ETH Zürich, D-INFK
Spring 2018

Prof. Ueli Maurer
Christian Badertscher
Fabio Banfi

Cryptography Foundations

Solution Exercise 6

6.1 Constructing Uniform Bits from Biased Bits

a) For $v^n = (v_1, \ldots, v_n) \in \{0,1\}^n$, consider the $(\mathcal{X}, \mathcal{Y})$-DDS $\mathbf{t}_{v^n}$ with $\mathbf{t}_{v^n}(x^i) = v_i$ for $i \leq n$, and which is undefined otherwise, that is, $\mathbf{t}^{\perp}_{v^n}(x^i) = \perp$ for $i > n$. Let $V^n = (V_1, \ldots, V_n)$ be a sequence of n independent and identically distributed random bits with $\Pr[V_i = 1] = p$ and $\Pr[V_i = 0] = 1 - p$ for all $i \in \{1, \ldots, n\}$. We then define the random variable $\mathbf{T}$ over $\{\mathbf{t}_{v^n} \mid v^n \in \{0,1\}^n\}$ as $\mathbf{T} := \mathbf{t}_{V^n}$, which is an $(\mathcal{X}, \mathcal{Y})$-PDS. Note that $\mathbf{T}(x^i) = V_i$ for $i \leq n$, whereas $\mathbf{T}(x^i)$ is undefined for $i > n$. Hence, we can compute the behavior of $\mathbf{T}$ using Definition 3.18 for $i \leq n$ as follows:

$$\begin{aligned}
\mathsf{p}^{\mathbf{T}}_{Y_i|X^iY^{i-1}}(y_i, x^i, y^{i-1}) &= \Pr[\mathbf{T}(x^i) = y_i \mid \mathbf{T}(x_1) = y_1, \ldots, \mathbf{T}(x^{i-1}) = y_{i-1}] \\
&= \Pr[V_i = y_i \mid V^{i-1} = y^{i-1}] \\
&= \Pr[V_i = y_i] \\
&= \begin{cases} p, & y_i = 1, \\ 1 - p, & y_i = 0. \end{cases}
\end{aligned}$$

We can therefore conclude that $\mathbf{T}$ has the behavior of $[n]\mathbf{S}_p$.

b) The probability that two consecutive bits output by $\mathbf{S}_{\frac{1}{\sqrt{2}}}$ are both equal to 1 is $\frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}} = \frac{1}{2}$. Now the idea is to define the converter α such that for every trigger input $\diamond$ (at the outside) it fetches two bits (by issuing two consecutive trigger inputs at the inside) and then outputs 1 (at the outside) if the two bits are both equal to 1, and 0 in the other three cases. Concretely, according to Definition 3.8, we need to define the function

$$\alpha : \{\diamond, 0, 1, \perp\}^* \setminus \{\varepsilon\} \to \{(\mathsf{out}, 0), (\mathsf{out}, 1), (\mathsf{in}, \diamond)\},$$

which we do recursively over the length of the argument string. For arguments x of length 1 only trigger inputs $\diamond$ (from the outside) are expected, according to Definition 3.8, and so we set

$$\alpha(\diamond) = (\mathsf{in}, \diamond).$$

Then, for $t \geq 2$, $\alpha(x_1, \ldots, x_t)$ is undefined if $\alpha(x_1, \ldots, x_{t-1})$ is. On the other hand, if $\alpha(x_1, \ldots, x_{t-1})$ is not undefined, we distinguish the three cases where t is congruent to 1, 2 or 3 modulo 3, respectively. In the case $t \equiv_3 1$ we have that $x_t = \diamond$, thus we set

$$\alpha(x_1, \ldots, x_{t-1}, \diamond) = (\mathsf{in}, \diamond).$$

When $t \equiv_3 2$ we have that $x_t \in \{0, 1\}$, thus we set

$$\alpha(x_1, \ldots, x_t) = (\mathsf{in}, \diamond).$$

And finally, if $t \equiv_3 3$,

$$\alpha(x_1, \ldots, x_t) = \begin{cases} (\mathsf{out}, 1) & \text{if } x_{t-1} = x_t = 1, \\ (\mathsf{out}, 0) & \text{if } (x_{t-1}, x_t) \in \{0,1\}^2 \setminus \{(1,1)\}. \end{cases}$$

