Cosmic Security

Benjamin Chan

Joint work with Cody Freitag & Rafael Pass

Cornell Tech

Reading Group, TAU. 12/16/2021

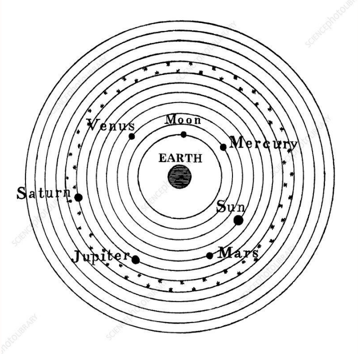
The Duality of Progress

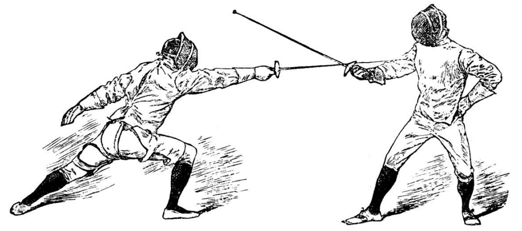
To Know the Unknown

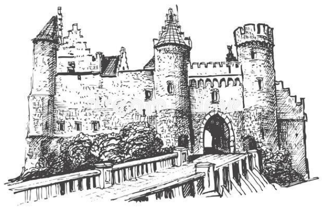
The desire to model the world, to build a *Theory of Everything*, so that we can know everything.

A World of Uncertainty

Acknowledgement of the *Unknown*, so that we can prepare for (and survive) the unknown tribulations of the cosmos.







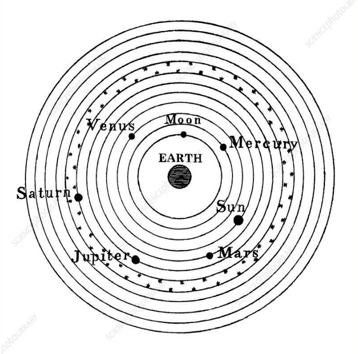
Cryptography Embraces the Unknown

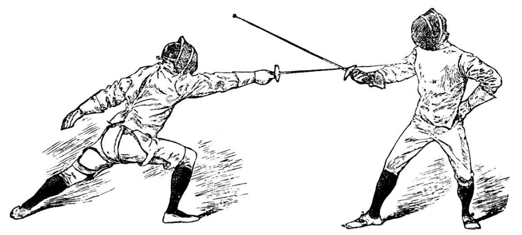
To Know the Unknown

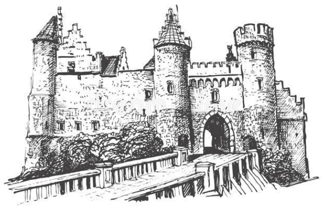
The desire to model the world, to build a *Theory of Everything*, so that we can know everything.

A World of Uncertainty

We want to build protocols that are secure against *any real-life attacker*, no matter when, where, or how (assuming computational hardness.)

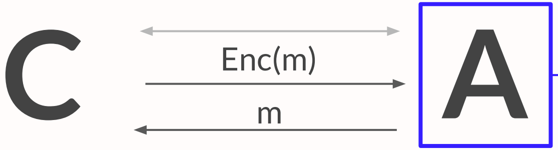






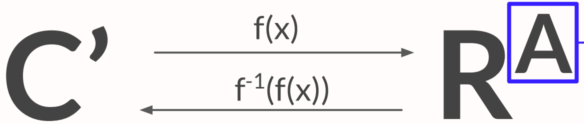
Reduction-Based Computational Security

Suppose **A** wins a *security game* **C** (e.g. breaking an encryption scheme):



Embraces the Unknown: Allows for any black-box attacker!

Then **R**$^{\mathbf{A}}$ breaks **C'** (e.g. inverting a OWF)



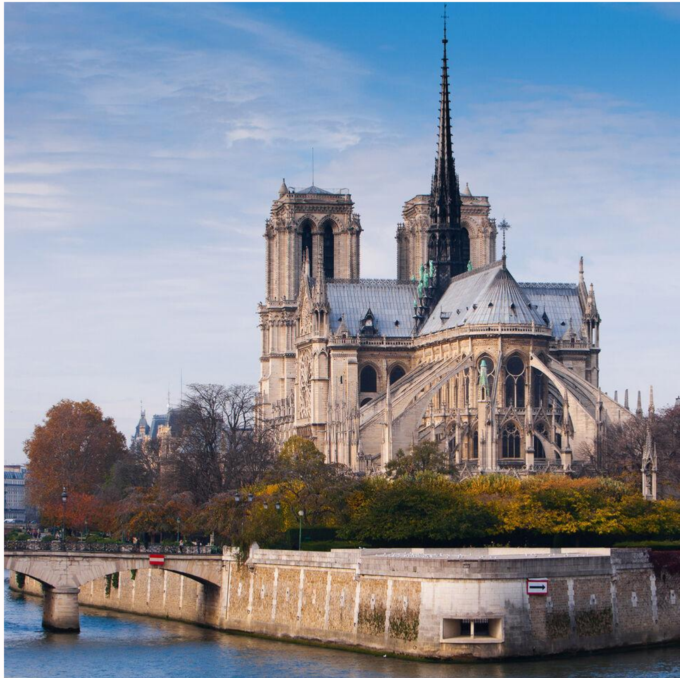
Classically, R can rewind or restart the attacker.

Contradiction! (assuming security of the OWF for **R**$^{\mathbf{A}}$.)

Embracing Uncertainty has done us remarkably well.

From OWFs, we can build,

- Hardcore Bits [GL89]
- Pseudorandom Generators [HILL99]
- Private-Key Encryption [GGM85+86]
- Commitment Schemes [Nao91]
- Digital Signatures [Lam79, Rom90, Mer90]
- Zero-Knowledge Proofs for all of NP [GMW86]

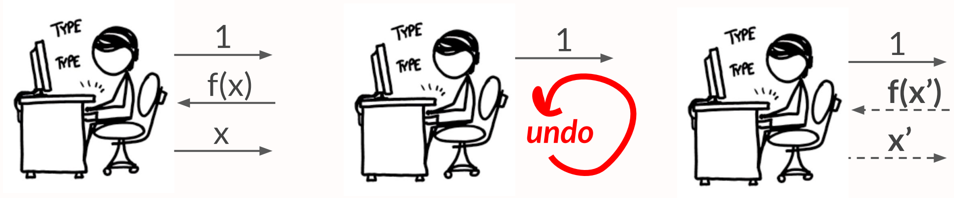


1980s: The Bizarre Nature of Quantum Computing

No-Cloning Theorem: can’t copy qubits without collapsing superposition.

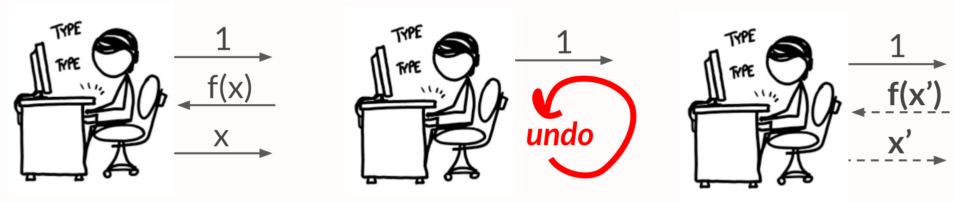
1980s: The Bizarre Nature of Quantum Computing

No-Cloning Theorem: can't copy qubits without collapsing superposition.



1980s: The Bizarre Nature of Quantum Computing

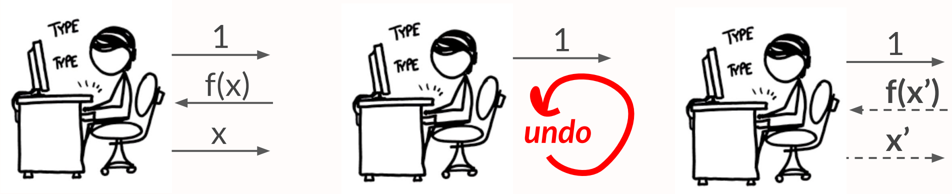
No-Cloning Theorem: can't copy qubits without collapsing superposition.



Can no longer reason about **Nature** as classical algorithm:
It is bizarrely stateful (Behavior changes on repeated invocations).

1980s: The Bizarre Nature of Quantum Computing

No-Cloning Theorem: can't copy qubits without collapsing superposition.



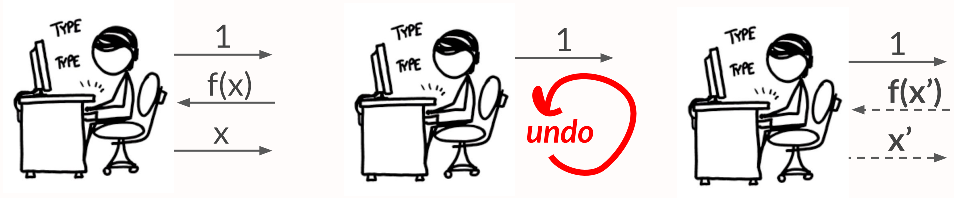
Can no longer reason about **Nature** as classical algorithm:
It is bizarrely stateful (Behavior changes on repeated invocations).

$$C' \underset{f^{-1}(f(x))}{\overset{f(x)}{\rightleftarrows}} R^{\boxed{A}}$$

Classically, R can just "rerun" A, where A is not stateful across runs

1980s: The Bizarre Nature of Quantum Computing

No-Cloning Theorem: can't copy qubits without collapsing superposition.



Can no longer reason about **Nature** as classical algorithm:
It is bizarrely stateful (Behavior changes on repeated invocations).

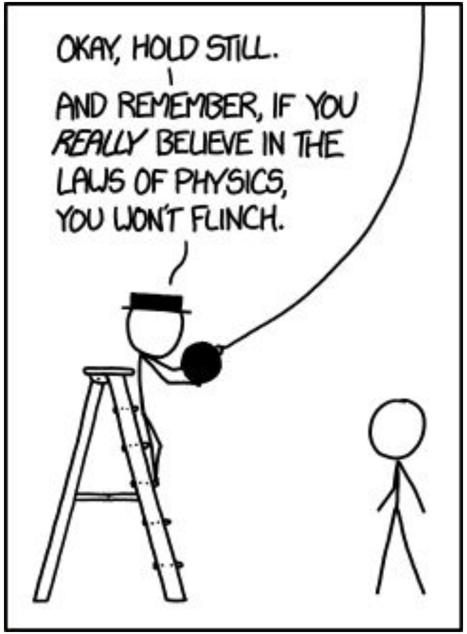
It isn't a stretch to imagine a fully stateful real world attacker...

Questioning Our Faith

Our world view is built on two implicit assumptions:

Extended Church Turing Hypothesis:
Real-life attackers are stateless, and (nu)PPT.

Quantum Extended Church Turing Hypothesis:
Real-life attackers are stateless, and (nu)QPT.

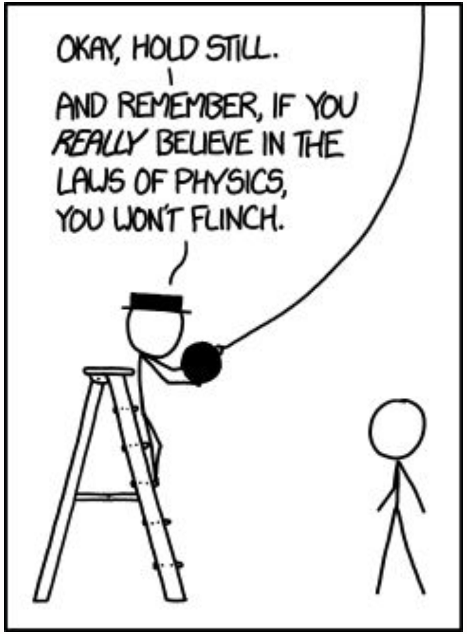


Questioning Our Faith

Our world view is built on two implicit assumptions:

Extended Church Turing Hypothesis:
Real-life attackers are stateless, and (nu)PPT.

Quantum Extended Church Turing Hypothesis:
Real-life attackers are stateless, and (nu)QPT.



These are religious, not scientific assumptions.

Popper's Falsifiability Test [Pop05]

"It must be possible for a scientific theory to be refuted by experience."

"It is easy to obtain confirmations for nearly every theory — if we look for confirmations."

"ALL MEN ARE MORTAL"

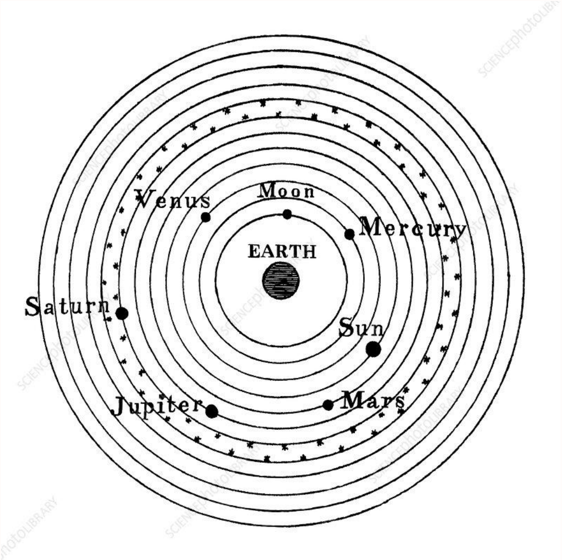
"Real Life Attackers Are Efficient Algorithms"

Thus, a scientific theory must be systematically falsifiable.

"ALL MEN ARE IMMORTAL"

The *Extended Church Turing Hypothesis* doesn't pass the test!

If Our Faith is Wrong… If Nature is Stateful...



It took 1400 years for humankind to develop the tools necessary to falsify geocentrism.

This talk:

Can we build a reduction-based
theory of cryptography
without making a *religious* assumption
on the properties of real-world attackers?

(acknowledging that unknown, that the world is vaster than we previously thought it to be,
and not just modeled by stateless algorithms?)

This talk:

Can we build a reduction-based
theory of cryptography
in the face of *newfound uncertainty*
about the Nature of real-world attackers?

(What if real-world attackers can change the way they play security games over time?)

Our work: Cosmic Security (Informal)

Suppose PPT **A** uses **Nat** to ‘break’ **C** (e.g. breaking an encryption scheme):

$$C \underset{m}{\overset{Enc(m)}{\rightleftarrows}} A \longleftrightarrow Nat$$

Can be stateful
Can be unbounded

Then ∃ PPT **A’** that uses **Nat** to ‘break’ **C’** (e.g. inverting a OWF)

$$C' \underset{f^{-1}(f(x))}{\overset{f(x)}{\rightleftarrows}} A' \longleftrightarrow Nat$$

A’ can no longer religiously rely on Nat behaving statelessly.

Contradiction! (assuming security of the OWF vs PPT+**Nat**)

Roadmap

1. ~~Motivation~~ *(10min)*
2. Defining Cosmic Security *(15min)*
3. Properties of Cosmic Security: a Sanity Check
   a. Composition, Black-box reductions *(5min)*
4. Summary of Key Results
   a. Feasibilities and Impossibilities (20*min*)
5. Other Notions of Cosmic Security (10min)
6. Conclusion (5min)

Roadmap

1. ~~Motivation~~ (*10min*)
2. **Defining Cosmic Security** **(*15min*)**
3. Properties of Cosmic Security: a Sanity Check
    a. Composition, Black-box reductions (*5min*)
4. Summary of Key Results
    a. Feasibilities and Impossibilities (20*min*)
5. Other Notions of Cosmic Security (10min)
6. Conclusion (5min)

Defining Cosmic Security

$$\underbrace{\mathbf{A} \leftrightarrow \mathbf{Nat}}_{\text{“Cosmic Adversary” (A, Nat)}}$$

“Attacker”
uniform **PPT**

“Nature”
nonuniform **any choice of runtime**
Stateful!

“Cosmic Adversary” (A, Nat)

Cosmic Adversaries

A ⟷ Nat

"Attacker"
uniform **PPT**

"Nature"
nonuniform **any choice of runtime**
Stateful

"Cosmic Adversary" (A, Nat)

to capture our uncertainty
regarding the
"Power of Nature"

A classic attacker
that uses Nature
to break some scheme

Cosmic Security Game

C $\leftrightarrow$ **A** $\leftrightarrow$ **Nat**

"Challenger"
uniform **PPT**
outputs "win"/"lose"

"Attacker"
uniform **PPT**

"Nature"
nonuniform **any choice of runtime**
Stateful

"Cosmic Adversary" (A, Nat)

***Observe*: the attacker can alter the state of Nature during the interaction.**
This is intentional and a key property of our definition.

Nature can be invoked many times, “*statefully*”

time

WIN.	C ⟷ A ⟷
LOSE.	C ⟷ A ⟷
LOSE.	C ⟷ A ⟷
LOSE.	C ⟷ A ⟷
LOSE.	C ⟷ A ⟷

Useful adversaries win repeatedly.

No point in inverting a OWF only once.

time

WIN. $C \leftrightarrow A$

WIN. $C \leftrightarrow A$

WIN. $C \leftrightarrow A$

WIN. $C \leftrightarrow A$

WIN. $C \leftrightarrow A$

Classically, we always have the option of re-running A from scratch, with independent coins.

