Generalized Abstract Non-Interference Abstract Secure Information-flow Analysis for Automata

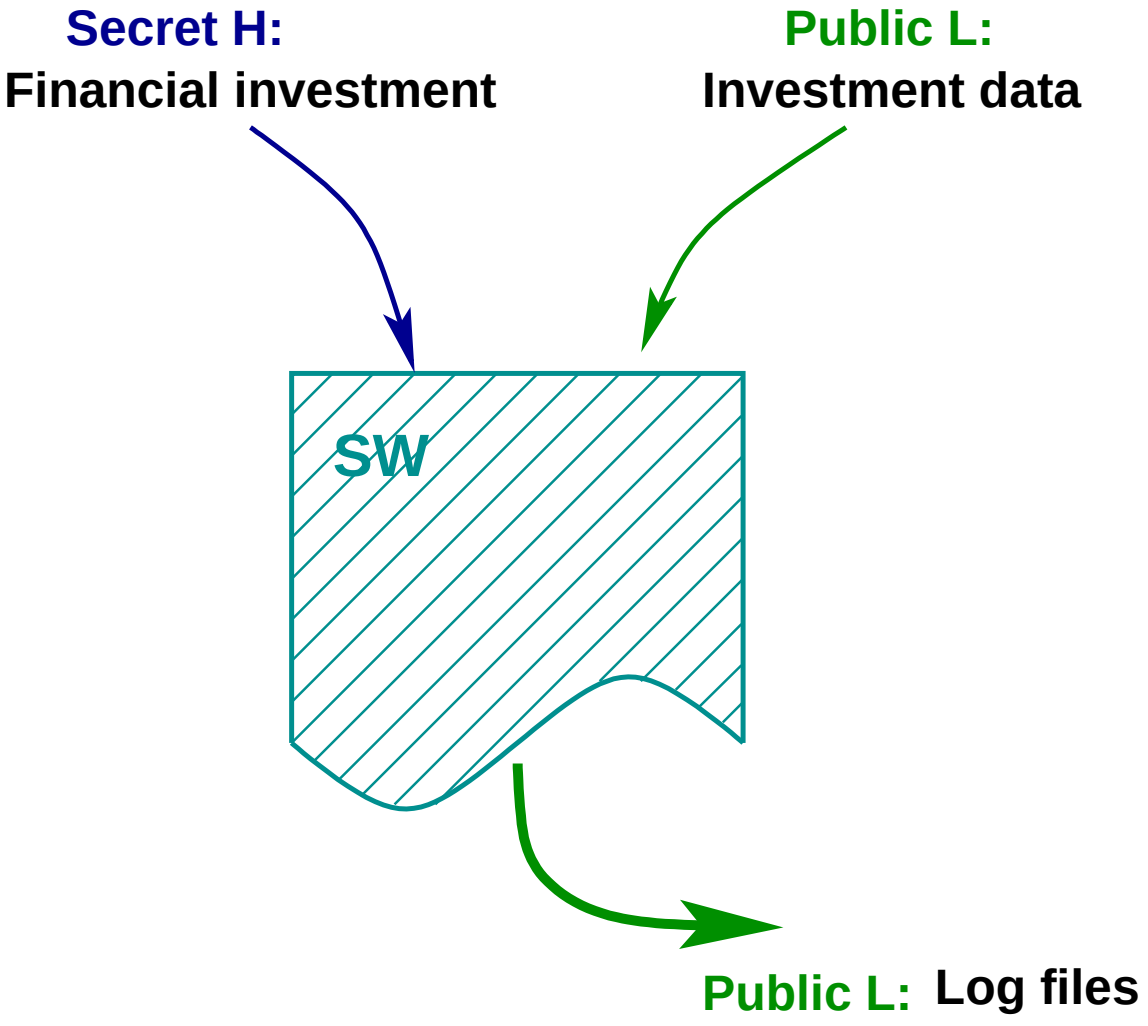
Roberto Giacobazzi and **Isabella Mastroeni**

Dipartimento di Informatica

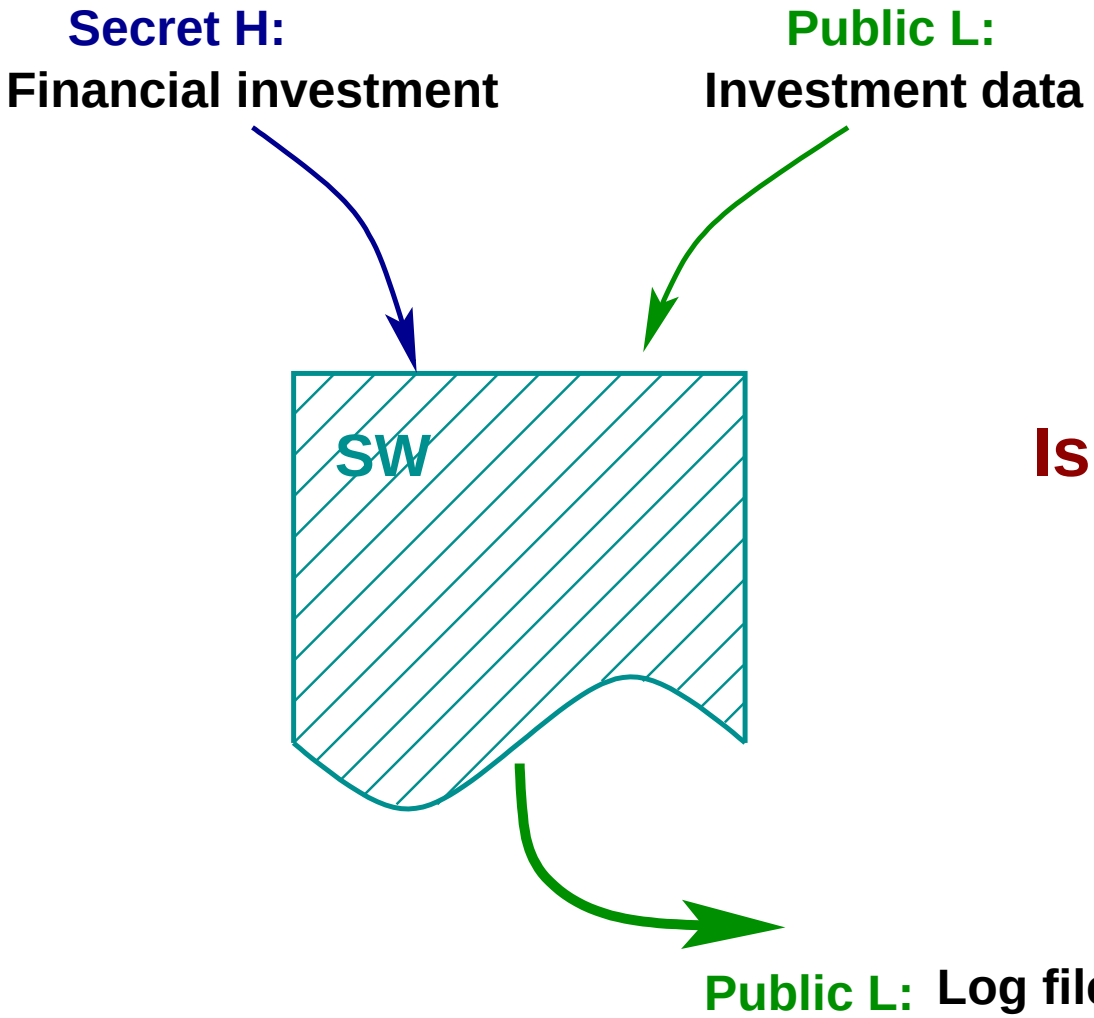
Università di Verona, Italy

MMM-ACNS, September 25, 2005

The Problem: Non-Interference

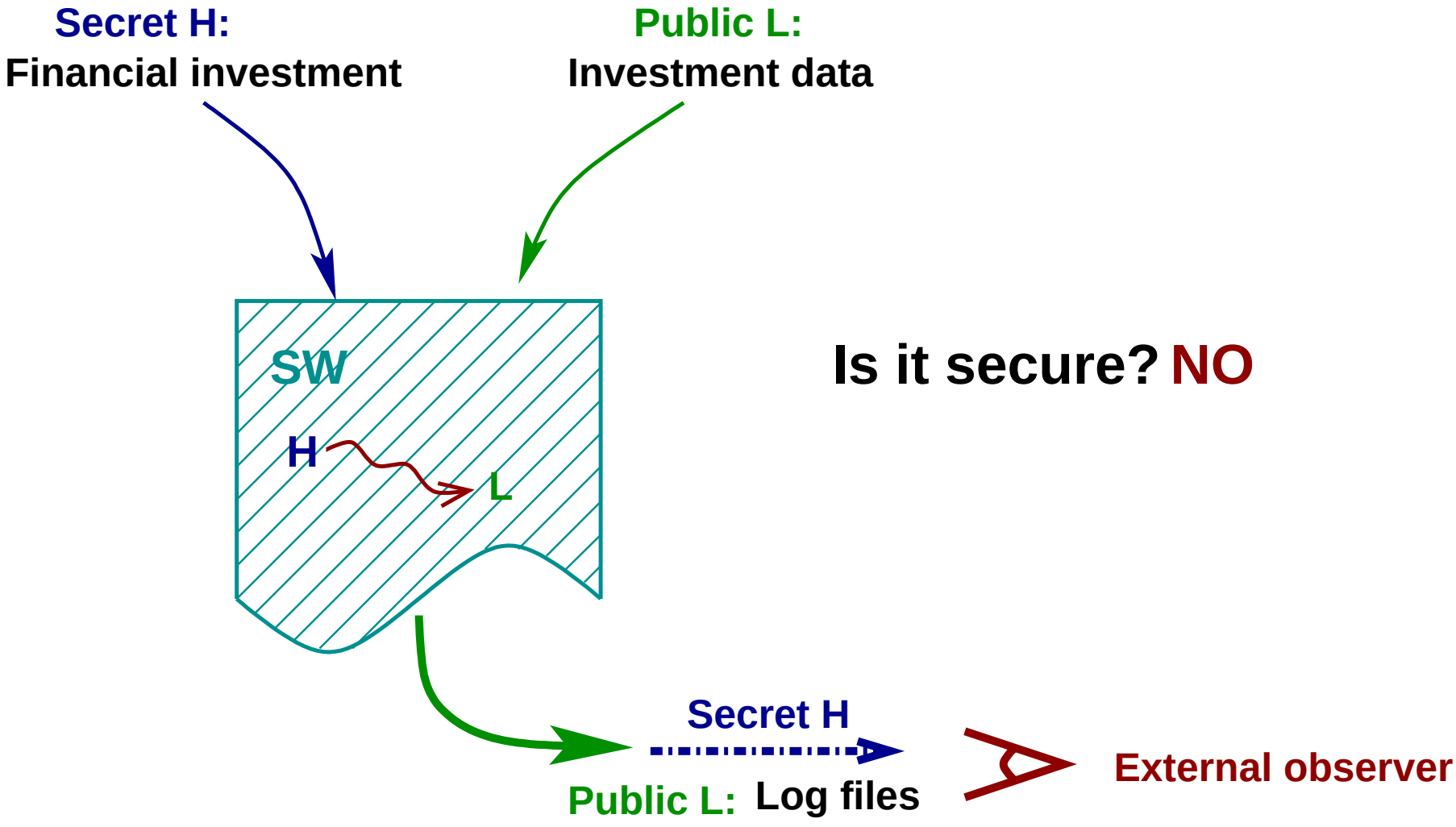


The Problem: Non-Interference



Is it secure?

The Problem: Non-Interference



Background

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

Background

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

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.*

Non-interference policies require that any *change upon confidential data has not to be revealed through the observation of public data.*

- Many real systems are intended to leak some kind of information
- Even if a system satisfies non-interference, some kind of tests could reject it as insecure

Background

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

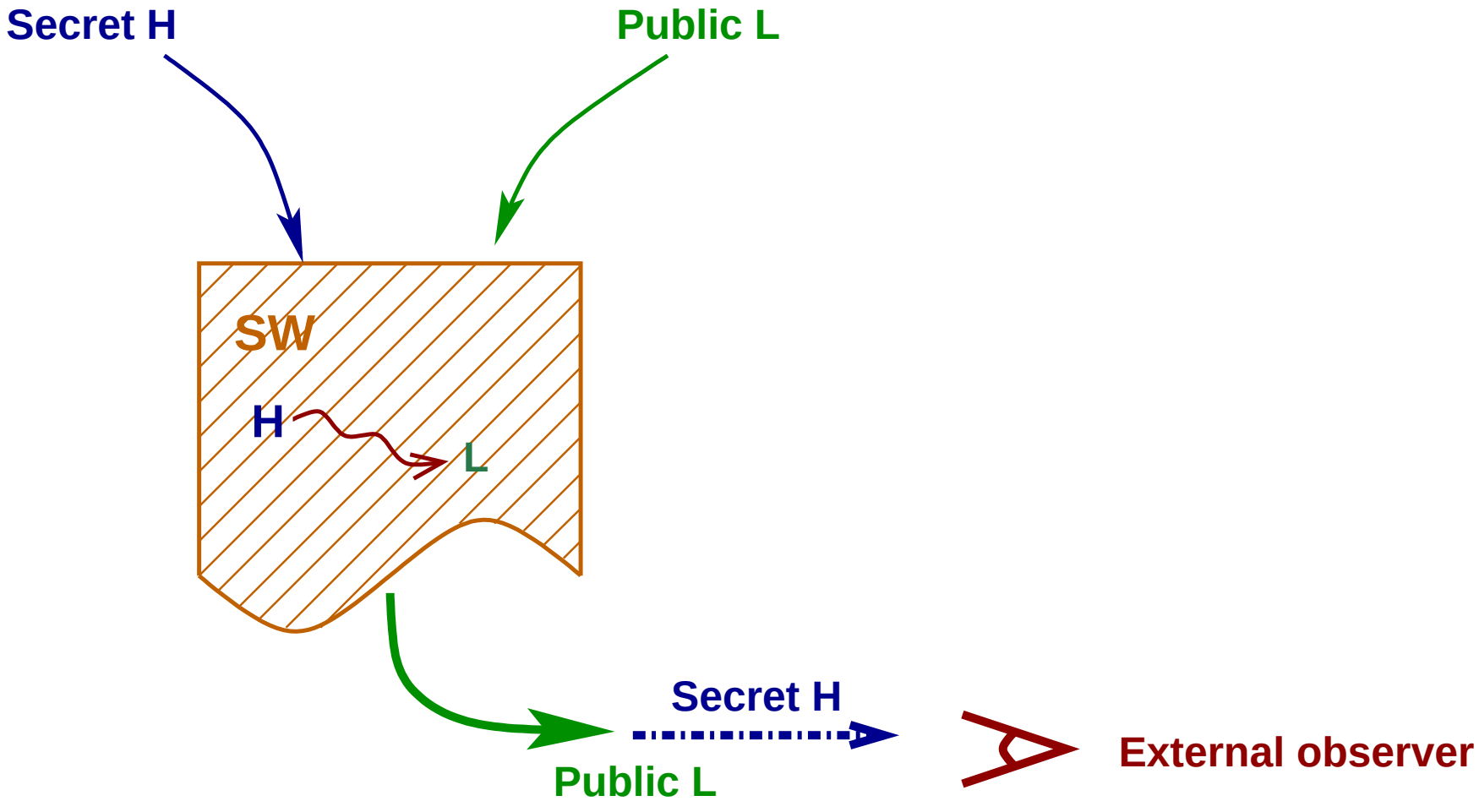
Confinement problem [Lampson'73]: *Preventing the results of computations leaking even partial information about the confidential inputs.*

Non-interference policies require that any *change upon confidential data has not to be revealed through the observation of public data.*

- Characterizing released information: [Cohen'77], [Zdancewic & Myers'01], [Clark et al.'04], [Lowe'02];
- Constraining attackers: [Di Pierro et al.'02], [Laud'01].

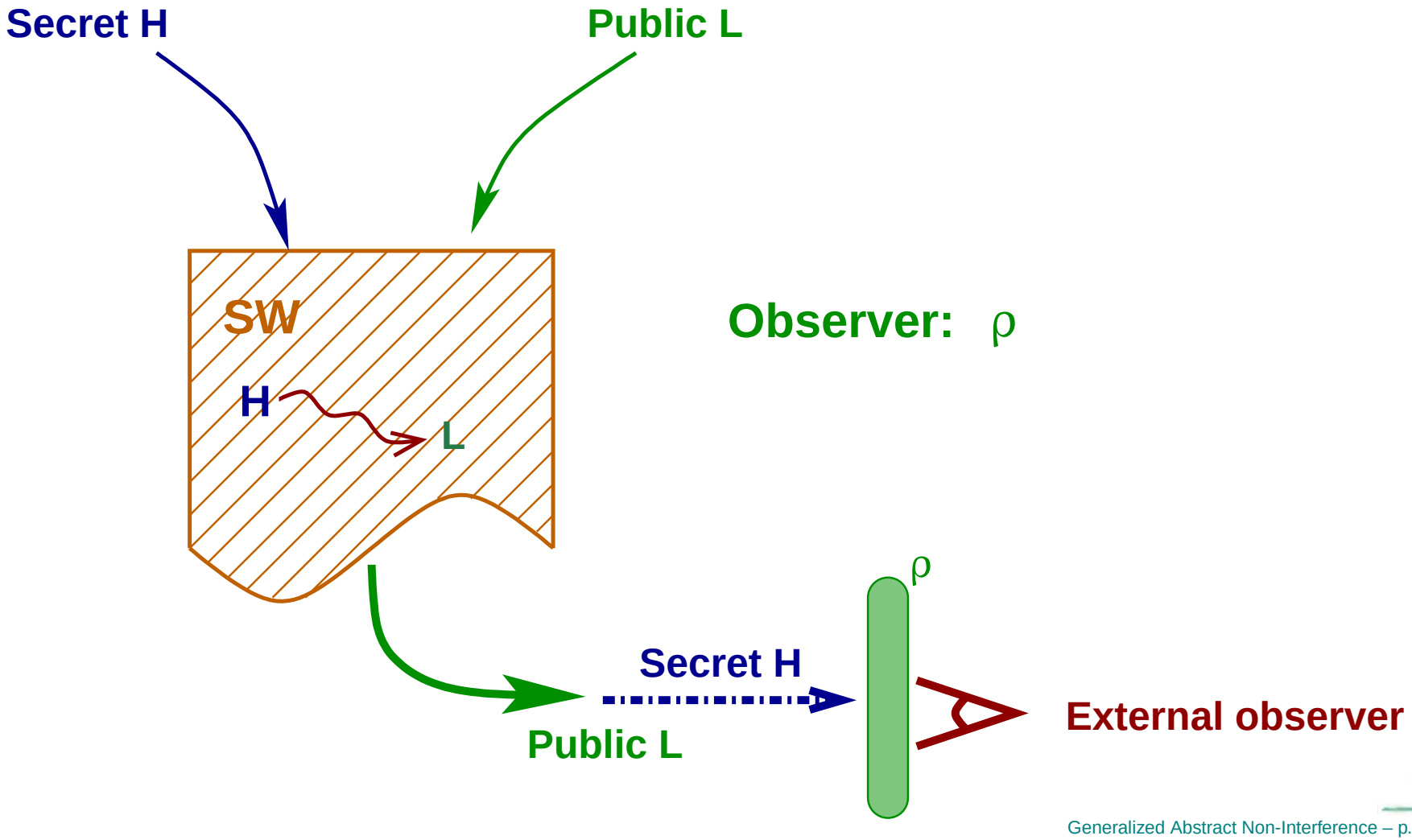
Abstracting Non-Interference

[Giacobazzi & Mastroeni, POPL'04]



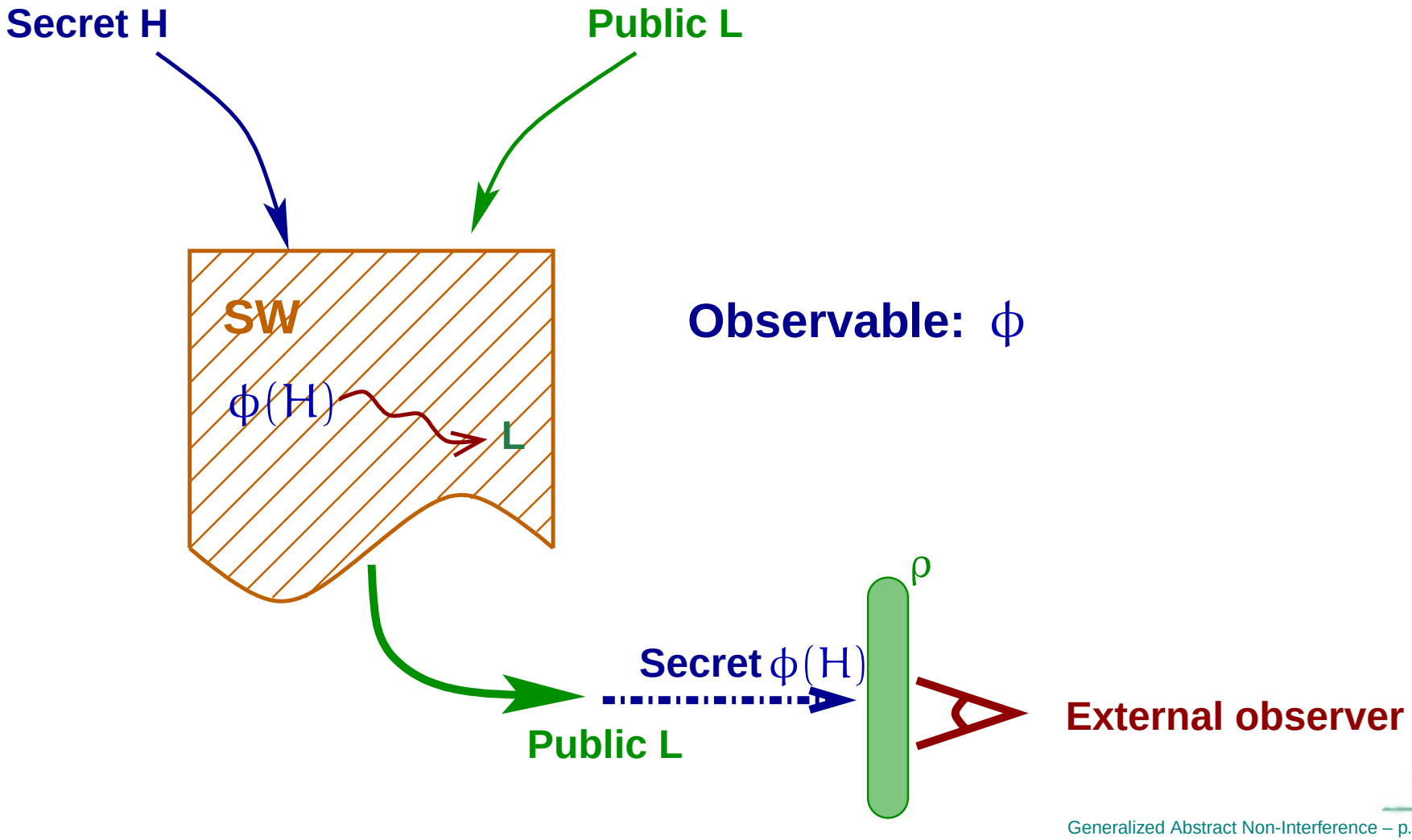
Abstracting Non-Interference

[Giacobazzi & Mastroeni, POPL'04]



Abstracting Non-Interference

[Giacobazzi & Mastroeni, POPL'04]



AI: Lattice of Abstractions

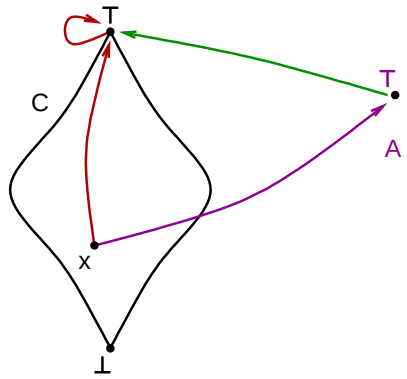
The concrete domain $< C, \leq, \wedge, \vee, \bot, \top >$ [Cousot & Cousot '79]

Lattice of abstract domains $\equiv Abs(C)$

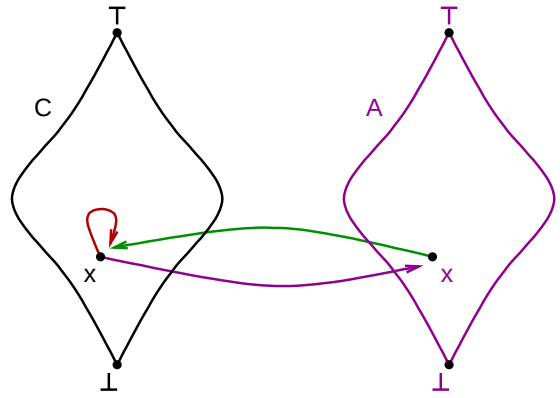
$< Abs(C), \sqsubseteq, \sqcap, \sqcup, \top, C >$

$A_1 \sqsubseteq A_2 \quad \Leftrightarrow \quad A_2 \subseteq A_1$ (A_1 more precise than A_2)

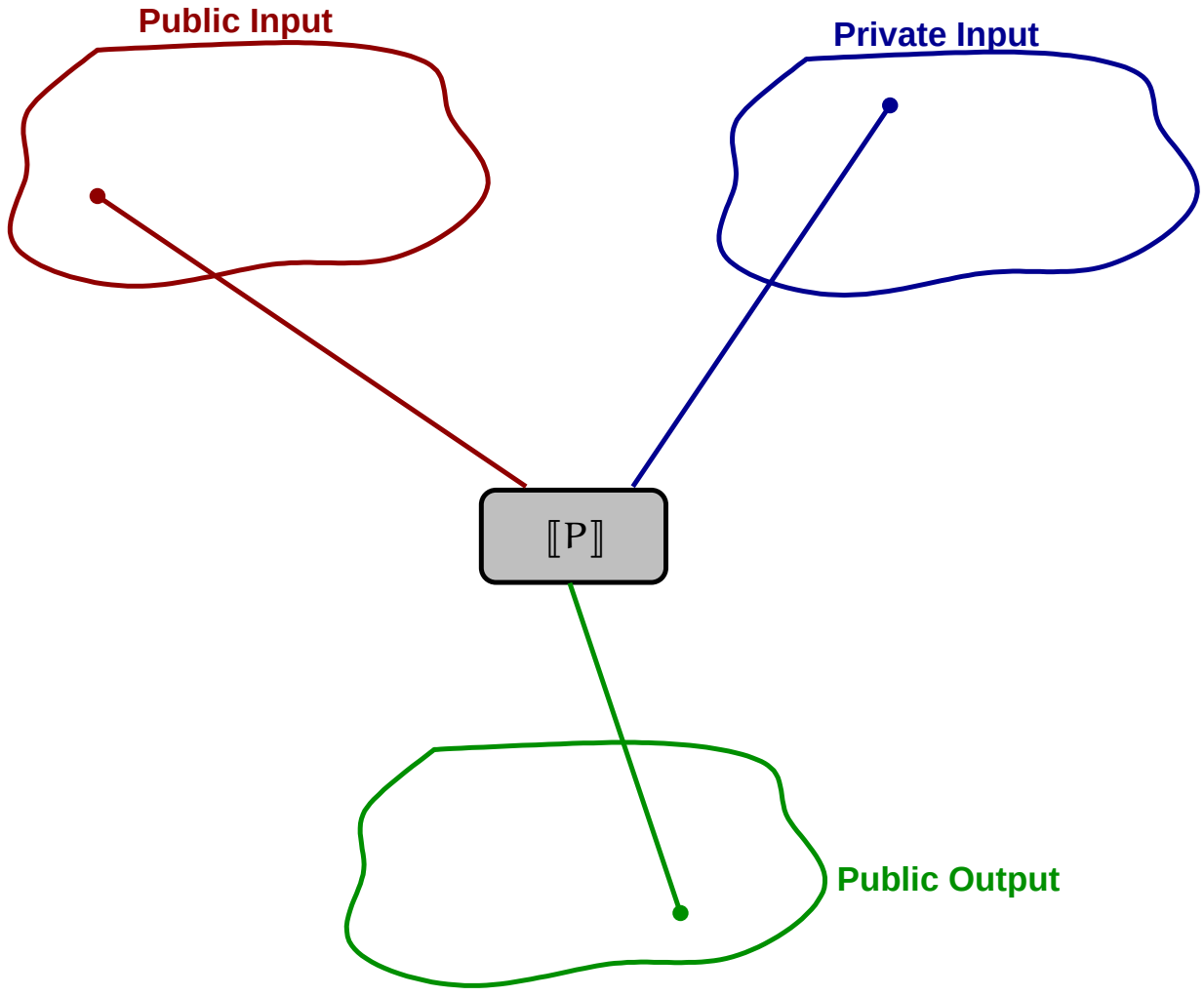
Top:



Bottom:

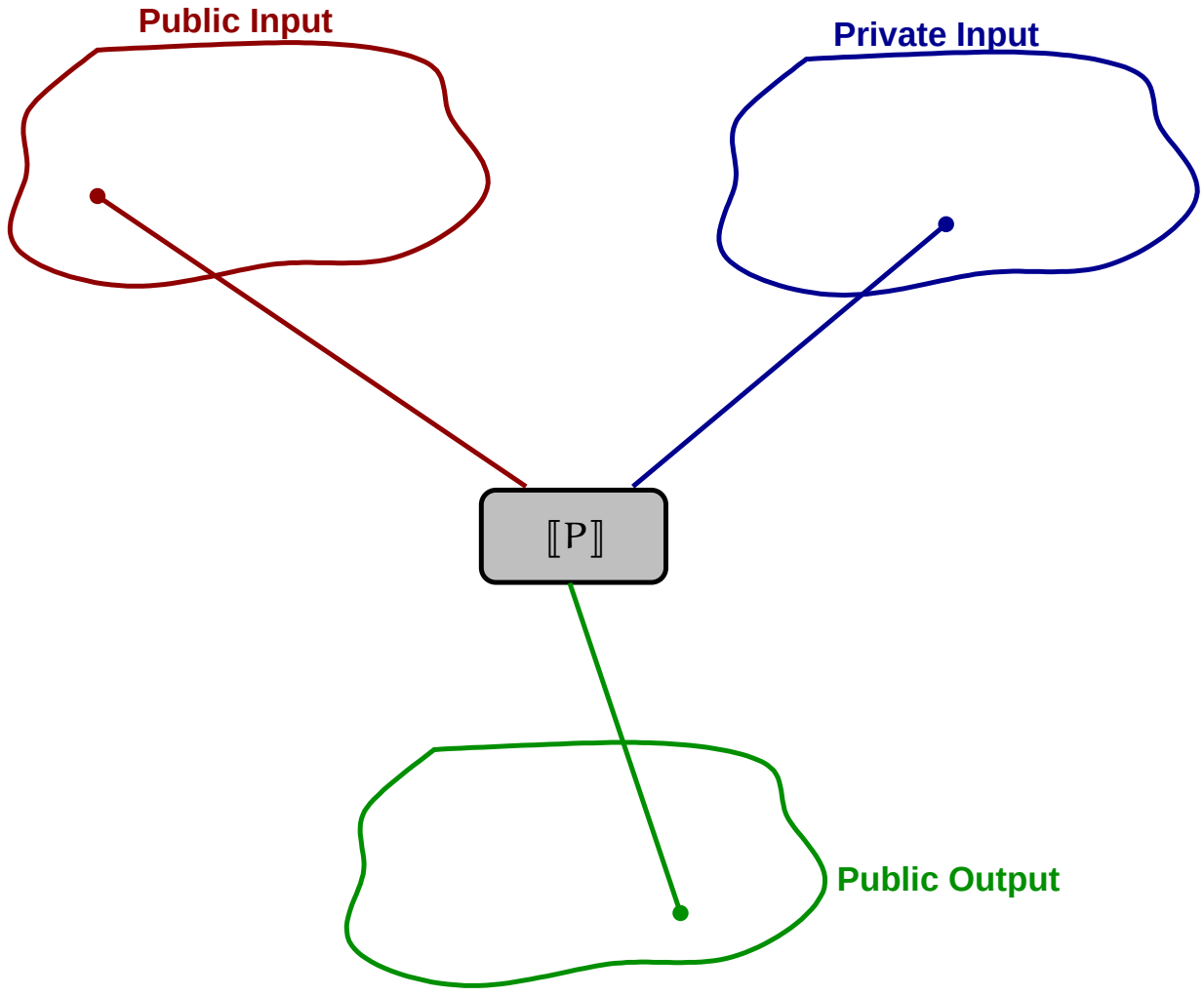


Standard non-interference



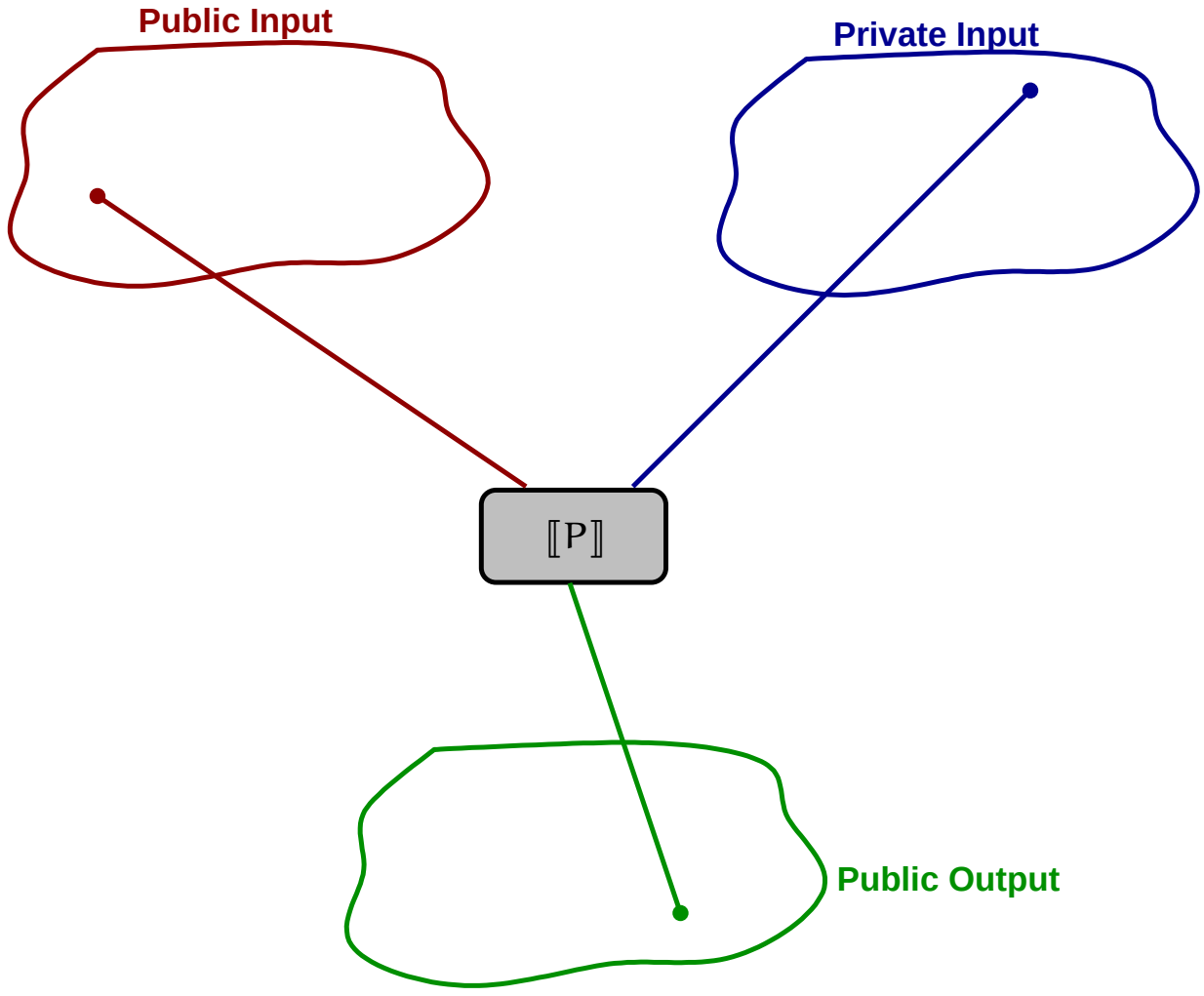
$$\forall l : \mathsf{L}, \forall h_1, h_2 : \mathsf{H}.\ [\![P]\!](h_1, l)^{\mathsf{L}} = [\![P]\!](h_2, l)^{\mathsf{L}}$$

Standard non-interference



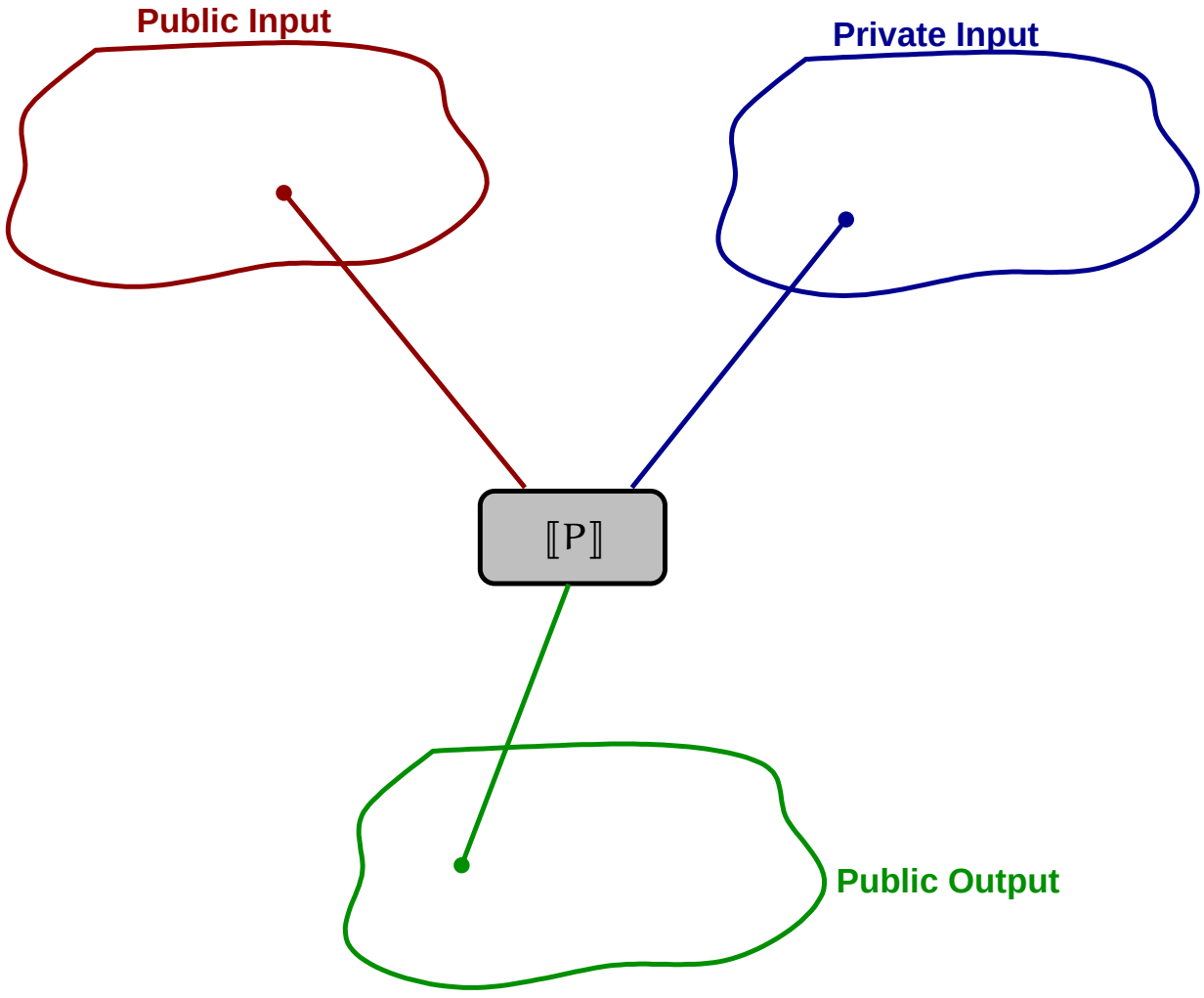
$$\forall l : \mathsf{L}, \forall h_1, h_2 : \mathsf{H}.\ [\![P]\!](h_1, l)^{\mathsf{L}} = [\![P]\!](h_2, l)^{\mathsf{L}}$$

Standard non-interference



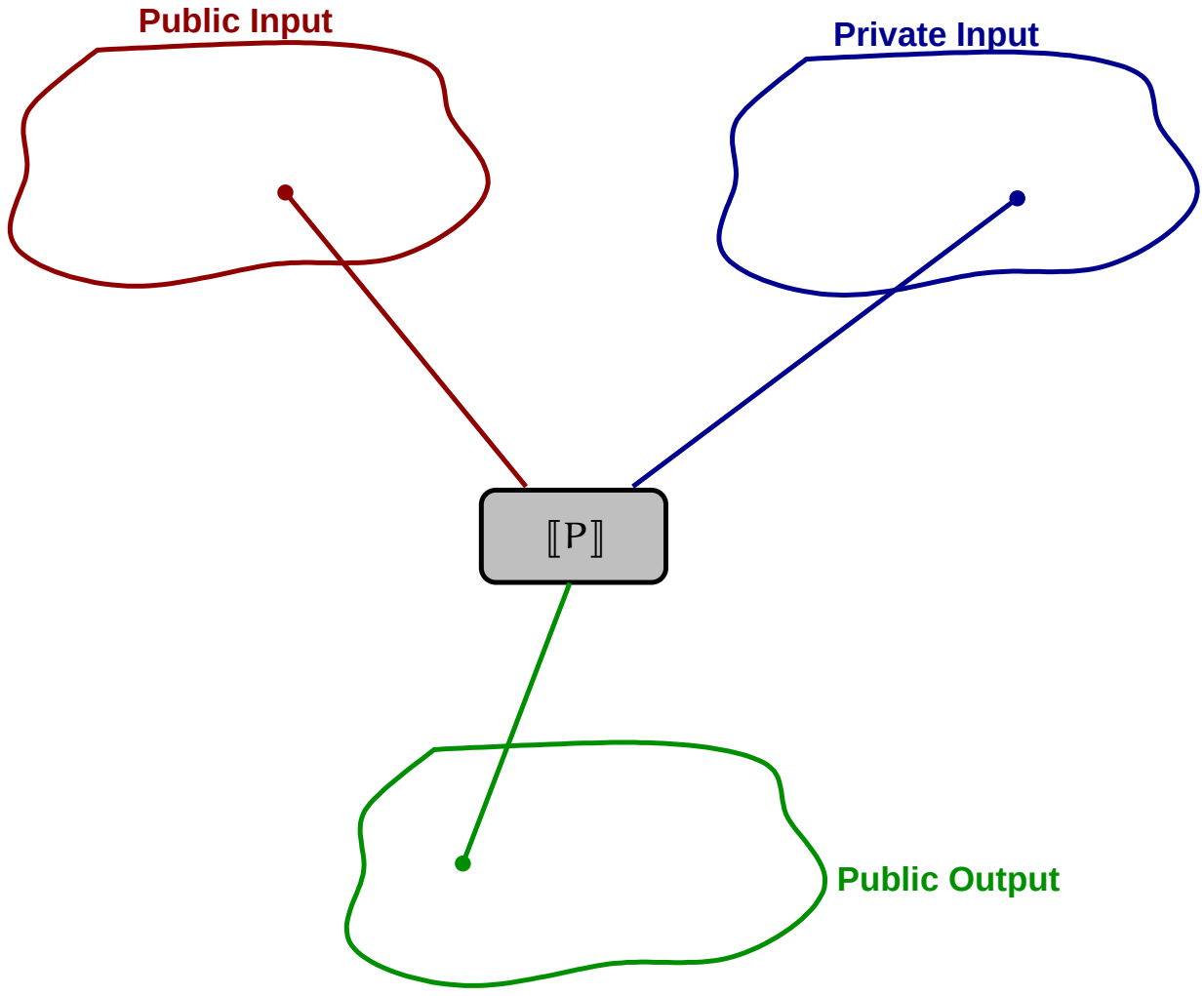
$$\forall l : \mathsf{L}, \forall h_1, h_2 : \mathsf{H}.\ [\![P]\!](h_1, l)^{\mathsf{L}} = [\![P]\!](h_2, l)^{\mathsf{L}}$$

Standard non-interference



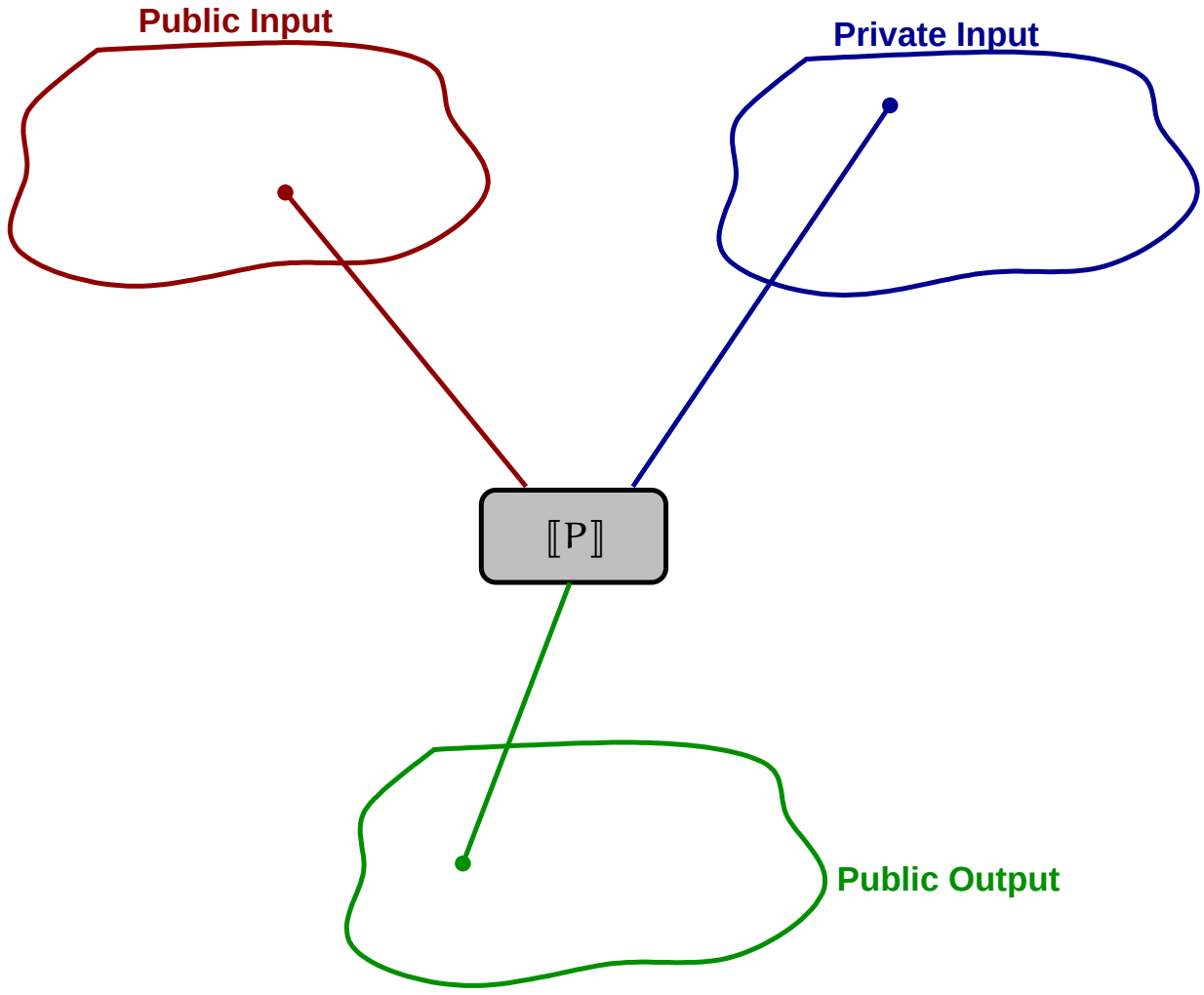
$$\forall l : \mathsf{L}, \forall h_1, h_2 : \mathsf{H}.\ [\![P]\!](h_1, l)^{\mathsf{L}} = [\![P]\!](h_2, l)^{\mathsf{L}}$$

Standard non-interference



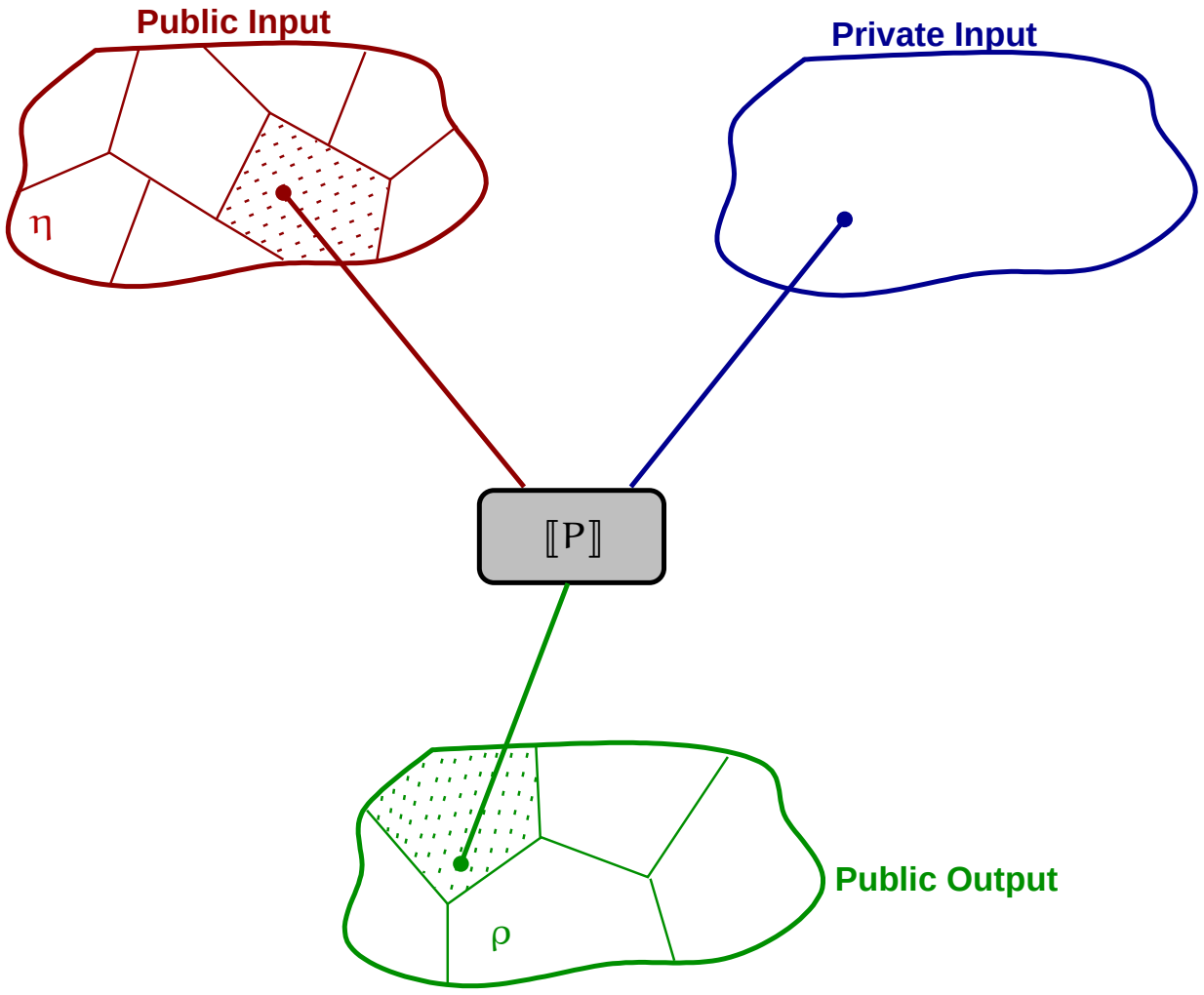
$$\forall l : \mathsf{L}, \forall h_1, h_2 : \mathsf{H}.\ [\![P]\!](h_1, l)^{\mathsf{L}} = [\![P]\!](h_2, l)^{\mathsf{L}}$$

Standard non-interference



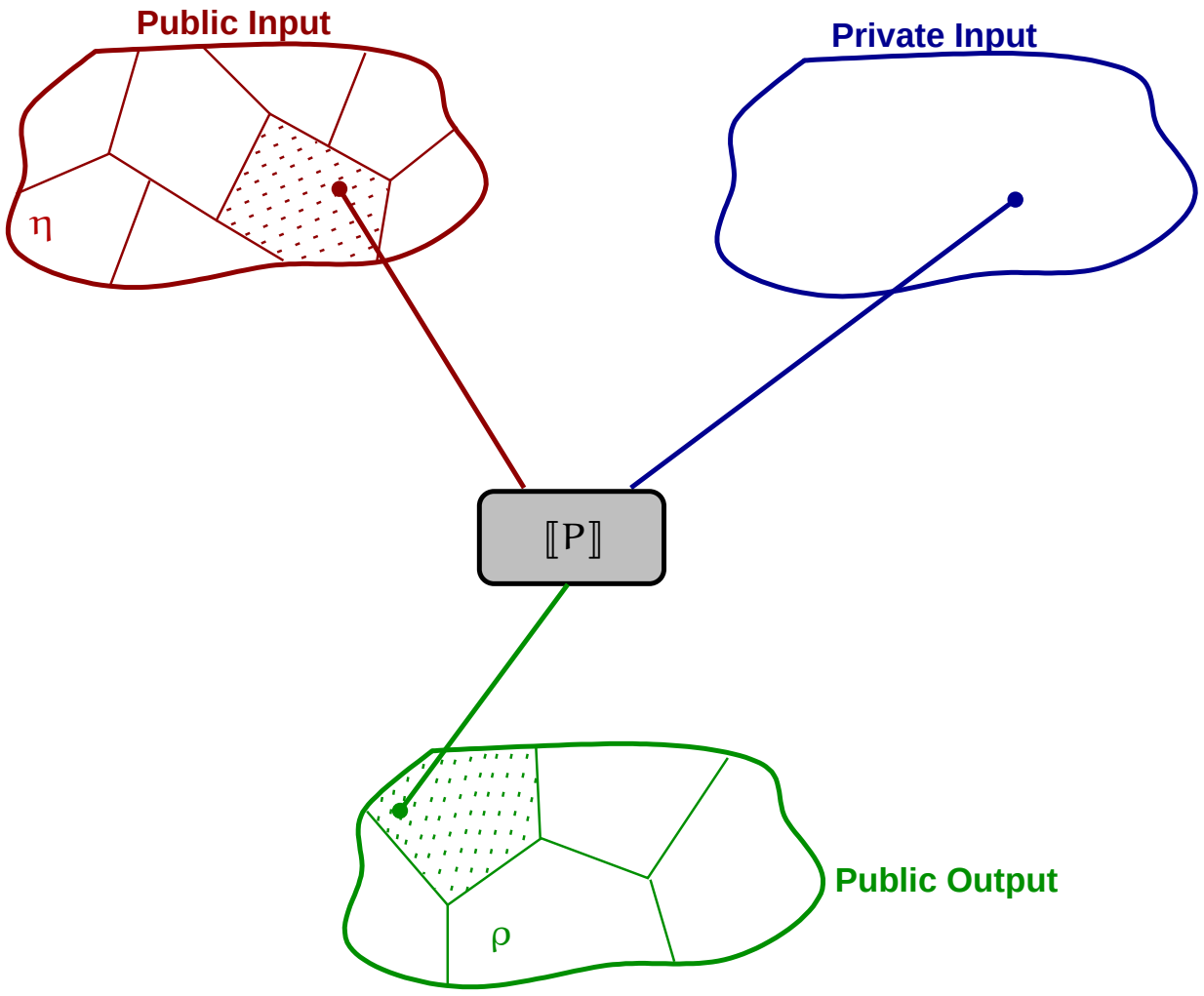
$$\forall l : \mathsf{L}, \forall h_1, h_2 : \mathsf{H}.\ [\![P]\!](h_1, l)^{\mathsf{L}} = [\![P]\!](h_2, l)^{\mathsf{L}}$$

Abstracting non-interference I: Narrow ANI



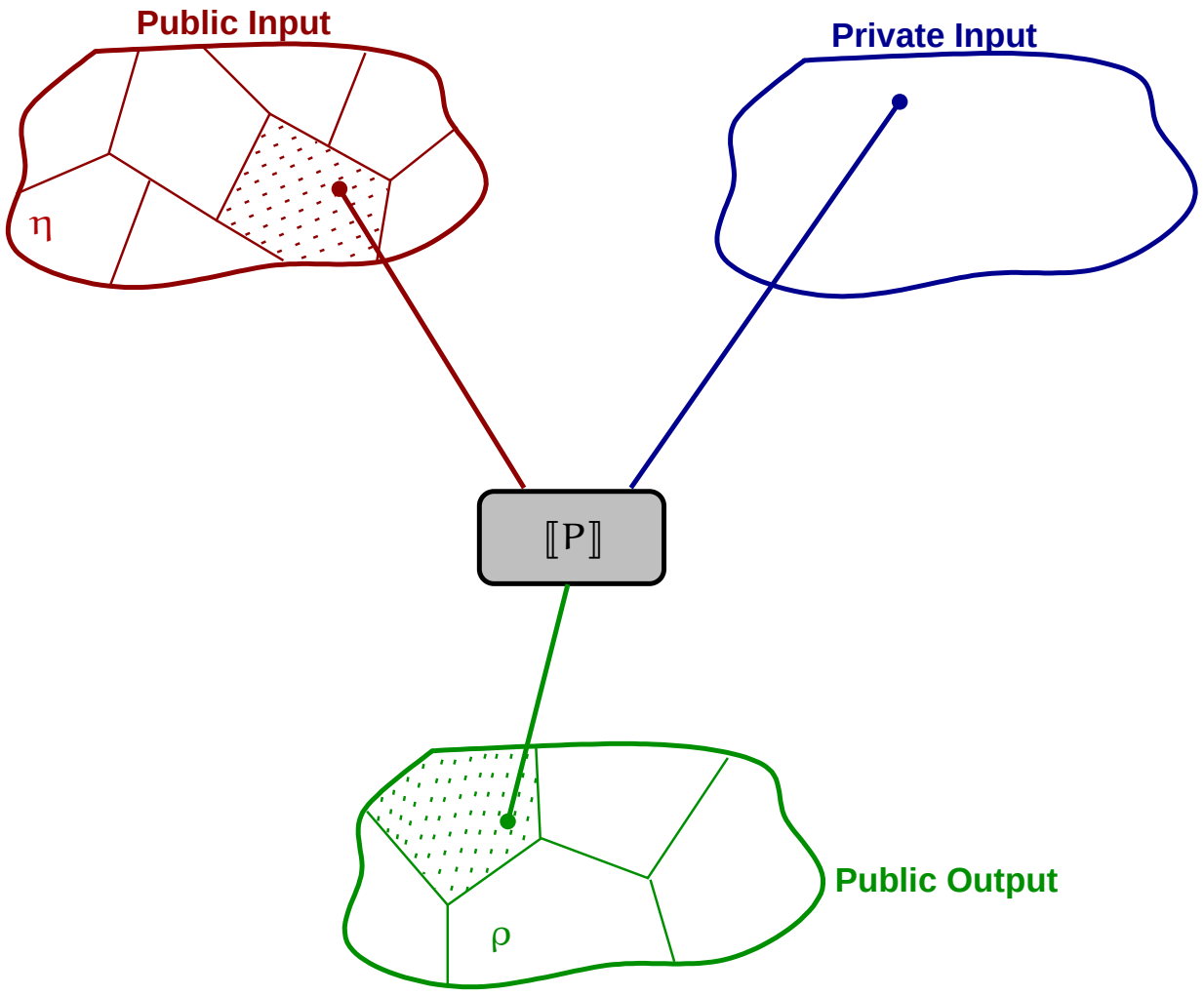
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})) \colon [\eta]\mathrm{P}(\rho) \colon \eta(l_1) = \eta(l_2) \Rightarrow \rho([\![\mathrm{P}]\!](h_1, l_1)^{\mathsf{L}}) = \rho([\![\mathrm{P}]\!](h_2, l_2)^{\mathsf{L}})$$

Abstracting non-interference I: Narrow ANI



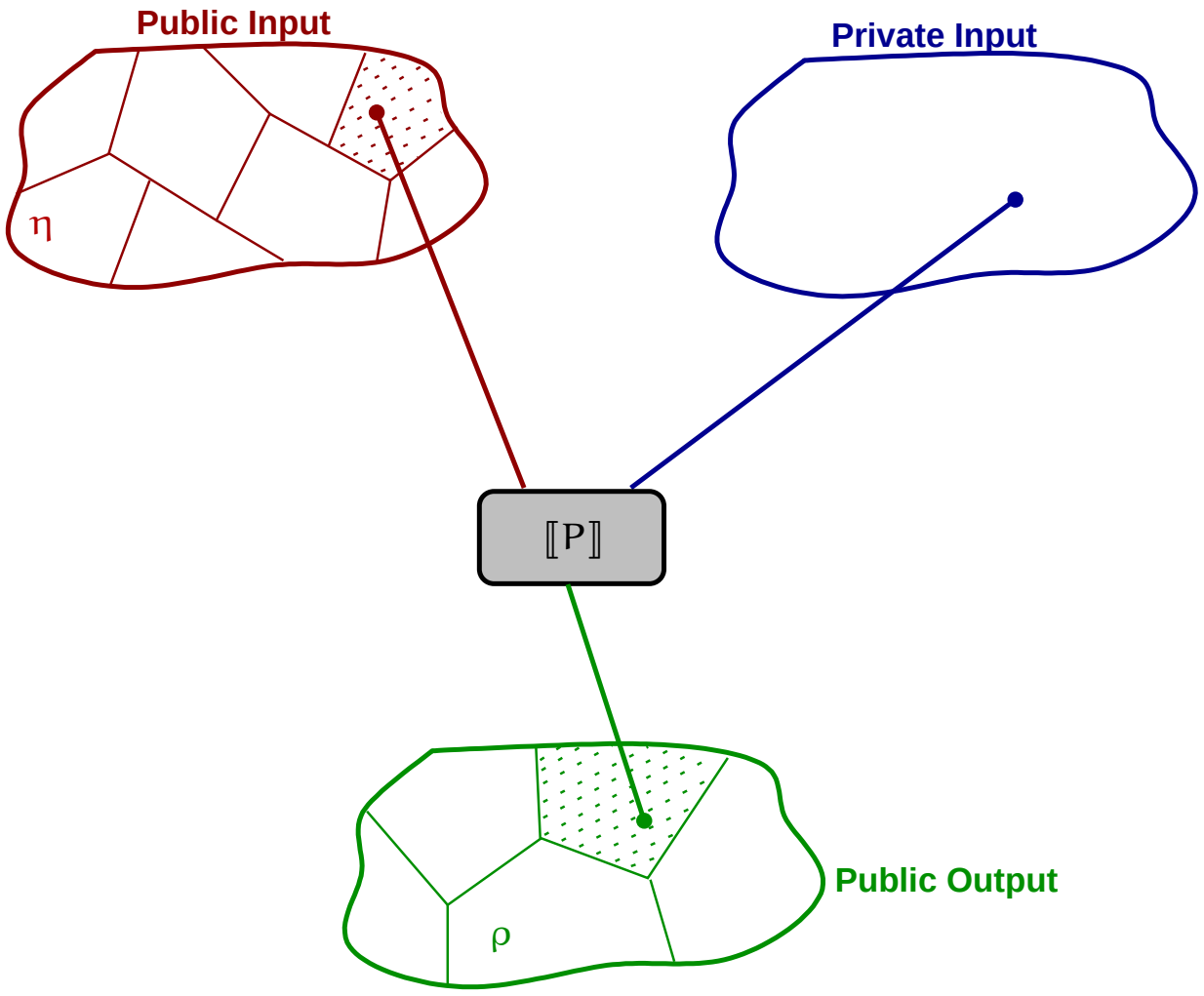
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})) \colon [\eta]\mathrm{P}(\rho) \colon \eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket \mathrm{P} \rrbracket(h_1, l_1)^{\mathsf{L}}) = \rho(\llbracket \mathrm{P} \rrbracket(h_2, l_2)^{\mathsf{L}})$$

Abstracting non-interference I: Narrow ANI



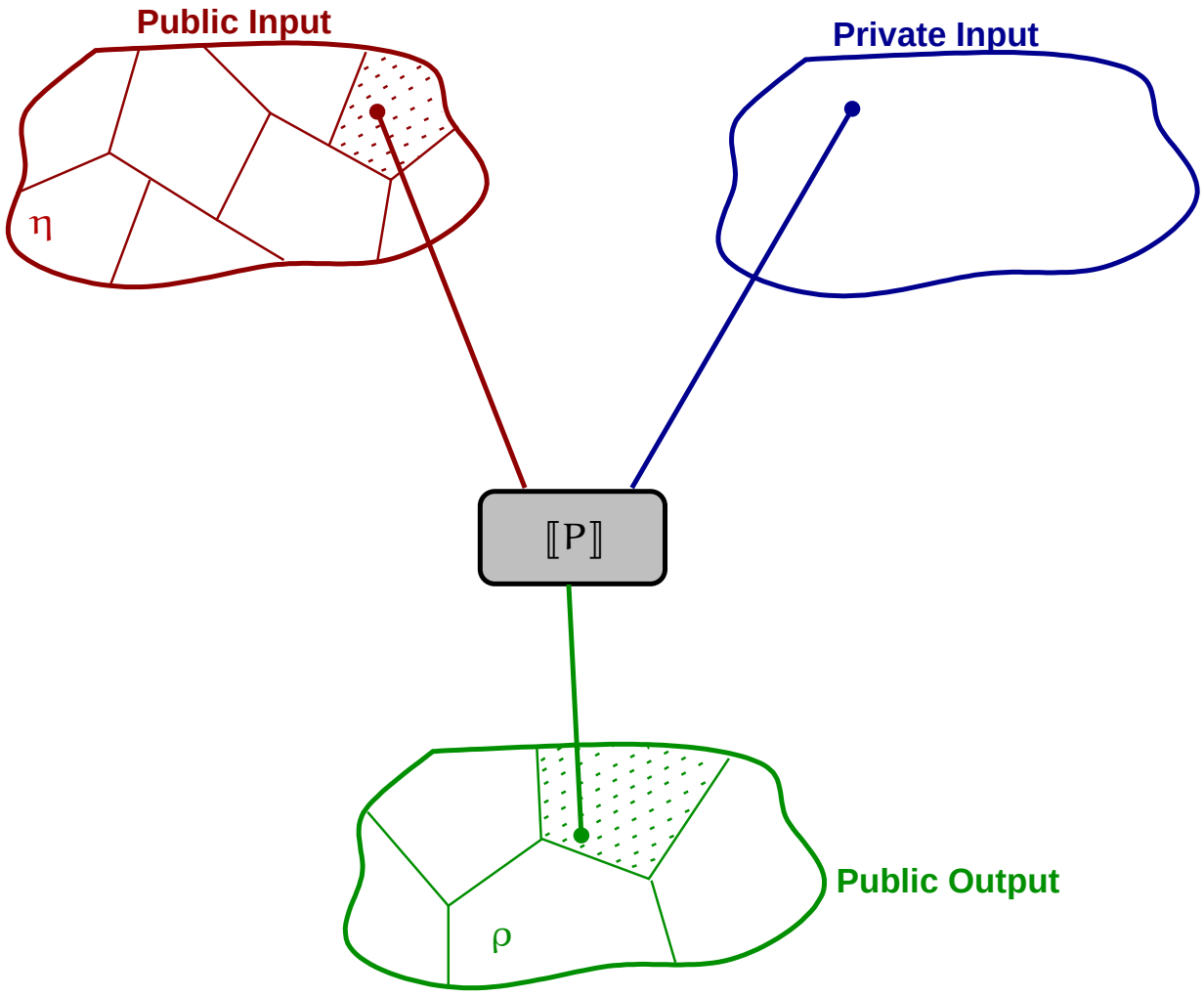
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})) \colon [\eta]\mathrm{P}(\rho) \colon \eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket \mathrm{P} \rrbracket(h_1, l_1)^{\mathsf{L}}) = \rho(\llbracket \mathrm{P} \rrbracket(h_2, l_2)^{\mathsf{L}})$$

Abstracting non-interference I: Narrow ANI



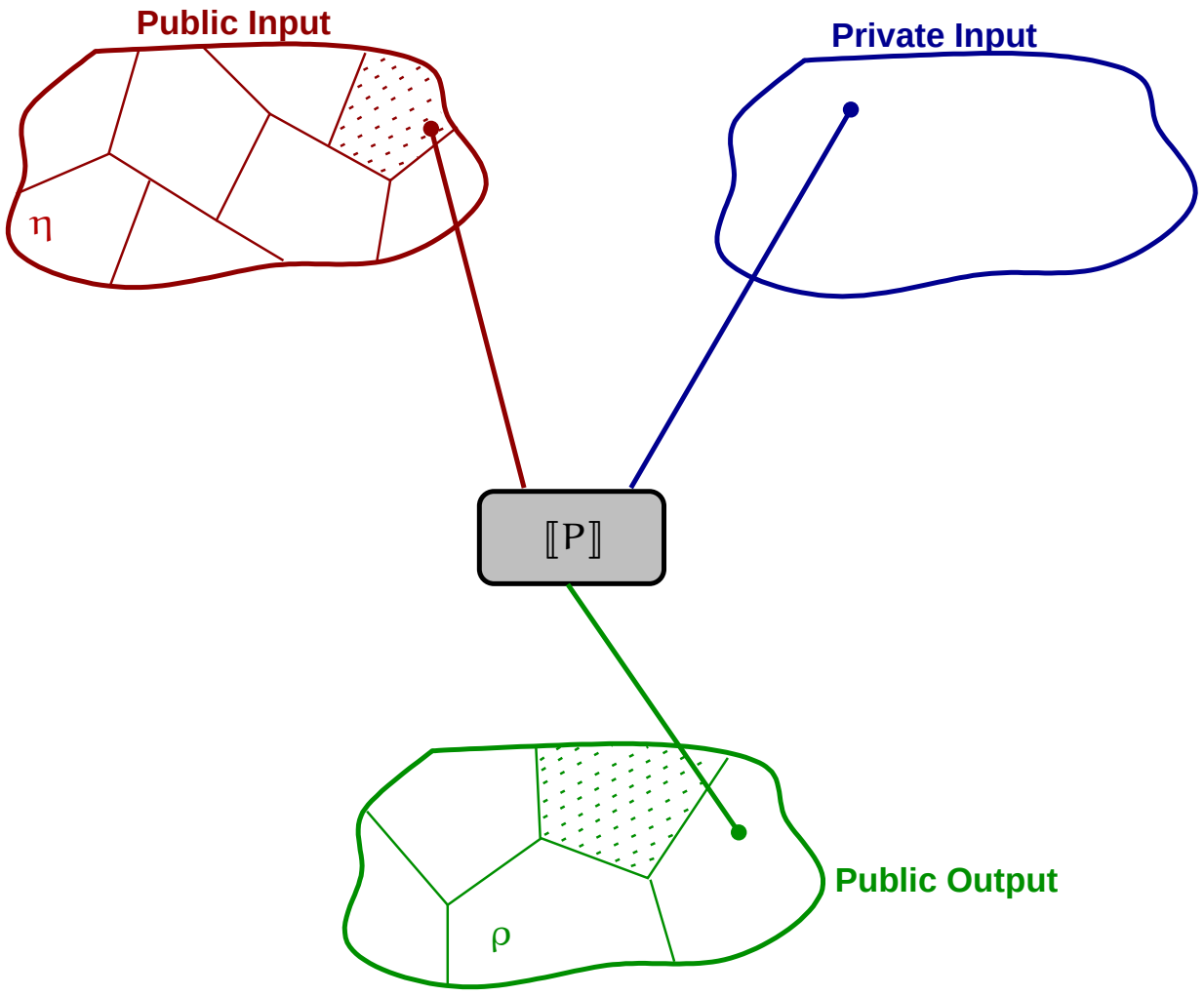
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})) \colon [\eta]\mathrm{P}(\rho) \colon \eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket \mathrm{P} \rrbracket(h_1, l_1)^{\mathsf{L}}) = \rho(\llbracket \mathrm{P} \rrbracket(h_2, l_2)^{\mathsf{L}})$$

Abstracting non-interference I: Narrow ANI



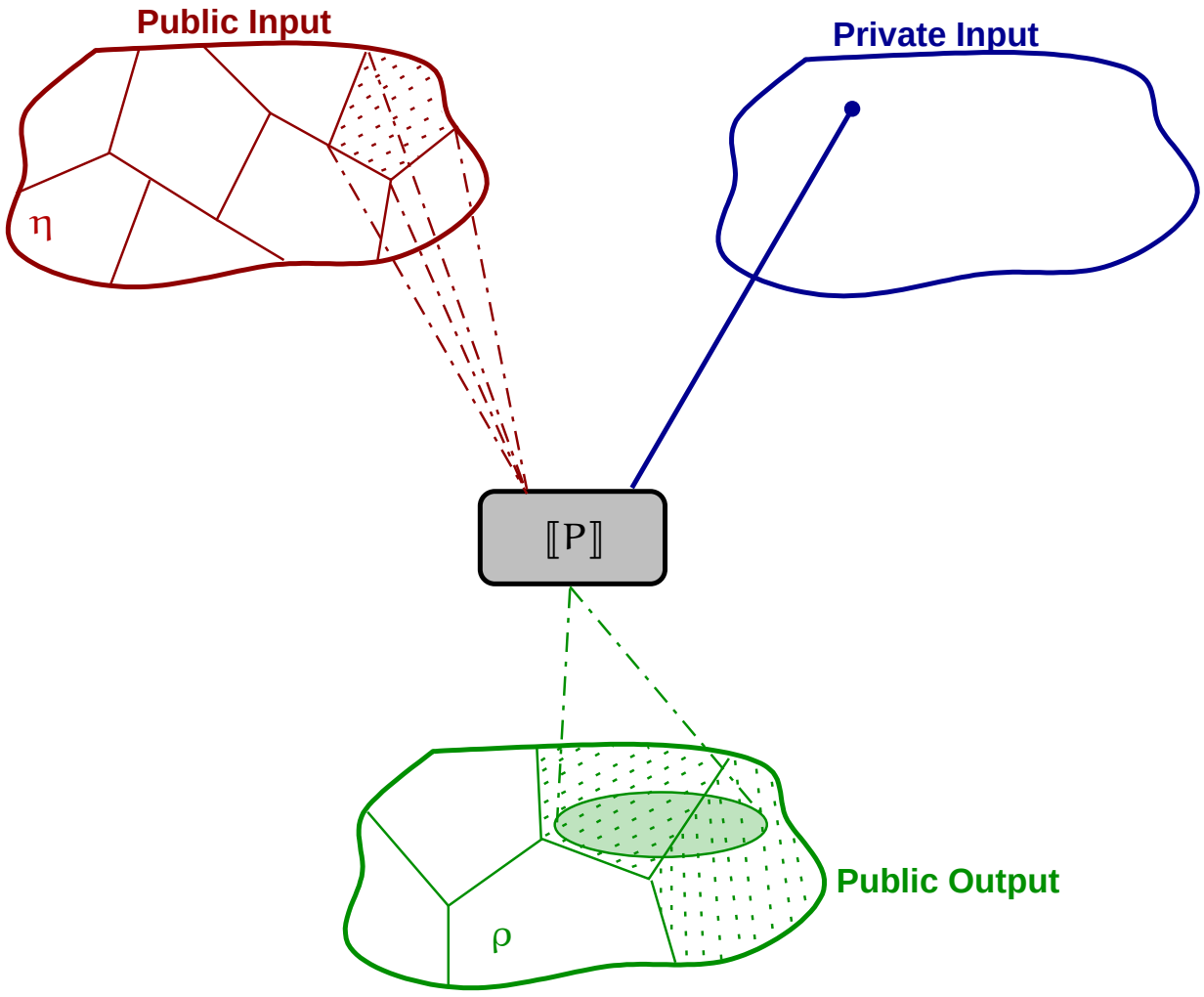
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})) \colon [\eta]\mathrm{P}(\rho) \colon \eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket \mathrm{P} \rrbracket(h_1, l_1)^{\mathsf{L}}) = \rho(\llbracket \mathrm{P} \rrbracket(h_2, l_2)^{\mathsf{L}})$$

Abstracting non-interference I: Narrow ANI



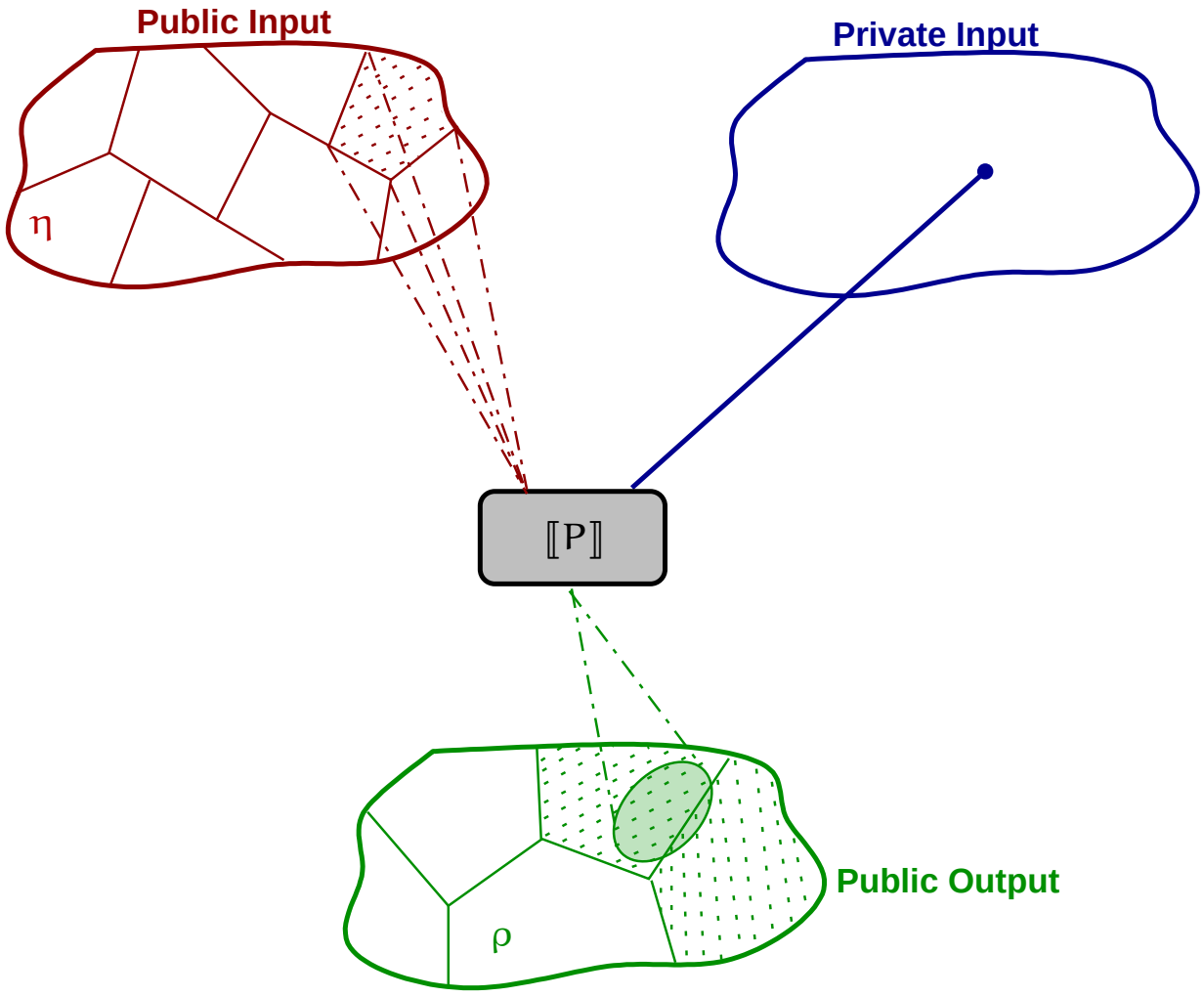
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})): [\eta]\mathrm{P}(\rho): \eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket \mathrm{P} \rrbracket(h_1, l_1)^{\mathsf{L}}) = \rho(\llbracket \mathrm{P} \rrbracket(h_2, l_2)^{\mathsf{L}})$$

Abstracting non-interference II



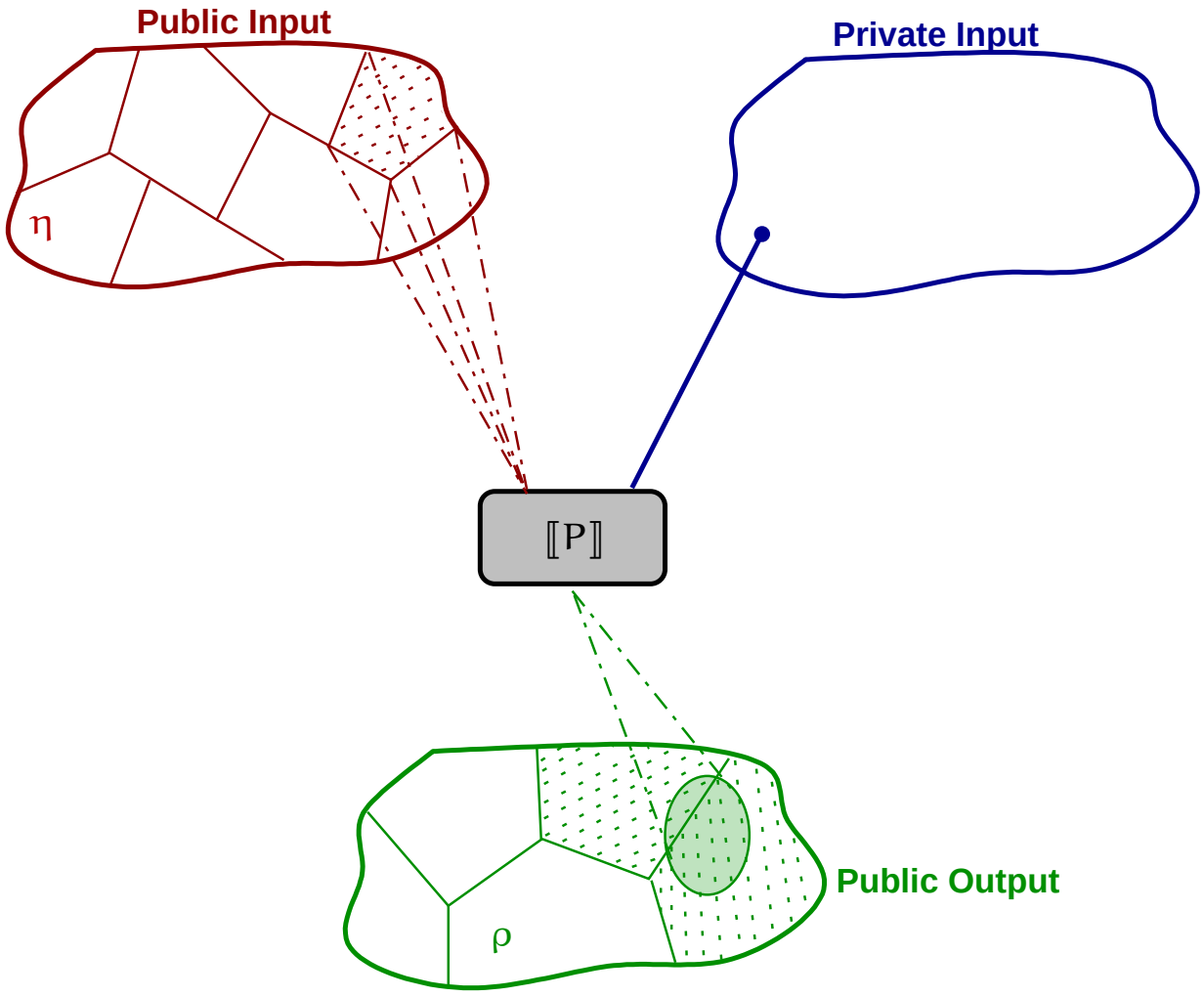
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})) \colon (\eta)\mathrm{P}(\rho) \colon$$
$$\eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket \mathrm{P} \rrbracket(h_1, \eta(l_1))^{\mathsf{L}}) = \rho(\llbracket \mathrm{P} \rrbracket(h_2, \eta(l_2))^{\mathsf{L}})$$

Abstracting non-interference II



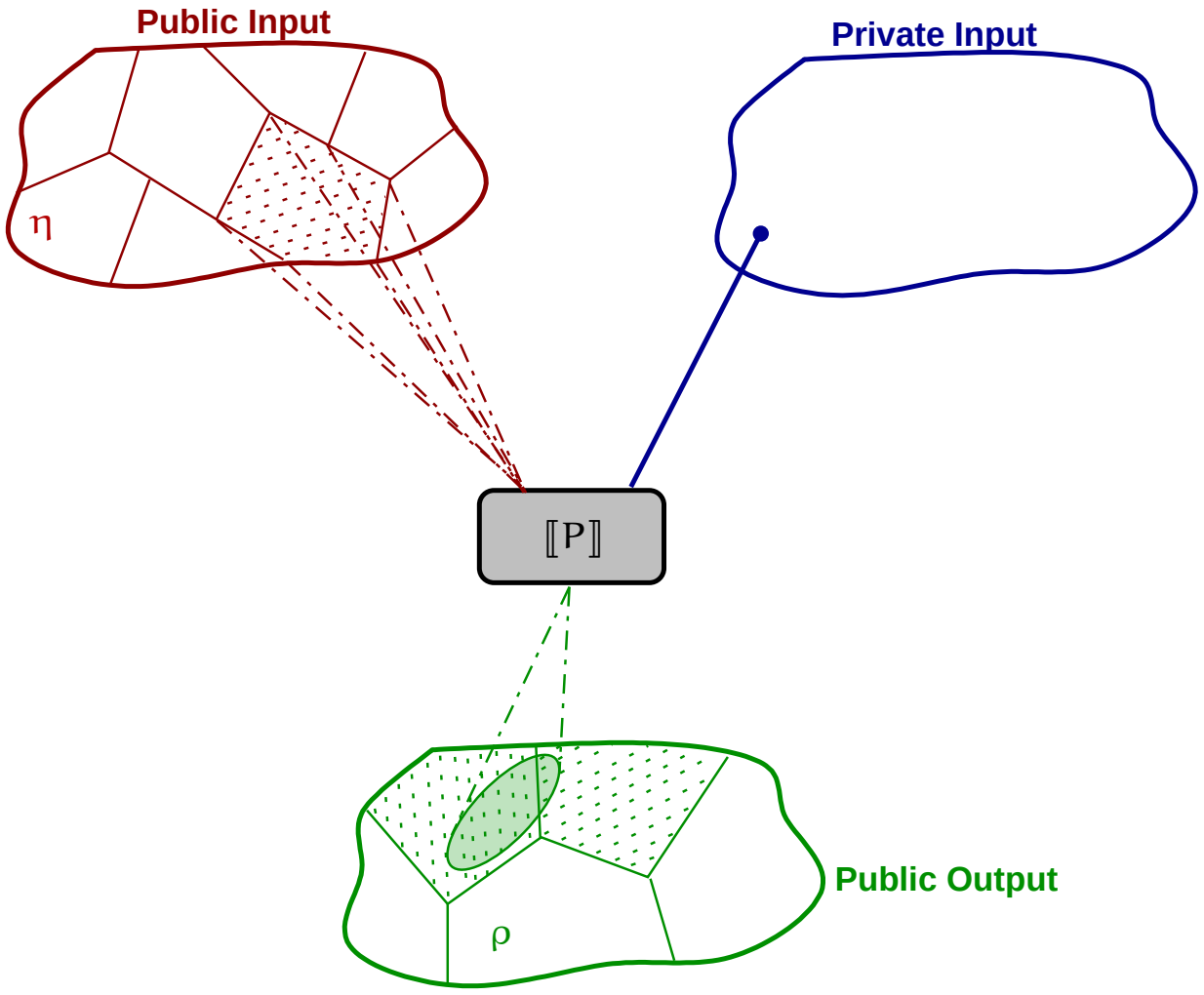
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})) \colon (\eta)\mathrm{P}(\rho) \colon$$
$$\eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket \mathrm{P} \rrbracket(h_1, \eta(l_1))^{\mathsf{L}}) = \rho(\llbracket \mathrm{P} \rrbracket(h_2, \eta(l_2))^{\mathsf{L}})$$

Abstracting non-interference II



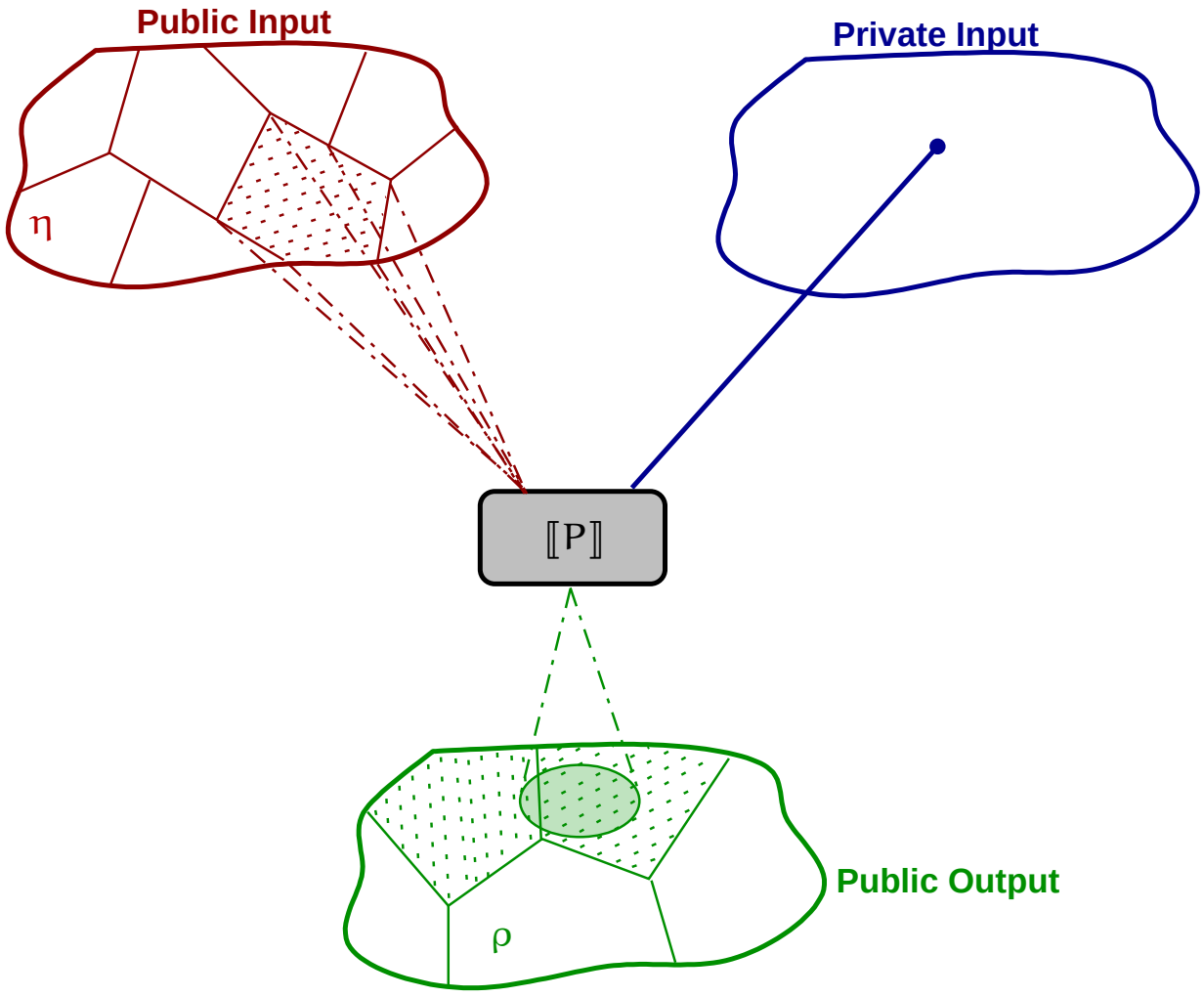
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})) \colon (\eta)\mathrm{P}(\rho) \colon$$
$$\eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket \mathrm{P} \rrbracket(h_1, \eta(l_1))^{\mathsf{L}}) = \rho(\llbracket \mathrm{P} \rrbracket(h_2, \eta(l_2))^{\mathsf{L}})$$

Abstracting non-interference II



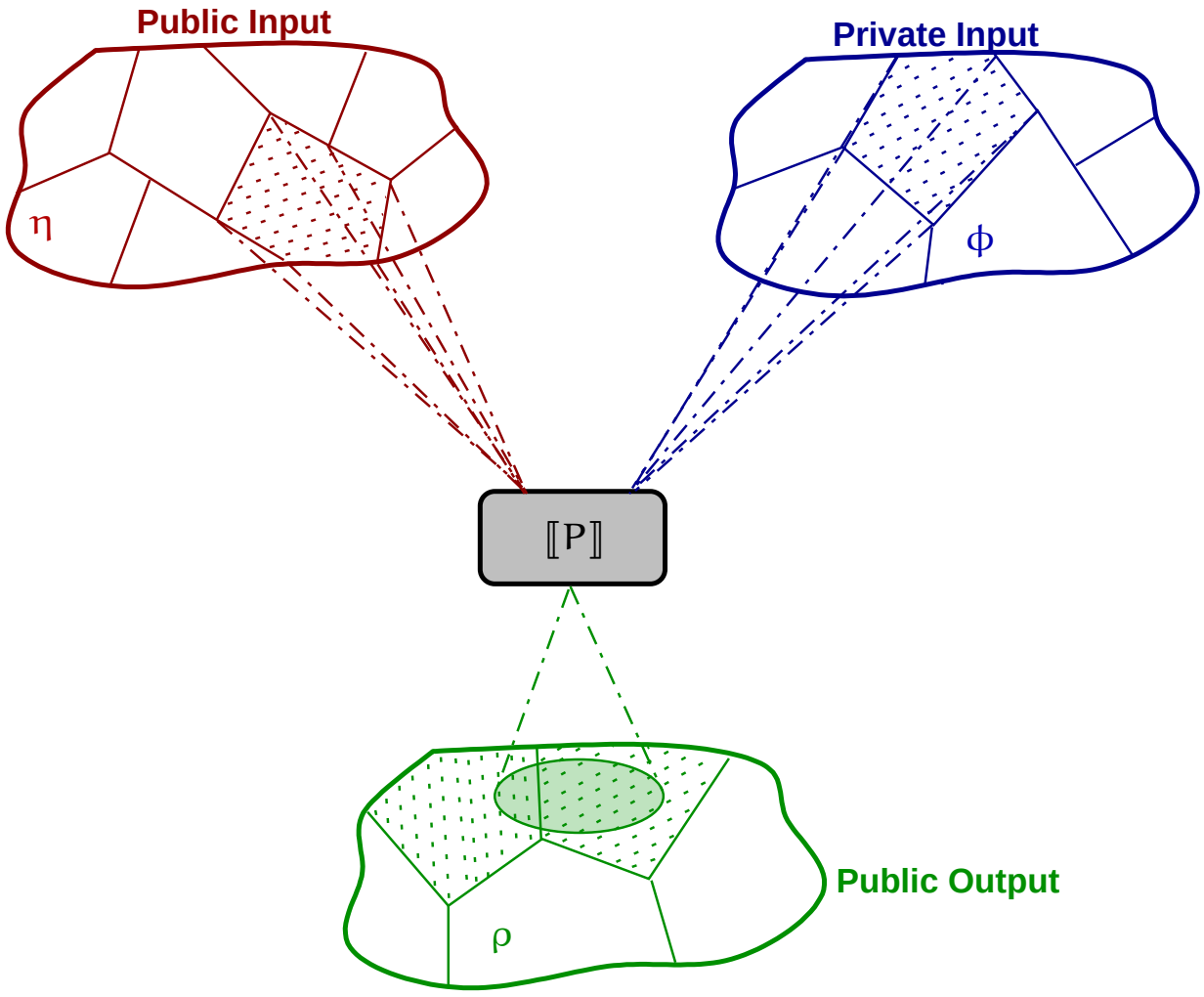
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})) \colon (\eta)\mathrm{P}(\rho) \colon$$
$$\eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket \mathrm{P} \rrbracket(h_1, \eta(l_1))^{\mathsf{L}}) = \rho(\llbracket \mathrm{P} \rrbracket(h_2, \eta(l_2))^{\mathsf{L}})$$

Abstracting non-interference II



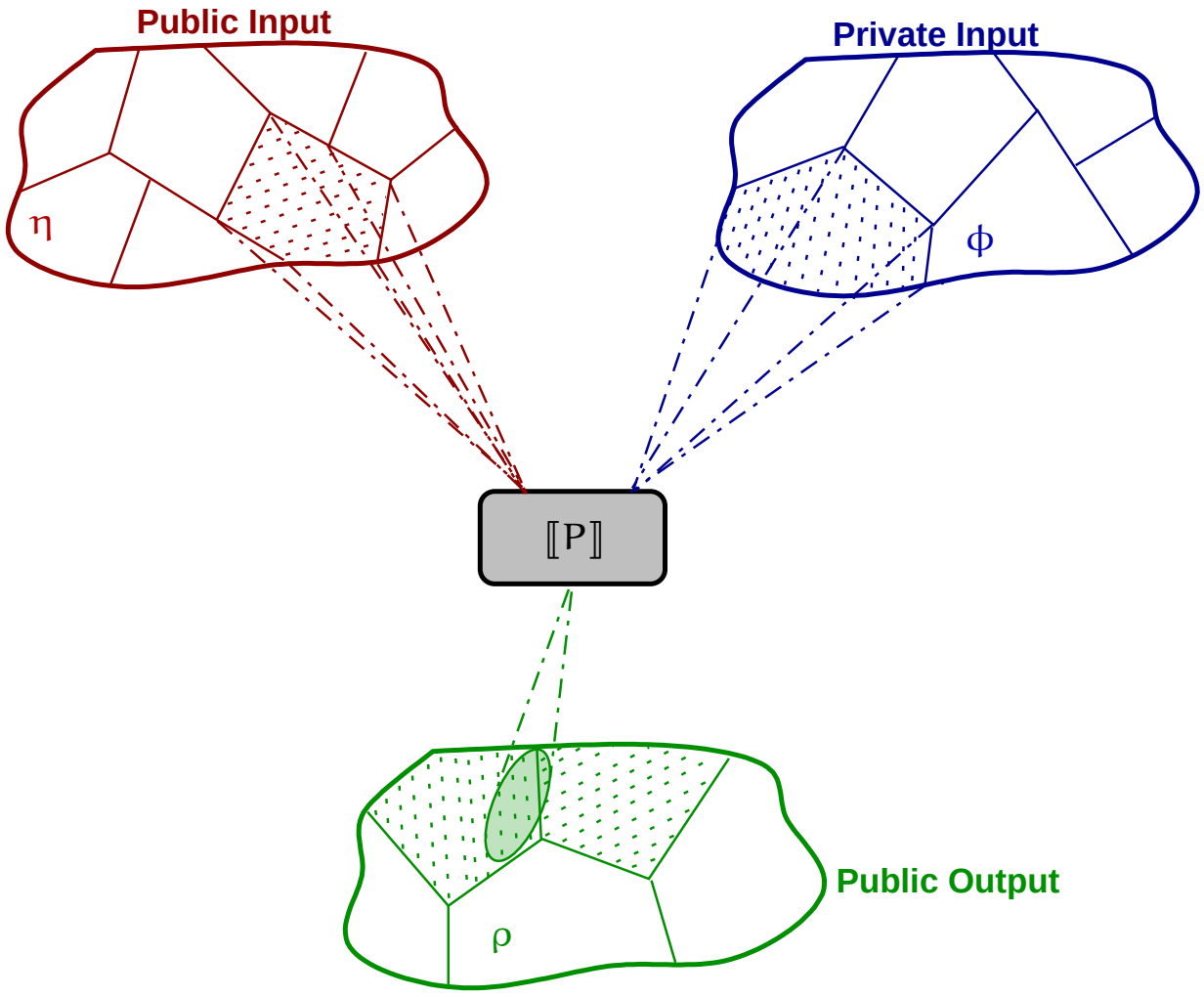
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})) \colon (\eta)\mathrm{P}(\rho) \colon$$
$$\eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket \mathrm{P} \rrbracket(h_1, \eta(l_1))^{\mathsf{L}}) = \rho(\llbracket \mathrm{P} \rrbracket(h_2, \eta(l_2))^{\mathsf{L}})$$

Abstracting non-interference III: ANI



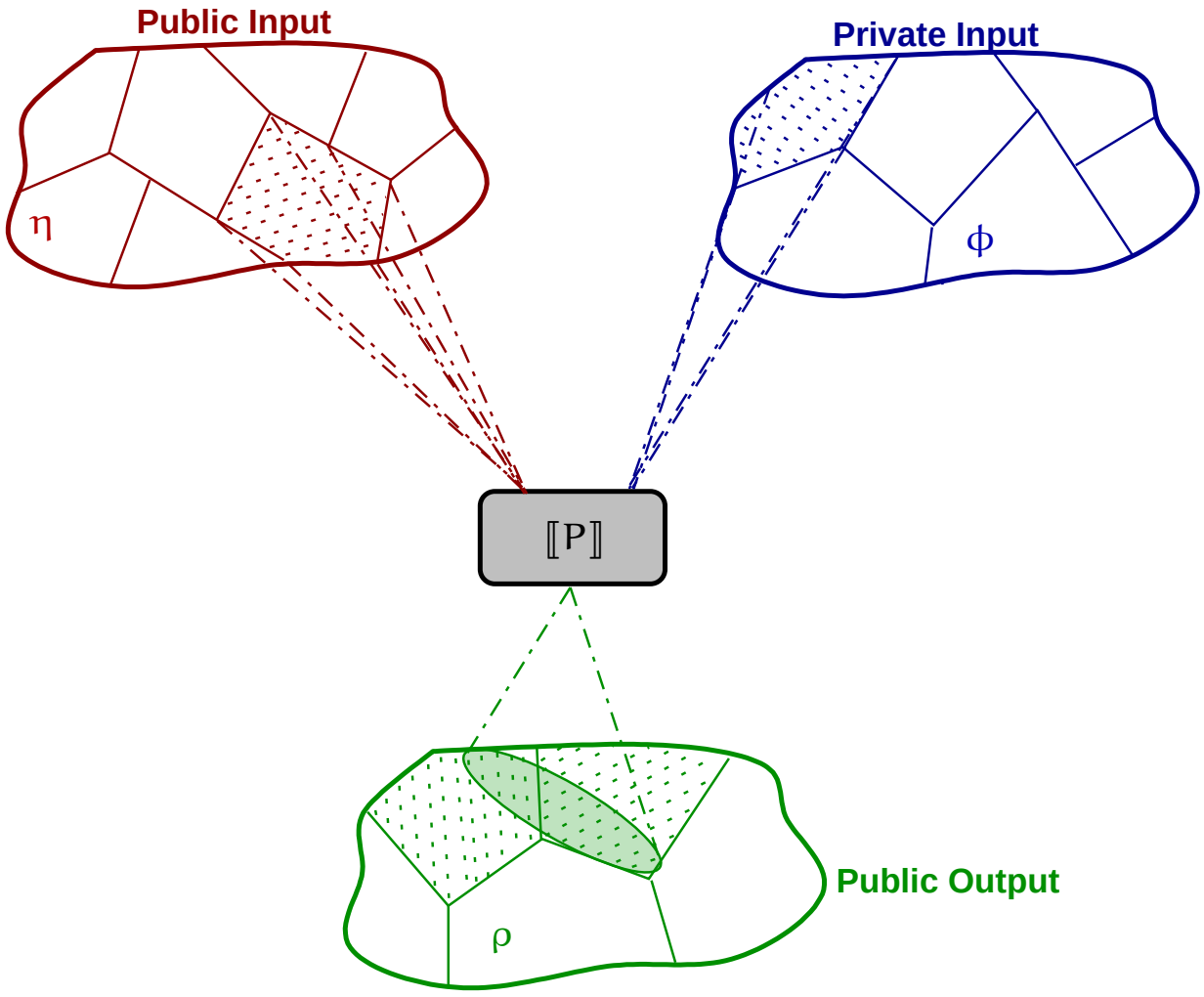
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})), \phi \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{H}})) \colon (\eta)\mathrm{P}(\phi \rightsquigarrow \rho) \colon$$
$$\eta(l_1) = \eta(l_2) \Rightarrow \rho([\![\mathrm{P}]\!](\phi(h_1), \eta(l_1))^{\mathsf{L}}) = \rho([\![\mathrm{P}]\!](\phi(h_2),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

Abstracting non-interference III: ANI



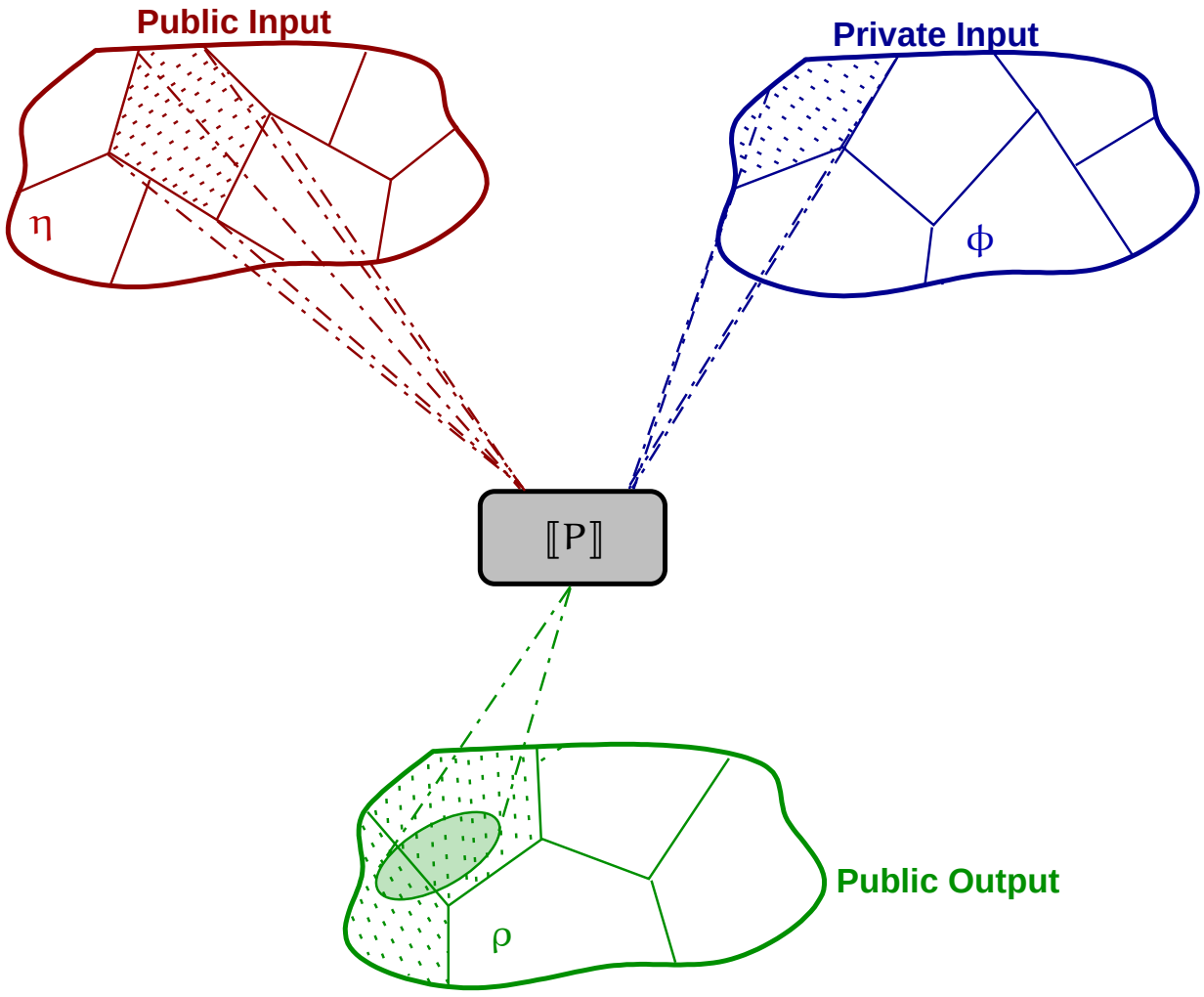
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})), \phi \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{H}})) \colon (\eta)\mathrm{P}(\phi \rightsquigarrow \rho) \colon$$
$$\eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket \mathrm{P} \rrbracket(\phi(h_1), \eta(l_1))^{\mathsf{L}}) = \rho(\llbracket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

Abstracting non-interference III: ANI



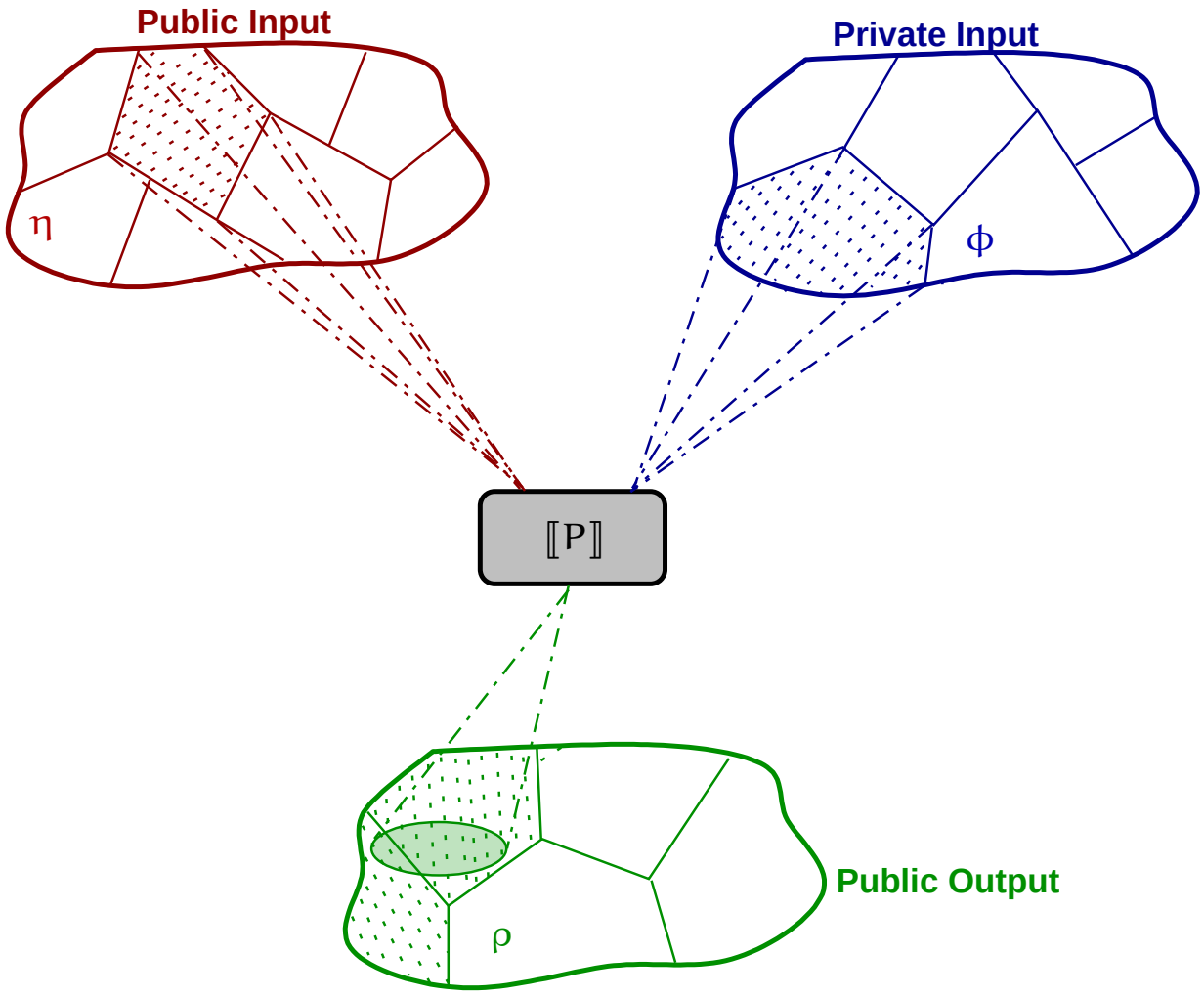
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})), \phi \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{H}})) \colon (\eta)\mathrm{P}(\phi \rightsquigarrow \rho) \colon$$
$$\eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket \mathrm{P} \rrbracket(\phi(h_1), \eta(l_1))^{\mathsf{L}}) = \rho(\llbracket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

Abstracting non-interference III: ANI



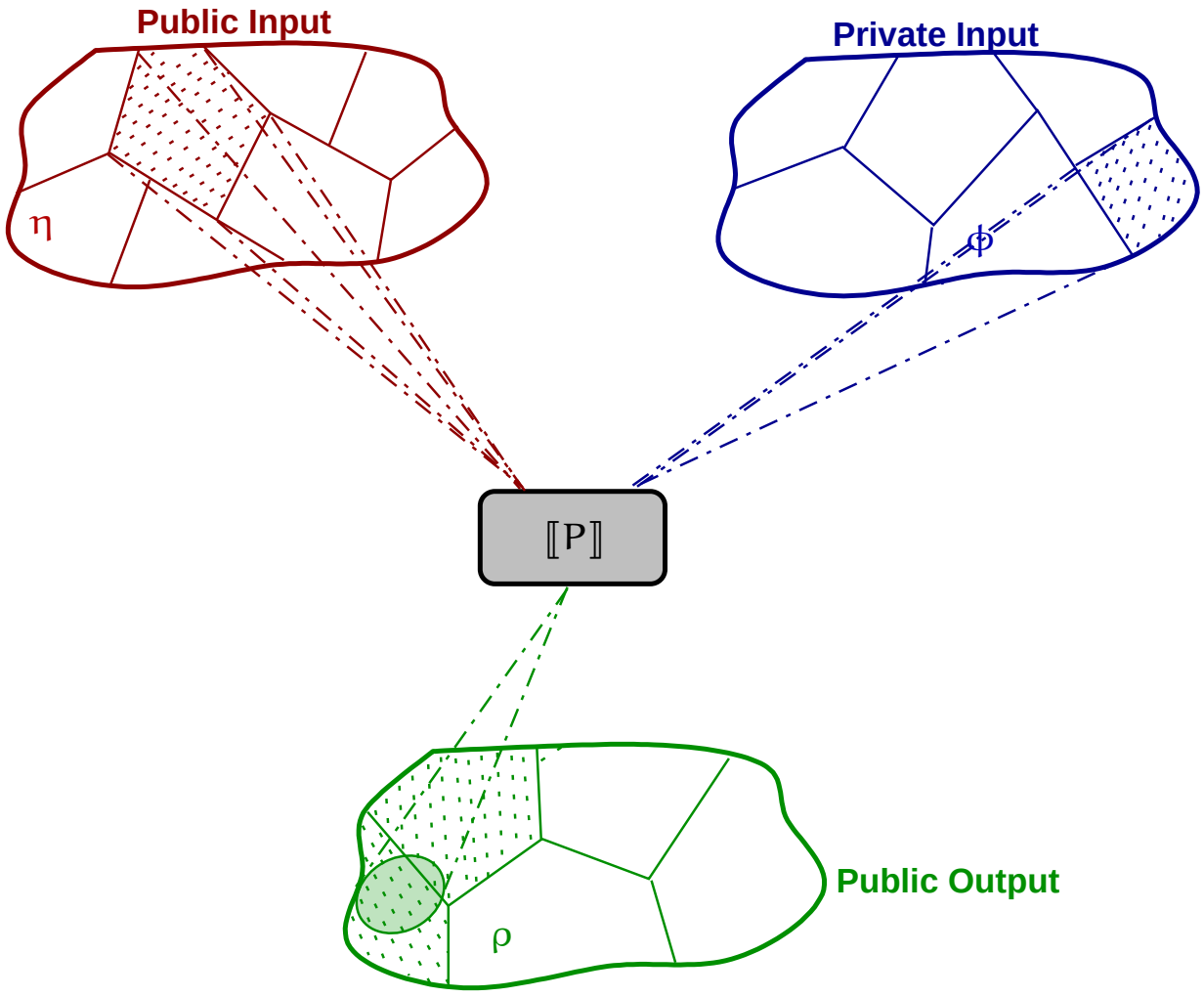
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})), \phi \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{H}})) \colon (\eta)\mathrm{P}(\phi \rightsquigarrow \rho) \colon$$
$$\eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket \mathrm{P} \rrbracket(\phi(h_1), \eta(l_1))^{\mathsf{L}}) = \rho(\llbracket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

Abstracting non-interference III: ANI



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

Abstracting non-interference III: ANI



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

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 $(\eta)\mathrm{P}(\phi \rightsquigarrow\!\!\!\!\!\!\Vdash \rho)$

  [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.

Generalized abstract non-interference

Non-Interference

Corresponds to asking that the behavior of the chosen relevant aspects of the computation be invariant with respect to what an attacker may observe.

Generalized abstract non-interference

NON-INTERFERENCE

Corresponds to asking that the behavior of the chosen relevant aspects of the computation be invariant with respect to what an attacker may observe.

- α_{OBS}: Specifies the semantics of the computations relevant for interference (*observation abstraction*);

Generalized abstract non-interference

NON-INTERFERENCE

Corresponds to asking that the behavior of the chosen relevant aspects of the computation be invariant with respect to what an attacker may observe.

- α_{OBS}: Specifies the semantics of the computations relevant for interference (*observation abstraction*);
- α_{INT}: Specifies the maximum amount of information that an attacker may observe concerning a computation (*interference abstraction*);

Generalized abstract non-interference

NON-INTERFERENCE

Corresponds to asking that the behavior of the chosen relevant aspects of the computation be invariant with respect to what an attacker may observe.

- α_{OBS}: Specifies the semantics of the computations relevant for interference (*observation abstraction*);
- α_{INT}: Specifies the maximum amount of information that an attacker may observe concerning a computation (*interference abstraction*);
- α_{ATT}: Characterizes what the model of the attacker can observe about the system behavior (*attacker abstraction*).

Generalized abstract non-interference

NON-INTERFERENCE

Corresponds to asking that the behavior of the chosen relevant aspects of the computation be invariant with respect to what an attacker may observe.

- α_{OBS}: Specifies the semantics of the computations relevant for interference (*observation abstraction*);
- α_{INT}: Specifies the maximum amount of information that an attacker may observe concerning a computation (*interference abstraction*);
- α_{ATT}: Characterizes what the model of the attacker can observe about the system behavior (*attacker abstraction*).

$$\alpha_{ATT} \circ \alpha_{OBS}([\![\mathrm{P}]\!]) = \alpha_{ATT} \circ \alpha_{INT} \circ \alpha_{OBS}([\![\mathrm{P}]\!]).$$

Generalized abstract non-interference

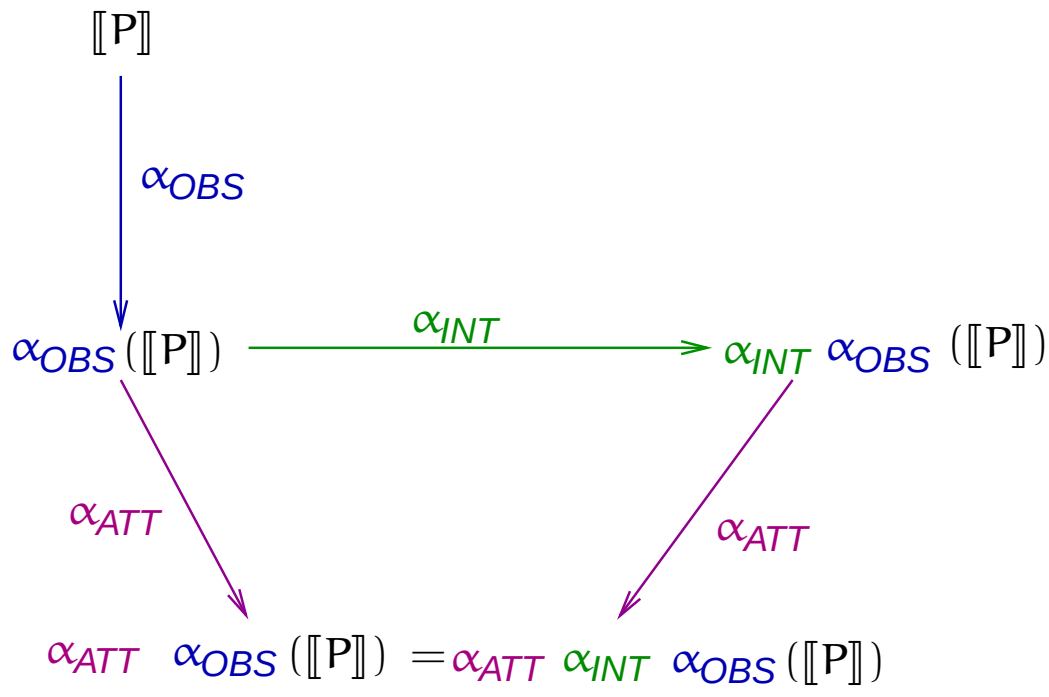
NON-INTERFERENCE

Corresponds to asking that the behavior of the chosen relevant aspects of the computation be invariant with respect to what an attacker may observe.

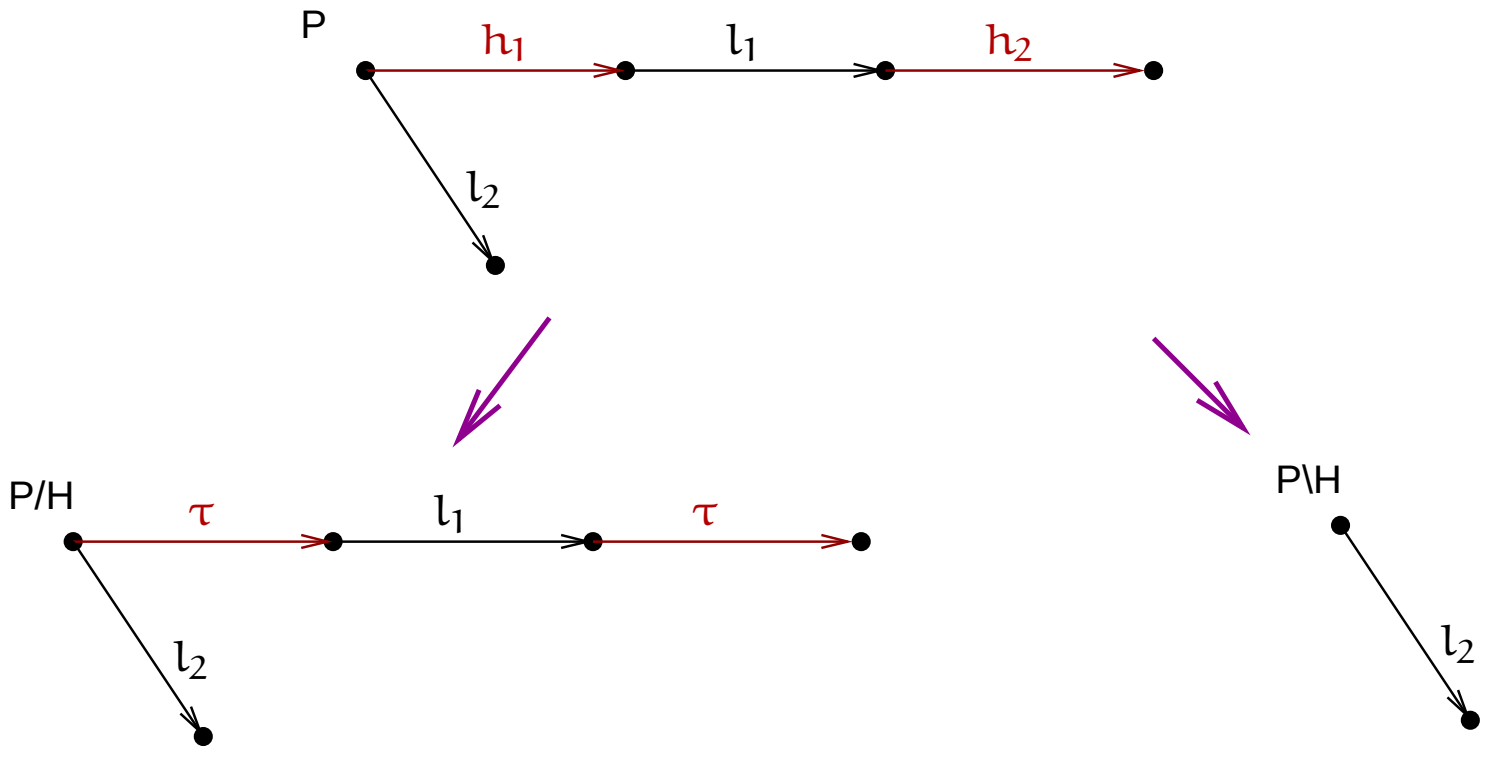
- α_{OBS}: Specifies the semantics of the computations relevant for interference (*observation abstraction*);
- α_{INT}: Specifies the maximum amount of information that an attacker may observe concerning a computation (*interference abstraction*);
- α_{ATT}: Characterizes what the model of the attacker can observe about the system behavior (*attacker abstraction*).

$\Rightarrow$ We characterize the minimal abstraction of α_{ATT} that guarantees GANI.

The global picture



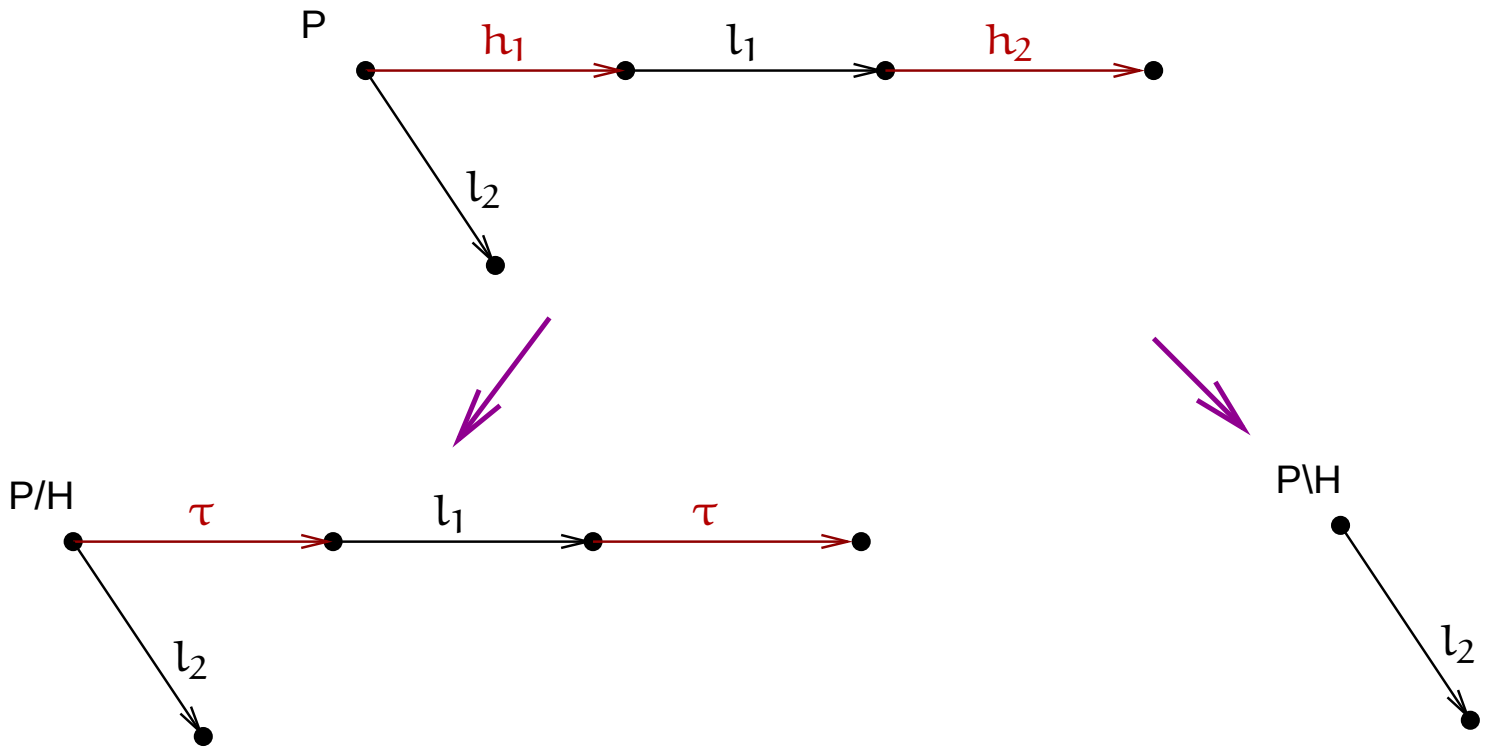
A general framework



SNNI= $P/H \approx P\backslash H$

[Focardi & Gorrieri '95]

A general framework

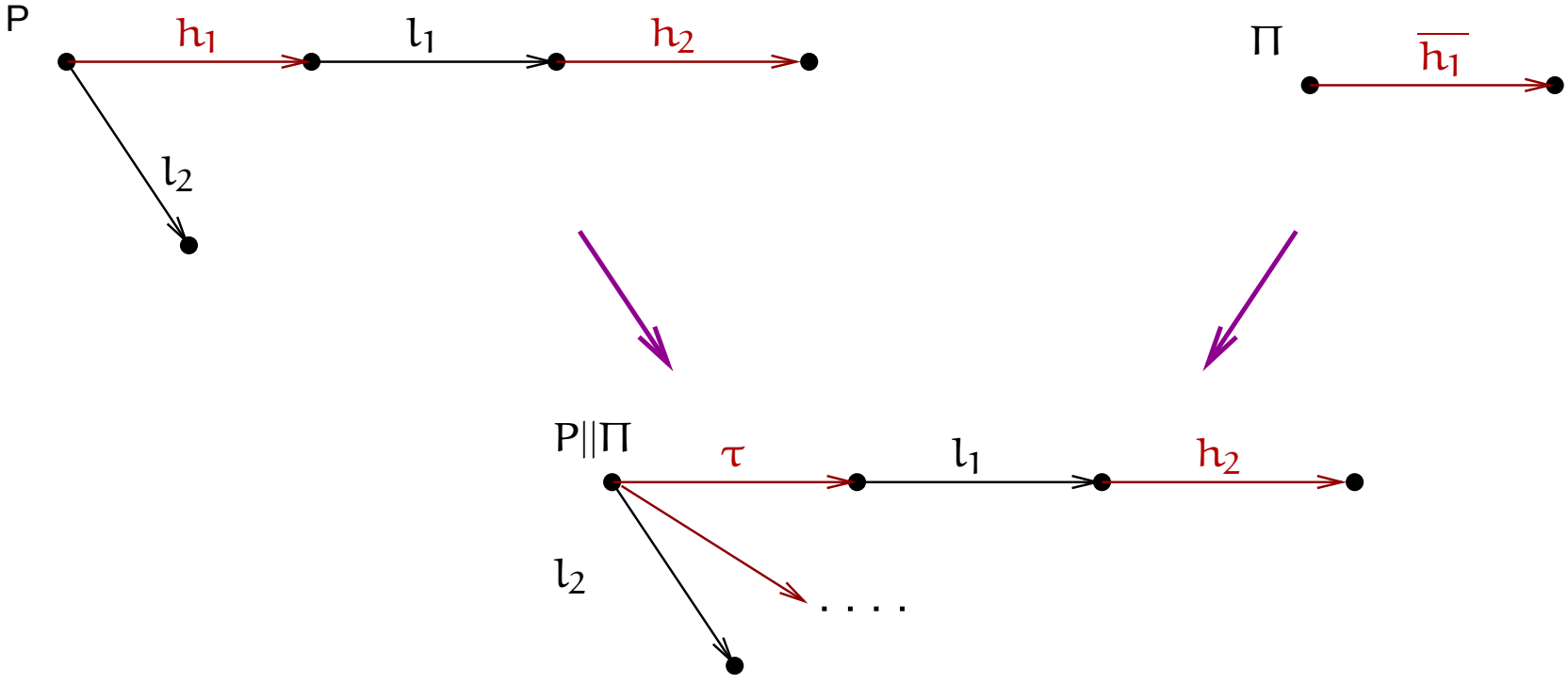


SNNI= $P/H \approx P\backslash H$

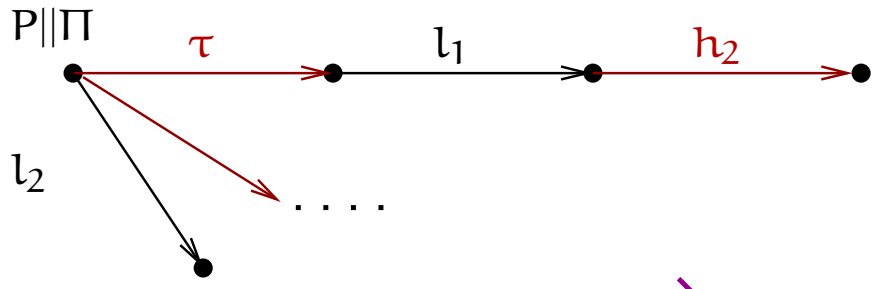
$$\Downarrow$$

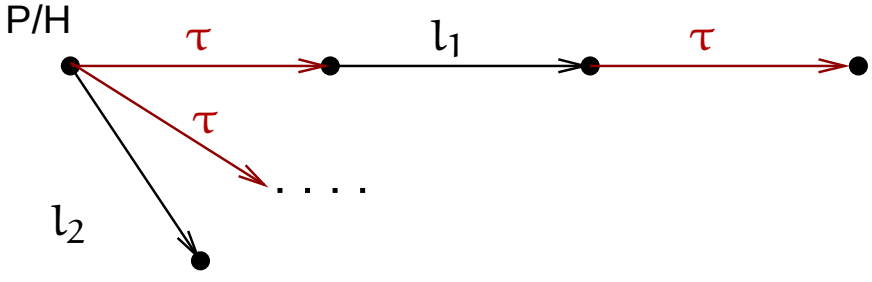
$$\text{SNNI} = \alpha_T \circ \alpha_{low} \circ id([\![P]\!]) = \alpha_T \circ \alpha_{low} \circ \alpha_L \circ id([\![P]\!]).$$

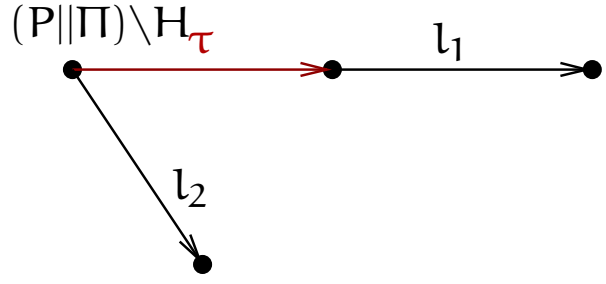
A general framework



A general framework



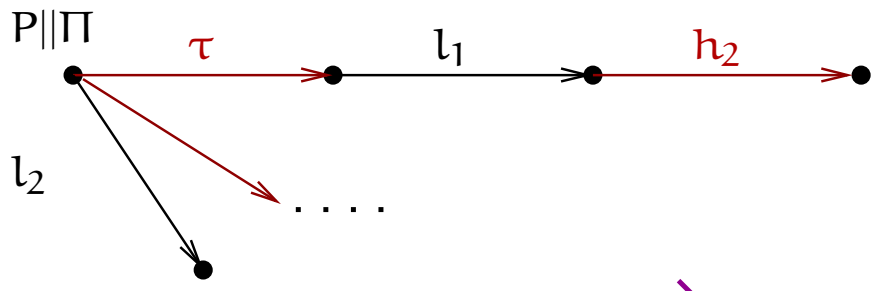


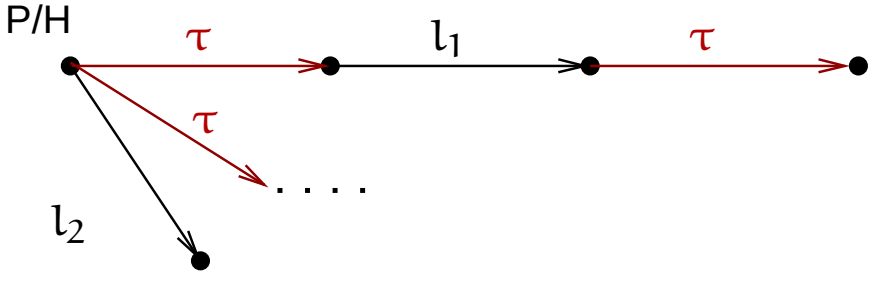


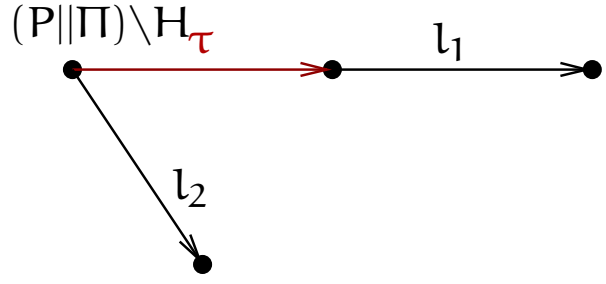
BNDC= $\forall \Pi.\ P/H \approx_B (P||\Pi)\backslash H$

[Focardi & Gorrieri '95]

A general framework





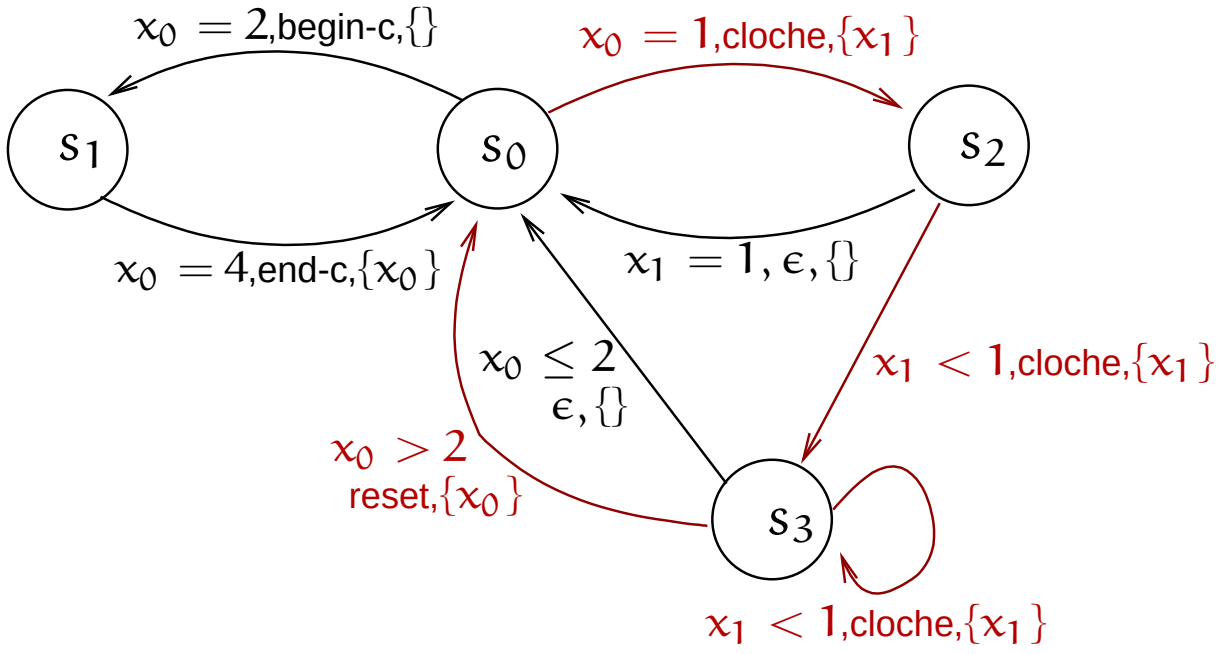


$$\text{BNDC} = \forall \Pi.\ P/H \approx_B (P||\Pi)\backslash H$$

$$\Downarrow$$

$$\text{BNDC} = \forall \Pi.\ \alpha_B \circ \alpha_L \circ id([\![P||\Pi]\!]) = \alpha_B \circ \alpha_L \circ \alpha_{sec} \circ id([\![P||\Pi]\!]).$$

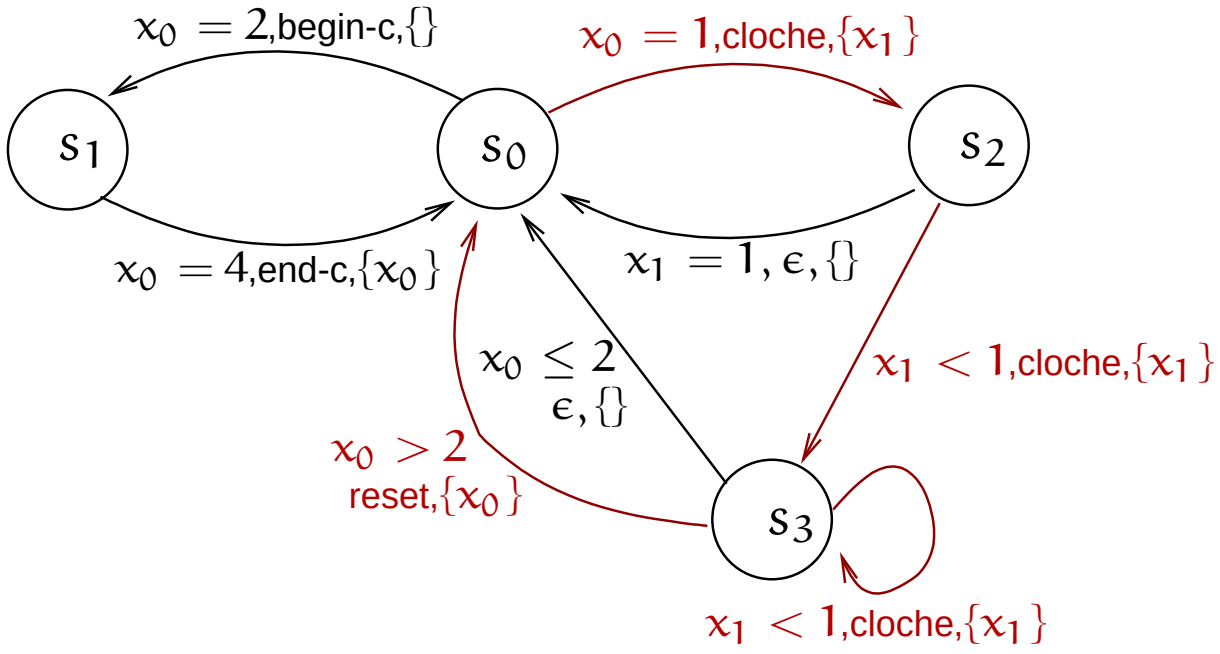
A general framework



n-Non-Int = $\mathcal{L}^n_H/H = \mathcal{L}|_L$

[Barbuti et al. '02]

A general framework



$$n\text{-Non-Int} = \mathcal{L}^n_H / H = \mathcal{L}|_L$$

$$\Downarrow$$

$$\boxed{n\text{-Non-Int} = \alpha_{low} \circ \alpha_n(\llbracket P \rrbracket) = \alpha_{low} \circ \alpha_L \circ \alpha_n(\llbracket P \rrbracket).}$$

Conclusion

- We introduced a generalized notion of Abstract Non-Interference for dealing with computational systems modeled by computational trees;

Conclusion

- We introduced a generalized notion of Abstract Non-Interference for dealing with computational systems modeled by computational trees;
- We show that many of the known notions of Non-Interference can be modeled as instantiation of GANI;

Conclusion

- We introduced a generalized notion of Abstract Non-Interference for dealing with computational systems modeled by computational trees;
- We show that many of the known notions of Non-Interference can be modeled as instantiation of GANI;
- We believe that generalized abstract non-interference may provide advanced techniques for analysing in a *modular* way how sub-components *interact* (e.g. in biological systems).

Conclusion

- We introduced a generalized notion of Abstract Non-Interference for dealing with computational systems modeled by computational trees;
- We show that many of the known notions of Non-Interference can be modeled as instantiation of GANI;
- We believe that generalized abstract non-interference may provide advanced techniques for analysing in a *modular* way how sub-components *interact* (e.g. in biological systems).
- We are working for designing a tool support for checking generalized abstract non-interference properties.