We have $\Pi_1 = (\text{Enc}, \text{Dec}) \Rightarrow$ CPA-secure

$\Pi_2 = \text{Tag} \Rightarrow$ UF-CMA

$\Pi = (\text{Enc}, \text{Dec})$; $k = (k_1, k_2)$

$\text{Enc}(k, m) = (c, \tau)$ $\quad c \leftarrow \$ \, \text{Enc}(k_1, m)$

$\tau = \text{Tag}(k_2, c)$

$\text{Dec}(k, (c, \tau))$: If $\text{Tag}(k_2, c) = \tau$

output $\text{Dec}(k_1, c)$

Else output $\perp$

<u>THM</u>: Above SKE Π is CCA-Secure.

Proof: Suffices to show that Π has both the properties of CPA and AUTH.

1) Π is CPA secure.

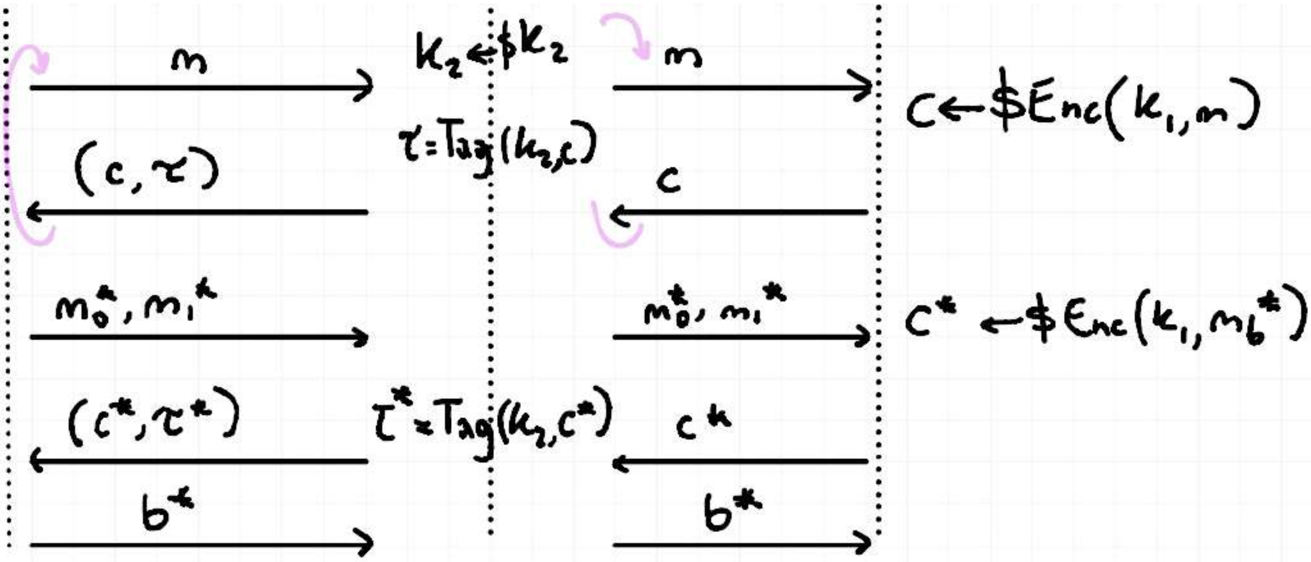
Assume not: $\exists$ PPT A s.t.

$$\left| \Pr\left[\text{GAME}^{cpa}_{\Pi, A}(\lambda, 1) = 1 \right] - \Pr\left[\text{GAME}^{cpa}_{\Pi, A}(\lambda, 0) = 1 \right] \right| \geq \frac{1}{\text{poly}(\lambda)}$$

