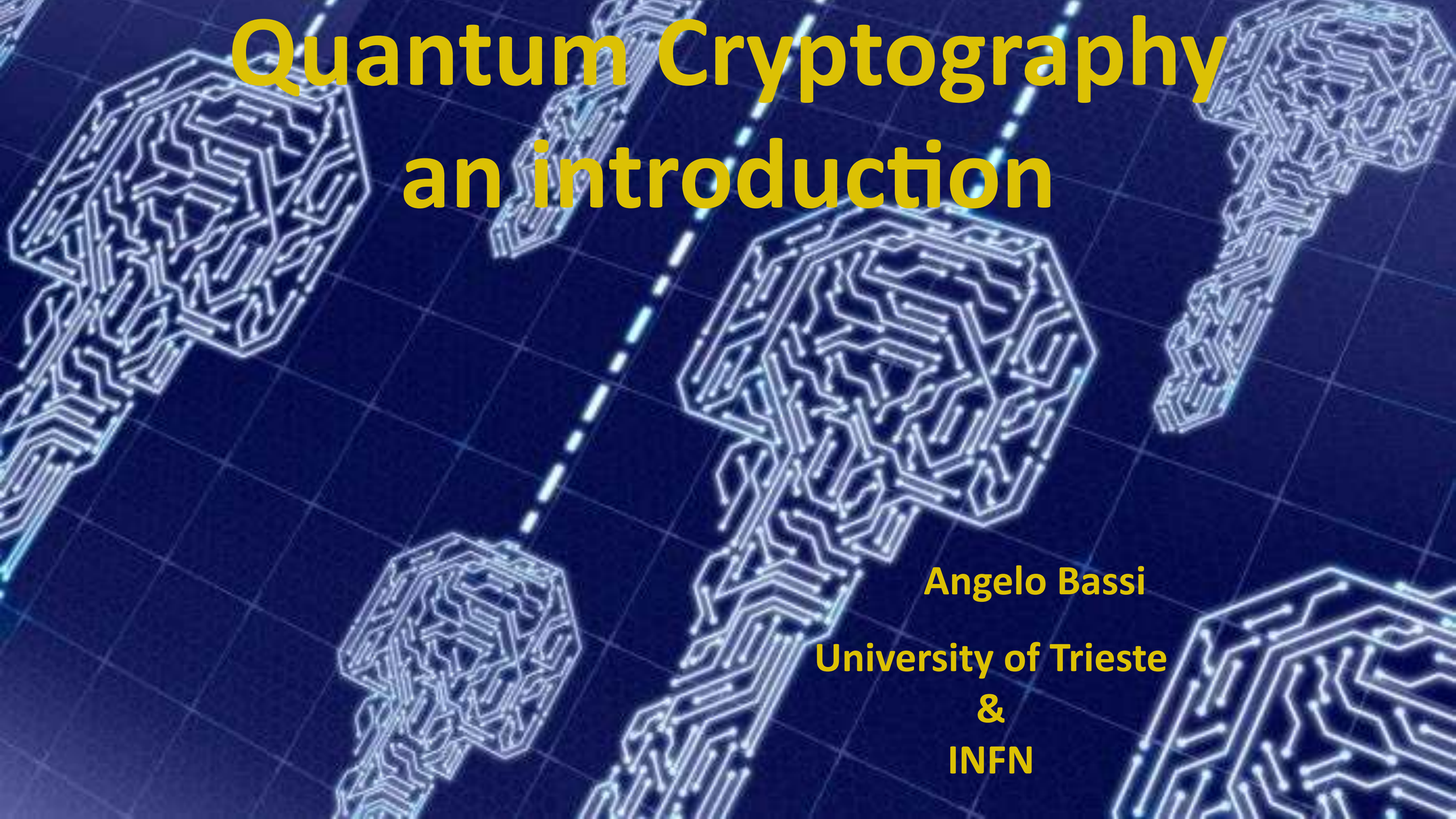
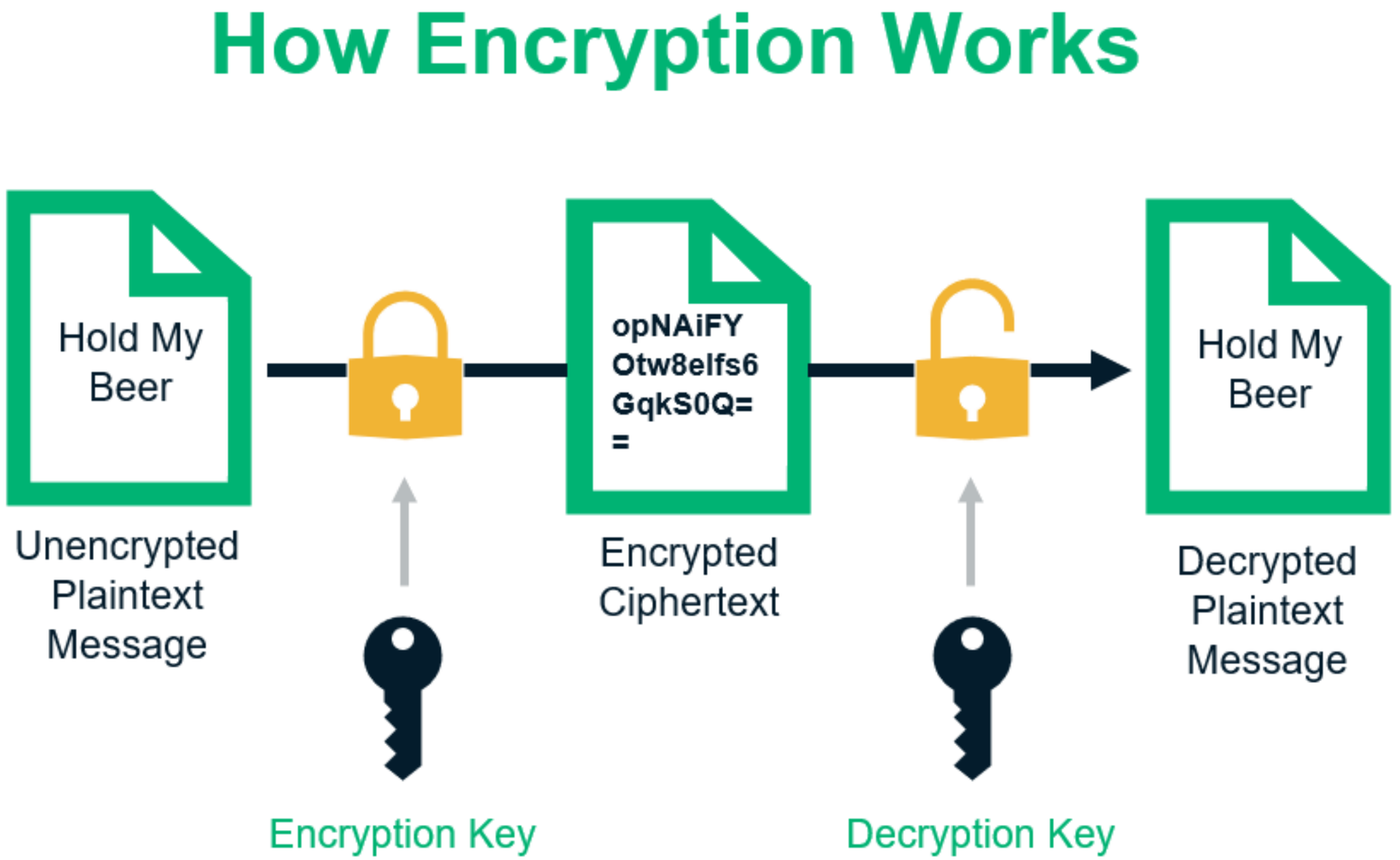
Quantum Cryptography an introduction



