Message Authentication

We now define security in the computational setting.

$$\text{GAME}^{\overbrace{\text{ufcma}}^{}}_{\Pi,A}(\lambda)$$ → UNIVERSAL UNFORGEABILITY AGAINST CHOSEN MESSAGE ATTACK

$A(1^\lambda)$ $\qquad\qquad\qquad\qquad$ $\mathcal{C}(1^\lambda)$

$\xrightarrow{\; m \in \mathcal{M} \;}$ $\quad k \leftarrow\$ \mathcal{K}$

$\xleftarrow{\; \tau = \text{Tag}(k, m) \;}$

$\xrightarrow{\; m^*, \tau^* \;}$ OUTPUT 1 if

$\tau^* = (k, m^*)$

$m^* \in \{m\}$

Definition: A MAC Π is UFCMA if $\forall$ PPT A

$$\exists\, \varepsilon(\lambda) = \text{negl}(\lambda) \mid \Pr[\text{GAME}^{\text{ufcma}}_{\Pi,A}(\lambda) = 1] \leq \varepsilon(\lambda)$$

PLAN: ① MACs are in MINICRYPT
(OWFs $\Rightarrow$ MACs) for fixed input length
② DOMAIN EXTENSION (i.e. variable input length)

THM: Every PRF family $\mathcal{F} = \{F_k : \{0,1\}^n \to \{0,1\}^\ell\}$ is a MAC for FIL.

Proof: Construction: $\text{Tag}(k, m) = F_k(m)$ for $k \leftarrow\$ \{0,1\}^\lambda$
$m \in \{0,1\}^n$

$\mathcal{A}(1^\lambda)$ $\qquad\qquad\qquad$ $\mathcal{C}(1^\lambda)$

$\xrightarrow{\quad m \quad}$ $k \leftarrow \$ \{0,1\}^\lambda$

$\xleftarrow{\quad \tau = F_k(m) \quad}$

OUTPUT 1 IF

$\xrightarrow{\quad m^*, \tau^* \quad}$ $F_K(m^*) = \tau^*$

m^* IS FRESH

We construct a $HYB(\lambda)$ where we pick a random function $R \leftarrow \$ \mathcal{R}(\lambda, n, \ell)$

