P-Congruences as Noninterference
for the $\pi$-Calculus

Silvia Crafa
Universita’ di Padova
Italy

Sabina Rossi
Universita’ Ca’ Foscari Venezia
Italy

FMSE 06, Fairfax Virginia USA, 3 Nov. 2006
Noninterference information does not flow from high to low if the high behavior has no effect on what can be observed at low level.

INGREDIENTS:

- something to modify the high behaviour: attackers affecting high components
- something that observes: contexts affecting low components
- something to compare behaviours: behavioral equivalence
Noninterference in $\pi$-calculus

$h().\ell() \mid \overline{h}()$ is insecure
Noninterference in $\pi$-calculus

\[ h() \cdot \ell() | \overline{h}\langle \rangle \text{ is insecure} \]

\[ \overline{h}\langle n \rangle | \overline{h}\langle m \rangle | h(x).\text{if } x = n \text{ then } \overline{\ell}_1\langle \rangle \text{ else } \overline{\ell}_2\langle \rangle \]

An attack can destroy the nondeterminism causing an interference.
Noninterference in $\pi$-calculus

$\text{◮ } h().\ell() \mid \overline{h}\langle \rangle$ is insecure

$\text{◮ } \overline{h}\langle n \rangle \mid \overline{h}\langle m \rangle \mid h(x).\text{if } x = n \text{ then } \overline{\ell}_1\langle \rangle \text{ else } \overline{\ell}_2\langle \rangle$

An attack can destroy the nondeterminism causing an interference.

$\text{◮ } P = (\nu \ell) (\overline{\ell}_1\langle \ell \rangle.\overline{\ell}\langle \rangle.P?)$ and $Q = (\nu \ell) (\overline{h}\langle \ell \rangle.\overline{\ell}\langle \rangle.Q?)$

The security of $P/Q$ depends on that of $P?/Q?$ ??

$P = (\nu \ell) \overline{\ell}_1\langle \ell \rangle.\overline{\ell}\langle \rangle.P? \xrightarrow{(\nu \ell)\overline{\ell}_1\langle \ell \rangle} \overline{\ell}\langle \rangle.P? \xrightarrow{\overline{\ell}\langle \rangle} P?$

$Q = (\nu \ell) \overline{h}\langle \ell \rangle.\overline{\ell}\langle \rangle.Q? \xrightarrow{(\nu \ell)\overline{h}\langle \ell \rangle} \overline{\ell}\langle \rangle.Q? \xrightarrow{\overline{\ell}\langle \rangle} Q?$

The low observer will be able to observe $P?$, which must be secure. However, it will not learn $\ell$, hence it will never observe $Q?$
Noninterference in $\pi$-calculus

- $h().l() \mid \overline{h}\langle \rangle$ is insecure

- $\overline{h}\langle n \rangle \mid \overline{h}\langle m \rangle \mid h(x).\text{if } x = n \text{ then } \overline{\ell_1}\langle \rangle \text{ else } \overline{\ell_2}\langle \rangle$

  An attack can destroy the nondeterminism causing an interference.

- $P = (\nu l) (\overline{\ell_1}\langle l \rangle.\overline{\ell}\langle \rangle. P^?)$ and $Q = (\nu l) (\overline{h}\langle l \rangle.\overline{\ell}\langle \rangle. Q^?)$

  The security of $P/Q$ depends on that of $P^?/Q^?$

  $\begin{align*}
P &= (\nu l) \overline{\ell_1}\langle l \rangle.\overline{\ell}\langle \rangle. P^？ \xrightarrow{(\nu l) \overline{\ell_1}\langle l \rangle} \overline{\ell}\langle \rangle. P^？ \xrightarrow{\overline{\ell}\langle \rangle} P^？ \\
Q &= (\nu l) \overline{h}\langle l \rangle.\overline{\ell}\langle \rangle. Q^？ \xrightarrow{(\nu l) \overline{h}\langle l \rangle} \overline{\ell}\langle \rangle. Q^？ \xrightarrow{\overline{\ell}\langle \rangle} Q^？
\end{align*}$

  The low observer will be able to observe $P^？$, which must be secure.
  However, it will not learn $\ell$, hence it will never observe $Q^？$

- $\nu h)(\overline{h} \mid !h.(\overline{k} \mid \overline{h}) \mid k.\overline{\ell})$ is it secure?
Noninterference in $\pi$-calculus

We provide a semantic characterization of noninterference in terms of the process behavior.

