Cryptography, winter term 16/17:
Sample solution to assignment 6

Cornelius Brand, Marc Roth

Exercise 6.1 (Be nice to yourselves, Knowledge) Refresh your knowledge about basic group theory by reading Chapter 8.1 in the book.

Exercise 6.2 (Be nice to your tutors and TAs, 1 Bonus Point) Write the name and matriculation number of every author as well as number, time slot and the name of the tutor of your tutorial group on the first page of your solution. Furthermore write in english and staple *all* sheets of your solution.

Exercise 6.3 (Canonical Verification, 5 Points) Let $\Pi = (\text{Gen}, \text{Mac}, \text{Vrfy})$ be a secure MAC that uses *canonical verification*. Prove that Π is a strong MAC.

Solution 6.3 (Canonical Verification, 5 Points) If Π uses canonical verification then Mac is deterministic. The only difference in the experiments $\text{Mac} - \text{forge}$ and $\text{Mac} - \text{sforge}$ is that, on output (m, t), the first one checks in the end whether m was already queried, whereas the latter checks whether m was already queried and additionally the result of the query was t. As Mac is deterministic we have that the query of any message m results in a unique tag t, i.e. m was already queried if and only if m was already queried and the output tag was t. Therefore, the experiments are equivalent for MACs that use canonical verification which implies that a secure MAC that uses canonical verification is also a strong secure MAC.

Exercise 6.4 (MACs, 6 Points) Let F be a PRF. Show that each of the following MACs is insecure, even if used to authenticate fixed-length messages. (In each case Gen outputs a uniform $k \in \{0,1\}^n$ and $[i]_2$ denotes the $\frac{n}{2}$-bit binary encoding of i.)

(a) To authenticate a message $m = m_1 \dots m_\ell$, where $m_i \in \{0,1\}^n$, compute

$$t := F_k(m_1) \oplus \cdots \oplus F_k(m_\ell)$$

(b) To authenticate a message $m = m_1 \dots m_\ell$, where $m_i \in \{0,1\}^{\frac{n}{2}}$, compute

$$t := F_k([1]_2 || m_1) \oplus \cdots \oplus F_k([\ell]_2 || m_\ell)$$

(c) To authenticate a message $m = m_1 \dots m_\ell$, where $m_i \in \{0,1\}^{\frac{n}{2}}$, choose uniform $r \leftarrow \{0,1\}$. and compute

$$t := (r, F_k(r) \oplus F_k([1]_2 || m_1) \oplus \cdots \oplus F_k([\ell]_2 || m_\ell))$$

Solution 6.4 (MACs, 6 Points) We construct and adversary $\mathcal{A}$ for each of the MACs.

(a) On input 1^n $\mathcal{A}$ queries (0^n1^n) and gets $t = \text{Mac}_k(0^n1^n) = F_k(0^n) \oplus F_k(1^n)$. Now $\mathcal{A}$ outputs $(1^n0^n, t)$. This is a valid message-tag pair as $\text{Mac}_k(1^n0^n) = F_k(1^n) \oplus F_k(0^n) = F_k(0^n) \oplus F_k(1^n) = t$, i.e. $\mathcal{A}$ wins with probability 1.

(b) On input 1^n $\mathcal{A}$ queries $m_0 = 0^n$, $m_1 = 0^{\frac{n}{2}}1^{\frac{n}{2}}$ and $m_2 = 1^n$. We denote the tags as t_0, t_1 and t_2. Now it holds that

$$\begin{aligned}
&t_0 \oplus t_1 \oplus t_2 \\
=&(F_k([1]||0^{\frac{n}{2}}) \oplus F_k([2]||0^{\frac{n}{2}})) \oplus (F_k([1]||0^{\frac{n}{2}}) \oplus F_k([2]||1^{\frac{n}{2}})) \oplus (F_k([1]||1^{\frac{n}{2}}) \oplus F_k([2]||1^{\frac{n}{2}})) \\
=&F_k([2]||0^{\frac{n}{2}}) \oplus F_k([1]||1^{\frac{n}{2}}) \\
=&F_k([1]||1^{\frac{n}{2}}) \oplus F_k([2]||0^{\frac{n}{2}}) \\
=&\text{Mac}_k(1^{\frac{n}{2}}0^{\frac{n}{2}})
\end{aligned}$$

Therefore, $\mathcal{A}$ outputs $(1^{\frac{n}{2}}0^{\frac{n}{2}}, t_0 \oplus t_1 \oplus t_2)$ and wins with probability 1.

