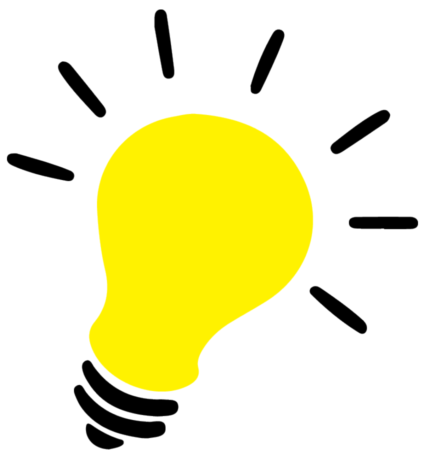
The Magic of ELFs

Mark Zhandry – Princeton University
(Work done while at MIT)

Prove this secure:

$$\mathbf{Enc(m) = (\ TDP(r),\ H(r) \oplus m\ )}$$

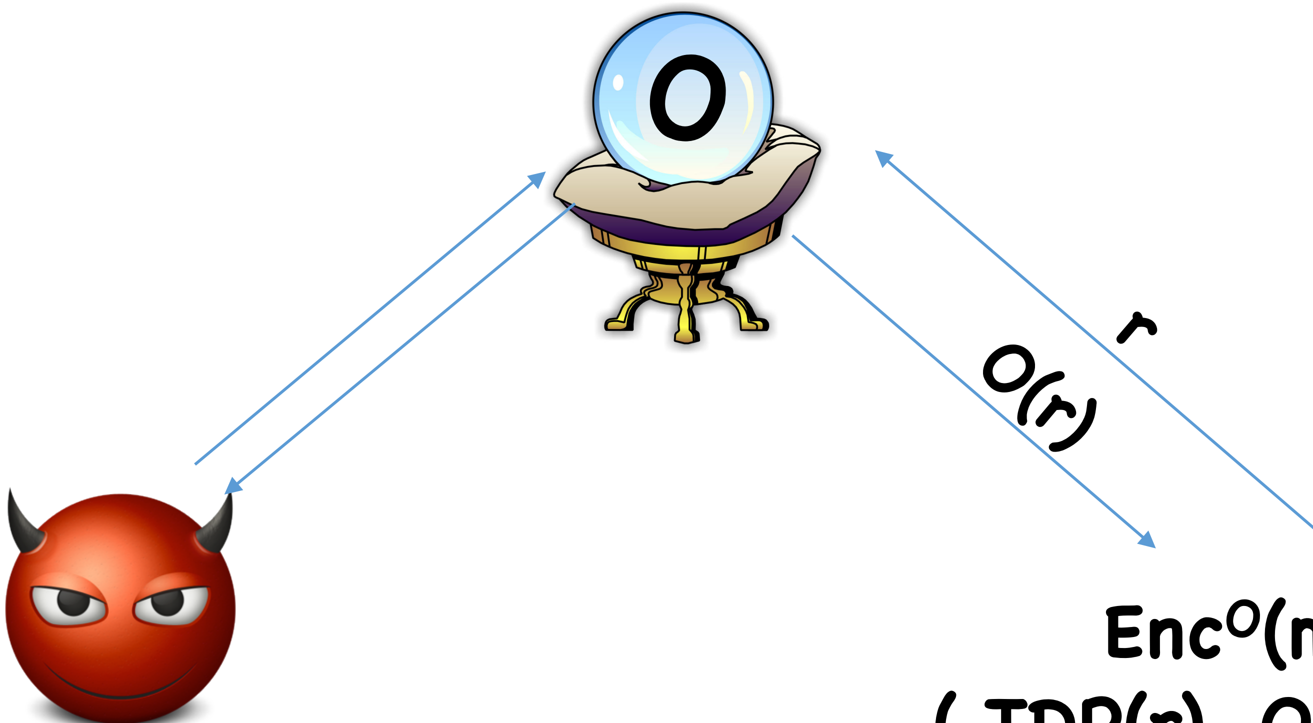
(CPA security, many-bit messages, arbitrary TDP)



Random Oracles

Random Oracle Model [BR'93]

Model **H** as random oracle **O**



$$\mathbf{Enc}^{O}(\mathbf{m}) =$$
$$(\ \mathbf{TDP}(\mathbf{r}),\ O(\mathbf{r}) \oplus \mathbf{m}\ )$$

Power of Random Oracles

- Great extractors, even for comp. unpredictability

  O(x) pseudorandom given **OWF(x)**

- Hard to find outputs with trapdoors

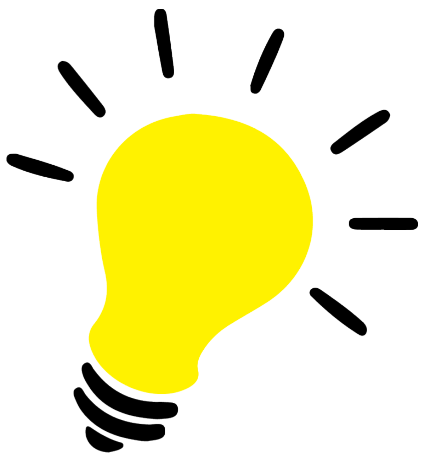
  (x,O(x)) with trapdoor **T** for **O(x)**

- Selective to adaptive security for Sigs, IBE

  Sign(m) $\Rightarrow$ **Sign(O(m))**

Limitations of Random Oracles

- Random oracles don’t exist!
- RO “proof” = heuristic security argument
- Heuristic known to fail in some cases [CGH’98,BBP’03,BFM’14]



Standard-model defs

Standard-model Security Defs for H

Standard defs: Assume H is a OWF, PRG, CRHF, etc

- Simple, easy to state definitions
- Can base on standard, plausible assumptions
- Limited usefulness for instantiating RO's

Standard-model Security Defs for H

Standard defs: Assume H is a OWF, PRG, CRHF, etc

- Simple, easy to state definitions
- Can base on standard, plausible assumptions
- Limited usefulness for instantiating RO's

Exotic defs: UCE's [BHK'15], "strong" OWF/PRG, etc

- Useful for some RO constructions
- Usually require "tautological assumptions"

Assumption Families

Ex: Strong PRG (strengthens strong OWF of [BP'11,Wee'05])

- Parameterized by sampler **S() → (x, aux)**
- Assume **x** is "computationally unpredictable" given **aux**
- Security requirement: **H(x)** pseudorandom given **aux**

Assumption Families

Ex: Strong PRG (strengthens strong OWF of [BP'11,Wee'05])

- Parameterized by sampler **S() → (x, aux)**
- Assume **x** is "computationally unpredictable" given **aux**
- Security requirement: **H(x)** pseudorandom given **aux**

How to gain confidence in assumption?

- Attempt cryptanalysis, post challenges, etc.
- Problem: which **S** to target?

Similar weaknesses for UCEs and other exotic assumptions

Security Properties vs Assumptions

UCE's, strong OWF/PRGs are useful as security *properties*

However, highly undesirable as security *assumptions*

Ideal scenario:

Single, simple, well-studied assumption

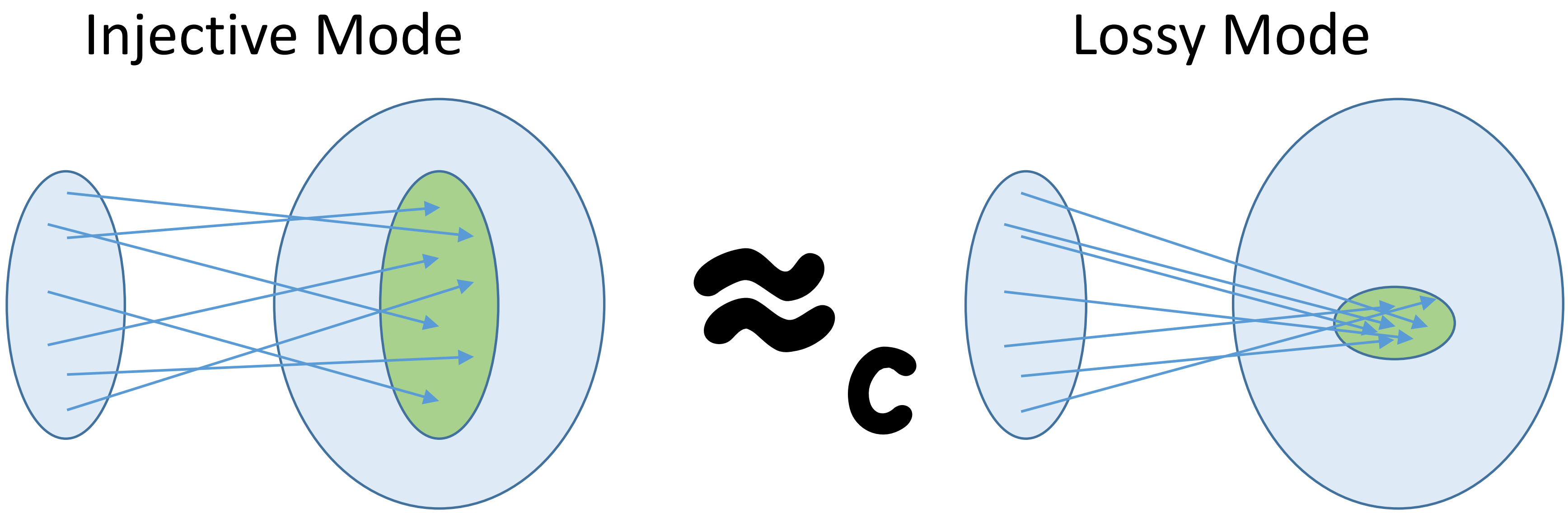
↓

Strong security properties

This Work:

Extremely Lossy Functions (ELFs)

Standard Lossy Functions [PW'08]

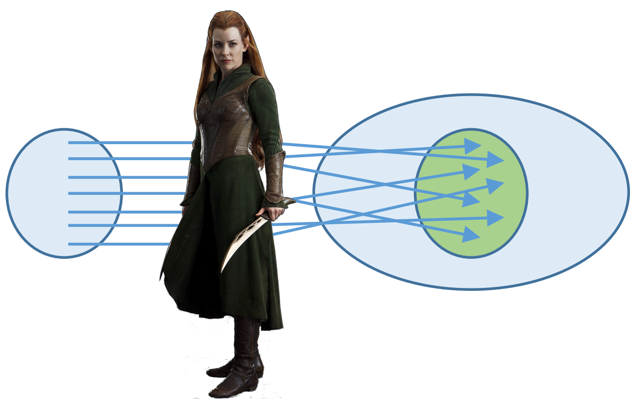


Notes:

- Lossy Mode image size typically exponential
- Generally also include trapdoor in injective mode

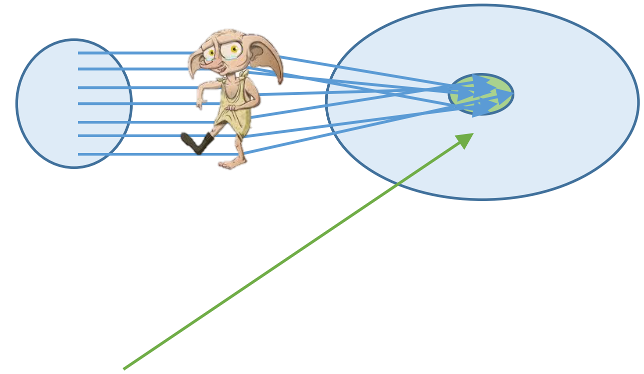
Extremely Lossy Functions (ELFs)

Injective Mode:



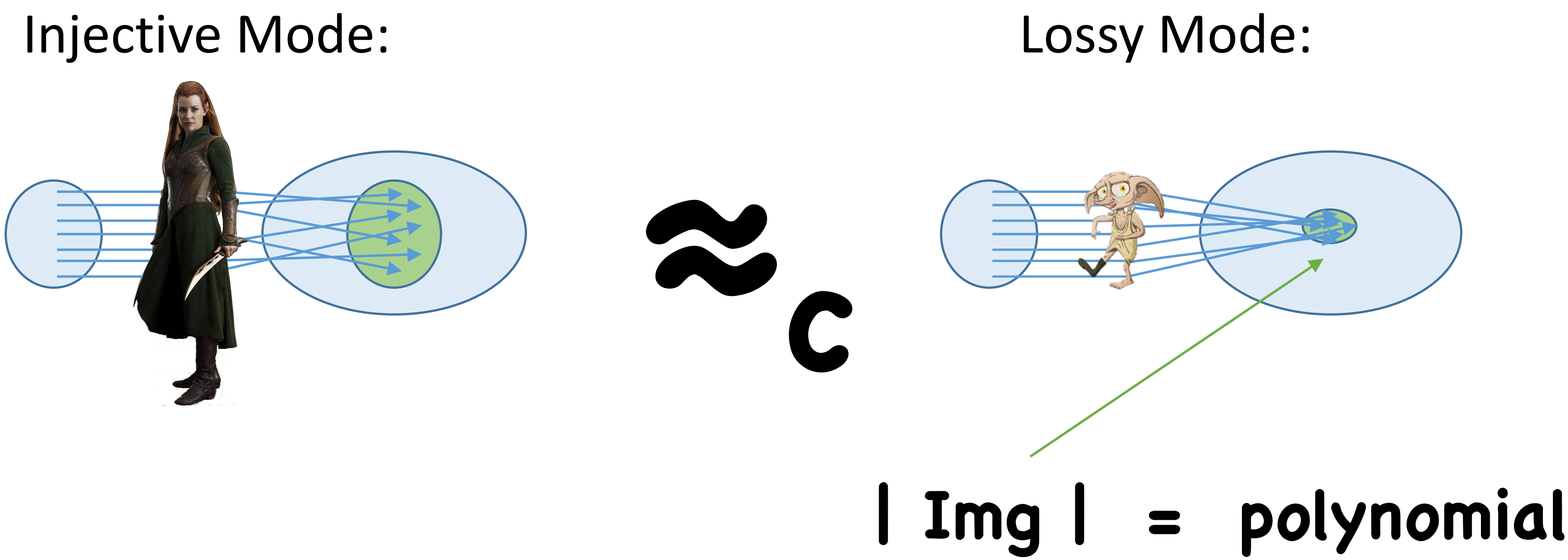
$\approx_c$

Lossy Mode:



| Img | = polynomial

Extremely Lossy Functions (ELFs)

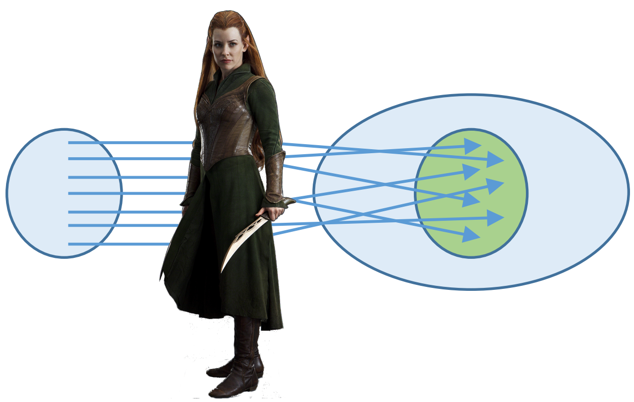


Problem: **| Img |**- time attack

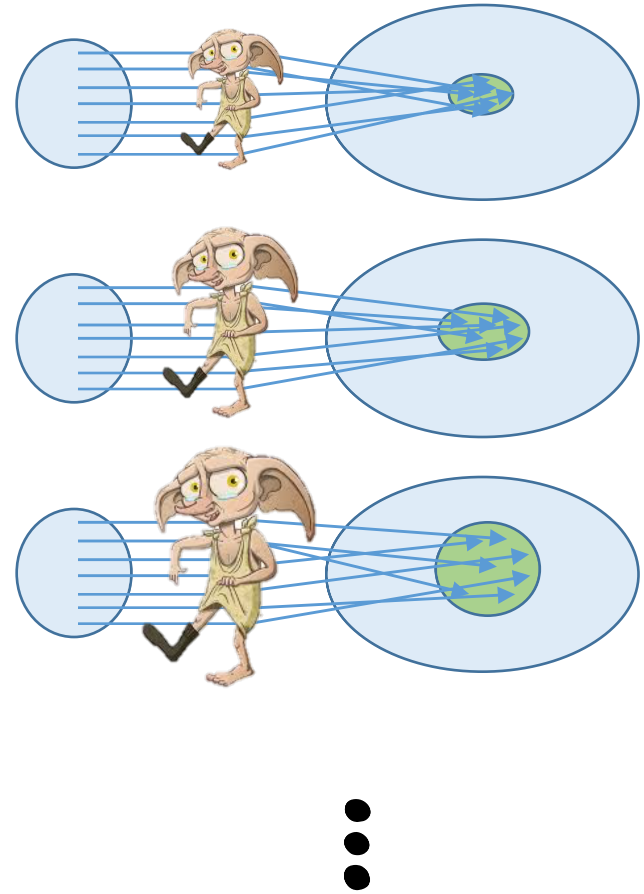
- Query on **| Img |+1** points
- Look for collision

