On the correlation intractability of obfuscated pseudorandom functions

Ran Canetti, Yilei Chen, Leonid Reyzin

CIS seminar
December 4, 2015

BOSTON UNIVERSITY
אוניברסיטת תל-אביב
TEL AVIV UNIVERSITY

Trailer

The Heuristic

Random Oracle

THE ASSASSINATION

Random Oracles don't exist

THE "MURDERER"

“Correlation Intractability”

(a property of Random Oracle)

The Redemption

Correlation Intractability

Correlation Intractability is achievable

Correlation Intractability is achievable (in some cases)

Starring

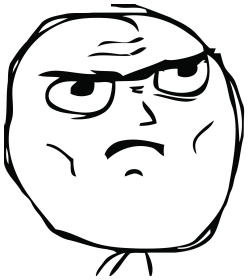
Puncturable Pseudorandom Functions

Indistinguishability Obfuscator

Input Hiding Obfuscator

(for evasive circuit families)

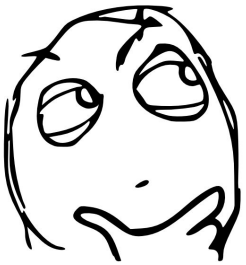
Miner



Adversary

(guest appearance: simulator)

Jackie Chan



Crypto student

(guest appearance: adversary)

Two Italians and a door

Directors

Ran Canetti

Yilei Chen

Leonid Reyzin

Act I

A: Please.

A: Please.

B: Please.

A: Please.

B: Please.

A: I insist.

A: Please.

B: Please.

A: I insist.

B: So do I.

…

A: Please.

B: Please.

A: I insist.

B: So do I.

…

"A protocol for two Italians to pass through a door. "

Source: Silvio Micali, 1985. In *Foundations of Cryptography, V2*, page 784, Oded Goldreich, originally used to demonstrate what is zero-knowledge. Photo credit: Oded's slides.

A: Please.

B: Please.

A: I insist.

B: So do I.

…

"A protocol for two Italians to pass through a door. "

Source: Silvio Micali, 1985. In *Foundations of Cryptography, V2*, page 784, Oded Goldreich, originally used to demonstrate what is zero-knowledge. Photo credit: Oded's slides.

Fiat-Shamir ‘86, Bellare-Rogaway ‘93:

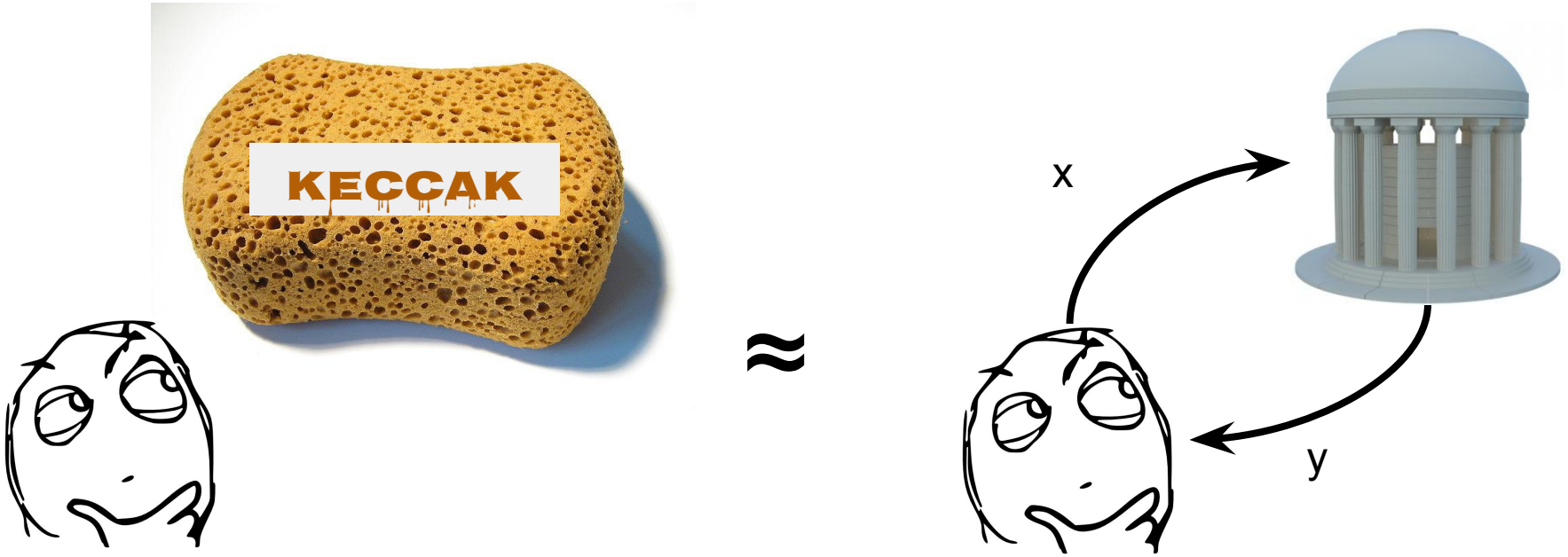
Can model cryptographic hash functions as “Random Oracles”

Fiat-Shamir ‘86, Bellare-Rogaway ‘93:

Can model cryptographic hash functions as “Random Oracles”

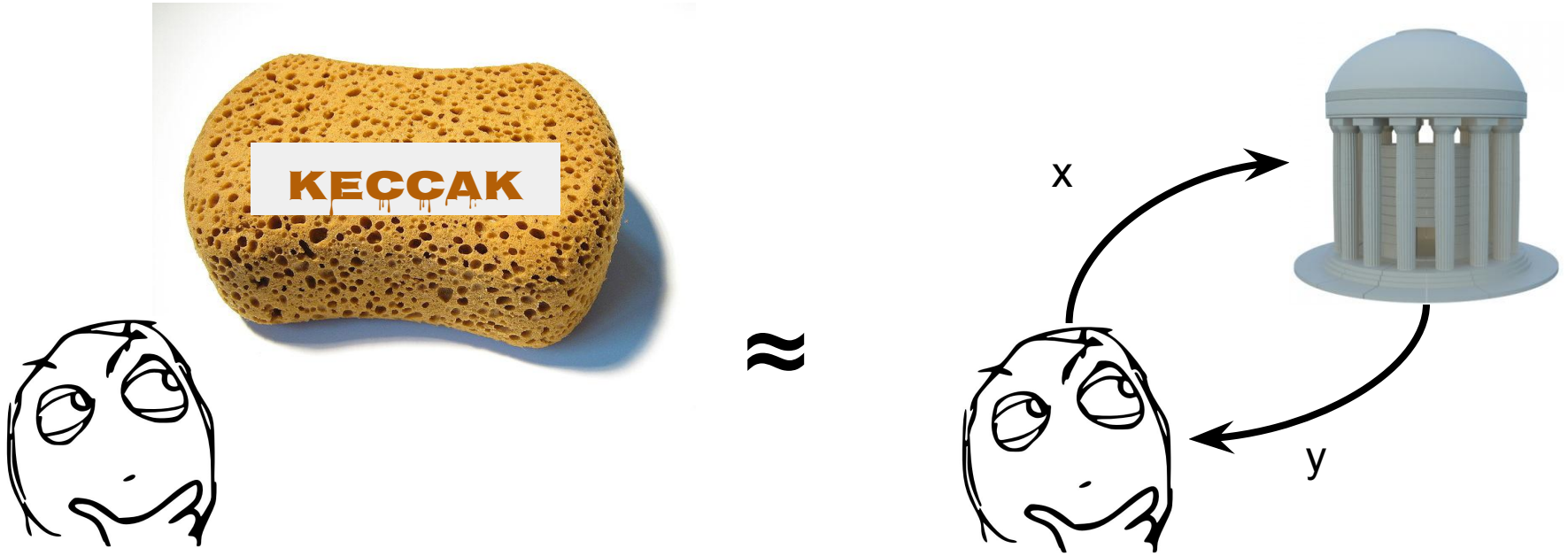
Fiat-Shamir ‘86, Bellare-Rogaway ‘93:

Can model cryptographic hash functions as “Random Oracles”



Fiat-Shamir ‘86, Bellare-Rogaway ‘93:

Can model cryptographic hash functions as “Random Oracles”

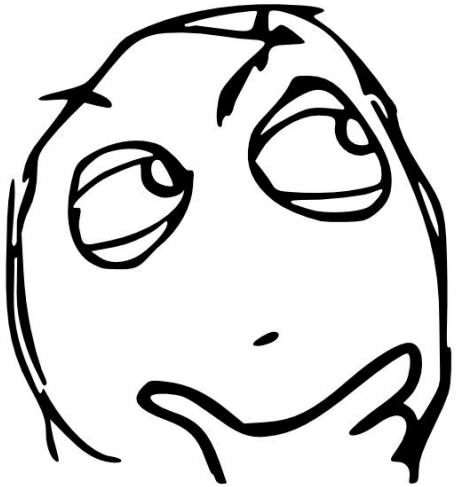


Build efficient crypto schemes (secure under heuristics):

- Efficient CCA secure encryptions
- Hash-and-sign paradigm
- Many applications

$h: \{0,1\}^l \rightarrow \{0,1\}^m$

looks like Random Oracle?



Crypto student

One of the properties held by Random Oracles is

Correlation Intractability

"infeasibility of finding 'sparse' input-output relations"

Sparse Relations

"For each input (x),
the fraction of outputs (y) in the relation is negligible"

Sparse Relations

"For each input (x),
the fraction of outputs (y) in the relation is negligible"

Implicit definition: hard for Random Oracles

For all (non-uniform) p.p.t. Adversary:

$$\text{Prob}_{\text{Adv, O}}[\ \text{Adv}^{O} \rightarrow x: R(x, O(x))=1\ ] < \text{negl}.$$

Sparse Relations

"For each input (x),
the fraction of outputs (y) in the relation is negligible"

Implicit definition: hard for Random Oracles

For all (non-uniform) p.p.t. Adversary:

$$\text{Prob}_{\text{Adv, O}}[\ \text{Adv}^{O} \rightarrow x: R(x, O(x))=1\ ] < \text{negl}.$$

*Can naturally generalize to multi-input-output relations

For all (non-uniform) p.p.t. Adversary:

$$\text{Prob}_{\text{Adv, O}}[\ \text{Adv}^{O} \rightarrow x1, x2: R(x1, O(x1), x2, O(x2))=1\ ] < \text{negl}.$$

Sparse Relations

"For each input (x),
the fraction of outputs (y) in the relation is negligible"

Examples: Interesting sparse relations

Sparse Relations

"For each input (x),
the fraction of outputs (y) in the relation is negligible"

Examples: Interesting sparse relations

Constant relation: R(x, y) = 1, if y=c

Sparse Relations

"For each input (x),
the fraction of outputs (y) in the relation is negligible"

Examples: Interesting sparse relations

Constant relation: R(x, y) = 1, if y=c
Partial constant relation: R(x, y) = 1, if the first half of y=c'

Sparse Relations

"For each input (x),
the fraction of outputs (y) in the relation is negligible"

Examples: Interesting sparse relations

Constant relation: R(x, y) = 1, if y=c
Partial constant relation: R(x, y) = 1, if the first half of y=c'
"Elliptic-curve" relation: R(x, y) = 1, if $y^2 = x^3$-ax+b

Sparse Relations

"For each input (x),
the fraction of outputs (y) in the relation is negligible"

Examples: Interesting sparse relations

Constant relation: $R(x, y) = 1$, if $y=c$
Partial constant relation: $R(x, y) = 1$, if the first half of $y=c'$
"Elliptic-curve" relation: $R(x, y) = 1$, if $y^2 = x^3-ax+b$
"Wild strawberry" relation: $R(x, y) = 1$, if $ax+|x+1|y-c^x = d$

Sparse Relations

"For each input (x),
the fraction of outputs (y) in the relation is negligible"

Examples: Interesting sparse relations

Constant relation: R(x, y) = 1, if y=c
Partial constant relation: R(x, y) = 1, if the first half of y=c'
"Elliptic-curve" relation: R(x, y) = 1, if $y^2 = x^3-ax+b$
"Wild strawberry" relation: R(x, y) = 1, if $ax+|x+1|y-c^x = d$

*Examples for interesting multi-input-output relations

Collision relation: R(x1, y1, x2, y2) = 1, if y1=y2 and (not x1=x2)

Sparse Relations

"For each input (x),
the fraction of outputs (y) in the relation is negligible"

Sparse Relations

"For each input (x),
the fraction of outputs (y) in the relation is negligible"

Correlation intractability [Canetti, Goldreich, Halevi '98]

Sparse Relations

"For each input (x),
the fraction of outputs (y) in the relation is negligible"

Correlation intractability [Canetti, Goldreich, Halevi '98]

Adversary Challenger

Sparse Relations

"For each input (x),
the fraction of outputs (y) in the relation is negligible"

Correlation intractability [Canetti, Goldreich, Halevi '98]

For all sparse relations R:

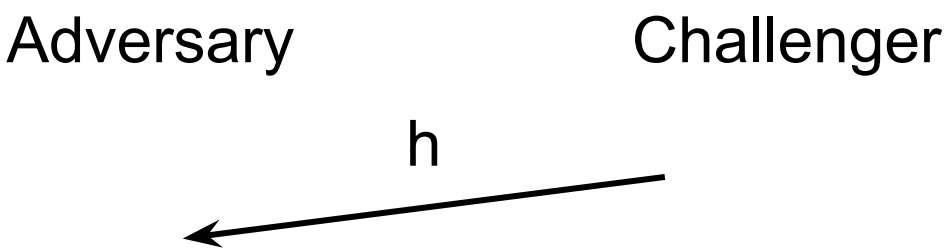
Adversary Challenger

Sparse Relations

"For each input (x),
the fraction of outputs (y) in the relation is negligible"

Correlation intractability [Canetti, Goldreich, Halevi '98]

For all sparse relations R:

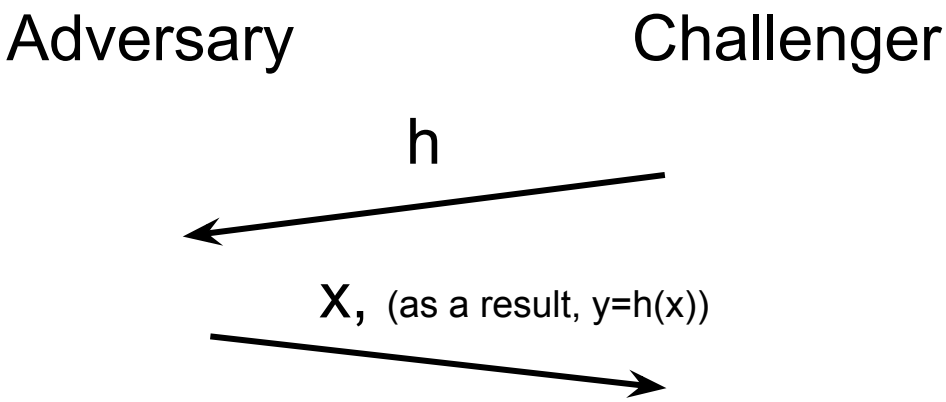


Sparse Relations

"For each input (x),
the fraction of outputs (y) in the relation is negligible"

Correlation intractability [Canetti, Goldreich, Halevi '98]

For all sparse relations R:

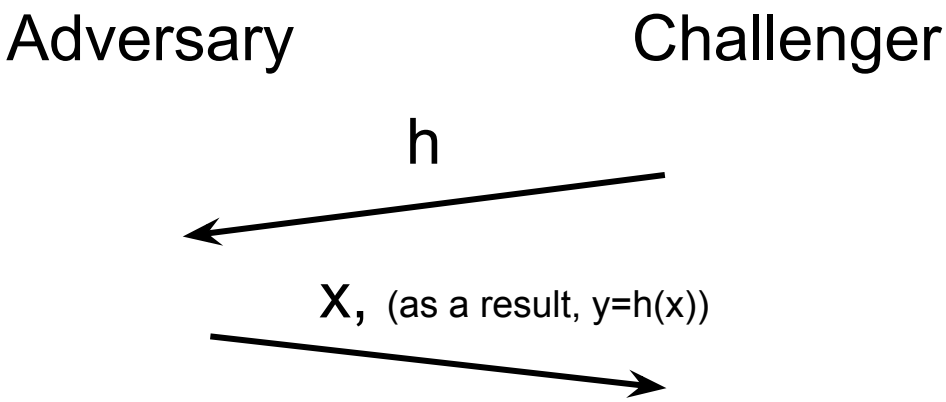


Sparse Relations

"For each input (x),
the fraction of outputs (y) in the relation is negligible"

Correlation intractability [Canetti, Goldreich, Halevi '98]

For all sparse relations R:

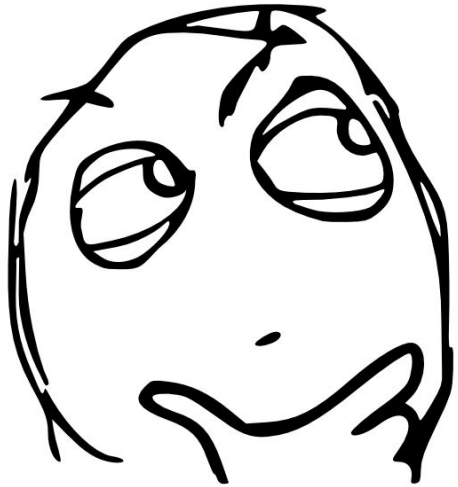


Adversary wins if R(x, y)=1

H(???...?)=000000….XYZ3d83h

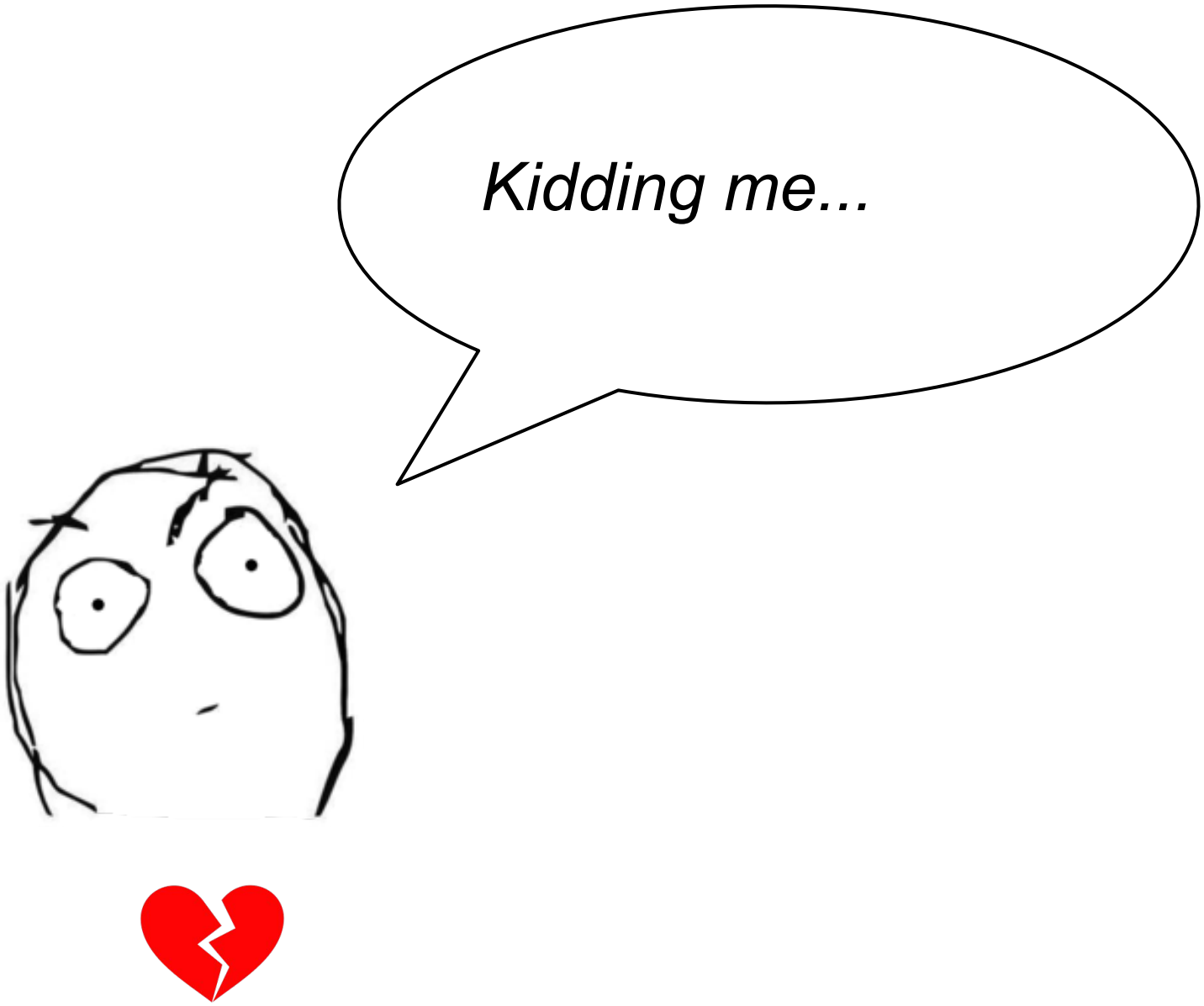
H(???...?)=000000….XYZ3d83h

Looks cool!
But … how to construct?



