Applications of IBE

1) CCA2-SECURE PKE

Ingredients:

a) selective IND-ID-CPE IBE

$\Pi = (Setup, KGen, Enc, Dec)$

b) strongly UF-CMA 1-TIME Signature

$\Pi' = (Kgen', Sign, Vrfy)$

Construction of a PKE $\Pi'' = (Kgen'', Enc'', Dec'')$

$Kgen''(1^\lambda)$: $(mpk, msk) \leftarrow\$ Setup(1^\lambda)$

$ek = mpk, \quad dk = msk$

$Enc''(ek, m)$: Sample $(vk, sk) \leftarrow Kgen'(1^\lambda)$
s.t. $|vk| = n(\lambda)$ where $\{0,1\}^n$ is the ID space of IBE.

Output $C'' = (c, vk, \sigma)$
$c \leftarrow\$ Enc(mpk, vk, m)$ i.e. $ID = vk$
$\sigma \leftarrow\$ Sign(sk, c)$ fresh everytime

$Dec''(dk, c'')$: Check $Vrfy(vk, c, \sigma) = 1$
if not return $\perp$ bottom

else return $\mathrm{Dec}(d_{vk}, c)$
where $d_{vk} \leftarrow \mathrm{KeyGen}(msk, vk)$

THM: The above is CCA2-secure

Proof: Intuition for answering Dec queries:

A Dec query $c = (c, vk, \sigma)$ either satisfies $vk = vk^*$

$(c^*, vk^*, \sigma^*) \leftarrow$ CHALLENGE CTX

or $vk \neq vk^*$

If $vk = vk^*$ the answer should be $\perp$.
If $vk \neq vk^*$ then we are decrypting c under a different identity.

Let A'' be a PPT attacker for CCA2-SECURITY.
Say (c, vk, σ) is valid if $\mathrm{Vrfy}(c, vk, \sigma) = 1$.
Let (c^*, vk^*, σ^*) be the challenge. Note $\mathcal{C}$ can sample vk^* at the very beginning of the GAME.

Define event FORGE: A'' submits a Dec query (c, vk, σ) that is valid and for which $vk = vk^*$

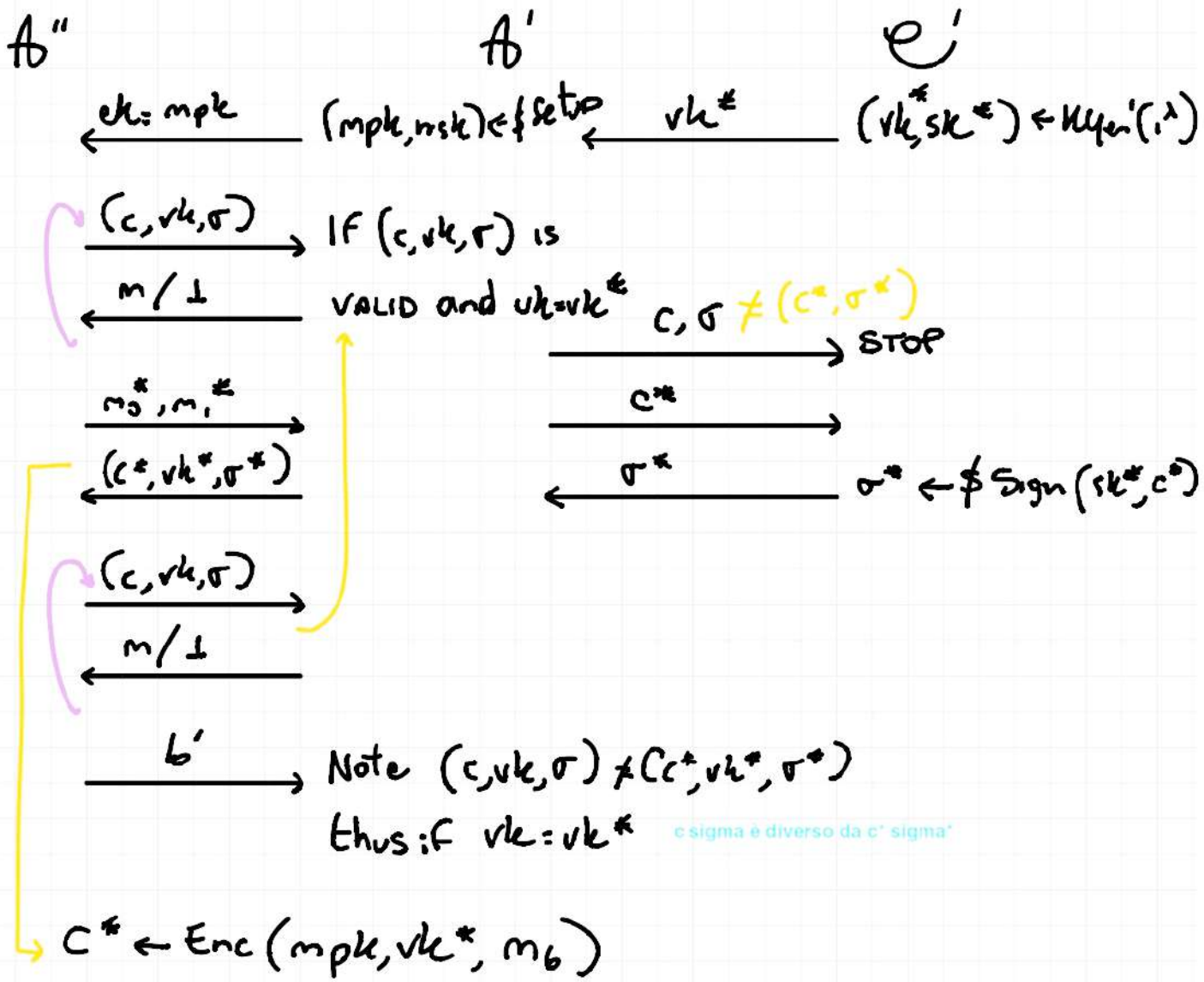
$$\left| \Pr\left[\mathrm{GAME}^{CCA}_{\Pi'', A''}(\lambda, 0) = 1 \right] - \Pr\left[\mathrm{GAME}^{CCA}_{\Pi'', A''} = 1 \right] \right| \leq$$

