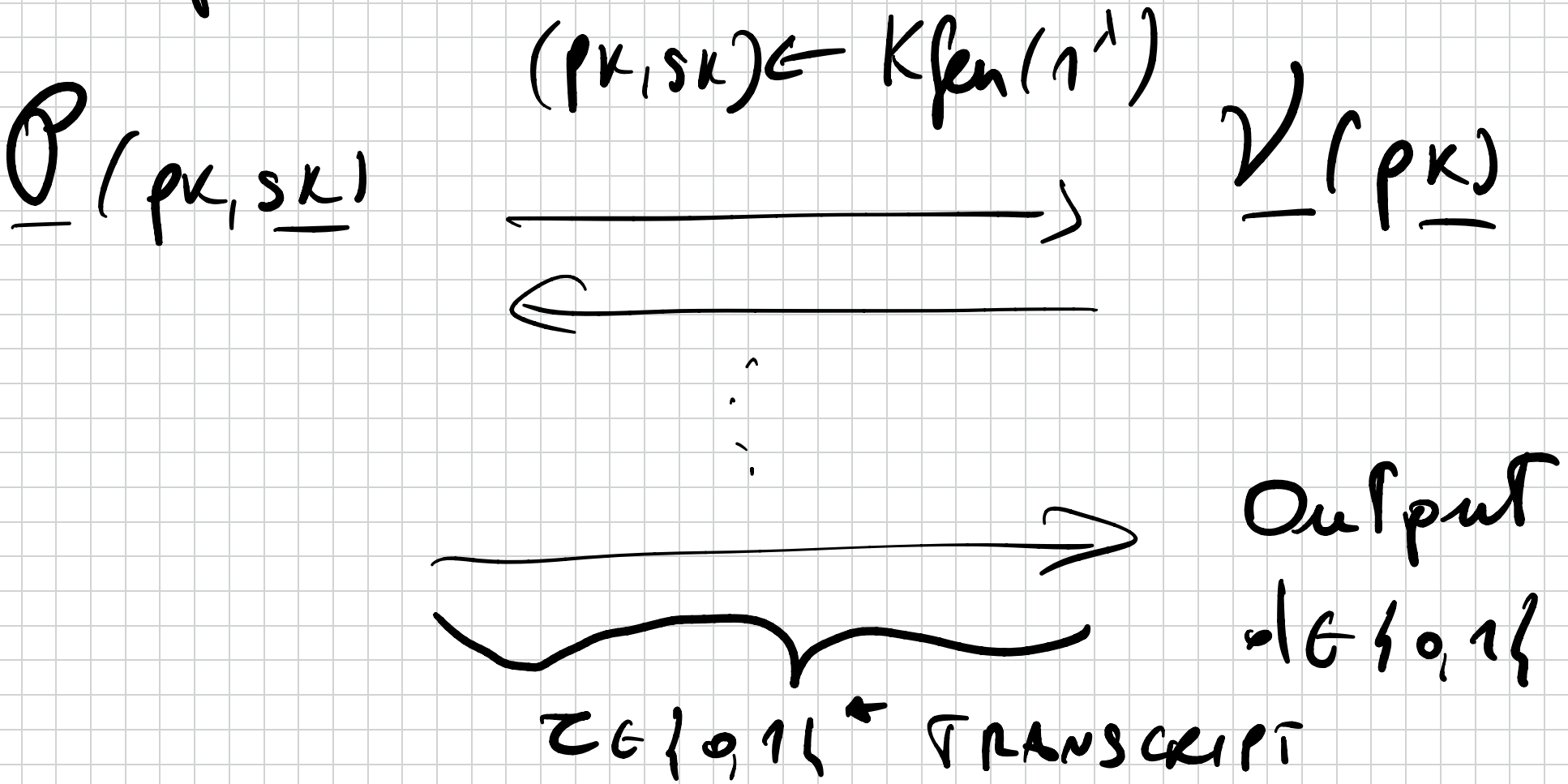
FIAT-SHAMIR SIGNATURES

Thus a standard approach to construct DS from IDENTIFICATION SCHEMES.



