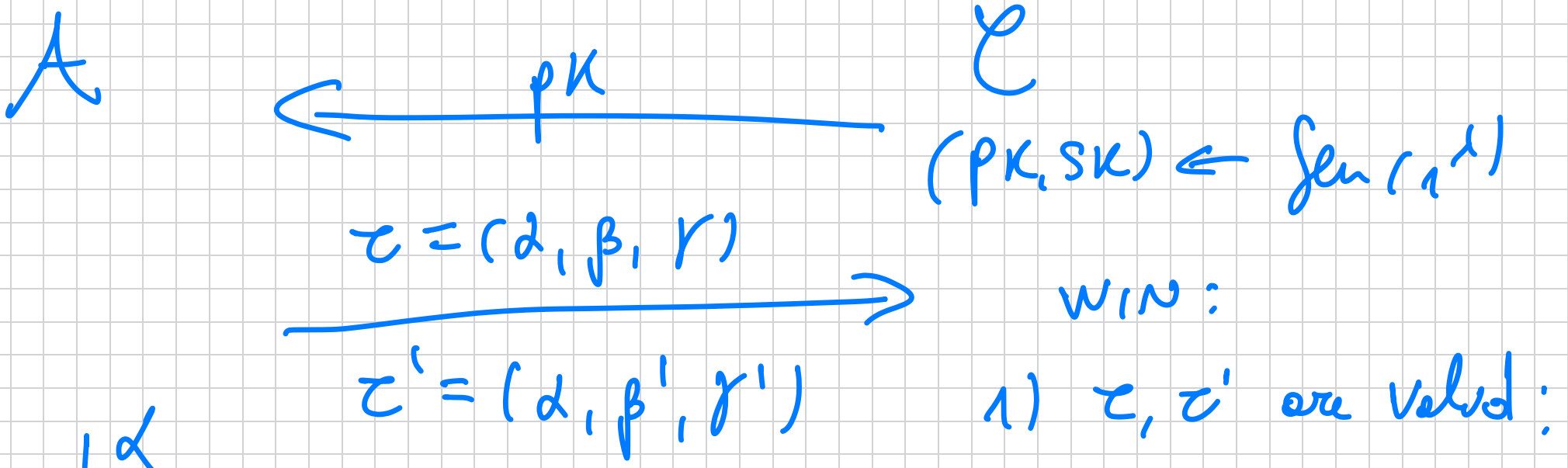
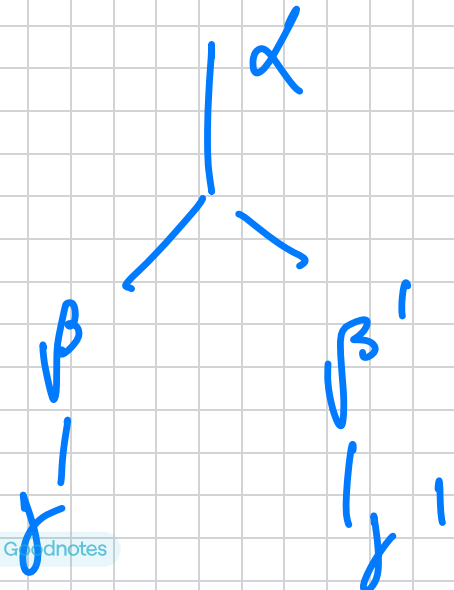
Def A canonical ID scheme satisfies special soundness if $\forall$ PPT A the following game can only be won with negl(λ) prob.:





Made with Goodnotes

What does it mean? So, soundness is about hardness of proving false statements for a MALICIOUS PROVER.

