Cryptography 101: From Theory to Practice

Chapter 11 – Authenticated Encryption

Rolf Oppliger

March 9, 2022

Terms of Use

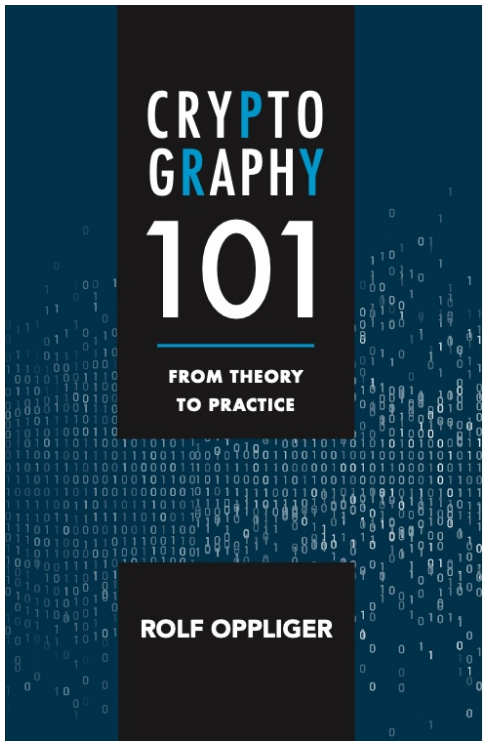
- This work is published with a CC BY-ND 4.0 license ()
  - CC = Creative Commons ()
  - BY = Attribution ()
  - ND = No Derivatives ()

whoami

rolf-oppliger.ch
rolf-oppliger.com

- Swiss National Cyber Security Centre NCSC (scientific employee)
- eSECURITY Technologies Rolf Oppliger (founder and owner)
- University of Zurich (adjunct professor)
- Artech House (author and series editor for information security and privacy)

Reference Book



ISBN 978-1-63081-846-3

`https://books.esecurity.ch/crypto101.html`

Challenge Me

Outline

11. Authenticated Encryption

11. Authenticated Encryption

11. Authenticated Encryption

11.1 Introduction

- According to Chapter 2, there are three approaches (generic composition methods) to combine symmetric encryption and message authentication:
  - Encrypt-then-MAC (EtM): $E_{k_e}(m) \parallel A_{k_a}(E_{k_e}(m))$ → IPsec
  - Encrypt-and-MAC (E&M): $E_{k_e}(m) \parallel A_{k_a}(m)$ → SSH
  - MAC-then-Encrypt (MtE): $E_{k_e}(m \parallel A_{k_a}(m))$ → SSL/TLS
- EtM provides the best level of security
- Contemporary cryptographic security protocols follow this approach or combine message encryption and authentication in **authenticated Encryption (AE)** or **AE with associated data (AEAD)**