Some notation:

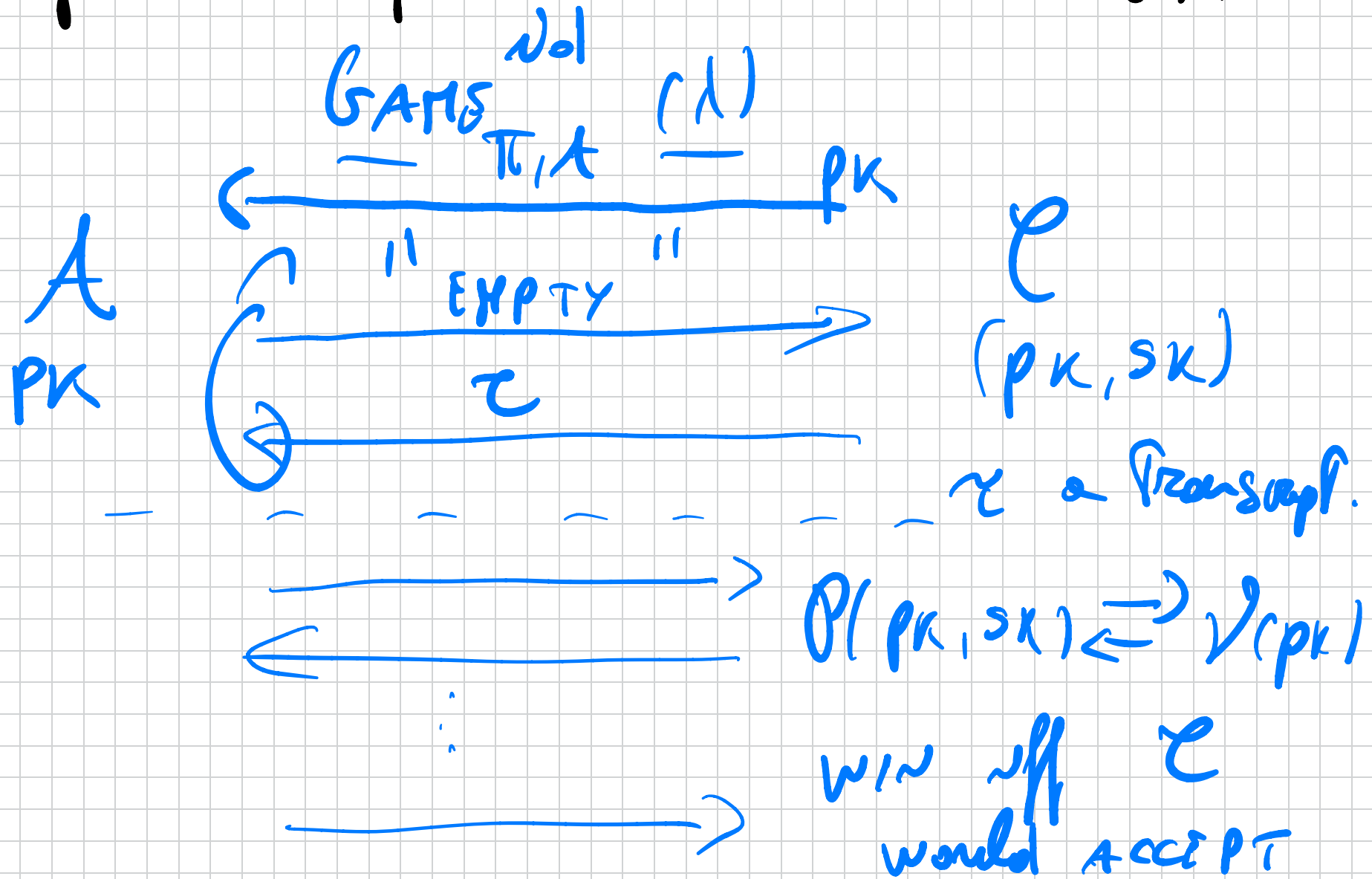
- $\tau \leftarrow \left(P(pk, sk) \rightleftarrows V(pk) \right)$
- $\text{Output}\left(P(pk, sk) \rightleftarrows V(pk) \right) = d \in \{0,1\}$

