HIT — Cryptography — Homework 4

September 26, 2014

Problem 1. Let F be a pseudorandom function. Show that the following MAC for messages of length $2n$ is insecure: The shared key is a random $k \in \{0,1\}^n$. To authenticate a message $m_1 \| m_2$ with $|m_1| = |m_2| = n$, compute the tag $\langle F_k(m_1), F_k(F_k(m_2)) \rangle$.

Problem 2. Let (Gen, H) be a collision-resistant hash function. Is $(\mathsf{Gen}, \hat{H})$ defined by $(\hat{H}^s(x) \stackrel{\text{def}}{=} H^s(H^s(x))$ necessarily collision resistant? Prove your answer.

Problem 3. For each of following modifications to the Merkle-Damgård transform, determine whether the result is collision resistant or not. If yes, provide a proof; if not, demonstrate an attack. Hint: you may use two facts on hash function: (1) $h(x) = x$ is collision resistant. Although x is leaked, there is no collision. (2) A crhf h can be constructed from another crhf g by letting $h(x) = x\|0$ for $x = 0$ and letting $h(x) = g(x)\|1$ for $x \neq 0$.

1. Modify the construction so that the input length is not included at all (i.e, output z_B and not $z_{B+1} = h^s(z_B \| L)$).
2. Modify the construction so that instead of outputting $z = h^s(z_B \| L)$, the algorithm outputs $z_B \| L$
3. Instead of using an IV, just start the computation from x_1. That is, define $z_1 := x_1$ and then compute $z_i := h^s(z_{i-1} \| x_i)$ for $i = 2, \ldots, B+1$ and output z_{B+1} as before.
4. Instead of using a fixed IV, set $z_0 := L$ and then compute $z_i := h^s(z_{i-1} \| x_i)$ for $i = 1, \ldots, B$ and output z_B.

Problem 4. We have learned that CCA-secure encryption schemes can be constructed by Enc-then-MAC in the class. Is there any other way to achieve CCA-secure scheme but without MAC? For example, (1) do you think the following scheme is CCA-secure? And why?

- message $m \in \{0,1\}^{n/2}$ and key $k \in \{0,1\}^n$. In encryption, choose a random string $r \leftarrow \{0,1\}^{n/2}$ and ciphertext $c := F_k(r \| m)$, where F is a strong PRP.

Furthermore, no matter what is your answer to the above question, (2) do you think CCA-security implies secure Authenticated Encryption (A.E.)? And why?

Problem 5. Show a message transmission scheme that achieves authentication communication (with integrity and authenticity) but is not a secure A.E (without confidentiality).