In principle demonstration of quantum secret sharing in the IBM quantum computer

Balija Subha Shree - CS19B1005
Akhil Nerella - CS19B1020
Thanai Sahu - CS19B1021
Vibhanshu Jain - CS19B1027

Guide: Dr. M V P Sir

Joy, Dintomon, Bikash K. Behera, and Prasanta K. Panigrahi. "In principle demonstration of quantum secret sharing in the IBM quantum computer." arXiv (2018): arXiv-1807.

Classical Secret Sharing

- Classic Secret sharing is method of distributing a secret among group of members each of whom is allocated a share of secret, such that it can be reconstructed only when a sufficient number of members come together.
- By the use of advanced quantum algorithms this Classical Secret Sharing Scheme is broken
- CSS schemes are not perfectly secure from eavesdrops attack.

Quantum Secret Sharing

- Quantum secret sharing is a way to share secret messages with unconditional security
- Alice shares the quantum information between two parties Bob and Charlie.
- To retrieve the secret fully one of Bob or Charlie should consent from the other.
- The presence a dishonest receiver or outsider can be detected without the secret being revealed.

Quantum Secret Sharing

- For splitting the message into two parts it uses the GHZ states or maximally entangled three-particle states.
- If we suppose Alice,Bob and Charlie each have one particle from the GHZ triplet which is in state.
- These three particles choose to measure in x or y direction randomly.
- By combining measurement results of Bob and Charlie result of Alice measurement can be known in half the time.

HBB Protocol

(i) The sender Alice and the users Bob and Charlie shares a 3-qubit GHZ state prior to the beginning of quantum secret sharing procedure.

(ii) Alice wants to send an arbitrary single qubit state, in her possession to Charlie (Bob) through the method of quantum teleportation.

(iii)Alice then performs a Bell basis measurement on the two particles (A, a) in her possession and keeps the measurement result to herself.

(iv) After confirming via public channel, that both Bob and Charlie have received one particle each, Alice sends her measurement result to Charlie (Bob).

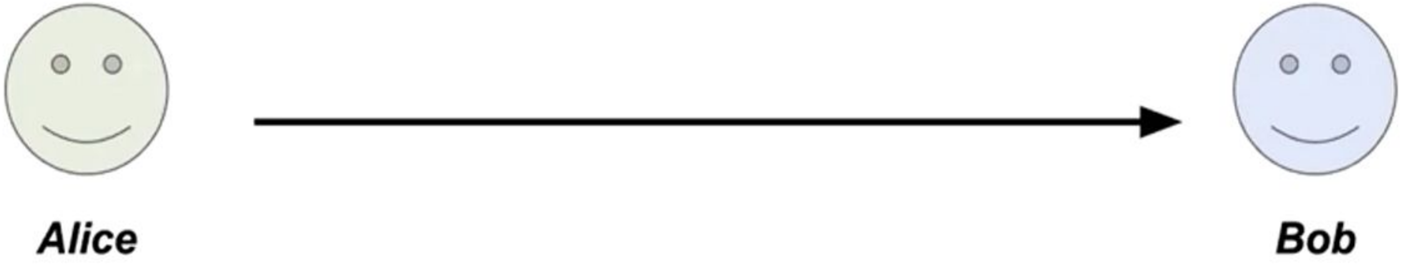
(v) Bob (Charlie) then performs a single particle measurement on his particle in X-basis and sends his measurement result to Charlie (Bob) .

(vi)Now, Charlie (Bob) can reconstruct the teleported information by getting one bit classical information from Bob (Charlie) and the two bits earlier sent by Alice .

Transporting Qubits

- According to the No-Cloning theorem,qubits cannot be duplicated
- Is there a way to transmit qubits from one point to another without destroying superposition and phase information?

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



Quantum Teleportation

- Quantum Teleportation enables the transfer of qubits,while perfectly preserving state information
- Allows for transmission over great distances (from Earth to Space)

    Does not involve:

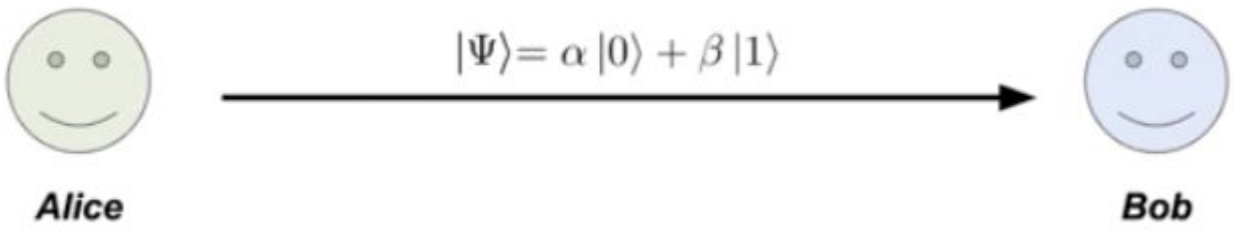
    - Moving matter from one point to another via Materialization or de-Materialization
    - Travelling forward or backward in time
    - Travelling faster than speed of light

Requirements for Quantum Teleportation

A qubit can be perfectly transmitted using 3 qubit and 2 classical bits.