- Our characterizations of secure processes admit effective proof techniques (for finite state processes)
- Use a lightweight type system to avoid explicit flows: no safety theorem.
- Our framework also consider a declassification mechanism.
### Prefixes

\[ \pi ::= \overline{a}(\tilde{b}) \quad \text{output} \]  
\[ a(\tilde{x}:\tilde{T}) \quad \text{input} \]

### Processes

\[ P ::= \pi.P \quad \text{prefix} \]  
\[ \text{if } a = b \text{ then } P \text{ else } P \quad \text{matching} \]  
\[ P | P \quad \text{parallel} \]

### Types

\[ T ::= \delta[] \]  
\[ (\nu n : T)P \quad \text{restriction} \]  
\[ \delta[\tilde{T}] \]  
\[ !P \quad \text{replication} \]  
\[ 0 \quad \text{inactive} \]

---

**(EMPTY TYPE)**  
\[ \vdash \delta[] \]

**CHANNEL TYPE**  
\[ \vdash T_i \quad \Lambda(T_i) \leq \delta \]

---

**absence of explicit flows**
High and Low Contexts

- \( P \) is a \( \sigma \)-low level source in \( \Gamma \), denoted \( \Gamma \vdash_\sigma P \), if \( \Gamma \vdash P \) and \( \forall m \in \text{fn}(P) \) it holds \( \Lambda(\Gamma(m)) \leq \sigma \).

- \( P \) is a \( \sigma \)-high level source in \( \Gamma \), denoted \( \Gamma \vdash^{\sigma} P \), if for all names \( a \) used in \( P \) as a subject in an input or an output prefix, \( \Lambda(\Gamma(a)) \not\leq \sigma \).

\[
C[\cdot \Gamma] ::= [\cdot \Gamma] \mid (\nu n : T)C[\cdot \Gamma] \mid C[\cdot \Gamma] \mid P \mid P \mid C[\cdot \Gamma]
\]

\( C[\cdot \Gamma] \) is a \( \sigma \)-low (resp. \( \sigma \)-high) context if it is a \((\Gamma'/\Gamma)\)-context generated by the grammar above where \( \Lambda(T) \leq \sigma \) (resp. \( \Lambda(T) \not\leq \sigma \)) and \( \Gamma' \vdash_\sigma P \) (resp. \( \Gamma' \vdash^{\sigma} P \)).

(\( \nu h \)(\( \overline{h}(\ell) \mid \cdot \Gamma \)) is a \( \sigma \)-high context whereas

(\( \nu h \)(\( \overline{h}(\ell) \mid h(x).\overline{x} \)) \mid [\cdot \Gamma] \) is a \( \sigma \)-low context.
The largest type-indexed relation over processes which is symmetric,

**reduction closed:**

if $\Gamma \models P \mathrel{\mathcal{R}} Q$ and $P \xrightarrow{\tau} P'$ then

$\exists Q'$ such that $Q \xrightarrow{} Q'$ and $\Gamma \models P' \mathrel{\mathcal{R}} Q'$.

**barb preserving:**

if $\Gamma \models P \mathrel{\mathcal{R}} Q$ and $\Gamma \vdash P \downarrow_n$ then $\Gamma \models Q \downarrow_n$.

Where $\Gamma \vdash P \downarrow_n$ means $P \xrightarrow{\overline{\pi}\langle m \rangle}$.

**contextual:**

if $\Gamma \models P \mathrel{\mathcal{R}} Q$ and $\Gamma' \vdash C[\cdot\Gamma]$ then

$\Gamma' \models C[P] \mathrel{\mathcal{R}} C[Q]$ for all typed contexts $C[\cdot\Gamma]$.

It captures the behaviour of processes.
\(\sigma\)-Reduction barbed congruence \(\Gamma \vdash P \cong_{\sigma} Q\)

The largest type-indexed relation over processes which is symmetric, reduction closed:

if \(\Gamma \vdash P \mathcal{R} Q\) and \(P \xrightarrow{\tau} P'\) then

\(\exists Q'\) such that \(Q \xrightarrow{} Q'\) and \(\Gamma \vdash P' \mathcal{R} Q'\).

