknown quantum state**

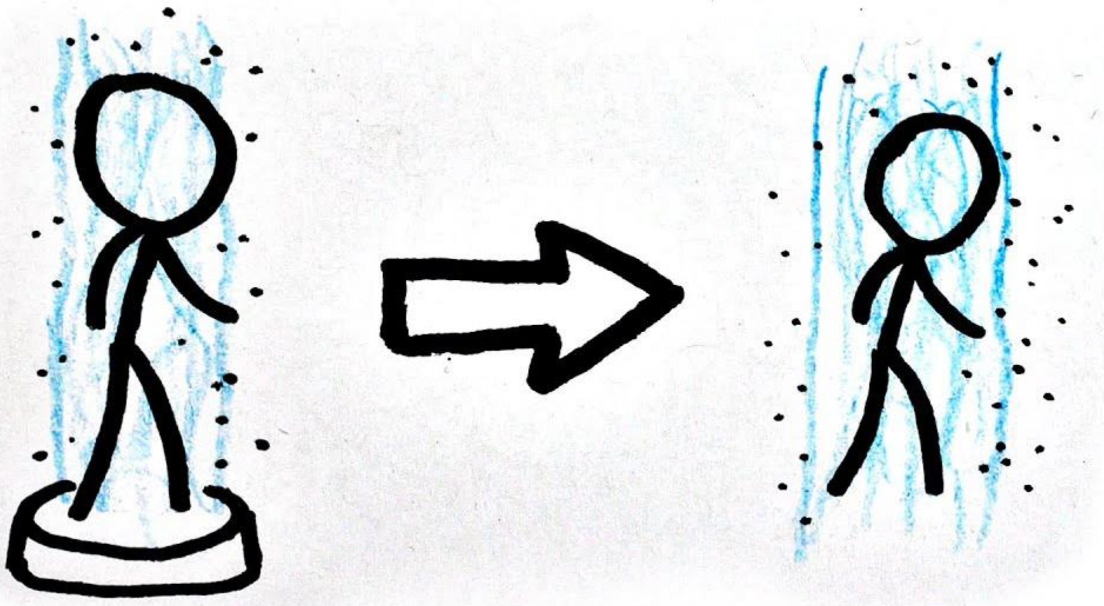
Does not exist an operator U such that, given a state $|\alpha\rangle$

relizes $U|\psi\rangle|\alpha\rangle = |\psi\rangle|\psi\rangle$

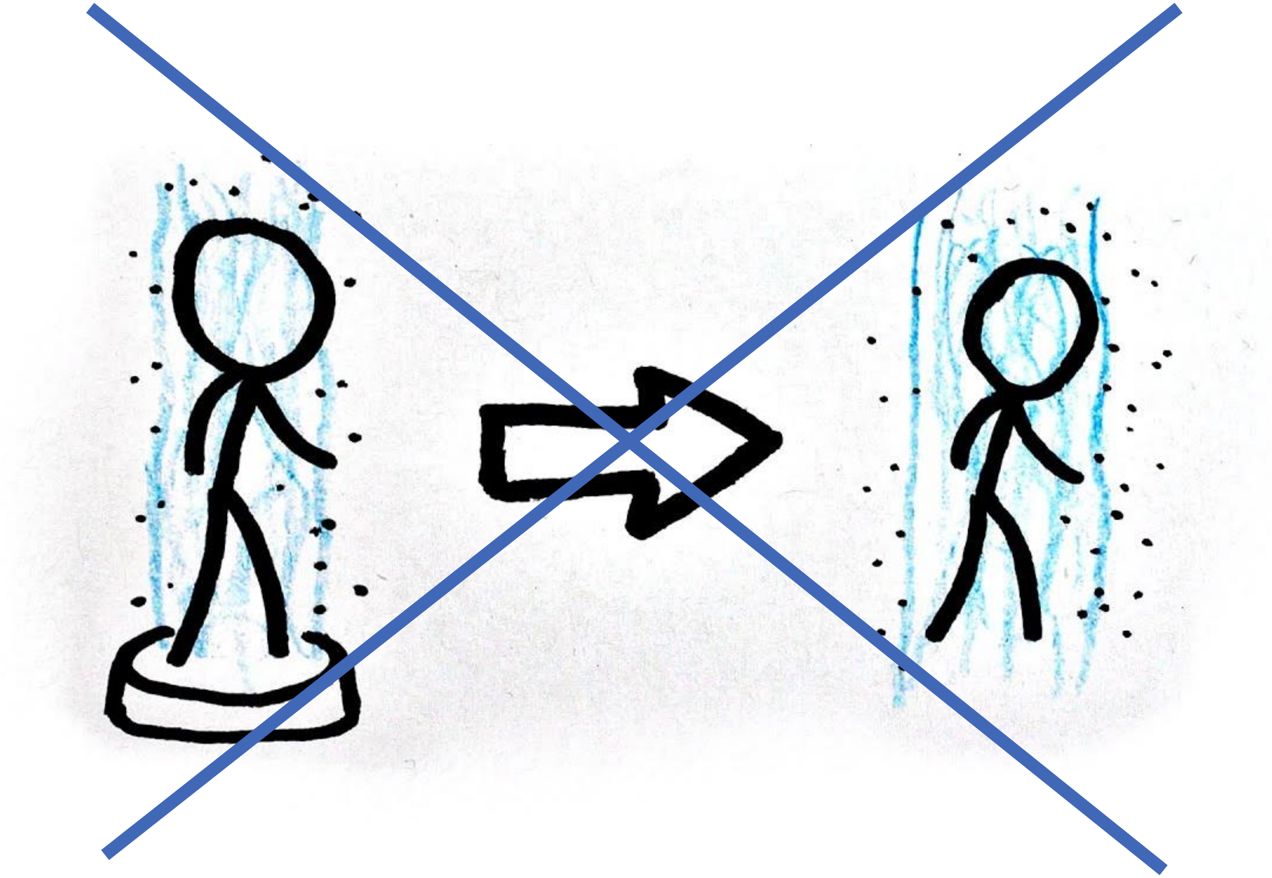
On the other hand, it is possible to perform cloning if the state belongs to an orthogonal set of states -> e.g. when it is a classic state

Quantum Teleportation

Quantum Teleportation

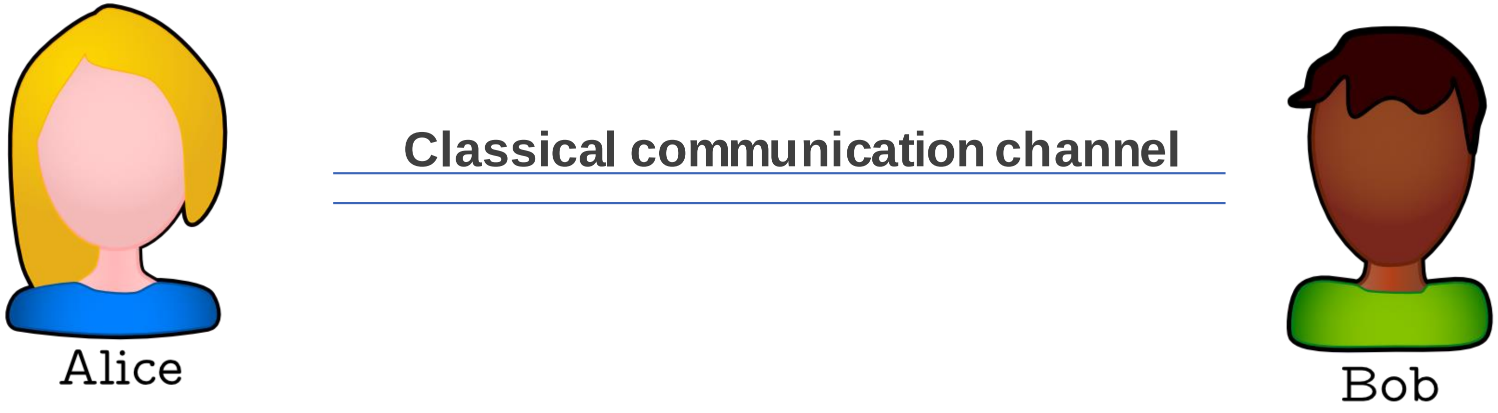


Quantum Teleportation



Quantum Teleportation

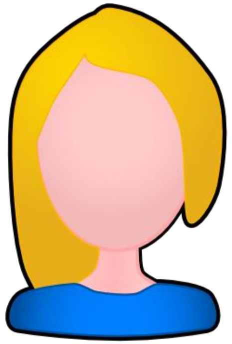
Alice wants to send a quantum state to Bob, having only a classical communication channel available.
Specifically, suppose you want to send the state of the qubit labelled C.



