QUANTUM COMPUTING ASSIGNMENT-2

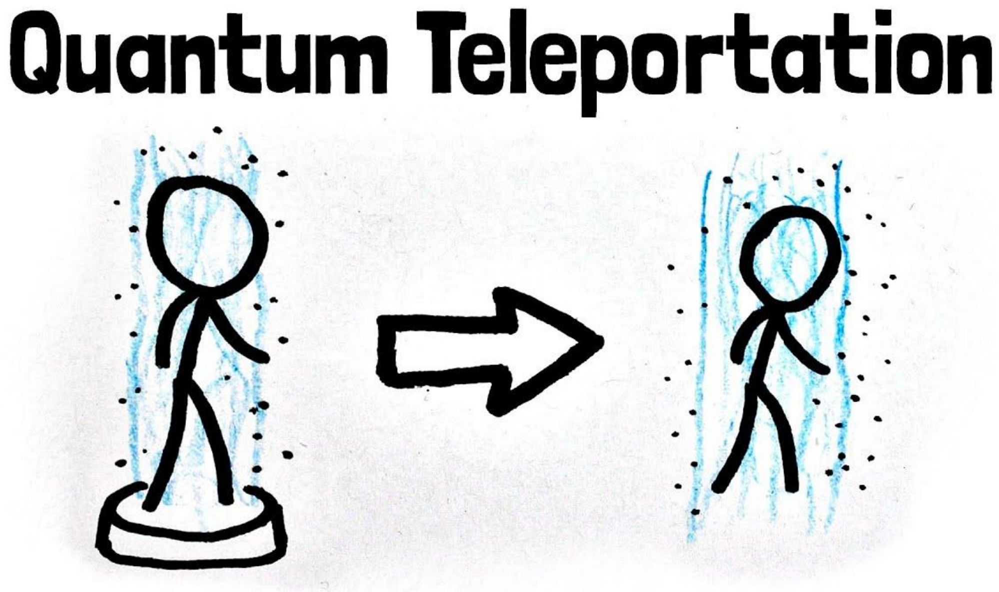
AVISHNA T
Mtech computer science Ds and Ai

QUANTUM TELEPORTATION

TELEPORTATION

A quantum information protocol by which the unknown quantum state of one particle can be transferred to another distant particle, using a pair of entangled particles, a projective measurement, and exchange of two bits of classical information.

The process is not instantaneous, because information must be communicated classically between observers as part of the process.



