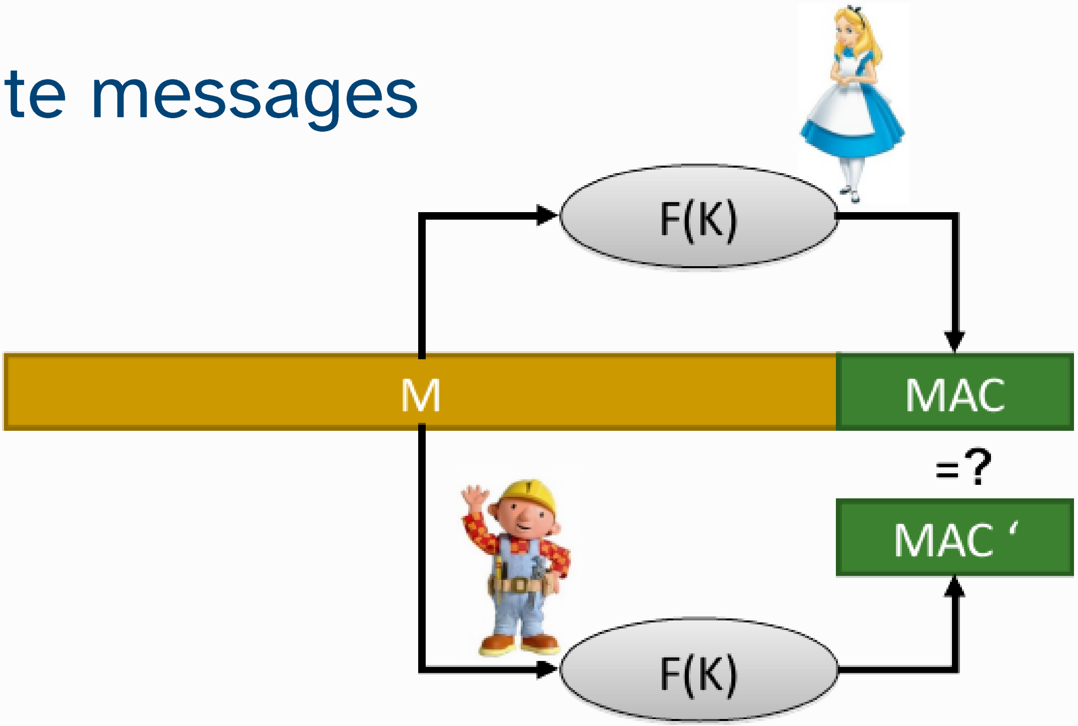
Message Authentication Codes

Message Authentication Code (MAC)

- MIC computed with a key
  - Only key holders can generate/validate the MAC

- Used to authenticate messages
  - M’ = M | MAC(M)



