

Quantum Cyber Security

Lecture 17: Properties of Quantum Systems and Cryptography

Petros Wallden

University of Edinburgh

25th March 2025



- **Indistinguishability:** theorem and implication
- **No-cloning:** theorem and implication
- **Monogamy of Entanglement:** theorem, implications and measures of entanglement
- **Teleportation:** what it is and its relation to Quantum One-Time Pad

Distinguishing Pure Quantum States

- Assume a fixed set of possible states $\{|\psi_1\rangle, \dots, |\psi_n\rangle\}$
- Alice chooses one of these states $|\psi_i\rangle$ and sends it to Bob

Distinguishing Pure Quantum States

- Assume a fixed set of possible states $\{|\psi_1\rangle, \dots, |\psi_n\rangle\}$
- Alice chooses one of these states $|\psi_i\rangle$ and sends it to Bob
- **Challenge:** Bob to find the index $i \in \{1, \dots, n\}$ (can make any measurement)

Distinguishing Pure Quantum States

- Assume a fixed set of possible states $\{|\psi_1\rangle, \dots, |\psi_n\rangle\}$
- Alice chooses one of these states $|\psi_i\rangle$ and sends it to Bob
- **Challenge:** Bob to find the index $i \in \{1, \dots, n\}$ (can make any measurement)

Case I: States $|\psi_i\rangle$ are orthogonal, i.e. $\langle \psi_i | \psi_j \rangle = \delta_{ij}$

We perform a (projective) measurement that consist of the following operators

$$P_i = |\psi_i\rangle \langle \psi_i| \text{ and } P_0 = \mathbb{I} - \sum_i |\psi_i\rangle \langle \psi_i|$$

Distinguishing Pure Quantum States

- Assume a fixed set of possible states $\{|\psi_1\rangle, \dots, |\psi_n\rangle\}$
- Alice chooses one of these states $|\psi_i\rangle$ and sends it to Bob
- **Challenge:** Bob to find the index $i \in \{1, \dots, n\}$ (can make any measurement)

Case I: States $|\psi_i\rangle$ are orthogonal, i.e. $\langle\psi_i|\psi_j\rangle = \delta_{ij}$

We perform a (projective) measurement that consist of the following operators

$$P_i = |\psi_i\rangle\langle\psi_i| \text{ and } P_0 = \mathbb{I} - \sum_i |\psi_i\rangle\langle\psi_i|$$

Exercise: Check that this measurement satisfies the completeness relation

We can see easily that if the state $|\psi_k\rangle$ is prepared, then $p(i) = \langle\psi_k|P_i|\psi_k\rangle = \delta_{ik}$ and therefore Bob finds with probability one the correct index.

Distinguishing Pure Quantum States

Case II: Some of the states are *not* orthogonal

Theorem

Non-orthogonal pure states cannot be distinguished with certainty

Case II: Some of the states are *not* orthogonal

Theorem

Non-orthogonal pure states cannot be distinguished with certainty

Proof by contradiction:

- Consider two non-orthogonal states $\langle \psi_1 | \psi_2 \rangle \neq 0$
- Related to these are two measurement operators (not necessarily projective) $E_1 = M_1^\dagger M_1$ and $E_2 = M_2^\dagger M_2$
- If we can distinguish them perfectly it means that when Alice sends $|\psi_1\rangle$ Bob has $p(i=1) = \langle \psi_1 | E_1 | \psi_1 \rangle = 1$ and when Alice sends $|\psi_2\rangle$ Bob has $p(i=2) = \langle \psi_2 | E_2 | \psi_2 \rangle = 1$

Case II: Some of the states are *not* orthogonal

Theorem

Non-orthogonal pure states cannot be distinguished with certainty

Proof by contradiction:

- Consider two non-orthogonal states $\langle \psi_1 | \psi_2 \rangle \neq 0$
- Related to these are two measurement operators (not necessarily projective) $E_1 = M_1^\dagger M_1$ and $E_2 = M_2^\dagger M_2$
- If we can distinguish them perfectly it means that when Alice sends $|\psi_1\rangle$ Bob has $p(i=1) = \langle \psi_1 | E_1 | \psi_1 \rangle = 1$ and when Alice sends $|\psi_2\rangle$ Bob has $p(i=2) = \langle \psi_2 | E_2 | \psi_2 \rangle = 1$
- From $\sum_i E_i = \mathbb{I}$ and $\langle \psi_1 | E_1 | \psi_1 \rangle = 1$ we conclude that $\langle \psi_1 | E_2 | \psi_1 \rangle = 0$ and thus $\sqrt{E_2} |\psi_1\rangle = 0$

