A
channel
B
M_1
||
K_s
||
H
K_s
M_1
||
H
compare
$H(M_1||K_S)$