But for some languages like:

$$L = \{ y \in G : \exists x \text{ s.t. } g^x = y \}$$

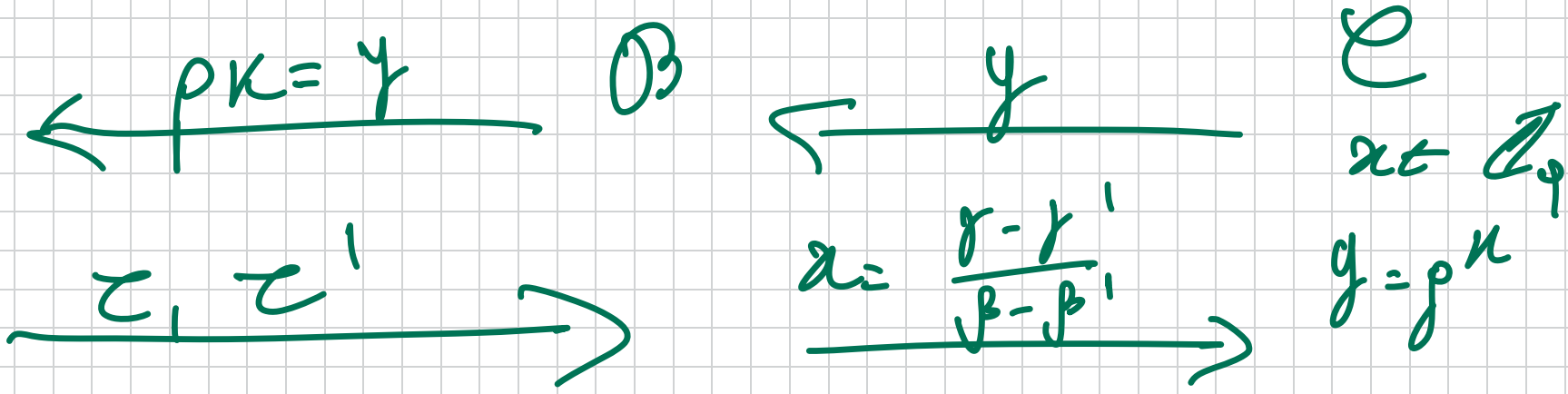
SOUNDNESS is trivial as every statement $y \in G$ is TRUE. But something better would be to say that any prover that can convince the verifier MUST KNOW x.

For Schnorr: Under the DL assumption in G, the protocol is SPECIAL SOUND.

Made with Goodnotes

Assume not, $\exists$ PPT A that w.p. $1/poly(\lambda)$ and given pk outputs $\tau = (\alpha, \beta, \gamma)$, $\tau' = (\alpha', \beta', \gamma')$ as above.

Then $\exists$ PPT B that breaks DL with the same probability:



How to find x? Well, by def.:

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

Made with Goodnotes

$$\Leftrightarrow \quad y^{\beta-\beta'} = g^{\gamma-\gamma'}$$

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

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

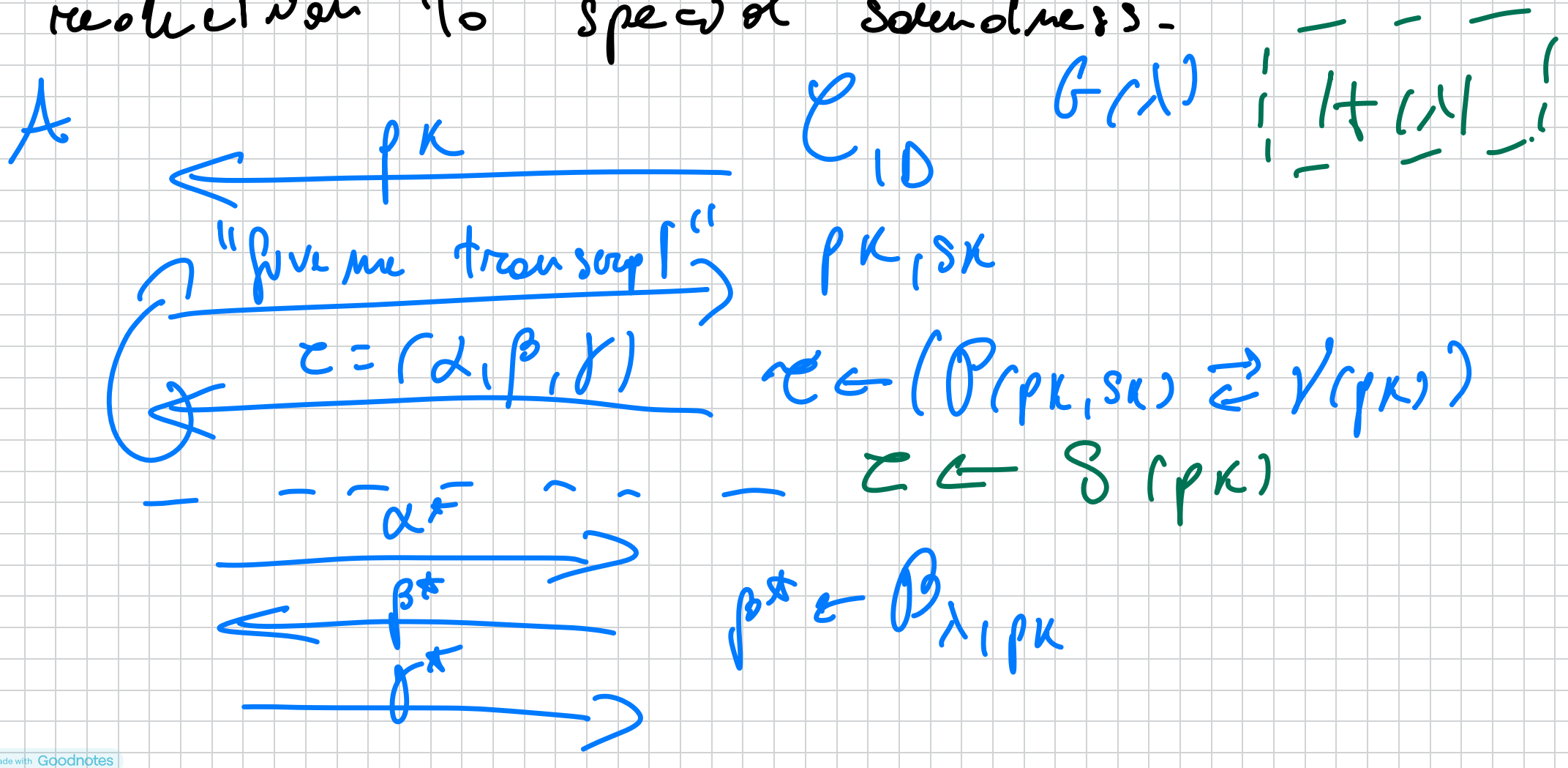
$\exists!$ exists as $\beta \neq \beta'$

$$\Pr[\mathcal{B} \text{ wins}] = \Pr[A \text{ wins}] \geq 1/\text{poly}(\lambda).$$

Next, we show the two properties imply passive security.

THM SS + HVZK $\Rightarrow$ PASSIVE ID so long as $|B_{pk,\lambda}| = \omega(\log \lambda)$.