Case II: Some of the states are *not* orthogonal

Theorem

Non-orthogonal pure states cannot be distinguished with certainty

Proof by contradiction:

- Consider two non-orthogonal states $\langle \psi_1 | \psi_2 \rangle \neq 0$
- Related to these are two measurement operators (not necessarily projective) $E_1 = M_1^\dagger M_1$ and $E_2 = M_2^\dagger M_2$
- If we can distinguish them perfectly it means that when Alice sends $|\psi_1\rangle$ Bob has $p(i=1) = \langle \psi_1 | E_1 | \psi_1 \rangle = 1$ and when Alice sends $|\psi_2\rangle$ Bob has $p(i=2) = \langle \psi_2 | E_2 | \psi_2 \rangle = 1$
- From $\sum_i E_i = \mathbb{I}$ and $\langle \psi_1 | E_1 | \psi_1 \rangle = 1$ we conclude that $\langle \psi_1 | E_2 | \psi_1 \rangle = 0$ and thus $\sqrt{E_2} |\psi_1\rangle = 0$
Since the two states are non-orthogonal we can write $|\psi_2\rangle = \alpha |\psi_1\rangle + \beta |\phi\rangle$ where $\langle \psi_1 | \phi \rangle = 0$ is a unit vector

Case II: Some of the states are *not* orthogonal

Theorem

Non-orthogonal pure states cannot be distinguished with certainty

Proof by contradiction:

- Consider two non-orthogonal states $\langle \psi_1 | \psi_2 \rangle \neq 0$
- Related to these are two measurement operators (not necessarily projective) $E_1 = M_1^\dagger M_1$ and $E_2 = M_2^\dagger M_2$
- If we can distinguish them perfectly it means that when Alice sends $|\psi_1\rangle$ Bob has $p(i=1) = \langle \psi_1 | E_1 | \psi_1 \rangle = 1$ and when Alice sends $|\psi_2\rangle$ Bob has $p(i=2) = \langle \psi_2 | E_2 | \psi_2 \rangle = 1$
- From $\sum_i E_i = \mathbb{I}$ and $\langle \psi_1 | E_1 | \psi_1 \rangle = 1$ we conclude that $\langle \psi_1 | E_2 | \psi_1 \rangle = 0$ and thus $\sqrt{E_2} |\psi_1\rangle = 0$

Since the two states are non-orthogonal we can write

$|\psi_2\rangle = \alpha |\psi_1\rangle + \beta |\phi\rangle$ where $\langle \psi_1 | \phi \rangle = 0$ is a unit vector

Then it follows : $\langle \psi_2 | E_2 | \psi_2 \rangle = |\beta|^2 \langle \phi | E_2 | \phi \rangle \leq |\beta|^2 < 1$

which contradicts our assumption \square

- B92 QKD protocol relies on this impossibility.
- One can also bound the probability of distinguishing, which is related with how far from orthogonal are the states.
- In many other quantum communication protocols this property is essential (e.g. some protocols that achieve: Quantum Digital Signatures, Quantum Coin-Flipping, Blind Quantum Computing, etc)

No-cloning Theorem

It is impossible to copy an unknown quantum state

No-cloning Theorem

It is impossible to copy an unknown quantum state

- **Classically** we can copy an (unknown) bit: $\text{CNOT}(a\ 0) = a\ a$

No-cloning Theorem

It is impossible to copy an unknown quantum state

- **Classically** we can copy an (unknown) bit: $\text{CNOT}(a\ 0) = a\ a$
CNOT between unknown bit (control) and the 0 bit (target)

No-cloning Theorem

It is impossible to copy an unknown quantum state

- **Classically** we can copy an (unknown) bit: $\text{CNOT}(a\ 0) = a\ a$
CNOT between unknown bit (control) and the 0 bit (target)
- Does not work in QM:

No-cloning Theorem

It is impossible to copy an unknown quantum state

- **Classically** we can copy an (unknown) bit: $\text{CNOT}(a\ 0) = a\ a$
CNOT between unknown bit (control) and the 0 bit (target)
- **Does not work in QM:**