We consider only (**A**, **Nat**) that
“wins repeatedly” over time.

time

WIN. C ↔ A ↔

WIN. C ↔ A ↔

WIN. C ↔ A ↔

WIN. C ↔ A ↔

It doesn’t matter that Nat is “stateful” if it only wins once.

robust winning

time

the past

$\longleftrightarrow$

42

$\longleftrightarrow$

C $\longleftrightarrow$ A $\longleftrightarrow$

C $\longleftrightarrow$ A $\longleftrightarrow$

WIN. C $\longleftrightarrow$ A $\longleftrightarrow$ Nat

(**A**, **Nat**) wins for **C** regardless of any interactions that **Nat** had in the past!

robust winning

$\longleftrightarrow$

42

$\longleftrightarrow$

the past

ρ

C $\longleftrightarrow$ A $\longleftrightarrow$

C $\longleftrightarrow$ A $\longleftrightarrow$

WIN. C $\longleftrightarrow$ A $\longleftrightarrow$ Nat(ρ)

Interaction prefix ρ: a transcript of messages previously sent to Nat before the beginning of execution, including coins flipped by Nat.

(**A**, **Nat**) wins for **C** regardless of any interactions that **Nat** had in the past!

robust winning

$\longleftrightarrow$

$\overset{42}{\longleftrightarrow}$

C $\longleftrightarrow$ A $\longleftrightarrow$

C $\longleftrightarrow$ A $\longleftrightarrow$

the past

ρ

WIN. C $\longleftrightarrow$ A $\longleftrightarrow$ Nat(ρ)

Interaction prefix ρ: a transcript of messages previously sent to Nat before the beginning of execution, including coins flipped by Nat.

Definition: (A, Nat) has **robust advantage a(.)** for C, if ∀ *interaction prefixes* ρ, ∀ λ: Pr[(**A**, **Nat**(ρ)) wins **C**] ≥ a(λ)

robust winning

42

the past

ρ

$C \leftrightarrow A \leftrightarrow$

$C \leftrightarrow A \leftrightarrow$

WIN. $C \leftrightarrow A \leftrightarrow$ Nat(ρ)

Interaction prefix ρ: a transcript of messages previously sent to Nat before the beginning of execution, including coins flipped by Nat.

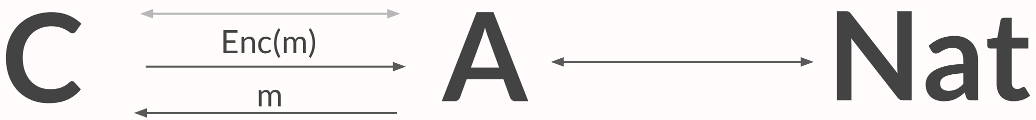
Definition: (A, Nat) has **robust advantage** a(.) for C, if ∀ *interaction prefixes* ρ, ∀ λ: Pr[(**A**, **Nat**(ρ)) wins **C**] ≥ a(λ)

A weak notion!
Can win in a different way for each prefix.

Cosmic Security (Final)

∃ an **ε-cosmic reduction** from **C** to **C'** if ∀ PPT **A**, ∃ PPT **A'** s.t. ∀**Nat**:

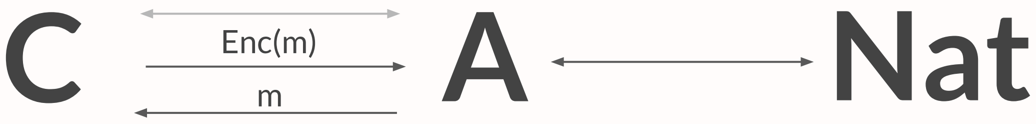
Suppose (**A**, **Nat**) has **robust advantage** a(·) for **C**



Cosmic Security (Final)

∃ an **ε-cosmic reduction** from **C** to **C'** if ∀ PPT **A**, ∃ PPT **A'** s.t. ∀**Nat**:

Suppose (**A**, **Nat**) has **robust advantage a(·)** for **C**

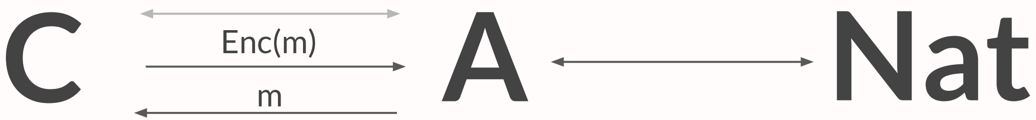


Then (**A'**, **Nat**) has **robust advantage ε(·,a(·))** for **C'**.

Cosmic Security (Final)

∃ an **ε-cosmic reduction** from **C** to **C'** if ∀ PPT **A**, ∃ PPT **A'** s.t. ∀**Nat**:

Suppose (**A**, **Nat**) has **robust advantage a(·)** for **C**



Then (**A'**, **Nat**) has **robust advantage ε(·,a(·))** for **C'**.

A' can now use the fact that (A, Nat) wins repeatedly.

Cosmic Security (Final)

∃ an **ε-cosmic reduction** from **C** to **C'** if ∀ PPT **A**, ∃ PPT **A'** s.t. ∀**Nat**:

Suppose (**A**, **Nat**) has **robust advantage a(·)** for **C**

$$\begin{tikzcd}[column sep=huge] \mathbf{C} \arrow[r, leftrightarrow, shift left=4] \arrow[r, shift left=1, "\mathrm{Enc}(m)"] & \mathbf{A} \arrow[l, shift left=1, "m"] \arrow[r, leftrightarrow] & \mathbf{Nat} \end{tikzcd}$$

Then (**A'**, **Nat**) has ~~**robust**~~ **advantage ε(·,a(·))** for **C'**.

A' can now use the fact that (A, Nat) wins repeatedly.

Equivalent definition!

$$\begin{tikzcd}[column sep=huge] \mathbf{C'} \arrow[r, shift left=1, "f(x)"] & \mathbf{A'} \arrow[l, shift left=1, "f^{-1}(f(x))"] \arrow[r, leftrightarrow] & \mathbf{Nat} \end{tikzcd}$$

Cosmic Security (Final)

∃ an **ε-cosmic reduction** from **C** to **C'** if ∀ PPT **A**, ∃ PPT **A'** s.t. ∀ **Nat**:

Suppose (**A**, **Nat**) has **robust advantage a(·)** for **C**

$$\mathbf{C} \;\underset{m}{\overset{\mathrm{Enc}(m)}{\rightleftarrows}}\; \mathbf{A} \longleftrightarrow \mathbf{Nat}$$

Then (**A'**, **Nat**) has ~~robust~~ **advantage ε(·,a(·))** for **C'**.

Equivalent definition!

A' can now use the fact that (A, Nat) wins repeatedly.

$$\mathbf{C'} \;\underset{f^{-1}(f(x))}{\overset{f(x)}{\rightleftarrows}}\; \mathbf{A'} \longleftrightarrow \mathbf{Nat}$$

Rest of this talk:
this is the right definition to work on!

Roadmap

1. ~~Motivation~~ *(10min)*
2. ~~Defining Cosmic Security~~ *(15min)*
3. **Properties of Cosmic Security: a Sanity Check**
    a. **Composition, Black-box reductions** ***(5min)***
4. Summary of Key Results
    a. Feasibilities and Impossibilities (20*min*)
5. Other Notions of Cosmic Security (10min)
6. Conclusion (5min)

Two Nice Properties

What makes us think that cosmic security is a good definition?

1. Composability: Cosmic reductions are composable; that is, *if* **C** *reduces to* **C'** *and* **C'** *reduces to* **C''**, *then* **C** *reduces to* **C''**.

<u>***Def***</u>**:** ε-*cosmic reduction* from **C** to **C'**:
∀ PPT attackers **A**, ∃ PPT **A'** s.t. ∀ **Nat**:

(**A**, **Nat**) has *robust adv* a(.) for **C**

⇓

(**A'**, **Nat**) has *robust adv* ε(.,a(.)) for **C'**.

Two Nice Properties

***Def*: ε-*cosmic reduction* from **C** to **C'**:**
∀ PPT attackers **A**, ∃ PPT **A'** s.t. ∀ **Nat**:

(**A**, **Nat**) has *robust adv* a(.) for **C**
⇓
(**A'**, **Nat**) has *robust adv* ε(.,a(.)) for **C'**.

What makes us think that cosmic security is a good definition?

1. Composability: Cosmic reductions are composable; that is, *if* **C** *reduces to* **C'** *and* **C'** *reduces to* **C''**, *then* **C** *reduces to* **C''**.

follows nicely from definition!

Two Nice Properties

What makes us think that cosmic security is a good definition?

1. Composability: Cosmic reductions are composable; that is, *if* **C** *reduces to* **C'** *and* **C'** *reduces to* **C''**, *then* **C** *reduces to* **C''**.

2. Dummy Lemma: Regular cosmic reductions are *equivalent* to black-box cosmic reductions.

Def**:** *ε-cosmic reduction* from **C** to **C'**:
∀ PPT attackers **A**, ∃ PPT **A'** s.t. ∀ **Nat**:

(**A**, **Nat**) has *robust adv* a(.) for **C**

$\Downarrow$

(**A'**, **Nat**) has *robust adv* ε(.,a(.)) for **C'**.

$\Updownarrow$

Def**:** ε-cosmic *black-box reduction* from **C** to **C'** if ∃ PPT **R** s.t. ∀ (**A**,**Nat**):

(**A**, **Nat**) has *robust adv* a(.) for **C**

$\Downarrow$

(**R**$^{\mathbf{A}}$, **Nat**) has *robust adv* ε(.,a(.)) for **C'**.

Two Nice Properties

What makes us think that cosmic security is a good definition?

1. Composability: Cosmic reductions are composable; that is, *if* **C** *reduces to* **C'** *and* **C'** *reduces to* **C''**, *then* **C** *reduces to* **C''**.

2. Dummy Lemma: Regular cosmic reductions are *equivalent* to black-box cosmic reductions.

Let's quickly intuit this to understand cosmic security better

Def*: ε-*cosmic reduction from **C** to **C'**:
∀ PPT attackers **A**, ∃ PPT **A'** s.t. ∀ **Nat**:

(**A**, **Nat**) has *robust adv* a(.) for **C**

$\Downarrow$

(**A'**, **Nat**) has *robust adv* ε(.,a(.)) for **C'**.

$\Updownarrow$

Def*: ε-cosmic *black-box reduction
from **C** to **C'** if ∃ PPT **R** s.t. ∀ (**A**,**Nat**):

(**A**, **Nat**) has *robust adv* a(.) for **C**

$\Downarrow$

($\mathbf{R}^{\mathbf{A}}$, **Nat**) has *robust adv* ε(.,a(.)) for **C'**.

Two Nice Properties

What makes us think that
cosmic security is a good definition?

1. Composability: Cosmic reductions are composable; that is, *if* **C** *reduces to* **C'** *and* **C'** *reduces to* **C''**, *then* **C** *reduces to* **C''**.

2. Dummy Lemma: Regular cosmic reductions are *equivalent* to black-box cosmic reductions.

Let's quickly intuit this to understand cosmic security better

Def: *ε-cosmic reduction* from **C** to **C'**:
∀ PPT attackers **A**, ∃ PPT **A'** s.t. ∀ **Nat**:

(**A**, **Nat**) has *robust adv* a(.) for **C**

⇓

(**A'**, **Nat**) has *robust adv* ε(.,a(.)) for **C'**.

Easy direction

Def: *ε-cosmic black-box reduction* from **C** to **C'** if ∃ PPT **R** s.t. ∀ (**A**,**Nat**):

(**A**, **Nat**) has *robust adv* a(.) for **C**

⇓

($\mathbf{R^A}$, **Nat**) has *robust adv* ε(.,a(.)) for **C'**.

Two Nice Properties

What makes us think that cosmic security is a good definition?

1. <u>Composability</u>: Cosmic reductions are composable; that is, *if* **C** *reduces to* **C'** *and* **C'** *reduces to* **C''**, *then* **C** *reduces to* **C''**.

2. <u>Dummy Lemma</u>: Regular cosmic reductions are *equivalent* to black-box cosmic reductions.

Let's quickly intuit this to understand cosmic security better

Def: *ε-cosmic reduction* from **C** to **C'**:
∀ PPT attackers **A**, ∃ PPT **A'** s.t. ∀ **Nat**:

(**A**, **Nat**) has *robust adv* a(.) for **C**

⇓

(**A'**, **Nat**) has *robust adv* ε(.,a(.)) for **C'**.

want to show

⇓

Def: *ε-cosmic black-box reduction* from **C** to **C'** if ∃ PPT **R** s.t. ∀ (**A**,**Nat**):

(**A**, **Nat**) has *robust adv* a(.) for **C**

⇓

($\mathbf{R}^{\mathbf{A}}$, **Nat**) has *robust adv* ε(.,a(.)) for **C'**.

From Existential to Constructive Reductions

$$\mathbf{C} \longleftrightarrow \underbrace{\mathbf{A} \longleftrightarrow \mathbf{Nat}}_{\textit{robust adv } a(.) \text{ for } \mathbf{C}}$$

Def: *ε-cosmic reduction* from **C** to **C'**:
∀ PPT attackers **A**, ∃ PPT **A'** s.t. ∀ **Nat**:

(**A**, **Nat**) has *robust adv* a(.) for **C**

(**A'**, **Nat**) has *robust adv* ε(.,a(.)) for **C'**.

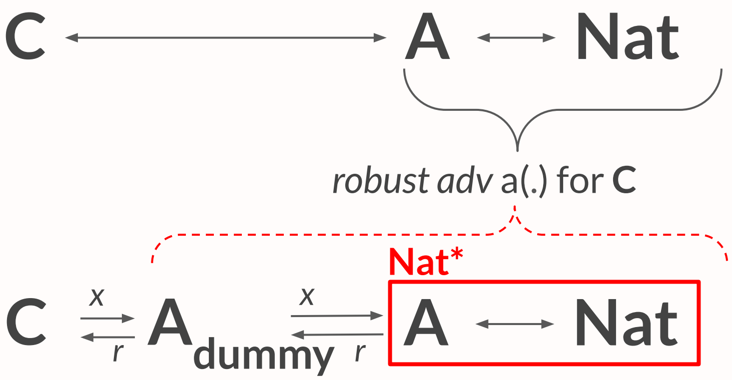
want to show

Def: *ε-cosmic black-box reduction* from **C** to **C'** if ∃ PPT **R** s.t. ∀ (**A**,**Nat**):

(**A**, **Nat**) has *robust adv* a(.) for **C**

($\mathbf{R}^{\mathbf{A}}$, **Nat**) has *robust adv* ε(.,a(.)) for **C'**.

From Existential to Constructive Reductions



Def: *ε-cosmic reduction* from **C** to **C'**:

∀ PPT attackers **A**, ∃ PPT **A'** s.t. ∀ **Nat**:

(**A**, **Nat**) has *robust adv* a(.) for **C**

⇓

(**A'**, **Nat**) has *robust adv* ε(.,a(.)) for **C'**.

⇓ want to show

Def: *ε-cosmic black-box reduction*

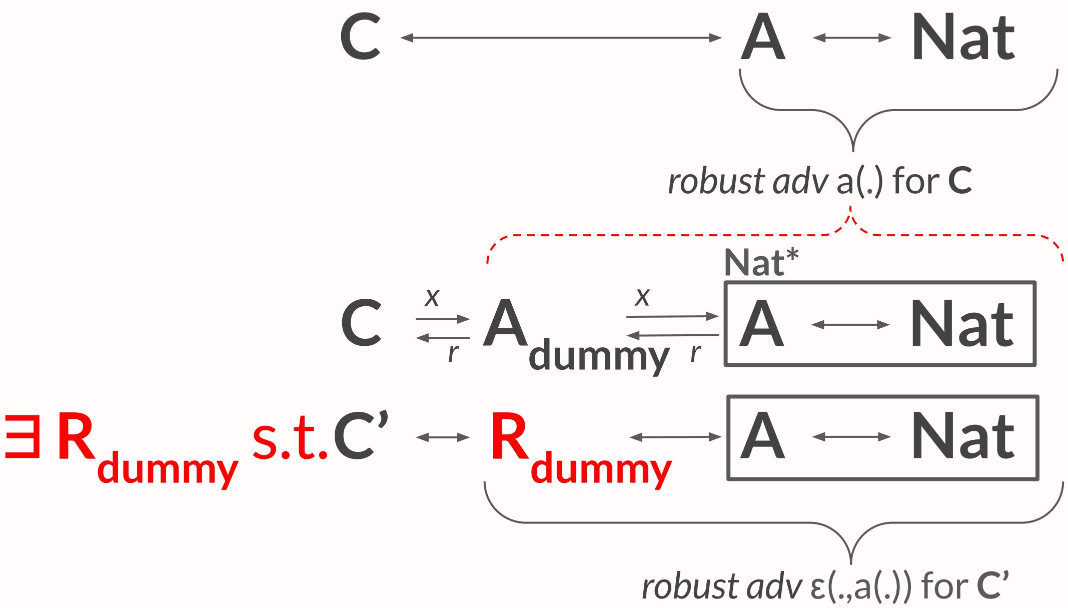
from **C** to **C'** if ∃ PPT **R** s.t. ∀ (**A**,**Nat**):

(**A**, **Nat**) has *robust adv* a(.) for **C**

⇓

($\mathbf{R}^{\mathbf{A}}$, **Nat**) has *robust adv* ε(.,a(.)) for **C'**.

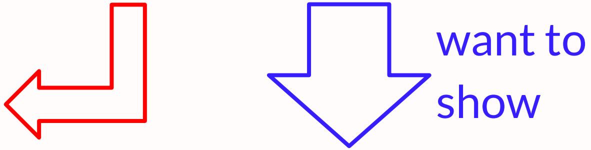
From Existential to Constructive Reductions



<u>*Def*</u>: *ε-cosmic reduction* from **C** to **C'**:
∀ PPT attackers **A**, ∃ PPT **A'** s.t. ∀ **Nat**:

(**A**, **Nat**) has *robust adv* a(.) for **C**

(**A'**, **Nat**) has *robust adv* ε(.,a(.)) for **C'**.