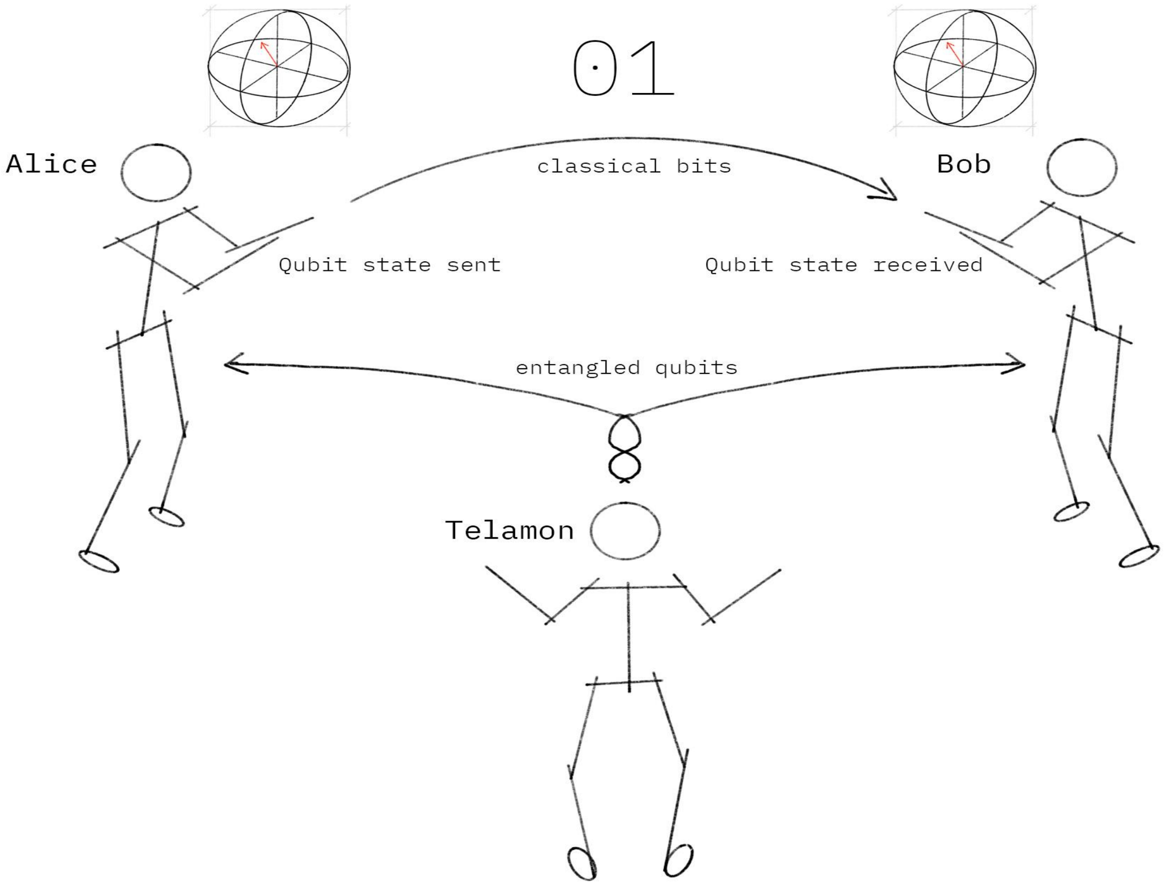
- Alice wants to send quantum information to Bob. Specifically, suppose she wants to send the qubit state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. This entails passing on information about $\alpha\alpha$ and $\beta\beta$ to Bob.

- There exists a theorem in quantum mechanics which states that you cannot simply make an exact copy of an unknown quantum state. This is known as the no-cloning theorem. As a result of this we can see that Alice can't simply generate a copy of $|\psi\rangle$ $|\psi\rangle$ and give the copy to Bob. We can only copy classical states (not superpositions).

- However, by taking advantage of two classical bits and an entangled qubit pair, Alice can transfer her state $|\psi\rangle$ $|\psi\rangle$ to Bob. We call this teleportation because, at the end, Bob will have $|\psi\rangle$ $|\psi\rangle$ and Alice won't anymore

The Quantum Teleportation Protocol

- To transfer a quantum bit, Alice and Bob must use a third party (Telamon) to send them an entangled qubit pair. Alice then performs some operations on her qubit, sends the results to Bob over a classical communication channel and Bob then performs some operations on his end to receive Alice's qubit.



Process of Quantum Teleportation

Below is a sketch of an algorithm for teleporting quantum information. Suppose Alice has state C, which she wants to send to Bob. To achieve this, Alice and Bob should follow the sequence of steps:

- 1) Generate an entangled pair of electrons with spin states A and B, in a particular Bell

$$|\Phi_0\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle_A \otimes |\uparrow\rangle_B + |\downarrow\rangle_A \otimes |\downarrow\rangle_B).$$

