Abstract Non-Interference

An Abstract Interpretation-based view on Code Security

Roberto Giacobazzi and Isabella Mastroeni

Dipartimento di Informatica
Università di Verona
Italy

London, April 2012

THE DIMENSIONS OF NON-INTERFERENCE

We distinguish two points of view [*Sabelfeld & Sands 2005*]:

- WHO observes the information flows?
- WHAT information flows?

THE DIMENSIONS OF NON-INTERFERENCE

We distinguish two points of view [*Sabelfeld & Sands 2005*]:

- WHO observes the information flows?

  How can we weaken non-interference by characterizing the observational capability of *who* observes?

  - ✔ By means of *Equivalence relations*: PER MODEL, ROBUST DECLASSIFICATION;
  - ✔ By means of *Abstract domains*: ABSTRACT NON-INTERFERENCE;

- WHAT information flows?

THE DIMENSIONS OF NON-INTERFERENCE

We distinguish two points of view [*Sabelfeld & Sands 2005*]:

- WHO observes the information flows?

  How can we weaken non-interference by characterizing the observational capability of *who* observes?

- WHAT information flows?

  How can we weaken non-interference by characterizing *what* of the private information flows?

THE DIMENSIONS OF NON-INTERFERENCE

We distinguish two points of view [*Sabelfeld & Sands 2005*]:

- WHO observes the information flows?

  How can we weaken non-interference by characterizing the observational capability of *who* observes?

- WHAT information flows?

  How can we weaken non-interference by characterizing *what* of the private information flows?

  - ✔ *Declassifying* what *can* flow: SELECTIVE DEPENDENCY, ENFORCING ROBUST DECLASSIFICATION, ABSTRACT NON-INTERFERENCE, DELIMITED RELEASE, RELAXED NONINTERFERENCE;

THE DIMENSIONS OF NON-INTERFERENCE

We distinguish two points of view [*Sabelfeld & Sands 2005*]:

- WHO observes the information flows?

  How can we weaken non-interference by characterizing the observational capability of *who* observes?

- WHAT information flows?

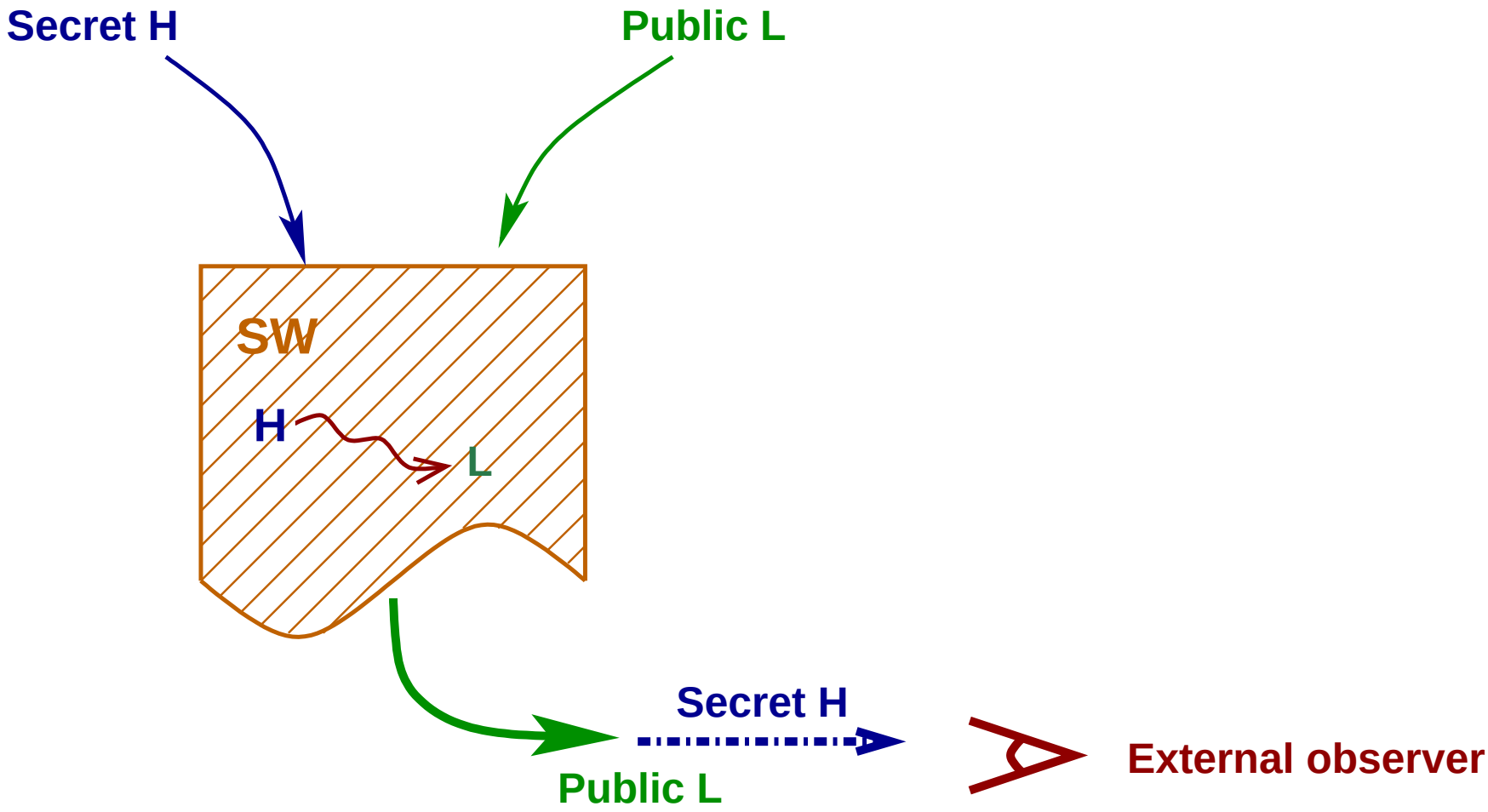
  How can we weaken non-interference by characterizing *what* of the private information flows?

  - *Declassifying* what *can* flow: SELECTIVE DEPENDENCY, ENFORCING ROBUST DECLASSIFICATION, ABSTRACT NON-INTERFERENCE, DELIMITED RELEASE, RELAXED NONINTERFERENCE;
  - *Classifying* what *cannot* flow: ABSTRACT NON-INTERFERENCE.

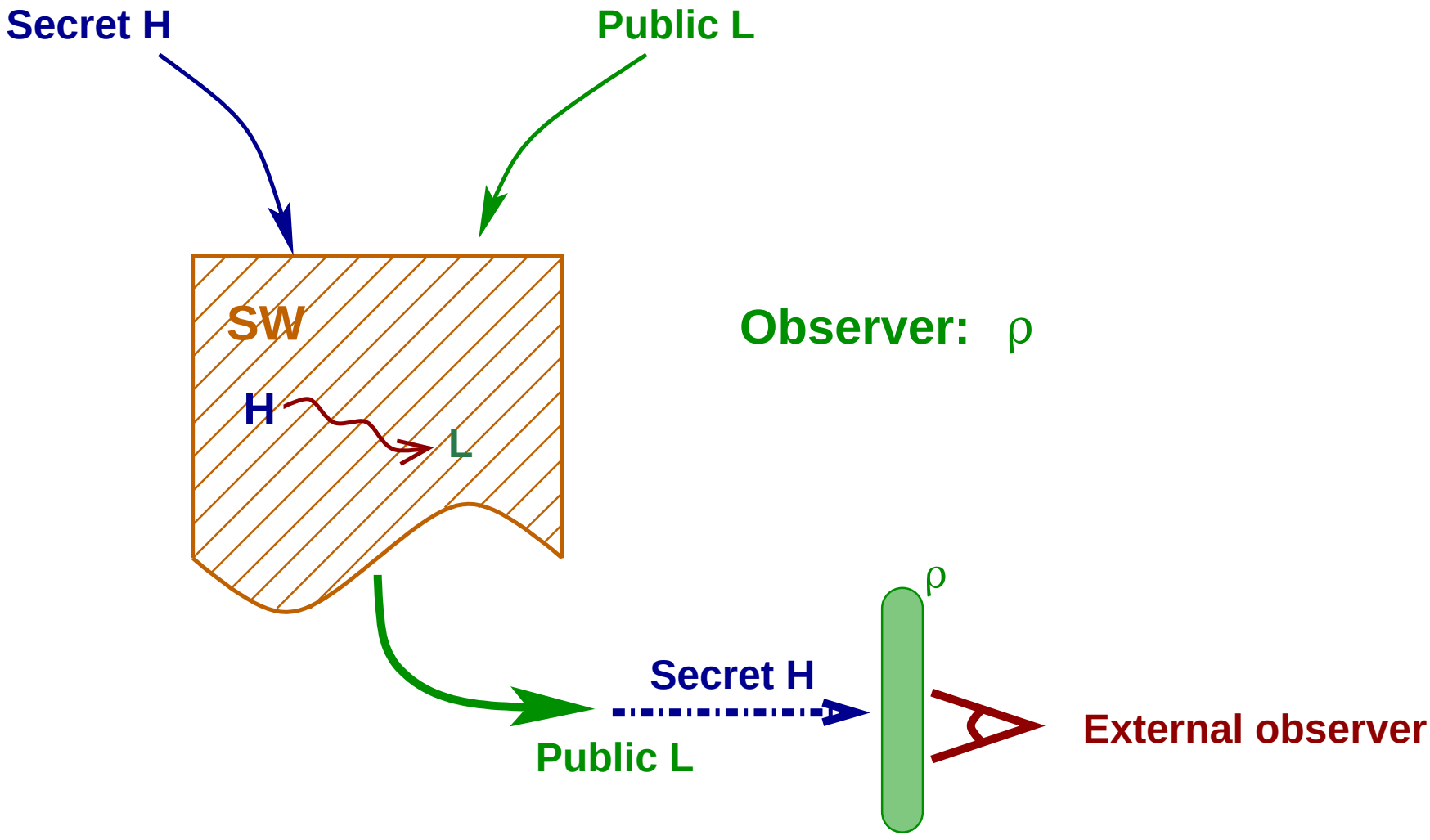
DEFINING

ABSTRACT NON-INTERFERENCE

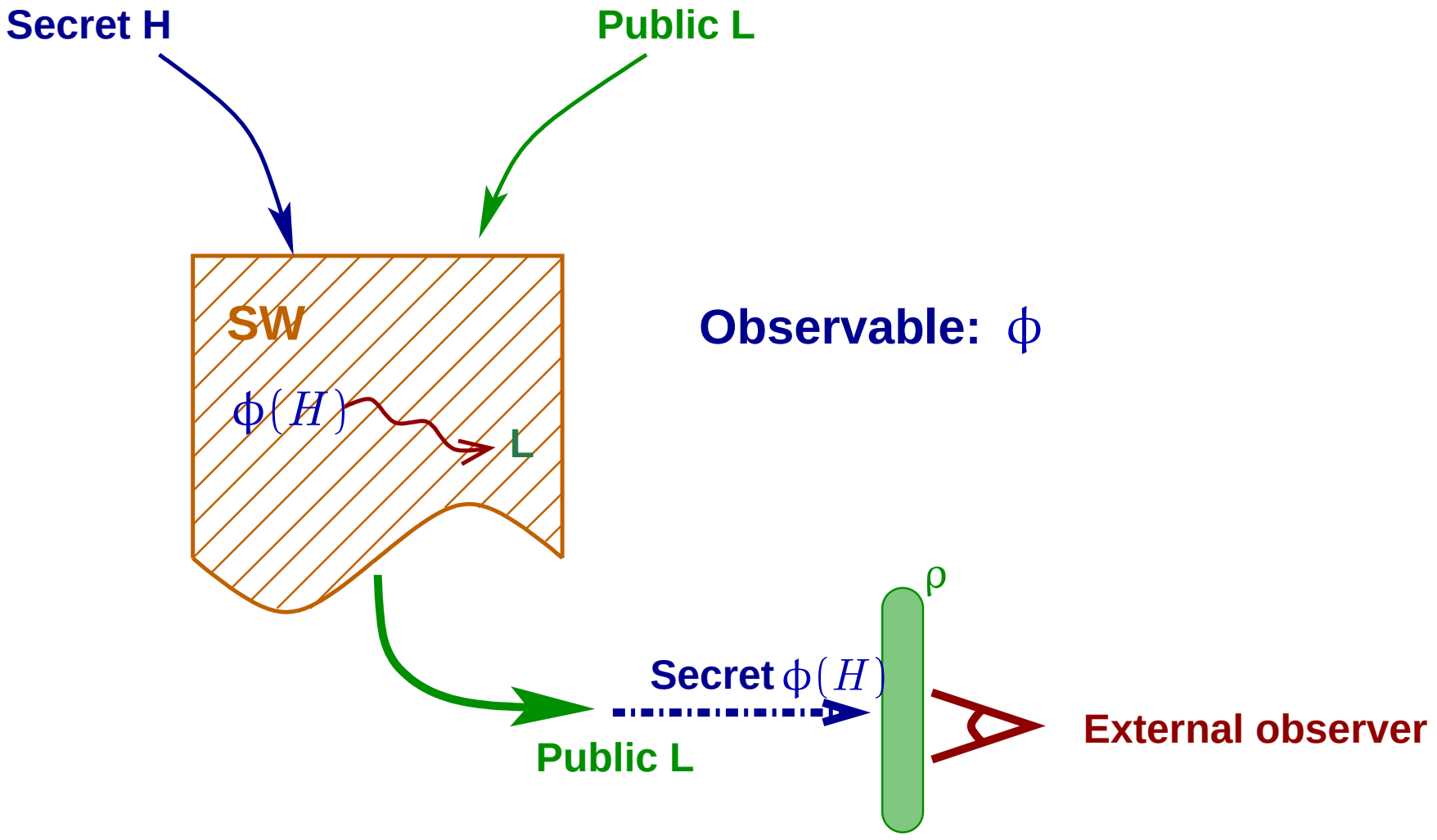
Our Idea



Our Idea

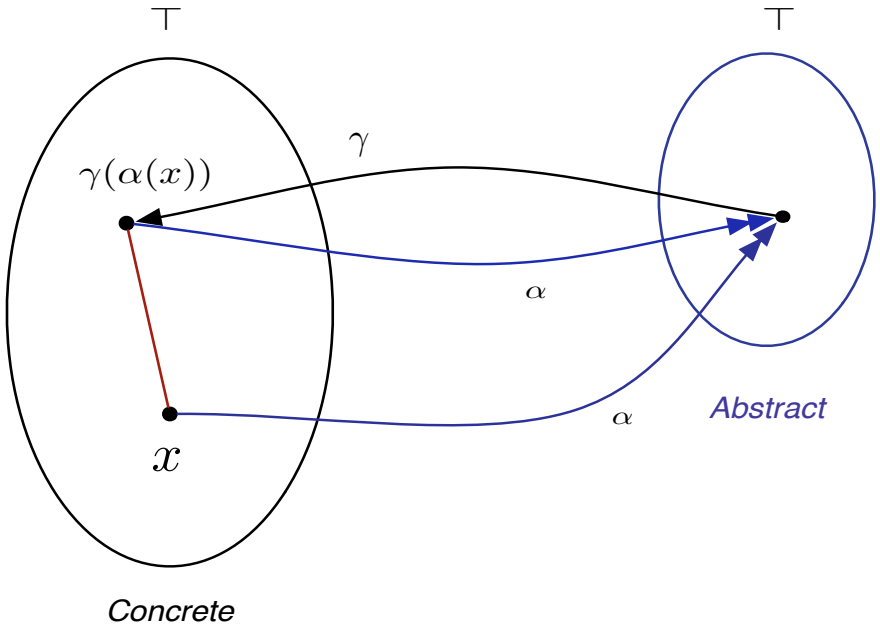

Secret H
Public L
SW
H
L
Observer: ρ
ρ
Secret H
Public L
External observer

Our Idea


Secret H
Public L
SW
$\phi(H)$
L
Observable: ϕ
ρ
Secret $\phi(H)$
Public L
External observer

ABSTRACT INTERPRETATION

Design approximate semantics of programs [Cousot & Cousot '77, '79].



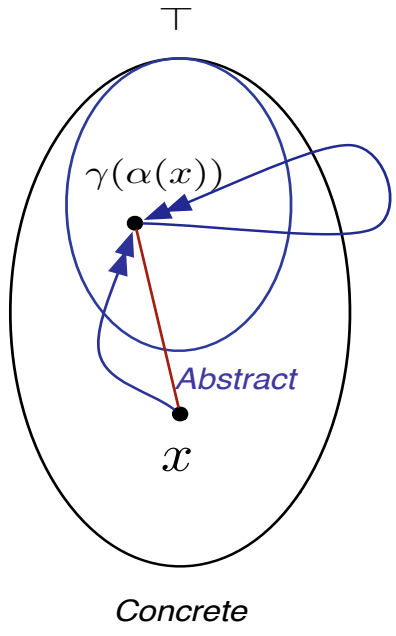
Galois Connection: $\langle C, \alpha, \gamma, A \rangle$, A and C are complete lattices.

Closures: $\langle \mathit{Abs}(C), \sqsubseteq \rangle$ set of all possible abstract domains,

$A_1 \sqsubseteq A_2$ if A_1 is more concrete than A_2

ABSTRACT INTERPRETATION

Design approximate semantics of programs [Cousot & Cousot '77, '79].



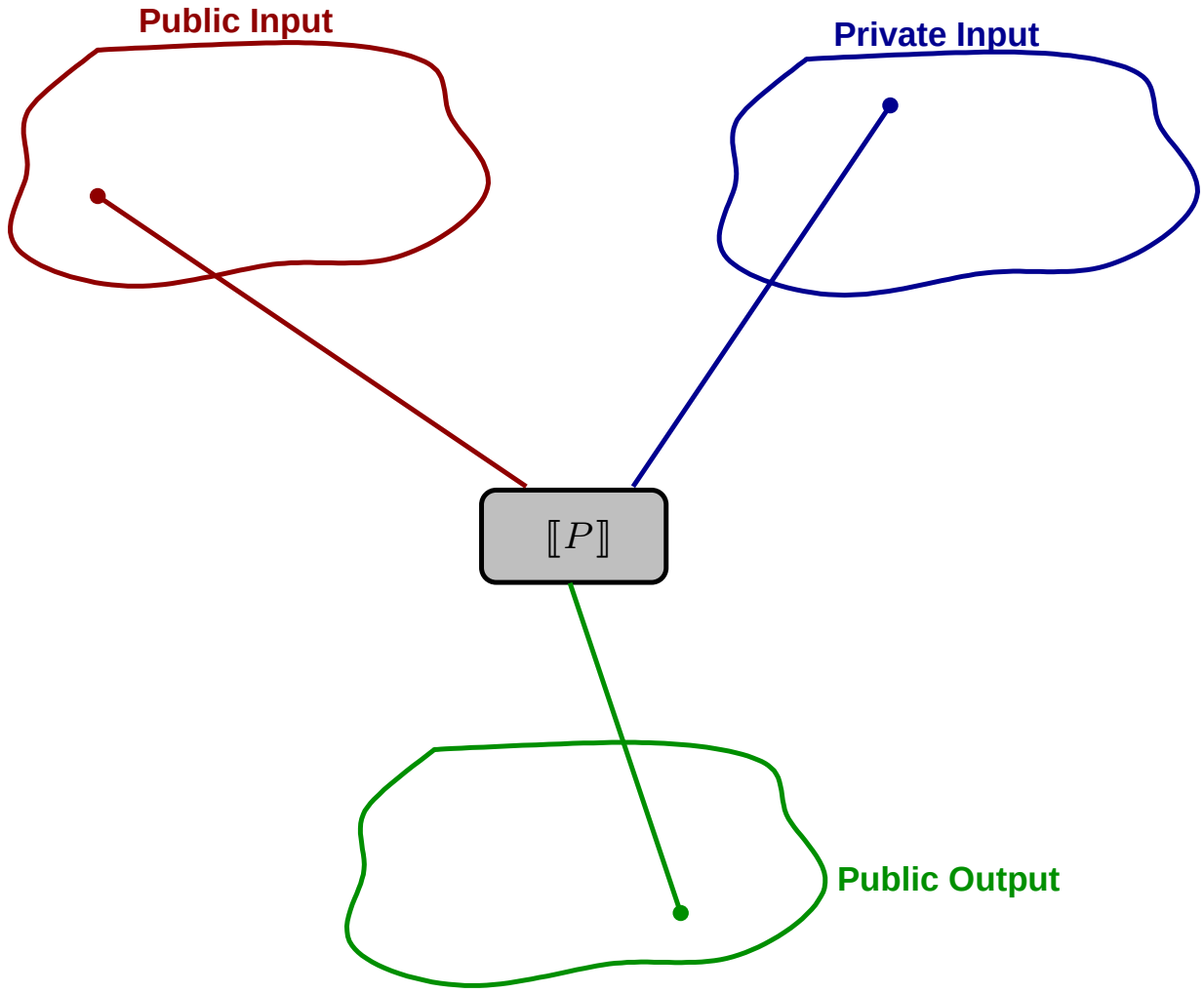
$\gamma \circ \alpha \in \mathit{Abs}(C)$

Galois Connection: $\langle C, \alpha, \gamma, A \rangle$, A and C are complete lattices.