\(\sigma\)-barb preserving:

if \(\Gamma \vdash P \mathcal{R} Q\) and \(\Gamma \vdash P \downarrow^{\sigma} n\) then \(\Gamma \vdash Q \downarrow^{\sigma} n\).

\(\Gamma \vdash P \downarrow^{\sigma} n\) when \(P \xrightarrow{n(m)}\) with \(\Lambda(\Gamma(n)) \leq \sigma\).

\(\sigma\)-contextual:

if \(\Gamma \vdash P \mathcal{R} Q\) and \(\Gamma' \vdash C[\cdot;\Gamma]\) then

\(\Gamma' \vdash C[P] \mathcal{R} C[Q]\) for all \(\sigma\)-low contexts \(C[\cdot;\Gamma]\)

(interacting with the hole just thorough \(\sigma\)-channels).

It captures the \(\sigma\)-low behaviour of processes
\[ \Gamma, \sigma \models P \cong_{\sigma} Q \]

- \( \models \) equates processes exhibiting the same behaviour
- \( \models \sigma \) equates processes exhibiting the same \( \sigma \)-low behaviour
- \( \models \sigma \) equates processes exhibiting the same \( \sigma \)-low behaviour whatever is the surrounding \( \sigma \)-high context
\(\sigma\)-reduction barbed P-congruence \(\Gamma \models P \simeq_{\sigma} Q\)

The largest type-indexed relation over processes which is symmetric,

- *reduction closed, \(\sigma\)-barb preserving*

- *\(\sigma\)-P-contextual:*
  
  if \(P \simeq_{\sigma} Q\), then \(C_L[C_H^1[P]] \simeq_{\sigma} C_L[C_H^2[Q]]\)
  
  for all \(\sigma\)-low contexts \(C_L\) and for all \(\sigma\)-high contexts \(C_H^1, C_H^2\)

*It captures the \(\sigma\)-low behaviour whatever is the surrounding \(\sigma\)-high context*
\( \sigma \)-reduction barbed P-congruence \( \Gamma \models P \cong_{\sigma} Q \)

The largest type-indexed relation over processes which is symmetric,

- reduction closed, \( \sigma \)-barb preserving
- \( \sigma \)-P-contextual:
  
  if \( P \cong_{\sigma} Q \), then \( CL[ C_{H}^{1}[ P ] ] \cong_{\sigma} CL[ C_{H}^{2}[ Q ] ] \)
  
  for all \( \sigma \)-low contexts \( CL \) and for all \( \sigma \)-high contexts \( C_{1H}, C_{2H} \)

It captures the \( \sigma \)-low behaviour whatever is the surrounding \( \sigma \)-high context

\[ \Rightarrow \quad ?? \quad P \cong_{\sigma} P \quad ?? \]
\(\sigma\text{-reduction barbed } P\text{-congruence } \Gamma \models P \cong_{\sigma} Q\)

The largest type-indexed relation over processes which is symmetric,

- reduction closed, \(\sigma\)-barb preserving
- \(\sigma\)-\(P\)-contextual:
  
  if \(P \cong_{\sigma} Q\), then
  
  \[CL[CL[1][P]] \cong_{\sigma} CL[CL[2][Q]]\]

  for all \(\sigma\)-low contexts \(CL\) and for all \(\sigma\)-high contexts \(CL[1], CL[2]\)

- It captures the \(\sigma\)-low behaviour whatever is the surrounding \(\sigma\)-high context

  \[\implies\]

- \(P\) exhibits the same \(\sigma\)-low behaviour whatever is the surrounding \(\sigma\)-high context
  
  when

- \(P\) is interference-free
P-congruences as Noninterference

\[ P \in \mathcal{NI}(\cong_\sigma) \]

iff
\[ P \cong_\sigma P \]

iff
\[ C_L[ C^1_H[ P ]] \cong_\sigma C_L[ C^2_H[ P ]] \]

for all \( \sigma \)-low contexts \( C_L \) and for all \( \sigma \)-high contexts \( C^1_H, C^2_H \)

\[ \cong \emptyset \cong_\sigma (P_1 = h().\ell()) \]

\[ \cong_\sigma \emptyset \cong (P_2 = \ell().h(), P_3 = \ell().k()) \]

If \( P \cong_\sigma P \) then \( \forall Q \) s.t. \( P \cong Q \) it holds \( Q \cong_\sigma Q \cong_\sigma P \)
Examples

For **INSECURE** processes, simply find distinguishing contexts.

