# TD 4: Pseudo-Random Functions

**Exercise 1.** *PRF from DDH*

Let $n \in \mathbb{N}$ be a security parameter. Let $\mathbb{G}$ be a cyclic group of prime order $q > 2^n$ which is generated by a public $g \in \mathbb{G}$ and for which DDH is presumably hard.
We want to build a secure Pseudo-Random Function (PRF) under the DDH assumption in $\mathbb{G}$. The following construction was proposed by Naor and Reingold in 1997.
We define the function $F : \mathbb{Z}_q^{n+1} \times \{0,1\}^n \to \mathbb{G}$ as:

$$F(K, x) = g^{a_0 \cdot \prod_{j=1}^{n} a_j^{x_j}},$$

where we parsed $K = (a_0, a_1, \ldots, a_n)^\top$ and $x = (x_1, x_2, \ldots, x_n)^\top$.
For an index $i \in [1, n]$, we consider an experiment where the adversary is given oracle access to a hybrid function $F^{(i)}(K, \cdot)$ such that

$$\forall x \in \{0,1\}^n, F^{(i)}(K, x) = g^{R^{(i)}(x[1\ldots i]) \cdot \prod_{j=i+1}^{n} a_j^{x_j}},$$

where $R^{(i)} : \{0,1\}^i \to \mathbb{Z}_q$ is a uniformly sampled function and $x[1 \ldots i]$ denotes the $i$ first bits of $x$.

1. Prove that in the adversary's view, $F^{(0)}$ behaves exactly as the function $F$ if we define $x[1 \ldots 0] = \varepsilon$, the empty string. How does $F^{(n)}$ behave in the adversary's view?

2. Let $(g^a, g^b, g^c)$ be a DDH instance, where $a, b \hookleftarrow U(\mathbb{Z}_q)$ and we have to decide whether $c = ab$ or if $c \hookleftarrow U(\mathbb{Z}_q)$. Describe a probabilistic polynomial-time algorithm that creates $Q$ randomized instances of DDH $\{g^a, g^{b_\ell}, g^{c_\ell}\}_{\ell=1}^{Q}$, where $\{b_\ell\}_{\ell=1}^{Q}$ are uniformly random and independent over $\mathbb{Z}_q$, with the properties that:
   - If $c = ab \bmod q$, then $c_\ell = ab_\ell$ for any $\ell \in [1, q]$.
   - If $c \neq ab \bmod q$, then $(b_1, c_1, \ldots, b_Q, c_Q)$ follows the uniform distribution over $(\mathbb{Z}_q)^{2Q}$.

3. For each $i \in [0, n]$, define the experiment $\mathsf{Exp}_i$ where $\mathcal{A}$ is given oracle access to $F^{(i)}(K, \cdot)$ for $K \hookleftarrow U(\mathbb{Z}_q^{n+1})$. After at most $Q$ evaluation queries, $\mathcal{A}$ outputs a bit $b'$. Prove that for each $i \in [0, n-1]$ it holds that $\mathsf{Exp}_i$ is computationally indistinguishable from $\mathsf{Exp}_{i+1}$ under the DDH assumption.

4. Conclude by giving an upper bound on the advatange of a PRF distinguisher as a function of the maximal advantage of a DDH distinguisher.

*Remark:* Contrary to the GGM construction, the advantage loss does not depend on $Q$. This is a consequence of the random self-reducibility.

**Exercise 2.** *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.

**Exercise 3.** *weak PRF*

In the PRF security game, the adversary may adaptively make function evaluation queries: for $i = 1, 2, \ldots$, it sends $x_i$ of its choice, and gets $F_k(x_i)$ (resp. $f(x_i)$) from the challenger, where $F_k$ is the PRF (resp. $f$ is the uniformly chosen function). A weak-PRF consists of the same algorithms as a PRF, but the queries are modified as follows: the adversary does not get to see $F_k(x_i)$ (resp. $f(x_i)$) for **an input $x_i$ of its choice**, but instead every time the adversary requests a new pair, **the challenger samples a fresh uniform** $x_i$ and sends $(x_i, F_k(x_i))$ (resp. $(x_i, f(x_i))$) to the adversary.

1. Give a formal definition of a weak-PRF, based on a security game.

2. Show that a PRF is a weak-PRF, by providing a security reduction.

3. Assuming that a weak-PRF exists, build a weak-PRF that is not a PRF.

4. What is the difference between a PRG and a weak-PRF?

Let $G = (g)$ be a cyclic group of known prime order $p$. We recall that the DDH hardness assumption states that the distributions $(g^a, g^b, g^{ab})$ and $(g^a, g^b, g^c)$ are computationally indistinguishable when $a, b$ and $c$ are independently and uniformly distributed in $\mathbb{Z}/p\mathbb{Z}$. Let $k \in \mathbb{Z}/p\mathbb{Z}$ a uniformly chosen key. We consider the function $F_k : h \in G \mapsto h^k \in G$.

5. Let $Q \geq 1$. Consider the (randomized) map $\phi$ that takes $(g_1, g_2, g_3) \in G^3$ as input, samples $(x_i, y_i) \in (\mathbb{Z}/p\mathbb{Z})^2$ uniformly and independently for $i \leq Q$ and returns $(g_1^{x_i} g^{y_i}, g_3^{x_i} g_2^{y_i})_{i \leq Q}$.
   - Show that if $(g_1, g_2, g_3) = (g^a, g^b, g^{ab})$, then the output is distributed as $(g^{r_i}, g^{br_i})_{i \leq Q}$ for $r_i$'s in $\mathbb{Z}/p\mathbb{Z}$ uniform and independent.
   - Show that if $(g_1, g_2, g_3) = (g^a, g^b, g^c)$ for $c \neq ab$, then the output is distributed as $(g^{r_i}, g^{s_i})_{i \leq Q}$ for $(r_i, s_i)$'s in $(\mathbb{Z}/p\mathbb{Z})^2$ uniform and independent.

6. Show that $F_k$ is a weak-PRF under the DDH hardness assumption.
   *Hint: set "$k = b$" and use the previous question to build the weak PRF challenger.*

7. Is $F_k$ a secure PRF? Justify your answer.