THM SS + HVZK $\Rightarrow$ PASSIVE SECURITY.

(We'll prove this next time.)

We further need one assumption:

- $|\mathcal{B}_{\lambda, pk}|$ is large enough (e.g. $\omega(\log \lambda)$)

Proof. Let $G_0(\lambda) \equiv G^{sd}_{\Pi, A}(\lambda)$

The game for passive security of Π.

Consider $G_1(\lambda)$, identical to $G_0(\lambda)$

but where we use $\mathrm{Sim}(pk)$ to

answer the transcript queries in the game $G_0(\lambda)$.

LEMMA $G_0(\lambda) \approx_c G_1(\lambda)$.

Proof. We will use the HVZK property. It requires a hybrid argument, along these lines: q = # queries.

$G_0(\lambda)$: $P(pk, sk) \rightleftarrows V(pk)$, ..., $P(pk, sk) \rightleftarrows V(pk)$

$H^1(\lambda)$: $\mathrm{Sim}(pk)$, $\underbrace{P \rightleftarrows V, \ldots\ldots, P \rightleftarrows V}_{q-1}$

$H^i(\lambda)$: $\underbrace{\mathrm{Sim}(pk), \ldots\ldots, \mathrm{Sim}(pk)}_{i}$, $P \rightleftarrows V$ ..... $P \rightleftarrows V$

$G_i(\lambda)$: $Sim(pk), \ldots\ldots, Sim(pk)$

$\forall i$: $H^i(\lambda) \approx_c H^{i+1}(\lambda)$

The reduction:

$\mathcal{A}$ $\qquad\qquad$ $\mathcal{A}_{HVZK}$ $\qquad\qquad$ $\mathcal{C}_{HVZK}$

$\mathcal{C}_{HVZK}$: pk, sk; $\tau \leftarrow P \rightleftarrows V$ or $\rightarrow Sim$

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

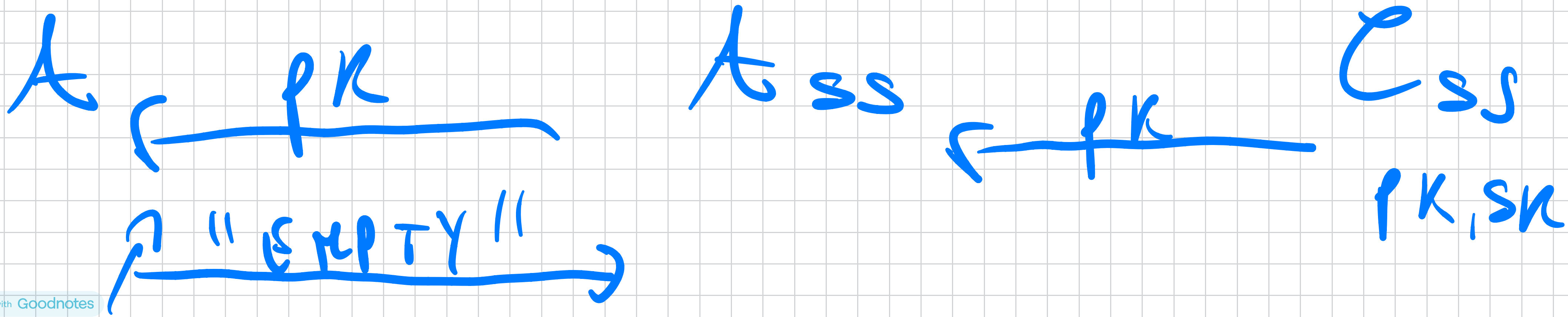
$\#q$: $\mathcal{A} \xrightarrow{\text{"EMPTY"}} \mathcal{A}_{HVZK}$, $\mathcal{A} \xleftarrow{\tau_j} \mathcal{A}_{HVZK}$

$$\tau_j = \begin{cases} Sim(pk), & j \le i \\ \tau, & j = i+1 \\ P \rightleftarrows V, & j \ge i+2 \end{cases}$$

Now, we show: $\forall$ PPT $\mathcal{A}$

$$\Pr[G_1(\lambda) = 1] \leq \mathrm{negl}(\lambda).$$

We make a reduction to SS. Assume not: $\exists$ PPT $\mathcal{A}$ s.t. the above is $\geq 1/\mathrm{poly}(\lambda)$. We build $\mathcal{A}_{SS}$ against SS:



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

$$\tau \leftarrow \mathrm{Sim}(pk)$$

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

$$\xleftarrow{\beta_1^* \leftarrow \mathcal{B}_{\lambda, pk}}$$

1st RUN

$$\xrightarrow{\gamma_1^*}$$

$$\tau_1 = (\alpha^*, \beta_1^*, \gamma_1^*)$$

$$\xleftarrow{\beta_2^* \leftarrow \mathcal{B}_{\lambda, pk}}$$

2nd RUN

$$\xrightarrow{\gamma_2^*}$$

$$\tau_2 = (\alpha^*, \beta_2^*, \gamma_2^*)$$

τ_1, τ_2

To analyze this resolution, let $z \in \{0,1\}^*$ be the RV representing the state of A after it sent α^*. Then we define:

$$\delta_z = \Pr[G_1(\lambda) = 1 \mid t = z]$$

This means: $\Pr[G_1(\lambda) = 1] =$

$$= \sum_z p_z \cdot \delta_z = \mathbb{E}[\delta_z] = \varepsilon(\lambda)$$

where $p_z = \Pr[Z = z]$.

