EECS 575: Advanced Cryptography
Fall 2022
Lecture 15

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Recap from last time
- Analysis of Encrypt-then-MAC
- AE in practice
- Public-key encryption (PKE)
- IND-CPA security for PKE

Agenda for this lecture

- Announcements
- Recap from last time
- Analysis of Encrypt-then-MAC
- AE in practice
- Public-key encryption (PKE)
- IND-CPA security for PKE

Announcements

- HW4 is out, due 11/7
- New theoretical computer science club
  - First meeting 11/7 at 6pm (ask Alexandra for location)
- Last Friday was global encryption day!
  - globalencryption.org

Agenda for this lecture

- Announcements
- Recap from last time
- Analysis of Encrypt-then-MAC
- AE in practice
- Public-key encryption (PKE)
- IND-CPA security for PKE

Authenticated Encryption

- Encryption + authenticity

ROR^{λ}_{AE}:

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

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

Enc(m):

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

$T[m] = C$

Ret C

Dec(C):

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

Ret $AE.Dec(K, C)$

ROR^{A}_{AE}:

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

$\$(m)$:

$\ell = |Clen(|m|)|$

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

Ret C

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

$(K_e, K_m) = K$

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

$t \leftarrow MAC.Tag(K_m, C)$

Ret (C, t)

ROR-CCA / IND-CCA

Authenticated Encryption

Thm: Let SKE be a ROR-CPA encryption, MAC is deterministic SUF-CMA MAC with pseudorandom tags. Then $ETM^{SKE,MAC}$ is ROR-CCA.

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

$(k_e, k_m) = K$

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

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

Ret (C, t)

Note:

$$SKE.Enc : \{0,1\}^\lambda \longrightarrow \{0,1\}^{2\lambda}$$

$$MAC.Tag : \{0,1\}^{2\lambda} \longrightarrow \{0,1\}^\lambda$$

Encrypt-then-MAC

Agenda for this lecture

- Announcements
- Recap from last time
- Analysis of Encrypt-then-MAC
- AE in practice
- Public-key encryption (PKE)
- IND-CPA security for PKE

Analysis of EtM

H_0 : RORO w/ EtM

H_1 : H_0 w/ random cts

H_0 : $\mathcal{A}^{EtM}$

$K_e \leftarrow SKE.Gen$

$K_m \leftarrow MAC.Gen$; $T = []$

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

Enc(m):

$(K_e, K_m) = K$

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

$t \leftarrow MAC.Tag(K_m, C)$

$T[m] = C \| t$

Ret (C, t)

Dec(C||t):

If $C\|t \in T$ Ret $\perp$

$b = Ver(K_m, C, t)$

If $b = 1$ Ret $SKE.Dec(K_e, C)$

Ret $\perp$

H_1 / EtM

Enc(m):

$C \leftarrow \{0,1\}^{2n}$

$t \leftarrow MAC.Tag(K_m, t)$

$T[m] = C \| t$

Ret $(C \| t)$

Dec(C||t):

If $C\|t \in T$ Ret $\perp$

$b = Ver(K_m, C, t)$

If $b = 1$ Ret $T^{-1}[C\|\cdot]$

Ret $\perp$

Show $H_0 \approx_c H_1$ by reduction to ROR-CPA of SKE ?

Analysis of EtM

Argue $H_0 \approx_c H_1$?

Reduce to ROR-CPA of SKE

$B^{Enc(\cdot),\tilde{Enc},\tilde{Dec}}$:

$K_m \leftarrow MAC.Gen$; $T = []$

$b \leftarrow A^{\tilde{Enc},\tilde{Dec}}$

$\tilde{Enc}(m)$:

$c \leftarrow Enc(m)$

$t = MAC.Tag(K_m, c)$

$T[m] = c||t$

Ret $c||t$

$\tilde{Dec}(c||t)$:

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

$b = Ver(k_m, c, t)$

If $b = 1$ Ret $T^{-1}[c||\cdot]$

Ret $\perp$

Exercise: Argue

$Pr[H_0 = 1] - Pr[H_1 = 1] \leq$ ROR-CPA^B

Analysis of EtM

Issue: in $\widetilde{Dec}$, can't decrypt non-outputs of Enc.

B only has table, no decryption oracle

Bug?

Could fix by reducing to ROR-CCA of SKE

Finish on Friday in discussion

Agenda for this lecture

- Announcements
- Recap from last time
- Analysis of Encrypt-then-MAC
- AE in practice
- Public-key encryption (PKE)
- IND-CPA security for PKE

AE in practice

Generic composition AE

Compose Enc/MAC

For efficiency, use "direct" construction

- AES-GCM
- ChaCha20/Poly1305

"Sort of" EtM - compute MAC on ciphertext

AE in practice

- Universal hash function
  "Pairwise independent hash"

AE in practice

AES → E

$SGCM^E(K, M)$: $\quad |M| \in \{0,1\}^{128}$

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

$P = E_K(IV \| 0^{31}\|1)$ → $IV+1$

$H = E_K(0)$ ← Not generic

$C = M \oplus E_K(IV \| 0^{30}\|10)$ ↔ $IV+2$

$t_0 = C \cdot H^2 \oplus [0^{64}\|(|C|)_{64}] \cdot H$ ← → $GF(2^{128})$

Very Fast

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

Agenda for this lecture

- Announcements
- Recap from last time
- Analysis of Encrypt-then-MAC
- AE in practice
- Public-key encryption (PKE)
- IND-CPA security for PKE

Public-key encryption (PKE)

Agenda for this lecture

- Announcements
- Recap from last time
- Analysis of Encrypt-then-MAC
- AE in practice
- Public-key encryption (PKE)
- IND-CPA security for PKE

IND-CPA for PKE