Limitations of the Meta-Reduction Technique

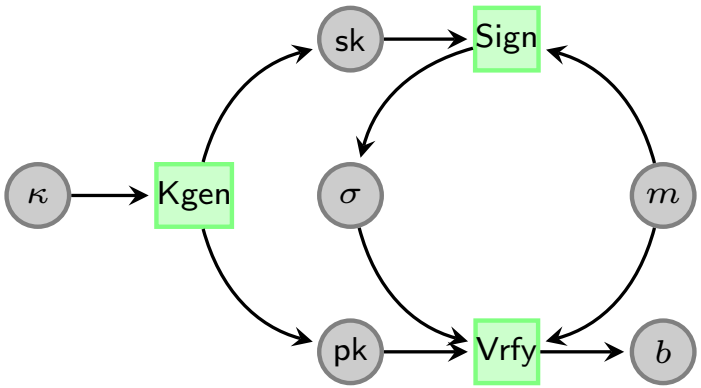
Nils Fleischhacker

Technische Universität Darmstadt

September 2, 2012

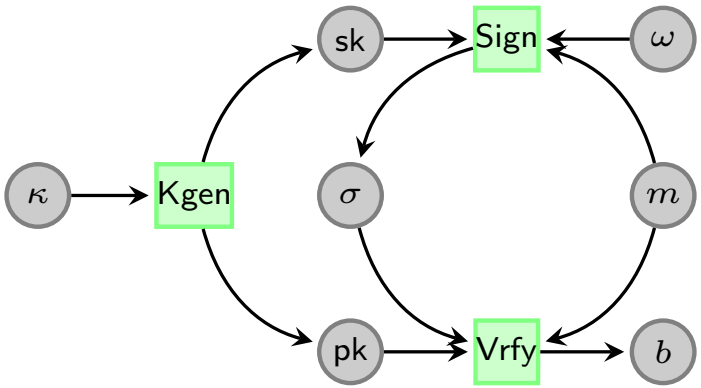
Signatures
... with Reasonable Randomization

$$\mathcal{S} = (\mathsf{Kgen}, \mathsf{Sign}, \mathsf{Vrfy})$$



Signatures
... with Reasonable Randomization

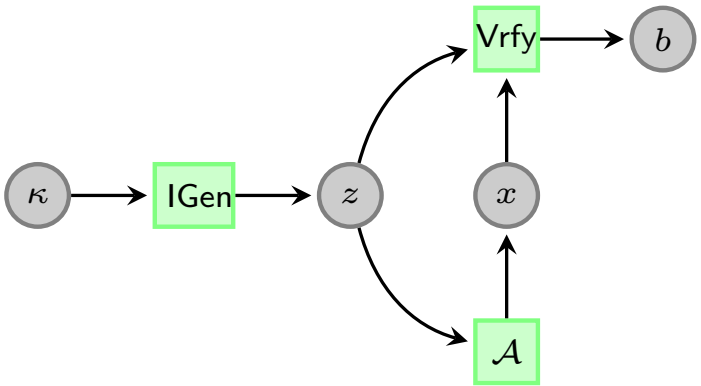
$$\mathcal{S} = (\mathsf{Kgen}, \mathsf{Sign}, \mathsf{Vrfy})$$



$$H_\infty\left(\mathsf{Sign}(\mathsf{pk}, m)\right) \in \omega(\log(\kappa))$$

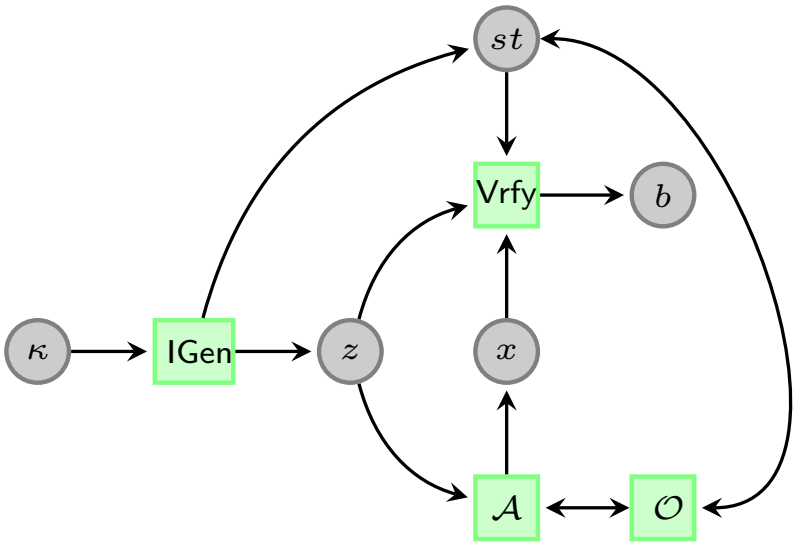
Problems

$$\Pi = (\mathsf{IGen}, \mathsf{Thresh}, \mathsf{Vrfy})$$



Problems

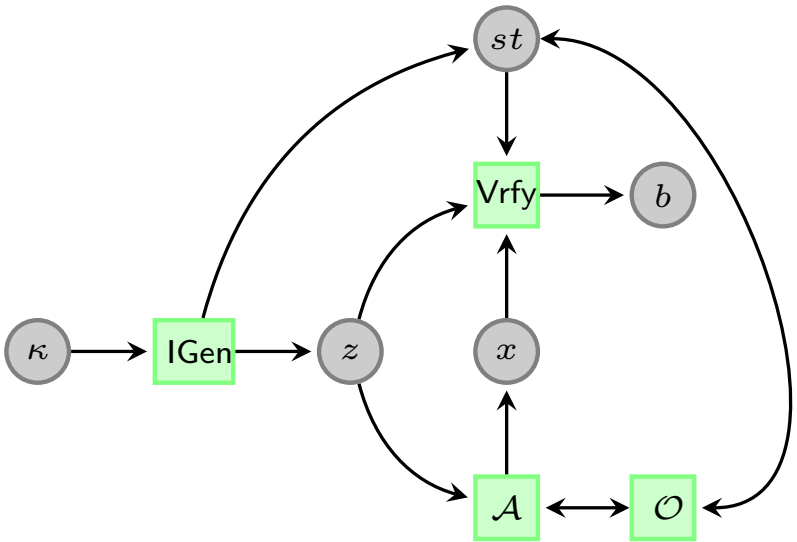
$$\Pi = (\mathsf{IGen}, \mathsf{Thresh}, \mathsf{Vrfy}, \mathcal{O})$$



TECHNISCHE UNIVERSITÄT DARMSTADT

Problems

$$\Pi = (\mathsf{IGen}, \mathsf{Thresh}, \mathsf{Vrfy}, \mathcal{O})$$

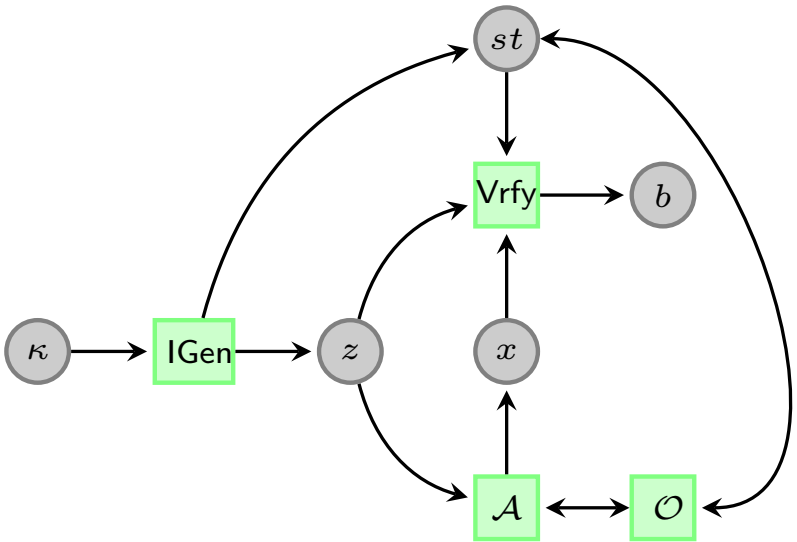


$$\mathsf{Exp}^{\Pi}_{\mathcal{A}}(\kappa) : \left[\begin{array}{c} z \leftarrow \mathsf{IGen}(\kappa) \\ x \leftarrow \mathcal{A}^{\mathcal{O}}(z) \\ b \leftarrow \mathsf{Vrfy}(z, x) \\ \text{output } b \end{array}\right]$$

TECHNISCHE UNIVERSITÄT DARMSTADT

Problems

$$\Pi = (\mathsf{IGen}, \mathsf{Thresh}, \mathsf{Vrfy}, \mathcal{O})$$

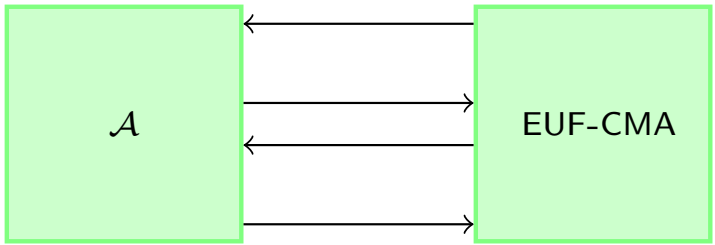


$$\mathsf{Exp}^{\Pi}_{\mathcal{A}}(\kappa) : \left[\begin{array}{c} z \leftarrow \mathsf{IGen}(\kappa) \\ x \leftarrow \mathcal{A}^{\mathcal{O}}(z) \\ b \leftarrow \mathsf{Vrfy}(z, x) \\ \text{output } b \end{array}\right]$$