Unknown state $|\psi\rangle = a|0\rangle + b|1\rangle$ and

$$\wedge X = |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|$$

$$\wedge X |\psi\rangle |0\rangle = a|00\rangle + b|11\rangle$$

which is different than: $|\psi\rangle |\psi\rangle$

No-cloning Theorem

It is impossible to copy an unknown quantum state

- **Classically** we can copy an (unknown) bit: $\text{CNOT}(a\ 0) = a\ a$
CNOT between unknown bit (control) and the 0 bit (target)
- **Does not work in QM:**

Unknown state $|\psi\rangle = a|0\rangle + b|1\rangle$ and

$$\wedge X = |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|$$

$$\wedge X |\psi\rangle |0\rangle = a|00\rangle + b|11\rangle$$

which is different than: $|\psi\rangle |\psi\rangle$

- **No-deleting Theroem:** The “time-reversed” version proves that it is impossible to **delete** a qubit using unitary gates.

No-cloning Theorem (Proof)

Proof: By contradiction. Assume that we could copy:

- Then there exists a unitary:

$$U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle \quad \forall |\psi\rangle$$

No-cloning Theorem (Proof)

Proof: By contradiction. Assume that we could copy:

- Then there exists a unitary:

$$U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle \quad \forall |\psi\rangle$$

- Consider $|\psi_1\rangle, |\psi_2\rangle$ where $\langle\psi_1|\psi_2\rangle = a \neq 1$ or 0

No-cloning Theorem (Proof)

Proof: By contradiction. Assume that we could copy:

- Then there exists a unitary:

$$U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle \quad \forall |\psi\rangle$$

- Consider $|\psi_1\rangle, |\psi_2\rangle$ where $\langle\psi_1|\psi_2\rangle = a \neq 1$ or 0
- Consider an ancilla initialised at $|0\rangle$, and then the inner product between $|\psi_1\rangle \otimes |0\rangle$ and $|\psi_2\rangle \otimes |0\rangle$:

$$(\langle\psi_1| \otimes \langle 0|)(|\psi_2\rangle \otimes |0\rangle) = \langle\psi_1|\psi_2\rangle \langle 0|0\rangle = a \quad (1)$$

No-cloning Theorem (Proof)

Proof: By contradiction. Assume that we could copy:

- Then there exists a unitary:

$$U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle \quad \forall |\psi\rangle$$

- Consider $|\psi_1\rangle, |\psi_2\rangle$ where $\langle\psi_1|\psi_2\rangle = a \neq 1$ or 0
- Consider an ancilla initialised at $|0\rangle$, and then the inner product between $|\psi_1\rangle \otimes |0\rangle$ and $|\psi_2\rangle \otimes |0\rangle$:

$$(\langle\psi_1| \otimes \langle 0|)(|\psi_2\rangle \otimes |0\rangle) = \langle\psi_1|\psi_2\rangle \langle 0|0\rangle = a \quad (1)$$

- Inner products are invariant under any unitary:

$$\begin{aligned} (\langle\psi_1| \otimes \langle 0|)(|\psi_2\rangle \otimes |0\rangle) &= (\langle\psi_1| \otimes \langle 0|)U^\dagger U(|\psi_2\rangle \otimes |0\rangle) \\ &= (\langle\psi_1| \otimes \langle\psi_1|)(|\psi_2\rangle \otimes |\psi_2\rangle) \\ &= \langle\psi_1|\psi_2\rangle \langle\psi_1|\psi_2\rangle = a^2 \end{aligned} \quad (2)$$

No-cloning Theorem (Proof)

Proof: By contradiction. Assume that we could copy:

- Then there exists a unitary:

$$U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle \quad \forall |\psi\rangle$$

- Consider $|\psi_1\rangle, |\psi_2\rangle$ where $\langle\psi_1|\psi_2\rangle = a \neq 1$ or 0
- Consider an ancilla initialised at $|0\rangle$, and then the inner product between $|\psi_1\rangle \otimes |0\rangle$ and $|\psi_2\rangle \otimes |0\rangle$:

$$(\langle\psi_1| \otimes \langle 0|)(|\psi_2\rangle \otimes |0\rangle) = \langle\psi_1|\psi_2\rangle \langle 0|0\rangle = a \quad (1)$$