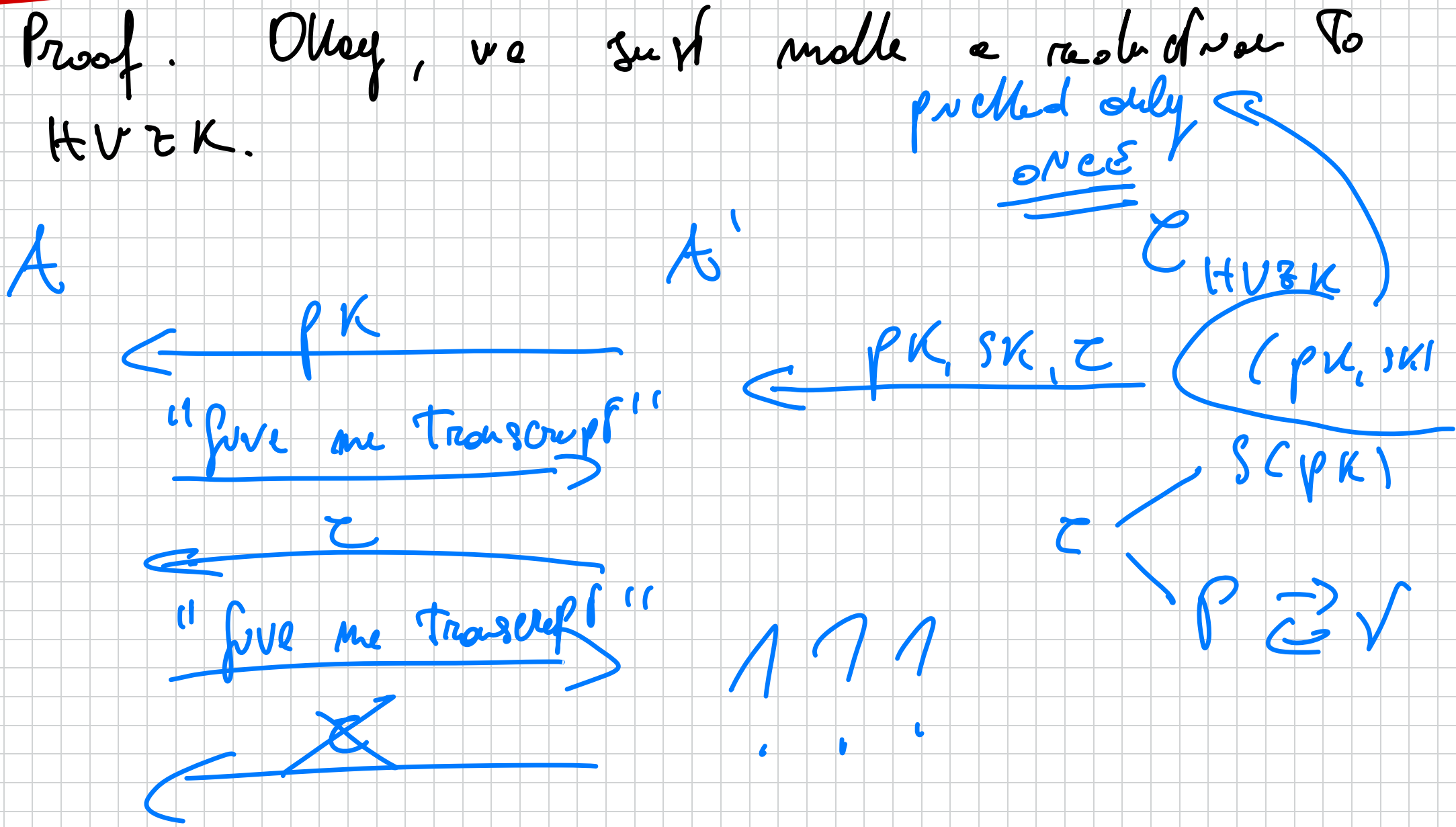
Proof. The main idea will be to make a reduction to special soundness.



Made with Goodnotes

LEMMA $H(\lambda) \tilde{\approx}_c G(\lambda)$.

Proof. Okay, we just make a reduction to HVZK.



Made with Goodnotes

Hybrid argument !

H_0 | H_1 | H_q

$c_1 \leftarrow (p \rightleftarrows v)$ | $c_1 \leftarrow S(pk)$ | $c_1 \leftarrow S(pk)$

$c_2 \leftarrow (p \rightleftarrows v)$ | $c_2 \leftarrow (p \rightleftarrows v)$ | ...