Angelo Bassi

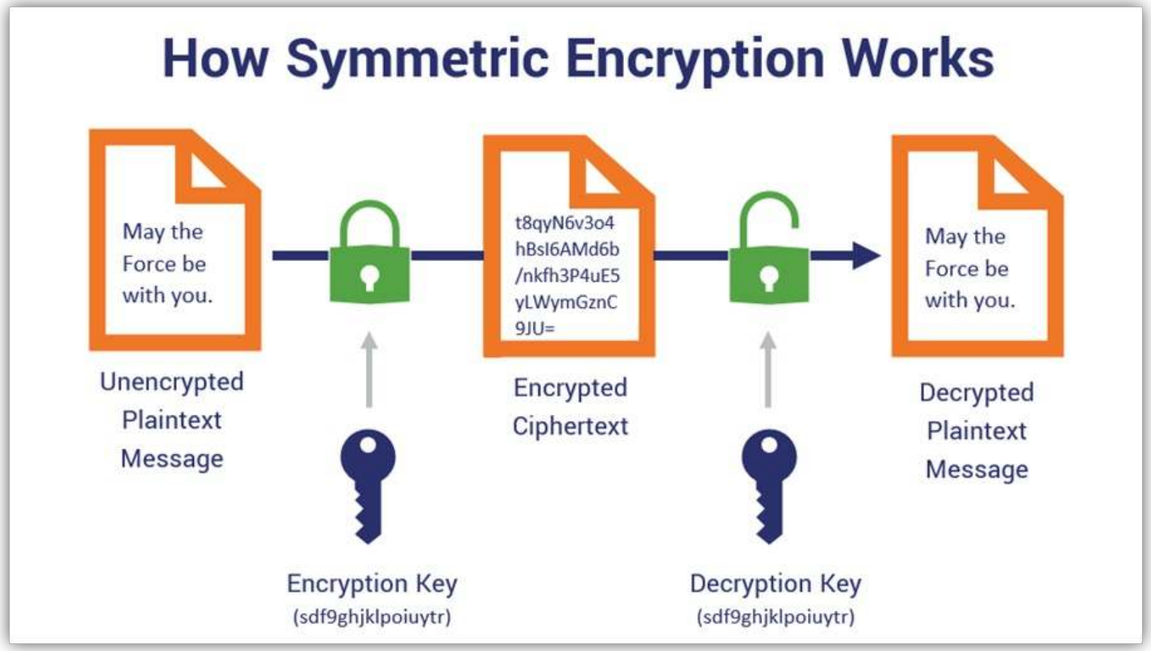
University of Trieste
&
INFN

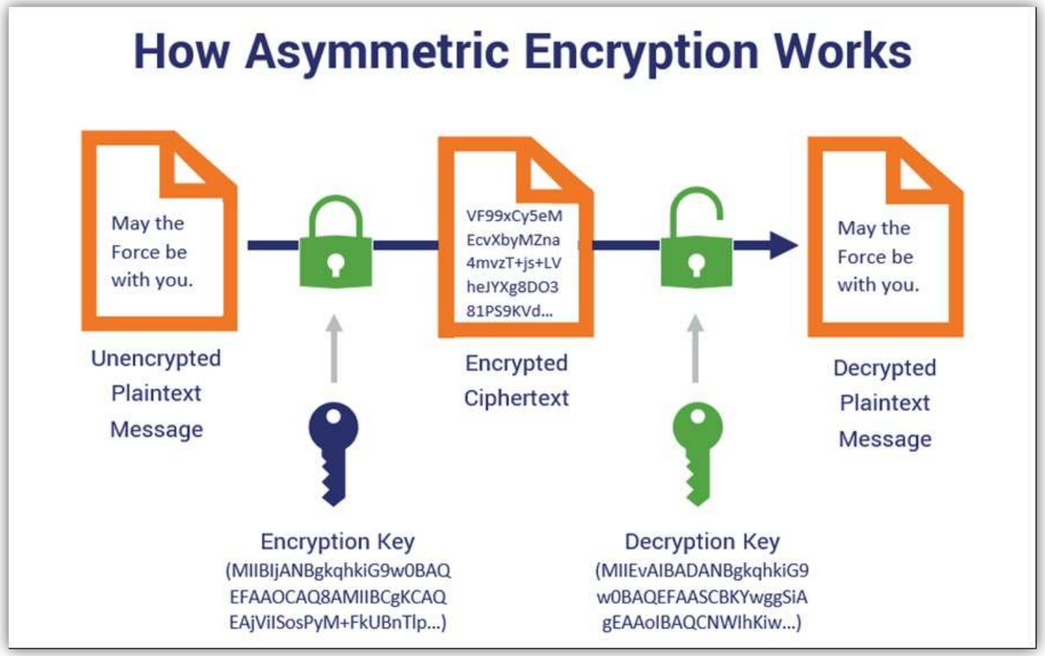
Cryptography