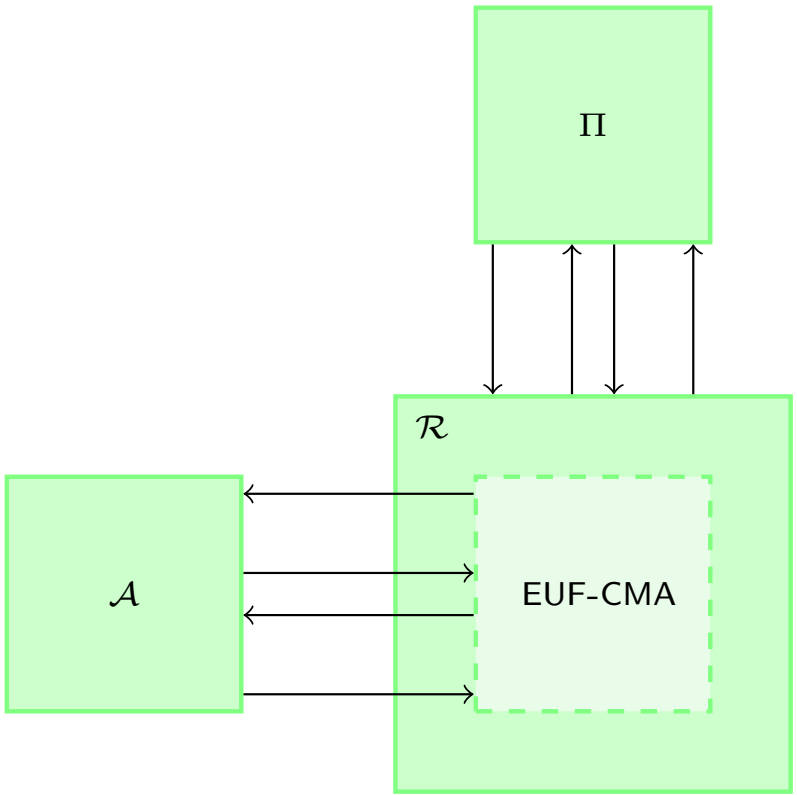
$$\mathsf{Adv}^{\mathcal{A}}_{\Pi}(\kappa) = \begin{array}{l} \Pr\left[\mathsf{Exp}^{\Pi}_{\mathcal{A}}(\kappa) \stackrel{?}{=} 1\right] \\ -\Pr\left[\mathsf{Exp}^{\Pi}_{\mathsf{Thresh}}(\kappa) \stackrel{?}{=} 1\right] \end{array}$$

