

How to Eat Your Entropy and  
Have It Too  
(Recovering from compromise)

Yevgeniy Dodis

Adi Shamir

Noah Stephens-Davidowitz

Daniel Wichs

# Our Goal

# Our Goal



figure 1a: Having

# Our Goal



figure 1a: Having



figure 1b: Eating it too

# Our Goal



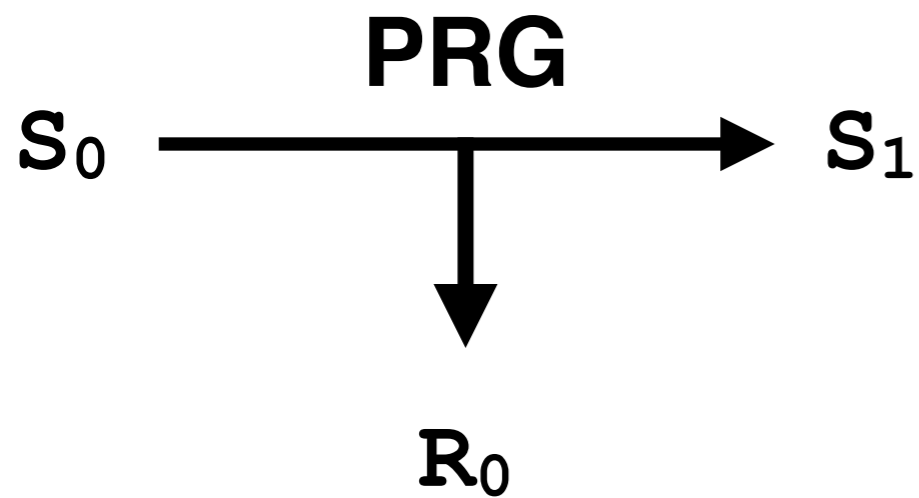
figure 1a: Having



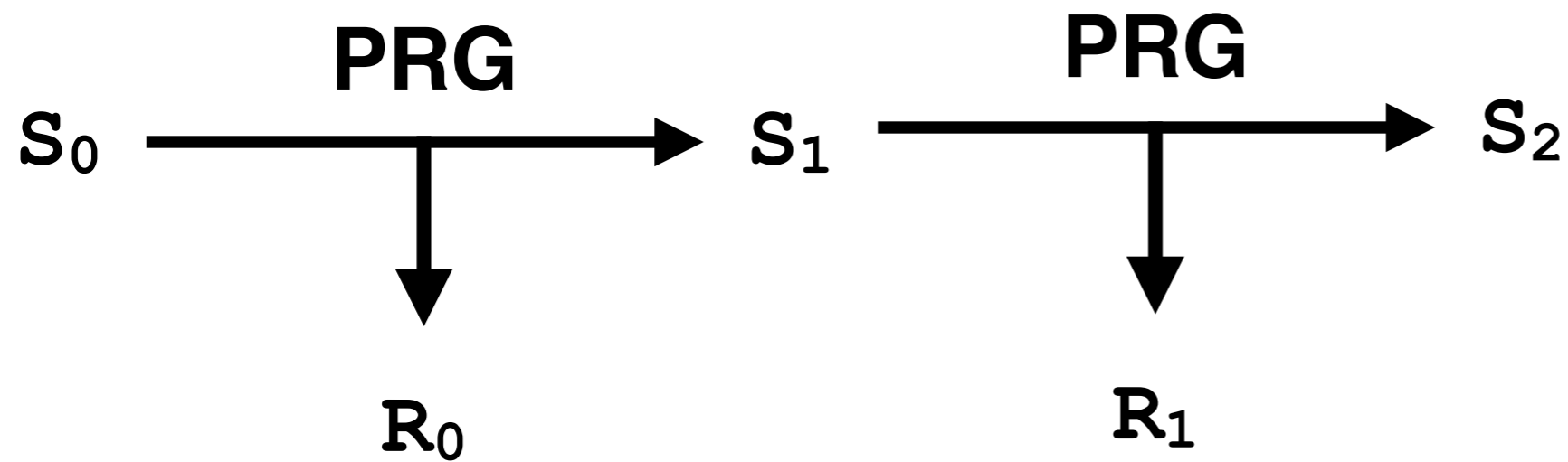
figure 1b: Eating it too

# How Does TCC Build a PRG?

# How Does TCC Build a PRG?

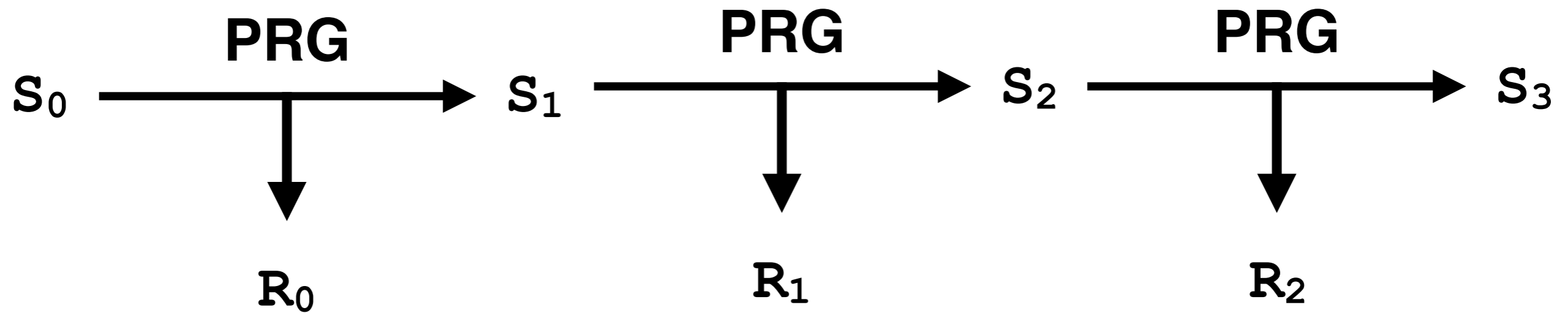


# How Does TCC Build a PRG?

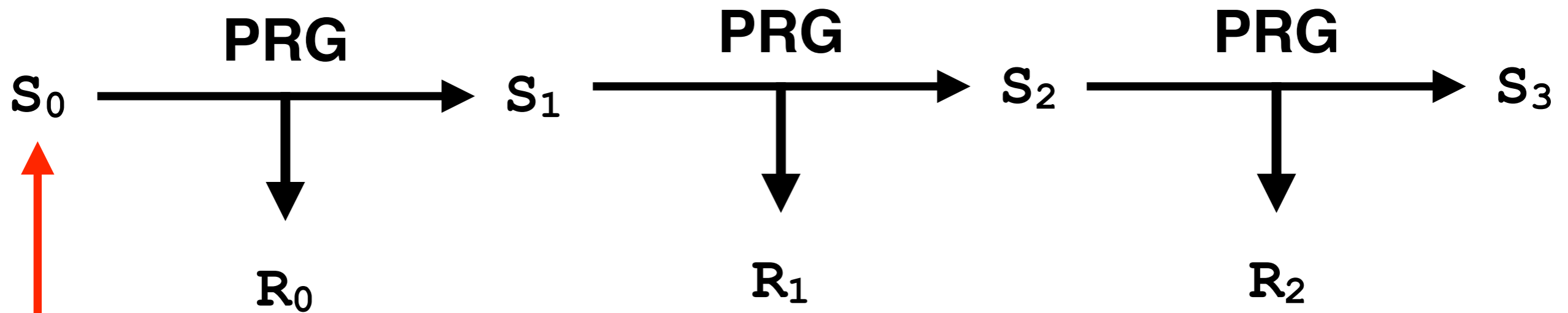




# How Does TCC Build a PRG?



# How Does TCC Build a PRG?



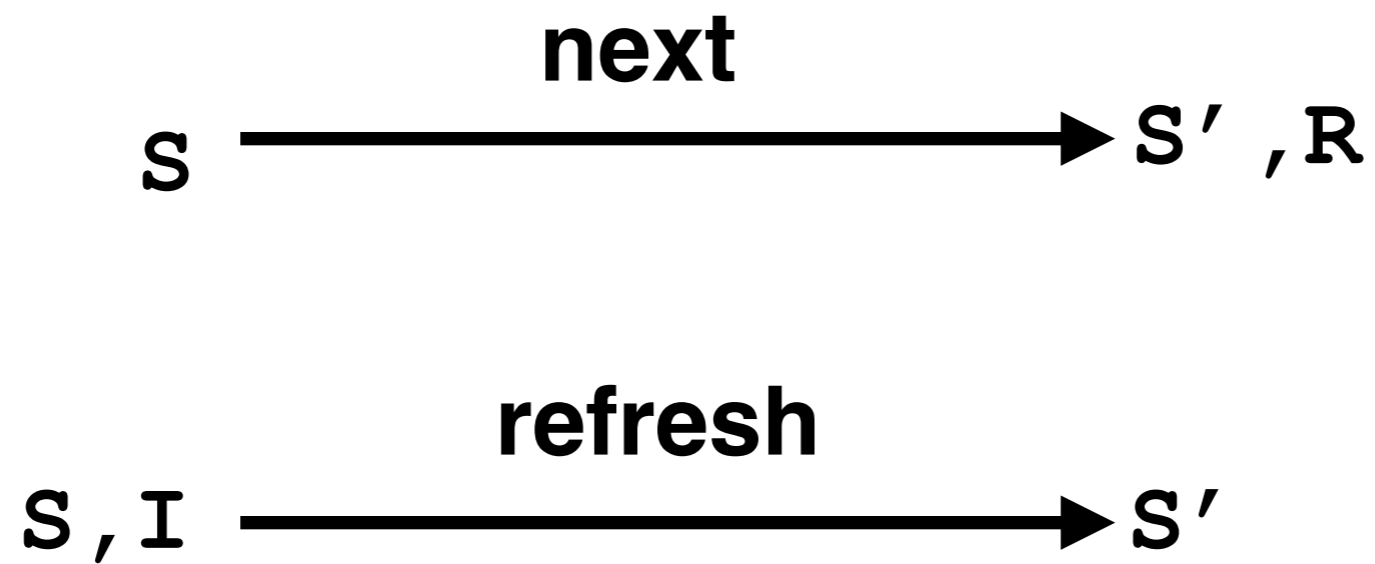
Perfect randomness...

Developers Build  
“RNGs with Input”

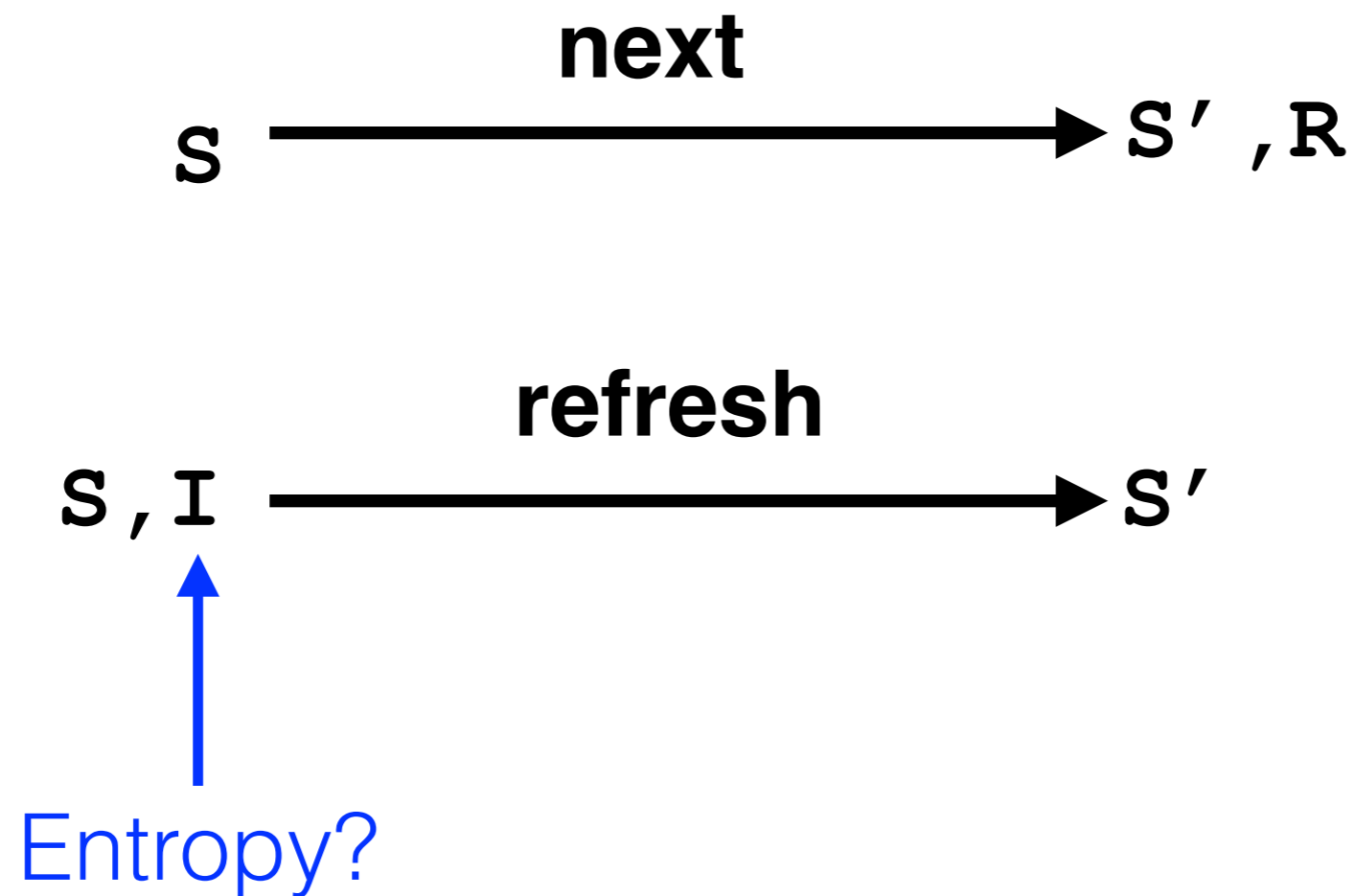
# Developers Build “RNGs with Input”



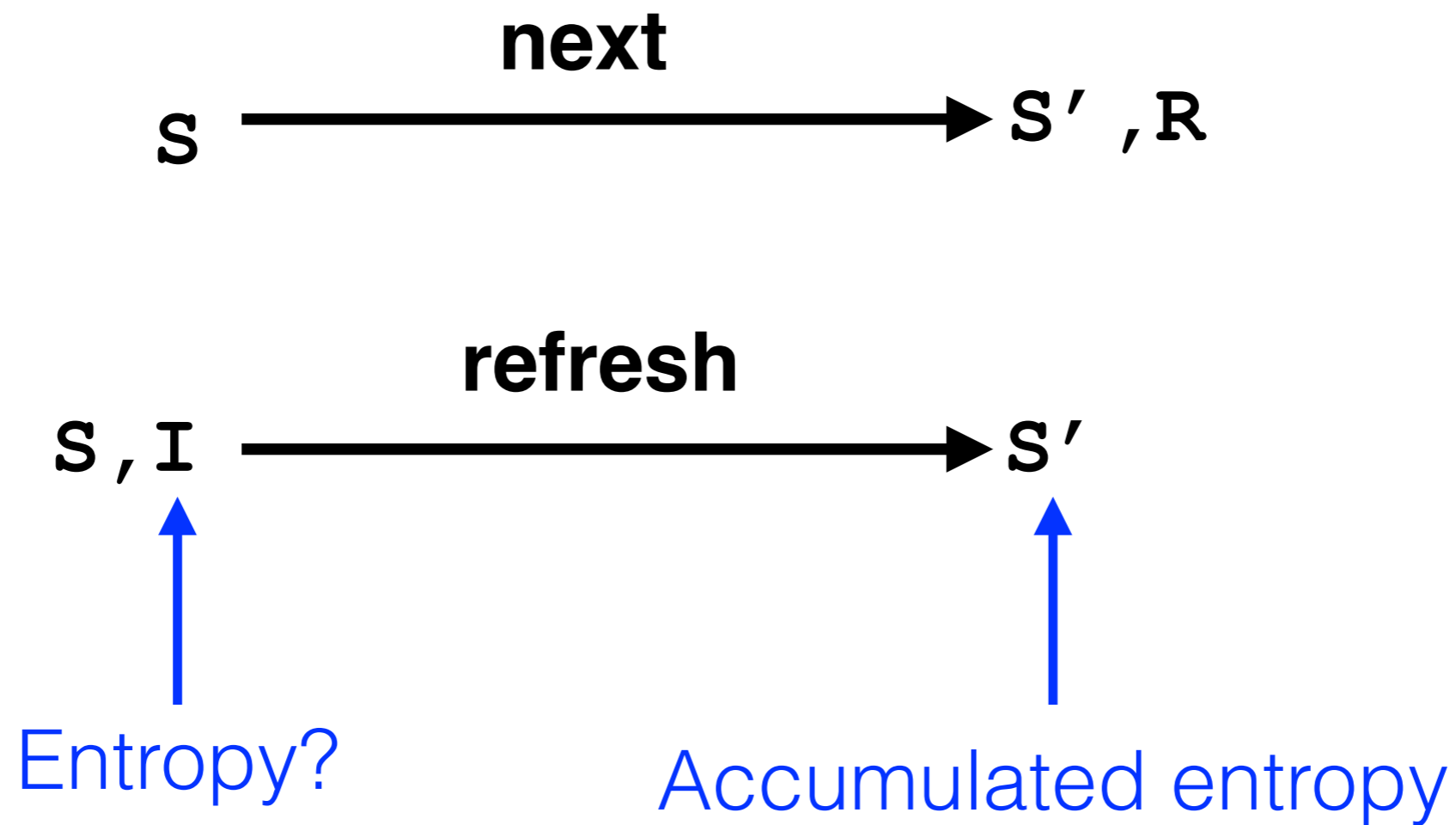
# Developers Build “RNGs with Input”



