ICS 562 - Quantum Cryptography

Dr. Sultan Almuhammadi

Homework 3 – Extra Problems

Coin: 10100101… (repeat). Use 1 for Heads and +, and 0 for Tails and x whenever applicable.

Note: If you need to make a random decision, use the above coin bit sequence. Restart the sequence for each question and each part. Repeat the sequence if you need more random bits in the same part.

EP1. In the BB84 QKE protocol, suppose Alice sent 12 qubits to Bob using random bases. Then Bob receives the qubits using random bases as shown in the table below.

Bit number	1	2	3	4	5	6	7	8	9	10	11	12
1. Alice bits	0	0	1	1	1	0	1	0	1	1	0	0
2. Alice bases	x	+	x	x	+	+	x	x	+	+	+	x
3. Alice sends	↗	→										
4. Bob bases												
5. Bob observes												
6. Bob bits												
7. Shared key												

(a) Show what Alice will send (complete Row 3 in the table above).
(b) Flip a coin to determine Bob random bases in Row 4. (Use the coin given above).
(c) Complete Bob observation (in Row 5) according to his basis for each bit. If more than one possible measurement is possible, select one at random (flip a coin to decide).
(d) Compute Bob bits (in Row 6) according to the observation in (c).
(e) Find the shared key exchanged by this protocol (in Row 7).
(f) Explain a verification method that allows Alice and Bob to ensure the security of the shared key. How many bits do they need to sacrifice? What happens if the verification fails?

EP2. In the B92 QKE protocol, suppose Alice sent 12 qubits to Bob. Then Bob receives the qubits using random bases as shown in the table below.

Bit number	1	2	3	4	5	6	7	8	9	10	11	12
1. Alice bits	1	0	0	1	1	0	1	0	1	1	0	0
2. Bob bases	x	+	x	x	+	+	x	x	+	+	+	x
3. Bob observes	↗	→										
4. Bob bits												
5. Shared key												

(a) Complete Bob observation (in Row 3) according to his basis for each bit. If more than one possible measurement is possible, select one at random (flip a coin to decide).
(b) Compute Bob bits (in Row 4) according to the observation in (a).
(c) Find the shared key exchanged by this protocol (in Row 5).
(d) Explain a verification method that allows Alice and Bob want to ensure the security of the shared key. Flip a coin for each bit to decide whether you want to sacrifice or not. How many bits got sacrificed? Find the secret key.
(e) What is the main advantage of this protocol over the BB84?