Finally, let Good be the event that $\beta_1^* \neq \beta_2^T$. Now:

$$\Pr\left[G^{ss}_{\Pi, A_{ss}}(\lambda) = 1 \right] \geq$$

$$\Pr\left[G^{ss}_{\Pi, A_{ss}}(\lambda) = 1 \wedge \text{Good} \right]$$

$$= \Pr[\text{Good}] \cdot \Pr[A_{ss} \text{ wins} \mid \text{Good}]$$

$$= \left(1 - \Pr[\overline{\text{good}}]\right) \cdot \Pr[A_{SS} \text{ wins} \mid \text{good}]$$

$$= \left(1 - \frac{1}{|\mathcal{B}_{\lambda, pk}|}\right) \cdot \Pr[A_{SS} \text{ wins} \mid \text{good}]$$

$$\geq \Pr[A_{SS} \text{ wins} \mid \text{good}] - \frac{1}{|\mathcal{B}_{\lambda, pk}|}$$

$$\geq \Pr[A_{SS} \text{ wins} \mid \text{good}] - \mathrm{negl}(\lambda).$$

$$= \sum_z p_z \delta_z^2 - \mathrm{negl}(\lambda)$$

$$= \mathbb{E}[\delta_z^2] - \mathrm{negl}(\lambda)$$

$\rightarrow$ JENSEN'S INEQUALITY

$$\geq \left(\mathbb{E}[\delta_z]\right)^2 - \mathrm{negl}(\lambda)$$

$$\geq \varepsilon^2(\lambda) - \mathrm{negl}(\lambda) \geq \frac{1}{\mathrm{poly}(\lambda)}$$

$\blacksquare$

Let's go back to FIAT-SHAMIR. Given $\Pi = (KGen, P, V)$ we construct $\Sigma = (KGen, Sign, Vrfy)$:

- $KGen(1^\lambda)$: pk, sk
- $Sign(sk, m)$: $\sigma = (\alpha, \gamma)$ s.t.

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

  can share state!

  $\gamma \leftarrow P_2(pk, sk, \alpha, \beta)$
- $Vrfy(pk, \sigma, m)$: Output 1 iff $\underbrace{V(pk, \alpha, \beta, \gamma)}_{=1}$

with $\beta = H(\alpha, m)$

Thm Assuming Π is NON-TRIVIAL and PASSIVELY SECURE, then Σ is UFCMA in the ROM.

Proof. Let A' be a PPT adv. breaking UFCMA of Σ w.p. $1/\text{poly}(\lambda)$.
Wlog. we make a few assumptions on A':

