A Coq Formalization of Lagois Connections for Secure Information Flow

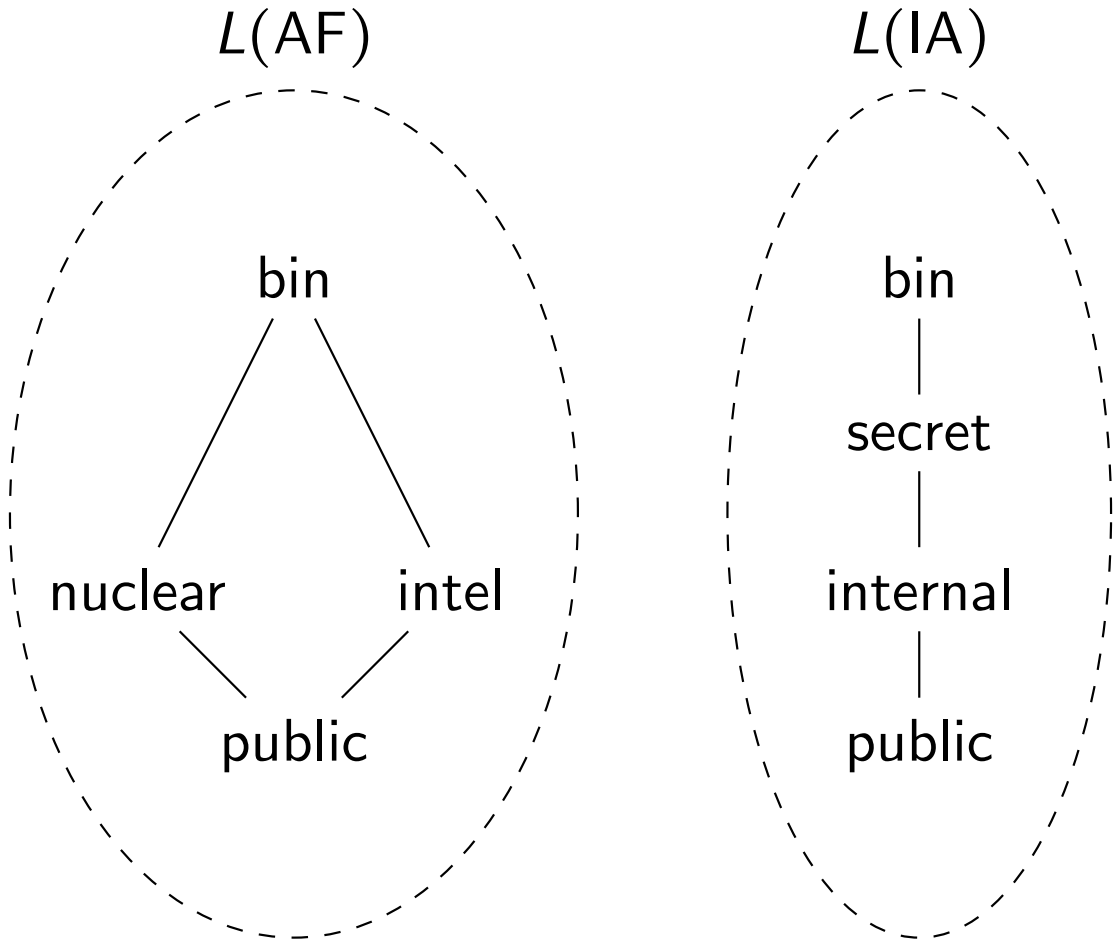
Casper Ståhl Levs Gondelmans René Rydhof Hansen
Danny Bøgsted Poulsen

Aalborg University, Aalborg, Denmark
cstahl20@student.aau.dk, {lego,rrh,dannybpoulsen}@cs.aau.dk

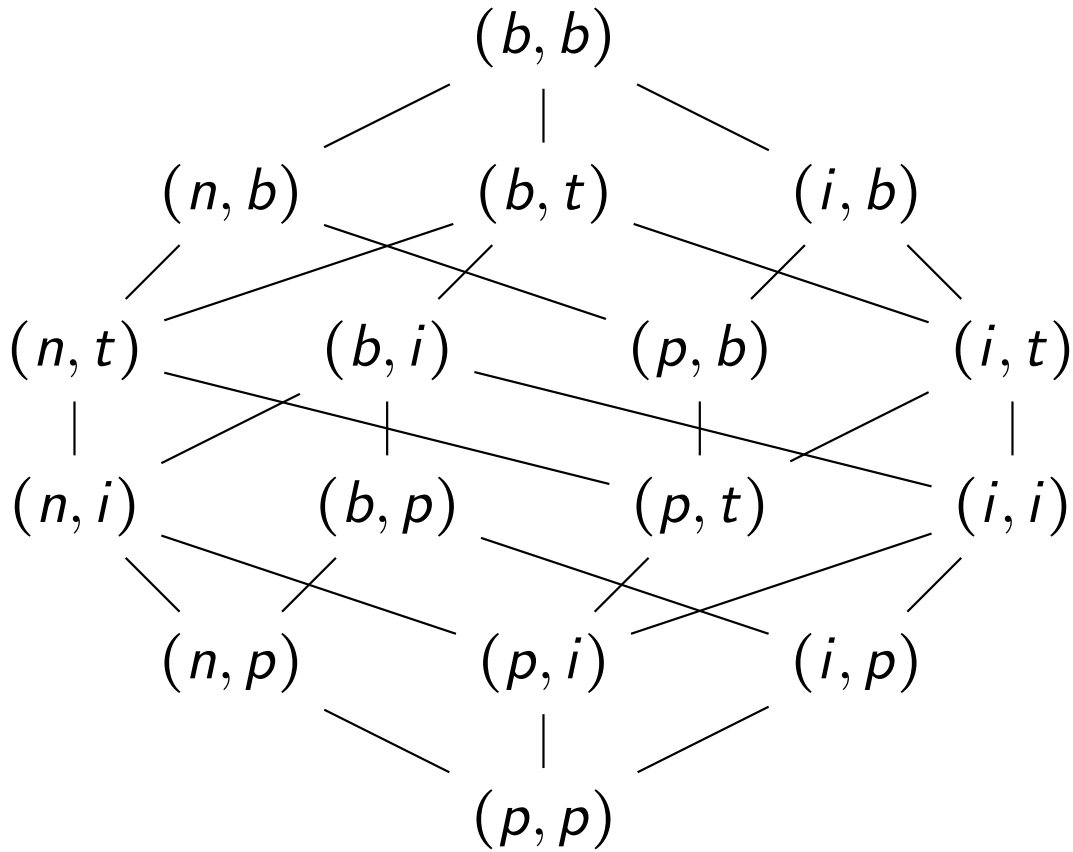
June 7, 2025

- Lagois connections for secure information flow due to Bhardwaj and Prasad [1, 2]
- Fully formalised results are not marked
- Unformalised results are marked like this*

