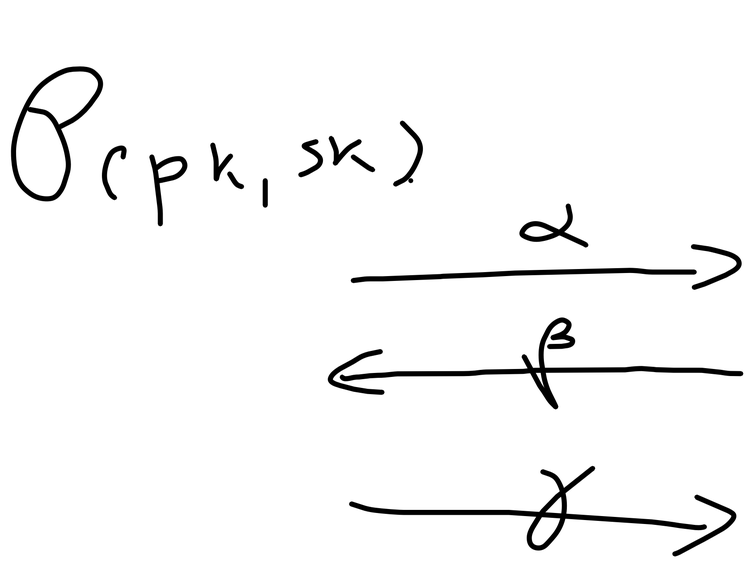
ID SCHEMES



PASSIVE SECURITY $\xRightarrow{H(\cdot)\ \text{ROM}}$ $\sigma = (\alpha, \beta, \gamma)$, $\beta = H(m \| \alpha)$ UF-CMA DS

Today: How to get PASSIVELY SECURE ID schemes from std assumptions. Two criteria:

- HVZK
- SPECIAL SOUNDNESS (SS)

DEF. $\Pi = (Kgen, P, V)$ ~s AVZK wf ∃ PPT SIMULATOR S s.t.

$$REAL_{\Pi,A}(\lambda) \tilde{\approx}_c IDEAL_{\Pi,S}(\lambda)$$

$REAL_{\Pi,A}(\lambda)$:

$(pk, sk) \leftarrow\$ Kgen(1^\lambda)$

$\tau = (\alpha, \beta, \gamma) \leftarrow\$ \langle P(pk, sk) \rightleftarrows V(pk) \rangle$

Output (pk, sk, τ)

$IDEAL_{\Pi,S}(\lambda)$:

$(pk, sk) \leftarrow\$ Kgen(1^\lambda)$

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

Output: (pk, sk, τ)

Example:

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

$\sigma = Sign(sk, m)$ — $m \leftarrow \mathcal{M}$

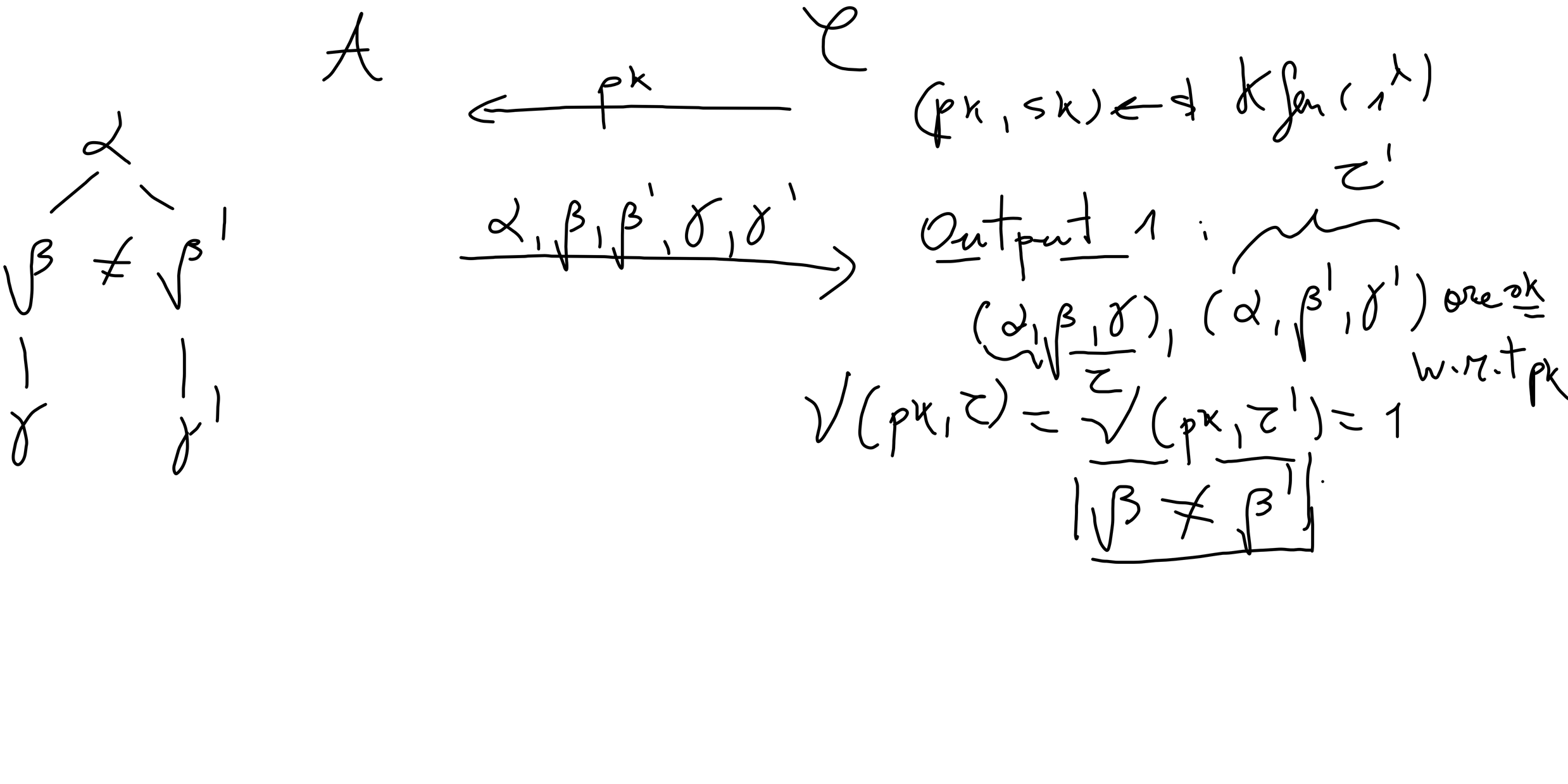
m ⟵

σ ⟶ Output 1 iff $Verify(pk, m, \sigma) = 1$.

REAL: $(pk, sk, (m, \sigma) = C)$

DEF. $\Pi = (Kgen, \mathcal{P}, \mathcal{V})$ is SPECIAL SOUND if $\forall$ PPT $\mathcal{A}$:

$$\Pr\left[GAME^{SS}_{\Pi,\mathcal{A}}(\lambda) = 1 \right] \leq negl(\lambda).$$



Here is a secure protocol:

$$\text{params} = (G, g, q), \quad pk = g^x = y$$

$$sk = x \leftarrow\!\$\ \mathbb{Z}_q$$

$\mathcal{P}(y, x)$		$\mathcal{V}(y)$
$\alpha = g^a$	$\xrightarrow{\alpha}$	
$a \leftarrow\!\$\ \mathbb{Z}_q$	$\xleftarrow{\beta}$	$\beta \leftarrow\!\$\ \mathbb{Z}_q$
$\gamma = \beta x + a \bmod q$	$\xrightarrow{\gamma}$	Output 1 iff: $g^\gamma \overset{?}{=} \alpha \cdot y^\beta \quad (\mathcal{V}(pk, (\alpha, \beta, \gamma)) = 1)$

$\Rightarrow$ CORRECT: $g^\gamma = g^{\beta x + a} = (g^x)^\beta \cdot g^a = y^\beta \cdot \alpha$ ✓

THEO. Above protocol vs HVZK SS.