Canetti, Goldreich, Halevi 1998:

Correlation Intractability is impossible to obtain

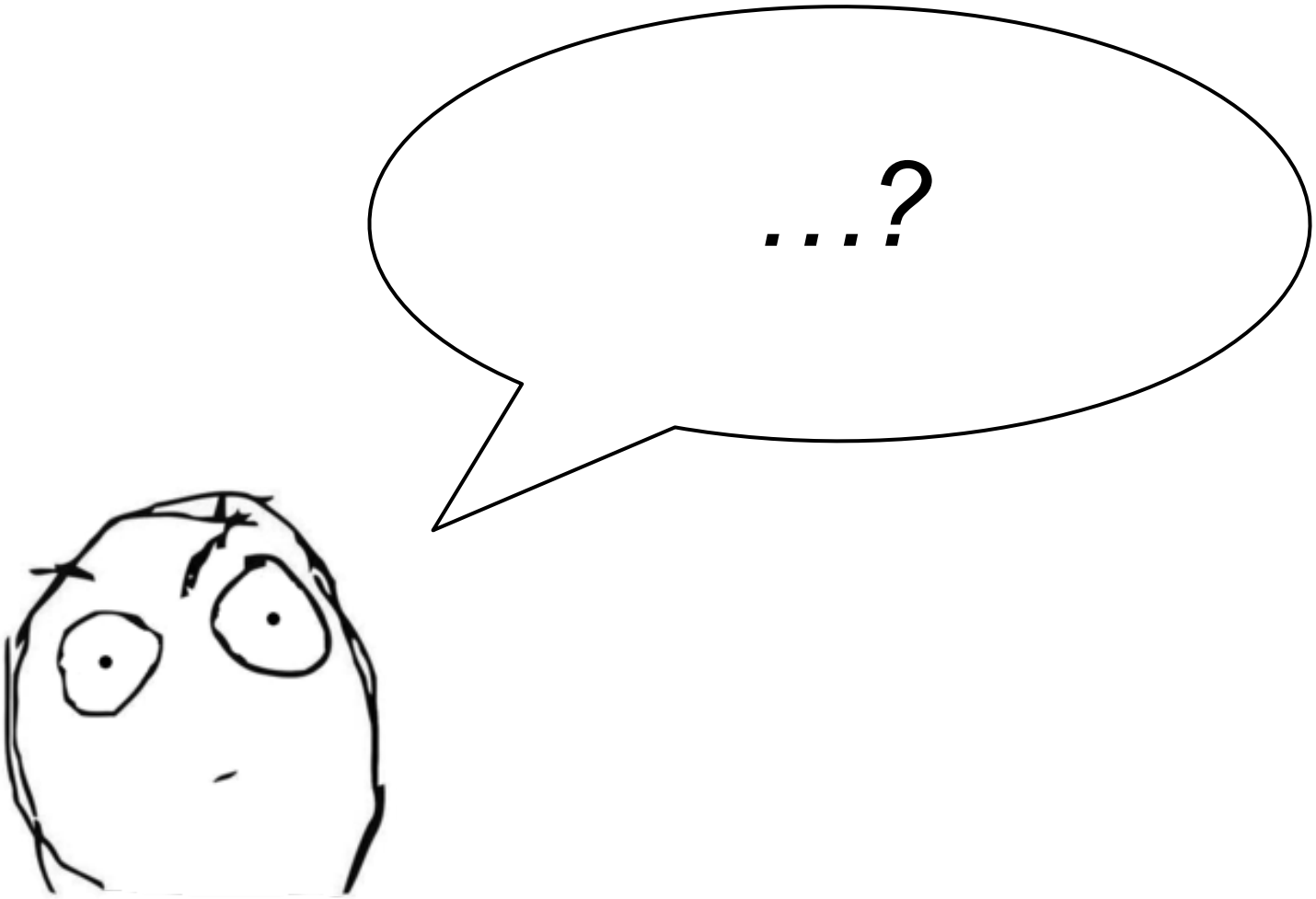

Kidding me...

Canetti, Goldreich, Halevi 1998:

Correlation Intractability is impossible to obtain

Canetti, Goldreich, Halevi 1998:

Correlation Intractability is impossible to obtain … in some cases



Canetti, Goldreich, Halevi:

H cannot be correlation intractable if **the key is short** !!!

Canetti, Goldreich, Halevi:

H cannot be correlation intractable if **the key is short** !!!

Consider the “Diagonal” relation:

$$R^H(x, y)=1 \text{ iff } y=x(x)$$

Canetti, Goldreich, Halevi:

H cannot be correlation intractable if **the key is short** !!!

Consider the "Diagonal" relation:

$$R^H(x, y)=1 \text{ iff } y=x(x)$$

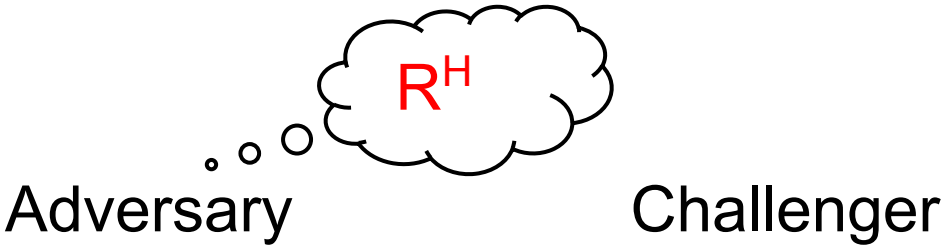
Adversary Challenger

Canetti, Goldreich, Halevi:

H cannot be correlation intractable if **the key is short** !!!

Consider the "Diagonal" relation:

$$R^H(x, y)=1 \text{ iff } y=x(x)$$

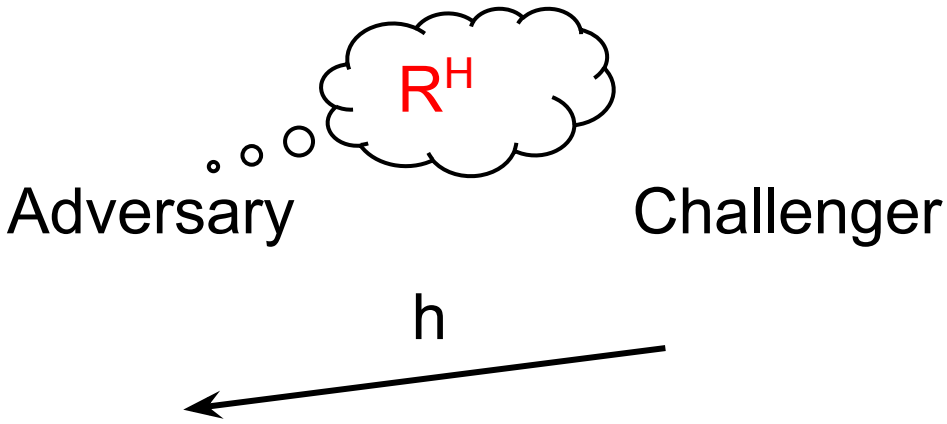


Canetti, Goldreich, Halevi:

H cannot be correlation intractable if **the key is short** !!!

Consider the "Diagonal" relation:

$$R^H(x, y)=1 \text{ iff } y=x(x)$$

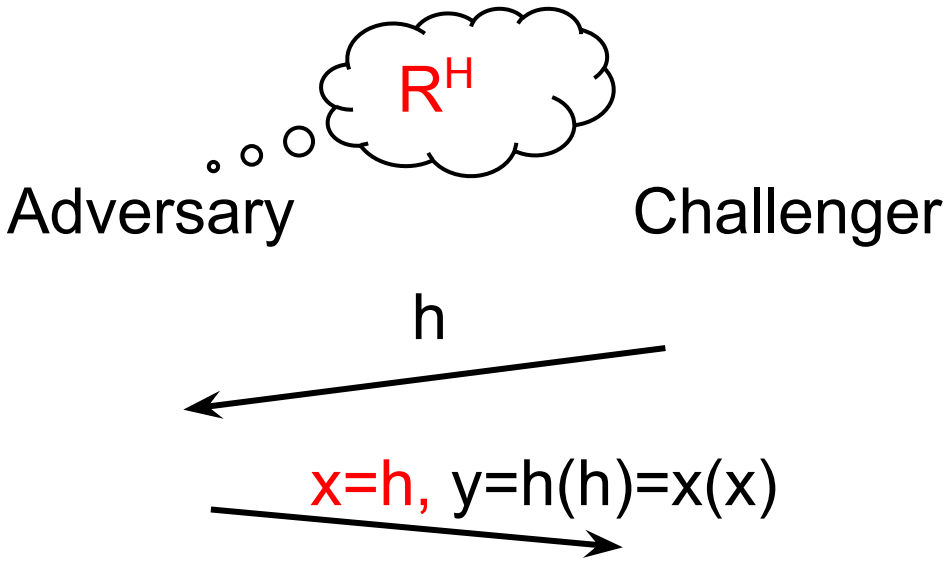


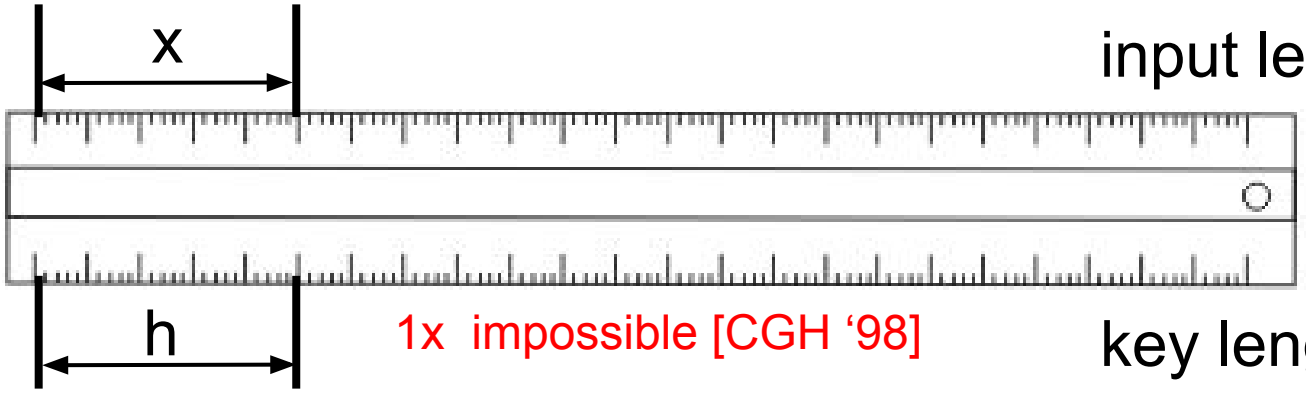
Canetti, Goldreich, Halevi:

H cannot be correlation intractable if **the key is short** !!!

Consider the "Diagonal" relation:

$R^H(x, y)=1$ iff $y=x(x)$

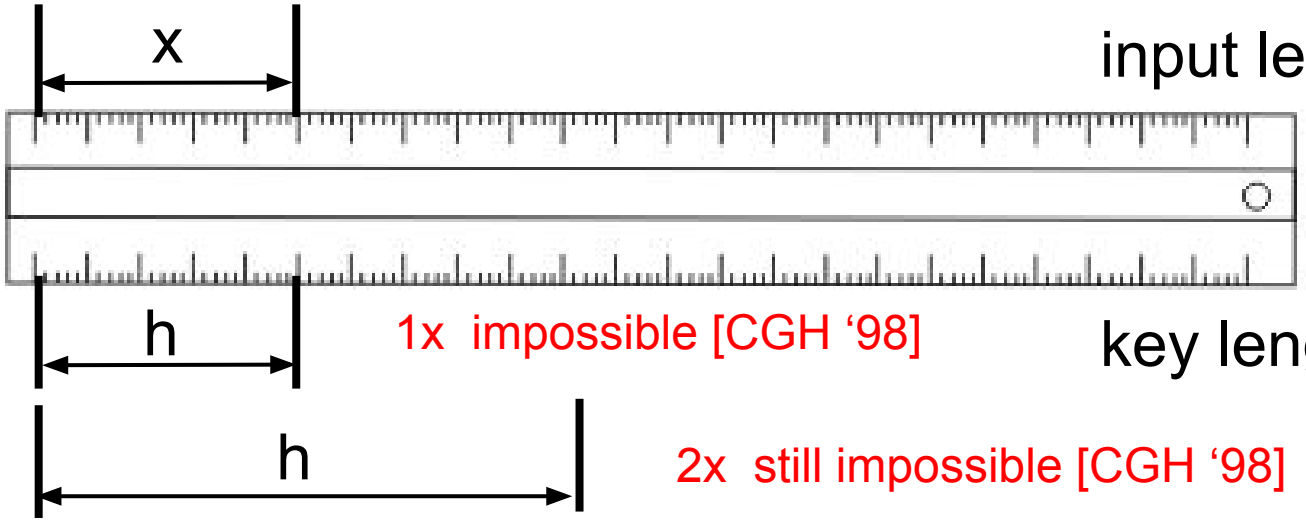


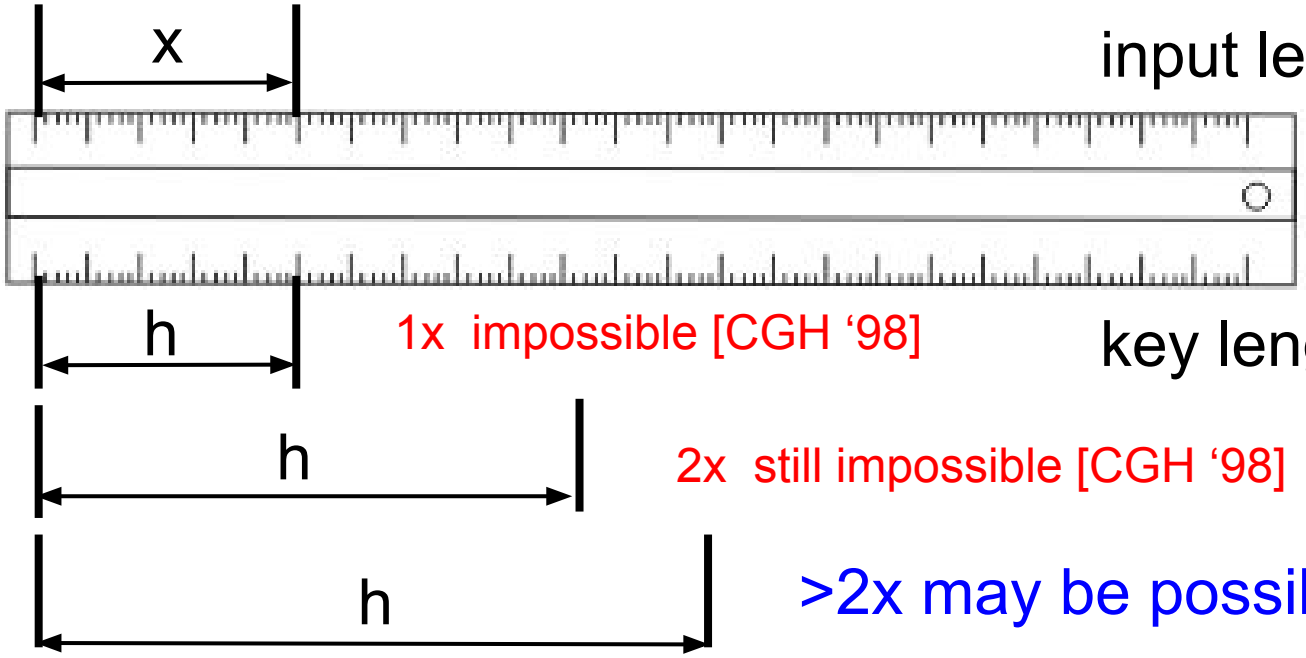


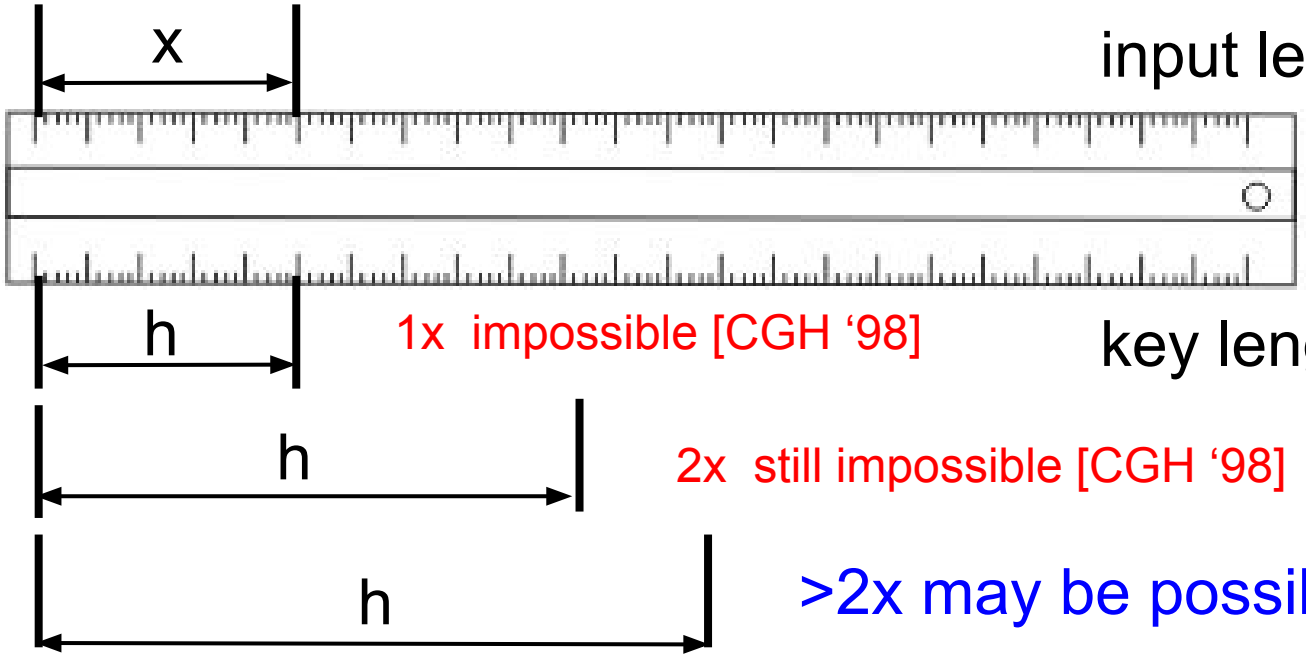
input length

1x impossible [CGH ‘98]

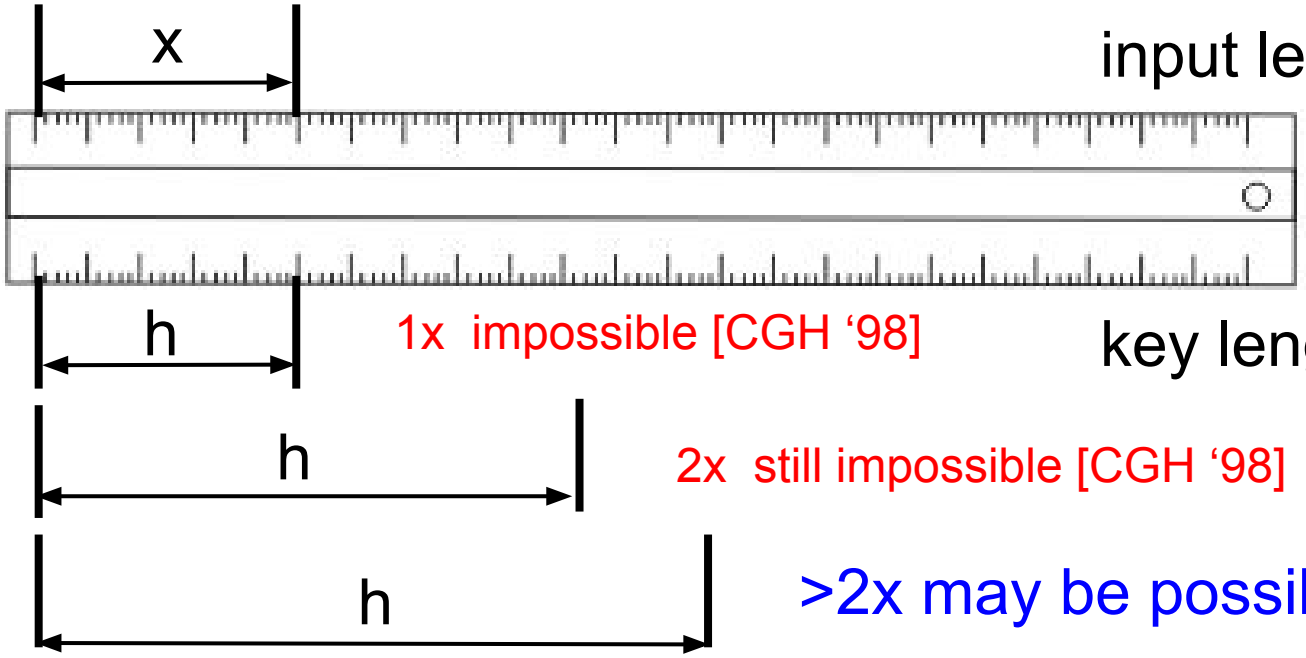
key length


x
input length
h
1x impossible [CGH '98]
key length
h
2x still impossible [CGH '98]


x
input length
h
1x impossible [CGH '98]
key length
h
2x still impossible [CGH '98]
h
>2x may be possible!!