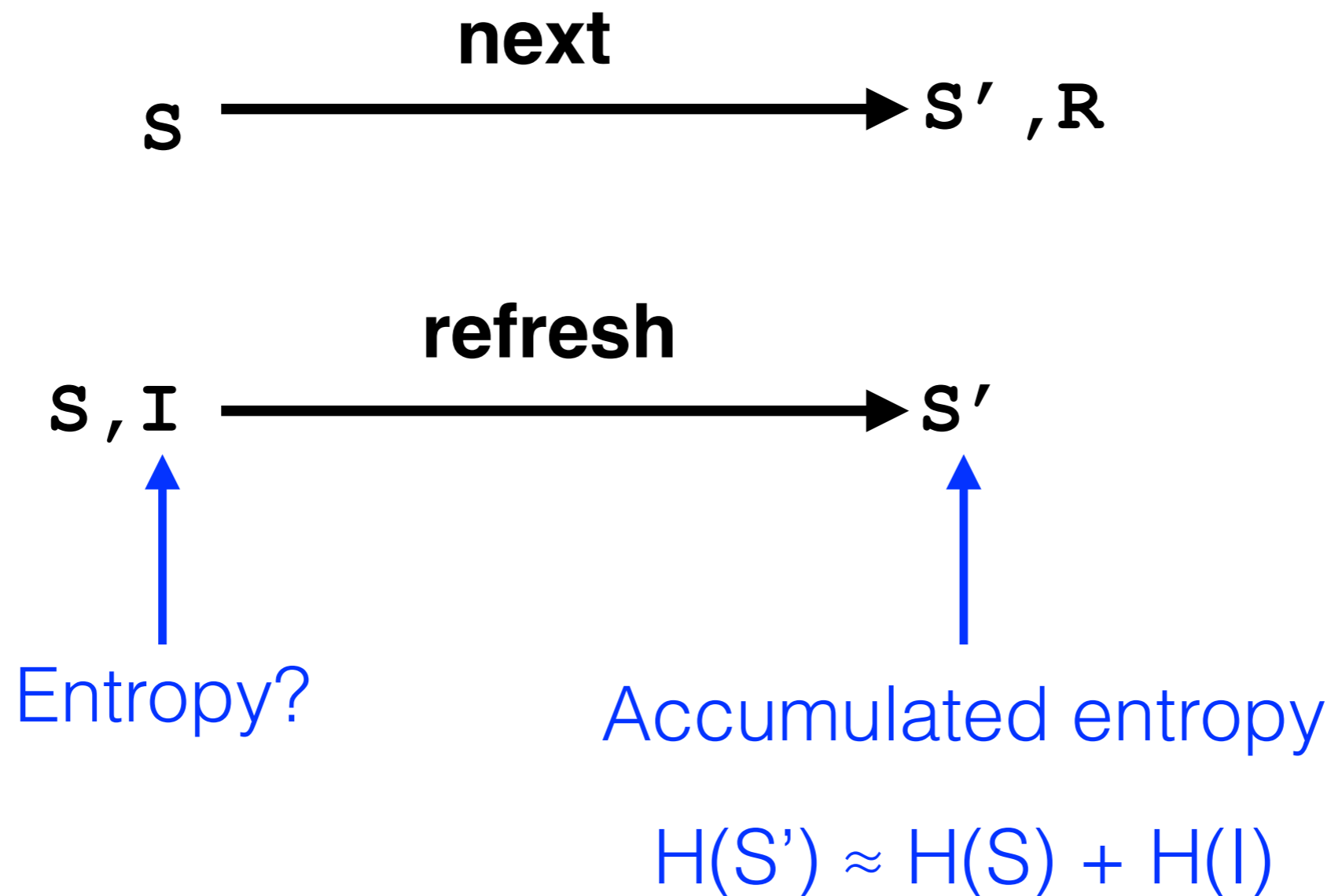
# Developers Build “RNGs with Input”



# Developers Build “RNGs with Input”



# Developers Build “RNGs with Input”





# (Limited) Formal Analysis

[BH05]

[DPRVW13]

# (Limited) Formal Analysis

[BH05]

[DPRVW13]



First formal model  
(In 2005!)

# (Limited) Formal Analysis

[BH05]

[DPRVW13]



First formal model  
(In 2005!)

Recover only after  
**full-entropy** input

# (Limited) Formal Analysis

[BH05]



First formal model  
(In 2005!)

Recover only after  
**full-entropy** input

[DPRVW13]



Gathers entropy  
as it comes

# (Limited) Formal Analysis

[BH05]



First formal model  
(In 2005!)

Recover only after  
**full-entropy** input

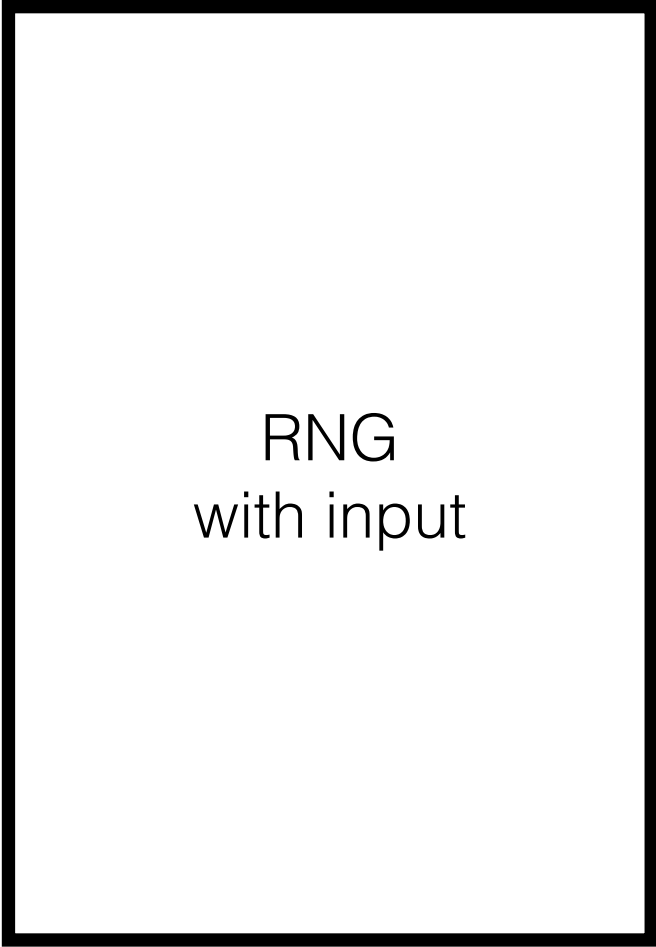
[DPRVW13]



Gathers entropy  
as it comes

But....

# Premature Next



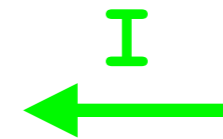
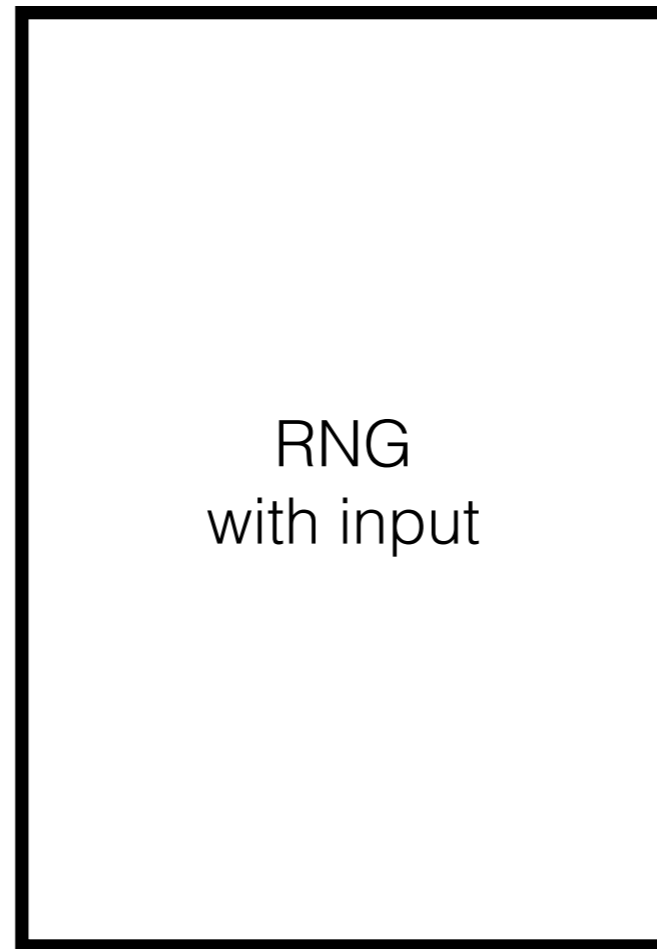
RNG  
with input

# Premature Next

RNG  
with input

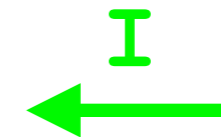
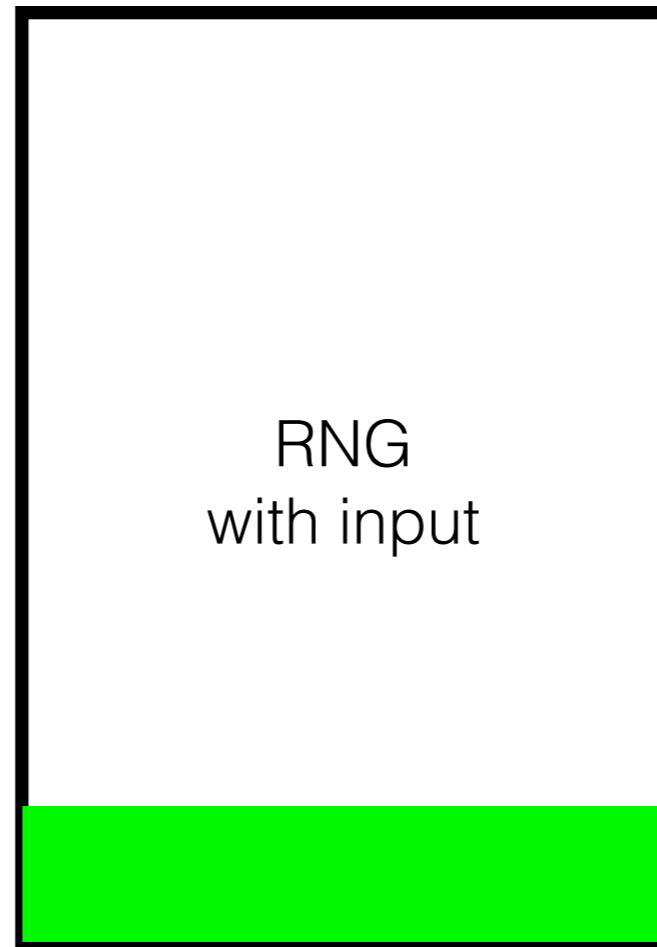


# Premature Next

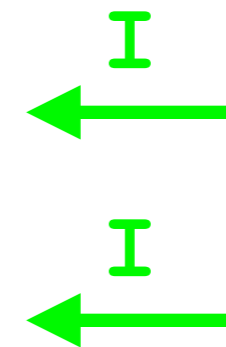
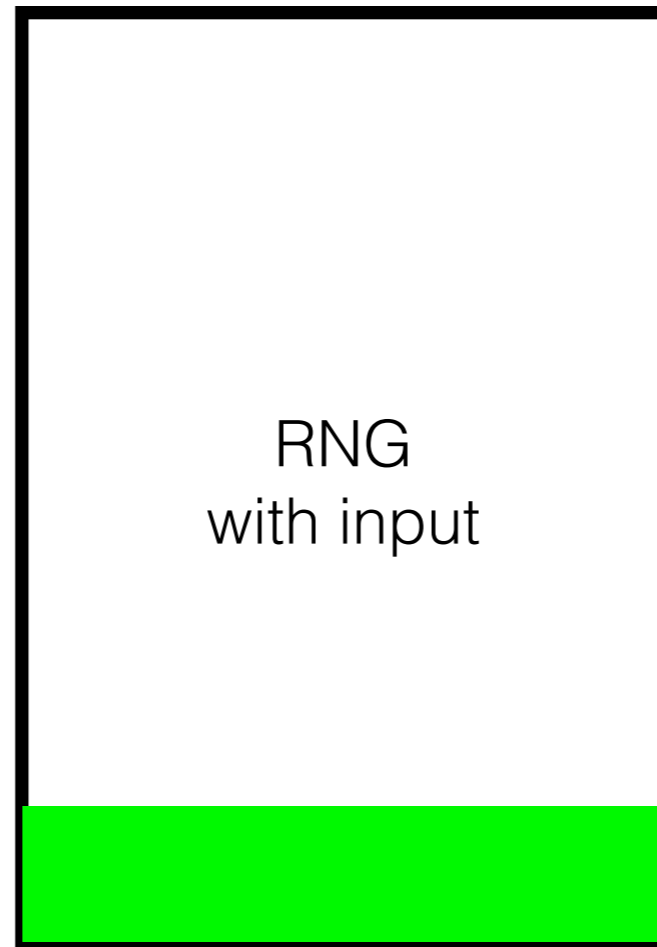




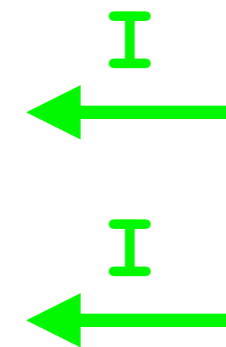
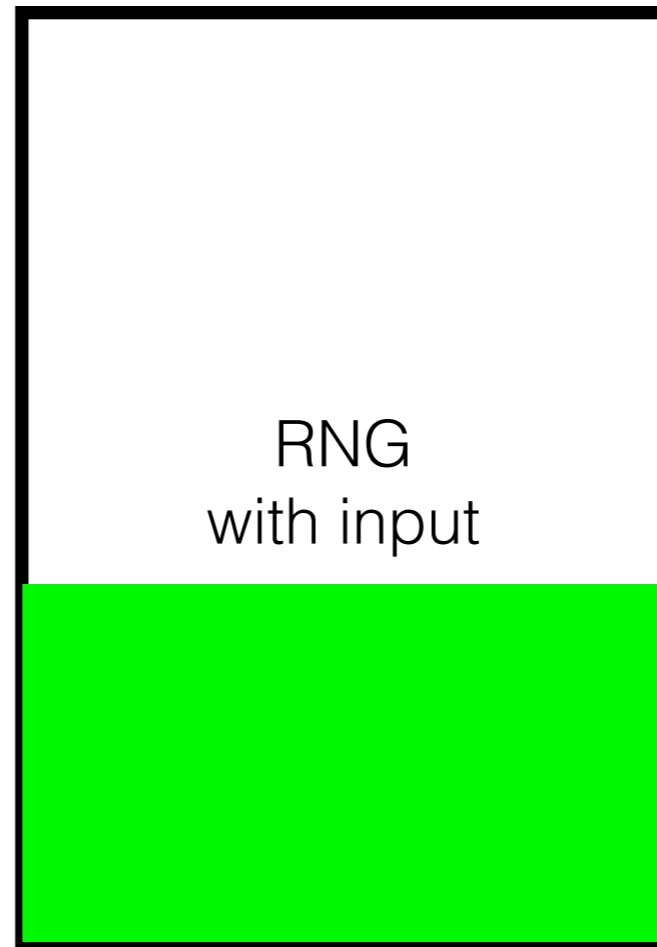
# Premature Next



