ETH Zürich, D-INFK
Spring 2018

Prof. Ueli Maurer
Christian Badertscher
Fabio Banfi

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

$$\mathsf{p}^{\mathbf{S}_p}_{Y_i|X^iY^{i-1}}(y_i, x^i, y^{i-1}) = \begin{cases} p, & y_i = 1 \\ 1-p, & y_i = 0. \end{cases}$$

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

b) Let n be even. Find a deterministic converter α (i.e., a $((\mathcal{X},\mathcal{Y}),(\mathcal{X},\mathcal{Y}))$-DDC) such that

$$\alpha[n]\mathbf{S}_{\frac{1}{\sqrt{2}}} \;\equiv\; [n/2]\mathbf{S}_{\frac{1}{2}}.$$

Describe α 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 $\mathbf{S}_p$ 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 β (not depending on p) such that $\beta[n]\mathbf{S}_p$ replies to each of the first few queries with an independent uniform bit and is undefined afterwards. Informally describe a suitable β. Give the conditional probabilites that define the behavior of $(\beta[n]\mathbf{S}_p)^{\perp}$.

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 $\mathbf{F}_{n,n}$, $\mathbf{R}_{n,n}$, $\mathbf{Q}_n$, $\mathbf{P}_n$, and $\mathbf{P}'_n$, where $\mathbf{F}_{n,n}$ is a *random function* from $\{0,1\}^n$ to $\{0,1\}^n$ with an arbitrary distribution, $\mathbf{R}_{n,n}$ is a *uniform random function (URF)* from $\{0,1\}^n$ to $\{0,1\}^n$, $\mathbf{Q}_n$ is a *random permutation* on $\{0,1\}^n$ with an arbitrary distribution, and $\mathbf{P}_n$ and $\mathbf{P}'_n$ are *uniform random permutations (URP)* on $\{0,1\}^n$.

a) Describe the behavior of $\mathbf{P}_n$ as a sequence $\mathsf{p}^{\mathbf{P}_n}_{Y_i|X^iY^{i-1}}$ and as a sequence $\mathsf{p}^{\mathbf{P}_n}_{Y^i|X^i}$, for $i \geq 1$. Also, describe the system $\mathbf{R}_{n,n}$ as a sequence of conditional distributions $\mathsf{p}^{\mathbf{R}_{n,n}}_{Y^i|X^i}$ for $i \geq 1$.

b) Show that $\mathbf{F}_{n,n} \oplus \mathbf{P}_n \not\equiv \mathbf{P}_n$.

c) Show that $\mathbf{Q}_n \triangleright \mathbf{P}_n \equiv \mathbf{P}_n$.

d) Show that $\mathbf{P}_n \oplus \mathbf{P}'_n \not\equiv \mathbf{R}_{n,n}$ for $n > 1$.

Hint: Consider the parity of all the bits in the function tables of $\mathbf{P}_n \oplus \mathbf{P}'_n$ and $\mathbf{R}_{n,n}$.