

$m, H(m), \sigma, n, \Sigma, H$

C

S

$H(m), i$

$\sigma, H(T'), M$

