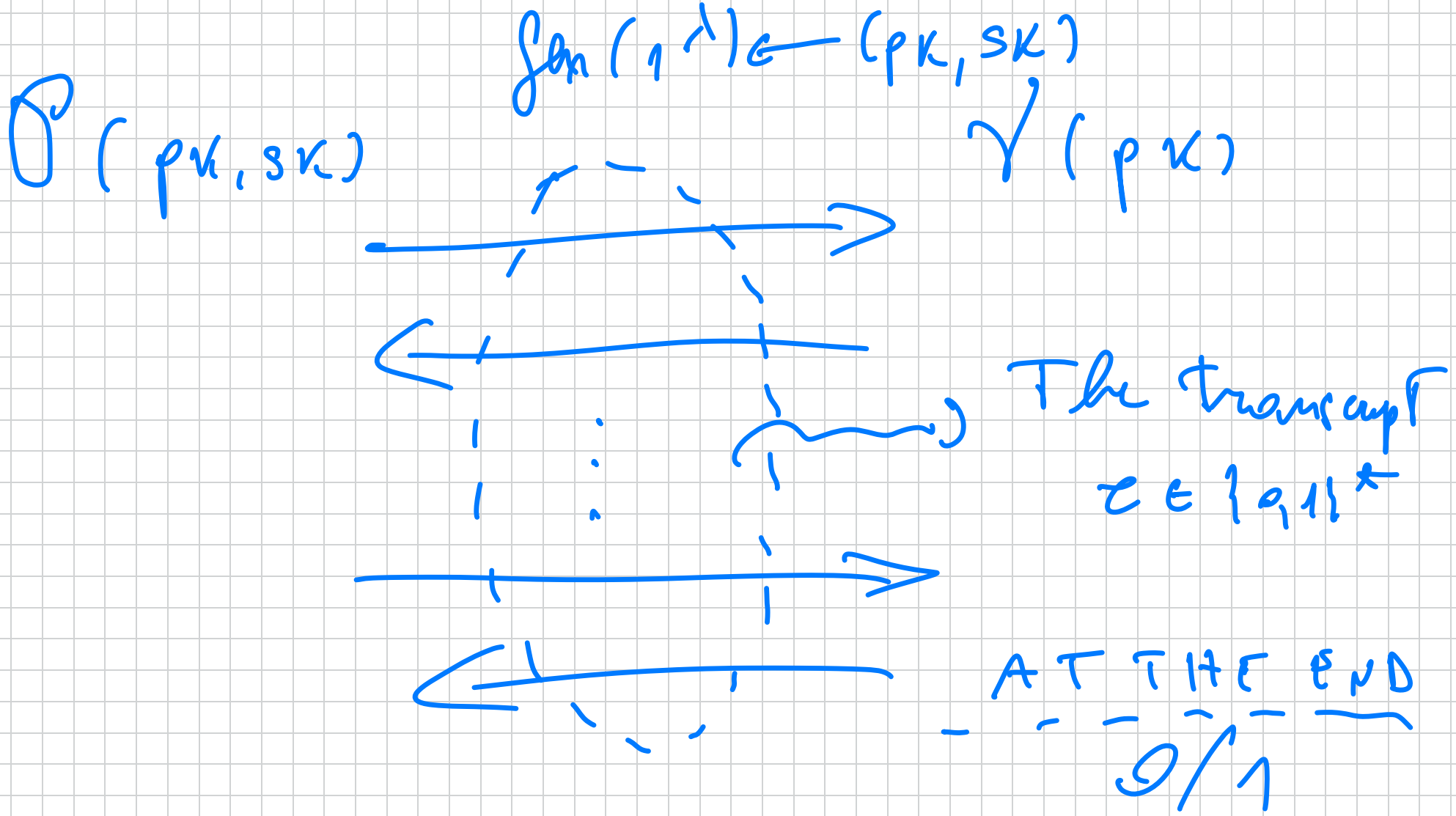
1D SCHEMES

What is an 1D scheme? It's a protocol between a PROVER and VERIFIER:



We want to study this primitive. The properties is always will be CORRECTNESS and SECURITY.

