Composite schemes

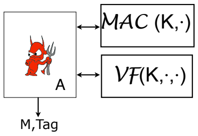
- Fix a symmetric encryption scheme and a message authentication code
- There are several ways to use them together
  1. Encrypt-and-MAC
  2. MAC-then-Encrypt
  3. Encrypt-then-MAC
- If the components are secure, are the composite schemes secure (provide privacy and integrity)?

Another (stronger) security definition for MACs

Fix Π=(*K*,MAC,VF)

Run *K* to get K

For an adversary A consider an experiment $\mathbf{Exp}_{\Pi}^{suf\text{-}cma}(A)$



Return 1 iff VF(K,M,Tag)=1 and Tag was never returned by the signing oracle as an answer to a query M.

The uf-cma advantage of A is defined as

$$\mathbf{Adv}_{\Pi}^{\text{suf-cma}}(A) = \Pr\left[\mathbf{Exp}_{\Pi}^{\text{suf-cma}}(A) = 1\right]$$

Claim. SUF-CMA ⇒ UF-CMA
Conjecture. Most of known UF-CMA secure MACs are also SUF-CMA

Encrypt-and-MAC

- Fix a symmetric encryption scheme $SE = (\mathcal{K}_e, \mathcal{E}, \mathcal{D})$ and a MAC $MAC = (\mathcal{K}_m, \mathcal{T}, \mathcal{V})$
- Consider a symmetric encryption scheme $EaM = (\overline{\mathcal{K}}, \overline{\mathcal{E}}, \overline{\mathcal{D}})$

Algorithm $\overline{\mathcal{K}}$	Algorithm $\overline{\mathcal{E}}_{\langle K_e,K_m\rangle}(M)$	Algorithm $\overline{\mathcal{D}}_{\langle K_e,K_m\rangle}(C)$
$K_e \xleftarrow{\$} \mathcal{K}_e$	$C' \leftarrow \mathcal{E}_{K_e}(M)$	Parse C as $C' \| \tau$
$K_m \xleftarrow{\$} \mathcal{K}_m$	$\tau \leftarrow \mathcal{T}_{K_m}(M)$	$M \leftarrow \mathcal{D}_{K_e}(C')$
Return $\langle K_e, K_m\rangle$	$C \leftarrow C' \| \tau$	$v \leftarrow \mathcal{V}_{K_m}(M,\tau)$
	Return C	If $v = 1$, return M
		else return $\perp$.

Theorem1. There exist an IND-CPA SE and SUF-CMA MAC s.t. EaM constructed as above is NOT IND-CPA secure.

MAC-then-Encrypt

- Fix a symmetric encryption scheme $SE = (\mathcal{K}_e, \mathcal{E}, \mathcal{D})$ and a MAC $MAC = (\mathcal{K}_m, \mathcal{T}, \mathcal{V})$
- Consider a symmetric encryption scheme $MtE = (\overline{\mathcal{K}}, \overline{\mathcal{E}}, \overline{\mathcal{D}})$

Algorithm $\overline{\mathcal{K}}$	Algorithm $\overline{\mathcal{E}}_{\langle K_e,K_m\rangle}(M)$	Algorithm $\overline{\mathcal{D}}_{\langle K_e,K_m\rangle}(C)$
$K_e \xleftarrow{\$} \mathcal{K}_e$	$\tau \leftarrow \mathcal{T}_{K_m}(M)$	$M' \leftarrow \mathcal{D}_{K_e}(C)$
$K_m \xleftarrow{\$} \mathcal{K}_m$	$C \leftarrow \mathcal{E}_{K_e}(M \| \tau)$	Parse M' as $M \| \tau$
Return $\langle K_e, K_m\rangle$	Return C	$v \leftarrow \mathcal{V}_{K_m}(M,\tau)$
		If $v = 1$, return M
		else return $\perp$.

Theorem2. There exist an IND-CPA SE and SUF-CMA MAC s.t. MtE constructed as above is NOT IND-CCA secure.

Encrypt-then-MAC !