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

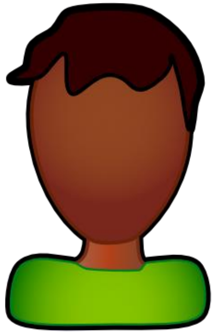
Quantum Teleportation

Remember that Alice cannot make a copy of the state of her qubit due to the No-Cloning theorem



Alice

Classical communication channel



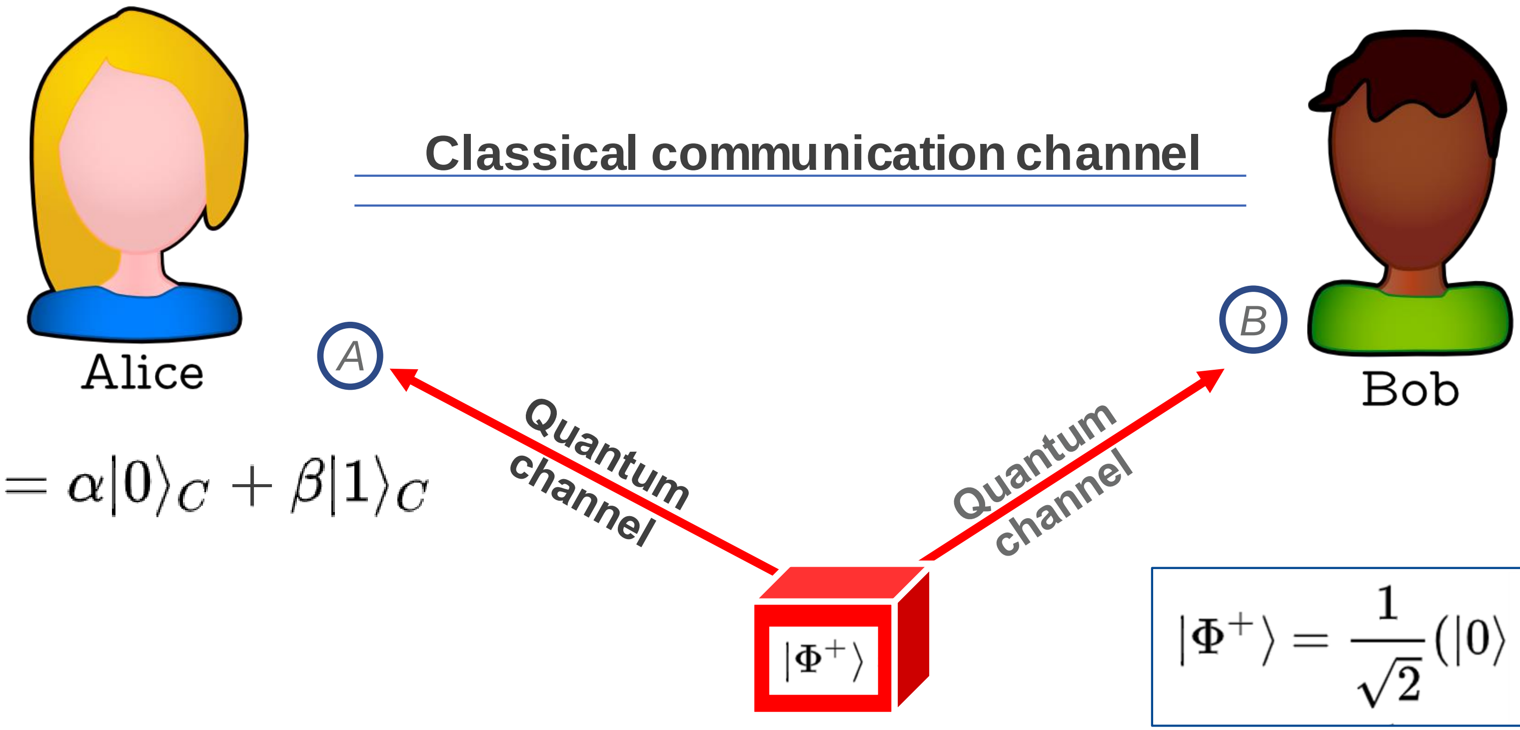
Bob

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

Cloning.. $\cancel{|\psi\rangle_C = \alpha|0\rangle_C + \beta|1\rangle_C}$

Quantum Teleportation

Alice and Bob share a pair of entangled qubits (named A and B) transmitted to them by an Entangled Qubit source (via quantum channels)



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

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

Quantum Teleportation

The global state of the three qubits possessed by Alice and Bob is

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

Quantum Teleportation

The global state of the three qubits possessed by Alice and Bob is

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

The state of qubit C that Alice wants to send to Bob

Entangled qubit pair A and B shared by Alice and Bob

Quantum Teleportation

The global state of the three qubits possessed by Alice and Bob is

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

Using the following relation (Bell states)

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

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

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

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

Quantum Teleportation

It is possible to **rewrite the global state as**

$$\frac{1}{2}\Big[\,|\Phi^{+}\rangle_{CA}\otimes(\alpha|0\rangle_B+\beta|1\rangle_B)\;+\;|\Phi^{-}\rangle_{CA}\otimes(\alpha|0\rangle_B-\beta|1\rangle_B)$$
$$+\;|\Psi^{+}\rangle_{CA}\otimes(\alpha|1\rangle_B+\beta|0\rangle_B)\;+\;|\Psi^{-}\rangle_{CA}\otimes(\alpha|1\rangle_B-\beta|0\rangle_B)\Big]$$

Teleportation occurs when Alice measures her two qubits A and C in the Bell basis

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

Quantum Teleportation

The result of Alice's measurement is that the **state of the three qubits collapses** into one of the following four states (with equal probability). **Alice uses two-bit encoding (also known to Bob) to describe the measurement result**

Encoding

- $|\Phi^+\rangle_{CA} \otimes (\alpha|0\rangle_B + \beta|1\rangle_B) \longrightarrow$ **00**
- $|\Phi^-\rangle_{CA} \otimes (\alpha|0\rangle_B - \beta|1\rangle_B) \longrightarrow$ **01**
- $|\Psi^+\rangle_{CA} \otimes (\alpha|1\rangle_B + \beta|0\rangle_B) \longrightarrow$ **10**
- $|\Psi^-\rangle_{CA} \otimes (\alpha|1\rangle_B - \beta|0\rangle_B) \longrightarrow$ **11**

Quantum Teleportation

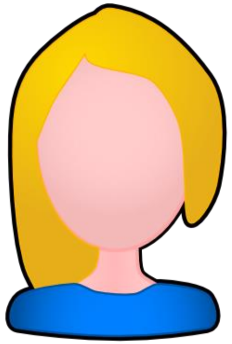
The result of Alice's measurement is that the **state of the three qubits collapses** into one of the following four states (with equal probability). **Alice uses two-bit encoding (also known to Bob) to describe the measurement result**

Encoding

- $|\Phi^+\rangle_{CA} \otimes (\alpha|0\rangle_B + \beta|1\rangle_B) \longrightarrow$ $\boxed{\mathbf{00}}$
- $|\Phi^-\rangle_{CA} \otimes (\alpha|0\rangle_B - \beta|1\rangle_B) \longrightarrow$ **01**
- $|\Psi^+\rangle_{CA} \otimes (\alpha|1\rangle_B + \beta|0\rangle_B) \longrightarrow$ **10**
- $|\Psi^-\rangle_{CA} \otimes (\alpha|1\rangle_B - \beta|0\rangle_B) \longrightarrow$ **11**

Quantum Teleportation

Alice sends the two bits of information to Bob via the classic channel. Bob applies appropriate local operations to achieve teleported state

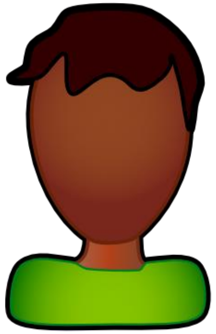


Alice

$|\Phi^+\rangle_{CA}$

Classical communication channel

00



Bob

$(\alpha|0\rangle_B + \beta|1\rangle_B)$

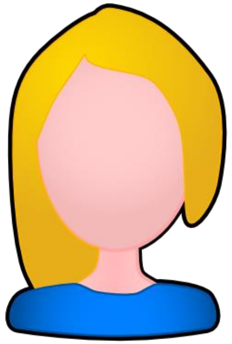
Quantum Teleportation

The result of Alice's measurement is that the **state of the three qubits collapses** into one of the following four states (with equal probability). **Alice uses two-bit encoding (also known to Bob) to describe the measurement result**

		Encoding
$\bullet\, \lvert\Phi^+\rangle_{CA} \otimes (\alpha\lvert 0\rangle_B + \beta\lvert 1\rangle_B)$	$\longrightarrow$	**00**
$\bullet\, \lvert\Phi^-\rangle_{CA} \otimes (\alpha\lvert 0\rangle_B - \beta\lvert 1\rangle_B)$	$\longrightarrow$	$\boxed{\mathbf{01}}$
$\bullet\, \lvert\Psi^+\rangle_{CA} \otimes (\alpha\lvert 1\rangle_B + \beta\lvert 0\rangle_B)$	$\longrightarrow$	**10**
$\bullet\, \lvert\Psi^-\rangle_{CA} \otimes (\alpha\lvert 1\rangle_B - \beta\lvert 0\rangle_B)$	$\longrightarrow$	**11**

Quantum Teleportation

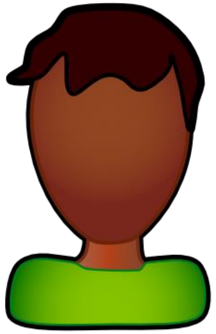
Alice sends the two bits of information to Bob via the classic channel. Bob applies appropriate local operations to achieve teleported state



Alice

Classical communication channel

01



Bob

Bob applies the Z operator

$$|\Phi^-\rangle_{CA}$$

$$Z\left(\alpha|0\rangle_B - \beta|1\rangle_B\right) =$$

$$= \left(\alpha|0\rangle_B + \beta|1\rangle_B\right)$$

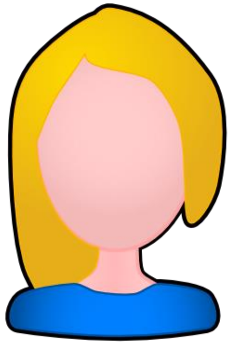
The result of Alice's measurement is that the **state of the three qubits collapses** into one of the following four states (with equal probability). **Alice uses two-bit encoding (also known to Bob) to describe the measurement result**

