CBC-MAC

Tag obtained from normal MAC is as long as the message. In order to use reduced tags, we can use the CBC-MAC.

m is first encrypted in CBC mode and the last output is considered the tag.

Basic CBC-MAC is secure if fixed length input is allowed. For variable length, it becomes insecure.

Example:- If we allow messages of length 1 and 2.

m_1, tag $\rightarrow t_1$

Let $m_2 = m_1 \| t_1 \oplus m_1$, tag $\rightarrow t_2$

t_2 is also a valid tag of m which hasn't been queried yet because

$$t_2 = F_k\left(\overbrace{F_k(0^n \oplus m_1)}^{t_1} \oplus t_1 \oplus m\right)$$

$$= F_k(t_1 \oplus t_1 \oplus m)$$

$$= F_k(m) = F_k(0^n \oplus m)$$

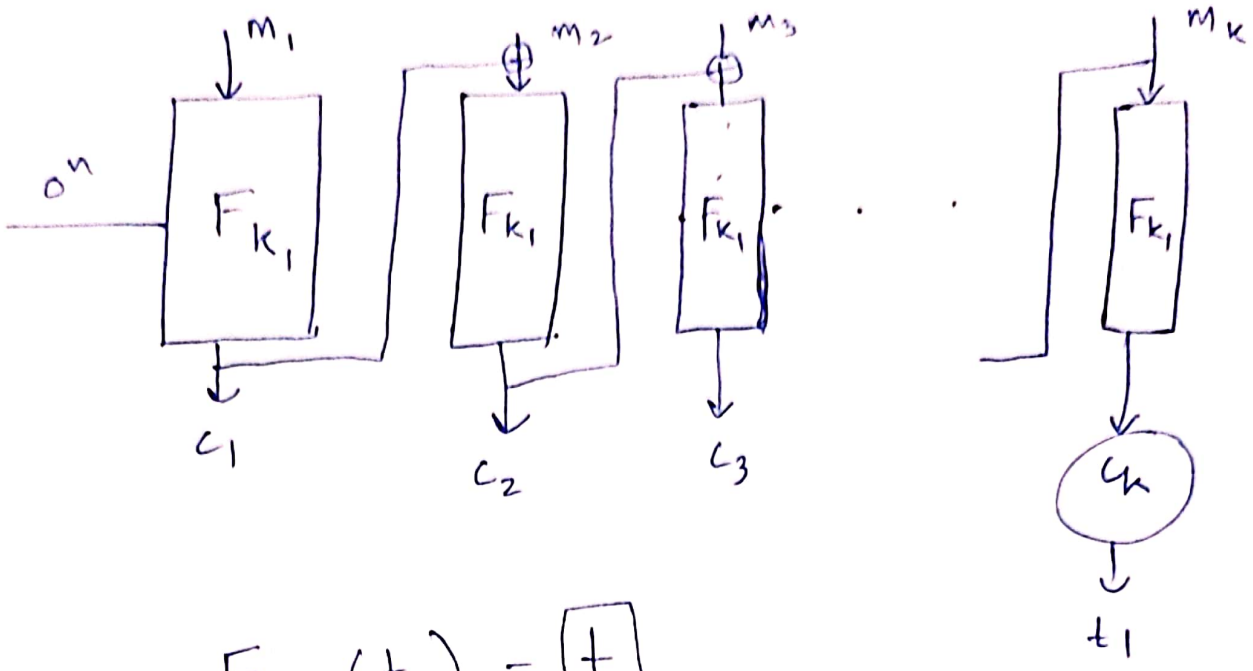
Hence, the tag obtained from CBC-MAC is passed through MAC again to make it secure.

Use 2 keys k_1, k_2

k_1 to obtain t_1 from basic CBC-MAC

Final: $t = F_{k_2}(t_1)$

Secure CBC-MAC :



$$F_{k_2}(t_1) = \boxed{t}$$

Previously discussed attacks are not possible in this situation because k_1, k_2 are secret and F is a pseudo-random function. Hence, it is practically impossible to get t_1 from t without k_2.