

## ID Schemes

Last lecture we proved that passively secure ID schemes imply UF-CMA signatures using Fiat-Shamir transform.  
(ROM)

We want to construct a passively secure scheme.

We'll see 2 criteria for ID schemes.

### 1) Honest verifier - zero knowledge HVZK

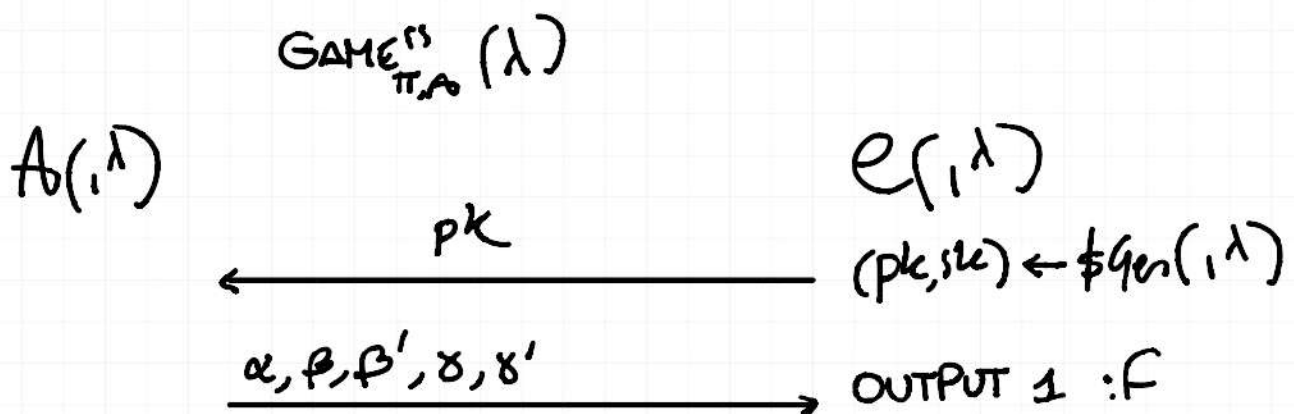
Def: We say an ID scheme  $\Pi$  is HVZK if

$\exists$  PPT algo Sim s.t.

$$\left\{ (pk, sk) \leftarrow \$Gen(1^\lambda) : sk, pk, Sim(pk) \right\} \approx_c \left\{ (pk, sk) \leftarrow \$Gen(1^\lambda) : sk, pk, Trans(pk, sk) \right\}$$

This shows that the  $Gen$  algo reveals nothing about  $sk$   
(zero knowledge)

### 2) Special Soundness



$(\alpha, \beta, \gamma)$   
 $(\alpha', \beta', \gamma')$  are VALID  
 $\wedge \beta \neq \beta'$

DEF: An ID scheme  $\Pi$  has special soundness  $\forall PPTA : \mathcal{F}$

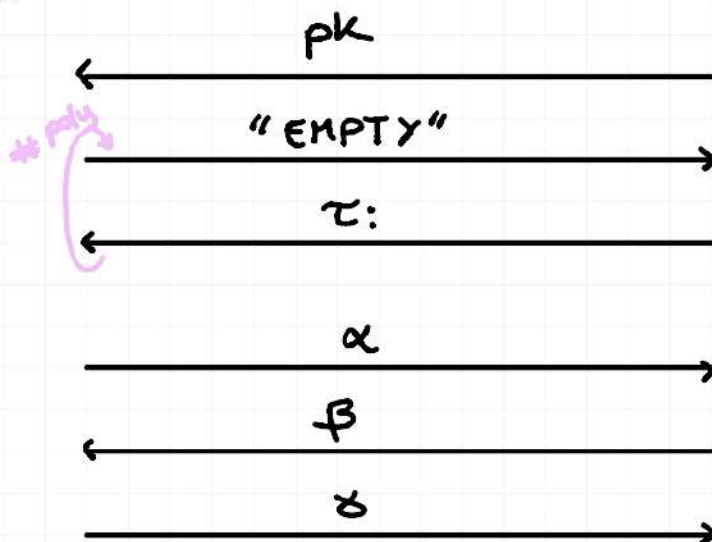
$$\Pr[\text{GAME}_{\Pi, A}''(\lambda) = 1] \leq \text{negl}(\lambda)$$

In this way ①+②  $\Rightarrow$  Passive Security

THM: Let  $\Pi$  be an ID scheme with ss and HVZK st.  
 $|B_{\lambda, pk}| = u(\log \lambda)$ . Then  $\Pi$  is passively secure.

