Introduction to Quantum Information Science

Shu-Yu Kuo

Outline

- Quantum Key Distribution

Quantum-key distribution (QKD, BB84)

- Alice and Bob uses filters to polarize the light, and encode the values.

$+$

Basis	Value	Encoding
Z (S)	0	$\vert\rightarrow\rangle$
Z (S)	1	$\vert\uparrow\rangle$

$|0\rangle$

$|1\rangle$

X

Basis	Value	Encoding
X (D)	0	$\vert\nearrow\rangle$
X (D)	1	$\vert\nwarrow\rangle$

$|+\rangle$

$|-\rangle$

Quantum-key distribution (QKD, BB84)

- ***Sending a quantum key***

1.	0	0	1	0	1	1	0	1	0	0	1	1	0	1
2.	S	S	D	S	D	D	D	S	D	D	S	S	D	S
3.	$\rightarrow$	$\rightarrow$	$\nwarrow$	$\rightarrow$	$\nwarrow$	$\nwarrow$	$\nearrow$	$\uparrow$	$\nearrow$	$\nearrow$	$\uparrow$	$\uparrow$	$\nearrow$	$\uparrow$
4.	D	S	S	S	D	D	S	D	S	D	S	D	D	D
5.	$\nwarrow$	$\rightarrow$	$\rightarrow$	$\rightarrow$	$\nwarrow$	$\nwarrow$	$\uparrow$	$\nwarrow$	$\rightarrow$	$\nearrow$	$\uparrow$	$\nwarrow$	$\nearrow$	$\nearrow$
6.	$\times$	$\bullet$	$\times$	$\bullet$	$\bullet$	$\bullet$	$\times$	$\times$	$\times$	$\bullet$	$\bullet$	$\times$	$\bullet$	$\times$
7.		$\rightarrow$		$\rightarrow$	$\nwarrow$	$\nwarrow$				$\nearrow$	$\uparrow$		$\nearrow$	
8.		0		0	1	1				0	1		0	

1. Alice's key. 2. Alice's polarizer settings.
3. The photons Alice sends.
4. Bob's detector settings.
5. Bob's measured photons.
6. Alice's report that tells Bob when he guessed wrong. × means an error, • means correct.
7. The photons Bob measured correctly.
8. The key Bob gets combining line 7 with line 4.

Basic Quantum Cryptography

- There are three key principles used in BB84 QKD:

The no-cloning theorem–quantum states cannot be copied.

Measurement leads to state collapse.

Measurements are irreversible

The Control Not Attack

- Suppose that Alice has the states

$$|0_A\rangle \quad |1_A\rangle \quad |+\rangle = \frac{|0_A\rangle + |1_A\rangle}{\sqrt{2}} \quad |-\rangle = \frac{|0_A\rangle - |1_A\rangle}{\sqrt{2}}$$

- Can Eve duplicate this state in any way?
- Let’s suppose that Eve wanted to make a state that gave the same measurement result for both Alice and Eve.
- What Eve can do is start with the state $|\mathbf{0}_E\rangle$ and create the product state

$$|0_A\rangle \otimes |\mathbf{0}_E\rangle = |0_A\rangle|\mathbf{0}_E\rangle$$

The Control Not Attack

$$|0_A\rangle \otimes |\mathbf{0}_E\rangle = |0_A\rangle|\mathbf{0}_E\rangle$$

$$|1_A\rangle \otimes |\mathbf{0}_E\rangle = |1_A\rangle|\mathbf{0}_E\rangle$$

- Now, if Eve applies a controlled NOT gate (CN) to the state, using Alice's qubit as the control bit and Eve's qubit as the target.
- The state becomes:

$$|0_A\rangle \otimes |\mathbf{0}_E\rangle \xrightarrow[CN]{} |0_A\rangle|\mathbf{0}_E\rangle$$

$$|1_A\rangle \otimes |\mathbf{0}_E\rangle \xrightarrow[CN]{} |1_A\rangle|\mathbf{1}_E\rangle$$

- If Alice measure 0, we've got 0 for Eve.
- If Alice measure 1, we've got 1 for Eve.

