BB22:The Most Advanced QKD

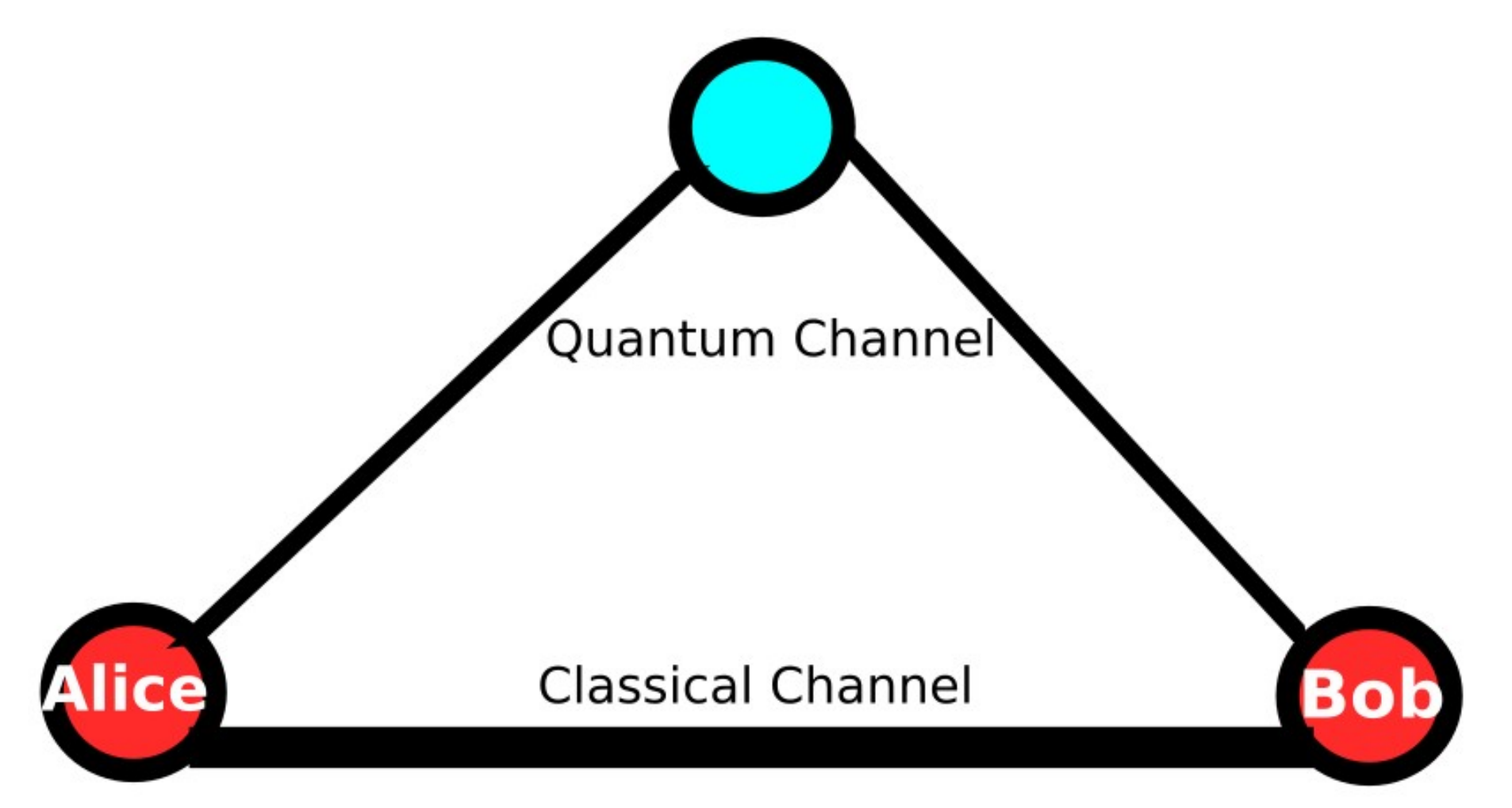
Motivation

- Creating a new algorithm for key distribution protocol

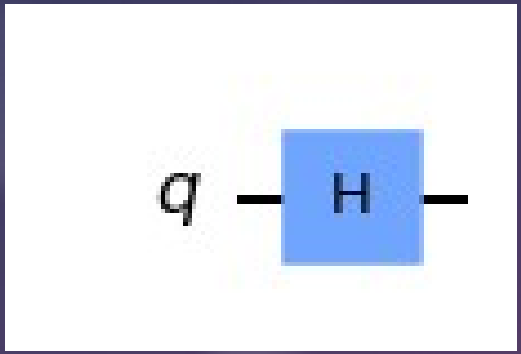
Benefits

- Sender only sends $|+\rangle$.
- Presence of eavesdropping can be detected apparently

How does it work?