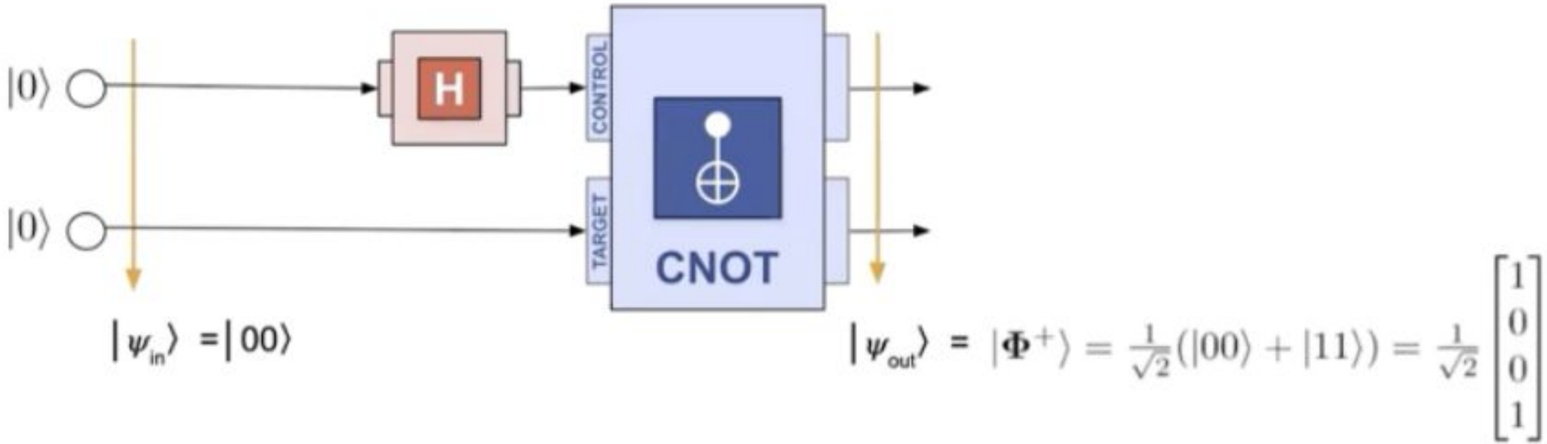
Teleportation needs:

- Two qubits that are entangled…each party has one half of the entangled pair
- A message qubit that will be send from one point to another
- A classical communication line between both parties for the transmission of two classical bits. (therefore it cannot be faster than the speed of light)



Step 1: Create an entangled pair of qubits

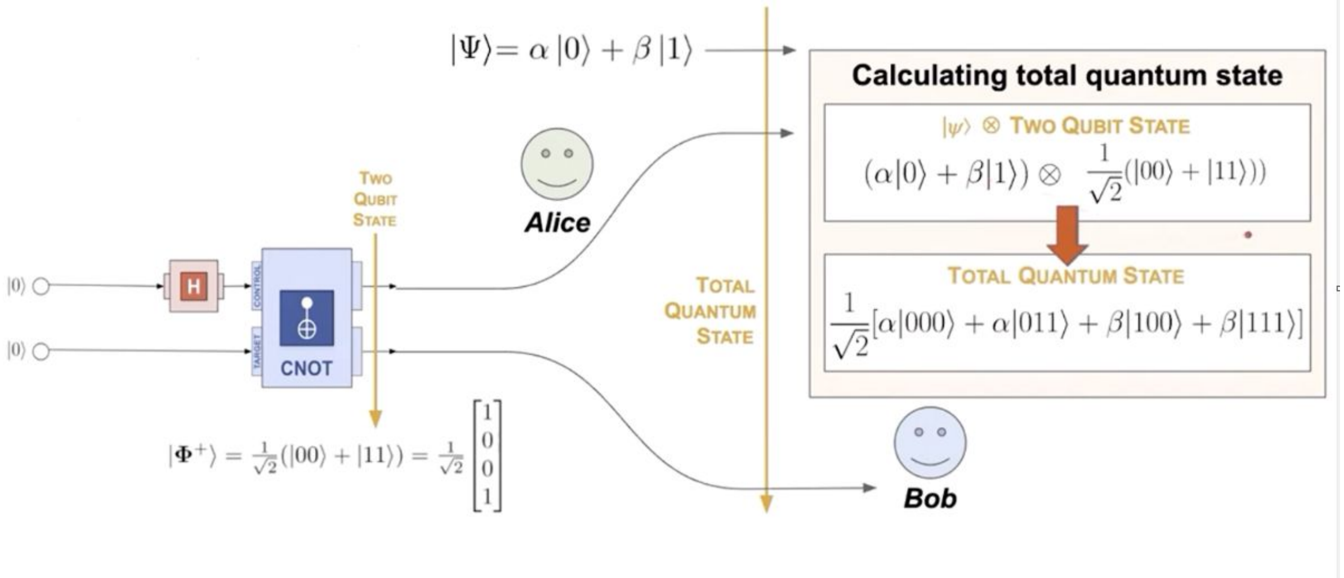
- Alice and Bob entangle the qubits using Hadamard and CNOT gate