Let be $L \preceq H$ and $\sigma = L$,

\[ P_2 = \overline{h}(x : T). \text{ if } x = n \text{ then } \ell_1 \langle \rangle \text{ else } \ell_2 \langle \rangle \]

(the level of $n$ is irrelevant). Then $P_2 \not\in NI(\equiv_\sigma)$ since one can choose

$C^1_H = \overline{h}(n) \mid []$, $C^2_H = C_L = []$ and observe that

$P_2 \not\equiv_\sigma P_2 \mid \overline{h}(n)$.
Examples

For **INSECURE** processes, simply find distinguishing contexts.
Let be $L \preceq H$ and $\sigma = L$,

$\Rightarrow P_2 = h(x : T). \text{if } x = n \text{ then } \overline{l_1} \langle \rangle \text{ else } \overline{l_2} \langle \rangle$

(the level of $n$ is irrelevant). Then $P_2 \notin \mathcal{NI}(\cong_\sigma)$ since one can choose $C_H^1 = \overline{h}\langle n \rangle \mid [], C_H^2 = C_L = []$ and observe that $P_2 \not\cong_\sigma P_2 \mid \overline{h}\langle n \rangle$.

$\Rightarrow P_3 = \overline{h}\langle n \rangle \mid \overline{h}\langle m \rangle \mid h(x). \text{if } x = n \text{ then } \overline{l_1} \langle \rangle \text{ else } \overline{l_2} \langle \rangle$,

where $x$ can be nondeterministically substituted either with $n$ or $m$. An external attack can destroy the nondeterminism causing an interference:

let $C_H^1 = h(y).h(z).\overline{h}\langle n \rangle \mid [], C_H^2 = C_L = [],$ then $P_3 \not\cong_\sigma P_3 \mid h(y).h(z).\overline{h}\langle n \rangle$. Hence $P_3 \notin \mathcal{NI}(\cong_\sigma)$. 

16
P-congruences as Noninterference

\[ P \in \mathcal{NI}(\equiv_{\sigma}) \]

iff

\[ P \equiv_{\sigma} P \]

iff

\[ C_L[C_H^1[P]] \equiv_{\sigma} C_L[C_H^2[P]] \]

for all \( \sigma \)-low contexts \( C_L \) and for all \( \sigma \)-high contexts \( C_H^1, C_H^2 \)
Looking for a proof technique

Define a LTS of *typed actions* over configurations \( \Gamma \triangleright P \) (that means \( \Gamma \vdash P \))

\[
\begin{array}{c}
\Gamma \triangleright P \xrightarrow{\alpha} \delta \quad \Gamma' \triangleright P' \\
\text{action of} \\
\text{level (at most) } \delta
\end{array}
\]

**OUT**

\[
\begin{array}{c}
\Gamma \vdash n : \delta_1[T] \quad \delta_1 \preceq \delta \\
\Gamma \triangleright \overline{n}(m).P \quad \overline{n}(m) \quad \Gamma \triangleright P
\end{array}
\]

**IN**

\[
\begin{array}{c}
\Gamma \vdash n : \delta_1[T] \quad \Gamma \vdash m : T \quad \delta_1 \preceq \delta \\
\Gamma \triangleright n(x:T).P \quad n(m) \quad \Gamma \triangleright P\{x := m\}
\end{array}
\]
A proof technique for $\simeq_\sigma$

\[
\Gamma, m : T \triangleright P \xrightarrow{n(m)} \delta \quad \Gamma' \triangleright P' \\
\Gamma \triangleright P \xrightarrow{(\nu m : T)n(m)} \delta \quad \Gamma' \triangleright P' \\
\Gamma, m : T \triangleright P \xrightarrow{\bar{n}(m)} \delta \quad \Gamma' \triangleright P' \quad m \neq n \\
\Gamma \triangleright (\nu m : T)P \xrightarrow{(\nu m : T)\bar{n}(m)} \delta \quad \Gamma' \triangleright P'
\]