Proof: We start with  $\text{GAME}_{\Pi, A}^{\text{id}}(\lambda)$

$A(i, \lambda)$

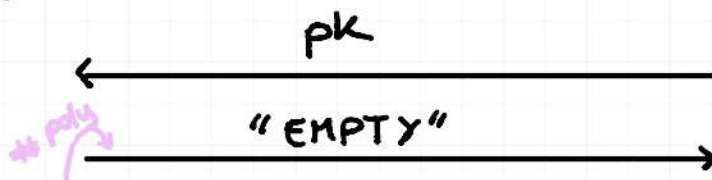


$C(i, \lambda)$

$pk, sk \leftarrow \mathcal{G}_n(1^\lambda)$   
 $\tau_i \leftarrow \mathcal{F}_{\text{Trans}}(pk, sk)$   
 $\tau_i = (\alpha_i, \beta_i, \gamma_i)$   
 $\beta \leftarrow \mathcal{B}_{\lambda, pk}$

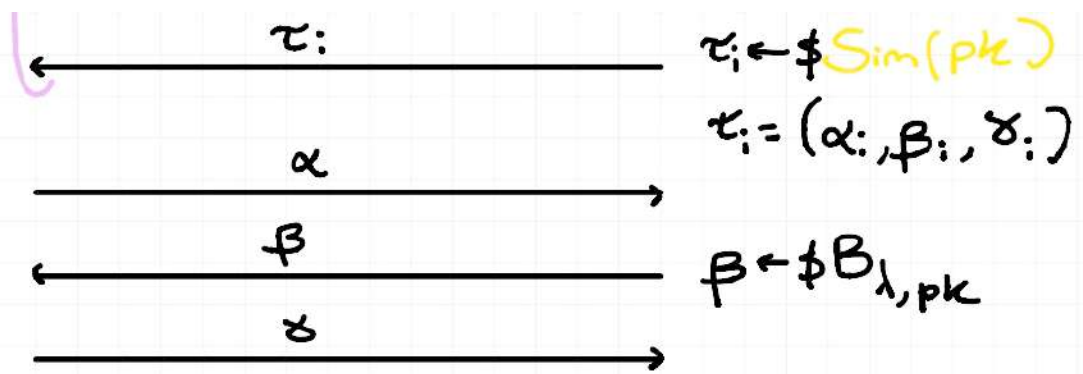
And  $\text{HVB}_{\Pi, A}^{\text{id}}(\lambda)$