Closures: $\langle \mathit{Abs}(C), \sqsubseteq \rangle$ set of all possible abstract domains,

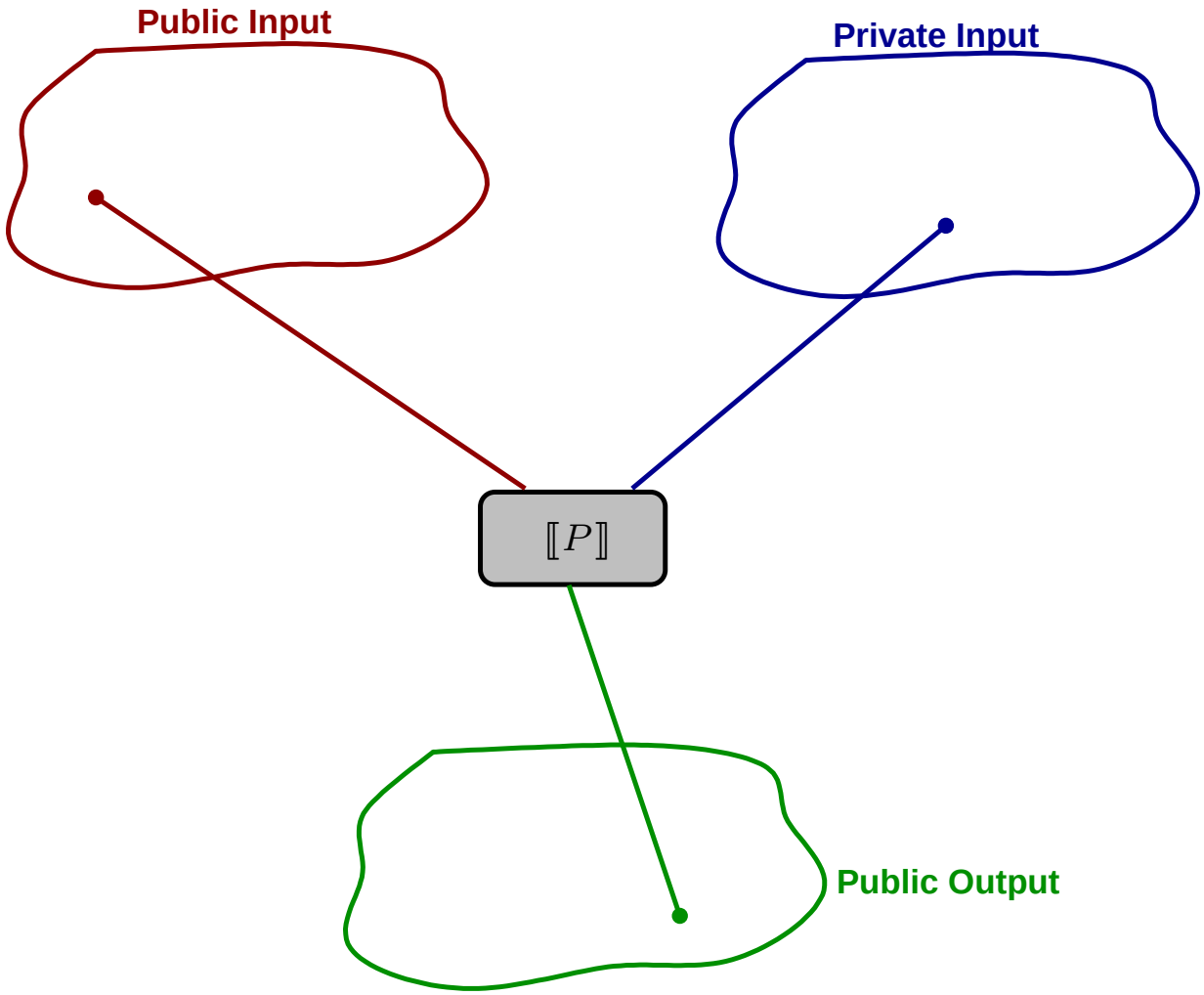
$A_1 \sqsubseteq A_2$ if A_1 is more concrete than A_2

STANDARD NON-INTERFERENCE



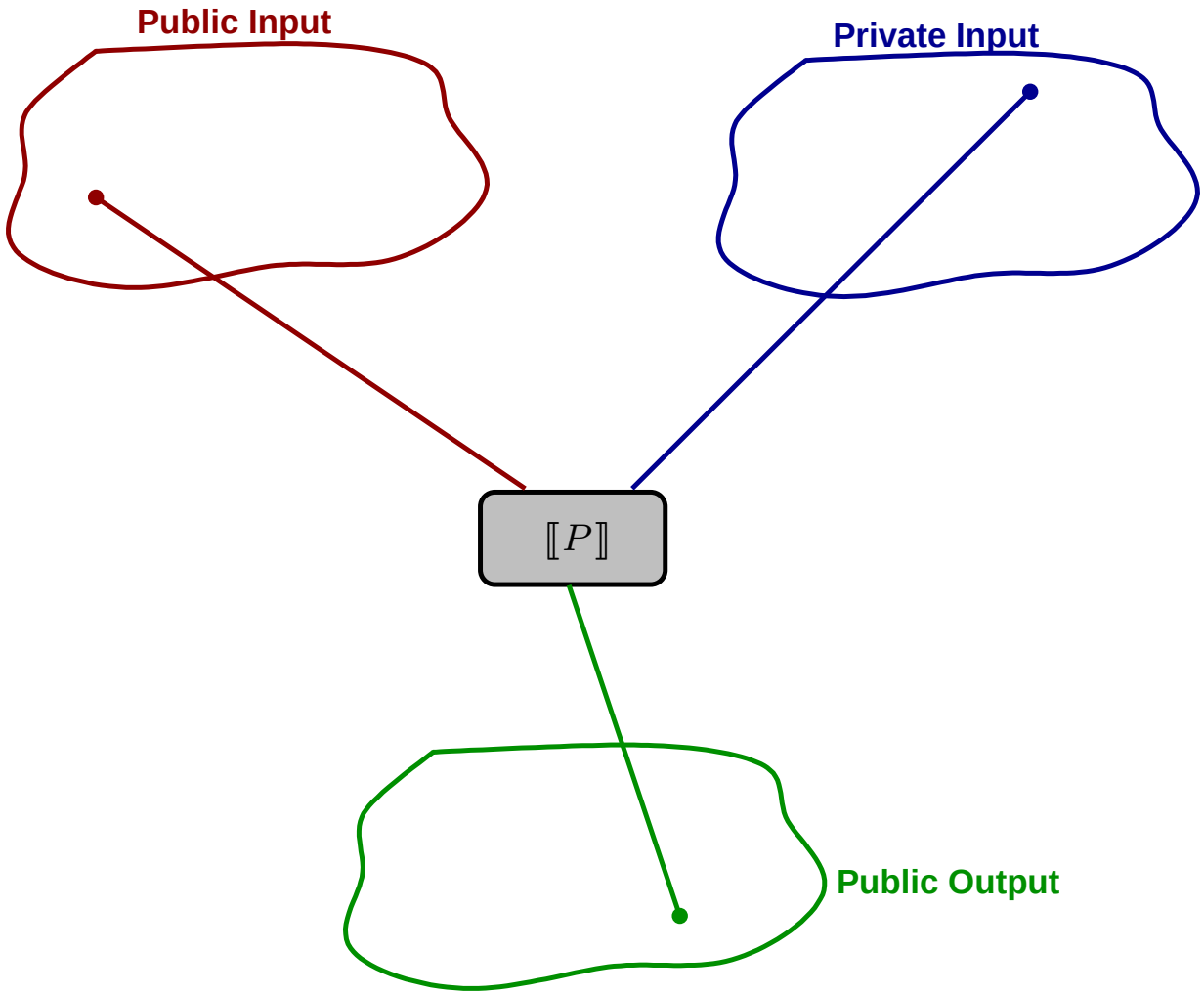
$$\forall l : \mathsf{L}, \forall h_1, h_2 : \mathsf{H}.\ [\![P]\!](h_1, l)^{\mathsf{L}} = [\![P]\!](h_2, l)^{\mathsf{L}}$$

STANDARD NON-INTERFERENCE



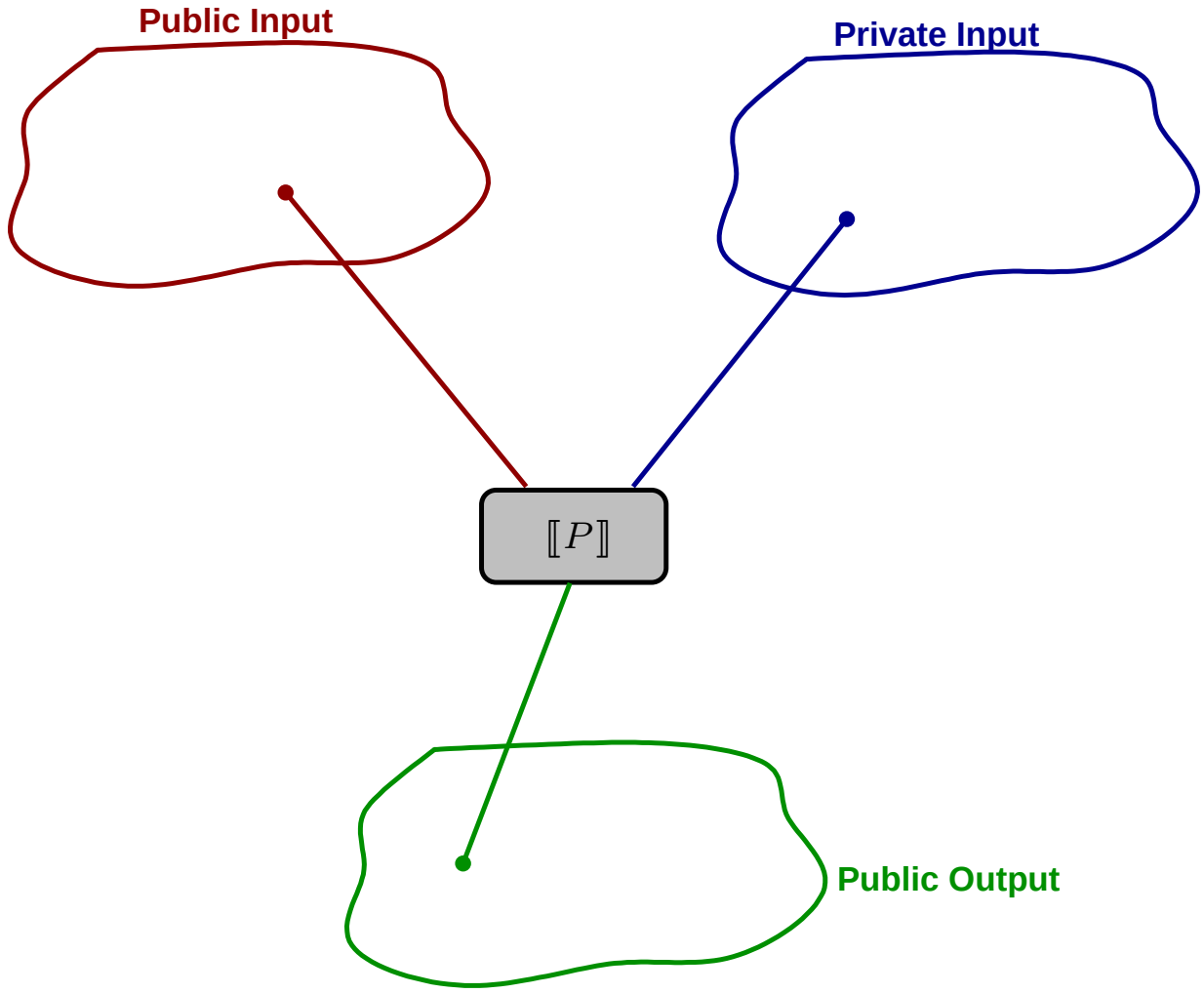
$$\forall l : \mathsf{L}, \forall h_1, h_2 : \mathsf{H}.\ [\![P]\!](h_1, l)^{\mathsf{L}} = [\![P]\!](h_2, l)^{\mathsf{L}}$$

STANDARD NON-INTERFERENCE



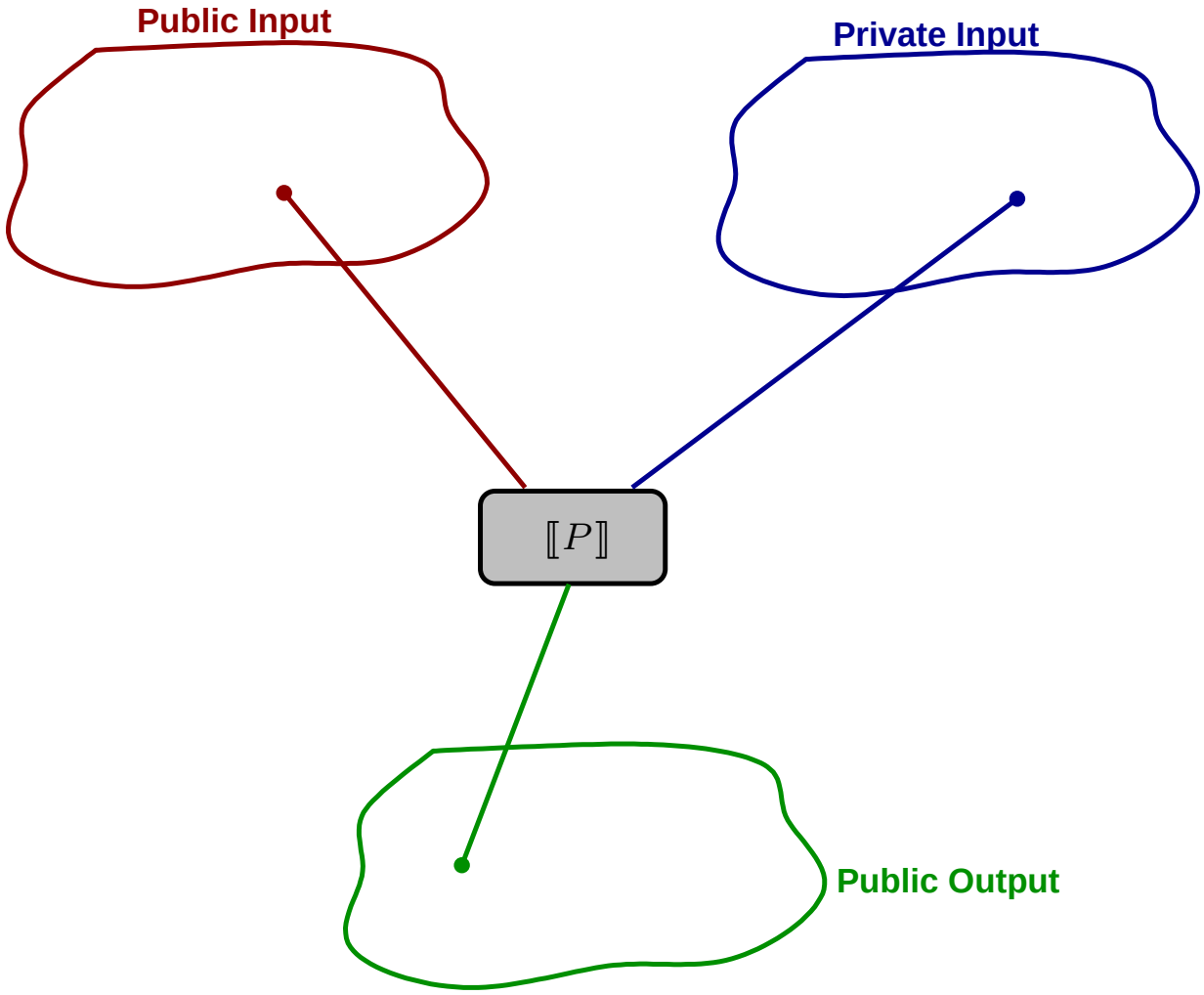
$$\forall l : \mathsf{L}, \forall h_1, h_2 : \mathsf{H}.\ [\![P]\!](h_1, l)^{\mathsf{L}} = [\![P]\!](h_2, l)^{\mathsf{L}}$$

STANDARD NON-INTERFERENCE



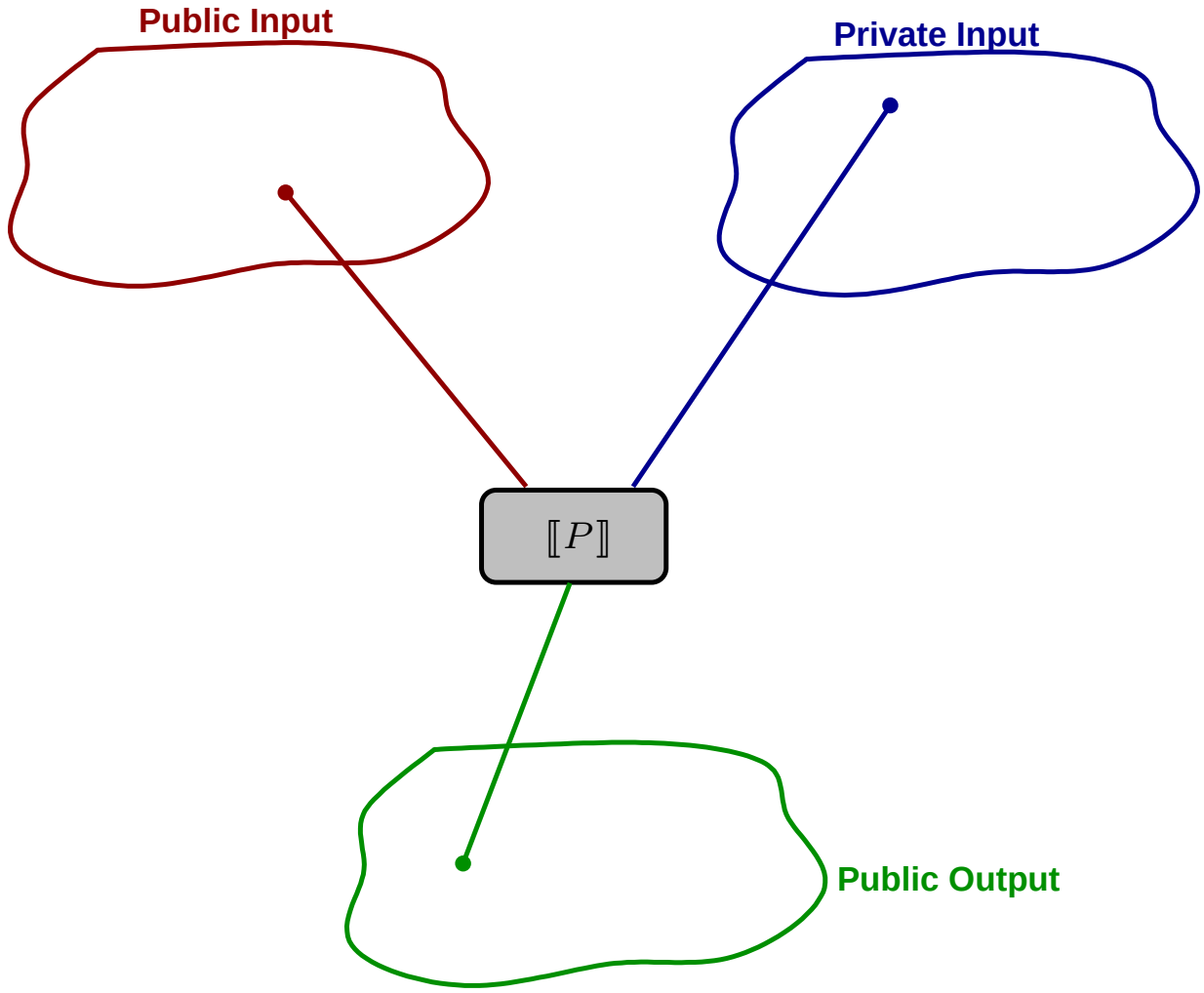
$$\forall l : \mathsf{L}, \forall h_1, h_2 : \mathsf{H}.\ [\![P]\!](h_1, l)^{\mathsf{L}} = [\![P]\!](h_2, l)^{\mathsf{L}}$$

