Problem Set 4 Solutions

Problem 1. [30 points] Define the family of functions $H\colon \{0,1\}^{64} \times \{0,1\}^{192} \to \{0,1\}^{128}$ as follows:

function $H_K(x)$ // $|K| = 64$ and $|x| = 192$
  Let a be the first 64 bits of x and b the rest // $|a| = 64$ and $|b| = 128$
  $y \leftarrow \mathsf{AES}_{K \,\|\, a}(b)$ // Apply AES with 128-bit key $K \,\|\, a$ and input b to get output y
  return y

Show that H is not collision-resistant by presenting a practical adversary A such that $\mathbf{Adv}^{\mathrm{cr}}_{H}(A)$ is close to one. (The better the attack, the more points you get.)

The first thing to do is look at the definition of collision-resistance. The game shows us that the adversary gets as input the randomly chosen key K defining the particular instance H_K of the family H that it is attacking. Now we use the fact that AES is a block cipher and thus given $K \,\|\, a_1$ one can easily compute $\mathsf{AES}^{-1}_{K \,\|\, a_1}$. The adversary with input the key K proceeds as follows:

adversary A
  Let a_1, a_2 be two different 64-bit strings and let b_1 be any 128-bit string
  $h \leftarrow \mathsf{AES}_{K \,\|\, a_1}(b_1)$; $b_2 \leftarrow \mathsf{AES}^{-1}_{K \,\|\, a_2}(h)$
  $x_1 \leftarrow a_1 \,\|\, b_1$; $x_2 \leftarrow a_2 \,\|\, b_2$
  return x_1, x_2

This adversary is very practical, using only two AES or AES^{-1} computations. We claim that the x_1, x_2 it returns is a collision for H_K, which means that $\mathbf{Adv}^{\mathrm{cr}}_{H}(A) = 1$. The claim is true because

$$\mathsf{AES}_{K \,\|\, a_2}(b_2) \;=\; \mathsf{AES}_{K \,\|\, a_2}(\mathsf{AES}^{-1}_{K \,\|\, a_2}(h)) \;=\; h \;=\; \mathsf{AES}_{K \,\|\, a_1}(b_1) \,,$$

and also a_1, a_2 being different implies $x_1 \neq x_2$.

Problem 2. [40 points] Let $h\colon \mathcal{K} \times \{0,1\}^{2b} \to \{0,1\}^{b}$ be a compression function. Define $H\colon \mathcal{K} \times \{0,1\}^{4b} \to \{0,1\}^{b}$ as follows:

function $H(K, M)$
  Break M into $2b$-bit blocks, $M = M_1 \,\|\, M_2$
  $V_1 \leftarrow h(K, M_1)$; $V_2 \leftarrow h(K, M_2)$
  $V \leftarrow h(K, V_1 \,\|\, V_2)$
  return V

Adversary $A_h(K)$

  Run $A_H(K)$ to get its output (y_1, y_2)
  Parse y_1 as $M_{1,1} \| M_{1,2}$ where $|M_{1,1}| = |M_{1,2}| = 2b$
  Parse y_2 as $M_{2,1} \| M_{2,2}$ where $|M_{2,1}| = |M_{2,2}| = 2b$
  $V_{1,1} \leftarrow h(K, M_{1,1})$; $V_{1,2} \leftarrow h(K, M_{1,2})$
  $V_{2,1} \leftarrow h(K, M_{2,1})$; $V_{2,2} \leftarrow h(K, M_{2,2})$
  $V_1 \leftarrow h(K, V_{1,1} \| V_{1,2})$
  $V_2 \leftarrow h(K, V_{2,1} \| V_{2,2})$
  If ($V_1 \neq V_2$ OR $y_1 = y_2$) return FAIL   // A_H did not find a collision, so neither will A_h
  If $V_{1,1} \| V_{1,2} \neq V_{2,1} \| V_{2,2}$ then return $(V_{1,1} \| V_{1,2}, V_{2,1} \| V_{2,2})$
  If $M_{1,1} \neq M_{2,1}$ then return $(M_{1,1}, M_{2,1})$
  If $M_{1,2} \neq M_{2,2}$ then return $(M_{1,2}, M_{2,2})$

Figure 1: Adversary A_h for the proof of the theorem.

Show that if h is collision-resistant then so is H. Do this by stating and proving an analogue of Theorem 6.8 in the course notes.

