MAC.

Construction: $m \in \{0,1\}^*$

we divide the message m into d blocks, each of size $n/4$.

$\Rightarrow m = m_1, m_2, m_3, m_4 \ldots\ldots m_d$

generate tags t_i for each block,

for $i = 1$ to d:

$t_i = F_k(r \| d \| i \| m_i)$

return $\langle r, t_1, t_2 \ldots\ldots, t_d \rangle$

$r \rightarrow n/4$ bit length encoded random seed

$d \rightarrow n/4$ bit length encoded (number of blocks)

$i \rightarrow n/4$ bit length, message specifier

$m_i \rightarrow n/4$ bit length message-block.

MAC is secure if,

$Pr(V(\langle m, t \rangle) | m \notin Q) \leq negl(n)$

or we could say that a non-queried tag matches with queried tag.

Proof of security

We then have the following ↓

Case I: r is re-used

The following cases arise depending on the length of messages. Consider messages m and m'. Then,

① $len(m) = len(m')$

where $m \notin Q$ → set of already queried messages

and $m' \& Q$ → this message isn't yet queried.

and $m \neq m'$

$\Rightarrow$ m and m' differ atleast one block m_i.

$\Rightarrow m_i \neq m_i'$

$\because$ the input seed, $input_1 = r \| d \| i \| m_i$

$input_2 = r \| d \| i \| m_i'$

$\} \; input_1 \neq input_2$

$\Rightarrow F_k(input_1) \neq F_k(input_2)$

$\because F_k(input_1) = F_k(input_2) \leq negl(n)$.

$\Rightarrow \because$ if the $m' \& Q$ → the tag t' generated would've been generated before

$\Rightarrow t'$ is not known.

② $len(m) \neq len(m')$

again 2 cases arise,

ⓐ $d \neq d'$ (number of blocks differ).

$t_i = F_k(r \| d \| i \| m_i)$

$t_i' = F_k(r \| d' \| i \| m_i')$

$\} \; P(t_i = t_i') \leq negl(n)$ [PRF].

$\Rightarrow \because$ if the $m' \& Q$ → the tag t' generated would've been generated before

$\Rightarrow t'$ is not known.

(b) $d = d'$

↳ This case could arise when, padding of $1(0)^*$ is applied to one of the blocks to make it multiple of $n/4$.

(1) $m' =$ prefix (m)
or
$m =$ prefix (m')

⇒ The last message block varies because of the padding

∵ the PRF output will vary greatly.

∴ tag t' of m' cannot be known if m' wasn't yet queried

(2) otherwise,

atleast one-block of the messages differ and thus The case (I.1) follows.

Case II: r is not re-used

∵ the input seed, $\text{input}_1 = r \| d \| i \| m_i$
$\text{input}_2 = r' \| d \| i \| m_i'$

$\left.\begin{array}{l} \text{input}_1 \neq \text{input}_2 \\ \Rightarrow F_k(\text{input}_1) \neq F_k(\text{input}_2) \end{array}\right\}$

∵ $F_k(\text{input}_1) = F_k(\text{input}_2) \leq \text{negl}(n)$.

⇒ ∴ if the m' & Θ ⇒ the tag t' generated wouldn't have been generated before ⇒ t' is not known.

Hence, the given construction is provably secure.