CS171 HW5

Q1. For Scheme 1: (i) A queries $m = M_0 || M_1$ and receives $t = F_k(m_0) || F_k(m_0 \oplus m_1)$
(ii) A queries $m' = m_1 || M_2$ and receives $t' = F_k(m_1) || F_k(m_1 \oplus m_2)$
(iii) A sends $m^* = m_1 || m_0$ and $t^* = F_k(m_1) || F_k(m_0 \oplus m_1)$
where $F_k(m_1)$ is the 1st n bits of t' and $F_k(m_0 \oplus m_1)$ is the last n bits of t

For Scheme 2: (i) A queries $m_{01} = m_0 || m_1$ and retrieves $t_{01}' = F_k(r) \oplus F_k(0||m_0) \oplus F_k(1||m_1)$
(ii) A queries $m_{00} = m_0 || m_0$ and retrieves $t_{00}' = F_k(r) \oplus F_k(0||m_0) \oplus F_k(1||m_0)$
(iii) A queries $m_{11} = m_1 || m_1$ and retrieves $t_{11}' = F_k(r) \oplus F_k(0||m_1) \oplus F_k(1||m_1)$
(iv) A sends $m^* = m_1 || m_0$ and $t^* = r || t_{01}' \oplus t_{00}' \oplus t_{11}'$ where r is retrieved from any of t_{01} & t_{00} & t_{11}, and $t_{01}' \oplus t_{00}' \oplus t_{11}' = F_k(r) \oplus F_k(0||m_1) \oplus F_k(1||m_0)$

Q2. (1) We construct Mac':
① $Gen'(1^n) := Gen(1^n)$
② $Mac'(k,m)$: output $t' = Mac(k,m) || LSB(Mac(k,m))$ where $LSB(x)$ is the least significant bit of the output of x
③ $Vrfy'(k,m,t)$: Let $t = t_0' || b$ where $t_0' \in \{0,1\}^{n-1}$ & $b \in \{0,1\}$. Output 1 if $t_0' = Mac(k,m)$ and output 0 otherwise.

(2) If there exists adversary A that breaks Mac' then adversary B can use A to break Mac:
(i) When A outputs a query m_i for the $Mac'(k,\cdot)$ oracle, B forwards m_i to its oracle for $Mac(k,\cdot)$ and sends $Mac(k,\cdot) || LSB(Mac(k,\cdot))$ to A
(ii) In the end when A outputs (m^*, t^*), B removes the last bit of t^* and denote it $t^*_{truncated}$. B outputs $(m^*, t^*_{truncated})$

(3) Since Mac' is only unforgeable, adversary A can possibly obtain t' for the same c, which (c, t') would pass the oracle for CCA which would output m_b, giving A the probability of 1 of breaking CCA security.

Q3. (1b) $\begin{cases} r = F(K_1, m) \\ t = MAC_R(r; K_2, m) \end{cases}$

(2b) Assume toward contradiction that adversary A can distinguish between Hyb 0 and Hyb 1 with non-negligible advantage, We can then construct B from A to distinguish between PRF F and the random function R with non-negligible advantage.

B is constructed:

(i) B receives a function G which is either F_K or R, but it doesn't know.

(ii) B runs A, simulating the MAC oracle using G in place of F in Hyb 0 and R in Hyb 1: When A makes a query on m, B provides the tag computed using G(m)

(iii) Whenever A determines that it is interacting with Hyb_0, B determines that it is interacting with F_K, vice-versa

(2c) $Pr[Hyb_1 \to 1] = 2^{-l}$ since R is truly random

∴ Prove by reduction to R

(2d) $Pr[Hyb_0 \to 1] \leq negl$

∴ MAC security game $MAC\text{-}forge_{A,\Pi_D}(n)$ is not breakable

∴ Π_0 is a secure MAC