Possible for hash functions with even just 'slightly' longer keys… not too bad.



Possible for hash functions with even just 'slightly' longer keys… not too bad.

Functions from $\{0,1\}^* \rightarrow \{0,1\}^m$ can never be correlation intractable.

(Widely) Open problem

since 1998, or since "the beginning", depending on your understanding of time and history

"Construct correlation intractable functions with prescribed input-output length."

Correlation Intractability* [Canetti-Goldreich-Halevi 98]

Magic Functions* [Dwork-Naor-Reingold-Stockmeyer 03]

Entropy preservation* [Barak-Lindell-Vadhan 04]

Seed-incompressible CI* [Halevi-Myers-Rackoff 08]

Perfect one-wayness
[Canetti 97, Canetti-Micciancio-Reingold 98]

Non-malleability
[Boldyreva-Cash-Fischlin-Warinschi 09]

Correlated-Input security
[Goyal-O'Neill-Rao 11]

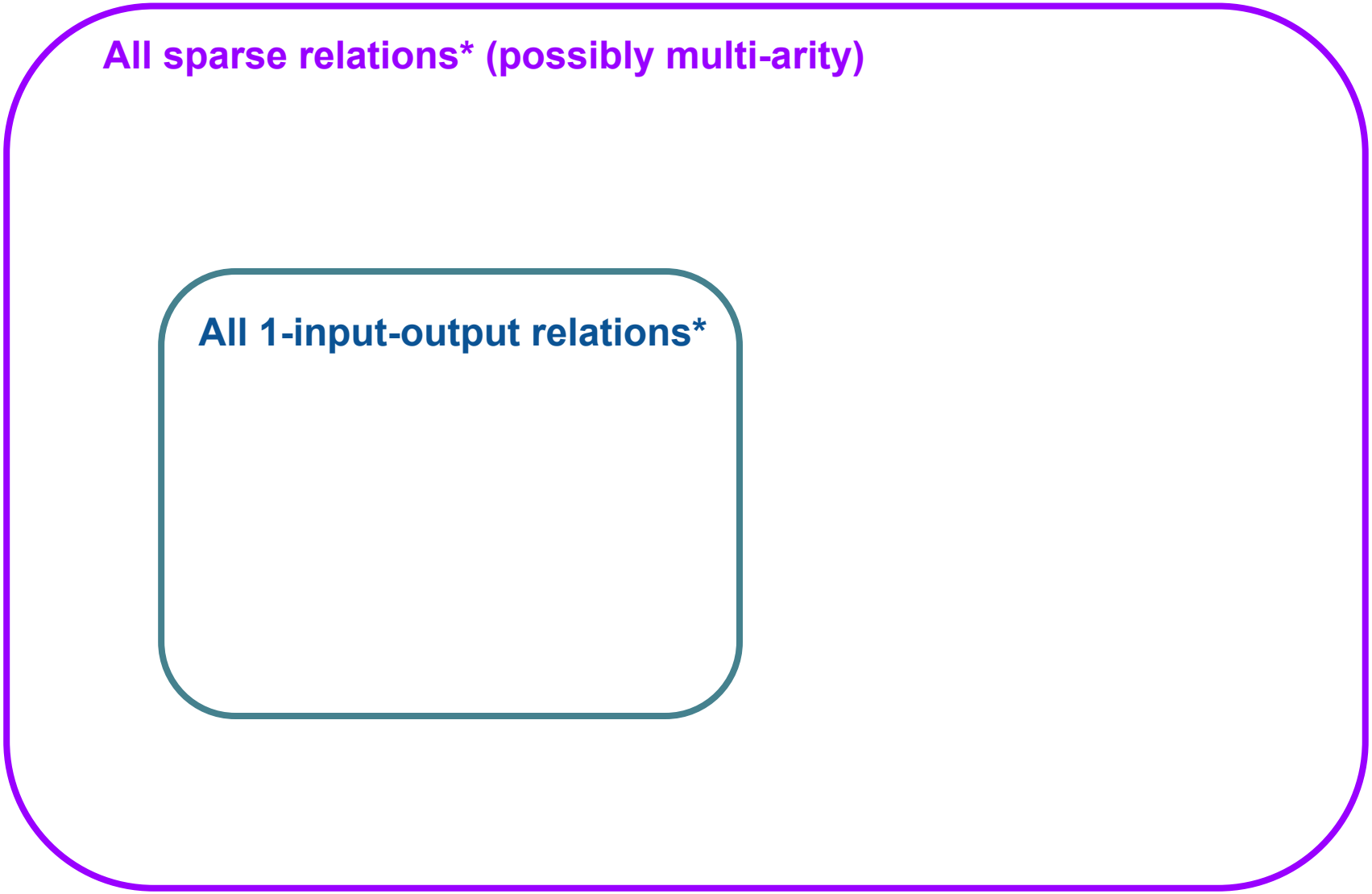
Universal Computational Extractor
[Bellare-Hoang-Keelveedhi 13]

* open

Correlation Intractability and its subclasses (classified by sparse relations)

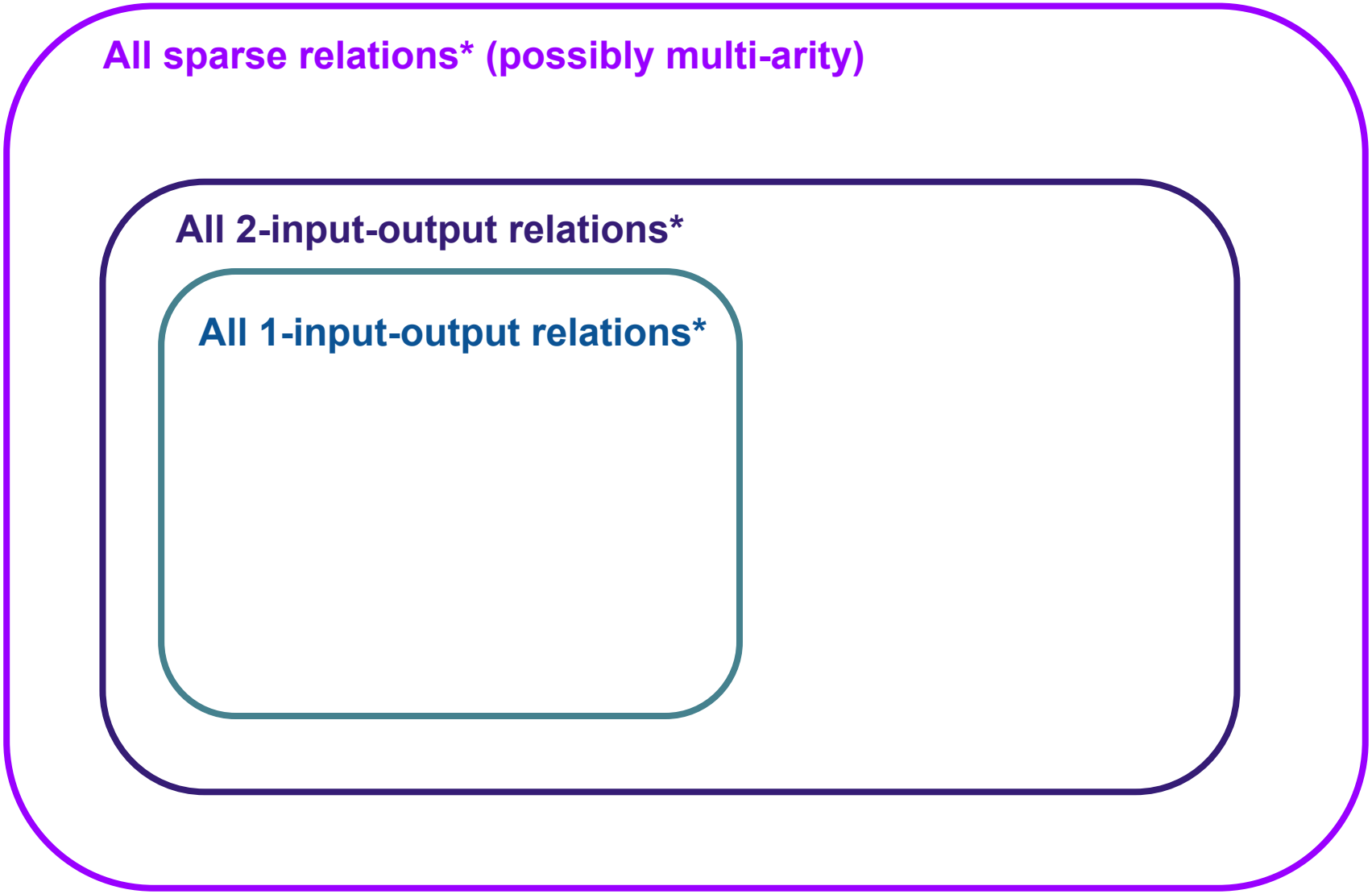
* open

Correlation Intractability and its subclasses (classified by sparse relations)



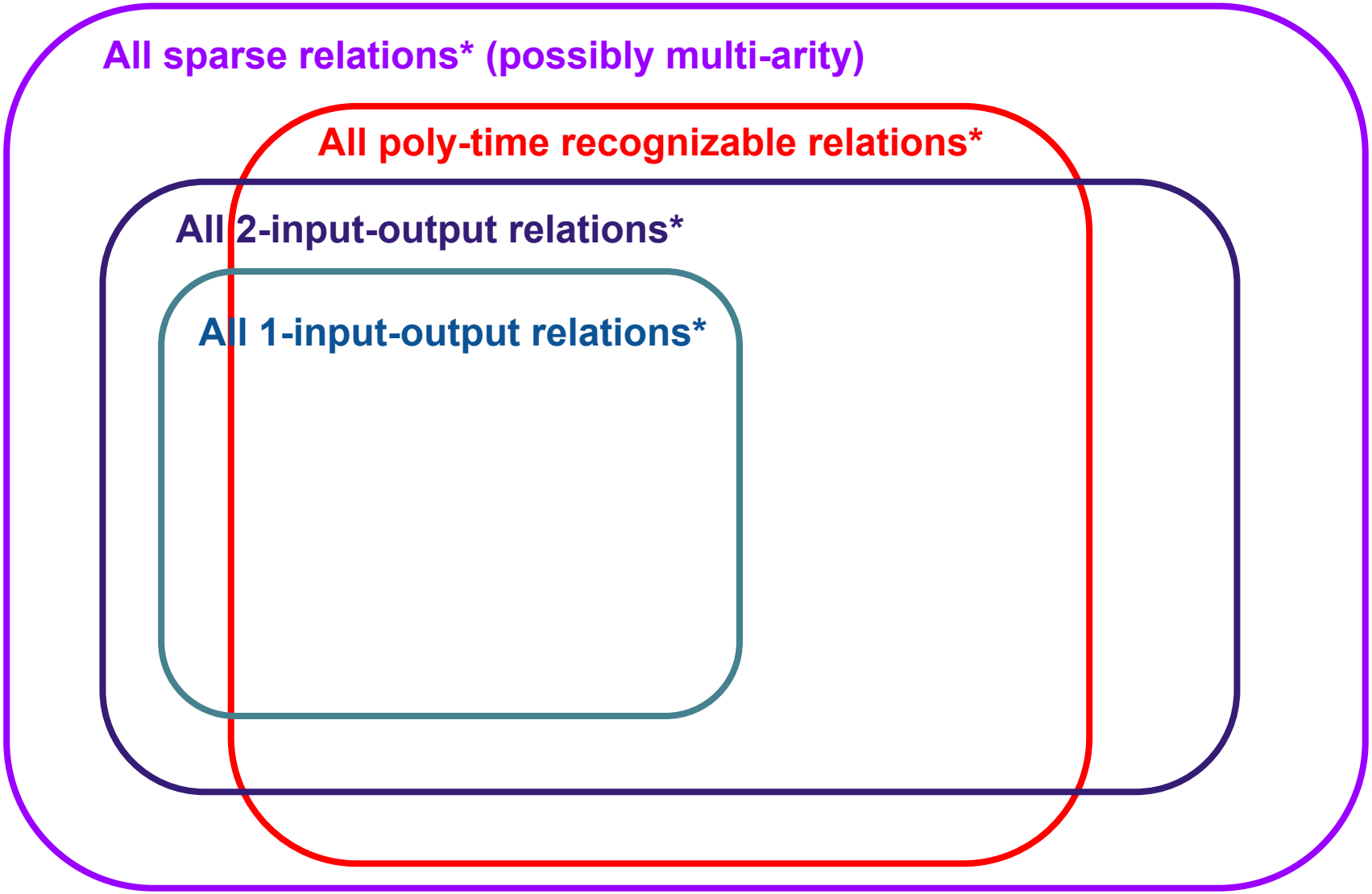
* open

Correlation Intractability and its subclasses (classified by sparse relations)



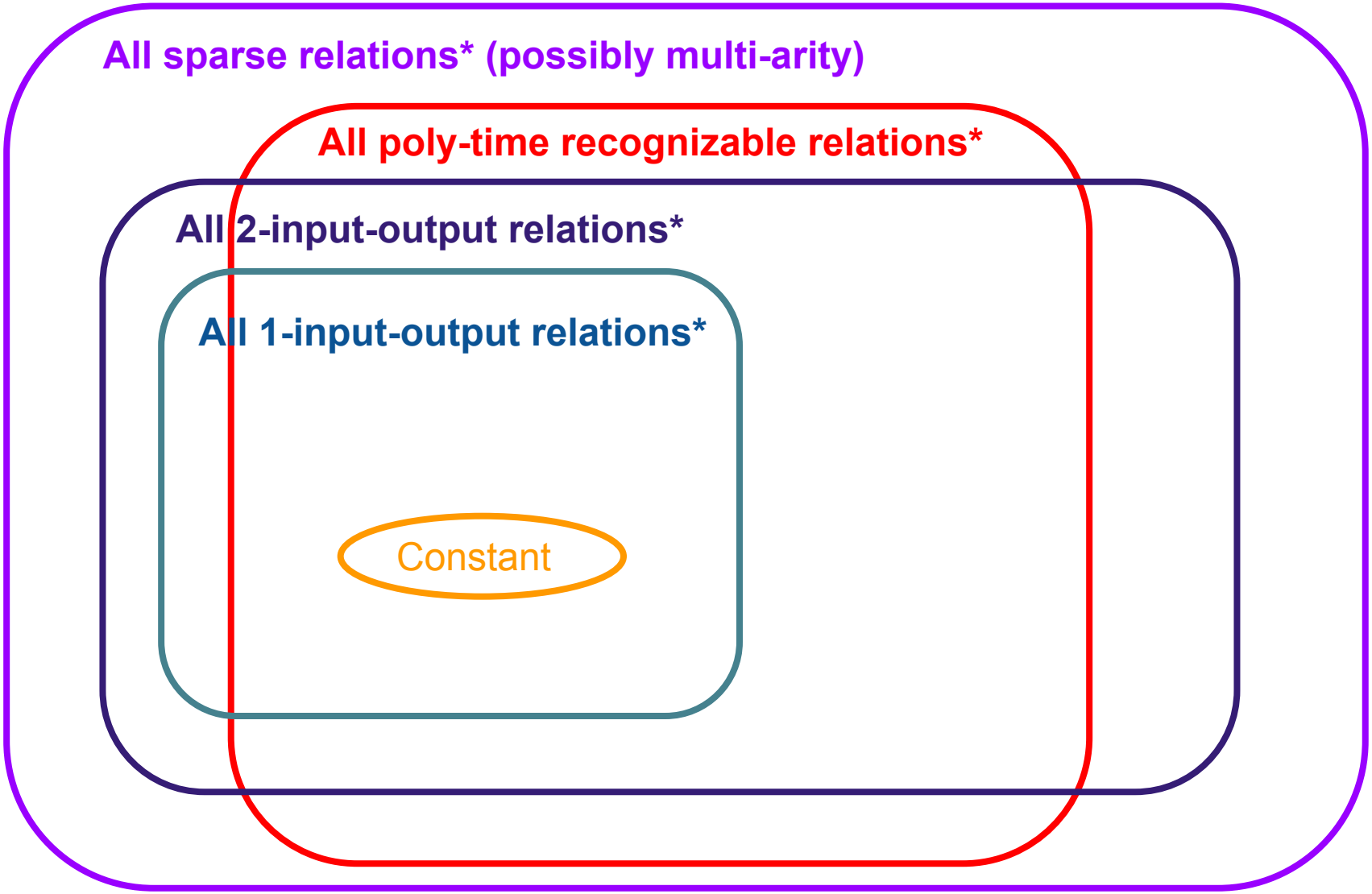
* open

Correlation Intractability and its subclasses (classified by sparse relations)



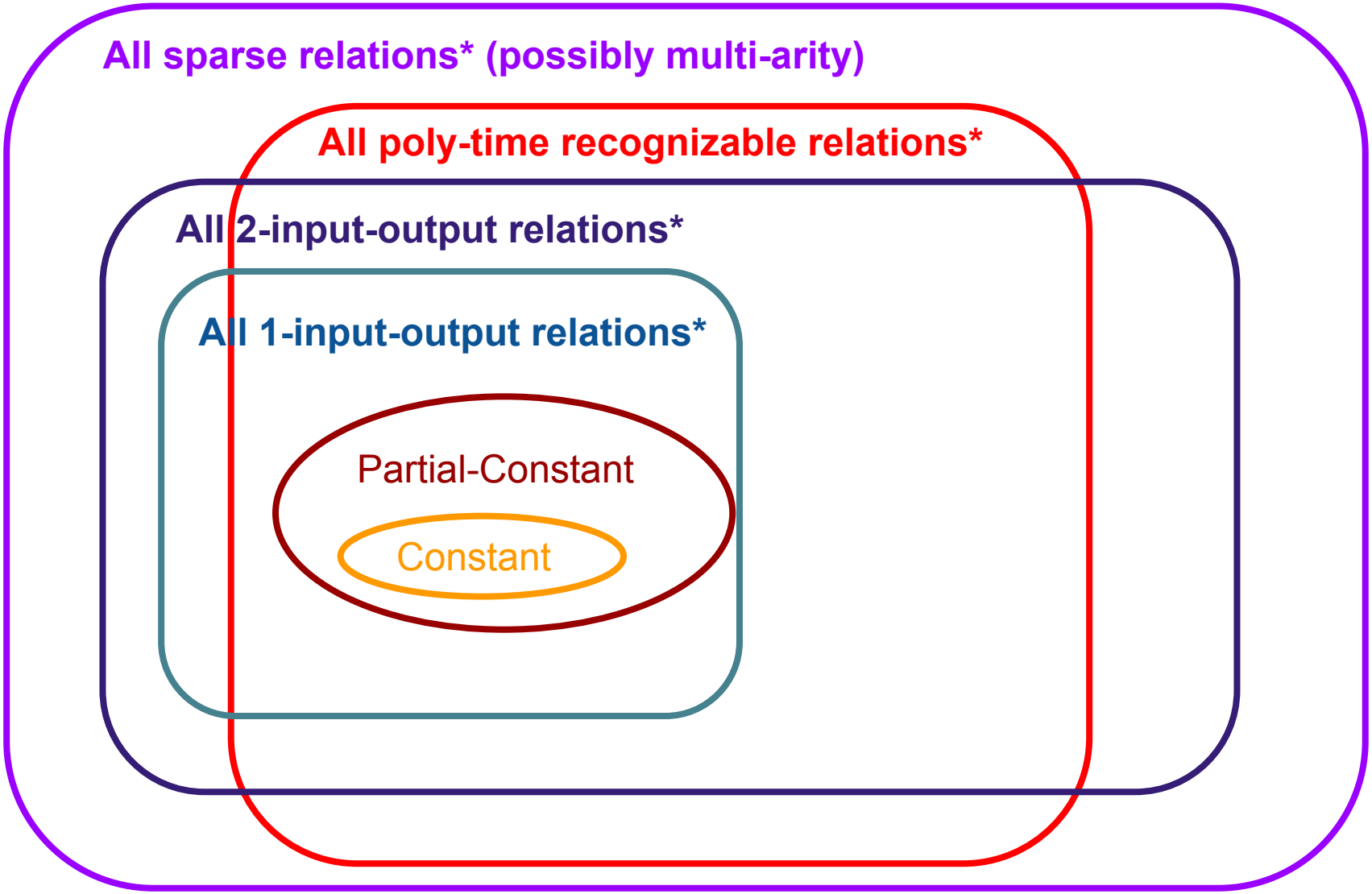
* open

Correlation Intractability and its subclasses (classified by sparse relations)