The Problem

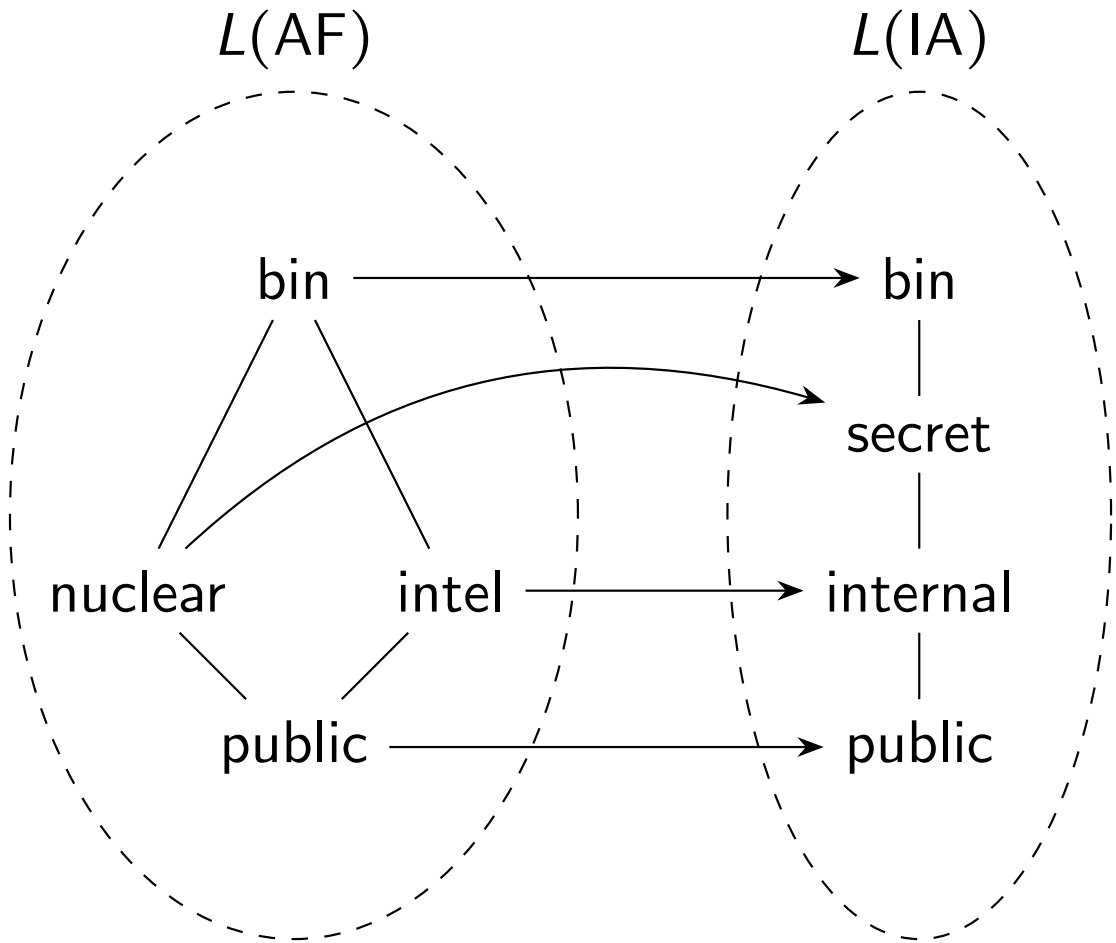

L(AF)
bin
nuclear
intel
public
L(IA)
bin
secret
internal
public

The Conventional Solution

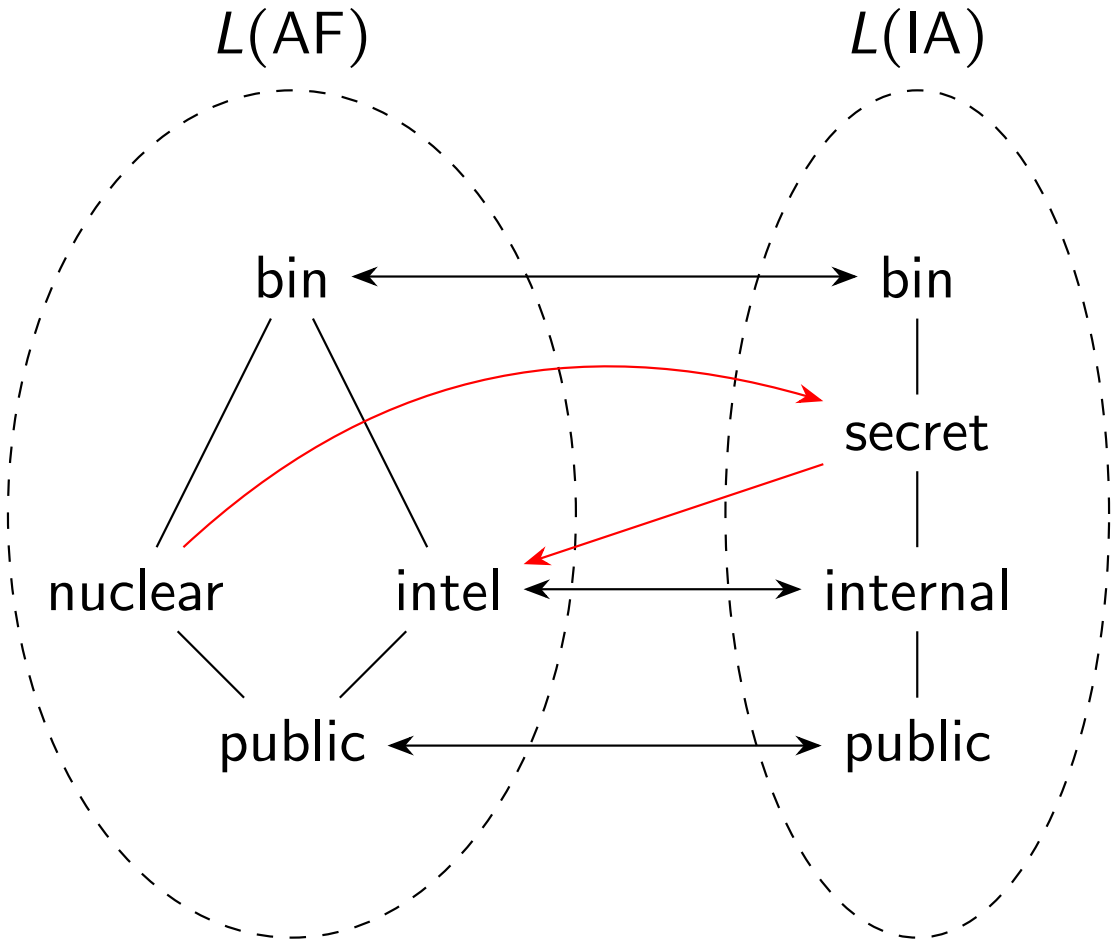


This Solution

- $p \leq p' \rightarrow f(p) \leq f(p')$ for all $p\ p' : P$

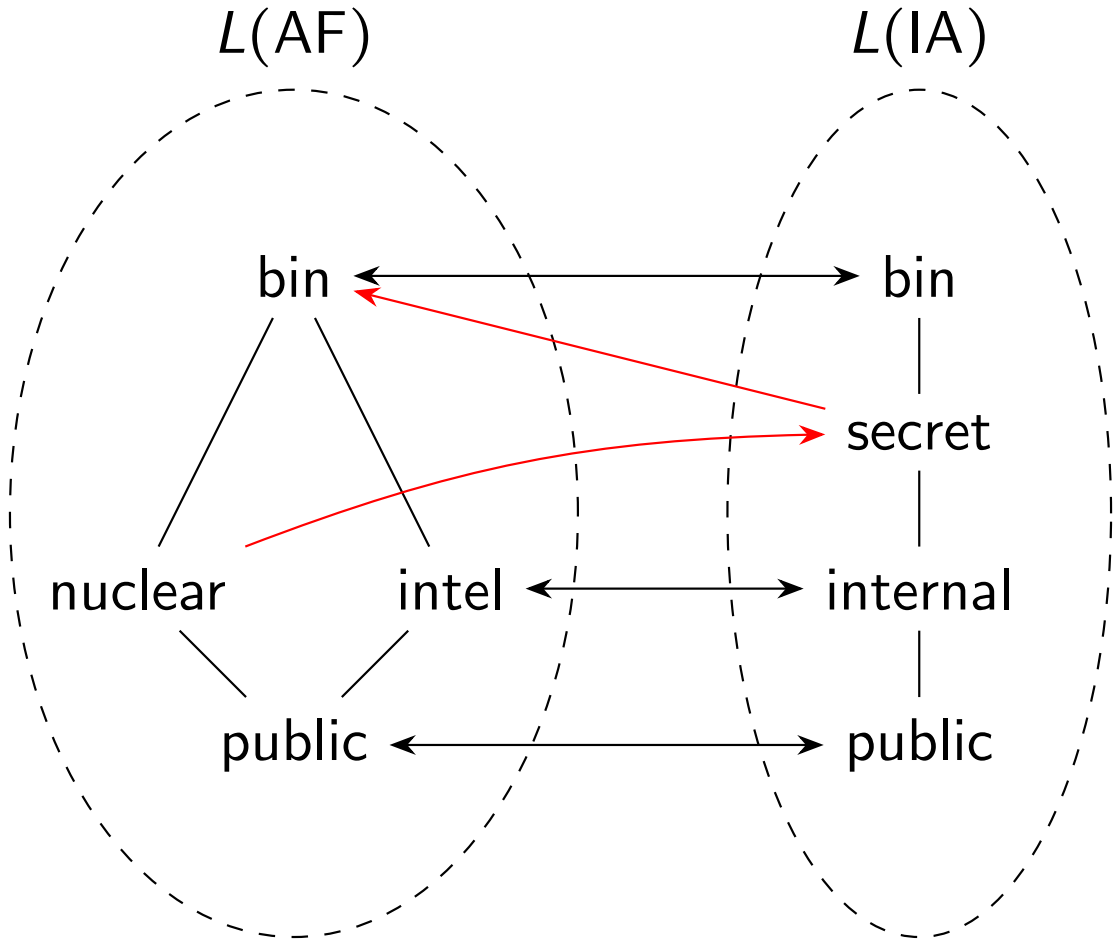


A new Problem



Security

- $p \leq (g \circ f)(p)$ for all $p : P$ (**LC1**)
- $q \leq (f \circ g)(q)$ for all $q : Q$ (**LC2**)



Galois Insertion $\prec$ Lagois Connection

Definition (Lagois connection [3])

A *poset system* (P, f, g, Q) is a *Lagois connection* whenever

- $p \leq (g \circ f)(p)$ for all $p : P$ (**LC1**)
- $q \leq (f \circ g)(q)$ for all $q : Q$ (**LC2**)
- $(f \circ g \circ f)(p) = f(p)$ for all $p : P$ (**LC3**)
- $(g \circ f \circ g)(q) = g(q)$ for all $q : Q$ (**LC4**)

