0368.4162: Introduction to Cryptography, Fall 2008 Instructor: Ran Canetti

Problem Set 3

December 31, 2008 Due: Thursday January 15 12:00pm

1. **[30 points]** For each one of the following MAC schemes, either prove that they are secure (in the sense defined in class, namely EU-CMA), or provide a counter example to their security. In all schemes the verification algorithm works by re-computing the tag and comparing to the received tag: $VER(k, m, t)$ =accept iff $AUTH(k, m) = t$.

   (a) Let (ENC, DEC) be an IND-CPA-secure encryption scheme. Then $AUTH(k, m) = m, ENC(k, m)$.

   (b) Let $H = \{H^n\}_{n\in\mathbf{N}}$, $H^n = \{H_k : \{0,1\}^* \to \{0,1\}^n\}_{k\in\{0,1\}^n}$ be a CRF ensemble. Then, $AUTH(k, m) = m, H_k(m)$. (Note that here k is secret, whereas H is designed to be collision resistant even when k is public.)

   (c) Let $F = \{F^n\}_{n\in\mathbf{N}}$, $F^n = \{F_k : \{0,1\}^* \to \{0,1\}^n\}_{k\in\{0,1\}^n}$ be a PRF ensemble, and let f be a one way function. Then, $AUTH(k, m) = m, f(F_k(m))$.

2. **[30 points]** Let $F = \{F^n\}_{n\in\mathbf{N}}$, $F^n = \{F_k : \{0,1\}^{2n} \to \{0,1\}^{2n}\}_{k\in\{0,1\}^n}$ be a PRP ensemble. Consider the following shared key encryption scheme for message space $M_n = \{0,1\}^n$:

   - For $m \in \{0,1\}^n$, $ENC(k, m) = f_k(m \circ r)$, where $r \leftarrow U_n$. (Here $\circ$ denotes concatenation.)
   - $DEC(k, c)$ outputs the first n bits of $f_k^{-1}(c)$.

   Is (ENC, DEC) IND-CPA secure, with respect to message space M and leakage function $l(m) = |n|$? Either prove based on the assumption that the underlying ensemble F is a PRF, or provide a counter example.

3. **[40 points]** Let $H = \{H^n\}_{n\in\mathbf{N}}$, $H^n = \{H_h : \{0,1\}^* \to \{0,1\}^n\}_{h\in\{0,1\}^n}$ be a function ensemble. Say that H is target collision resistant (TCR) if any polytime adversary A wins in the following game only with negligible probability (in n):

   - h is chosen at random from $\{0,1\}^n$

   - A gets h, generates m

   - A gets r chosen at random from $\{0,1\}^n$

   - A generates m', r' and wins if $H_h(m, r) = H_h(m', r')$.

   (a) Show that if there exist TCRs then there exist TCRs which are not CRFs.

   (b) Let $S = (GEN, SIG, VER)$ be a signature scheme that's EU-CMA secure when applies to messages of fixed length n. Consider the following scheme $S' = (GEN', SIG', VER')$:

   - GEN' runs GEN, and in addition chooses $h \in \{0,1\}^n$ and adds h to both the signing key and the verification key.
   - $SIG'((sk, h), m) = SIG(sk, h(m, r)), r$. Here $r \leftarrow \{0,1\}^n$ and sk is the signing key of SIG.
   - $VER'((vk, h), m, (s, r)) = VER(vk, H_h(m, r), s)$. Here vk is the verification key of VER.

   Show that S' is EU-CMA secure for messages with arbitrary length.

   Direction: Note that the security of S' depends on two primitives: the EU-CMA unforgeable scheme S and the TCR ensemble H. One way to handle this situation is to first reduce the security of S to that of S', under the assumption that the TCR never breaks, and then bound the probability that the TCR breaks. To do that, you need to precisely specify the meaning of the "CTR never breaks" event. (This is not the only way to go about this proof, but it might be the simplest.)

4. **[Bonus: 30 points]** Consider the following signature scheme $S = (GEN, SIG, VER)$. The scheme uses a trapdoor permutation ensemble $\{P^n\}_{n\in\mathbf{N}}$, where for each value of n, $P^n = \{P_i : \{0,1\}^{2n} \to \{0,1\}^{2n}\}_{i\in I_n}$, and a collision resistant function ensemble $\{H^n\}_{n\in\mathbf{N}}$ where for each value of n, $H^n = \{H_h : \{0,1\}^* \to \{0,1\}^n\}_{h\in I_n}$. The scheme proceeds as follows:

   - Algorithm GEN runs the index generation algorithms of P and H and obtains an index i and a trapdoor t for P, and an index h for H. Then GEN outputs verification key (i, h) and signature key (t, h).
   - $SIG(t, h, m) = P_i^{-1}(H_h(m) \circ h)$. (Here t is used to invert P_i.)
   - $VER(i, h, m, s)$ =accept iff $H_h(m) \circ h = P_i(s)$.

   Show that for any collision resistant function ensemble H there exists a trapdoor permutation ensemble P such that the above scheme is *not* EU-CMA.

   Remark: The above scheme is a variant on the "hash and invert" paradigm that we discussed in class, and is intended to demonstrate the inherent unsoundness of this paradigm. Note however that this scheme differs from the original "hash and invert" scheme, in that index h is given to the trapdoor permutation. I don't know how to prove above statement with respect to the original scheme. An idea on how to do it would be nice (even beyond points in the homework), since it would further demonstrate the unsoundness of the "hash and invert" paradigm in general.