600.641 Special Topics in Theoretical Cryptography March 5, 2007

Handout 5: Problem Set 2

Instructor: Susan Hohenberger

Due: 11:59pm on Wednesday, March 21. 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.

Problem 1: Types of Interactive Protocols

(20 points) In your own words, briefly explain the differences between:

(a) a *perfect* zero-knowledge *argument*, and

(b) a *computational* zero-knowledge *proof*.

Problem 2: Proofs of Knowledge

(40 points) Let $\mathbb{G}$ be a group of prime order q with random generators g, h and f. Assume the discrete logarithm (DL) problem is hard in $\mathbb{G}$.

For each of the following, **write out the protocol in clear, detailed steps.** We are using the notation introduced by Camenisch and Stadler [CS97] for various proofs of knowledge of discrete logarithms and proofs of the validity of statements about discrete logarithms. For instance,

$$PK\{(\alpha, \beta, \delta) : A = g^{\alpha} h^{\beta} \wedge B = f^{\delta}\}$$

denotes a "*zero-knowledge Proof of Knowledge of integers* α, β, *and* δ *such that* $A = g^{\alpha} h^{\beta}$ *and* $B = f^{\delta}$," where A, B, g, h, and f are elements of some group $\mathbb{G}$. The convention is that Greek letters denote quantities of which knowledge is being proven, while all other values are known to the verifier.

1. Suppose $A = g^x h^y f^z$. Describe $PK\{(\alpha, \beta, \delta) : A = g^{\alpha} h^{\beta} f^{\delta}\}$.
2. Suppose $A = g^x h^y$ and $B = f^z$. Describe $PK\{(\alpha, \beta, \delta) : A = g^{\alpha} h^{\beta} \wedge B = f^{\delta}\}$.
3. Suppose $A = g^x h^y$ and $B = f^x$. Describe $PK\{(\alpha, \beta) : A = g^{\alpha} h^{\beta} \wedge B = f^{\alpha}\}$.
4. Suppose $A = g^x$, $B = h^y$, and $C = f^z$. Describe $PK\{(\alpha, \beta, \delta) : A = g^{\alpha} \vee B = h^{\beta} \vee C = f^{\delta}\}$. (Without loss of generality, assume the prover knows x but not y or z.)

Problem 3: Practicing Proofs

(30 points) Pick any one of the four protocols you presented in problem 2. (Again, you only need to do this for *one* protocol.) Consider the pair of algorithms (P, V) that you described for this protocol. Prove that your protocol has the following two properties.

Let $R = \{(x, w)\}$ be an NP-relation. For any x, define its witness set as follows $W(x) = \{w : (x, w) \in R\}$. Also, define $L_R = \{x : \exists\ w \text{ such that } (x, w) \in R\}$.

1. **Honest-Verifier Zero-Knowledge:** There exists a p.p.t. simulator that can produce conversations that are computationally indistinguishable from those between the honest prover and the honest verifier. A protocol (P, V) is honest-verifier zero-knowledge if $\exists\ S_{\mathsf{PPT}}$, $\forall\ (x, w) \in R$, $VIEW_{P(w),V}(x) \approx S^V(x)$.

2. **Special Soundness [CDS94]:** There exists a p.p.t. extractor that can extract a witness from any prover that is successful with non-negligible probability. More precisely, suppose we restrict our focus to three-round public-coin protocols, where conversations in the protocol are ordered triples of the form (m_1, c, m_2). A protocol (P, V) has special soundness if $\forall\ P^*$, $\forall\ x \in L_R$, given two accepting conversations (m_1, c, m_2) and (m_1, c', m_2') between P^* and V about x, where $c \neq c'$, an element of $W(x)$ can be computed in polynomial time.

Problem 4: Current Research

(10 points) For the final project (i.e., problem set 3), everyone will focus on an area of cryptography of particular interest to them. Each student will choose a cryptography paper published in 2002 or later in ASIACRYPT, CRYPTO, EUROCRYPT, or TCC.[1] Each student will then have a chance to present a summary of the work to the class and turn in a written portion as well. (More details on this final project to be announced later.)

For now, *in order of your preference*, please list **three** papers that you find particularly interesting. Include the title, authors' names, conference, and year. This will allow me to give you some feedback and perhaps additional information about your choices.

References

[CDS94] Ronald Cramer, Ivan Damgärd, and Berry Schoenmakers. Proofs of partial knowledge and simplified design of witness hiding protocols. In *Advances in Cryptology – CRYPTO '94*, volume 839 of LNCS, pages 174–187, 1994.

[CS97] Jan Camenisch and M. Stadler. Efficient group signature schemes for large groups. In Burton S. Kaliski Jr., editor, *Advances in Cryptology – CRYPTO '97*, volume 1296 of LNCS, pages 410–424, 1997.

[1] Exceptions will be made on a case-by-case basis for papers in FOCS, ICALP, or STOC.