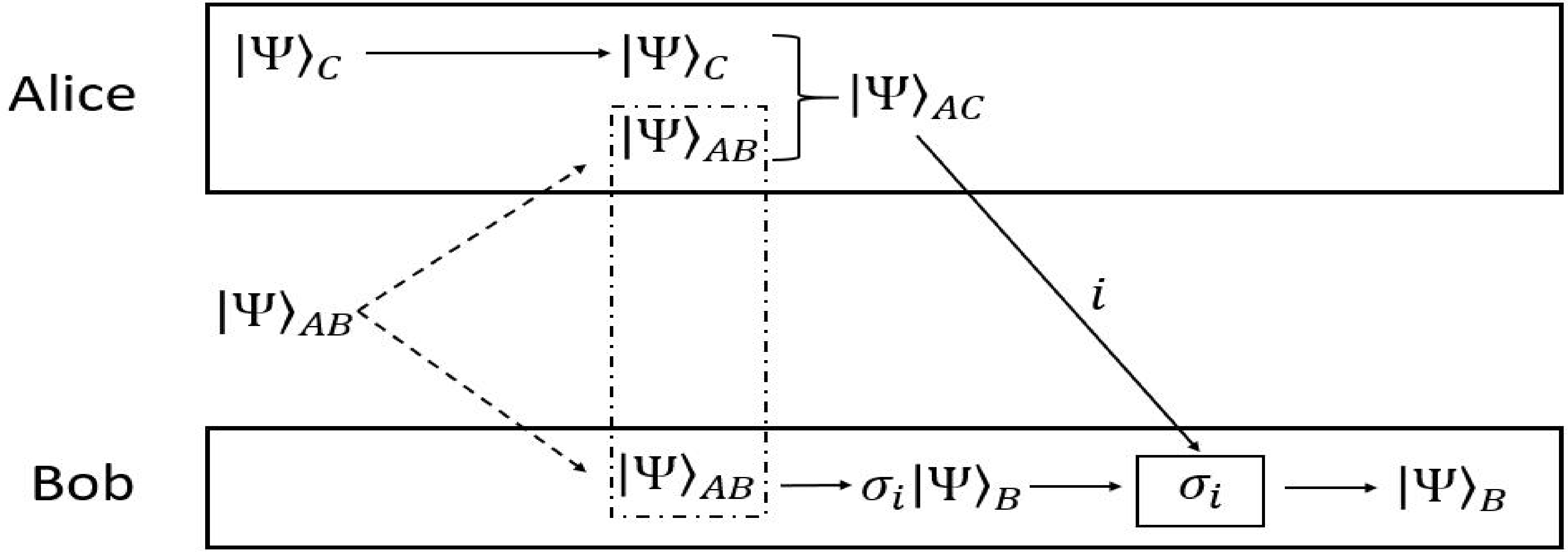
Separate the entangled electrons, sending A to Alice and B to Bob.

- 2) Alice measures the "Bell state" (described below) of A and C, entangling A and C.

- 3) Alice sends the result of her measurement to Bob via some classical method of communication.

