EPR Protocol:

Wednesday, April 14, 2021 4:49 PM

Recall: B92

① Alice sends n random bits in ∠ basis

② Bob measures them in either + or X basis's

+ : $|\uparrow\rangle \Rightarrow |\nearrow\rangle = |1\rangle$,

: $|\rightarrow\rangle \Rightarrow$ skip

X : $|\nwarrow\rangle \Rightarrow |\rightarrow\rangle = |0\rangle$

$|\nearrow\rangle \Rightarrow$ skip

③ Bob tells the skipped bits, and finalizes the shared key

④ Verification: sacrifice half of the shared bits to ensure the secrecy of the other half.

1] e.g. B92 Suppose the coin : C = 1 0 1 1 0 0 1

	1	2	3	4	5	6	7	8	9	10	11	12
① Alice bits	1	0	1	1	0	0	1	0	0	0	1	0
Alice qubits	↗	→	↗	↗	→	→	↗	→	→	→	↗	→
Sending	over quantum channel .											
② Bob bases	+	+	X	X	+	X	X	X	+	X	+	+
Bob observes	↑	→	↗	↗	→	↖	↗	↖	→	↗	↑	→
③ Bob bits	1	?	?	?	?	0	?	0	?	?	1	?
Shared key	1			0			0			1		
④ Verification	✓						✓					
Secret key				0						1		

Secret key	0	1

2] The EPR Protocol

- Ekert, in 1991
- Use some pairs of entangled qubits
  EPR: Einstein - Podolsky - Rosen
- two qubits in entangled state: $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

3] EPR Setup:

Alice and Bob are assigned one of each of the entangled pairs from a sequence of entangled qubits. When they are ready to communicate they follow the protocol.

To detect eavesdroping, Alice and Bob can measure the qubits in two different bases: +, X

4] EPR Protocol:

① Alice and Bob measures each qubits in random basis

- measurement can be done in order.

	1	2	3	4	5	6	7	8	9	10	11	12
Alice bases	X	X	+	+	X	+	X	+	+	X	+	X
Alice observes	↗	↖	→	↑	↗	→	↖	→	→	↗	→	↗
Bob bases	X	+	+	X	X	+	+	+	+	X	X	+

Bob bases	X	+	+	X	X	+	+	+	+	X	X	+
Bob observes	↗	→	→	↗	↗	→	↑	→	→	↗	↖	→

② Alice and Bob publicly compare their bases

Agree?	✓	✓	✓	✓	✓
	↗	→	↗ →	→ →	↗

5] Note: • The entangled pair could be exposed to noise and become disentangled, or Eve could take hold of it, measure it, and send it back.

• A verification step (like step ④ in BB84) can be applied: Alice and Bob randomly sacrifice half of the shared bit and publicly compare them, to ensure the secrecy of the other half.