Foundations of Cryptography 2021-22

Homework Set No. 2

Date Due: Dec 20th 2021

1. Show how to construct from a signature scheme that is existentially unforgeable against random message attack a signature scheme that is existentially unforgeable against adaptively chosen message attacks

Hint: use two schemes of the first type

2. Consider an authentication scheme that was suggested by one of the students in past years:

Alice and Bob want to perform a one-time authentication of a message $m \in \{0,1\}^n$. They share a secret string $r \in \{0,1\}^n$ and $g\colon \{0,1\}^n \mapsto \{0,1\}^\ell$ is a function. To authenticate message m, Alice adds $g(r \bigoplus m)$ (and bob checks for consistency).

(i) Show that if one-way functions exist, then there exists a function g' that is one-way but where this scheme is not secure, i.e. it is possible to make Bob accept a message $m' \neq m$ whp.

(ii) Now consider the instantiation for g: think of $m \bigoplus r$ as being a_1 concatenated with a_2, where a_1 and a_2 are $n/2$ bit strings. The function $g(m \bigoplus r)$ sent by Alice is $a_1 \cdot a_2$ where we think of a_1 and a_2 as elements of $GF[2^{n/2}]$.

Prove that the scheme is secure in the sense that a cheating adversary that tries to send a message $m' \neq m$ has probability around $2^{-n/2}$ not to be caught. Watch out for the zeroes!

Hint: we want a function $g\colon \{0,1\}^n \mapsto \{0,1\}^\ell$ s.t. for random $z \in \{0,1\}^N$ we have that given $g(z)$ it is (in terms of information) hard to predict $g(z \bigoplus \Delta)$ for any $\Delta \in \{0,1\}^n$ and $\Delta \neq 0^n$.

3. Show that for $\ell(n) < n$, if the subset problem is one-way then it is also a UOWHF. You will probably need the following fact: the distribution of the output of a random subset for most sets $a_1, a_2, \ldots a_n$ (when $\ell(n) < (1-\alpha)n$) is close to uniform.