$$\leq \Pr[\mathrm{Forge}] + \left| \Pr\left[\mathrm{GAME}^{CCA}_{\Pi'', A''}(\lambda, 0) = 1 \mid \overline{\mathrm{FORGE}} \right] - \right.$$

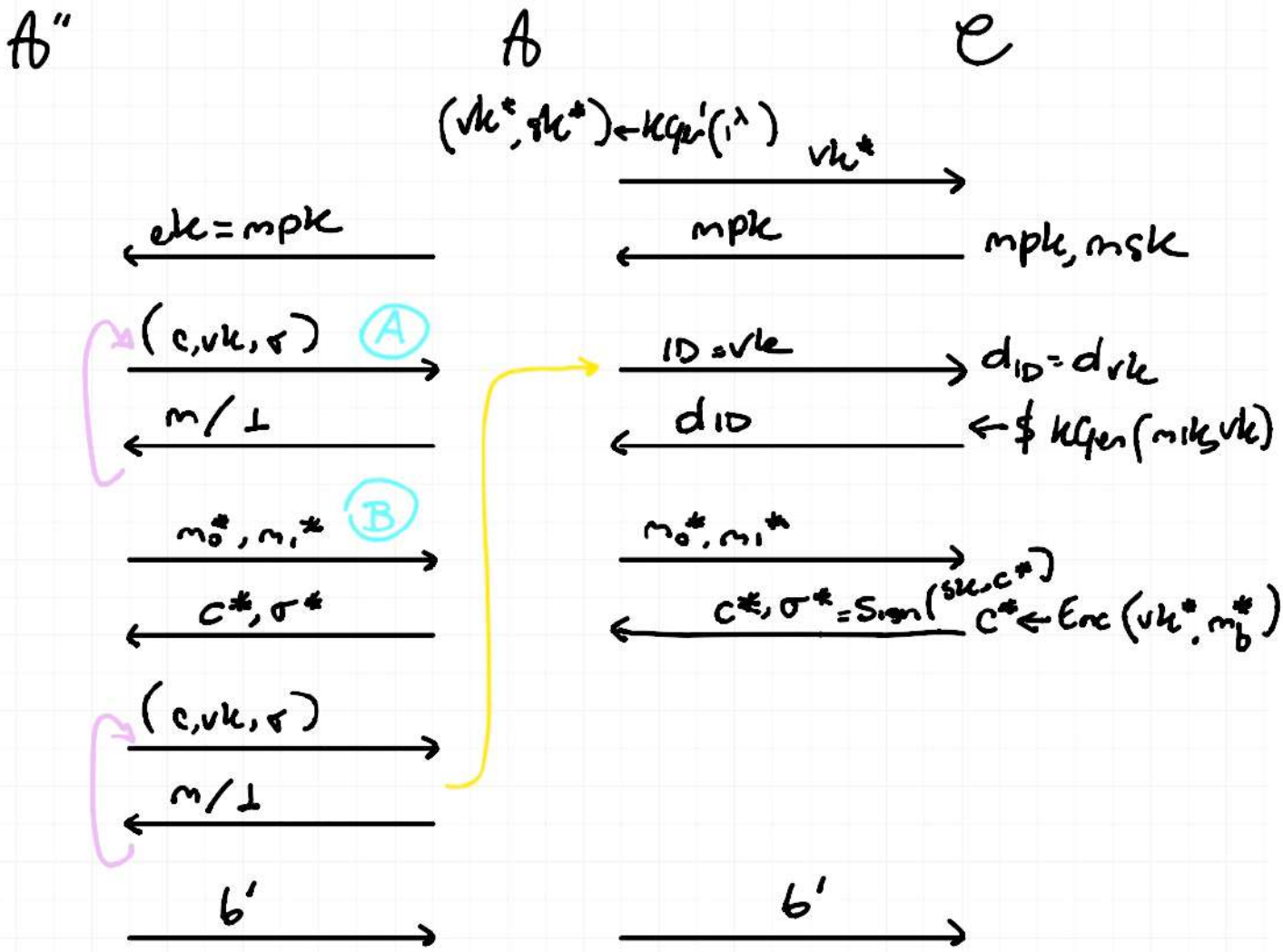
$$\left. - \Pr[\mathrm{GAME}(\lambda, 1) = 1 \mid \overline{\mathrm{FORGE}}] \right|$$