TECHNISCHE UNIVERSITÄT DARMSTADT

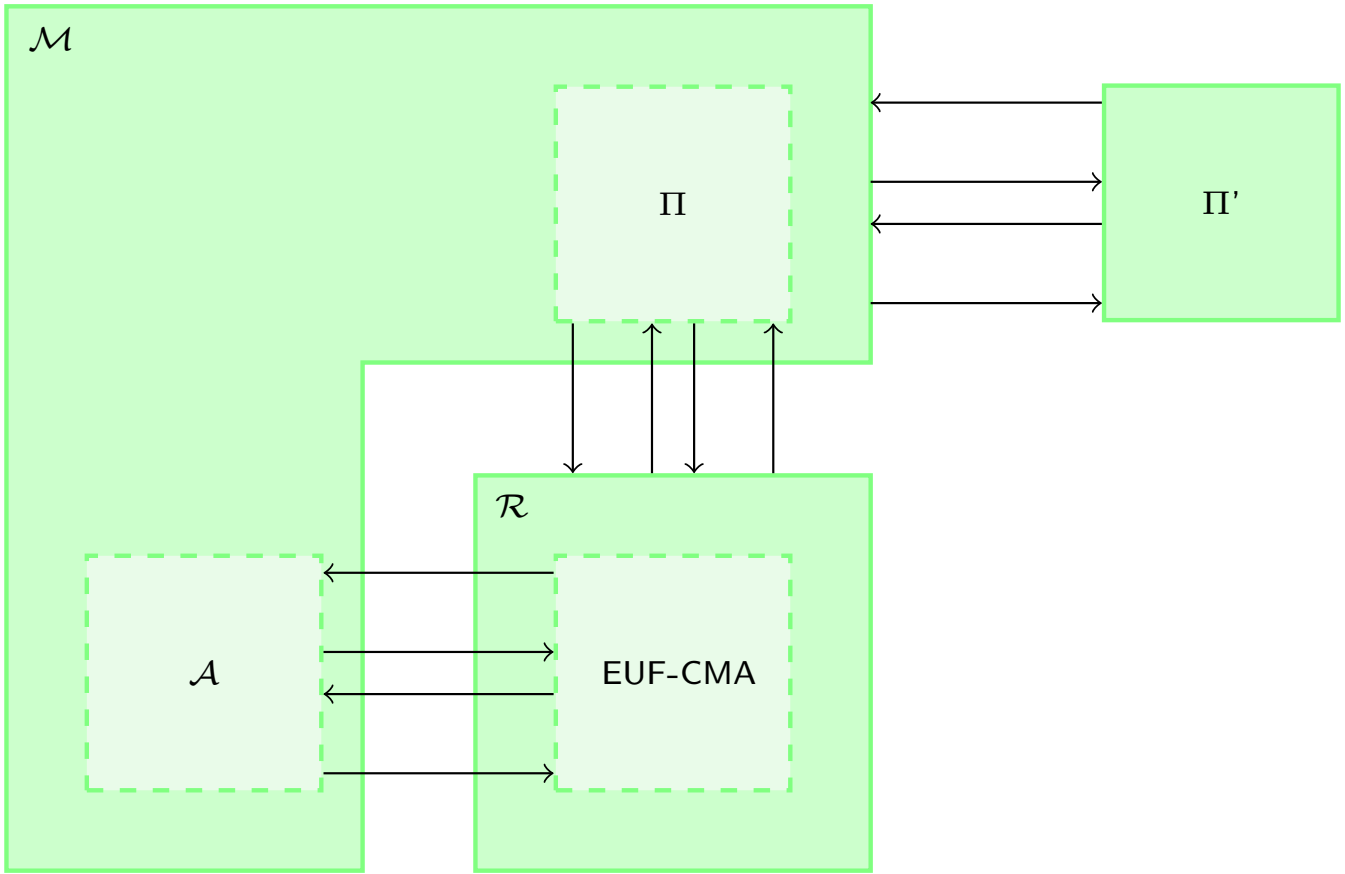
Reductions and Meta-Reductions



Reductions and Meta-Reductions

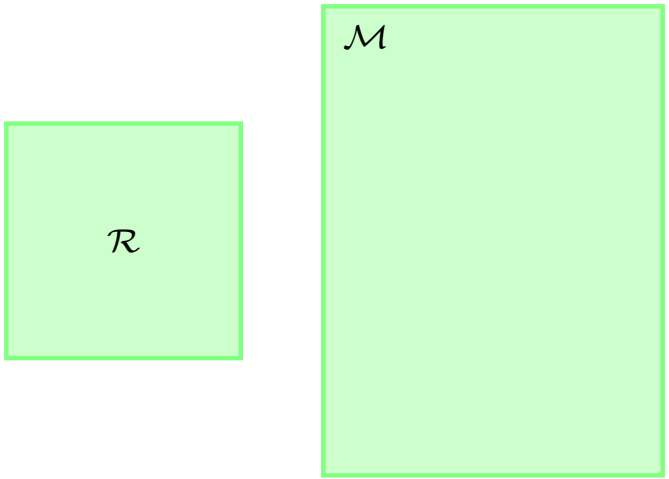


Reductions and Meta-Reductions

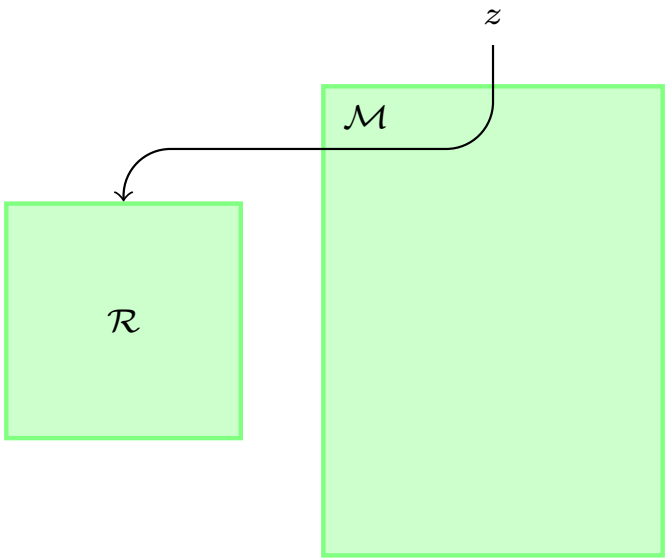


TECHNISCHE UNIVERSITÄT DARMSTADT

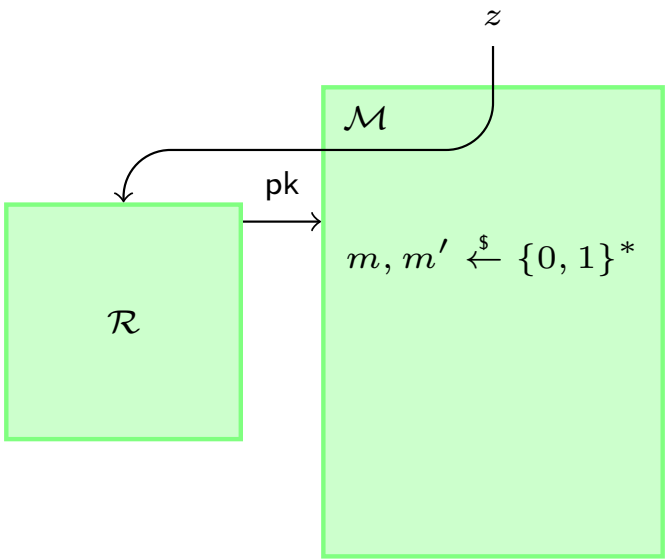
The “Standard” Technique



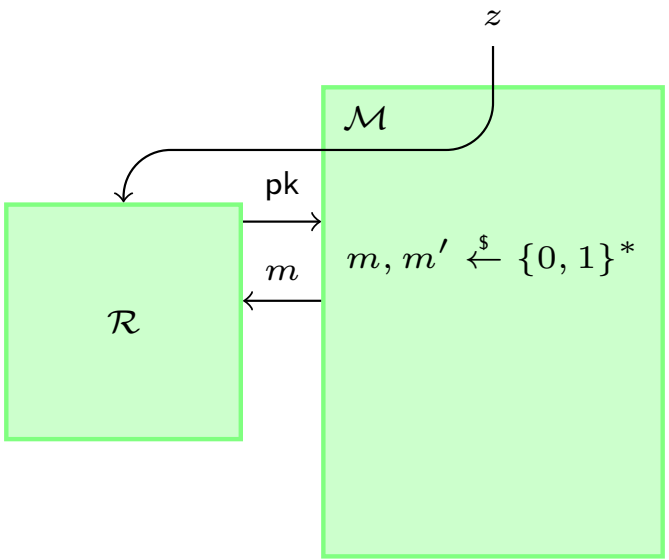
The “Standard” Technique



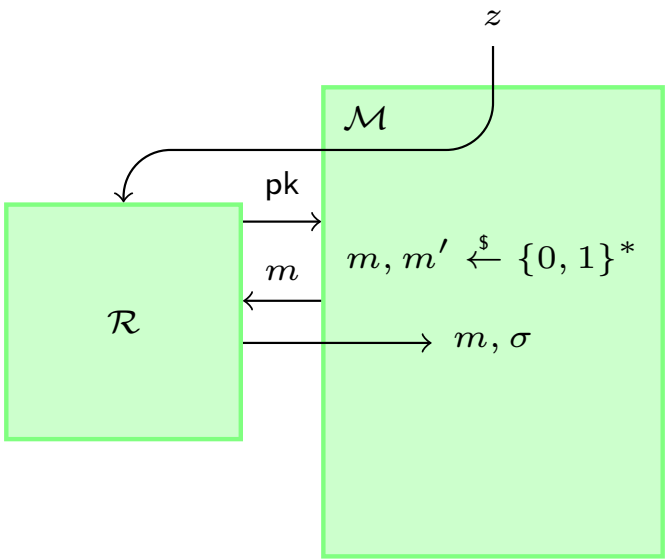
The "Standard" Technique