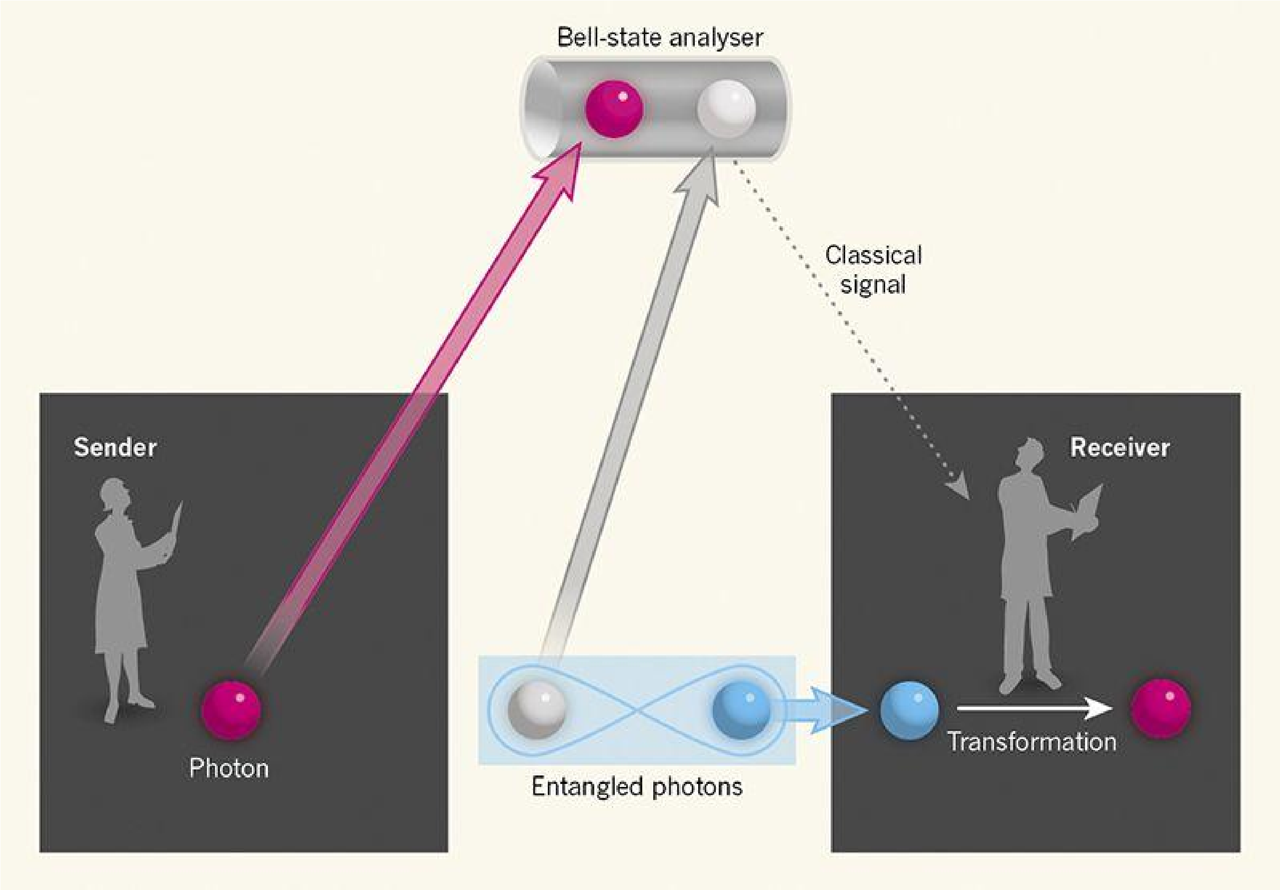
- 4) Bob measures the spin of state B along an axis determined by Alice's measurement

Since step 3 involves communicating via some classical method, the information in the entangled state must respect causality. Relativity is not violated because the information cannot be communicated faster than the classical communication in step 3 can be performed, which is sub-lightspeed.

