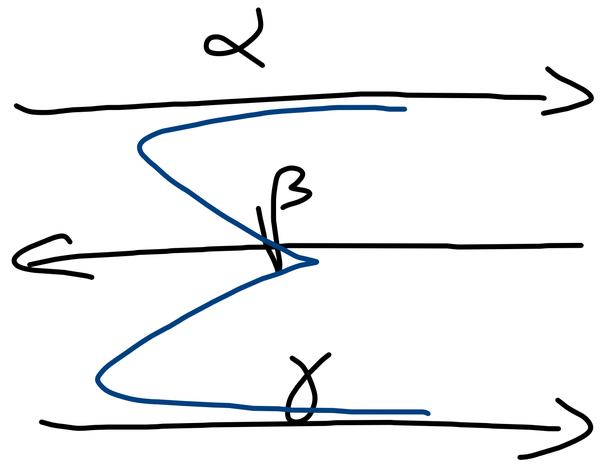
ID SCHEMES

$(pk, sk) \leftarrow\$ \; KGen(1^\lambda)$

$\mathcal{P}(pk, sk)$

CANONICAL ID SCHEME



$\mathcal{V}(pk)$

$\beta \leftarrow\$ \; \mathcal{B}_{\lambda, pk}$

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

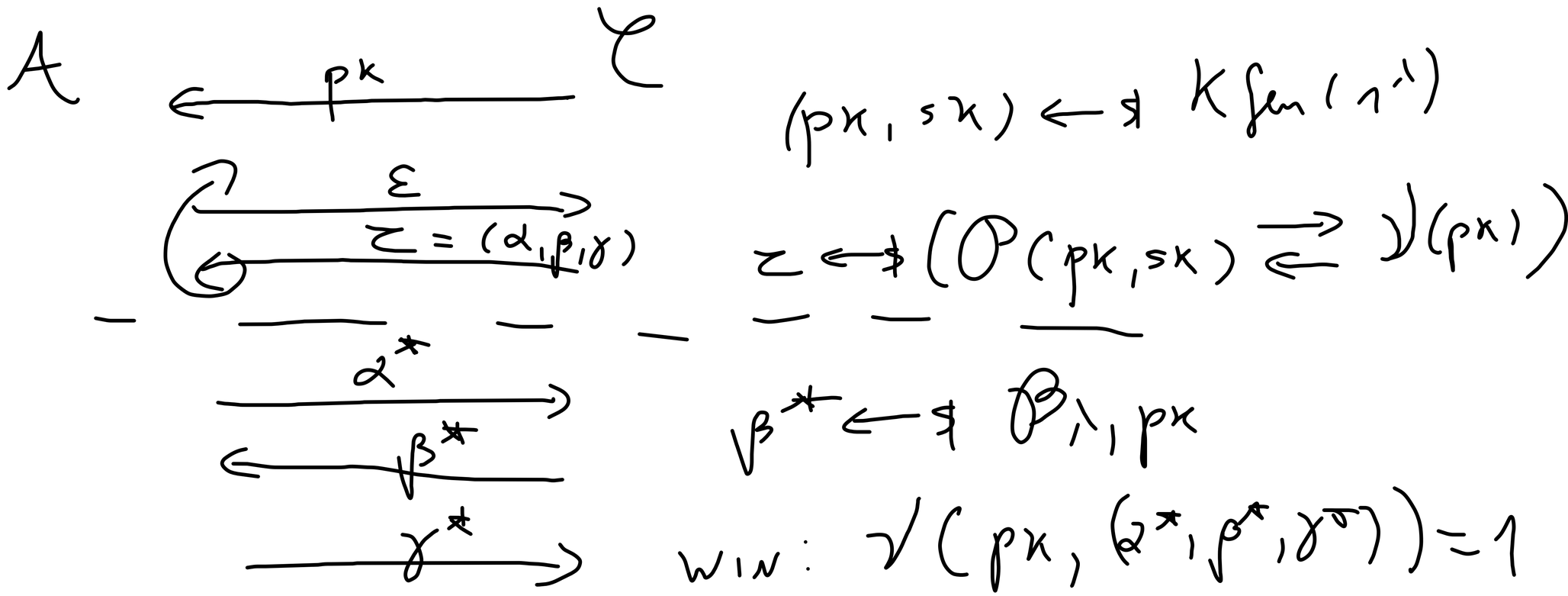
Σ - PROTOCOL

$\mathcal{V}(pk, \underbrace{\tau = (\alpha, \beta, \gamma)}) = 0/1$

TRANSCRIPT

We need 2 properties:

1) PASSIVE SECURITY.



2) The commitment α has non-trivial min-entropy.

$\forall \hat{\alpha}$: $\Pr[\alpha = \hat{\alpha} : \alpha \text{ from } O(pk, sk)] \leq \text{negl}(\lambda)$.

Application : UF-CMA DS in the ROM.

FIAT-SHAMIR TRANSFORM

$$H : \{0,1\}^* \to \mathcal{B}_{\lambda, p_K}$$

-) $KGen(1^\lambda)$: pk, sk from ID scheme.