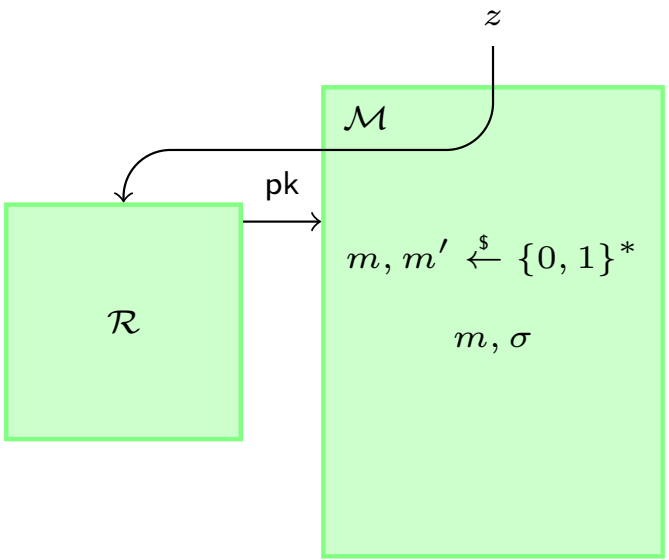
The "Standard" Technique



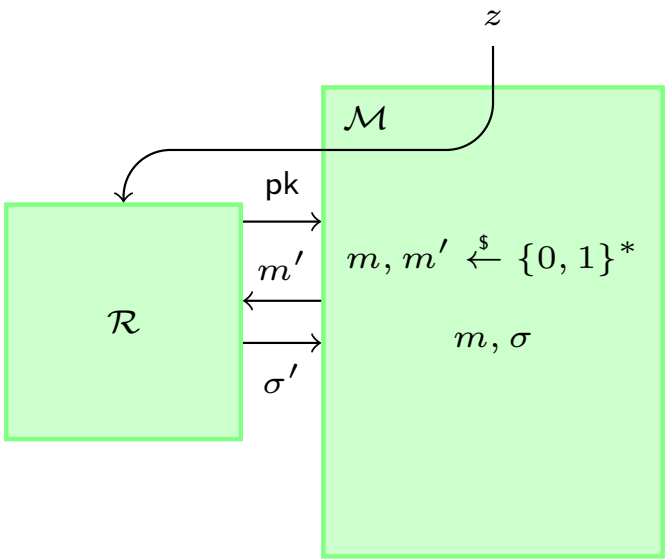
The "Standard" Technique



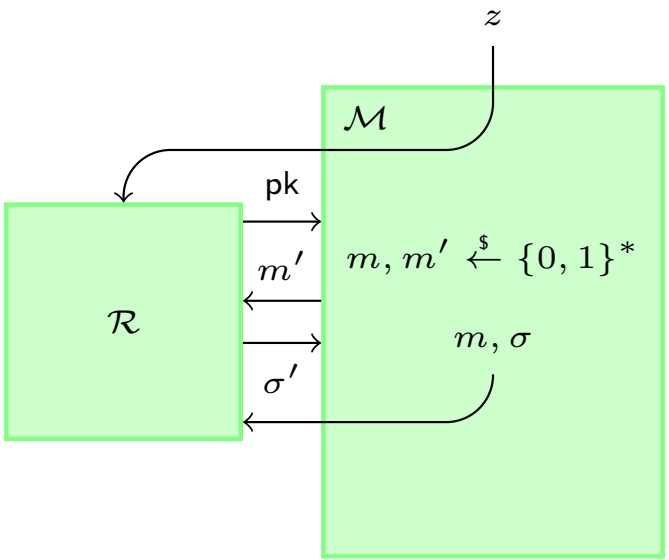
The "Standard" Technique



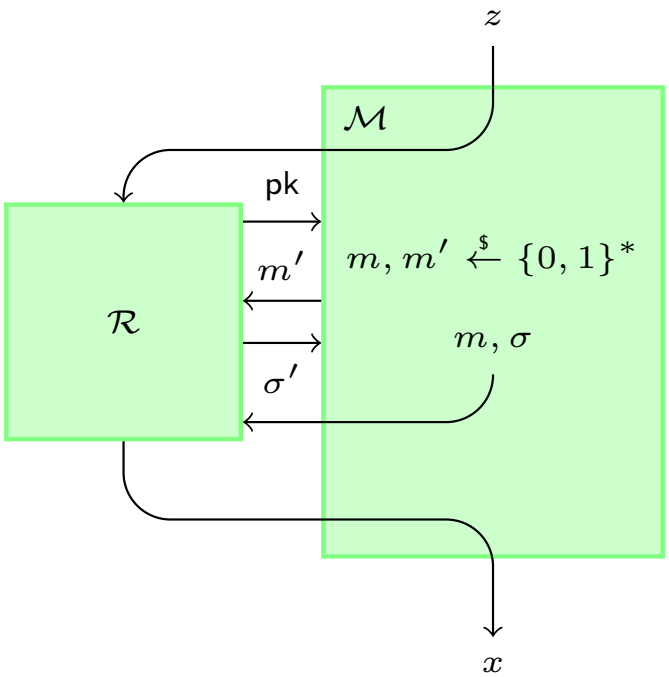
The "Standard" Technique



The "Standard" Technique



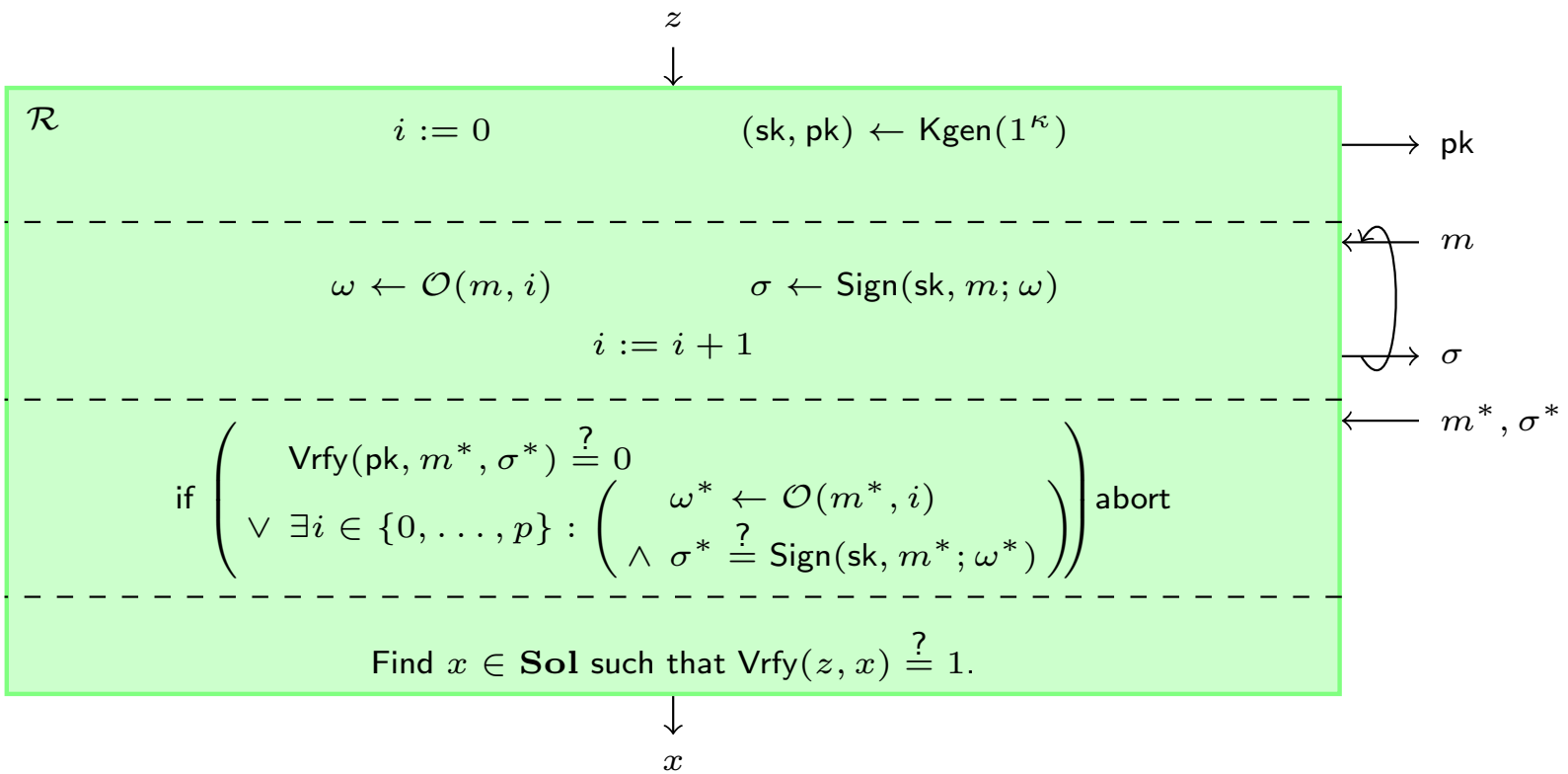
The "Standard" Technique



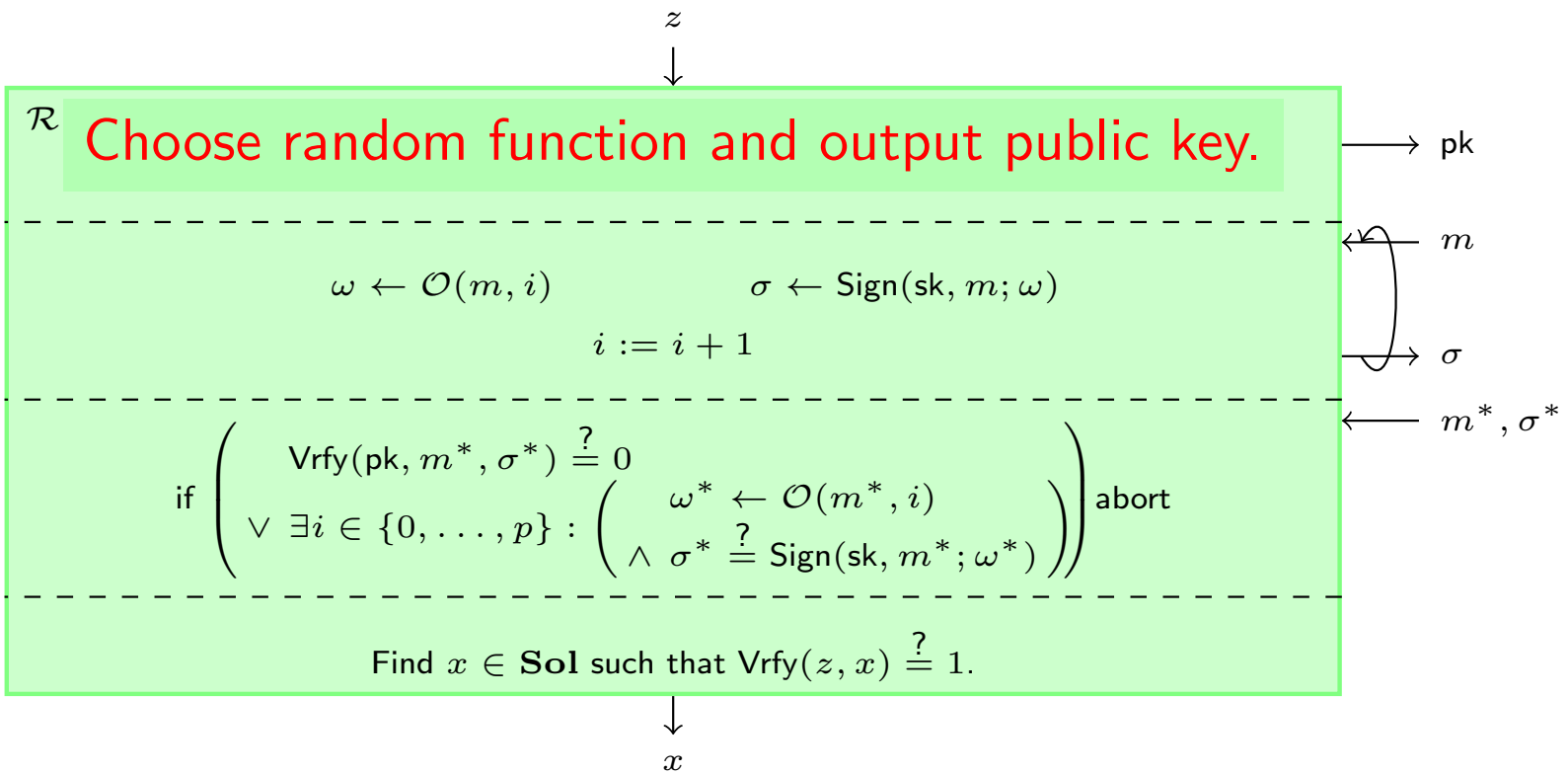
The “Standard” Technique

So, what’s the problem?

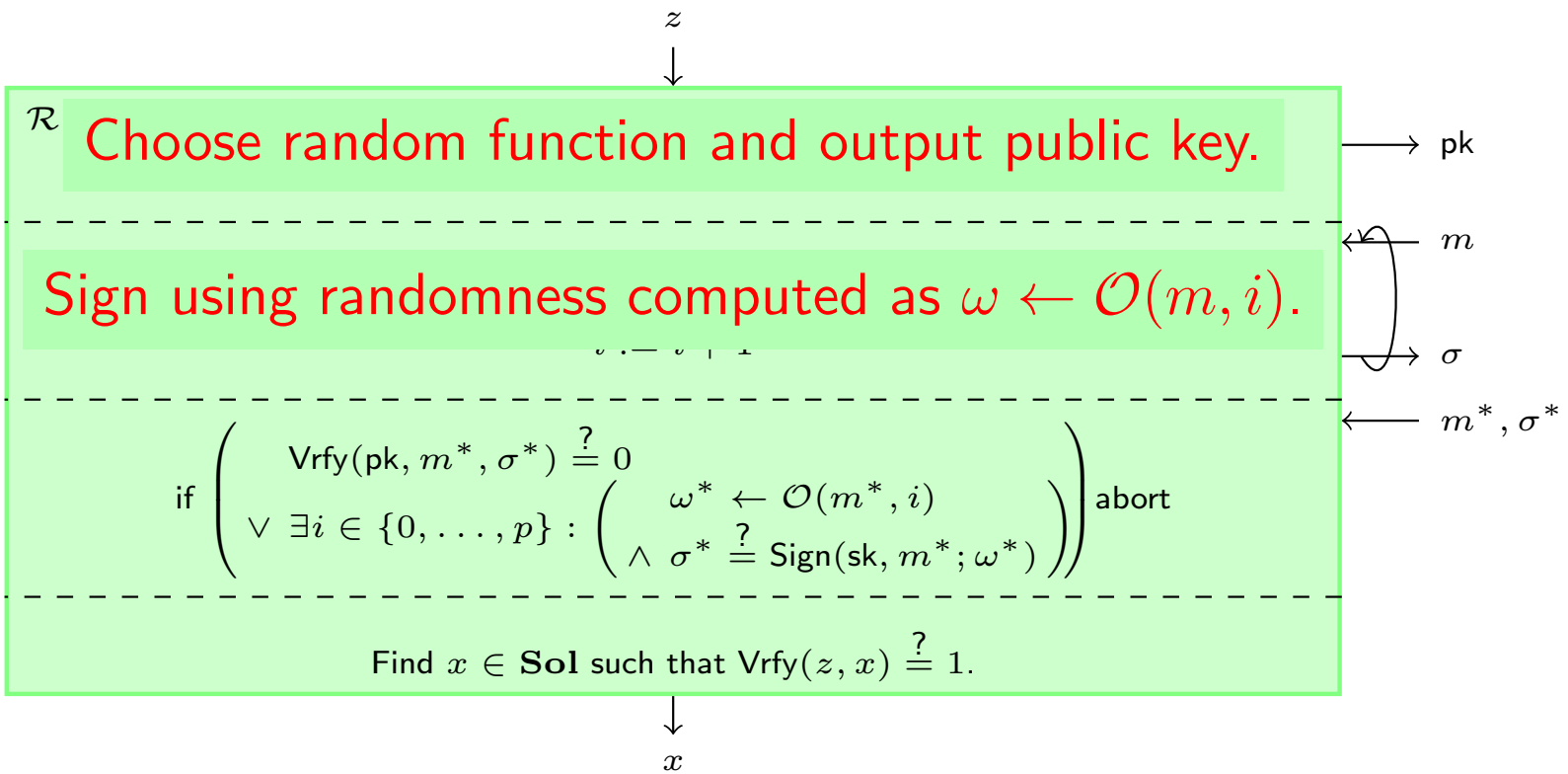
Well, as it turns out...