Extremely Lossy Functions (ELFs)

Injective Mode:



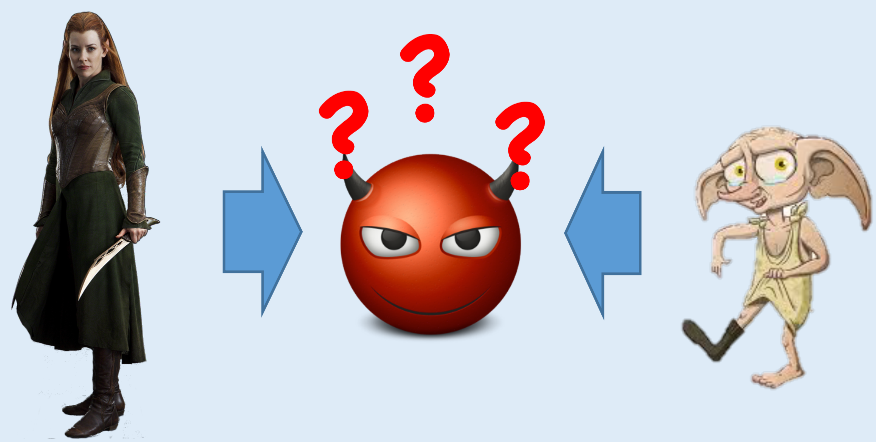
Lossy Modes:



Extremely Lossy Functions (ELFs)

Rough* security statement:

∀  ∃  **s.t.**



* Must also consider adversary's success probability

Constructing ELFs

Step 1: Bounded-adversary ELFs

=

Only one 

Security against a priori bounded 

Step 1: Bounded-adversary ELFs

Use standard lossy functions based on elliptic curves

[PW'08, FGKRS'10]

$$x \in Z_p^n \Rightarrow g^{A \cdot x} = (g^A) \cdot x$$

Hand out $\mathbf{g^A}$ as description of function

Injective mode: $\mathbf{A}$ random full rank matrix

Lossy mode: $\mathbf{A}$ random rank-$\mathbf{1}$ matrix

Lossy image size $\mathbf{p}$ $\Rightarrow$ Set $\mathbf{p}$ to be some polynomial

Thm [Adapt FGKRS'10]: Exponential DDH assumption $\Rightarrow$ modes indistinguishable to $\mathbf{p^c}$-time adversaries $\mathbf{(0<c<1)}$

Plausibility of Exponential DDH

Non-standard assumption

- Not truly falsifiable in the sense of [Naor'03]

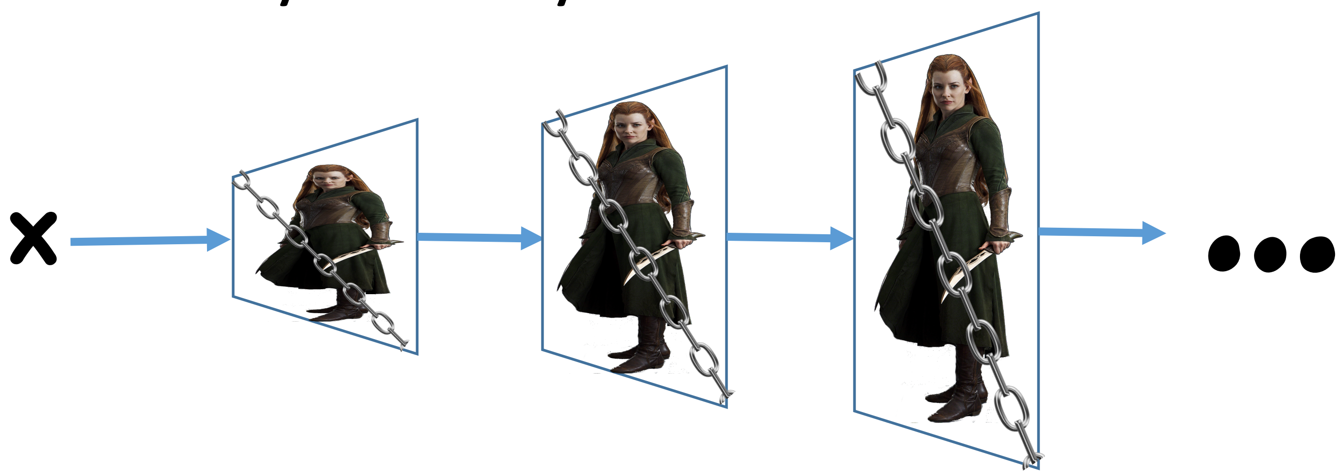
However, still very "reasonable"

- "Complexity assumption" [GK'15]
- On elliptic curves, best known attack: $\mathbf{p}^{1/2}$
  - "Generic attack", essentially no non-trivial attacks known
- In practice, parameters set assuming $\mathbf{p}^{1/2}$ is optimal

If exponential DDH is false,
much more to worry about

Step 2: Bounded to Unbounded

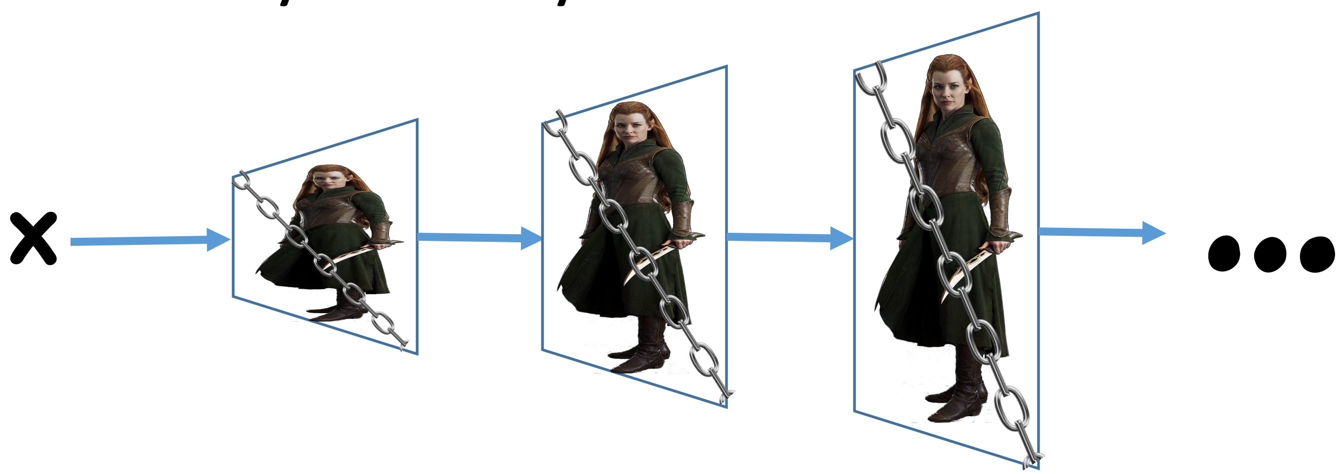
Iterate at many security levels



ith lossy mode image size at most $\mathbf{2^i}$,
security against $\mathbf{(2^i)^c}$-time adversaries

Step 2: Bounded to Unbounded

Iterate at many security levels

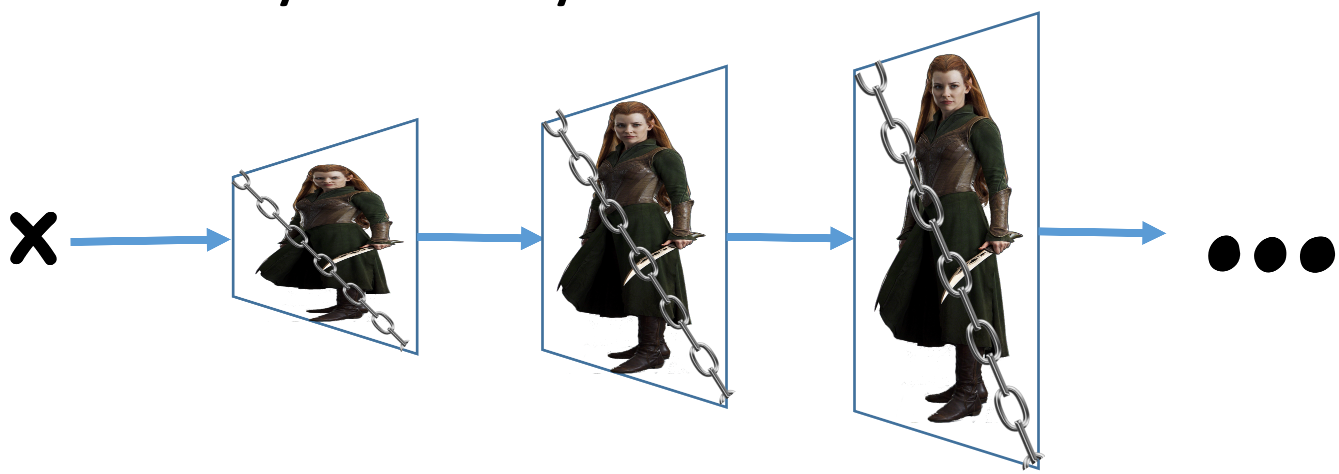


ith lossy mode image size at most 2^i,
security against $(2^i)^c$-time adversaries

Given t-time , invoke lossiness at i such that $t < 2^{ic} \le 2t$
$\Rightarrow$ Image size at most $(2t)^{1/c}$

Step 2: Bounded to Unbounded

Iterate at many security levels



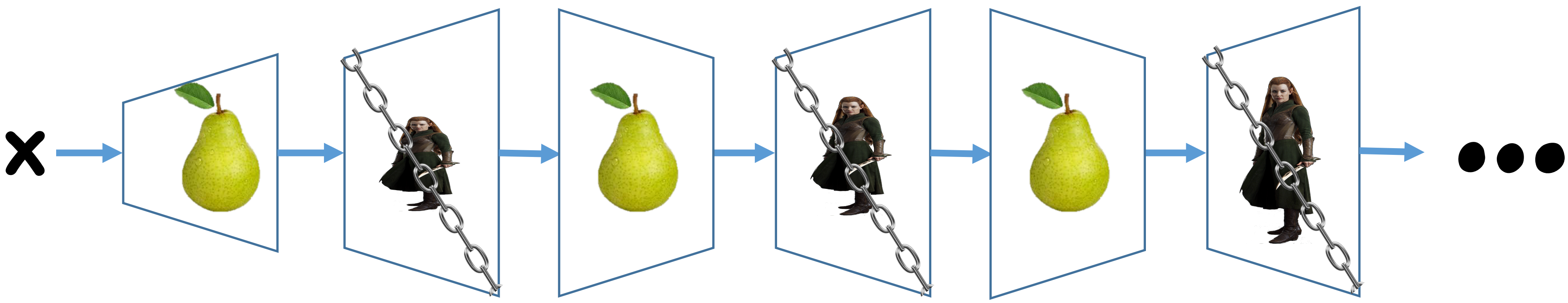
ith lossy mode image size at most 2^i,
security against $(2^i)^c$-time adversaries

Given t-time , invoke lossiness at i such that $t < 2^{ic} \le 2t$
$\Rightarrow$ Image size at most $(2t)^{1/c}$

Problem: output size grows too fast!

Step 2: Bounded to Unbounded

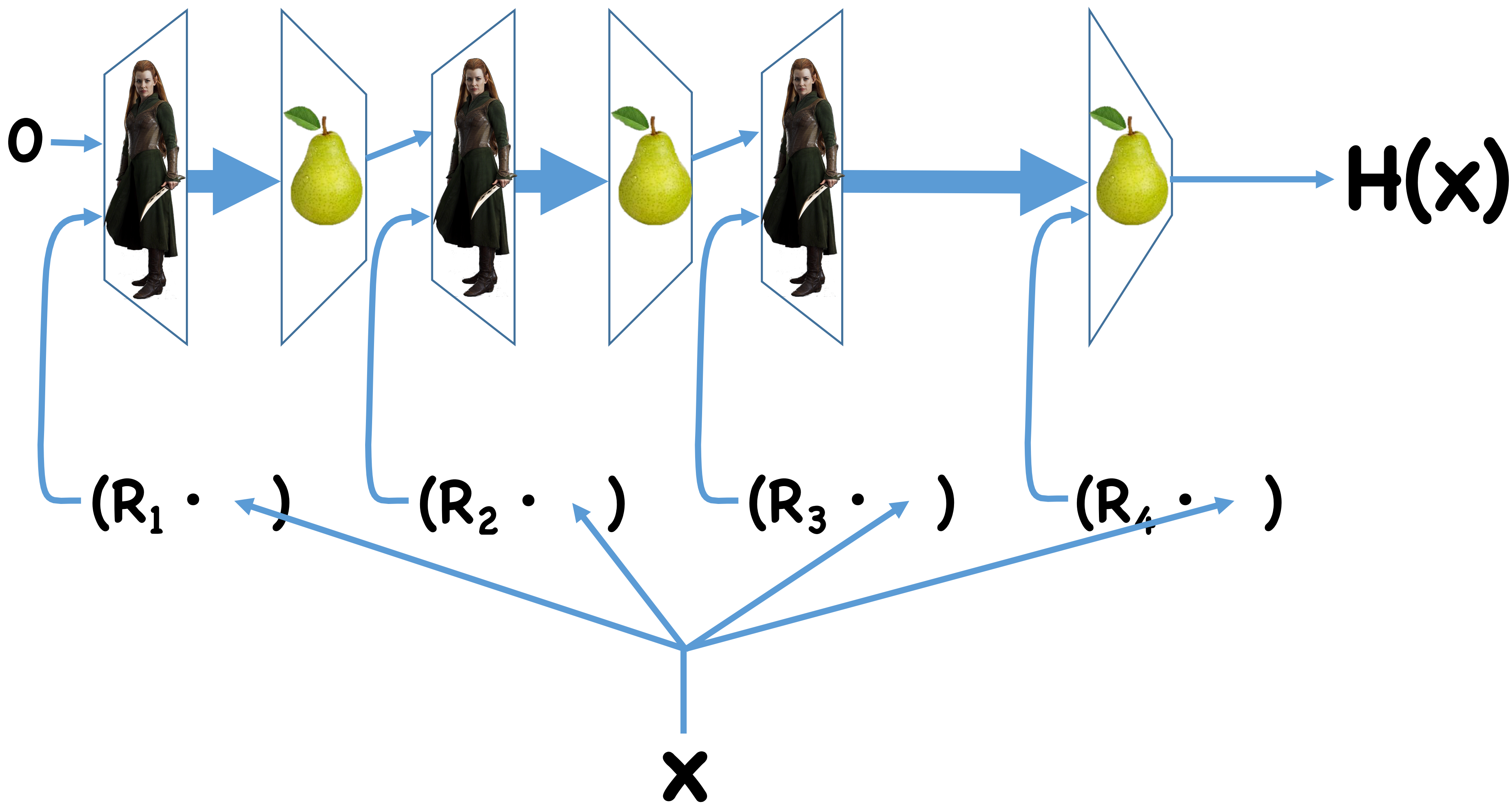
Keep output small by pairwise-independent hashing



