EXTRACTABLE FUNCTIONS

FICTION OR REALITY?

Nir Bitansky (TAU)

Ran Canetti (BU & TAU)

Omer Paneth (BU)

Alon Rosen (IDC)

Knowledge is Elusive
(assuming $\mathrm{P} \neq \mathrm{NP}$)

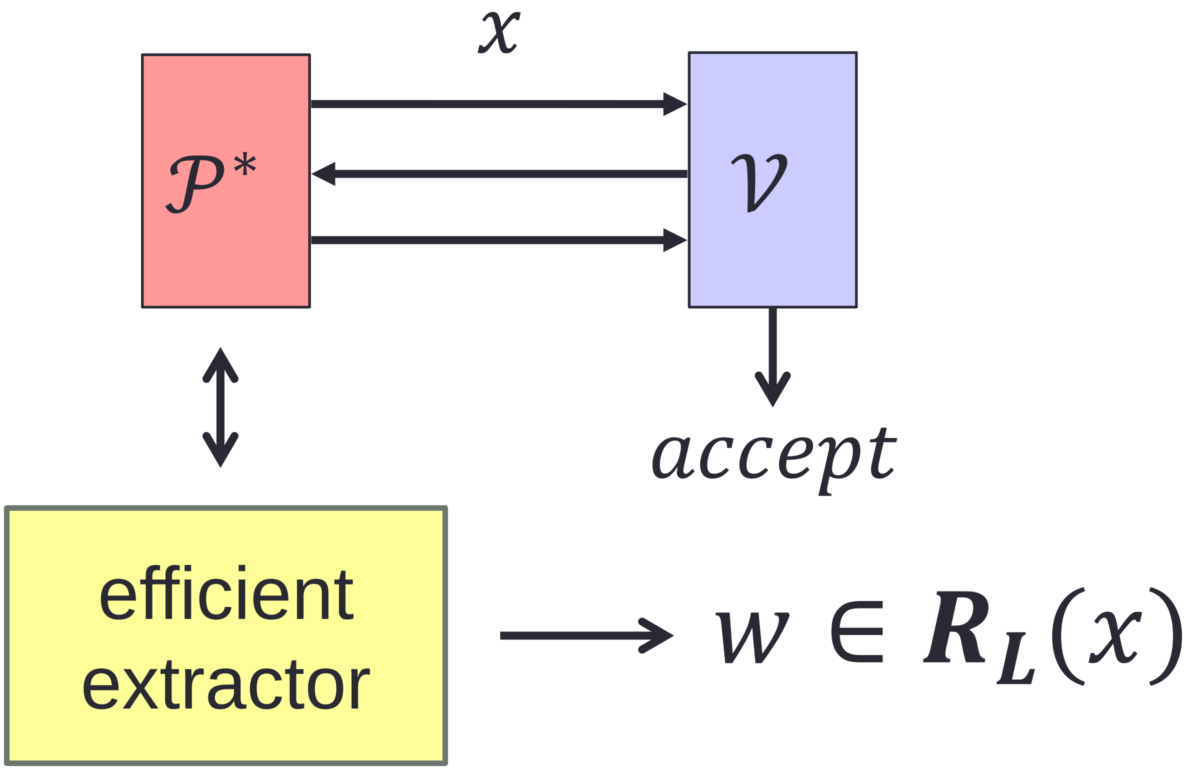
Knowing $N \notin \mathbf{Primes}$ isn't like knowing $p|N$

Knowing $\mathbf{Enc}(x)$ isn't like knowing x

Knowing how to prove $x \in \mathbf{L}$
isn't like knowing $w \in \boldsymbol{R_L}(x)$

ZK Proofs of Knowledge

Goldwasser-Micali-Rackoff, Feige-Shamir, Goldreich-Bellare



x

$\mathcal{P}^*$

$\mathcal{V}$

$accept$

efficient extractor

$w \in \boldsymbol{R}_L(x)$

Effective Knowledge

=

what can be *efficiently extracted* from the adversary

Extraction is Essential to Cryptographic Analysis

⋮

Input Independence in MPC

Composition

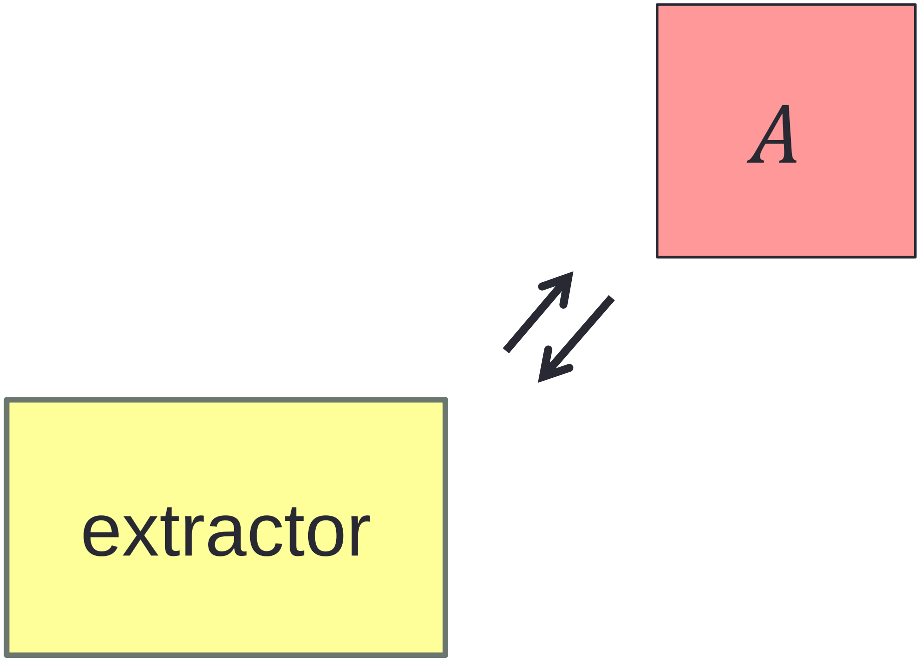
ZK simulation (the trapdoor paradigm)

⋮

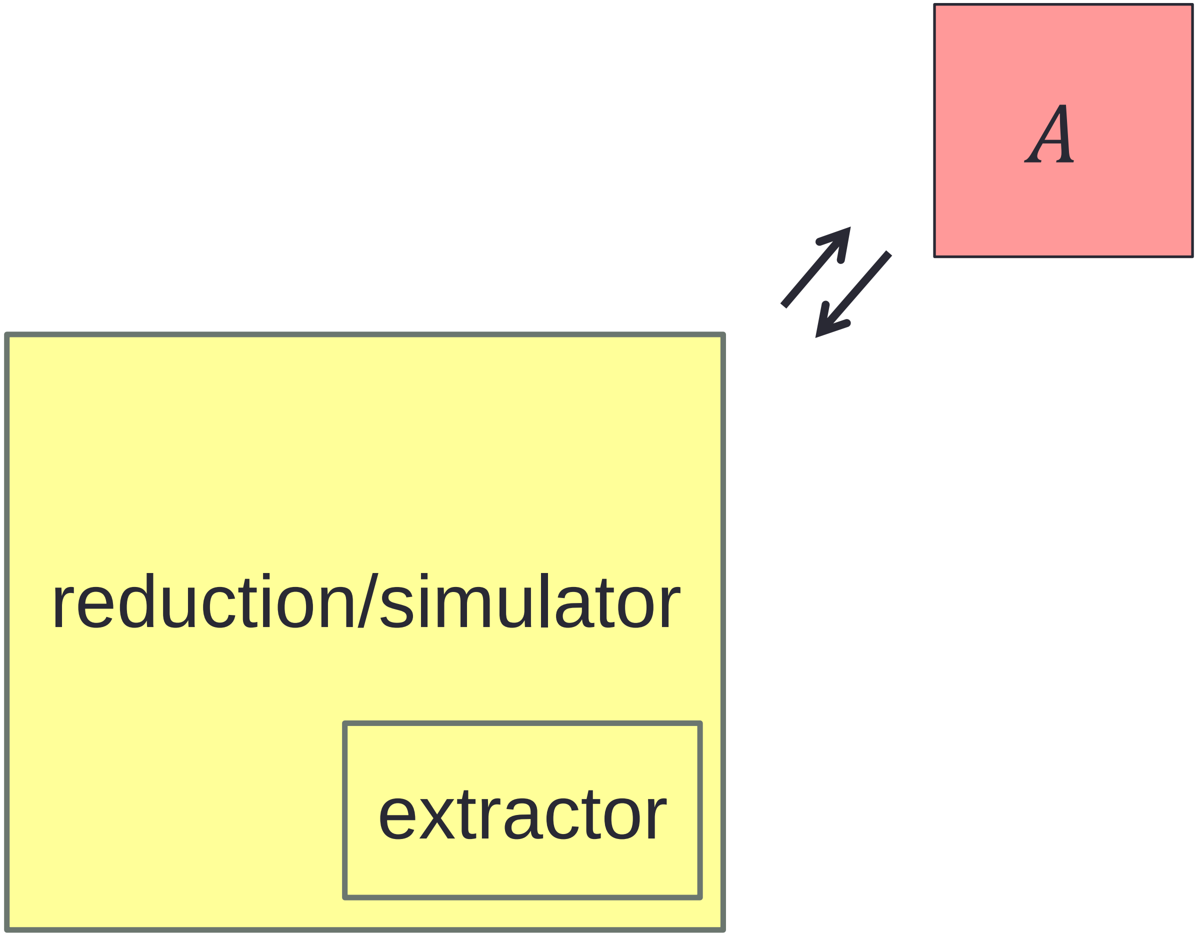
How is Knowledge Extracted?

The Black-Box Tradition

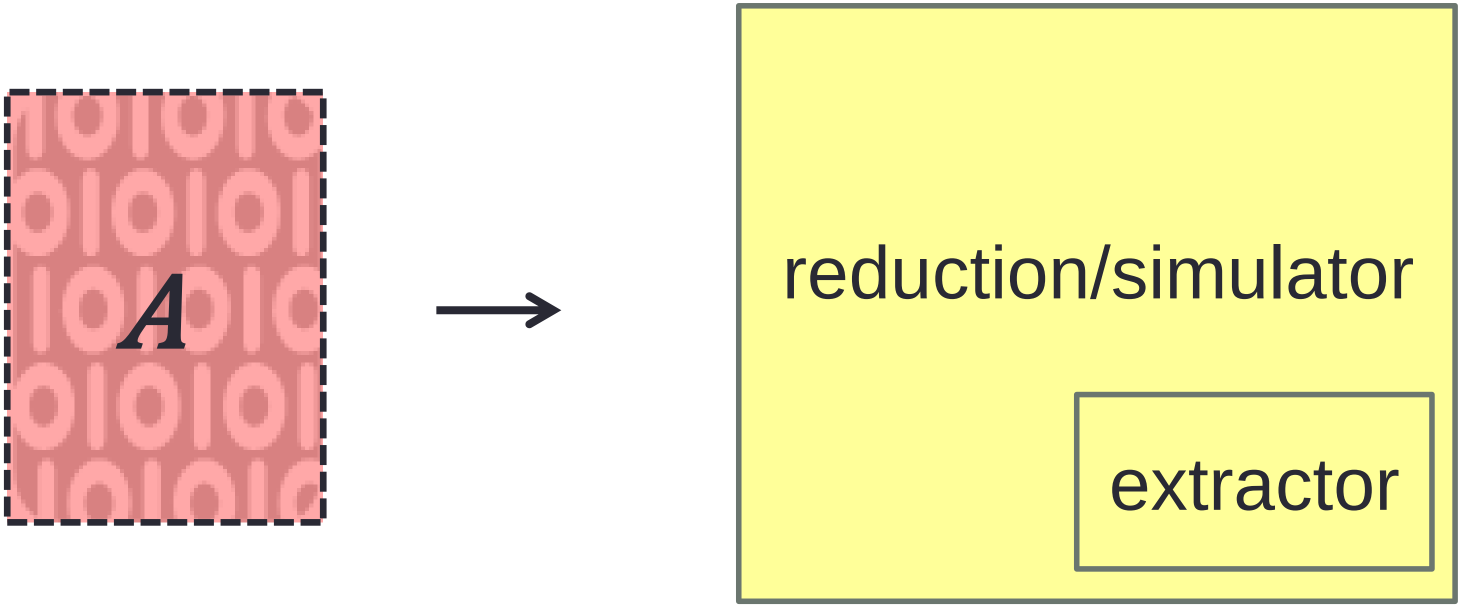
(aka Rewinding)



Black-Box (Turing) Reductions/Simulators



Using The Adversary’s Code



A

reduction/simulator

extractor

The Black-Box Barrier

O(1)-public-coin-ZK
Goldreich-Krawczyk

3-ZK
Goldreich-Krawczyk

⋱

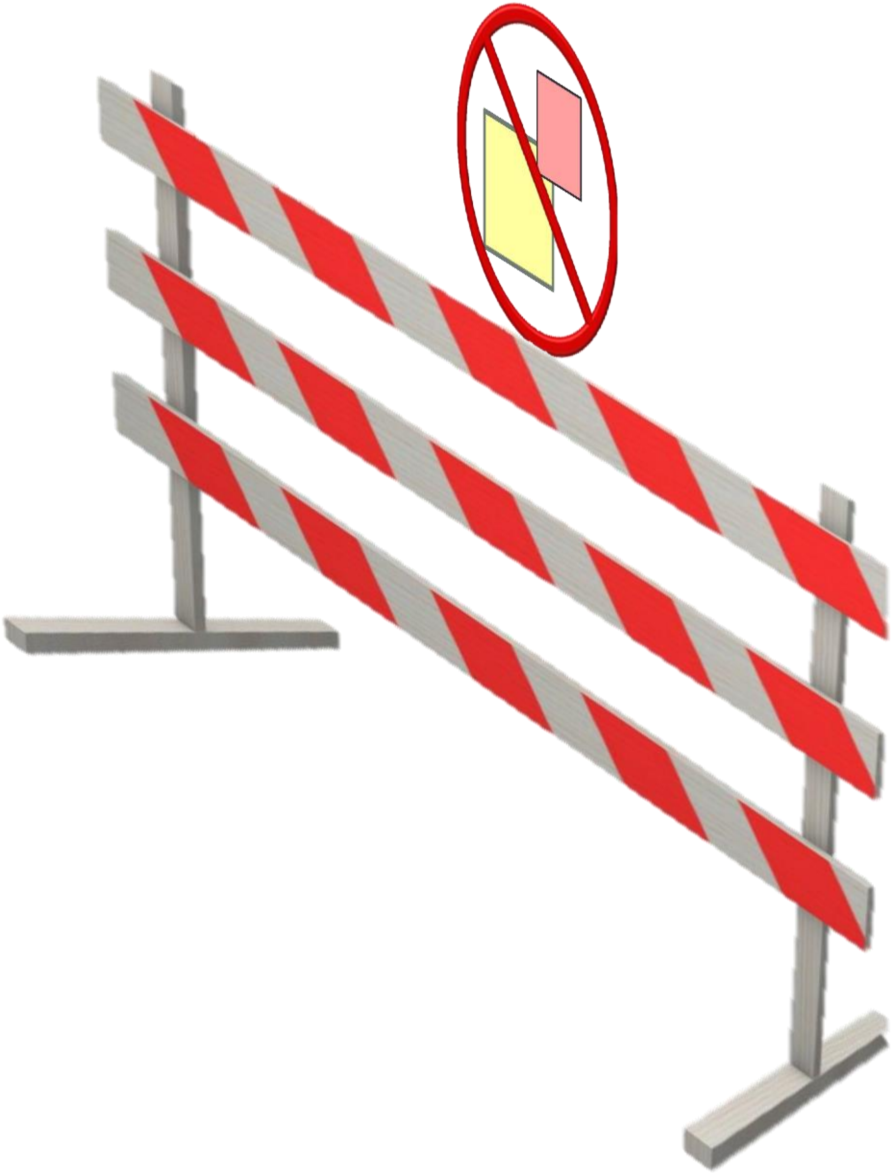
SNARGs for NP
(Succinct Non-Interactive Arguments)
Gentry-Wichs

most of crypto
as we know it!

Black-Box

Non-Black-Box

Beyond the Barrier



Barak

$O(1)$-round public-coin ZK
with
non-black-box simulation

Post Barak

resettably-sound-ZK
Barak-Goldreich-Goldwasser-Lindell

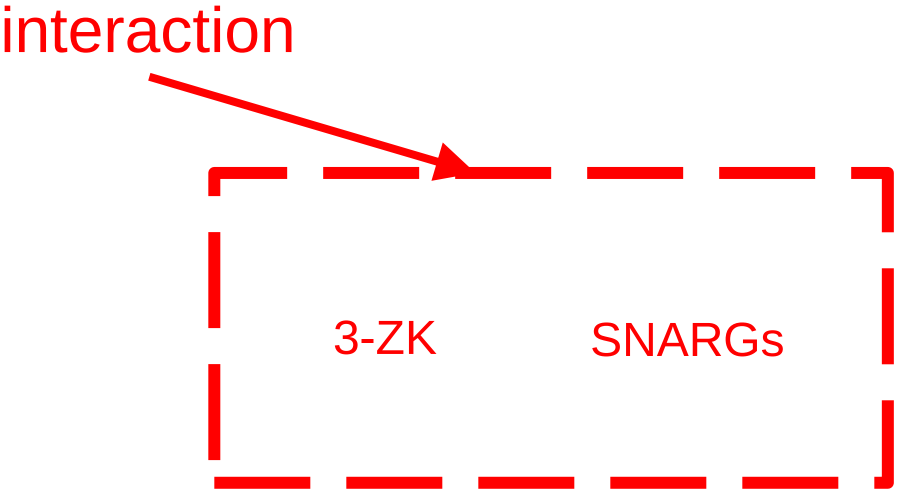
O(1)-public-coin-ZK
Barak

simultaneously-resettable-ZK
Deng-Goyal-Sahai

...

