TD 5 – Message authentication codes

Exercise 1. *Insecure MACs*

Let E_k be block cipher of block length λ. Prove in the two cases that however good is the block cipher, the resulting MAC is insecure.

1. $\mathsf{Mac}_k(m_1\|\cdots\|m_\ell) = E_k(m_1 \oplus \cdots \oplus m_\ell)$. *Hint. One query is sufficient.*

2. $\mathsf{Mac}_k(m_1\|\cdots\|m_\ell) = E_k(m_1) \oplus \cdots \oplus E_k(m_\ell)$.

Exercise 2. *SuffixMAC*

Let $H : \{0,1\}^* \to \{0,1\}^n$ be a Merkle-Damgård hash function, built from a compression function $f : \{0,1\}^n \times \{0,1\}^w \to \{0,1\}^n$. Let F be the iterated compression function such that $H(m) = F(\text{pad}(m))$ where $\text{pad}(m) = m\|\text{pad}_{|m|}$. Define $\mathsf{SuffixMac}_H : \{0,1\}^\kappa \times \{0,1\}^* \to \{0,1\}^n$ by $\mathsf{SuffixMac}_H(k,m) = H(m\|k)$.

1. **i.** What is the (generic) complexity of finding a collision $F(m) = F(m')$?

ii. Does the complexity changes if one requires m and m' to be of the same length $\ell > n$?

2. Let $m \neq m'$ of a same length kw, such that $F(m) = F(m')$.

i. Give an existential forgery attack for $\mathsf{SuffixMac}_H$ with one query.

ii. What is the total cost of the attack, including the computation of m and m'?

iii. Is the attack interesting if $\kappa = n/2$? And if $\kappa = n$?

Exercise 3. *GMAC security*

Recall that $\mathsf{GMac}_{k_1\|k_2}(m) = (r, m(k_1) + E_{k_2}(r))$ where $r \twoheadleftarrow \{0,1\}^{128}$, E is a block cipher with block size 128 and $m(k)$ is defined as follows: k is viewed as an element of $\mathbb{F}_{2^{128}}$, $m \in \{0,1\}^*$ is split into 128-bit blocks $m_0, \dots, m_{\ell-1}$ viewed as elements of $\mathbb{F}_{2^{128}}$, and $m(k) = m_0k + m_1k^2 + \cdots m_{\ell-1}k^\ell$.

We aim to prove that GMAC satisfies the *strong* EUF-CMA security.[1] It is defined using the EUF-CMA game: The adversary makes queries $m^1, \dots, m^q$, gets valid tags $t^1, \dots, t^q$ and must output a valid pair $(m,t) \neq (m^i, t^i)$ for $1 \leq i \leq q$. (*It may output $m = m^i$ for some i as long as $t \neq t^i$.*)

[1] Strong existential unforgeability under chosen message attack.

Let $(m,(r,s))$ be the pair output by the adversary. The goal is to bound the probability that (r,s) is a valid tag for m, in the *ideal block cipher model*: E_{k_2} is replaced by a random function $f : \{0,1\}^{128} \to \{0,1\}^{128}$ in GMAC.

1. Intuitively, why is the advantage of an adversary almost the same with a good block cipher E or a random function f?

Let C be the event "$\exists i \neq j, r^i = r^j$", N be the event "$\forall i,\ r \neq r^i$" and V be the event "$(m,(r,s))$ is a valid pair."

2. *(optional)* Prove that $\Pr[V] \leq \Pr[C] + \Pr[V|N] + \Pr[V|\neg C \wedge \neg N]$.
   Hint. True for any events V, C, N using twice the law of total probability.
3. Give an upper bound on $\Pr[C]$.
4. Prove that $\Pr[V|N] \leq 2^{-128}$. *Hint. Translate* $\Pr[V|N]$ *into plain English.*
5. We now bound $\Pr[V|\neg C \wedge \neg N]$. We assume that $\neg C \wedge \neg N$ holds.
   - **i.** Translate $\Pr[V|\neg C \wedge \neg N]$ into plain English.
   - **ii.** Prove that the adversary learns no information on k_1 from its queries.
   - **iii.** Prove that there exists i such that (r,s) is a valid tag for m if and only if $m(k) - m^i(k) = s - s^i$.
   - **iv.** Prove that $\Pr[V|\neg C \wedge \neg N] \leq L/2^{135}$ where L is the largest length amongst $|m|$, $|m^1|, \ldots, |m^q|$.
6. Conclude on the maximal advantage of an adversary, independently of its running time.