THE PER MODEL OF ABSTRACT NON-INTERFERENCE

Sebastian Hunt and **Isabella Mastroeni**

Department of Computing, School of Informatics

City University, London, UK

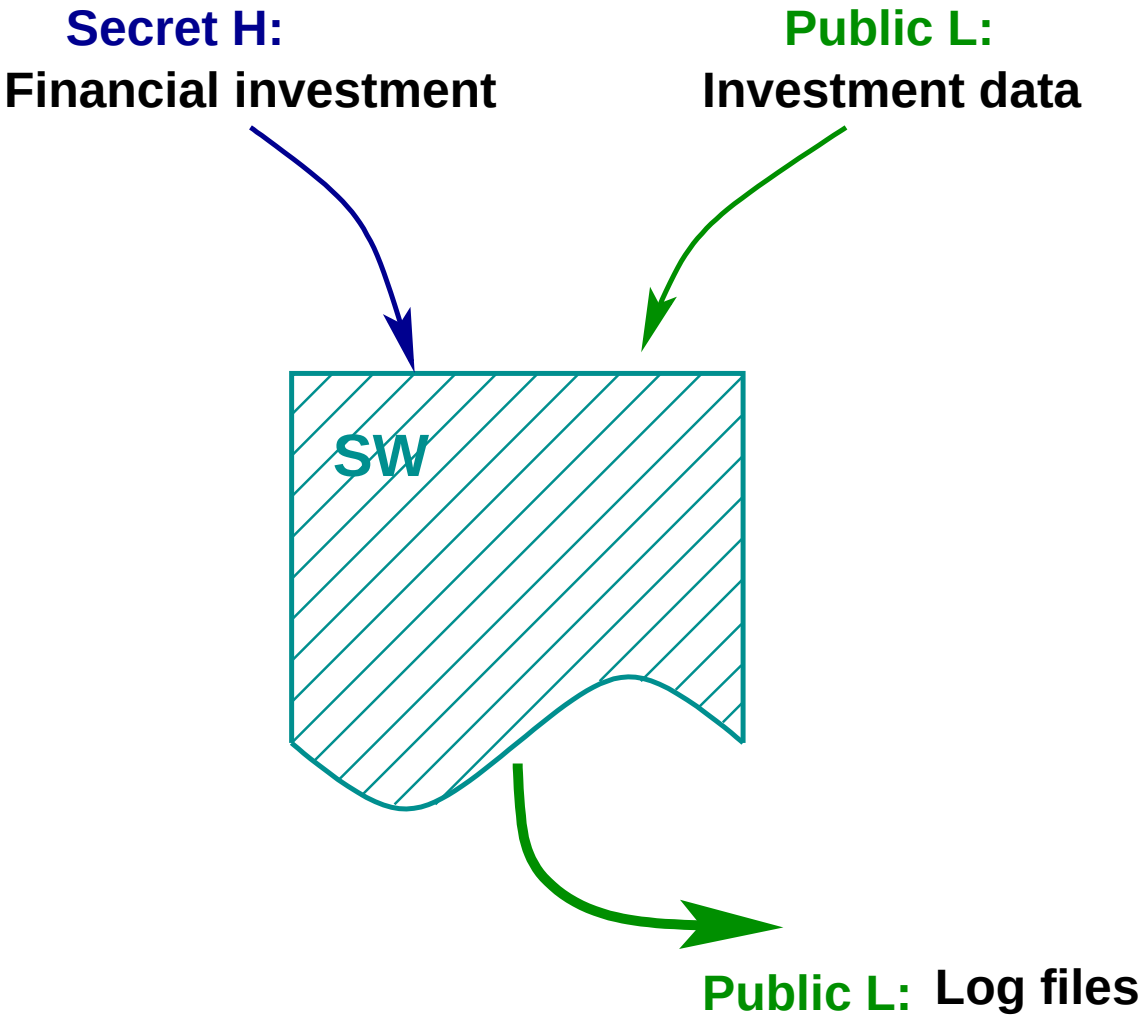
and

Department of Computing and Informatic Sciences

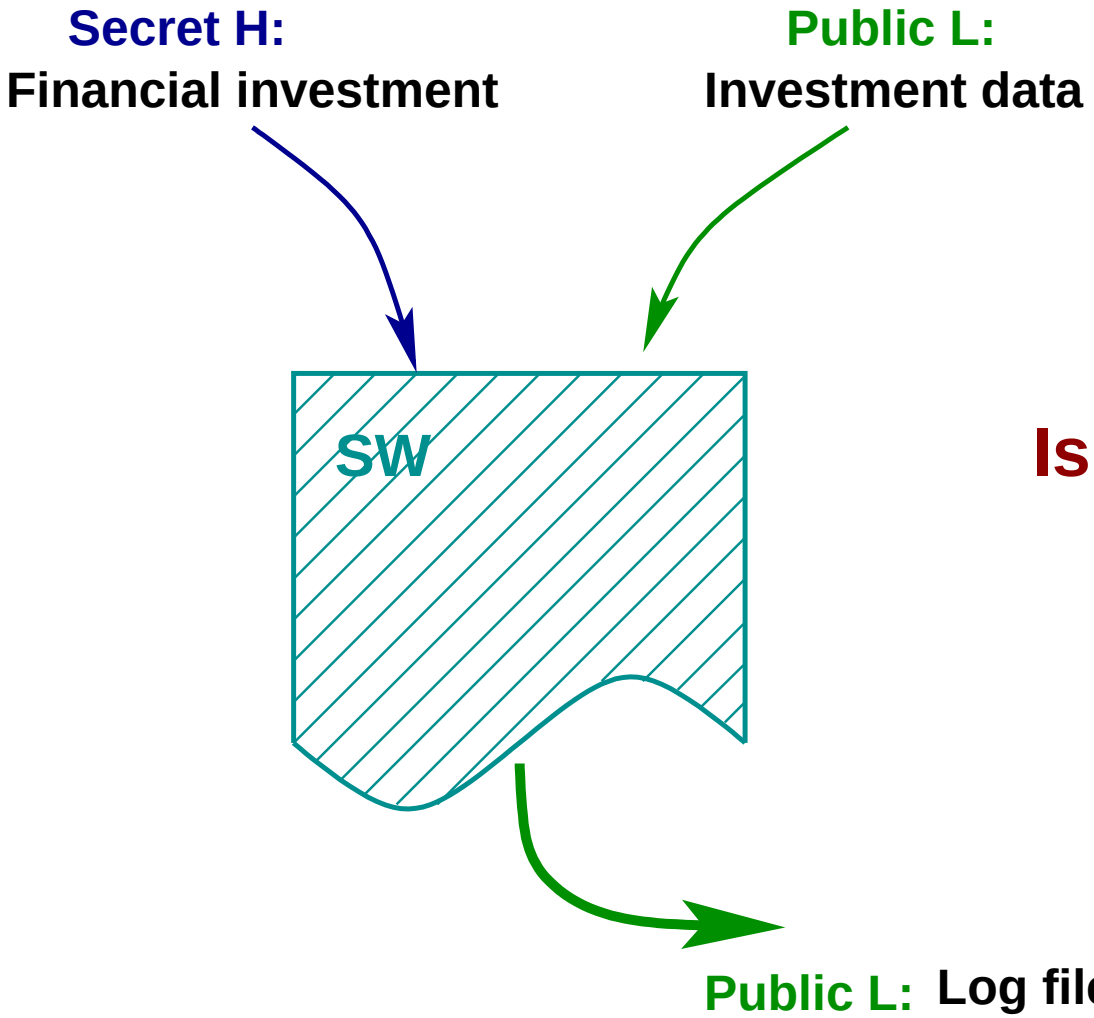
Kansas State University, Manhattan, KS, USA

SAS, September 9th, 2005

The Problem: Non-Interference

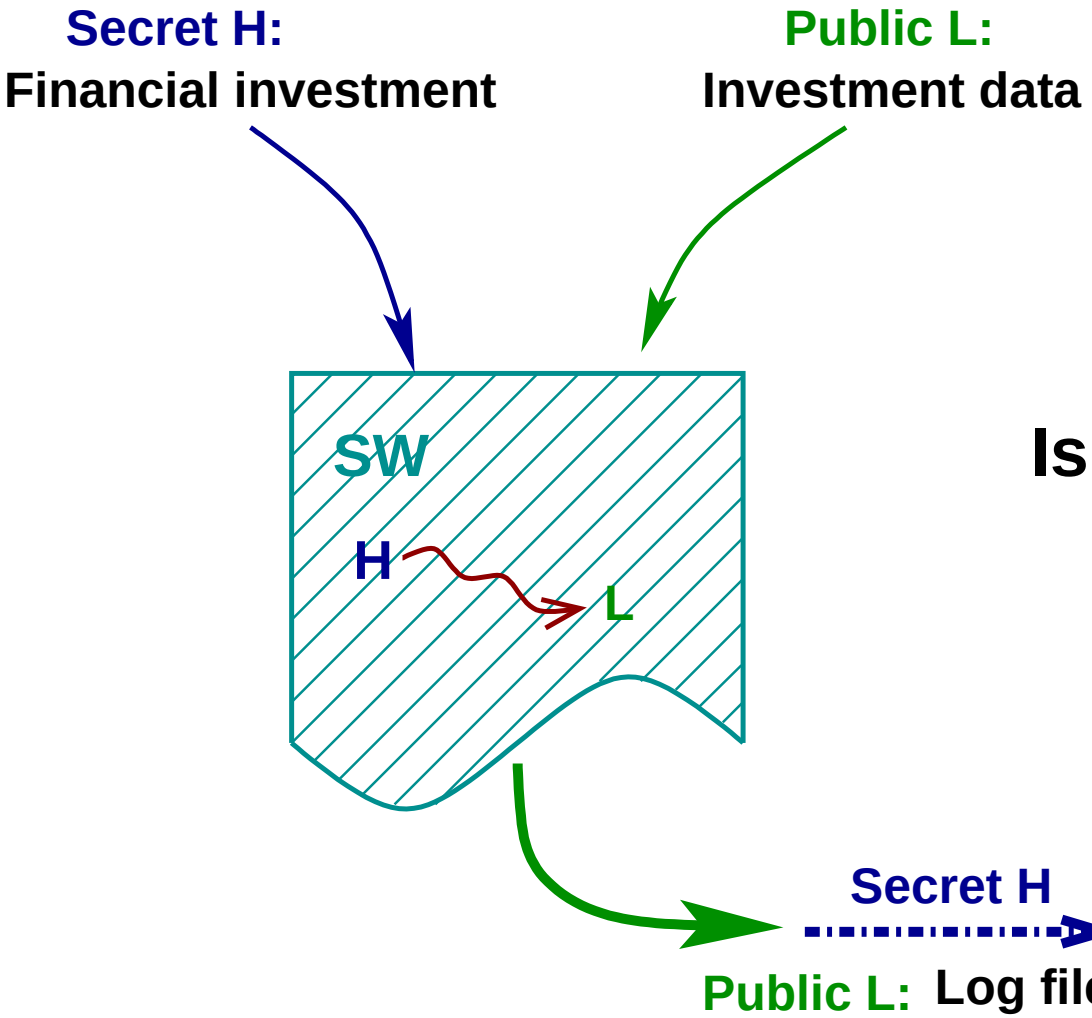


The Problem: Non-Interference



Is it secure?

The Problem: Non-Interference



Is it secure? NO

Background: The PER model

SECURITY PROPERTY: States which classes have not to interfere with other classes of objects.

Background: The PER model

SECURITY PROPERTY: States which classes have not to interfere with other classes of objects.

Confinement problem [Lampson'73]: *Preventing the results of computations leaking even partial information about the confidential inputs.*

Background: The PER model

SECURITY PROPERTY: States which classes have not to interfere with other classes of objects.

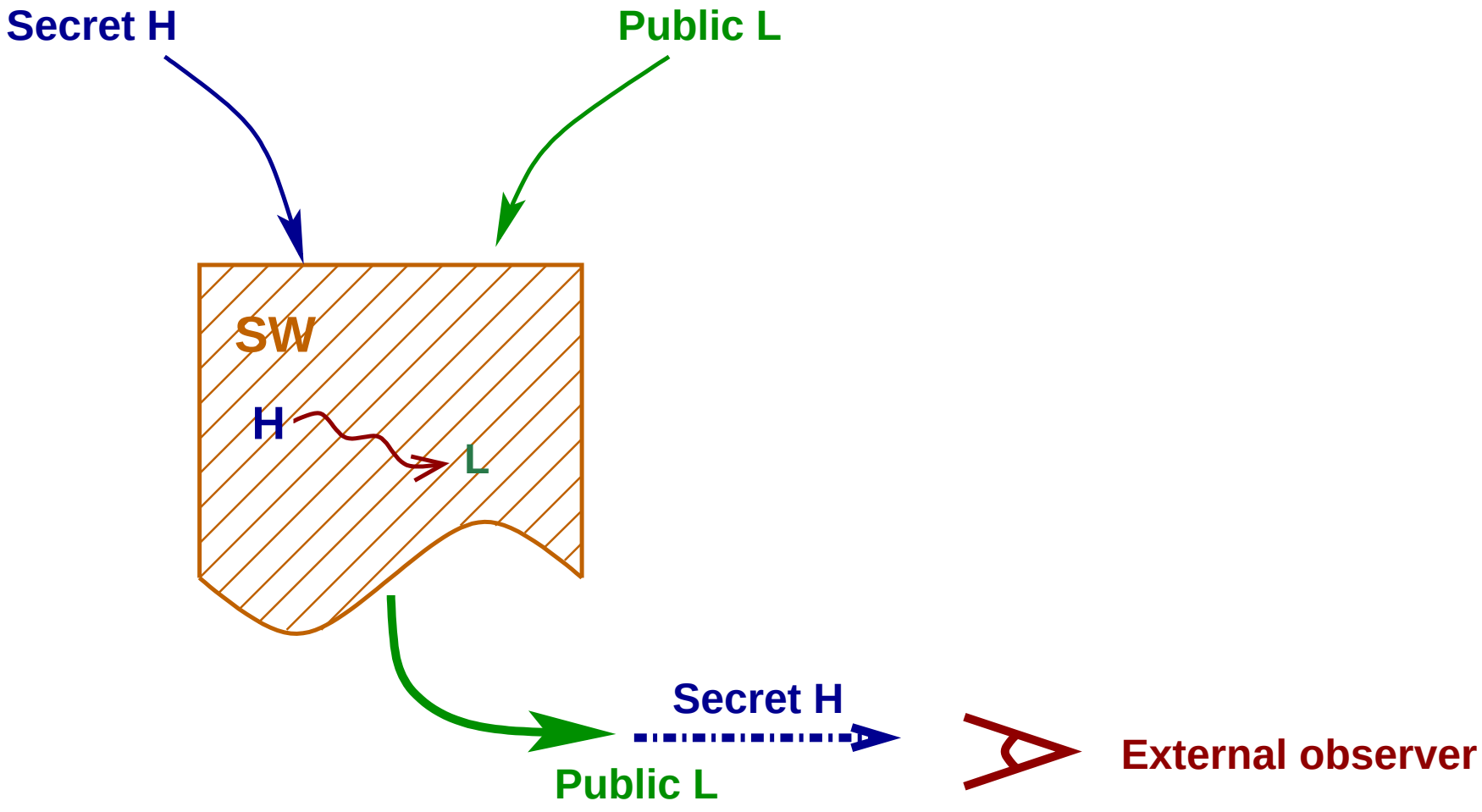
Confinement problem [Lampson'73]: *Preventing the results of computations leaking even partial information about the confidential inputs.*

- PER model [Sabelfeld & Sands'01]:
  Let $\forall x, x'.\ x\ \mathtt{All}\ x'$ and $x\ \mathtt{Id}\ x' \Leftrightarrow x = x'$.

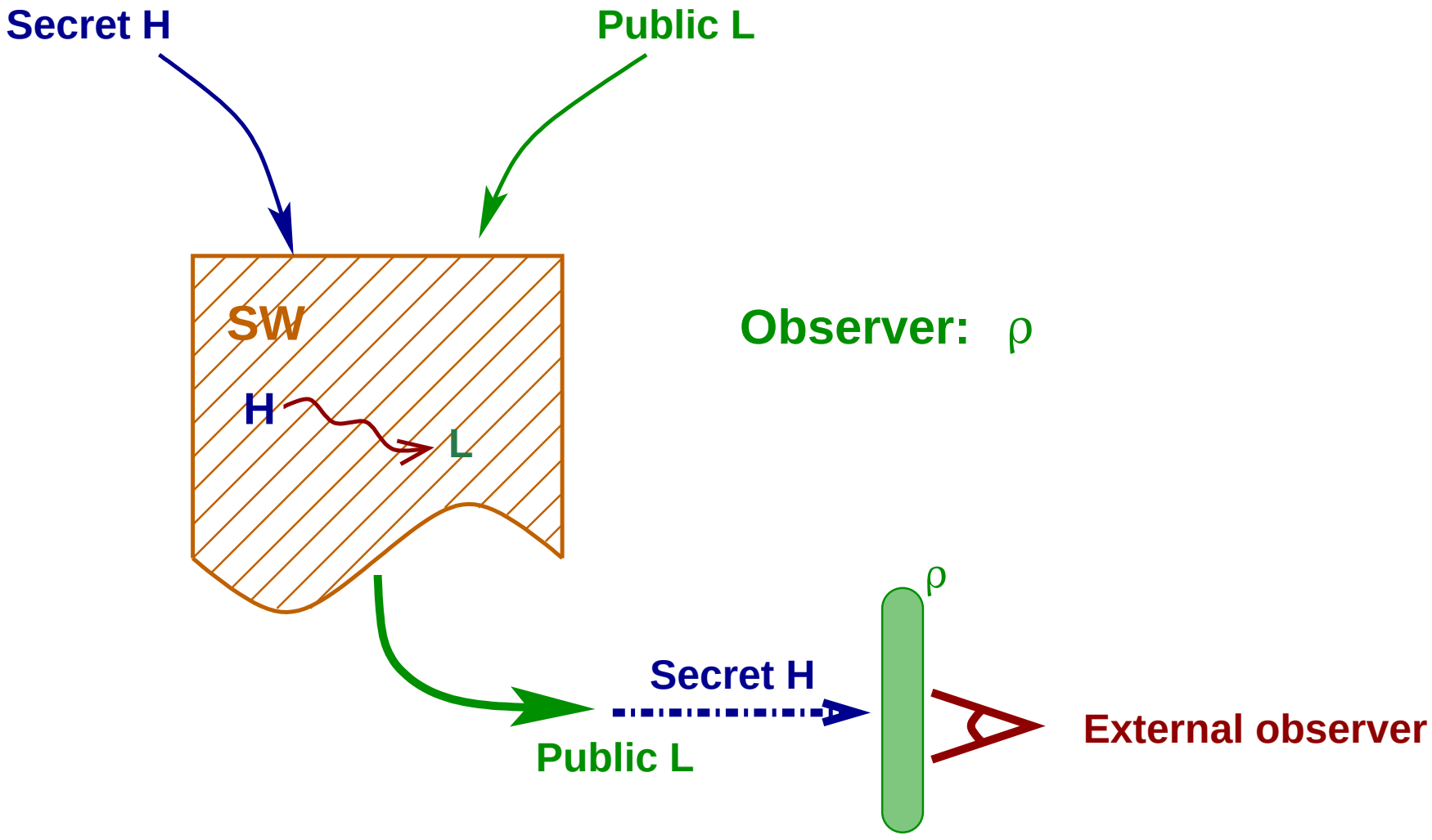
$$\mathtt{P} \text{ is } \textit{secure} \quad \text{iff}$$

$$\forall s, t\ .\ \langle s^{\mathtt{H}}, s^{\mathtt{L}}\rangle\ \mathtt{All} \times \mathtt{Id}\ \langle t^{\mathtt{H}}, t^{\mathtt{L}}\rangle \Rightarrow [\![\mathtt{P}]\!](s)\ \mathtt{All} \times \mathtt{Id}\ [\![\mathtt{P}]\!](t)$$

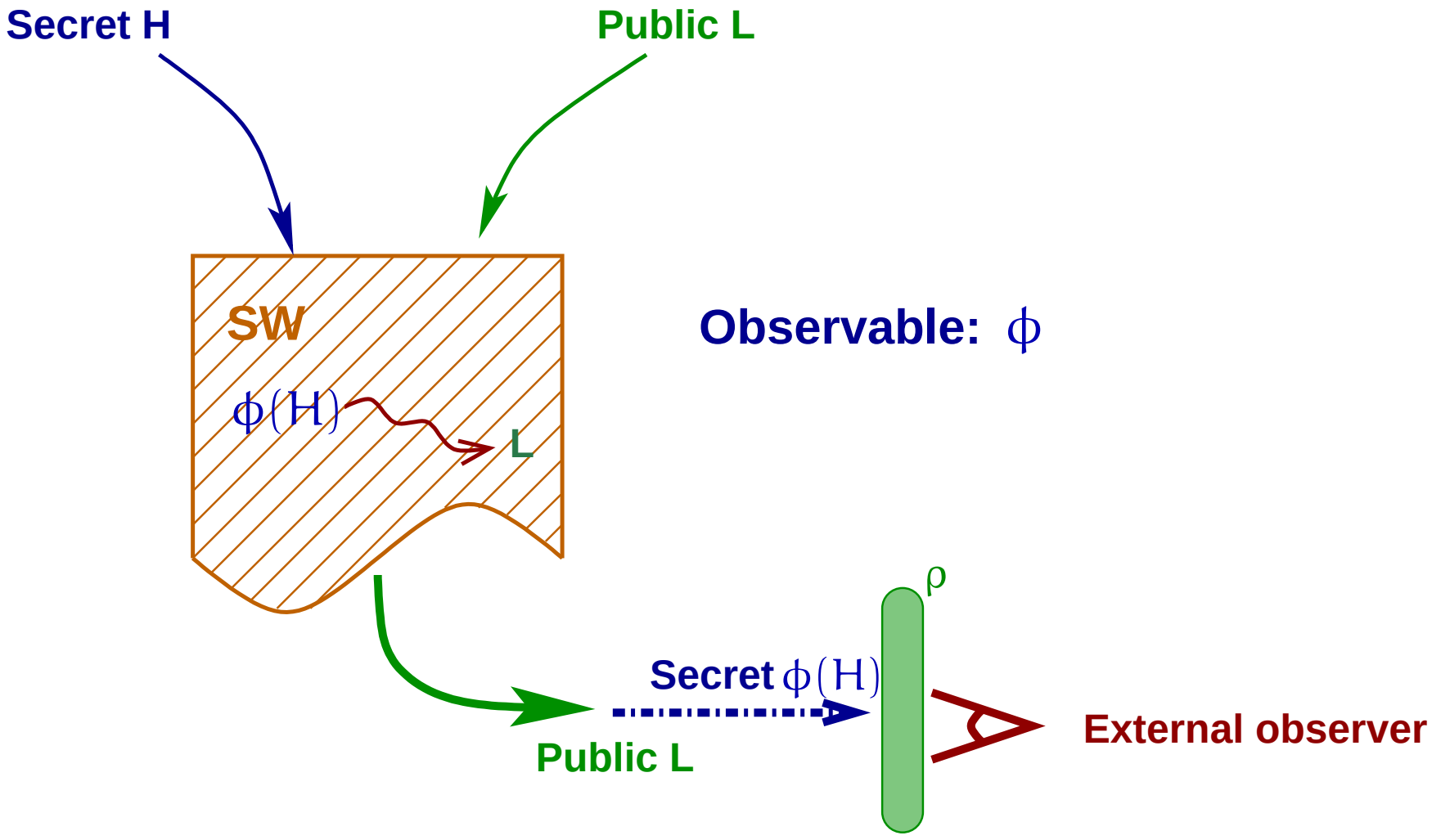
Abstracting Non-Interference



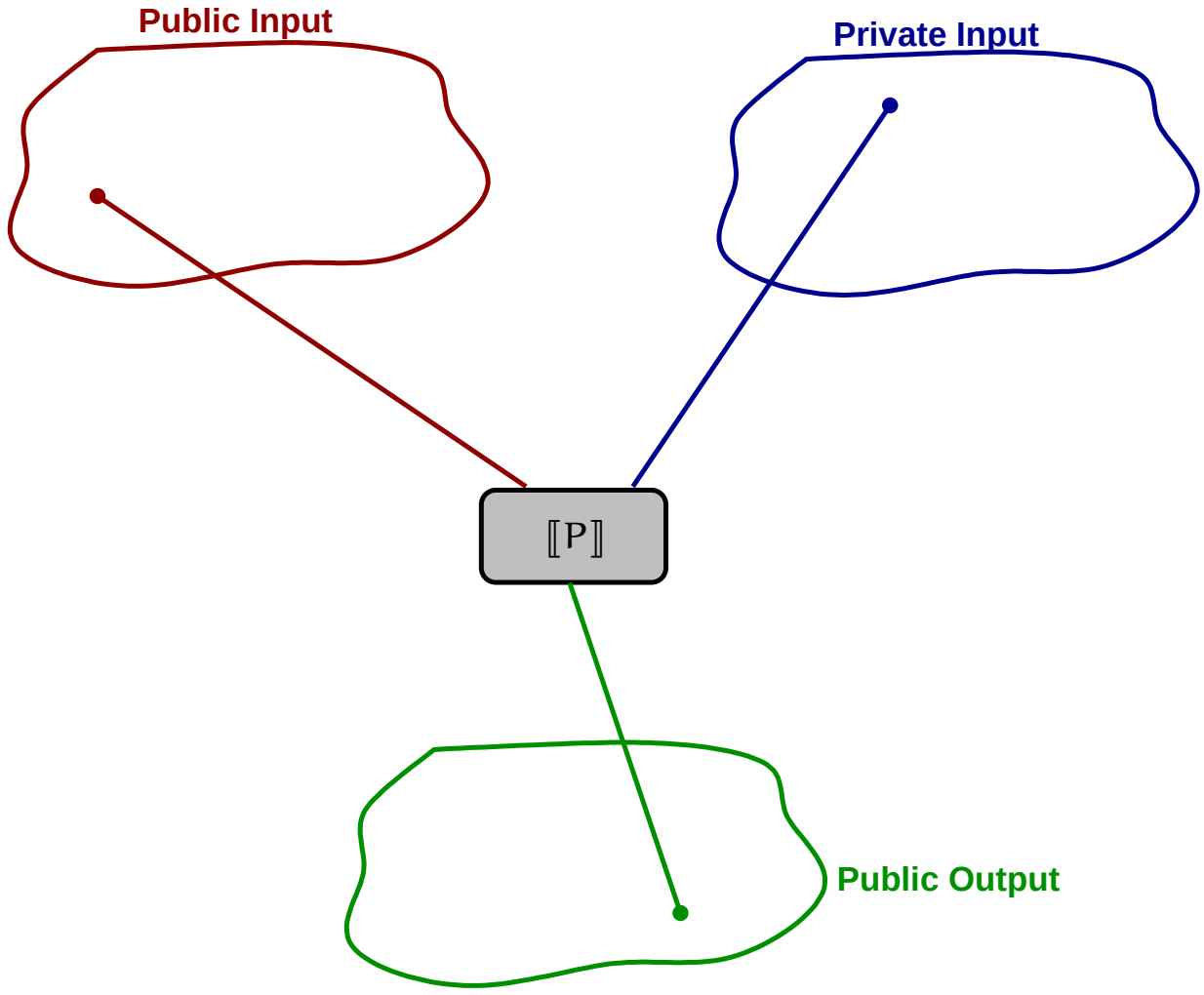
Abstracting Non-Interference



Abstracting Non-Interference

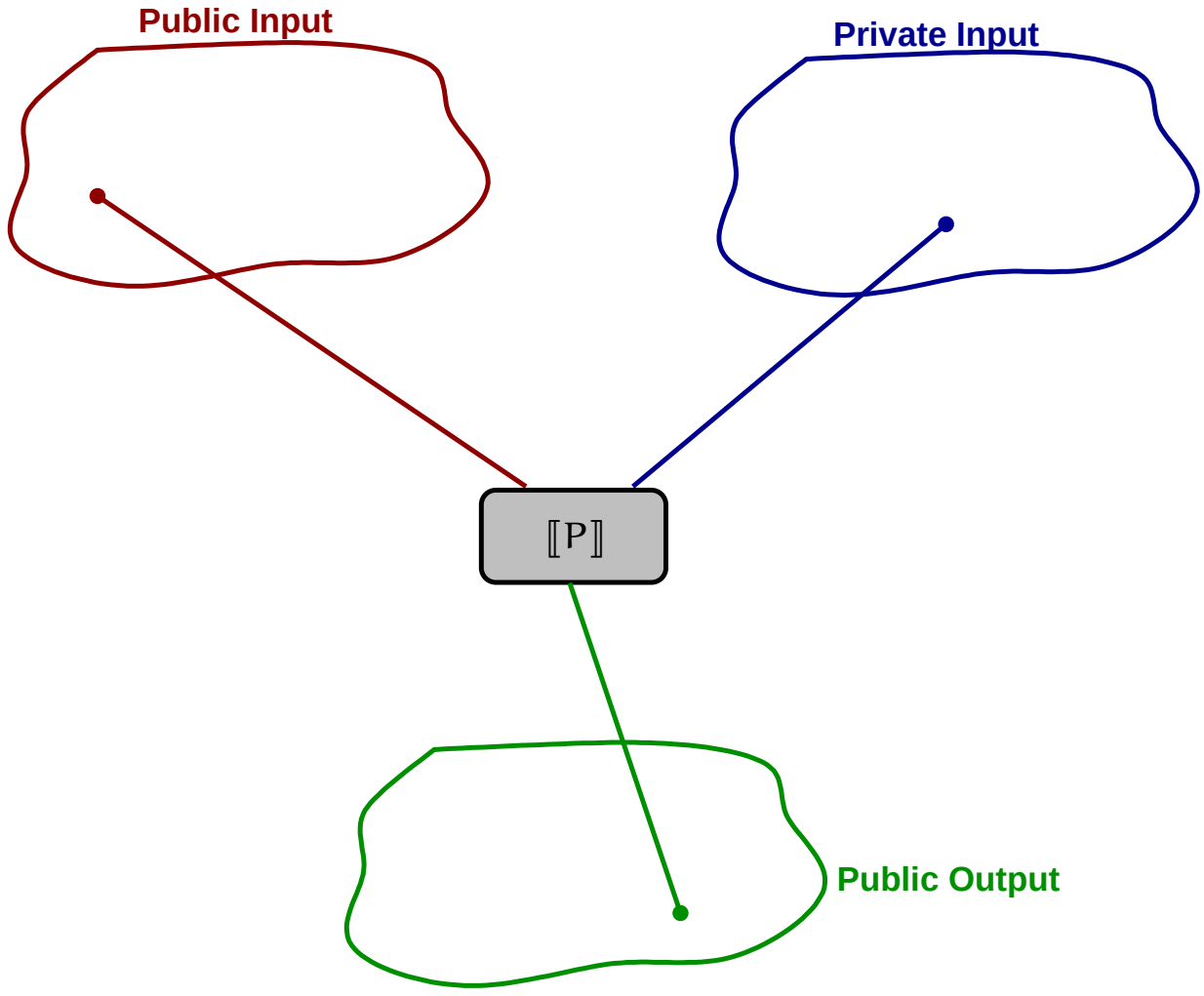


Standard non-interference



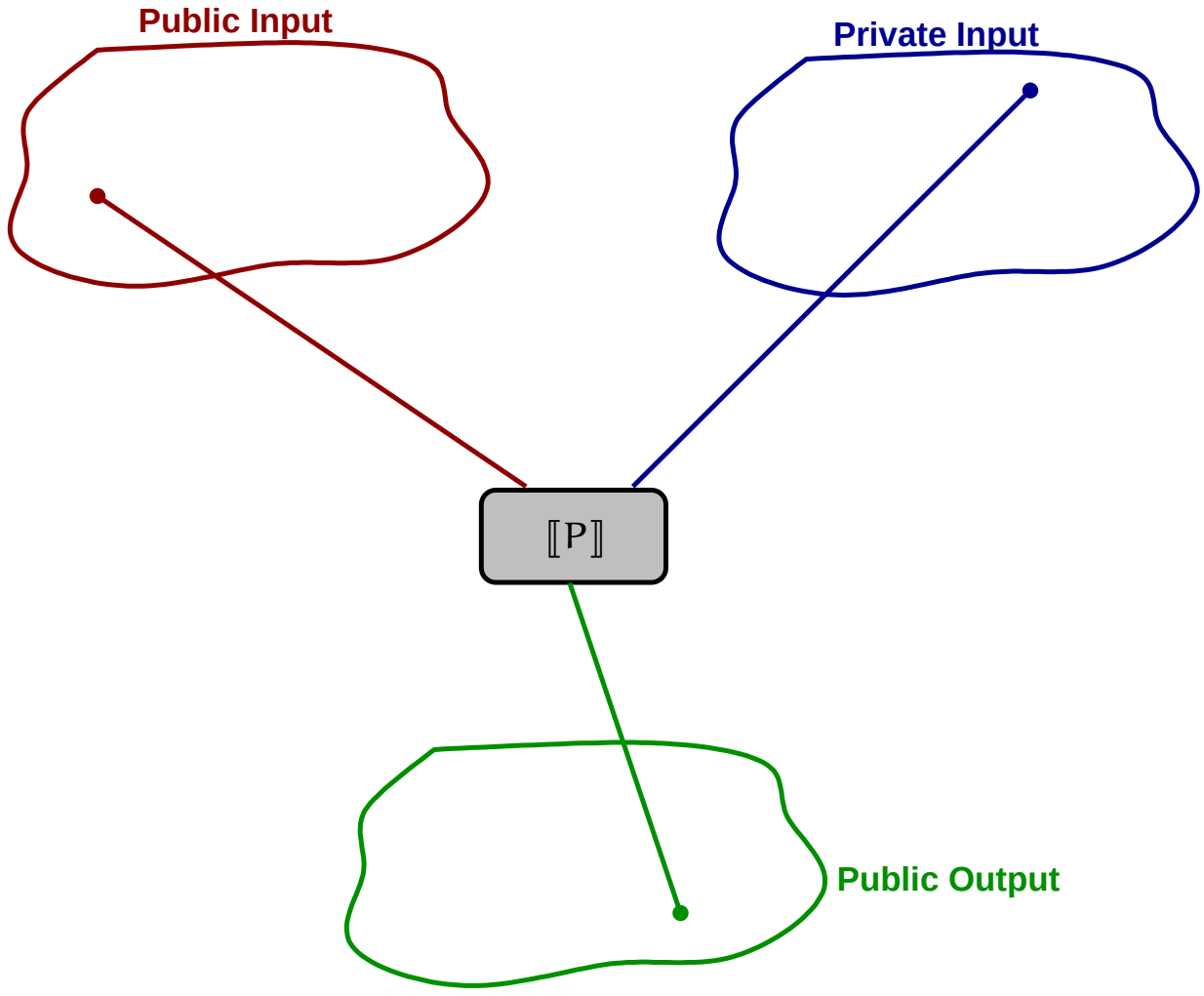
$$\forall l : \mathsf{L}, \forall h_1, h_2 : \mathsf{H}.\ [\![P]\!](h_1, l)^{\mathsf{L}} = [\![P]\!](h_2, l)^{\mathsf{L}}$$

Standard non-interference



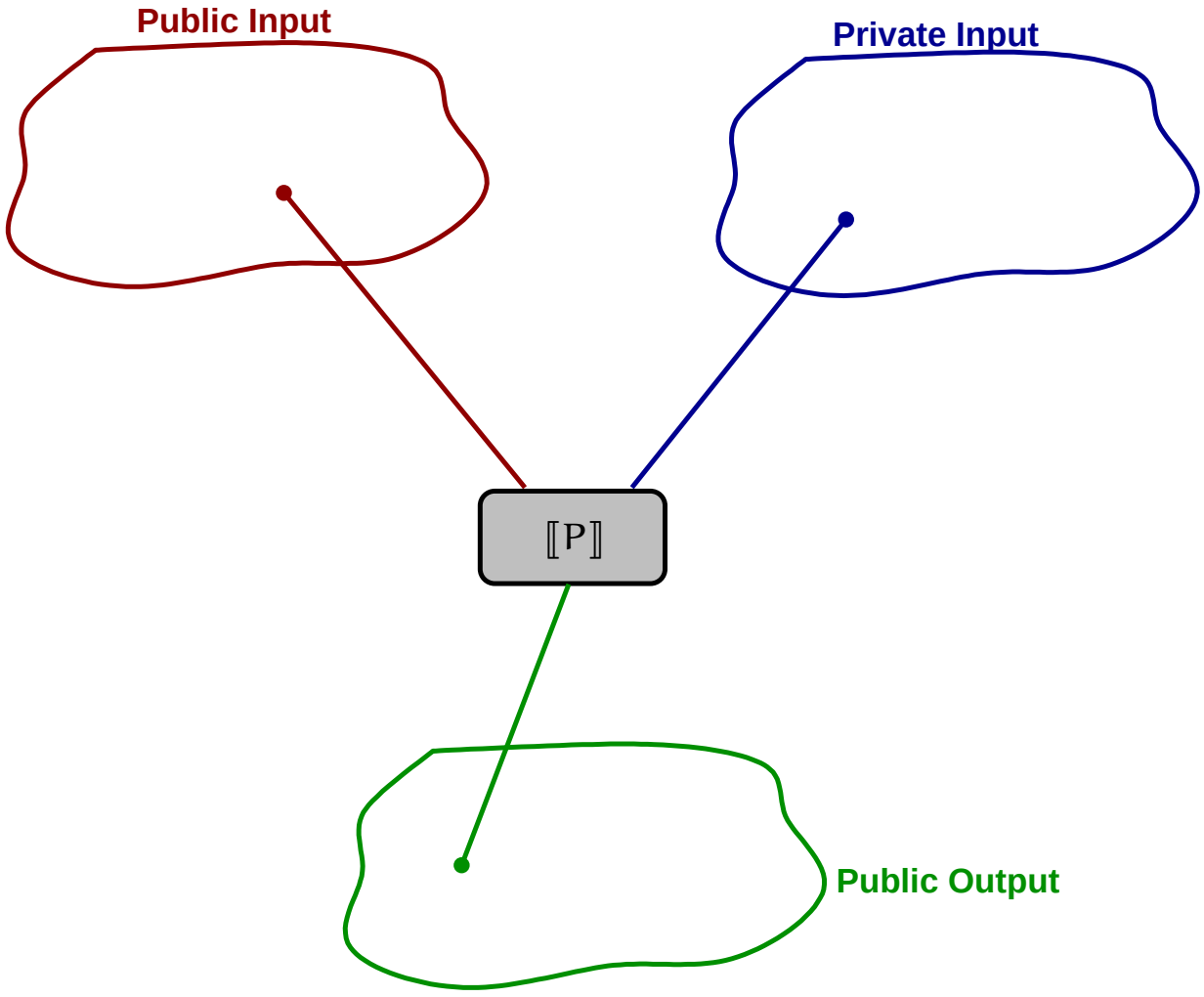
$$\forall l : \mathsf{L}, \forall h_1, h_2 : \mathsf{H}.\ [\![P]\!](h_1, l)^{\mathsf{L}} = [\![P]\!](h_2, l)^{\mathsf{L}}$$

Standard non-interference



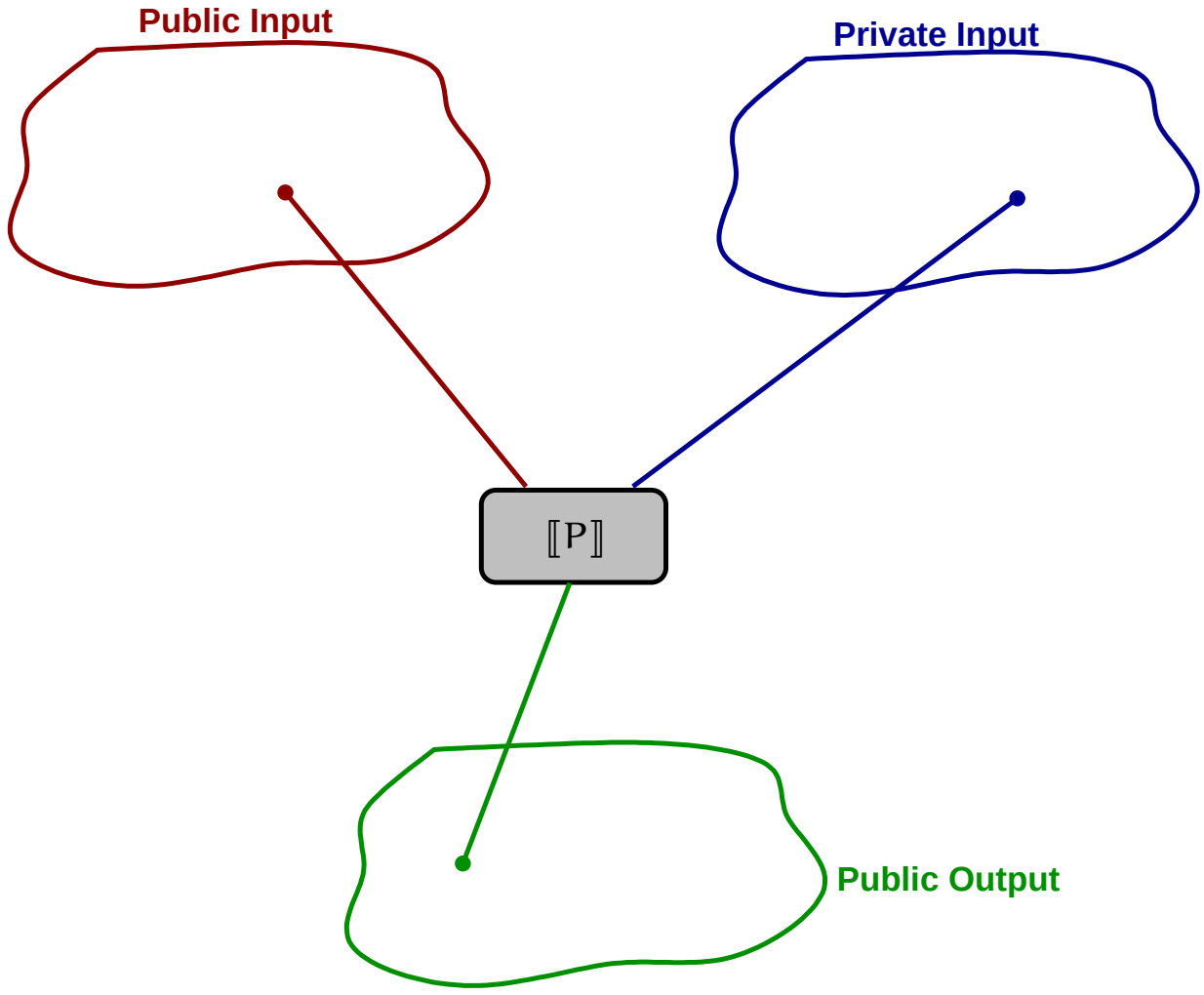
$$\forall l : \mathsf{L}, \forall h_1, h_2 : \mathsf{H}.\ [\![P]\!](h_1, l)^{\mathsf{L}} = [\![P]\!](h_2, l)^{\mathsf{L}}$$

Standard non-interference



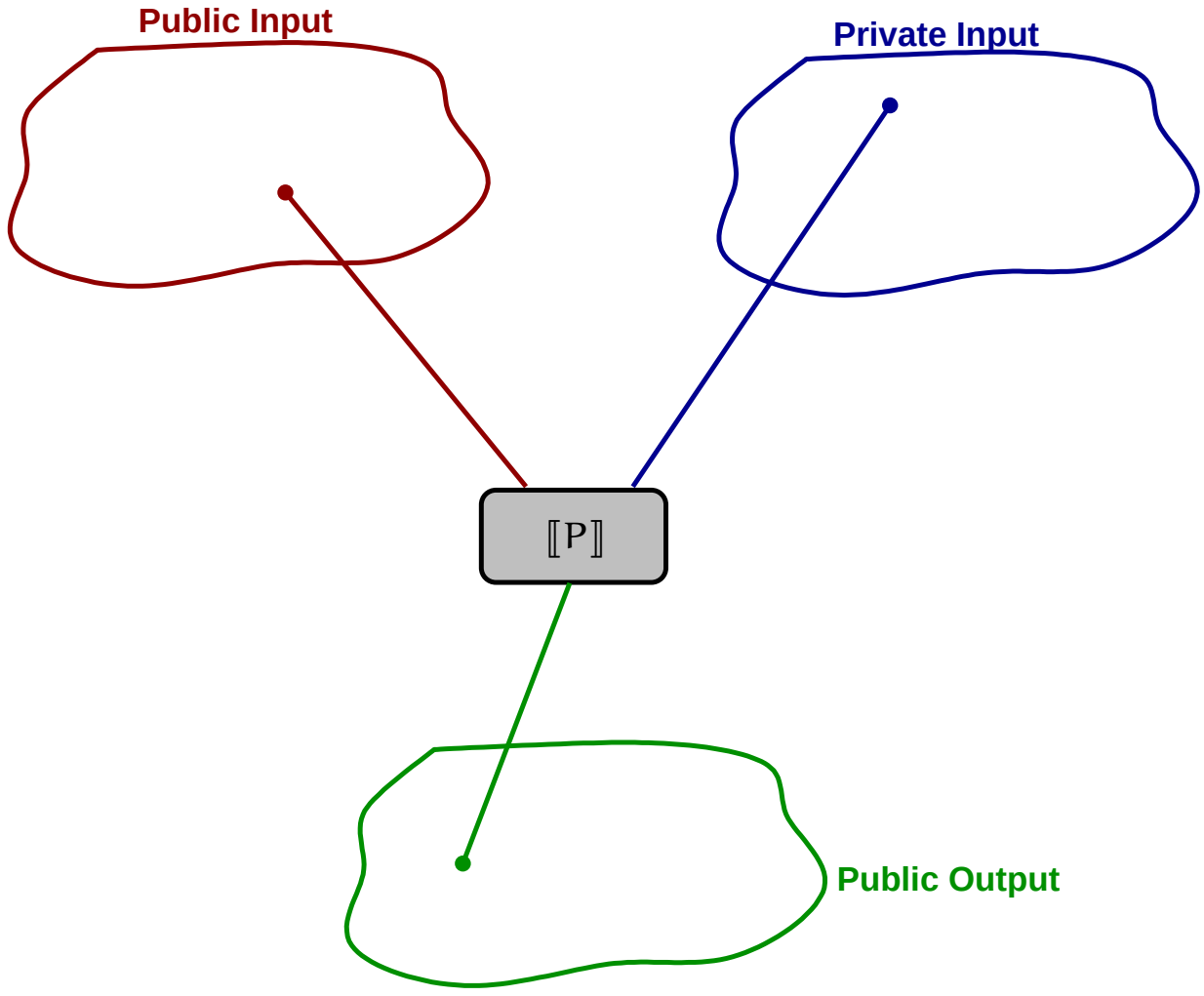
$$\forall l : \mathsf{L}, \forall h_1, h_2 : \mathsf{H}.\ [\![P]\!](h_1, l)^{\mathsf{L}} = [\![P]\!](h_2, l)^{\mathsf{L}}$$

Standard non-interference



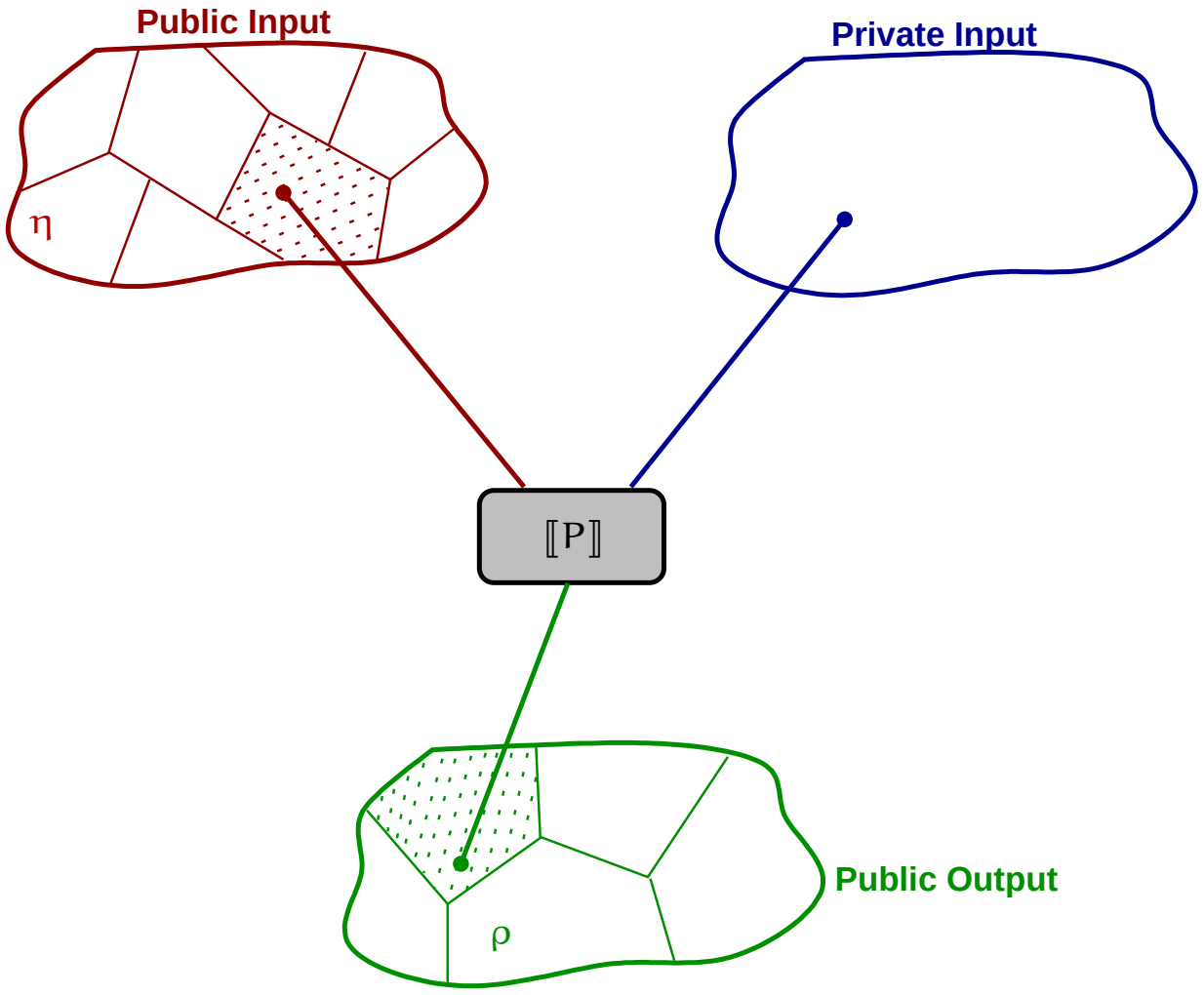
$$\forall l : \mathsf{L}, \forall h_1, h_2 : \mathsf{H}.\ [\![P]\!](h_1, l)^{\mathsf{L}} = [\![P]\!](h_2, l)^{\mathsf{L}}$$

Standard non-interference



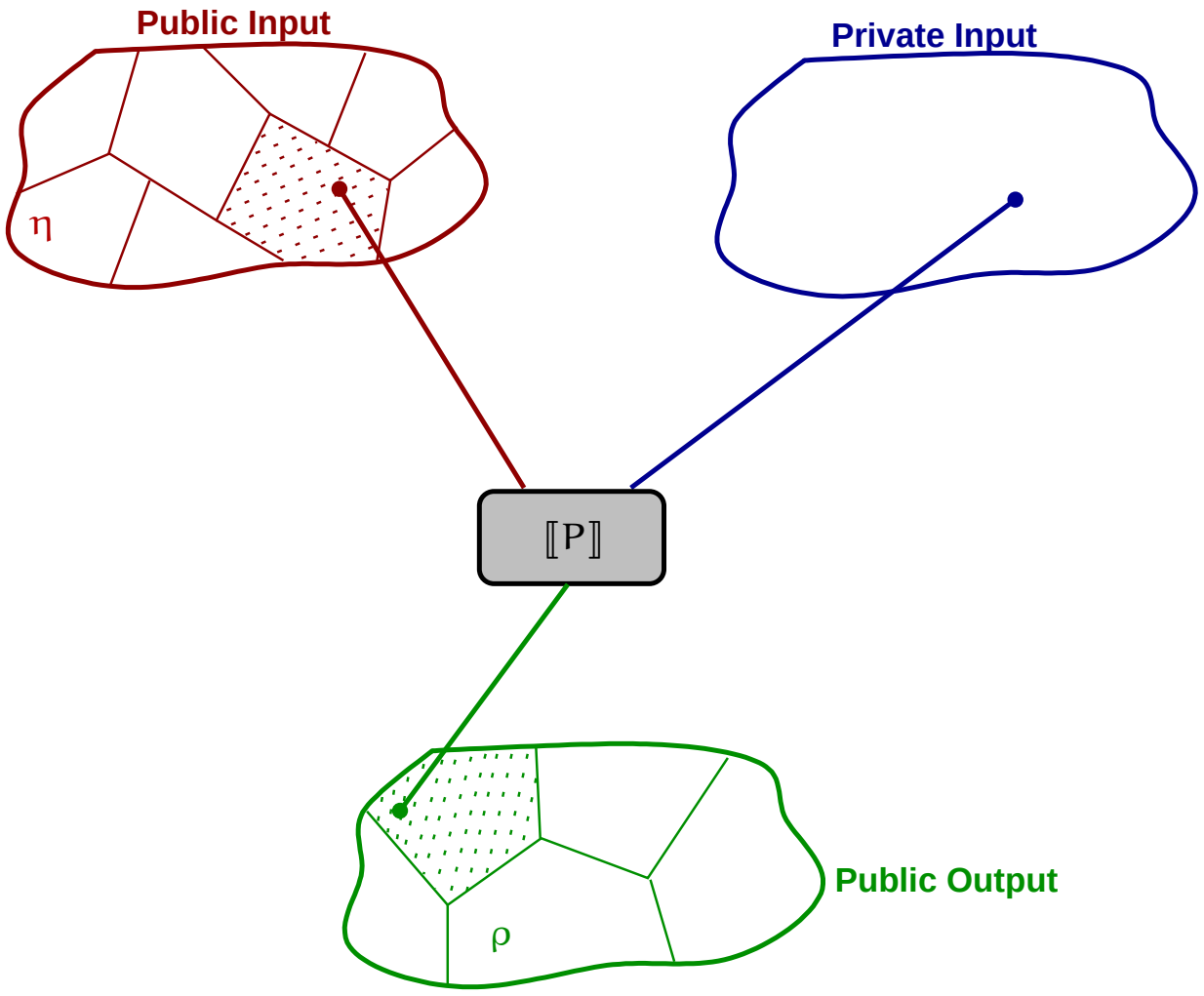
$$\forall l : \mathsf{L}, \forall h_1, h_2 : \mathsf{H}.\ [\![P]\!](h_1, l)^{\mathsf{L}} = [\![P]\!](h_2, l)^{\mathsf{L}}$$

Abstracting non-interference I: Narrow ANI



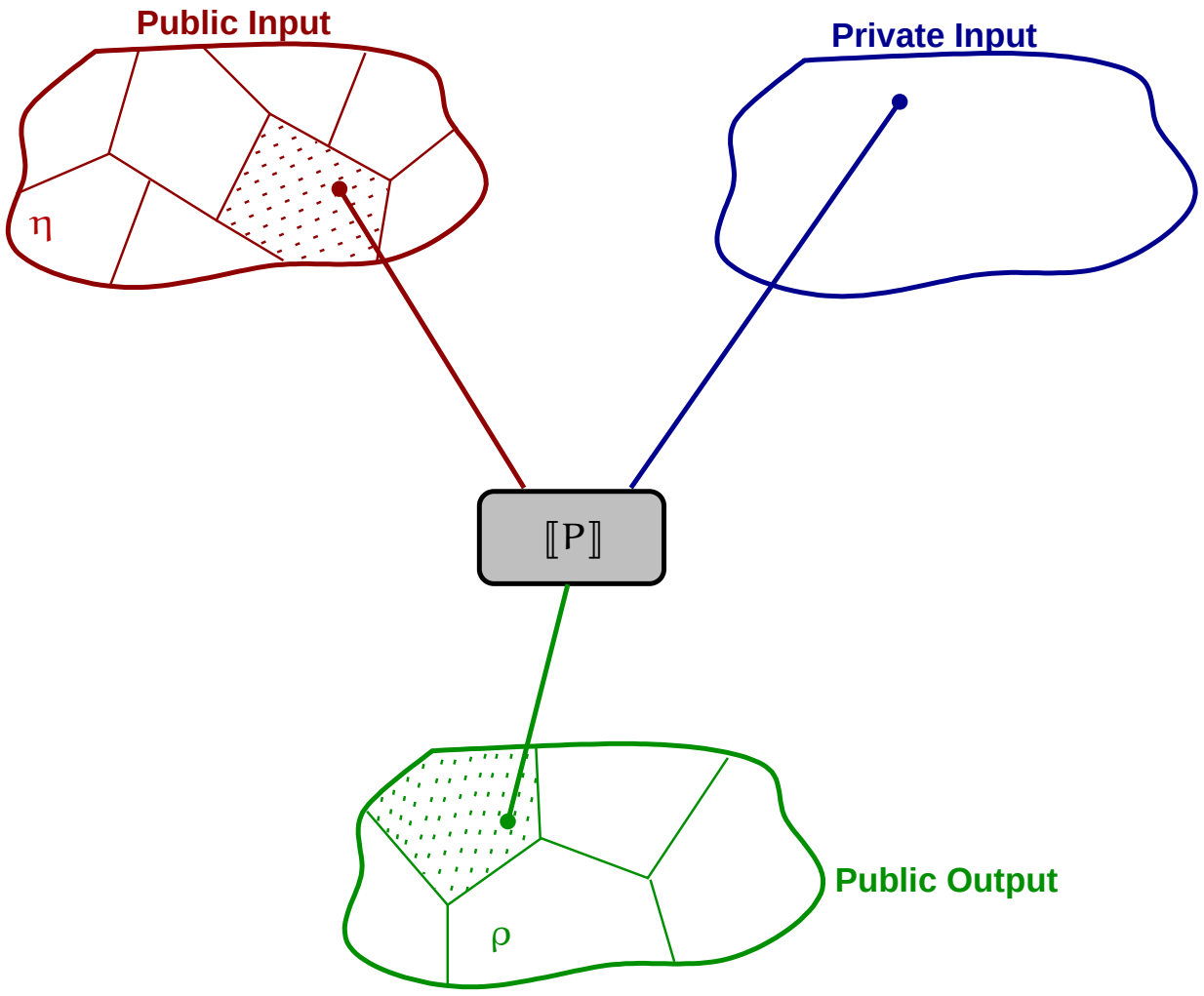
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})) \colon [\eta]\mathrm{P}(\rho) \colon \eta(l_1) = \eta(l_2) \Rightarrow \rho([\![\mathrm{P}]\!](h_1, l_1)^{\mathsf{L}}) = \rho([\![\mathrm{P}]\!](h_2, l_2)^{\mathsf{L}})$$

Abstracting non-interference I: Narrow ANI



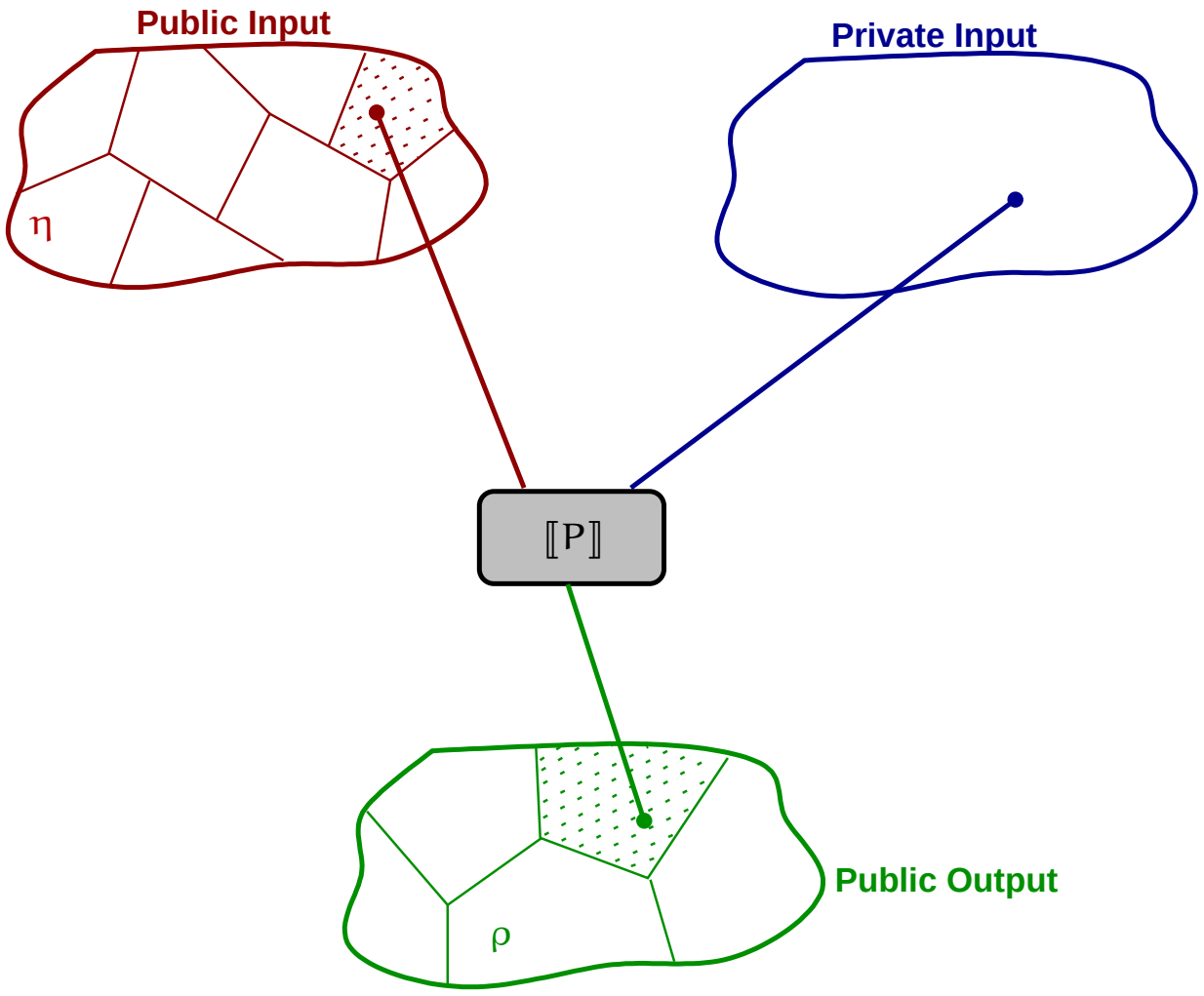
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})) \colon [\eta]\mathrm{P}(\rho) \colon \eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket \mathrm{P} \rrbracket(h_1, l_1)^{\mathsf{L}}) = \rho(\llbracket \mathrm{P} \rrbracket(h_2, l_2)^{\mathsf{L}})$$

Abstracting non-interference I: Narrow ANI



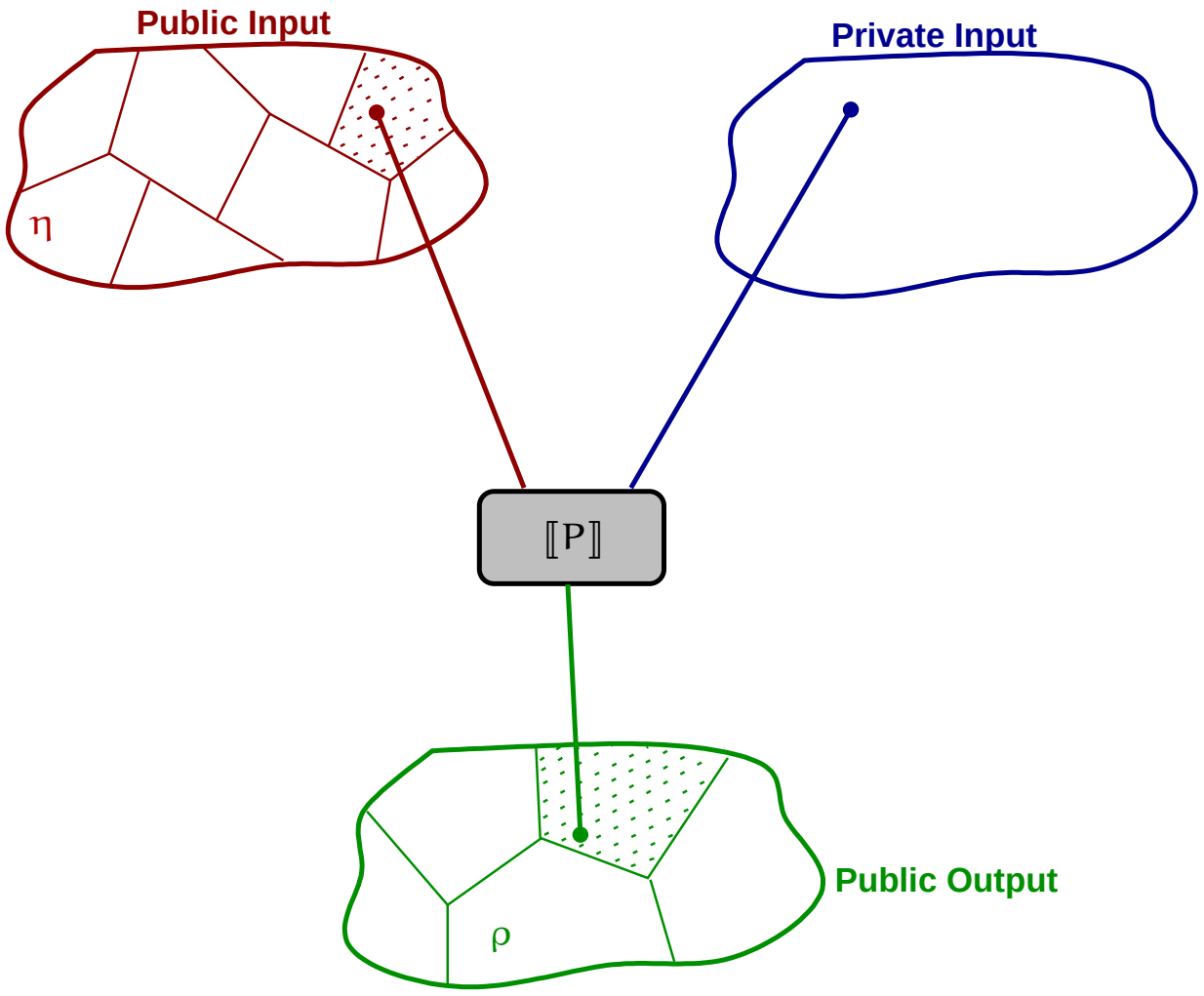
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})) \colon [\eta]\mathrm{P}(\rho) \colon \eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket \mathrm{P} \rrbracket(h_1, l_1)^{\mathsf{L}}) = \rho(\llbracket \mathrm{P} \rrbracket(h_2, l_2)^{\mathsf{L}})$$

Abstracting non-interference I: Narrow ANI



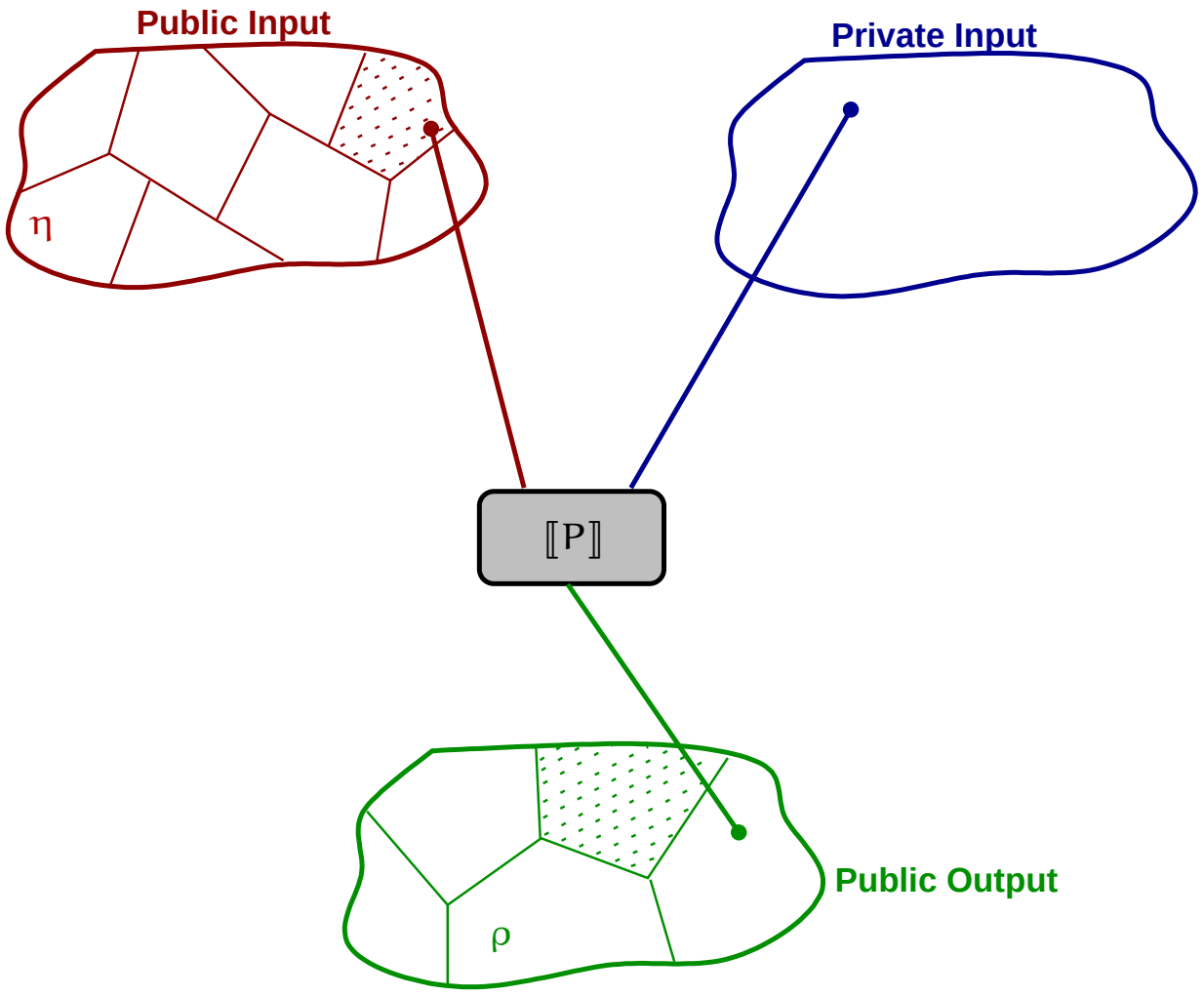
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})) \colon [\eta]\mathrm{P}(\rho) \colon \eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket \mathrm{P} \rrbracket(h_1, l_1)^{\mathsf{L}}) = \rho(\llbracket \mathrm{P} \rrbracket(h_2, l_2)^{\mathsf{L}})$$

Abstracting non-interference I: Narrow ANI



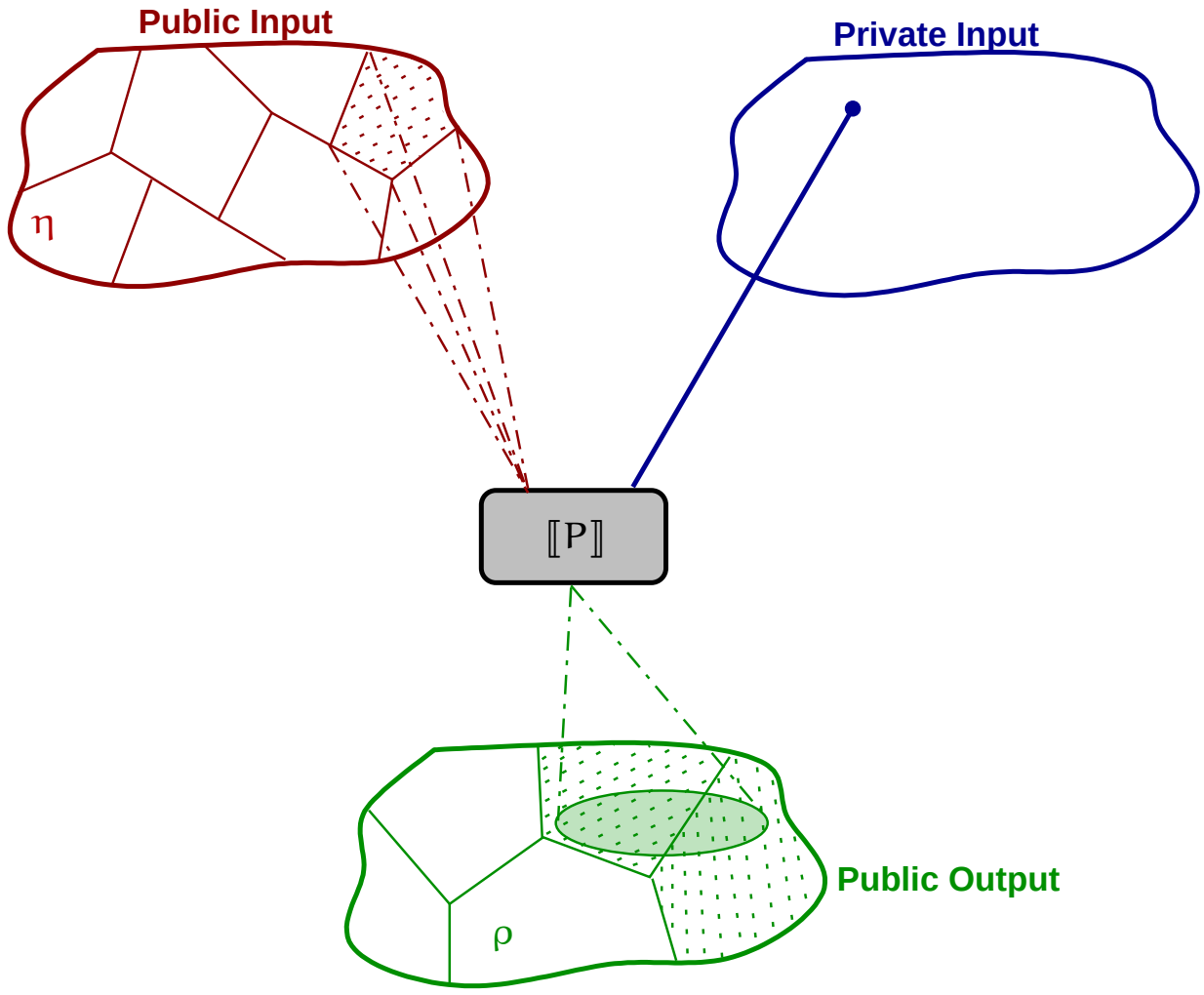
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})) \colon [\eta]\mathrm{P}(\rho) \colon \eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket \mathrm{P} \rrbracket(h_1, l_1)^{\mathsf{L}}) = \rho(\llbracket \mathrm{P} \rrbracket(h_2, l_2)^{\mathsf{L}})$$

Abstracting non-interference I: Narrow ANI



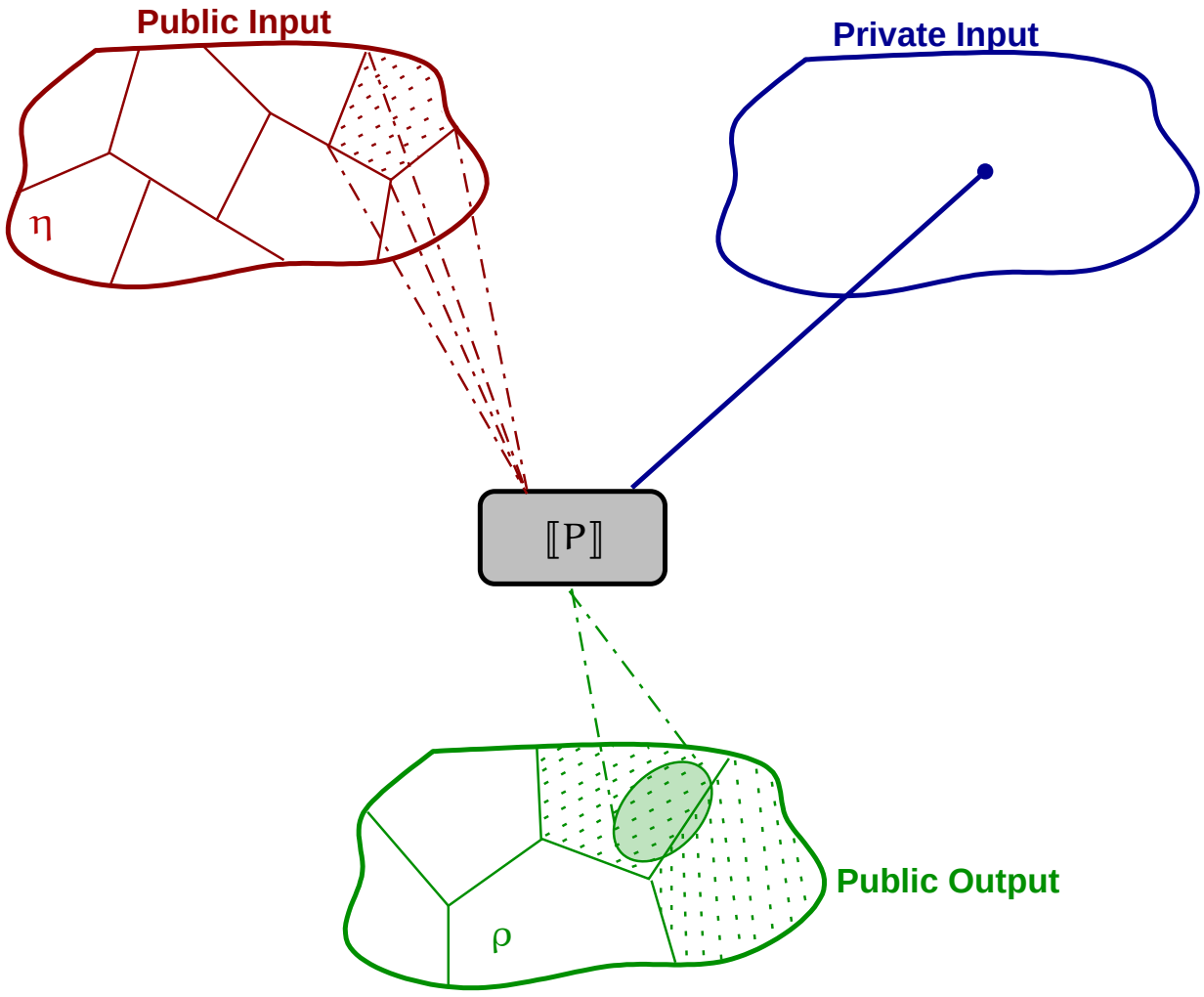
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})) \colon [\eta]\mathrm{P}(\rho) \colon \eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket \mathrm{P} \rrbracket(h_1, l_1)^{\mathsf{L}}) = \rho(\llbracket \mathrm{P} \rrbracket(h_2, l_2)^{\mathsf{L}})$$

Abstracting non-interference II



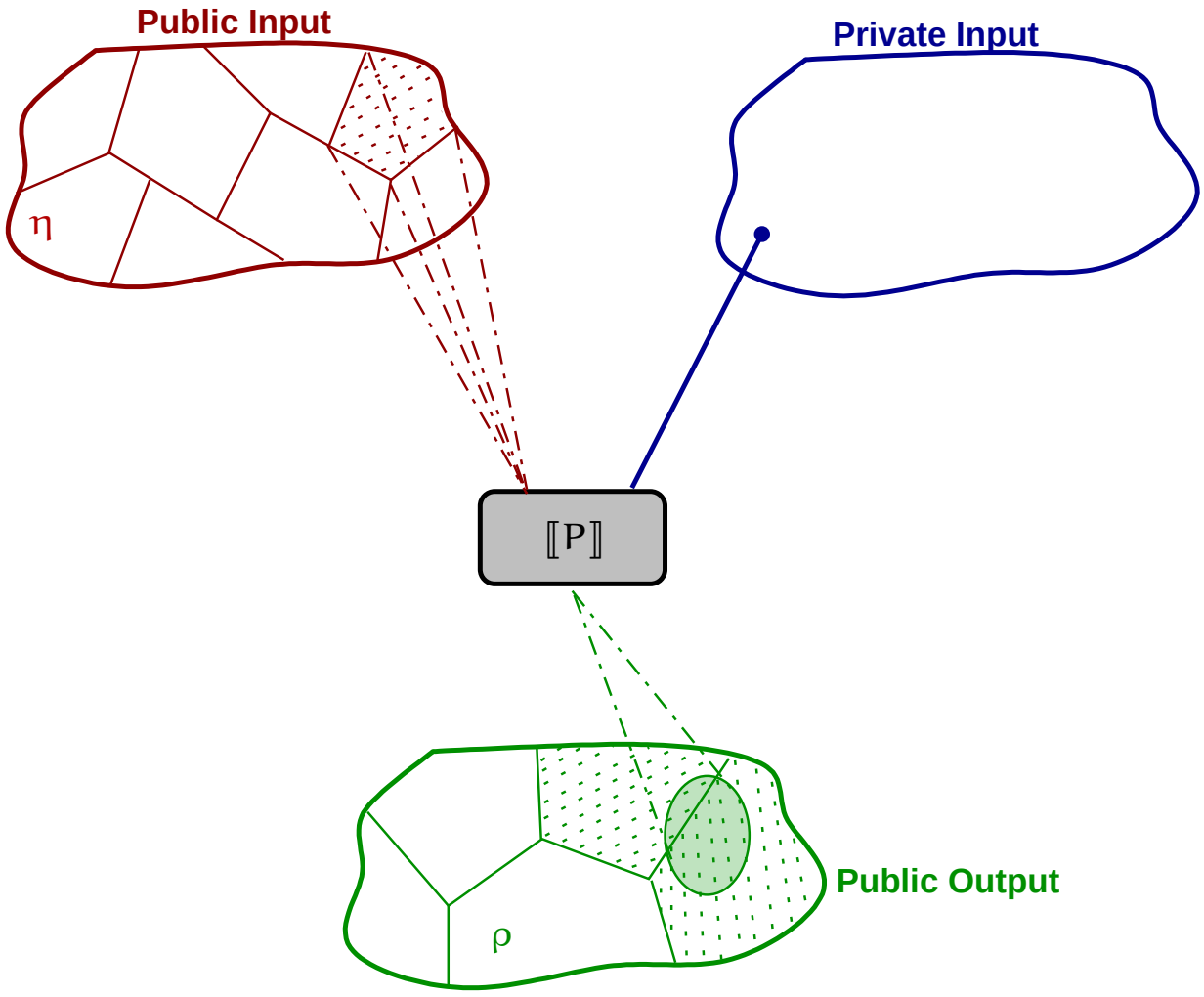
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})) \colon (\eta)\mathrm{P}(\rho) \colon$$
$$\eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket \mathrm{P} \rrbracket(h_1, \eta(l_1))^{\mathsf{L}}) = \rho(\llbracket \mathrm{P} \rrbracket(h_2, \eta(l_2))^{\mathsf{L}})$$

Abstracting non-interference II



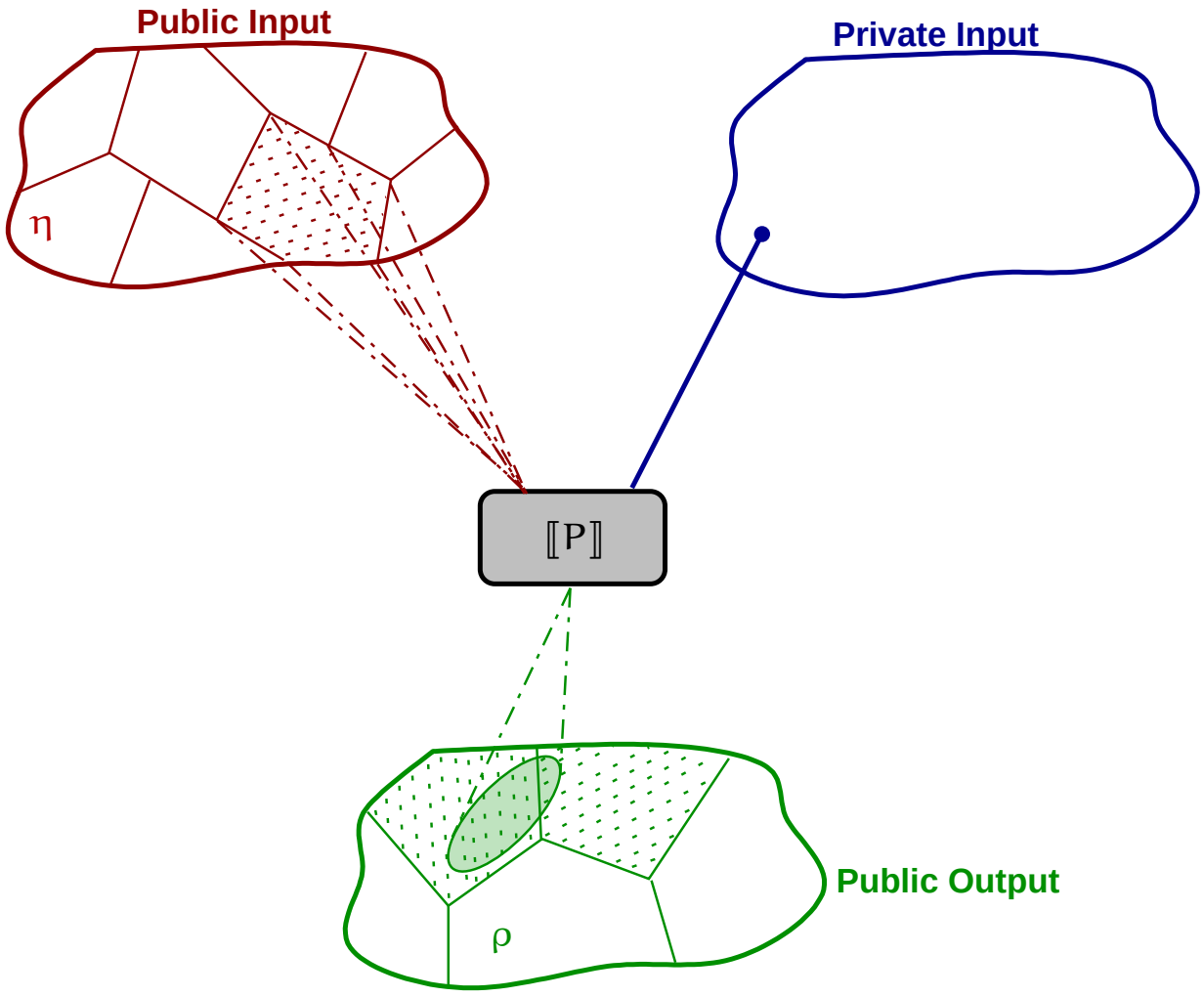
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})) \colon (\eta)\mathrm{P}(\rho) \colon$$
$$\eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket \mathrm{P} \rrbracket(h_1, \eta(l_1))^{\mathsf{L}}) = \rho(\llbracket \mathrm{P} \rrbracket(h_2, \eta(l_2))^{\mathsf{L}})$$

Abstracting non-interference II



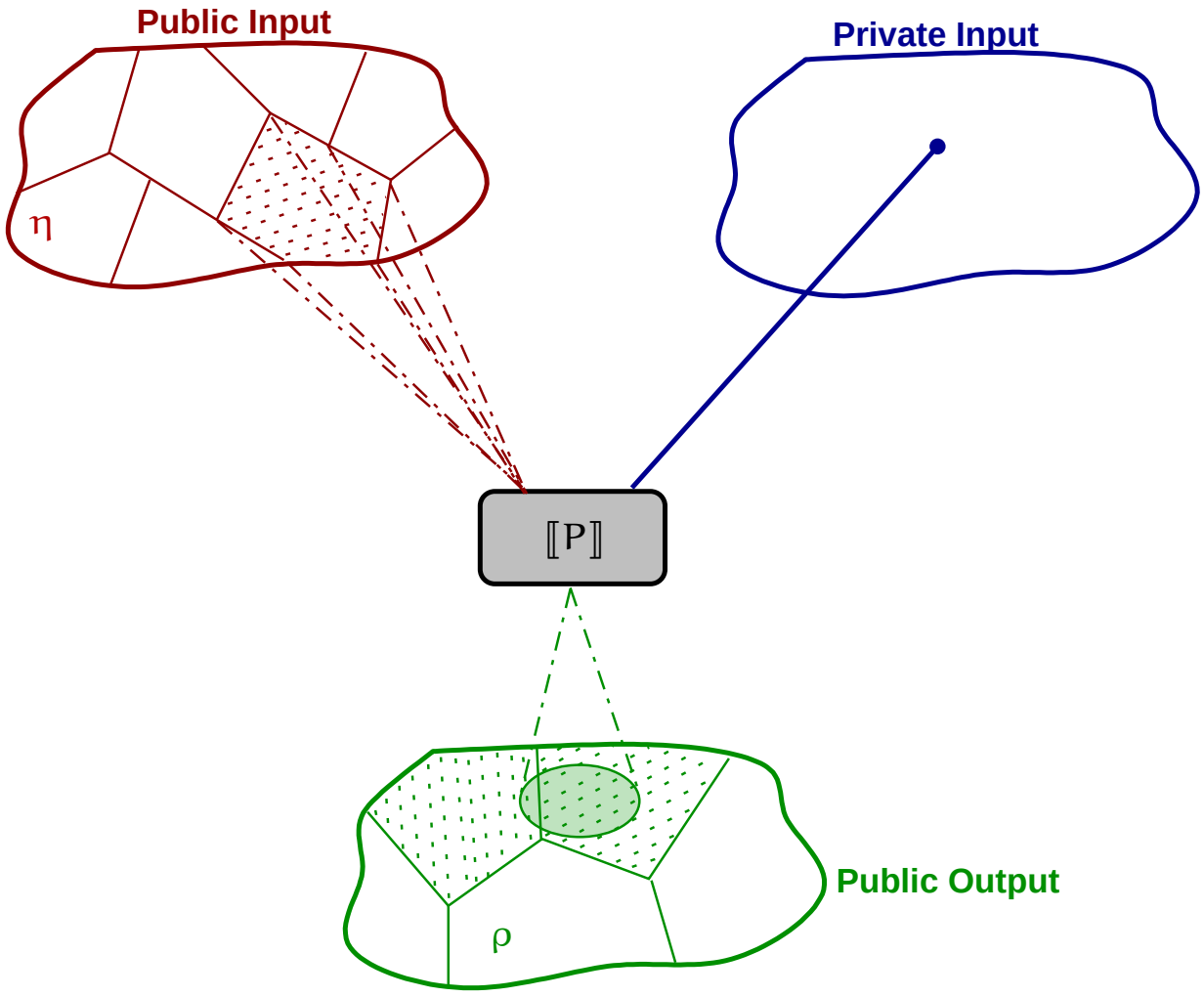
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})) \colon (\eta)\mathrm{P}(\rho) \colon$$
$$\eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket \mathrm{P} \rrbracket(h_1, \eta(l_1))^{\mathsf{L}}) = \rho(\llbracket \mathrm{P} \rrbracket(h_2, \eta(l_2))^{\mathsf{L}})$$

Abstracting non-interference II



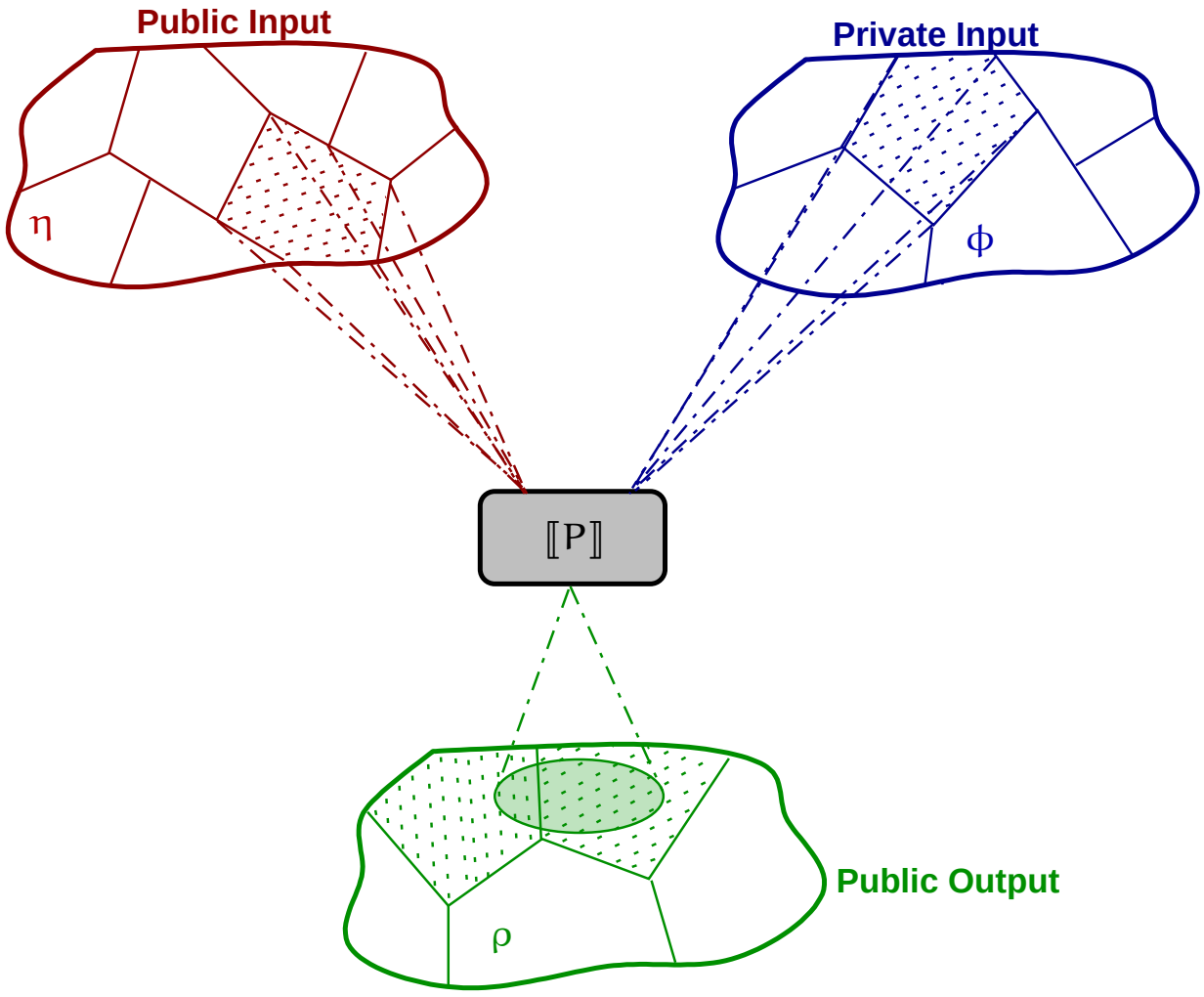
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})) \colon (\eta)\mathrm{P}(\rho) \colon$$
$$\eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket \mathrm{P} \rrbracket(h_1, \eta(l_1))^{\mathsf{L}}) = \rho(\llbracket \mathrm{P} \rrbracket(h_2, \eta(l_2))^{\mathsf{L}})$$

Abstracting non-interference II



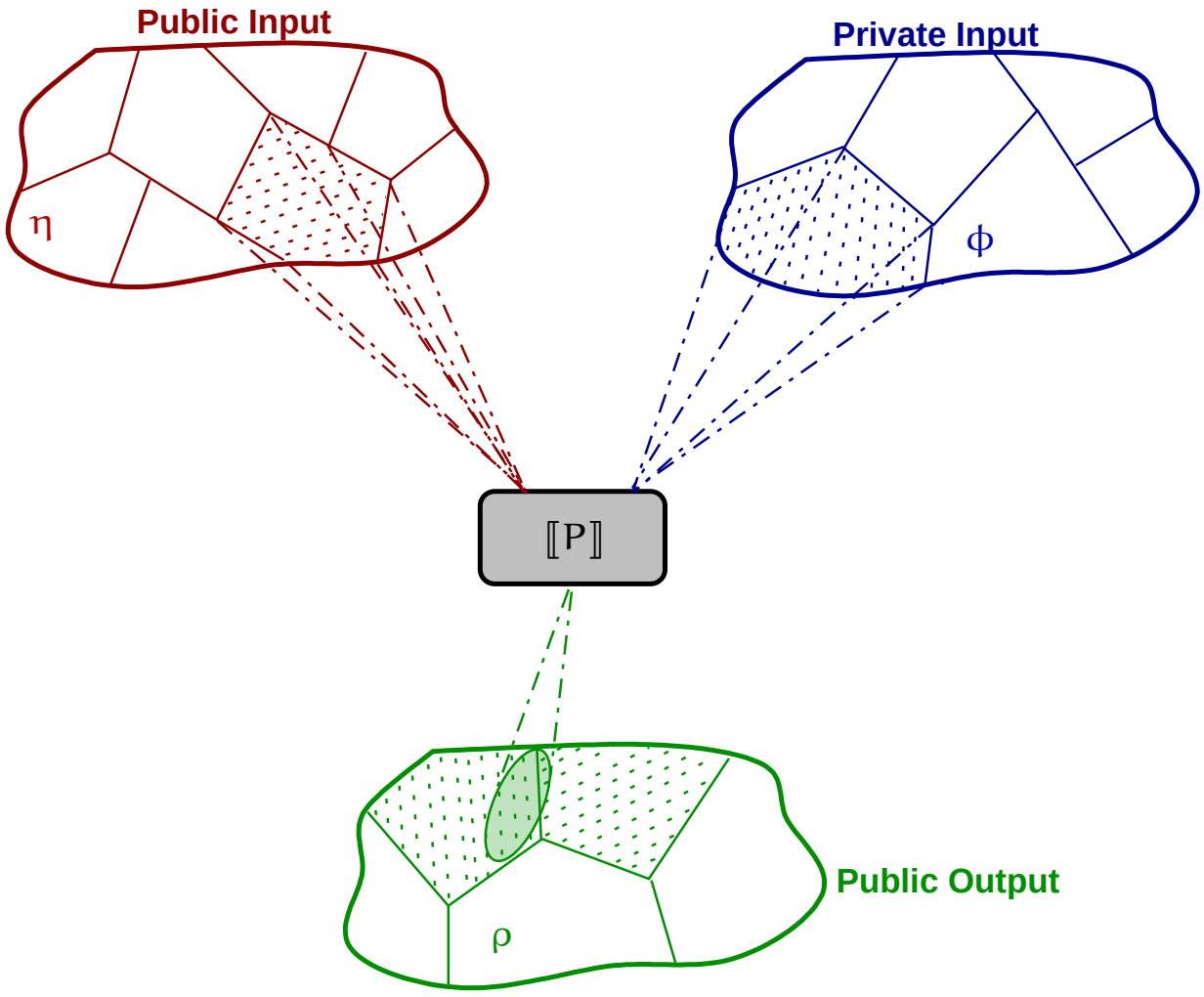
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})) \colon (\eta)\mathrm{P}(\rho) \colon$$
$$\eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket \mathrm{P} \rrbracket(h_1, \eta(l_1))^{\mathsf{L}}) = \rho(\llbracket \mathrm{P} \rrbracket(h_2, \eta(l_2))^{\mathsf{L}})$$

Abstracting non-interference III: ANI



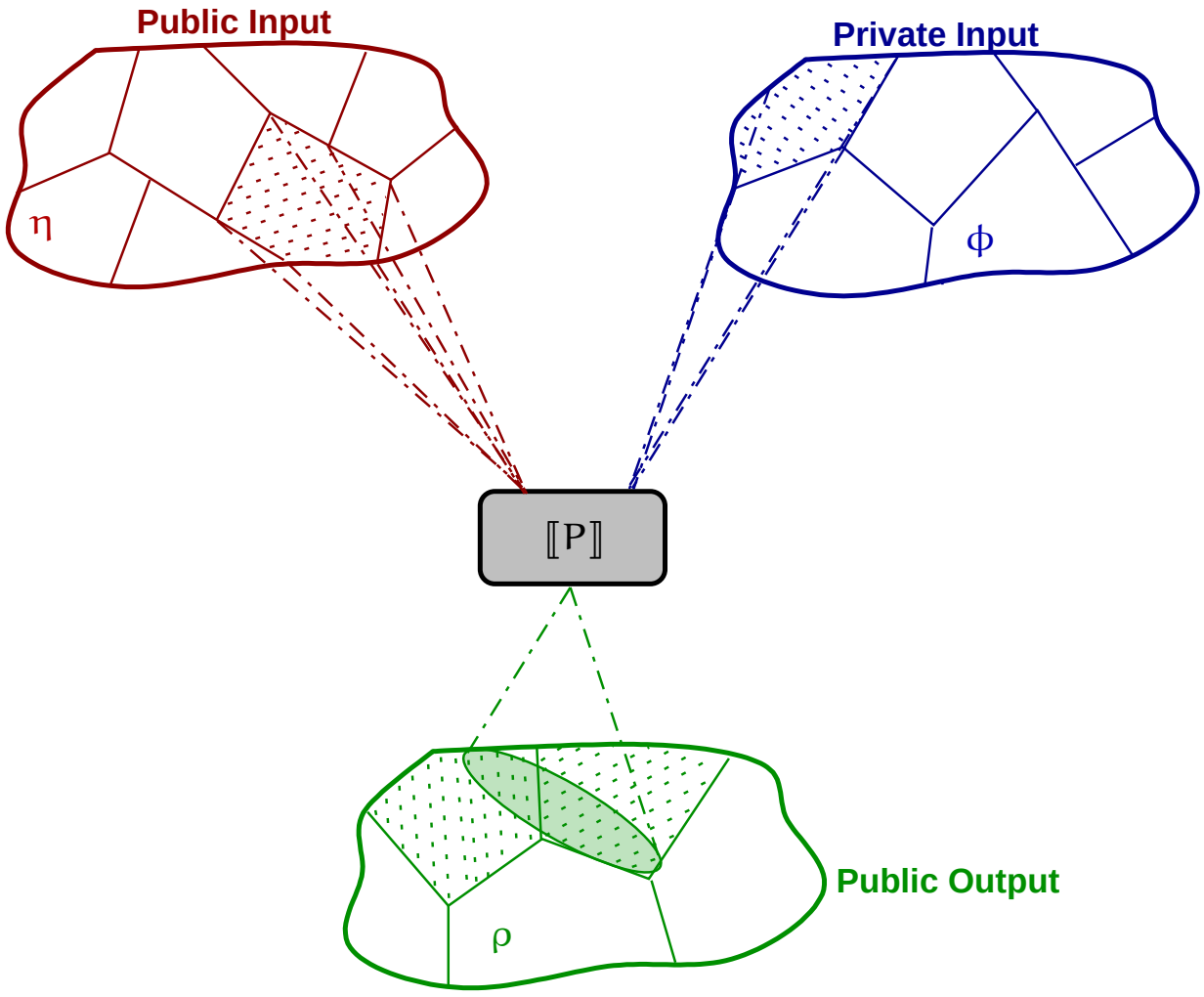
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})), \phi \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{H}})) \colon (\eta)\mathrm{P}(\phi \rightsquigarrow \rho) \colon$$
$$\eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket \mathrm{P} \rrbracket(\phi(h_1), \eta(l_1))^{\mathsf{L}}) = \rho(\llbracket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

Abstracting non-interference III: ANI



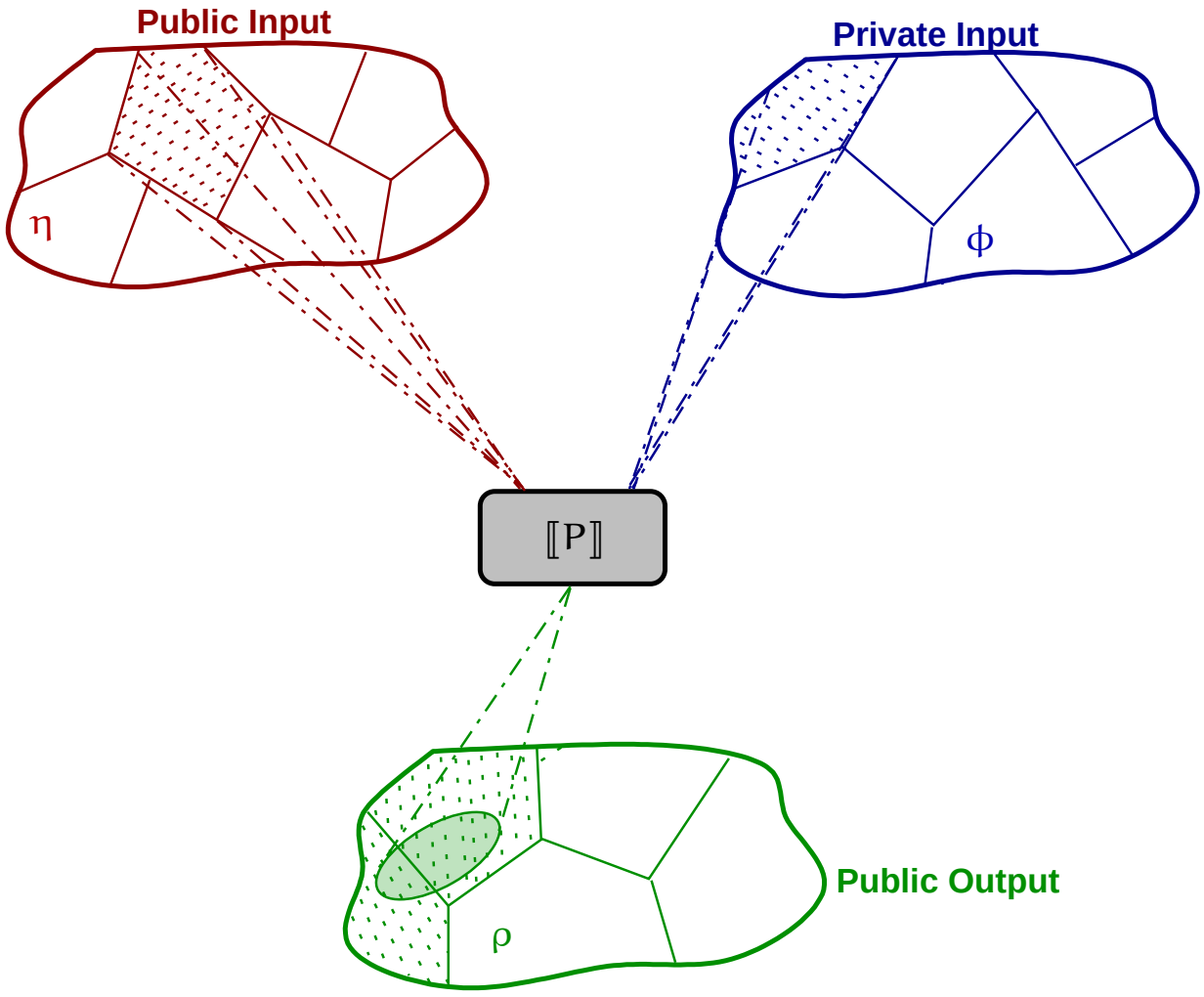
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})), \phi \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{H}})) \colon (\eta)\mathrm{P}(\phi \rightsquigarrow \rho) \colon$$
$$\eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket \mathrm{P} \rrbracket(\phi(h_1), \eta(l_1))^{\mathsf{L}}) = \rho(\llbracket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

Abstracting non-interference III: ANI



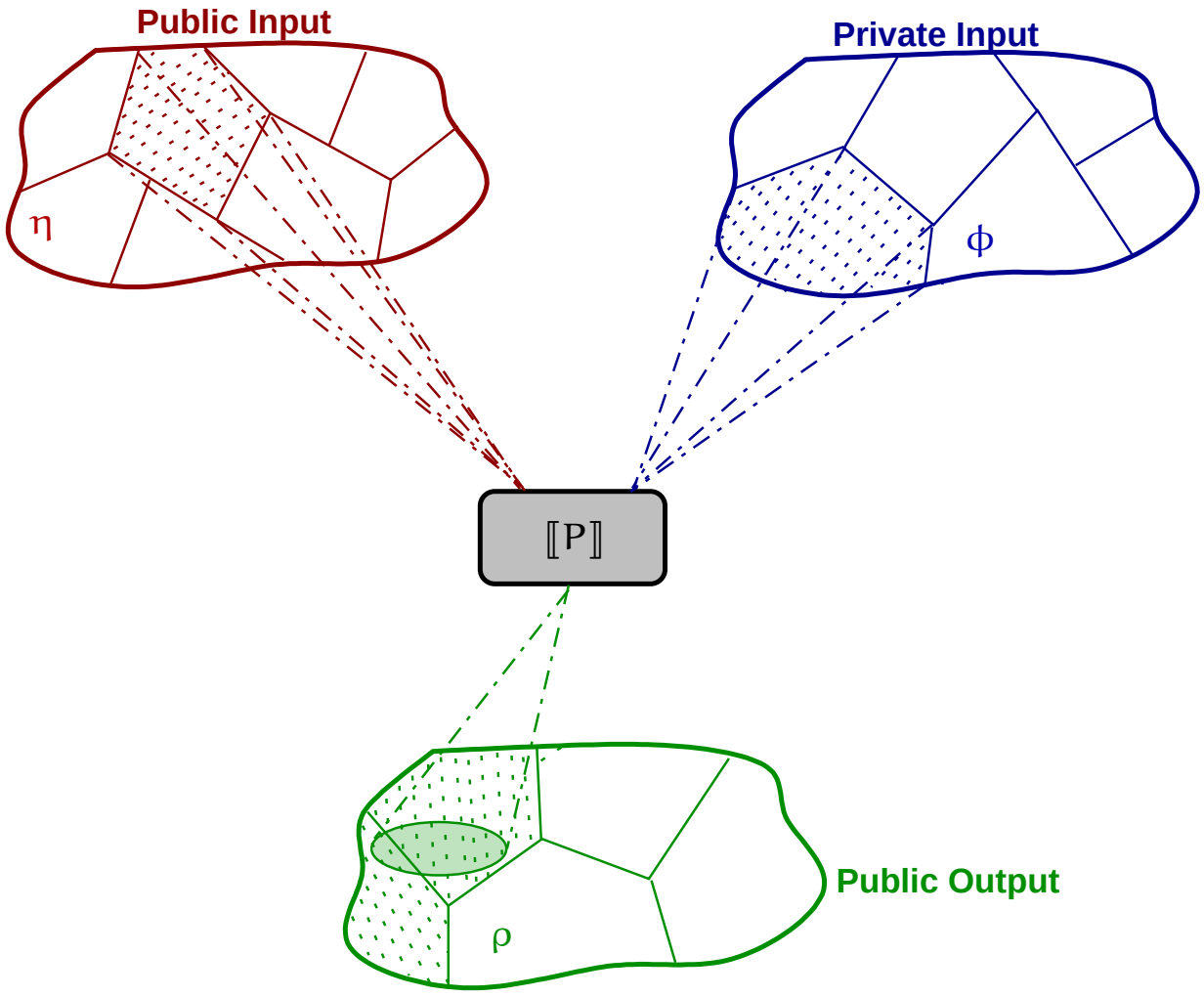
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})), \phi \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{H}})) \colon (\eta)\mathrm{P}(\phi \rightsquigarrow \rho) \colon$$
$$\eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket P \rrbracket(\phi(h_1), \eta(l_1))^{\mathsf{L}}) = \rho(\llbracket P \rrbracket(\phi(h_2),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

Abstracting non-interference III: ANI



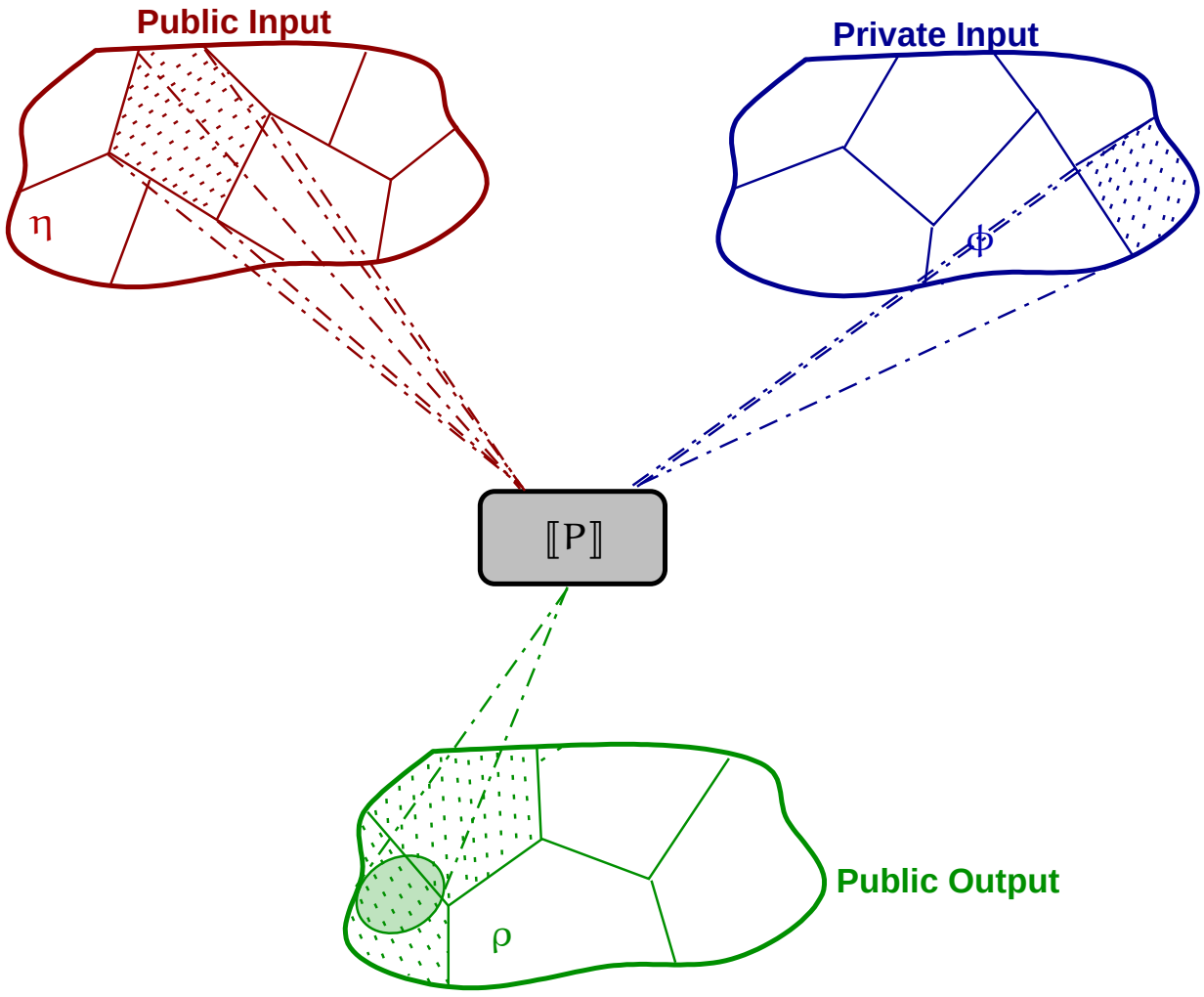
$$\rho,\eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})),\phi \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{H}})):\ (\eta)\mathrm{P}(\phi \rightsquigarrow \rho):$$
$$\eta(l_1)=\eta(l_2) \Rightarrow \rho([\![\mathrm{P}]\!](\phi(h_1),\eta(l_1))^{\mathsf{L}})=\rho([\![\mathrm{P}]\!](\phi(h_2),\eta(l_2))^{\mathsf{L}})$$

Abstracting non-interference III: ANI



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

Abstracting non-interference III: ANI



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

Deriving output attackers

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

Designing abstractions = designing attackers

Deriving output attackers

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

Designing abstractions = designing attackers

- Characterize the most concrete ρ such that $(\eta)P(\phi \rightsquigarrow\!\!\!\!\!\!\rceil\rho)$

  [The most powerful *public observer*]

Deriving output attackers

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

Designing abstractions = designing attackers

- Characterize the most concrete ρ such that $(\eta)\mathrm{P}(\phi \rightsquigarrow\!\!\!\!\!\!\rceil\, \rho)$

  [The most powerful *public observer*]

$\Rightarrow$ This would provide a certificate for security with a fixed input observation.

Equivalence relation vs Closure Operators

Equivalence relations uniquely correspond to particular upper closure operators:

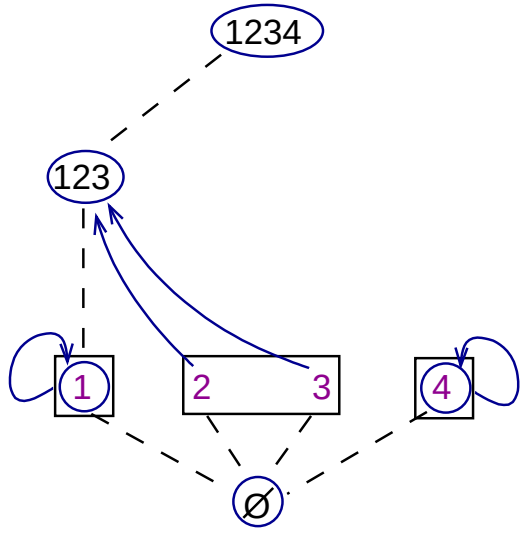
PARTITIONING
[Ranzato and Tapparo'04]

Equivalence relation vs Closure Operators

Equivalence relations uniquely correspond to particular upper closure operators:

PARTITIONING
[Ranzato and Tapparo'04]

- $\eta \in \mathit{uco}(\wp(C)) \Rightarrow \forall x, y.\, x \mathit{Rel}^{\eta} y$ iff $\eta(x) = \eta(y)$

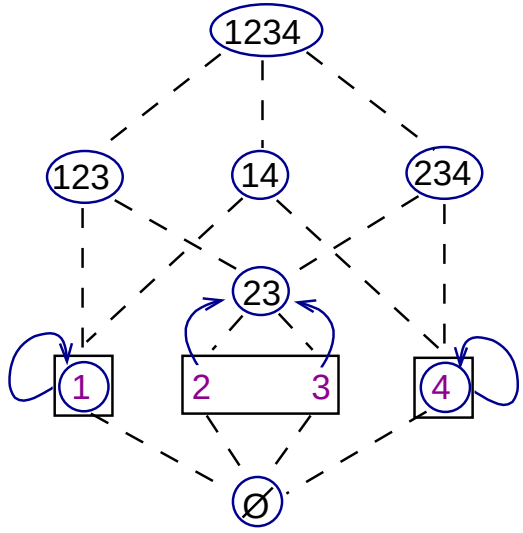


Equivalence relation vs Closure Operators

Equivalence relations uniquely correspond to particular upper closure operators:

PARTITIONING
[Ranzato and Tapparo'04]

- $\eta \in \mathit{uco}(\wp(C)) \Rightarrow \forall x, y.\, x \mathit{Rel}^{\eta} y$ iff $\eta(x) = \eta(y)$

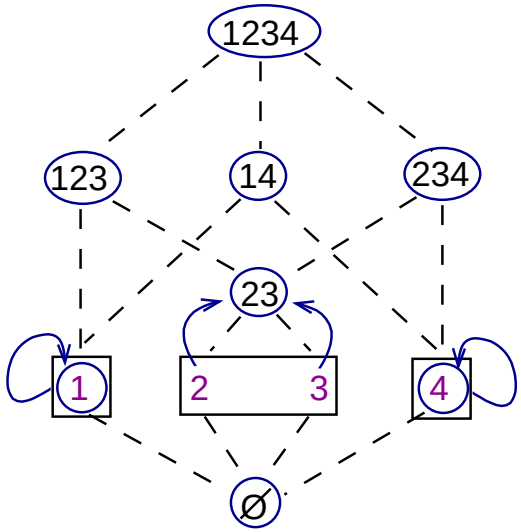


Equivalence relation vs Closure Operators

Equivalence relations uniquely correspond to particular upper closure operators:

PARTITIONING
[Ranzato and Tapparo'04]

- $\eta \in \mathit{uco}(\wp(C)) \Rightarrow \forall x, y.\, x \mathit{Rel}^{\eta} y$ iff $\eta(x) = \eta(y)$
- $R \in \mathit{Eq}(C) \Rightarrow \mathit{Clo}^{R}(X) \stackrel{\text{def}}{=} \bigcup_{x \in X} [x]_R$



Equivalence relation vs Closure Operators

Equivalence relations uniquely correspond to particular upper closure operators:

PARTITIONING
[Ranzato and Tapparo'04]

- $\eta \in \mathit{uco}(\wp(C)) \Rightarrow \forall x, y.\, x \mathit{Rel}^{\eta} y$ iff $\eta(x) = \eta(y)$
- $R \in \mathit{Eq}(C) \Rightarrow \mathit{Clo}^{R}(X) \stackrel{\text{def}}{=} \bigcup_{x \in X} [x]_R$
- $\Pi(\eta) \stackrel{\text{def}}{=} \mathit{Clo}^{\mathit{Rel}^{\eta}} \sqsubseteq \eta$

PER model vs Narrow ANI

PROPOSITION:

$$[\eta]\mathrm{P}(\rho) \quad \text{iff} \quad [\![\mathrm{P}]\!] : \mathit{All} \times \mathit{Rel}^{\eta} \to \mathit{All} \times \mathit{Rel}^{\rho}$$
$$\text{iff} \quad [\Pi(\eta)]\mathrm{P}(\Pi(\rho))$$

PER model vs Narrow ANI

PROPOSITION:

$$[\eta]\mathrm{P}(\rho) \quad \text{iff} \quad [\![\mathrm{P}]\!] : \mathit{All} \times \mathit{Rel}^{\eta} \to \mathit{All} \times \mathit{Rel}^{\rho}$$
$$\text{iff} \quad [\Pi(\eta)]\mathrm{P}(\Pi(\rho))$$

$$\Downarrow$$

$$[\mathrm{R}]\mathrm{P}(\mathrm{S}) \text{ iff } [\![\mathrm{P}]\!] : \mathit{All} \times \mathrm{R} \to \mathit{All} \times \mathrm{S}$$

PER model vs ANI

PROPOSITION 2:

$$(\eta)\mathrm{P}(\phi \rightsquigarrow\!\!\!\!\!\rightarrow\!\!\!] \rho) \quad \text{if} \quad (\Pi(\eta))\mathrm{P}(\Pi(\phi) \rightsquigarrow\!\!\!\!\!\rightarrow\!\!\!] \Pi(\rho))$$

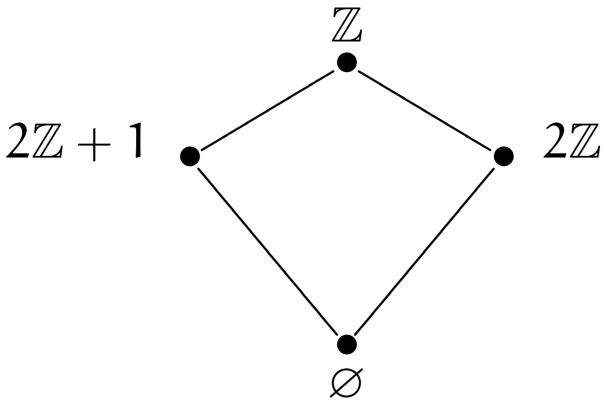
PER model vs ANI

PROPOSITION 2:

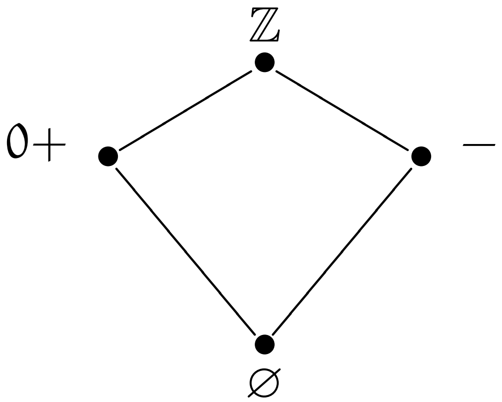
$$(\eta)P(\phi \rightsquigarrow\!\!\!\!\rrbracket \rho) \quad \text{if} \quad (\Pi(\eta))P(\Pi(\phi) \rightsquigarrow\!\!\!\!\rrbracket \Pi(\rho))$$

EXAMPLE:

$$P \stackrel{\text{def}}{=} \textbf{if } h = 0 \textbf{ then } l := l \; mod \; 6 + 2; \textbf{else if } l < 0 \textbf{ then } l := 2 \textbf{ else } l := 7;$$



$\eta = \mathit{Par}$



$\phi = \mathit{Sign}$

$\rho = \mathit{Int}$

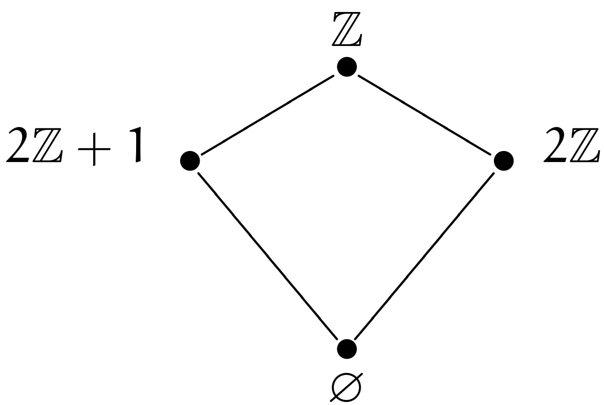
PER model vs ANI

PROPOSITION 2:

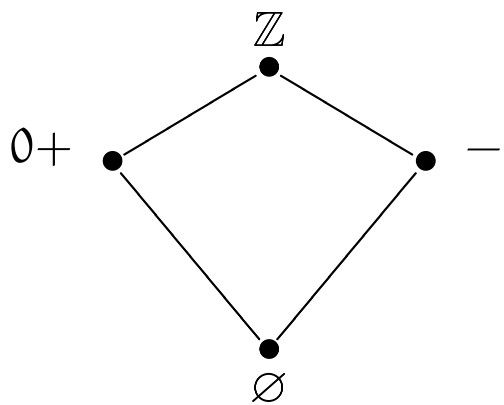
$$(\eta)P(\phi \rightsquigarrow\!\!\rrbracket \rho) \quad \text{if} \quad (\Pi(\eta))P(\Pi(\phi) \rightsquigarrow\!\!\rrbracket \Pi(\rho))$$

EXAMPLE:

$$P \stackrel{\text{def}}{=} \textbf{if } h = 0 \textbf{ then } l := l \; \textit{mod} \; 6 + 2; \textbf{else if } l < 0 \textbf{ then } l := 2 \textbf{ else } l := 7;$$



$\eta = \textit{Par}$



$\phi = \textit{Sign}$

$\rho = \textit{Int}$

$$\eta(l) = 2\mathbb{Z}: \quad \rho(\llbracket P \rrbracket(0+, 2\mathbb{Z})^L) = \rho(\{2,3,5,7\}) = [2,7] = \rho(\llbracket P \rrbracket(-, 2\mathbb{Z})^L) = \rho(\{2,7\})$$

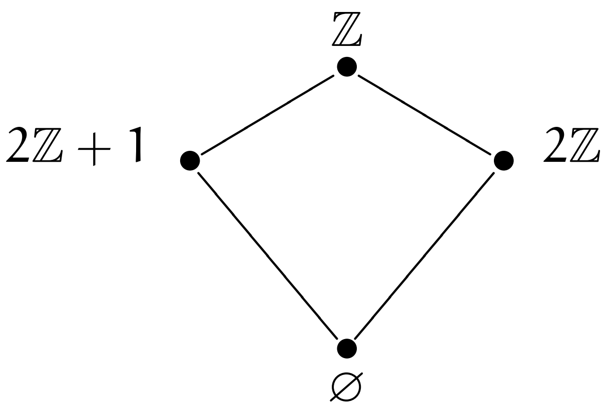
PER model vs ANI

PROPOSITION 2:

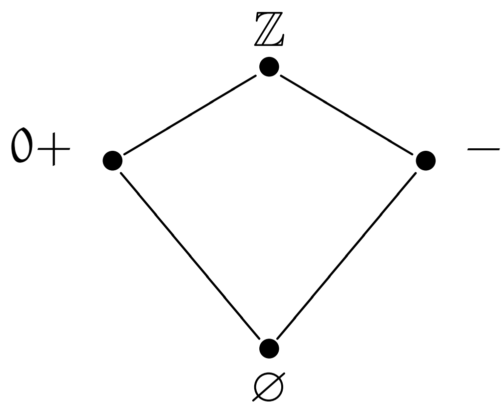
$$(\eta)P(\phi \rightsquigarrow\!\!\!\!\rightarrow\!\!\!\! \| \rho) \quad \text{if} \quad (\Pi(\eta))P(\Pi(\phi) \rightsquigarrow\!\!\!\!\rightarrow\!\!\!\! \| \Pi(\rho))$$

EXAMPLE:

$$P \stackrel{\text{def}}{=} \textbf{if } h = 0 \textbf{ then } l := l \; mod \; 6 + 2; \textbf{else if } l < 0 \textbf{ then } l := 2 \textbf{ else } l := 7;$$



$\eta = Par$



$\phi = Sign$

$\rho = Int$

$$\eta(l) = 2\mathbb{Z}: \quad \Pi(\rho)(\llbracket P \rrbracket(0+, 2\mathbb{Z})^{L}) = \Pi(\rho)(\{2,3,5,7\}) = \{2,3,5,7\} \neq \{2,7\}$$

$$\Pi(\rho)(\llbracket P \rrbracket(-, 2\mathbb{Z})^{L}) = \Pi(\rho)(\{2,7\})$$

Deriving un-constrained attackers

Input Observation: R;

Output Observation: S;

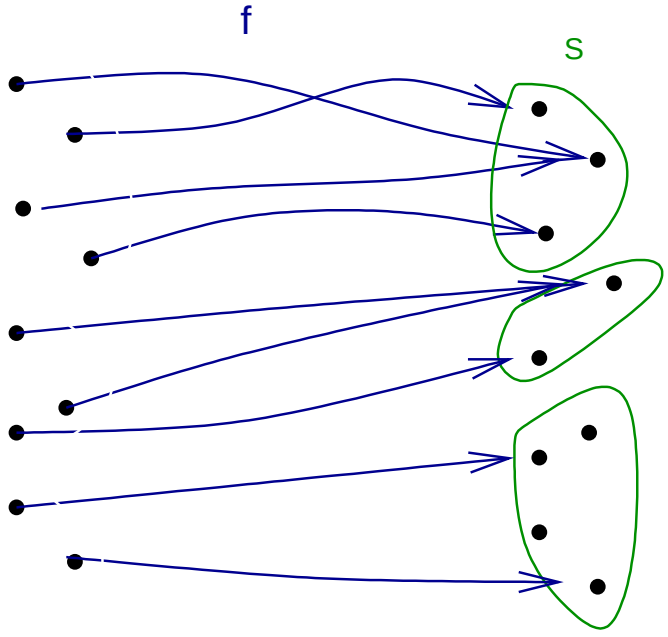
Non-Interference: $f : R \rightarrowtriangle S$ iff $x \, R \, y \;\Rightarrow\; f(x) \, S \, f(y)$

Deriving un-constrained attackers

Input Observation: R;

Output Observation: S;

Non-Interference: $f : R \rightarrowtriangle S$ iff $x \, R \, y \;\Rightarrow\; f(x) \, S \, f(y)$

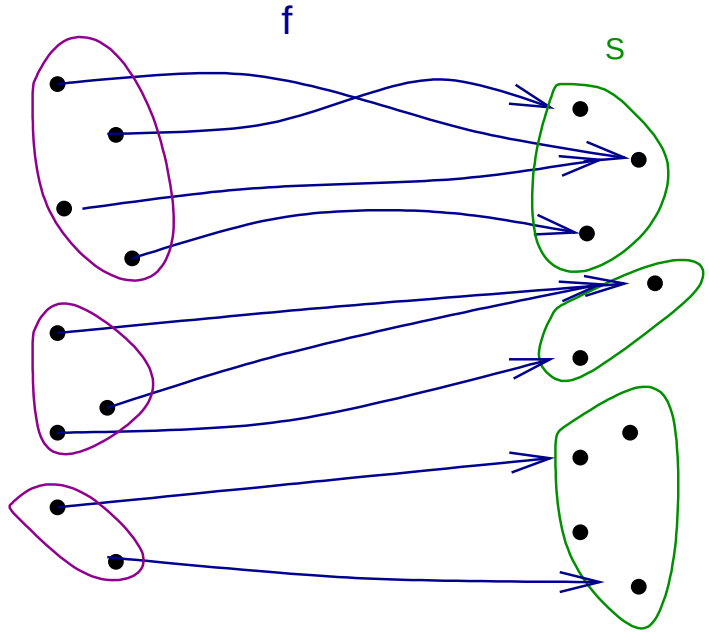


Deriving un-constrained attackers

Input Observation: R;

Output Observation: S;

Non-Interference: $f : R \rightarrowtriangle S$ iff $x \, R \, y \;\Rightarrow\; f(x) \, S \, f(y)$



$x \, \widehat{f^{-1}}(S) \, y$ iff $f(x) \, S \, f(y)$

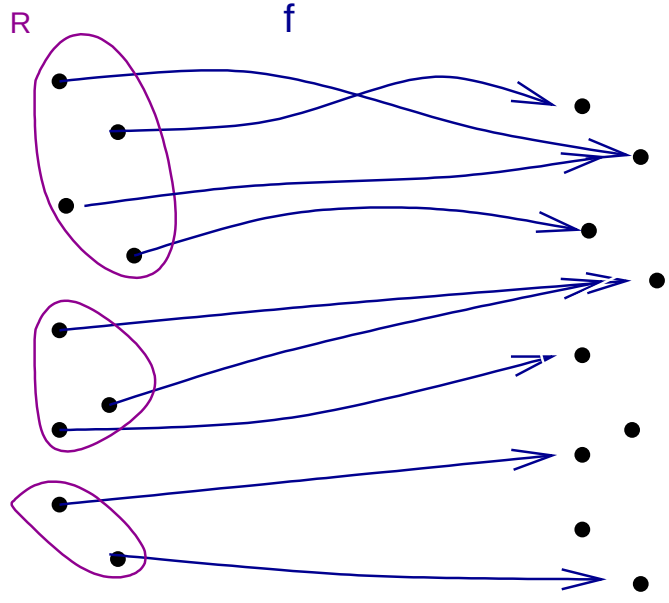
Deriving un-constrained attackers

Input Observation: R;

Output Observation: S;

Non-Interference: $f : R \rightarrowtriangle S$ iff $x \, R \, y \;\Rightarrow\; f(x) \, S \, f(y)$

$$x \, \widehat{f^{-1}}(S) \, y \text{ iff } f(x) \, S \, f(y)$$



$$x' \, R \, y'$$

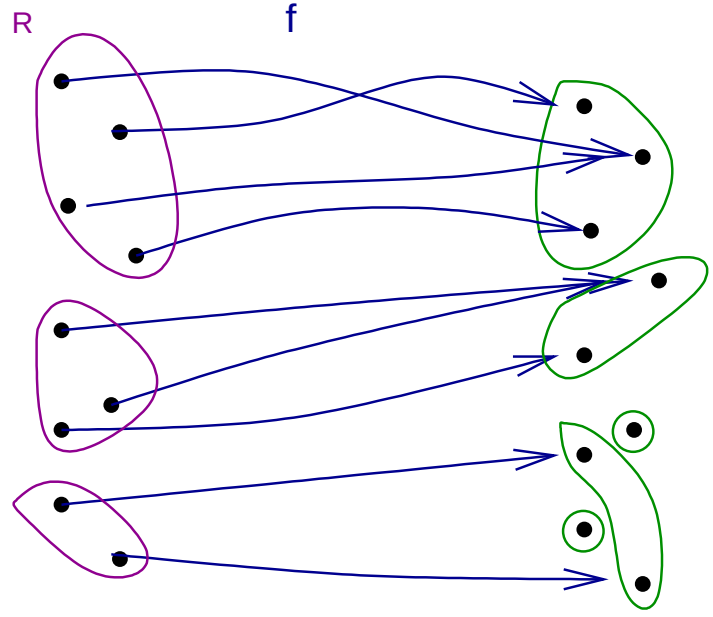
Deriving un-constrained attackers

Input Observation: R;

Output Observation: S;

Non-Interference: $f : R \rightarrowtriangle S$ iff $x\, R\, y \;\Rightarrow\; f(x)\, S\, f(y)$

$$x\, \widehat{f^{-1}}(S)\, y \text{ iff } f(x)\, S\, f(y)$$



$$x\, \widehat{f}(R)\, y \text{ iff } x = y \text{ or } x = f(x'),\ y = f(y'),\ x'\, R\, y'$$

Deriving un-constrained attackers

Input Observation: R;

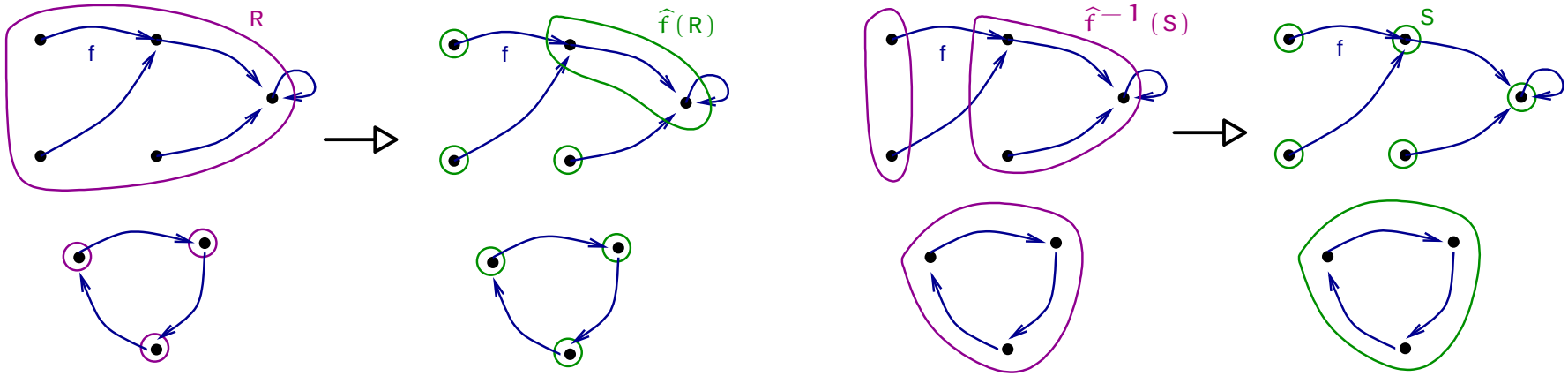
Output Observation: S;

Non-Interference: $f : R \rightarrowtriangle S$ iff $x\, R\, y \;\Rightarrow\; f(x)\, S\, f(y)$

$$x\, \widehat{f}^{-1}(S)\, y \text{ iff } f(x)\, S\, f(y)$$

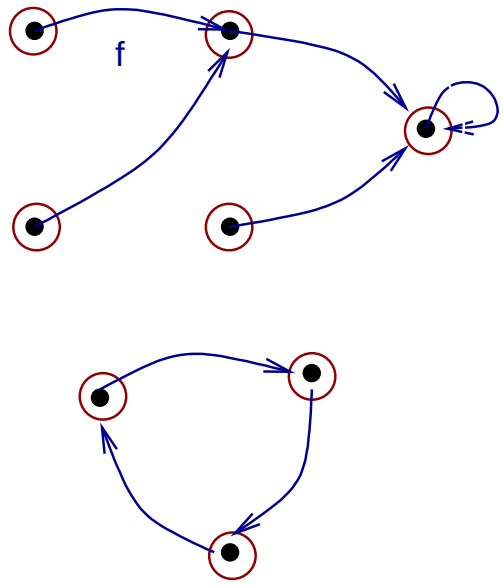
$$x\, \widehat{f}(R)\, y \text{ iff } x = y \text{ or } x = f(x'),\ y = f(y'),\ x'\, R\, y'$$

EXAMPLE:



Fix point attackers

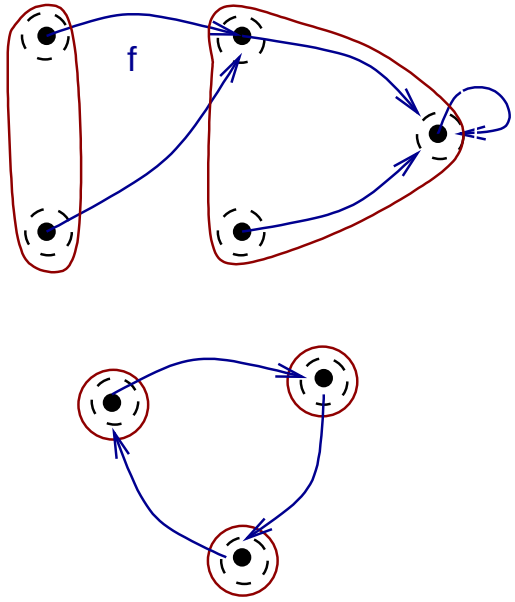
- Least fix point of $\widehat{f}^{-1}$



(a)

Fix point attackers

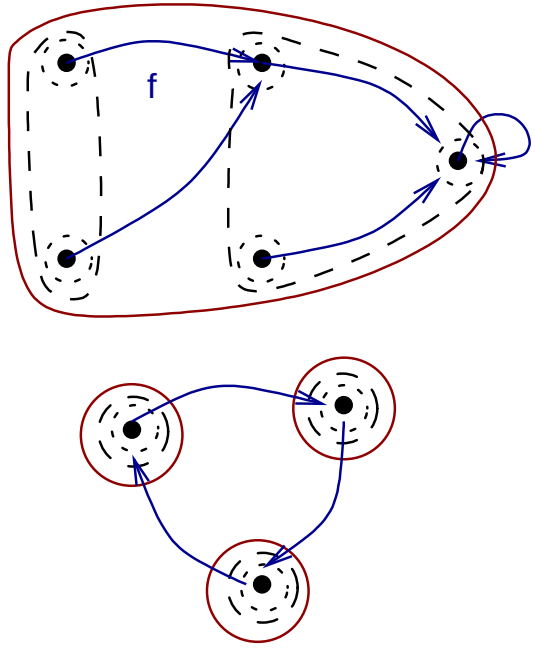
- Least fix point of $\widehat{f}^{-1}$



(a)

Fix point attackers

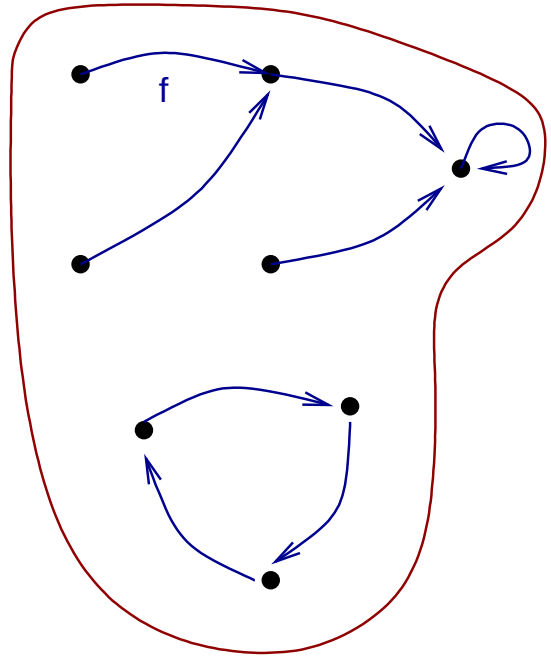
- Least fix point of $\widehat{f}^{-1}$



(a)

Fix point attackers

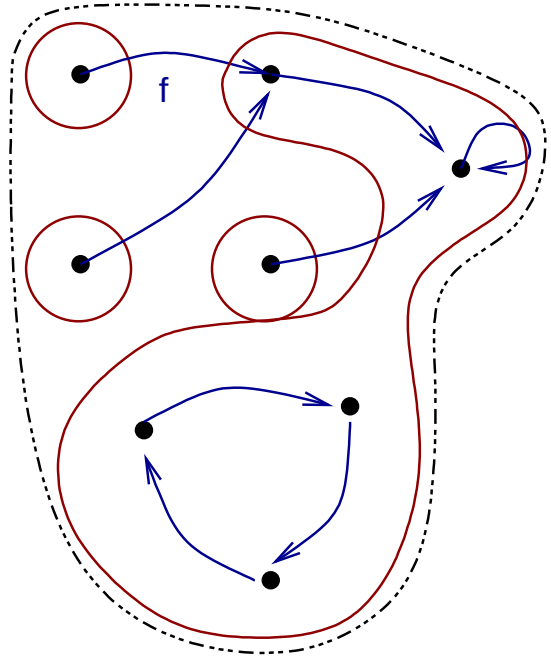
- Least fix point of $\widehat{f}^{-1}$
- Greatest fix point of $\widehat{f}$



(b)

Fix point attackers

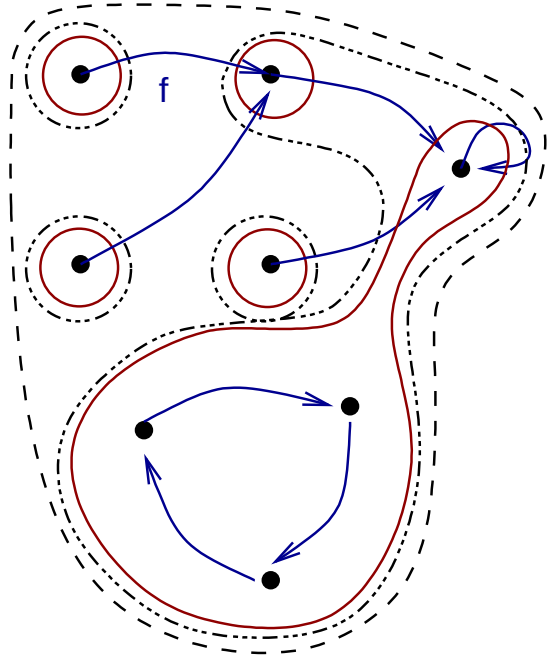
- Least fix point of $\widehat{f}^{-1}$
- Greatest fix point of $\widehat{f}$



(b)

Fix point attackers

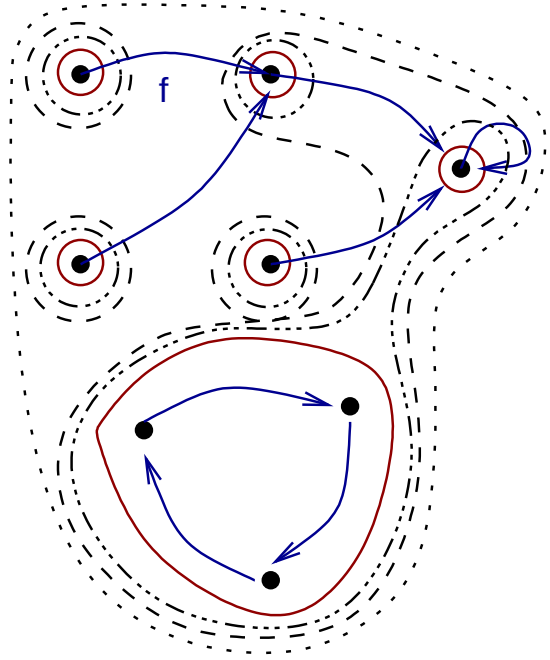
- Least fix point of $\widehat{f}^{-1}$
- Greatest fix point of $\widehat{f}$



(b)

Fix point attackers

- Least fix point of $\widehat{f}^{-1}$
- Greatest fix point of $\widehat{f}$



(b)

Fix point attackers

- Least fix point of $\widehat{f}^{-1}$
- Greatest fix point of $\widehat{f}$
- The smallest R such that $[R]P(R)$ is the least fix point of $\widehat{f}(\mathit{All} \times R)$.

PER model and completeness

Completeness in abstract interpretation can be formalized as follows:

$$\rho \circ f \circ \eta = \rho \circ f$$

[Giacobazzi et al. '00]

iff

$$\forall x, y.\, \eta(x) = \eta(y) \;\Rightarrow\; \rho(f(x)) = \rho(f(y))$$

PER model and completeness

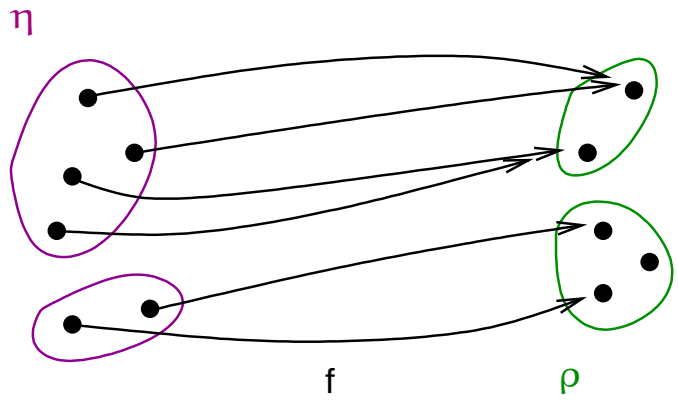
Completeness in abstract interpretation can be formalized as follows:

$$\rho \circ f \circ \eta = \rho \circ f$$

[Giacobazzi et al. '00]

iff

$$\forall x, y.\, \eta(x) = \eta(y) \;\Rightarrow\; \rho(f(x)) = \rho(f(y))$$



PER model and completeness

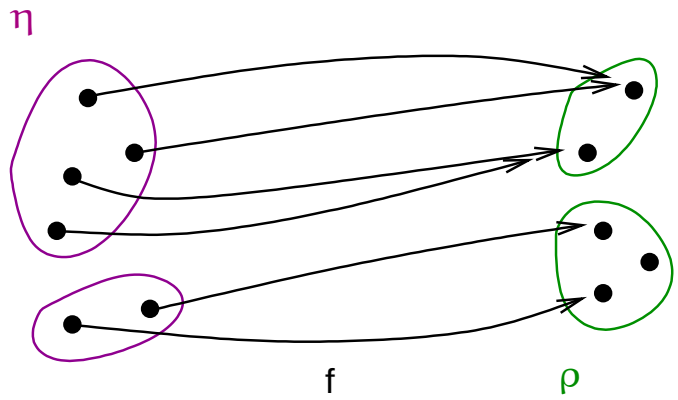
Completeness in abstract interpretation can be formalized as follows:

$$\rho \circ f \circ \eta = \rho \circ f$$

[Giacobazzi et al. '00]

iff

$$\forall x, y.\, \eta(x) = \eta(y) \;\Rightarrow\; \rho(f(x)) = \rho(f(y))$$



$$\Downarrow$$

$$f : R \rightarrowtriangle S$$

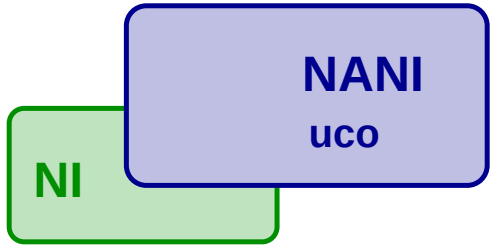
iff

$$Clo^S \circ f \circ Clo^R = Clo^S \circ f$$

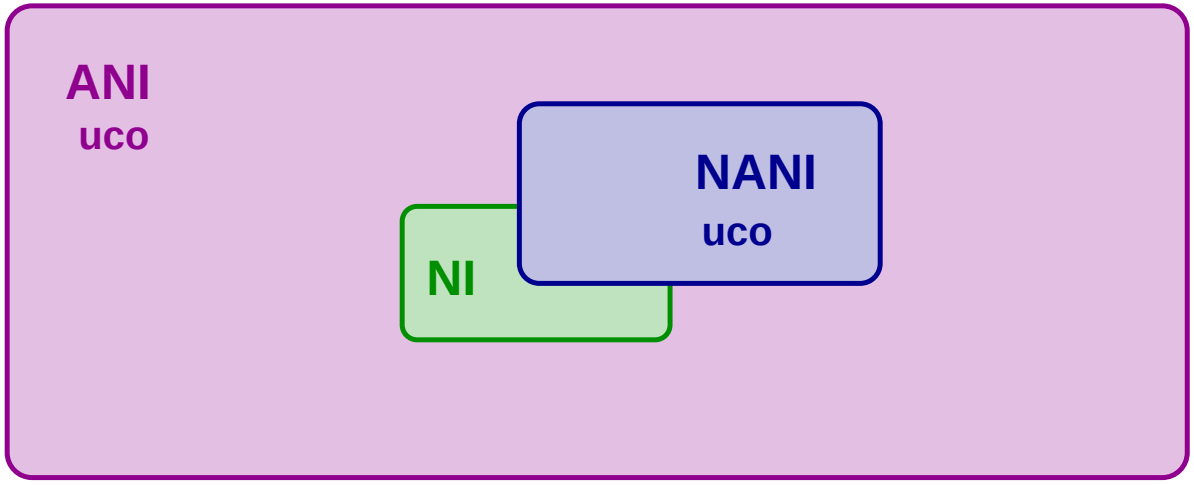
Conclusion

NI

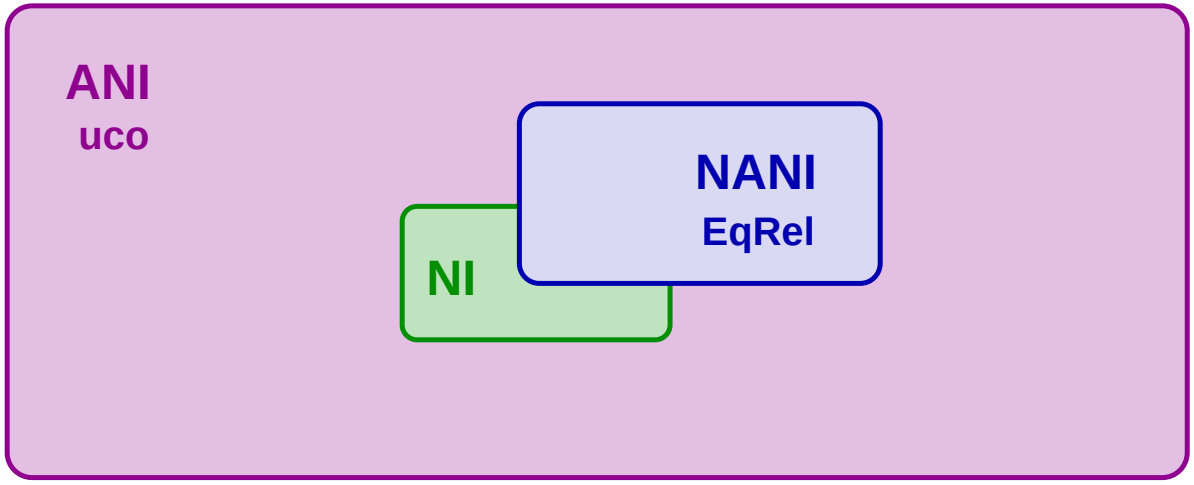
Conclusion



Conclusion



Conclusion



Conclusion