

Cryptology: Problem Sheet 2

Topic: PRG, PRF, PRP, IND-CPA Security

- Let F be a secure PRF defined over $(\{0, 1\}^n, \{0, 1\}^n, \{0, 1\}^n)$.
 - Prove that $G_k(x) := F_k(x) \oplus x$ is a secure PRF.
 - Prove that $G_{(k,k')}(x) := F_k(x) \oplus F_{k'}(x)$ is a secure PRF.
 - Show that $G_k(x) := F_k(x) \| F_k(F_k(x))$ is insecure.

- Prove that if F is a pseudorandom function defined over $(\{0, 1\}^n, \{0, 1\}^n, \{0, 1\}^n)$, then

$$G(s) := F_s(1) \| F_s(2) \| \dots \| F_s(\ell)$$

is a pseudorandom generator with expansion factor $n\ell$.

- Let G be a pseudorandom generator with expansion factor $\ell(n) > 2n$. In each of the following cases, say whether G' is a pseudorandom generator. If yes, give a proof; if not, show a counterexample.

- Define $G'(s) = G(s_1 \dots s_{n/2})$, where $s = s_1 \dots s_n$.
- Define $G'(s) = G(0^{|s|} \| s)$.
- Define $G'(s) = G(s) \| G(s+1)$.

- Let F be a pseudorandom function from n -bits to n -bits and G be a pseudorandom generator with expansion factor $n+1$. For each of the following encryption schemes, state whether the scheme (i) has indistinguishable encryptions in the presence of an eavesdropper and whether (ii) it is IND-CPA secure.

- $Enc_k(m) := \langle r, G(r) \oplus m \rangle$, where $m \in \{0, 1\}^{n+1}$, $r \leftarrow_{\$} \{0, 1\}^n$.
- $Enc_k(m) := m \oplus F_k(0^n)$.
- $Enc_k(m) := \langle r, m_1 \oplus F_k(r), m_2 \oplus F_k(r+1) \rangle$, where $r \leftarrow_{\$} \{0, 1\}^n$, where $m = m_1 \| m_2$, $|m_1| = |m_2| = n$.

- Let F be a pseudorandom permutation. Consider the mode of operation in which a uniform value $r \leftarrow_{\$} \{0, 1\}^n$ is chosen, and the i -th ciphertext block c_i is computed as

$$c_i := F_k(r \oplus i \oplus m_i).$$

Show that this scheme does not have indistinguishable encryptions in the presence of an eavesdropper.