

A formalization of the spi calculus in Coq

Sébastien Briaïs

École Normale Supérieure de Lyon

INRIA-Microsoft Research
2007, November 29th
Orsay, FRANCE

Plan

1 The spi calculus

2 ... in Coq

3 Proofs

Plan

1 The spi calculus

2 ... in Coq

3 Proofs

The spi calculus

- Extension of the pi calculus that incorporates cryptographic messages [AG98]
- To model and study cryptographic protocols.

Syntax

- Countably infinite set of *names*.
Communication channels, nonces, atomic data, ...

- Messages

$$M, N ::= x \mid (M.N) \mid \text{Enc}_N^S M$$

- Expressions

$$E, F ::= x \mid (E.F) \mid \text{Enc}_F^S E \\ \mid \pi_1(E) \mid \pi_2(E) \mid \text{Dec}_F^S E$$

- Guards

$$\phi ::= [E=F] \mid [E:N]$$

Syntax (continued)

- Processes

$$\begin{array}{l}
 P, Q ::= \mathbf{0} \mid E(x).P \mid \bar{E}\langle F \rangle.P \\
 \quad \mid \phi P \mid (\nu x) P \\
 \quad \mid P \mid Q \mid P + Q \mid !P
 \end{array}$$

Syntax (continued)

- Processes

$$\begin{array}{l}
 P, Q ::= \mathbf{0} \mid E(x).P \mid \bar{E}\langle F \rangle.P \\
 \mid \phi P \mid (\nu x)P \\
 \mid P \mid Q \mid P + Q \mid !P
 \end{array}$$

Late LTS

INPUT $\frac{\quad}{E(x).P}$

Evaluation of expressions and guards

- Expressions :

$$\begin{array}{ll}
 \mathbf{e}_c(a) & := a \\
 \mathbf{e}_c(\text{Enc}_F^S E) & := \text{Enc}_N^S M \quad \text{if } \mathbf{e}_c(E) = M \in \mathbf{M} \\
 & \quad \text{and } \mathbf{e}_c(F) = N \in \mathbf{M} \\
 \mathbf{e}_c((E_1 . E_2)) & := (M_1 . M_2) \quad \text{if } \mathbf{e}_c(E_1) = M_1 \in \mathbf{M} \\
 & \quad \text{and } \mathbf{e}_c(E_2) = M_2 \in \mathbf{M} \\
 \mathbf{e}_c(\text{Dec}_F^S E) & := M \quad \text{if } \mathbf{e}_c(E) = \text{Enc}_N^S M \in \mathbf{M} \\
 & \quad \text{and } \mathbf{e}_c(F) = N \in \mathbf{M} \\
 \mathbf{e}_c(\pi_1(E)) & := M_1 \quad \text{if } \mathbf{e}_c(E) = (M_1 . M_2) \in \mathbf{M} \\
 \mathbf{e}_c(\pi_2(E)) & := M_2 \quad \text{if } \mathbf{e}_c(E) = (M_1 . M_2) \in \mathbf{M} \\
 \mathbf{e}_c(E) & := \perp \quad \text{otherwise}
 \end{array}$$

Late LTS

$$\text{INPUT} \frac{\mathbf{e}_c(E) = a \in \mathbf{N}}{E(x).P}$$

Late LTS

$$\text{INPUT } \frac{\mathbf{e}_c(E) = a \in \mathbf{N}}{E(x).P \xrightarrow{a}}$$

Syntax (continued)

- Processes

$$\begin{aligned}
 P, Q \quad ::= & \mathbf{0} \mid E(x).P \mid \bar{E}\langle F \rangle.P \\
 & \mid \phi P \mid (\nu x) P \\
 & \mid P \mid Q \mid P + Q \mid !P
 \end{aligned}$$

- Agents

$$\begin{aligned}
 A \quad ::= & P \\
 & \mid (x)P \\
 & \mid (\nu \tilde{z}) \langle M \rangle P \quad \text{where } \{\tilde{z}\} \subseteq n(M)
 \end{aligned}$$

Syntax (continued)

- Processes

$$\begin{aligned}
 P, Q &::= \mathbf{0} \mid E(x).P \mid \bar{E}\langle F \rangle.P \\
 &\mid \phi P \mid (\nu x)P \\
 &\mid P \mid Q \mid P + Q \mid !P
 \end{aligned}$$

