TD 4: LWE and PRFs

Exercise 1. *Around the DDH assumption*

We recall the definition of the DDH assumption.

Definition 1 (Decisional Diffie-Hellman distribution). *Let $\mathbb{G}$ be a cyclic group of (prime) order p, and let g be a public generator of $\mathbb{G}$. The* decisional Diffie-Hellman *distribution (DDH) is, $D_{\text{DDH}} = (g^a, g^b, g^{ab}) \in \mathbb{G}^3$ with a, b sampled independently and uniformly in $\mathbb{Z}/p\mathbb{Z} =: \mathbb{Z}_p$.*

Definition 2 (Decisional Diffie-Hellman assumption). *The decisional Diffie-Hellman assumption states that there exists no probabilistic polynomial-time distinguisher between D_{DDH} and (g^a, g^b, g^c) with a, b, c sampled independently and uniformly at random in $\mathbb{Z}_p$.*

1. Does the DDH assumption hold in $\mathbb{G} = (\mathbb{Z}_p, +)$ for $p = \mathcal{O}(2^\lambda)$ prime?

2. Same question for $\mathbb{G} = (\mathbb{Z}_p^\star, \times)$ of order $p-1$, with p an odd prime.

Exercise 2. *PRG from LWE*

We recall the Learning with Errors assumption.

Definition 3 (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 $\mathbf{e} \hookleftarrow U\left((-B, B]^m\right)$.*

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 3. *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 $D_B = U\left((-B, B] \cap \mathbb{Z}\right)$, and $m' = m - n$.

   Show that under the 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.