B92 Protocol

Monday, April 12, 2021 8:30 AM

New Class Time: 4:45 PM (Ramadan)

Recall: BB84 Protocol:

uses 2 different orthogonal bases +, ×

① Alice sends n random bits using random bases

② Bob receives n bits using random basis measurements

③ Alice and Bob publicly compare bases used.

Bit #	1	2	3	4	5	6	7	8	9	10	11	12
① random bit	0	1	1	0	1	1	1	0	1	0	1	0
bases	+	+	×	+	+	+	×	+	×	×	×	+
Alice sends	→	↑	↖	→	↑	↑	↖	→	↖	↗	↖	→

Sending over quantum channel (qubits)

② Received	→	↑	↖	→	↑	↑	↖	→	↖	↗	↖	→
random bases	×	+	×	×	+	×	+	+	×	×	×	+
Bob observes	↗	↑	↖	↗	↑	↗	↑	→	↖	↗	↖	→
Bob bits	0	1	1	0	1	0	1	0	1	0	1	0
③ Compare	–	✓	✓	–	✓	–	–	✓	✓	✓	✓	✓
Shared key		1	1		1			0	1	0	1	0

1] Cont. BB84 (security verification)

④ Alice and Bob publicly compare half of the shared bits

④ Alice and Bob publicly compare half of the shared bits for verification.

- On average, number of shared key bits = $\frac{n}{2}$ bits
- Bob randomly chooses half of them ($\frac{n}{4}$ bits) and compares them with Alice bits (for verification)
  - if they disagree by more than t bits, then it means Eve was listening.
    - discard the key, try another protocol.
  - if they agree by more than ($\frac{n}{4} - t$ bits); then then key is "correct" and secure.

Here, the t bits are attributed to the noise in the quantum channel.

③ Compare	—	✓	✓	—	✓	—	—	✓	✓	✓	✓	✓
Shared key		1	1		1			0	1	0	1	0
④ Agree			✓						✓	✓		✓
Secret key		1			1			0			1	

2] Usage:

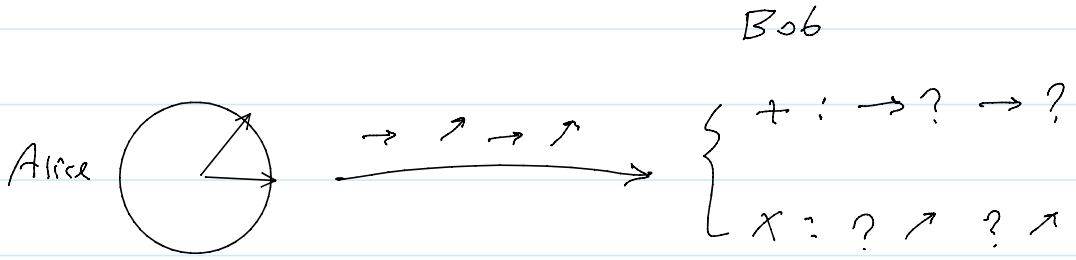
- the secret key can be generated at any desired length (m) by sending $n \geq 4m$ qubits at step ①

- the secret key in One-time pad or any crypto system.

cryptosystem.

3] The B92 QKE Protocol: (§9.3)

- by Bennett, in 1992
- uses nonorthogonal basis ($\angle$) to send and (+), (X) to receive.



4] B92 set up:

Alice uses one basis ($\angle$)

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

0 1

5] B92 Protocol:

① Alice sends n random bits in $\angle$ basis
- flip a coin n times, and sends the qubits.

② Bob measures the qubits in either + or X basis.
- flip a coin to determine the basis.
- There are 4 possible cases:

Bob uses	Bob observes	outcome

Bob uses	Bob observes	outcome
+	$\|\uparrow\rangle$	Alice must send $\nearrow = \|\frac{1}{2}\rangle$
	$\|\rightarrow\rangle$	not sure, skip
×	$\|\nearrow\rangle$	not sure, skip
	$\|\nwarrow\rangle$	Alice must send $\rightarrow = \|0\rangle$

(3) Bob publicly tells Alice the skipped bits.
$\Rightarrow$ the remaining bits are the shared key.

(4) for verification, Alice and Bob can sacrifice half the key to ensure the secrecy of the other half of the key (as in BB84)
Thus, to make sure Eve was not listening.

See Example on p. 275