Hashing resistente a colisiones

Una función hash sin clave resistente a colisiones es un mapa H: M→T de un mensaje largo M a un espacio digest T pequeño de tal forma que encontrar dos mensajes m0 y m1 con el mismo digest H(m0) = H(m1) es difícil. Una función resistente a colisiones H es un lossy compressor que asigna una huella t a un mensaje m. Si tenemos I=(S,V) que es un MAC seguro y H es resistente a colisiones, le MAC derivado: I' = (S',V'):

$S'(k,m) = S(k,H(m))$ → $V'(k,H(m))$

es un MAC seguro.