FIAT - SHAMIR

We will now show that in the ROM, PASSIVE ID schemes (CANONICAL) $\Rightarrow$ UF-CMA SIGNATURES.

$\Pi = (\text{Gen}, \mathcal{P}, \mathcal{V})$

$\text{KGen}(1^\lambda) = \text{Gen}(1^\lambda) \leftarrow (pk, sk)$

$\text{Sign}(sk, m)$: - Generate α using $\mathcal{P}(pk, sk)$
- Let $\beta = H(\alpha \| m)$
- Get γ from $\mathcal{P}(pk, sk)$

- Output $\sigma = (\alpha, \gamma)$

Vrfy$(pk, m, \sigma = (\alpha, \gamma))$: let $\beta := H(\alpha \| m)$

Output same as $V(pk, (\alpha, \beta, \gamma))$

THM The Fiat-Shamir transform gives UF-CMA signatures in the ROM, assuming the ID scheme is passively secure.

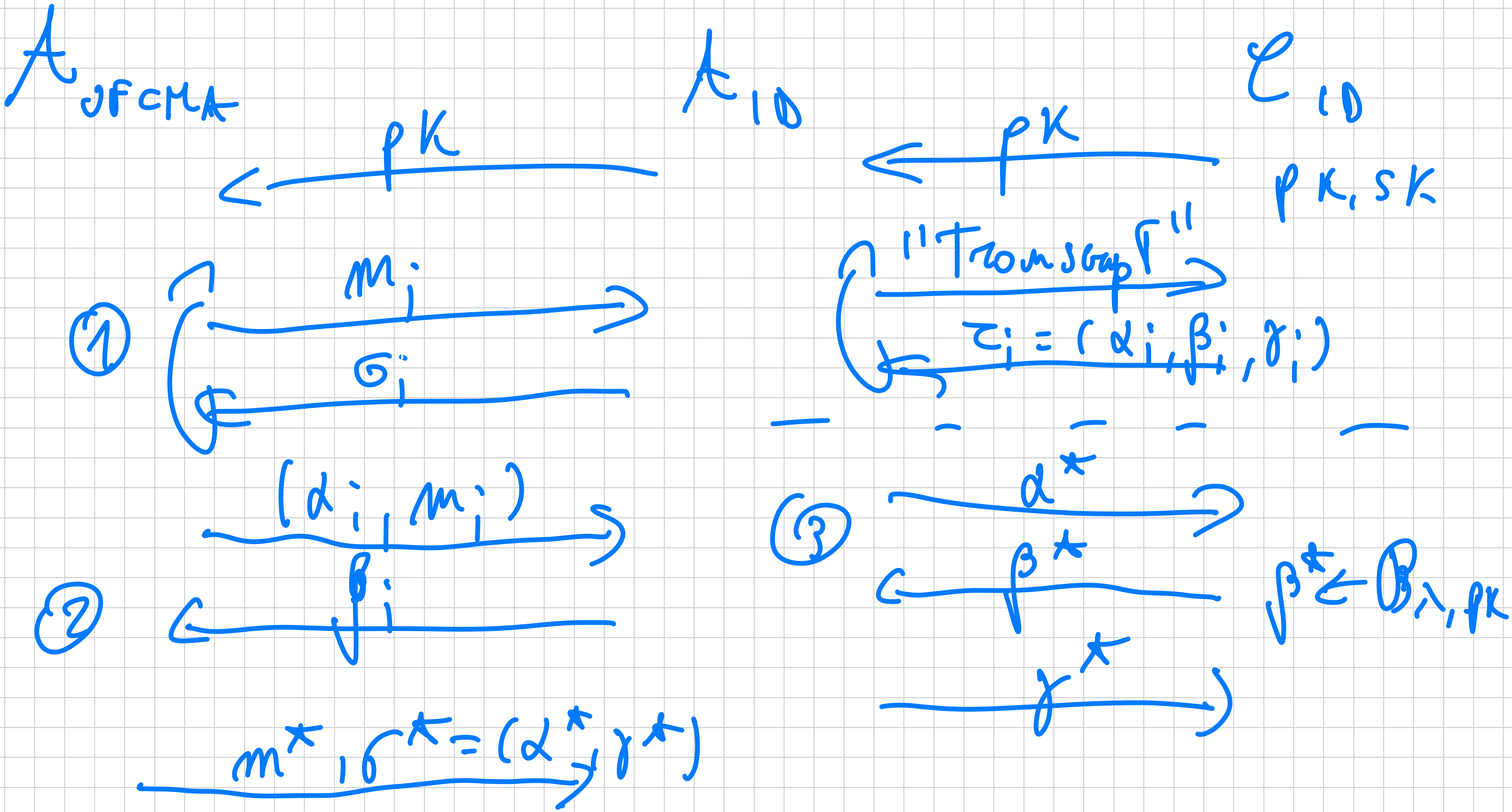
Proof. The proof will use similar ideas as the proof for FDH. The UF-CMA adversary A can make 2 kind of queries:

- RO queries (α_i, m_i) (# queries $= q_h = poly(\lambda)$)
- sign queries m_i (# queries $= q_s = poly(\lambda)$)

Wlog, we make a few assumptions on $\mathcal{A}$:

- It does not repeat RO queries.
- If $\mathcal{A}$ makes a signature query m and gets $\sigma = (\alpha, \gamma)$, then it already queried the RO on (α, m).
- The same for forgery $m^*, \sigma^* = (\alpha^*, \gamma^*)$, the $\mathcal{A}$ made a RO query of the form (α^*, m^*).

We can now describe the reduction.



- Similar to the proof for FDH the reduction tries to guess the RO query corresponding

To the forgery m^*. Let's say it samples $i \leftarrow [q_h]$.

- Next, A_{ID} makes q_s "transcript queries" and obtains $\tau_1 = (\alpha_1, \beta_1, \gamma_1), \dots, \tau_{q_s} = (\alpha_{q_s}, \beta_{q_s}, \gamma_{q_s})$
- Upon input a RO query (m_j, α_j) from A_{UFCMA}:
  - If $j \neq i$, then return $\beta_j \leftarrow B_{\lambda, pk}$.
  - If $j = i$, it will start step ③ and forward α_i to $\mathcal{C}_{ID}$.

$$\alpha_i = \alpha^*$$

Then, return β^* to A_{UFCMA}.

- Upon a signature query m_i from A_{UFCMA} the idea is to return $\sigma_i = (\alpha_i, \gamma_i)$ where α_i, γ_i are from τ_i.
There could be a problem: What if the A_{UF-CMA} already made a RO query (α_i, m_i) ?? Then we would have sampled a different β_i making the simulation FAIL. So, in this case ABORT.

- Finally, upon a forgery $m^*, \sigma^* = (\alpha^*, \gamma^*)$ check that $(\alpha^*, m^*) = (\alpha_i, m_i)$ is the RO query that we tried to guess.

Then send γ^* to $\mathcal{C}_{ID}$, which concludes the reduction.
Now the theorem follows by observing that $\mathcal{A}_{ID}$ guesses i w.p. $1/poly(\lambda)$.
Moreover, the prob. that $\mathcal{A}_{UFCMA}$ asked no query (α_i, m_i) before it receives a signature $\sigma_i = (\alpha_i, \gamma_i)$ is negligible.
Overall, we don't abort w.p.

$$\geq \left(1 - q_s \cdot negl(\lambda)\right)$$

Hence:

$$\Pr[\mathcal{A}_{1D} \text{ wins}] \geq \frac{1}{\mathrm{poly}(\lambda)} \cdot \left(1 - \mathrm{negl}(\lambda)\right)$$

$$\Pr[\mathcal{A}_{\mathrm{UFCMA}} \text{ wins}] = \frac{1}{\mathrm{poly}(\lambda)} \cdot \frac{1}{\mathrm{poly}(\lambda)}$$

$$\geq \frac{1}{\mathrm{poly}(\lambda)}. \qquad \blacksquare$$