7. Exercise sheet

Hand in solutions until Saturday, 19 December 2015, 12:00

Exercise 7.1 (PRF ⇒ PRG). (4+4 points)

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

Prove that \( G \) is a pseudorandom generator.

Exercise 7.2 (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 uniformly random, \( k \in \{0,1\}^\kappa \).

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

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

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

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

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