Opacity with Orwellian Observers and Intransitive Non-Interference

John Mullins

Université Pierre & Marie Curie
Laboratoire d'Informatique de Paris 6 (LIP6)

On leave from
École Polytechnique de Montréal

Meeting on
Hiding and Disclosing Information
Paris, December 3, 2013

Contents

ÉCOLE POLYTECHNIQUE MONTRÉAL

Outline

ÉCOLE POLYTECHNIQUE MONTRÉAL

Context

Need for relax security properties based on information flow

1. Quantify information flow
2. Declassify information

Opacity

Generic property expressing the capability of an observer to infer information from a secret behaviour of a partially observable system

Introduced in [Mazaré (WITS'2004), Bryans et al. (FAST'2005)]

In this talk:

Characterize opacity in the presence of intentional opacity disclosure

Opacity – Definition

Intuition

Environment has a perfect knowledge but a partial observation of the system's behavior.

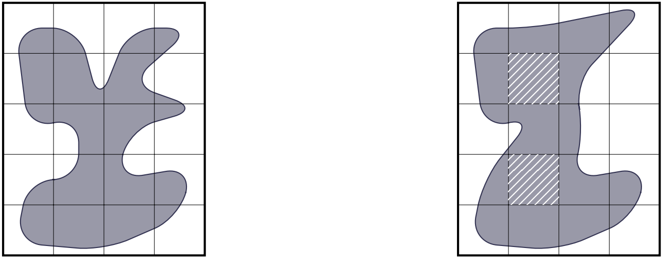
Definition

- $Exec(\mathcal{S})$: the set of executions of a system $\mathcal{S}$,
- $\mathcal{O} : Exec(\mathcal{S}) \rightarrow Obs^*$: an observation function.
- $\varphi \subseteq Exec(\mathcal{S})$: a predicate on $Exec(\mathcal{S})$ (the secret).

φ is opaque on $\mathcal{S}$ w.r.t. $\mathcal{O}$ if, for any $o \in Obs^*$, the following holds:

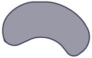
$$\mathcal{O}^{-1}(o) \not\subseteq \varphi.$$

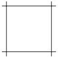
Opacity – Illustration



(a) φ is opaque on $\mathcal{S}$ w.r.t. $\mathcal{O}$

(b) φ is not opaque on $\mathcal{S}$ w.r.t. $\mathcal{O}$

 φ

 $\mathcal{O}^{-1}(o)$

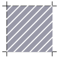
 Classes leaking their inclusion into φ

Figure: Opacity.

Computational power of observers

Definition

An observation function $\mathcal{O} : Exec(\mathcal{S}) \rightarrow Obs^*$ is called

- *static*: Observer's interpretation of events is fixed *a priori*
- *dynamic*: Observer's interpretation of the current event change dynamically depending on the the prefix of an execution observed so far
- *orwellian*: Observer's interpretation of the current event depends as well on the prefix as on the suffix of the execution

In this talk: Opacity w.r.t. a class of orwellian observers

ÉCOLE POLYTECHNIQUE MONTRÉAL

Outline

ÉCOLE POLYTECHNIQUE MONTRÉAL

Deterministic transition systems

Definition (Labelled transition system)

A finite deterministic *labelled transition system* over Σ is a 4-tuple $G = (\Sigma, Q, \delta, q_0)$, where

- Σ: alphabet of events,
- Q: the state space,
- δ: a partial function from $Q \times \Sigma$ to Q (*labelled transition function*)
- q_0:*initial state*.

Some notations

- G is complete if δ is total
- G^q : G by starting from q
- $L(G) = \{s \in \Sigma^* : \delta(q_0, s)$ is defined$\}$ (*language of G*)
- $L_F(G) = \{s \in \Sigma^* : \delta(q_0, s) \in F\}$ (*language recognized* by $F \subseteq Q$)

Some LTS constructors

Definition (Synchronization product)

Let LTSs $G = (\Sigma, Q, \delta, q_0, F)$ and $G' = (\Sigma, Q', \delta', q_0', F')$. The *synchronization product* of G and G' denoted $G \times G'$ is the LTS $(\Sigma, Q \times Q', \delta \times \delta', (q_0, q_0'), F \times F')$ with

$$\delta \times \delta'((q, q'), a) = (\delta(q, a), \delta'(q', a))$$

Definition (Restriction)