- Agents

$$\begin{aligned}
 A &::= P \\
 &\mid (x)P \\
 &\mid (\nu \tilde{z}) \langle M \rangle P \quad \text{where } \{\tilde{z}\} \subseteq n(M)
 \end{aligned}$$

Late LTS

$$\text{INPUT } \frac{\mathbf{e}_c(E) = a \in \mathbf{N}}{E(x).P \xrightarrow{a}(x)P}$$

Late LTS

$$\text{INPUT } \frac{\mathbf{e}_c(E) = a \in \mathbf{N}}{E(x).P \xrightarrow{a}(x)P}$$

$$\text{OUTPUT } \frac{\mathbf{e}_c(E) = a \in \mathbf{N} \quad \mathbf{e}_c(F) = M \in \mathbf{M}}{\bar{E}\langle F \rangle.P \xrightarrow{\bar{a}} \langle M \rangle P}$$

Late LTS

$$\text{INPUT } \frac{\mathbf{e}_c(E) = a \in \mathbf{N}}{E(x).P \xrightarrow{a}(x)P}$$

$$\text{OUTPUT } \frac{\mathbf{e}_c(E) = a \in \mathbf{N} \quad \mathbf{e}_c(F) = M \in \mathbf{M}}{\bar{E}\langle F \rangle.P \xrightarrow{\bar{a}} \langle M \rangle P}$$

$$\text{CLOSE-L } \frac{P \xrightarrow{a} F \quad Q \xrightarrow{\bar{a}} C}{P | Q \xrightarrow{\tau}}$$

Operations on agents

- Pseudo-application :

If $F = (x)P$ is an abstraction and

$C = (\nu \tilde{z}) \langle M \rangle Q$ is a concretion (with $\{\tilde{z}\} \cap \text{fn}(P) = \emptyset$),

then $F \bullet C := (\nu \tilde{z}) (P\{M/x\} \mid Q)$

Late LTS

$$\text{INPUT } \frac{\mathbf{e}_c(E) = a \in N}{E(x).P \xrightarrow{a}(x)P}$$

$$\text{OUTPUT } \frac{\mathbf{e}_c(E) = a \in N \quad \mathbf{e}_c(F) = M \in M}{\bar{E}\langle F \rangle.P \xrightarrow{\bar{a}} \langle M \rangle P}$$

$$\text{CLOSE-L } \frac{P \xrightarrow{a} F \quad Q \xrightarrow{\bar{a}} C}{P | Q \xrightarrow{\tau} F \bullet C}$$

Late LTS

$$\text{INPUT } \frac{\mathbf{e}_c(E) = a \in \mathbf{N}}{E(x).P \xrightarrow{a}(x)P}$$

$$\text{OUTPUT } \frac{\mathbf{e}_c(E) = a \in \mathbf{N} \quad \mathbf{e}_c(F) = M \in \mathbf{M}}{\bar{E}\langle F \rangle.P \xrightarrow{\bar{a}} \langle M \rangle P}$$

$$\text{CLOSE-L } \frac{P \xrightarrow{a} F \quad Q \xrightarrow{\bar{a}} C}{P | Q \xrightarrow{\tau} F \bullet C}$$

$$\text{IFTHEN } \frac{P \xrightarrow{\mu} P'}{\phi P \xrightarrow{\mu} P'}$$

Evaluation of expressions and guards

- Expressions :

$$\begin{array}{ll}
 \mathbf{e}_c(a) & := a \\
 \mathbf{e}_c(\text{Enc}_F^s E) & := \text{Enc}_N^s M \quad \text{if } \mathbf{e}_c(E) = M \in \mathbf{M} \\
 & \quad \text{and } \mathbf{e}_c(F) = N \in \mathbf{M} \\
 \mathbf{e}_c((E_1 . E_2)) & := (M_1 . M_2) \quad \text{if } \mathbf{e}_c(E_1) = M_1 \in \mathbf{M} \\
 & \quad \text{and } \mathbf{e}_c(E_2) = M_2 \in \mathbf{M} \\
 \mathbf{e}_c(\text{Dec}_F^s E) & := M \quad \text{if } \mathbf{e}_c(E) = \text{Enc}_N^s M \in \mathbf{M} \\
 & \quad \text{and } \mathbf{e}_c(F) = N \in \mathbf{M} \\
 \mathbf{e}_c(\pi_1(E)) & := M_1 \quad \text{if } \mathbf{e}_c(E) = (M_1 . M_2) \in \mathbf{M} \\
 \mathbf{e}_c(\pi_2(E)) & := M_2 \quad \text{if } \mathbf{e}_c(E) = (M_1 . M_2) \in \mathbf{M} \\
 \mathbf{e}_c(E) & := \perp \quad \text{otherwise}
 \end{array}$$

