TD 2: Pseudo Random Generators

Exercise 1. *PRG implies smCPA with hybrid argument*

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 $\mathcal{U}_2 = m_2 \oplus \mathcal{U}(\{0,1\}^m)$?

5. Prove that if G is a PRG, then $(\mathsf{Enc}, \mathsf{Dec})$ is smCPA-secure using a hybrid argument.

(Bonus) We just proved 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.

6. 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

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

7. 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.

Exercise 2. *smCPA does not imply PRG*

Let $(\mathsf{Enc}, \mathsf{Dec})$ be an encryption scheme over $K \times P \times \{0,1\}^n$.

1. In this question, we assume that $(\mathsf{Enc}, \mathsf{Dec})$ is smCPA-secure. Prove that there exists a smCPA-secure encryption scheme $(\mathsf{Enc}', \mathsf{Dec}')$ such that $G : k \mapsto \mathsf{Enc}'(k, 0)$ is not a secure PRG. *Hint: try to concatenate constant bits to every ciphertext.*

Exercise 3. *Enlarge your PRG*

Let $G : \{0,1\}^k \to \{0,1\}^{k+1}$ be a secure pseudo-random generator.

1. Let $\ell < k+1$ and define $G_\ell : \{0,1\}^k \to \{0,1\}^\ell$ such that $G_\ell(x) = [G(x)]_{1\ldots\ell}$, where this denotes the first ℓ bits of $G(x)$. Prove that G_ℓ satisfies the security notion of a PRG[1].

2. Consider $G^{(1)} : \{0,1\}^k \to \{0,1\}^{k+2}$ defined as follows. On input $x \in \{0,1\}^k$, algorithm $G^{(1)}$ first evaluates $G(x)$ and obtains $(x^{(1)}, y^{(1)}) \in \{0,1\}^k \times \{0,1\}$ such that $G(x) = x^{(1)} \parallel y^{(1)}$. It then evaluates G on $x^{(1)}$ and eventually returns $G(x^{(1)}) \parallel y^{(1)}$. Show that if G is a secure PRG, then so is $G^{(1)}$.

[1] It is however NOT a PRG as its input size is less than its output size.

3. **(a)** Let $n \geq 1$. Propose a construction of a PRG $G^{(n)} : \{0,1\}^k \to \{0,1\}^{k+n+1}$ based on G. Show that if G is a secure PRG, then so is $G^{(n)}$.

   (b) Evaluate the cost of your construction.

4. In this question only, we assume that $G : \{0,1\}^k \to \{0,1\}^{2k}$ is a secure PRG. Adapt the previous questions to build a secure PRG $G' : \{0,1\}^k \to \{0,1\}^{2^n \cdot k}$ for any $n \geq 1$. Evaluate the cost of your construction and compare it with the previous one.

An arbitrary-length PRG is a function $G^\star$ taking as inputs $x \in \{0,1\}^n$ and $\ell \geq 1$ in unary, and returning an element of $\{0,1\}^\ell$. It is said to be secure if for all ℓ polynomially bounded with respect to n, the distributions $G^\star(U(\{0,1\}^n), 1^\ell)$ and $U(\{0,1\})^\ell$ are computationally indistinguishable.

5. Let $n \geq 1$. Propose a construction of an arbitrary-length PRG G^* based on G. Show that if G is a secure PRG, then so is G^*.

To be continued…