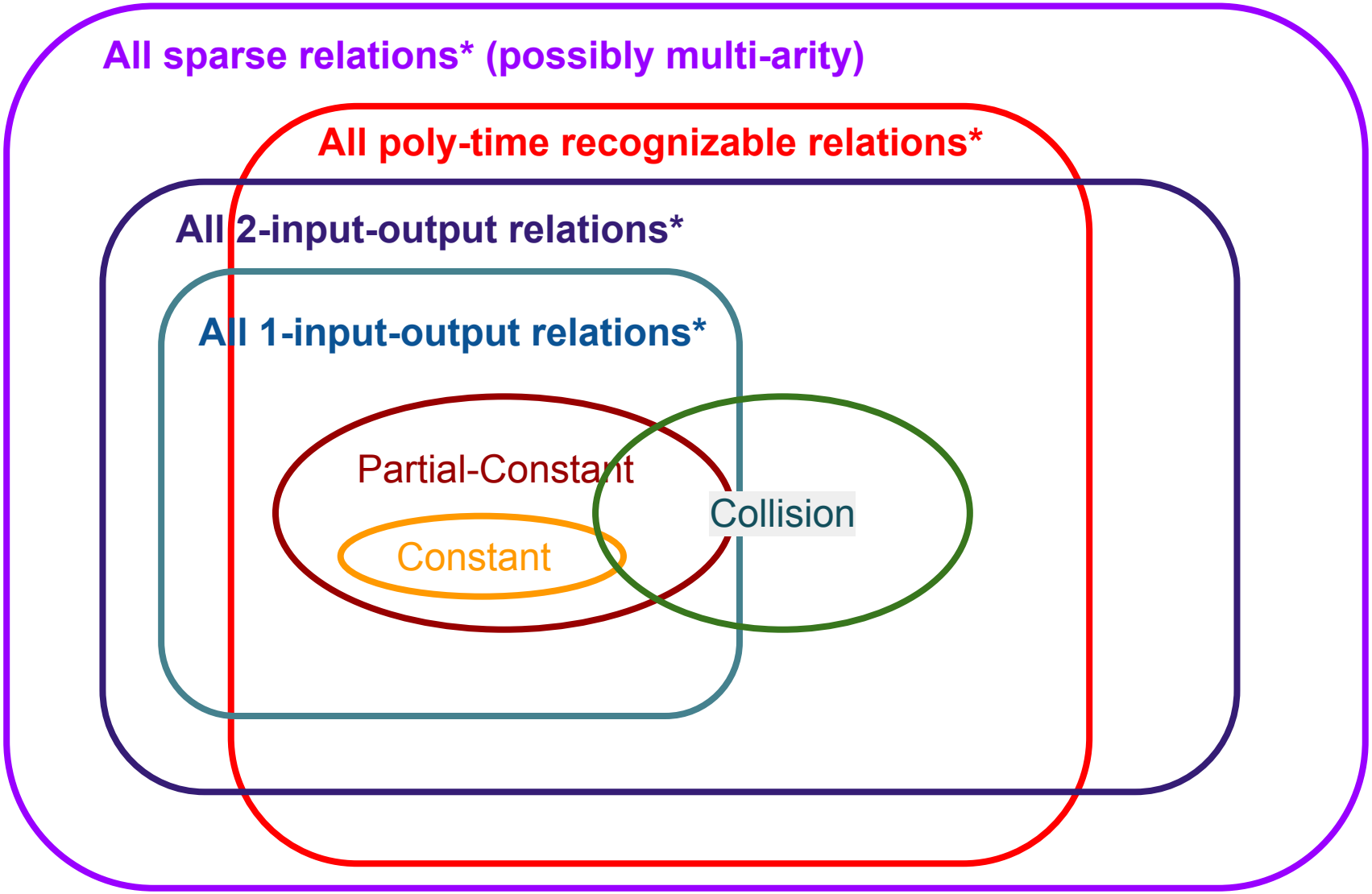
* open

Correlation Intractability and its subclasses (classified by sparse relations)



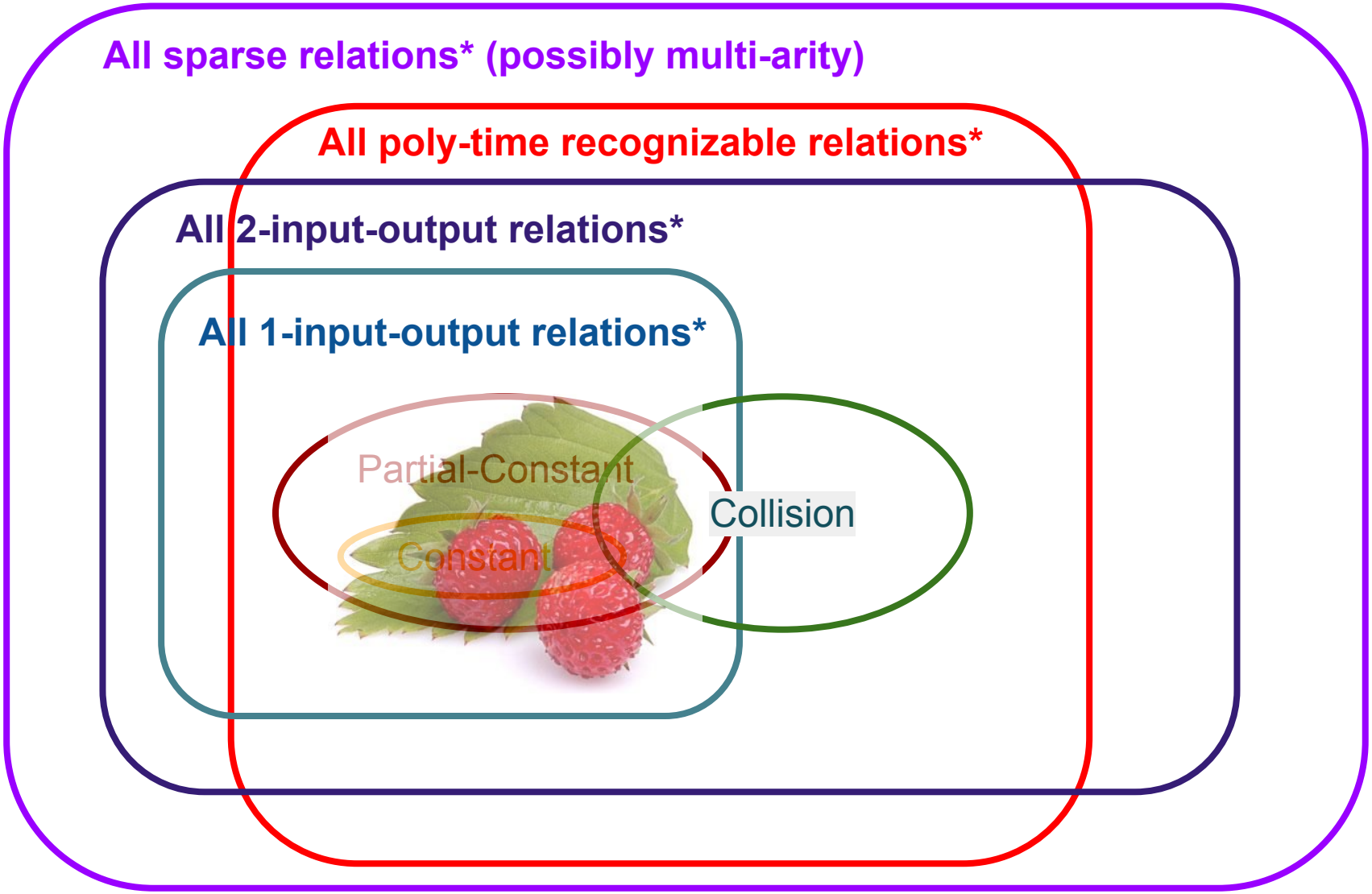
* open

Correlation Intractability and its subclasses (classified by sparse relations)



* open

Correlation Intractability and its subclasses (classified by sparse relations)



* open

(Widely) Open problem

since 1998, or since "the beginning", depending on your understanding of time and history

"Construct correlation intractable functions with prescribed input-output length, that covers a considerably wide relation class."

Act II

Our Result

Ind.Obf(Puncturable.PRF( ))

is bounded correlation intractable.

Ind.Obf(Puncturable.PRF( ) {with Padding})

is bounded correlation intractable.

Ind.Obf(Puncturable.PRF( ) {with Padding})

is bounded correlation intractable.

↓

given a polynomial upper bound on the computational complexity of the relation.

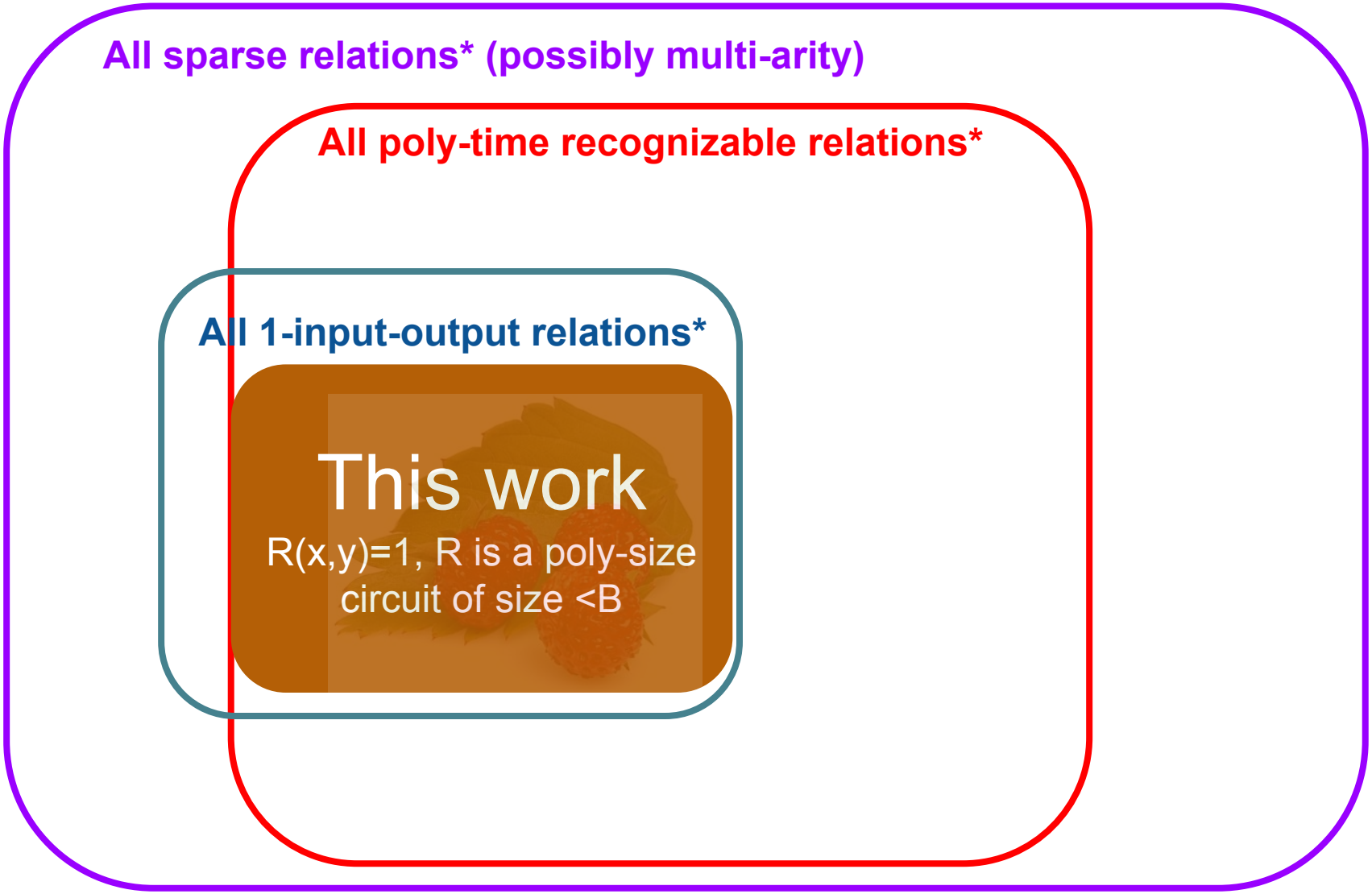
Here we are ...

All sparse relations* (possibly multi-arity)

All poly-time recognizable relations*

All 1-input-output relations*

Here we are …


All sparse relations* (possibly multi-arity)
All poly-time recognizable relations*
All 1-input-output relations*
This work
R(x,y)=1, R is a poly-size circuit of size <B

Assuming Puncturable_PRF (PPRF)
Assuming Indistinguishability_Obfuscation (iO)
Assuming Input_Hiding_Obfuscation_for_Evasive_Circuits (IHO)

Ind.Obf(Puncturable.PRF( ) {with Padding})

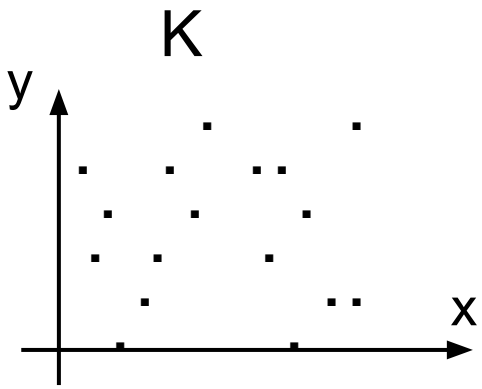
is bounded correlation intractable.

↓

given a polynomial upper bound on the computational complexity of the relation.

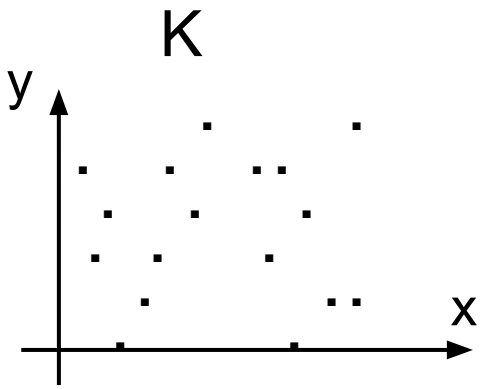
Puncturable Pseudorandom Functions

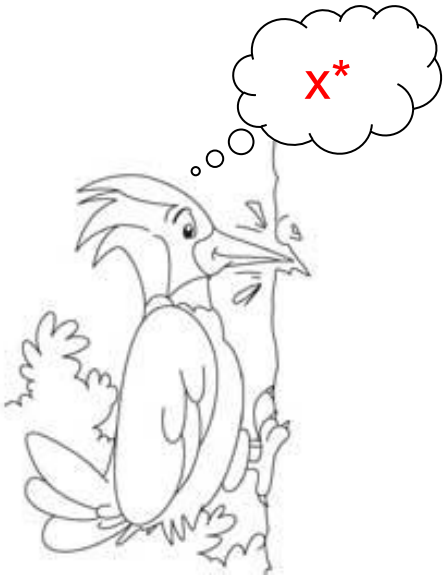
Puncturable PRF



K defines the entire PRF F_K

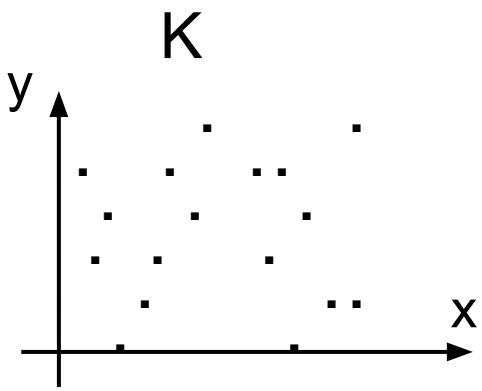
Puncturable PRF

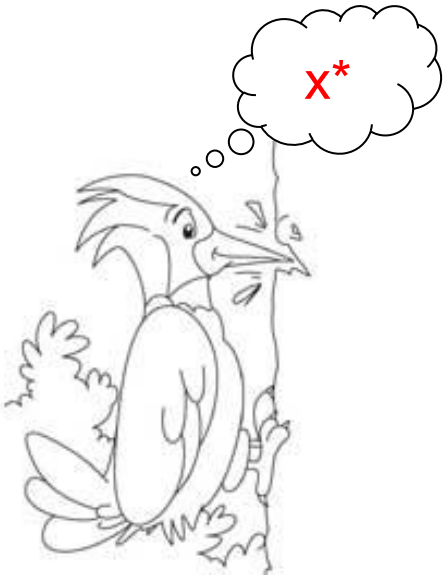


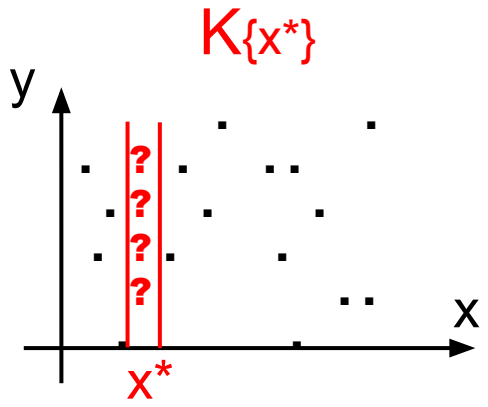


K defines the entire PRF F_K

Puncturable PRF



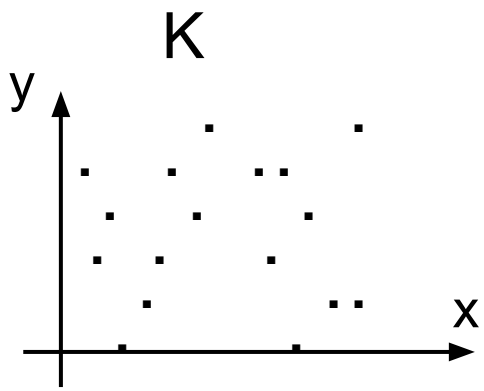


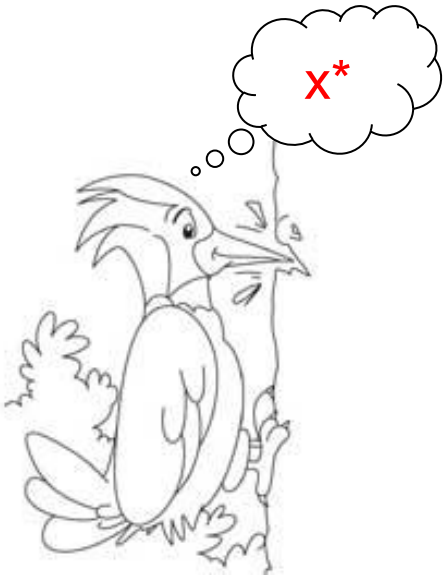


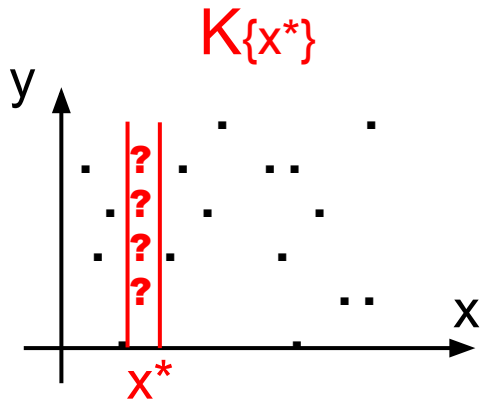
K defines the entire PRF F_K

K{x*} defines everywhere except x*

Puncturable PRF







K defines the entire PRF F_K

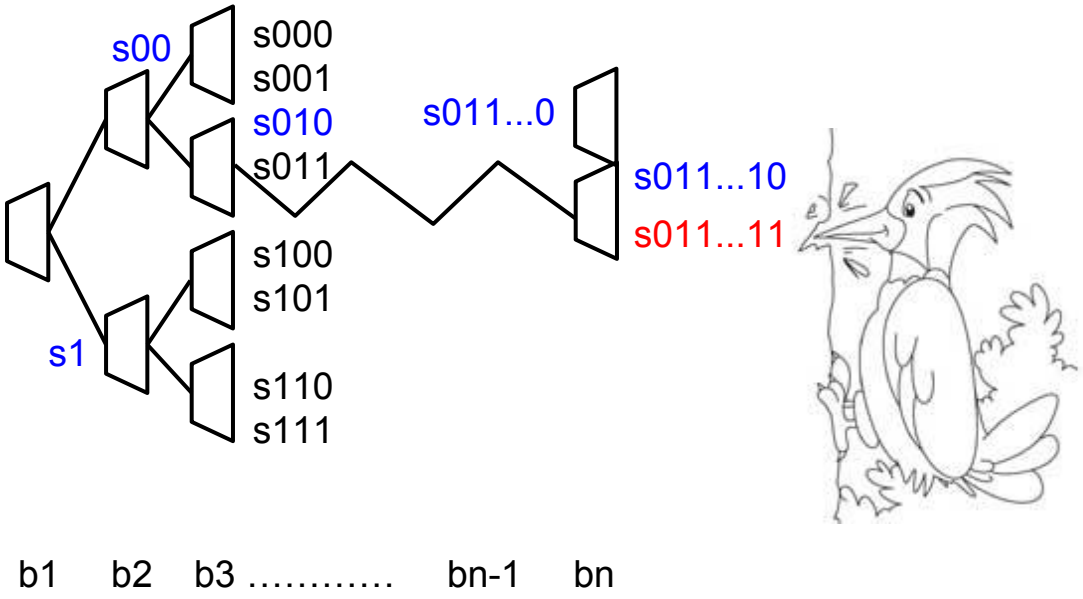
K{x*} defines everywhere except x*

Definition: [Kiayias-Papadopoulos-Triandopoulos-Zacharias '13, Boneh-Waters '13, Boyle-Goldwasser-Ivan '14, Sahai-Waters '14]

Constructions: [Goldreich-Goldwasser-Micali '86, Naor-Reingold '97, Banerjee-Peikert '14, Brakerski-Vaikuntanathan '15, ...]

