Problem 1

Let $G\colon \{0,1\}^k \to \{0,1\}^{4k}$ be an (s, ε) pseudorandom generator. Consider the following bit commitment protocol. Here, Alice gets no input, and Bob gets input $b \in \{0,1\}$:

A: Choose a random $R \in \{0,1\}^{4k}$ and send it to Bob.

B: **(Commitment phase)** Upon receiving R', choose a random $K \in \{0,1\}^k$. To commit to $b = 0$, send $G(K)$. To commit to $b = 1$, send $G(K) + R'$.

A: Receive the commitment C'.

B: **(Revealment phase)** Send K and the committed bit b to Alice.

A: If $C' = G(K')$ and $b' = 0$ or $C' = G(K') + R$ and $b' = 1$, accept; otherwise, output `error`.

This is a bit different from the commitment scheme we say in class because it is interactive: Alice has to send a message to Bob before Bob does his commitment and revealment.

(a) Show that if Alice is honest, the scheme has the following binding property: For every B^*,

$$\Pr_{R \sim \{0,1\}^{4k}}[A \text{ accepts and } b' \neq b] = 2^{-\Omega(k)}.$$

(b) Show that if Bob is honest, the scheme has the following hiding property: For every A^* of size at most s',

$$\left|\Pr_{(A^*, B(b))}[A^* \text{ accepts} \mid b = 0] - \Pr_{(A^*, B(b))}[A^* \text{ accepts} \mid b = 1]\right| \leq \varepsilon'$$

(for a suitable choice of s' and ε').

(c) Can you extend this protocol so that Bob can commit not only to a single bit, but to any value in the set $\{0,1\}^k$?

Problem 2

Let p, q be prime numbers where $(p-1)/2$ and $(q-1)/2$ are odd and let $n = pq$. Suppose Alice holds some $a \in \mathbb{Z}_n^*$ and Bob has an x such that $x^2 = a$. Bob wants to prove to Alice that a is a quadratic residue. Consider the following protocol:

B: Choose a random $r \in \mathbb{Z}_n^*$ and send r^2 to Alice.

A: Upon receiving b, choose a random message $\{\mathtt{b}, \mathtt{ab}\}$ and send it to Bob.

B: If you receive `b`, send r; if you receive `ab`, send xr.

A: Upon receiving z: If you sent `b`, accept if $z^2 = b$; if you sent `ab`, accept if $z^2 = ab$; reject otherwise.

Show that this protocol is zero-knowledge for the proof relation QR given by

$$((n, a), x) \in QR \quad \text{if} \quad a = x^2, \text{ where } a, x \in \mathbb{Z}_n^*.$$

Calculate the simulation overhead of this protocol.