Build PPT A_1 attacking Π_1

$A(1^\lambda)$ $\qquad$ $A_1(1^\lambda)$ $\qquad$ $\mathcal{C}$

$\xleftarrow{\text{"START"}}$ $\qquad$ $k_1 \leftarrow \$ \, \mathcal{K}_1$



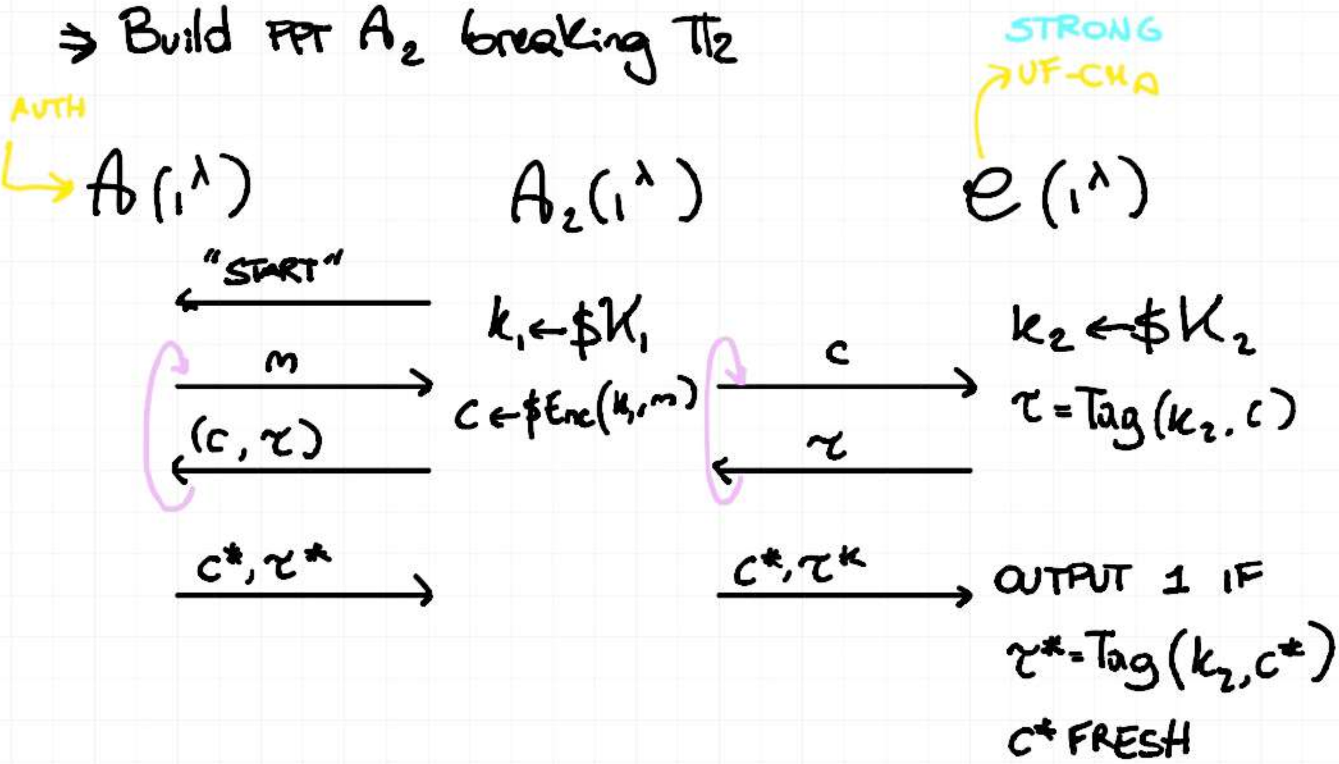
Analysis is immediate.

2) AUTH

Assume not: $\exists$ PPT A such that

$$\Pr\left[\mathrm{GAME}^{auth}_{\Pi, A}(\lambda) = 1\right] \geq \frac{1}{poly(\lambda)}$$

$\Rightarrow$ Build PPT A_2 breaking Π_2



Can we claim c^* is fresh?

With $Pr \geq 1/poly(\lambda)$ A forgery c^*, τ^* is such that

$$(c^*, \tau^*) \neq (c, \tau) \ \forall \text{ query}$$

non imlica $\Rightarrow c^* \neq c \ \forall$ query!

Analysis is STRAIGHTFORWARD.

STRONG UF-CMA: Easy to show: Deterministic and Unique tags. UFCMA $\rightarrow$ STRONG UF-CMA

CBC-MAC has this property

Hash Functions

Let $\mathcal{H} = \{H_s : \{0,1\}^{\ell(\lambda)} \rightarrow \{0,1\}^{n(\lambda)}\}_{s \leftarrow \$ \{0,1\}^\lambda}$

with $\ell(\lambda) \gg n(\lambda)$.