- Guards :

$$\begin{array}{ll}
 \mathbf{e}([E = F]) & := \mathbf{true} \quad \text{si } \mathbf{e}_c(E) = \mathbf{e}_c(F) = M \in \mathbf{M} \\
 \mathbf{e}([E : N]) & := \mathbf{true} \quad \text{si } \mathbf{e}_c(E) = a \in \mathbf{N} \\
 \mathbf{e}(\phi) & := \mathbf{false} \quad \text{dans les autres cas}
 \end{array}$$

Late LTS

$$\text{INPUT } \frac{\mathbf{e}_c(E) = a \in \mathbf{N}}{E(x).P \xrightarrow{a}(x)P}$$

$$\text{OUTPUT } \frac{\mathbf{e}_c(E) = a \in \mathbf{N} \quad \mathbf{e}_c(F) = M \in \mathbf{M}}{\bar{E}\langle F \rangle.P \xrightarrow{\bar{a}} \langle M \rangle P}$$

$$\text{CLOSE-L } \frac{P \xrightarrow{a} F \quad Q \xrightarrow{\bar{a}} C}{P | Q \xrightarrow{\tau} F \bullet C}$$

$$\text{IFTHEN } \frac{P \xrightarrow{\mu} P'}{\phi P \xrightarrow{\mu} P'} \mathbf{e}(\phi) = \mathbf{true}$$

Late LTS

$$\text{INPUT } \frac{\mathbf{e}_c(E) = a \in \mathbf{N}}{E(x).P \xrightarrow{a}(x)P}$$

$$\text{OUTPUT } \frac{\mathbf{e}_c(E) = a \in \mathbf{N} \quad \mathbf{e}_c(F) = M \in \mathbf{M}}{\bar{E}\langle F \rangle.P \xrightarrow{\bar{a}} \langle M \rangle P}$$

$$\text{CLOSE-L } \frac{P \xrightarrow{a} F \quad Q \xrightarrow{\bar{a}} C}{P | Q \xrightarrow{\tau} F \bullet C}$$

$$\text{IFTHEN } \frac{P \xrightarrow{\mu} P'}{\phi P \xrightarrow{\mu} P'} \quad \mathbf{e}(\phi) = \mathbf{true}$$

$$\text{RES } \frac{P \xrightarrow{\mu} A}{(\nu z) P \xrightarrow{\mu} (\nu z) A} \quad z \notin n(\mu)$$

$$\text{PAR-L } \frac{P \xrightarrow{\mu} A}{P | Q \xrightarrow{\mu} A | Q}$$

+ SUM, REP- et ALPHA.

Bisimulations

Two processes are bisimilar if they can play the same transitions, i.e. they obey the game

$$\begin{array}{c} P \\ \mathcal{R} \\ Q \end{array}$$

Bisimulations

Two processes are bisimilar if they can play the same transitions, i.e. they obey the game

$$\begin{array}{c} P \xrightarrow{\mu} P' \\ \mathcal{R} \\ Q \end{array}$$

Bisimulations

Two processes are bisimilar if they can play the same transitions, i.e. they obey the game

$$\begin{array}{ccc} P & \xrightarrow{\mu} & P' \\ \mathcal{R} & & \\ Q & \dashrightarrow^{\mu} & Q' \end{array}$$

Bisimulations

Two processes are bisimilar if they can play the same transitions, i.e. they obey the game

$$\begin{array}{ccc} P & \xrightarrow{\mu} & P' \\ \mathcal{R} & & \mathcal{R} \\ Q & \dashrightarrow^{\mu} & Q' \end{array}$$