Encoding

- $|\Phi^+\rangle_{CA} \otimes (\alpha|0\rangle_B + \beta|1\rangle_B) \longrightarrow$ **00**
- $|\Phi^-\rangle_{CA} \otimes (\alpha|0\rangle_B - \beta|1\rangle_B) \longrightarrow$ **01**
- $|\Psi^+\rangle_{CA} \otimes (\alpha|1\rangle_B + \beta|0\rangle_B) \longrightarrow$ $\boxed{\mathbf{10}}$
- $|\Psi^-\rangle_{CA} \otimes (\alpha|1\rangle_B - \beta|0\rangle_B) \longrightarrow$ **11**

Quantum Teleportation

Alice sends the two bits of information to Bob via the classic channel. Bob applies appropriate local operations to achieve teleported state

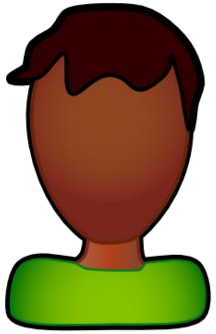


Alice

$$|\Psi^+\rangle_{CA}$$

Classical communication channel

10



Bob

Bob applies the *X* operator

$$X \ (\alpha|1\rangle_B + \beta|0\rangle_B) =$$

$$= \ (\alpha|0\rangle_B + \beta|1\rangle_B)$$

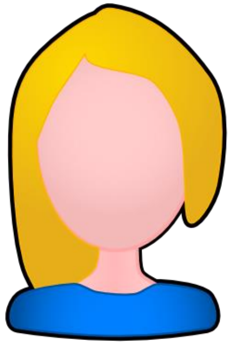
Quantum Teleportation

The result of Alice's measurement is that the **state of the three qubits collapses** into one of the following four states (with equal probability). **Alice uses two-bit encoding (also known to Bob) to describe the measurement result**

		Encoding
• $\lvert\Phi^+\rangle_{CA} \otimes (\alpha\lvert 0\rangle_B + \beta\lvert 1\rangle_B)$	$\longrightarrow$	**00**
• $\lvert\Phi^-\rangle_{CA} \otimes (\alpha\lvert 0\rangle_B - \beta\lvert 1\rangle_B)$	$\longrightarrow$	**01**
• $\lvert\Psi^+\rangle_{CA} \otimes (\alpha\lvert 1\rangle_B + \beta\lvert 0\rangle_B)$	$\longrightarrow$	**10**
• $\lvert\Psi^-\rangle_{CA} \otimes (\alpha\lvert 1\rangle_B - \beta\lvert 0\rangle_B)$	$\longrightarrow$	$\boxed{\mathbf{11}}$

Quantum Teleportation

Alice sends the two bits of information to Bob via the classic channel. Bob applies appropriate local operations to achieve teleported state

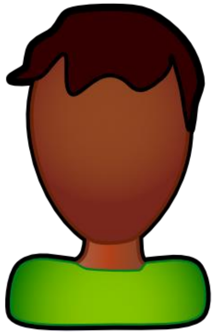


Alice

$$|\Psi^+\rangle_{CA}$$

Classical communication channel

11



Bob

Bob applies the ZX operator

$$ZX \ (\alpha|1\rangle_B - \beta|0\rangle_B) =$$

$$= (\alpha|0\rangle_B + \beta|1\rangle_B)$$

Quantum Teleportation Protocol: Final Comments

- **Quantum teleportation is not instantaneous**: in order to reconstruct the initial state, Bob must first receive the two bits associated with Alice's measurement. These are transmitted via a classical communication channel, so the signal cannot travel at superluminal speed (in accordance with special relativity).

- **Quantum teleportation respects No-Cloning**: the measurement by Alice leads to the collapse of the wave function and therefore to the loss of the initial state in her possession, respecting the No-Cloning theorem.

Quantum Teleportation Protocol: Final Comments

Experimental realizations of the protocol:

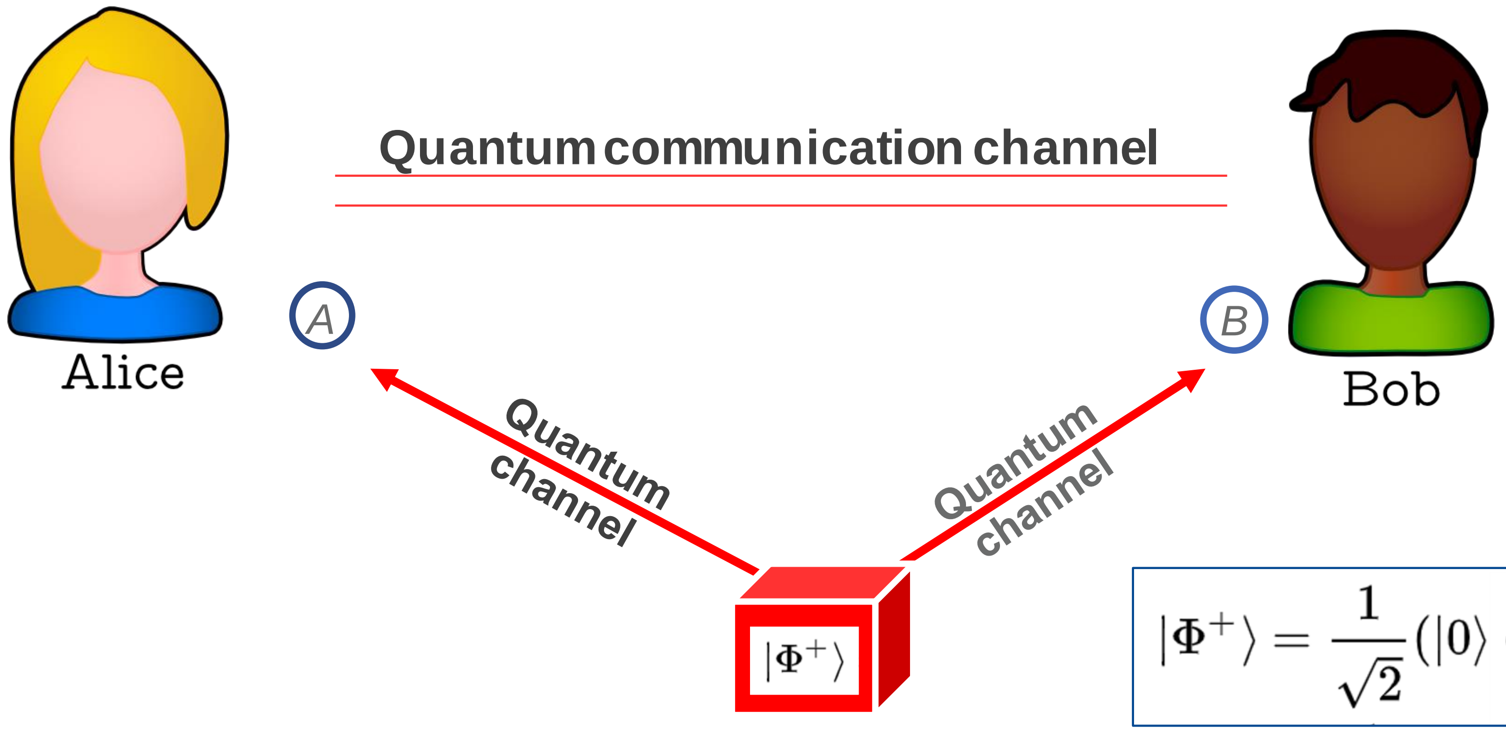
- In **2020**, a team of researchers used quantum teleportation over **44 km** of **optical fiber** -> https://arxiv.org/abs/2007.11157

- In **2017** the record for the implementation of the "**ground-to-satellite**" quantum teleportation protocol over a distance ranging from **500 km up to 1,400 km** -> https://www.nature.com/articles/nature23675

Superdense Coding

Superdense Coding

Alice and Bob pre-share a pair of entangled qubits.
Alice wants to communicate two bits of information to Bob by sending a single qubit.



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

Superdense Coding

Alice applies a certain **local operation on the qubit in her possession** in order to **encode two bits of information**

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

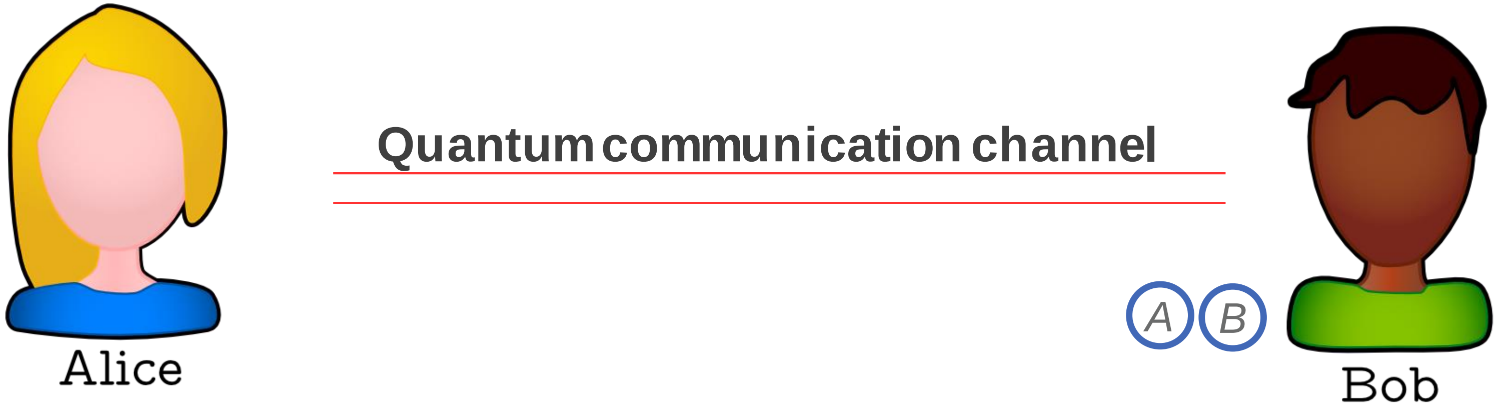
		Encoding
$\xrightarrow{I}$	$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) \longrightarrow$	**00**
$\xrightarrow{X}$	$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle) \longrightarrow$	**01**
$\xrightarrow{ZX}$	$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle) \longrightarrow$	**11**
$\xrightarrow{Z}$	$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle) \longrightarrow$	**10**

Superdense Coding

Alice sends her qubit to Bob through the quantum communication channel, hence qubit of information is communicated from Alice to Bob

Superdense Coding

Alice sends her qubit to Bob through the quantum communication channel, hence qubit of information is communicated from Alice to Bob



<u>Superdense Coding occurs when Bob measures his two qubits in the "Bell" basis to determine which state was prepared by Alice</u>

00: $|\Phi^+\rangle$ **01:** $|\Psi^+\rangle$ **10:**$|\Phi^-\rangle$ **11**$|\Psi^-\rangle$

Teleportation vs Superdense Coding

The **teleportation** protocol can be thought of as an **inverted version** of the **superdense coding** protocol, in the sense that Alice and Bob "**swap their equipment**".

