EECS 575: Advanced Cryptography
Fall 2021
Lecture 13

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Recap from last time
- Computationally-secure message authentication
- PRFs are good MACs
- Authenticated Encryption
- Generic composition of encryption and MACs

Agenda for this lecture

- Announcements
- Recap from last time
- Computationally-secure message authentication
- PRFs are good MACs
- Authenticated Encryption
- Generic composition of encryption and MACs

Announcements

- Hopefully everyone had a good fall break!
- HW4 is due next Monday, 10/25
- Exams are about half-graded

Recap from last time

Message Authentication codes (MACs)

MACs authenticate and ensure integrity of msgs

* Gen: returns $K \leftarrow \{0,1\}^n$
* Tag(k, m): returns $t \in \mathcal{T}$
* Ver(k, m, t): returns 0/1

  $t' \leftarrow$ Tag(k, m)

  Return $t = t'$

Recap from last time

Pairwise-Independent Hash Function (families)

$\{h_s : \mathcal{M} \to \mathcal{Z}\}$ is PWI if $\forall m_0 \neq m_1$,

$$\Pr_{s \leftarrow S}[h_s(m_0) = t_0 \wedge h_s(m_1) = t_1] \leq \frac{1}{|\mathcal{Z}|^2}$$

* MACs from PWI families
* Perfect Unforgeability

$$Adv_{MAC}(F) = \Pr_{\substack{k \leftarrow Gen \\ t \leftarrow Tag(k,m)}}[F(m,t) \text{ succeeds}] \leq \frac{1}{|\mathcal{T}|}$$

outputs $m', t' \in \mathcal{M} \times \mathcal{Z}$ where $m' \neq m$ and $Ver(k, m', t') = 1$

Agenda for this lecture

- Announcements
- Recap from last time
- Computationally-secure message authentication
- PRFs are good MACs
- Authenticated Encryption
- Generic composition of encryption and MACs

Message Authentication

MACs from PWIs have large keys

→ This is inherent for IT-secure MACs

Relax security to computationally-efficient forgers

* UF-CMA $\forall$ nuppt $\mathcal{F}$,

$$Adv^{MAC}(\mathcal{F}) = \Pr_{k \leftarrow Gen}\left[\mathcal{F}^{Tag_k(\cdot)} \text{ succeeds}\right] \leq negl(n)$$

(weak) Returns (m', t') s.t.
m' not input to Tag
and $Ver(k, m', t') = 1$

(Strong) Returns (m', t') s.t.
(m', t') not input-output of Tag
and $Ver(k, m', t') = 1$

Message Authentication

Can call Ver on many (m', t') pairs!

$$Adv_{MAC}(F) = \Pr_{k \leftarrow Gen}\left[F^{Tag_k(\cdot), Ver_k(\cdot,\cdot)} \text{ succeeds}\right] \leq negl(n)$$

Equiv for SUF-CMA but not weak!

UF-1 UF-M

SUF-1 $\Longleftrightarrow$ SUF-M

Agenda for this lecture

- Announcements
- Recap from last time
- Computationally-secure message authentication
- PRFs are good MACs
- Authenticated Encryption
- Generic composition of encryption and MACs

PRFs are good MACs

$\{F_s : \{0,1\}^n \longrightarrow \{0,1\}^n\}$

* Gen: Generate $s \leftarrow \{0,1\}^n$
* Tag(k,m): Return $F_k(m)$
* Ver(k,m,t): $t' \leftarrow$ Tag(k,m); Ret $t \stackrel{?}{=} t'$

Theorem: This MAC is UF-CMA if F_s PRF family

Proof: By reduction.

PRFs are good MACs

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

* Gen: Generate $s \leftarrow \{0,1\}^n$
* Tag(k, m): Return $F_k(m)$
* Ver(k, m, t): $t' \leftarrow$ Tag(k, m); Ret $t' \stackrel{?}{=} t$

Theorem: This MAC is UF-CMA if F_s PRF family

Proof: By reduction. Suppose we have Forger $\mathcal{A}$. $\Pr[\mathcal{A}^{\text{Tag}_K(\cdot)} \text{ strongly succeeds}] \geq 1/p(n)$ for some poly $p(n)$. Build distinguisher D for PRF:

$$\left| \Pr[D^{g}=1] - \Pr[D^{g}=1] \right| =$$

(g is F_s / g is $U(\{0,1\}^n \to \{0,1\}^n)$)

$$\left| \Pr[\mathcal{A}^{\text{Tag}_K(\cdot)} \text{ Succeeds}] - \frac{1}{2^n} \right|$$

($\mathcal{A}$ guesses output of rand. f'n)

$\geq 1/p(n) - \frac{1}{2^n}$, non-negl ☒

$D^{g(\cdot)}$:

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

Ret $(t' \stackrel{?}{=} g(m') \wedge (m', t') \notin T)$

$\widetilde{\text{Tag}}(m)$:

$t \leftarrow g(m)$; $i = i+1$

$T[i] = (m, t)$

Only way to win is if m' not seen

D's simulated Tag oracle for $\mathcal{A}$

PRFs are good MACs

Ver(k, m, t): n-byte strings

$t' \leftarrow Tag_k(m)$; $b \leftarrow True$

For i=0 to n-1:

IF $t[i] \neq t'[i]$ Return False

$b \leftarrow b \wedge t[i] = t'[i]$

Return b

Learns length of common prefix between t and t'

$\Rightarrow$ can forge tag via timing!!

Agenda for this lecture

- Announcements
- Recap from last time
- Computationally-secure message authentication
- PRFs are good MACs
- Authenticated Encryption
- Generic composition of encryption and MACs

Authenticated Encryption

We have Symmetric-key encryption (IND-CPA)
Symmetric-key MAC (UF-CMA)

90s-00s: try to compose encryption + MAC primitives
They failed. A lot.

Early-mid 00s: combine them! one primitive with both.

Authenticated Encryption scheme $AE = (Gen, Enc, Dec)$

* Gen
* $Enc(K, m)$: Returns $c \in \mathcal{C}$
* $Dec(K, c)$: Returns either $m \in \mathcal{M}$ or $\perp$ ← failure symbol

Authenticated Encryption

$\$(\cdot)$ is random-bits oracle

$\perp(\cdot)$ is "fail" oracle

Authenticated Encryption scheme $AE = (Gen, Enc, Dec)$

* Gen
* $Enc(K, m)$: Returns $C \in \mathcal{C}$
* $Dec(K, C)$: Returns either $m \in \mathcal{M}$ or $\perp$ ← failure symbol

$$Adv_{AE}(D) = \left| \Pr_{K \leftarrow Gen}\left[D^{Enc_K(\cdot), Dec_K(\cdot)} = 1\right] - \Pr_{\$(\cdot)}\left[D^{\$(\cdot), \perp(\cdot)} = 1\right] \right|$$

Agenda for this lecture

- Announcements
- Recap from last time
- Computationally-secure message authentication
- PRFs are good MACs
- Authenticated Encryption
- Generic composition of encryption and MACs

AE via generic composition