STANDARD NON-INTERFERENCE



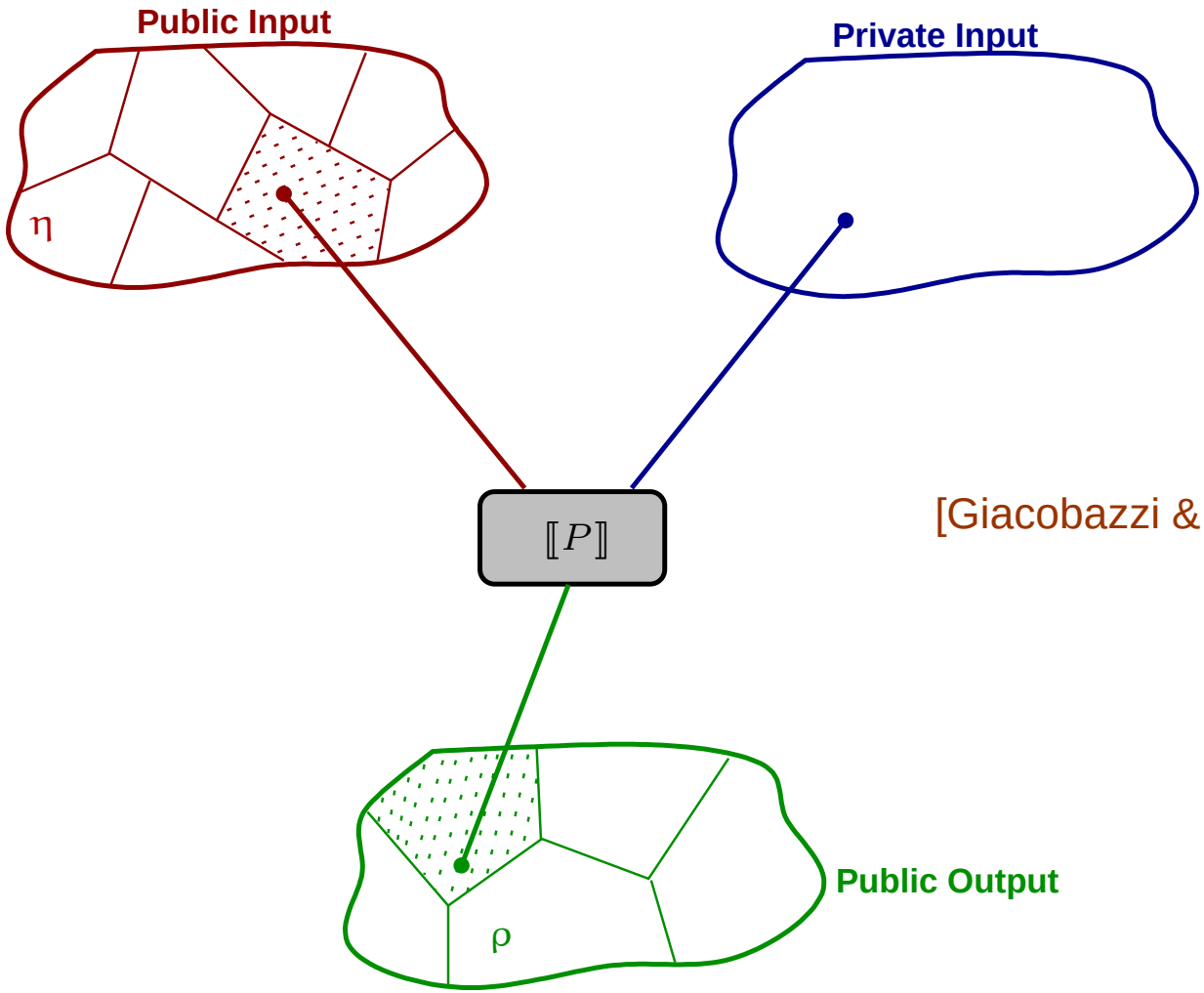
$$\forall l : \mathsf{L}, \forall h_1, h_2 : \mathsf{H}.\ [\![P]\!](h_1, l)^{\mathsf{L}} = [\![P]\!](h_2, l)^{\mathsf{L}}$$

STANDARD NON-INTERFERENCE



$$\forall l : \mathsf{L}, \forall h_1, h_2 : \mathsf{H}.\ [\![P]\!](h_1, l)^{\mathsf{L}} = [\![P]\!](h_2, l)^{\mathsf{L}}$$

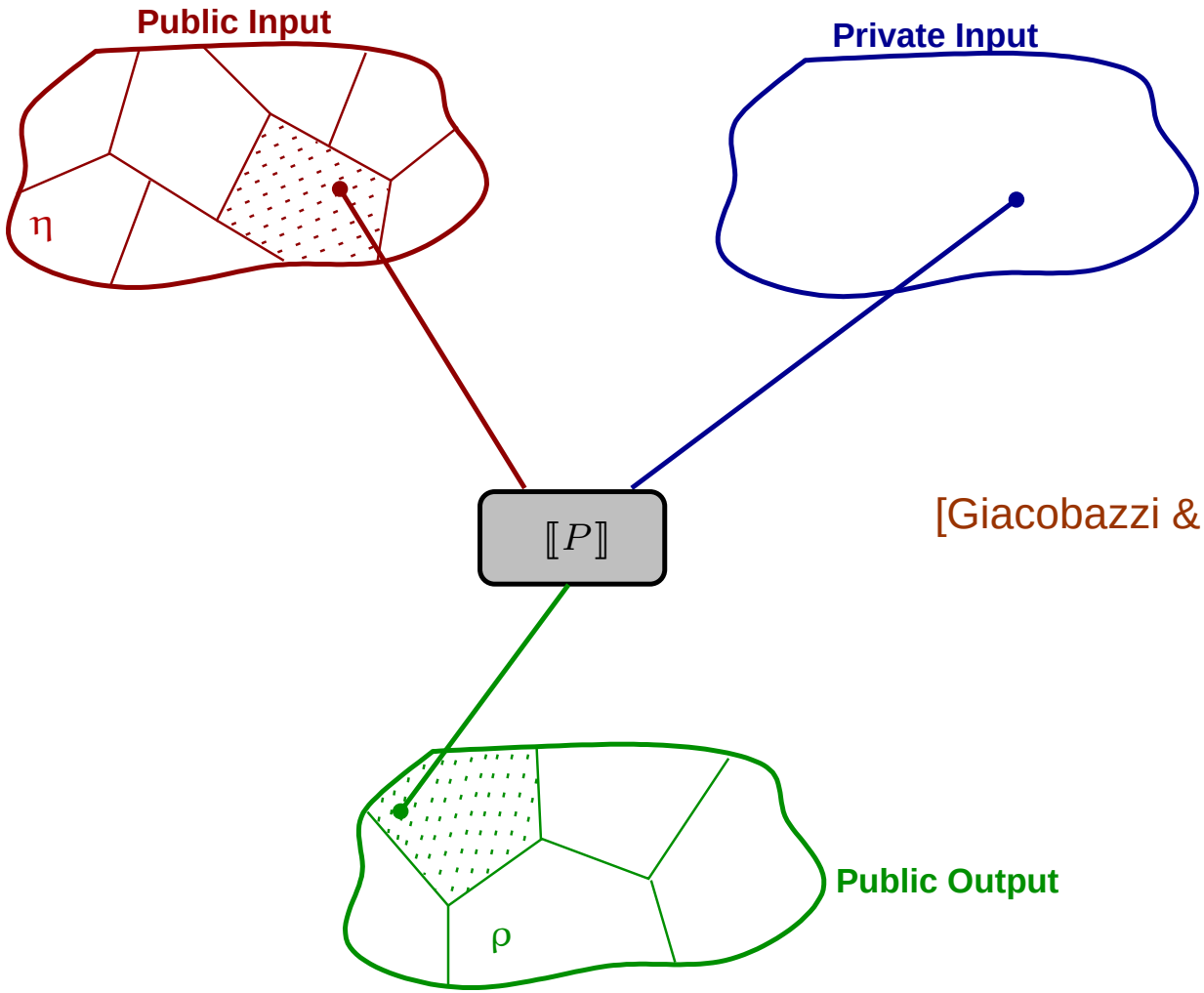
ABSTRACT NON-INTERFERENCE (NARROW)



[Giacobazzi & Mastroeni '04]

$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}}))$: $[\eta]P(\rho)$: $\eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket P \rrbracket(h_1, l_1)^{\mathsf{L}}) = \rho(\llbracket P \rrbracket(h_2, l_2)^{\mathsf{L}})$

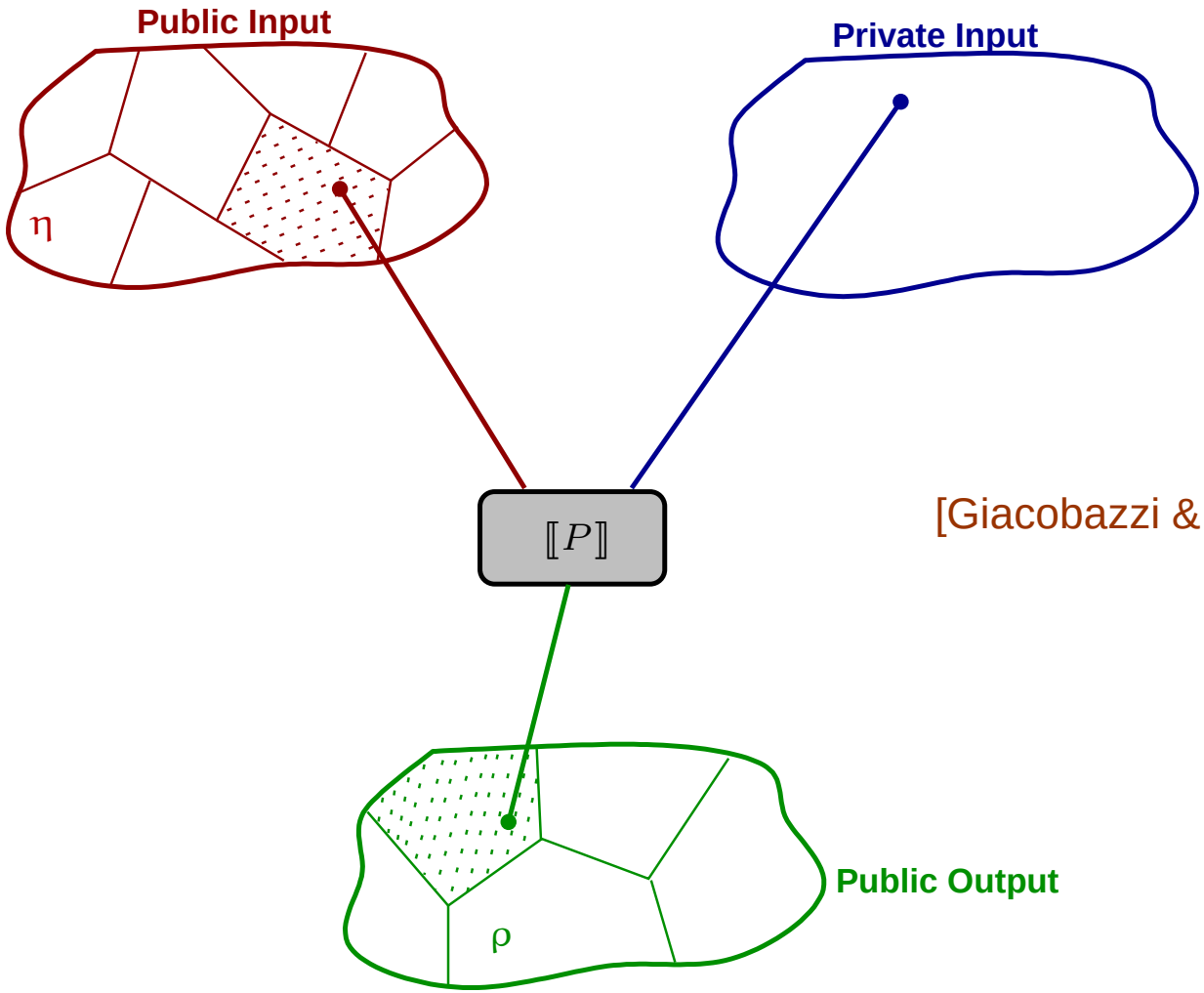
ABSTRACT NON-INTERFERENCE (NARROW)



[Giacobazzi & Mastroeni '04]

$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}}))$: $[\eta]P(\rho)$: $\eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket P \rrbracket(h_1, l_1)^{\mathsf{L}}) = \rho(\llbracket P \rrbracket(h_2, l_2)^{\mathsf{L}})$

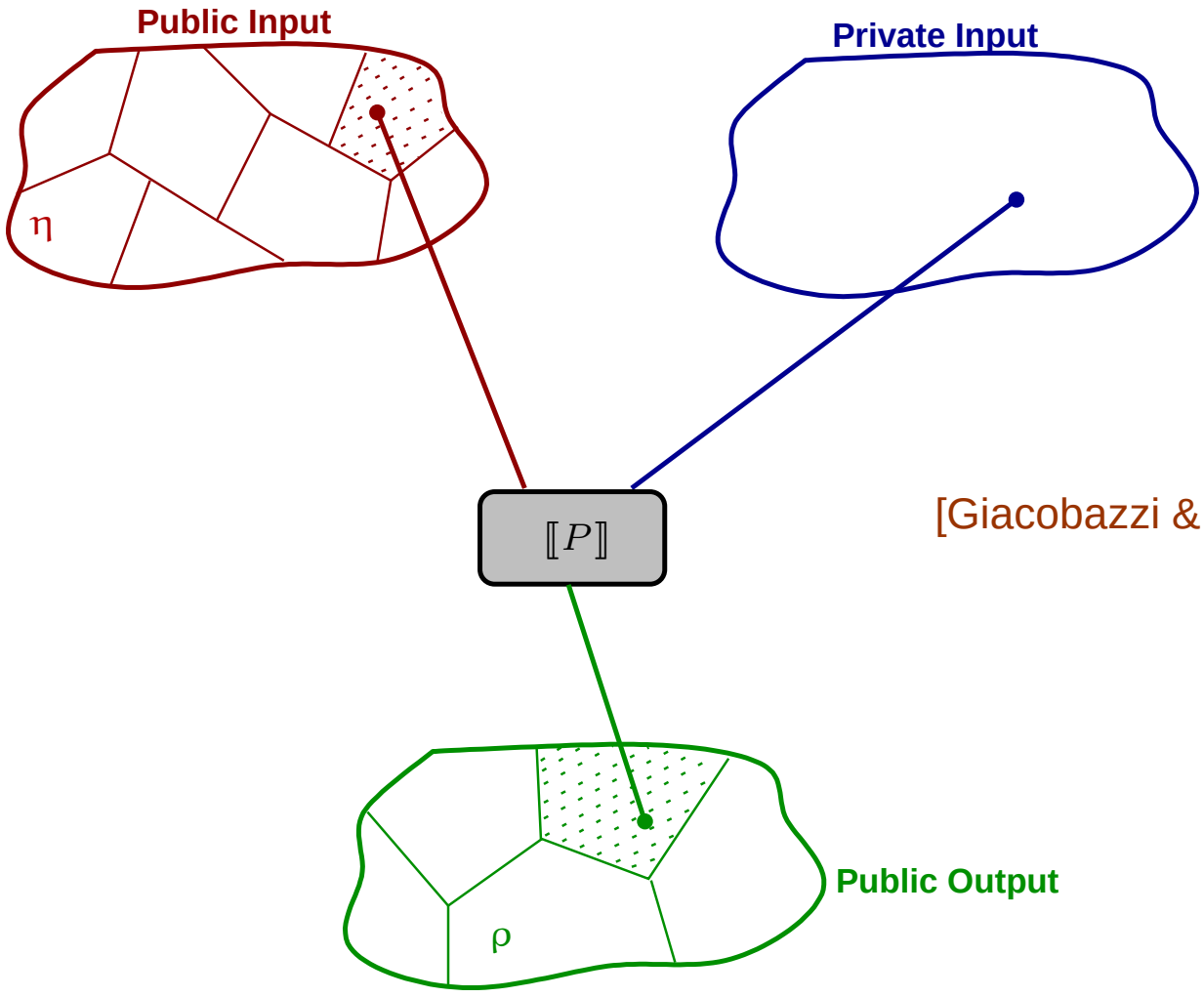
ABSTRACT NON-INTERFERENCE (NARROW)



[Giacobazzi & Mastroeni '04]

$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}}))$: $[\eta]P(\rho)$: $\eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket P \rrbracket(h_1, l_1)^{\mathsf{L}}) = \rho(\llbracket P \rrbracket(h_2, l_2)^{\mathsf{L}})$

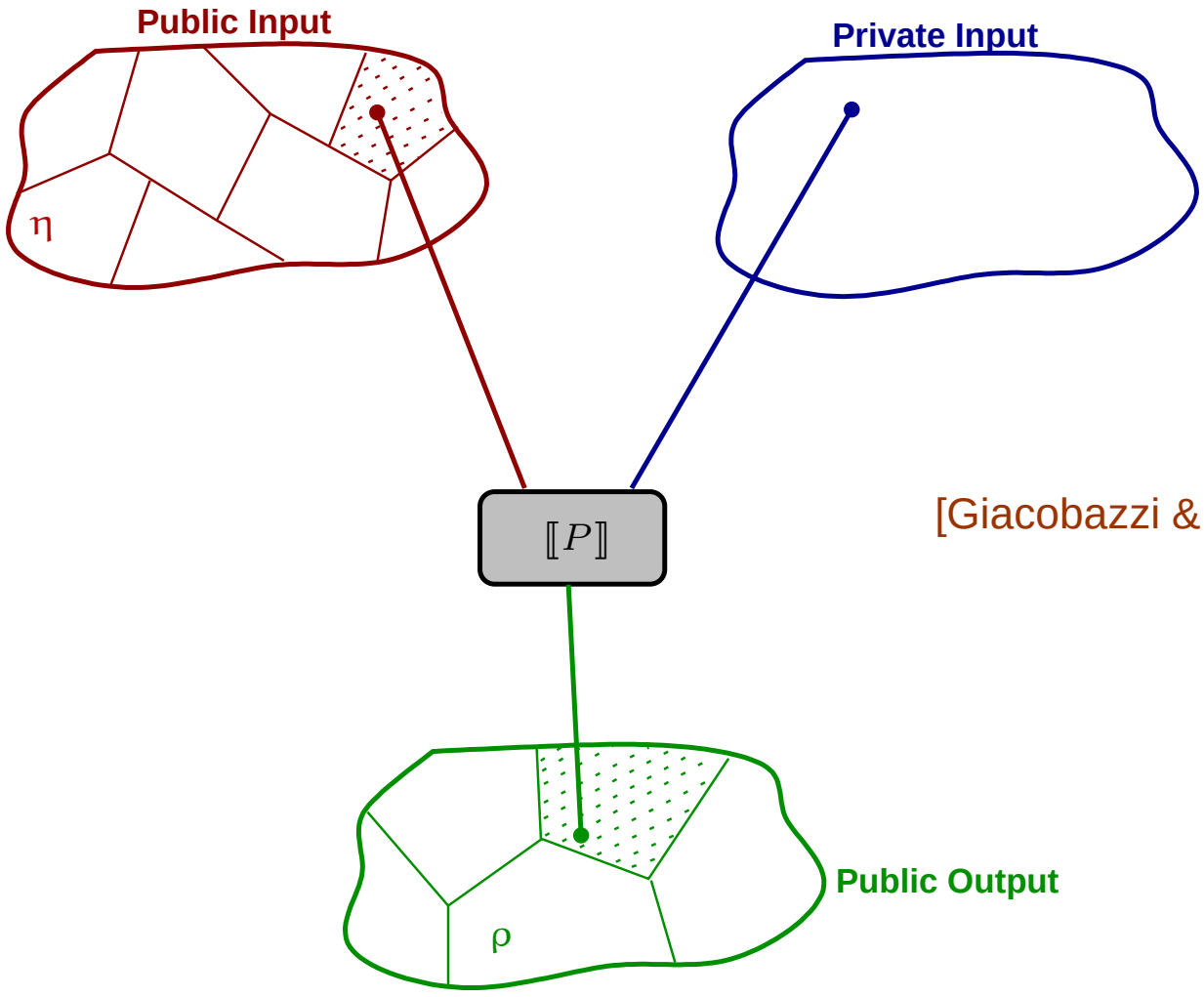
ABSTRACT NON-INTERFERENCE (NARROW)



[Giacobazzi & Mastroeni '04]

$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}}))$: $[\eta]P(\rho)$: $\eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket P \rrbracket(h_1, l_1)^{\mathsf{L}}) = \rho(\llbracket P \rrbracket(h_2, l_2)^{\mathsf{L}})$

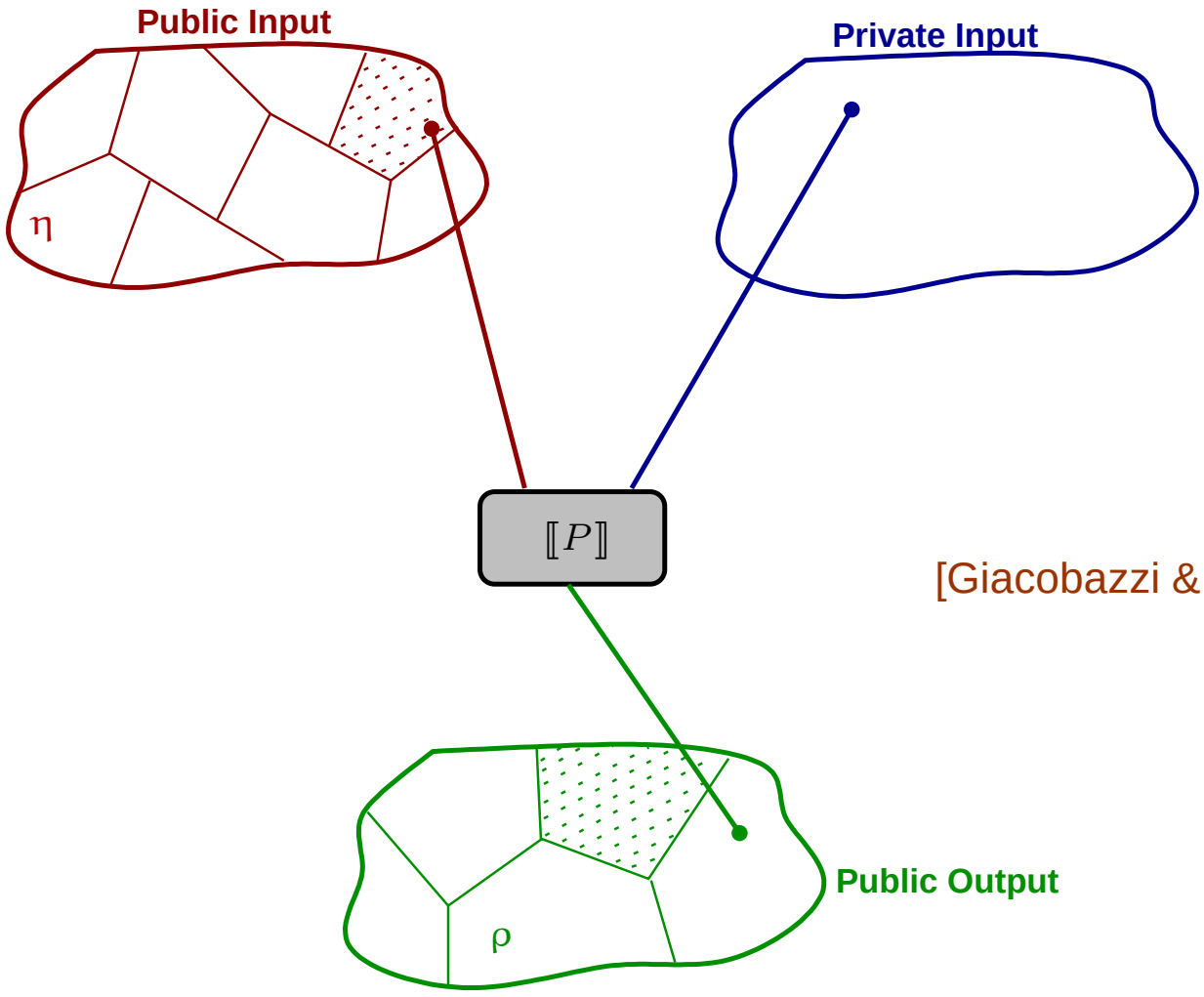
ABSTRACT NON-INTERFERENCE (NARROW)



[Giacobazzi & Mastroeni '04]

$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}}))$: $[\eta]P(\rho)$: $\eta(l_1) = \eta(l_2) \Rightarrow \rho([\![P]\!](h_1, l_1)^{\mathsf{L}}) = \rho([\![P]\!](h_2, l_2)^{\mathsf{L}})$

ABSTRACT NON-INTERFERENCE (NARROW)

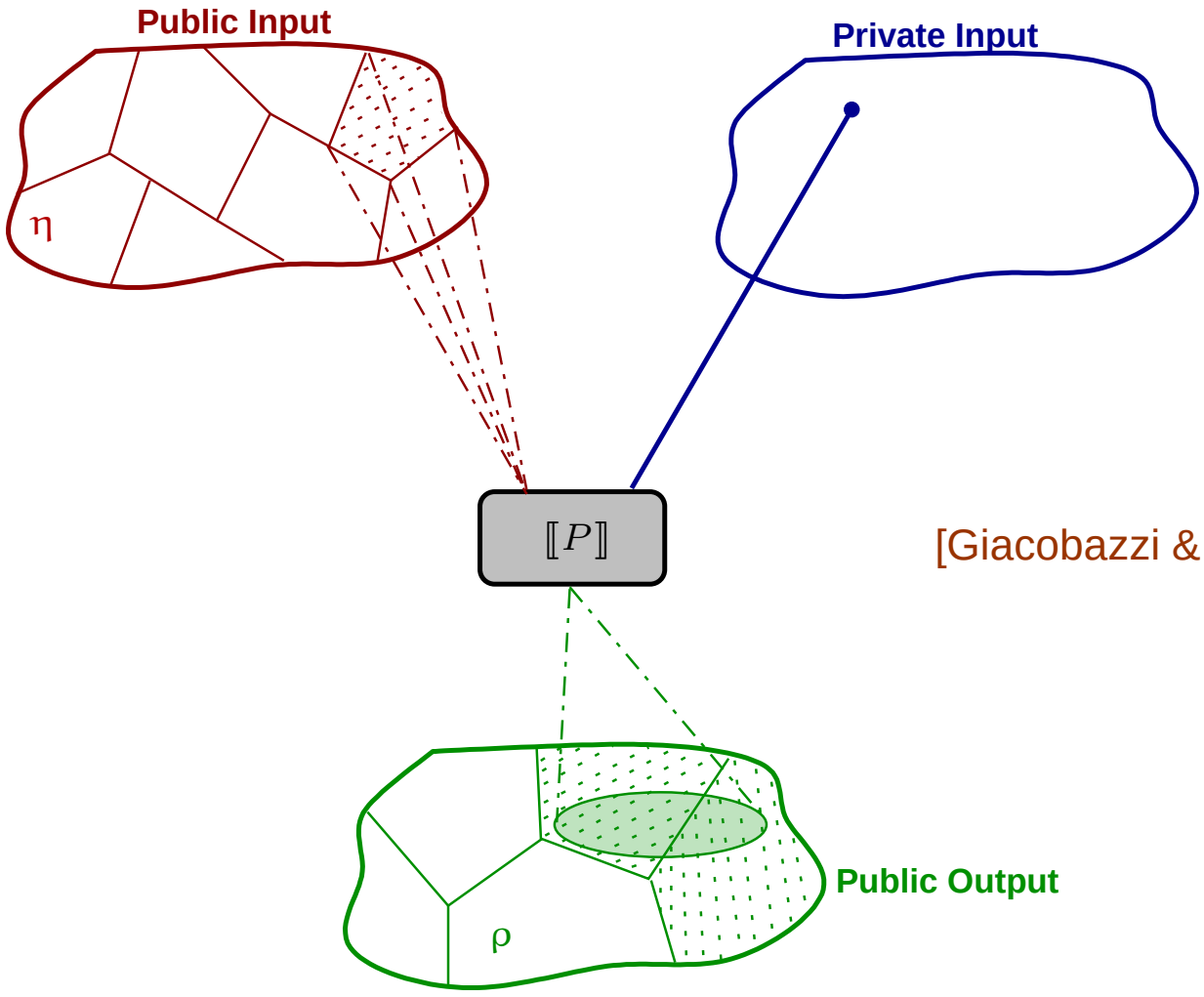


[Giacobazzi & Mastroeni '04]

Deceptive flow!!

$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}}))$: $[\eta]P(\rho)$: $\eta(l_1) = \eta(l_2) \Rightarrow \rho([\![P]\!](h_1, l_1)^{\mathsf{L}}) = \rho([\![P]\!](h_2, l_2)^{\mathsf{L}})$

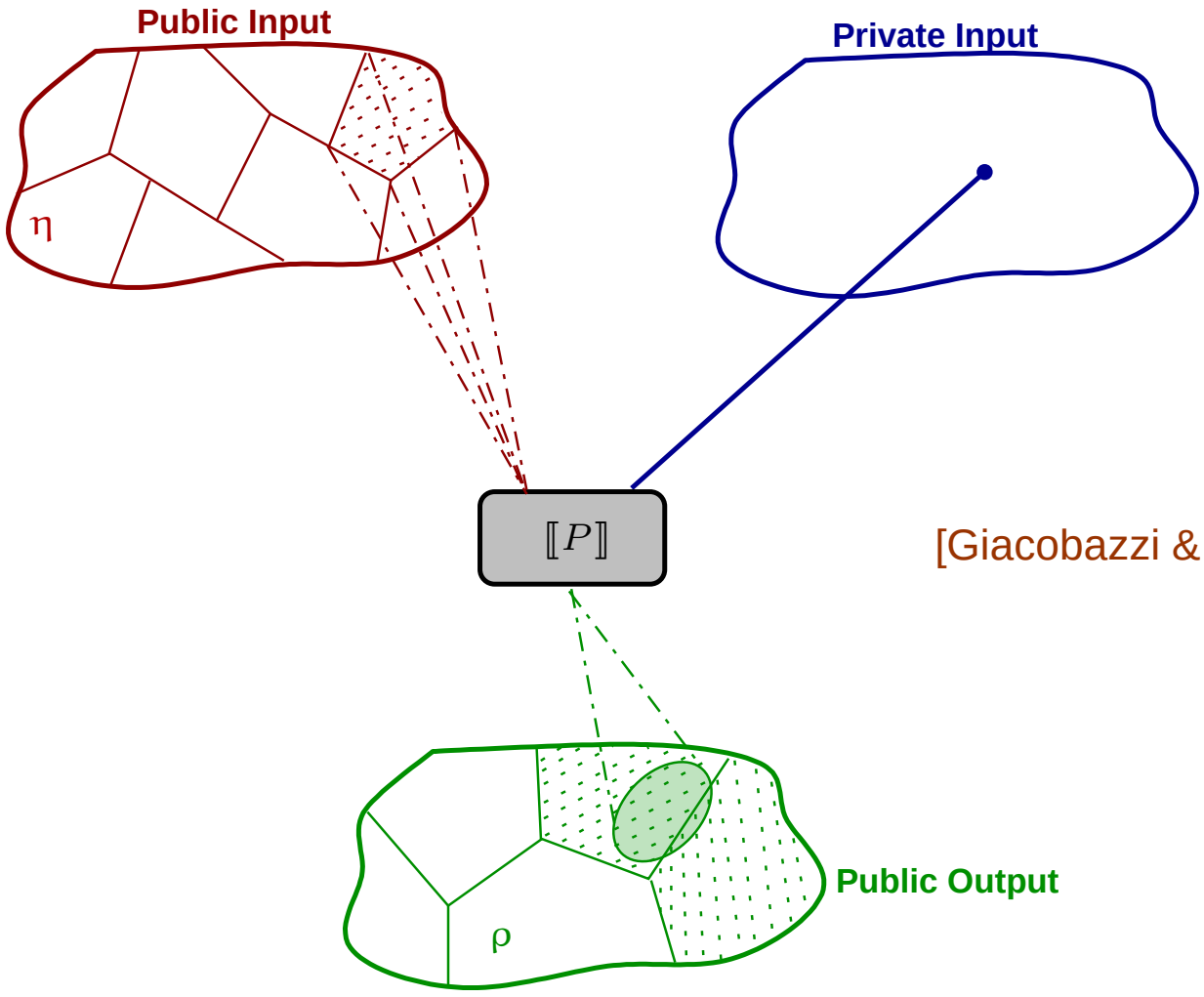
ABSTRACT NON-INTERFERENCE (ANI)



[Giacobazzi & Mastroeni '04]

$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})) \colon (\eta)P(\rho) \colon$$
$$\eta(l_1) = \eta(l_2) \Rightarrow \rho([\![P]\!](h_1, \eta(l_1))^{\mathsf{L}}) = \rho([\![P]\!](h_2, \eta(l_2))^{\mathsf{L}})$$

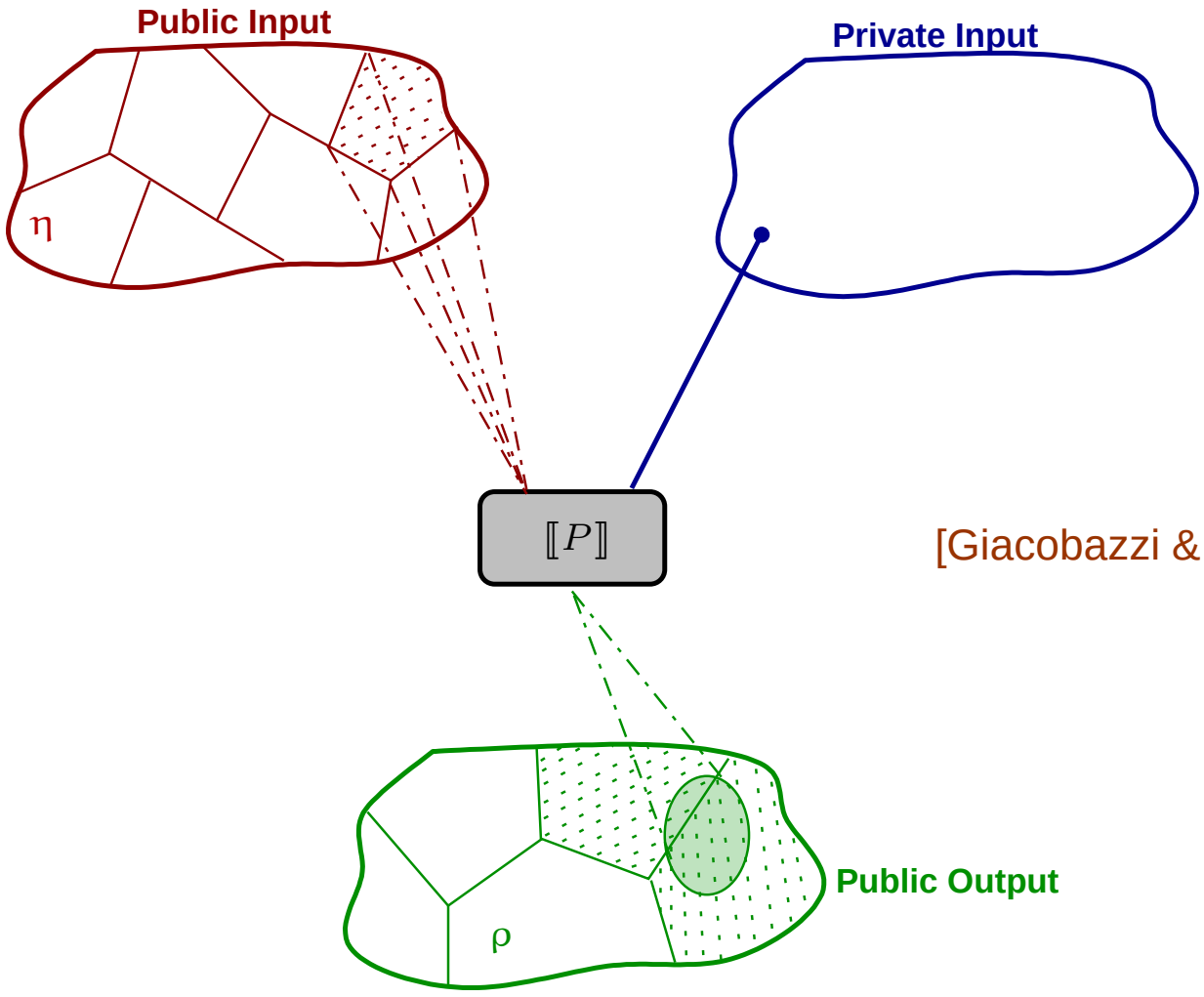
ABSTRACT NON-INTERFERENCE (ANI)



[Giacobazzi & Mastroeni '04]

$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})) \colon (\eta)P(\rho) \colon$$
$$\eta(l_1) = \eta(l_2) \Rightarrow \rho([\![P]\!](h_1, \eta(l_1))^{\mathsf{L}}) = \rho([\![P]\!](h_2, \eta(l_2))^{\mathsf{L}})$$

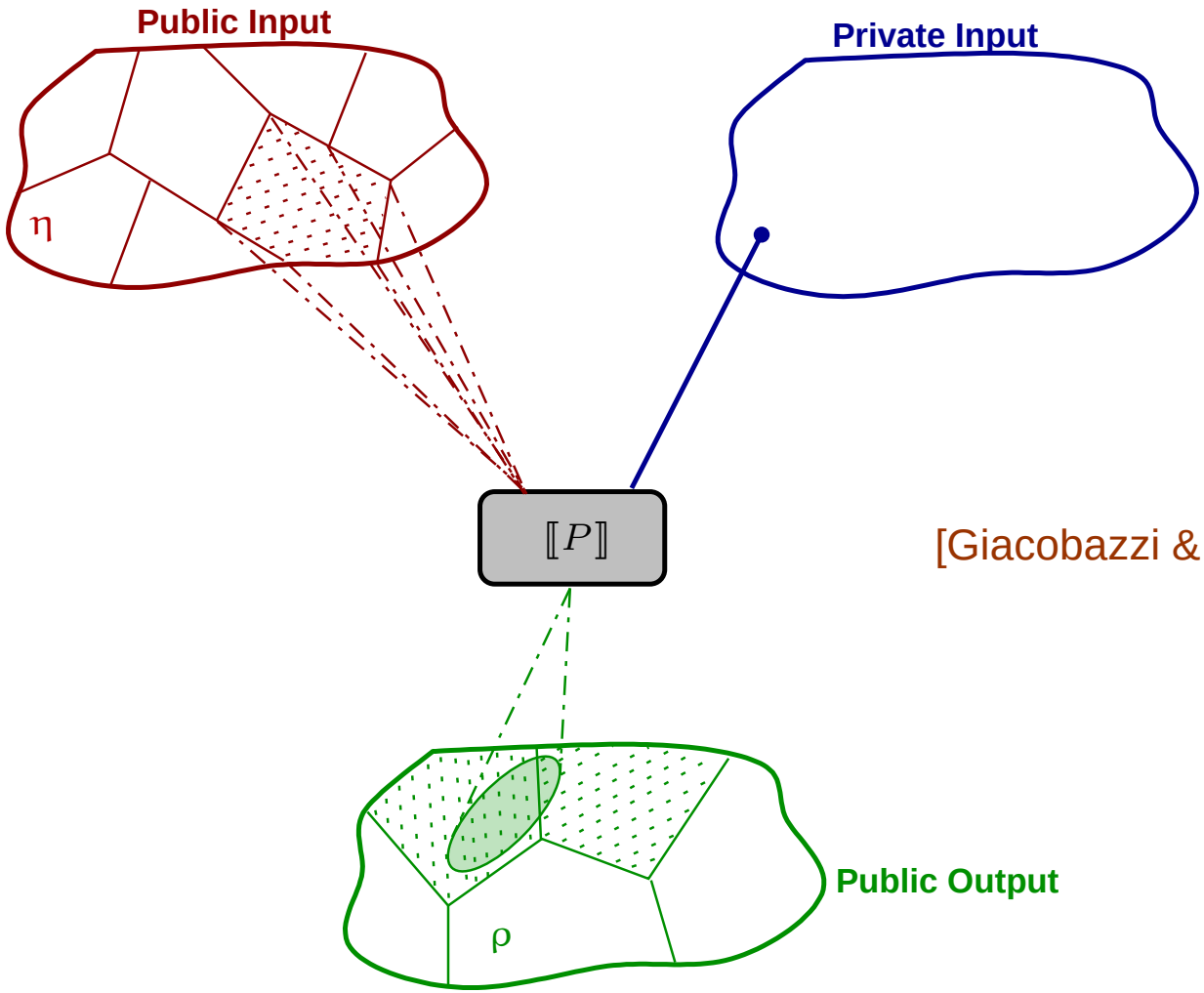
ABSTRACT NON-INTERFERENCE (ANI)



[Giacobazzi & Mastroeni '04]

$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})):\ (\eta)P(\rho):$$
$$\eta(l_1) = \eta(l_2) \Rightarrow \rho([\![P]\!](h_1, \eta(l_1))^{\mathsf{L}}) = \rho([\![P]\!](h_2, \eta(l_2))^{\mathsf{L}})$$

ABSTRACT NON-INTERFERENCE (ANI)

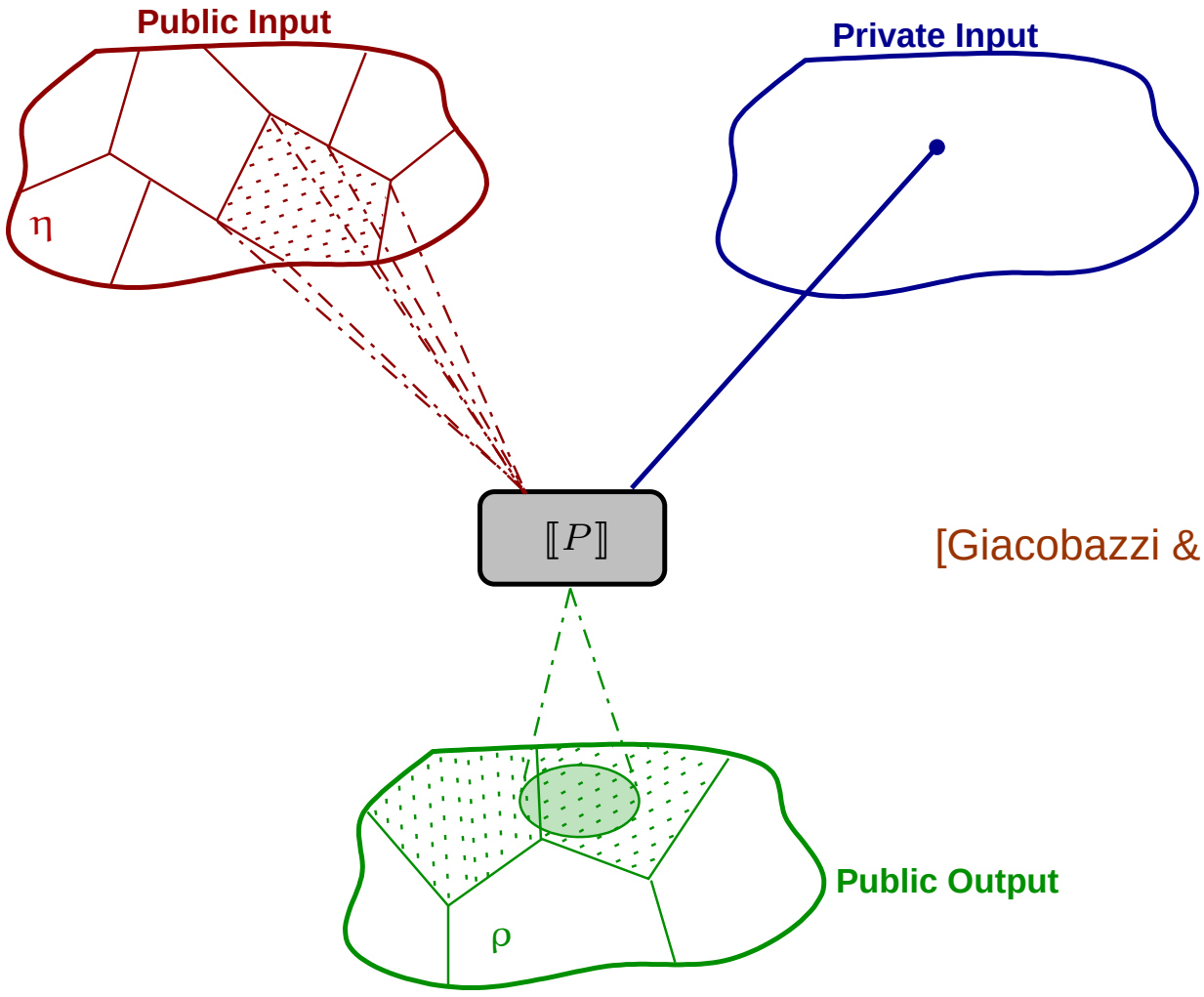


[Giacobazzi & Mastroeni '04]

$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}}))$: $(\eta)P(\rho)$:

$\eta(l_1) = \eta(l_2) \Rightarrow \rho([\![P]\!](h_1, \eta(l_1))^{\mathsf{L}}) = \rho([\![P]\!](h_2, \eta(l_2))^{\mathsf{L}})$

ABSTRACT NON-INTERFERENCE (ANI)



[Giacobazzi & Mastroeni '04]

$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})) \colon (\eta)P(\rho) \colon$$

$$\eta(l_1) = \eta(l_2) \Rightarrow \rho([\![P]\!](h_1, \eta(l_1))^{\mathsf{L}}) = \rho([\![P]\!](h_2, \eta(l_2))^{\mathsf{L}})$$

EXAMPLES

EXAMPLE I:

$$\textbf{while } h \textbf{ do } (l := l + 2;\ h := h - 1).$$

$$\boxed{\text{Standard Non-Interference} \equiv\ [id]P(id)}$$

$$h = 0,\ l = 1 \ \rightsquigarrow\ l = 1$$
$$h = 1,\ l = 1 \ \rightsquigarrow\ l = 3$$
$$h = n,\ l = 1 \ \rightsquigarrow\ l = 1 + 2n$$

EXAMPLE I:

while h **do** $(l := l + 2;\ h := h - 1)$.

$$\boxed{\text{Standard Non-Interference} \equiv\ [id]P(id)}$$

$$h = 0,\ l = 1 \ \rightsquigarrow\ l = 1$$
$$h = 1,\ l = 1 \ \rightsquigarrow\ l = 3$$
$$h = n,\ l = 1 \ \rightsquigarrow\ l = 1 + 2n$$

$$\Downarrow$$

$$\boxed{[id]P(Par)}$$

$$h = 0,\ l = 1 \ \rightsquigarrow\ Par(l) = \text{odd}$$
$$h = 1,\ l = 1 \ \rightsquigarrow\ Par(l) = \text{odd}$$
$$h = n,\ l = 1 \ \rightsquigarrow\ Par(l) = \text{odd}$$

EXAMPLE II (DECEPTIVE FLOW):

$$P = \quad l := 2 * l * h^2.$$

$$\boxed{[Par]P(Sign)}$$

$$h = 1,\ l = 4\ (Par(4) = \text{even}) \rightsquigarrow Sign(l) = +$$
$$h = 1,\ l = -4\ (Par(-4) = \text{even}) \rightsquigarrow Sign(l) = -$$

EXAMPLE II:

$$P = \quad l := 2 * l * h^2.$$

$$\boxed{[Par]P(Sign)}$$

$$h = 1,\ l = 4\ (Par(4) = \text{even}) \rightsquigarrow Sign(l) = +$$
$$h = 1,\ l = -4\ (Par(-4) = \text{even}) \rightsquigarrow Sign(l) = -$$

$$\boxed{(Par)P(Sign)}$$

$$h = -3,\ Par(l) = \text{even} \rightsquigarrow Sign(l) = \text{I don't know}$$
$$h = 1,\ Par(l) = \text{even} \rightsquigarrow Sign(l) = \text{I don't know}$$

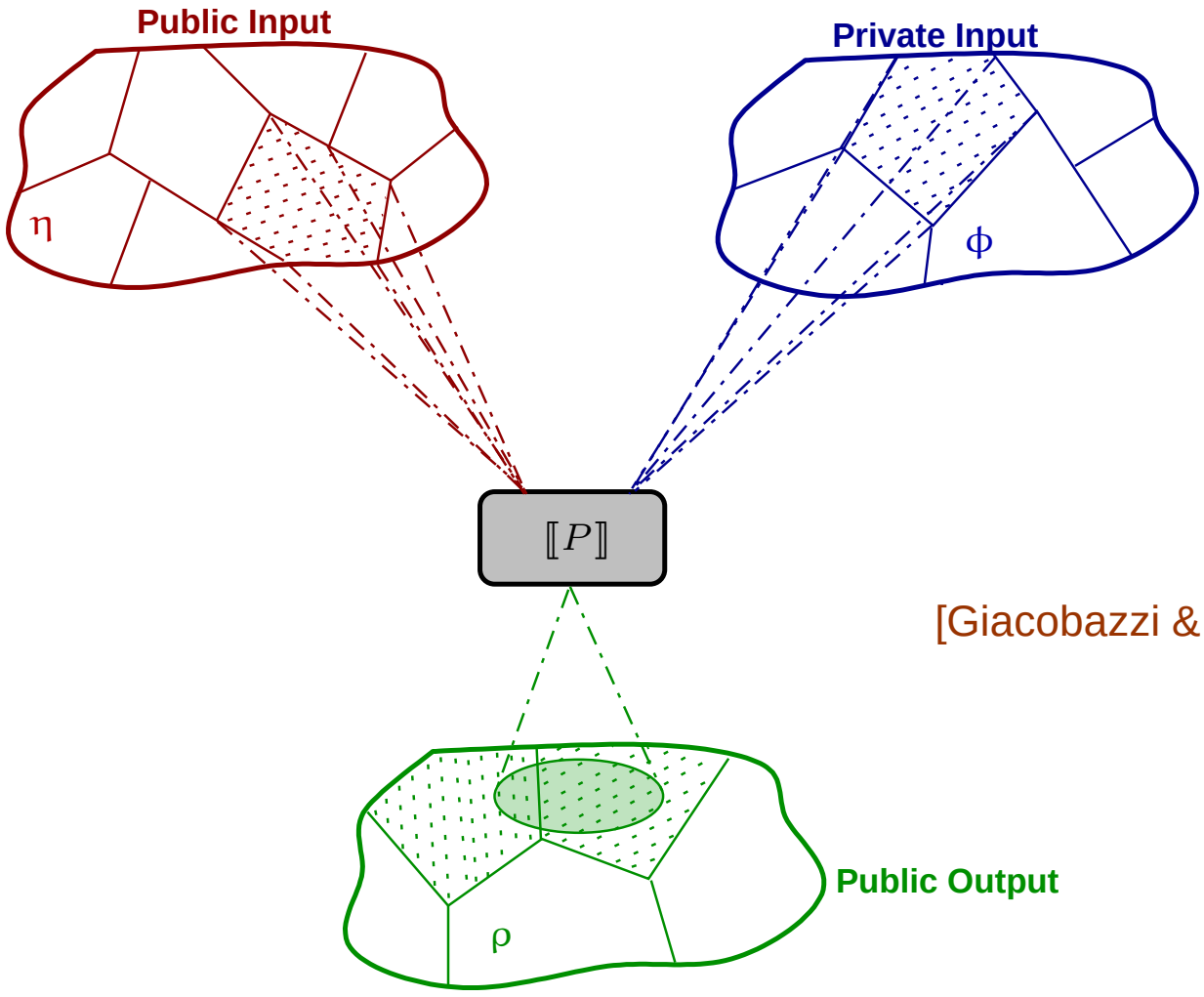
EXAMPLE III:

$$P = \quad l := l * h^2.$$

$$\boxed{(id)P(Par)}$$

$$h = 2,\ l = 1 \ \rightsquigarrow\ Par(l) = \text{even}$$
$$h = 3,\ l = 1 \ \rightsquigarrow\ Par(l) = \text{odd}$$
$$h = n,\ l = 1 \ \rightsquigarrow\ Par(l) = Par(n)$$

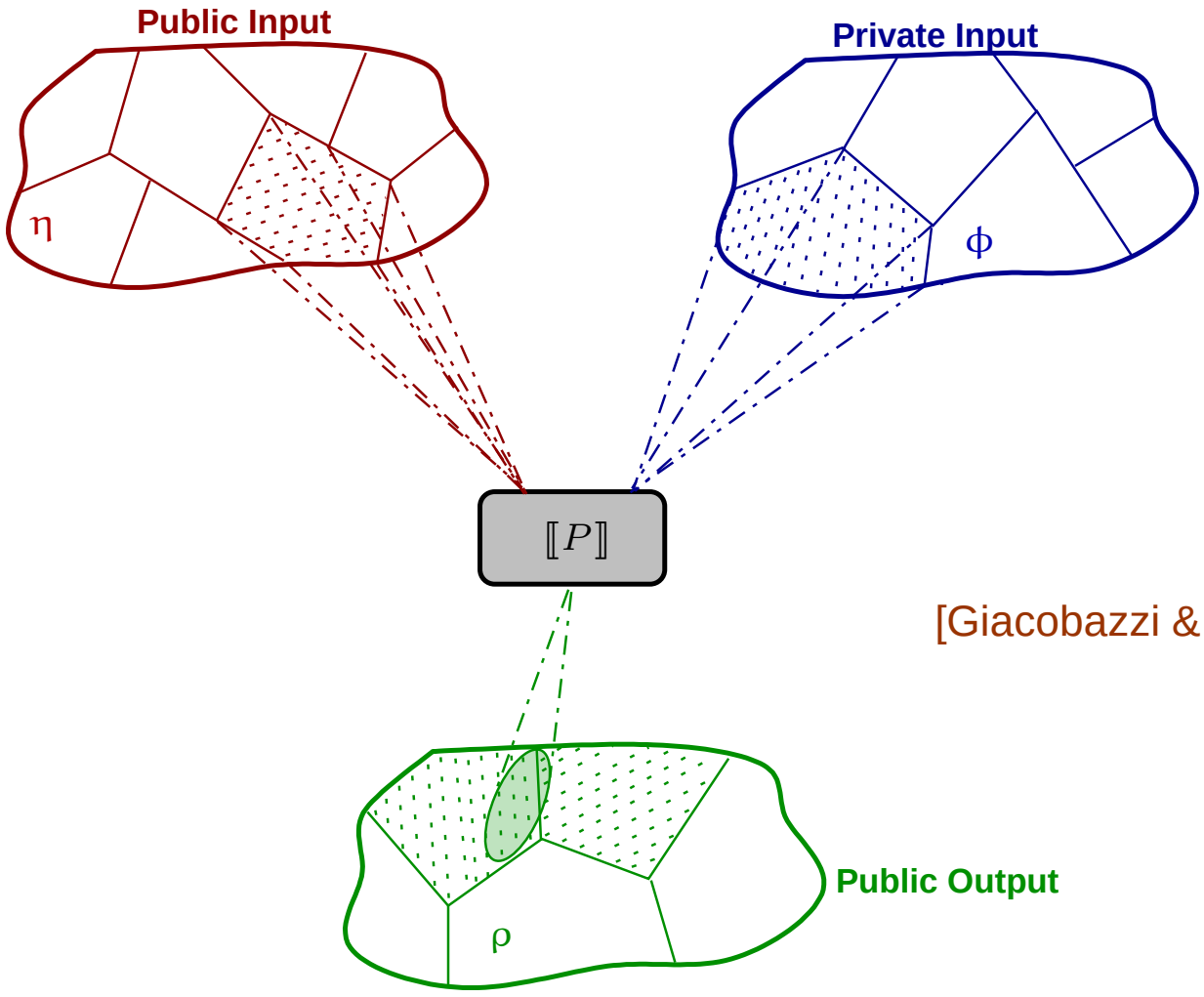
DECLASSIFIED ANI VIA BLOCKING



[Giacobazzi & Mastroeni '04]

$$\rho,\eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})),\phi \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{H}})):\ (\eta)P(\phi \rightsquigarrow \rho):$$
$$\eta(l_1)=\eta(l_2) \Rightarrow \rho([\![P]\!](\phi(h_1),\eta(l_1))^{\mathsf{L}})=\rho([\![P]\!](\phi(h_2),\eta(l_2))^{\mathsf{L}})$$

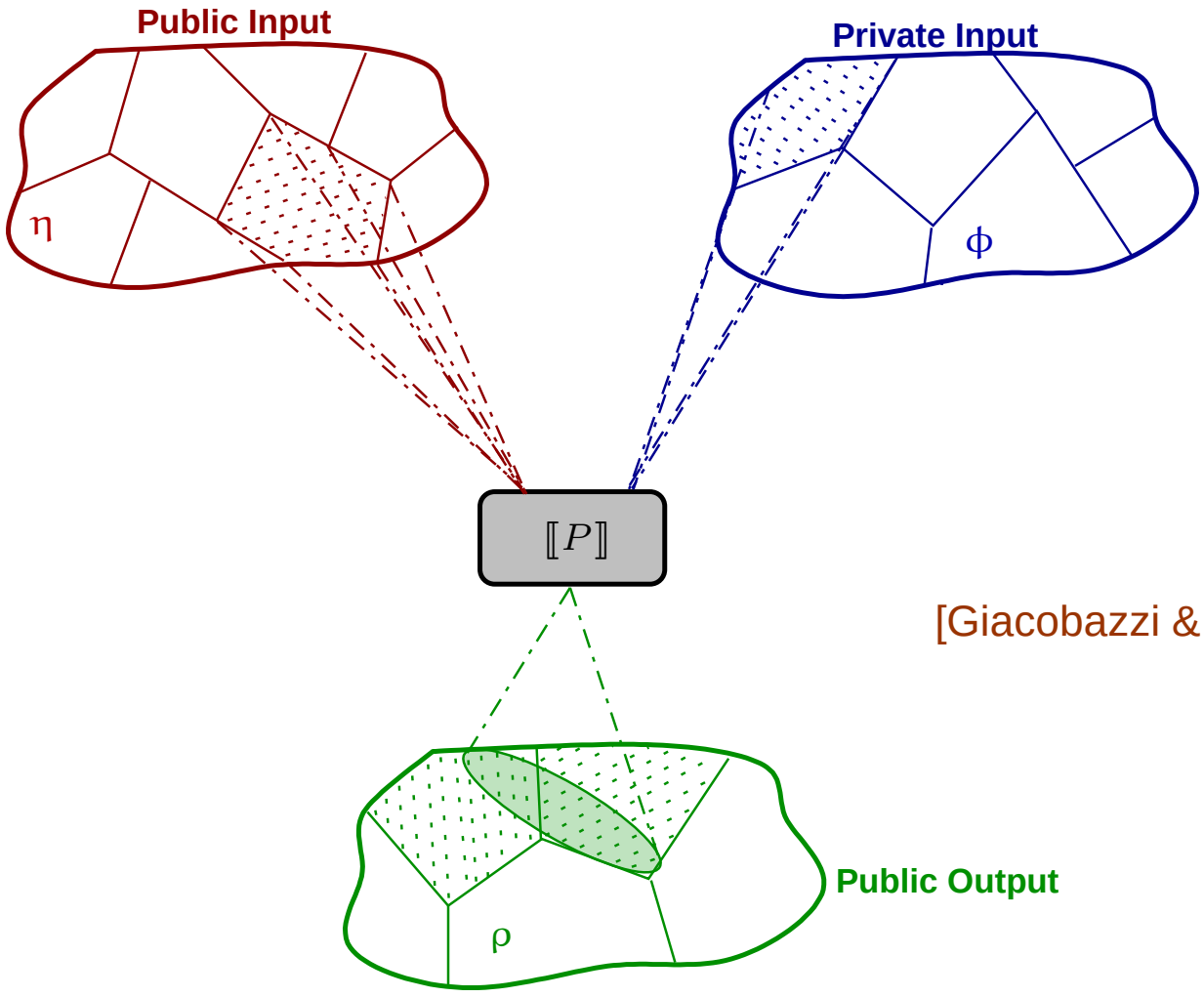
DECLASSIFIED ANI VIA BLOCKING



[Giacobazzi & Mastroeni '04]

$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})), \phi \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{H}})) \colon (\eta)P(\phi \rightsquigarrow \rho) \colon$$
$$\eta(l_1) = \eta(l_2) \Rightarrow \rho([\![P]\!](\phi(h_1), \eta(l_1))^{\mathsf{L}}) = \rho([\![P]\!](\phi(h_2), \eta(l_2))^{\mathsf{L}})$$

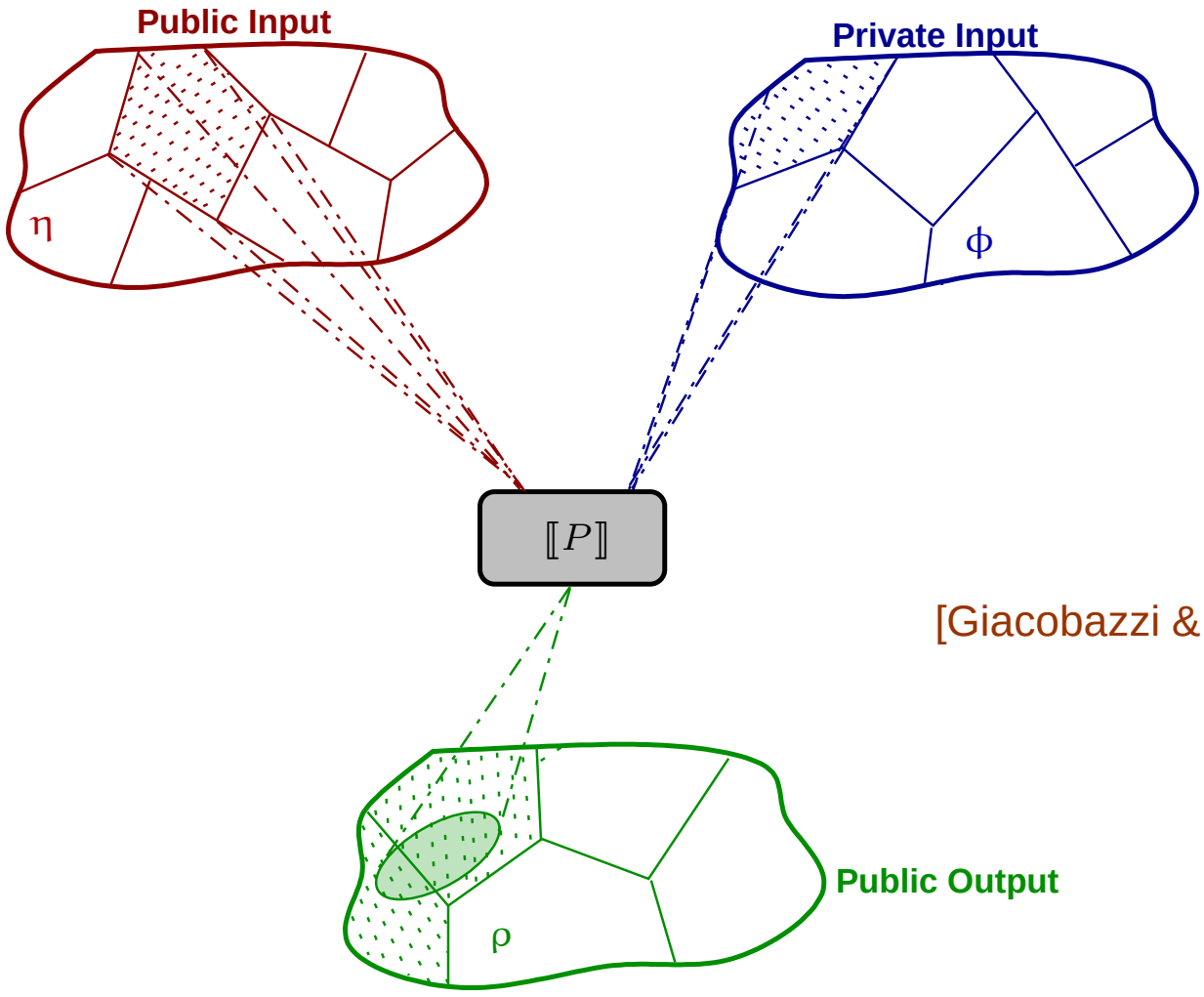
DECLASSIFIED ANI VIA BLOCKING



[Giacobazzi & Mastroeni '04]

$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})), \phi \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{H}})) \colon (\eta)P(\phi \rightsquigarrow \rho) \colon$$
$$\eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket P \rrbracket(\phi(h_1), \eta(l_1))^{\mathsf{L}}) = \rho(\llbracket P \rrbracket(\phi(h_2), \eta(l_2))^{\mathsf{L}})$$

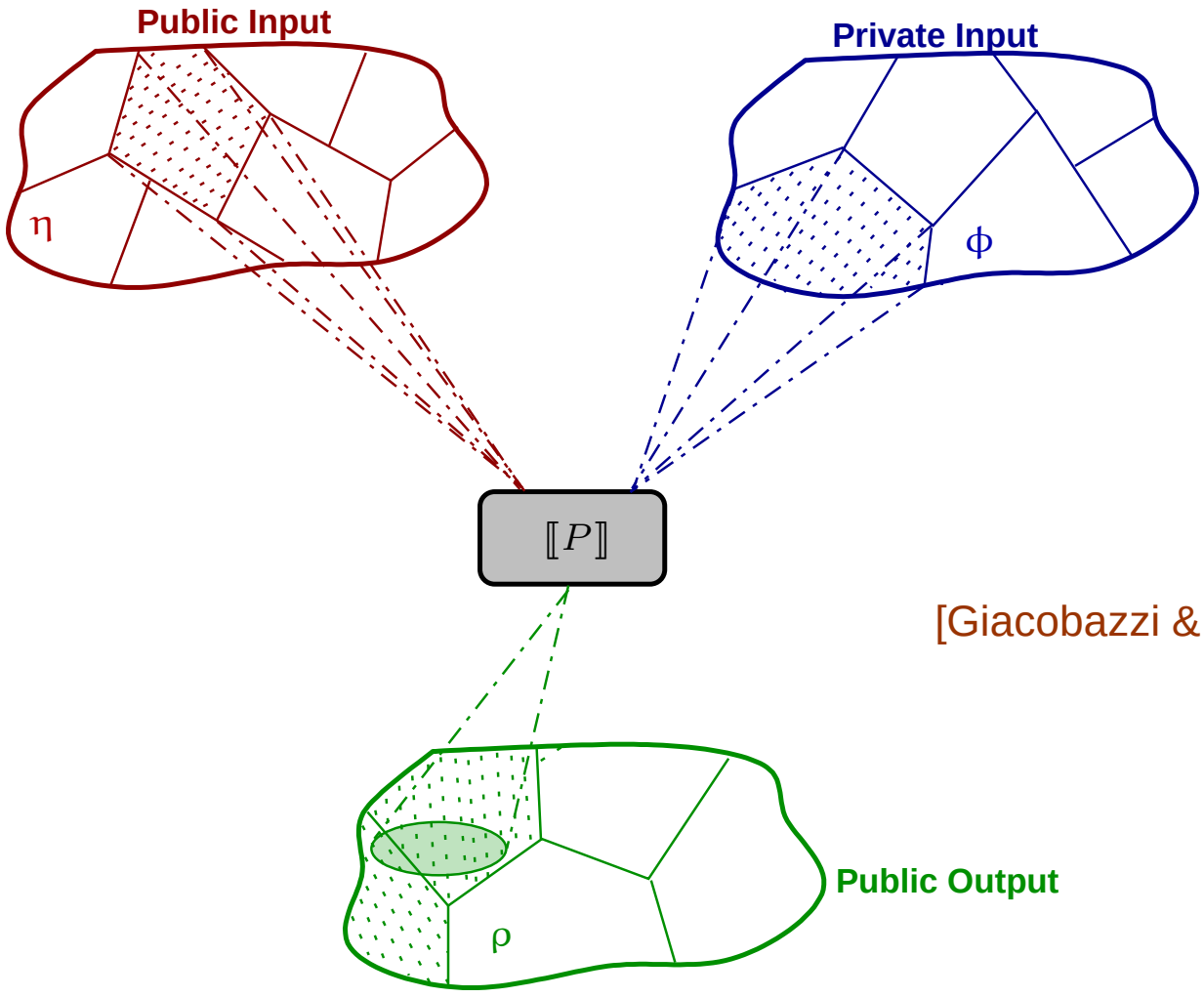
DECLASSIFIED ANI VIA BLOCKING



[Giacobazzi & Mastroeni '04]

$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})), \phi \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{H}})) \colon (\eta)P(\phi \rightsquigarrow \rho) \colon$$
$$\eta(l_1) = \eta(l_2) \Rightarrow \rho([\![P]\!](\phi(h_1), \eta(l_1))^{\mathsf{L}}) = \rho([\![P]\!](\phi(h_2), \eta(l_2))^{\mathsf{L}})$$

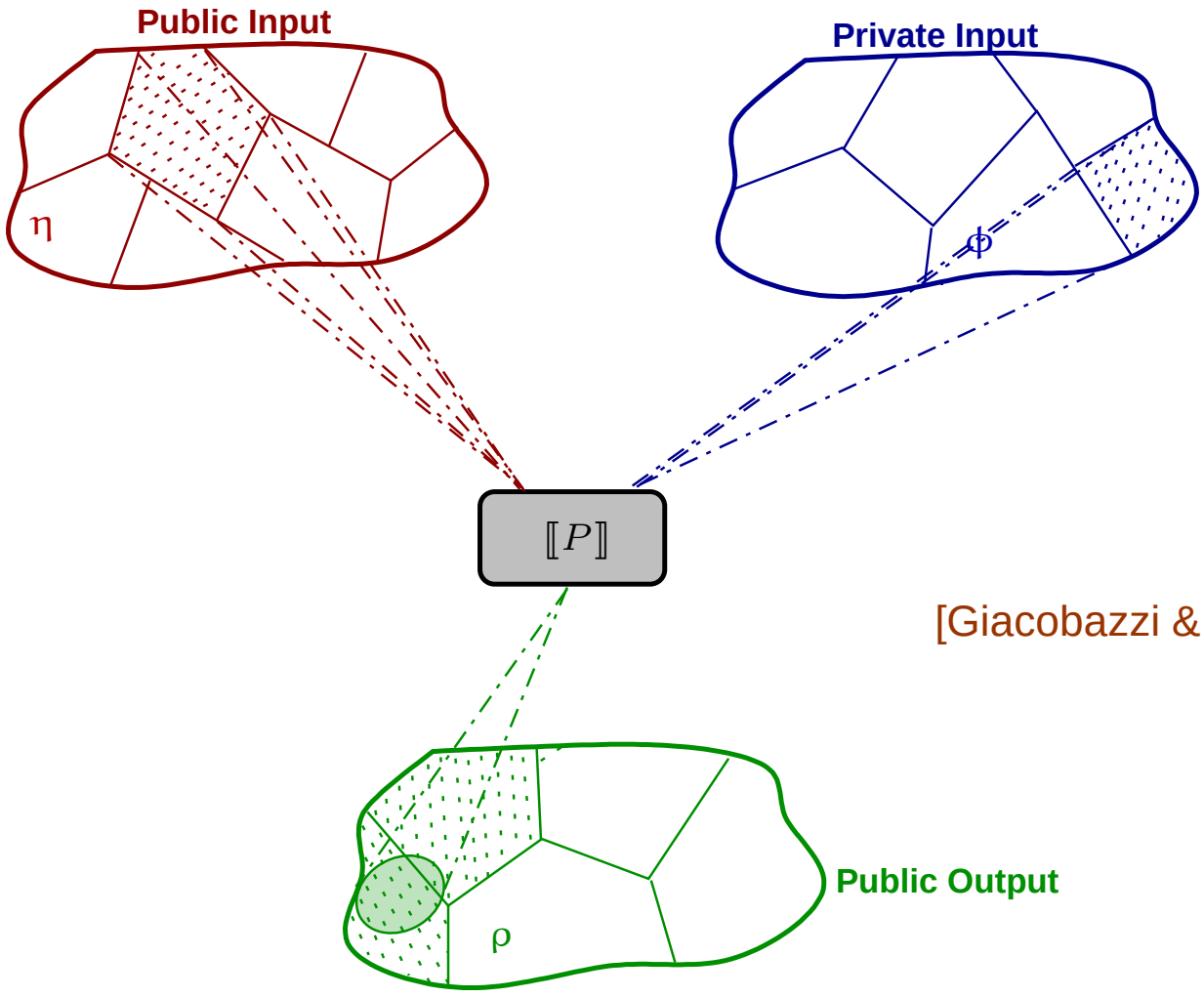
DECLASSIFIED ANI VIA BLOCKING



[Giacobazzi & Mastroeni '04]

$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})), \phi \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{H}})) \colon (\eta)P(\phi \rightsquigarrow \rho) \colon$$
$$\eta(l_1) = \eta(l_2) \Rightarrow \rho([\![P]\!](\phi(h_1), \eta(l_1))^{\mathsf{L}}) = \rho([\![P]\!](\phi(h_2), \eta(l_2))^{\mathsf{L}})$$

DECLASSIFIED ANI VIA BLOCKING



[Giacobazzi & Mastroeni '04]

$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})), \phi \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{H}})) \colon (\eta)P(\phi \rightsquigarrow \rho) \colon$$
$$\eta(l_1) = \eta(l_2) \Rightarrow \rho([\![P]\!](\phi(h_1), \eta(l_1))^{\mathsf{L}}) = \rho([\![P]\!](\phi(h_2), \eta(l_2))^{\mathsf{L}})$$

EXAMPLE

EXAMPLE:

$$P = \quad l := l * h^2.$$

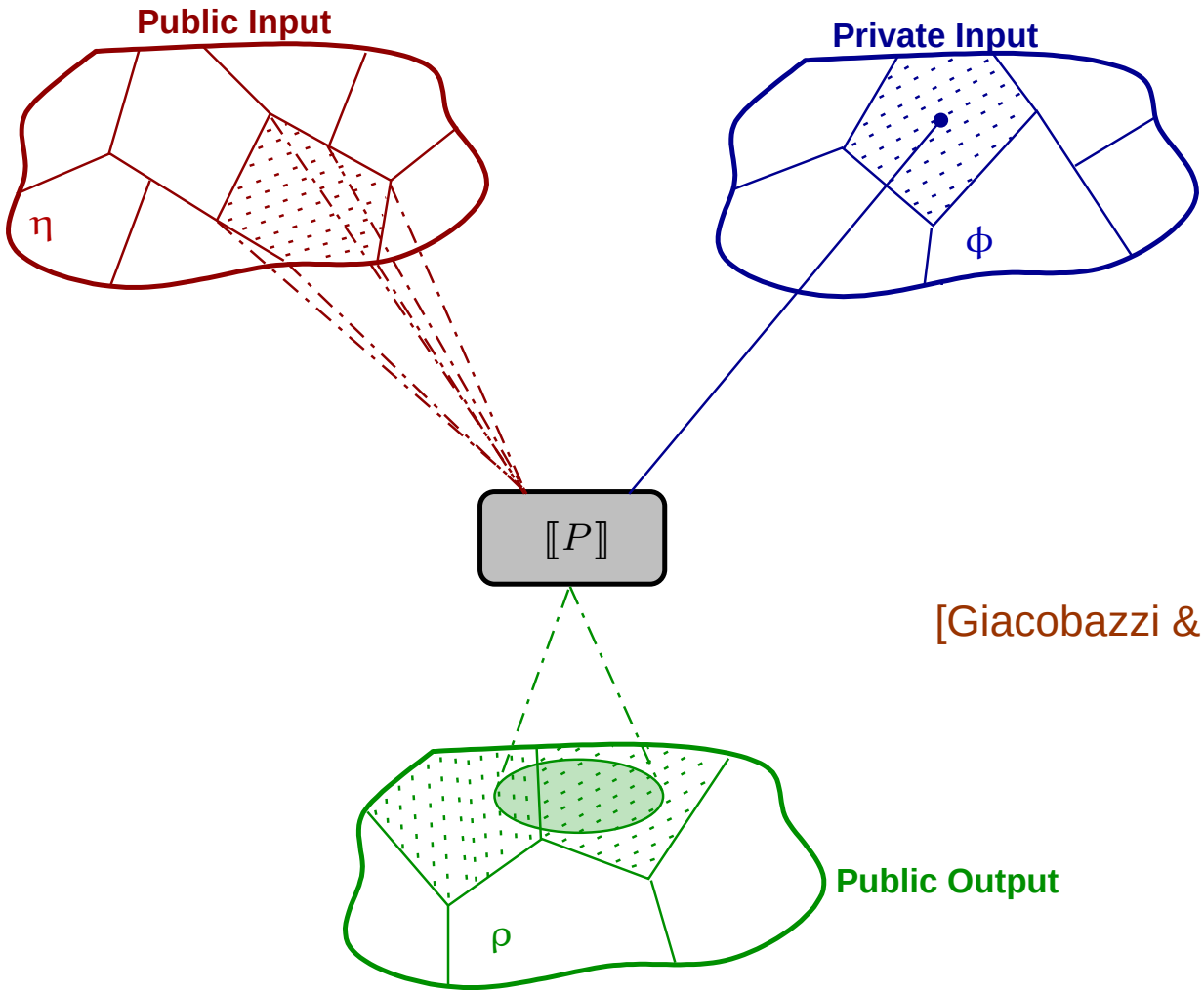
$$\boxed{(id)P(Par)}$$

$$h = 2,\ l = 1 \ \rightsquigarrow\ Par(l) = \text{even}$$
$$h = 3,\ l = 1 \ \rightsquigarrow\ Par(l) = \text{odd}$$
$$h = n,\ l = 1 \ \rightsquigarrow\ Par(l) = Par(n)$$

$$\boxed{(id)P(Sign \rightsquigarrow\!\!] Par)}$$

$$Sign(h) = +,\ l = 1 \ \rightsquigarrow\ Par(l) = \text{I don't know}$$
$$Sign(h) = -,\ l = 1 \ \rightsquigarrow\ Par(l) = \text{I don't know}$$

DECLASSIFIED ANI (VIA ALLOWING)

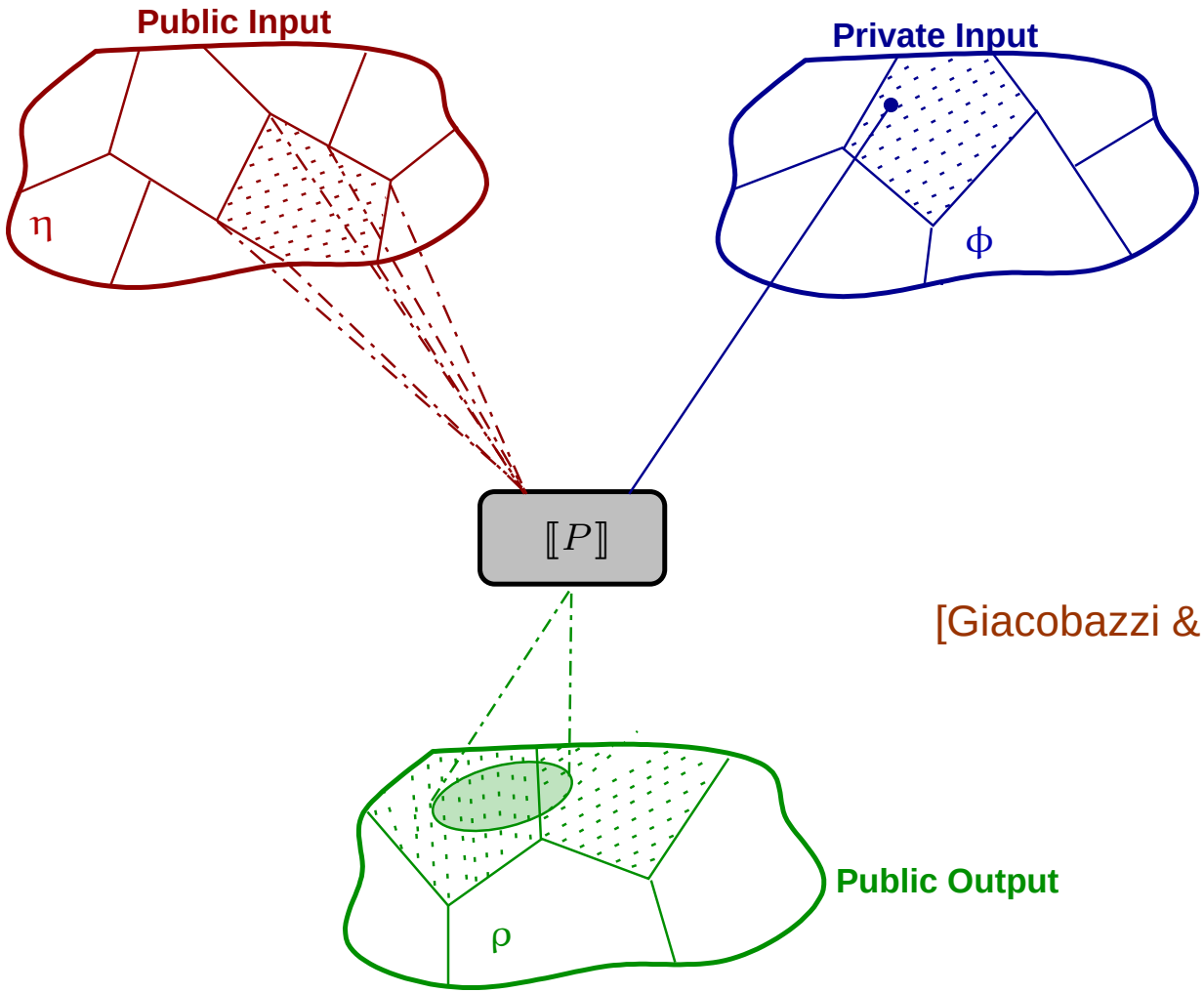


[Giacobazzi & Mastroeni '04]

$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}}))$, $\phi \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{H}}))$: $(\eta)P(\phi \Rightarrow \rho)$:

$\eta(l_1) = \eta(l_2)$ and $\phi(h_1) = \phi(h_2) \Rightarrow \rho([\![P]\!](h_1, \eta(l_1))^{\mathsf{L}}) = \rho([\![P]\!](h_2, \eta(l_2))^{\mathsf{L}})$

DECLASSIFIED ANI (VIA ALLOWING)

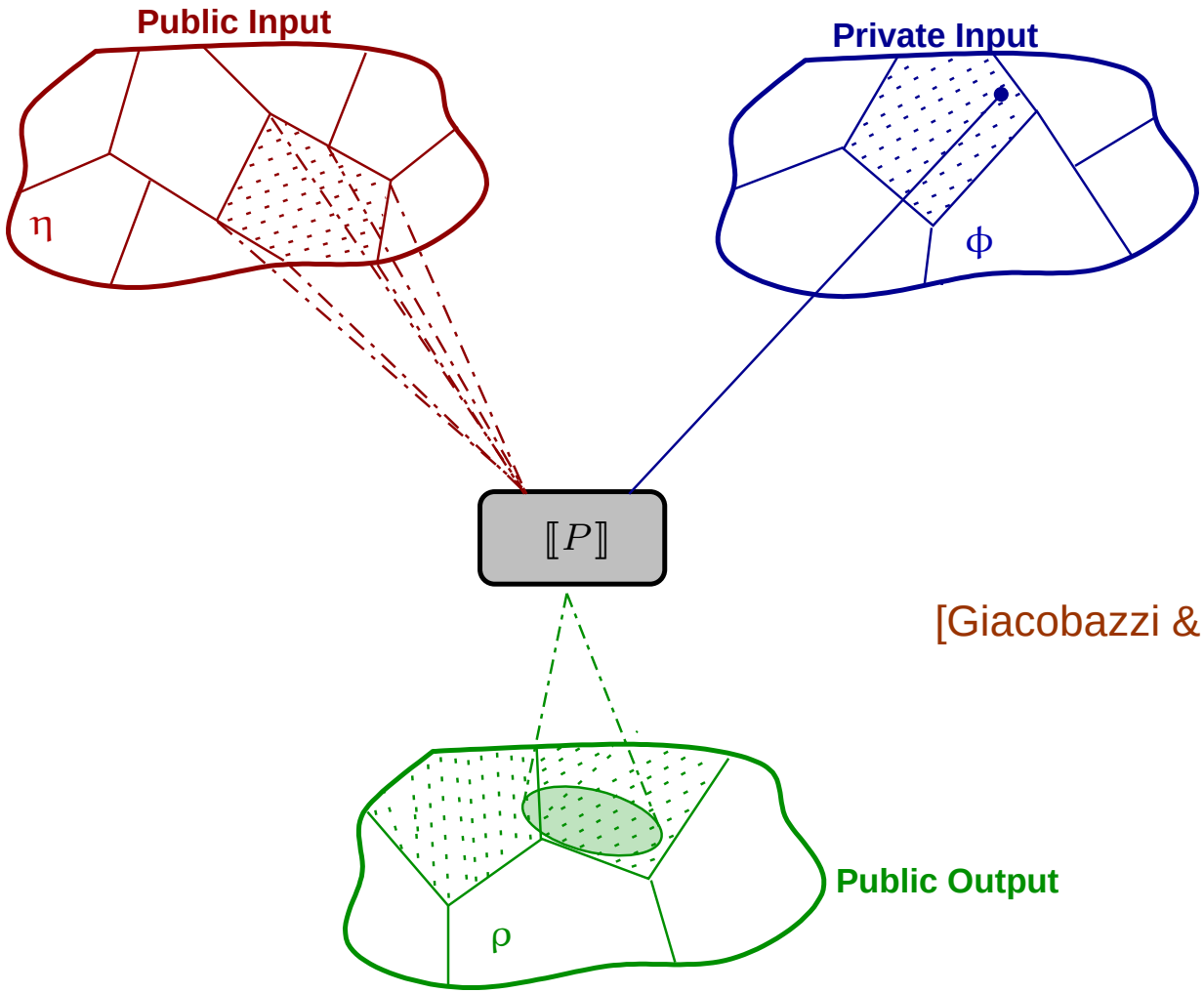


[Giacobazzi & Mastroeni '04]

$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}}))$, $\phi \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{H}}))$: $(\eta)P(\phi \Rightarrow \rho)$:

$\eta(l_1) = \eta(l_2)$ and $\phi(h_1) = \phi(h_2) \Rightarrow \rho([\![P]\!](h_1, \eta(l_1))^{\mathsf{L}}) = \rho([\![P]\!](h_2, \eta(l_2))^{\mathsf{L}})$

DECLASSIFIED ANI (VIA ALLOWING)



[Giacobazzi & Mastroeni '04]

$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}}))$, $\phi \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{H}}))$: $(\eta)P(\phi \Rightarrow \rho)$:

$\eta(l_1) = \eta(l_2)$ and $\phi(h_1) = \phi(h_2) \Rightarrow \rho([\![P]\!](h_1, \eta(l_1))^{\mathsf{L}}) = \rho([\![P]\!](h_2, \eta(l_2))^{\mathsf{L}})$

MODELING

ABSTRACT NON-INTERFERENCE

DERIVING "HARMLESS" ATTACKERS

Abstract interpretation provides advanced methods for designing abstractions (refinement, simplification, compression ...) [Giacobazzi & Ranzato '97]

Transforming abstractions = transforming attackers

DERIVING "HARMLESS" ATTACKERS

Abstract interpretation provides advanced methods for designing abstractions (refinement, simplification, compression ...) [Giacobazzi & Ranzato '97]

Transforming abstractions = transforming attackers

Characterize the most concrete δ such that $(\delta)P(\phi \rightsquigarrow\!\!\!\!\!|\,\delta)$

[The most powerful *harmless* public observer]

$\Rightarrow$ This would provide a "measure" of security!

DERIVING "HARMLESS" ATTACKERS

EXAMPLE:

$$P = \quad \textbf{while } h \textbf{ do } (l := l * 2;\ h := h - 1)$$

.... we derive a secure attacker $\pi = \Upsilon\left(\left\{ n\{2\}^{\mathbb{N}} \;\middle|\; n \in 2\mathbb{N}+1 \right\} \cup \{\{0\}\}\right)$:

$$(\pi)[\![P]\!](id \rightsquigarrow\!\!\!\!\!\!\Vdash \pi)$$

$$h = 0,\ \pi(l) = 3\{2\}^{\mathbb{N}} \ \rightsquigarrow\ \pi(l) = 3\{2\}^{\mathbb{N}}$$
$$h = 2,\ \pi(l) = 3\{2\}^{\mathbb{N}} \ \rightsquigarrow\ \pi(l) = 3\{2\}^{\mathbb{N}}$$

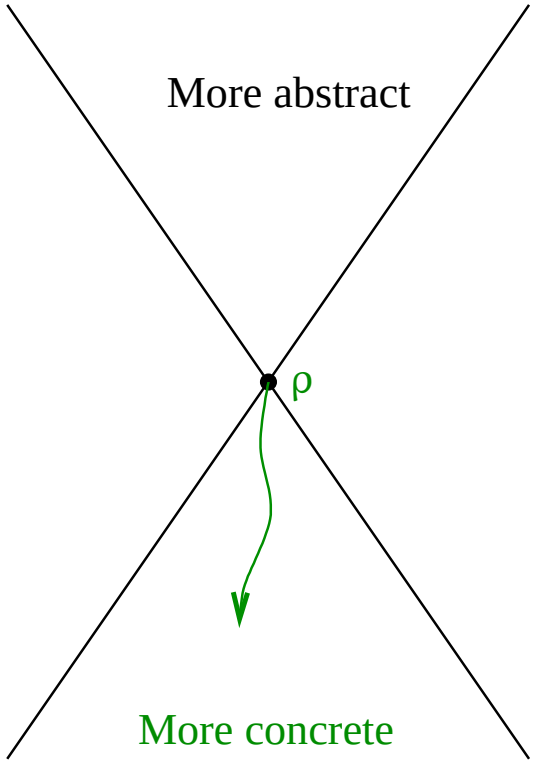
$\rightsquigarrow$ In the program l is always multiplied by 2!

Observer vs Observable

Consider $\models (\eta) P(\phi \rightsquigarrow [\![\rho)$: *In order to preserve non-interference...*

OBSERVER VS OBSERVABLE

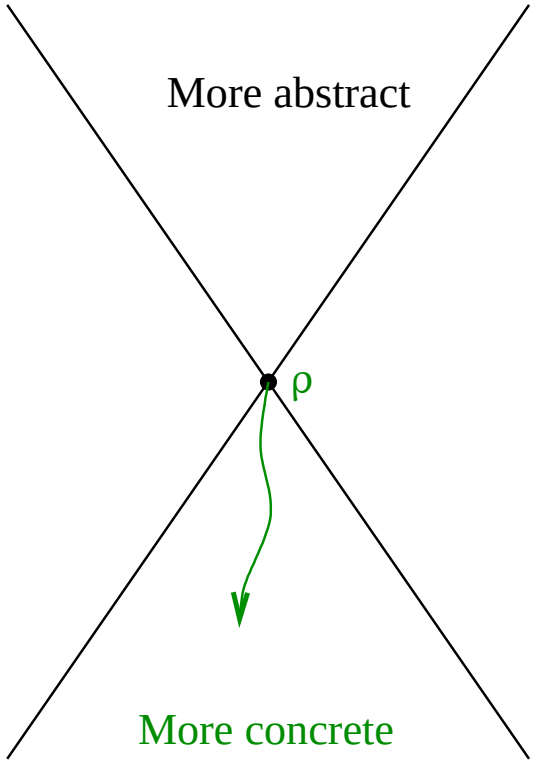
Consider $\models (\eta) P (\phi \rightsquigarrow\!\!\!\!\!\!\rceil\, \rho)$: *In order to preserve non-interference...*



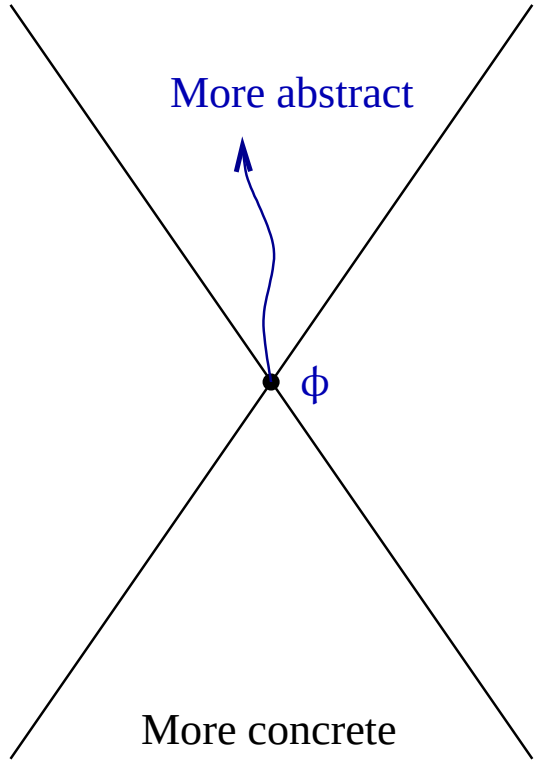
$uco(\wp(\mathbb{V}^{\mathsf{L}}))$

OBSERVER VS OBSERVABLE

Consider $\models (\eta) P (\phi \rightsquigarrow\!\!\!\!\!\!\rceil\, \rho)$: *In order to preserve non-interference...*



AND

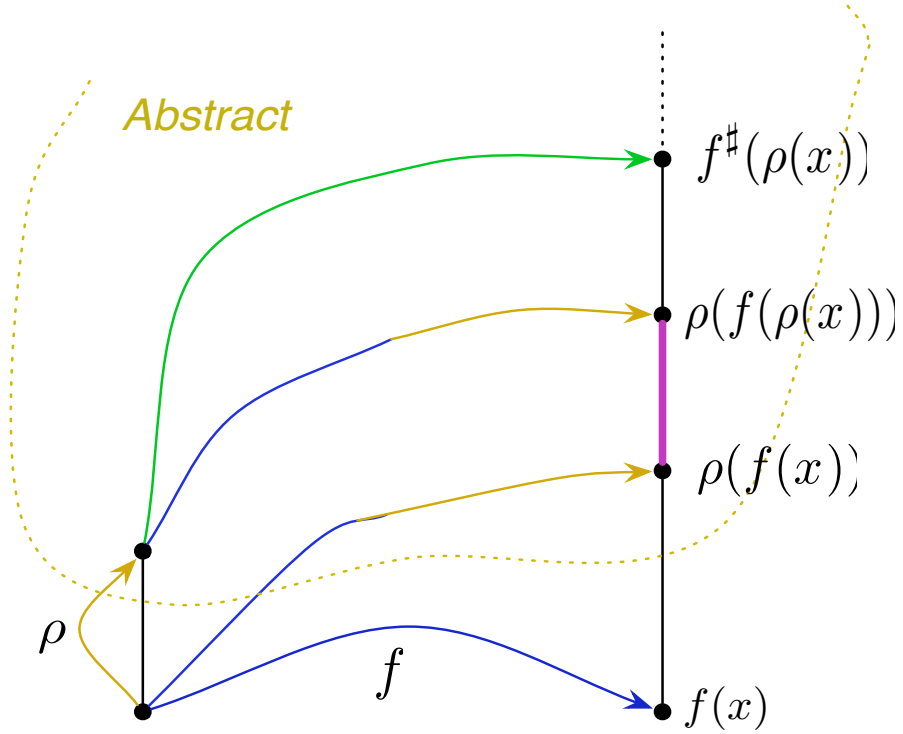


$uco(\wp(\mathbb{V}^{\mathsf{L}}))$ $uco(\wp(\mathbb{V}^{\mathsf{H}}))$

COMPLETENESS IN ABSTRACT INTERPRETATION

- SOUNDNESS:
  NO INFORMATION IS LOST BY APPROXIMATING THE INPUT/OUTPUT

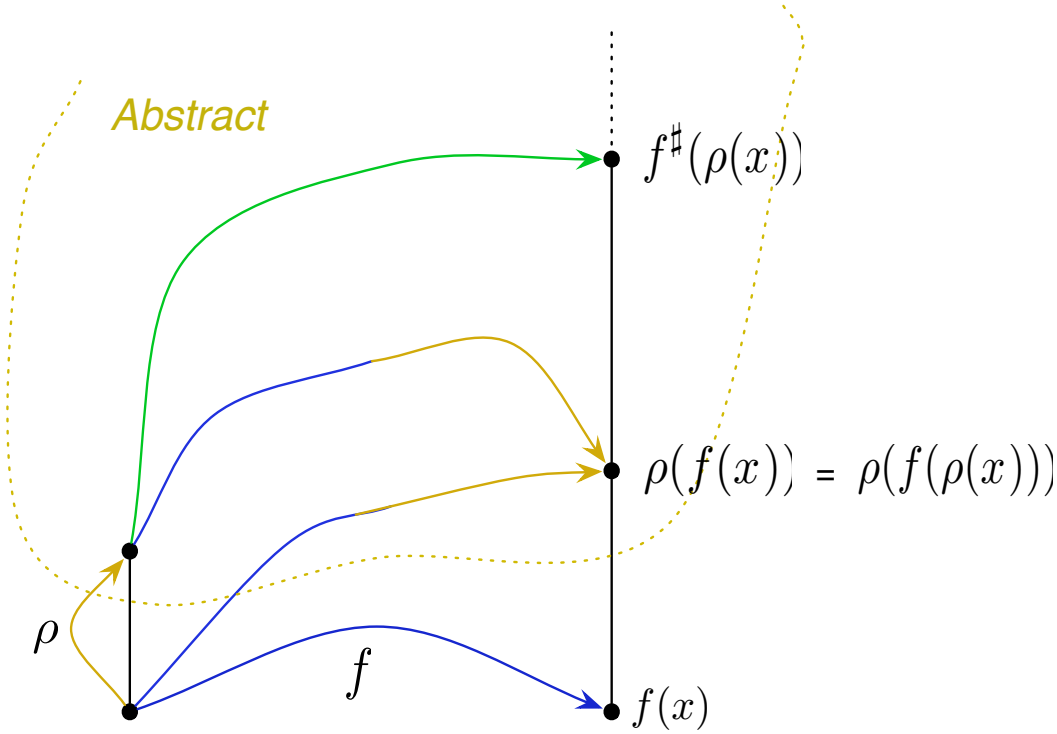
- $\rho \circ f \leq \rho \circ f \circ \rho$



COMPLETENESS IN ABSTRACT INTERPRETATION

- COMPLETENESS:
  NO LOSS OF PRECISION IS ACCUMULATED BY APPROXIMATING THE INPUT

- $\rho \circ f = \rho \circ f \circ \rho$



ANI IS A COMPLETENESS PROBLEM

Recall that [Joshi & Leino'00]

P is *secure* iff $\texttt{HH}\ ;\ P;\ \texttt{HH} \ \dot{=}\ P\ ;\ \texttt{HH}$

ANI IS A COMPLETENESS PROBLEM

Recall that [Joshi & Leino'00]

P is *secure* iff $\mathtt{HH}\,;\, P;\, \mathtt{HH} \doteq P\,;\, \mathtt{HH}$

Let $X = \langle X^{\mathsf{H}}, X^{\mathsf{L}} \rangle \Rightarrow \mathcal{H}(X) \stackrel{\text{def}}{=} \langle \top^{\mathsf{H}}, X^{\mathsf{L}} \rangle \in \mathit{Abs}(\wp(\mathbb{V}))$

$$\begin{array}{ccc} \mathtt{HH}\,;\, P;\, \mathtt{HH} & \doteq & P\,;\, \mathtt{HH} \\ & \Downarrow & \\ \mathcal{H} \circ [\![P]\!] \circ \mathcal{H} & = & \mathcal{H} \circ [\![P]\!] \end{array}$$

ANI IS A COMPLETENESS PROBLEM

Recall that [Joshi & Leino'00]

P is *secure* iff $\mathtt{HH}\,;\, P;\, \mathtt{HH} \doteq P\,;\, \mathtt{HH}$

Let $X = \langle X^{\mathsf{H}}, X^{\mathsf{L}} \rangle \Rightarrow \mathcal{H}(X) \stackrel{\text{def}}{=} \langle \top^{\mathsf{H}}, X^{\mathsf{L}} \rangle \in \mathit{Abs}(\wp(\mathbb{V}))$

$$\begin{array}{ccc} \mathtt{HH}\,;\, P;\, \mathtt{HH} & \doteq & P\,;\, \mathtt{HH} \\ & \Downarrow & \\ \mathcal{H} \circ [\![P]\!] \circ \mathcal{H} & = & \mathcal{H} \circ [\![P]\!] \end{array}$$

$\Rightarrow$ A COMPLETENESS PROBLEM

ANI IS A COMPLETENESS PROBLEM

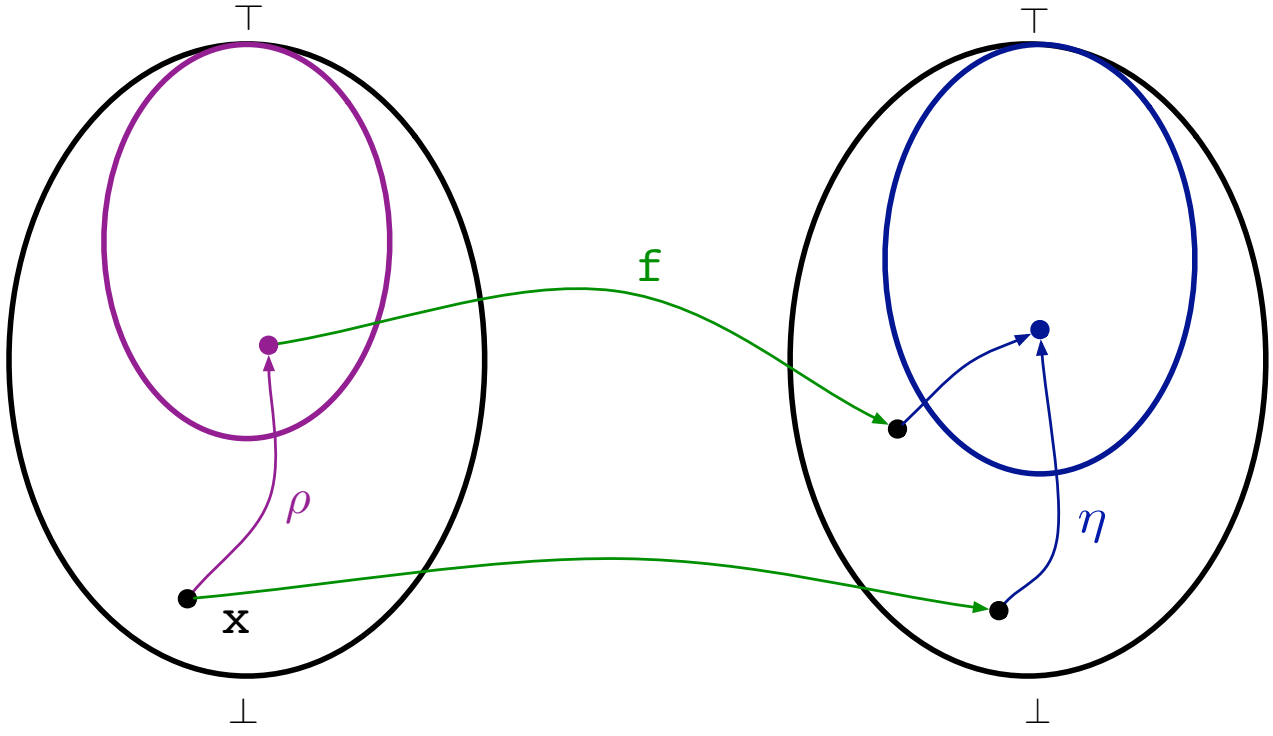
Let $X = \langle X^{\mathsf{H}}, X^{\mathsf{L}} \rangle \Rightarrow \mathcal{H}(X) \stackrel{\mathsf{def}}{=} \langle \top^{\mathsf{H}}, X^{\mathsf{L}} \rangle \in \mathit{Abs}(\wp(\mathbb{V}))$

$$\mathcal{H} \circ [\![P]\!] \circ \mathcal{H} \quad = \quad \mathcal{H} \circ [\![P]\!]$$

COMPLETENESS = NON-INTERFERENCE

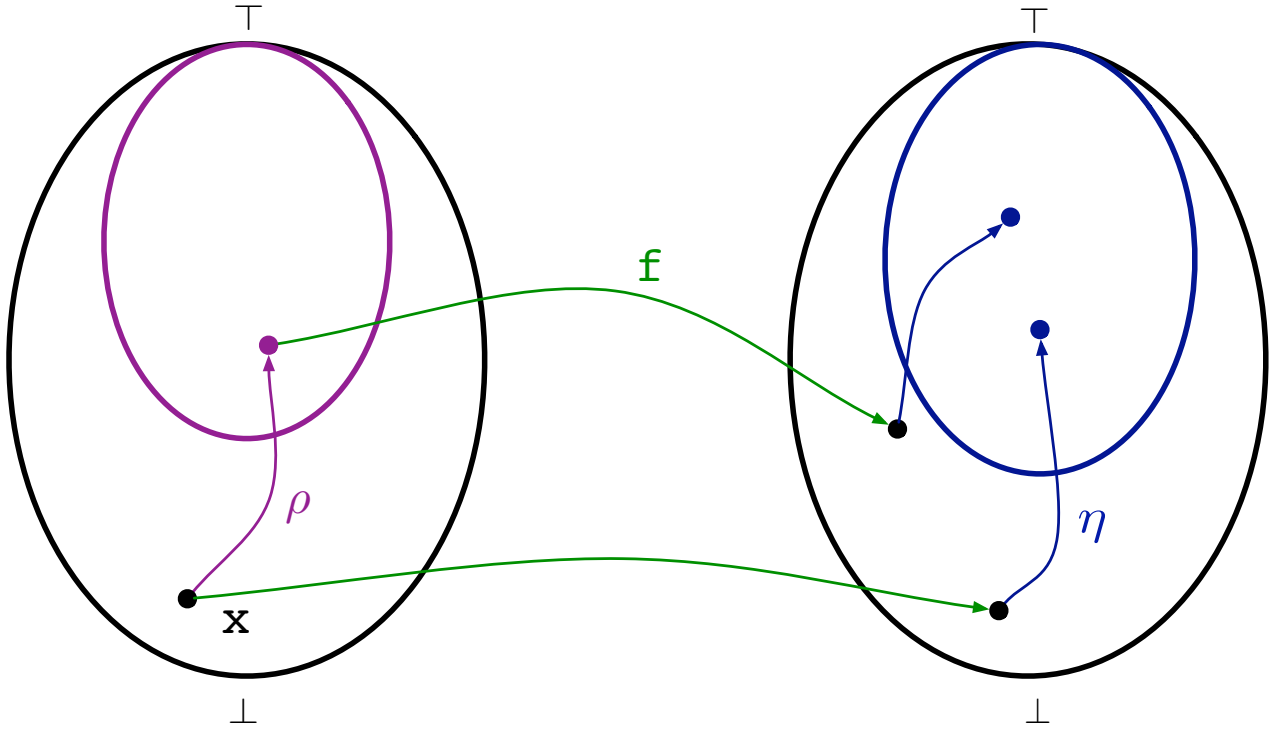
- Transform $\mathcal{H}$ vs *Core:* $\mathcal{C}$
- Transform $\mathcal{H}$ vs *Shell:* $\mathcal{S}$ [Giacobazzi et al. JACM'00]

COMPLETENESS



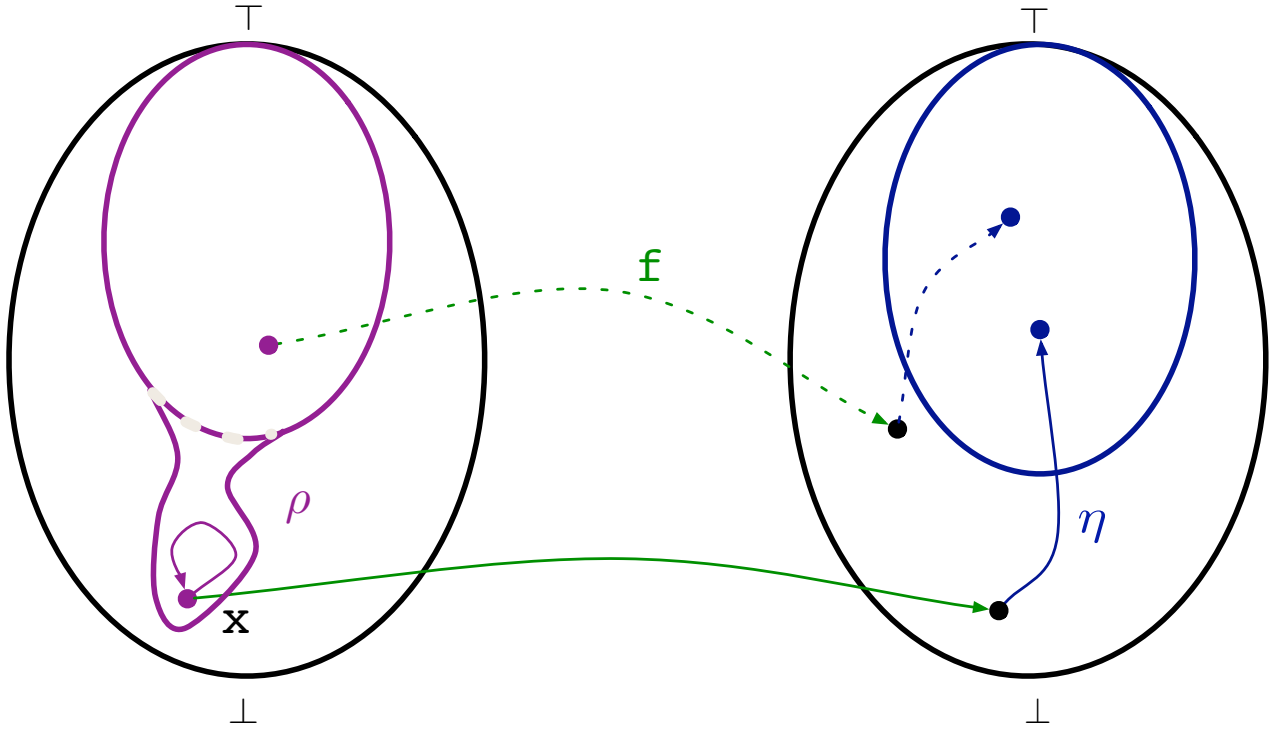
COMPLETENESS: $\eta \circ f \circ \rho = \eta \circ f$

COMPLETENESS



IN-COMPLETENESS: $\eta \circ f \circ \rho \geq \eta \circ f$

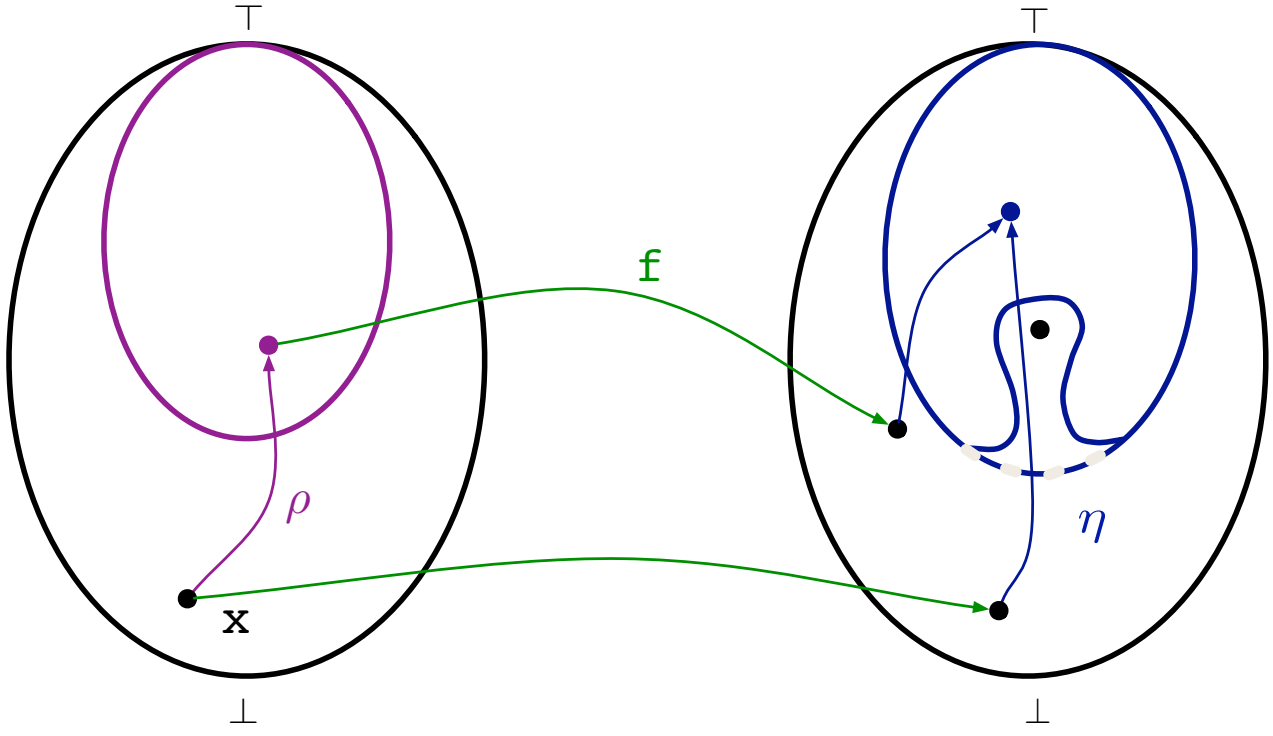
COMPLETENESS



Making ABSTRACTIONS COMPLETE: Refining input domains

[*Giacobazzi et al. JACM'00*]

COMPLETENESS



Making ABSTRACTIONS COMPLETE: Simplifying output domains

[*Giacobazzi et al. JACM'00*]

ANI AS COMPLETENESS

Let $\rho \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})) \Rightarrow \mathcal{H}_\rho(X) \stackrel{\mathsf{def}}{=} \langle \top^{\mathsf{H}}, \rho(X^{\mathsf{L}}) \rangle \in \mathit{Abs}(\wp(\mathbb{V}))$

- *Narrow abstract non-interference:* $\mathcal{H}_\rho \circ [\![P]\!] \circ \mathcal{H}_\eta = \mathcal{H}_\rho \circ [\![P]\!]$;
- *Abstract non-interference:* $\mathcal{H}_\rho \circ [\![P]\!]^{\eta,\Phi} \circ \mathcal{H}_\eta = \mathcal{H}_\rho \circ [\![P]\!]^{\eta,\Phi}$

ANI AS COMPLETENESS

Let $\rho \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})) \Rightarrow \mathcal{H}_\rho(X) \stackrel{\text{def}}{=} \langle \top^{\mathsf{H}}, \rho(X^{\mathsf{L}}) \rangle \in \mathit{Abs}(\wp(\mathbb{V}))$

- *Narrow abstract non-interference:* $\mathcal{H}_\rho \circ [\![P]\!] \circ \mathcal{H}_\eta = \mathcal{H}_\rho \circ [\![P]\!]$;
- *Abstract non-interference:* $\mathcal{H}_\rho \circ [\![P]\!]^{\eta,\phi} \circ \mathcal{H}_\eta = \mathcal{H}_\rho \circ [\![P]\!]^{\eta,\phi}$

$\Downarrow$

- PUBLIC "HARMLESS" OBSERVER AS COMPLETENESS CORE:
$\mathcal{C}^{\mathcal{H}_\eta}_{[\![P]\!]^{\eta,\phi}}(\mathcal{H}) = (\eta)[\![P]\!](\phi \rightsquigarrow [\![id)$

ANI AS COMPLETENESS

Let $\rho \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})) \Rightarrow \mathcal{H}_\rho(X) \stackrel{\mathsf{def}}{=} \langle \top^{\mathsf{H}}, \rho(X^{\mathsf{L}}) \rangle \in \mathit{Abs}(\wp(\mathbb{V}))$

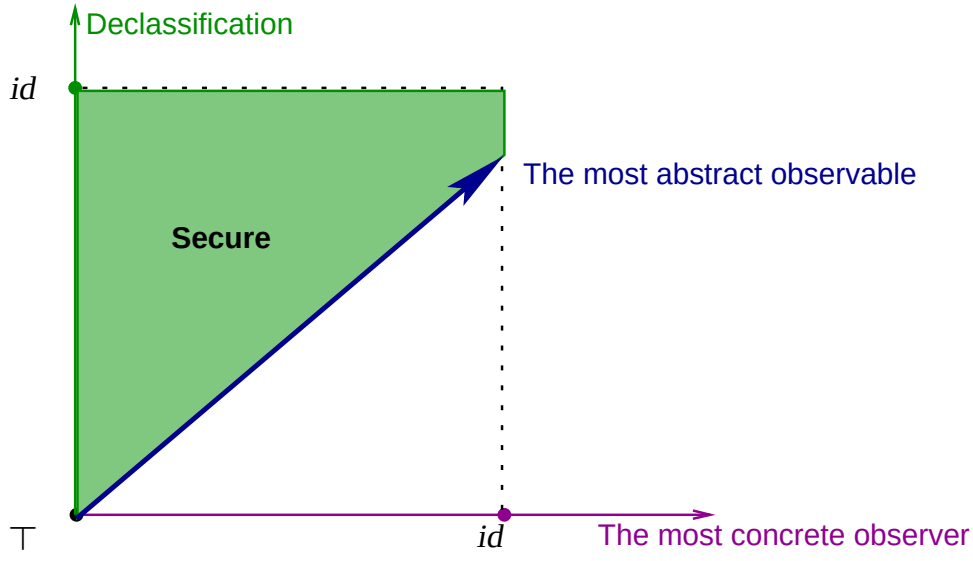
- *Narrow abstract non-interference:* $\mathcal{H}_\rho \circ [\![P]\!] \circ \mathcal{H}_\eta = \mathcal{H}_\rho \circ [\![P]\!]$;
- *Abstract non-interference:* $\mathcal{H}_\rho \circ [\![P]\!]^{\eta,\phi} \circ \mathcal{H}_\eta = \mathcal{H}_\rho \circ [\![P]\!]^{\eta,\phi}$

$\Downarrow$

- PUBLIC "HARMLESS" ATTACKER AS COMPLETENESS CORE:
  $\mathcal{C}^{\mathcal{H}_\eta}_{[\![P]\!]^{\eta,\phi}}(\mathcal{H}) = (\eta)[\![P]\!](\phi \rightsquigarrow [\![id)$
- PRIVATE "FLOWING" OBSERVABLE AS COMPLETENESS SHELL:
  $(\eta)P(\mathcal{S}^{\mathcal{H}_\rho}_{[\![P]\!]^{\eta,id}}(\mathcal{H}_\eta) \Rightarrow \rho)$

BACK TO DIMENSIONS

ADJOINING ATTACKERS AND DECLASSIFICATION BY COMPLETENESS

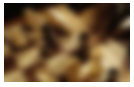


OBSCURITY AND NON-INTERFERENCE

THE IDEA

THE IDEA

OBSCURITY AS INCOMPLETENESS

- $\texttt{WhichChess} : Img \longrightarrow \wp(Chess)$ returns the type of chess on the chessboard.
- $\rho : Img \longrightarrow Img$ such that: $\rho\left(\right.$  $\left.\right) =$ 
- $\eta : \wp(Chess) \longrightarrow [0, 12]$ counts the number of different types of chess

$$\begin{aligned}
\eta\left(\texttt{WhichChess}\left(\rho\left(\right.\right.\right. \text{  } \left.\left.\left.\right)\right)\right) &= \eta\left(\texttt{WhichChess}\left(\right.\right. \text{  } \left.\left.\right)\right) \\
&= 12 \\
&\geq \eta\left(\texttt{WhichChess}\left(\right.\right. \text{  } \left.\left.\right)\right) \\
&= 7
\end{aligned}$$

OBSCURITY AS INCOMPLETENESS

Failing precision means failing completeness! [*Giacobazzi et al., 2008–12*]

Obfuscating programs is making abstract interpreters incomplete

- Let $\rho \in \mathit{Abs}(\Sigma)$ with Σ semantic objects (data, traces etc)
- A program transformation $\tau : \mathbb{P} \to \mathbb{P}$ such that $[\![P]\!] = [\![\tau(P)]\!]$.
- ρ $\mathcal{B}$-complete for $[\![\cdot]\!]$ if $\rho([\![P]\!]) = [\![P]\!]^\rho$

τ obfuscates P if $[\![P]\!]^\rho \sqsubset [\![\tau(P)]\!]^\rho$

$$[\![P]\!]^\rho \sqsubset [\![\tau(P)]\!]^\rho \iff \rho([\![\tau(P)]\!]) \sqsubset [\![\tau(P)]\!]^\rho$$

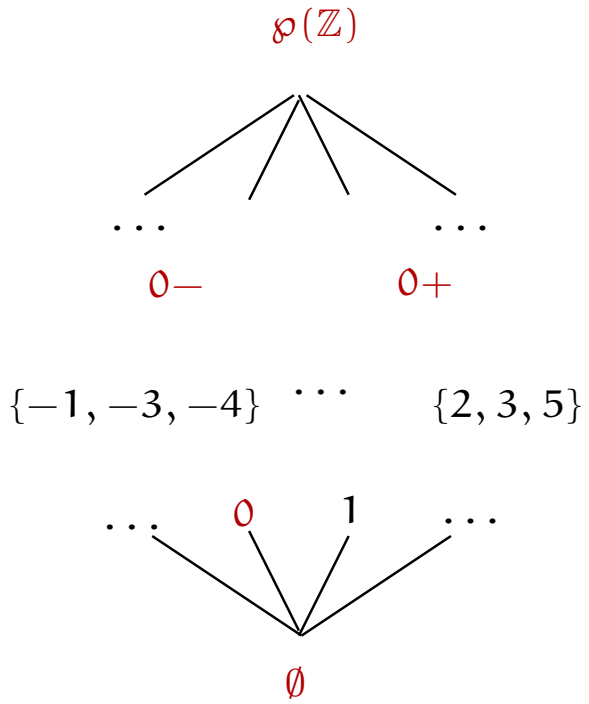
OBSCURITY AS INCOMPLETENESS

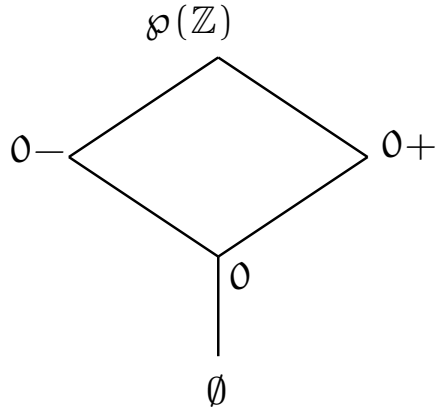
Failing precision means failing completeness! [*Giacobazzi et al., 2008–12*]

Obfuscating programs is making abstract interpreters incomplete

P : x = a ∗ b

$Sign$ is an obvious abstraction of $\wp(\mathbb{Z})$:





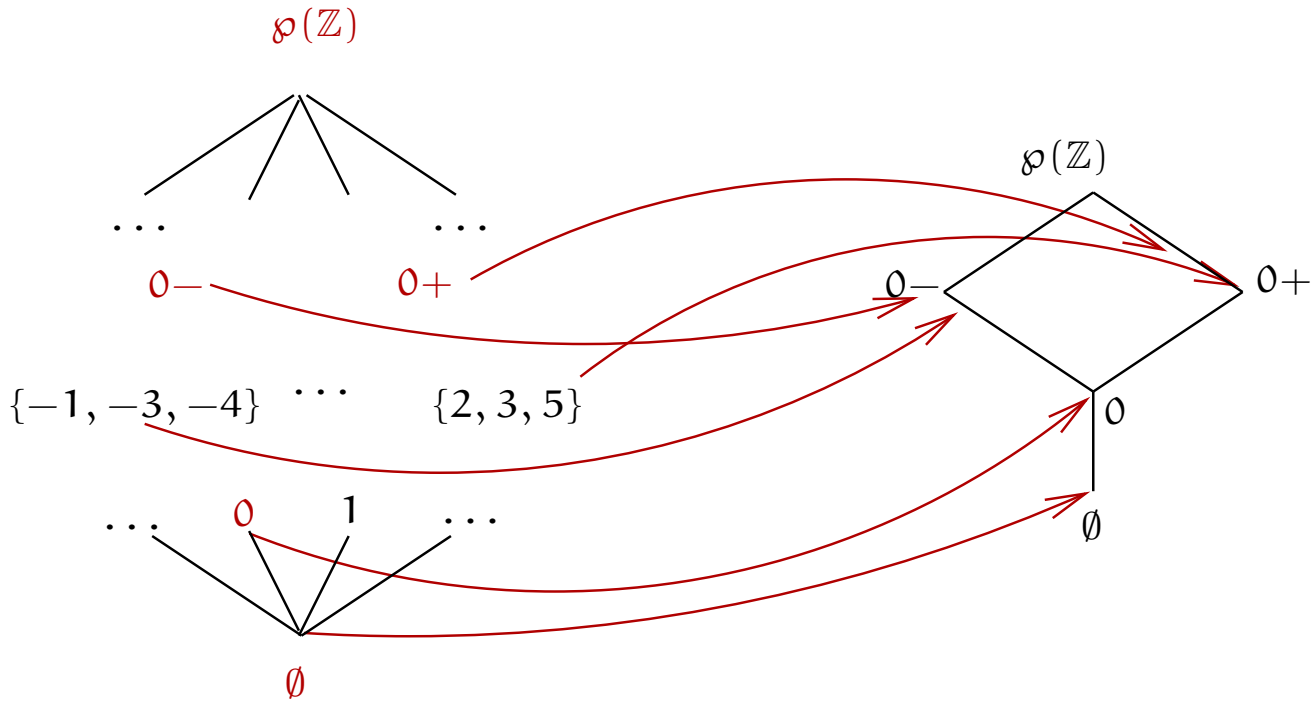
OBSCURITY AS INCOMPLETENESS

Failing precision means failing completeness! [*Giacobazzi et al., 2008–12*]

Obfuscating programs is making abstract interpreters incomplete

P : x = a ∗ b

$Sign$ is an abstraction of $\wp(\mathbb{Z})$:



OBSCURITY AS INCOMPLETENESS

Failing precision means failing completeness! [*Giacobazzi et al., 2008–12*]

Obfuscating programs is making abstract interpreters incomplete

$$P: \quad \mathtt{x} = \mathtt{a} * \mathtt{b} \quad \longrightarrow \quad \tau(P): \quad \begin{array}{l} \mathtt{x} = 0; \\ \mathtt{if\ b} \leq 0\ \mathtt{then}\ \{\mathtt{a} = -\mathtt{a}; \mathtt{b} = -\mathtt{b}\}; \\ \mathtt{while\ b} \neq 0\ \{\mathtt{x} = \mathtt{a} + \mathtt{x}; \mathtt{b} = \mathtt{b} - 1\} \end{array}$$

- $Sign$ is complete for P:
  - ✔ $[\![P]\!]^{Sign} = \lambda \mathtt{a}, \mathtt{b}.\ Sign(\mathtt{a} * \mathtt{b})$
- $Sign$ is incomplete for $\tau(P)$:
  - ✔ $[\![\tau(P)]\!]^{Sign} = \lambda \mathtt{a}, \mathtt{b}. \begin{cases} 0 & \text{if } \mathtt{a} = 0 \vee \mathtt{b} = 0 \\ \top & \text{otherwise} \end{cases}$
- There is a way to get $\tau(P)$ systematically from P [*Giacobazzi et al, 2012*]

EXPLOITING INCOMPLETENESS

Maximize $[\![P]\!]^{\rho}$ incompleteness! [*Giacobazzi et al., 2012*]

- The abstraction is the specification of the attacker
  - Profiling: Abstract memory keeping only (partial) resource usage
  - Tracing: Abstraction of traces (e.g., by trace compression)
  - Slicing: Abstraction of traces (relative to variables)
  - Monitoring: Abstraction of trace semantics ([Cousot&Cousot POPL02])
  - Decompilation: Abstracts syntactic structures (e.g., reducible loops)
  - Disassembly: Abstracts binary structures (e.g., recursive traversal)
- Each abstraction is incomplete for a concrete enough trace semantics
- Maximize incompleteness by code transformation: Obfuscation
- Exploit incompleteness for hiding information: Steganography

CODE OBFUSCATION AS ANI?

A challenging and open question!

- OBFUSCATING NON-INTERFERENCE: means creating *fake* dependencies (interference)
  - ✔ Making non-interference incomplete
- OBFUSCATING INTERFERENCE: means disconnecting dependencies
  - ✔ Making interference (dependence analysis) incomplete
- ABSTRACT SLICING: is a way for de-obfuscating (e.g., watermark extraction) see Isabella's talk next!

CURRENT DIRECTIONS

- ANI is general enough to weaken non-interference and deal with the WHO and WHAT dimensions!
  - ✔ Transforming abstractions means modeling attackers in ANI
  - ✔ Transforming programs means making code secure
- ANI for obfuscation & for information hiding
  - ✔ Isolate non-interfering code slices to act obfuscation
  - ✔ Associate with Φ a stegomark disclosable by ANI via allowing
- Move from syntactic to semantic-based metrics for measuring the potency of obfuscation
  - ✔ measuring incompleteness as a measure of obscurity
  - ✔ measuring the difficulty of proving semantic equivalence (the Coq proof is indeed a deobfuscation)

DAPA

Digital Asset
Protection Association

MANY THANKS!!