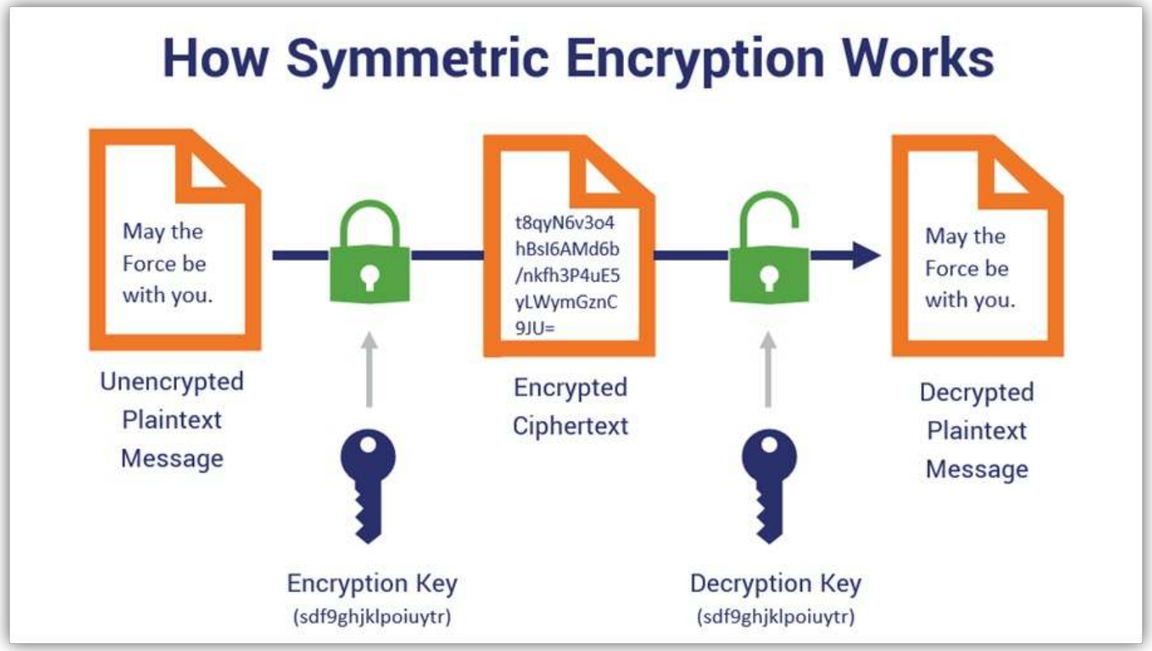
Cryptography

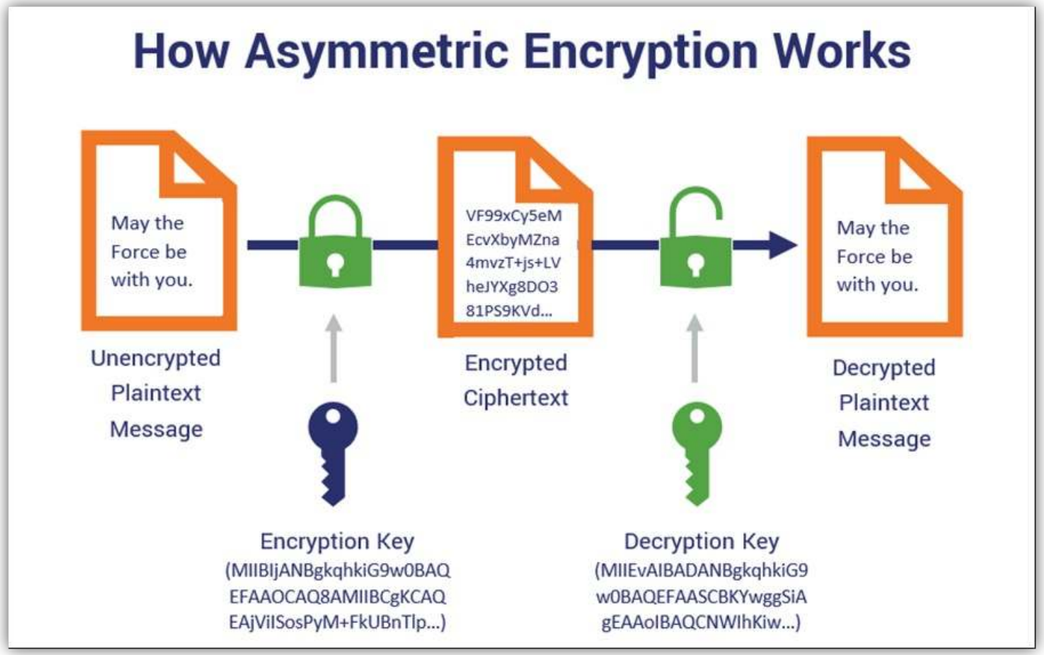
Two major branches: symmetric cryptography & asymmetric cryptography