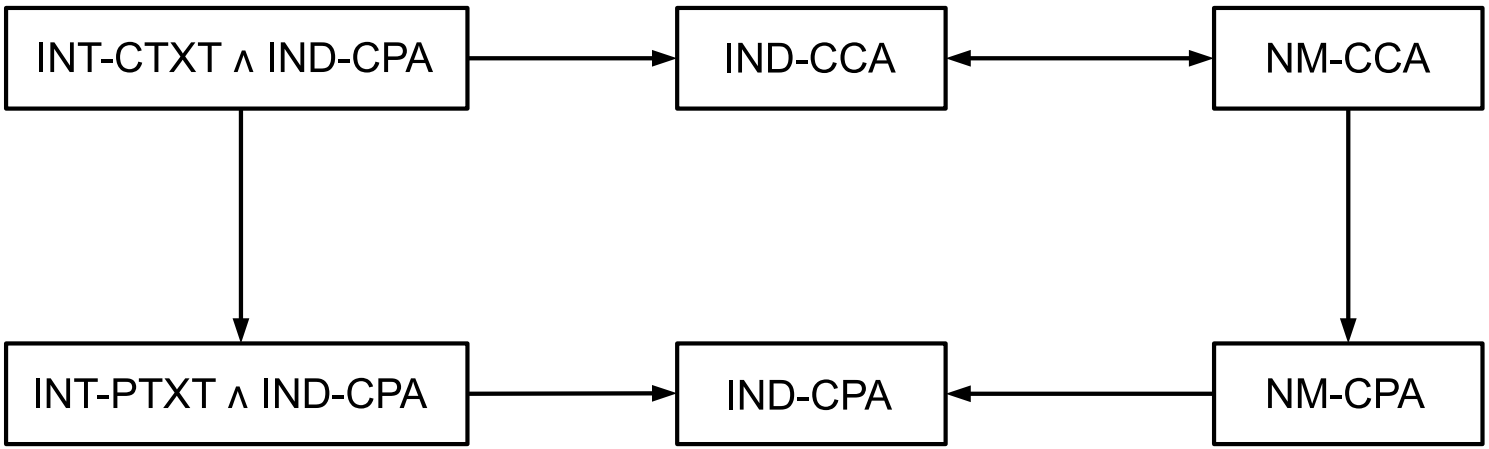
11. Authenticated Encryption

11.1 Introduction

- AE and AEAD systems combine symmetric encryption that provides IND-CPA and message authentication that protects the authenticity and integrity of messages
- People sometimes distinguish whether message authentication protects the integrity of the plaintext messages (INT-PTXT) or the integrity of the respective ciphertexts (INT-CTXT)
- INT-CTXT is a stronger requirement, but the difference is subtle and INT-PTXT is sometimes more intuitive

11. Authenticated Encryption

11.1 Introduction



11. Authenticated Encryption

11.2 AEAD Constructions

- AEAD constructions (modes) currently standardized by NIST
  - Counter with CBC-MAC (CCM)
  - Galois/counter mode (GCM)
- These modes are important in the field and widely used in many Internet security protocols (to replace CBC)
- With regard to encryption, both modes use a block cipher with a block length of 128 bits (e.g., AES) operated in CTR mode
- With regard to authentication, they use different MAC constructions

11. Authenticated Encryption

11.2 AEAD Constructions

- Encryption interface
  - Input: Secret key k, nonce r, plaintext message m, and some additional data a that need to be authenticated (but not encrypted)
  - Output: Ciphertext c and an authentication tag t (that may also be an integral part of c)
- Decryption interface
  - Input: k, r, a, c, and t (or only c, if t is included in c)
  - Output: m or **FAIL**

11. Authenticated Encryption

11.2 AEAD Constructions — CCM

- CCM uses a 128-bit block cipher (e.g., AES) operated in CTR mode for encryption and CBC-MAC for authentication
- The two operations are combined according to MtE
- Advantages
  - Use of standard cryptographic primitives (that are well understood)
  - Use of a single key
- The disadvantage is that the construction requires two applications of the block cipher

11. Authenticated Encryption

11.2 AEAD Constructions — CCM

Algorithm 11.1 CCM authenticated encryption

(k, r, a, m)

$b = \text{format}(r, a, m)$
$x_0 = E_k(b_0)$
for $i = 1$ to $(|a|_l + |m|_l)$ do $x_i = E_k(b_i \oplus x_{i-1})$
$t = \text{MSB}_{|t|}(x_{|a|_l+|m|_l})$
generate $|m|_l + 1$ counter blocks $y_0, y_1, \ldots, y_{|m|_l}$
for $i = 0$ to $|m|_l$ do $s_i = E_k(y_i)$
$s = s_1 \parallel s_2 \parallel \ldots \parallel s_{|m|_l}$
$c = (m \oplus \text{MSB}_{|m|}(s)) \parallel (t \oplus \text{MSB}_{|t|}(s_0))$

(c)

$|a|_l$ and $|m|_l$ refer to the block lengths [= number of l-bit blocks] of a and m

Algorithm 11.2 CCM authenticated decryption

(k, r, c, a)