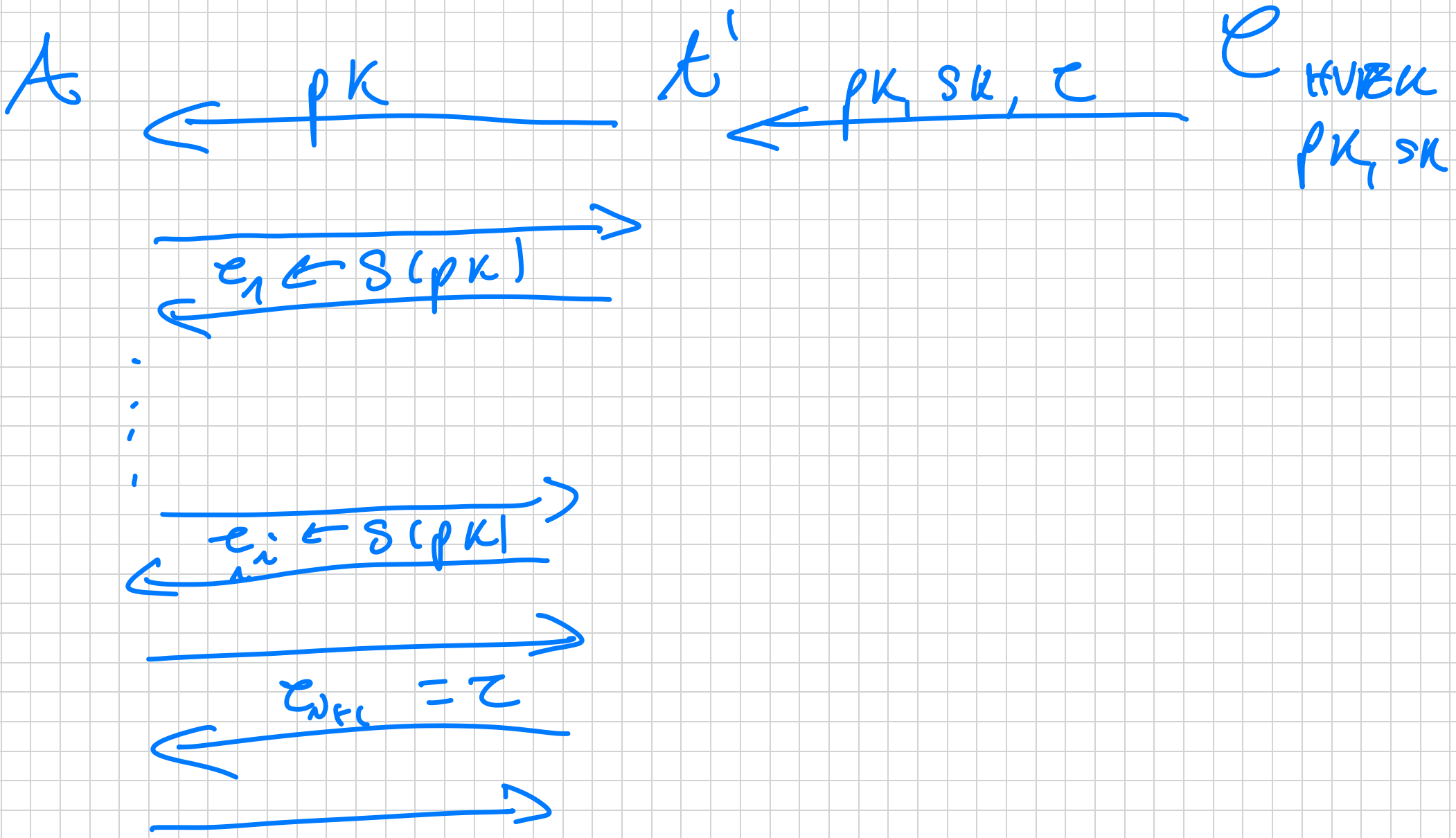
$c_q \leftarrow (p \rightleftarrows v)$ | $c_q \leftarrow (p \rightleftarrows v)$ | $c_q \leftarrow S(pk)$