$\mathcal{A}(1^\lambda)$ $\qquad\qquad\qquad$ $\mathcal{C}(1^\lambda)$

$\xrightarrow{\quad m \quad}$ $R \leftarrow \$ \mathcal{R}(\lambda, n, \ell)$

$\xleftarrow{\quad \tau = F_k(m) \quad}$ $\tau = R(m)$

OUTPUT 1 IF

$\xrightarrow{\quad m^*, \tau^* \quad}$ $\tau^* = R(m^*)$

m^* IS FRESH

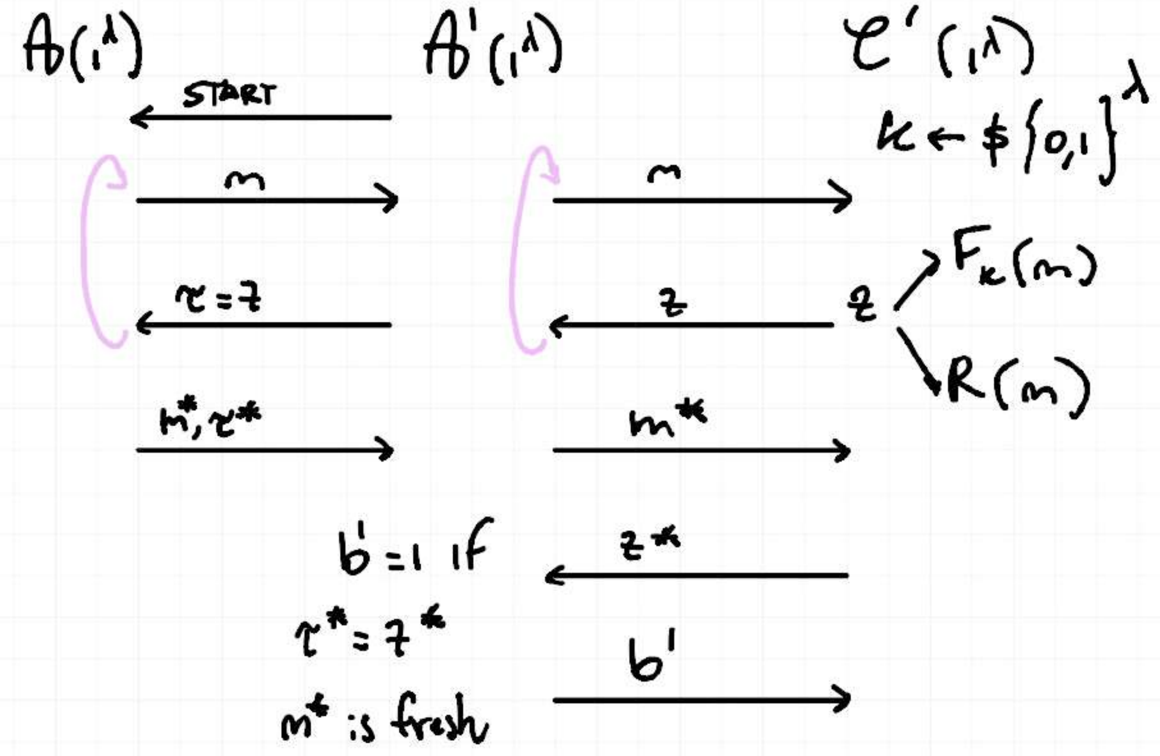
LEMMA: $\text{GAME}^{\text{ufcma}}_{\pi,\mathcal{A}} \approx_c HYB$, i.e. $\forall$ PPT $\mathcal{A}$

$$\left| \Pr[\text{GAME}^{\text{ufcma}}_{\pi,\mathcal{A}}(\lambda) = 1] - \Pr[HYB(\lambda) = 1] \right| \leq \text{negl}(\lambda)$$

Proof by reduction: Assume $\nexists$ PPT $\mathcal{A}$ such that

$$\left| \Pr[\text{GAME}(\lambda) = 1] - \Pr[HYB(\lambda) = 1] \right| \geq 1/\text{poly}(\lambda)$$

We show PPT $\mathcal{A}'$ against $\mathcal{F}$



Analysis: $\Pr[\text{REAL}_{\mathcal{F},\mathcal{A}'}(\lambda) = 1] = \Pr[\text{GAME}_{\Pi,\mathcal{A}}(\lambda) = 1]$

$\Pr[\text{RAND}_{\mathcal{F},\mathcal{A}'}(\lambda) = 1] = \Pr[\text{HYB}_{\Pi,\mathcal{A}}(\lambda) = 1]$

$\Rightarrow$ CONTRODDICTION!

(because $\mathcal{A}'$ breaks the definition of PRF)

<u>LEMMA</u> For all $\mathcal{A}$: $\Pr[\text{HYB}_{\Pi,\mathcal{A}}(\lambda) = 1] \leq 2^{-\ell}$

Follows by definition of HYB even if attacker is unbounded

Theorem follows by above lemmas + TRIANGLE INEQUALITY (so long as $\ell = \omega(\log \lambda)$)

What if $m = (m_1, m_2, \ldots, m_t)$ for $t \in \mathbb{N}$, $m_i \in \{0,1\}^n$

TRIVIAL SOLUTION: Design $\mathcal{F}$ with domain $\{0,1\}^{nt}$

Better solution: Assume $\mathcal{F} = \{F_k\}$ is fixed with domain $\{0,1\}^n$ and use it as a MAC for FIL/VIL domain $\{0,1\}^{n \cdot t}$, $Tag_k : \{0,1\}^n \to \{0,1\}^\ell$

EXERCISE: Decide if the following constructions work:

1) $m_i = \bigoplus_{i=1}^{t} m_i$ and $\tau = Tag(k, m)$

non ho capito un cazzo!

