Example reduction

Claim Suppose m_1 is UNF-CMA secure MAC-scheme. Now m_2 is also UNF-CMA secure, where

$m_2.mac(k,x) = m_1.mac(k,x) \| 1$

$m_2.verify(k,x,t)$:

$t' \| b \leftarrow t$ where $|b| = 1$, $t_{|t|} = b$

if $b \neq 1$

return 0

return $m_1.verify(k,x,t')$

proof:

Assume m_1 is secure.

For contr. assume m_2 is not secure

i.e. $\exists$ PPT $\mathcal{A}$ s.t.

$$\left| Pr\left[1 = \mathcal{A} \rightarrow Guf\text{-}cma^0_{m_2}\right] - Pr\left[1 = \mathcal{A} \rightarrow Guf\text{-}cma^1_{m_2}\right] \right| = \text{non-negl.}$$

Let's define $\mathcal{B}$ that interacts with $Guf\text{-}cma_{m_1}$

$\mathcal{B}$:

$MAC_{\mathcal{B}}(x)$:

$t \leftarrow MAC(x)$

$t' \leftarrow t \| 1$

return t'

$VERIFY_{\mathcal{B}}(x,t)$:

$t' \| b \leftarrow t$

if $b \neq 1$

return 0

$d \leftarrow VERIFY(x,t')$

return d

Now $\mathcal{A} \to \mathcal{B} \to \text{Gunf-cma}_{m_1}$ is code equivalent to $\mathcal{A} \to \text{Gunf-cma}_{m_2}$

Case $\mathcal{O}$

Now $\mathcal{A} \to \mathcal{B} \to \text{Gunf-cma}^{\mathcal{O}}_{m_1}$ is code equivalent to $\mathcal{A} \to \text{Gunf-cma}^{\mathcal{O}}_{m_2}$

in $\mathcal{B} \to \text{Gunf-cma}^{\mathcal{O}}_{m_1}$

$\underline{\text{MAC}_{\mathcal{B}}(x)}$:

$t \leftarrow \text{MAC}(x)$

$t' \leftarrow t \| 1$

return t'

if $k = \perp$: $k \leftarrow \$\{0,1\}^\lambda$; $t \leftarrow m_1.\text{mac}(k, x)$

$\Rightarrow$

$\underline{\text{MAC}_{\mathcal{B}}(x)}$:

$t \leftarrow \text{MAC}(x)$

$t' \leftarrow t \| 1$

return t'

$\Leftrightarrow$

$\underline{\text{MAC}_{\mathcal{B}}(x)}$:

if $k = \perp$: $k \leftarrow \$\{0,1\}^\lambda$

$t \leftarrow m_1.\text{mac}(k, x)$

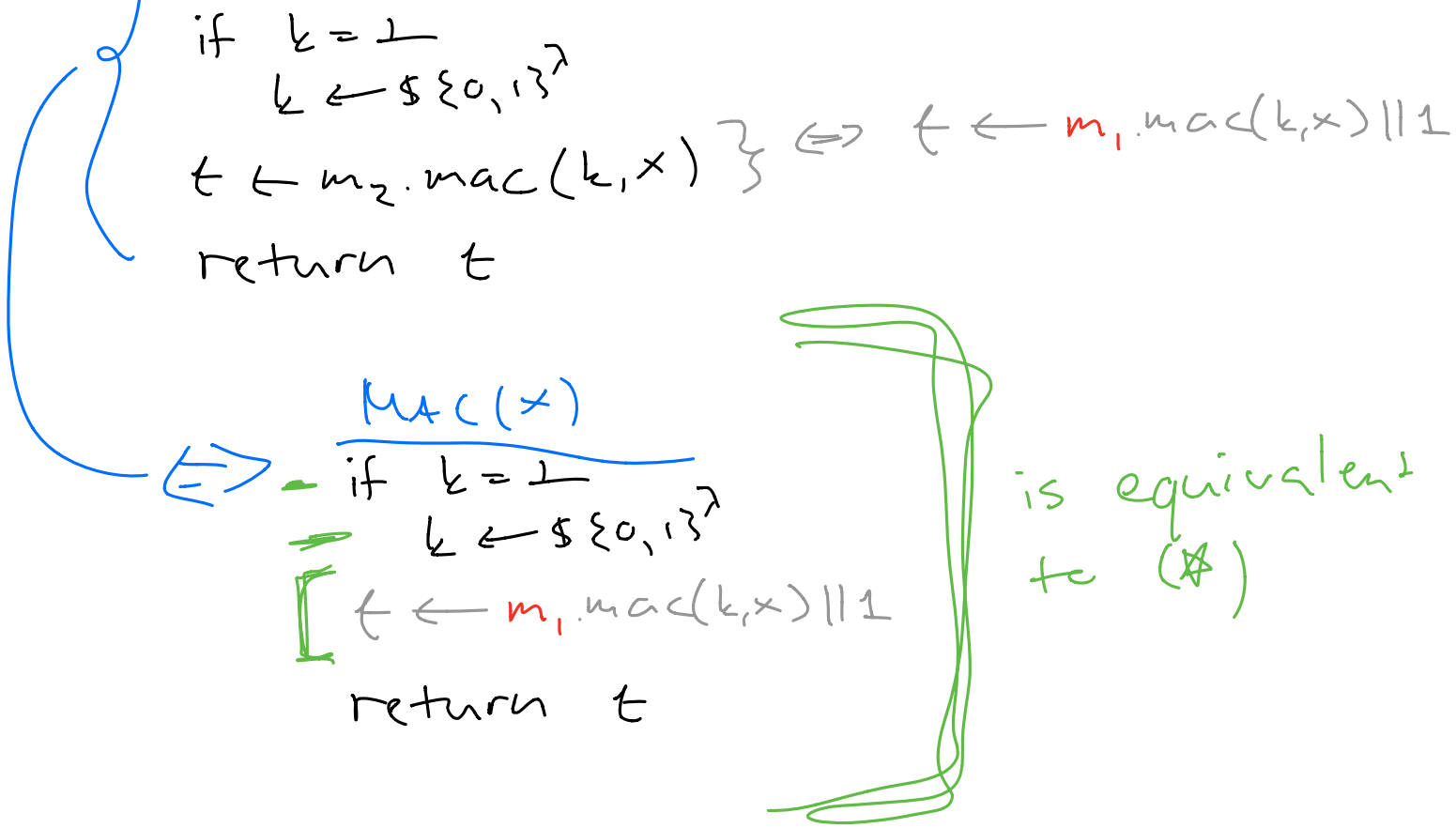
$t' \leftarrow t \| 1$

return t'

(*)

in $\mathcal{A} \to \text{Gunf-cma}^{\mathcal{O}}_{m_2}$

$\underline{\text{MAC}(x)}$:



TODO:

prove that

Now $\mathcal{A} \to \mathcal{B} \to \text{Gunf-cma}'_{m_1}$ is code equivalent to $\mathcal{A} \to \text{Gunf-cma}'_{m_2}$

and show that

$\text{VERIFY}_{\mathcal{B}}$ when $\mathcal{B}$ is interacting with $\text{Gunf-cma}^{0}_{m_1}$ is code equivalent to VERIFY of $\text{Gunf-cma}^{0}_{m_2}$.

Now $\mathcal{A} \to \mathcal{B} \to \text{Gunf-cma}_{m_1}$ is code equivalent to $\mathcal{A} \to \text{Gunf-cma}_{m_2}$

$$\left| \Pr\left[1 = \underbrace{\mathcal{A} \to \text{Gunf-cma}^0_{m_2}}_{\equiv \text{ code } \mathcal{A} \to \mathcal{B} \to \text{Gunf-cma}^0_{m_1}}\right] - \Pr\left[1 = \underbrace{\mathcal{A} \to \text{Gunf-cma}^1_{m_2}}_{\equiv \text{ code } \mathcal{A} \to \mathcal{B} \to \text{Gunf-cma}^1_{m_1}}\right] \right| = \text{non-negl.}$$

$\Downarrow$

$$\left| \Pr\left[1 = \mathcal{A} \to \mathcal{B} \to \text{Gunf-cma}^0_{m_1}\right] - \Pr\left[1 = \mathcal{A} \to \mathcal{B} \to \text{Gunf-cma}^1_{m_1}\right] \right| = \text{non-negl.}$$

Now $\mathcal{A} \to \mathcal{B}$ can distinguish $\text{Gunf-cma}^0_{m_1}$ and $\text{Gunf-cma}^1_{m_1}$

↯ (because m_1 was secure) □