$\equiv G(\lambda)$ | $H(\lambda)$

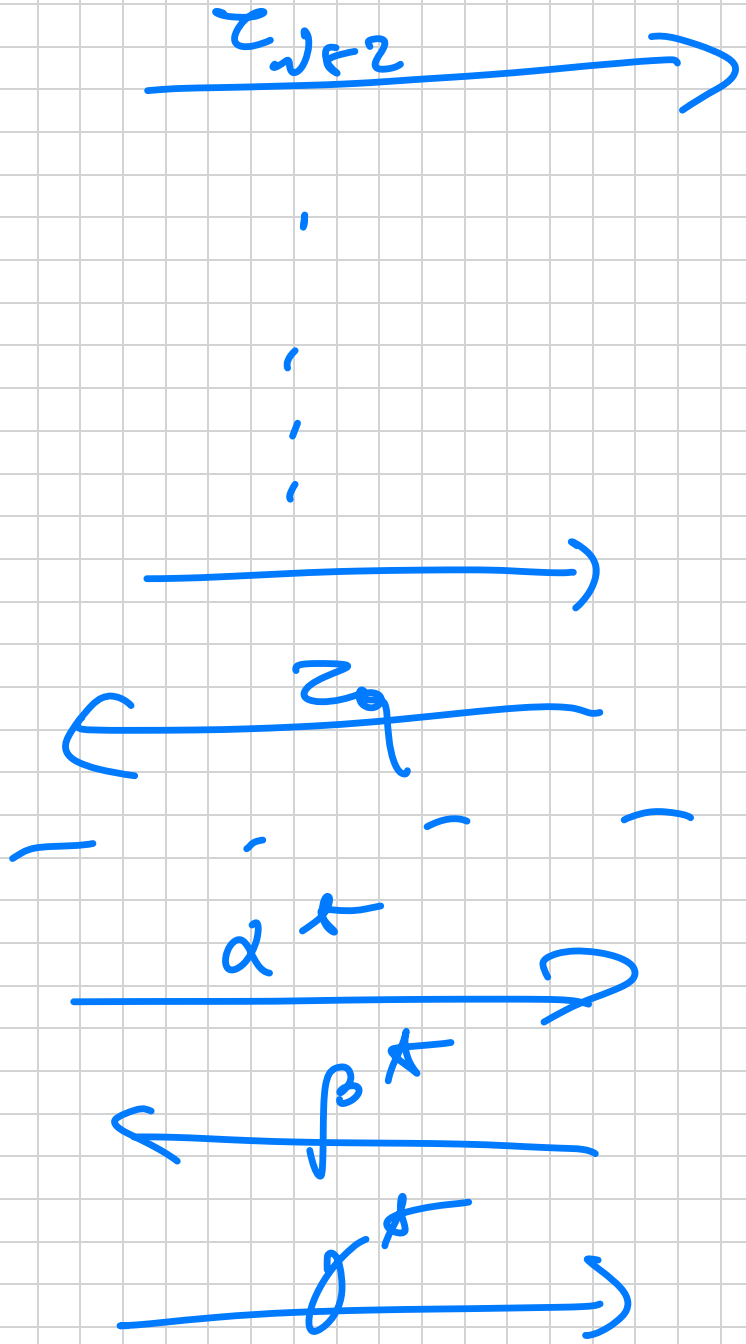
$\forall \lambda$: $H_\lambda \approx_c H_{\lambda+1}$

Made with Goodnotes

Now we can make the reduction!



Made with Goodnotes



$\tau_{N+2}, \dots, \tau_q$

$\leftarrow \left(\beta(\rho_k, s_k) \rightleftarrows \gamma(\rho_k) \right)$

↳ The reduction

Knows s_k !!!