---

if $|c| \leq |t|$ then abort and return **FAIL**
generate $|m|_l + 1$ counter blocks $y_0, y_1, \ldots, y_{|m|_l}$
for $i = 0$ to $|m|_l$ do $s_i = E_k(y_i)$
$s = s_1 \parallel s_2 \parallel \ldots \parallel s_{|m|_l}$
$m = \text{MSB}_{|c|-|t|}(c) \oplus \text{MSB}_{|c|-|t|}(s)$
$t = \text{LSB}_{|t|}(c) \oplus \text{MSB}_{|t|}(s_0)$
if r, a, or m is invalid
  then abort and return **FAIL**
  else $b = \text{format}(r, a, m)$
$x_0 = E_k(b_0)$
for $i = 1$ to $(|a|_l + |m|_l)$ do $x_i = E_k(b_i \oplus x_{i-1})$
if $t \neq \text{MSB}_{|t|}(x_{|a|_l+|m|_l})$
  then return **FAIL**
  else return m

$(m$ or **FAIL**$)$

11. Authenticated Encryption

11.2 AEAD Constructions — GCM

- Like CCM, GCM uses a 128-bit block cipher (e.g., AES) in CTR mode for encryption
- Unlike CCM, GCM uses a Carter-Wegman MAC for authentication (instead of CBC-MAC)
- The two operations are combined according to EtM
- The message authentication construction is based on polynomial evaluation in $GF(2^{128})$
- $GF(2^{128})$ is a binary extension field of $GF(2)$

11. Authenticated Encryption

11.2 AEAD Constructions — GCM

- The elements of $GF(2^{128})$ are 128-bit strings
- The (field) operations are addition ($\oplus$) and multiplication ($\cdot$)
  - $x \oplus y$ can be implemented as bitwise addition modulo 2
  - $x \cdot y$ can be implemented as polynomial multiplication modulo the irreducible polynomial $f(x) = 1 + x + x^2 + x^7 + x^{128}$
- GCM employs two complementary functions
  - A hash function called GHASH (that uses a 128-bit subkey h)
  - An encryption function called GCTR (that is a variant of "normal" CTR mode encryption)

11. Authenticated Encryption

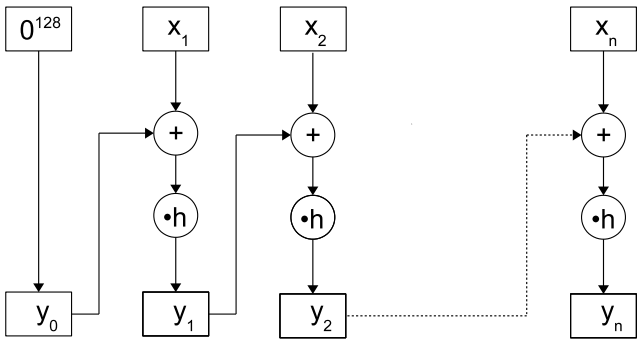
11.2 AEAD Constructions — GCM

Algorithm 11.3 GHASH function

(h, x)

$y_0 = 0^{128}$
for $i = 1$ to n do $y_i = (y_{i-1} \oplus x_i) \cdot h$

(y_n)



$$
\begin{aligned}
y_1 &= (y_0 \oplus x_1) \cdot h = x_1 \cdot h \\
y_2 &= (y_1 \oplus x_2) \cdot h = (((y_0 \oplus x_1) \cdot h) \oplus x_2) \cdot h \\
&= x_1 \cdot h^2 \oplus x_2 \cdot h \\
y_3 &= (y_2 \oplus x_3) \cdot h = ((x_1 \cdot h^2 \oplus x_2 \cdot h) \oplus x_3) \cdot h \\
&= x_1 \cdot h^3 \oplus x_2 \cdot h^2 \oplus x_3 \cdot h \\
&\dots \\
y_n &= x_1 \cdot h^n \oplus x_2 \cdot h^{n-1} \oplus \dots \oplus x_{n-1} \cdot h^2 \oplus x_n \cdot h \\
&= \bigoplus_{i=1}^{n} x_i \cdot h^{n+1-i}
\end{aligned}
$$