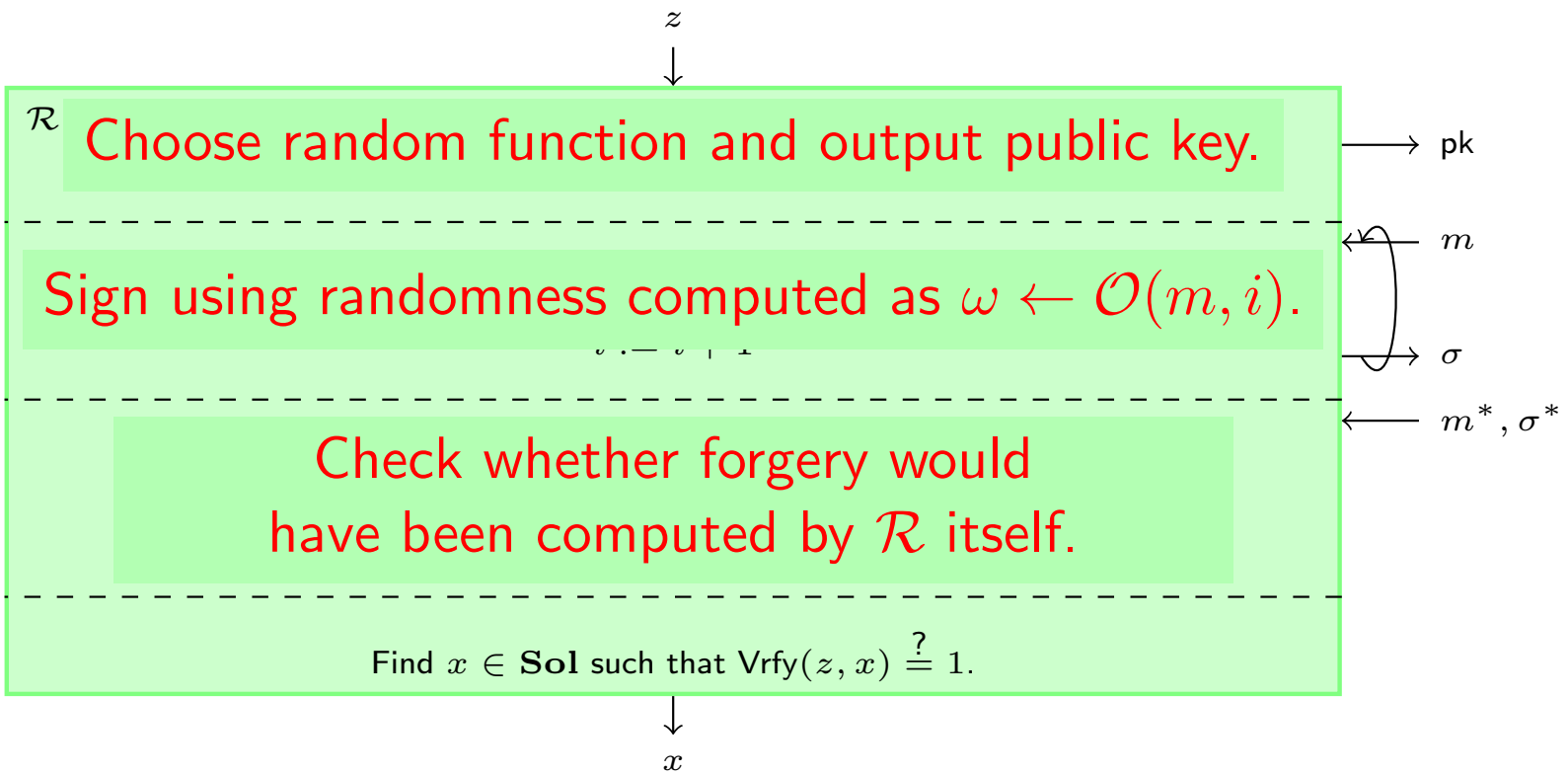
Well, as it turns out...



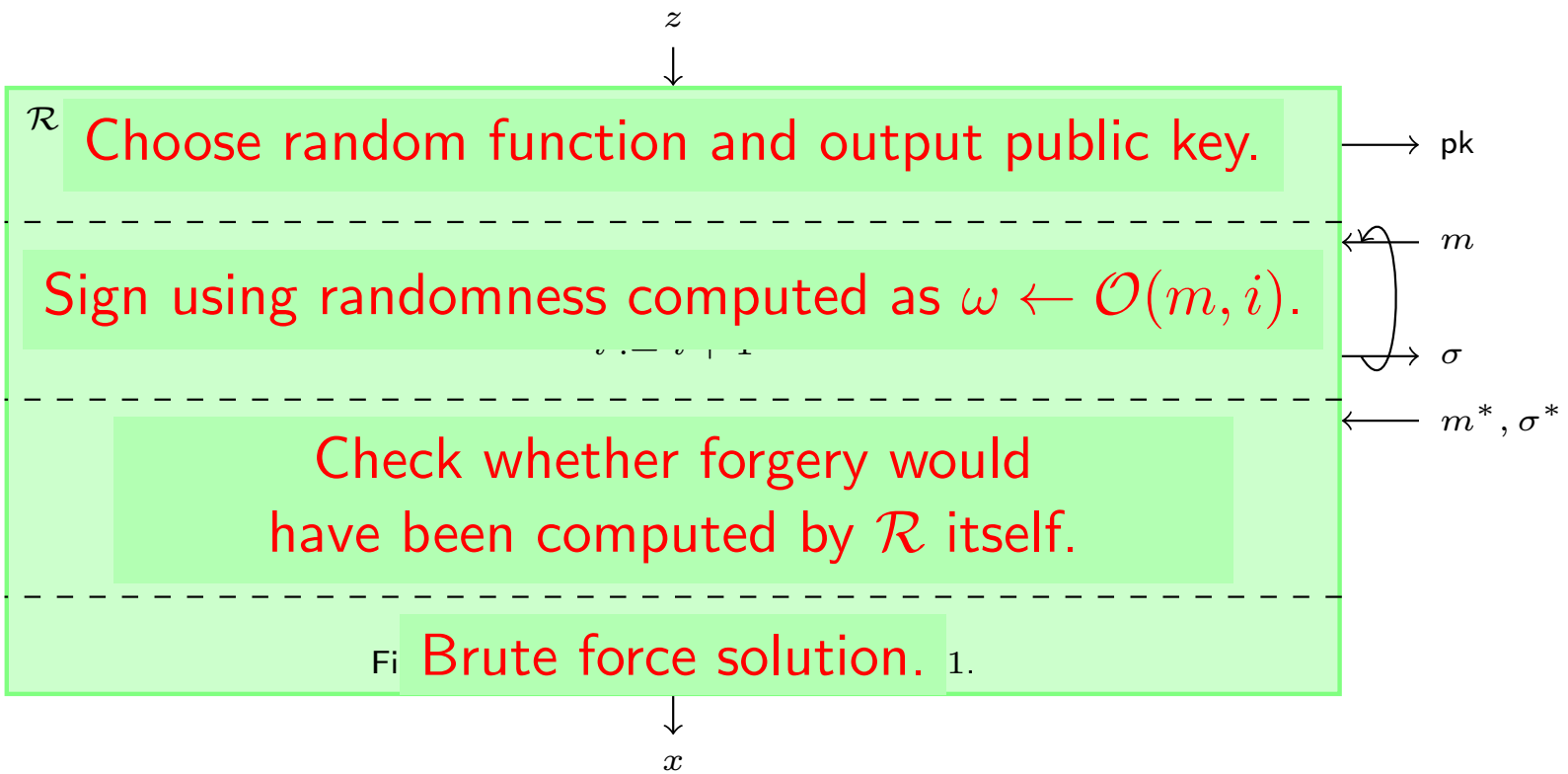
Well, as it turns out...



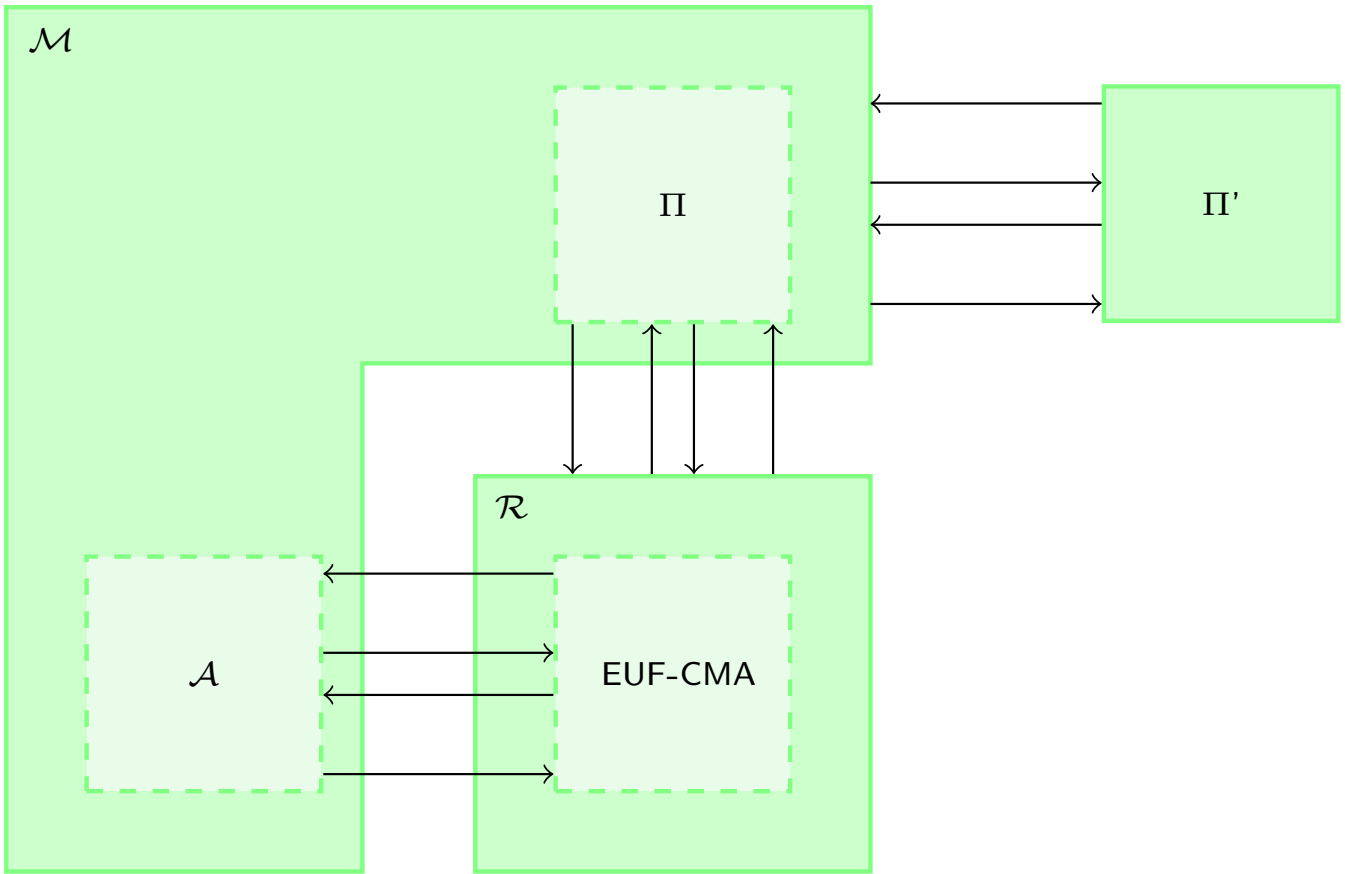
Well, as it turns out...