Step 2: Distribute entangled qubits to Alice & Bob

Alice now has two qubits:

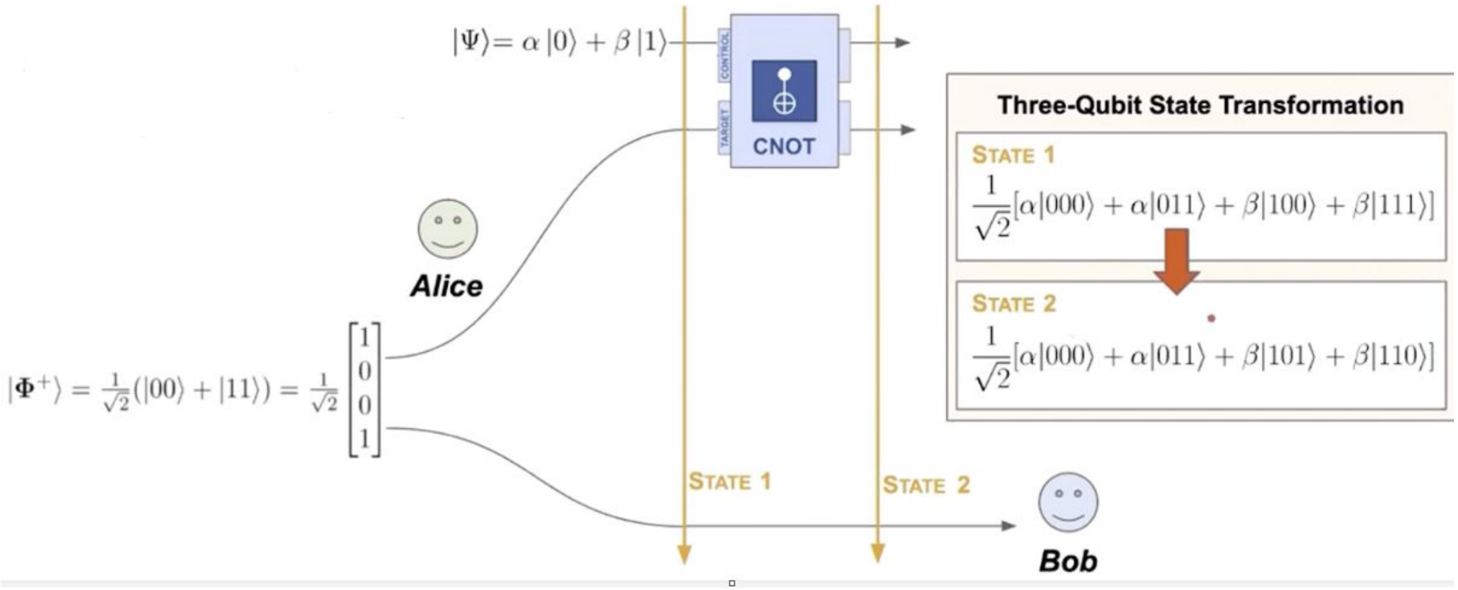
- Half of the entangled pair
- The message qubit, |ψ>



