6.897: Selected Topics In Cryptography Canetti

Problem Set 1

February 27, 2004 *Due: March 12, 2004*

1 Question 1: Equivalence of Zero-Knowledge arguments of knowledge and protocols for realizing f_{zk}

Recall the definition of Zero-Knowledge Proofs of Knowledge (ZKPoK) protocols, as it appears on the slides for lecture 3. Here we're considering two-party protocols where one party (P, the prover) gets input (x, w) and the other party (V, the verifier) gets no input. The notation $(P(p), V(v))$ means (the random variable describing) the outputs of P and V from an interaction where P runs on input p and V runs on input v. $(P(p), V(v))_P$ descrives the output of P, and $(P(p), V(v))_V$ described the output of V. (That is, $(P(p), V(v)) = ((P(p), V(v))_P, (P(p), V(v))_V)$).

Definition 1 *Let $R(\cdot, \cdot)$ be a binary relation. A protocol for P, V is a ZKPoK protocol for R if the following holds:*

Completeness: *If P and V follow the protocol then $(P(x, w), V)_V = (x, R(x, w))$ except with negligible probability.*

Soundness (PoK): *For any "cheating prover P^*" there exists an "extractor" E such that for all z we have $E(z) = (t, x^*, w^*)$ where $(t, (x^*, R(x^*, w^*))) \approx (P^*(z), V)$. Here "$\approx$" means "computationally indistinguishable" as defined in class.*

Zero-Knowledge: *For any "cheating verifier" V^* there exists a "simulator" S such that for all inputs x, w, z we have $S(x, R(x, w), z) \approx (P(x, w), V^*(z))_V$.*

1.1 Relation to the standard notion of ZK

Show how to construct, given a protocol π that is ZKPoK for R as defined above, a protocol π' that is ZK using the standard notion (i.e., where both parties are guaranteed to get the same public input x), without any additional computational assumptions. For this purpose, you can you any standard definition of ZK (e.g. the definitions in Oded Goldreich's book).

1.2 Relation to the standard notion of PoK

Is the protocol π' constructed above a PoK using standard notions (say, the notion in Oded's book)? If not, how can the above notion of ZKPoK be changed so that π will become a PoK according to standard notions?

1.3 Equivalence with realizing f_{zk}

Let R by a binary relation, and let f_{zk}^R denote the two party function $f_{zk}^R((x, w), -, -) = (-, (x, R(x, w), -)$. Show that a protocol is a ZKPoK for R as defined here if and only if it securely evaluates f_{zk}^R according to the basic definition.

2 Question 2: Universal composition of arbitrary functionalities.

The universal composition theorem was proven in class only for the case where the ideal functionality is PPT. Prove or disprove: The universal composition theorem holds for all ideal functionalities, even ones that are not PPT.