Let $G = (\Sigma, Q, \delta, q_0, F)$, a LTS and $\Sigma' \subseteq \Sigma$. The restriction of G to Σ' denoted $G \setminus \Sigma'$ is the LTS $(\Sigma \setminus \Sigma', Q, \delta', q_0)$ with

$$\delta' = \delta|(\Sigma \setminus \Sigma')$$

ÉCOLE POLYTECHNIQUE MONTRÉAL

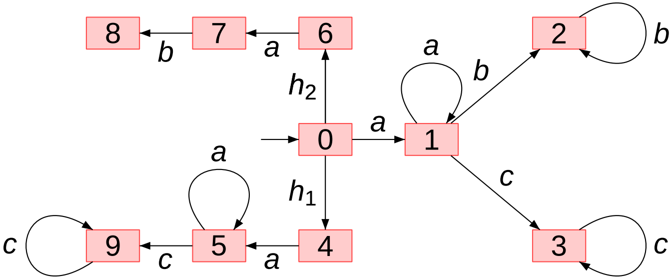
Opacity w.r.t. static observation

Natural projection

$$\pi_o(\epsilon) = \epsilon$$

$$\pi_o(s\cdot\alpha) = \begin{cases} \pi_o(s)\cdot\alpha & \text{if } \alpha \in \Sigma_o, \\ \pi_o(s) & \text{otherwise.} \end{cases}$$

- $\Sigma = \{h_1, h_2, a, b, c\}$
- $\Sigma_o = \{a, b, c\}$
- $\varphi = a^*(b^* + c^*)$



ÉCOLE POLYTECHNIQUE MONTRÉAL

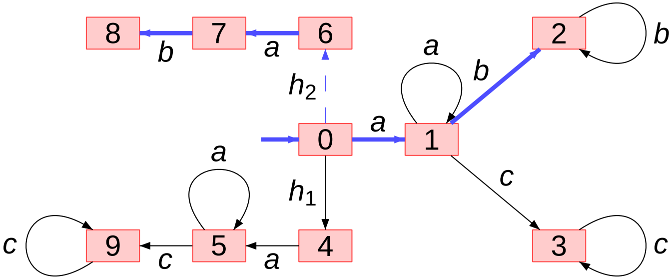
Opacity w.r.t. static observation

Natural projection

$$\pi_o(\epsilon) = \epsilon$$

$$\pi_o(s \cdot \alpha) = \begin{cases} \pi_o(s) \cdot \alpha & \text{if } \alpha \in \Sigma_o, \\ \pi_o(s) & \text{otherwise.} \end{cases}$$

- $\Sigma = \{h_1, h_2, a, b, c\}$
- $\Sigma_o = \{a, b, c\}$
- $\varphi = a^*(b^* + c^*)$



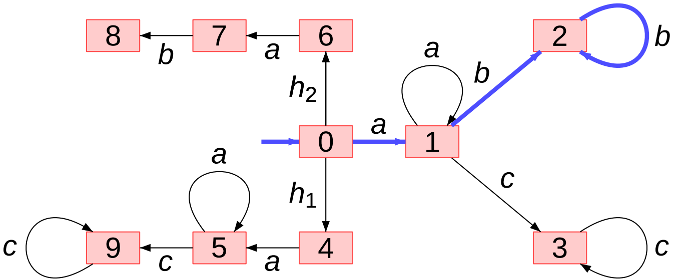
Opacity w.r.t. static observation

Natural projection

$$\pi_o(\epsilon) = \epsilon$$

$$\pi_o(s \cdot \alpha) = \begin{cases} \pi_o(s) \cdot \alpha & \text{if } \alpha \in \Sigma_o, \\ \pi_o(s) & \text{otherwise.} \end{cases}$$

- $\Sigma = \{h_1, h_2, a, b, c\}$
- $\Sigma_o = \{a, b, c\}$
- $\varphi = a^*(b^* + c^*)$



