DEF A CANONICAL ID scheme satisfies SPECIAL SOUNDNESS if $\forall$ PPT $\mathcal{A}$ the following game can only be won with negl(λ) prob.:

$$
\begin{array}{ccc}
\mathcal{A} & & \mathcal{C} \\
& \xleftarrow{\quad pk \quad} & (pk, sk) \leftarrow Gen(1^\lambda) \\
& \xrightarrow[\tau' = (\alpha, \beta', \gamma')]{\tau = (\alpha, \beta, \gamma)} &
\end{array}
$$

WIN:

1) τ, τ' are valid: $V(pk, \tau) = V(pk, \tau') = 1$

2) $\beta \neq \beta'$

$$
\begin{tikzcd}
& \bullet \arrow[d, "\alpha"] & \\
& \bullet \arrow[dl, "\beta"'] \arrow[dr, "\beta'"] & \\
\bullet \arrow[d, "\gamma"'] & & \bullet \arrow[d, "\gamma'"] \\
\bullet & & \bullet
\end{tikzcd}
$$

What does it mean? So, soundness is about hardness of proving false statements for a MALICIOUS PROVER.

But for some languages like:

$$L = \{ y \in G : \exists x \text{ s.t. } g^x = y \}$$

SOUNDNESS IS trivial as every statement $y \in G$ is TRUE, But something better would be to say that any prover that can convince the verifier MUST KNOW x.

For Schnorr: Under the DL assumption in G, The protocol is SPECIAL SOUND.

Assume not, $\exists$ PPT $\mathcal{A}$ that w.p. $1/poly(\cdot)$ and given pk outputs $\tau = (\alpha, \beta, \gamma)$, $\tau' = (\alpha', \beta', \gamma')$ as above.

Then $\exists$ PPT $\mathcal{B}$ that breaks DL with the same probability:

$$\begin{array}{ccccc}
\mathcal{A} & \xleftarrow{\quad pk = y \quad} & \mathcal{B} & \xleftarrow{\quad y \quad} & \mathcal{C} \\
 & & & & x \leftarrow \mathbb{Z}_q \\
 & \xrightarrow{\quad \tau,\ \tau' \quad} & & \xrightarrow{\quad x = \frac{\gamma - \gamma'}{\beta - \beta'} \quad} & y = g^x
\end{array}$$

How to find x? Well, by def.:

$$g^{\gamma'} \cdot y^{-\beta'} = \alpha = g^{\gamma} \cdot y^{-\beta}$$

$$\iff \quad y^{\beta-\beta'} = g^{\gamma-\gamma'}$$

$$\iff \quad y = g^{(\gamma-\gamma')\cdot(\beta-\beta')^{-1}}$$

$$\iff \quad x = (\gamma-\gamma')\cdot\underbrace{(\beta-\beta')^{-1}}_{\text{it exists as } \beta\neq\beta'}$$

$$\Pr[\mathcal{B} \text{ wins}] = \Pr[\mathcal{A} \text{ wins}] \geq 1/\text{poly}(\lambda).$$

Next, we show the two properties imply passive security.

THM SS + HVZK $\Longrightarrow$ PASSIVE ID so long as $|\mathcal{B}_{pk,\lambda}| = \omega(\log \lambda)$.

Proof. The main idea will be to make a reduction to special soundness.

$\mathcal{A}$ $\qquad\qquad\qquad\qquad$ $\mathcal{C}_{ID}$ $\qquad$ $G(\lambda)$ $\quad$ $H(\lambda)$

$\xleftarrow{\quad pk \quad}$ $\qquad$ pk, sk

$\xrightarrow{\text{"give me transcript"}}$

$\xleftarrow{\tau = (\alpha, \beta, \gamma)}$ $\qquad$ $\tau \leftarrow (P(pk, sk) \rightleftarrows V(pk))$

$\qquad\qquad\qquad\qquad\qquad\qquad$ $\tau \leftarrow S(pk)$

$\xrightarrow{\quad \alpha^* \quad}$

$\xleftarrow{\quad \beta^* \quad}$ $\qquad$ $\beta^* \leftarrow \mathcal{B}_{\lambda, pk}$

$\xrightarrow{\quad \gamma^* \quad}$

LEMMA $H(\lambda) \approx_c G(\lambda)$.

Proof. Okay, we just make a reduction to HVZK.

$\mathcal{A}$ $\qquad\qquad\qquad\qquad$ $\mathcal{A}'$

$\xleftarrow{\quad pk \quad}$

"give me transcript" $\longrightarrow$

$\xleftarrow{\quad \tau \quad}$

"give me transcript" $\longrightarrow$

$\xleftarrow{\quad \cancel{\tau} \quad}$

$\xleftarrow{\quad pk, sk, \tau \quad}$ $\mathcal{C}_{HVZK}$

(pk, sk)

$S(pk)$

τ

$P \rightleftarrows V$

pulled only <u>ONCE</u>

???

Hybrid argument !

