CSE 575: Advanced Cryptography
Fall 2024
Lecture 11

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Authenticated encryption
- Real-or-random security
- Generic composition
- Simplified GCM scheme + analysis

Agenda for this lecture

- Announcements
- Authenticated encryption
- Real-or-random security
- Generic composition
- Simplified GCM scheme + analysis

Announcements

- Midterm starts tonight - thoughts? Could also release it tomorrow

Friday 10/4

Agenda for this lecture

- Announcements
- Authenticated encryption
- Real-or-random security
- Generic composition
- Simplified GCM scheme + analysis

Authenticated Encryption

- SSLv2 '96 : No authentication
- SSLv3 : also broken
- Phil Rogaway : new abstraction!
  Authenticated encryption → 2-for-1
- Syntax : Same as SKE
  except Dec can output ⊥
- Associated data : auth but not enc
  AEAD

Agenda for this lecture

- Announcements
- Authenticated encryption
- Real-or-random security
- Generic composition
- Simplified GCM scheme + analysis

Real-or-random security

$\mathrm{ROR0}^{\mathcal{A}}_{AE}$:

$k \leftarrow \mathrm{Gen}$; $T = [\,]$

$b \leftarrow \mathcal{A}^{E, D}$

Ret b

$E(m)$:

$c \leftarrow AE.\mathrm{Enc}(k, m)$

$T[m] = c$

Ret c

$D(c)$:

If $c \in T$
  Ret $\perp$

Ret $\mathrm{Dec}(k, c)$

$\mathrm{ROR1}^{\mathcal{A}}_{AE}$:

$b \leftarrow \mathcal{A}^{\$, \perp}$

$\$(m)$:

$\ell = \mathrm{clen}(|m|)$

$c \leftarrow \{0,1\}^{\ell}$

Ret c

$\perp(c)$:

Ret $\perp$

AE is ROR

if $\forall$ nuPPT $\mathcal{A}$,

$$\left| \Pr[\mathrm{ROR0}^{\mathcal{A}}_{AE} = 1] - \Pr[\mathrm{ROR1}^{\mathcal{A}}_{AE} = 1] \right| = \mathrm{negl}(n)$$

$\mathrm{EtM}(k_e, k_m, m)$:

$c \leftarrow \mathrm{Enc}(k_e, m)$

$t \leftarrow \mathrm{Tag}(k_m, c)$

Ret c, t

Agenda for this lecture

- Announcements
- Authenticated encryption
- Real-or-random security
- Generic composition
- Simplified GCM scheme + analysis

SKE, MAC Generic composition

$\underline{\text{EaM}(k_e, k_m, m)}$

$c \leftarrow \text{Enc}(k_e, m)$

$t \leftarrow \text{Tag}(k_m, m)$

$\text{Ret } c, t$

$\underline{\text{MtE}(k_e, k_m, m):}$

$t \leftarrow \text{Tag}(k_m, m)$

$c \leftarrow \text{En}(k_e, m \| t)$

$\text{Ret } c$

$\underline{\text{EtM}(k_e, k_m, m):}$

$c \leftarrow \text{Enc}(k_e, m)$

$t \leftarrow \text{Tag}(k_m, c)$

$\text{Ret } c, t$

Analyzing EtM

Agenda for this lecture

- Announcements
- Authenticated encryption
- Real-or-random security
- Generic composition
- Simplified GCM scheme + analysis

$F: \{0,1\}^n \to \{0,1\}^n$

SGCM scheme

$\mathrm{SGCM}[F].\mathrm{Enc}((K,H), m)$:

$IV \leftarrow \{0,1\}^{n-1}$

$P = f_K(IV \| 0)$

$C = m \oplus P$

$t = C \cdot H \oplus f_K(IV \| 1)$

Ret IV, C, t

$\mathrm{SGCM}[F].\mathrm{Dec}((K,H), C')$:

Parse IV, C, t

$t' = C \cdot H \oplus f_K(IV \| 1)$

If $t = t'$:

Ret $C \oplus f_K(IV \| 0)$

Ret $\perp$

- polynomial MAC in $\mathbb{F} = GF(2^n)$
- Same key twice!

Analyzing SGCM

Sketch:

1. replace PRF outputs w/ rand. bits
2. get rid of IV collisions
3. use "polynomial over $\mathbb{F}$" lemma to argue non-$\perp$ outputs D happen w/ negl. prob