2) $\tau_i = Tag(k, m_i)$; $\tau = \tau_1 \| \tau_2 \dots \| \tau_t$

3) $\tau_i = Tag(k, i \| m_i)$ $\quad Tag : \{0,1\}^{n + \log t} \to \{0,1\}^\ell$

Say $t = 3$:
$$
\left.\begin{aligned}
m &= m_1 \| m_2 \| m_3 \, ; \; \tau = \tau_1 \| \tau_2 \| \tau_3 \\
m' &= m_1' \| m_2' \| m_3' \, ; \; \tau' = \tau_1' \| \tau_2' \| \tau_3' \\
m^* &= m_1 \| m_2' \| m_3 \, ; \; \tau^* = \tau_1 \| \tau_2' \| \tau_3
\end{aligned}\right\} \text{some kind of mix-n-match attack}
$$

SOLUTION: Design INPUT-SHRINKING FUNCTION
$$h_s : \{0,1\}^{nt} \to \{0,1\}^n$$
from a family $\mathcal{H} = \{h_s : \{0,1\}^{nt} \to \{0,1\}^n\}$

$$\Rightarrow \mathcal{F}(\mathcal{H}) : F_k(h_s(m)) \quad \begin{aligned} k &\leftarrow \$ \{0,1\}^\lambda \\ s &\leftarrow \$ \{0,1\}^\lambda \end{aligned}$$

What property from $\mathcal{H}$ we can extract to prove this generally? Note that for any valid (τ, m), τ is also valid for $m' \neq m$ such that $h_s(m') = h_s(m)$ collision

Approach 1: assume COLLISION is hard to find, even if S is public $\begin{pmatrix} \text{CRH} \\ \text{not in MINICRYPT} \end{pmatrix}$ collision-resistant hash function

Approach 2: Let s be secret!

<u>DEFINITION:</u> We say $\mathcal{H}$ is ε-ALMOST UNIVERSAL (AU) if

$$\Pr_{s \leftarrow \$ \{0,1\}^\lambda} \left[h_s(m) = h_s(m') \right] \leq \varepsilon$$

$$\forall m, m' \in \{0,1\}^{nt} \text{ with } m \neq m'$$

In general, $\varepsilon = \text{negl}(\lambda)$, with $\varepsilon = 2^{-\ell}$ we say $\mathcal{H}$ is PERFECTLY UNIVERSAL

<u>THM</u>: If $\mathcal{F}$ is a PRF for domain $\{0,1\}^n$

If $\mathcal{H}$ is AU

Then $\mathcal{F}(\mathcal{H})$ $\rightarrow \mathcal{F}^*$ is a PRF (and thus a MAC) with domain $\{0,1\}^{nt}$

Proof: We consider two experiments:

$\text{REAL}_{\mathcal{F}^*, \mathcal{A}}(\lambda)$

$\mathcal{A}(1^\lambda)$ $\qquad\qquad$ $\mathcal{C}(1^\lambda)$

$\xrightarrow{\quad x \quad}$ $k, s \leftarrow \$ \{0,1\}^\lambda$

$\xleftarrow{\quad y \quad}$ $y = F_k(h_s(x))$

$\xrightarrow{\quad b' \quad}$

$\mathrm{RAND}_{\mathcal{F}^*,\mathcal{A}}(\lambda)$

$$\begin{array}{ccl}
\mathcal{A}(1^\lambda) & & \mathcal{C}(1^\lambda) \\
 & \xrightarrow{\quad x \quad} & R^* \leftarrow \$ \, \mathcal{R}(\lambda, nt, \ell) \\
 & \xleftarrow{\quad y \quad} & y = R^*(x) \\
 & \xrightarrow{\quad b' \quad} &
\end{array}$$

We also construct a $\mathrm{HYB}_{\mathcal{F}^*,\mathcal{A}}$

$$\begin{array}{ccl}
\mathcal{A}(1^\lambda) & & \mathcal{C}(1^\lambda) \\
 & \xrightarrow{\quad x \quad} & s \leftarrow \$ \, \{0,1\}^\lambda \\
 & \xleftarrow{\quad y \quad} & R \leftarrow \$ \, \mathcal{R}(\lambda, n, \ell) \\
 & \xrightarrow{\quad b' \quad} & y = R(h_s(x))
\end{array}$$