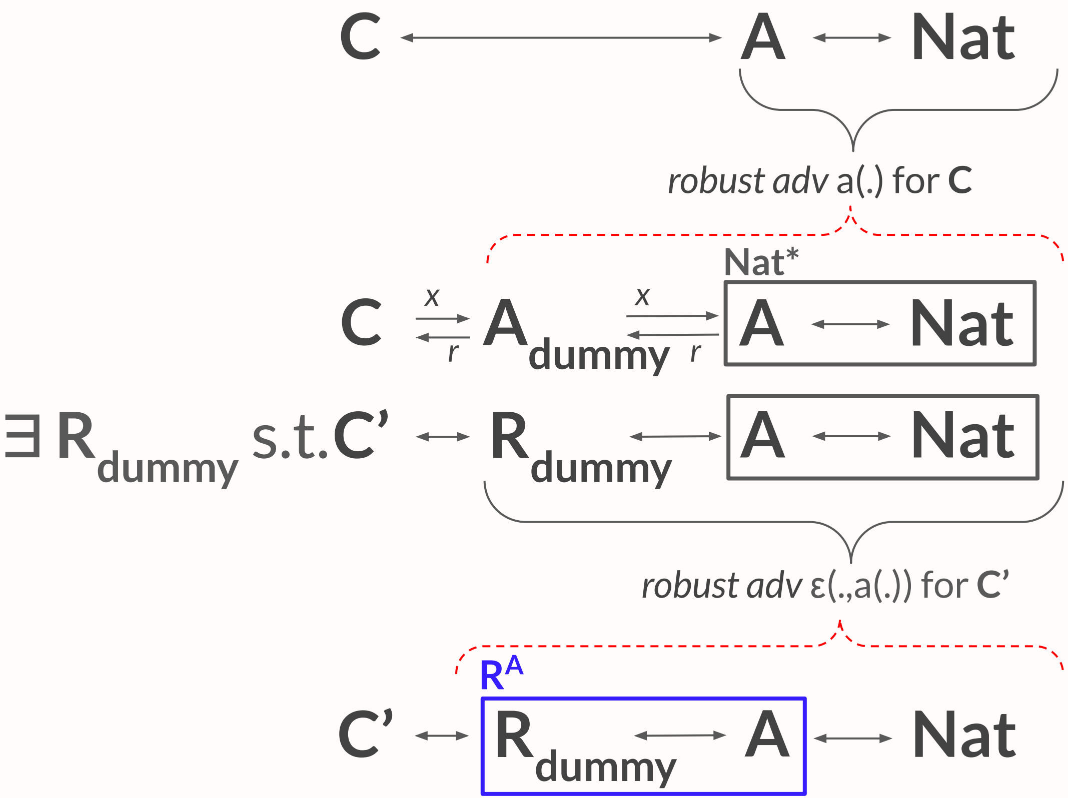


<u>*Def*</u>: *ε-cosmic black-box reduction* from **C** to **C'** if ∃ PPT **R** s.t. ∀ (**A**,**Nat**):

(**A**, **Nat**) has *robust adv* a(.) for **C**

($\mathbf{R}^{\mathbf{A}}$, **Nat**) has *robust adv* ε(.,a(.)) for **C'**.

From Existential to Constructive Reductions



Def: *ε-cosmic reduction* from **C** to **C'**:
∀ PPT attackers **A**, ∃ PPT **A'** s.t. ∀ **Nat**:

(**A**, **Nat**) has *robust adv* a(.) for **C**

(**A'**, **Nat**) has *robust adv* ε(.,a(.)) for **C'**.

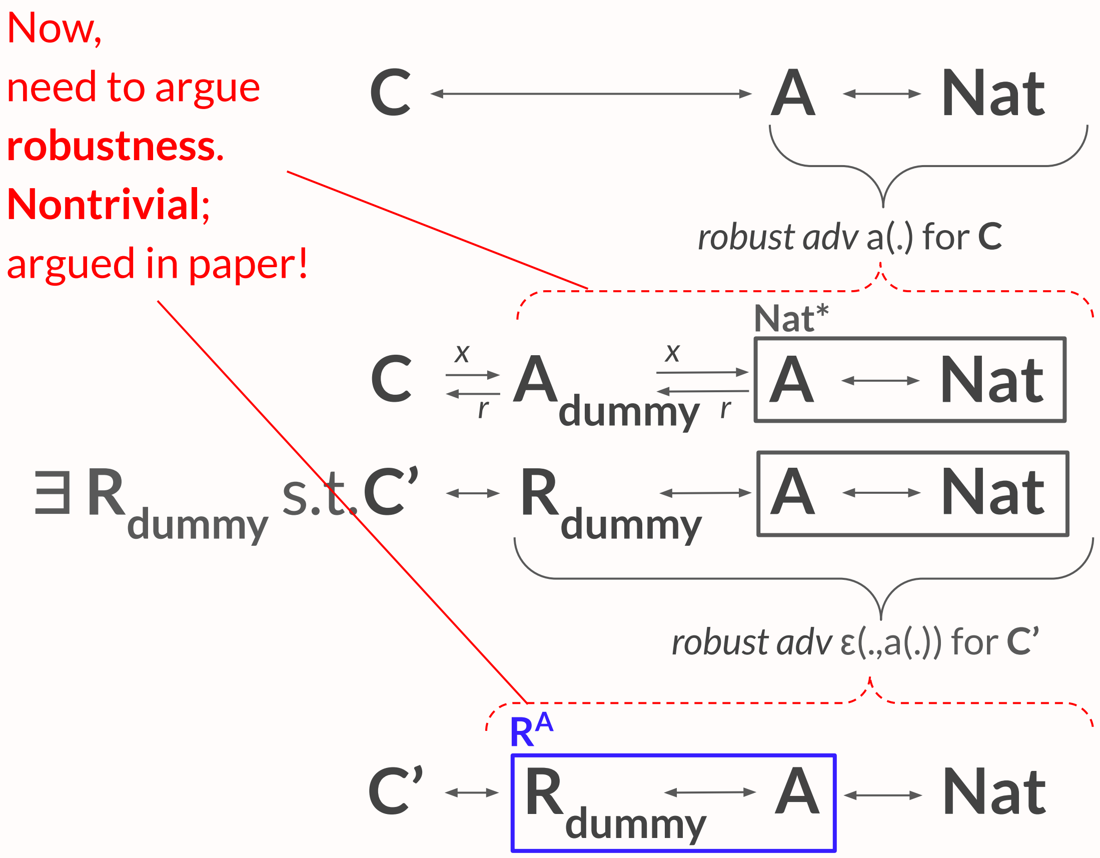
want to show

Def: *ε-cosmic black-box reduction*
from **C** to **C'** if ∃ PPT **R** s.t. ∀ (**A**,**Nat**):

(**A**, **Nat**) has *robust adv* a(.) for **C**

($\mathbf{R}^{\mathbf{A}}$, **Nat**) has *robust adv* ε(.,a(.)) for **C'**.

From Existential to Constructive Reductions



***Def*: ε-cosmic reduction** from **C** to **C'**:
∀ PPT attackers **A**, ∃ PPT **A'** s.t. ∀ **Nat**:

(**A**, **Nat**) has *robust adv* a(.) for **C**

⇓

(**A'**, **Nat**) has *robust adv* ε(.,a(.)) for **C'**.

want to show

Def*: *ε-cosmic black-box reduction
from **C** to **C'** if ∃ PPT **R** s.t. ∀ (**A**,**Nat**):

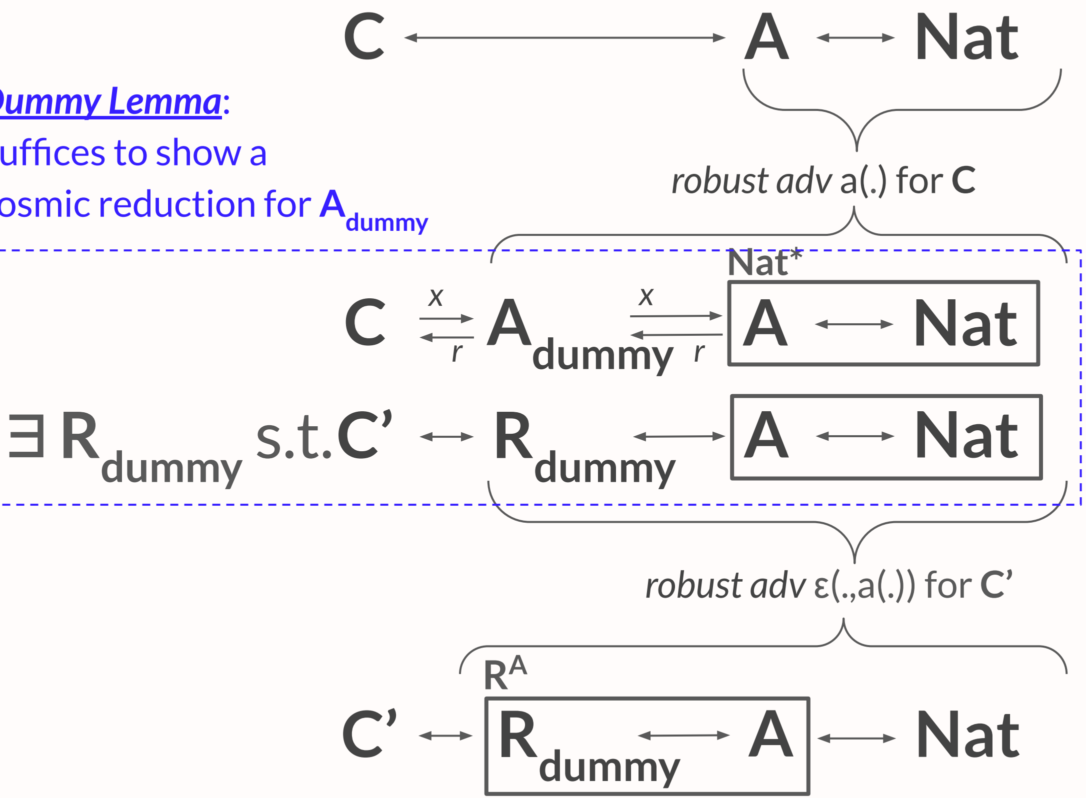
(**A**, **Nat**) has *robust adv* a(.) for **C**

⇓

(R^A, **Nat**) has *robust adv* ε(.,a(.)) for **C'**.

From Existential to Constructive Reductions

Dummy Lemma:
Suffices to show a
cosmic reduction for $\mathbf{A}_{\text{dummy}}$



Def: ε-*cosmic reduction* from **C** to **C'**:
∀ PPT attackers **A**, ∃ PPT **A'** s.t. ∀ **Nat**:

(**A**, **Nat**) has *robust adv* a(.) for **C**

(**A'**, **Nat**) has *robust adv* ε(.,a(.)) for **C'**.

Def: ε-*cosmic black-box reduction* from **C** to **C'** if ∃ PPT **R** s.t. ∀ (**A**,**Nat**):

(**A**, **Nat**) has *robust adv* a(.) for **C**

($\mathbf{R}^{\mathbf{A}}$, **Nat**) has *robust adv* ε(.,a(.)) for **C'**.

Recap So Far: A Necessary, Natural Definition

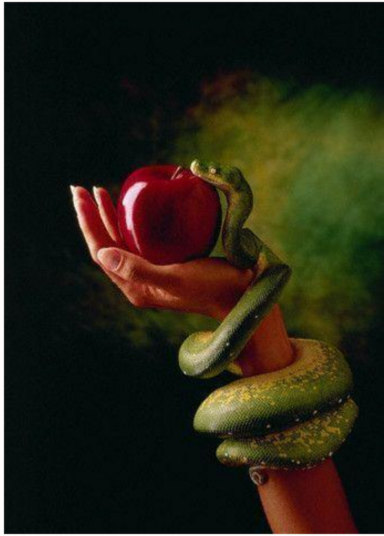
Why do we like Cosmic Security?

1. Acknowledges the Unknown: allows Nature to be *stateful* in a way previously not considered, but that we are now compelled to acknowledge.

Moreover, the definition is Well-Behaved.

2. Composability: Cosmic reductions are composable; that is, *if* **C** *reduces to* **C'** *and* **C'** *reduces to* **C''**, *then* **C** *reduces to* **C''**.

3. Dummy Lemma: Regular cosmic reductions are *equivalent* to black-box cosmic reductions.



Recap So Far: A Necessary, Natural Definition

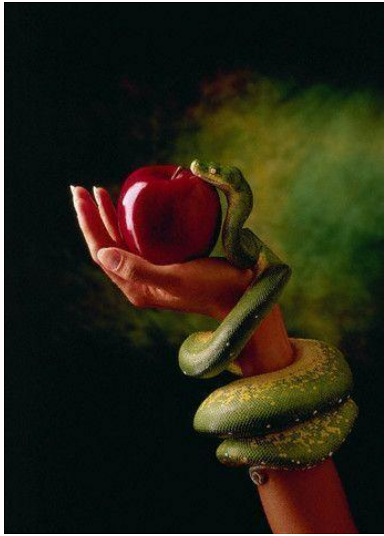
Why do we like Cosmic Security?

1. Acknowledges the Unknown: allows Nature to be *stateful* in a way previously not considered, but that we are now compelled to acknowledge.

Moreover, the definition is Well-Behaved.

2. Composability: Cosmic reductions are composable; that is, *if* **C** *reduces to* **C'** *and* **C'** *reduces to* **C''**, *then* **C** *reduces to* **C''**.

3. Dummy Lemma: Regular cosmic reductions are *equivalent* to black-box cosmic reductions.



NEXT UP, The Real Test:
What Can We Build?

Roadmap

1. ~~Motivation~~ *(10min)*
2. ~~Defining Cosmic Security~~ *(15min)*
3. ~~Properties of Cosmic Security: a Sanity Check~~
   a. ~~Composition, Black-box reductions~~ *(5min)*
4. **Summary of Key Results**
   a. **Feasibilities and Impossibilities** ***(20min)***
5. Other Notions of Cosmic Security (10min)
6. Conclusion (5min)

Key Results: Feasibilities and Impossibilities

<u>Thm 1</u> (*Feasibility*): classical 1-shot straight-line black-box reductions imply cosmic reductions.

<u>Corollaries</u>: PRFs/SKE/Commitments/Witness Indistinguishability/PRG Length Extension

> Not surprising, since it doesn't matter that Nature is stateful: a 1-shot reduction only uses Nature once.

Key Results: Feasibilities and Impossibilities

Thm 1 (*Feasibility*): classical 1-shot straight-line black-box reductions imply cosmic reductions.

Corollaries: PRFs/SKE/Commitments/Witness Indistinguishability/PRG Length Extension

> Not surprising, since it doesn't matter that Nature is stateful: a 1-shot reduction only uses Nature once.

New 1-shot straight-line black-box proof for WI! (See Paper)

Key Results: Feasibilities and Impossibilities

<u>Thm 1</u> (*Feasibility*): classical 1-shot straight-line black-box reductions imply cosmic reductions.

<u>Corollaries</u>: PRFs/SKE/Commitments/Witness Indistinguishability/PRG Length Extension

> Not surprising, since it doesn't matter that Nature is stateful: a 1-shot reduction only uses Nature once.

What about reductions that use the attacker multiple times?

Key Results:
Feasibilities and Impossibilities

<u>Thm 1</u> (*Feasibility*): classical 1-shot straight-line black-box reductions imply cosmic reductions.

<u>Corollaries</u>: PRFs/SKE/Commitments/Witness Indistinguishability/PRG Length Extension

> Not surprising, since it doesn't matter that Nature is stateful: a 1-shot reduction only uses Nature once.

<u>Thm 2</u> (*Impossibility*): Hardness amplification of arbitrary weak OWFs via direct product, using only black-box access to the OWF, is impossible.

<u>Thm 3</u> (*Impossibility*): A Goldreich Levin Theorem, where the reduction has only black-box access to the OWF, is impossible.

Key Results: Feasibilities and Impossibilities

Thm 1 (*Feasibility*): classical 1-shot straight-line black-box reductions imply cosmic reductions.

Corollaries: PRFs/SKE/Commitments/Witness Indistinguishability/PRG Length Extension

> Not surprising, since it doesn't matter that Nature is stateful: a 1-shot reduction only uses Nature once.

Thm 2 (*Impossibility*): Hardness amplification of arbitrary weak OWFs via direct product, using only black-box access to the OWF, is impossible.

Thm 3 (*Impossibility*): A Goldreich Levin Theorem, where the reduction has only black-box access to the OWF, is impossible.

> Teaser: the cosmic adversary can notice when it is sent correlated inputs.

Key Results:
Feasibilities and Impossibilities

Thm 1 (*Feasibility*): classical 1-shot straight-line black-box reductions imply cosmic reductions.

Corollaries: PRFs/SKE/Commitments/Witness Indistinguishability/PRG Length Extension

> Not surprising, since it doesn't matter that Nature is stateful: a 1-shot reduction only uses Nature once.

Thm 2 (*Impossibility*): Hardness amplification of arbitrary weak OWFs via direct product, using only black-box access to the OWF, is impossible.

Thm 3 (*Impossibility*): A Goldreich Levin Theorem, where the reduction has only black-box access to the OWF, is impossible.