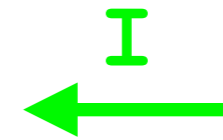
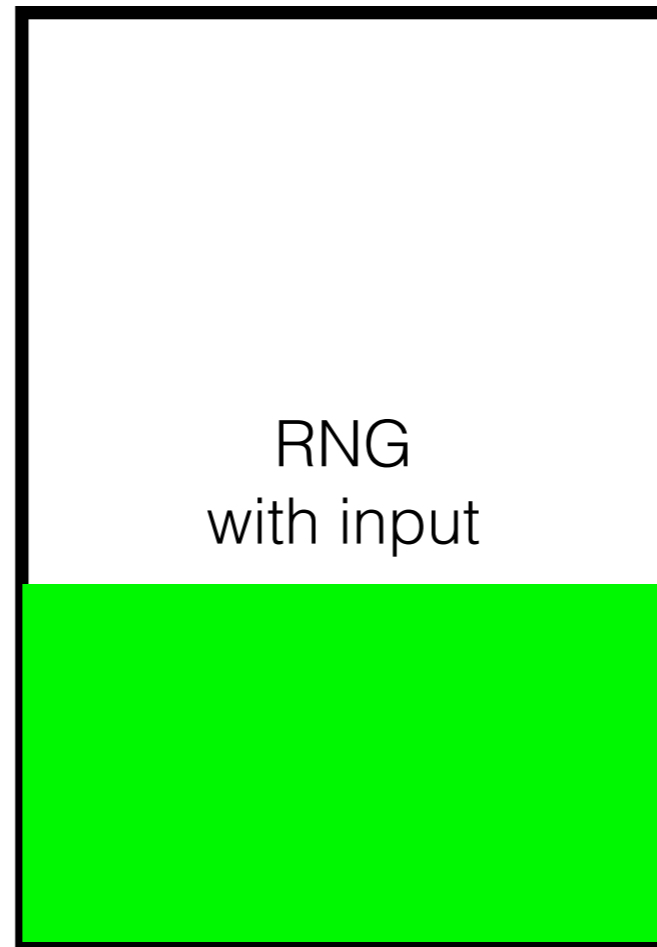
# Premature Next



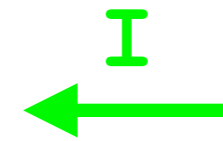
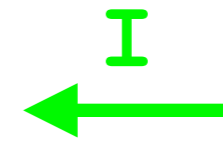
# Premature Next



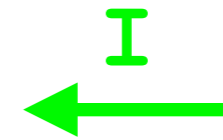
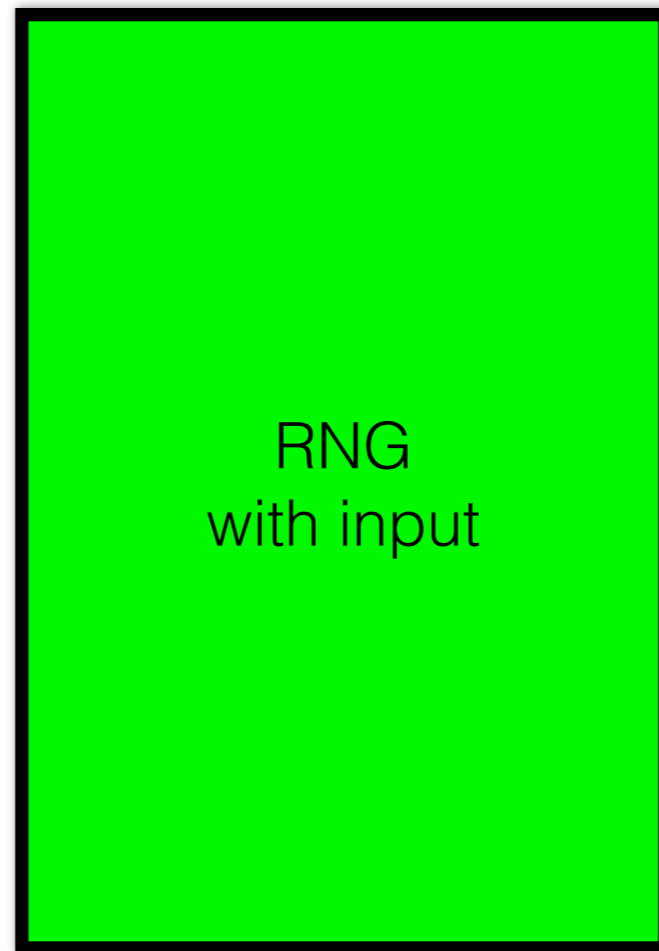
# Premature Next



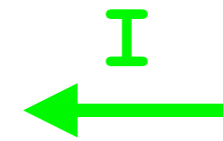
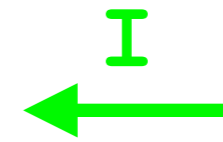
...



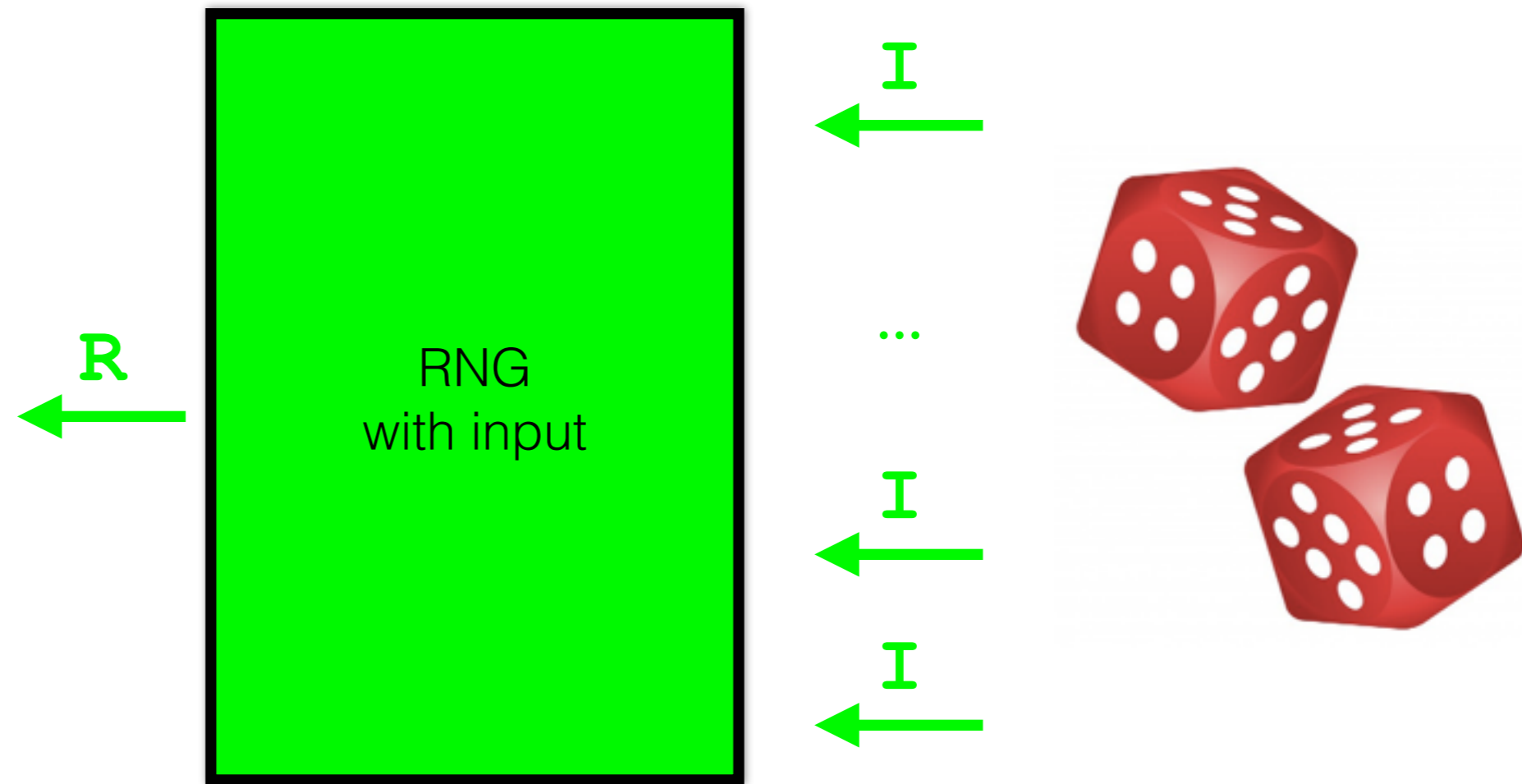
# Premature Next



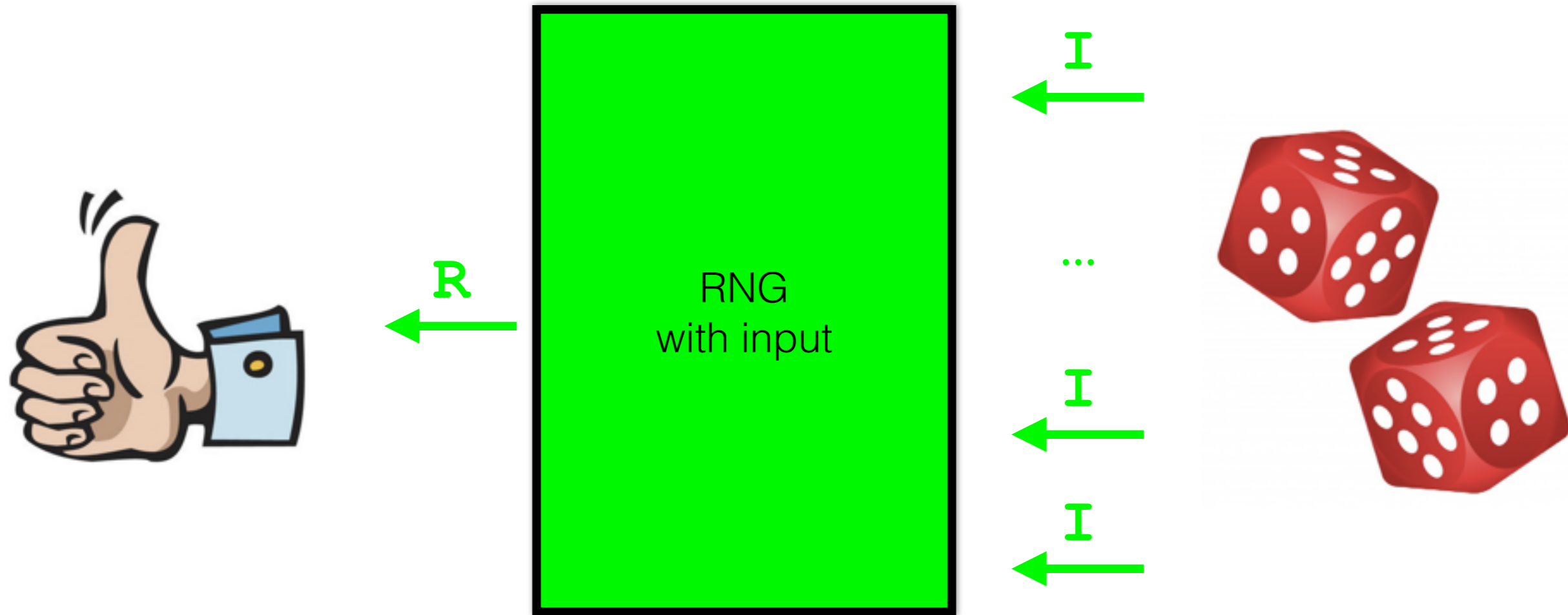
...



# Premature Next



# Premature Next



# Premature Next

RNG  
with input





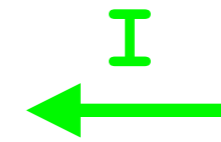
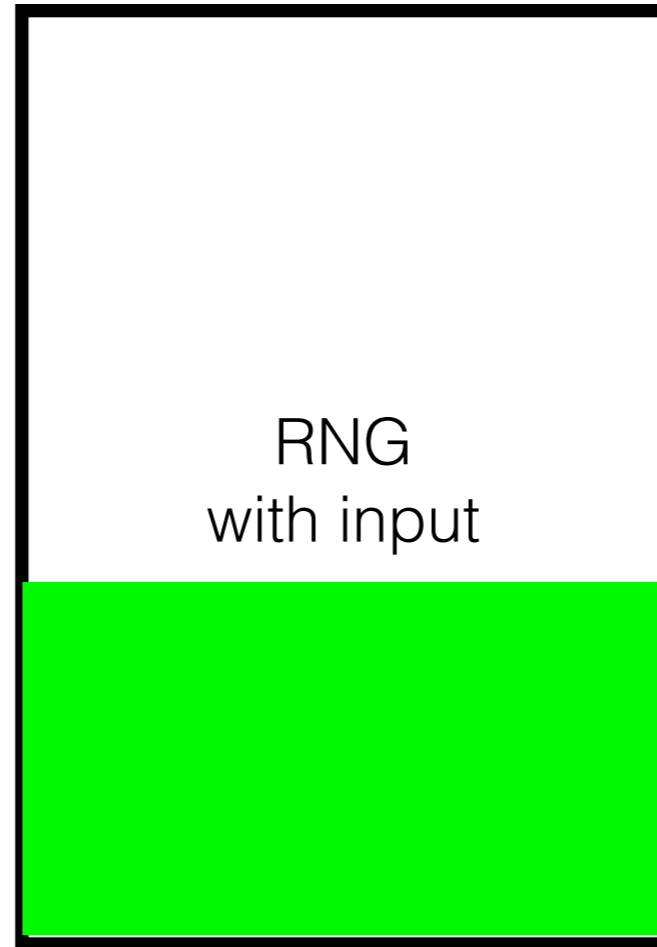
# Premature Next