Well, as it turns out...

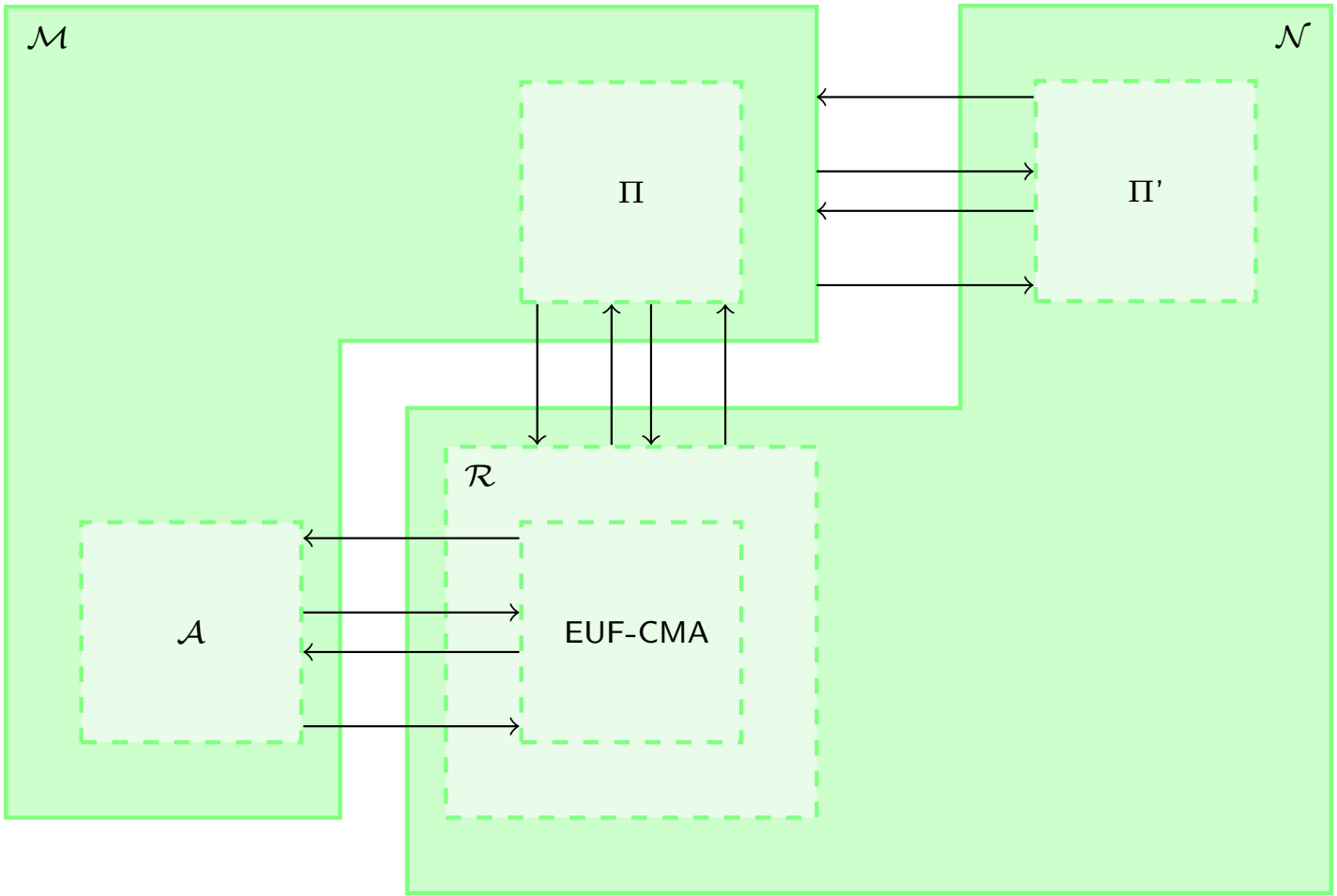


Meta-Meta-Reduction

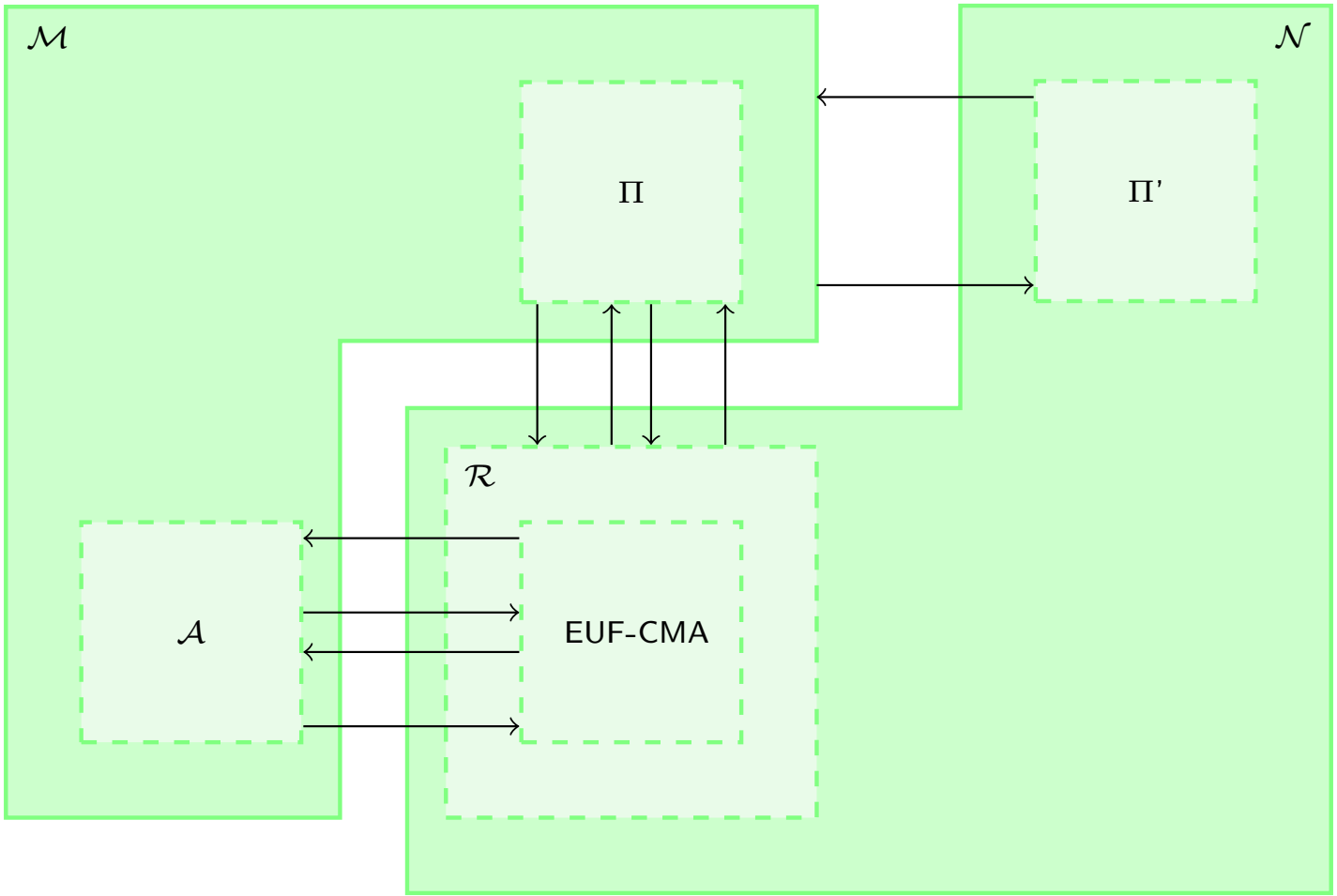


TECHNISCHE UNIVERSITÄT DARMSTADT

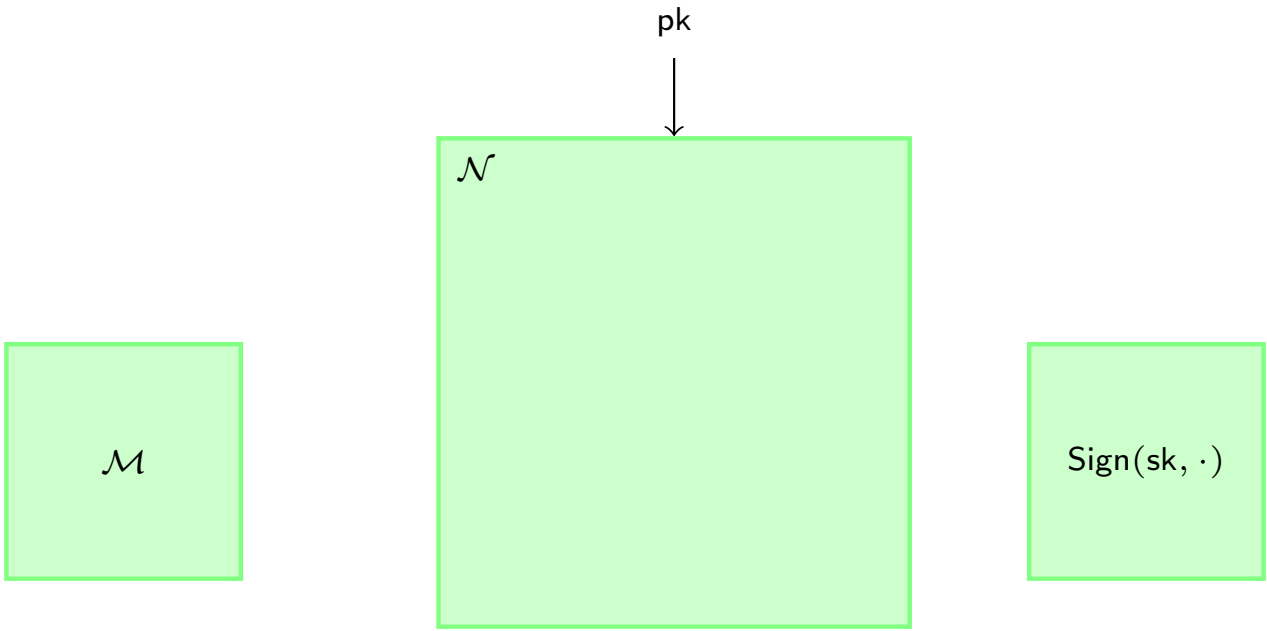
Meta-Meta-Reduction