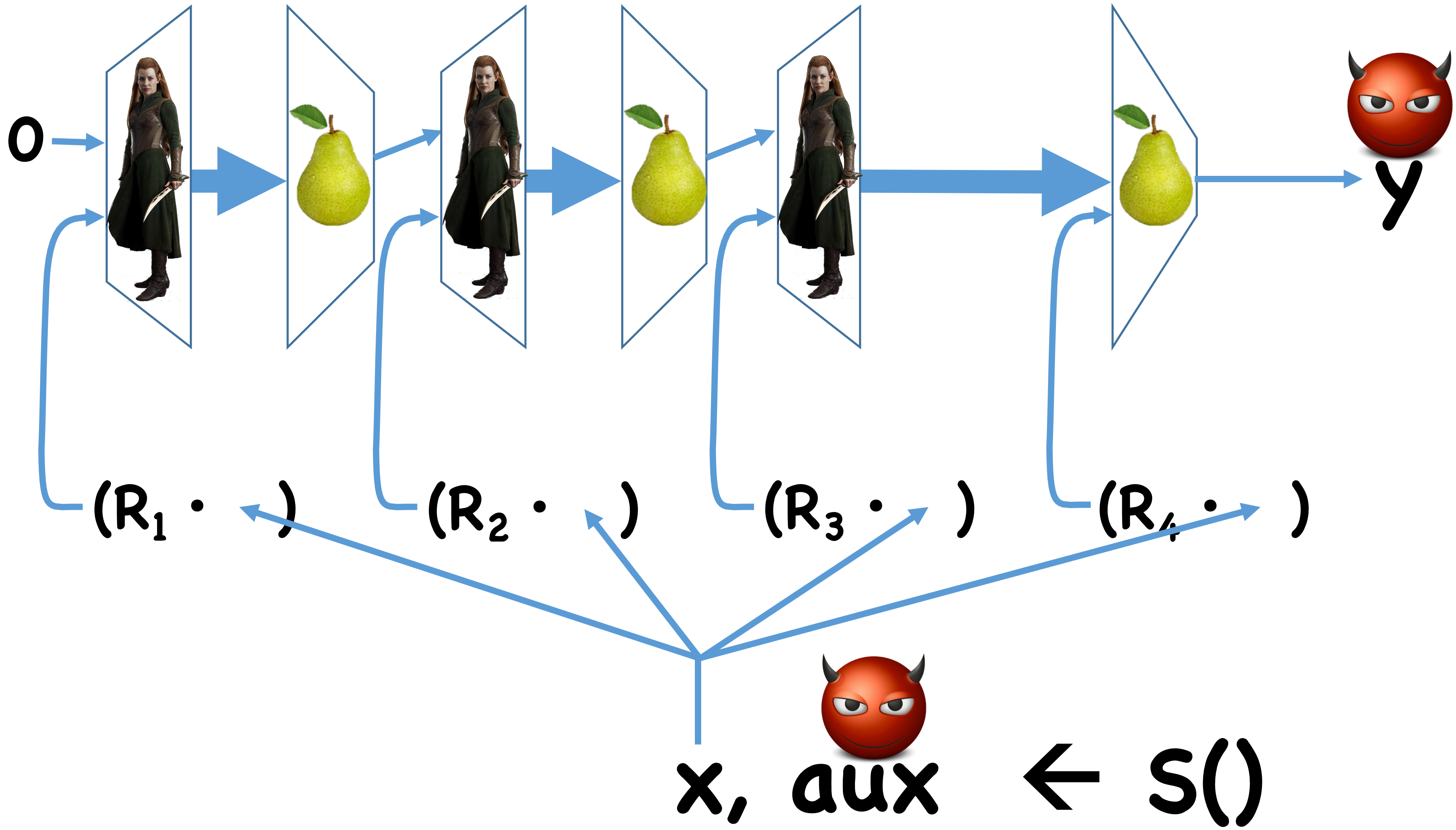
 = Pairwise independent function

Using ELFs

A Strong PRG

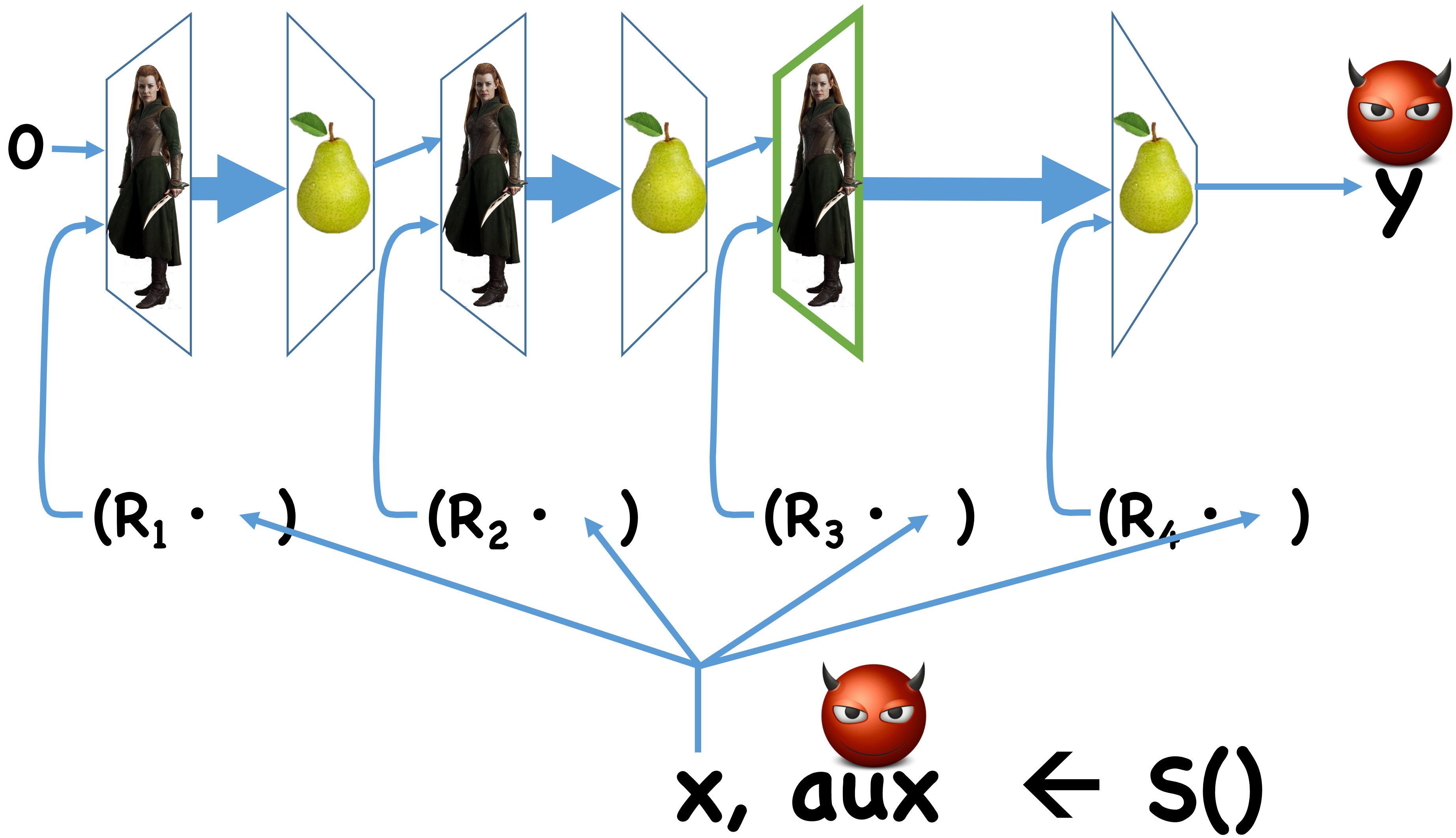


Security Proof Sketch

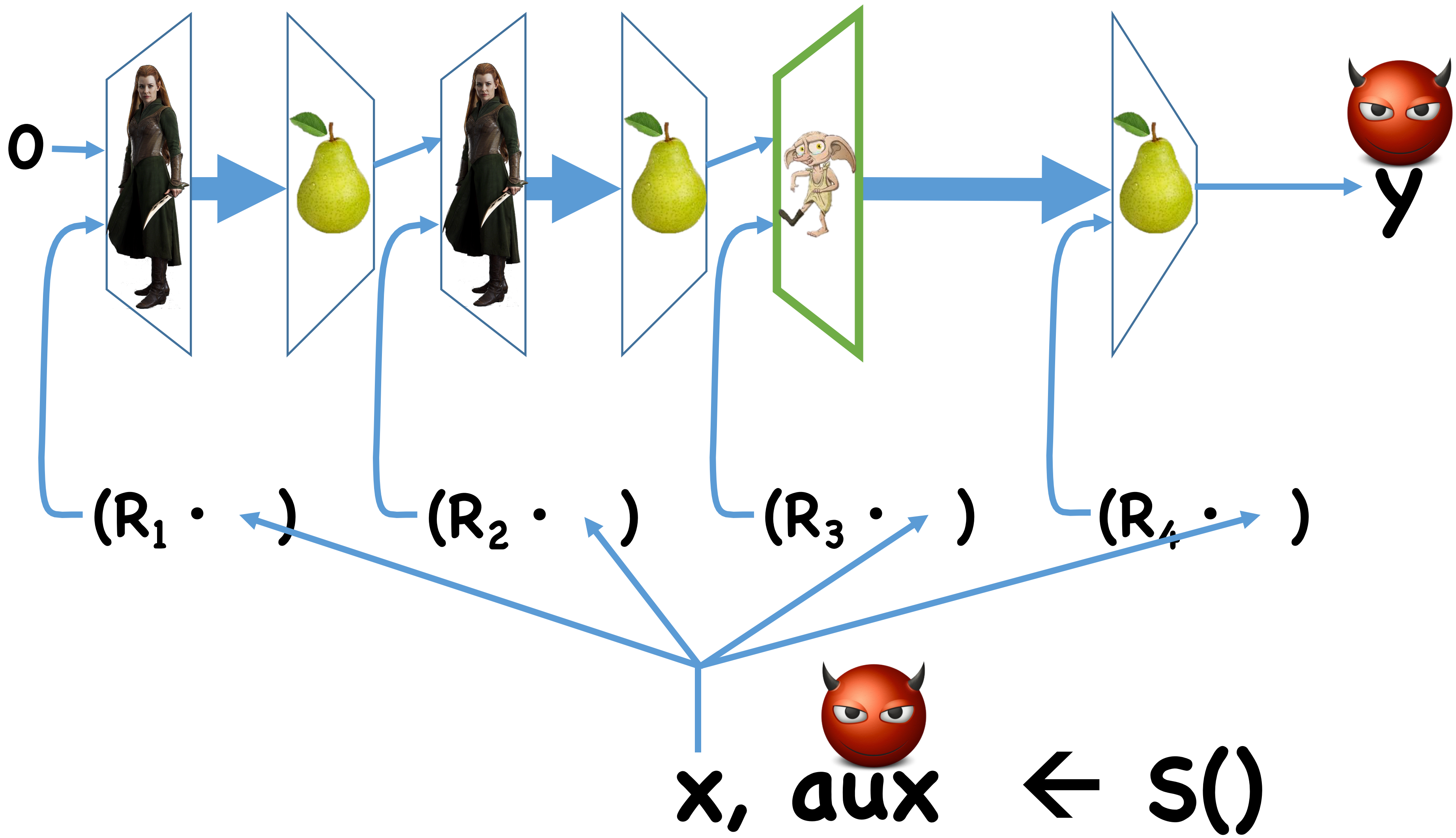


Guarantee: **x** computationally unpredictable, given **aux**

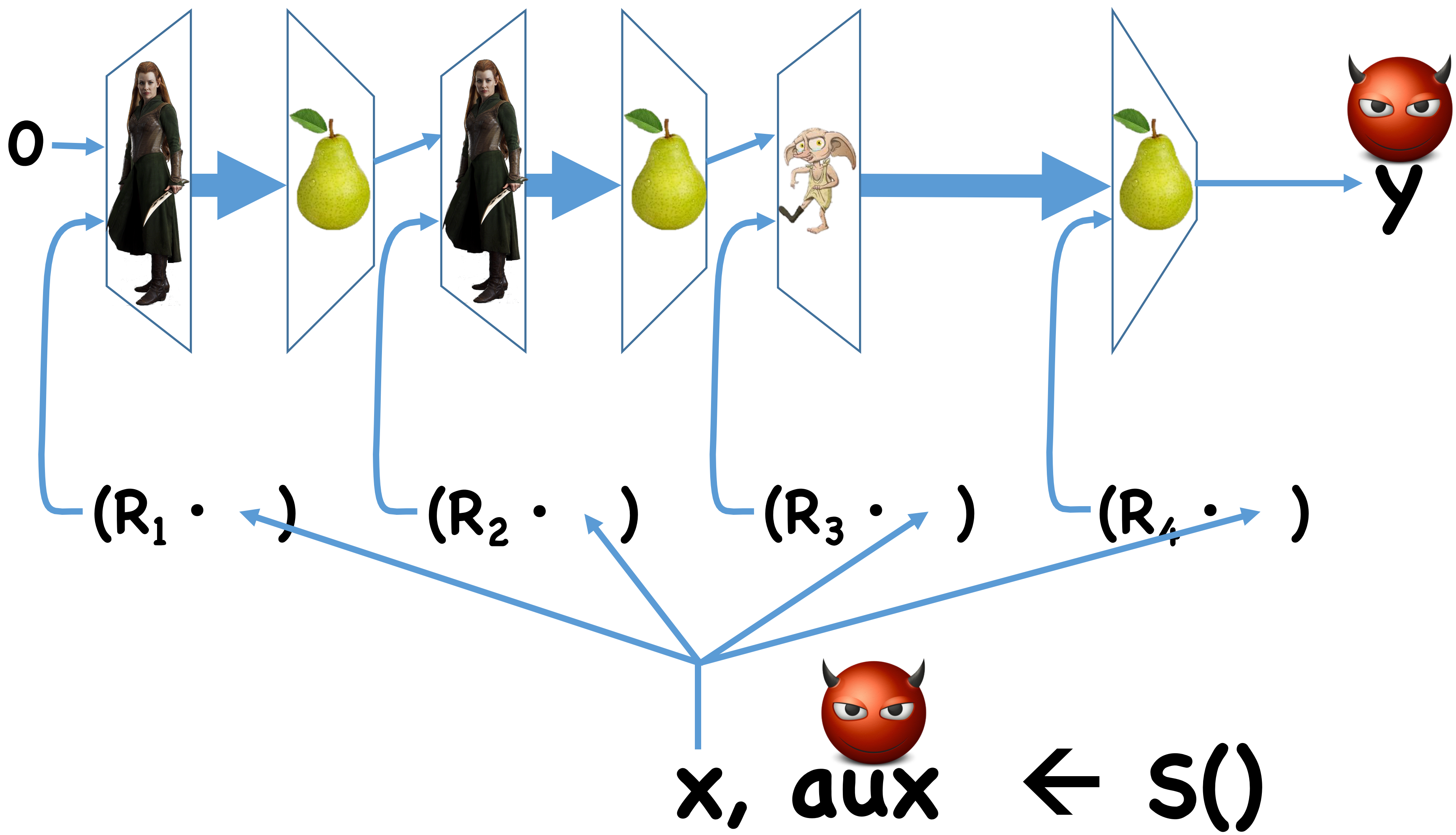
Step 1: Invoke ELF Magic



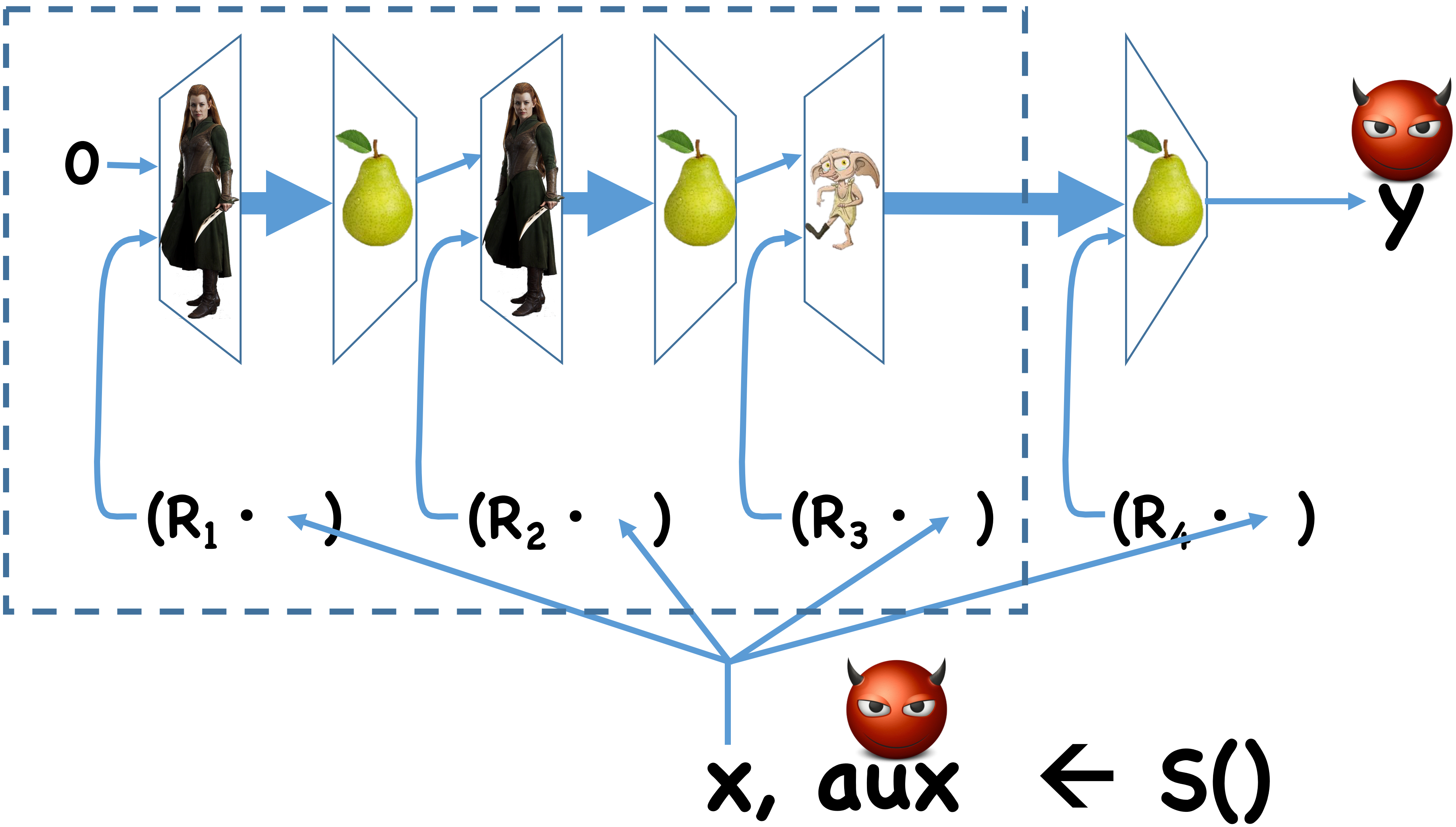
Step 1: Invoke ELF Magic



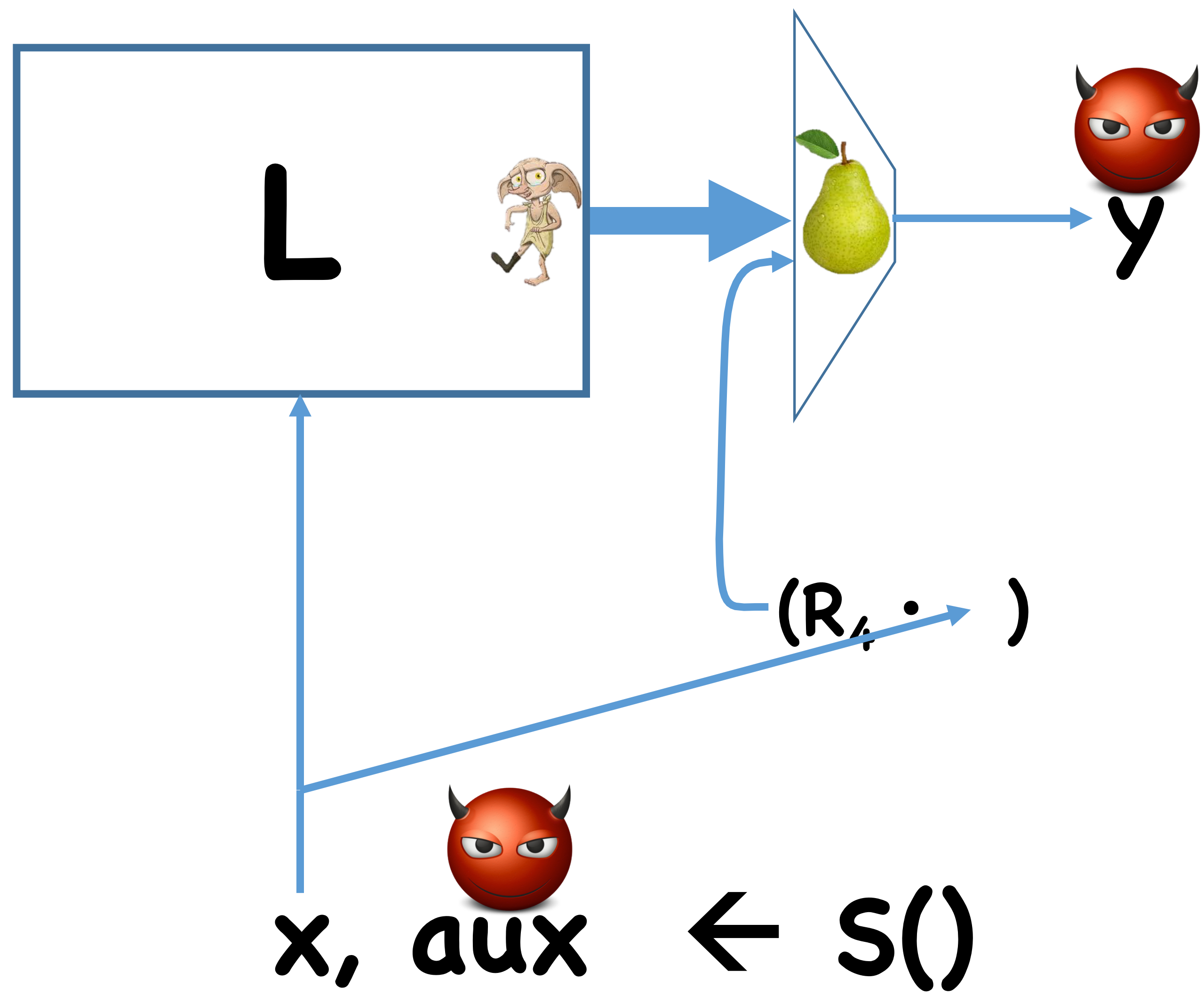
Step 2: Invoke Goldreich-Levin



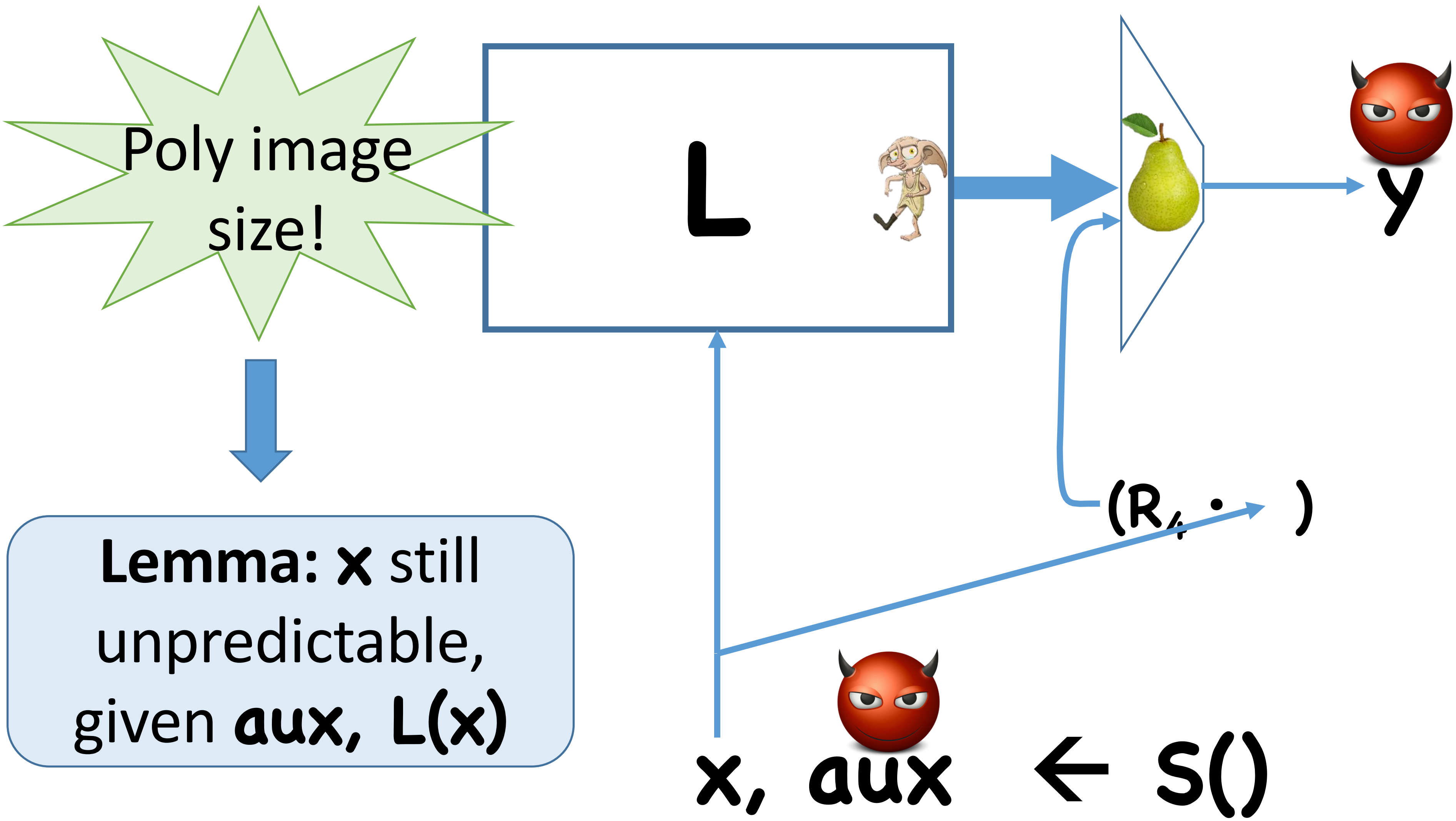
Step 2: Invoke Goldreich-Levin



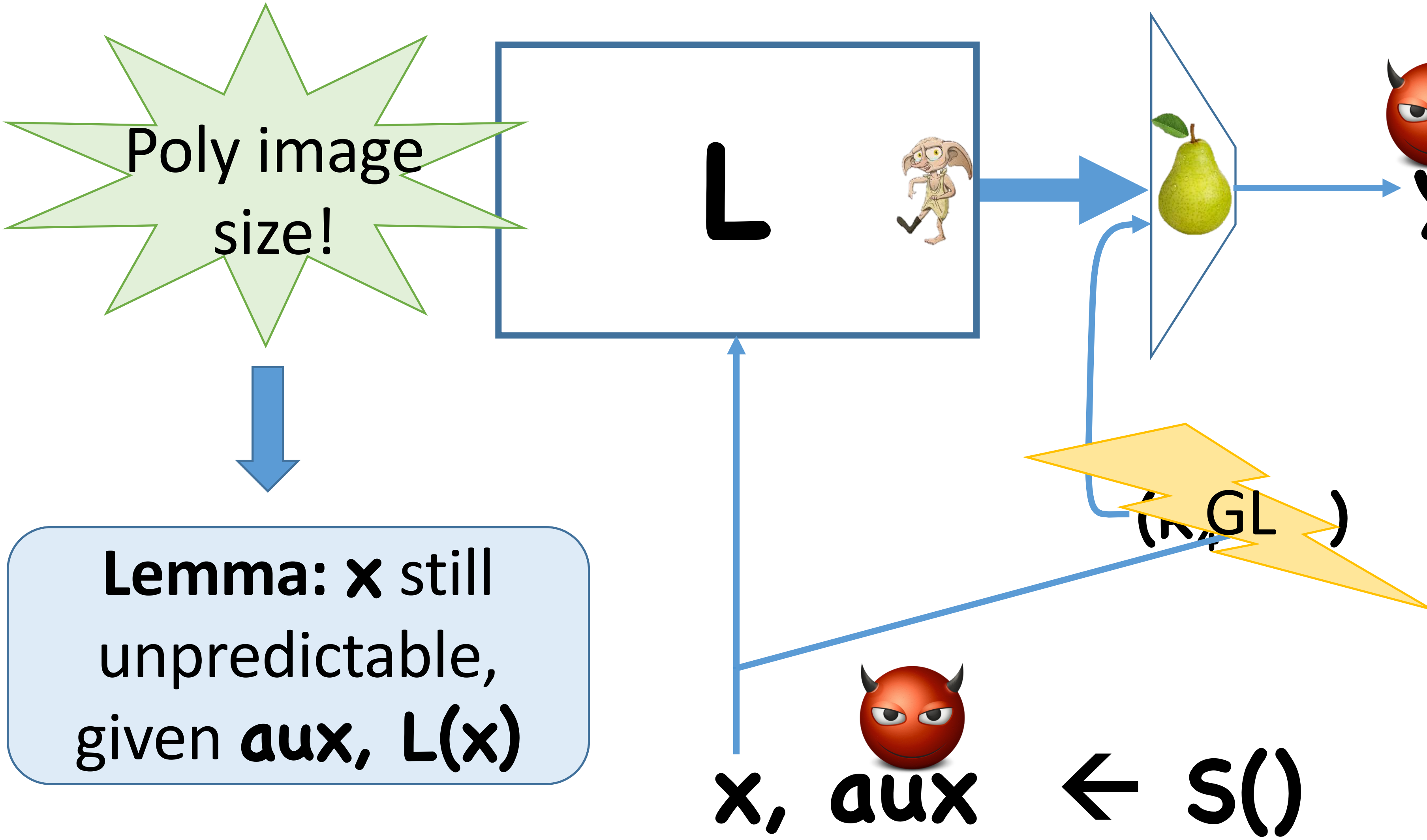
Step 2: Invoke Goldreich-Levin



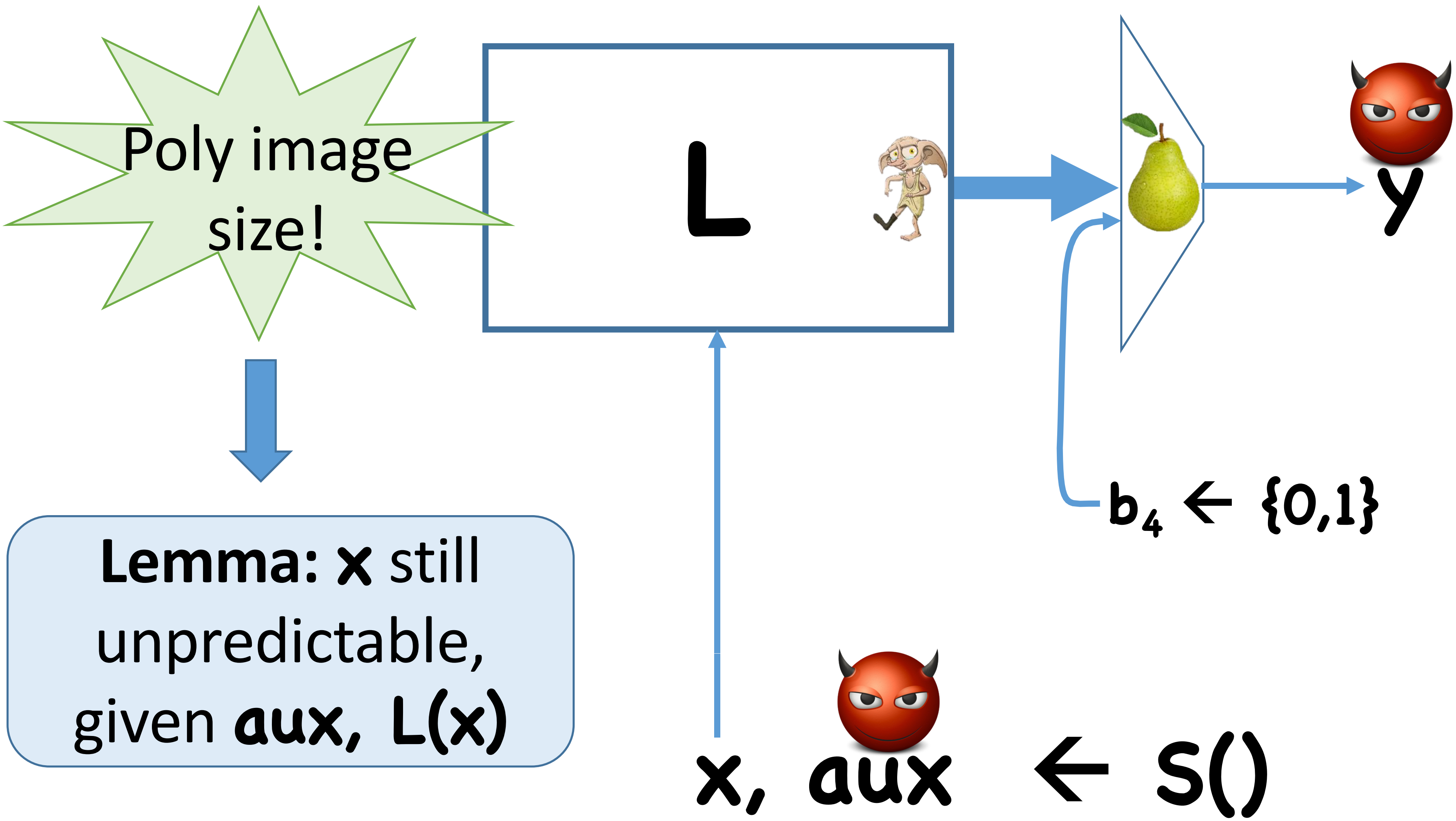
Step 2: Invoke Goldreich-Levin



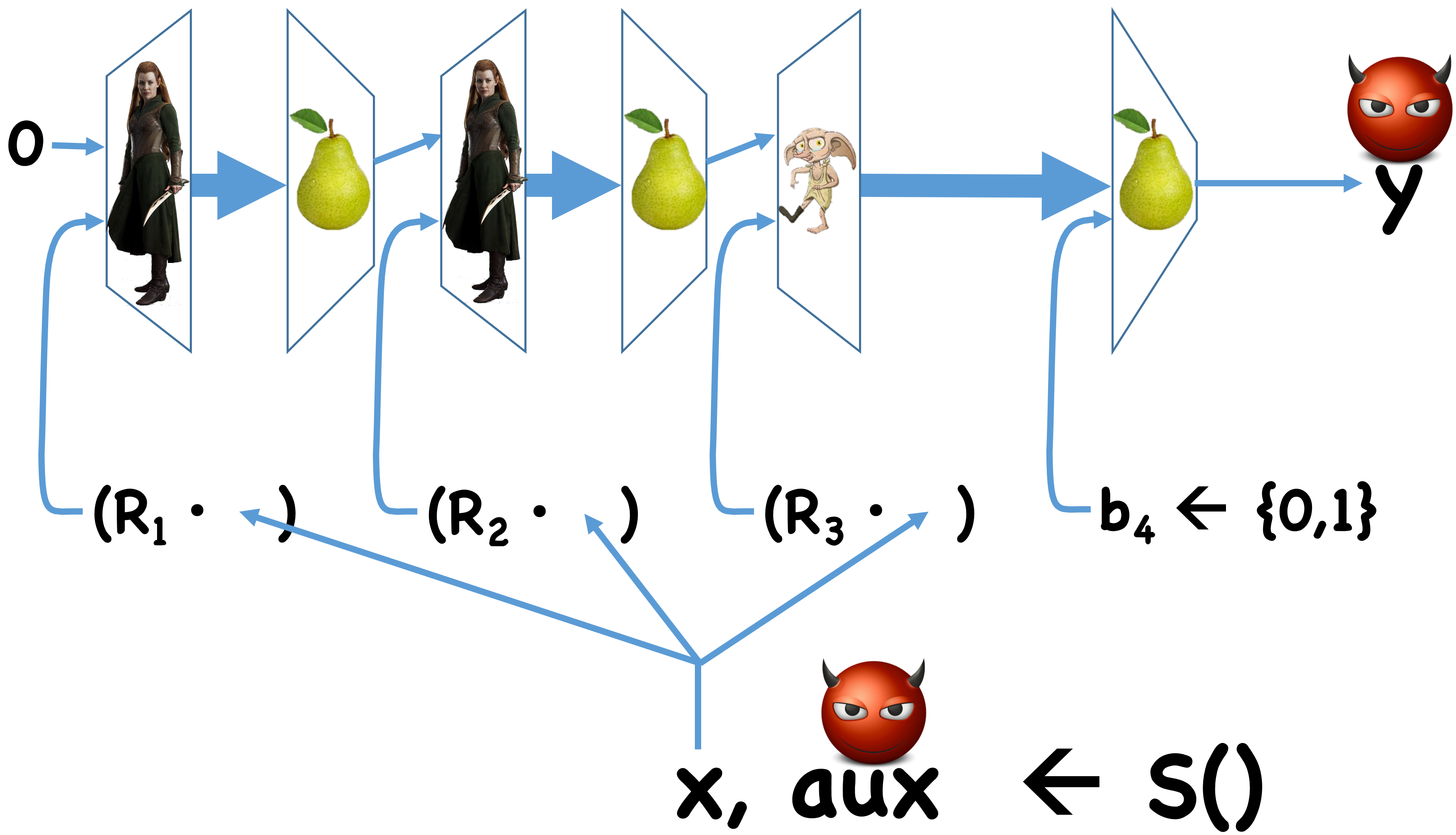