O(1)-covert-MPC
Goyal-Jain

(uniform) O(1)-concurrent-ZK
Chung-Lin-Pass



interaction

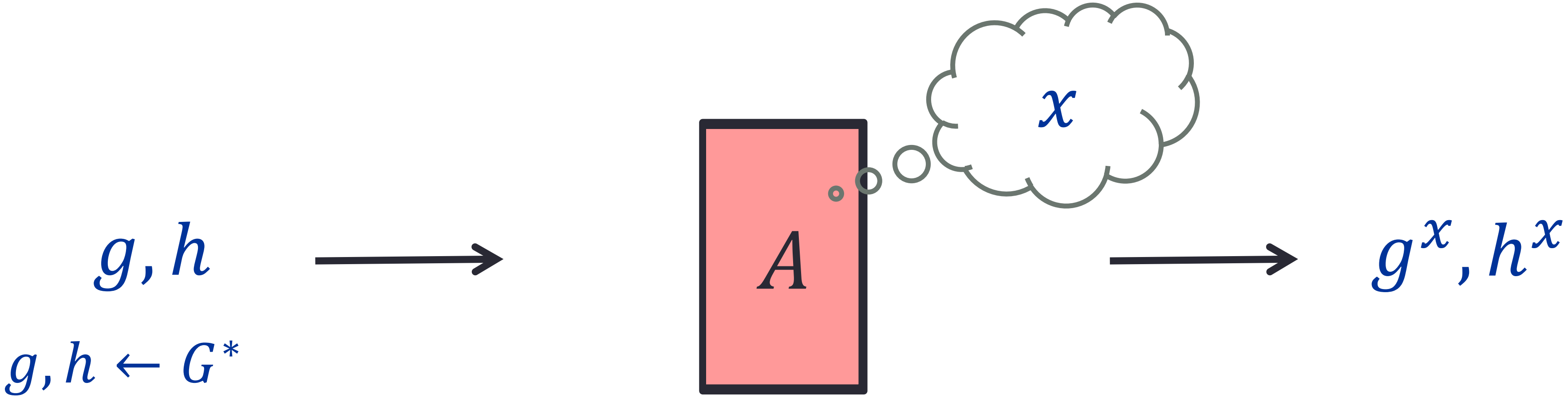
3-ZK

SNARGs

Knowledge Assumptions
and
Extractable Functions

Damgård’s Knowledge of Exponent Assumption

Damgård’s Knowledge of Exponent Assumption



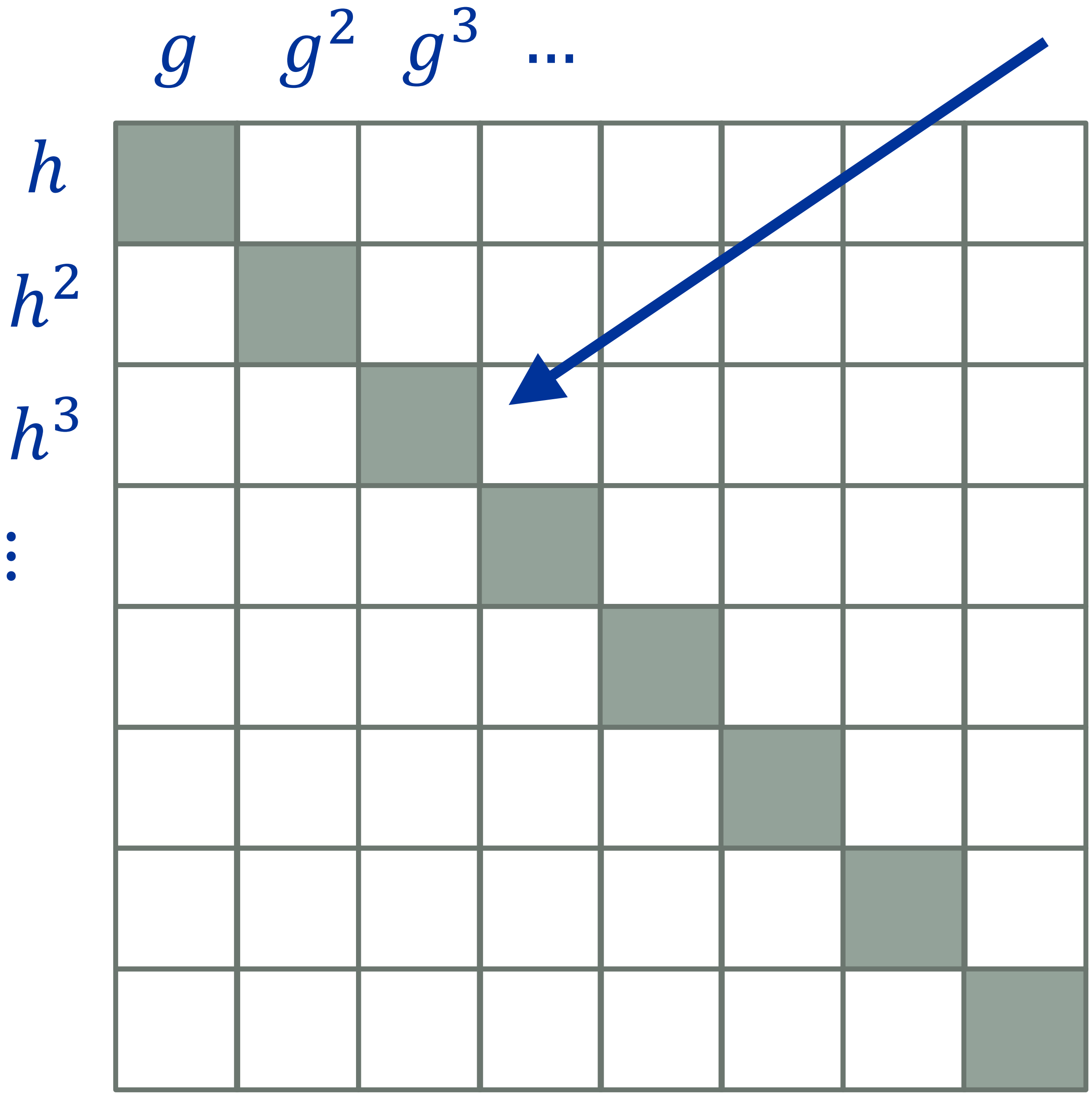
g, h

$g, h \leftarrow G^*$

A

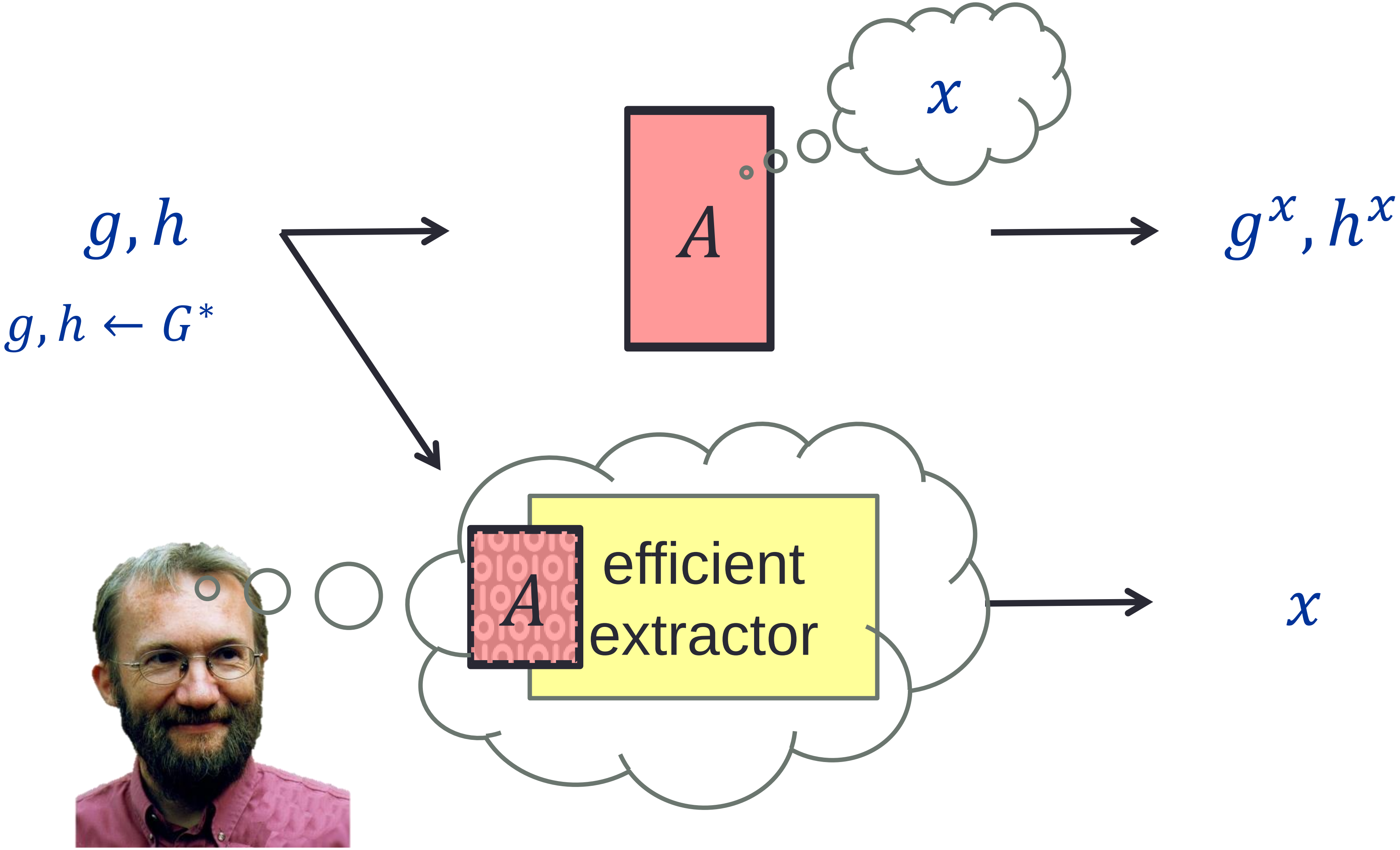
x

g^x, h^x



$\{g^x, h^x : x \in Z_q\}$ is $\frac{1}{q}$-sparse

Damgård’s Knowledge of Exponent Assumption



g, h

$g, h \leftarrow G^*$

A

x

g^x, h^x

A

efficient extractor

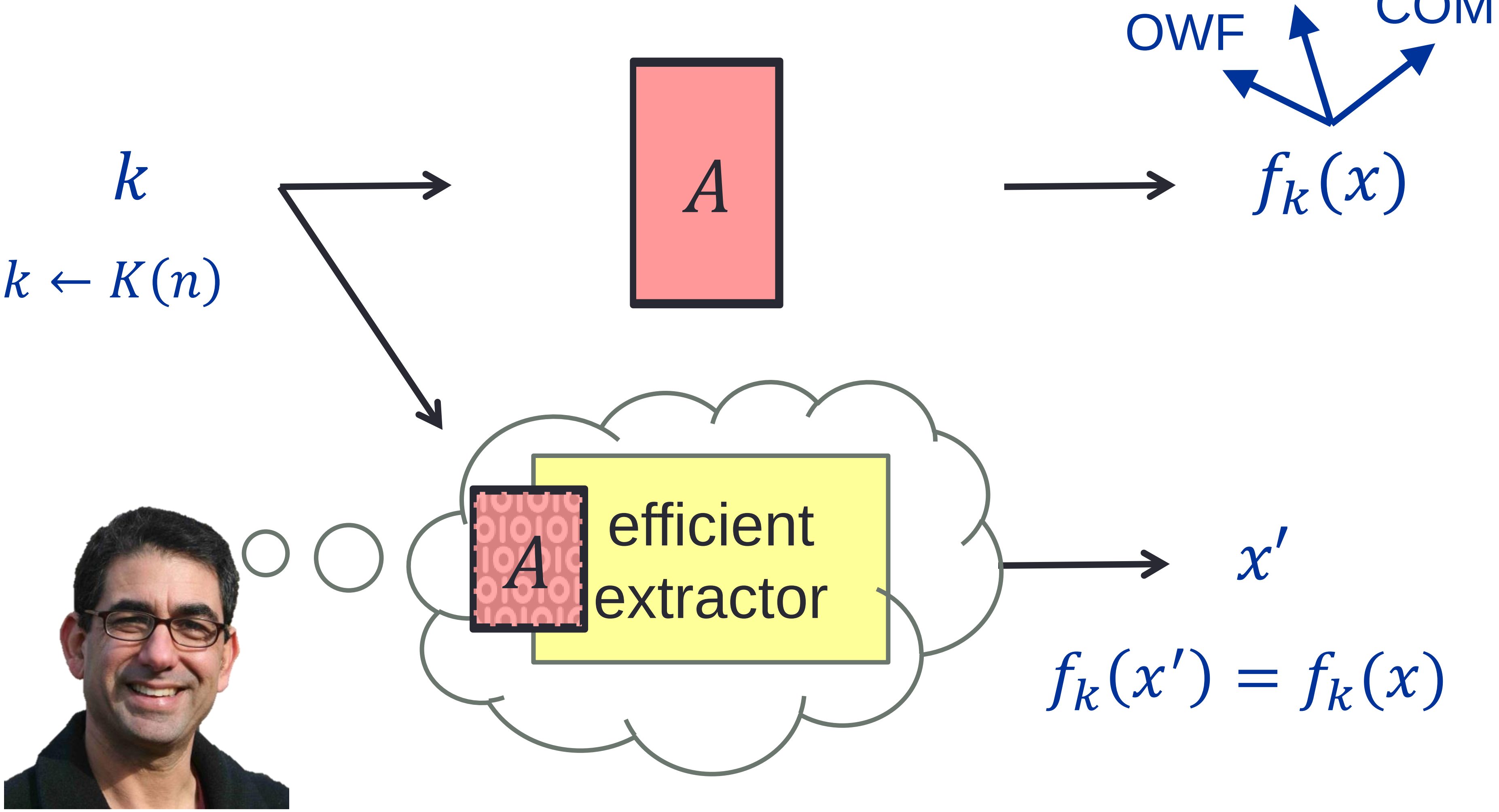
x

Extractable Functions

Canetti-Dakdouk

Extractable Functions

Canetti-Dakdouk



k

$k \leftarrow K(n)$

A

$f_k(x)$

OWF

CRH

COM

A

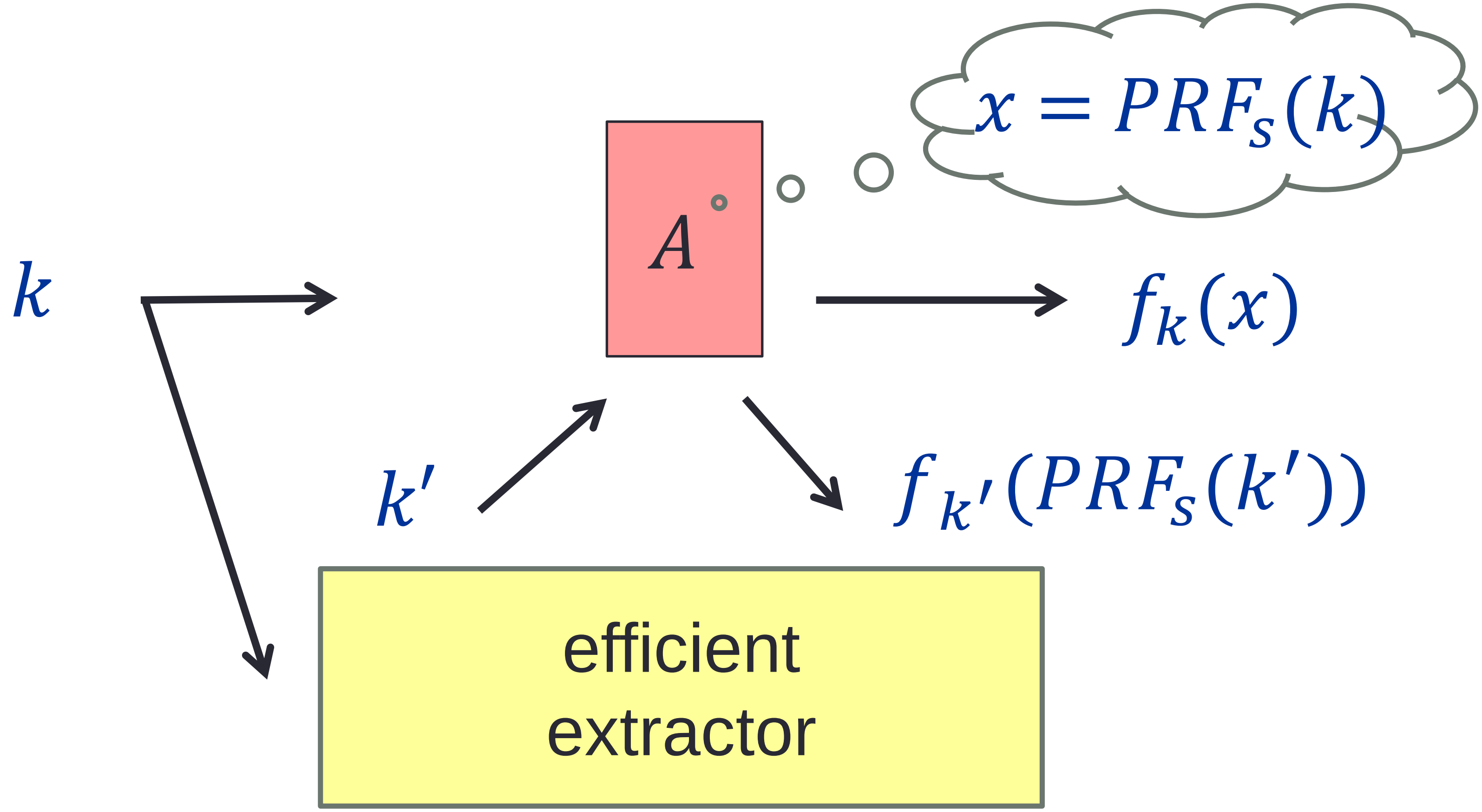
efficient extractor

x'

$f_k(x') = f_k(x)$

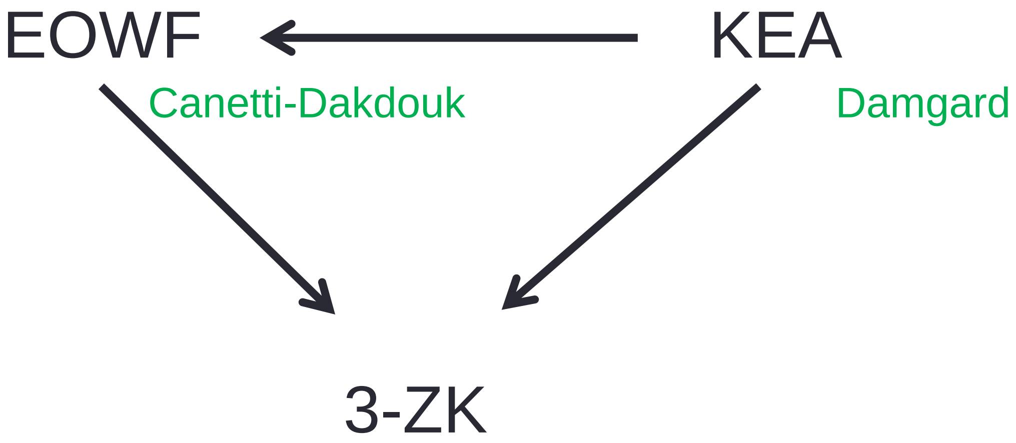
Black-Box Extraction is Impossible

Black-Box Extraction is Impossible



black-box extractor must invert the one-way f_k

Extractable Functions in Non-Interactive Applications



EOWF

KEA

Canetti-Dakdouk

Damgard

3-ZK

B-Canetti-Chiesa-Goldwasser-Lin-Rubinstein-Tromer

Hada-Tanaka,
Micali-Lepinski*,
Bellare-Palacio

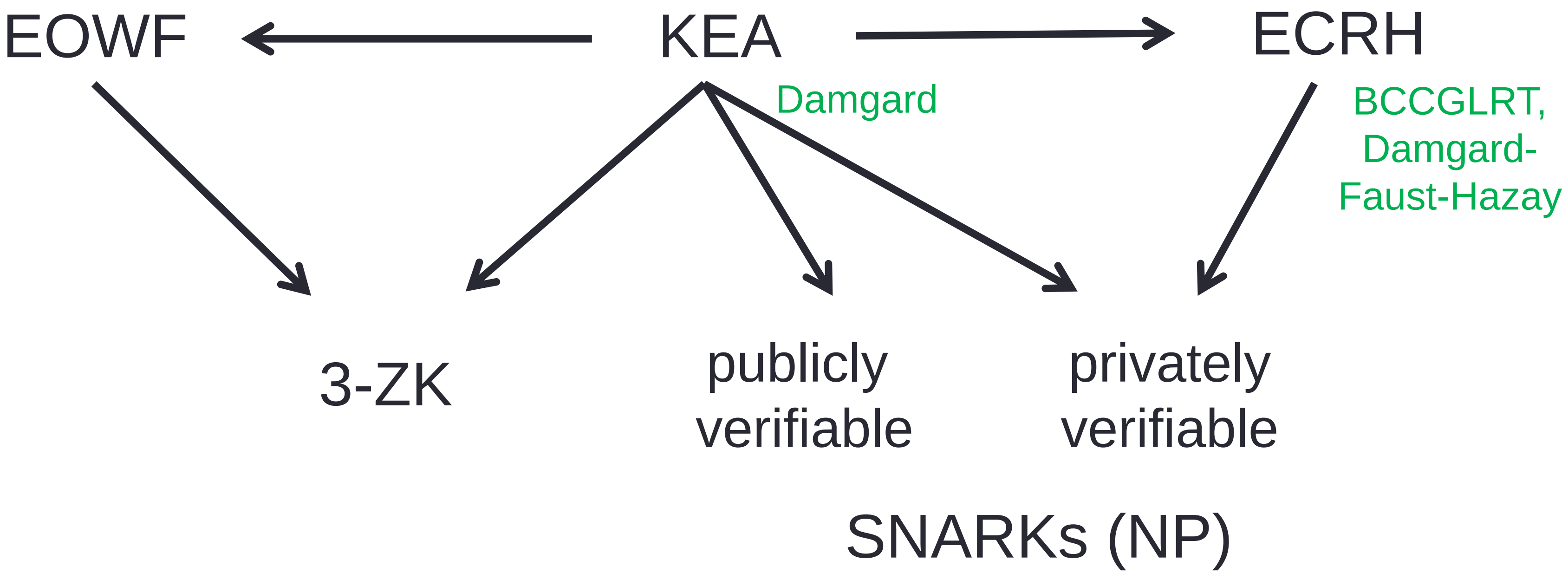
O(1)-concurrent ZK

*assuming concurrent extraction

BCCGLRT

Gupta-Sahai

Extractable Functions in Non-Interactive Applications



EOWF

KEA

ECRH

Damgard

BCCGLRT, Damgard-Faust-Hazay

3-ZK

publicly verifiable

privately verifiable

SNARKs (NP)