LEMMA: $\{\mathrm{REAL}_{\mathcal{F}^*,\mathcal{A}}(\lambda)\} \approx_c \{\mathrm{HYB}_{\mathcal{F}^*,\mathcal{A}}(\lambda)\}$

statistically close

LEMMA: $\{\mathrm{HYB}_{\mathcal{F}^*,\mathcal{A}}(\lambda)\} \approx_s \{\mathrm{RAND}_{\mathcal{F}^*,\mathcal{A}}(\lambda)\}$

(I claim that even an all-powerful adv. can't distinguish HYB from RAND)

PROOF: Define event BAD in the HYB experiment

$$\exists\, i,j \in [q] \mid h_s(x_i) \neq h_s(x_j)$$

So long as BAD doesn't happen, R is called upon a series of distinct $h_s(x_1), h_s(x_2), \dots, h_s(x_q)$

$\Rightarrow$ HYB $\equiv$ RAND

By a previous lemma, we just need to show

$$\Pr[\text{BAD}] \leq \text{negl}(\lambda)$$

We define a new experiment such that we can use AU.

$\mathcal{A}(\cdot, \lambda)$ $\qquad\qquad$ $\mathcal{C}(\cdot, \lambda)$

$\xrightarrow{\quad x \quad}$ $\quad y_i \leftarrow \$ \{0,1\}^{\ell}$

$\xleftarrow{\quad y \quad}$ $\quad \forall i \in [q]$

$\xrightarrow{\quad b' \quad}$ $\quad s \leftarrow \$ \{0,1\}^{\lambda}$

check BAD

$\exists i, j$ such that $h_s(x_i) = h_s(x_j)$

Until BAD doesn't happen, HYB and the new experiment are the same!

$$\Pr[\text{BAD in HYB}] = \Pr[\text{BAD in new}]$$

$$\Pr[\text{BAD in new}] = \Pr_{s \leftarrow \$ \{0,1\}^{\lambda}}[\exists i, j \in [q] : h_s(x_i) = h_s(x_j)]$$

$$\leq \sum_{\substack{i,j=1 \\ i \neq j}}^{q} \Pr[h_s(x_i) = h_s(x_j)] \leq \binom{q}{2} \text{negl} = \text{negl}(\lambda)$$

if $q = \text{poly}(\lambda)$

CONSTRUCTION of AU families

1) Take $\mathbb{F} = GF(2^n)$ let $m = m_1, m_2, \dots, m_t$

$m_i \in \{0,1\}^n$

Seed is $s = a_1, a_2, \dots, a_t \in \mathbb{F}$

$$h_s(m) = h_{a_1,a_2,\dots,a_t}(m) = \sum_{i=1}^{t} a_i m_i$$

Proof of AU: Take $m = m_1 \dots m_t$

$m' = m_1' \dots m_t'$

and let $\delta_i = m_i' - m_i$

$\forall m \neq m'$ $\exists i$ such that $\delta_i \neq 0$

n_{log} let $i = 1$ sol $\delta \neq 0$

In order to have a collision

$$h_s(m) = \sum a_i m_i = \sum a_i m_i' = h_s(m_i')$$

$$\Rightarrow a_1 \delta_1 = -\sum_{i=2}^{t} a_i \delta_i$$

$$\Rightarrow a_1 = \frac{-\sum_{i=2}^{t} a_i \delta_i}{\delta_1}$$

$$\Rightarrow \Pr_{s \leftarrow \$ \{0,1\}^\lambda}\left[h_s(m) = h_s(m_i) \right] \leq 2^{-n}$$

<u>EX</u>: Show following $\mathcal{H}$ is AU

$\mathbb{F} = GF(2^n)$; $m = m_1 \| \dots \| m_t$

seed is $s \leftarrow \$ \mathbb{F}$

$$h_s(m) = \sum_{i=1}^{t} m_i \cdot s^{i-1}$$

$$q_m(X) = \sum_{i=1}^{t} m_i \cdot X^{i-1}$$