- It never repeats queries.
- Because each signature query in

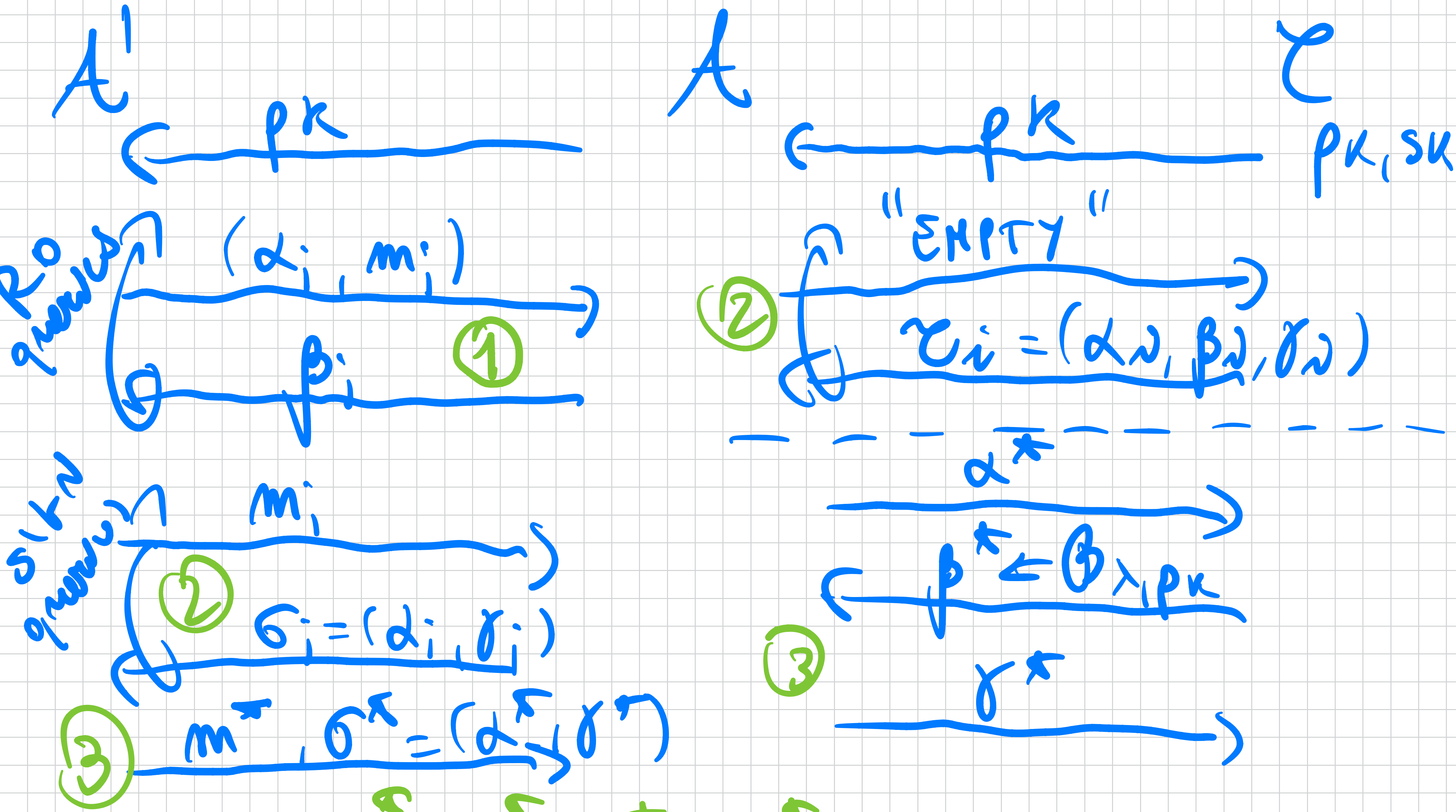
defines $\sigma = (\alpha, \gamma)$ and $\beta = H(\alpha, m)$,
we assume A never queries (α, m)
to the RO after receiving σ.

- Before outputting $\sigma^* = (\alpha^*, \gamma^*)$
it queried (α^*, m^*) to the RO.

Let $q_s = poly(\lambda) = \#$ sign queries

$q_h = poly(\lambda) = \#$ RO queries.

We build A breaking PASSIVE SECURITY



WIN: $\tau^* = (\alpha^*, \beta^*, \gamma^*)$ IS ACCEPTING

At the beginning $\mathcal{A}$:

- Obtains $\tau_i = (\alpha_i, \beta_i, \gamma_i)$ from $\mathcal{C}$ $\forall i \in [q_s]$
- It samples $i^* \leftarrow [q_h]$ as the guess for the RO query (α^*, m^*).

Next:

1. Upon input a RO query (m_i, α_i):
   - If $i \neq i^*$, let $\beta_i \leftarrow \mathbb{Z}_q$ λ, pk

Made with Goodnotes

the reduction hopes

- If $i = i^*$, then $V(m_i, \alpha_i) = (m^*, \alpha^*)$

Then initiate the impersonation (3)
by sending α^* to C.
Let β^* be the challenge from C.
Reply to the RO query with β^*.
(Then, pause the impersonation.)

(2) Upon input a SIGN query m_i
output $\sigma_i = (\alpha_i, \gamma_i)$ where
γ_i, α_i are from $\tau_i = (\alpha_i, \beta_i, \gamma_i)$

Also, program the RO s.t.

$$H(\alpha_\nu, m_\nu) \overset{!}{=} \beta_\nu .$$

If (α_ν, m_ν) was queried before to the RO, then ABORT.

③ When A' outputs $m^*, \sigma^* = (\alpha^*, \gamma^*)$ check that the guess on ν^* was correct. If not, ABORT.
If yes, resume ③ and send γ^* to C.

Analysis :

- If it doesn't abort, the reduction is perfect.

- Prob. of not ABORTING in step ③ is $1/\mathrm{poly}(\lambda) = 1/q_h$.

- Proob of aborting in step ② is negligible. This is because for each signature query $\alpha_i = \alpha_j$

from a previous RO query with negl prob. by NON-TRIVIALITY of Π.

$\Rightarrow$ Prob. of NOT ABORTING in step ② is: $\left(1 - q_s \cdot \mathrm{negl}(\lambda)\right)$

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

$$\Rightarrow \Pr[A \text{ WINS}] \geq \frac{1}{\mathrm{poly}(\lambda)} \cdot \frac{1}{\mathrm{poly}} \cdot \Pr[A' \text{ WINS}]$$

$\blacksquare$

- In the next couple of lectures we will study a little bit of post-quantum crypto.

- Let's do a poll for the last topic:
  *) ZK for all of NP.
  *) CCA security for PKE.
  In particular the Cramer-Shoup PKE from DDH.

*) IDENTITY-BASED ENCRYPTION.

*) CRYPTO WITH WEAK KEYS:
what happens when the secret key is not UNIFORM but has some min-entropy.

- We'll also do one session of exercises.