Homework 3

05 November 2018

1 Message Authentication Codes (MAC) (20 points)

1. Consider the following fixed-length MAC for messages of length $\ell(n) = 2n - 2$ using a pseudorandom function $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$:

   $\underline{\mathsf{MAC}(k, m)}$

   - Parse $m = m_0||m_1$.
   - Output $t = F_k(0\|m_0)\|F_k(1\|m_1)$

   Is this a secure MAC? Prove your answer.

2. Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom function. Consider the following MAC algorithm:

   $\underline{\mathsf{MAC}(k, m)}$

   - Parse $m = m_1\| \cdots \|m_\ell$ where $m_i \in \{0,1\}^{n/2}$.
   - Choose $r \leftarrow \{0,1\}^n$ at random,
   - Compute $t := F_k(r) \oplus F_k(\langle 1\rangle\|m_1) \oplus \cdots \oplus F_k(\langle \ell\rangle\|m_\ell)$ where $\langle i\rangle$ is the $n/2$-bit encoding of the integer i.
   - Output (r, t).

   Is this a secure MAC? Prove your answer.

2 Hash Function (40 points)

For each of the following modifications to the Merkle-Damgaard transform (see the construction 5.3 in the textbook), determine whether the result is collision-resistant. If yes, provide a proof; If not, give a concrete attack.

3) (**20 points**) Modify the construction so that the first block is set as $z_0 := B$, z_i is computed as $z_i := h_s(z_{i-1} \| x_i)$ for $i = 1, \cdots, B$ and the final output is z_B.

4) (**20 points**) Modify the construction so that we just start the computation from x_1 instead of using an IV. Namely, we define $z_1 := x_1$ and then compute $z_i = h_s(z_{i-1} \| x_i)$ for $i = 2, \cdots, B+1$, and output z_{B+1} as the digest.

3 Digital Signatures (40 points)

Let f be a one-way permutation. Consider the following signature scheme for messages in the set $\{1, \ldots, n\}$:

- To generate keys, choose uniform $x \in \{0,1\}^n$ and set $y := f^{(n)}(x)$ (where $f^{(i)}(\cdot)$ refers to the i-fold iteration of f, and $f^{(0)}(x) \stackrel{\mathsf{def}}{=} x$). The public key is y and the private key is x.
- To sign message $i \in \{1, \ldots, n\}$, output $f^{(n-i)}(x)$.
- To verify signature σ on message i with respect to public key y, check whether $y \stackrel{?}{=} f^{(i)}(\sigma)$

5) (**15 points**) Show that the above is not a one-time-secure signature scheme. Given a signature on a message i, for what messages j can an adversary output a forgery.

6) (**25 points**) Prove that no PPT adversary given a signature on i can output a forgery on any message $j > i$, except with negligible probability. *Hint.* For this proof you need to show a reduction to the security of the underlying one-way function (we did a similar proof in class and you can read it in Chapter 12.6.1, Theorem 12.16 of Introduction to Modern Cryptography.) Start by assuming that you have a PPT adversary $\mathsf{A}_{\mathsf{forge}}$ that on input y and (i, σ_i), outputs a forgery for $j > i$. You should use this adversary to construct an adversary $\mathsf{A}_{\mathsf{owf}}$ to break the one-wayness of f (namely, that inverts an output z that she received from an oracle).