Now consider the system $\alpha[n]\mathbf{S}_{\frac{1}{\sqrt{2}}}$. For each of the first $\frac{n}{2}$ queries α gets two bits on the inside and it follows from the explanation above that the systems outputs a uniform bit. From the $(\frac{n}{2}+1)$-th query on, there are no bits available anymore and the system in undefined. Therefore, the construction on the exercise sheet is realized.

c) Note that (no matter what p is), the probability of any two consecutive bits output by $[n]\mathbf{S}_p$ being 01 equals the probability of them being 10 (namely $p(1-p)$). We use this fact to define the converter β as follows: On trigger input $\diamond$ (at the outside), β forwards the trigger (to the inside), receives y_1, then again outputs a trigger (to the inside), and receives y_2. If $(y_1, y_2) = (0,1)$, β outputs 1 (at the outside) and if $(y_1, y_2) = (1,0)$, it outputs 0 (at the outside). Otherwise (i.e., $y_1 = y_2 \in \{0,1\}$) , β repeats this procedure until either y_2 is undefined or $y_1 \neq y_2$. This is guaranteed to happen after finitely many iterations because $[n]\mathbf{S}_p$ is undefined after more than n inputs, that is, $([n]\mathbf{S}_p)^\perp(x^i) = \perp$ for $i > n$, and in this case β is also undefined, that is, $(\beta[n]\mathbf{S}_p)^\perp(x^i) = \perp$ for $i > n$.

Let $m \coloneqq \lfloor n/2 \rfloor$. We then have for $i \leq m$ that $\beta[n]\mathbf{S}_p(x^i)$ is not undefined if and only if $\mathbf{S}_p(x^{2m})$ returns at most $m-i$ pairs $(0,0)$ or $(1,1)$. For each of the m returned pairs, the probability that it is $(0,0)$ or $(1,1)$ equals $(1-p)^2 + p^2$. Hence,

$$\varepsilon_i \coloneqq \Pr[(\beta[n]\mathbf{S}_p)^\perp(x^i) \neq \perp] = \sum_{k=0}^{m-i} \binom{m}{k} \big((1-p)^2+p^2\big)^k \big(1-(1-p)^2-p^2\big)^{m-k}.$$

Furthermore, since each output bit has the same probability, for $b \in \{0,1\}$ we have

$$\Pr(\beta[n]\mathbf{S}_p(x^i) = b \mid (\beta[n]\mathbf{S}_p)^\perp(x^i) \neq \perp) = \frac{1}{2}.$$

Since the output bits are independent, this implies for all $y_1, \ldots, y_i \in \{0,1\}$,

$$\begin{aligned}
&\Pr[\beta[n]\mathbf{S}_p(x^1) = y_1, \ldots, \beta[n]\mathbf{S}_p(x^i) = y_i] \\
&= \Pr[\beta[n]\mathbf{S}_p(x^1) = y_1, \ldots, \beta[n]\mathbf{S}_p(x^i) = y_i \mid (\beta[n]\mathbf{S}_p)^\perp(x^i) \neq \perp] \cdot \Pr[(\beta[n]\mathbf{S}_p)^\perp(x^i) \neq \perp] \\
&= \frac{\varepsilon_i}{2^i}.
\end{aligned}$$

We therefore have for $y_1, \ldots, y_i \in \{0,1\}$,

$$\begin{aligned}
&\Pr[\beta[n]\mathbf{S}_p(x^i) = y_i \mid \beta[n]\mathbf{S}_p(x^1) = y_1, \ldots, \beta[n]\mathbf{S}_p(x^{i-1}) = y_{i-1}] \\
&\quad = \frac{\Pr[\beta[n]\mathbf{S}_p(x^1) = y_1, \ldots, \beta[n]\mathbf{S}_p(x^i) = y_i]}{\Pr[\beta[n]\mathbf{S}_p(x^1) = y_1, \ldots, \beta[n]\mathbf{S}_p(x^{i-1}) = y_{i-1}]} \\
&\quad = \frac{\varepsilon_i}{2\varepsilon_{i-1}}.
\end{aligned}$$

