Quiz Assignment 5 Solutions

Note: All multi-qubit state representations are written with LSB on the left, unless specified otherwise

Quantum Key Distribution

1. The key generated during BB84 is. (1 point)
    A. Deterministic
    B. Random

    Solution: B
    The key generated by QKD is always random.
2. It is possibly to detect an 'Intercept and Resend' attack on BB84 (1 point)
    A. True
    B. False

    Solution: A
    There is a possibility that measurement by the eavesdropper will change the state that is sent to Bob, so such an attack can be detected by comparing some of the key bits between Alice and Bob.
3. The quantum channel used in the BB84 protocol is: (1 point)
    A. Bidirectional
    B. Unidirectional

    Solution: B
    Only Alice can send her qubits to Bob, so the channel is unidirectional.
4. Is it possible for Oscar to copy any state Alice sends without being detected? (1 point)
    A. Possible
    B. Impossible

    Solution: B
    This is a consequence of the no-cloning theorem.
5. Given the following information, find the key generated by the BB84 QKD protocol:(3 points)

    Alice's State: 1110001000000100100101010111011000
    Alice's Bases: 1011101011010011111011111011110001
    Bob's Bases: 0000010101111000010001010111010000

    A. 00010000011000
    B. 0000000000010011
    C. 1001001111100
    D. 11000111110

    Solution: C
    Alice's and Bob's chosen bases match only 13 times. If we look at the bits Alice encoded for those basis choices, we can see that option C is the correct choice.
6. Out of all the qubits that Alice sends to Bob, what fraction (on average) of it will be a part of the key after comparing basis choices? (3 points)
    A. 1/2
    B. 1/4
    C. 1/3
    D. 3/4

    Solution: A
    A bit will become part of the key only if Alice and Bob chose the same basis for that bit. There are four possible situations: 'CC', 'CH', 'HC' and 'HH' (the first letter is Alice's basis choice, and the second letter is Bob's). Only 2/4 correspond to them choosing the same basis. Hence, on average, the key will contain 1/2 of the original number of bits Alice prepared.

7. For large enough key length, the key generated by BB84 will have an equal number of zeros and ones. (3 points)
    A. True
    B. False

    Solution: A

    Since the choice of Alice's bit (that they want to encode) and the choice of Alice's basis are unrelated, each bit is equally likely to be zero or one. This can be seen from the table provided in the programming notebook on BB84.

8. In the presence of an eavesdropper and under the 'intercept and re-send' attack model, what is the probability of a bit mismatch when Alice and Bob compare their key bits? (2 points)
    A. 1/2
    B. 1/4
    C. 1/3
    D. 3/4

    Solution: B
    The key bits are decided based on the places where Alice's and Bob's bases choices match. Unbeknownst to them, Oscar (the adversary) might have chosen a different basis. The probability of this is 1/2 (refer Q6). Now, since Oscar has chosen a different basis in these cases, there are two equally probable outcomes when Bob measures the qubit. Only one of the two outcomes matches the original bits Alice encoded. So, the probability that Bob measures the different outcome is 1/2 again. Hence the total probability is

$$P_{mismatch} = P_{basis\ mismatch} \times P_{different\ outcome} = 1/2 \times 1/2 = 1/4$$

9. Given the following information for a BB84 process with an 'intercept and re-send' adversary Oscar,

Alice's State:	00001111110110011010110111100100
Alice's Bases:	11011110011000110111110111111001
Oscar's Bases:	11111010101111001011000110000011
Bob's Bases:	10001101001001111010001000010001

    Find the length key generated by the BB84 QKD protocol after sifting: (2 points)
    A. 11
    B. 15
    C. 17
    D. 28

    Solution: B
    The key length is determined only by the number of places where Alice and Bob chose the same bases. In this case, it is 15.
10. Using the information in Q9, what is the least number of key bits that Oscar knows? (3 points)
    A. 2
    B. 4
    C. 5
    D. 6

    Solution: D
    If Oscar chooses the same basis as Alice and Bob, then he has perfect knowledge of those bits. This is the minimum number of key bits he knows.