Cryptography, winter 2016/17

MICHAEL NÜSKEN, JAKOB NUSSBAUMER

6. Exercise sheet
Hand in solutions until Friday, 9 December 2016, 12:00 (noon)

Exercise 6.1 (PRF $\Rightarrow$ PRG). (6 points)

Let $F\colon \{0,1\}^\kappa \to \{\{0,1\}^\kappa \to \{0,1\}^\kappa\}\,,\ k \mapsto F_k$ be a pseudorandom function. Fix $w_0, w_1, w_2 \in \{0,1\}^\kappa$, all different. Define $G(s) := F_s(w_0)|F_s(w_1)|F_s(w_2)$. $\boxed{6}$

Prove that G is a pseudorandom generator.

Exercise 6.2 (IND-CPA?). (12 points)

Let F be a pseudorandom function and G a pseudorandom generator with expansion factor $\ell(\kappa) = \kappa + 1$. For each of the following encryption schemes, classify the scheme is insecure, IND-POA secure (but not IND-CPA) or IND-CPA secure. In each case, the shared key k is chosen unformly random, $k \in \{0,1\}^\kappa$.

(i) To encrypt $m \in \{0,1\}^{2\kappa+2}$ send $m \oplus (G(k)|G(k+1))$. $\boxed{3}$

(ii) To encrypt $m \in \{0,1\}^{\kappa+1}$ choose a random $r \xleftarrow{\$} \{0,1\}^\kappa$ and send $[r, G(r) \oplus m]$. $\boxed{3}$

(iii) To encrypt $m \in \{0,1\}^\kappa$ send $m \oplus F_k(0^\kappa)$. $\boxed{3}$

(iv) To encrypt $m \in \{0,1\}^{2\kappa}$ choose a random $r \xleftarrow{\$} \{0,1\}^\kappa$ and send $[r, m \oplus (F_k(r)|F_k(r+1))]$. $\boxed{3}$

Even if not mentioned explicitly: any statement needs a proof.

Exercise 6.3 (CTR mode). (0+8 points)

Prove this: $\boxed{+8}$

Theorem. *If F is a pseudorandom function then CTR mode with F_k using a randomly chosen initial value* ctr *on ℓ blocks is IND-CPA secure.*

Hint: First, consider $\ell = 2$.