CORRECTNESS: $\forall (pk, sk) \in \text{Kgen}(1^\lambda)$

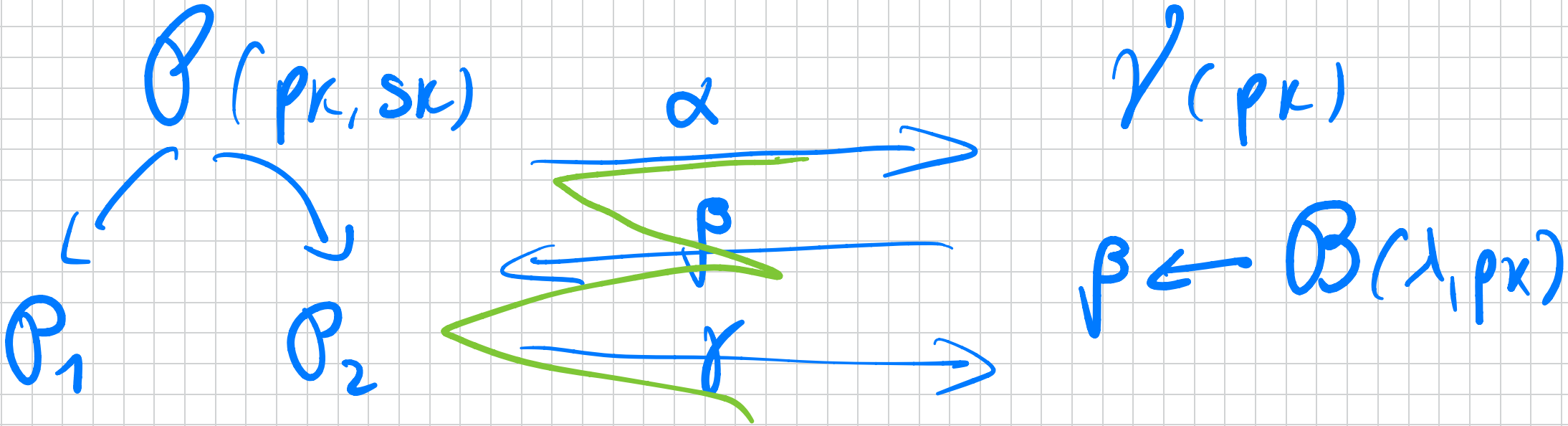
$$\Pr\left[d = 1 : d \leftarrow \text{Output}\left(P(pk, sk), V(pk) \right) \right] \geq 1$$

SECURITY: Passive security. If the attacker does not know sk, it can't impersonate P.

It should be true, even given many accepting transcripts between honest P, V.



We will work with special ID schemes.
The so-called "Σ-protocols":



NOT-TRIVIALITY: $\alpha \leftarrow P_1(pk, sk)$

$$Pr[\alpha = \hat{\alpha}] \leq negl(\lambda)$$

$\forall\ pk, sk$
$\forall\ \hat{\alpha}$.

$$\Sigma = (\alpha, \beta, \gamma)$$

Looking ahead: given a Σ-protocol, we can easily obtain a DS in the ROM.

FIAT-SHAMIR TRANSFORM

Alice $\xrightarrow{m,\ \sigma = (\alpha, \beta, \gamma)}$ Bob

pk, sk $\qquad$ pk

$\alpha \leftarrow P_1(pk, sk)$; $\beta = H(\alpha, m)$

$\gamma \leftarrow P_2(pk, sk, \alpha, \beta)$

$Verify(pk, m, \sigma)$: Output 1 iff $\beta = H(\alpha, m)$ and σ is a VALID Σ.

Example: The Schnorr Σ-protocol.

(G, g, q) = params

g^x x

$\| \quad \|$

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

$pk = g^x$; $sk = x$

$\alpha = g^a$ $\longrightarrow$

$\beta \leftarrow \mathbb{Z}_q$ $\longleftarrow$ β

$a \leftarrow \mathbb{Z}_q$

$\gamma = \beta x + a$ $\longrightarrow$

CHECK:

$g^\gamma = (pk)^\beta \cdot \alpha$

CORRECTNESS:

$$g^\gamma = g^{\beta x + a} = (g^x)^\beta \cdot g^a = (pk)^\beta \cdot \alpha \quad \checkmark$$

THM If Π is passively secure, then FIAT-SHAMIR signatures are UF-CMA in the ROM.

(We'll prove this next time.)

Let's focus first on constructing passively secure ID schemes. Two sufficient properties:

- HONEST-VERIFIER ZERO KNOWLEDGE
- SPECIAL SOUNDNESS.

Let's define them.