Advantages & Disadvantages





\+ One-time pad: provably secure
\- Difficult to implement

\+ Easier to implement
\- Vulnerable to attacks

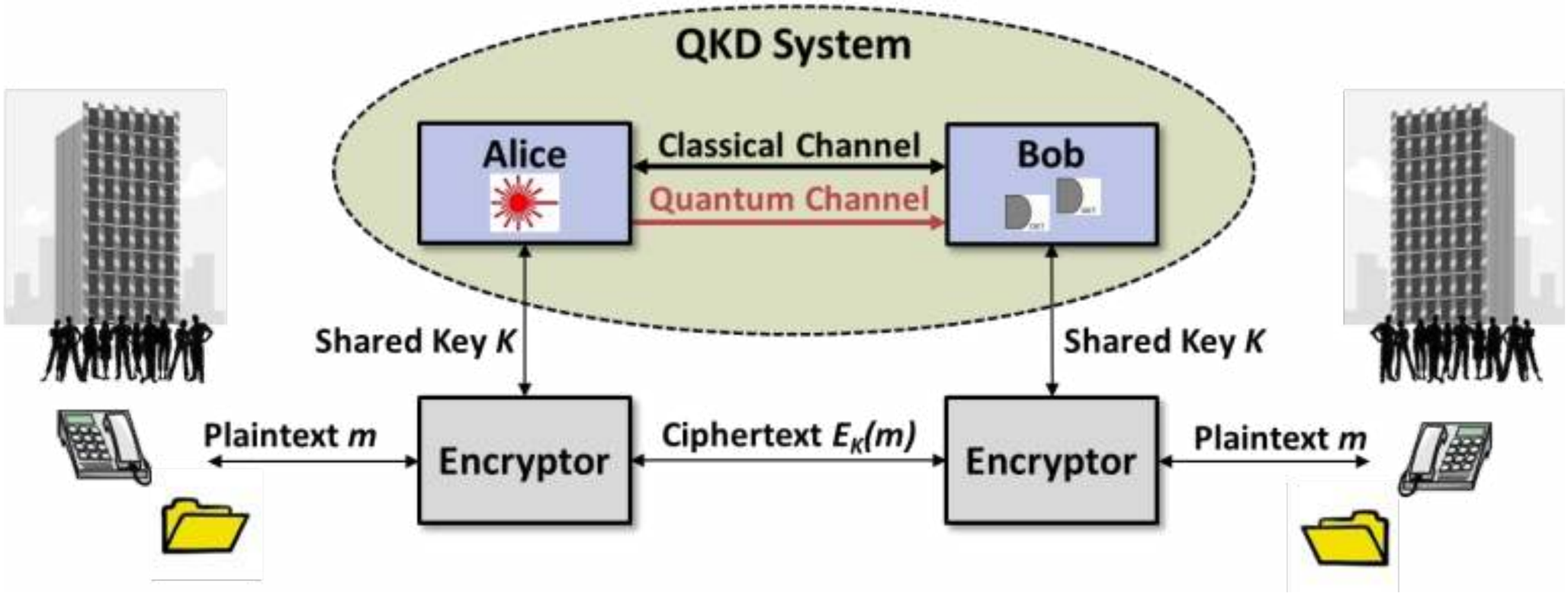
The Quantum way

The key issue is the **distribution** of the keys among the two parties

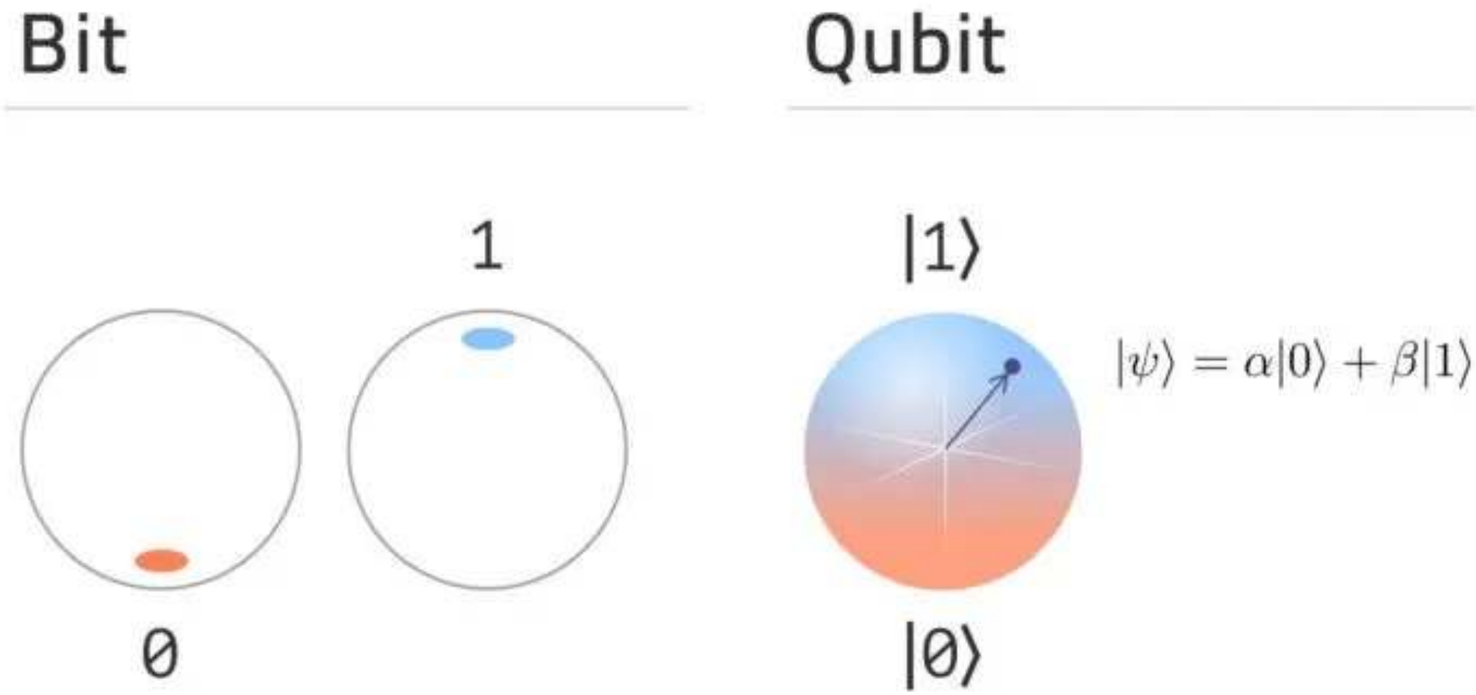
Quantum physics allows for a provably secure way of distributing the cryptographic keys for implementing symmetric cryptograph