Puncturable PRF from GGM (proof by picture)

Given an input x*, can derive a "punctured" key k{x*}, that doesn't reveal the information about F_k(x*)



Indistinguishability Obfuscator

Indistinguishability Obfuscator

Defined by
[Barak-Goldreich-Impagliazzo-Rudich-Sahai-Vadhan-Yang ‘01]

Indistinguishability Obfuscator

Defined by
[Barak-Goldreich-Impagliazzo-Rudich-Sahai-Vadhan-Yang '01]

Security:

$$iO[F_0] \approx iO[F_1]$$

if F_0 and F_1 have identical functionality

Indistinguishability Obfuscator

Defined by
[Barak-Goldreich-Impagliazzo-Rudich-Sahai-Vadhan-Yang '01]

Security:

$$iO[\, F_0 \,] \approx iO[\, F_1 \,]$$

if F_0 and F_1 have identical functionality

Candidate constructions:
[Garg-Gentry-Halevi-Raykova-Sahai-Waters '13], [Brakerski-Rothblum '14], [Barak-Garg-Kalai-Paneth-Sahai '14], [Pass-Seth-Telang '14], [Zimmerman '15], [Applebaum-Brakerski '15], [Ananth-Jain '15], [Bitansky-Vaikuntanathan '15]

Input Hiding Obfuscator

(for evasive circuit families)

Obfuscators for Evasive Circuit families

Defined in [Barak-Bitansky-Canetti-Kalai-Paneth-Sahai ‘14]

Obfuscators for Evasive Circuit families

Defined in [Barak-Bitansky-Canetti-Kalai-Paneth-Sahai '14]

Evasive circuit families:

"Almost 0 circuits."

for each input x, $\Pr_k[\, C_k(x) \neq 0 \,] < \text{negl}$.

Obfuscators for Evasive Circuit families

Defined in [Barak-Bitansky-Canetti-Kalai-Paneth-Sahai '14]

Evasive circuit families:

"Almost 0 circuits."

for each input x, $\Pr_k[\ C_k(x) \neq 0\ ] < \text{negl}$.

Input-Hiding Obfuscation for evasive circuit families:

"Hide the inputs that evaluate to non-zero."

$$\Pr_k[\ \text{Adv}(\ \text{IHO}\{\ C_k\ \}\ ) \rightarrow x\colon C_k(x) \neq 0\ ] < \text{negl}$$

Input Hiding Obfuscator

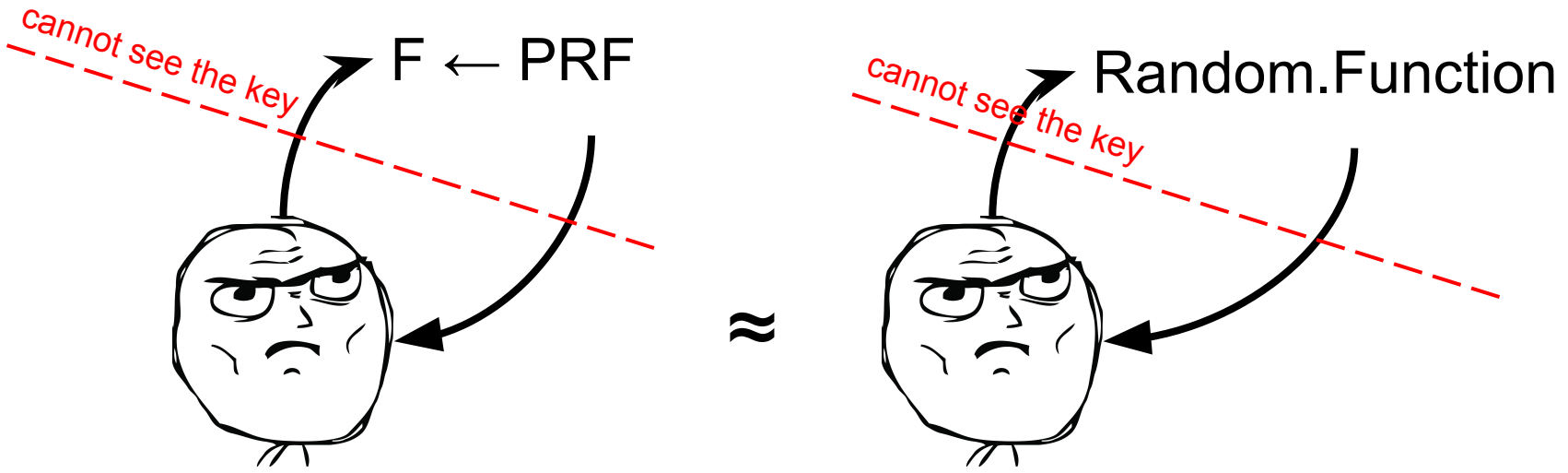
(for evasive circuit families)

Input Hiding Obfuscator
(for evasive circuit families)

Let's take a step back

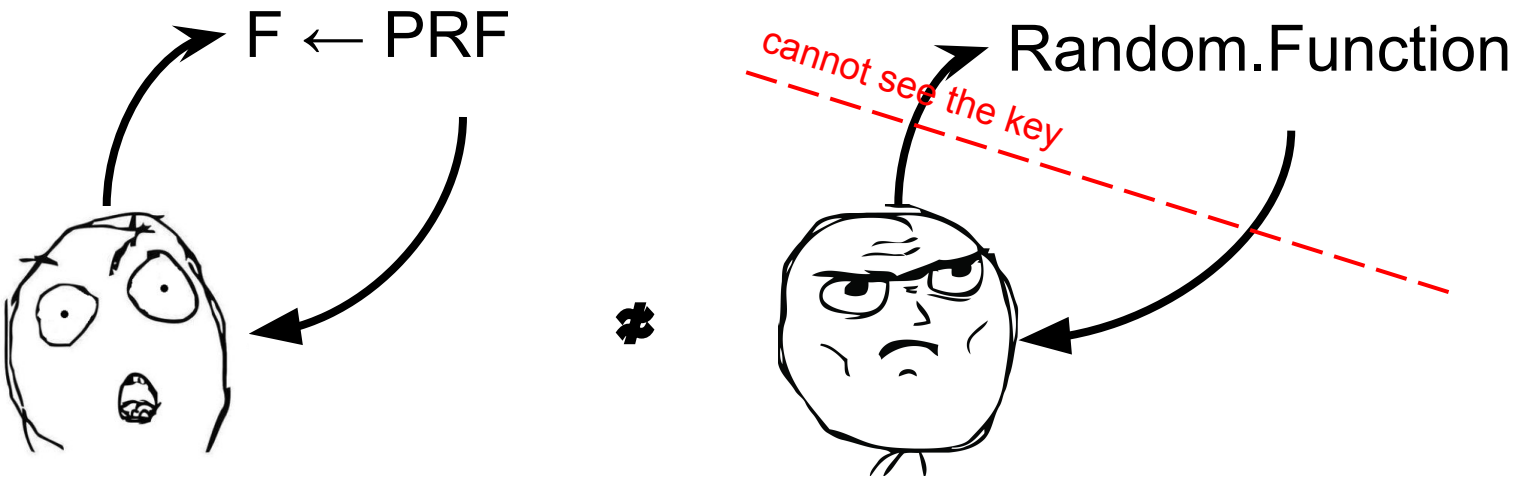
⟦Alessandra said "Vinod said this sounds smart."⟧

Pseudorandom Functions



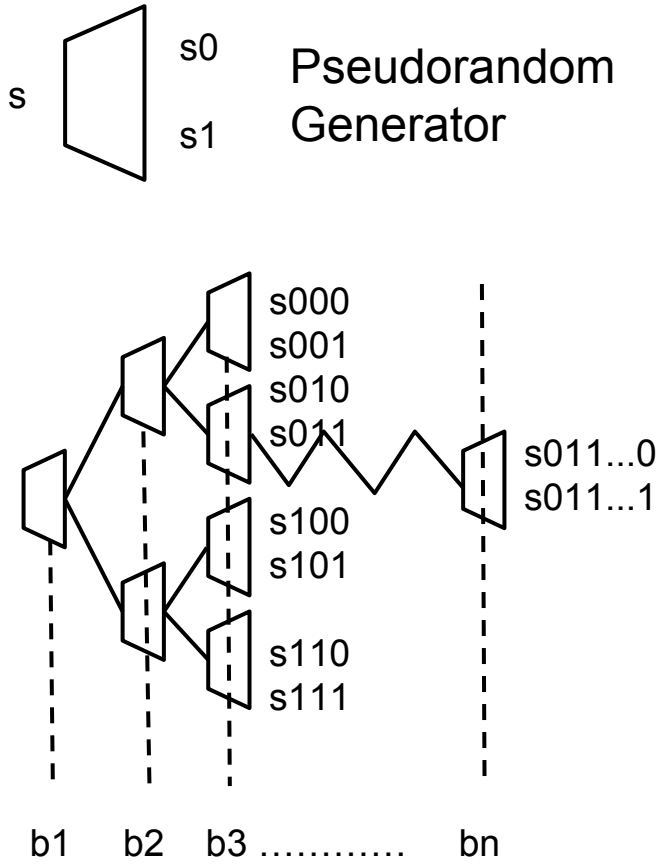
- Any PRF is correlation intractable with black box access

Pseudorandom Functions (revealing the seed)



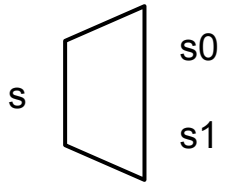
- Any PRF is correlation intractable with black box access
- But if the key is revealed without any protections … easy to build an intriguing PRF where revealing the key may break correlation intractability

PRF by Goldreich, Goldwasser, Micali 1984

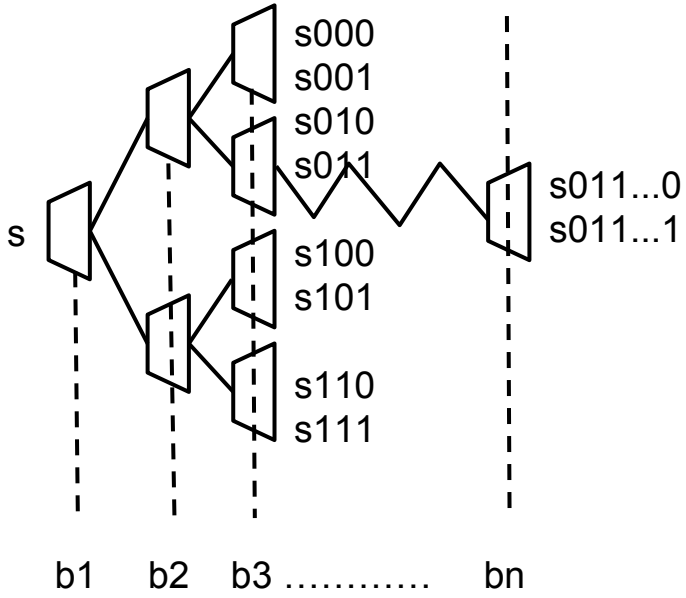


Pseudorandom Function
[Goldreich-Goldwasser-Micali 84']

PRF by Goldreich, Goldwasser, Micali 1984



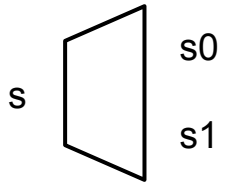
Pseudorandom Generator



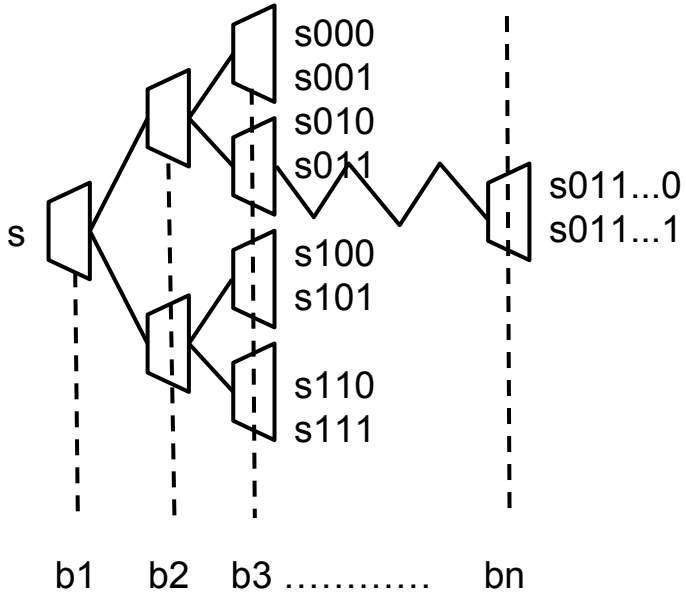
Micali 90s: What if we publish the seed of GGM's PRF? Is that correlation intractable?

Pseudorandom Function
[Goldreich-Goldwasser-Micali 84']

PRF by Goldreich, Goldwasser, Micali 1984



Pseudorandom Generator



Pseudorandom Function
[Goldreich-Goldwasser-Micali 84']

Micali 90s: What if we publish the seed of GGM's PRF? Is that correlation intractable?

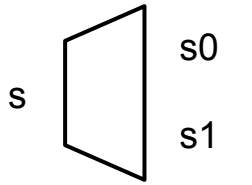
…

…

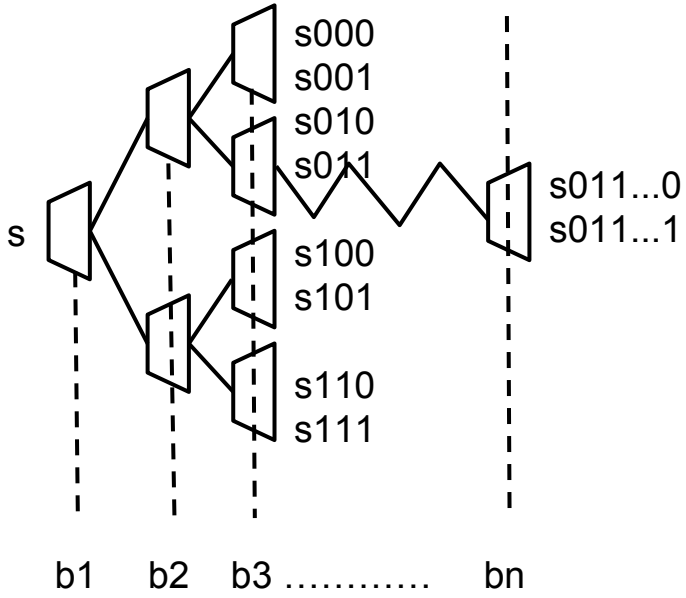
…

Barak 00s: Does that work?

PRF by Goldreich, Goldwasser, Micali 1984



Pseudorandom Generator



Pseudorandom Function
[Goldreich-Goldwasser-Micali 84']

Micali 90s: What if we publish the seed of GGM's PRF? Is that correlation intractable?

…

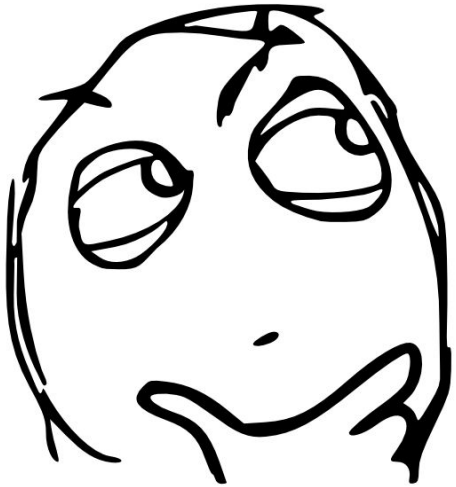
…

…

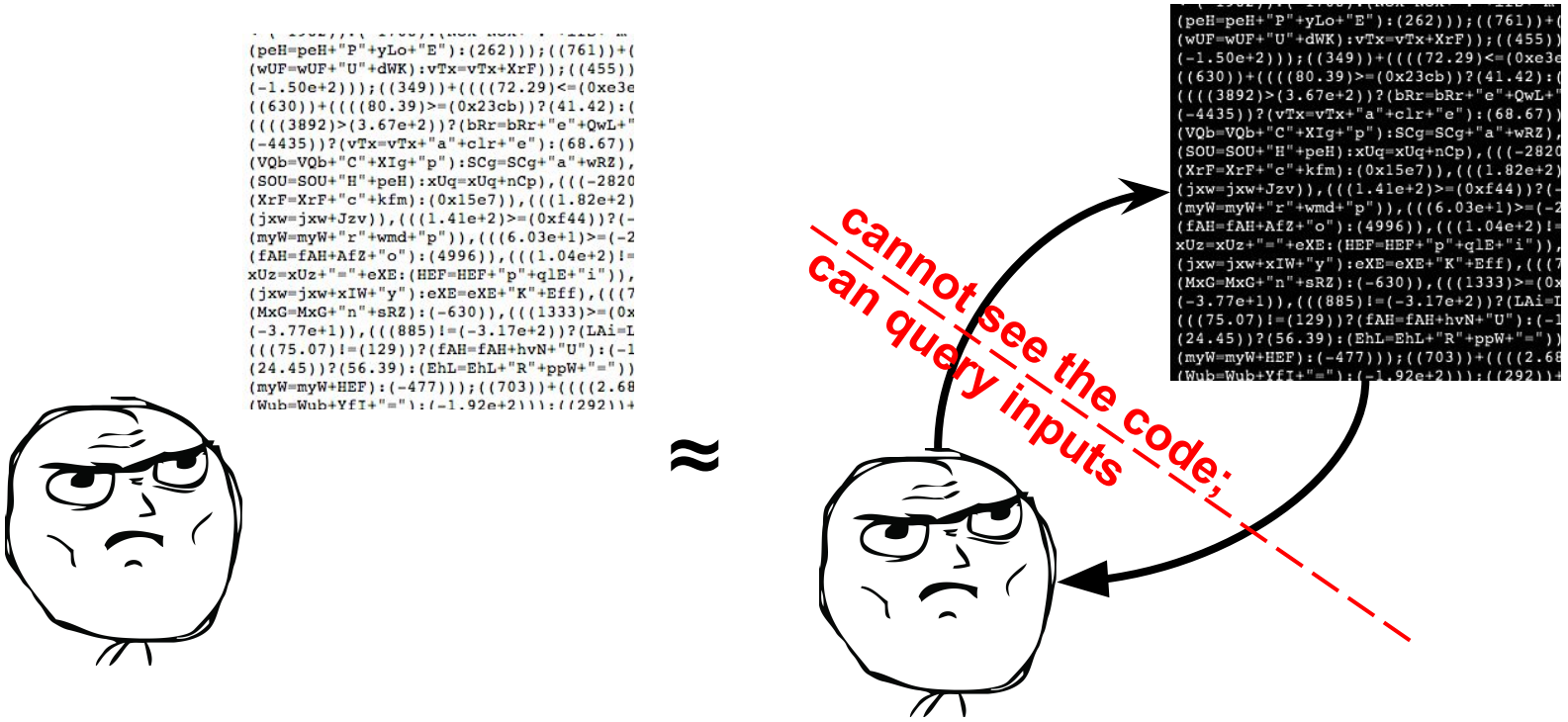
Barak 00s: Does that work?

Goldreich '02: No.
There is a problematic PRG s.t. the resulting PRF is not correlation intractable.