O(1)-concurrent ZK

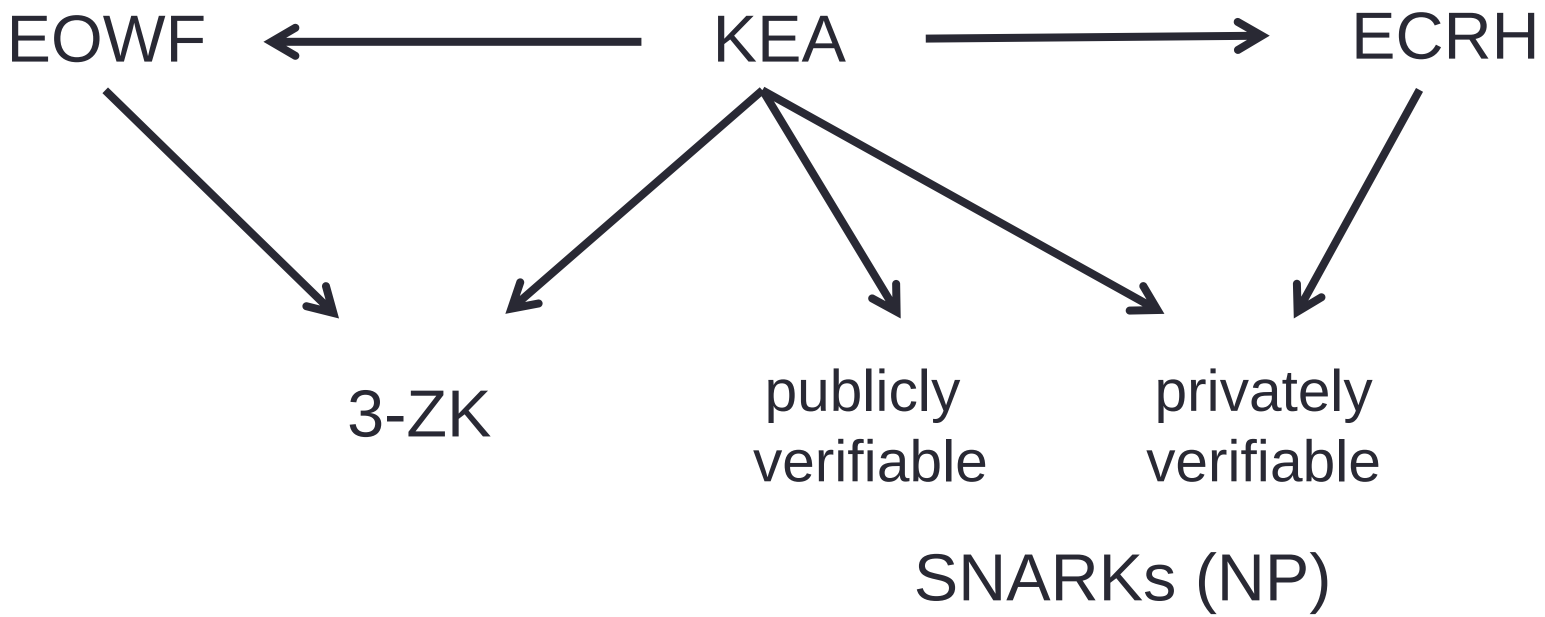
*assuming concurrent extraction

Groth,Lipmaa, B-Canetti-Chiesa-Tromer, Gennaro-Gentry-Parno-Raykiova, B-Chiesa-Ishai-Ostrovsky-Paneth

Mie, DiCrescenzo -Lipmaa*

BCCGLRT, DFH

Extractable Functions in Non-Interactive Applications



EOWF

KEA

ECRH

3-ZK

publicly verifiable

privately verifiable

SNARKs (NP)

O(1)-concurrent ZK

*assuming concurrent extraction

succinct keys
in functional
enc/sig

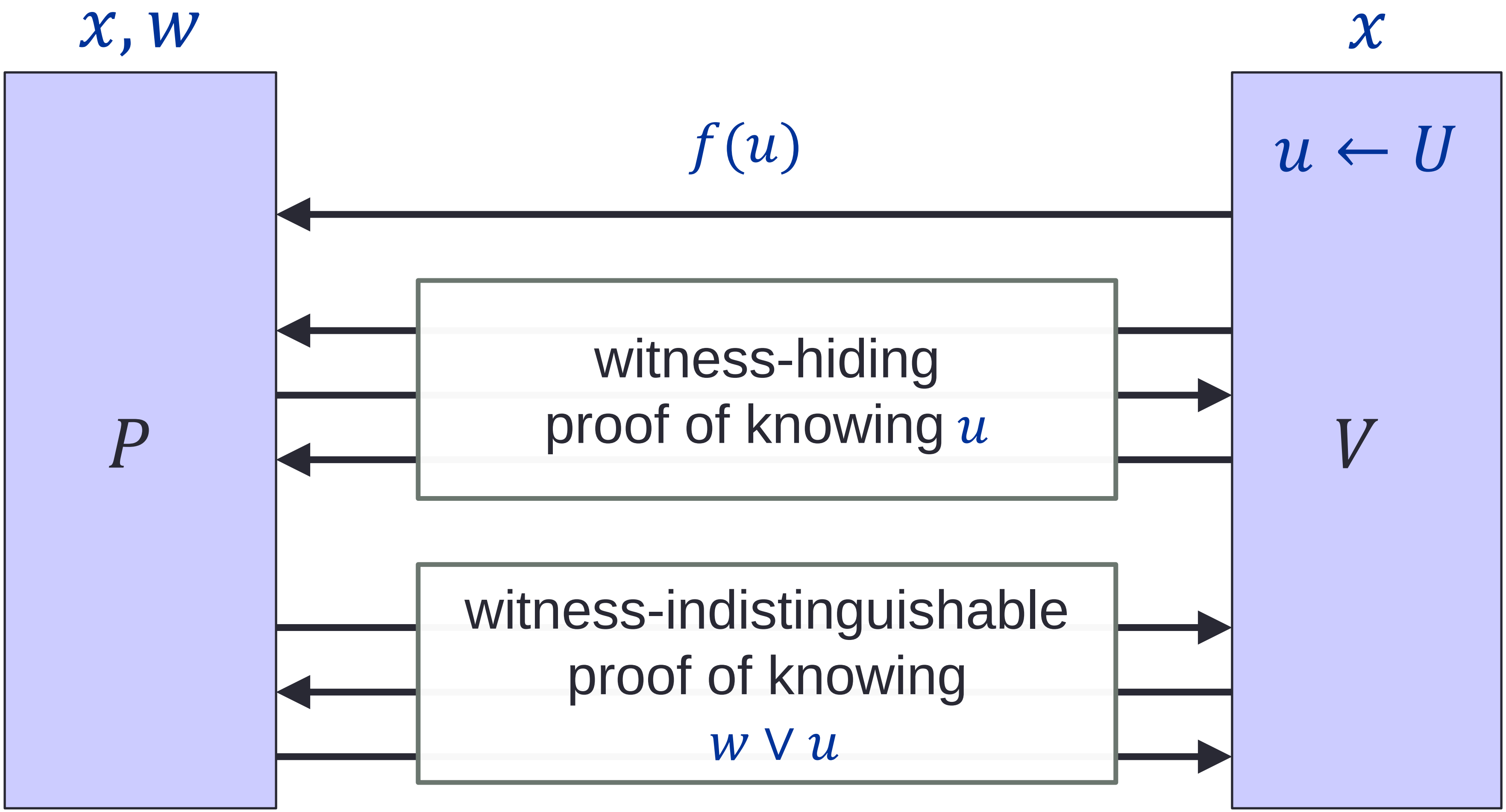
delegation

targeted-malleability

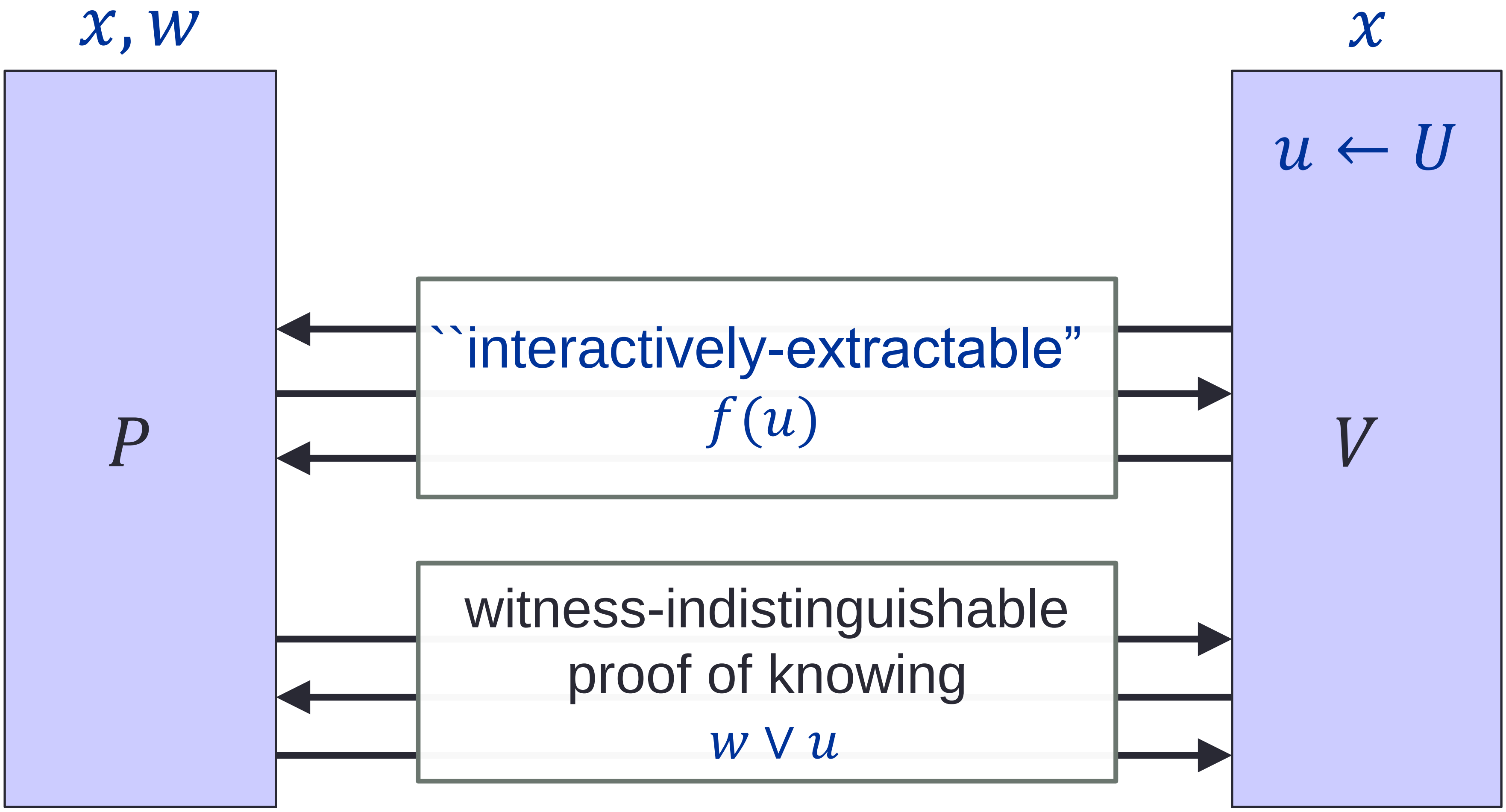
proof-carrying data

Example: 3-ZK

The Feige-Shamir Protocol



The Feige-Shamir Protocol



x, w

x

$u \leftarrow U$

``interactively-extractable”