Bisimulations

Two processes are bisimilar if they can play the same transitions, i.e. they obey the game

$$\begin{array}{ccc}
 P & \xrightarrow{\mu} & P' \\
 \mathcal{R} & & \mathcal{R} \\
 Q & \dashrightarrow^{\mu} & Q'
 \end{array}$$

and

$$\begin{array}{ccc}
 Q & \xrightarrow{\mu} & Q' \\
 \mathcal{R} & & \mathcal{R} \\
 P & \dashrightarrow^{\mu} & P'
 \end{array}$$

Bisimulations in the spi calculus

- Bisimulations of pi calculus are too fine-grained.
- Indeed, if $P(c, M) := (\nu k) \bar{c} \langle \text{Enc}_k^s M \rangle. \mathbf{0}$ (where $k \notin \{c\} \cup n(M)$)
 Requiring an exact match between actions makes distinguish $P(c, M)$ from $P(c, N)$.
 Whereas these two processes should be considered equivalent (since the encryption key is not disclosed to the environment).
- Environment-sensitive bisimulations : extend the notion of bisimulation with a data structure to encode environment knowledge.
- Framed bisimulation (Abadi, Gordon), alley bisimulation (Boreale et al.), hedged bisimulation (Borgström, Nestmann), ...

The attacker knowledge represented as hedges

- A hedge $h \in \mathbf{H}$ is a finite set of pairs of messages.
- Intuitively $(M, N) \in h$ means that M and N are indistinguishable.

Late hedged bisimulation

A **symmetric** hedged relation \mathcal{R}

Hedged relations

- A **hedged relation** \mathcal{R} is a subset of $\mathbf{H} \times \mathbf{P} \times \mathbf{P}$ such that whenever $(h, P, Q) \in \mathcal{R}$, we have $\text{fn}(P) \subseteq n(\pi_1(h))$ and $\text{fn}(Q) \subseteq n(\pi_2(h))$.
- A hedged relation \mathcal{R} is **symmetric** if whenever $(h, P, Q) \in \mathcal{R}$ we have $(h^{-1}, Q, P) \in \mathcal{R}$.

Late hedged bisimulation

A symmetric hedged relation \mathcal{R} is a *(strong) late hedged bisimulation* if whenever $(h, P, Q) \in \mathcal{R}$, we have that

- 1 if $P \xrightarrow{\tau} P'$ then
there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $(h, P', Q') \in \mathcal{R}$

Late hedged bisimulation

A symmetric hedged relation \mathcal{R} is a (*strong*) *late hedged bisimulation* if whenever $(h, P, Q) \in \mathcal{R}$, we have that

- 1 if $P \xrightarrow{\tau} P'$ then
there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $(h, P', Q') \in \mathcal{R}$
- 2 if $P \xrightarrow{a} (x)P'$ (with $x \notin n(\pi_1(h))$)
then

Late hedged bisimulation

A symmetric hedged relation \mathcal{R} is a (*strong*) *late hedged bisimulation* if whenever $(h, P, Q) \in \mathcal{R}$, we have that

- 1 if $P \xrightarrow{\tau} P'$ then
there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $(h, P', Q') \in \mathcal{R}$
- 2 if $P \xrightarrow{a} (x)P'$ (with $x \notin n(\pi_1(h))$)
then
there exist y and Q' such that $Q \xrightarrow{a} (y)Q'$
(with $y \notin n(\pi_2(h))$)

Late hedged bisimulation

A symmetric hedged relation \mathcal{R} is a (*strong*) *late hedged bisimulation* if whenever $(h, P, Q) \in \mathcal{R}$, we have that

- 1 if $P \xrightarrow{\tau} P'$ then
there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $(h, P', Q') \in \mathcal{R}$
- 2 if $P \xrightarrow{a} (x)P'$ (with $x \notin n(\pi_1(h))$)
and $(a, b) \in h$ then
there exist y and Q' such that $Q \xrightarrow{b} (y)Q'$
(with $y \notin n(\pi_2(h))$)

Late hedged bisimulation

A symmetric hedged relation \mathcal{R} is a *(strong) late hedged bisimulation* if whenever $(h, P, Q) \in \mathcal{R}$, we have that

- 1 if $P \xrightarrow{\tau} P'$ then
there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $(h, P', Q') \in \mathcal{R}$
- 2 if $P \xrightarrow{a} (x)P'$ (with $x \notin n(\pi_1(h))$)
and $(a, b) \in h$ then
there exist y and Q' such that $Q \xrightarrow{b} (y)Q'$
(with $y \notin n(\pi_2(h))$)
and for all M
we have $(h, P'\{M/x\}, Q'\{M/y\}) \in \mathcal{R}$.