CORRECTNESS: $\forall \lambda \in \mathbb{N}$, $\forall (pk, sk) \in Gen(1^\lambda)$

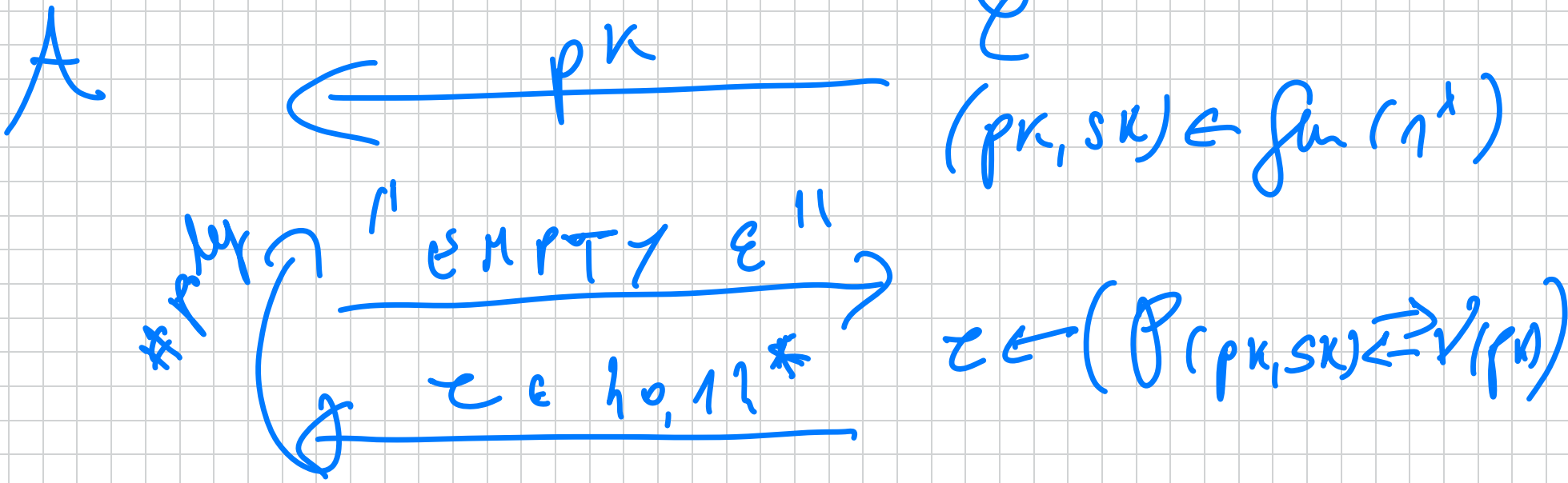
$$Pr\left[out\left(P(pk, sk) \rightleftarrows V(pk) \right) = 1 \right] = 1$$

) where out is the output of V after the interaction.

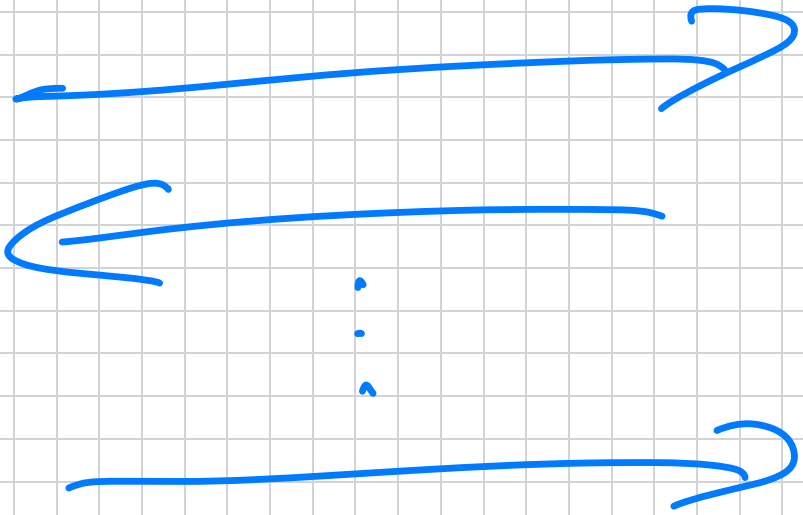
SECURITY: There are many possibilities. But for us, we will just need weak

security, so-called PASSIVE SECURITY.
This means an eavesdropper monitoring interactions between P and V should not be able to impersonate P.

$\underline{\text{GAME}^{id}_{\Pi,A}(\lambda)}$:



— IMPERSONATION

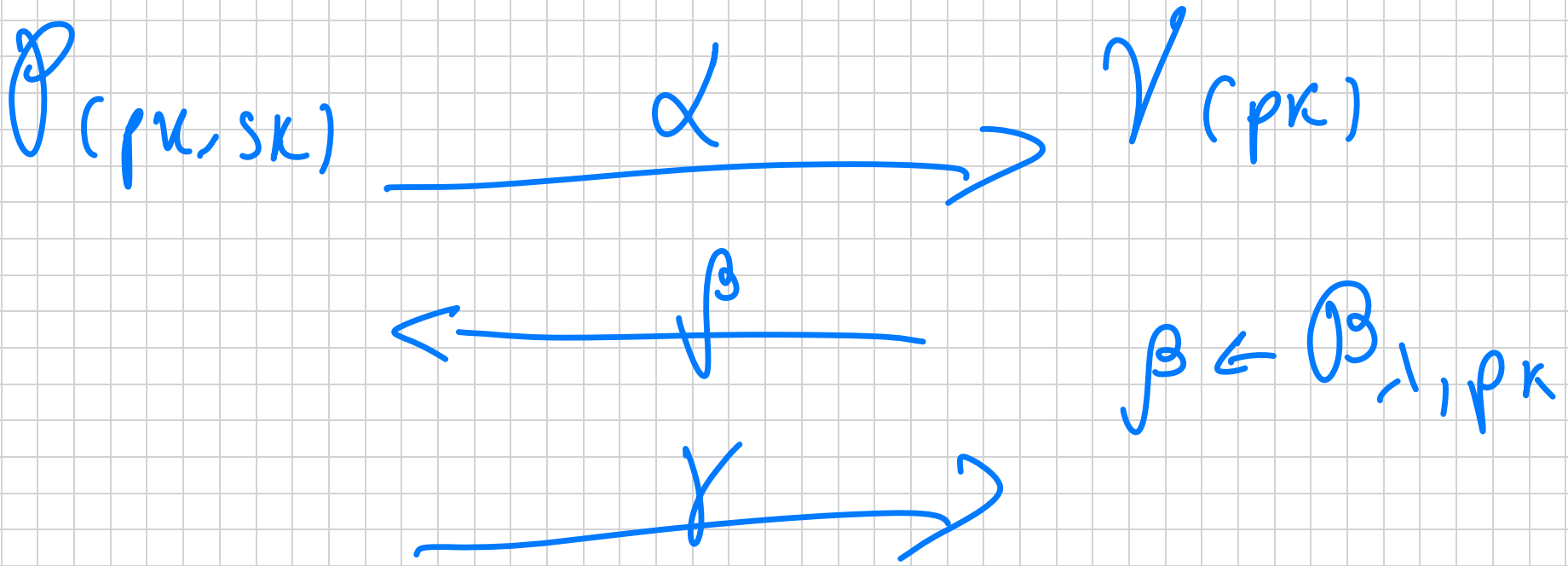


ADV WINS iff $V(pk)$ would ACCEPT

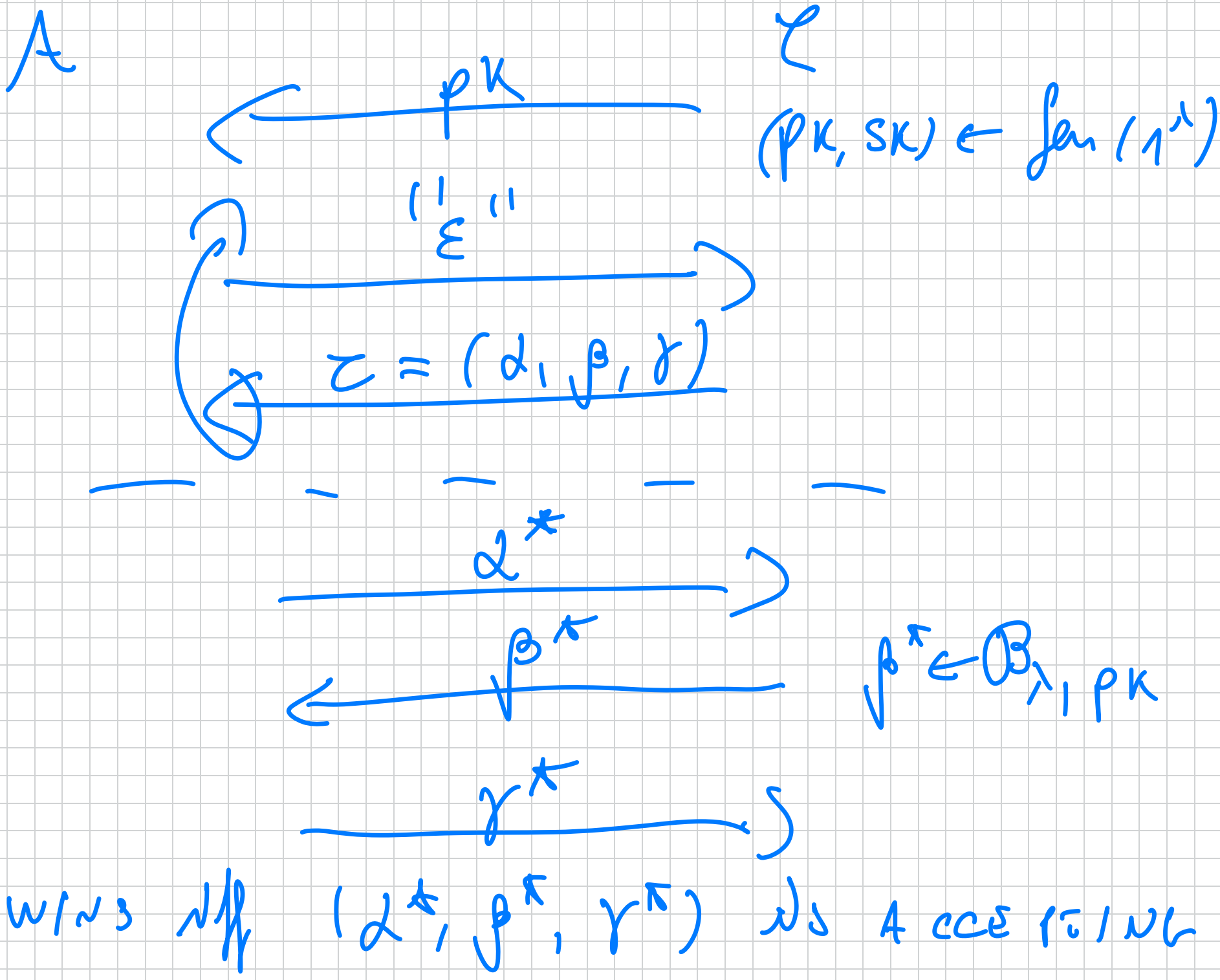
Def. $\pi = (Gen, P, V)$ is PASSIVELY SECURE if $\forall$ PPT A:

$$Pr[GAME^{real}_{\pi,A}(\lambda) = 1] \leq negl(\lambda).$$

We will only consider very special ID schemes: 3-ROUND and PUBLIC COIN.



In such a case note that the security game looks like this:



Looking ahead, let's consider a RUNNING EXAMPLE. The Schnorr protocol:

$(\mathbb{G}, g, q) \leftarrow \text{GroupGen}(1^\lambda)$

$(x, y) \leftarrow \text{Gen}(1^\lambda)$

$SK = x \leftarrow \mathbb{Z}_q$; $y = g^x$

$PK = y$

$\mathcal{P}(x, y)$		$\mathcal{V}(y)$
$r \leftarrow \mathbb{Z}_q$		
$\alpha = g^r$	$\xrightarrow{\alpha \in \mathbb{G}}$	
	$\xleftarrow{\beta \in \mathbb{Z}_q}$	$\beta \leftarrow \mathbb{Z}_q$
$\gamma = \beta x + r \bmod q$	$\xrightarrow{\gamma \in \mathbb{Z}_q}$	

(α, β, γ) is ACCEPTING (by V) iff:

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

CORRECTNESS:

$$g^{\gamma} = g^{\beta x + a}$$

$$= g^{a} \cdot g^{\beta x}$$

$$= \alpha \cdot (g^{x})^{\beta}$$

$$= \alpha \cdot y^{\beta} \quad \checkmark$$

An important property: The first message should be NON-DEGENERATE (have HIGH MIN-ENTROPY): $\forall \hat{\alpha} \in \{0,1\}^*$

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

↳ α is $\Theta(pk, sk)$ first msg

Here is the plan:

1) Construct PASSIVELY SECURE ID schemes.

2) Show that 1) $\Rightarrow$ UF-CMA signatures

in the ROM.

Let's do a proof. In fact, we'll prove a general result that PASSIVE SECURITY follows by two properties:

- Honest-Verifier ZERO KNOWLEDGE

- SPECIAL SOUNDNESS.

HVZK: What does a protocol execution reveal about sk ??? When the verifier is honest it reveals NOTHING!

DEF $\Pi = (Gen, P, V)$ is HVZK if:

$\exists$ PPT SIMULATOR S s.t.

$$\left\{ (pk, sk, \tau) : (pk, sk) \leftarrow Gen(1^\lambda); \tau \leftarrow \left(P(pk, sk) \rightleftarrows V(pk) \right) \right\}$$

$$\approx_c$$

$$\left\{ (pk, sk, \tau) : (pk, sk) \leftarrow Gen(1^\lambda) \right.$$
$$\left. \tau \leftarrow S(pk) \right\}.$$

Intuition: All that HONEST V learns about sk when running Π, he can compute also without running Π (just running $S(pk)$)!

Sanity check: let's prove it for Schnorr. Here is the simulator:

$S(pk) = S(y)$:

Pick $r, \beta \in \mathbb{Z}_q$

Let $\alpha = g^r \cdot y^{-\beta}$

Fix any $pk = y$, $sk = x$ and $\beta \in \mathbb{Z}_q$.
In a real (α, β, γ), the distribution of γ is UNIFORM regardless of β.
$\gamma = \beta x + \alpha \bmod q$
Moreover $\alpha = g^{\gamma} \cdot y^{-\beta}$ is the only value that makes the verifier accept.
The simulated (α, β, γ) has the same distribution. Thus, Schnorr satisfies
PERFECT HVZK