BB84 QKE

Friday, October 20, 2023 4:55 PM

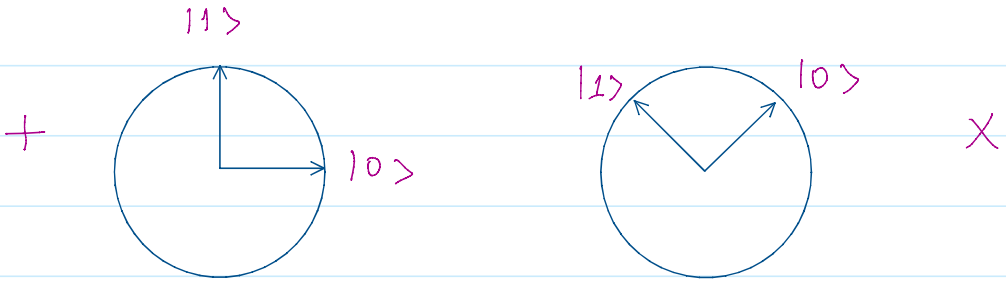
Recall: Quantum Channel

① Measuring a qubit alters it.

② No-cloning

1] BB84:

Bennett and Brassard Protocol, 1984



2] BB84 Setup:

① Basis:

Rectilinear (+): $\{|\rightarrow\rangle, |\uparrow\rangle\} = \{|0\rangle, |1\rangle\} = \{\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}\}$

Diagnal (X): $\{|\nwarrow\rangle, |\nearrow\rangle\} = \{\frac{1}{\sqrt{2}}\begin{bmatrix}-1\\1\end{bmatrix}, \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}\}$

② States

State	Basis +	Basis X
$\|0\rangle$	$\|\rightarrow\rangle$	$\|\nearrow\rangle$
$\|1\rangle$	$\|\uparrow\rangle$	$\|\nwarrow\rangle$

3] Superposition:

3] Superposition:

"When Alice uses (X) basis to send $|\nearrow\rangle$ to Bob and Bob measures it in (+) basis"

$$|\nearrow\rangle = \frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\rightarrow\rangle \quad \text{in (+) basis}$$

$$|\nwarrow\rangle = \frac{1}{\sqrt{2}}|\uparrow\rangle - \frac{1}{\sqrt{2}}|\rightarrow\rangle \quad \text{in (+) basis}$$

$$|\uparrow\rangle = \frac{1}{\sqrt{2}}|\nearrow\rangle + \frac{1}{\sqrt{2}}|\nwarrow\rangle \quad \text{in (X) basis}$$

$$|\rightarrow\rangle = \frac{1}{\sqrt{2}}|\nearrow\rangle - \frac{1}{\sqrt{2}}|\nwarrow\rangle \quad \text{in (X) basis}$$

4] BB 84 Protocol (§ 9.2)

① Alice send n random bits in random basis {+, x}

- flip a coin n times to determine the classical bits {0,1}

  e.g. 0 1 1 0 1 1 1 0 1 0 1 0

- flip a coin n times to choose the basis for each bit:

  + + X + + + X + X X X +

② Bob receives the n bits using random measurements

- flip a coin n times to select the basis for each bit:

  X + X X + X + + X X X +

- Measure each received qubits using the selected basis:

- Bit Received: $b_1\ b_2\ b_3 \ldots$

$$\text{BitReceived}[i] = \begin{cases} \text{BitSent}[i] & \text{if SendBasis} = \text{MeasuredBasis} \\ \text{random } \{0,1\} & \text{otherwise} \end{cases}$$

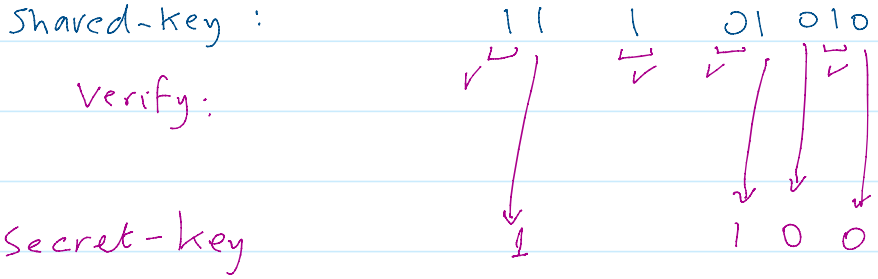
③ Alice and Bob publicly compare the used basis.

Alice (Send Bits)	0 1 1 0 1 1 1 0 1 0
Alice Basis:	+ + X + + + X + X X +
Bob (Basis):	X + X X + X + + X X +
Bob (check)	- √ √ - √ - - √ √ √ √
Shared-key:	1 1 1 0 1 0

④ To ensure privacy:

Alice and Bob publicly compare half of the bits in the shared-key to ensure the secrecy of the key.

- Choose half of the shared key at random, and verify that public-key.



5] How many qubits are needed?

For n-bit secret-key, we need (4n) qubit at step ①

Quiz 1

#1. Integrity

#2. $27543_0 \times 18356_2 \pmod 9$

$\equiv 3 \times 7$

$\equiv 3 \pmod 9$

#3. Playfair $25!$

Hill $\leq 26^{5\times 5} = 26^{25}$

#4.

$198 = 1 \cdot 153 + 45$ ——— ①

$153 = 3 \cdot 45 + 18$ ——— ②

$45 = 2 \cdot 18 + 9$ ——— ③

$18 = 2 \cdot 9 + 0$ ← gcd

$9 = \square \cdot a + \square \cdot b$

by ③ $9 = 45 - 2 \cdot 18$

$= 45 - 2 \cdot (153 - 3 \cdot 45)$

$= -2 \cdot 153 + 7 \cdot 45$

$= -2 \cdot 153 + 7 (198 - 1 \cdot 153)$

$= +7 \cdot 198 -$