ECS 227 — Modern Cryptography — Winter 2014

Phillip Rogaway

Out: Wednesday, 19 February 2014.
Due: Monday, 5 March 2014.

1. Consider the following variant of the CBC MAC, intended to allow one to MAC messages of arbitrary length. The construction uses a blockcipher $E\colon \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$, which you should assume to be secure in the sense of a PRP. The domain for the MAC is $(\{0,1\}^n)^+$. To MAC a message M under key $K1 \parallel K2$, where $|K1| = \kappa$ and $|K2| = n$, first compute the "ordinary" CBC MAC of M, keyed by $K1$, and then xor into the result the key $K2$. Show that this MAC is completely insecure: break it (getting advantage of about 1) by a simple adversary that asks a constant number of queries.

2. Let $F\colon \mathcal{K} \times \{0,1\}^* \to \{0,1\}^n$ be a secure but slow and inherently serial MAC: a hardware engine you have to compute F takes t microseconds to MAC a t-byte string. You have a petabyte (10^{15}) of data you need to MAC. On the back of a paper napkin you estimate that your MAC engine will need about 30 years to do its job.

   Fortunately, your boss offers to let you have more MAC engines for computing F—as many as you need. Develop and analyze a way to use them to MAC your data in a reasonable amount of time. Your method should give a provably secure MAC if F is a good MAC. Don't use any cryptographic functionality other than F itself.

3. Let $h\colon \{0,1\}^* \to \{0,1\}^n$ be a collision-intractable hash function. Which of the following functions will be as well? Convincingly explain all answers. Where appropriate, make your reason a counterexample.

   (a) $H(x) = h(h(x))$

   (b) $H(x) = h(0 \parallel x) \parallel h(1 \parallel x)$

   (c) $H(x) = h(0 \parallel x) \oplus h(1 \parallel x)$

   (d) $H(x) = h(x[1..|x|-1])$

   (e) $H(x) = h(x)[1..n-1]$

4. Formalize and prove the following claim: *nonce-based authenticated encryption implies nonce-based indistinguishability under a CCA.*