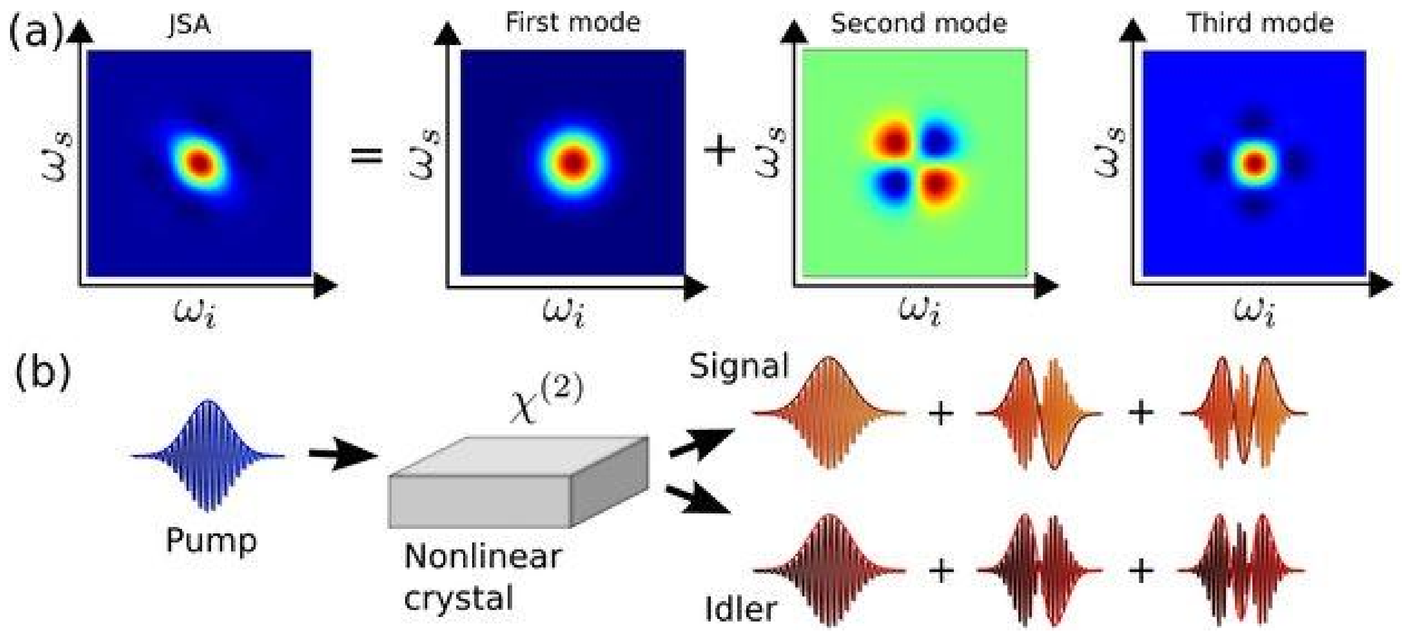


- The idea of quantum teleportation, is that Alice's measurement disentangles A and B and entangles A and C. Depending on what particular entangled state Alice sees, Bob will know exactly how B was disentangled, and can manipulate B to take the state that C had originally. Thus the state C was "teleported" from Alice to Bob, who now has a state that looks identical to how C originally looked.

- It is important to note that state C is not preserved in the processes: the no-cloning and no-deletion theorems of quantum mechanics prevent quantum information from being perfectly replicated or destroyed. Bob receives a state that looks like C did originally, but Alice no longer has the original state C in the end, since it is now in an entangled state with A.



SCHMIDT DECOMPOSITION



In linear algebra, the Schmidt decomposition (named after its originator Erhard Schmidt) refers to a particular way of expressing a vector in the tensor product of two inner product spaces. It has numerous applications in quantum information theory, for example in entanglement characterization and in state purification, and plasticity.

Visualization of a Schmidt decomposition: Each pair of Schmidt modes of signal and idler, depicted in (b), forms a spectral distribution, which, combined and weighted by their r k-values form the JSA (a).

SCHMIDT DECOMPOSITION

- Let $|\psi\rangle$ be any bipartitquantum state:

$$|\psi\rangle = \sum_{a=1}^{m} \sum_{b=1}^{m} \alpha_{a,b} |a\rangle \otimes |b\rangle$$

Then there exist orthonormal states

$|\mu_1\rangle, |\mu_2\rangle, \ldots, |\mu_m\rangle$ and $|\varphi_1\rangle, |\varphi_2\rangle, \ldots, |\varphi_m\rangle$ such that

$$|\psi\rangle = \sum_{c=1}^{m} \sqrt{p_c} |\mu_c\rangle \otimes |\phi_c\rangle$$

Eigenvectors of $\mathrm{Tr}_1|\psi\rangle\langle\psi|$

With respect to the above bases, the state "looks" like:

$$|\psi\rangle = \sum_{c=1}^{m} \sqrt{p_c} |c\rangle \otimes |c\rangle$$

Schmidt decomposition: proof (I)

- The density matrix for state $|\psi\rangle$ is given by $|\psi\rangle\langle\psi|$
- Tracing out the first system, we obtain the density matrix of the second system, $\rho = \mathrm{Tr}_1|\psi\rangle\langle\psi|$
- Since ρ is a density matrix, we can express $\rho = \sum_{c=1}^{m} p_c |\varphi_c\rangle\langle\varphi_c|$,

where $|\varphi_1\rangle, |\varphi_2\rangle, \ldots, |\varphi_m\rangle$ are orthonormal eigenvectors of ρ

