ADJOINING DECLASSIFICATION AND ATTACK MODELS BY ABSTRACT INTERPRETATION

Roberto Giacobazzi and **Isabella Mastroeni**

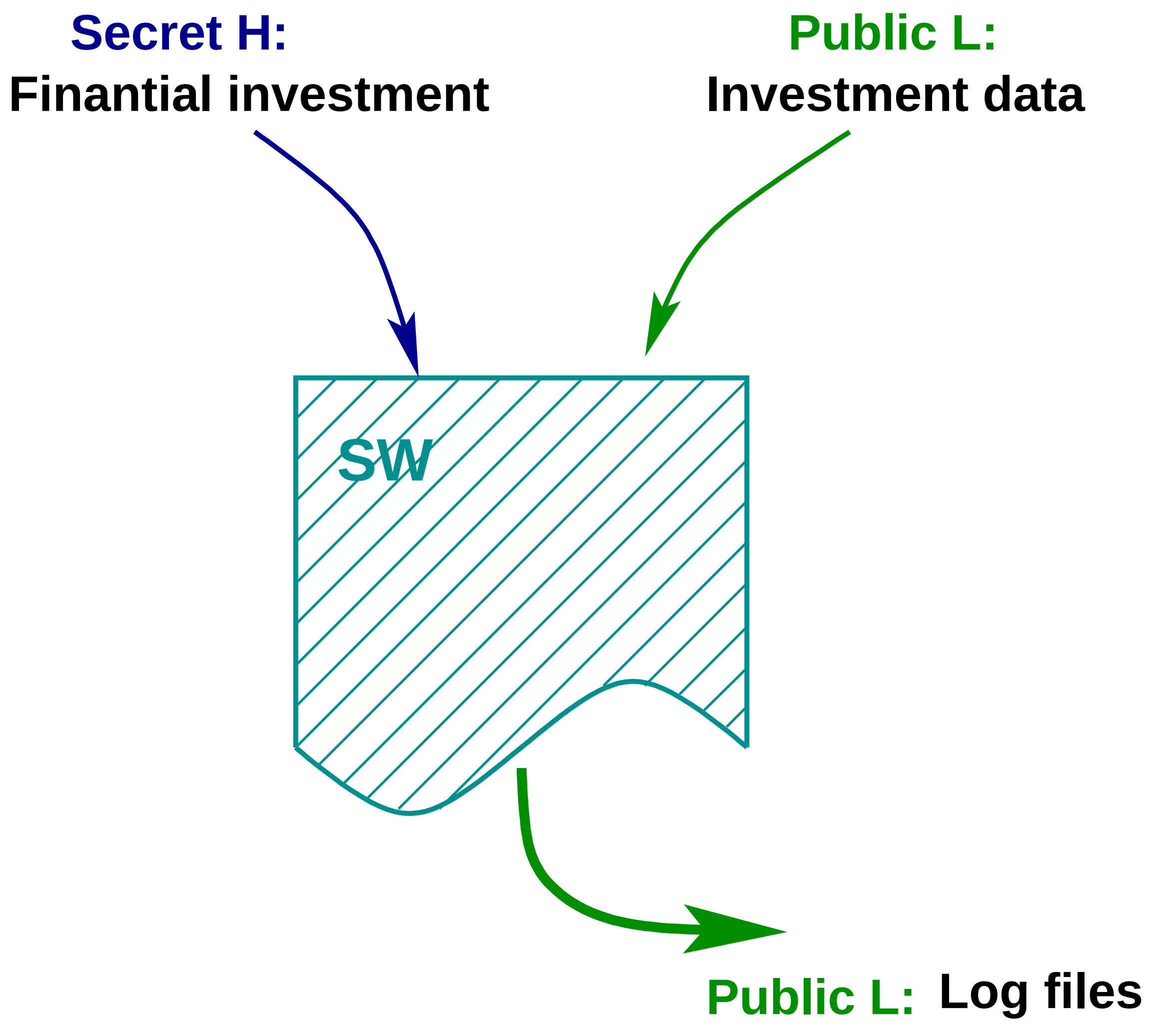
Dipartimento di Informatica

Università di Verona

Italy

Edimburgh, April 8th, 2005

The Problem: Non-Interference

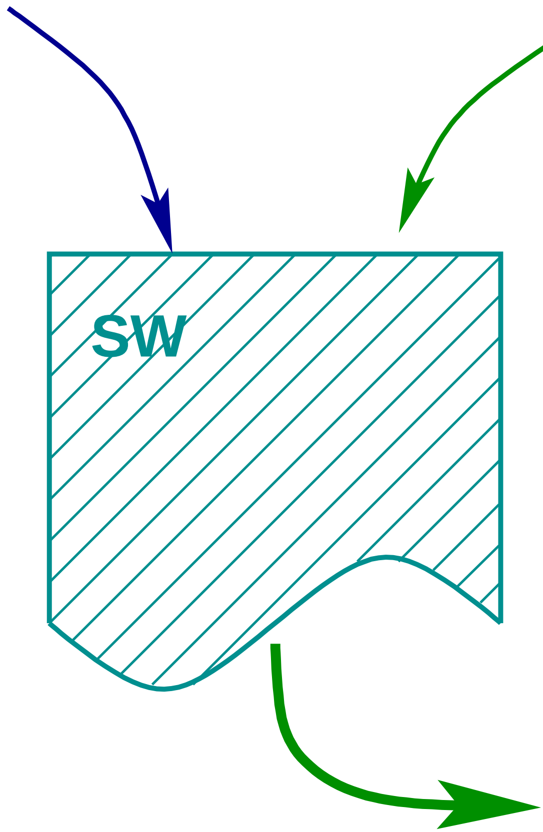


[Sabelfeld and Sands'01]

The Problem: Non-Interference

Secret H:
Finantial investment

Public L:
Investment data



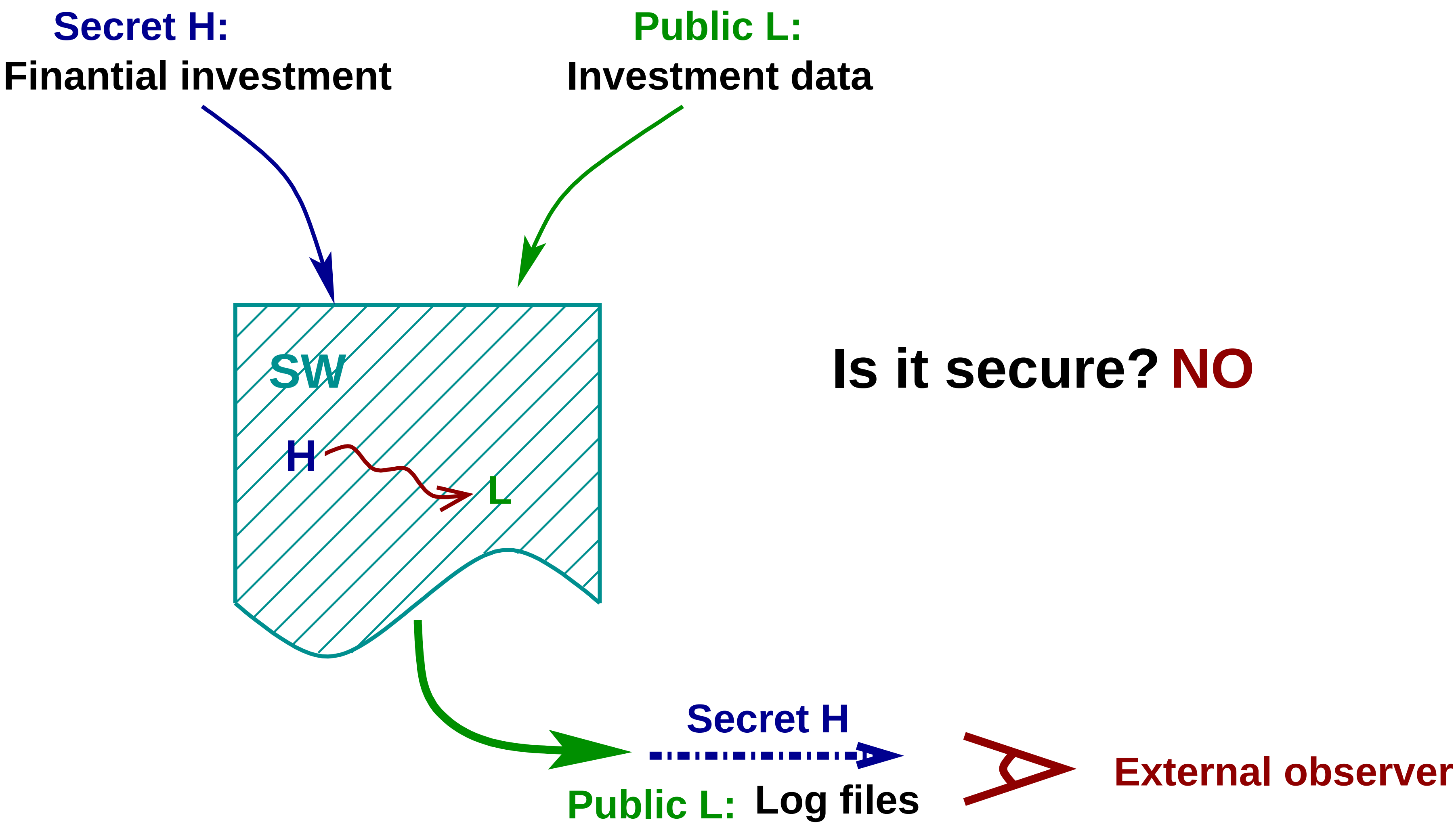
Is it secure?

Public L: Log files

External observer

[Sabelfeld and Sands'01]

The Problem: Non-Interference



Is it secure? NO

[Sabelfeld and Sands'01]

Background: Non-Interference

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

Background: Non-Interference

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

$$\Downarrow$$

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

Background: Non-Interference

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

$\Downarrow$

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

$\Downarrow$

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: Non-Interference

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

$\Downarrow$

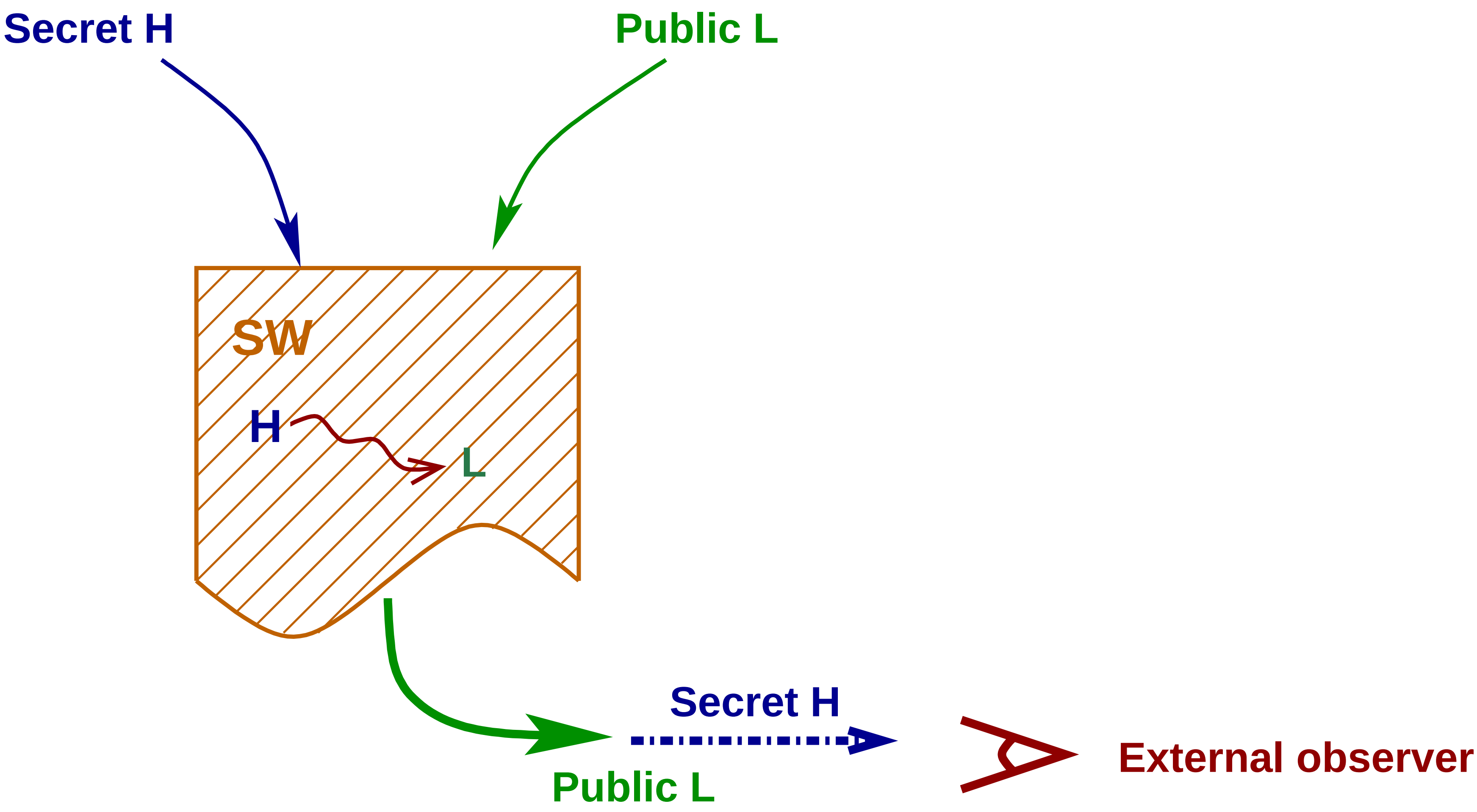
Confi nement problem[Lampson'73]: *Preventing the results of computations leaking even partial information about the confidential inputs.*

$\Downarrow$

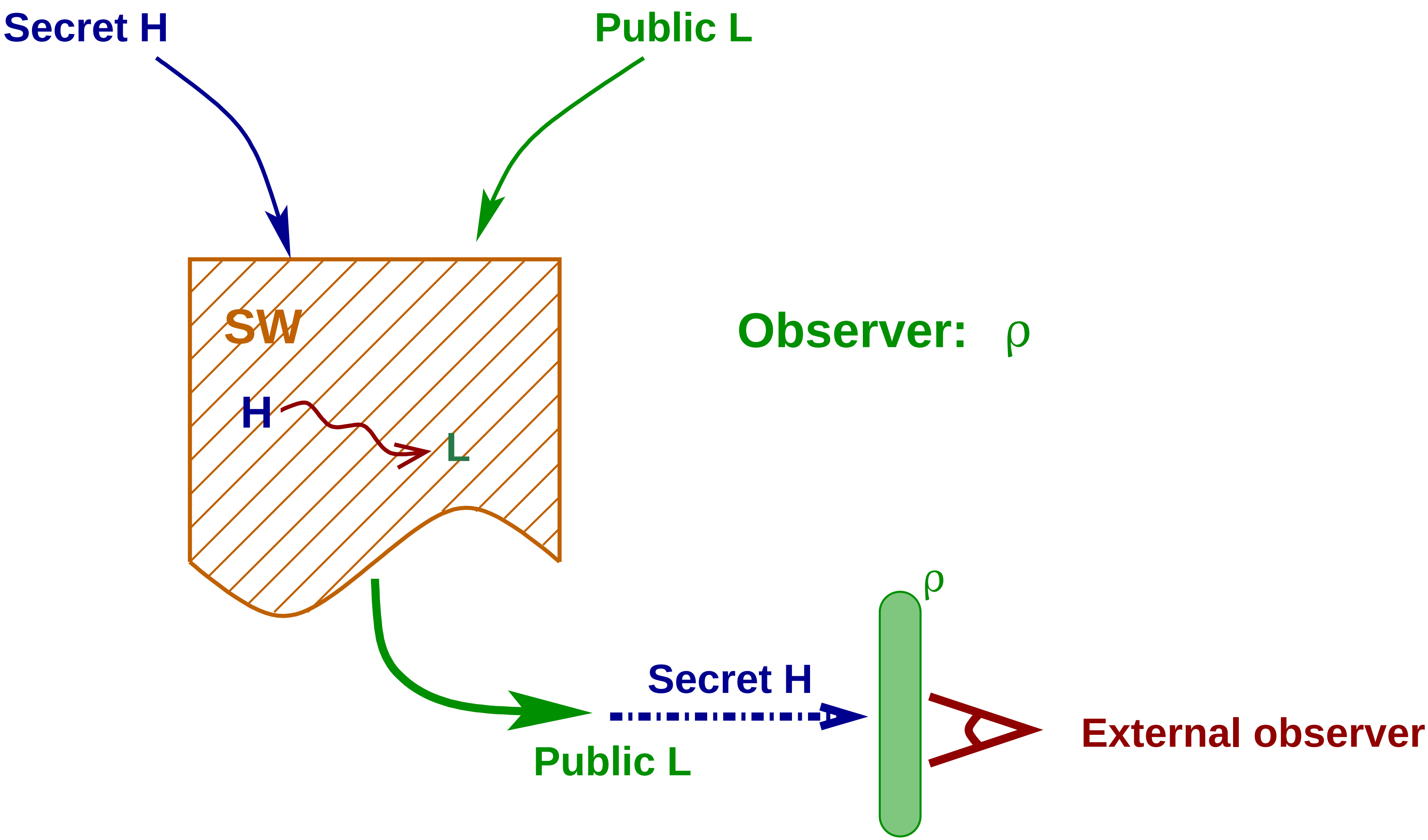
Non-interference policies require that any *change upon confidential data has not to be revealed through the observation of public data.*