> Teaser: the cosmic adversary can notice when it is sent correlated inputs.

Claim: we need new techniques to build advanced cosmic cryptography!

Key Results: Feasibilities and Impossibilities

Thm 1 (*Feasibility*): classical 1-shot straight-line black-box reductions imply cosmic reductions.

Corollaries: PRFs/SKE/Commitments/Witness Indistinguishability/PRG Length Extension

> Not surprising, since it doesn't matter that Nature is stateful: a 1-shot reduction only uses Nature once.

Thm 2 (*Impossibility*): Hardness amplification of arbitrary weak OWFs via direct product, using only black-box access to the OWF, is impossible.

Thm 3 (*Impossibility*): A Goldreich Levin Theorem, where the reduction has only black-box access to the OWF, is impossible.

> Teaser: the cosmic adversary can notice when it is sent correlated inputs.

Thm 4 (*Feasibility*): Hardness amplification is possible for "re-randomizable" OWFs.

Key Results:
Feasibilities and Impossibilities

Thm 1 (*Feasibility*): classical 1-shot straight-line black-box reductions imply cosmic reductions.

Corollaries: PRFs/SKE/Commitments/Witness Indistinguishability/PRG Length Extension

> *Not surprising, since it doesn't matter that Nature is stateful: a 1-shot reduction only uses Nature once.*

Thm 2 (*Impossibility*): Hardness amplification of arbitrary weak OWFs via direct product, using only black-box access to the OWF, is impossible.

Thm 3 (*Impossibility*): A Goldreich Levin Theorem, where th… cess to the OWF, is impossible.

"A First Stab" at feasibility in the cosmic setting

> *Teaser: the cosmic adversary can notice when it is sent correlated inputs.*

Thm 4 (*Feasibility*): Hardness amplification is possible for "re-randomizable" OWFs.

Plain Cosmic Security

Claim: a non-trivial setting (for feasibility),
since we rule out some classical approaches.

Plain Cosmic Security

Claim: a non-trivial setting (for feasibility),
since we rule out some classical approaches.

Later: “Relaxed” Cosmic Security

Suppose Nature isn’t fully stateful; the only state it keeps is the “time”.

Plain Cosmic Security

Claim: a non-trivial setting (for feasibility),
since we rule out some classical approaches.

Later: “Relaxed” Cosmic Security

Suppose Nature isn’t fully stateful; the only state it keeps is the “time”.

Thm 5 (*Informal*): Non-adaptive straight-line black-box reductions give cosmic reductions for Natures that evolve over time (but are otherwise stateless).

Plain Cosmic Security

Claim: a non-trivial setting (for feasibility),
since we rule out some classical approaches.

Later: “Relaxed” Cosmic Security

Suppose Nature isn’t fully stateful; the only state it keeps is the “ti…”

Thm 5 (*Informal*): Non-adaptive straight-line black-box reductio…
reductions for Natures that evolve over time (but are otherwise stateless).

Table this for now.

Intermission

Next Up:
Walkthrough of our results

Key Results:
Feasibilities and Impossibilities

Thm 1 (*Feasibility*): classical 1-shot straight-line black-box reductions imply cosmic reductions.

Corollaries: PRFs/SKE/Commitments/Witness Indistinguishability/PRG Length Extension

> Not surprising, since it doesn't matter that Nature is stateful: a 1-shot reduction only uses Nature once.

Thm 2 (*Impossibility*): Hardness amplification of arbitrary weak OWFs via direct product, using only black-box access to the OWF, is impossible.

Thm 3 (*Impossibility*): A Goldreich Levin Theorem, where the reduction has only black-box access to the OWF, is impossible.

> Teaser: the cosmic adversary can notice when it is sent correlated inputs.

Thm 4 (*Feasibility*): Hardness amplification is possible for "re-randomizable" OWFs.

Key Results:
Feasibilities and Impossibilities

<u>Thm 1</u> (*Feasibility*): classical 1-shot straight-line black-box reductions imply cosmic reductions.

<u>**Corollaries**</u>: PRFs/SKE/Commitments/Witness Indistinguishability/PRG Length Extension

> Not surprising, since it doesn't matter that Nature is stateful: a 1-shot reduction only uses Nature once.

<u>**Thm 2**</u> (*Impossibility*): Hardness amplification of arbitrary weak OWFs via direct product, using only black-box access to the OWF, is impossible.

<u>**Thm 3**</u> (*Impossibility*): A Goldreich Levin Theorem, where the reduction has only black-box access to the OWF, is impossible.

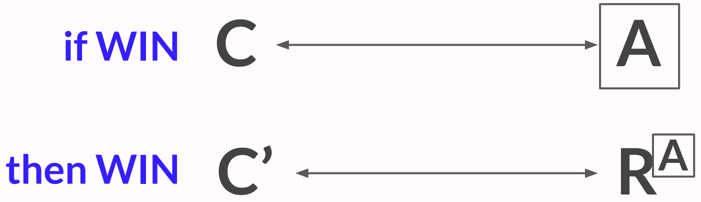
> Teaser: the cosmic adversary can notice when it is sent correlated inputs.

<u>**Thm 4**</u> (*Feasibility*): Hardness amplification is possible for "re-randomizable" OWFs.

Basic Feasibility

Thm 1 (*Feasibility*): classical 1-shot straight-line black-box reductions imply cosmic reductions.

1-shot straightline black-box **R**



Basic Feasibility

Thm 1 (*Feasibility*): classical 1-shot straight-line black-box reductions imply cosmic reductions.

1-shot straightline black-box **R**

if WIN $C \longleftrightarrow \boxed{A}$

then WIN $C' \longleftrightarrow R^{\boxed{A}}$

Cosmic reduction $\forall \rho$

if WIN $C \longleftrightarrow A \longleftrightarrow \mathrm{Nat}(\rho)$

Basic Feasibility

<u>**Thm 1**</u> (*Feasibility*): classical 1-shot straight-line black-box reductions imply cosmic reductions.

1-shot straightline black-box **R**

if WIN $C \longleftrightarrow \boxed{A}$

then WIN $C' \longleftrightarrow R^{\boxed{A}}$

Cosmic reduction $\forall \rho$

if WIN $C \longleftrightarrow A \longleftrightarrow \mathrm{Nat}(\rho)$

then WIN $C \longleftrightarrow \boxed{A \longleftrightarrow \mathrm{Nat}(\rho)}$

Basic Feasibility

Thm 1 (*Feasibility*): classical 1-shot straight-line black-box reductions imply cosmic reductions.

1-shot straightline black-box **R**

if WIN $C \longleftrightarrow \boxed{A}$

then WIN $C' \longleftrightarrow R^{\boxed{A}}$

Cosmic reduction $\forall \rho$

if WIN $C \longleftrightarrow A \longleftrightarrow Nat(\rho)$

then WIN $C \longleftrightarrow \boxed{A \longleftrightarrow Nat(\rho)}$

then WIN $C' \longleftrightarrow R^{\boxed{A \longleftrightarrow Nat(\rho)}}$

Basic Feasibility

<u>Thm 1</u> (*Feasibility*): classical 1-shot straight-line black-box reductions imply cosmic reductions.

1-shot straightline black-box **R**

if WIN $\mathbf{C} \longleftrightarrow \boxed{\mathbf{A}}$

then WIN $\mathbf{C'} \longleftrightarrow \mathbf{R}^{\boxed{A}}$

Cosmic reduction $\forall \rho$

if WIN $\mathbf{C} \longleftrightarrow \mathbf{A} \longleftrightarrow \mathrm{Nat}(\rho)$

then WIN $\mathbf{C} \longleftrightarrow \boxed{\mathbf{A} \longleftrightarrow \mathrm{Nat}(\rho)}$

then WIN $\mathbf{C'} \longleftrightarrow \mathbf{R}^{\boxed{A \longleftrightarrow \mathrm{Nat}(\rho)}}$

then WIN $\mathbf{C'} \longleftrightarrow \mathbf{R}^{A} \longleftrightarrow \mathrm{Nat}(\rho)$

Basic Feasibility

<u>**Thm 1**</u> (*Feasibility*): classical 1-shot straight-line black-box reductions imply cosmic reductions.

1-shot straightline black-box **R**

if WIN $C \longleftrightarrow \boxed{A}$

then WIN $C' \longleftrightarrow R^{\boxed{A}}$

Cosmic reduction $\forall \rho$

if WIN $C \longleftrightarrow A \longleftrightarrow \mathrm{Nat}(\rho)$

then WIN $C \longleftrightarrow \boxed{A \longleftrightarrow \mathrm{Nat}(\rho)}$

then WIN $C' \longleftrightarrow R^{\boxed{A \longleftrightarrow \mathrm{Nat}(\rho)}}$

then WIN $C' \longleftrightarrow R^{A} \longleftrightarrow \mathrm{Nat}(\rho)$

<u>**Corollaries**</u>: PRFs/SKE/Commitments/Witness Indistinguishability/PRG Length Extension

Key Results:
Feasibilities and Impossibilities

Thm 1 (*Feasibility*): classical 1-shot straight-line black-box reductions imply cosmic reductions.

Corollaries: PRFs/SKE/Commitments/Witness Indistinguishability/PRG Length Extension

> Not surprising, since it doesn't matter that Nature is stateful: a 1-shot reduction only uses Nature once.

Thm 2 (*Impossibility*): Hardness amplification of arbitrary weak OWFs via direct product, using only black-box access to the OWF, is impossible.

Thm 3 (*Impossibility*): A Goldreich Levin Theorem, where the reduction has only black-box access to the OWF, is impossible.

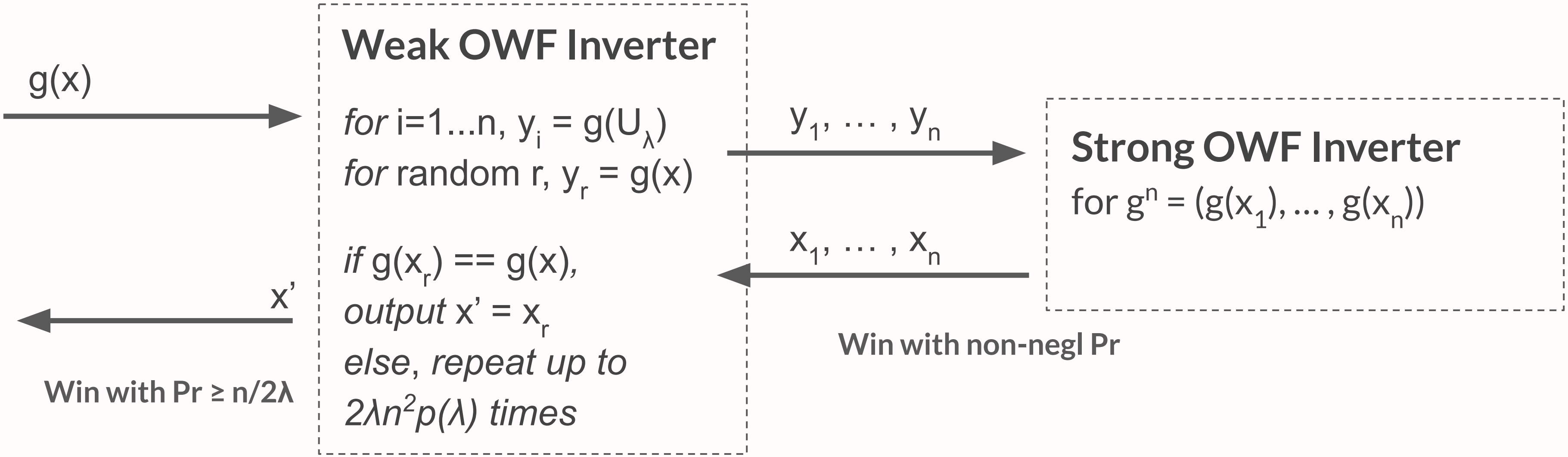
> Teaser: the cosmic adversary can notice when it is sent correlated inputs.

Thm 4 (*Feasibility*): Hardness amplification is possible for "re-randomizable" OWFs.

Key Results:
Feasibilities and Impossibilities

<u>Thm 2</u> (*Impossibility of Hardness Amplification*):
Suppose there is an ε-cosmic black reduction from the OWF security of $g^n(x_1 \ldots x_n) = (g(x_1), \ldots, g(x_n))$ to the OWF security of $g(x)$ that uses only black-box access to g, and that works for any function g.
Then, there exists a negligible function μ such that $\varepsilon(\lambda, a) \leq a + \mu(\lambda)$.

Recall: Classical Hardness Amplification



Recall: Classical Hardness Amplification

$g(x)$

Weak OWF Inverter

for $i=1\ldots n$, $y_i = g(U_\lambda)$

for random r, $y_r = g(x)$

if $g(x_r) == g(x)$,

output $x' = x_r$

else, repeat up to

$2\lambda n^2 p(\lambda)$ *times*

x'

embed g(x) in random location
in uniformly generated image of g^n

$y_1, \ldots, y_n$

Strong OWF Inverter

for $g^n = (g(x_1), \ldots, g(x_n))$

$x_1, \ldots, x_n$

repeat!

with non-negl probability,
all n are preimages

High Level Idea: Cosmic Hardness Amplification

$g(x)$

Weak OWF Inverter

for $i=1\ldots n$, $y_i = g(U_\lambda)$

for random r, $y_r = g(x)$

if $g(x_r) == g(x)$,

output $x' = x_r$

else, repeat up to

$2\lambda n^2 p(\lambda)$ times

x'

embed g(x) in random location
in uniformly generated image of g^n

$y_1, \ldots, y_n$

$x_1, \ldots, x_n$

A_{dummy} $\leftrightarrow$ **Nat**

repeat!

High Level Idea: Cosmic Hardness Amplification

$g(x)$

Weak OWF Inverter

for $i=1\ldots n$, $y_i = g(U_\lambda)$
for random r, $y_r = g(x)$

if $g(x_r) == g(x)$,
output $x' = x_r$
else, repeat up to
$2\lambda n^2 p(\lambda)$ *times*

x'

embed g(x) in random location
in uniformly generated image of g^n

$y_1, \ldots, y_n$

$x_1, \ldots, x_n$

repeat!

$A_{\text{dummy}} \leftrightarrow$ **Nat**

Problem: Nat is only guaranteed to invert on uniformly generated input $y_r = g(U_\lambda)$ from a fresh instance of C

High Level Idea: Cosmic Hardness Amplification

$g(x) \longrightarrow$

Weak OWF Inverter

for $i=1\ldots n$, $y_i = g(U_\lambda)$

for random r, $y_r = g(x)$

if $g(x_r) == g(x)$,

output $x' = x_r$

else, repeat up to

$2\lambda n^2 p(\lambda)$ times

$\longleftarrow x'$

embed g(x) in random location
in uniformly generated image of g^n

$y_1, \ldots, y_n \longrightarrow$

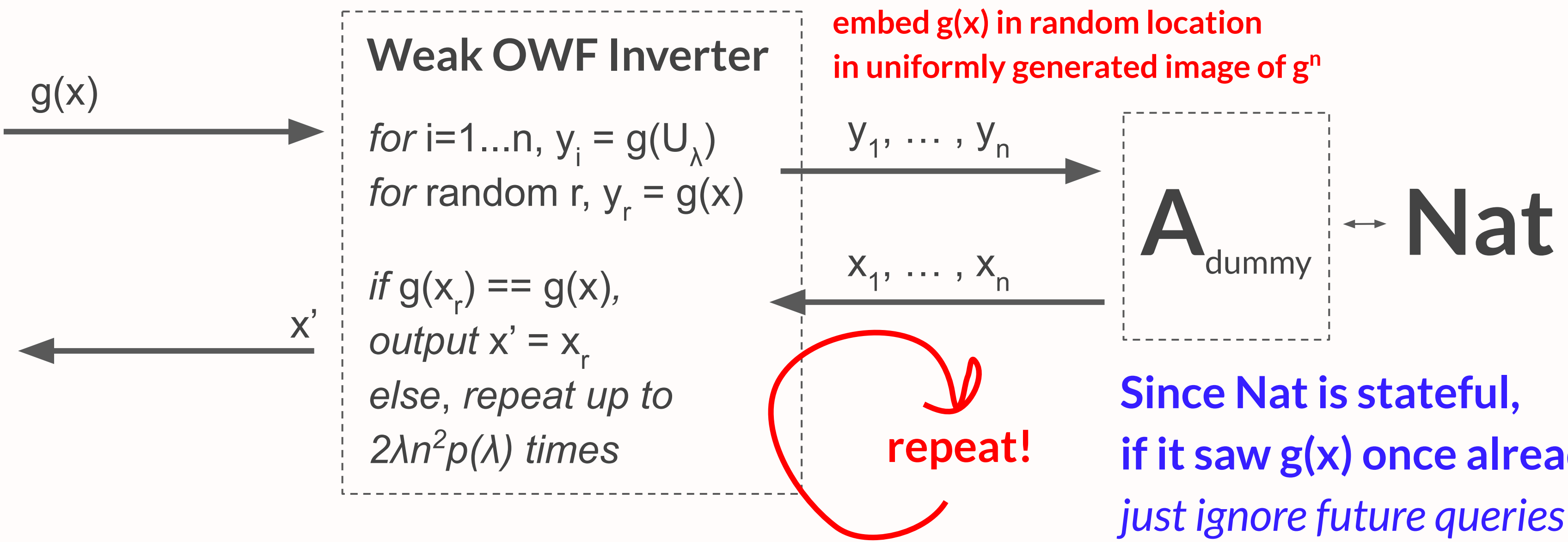
$\longleftarrow x_1, \ldots, x_n$

$A_{dummy} \leftrightarrow$ **Nat**

repeat!