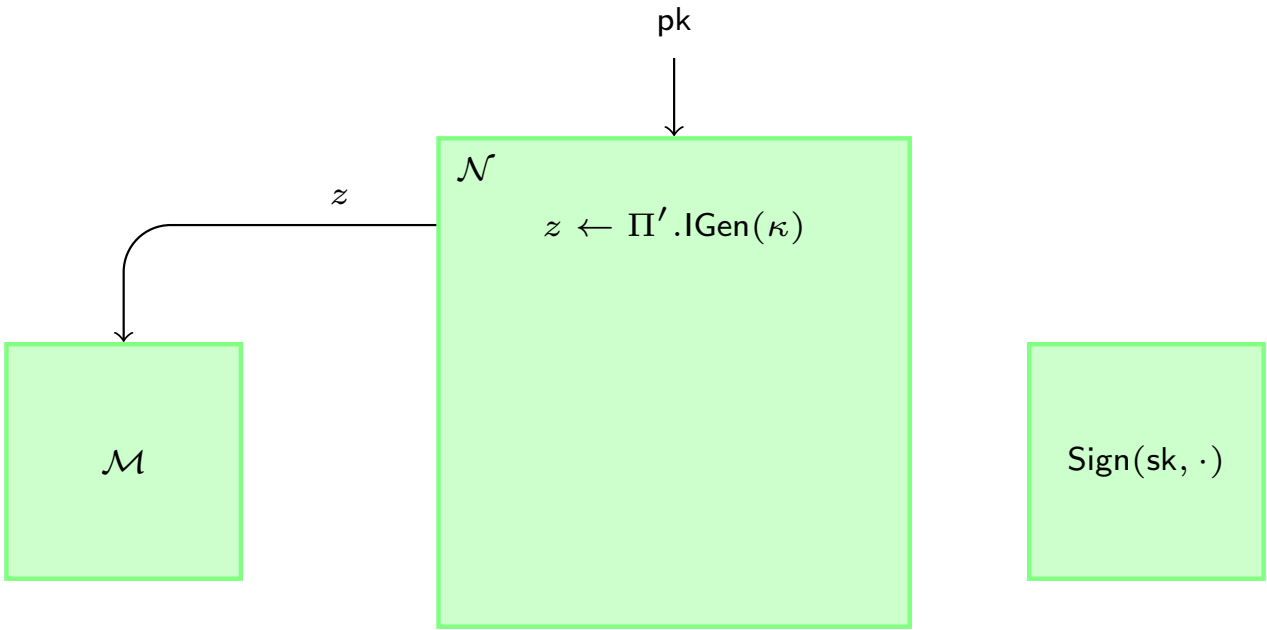
Meta-Meta-Reduction



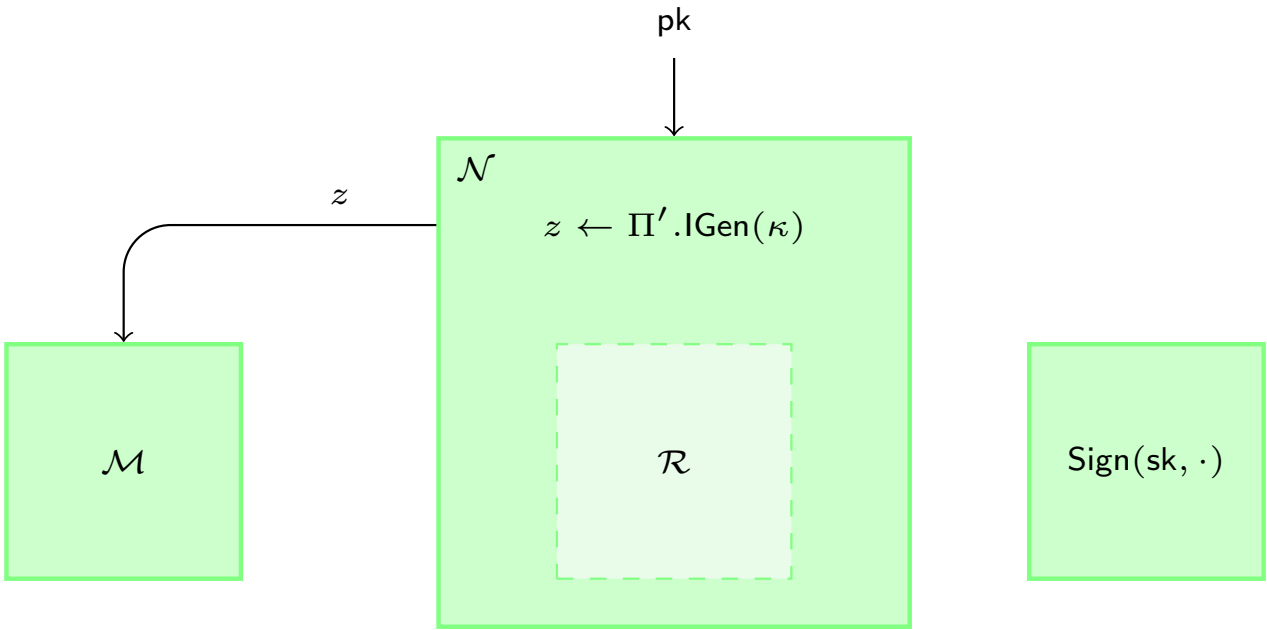
What does it mean?



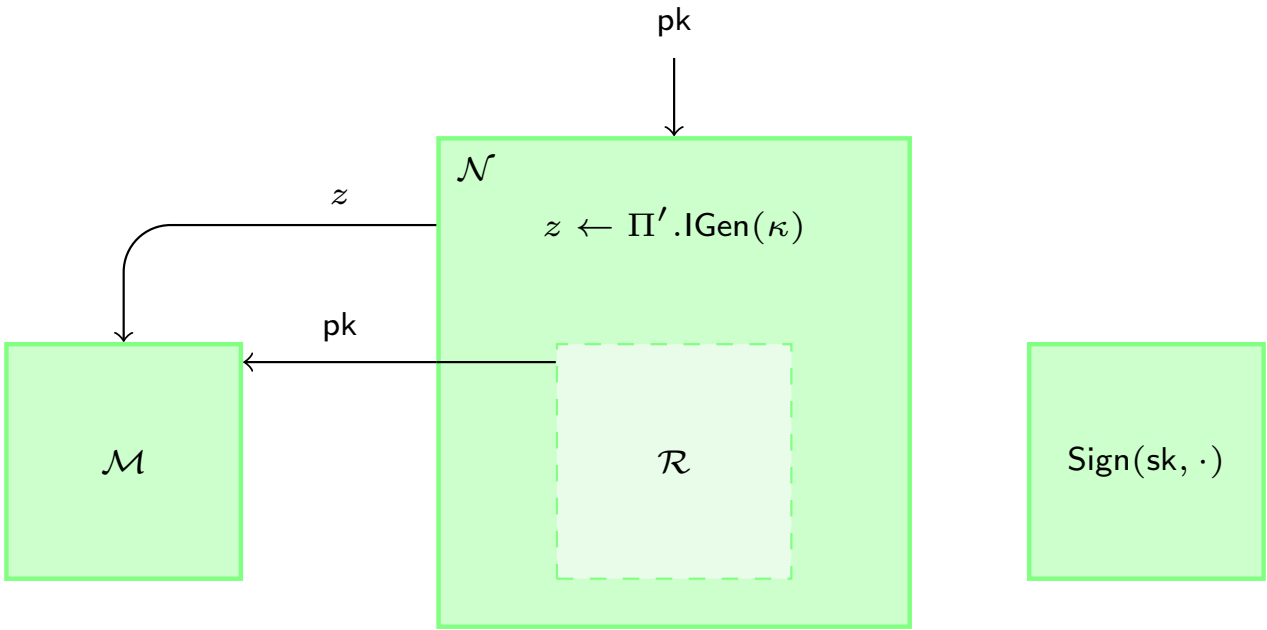
What does it mean?



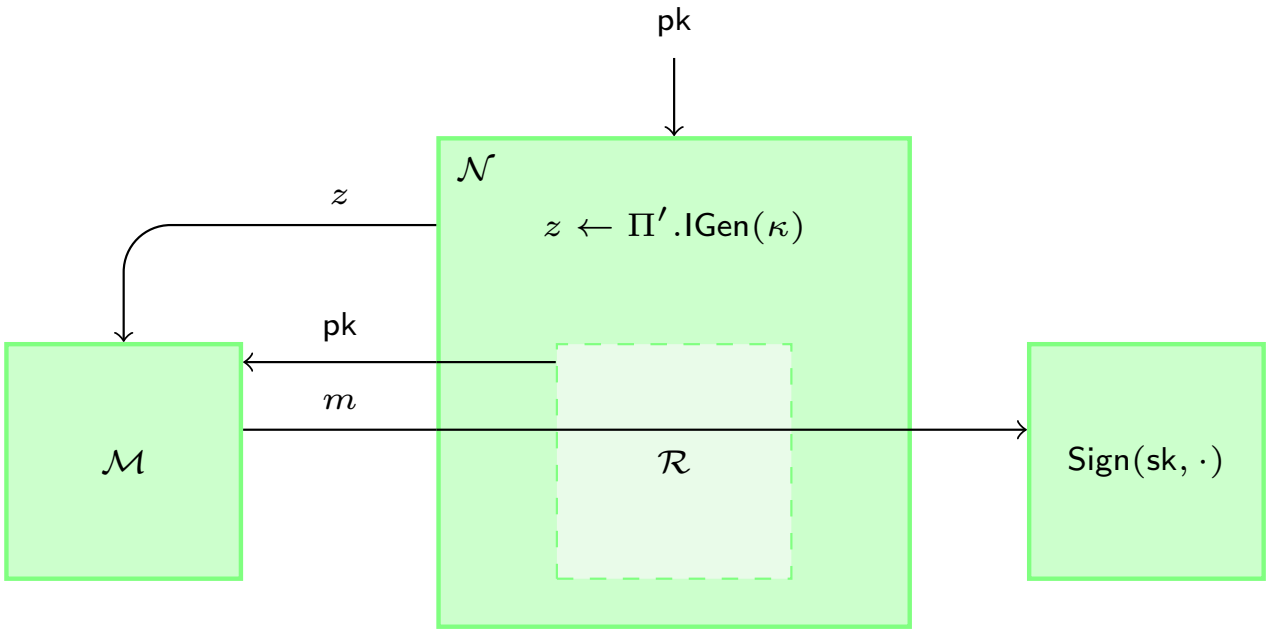
What does it mean?