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

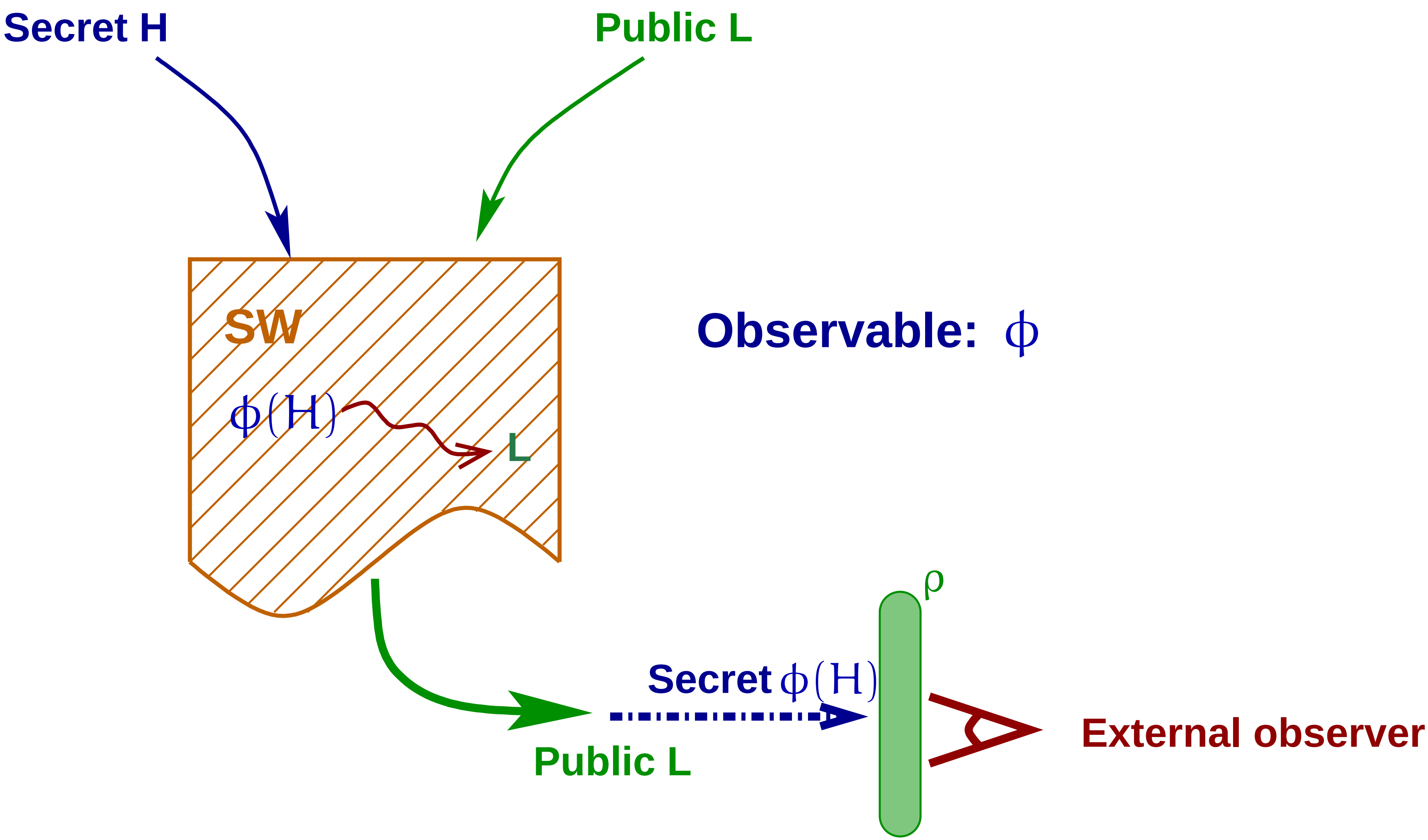
Our idea: Abstracting Non-Interference



Our idea: Abstracting Non-Interference



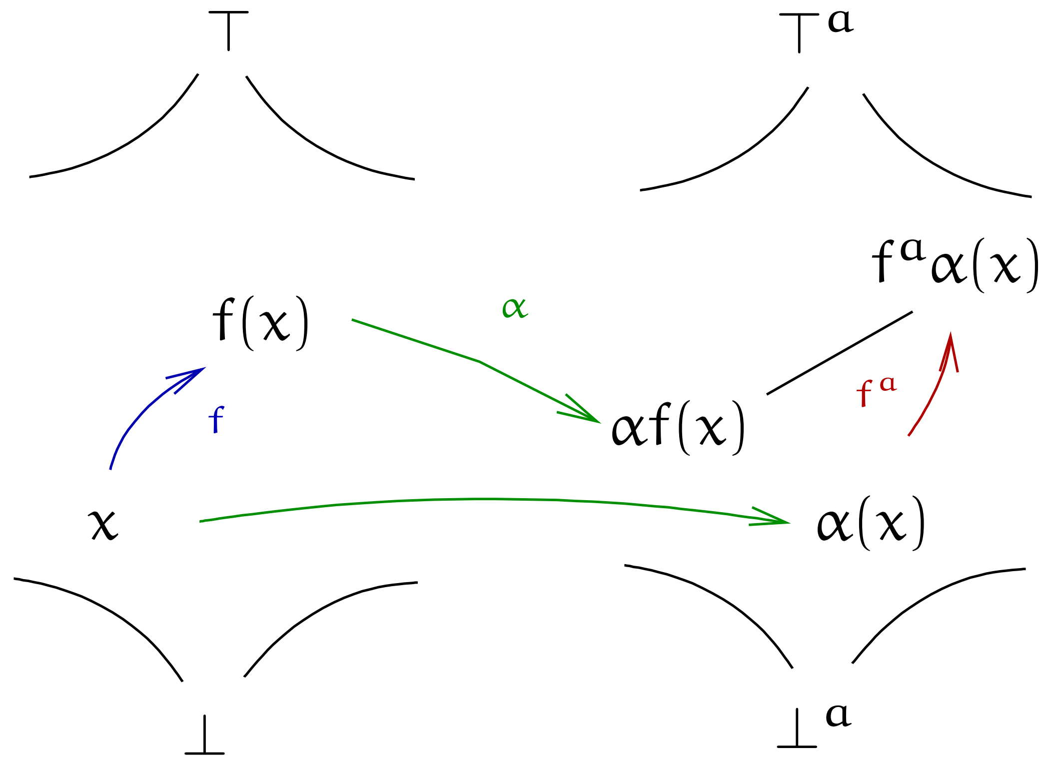
Our idea: Abstracting Non-Interference



Abstract domain completeness

Let $< A, \alpha, \gamma, C >$ a Galois insertion. [Cousot & Cousot '77,'79]
$f : C \longrightarrow C$, $f^a = \alpha \circ f \circ \gamma : A \longrightarrow A$ (b.c.a. of f) and ρ=$\gamma \circ \alpha$

ρ correct for f



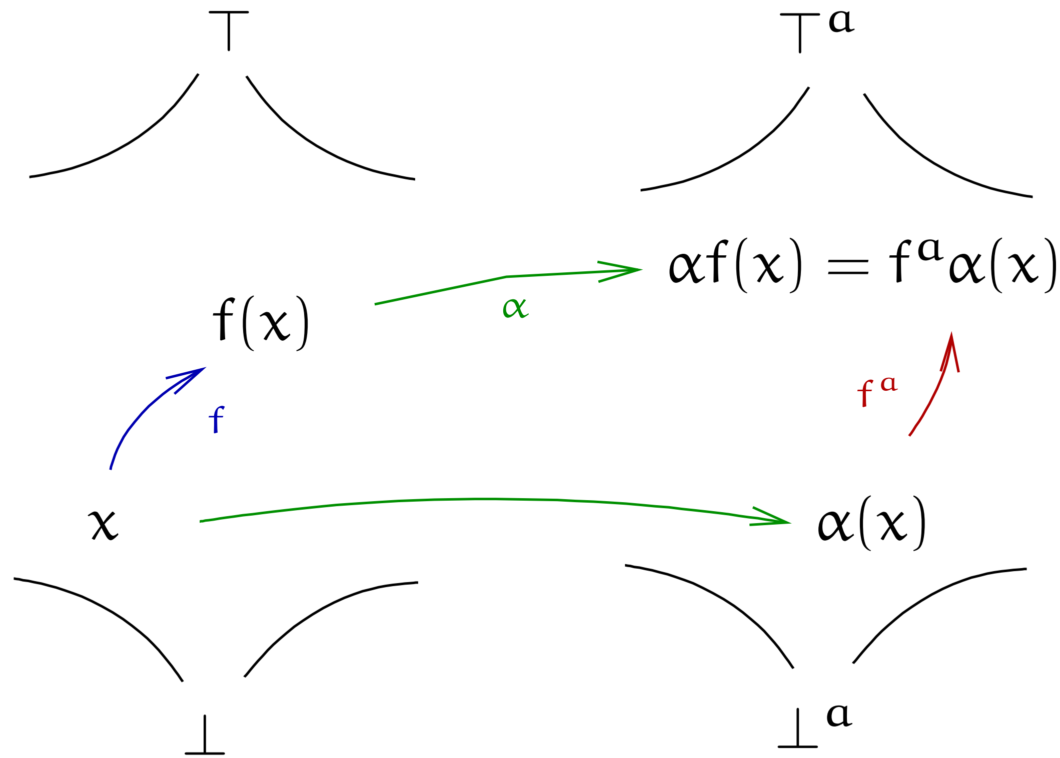
Abstract domain completeness

Let $< A, \alpha, \gamma, C >$ a Galois insertion. [Cousot & Cousot '77,'79]
$f : C \longrightarrow C$, $f^a = \alpha \circ f \circ \gamma : A \longrightarrow A$ (b.c.a. of f) and $\rho = \gamma \circ \alpha$

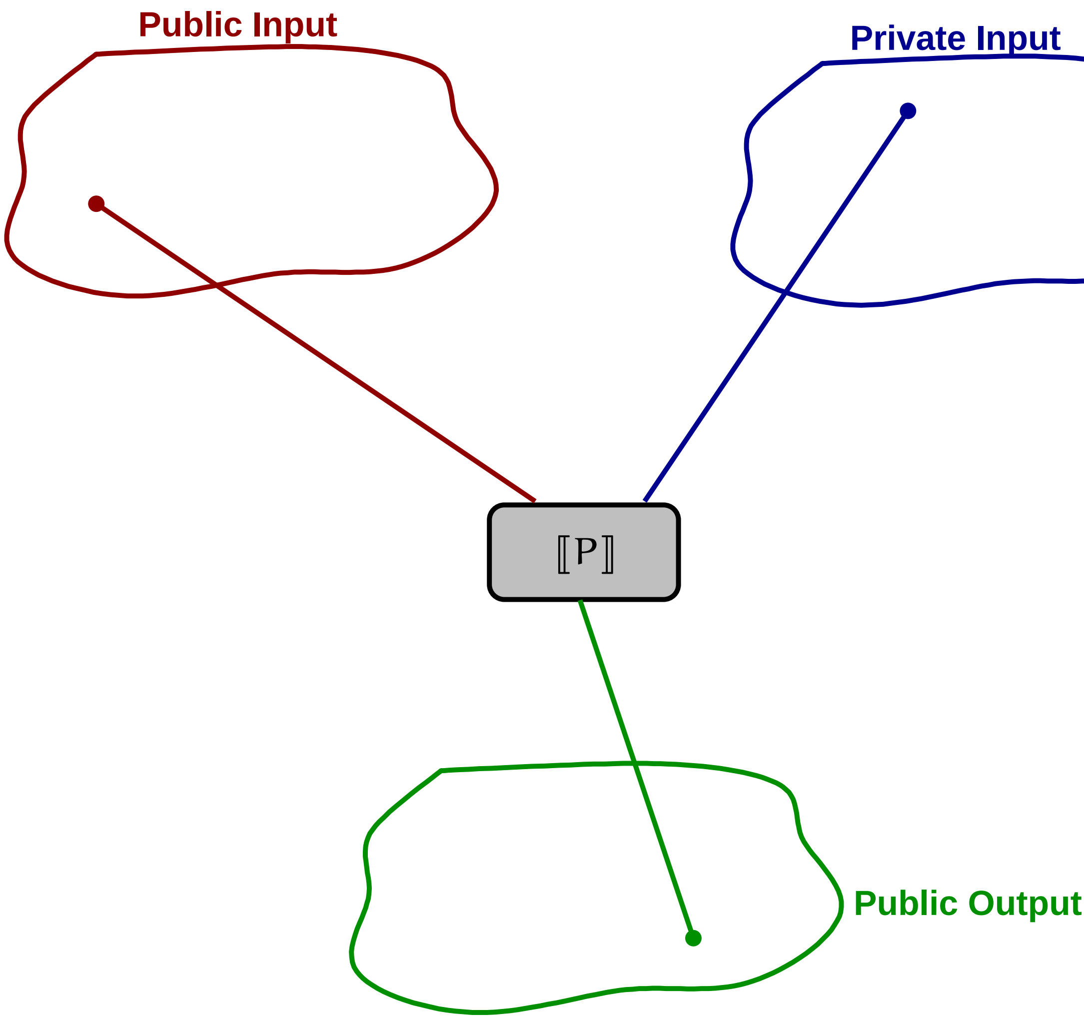
ρ complete for f

$|||$

$\rho f \rho = \rho f$

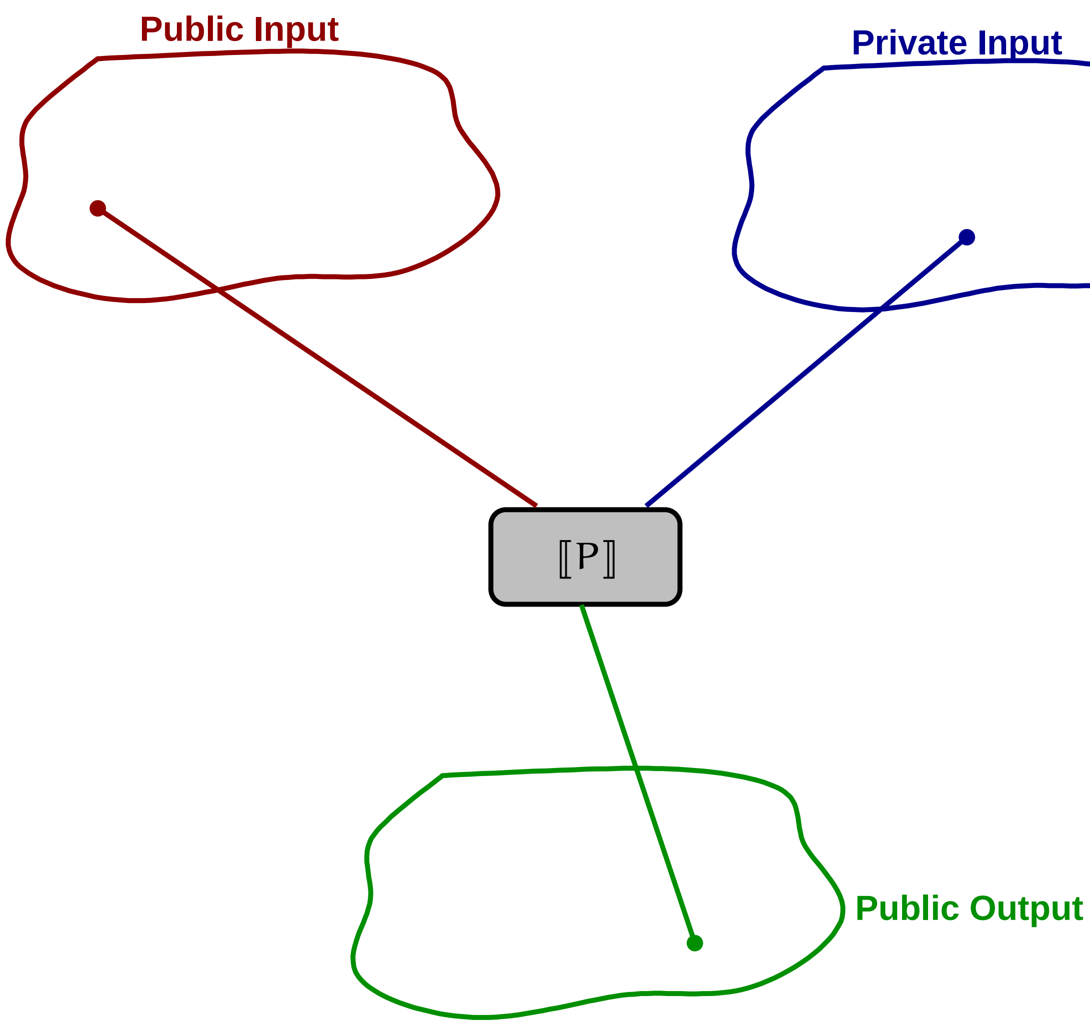


Standard non-interference



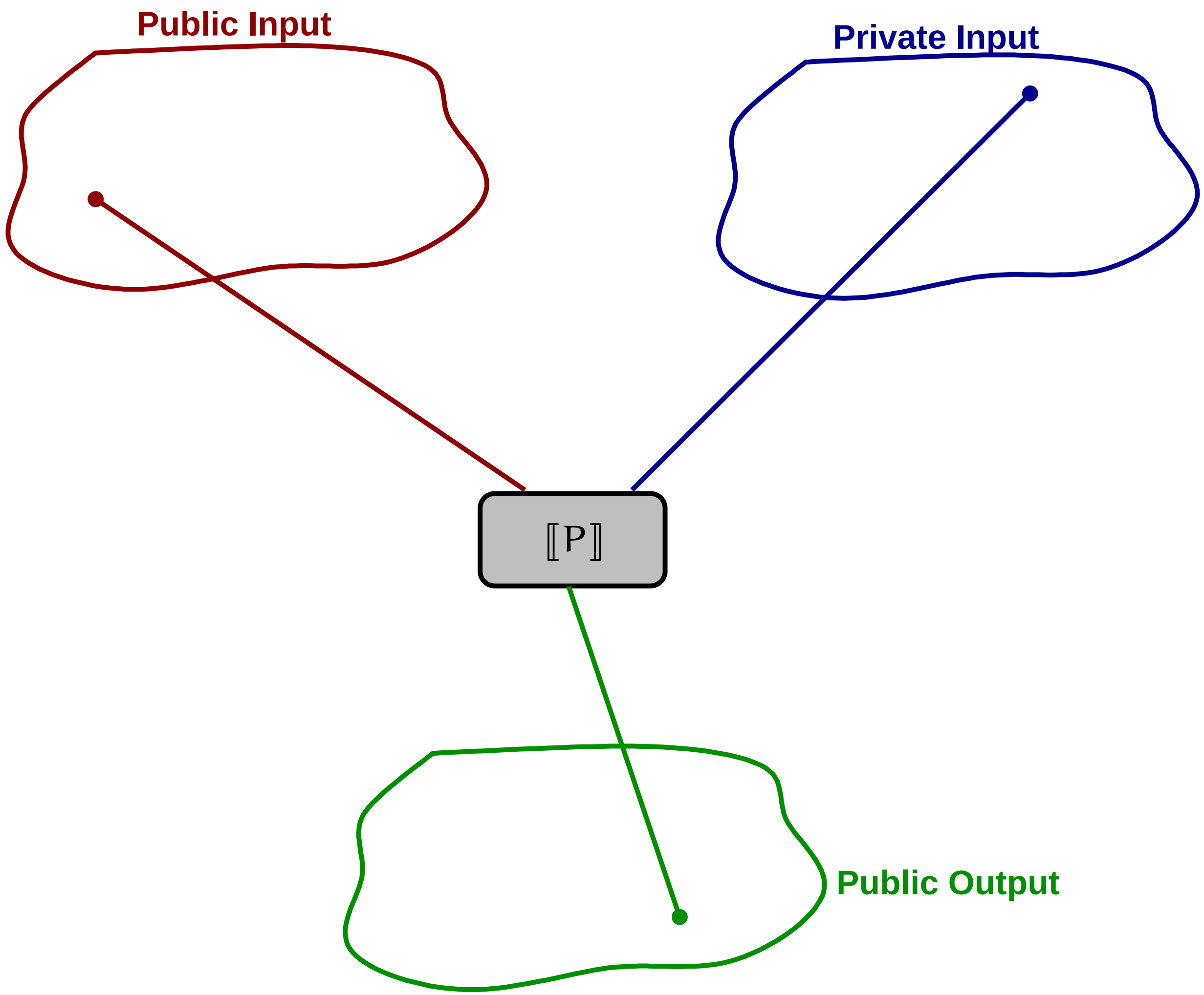
$$\forall l : \mathsf{L}\ , \forall h_1, h_2 : \mathsf{H}\ .\ [\![P]\!](h_1, l)^{\mathsf{L}} = [\![P]\!](h_2, l)^{\mathsf{L}}$$