ÉCOLE POLYTECHNIQUE MONTRÉAL

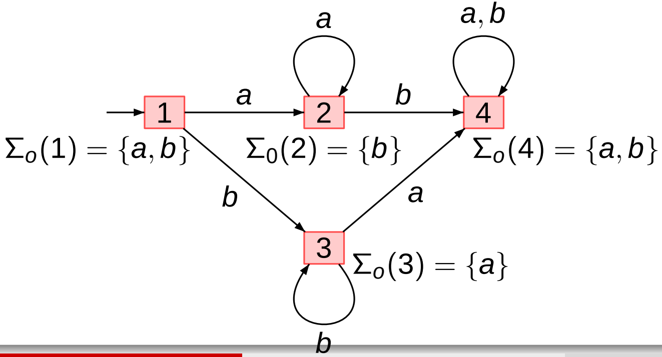
Opacity w.r.t. dynamic observation

Dynamic projection

$$\pi_{\mathcal{O}}(\epsilon) = \epsilon$$

$$\pi_{\mathcal{O}}(s \cdot \alpha) = \begin{cases} \pi_{\mathcal{O}}(s) \cdot \alpha & \text{if } \alpha \in \Sigma_o(\delta(q_o, s)), \\ \pi_{\mathcal{O}}(s) & \text{otherwise.} \end{cases}$$

- $\Sigma = \{a, b\}$
- $\mathcal{O} = (\Sigma, Q, \delta, q_0, \Sigma_0)$



Opacity verification problem

Opacity Verification Problem (OVP)

Is φ opaque on $\mathcal{S}$ w.r.t. $\mathcal{O}$?

Theorem (Bryans et al. (2005))

OVP is undecidable even for finite systems.

Theorem (Darondeau et al. (2007))

OVP is decidable for finite systems, regular secrets and static observation.

Theorem (Cassez et al. (2012))

OVP is decidable for finite systems, regular secrets and dynamic projections

Opacity verification problem

Opacity Verification Problem (OVP)

Is φ opaque on $\mathcal{S}$ w.r.t. $\mathcal{O}$?

Theorem (Bryans et al. (2005))

OVP is undecidable even for finite systems.

Theorem (Darondeau et al. (2007))

OVP is decidable for finite systems, regular secrets and static observation. *Hint.:* $\pi(\varphi) \subseteq \pi(L \setminus \varphi)$ *is decidable for* π*: morphism*

Theorem (Cassez et al. (2012))

OVP is decidable for finite systems, regular secrets and dynamic projections

Opacity verification problem

Opacity Verification Problem (OVP)

Is φ opaque on $\mathcal{S}$ w.r.t. $\mathcal{O}$?

Theorem (Bryans et al. (2005))

OVP is undecidable even for finite systems.

Theorem (Darondeau et al. (2007))

OVP is decidable for finite systems, regular secrets and static observation. *Hint.:* $\pi(\varphi) \subseteq \pi(L \setminus \varphi)$ *is decidable for* π*: morphism*

Theorem (Cassez et al. (2012))

OVP is decidable for finite systems, regular secrets and dynamic projections *Hint.:* $\pi(\varphi) \subseteq \pi(L \setminus \varphi)$ *is decidable for* π*: sequential*

Outline

ÉCOLE POLYTECHNIQUE MONTRÉAL

Orwellian projection

Orwellian projection

$$\pi_{o,d}(\epsilon) = \epsilon$$

$$\pi_{o,d}(s\alpha) = \begin{cases} s\alpha & \text{if } \alpha \in \Sigma_d, \\ \pi_{o,d}(s)\alpha & \text{if } \alpha \in \Sigma_o, \\ \pi_{o,d}(s) & \text{otherwise.} \end{cases}$$

- $\Sigma = \{h, d, l\}$
- $\Sigma_o = \{l\}$
- $\Sigma_d = \{d\}$
- $\varphi = \{hl\} \cup \{hdhl\}\{l\}^*$

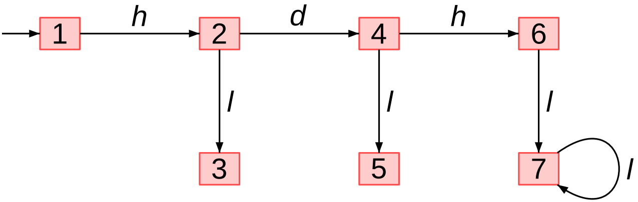


Figure: *A non opaque system w.r.t.* $\pi_{o,d}$

ÉCOLE POLYTECHNIQUE MONTRÉAL

Orwellian projection

Orwellian projection

$$\pi_{o,d}(\epsilon) = \epsilon$$

$$\pi_{o,d}(s\alpha) = \begin{cases} s\alpha & \text{if } \alpha \in \Sigma_d, \\ \pi_{o,d}(s)\alpha & \text{if } \alpha \in \Sigma_o, \\ \pi_{o,d}(s) & \text{otherwise.} \end{cases}$$