- Inner products are invariant under any unitary:

$$\begin{aligned} (\langle\psi_1| \otimes \langle 0|)(|\psi_2\rangle \otimes |0\rangle) &= (\langle\psi_1| \otimes \langle 0|)U^\dagger U(|\psi_2\rangle \otimes |0\rangle) \\ &= (\langle\psi_1| \otimes \langle\psi_1|)(|\psi_2\rangle \otimes |\psi_2\rangle) \\ &= \langle\psi_1|\psi_2\rangle \langle\psi_1|\psi_2\rangle = a^2 \end{aligned} \quad (2)$$

- From Eq. (1) and Eq. (2) we have $a = a^2$ possible only if $\langle\psi_1|\psi_2\rangle = 1$ or 0 reaching contradiction \square

- Security of QKD relies on this. If one could copy the BB84 states, then the adversary could measure one copy in each basis, and then compromise the security completely.
- No-Cloning is essential for the indistinguishability too

Q: Can you come up with a way to distinguish states if you had a copying machine?

- Can put a bound on how well one can copy an unknown quantum state – this is used in certain security proofs

The “maximally” entangled states have some unique properties

- 1 **Perfect correlation:** Alice’s and Bob’s results are perfectly correlated in all bases

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle)$$

The “maximally” entangled states have some unique properties

- ① **Perfect correlation:** Alice’s and Bob’s results are perfectly correlated in all bases

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle)$$

This is not the case for “partially” entangled e.g.

$$|\psi\rangle = \sqrt{\frac{2}{3}}|00\rangle + \sqrt{\frac{1}{3}}|11\rangle = \frac{1}{2} \left(\sqrt{\frac{2}{3}}(|+\rangle + |-\rangle)(|+\rangle + |-\rangle) + \sqrt{\frac{1}{3}}(|+\rangle - |-\rangle)(|+\rangle - |-\rangle) \right)$$

which clearly is not perfectly correlated

Monogamy of Entanglement

- ② **Monogamy:** If two qubits are maximally entangled, then they are separable with respect to any third qubit

$$\rho_{AB} = \text{Tr}_E(\rho_{ABE}) = |\Phi^+\rangle_{AB} \langle \Phi^+| \Rightarrow \rho_{ABE} = |\Phi^+\rangle_{AB} \langle \Phi^+| \otimes \rho_E$$

- By knowing A and B are strongly (quantum) correlated, we know that A and B are **not correlated with anything else!**

Monogamy of Entanglement

- ② **Monogamy:** If two qubits are maximally entangled, then they are separable with respect to any third qubit

$$\rho_{AB} = \text{Tr}_E(\rho_{ABE}) = |\Phi^+\rangle_{AB} \langle \Phi^+| \Rightarrow \rho_{ABE} = |\Phi^+\rangle_{AB} \langle \Phi^+| \otimes \rho_E$$

- By knowing A and B are strongly (quantum) correlated, we know that A and B are **not correlated with anything else!**
- Need a measure to quantify how entangled are two subsystems (see later)
- This can be used both to define properly what “**perfect correlation**” means, and to demonstrate that they are **not correlated with third systems**

Implications of Monogamy of Entanglement

- Is the basis for entanglement-based QKD protocols (e.g. BBM92 and E91) security.
- Even for other QKD protocols, their formal security is proven by reduction to entanglement-based protocols.
- Can quantify this since the more quantumly-correlated with one system, the closer it is to being uncorrelated with other systems.

Measure of Entanglement

- Bipartite state ρ_{AB} , how can we measure how entangled it is?

Measure of Entanglement

- Bipartite state ρ_{AB} , how can we measure how entangled it is?
- Assume pure (global) state $\rho_{AB} = |\psi\rangle\langle\psi|_{AB}$
Entanglement Entropy: $S(\rho_A) = -\text{Tr}\rho_A \log \rho_A = S(\rho_B)$,
where ρ_A, ρ_B the reduced density matrices
- This measures entanglement (check that separable states $|\psi_1\rangle_A \otimes |\psi_2\rangle_B$ have zero entanglement entropy)

Measure of Entanglement

- Bipartite state ρ_{AB} , how can we measure how entangled it is?
- Assume pure (global) state $\rho_{AB} = |\psi\rangle\langle\psi|_{AB}$
Entanglement Entropy: $S(\rho_A) = -\text{Tr}\rho_A \log \rho_A = S(\rho_B)$,
where ρ_A, ρ_B the reduced density matrices
- This measures entanglement (check that separable states $|\psi_1\rangle_A \otimes |\psi_2\rangle_B$ have zero entanglement entropy)
- For qubit, maximum entanglement is given by:
 $|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ (check!)