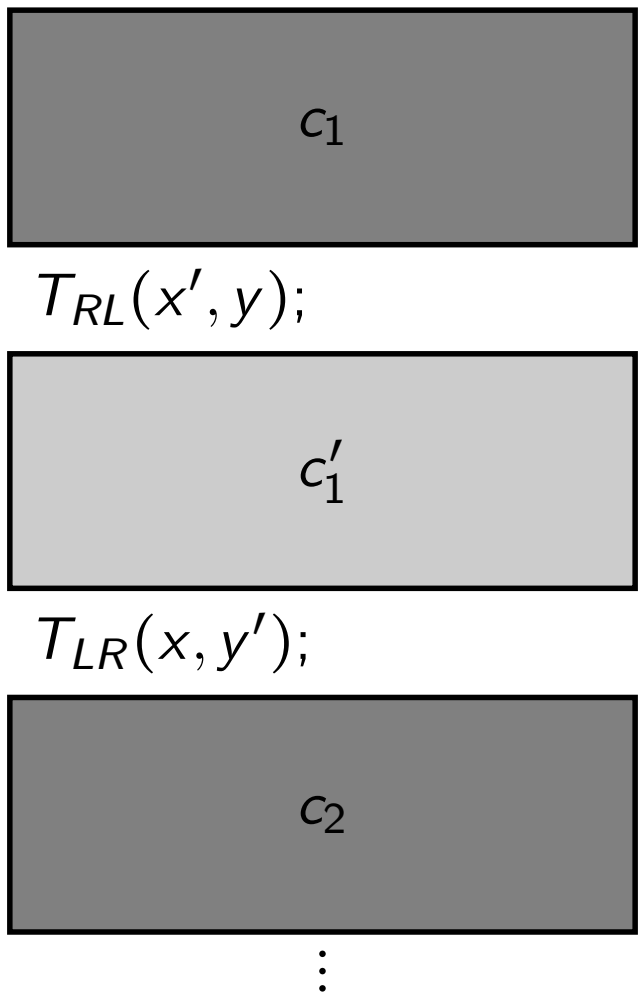
Definition* (Galois insertion)

A poset system (P, f, g, Q) *is a Galios insertion whenever*

- $p \leq (g \circ f)(p)$ *for all* $p : P$
- $q = (f \circ g)(q)$ *for all* $q : Q$

Operational Model

- $p ::= T_{RL}(x', y) \mid T_{LR}(x, y') \mid c \mid c' \quad$ where $c : C$ and $c' : C'$
- $s ::= \varepsilon \mid s; p$
- $(\nu, \mu) \vdash s \Rightarrow (\nu_f, \mu_f)$ where $\nu\ \nu_f\ \mu\ \mu_f : \mathrm{Var} \to \mathbb{N}$



Type System

- (P, f, g, Q) is a Lagois connection
- $\lambda : \mathrm{Var} \to P$ and $\lambda' : \mathrm{Var} \to Q$
- $(\lambda, \lambda') \vdash s : (p, q)$

$$\frac{f(\lambda(x)) \leq \lambda'(y')}{(\lambda, \lambda') \vdash T_{LR}(y', x) : (\lambda(y), \lambda'(x'))}$$

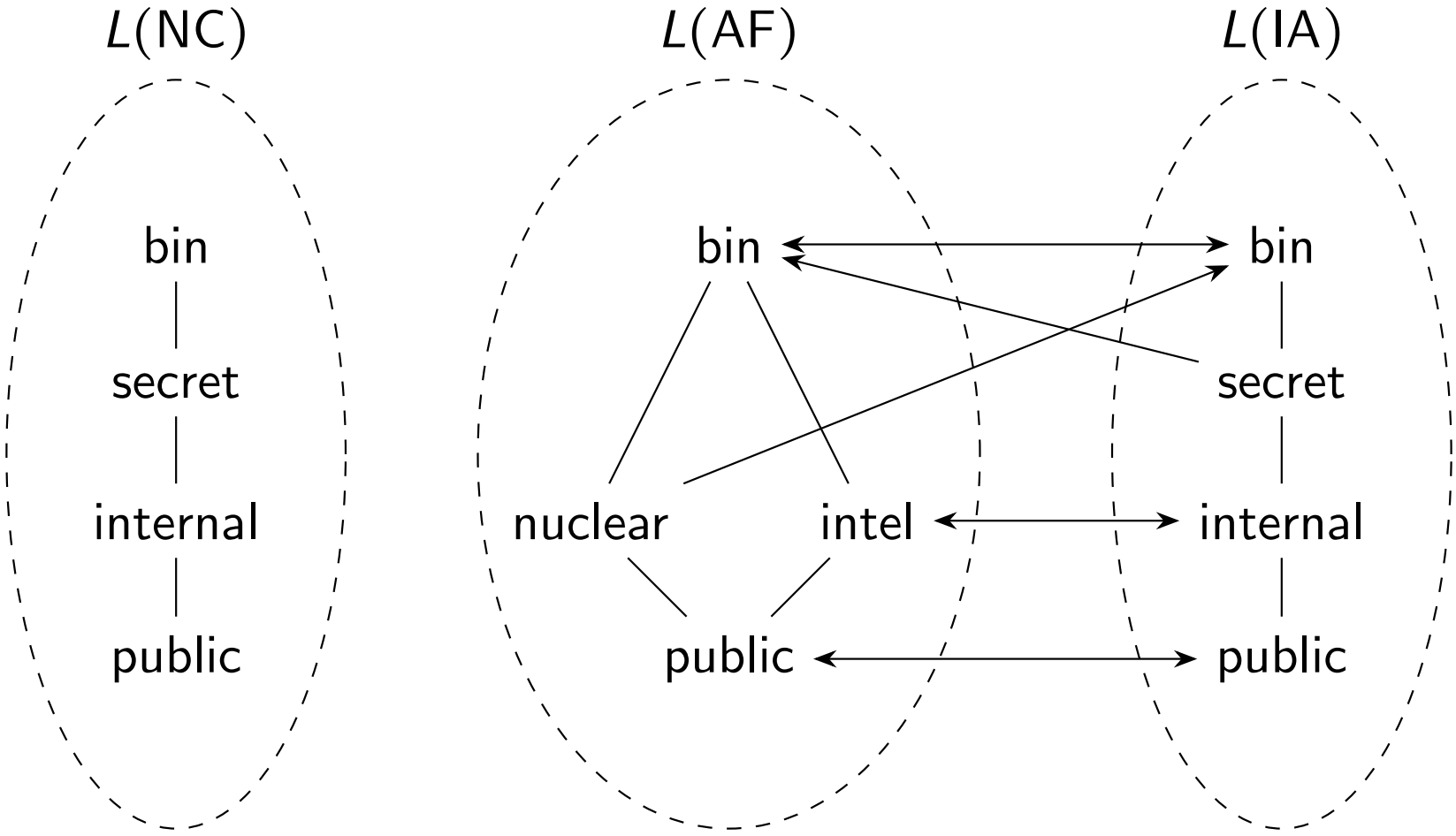
Theorem (Soundness w.r.t. noninterference [1, 2])