Now, returning to $|\psi\rangle$, we can express $|\psi\rangle = \sum_{c=1}^{m} |\nu_c\rangle \otimes |\varphi_c\rangle$

- where $|\nu_1\rangle, |\nu_2\rangle, \ldots, |\nu_m\rangle$ are ***just some arbitrary vectors*** (not necessarily valid quantum states; for example, they might not have unit length, and we cannot presume they're orthogonal)
- We will next show that $\langle\nu_c|\nu_{c'}\rangle = \begin{cases} p_c & \text{if } c = c' \\ 0 & \text{if } c \neq c' \end{cases}$
- we compute the partial trace Tr_1 of $|\psi\rangle\langle\psi|$ in terms of

$$|\psi\rangle\langle\psi| = \left(\sum_{c=1}^{m} |\nu_c\rangle \otimes |\varphi_c\rangle\right)\left(\sum_{c'=1}^{m} \langle\nu_{c'}| \otimes \langle\varphi_{c'}|\right) = \sum_{c=1}^{m}\sum_{c'=1}^{m} |\nu_c\rangle\langle\nu_{c'}| \otimes |\varphi_c\rangle\langle\varphi_{c'}|$$

- A careful calculation (shown later) of this partial trace yields

$$\sum_{c=1}^{m}\sum_{c'=1}^{m} \langle\nu_{c'}|\nu_c\rangle \otimes |\varphi_c\rangle\langle\varphi_{c'}|$$

- which must equal $\sum_{c=1}^{m} p_c |\varphi_c\rangle\langle\varphi_c|$

The claimed result about $\langle \nu_c | \nu_{c'} \rangle$ now follows

Next, setting $|\mu_c\rangle = \frac{1}{\sqrt{p_c}} |\nu_c\rangle$ completes the construction

For completeness, we now give the "careful calculation" of

$$\mathrm{Tr}_1\left(\sum_{c=1}^{m} \sum_{c'=1}^{m} |\nu_c\rangle\langle\nu_{c'}| \otimes |\phi_c\rangle\langle\phi_{c'}| \right)$$

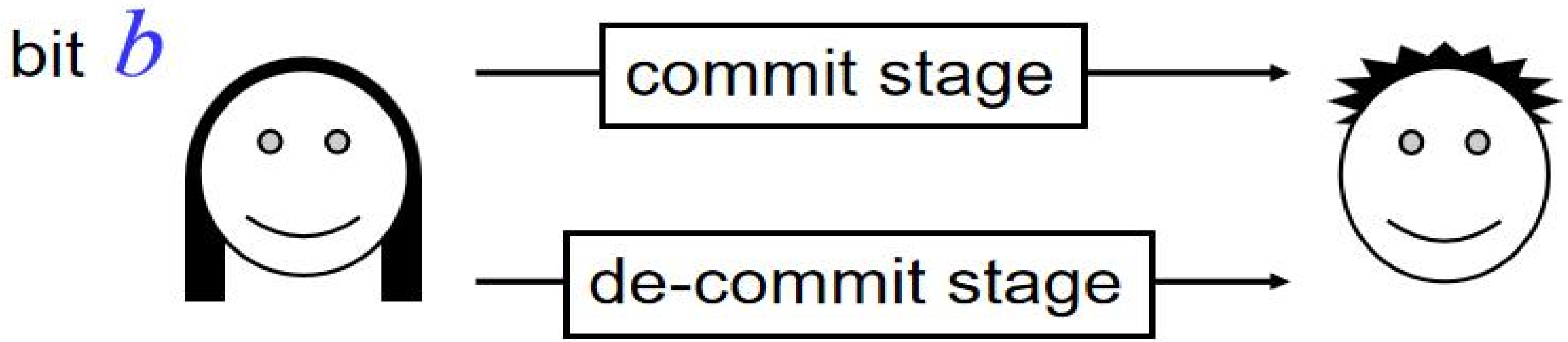
$$= \sum_{a=1}^{m} \left(\langle a| \otimes I \right) \left(\sum_{c=1}^{m} \sum_{c'=1}^{m} |v_c\rangle\langle v_{c'}| \otimes |\varphi_c\rangle\langle\varphi_{c'}| \right) \left(|a\rangle \otimes I \right)$$ (by definition of Tr_1)