$f(u)$

P

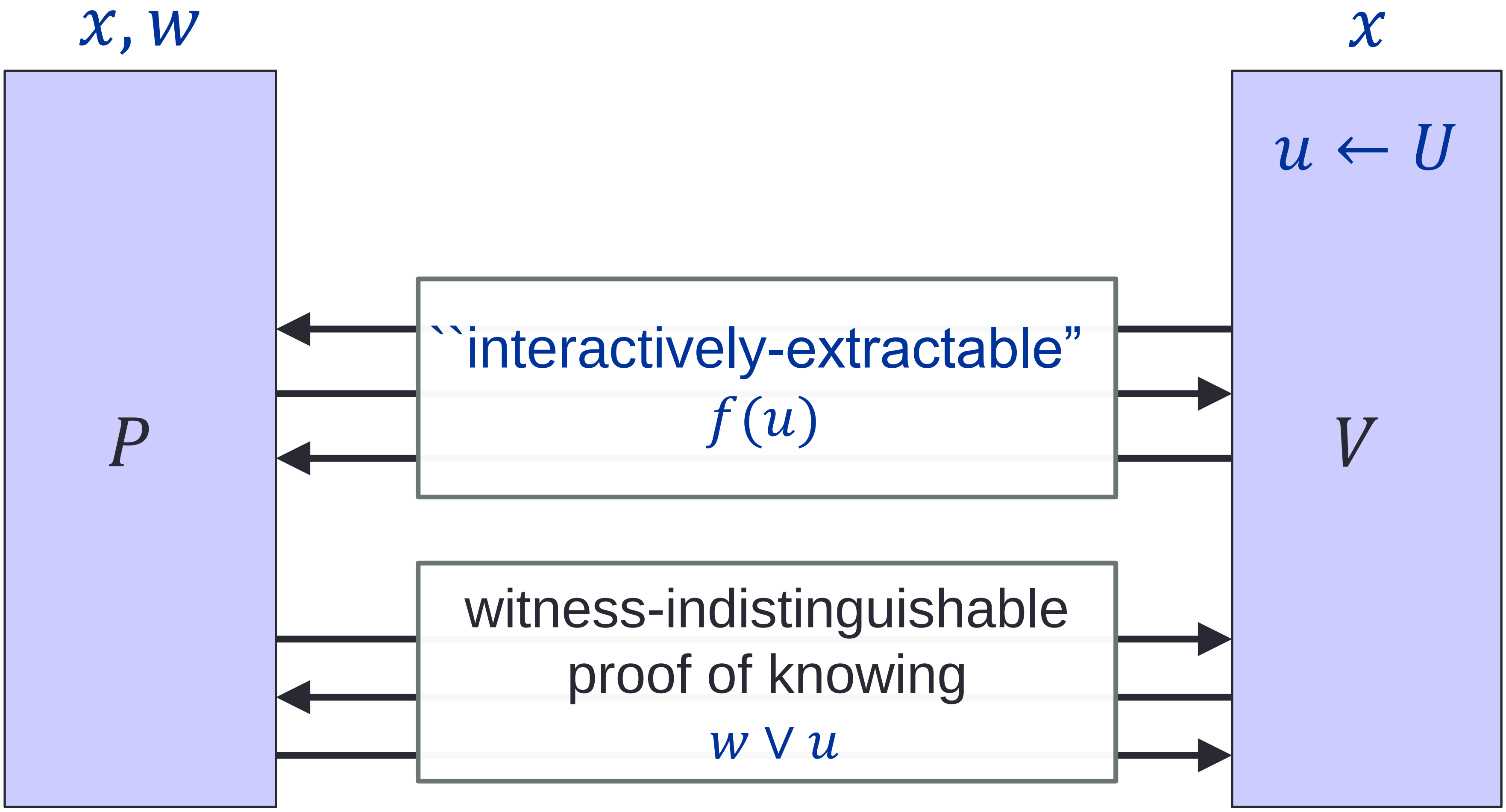
V

witness-indistinguishable proof of knowing

$w \vee u$

3-ZK from EOWFs

B-Goldwasser-Canetti-Chiesa-Lin-Rubinstein-Tromer



x, w

x

$u \leftarrow U$

P

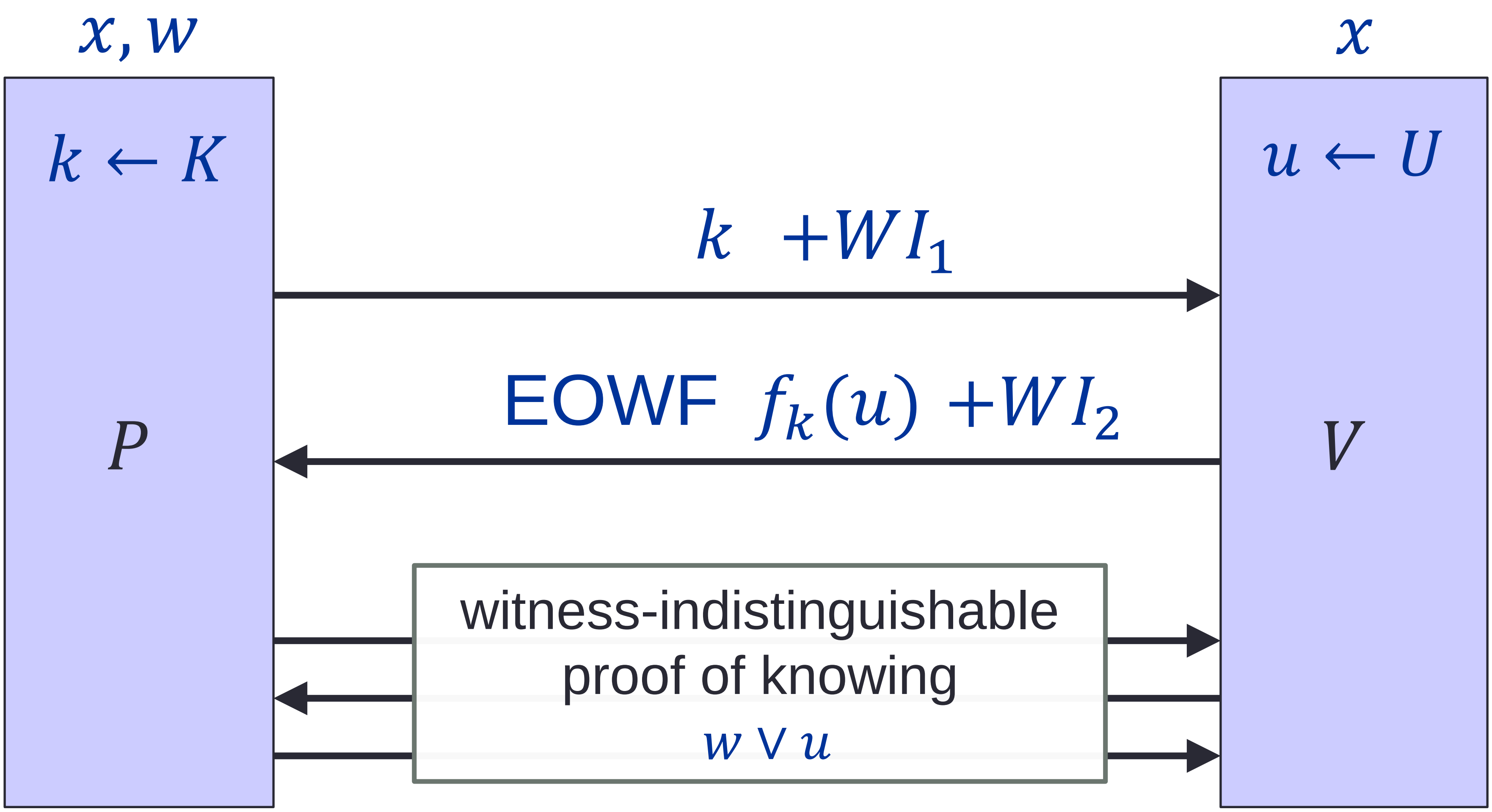
V

``interactively-extractable”
$f(u)$

witness-indistinguishable
proof of knowing
$w \vee u$

3-ZK from EOWFs

B-Goldwasser-Canetti-Chiesa-Lin-Rubinstein-Tromer



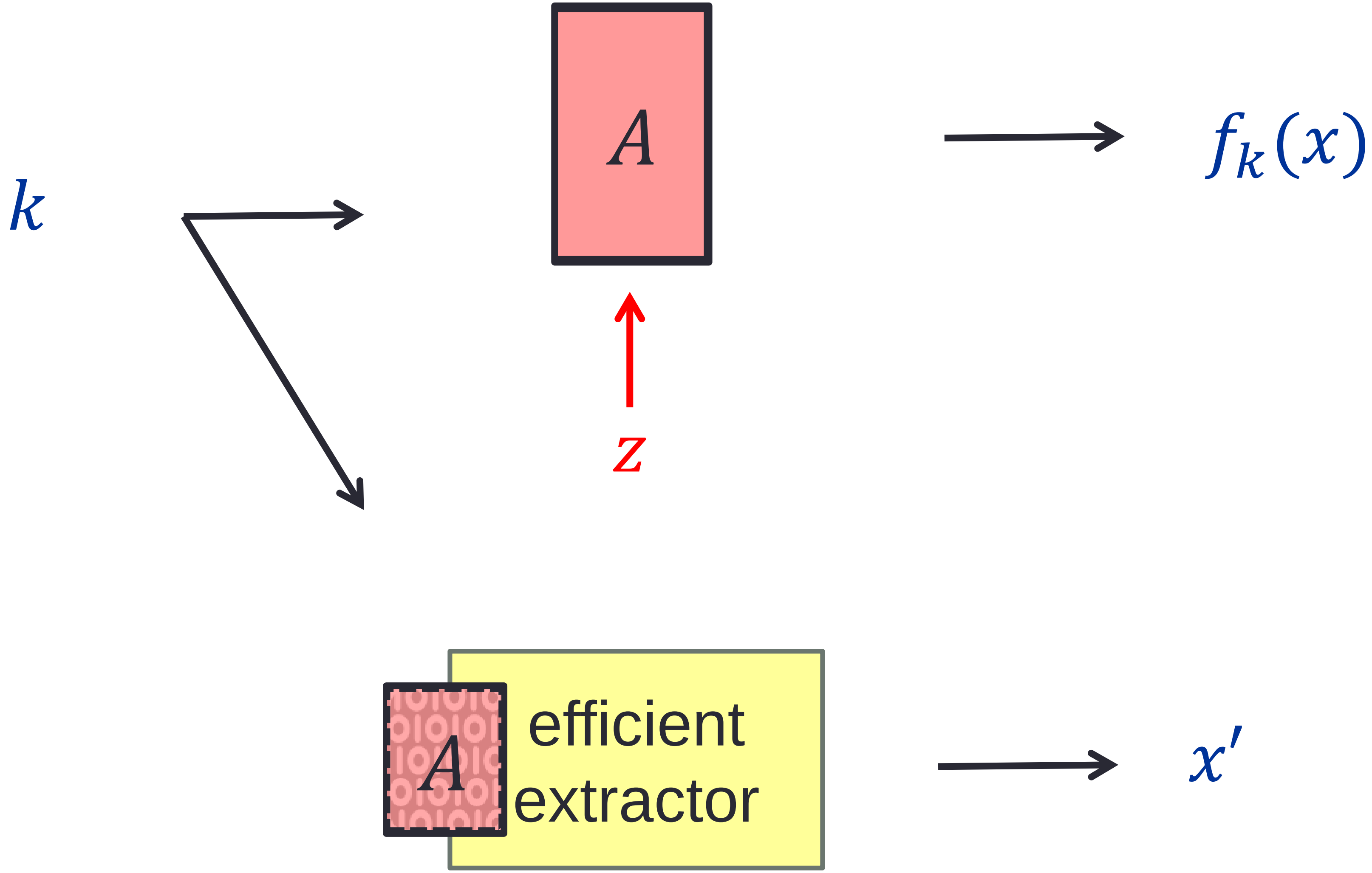
Do Extractable Functions Really Exist?

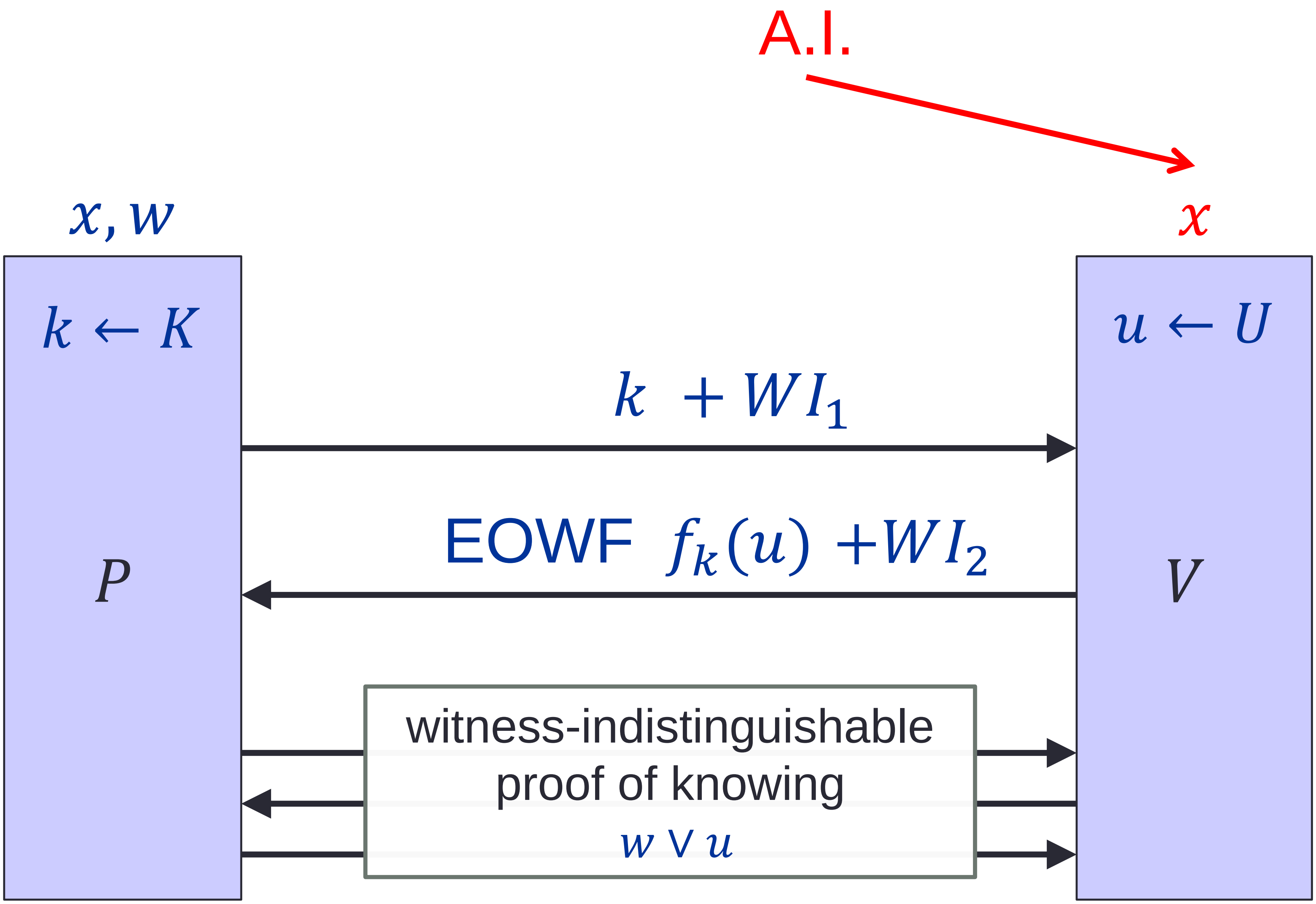
What’s Beyond Knowledge Assumptions?

Can We Construct Explicit Extractors?

Auxiliary Information

Auxiliary Information





A.I.

x, w

x

$k \leftarrow K$

$u \leftarrow U$

$k \ + WI_1$

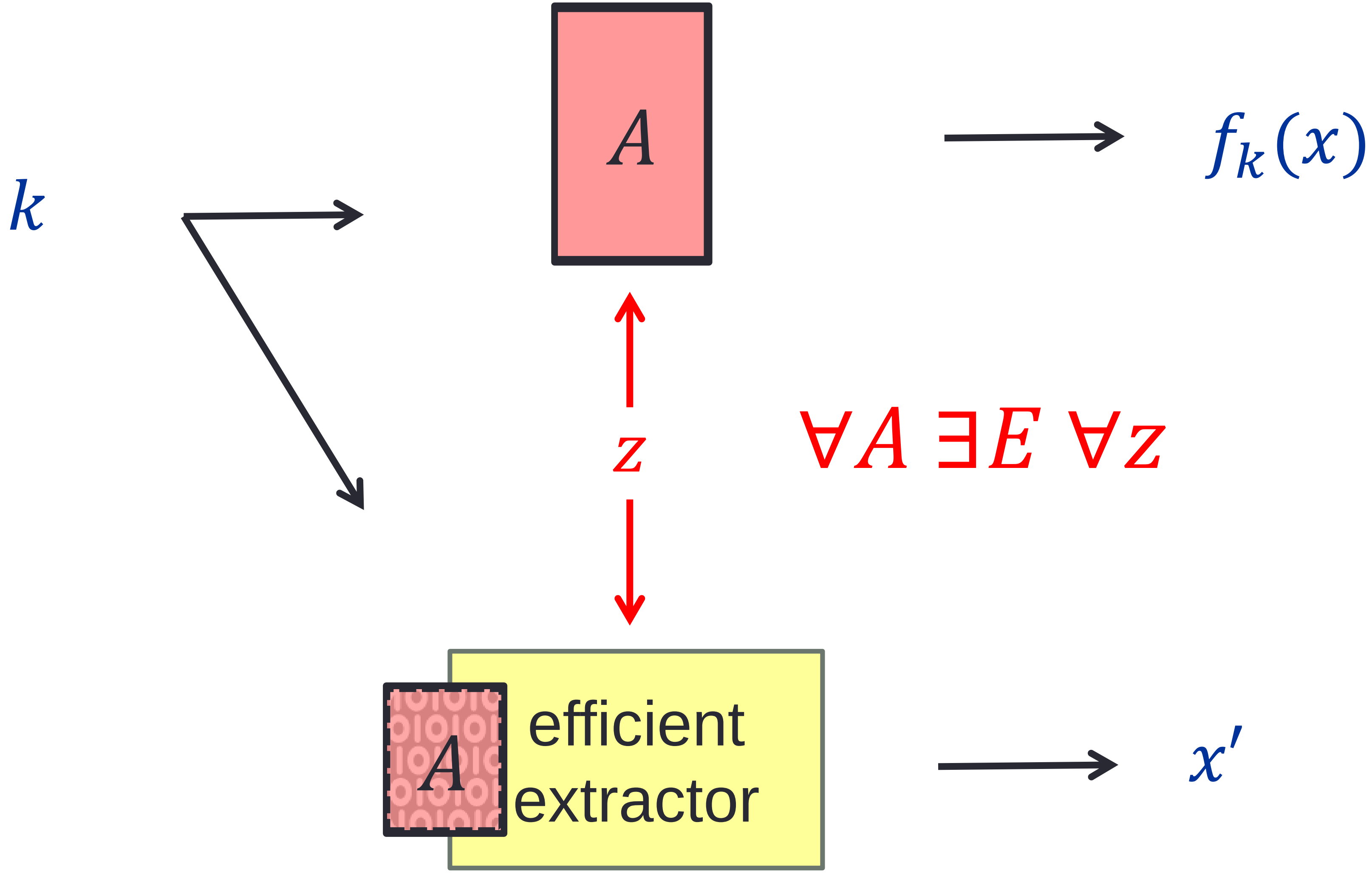
EOWF $f_k(u) + WI_2$

P

V

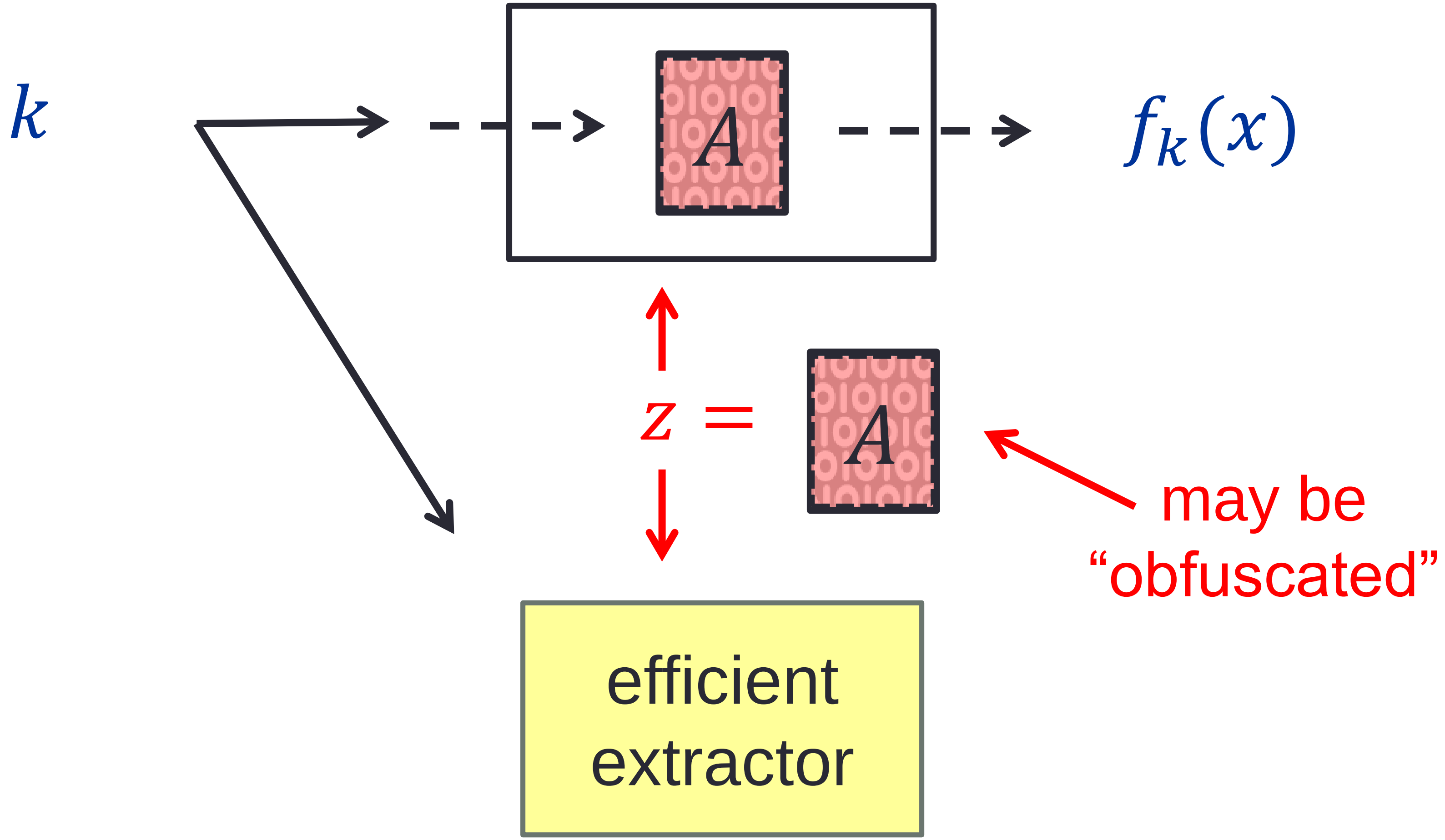
witness-indistinguishable
proof of knowing
$w \vee u$