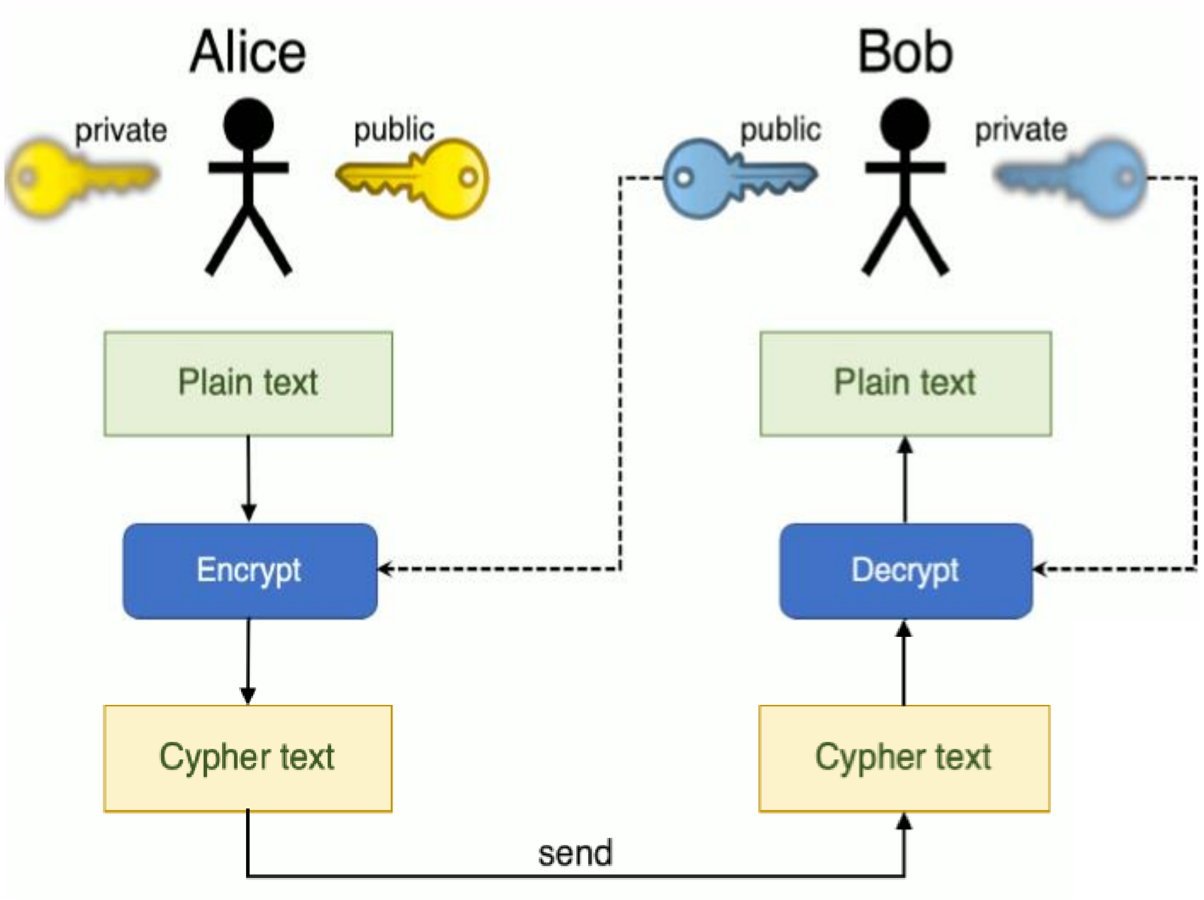
Teleportation	Superdense Coding
Transmit one qubit using two classical bits	Transmit two classical bits using one qubit

Superdense Coding Experiments:

- In 2017, a fidelity of 0.87 achieved with optical fibers. https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.118.050501
- Nel 2018, High dimensional ququarts (states obtained in photon pairs via non-degenerate spontaneous parametric down-conversion) used to achieve a 0.98 fidelity. https://advances.sciencemag.org/content/4/7/eaat9304

Quantum Cryptography

Public Key Cryptography: RSA



Public key:
Known by all. Used by the sender to encrypt a secret message

Private key:
Known to the owner only. Used by the receiver to decrypt the message

Public Key Cryptography: RSA

The RSA cryptosystem (Rivest, Shamir, Adleman, 1977)

- Alice chooses two (big) primes p and q, and computes $N = p \times q$
- Alice randomly chooses e coprime with $\phi(N) = (p-1)(q-1)$, and computes d s.t. $ed = 1\ (mod\ \phi(N))$ [i.e. $ed = 1 + j\phi(N)$]
- Alice makes N and e public
- Bob represents a message with an integer m coprime with N
- Bob computes $c = m^e\ (mod\ N)$ and sends it to Alice
- Alice receives c and computes $c^d\ (mod\ N)$ thus recovering m:

  $$c^d = m^{ed} = m^{1+j\phi(N)} = m \times \left(m^{\phi(N)}\right)^j \equiv m\ (mod\ N)$$

  Euler Theorem (1736): $gcd(m, N) = 1 \Rightarrow m^{\phi(N)} = 1\ (mod\ N)$

Public Key Cryptography: RSA

The RSA cryptosystem (Rivest, Shamir, Adleman, 1977)

- Alice chooses two (big) primes p and q, and computes $N = p \times q$
- Alice randomly chooses e coprime with $\phi(N) = (p-1)(q-1)$, and computes d s.t. $ed = 1 \ (mod\ \phi(N))$ [i.e. $ed = 1 + j\phi(N)$]
- Alice makes N and e public
- Bob represents a message with an integer m coprime with N
- Bob computes $c = m^e \ (mod\ N)$ and sends it to Alice
- Alice receives c and computes $c^d \ (mod\ N)$ thus recovering m:
  $c^d = m^{ed} = m^{1+j\phi(N)} = m \times \left(m^{\phi(N)}\right)^j \equiv m \ (mod\ N)$
  Euler Theorem (1736): $gcd(m, N) = 1 \Rightarrow m^{\phi(N)} = 1 \ (mod\ N)$

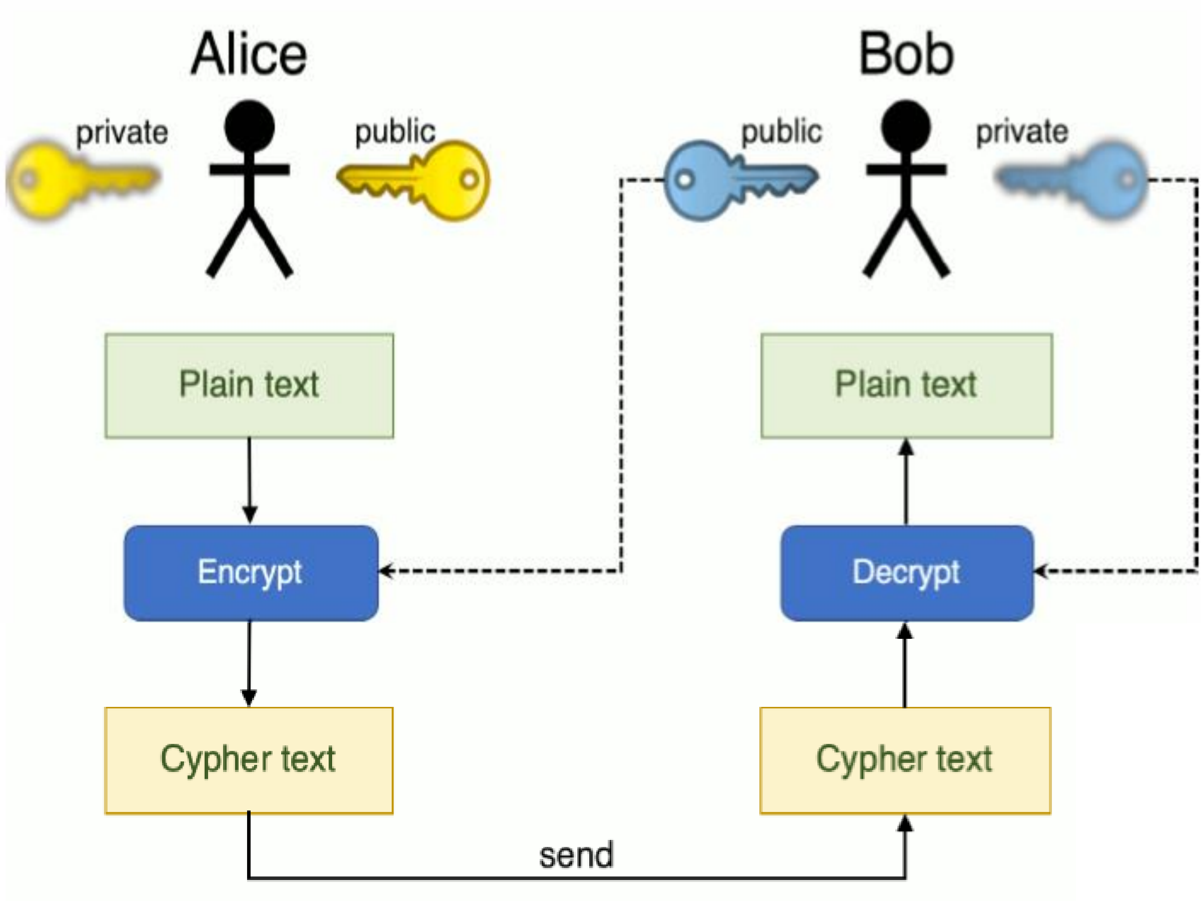
An eavesdropper has to factorize N in order to break this cryptosystem.

