COMP-647B Advanced Cryptography

Problem set #2

due on ***Tuesday February 27, 2007***

5. BCSS from BSC

Suppose Alice and Bob have access to a Binary Symmetric Channel (**BSC**) with error probability ε, $0 < \varepsilon < 1/2$. More precisely, for both bits b, $\mathbf{BSC}_\varepsilon(b)$ outputs b wih probability $1-\varepsilon$ and $\neg b$ with probability ε. Typically, Alice sends a random bit b into the channel and Bob gets the output b'. Alice and Bob remain uncertain about the exact value of the other party's bit.

Show how they can use this channel to construct a statistically binding and concealing Bit Commitment scheme (**BCSS**).

6. MA in IA-PZK.

Show that under the assumption of existence of a **BCCP**, it is possible for a poly-time prover to demonstrate membership to a language $\boldsymbol{L}$ in **MA** in perfect zero-knowledge. Assume that for every $\boldsymbol{x} \in \boldsymbol{L}$, the prover is given a witness $\boldsymbol{w}$ of membership to $\boldsymbol{L}$.

7. Expected running time.

Compute precisely the expected running time (total number of calls to **random**) of the following algorithm related to [NOVY98]:

i:=1;
WHILE $i<n$ **DO**
    q_i:=(0,0,0,…,0);
    WHILE $q_i \in \mathrm{SPAN}(q_1,q_2,\ldots,q_{i-1})$ **DO** **random**(q_i);
    i:=i+1;

8. Claw-free collections.

Consider the following definition:

Definition 3 (Claw-Free Collection). A triple of algorithms, (I, D, F), is called a **claw-free collection** if the following conditions hold:

1. *The algorithms are efficient*: Both I and D are probabilistic polynomial time, whereas F is deterministic polynomial time. We denote by $f_i^\sigma(x)$ the output of F on input (σ, i, x), and by D_i^σ the support of the random variable $D(\sigma, i)$.
2. *Identical range distribution*: For every i in the range of algorithm I, the random variables $f_i^0(D(0, i))$ and $f_i^1(D(1, i))$ are identically distributed.
3. *Hard to form claws*: For every probabilistic polynomial time algorithm, A', every polynomial $p(\cdot)$, and all sufficiently large n's,

$$\text{Prob}(f_{I_n}^0(X_n) = f_{I_n}^1(Y_n)) < \frac{1}{p(n)},$$

where I_n is a random variable describing the output distribution of algorithm I on input 1^n, and (X_n, Y_n) is a random variable describing the output of algorithm A' on input (random variable) I_n.

8.A Let p be a prime (with known factorization of p-1) sufficiently large so that the discrete logarithm problem (mod p) is considered infeasible. Show how we can construct a Claw-Free Collection from this assumption.

8.B Show how we can use Claw-Free Collections to construct a **BCCP** under the extra assumption below:

Proposition 1. *Let* (I, D, F) *be a claw-free collection* **with a probabilistic polynomial-time recognizable set of indices** (*i.e., the range of algorithm* I *is in* $\mathcal{BPP}$).

8.C Explain why this extra assumption is useful.