H_0	H_1	$\cdots$	H_q
$\tau_1 \leftarrow (P \rightleftarrows V)$	$\tau_1 \leftarrow S(pk)$		$\tau_1 \leftarrow S(pk)$
$\tau_2 \leftarrow (P \rightleftarrows V)$	$\tau_2 \leftarrow (P \rightleftarrows V)$	$\cdots$	$\vdots$
$\vdots$	$\vdots$		
$\tau_q \leftarrow (P \rightleftarrows V)$	$\tau_q \leftarrow (P \rightleftarrows V)$		$\tau_q \leftarrow S(pk)$
$\equiv G(\lambda)$			$H(\lambda)$

$$\forall i: \quad H_i \approx_c H_{i+1}$$

Now we can make the reduction!

$\mathcal{A}$ $\xleftarrow{pk}$ $\mathcal{A}'$ $\xleftarrow{pk,\ sk,\ c}$ $\mathcal{C}_{HVZK}$

pk, sk

$e_1 \leftarrow S(pk)$

$\vdots$

$e_i \leftarrow S(pk)$

$e_{N+1} = c$

$\xrightarrow{\tau_{N+2}}$

$\vdots$

$\xrightarrow{\hspace{3em}}$

$\xleftarrow{\tau_q}$

$\tau_{N+2}, \dots, \tau_q$

$\leftarrow \left(P(pk, sk) \rightleftarrows V(pk) \right)$

↪ The reduction knows sk !!!

$\xrightarrow{\alpha^*}$

$\xleftarrow{\beta^*}$

$\beta^* \leftarrow \beta_{i, pk}$

$\xrightarrow{\gamma^*}$

$\blacksquare$

LEMMA $\forall$ PPT $\mathcal{A}$: $\Pr[\,H(\lambda)=1\,] \leq \mathrm{negl}(\lambda)$.

Proof. We now make the reduction to SS.

Assume $\exists$ PPT $\mathcal{A}$ s.t. $\Pr[\,H(\lambda)=1\,] = \varepsilon(\lambda)$

$\geq 1/\mathrm{poly}(\lambda)$.

$$\mathcal{A}_{ID} \xleftarrow{\quad pk \quad} \mathcal{A}'_{SS} \xleftarrow{\quad pk \quad} \mathcal{C}_{SS}$$

(pk, sk)

#poly

$$\xrightarrow{\quad \text{"Transcript"} \quad}$$

$$\xleftarrow{\quad \tau \leftarrow S(pk) \quad}$$

$$\xrightarrow{\quad \alpha \quad}$$

$$\xleftarrow{\quad \beta \quad} \qquad \beta \leftarrow B_{\lambda, pk}$$

$$\xrightarrow{\quad \gamma \quad}$$

To the state $s \in \{0,1\}^*$ where α was sent

REWIND

$\xleftarrow{\quad \beta' \quad}$ $\qquad \beta' \leftarrow B_{\lambda, pk}$

$\xrightarrow{\quad \gamma' \quad}$

$$\frac{\tau = (\alpha, \beta, \gamma)}{\tau' = (\alpha, \beta', \gamma')}$$

All we need is to show: (i) $\beta \neq \beta'$; (ii) τ', τ' ACCEPTING w.p. $\geq 1/\text{poly}(\lambda)$.

If τ, τ' would be independent, we'd be already done. But they are not.

As we said, $\varepsilon(\lambda) = \Pr[H(\lambda) = 1]$. Let

$s \in \{0,1\}^k$ be the state of A after it sent α_i and call $p_s = \Pr[S = s]$. Now:

$$\varepsilon(\lambda) = \mathbb{E}[\delta_s] = \sum_s p_s \cdot \delta_s$$

$$\delta_s = \Pr[H(\lambda) = 1 \mid S = s]$$

Moreover, let GOOD : Event that $\beta' \neq \beta$.

$$\Pr[A' \text{ WINS}] \geq \Pr[\tau, \tau' \text{ ACCEPTING} \wedge \text{GOOD}]$$

$$= \Pr[\tau, \tau' \text{ ACCEPTING} \mid \text{GOOD}] \cdot (1 - \Pr[\overline{\text{GOOD}}])$$

$$= \Pr[\tau, \tau' \text{ ACCEPTING} \mid \text{GOOD}]$$

$$- \underbrace{\Pr[\overline{\mathrm{GOOD}}]}_{|\mathcal{B}_{\lambda,pk}|^{-1}} \cdot \underbrace{\Pr[\tau, \tau' \text{ ACC.} \mid \mathrm{GOOD}]}_{\leq 1}$$

$$\geq \Pr[\tau, \tau' \text{ ACC.} \mid \mathrm{GOOD}] - |\mathcal{B}_{\lambda,pk}|^{-1}$$

$$= \sum_{s} \rho_s \cdot \delta_s^2 - |\mathcal{B}_{\lambda,pk}|^{-1}$$

$$= \mathbb{E}[\delta_s^2] - |\mathcal{B}_{\lambda,pk}|^{-1}$$

$$\geq (\mathbb{E}[\delta_\tau])^2 - |\mathcal{B}_{\lambda,pk}|^{-1}$$

$\hookrightarrow$ JENSEN

$$= \varepsilon^2(\lambda) - \mathrm{negl}(\lambda) = 1/\mathrm{poly}(\lambda) \qquad \blacksquare$$