\[
\Gamma \triangleright P \xrightarrow{\alpha} \delta \quad \Gamma' \triangleright P' \quad bn(\alpha) \cap fn(Q) = \emptyset \\
\Gamma \triangleright P \mid Q \xrightarrow{\alpha} \delta \quad \Gamma' \triangleright P' \mid Q \\
\Gamma \triangleright P \xrightarrow{\tau} \Gamma \triangleright P' \\
\Gamma \triangleright P \xrightarrow{\tau} \delta \quad \Gamma \triangleright P'
\]

\[
\Gamma, n : T \triangleright P \xrightarrow{\alpha} \delta \quad \Gamma', n : T \triangleright P' \quad n \notin fn(\alpha) \cup bn(\alpha) \\
\Gamma \triangleright (\nu n : T)P \xrightarrow{\alpha} \delta \quad \Gamma' \triangleright (\nu n : T)P' \\
\Gamma \triangleright P \xrightarrow{\alpha} \delta \quad \Gamma' \triangleright P' \\
\Gamma \triangleright P \xrightarrow{\alpha} \delta \quad \Gamma \triangleright P' \mid !P
\]
Noninterference through a PER model

Partial bisimilarity on $\sigma$-low actions:

it is the largest symmetric relation $\approx_{\sigma}$ s.t. whenever $P \approx_{\sigma} Q$

- on observable ($\sigma$-low) actions it behaves as bisimilarity:
  
  if $P \xrightarrow{\alpha} P'$, then $\exists Q'$ s.t. $Q \xrightarrow{\hat{\alpha}} Q'$ with $Q' \approx_{\sigma} P'$.

- $\sigma$-high actions are simulated by internal transitions:
Noninterference through a PER model

Partial bisimilarity on $\sigma$-low actions:

it is the largest symmetric relation $\approx_\sigma$ s.t. whenever $P \approx_\sigma Q$

- on observable ($\sigma$-low) actions it behaves as bisimilarity:
  
  if $P \xrightarrow{\alpha}_\sigma P'$, then $\exists Q'$ s.t. $Q \xrightarrow{\hat{\alpha}}_\sigma Q'$ with $Q' \approx_\sigma P'$.

- $\sigma$-high actions are simulated by internal transitions:
Noninterference through a PER model

Partial bisimilarity on $\sigma$-low actions:
it is the largest symmetric relation $\cong_\sigma$ s.t. whenever $P \cong_\sigma Q$

- on observable ($\sigma$-low) actions it behaves as bisimilarity:
  if $P \xrightarrow{\alpha}_\sigma P'$, then $\exists Q'$ s.t. $Q \xrightarrow{\hat{\alpha}}_\sigma Q'$ with $Q' \cong_\sigma P'$.

- $\sigma$-high actions are simulated by internal transitions:
  if $\Gamma \triangleright P \xrightarrow{\alpha}_\sigma P'$ with $\alpha \in \{(\nu\tilde{p}:\tilde{T})n(\tilde{m}), (\nu\tilde{p}:\tilde{T})\tilde{n}(\tilde{m})\}$
  where $\tilde{p} : \tilde{T} = \tilde{p}_1 : \tilde{T}_1, \tilde{p}_2 : \tilde{T}_2$ such that $\Lambda(\tilde{T}_1) \not\preceq \sigma$, and $\Lambda(\tilde{T}_2) \preceq \sigma$,
  then $\exists Q'$ s. t. $\Gamma \triangleright Q \Longrightarrow \Gamma \triangleright Q'$ with
  $\Gamma, \tilde{p}_1 : \tilde{T}_1 \models Q' \cong_\sigma (\nu\tilde{p}_2 : \tilde{T}_2) P'$.

\[
P_1 = (\nu\ell)(\overline{h}\langle\ell\rangle.\overline{\ell}\rangle.R) \quad P_2 = (\nu k)(\overline{h}\langle k\rangle.\overline{k}\rangle.R)
\]
Time for an assessment

\[ P \text{ is secure} \]

\[ \text{iff } P \in \mathcal{NI}(\equiv_\sigma) \text{ iff } P \approx_\sigma P \]

- almost independent of typing constraints

- compositionality results:
  \[ \text{if } P, Q \in \mathcal{NI}(\equiv_\sigma) \text{ then} \]
  \[ P \mid Q \in \mathcal{NI}(\equiv_\sigma), \; !P \in \mathcal{NI}(\equiv_\sigma), \; (\nu n)P \in \mathcal{NI}(\equiv_\sigma) \]
Time for an assessment