Since Nat is stateful,
if it saw g(x) once already,
$y_r = g(x)$ no longer looks like
part of a fresh challenge!

High Level Idea: Cosmic Hardness Amplification



Since Nat is stateful,
if it saw g(x) once already,
just ignore future queries that contain g(x).

Thus, Black-Box Cosmic Hardness Amplification is *Impossible*.

Classical reductions that use an attacker repeatedly on correlated inputs may fail, if the attacker notices the correlation and halts.

We may need to hide the correlation.

Key Results: Feasibilities and Impossibilities

<u>Thm 1</u> (*Feasibility*): classical 1-shot straight-line black-box reductions imply cosmic reductions.

<u>Corollaries</u>: PRFs/SKE/Commitments/Witness Indistinguishability/PRG Length Extension

> Not surprising, since it doesn't matter that Nature is stateful: a 1-shot reduction only uses Nature once.

<u>Thm 2</u> (*Impossibility*): Hardness amplification of arbitrary weak OWFs via direct product, using only black-box access to the OWF, is impossible.

<u>Thm 3</u> (*Impossibility*): A Goldreich Levin Theorem, where the reduction has only black-box access to the OWF, is impossible. Same High Level Idea!

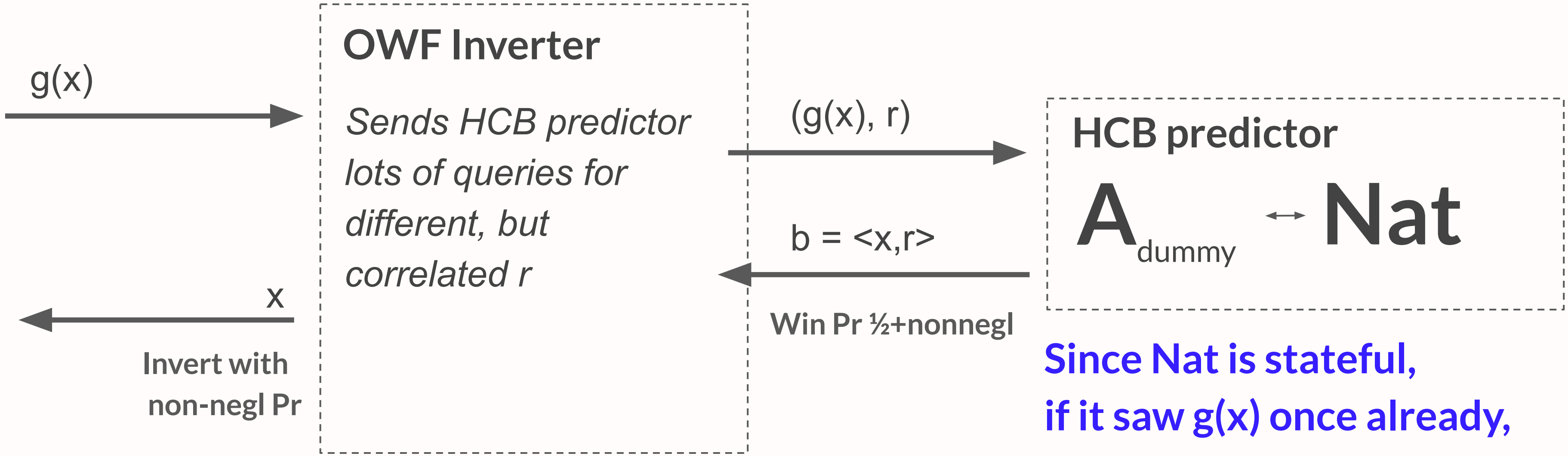
> Teaser: the cosmic adversary can notice when it is sent correlated inputs.

<u>Thm 4</u> (*Feasibility*): Hardness amplification is possible for "re-randomizable" OWFs.

Key Results:
Feasibilities and Impossibilities

<u>Thm 3</u> (*Impossibility of a Goldreich Levin Theorem*):
Suppose there is an ε-cosmic black-box reduction from the security of the hardcore predicate $h(x,r) = \langle x,r \rangle$ w.r.t. $f(x, r) = (g(x), r)$ to the OWF security of g that uses only black-box access to g and that works for any function g. Then, there is a negligible function μ such that $\varepsilon(\lambda, a) \leq \mu(\lambda)$ for all a.

Recall: Goldreich Levin Theorem



Since Nat is stateful,
if it saw g(x) once already,
just ignore future queries that contain g(x).

Thus, a Goldreich Levin Theorem is *Impossible*.

Takeaway: classical techniques fail.

To get around it, need techniques that are non-black-box in the OWF.

Key Results:
Feasibilities and Impossibilities

Thm 1 (*Feasibility*): classical 1-shot straight-line black-box reductions imply cosmic reductions.

Corollaries: PRFs/SKE/Commitments/Witness Indistinguishability/PRG Length Extension

> *Not surprising, since it doesn't matter that Nature is stateful: a 1-shot reduction only uses Nature once.*

Thm 2 (*Impossibility*): Hardness amplification of arbitrary weak OWFs via direct product, using only black-box access to the OWF, is impossible.

Thm 3 (*Impossibility*): A Goldreich Levin Theorem, where th… cess to the OWF, is impossible.

> *Teaser: the cosmic adversary can notice when it is sent correlated i…puts.*

"A First Stab" at feasibility in the cosmic setting

Thm 4 (*Feasibility*): Hardness amplification is possible for "re-randomizable" OWFs.

Feasibility: Hardness Amplification

Suppose $g(x)$ is <u>re-randomizable</u>.

<u>Def:</u> A one-way function g is **re-randomizable** if $\exists$ PPT *rand*(.), *recover*(.) s.t.

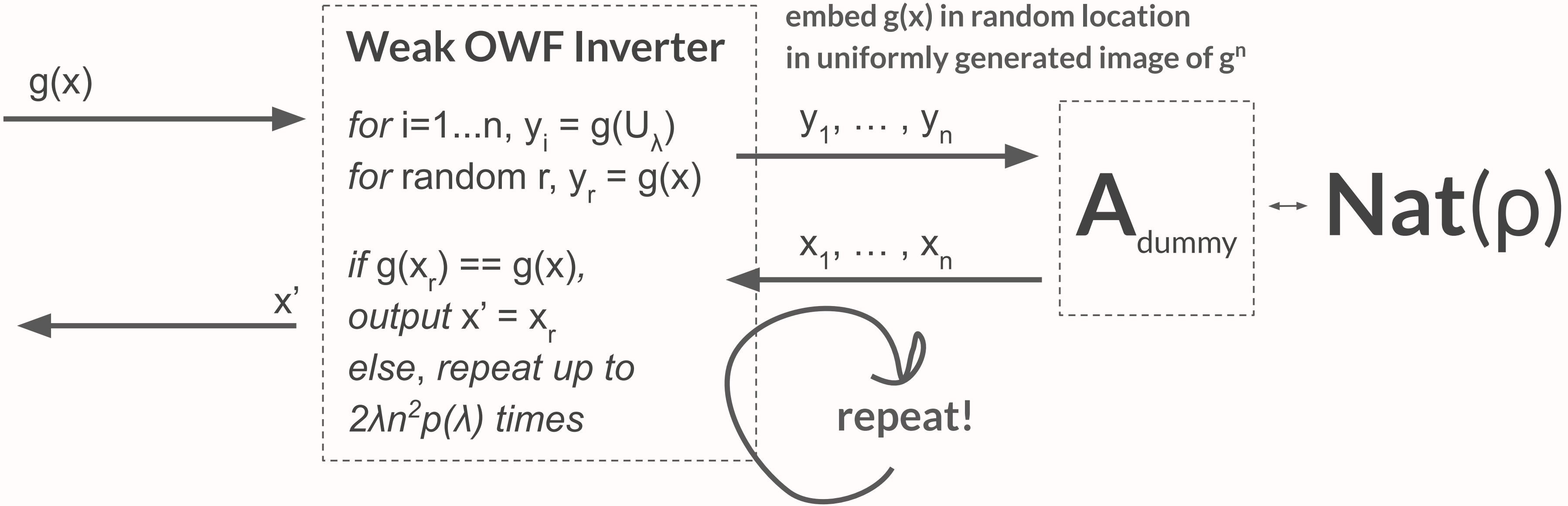
$$\forall x, \{r \leftarrow \{0,1\}^\lambda : \mathit{rand}(g(x), r)\} \equiv \{x' \leftarrow \{0,1\}^\lambda : g(x')\}$$

$$\forall x, r, \text{ let } y \leftarrow \mathit{rand}(g(x), r),\ x' \leftarrow \mathit{recover}(g^{-1}(y), r)\text{, then } g(x) = g(x').$$

Denote **g(x)** = $\mathit{rand}(g(x), U_\lambda)$ and **x'** = $\mathit{recover}(x', r)$, where r is the previous seed used.

Feasibility: Hardness Amplification

Suppose $g(x)$ is <u>re-randomizable</u>.



Feasibility: Hardness Amplification

Suppose $g(x)$ is re-randomizable.

$g(x)$

Weak OWF Inverter

for $i=1\ldots n$, $y_i = g(U_\lambda)$
for random r, y_r = $g(x)$

if $g(x_r) == g(x)$,
output $x' = x_r$
else, repeat up to
$2\lambda n^2 p(\lambda)$ times

x'

embed $g(x)$ in random location
in uniformly generated image of g^n

$y_1, \ldots, y_n$

$x_1, \ldots, x_n$

repeat!

$A_{\text{dummy}} \leftrightarrow \text{Nat}(\rho)$

y_r = $g(x)$ always looks uniformly random, so Nat must win with nonnegl probability.

We Can Go Beyond
Single-Shot Straight-Line Reductions!

Key Point: We need to hide any correlation between queries in the view of the adversary. For example, by re-randomizing **$g(x)$**.

How Far Can We Go?

Open Problem:
Even though a Goldreich-Levin Theorem (that is black-box in the OWF) is impossible, can we build cosmic PRGs from OWFs?

For now…

…let's climb a different mountain.

Roadmap

1. ~~Motivation~~ *(10min)*
2. ~~Defining Cosmic Security~~ *(15min)*
3. ~~Properties of Cosmic Security: a Sanity Check~~
    a. ~~Composition, Black-box reductions~~ *(5min)*
4. ~~Summary of Key Results~~
    a. ~~Feasibilities and Impossibilities (20min)~~
5. **Other Notions of Cosmic Security (10min)**
6. Conclusion (5min)

Recall: Why did this fail?

Because Nat can adjust future behavior based on prior game outcomes.

$g(x)$

Weak OWF Inverter

for $i=1\ldots n$, $y_i = g(U_\lambda)$

for random r, $y_r = g(x)$

if $g(x_r) == g(x)$,

output $x' = x_r$

else, *repeat up to*

$2\lambda n^2 p(\lambda)$ times

x'

embed $g(x)$ in random location in uniformly generated image of g^n

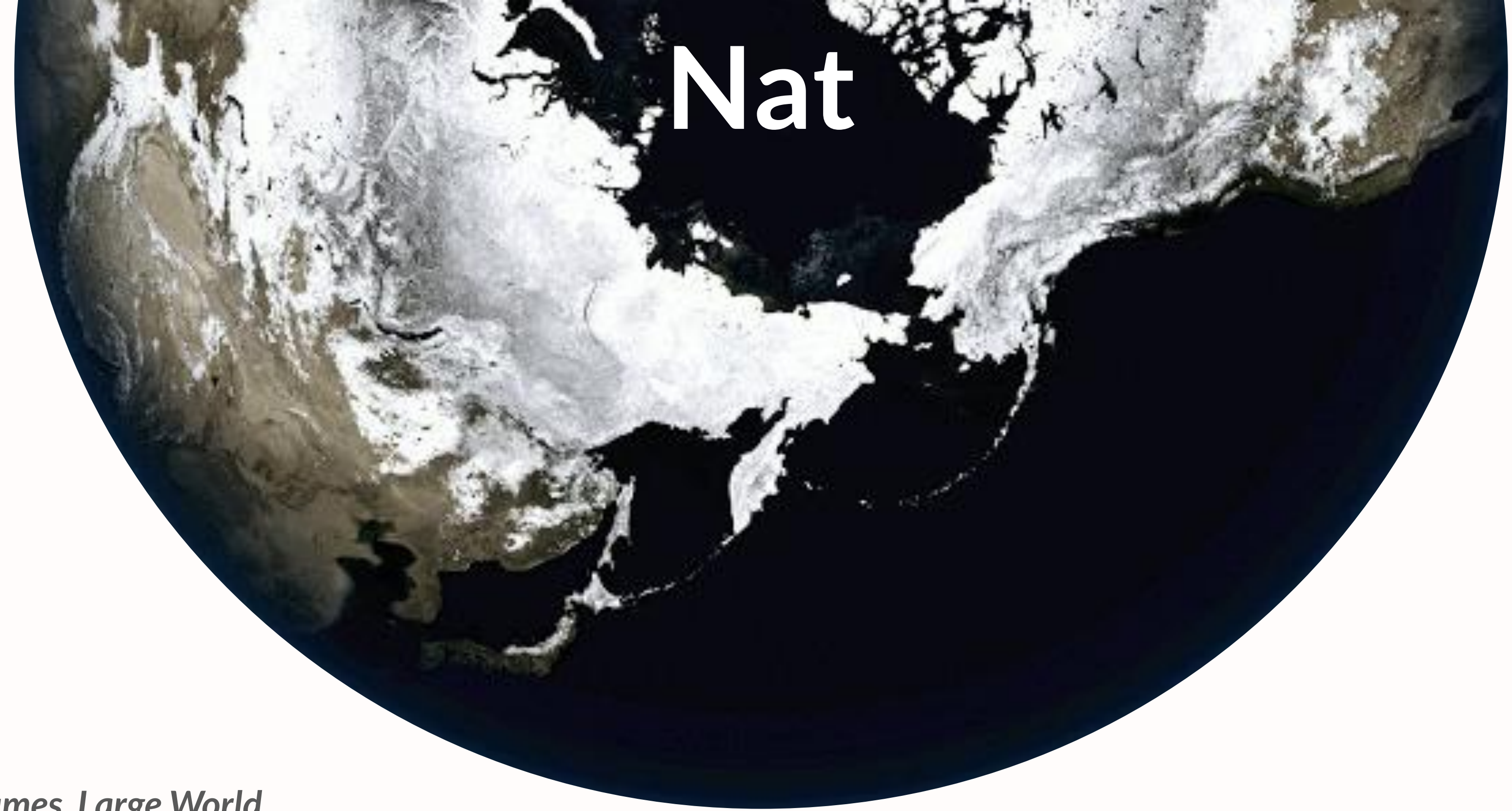
$y_1, \ldots, y_n$

$x_1, \ldots, x_n$

repeat!

$A_{dummy} \leftrightarrow \mathrm{Nat}(\rho)$

Since Nat is stateful,
if it saw $g(x)$ once already,
just ignore future queries that contain $\boldsymbol{g(x)}$**.**



Small Games, Large World

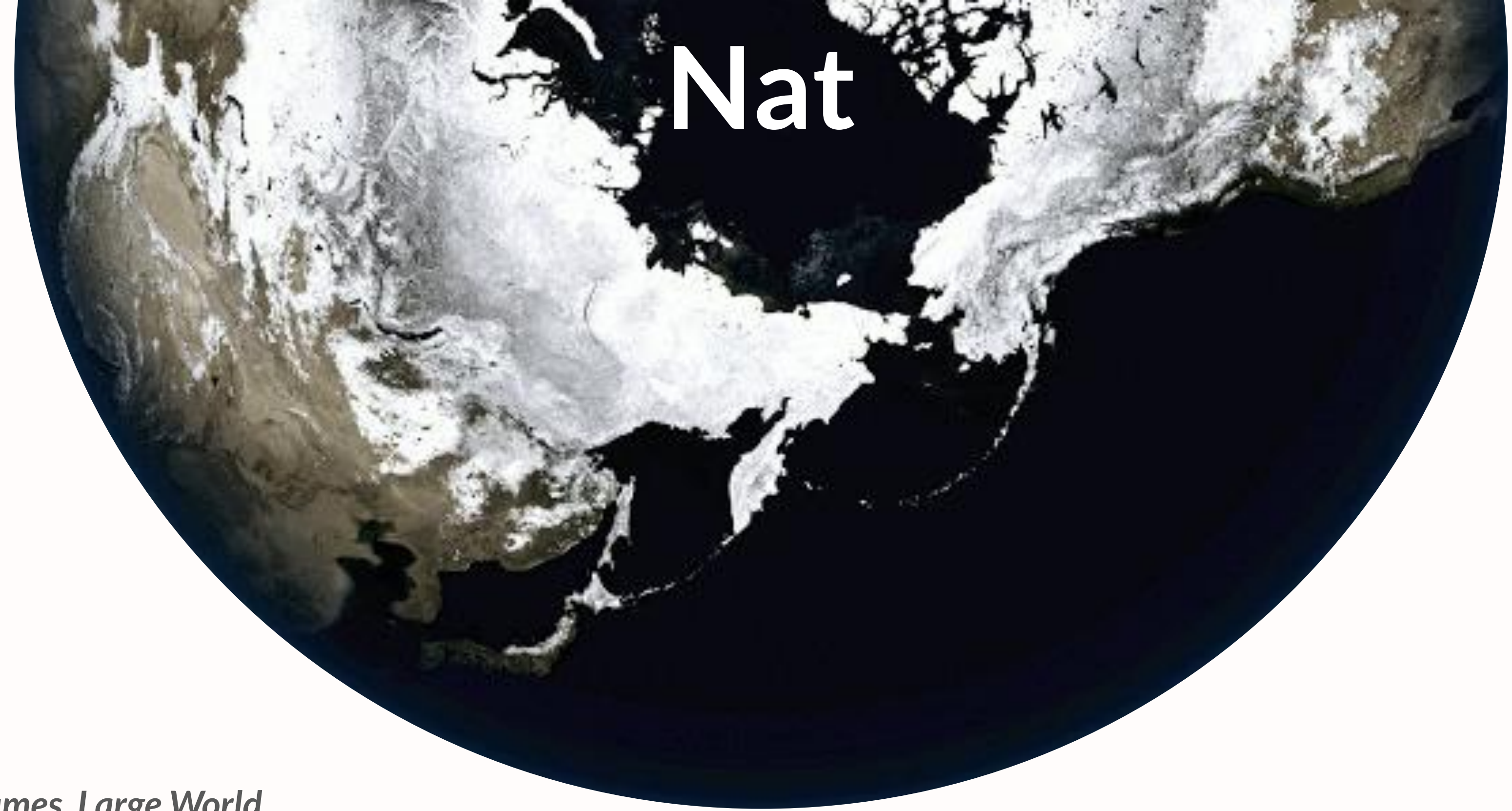
It may be presumptuous to think that **C** or **A** can *influence* the future behavior of **Nat**.