This is called **Quantum Key Distribution- QKD**

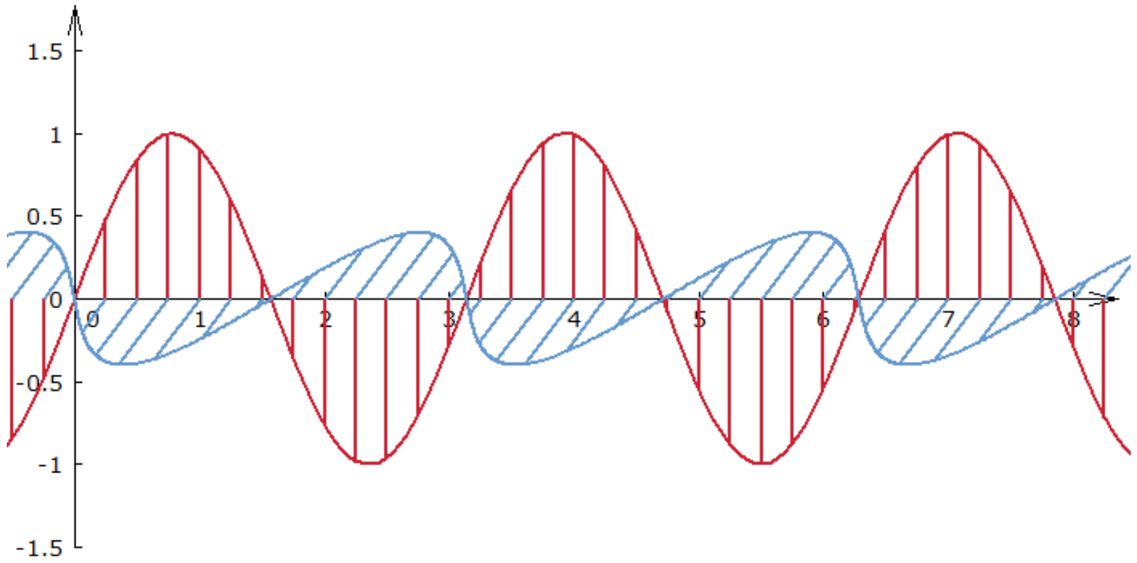
Quantum Key Distribution



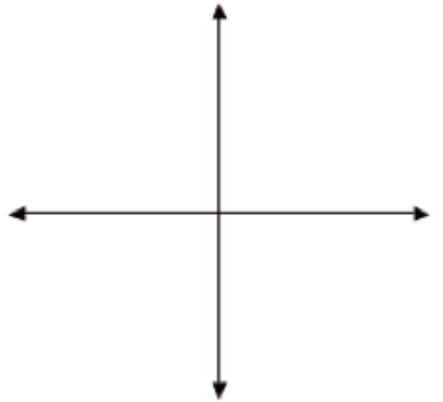
QM essential 1: the Qubit



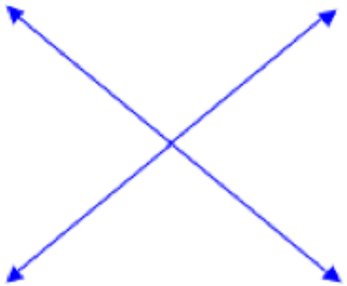
QM essential 1: Photons



Linearly polarized light



Horizontal and vertical polarization



Polarization at 45° and 135°

QKD- BB84

Two ways to encode the bit

Rectilinear basis

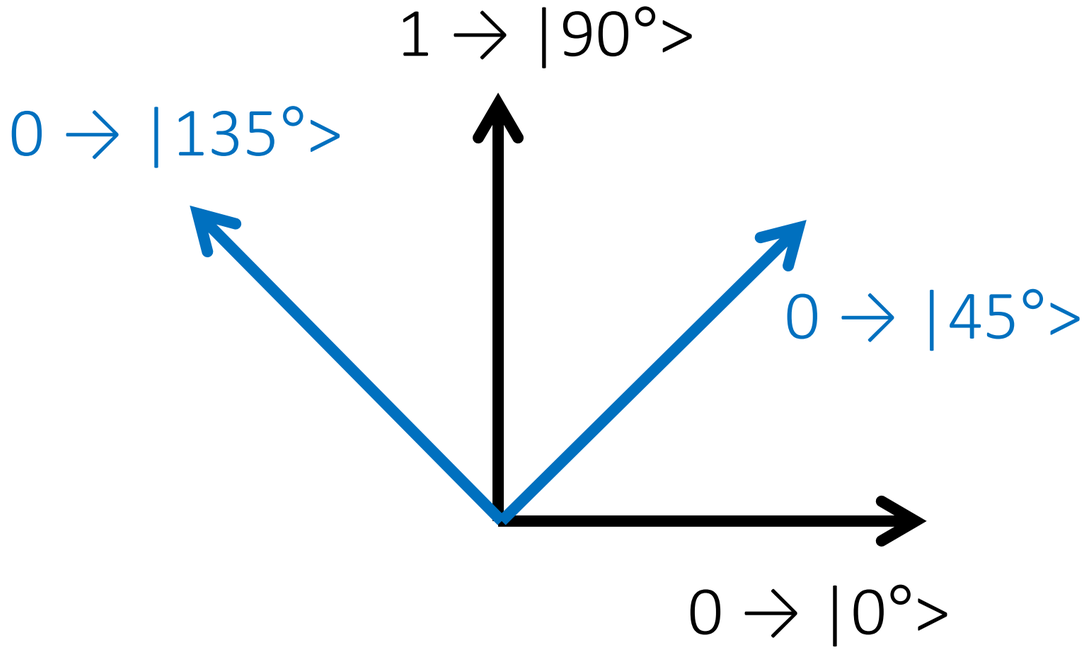
$0 \rightarrow |0°\rangle$

$1 \rightarrow |90°\rangle$

Diagonal basis

$0 \rightarrow |45°\rangle$

$1 \rightarrow |135°\rangle$



QKD- BB84

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

Alice: random sequence of bit	0	1	1	0	1	0	0	1

QKD - BB84

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

2. For each bit, Alice chooses randomly the basis to encode it.

Alice: random sequence of bit	0	1	1	0	1	0	0	1
Alice: random sequence of bases	+	+	×	+	×	×	×	+

QKD - BB84

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

2. For each bit, Alice chooses randomly the basis to encode it.

3. Alice encodes the bit in the polarization and sends the photon to Bob.

Alice: random sequence of bit	0	1	1	0	1	0	0	1
Alice: random sequence of bases	+	+	×	+	×	×	×	+
Alice: encoding of the bits	→	↑	↖	→	↖	↗	↗	↑

QKD - BB84

4. Bob choses a basis for measuring the polarization.

Alice: random sequence of bit	0	1	1	0	1	0	0	1
Alice: random sequence of bases	+	+	×	+	×	×	×	+
Alice: encoding of the bits	→	↑	↖	→	↖	↗	↗	↑
Bob: random sequence of bases	+	×	×	×	+	×	+	+

QKD - BB84

4. Bob choses a basis for measuring the polarization.

5. Bob measures the polarization in the chosen basis.

Alice: random sequence of bit	0	1	1	0	1	0	0	1
Alice: random sequence of bases	+	+	×	+	×	×	×	+
Alice: encoding of the bits	→	↑	↖	→	↖	↗	↗	↑
Bob: random sequence of bases	+	×	×	×	+	×	+	+
Bob: polarization measurement	→	↗	↖	↖	↑	↗	→	↑