RNG  
with input



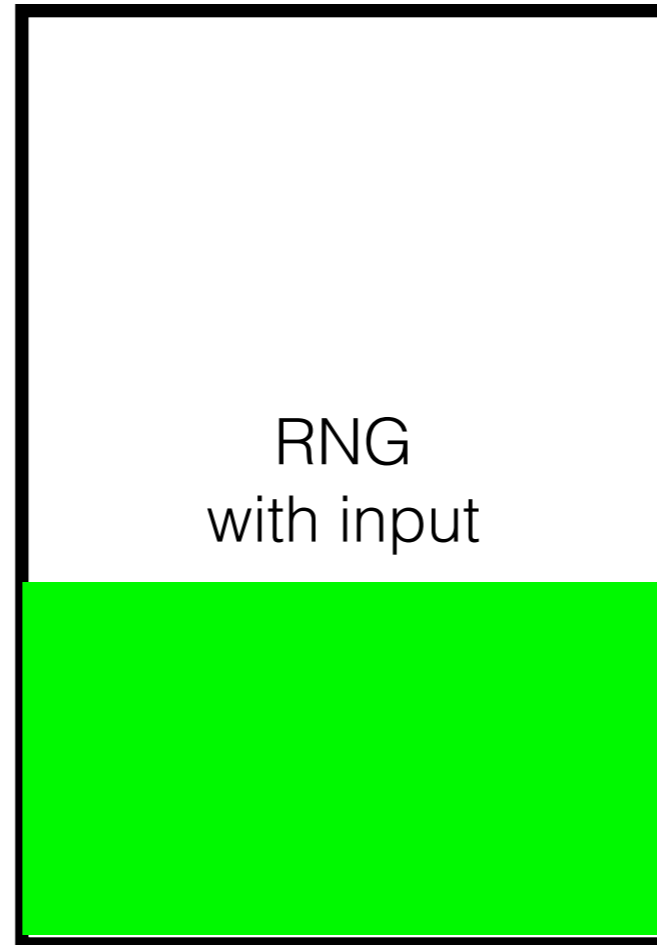
# Premature Next



# Premature Next



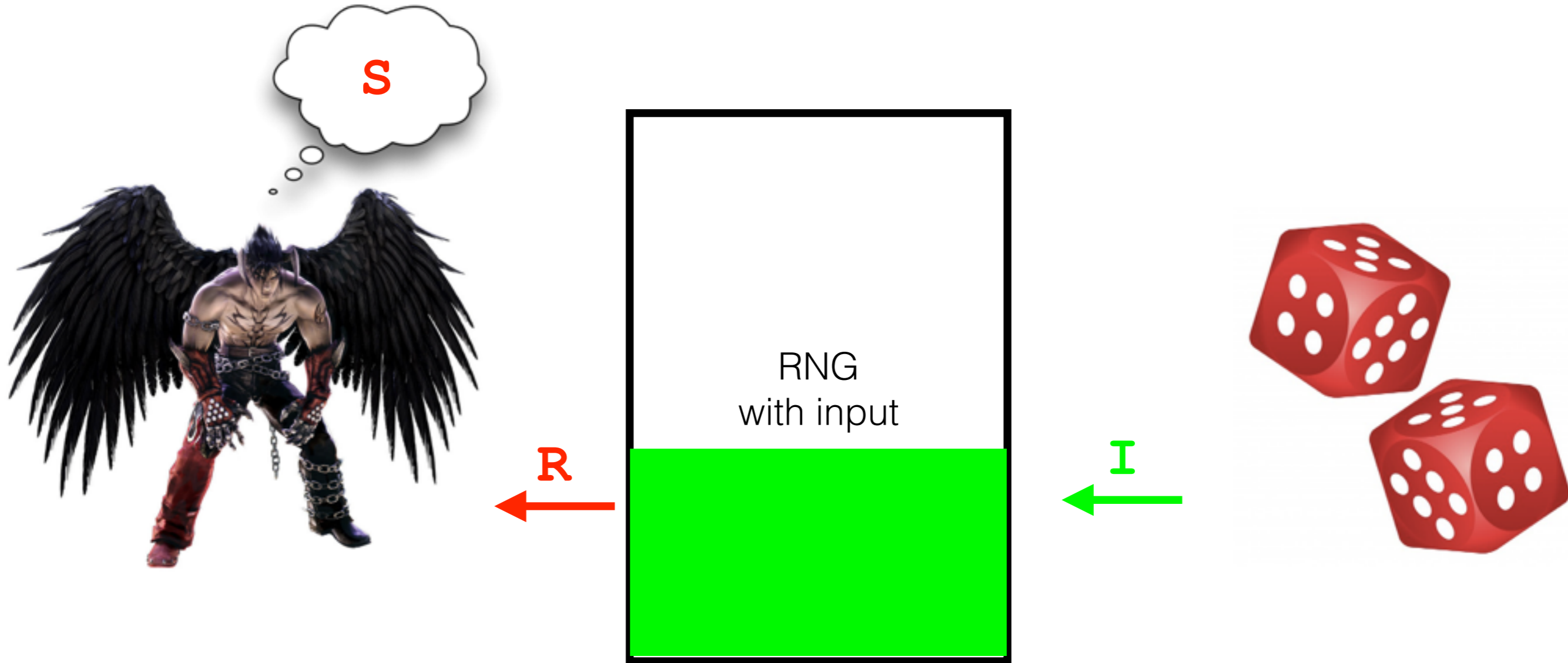
R



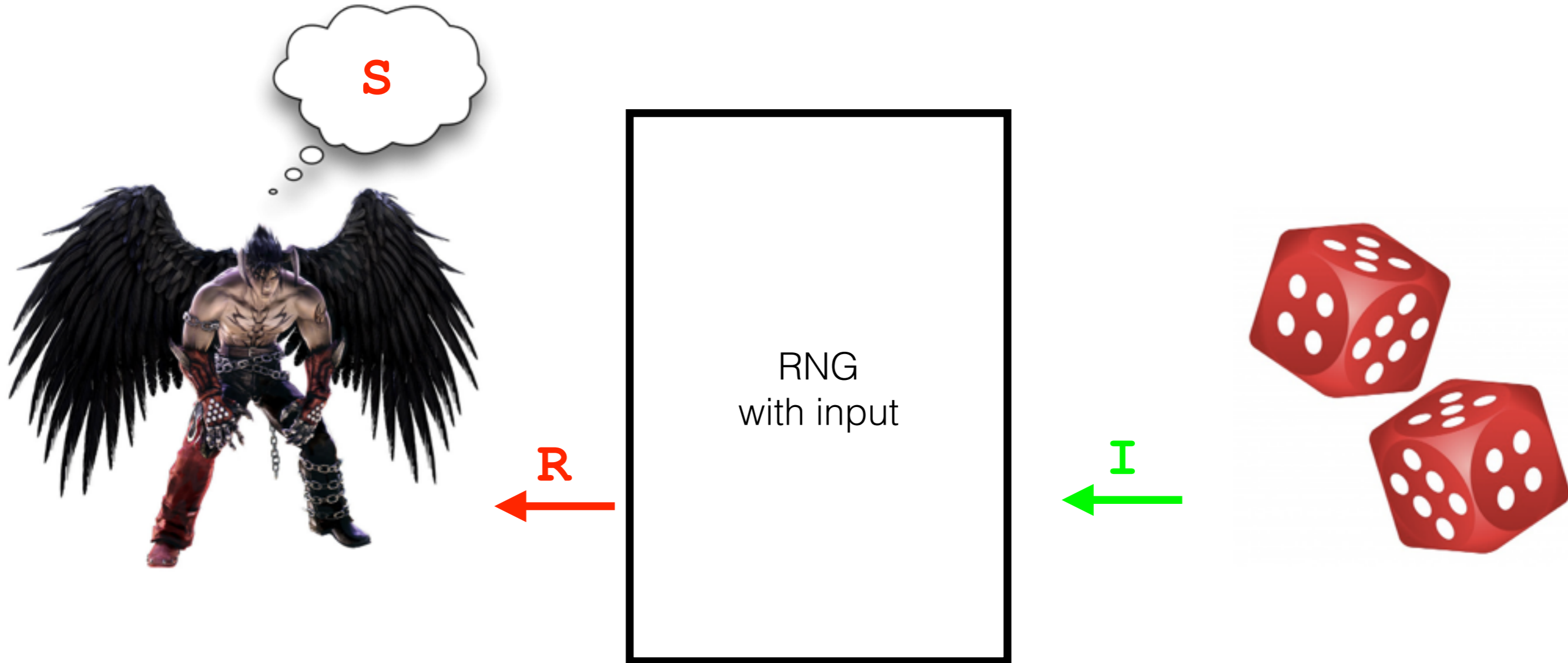
I



# Premature Next



# Premature Next



How do we deal  
with this?

# Option 1: Don't Let The Adversary Look



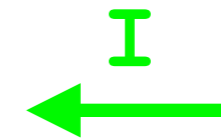
RNG  
with input



# Option 1: Don't Let The Adversary Look

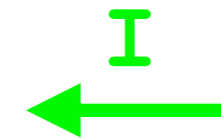
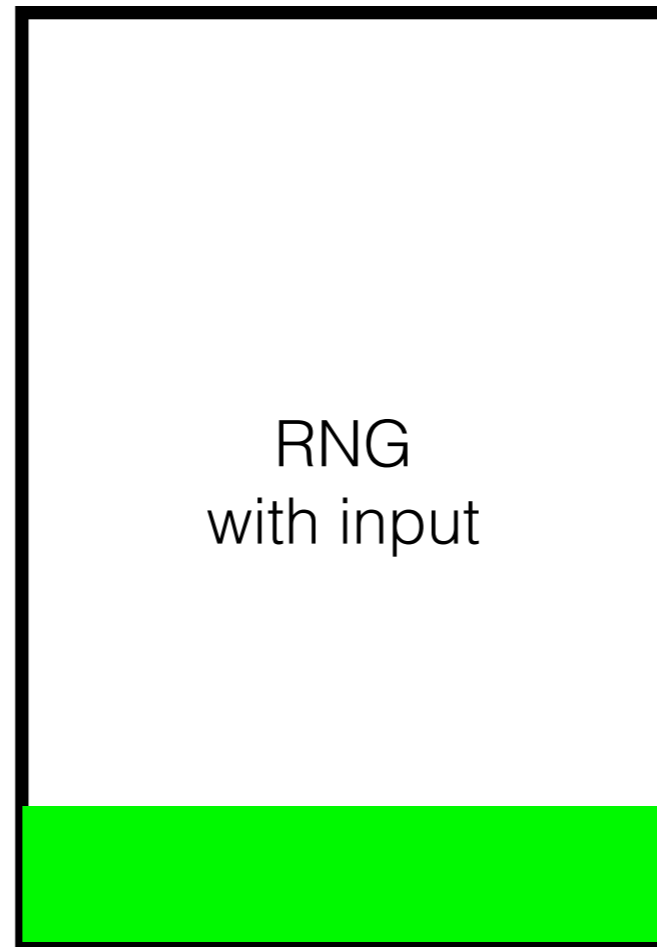


RNG  
with input

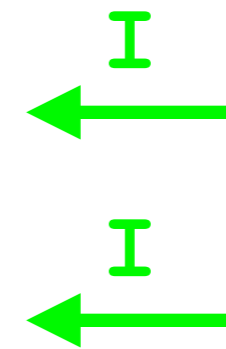
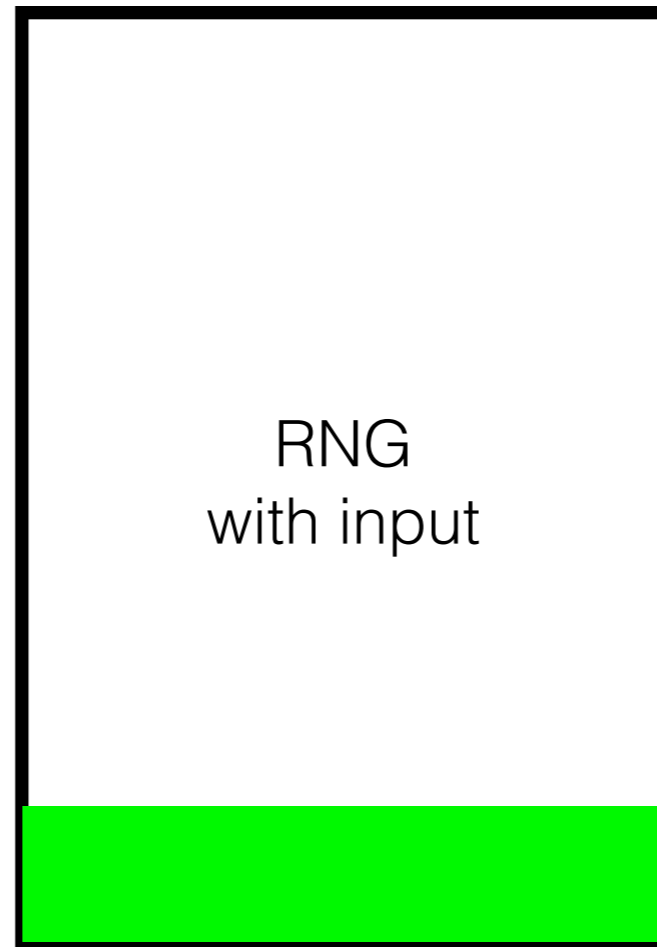




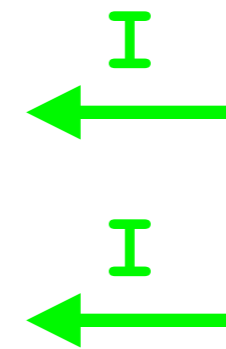
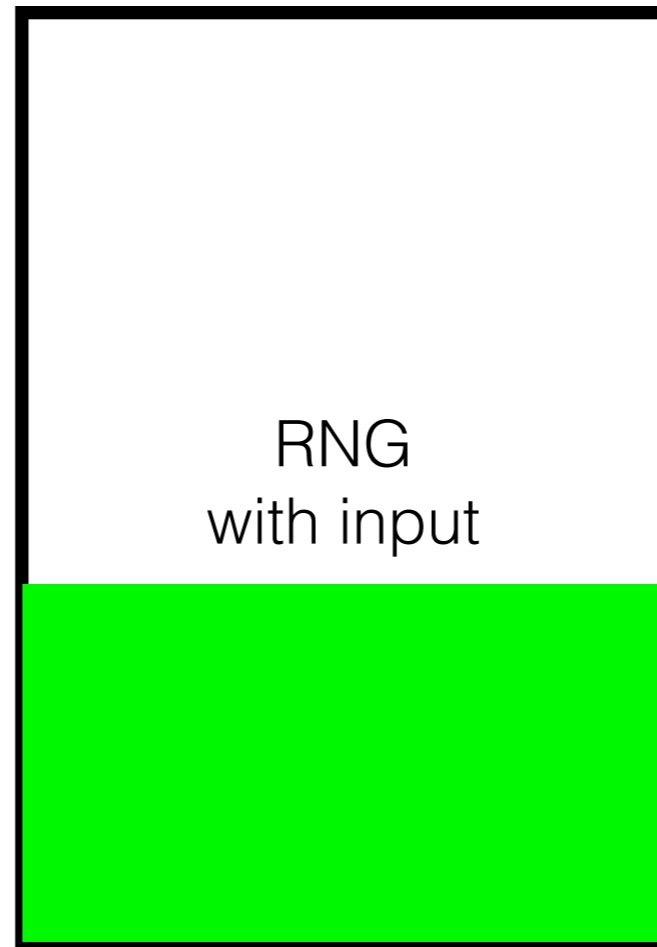
# Option 1: Don't Let The Adversary Look



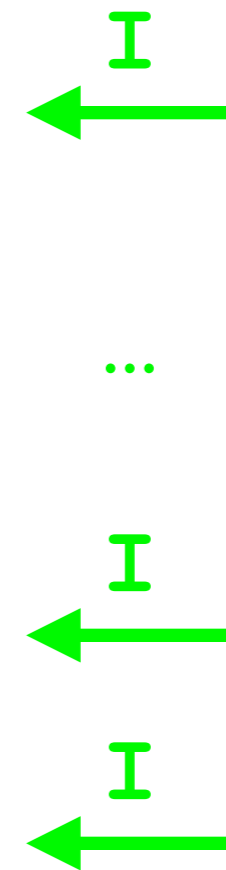
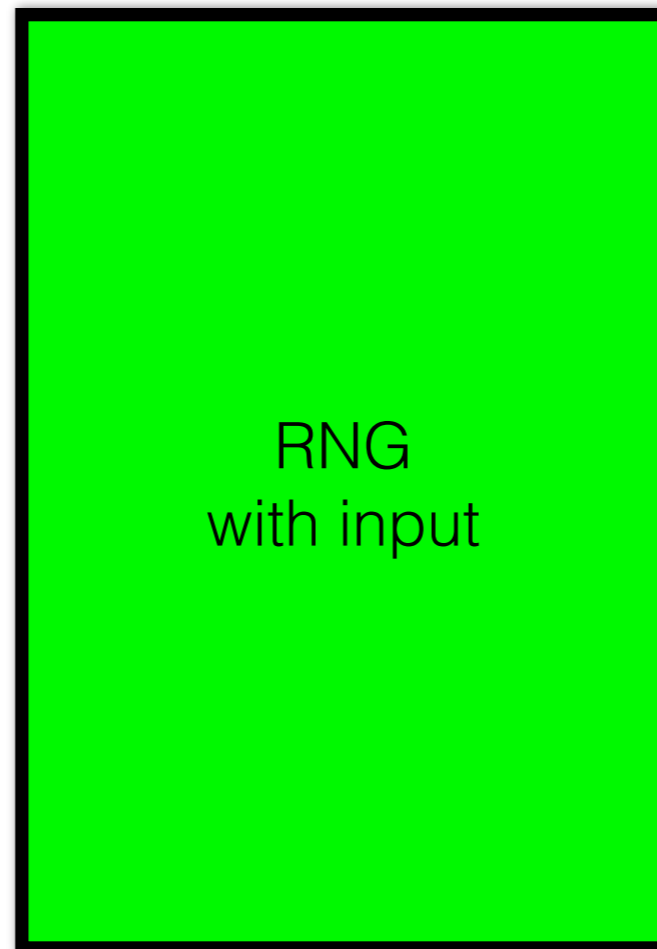
# Option 1: Don't Let The Adversary Look



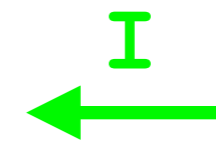
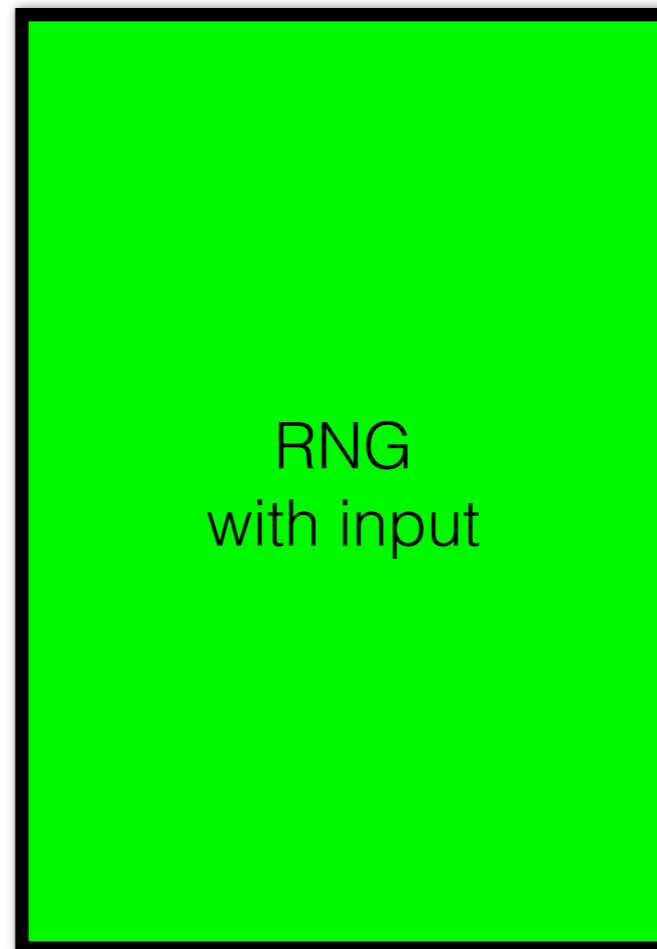
# Option 1: Don't Let The Adversary Look