Public Key Cryptography: RSA

Easy example

- Choose p = 3 and q = 11
- Compute n = p * q = 3 * 11 = 33
- Compute φ(n) = (p - 1) * (q - 1) = 2 * 10 = 20
- Choose e such that 1 < e < φ(n) and e and φ (n) are coprime. Let e = 7
- Compute a value for d such that (d * e) % φ(n) = 1. One solution is d = 3 [(3 * 7) % 20 = 1]
- Public key is (e, n) => (7, 33)
- Private key is (d, n) => (3, 33)
- The encryption of $m = 2$ is $c = 2^7 \% 33 = 29$
- The decryption of $c = 29$ is $m = 29^3 \% 33 = 2$

Public Key Cryptography: RSA



Public key:
Known by all. Used by the sender to encrypt a secret message

Private key:
Known to the owner only. Used by the receiver to decrypt the message

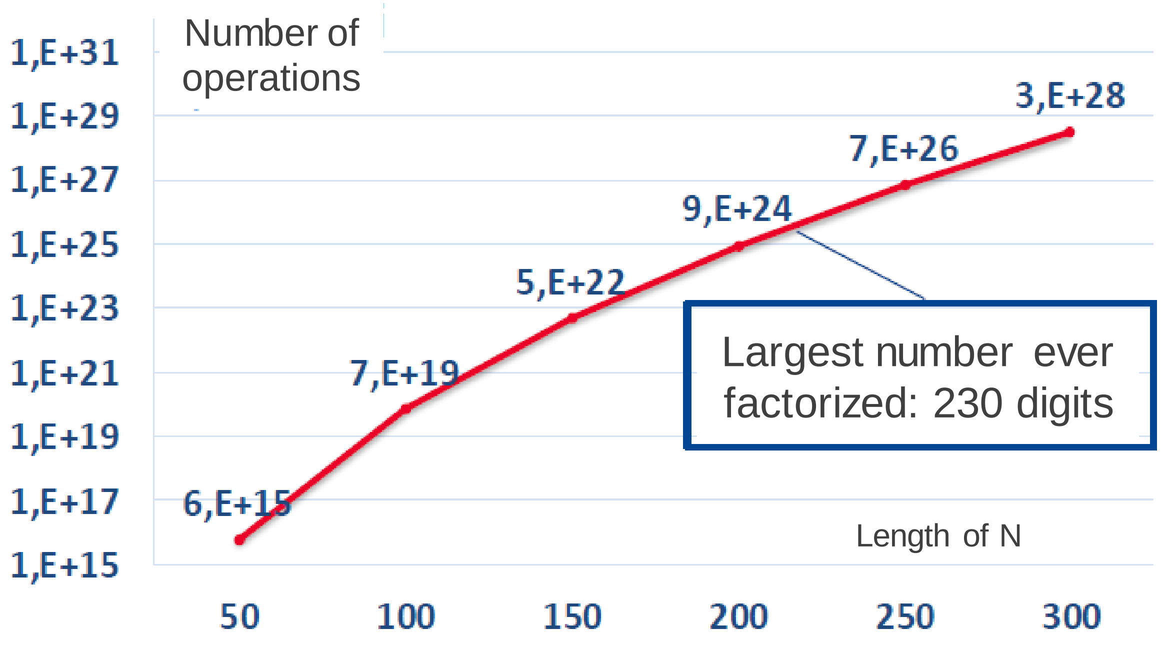
In theory it is possible to extrapolate the private key

Public Key Cryptography: RSA

In order to obtain the private key, we need to solve a hard mathematical problem

Facorization of integer numbers

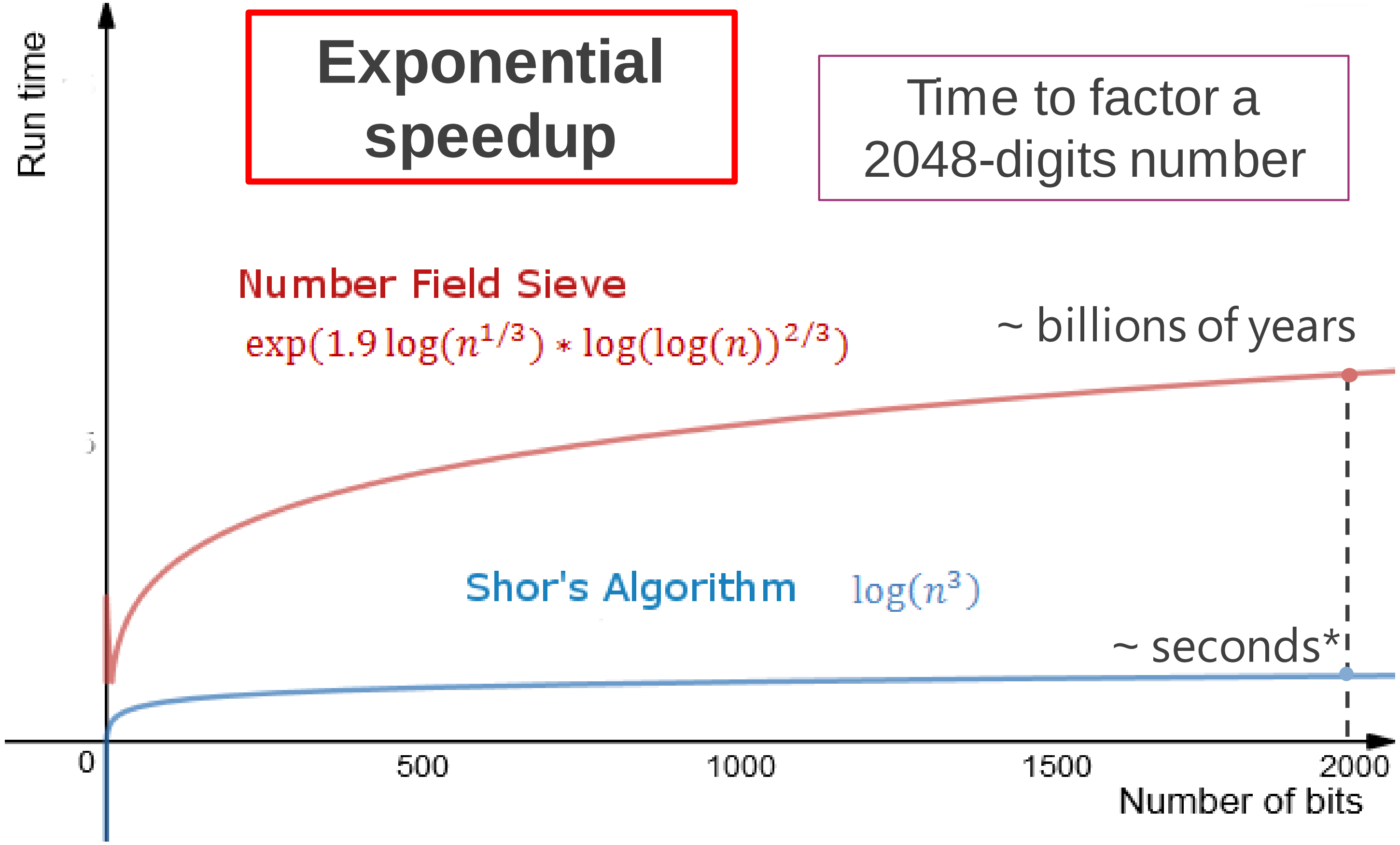
N= p x q

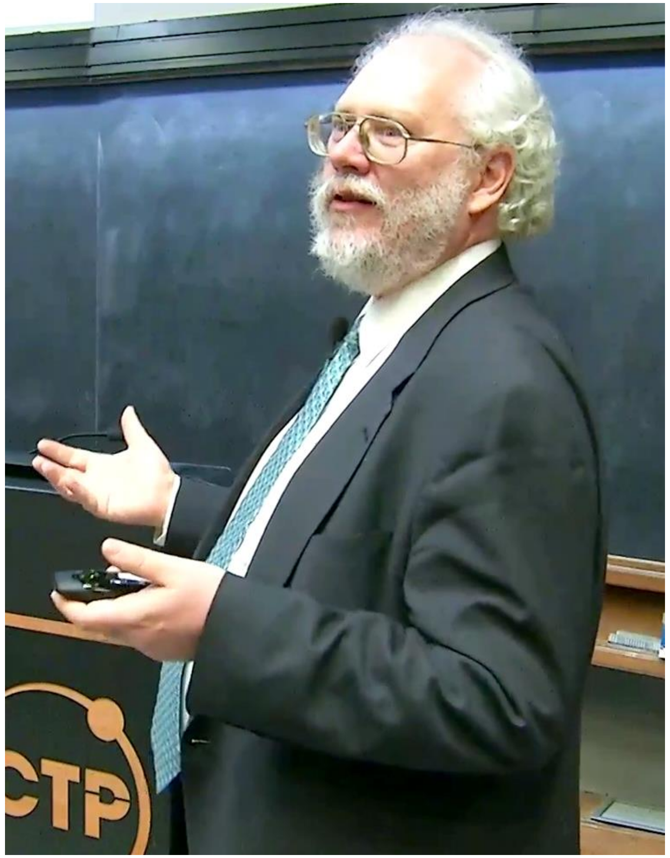


Run-time best classical algorithm:

$$e^{log(N)^{1/3}}$$

Quantum Cryptography: Shor Algorithm





* Assuming we have a fault-tolerant quantum computer capable of executing Shor's algorithm by applying gates at the speed of current quantum computers based on superconducting circuits

