Please list your collaborators and provide any references that you may have used in your solutions.

Question 1

In this question you will analyze the following bit commitment protocol based on a pseudorandom generator $G\colon \{0,1\}^k \to \{0,1\}^{3k}$. First, receiver picks a random string $R \in \{0,1\}^{3k}$ and shares it with sender. To commit to a bit s, sender chooses a random X and sends $G(X) + s \cdot R$ (i.e., $G(X)$ when $s = 0$ and $G(X) + R$ when $s = 1$). To reveal, sender reveals s and X and receiver checks that his commitment C equals $G(X) + s \cdot R$.

(a) Prove that if G is a pseudorandom generator then the commitment is hiding. Work out the parameters.

(b) Show that with probability $1 - 2^{-k}$ over the choice of R there does not exist a pair of inputs X and X' such that $G(X) + G(X') = R$. (**Hint:** Take a union bound over all pairs.)

(c) Prove that the commitment is binding. Work out the parameters.

Question 2

Let $f\colon \{0,1,2\} \times \{0,1,2\} \to \{0,1\}$ is the equality function $f(x,y) = 1$ if $x = y$ and 0 if $x \neq y$. Consider the following key exchange protocol based on a two-party protocol for f: Alice and Bob choose random inputs x and y from $\{0,1,2\}$ and run the protocol. After Bob obtains $f(x,y)$ he forwards this value to Alice. If $f(x,y) = 1$ each party outputs their input, and otherwise they repeat.

(a) Show that Alice's and Bob's output are equal and uniformly random with probability 1. What is the expected number of repetitions?

(b) In question 4 of the midterm you showed that if a two-party protocol for f is simulatable against honest-but-curious then any two transcripts of the protocol are (s, ε)-indistinguishable. Assuming this, show that the key exchange protocol is secure, namely that the the key and the transcript are indistinguishable from a pair of independent random variables. Work out the parameters.

Question 3

(20 points) Let Com be a bit commitment scheme. Consider the following variant Com': To commit to a bit x, Sender chooses a random bit r and sends $Com'(x) = (Com(r), Com(x + r))$ as his commitment. Here + stands for XOR.

(a) Describe the revealment and the verification procedures for Com'.

(b) Prove that if Com is perfectly binding then so is Com'.

(c) Prove that if Com is hiding then Com' is also hiding. Work out the parameters.

Now Alice has committed to two bits x and x' using Com' and wants to prove to Bob that the two are equal. Their commitments are

$$Com'(x) = (Com(r), Com(x + r)) \quad \text{and} \quad Com'(x') = (Com(r'), Com(x' + r')).$$

Consider the following proof system:

1. Alice sends Bob the value $s = r + r'$.
2. Bob sends Alice a random bit b.
3. If $b = 0$, Alice reveals r and r'. If $b = 1$, Alice reveals $x + r$ and $x' + r'$.
4. Bob verifies the values revealed by Alice and accepts if their XOR equals s.

Assume that Com is perfectly binding and show the following.

(d) Completeness: If x equals x' then Bob accepts with probability 1.

(e) Soundness: If x does not equal x' then upon interacting with a cheating Alice, Bob accepts with probability at most half.

(f) Zero-knowledge: If x equals x' and Com is hiding then the view of a cheating Bob (consisting of $Com'(x)$, $Com'(x')$, his randomness, and Alice's messages) is efficiently simulatable. Work out the parameters.