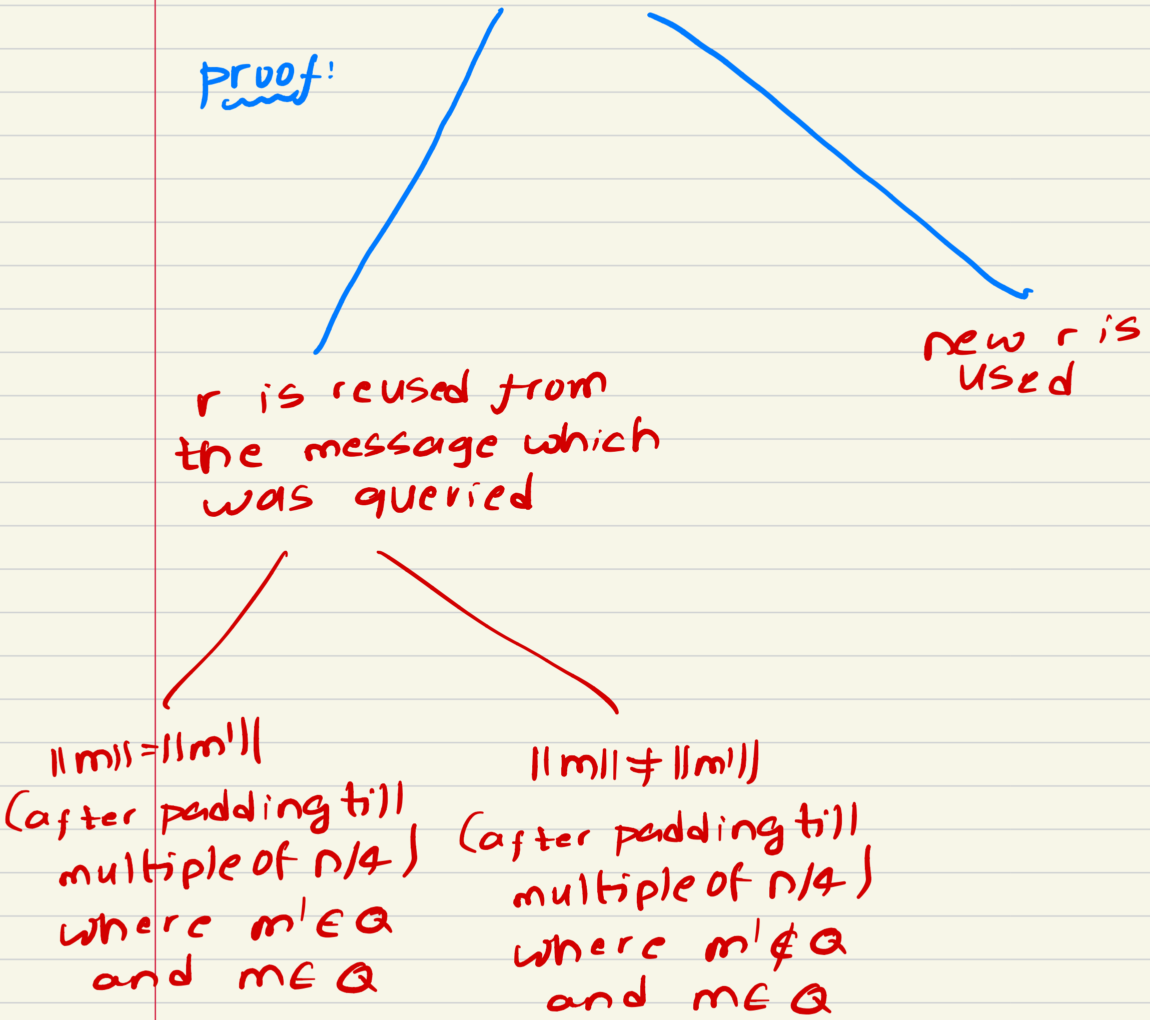
To prove,

$$\Pr(\mathrm{Vrfy}(\langle m, t\rangle) ; \text{ st } m \notin Q) \leq \mathrm{negl}(n)$$



Proof:

r is reused from the message which was queried

new r is used

$\|m\| = \|m'\|$ (after padding till multiple of $n/4$) where $m' \in Q$ and $m \in Q$

$\|m\| \neq \|m'\|$ (after padding till multiple of $n/4$) where $m' \notin Q$ and $m \in Q$

$||m|| = ||m'||$
(after padding till
multiple of $n/4$)
where $m' \in Q$
and $m \in Q$:

$m \neq m' \Rightarrow$ there exists a message block $i$ for which $m_i \neq m_i'$.

now, $t_i = F_K(r||d||i||m_i)$, $t_i' = F_K(r||d||i||m_i')$

since $m'$ is never queried we have no way to know $t_i'$.

Assuming $F_K$ is provably secure PRF

$\Rightarrow Pr(t_i \neq t_i') \leq negl(n)$

$||m|| \neq ||m'||$

(after padding till multiple of $n/4$)
where $m' \notin Q$
and $m \in Q$

Let the length of $m'$ be $l'$,

|||y Here we dont know the value

$t' = F(r||d'||\cdots)$, $t = E(r||d||\cdots)$

Assuming $F_K$ is provably secure PRF

$\Rightarrow$ $Pr(t = t') \leq negl(n)$

New $r$ is used

Let the length of $m'$ be $l'$,

|||y, Here we don't have the value,

$t' = F(r'||\cdots)$
$t = F(r||\cdots)$

Assuming $F_k$ is provably secure PRF

→ $Pr(t = t') \leq negl(n)$