$\beta^* \leftarrow \beta_{\lambda, \rho_k}$

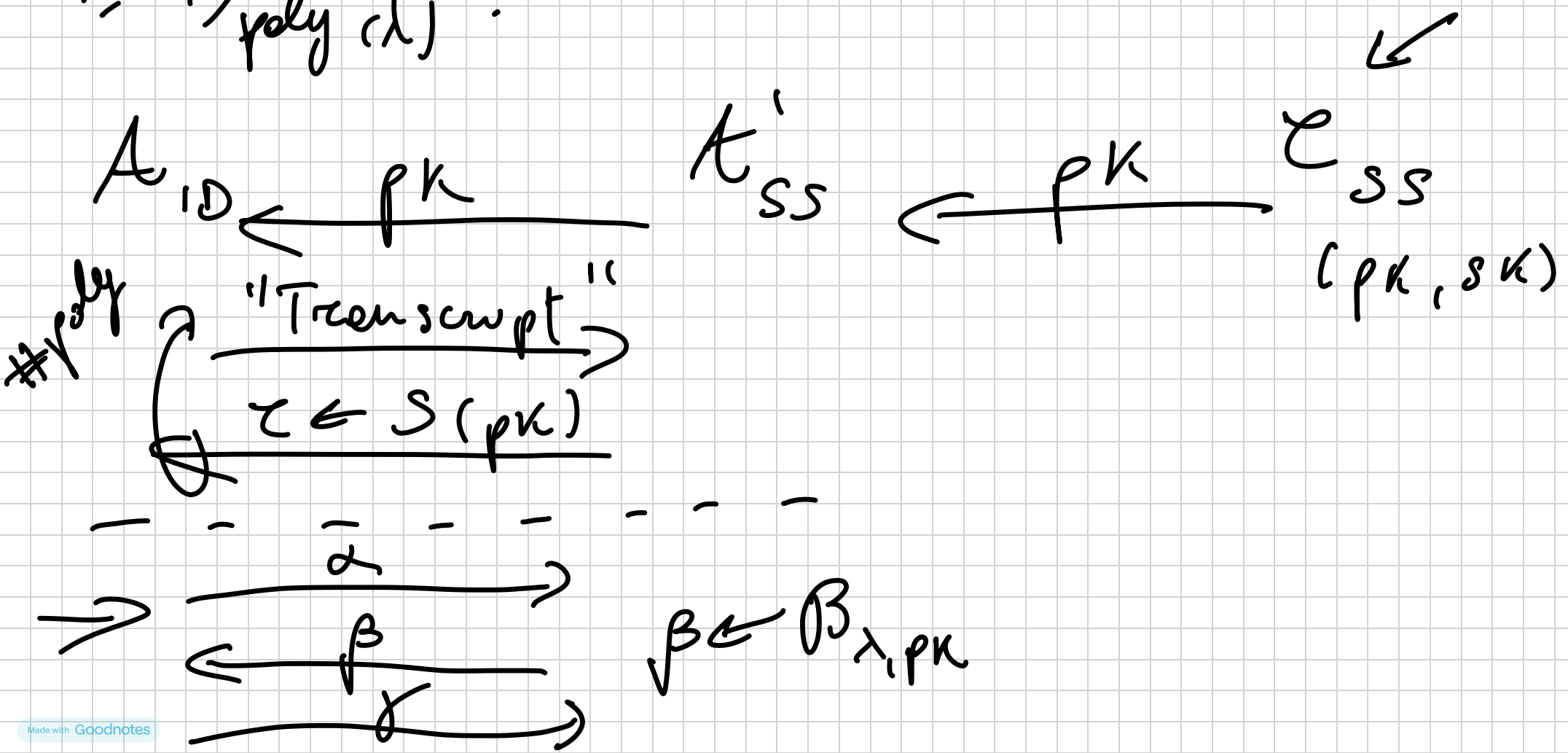
Made with Goodnotes

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

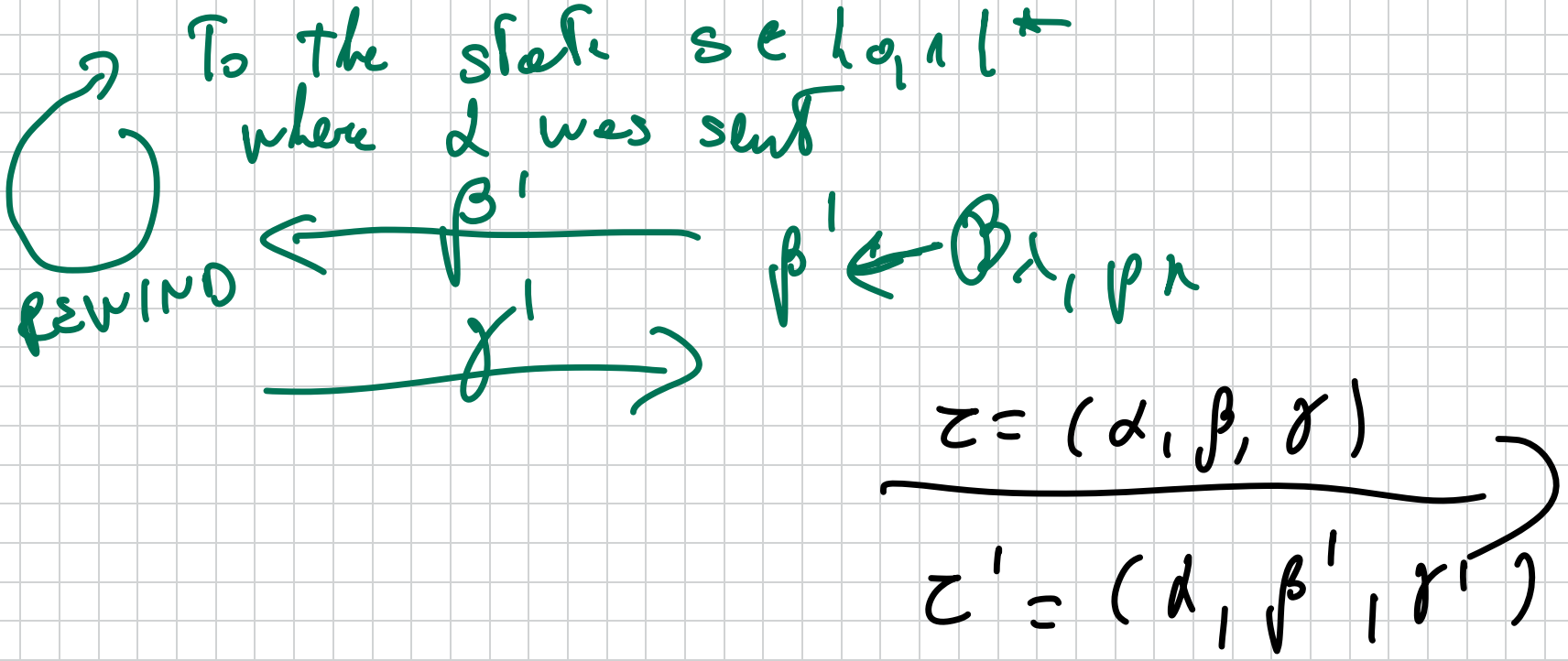
Proof. We now make the reduction to SS.

Assume $\exists$ PPT A s.t. $\Pr[H(\lambda)=1] = \varepsilon(\lambda)$

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



Made with Goodnotes



All we need is to show : (1) $\beta \neq \beta'$; (2)
τ, τ' accepting w.p. $\geq 1/poly(\lambda)$.

If τ, τ' would be independent, we'd be already done. But they are not.

As we said, $\varepsilon(\lambda) = Pr[H(\lambda) = 1]$. Let

Made with Goodnotes

$s \in \{0,1\}^k$ be the state of A after it sent α; and call $p_s = Pr[S = s]$. Now:

$$\varepsilon(\lambda) = \mathbb{E}[\delta_S] = \sum_s p_s \cdot \delta_s$$

$$\delta_s = Pr[H(\lambda) = \lambda \mid S = s]$$