11. Authenticated Encryption

11.2 AEAD Constructions — GCM

Algorithm 11.4 GCTR encryption function

ICB refers to an initial counter block

(k, ICB, x)

---

if x is empty then return empty bit string y
$n = \lceil |x|/128 \rceil$
$b_1 = \text{ICB}$
for $i = 2$ to n do $b_i = \text{inc}_{32}(b_{i-1})$
for $i = 1$ to $n-1$ do $y_i = x_i \oplus E_k(b_i)$
$y_n = x_n \oplus \text{MSB}_{|x_n|}(E_k(b_n))$
$y = y_1 \parallel y_2 \parallel \cdots \parallel y_{n-1} \parallel y_n$

(y)

$$\text{inc}_s(x) = \text{MSB}_{128-s}(x) \parallel [\text{int}(\text{LSB}_s(x)) + 1 \pmod{2^s}]_s$$

In GCTR and GCM, s is 32 bits

This means that the first 96 bits of x remain unchanged

and only the last 32 bits are incremented in each step

11. Authenticated Encryption

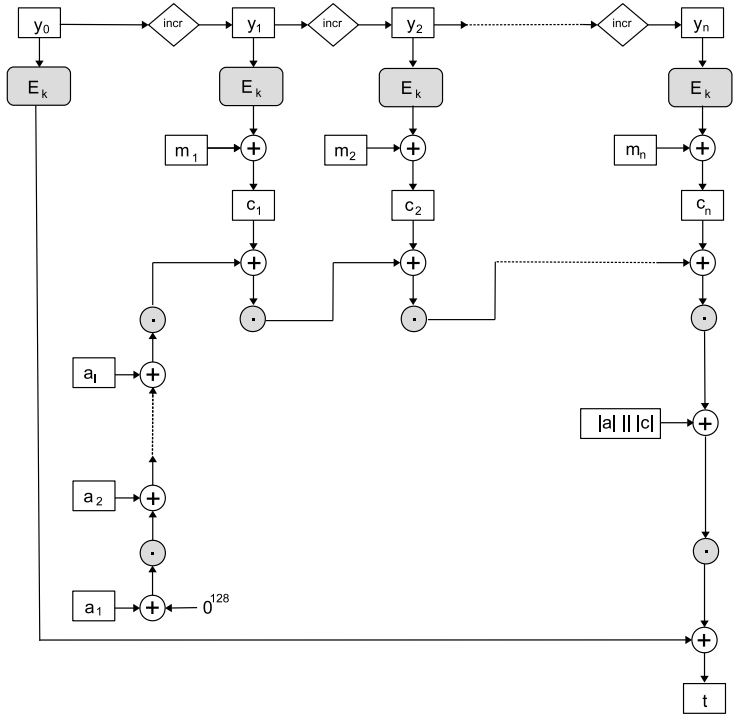
11.2 AEAD Constructions — GCM

Algorithm 11.5 GCM authenticated encryption

(k, r, m, a)

$h = E_k(0^{128})$
if $|r| = 96$ then $y_0 = r \parallel 0^{31}1$
else $s = 128 \cdot \lceil |r|/128 \rceil - |r|$
$y_0 = \text{GHASH}(h, (r \parallel 0^{s+64} \parallel [|r|]_{64}))$
$c = \text{GCTR}(k, \text{inc}_{32}(y_0), m)$
$pad_a = 128 \cdot \lceil |a|/128 \rceil - |a|$
$pad_c = 128 \cdot \lceil |c|/128 \rceil - |c|$
$b = \text{GHASH}(h, (a \parallel 0^{pad_a} \parallel c \parallel 0^{pad_c} \parallel [|a|]_{64} \parallel [|c|]_{64}))$
$t = \text{MSB}_{|t|}(\text{GCTR}(k, y_0, b))$

(c, t)



