Assignment 3

Q1 (10 points)

Show that if an encryption scheme is IND-CCA secure, it is IND-CPA secure.

Q2 (20 points)

Suppose that we remove the final error in an LWE encryption. That is, to encrypt a message m with public key (A, b), we sample random $r \leftarrow \chi_s'$ and $e' \leftarrow \chi_e'$, and output

$$c_1 = r^T A + e'^T,\ c_2 = r^T b + m\lfloor \frac{q}{2} \rceil. \tag{1}$$

1. (10 points) Explain how and why the proof of IND-CPA security for the Kyber-like PKE fails for this modified scheme.
2. (10 points) Assume the above is instantiated as ring-LWE (that is, A, b, r, e', c_1, c_2, m are all elements of the polynomial ring $\mathbb{Z}_q[x]/p(x)$). Construct a message distinguishing attack (hint: you will need to assume some polynomial is invertible).

Q3 (10 points)

Someone decides that rounding is too complicated, so they just implement naive Dilithium. That is:

KeyGen: Sample A uniformly at random as a $k \times \ell$ matrix, $s \leftarrow \chi_s$, and $e \leftarrow \chi_e$. Let $PK = (A, t = As + e)$, $SK = s$

Sign(SK, m): Select random y such that $\|y\|_\infty \leq \gamma$. Compute $c = H(Ay, m)$, where H hashes onto the space of polynomials with exactly τ non-zero coefficients, all in ± 1. Set $z = y + cs$; if $\|z\|_\infty \leq \beta - \tau\|\chi_s\|_\infty$, output (w, c, z) as a signature; otherwise try again.

Verify$(PK = (A, t), m, (w, z))$: Compute $c = H(w)$; output 1 if and only if $Az \approx w + ct$.

Show that with if c is invertible, one can recover the error e from this transcript. Does this matter?

Q4 (15 points)

Let KeyGen, Sign, and Verify, be digital signature scheme secure against strong existential forgery under chosen-message attack. Let $H : \{0,1\}^* \rightarrow \{0,1\}^n$ be a collision-resistant hash function.

1. (5 points) Show how to make a new signature scheme with a public key that is only n bits long.
2. (10 points) Prove that your new signature scheme is also secure against strong existential forgery under chosen-message attack.

Q5 (10 points)

In an attempt to avoid rejection sampling, someone modifies proto-Dilithium so that γ_1, the bound on y, is increased. Recall the module-ISIS($k, \ell, q, p(x), \beta$) problem:

Input: A matrix $A \in R_q^{k \times \ell}$, a vector $x \in R_q^k$ ($R_q = \mathbb{Z}_q[x]/p(x)$).

Output: A vector $v \in R_q$ such that $Av = x$ and $|v|_\infty \leq \beta$

1. (5 points) Given an algorithm $\mathcal{A}$ that solves module-ISIS($k, \ell, q, p(x), \gamma_1 - np\tau$), construct a signature forgery attack on proto-Dilithium that uses no signature queries.
2. (5 points) Allowing signature queries, given an algorithm $\mathcal{A}$ that solves module-ISIS($k, \ell, q, p(x), \gamma_1$), recover the secret key in proto-Dilithium, if $\gamma_1 < \frac{q^{\frac{k}{\ell}} - 1}{2}$.

Q0 (0 points)

Write the names of all of your collaborators.