Standard non-interference



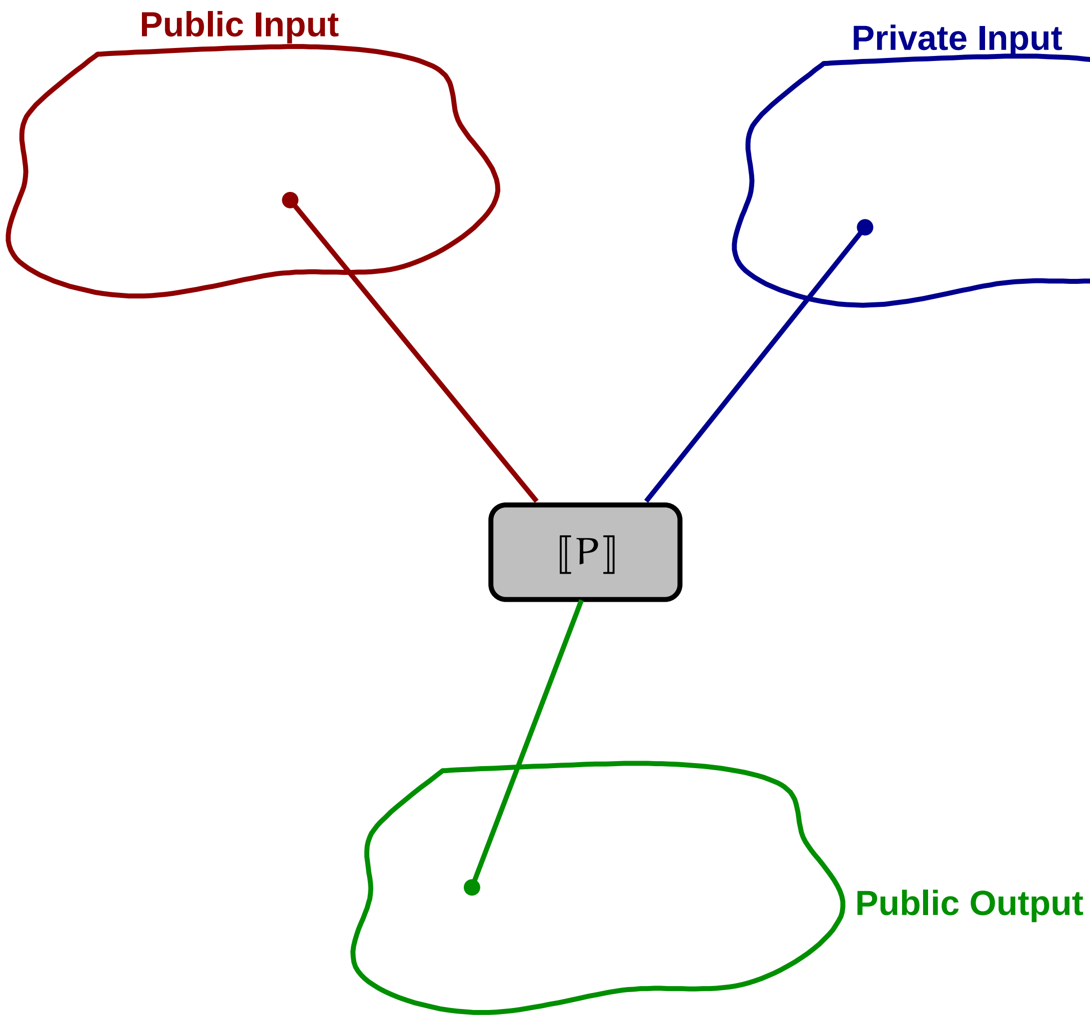
$$\forall l : \mathsf{L}\,, \forall h_1, h_2 : \mathsf{H}\,.\ [\![P]\!](h_1, l)^{\mathsf{L}} = [\![P]\!](h_2, l)^{\mathsf{L}}$$

Standard non-interference



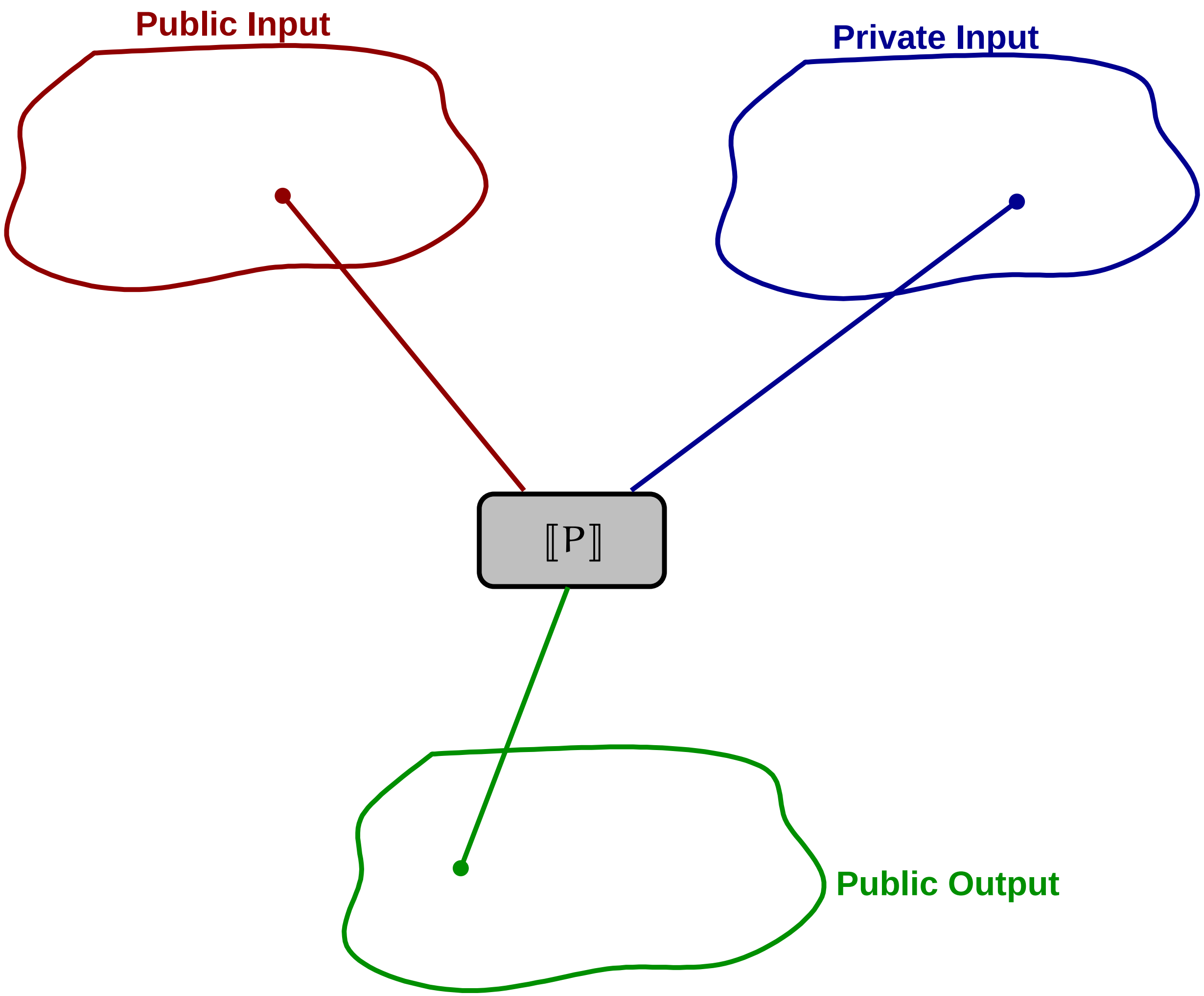
$$\forall l : \mathsf{L}\,, \forall h_1, h_2 : \mathsf{H}\,.\; [\![P]\!](h_1, l)^{\mathsf{L}} = [\![P]\!](h_2, l)^{\mathsf{L}}$$

Standard non-interference



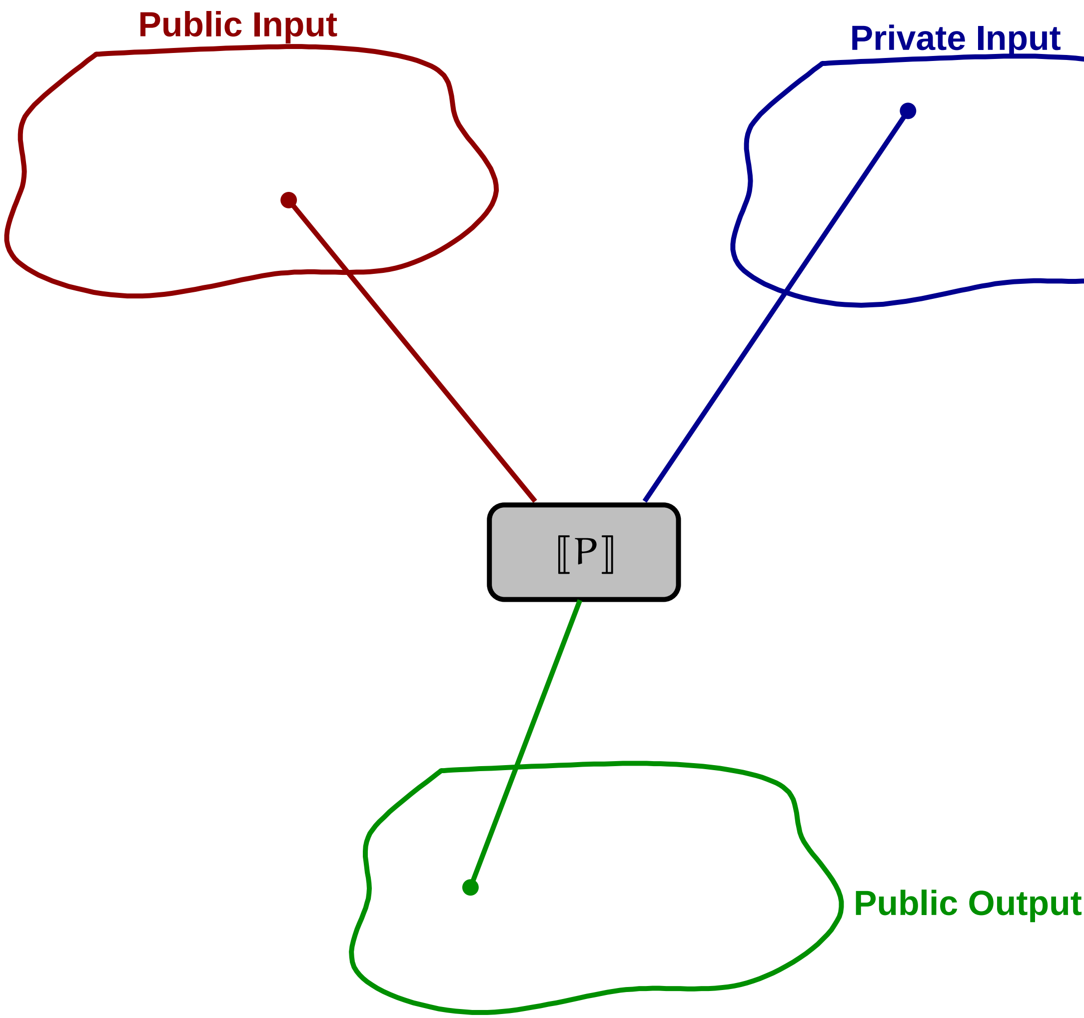
$$\forall l : \mathsf{L}\,, \forall h_1, h_2 : \mathsf{H}\,.\; [\![P]\!](h_1, l)^{\mathsf{L}} = [\![P]\!](h_2, l)^{\mathsf{L}}$$

Standard non-interference



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

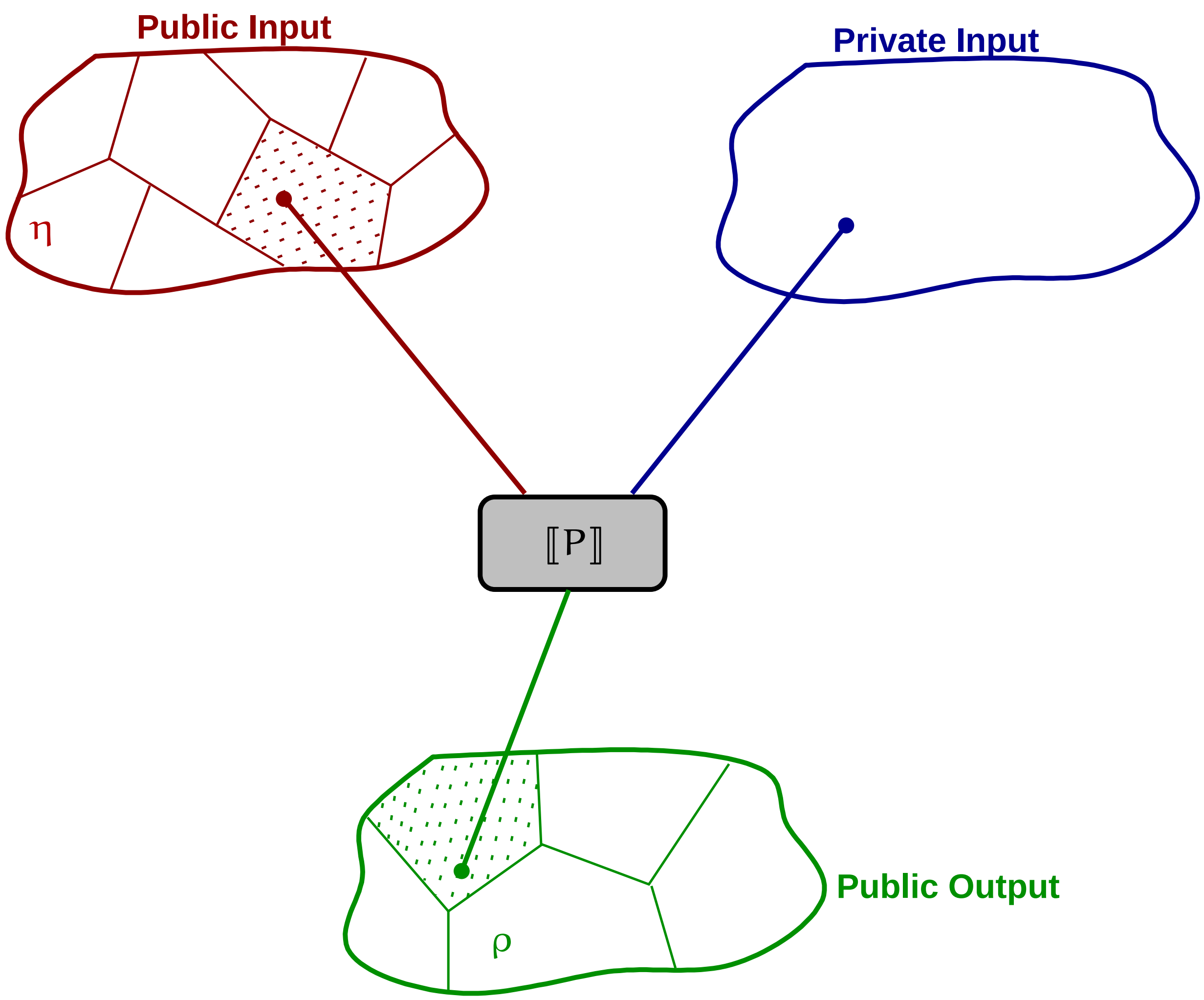
Standard non-interference



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

Abstracting non-interference I: Narrow ANI

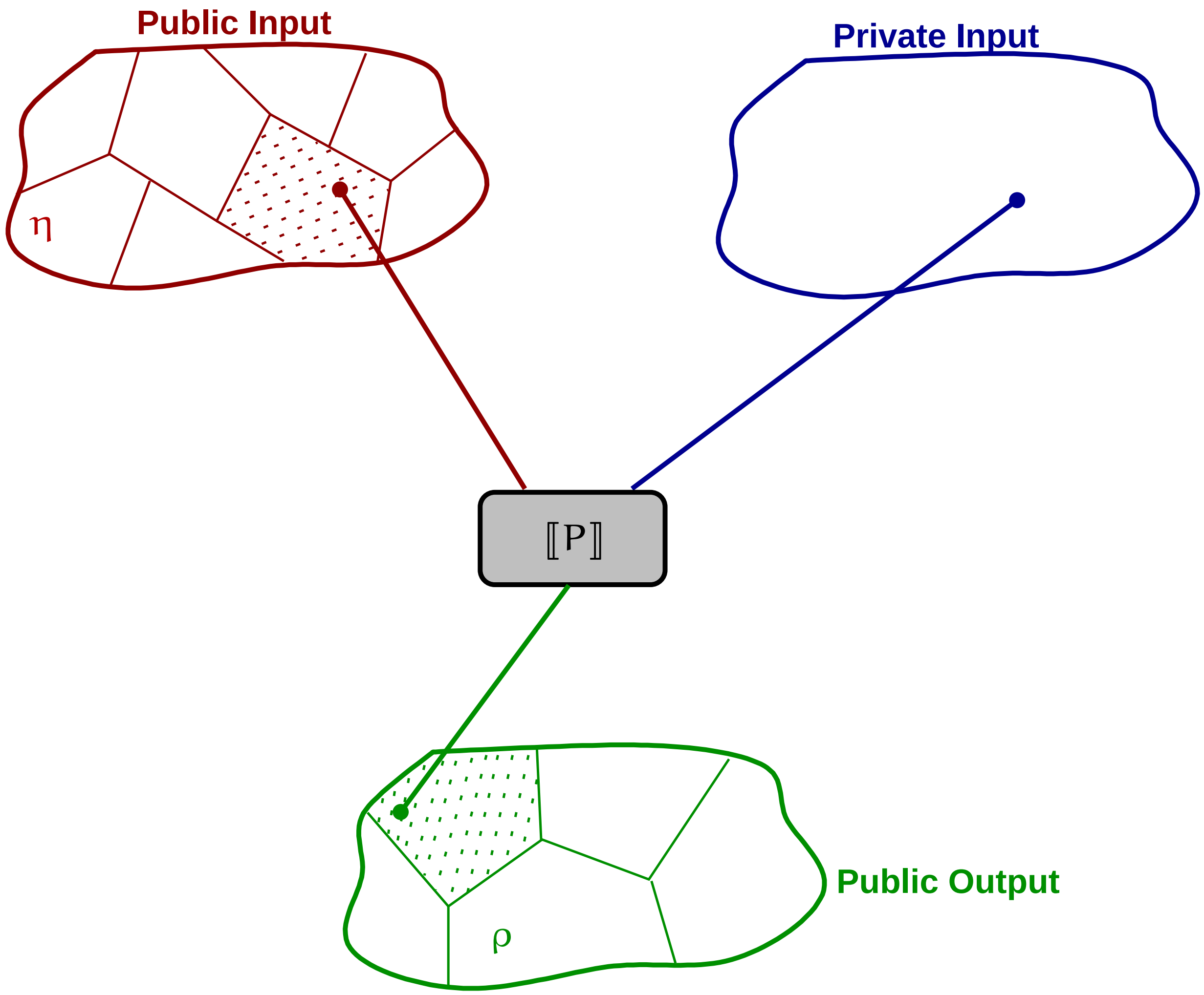
[POPL'04]



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

Abstracting non-interference I: Narrow ANI

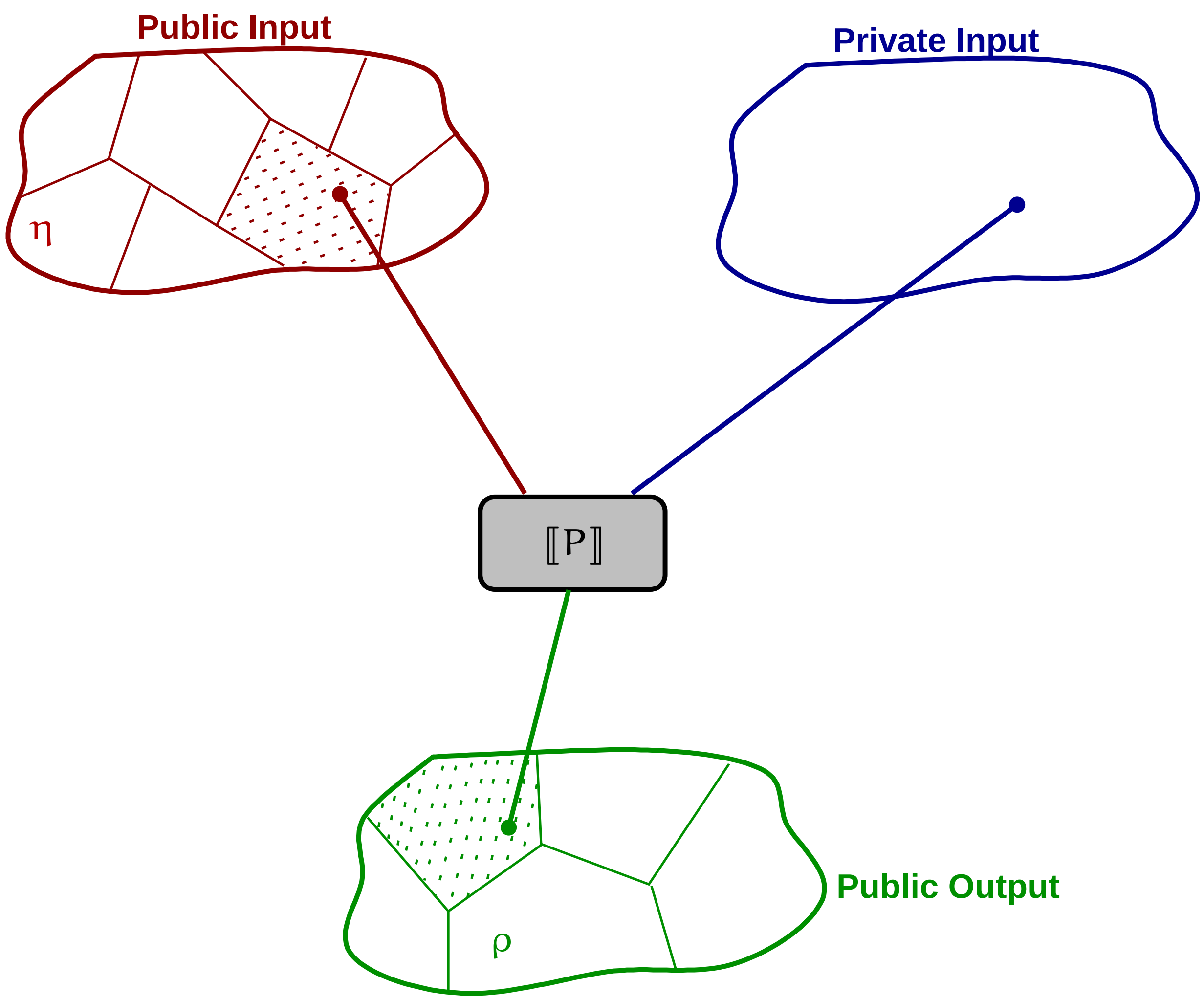
[POPL'04]