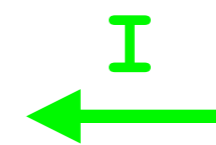
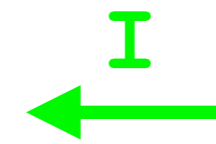
# Option 1: Don't Let The Adversary Look



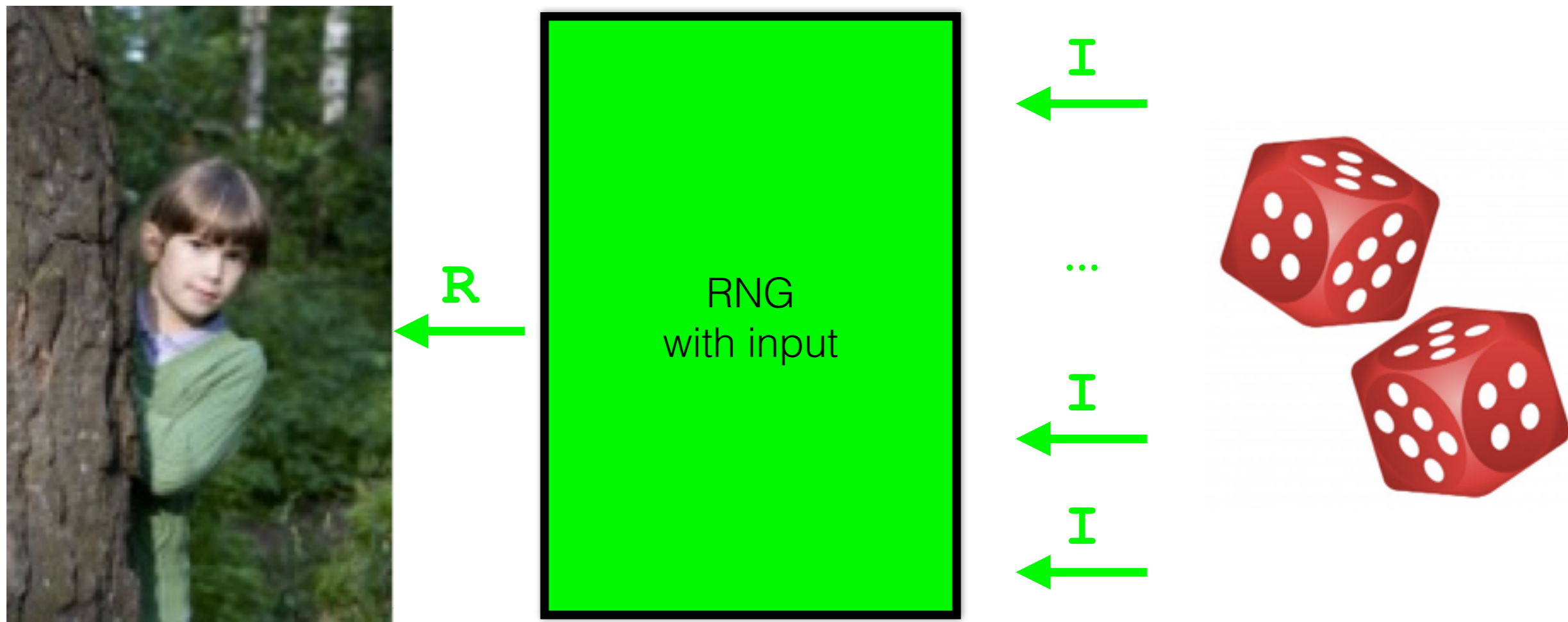
# Option 1: Don't Let The Adversary Look



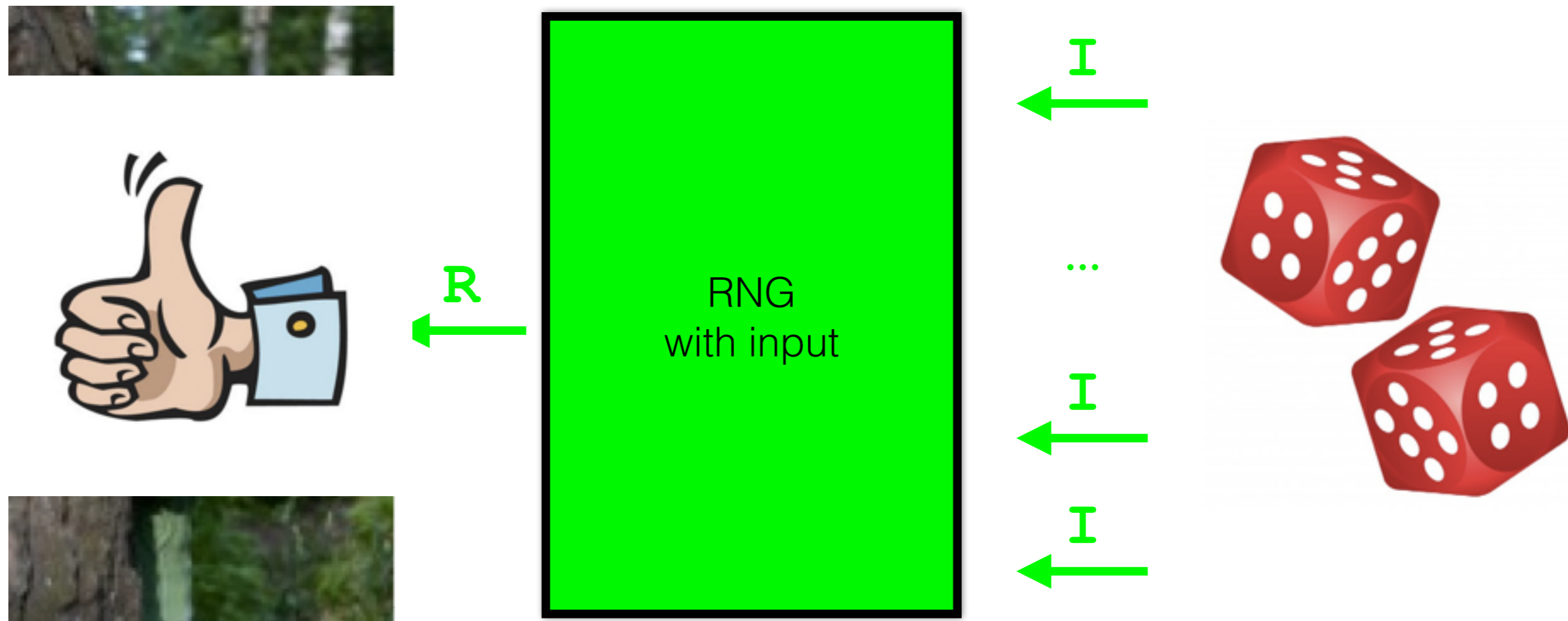
...



# Option 1: Don't Let The Adversary Look



# Option 1: Don't Let The Adversary Look



# Option 2: Estimate Entropy



RNG  
with input



# Option 2: Estimate Entropy



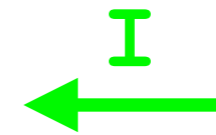
RNG  
with input



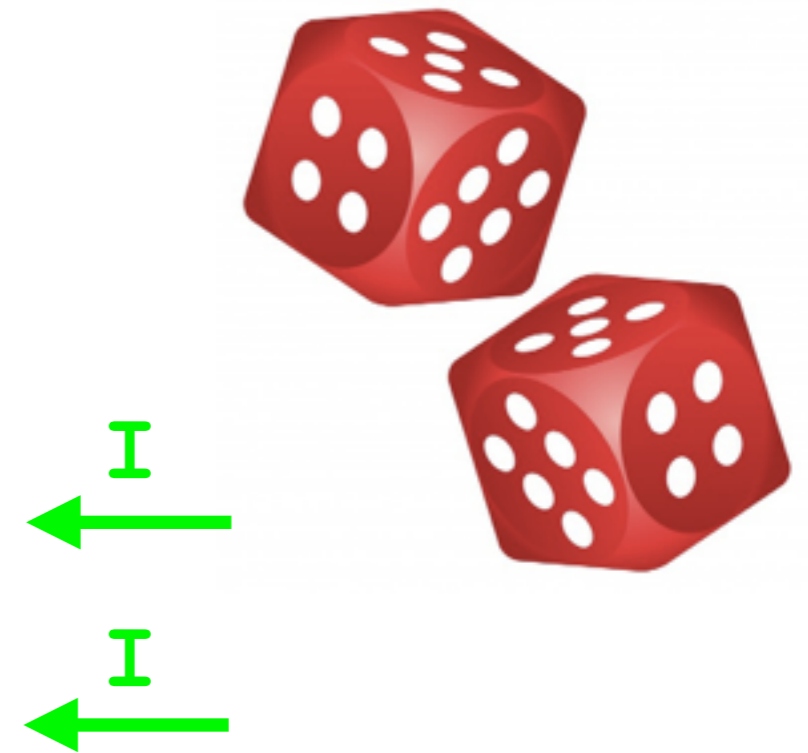
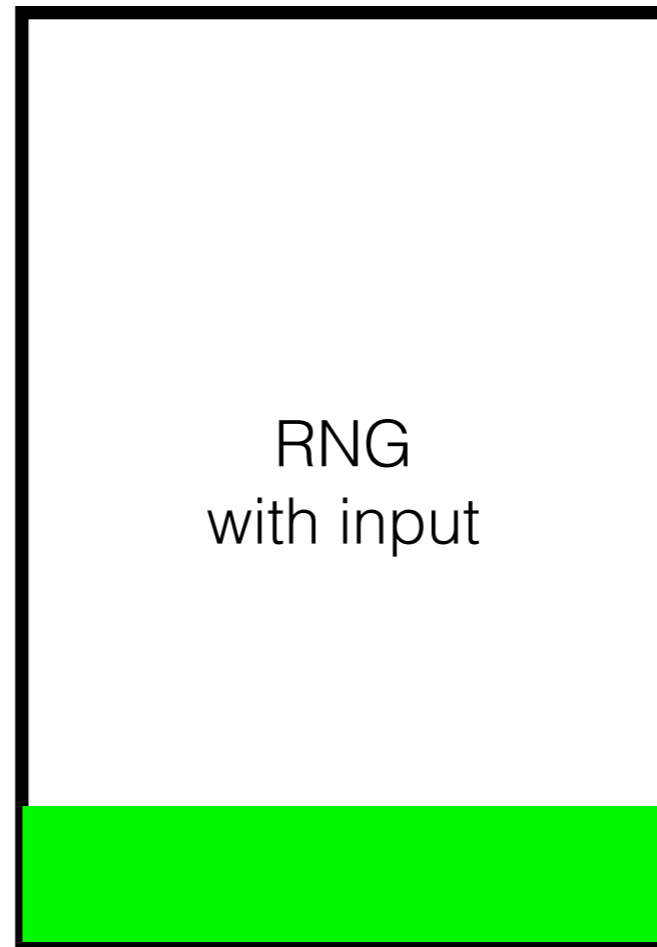
# Option 2: Estimate Entropy



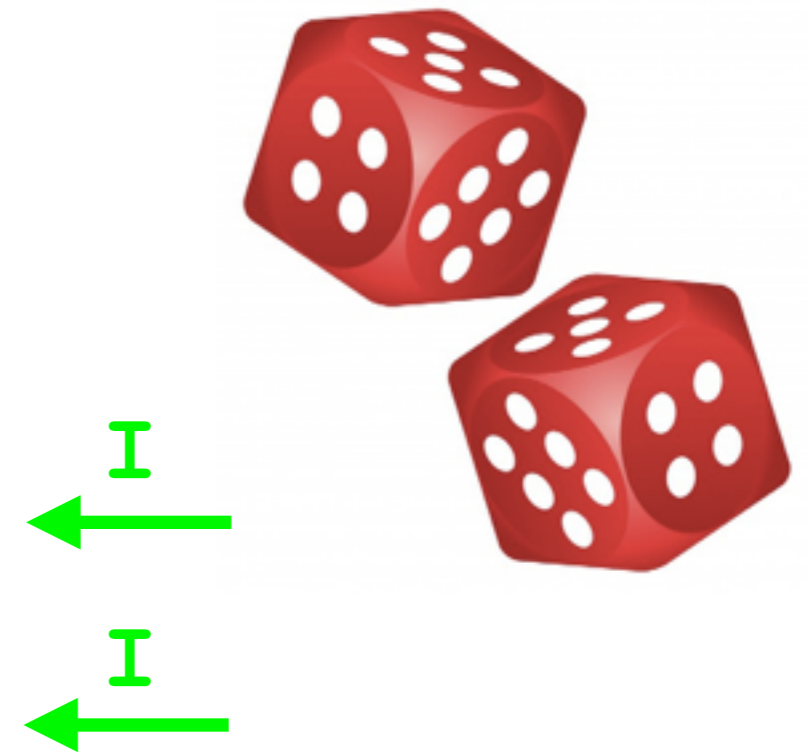
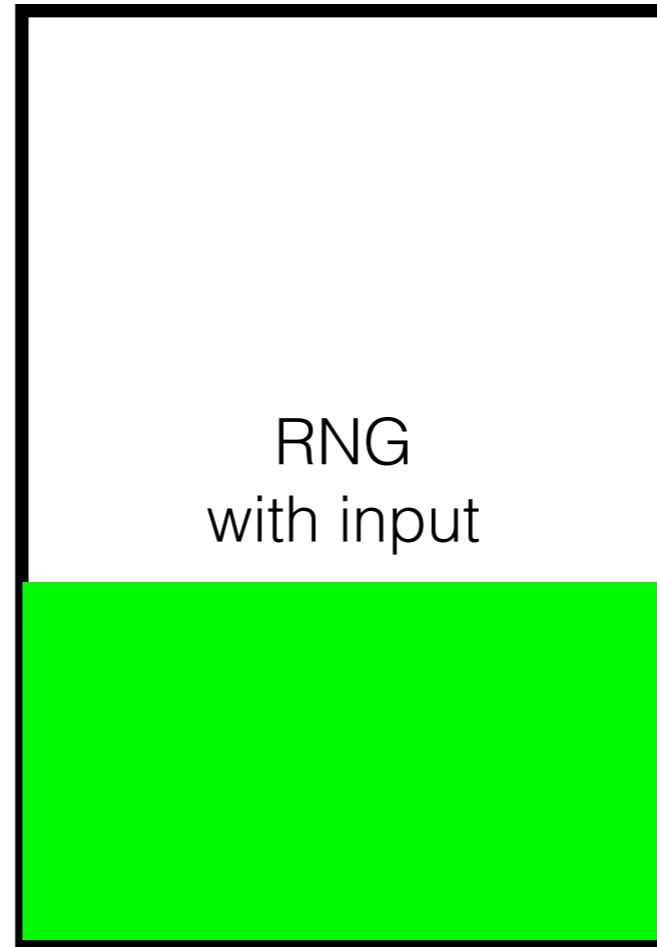
RNG  
with input



