Authenticated Encryption

Gianluca Dini
Dept. of Ingegneria dell'Informazione
University of Pisa
Emai: gianluca.dini@unipi.it
Version: 2022-04-05

1

Secrecy and integrity

- We have primitives for secrecy and integrity
  - Secrecy: ciphers
  - Integrity: MAC
- What if we wish to achieve secrecy and integrity

apr. '22 Authenticated encryption 2

2

Encrypt and authenticate

- Alice and Bob want to achieve both confidentiality and integrity

Alice (k1, k2)
message x
$y = E_{k1}(x)$
$t = MAC_{K2}(x)$

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

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

apr. '22 Authenticated encryption 3

3

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

apr. '22 Authenticated encryption 4

4

Encrypt then authenticate

- Alice and Bob want to achieve confidentiality and integrity

Alice (k1, k2) **Bob** (k1, k2)

x

$y = E_{k1}(x)$

$t = MAC_{K2}(y)$

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

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

else return "error"

apr. '22 Authenticated encryption 5

5

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
  - The combination is a secure MAC

apr. '22 Authenticated encryption 6

6

Security of encrypt then authenticate

- EtM achieve something stronger
  - Given ciphertexts corresponding to (chosen) plaintexts x_1, …, x_m, it is infeasible for the attacker to generate any new valid ciphertext (ciphertext is the pair y, t)
  - The adversary cannot trick Bob into outputting any message that was not sent by Alice
- *Authenticated encryption scheme*
  - Impossible to generate any, new valid ciphertexts
- In combination with CPA-security this gives CCA-security

apr. '22 Authenticated encryption 7

7

Authenticated encryption

- Encryption-then-authenticate (with independent keys) is a sound way to construct authenticated encryption
  - Plug-in any CPA-secure Enc and any secure MAC
- Encryption-then-authenticate is CCA-secure
- More schemes have been proposed, active field of research

apr. '22 Authenticated encryption 8

8

Three different approaches

- Encrypt and MAC (E&M)
  - Discouraged
  - SSH
- Encrypt then MAC (EtM)
  - Always correct
  - Ipsec
- MAC then Encrypt (MtE)
  - correctness depends on Enc-MAC combinations
  - TLS/SSL

apr. '22 Authenticated encryption 9

9

Standards and associated data

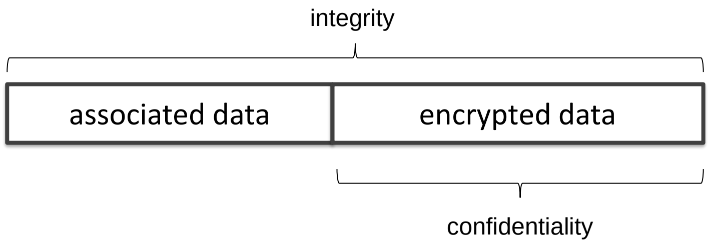
- NIST
  - CCM: CBC-MAC then CTR mode encryption
    - 802.11i
  - GCM: CTR mode encryption then MAC
    - Very efficient
- IETF
  - EAX: CTR mode encryption than OMAC

apr. '22 Authenticated encryption 10

10

Standards and associated data

- NIST and IETF standards support authenticated encryption with *associated data* (AEAD)
  - E.g. the header of a packet is just authenticated



11

Authenticated encryption

GALOIS COUNTER MODE (GCM)

12

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 additional authenticated data (AAD) which is left in the clear
    - ADD might include addresses and parameters in network protocols

apr. '22 Authenticated encryption 13

13

Main components

- Cipher in the Counter Mode (CTR)
  - Confidentiality
  - Block size: 128 bit (e.g. AES-128)
- Galois field multiplication
  - Authentication
  - Multiplication in $GF(2^{128})$ with irreducible polynomial $P(x) = x^{128} + x^7 + x^2 + x + 1$

apr. '22 Authenticated encryption 14

14

Encryption

a. Derive a counter value CTR_0 from the IV and compute $CTR_1 = CTR_0 + 1$.
b. Compute ciphertext: $y_i = E_k(CTR_i) \oplus x_i,\ i \geq 1$

Authentication

a. Generate authentication subkey $H = E_k(0)$
b. Compute $g_0 = AAD \times H$ (Galois field multiplication)
c. Compute $g_i = (g_{i-1} \oplus y_i) \times H,\ 1 \leq i \leq n$ (Galois field multiplication)
d. Final authentication tag:
   $T = (g_n \times H) \oplus E_k(CTR_0)$

GF(2^m) - elements

- Elements are represented as polynomials with coefficient in GF(2)
- Polynomials have maximum degree of m – 1
- Example: GF(2^8)
  - Element $A \in GF(2^8)$ is represented as $A = a_7 \cdot x^7 + \ldots + a_1 \cdot x + a_0$, $a_i \in GF(2)$
  - Element A can be simply stored as $(a_7, a_6, \ldots, a_1, a_0)$

apr. '22 Authenticated encryption 17

17

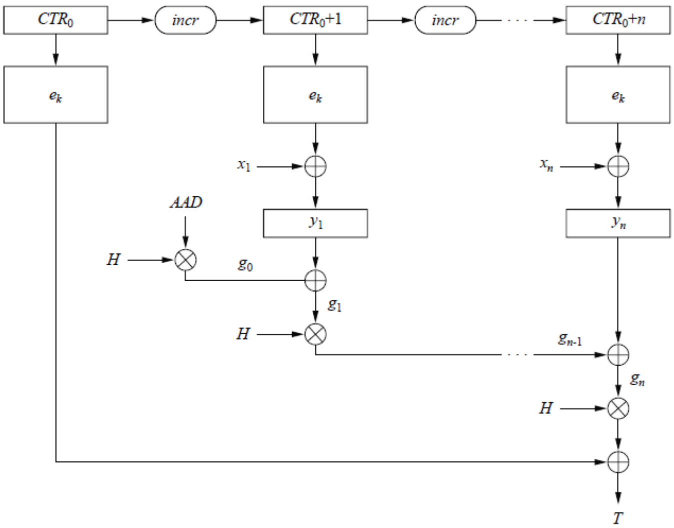
GF(2^m) – operations

- Addition and subtraction
  - $C(x) = A(x) + B(x)$
  - Addition/subtraction modulo 2 of coefficients
- Multiplication
  - $C(x) = A(x) \times B(x)$
    - Order greater than m – 1, thus has to be *reduced* ➔
    - The operation becomes $C(x) \equiv A(x) \times B(x) \bmod P(x)$
      - P(x) is an *irreducible* polynomial
- Inversion
  - $A(x) \times A^{-1}(x) \equiv 1 \bmod P(x)$
    - P(x) is an *irreducible* polynomial

apr. '22 Authenticated encryption 18

18

Diagram of GCM



apr. ’22 Authenticated encryption 19

19

The protocol

- Sender
  - Computes $(y_1, y_2,\ldots, y_n)$ and T
  - Sends [IV, $(y_1, y_2,\ldots, y_n)$, T, ADD]
- Receiver
  - Receives [IV, $(y_1, y_2,\ldots, y_n)$, T, ADD]
  - Decrypts $(y_1, y_2,\ldots, y_n)$ by applying CTR with IV
  - Computes T’ from $(y_1, y_2,\ldots, y_n)$ and ADD
  - Checks whether T == T’
    - If so, ciphertext and ADD were not manipulated in transit and only the sender could have generated the message

apr. ’22 Authenticated encryption 20

20