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

Abstracting non-interference I: Narrow ANI

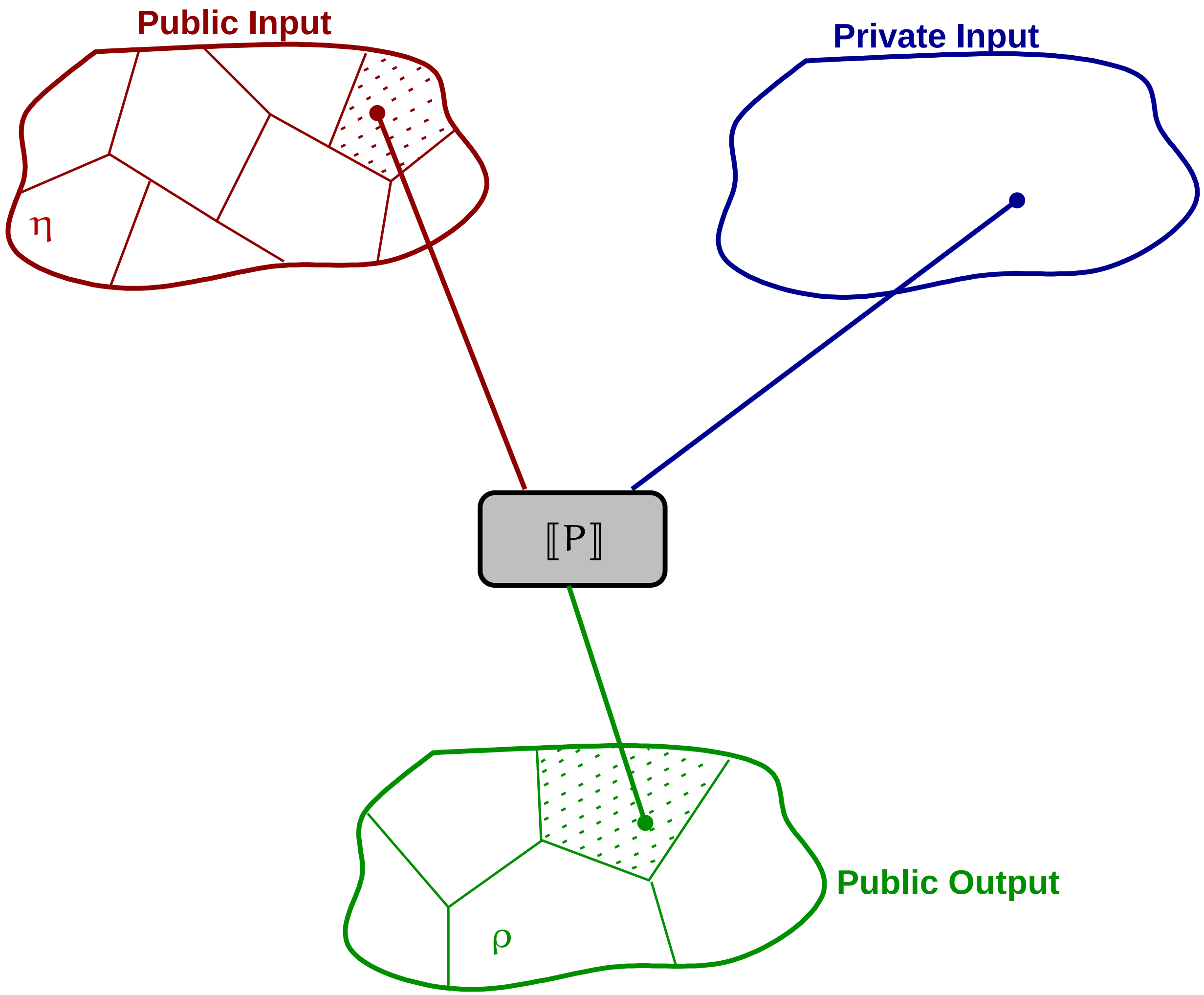
[POPL'04]



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

Abstracting non-interference I: Narrow ANI

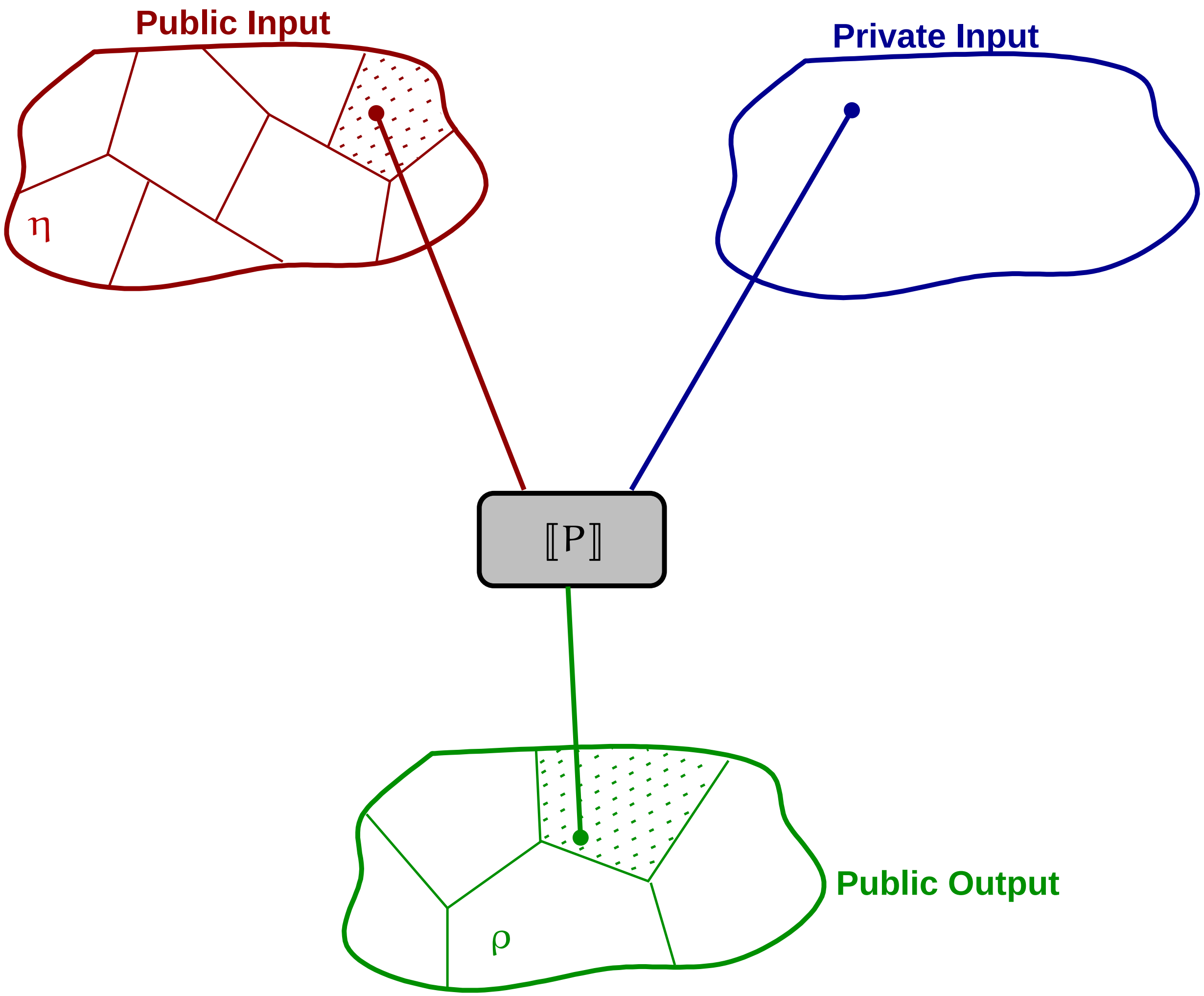
[POPL'04]



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

Abstracting non-interference I: Narrow ANI

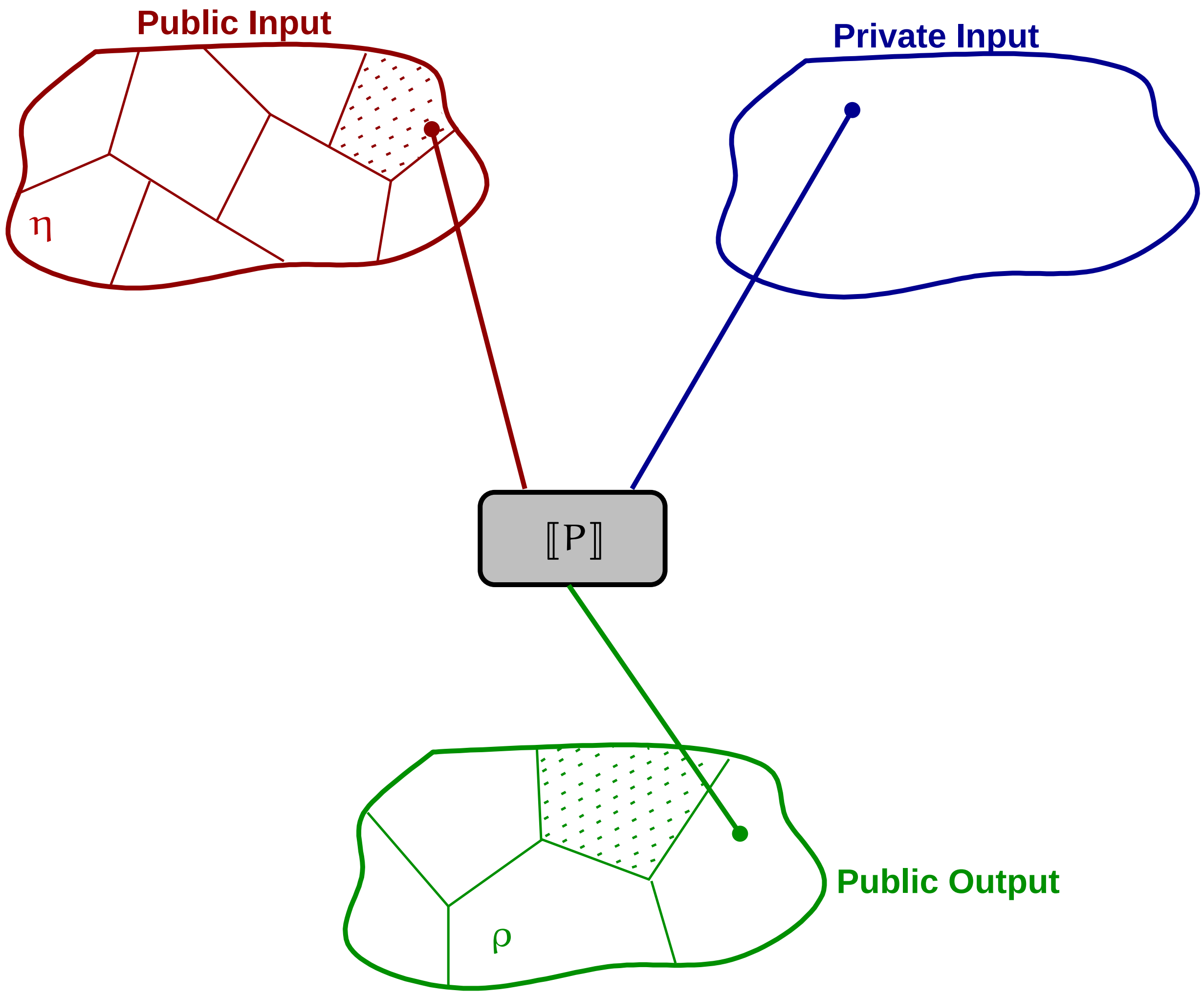
[POPL'04]



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

Abstracting non-interference I: Narrow ANI

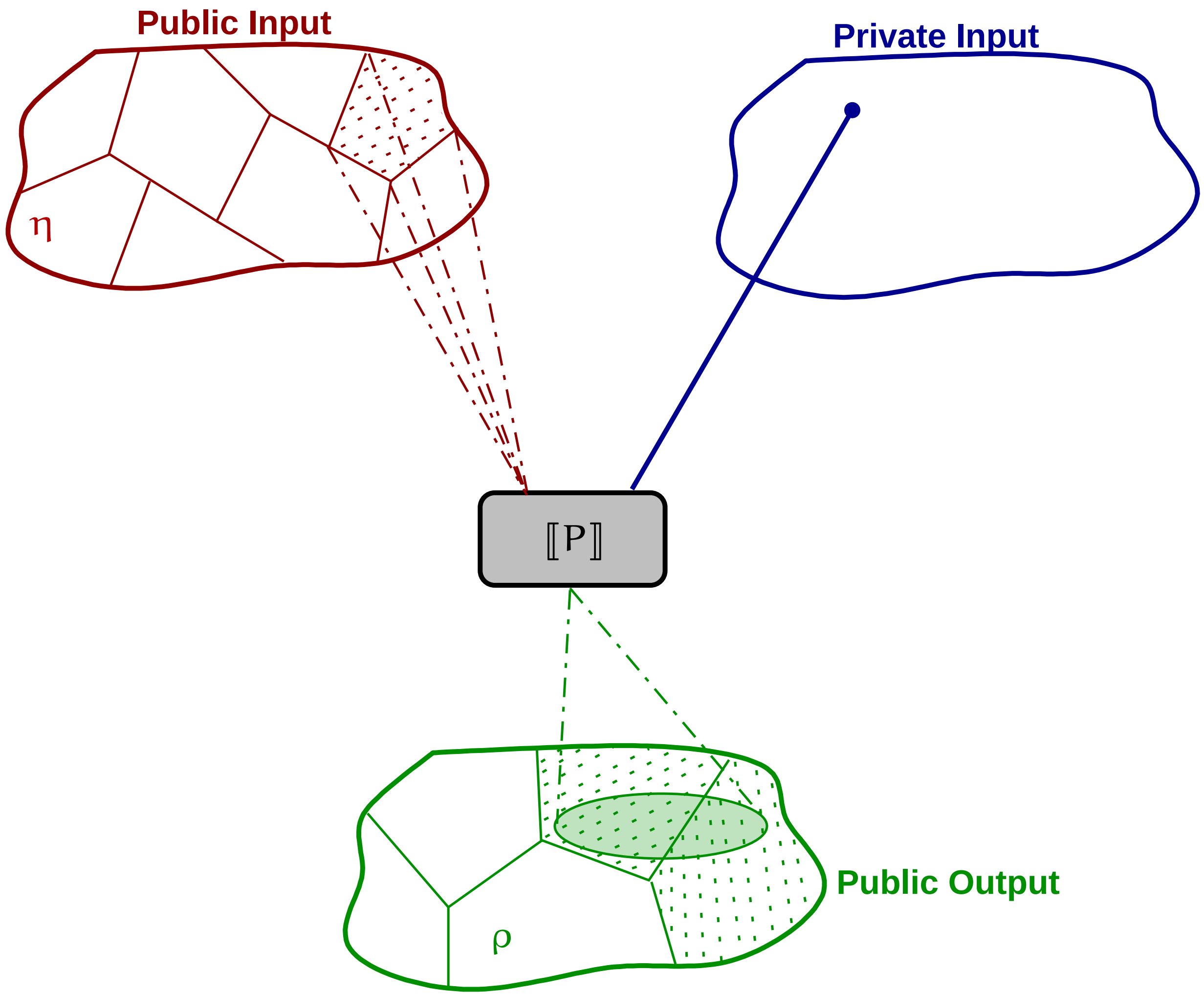
[POPL'04]



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

Abstracting non-interference II

[POPL'04]

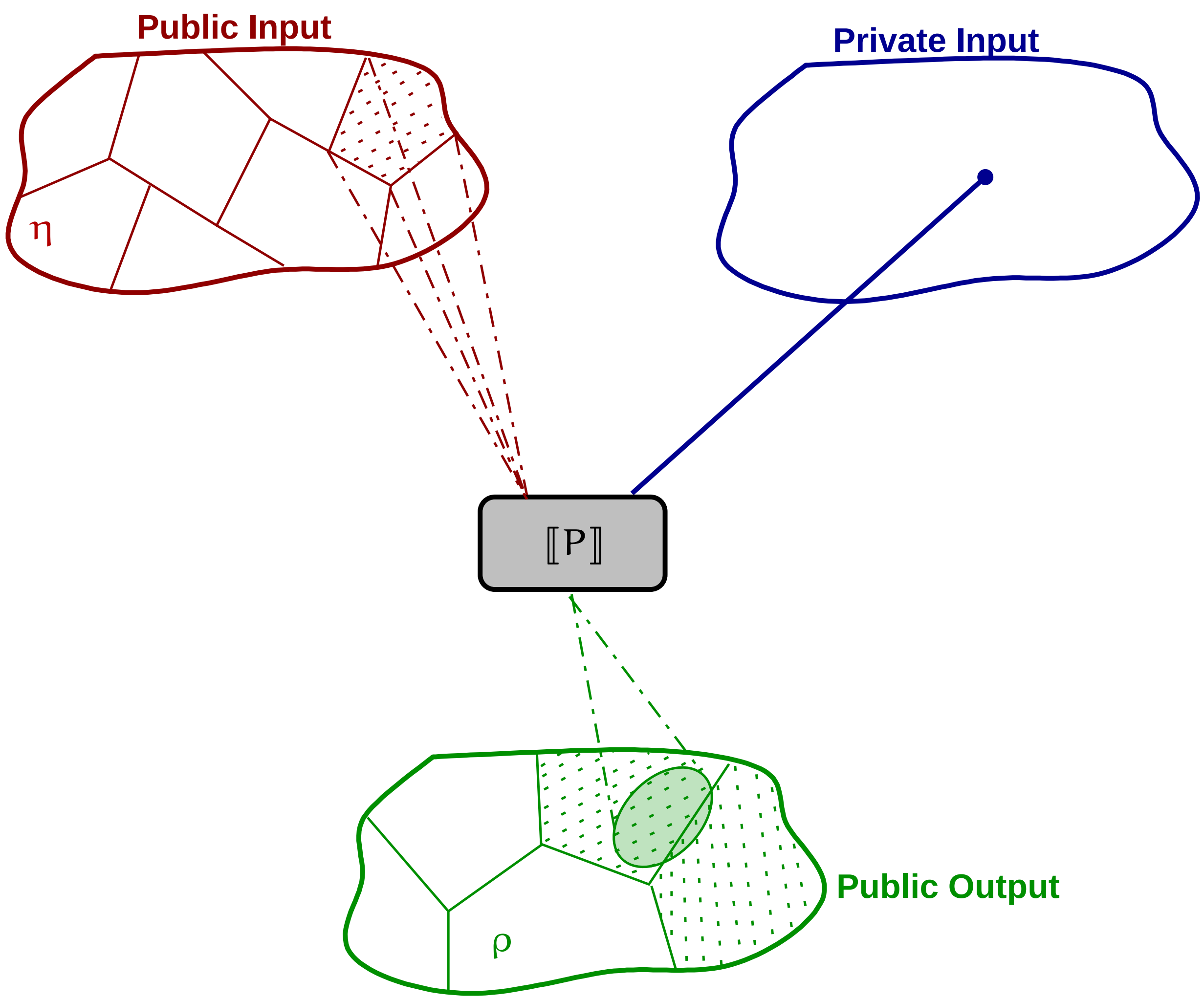


$$\rho, \eta \in Abs(\wp(\mathbb{V}^{L})) \colon (\eta)P(\rho) \colon$$

$$\eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket P \rrbracket(h_1, \eta(l_1))^{L}) = \rho(\llbracket P \rrbracket(h_2, \eta(l_2))^{L})$$