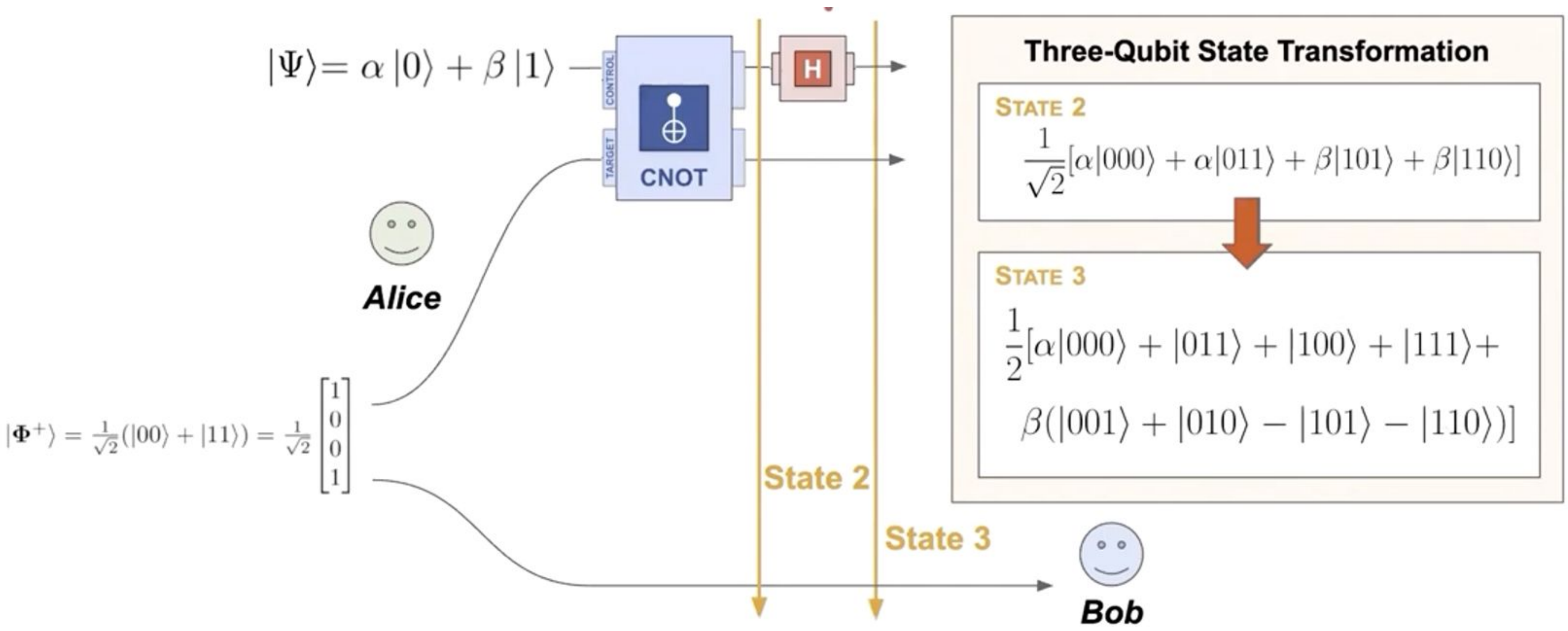
Step 3: Alice applies CNOT to her qubits

Alice applies CNOT on:

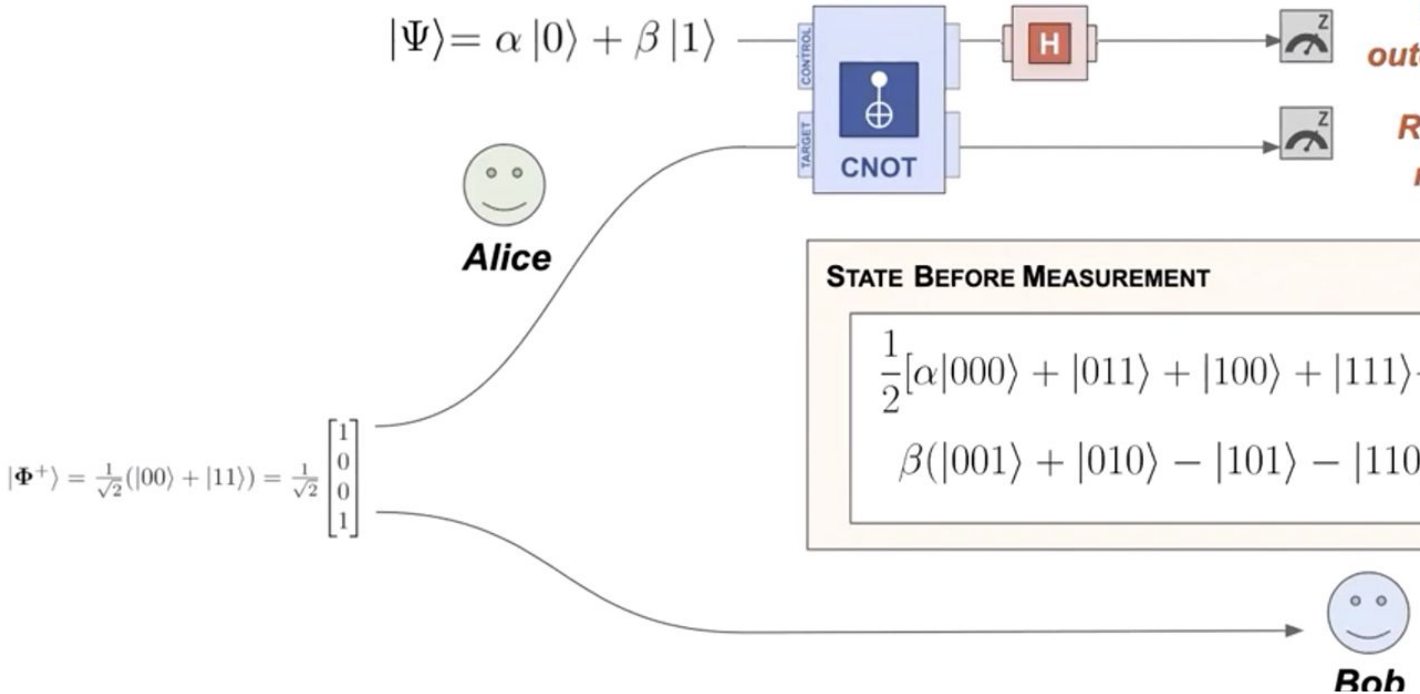
- Message qubits |ψ> (control)
- Her qubit (target)