$\updownarrow$

A

$\updownarrow$

C



A

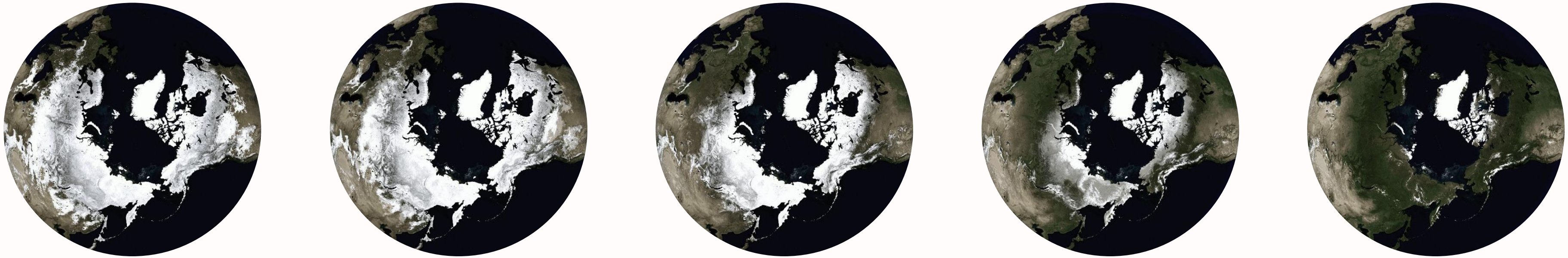
C

<u>Small Games, Large World</u>

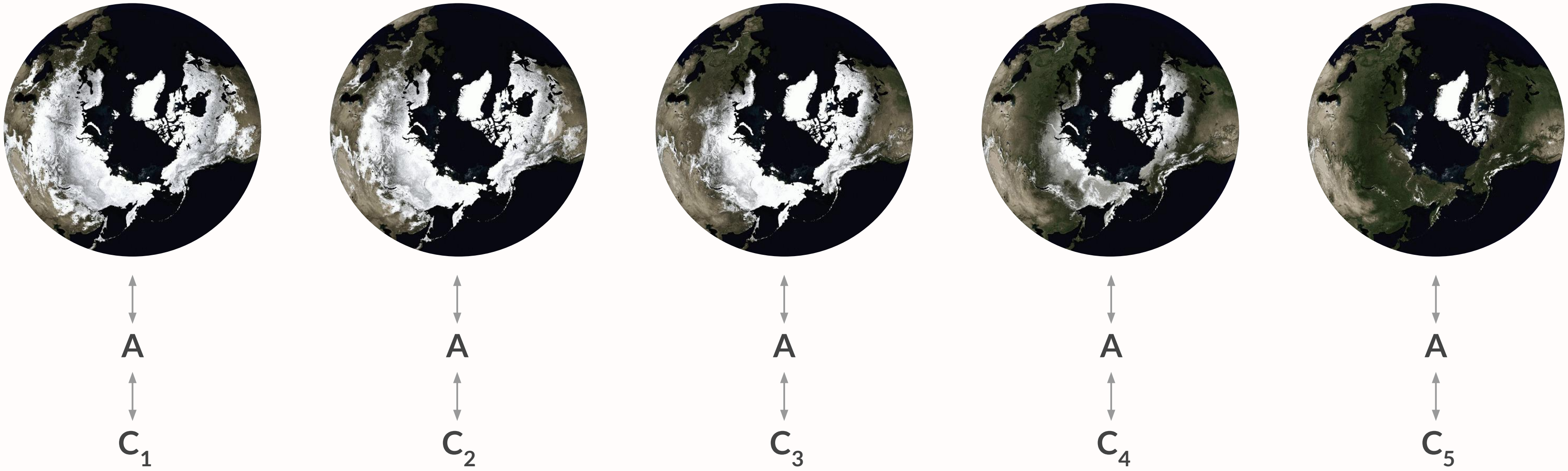
It may be presumptuous to think that **C** or **A** can *influence* the future behavior of **Nat**.

What if Nat plays every game independently, the same way? “Restartable”, and *classic*.

maybe **Nat** evolves over time...



maybe **Nat** evolves over time...



...the same way regardless of any interaction we have with it.

Let's formalize it.

Def: (**A**, **Nat**) is μ-weakly restartable if ∃ **Sim** s.t. ∀λ, ∀C, ∀ interaction prefixes ρ,

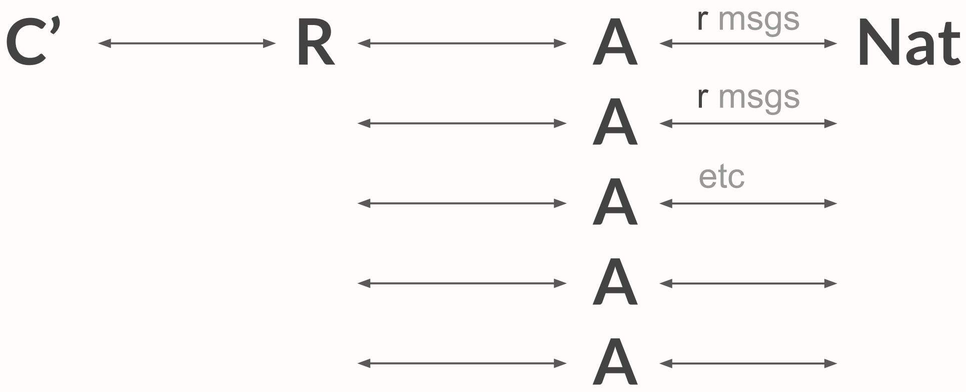
$$C \leftrightarrow A \leftrightarrow \mathrm{Nat}(\rho) \overset{\mu(\lambda)}{\approx} C \leftrightarrow \mathrm{Sim}(\overbrace{|\rho|}^{\text{Number of messages in } \rho})$$

statistical distance

"Simulator"
any distribution

In other words, the behavior of (A, Nat) in the view of any C is pre-programmed and depends only on |ρ|.

Regular Cosmic Adversaries



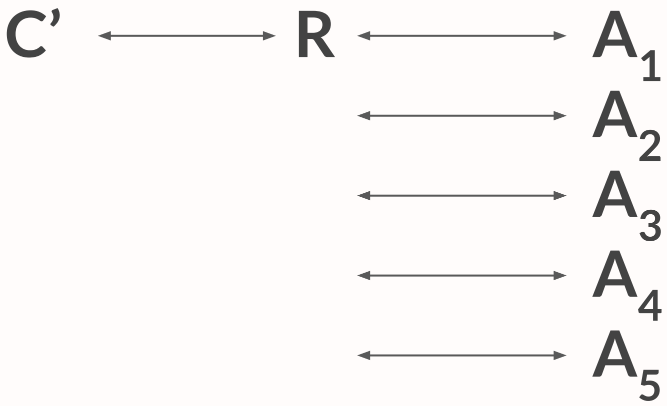
Weakly-Restartable Cosmic Adversaries

(**A**, **Nat**) is now a sequence of attackers **Sim**(0), **Sim**(1), **Sim**(2), …

$$\begin{tikzcd}
\mathbf{C'} \arrow[r, leftrightarrow] & \mathbf{R} \arrow[r, leftrightarrow] & \mathbf{Sim}(0) \\
& {} \arrow[r, leftrightarrow] & \mathbf{Sim}(r) \\
& {} \arrow[r, leftrightarrow] & \mathbf{Sim}(2r) \\
& {} \arrow[r, leftrightarrow] & \mathbf{Sim}(3r) \\
& {} \arrow[r, leftrightarrow] & \mathbf{Sim}(4r)
\end{tikzcd}$$

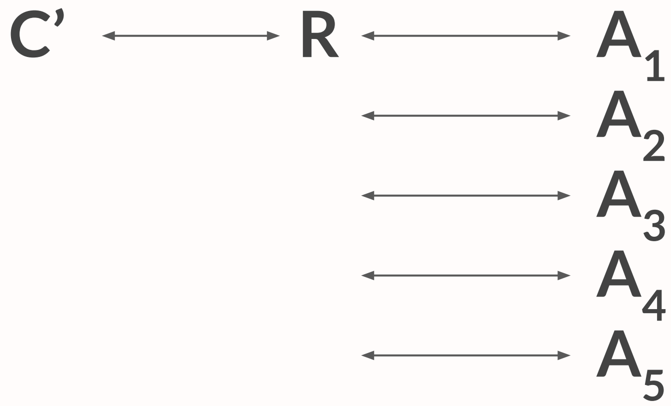
Weakly-Restartable Cosmic Adversaries

(**A**, **Nat**) is now a sequence of attackers $\mathbf{A_1}$ $\mathbf{A_2}$ $\mathbf{A_3}$ ...



Weakly-Restartable Cosmic Adversaries

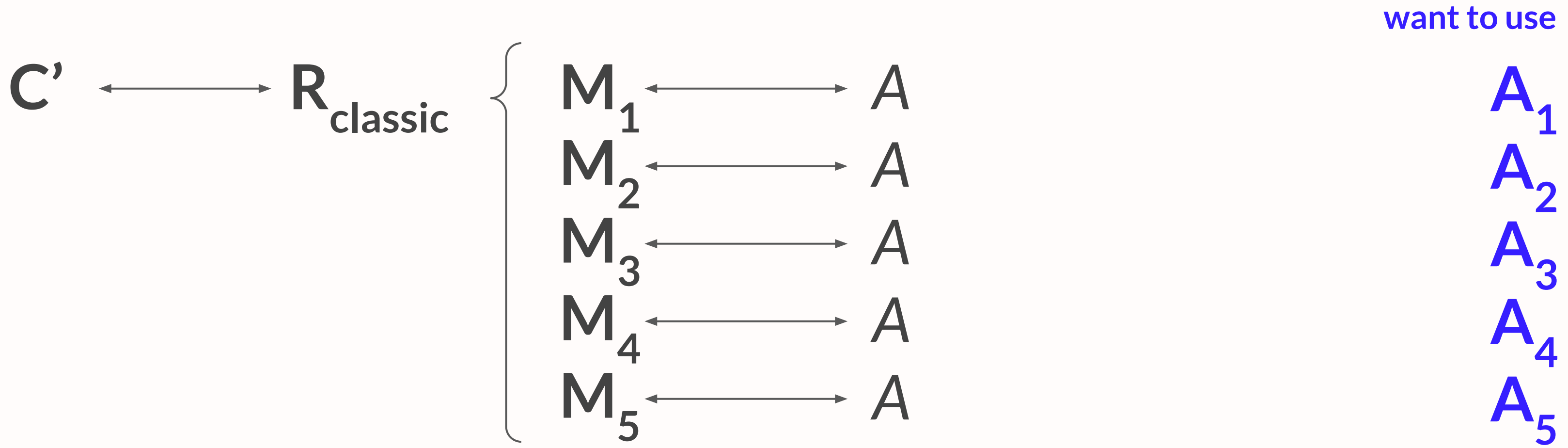
(**A**, **Nat**) is now a sequence of attackers **A_1 A_2 A_3 …** (informal)



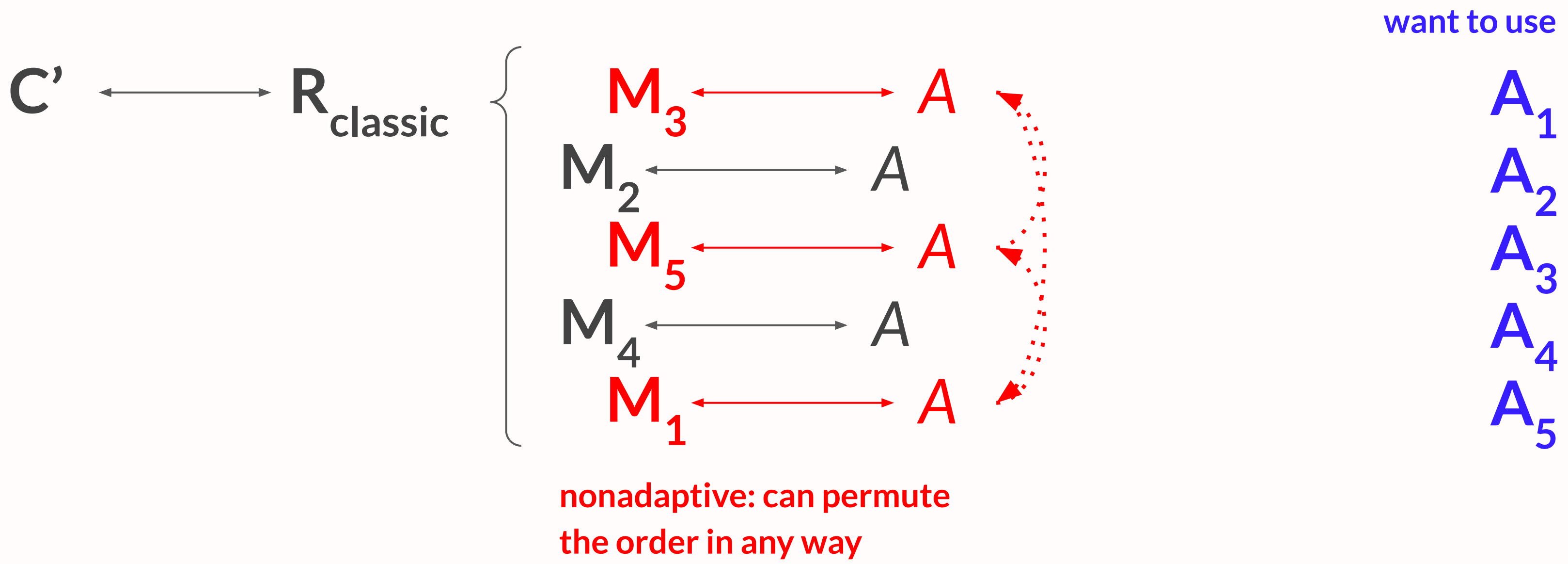
Theorem: Suppose there is a **non-adaptive** (straight-line black-box) reduction $\mathbf{R}_{\mathbf{classic}}$ from **C** to **C'**.
Then there is a cosmic reduction from **C** to **C'**, assuming (**A**, **Nat**) is weakly restartable.

Corollaries: Hardcore Bits from OWFs, Hardness Amplification.

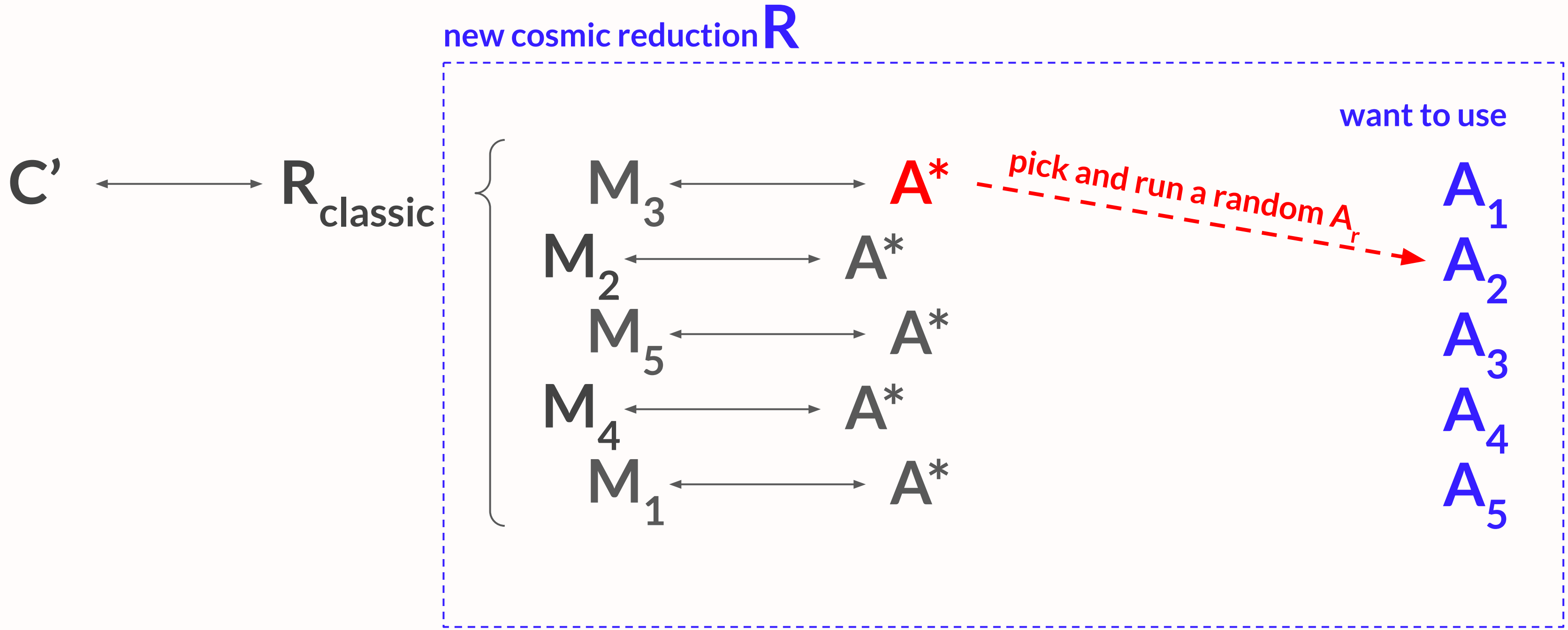
Theorem: Suppose there is a **non-adaptive** (straight-line black-box) reduction $\mathbf{R}_{\text{classic}}$ from **C** to **C'**.
Then there is a cosmic reduction from **C** to **C'**, assuming (**A**, **Nat**) is weakly restartable.