- Fix a symmetric encryption scheme $SE = (\mathcal{K}_e, \mathcal{E}, \mathcal{D})$ and a MAC $MAC = (\mathcal{K}_m, \mathcal{T}, \mathcal{V})$
- Consider a symmetric encryption scheme $EtM = (\overline{\mathcal{K}}, \overline{\mathcal{E}}, \overline{\mathcal{D}})$

Algorithm $\overline{\mathcal{K}}$	Algorithm $\overline{\mathcal{E}}_{\langle K_e,K_m\rangle}(M)$	Algorithm $\overline{\mathcal{D}}_{\langle K_e,K_m\rangle}(C)$
$K_e \xleftarrow{\$} \mathcal{K}_e$	$C' \leftarrow \mathcal{E}_{K_e}(M)$	Parse C as $C' \| \tau'$
$K_m \xleftarrow{\$} \mathcal{K}_m$	$\tau' \leftarrow \mathcal{T}_{K_m}(C')$	$M \leftarrow \mathcal{D}_{K_e}(C')$
Return $\langle K_e, K_m \rangle$	$C \leftarrow C' \| \tau'$	$v \leftarrow \mathcal{V}_{K_m}(C', \tau')$
	Return C	If $v = 1$, return M
		else return $\perp$.

<u>Theorem3</u>. For every IND-CPA SE and SUF-CMA MAC, EtM constructed as above is IND-CPA, INT-CTXT and IND-CCA secure.

<u>Proof</u>. We will show that for every adversary A attacking *ind-cpa* security of EtM there exists an adversary B attacking *ind-cpa* security of SE with the same resources, and for every adversary A attacking *int-ctxt* security of EtM there exists an adversary F attacking *suf-cma* security of MAC with the same resources s.t.

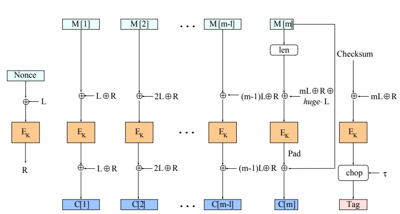
- 1) $\mathbf{Adv}_{EtM}^{ind-cpa}(A) \le \mathbf{Adv}_{SE}^{ind-cpa}(B)$
- 2) $\mathbf{Adv}_{EtM}^{int-ctxt}(A) \le \mathbf{Adv}_{MAC}^{suf-cma}(F)$

and the statement of the theorem will follow by using the theorem we proved before: [IND-CPA ∧ INT-CTXT ⇒ IND-CCA].

Adversary $B^{\mathcal{E}_{K_e}(\mathcal{LR}(\cdot,\cdot,b))}$
$K_m \xleftarrow{\$} \mathcal{K}_m$
For $i = 1, \ldots, q$ do
  When A makes a query $(M_{i,0}, M_{i,1})$ to its left-or-right encryption oracle do
    $C_i \leftarrow \mathcal{E}_{K_e}(\mathcal{LR}(M_{i,0}, M_{i,1}, b))$; $\tau_i \leftarrow \mathcal{T}_{K_m}(C_i)$; $A \Leftarrow C_i \| \tau_i$
$A \Rightarrow b'$
Return b'

2) Adversary $F^{\mathcal{T}_{K_m}(\cdot), \mathcal{V}_{K_m}(\cdot,\cdot)}$
$K_e \xleftarrow{\$} \mathcal{K}_e$
For $i = 1, \ldots, q_e + q_d$ do
  When A makes a query M_i to its encryption oracle do
    $C'_i \leftarrow \mathcal{E}_{K_e}(M_i)$; $\tau_i \leftarrow \mathcal{T}_{K_m}(C'_i)$; $A \Leftarrow C'_i \| \tau_i$
  When A makes a query C_i to its verification oracle do
    Parse C_i as $C'_i \| \tau'_i$; $v_i \leftarrow \mathcal{V}_{K_m}(C'_i, \tau'_i)$; $A \Leftarrow v_i$

- It's possible to construct a secure (IND-CPA and INT-CTXT) symmetric encryption scheme without using a generic composition.
- Example: OCB



Checksum = M[1] ⊕ M[2] ⊕ ··· ⊕ M[m-1] ⊕ C[m]0* ⊕ Pad L = $E_K(\mathbf{0})$