Cryptography and Machine Learning - Homework 4

Due date: November 24, 2026. **Submission:** Via Moodle.

Question 1. In LPN, each label is corrupted by an independent bit $e \sim \mathrm{Ber}(\eta)$, where $0 < \eta < 1/2$. Suppose we add t independent LPN equations modulo 2.

1. Prove that the probability that the resulting error bit is 1 equals
$$\frac{1-(1-2\eta)^t}{2}.$$
Explain why combining many equations makes their labels less useful for recovering the secret.

2. Now consider LWE, where each error is bounded in absolute value by $B < q/(2t)$. What bound can you give on the error obtained by adding t LWE equations?

Question 2. Recall that a CLWE sample has the form
$$a \sim N(0, I_n), \qquad b = \gamma\langle a, w\rangle + e \pmod 1,$$
where w is a hidden unit vector. The hCLWE distribution is obtained by keeping samples whose labels are close to 0 and then discarding the labels.

1. Let $e = 0$ and $0 < \varepsilon < 1/2$. For $b \in [-1/2, 1/2)$, prove that $|b| \le \varepsilon$ implies $|\langle a, w\rangle - k/\gamma| \le \varepsilon/\gamma$ for some $k \in \mathbb{Z}$. Describe the resulting regions geometrically.

2. Given w, distinguish hCLWE samples satisfying $\mathrm{dist}(\gamma\langle a, w\rangle, \mathbb{Z}) \le \varepsilon$ from standard Gaussians with advantage at least $1/2$, assuming the event has Gaussian probability at most $1/2$.

Question 3. Consider the two classifiers $f_1, f_2 : \mathbb{R}^n \to \{-1, 1\}$ defined by
$$f_1(x) = \mathrm{sign}(x_1), \qquad f_2(x) = \mathrm{sign}(x_1 + \cdots + x_n),$$
where $n \ge 2$. Suppose the data distribution assigns equal probability to the two labeled examples $((1, \ldots, 1), 1)$ and $((-1, \ldots, -1), -1)$.

1. Show that both classifiers have accuracy 100%.

2. For each classifier, find the smallest ℓ_2- and ℓ_∞-norms of a perturbation that reaches its decision boundary, starting from either example. Explain what this tells us about accuracy and adversarial robustness.

Question 4. 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"

Question 5. Read Chapter 3.5, "Eigenvalues and Variance Directions."