The Control Not Attack

$$\frac{|0_A\rangle + |1_A\rangle}{\sqrt{2}} \otimes |\mathbf{0}_E\rangle = \frac{|0_A\rangle|\mathbf{0}_E\rangle + |1_A\rangle|\mathbf{0}_E\rangle}{\sqrt{2}}$$

- Now, if Eve applies a controlled NOT gate (CN) to the state, using Alice's qubit as the control bit and Eve's qubit as the target.
- The state becomes:

$$\frac{|0_A\rangle|\mathbf{0}_E\rangle + |1_A\rangle|\mathbf{0}_E\rangle}{\sqrt{2}} \xrightarrow[CN]{} \frac{|0_A\rangle|\mathbf{0}_E\rangle + |1_A\rangle|\mathbf{1}_E\rangle}{\sqrt{2}}$$

- If Alice measure 0, we've got 0 for Eve.
- If Alice measure 1, we've got 1 for Eve.

The Control Not Attack

- What happens if the measurement is made in the X basis?

$$\frac{|0_A\rangle|\mathbf{0}_{\boldsymbol{E}}\rangle + |1_A\rangle|\mathbf{1}_{\boldsymbol{E}}\rangle}{\sqrt{2}} = \frac{|+_A\rangle|+_{\boldsymbol{E}}\rangle + |-_A\rangle|-_{\boldsymbol{E}}\rangle}{\sqrt{2}}$$

- Interestingly the correlation between Alice and Eve has been maintained! Eve's qubit assumes the same value as Alice's qubit in both bases.

The Control Not Attack

- Suppose instead that Alice has

$$|-\rangle = \frac{|0_A\rangle - |1_A\rangle}{\sqrt{2}}$$

- The state becomes:

$$\frac{|0_A\rangle - |1_A\rangle}{\sqrt{2}} \otimes |\mathbf{0}_{\boldsymbol{E}}\rangle = \frac{|0_A\rangle|\mathbf{0}_{\boldsymbol{E}}\rangle - |1_A\rangle|\mathbf{0}_{\boldsymbol{E}}\rangle}{\sqrt{2}}$$

$$\frac{|0_A\rangle|\mathbf{0}_{\boldsymbol{E}}\rangle - |1_A\rangle|\mathbf{1}_{\boldsymbol{E}}\rangle}{\sqrt{2}} \xrightarrow[\boldsymbol{CN}]{} \frac{|0_A\rangle|\mathbf{0}_{\boldsymbol{E}}\rangle - |1_A\rangle|\mathbf{1}_{\boldsymbol{E}}\rangle}{\sqrt{2}}$$

The Control Not Attack

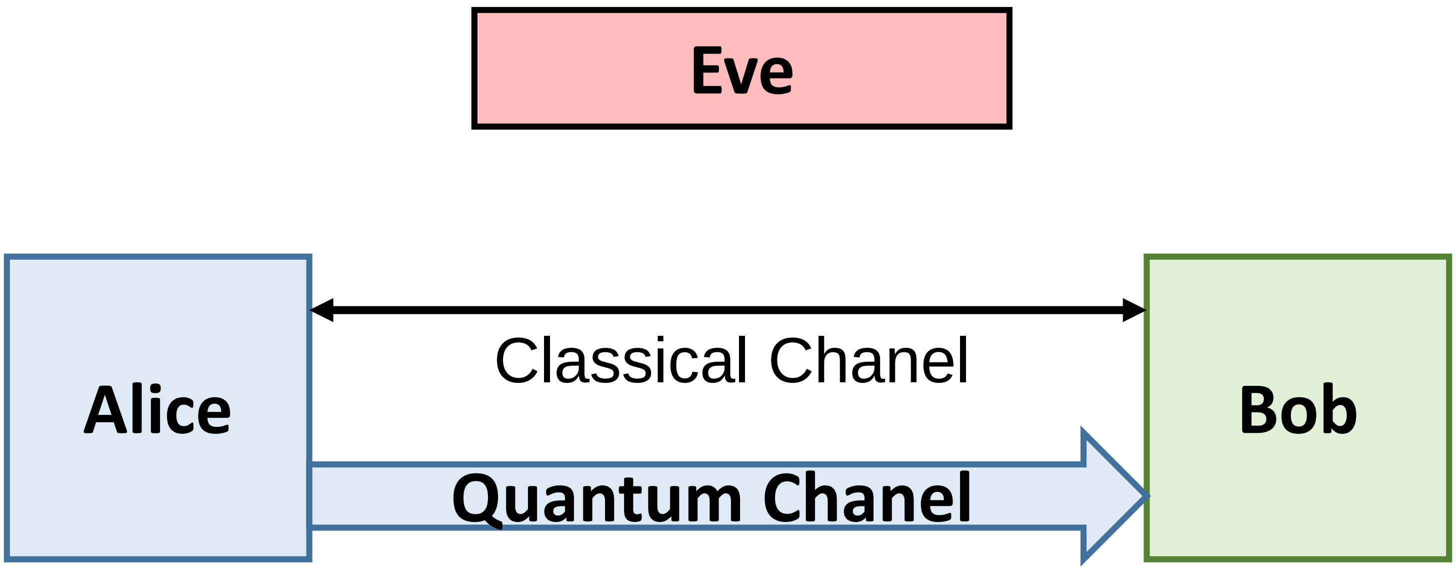
- Does the correlation still hold?
- if we apply the same procedure, we end up with the state