QKD - BB84

6. Alice and Bob compare through a public (unsecure) channel their choices of bases.

Alice: random sequence of bit	0	1	1	0	1	0	0	1
Alice: random sequence of bases	+	+	×	+	×	×	×	+
Alice: encoding of the bits	→	↑	↖	→	↖	↗	↗	↑
Bob: random sequence of bases	+	×	×	×	+	×	+	+
Bob: polarization measurement	→	↗	↖	↖	↑	↗	→	↑
Alice & Bob: discussion	Ok	No	Ok	No	No	Ok	No	Ok

QKD - BB84

6. Alice and Bob compare through a public (unsecure) channel their choices of bases.

7. Alice and Bob retain only those cases where they made the same choice of basis (50%).

Alice: random sequence of bit	0	1	1	0	1	0	0	1
Alice: random sequence of bases	+	+	×	+	×	×	×	+
Alice: encoding of the bits	→	↑	↖	→	↖	↗	↗	↑
Bob: random sequence of bases	+	×	×	×	+	×	+	+
Bob: polarization measurement	→	↗	↖	↖	↑	↗	→	↑
Alice & Bob: discussion	Ok	No	Ok	No	No	Ok	No	Ok

QKD - BB84

8. Bob converts the outcome of the measurement in bits.

9. Alice and Bob possess two copies of the same key.

Alice: random sequence of bit	0	1	1	0	1	0	0	1
Alice: random sequence of bases	+	+	×	+	×	×	×	+
Alice: encoding of the bits	→	↑	↖	→	↖	↗	↗	↑
Bob: random sequence of bases	+	×	×	×	+	×	+	+
Bob: polarization measurement	→	↗	↖	↖	↑	↗	→	↑
Alice & Bob: discussion	Ok	No	Ok	No	No	Ok	No	Ok
Bob: outcomes in bits	0		1			0		1

An eavesdropper?

According to the rules of QM, Eve can do only two things:

- Interactions
- Measurements

Interactions

Eve aims at inferring the polarizations, without being noticed.

- She cannot steal the photons (this is why single photons are used)
- She can try to copy the photons' state

Cloning photons’ states?

Alice’s choice
of basis

+

×

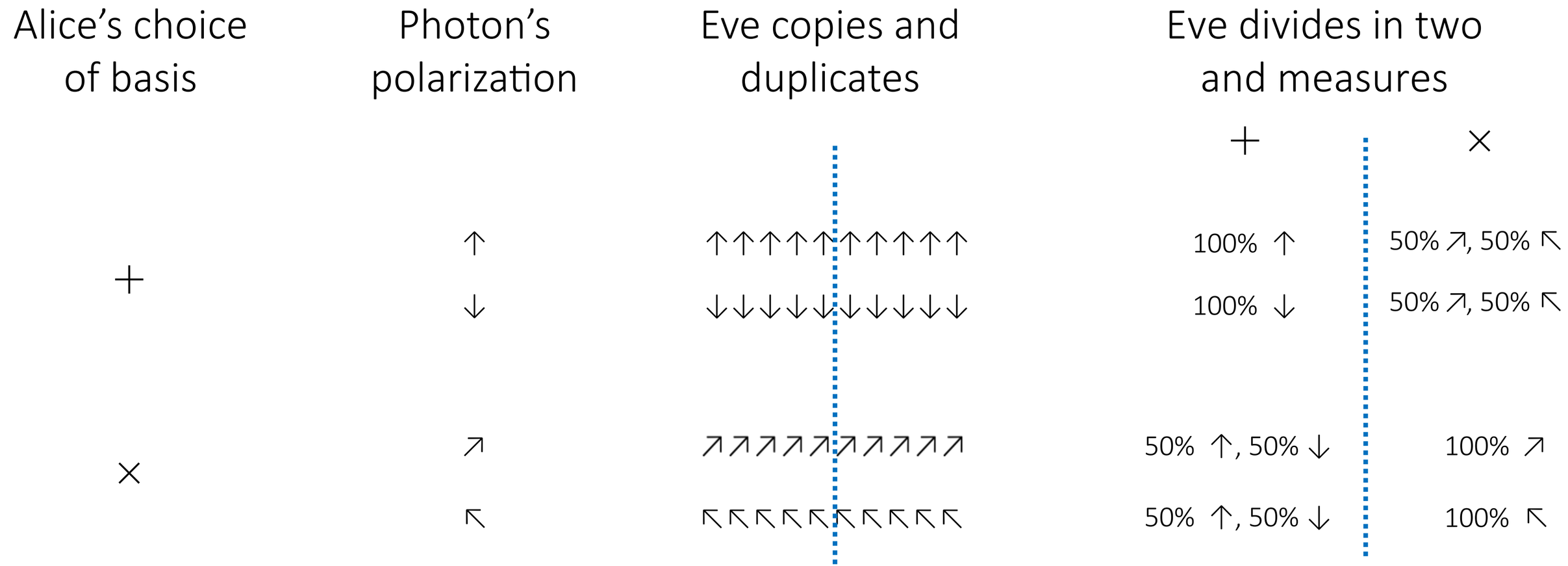
Cloning photons’ states?

