MTAT.07.003 Cryptology II
Spring 2010 / Exercise Session IV / Additional Exercises

1. Pseudorandom permutation family $\mathcal{F}$ can be converted into a pseudorandom generator by choosing a function $f \xleftarrow{u} \mathcal{F}$ and then using the counter scheme $\textsc{Ctr}_f(n) = f(0)\|f(1)\|\ldots\|f(n)$. Alternatively, we can use the following iterative output feedback $\textsc{Ofb}_f(n)$ scheme

$$c_1 \leftarrow f(0), c_2 \leftarrow f(c_1), \ldots, c_n \leftarrow f(c_{n-1}) \enspace ,$$

where $c_1, \ldots, c_n$ is the corresponding output. In both cases, the function f is the seed of the pseudorandom function. Compare the corresponding security guarantees. Which of them is better if we assume that $\mathcal{F}$ is (n, t, ε)-pseudorandom permutation family?

Hint: To carry out the security analysis, formalise the hypothesis testing scenario as a game pair and then gradually convert one game to another by using the techniques introduced in Exercise Session IV. Pay a specific attention to the cases when $c_i = c_{i+k}$ for some $k > 0$.

(⋆) The counter mode converts any pseudorandom function into a pseudorandom generator. Give a converse construction that converts any pseudorandom generator into a pseudorandom function. Give the corresponding security proof together with precise security guarantees.

Hint: Use a stretching function $f : \{0,1\}^n \to \{0,1\}^{2n}$ to fill a complete binary tree with n-bit values.

2. A predicate $\pi : \{0,1\}^n \to \{0,1\}$ is said to be a ε-*regular* if the output distribution for uniform input distribution is nearly uniform:

$$|\Pr[s \xleftarrow{u} \{0,1\}^n : \pi(s) = 0] - \Pr[s \xleftarrow{u} \{0,1\}^n : \pi(s) = 1]| \le \varepsilon \enspace .$$

A predicate π is a (t, ε)-*unpredictable* also known as (t, ε)-*hardcore predicate* for a function $f : \{0,1\}^n \to \{0,1\}^{n+\ell}$ if for any t-time adversary

$$\mathsf{Adv}_f^{\mathsf{hc\text{-}pred}}(\mathcal{A}) = 2 \cdot \left|\Pr[s \xleftarrow{u} \{0,1\}^n : \mathcal{A}(f(s)) = \pi(s)] - \tfrac{1}{2}\right| \le \varepsilon \enspace .$$

Prove the following statements.

(a) Any (t, ε)-hardcore predicate is 2ε-regular.

(b) For a function $f : \{0,1\}^n \to \{0,1\}^{n+\ell}$, let $\pi_k(s)$ denote the kth bit of $f(s)$ and $f_k(s)$ denote the output of $f(s)$ without the kth bit. Show that if f is a (t, ε)-secure pseudorandom generator, then π_k is (t, ε)-hardcore predicate for f_k.

(⋆) If a function $f : \{0,1\}^n \to \{0,1\}^{n+\ell}$ is (t, ε_1)-pseudorandom generator and $\pi : \{0,1\}^n \to \{0,1\}$ is efficiently computable predicate (t, ε_1)-hardcore , then a concatenation $f_*(s) = f(s)||\pi(s)$ is $(t, \varepsilon_1 + \varepsilon_2)$-pseudorandom generator.

3. Let $\mathcal{F}$ be a (t, q, ε)-pseudorandom function family that maps a domain $\mathcal{M}$ to the range $\mathcal{C}$. Let $g : \mathcal{M} \to \{0,1\}$ be an arbitrary predicate. What is the success probability of a t-time adversary $\mathcal{A}$ in the following games?

$$\mathcal{G}_0^{\mathcal{A}} \left[\begin{array}{l} m \xleftarrow[u]{} \mathcal{M} \\ f \xleftarrow[u]{} \mathcal{F} \\ c \leftarrow f(m) \\ \textbf{return } [\mathcal{A}(c) \stackrel{?}{=} m] \end{array}\right. \qquad \mathcal{G}_1^{\mathcal{A}} \left[\begin{array}{l} m \xleftarrow[u]{} \mathcal{M} \\ f \xleftarrow[u]{} \mathcal{F} \\ c \leftarrow f(m) \\ \textbf{return } [\mathcal{A}(c) \stackrel{?}{=} g(m)] \end{array}\right.$$