Step 2: Invoke Goldreich-Levin



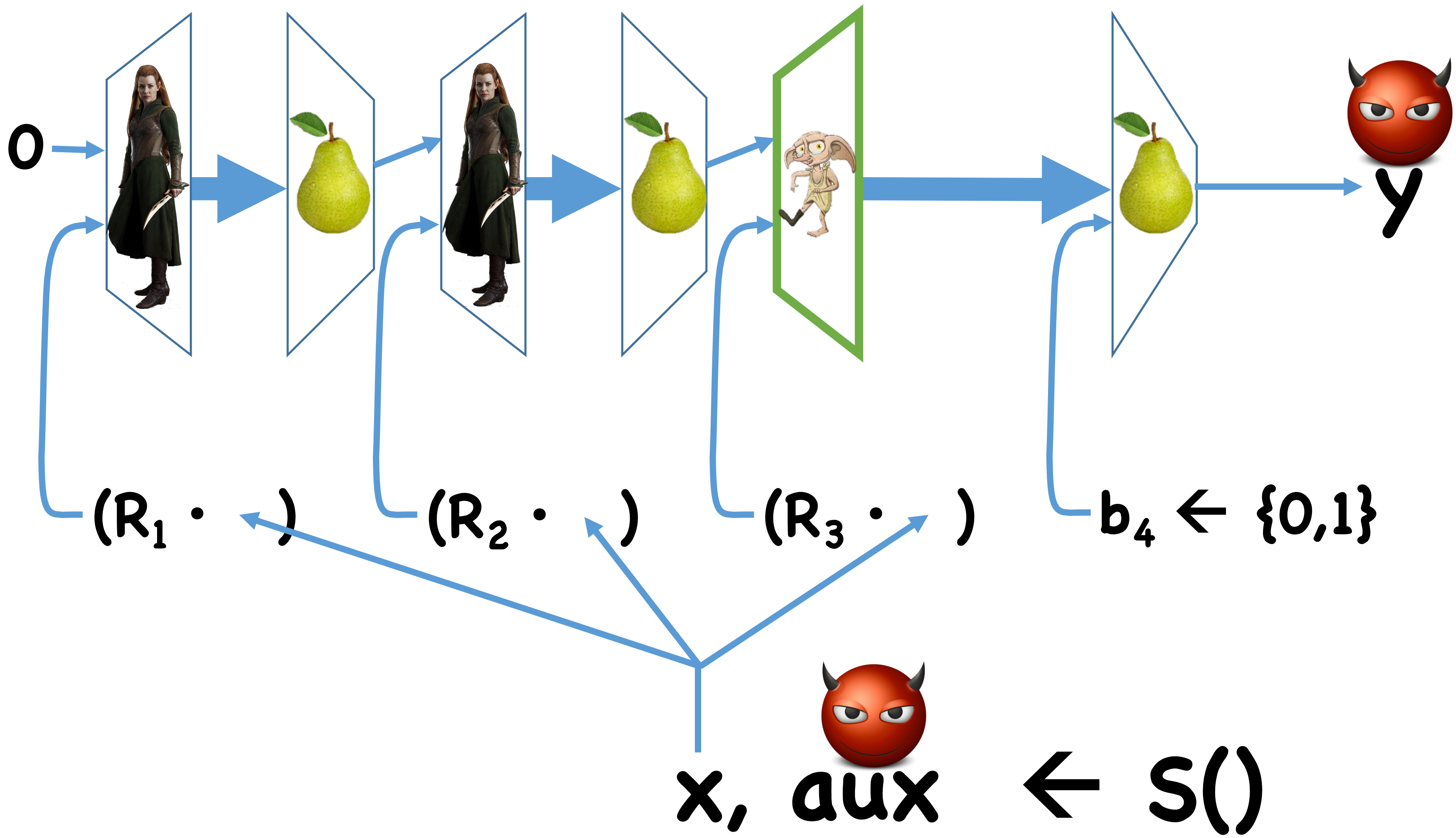
Step 2: Invoke Goldreich-Levin



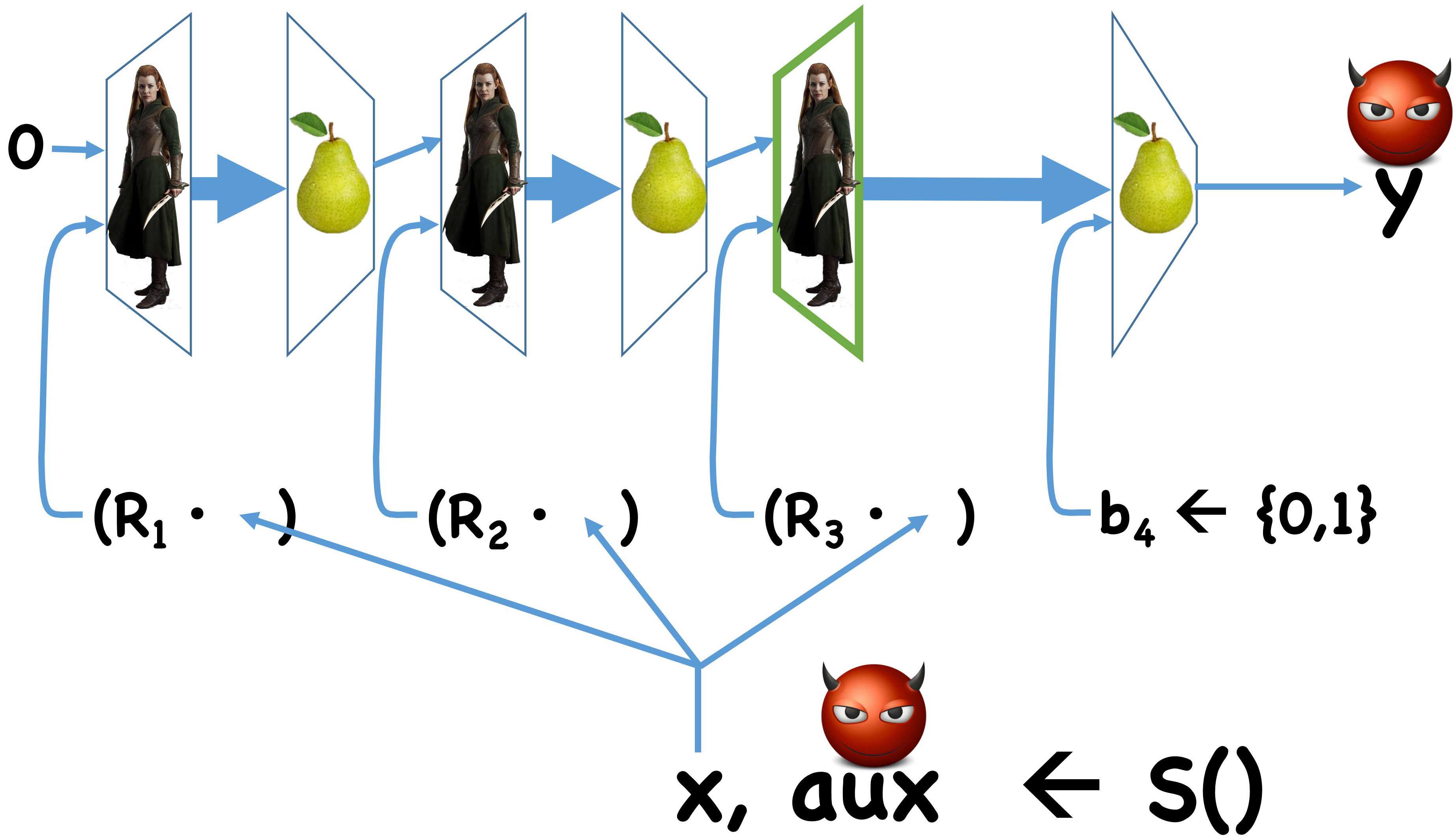
Step 2: Invoke Goldreich-Levin



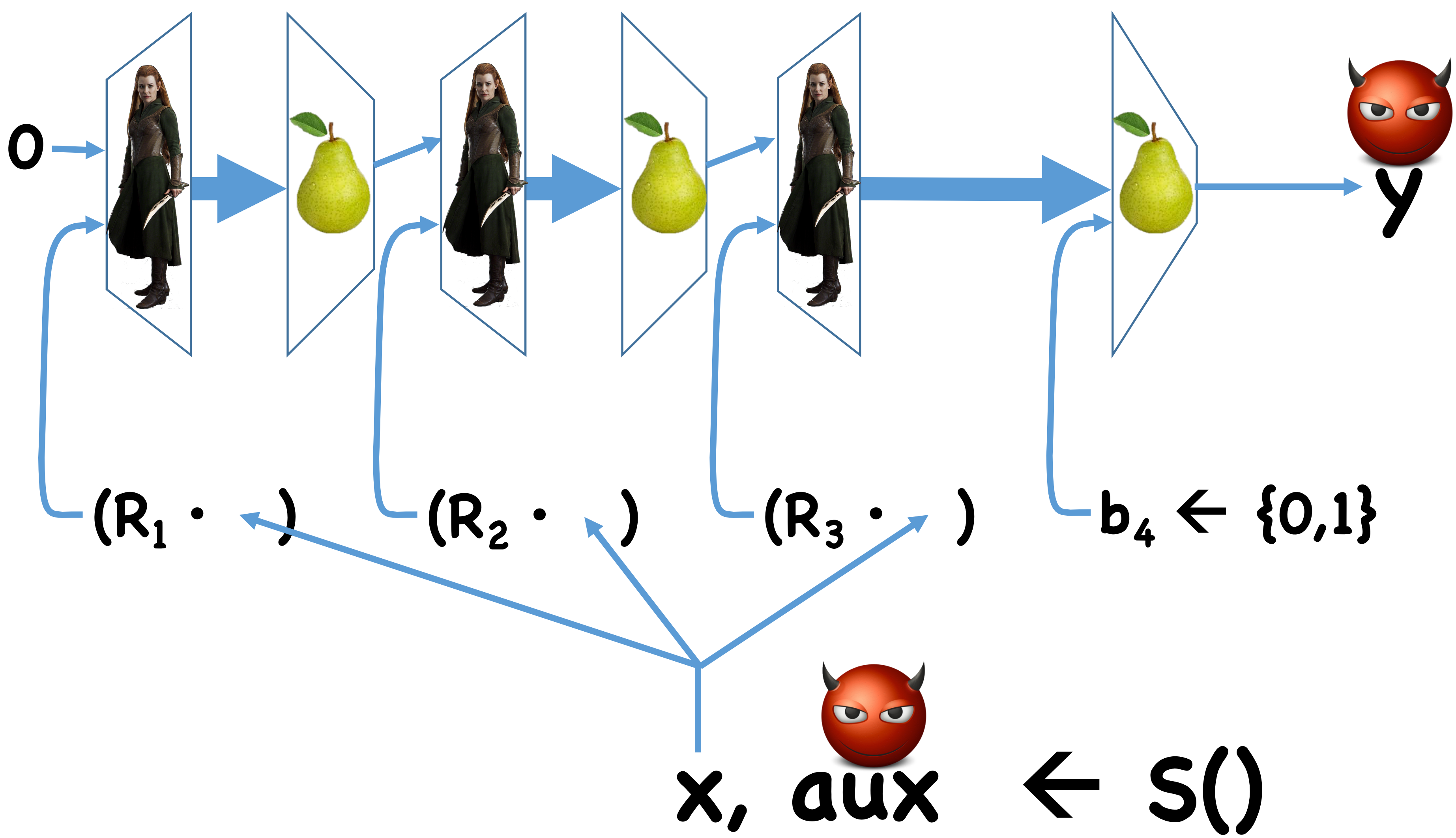
Step 3: Undo ELF Magic



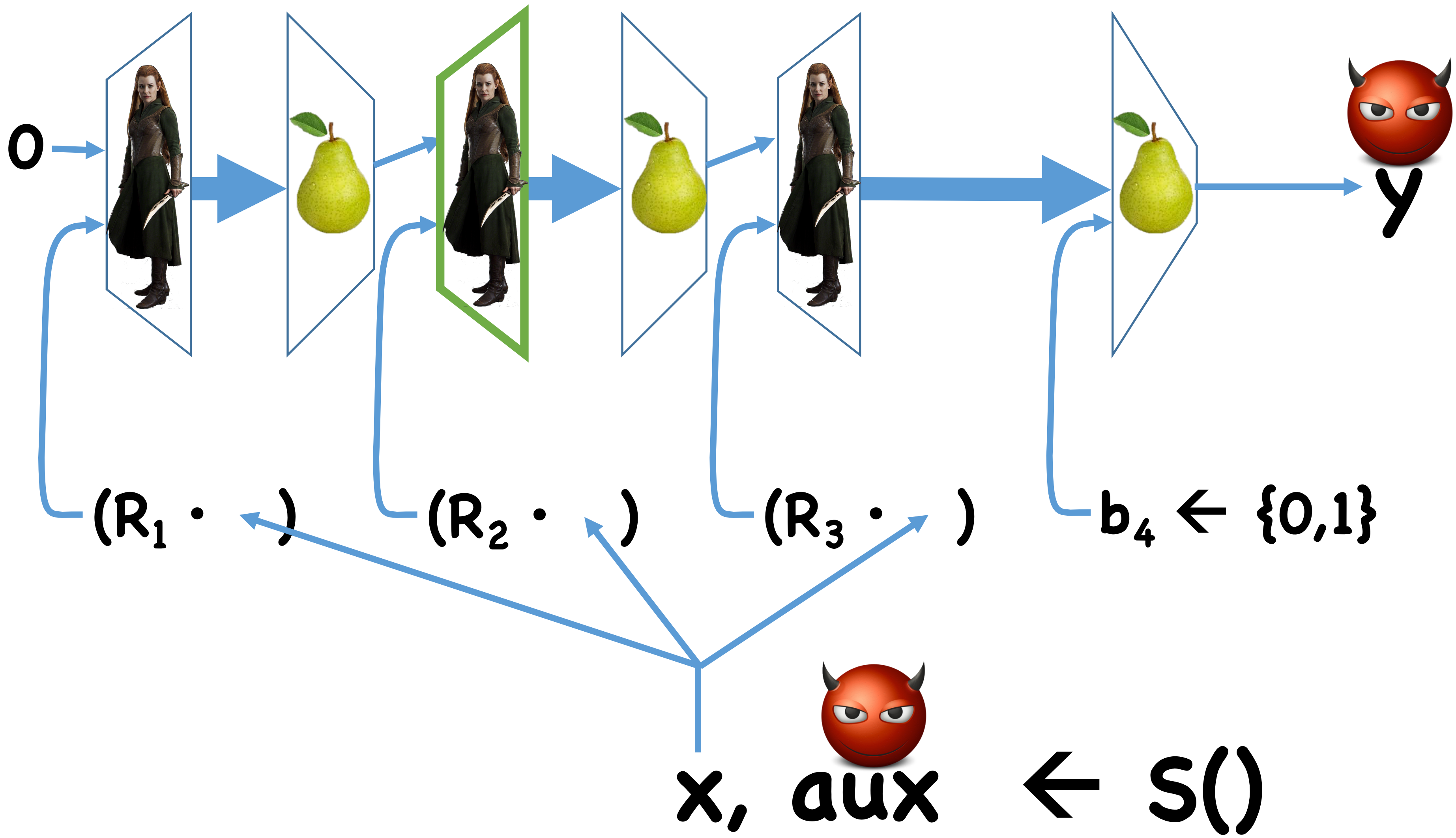
Step 3: Undo ELF Magic



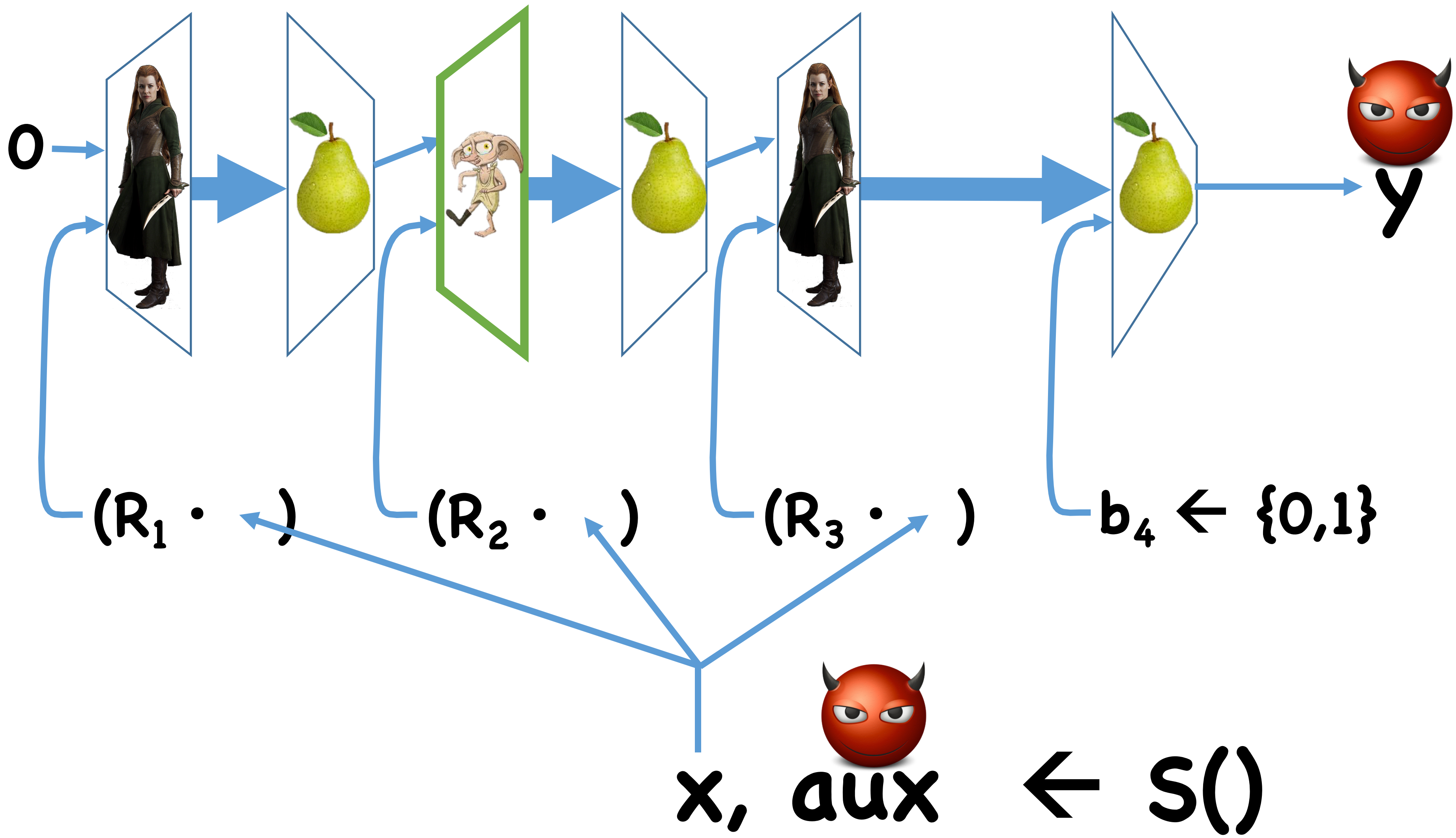
Step 4: Repeat



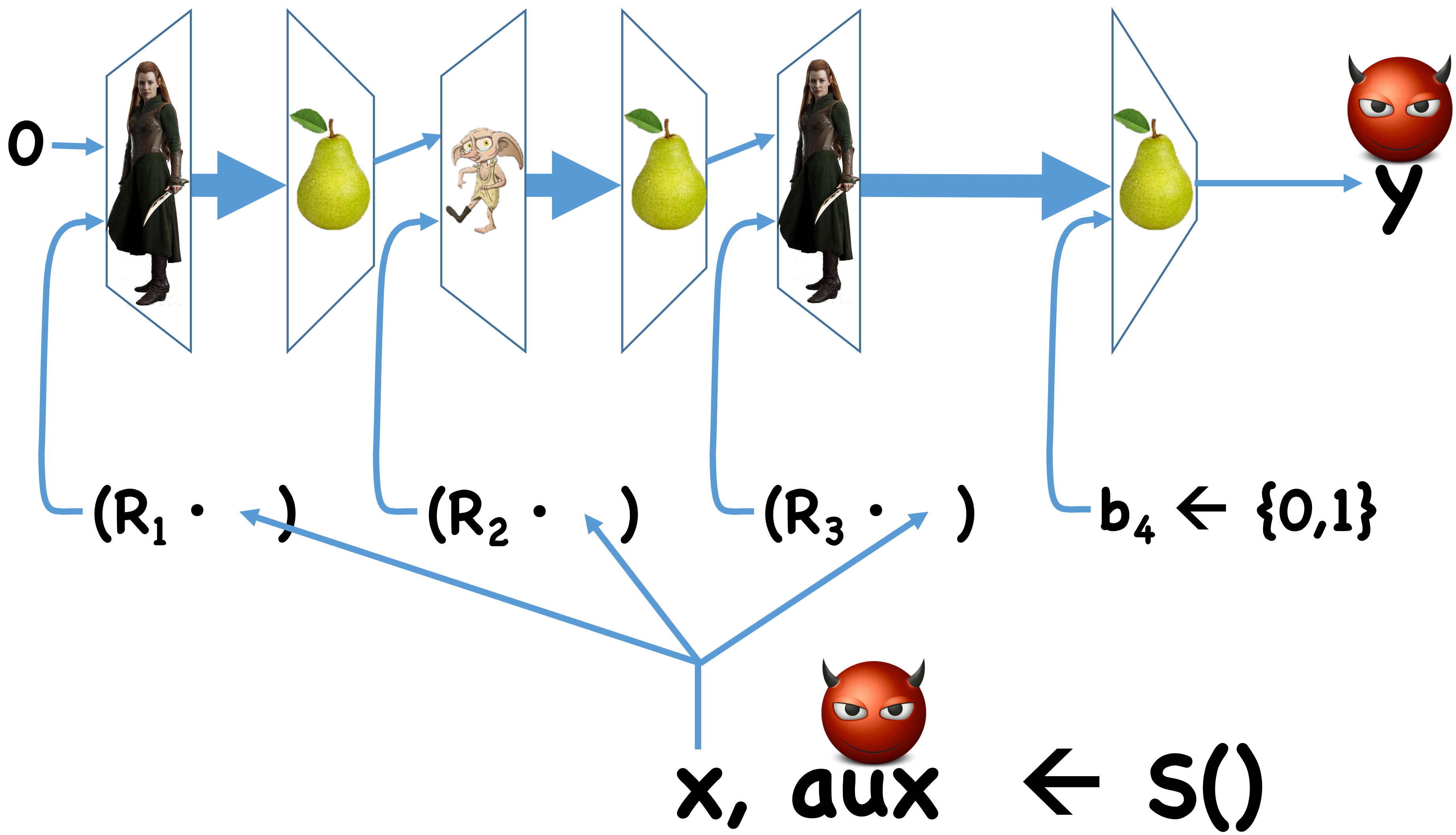
Step 4: Repeat



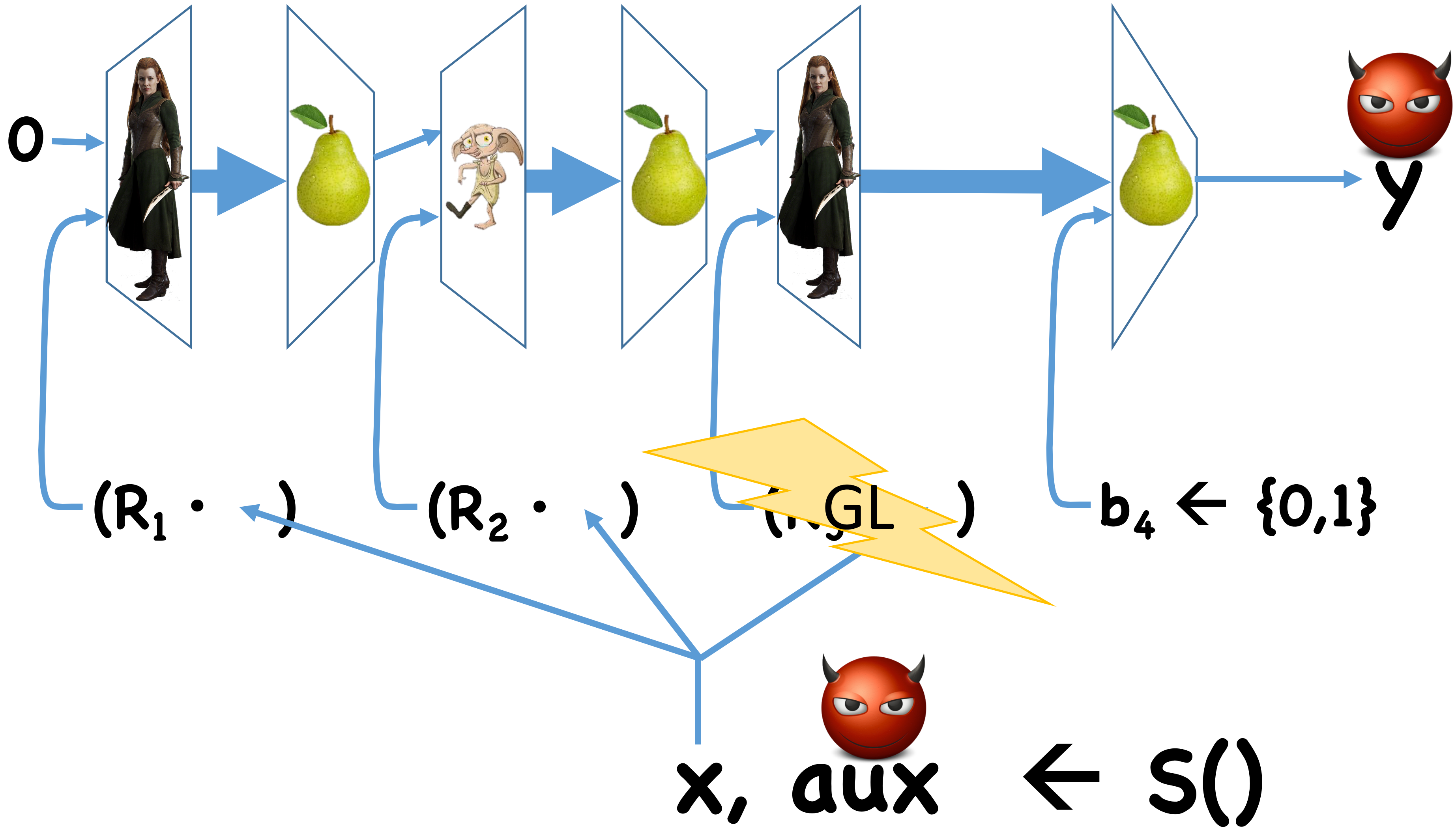
Step 4: Repeat



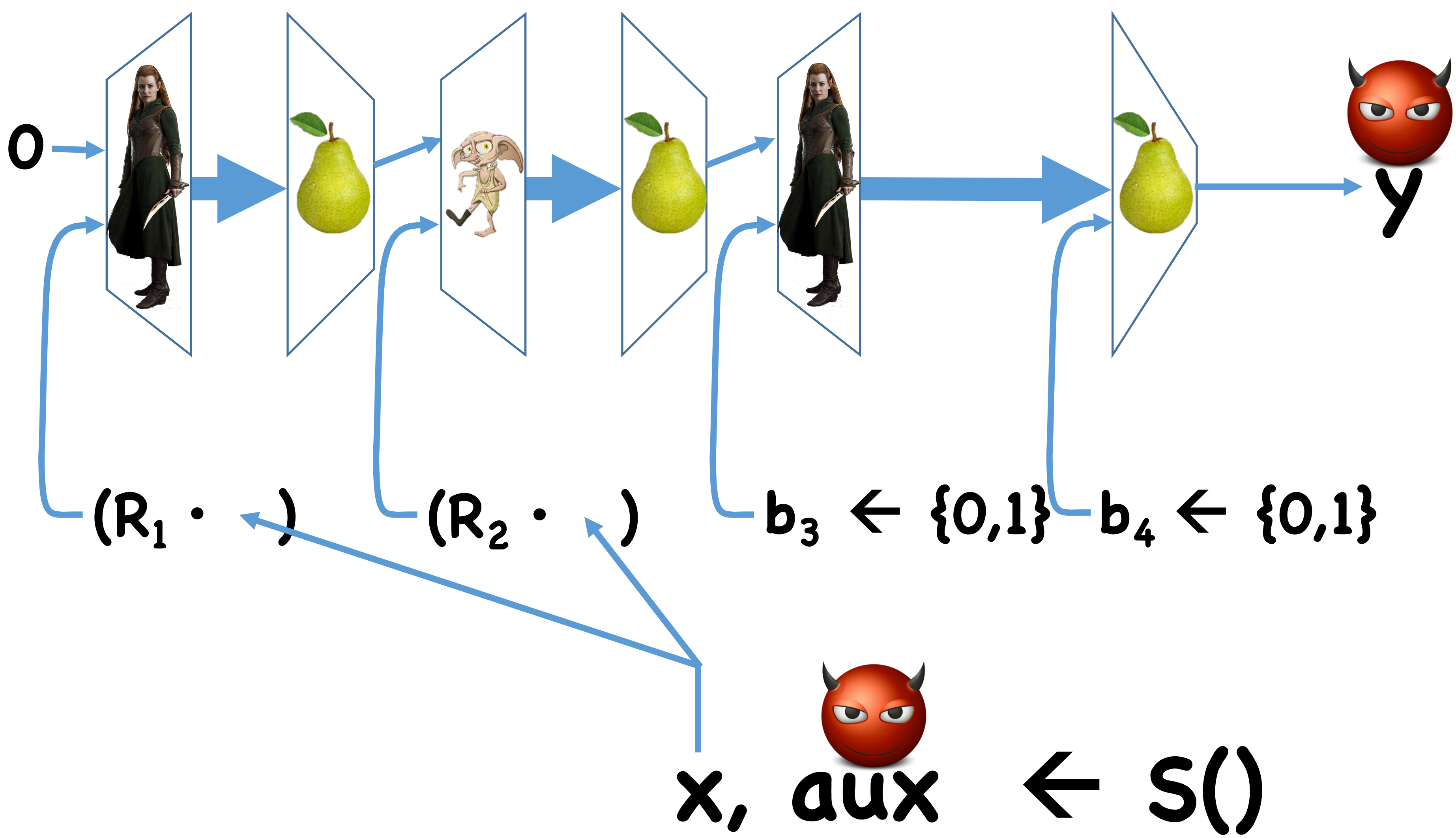
Step 4: Repeat



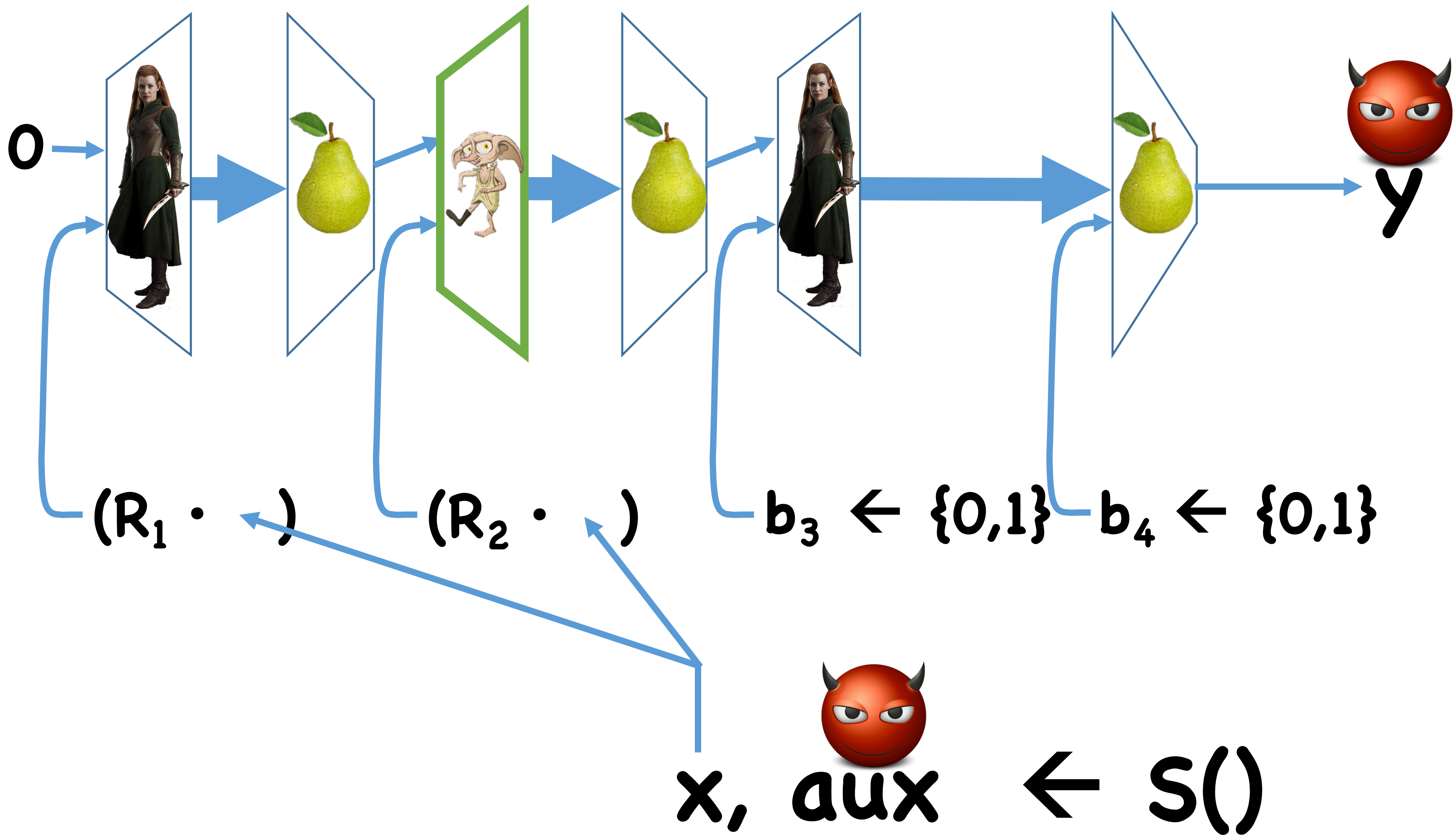
Step 4: Repeat



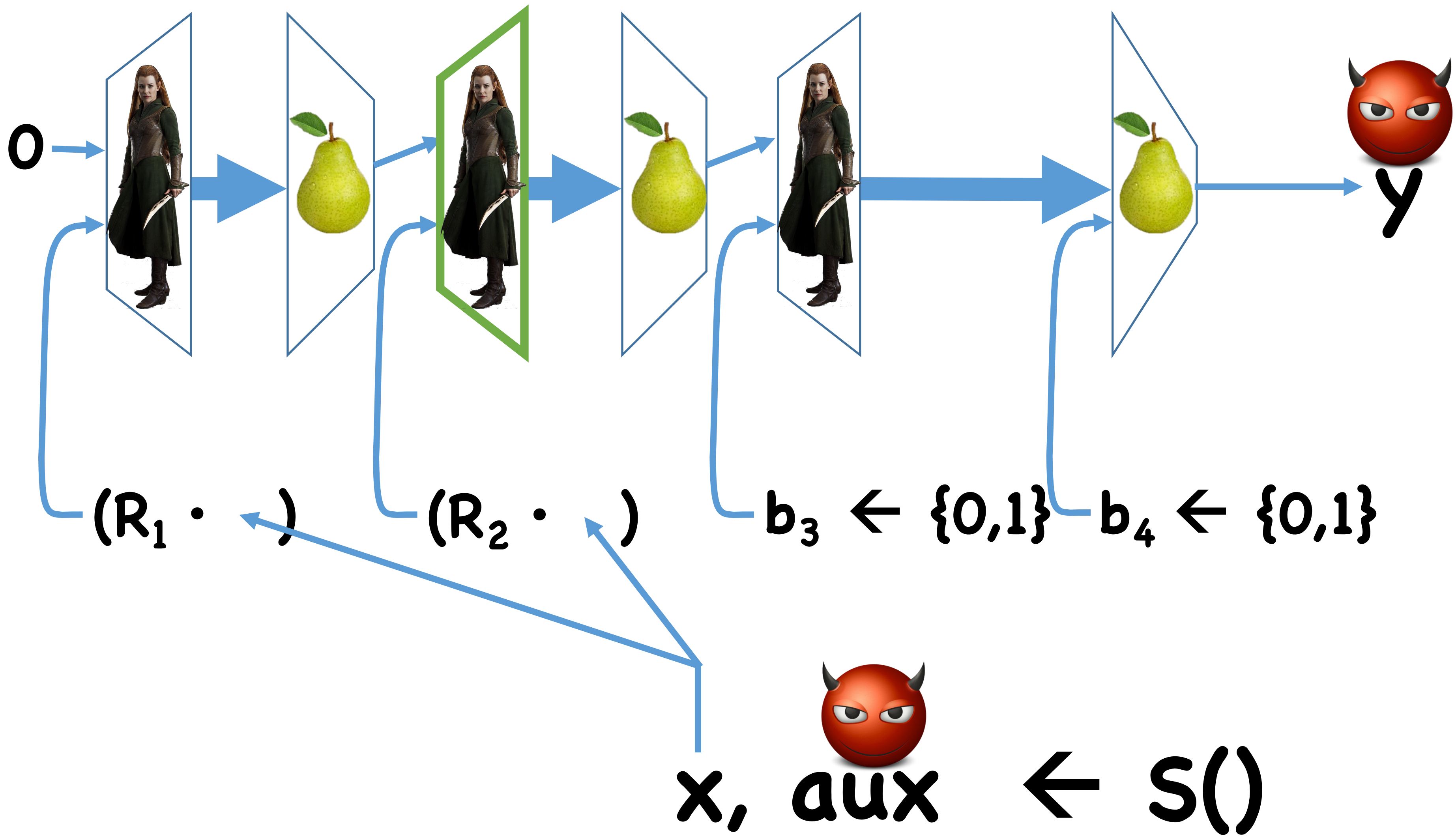
Step 4: Repeat



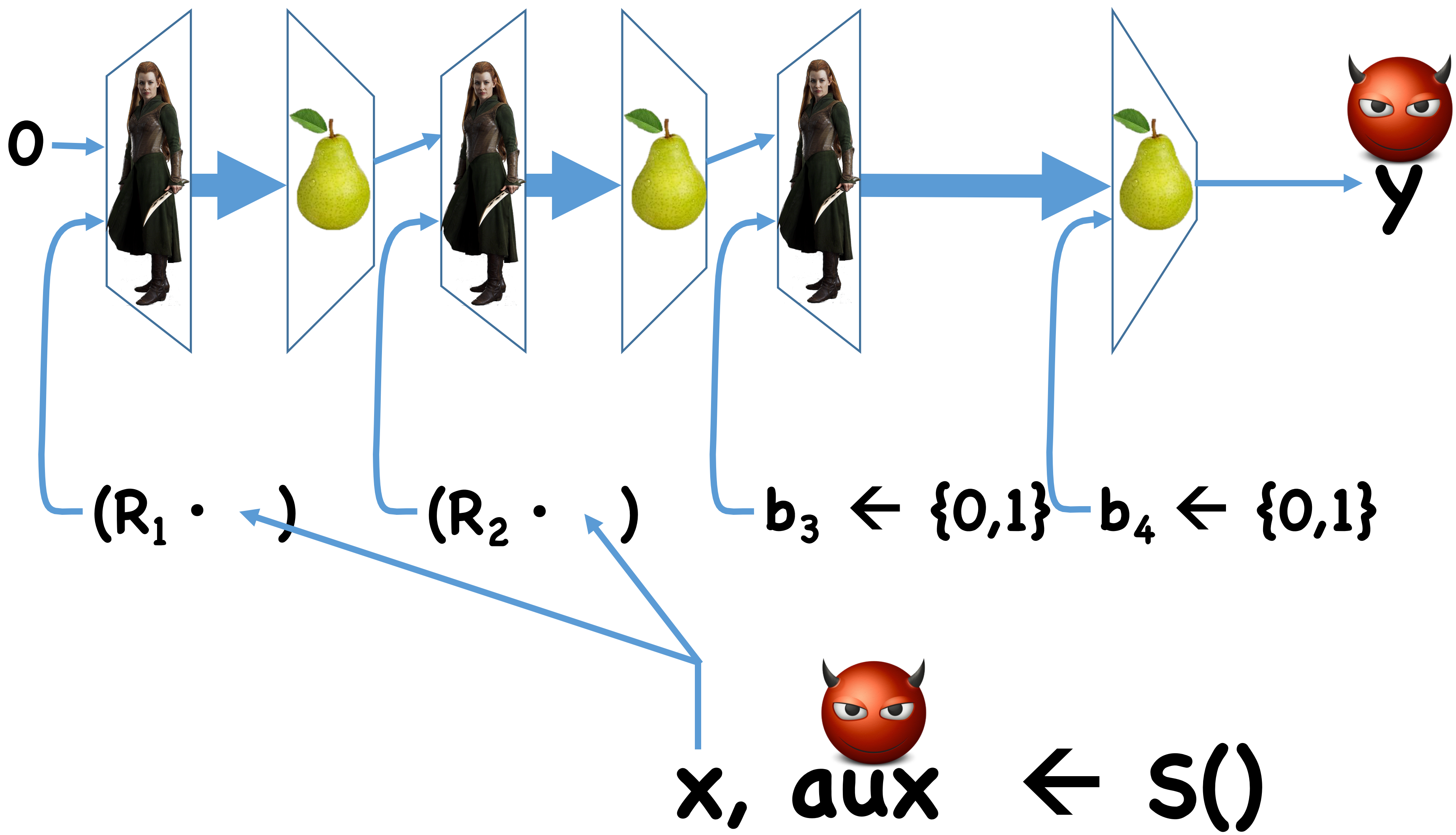
Step 4: Repeat