Quantum Cryptography

Quantum creates the problem but also provides the solution

Quantum Mechanics

Shor Quantum Algorithm

↓

Breaks RSA cryptograpy

Quantum Cryptography (QKD)

↓

Secure quantum communication

Quantum Key Distribution (QKD)

Quantum Key Distribution (QKD)

Quantum key distribution is a system for ensuring secure communications. It enables **two parties to produce and share a random secret key** only between themselves which they can **use to encrypt and decrypt their messages.**

The **security** of **QKD relies** on the **fundamentals of quantum mechanics** compared to the **traditional classical protocol** which is **based** on the **computational hardness of** certain mathematical **functions**, and **cannot provide** any **indications** regarding possible **interceptions**.

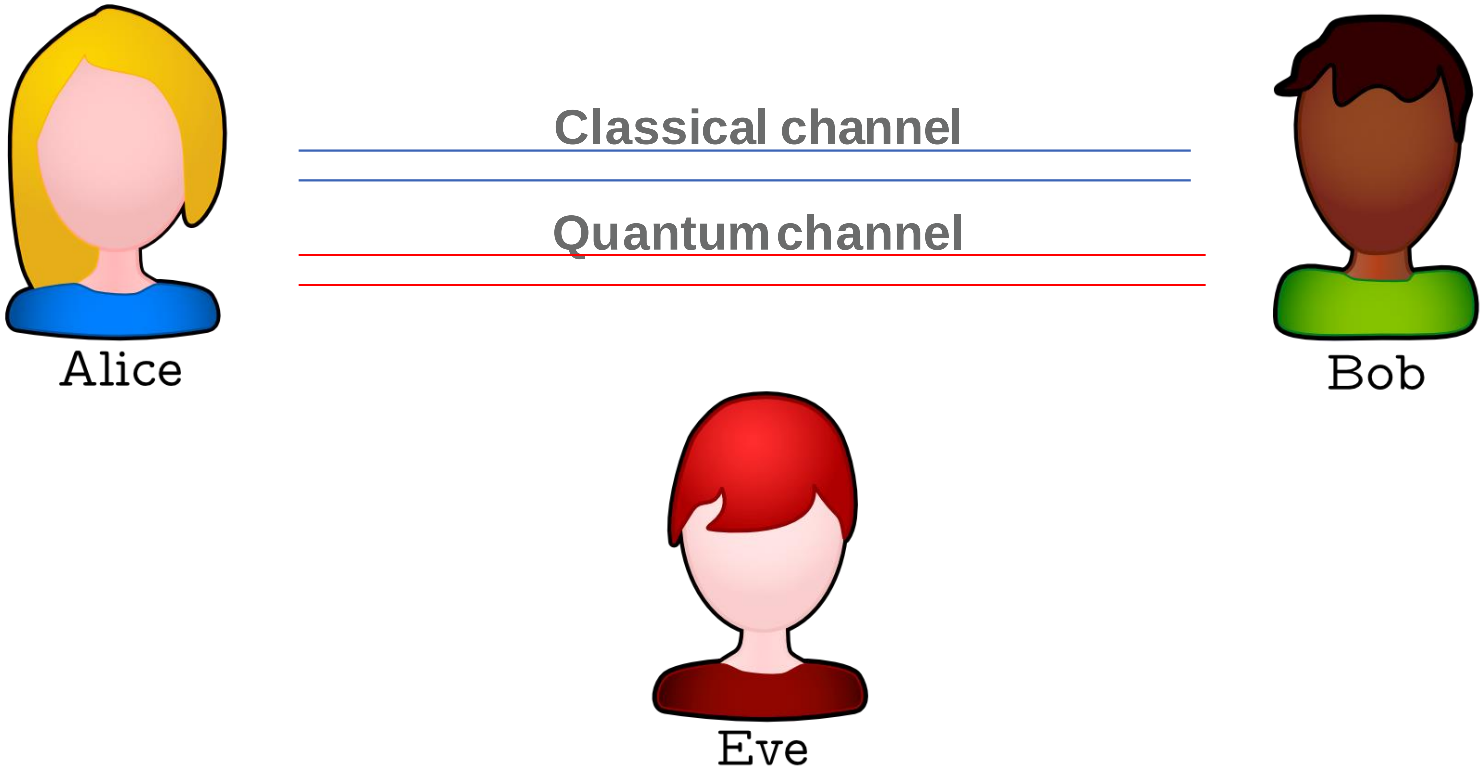
Quantum Key Distribution (QKD)

Quantum key distribution is a system for ensuring secure communications. It enables **two parties to produce and share a random secret key** only between themselves which they can **use to encrypt and decrypt their messages.**

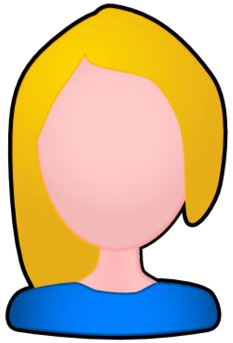
An **important and unique property of the QKD** is the **ability** of the two communicating users (Alice and Bob) **to detect the presence of a third party (Eve) who tries to obtain information on the secret key**, due to the fact that a **measurement process disturbs the quantum system**.

Quantum Key Distribution (QKD)

Quantum key distribution is a system for ensuring secure communications. It enables **two parties to produce and share a random secret key** only between themselves which they can **use to encrypt and decrypt their messages.**



Quantum Key Distribution (QKD)

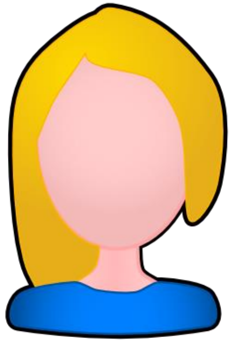


Alice

1. **Alice uses two random bit** (a, b) in order to **preare a qubit state** $|\psi_{\mathrm{ab}}\rangle$

$$|\psi_{00}\rangle = |0\rangle, \quad |\psi_{10}\rangle = |1\rangle, \quad |\psi_{01}\rangle = |+\rangle, \quad |\psi_{11}\rangle = |-\rangle,$$

Quantum Key Distribution (QKD)



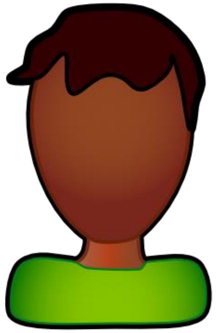
Alice

1. **Alice uses two random bit** (a, b) in order to **preare a qubit state** $|\psi_{\mathrm{ab}}\rangle$

$$|\psi_{00}\rangle = |0\rangle, \quad |\psi_{10}\rangle = |1\rangle, \quad |\psi_{01}\rangle = |+\rangle, \quad |\psi_{11}\rangle = |-\rangle,$$

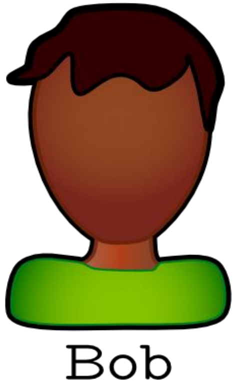
2. **Alice** sends the **qubit** $|\psi_{\mathrm{ab}}\rangle$ to **Bob via a quantum channel**

$|\psi_{\mathrm{ab}}\rangle$



Bob

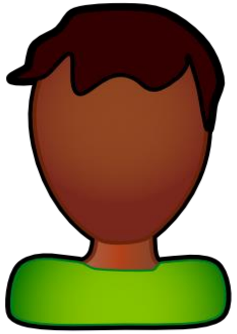
Quantum Key Distribution (QKD)



3. Bob throws a random bit b' to decide how to measure the state $|\psi_{\mathrm{ab}}\rangle$ of the qubit that Alice transmitted

$$(0 \leftrightarrow Z, 1 \leftrightarrow X)$$

Quantum Key Distribution (QKD)



Bob

3. Bob throws a random bit b' to decide how to measure the state $|\psi_{\mathrm{ab}}\rangle$ of the qubit that Alice transmitted

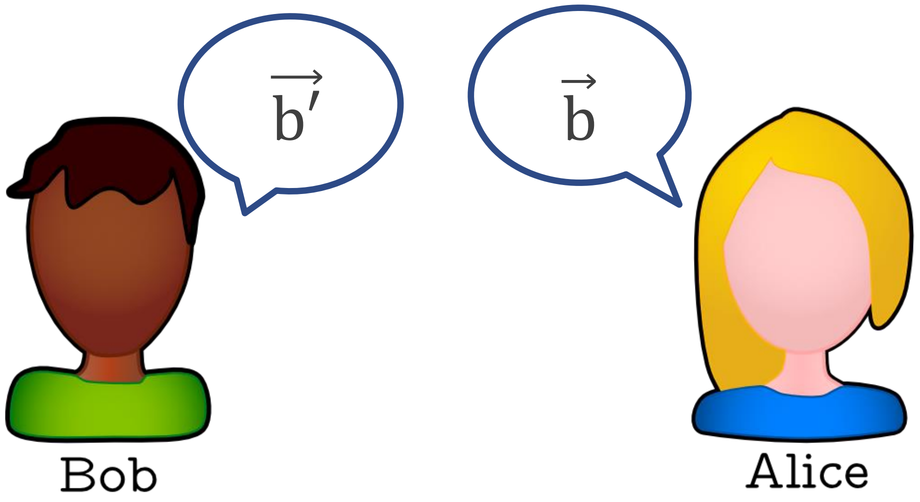
$$(0 \leftrightarrow Z, 1 \leftrightarrow X)$$