$A(i, \lambda)$



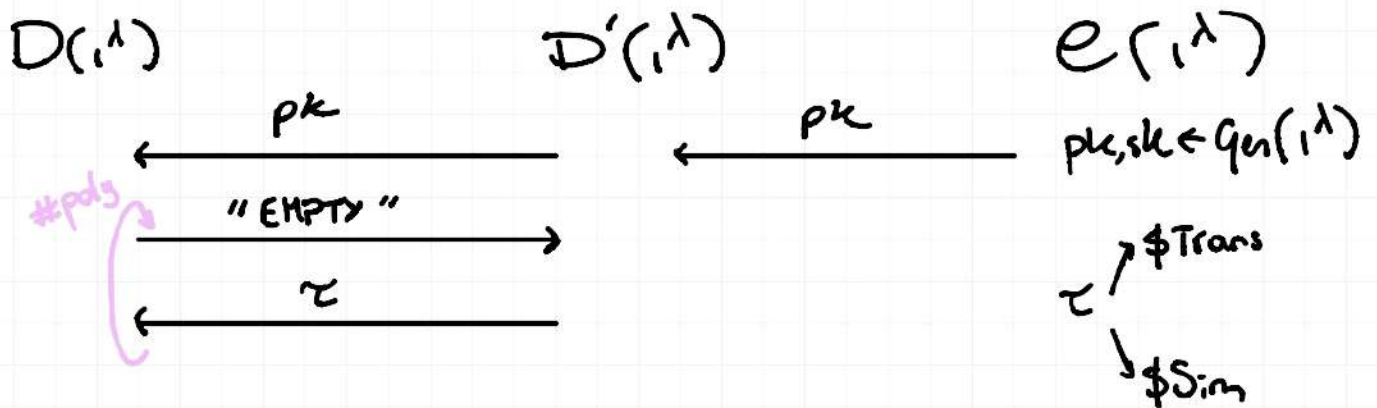
$C(i, \lambda)$

$pk, sk \leftarrow \mathcal{G}_n(1^\lambda)$



LEMMA:  $GAME_{\pi, \lambda}^{id} \approx_c HYB_{\pi, \lambda}^{id}$

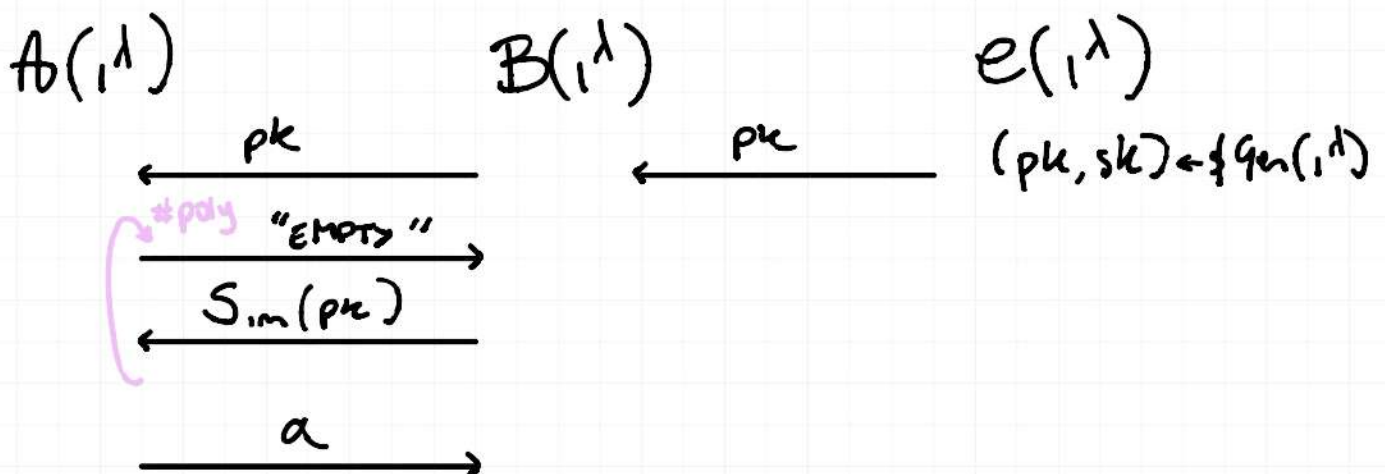
Proof: Assume  $\exists$  PPT distinguisher  $D$  that can distinguish  $GAME$  from  $HYB$ .

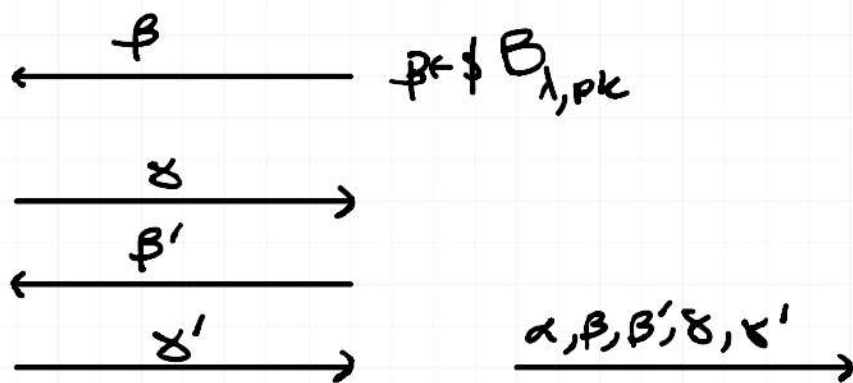


Solve through Hybrid argument.

LEMMA:  $\Pr[HYB(\lambda) = 1] \leq \text{negl}(\lambda)$

Proof: Reduction to ss.





The analysis is a bit tricky.

Let  $z$  be the state of  $A$  after sending  $\alpha$ .  
 ( $z$  is a random variable).

Let  $\varepsilon(\lambda) = \Pr[H_1(\lambda) = 1]$  and  
 $\delta_z = \Pr[H_1(\lambda) = 1 \mid z]$

$$\Rightarrow \varepsilon(\lambda) = \sum_z p_z \cdot \delta_z \quad \varepsilon \text{ is just the average of each } \delta_z.$$

$$= E[\delta_z]$$

Let  $\text{GOOD}$  be the event  $\beta \neq \beta'$ .

$$\begin{aligned}
 \Pr[B \text{ wins}] &\geq \Pr[H_1(\lambda) = 1 \wedge \text{GOOD}] \\
 &\geq \Pr[B \text{ wins} \wedge \text{GOOD}] \\
 &\geq \Pr[B \text{ wins} \mid \text{GOOD}] - |B_{\lambda, pk}|^{-1} \\
 &= \sum_z p_z \delta_z^2 - |B_{\lambda, pk}|^{-1} \\
 &= E[\delta_z^2] - |B_{\lambda, pk}|^{-1} \\
 &= \varepsilon^2(\lambda) - \text{negl}(\lambda)
 \end{aligned}$$



$$\geq 1/\text{poly} - \text{negl}(\lambda)$$

SCHNORR

$$(\mathbb{G}, g, q) \leftarrow \$\text{GroupGen}(1^\lambda), y = g^x, x \leftarrow \$\mathbb{Z}_q$$

$\mathcal{P}(x, y)$		$\mathcal{V}(y)$
$\alpha = g^a$	$\xrightarrow{\alpha}$	
$a \leftarrow \$\mathbb{Z}_q$	$\xleftarrow{\beta}$	$\beta \leftarrow \mathbb{Z}_q$
$\delta = \beta x + a \bmod q$	$\xrightarrow{\delta}$	Check $g^\delta = \alpha y^\beta$

Let's now prove passive security (from last lecture).

1) HVZK. Consider following  $\text{Sim}(y)$

$$\delta, \beta \leftarrow \mathbb{Z}_q, \alpha = g^\delta \cdot y^{-\beta}$$

OUTPUT  $(\alpha, \beta, \delta)$

2) SS

Assume  $\exists \text{PPT } A(y)$

outputs  $\alpha, \beta, \beta', \delta, \delta'$  s.t.

$$(i) (\alpha, \beta, \delta) = (\alpha, \beta', \delta')$$

$$ii) \beta \neq \beta'$$