Cryptography Foundations

Exercise 6

6.1 Constructing Uniform Bits from Biased Bits

Goal: We get acquainted with DDSs and PDSs (and their behavior), by exploring how a deterministic converter can transform a source of biased bits into a source of uniform bits.

Let $\mathcal{X} = \{\varnothing\}$ and $\mathcal{Y} = \{0, 1\}$. Consider for $p \in [0, 1]$ an $(\mathcal{X}, \mathcal{Y})$-PDS $S_p$ that on each trigger input $\varnothing$ outputs a bit that is 1 with probability $p$, i.e., $S_p$ has the following behavior:

$$p^{S_p}_{\mathcal{X}|\mathcal{Y}}(y_i, x^i, y^{i-1}) = \begin{cases} p, & y_i = 1 \\ 1 - p, & y_i = 0. \end{cases}$$

Recall that for $n \in \mathbb{N}$, $[n]S_p$ is the PDS $S_p$ restricted to $n$ inputs, i.e., it is an $(\mathcal{X}, \mathcal{Y})$-PDS that for the first $n$ inputs is identical to $S_p$, and is undefined afterwards.

a) Describe an $(\mathcal{X}, \mathcal{Y})$-PDS as a random variable over $(\mathcal{X}, \mathcal{Y})$-DDSs that has the behavior of $[n]S_p$.

b) Let $n$ be even. Find a deterministic converter $\alpha$ (i.e., a $(\mathcal{X}, \mathcal{Y}, (\mathcal{X}, \mathcal{Y}))$-DDC) such that $\alpha[n]S_{1/2}^{1} \equiv [n/2]S_{1/2}^{1}$.

Describe $\alpha$ both in words and formally according to Definition 3.8. Argue why the two systems are equivalent (a formal proof is not required).

c) Now assume you are given $S_p$ and you again want to transform it into an $(\mathcal{X}, \mathcal{Y})$-PDS that outputs uniform bits, but this time you do not know $p$. That is, you are looking for a deterministic converter $\beta$ (not depending on $p$) such that $\beta[n]S_p$ replies to each of the first few queries with an independent uniform bit and is undefined afterwards. Informally describe a suitable $\beta$. Give the conditional probabilities that define the behavior of $([\beta[n]S_p])^{1}$.

6.2 Random Functions and Random Permutations

Goal: Random functions and random permutations are idealized cryptographic primitives of great importance. We familiarize with them by describing their behavior and analyzing some of their key properties.

In this task, we consider the independent PDSs $F_{n,n}$, $R_{n,n}$, $Q_{n}$, $P_{n}$, and $P'_{n}$, where $F_{n,n}$ is a random function from $\{0, 1\}^{n}$ to $\{0, 1\}^{n}$ with an arbitrary distribution, $R_{n,n}$ is a uniform random function (URF) from $\{0, 1\}^{n}$ to $\{0, 1\}^{n}$, $Q_{n}$ is a random permutation on $\{0, 1\}^{n}$ with an arbitrary distribution, and $P_{n}$ and $P'_{n}$ are uniform random permutations (URP) on $\{0, 1\}^{n}$.

a) Describe the behavior of $P_{n}$ as a sequence $p^{P_{n}}_{\mathcal{X}|\mathcal{X}}$ and as a sequence $p^{P_{n}}_{\mathcal{Y}|\mathcal{X}}$, for $i \geq 1$.

Also, describe the system $R_{n,n}$ as a sequence of conditional distributions $p^{R_{n,n}}_{\mathcal{Y}|\mathcal{X}}$, for $i \geq 1$.

b) Show that $F_{n,n} \oplus P_{n} \neq P_{n}$.

c) Show that $Q_{n} \triangleright P_{n} \equiv P_{n}$.

d) Show that $P_{n} \oplus P'_{n} \neq R_{n,n}$ for $n > 1$.

*Hint:* Consider the parity of all the bits in the function tables of $P_{n} \oplus P'_{n}$ and $R_{n,n}$.