The attacker knowledge represented as hedges

- A hedge $h \in \mathbf{H}$ is a finite set of pairs of messages.
- Intuitively $(M, N) \in h$ means that M and N are indistinguishable.
- The synthesis $\mathcal{S}(h)$ of a hedge h

$$\text{SYN-INC} \frac{(M, N) \in h}{(M, N) \in \mathcal{S}(h)}$$

$$\text{SYN-ENC-S} \frac{(M_1, N_1) \in \mathcal{S}(h) \quad (M_2, N_2) \in \mathcal{S}(h)}{(\text{Enc}_{M_2}^s M_1, \text{Enc}_{N_2}^s N_1) \in \mathcal{S}(h)}$$

$$\text{SYN-PAIR} \frac{(M_1, N_1) \in \mathcal{S}(h) \quad (M_2, N_2) \in \mathcal{S}(h)}{((M_1 \cdot M_2), (N_1 \cdot N_2)) \in \mathcal{S}(h)}$$

Late hedged bisimulation

A symmetric hedged relation \mathcal{R} is a (*strong*) *late hedged bisimulation* if whenever $(h, P, Q) \in \mathcal{R}$, we have that

- 1 if $P \xrightarrow{\tau} P'$ then
there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $(h, P', Q') \in \mathcal{R}$
- 2 if $P \xrightarrow{a} (x)P'$ (with $x \notin n(\pi_1(h))$)
and $(a, b) \in h$ then
there exist y and Q' such that $Q \xrightarrow{b} (y)Q'$
(with $y \notin n(\pi_2(h))$)
and for all $(M, N) \in \mathcal{S}(h)$
we have $(h, P'\{M/x\}, Q'\{N/y\}) \in \mathcal{R}$.

Late hedged bisimulation

A symmetric hedged relation \mathcal{R} is a (*strong*) *late hedged bisimulation* if whenever $(h, P, Q) \in \mathcal{R}$, we have that

- 1 if $P \xrightarrow{\tau} P'$ then
there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $(h, P', Q') \in \mathcal{R}$
- 2 if $P \xrightarrow{a} (x)P'$ (with $x \notin n(\pi_1(h))$)
and $(a, b) \in h$ then
there exist y and Q' such that $Q \xrightarrow{b} (y)Q'$
(with $y \notin n(\pi_2(h))$)
and for all B and (M, N) such that $h \vdash_B (M, N)$
we have $(h \cup B, P' \{M/x\}, Q' \{N/y\}) \in \mathcal{R}$.

Late hedged bisimulation

A symmetric hedged relation \mathcal{R} is a (*strong*) *late hedged bisimulation* if whenever $(h, P, Q) \in \mathcal{R}$, we have that

- 1 if $P \xrightarrow{\tau} P'$ then
there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $(h, P', Q') \in \mathcal{R}$
- 2 if $P \xrightarrow{a} (x)P'$ (with $x \notin n(\pi_1(h))$)
and $(a, b) \in h$ then
there exist y and Q' such that $Q \xrightarrow{b} (y)Q'$
(with $y \notin n(\pi_2(h))$)
and for all B and (M, N) such that $h \vdash_B (M, N)$
we have $(h \cup B, P' \{M/x\}, Q' \{N/y\}) \in \mathcal{R}$.
- 3 if $P \xrightarrow{\bar{a}} (\nu \tilde{c}) \langle M \rangle P'$ (with $\{\tilde{c}\} \cap n(\pi_1(h)) = \emptyset$)
and $(a, b) \in h$ then
there exist $\{\tilde{d}\}$, Q' and N such that $Q \xrightarrow{\bar{b}} (\nu \tilde{d}) \langle N \rangle Q'$
(with $\{\tilde{d}\} \cap n(\pi_2(h)) = \emptyset$)