- $\Sigma = \{h, d, l\}$
- $\Sigma_o = \{l\}$
- $\Sigma_d = \{d\}$
- $\varphi = \{hl\} \cup \{hdhl\}\{l\}^*$

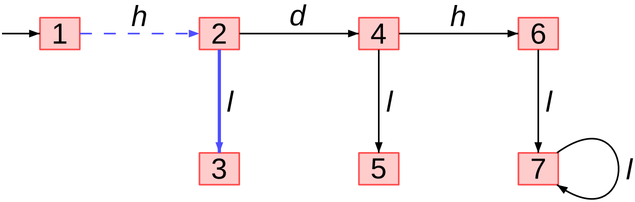


Figure: *A non opaque system w.r.t.* $\pi_{o,d}$

Orwellian projection

Orwellian projection

$$\pi_{o,d}(\epsilon) = \epsilon$$

$$\pi_{o,d}(s\alpha) = \begin{cases} s\alpha & \text{if } \alpha \in \Sigma_d, \\ \pi_{o,d}(s)\alpha & \text{if } \alpha \in \Sigma_o, \\ \pi_{o,d}(s) & \text{otherwise.} \end{cases}$$

- $\Sigma = \{h, d, l\}$
- $\Sigma_o = \{l\}$
- $\Sigma_d = \{d\}$
- $\varphi = \{hl\} \cup \{hdhl\}\{l\}^*$

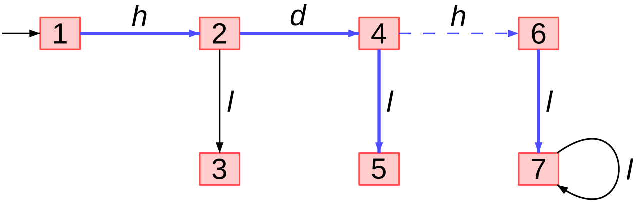


Figure: *A non opaque system w.r.t.* $\pi_{o,d}$

ÉCOLE POLYTECHNIQUE MONTRÉAL

Orwellian projection

Orwellian projection

$$\pi_{o,d}(\epsilon) = \epsilon$$

$$\pi_{o,d}(s\alpha) = \begin{cases} s\alpha & \text{if } \alpha \in \Sigma_d, \\ \pi_{o,d}(s)\alpha & \text{if } \alpha \in \Sigma_o, \\ \pi_{o,d}(s) & \text{otherwise.} \end{cases}$$

- $\Sigma = \{h, d, l\}$
- $\Sigma_o = \{l\}$
- $\Sigma_d = \{d\}$
- $\varphi = \{hl\} \cup \{hdhl\}\{l\}^*$

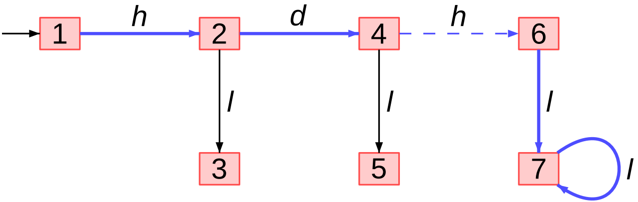


Figure: *A non opaque system w.r.t.* $\pi_{o,d}$

ÉCOLE POLYTECHNIQUE MONTRÉAL

Some additional facts and notations

- For $s \in L$, $[s]^L_\pi = \pi^{-1}(\pi(s))$
- $D(L)$= prefixes of L terminating with a d
- for $s \in D(L)$, $C(s, L)$ is its set of d-free continuations in L

Proposition (Factorization)

Any u in L admits a unique factorization $u = st$ *such that* $s \in D(L)$ *and* $t \in C(s, L)$.

