TD 5 – Message authentication codes and authenticated encryption

Exercise 1. $\mathsf{Suffix-MAC}$

Let $H:\{0,1\}^*\to\{0,1\}^n$ be a Merkle-Damgård hash function. 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 for (m,m') for H?
   ii. Does the complexity changes if one requires m and m' to be of the same length $\ell>n$?
2. Let (m,m') be a colliding pair for H, with m and m' having the same length.
   i. Give an existential forgery attack for $\mathsf{SuffixMac}_H$ with query cost 1.
   ii. What is the total cost of the attack, if one has to compute (m,m')?
   iii. Is the attack interesting if $\kappa=n/2$? And if $\kappa=n$?

Exercise 2. GMAC *security*

The goal of this exercise is to study the security of the message authentication code GMAC.
In the following we identify 128-bit strings with elements of the finite field with 2^{128} elements $\mathbb{F}_{2^{128}}$. For $m\in\{0,1\}^*$, write $m=m_0\|\cdots\|m_{\ell-1}$ where each m_i has 128 bits. (We ignore the need for some padding if $m_{\ell-1}$ is shorter.) For any $k\in\{0,1\}^{128}$, we write $m(k)=m_0k+m_1k^2+\cdots+m_{\ell-1}k^\ell$ where the computation is done in $\mathbb{F}_{2^{128}}$.
Let E be a block cipher with block size 128. Let $\mathsf{GMac}_{k_1\|k_2}(m)=(r,m(k_1)+E_{k_2}(r))$ where $r\twoheadleftarrow\{0,1\}^{128}$. We defined the "*strong* universal unforgeability under chosen message attack experiment" $\mathsf{Exp}^{\mathsf{sEUF-CMA}}_{\mathsf{GMac}}(A)$: The challenger draws a random key $k=k_1\|k_2$; The adversary queries q messages $m_1,\dots,m_q$ and gets corresponding valid tags $t_i=(r_i,s_i)$; Then, the adversary must output a message m with a valid tag $t=(r,s)$ where $(m,t)\notin\{(m_1,t_1),\dots,(m_q,t_q)\}$. The result of the experiment is 1 if the pair is valid, and 0 otherwise. *Note that the adversary can output a pair (m,t) where $m=m_i$ for some i, but then t must be different from t_i.*
Our goal is to upper bound the advantage of an adversary A in $\mathsf{Exp}^{\mathsf{sEUF-CMA}}_{\mathsf{GMac}}(A)$.

1. **i.** Assume there exists $i\neq j$ s.t. $r_i=r_j$. Prove that the adversary can compute a (small) set of possible values k_1, and output a valid pair $(m,(r,s))$ with good probability.
   ii. Let R be the event "the values of r_i are not pairwise distinct." Give an upper bound for $\Pr[R]$.

In the rest of the exercise, we replace E_{k_2} in GMac by a random function f from $\{0,1\}^{128}$ to itself.

2. Intuitively, why is the advantage of an adversary almost the same with a good block cipher E or a random function f?
3. Let $(m,(r,s))$ be the pair output by the adversary. Let S (*success*) be the event "$\mathsf{Exp}^{\mathsf{sEUF-CMA}}_{\mathsf{GMac}}(A)=1$" and N be the event "$r\neq r_i$ for all i."
   i. Prove that $\Pr[S]\le\Pr[R]+\Pr[S|N]+\Pr[S|\neg R\wedge\neg N]$. *This is true for any event S, R, N.*
   ii. Prove that $\Pr[S|N]\le 2^{-128}$. *Translate* $\Pr[S|N]$ *into plain English.*
4. We now bound $\Pr[S|\neg R\wedge\neg N]$. We assume that $\neg R\wedge\neg N$ holds.
   i. Translate $\Pr[S|\neg R\wedge\neg N]$ in plain English.
   ii. Prove that the adversary does not learn any 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. Deduce that $\Pr[S|\neg R\wedge\neg N]\le\ell/2^{135}$ where ℓ is the maximal bitlength of m and the m_i's.
5. Conclude on the maximal advantage of an adversary, independently of its running time.