$$\frac{|0_A\rangle|\mathbf{0}_{\boldsymbol{E}}\rangle - |1_A\rangle|\mathbf{1}_{\boldsymbol{E}}\rangle}{\sqrt{2}} = \frac{|+_A\rangle|-_{\boldsymbol{E}}\rangle + |-_A\rangle|+_{\boldsymbol{E}}\rangle}{\sqrt{2}}$$

- We see that Alice and Eve get opposite measurement results. But Eve doesn't know what state Alice had ahead of time—so her measurement results are meaningless.
- Eve cannot, in general, form a product state with $|0_E\rangle$and apply a controlled NOT gate to find out what Alice has.

BB84: Man in the middle attack

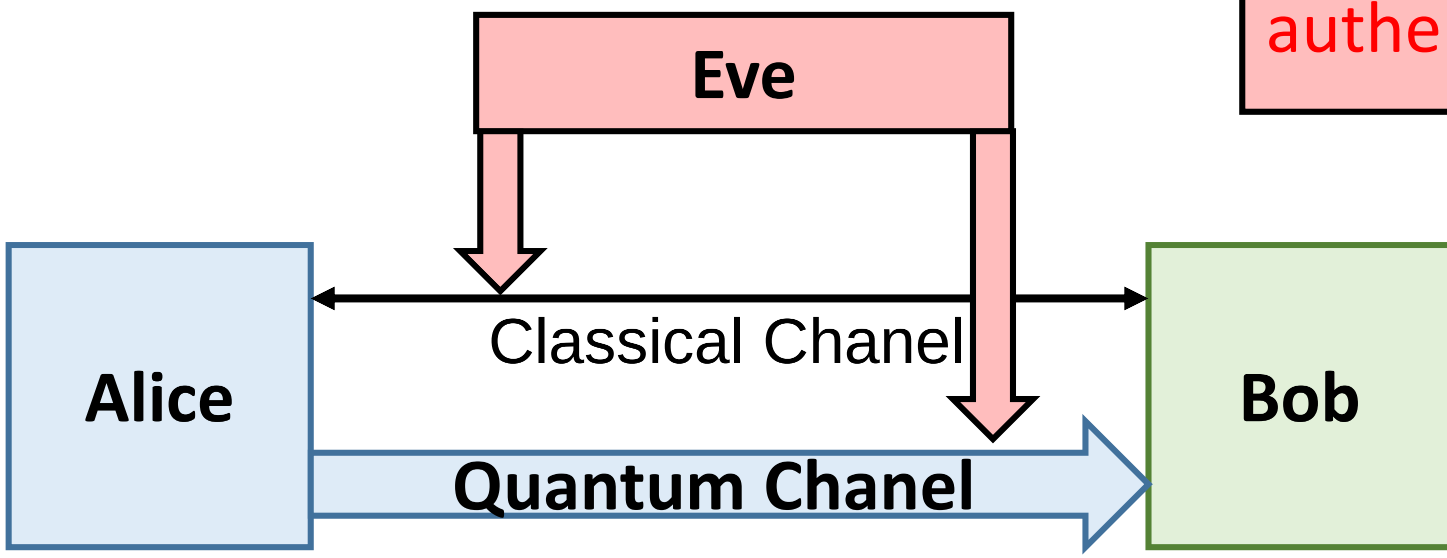
- It is well known that QKD requires a classical public channel with trusted integrity as otherwise a potential eavesdropper (Eve) can easily amount a man-in-the-middle attack