Proof. First HVZK S:

$S(pk)$: ← $pk = y$

$\beta, \gamma \leftarrow\!\$ \; \mathbb{Z}_q$

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

(α, β, γ)

THIS IS THE SAME DISTRIBUTION.

Given x, y we have

β, α are uniform

and γ is the unique value (mod q)

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

$\equiv$ PERFECT HVZK

$\text{REAL}_{\Pi,t}(\lambda)$

Now SS. Assume PPT $A(y)$ outputting

$\alpha, \beta, \beta', \gamma, \gamma'$ s.t. $\beta \neq \beta'$ and

(α, β, γ), $(\alpha, \beta', \gamma')$ are accepting w.r.t. y.

Then:

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

If exists a, $\beta \neq \beta'$

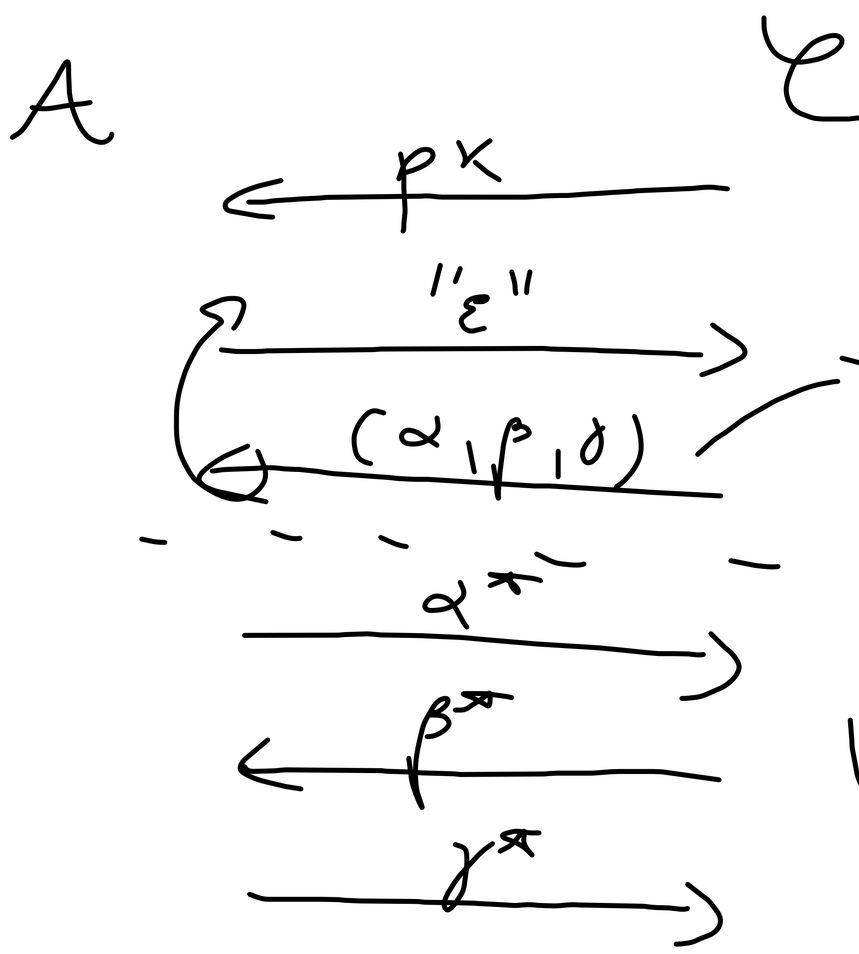
$$g^{\gamma - \gamma'} = y^{\beta - \beta'} \quad ; \quad y = g^{(\gamma - \gamma') \cdot (\beta - \beta')^{-1}} = g^{x}$$

$$x = (\gamma - \gamma') \cdot (\beta - \beta')^{-1}$$

TEO. HVZK + SS $\Rightarrow$ PASSIVE SECURITY.

$(|\mathcal{B}_{\lambda|pk}| = \omega(\log \lambda))$

Proof.

