Quantum Cryptography

Dr. Sultan Almuhammadi

Homework 4

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.

Q1. In the EPR protocol, suppose Alice and Bob are given 10 pairs of entangled qubits. They measured these qubits using the bases in the table below. Complete the table below and give a valid example of a shared key. (Hint: flip a coin whenever needed to decide on random measurements)

Bit number	1	2	3	4	5	6	7	8	9	10
Alice bases	x	+	x	x	+	+	x	x	+	+
Bob Bases	+	+	x	+	+	x	x	+	x	x

Q2. In the classical telephone coin-flipping protocol, explain the potential risk in each of the following scenario. Also explain what Alice can/should do to take advantage/reduce the risk in each situation.

(a) If Alice knows that Bob never checks if $p < q$.
(b) If Alice knows that Bob never checks if both p and q are primes.
(c) If Alice doubts that Bob might have access to a decent quantum computer.

Q3. In the quantum coin-flipping protocol, suppose Alice sent 10 qubits to Bob using the (x) basis. 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
1. Alice bits	1	0	0	1	1	0	1	0	0	1
2. Alice sends										
3. Bob bases	x	+	x	x	+	+	x	x	+	x

(a) Complete Row 2 by showing the states of the qubits Alice sends to Bob.
(b) Show both the *rectilinear* and *diagonal* tables computed by Bob. (Hint: flip a coin to determine random choices if needed).
(c) If Bob correctly guesses Alice basis (x), explain why Alice cannot cheat and claim winning at this point.

Q4. Suppose Alice and Bob use quantum one-time pad cryptosystem to communicate qubits.
(a) Show how the encryption is performed to encrypt a single qubit.
(b) Show how the decryption is done, and briefly argue about the correctness.
(c) Suggest a way to implement the (X^k) gate in the encryption/decryption circuits.

Q5. Let $b_1 = [-1, 1]^T$ and $b_2 = [1, 2]^T$ be the basis of the lattice Λ.

(a) Plot the points for all vectors in Λ to show the pattern of the lattice between coordinates (–10) and (10) in both dimensions.

(b) Determine whether following vectors belong to Λ, and briefly justify your answer in each case:

- [74, 70]
- [70, 75]
- [15, 135]

Q6. Find another basis (B') for the lattice Λ in Q5. Use a unimodular matrix to prove that both bases generate the same lattice.

Q7. Consider the lattice defined by the following basis: $[1, 4]^T$ and $[3, 7]^T$. Find:

(a) A shortest non-zero vector in this lattice

(b) A vector closest to $[20, 21]^T$

Q8. In post-quantum cryptography, given the public matrix A, Alice's secret s, and error vector e all defined in Z_{17} as shown below:

$$A = \begin{pmatrix} 15 & 2 & 8 & 1 \\ 3 & 4 & 3 & 2 \\ 7 & 6 & 5 & 4 \\ 10 & 1 & 2 & 3 \\ 12 & 3 & 9 & 0 \end{pmatrix}, \; s = \begin{pmatrix} 9 \\ 1 \\ 14 \\ 8 \end{pmatrix}, \; e = \begin{pmatrix} 1 \\ 0 \\ -1 \\ 1 \\ 2 \end{pmatrix}$$

(a) Compute Alice's public key ($x = A.s + e$)

(b) Explain why it is computationally infeasible for Eve to find the secret s knowing only the matrices A and x in general.

Total: 8 exercises.