Common Auxiliary Information

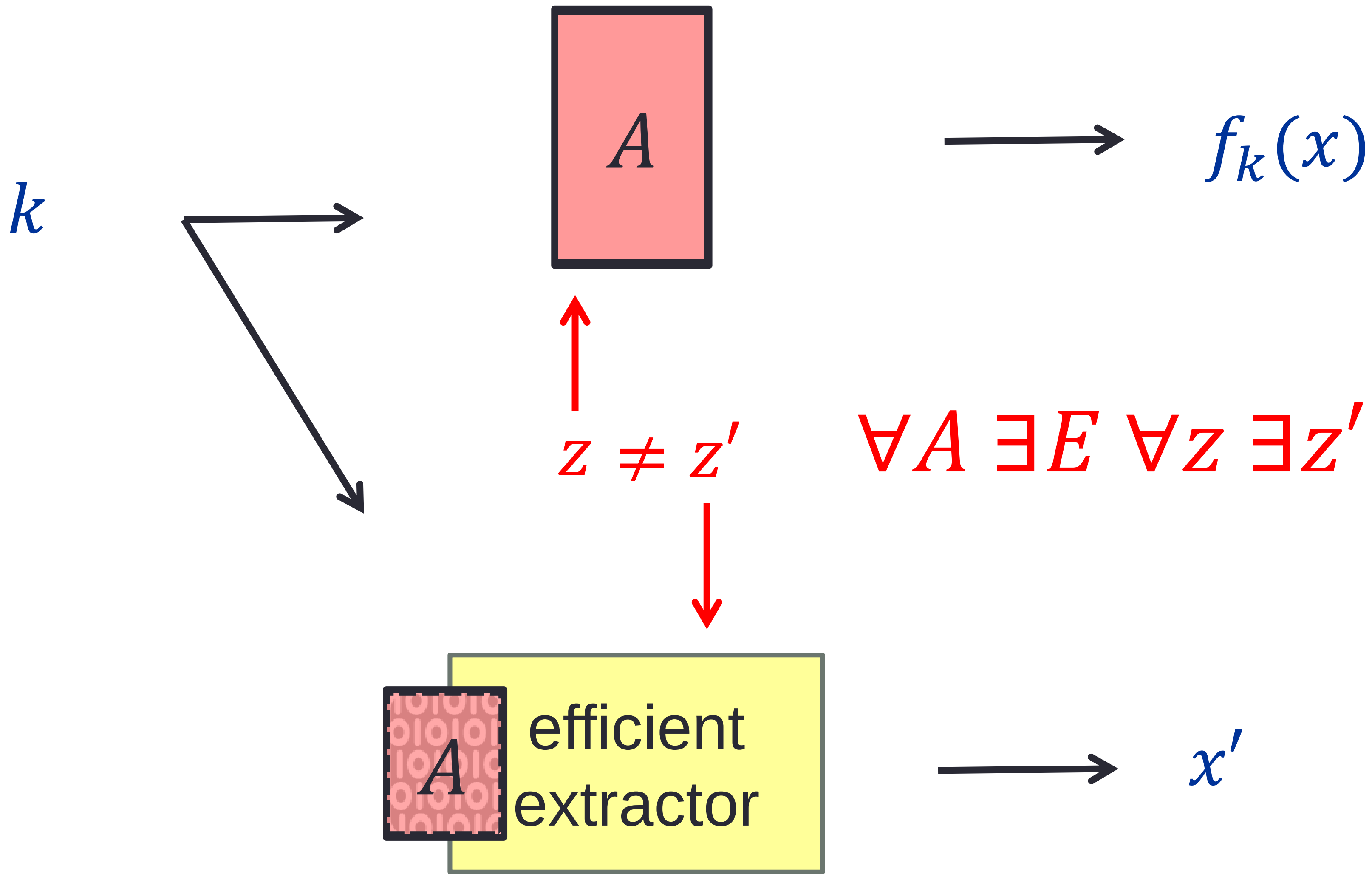


Common A.I. EOWFs vs obfuscation

Hada-Tanaka, Goldreich



Individual Auxiliary Information



k

A

$f_k(x)$

$z \neq z'$

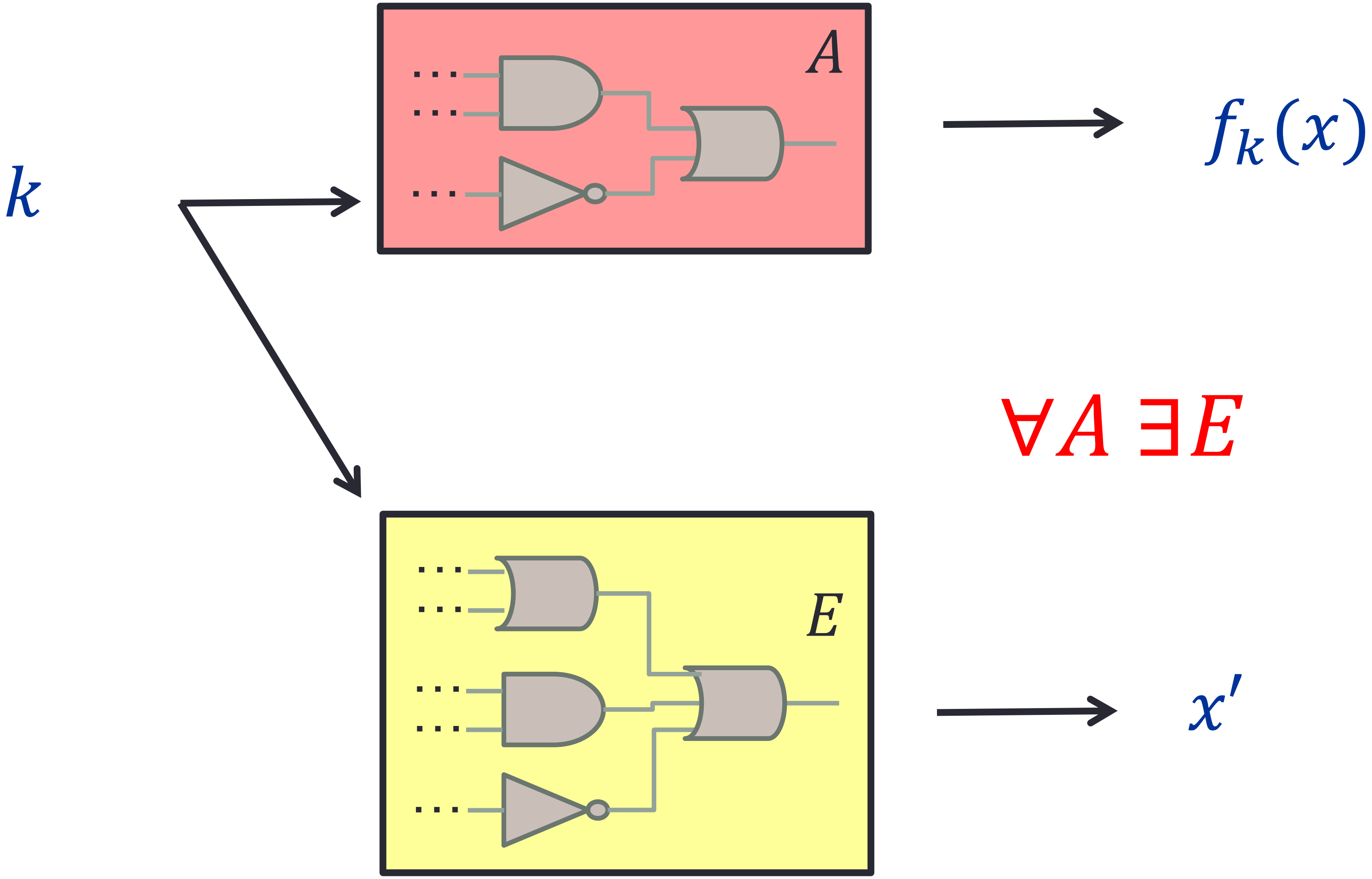
$\forall A \; \exists E \; \forall z \; \exists z'$

A

efficient extractor

x'

Individual Auxiliary Information



k

A

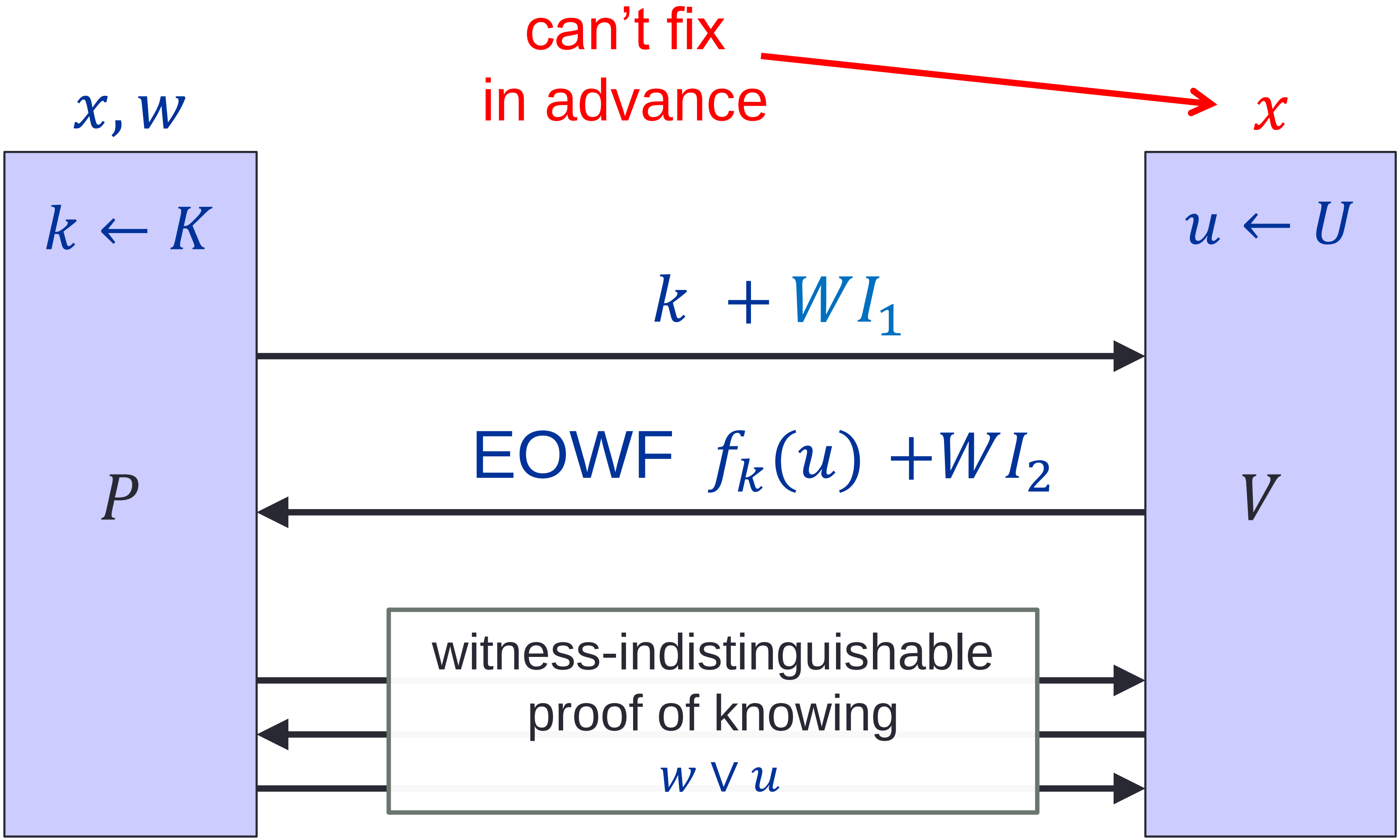
$f_k(x)$

$\forall A \; \exists E$

E

x'

Is Individual A.I. Enough?



can’t fix
in advance

x, w

x

$k \leftarrow K$

$u \leftarrow U$

$k \ + WI_1$

EOWF $f_k(u)$ $+WI_2$

P

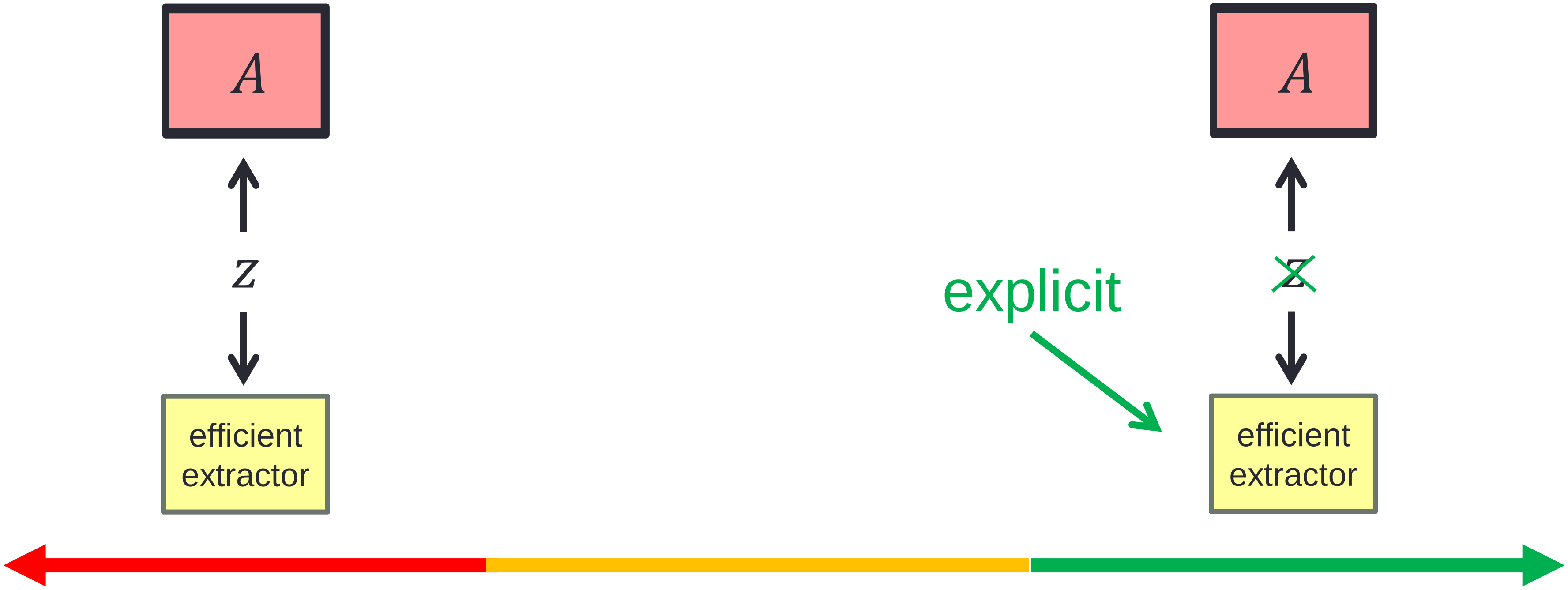
V

witness-indistinguishable
proof of knowing
$w \vee u$

Some Answers

EOWFs
with *common* A.I.

uniform EOWFs
with *no* A.I.



impossible

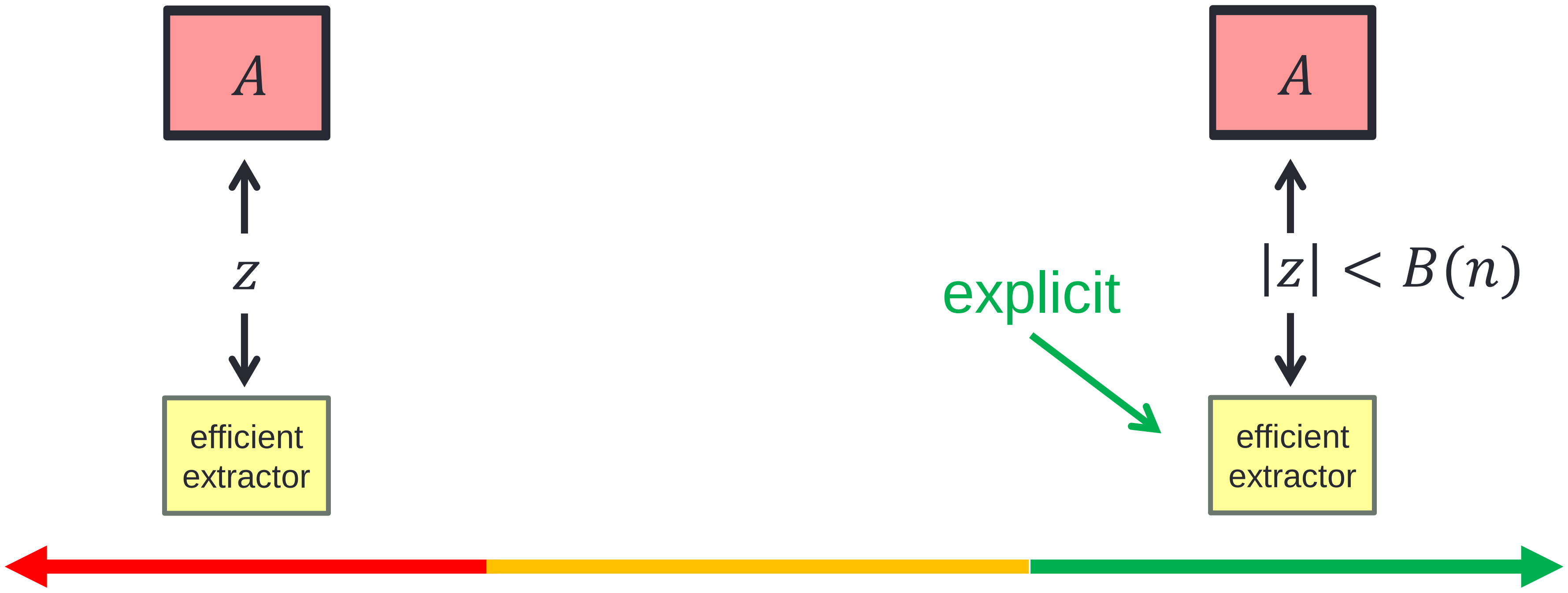
open

possible

indistinguishability
obfuscation

EOWFs
with *common* A.I.

EOWFs
with *bounded* A.I.



A

z

efficient extractor

A

$|z| < B(n)$

explicit

efficient extractor

impossible

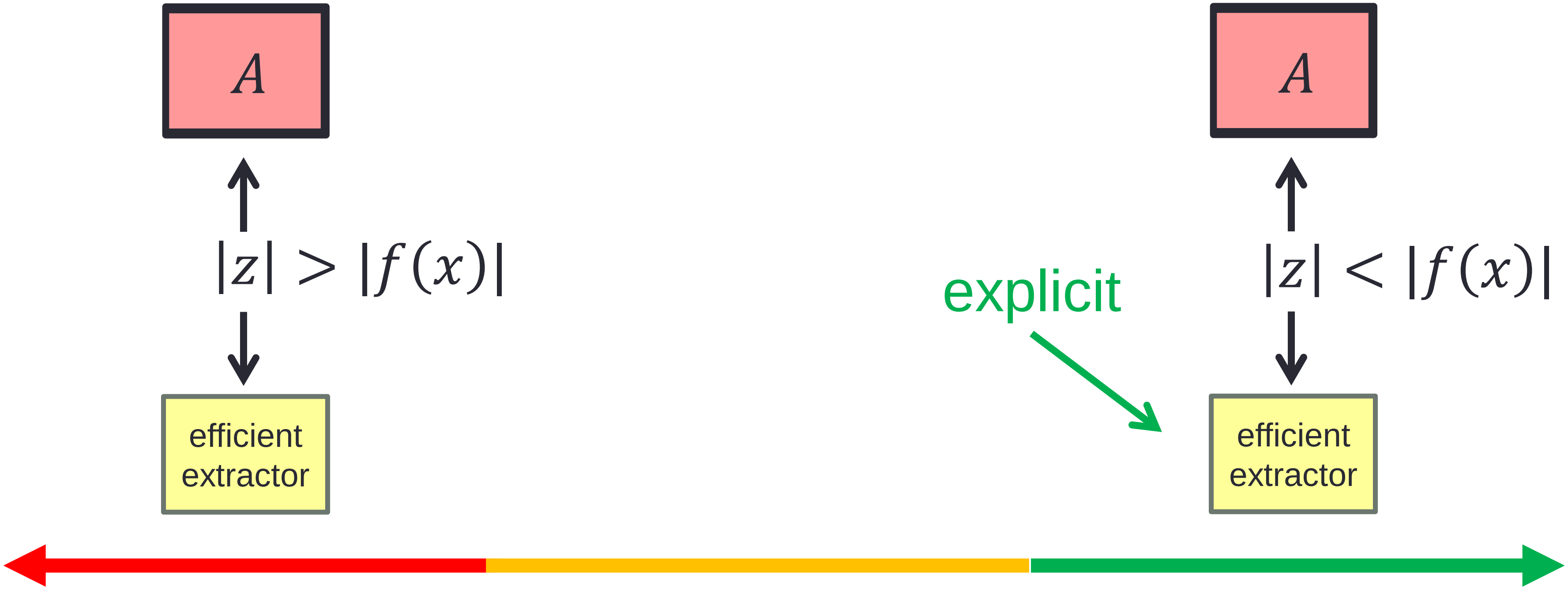
open

possible

indistinguishability
obfuscation

EOWFs with
common unbounded A.I.