Abstracting non-interference II

[POPL'04]

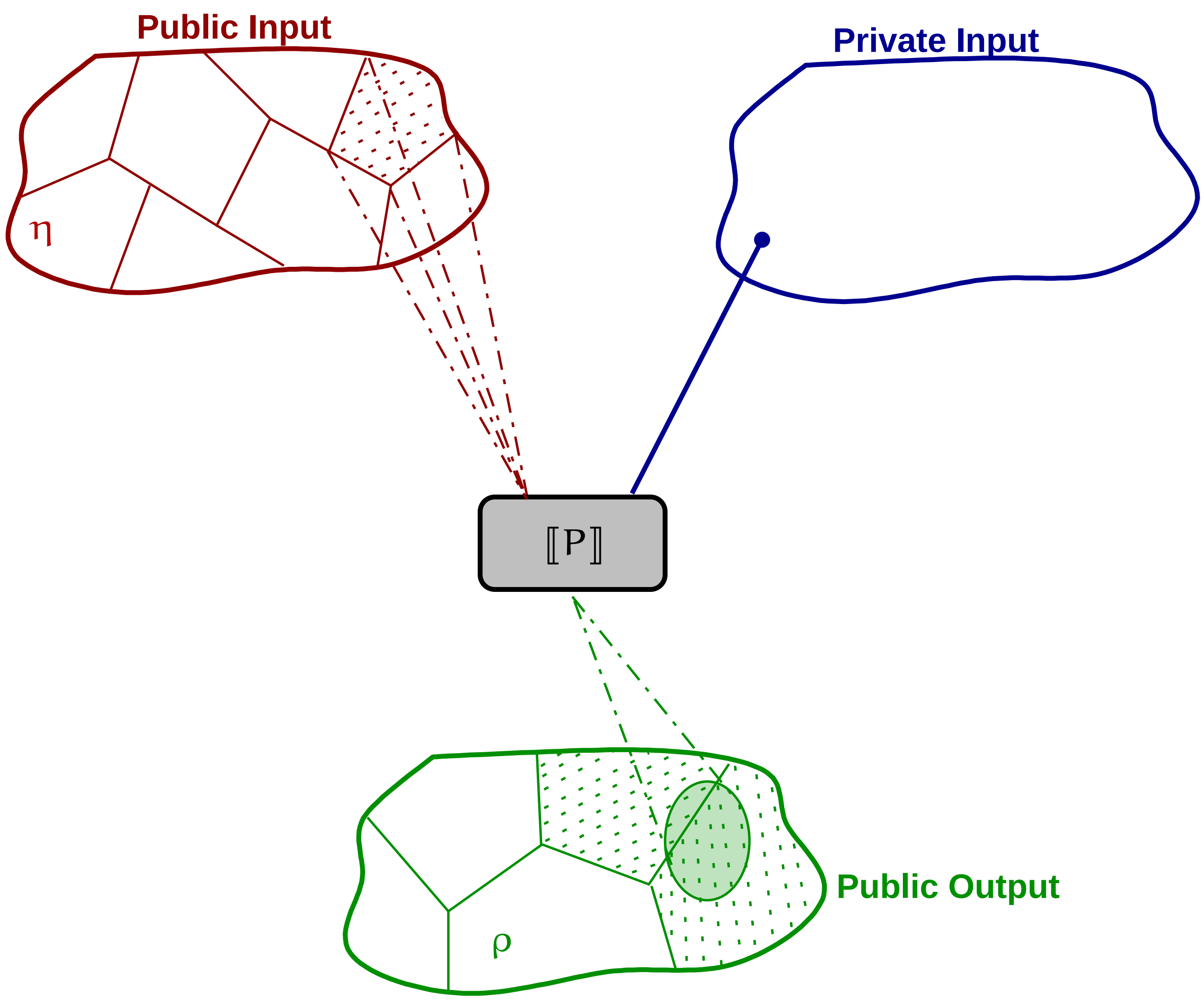


$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{\mathtt{L}})) \text{: } (\eta)P(\rho)\text{:}$$

$$\eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket P \rrbracket(h_1, \eta(l_1))^{\mathtt{L}}) = \rho(\llbracket P \rrbracket(h_2, \eta(l_2))^{\mathtt{L}})$$

Abstracting non-interference II

[POPL'04]

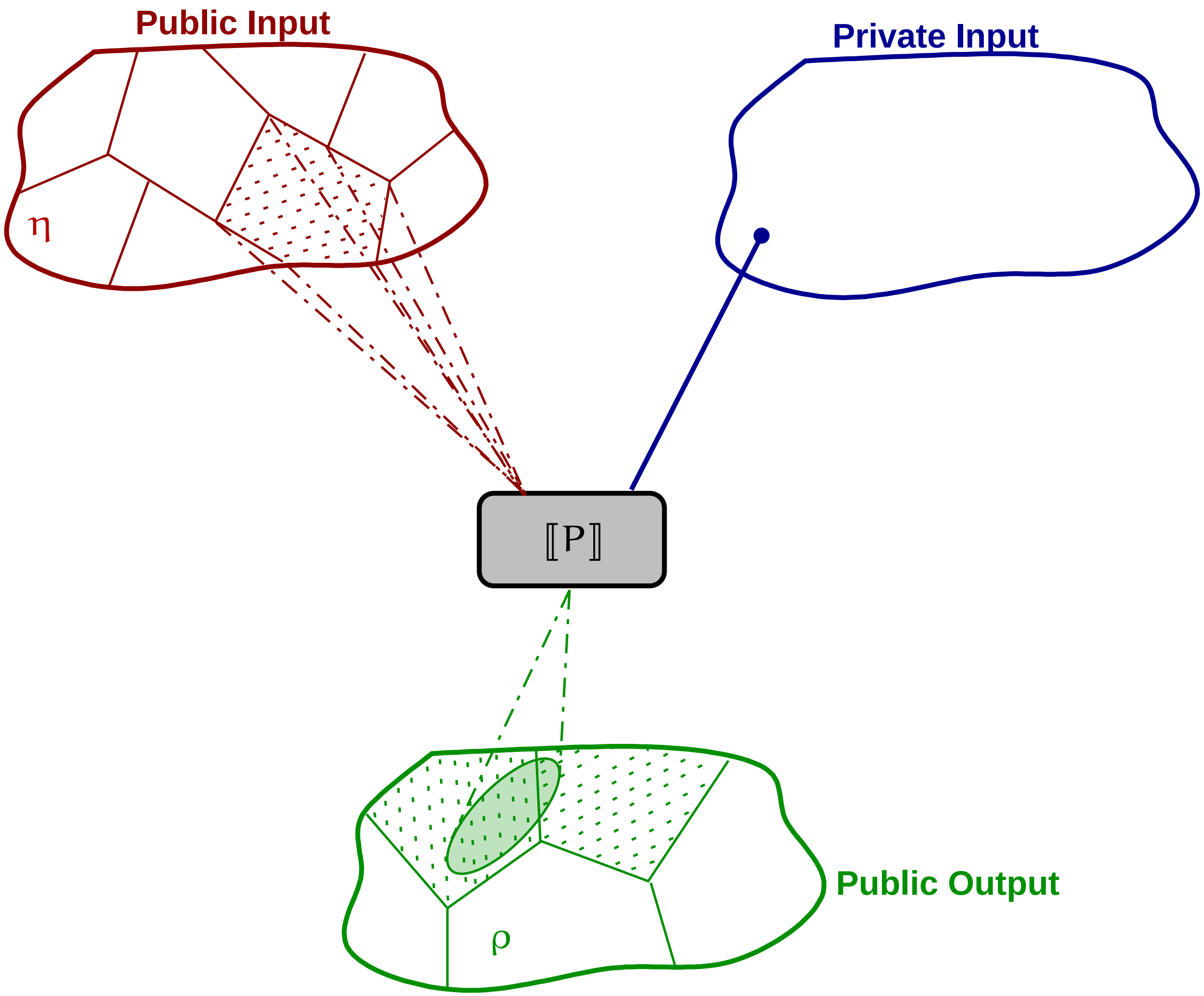


$$\rho, \eta \in Abs(\wp(\mathbb{V}^{\mathtt{L}})) \colon \; (\eta)P(\rho) \colon$$

$$\eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket P \rrbracket(h_1, \eta(l_1))^{\mathtt{L}}) = \rho(\llbracket P \rrbracket(h_2, \eta(l_2))^{\mathtt{L}})$$

Abstracting non-interference II

[POPL'04]

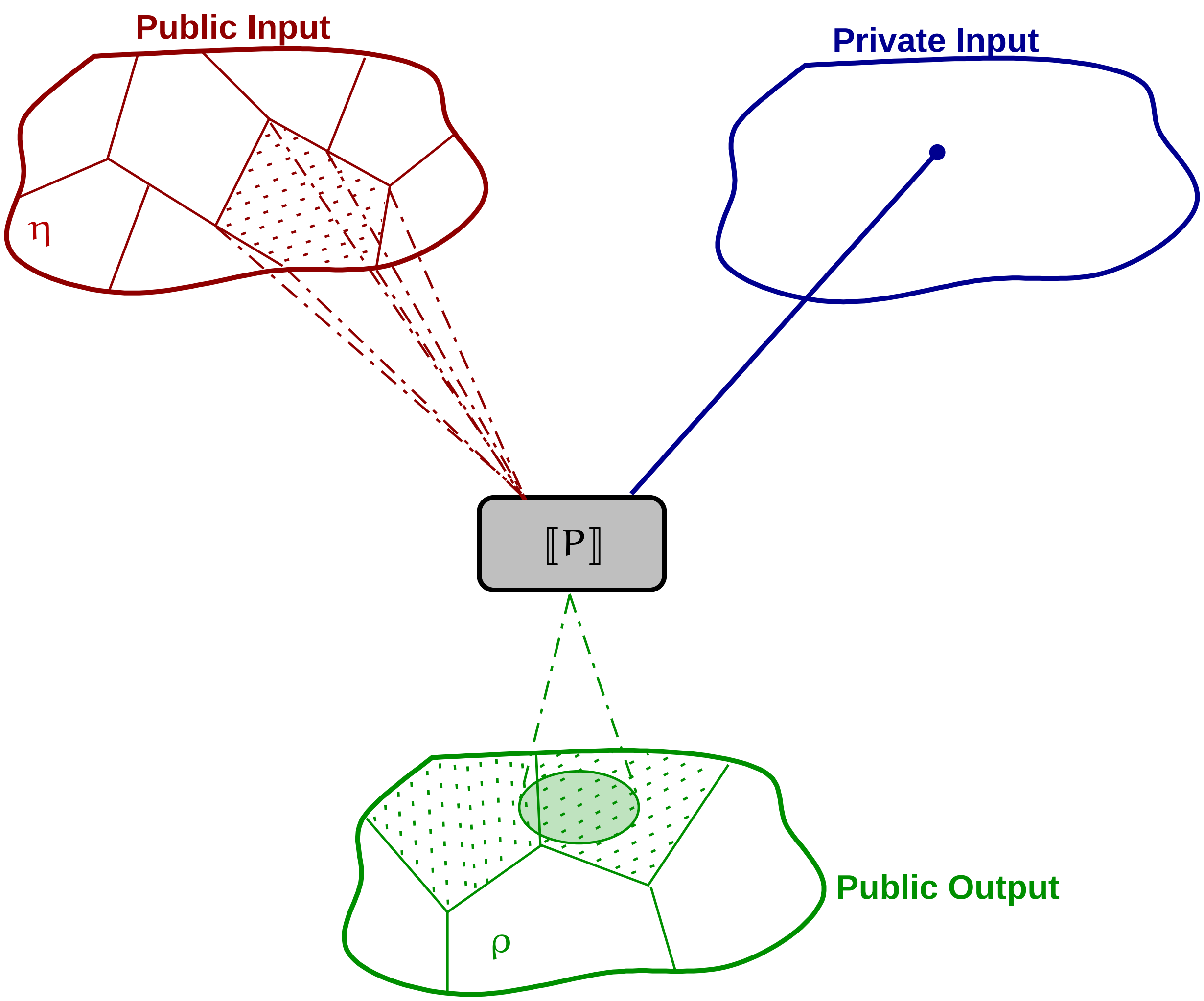


$$\rho, \eta \in Abs(\wp(\mathbb{V}^{\mathrm{L}})) \colon (\eta)P(\rho) \colon$$

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

Abstracting non-interference II

[POPL'04]

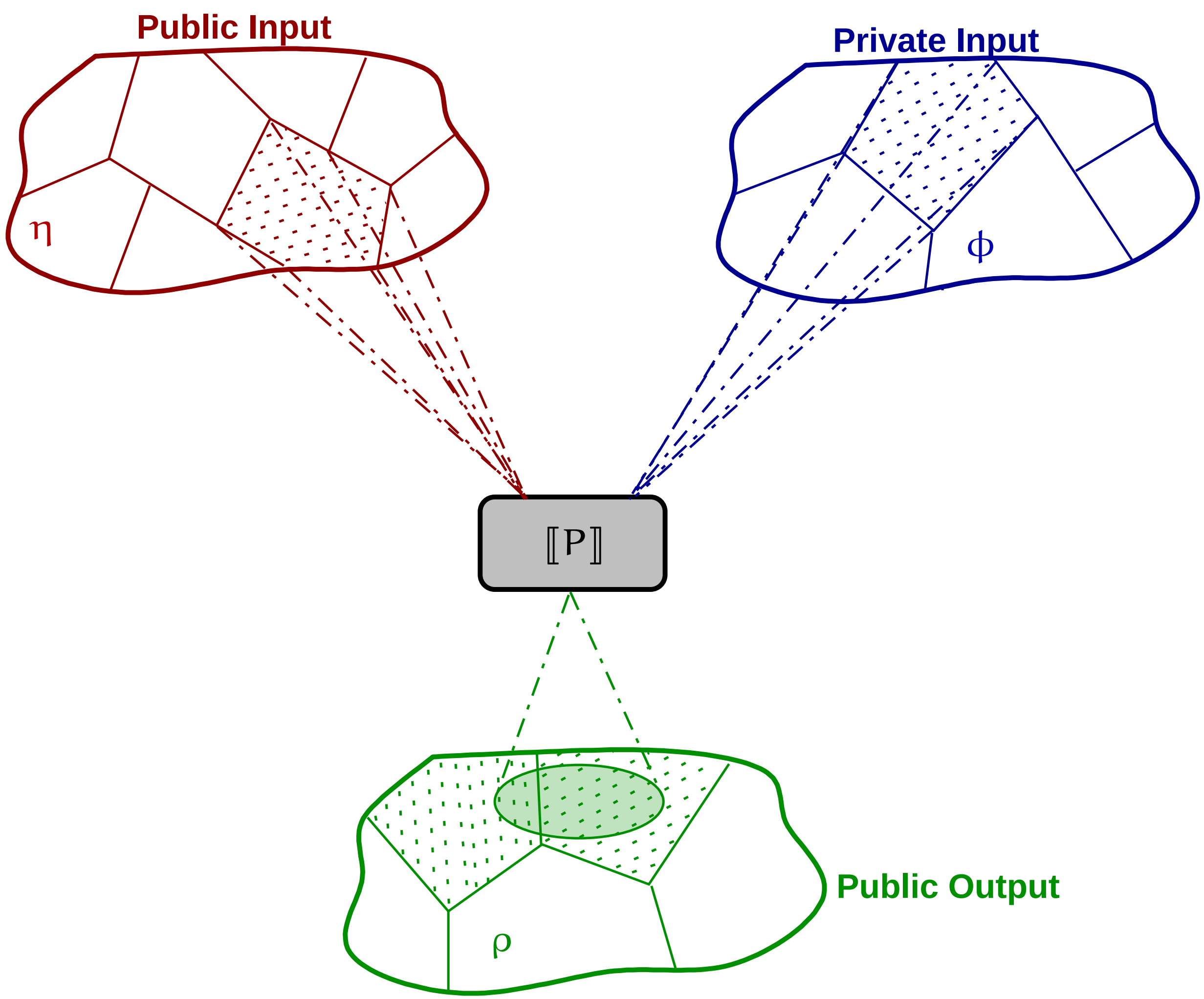


$$\rho, \eta \in Abs(\wp(\mathbb{V}^{L})):\ (\eta)P(\rho):$$

$$\eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket P \rrbracket(h_1, \eta(l_1))^{L}) = \rho(\llbracket P \rrbracket(h_2, \eta(l_2))^{L})$$

Abstracting non-interference III: ANI

[POPL'04]

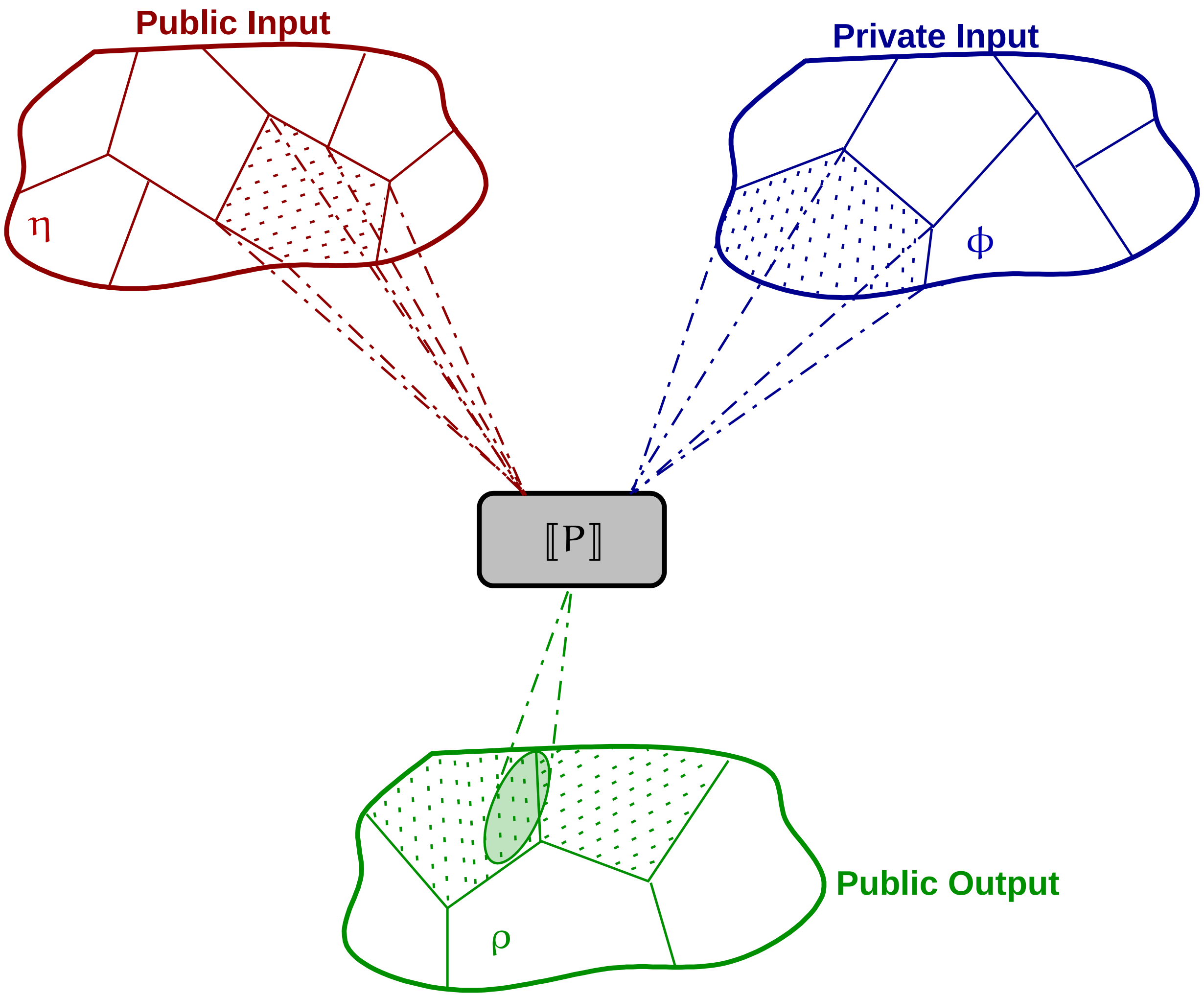


$$\rho, \eta \in Abs(\wp(\mathbb{V}^{L})), \phi \in Abs(\wp(\mathbb{V}^{H})) \text{: } (\eta)P(\phi \rightsquigarrow\!\!\| \rho)\text{:}$$