Step 4: Alice applies an H gate on |ψ>



Step 5: Alice measures both of her qubits



There are four possible outcomes for Alice's qubits…

Remember: measurement results in classical bits!

STATE BEFORE MEASUREMENT

$$\frac{1}{2}[\alpha|000\rangle + |011\rangle + |100\rangle + |111\rangle +$$
$$\beta(|001\rangle + |010\rangle - |101\rangle - |110\rangle)]$$

Step 6: Process results of measurements

We deduce information about Bob's state by using partial measurements!

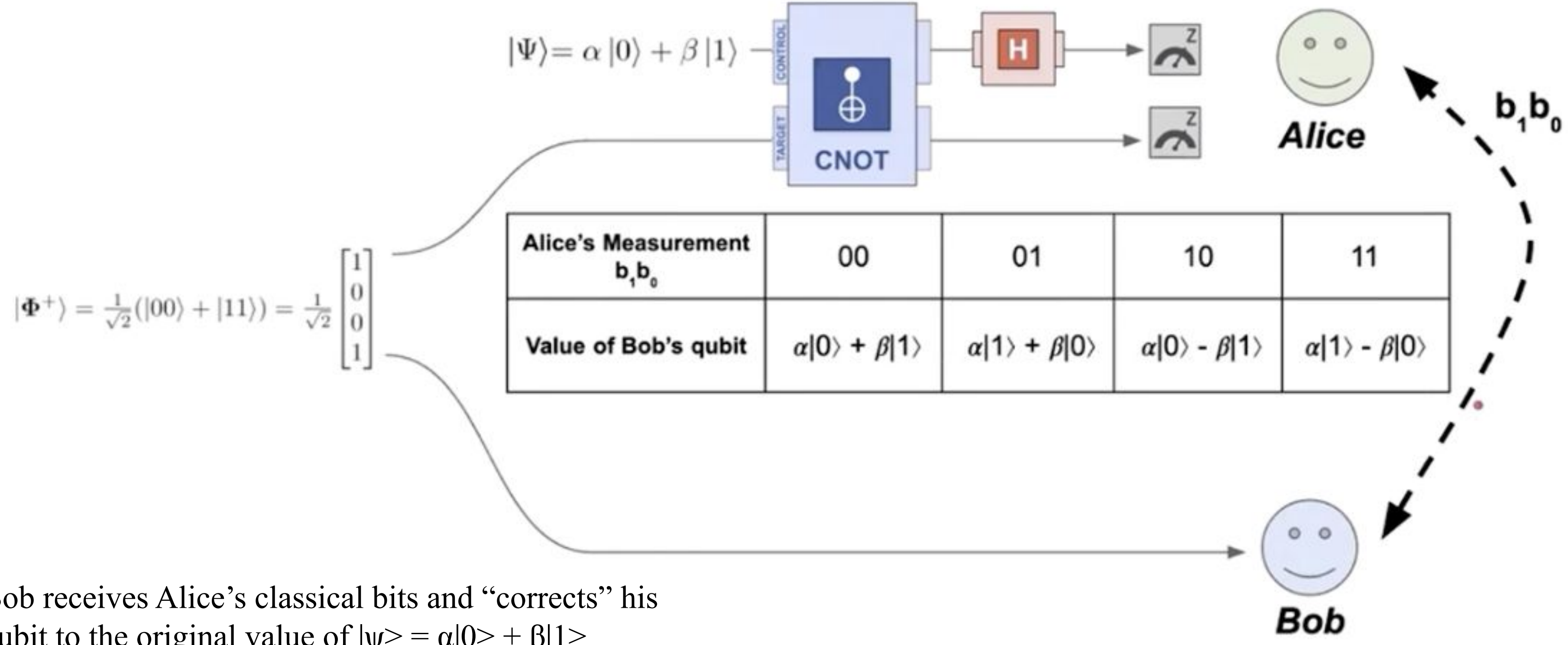
State before Measurement:

$$\frac{1}{2}[\alpha|000\rangle + |011\rangle + |100\rangle + |111\rangle + \beta(|001\rangle + |010\rangle - |101\rangle - |110\rangle)]$$

For example, if Alice sees 00, we narrow down the state of the entire system to the possibilities that satisfy this observation:
|000> and |001>.