LEMMA : ① and ② are negligible.

① Assume NOT: $\exists$ PPT A'' that provokes event FORGE w.p. $\geq 1/poly$
Build reduction A' to strong UF-CMA of Π'.



② Let A be a PPT adversary distinguishing in the CCA-2 experiment when $\overline{\text{FORGE}}$
Build reduction A to selective IND-ID-CPA IBE



(A) Decription queries (c, vk, σ):

First check $Vrfy(vk, c, \sigma) = 1$. If not, $\perp$.

Else if $vk = vk^*$, ABORT, (happens with negl pr)

if $vk \neq vk^*$ query vk to $\mathcal{C}'$ and obtain d_{ID} and output $m = Dec(d_{ID}, c)$

(B) Challenge CTX

Trivial. You idiot.

2) Signatures from IBE

Let $\Pi = (\text{Setup}, \text{KGen}, \text{Enc}, \text{Dec})$ be an IBE. Consider $\Pi' = (\text{KGen}', \text{Sign}, \text{Vrfy})$.

$\underline{\text{KGen}'(1^\lambda)}$: $(mpk, msk) \leftarrow\$ \text{Setup}(1^\lambda)$

$vk = mpk$; $sk = msk$

$\underline{\text{Sign}(sk, m)}$: $d_m \leftarrow\$ \text{KGen}(sk = msk, ID = m)$

$\sigma = d_m$

$\underline{\text{Vrfy}(vk, m, \sigma)}$: Let $m = ID$ and $\sigma = d_{ID}$.

Pick $\mu \leftarrow\$ \mathcal{M}_{IBE}$

Encrypt $c \leftarrow \text{Enc}(ID, \mu)$

Check that $\text{Dec}(\sigma, c) = \mu$.

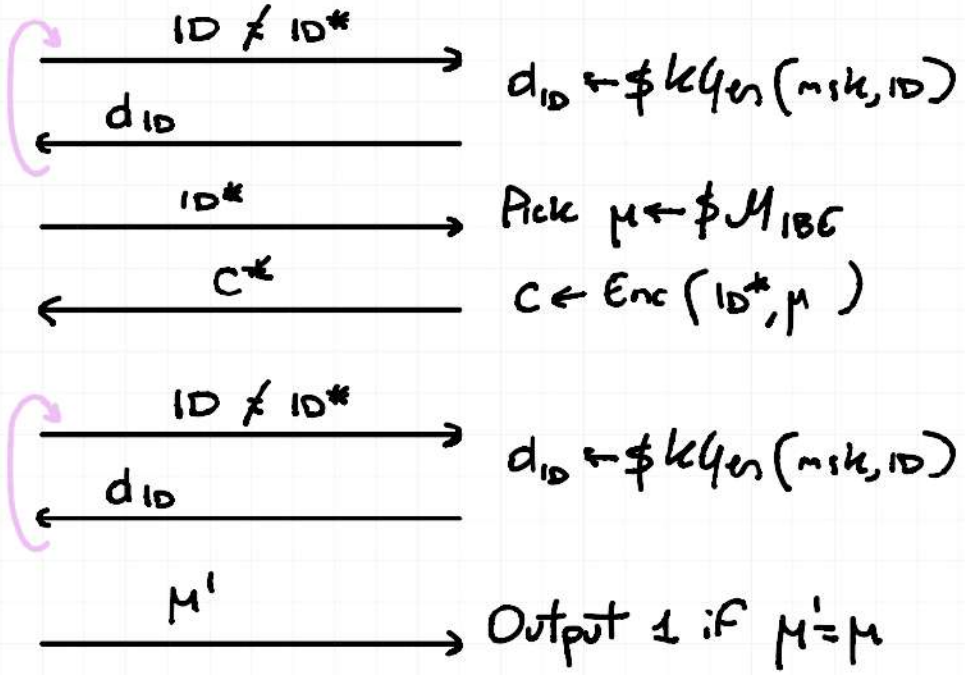
THM Assuming Π is IND-ID-CPA, then Π' is UF-CMA so long as $|\mathcal{M}_{IBE}| = \omega(\log \lambda)$.