For an adversarial residing at level $p : P$ and $q : Q$ such that $p = g(q)$ and $q = f(p)$. If for a program s, memories μ, μ_f, μ', μ'_f and ν, ν_f, ν', ν'_f it is the case that

- $(\lambda, \lambda') \vdash s : (p', q')$
- $(\nu, \mu) \vdash s \Rightarrow (\nu_f, \mu_f)$,
- $(\nu', \mu') \vdash s \Rightarrow (\nu'_f, \mu'_f)$, *and*
- $\nu(v) = \nu'(v)$ *for all* $v : \mathsf{Var}$ *such that* $\lambda(v) \leq p$ *(analogous for* μ, μ' *and* q*)*

then $\nu_f(v) = \nu'_f(v)$ *for all* $v : \mathsf{Var}$ *such that* $\lambda(v) \leq p$ *(analogous for* μ_f, μ'_f *and* q*)*

A new Problem



Chaining

Theorem* (Melton et al. [3])

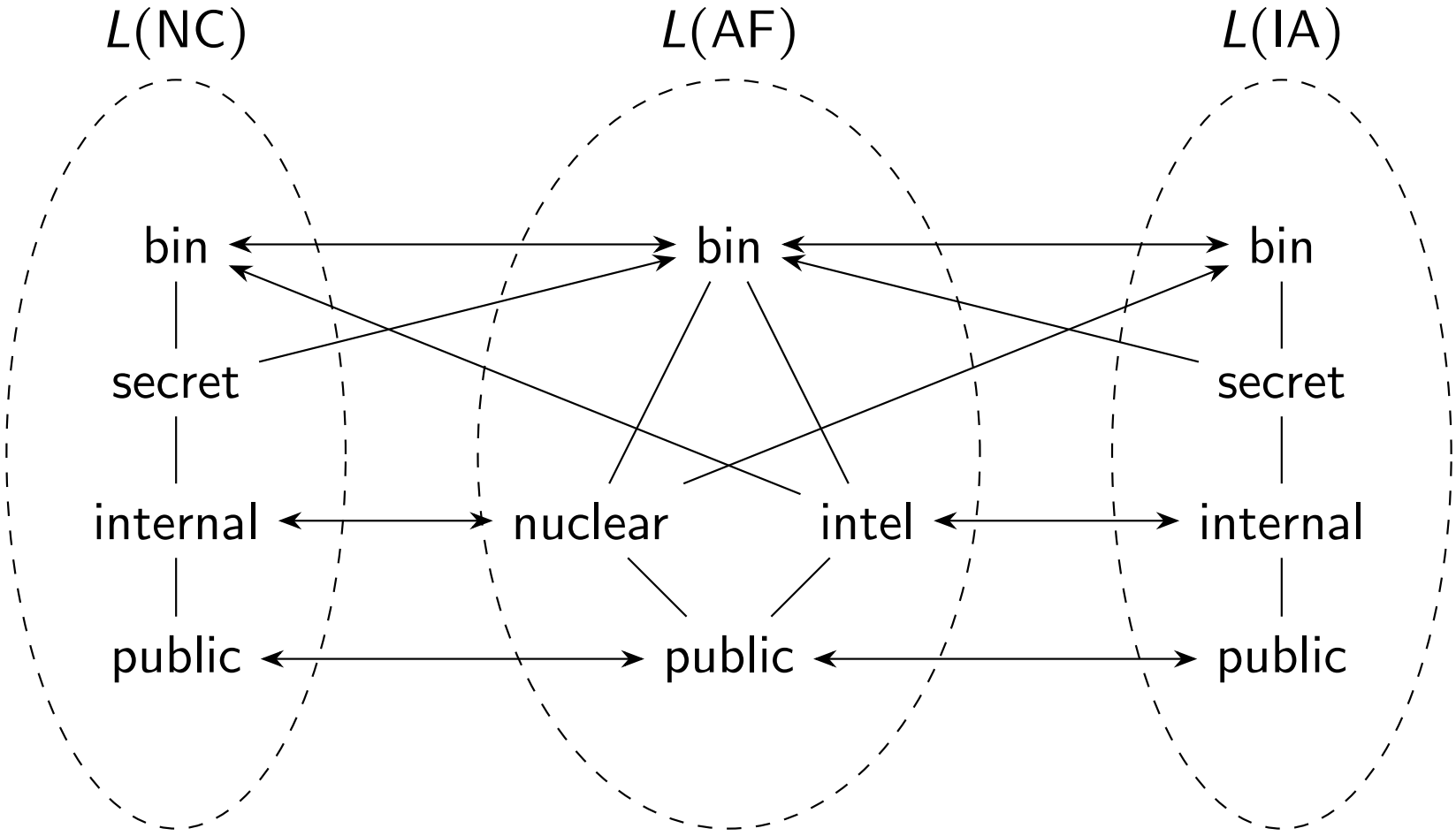
Let (P, f, g, Q) *and* $(Q, \hat{f}, \hat{g}, R)$ *be Lagois connections. Then* $(P, \hat{f} \circ f, \hat{g} \circ g, R)$ *is a Lagois connection iff*

$$(\hat{g} \circ \hat{f} \circ f)[P] \subseteq f[P] \text{ and } (f \circ g \circ \hat{g})[R] \subseteq \hat{g}[R].$$