11. Authenticated Encryption

11.2 AEAD Constructions — GCM

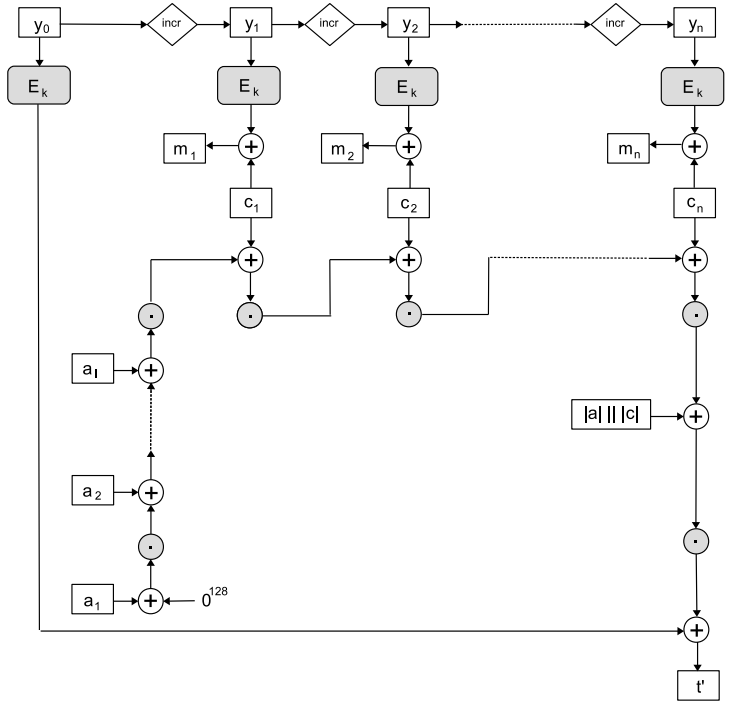
Algorithm 11.6 GCM authenticated decryption

(k, r, c, a, t)

---

verify lengths of r, c, a, and t
$h = E_k(0^{128})$
if $|r| = 96$ then $y_0 = r \parallel 0^{31}1$
else $s = 128 \cdot \lceil |r|/128 \rceil - |r|$
$y_0 = \text{GHASH}(h, (r \parallel 0^{s+64} \parallel [|r|]_{64}))$
$m = \text{GCTR}(k, \text{inc}_{32}(y_0), c)$
$pad_c = 128 \cdot \lceil |c|/128 \rceil - |c|$
$pad_a = 128 \cdot \lceil |a|/128 \rceil - |a|$
$b = \text{GHASH}(h, (a \parallel 0^{pad_a} \parallel c \parallel 0^{pad_c} \parallel [|a|]_{64} \parallel [|c|]_{64}))$
$t' = \text{MSB}_{|t|}(\text{GCTR}(k, y_0, b))$
if $t = t'$ then return m else return **FAIL**

(m or **FAIL**)



11. Authenticated Encryption

11.2 AEAD Constructions — GCM

- It is believed that the GCM mode is secure as long as a new nonce is used for every message
- If a nonce is reused, then it may be feasible to learn the authentication key h and use it to forge authentication tags
- Unfortunately, some Internet protocol specifications do not clearly specify how to generate nonces in a secure way
- This means that nonces are sometimes reused in the field

11. Authenticated Encryption

11.2 AEAD Constructions — GCM

- To mitigate the risk of nonce reuse, people sometimes recommend to deterministically derive the nonce from the message
- A respective construction is known as **synthetic IV (SIV)**
- Exemplary standards
  - AES-SIV (RFC 5297)
  - AES-GCM-SIV (RFC 8452)

11. Authenticated Encryption

11.3 Final Remarks

- In addition to CCM and GCM, there are a few other AE or AEAD modes for block ciphers, such as EAX and OCB
- Mainly due to patent claims, OCB has not yet found the distribution it deserves
- Also due to some recent cryptanalytic results, people are looking for AE(AD) ciphers that provide support for key commitment, meaning that the encryption process must also commit to the key that is being used
- This is ongoing research

Questions and Answers

Thank you for your attention