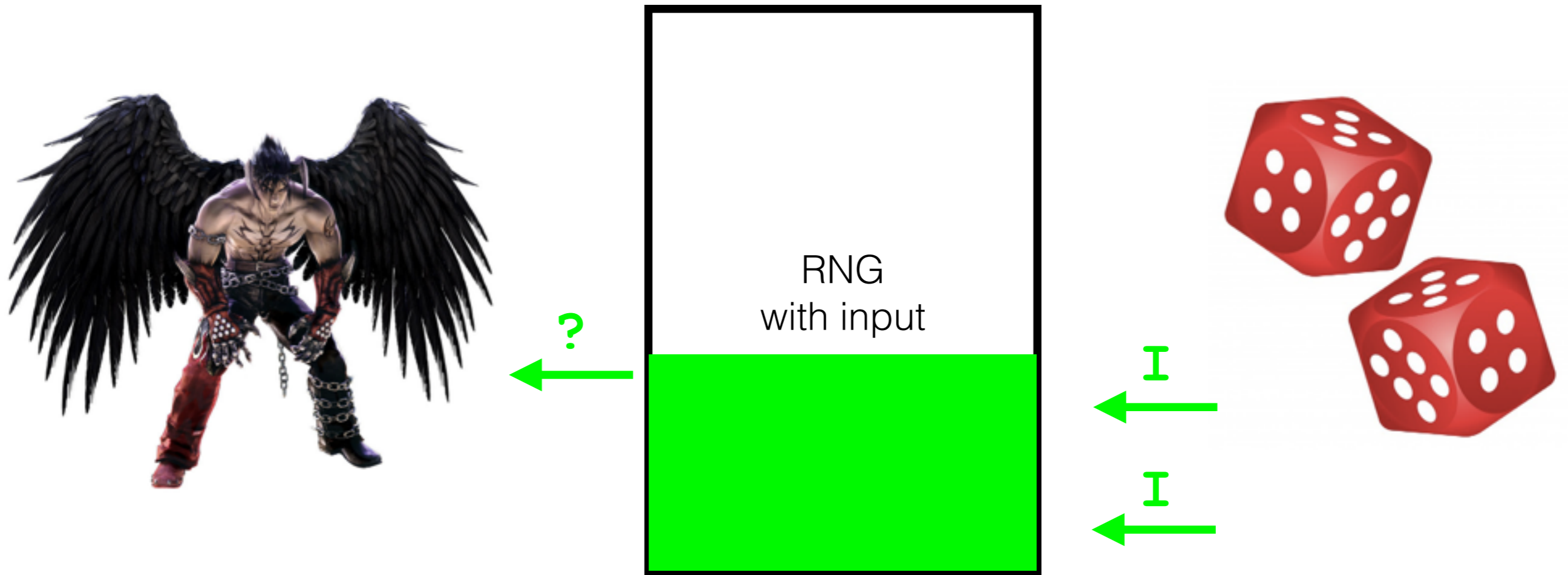
# Option 2: Estimate Entropy



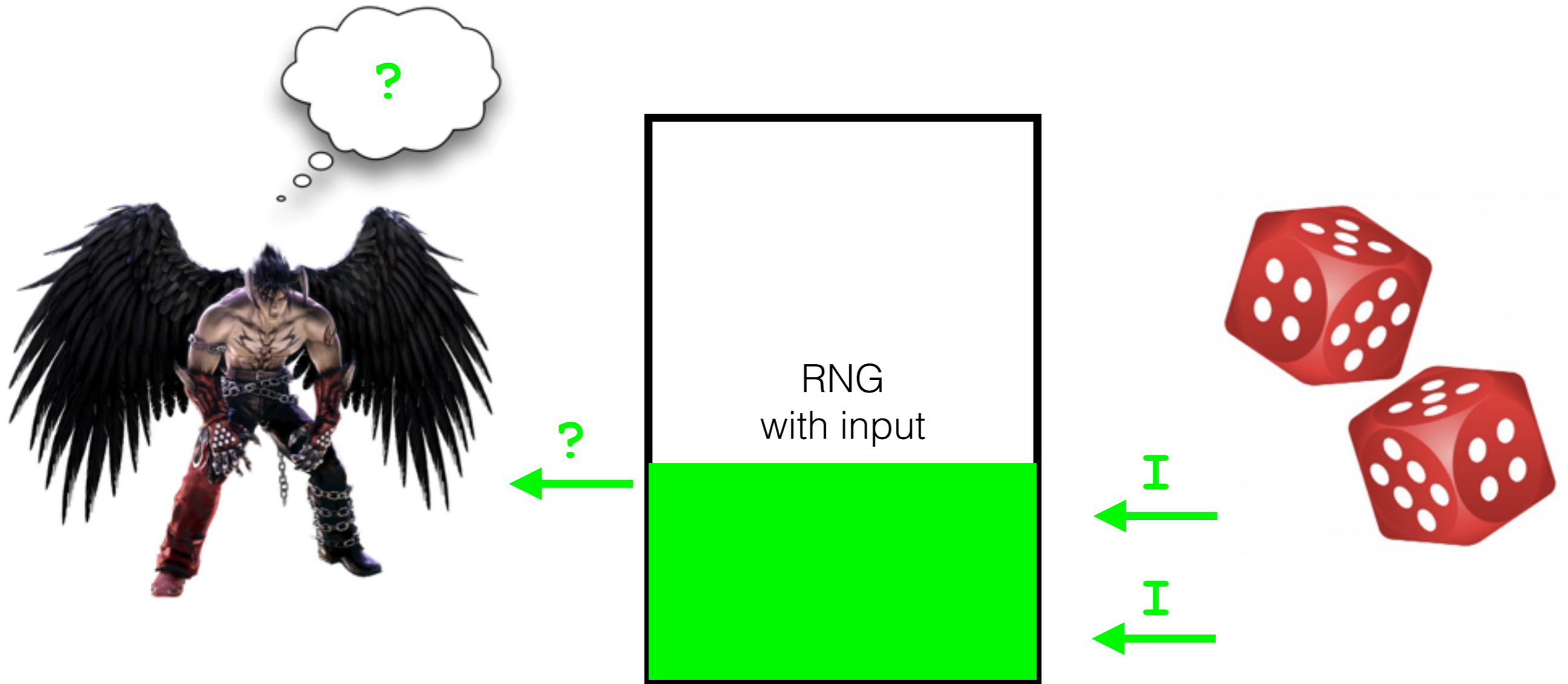
# Option 2: Estimate Entropy



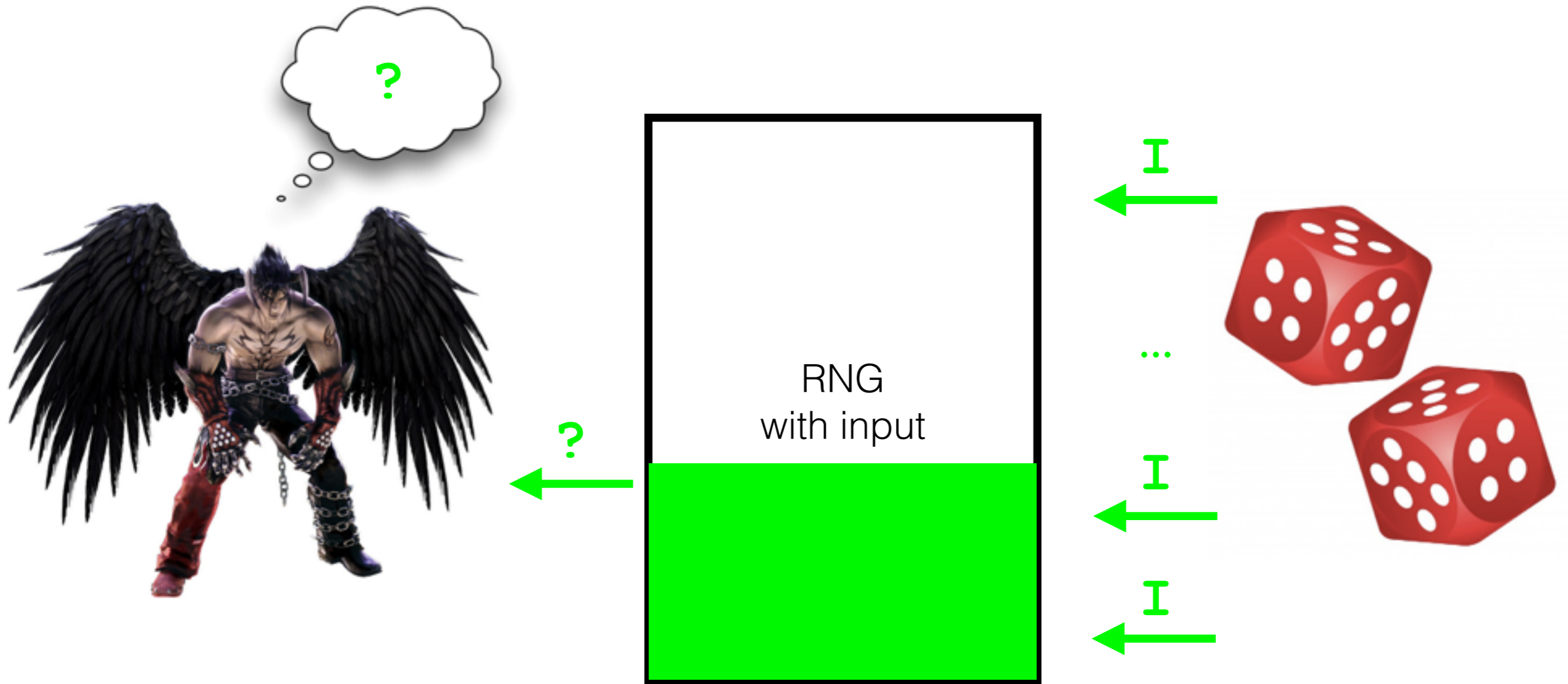
# Option 2: Estimate Entropy



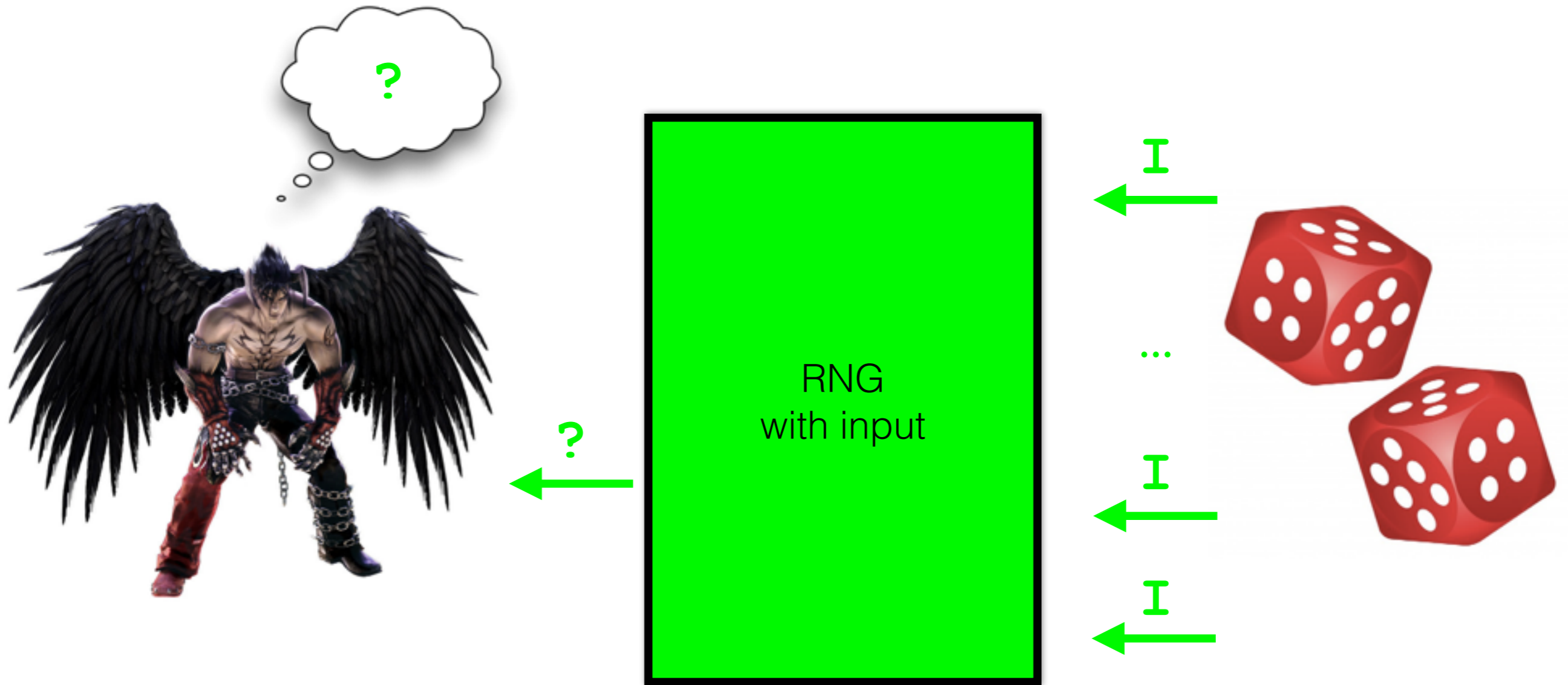
# Option 2: Estimate Entropy



# Option 2: Estimate Entropy

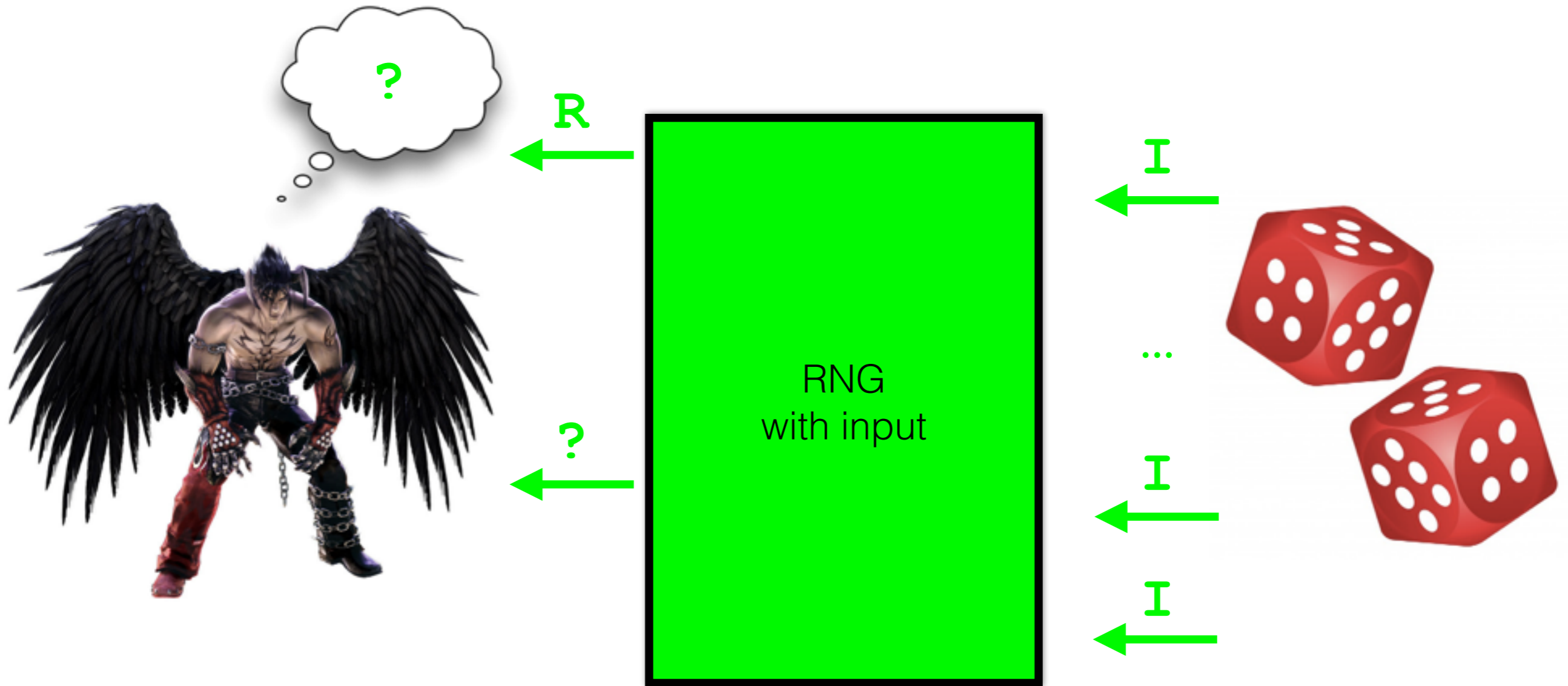


# Option 2: Estimate Entropy

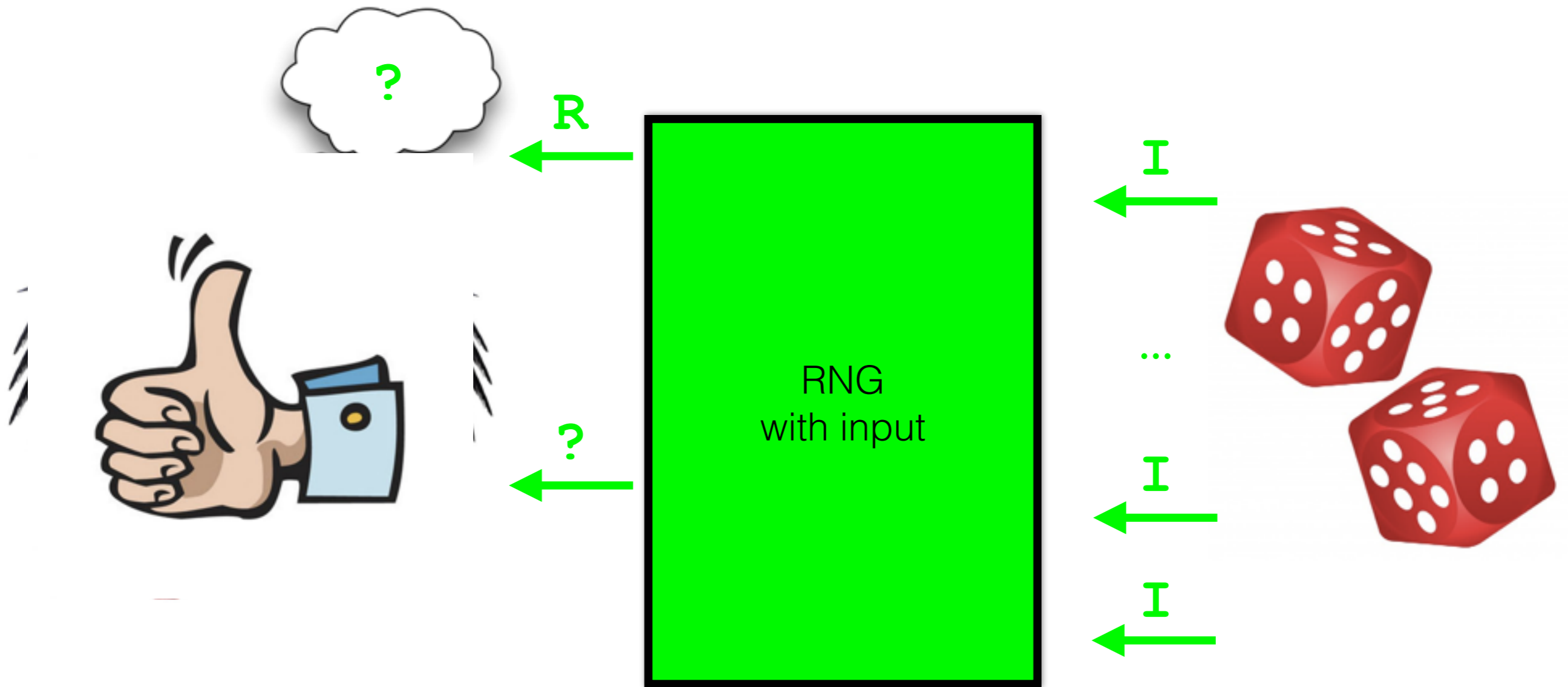




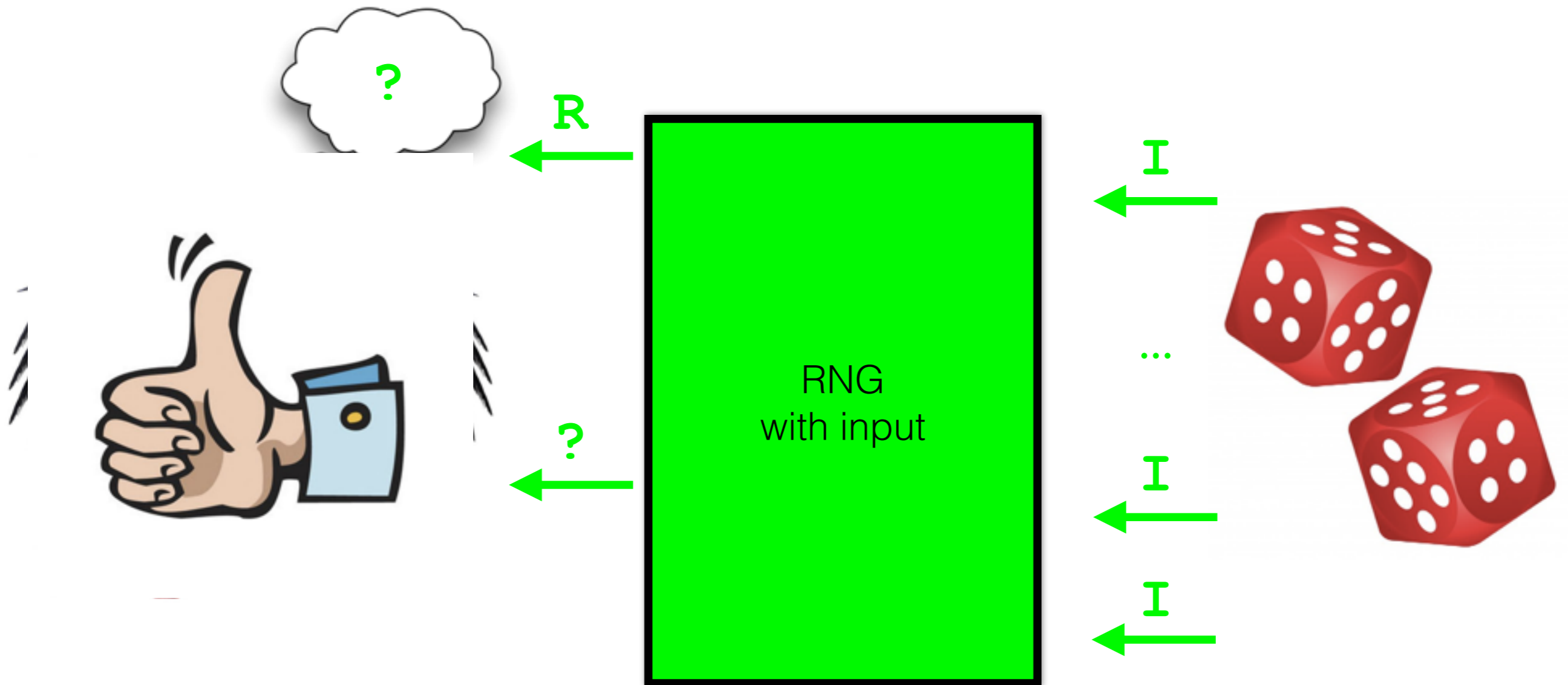
# Option 2: Estimate Entropy



# Option 2: Estimate Entropy



# Option 2: Estimate Entropy



But we **can't** estimate entropy.....