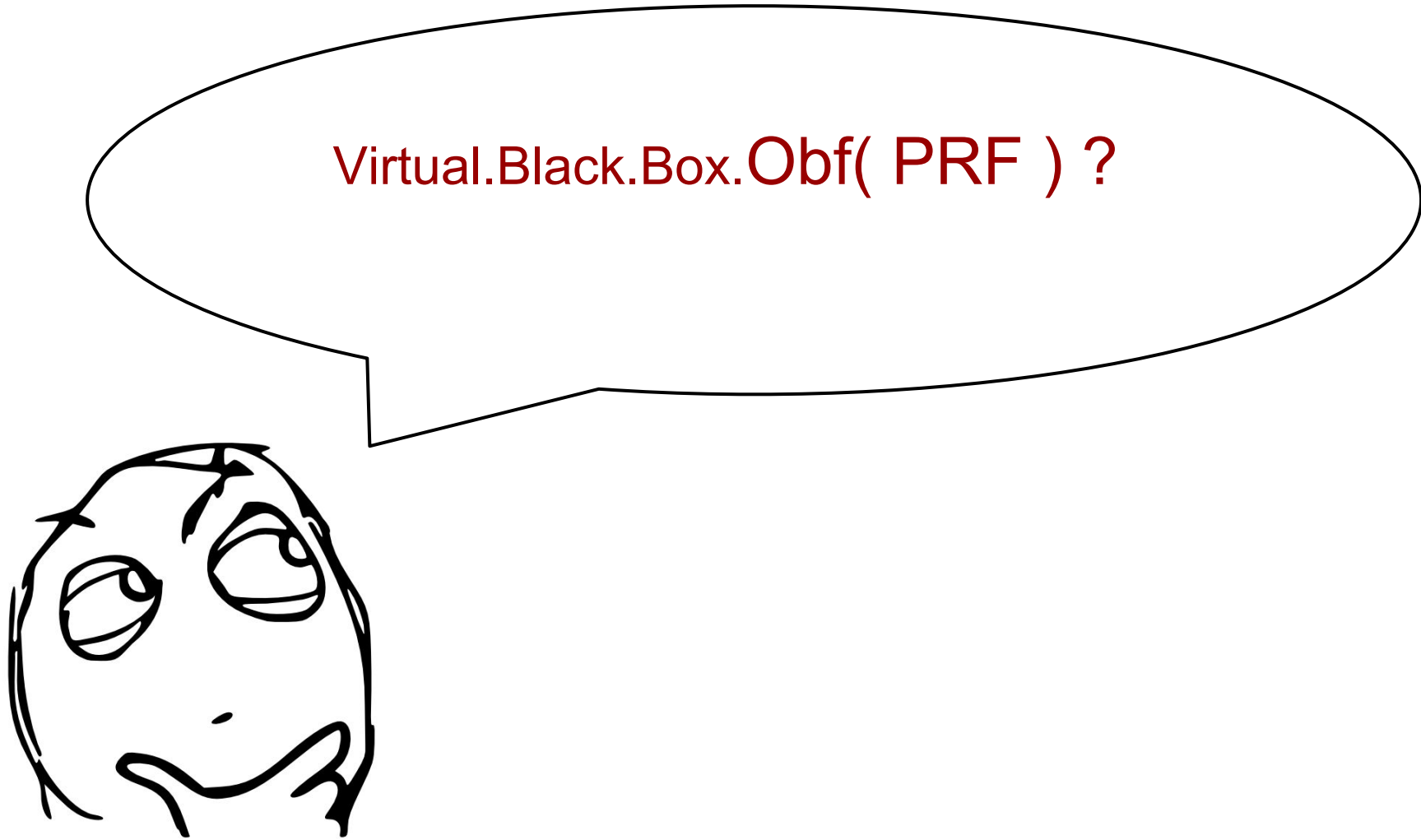
What if we obfuscate the pseudorandom functions?



Virtual-Black-Box Obfuscation



[Barak-Goldreich-Impagliazzo-Rudich-Sahai-Vadhan-Yang 01]


Virtual.Black.Box.Obf(PRF) ?

Virtual.Black.Box.Obf(PRF)

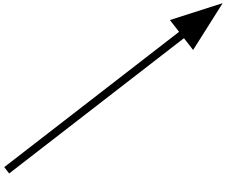
There are PRFs that cannot be obfuscated at all. [BGIRSVY‘01]

Virtual.Black.Box.Obf(PRF)

There are PRFs that cannot be obfuscated at all. [BGIRSVY‘01]

In fact, not even C-intractable

Virtual.Black.Box.Obf(PRF)



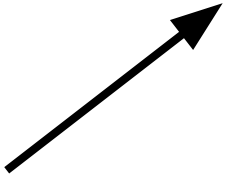
VBB is unachievable for ANY PRF

[Goldwasser-Kalai'05, Bitansky-Canetti-Cohn-Goldwasser-Kalai-Paneth-Rosen'14]

There are PRFs that cannot be obfuscated at all. [BGIRSVY'01]

In fact, not even C-intractable

Virtual.Black.Box.Obf(PRF)



VBB is unachievable for ANY PRF

[Goldwasser-Kalai'05, Bitansky-Canetti-Cohn-Goldwasser-Kalai-Paneth-Rosen'14]

There are PRFs that cannot be obfuscated at all. [BGIRSVY'01]

In fact, not even C-intractable

However, not explicitly breaking CI.

	some PRF	Puncturable PRF
VBB	X	X
Indistinguishability Obfuscator	X	HOPE

How to use iO + Puncturable PRF?

How to use iO + Puncturable PRF?
Key idea: Using hybrid argument to move out some "dangerous" input x* and its output value F_K(x*)

How to use iO + Puncturable PRF?
Key idea: Using hybrid argument to move out some "dangerous" input x* and its output value F_K(x*)

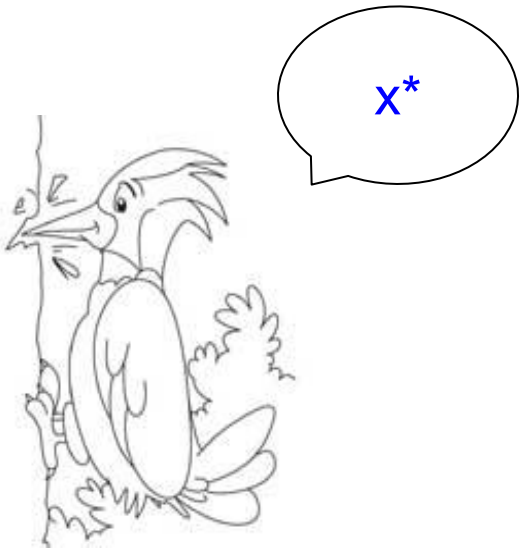
IO[F_K(x)]

How to use iO + Puncturable PRF?
Key idea: Using hybrid argument to move out some "dangerous" input x* and its output value F_K(x*)

IO[F_K(x)]

indistinguishability Obfuscation

IO[if x = x*, F_K(x) ;
else, F_K{x*}(x).]



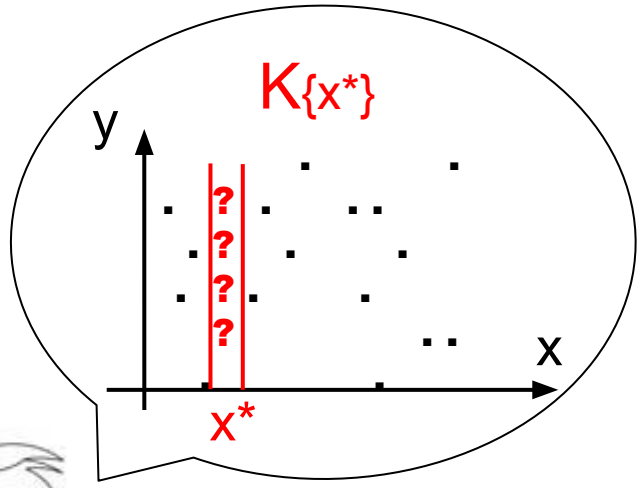
How to use iO + Puncturable PRF?

Key idea: Using hybrid argument to move out some "dangerous" input x* and its output value F_K(x*)

IO[F_K(x)]

indistinguishability Obfuscation

IO[if x = x*, F_K(x) ;
else, F_K{x*}(x).]



How to use iO + Puncturable PRF?

Key idea: Using hybrid argument to move out some "dangerous" input x* and its output value F_K(x*)

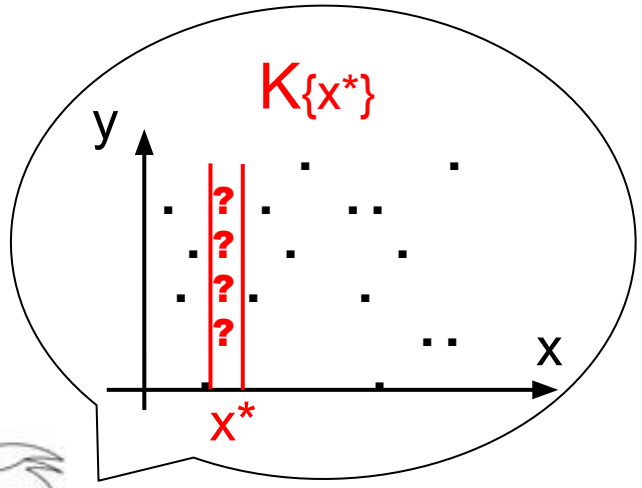
IO[F_K(x)]

indistinguishability Obfuscation

IO[if x = x*, F_K(x) ;
else, F_K{x*}(x).]

Puncturable PRF

IO[if x = x*, r* ;
else, F_K{x*}(x).]



iO + Puncturable PRF is very powerful

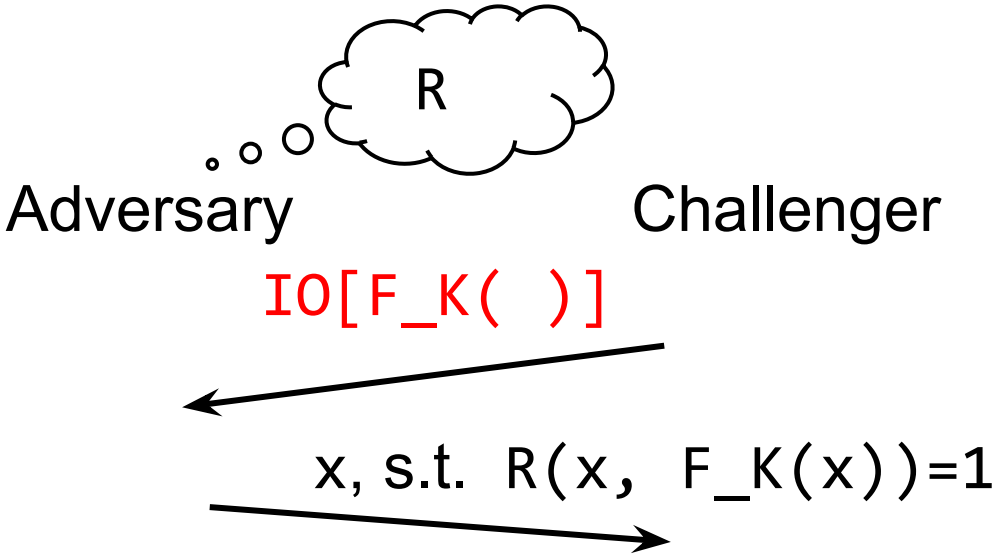
- Deniable Encryption [Sahai-Waters ‘14],
- Full-fledged Functional Encryption [Waters ‘15],
- Hard instances for NASH [Bitansky-Paneth-Rosen ‘15].
- Watermarking [Cohen-Holmgren-Nishimaki-Vaikuntanathan-Wichs ’15]
- …

Including for obtaining random-oracle-like properties

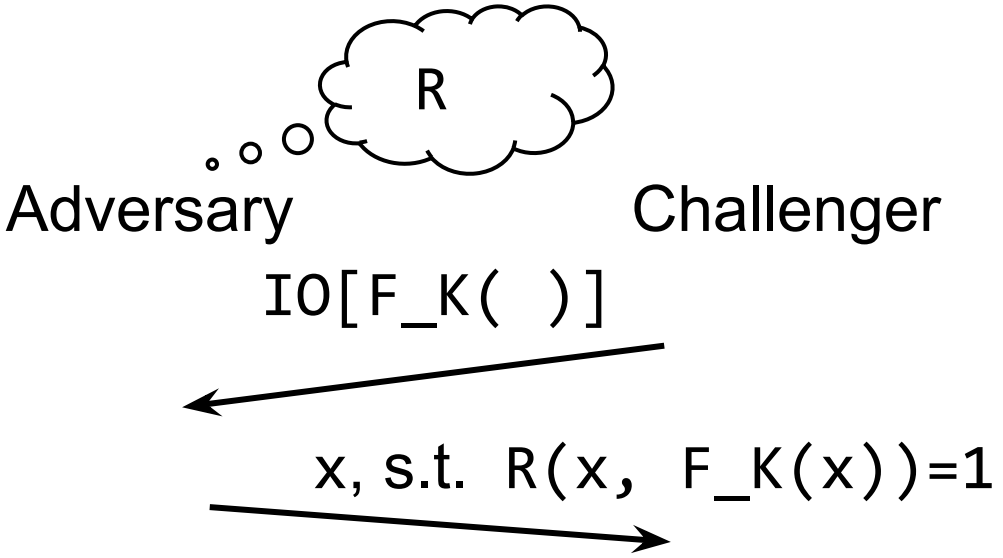
- Universal hardcore functions [Bellare-Stepanovs-Tessaro ‘14],
- (some kind of) UCE [Brzuska-Mittelbach ‘14].

What we want to prove:

What we want to prove:

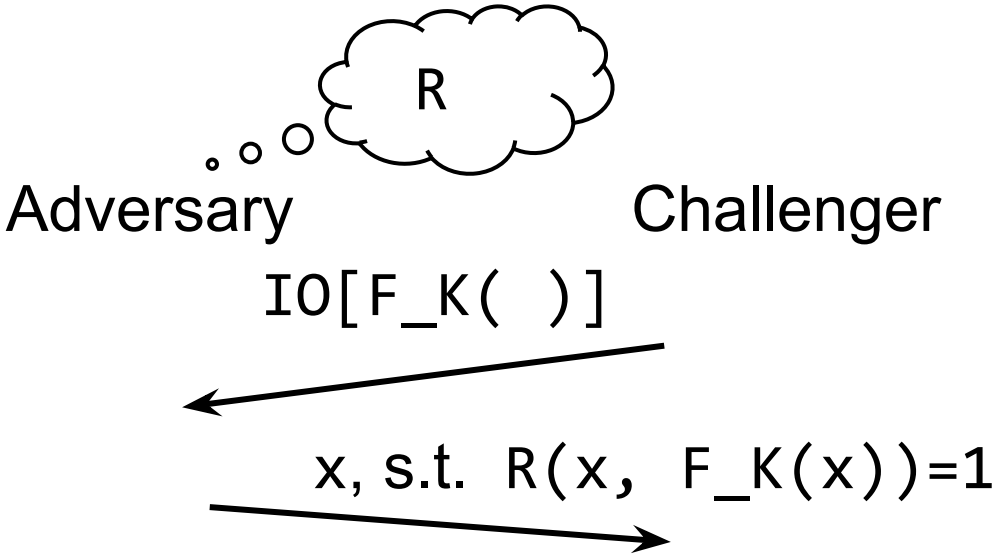


What we want to prove:



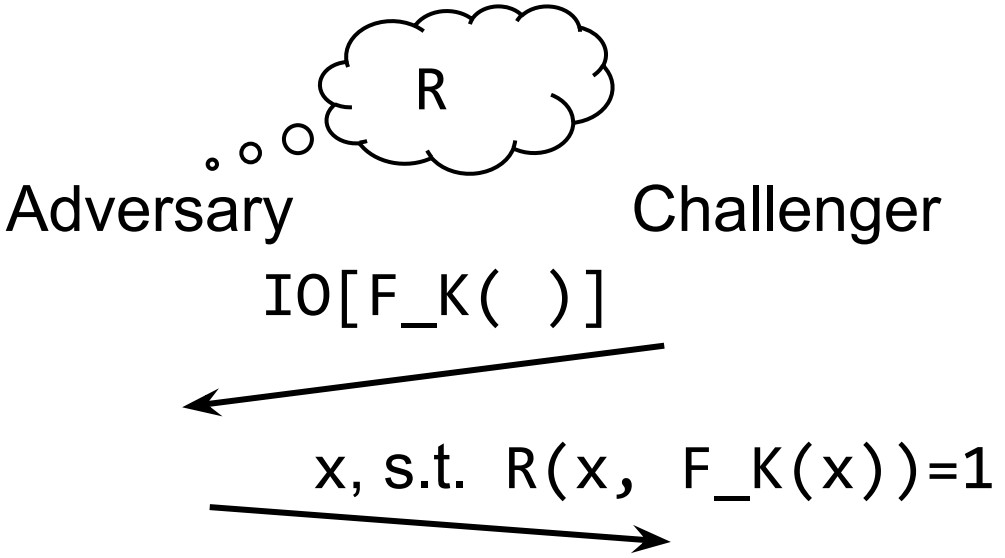
Attempt: Puncture out the "bad" points

What we want to prove:



IO[F_K(x)]

What we want to prove:

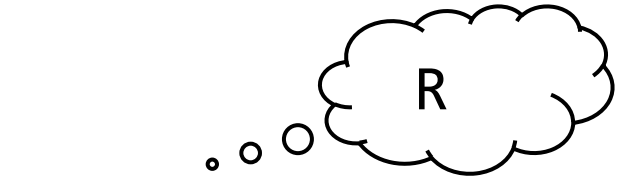


IO[F_K(x)]

indistinguishability Obfuscation

IO[if R(x, F_K(x))=1, F_K(x);
else, F_K(x).]

What we want to prove:



Adversary Challenger

IO[F_K( )]

x, s.t. R(x, F_K(x))=1

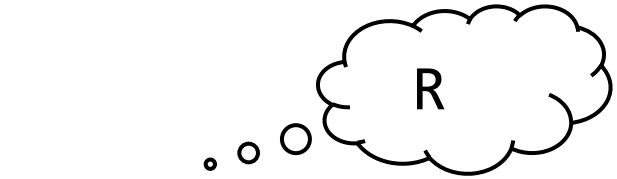
IO[F_K(x)]

indistinguishability Obfuscation

IO[if R(x, F_K(x))=1, F_K(x);
else, F_K(x).]

x* s.t.
R(x*, F_K(x*))=1

What we want to prove:



Adversary Challenger

IO[F_K( )]

x, s.t. R(x, F_K(x))=1

IO[F_K(x)]

indistinguishability Obfuscation

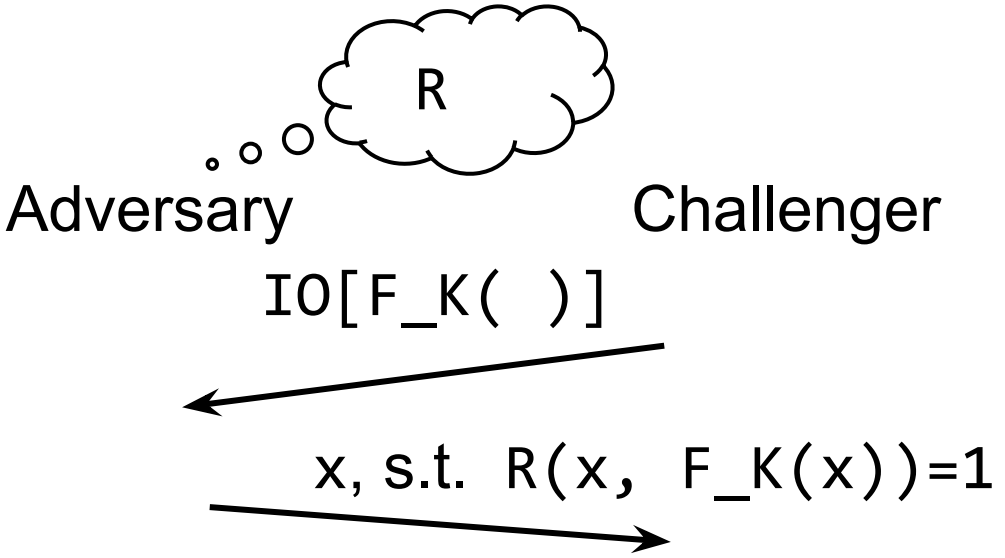
IO[if R(x, F_K(x))=1, F_K(x);
else, F_K(x).]

. . .

IO[if R(x, F_K(x))=1, ??? ;
else, F_K(x).]

x* s.t.
R(x*, F_K(x*))=1

What we want to prove:



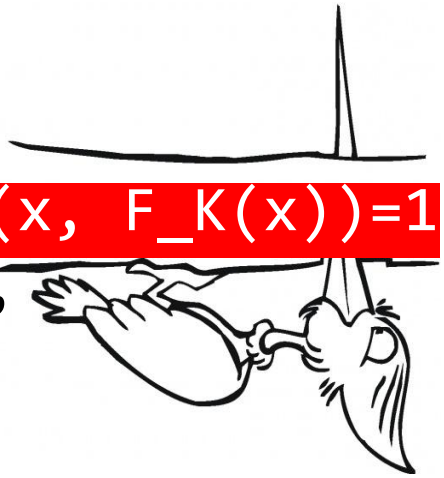
IO[F_K(x)]

indistinguishability Obfuscation

IO[if R(x, F_K(x))=1, F_K(x);
else, F_K(x).]

. . . stuck (key dependent inputs)

IO[if R(x, F_K(x))=1, F_K(x);
else, F_K(x).]



