CS355: Topics in cryptography **Fall 2004**

Assignment #1

Due: Monday, Nov. 1st, 2004.

Problem 1: **a.** Let $f : \{0,1\}^n \to \{0,1\}^m$ be an efficiently computable one-to-one function. Show that if f has a (t, ϵ) hard core bit then f is $(t, 2\epsilon)$ one-way.

b. Show that if $G : \{0,1\}^n \to \{0,1\}^{2n}$ is a (t, ϵ) PRNG then G is also (t', ϵ') one-way for some (t', ϵ') close to (t, ϵ). Give the best bounds you can.

c. Show that if $F : \{0,1\}^n \times \{0,1\}^k \to \{0,1\}^n$ is a (t, ϵ, q) PRF then

$$G(s) = F(1,s) \| F(2,s) \| \cdots \| F(q,s)$$

is a $(t - q, \epsilon)$ PRNG. We are assuming that evaluating F takes unit time.

Problem 2: Hybrid arguments (in part (a)).

a. Let $G : \{0,1\}^n \to \{0,1\}^m$ be a (t, ϵ) PRNG. Define the distributions P_1 and P_2 as:

$$\begin{aligned} P_1 &= \{G(x_1), \ldots, G(x_q) \in \{0,1\}^m \ : \ x_1, \ldots, x_q \leftarrow \{0,1\}^n\} \\ P_2 &= \{y_1, \ldots, y_q \leftarrow \{0,1\}^m\} \end{aligned}$$

Show that P_1 and P_2 are $(t - cq, q\epsilon)$ indistinguishable for some constant $c > 0$.

b. Let H be a group of prime order q and $g \in H$ a fixed public generator. Consider the following PRNG, $G : \mathbb{Z}_q^2 \to H^3$, defined by $G(a,b) = [g^a, g^b, g^{ab}]$. As above, define the two distributions:

$$\begin{aligned} P_1 &= \left\{G(a_1, b_1), \ldots, G(a_q, b_q) \in H^3 \ : \ a_1, b_1 \ldots, a_q, b_q \leftarrow \mathbb{Z}_q\right\} \\ P_2 &= \{h_1, \ldots, h_{3q} \leftarrow H\} \end{aligned}$$

Show that if the (t, ϵ)-DDH assumption holds in H then P_1 and P_2 are $(t - cq, \epsilon)$ indistinguishable for some constant $c > 0$ (assuming exponentiation in H takes constant time). Hence, for DDH PRNG we get a more efficient reduction than for general PRNG's.

Problem 3: Let $F : \{0,1\}^n \times \{0,1\}^s \to \{0,1\}^t$ be a (t, ϵ, q) unpredictable function (UF). For vectors $x, y \in \{0,1\}^t$ define $x \cdot y$ to be the inner product of x and y modulo 2, i.e. $x \cdot y = \sum_{i=1}^n x_i y_i \bmod 2$. Define the function $F' : \{0,1\}^n \times \{0,1\}^{s+t} \to \{0,1\}$ by

$$F'_{k,r}(x) = F'(x, (k,r)) \stackrel{def}{=} F_k(x) \cdot r \ \in \{0,1\}$$

Prove using the Goldreich-Levin algorithm that F' is a (t', ϵ', q')-PRF for some t', ϵ', q'. Give the best parameters t', ϵ', q' you can.

As a simple application for this result, note that your proof suggests one way for converting any determinstic MAC into a symmetric encryption scheme.

Problem 4: Let $H = \{h_k : \{0,1\}^N \to \{0,1\}^n\}$ be a family of hash functions such that

$$\forall x \neq y \in \{0,1\}^N : \Pr_{h \leftarrow H}[h(x) = h(y)] < \epsilon'.$$

Let $F : \{0,1\}^n \times \{0,1\}^s \to \{0,1\}^t$ be a (t, ϵ, q)-PRF.
Prove that $HF_{k1,k2}(M) = F_{k1}(h_{k2}(M))$ is a $(t, \epsilon + \epsilon', q)$ unpredictable function (UF).
This gives a simple construction for a MAC on large inputs from a PRF and a Universal Hash Function (UHF).

Problem 5: Let $\pi : \{0,1\}^n \times \{0,1\}^k \to \{0,1\}^n$ be a (t, ϵ, q) PRP. Given k, both $\pi_k(x)$ and $\pi_k^{-1}(x)$ can be efficiently computed. Show how to construct an SPRP out of π. Prove that your construction is a (t', ϵ', q) SPRP. Give the best values of t', ϵ' you can. Your solution suggests a way of converting any block cipher that is resistant to chosen PT attacks into a block cipher that resists both chosen PT and chosen CT attacks.

Problem 6: Let p be a prime and let $g \in \mathbb{Z}_p^*$ generate a subgroup of order q for some $q \equiv 3 \bmod 4$. Define $\text{lsb}_2(x) = 0$ if $x \bmod 4$ is 0 or 1 and $\text{lsb}_2(x) = 1$ otherwise. Let $f : \{0, 1, \ldots, q-1\} \to \mathbb{Z}_p^*$ be the function $f(x) = g^x \bmod p$. Show that if $\text{lsb}(x)$ is a (t, ϵ) hard core bit of f then so is $\text{lsb}_2(x)$.