$$= \sum_{c=1}^{m} \sum_{c'=1}^{m} \left(\sum_{a=1}^{m} \langle a|v_c\rangle\langle v_{c'}|a\rangle \right) \otimes |\varphi_c\rangle\langle\varphi_{c'}|$$ (linearity & properties of $\otimes$)

$$= \sum_{c=1}^{m} \sum_{c'=1}^{m} \left(\mathrm{Tr}|v_c\rangle\langle v_{c'}| \right) \otimes |\varphi_c\rangle\langle\varphi_{c'}|$$ (definition of Tr)

$$= \sum_{c=1}^{m} \sum_{c'=1}^{m} \langle v_{c'}|v_c\rangle \otimes |\varphi_c\rangle\langle\varphi_{c'}|$$ (since $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$)

Bit-commitment



- Alice has a bit b that she wants to ***commit*** to Bob:
- After the ***commit*** stage, Bob should know nothing about b, but Alice should not be able to change her mind
- After the ***de-commit*** stage, either:
  - Bob should learn b and accept its value, or
  - Bob should reject Alice's de-commitment message, if she deviates from the protocol

Simple physical implementation

- **Commit:** Alice writes b down on a piece of paper, locks it in a safe, sends the safe to Bob, but keeps the key

- **De-commit:** Alice sends the key to Bob, who then opens the safe

- Desirable properties:
  - **Binding:** Alice cannot change b after **commit**
  - **Concealing:** Bob learns nothing about b until **de-commit**

SUPERDENSE CODING

- In quantum information theory, superdense coding (also referred to as dense coding) is a quantum communication protocol to communicate a number of classical bits of information by only transmitting a smaller number of qubits, under the assumption of sender and receiver pre-sharing an entangled resource.
- Now, it is important to note that while Superdense Coding and Quantum Teleportation are closely related, there is a key difference between them. Quantum teleportation is a process by which a user can transmit one qubit using two classical bits whereas Superdense Coding is a process by which a user can transmit two classical bits using one qubit. Basically, Superdense Coding can be thought of as the flipped version of Quantum Teleportation.

THE PROTOCOL

- Superdense coding involves three parties, let's just call them Charlie, Alice and Bob. It requires two parties who wish to communicate a two-bit message, a pair of entangled qubits, and a quantum channel.