The standard puncturing technique doesn't work

Let's take a walk around

$$[\![\int_{-\infty}^{+\infty} \text{Vinod's ``sounds smart lemma''} \, e^{2\pi i t} dt \,]\!]$$


China,
B.C.E. 354

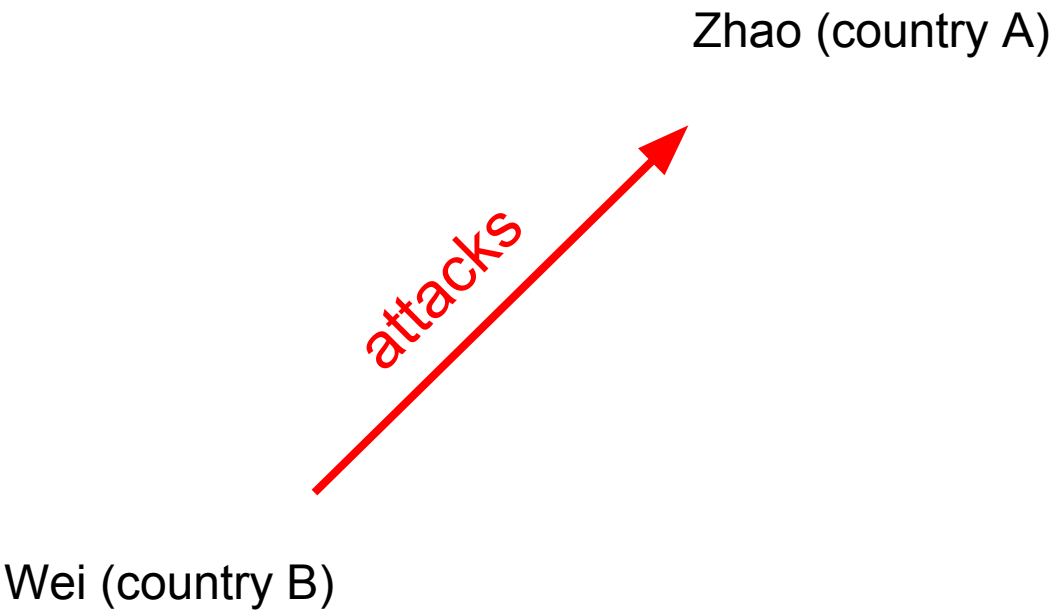
#whystudyChinese

Zhao (country A)

Wei (country B)

“Wei Wei Jiu Zhao” (Besiege Wei to save Zhao) B.C.E. 354

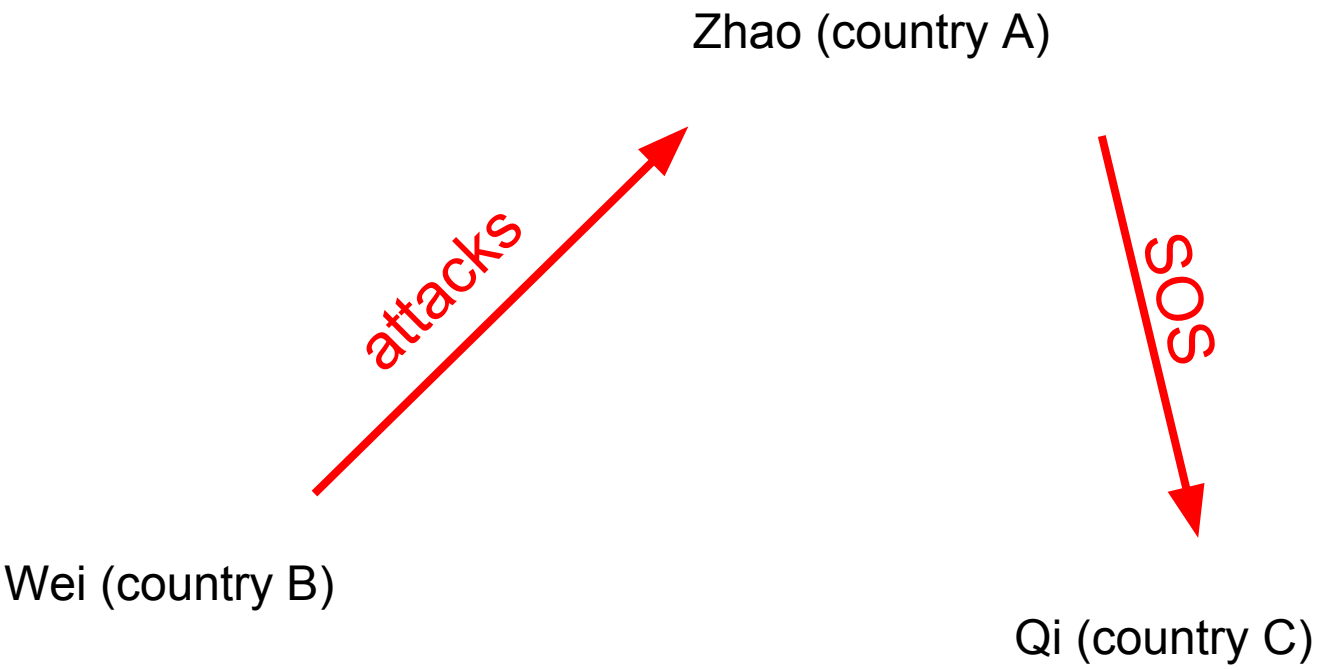
#whystudyChinese



“Wei Wei Jiu Zhao” (Besiege Wei to save Zhao) B.C.E. 354

圍魏救趙

#whystudyChinese



“Wei Wei Jiu Zhao” (Besiege Wei to save Zhao) B.C.E. 354

圍魏救趙

#whystudyChinese

Zhao (country A)

attacks

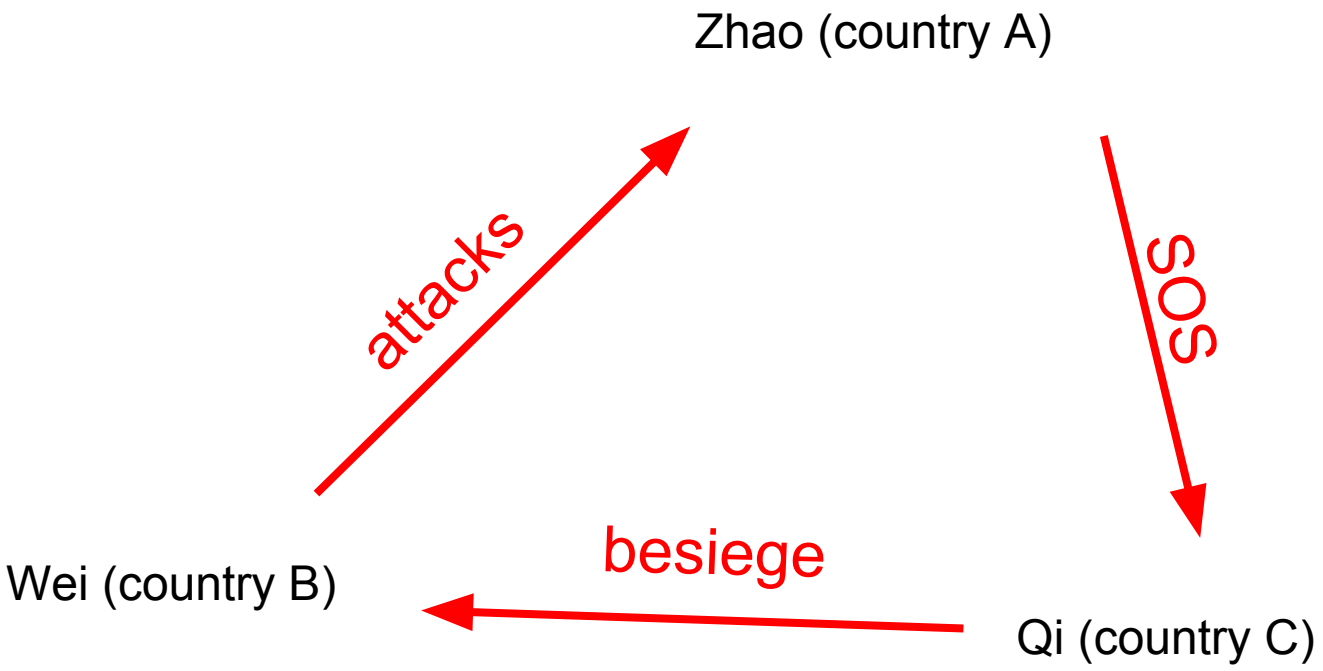
SOS

Wei (country B)

“Wei Wei Jiu Zhao” (Besiege Wei to save Zhao) B.C.E. 354

圍魏救趙

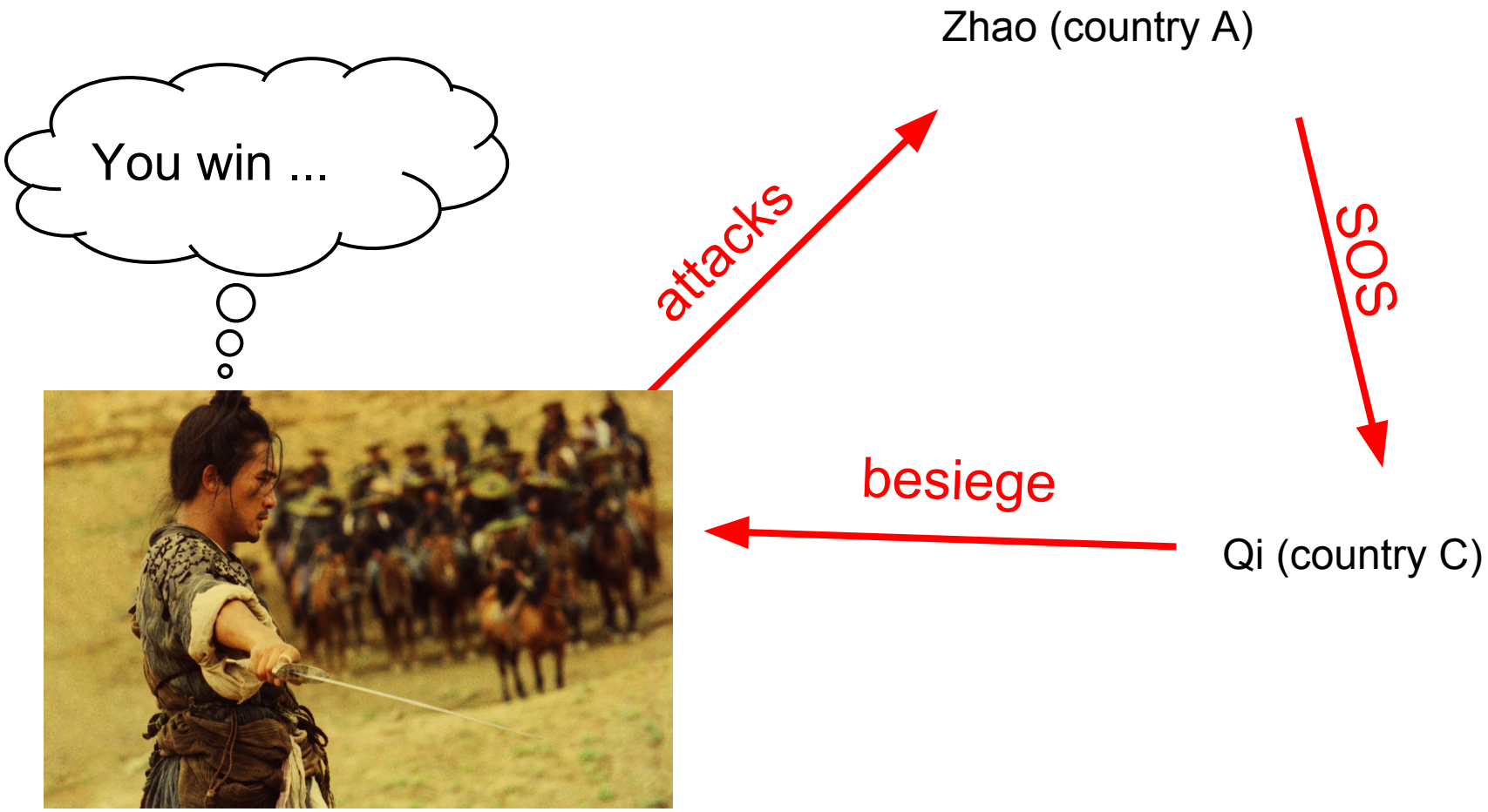
#whystudyChinese



“Wei Wei Jiu Zhao” (Besiege Wei to save Zhao) B.C.E. 354

圍魏救趙

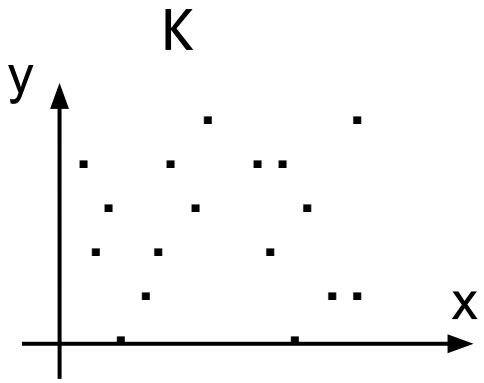
#whystudyChinese



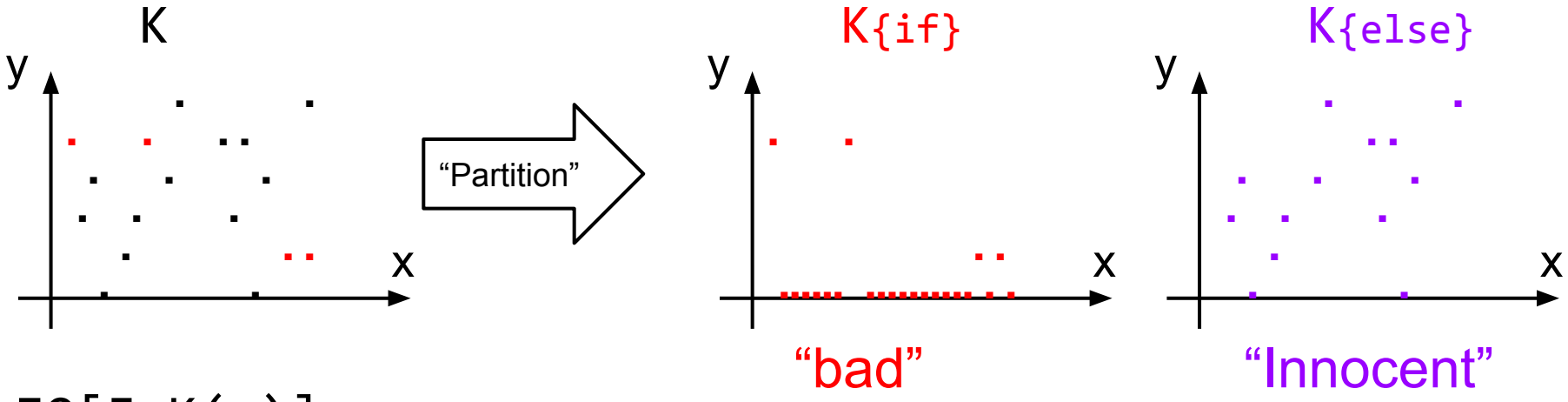
“Wei Wei Jiu Zhao” (Besiege Wei to save Zhao) B.C.E. 354

圍魏救趙

New proof strategy



IO[F_K(x)]



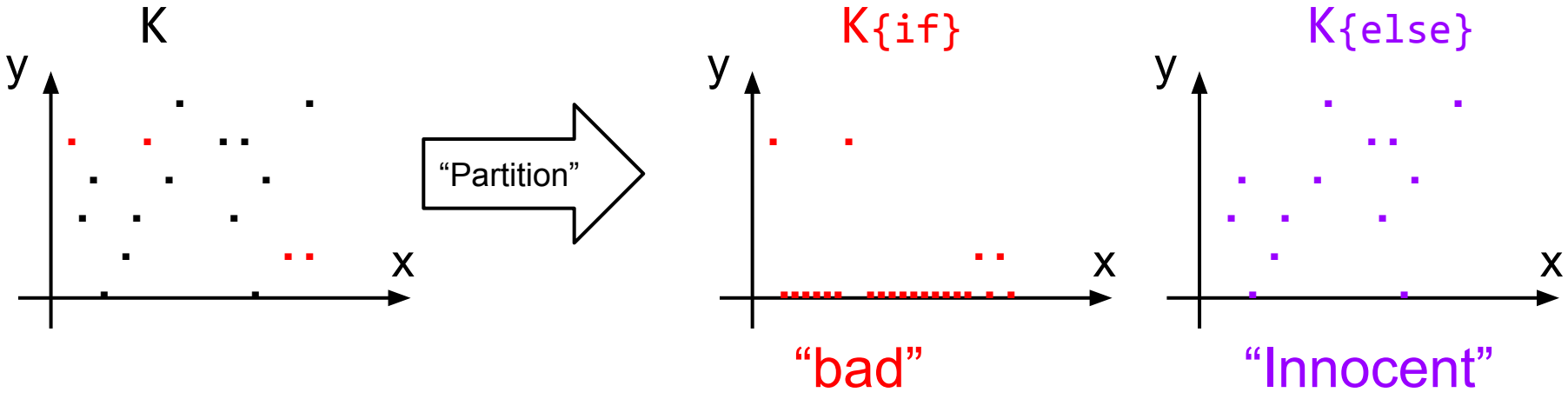
"bad"

"Innocent"

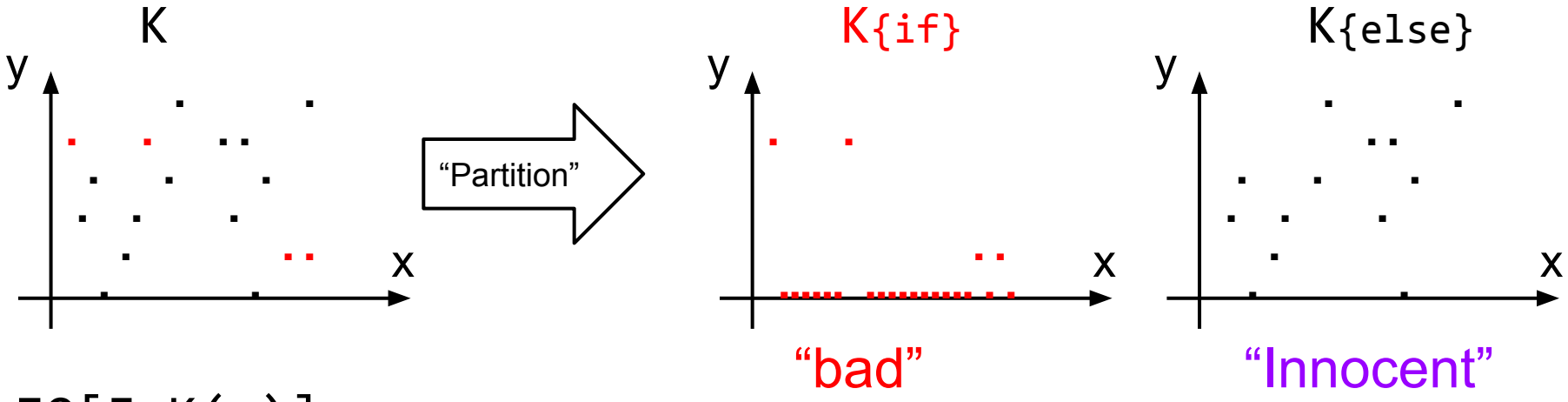
IO[F_K(x)]

indistinguishability Obfuscation

IO[if R(x, F_K(x))=1, F_K(x);
else, F_K(x).]



Attempt:
Hide the "bad" points
& puncture the "innocents"



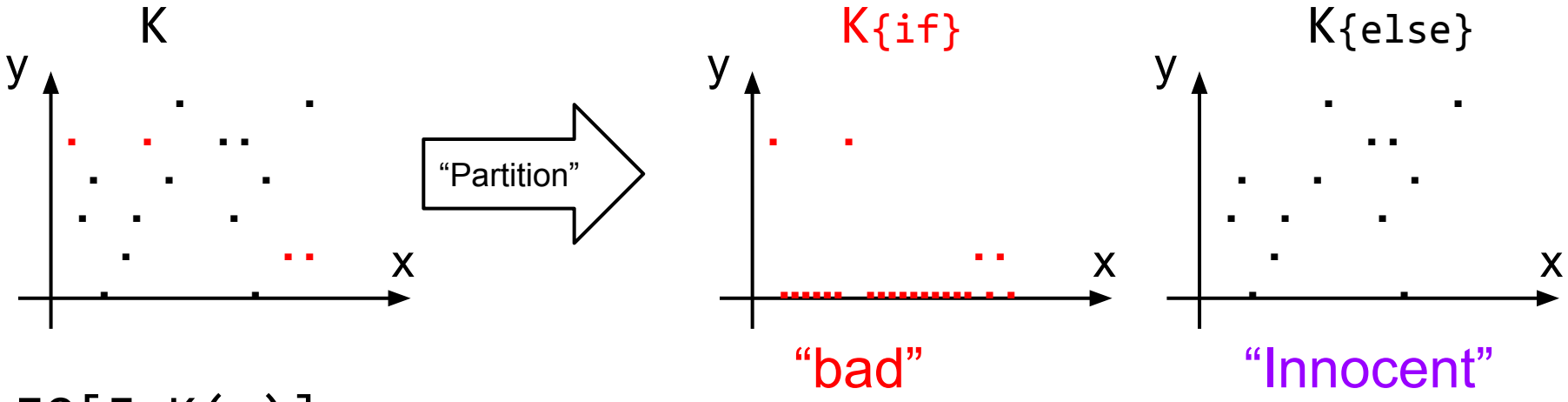
"bad"

"Innocent"

IO[F_K(x)]

indistinguishability Obfuscation

IO[OBF{ if R(x, F_K(x))=1, F_K(x)
else, "continue" };
if "continue", F_K(x).]



