Advisor-Verifier-Prover Games
&
The Hardness of Information Theoretic Cryptography

Benny Applebaum and Oded Nir

Under what assumptions **Cryptography** needs assumptions?

Minimal Complexity Assumptions for Cryptography: Simons 2023

Impagliazzo's OZ

Fundamental Thm of Crypto [IL89…]: Interesting Crypto requires OWFs

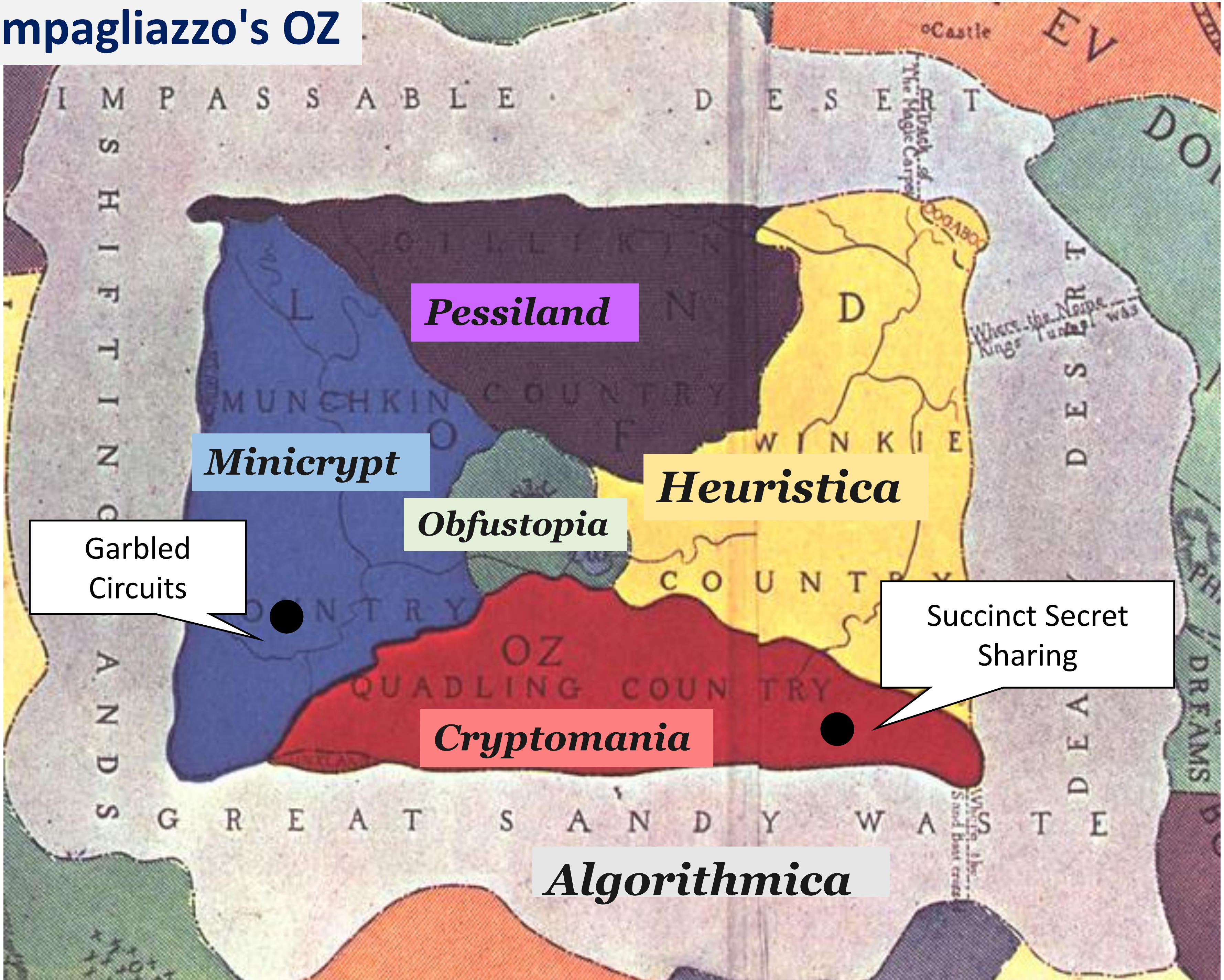
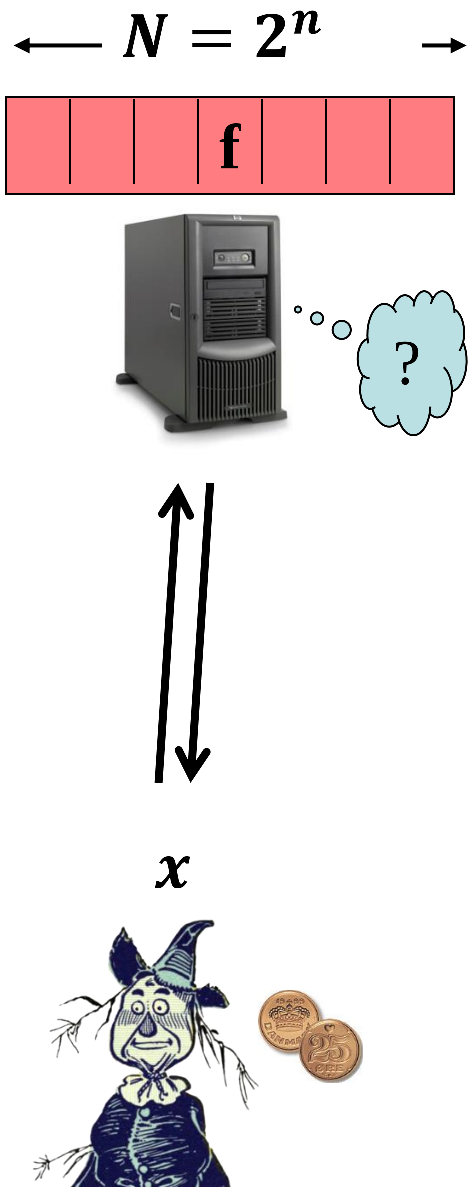


Image credits:
Author:
Neill, John R.
Publisher:
Reilly & Britton Co.
Date: 1914
Location: Oz (Imaginary place)
Some rights reserved by Norman B. Leventhal Map Center at the BPL

Private Information Retrieval [CKGS 98]

$\boldsymbol{f} : \{\mathbf{0}, \mathbf{1}\}^{n} \rightarrow \{\mathbf{0}, \mathbf{1}\}$



$\boldsymbol{N} = \mathbf{2}^{n}$

f

?

$\boldsymbol{x}$

Information-Theoretic PIR [CKGS 98]

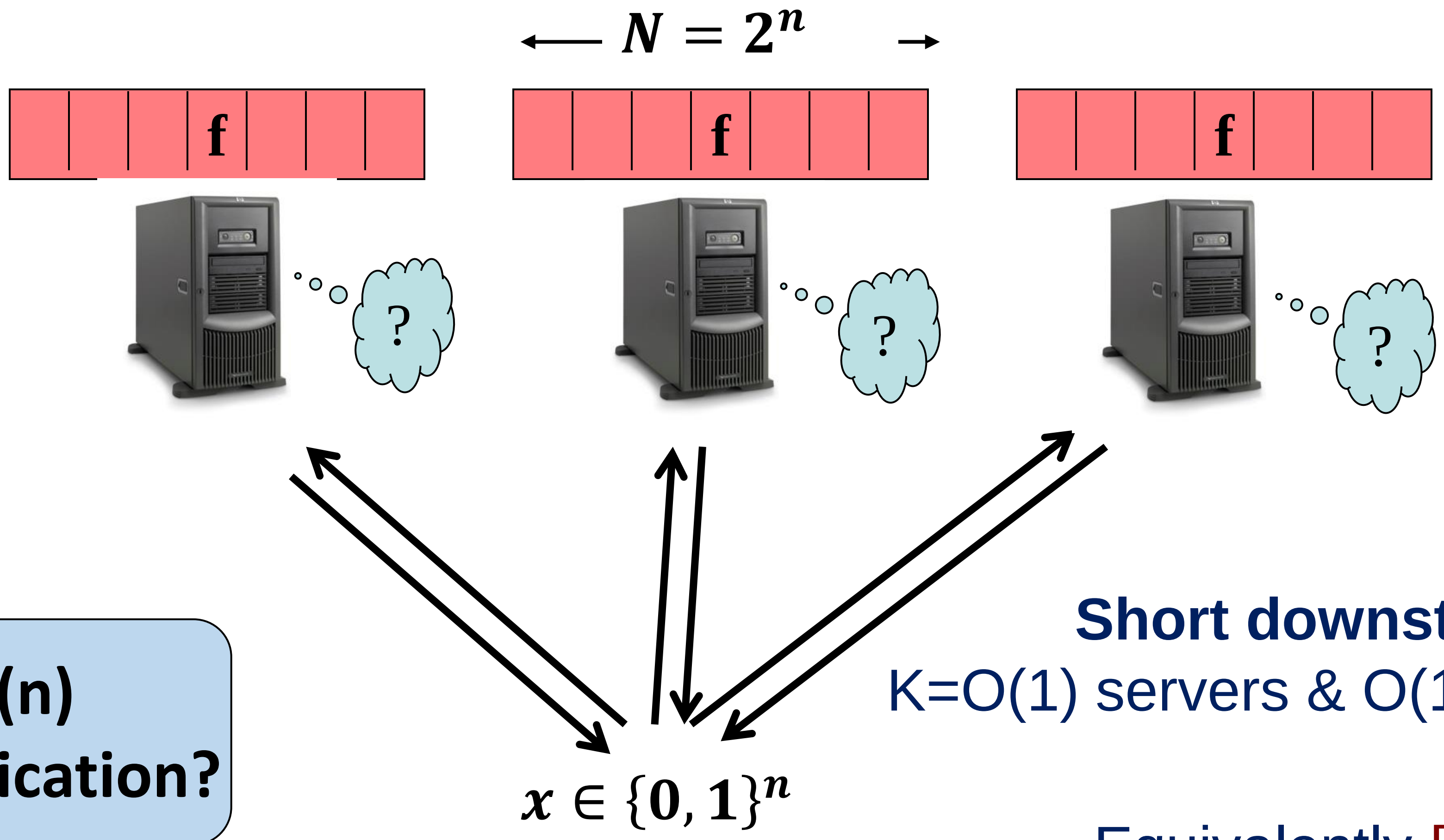
$f: \{0,1\}^n \to \{0,1\}$

[AlrGurKotMan23]
~3n for 3 servers

[Man98,KT00,…,Woo07]

$n + \Omega_k(n) \le$

Poly(n) communication?



$\le \exp(\tilde{O}(\sqrt{n}))$

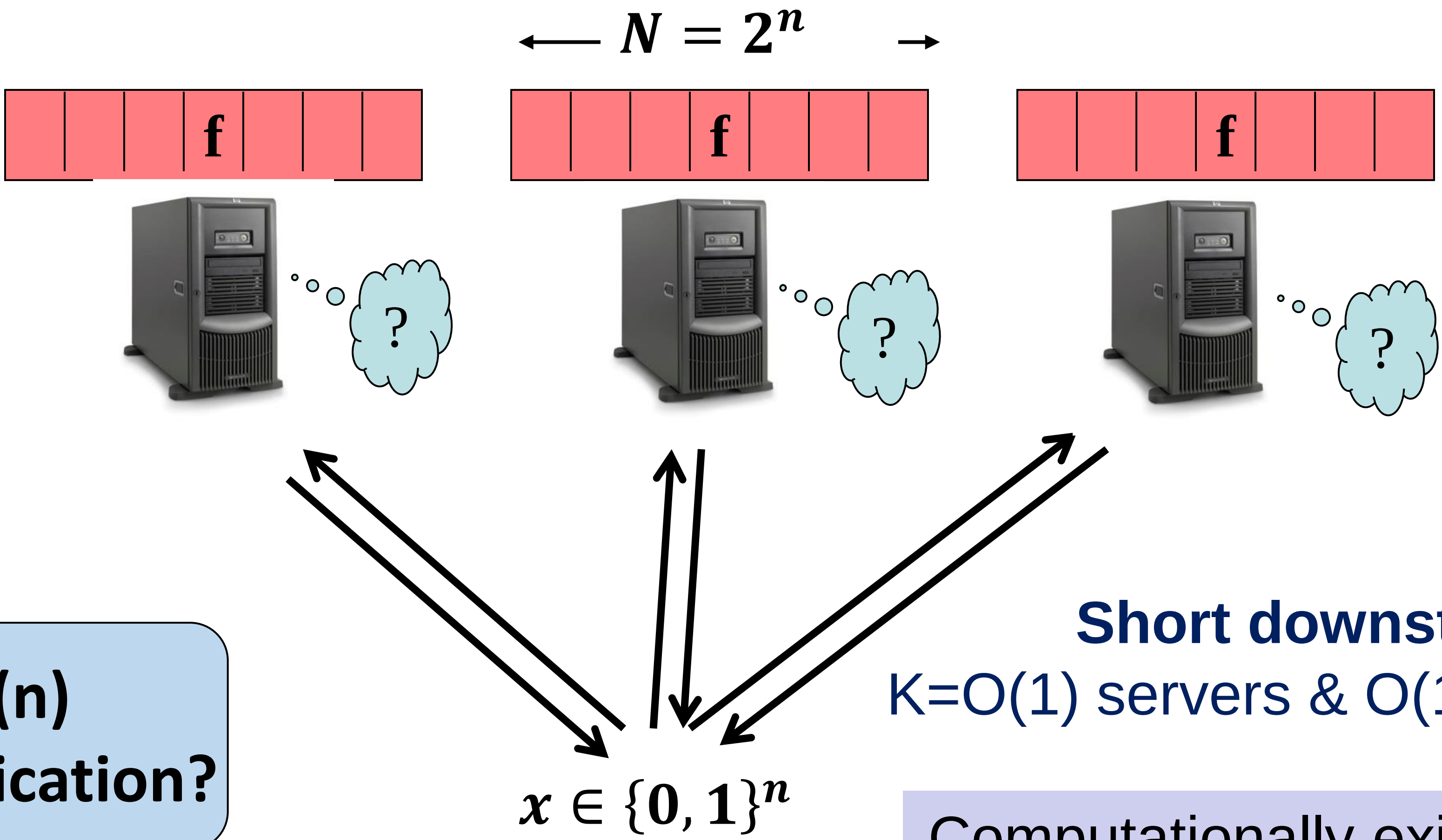
[Yek08, Efr09, DGY11]

Short downstream:
K=O(1) servers & O(1)-bit answers

Equivalently [KT00],
Binary Locally-Decodable Codes
with “short” length?

Information-Theoretic PIR [CKGS 98]

$\boldsymbol{f}\colon \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{n}} \to \{\mathbf{0},\mathbf{1}\}$



$\longleftarrow \boldsymbol{N} = \mathbf{2}^{\boldsymbol{n}} \longrightarrow$
f
f
f
?
?
?
$\boldsymbol{x} \in \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{n}}$

[Man98,KT00,…,Woo07]

$n + \Omega_k(n) \leq$

Poly(n) communication?

$\leq \exp(\tilde{O}(\sqrt{n}))$

[Yek08, Efr09, DGY11]

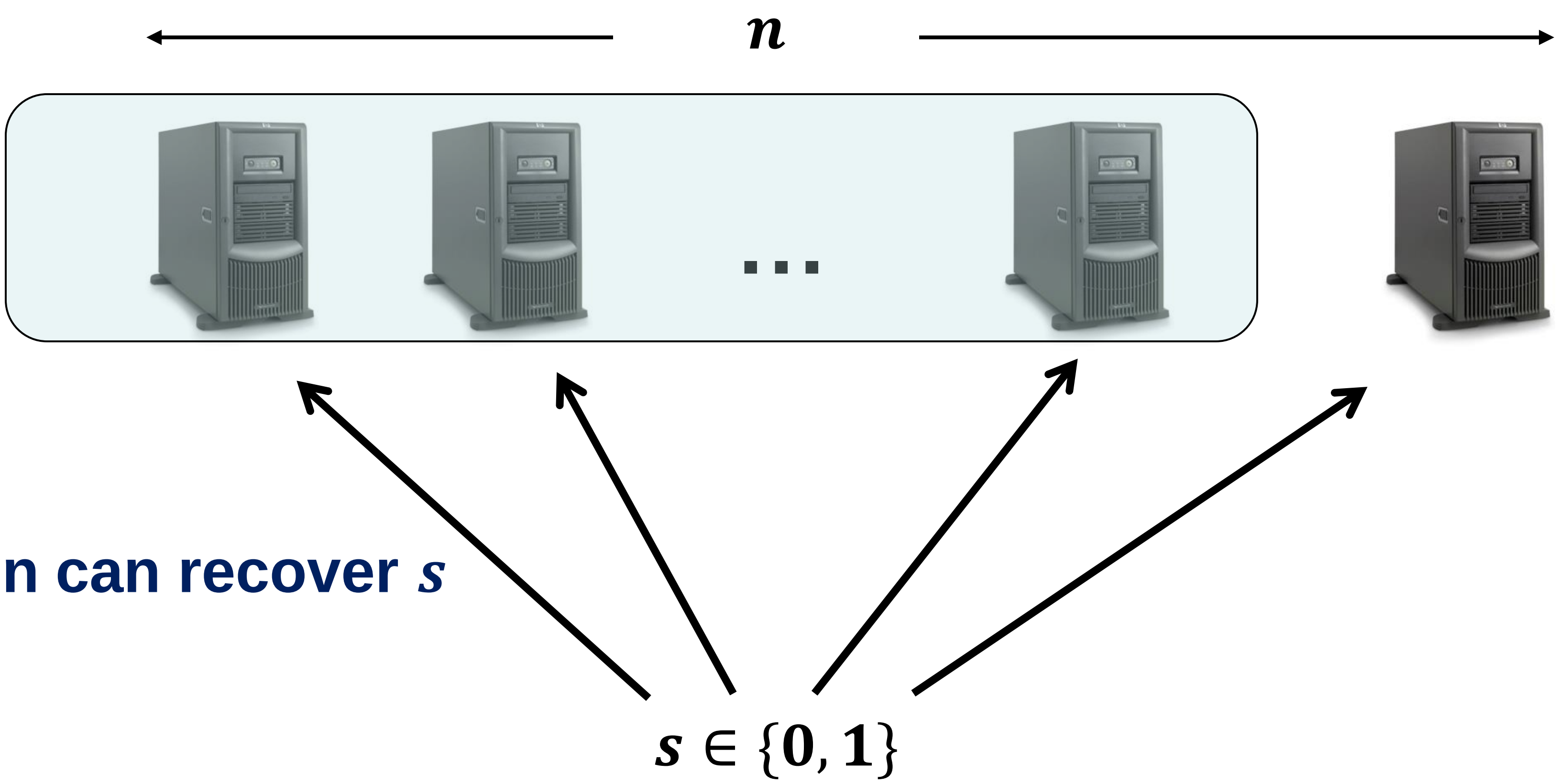
Short downstream:
K=O(1) servers & O(1)-bit answers

Computationally exists assuming sub-exp strong OWFs [GI14]!

Generalized Secret Sharing

[Sha,Bla79,ISN87]

$f:\{0,1\}^n \to \{0,1\}$

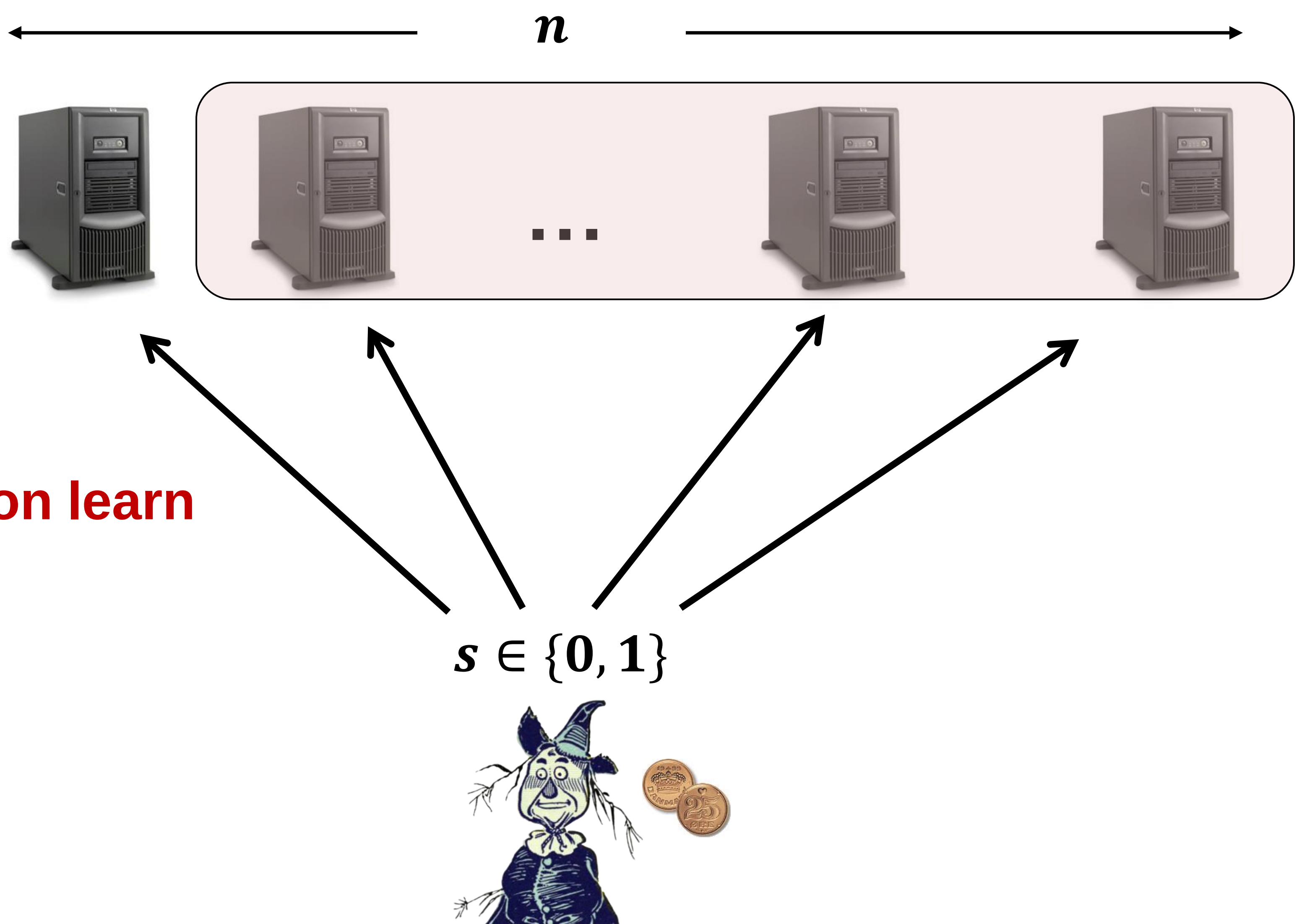


Authorized coalition can recover s

Generalized Secret Sharing

[Sha,Bla79,ISN87]

$\boldsymbol{f} : \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{n}} \rightarrow \{\mathbf{0}, \mathbf{1}\}$



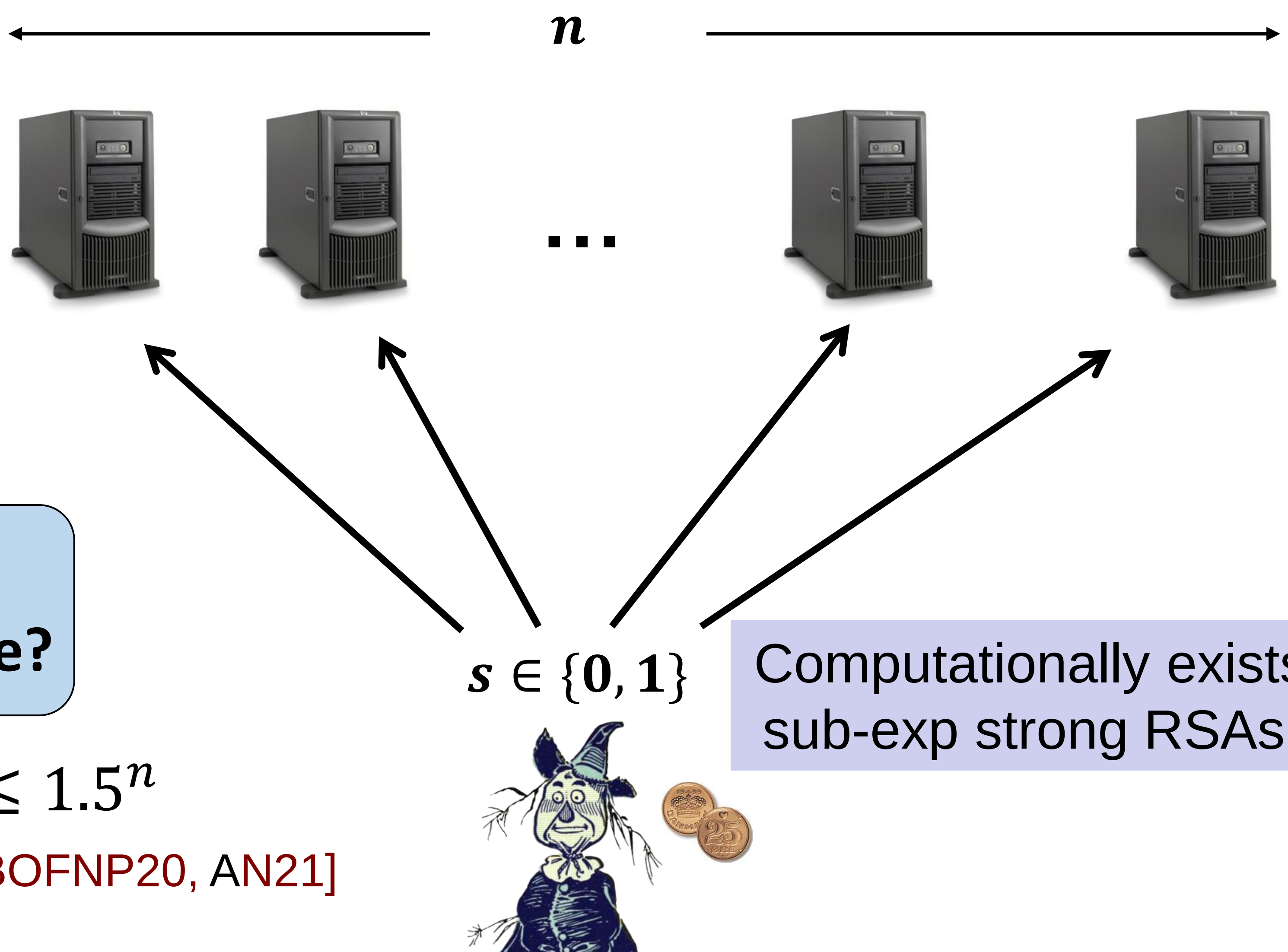
Unauthorized coalition learn nothing on s

Generalized Secret Sharing

[Sha,Bla79,ISN87]

$\boldsymbol{f}: \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{n}} \rightarrow \{\mathbf{0},\mathbf{1}\}$

Monotone function



$\boldsymbol{s} \in \{\mathbf{0},\mathbf{1}\}$

Computationally exists assuming sub-exp strong RSAs [ABIKLV23]!

[Csirmaz 94]

$\widetilde{\Omega}(n) \leq$

poly(n)
max-share size?

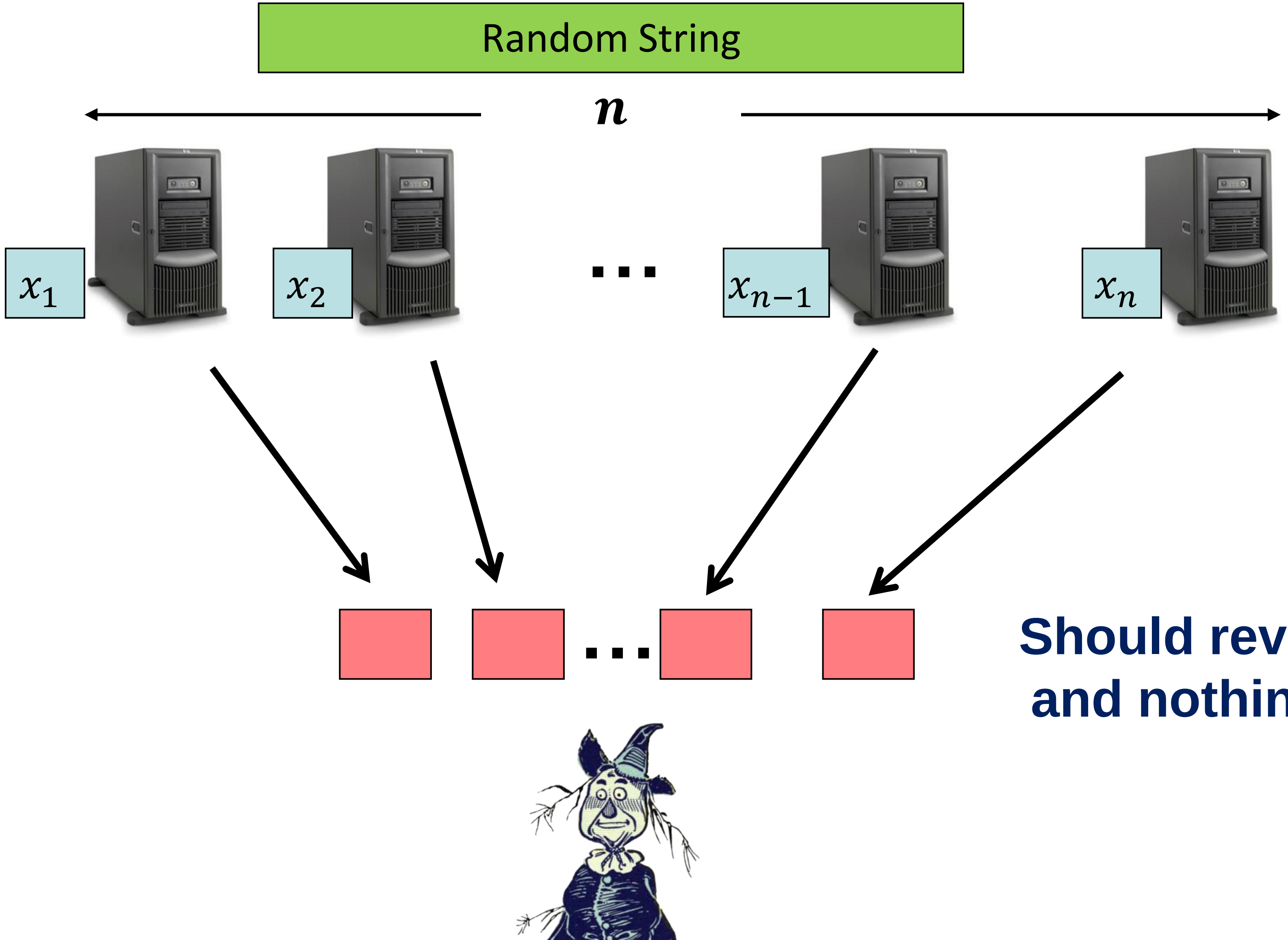
$\leq 1.5^{n}$

[LVW18,LV18,ABOFNP19, ABOFNP20, AN21]

Fully-Decomposable Randomized Encodings

[Yao,FKN90,IK00, AIK04]

$\boldsymbol{f}: \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{n}} \to \{\mathbf{0},\mathbf{1}\}$



Random String

$\boldsymbol{n}$

x_1

x_2

…

x_{n-1}

x_n

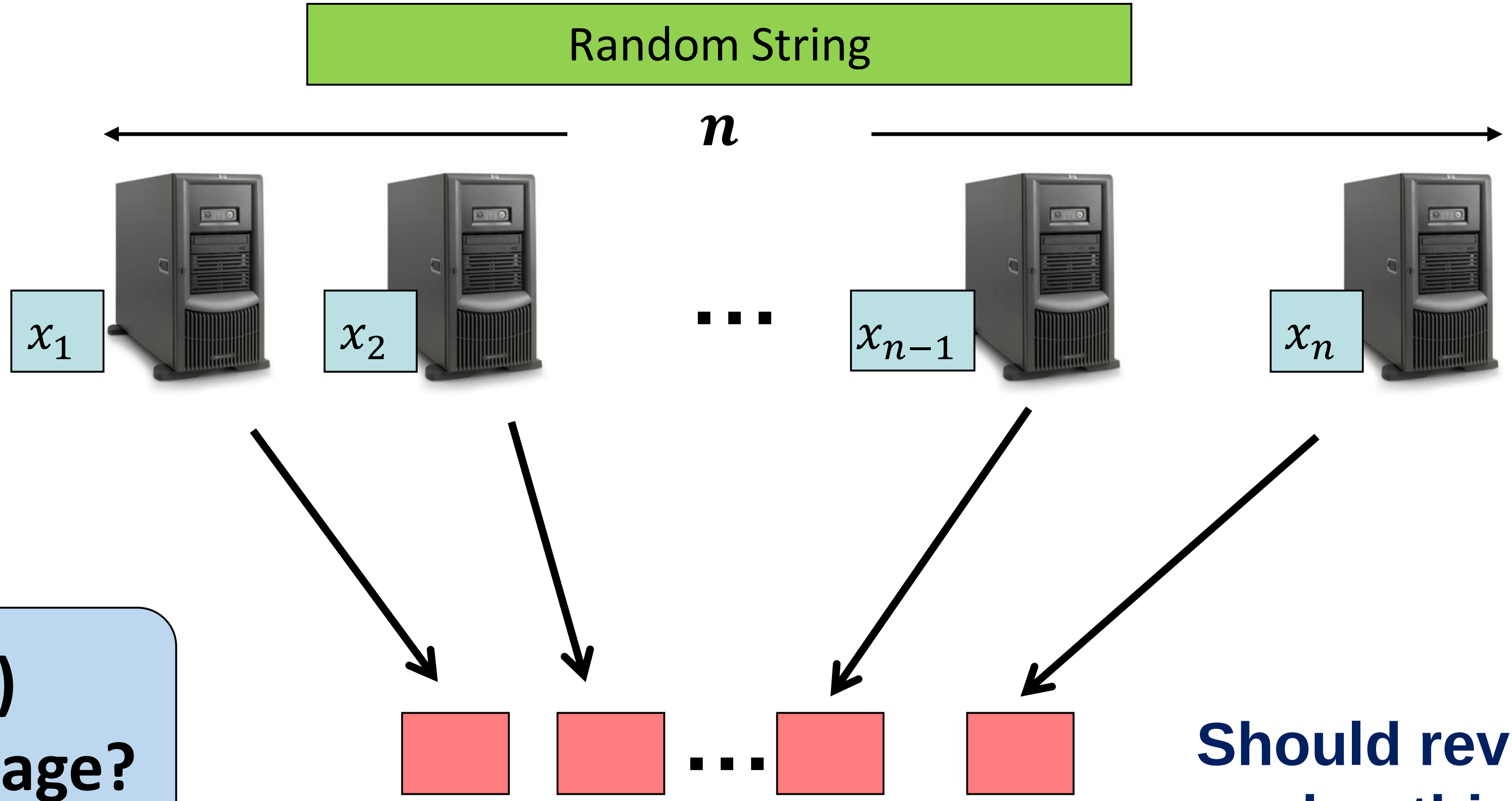
…

Should reveal f(x) and nothing else

Fully-Decomposable Randomized Encodings

[Yao,FKN90,IK00, AIK04]

$\boldsymbol{f}: \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{n}} \rightarrow \{\mathbf{0}, \mathbf{1}\}$



Random String

$\boldsymbol{n}$

x_1 x_2 … x_{n-1} x_n

…

[BHILM20]

$\tilde{\Omega}(n) \leq$

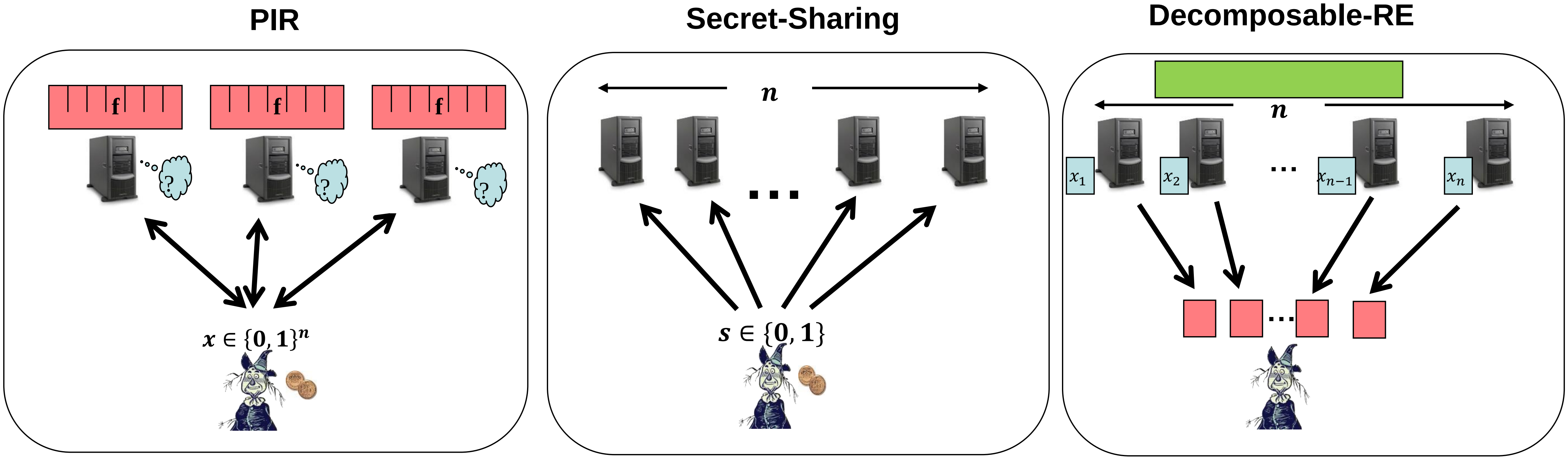
poly(n) max-message?

$\leq 2^{n/2}$

[BIKK14,BKN18]

Should reveal f(x) and nothing else

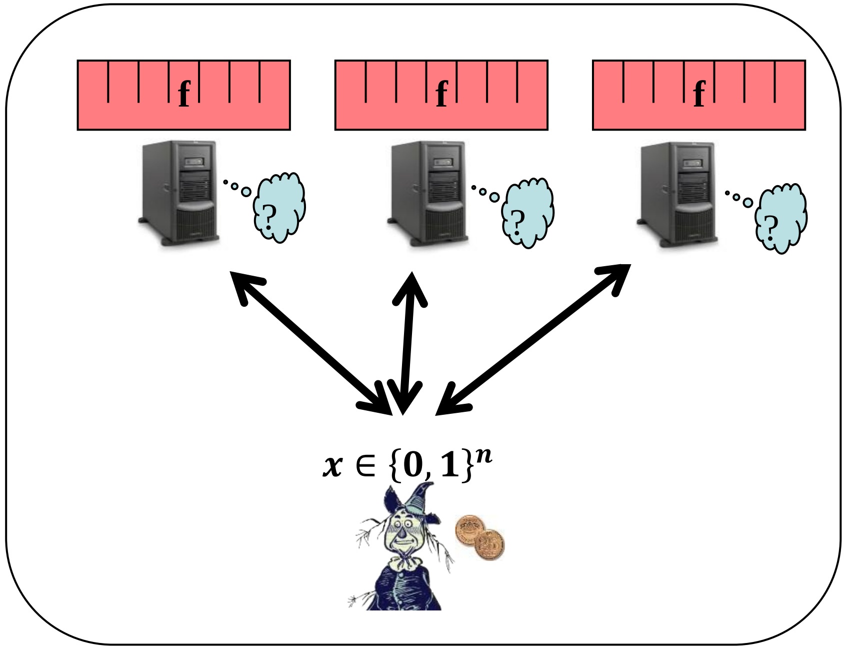
$$f: \{0,1\}^n \to \{0,1\}$$



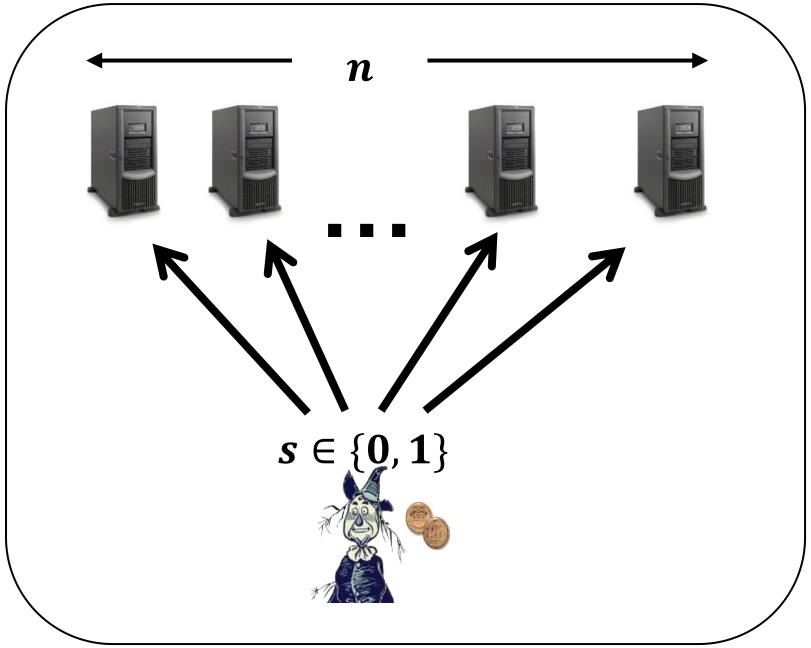
- Upper-bounds: (sub-)Exponential vs Lower-bounds: (almost) Linear
- Unlike Complexity theory, not even non-constructive LB, no general reductions
- Why should we care?
  - Basic questions
  - Toy versions of advanced primitives (witness encryption, functional encryption,..)
  - Highlights basic gaps in our understandings

$$f:\{0,1\}^n \to \{0,1\}$$

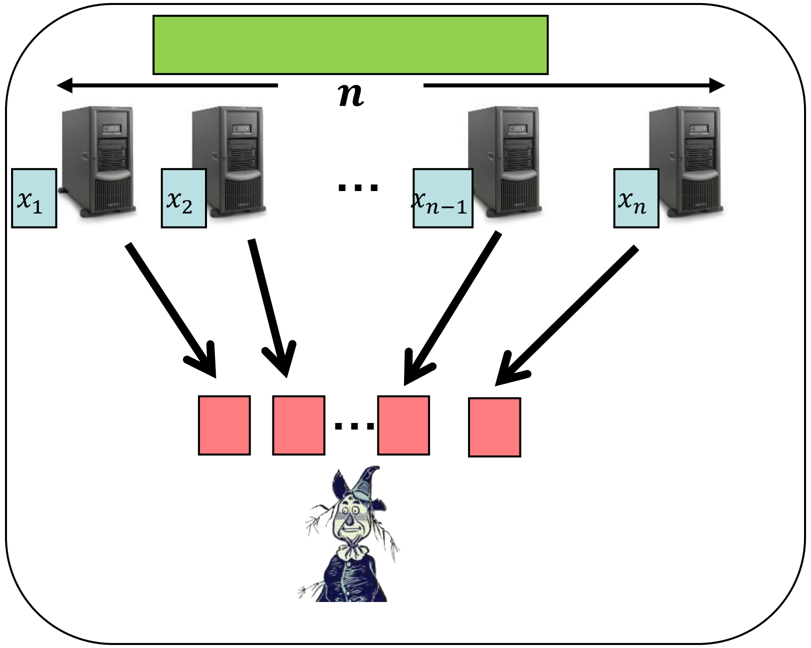
PIR



Secret-Sharing



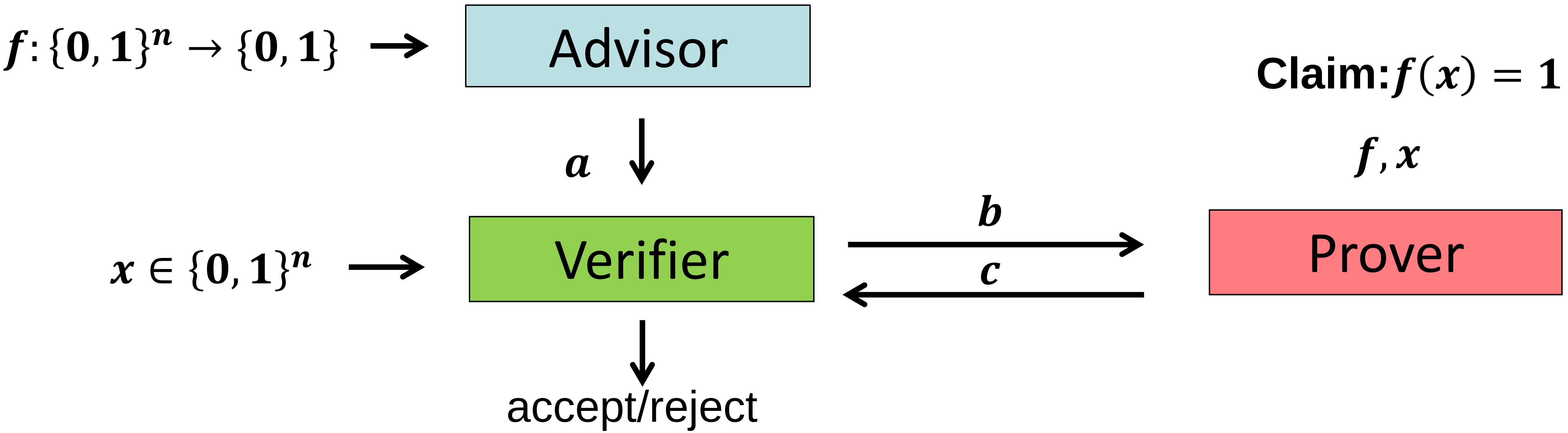
Decomposable-RE



This work: New Hypothesis ⇒ super-polynomial lower-bounds for all the above

- Space/Query tradeoff in Interactive Proof setting
- Provides new insights regarding the differences
- Unifies some existing lower-bounds
- Separate some existing LB's techniques

Advisor-Verifier-Prover Games

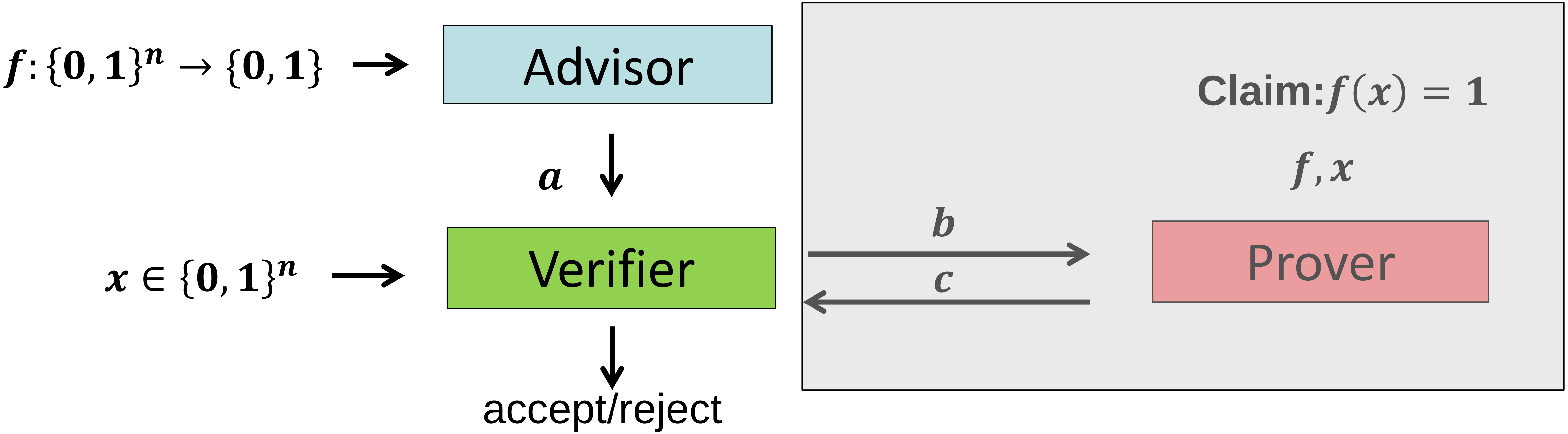


Defaults:

- All parties are computationally-unbounded (can’t talk about fixed f)
- Perfect completeness and constant soundness (e.g., 1/2)
- One-time advice

Goal: Minimize total communication |a|+|b|+|c|

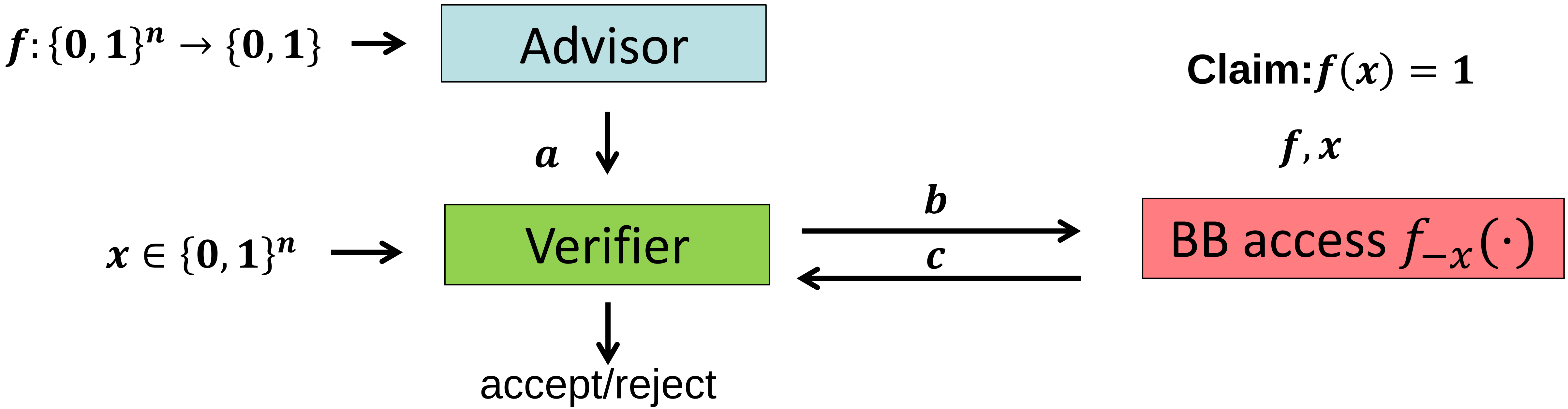
Related Models


$\boldsymbol{f}: \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{n}} \to \{\mathbf{0},\mathbf{1}\}$
Advisor
$\boldsymbol{a}$
$\boldsymbol{x} \in \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{n}}$
Verifier
accept/reject
Claim: $\boldsymbol{f}(\boldsymbol{x}) = \mathbf{1}$
$\boldsymbol{f}, \boldsymbol{x}$
$\boldsymbol{b}$
$\boldsymbol{c}$
Prover

No prover: one-way communication complexity [KNR95]

- Lower-bound of $\Omega(2^n)$

Related Models



$f:\{0,1\}^n \rightarrow \{0,1\}$

Advisor

a

$x \in \{0,1\}^n$

Verifier

accept/reject

b

c

Claim: $f(x) = 1$

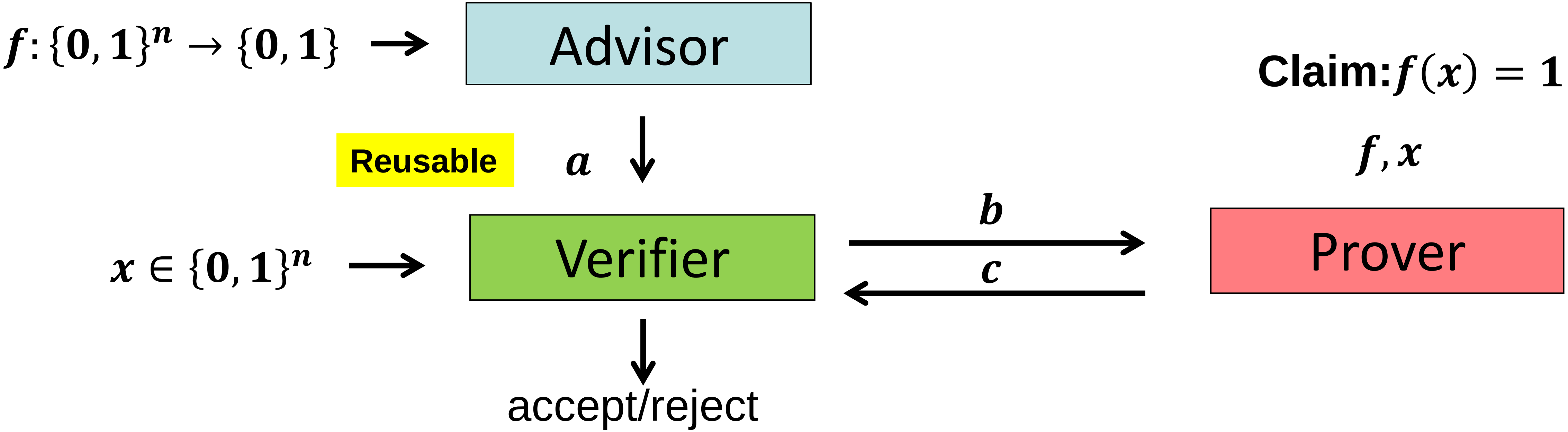
f, x

BB access $f_{-x}(\cdot)$

Non-adaptive Yao's BB model [Yao90]

- Lower-bound of $\Omega(2^{n/2})$

Related Models



$f: \{0,1\}^n \to \{0,1\}$

Advisor

Reusable

a

Claim: $f(x) = 1$

f, x

$x \in \{0,1\}^n$

Verifier

b

c

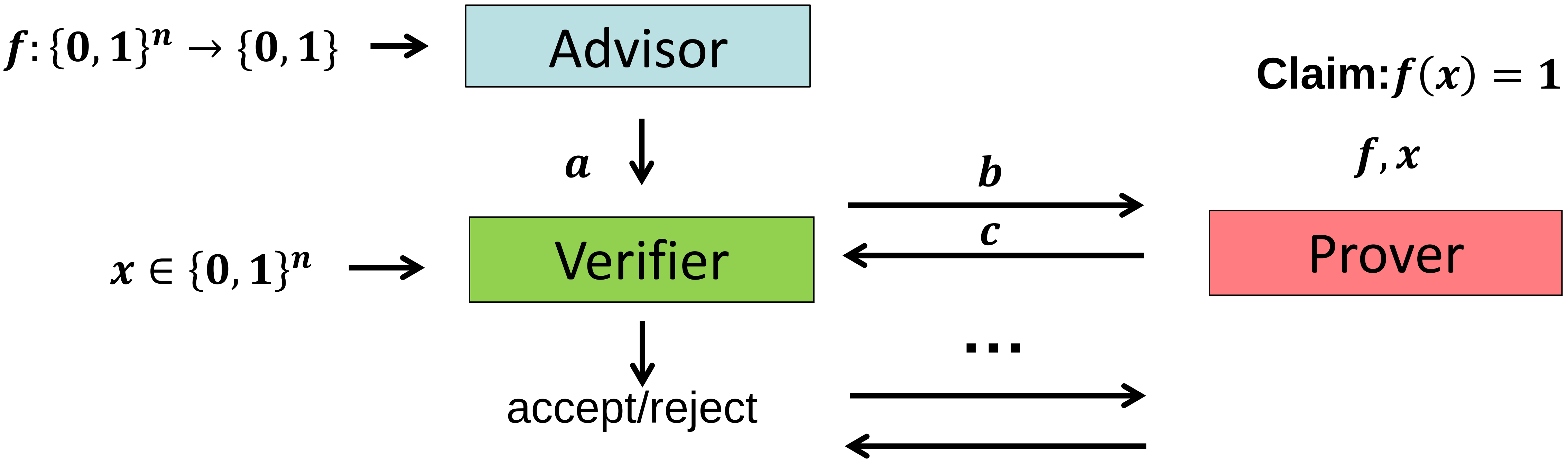
Prover

accept/reject

Online (read-only) Memory Checking [BEGKN94, NR09]

- Lower-bound of $\Omega(2^{n/2})$

Related Models

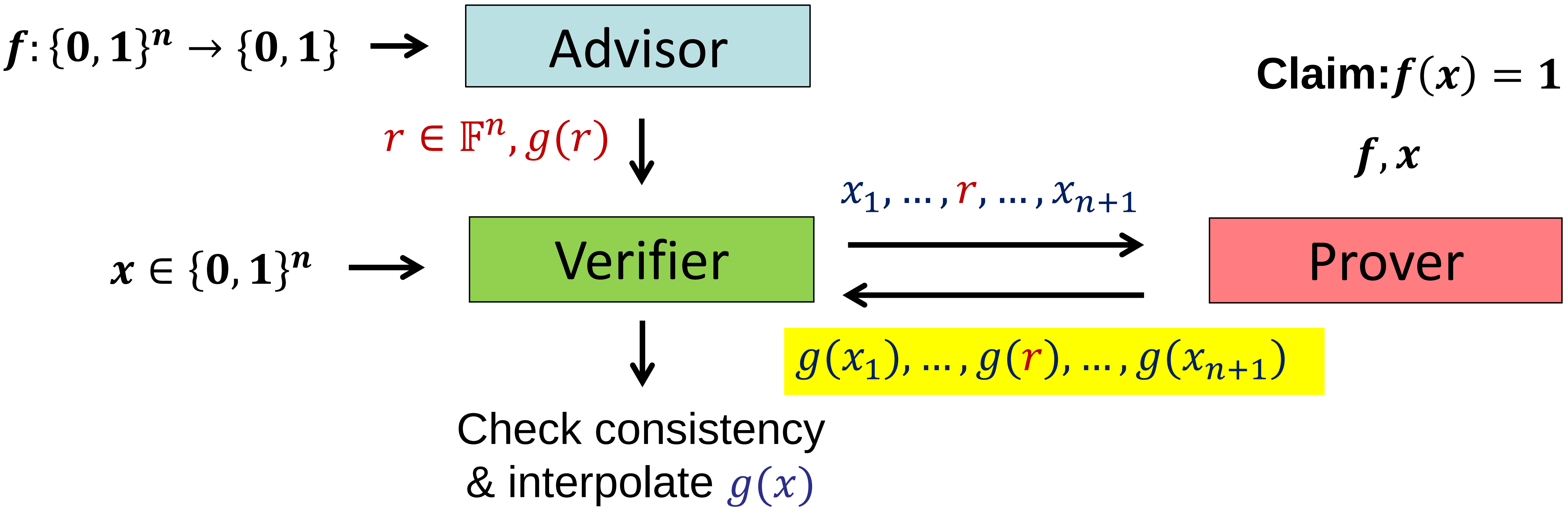


Non-Uniform Delegation [GKR08]

- Upper-bound: poly(n) communication in O(n log n)
- f in (D-depth,S-size) ⇒ poly(D, log(S)) communication in D log n rounds

Poly(n) Communication in a single round?

$\boldsymbol{g}: \mathbb{F}^{\boldsymbol{n}} \to \mathbb{F}$ Multilinear extension of f



$\boldsymbol{f}: \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{n}} \to \{\mathbf{0},\mathbf{1}\}$ $\longrightarrow$ Advisor

$r \in \mathbb{F}^n, g(r)$ $\downarrow$

$\boldsymbol{x} \in \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{n}}$ $\longrightarrow$ Verifier

$x_1, \dots, r, \dots, x_{n+1}$ $\longrightarrow$

$\longleftarrow$ $g(x_1), \dots, g(r), \dots, g(x_{n+1})$

Prover

Claim: $\boldsymbol{f}(\boldsymbol{x}) = \mathbf{1}$

$\boldsymbol{f}, \boldsymbol{x}$

$\downarrow$

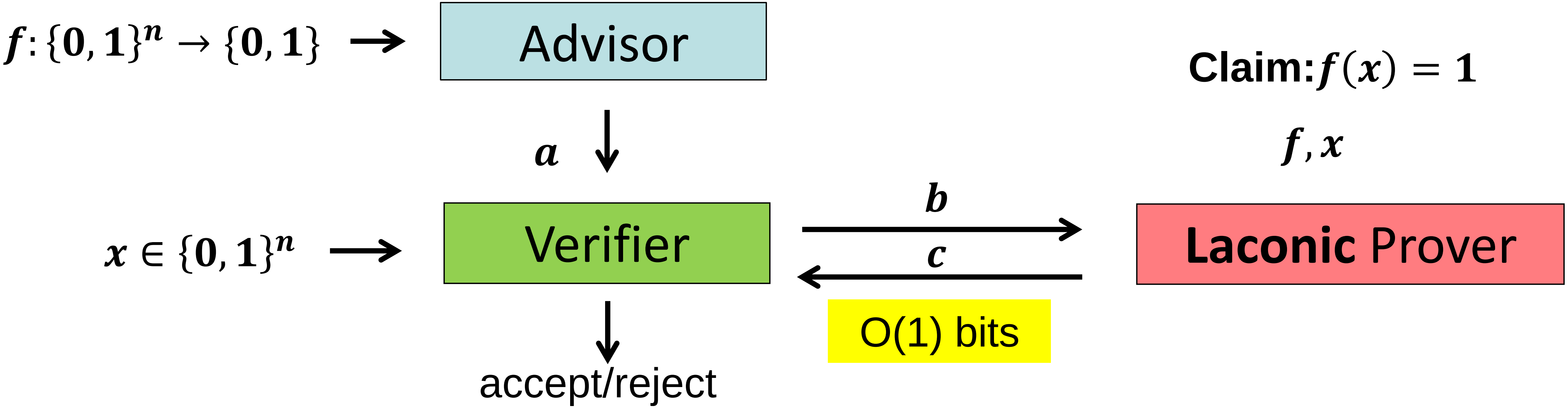
Check consistency
& interpolate $g(x)$

Soundness error: 1-1/n, amplify via parallel repetitions

Communication complexity (after repetitions): $O(n^3 \log n)$

Prover’s message: polynomially-long

Hypothesis:
Prover-Laconic AVP has super-poly complexity



$f: \{0,1\}^n \to \{0,1\}$

Advisor

a

$x \in \{0,1\}^n$

Verifier

accept/reject

b

c

O(1) bits

Claim: $f(x) = 1$

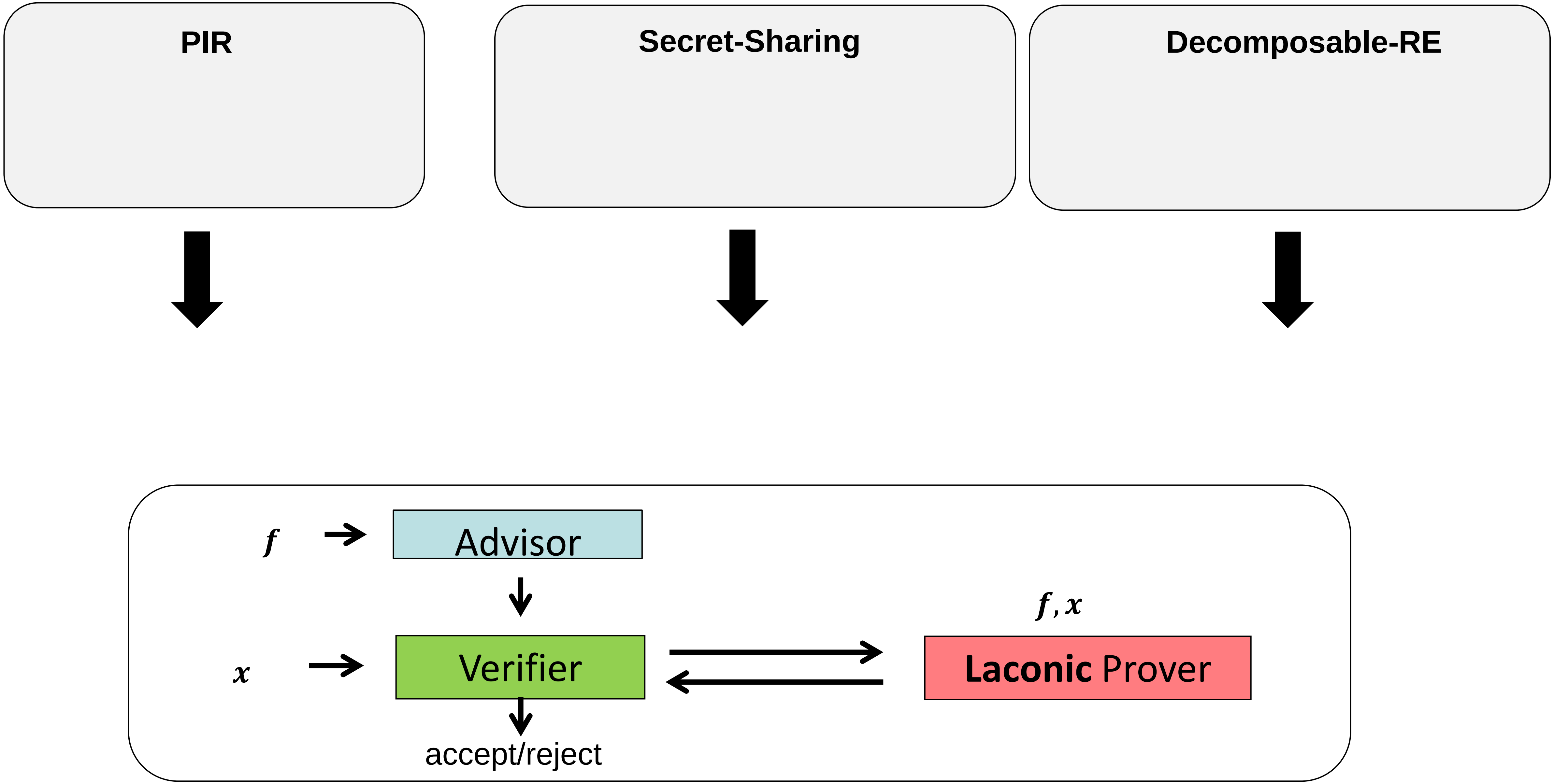
f, x

Laconic Prover

Thm: poly(n) PIR/SSS/DRE ⇒ Prover-Laconic AVP with polynomial complexity

Cor: Hypothesis ⇒ super-poly lower-bounds for PIR, Secret Sharing, DRE

From Secrecy to Soundness



PIR

Secret-Sharing

Decomposable-RE

f

Advisor

x

Verifier

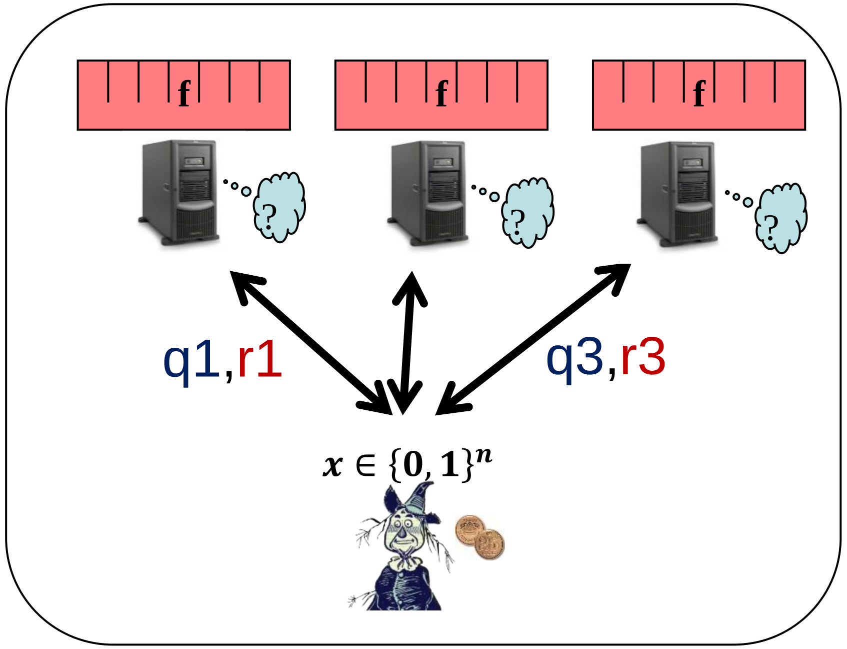
accept/reject

f, x

Laconic Prover

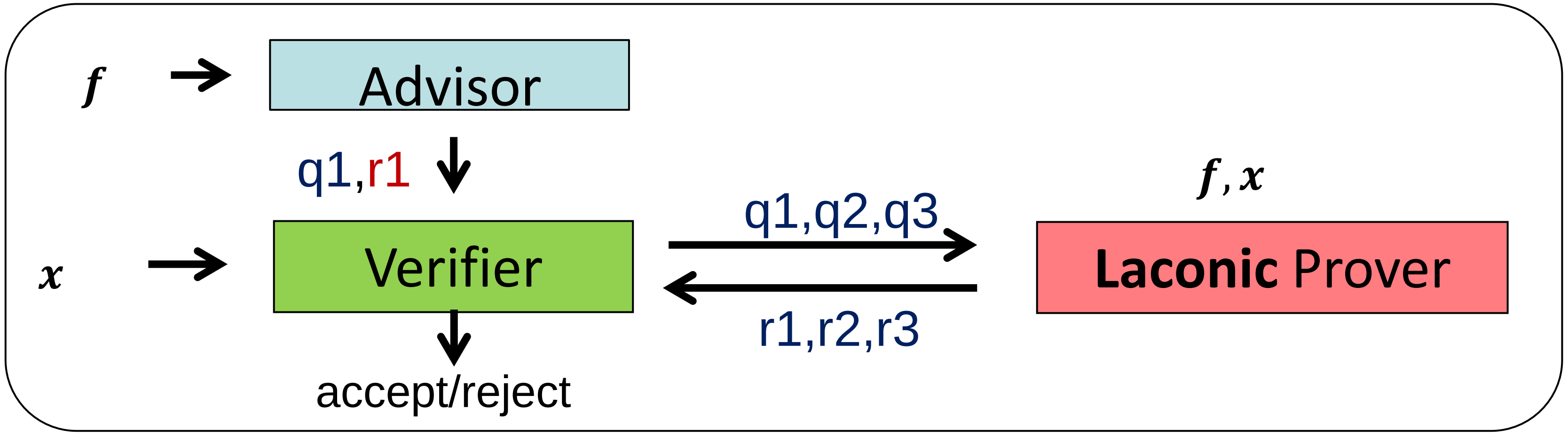
From Secrecy to Soundness

PIR



Secret-Sharing

Decomposable-RE


f → Advisor

q1,r1

x → Verifier

q1,q2,q3

r1,r2,r3

f, x

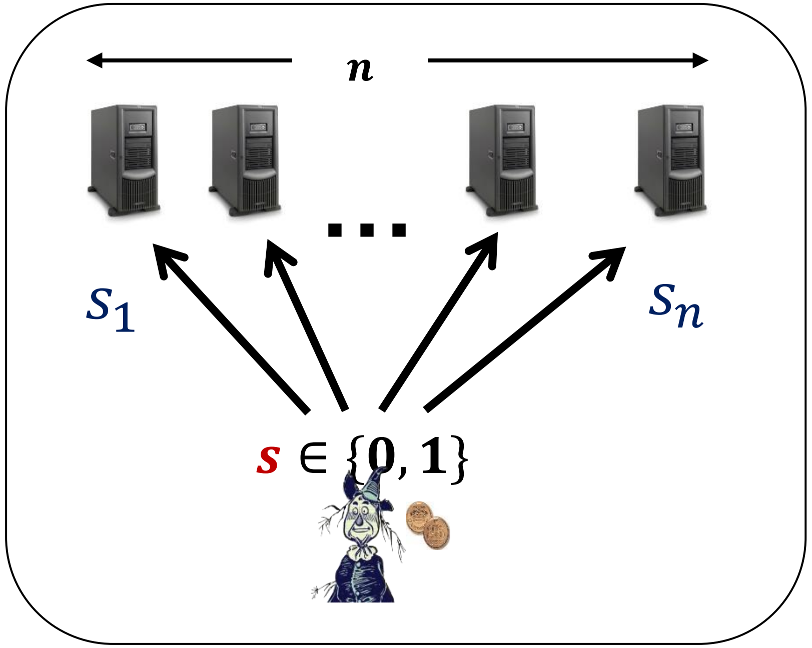
Laconic Prover

accept/reject

From Secrecy to Soundness

PIR

Secret-Sharing



n

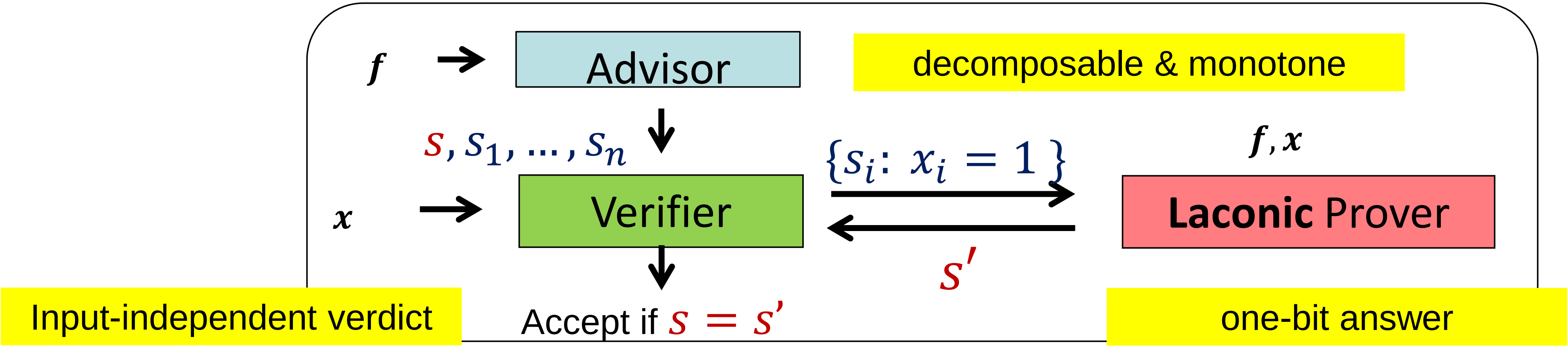
s_1

s_n

...

$s \in \{0, 1\}$

Decomposable-RE



f → Advisor

decomposable & monotone

$s, s_1, \ldots, s_n$

$\{s_i \colon x_i = 1\}$

f, x

x → Verifier

Laconic Prover

s'

Input-independent verdict

Accept if $s = s'$

one-bit answer

AVPs with Extra Features

PIR

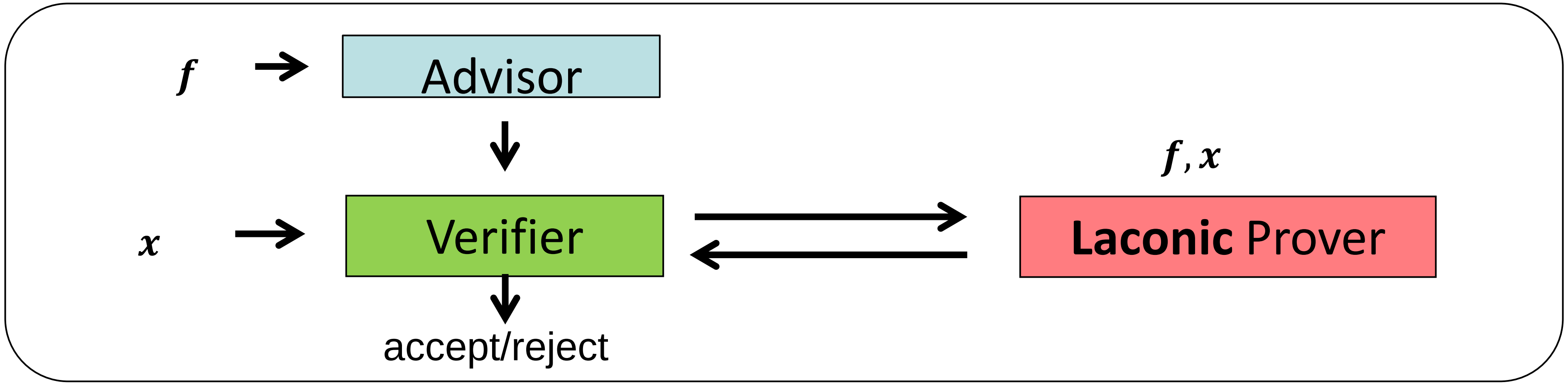
NONE

Secret-Sharing

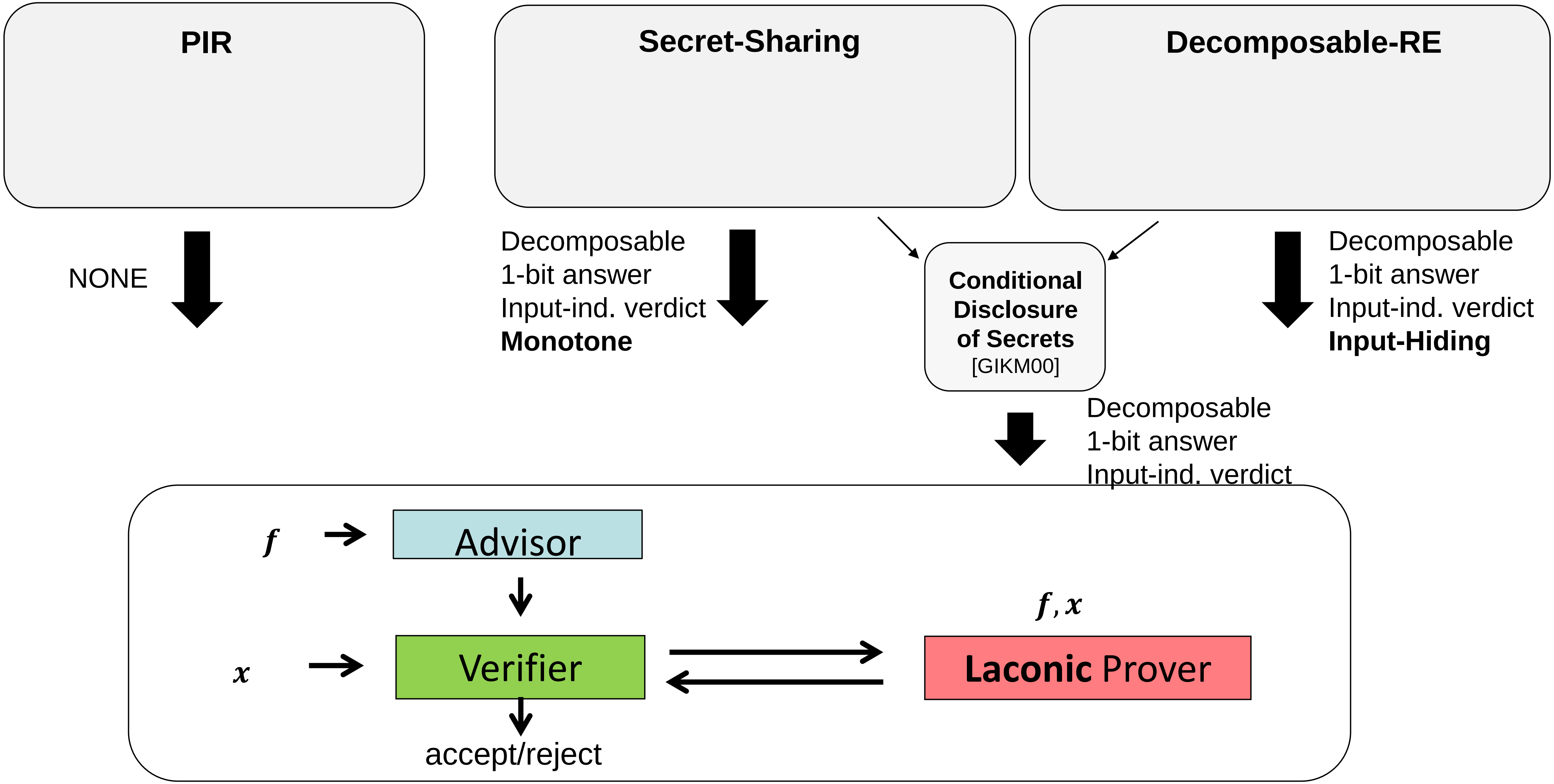
Decomposable
1-bit answer
Input-ind. verdict
Monotone

Decomposable-RE

Decomposable
1-bit answer
Input-ind. verdict
Input-Hiding



AVPs with Extra Features



PIR

Secret-Sharing

Decomposable-RE

NONE

Decomposable
1-bit answer
Input-ind. verdict
Monotone

Conditional Disclosure of Secrets
[GIKM00]

Decomposable
1-bit answer
Input-ind. verdict
Input-Hiding

Decomposable
1-bit answer
Input-ind. verdict

f → Advisor

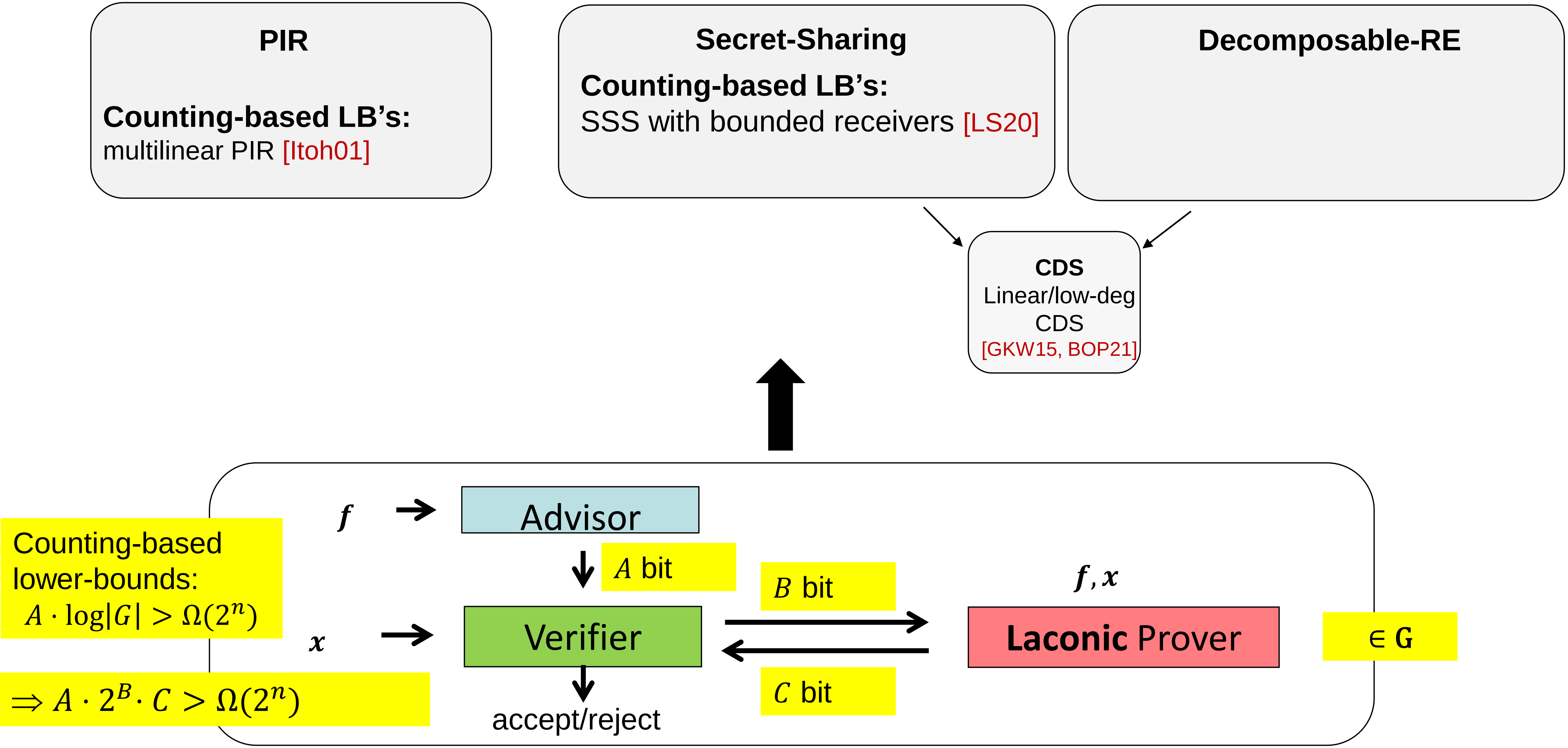
x → Verifier

accept/reject

f, x

Laconic Prover

Can we unify LBs?



PIR

Counting-based LB’s:
multilinear PIR [Itoh01]

Secret-Sharing

Counting-based LB’s:
SSS with bounded receivers [LS20]

Decomposable-RE

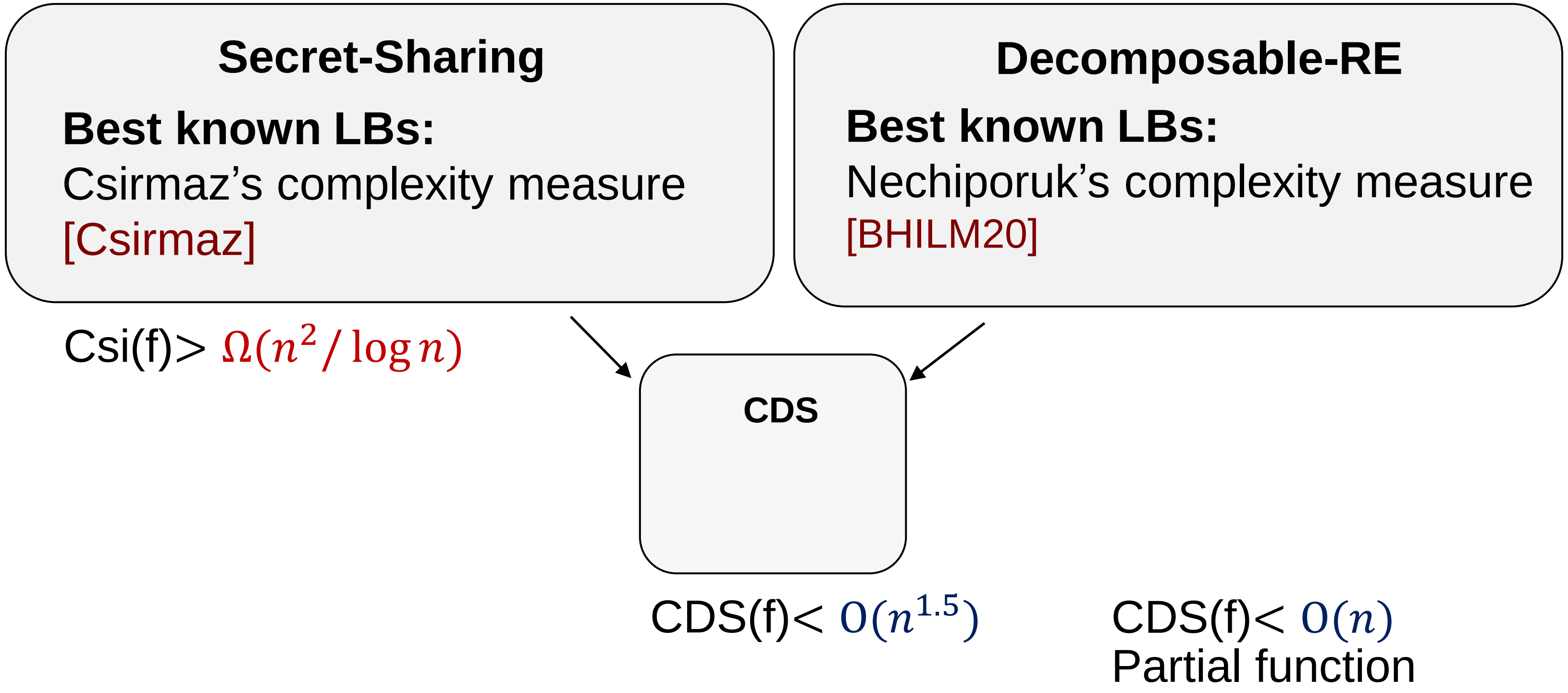
CDS
Linear/low-deg CDS
[GKW15, BOP21]

Counting-based lower-bounds:
$A \cdot \log|G| > \Omega(2^n)$

$\Rightarrow A \cdot 2^B \cdot C > \Omega(2^n)$

Can we unify LBs?

Cannot be unified!



Secret-Sharing

Best known LBs:
Csirmaz's complexity measure
[Csirmaz]

Csi(f)> $\Omega(n^2/\log n)$

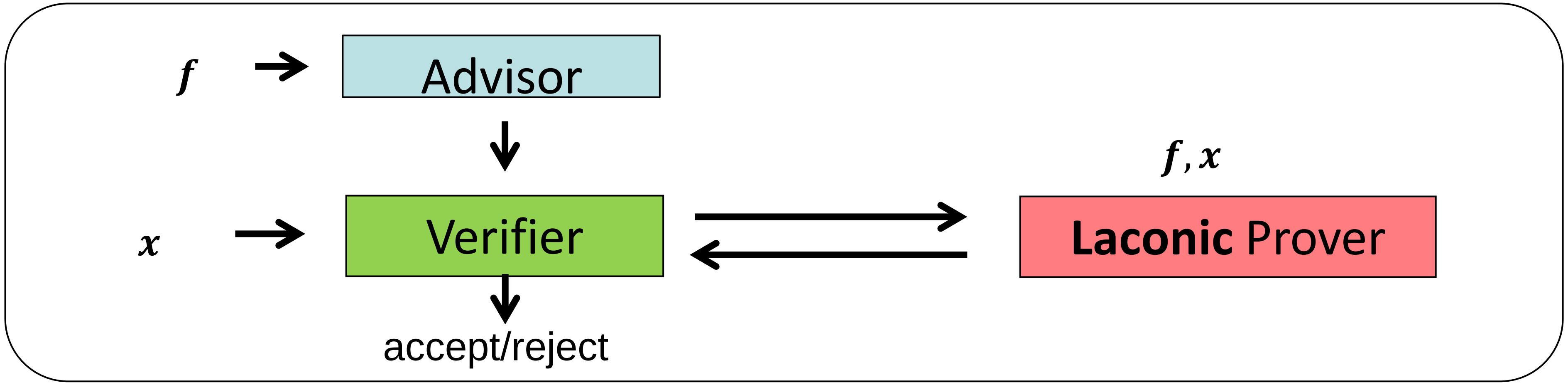
Decomposable-RE

Best known LBs:
Nechiporuk's complexity measure
[BHILM20]

CDS

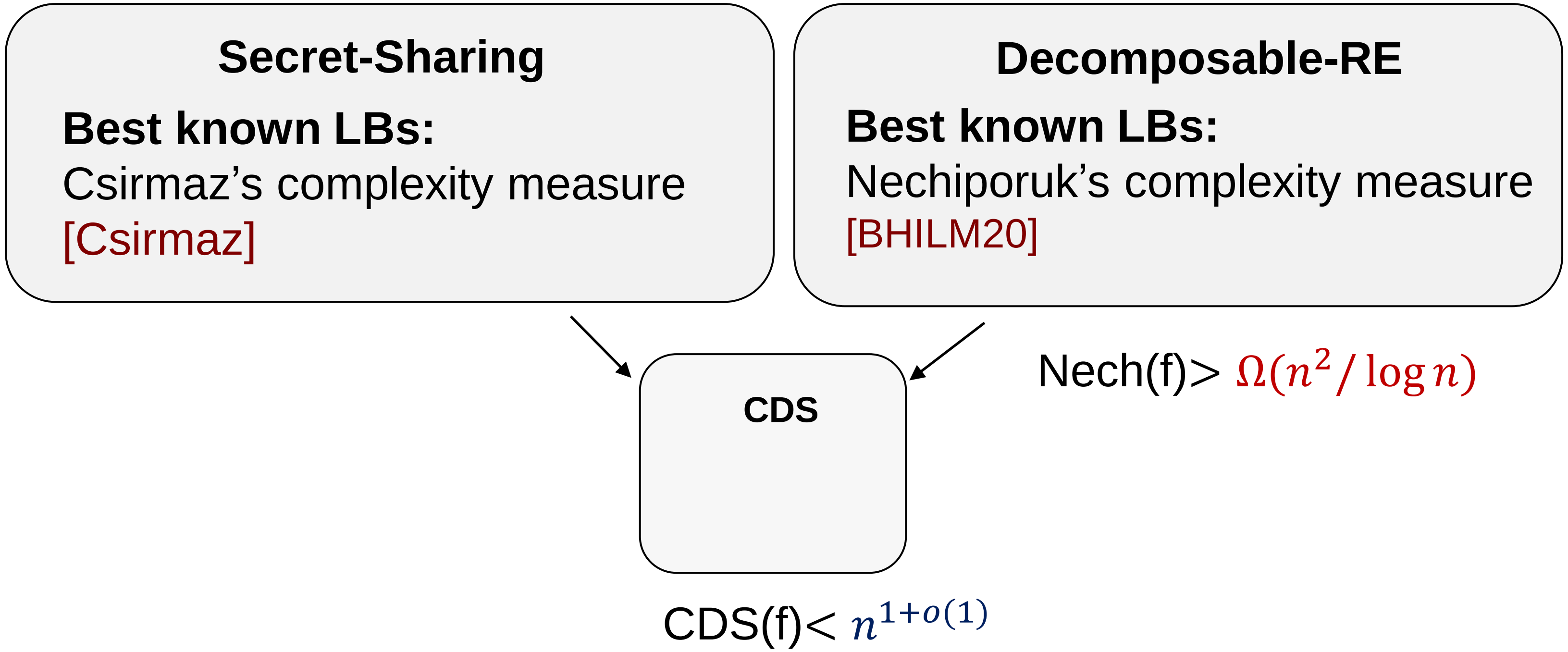
CDS(f)< $O(n^{1.5})$

CDS(f)< $O(n)$
Partial function



Can we unify LBs?

Cannot be unified!



Secret-Sharing

Best known LBs:
Csirmaz's complexity measure
[Csirmaz]

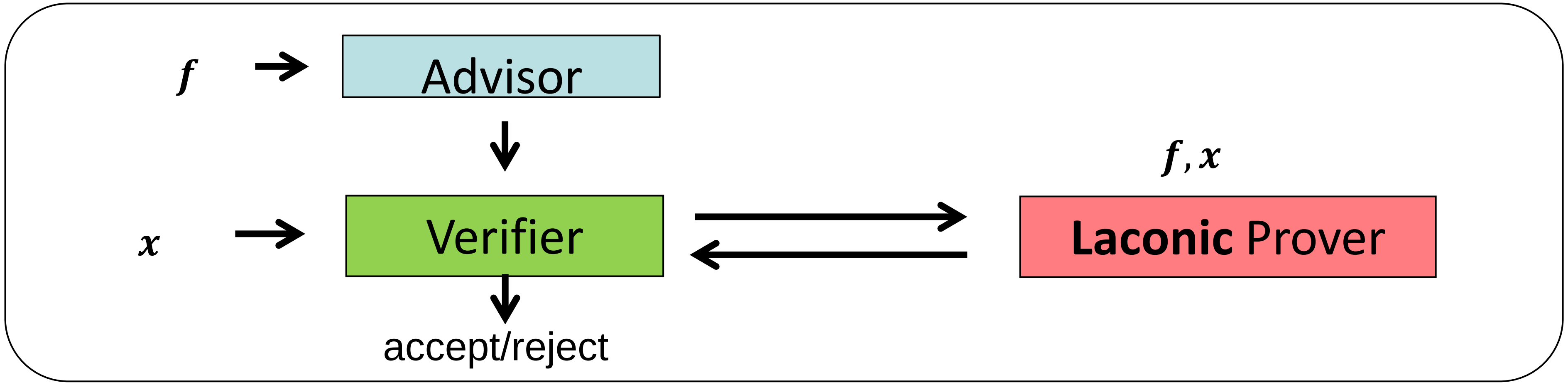
Decomposable-RE

Best known LBs:
Nechiporuk's complexity measure
[BHILM20]

CDS

Nech(f)> $\Omega(n^2/\log n)$

CDS(f)< $n^{1+o(1)}$



f → Advisor

x → Verifier

f, x

Laconic Prover

accept/reject

Conclusion

Basic IT-primitives $\Rightarrow$ Online/Offline Decomposition

New Advisor-Verifier-Prover Model

- Single hypothesis $\Rightarrow$ several super-poly LBs
- Induces new partial order over primitives
- Unify some existing lower bounds
- New separations

Future:

- Scale down to functions in P
- More (conditional) lower-bounds? Relations to existing questions?