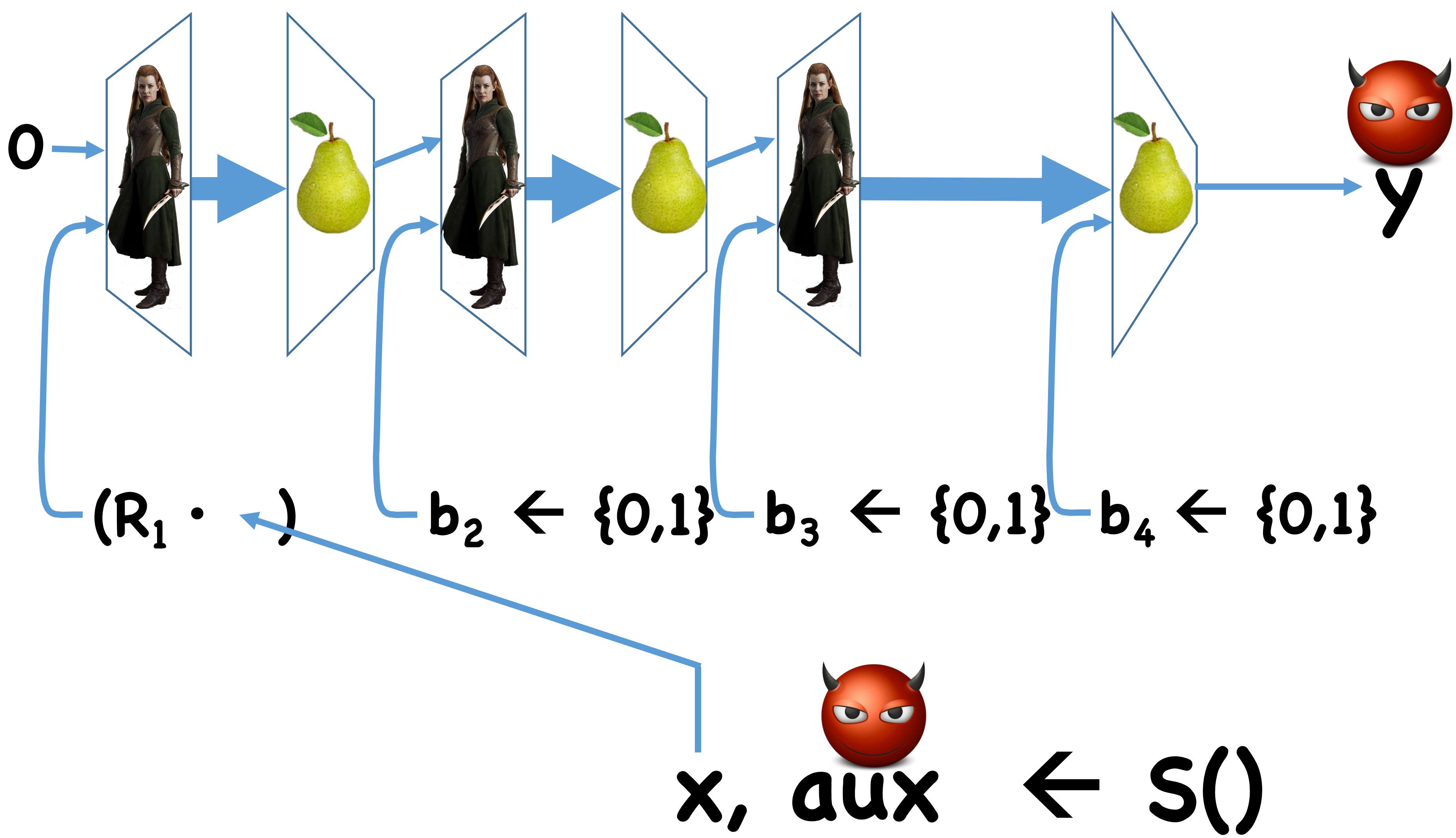
Step 4: Repeat



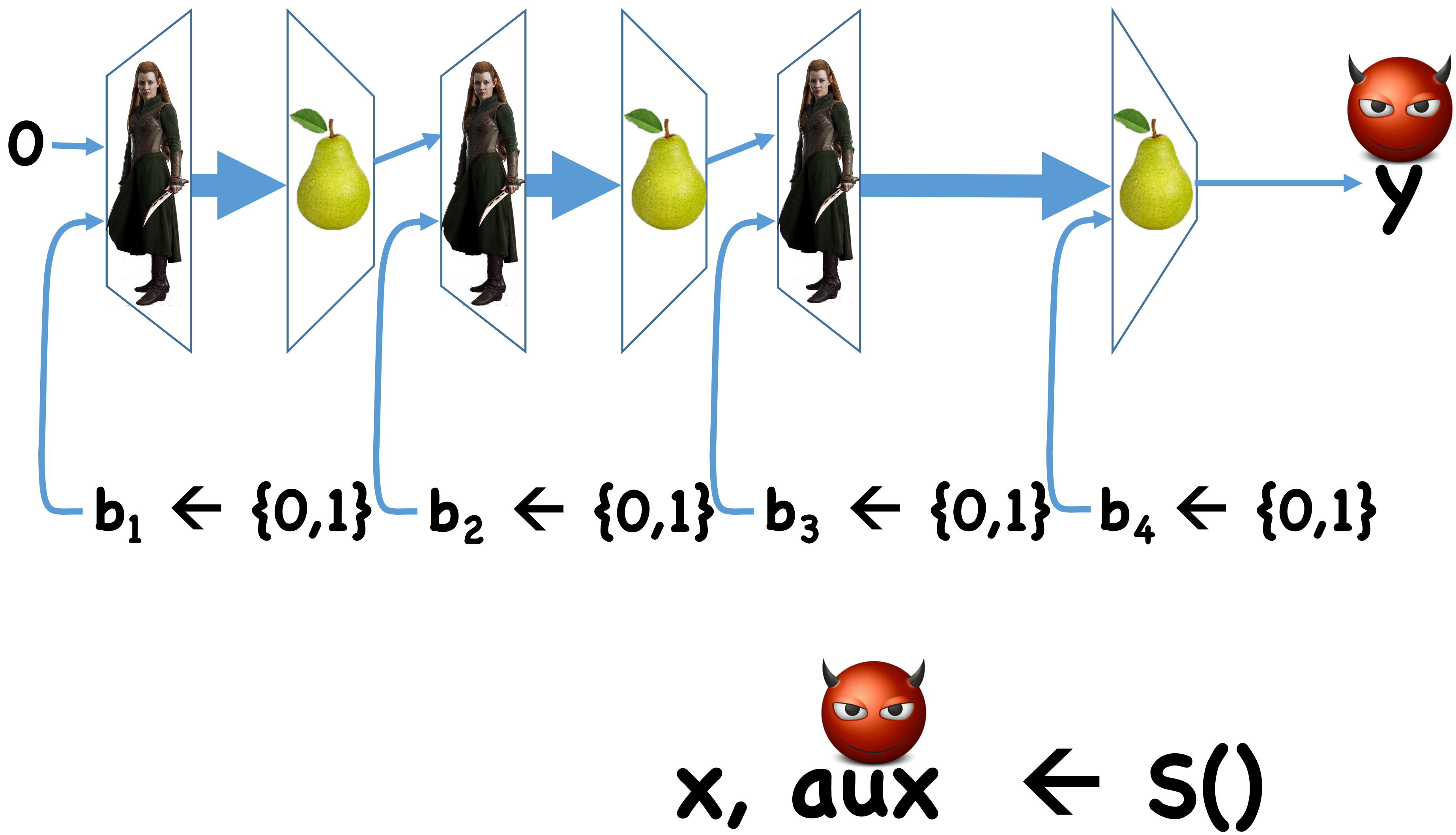
Step 4: Repeat



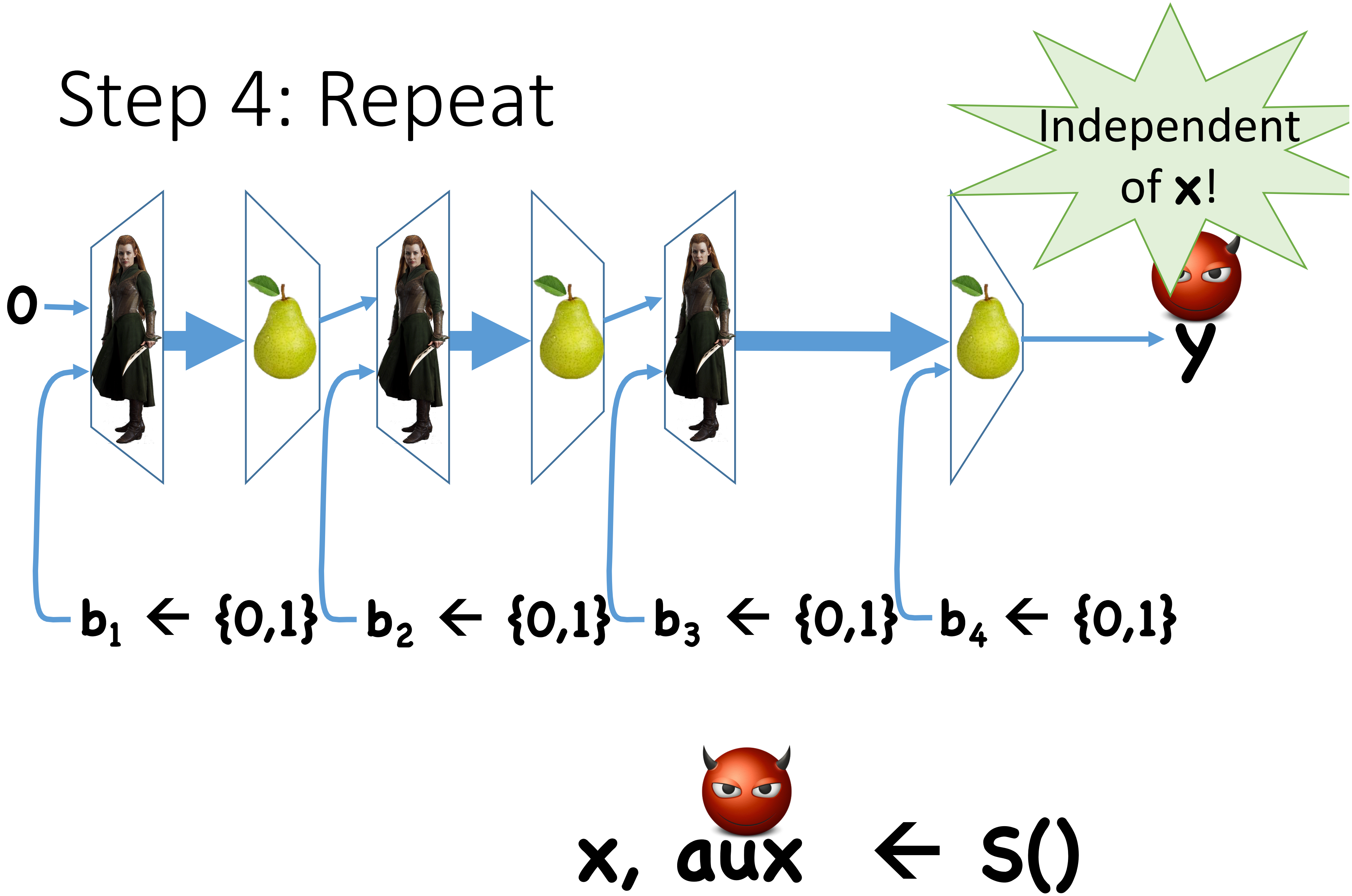
Step 4: Repeat



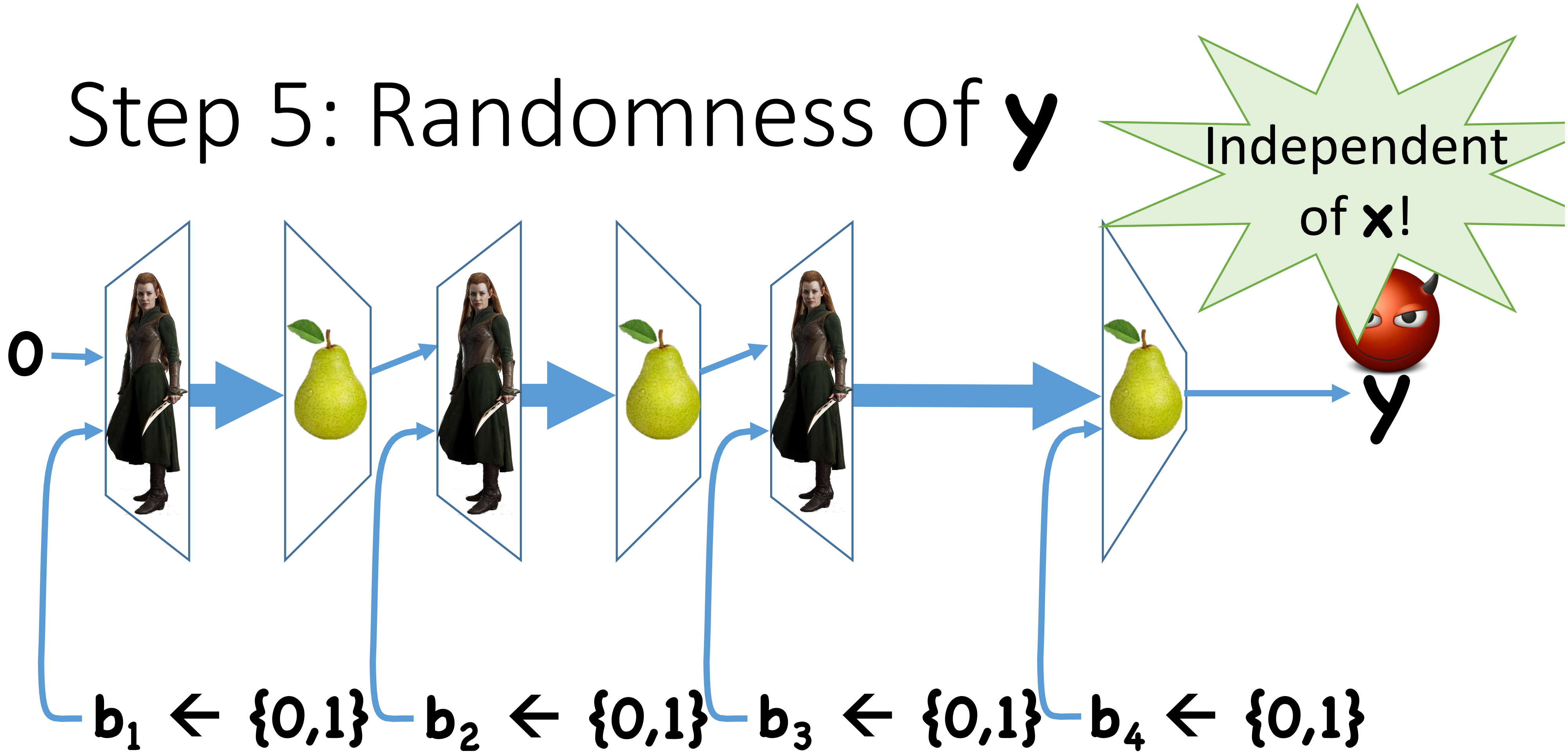
Step 4: Repeat



Step 4: Repeat



Step 5: Randomness of **y**



Lemma: If $\mathbf{b}_i$ are uniform, **y** is statistically close to random, given all the s and s (w.h.p.)

Theorem: For any computationally unpredictable **(x,aux)**,

$$(H,\ H(x),\ aux) \approx_c (H,\ random,\ aux)$$

Also:

Theorem: H is injective w.h.p.

Applications

- (Injective) one-way function satisfying [BP'11]
- Auxiliary Input Point Obfuscation (AIPO)

$$\mathbf{Obf(I_x) = H, H(x)}$$

- Poly-many hardcore bits for any computationally unpredictable source
