Homework 2

This problem set is due in class on **Thursday, March 9.**

It contains two "long answer" questions, where you are requested to provide full proofs, and three "short answer" questions, where you are expected to check on your own that you could do a careful proof if you had to, but where you only need to write down a one-sentence answer.

1 Long Answer: A Simpler Block Cipher Based MAC

Let E be a (t, q, ϵ)-PRF with 128-bit keys and 128-bit block width. Fix $n > 0$. Define $F : \{0,1\}^{128} \times \{0,1\}^{128n} \to \{0,1\}^{128}$ by $F_K(M) = X_n$, where $X_0 = K$, $X_i = E_{X_{i-1}}(M_i)$, and $M = (M_1, \ldots, M_n)$.

Prove that F is a (t', q', ϵ')-PRF, for some values of t', q', ϵ' which you should specify as a function of n, t, q, ϵ. (Make sure to spell out the reduction carefully—it's a little tricky.)

2 Long Answer: Strong Encryption with a Weak Cipher

Suppose that AES with a 128-bit key is a $(t, 2, t/2^{128})$-PRF for all t. However, suppose you have no guarantees on the security of AES against adversaries who can make three or more chosen-plaintext queries. (In other words, AES is secure for up to two queries—but no more!)

Design an encryption scheme (E, D) that is IND-CCA2 secure and INT-CTXT secure, under this assumption. Your scheme should have a single 128-bit key and should be able to process variable-length messages. Try to avoid an unreasonable loss of security or unreasonably poor performance. Avoid making any other unproven assumptions.

You should: (a) specify your encryption scheme E and decryption scheme D; (b) state and prove a security theorem which shows (E, D) is (t, q_s, q_v, ϵ)-IND-CCA2 secure for some value of (t, q_s, q_v, ϵ) that you should specify; (c) state and prove a security theorem which shows (E, D) is $(t', q'_s, q'_v, \epsilon')$-INT-CTXT secure for some value of $(t', q'_s, q'_v, \epsilon')$ that you should specify; (d) quantify the running time performance by providing an estimate of the number of AES operations performed per 128 bits of plaintext.

3 Short Answer: A CBC-MAC Variant

Definition: Say that $H : \mathcal{K} \times \mathcal{M} \to \mathcal{S}$ is *ϵ-weakly 2-universal* if $\Pr[K \xleftarrow{\$} \mathcal{K}; H_K(x) = H_K(x')] \le \epsilon$ for all $x, x' \in \mathcal{M}$ with $x \ne x'$.

Fill in the blanks to make each of the following statements true, and provide a one- or two-line justification of the key idea behind a proof of the statement. (No need to write down a proof of the statement; just the key insight. Try to make the security parameters as tight as possible.)

(a) If $F : \mathcal{K} \times \mathcal{M} \to \mathcal{S}$ is a (t, q, ϵ)-PRF, then $H : \mathcal{K} \times (\mathcal{M} \times \mathcal{S}) \to \mathcal{S}$ defined by $H_k(x, y) = F_k(x) \oplus y$ is $\underline{\ ?\ }$-weakly 2-universal.

(b) If H is ϵ-weakly 2-universal and F is a (t, q, ϵ')-PRF, then F' defined by $F_{k,k'}(x) = F_k(H_{k'}(x))$ is a $(\underline{\ ?\ }, \underline{\ ?\ }, \underline{\ ?\ })$-PRF.

(c) Fix $n > 0$. Define the function $F : \{0,1\}^{128n} \times \{0,1\}^{128n} \to \{0,1\}^{128}$ by $F_K(M) = X_n$, where $X_0 = 0$, $X_i = \mathrm{AES}_{K_i}(X_{i-1} \oplus M_i)$, $K = (K_1, \ldots, K_n)$, and $M = (M_1, \ldots, M_n)$. If AES is a (t, q, ϵ)-PRF, then F is a $(\underline{\ ?\ }, \underline{\ ?\ }, \underline{\ ?\ })$-PRF.

(d) The scheme in part (c) requires a $128n$-bit key. How could you augment it to work with a 128-bit key, without relying on any other unproven assumptions and without complicating the security proof too much?

4 Short Answer: PRGs

For each of the following statements, say whether the claim is true or false. If true, provide a one- or two-line justification of the key idea behind a proof of the statement. If false, provide a one- or two-line sketch of a counterexample.

(a) True or false: If G is a secure PRG, then H given by $H(k) = (G(k), G(k \oplus 1))$ is a secure PRG.

(b) True or false: If G is a secure PRG, then F given by $F_k(x) = G(k||x)$ is a secure PRF, where $k||x$ denotes the concatenation of k and x.

5 Short Answer: Reaction Attacks

Let (E, D) be a symmetric-key encryption scheme. Define V by

$$V_k(c) = \begin{cases} \text{false} & \text{if } D_k(c) = \perp \\ \text{true} & \text{otherwise.} \end{cases}$$

Say that (E, D) is (t, q_s, q_v, ϵ)-*secure against reaction attacks* if, for all adversaries A running in time t and making at most q_s queries to their first oracle and at most q_v queries to their second oracle, we have

$$\left| \Pr[K \xleftarrow{\$} \mathcal{K}; A^{E_K, V_K} = 1] - \Pr[K \xleftarrow{\$} \mathcal{K}; A^{E_K \circ \$, V_K} = 1] \right| \leq \epsilon.$$

For each of the following statements, say whether the claim is true or false. If true, provide a one- or two-line justification of the key idea behind a proof of the statement. If false, provide a one- or two-line sketch of a counterexample.

(a) True or false: If (E, D) is IND-CPA secure, then (E, D) is secure against reaction attacks.

(b) True or false: If (E, D) is IND-CCA2 secure, then (E, D) is secure against reaction attacks.