B92 QKE

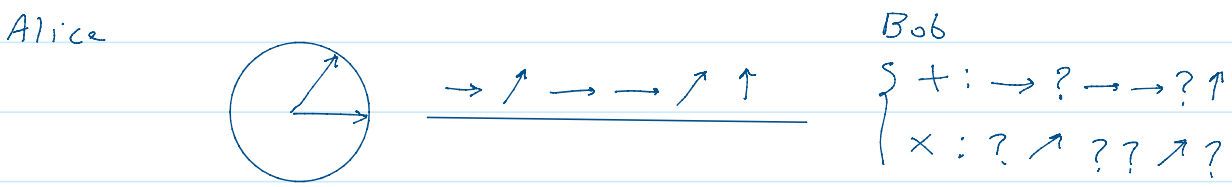
Tuesday, October 24, 2023 5:40 PM

Recall: BB84 QKE protocol

- Use 2 different orthogonal basis: +, ×

1] The B92 QKE protocol:

- by Bennett, in 1992
- use one non-orthogonal basis (∠) to send the qubits, and 2 bases (+, ×) to receive.



2] B92 Setup:

① Alice uses ∠ basis to send n qubits

$$\{|\rightarrow\rangle, |\nearrow\rangle\} = \{\begin{bmatrix}1\\0\end{bmatrix}, \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}\}$$

($|0\rangle = |\rightarrow\rangle$, $|1\rangle = |\nearrow\rangle$)

② Bob uses + or × to measure the received qubits.

3] B92 protocol:

① Alice send n random qubits to Bob in ∠ basis.

- flip a coin n times to determine the qubits

$$\text{Coin} = \begin{cases} H: & |0\rangle = |\rightarrow\rangle \\ T: & |1\rangle = |\nearrow\rangle \end{cases}$$

② Bob measures the qubits in eithe + or × basis.

- flip a coin to determine the basis
- There are 4 possible cases:

Bob uses	Bob observes	Outcome
+	$\|\uparrow\rangle$	Alice sent $\|\nearrow\rangle = \|1\rangle$
	$\|\rightarrow\rangle$	not sure, skip this bit
×	$\|\nearrow\rangle$	not sure, skip this bit.
	$\|\nwarrow\rangle$	Alice sent $\|\rightarrow\rangle = \|0\rangle$

③ Bob publicly tells Alice the skipped bits.
⇒ the remaining bits are the shared key.

④ For verification, Alice and Bob sacrifice half of the shared key to ensure the secrecy of the other half (the secret-key) similar to BB84.
⇒ The length of the secret key is $n/4$ on average.

4] Usage:

① the secret key can be used in any symmetric chiper (like AES) ore one-time-pad.

② Alice and Bob can obtain a secret key of any desired length (m bit) by sending $n \geq 4 \cdot m$ qubits initially (at step ①)

5] e.g. B92

bit #	1	2	3	4	5	6	7	8	7	10	11	12
① Alice bits	0	0	1	0	1	0	1	0	1	1	1	0
Alice qubits	→	→	↗	→	↗	→	↗	→	↗	↗	↗	→

↓ sending over Q-channel.

② Bob basis	×	+	×	×	+	×	+	+	×	+	×	+

↓ sending over Q-channel.

② Bob basis X + X X + X + + X + X +

Bob observes ↖ → ↗ ↖ ↑ ↖ → → ↗ ↑ ↗ →

③ Bob bits 0 ? ? 0 1 0 ? ? ? 1 ? ?

shared key 0 0 1 0 1

④ verification ↓ ✓ ↓ ↓ ✓

Secret-key: 0 1 0 = 010