TD 4: LWE and PRFs

Exercise 1. *PRG from LWE*

We recall the Learning with Errors assumption.

Definition 1 (Learning with Errors). *Let $q \in \mathbb{N}$, $B \in \mathbb{N}$, $\mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{m\times n})$. The Learning with Errors (*LWE*) distribution is defined as follows: $D_{\text{LWE}} = (\mathbf{A}, \mathbf{A}\cdot\mathbf{s} + \mathbf{e} \bmod q)$ for $\mathbf{s} \hookleftarrow U(\mathbb{Z}_q^n)$, $\mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{m\times n})$ and $\mathbf{e} \hookleftarrow U((-B, B]^m)$.*

In this setting, the vector $\mathbf{s}$ is called the secret, and $\mathbf{e}$ the noise.
Remark. If q and B are powers of 2, we are manipulating bits, contrary to the DDH-based PRG from the lecture.

The *LWE assumption* states that, given suitable parameters q, B, m, n, it is computationally hard to distinguish D_{LWE} from the distribution $U(\mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^m)$.
Let us propose the following pseudo-random generator: $G(\mathbf{A}, \mathbf{s}, \mathbf{e}) = (\mathbf{A}, \mathbf{A}\cdot\mathbf{s} + \mathbf{e} \bmod q)$.

1. By definition, a PRG must have a bigger output size than input size. Give a bound on B that depends on the other parameters if we want G to satisfy this.

2. Given suitable B, q, n, m such that the LWE assumption and previous bound hold, show that G is a secure pseudo-random generator.

Exercise 2. *LWE with small secret*

We once more work in the setting of the LWE assumption. Let q, B, n, m such that the LWE assumption holds. Moreover, we assume that q is prime.

1. **(a)** What is the probability that $\mathbf{A}_1 \in \mathbf{Z}_q^{n\times n}$ is invertible where $\mathbf{A} =: [\mathbf{A}_1^\top | \mathbf{A}_2^\top]^\top$ is uniformly sampled?

   (b) Assume that $m \geq 2n$. Prove that there exists a subset of n lineraly independent rows of $\mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{m\times n})$ with probability $\geq 1 - 1/2^{\Omega(n)}$ and that we can find them in polynomial time.

2. Let us define the distribution $D_B = U((-B, B] \cap \mathbb{Z})$, and $m' = m - n$.

   Show that under the $\text{LWE}_{q,m,n,B}$ assumption, the distributions $(\mathbf{A}', \mathbf{A}'\mathbf{s}' + \mathbf{e}') \in \mathbb{Z}_q^{m'\times n} \times \mathbb{Z}_q^{m'}$, with $\mathbf{s}' \hookleftarrow D_B^n$ and $\mathbf{e}' \hookleftarrow D_B^{m'}$, and $(\mathbf{A}', \mathbf{b}')$ with $\mathbf{b}' \leftarrow U(\mathbb{Z}_q^{m'})$ are indistinguishable.

Exercise 3. *CTR Security*

Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a PRF. To encrypt a message $M \in \{0,1\}^{d\cdot n}$, CTR proceeds as follows:

- Write $M = M_0 \| M_1 \| \ldots \| M_{d-1}$ with each $M_i \in \{0,1\}^n$.
- Sample IV uniformly in $\{0,1\}^n$.
- Return $IV \| C_0 \| C_1 \| \ldots \| C_{d-1}$ with $C_i = M_i \oplus F(k, IV + i \bmod 2^n)$ for all i.

The goal of this exercise is to prove the security of the CTR encryption mode against chosen plaintext attacks, when the PRF F is secure.

1. Recall the definition of security of an encryption scheme against chosen plaintext attacks.

2. Assume an attacker makes Q encryption queries. Let $IV_1, \ldots, IV_Q$ be the corresponding IV's. Let `Twice` denote the event "there exist $i, j \leq Q$ and $k_i, k_j < d$ such that $IV_i + k_i = IV_j + k_j \bmod 2^n$ and $i \neq j$." Show that the probability of `Twice` is bounded from above by $Q^2 d / 2^{n-1}$.

3. Assume the PRF F is replaced by a uniformly chosen function $f : \{0,1\}^n \to \{0,1\}^n$. Give an upper bound on the distinguishing advantage of an adversary $\mathcal{A}$ against this idealized version of CTR, as a function of d, n and the number of encryption queries Q.

4. Show that if there exists a probabilistic polynomial-time adversary $\mathcal{A}$ against CTR based on PRF F, then there exists a probabilistic polynomial-time adversary $\mathcal{B}$ against the PRF F. Give a lower bound on the advantage degradation of the reduction.