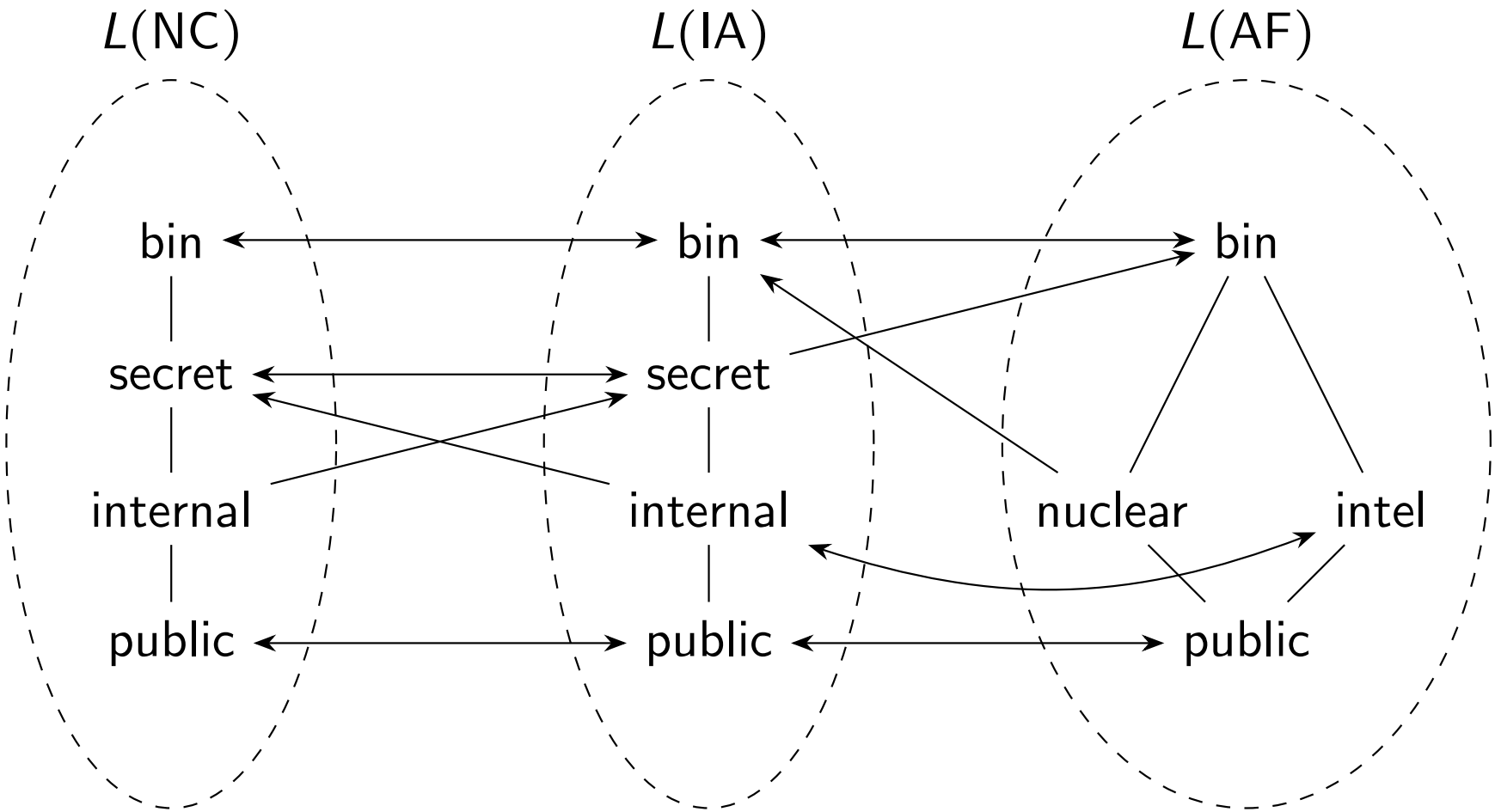
Proposition*

If (P, f, g, Q) *and* $(Q, \hat{f}, \hat{g}, R)$ *both satify* **LC1** *and* **LC2** *then* $(P, \hat{f} \circ f, g \circ \hat{g}, R)$ *satifies* **LC1** *and* **LC2**.

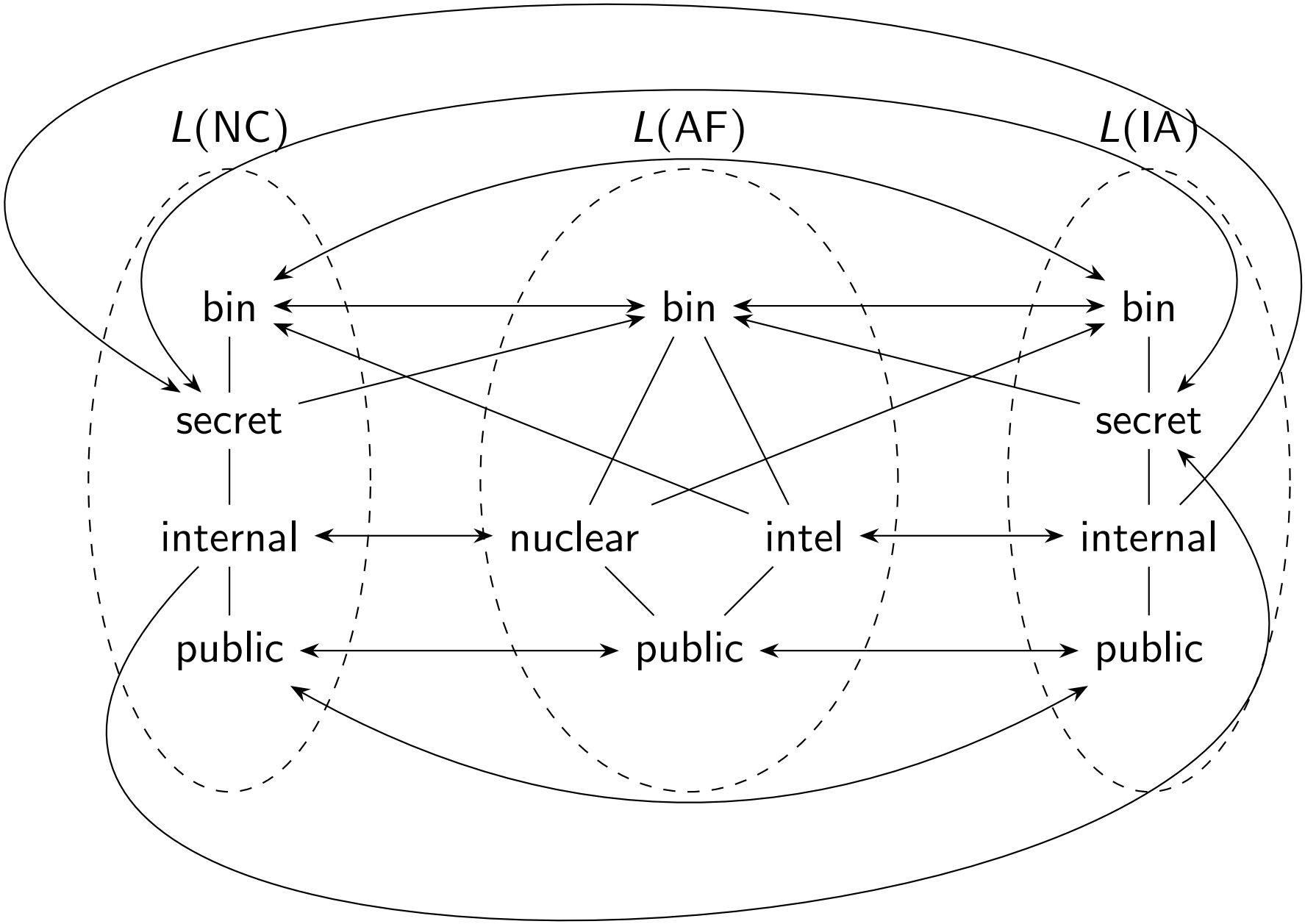
Chaining (a new problem!)