- $[st]^L_{o,d} = s[t]^{C(s,L)}_o$

ÉCOLE POLYTECHNIQUE MONTRÉAL

Incorporating the secret into the transition system

Given

- $G = (\Sigma, Q, \delta, q_0, F)$ s.t. $L_F(G) = L$
- A regular secret $\varphi \subseteq L$

One constructs:

1. a complete deterministic transition system

$$G_\varphi = (\Sigma, Q', \delta', q'_0, F_\varphi) \text{ s.t. } L_{F_\varphi}(G_\varphi) = \varphi$$

2. $G_\# = G \times G_\varphi$, $F_\# = F \times Q'$ and $F_{\varphi\#} = F \times F_\varphi$.

Proposition

- $L_{F_{\varphi\#}}(G_\#) = \varphi$
- $L_{F_\#}(G_\#) = L$

Checking opacity w.r.t. an orwellian projection

Theorem

Let $Q_d = \{q : \cdot \xrightarrow{d} q\}$. φ is opaque for $L_F(G)$ w.r.t. $\pi_{o,d}$ iff for all $q \in Q_d$, $L_{F_\varphi}(G^q \setminus \Sigma_d)$ is opaque for $L_F(G^q \setminus \Sigma_d)$ w.r.t. π_o.

Proof.

$\Longleftarrow$: φ is not opaque for L w.r.t. $\pi_{o,d}$ then

$$(\exists s_0 \in D(\varphi), t_0 \in C(s_0, \varphi))\ [s_0 \cdot t_0]_{o,d}^{L_F(G)} \subseteq \varphi.$$

And as
$[s_0 \cdot t_0]_{o,d}^{L_F(G)} = s_0 \cdot [t_0]_o^{C(s_0, L_F(G))} = s_0 \cdot [t_0]_o^{L_F(G^{\overline{q}} \setminus \Sigma_d)}$ for $\delta(q_0, s_0) = \overline{q}$
We get that $[t_0]_o^{L_F(G^{\overline{q}} \setminus \Sigma_d)} \subseteq L_{F_\varphi}(G^{\overline{q}} \setminus \Sigma_d)$
and hence , $L_{F_\varphi}(G^{\overline{q}} \setminus \Sigma_d)$ is not opaque for $L_F(G^{\overline{q}} \setminus \Sigma_d)$ w.r.t. π_o. □

Outline

ÉCOLE POLYTECHNIQUE MONTRÉAL

Non-interference

Definition

Let a LTS $G = (\Sigma, Q, \delta, q_0, F)$ and $L = L_F(G)$ then L satisfies *non-interference* (NI) if $\pi_{Low}(L) \subseteq L$.

For $h \in High$
and $l \in Low$

1. Causal dependency on left handside: $h \Longrightarrow l$
2. No causal dependency on right hand side

Non-interference

Definition

Let a LTS $G = (\Sigma, Q, \delta, q_0, F)$ and $L = L_F(G)$ then L satisfies *non-interference* (NI) if $\pi_{Low}(L) \subseteq L$.

For $h \in High$
and $l \in Low$

1. Causal dependency on left handside: $h \Longrightarrow l$
2. No causal dependency on right hand side

Non-interference

Definition

Let a LTS $G = (\Sigma, Q, \delta, q_0, F)$ and $L = L_F(G)$ then L satisfies *non-interference* (NI) if $\pi_{Low}(L) \subseteq L$.

For $h \in High$
and $l \in Low$

1. Causal dependency on left handside: $h \Longrightarrow l$
2. No causal dependency on right hand side

Intransitive Non-interference

Definition

Let a LTS $G = (\Sigma, Q, \delta, q_0, F)$ and $L = L_F(G)$ then L satisfies *intransitive non-interference* (INI) if $\pi_{High,Down}(L) \subseteq L$.

1. Not admissible causal dependency on left handside: $hh \Longrightarrow l$
2. Admissible causal dependency on right hand side

Theorem (Mullins2000)

Let a LTS $G = (\Sigma, Q, \delta, q_0, F)$ and $L = L_F(G)$. L satisfies INI iff for all $q \in Q_d$, $L_F(G^q \setminus Down)$ satisfies NI.

Intransitive Non-interference

Definition

Let a LTS $G = (\Sigma, Q, \delta, q_0, F)$ and $L = L_F(G)$ then L satisfies *intransitive non-interference* (INI) if $\pi_{High,Down}(L) \subseteq L$.