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

Abstracting non-interference III: ANI

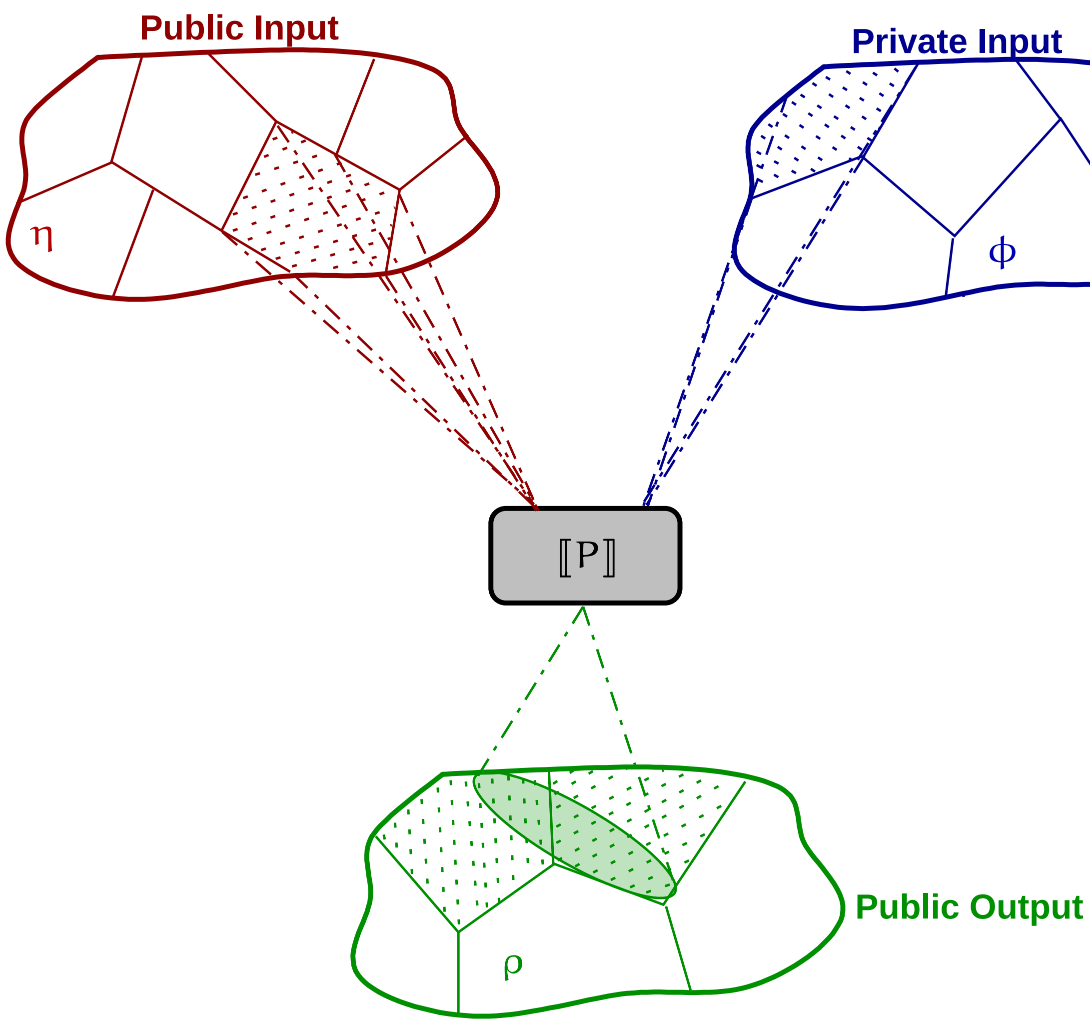
[POPL'04]



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

Abstracting non-interference III: ANI

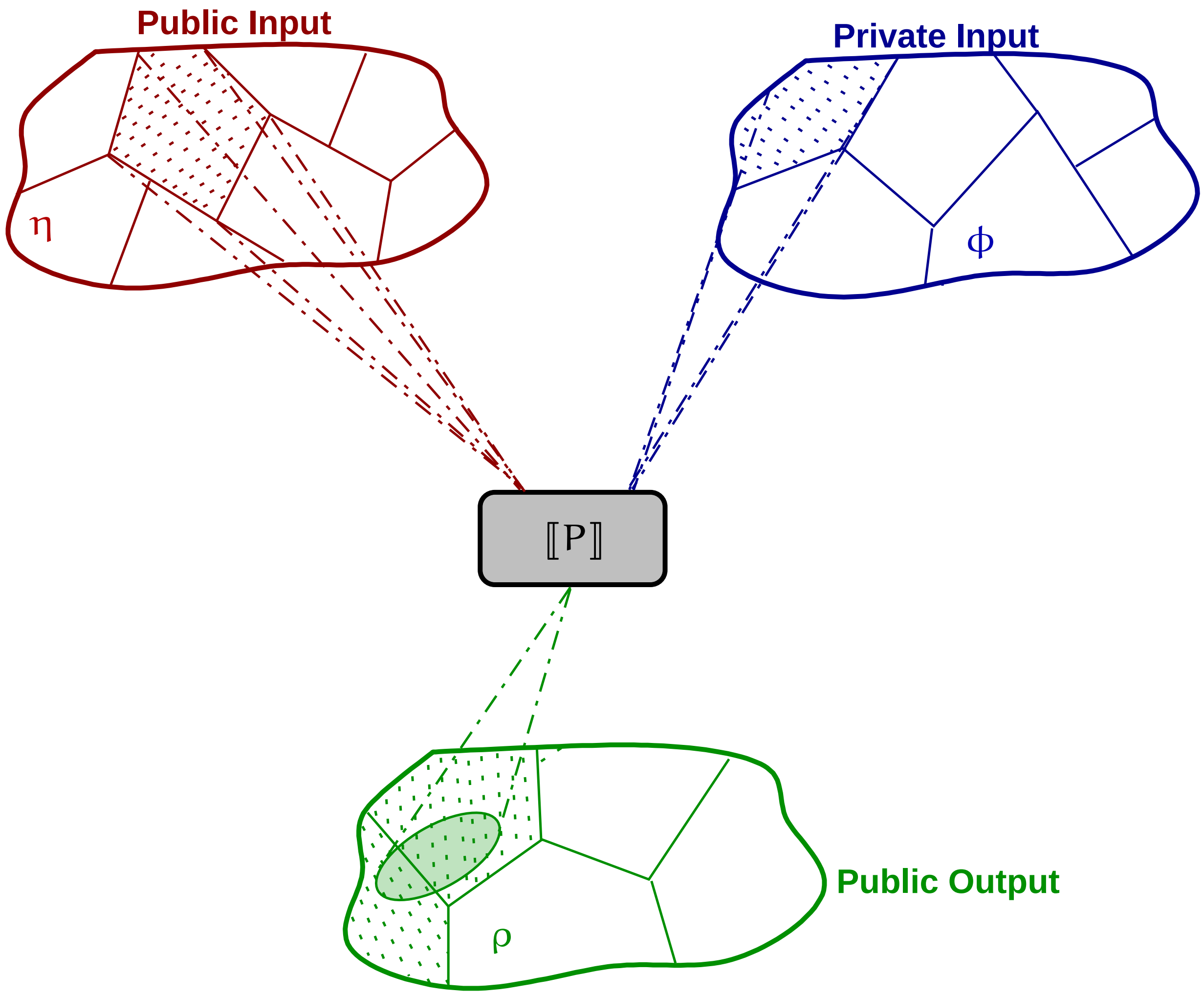
[POPL'04]



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

Abstracting non-interference III: ANI

[POPL'04]

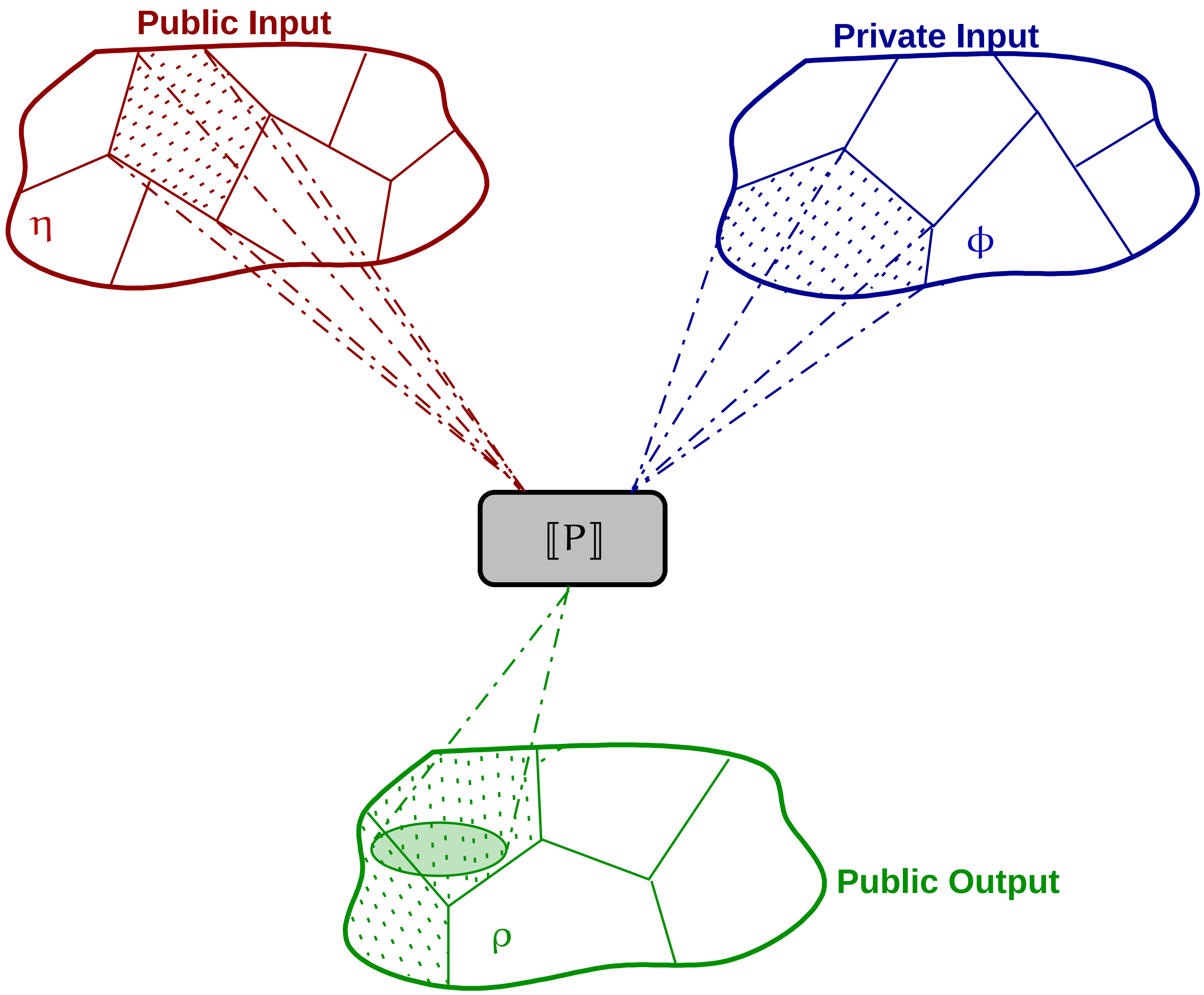


$$\rho, \eta \in Abs(\wp(\mathbb{V}^{L})), \phi \in Abs(\wp(\mathbb{V}^{H})) \colon (\eta)P(\phi \rightsquigarrow\!\!\parallel \rho) \colon$$

$$\eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket P \rrbracket(\phi(h_1), \eta(l_1))^{L}) = \rho(\llbracket P \rrbracket(\phi(h_2), \eta(l_2))^{L})$$

Abstracting non-interference III: ANI

[POPL'04]

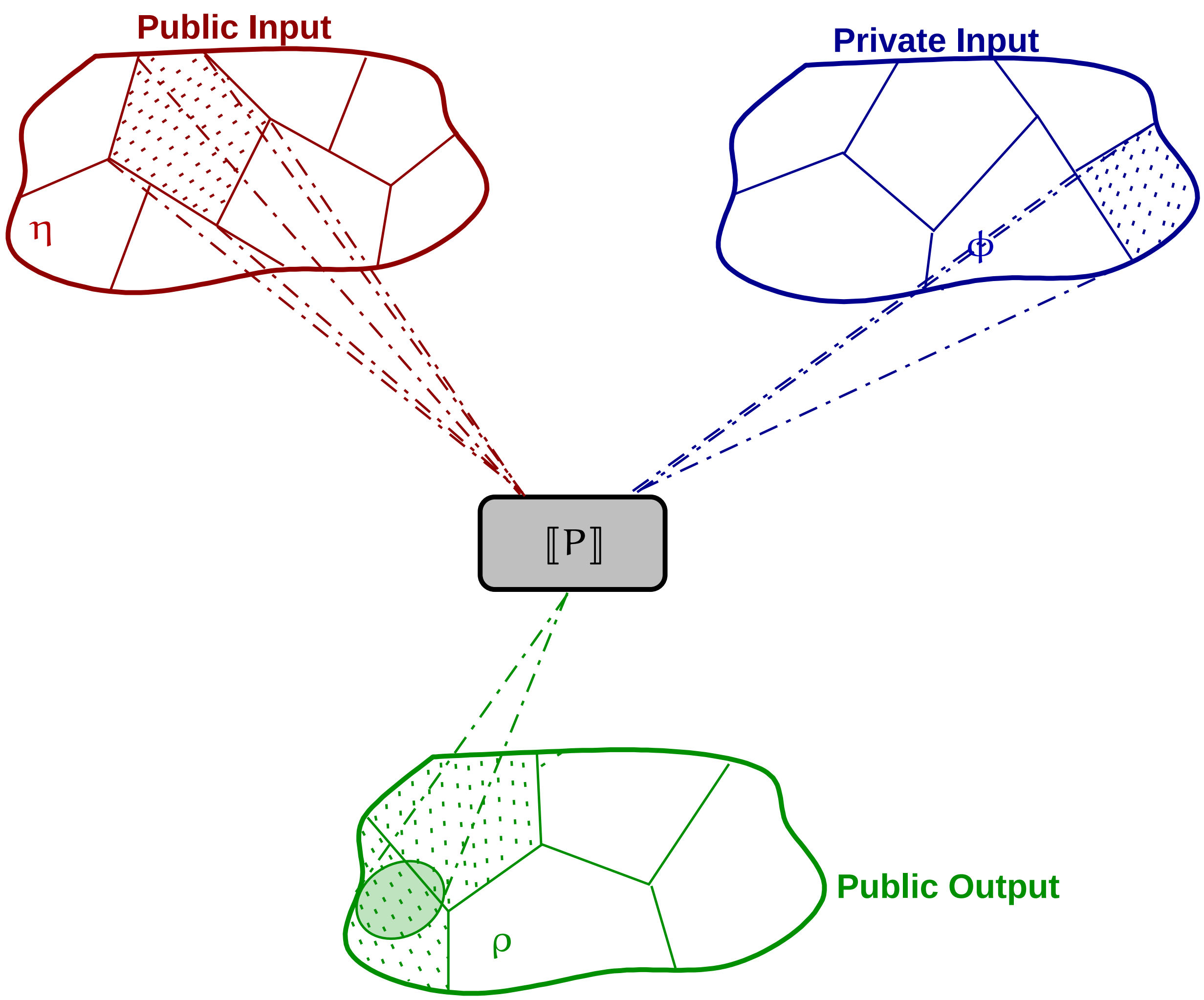


$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{L})), \phi \in \mathit{Abs}(\wp(\mathbb{V}^{H})) \text{: } (\eta)P(\phi \rightsquigarrow\!\!\!\parallel \rho)\text{:}$$

$$\eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket P \rrbracket(\phi(h_1), \eta(l_1))^{L}) = \rho(\llbracket P \rrbracket(\phi(h_2), \eta(l_2))^{L})$$

Abstracting non-interference III: ANI

[POPL'04]



$$\rho, \eta \in \mathit{Abs}(\wp(\mathbb{V}^{L})), \phi \in \mathit{Abs}(\wp(\mathbb{V}^{H})) \colon (\eta)P(\phi \rightsquigarrow\!\!\!] \rho) \colon$$

$$\eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket P \rrbracket(\phi(h_1), \eta(l_1))^{L}) = \rho(\llbracket P \rrbracket(\phi(h_2), \eta(l_2))^{L})$$

Examples

EXAMPLE I:

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

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

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

Examples

EXAMPLE I:

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

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

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

$$\Downarrow$$

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

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

Examples

EXAMPLE II:

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

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

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

Examples

EXAMPLE II:

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

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

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

$$\Downarrow$$

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

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

Examples

EXAMPLE III:

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

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

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

Examples

EXAMPLE III:

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

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

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

$$\Downarrow$$

$$\boxed{(id)P(Sign \leadsto\!\!\!\!\parallel Par)}$$

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

Deriving output attackers

Abstract interpretation provides advanced methods for designing abstractions (refi nement, simplifi cation, compression ...)

Designing abstractions = designing attackers

Deriving output attackers

Abstract interpretation provides advanced methods for designing abstractions (refinement, simplification, compression ...)

Designing abstractions = designing attackers

$$\Downarrow$$

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

  [The most powerful *public observer*]

Deriving canonical attackers

Abstract interpretation provides advanced methods for designing abstractions (refinement, simplification, compression ...)

Transforming abstractions = transforming attackers

Deriving canonical attackers

Abstract interpretation provides advanced methods for designing abstractions (refinement, simplification, compression ...)

Transforming abstractions = transforming attackers

$$\Downarrow$$

- Characterize the most concrete δ such that $(\delta)P(\phi \rightsquigarrow\rrbracket \delta)$

  [The most powerful *canonical* public observer]

$\Rightarrow$ This would provide a certificate for security.

Abstract declassification

Consider a program P and its finite computations.

A passive attacker may be able to learn some information by observing the system but, by assumption, that information leakage is allowed by the security policy.

[Zdancewic and Myers 2001]

Abstract declassification

Consider a program P and its finite computations.