Thus, we obtain the following for the behavior of $(\beta[n]\mathbf{S}_p)^\perp$:

$$\mathsf{p}^{(\beta[n]\mathbf{S}_p)^\perp}_{Y_i|X^iY^{i-1}}(y_i, x^i, y^{i-1}) = \begin{cases} \frac{\varepsilon_i}{2\varepsilon_{i-1}}, & y_i \in \{0,1\} \ \wedge \ i \leq m \ \wedge \ y_{i-1} \neq \perp, \\ 1 - \frac{\varepsilon_i}{\varepsilon_{i-1}}, & y_i = \perp \ \wedge \ i \leq m \ \wedge \ y_{i-1} \neq \perp, \\ 0, & y_i \in \{0,1\} \wedge (i > m \ \vee \ y_{i-1} = \perp), \\ 1, & y_i = \perp \ \wedge \ (i > m \ \vee \ y_{i-1} = \perp). \end{cases}$$

6.2 Random Functions and Random Permutations

a) Note that permutations are stateless, hence we have for a DDS $\mathbf{s}$ implementing a permutation π,

$$\mathbf{s}(x_1, \ldots, x_i) = \pi(x_i).$$

A uniform random permutation $\mathbf{P}_n$ corresponds to a random variable that is uniformly distributed over the set of permutations $\pi\colon \{0,1\}^n \to \{0,1\}^n$. We denote this random variable by $\pi^{\mathbf{P}_n}$. Therefore, we have for the behavior

$$\mathsf{p}^{\mathbf{P}_n}_{Y_i|X^iY^{i-1}}(y_i, x^i, y^{i-1}) = \Pr\left[\pi^{\mathbf{P}_n}(x_i) = y_i \mid \pi^{\mathbf{P}_n}(x_1) = y_1, \ldots, \pi^{\mathbf{P}_n}(x_{i-1}) = y_{i-1}\right].$$

Using a counting argument, this yields

$$\mathsf{p}^{\mathbf{P}_n}_{Y_i|X^iY^{i-1}}(y_i, x^i, y^{i-1}) = \frac{|\{\pi \mid \pi(x_1) = y_1, \ldots, \pi(x_i) = y_i\}|}{|\{\pi \mid \pi(x_1) = y_1, \ldots, \pi(x_{i-1}) = y_{i-1}\}|}. \tag{1}$$

Both the denominator and the numerator can be zero if the values x^i and y^i are not consistent with a permutation. If the denominator is zero, then the behavior is undefined. Otherwise, if the last output y_i is not consistent, i.e., $(x_i = x_j \wedge y_i \neq y_j) \vee (x_i \neq x_j \wedge y_i = y_j)$ for some $j < i$, then the set in the numerator is empty and the expression is zero.

For a sequence $x^i = (x_1, \ldots, x_i)$, let $\mathsf{d}(x^i) := |\{x_1, \ldots, x_i\}|$ denote the number of distinct components in x^i. If the numerator is nonzero, i.e., all values are consistent with a permutation, the numerator counts the number of permutations on $\{0,1\}^n$ that have some fixed values in $\mathsf{d}(x^i)$ positions. This number corresponds to the number of permutations on the remaining elements. Since $2^n - \mathsf{d}(x^i)$ elements remain and by using the same argument for the denominator, the fraction in equation (1) becomes

$$\frac{(2^n - \mathsf{d}(x^i))!}{(2^n - \mathsf{d}(x^{i-1}))!} = \begin{cases} 1, & \text{if } \mathsf{d}(x^i) = \mathsf{d}(x^{i-1}), \\ \frac{1}{2^n - (\mathsf{d}(x^i) - 1)}, & \text{if } \mathsf{d}(x^i) = \mathsf{d}(x^{i-1}) + 1, \end{cases}$$

in case all values are consistent with a permutation. Since $\mathsf{d}(x^i) = \mathsf{d}(x^{i-1})$ if and only if $x_i = x_j$ for some $j < i$, we get (for the defined cases)

$$\mathsf{p}^{\mathbf{P}_n}_{Y_i|X^iY^{i-1}}\left(y_i, x^i, y^{i-1}\right) = \begin{cases} 1, & \text{if } x_i = x_j \wedge y_i = y_j \text{ for some } j < i, \\ 0, & \text{if } (x_i = x_j \wedge y_i \neq y_j) \\ & \quad \vee\ (x_i \neq x_j \wedge y_i = y_j) \text{ for some } j < i, \\ \frac{1}{2^n - (\mathsf{d}(x^i) - 1)}, & \text{else.} \end{cases}$$