Proof: We will rely on this property of IBE called OW-IND-CPA.

$\text{GAME}^{\text{ow-id-cpa}}_{\Pi,\mathcal{A}}$

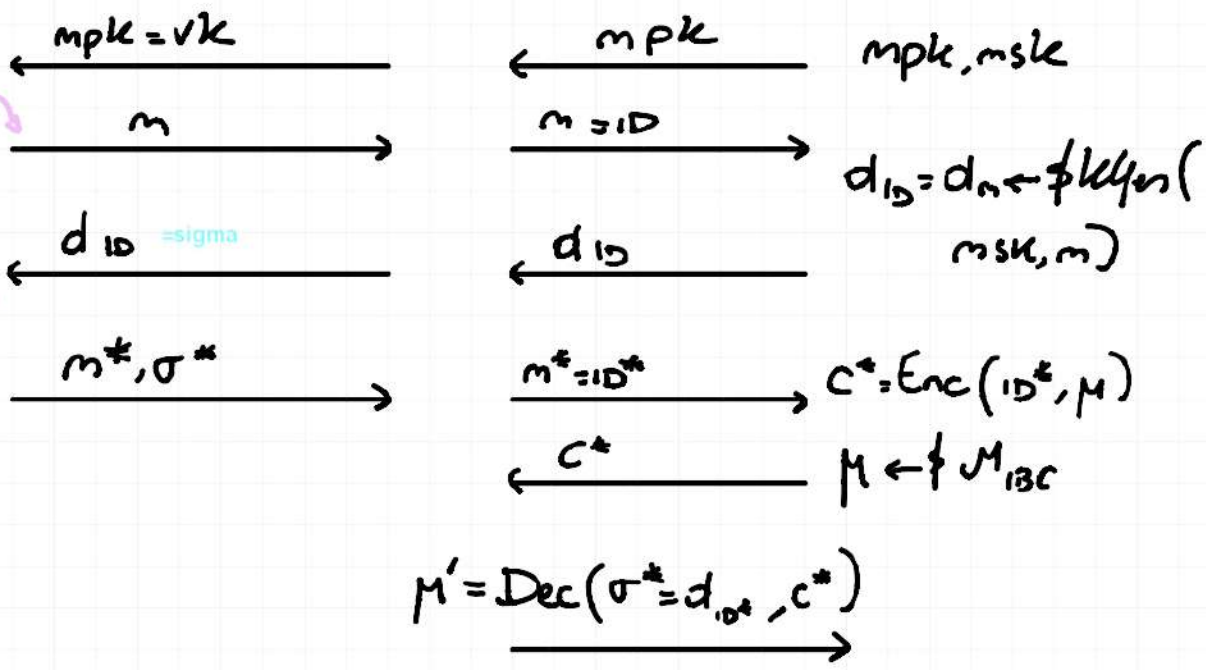
$\mathcal{A}(1^\lambda)$ $\qquad$ $\mathcal{C}(1^\lambda)$

$\xleftarrow{mpk}$ $\qquad$ $(mpk, msk) \leftarrow\$ \text{Setup}(1^\lambda)$



Exercise: IND-ID-CPA $\Rightarrow$ OW-ID-CPA when $|\mathcal{M}_{IBE}| = \omega(\log \lambda)$

Assume $\exists$ PPT A' breaking UF-CMA. Build reduction A against OW-ID-CPA



$Pr[\mu' = \mu] = Pr[Vrfy(vk, m^*, \sigma^*) = 1] \geq 1/poly$