1. Not admissible causal dependency on left handside: $hh \Longrightarrow l$
2. Admissible causal dependency on right hand side

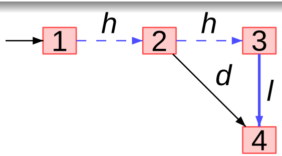
Theorem (Mullins2000)

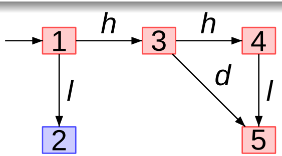
Let a LTS $G = (\Sigma, Q, \delta, q_0, F)$ and $L = L_F(G)$. L satisfies INI iff for all $q \in Q_d$, $L_F(G^q \setminus Down)$ satisfies NI.

Intransitive Non-interference

Definition

Let a LTS $G = (\Sigma, Q, \delta, q_0, F)$ and $L = L_F(G)$ then L satisfies *intransitive non-interference* (INI) if $\pi_{High,Down}(L) \subseteq L$.





1. Not admissible causal dependency on left handside: $hh \Longrightarrow l$
2. Admissible causal dependency on right hand side

Theorem (Mullins2000)

Let a LTS $G = (\Sigma, Q, \delta, q_0, F)$ and $L = L_F(G)$. L satisfies INI iff for all $q \in Q_d$, $L_F(G^q \setminus Down)$ satisfies NI.

Intransitive Non-interference

Definition

Let a LTS $G = (\Sigma, Q, \delta, q_0, F)$ and $L = L_F(G)$ then L satisfies *intransitive non-interference* (INI) if $\pi_{High,Down}(L) \subseteq L$.

1. Not admissible causal dependency on left handside: $hh \Longrightarrow l$
2. Admissible causal dependency on right hand side

Theorem (Mullins2000)

Let a LTS $G = (\Sigma, Q, \delta, q_0, F)$ and $L = L_F(G)$. L satisfies INI iff for all $q \in Q_d$, $L_F(G^q \setminus Down)$ satisfies NI.

Intransitive Non-interference

Definition

Let a LTS $G = (\Sigma, Q, \delta, q_0, F)$ and $L = L_F(G)$ then L satisfies *intransitive non-interference* (INI) if $\pi_{High,Down}(L) \subseteq L$.

1. Not admissible causal dependency on left handside: $hh \Longrightarrow l$
2. Admissible causal dependency on right hand side

Theorem (Mullins2000)

Let a LTS $G = (\Sigma, Q, \delta, q_0, F)$ and $L = L_F(G)$. L satisfies INI iff for all $q \in Q_d$, $L_F(G^q \setminus Down)$ satisfies NI.

Intransitive Non-interference

Definition

Let a LTS $G = (\Sigma, Q, \delta, q_0, F)$ and $L = L_F(G)$ then L satisfies *intransitive non-interference* (INI) if $\pi_{High,Down}(L) \subseteq L$.

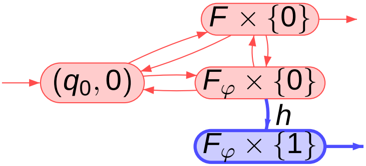
1. Not admissible causal dependency on left handside: $hh \Longrightarrow l$
2. Admissible causal dependency on right hand side

Theorem (Mullins2000)

Let a LTS $G = (\Sigma, Q, \delta, q_0, F)$ and $L = L_F(G)$. L satisfies INI iff for all $q \in Q_d$, $L_F(G^q \setminus Down)$ satisfies NI.

Opacity w.r.t. π_o reduces to NI

$G = (\Sigma, Q, \delta, q_0)$: LTS
$F, F_\varphi \subseteq Q$
$Low = \Sigma_o$, $High = \{h\}$



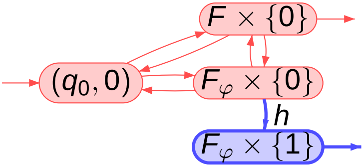
$G^\flat = (\Sigma^\flat, Q^\flat, \delta^\flat, q_0^\flat)$ and $F^\flat \subseteq Q^\flat$ s.t.