Measure of Entanglement

- Bipartite state ρ_{AB} , how can we measure how entangled it is?
- Assume pure (global) state $\rho_{AB} = |\psi\rangle\langle\psi|_{AB}$
Entanglement Entropy: $S(\rho_A) = -\text{Tr}\rho_A \log \rho_A = S(\rho_B)$,
where ρ_A, ρ_B the reduced density matrices
- This measures entanglement (check that separable states $|\psi_1\rangle_A \otimes |\psi_2\rangle_B$ have zero entanglement entropy)
- For qubit, maximum entanglement is given by:
 $|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ (check!)
- A general (for mixed states too) measure of entanglement:
Relative Entropy of Entanglement: Measures the minimum relative entropy between our state ρ_{AB} and *any* separable state
 $D_{REE}(\rho_{AB}) = \min_{\sigma_{AB} \in \text{separable states}} S(\rho_{AB} \parallel \sigma_{AB})$

- **Setting:** Alice and Bob share a pair of entangled qubits

$$|\Phi^+\rangle = \frac{|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B}{\sqrt{2}}$$

There is **no quantum channel** between them (i.e. no quantum state can be physically sent)

They can **classically communicate**

Alice has an unknown state $|\psi\rangle_C = a|0\rangle_C + b|1\rangle_C$
(Alice does NOT know a and b)

- **Setting:** Alice and Bob share a pair of entangled qubits

$$|\Phi^+\rangle = \frac{|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B}{\sqrt{2}}$$

There is **no quantum channel** between them (i.e. no quantum state can be physically sent)

They can **classically communicate**

Alice has an unknown state $|\psi\rangle_C = a|0\rangle_C + b|1\rangle_C$
(Alice does NOT know a and b)

- **Task:** Alice wants to send the state $|\psi\rangle$ to Bob

- The overall initial state (entangled pair plus unknown state) is $|\Phi^+\rangle_{AB} |\psi\rangle_C$, where qubits A and C are in Alice's lab, while qubit B in Bob's.

- The overall initial state (entangled pair plus unknown state) is $|\Phi^+\rangle_{AB} |\psi\rangle_C$, where qubits A and C are in Alice's lab, while qubit B in Bob's.
- Alice measures her two qubits in the Bell basis $\{|\Phi^+\rangle_{AC}, |\Phi^-\rangle_{AC}, |\Psi^+\rangle_{AC}, |\Psi^-\rangle_{AC}\}$

- The overall initial state (entangled pair plus unknown state) is $|\Phi^+\rangle_{AB} |\psi\rangle_C$, where qubits A and C are in Alice's lab, while qubit B in Bob's.

- Alice measures her two qubits in the Bell basis

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

Note: The following identities hold

$$|00\rangle = \frac{1}{\sqrt{2}}(|\Phi^+\rangle + |\Phi^-\rangle); |01\rangle = \frac{1}{\sqrt{2}}(|\Psi^+\rangle + |\Psi^-\rangle)$$

$$|10\rangle = \frac{1}{\sqrt{2}}(|\Psi^+\rangle - |\Psi^-\rangle); |11\rangle = \frac{1}{\sqrt{2}}(|\Phi^+\rangle - |\Phi^-\rangle)$$

- The overall initial state (entangled pair plus unknown state) is $|\Phi^+\rangle_{AB} |\psi\rangle_C$, where qubits A and C are in Alice's lab, while qubit B in Bob's.

