Midterm

This take-home midterm is due in class on **Thursday, April 13.** It contains three "long answer" questions. Prove all statements carefully. Make sure you give a fully specified reduction. Define all adversaries precisely. Define all events, random variables, and probabilities clearly and unambiguously, and show your work when calculating advantages and probabilities. Use standard notation. Double-check the details to make sure that all steps are fully justified. You do not need to re-prove anything proven or stated without proof in class or in the homeworks.

1 Generic Composition

Let (E, D) and (E', D') be two symmetric-key encryption schemes, $E : \mathcal{K} \times \{0,1\}^* \to \{0,1\}^*$ and $E' : \mathcal{K}' \times \{0,1\}^* \to \{0,1\}^*$. Define the encryption scheme $(\hat{E}, \hat{D})$, where $\hat{E} : (\mathcal{K} \times \mathcal{K}') \times \{0,1\}^* \to \{0,1\}^*$, by

$$\hat{E}_{k,k'}(m) = E'_{k'}(E_k(m))$$

and

$$\hat{D}_{k,k'}(c) = \text{let } t \leftarrow D'_{k'}(c).\ \text{if } t = \perp \text{ then return } \perp \text{ else return } D_k(t).$$

For each of the following, decide whether the claim is true or false. If true, give a proof. If false, provide a counterexample (more precisely, show that if there exists any IND-CCA2 secure scheme, then there exist schemes (E, D) and (E', D') that satisfy the premises of the claim but not the conclusion).

(a) True/false: If (E, D) and (E', D') are both IND-CCA2, then $(\hat{E}, \hat{D})$ is guaranteed to be IND-CCA2.

(b) True/false: If (E, D) is IND-CCA2 and (E', D') is IND-CPA, then $(\hat{E}, \hat{D})$ is guaranteed to be IND-CCA2.

(c) True/false: If (E, D) is IND-CCA2 and (E', D') is INT-CTXT, then $(\hat{E}, \hat{D})$ is guaranteed to be IND-CCA2.

2 Bit Commitment in the Random Oracle Model

Your goal is to construct a bit commitment scheme and prove it secure in the random oracle model. A bit commitment scheme is a pair of deterministic algorithms (Commit, Verify) with type signatures Commit : $\mathcal{M} \times \mathcal{R} \to \{0,1\}^*$, Verify : $\{0,1\}^* \times \mathcal{M} \times \mathcal{R} \to \{0,1\}$. If we choose $r \xleftarrow{\$} \mathcal{R}$, then the value Commit$(m, r)$ is a commitment to the message m. We require that Verify(Commit$(m, r), m, r) = 1$ for all m, r. In the random oracle model with hash function $\mathcal{H}$, Commit and Verify are given oracle access to $\mathcal{H}$. There are two security goals:

- **Binding:** It must be infeasible to find a commitment that can be opened two different ways. More precisely, (Commit, Verify) is (t, ϵ)-binding if, for all adversaries A running in time at most t, we have

$$\Pr[(c, m, r, m', r') \leftarrow A^{\mathcal{H}}(); \text{Verify}^{\mathcal{H}}(c, m, r) = 1 \text{ and Verify}^{\mathcal{H}}(c, m', r') = 1 \text{ and } m \neq m'] \leq \epsilon.$$

- **Concealing:** It must be infeasible to learn anything about the message from the commitment. More precisely, (Commit, Verify) is (t, ϵ)-concealing if, for all m, m', $\text{Commit}^{\mathcal{H}}(m, r)$ is (t, ϵ)-indistinguishable from $\text{Commit}^{\mathcal{H}}(m', r')$, where $r, r' \xleftarrow{\$} \mathcal{R}$. In other words, for all adversaries A running in time at most t and for all m, m', we have

$$\left|\Pr[r \xleftarrow{\$} \mathcal{R}; A^{\mathcal{H}}(\text{Commit}^{\mathcal{H}}(m, r)) = 1] - \Pr[r' \xleftarrow{\$} \mathcal{R}; A^{\mathcal{H}}(\text{Commit}^{\mathcal{H}}(m', r')) = 1]\right| \leq \epsilon.$$

We say that the bit commitment scheme (Commit, Verify) is (t, ϵ)-secure in the random oracle model if it is (t, ϵ)-binding and (t, ϵ)-concealing.

(a) What's wrong with the following scheme? $\mathcal{M} = \{0, 1\}$; $\text{Commit}^{\mathcal{H}}(m, r) = \mathcal{H}(m)$; $\text{Verify}^{\mathcal{H}}(c, m, r) = 1$ if $\mathcal{H}(m) = c$, and 0 otherwise. Is it binding? concealing?

(b) Specify a pair of algorithms (Commit, Verify) that form a bit commitment scheme that is (t, ϵ)-secure in the random oracle model, for some reasonable values of (t, ϵ) (say, $t = 2^{80}$, $\epsilon = 2^{-64}$). Specify your choice of the sets $\mathcal{M}$ and $\mathcal{R}$ and any assumptions you are making about the length of the output of $\mathcal{H}$.

(c) State explicitly the values of (t, ϵ) for which you are claiming your scheme from part (b) is secure.

(d) Prove that your scheme from part (b) is secure with the parameters listed in part (c).

3 Block Ciphers on Smaller Domains

As far as we know, AES is a perfectly good 128-bit block cipher $\text{AES} : \mathcal{K} \times \{0, 1\}^{128} \to \{0, 1\}^{128}$. But suppose we want a 127-bit block cipher $E : \mathcal{K}' \times \{0, 1\}^{127} \to \{0, 1\}^{127}$. How do we do it? Describe a construction E that you can prove will be a secure pseudorandom permutation, assuming only that AES is a secure pseudorandom permutation. Your scheme E should be such that we can compute $E_{k'}(x)$ efficiently: the expected running time to compute $E_{k'}(x)$ should be some small constant. Provide a proof of security for your construction.