What does it mean?

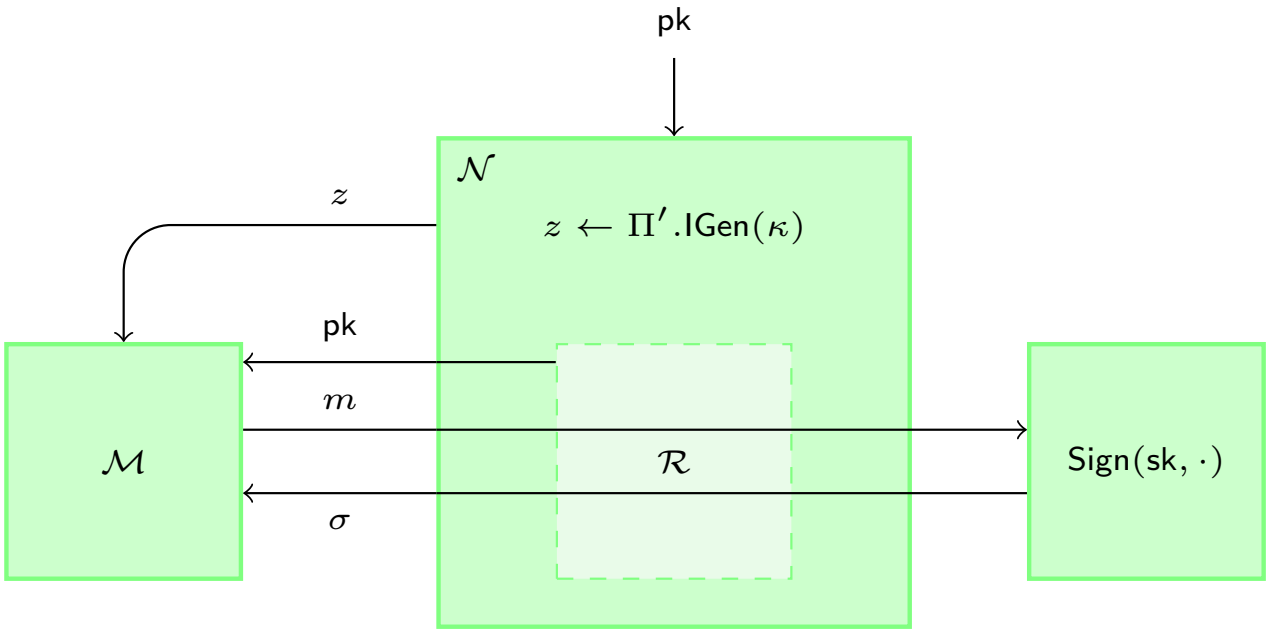


What does it mean?

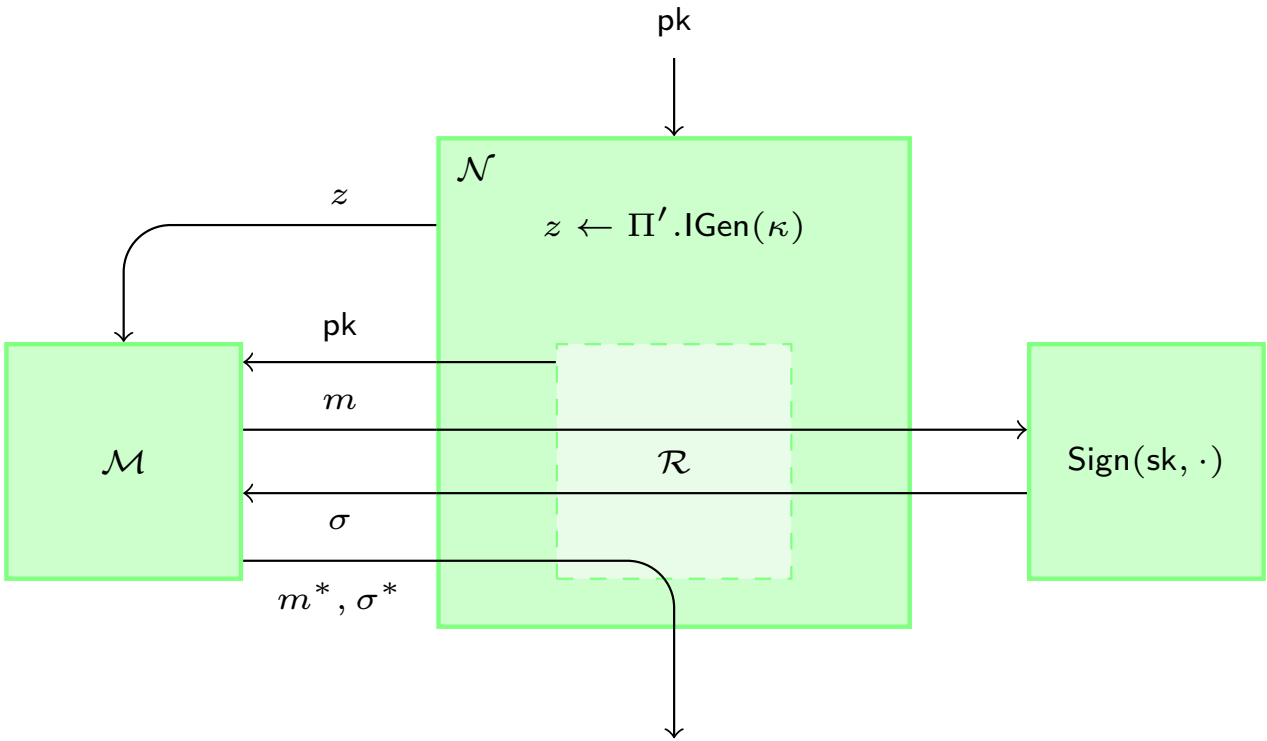


TECHNISCHE UNIVERSITÄT DARMSTADT

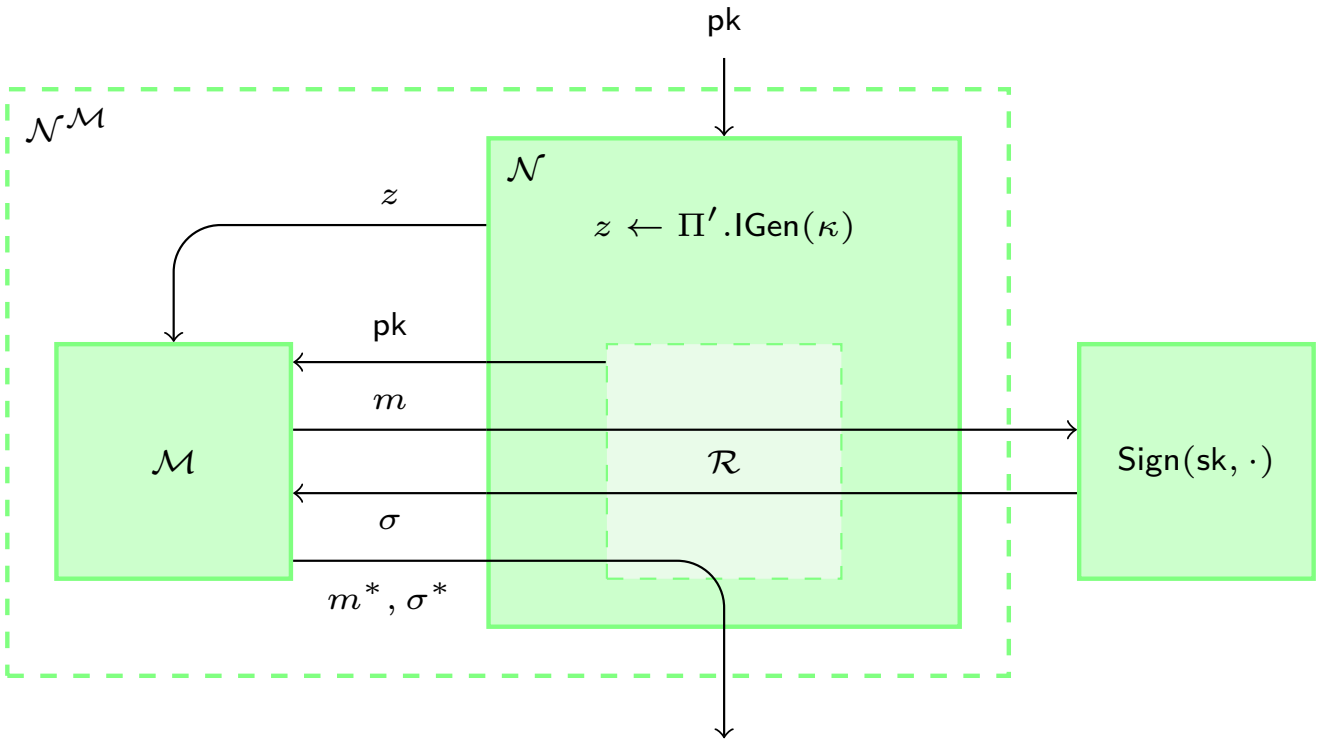
What does it mean?



What does it mean?



What does it mean?



So, what?

This is **no** impossibility result. We are trying to show that EUF-CMA security cannot be proven. Of course an sEUF-CMA adversary might exist.
There is no contradiction whatsoever.

So, what?

However, why are we trying to find a meta-reduction?
Because we are unable find an adversary.

Conclusion

For reasonably randomized signature schemes (without obvious rerandomization) and non-interactive problems the meta-reduction technique is not as useful as one might hope.

TECHNISCHE UNIVERSITÄT DARMSTADT