CS-7810 Graduate Cryptography October 16, 2017

Problem Set 3

Lecturer: Daniel Wichs *Due: 10/25, 2017*

Problem 1 (Modifying CPA Definition) 10 pts

A. Let us modify the definition of CPA security (see lecture notes 7) by changing the experiment $\mathbf{CPAGame}^b$ so that the adversary does not get access to the encryption oracle before choosing the messages m_0^*, m_1^*. That is, we simply remove step 2 from the game. The adversary still gets access to the encryption oracle in step 4 after receiving the challenge ciphertext c^*. Show that this modified definition is weaker than the original. In other words, show that assuming pseudorandom functions exist, you can construct a contrived scheme which satisfies the modified definition but does not satisfy the original definition.

B. Alternately, we can modify the CPA definition by removing step 4 from the game so that the adversary does not get access to the encryption oracle after choosing the messages m_0^*, m_1^*. In this variant, the adversary still gets access to the encryption oracle in step 2 before it chooses the messages m_0^*, m_1^* and gets the challenge ciphertext c^*. Again, show that this modified definition is weaker than the original

Problem 2 (CRHF or Not) 10 pts

Let $\{H_s : \{0,1\}^{2n} \to \{0,1\}^n\}_{n\in\mathbb{N}, s\in\{0,1\}^n}$ be a collision resistant hash function (CRHF) that compresses $2n$ bits to n bits. For each of the following either show that it is also a CRHF or give a counter-example.

- $H'_s(x)$ outputs the first $n-1$ bits of $H_s(x)$.
- $H'_s(x_1, x_2) = H_s(H_s(x_1), H_s(x_2))$ where $x_1, x_2 \in \{0,1\}^{2n}$.
- $H'_s(x) = H_s(G(x))$ where $x \in \{0,1\}^{n+1}$ and $G : \{0,1\}^{n+1} \to \{0,1\}^{2n}$ is a PRG.

Problem 3 (Are CHRHFs also OWFs?) 15 pts

Let $\{H_s : \{0,1\}^{2n} \to \{0,1\}^n\}_{n\in\mathbb{N}, s\in\{0,1\}^n}$ be a collision resistant hash function (CRHF) that compresses $2n$ bits to n bits. Show that $f(s,x) = (s, H_s(x))$ is a OWF.

Show that this may not hold if $\{H_s : \{0,1\}^{n+1} \to \{0,1\}^n\}_{n\in\mathbb{N}, s\in\{0,1\}^n}$ only compresses $n+1$ bits to n bits.

Problem 4 (CRHF + PRF $\Rightarrow$ MAC) 10 pts

Let $\{H_s : \{0,1\}^* \to \{0,1\}^n\}_{n\in\mathbb{N}, s\in\{0,1\}^n}$ be a collision resistant hash function (CRHF) that takes an arbitrary long input and hashes it to n bits. Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a PRF.

Show that $\mathsf{MAC}((k,s),m) = F_k(H_s(m))$ is a secure MAC with secret key (k,s) that can be used to authenticate arbitrarily long messages m.

Problem 5 (Combiners) 10 pts

- Suppose you have two candidate one-way functions f and f'. You are told that at least one of them is secure but you don't know which. Show how to combine them to get a function f^* which is guaranteed to be one-way.
- Same question for two candidate PRFs F, F'. Show how to construct F^* which is guaranteed to be a PRF if at least one of F, F' is.
- Same question for CPA secure encryption schemes $(\mathsf{Enc}, \mathsf{Dec})$ and $(\mathsf{Enc}', \mathsf{Dec}')$.
- Same question for CRHFs H, H'.