Late hedged bisimulation

A symmetric hedged relation \mathcal{R} is a (*strong*) *late hedged bisimulation* if whenever $(h, P, Q) \in \mathcal{R}$, we have that

- 1 if $P \xrightarrow{\tau} P'$ then
there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $(h, P', Q') \in \mathcal{R}$
- 2 if $P \xrightarrow{a} (x)P'$ (with $x \notin n(\pi_1(h))$)
and $(a, b) \in h$ then
there exist y and Q' such that $Q \xrightarrow{b} (y)Q'$
(with $y \notin n(\pi_2(h))$)
and for all B and (M, N) such that $h \vdash_B (M, N)$
we have $(h \cup B, P' \{M/x\}, Q' \{N/y\}) \in \mathcal{R}$.
- 3 if $P \xrightarrow{\bar{a}} (\nu \tilde{c}) \langle M \rangle P'$ (with $\{\tilde{c}\} \cap n(\pi_1(h)) = \emptyset$)
and $(a, b) \in h$ then
there exist $\{\tilde{d}\}$, Q' and N such that $Q \xrightarrow{\bar{b}} (\nu \tilde{d}) \langle N \rangle Q'$
(with $\{\tilde{d}\} \cap n(\pi_2(h)) = \emptyset$)
and $(h \cup \{(M, N)\}, P', Q') \in \mathcal{R}$.

Analysis of a hedge

- The analysis $\mathcal{A}(h)$ is the smallest hedge that is closed by $\text{analz}(\cdot)$.

$$\text{ANA-INC} \frac{(M, N) \in h}{(M, N) \in \text{analz}(h)}$$

$$\text{ANA-DEC-S} \frac{(\text{Enc}_{M_2}^s M_1, \text{Enc}_{N_2}^s N_1) \in \text{analz}(h) \quad (M_2, N_2) \in \mathcal{S}(h)}{(M_1, N_1) \in \text{analz}(h)}$$

$$\text{ANA-FST} \frac{((M_1 \cdot M_2), (N_1 \cdot N_2)) \in \text{analz}(h)}{(M_1, N_1) \in \text{analz}(h)}$$

$$\text{ANA-SND} \frac{((M_1 \cdot M_2), (N_1 \cdot N_2)) \in \text{analz}(h)}{(M_2, N_2) \in \text{analz}(h)}$$

Late hedged bisimulation

A symmetric hedged relation \mathcal{R} is a (*strong*) *late hedged bisimulation* if whenever $(h, P, Q) \in \mathcal{R}$, we have that

- 1 if $P \xrightarrow{\tau} P'$ then
there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $(h, P', Q') \in \mathcal{R}$
- 2 if $P \xrightarrow{a} (x)P'$ (with $x \notin n(\pi_1(h))$)
and $(a, b) \in h$ then
there exist y and Q' such that $Q \xrightarrow{b} (y)Q'$
(with $y \notin n(\pi_2(h))$)
and for all B and (M, N) such that $h \vdash_B (M, N)$
we have $(h \cup B, P' \{M/x\}, Q' \{N/y\}) \in \mathcal{R}$.
- 3 if $P \xrightarrow{\bar{a}} (\nu \tilde{c}) \langle M \rangle P'$ (with $\{\tilde{c}\} \cap n(\pi_1(h)) = \emptyset$)
and $(a, b) \in h$ then
there exist $\{\tilde{d}\}$, Q' and N such that $Q \xrightarrow{\bar{b}} (\nu \tilde{d}) \langle N \rangle Q'$
(with $\{\tilde{d}\} \cap n(\pi_2(h)) = \emptyset$)
and $(\mathcal{A}(h \cup \{(M, N)\}), P', Q') \in \mathcal{R}$.

