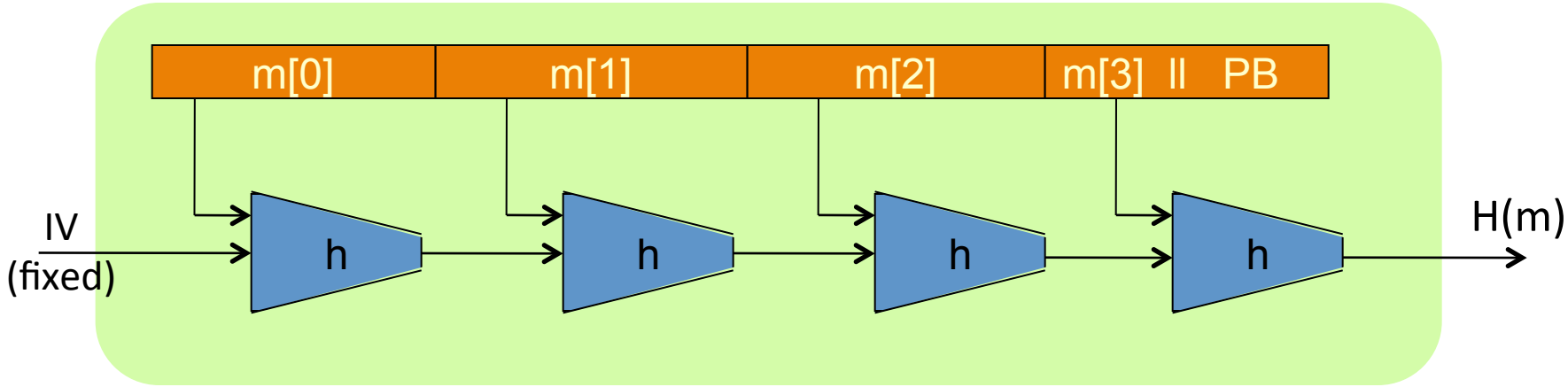
Collision resistance

HMAC:

a MAC from SHA-256

The Merkle-Damgard iterated construction



Thm: h collision resistant ⇒ H collision resistant

Can we use H(.) to directly build a MAC?

MAC from a Merkle-Damgard Hash Function

H: $X^{\leq L} \longrightarrow T$ a C.R. Merkle-Damgard Hash Function

<u>Attempt #1</u>: **S(k, m) = H(k || m)**

This MAC is insecure because:

- Given H(k || m) can compute H(w || k || m || PB) for any w.
- Given H(k || m) can compute H(k || m || w) for any w.
- Given H(k || m) can compute H(k || m || PB || w) for any w.
- Anyone can compute H(k || m) for any m.

Standardized method: HMAC (Hash-MAC)

Most widely used MAC on the Internet.

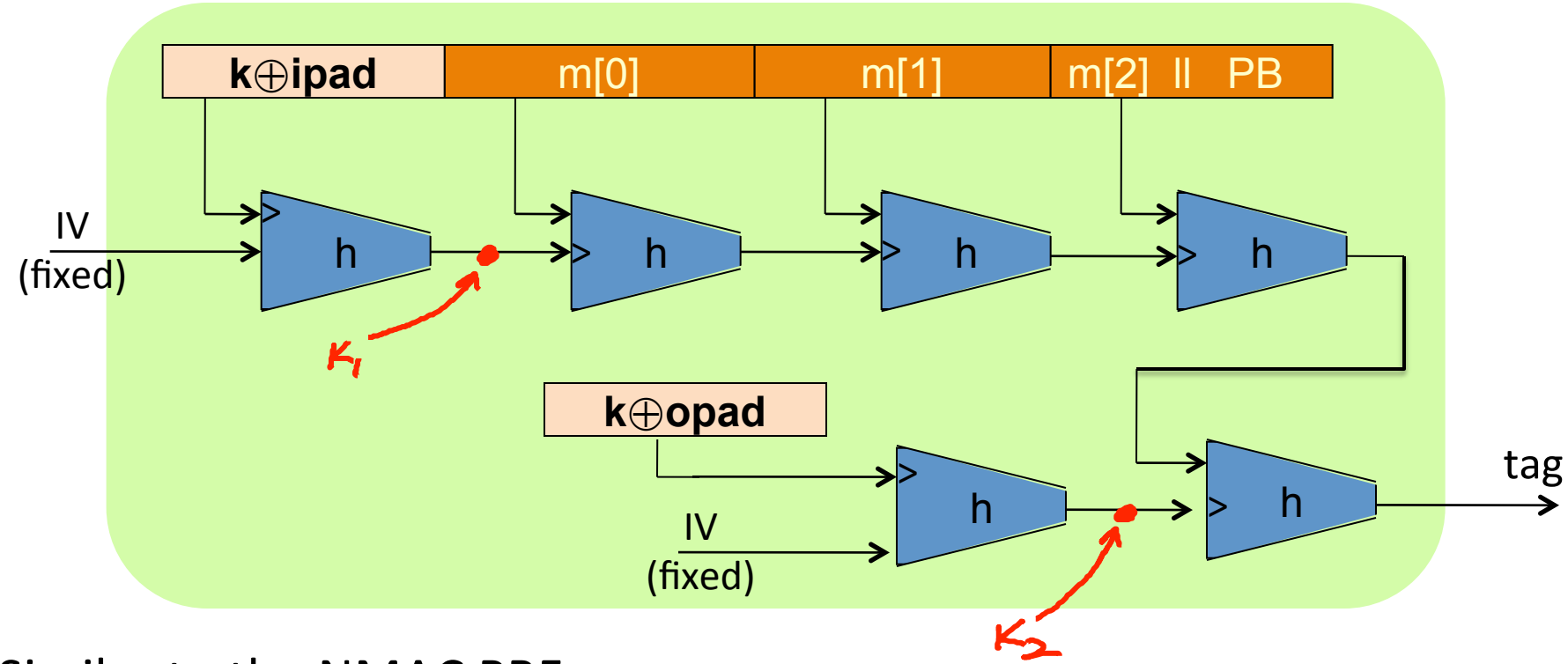
H: hash function.

example: SHA-256 ; output is 256 bits

Building a MAC out of a hash function:

HMAC: $S(k, m) = H(k \oplus \text{opad}, \mathbf{H(k \oplus ipad \,||\, m)})$

HMAC in pictures



Similar to the NMAC PRF.

main difference: the two keys k_1, k_2 are dependent

HMAC properties

HMAC is assumed to be a secure PRF

- Can be proven under certain PRF assumptions about h(.,.)
- Security bounds similar to NMAC
  - Need $q^2/|T|$ to be negligible ($q << |T|^{½}$)

In TLS: must support HMAC-SHA1-96

End of Segment