Authenticated Encryption

Gianluca Dini
Dept. of Ingegneria dell'Informazione
University of Pisa
Emai: gianluca.dini@unipi.it
Version: 14/04/2025

1

Authenticated encryption

HOW TO MIX CIPHERS AND MACS

2

Secrecy and integrity

- We have primitives for secrecy and integrity
  - Secrecy: ciphers
  - Integrity: MAC
- What if we wish to achieve secrecy and integrity at the same time?

3

Encrypt and authenticate (E&M)

- Alice and Bob want to achieve both confidentiality and integrity

k_1 for confidentiality, cypher
k_2 for authenticity via MAC

Alice (k1, k2)
message x
$y = Enc_{k1}(x)$
$t = MAC_{k2}(x)$

---------- [y, t] --------- >

Bob (k1, k2)
$x = Dec_{k1}(y)$
if $V_{k2}(x, t)$ return x
else return «error»

4

Is it secure?

- The tag t might leak information about x
  - Nothing in the definition of security for a MAC implies that it hides information about x
- If the MAC is deterministic (e.g., CBC-MAC and HMAC), then it leaks whether the same message is encrypted twice
  - Traffic analysis
  - Using CBC becomes almost useless

5

Encrypt then authenticate (EtM)

Secure one here!

- Alice and Bob want to achieve confidentiality and integrity

Alice (k1, k2)

x

$y = Enc_{k1}(x)$

$t = MAC_{k2}(y)$

------- [y, t] --- >

Bob (k1, k2)

if ($V_{k2}(y, t)$)
return ($x = D_{k1}(y)$)
else return "error"

6

Security of encrypt then authenticate

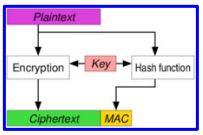
- It can be proved that if Enc is CPA-secure and MAC is secure then:
  - The combination is CPA-secure (encryption must be randomized)
  - The combination is a secure MAC

7

Three different approaches

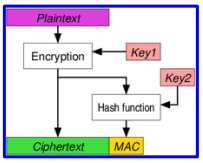
- Encrypt and MAC (E&M)
  - Discouraged
  - SSH

(1st one discussed)



- Encrypt then MAC (EtM)
  - Always correct
  - Ipsec

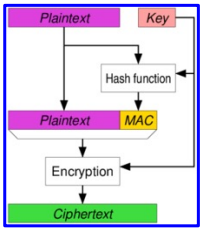
(second one discussed)



- MAC then Encrypt (MtE)
  - correctness depends on Enc-MAC combinations
  - TLS/SSL

3 possibilities

↳ Attach mac to pt and encrypt resulting bundle. (1)



10

(1) Can be proven that security depends on Enc and MAC: MAC contains a cypher and you might have interference between the two cyphers.

Authenticated encryption

AUTHENTICATED ENCRYPTION

Particular encryption mode

11

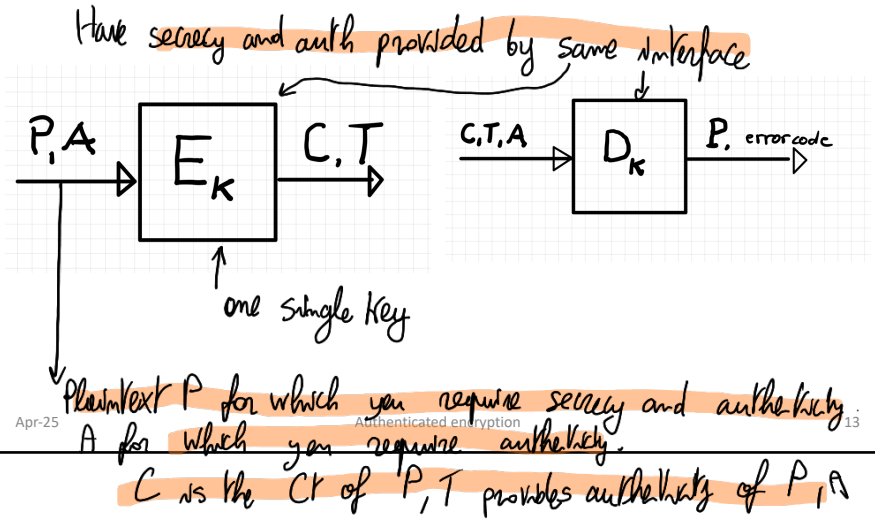
Authenticated Encryption

- Most of applications require *message privacy* and *message authentication*
- Combining privacy and authentication is a challenging task that is rarely done *securely* with *ad-hoc* constructions
- Authenticated Encryption (AE) are *encryption modes* which simultaneously assure the confidentiality and authenticity of data.