DEF (HVZK) An ID scheme $\Pi = (KGen, \mathcal{P}, \mathcal{V})$ is HVZK if $\exists$ PPT Sim s.t.

$$\left(pk, sk, \underbrace{Sim(pk)}_{\text{SIMULATED}}\right) \approx_c \left(pk, sk, \underbrace{\langle \mathcal{P}(pk, sk) \rightleftarrows \mathcal{V}(pk) \rangle}_{\text{HONEST}}\right)$$

τ

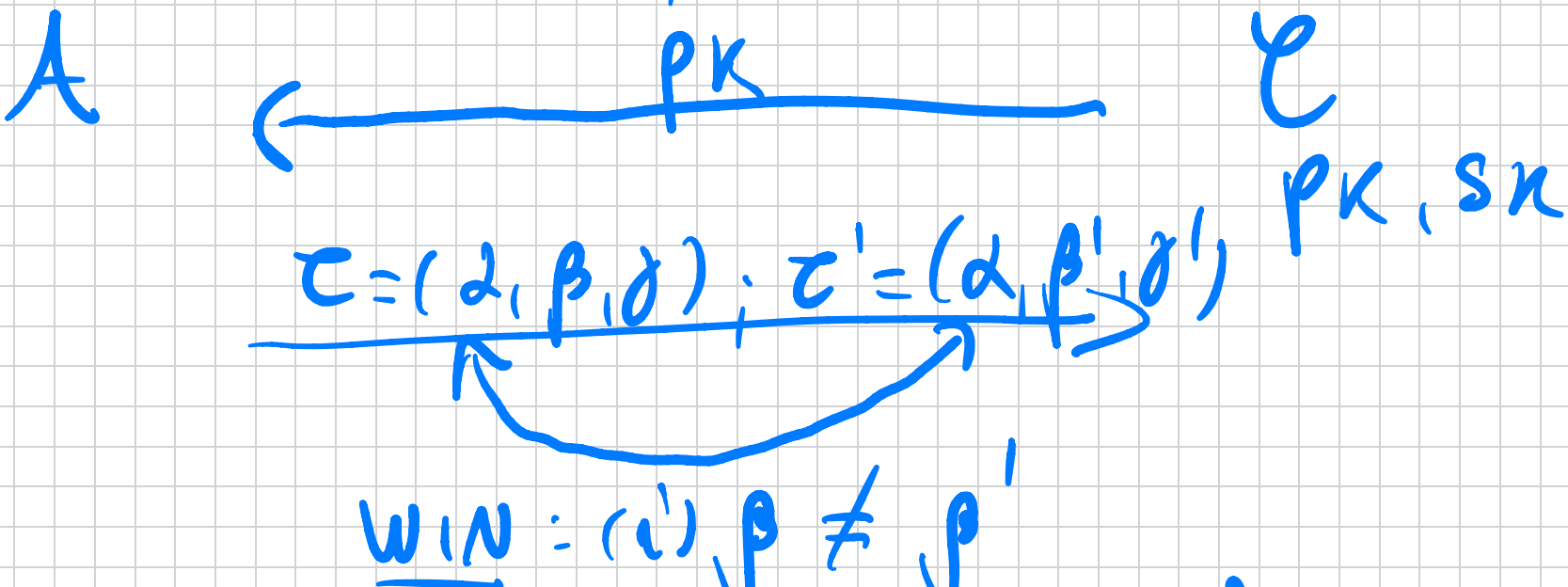
EXAMPLE: Schnorr has this property.

Sim (pk): $\beta, \gamma \leftarrow \mathbb{Z}_q$; $\alpha = g^{\gamma} \cdot (pk)^{-\beta}$

Output $(\alpha, \beta, \gamma) = \tau$. The distribution is IDENTICAL !!

DEF (SS) $\Pi = (Kgen, \mathcal{P}, V)$ is SPECIAL SOUND if $\forall$ PPT $\mathcal{A}$ the following game can be won w.p. $\leq negl(\lambda)$

$$G^{SS}_{AMS_{\Pi,\mathcal{A}}}(\lambda)$$



WIN : (i) $\beta \neq \beta'$

(ii) $V(pk, \tau) = V(pk, \tau') = 1$

Example: Schwarz has this property assuming $\mathbb{D}_2$ is closed. In fact; given τ, τ' as above we have:

$$g^{\gamma} = (\rho\kappa)^{\beta} \cdot \alpha$$

$$g^{\gamma'} = (\rho\kappa)^{\beta'} \cdot \alpha$$

$$\Rightarrow g^{\gamma-\gamma'} = (g^{\kappa})^{\beta-\beta'}$$

$$\Rightarrow g^{\kappa} = g^{(\gamma-\gamma')(\beta-\beta')^{-1}}$$

$\Rightarrow \kappa = (\gamma-\gamma')(\beta-\beta')^{-1}$ since $\beta \neq \beta'$

$\beta-\beta'$ is always invertible

THM SS + HVZK $\Rightarrow$ PASSIVE SECURITY.

(We'll prove this next time.)