1 Secure MACs

Let \((S, V)\) be a secure MAC defined over \((K, M, T)\) where \(M = \{0, 1\}^n\) and \(T = \{0, 1\}^{128}\). Which of the following is a secure MAC:

- \(S'(k, m) = (t, t)\) where \(t = S(k, m)\) and
  \[
  V(k, m, (t_1, t_2)) = \begin{cases} 
  V(k, m, t_1) & \text{if } t_1 = t_2 \\
  0 & \text{otherwise}
  \end{cases}
  \]

- \(S'(k, m) = S(k, m)\) and \(V'(k, m, t) = V(k, m, t) \lor V(k, m \oplus 1^n, t)\)

- \(S'(k, m) = S(k, m)\) and
  \[
  V'(k, m, t) = \begin{cases} 
  V(k, m, t) & \text{if } m \neq 0^n \\
  1 & \text{otherwise}
  \end{cases}
  \]

- \(S'(k, m) = S(k, m)[0, \ldots, 126]\) and \(V'(k, m, t) = V(k, m, t|0) \lor V(k, m, t|1)\)

- \(S'(k, m) = S(k, m \oplus 1^n)\) and \(V'(k, m, t) = V(k, m \oplus 1^n, t)\)

2 Insecure ECBC-MAC with random IV

The ECBC-MAC uses a fixed IV. In the circuit below, the IV is simply set to 0^n.
Suppose that we choose instead a random IV for each message and include it as part of the tag. More precisely, let \( S(k, m) = (r, \text{ECBC}_r((k, k_1), m)) \) where \( \text{ECBC}_r((k, k_1), m) \) refers to the ECBC-function with \( IV = r \) in the circuit below.

The resulting MAC is insecure. An attacker queries for the tag of a one-block message \( m_0 \) and obtains the tag \((r, t)\). Show that he can forge a tag for the one-block message \( 0^n \).

### 3 Collison resistance

Assume \( H_1 \) and \( H_2 \) are collision resistant hash functions mapping inputs in \( \mathcal{M} \) to \( \{0, 1\}^{256} \). We seek to prove that the concatenation \( H_2(H_1(\cdot)) \) is also collision resistant. To this end, we prove the contra-positive: suppose \( H_2(H_1(\cdot)) \) is not collision-resistant, i.e., there exist \( x \neq y \) such that \( H_2(H_1(x)) = H_2(H_1(y)) \).

We now construct a collision for either \( H_1 \) or \( H_2 \), which implies that \( H_2(H_1(\cdot)) \) must collision resistant.

Which of the following statements is true:

- either \( x \) and \( y \) are a collision of \( H_1 \) or \( H_1(x) \) and \( H_1(y) \) are a collision for \( H_2 \)
- either \( x \) and \( H_1(y) \) are a collision of \( H_2 \) or \( H_2(x) \) and \( y \) are a collision for \( H_1 \)
- either \( x \) and \( y \) are a collision of \( H_1 \) or \( x \) and \( y \) are a collision for \( H_2 \)
- either \( H_2(x) \) and \( H_2(y) \) are a collision of \( H_1 \) or \( x \) and \( y \) are a collision for \( H_2 \)

### 4 Triple collision

Let \( H : \mathcal{M} \to \mathcal{T} \) be a random hash function with \( |\mathcal{M}| \gg |\mathcal{T}| \). We proved that that a collision can be found by taking \( O(\sqrt{|\mathcal{T}|}) \) random samples of \( H \).

How many samples would it take until we obtain a triple collision, i.e., three distinct strings \( x, y, z \) such that \( H(x) = H(y) = H(z) \). Provide a detailed proof.
5 MAC from symmetric encryption

Let \((E, D)\) be a symmetric encryption system where the message space \(M\) consists of short messages of length, say, 32 bytes. Define the following MAC \((S, V)\) for messages in \(M\):

\[
S(k, m) = E(k, m) \quad \text{and} \quad V(k, m, t) = \begin{cases} 
1 & \text{if } D(k, t) = m \\
0 & \text{otherwise}
\end{cases}
\]

Which property should the encryption scheme \((E, D)\) satisfy to ensure that the resulting MAC is secure:

- semantic security under a chosen plaintext attack
- authenticated encryption
- perfect security