Week 10 Exercises (ECE 598 DA)

Exercise (Random Linear Combination for Multiple Equations): Suppose $x = (x_1, \ldots, x_n)$ are values secret-shared among two verifiers, and the prover claims that x satisfies m independent linear equations: $Ax = b$, where A is an $m \times n$ public matrix over $\mathbb{F}$ and $b \in \mathbb{F}^m$ is public. Describe a protocol using a single random linear query that allows the verifiers to check all m equations at once with soundness error at most $1/|\mathbb{F}|$. Prove that your protocol has perfect completeness and statistical soundness, and argue why it is honest-verifier zero-knowledge.*(Hint: Use a random weight for each equation to combine them.)*

Exercise (Fully Linear PCP for a Simple Relation): Consider the language $L = \{(a, b, c) \in \mathbb{F}^3 : c = a + b\}$, a simple relation stating that c is the sum of a and b. Construct a fully linear PCP for this relation and prove that it satisfies completeness, soundness, and strong HVZK (input hiding). Then describe how this proof can be carried out if a, b, c are secret-shared between two verifiers.*(Hint: No additional proof string π is actually needed here aside from the input itself.)*

Exercise (Simulation in Distributed ZK Proofs): Consider a general fully linear PCP-based protocol where a prover shares a proof π among M verifiers who hold shares of input x. They perform linear queries and combine answers to decide acceptance. Explain how one would simulate the view of all M verifiers in such a protocol (assuming they are honest-but-curious) to prove the strong HVZK property. Specifically, argue why the distributed transcript (consisting of each verifier's received queries, their share of queries/answers, and final decision) can be simulated without knowing the secret input x or proof π, given that the underlying FLPCP is HVZK.