\( P \) is secure

\[
\text{iff } P \in \mathcal{ NI}(\cong_\sigma) \text{ iff } P \cong_\sigma P
\]

- almost independent of typing constraints
- compositionality results:
  
  if \( P, Q \in \mathcal{ NI}(\cong_\sigma) \) then
  
  \[
P \parallel Q \in \mathcal{ NI}(\cong_\sigma), \; \!P \in \mathcal{ NI}(\cong_\sigma), \; (\nu n)P \in \mathcal{ NI}(\cong_\sigma)
  \]

\( \mathcal{ NI}(\cong_\sigma) \) is a strong security property!!

... well suited in open networks

... but what about the expressivity and flexibility of secure systems?
To increase the flexibility of the system, we add a declassification mechanism that coerces the security level of (specific) expressions downwards.

By declassifying certain expressions, the programmer may intentionally violate noninterference, but only in a controlled way.

*Which expressions are downgraded?*
To increase the flexibility of the system, we add a declassification mechanism that coerces the security level of (specific) expressions downwards.

By declassifying certain expressions, the programmer may intentionally violate noninterference, but only in a controlled way.

\[ \ell \langle \text{dec}(h) \rangle . P \text{ or } \ell \langle \text{dec}(F(h_1, \ldots, h_k)) \rangle . P \]
To increase the flexibility of the system, we add a declassification mechanism that coerces the security level of (specific) expressions downwards. By declassifying certain expressions, the programmer may intentionally violate noninterference, but only in a controlled way.

Which expressions are downgraded?

- downgrade names, or values, as in imperative languages: 
  \[ \overline{\ell}\langle \text{dec}(h) \rangle.P \text{ or } \overline{\ell}\langle \text{dec}(F(h_1, \ldots, h_k)) \rangle.P \]

- downgrade process actions:
  \[ \text{dec} \ h(x).P \text{ and } \text{dec} \ h\langle n \rangle.P \] stand for a declassified read/write action over the channel \( h \), which can still be used as a secret channel!
Declassifying actions: $\text{Dec } \pi$-calculus

- $\text{dec}_\delta n(x).P$ and $\text{dec}_\delta n\langle m \rangle. P$ represent “escape hatches” for information release: they allow info arising from these actions to flow down up to level $\delta$.

- Both users of the channel must agree to downgrade the communication:

  $$\text{dec}_\delta n(x).P \mid \text{dec}_\delta n\langle m \rangle.Q \rightarrow P\{m/x\} \mid Q$$

- Only programmers may enable the downgrading of secret information to an observable level; no external entities can synch on such declassified actions.
The theory of P-congruences scales to the $\text{Dec } \pi$-calculus:

$\simeq_{\text{dec}}^{\sigma}$ is the largest relation which is symmetric, reduction closed, $\sigma$-barb preserving and $\sigma$-contextual, where $\sigma$-low and $\sigma$-high context cannot fire declassified communications.
The theory of P-congruences scales to the \( \text{Dec } \pi \)-calculus:

- \( \sim_{\text{dec}}^{\sigma} \) is the largest relation which is symmetric, reduction closed, \( \sigma \)-barb preserving and \( \sigma \)-contextual, where \( \sigma \)-low and \( \sigma \)-high context cannot fire declassified communications.

- The downgrading does not affect the level of typed actions, it only has an impact on the admissible info flows: \( \Gamma \triangleright \text{dec}_{L} h \langle m \rangle . P \xrightarrow{\text{dec}_{L} h \langle m \rangle} H \Gamma \triangleright P \)
The theory of P-congruences scales to the Dec π-calculus:

- $\cong_{\sigma}^{\text{dec}}$ is the largest relation which is symmetric, reduction closed, $\sigma$-barb preserving and $\sigma$-contextual, where $\sigma$-low and $\sigma$-high context cannot fire declassified communications.