Theorem: Let h, H be as above. Suppose we are given an adversary A_H that attempts to find collisions in H. Then we can construct an adversary A_h that attempts to find collisions in h, and

$$\mathbf{Adv}_H^{\mathrm{cr}}(A_H) \ \leq \ \mathbf{Adv}_h^{\mathrm{cr}}(A_h) \ . \tag{1}$$

Furthermore, the running time of A_h is that of A_H plus the time to perform 6 computations of h. ▮

This theorem says that if h is collision-resistant then so is H. Why? Let A_H be a practical adversary attacking H. Then A_h is also practical, because its running time is that of A_H plus a little more, namely the time for 6 computations of h. But h is collision-resistant so we know that $\mathbf{Adv}_h^{\mathrm{cr}}(A_h)$ is low. Equation (1) then tells us that $\mathbf{Adv}_H^{\mathrm{cr}}(A_H)$ is low, meaning H is collision-resistant as well.

Proof of theorem: We follow the proof of Theorem 6.8 in the notes. Adversary A_h, taking input a key $K \in \mathcal{K}$, is depicted in Fig. 1. It runs A_H on input K to get a pair (y_1, y_2) of messages, each $4b$ bits long. We claim that if y_1, y_2 is a collision for H_K then A_h will return a collision for h_K.

Adversary A_h computes $V_1 = H_K(y_1)$ and $V_2 = H_K(y_2)$. If y_1, y_2 is a collision for H_K then we know that $V_1 = V_2$. Let us assume this. Now, let us look at the inputs to the application of h_K that yielded these outputs. These are $V_{1,1} \| V_{1,2}$ and $V_{2,1} \| V_{2,2}$. If these inputs are different, they form a collision for h_K, and A_h outputs them.

If they are not different then we know that $V_{1,1} = V_{2,1}$ and $V_{1,2} = V_{2,2}$. That $V_{1,1} = V_{2,1}$ means that $h(K, M_{1,1}) = h(K, M_{2,1})$. So $M_{1,1}, M_{2,1}$ form a collision for h unless they happen to be equal. Similarly, that $V_{1,2} = V_{2,2}$ means that $h(K, M_{1,2}) = h(K, M_{2,2})$ and so $M_{1,2}, M_{2,2}$ form a collision for h unless they happen to be equal. Adversary A_h checks for these equalities and returns an unequal pair. The key point is that we cannot have *both* $M_{1,1} = M_{2,1}$ and $M_{1,2} = M_{2,2}$ since that would imply $y_1 = y_2$, but we know that $y_1 \neq y_2$ because it is a collision for H_K. ▮

Problem 3. **[50 points]** Let $\mathsf{sha1}\colon \{0,1\}^{672} \to \{0,1\}^{160}$ be the compression function underlying the $\mathsf{SHA1}$ hash function. We define a message authentication scheme $\Pi = (\mathcal{K}, \mathrm{MAC}, \mathrm{VF})$ as follows. The key generation algorithm returns a random 160 bit string as the key K, and the tagging and verifying algorithms are:

Algorithm $\mathrm{MAC}_K(M)$	Algorithm $\mathrm{VF}_K(M, \sigma)$
Divide M into 512 bit blocks, $M = M[1] \ldots M[n]$	If $\sigma = \mathrm{MAC}_K(M)$ then return 1
$C[0] \leftarrow K$	Else return 0
For $i = 1, \ldots, n$ do	
$C[i] \leftarrow \mathsf{sha1}(C[i-1] \parallel M[i])$	
EndFor	
Return $C[n]$	

The message space is the set of all strings whose length is a positive multiple of 512.

Present a practical chosen-message attack that succeeds in forgery using one query to the tagging oracle.

Adversary $A(K)$
$x \leftarrow 0^{512}$
$y \leftarrow \mathbf{Tag}(x)$
$T \leftarrow \mathsf{sha1}(y \parallel 1^{512})$
return $(0^{512} \parallel 1^{512}, T)$

We have

$$\begin{aligned} y &= \mathsf{sha1}(K \parallel 0^{512}) \\ T &= \mathsf{sha1}(y \parallel 1^{512}) \\ &= \mathrm{MAC}_K(0^{512} \parallel 1^{512}) \end{aligned}$$

So $\mathbf{Adv}_{\Pi}^{\text{uf-cma}}(A) = 1$.