We want COLLISION RESISTANCE, meaning collisions exist but are hard to find.

- SECRET SEEDS (universal hash functions)
- PUBLIC SEEDS (collision-resistant hash function) MD5 SHA-1, 2, 3

Why public seed? Because no need for sharing keys.
The price to pay: computational assumptions (INHERENT)

$$\text{GAME}^{CRH}_{\mathcal{H}, A}(\lambda)$$

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

$\xleftarrow{\quad s \quad}$ $\quad s \leftarrow\$ \{0,1\}^\lambda$

↳ pick a function from $\mathcal{H}$

$\xrightarrow{\quad x, x' \quad}$

OUTPUT 1 if

$x \neq x'$

$H_s(x) \neq H_s(x')$

uguale

<u>DEF</u>: Family $\mathcal{H}$ is a CRH family if $\forall$ PPT $\mathcal{A}$

$$\Pr\left[\mathrm{GAME}^{CRH}_{\mathcal{H},\mathcal{A}}(\lambda) = 1\right] \leq \mathrm{negl}(\lambda)$$

EX: Remember $\mathcal{F}(\mathcal{H})$ for DOMAIN EXTENSION of PRFs.

a. Show that the above construction doesn't work in general if $\mathcal{H}$ is UNIVERSAL (secret seed) and if $\mathcal{F}$ is a UF-CMA Tag (i.e. $\mathrm{Tag}(k, h_s(m))$ NOT necessarily UF-CMA for large inputs)

b. $\mathrm{Tag}(k, H_s(m))$ is UF-CMA if $H_s \in \mathcal{H}$ CRH family

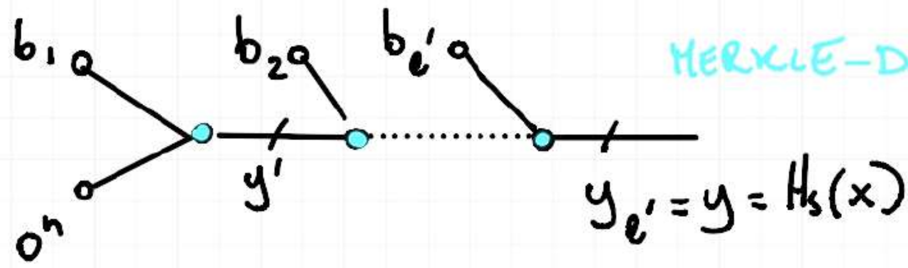
Recipe for CRH Families:

1) Build compression function $\ell \to n$ (such as CRH but with small compression for FIL m)

2) Bootstrap compression to $\ell' \to n$ with $\ell' \gg n$

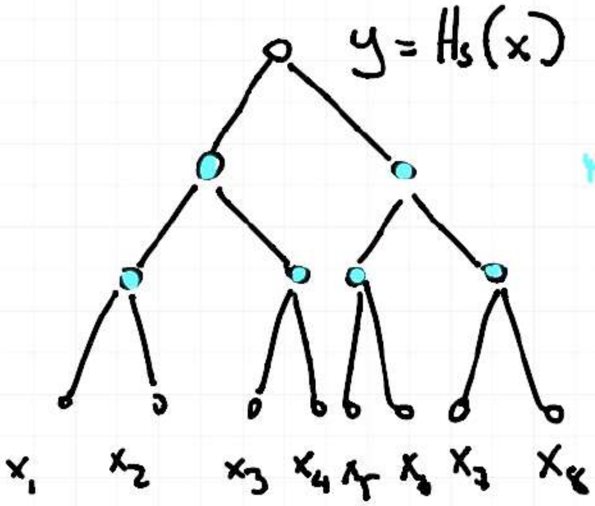
either for FIL or VIL messages

Start with ②. Two options for design:



MERKLE–DAMGAARD

$\bullet : H'_s : \{0,1\}^{n+1} \longrightarrow \{0,1\}^n$ minimal compression function



MERKLE TREE

used in bitcoin

wow such crypto

$\bullet : H'_s : \{0,1\}^{2n} \to \{0,1\}^n$

$\ell' = 2^{d} \cdot n \longrightarrow n$ (d = depth)

<u>THM</u>: The MD construction gives a CRH $\mathcal{H}'$ from

$\ell'(\lambda)$ bits to $n(\lambda)$ bits, assuming $\mathcal{H}$ is CRH from $n+1 \to n$.