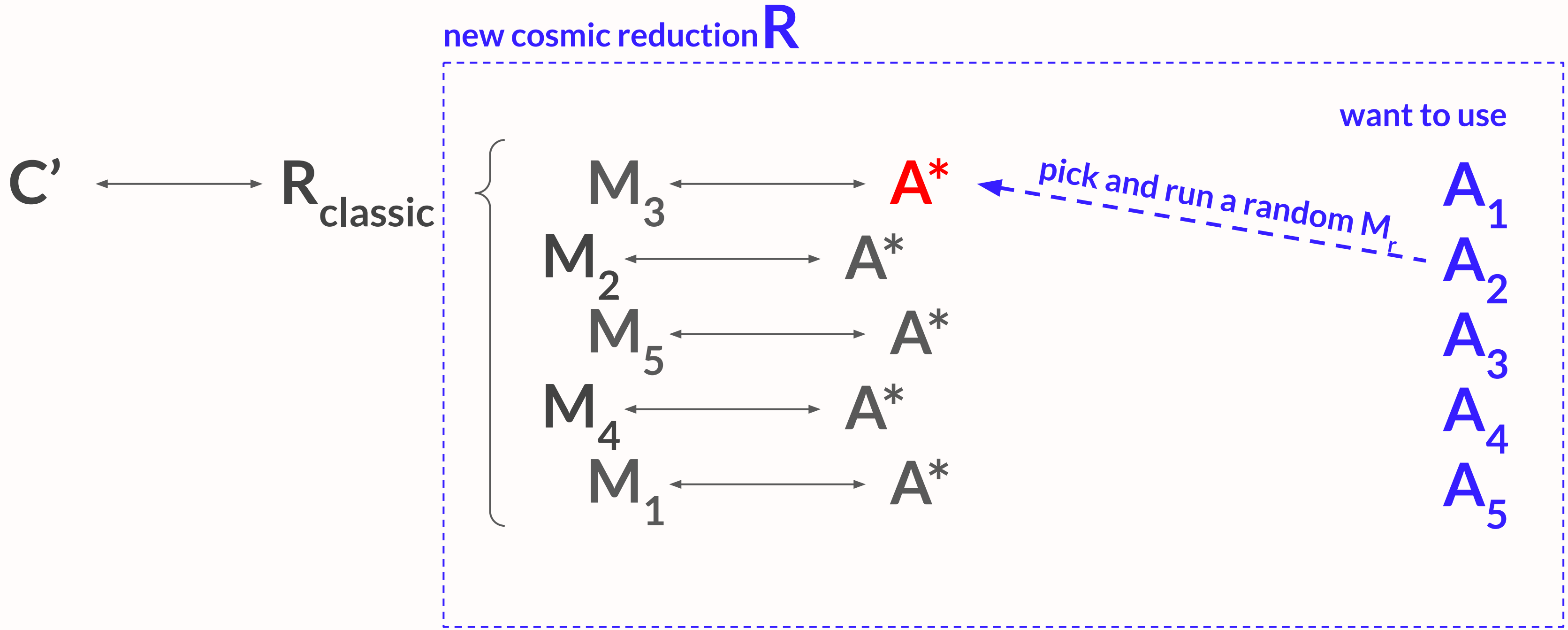
Theorem: Suppose there is a **non-adaptive** (straight-line black-box) reduction $\mathbf{R}_{\text{classic}}$ from **C** to **C'**.
Then there is a cosmic reduction from **C** to **C'**, assuming (**A**, **Nat**) is weakly restartable.



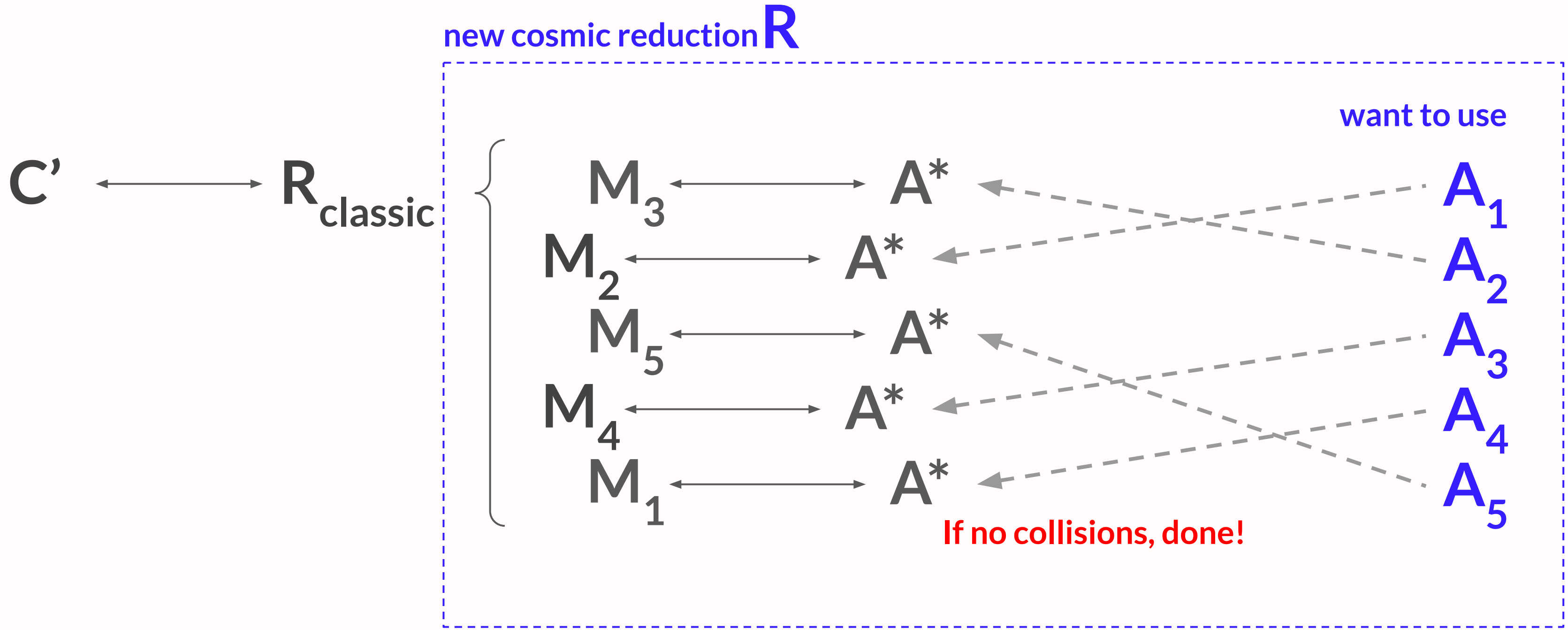
Theorem: Suppose there is a non-adaptive (straight-line black-box) reduction $\mathbf{R}_{\text{classic}}$ from **C** to **C'**.
Then there is a cosmic reduction from **C** to **C'**, assuming (**A**, **Nat**) is weakly restartable.



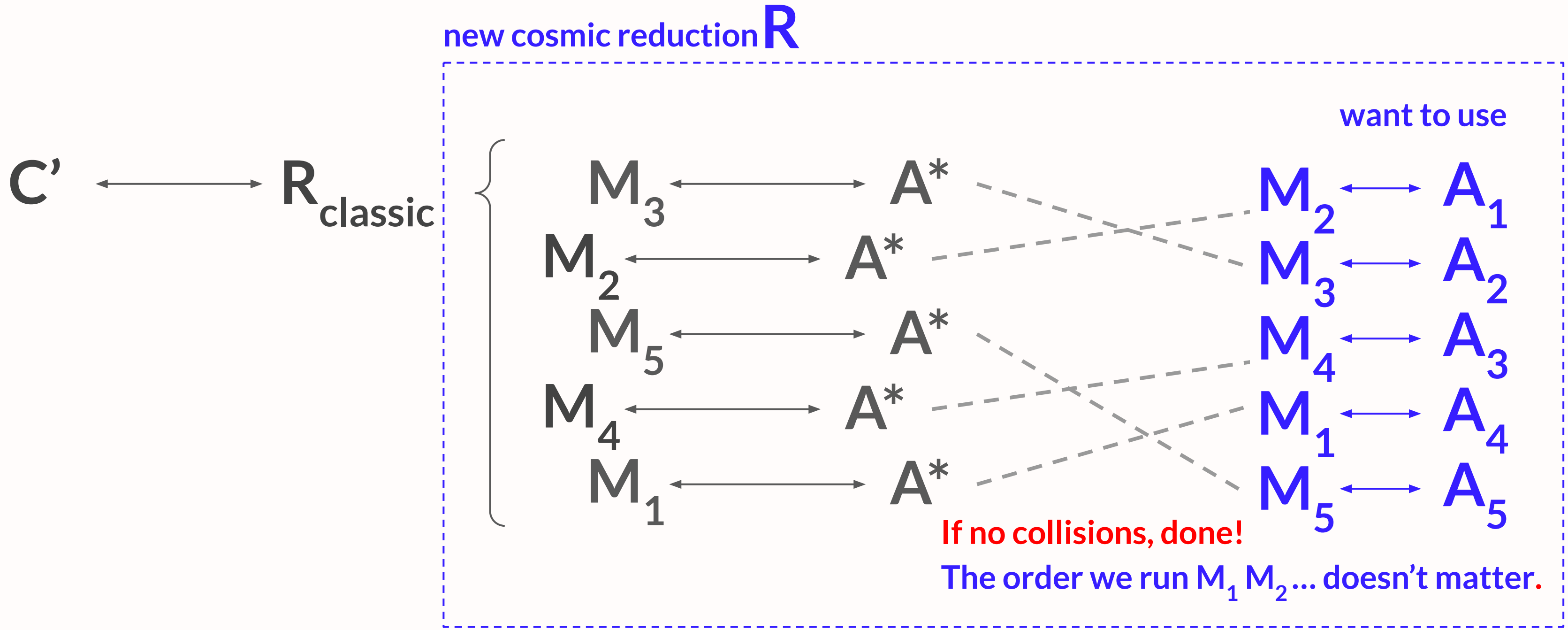
Theorem: Suppose there is a non-adaptive (straight-line black-box) reduction $\mathbf{R}_{\text{classic}}$ from **C** to **C'**. Then there is a cosmic reduction from **C** to **C'**, assuming (**A**, **Nat**) is weakly restartable.



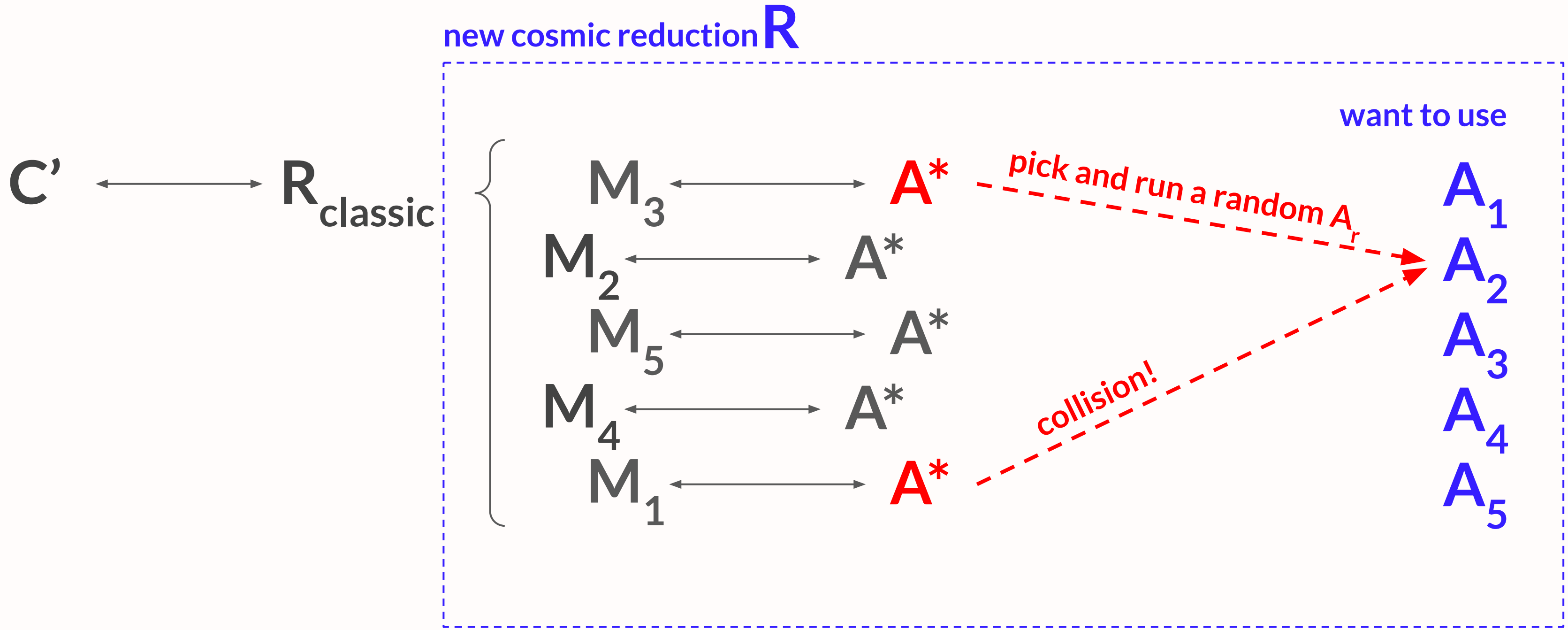
Theorem: Suppose there is a non-adaptive (straight-line black-box) reduction $\mathbf{R}_{\text{classic}}$ from **C** to **C'**. Then there is a cosmic reduction from **C** to **C'**, assuming (**A**, **Nat**) is weakly restartable.



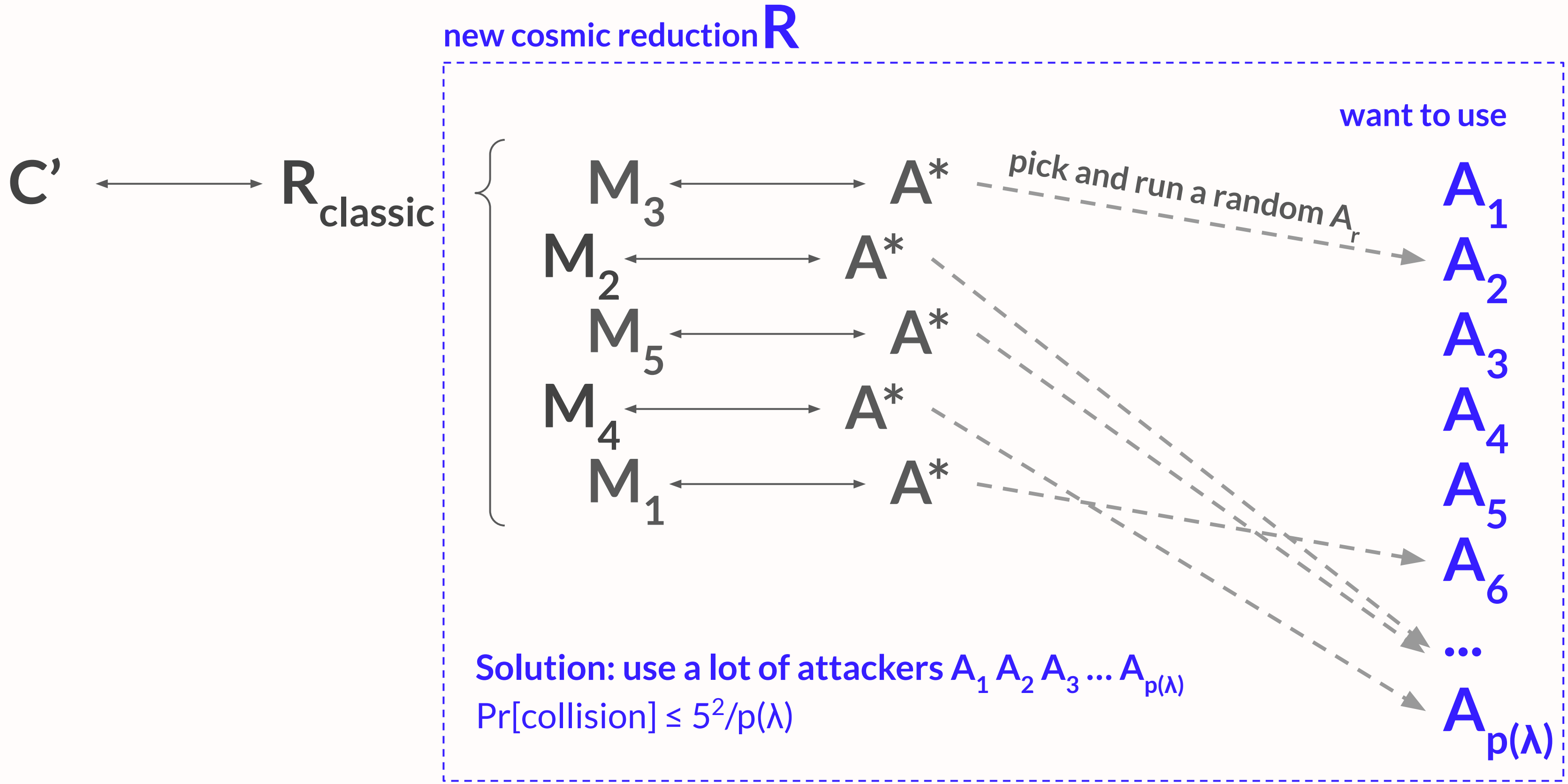
Theorem: Suppose there is a non-adaptive (straight-line black-box) reduction $\mathbf{R}_{\text{classic}}$ from **C** to **C'**. Then there is a cosmic reduction from **C** to **C'**, assuming (**A**, **Nat**) is weakly restartable.



