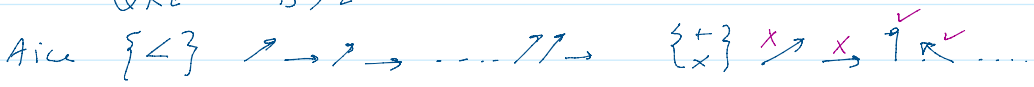
EPR QKE

Sunday, October 29, 2023 5:51 PM

Recall: QKE - BB84

QKE - B92



1] EPR QKE (§9.4)

- by Ekert in 1991
- EPR: Einestein - Podolsky - Rosen
- Based on entanglement
- Use entangled qubits: $|\varphi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

2] EPR Setup:

① Generate a sequence of entangled qubit pairs $\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)$

② Alice and Bob are assigned one of qubit of each pair from the sequence in ①

③ When they are ready to communicate, they follow the protocol using these entangled qubits to exchange the key.

④ To detect eavesdroping, Alice and Bob can measure the qubits in two different basis: +, ×

3] The EPR protocol:

① Alice and Bob measure each qubit in random bases
- flip a coin to determine the basis {+, ×}, and measure
- measuring can be done in any order.

② Alice and Bob publicly compare the bases. If they match, the measured bit stored as a shared bit.

③ Verification: Alice and Bob can verify the secrecy of the bits by randomly sarificing half of the shared bits and publicly compare them.

4] e.g.

pair # →	1	2	3	4	5	6	7	8	9	10	11	12
① Alice bases	×	×	+	+	×	+	×	+	+	×	+	×
Alice observes -	↗	↖	→	↑	↗	→	↖	→	→	↗	→	↗
Bob bases	×	+	+	×	×	+	+	+	+	×	×	+
Bob obsereves	↗	→	→	↗	↗	→	↑	→	→	↗	↖	→
② Compare bases	✓		✓		✓	✓		✓	✓	✓		
Shared bit	1		0		1	0		0	0	1		
③ Verification	✓		✓							✓		
					1	0		0	0			