Moreover, let GOOD : event that $\beta' \neq \beta$.

$$Pr[A' \text{ WINS}] \geq Pr[\tau, \tau' \text{ ACCEPTING} \wedge \text{GOOD}]$$

$$= Pr[\tau, \tau' \text{ ACCEPTING} \mid \text{GOOD}] \cdot (1 - Pr[\overline{\text{GOOD}}])$$

$$= Pr[\tau, \tau' \text{ ACCEPTING} \mid \text{GOOD}]$$

Made with Goodnotes

$$- \underbrace{\Pr[\overline{\text{GOOD}}]}_{\geq |B_{\lambda,pk}|^{-1}} \cdot \underbrace{\Pr[\tau, \tau' \text{ Acc.} \mid \text{GOOD}]}_{\leq 1}$$

$$\geq \Pr[\tau, \tau' \text{ Acc.} \mid \text{GOOD}] - |B_{\lambda,pk}|^{-1}$$

$$= \sum_s p_s \cdot \delta_s^2 - |B_{\lambda,pk}|^{-1}$$

$$= \mathbb{E}[\delta_s^2] - |B_{\lambda,pk}|^{-1}$$

$$\geq (\mathbb{E}[\delta_z])^2 - |B_{\lambda,pk}|^{-1}$$

↳ JENSEN

$$= \varepsilon^2(\lambda) - \text{negl}(\lambda) = 1/\text{poly}(\lambda) \quad \blacksquare$$

Made with Goodnotes