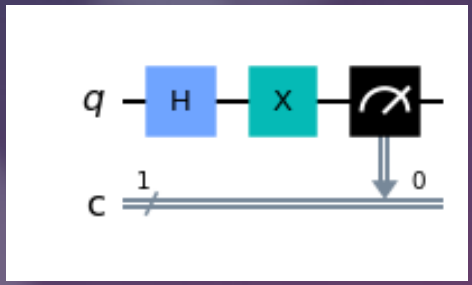


- Alice prepares state of $|+\rangle$ by applying Hadamard Gate, then sends it to Bob.

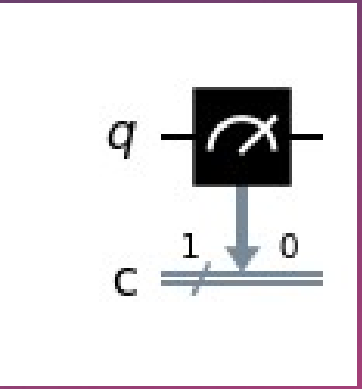


- Bob picks a random number, 0 or 1.

- Bob measures the incoming state with computational or hadamard basis, depending on which random number is picked up.
- If the number is 0, state is measured with hadamard basis.



- If the number is 1, state is measured with computational basis.



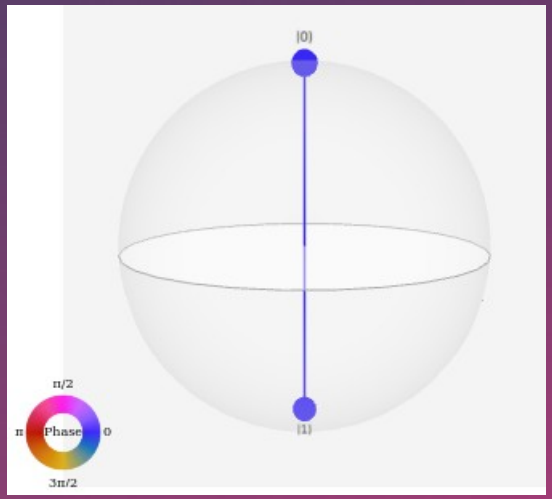
- Bob sends what he measured through classical channel.
- Alice correlates the Bob’s measurement to determine if eavesdropper disturbing channel.
- If the channel is safe, Alice sends the key.

The Correlation Function

- Correlation function can detect eavesdropper

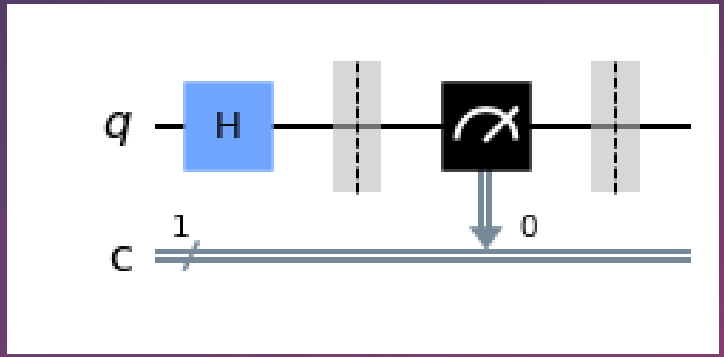
What if there is no eavesdropper?

- The state is the same just like Alice sent
- Alice always send $|+\rangle$



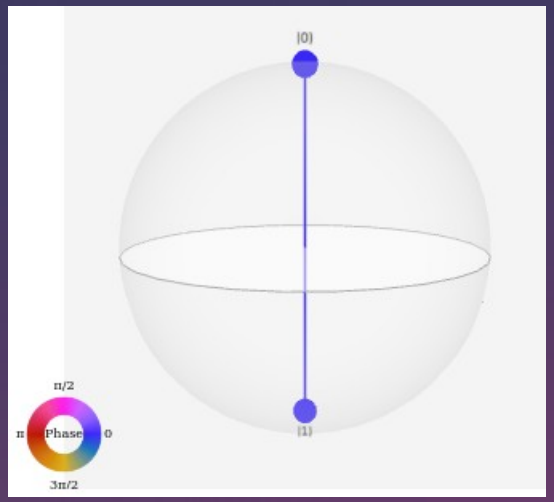
What if the channel eavesdropped?

- Presence of eavesdropper will make $|+\rangle$ collapsed.

