600.472 Theoretical Cryptography March 27, 2008

Handout 9: Homework 4

Instructor: Susan Hohenberger *TA: Matthew Green*

Due at the start of lecture on Tuesday, April 15, 2008.

For problems 1 and 2, no collaboration is allowed.

Problem 1 *Reviewing Reductions (30 points)*

1. Let $\{f_s : \{0,1\}^k \to \{0,1\}^k \mid s \in \{0,1\}^k\}$ be a PRF family. Consider the construction:

$$H_{s_1,s_2,s_3}(x) = f_{s_1}(x \oplus s_2) \oplus s_3, \text{ where } |s_1| = |s_2| = |s_3| = k.$$

   Prove that H is always a PRF.
2. Let G be a PRG and F be a one-way function. Is $G \circ F$ a PRG? Prove your answer.

Problem 2 *Zero-Knowledge Proofs and Proofs of Knowledge (20 points)*

For this problem, you may talk to other students about what ZKPs and ZKPoKs are, but you must independently think up your own solution.

Be creative. Describe a real-world application where you could use a zero-knowledge proof (ZKP) or a zero-knowledge proof of knowledge (ZKPoK). Clearly state if you are using a ZKP or a ZKPoK. Then briefly describe the application and how this technology would be used/useful in this application.

Bonus (5 points): We will award 5 bonus points (each) for the three solutions which we deem to be most creative, well motivated and/or elegantly explained.

Problem 3 *Robust Combiners (30 points)*

Suppose you are in charge of securing important military communications. You are allowed to purchase one or more products from vendors (which you don't necessarily trust) in order to (hopefully) obtain message integrity and/or privacy.

1. (10 points) Let's first consider message integrity. Two different vendors are offering MAC schemes for the message space $\{0,1\}^\ell$:

   - scheme A with algorithms $(\mathsf{Gen}^A, \mathsf{Tag}^A, \mathsf{Vrfy}^A)$ and
   - scheme B with algorithms $(\mathsf{Gen}^B, \mathsf{Tag}^B, \mathsf{Vrfy}^B)$.

   Suppose one of these schemes is a secure MAC scheme, but we do not know which one.[1] Consider the MAC scheme $(\mathsf{Gen}, \mathsf{Tag}, \mathsf{Vrfy})$ formed by :

[1] In both parts of this problem, you may not assume anything about the security of the "other" scheme.

- Key Generation: $\mathsf{Gen}(1^n)$ runs $k_1 \leftarrow \mathsf{Gen}^A(1^n)$ and $k_2 \leftarrow \mathsf{Gen}^B(1^n)$, and then outputs the key (k_1, k_2).
- Authentication: $\mathsf{Tag}_{k_1,k_2}(m) = \mathsf{Tag}^A_{k_1}(m) \mid\mid \mathsf{Tag}^B_{k_2}(m)$.
- Verify: $\mathsf{Vrfy}_{k_1,k_2}(m, (a||b))$ outputs 1 iff both of $\mathsf{Vrfy}^A_{k_1}(a)$ and $\mathsf{Vrfy}^B_{k_2}(b)$ output 1.

(Here the || means string concatenation.) Is this scheme a secure MAC scheme? Prove or provide a counterexample.

2. (15 points) Next, let's consider message privacy. Two different vendors are offering *public-key* encryption products for the message space $\{0,1\}^\ell$:

   - system A with algorithms $(\mathsf{Gen}_A, \mathsf{Enc}_A, \mathsf{Dec}_A)$ and
   - system B with algorithms $(\mathsf{Gen}_B, \mathsf{Enc}_B, \mathsf{Dec}_B)$.

   Suppose one of these schemes is a CPA-secure system, but we do not know which one. Without assuming any specifics about *how* these encryption schemes work, describe a new encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ which is CPA-secure. First clearly explain what your algorithms do (as we did in the MAC case above) and then prove that your scheme works.

3. (5 points) Consider the encryption scheme you proposed in the last part. Suppose one of these schemes is actually CCA2-secure, but we do not know which one. Would your prior construction be CCA2-secure? Why or why not?

Note: here we are referring to the *public key* definitions of CPA and CCA2 security.

Problem 4 *Red Teaming an Online Auction (20 points)*

Suppose you are called in to "red team" (i.e., point out all the security flaws in) an online auction protocol for an important auction house *before* the auction occurs. They are selling a very rare Mozart manuscript appraised at $6 million. The auction protocol is planned to run as follows:

1. The auction house will securely generate and post online a public key for some CPA-secure encryption scheme, keeping the secret key private.
2. At noon on the auction day, bidders will have two hours to electronically submit an encryption of their bid. That is, they can email in their ciphertext. (Here assume that the message encrypted is the exact dollar amount the bidder is willing to pay.)
3. At the end of two hours, the auction house will close out the bidding and use their secret key to decrypt all of the bids and award the manuscript to the highest bidder, who must pay exactly his/her bid price.[2]

Submit your red team "report" highlighting any potential problems you see as well as any suggestions you have for fixing the problems. Be as organized and concise as possible.

[2]For the sake of this assignment, ignore that a "first-priced sealed-bid auction" may not be the best strategy for all concerned parties from a game theoretic perspective.