$$Pr(Vrfy(<m,t>); stm \notin Q) \leq negl(n)$$

1 Proof

Case 1 : r is reused from the message which was queried

In this case, we consider two subcases:

Case 1.1$\|\text{m}\| = \|\text{m}'\|$ (after padding till multiple of n/4) where $m' \notin Q$ and $m \in Q$

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

now $ti = F_k\left(r\|d\|i\|m_i\right)$, $t_i' = F_k\left(r\|d\| \mid i\|m_i'\right)$

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

Assuming F_k is provably secure PRF $\implies Pr\left(t_i = t_i'\right) \leq negl(n)$

This means that m and m' have the same length after padding to a multiple of $n/4$. We can assume that $m \neq m'$ because otherwise, the statement we are trying to prove is vacuously true.

Since m' has not been queried, we have no way of knowing t_i' for any block i. However, we do know that $t_i = F_k(r|d|i|m_i)$ where d is the number of blocks in m. If F_k is a provably secure PRF, then we can assume that the probability of $t_i = t_i'$ is negligible.

Case 1.2$\|\text{ m}\| \neq \|\text{m}'\|$ ((after padding till multiple of n/4)) where $m' \notin Q$ and $m \in Q$

Let the d$'$ be the no. of block is m$'$

Similarly Here we dont know the value

$t' = F\left(r\ \|d'\| \ldots\right.$

$t = F(r\|d\| \ldots$

Assuming F_k is provably secure PRF $\implies Pr\left(t = t'\right) \leq negl(n)$ This means that m and m' have different lengths after padding to a multiple of $n/4$. We can assume that $m \neq m'$ because otherwise, the statement we are trying to prove is vacuously true.

As in Case 1.1, we have no way of knowing t' for any block i in m'. However, we do know that $t_i = F_k(r|d|i|m_i)$ and $t_i' = F_k(r'|d'|i|m_i')$. Since r and r' are independent and chosen uniformly at random, we can assume that the probability of $t = t'$ is negligible if F_k is a provably secure PRF.

2 Case 2: new r is used

Let the length of m ' be I'

similarly Here we dont know the value

$t' = F\left(r'\| \ldots\right.$

$t = F(r\| \ldots$

Assuming F_k is provably secure PRF $\implies Pr\left(t = t'\right) \leq negl(n)$

In this case, r is chosen uniformly at random and independent of any previous values of r. We again have no way of knowing t' for any block i in m', but we do know that $t_i = F_k(r|d|i|m_i)$ and $t'_i = F_k(r'|d'|i|m'_i)$. As in Case 1.2, we can assume that the probability of $t = t'$ is negligible if F_k is a provably secure PRF.

Therefore, in all cases, we can assume that the probability of a successful verification of a signature on a message that has not been previously queried is negligible, and the statement we set out to prove is true