"bad"

"Innocent"

IO[F_K(x)]

indistinguishability Obfuscation

IO[OBF{ if R(x, F_K(x))=1, F_K(x)
else, "continue" };
if "continue", F_K(x).]

Evasive

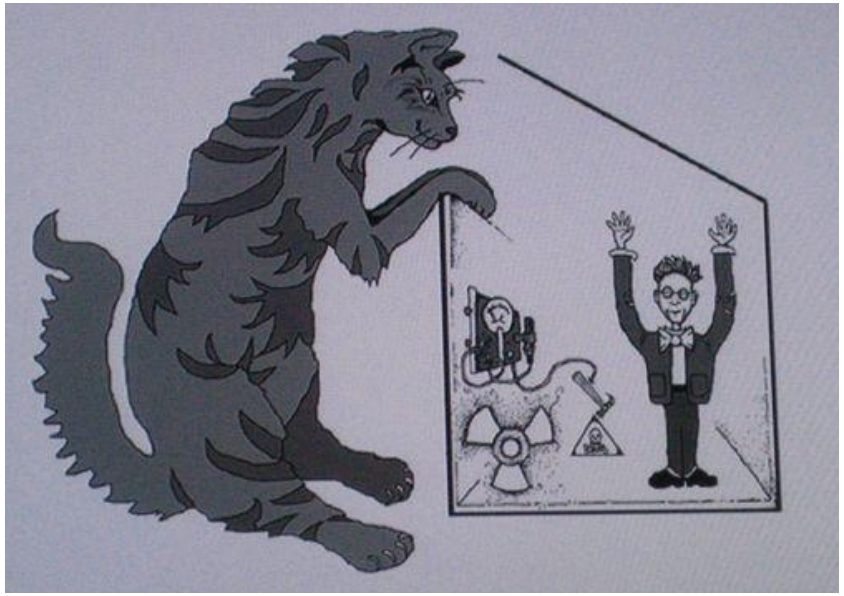
What do we know about the existence of obfuscators for Evasive circuit families?

	Evasive	General
Worst-case VBB	X	X
Average-case VBB		X
Worst-case VGB		
Average-case VGB		
Input-hiding Obf		Not apply

*not considering the definitions with related auxiliary input

	Evasive	General
Worst-case VBB	X	X
Average-case VBB	why not?	X
Worst-case VGB	why not?	why not?
Average-case VGB	why not?	why not?
Input-hiding Obf	why not?	Not apply

*not considering the definitions with related auxiliary input



Input-Hiding Obfuscation:

"Hide the inputs that evaluate to non-zero."

$$Pr_k[\ Adv(IHO(C_k(\ )),\ aux) \rightarrow x:\ C_k(x) \neq 0] < negl.$$

Input Hiding Obfuscation for Evasive Circuits

Candidate constructions

[Bitansky-Canetti-Kalai-Paneth ‘14]
VGB for NC^1 circuits can be constructed from semantic secure graded encoding.
VGB for NC^1 circuits implies IHO for NC^1 circuits.

[Badrinarayanan-Miles-Sahai-Zhandry ‘15]
IHO for NC^1 circuits in the “zeroing-free” idealized model.

+ Assuming the known bootstrapping techniques [GGHRSW ’13, BR ‘14] achieves IHO for evasive circuits in P/poly.

Input Hiding Obfuscation for Evasive Circuits

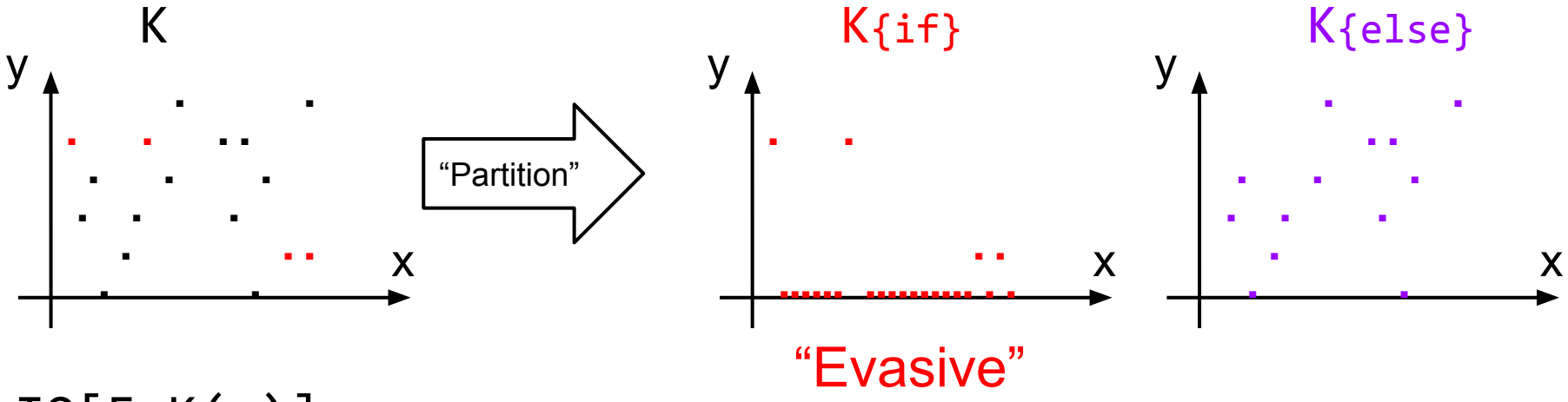
Candidate constructions

[Bitansky-Canetti-Kalai-Paneth ‘14]
VGB for NC^1 circuits can be constructed from semantic secure graded encoding.
VGB for NC^1 circuits implies IHO for NC^1 circuits.

[Badrinarayanan-Miles-Sahai-Zhandry ‘15]
IHO for NC^1 circuits in the “zeroing-free” idealized model.

+ Assuming the known bootstrapping techniques [GGHRSW ’13, BR ‘14] achieves IHO for evasive circuits in P/poly.

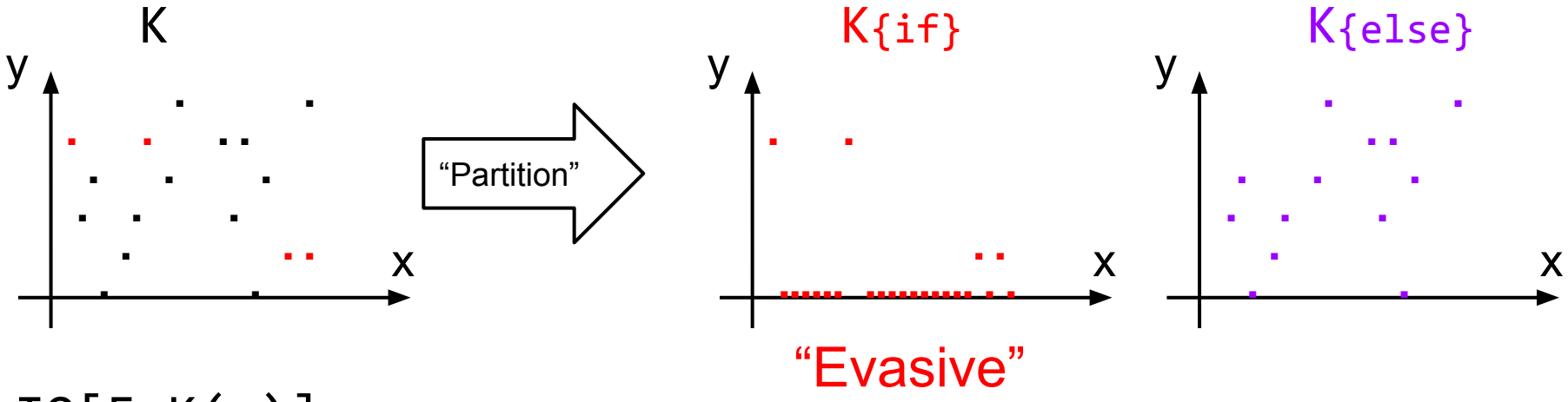
[Goldwasser-Rothblum ‘07]: “iO is the best-possible obfuscator”



IO[F_K(x)]

indistinguishability Obfuscation

IO[IHO{ if R(x, F_K(x))=1, F_K(x)
else, "continue" };
if "continue", F_K(x).]



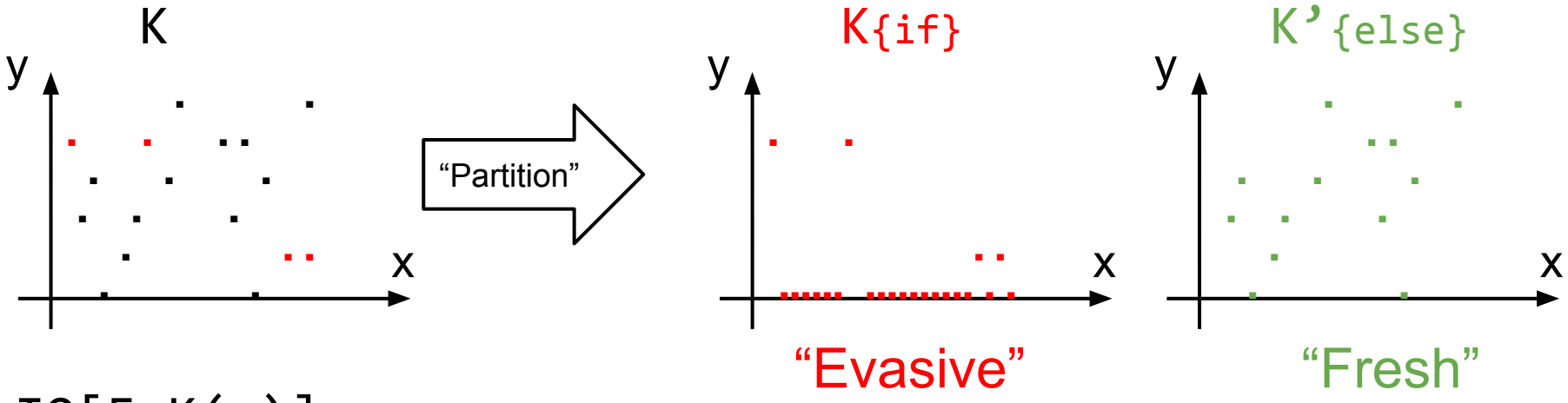
"Evasive"

IO[F_K(x)]

indistinguishability Obfuscation

IO[IHO{ if R(x, F_K(x))=1, F_K(x)
else, "continue" };
if "continue", F_K(x).]

Still, have to get rid of the related key outside the IHO Box



IO[F_K(x)]

indistinguishability Obfuscation

IO[IHO{ if R(x, F_K(x))=1, F_K(x)
else, "continue" };
if "continue", F_K(x).]

IO[IHO{ if R(x, F_K(x))=1, F_K(x)
else, "continue" };
if "continue", G_K'(x).]

s.t. G_K'(x) is:
(1) Independent from F_K;
(2) No (x,y) on G_K' are in R

Shown to be indistinguishable by a lemma derived from [Canetti-Lin-Tessaro-Vaikuntanathan 15]:

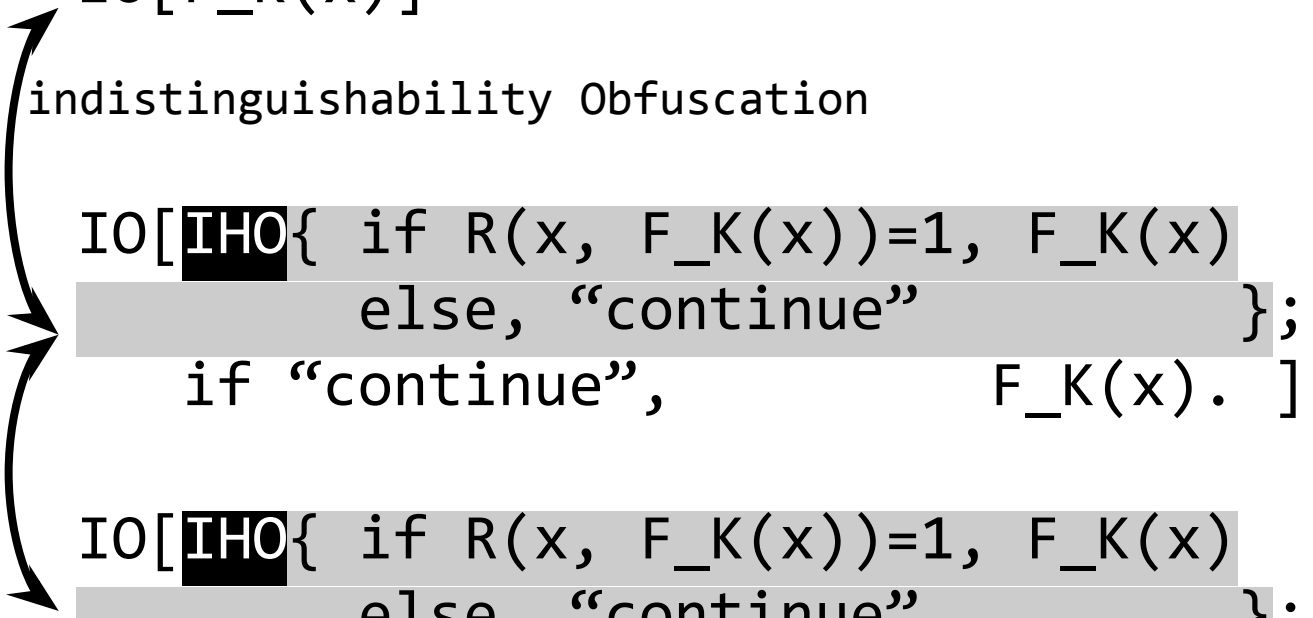
if F1 and F2 are subexp. secure puncturable PRFs, and iO is subexp. secure, then:

$$iO(F1) \approx iO(F2)$$

```
IO[F_K(x)]

indistinguishability Obfuscation

IO[IHO{ if R(x, F_K(x))=1, F_K(x)
        else, “continue”          };
   if “continue”,          F_K(x). ]

IO[IHO{ if R(x, F_K(x))=1, F_K(x)
        else, “continue”          };
   if “continue”,          G_K’(x). ]
```

s.t. G_K’(x) is:
(1) Independent from F_K;
(2) No (x,y) on G_K’ are in R

Assuming Puncturable_PRF (sub.exp.hard)
Assuming Indistinguishability_Obfuscation (sub.exp.hard)
Assuming Input_Hiding_Obfuscation_for_Evasive_Circuits



s.t. G_K’(x) is:
(1) Independent from F_K;
(2) No (x,y) on G_K’ are in R

Assuming Puncturable_PRF (sub.exp.hard)
Assuming Indistinguishability_Obfuscation (sub.exp.hard)
Assuming Input_Hiding_Obfuscation_for_Evasive_Circuits

Ind.Obf(Puncturable.PRF( ) {with Padding})

is bounded correlation intractable.

↓

given a polynomial upper bound on the computational complexity of the relation.

The Redemption

Correlation intractability was sometimes cited as unconditionally impossible.
It becomes the “excuse” for the alternative definitions of Random Oracles to avoid some desirable properties.

Correlation intractability was sometimes cited as unconditionally impossible.
It becomes the "excuse" for the alternative definitions of Random Oracles to avoid some desirable properties.

Canetti et al. [6] as the inability of the attacker to find any input x such that the pair $(x, f_s(x))$ satisfies any "non-trivial relation" (cf. Section 4). Canetti et al. proved that correlation-intractability is not realizable when the adversary sees the entire seed s, but we point out that it may be realizable when the adversary is only given the "compressed seed" σ. We note that the negative

DISCUSSION, LIMITATIONS AND RELATED WORK. That the source adversary in UCE does not get the key is important in avoiding impossibility results like those in [55, 103]. (For example, UCE does not imply correlation intractability as defined, and shown to be unachievable in the standard model, by [55].)

Open Problems

Open Problems

Checklist

CI for more relations
"Fiat-Shamir" relations
CI with assumptions that are better understood
CI that is more environmental friendly
Cryptoanalysis of SHA2, Keccak, Spritz, ...

Input-hiding obfuscation related questions

A: Please.
B: Please.
A: I insist.
B: So do I.
A: OK then, thank you.
B: You are most welcome.

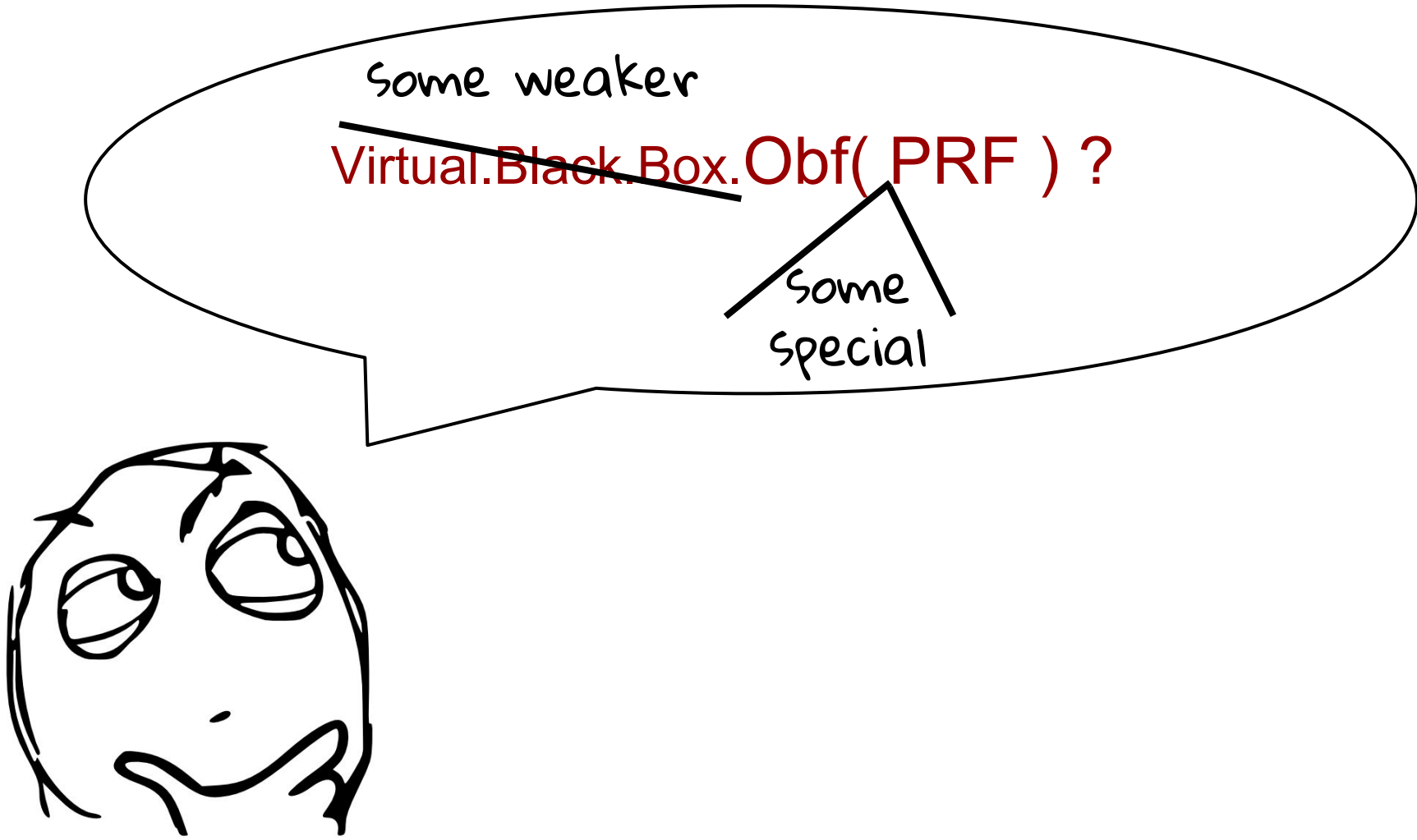
A protocol for two Italians to pass through a door.
Source: Silvio Micali, 1985.

...without knowing any of
...well

The End

Scenes

(a.k.a. slides that are removed from the earlier versions)


Some weaker
Virtual Black Box
Obf(PRF) ?
Some
special

The “diagonal” relation is sparse when the key is “short” (compared to the input).

h \ A(h)->h	000	001	010	011	...	111
000	■				...	
001		■			...	
010			■		...	
011				■	...	
...	...	...	...	...	...	...
111					...	■

R^H: (x, y) ∈ R^H if y=x(x)