- $\mathbf{Enc(m) = (\ TDP(r), H(r) \oplus m\ )}$ is CPA secure

Applications

- (Injective) one-way function satisfying [BP'11]

Previous constructions:

- Tautological assumption [BP'11]
  - Assumption "family"
- Canetti's strong variant of DDH [Can'97]
  - Assumption "family"
  - Incompatible with certain forms of obfuscation [BST'15]

- Enc(m) = (TDP(r), H(r) $\oplus$ m) is CPA secure

Applications

- (Injective) one-way function satisfying [BP'11]

- Auxiliary Input Point Obfuscation (AIPO)

$$\mathbf{Obf(I_x) = H,\ H(x)}$$

Previous constructions:

- Canetti's strong variant of DDH [Can'97]
- [BP'11]-one-way *permutations*

  (our **H** is not a permutation)

Applications

Previous constructions:

- UCE's [BHK'13]
  - "Tautological" assumption "family"
- Differing inputs obfuscation [BST'14] or extractable witness PRFs [Zha'14]
  - Only for OWF (for injective OWF, can use iO)
  - Assumption "family"
  - Believed to implausible in general [GGHW'14]
  - Extraordinarily inefficient

- Poly-many hardcore bits for any computationally unpredictable source

- **Enc(m) = (TDP(r), H(r) $\oplus$ m)** is CPA secure

Applications

- (Injective) one-way function satisfying [BP'11]
- Auxiliary Input Point Obfuscation (AIPO)

$$\mathbf{Obf}(I_x) = H, H(x)$$

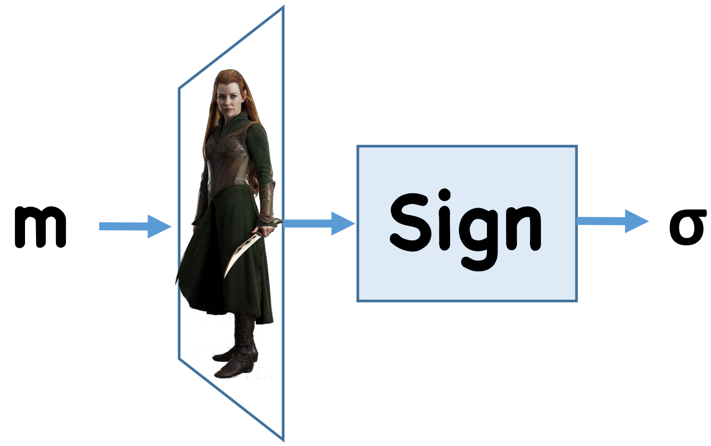
- Poly-many hardcore bits for any computationally

Follows from hardcore bits for injective OWF

- $\mathbf{Enc}(m) = (\ \mathbf{TDP}(r), \mathbf{H}(r) \oplus \mathbf{m}\ )$ is CPA secure