EOWFs
with *bounded* A.I.



impossible

open

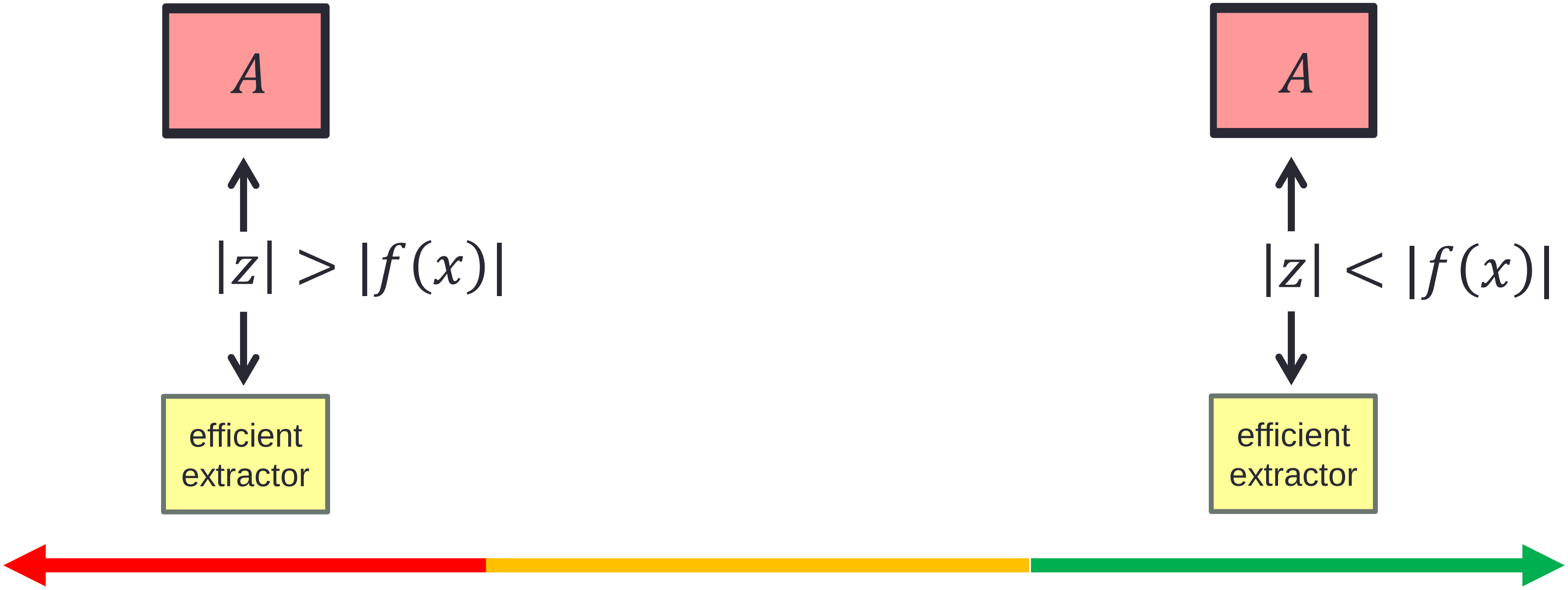
possible

indistinguishability
obfuscation

NIUA for $\mathrm{Dtime}(n^{\omega(1)})$
(SNARGs for P,
P-certificates Chung-Lin-Pass)

EOWFs with
common unbounded A.I.

privately-verifiable
Generalized EOWFs
with *bounded* A.I.



impossible

open

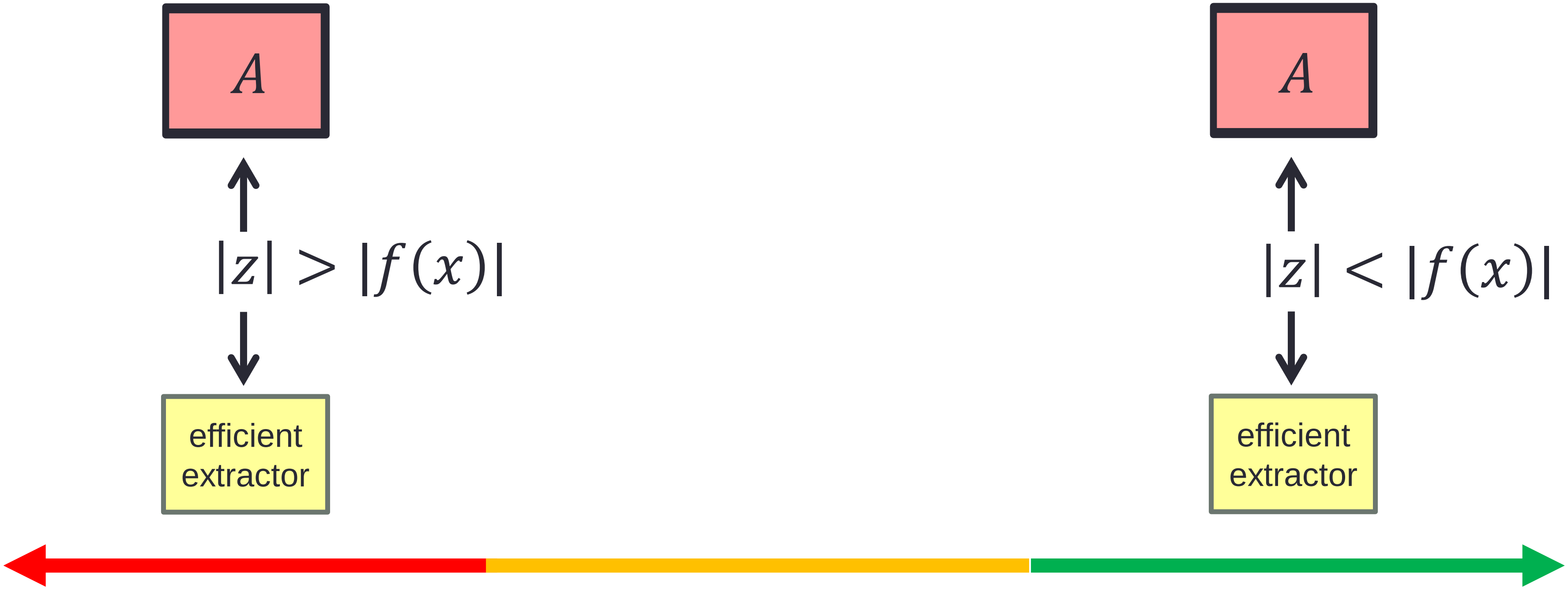
possible

indistinguishability
obfuscation

priv’-ver’ SNARGs for P
Kalai-Raz-Rothblum:
subexp-PIR (e.g., LWE)

privately-verifiable
Generalized EOWFs
common (unbounded) A.I.

privately-verifiable
Generalized EOWFs
with *bounded* A.I.


A

$|z| > |f(x)|$

efficient extractor

A

$|z| < |f(x)|$

efficient extractor

impossible

open

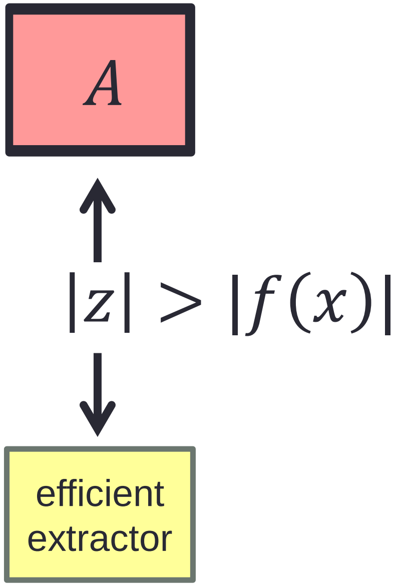
possible

indistinguishability
obfuscation

priv’-ver’ SNARGs for P
Kalai-Raz-Rothblum:
subexp-PIR (e.g., LWE)

privately-verifiable
Generalized EOWFs
common (unbounded) A.I.

privately-verifiable
Generalized EOWFs
with *bounded* A.I.



3-ZK ArgOK
2-ZK Arg
bounded A.I. *verifiers*

impossible

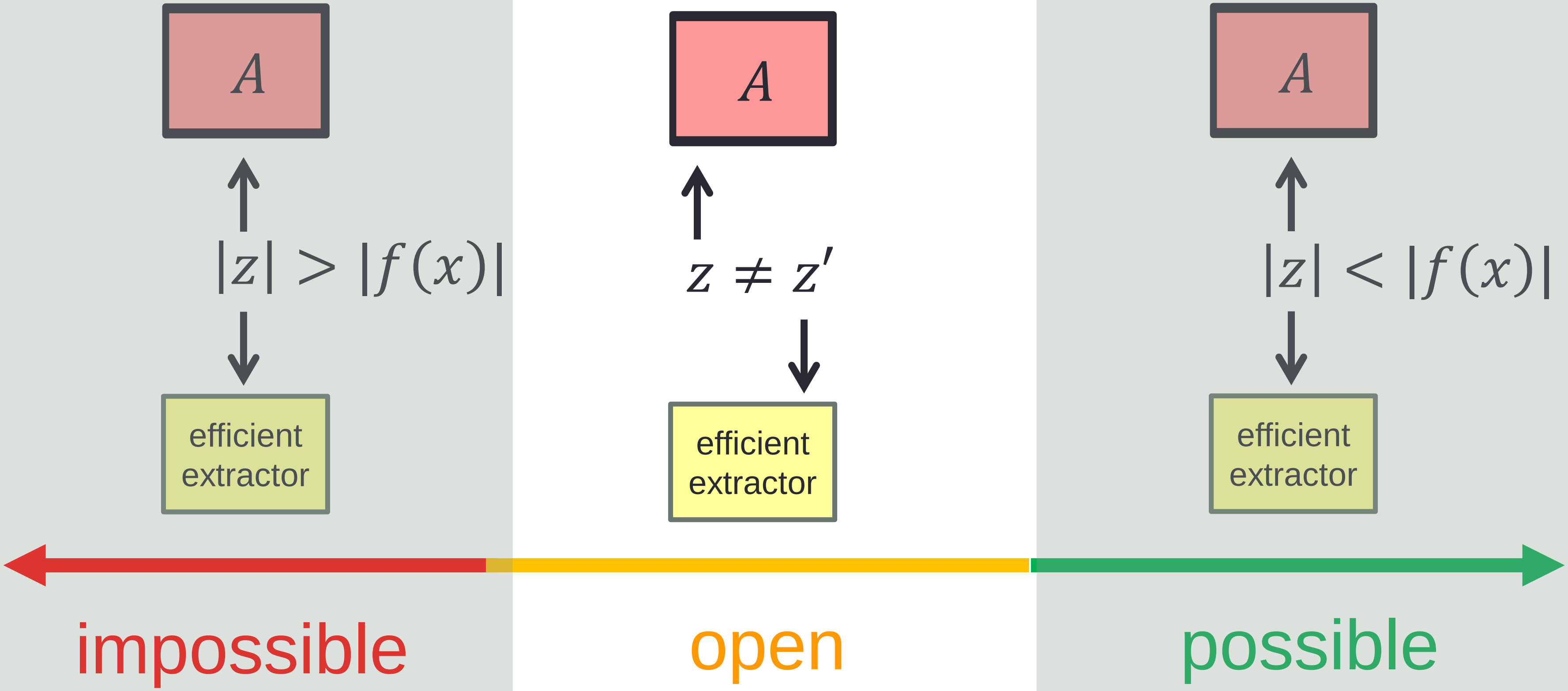
open

possible

indistinguishability
obfuscation

priv'-ver' SNARGs for P
Kalai-Raz-Rothblum:
subexp-PIR (e.g., LWE)

EOWFs
with *(unbounded)*
individual A.I.