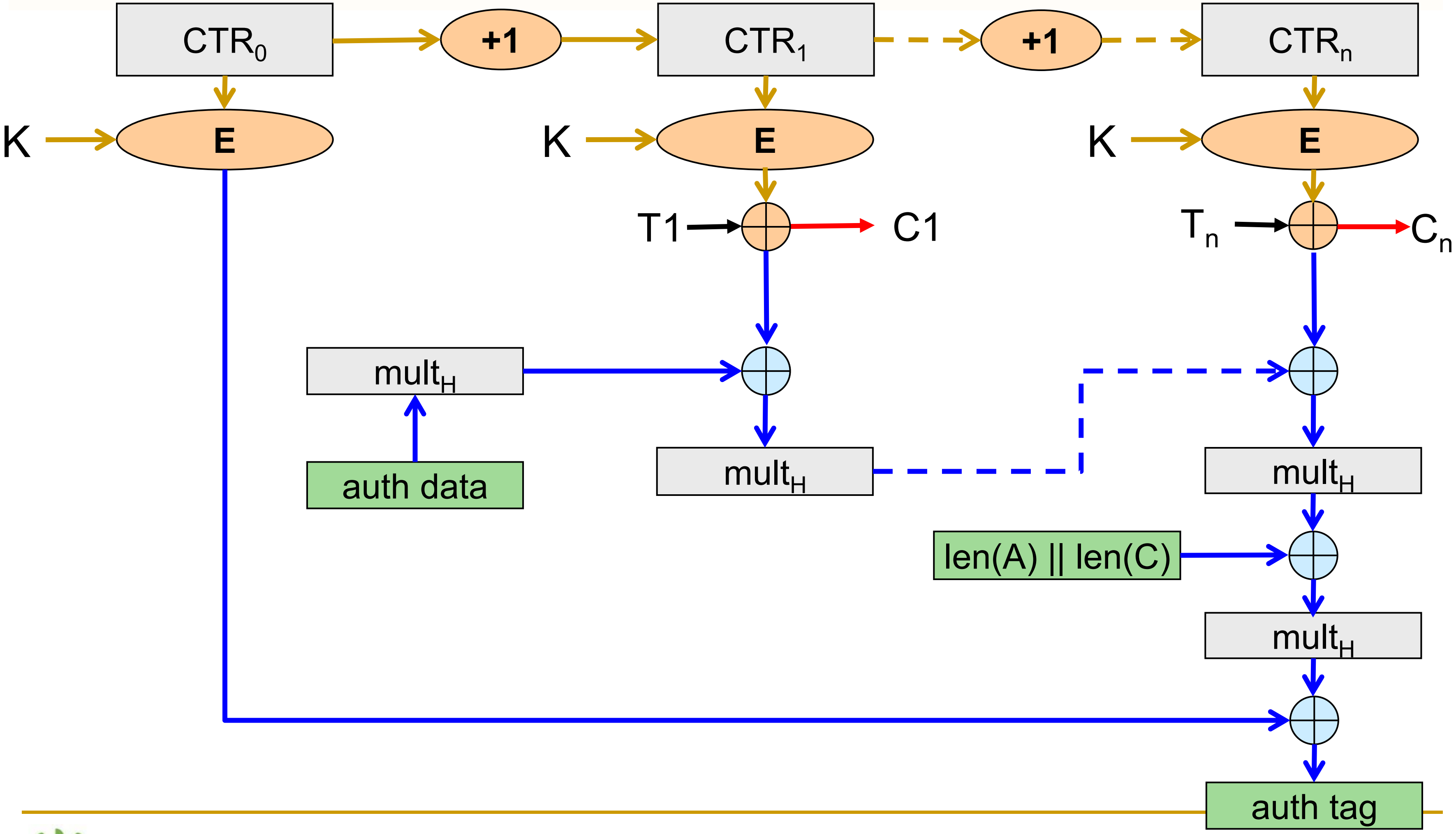
MAC: approaches

- Encryption of an ordinary digest
  - Using, for instance, a symmetric block cipher
- Using encryption with feedback & error propagation
  - CBC-MAC
- Adding a key to the hashed data
  - HMAC (output length depends on the function H used)
    - H(K, opad, H(K, ipad, text))
    - ipad = 0x36 B times opad = 0x5C B times B = size of H input block
      - HMAC-MD5, HMAC-SHA-1, etc.

Encryption + Authentication

- Encrypt-then-MAC: MAC is computed from cryptogram
  - Allows verifying integrity before (the longer) decryption
  - Preferable option
- Encrypt-and-MAC: MAC is computed from plaintext
  - MAC is not encrypted
  - May give information regarding original text (if similar to other)
- MAC-then-Encrypt: MAC is computed from plaintext
  - MAC is encrypted
  - Requires full decryption before MAC is validated

GCM (Galois Counter Mode)



CTR_0
+1
CTR_1
+1
CTR_n
K
E
K
E
K
E
T1
C1
T_n
C_n
$mult_H$
auth data
$mult_H$
$mult_H$
len(A) || len(C)
$mult_H$
auth tag