Assignment 1

Due: Tuesday, January 30, 2024 11:30 pm (Eastern Standard Time)

Time left Show

Assignment description

These questions cover material from the first 2 weeks of lectures. Question grades are based on importance to the topic, not the relative difficulty or length.

Submit your assignment

Help

After you have completed the assignment, please save, scan, or take photos of your work and upload your files to the questions below. Crowdmark accepts PDF, JPG, and PNG file formats.

Q1 (12 points)

1. (6 marks) Show that the probability of sampling $m \leq n$ uniformly random vectors $a_i \in \mathbb{F}_q^n$ and having them all be linearly independent is

$$\prod_{i=0}^{m-1} \left(1 - q^{i-n}\right) \tag{1}$$

2. (6 marks) In Kyber, $q = 3329$ and for all parameter sets, $m = n$ and $n \leq 1024$. With these parameters, show that the probability is at least $2/3$ that a uniformly random $n \times n$ matrix A is invertible in $\mathbb{F}_q$.
3. (1 bonus mark): Compute the actual probability that an $n \times n$ matrix A is invertible for Kyber-512.

Q2 (5 points)

Show the the decisional LWE problem is information-theoretically hard for parameters $m \leq n$, q prime, s uniform, and any error distribution, if A is chosen such that it has full rank.

Q3 (21 points)

This question concerns LWE error distributions. Some programming may be necessary, but you could solve these problems with a spreadsheet.

1. (3 marks) A binomial distribution with parameters n and p can be approximated by a normal distribution with mean $\mu = np$ and variance $\sigma^2 = np(1-p)$. For $q = 3329$, compute the statistical distance between a centered binomial distribution with $n = 6$ and $p = 1/2$ (Kyber's error distribution) and a discrete Guassian with parameters given by the normal approximation to a binomial distribution.
2. (6 marks) Kyber has $q = 3329$ and uses a centered binomial distribution with $n = 6$. What is the most likely secret s? What is the probability of drawing this secret for Kyber with dimension 512?
3. (6 marks) For Kyber of dimension 512, what is the most likely number of 0s in a secret s? Most likely number of 1s, etc?
4. (12 marks total) Given someone's public Kyber key (A, b), where $b = As + e$, suppose their secret key s has exactly the number of 0s, 1s, -1s, etc. as you stated in the previous question. We hope to find their secret by brute-force: trying all possible keys of that shape.

   a) (6 marks) How do we test if a guess is correct?

   b) (6 marks) How many keys will we need to test, on average?

Q4 (10 points)

What is the expected norm-squared of a Kyber secret key s, and expected norm-squared of the error e, in terms of the dimension n? Compute the variance as well.

Q5 (6 points)

1. (3 marks) Suppose we generate a q-ary lattice from an $m \times n$ matrix A, i.e., we take the lattice $A\mathbb{Z}^n + q\mathbb{Z}^m$. Show that if A does not have full column rank as a matrix in $\mathbb{Z}_q^{m \times n}$, then $A\mathbb{Z}^n + q\mathbb{Z}^m = A'\mathbb{Z}^{n-1} + q\mathbb{Z}^m$ where A' is A with a linearly dependent column removed.

2. (3 marks) Show that LWE(m, n, q, U_s, χ_e) reduces to full-rank LWE(m, n, q, U_s, χ_e) (assuming the second problem is parameterized so solutions are unique).

Q6 (6 points)

1. (3 marks) Show that the sum of independent and identically distributed binomial distributions with parameters n_1, p and n_2, p gives a binomial distribution with parameters $n_1 + n_2$, p. Show that the sum of i.i.d. centered binomial distributions with parameters n_1,p and n_2,p is also centered binomial with parameter $n_1 + n_2$, p.
2. (3 marks) Given m samples of LWE where the error is drawn from a centered binomial distribution of parameters (n, p), show how to generate $\binom{m}{k} \approx m^k$ samples with parameters (kn, p) (Hint: the samples do not need to be independent).

Q7 (3 points)

For any positive number R, construct a lattice $L \in \mathbb{R}^n$ and a point $t \in \mathbb{R}^n$ such that $||L - t|| > R\lambda_1(L)$.

Q8 (8 points)

Choose a modulus q such that Kyber-512 would have never have decryption failures.

Q9 (4 points)

(4 marks) Show that full-rank LWE$(n, n, q, \chi_s, \chi_e)$ is equivalent to full-rank LWE$(n, n, q, \chi_e, \chi_s)$.

Q10 (30 points)

Imagine your friend Alice wants to encrypt her emails with LWE. However, she uses "textbook'' LWE, i.e., the protocol as shown in lectures, not the standard protocol. She generates a public key and private key, stores the private key securely, and publishes the public key. When someone wants to send her encrypted email, they encrypt it with the public key.

Alice goes on vacation and sets up an autoresponder. Any encrypted email which decrypts properly will get a response which quotes the entire original email. Eve will use this to recover Alice's private key.

1. (10 marks) Eve will generate a ciphertext $c_1 = s_1^T A + e_1^T$ and $c_2 = s_1^T b + e' + m\lfloor \frac{q}{2} \rceil$, where e_1 is all-zeros except in the ith component she sets it to $\lfloor \frac{q}{2} \rceil$. Show that as long as s_i is relatively small, Alice will correctly decrypt m if and only if s_i is even (technically it will not be precisely ``if and only if'', but with high probability in both directions).
2. (10 marks) Develop an efficient attack for Eve to determine which components of s which are even or odd.
3. (10 marks) Expand the attack to recover all values of s.
4. (0 marks) Discuss whether this attack scenario is reasonable and if there are some countermeasures (we will discuss this in more detail in the lectures).