A passive attacker may be able to learn some information by observing the system but, by assumption, that information leakage is allowed by the security policy.
[Zdancewic and Myers 2001]

- We want to characterize the most abstract *private observable* property such that $(\eta)P(\phi \Rightarrow \rho)$

  [The maximal amount of information disclosed]

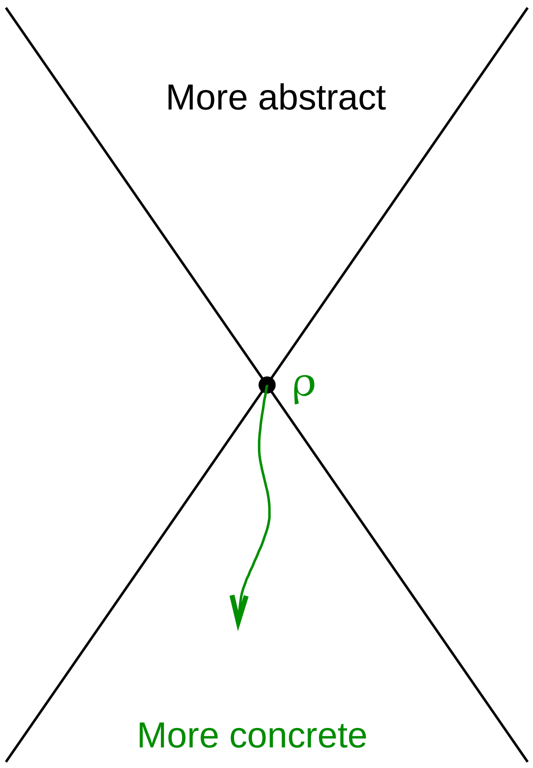
$\Rightarrow$ This would provide a certificate for disclosed secrets.

Observer vs Observable

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

Observer vs Observable

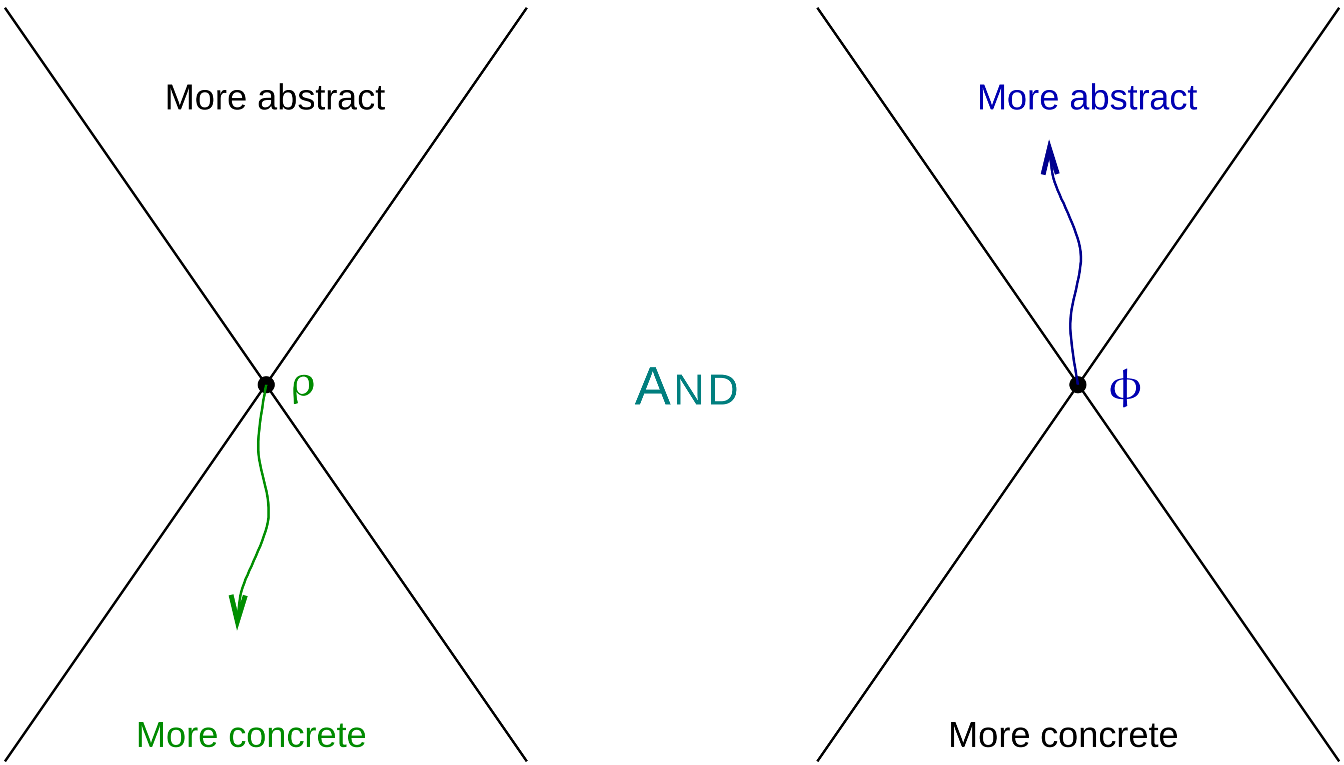
Consider $\models (\eta)P(\phi \rightsquigarrow\!\!]\, \rho)$: *In order to keep non-interference...*



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

Observer vs Observable

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



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

ANI: A completeness problem

Recall that [Joshi & Leino'00]

$$P \text{ is } \textit{secure} \qquad \text{iff} \qquad HH\ ;\ P;\ HH \ \doteq\ P\ ;\ HH$$

ANI: A completeness problem

Recall that [Joshi & Leino'00]

$$\mathrm{P} \text{ is } \textit{secure} \qquad \text{iff} \qquad \mathsf{HH}\ ;\ \mathrm{P};\ \mathsf{HH}\ \doteq\ \mathrm{P}\ ;\ \mathsf{HH}$$

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

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

ANI: A completeness problem

Recall that [Joshi & Leino'00]

$$\mathrm{P} \text{ is } \textit{secure} \qquad \text{iff} \qquad \mathrm{H\,H} \ ; \mathrm{P}; \ \mathrm{H\,H} \ \doteq \ \mathrm{P} \ ; \ \mathrm{H\,H}$$

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

$$\mathrm{H\,H} \ ; \ \mathrm{P}; \ \mathrm{H\,H} \quad \doteq \quad \mathrm{P} \ ; \ \mathrm{H\,H}$$

$$\Downarrow$$

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

$$\boxed{\Rightarrow \text{A COMPLETENESS PROBLEM}}$$

ANI: A completeness problem

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

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

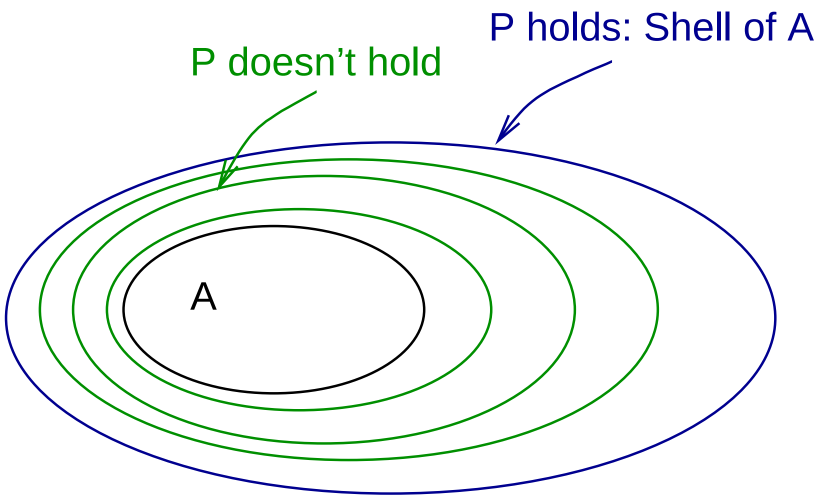
$$\boxed{\text{COMPLETENESS = NON-INTERFERENCE}}$$

$$\Downarrow$$

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

Completeness shells and cores

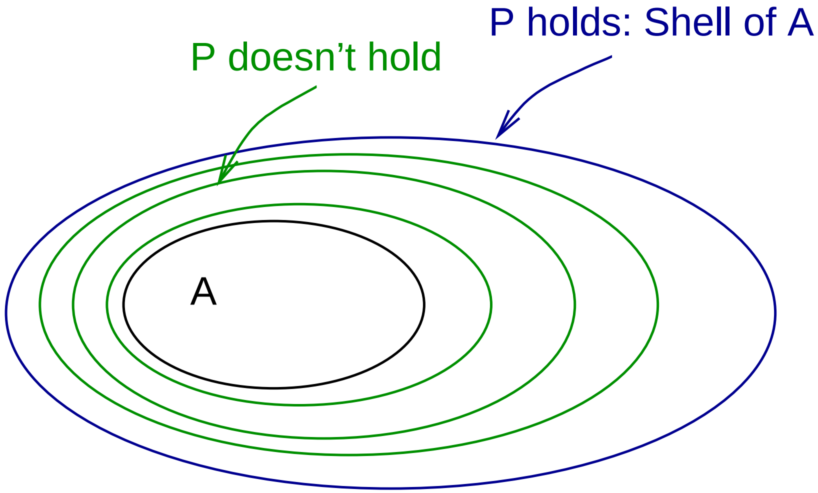
[Giacobazzi et al.'00]



$$R_f \stackrel{\text{def}}{=} \lambda \rho . \mathcal{M}\left(\bigcup_{y \in \rho} max(f^{-1}(\downarrow y)) \right)$$

Completeness shells and cores

[Giacobazzi et al.'00]

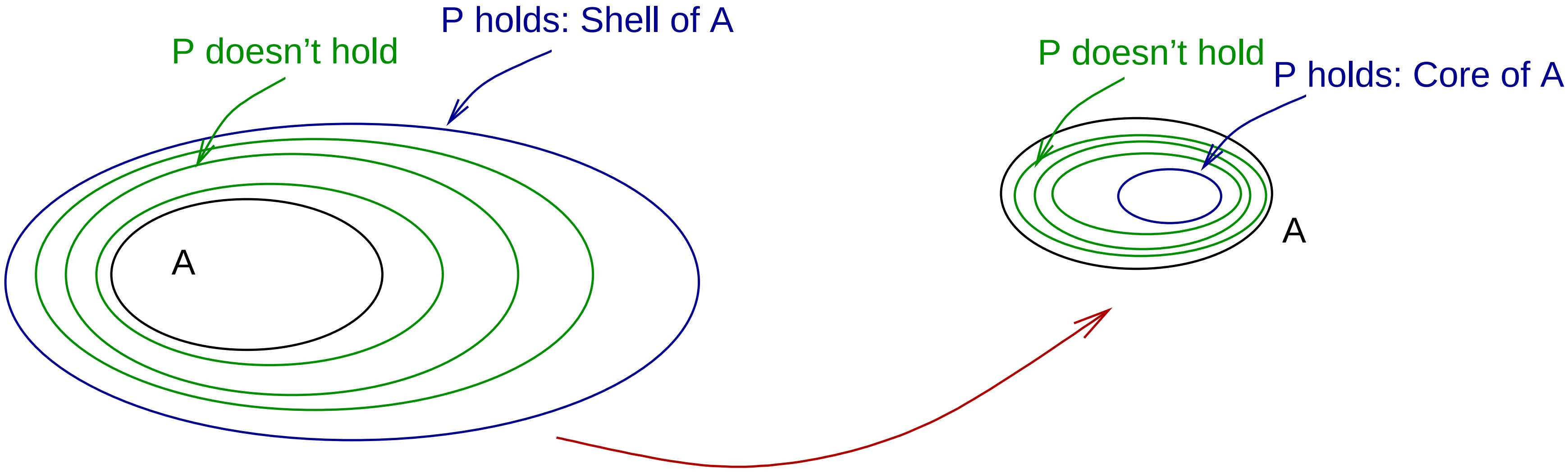


$$R_f \stackrel{\text{def}}{=} \lambda\rho.\mathcal{M}\Big(\bigcup_{y\in\rho} \mathit{max}(f^{-1}(\downarrow y))\Big)$$

- *Absolute shell* of ρ: $\mathcal{R}_f(\rho) = \mathit{gfp}^{\sqsubseteq}_{\rho}\lambda\varphi.\rho \sqcap R_f^{\mathcal{B}}(\varphi)$;
- *Relative shell* of η *relative to* ρ: $\mathcal{R}_f^{\rho}(\eta) = \eta \sqcap R_f(\rho)$.

Completeness shells and cores

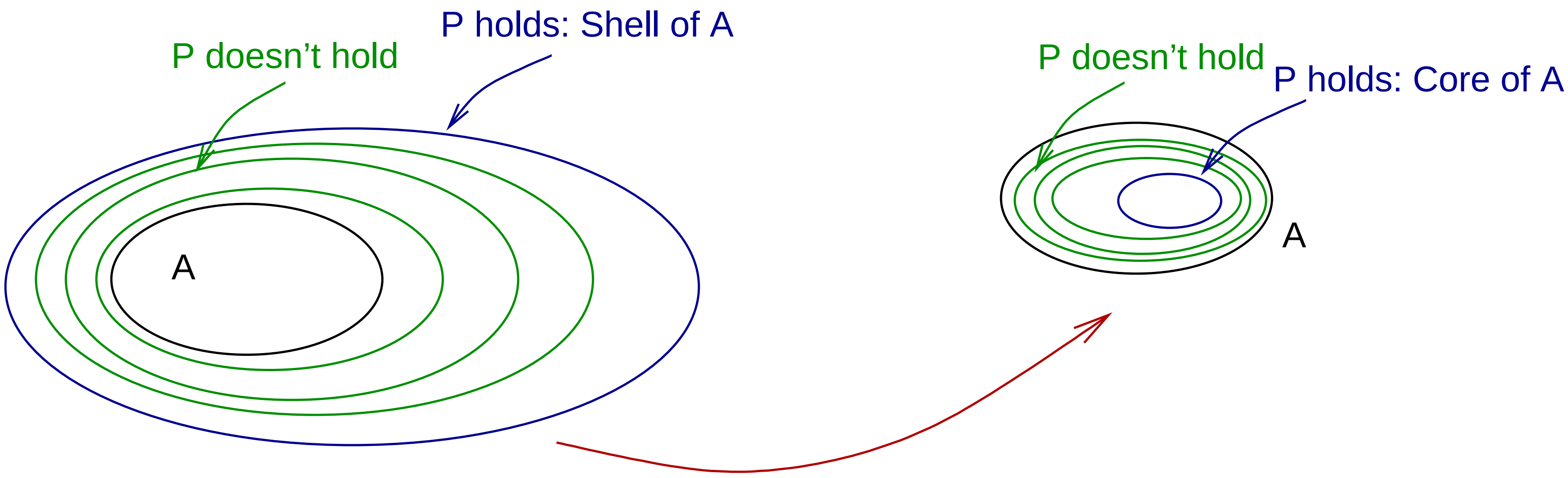
[Giacobazzi et al.'00]



$$C_f \stackrel{\text{def}}{=} \lambda\rho.\left\{ y \in C \;\middle|\; \mathit{max}(f^{-1}(\downarrow y)) \subseteq \rho \right\}$$

Completeness shells and cores

[Giacobazzi et al.'00]



$$C_f \stackrel{\text{def}}{=} \lambda\rho.\left\{\, y \in C \;\middle|\; \mathit{max}(f^{-1}(\downarrow y)) \subseteq \rho \,\right\}$$

- *Absolute core* of ρ: $\mathcal{C}_f(\rho) = \mathit{lfp}^{\sqsubseteq}_{\rho}\lambda\varphi.\rho \sqcup C_f^{\mathcal{B}}(\varphi)$;
- *Relative core* of ρ *relative to* η: $\mathcal{C}_f^{\eta}(\rho) = \rho \sqcup C_f(\eta)$.

ANI as completeness

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

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

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

ANI as completeness

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

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

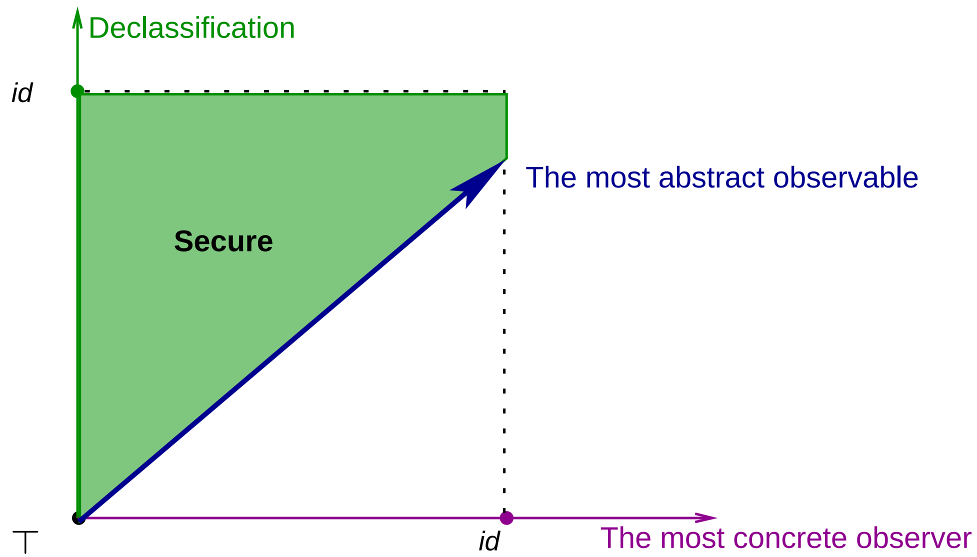
$$\Downarrow$$

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

ANI as completeness

- PUBLIC OBSERVER AS COMPLETENESS CORE: $\mathcal{C}^{\mathcal{H}_\eta}_{[\![P]\!]^\eta,\phi}(\mathcal{H}) = (\eta)[\![P]\!](\phi \rightsquigarrow\!\!\| id)$
- PRIVATE OBSERVABLE AS COMPLETENESS SHELL: $(\eta)P(\mathcal{R}^{\mathcal{H}_\rho}_{[\![P]\!]^\eta,id}(\mathcal{H}_\eta) \Rightarrow \rho)$
- ADJOINING ATTACKERS AND DECLASSIFICATION

$$id \sqsubseteq (\eta)[\![P]\!](id \rightsquigarrow\!\!\| id) \Leftrightarrow \mathcal{P}(\sqcap_{L\in\eta}\mathcal{M}(\Pi_P(\eta, id)_{|L})) \sqsubseteq \top$$



