EECS 575: Advanced Cryptography
Fall 2022
Lecture 14

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Recap from last time
- Authenticated encryption (AE)
- AE via generic composition
- AE in practice
- (if time) Committing AE

Agenda for this lecture

- Announcements
- Recap from last time
- Authenticated encryption (AE)
- AE via generic composition
- AE in practice
- (if time) Committing AE

Announcements

- ~~HW3 is out, due 10/21~~

HW4 out tonight, due 11/7

Agenda for this lecture

- Announcements
- Recap from last time
- Authenticated encryption (AE)
- AE via generic composition
- AE in practice
- (if time) Committing AE

IND-CPA symmetric encryption

$\text{IND-CPA}\ 0^{\mathcal{A}}_{SKE}$:

$K \leftarrow SKE.Gen$

$b \leftarrow \mathcal{A}^{Enc(\cdot), C_0(\cdot,\cdot)}$

$\underline{Enc(m):}$

Ret $SKE.Enc(k, m)$

$\underline{C_0(m_0, m_1):}$

Ret $Enc(k, m_0)$

$\text{IND-CPA}\ 1^{\mathcal{A}}_{SKE}$:

$K \leftarrow SKE.Gen$

$b \leftarrow \mathcal{A}^{Enc(\cdot), C_1(\cdot,\cdot)}$

$\underline{Enc(m):}$

Ret $SKE.Enc(k, m)$

$\underline{C_1(m_0, m_1):}$

Ret $Enc(k, m_1)$

IND-CPA symmetric encryption

$\underline{ROR0^{A}_{SKE}:}$

$K \leftarrow Gen$

$b \leftarrow A^{Enc(\cdot)}$

$\underline{ROR1^{A}_{SKE}:}$

$b \leftarrow A^{\$(\cdot)}$

$\underline{\$(m):}$

$\ell = SKE.clen(|m|)$

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

Ret C

$\forall$ nuppt A,

$|Pr[ROR0^{A}=1] - Pr[ROR1^{A}=1]| = negl(n)$

Define $SKE.clen(|m|)$:

length of ctxt for any $|m|$ message

UF-CMA message authentication codes

$\mathrm{UFCMA}^{\mathcal{A}}_{\mathrm{MAC}}$:

$K \leftarrow \mathrm{Gen}$; $Q = []$

$(m', t') \leftarrow \mathcal{A}^{\mathrm{Tag}(\cdot),\ \mathrm{Ver}(\cdot,\cdot)}$

Ret $\mathrm{Success}(K, m', t', Q)$

$\mathrm{Tag}(m)$:

$t \leftarrow \mathrm{MAC.Tag}(K, m)$

$Q[m] = t$

Ret t

$\mathrm{Ver}(m, t)$:

Ret $\mathrm{Ver}(K, m, t)$

Agenda for this lecture

- Announcements
- Recap from last time
- Authenticated encryption (AE)
- AE via generic composition
- AE in practice
- (if time) Committing AE

Authenticated Encryption (AE)

1990s – Netscape WWW

Secure Sockets Layer (SSL)

'95 or '96

Bellare/Rogaway/etc.

Authenticated Encryption

No MACs

SSL v2 – broken

SSL v3 – not as broken

Composed SKE + MACs Separately

Authenticated Encryption (AE)

Guarantee confidentiality + auth in one primitive

Gives correct "abstractions" for protocols

AE Syntax

AE = (Gen, Enc, Dec)

Gen / Enc same as SKE

Dec - same except

Can output ⊥

AE with associated data (AEAD)

Same syntax except

Enc/Dec take "header" H

Authenticated Encryption (AE)