# Option 3: Prove Impossibility

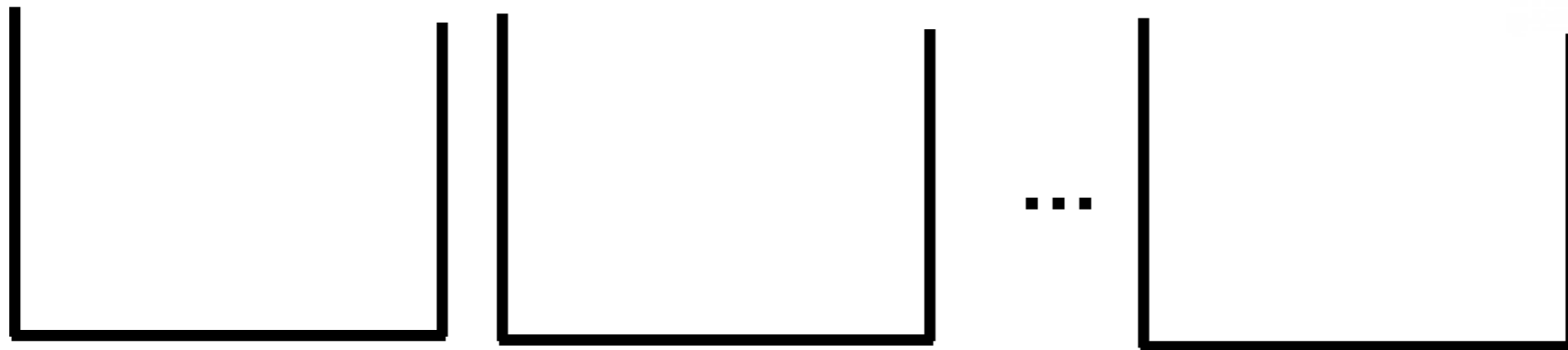
Option 3: Prove Impossibility

But it's possible.....

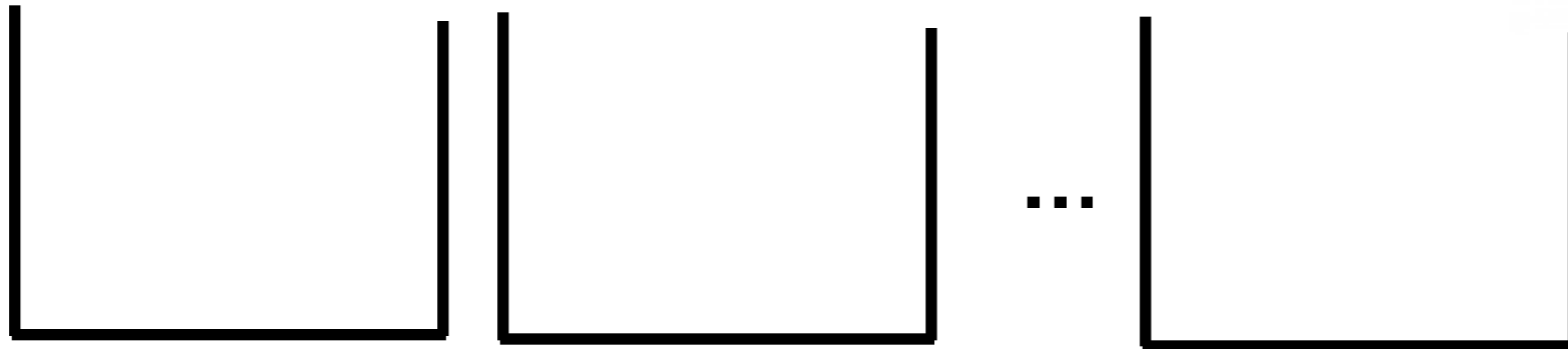


# Option 4: Eat Your Entropy and Have It Too

# Option 4: Eat Your Entropy and Have It Too

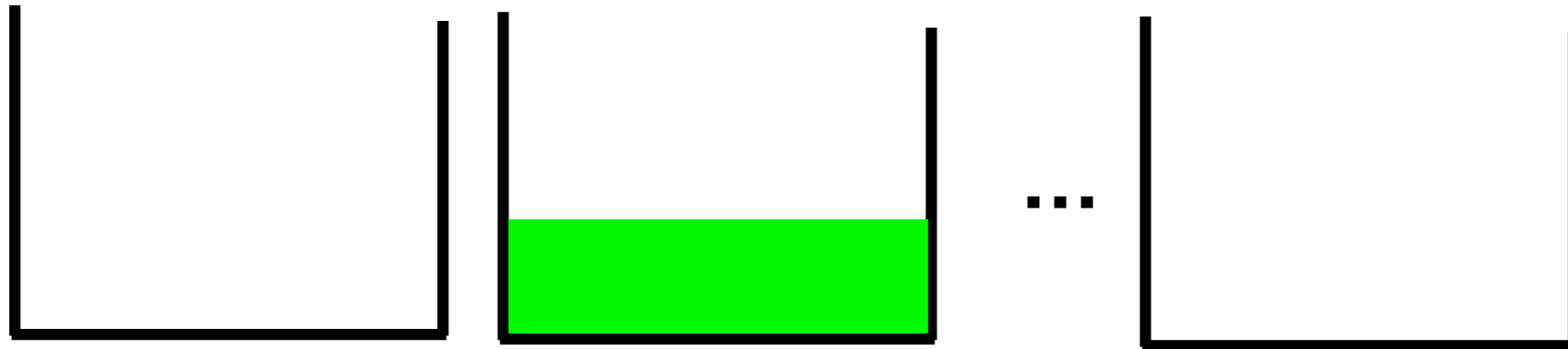


# Option 4: Eat Your Entropy and Have It Too

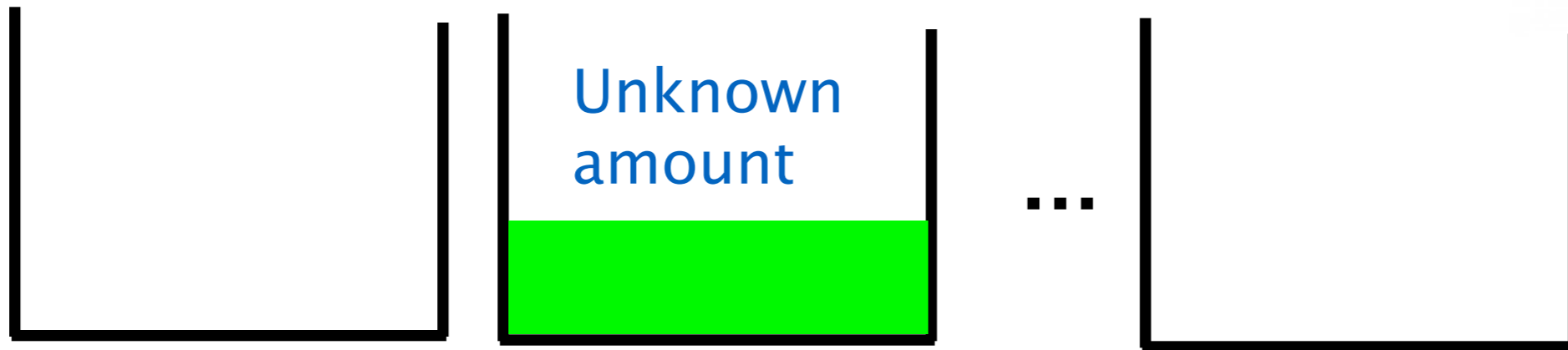




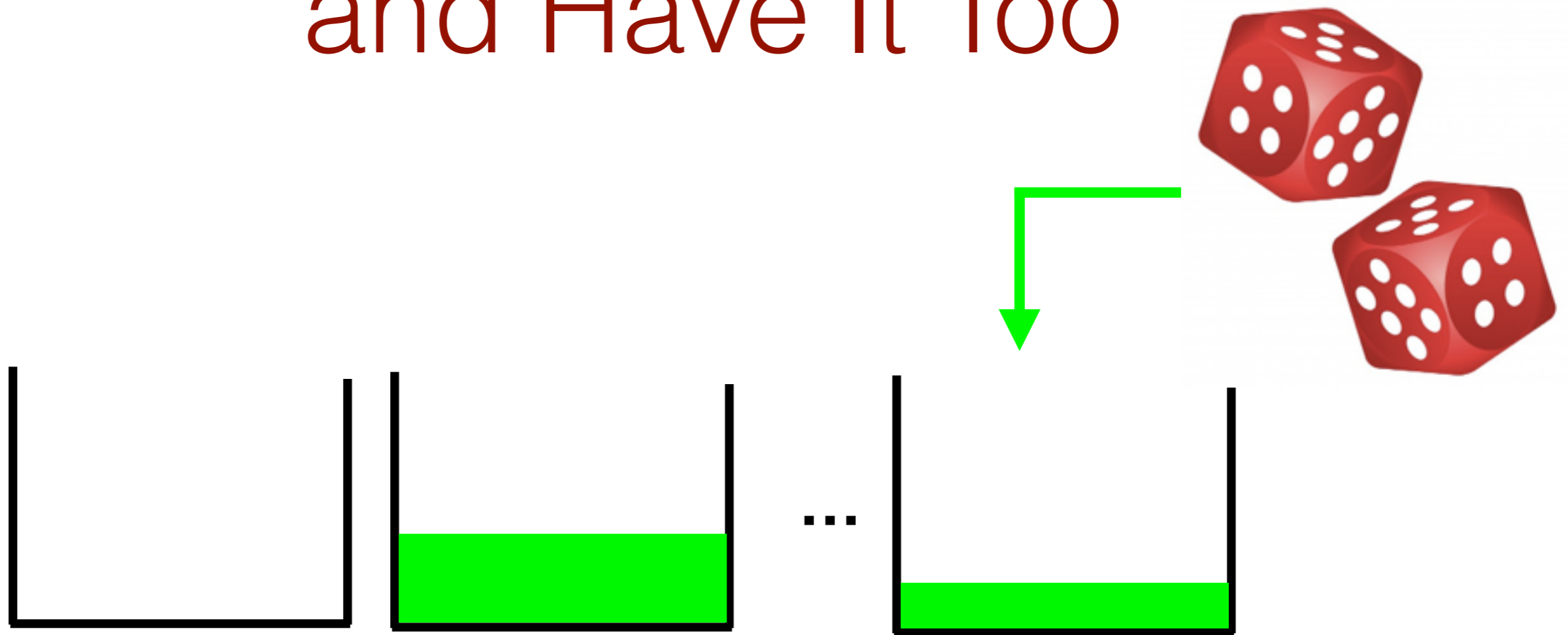
# Option 4: Eat Your Entropy and Have It Too



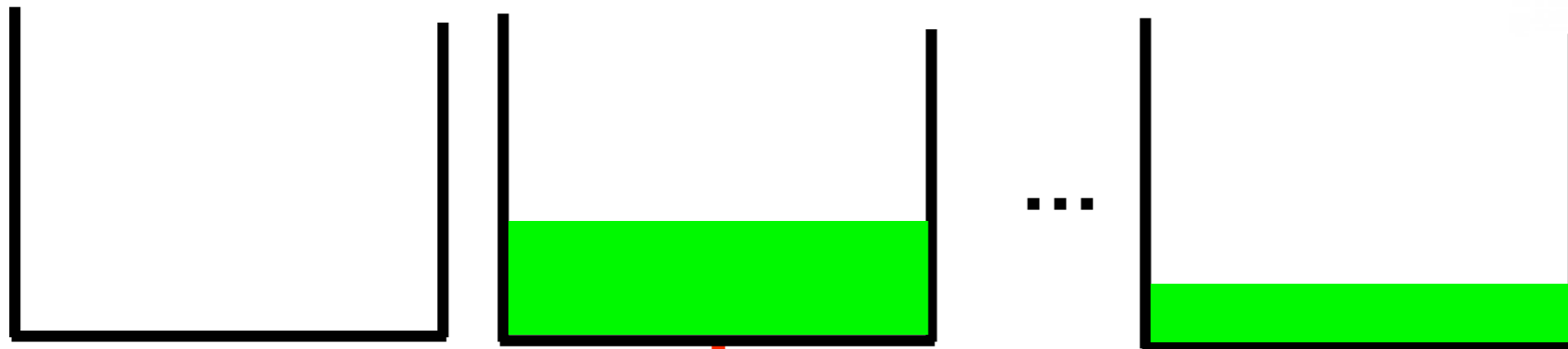
# Option 4: Eat Your Entropy and Have It Too