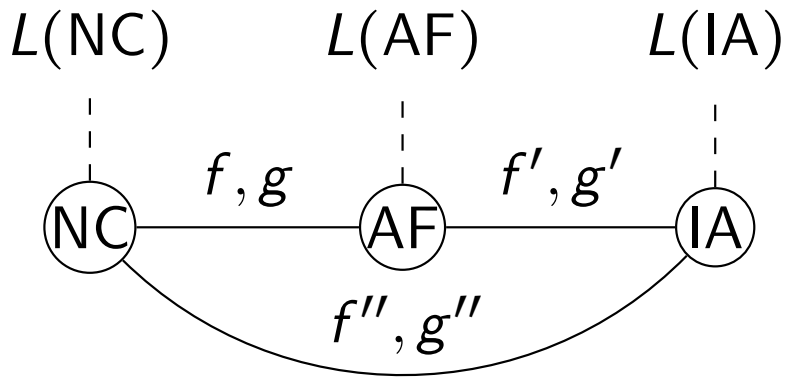
Chaining (a new problem!)



Solution

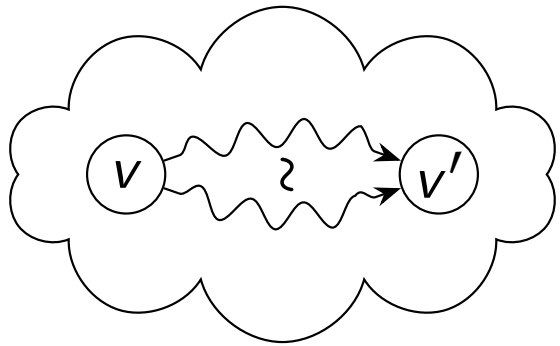

L(NC)
L(AF)
L(IA)
bin
bin
bin
secret
secret
internal
nuclear
intel
internal
public
public
public

Solution

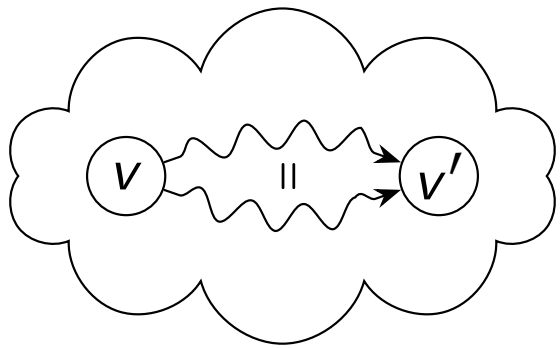


Secure Networks

- Security of a network can be determined in cubic time* [4].
- Secure if for all pairs of verticies all simple paths behave the same.

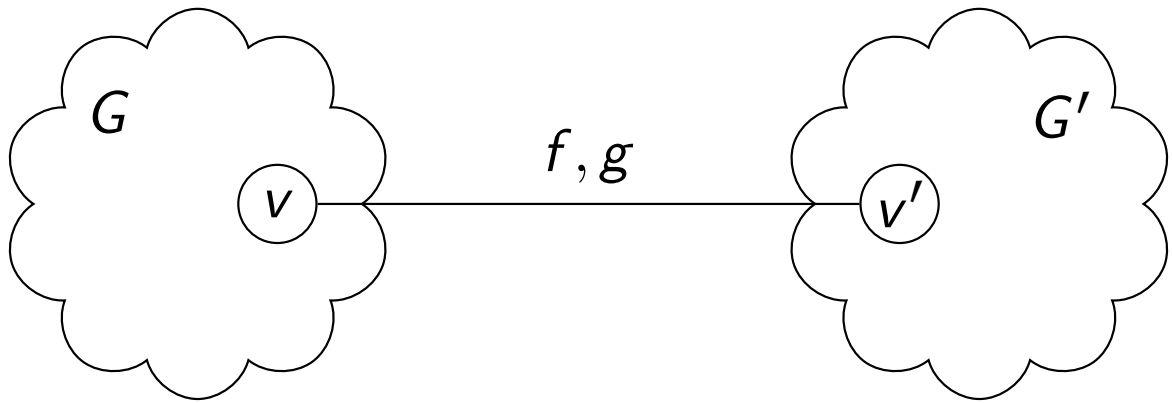


- Secure if for all pairs of verticies there is at most one simple path between (forest).



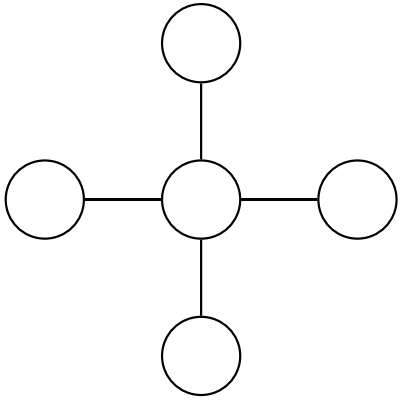
Composition

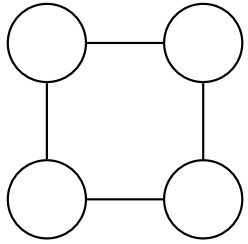
For graphs G, G', vertices $v : G$ and $v' : G'$ and a Lagois connection $(L(v), f, g, L(v')$ let $G \overset{f}{v} \rightleftharpoons \overset{v'}{g} G'$ be the graph depicted below:

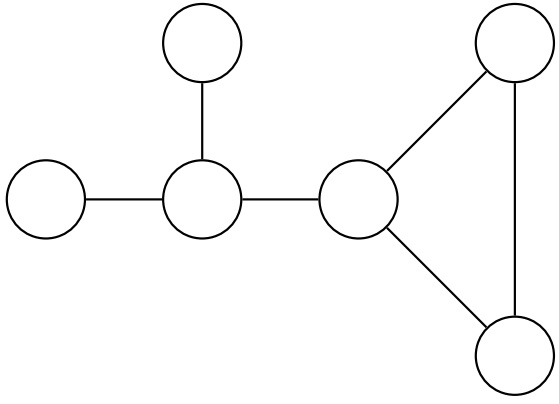


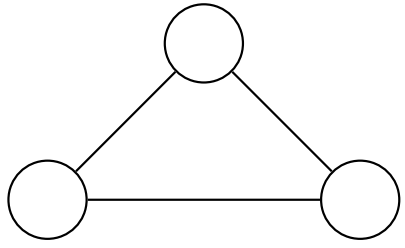
Theorem*

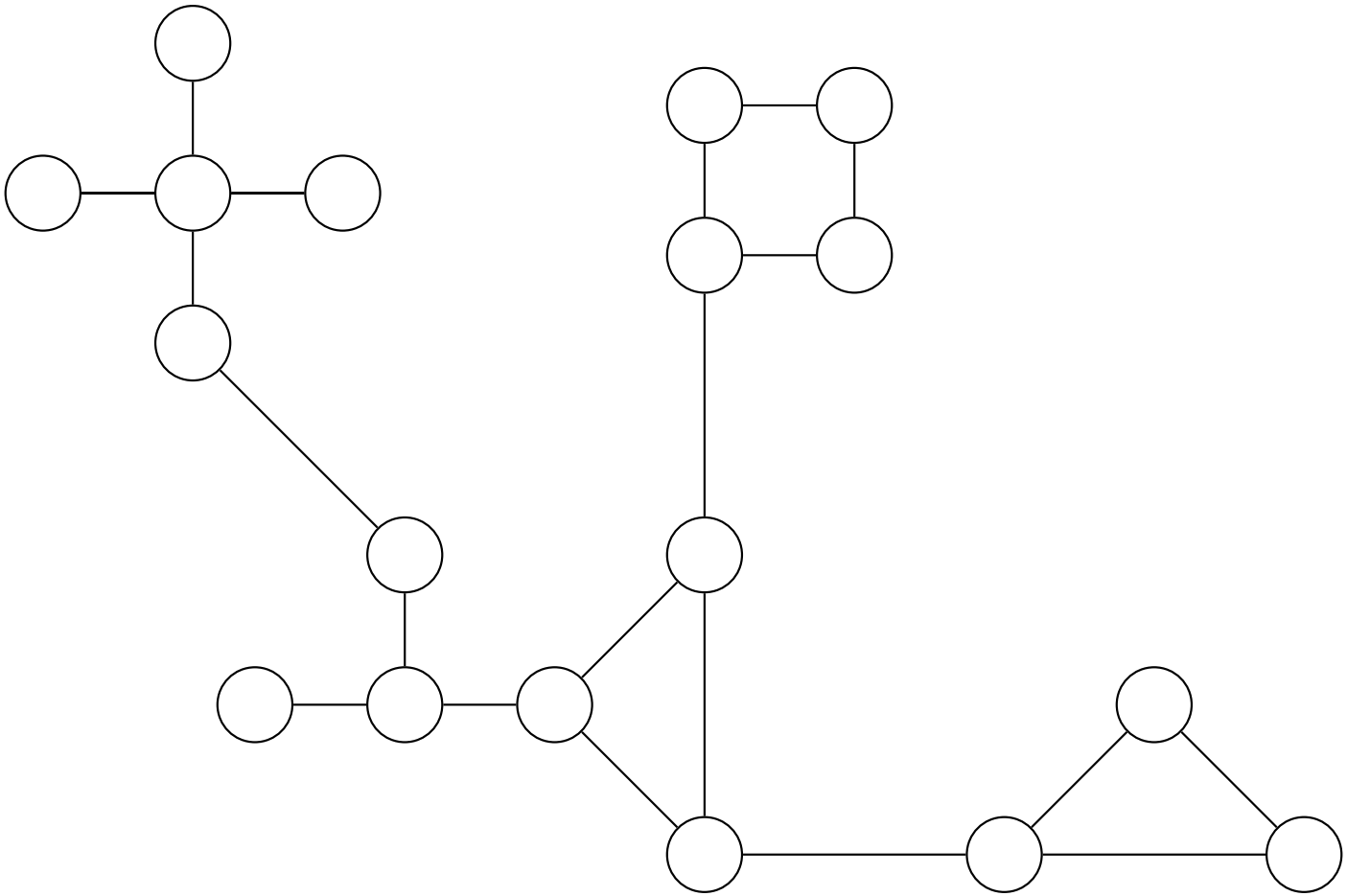
If G and G' are secure graphs then for all $v : G$, $v' : G$ and f, g such that $(L(v), f, g, L(v'))$ is a Lagois connection it is the case that $G \overset{f}{v} \rightleftharpoons \overset{v'}{g} G'$ is secure.











Conclusion

- Soundness proof (w.r.t. noninterference)
- Dynamism of organisations and policies

References I

[1] Chandrika Bhardwaj and Sanjiva Prasad. "Only connect, securely". In: *Formal Techniques for Distributed Objects, Components, and Systems: 39th IFIP WG 6.1 International Conference, FORTE 2019, Held as Part of the 14th International Federated Conference on Distributed Computing Techniques, DisCoTec 2019, Kongens Lyngby, Denmark, June 17–21, 2019, Proceedings 39*. Springer. 2019, pp. 75–92.

[2] Chandrika Bhardwaj and Sanjiva Prasad. "Secure information flow connections". In: *Journal of Logical and Algebraic Methods in Programming* 127 (2022), p. 100761.

[3] Austin Melton, Bernd SW Schröder, and George E Strecker. "Lagois connections—a counterpart to Galois connections". In: *Theoretical Computer Science* 136.1 (1994), pp. 79–107.

References II

[4] Flemming Nielson, René Rydhof Hansen, and Hanne Riis Nielson. "Adaptive security policies". In: *Leveraging Applications of Formal Methods, Verification and Validation: Engineering Principles: 9th International Symposium on Leveraging Applications of Formal Methods, ISoLA 2020, Rhodes, Greece, October 20–30, 2020, Proceedings, Part II 9*. Springer. 2020, pp. 280–294.