Alice's Measurement	00	01	10	11
Value of Bob's qubit	$\alpha\|0\rangle + \beta\|1\rangle$	$\alpha\|1\rangle + \beta\|0\rangle$	$\alpha\|0\rangle - \beta\|1\rangle$	$\alpha\|1\rangle - \beta\|0\rangle$

Step 7: Alice transmits her two classical bits to Bob



Alice's Measurement b_1b_0	00	01	10	11
Value of Bob's qubit	$\alpha\|0\rangle + \beta\|1\rangle$	$\alpha\|1\rangle + \beta\|0\rangle$	$\alpha\|0\rangle - \beta\|1\rangle$	$\alpha\|1\rangle - \beta\|0\rangle$

Bob receives Alice's classical bits and "corrects" his qubit to the original value of $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

Step 8: Bob Recovers |ψ>

To recover |ψ>:

- If b_1 is 1, then apply a Z gate
- If b_2 is 1, then apply a NOT (X) gate

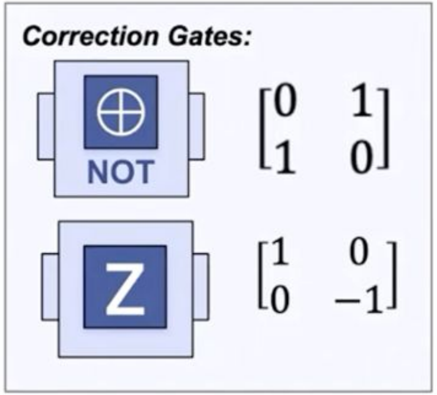
Alice's Measurement b_1b_0	00	01	10	11
Value of Bob's qubit	$\alpha\|0\rangle + \beta\|1\rangle$	$\alpha\|1\rangle + \beta\|0\rangle$	$\alpha\|0\rangle - \beta\|1\rangle$	$\alpha\|1\rangle - \beta\|0\rangle$

No Gates Needed!

