EECS 575: Advanced Cryptography
Fall 2021
Lecture 14

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Recap from last time
- Security of Authenticated Encryption
  - (with associated data)
- AE from generic composition
- AE in practice: Galois/Counter Mode (GCM) and variants

Agenda for this lecture

- Announcements
- Recap from last time
- Security of Authenticated Encryption
  - (with associated data)
- AE from generic composition
- AE in practice: Galois/Counter Mode (GCM) and variants

Announcements

- HW4 is due tonight at 10pm
- HW5 will be released tonight, due 11/8
- Exams are (still) about half-graded

Recap from last time

- Message authentication
- PRFs are good MACs
  - weak/strong unforgeability
    - → whether adv. can win by forging tag for new msg, or just new msg/tag pair
- Verification queries

Recap from last time

How to build secure channels?

Before '04, use ad-hoc compositions of Enc + MAC

Insecure, all the time!

Instead, build Enc + MAC in one package:

AE (AD)

Agenda for this lecture

- Announcements
- Recap from last time
- Security of Authenticated Encryption
  - (with associated data)
- AE from generic composition
- AE in practice: Galois/Counter Mode (GCM) and variants

Security of AE

- Interface of AE
  - Same as SKE, except Dec can output $\perp$

Let $AE = (Gen, Enc, Dec)$ be an AE scheme

$$Adv^{AE}_{ror}(\mathcal{A}) = \left| \Pr_{K \leftarrow Gen}[\mathcal{A}^{Enc, Dec} \Rightarrow 1] - \Pr[\mathcal{A}^{\$(\cdot), \perp(\cdot)} = 1] \right|$$

Can't call on Prev-Enc outputs

Generates correct # of random bits for ctxt

Say AE is ror-secure if this is $negl(\lambda)$

Agenda for this lecture

- Announcements
- Recap from last time
- Security of Authenticated Encryption
  - (with associated data)
- AE from generic composition
- AE in practice: Galois/Counter Mode (GCM) and variants

Generic Composition

Let SKE = (Gen, Enc, Dec) be an SKE scheme
MAC = (Gen, Tag, Ver) be a msg. auth. code

$AE.Enc_k(m)$:

$t \leftarrow MAC.Tag_{k_m}(m)$

$c \leftarrow SKE.Enc_{k_e}(m||t)$

Ret c

Is AE_{MtE} ror-secure?

No. (In general):

SKE can have malleable cts

E.g. Take SKE, define SKE'

$SKE'.Enc_k(m)$:

$U_1 || SKE.Enc_k(m)$

Nor in practice

Attacks on TLS

POODLE, Lucky13, etc.

Generic Composition

AE.Gen = (SKE.Gen, MAC.Gen)

Let SKE = (Gen, Enc, Dec) be an SKE scheme

MAC = (Gen, Tag, Ver) be a msg. auth. code

$AE.Enc_k(m)$:

$t \leftarrow MAC.Tag_{k_m}(m)$

$c \leftarrow SKE.Enc_{k_c}(m)$

Return $c \| t$

Is AE_{EaM} not-secure?

No. Not even IND-CPA, b/c tag can reveal msg bits

Generic Composition

AE.Gen = (SKE.Gen, MAC.Gen)

Let SKE = (Gen, Enc, Dec) be an SKE scheme

MAC = (Gen, Tag, Ver) be a msg. auth. code

$AE.Enc_k(m)$:

$c \leftarrow SKE.Enc_{k_e}(m)$

$t \leftarrow MAC.Tag_{k_m}(c)$

Ret. $c \| t$

Is AE_{Etm} CCA-secure

Yes! (As long as MAC has pseudorandom tags)

Encrypt-then-MAC analysis

Theorem: Let AE_{EtM}, SKE, MAC, be as before. Let SKE = ⟨Gen, Enc, Dec⟩ be an SKE scheme, MAC = ⟨Gen, Tag, Ver⟩ be a msg. auth. code. AE.Gen = (SKE.Gen, MAC.Gen)

$AE.Enc_k(m)$:
$c \leftarrow SKE.Enc_{k_e}(m)$
$t \leftarrow MAC.Tag_{k_m}(c)$
Ret. $c||t$

If SKE has pseudorandom cts, MAC SUF-CMA and pseudorandom tags, then AE_{EtM} is ror-secure.

Proof: (sketch):

#Assume ∃ A s.t. $Adv^{AE_{EtM}}_{ror}(A) \geq 1/p(\lambda)$

Build adversaries against pseudorandomness of SKE + MAC's tags, and SUF-CMA of MAC

Exercise: Fill in details.

G_0 is Enc, Dec

G_1 is G_0 except SKE.Enc random

G_2 is G_1 except Dec is $\perp$

G_3 is G_2 except Tag outputs random

G_4 is $\$(\cdot), \perp(\cdot)$

Agenda for this lecture

- Announcements
- Recap from last time
- Security of Authenticated Encryption
  - (with associated data)
- AE from generic composition
- AE in practice: Galois/Counter Mode (GCM) and variants

Associated Data

In practice, often need "context" in CTs

E.g., length of CT. Aids network-level ops

Associated Data is "context" that's authentic but not confidential

AEAD = ⟨ Gen, Enc, Dec ⟩

Enc/Dec take assoc. data as argument

→ Extend EtM composition to securely handle AD

(Simplified) GCM

TLS 1.3 defaults to GCM

SGCM.Enc(K, AD, M):

$IV \leftarrow \{0,1\}^{96}$

$P =: PRP_K(IV \| 0^{31}1)$

$H = E_K(0)$

For $i = 1$ to $|M|/128$:

$C = C \| (M[i] \oplus E_K(IV \| (i+1)_{32}))$

$t_0 = GHASH(H, AD, C)$

Ret $IV \| C \| t_0 \oplus P$

PRP is a pseudorandom permutation family on 128 bits

Same key

Deriving OTP to XOR

Basically a PMAC hash with key H

SGCM is RCR-secure

AE in practice