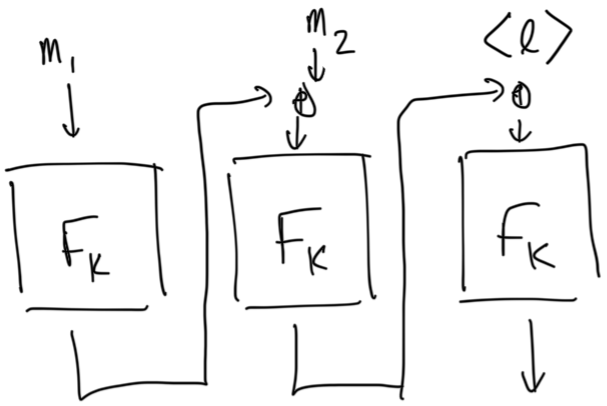
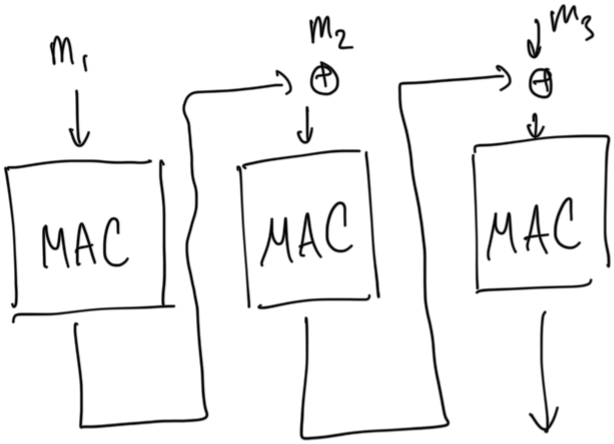
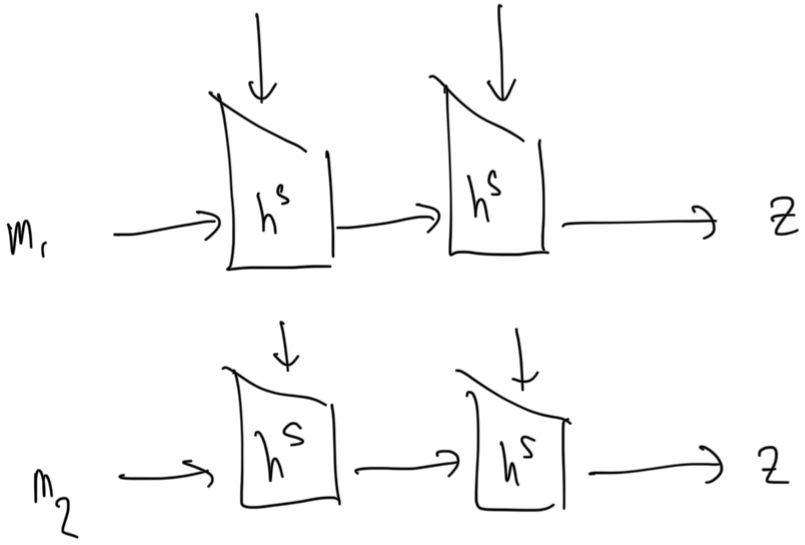


128+3 binary string for 133

~~Secure~~ modification of CBC-MAC



Consider a MAC that leaks inf. about its input



Are there collisions on h^s that wouldn't help you find collisions on MD.

"Helpful collisions" are collisions for which the input to the collisia is in the image of h^s.

Can you construct h^s that has collisions, but no helpful collisions.