Alice’s choice of basis	Photon’s polarization
+	↑
	↓
×	↗
	↖

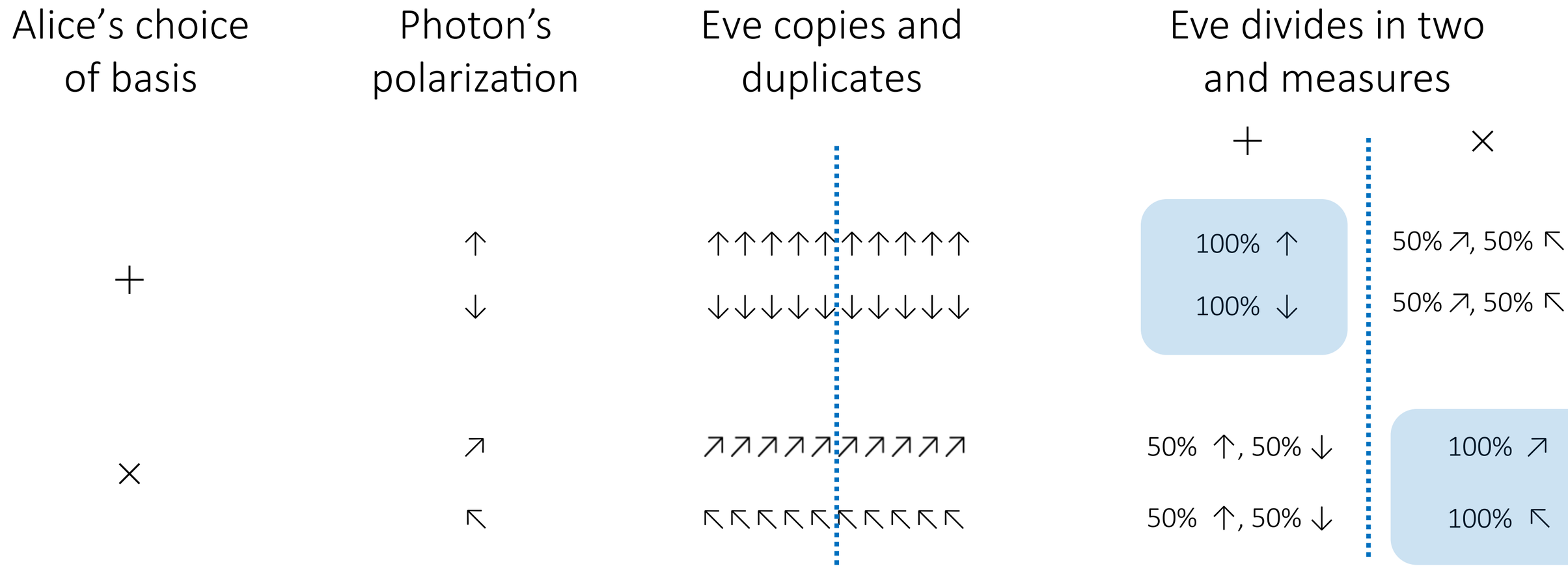
Cloning photons’ states?

Alice’s choice of basis	Photon’s polarization	Eve copies and duplicates
+	↑	↑↑↑↑↑↑↑↑↑↑
	↓	↓↓↓↓↓↓↓↓↓↓
×	↗	↗↗↗↗↗↗↗↗↗↗
	↖	↖↖↖↖↖↖↖↖↖↖

Cloning photons' states?



Cloning photons' states?



Cloning photons' states?

If Eve can copy the states, she can infer them without being noticed.

Actually (and this was the first application of the copying machine) if cloning were possible, one could use quantum entanglement for faster than light signaling.

However, universal cloning is not possible.

No cloning theorem

Consider a unitary operator U such that:

$$U|\psi\rangle \otimes |s\rangle \rightarrow |\psi\rangle \otimes |\psi\rangle \qquad \forall \psi \in \mathcal{H}$$

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

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

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 not possible to copy arbitrary non-orthogonal states.

Eve and cloning

Alice's choice of basis	Photon's polarization	Eve copies and duplicates	Eve divides in two and measures	
			+	×
+	$\|\uparrow\rangle$	$\|\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\rangle$	100% ↑	50% ↗, 50% ↖
	$!\downarrow\rangle$	$\|\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\rangle$	100% ↓	50% ↗, 50% ↖
×	$\|\nearrow\rangle = \|\uparrow\rangle + \|\downarrow\rangle$	$\|\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\rangle + \|\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\rangle$	100% ↑	50% ↗, 50% ↖
	$\|\nwarrow\rangle = \|\uparrow\rangle - \|\downarrow\rangle$	$\|\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\rangle - \|\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\rangle$	100% ↓	50% ↗, 50% ↖

Normalization factors have been omitted

Eve and cloning

Eve can clone only orthogonal states (a basis). Then the action of the machine on all other states is governed by the unitarity of the evolution.

It is not possible for Eve to understand in which states the bits have been encoded.

Measurements

Assume that Eve tries to directly measure the photon’s state, by randomly choosing the horizontal or diagonal basis.

Measurements

Assume that Eve tries to directly measure the photon's state, by randomly choosing the horizontal or diagonal basis.

Alice's choice of basis	Photon's polarization	Eve measures in one of the two bases
+	→	50% +
		50% ×

Measurements

Assume that Eve tries to directly measure the photon's state, by randomly choosing the horizontal or diagonal basis.

Alice's choice of basis	Photon's polarization	Eve measures in one of the two bases
+	→	50% + 100% →
		50% × 50% ↗, 50% ↖

Measurements

Assume that Eve tries to directly measure the photon's state, by randomly choosing the horizontal or diagonal basis.

Alice's choice of basis	Photon's polarization	Eve measures in one of the two bases	Bob measures in the same basis as Alice
+	→	50% + : 100% → 50% × : 50% ↗, 50% ↖	100% → 50% → , 50% ↖

Measurements

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

Measurements

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

Then 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

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

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

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

Measurements

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

QKD- Physical realization

There are essentially two ways to realize QKD

- Optical fibers (about 100 Km because of photon loss)
- Free space (via satellite)

QKD- Physical realization

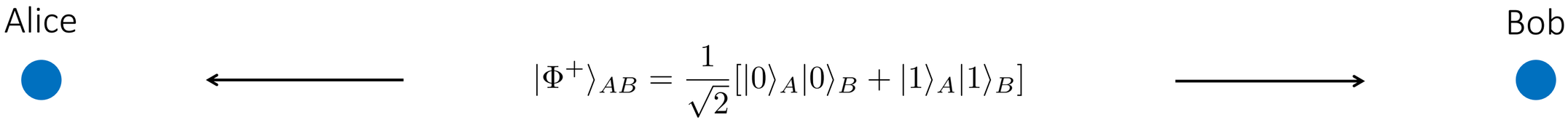
There are essentially two ways to realize QKD

- Optical fibers (about 100 Km because of photon loss)
- Free space (via satellite)

To increase distances on ground, one needs a quantum repeater (classical repeaters don’t work)

Quantum Teleportation

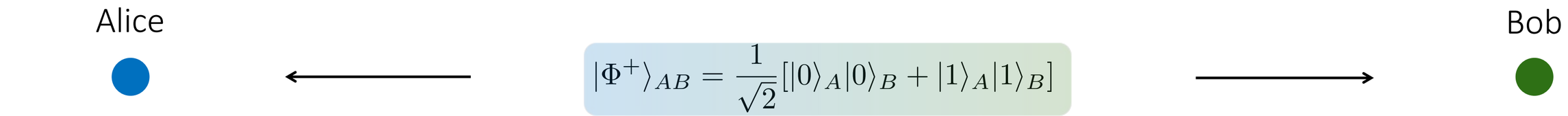
The protocol aims at the following



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

Alice and Bob share an entangled state, and through this Alice wants to transmit her state to Bob

