EECS 575: Advanced Cryptography
Fall 2021
Lecture 12

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Announcements

- HW4 online. 25th Oct is due date
- New version online - redownload

Recap from last time

- Symmetric encryption
- IND-CPA

$\{Enc_K(\cdot), C_0(\cdot,\cdot)\} \approx_c \{Enc_K(\cdot), C_1(\cdot,\cdot)\}$

$C_0(\cdot,\cdot)$: m_0, m_1, output $Enc_K(m_0)$

$C_1(\cdot,\cdot)$: output $Enc_K(m_1)$

- IND-CPA requires randomized Enc
- Fixed-length IND-CPA encryption from PRF F

$Enc_K(m)$: $r \leftarrow \{0,1\}^n$; Return $(r, F_K(r) \oplus m)$

Message Authentication

Authenticates messages

- Authenticity (who sent this message?)
- Integrity (is this msg the one I was sent?)

Person

Stonks

c = "Buy Intel FB" ⊕ k

m = Buy Intel FB

Tack(m)

OTP is not authentic, nor integral

"Integrity isn't important"

break conf. b/c no integrity

- Padding oracle

Message Authentication

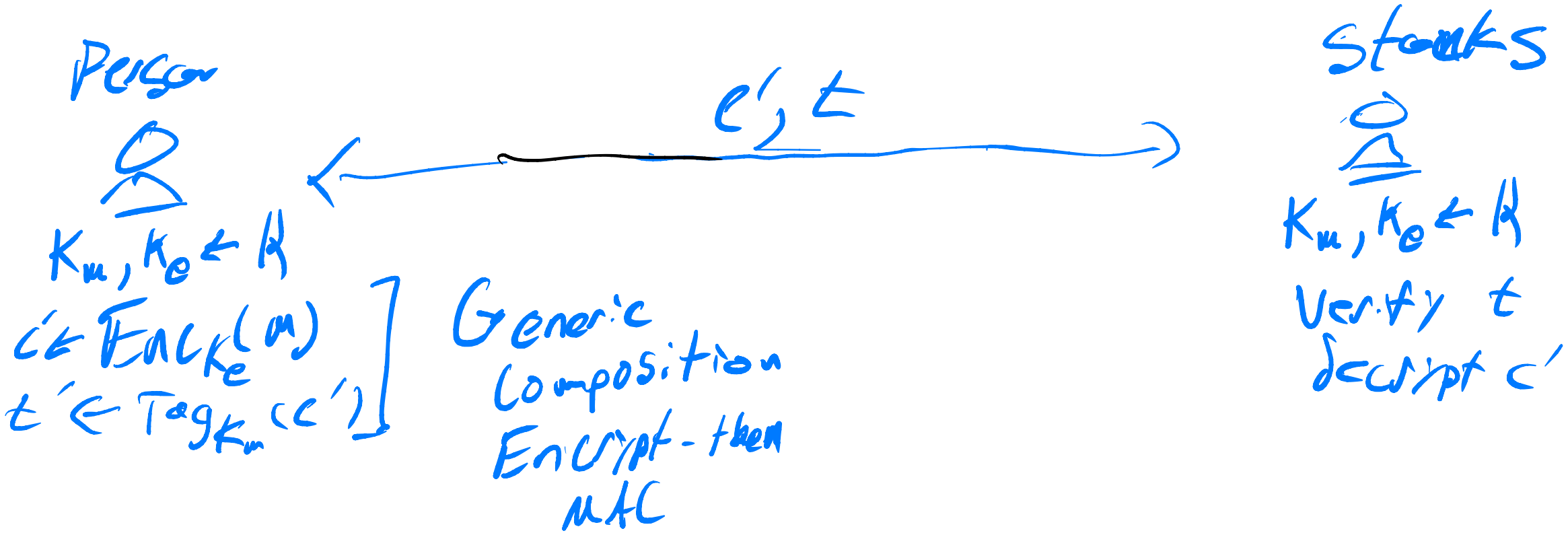
Message Authentication Code (MAC)

* Gen: $k \leftarrow \{0,1\}^n$
* $Tag_k(m)$: outputs t "a tag" in $\mathcal{T}$
* $Ver_k(m,t)$: output 1, 0 otherwise

(For deterministic MACs, wlog $Ver_k(m,t)$: $t \stackrel{?}{=} Tag_k(m)$)

Message Authentication

How to build MACs?