(c) Let $m \in \{0,1\}^{\frac{n}{2}}$ be an arbitrary message. Then $\mathcal{A}$ outputs $(m, ([1]_2||m, 0^n))$. This is a valid message-tag pair as Mac_k could choose $r = [1]_2||m$ and output

$$t = (r, F_k(r) \oplus F_k([1]_2||m)) = (r, 0^n)$$

Consequently, $\mathcal{A}$ wins with probability 1.

Exercise 6.5 (Hash Functions, 5 Points) Let $\Pi = (\text{Gen}, H)$ be a collision resistant hash function and define the hash function $\hat{\Pi} := (\text{Gen}, \hat{H})$ such that

$$\hat{H}^s(x) := H^s(H^s(x)) \,.$$

Prove or disprove: $\hat{\Pi}$ is a collision resistant hash function.

Solution 6.5 (Hash Functions, 5 Points) $\hat{\Pi}$ is a collision resistant hash function. We will prove this by reduction, i.e. we assume that $\hat{\Pi}$ is not collision resistant and show that this would imply that Π is not collision resistant.
If $\hat{\Pi}$ is not collision resistant, then there is a ppt adversary $\hat{\mathcal{A}}$ such that

$$\Pr[\text{Hash} - \text{col}_{\hat{\mathcal{A}},\hat{\Pi}}(n) = 1] > \frac{1}{q(n)}$$

We use $\hat{\mathcal{A}}$ to construct $\mathcal{A}$ as follows:
On input s, $\mathcal{A}$ simulates $\hat{\mathcal{A}}$. The latter will output x, x' eventually. Now $\mathcal{A}$ checks whether $\hat{H}^s(x) = \hat{H}^s(x')$ and $x \neq x'$. If this is not the case $\mathcal{A}$ will just output x and x' (we do not care about this case). Otherwise $\mathcal{A}$ checks wether $H^s(x) = H^s(x')$. If this is the case, then a collision was found and $\mathcal{A}$ outputs x and x'. Otherwise we know that $H^s(x) \neq H^s(x')$ and $H^s(H^s(x)) = H^s(H^s(x'))$, that is, a collision is found, too. $\mathcal{A}$ outputs $H^s(x)$ and $H^s(x')$ in this case.

For the analysis let $\mathrm{Succ}_{\hat{\mathcal{A}}}(n)$ be the event that $\hat{\mathcal{A}}$ finds a collision in the execution of the $\mathrm{Hash}-\mathrm{col}$ experiment with adversary $\mathcal{A}$ on input n. Clearly we have

$$\Pr[\mathrm{Succ}_{\hat{\mathcal{A}}}(n)] = \Pr[\mathrm{Hash}-\mathrm{col}_{\hat{\mathcal{A}},\hat{\Pi}}(n) = 1] > \frac{1}{q(n)}\,.$$

Furthermore the case analysis above shows that

$$\Pr[\mathrm{Hash}-\mathrm{col}_{\mathcal{A},\Pi}(n) = 1 \mid \mathrm{Succ}_{\hat{\mathcal{A}}}(n)] = 1\,.$$

Putting everything together and by applying the law of total probability we get

$$\begin{aligned}
&\Pr[\mathrm{Hash}-\mathrm{col}_{\mathcal{A},\Pi}(n) = 1]\\
=&\Pr[\mathrm{Hash}-\mathrm{col}_{\mathcal{A},\Pi}(n) = 1 \mid \mathrm{Succ}_{\hat{\mathcal{A}}}(n)] \cdot \Pr[\mathrm{Succ}_{\hat{\mathcal{A}}}(n)]\\
+&\Pr[\mathrm{Hash}-\mathrm{col}_{\mathcal{A},\Pi}(n) = 1 \mid \neg\mathrm{Succ}_{\hat{\mathcal{A}}}(n)] \cdot \Pr[\neg\mathrm{Succ}_{\hat{\mathcal{A}}}(n)]\\
\geq&\Pr[\mathrm{Hash}-\mathrm{col}_{\mathcal{A},\Pi}(n) = 1 \mid \mathrm{Succ}_{\hat{\mathcal{A}}}(n)] \cdot \Pr[\mathrm{Succ}_{\hat{\mathcal{A}}}(n)]\\
=&1 \cdot \Pr[\mathrm{Succ}_{\hat{\mathcal{A}}}(n)]\\
>&\frac{1}{q(n)}
\end{aligned}$$

This completes the reduction as Π is a collision resistant hash function. Therefore our assumption was wrong and $\hat{\Pi}$ is indeed collision resistant.