4. Bob saves the result of a measurement in a bit a'

$$\mathrm{a}' = \begin{cases} 0 & \text{if outcome is } +1 \\ 1 & \text{if outcome is } -1 \end{cases}$$

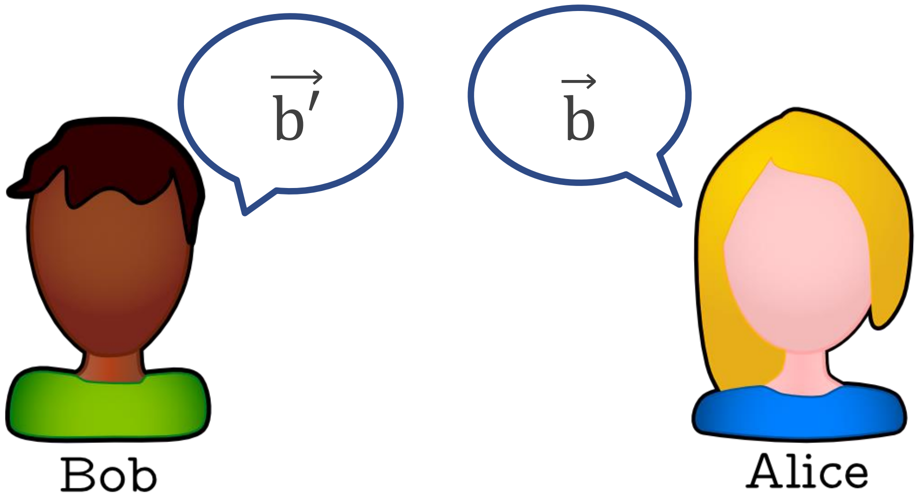
Quantum Key Distribution (QKD)

After repeting steps 1,2,3 and 4 a number *n* of times,
Alice e Bob publicly share their strings $\vec{\mathrm{b}}$ ***e*** $\vec{\mathrm{b}'}$



Quantum Key Distribution (QKD)

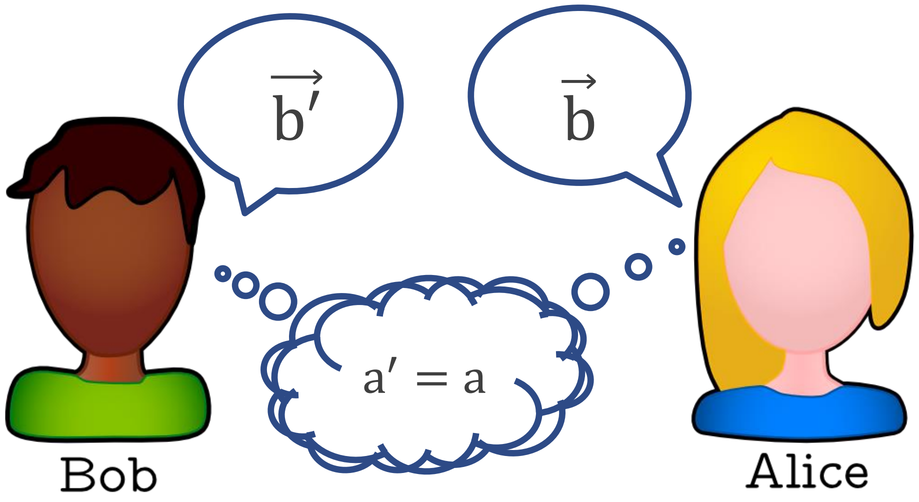
After repeting steps 1,2,3 and 4 a number *n* of times,
Alice e Bob publicly share their strings $\vec{\mathrm{b}}$ ***e*** $\vec{\mathrm{b}'}$



They discard all bits of the two strings except those for which $\mathrm{b}' = \mathrm{b}$

Quantum Key Distribution (QKD)

After repeting steps 1,2,3 and 4 a number *n* of times,
Alice e Bob publicly share their strings $\vec{\mathrm{b}}$ ***e*** $\vec{\mathrm{b}'}$



They discard all bits of the two strings except those for which $\mathrm{b}' = \mathrm{b}$

The remaining bits (asymptotically n / 2) will satisfy the relation $\mathrm{a}' = \mathrm{a}$ **and thus constitute their secret key.**

Quantum Key Distribution (QKD)

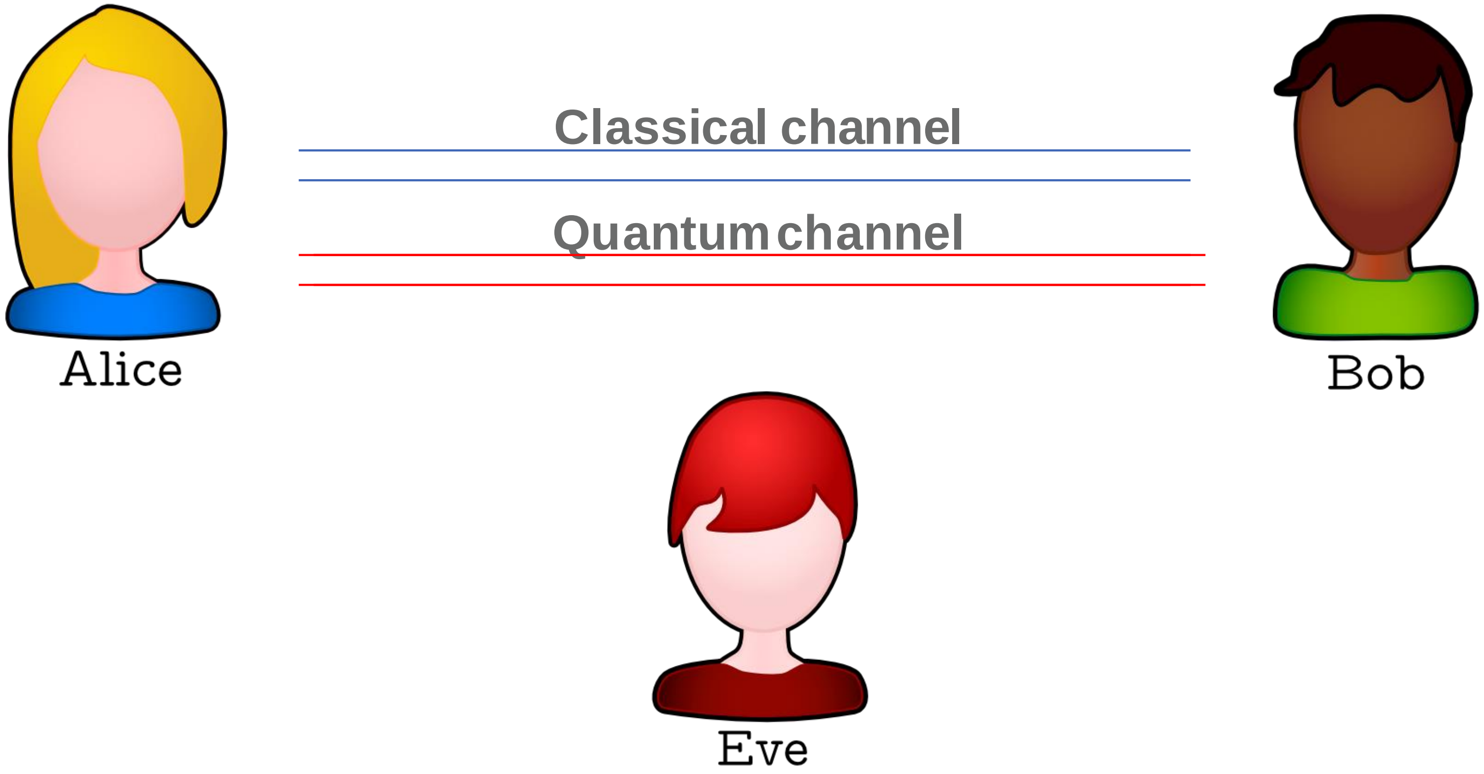
Alice basis (b)	Encoding (a)	q-ch	Bob basis (b')	Bob result	Decoding (a')	public-ch
Z	$0 \leftrightarrow \|0\rangle$	$\rightsquigarrow$	Z	$\|0\rangle,\ \Pr = 1$	0	OK
			X	$\|+\rangle,\ \Pr = 1/2$	0	-
			X	$\|-\rangle,\ \Pr = 1/2$	1	-
Z	$1 \leftrightarrow \|1\rangle$	$\rightsquigarrow$	Z	$\|1\rangle,\ \Pr = 1$	1	OK
			X	$\|+\rangle,\ \Pr = 1/2$	0	-
			X	$\|-\rangle,\ \Pr = 1/2$	1	-
X	$0 \leftrightarrow \|+\rangle$	$\rightsquigarrow$	Z	$\|0\rangle,\ \Pr = 1/2$	0	-
			Z	$\|1\rangle,\ \Pr = 1/2$	1	-
			X	$\|+\rangle,\ \Pr = 1$	0	OK
X	$1 \leftrightarrow \|-\rangle$	$\rightsquigarrow$	Z	$\|0\rangle,\ \Pr = 1/2$	0	-
			Z	$\|1\rangle,\ \Pr = 1/2$	1	-
			X	$\|-\rangle,\ \Pr = 1$	1	OK