BB84: Man in the middle attack

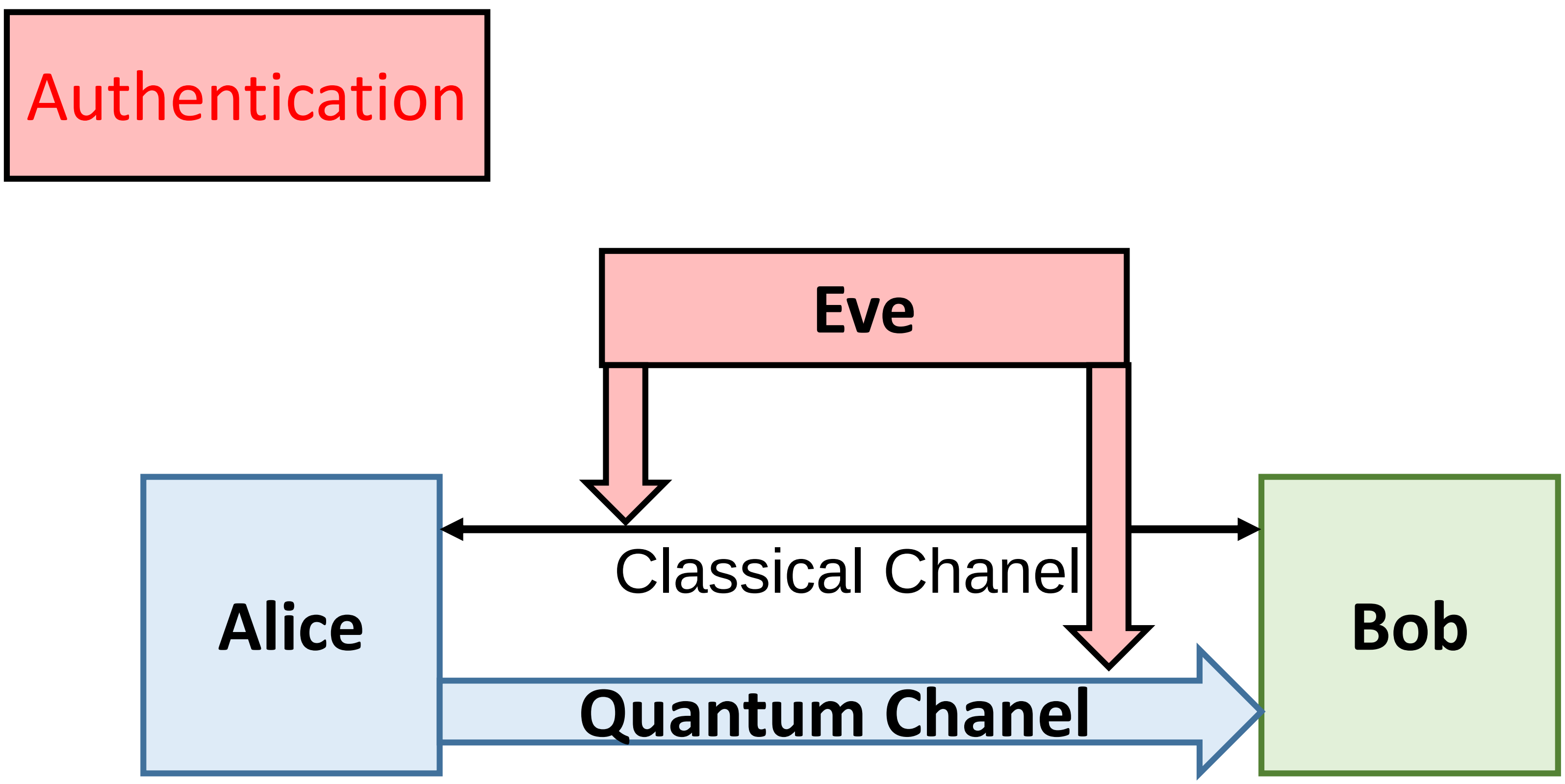
- In case that Eve can **manipulate** messages on the public channel, it is clear that she could sit between Alice and Bob impersonating each of them to the other.
- As a result, Eve would thus share two independent keys with the two legitimate parties and gain full control of all the subsequent communication, without being noticed

authentication



BB84: Man in the middle attack

- It was suggested that this crucial property of the public channel can be implemented using an information-theoretically (i.e., unconditionally) secure authentication scheme