- The downgrading does not affect the level of typed actions, it only has an impact on the admissible info flows: $\Gamma \triangleright \text{dec}_L \langle m \rangle . P \xrightarrow{\text{dec}_L \langle m \rangle} H \Gamma \triangleright P$

- $\approx_{\sigma}^{\text{dec}}$ scales to Dec π:
  - $\sigma$-low actions must be precisely matched
  - $\sigma$-high actions must be matched by $\tau$-steps
  - $\sigma$-high declassified actions need not to be matched by $\tau$-steps since they represent an explicitly allowed info flow.

- $P \in N\mathcal{I}(\cong_{\sigma}^{\text{dec}})$ iff $P \approx_{\sigma}^{\text{dec}} P$
\( P = \overline{h} \mid h.\ell \) is obviously insecure, whereas \( P' = \overline{\text{dec } h} \mid \text{dec } h.\ell \) can be shown to be a secure process such that \( \Gamma \models P' \cong_\sigma \ell \). On the other hand, \( P_1 = \overline{k}.(\overline{\text{dec } h} \mid \text{dec } h.\ell) \) is not secure since the observable action \( \ell \) depends on the firing of the high action \( \overline{k} \).
Downgrading

- $P = \overline{h} \mid h.\ell$ is obviously insecure, whereas $P' = \overline{\text{dec } h} \mid \text{dec } h.\ell$ can be shown to be a secure process such that $\Gamma \models P' \equiv_{\sigma} \ell$. On the other hand, $P_1 = \overline{k}.(\overline{\text{dec } h} \mid \text{dec } h.\ell)$ is not secure since the observable action $\ell$ depends on the firing of the high action $\overline{k}$.

- $P = \overline{\text{dec } h}. \overline{h}.\overline{\text{dec } h} \mid \text{dec } h.\ell.\overline{h}.\text{dec } h$ is **secure**: a high channel can be used as a secure channel even after a downgrading,
**Downgrading**

\[ P = h \parallel h.\ell \] is obviously insecure, whereas \( P' = \text{dec } h \parallel \text{dec } h.\ell \) can be shown to be a secure process such that \( \Gamma \models P' \cong \sigma \ell \). On the other hand, \( P_1 = k.(\text{dec } h \mid \text{dec } h.\ell) \) is not secure since the observable action \( \ell \) depends on the fire of the high action \( k \).

\[ P = \text{dec } h. h.\text{dec } h \mid \text{dec } h.\overline{\ell}.\overline{h.\text{dec } h} \] is **secure**: a high channel can be used as a secure channel even after a downgrading,

\[ P = h(x).\text{if } x = n \text{ then } \ell_1 \langle \rangle \text{ else } \ell_2 \langle \rangle \mid \overline{h(n)} \mid \overline{h(m)} \] is insecure, but by declassifying the communication on the channel \( h \), we obtain \( P' = \text{dec } h(x).\text{if } x = n \text{ then } \ell_1 \langle \rangle \text{ else } \ell_2 \langle \rangle \mid \text{dec } \overline{h(n)} \mid \text{dec } \overline{h(m)} \) which is **secure**.
Conclusions

- a rich and elegant theory of noninterference intrinsic of the $\pi$-calculus, where types play a limited role

- a sound and complete characterization leading to efficient verification techniques.

- we integrated the $\pi$-calculus with a downgrading mechanism that allows a controlled information release which scales to noninterference.
Dec$\pi$-calculus

\[
\begin{align*}
\Gamma \vdash \overline{\alpha(b)}.P & \quad \Gamma \vdash a : \delta_1[\tilde{T}] \quad \delta \prec \delta_1 & \quad \Gamma \vdash a(\tilde{x} : \tilde{T}).P & \quad \Gamma \vdash a : \delta_1[\tilde{T}] \quad \delta \prec \delta_1 \\
\Gamma \vdash \overline{\text{deca}(b)}.P & \\
\end{align*}
\]

\[
\begin{align*}
\overline{\text{dec}(\tilde{m})}.P & \xrightarrow{\text{dec}(\tilde{m})} P & \text{dec}(\tilde{x} : \tilde{T}).P & \xrightarrow{\text{dec}(\tilde{m})} P\{\tilde{x} := \tilde{m}\} \\
\end{align*}
\]