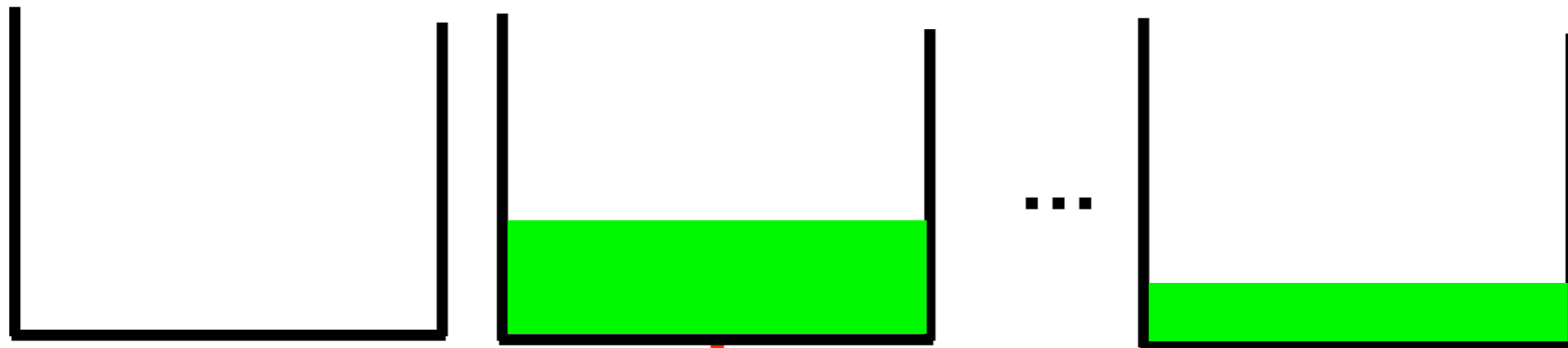
# Option 4: Eat Your Entropy and Have It Too



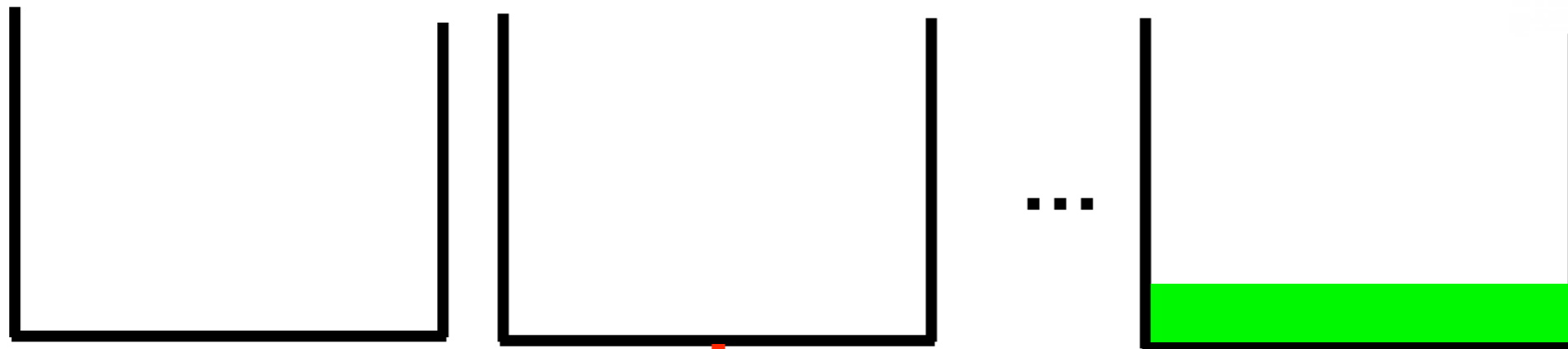
# Option 4: Eat Your Entropy and Have It Too



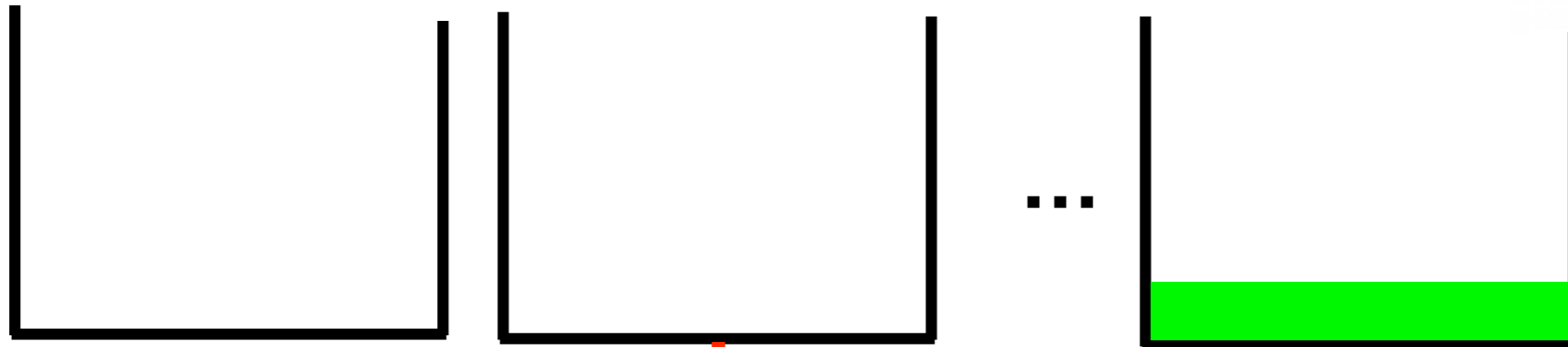
# Option 4: Eat Your Entropy and Have It Too



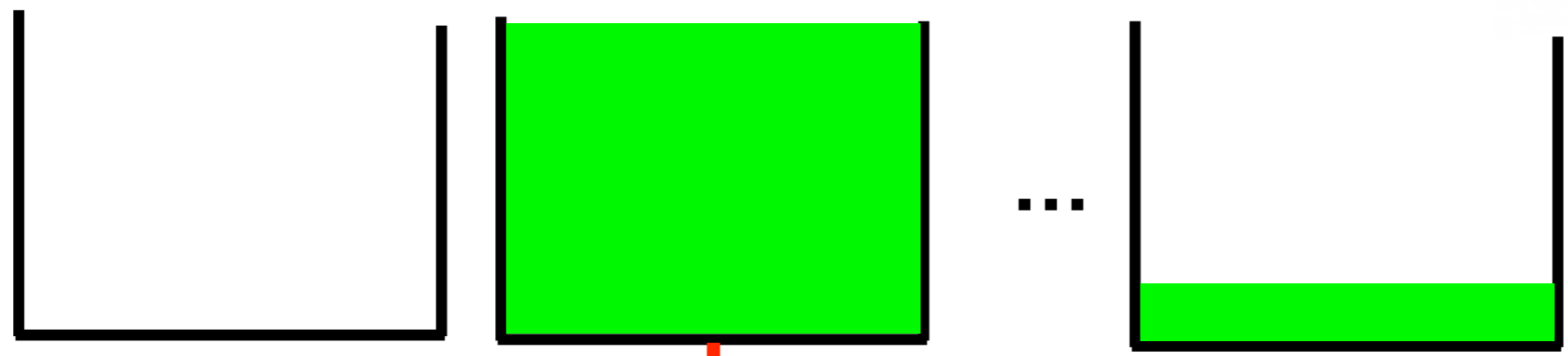
# Option 4: Eat Your Entropy and Have It Too



# Option 4: Eat Your Entropy and Have It Too

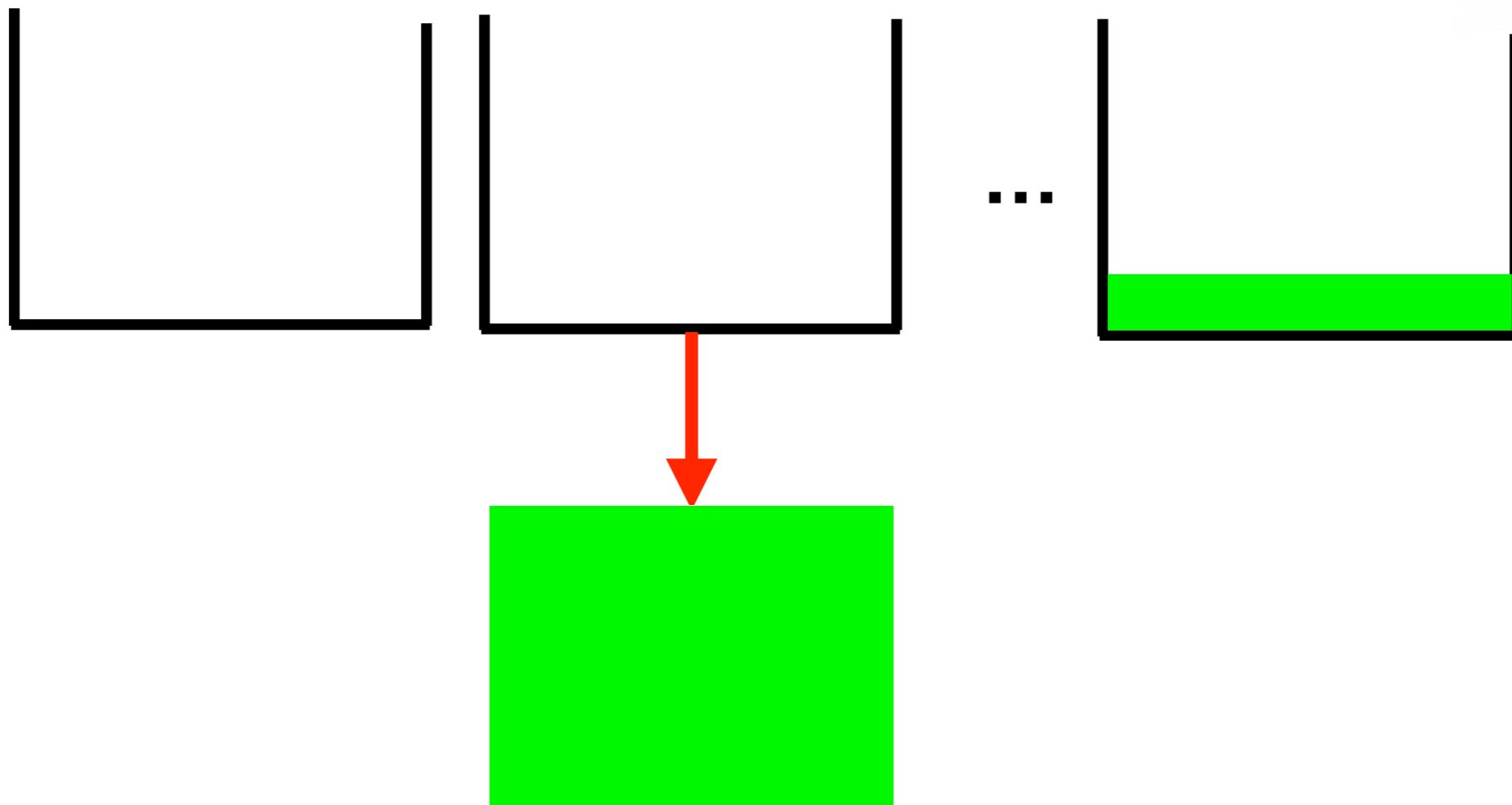


# Option 4: Eat Your Entropy and Have It Too

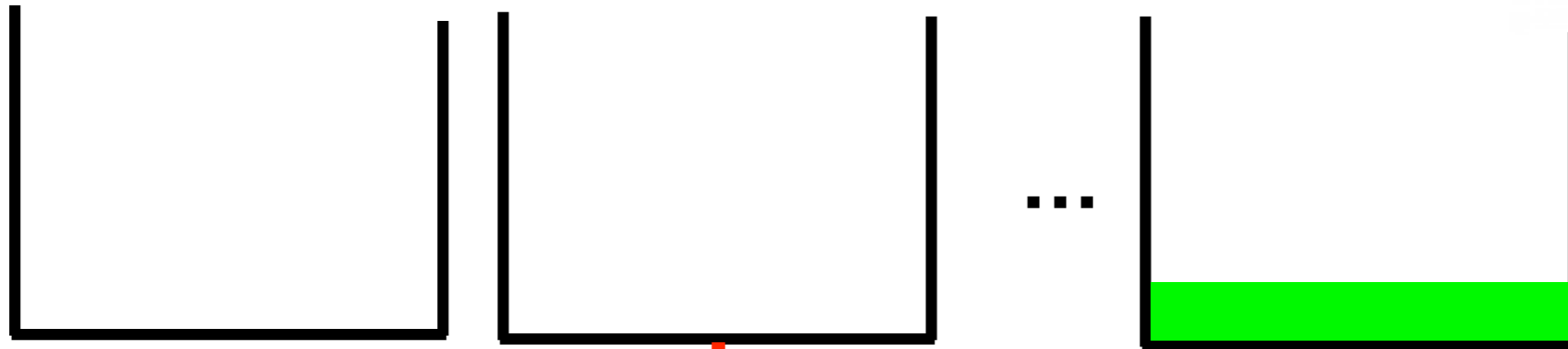




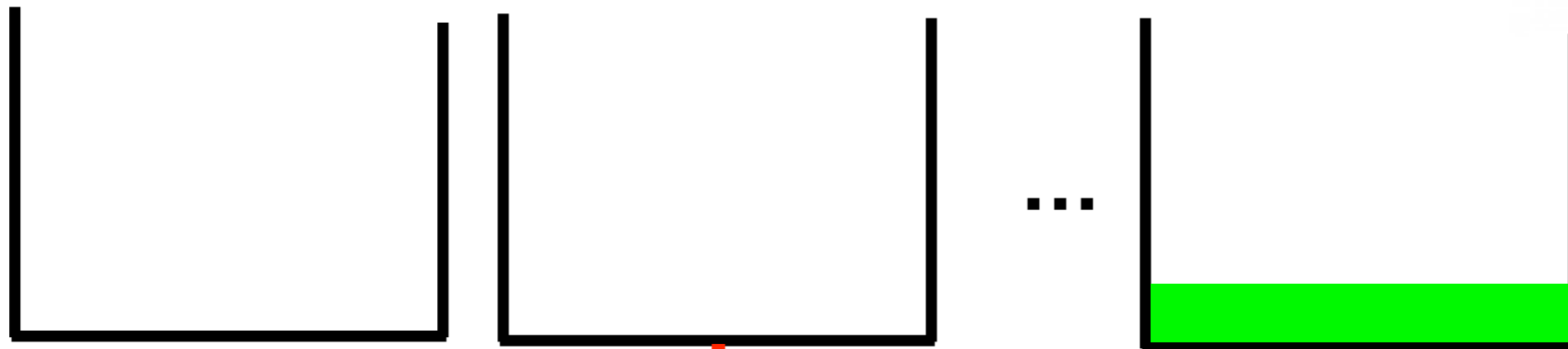
# Option 4: Eat Your Entropy and Have It Too



# Option 4: Eat Your Entropy and Have It Too



# Option 4: Eat Your Entropy and Have It Too



← Adi Shamir

# Idea Used in Practice (but not theory...)

[KSF99]'s Yarrow

[FS03]'s Fortuna

# Idea Used in Practice (but not theory...)

Only two pools



[KSF99]'s Yarrow

[FS03]'s Fortuna

# Idea Used in Practice (but not theory...)

Only two pools



[KSF99]'s Yarrow

Many pools with clever  
scheduling



[FS03]'s Fortuna

# Idea Used in Practice (but not theory...)

Only two pools



[KSF99]'s Yarrow

OS X iOS

Many pools with clever  
scheduling



[FS03]'s Fortuna



# Idea Used in Practice (but not theory...)

Only two pools



[KSF99]'s Yarrow

OS X iOS



Many pools with clever  
scheduling



[FS03]'s Fortuna





# Our Work

# Our Work

- Formal model (very strong security notion)

# Our Work

- Formal model (very strong security notion)
- Provably secure construction in this model
  - Inspired by Fortuna
  - Proof in standard model (from OWF)

# Our Work

- Formal model (very strong security notion)
- Provably secure construction in this model
  - Inspired by Fortuna
  - Proof in standard model (from OWF)
- Attacks on prior constructions

# Our Work

- Formal model (very strong security notion)
- Provably secure construction in this model
  - Inspired by Fortuna
  - Proof in standard model (from OWF)
- Attacks on prior constructions
- Formal analysis of and improvement of Fortuna
  - Secure in limited setting
  - Doubled entropy efficiency

# Thanks!