Quantum Teleportation



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

Simple calculations show that

$$\begin{aligned}
|\psi\rangle_C|\Phi^+\rangle_{AB} &= [\alpha|0\rangle_C + \beta|1\rangle_C]\frac{1}{\sqrt{2}}[|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B] \\
&= \frac{1}{2}[|\Phi^+\rangle_{CA}(\alpha|0\rangle_B + \beta|1\rangle_B) + |\Phi^-\rangle_{CA}(\alpha|0\rangle_B - \beta|1\rangle_B) \\
&\quad + |\Psi^+\rangle_{CA}(\alpha|1\rangle_B + \beta|0\rangle_B) + |\Psi^-\rangle_{CA}(\alpha|1\rangle_B - \beta|0\rangle_B)]
\end{aligned}$$

Quantum Teleportation

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

Alices measures her two photons in the states $|\Phi^+\rangle_{CA}, |\Phi^-\rangle_{CA}, |\Psi^+\rangle_{CA}, |\Psi^-\rangle_{CA}$

There are four possible outcomes, each with probability 1/4:

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

Quantum Teleportation

Depending on the outcome, Alice tells Bob (over a classical unsecure channel) to perform the following operations

$\|\Phi^+\rangle_{CA}(\alpha\|0\rangle_B + \beta\|1\rangle_B)$	→	Do nothing
$\|\Phi^-\rangle_{CA}(\alpha\|0\rangle_B - \beta\|1\rangle_B)$	→	Change the sign of $\|1\rangle$
$\|\Psi^+\rangle_{CA}(\alpha\|1\rangle_B + \beta\|0\rangle_B)$	→	Exchange $\|0\rangle$ and $\|1\rangle$
$\|\Psi^-\rangle_{CA}(\alpha\|1\rangle_B - \beta\|0\rangle_B)$	→	Exchange $\|0\rangle$ and $\|1\rangle$ & change the sign of $\|1\rangle$

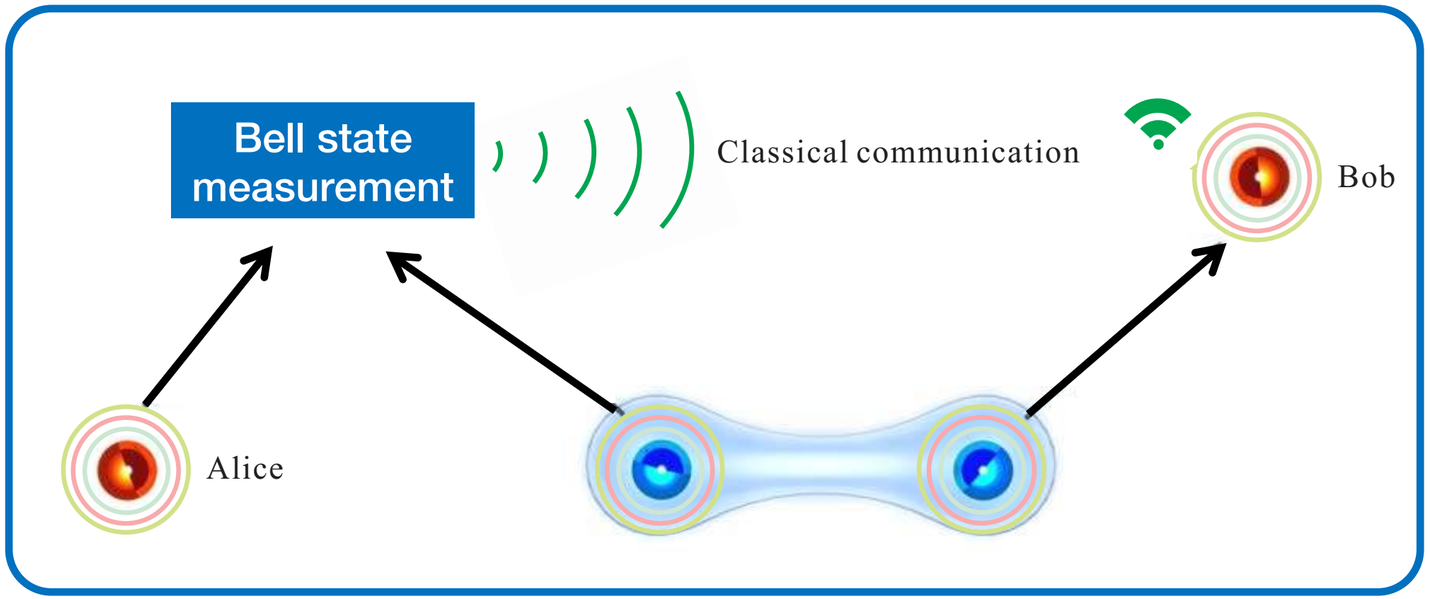
In the end, Bob will end up with his photon being in the state $\alpha|0\rangle_B + \beta|1\rangle_B$

Quantum Teleportation

- The state of Alice's photon is not transferred through space to Bob's photon. It appears "instantly" on the other side. This is because Alice and Bob share an entangled state.

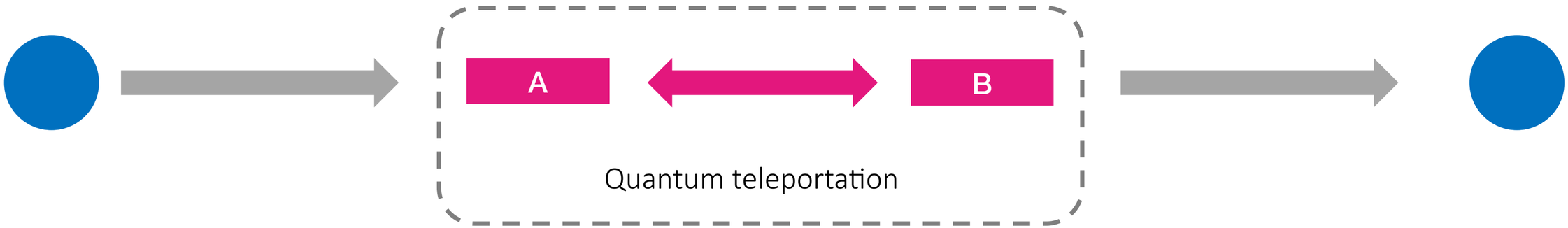
- The classical communication does not reveal anything about the state being teleported.

- The whole process does not occur faster than light.



Quantum Repeater

For long distances, one can break up the path in smaller segments



Thank you for the attention