Cryptography, winter 2015/16

MICHAEL NÜSKEN, SIMON SCHNEIDER

5. Exercise sheet
Hand in solutions until Saturday, 5 December 2015, 12:00

Exercise 5.1 (A toy generator). (8 points)

Consider the (one-size) generator given by the following table:

s	$G(s)$
000	000000
001	010001
010	111001
011	101110
100	010111
101	101101
110	110011
111	010100

(i) Determine the advantage of the distinguisher that on input w returns whether $\text{bit}_0\, w$ equals $\text{bit}_2\, w$. 3

(ii) Construct a distinguisher with advantage $\frac{1}{2}$. 5

Exercise 5.2 (Game definition for pseudorandomness). (8+4 points)

Show that the definition for pseudorandomness coincides with the game-based 8+4

Definition. *A generator is a pseudorandom generator iff $\ell(\kappa) > \kappa$ and*

$$\text{adv}_G^{PRG}(\mathcal{D}) = 2\left|\text{prob}\left(G^{\text{PRG}}(\mathcal{D}) = \textit{ACCEPT}\right) - \frac{1}{2}\right|$$

is negligible with the game

Game G^{PRG}.

1. Pick $s \in_{\text{🎲}} \{0,1\}^{\kappa}$, $w_0 \leftarrow G(s)$.
2. Pick $r \in_{\text{🎲}} \{0,1\}^{\ell(\kappa)}$, $w_1 \leftarrow r$.
3. Choose $h^{\text{PRG}} \in_{\text{🎲}} \{0,1\}$.
4. Call $\mathcal{D}$ with w_h and await $h'^{,\text{PRG}}$.
5. If $h^{\text{PRG}} = h'^{,\text{PRG}}$ then ACCEPT else REJECT .

Exercise 5.3 (Yao, simple). (0+4 points)

+4 Write down the proof for the

Theorem. *If there is a predictor $\mathcal{P}$ for a generator G with advantage*

$$\mathrm{adv}_{G^{\text{predict}}}(\mathcal{P}) = \Big| \operatorname{prob}\left(\mathcal{P}(G(s)[1..(i-1)]) = G(s)[i]\right) - \operatorname{prob}\left(\mathcal{P}(r[1..(i-1)]) = r[i]\right) \Big|$$

then there is a distinguisher $\mathcal{D}$ with the same advantage.