-) $Sign(sk, m)$: Generate α from prover $\mathcal{P}(pk, sk)$

Let $\beta = H(\alpha, m)$

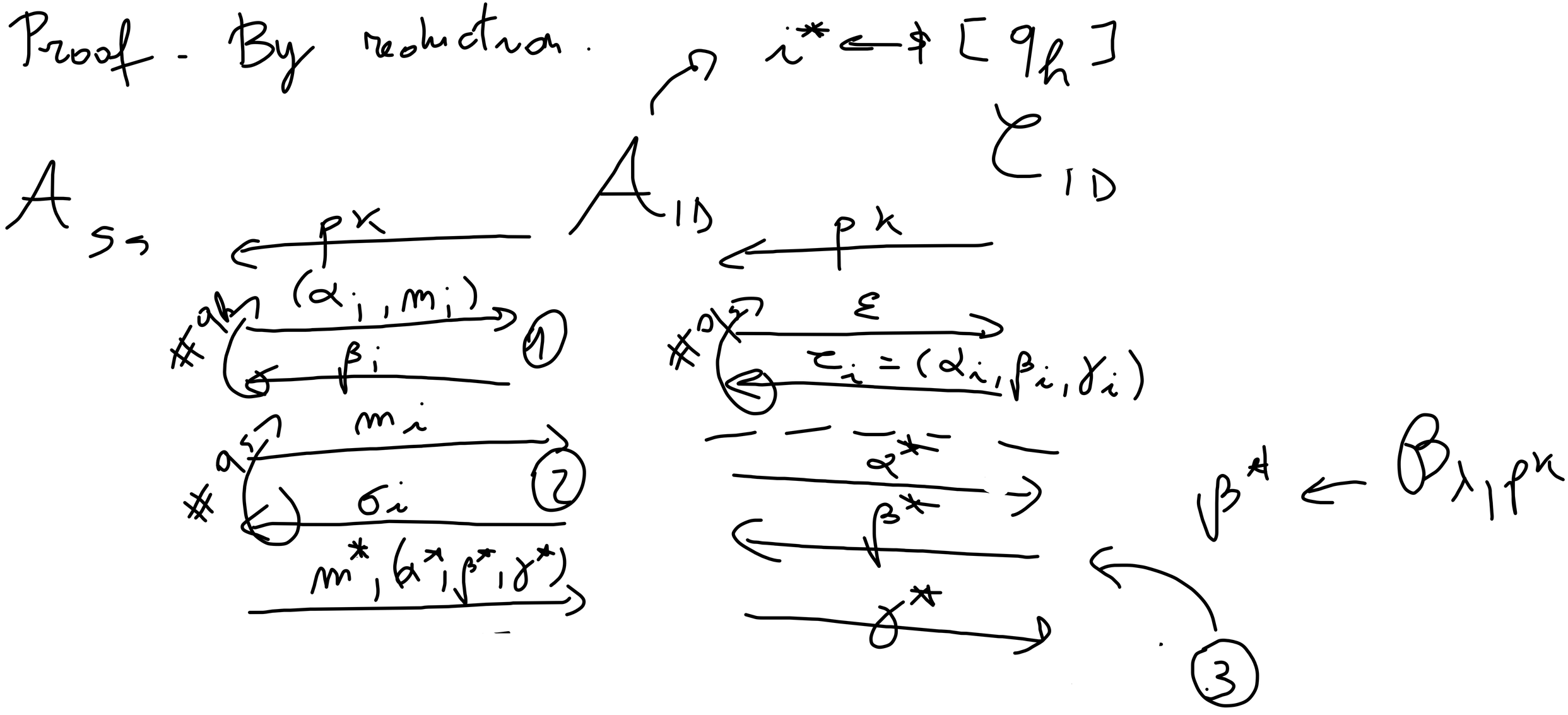
Let γ from prover $\mathcal{P}(pk, sk, \alpha, \beta)$

Output $\sigma = (\alpha, \beta, \gamma)$.

-) $Vrfy(pk, m, \sigma)$: $\mathcal{V}(pk, (\alpha, \beta, \gamma))$; $\beta \overset{?}{=} H(\alpha, m)$.

Teo The above DS is UF-CMA in the ROM assuming canonical ID scheme with PASSIVE security.

Proof - By reduction.



Assumptions (wlog): - After getting σ_i, on m_i, don't query RO on (m_i, α_i)

- Let $q_s, q_h \in poly(\lambda)$ be # of SIGN / RO queries

- If A_{ss} forges on $\hookrightarrow (\alpha^*, \beta^*, \gamma^*), m^*$ σ^*

then it asked α^*, m^* to RO. Call this query i^*.

- Assume A_{ss} never repeats queries to RO.

① RO queries: (α_i, m_i). If $i = i^*$, Then send $\alpha^* = \alpha_i$ to $\mathcal{C}_{ID}$ and receive β^*. Reply $\beta^* = \beta_i$.

If $i \neq i^*$, let $\beta_i \leftarrow\!\$ \mathcal{B}_{\lambda, pk}$.

② SIGN queries: m_i. $\sigma_i = (\alpha_i, \beta_i, \gamma_i)$ from τ_i. Set $\beta_i = H(\alpha_i, m_i)$

If A_{ss} asked RO for α_i, m_i before, ABORT.

③ Given forgery $(\alpha^*, \beta^*, \gamma^*)$, check guess on i^*. If correct output γ^* to $\mathcal{C}_{ID}$.

Reduction does not abort w.p. $1/poly(\lambda)$

and thus wins w.p. $1/poly(\lambda)$. ∎