- Alice measures her two qubits in the Bell basis

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

Note: The following identities hold

$$|00\rangle = \frac{1}{\sqrt{2}}(|\Phi^+\rangle + |\Phi^-\rangle); |01\rangle = \frac{1}{\sqrt{2}}(|\Psi^+\rangle + |\Psi^-\rangle)$$

$$|10\rangle = \frac{1}{\sqrt{2}}(|\Psi^+\rangle - |\Psi^-\rangle); |11\rangle = \frac{1}{\sqrt{2}}(|\Phi^+\rangle - |\Phi^-\rangle)$$

- The state (before the Bell measurement) can be written as:

$$|\Phi^+\rangle_{AB} |\psi\rangle_C =$$

$$\frac{1}{2} [|\Phi^+\rangle_{AC} (a|0\rangle_B + b|1\rangle_B) + |\Phi^-\rangle_{AC} (a|0\rangle_B - b|1\rangle_B) + |\Psi^+\rangle_{AC} (a|1\rangle_B + b|0\rangle_B) + |\Psi^-\rangle_{AC} (-a|1\rangle_B + b|0\rangle_B)]$$

- Alice by making a Bell measurement, she gets as outcome one of the four states and collapses the state to one of the four terms in the previous expression (brown)

- Alice by making a Bell measurement, she gets as outcome one of the four states and collapses the state to one of the four terms in the previous expression (brown)
- Depending on the outcome, Alice sends to Bob using a classical channel a “correction” to make:

$$|\Phi^+\rangle_{AC} \rightarrow \mathbb{I}_B; |\Phi^-\rangle_{AC} \rightarrow Z_B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$|\Psi^+\rangle_{AC} \rightarrow X_B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}; |\Psi^-\rangle_{AC} \rightarrow -(ZX)_B = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

- Alice by making a Bell measurement, she gets as outcome one of the four states and collapses the state to one of the four terms in the previous expression (brown)
- Depending on the outcome, Alice sends to Bob using a classical channel a “correction” to make:

$$|\Phi^+\rangle_{AC} \rightarrow \mathbb{I}_B; |\Phi^-\rangle_{AC} \rightarrow Z_B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$|\Psi^+\rangle_{AC} \rightarrow X_B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}; |\Psi^-\rangle_{AC} \rightarrow -(ZX)_B = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

- Bob in all four cases ends up with the state $|\psi\rangle_B$ completing the teleportation

- **Alice** by making a Bell measurement, she gets as outcome one of the four states and collapses the state to one of the four terms in the previous expression (**brown**)
- Depending on the outcome, **Alice** sends to **Bob** using a classical channel a “*correction*” to make:

$$|\Phi^+\rangle_{AC} \rightarrow \mathbb{I}_B; |\Phi^-\rangle_{AC} \rightarrow Z_B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

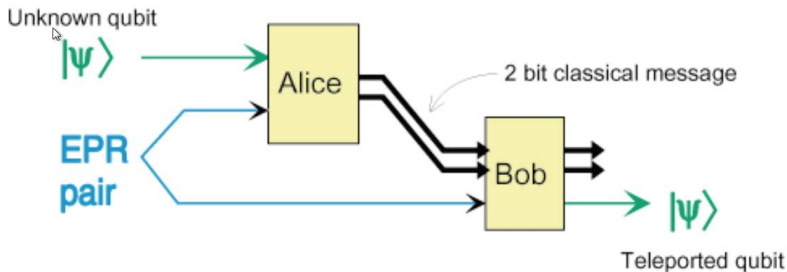
$$|\Psi^+\rangle_{AC} \rightarrow X_B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}; |\Psi^-\rangle_{AC} \rightarrow -(ZX)_B = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

- **Bob** in **all four cases** ends up with the state $|\psi\rangle_B$ completing the teleportation

Note: To complete the teleportation, some corrections are needed which **Alice** communicates classically to **Bob**.

Otherwise she could “signal” faster than the speed of light!

Pictorially:



Classical Channel + Entanglement = Quantum Channel

Teleportation and QOTP

- Let us label the outcomes as 2-bit string ab

$$|\Phi^+\rangle \rightarrow 00 \quad ; \quad |\Phi^-\rangle \rightarrow 01$$

$$|\Psi^+\rangle \rightarrow 10 \quad ; \quad |\Psi^-\rangle \rightarrow 11$$

- We can then rewrite the output state as:

$$X^a Z^b |\psi\rangle$$

- This is really the QOTP where the padding is the outcomes Alice got in her Bell measurement
- The state for Bob (without knowing Alice's outcomes/secret key) is totally random
Contains no information and thus doesn't violate non-signalling
- Bob cannot know whether Alice has made the measurement (and thus teleportation) or that he holds one side of a Bell pair
- Conversely in QOTP Bob could have received one side of a Bell pair, and not the padded state, thus he has no information!