Proof: Let A' be a PPT adversary that given s outputs

$$x = (b_1, \ldots, b_{l'}) \neq (b'_1, \ldots, b'_{l'}) = x'$$

such that $H'_s(x) = H'_s(x')$ with probability $1/poly(\lambda)$

Let j be the largest index such that

$(b_j, y_{j-1}) \neq (b'_j, y'_{j-1})$. Since j is the largest index

and A outputs a collision

$$H_s(b_j \| y_{j-1}) = H_s(b'_j \| y'_{j-1})$$

$\Rightarrow$ This immediately give reduction $A(s)$

$$A'(1^\lambda) \qquad\qquad A(1^\lambda) \qquad\qquad C(1^\lambda)$$

$$A'(1^\lambda) \xleftarrow{\;s\;} A(1^\lambda) \xleftarrow{\;s\;} C(1^\lambda)$$

$$A'(1^\lambda) \xrightarrow{\;x, x'\;} A(1^\lambda)$$

$A(1^\lambda)$: Let $b_1, \ldots, b_{l'}$, $b'_1, \ldots, b'_{l'}$, $y_1, \ldots, y_{l'}$, $y'_1, \ldots, y'_{l'}$ and j be as above

$$A(1^\lambda) \xrightarrow{\;(b_j \| y_{j-1},\, b'_j \| y'_{j-1})\;} C(1^\lambda)$$

But this is not secure for VIL (show this in exercise)

<u>Ex</u>: Give example of bad CRH $\mathcal{H}$ such that MD is not secure for VIL.

Let $\mathcal{H}$ be such that $H_s(0^{n+1}) = 0^n \; \forall s \in \{0,1\}^\lambda$

Problem: $\forall x : H_s(0^n \| x) = H_s(x)$

It is possible to fix this through SUFFIX-FREE encoding of x.

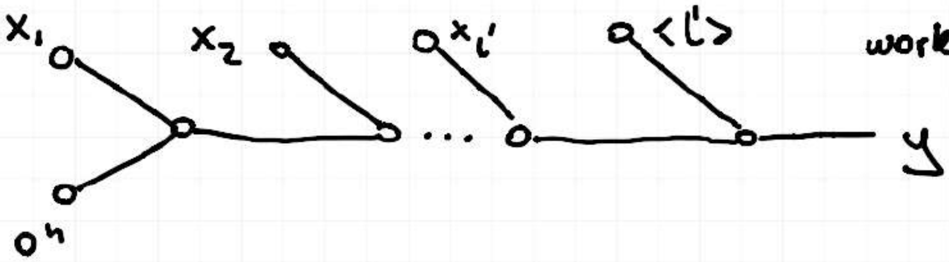
Namely, pick input so that no legal x is a SUFFIX of another input $x' \neq x$

Let $<l>$ be the representation of the length of x

$$H'_s(x) = H_s(<l>, H_s(x_{l'}, \dots H_s(x_1, 0^n)\dots))$$

where $H_s : \{0,1\}^{n+c} \to \{0,1\}^n$ for $c \geq 1$

$x = (x_1, \dots, x_{l'})$ with $|x_i| = c$



works for $l' \leq 2^c$

<u>THM</u> The above strengthening of MD is CRH for VIL.

<u>Proof</u> Let $x = x_1, \dots x_{l'}$ and $x' = (x'_1, \dots, x'_{l''})$ be a collision for $\mathcal{H}'$.

There are two cases

1) $l' = l''$.

As in the previous proof for FIL we can build a reduction to CRH $\mathcal{H}$.

2) $l' \neq l''$

But notice that

$$H_s(y_{l'}, \langle l' \rangle) = H'_s(x) = H_s(y'_{l''}, \langle l'' \rangle)$$

But $\langle l' \rangle \neq \langle l \rangle \Rightarrow$ COLLISION!

How to get compression functions?

THEORY	PRACTICE
· OWF? Impossible...	· AD-HOC DESIGN SHA1, 2, 3, MD5
· NUMBER THEORY	· $H(x_1 \| x_2) = AES(x_1, x_2) \oplus x_2$
· CLAW-FREE permutation	

But why do we ever need the seed?