COS 496: Cryptography Due: Dec 4

Problem Set 5

Professor Amit Sahai

Please list everyone you collaborated with when solving the problems on this problem set. If you make use of outside material, make a note of that as well. Make sure you write up your solutions on your own.

Problem 1. This problem asks you to use our result about zero-knowledge proof systems for NP to construct new secure cryptographic protocols. Please provide a security proof for all your constructions. (This is exercise 4.18 from Goldreich's book.)

1. Suppose that party S sends, over a public channel, encrypted data to several parties, $R_1, \ldots, R_t$. Specifically, the data sent to R_i are encrypted using the public encryption key of party R_i. We assume that all parties have access to the ciphertexts sent over the public channel. Give a secure protocol that allows S to prove to some other party that it has sent the same data to all R_i's, but without revealing the data.

2. Referring to the same communication setting, consider a party R that has received data encrypted using its own public encryption key. Suppose that these data consist of two parts, and party R wishes to reveal to someone the first part of the data but not the second. Further suppose that the other party wants a proof that R has indeed revealed the correct content of the first part of the data.

3. Suppose that party S wishes to send party R a signature to a publicly known document such that only R receives the signature, but everyone else can verify that such a signature was indeed sent by S. (We assume, again, that all parties share a public channel.)

Problem 2. In this problem we see how zero-knowledge allows us to simulate 'proofs' of false theorems.

Suppose you are given an oracle for the "sampler function" $S_1(1^k)$ which produces a random string of length k from language L, and $S_0(1^k)$ which produces random strings not in L. Furthermore, suppose that the output of these two machines is computationally indistinguishable, $S_0(1^k) \equiv_c S_1(1^k)$.

Now consider a zero-knowledge proof system (P, V) for L, and the following output distributions: (1) Given an $x \leftarrow S_1$, output $(x, (P, V)(x))$, and (2) Given an $x \leftarrow S_0$, output $(x, S(x))$ where S is the polynomial-time simulator of the zero-knowledge protocol for a given V.

Show that distributions (1) and (2) are computationally indistinguishable. Remember that we only defined the behavior of a zero-knowledge proof system for $x \in L$, so you'll have to think about exactly what (2) means. You may assume that V is honest-but-curious.

Problem 3. In this problem you will prove that strong proofs of knowledge exist for all problems in NP. If R is a binary relation (e.g. an NP relation) then the interactive function V is a *strong knowledge verifier* for R if

1. There exists an interactive machine P such that for every $(x, w) \in R$ all possible interactions of V with P on input x and auxiliary input w are accepting (This requirement prevents trivial systems.)

2. There exists a negligible funcion α and a PPT oracle machine E such that for a given polynomial-time *deterministic* prover P^* and all strings x, if $\Pr[(P^*, V)(x) \text{ succeeds}] > \alpha(|x|)$ then $\Pr[E^{P^*(x)} = w \text{ such that } (x, w) \in R] > 1 - \alpha(|x|)$.

The oracle machine E is a *strong knowledge extractor* for V, as discussed in class. Consider the zero-knowledge proof system given for the directed Hamiltonian cycle problem. Prove that the proof system that results from sequentially iterating the basic system many times is a strong proof of knowledge for a Hamiltonian cyle.

Problem 4. In class we saw an example of a bit commitment scheme C with computational secrecy: $(C(0; \cdot)) \equiv_c (C(1; \cdot))$. This scheme had perfect binding, meaning that revealing the bit is unambiguous: $C(0; \cdot) \cap C(1; \cdot) = \emptyset$.

Now consider the definition of a scheme with perfect *secrecy*. This means that the distributions produced by a commitment of zero and a commitment of one are identically distributed: $(C(0, ; \cdot)) \equiv (C(1; \cdot))$. Prove that there exists no two-party protocol which simultaneously has perfect binding and perfect secrecy. (This is exercise 4.32 from Goldreich's book.)

Problem 5. To solve this problem, you need to recall the discrete logarithm assumption, as given on the number theory handout provided at the beginning of the semester.

Consider the following commitment scheme: There is a ranomly chosen prime p, a randomly chosen generator $g \in Z_p$, and $h = g^x$, where x is randomly chosen. Of these, p, g, and h are publicly known, but *not* x. To commit a zero, send $C(0; r) = g^r$, $r \leftarrow Z_p$. To commit a one, send $C(1; r) = g^r \cdot h$.

1. Prove that this scheme has perfect secrecy (as the definition in problem 3) and computational binding, as defined here: No PPT committer A, given randomly chosen g, h, and p as input, can output a commitment c and openings for c to both 0 and 1 with non-negligible probability.

2. Now take our zero-knowledge protocol for directed Hamiltonian cycle, and replace its commitment scheme with this one. Prove that this protocol has *perfect* zero-knowledge and is *computationally* sound. Define computational soundness as follows: $\exists$ negligible $\alpha()$ s.t. $x \notin L \Rightarrow \forall$ PPT $P^*, \Pr[(P^*, V)(x) = 1] \leq \frac{1}{2} + \alpha()$.