12

AE APIs

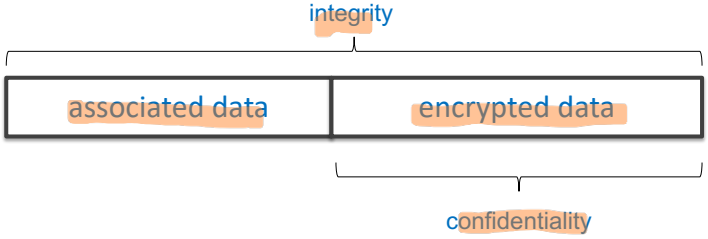
Encryption **Decryption**



13

Authenticated Encryption with Associated Data (AEAD) (Ass. Data: part that is only authenticated)

- AEAD allows checking the integrity of both the encrypted and unencrypted information in a message.
  - E.g., network packets or frames where the header needs visibility, the payload needs confidentiality, and both need integrity and authenticity.



14

Standards and associated data

- NIST
  - CCM: CBC-MAC then CTR mode encryption
    - 802.11i
  - GCM: CTR mode encryption then MAC
    - Very efficient
- IETF
  - EAX: CTR mode encryption than OMAC
- NIST and IETF standards support AEAD

15

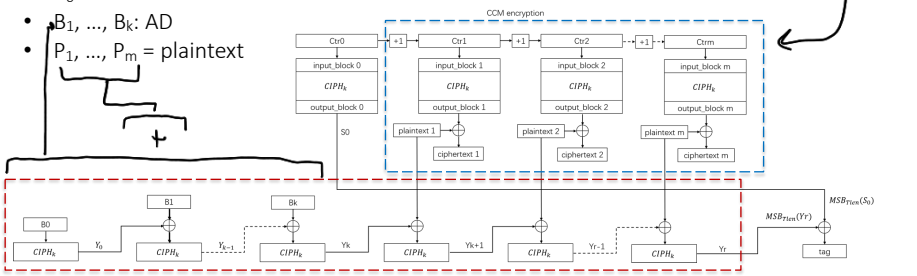
Cipher Block Chaining Message Authentication Code (CCM)

- NIST SP 800-38C
- For IEEE 802.11 WiFi
- AES-CTR and CMAC
- Single key K
- Drawback:
  - CCM is quite complex: it requires two passes through the plaintext

16

CCM – encryption flow chart

- B_0 = nonce
- B_1, …, B_k: AD
- P_1, …, P_m = plaintext



CTR

CMAC

17

Galois Counter Mode (GCM)

- GCM is an encryption mode which also computes a MAC
  - Confidentiality and authenticity
- GCM protects
  - Confidentiality of a plaintext x
  - Authenticity of plaintext x and
  - Authenticity of AAD which is left in the clear

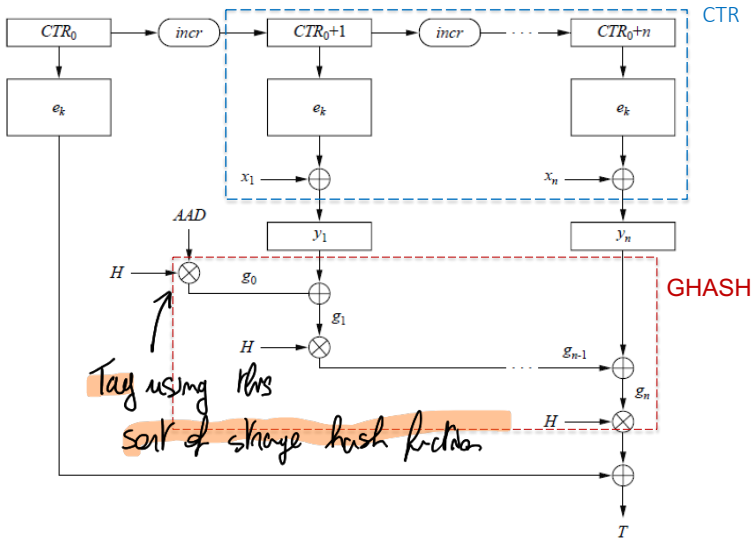
18

GCM - main components

- Cipher in the Counter Mode (CTR)
  - Confidentiality
  - Block size: 128 bit (e.g., AES-128)
- Galois field multiplication
  - Authentication
  - GMAC exploits multiplication in Galois field
    - Based on GHASH which exploits multiplication in GF(2^{128})
      - Irreducible polynomial P(x) = $x^{128} + x^7 + x^2 + x + 1$
      - Easy and efficient in HW

19

GCM – flow chart



20

GCM - advantage

- Assume that AAD and ciphertext (y_1, y_2, …, y_n) constitute a sequence of blocks X = X_1, X_2, …, X_m
- GHASH(X, H)
  - H = $E_k(0)$
  - $Y_0 = 0^{128}$
  - $Y_i = (Y_{i-1} \oplus X_i) \cdot H$ which can be re-written as
  - $(X_1 \cdot H^m) \oplus (X_2 \cdot H^{m-1}) \oplus \cdots \oplus (X_{m-1} \cdot H^2) \oplus (X_m \cdot H^1)$
  - H^2, H^3, …, H^m can be *precomputed*
  - Xi's can be processed *in parallel*

Some factors can be precomputed and you accelerate computation.

21