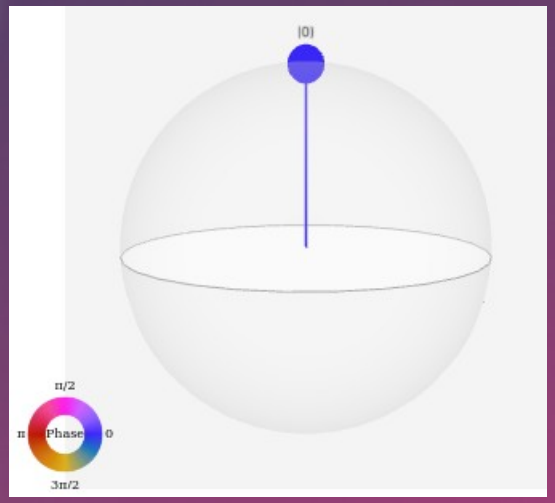


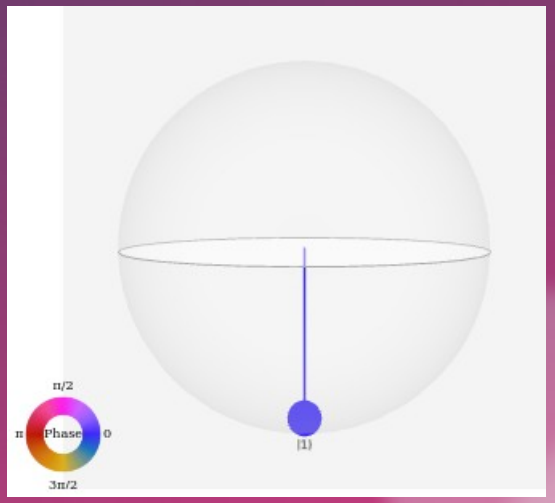
- By this way, Bob receives the state of $|0\rangle$ or $|1\rangle$

- Without eavesdropping, Bob receives $|+\rangle$

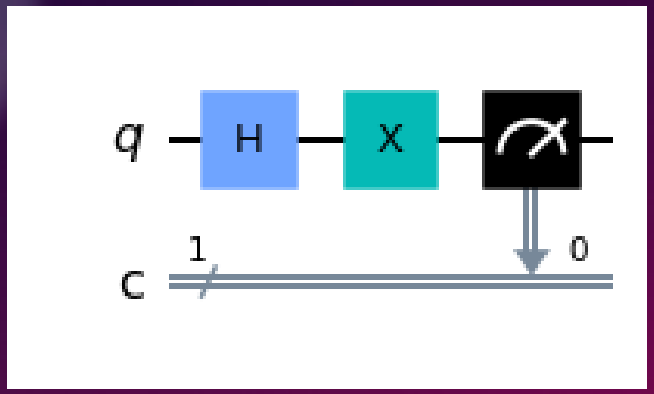


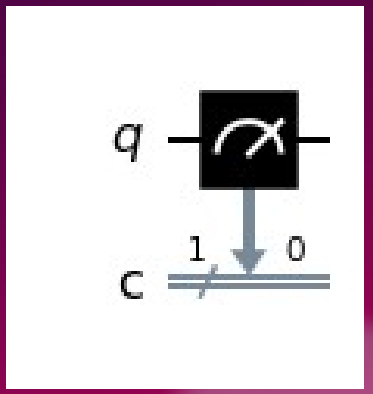
- With eavesdropping, Bob receives $|0\rangle$ or $|1\rangle$





- Bob measures the state in X or Z basis again and again. Then he analyzes the number of zeros and ones.





If Bob Measures with Z Basis:

- If he measures “1”s vast majority of the time, he is receiving the state of $|1\rangle$
- If he measures “0”s vast majority of the time, he is receiving the state of $|1\rangle$
- If he measures “0”s and “1”s 50:50 distributed, he is receiving the state of $|+\rangle$

If Bob Measures with X-Basis

- If he measures “0”s vast majority of the time, he is receiving $|+\rangle$
- If he measures “0”s vast majority of the time, he is receiving $|-\rangle$
- If he measures “0”s and “1”s 50:50 distributed, he is receiving the state of $|0\rangle$ or $|1\rangle$, depending on phase which cannot be measured directly

- After bob deduced which state he is receiving, he send “0” through classical channel if he detects $|+\rangle$ or he send “1” through classical channel if he detects $|1\rangle$.
- Alice receives the value. Receiving “1”s she accumulates them on a variable.
- Lastly, she divides accumulates the value by number of incoming bits. It’s the correlation value. If it’s 0, there is eavesdropper. If it’s different from 0 ,the quantum channel is safe.