Establish the same result by using the IND-SEM theorem. More precisely, show that the hypothesis testing games

$$\mathcal{G}_{m_0}^{\mathcal{A}} \left[\begin{array}{l} f \xleftarrow[u]{} \mathcal{F} \\ c \leftarrow f(m_0) \\ \textbf{return } \mathcal{A}(c) \end{array}\right. \qquad \mathcal{G}_{m_1}^{\mathcal{A}} \left[\begin{array}{l} f \xleftarrow[u]{} \mathcal{F} \\ c \leftarrow f(m_1) \\ \textbf{return } \mathcal{A}(c) \end{array}\right.$$

are $(t, 2\varepsilon)$-indistinguishable for all $m_0, m_1 \in \mathcal{M}$.

4. Feistel cipher $\textsc{Feistel}_{f_1,\ldots,f_k} : \{0,1\}^{2n} \to \{0,1\}^{2n}$ is a classical block cipher construction that consists of many rounds. In the beginning of the first round, the input x is split into two halves such that $L_0 \| R_0 = x$. Next, each round uses a random function $f_i \leftarrow \mathcal{F}_{\mathrm{all}}$ to update both halves:

$$L_{i+1} \leftarrow R_i \qquad \text{and} \qquad R_{i+1} \leftarrow L_i \oplus f_i(R_i) \ .$$

The output of the Feistel cipher $\textsc{Feistel}_{f_1,\ldots,f_k}(L_0 \| R_0) = L_k \| R_k$.

(a) Show that the Feistel cipher is indeed a permutation.

(b) Show that the two-round Feistel cipher $\textsc{Feistel}_{f_1,f_2}(L_0 \| R_0)$ where $f_1, f_2 \leftarrow \mathcal{F}_{\mathrm{all}}$ is not a pseudorandom permutation. Give a corresponding distinguisher that uses two encryption queries.

(c) Show the three-round Feistel cipher $\textsc{Feistel}_{f_1,f_2,f_3}(L_0 \| R_0)$ where $f_1, f_2, f_3 \leftarrow \mathcal{F}_{\mathrm{all}}$ is a pseudorandom permutation. For the proof, note that the output of the three round Feistel cipher can be replaced with uniform distribution if f_2 and f_3 are always evaluated at distinct inputs. Estimate the probability that the ith encryption query creates the corresponding input collision for f_2. Estimate the probability that the ith encryption query creates an input collision for f_3.

(•) Show that the tree-round Feistel cipher $\textsc{Feistel}_{f_1,f_2,f_3}(L_0 \| R_0)$ is not pseudorandom if the adversary can also make decryption queries.

(⋆) Show that the four-round Feistel cipher $\textsc{Feistel}_{f_1,f_2,f_3,f_4}(L_0 \| R_0)$ where $f_1, f_2, f_3, f_4 \leftarrow \mathcal{F}_{\mathrm{all}}$ is indistinguishable from $\mathcal{F}_{\mathrm{prm}}$ even if the adversary can make also decryption calls.

($\star$) Note that exercises above and the PRP/PRF swithing lemme give a circular constructions: PRP $\Rightarrow$ PRF $\Rightarrow$ PRF, PRF $\Rightarrow$ PRG $\Rightarrow$ PRF. Consequently, the existence assumptions for pseudorandom permutations, pseudorandom functions and pseudorandom generators are equivalent. However, the equivalence of existence assumptions is only quantitative.

(a) Analyse the tightness of all constructions. More precisely, start with a certain primitive, do the full cycle and analyse how much the resulting degradation of efficiency and security guarantees. Interpret the results: which existence assumptions is the must powerful.

(b) Give a direct circular construction: PRP $\Rightarrow$ PRG $\Rightarrow$ PRG that is better than combined construction over PRF or show that both combined construction are optimal.