B92 Protocol

- We now give an overview of an updated QKD protocol that is a **simplification of the BB84 protocol**.
- B92 protocol, proposed by Bennett in 1992, uses two non-orthogonal states, for instance S for 0 and D for 1

B92 Protocol

- Alice sends 0 or 1 bits, but 0 she sends in the '+' basis, and 1, in the 'X' basis, and again she randomly chooses the basis.

+

Basis	Value	Encoding
Z	0	$\vert\rightarrow\rangle$

$|0\rangle$

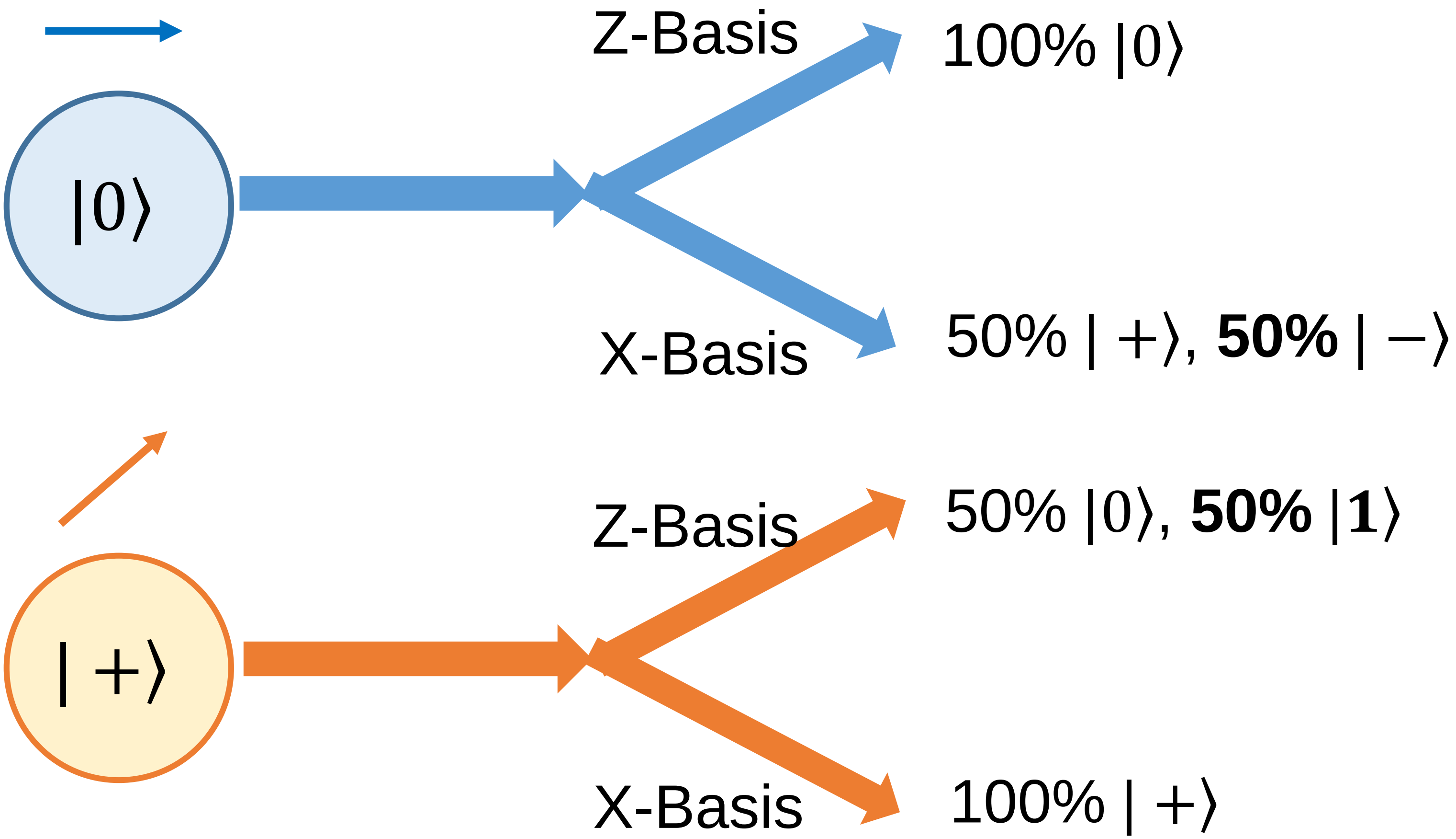
X

Basis	Value	Encoding
X	1	$\vert\nearrow\rangle$

$|+\rangle$

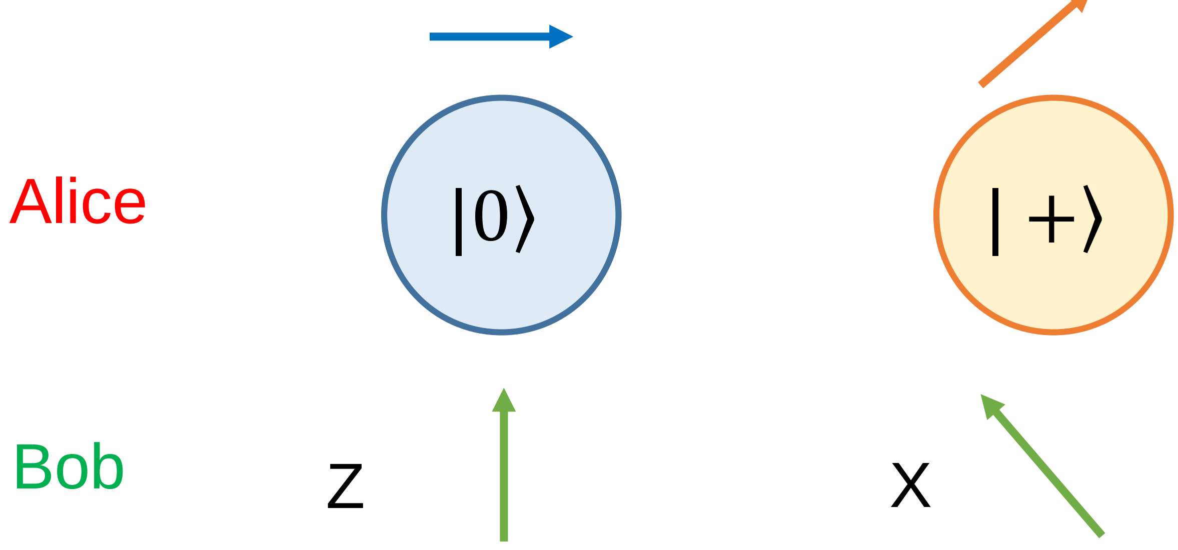
B92 Protocol

- Bob measures the qubits, randomly selecting the computational basis.



B92 Protocol

- Bob measures the qubits, randomly selecting the computational basis.
- Bob can simply tell Alice after each bit she sends whether or not he measured it correctly.
- if Bob obtains the light in the 'X' basis, he writes down '0'
- if Bob obtains the light in the 'Z' basis, he writes down '1'



B92 Protocol

- Simplification of the BB84 protocol
- Bit survival rates: 25%.
- Catch Eve: about 25%

E91 Protocol

- E91 protocol, proposed by Artur Ekert in 1991.

- Quantum Cryptography based on **quantum entanglement.**

E91 Protocol

- We create a **Bell state**, giving one member of the EPR pair to Alice and the second member of the EPR pair to Bob. Suppose that the state used for the EPR pair is

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

- Then we know that Alice and Bob will have measurement results that are completely correlated.

- On the other hand, if the state used is

$$\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

then Alice and Bob will have measurement results that are perfectly anticorrelated.

E91 Protocol

- Alice and Bob measure their respective qubits in randomly chosen bases.
- They keep their series of basis choices private until measurements are completed.
- Then they communicate over an ordinary channel and figure out on which bit positions they used the same basis. They keep these bits to create the key.

E91 Protocol

- Since the measurement results will be perfectly correlated or perfectly anticorrelated, it is easy for Alice and Bob to determine whether or not an eavesdropper is present.

- To check the existence of an eavesdropper, Alice and Bob test Bell's inequalities.

Thank You