Cryptography and Machine Learning - Homework 1

Due date: November 3, 2026. **Submission:** Via Moodle.

AI guidelines. AI may be used for tutoring and conceptual clarification, but not to write the personal text (Question 3). It is your choice if you want to write the answers to Questions 1 and 2 on your own (I do recommend writing these answers on your own but will not enforce it).

Question 1. Let $F_s : \{0,1\}^n \to \{0,1\}$ be a secure PRF family with a k-bit key. Assume $2^n \geq 2k$, choose any fixed distinct inputs $x_1, \ldots, x_{2k}$, and define

$$G(s) = F_s(x_1) \| \cdots \| F_s(x_{2k}) \in \{0,1\}^{2k}.$$

Prove that G is a secure length-doubling PRG by showing that if G is not a secure PRG, then one can distinguish F_s from a truly random function.

Question 2. Read Lecture 1.5. Our goal is to show that conditioning a Gaussian on an event determined by its one-dimensional projection leaves its orthogonal component distributed as a standard $(n-1)$-dimensional Gaussian.

Let $g \sim N(0, I_n)$, let $w \in \mathbb{R}^n$ be a fixed unit vector, and fix $b > 0$. Let X have the distribution of g conditioned on $|\langle w, g\rangle| \leq b$.

1. Show that $\langle w, g\rangle \sim N(0,1)$.
2. Show that $\langle w, g\rangle$ and $g - \langle w, g\rangle w$ are independent.
3. Show that $X - \langle w, X\rangle w$ has the same distribution as $g - \langle w, g\rangle w$.

Question 3. Write two paragraphs of personal text describing what you learned in the last lecture. Focus on what you found important, surprising, or difficult, and explain it in your own words.

Include the following declaration verbatim at the end of your submission:

> "I hereby declare that I wrote the above paragraphs on my own"