Message Authentication

How to build MACs? How to define security?

$\forall$ messages m,

$$Adv_{MAC}(F) = \Pr\left[\begin{array}{l} k \leftarrow Gen \\ t \leftarrow Tag_k(m) \end{array} \;\middle|\; \begin{array}{l} F(m,t) = (m',t') : \\ Ver_k(m',t') = 1 \\ \wedge\ m \neq m' \end{array}\right] \leq \frac{1}{|\mathcal{T}|} = 0 ?$$

Impossible - random guess

Message Authentication

Pairwise-independent function families (hashing)

Func family $\{h_k : \mathcal{M} \to \mathcal{Z}\}$ ⇒ PWI

if $k \leftarrow \mathcal{K}$, $\forall m_0 \neq m_1 \in \mathcal{M}$, $\forall t_0, t_1$,

$$\Pr_{k}[h_k(m_0) = t_0 \wedge h_k(m_1) = t_1] = \frac{1}{|\mathcal{Z}|^2}$$

Alternatively, can $(h_k(m_0), h_k(m_1))$ is uniform over $\mathcal{Z}^2$

Message Authentication

Let p be prime. Define, $a, b, x \in \mathbb{Z}_p$

$h_{a,b}(x) = ax + b \bmod p$.

$\mathcal{M} = \mathcal{Z} = \mathbb{Z}_p$

Lemma: This is a PWI family.

Proof: If $m_0 \neq m_1 \in \mathbb{Z}_p$, $t_0, t_1 \in \mathbb{Z}_p$,

$$\Pr_{a,b}[h_{a,b}(m_0) = t_0 \wedge h_{a,b}(m_1) = t_1] = \Pr[am_0 + b = t_0 \wedge am_1 + b = t_1] =$$

$$\Pr_{a,b}\left[\underbrace{\begin{pmatrix} m_0 & 1 \\ m_1 & 1 \end{pmatrix}}_{m_0 \neq m_1} \cdot \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} t_0 \\ t_1 \end{pmatrix}\right] = \Pr_{a,b}\left[\begin{pmatrix} a \\ b \end{pmatrix} = \underbrace{\begin{pmatrix} m_0 & 1 \\ m_1 & 1 \end{pmatrix}^{-1} \begin{pmatrix} t_0 \\ t_1 \end{pmatrix}}_{\text{arbitrary in } \mathbb{Z}_p^2}\right] = \frac{1}{p^2}$$

Message Authentication

PWIs give one-time MACs.

* Gen : output (a,b)
* $Tag_K(m)$: $am+b \bmod p$
* $Ver_K(m,t)$: Return $t \stackrel{?}{=} am+b \bmod p$

Theorem: $\forall F$

$$Adv^{PWI}_{MAC}(F) = \frac{1}{|Z|} = \frac{1}{p}$$

Proof: Exercise.

Note

$$Pr[am_1+b = t_1 \mid \underbrace{am_0+b = t_0}_{\text{what the adv. gets}}] = \frac{1}{p}$$

Message Authentication

Problem: Many-time secure MACs with "short" keys

Computational security. Unforgeability under chosen-message attack (UF-CMA)

A MAC is UF-CMA if $\forall$ nuppt F,

$$Adv_{MAC}(F) = \Pr_{K \leftarrow Gen}\left[F^{Tag_K(\cdot)} = (m', t') : \begin{array}{l} Ver_K(m', t') = 1 \text{ and} \\ m' \text{ not prev. query} \end{array} \right] = negl(n)$$

$[m', t' \text{ not prev. input output pair}]$