A discussion

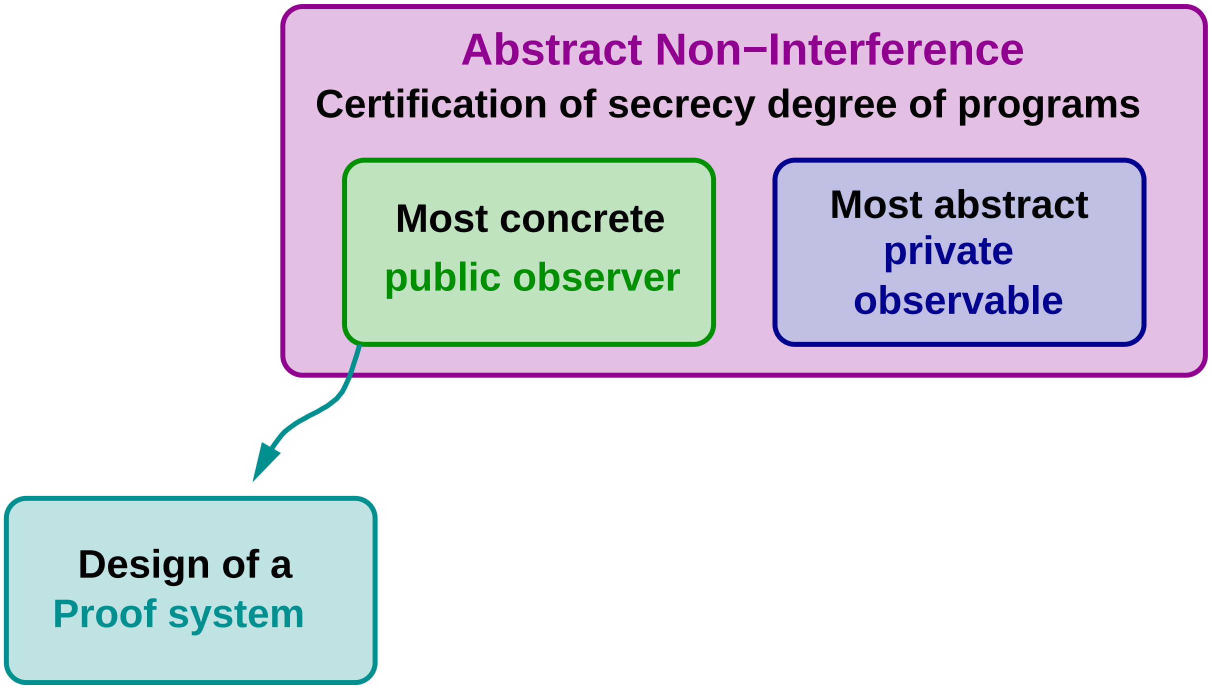
Abstract Non−Interference

Certification of secrecy degree of programs

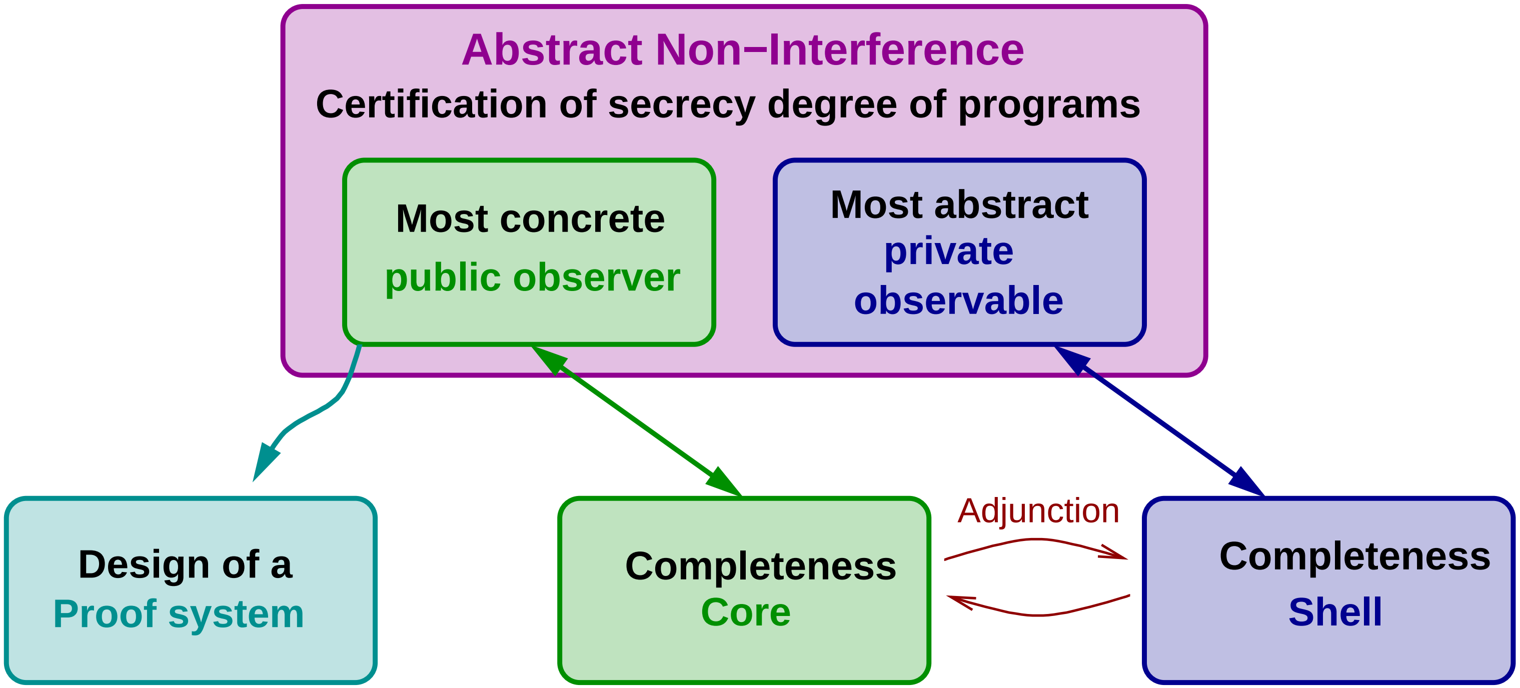
Most concrete
public observer

Most abstract
private observable

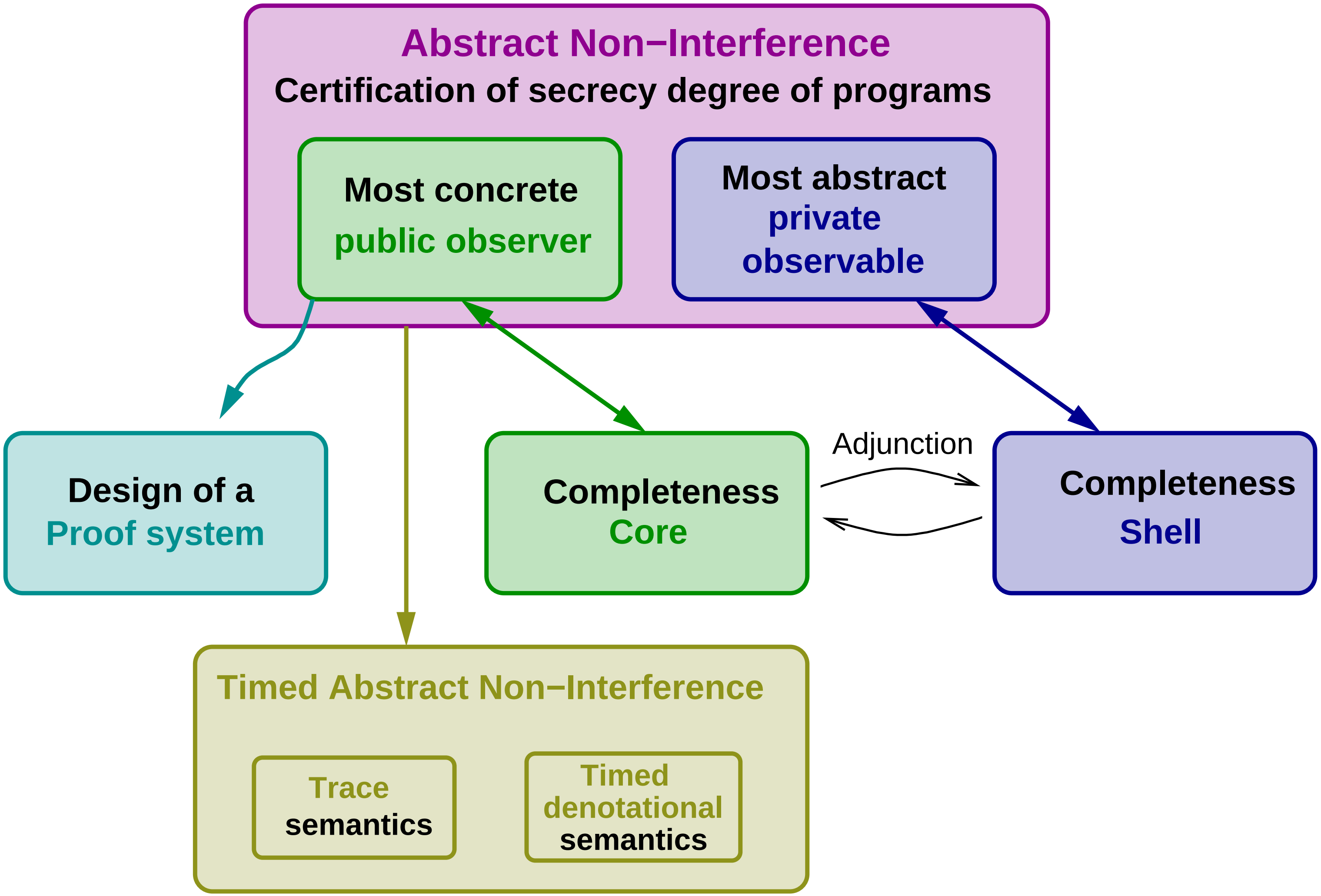
A discussion



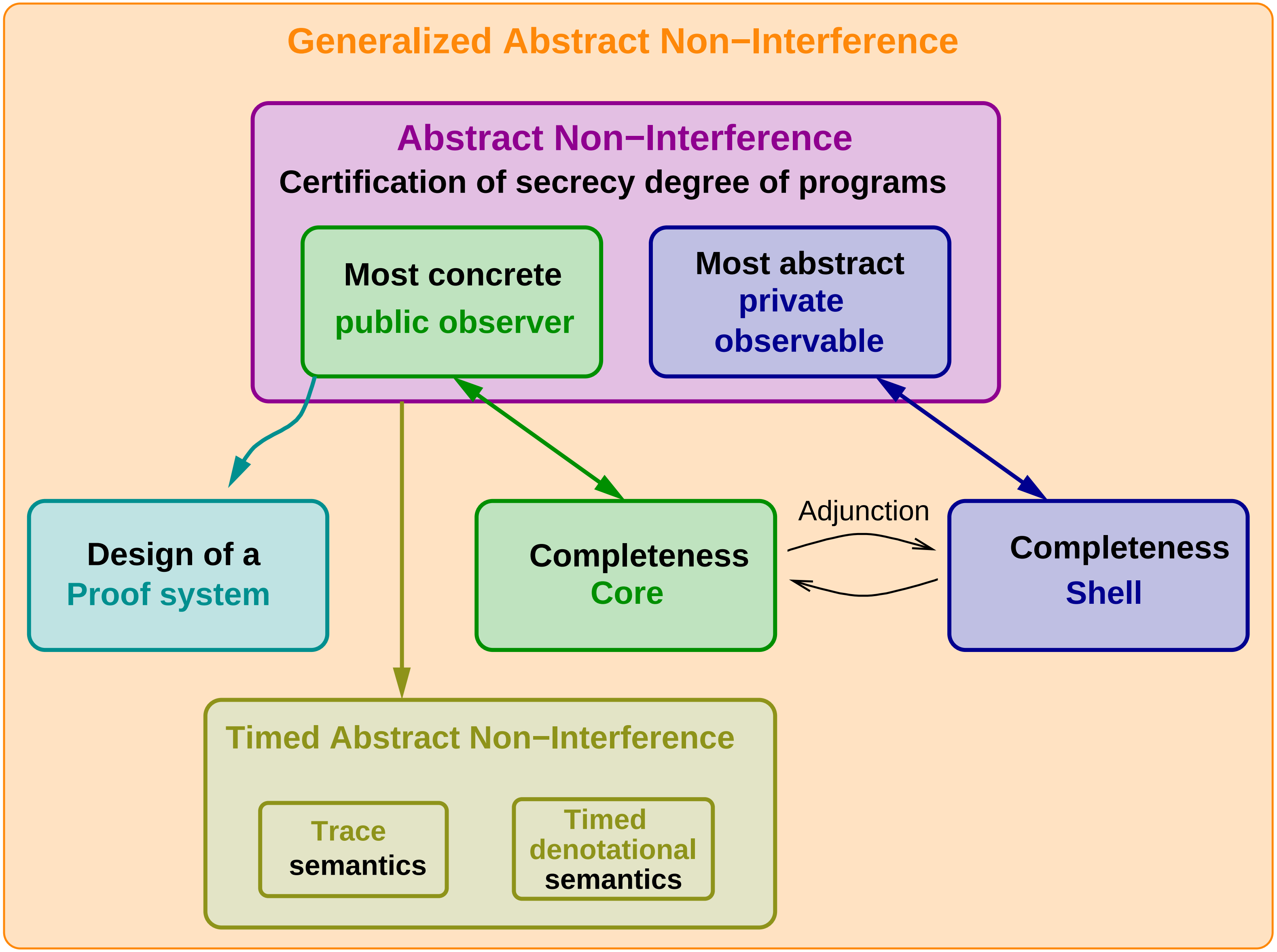
A discussion



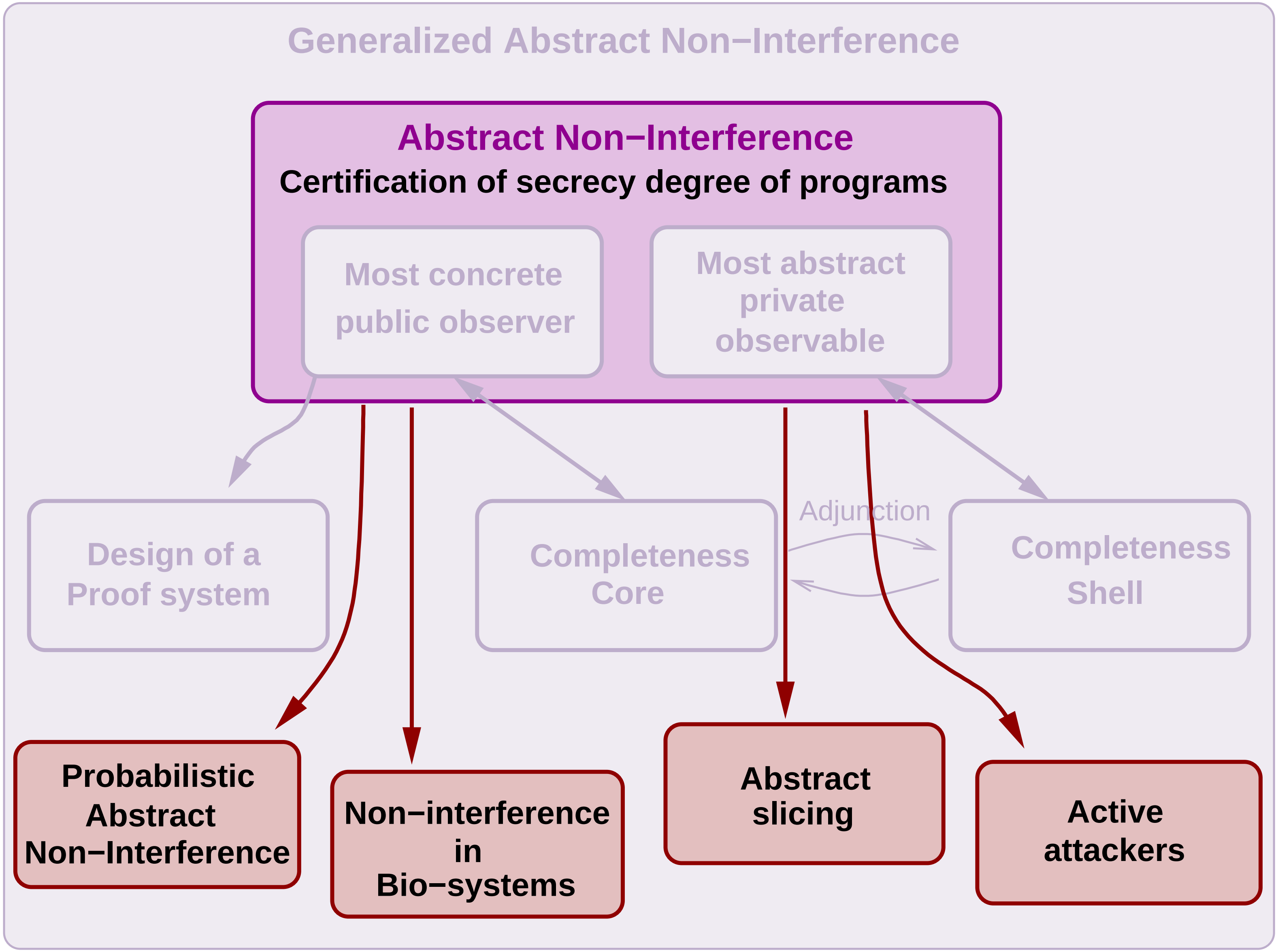
A discussion



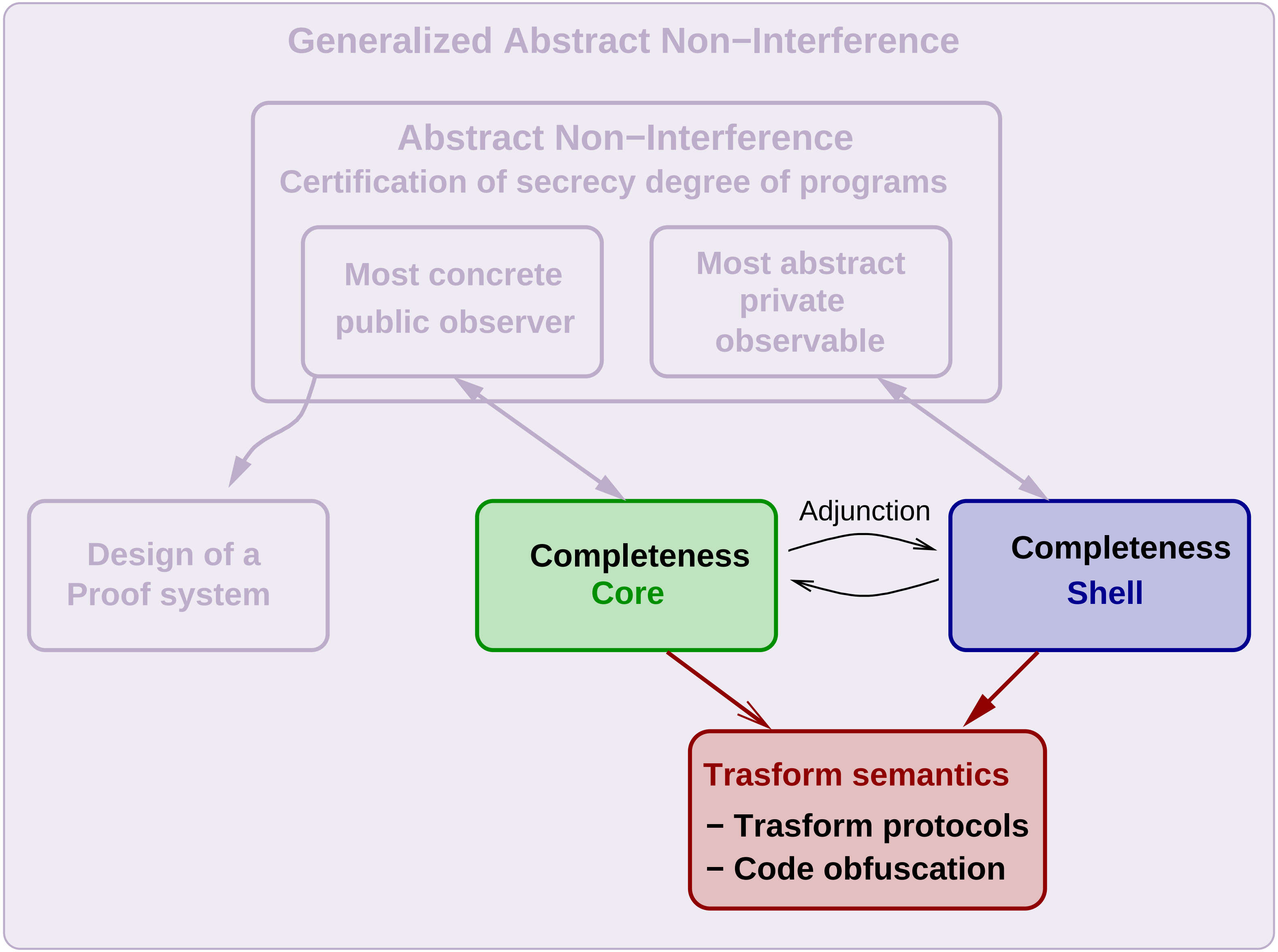
A discussion



A discussion: Future works



A discussion: Future works



A discussion: Future works