Since $\mathsf{p}^{\mathbf{P}_n}_{Y^i|X^i} = \prod_{j=1}^{i} \mathsf{p}^{\mathbf{P}_n}_{Y_j|X^jY^{j-1}}$ by equation (3.2) in the lecture notes, we further have

$$\mathsf{p}^{\mathbf{P}_n}_{Y^i|X^i}\left(y^i, x^i\right) = \begin{cases} 0, & \text{if there are } 1 \leq j, j' \leq i \text{ with} \\ & \quad (x_j = x_{j'} \wedge y_j \neq y_{j'}) \vee (x_j \neq x_{j'} \wedge y_j = y_{j'}), \\ \prod_{j=0}^{\mathsf{d}(x^i)-1} \frac{1}{2^n - j}, & \text{else.} \end{cases}$$

Since $\mathsf{p}^{\mathbf{R}_{n,n}}_{Y^i|X^i} = \prod_{j=1}^{i} \mathsf{p}^{\mathbf{R}_{n,n}}_{Y_j|X^jY^{j-1}}$, and using the formula for $\mathsf{p}^{\mathbf{R}_{n,n}}_{Y_j|X^jY^{j-1}}$ from Example 3.6 in the lecture notes, we have

$$\mathsf{p}^{\mathbf{R}_{n,n}}_{Y^i|X^i}\left(y^i, x^i\right) = \begin{cases} 0, & \text{if there are } 1 \leq j, j' \leq i \text{ with } x_j = x_{j'} \wedge y_j \neq y_{j'}, \\ 2^{-n\mathsf{d}(x^i)}, & \text{else.} \end{cases}$$

b) $\mathbf{F}_{n,n} \oplus \mathbf{P}_n$ is not a URP in general because it can output the same value for two different inputs with positive probability. To see this, let $x_1, x_2 \in \{0,1\}^n$, $x_1 \neq x_2$ and let y_1 be the first output of $\mathbf{F}_{n,n} \oplus \mathbf{P}_n$ in an experiment where x_1 is the first and x_2 the second input. Then, its second output is $y_2 = y_2^f \oplus y_2^p$ where y_2^f and y_2^p are the outputs of $\mathbf{F}_{n,n}$ and $\mathbf{P}_n$,

respectively. We then have $y_2 = y_1$ if $y_2^f = y_1 \oplus y_2^p$, which can have positive probability, depending on the distribution of $\mathbf{F}_{n,n}$. (Note however, that $\mathbf{F}_{n,n} \oplus \mathbf{P}_n$ can be a URP, e.g., if $\mathbf{F}_{n,n}$ is 0^n for all inputs with probability 1.)

c) Note that the set of permutations on $\{0,1\}^n$ form a group where the operation $\circ$ is the composition of permutations. Thus, for all permutations p, p', and q, we have $p \circ q = p'$ if and only if $p = p' \circ q^{-1}$. Since the cascade of two permutation systems corresponds to the system for the composed permutations, we have

$$\mathsf{P}_{\mathbf{Q}_n \rhd \mathbf{P}_n | \mathbf{Q}_n}(\mathbf{p}', \mathbf{q}) = \mathsf{P}_{\mathbf{P}_n | \mathbf{Q}_n}\left(\mathbf{q}^{-1} \rhd \mathbf{p}', \mathbf{q}\right),$$

where $\mathbf{q}^{-1}$ denotes the system that corresponds to the permutation q^{-1} where q is the permutation to which the system $\mathbf{q}$ corresponds. Using the independence of $\mathbf{P}_n$ and $\mathbf{Q}_n$, we get

$$\mathsf{P}_{\mathbf{P}_n | \mathbf{Q}_n}\left(\mathbf{q}^{-1} \rhd \mathbf{p}', \mathbf{q}\right) = \mathsf{P}_{\mathbf{P}_n}\left(\mathbf{q}^{-1} \rhd \mathbf{p}'\right) = \mathsf{P}_{\mathbf{P}_n}(\mathbf{p}'),$$

where the last step follows from the uniformity of $\mathbf{P}_n$. Thus, overall

$$\mathsf{P}_{\mathbf{Q}_n \rhd \mathbf{P}_n}(\mathbf{p}) = \sum_{\mathbf{q}} \mathsf{P}_{\mathbf{Q}_n \rhd \mathbf{P}_n | \mathbf{Q}_n}(\mathbf{p}, \mathbf{q}) \cdot \mathsf{P}_{\mathbf{Q}_n}(\mathbf{q}) = \mathsf{P}_{\mathbf{P}_n}(\mathbf{p}) \sum_{\mathbf{q}} \mathsf{P}_{\mathbf{Q}_n}(\mathbf{q}) = \mathsf{P}_{\mathbf{P}_n}(\mathbf{p}).$$

