600.641 Special Topics in Theoretical Cryptography February 5, 2007

Handout 4: Problem Set 1

Instructor: Susan Hohenberger

Due: Midnight on Friday, Feb 16. Please send a pdf of your solutions to susan@cs.jhu.edu.

You are encouraged to collaborate. Each person must, however, write up their own solutions separately. For each problem, please indicate who you collaborated with and if you used any reference materials please list those as well.

Recall our working definition of a zero-knowledge proof system from lecture.

Definition 0.1 (A Working Definition of Zero-Knowledge Proofs) *Let k be the security parameter. We say that a pair of algorithms (P, V), where V runs in probabilistic polynomial time, are a zero-knowledge proof system for a language L if the following properties hold:*

1. **Completeness:** $\forall x \in L$, $\Pr[(P,V)[x] = accept] \geq 1 - negl(k)$.
2. **Soundness:** $\forall P^*$, $\forall x \notin L$, $\Pr[(P^*,V)[x] = accept] \leq \frac{1}{2}$.
3. **Zero-Knowledgeness:** $\forall V^*_{\mathsf{PPT}}$, $\exists S_{\mathsf{PPT}}$, $\forall x \in L$, $\forall a \in \{0,1\}^{poly(|x|)}$, $VIEW_{P,V^*(a)}(x) \approx S(x,a)$.

Problem 1: Quick Questions

(25 points) True or False or Unknown: (You do not need to justify your answer, but you may for partial credit.)

1. T or F or U: IP = PSPACE.
2. T or F or U: Suppose language L has an interactive proof system, then there exists a (non-interactive) algorithm that decides L in polynomial space.
3. T or F or U: (Computational) ZK $\subseteq$ NP.
4. T or F or U: Co-NP $\subseteq$ (Computational) ZK.
5. T or F or U: The definition of zero-knowledge proofs given above is closed under parallel composition.

Problem 2: Making Commitments

(30 points) Consider the "valentine" commitment scheme[1]: Let g and h generate a group $\mathbb{G}$ of prime order q. The values $(g, h, \mathbb{G}, q)$ form the public parameters of the commitment

[1] We'll credit the inventor(s) of this scheme after Feb 16.

scheme. To commit to a value v, choose a random value $r \in \mathbb{Z}_q$ and output the commitment $C = g^v \cdot h^r$. Commitment C is opened by revealing (v, r), and this opening is verified by checking that C indeed is equal to $g^v \cdot h^r$.

Now, we define the Discrete Logarithm (DL) problem in $\mathbb{G}$ as follows: on input a random value $t \in \mathbb{G}$, output a value $x \in \mathbb{Z}_q$ such that $t = g^x$.

(a) Is the valentine commitment scheme perfectly or computationally *binding*? Do you need to assume the DL problem is hard in $\mathbb{G}$? Provide an argument to support your answer.

(b) Is the valentine commitment scheme perfectly or computationally *hiding*? Do you need to assume the DL problem is hard in $\mathbb{G}$? Provide an argument to support your answer.

Problem 3: Flavors of Zero-Knowledge

(40 points) Recall the zero-knowledge proof system described in class for Graph 3-Coloring (3COL). We used a commitment scheme which was perfectly binding and computationally hiding based on the quadratic residuosity assumption. Now, suppose we instead want to use the valentine commitment scheme to implement our 3COL protocol.

(a) Describe the steps of this protocol.

It should be obvious that completeness holds.

(b) Does soundness hold? If your answer is yes, provide an argument to support your answer. If your answer is no, write a reasonable definition of soundness that your protocol does meet, intuitively explain why this definition makes sense, and then argue why your protocol meets it.

(c) Does zero-knowledgeness hold? If your answer is yes, describe a simulator and argue why it works. If your answer is no, keep thinking about it or go back to step (a).

Problem 4: Applications of ZK Proofs and Proofs of Knowledge

(5 points) Briefly describe a real-world application of a zero-knowledge proof or a zero-knowledge proof of knowledge. Feel free to be creative.