Foundations of Cryptography

Homework Set No. 6

Date Due: Feb 11th 2007

1. Suggest a commitment protocol for two provers. The setting is where the two provers agree on a random string *before* the beginning of the protocol; afterwards they are assumed not to talk to each other. The Verifier/receiver talks to both of them. Only one of the provers needs to know the string x to which they are committing

   Define the properties of the protocol (hiding, binding).

2. Give a direct protocol (i.e. *not* through a reduction to Hamiltonicity) for the subset sum problem. Recall that the Subset sum problem is: given n numbers $0 \leq a_1, a_2, \ldots a_n \leq 2^m$ and a target sum T, is there a subset $S \subseteq \{1, \ldots n\}$ such that $\sum_{i \in S} a_i = T mod 2^m$.

3. Computational binding commitment from collision intractable has function: Our goal is to construct a commitment scheme where the induced distribution of the transcript is (nearly) independent of the string committed to and where no PPT sender can, with probability better than (1-negligible) reveal two different strings.

   Consider the following protocol for committing to a bit b. Let H be a family of collision intractable hash functions:

   Commit:
   - Receiver: choose $h \in_R H$ and give h to sender
   - Sender choose random z and r. Send $h(z), r$ and $\langle z, r \rangle \oplus b$.

   Reveal: publish z.

   Prove that the protocol satisfies the above requirements. To give a full proof provide the lengths of the strings that the function h maps.

   Hint: use pair-wise independence and Chebyshev's inequality (Lecture 6).

4. Find the error: Let E be an public-key encryption scheme which is errorless. Let H be a family of collision intractable hash functions. Consider the following protocol for commitment to x:

   Commit: Sender chooses keys (K_P, K_S) for E and $h \in H$ and sends

   $$K_P, E(K_P, x), H(x \circ E(K_p, x)).$$

   Reveal: publish K_S.

   Show that there exists a family H of collision intractable hash functions such that the scheme is insecure for any E (assuming that collision intractable hash functions exist).