Theorem: Suppose there is a non-adaptive (straight-line black-box) reduction $\mathbf{R}_{\text{classic}}$ from **C** to **C'**. Then there is a cosmic reduction from **C** to **C'**, assuming (**A**, **Nat**) is weakly restartable.



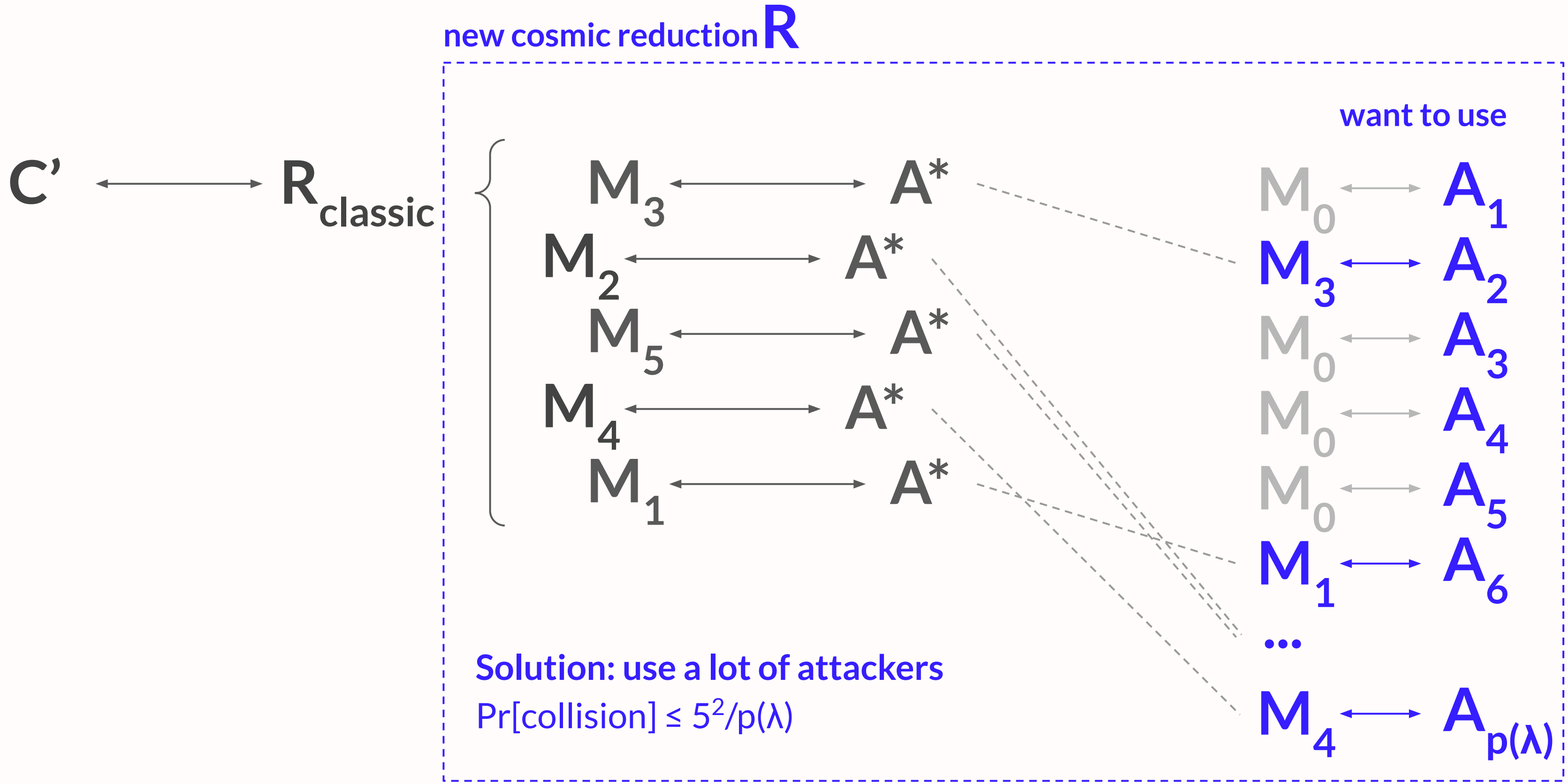
Theorem: Suppose there is a non-adaptive (straight-line black-box) reduction $\mathbf{R}_{\text{classic}}$ from **C** to **C'**.
Then there is a cosmic reduction from **C** to **C'**, assuming (**A**, **Nat**) is weakly restartable.



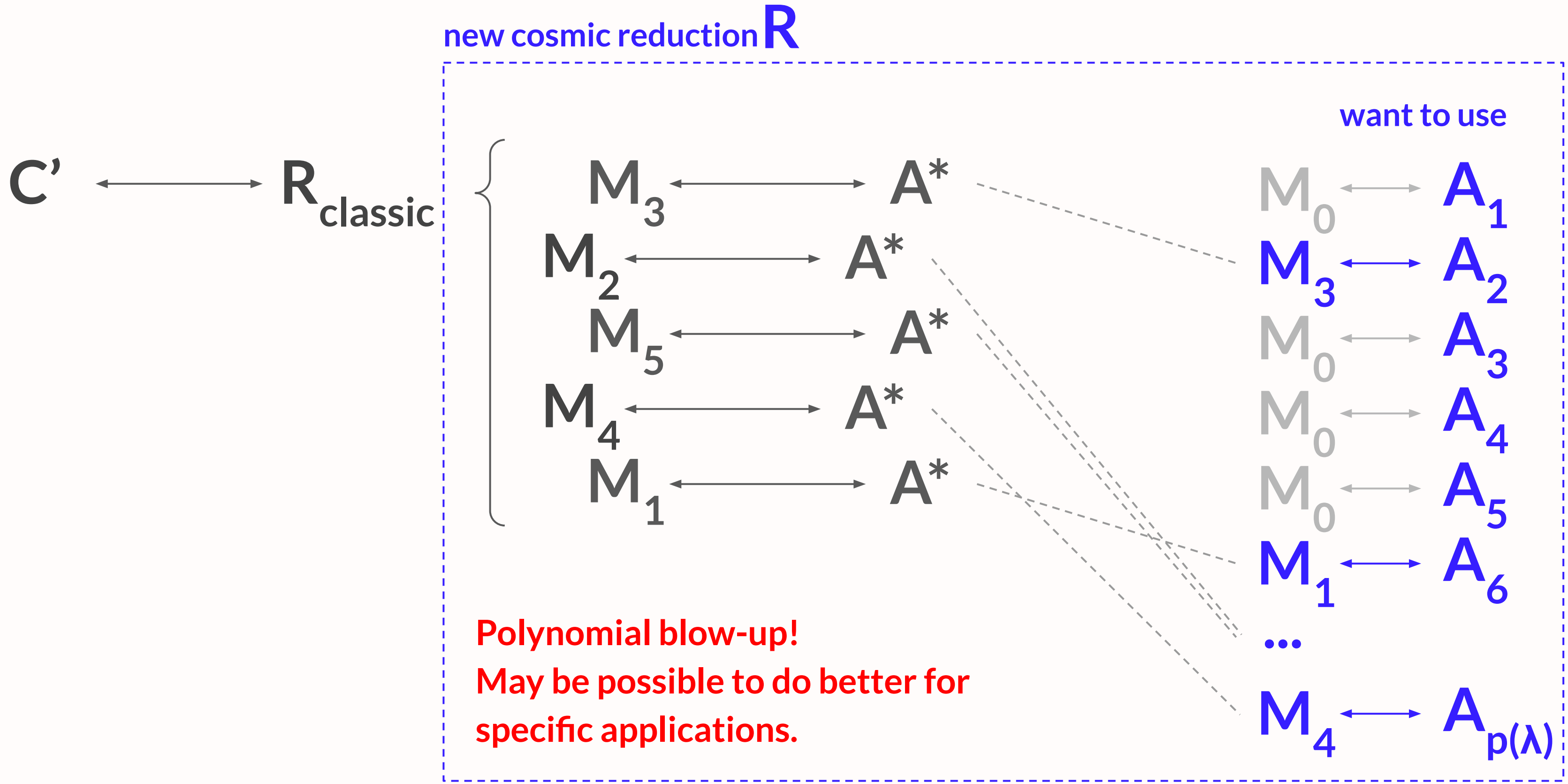
Solution: use a lot of attackers $A_1\ A_2\ A_3 \ldots A_{p(\lambda)}$

Pr[collision] $\leq 5^2/p(\lambda)$

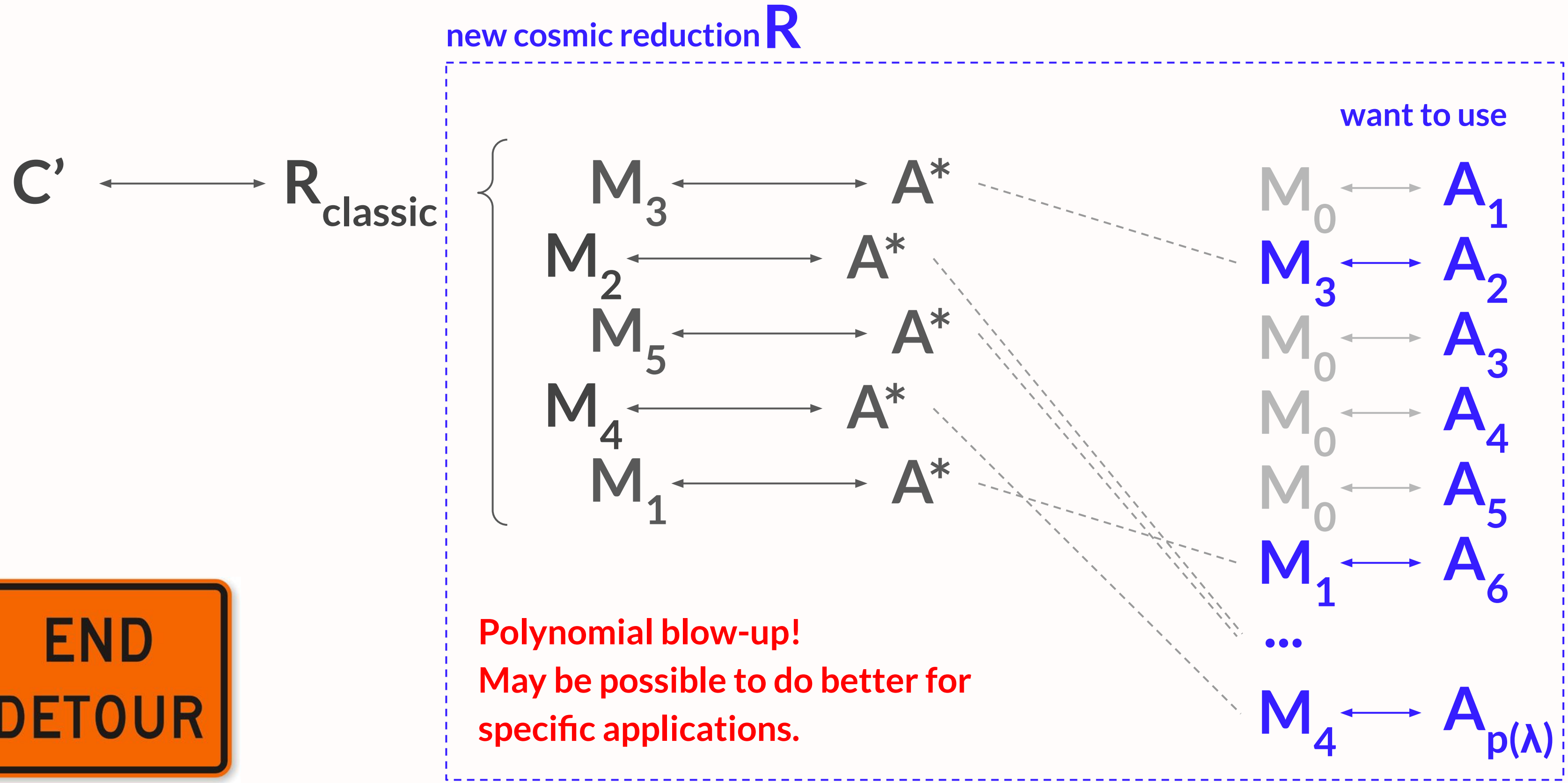
Theorem: Suppose there is a non-adaptive (straight-line black-box) reduction $\mathbf{R}_{\text{classic}}$ from **C** to **C'**. Then there is a cosmic reduction from **C** to **C'**, assuming (**A**, **Nat**) is weakly restartable.



Theorem: Suppose there is a non-adaptive (straight-line black-box) reduction $\mathbf{R}_{\text{classic}}$ from **C** to **C'**. Then there is a cosmic reduction from **C** to **C'**, assuming (**A**, **Nat**) is weakly restartable.



Theorem: Suppose there is a non-adaptive (straight-line black-box) reduction $\mathbf{R}_{classic}$ from **C** to **C'**. Then there is a cosmic reduction from **C** to **C'**, assuming (**A**, **Nat**) is weakly restartable.



Roadmap

1. ~~Motivation~~ *(10min)*
2. ~~Defining Cosmic Security~~ *(15min)*
3. ~~Properties of Cosmic Security: a Sanity Check~~
   a. ~~Composition, Black-box reductions~~ *(5min)*
4. ~~Summary of Key Results~~
   a. ~~Feasibilities and Impossibilities (20min)~~
5. ~~Other Notions of Cosmic Security (10min)~~
6. **Conclusion (5min)**

Let’s wrap it up.

In Sum

It is perhaps surprising that classical
non-adaptive reductions “work” for the
cosmic weakly-restartable “A_1 A_2 A_3” model.

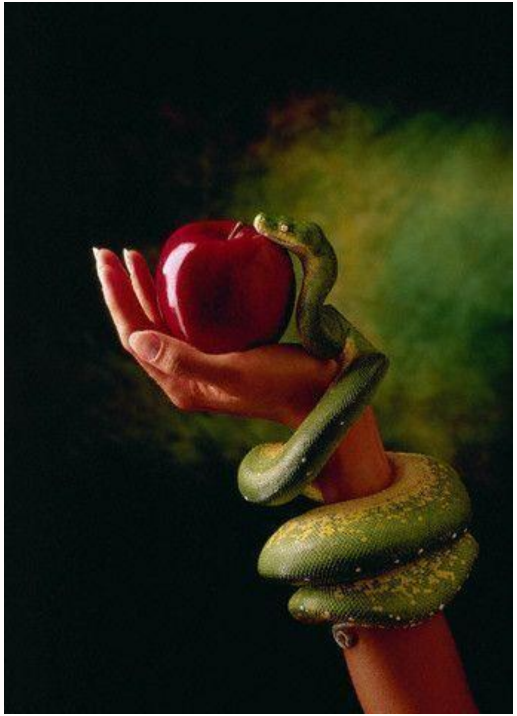
Implication: we can treat slightly stateful Natures
(that keep only time as state) as stateless!
(if we don’t make adaptive queries)

In Greater Sum

For fully stateful Natures,

- Several black-box classical reductions that run the adversary repeatedly on correlated inputs cannot have cosmic equivalents.
- So far, feasibility for cosmic reductions is limited to either re-randomizing correlated queries, or sticking to one-shot reductions.

In Greater, Greater Sum



Biggest Takeaway: we should consider stateful adversaries that may behave differently each time its run.

What’s Next?
An Unexplored Universe.

- PRGs from OWFs?
- MPC?
- New techniques to deal with a stateful Cosmos?

What's Next?
An Unexplored Universe.

- **PRGs from OWFs?**
- **MPC?**
- **New techniques to deal with a stateful Cosmos?**

Thank You!

Image Credits: NASA/ESA/Hubble

Extra Slides