Quantum Key Distribution (QKD)

Alice basis (b)	Encoding (a)	q-ch	Bob basis (b')	Bob result	Decoding (a')	public-ch
Z	$0 \leftrightarrow \|0\rangle$	$\rightsquigarrow$	Z	$\|0\rangle,\ \Pr = 1$	0	OK
			X	$\|+\rangle,\ \Pr = 1/2$	0	-
			X	$\|-\rangle,\ \Pr = 1/2$	1	-
Z	$1 \leftrightarrow \|1\rangle$	$\rightsquigarrow$	Z	$\|1\rangle,\ \Pr = 1$	1	OK
			X	$\|+\rangle,\ \Pr = 1/2$	0	-
			X	$\|-\rangle,\ \Pr = 1/2$	1	-
X	$0 \leftrightarrow \|+\rangle$	$\rightsquigarrow$	Z	$\|0\rangle,\ \Pr = 1/2$	0	-
			Z	$\|1\rangle,\ \Pr = 1/2$	1	-
			X	$\|+\rangle,\ \Pr = 1$	0	OK
X	$1 \leftrightarrow \|-\rangle$	$\rightsquigarrow$	Z	$\|0\rangle,\ \Pr = 1/2$	0	-
			Z	$\|1\rangle,\ \Pr = 1/2$	1	-
			X	$\|-\rangle,\ \Pr = 1$	1	OK

Quantum Key Distribution (QKD)

Let's imagine that Eve wants to intercept the secret key.
Eve opts for an "Intercept-Resending" strategy in which she intercepts the qubit sent by Alice and measures it. She then sends back to Bob the state she measured.



Quantum Key Distribution (QKD)

Alice	q-ch	Eve	Eve result	q-ch	Bob	Bob result	Pr
$0 \leftrightarrow \|0\rangle$	$\rightsquigarrow$	$Z,\ \Pr = 1/2$	$\|0\rangle,\ \Pr = 1$	$\rightsquigarrow$	Z	$\|0\rangle \leftrightarrow 0,\ \Pr = 1$	$1/2$
		$X,\ \Pr = 1/2$	$\|+\rangle,\ \Pr = 1/2$	$\rightsquigarrow$	Z	$\|0\rangle \leftrightarrow 0,\ \Pr = 1/2$	$1/8$
			$\|+\rangle,\ \Pr = 1/2$	$\rightsquigarrow$	Z	$\|1\rangle \leftrightarrow 1,\ \Pr = 1/2$	$1/8$
		$X,\ \Pr = 1/2$	$\|-\rangle,\ \Pr = 1/2$	$\rightsquigarrow$	Z	$\|0\rangle \leftrightarrow 0,\ \Pr = 1/2$	$1/8$
			$\|-\rangle,\ \Pr = 1/2$	$\rightsquigarrow$	Z	$\|1\rangle \leftrightarrow 1,\ \Pr = 1/2$	$1/8$

- **If Eve uses the same basis used by Alice, then she can perfectly understand the bit encoded by Alice, which will then be the same bit measured by Bob (if he also measures in the correct basis)**

- **If Eve uses a different basis from the one used by Alice, then her bit will be random and so will the one measured by Bob.**

Quantum Key Distribution (QKD)

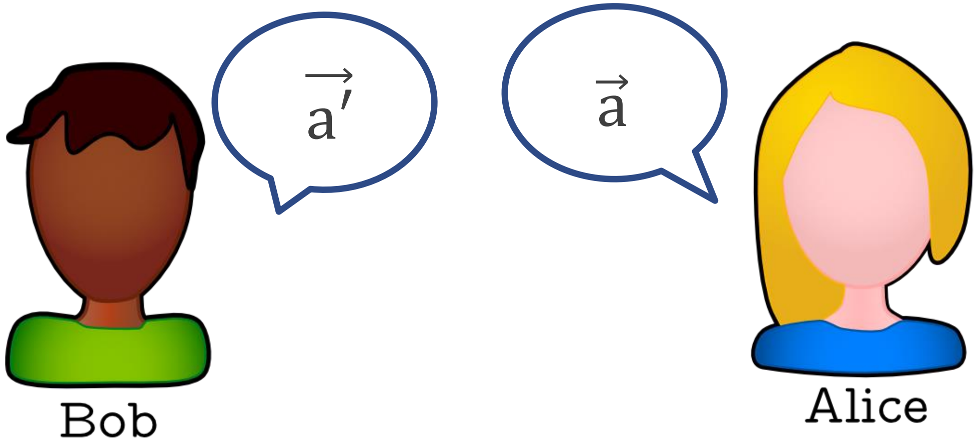
If Eve uses a different basis from the one used by Alice, then its bit will be random as well as the bit measured by Bob

Eve destroys the state if she doesn't measure in the correct basis

Quantum Key Distribution (QKD)

If Eve uses a different basis from that used by Alice, then its bit will be random as well as that measured by Bob

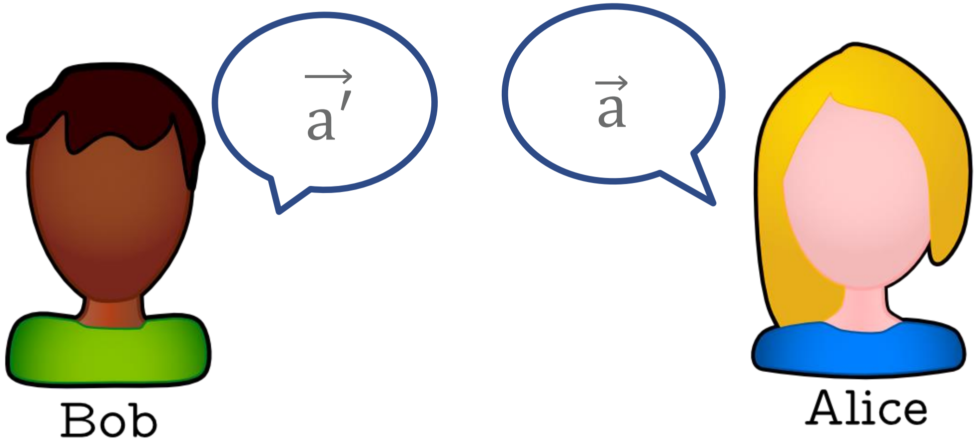
Eve destroys the state if she doesn't measure in the correct basis



Alice and Bob extract part of the secret key and make it public

Quantum Key Distribution (QKD)

Alice	q-ch	Eve	Eve result	q-ch	Bob	Bob result	Pr
$0 \leftrightarrow \|0\rangle$	$\rightsquigarrow$	$Z,\ \mathrm{Pr} = 1/2$	$\|0\rangle,\ \mathrm{Pr} = 1$	$\rightsquigarrow$	Z	$\|0\rangle \leftrightarrow 0,\ \mathrm{Pr} = 1$	$1/2$
		$X,\ \mathrm{Pr} = 1/2$	$\|+\rangle,\ \mathrm{Pr} = 1/2$	$\rightsquigarrow$	Z	$\|0\rangle \leftrightarrow 0,\ \mathrm{Pr} = 1/2$	$1/8$
			$\|+\rangle,\ \mathrm{Pr} = 1/2$	$\rightsquigarrow$	Z	$\|1\rangle \leftrightarrow 1,\ \mathrm{Pr} = 1/2$	$1/8$
		$X,\ \mathrm{Pr} = 1/2$	$\|-\rangle,\ \mathrm{Pr} = 1/2$	$\rightsquigarrow$	Z	$\|0\rangle \leftrightarrow 0,\ \mathrm{Pr} = 1/2$	$1/8$
			$\|-\rangle,\ \mathrm{Pr} = 1/2$	$\rightsquigarrow$	Z	$\|1\rangle \leftrightarrow 1,\ \mathrm{Pr} = 1/2$	$1/8$



If (asymptotically) ¼ of the bits of the public secret key are different, then they can claim that Eve is spying on them

Quantum Key Distribution (QKD)

QKD Experiments:

- 2015 Longest distance QKD for optical fiber (approx 300Km) achieved by University of Geneve
- 2017 University of Waterloo achieved the QKD between a ground transmitter and an aircraft
- 2017 University of Science and Technology of China performed experiments at space scale

QKD Systems in the market

- ID Quantique (Geneva)
- MagiQ Technologies, Inc. (New York)
- QuintessenceLabs (Australia)
- SeQureNet (Paris)

QKD Networks

- DARPA
- SECOQC
- SWISS QUANTUM
- CHINESE NET
- TOKYO NET
- Los Alamos National Lab

Quantum Cryptography

Quantum creates the problem but also provides the solution

Quantum Mechanics

Shor Quantum Algorithm

Breaks RSA cryptograpy

Quantum Cryptography (QKD)

Secure quantum communication

Quantum Key Distribution (QKD)

Quantum creates the problem but also provides the solution

Quantum Mechanics

Shor Quantum Algorithm → Breaks RSA cryptograpy

Quantum Cryptography (QKD) → Secure quantum communication

Post-Quantum Cryptography

Symmetric cryptographic algorithms and hash functions are considered safe from attacks by quantum computers.

- **Lattice-based cryptography**
- **Multivariate cryptography**
- **Hash-based cryptography**

NIST Call for standardization

https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

Quantum Computing @ CINECA

CINECA: Italian HPC center

CINECA Quantum Computing Lab:

- Research with Universities, Industries and QC startups
- Internship programs, Courses and Conference (HPCQC)

https://www.quantumcomputinglab.cineca.it

r.mengoni@cineca.it