A

$|z| > |f(x)|$

efficient extractor

A

$z \neq z'$

efficient extractor

A

$|z| < |f(x)|$

efficient extractor

impossible

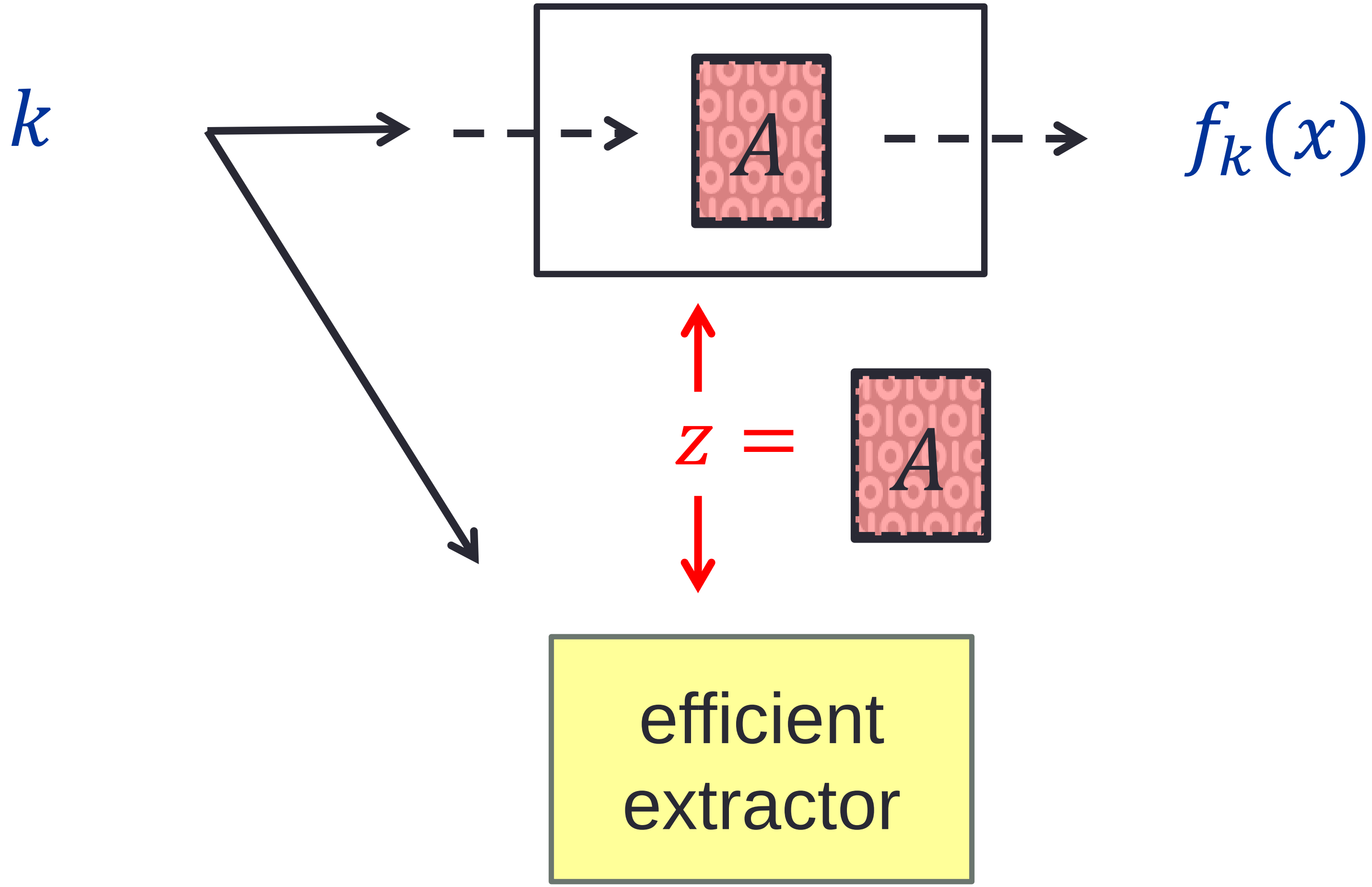
open

possible

Ideas

Common A.I. Extraction
vs.
Indistinguishability Obfuscation

The Universal Adversary



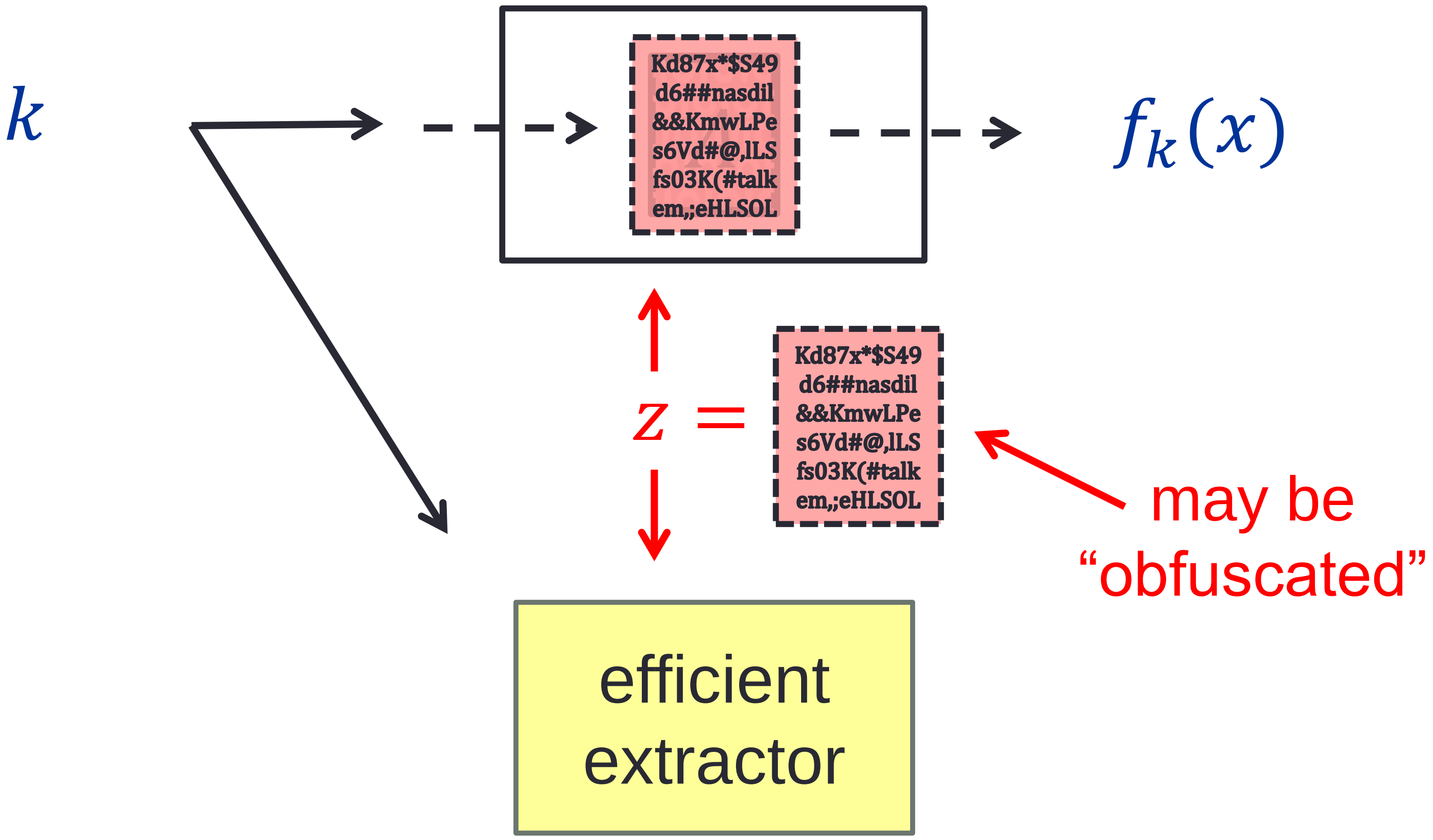
k

$f_k(x)$

$z =$

efficient extractor

The Universal Adversary



k

Kd87x*$S49
d6##nasdil
&&KmwLPe
s6Vd#@,lLS
fs03K(#talk
em,;eHLSOL

$f_k(x)$

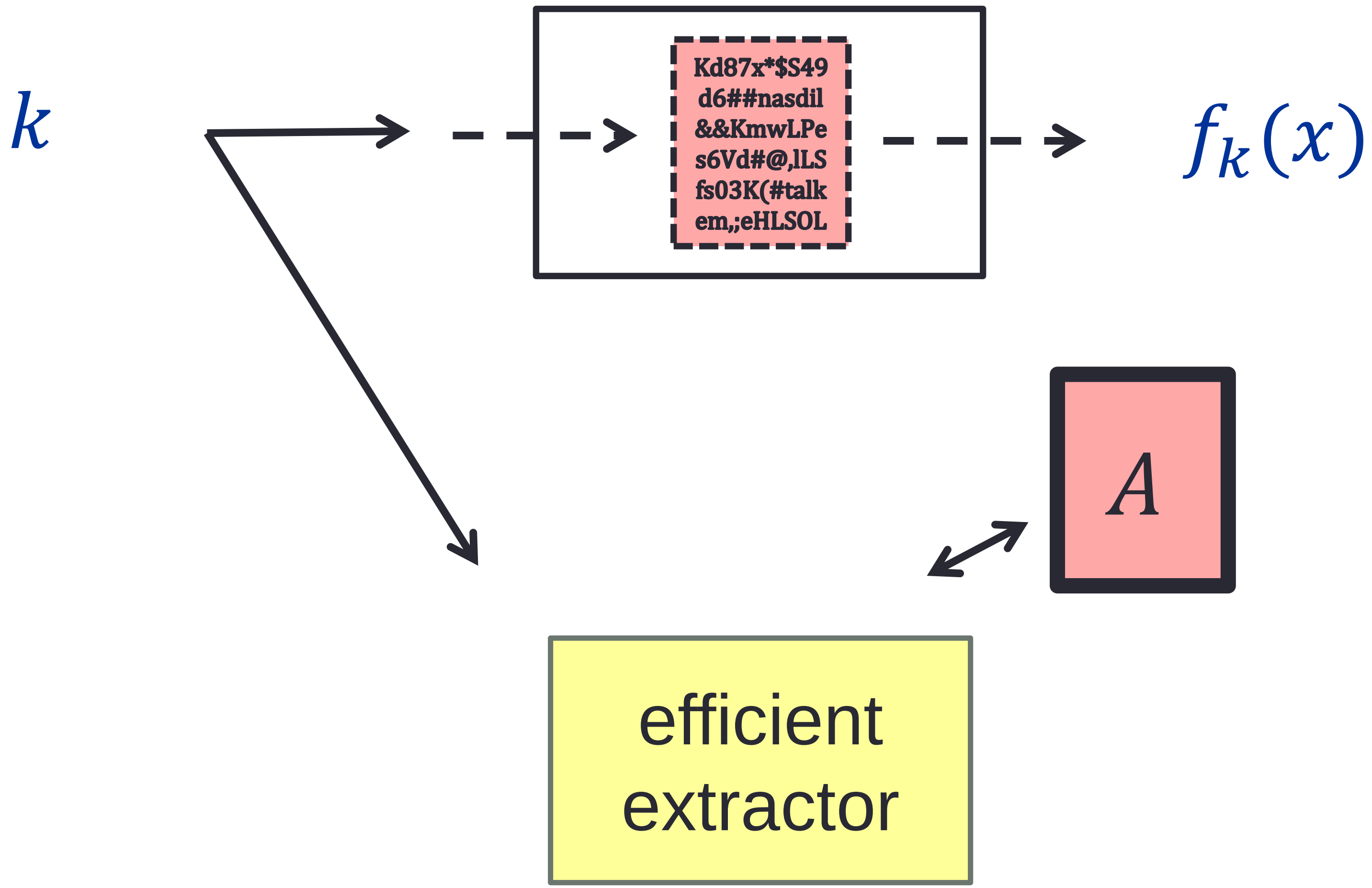
$z =$

Kd87x*$S49
d6##nasdil
&&KmwLPe
s6Vd#@,lLS
fs03K(#talk
em,;eHLSOL

may be
“obfuscated”

efficient
extractor

The Universal Adversary



k

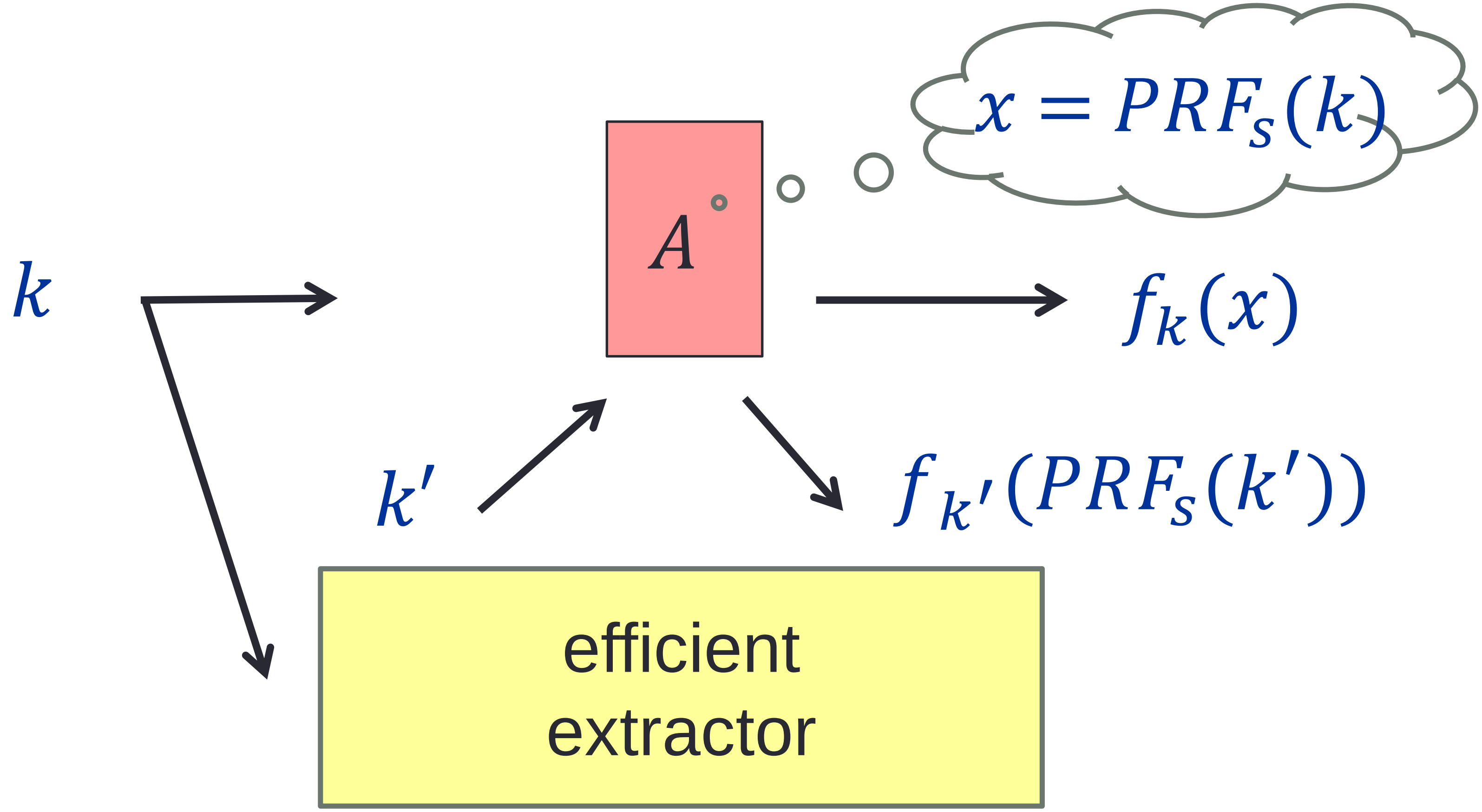
Kd87x*$S49
d6##nasdil
&&KmwLPe
s6Vd#@,lLS
fs03K(#talk
em,;eHLSOL

$f_k(x)$

A

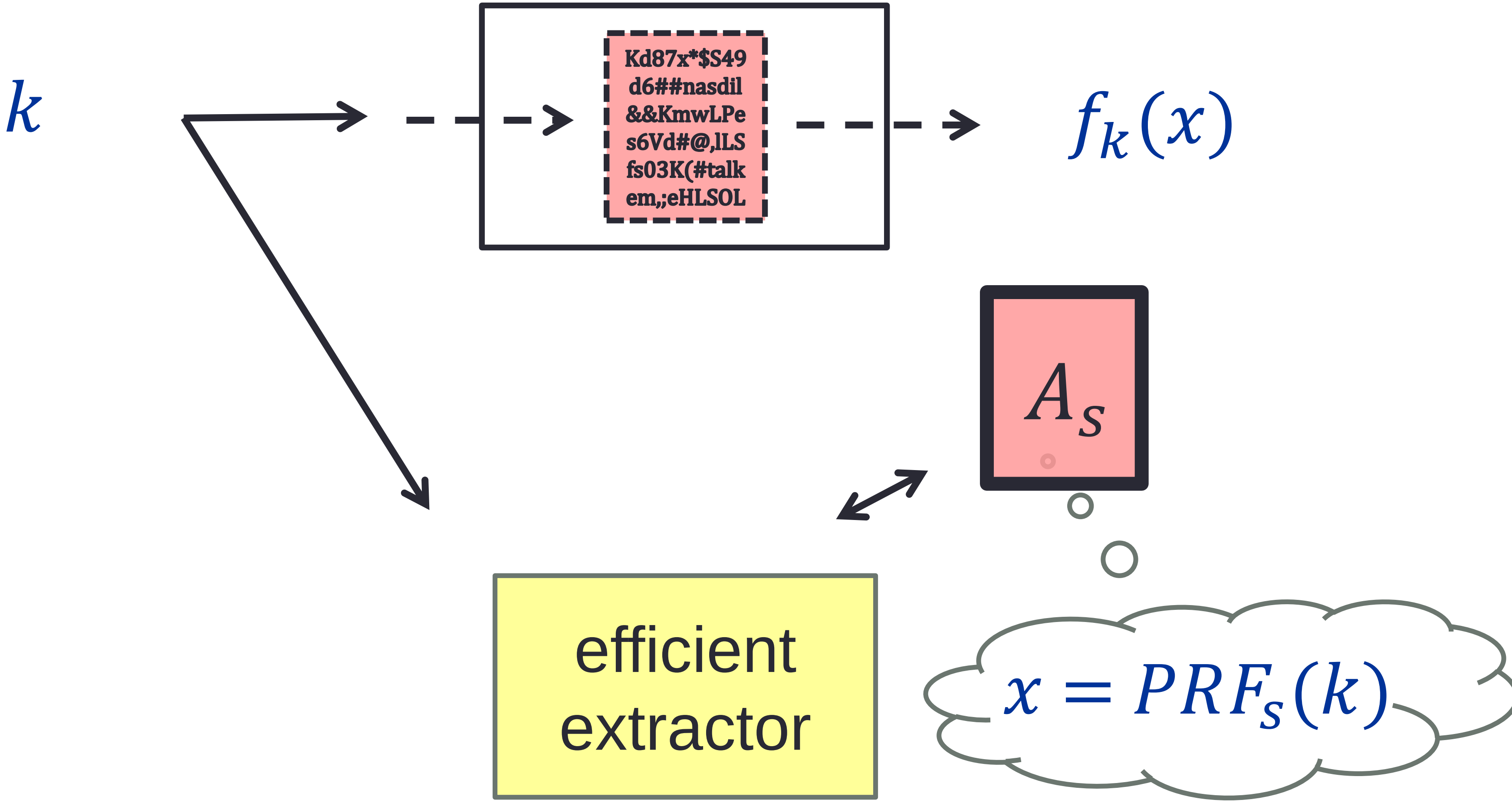
efficient extractor

Black-Box Extraction is Impossible



black-box extractor must invert the one-way f_k

The Universal Adversary



k

Kd87x*$S49
d6##nasdil
&&KmwLPe
s6Vd#@,lLS
fs03K(#talk
em,;eHLSOL

$f_k(x)$

A_s

efficient extractor

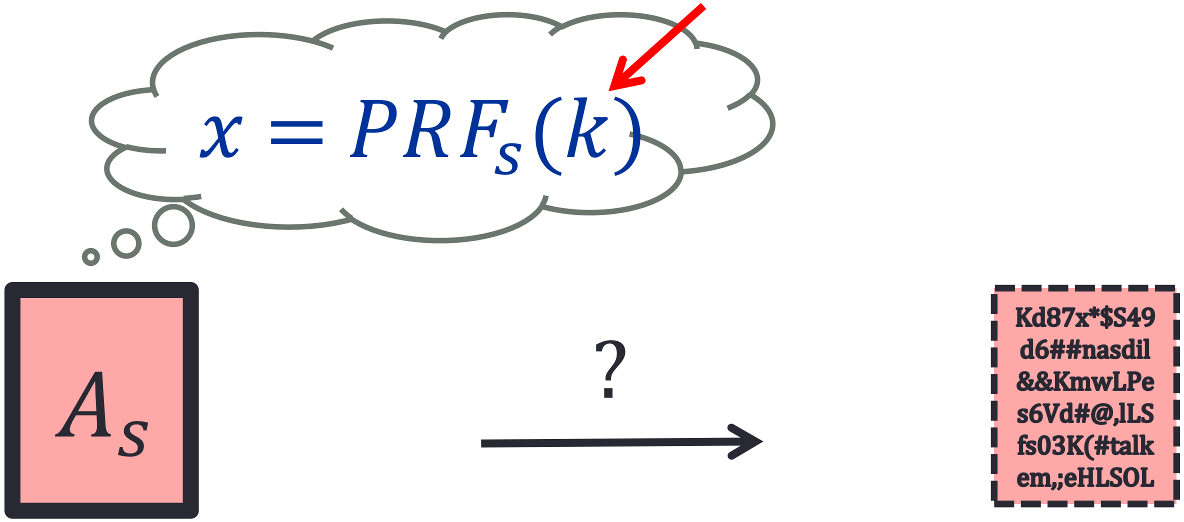
$x = PRF_s(k)$

What Kind of Obfuscation?

Evidence that VBB obfuscation of A_s is impossible
(it is pseudo-entropic)

Goldwasser-Kalai, B-Canetti-Paneth-Rosen

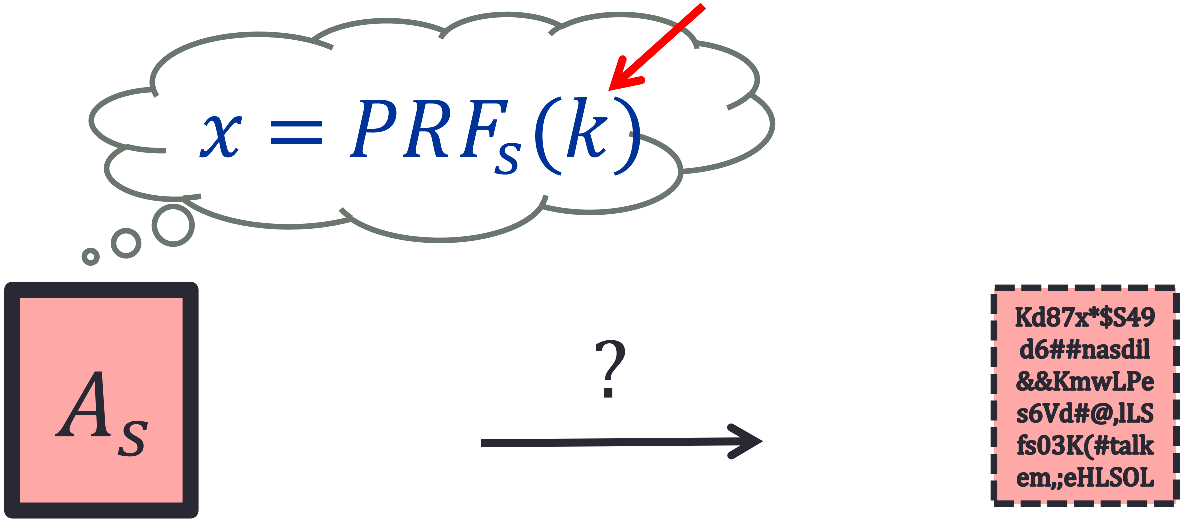
Need to hide PRF value only on the particular point k
(out of Ext's control)



What Kind of Obfuscation?

Evidence that VBB obfuscation of A_s is impossible
(it is pseudo-entropic)
Goldwasser-Kalai, B-Canetti-Paneth-Rosen

Need to hide PRF value only on the particular point k
(out of Ext's control) – use Sahai-Waters puncturing

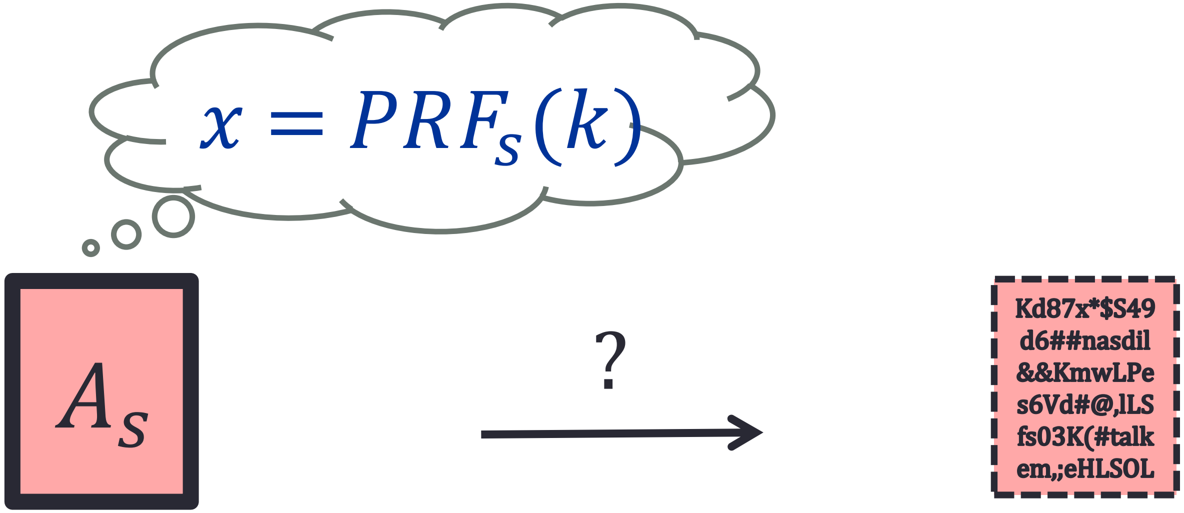


What Kind of Obfuscation?

Evidence that VBB obfuscation of A_s is impossible
(it is pseudo-entropic)
Goldwasser-Kalai, B-Canetti-Paneth-Rosen

Need to hide PRF value only on the particular point k
(out of Ext’s control) – use Sahai-Waters puncturing

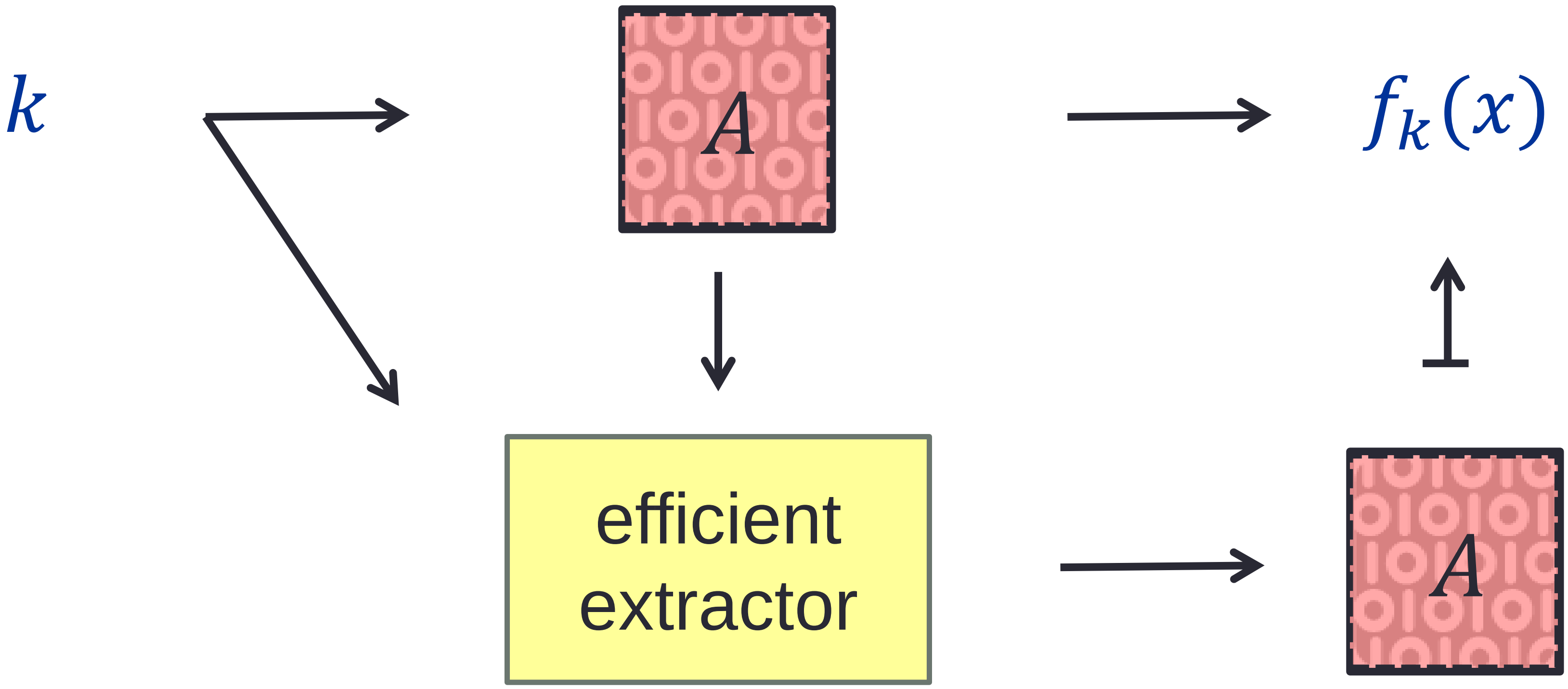
A.I. depends on k – but, with IndObf looks as if it doesn’t



$x = PRF_s(k)$

Extractable One-Way Functions w.r.t Bounded A.I.

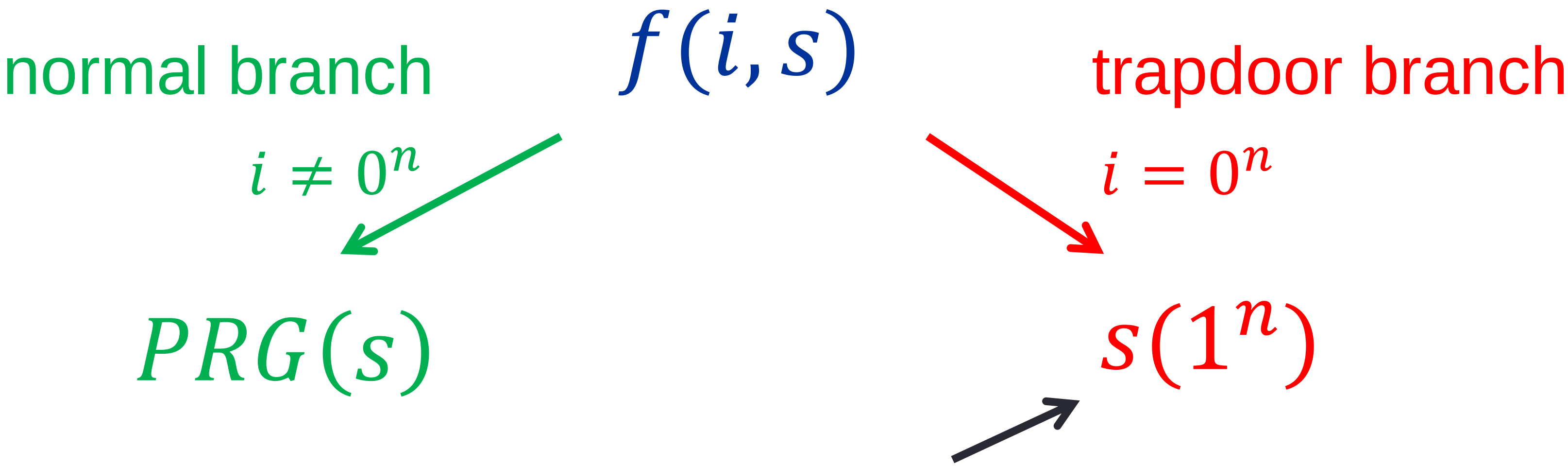
If You Can’t Extract What’s inside the Head, Extract the Head [Barak]



First Attempt

Goal: *keyless* $f: \{0,1\}^{2n} \rightarrow \{0,1\}^{2n}$

Ingredient: $PRG: \{0,1\}^{n} \rightarrow \{0,1\}^{2n}$



$f(i,s)$

normal branch

$i \neq 0^n$

$PRG(s)$

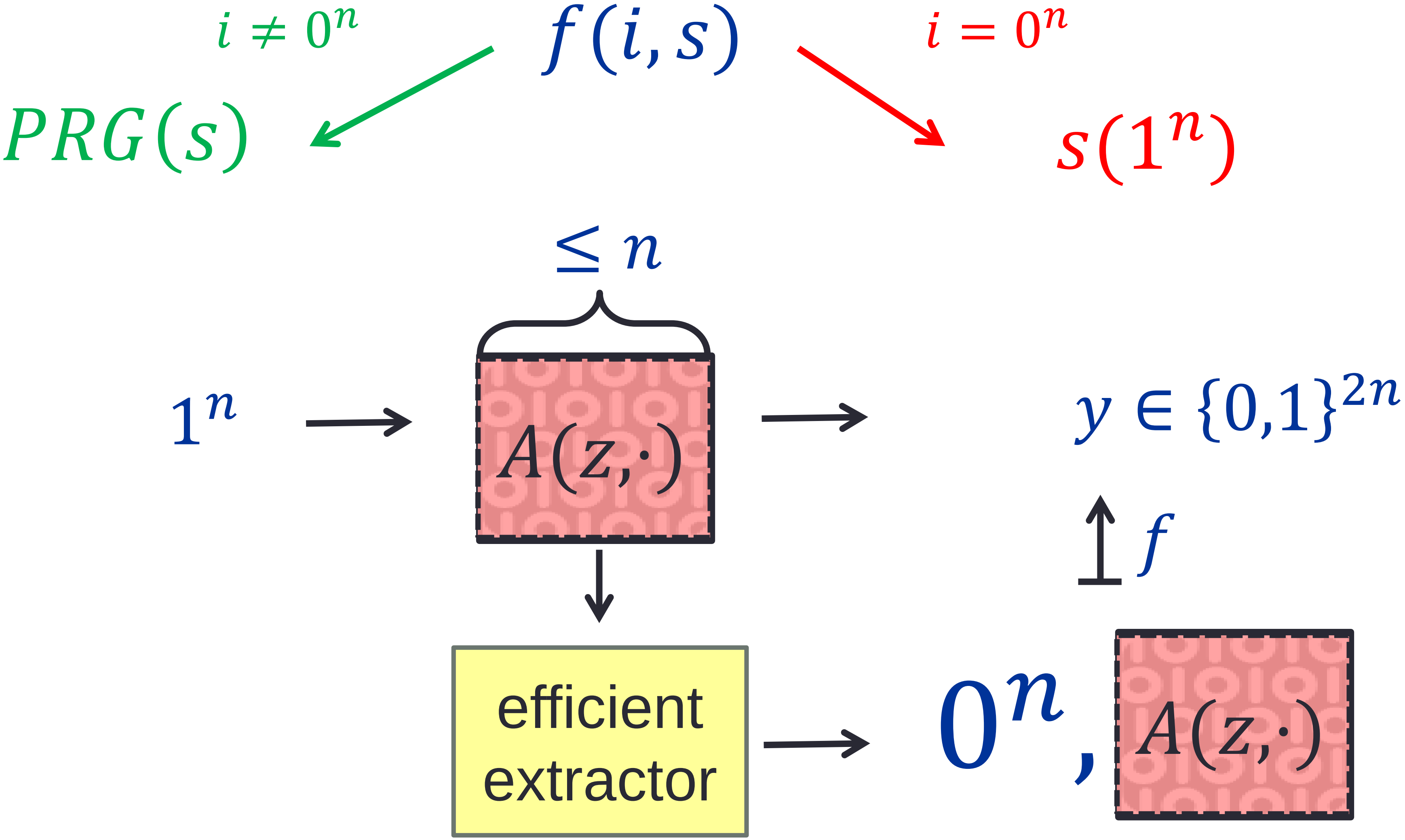
trapdoor branch

$i = 0^n$

$s(1^n)$

parsed as a machine
with $2n$ output bits

Extractability



$f(i,s)$

$i \neq 0^n$

$PRG(s)$

$i = 0^n$

$s(1^n)$

$\leq n$

1^n

$A(z,\cdot)$

$y \in \{0,1\}^{2n}$

f

efficient extractor

$0^n, A(z,\cdot)$

One-Wayness

$$\begin{tikzcd}
 & f(i,s) \arrow[dl, "i \neq 0^n"'] \arrow[dr, "i = 0^n"] & \\
PRG(s) & & s(1^n)
\end{tikzcd}$$

For $i, s \leftarrow \{0,1\}^{2n}$:

$$f(i,s) \approx_c U \leftarrow \{0,1\}^{2n}$$

Inverter finds $s \in \{0,1\}^n$ s.t $U \in \{PRG(s), s(1^n)\}$
But U a.s. has Kolmogorov complexity $\gg n = |s|$

Problem

$$\begin{tikzcd} & f(i,s) \arrow[dl, "i \neq 0^n"'] \arrow[dr, "i = 0^n"] & \\ PRG(s) & & s(1^n) \end{tikzcd}$$

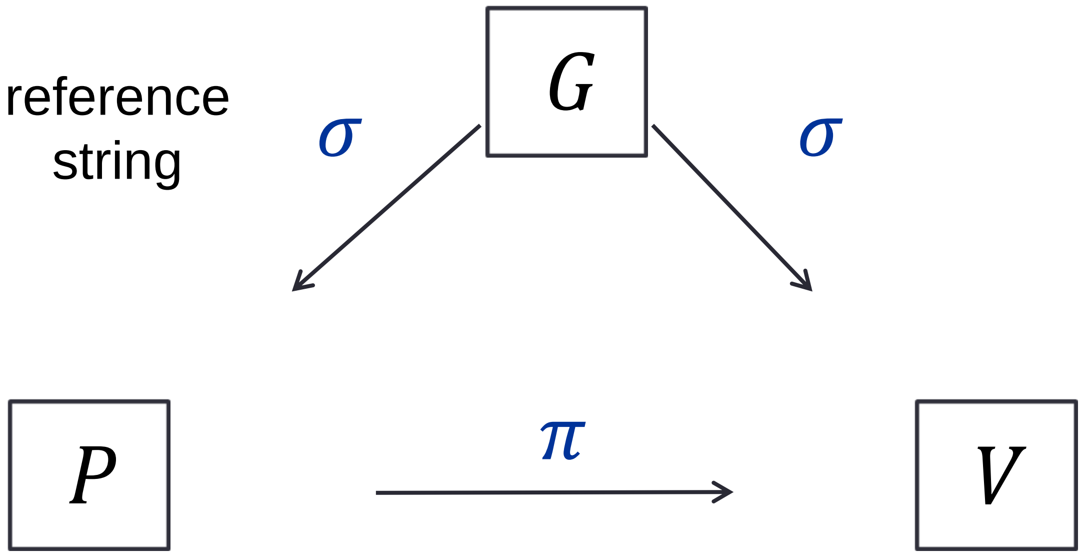
$$\mathrm{Time}(f(0^n, s)) \geq \mathrm{Time}(s(1^n))$$

not bounded by any polynomial

Barak ZK: solved by interactive universal arguments for non-deterministic computations

Barak-Lindell-Vadhan ZK: solved assuming **non**-interactive universal arguments for non-deterministic computations (Micali’s CS proofs)

NIUAs for Deterministic Computations



(M, y) = “$M(1^n)$ outputs y after $T_M < n^{\log n}$ steps”

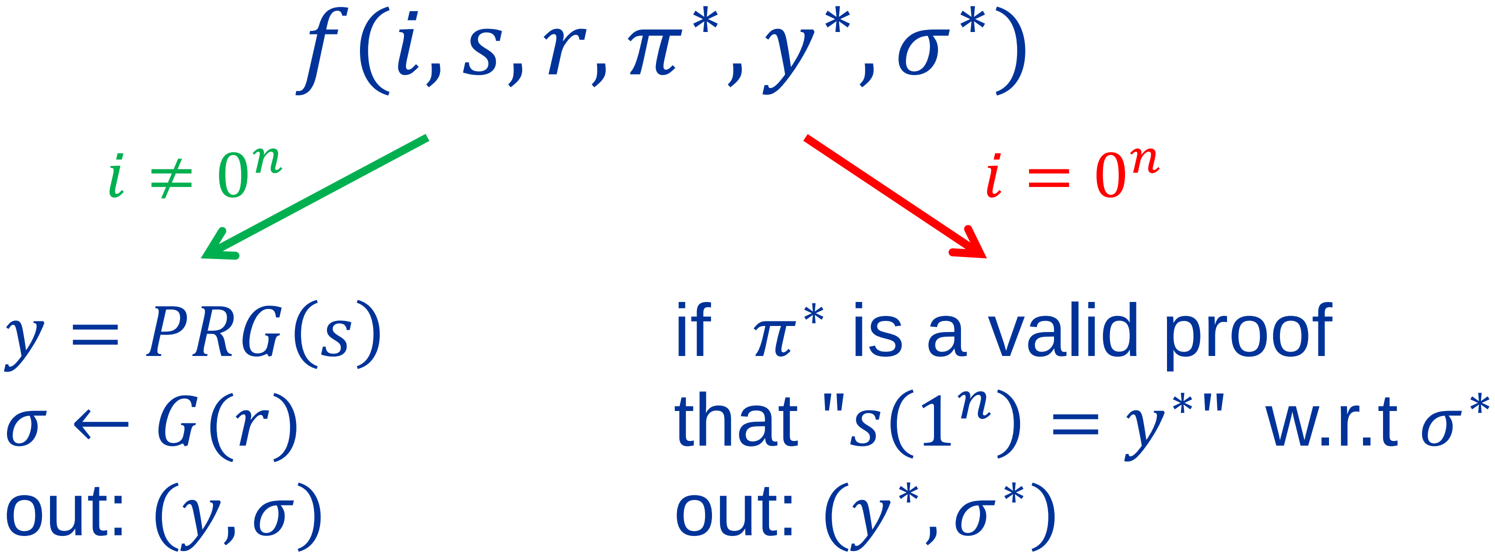
$\text{poly}(T_M, |M.y|)$ $\text{poly}(\log T_M, |M.y|)$

EOWFs from NIUAs

Instead of running $s(1^n)$,
the trapdoor branch verifies a proof that $s(1^n) = y$

One-wayness: maintained by the soundness of the NIUA.

Extraction: given the code of A, compute a proof for $A(1^n) = y$.



$$f(i, s, r, \pi^*, y^*, \sigma^*)$$

$i \neq 0^n$

$y = PRG(s)$
$\sigma \leftarrow G(r)$
out: (y, σ)

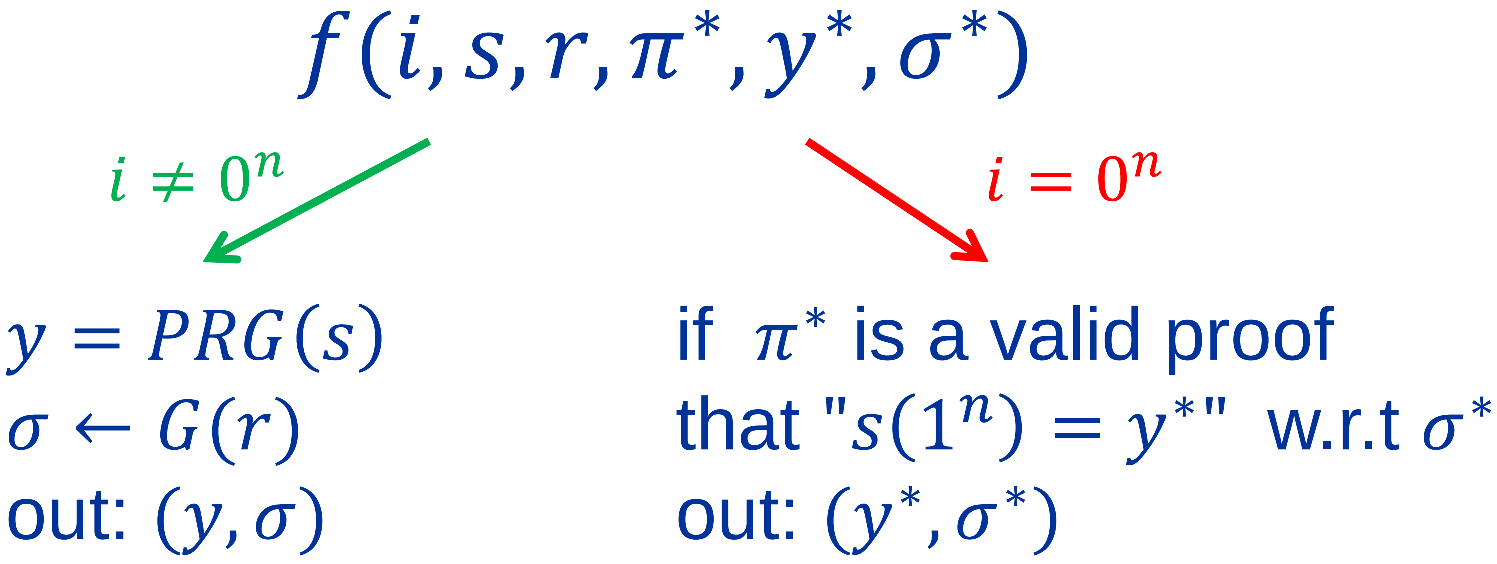
$i = 0^n$

if π^* is a valid proof
that "$s(1^n) = y^*$" w.r.t σ^*
out: (y^*, σ^*)

EOWFs from NIUAs

Instead of running $s(1^n)$,
the trapdoor branch verifies a proof that $s(1^n) = y$

relies on public-verifiability
(soundness holds in presence of verification key σ)



$$f(i, s, r, \pi^*, y^*, \sigma^*)$$

$i \neq 0^n$

$y = PRG(s)$
$\sigma \leftarrow G(r)$
out: (y, σ)

$i = 0^n$

if π^* is a valid proof
that "$s(1^n) = y^*$" w.r.t σ^*
out: (y^*, σ^*)

Generalized EOWFs from privately-verifiable NIUAs

$$R(f(x), x')$$

Hardness:
given $f(x)$ where $x \leftarrow U$
hard to find $x' \in R(f(x))$

Extractability
given code A that outputs
$f(x)$, can extract $x' \in R(f(x))$

Public-verification: $R(f(x), x')$ can be eff' computed by anyone

Private-verification: can be computed given the private x.

Can be constructed from subexp LWE [Kalai-Raz-Rothblum]
Sufficient for 2/3-ZK

Open Questions

Construct a (uniform) ECRH

EOWFs w.r.t *individual* auxiliary information

impossible

open

possible