$$\begin{aligned}
\Sigma^\flat &= \Sigma_o \uplus \{h\} \\
Q^\flat &= (Q \times \{0\}) \cup (F_\varphi \times \{1\}) \\
\delta^\flat &= \{((q,0), \alpha, (q',0)) : (q, \alpha, q') \in \delta \text{ and } \alpha \in \Sigma_o\} \cup \\
&\quad \{((q,0), \epsilon, (q',0)) : (q, \alpha, q') \in \delta \text{ and } \alpha \in \Sigma_u\} \cup \\
&\quad \{((q,0), h, (q,1)) : q \in F_\varphi\} \\
q_0^\flat &= (q_0, 0) \\
F^\flat &= (F \cap (Q \setminus F_\varphi) \times \{0\}) \cup (F_\varphi \times \{1\}).
\end{aligned}$$

Opacity w.r.t. π_o reduces to NI (2)

The reduction

φ is opaque for L w.r.t. π_o iff $L^\flat = L_{F^\flat}(G^\flat)$ satisfies NI



Proof.

$\Longrightarrow$: Otherwise, there is $s'_0 \in \pi_{Low}(L^\flat)$ ($= L_{F_\varphi \times \{0\}}(G^\flat)$) s.t. $s'_0 \notin L^\flat$. Hence $s'_0 \in L_{F_\varphi \times \{0\}}(G^\flat)$ meaning that $[s_0]^L_o \subseteq \varphi$ for s_0 s.t. $\pi_o(s_0) = s'_0$ and consequently that s_0 discloses φ w.r.t. π_o.

$\Longleftarrow$: We show that if s_0 discloses the secret φ then let $s'_0 = \pi_o(s_0) \cdot h$ then $\pi_{Low}(s'_0) \notin L^\flat$ and $s'_0 \in L^\flat$ and hence, $L^\flat$ violates NI. □

Opacity w.r.t. $\pi_{o,d}$ reduces to INI

$G = (\Sigma, Q, \delta, q_0)$: LTS

$F, F_\varphi \subseteq Q$

$Low = \Sigma_o, Down = \Sigma_d$ and $High = \{h\}$

$G^\natural = (\Sigma^\natural, Q^\natural, \delta^\natural, q_0^\natural)$ and $F^\natural \subseteq Q'$ s.t.

The reduction

φ is opaque for L w.r.t. $\pi_{o,d}$ iff $L^\natural = L_{F^\natural}(G^\natural)$ satisfies INI

ÉCOLE POLYTECHNIQUE MONTRÉAL

INI reduces to opacity w.r.t. $\pi_{o,d}$

The construction

$G = (\Sigma, Q, \delta, q_0)$: LTS
$F \subseteq Q$ s.t. $L = L_F(G)$
$\Sigma = High \uplus Low \uplus Down$

$$\varphi = \{s \in L_F(G) : \pi_{Low,Down}(s) \neq s\}$$

The reduction

L satisfies INI iff φ is opaque for L w.r.t. $\pi_{Low,Down}$.

ÉCOLE POLYTECHNIQUE MONTRÉAL

Outline

ÉCOLE POLYTECHNIQUE MONTRÉAL

Summary

1. We have investigated
   - A class of orwellian observation functions
   - Computability of OVP in the context of
     - finite systems,
     - regular secrets and
     - orwellian projections
2. As an illustration of the relevancy to security we have related opacity w.r.t. $\pi_{o,d}$ to INI by
   - showing an equivalence between both notions,
   - providing, as a side effect a characterization of NI with opacity w.r.t. natural projections.

   also in the context of
   - finite systems,
   - regular secrets

ÉCOLE POLYTECHNIQUE MONTRÉAL

Future work

- Instantiate opacity to INI with selective downgrading (INISD), allowing to each downgrading action d to declassify only a subset $H(d)$ of Σ_u as defined in [Best, Darondeau (POST '12)].
- Instantiate to known information flow properties. (Non-deducibility on strategies) [Wittbold, Johnson (1990)],
- Address the problem of supremal sub-language L of K such that φ is opaque for L w.r.t. $\pi_{o,d}$ and its dual problem.
- Address the problem of supervisory control for opacity w.r.t. $\pi_{o,d}$ along the lines of [Dubreil, Darondeau, Marchand (2010)].

Thank you

Any questions ?