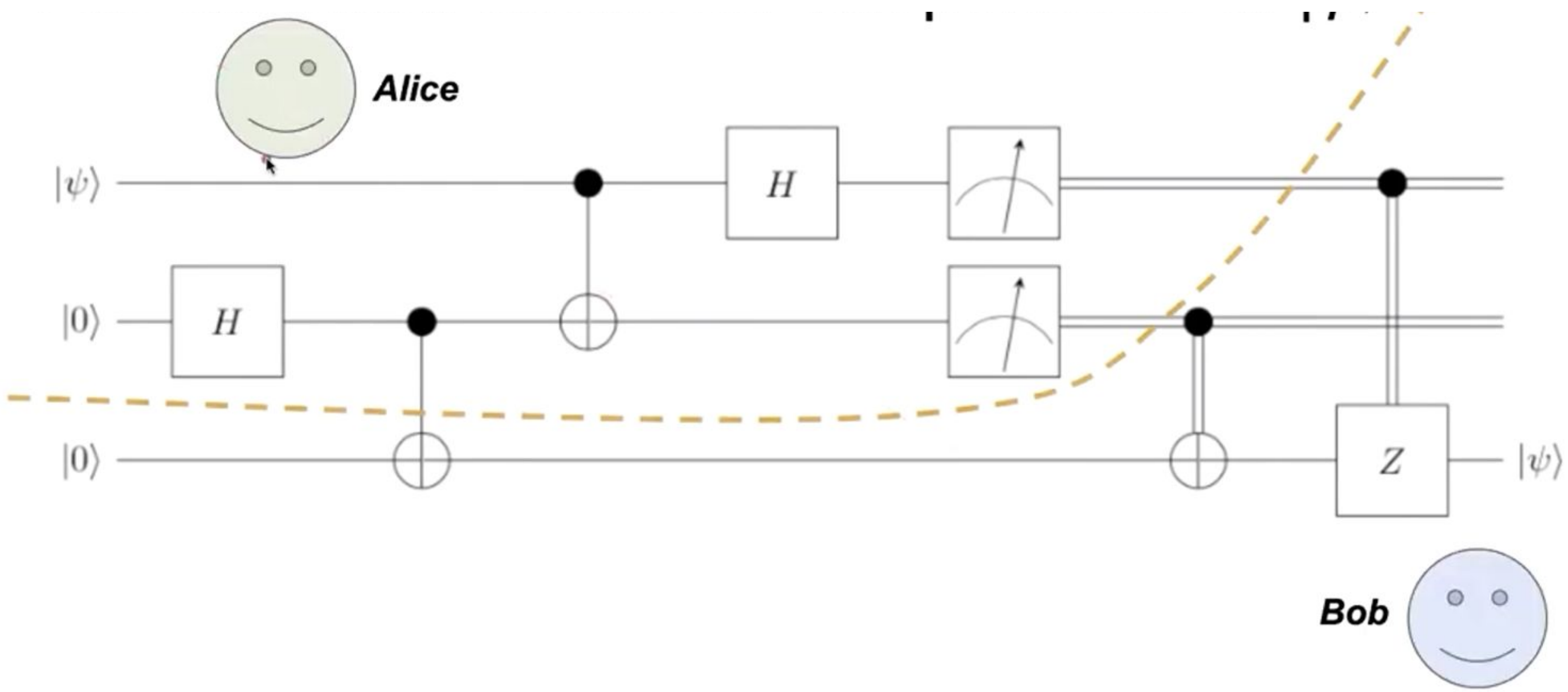
Apply NOT Gate

Apply Z Gate

Apply NOT and Z Gate



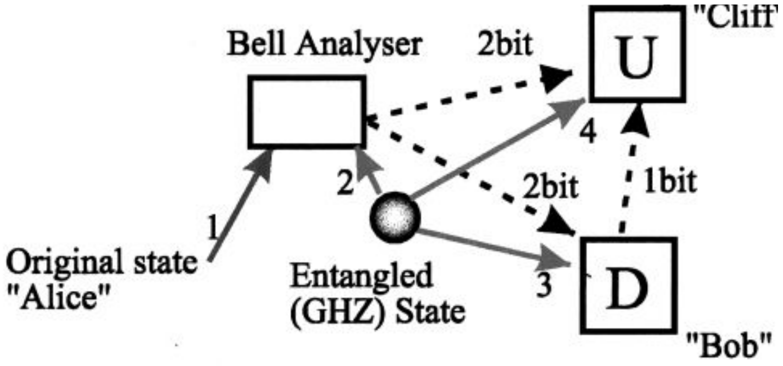
Quantum Circuit for Teleportation of |ψ>



Teleportation using Three particle Entanglement

Quantum State $|\Psi_A\rangle = a|\updownarrow\rangle_1 + b|\leftrightarrow\rangle_1$

Three particle entangled state used: $|\psi_{GHZ}\rangle = \frac{1}{\sqrt{2}}(|\updownarrow\rangle_2|\updownarrow\rangle_3|\updownarrow\rangle_4 + |\leftrightarrow\rangle_2|\leftrightarrow\rangle_3|\leftrightarrow\rangle_4)$



Initial Product State

$$|\Psi_A\rangle \otimes |\psi_{GHZ}\rangle = \frac{1}{2}[|\phi_{12}^+\rangle \otimes (a|\updownarrow\rangle_3|\updownarrow\rangle_4 + b|\leftrightarrow\rangle_3|\leftrightarrow\rangle_4)$$
$$+|\phi_{12}^-\rangle \otimes (a|\updownarrow\rangle_3|\updownarrow\rangle_4 - b|\leftrightarrow\rangle_3|\leftrightarrow\rangle_4)$$
$$+|\psi_{12}^+\rangle \otimes (a|\updownarrow\rangle_3|\leftrightarrow\rangle_4 + b|\leftrightarrow\rangle_3|\updownarrow\rangle_4)$$
$$+|\psi_{12}^-\rangle \otimes (a|\updownarrow\rangle_3|\leftrightarrow\rangle_4 - b|\leftrightarrow\rangle_3|\updownarrow\rangle_4)]$$

A measurement using Bell state analyzers on particles 1 and 2 will project the state of particles 3 and 4 onto the joint, generally entangled states

Take the case where, Bell State analyzers give the readout $|\phi_{12}^{+}\rangle$

Therefore the states of the particles 3 & 4 will be $|\psi_{34}\rangle = a|\updownarrow\rangle_3|\updownarrow\rangle_4 + b|\leftrightarrow\rangle_3|\leftrightarrow\rangle_4$

Constructing the state at location 4, “Charlie” with the help of “Bob” at location 3

$$|\updownarrow\rangle_3 = \sin\theta|x_1\rangle_3 + \cos\theta|x_2\rangle_3,$$

$$|\leftrightarrow\rangle_3 = \cos\theta|x_1\rangle_3 - \sin\theta|x_2\rangle_3,$$

$$\begin{aligned}|\psi_{34}\rangle = {} & (a\ \sin\ \theta|\updownarrow\rangle_4 + b\ \cos\ \theta|\leftrightarrow\rangle_4)|x_1\rangle_3 \\ & + (a\ \cos\ \theta|\updownarrow\rangle_4 - b\ \sin\ \theta|\leftrightarrow\rangle_4)|x_2\rangle_3\end{aligned}$$

$$|\psi_{34}\rangle = (a \sin\theta|\updownarrow\rangle_4 + b\cos\theta|\leftrightarrow\rangle_4)|x_1\rangle_3$$
$$+(a\cos\theta|\updownarrow\rangle_4 - b\sin\theta|\leftrightarrow\rangle_4)|x_2\rangle_3$$

