TD2: Pseudorandom Generators

Exercise 1. *Bit-flip of a PRG*

Let G a pseudo-random generator (PRG) of input range $\{0,1\}^s$ and output range $\{0,1\}^n$. We define $\bar{G}$ as follows:

$$\forall x \in \{0,1\}^s, \bar{G}(x) := 1^n \oplus G(x),$$

where $\oplus$ denotes the XOR operation. This corresponds to flipping every bit of the output of G.

1. Prove that $\bar{G}$ is secure if and only if G is secure.

Exercise 2. *Variable-length OTP is not secure*

A *variable length one-time pad* is a cipher (E, D), where the keys are bit strings of some fixed length L, while messages and ciphertexts are variable length bit strings, of length at most L. Thus, the cipher (E, D) is defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$, where

$$\mathcal{K} := \{0,1\}^L \text{ and } \mathcal{M} := \mathcal{C} = \{0,1\}^{\leq L}$$

for some parameter L. Here, $\{0,1\}^{\leq L}$ denotes the set of all bit strings of length at most L (including the empty string). For a key $k \in \{0,1\}^L$ and a message $m \in \{0,1\}^{\leq L}$ of length ℓ, the encryption function is defined as follows:

$$E(k, m) := k[0 \mathinner{..} \ell - 1] \oplus m$$

1. Provide a counter-example showing that the variable length OTP is not secure for perfect secrecy.

Exercise 3.

Let $\mathsf{G} : \{0,1\}^n \to \{0,1\}^m$ be a function, with $m > n$.

1. Recall the definition of a PRG from the lecture.

Let $\mathsf{Enc} : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}^m$ defined by $\mathsf{Enc}(k, m) = \mathsf{G}(k) \oplus m$.

2. Give the associated decryption algorithm.

3. Recall the smCPA security notion from the lecture.

Let $m_1, m_2 \in \{0,1\}^m$ be arbitrary messages.

4. What is the statistical distance between the distributions $\mathcal{U}_1 = m_1 \oplus \mathcal{U}(\{0,1\}^m)$ and $\mathcal{U}_2 = m_2 \oplus \mathcal{U}(\{0,1\}^m)$?

We proved in class that G PRG $\Rightarrow$ $(\mathsf{Enc}, \mathsf{Dec})$ smCPA-secure. We are going to prove $(\mathsf{Enc}, \mathsf{Dec})$ not smCPA-secure $\Rightarrow$ G not PRG.

5. Let $\mathcal{A}$ be an distinguisher between two games G_0 and G_1. We say that $\mathcal{A}$ wins if it output 0 (resp 1) during the game G_0 (resp G_1). Show that

$$\mathsf{Adv}_{\mathcal{A}}(G_0, G_1) = 2 \cdot \left| \Pr_{b \sim \mathcal{U}(\{0,1\})}(\mathcal{A} \text{ wins in } G_b) - \frac{1}{2} \right|$$

6. Assume that $\mathcal{A}$ is an adversary with non-negligible advantage ε against the smCPA-security of $(\mathsf{Enc}, \mathsf{Dec})$. Construct an explicit distinguisher between $\mathcal{U}(\{0,1\}^m)$ and $G(\mathcal{U}(\{0,1\}^n))$ and compute its advantage.