In summary, we have that $\mathbf{Q}_n \rhd \mathbf{P}_n$ and $\mathbf{P}_n$ are equally distributed, which implies $\mathbf{Q}_n \rhd \mathbf{P}_n \equiv \mathbf{P}_n$.

d) Note that for every $i \in \{1, \ldots, n\}$, there are exactly 2^{n-1} bit strings $x \in \{0,1\}^n$ such that the ith bit of x is 1. Since 2^{n-1} is even for $n > 1$, we have $\bigoplus_{x \in \{0,1\}^n} x = 0^n$ (where 0^n is the string consisting of n zeros). This implies $\bigoplus_{x \in \{0,1\}^n} p(x) = 0^n$ for any permutation $p\colon \{0,1\}^n \to \{0,1\}^n$. Hence, for all permutations p and p' on $\{0,1\}^n$, we have

$$\bigoplus_{x \in \{0,1\}^n} (p \oplus p')(x) = \bigoplus_{x \in \{0,1\}^n} \big(p(x) \oplus p'(x)\big) = \bigoplus_{x \in \{0,1\}^n} p(x) \;\oplus\; \bigoplus_{x \in \{0,1\}^n} p'(x) = 0^n.$$

Therefore, the XOR of all bits in the function table corresponding to $\mathbf{P}_n \oplus \mathbf{P}'_n$ is 0 with probability 1. However, the XOR of all bits in the function table corresponding to $\mathbf{R}_{n,n}$ is 0 with probability 1/2 (since the last bit of the last function value is chosen uniformly and independently of the other bits).

It remains to be shown that this implies that the behaviors differ. To this end, consider the environment $\mathbf{E}$ that sequentially queries every element of $\{0,1\}^n$. By the above argument, we have that the distributions of the generated transcripts differ, that is for $k = 2^n$,

$$\mathsf{P}_{X^k Y^k}^{\mathbf{E}(\mathbf{P}_n \oplus \mathbf{P}'_n)} \neq \mathsf{P}_{X^k Y^k}^{\mathbf{E}\mathbf{R}_{n,n}}.$$

Using Lemma 3.2 in the lecture notes, we further have

$$\mathsf{P}_{X^k Y^k}^{\mathbf{E}(\mathbf{P}_n \oplus \mathbf{P}'_n)}(x^k, y^k) = \mathsf{p}_{X^k | Y^{k-1}}^{\mathbf{E}}(x^k, y^{k-1}) \cdot \mathsf{p}_{Y^k | X^k}^{\mathbf{P}_n \oplus \mathbf{P}'_n}(y^k, x^k) \qquad \text{and}$$
$$\mathsf{P}_{X^k Y^k}^{\mathbf{E}\mathbf{R}_{n,n}}(x^k, y^k) = \mathsf{p}_{X^k | Y^{k-1}}^{\mathbf{E}}(x^k, y^{k-1}) \cdot \mathsf{p}_{Y^k | X^k}^{\mathbf{R}_{n,n}}(y^k, x^k).$$

This implies that there exist y^k, x^k such that

$$\mathsf{p}_{Y^k | X^k}^{\mathbf{P}_n \oplus \mathbf{P}'_n}(y^k, x^k) \neq \mathsf{p}_{Y^k | X^k}^{\mathbf{R}_{n,n}}(y^k, x^k).$$

Using equation (3.2) in the lecture notes, we conclude that $\mathsf{p}_{Y_j | X^j Y^{j-1}}^{\mathbf{P}_n \oplus \mathbf{P}'_n} \neq \mathsf{p}_{Y_j | X^j Y^{j-1}}^{\mathbf{R}_{n,n}}$ for some j, and therefore $\mathbf{P}_n \oplus \mathbf{P}'_n \not\equiv \mathbf{R}_{n,n}$.