CS355: Topics in cryptography **Spring 2010**

Assignment #1

Due: Thursday, May. 6, 2010.

Problem 1: PRFs. In this problem we study an alternate experiment used to define a secure PRF $F : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$. As usual we define two experiments EXP(0) and EXP(1). In both experiments the challenger begins by choosing a random key k in $\mathcal{K}$. The attacker then (adaptively) submits q queries $x_1, \ldots, x_q \in \mathcal{X}$ and the challenger responds with $F(k, x_i)$ for $i = 1, \ldots, q$. Once the query phase is over, the attacker submits an $x^* \in \mathcal{X}$.

- In EXP(0) the challenger responds with $F(k, x^*)$.
- In EXP(1) the challenger responds with a fresh random $y \stackrel{\text{R}}{\leftarrow} \mathcal{Y}$.

For $b = 0, 1$ let W_i be the probability that the attacker A outputs 1 in EXP(b). Define

$$\text{adv}[A, F] = |W_0 - W_1|$$

Show that for all q-query adversaries A there exists a q-query adversary B (with about the same running time as A) such that

$$\text{PRFadv}[A, F] \le q \cdot \text{adv}[B, F]$$

where PRFadv is B's advantage in the standard PRF security experiments. Hence, if F is secure by these new experiments then F is also a secure PRF by the standard experiments.
Hint: define q hybrid distributions such that if A is able to distinguish any two then we obtain an adversary B with advantage at least PRFadv$[A, F]/q$.

Problem 2: Naor-Reingold PRF.

a. Show that if the Naor-Reingold PRF is implemented in a group where the DDH problem is easy then the PRF is insecure.

b. Suppose we define a PRF as $F(\ (k_1, \ldots, k_n, h),\ (b_1 \ldots b_n)\ ) := h^{(\sum_{i=1}^{n} k_i^{b_i})}$ where $(b_1 \ldots b_n)$ is in $\{0, 1\}^n$. Show that the resulting function is not a secure PRF.

Problem 3: Private information Retrieval. In class we saw how to use the ϕ-hiding assumption to construct a PIR protocol. Show that this PIR can be used to lookup k bits in the database (for small k, e.g. $k \le 5$) with no additional communication beyond what is needed to lookup one bit.

Problem 4: Oblivious Transfer. Describe a variant of the Naor-Pinkas OT protocol that works in a group where DDH is easy, but the 2-linear assumption holds.
Hint: use the random self reduction of the 2-linear assumption given in the Lewko-Waters paper referenced on the course web site.

Problem 5: In class we described Pallier encryption as follows: the public key is (n, g) where $n = pq$ (p, q are prime) and $g \in \mathbb{Z}_{n^2}$ with $g = 1 \bmod n$. To encrypt a message $m \in \mathbb{Z}_n$ choose a random $r \in \mathbb{Z}_{n^2}$ and set $c := r^n g^m \in \mathbb{Z}_{n^2}$. Show that the factorization of n is sufficient to decrypt c.
Hint: first consider the multiplicative subgroup $G = \{h \in \mathbb{Z}_{n^2} \text{ s.t. } h = 1 \bmod n\}$ and show that discrete log in this group is easy. Then use this fact to decrypt c.

Problem 6: Generalized CBC-MAC. Let $f : K \times (X \times M) \to X$ be a secure PRF. Consider the following function on M^n:

input: key $k \in K$, and $(m_1, \ldots, m_n) \in M^n$

$x_0 \leftarrow 0$
for $i = 1, \ldots, n$ do:
$\quad x_i \leftarrow f\big(k,\ (x_{i-1}, m_i)\ \big)$

output x_n

Show that the resulting function is a secure PRF on the domain M^n assuming f is a secure PRF on the domain $X \times M$. The proof of Theorem 6.4 in the book will be helpful. Can you think of a weaker condition on f that still guarantees that the constructed function is a secure PRF?

Problem 7: Give an example of a secure PRF with key space $\{0,1\}^k$ such that if the adversary learns the first bit of the key then the PRF is no longer secure.