Cryptography ENEE/CMSC/MATH 456: Homework 6

Due by 11:59pm on 5/8/2024.

1. Assume the Schnorr identification scheme is run in the group Z_p^*, where p is a sufficiently large prime. Recall that in this case, one can efficiently compute the Legendre symbol of $y = g^x, g^k$. Explain how a verifier can use this information to cause the distribution of s to not be uniform random. In particular, if x is odd, the verifier can cause s to always be even. Explain why this would mean that the simulation strategy we gave in class for Schnorr's algorithm would fail. Why does this not contradict the security of Schnorr's signatures?

2. Prove that LWE with secret s chosen from the noise distribution χ is as hard as LWE with secret s chosen uniformly at random from $\mathbb{Z}_p$.

   Specifically, given $(A_1, u_1 = A_1 s + e_1 \mod p)$ and $(A_2, u_2 = A_2 s + e_2 \mod p)$, where A_1 is invertible, show how to construct an instance $(A_3, u_3 = A_3 e_1 + e_3 \mod p)$, where e_1 becomes the LWE secret.

   Hint: Consider setting $A_3 = -A_2 A_1^{-1}$.

3. Prove that Decision-LWE is as hard as Search-LWE. Specifically, show a "divide-and-conquer" attack, where given an adversary who solves Decision-LWE, it is possible to guess the entries of s one by one. Recall that the modulus p is polynomial in the security parameter.

   Hint: Consider guessing the value of the first entry of s, denoted $s_1 \in \mathbb{Z}_q$ and choosing a column vector $a' \in \mathbb{Z}_p^m$ uniformly at random. Given an LWE instance (A, u), update the instance to $(A', u + s_1 \cdot a' \mod p)$, where A' is the matrix A with column vector a' added to its first column. What is the distribution of $(A', u + s_1 \cdot a' \mod p)$ in case the guess for s_1 is correct or incorrect?

4. Two bases $B_1, B_2 \in \mathbb{Z}^{n \times n}$ define the same lattice (i.e. $\Lambda(B_1) = \Lambda(B_2)$) if and only if $B_1 = B_2 \cdot U$, where U is a unimodular matrix.
   Using the above fact, construct three distinct bases $B1, B2, B3$ for the lattice $\mathbb{Z}^3$.

5. Show that given an algorithm that solves the SIS problem, one can obtain an algorithm for solving the Decision-LWE problem.

   Hint: Given an input (A, u), where either $u = As + e \mod p$ or u is uniform random in $\mathbb{Z}_p^m$, consider using SIS to find a short, non-zero vector $z \in \{0,1\}^m$ such that $zA = 0^n \mod p$. What happens in either case when you compute the inner product $\langle z, u \rangle$?

6. Show that given an algorithm that solves the SVP problem, one can obtain an algorithm for solving the SIS problem. Specifically, given $A \leftarrow \mathbb{Z}_p^{n \times m}$, define a basis B and a lattice $\Lambda(B)$ such that the shortest non-zero vector of $\Lambda(B)$ is equal to the shortest non-zero vector $z \in \mathbb{Z}_p^m$ such that $Az = 0^n \mod p$. You may assume that A is full-rank.