FIAT - SHAMIR

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

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

$\mathsf{KGen}(1^\lambda) = \mathsf{Gen}(1^\lambda) \rightarrow (pk, sk)$

$\mathsf{Sign}(sk, m)$: - 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:

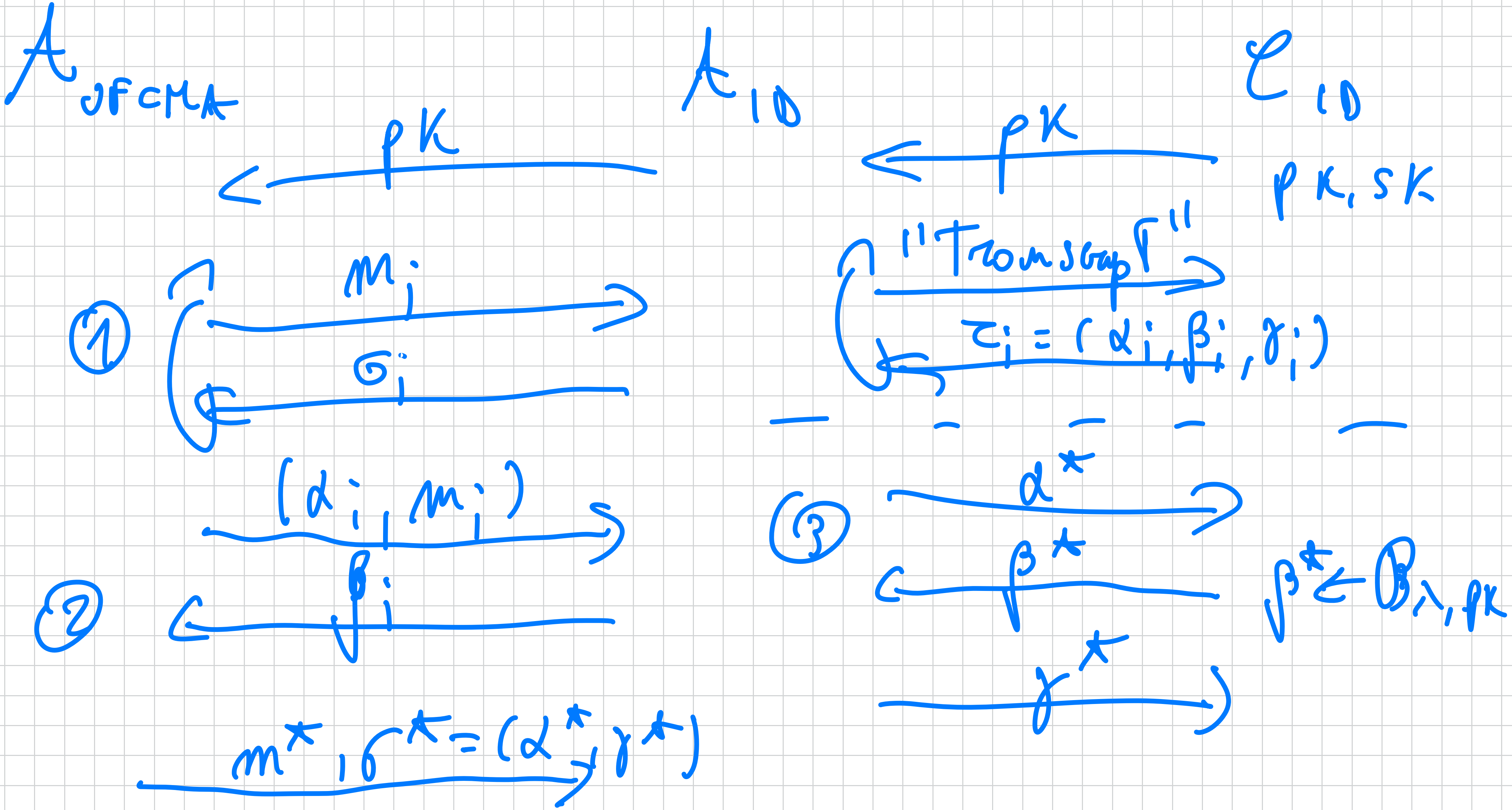
- RO queries (α_i, m_i) (# queries $= q_h = poly(\lambda)$)
- sign queries m_i (# queries $= q_s = poly(\lambda)$)

Wlog, we make a few assumptions on A:

- It does not repeat RO queries.
- If 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^*, σ^*, the A made a RO query of the form (α^*, m^*).

$$\sigma^* = (\alpha^*, \gamma^*)$$

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

    Then, return β^* to $\mathcal{A}_{UFCMA}$.

Made with Goodnotes

- 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 A_{ID} guesses i w.p. $1/\text{poly}(\lambda)$.

Moreover, the prob. that 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.

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

Hence:

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

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

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