Cipher block chaining MAC (CBC-MAC)

Using the tag t_1 obtained in MAC we apply F_{k_2} on t_1 · "$F_{k_2}(t_1)$".

valid tag of m

$m_2 = m_1 \| t_1 \oplus m_1, \boxed{t_2}$

$F_k(l)$ is a truly random and secure.

∴ Adversary 'A' cannot distinguish b/w $F_k(t)$ and message m.