- Bob performs a single particle measurement on his particle in X-basis and sends his measurement result to Charlie
- If the outcome is x_1 and $\theta=\pi/4$, the state of particle 4 will be

$$|\psi_4\rangle = a|\updownarrow\rangle_4 + b|\leftrightarrow\rangle_4$$

- If the outcome is x_2 and $\theta=\pi/4$ then Charlie applies Z gate
- We have successfully teleported the particle from Alice to Charlie.

Quantum Circuit for Teleportation of |ψ>

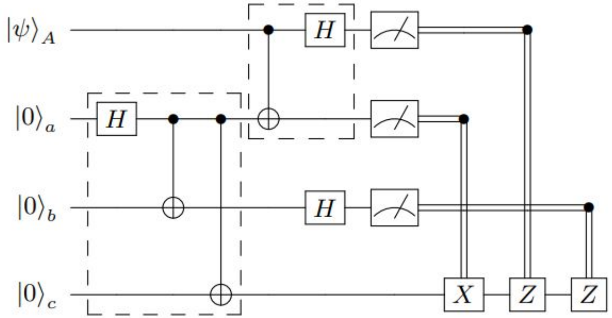


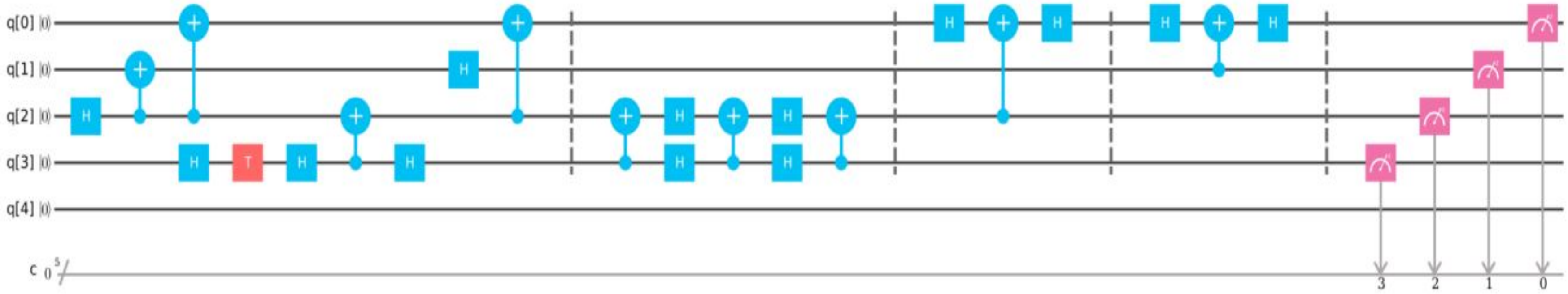
FIG. 1: **Quantum circuit to implement quantum secret sharing (QSS) protocol.** Here, $|\psi\rangle_A$ represents the quantum secret in Alice's possession. Qubits a, b and c represent the GHZ channel shared between Alice, Bob and Charlie respectively. The measurement device at the end of each qubit line measures the qubit in Z-basis. The double line after measurement represents the classical information corresponding to the output state. The first dashed box (from left to right) represents the 3-qubit GHZ state and the second one represents Bell measurement.

References

- W. K. Wootters and W. H. Zurek, Nature 299, 802–803 (1982).
- M. Hillery, V. Buˇzek, and A. Berthiaume, Phys. Rev. A. 59, 1829 (1999).
- Hillery et al. “Quantum Secret Sharing”. https://arxiv.org/pdf/quant-ph/9806063.pdf
- M. A. Nielsen and I. L. Chuang, Quantum computation and quantum information, Cambridge University Press, Cambridge, UK, 2010

THANK YOU!!

Quantum Circuit Implementation



Simulated Results

TABLE II: Simulated results

No. of Shots	Probability of $\lvert 0\rangle_C$	Probability of $\lvert 1\rangle_C$
8192	0.853	0.147
4096	0.860	0.139
1024	0.850	0.151

No. of shots	Probability of $\lvert 0>_C$	Probability of $\lvert 1>_C$
1024	0.853	0.147
4096	0.869	0.131
8192	0.858	0.142

Run Results

No. of Shots	Probability of $\|0\rangle_C$	Probability of $\|1\rangle_C$
8192	0.800	0.200
4096	0.803	0.197
1024	0.798	0.203

No. of shots	Probability of $\|0>_C$	Probability of $\|1>_C$
1024	0.662	0.338
4096	0.623	0.377
8192	0.734	0.266