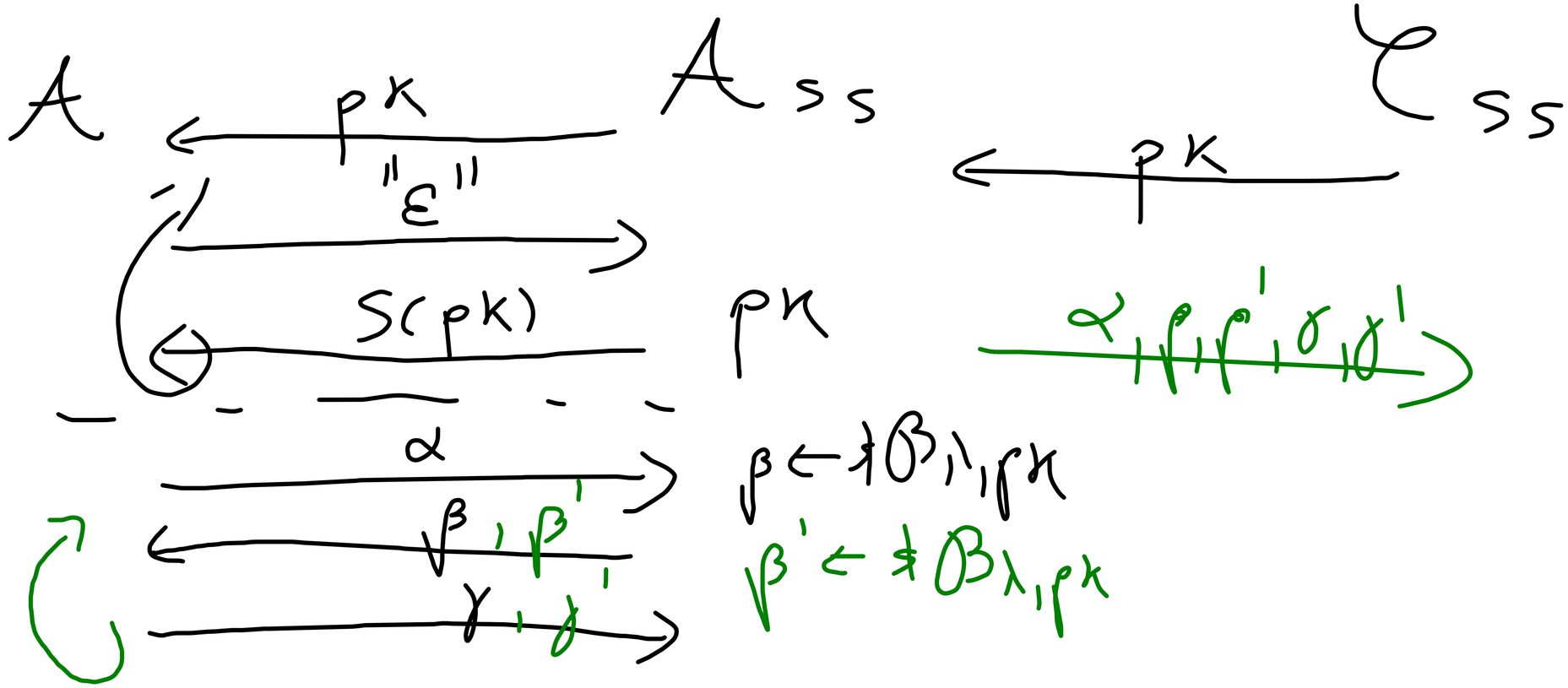


LEMMA. $G(\lambda) \approx_c H(\lambda)$.

Proof. Requires hybrid argument using HVZK. ☒

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

Proof. Reduction to SS.



$\Pr[\text{Adv wins}]$ is the prob. that $\beta \neq \beta'$, and that both

$$\left(> \frac{1}{|B_{\lambda,1,pk}|} \right)$$

here is why we need $|B| = \omega(\log \lambda)$.

(α, β, γ), $(\alpha, \beta', \gamma')$ are accepting.

If the 2 runs of A are indep., then this probability would be $(1/\text{poly})^2$. But they aren't; still one can prove this happens w.p $1/\text{poly}(\lambda)$ ☒