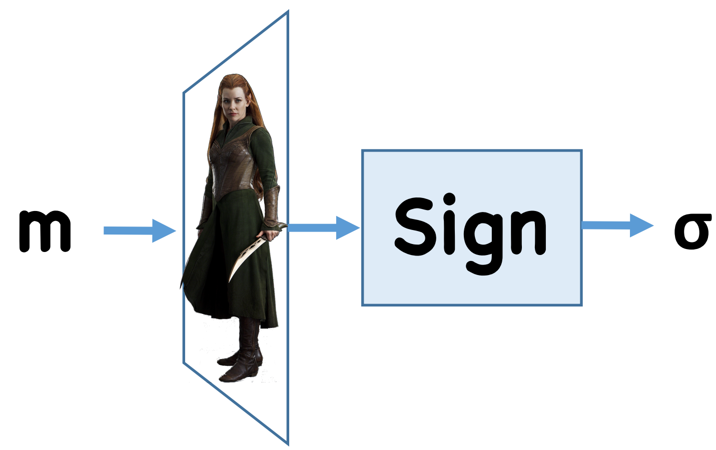
Other Results

- Selective to Adaptive security in Sigs/IBE

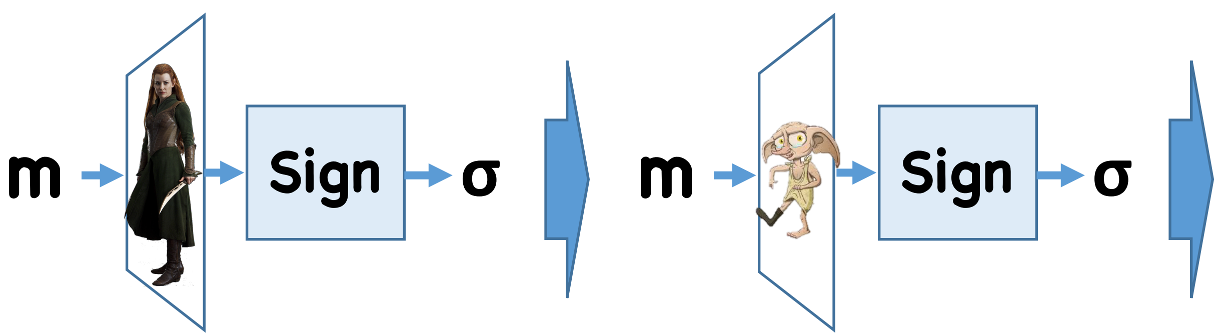


Other Results

- Selective to Adaptive security in Sigs/IBE



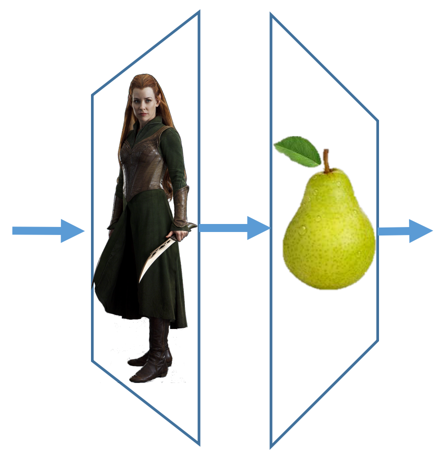
Proof:



Guess  **(m)**, incur poly loss

Other Results

- *Output intractable hash functions* (captures using hash functions to generate crs's)



- For proofs and more results, see paper

Conclusion

This work:

Exponential DDH

Interesting Applications

Open questions:

- ELFs from other assumptions
- Post-quantum ELFs
- More applications

Conclusion

This work:

Exponential DDH

Interesting Applications

Open questions:

- ELFs from other assumptions
- Post-quantum ELFs
- More applications

Thanks!