$\underline{RORO^{\lambda}_{AE}:}$

$K \leftarrow Gen$; $T = []$

$b \leftarrow A^{Enc(\cdot), Dec(\cdot)}$

$\underline{Enc(m):}$

$C \leftarrow AE.Enc(K, m)$

$T[m] = C$

Ret C

$\underline{Dec(C):}$

If $C \in T$: Ret $\perp$

Ret $AE.Dec(K, C)$

$\underline{ROR1^{A}_{AE}:}$

$b \leftarrow A^{\$(\cdot), 1C(\cdot)}$

$\underline{\$(m):}$

$\ell = Clen(|m|)$

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

Ret C

"AE is ROR-CCA secure, if $\forall$ nuppt t,

$|Pr[RORO^{A} = 1] - Pr[ROR1^{A} = 1]| = negl(\lambda)$

Agenda for this lecture

- Announcements
- Recap from last time
- Authenticated encryption (AE)
- AE via generic composition
- AE in practice
- (if time) Committing AE

Generic Composition

SKE + MAC $\stackrel{?}{=}$ AE

Encrypt-then-MAC (ETM)

MAC-then-encrypt (MtE)

Encrypt-and-MAC (E&M)

$MtE^{SKE,MAC}(k, m)$:

$(k_e, k_m) = k$

$t \leftarrow MAC.Tag(k_m, m)$

$c \leftarrow SKE.Enc(k_e, m||t)$

Ret c

$E\&M^{SKE,MAC}(k, m)$

$(k_e, k_m) = k$

$c \leftarrow SKE.Enc(k_e, m)$

$t \leftarrow MAC.Tag(k_m, m)$

Ret (c, t)

$ETM^{SKE,MAC}(k, m)$:

$(k_e, k_m) = k$

$c \leftarrow SKE.Enc(k_e, m)$

$t \leftarrow MAC.Tag(k_m, c)$

Ret (c, t)

Which is secure?

- ETM b/c can authenticate before decrypting

Generic Composition

Break E a M :

(Show t that wins ROR-CCA w.h.p.)

$\underline{E\,a\,M^{SKE,MAC}(k,m)}$

$(k_e, k_m) = k$

$C \leftarrow SKE.Enc(k_e, m)$

$t \leftarrow MAC.Tag(k_m, m)$

Ret (C, t)

Enc, Dec

$\underline{A_{cam}}$

$(C_1, t_1) = Enc(m)$

$(C_2, t_2) = Enc(m)$

If $t_1 = t_2$ Ret 0

Ret 1

wins w.p. $\geq 1 - \frac{1}{2^n}$

Exercise:

Secure with randomized tags?

Generic Composition

Break M+E

(Give ROR-CCA distinguisher)

$\exists$ ROR-CPA SKE

s.t. ROR-CCA insecure

(Exercise: Prove this ROR-CPA)

$MtE^{SKE, MAC}(k, m)$:

$(k_e, k_m) = k$

$t \leftarrow MAC.Tag(k_m, m)$

$c \leftarrow SKE.Enc(k_e, m \| t)$

Ret c

$Enc(k, m)$:

$b \leftarrow \{0,1\}$

$c \leftarrow SKE.Enc(k, m)$

Ret $b \| c$

$\mathcal{A}^{Enc, Dec}$:

$b \| c = Enc(m)$

$\bar{m} = Dec(\bar{b} \| c)$

If $\bar{m} \neq \perp$ Ret 0

Ret 1

Dec ignores

Generic Composition

Thm: E_{tm} is ROR-CCA.

Let SKE be ROR-CPA, and
MAC be UF-CMA, deterministic,
pseudorandom tags

then $E_{tm}[SKE, MAC]$ is ROR-CCA.

Proof (sketch):

ROR-CPA
- $H_0 = ROR0^{E_{tm}}$
- $H_1 = ROR0$ but enc is random bits

UF-CMA
- $H_2 = $ Dec always returns $\perp$ — PR of tag
- $H_3 = $ Tag is random fn — PR of tag

Birthday Bound
- $H_4 = ROR1$

Agenda for this lecture

- Announcements
- Recap from last time
- Authenticated encryption (AE)
- AE via generic composition
- AE in practice
- (if time) Committing AE

AE in practice

Agenda for this lecture

- Announcements
- Recap from last time
- Authenticated encryption (AE)
- AE via generic composition
- AE in practice
- (if time) Committing AE

Committing AE