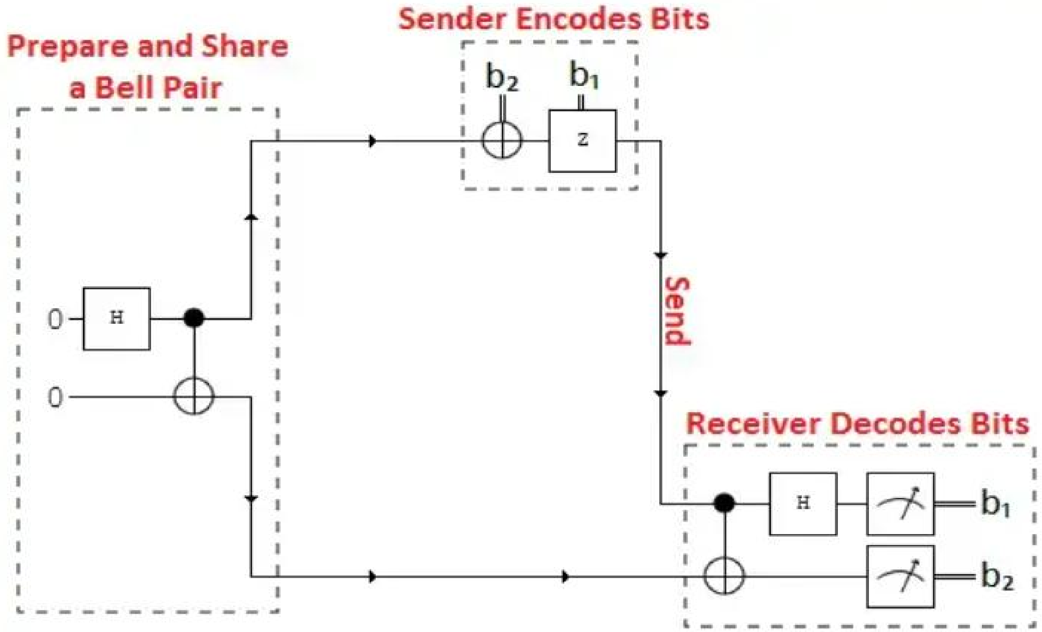


Diagram of Protocol

- Charlie prepares a pair of Bell state, or maximally entangled, qubits, which just means that the two qubits exhibit perfect correlations even though they are spatially seperated (even with great distances).

- Charlie then sends those qubits to Alice and Bob so that they can share them between themselves (1 qubit with Alice and the other with Bob). However, before Alice can attempt to transmit 2 classical bits of infortmation to Bob using her Bell state qubit, she has to apply a single gate operation based off of the intended message:

Intended Message	Applied Gate	Resulting State $(\cdot\sqrt{2})$
00	I	$\|00\rangle + \|11\rangle$
10	X	$\|01\rangle + \|10\rangle$
01	Z	$\|00\rangle - \|11\rangle$
11	ZX	$-\|01\rangle + \|10\rangle$

Qiskit: Encoding Rules (Alice Protocol)

Now, Bob is a very smart guy. He knows that since Alice’s qubits are entangled the two qubits must be in one of the four Bell states. So, once Bob recieves Alice’s encoded qubit, he will pass it and his untouched Bell state qubit through a reverse Bell circuit (where Alice’s qubit acts as the control and Bob’s is the target) in order to decode Alice’s message. Thus, Bob will obtain two classical bits of information from a single qubit!

Bob Receives:	**After CNOT-gate:**	**After H-gate:**
$\lvert 00\rangle + \lvert 11\rangle$	$\lvert 00\rangle + \lvert 01\rangle$	$\lvert 00\rangle$
$\lvert 01\rangle + \lvert 10\rangle$	$\lvert 11\rangle + \lvert 10\rangle$	$\lvert 10\rangle$
$\lvert 00\rangle - \lvert 11\rangle$	$\lvert 00\rangle - \lvert 01\rangle$	$\lvert 01\rangle$
$-\lvert 01\rangle + \lvert 10\rangle$	$-\lvert 11\rangle + \lvert 10\rangle$	$\lvert 11\rangle$

Qiskit: Bob Decoding Process

SECURITY

- Superdense Coding, along with Quantum Teleportation, is the underlying principle of secure quantum coding since it eliminates the possibility of eavesdroppers intercepting messages.

- Let’s say an eavesdropper named Eve intercepted Alice’s encoded qubit en rout to Bob. Eve would only have 1/2 of an entangled state and without access to Bob’s qubit (which is necessary to decode Alice’s qubit), Eve would have no way of getting the information from Alices qubit. Furthermore, any attempt to measure either Alice’s or Bob’s qubit would collapse the state of said qubit and alert both of them.

Coding it in Qiskit

1. Import the neccessary packages

2. Create the entangled qubit pair by applying an H-gate followed by a CNOT in a 2 qubit circuit

3. Encode message with appropriate gates

4. Decode message by applying a CNOT followed by a H-gate

- Here's a visual representation of the quantum circuit: