TIMED ABSTRACT NON-INTERFERENCE

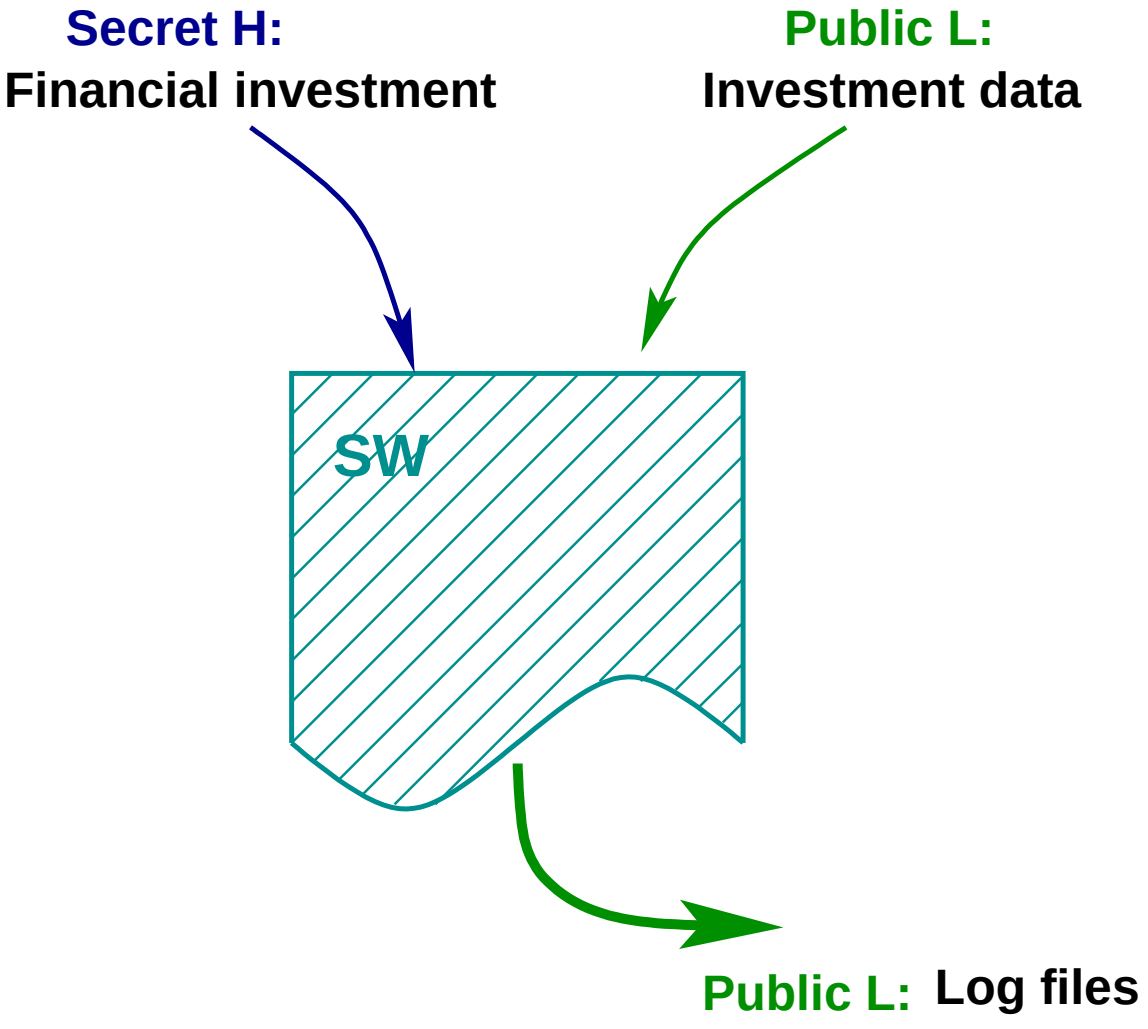
Roberto Giacobazzi and **Isabella Mastroeni**

Dipartimento di informatica

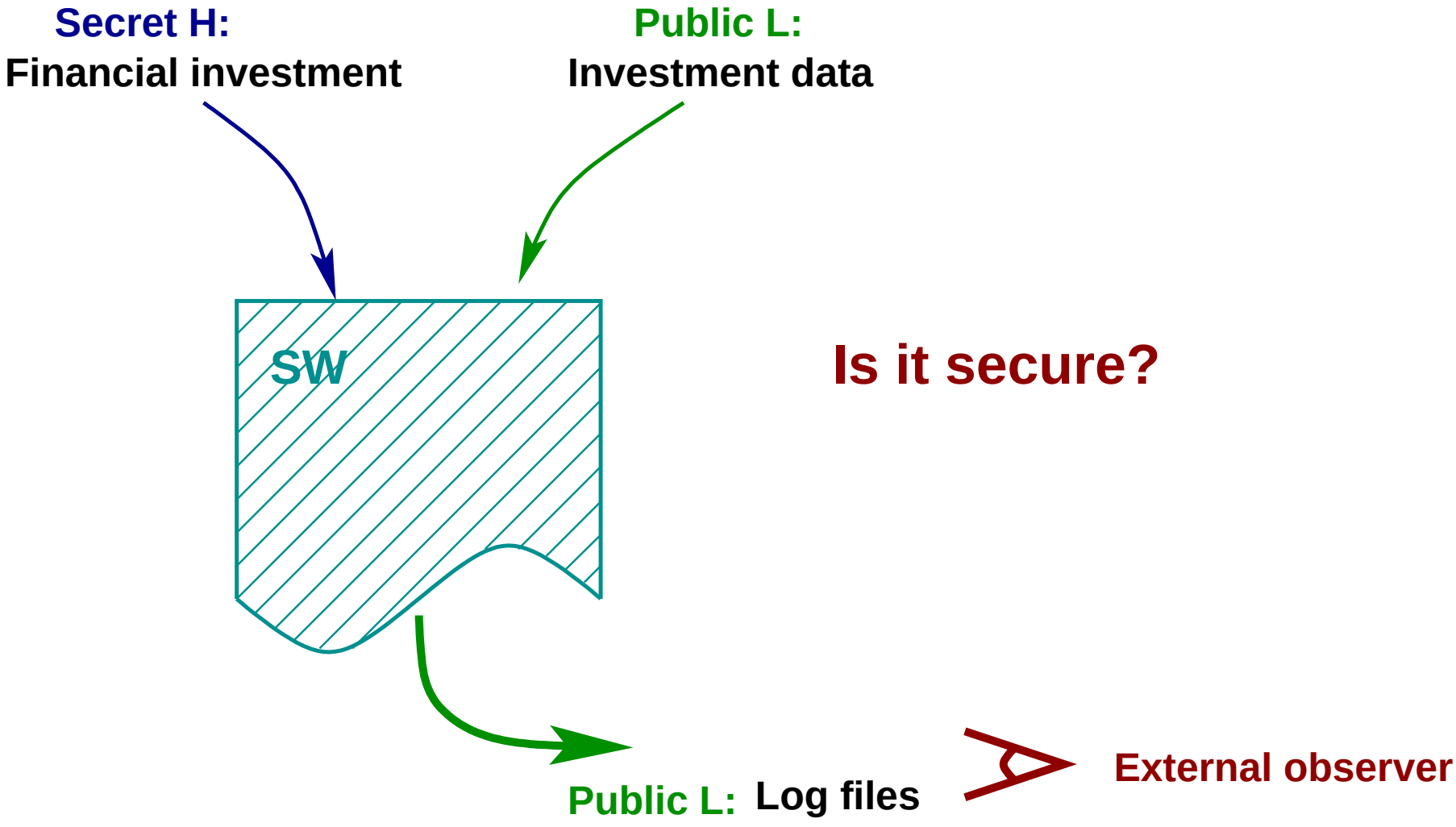
Università di Verona, Italy

FORMATS'05, September 28, 2005

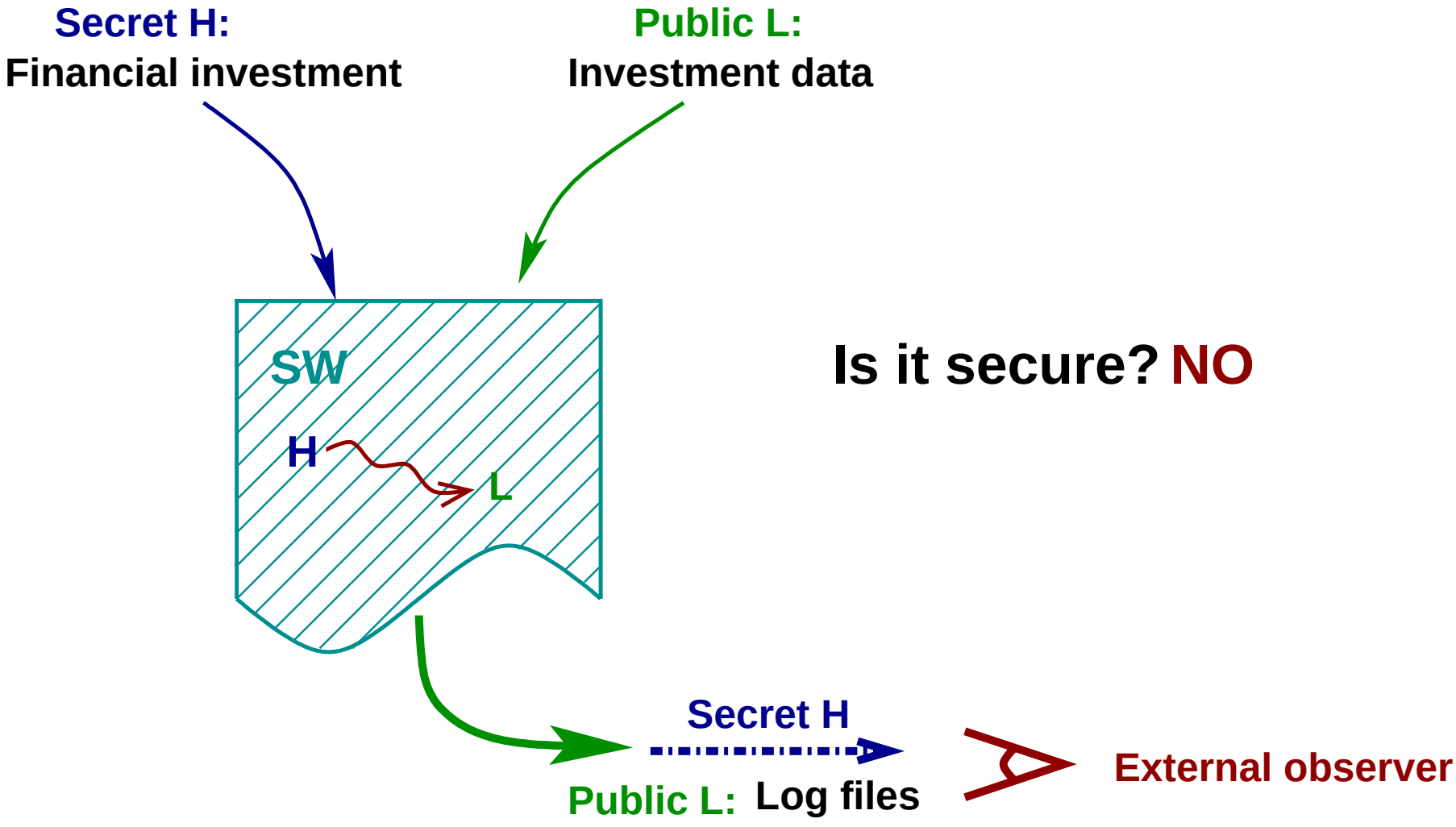
The Problem: Non-Interference



The Problem: Non-Interference



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.*

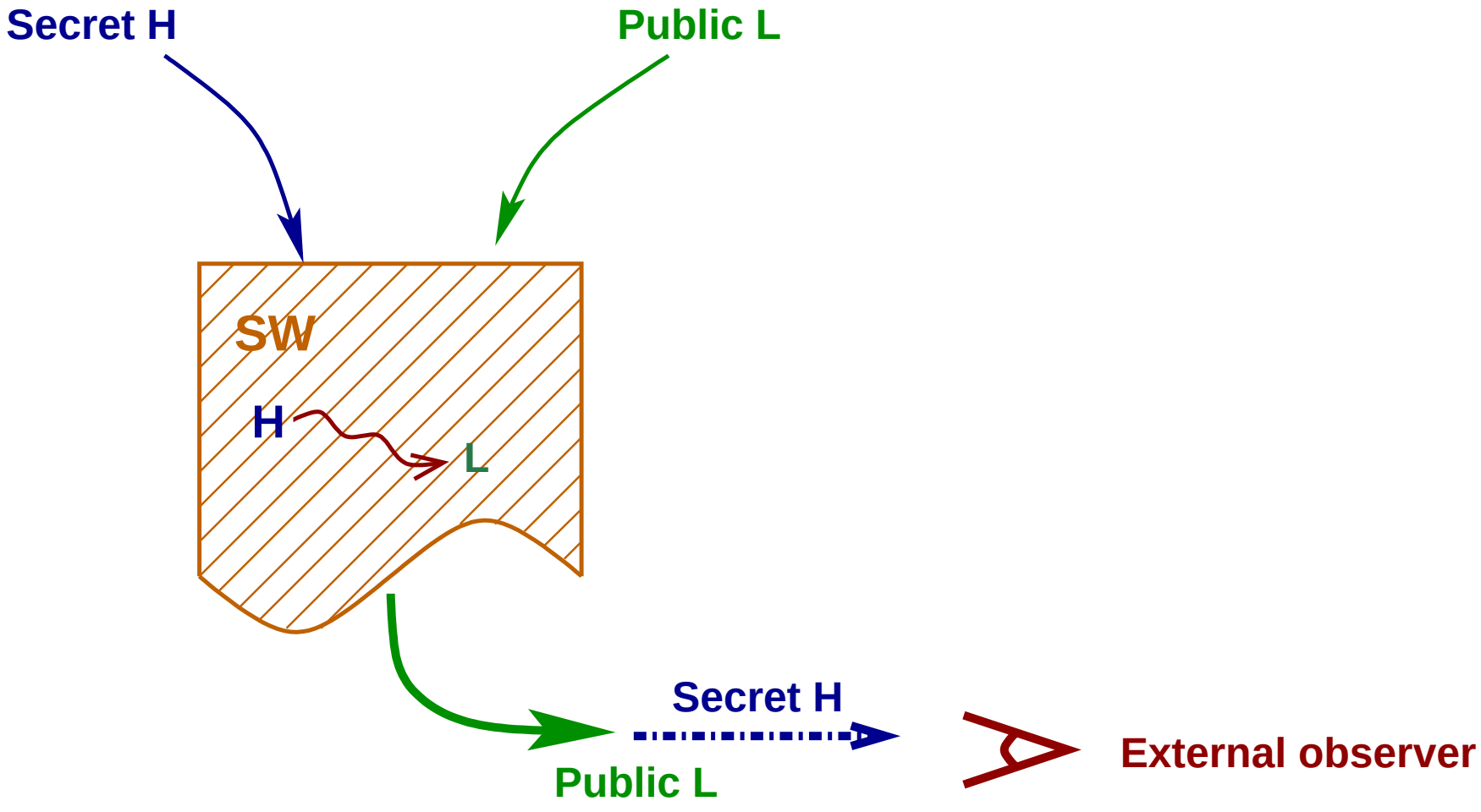
⇓

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].

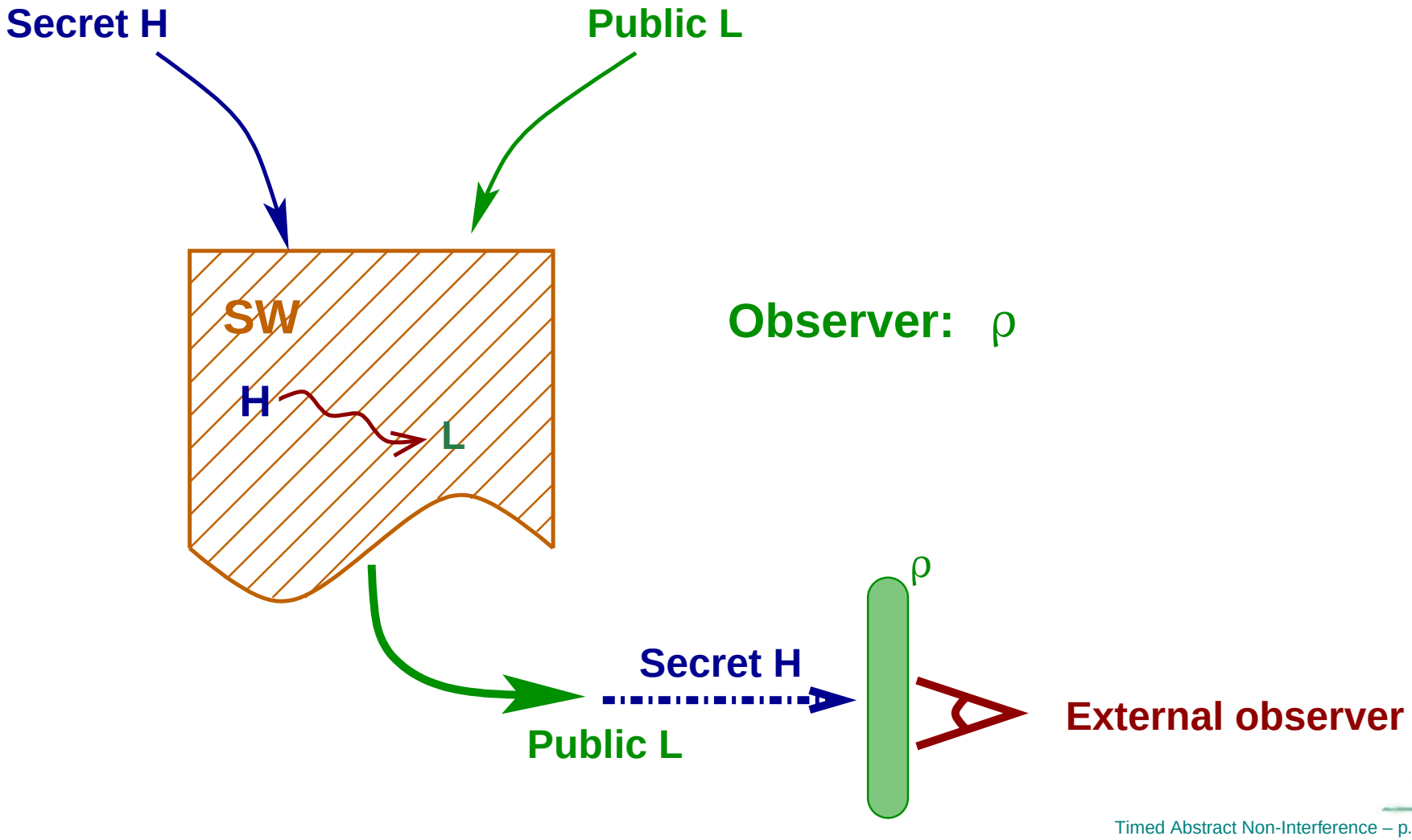
Abstracting Non-Interference

[Giacobazzi & Mastroeni, POPL'04]



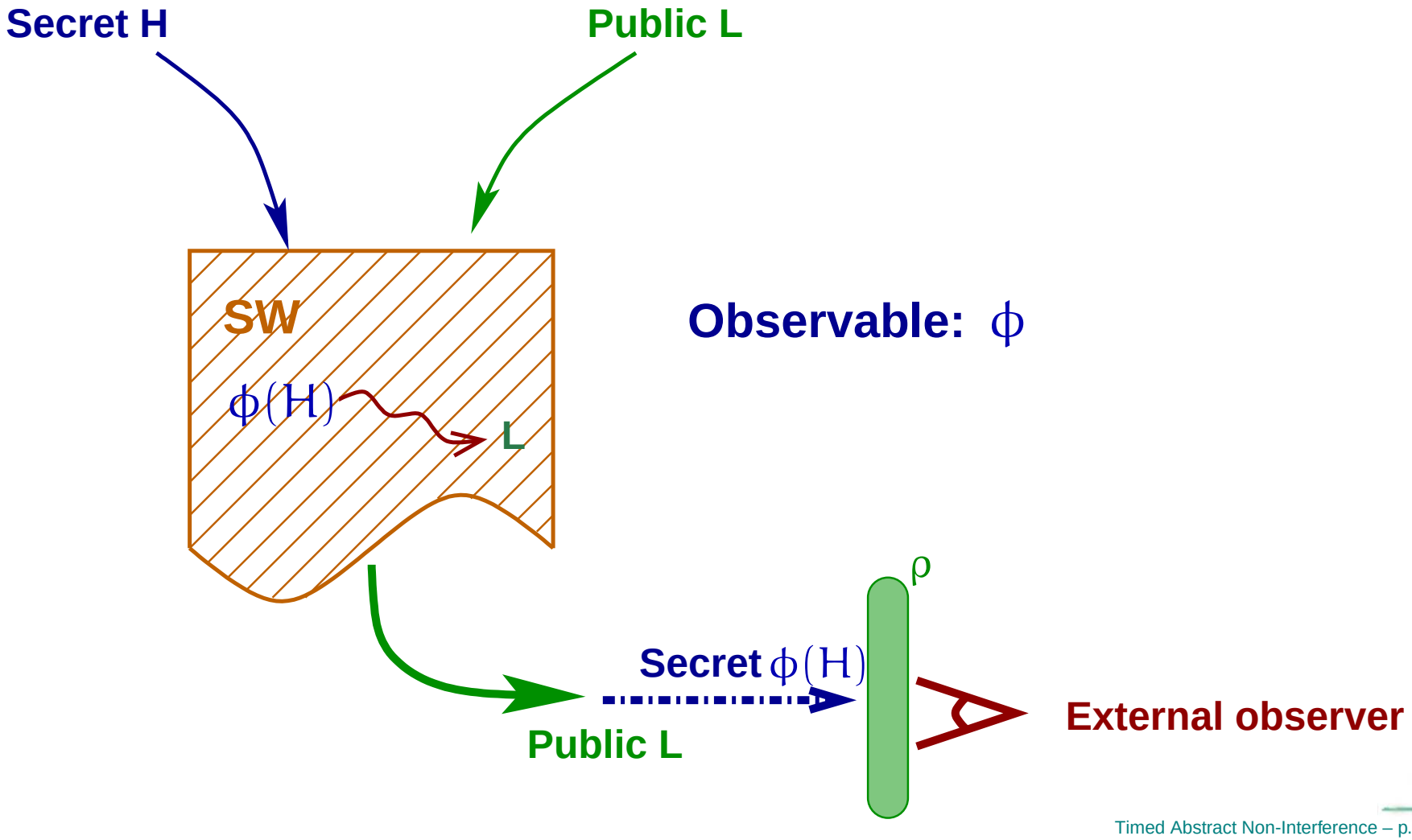
Abstracting Non-Interference

[Giacobazzi & Mastroeni, POPL'04]



Abstracting Non-Interference

[Giacobazzi & Mastroeni, POPL'04]



AI: Lattice of Abstractions

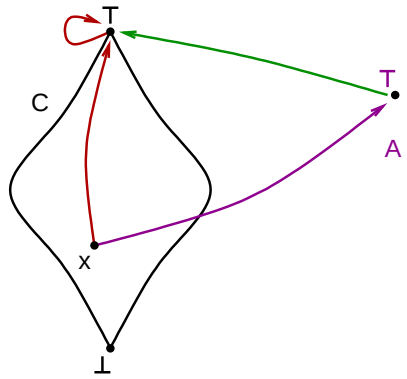
The concrete domain $< C, \leq, \wedge, \vee, \bot, \top >$ [Cousot & Cousot '79]

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

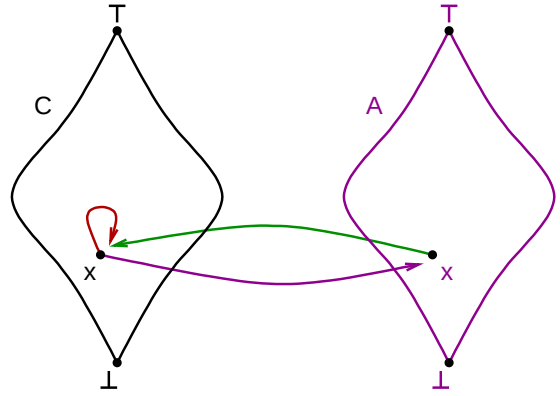
$< Abs(C), \sqsubseteq, \sqcap, \sqcup, \top, C >$

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

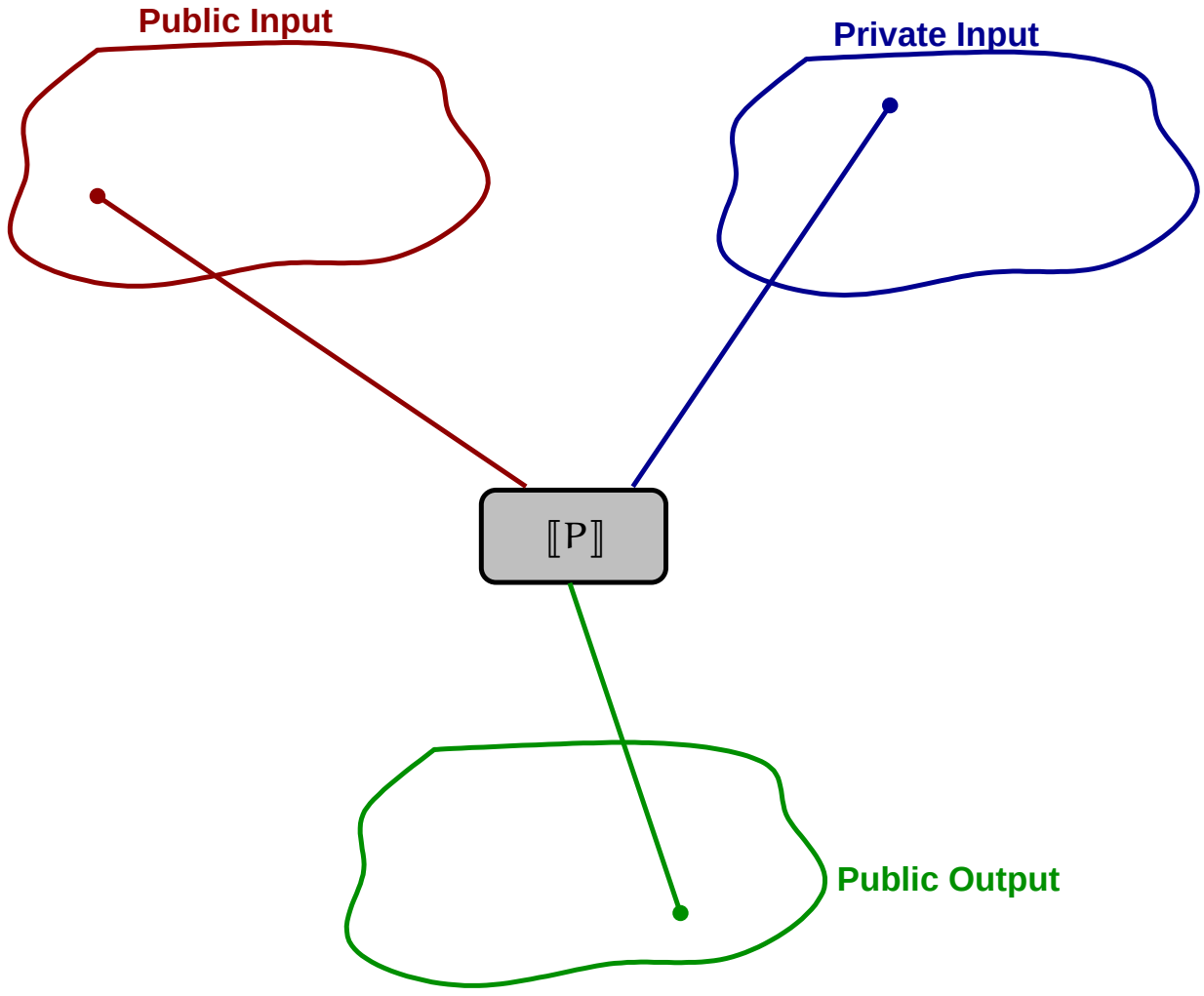
Top:



Bottom:

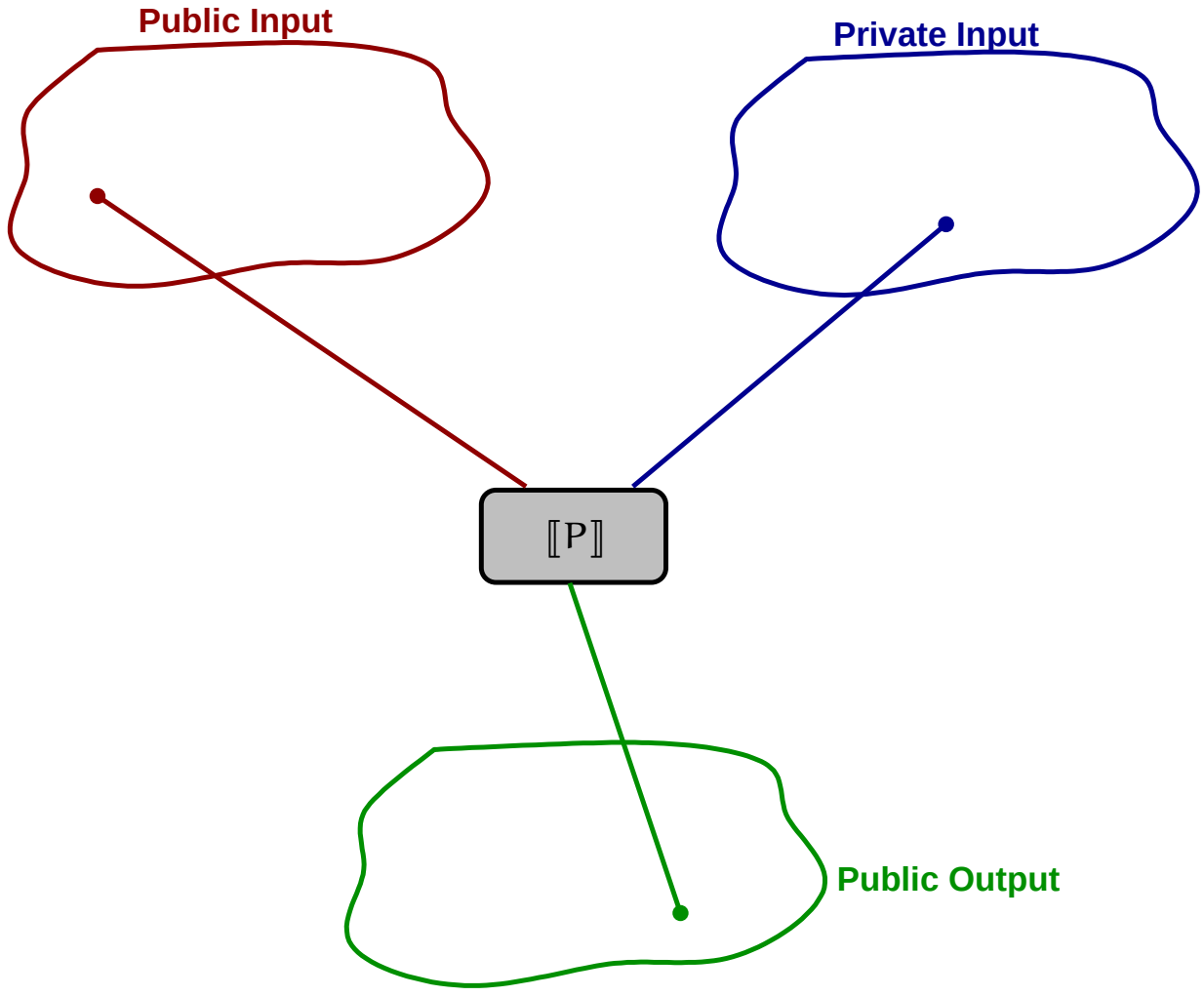


Standard non-interference



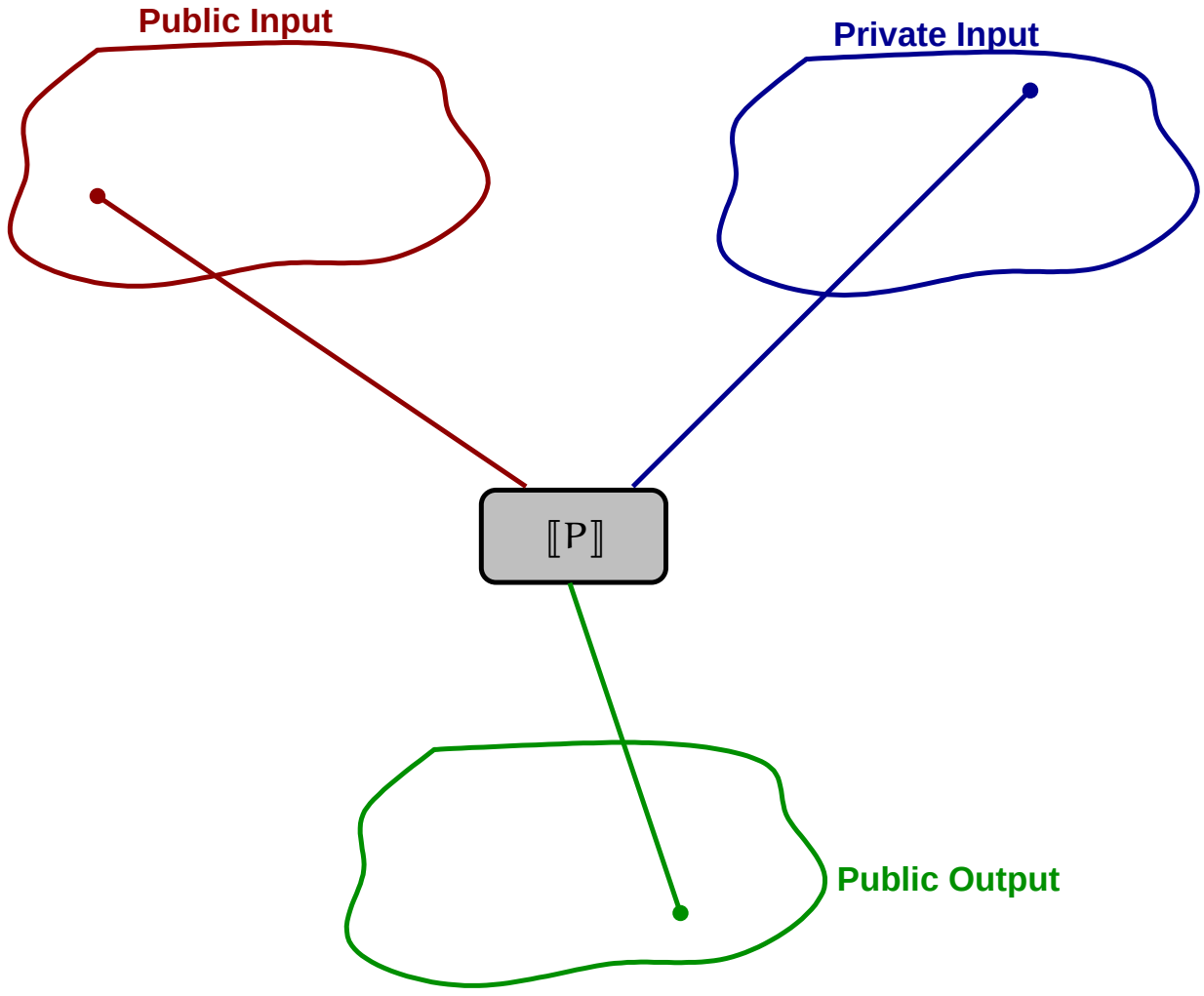
$$\forall l : L, \forall h_1, h_2 : H.\ [\![P]\!](h_1, l)^L = [\![P]\!](h_2, l)^L$$

Standard non-interference



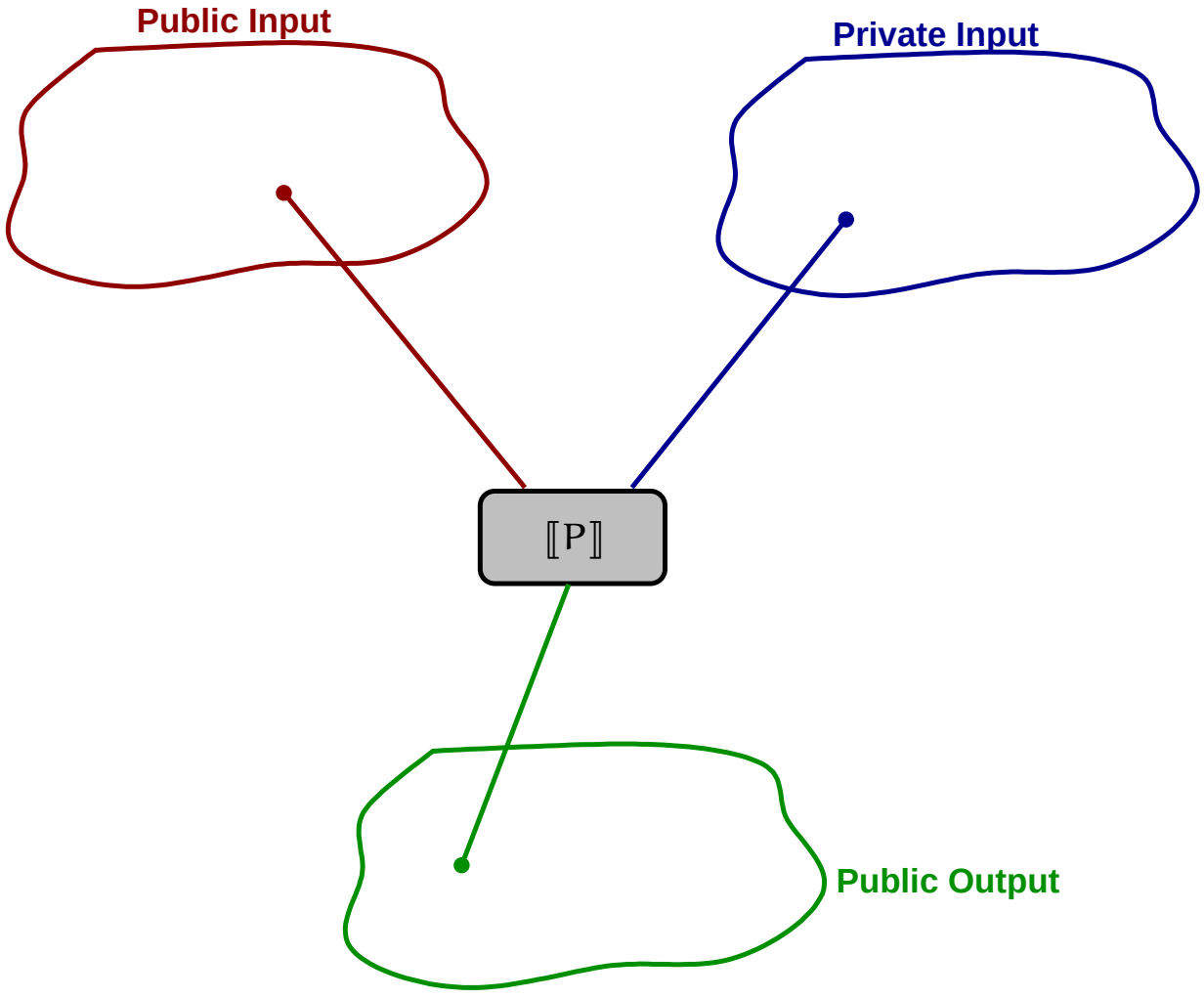
$$\forall l : L, \forall h_1, h_2 : H.\ [\![P]\!](h_1, l)^L = [\![P]\!](h_2, l)^L$$

Standard non-interference



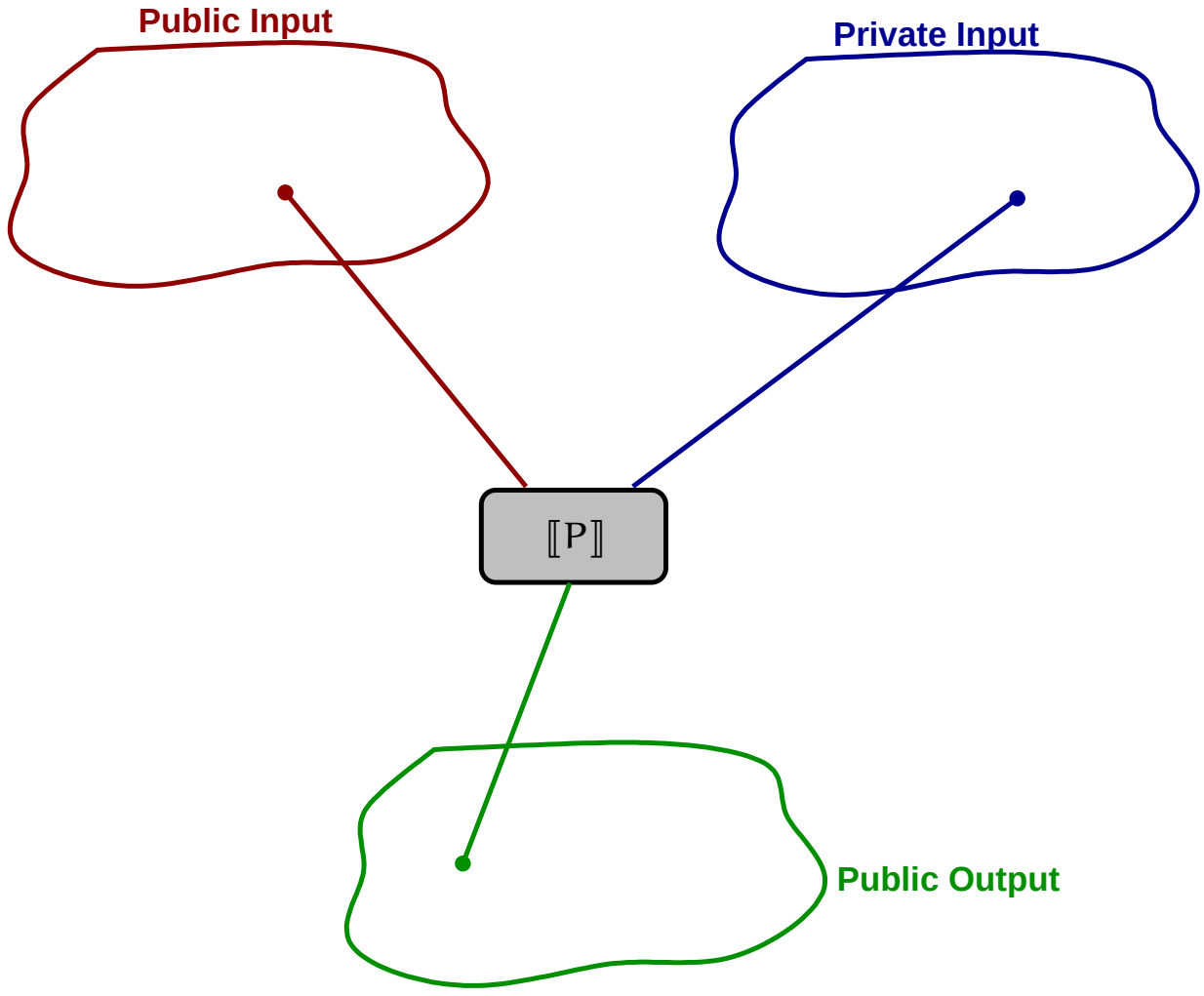
$$\forall l : L, \forall h_1, h_2 : H.\ [\![P]\!](h_1, l)^L = [\![P]\!](h_2, l)^L$$

Standard non-interference



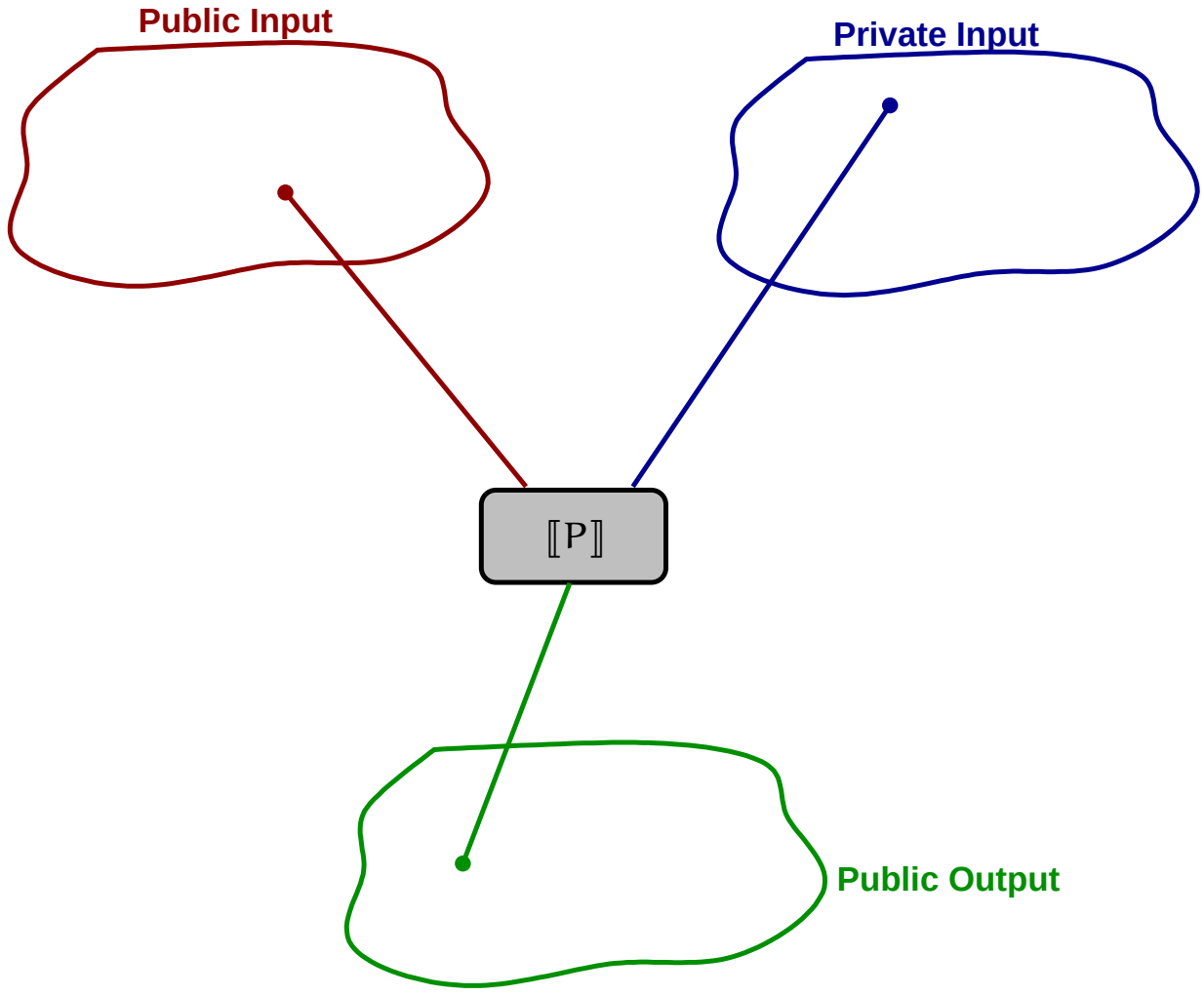
$$\forall l : L, \forall h_1, h_2 : H.\ [\![P]\!](h_1, l)^L = [\![P]\!](h_2, l)^L$$

Standard non-interference



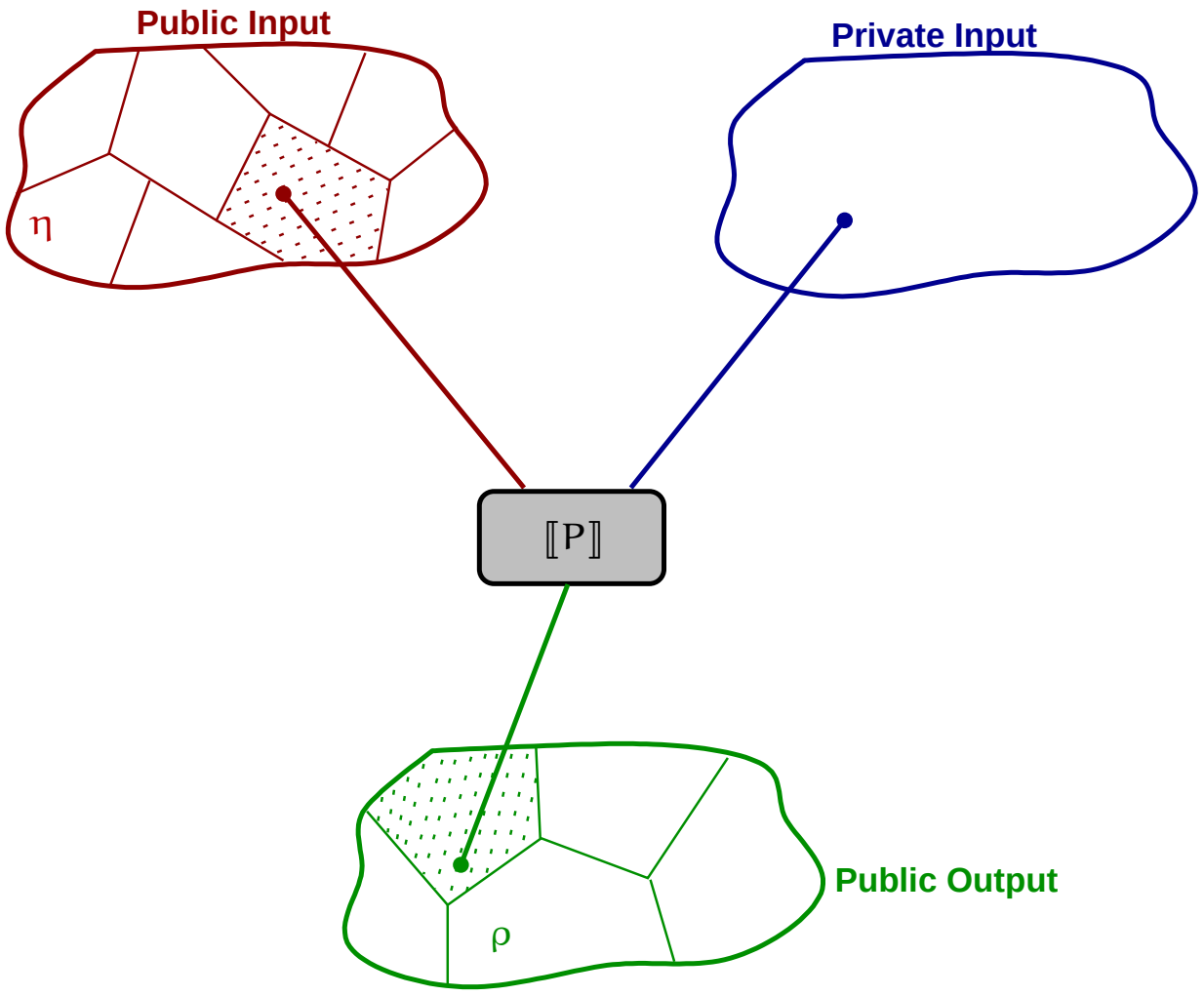
$$\forall l : L, \forall h_1, h_2 : H.\ [\![P]\!](h_1, l)^L = [\![P]\!](h_2, l)^L$$

Standard non-interference



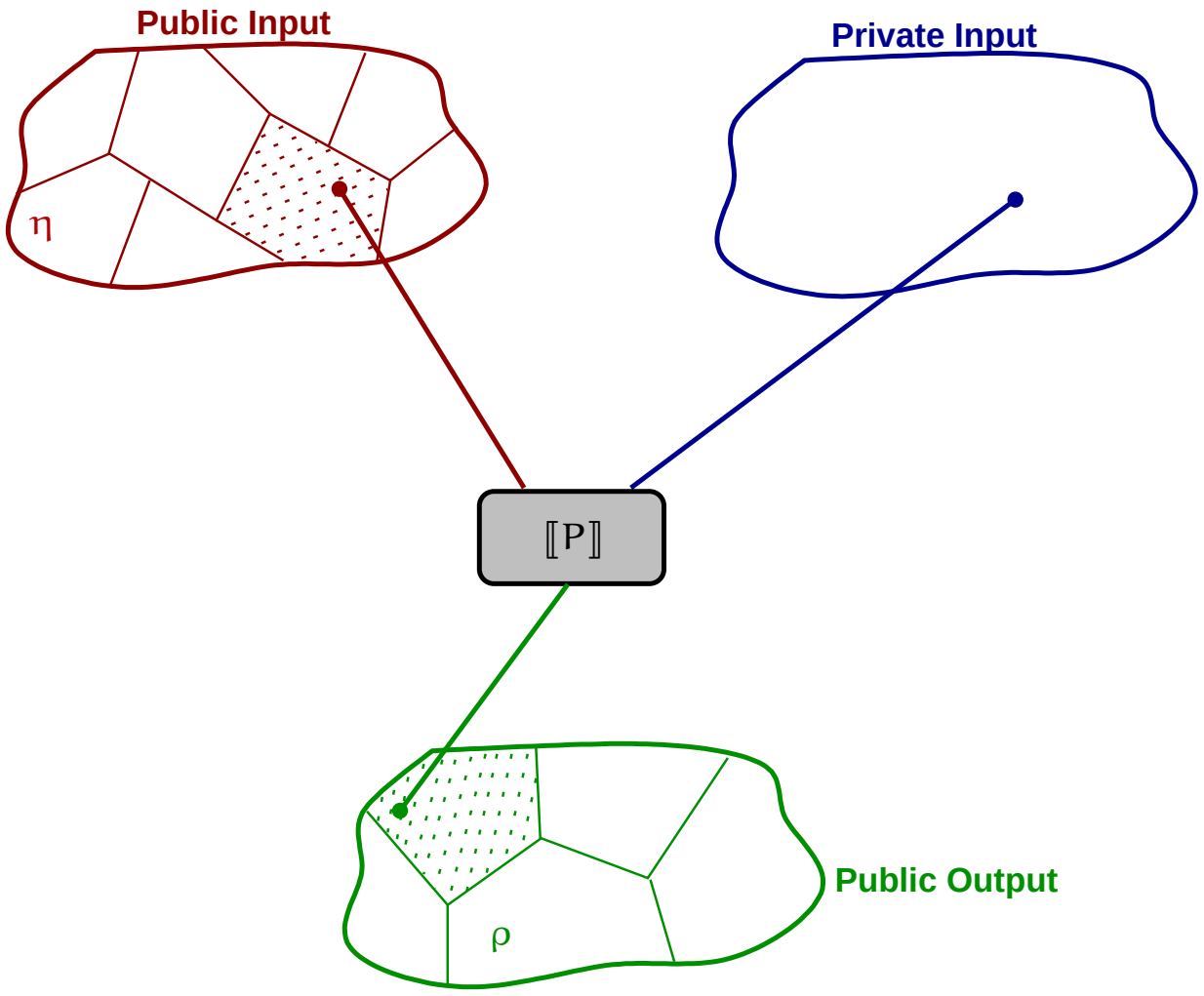
$$\forall l : L, \forall h_1, h_2 : H.\ [\![P]\!](h_1, l)^L = [\![P]\!](h_2, l)^L$$

Abstracting non-interference I: Narrow ANI



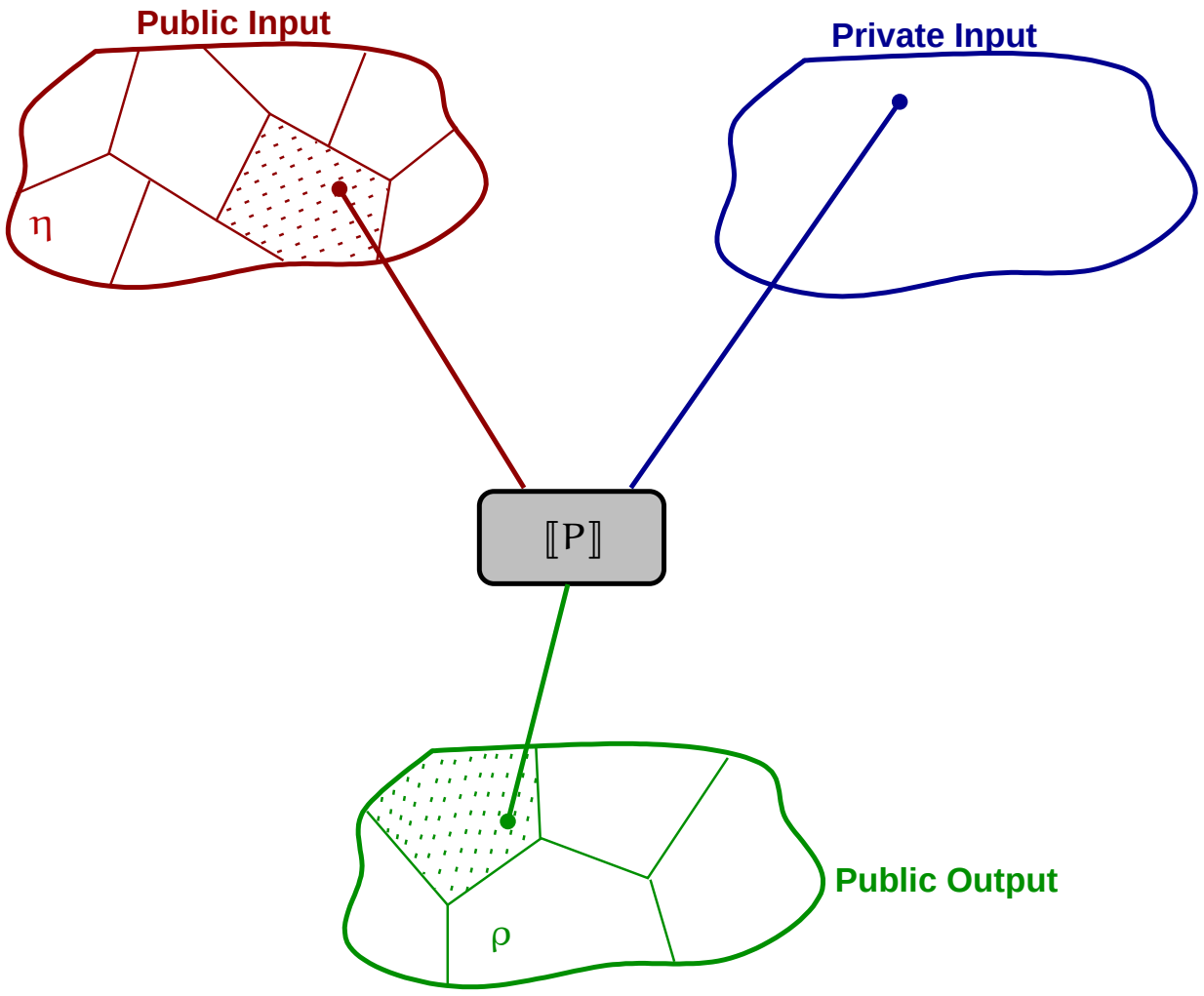
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})) \colon [\eta]\mathrm{P}(\rho) \colon \eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket \mathrm{P} \rrbracket(h_1, l_1)^{\mathsf{L}}) = \rho(\llbracket \mathrm{P} \rrbracket(h_2, l_2)^{\mathsf{L}})$$

Abstracting non-interference I: Narrow ANI



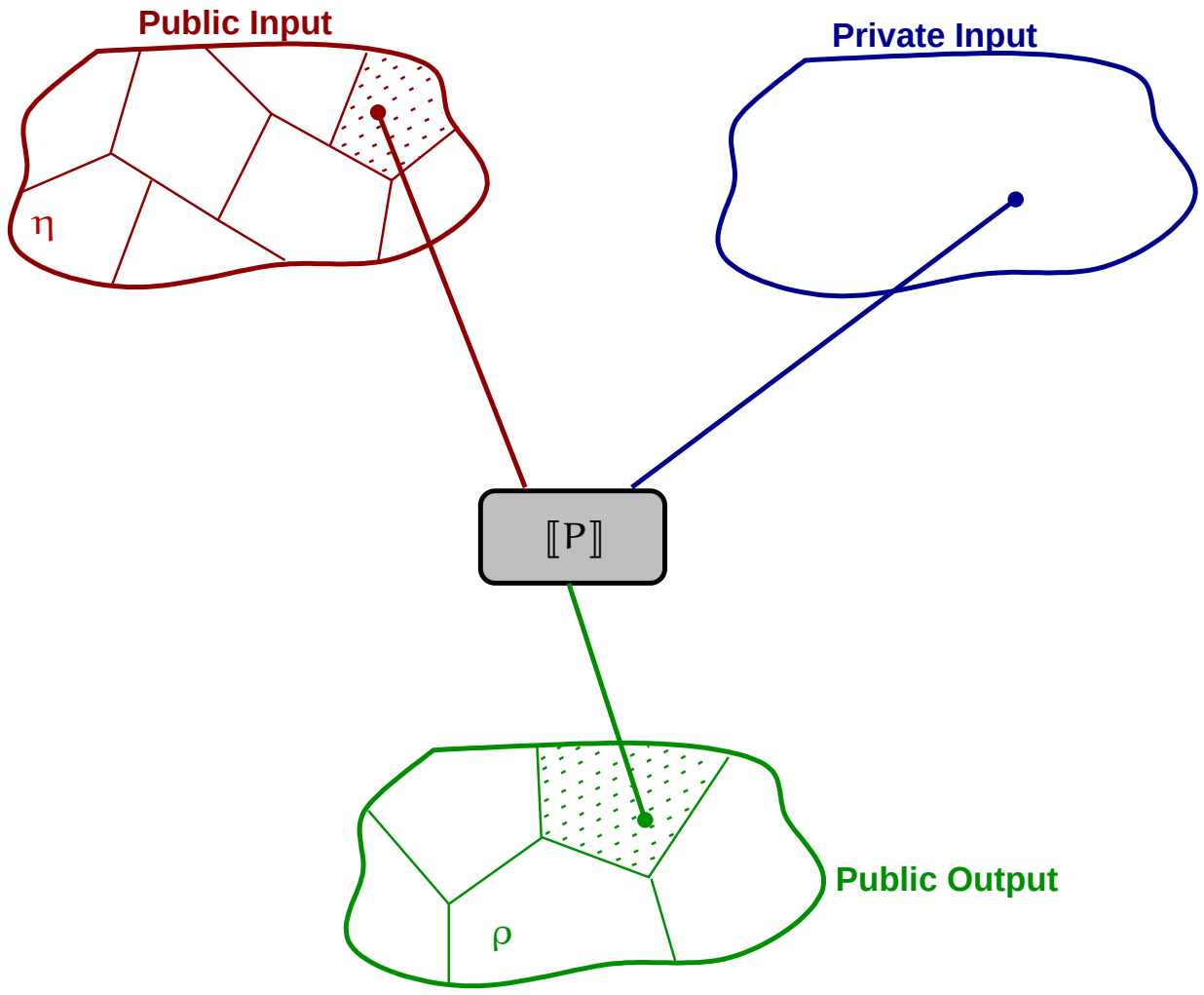
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})) \colon [\eta]\mathrm{P}(\rho) \colon \eta(l_1) = \eta(l_2) \Rightarrow \rho([\![\mathrm{P}]\!](h_1, l_1)^{\mathsf{L}}) = \rho([\![\mathrm{P}]\!](h_2, l_2)^{\mathsf{L}})$$

Abstracting non-interference I: Narrow ANI



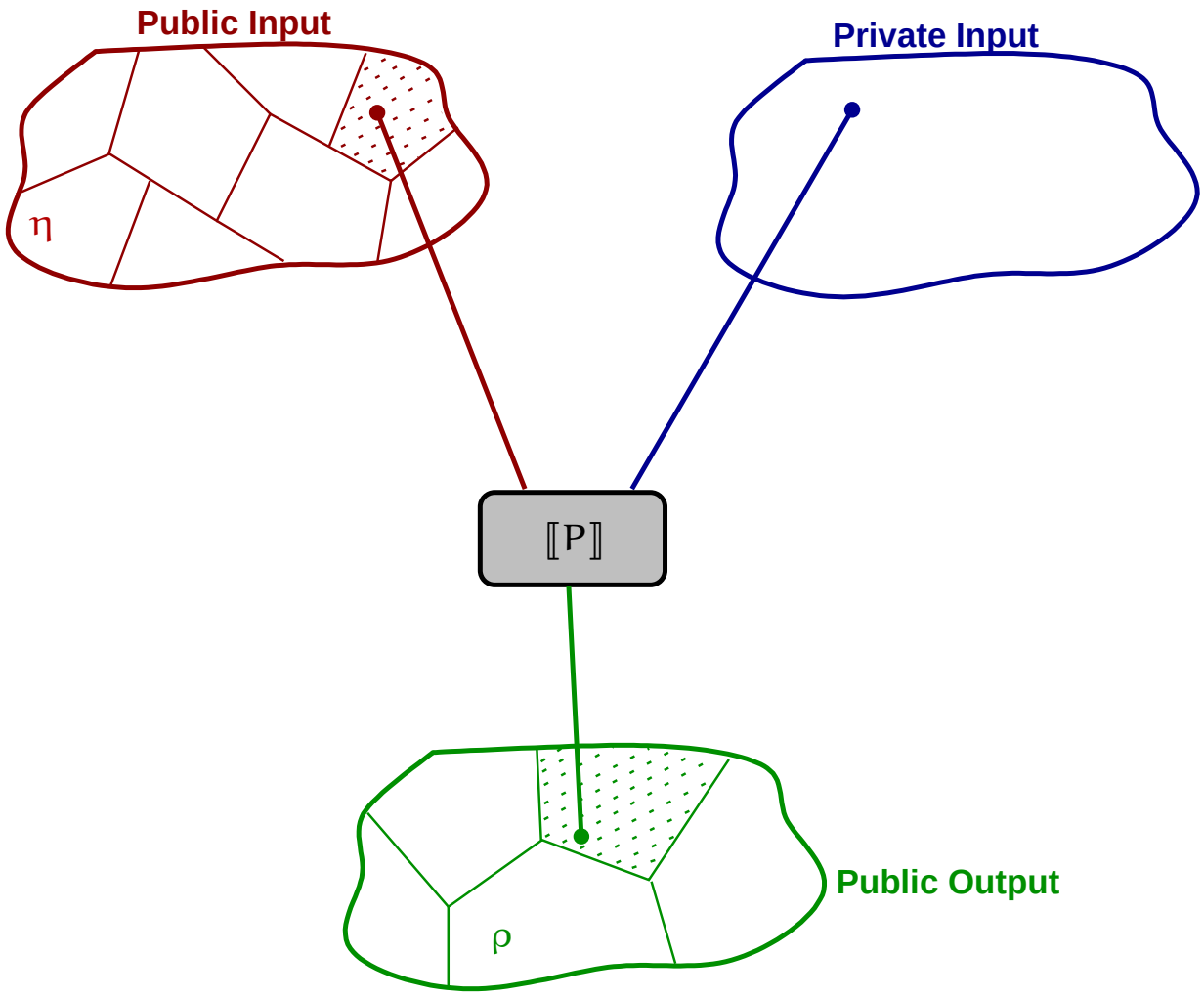
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})) \colon [\eta]\mathrm{P}(\rho) \colon \eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket \mathrm{P} \rrbracket(h_1, l_1)^{\mathsf{L}}) = \rho(\llbracket \mathrm{P} \rrbracket(h_2, l_2)^{\mathsf{L}})$$

Abstracting non-interference I: Narrow ANI



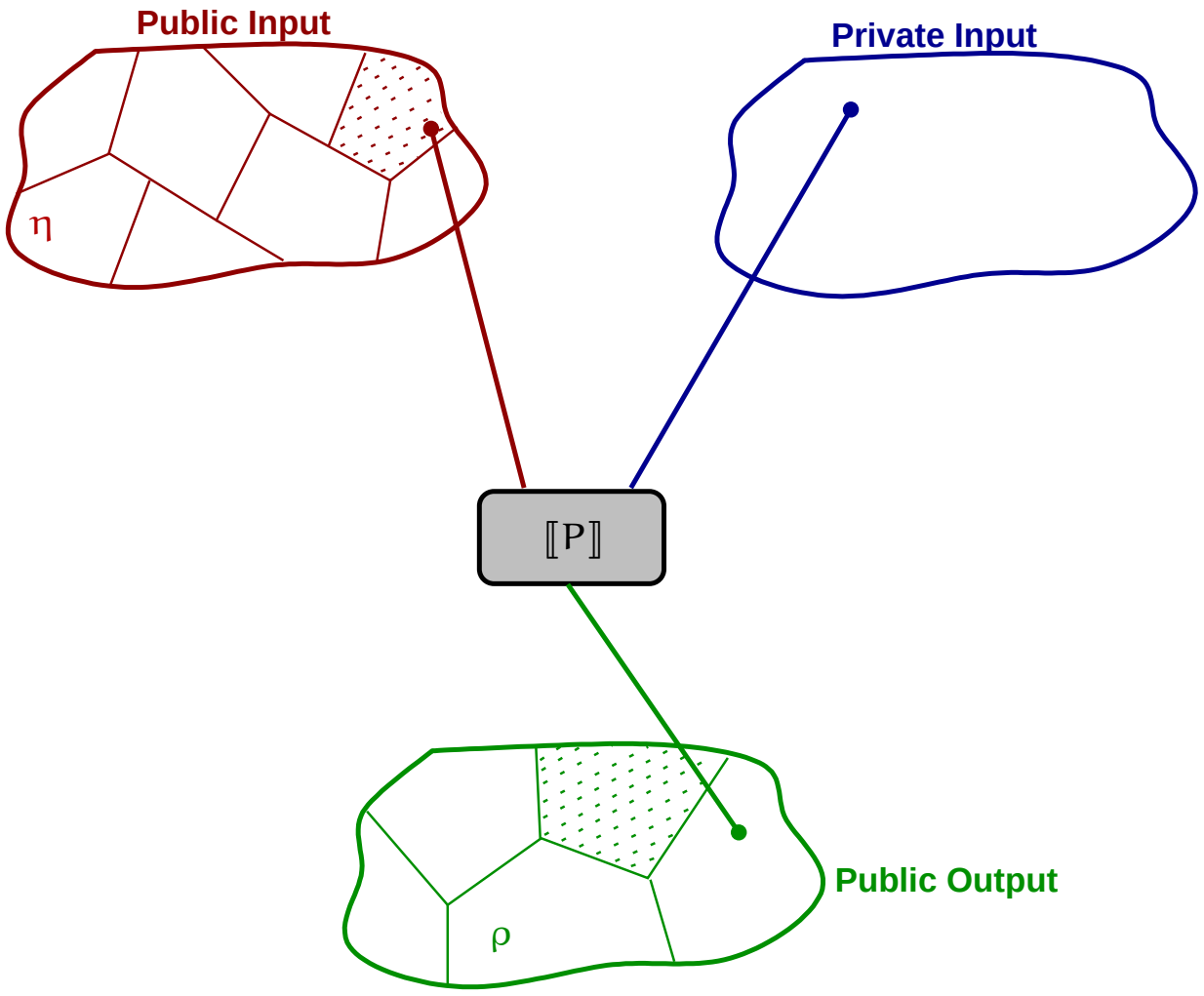
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})) \colon [\eta]\mathrm{P}(\rho) \colon \eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket \mathrm{P} \rrbracket(h_1, l_1)^{\mathsf{L}}) = \rho(\llbracket \mathrm{P} \rrbracket(h_2, l_2)^{\mathsf{L}})$$

Abstracting non-interference I: Narrow ANI



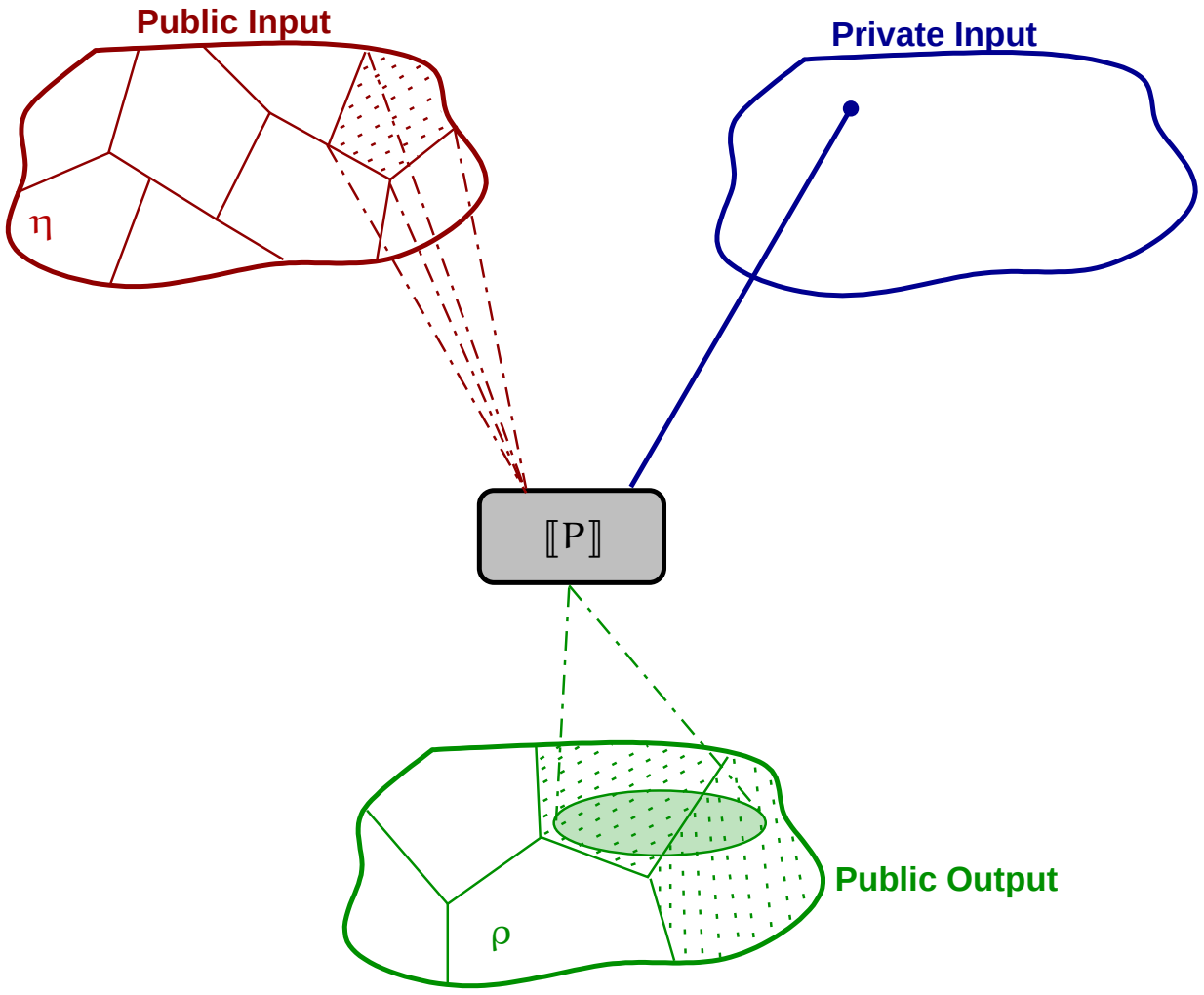
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})) \colon [\eta]\mathrm{P}(\rho) \colon \eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket \mathrm{P} \rrbracket(h_1, l_1)^{\mathsf{L}}) = \rho(\llbracket \mathrm{P} \rrbracket(h_2, l_2)^{\mathsf{L}})$$

Abstracting non-interference I: Narrow ANI



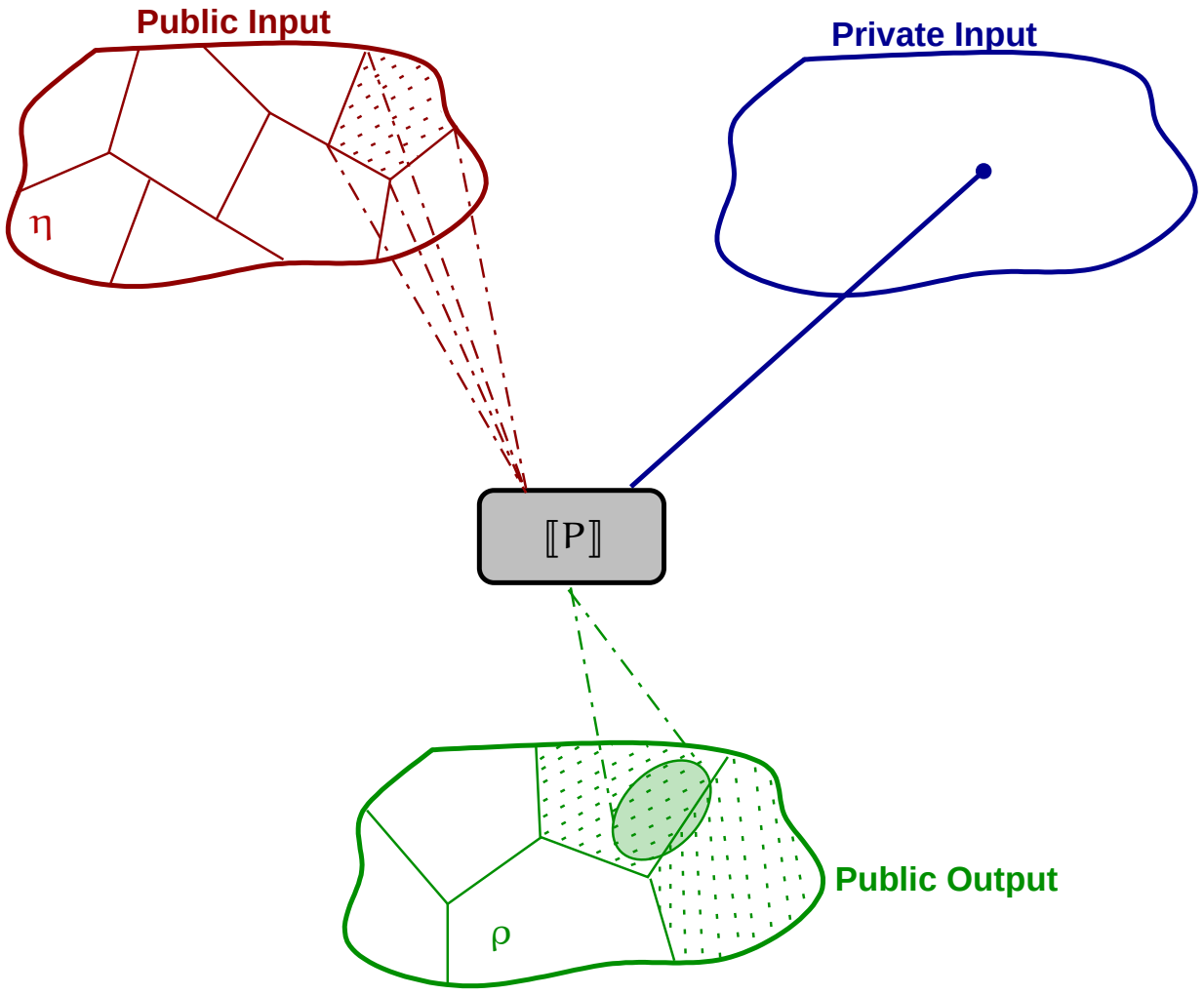
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})) \colon [\eta]\mathrm{P}(\rho) \colon \eta(l_1) = \eta(l_2) \Rightarrow \rho([\![\mathrm{P}]\!](h_1, l_1)^{\mathsf{L}}) = \rho([\![\mathrm{P}]\!](h_2, l_2)^{\mathsf{L}})$$

Abstracting non-interference II



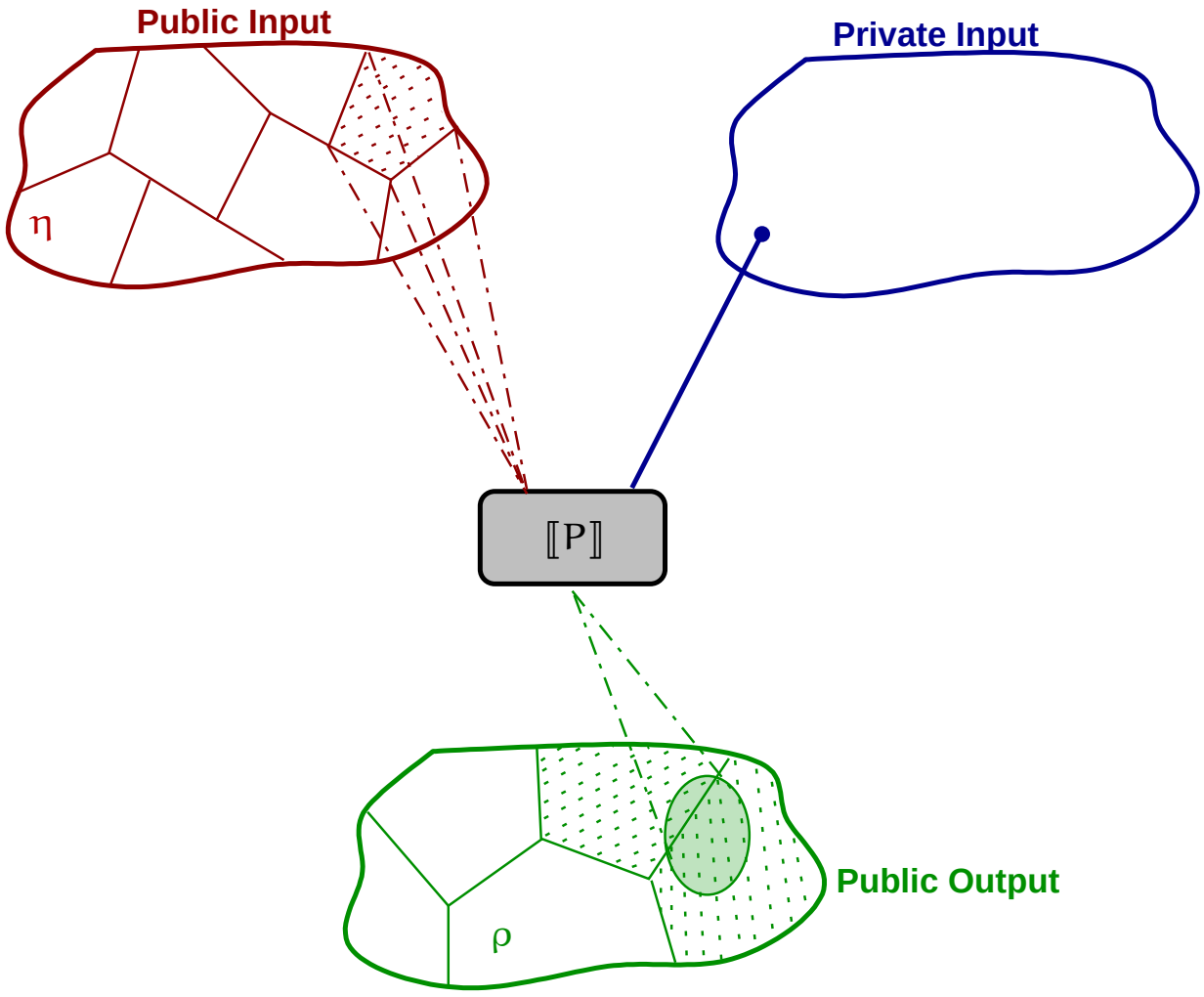
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})) \colon (\eta)\mathrm{P}(\rho) \colon$$
$$\eta(l_1) = \eta(l_2) \Rightarrow \rho([\![\mathrm{P}]\!](h_1, \eta(l_1))^{\mathsf{L}}) = \rho([\![\mathrm{P}]\!](h_2, \eta(l_2))^{\mathsf{L}})$$

Abstracting non-interference II



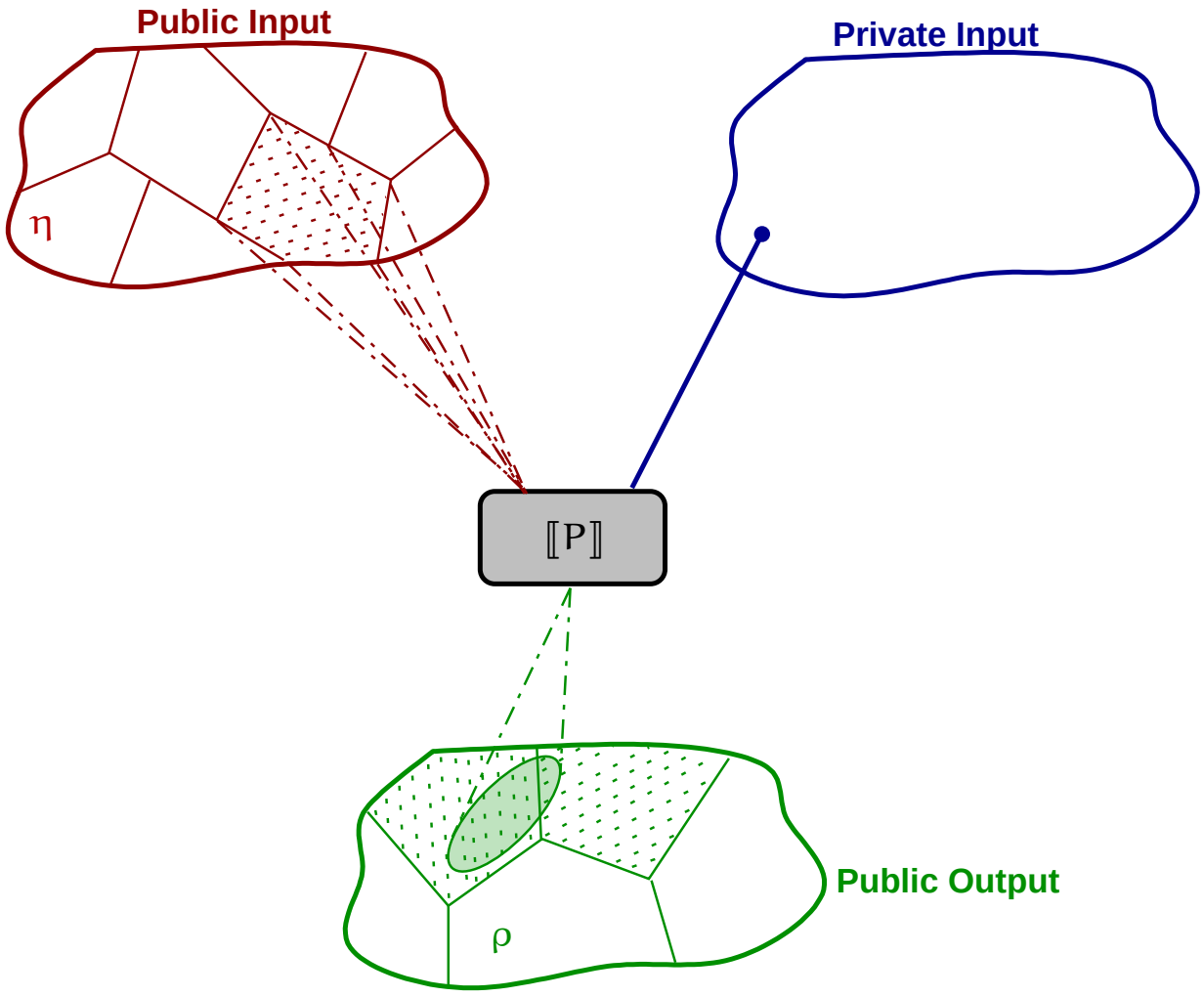
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathsf{L}})) \colon (\eta)\mathrm{P}(\rho) \colon$$
$$\eta(l_1) = \eta(l_2) \Rightarrow \rho([\![\mathrm{P}]\!](h_1, \eta(l_1))^{\mathsf{L}}) = \rho([\![\mathrm{P}]\!](h_2, \eta(l_2))^{\mathsf{L}})$$

Abstracting non-interference II



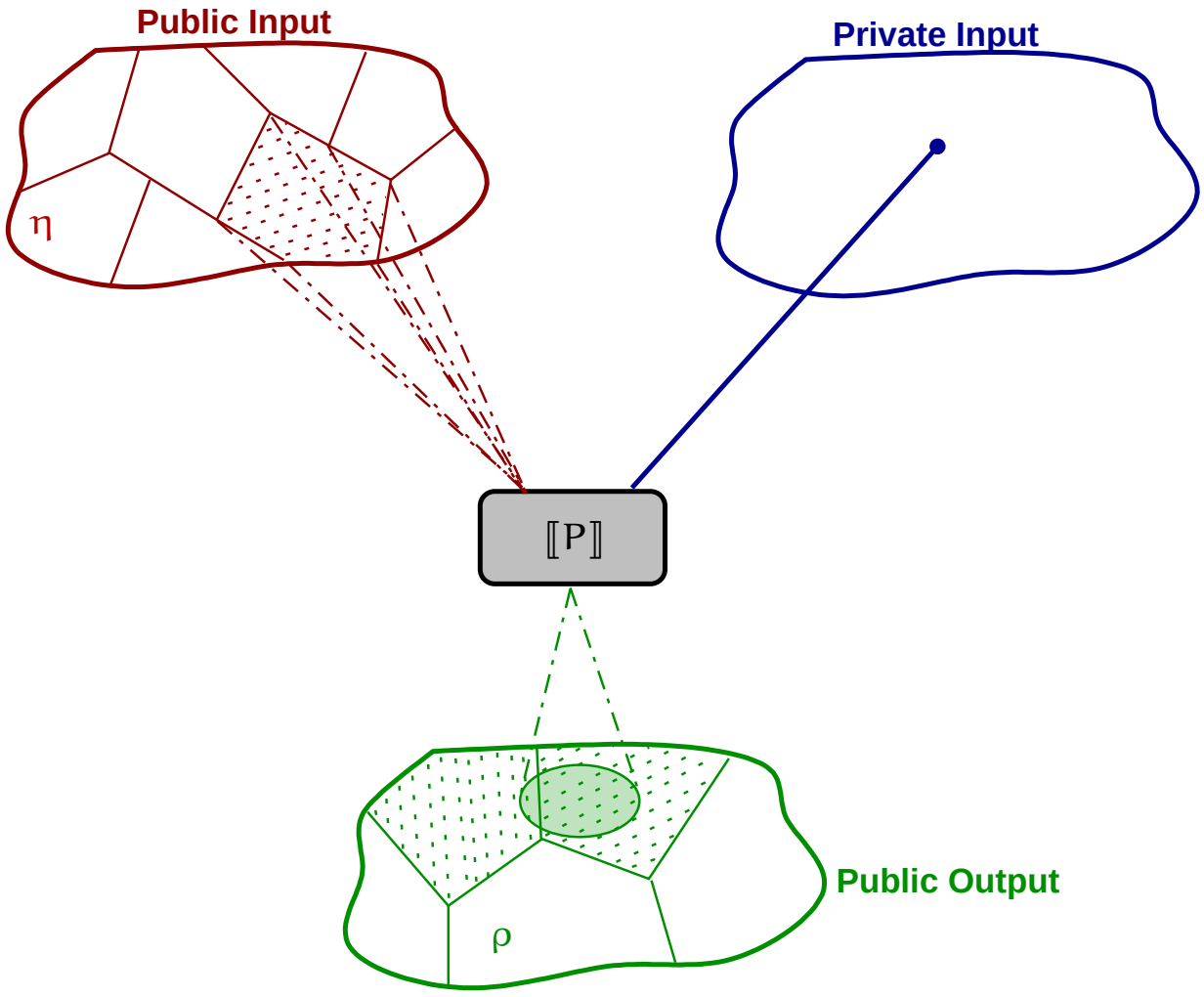
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{L})) \colon (\eta)P(\rho) \colon$$
$$\eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket P \rrbracket(h_1, \eta(l_1))^{L}) = \rho(\llbracket P \rrbracket(h_2, \eta(l_2))^{L})$$

Abstracting non-interference II



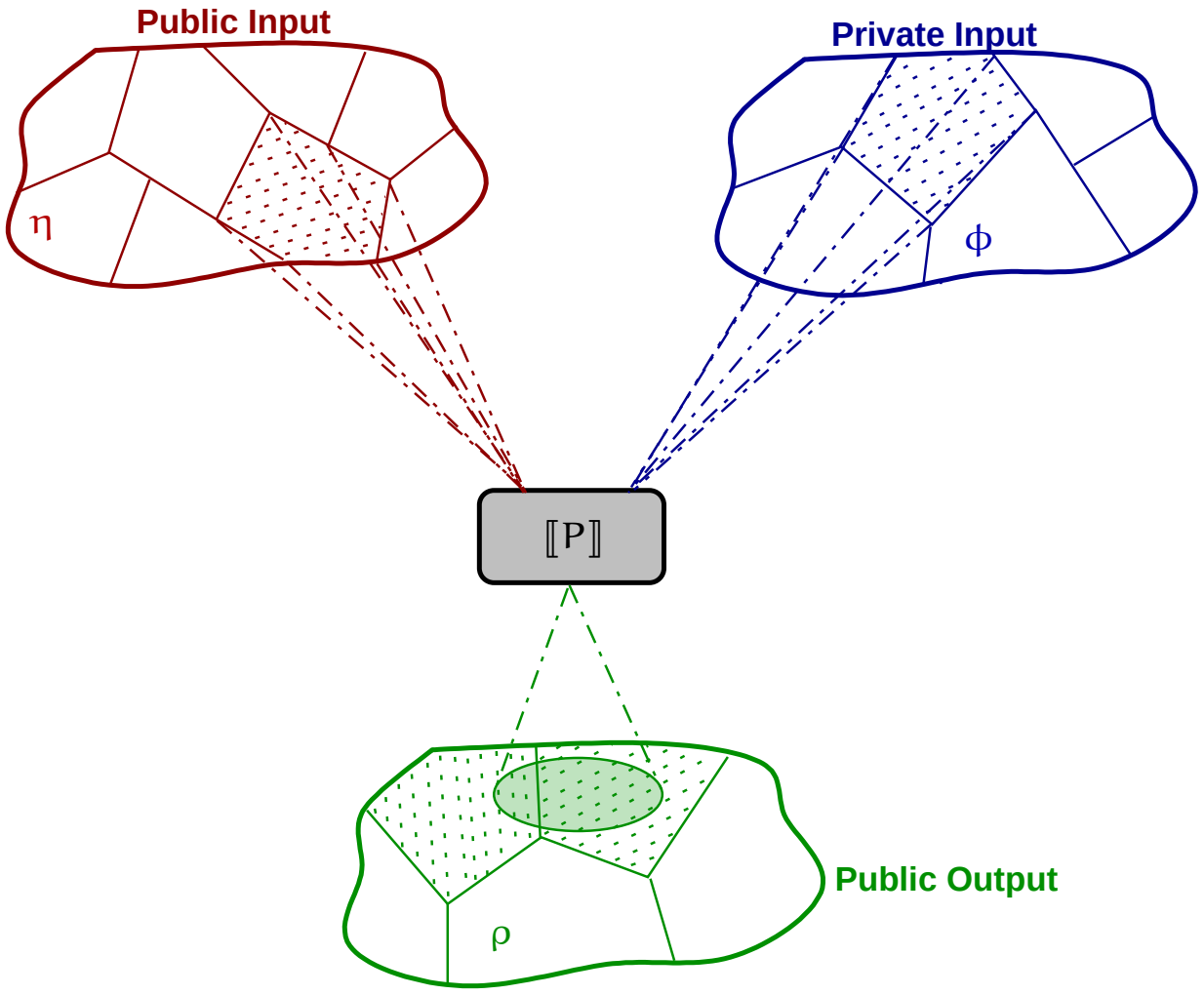
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^L)) \colon (\eta)P(\rho) \colon$$
$$\eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket P \rrbracket(h_1, \eta(l_1))^L) = \rho(\llbracket P \rrbracket(h_2, \eta(l_2))^L)$$

Abstracting non-interference II



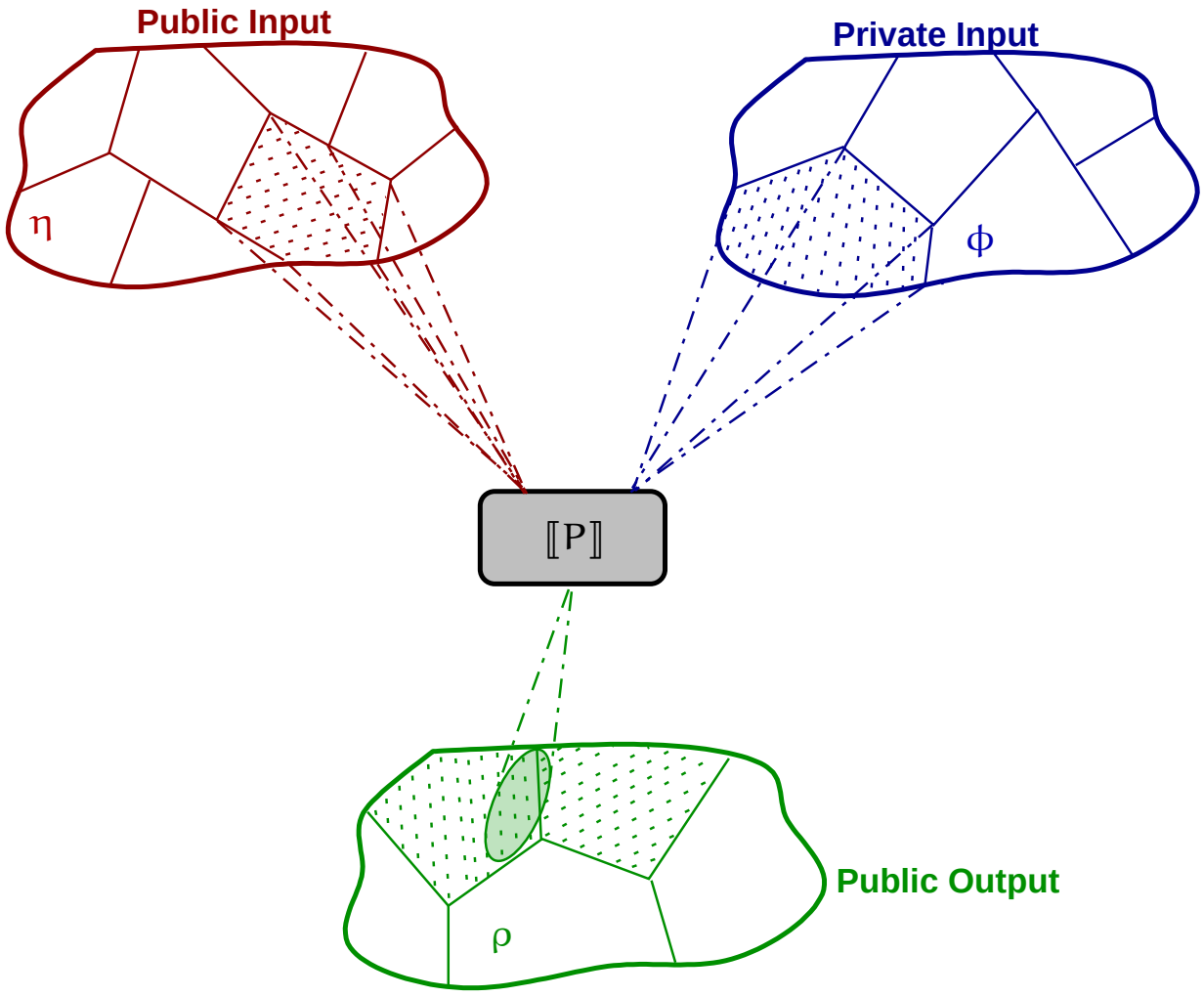
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{L})) \colon (\eta)P(\rho) \colon$$
$$\eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket P \rrbracket(h_1, \eta(l_1))^{L}) = \rho(\llbracket P \rrbracket(h_2, \eta(l_2))^{L})$$

Abstracting non-interference III: ANI



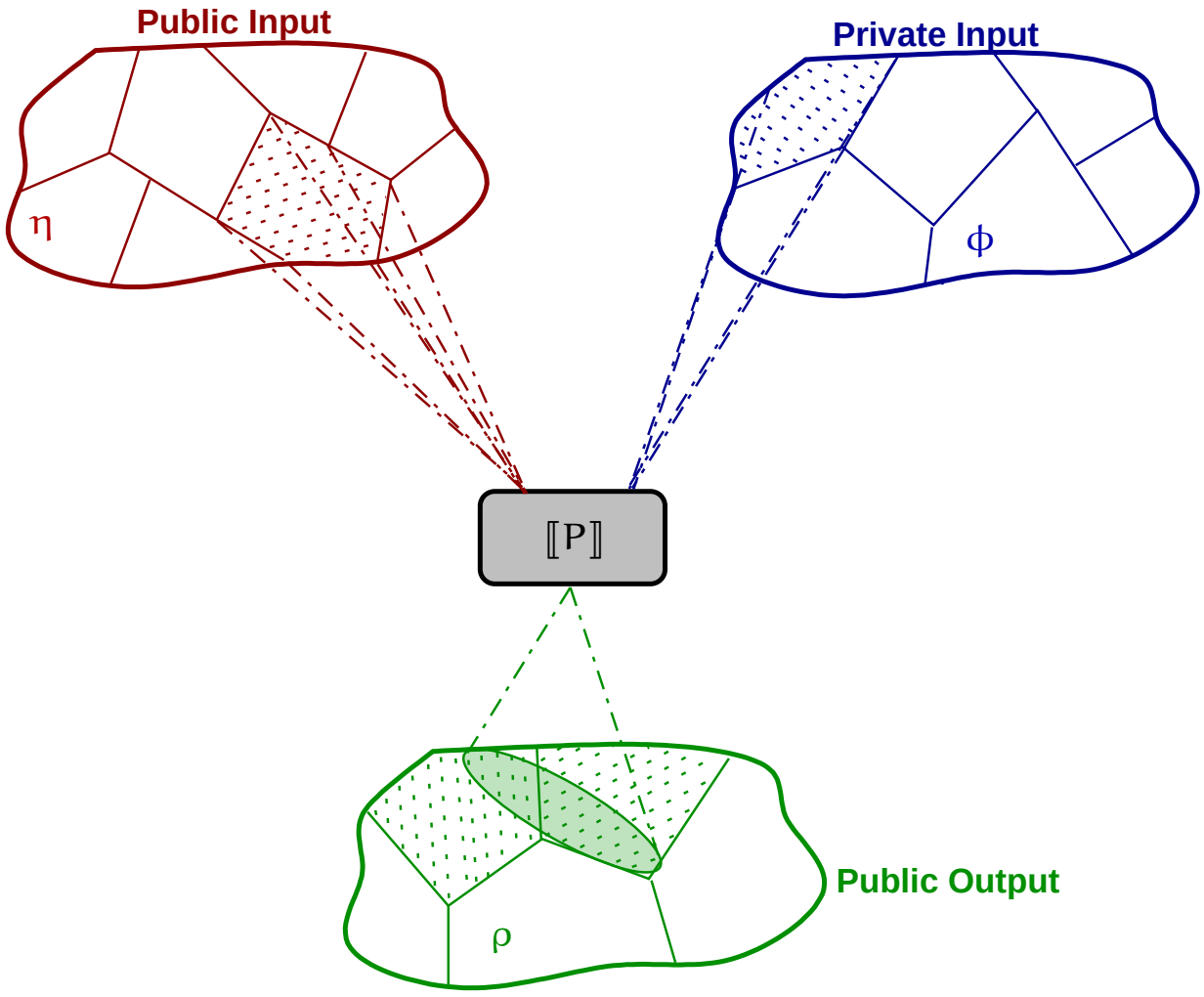
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{L})), \phi \in \mathit{Abs}(\wp(\mathbb{V}^{H})) \colon (\eta) P (\phi \rightsquigarrow \rho) \colon$$
$$\eta(l_1) = \eta(l_2) \Rightarrow \rho([\![P]\!](\phi(h_1), \eta(l_1))^{L}) = \rho([\![P]\!](\phi(h_2), \eta(l_2))^{L})$$

Abstracting non-interference III: ANI



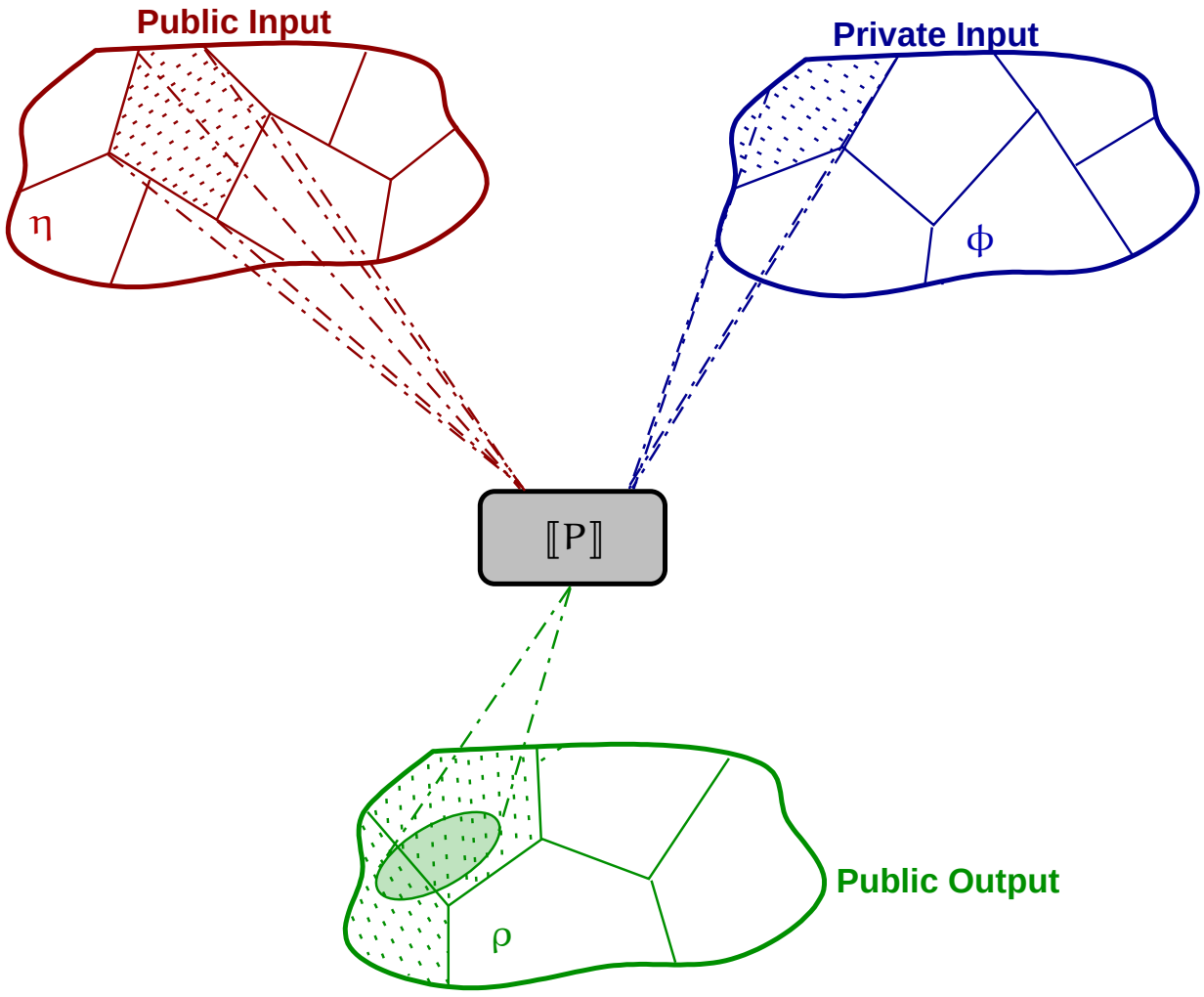
$$\rho,\eta \in \mathit{Abs}(\wp(\mathbb{V}^{L})),\phi \in \mathit{Abs}(\wp(\mathbb{V}^{H})):\ (\eta)P(\phi \rightsquigarrow\!\!\!\!\downarrow\rho):$$
$$\eta(l_1)=\eta(l_2) \Rightarrow \rho([\![P]\!](\phi(h_1),\eta(l_1))^{L})=\rho([\![P]\!](\phi(h_2),\eta(l_2))^{L})$$

Abstracting non-interference III: ANI



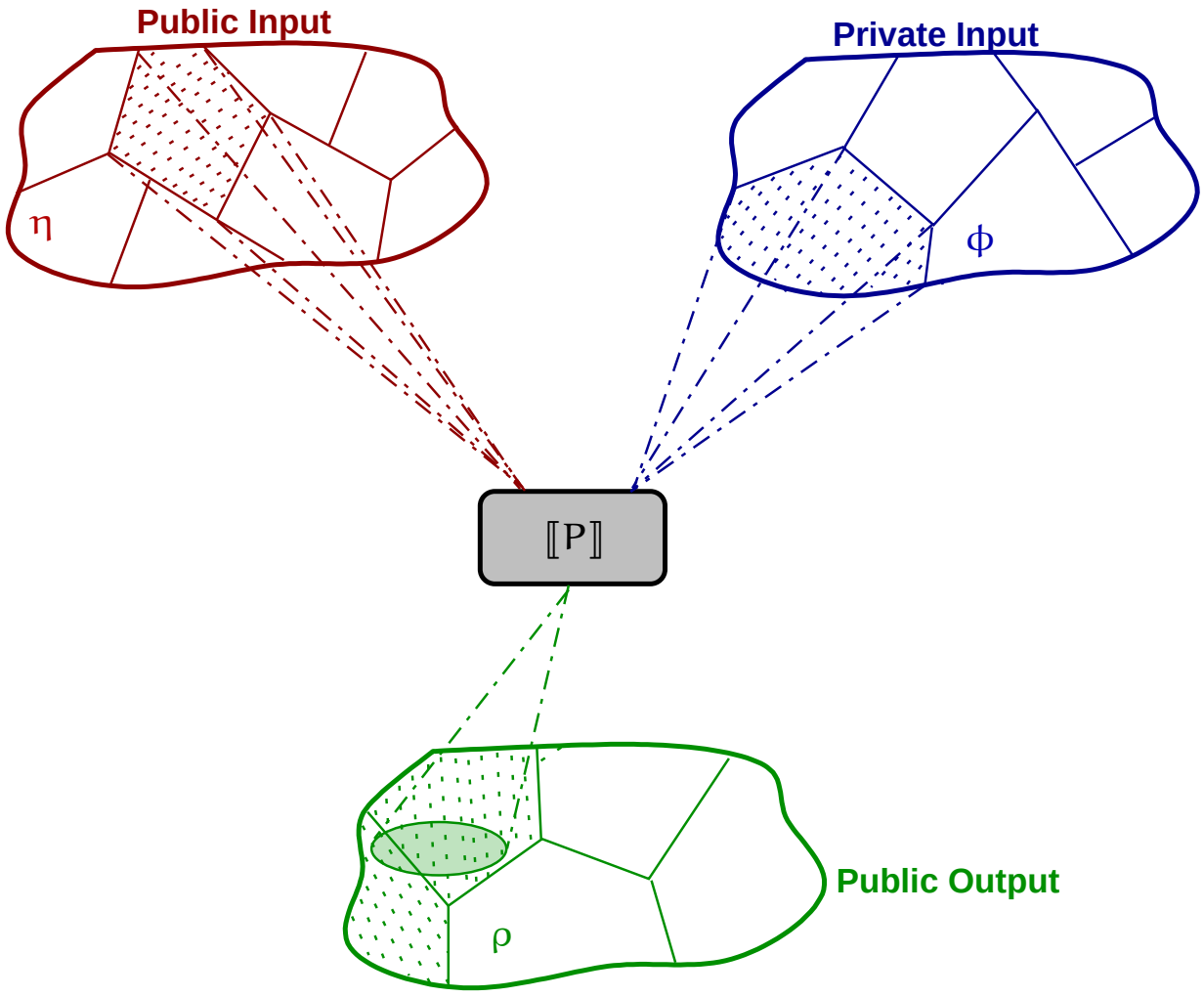
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{L})), \phi \in \mathit{Abs}(\wp(\mathbb{V}^{H})) \colon (\eta) P (\phi \rightsquigarrow \rho) \colon$$
$$\eta(l_1) = \eta(l_2) \Rightarrow \rho([\![P]\!](\phi(h_1), \eta(l_1))^{L}) = \rho([\![P]\!](\phi(h_2), \eta(l_2))^{L})$$

Abstracting non-interference III: ANI



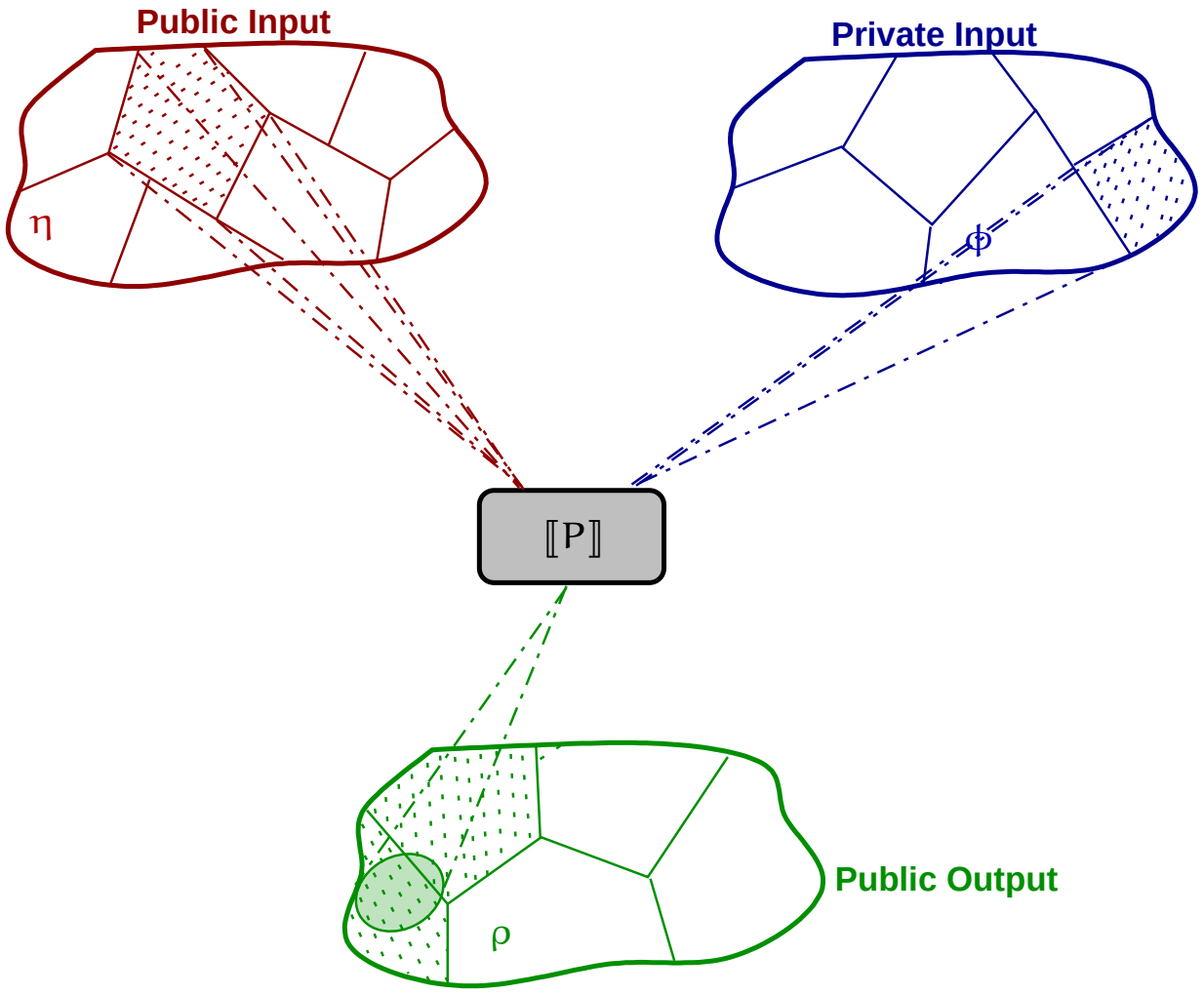
$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{L})), \phi \in \mathit{Abs}(\wp(\mathbb{V}^{H})) \colon (\eta) P (\phi \rightsquigarrow \rho) \colon$$
$$\eta(l_1) = \eta(l_2) \Rightarrow \rho([\![P]\!](\phi(h_1), \eta(l_1))^{L}) = \rho([\![P]\!](\phi(h_2), \eta(l_2))^{L})$$

Abstracting non-interference III: ANI



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

Abstracting non-interference III: ANI



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

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

  [The most powerful *public observer*]

Deriving output attackers

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

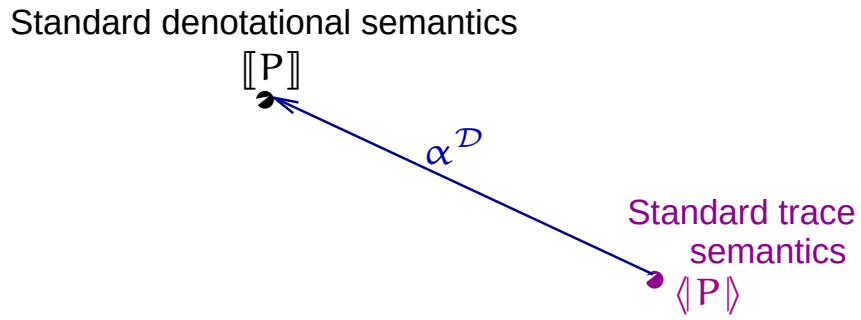
Designing abstractions = designing attackers

- 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.

Timed abstract non-interference...



Trace semantics

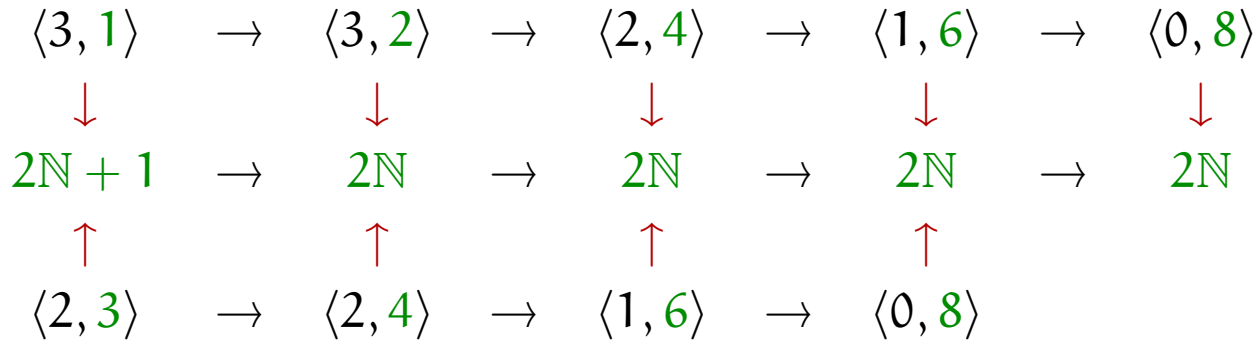
Traces' length = TIME ELAPSED

On traces

$l := l + 1;$

while $h \neq 0$ **do**

$h := h - 1;\ l := l + 2;$



On traces

$$
\begin{array}{ccccccccc}
\langle 3,1\rangle & \rightarrow & \langle 3,2\rangle & \rightarrow & \langle 2,4\rangle & \rightarrow & \langle 1,6\rangle & \rightarrow & \langle 0,8\rangle \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
2\mathbb{N}+1 & \rightarrow & 2\mathbb{N} & \rightarrow & 2\mathbb{N} & \rightarrow & 2\mathbb{N} & \rightarrow & 2\mathbb{N} \\
\uparrow & & \uparrow & & \uparrow & & \uparrow & & \\
\langle 2,3\rangle & \rightarrow & \langle 2,4\rangle & \rightarrow & \langle 1,6\rangle & \rightarrow & \langle 0,8\rangle & &
\end{array}
$$

Stuttering removes time from traces!

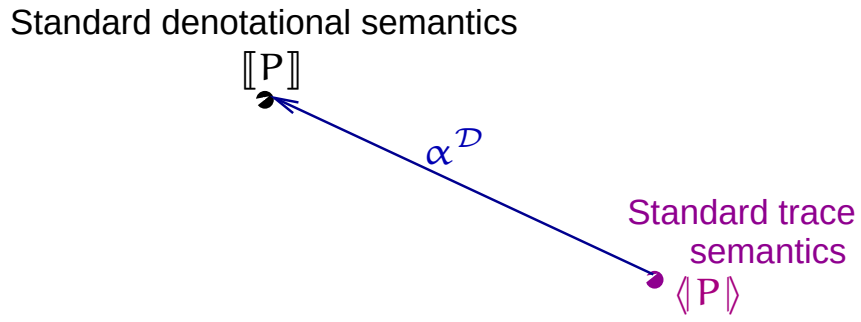
TRACE SEMANTICS

$$
\begin{array}{c}
2\mathbb{Z} \longrightarrow 2\mathbb{Z} \longrightarrow 2\mathbb{Z}+1 \longrightarrow 2\mathbb{Z} \\
\neq \\
2\mathbb{Z} \longrightarrow 2\mathbb{Z}+1 \longrightarrow 2\mathbb{Z}+1 \longrightarrow 2\mathbb{Z}
\end{array}
$$

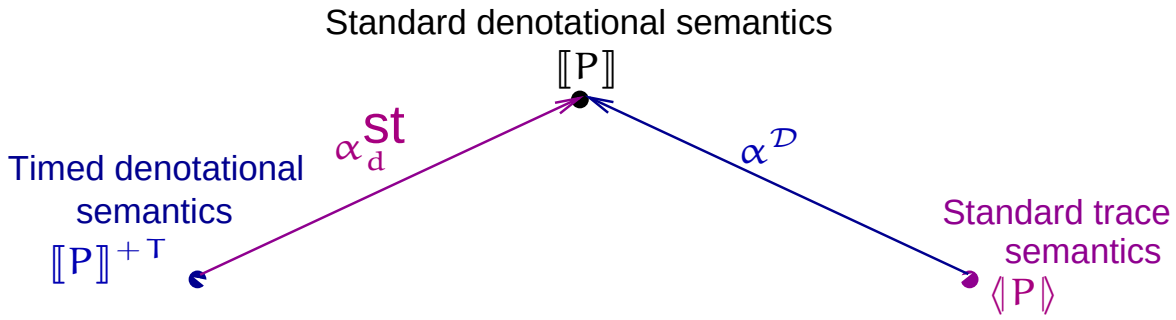
TRACE WITHOUT STUTTERING

$$
\begin{array}{c}
2\mathbb{Z} \longrightarrow 2\mathbb{Z}+1 \longrightarrow 2\mathbb{Z} \\
= \\
2\mathbb{Z} \longrightarrow 2\mathbb{Z}+1 \longrightarrow 2\mathbb{Z}
\end{array}
$$

Timed abstract non-interference...



Timed abstract non-interference...

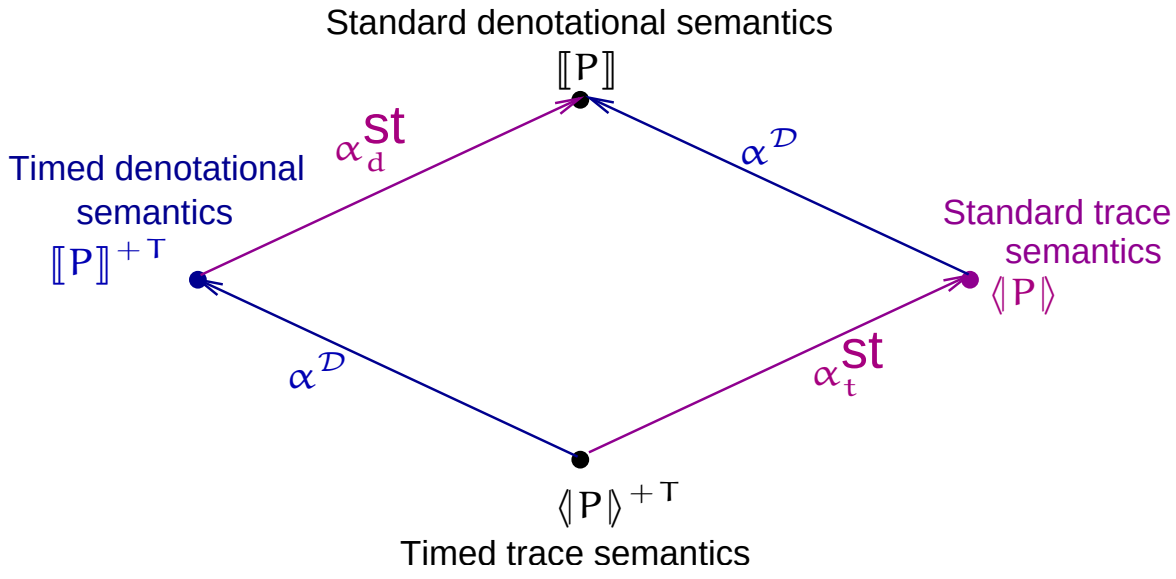


Timed denotational semantics

⇓

Time counter = TIME ELAPSED

Timed abstract non-interference...



Timed denotational semantics

Time counter = TIME ELAPSED

On timed semantics

$t_A = t_T = 1$

$h := h \ mod \ 4;$
while $h \neq 0$ **do**
$h := h - 1;\ l := 2l - l;$

$$\begin{array}{ccccccccc} \langle 7,2,0\rangle & \rightarrow & \langle 3,2,1\rangle & \rightarrow & \langle 2,2,4\rangle & \rightarrow & \langle 1,2,7\rangle & \rightarrow & \langle 0,2,10\rangle \\ \langle 10,2,0\rangle & \rightarrow & \langle 2,2,1\rangle & \rightarrow & \langle 1,2,4\rangle & \rightarrow & \langle 0,2,7\rangle & & \end{array}$$

In general $[\![P]\!](\langle h,l,0\rangle) = \langle 0,l,3h+1\rangle$.

On timed semantics

$t_A = t_T = 1$

$$\begin{array}{lllllllll} \langle 7,2,0\rangle & \to & \langle 3,2,1\rangle & \to & \langle 2,2,4\rangle & \to & \langle 1,2,7\rangle & \to & \langle 0,2,10\rangle \\ \langle 10,2,0\rangle & \to & \langle 2,2,1\rangle & \to & \langle 1,2,4\rangle & \to & \langle 0,2,7\rangle & & \end{array}$$

In general $[\![P]\!](\langle h,l,0\rangle) = \langle 0,l,3h+1\rangle$.

$\Longrightarrow$ We can derive the maximal harmless observable property of time.

On timed semantics

$t_A = t_T = 1$

$$\begin{array}{ccccccccc} \langle 7,2,0\rangle & \to & \langle 3,2,1\rangle & \to & \langle 2,2,4\rangle & \to & \langle 1,2,7\rangle & \to & \langle 0,2,10\rangle \\ \langle 10,2,0\rangle & \to & \langle 2,2,1\rangle & \to & \langle 1,2,4\rangle & \to & \langle 0,2,7\rangle & & \end{array}$$

In general $[\![P]\!](\langle h,l,0\rangle) = \langle 0,l,3h+1\rangle$.

We provide necessary and sufficient conditions such that

$\Downarrow$

Abstraction removes time from timed denotational semantics!

TIMED SEMANTICS	UNTIMED SEMANTICS
$Par([\![P]\!](2,4,0))^{\mathsf{TL}} = Par(6,3) = \langle 2\mathbb{Z}, 2\mathbb{Z}+1\rangle$	$\Pi^{\mathsf{T}}(\langle 2\mathbb{Z}, 2\mathbb{Z}+1\rangle) = \langle 2\mathbb{Z}, \mathbb{Z}\rangle$
$\neq$	$=$
$Par([\![P]\!](4,4,0))^{\mathsf{TL}} = Par(8,6) = \langle 2\mathbb{Z}, 2\mathbb{Z}\rangle$	$\Pi^{\mathsf{T}}(\langle 2\mathbb{Z}, 2\mathbb{Z}\rangle) = \langle 2\mathbb{Z}, \mathbb{Z}\rangle$

Conclusion

- We extended the notion of abstract non-interference with time:
  - We can model stronger attackers able to measure time;
  - We can model abstract non-interference in systems with time;

Conclusion

- We extended the notion of abstract non-interference with time:
  - We can model stronger attackers able to measure time;
  - We can model abstract non-interference in systems with time;
- We can simply generalize this construction for systems where time is changed by time;

Conclusion

- We extended the notion of abstract non-interference with time:
  - We can model stronger attackers able to measure time;
  - We can model abstract non-interference in systems with time;
- We can simply generalize this construction for systems where time is changed by time;
- We are working on a implementation of a tool for deriving certifications of abstract non-interference properties.