\[
\begin{align*}
P & \xrightarrow{\nu \tilde{p} : \tilde{T}} \overline{\text{dec}⟨\tilde{m}⟩} & \text{dec}(\tilde{x} : \tilde{T}).P & \xrightarrow{\text{dec}(\tilde{m})} P\{\tilde{x} := \tilde{m}\} \\
QC & \text{dec}(\tilde{m}) & QC & \tilde{p} \cap \text{fn}(Q) = \emptyset \\
\end{align*}
\]

\[
\begin{align*}
P & \xrightarrow{\text{dec}⟨\tilde{m}⟩} P' & Q & \xrightarrow{\text{dec}(\tilde{m})} Q' & \tilde{p} \cap \text{fn}(Q) = \emptyset \\
\end{align*}
\]

\[
\begin{align*}
P | Q & \xrightarrow{\tau} (\nu \tilde{p} : \tilde{T})(P' | Q') \\
\end{align*}
\]
\[
\Gamma \vdash n : \delta_1 [\tilde{T}] \\
\Gamma \vdash \text{dec}_{\delta_2} n\langle \tilde{m} \rangle \cdot P \quad \xrightarrow{\delta} \quad \Gamma \vdash P
\]

\[
\Gamma \vdash n : \delta_1 [\tilde{T}] \quad \Gamma \vdash \tilde{m} : \tilde{T} \\
\Gamma \vdash \text{dec}_{\delta_2} n(\tilde{x} : \tilde{T}).P \quad \xrightarrow{\delta} \quad \Gamma \vdash P\{\tilde{x} := \tilde{m}\}
\]

\[
\Gamma, q : T \vdash P \\
\quad \xrightarrow{(\nu \tilde{p} : \tilde{T}) \text{dec}_{\delta_1} n\langle \tilde{m} \rangle} \\
\Gamma' \vdash P' \quad q \neq n, \tilde{p} \quad q \in \tilde{m}
\]

\[
\Gamma \vdash P \\
\quad \xrightarrow{(\nu q : T)(\nu \tilde{p} : \tilde{T}) \text{dec}_{\delta_1} n\langle \tilde{m} \rangle} \\
\Gamma' \vdash P' \quad q \neq n, \tilde{p} \quad q \in \tilde{m}
\]

\[
\Gamma, q : T \vdash P \\
\quad \xrightarrow{(\nu \tilde{p} : \tilde{T}) \text{dec}_{\delta_1} n\langle \tilde{m} \rangle} \\
\Gamma' \vdash P' \quad q \neq n, \tilde{p} \quad q \in \tilde{m}
\]

\[
\Gamma \vdash (\nu q : T)P \\
\quad \xrightarrow{(\nu q : T)(\nu \tilde{p} : \tilde{T}) \text{dec}_{\delta_1} n\langle \tilde{m} \rangle} \\
\Gamma' \vdash P'
\]
\[ \overline{n}(m).P \xrightarrow{\overline{n}(m)} P \quad n(x : T).P \xrightarrow{n(m)} P\{x := m\} \]

\[ P \xrightarrow{\overline{n}(m)} P' \quad Q \xrightarrow{n(m)} Q' \]

\[ P \mid Q \xrightarrow{\tau} P' \mid Q' \]

\[ (\nu m : T)P \xrightarrow{\overline{n}(m)} P' \quad m \neq n \]

\[ P \xrightarrow{(\nu m : T)\overline{n}(m)} P' \quad Q \xrightarrow{n(m)} Q' \quad m \notin \text{fn}(Q) \]

\[ P \mid Q \xrightarrow{\tau} (\nu m : T)(P' \mid Q') \]
if \( n = n \) then \( P \) else \( Q \) \( \xrightarrow{\tau} P \)

if \( n = m \) then \( P \) else \( Q \) \( \xrightarrow{\tau} Q \)

\((\text{PAR})\)

\[
P \xrightarrow{\alpha} P' \quad \text{bn}(\alpha) \cap \text{fn}(Q) = \emptyset
\]

\[
P | Q \xrightarrow{\alpha} P' | Q
\]

\((\text{RES})\)

\[
P \xrightarrow{\alpha} P' \quad n \notin \text{fn}(\alpha) \cup \text{bn}(\alpha)
\]

\[
(\nu n:T)P \xrightarrow{\alpha} (\nu n:T)P'
\]

\((\text{REP-ACT})\)

\[
P \xrightarrow{\alpha} P'
\]

\[
!P \xrightarrow{\alpha} P' | !P
\]