Irreducibles

- $\mathcal{I}(h)$ is the smallest hedge such that $\mathcal{S}(\mathcal{I}(h)) = \mathcal{S}(\mathcal{A}(h))$.
- A hedge h is irreducible iff $\mathcal{I}(h) = h$

Late hedged bisimulation

A symmetric hedged relation \mathcal{R} is a (*strong*) *late hedged bisimulation* if whenever $(h, P, Q) \in \mathcal{R}$, we have that

- 1 if $P \xrightarrow{\tau} P'$ then
there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $(h, P', Q') \in \mathcal{R}$
- 2 if $P \xrightarrow{a} (x)P'$ (with $x \notin n(\pi_1(h))$)
and $(a, b) \in h$ then
there exist y and Q' such that $Q \xrightarrow{b} (y)Q'$
(with $y \notin n(\pi_2(h))$)
and for all B and (M, N) such that $h \vdash_B (M, N)$
we have $(h \cup B, P' \{M/x\}, Q' \{N/y\}) \in \mathcal{R}$.
- 3 if $P \xrightarrow{\bar{a}} (\nu \tilde{c}) \langle M \rangle P'$ (with $\{\tilde{c}\} \cap n(\pi_1(h)) = \emptyset$)
and $(a, b) \in h$ then
there exist $\{\tilde{d}\}$, Q' and N such that $Q \xrightarrow{\bar{b}} (\nu \tilde{d}) \langle N \rangle Q'$
(with $\{\tilde{d}\} \cap n(\pi_2(h)) = \emptyset$)
and $(\mathcal{I}(h \cup \{(M, N)\}), P', Q') \in \mathcal{R}$.

Irreducibles, consistency

- $\mathcal{I}(h)$ is the smallest hedge such that $\mathcal{S}(\mathcal{I}(h)) = \mathcal{S}(\mathcal{A}(h))$.
- A hedge h is irreducible iff $\mathcal{I}(h) = h$
- A hedge h is consistent iff :
Whenever $(M, N) \in h$
 - ▶ $M \in \mathbf{N} \iff N \in \mathbf{N}$
 - ▶ whenever $(M', N') \in h : M = M' \iff N = N'$
 - ▶ $M \neq (M_1 . M_2)$ and $N \neq (N_1 . N_2)$
 - ▶ if $M = \text{Enc}_{M_2}^s M_1$ then $(M_2, N_2) \notin \mathcal{S}(h)$
 - ▶ if $N = \text{Enc}_{N_2}^s N_1$ then $(M_2, N_2) \notin \mathcal{S}(h)$
- A consistent hedge is irreducible.

Hedged relations

- A hedged relation \mathcal{R} is a subset of $\mathbf{H} \times \mathbf{P} \times \mathbf{P}$ such that whenever $(h, P, Q) \in \mathcal{R}$, we have $\text{fn}(P) \subseteq n(\pi_1(h))$ and $\text{fn}(Q) \subseteq n(\pi_2(h))$.
- A hedged relation \mathcal{R} is *symmetric* if whenever $(h, P, Q) \in \mathcal{R}$ we have $(h^{-1}, Q, P) \in \mathcal{R}$.
- A hedged relation \mathcal{R} is *consistent* if whenever $(h, P, Q) \in \mathcal{R}$, we have that h is a consistent hedge.

Late hedged bisimulation

A symmetric **consistent** hedged relation \mathcal{R} is a (*strong*) *late hedged bisimulation* if whenever $(h, P, Q) \in \mathcal{R}$, we have that

- 1 if $P \xrightarrow{\tau} P'$ then
there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $(h, P', Q') \in \mathcal{R}$
- 2 if $P \xrightarrow{a} (x)P'$ (with $x \notin n(\pi_1(h))$)
and $(a, b) \in h$ then
there exist y and Q' such that $Q \xrightarrow{b} (y)Q'$
(with $y \notin n(\pi_2(h))$)
and for all B and (M, N) such that $h \vdash_B (M, N)$
we have $(h \cup B, P' \{M/x\}, Q' \{N/y\}) \in \mathcal{R}$.
- 3 if $P \xrightarrow{\bar{a}} (\nu \tilde{c}) \langle M \rangle P'$ (with $\{\tilde{c}\} \cap n(\pi_1(h)) = \emptyset$)
and $(a, b) \in h$ then
there exist $\{\tilde{d}\}$, Q' and N such that $Q \xrightarrow{\bar{b}} (\nu \tilde{d}) \langle N \rangle Q'$
(with $\{\tilde{d}\} \cap n(\pi_2(h)) = \emptyset$)
and $(\mathcal{I}(h \cup \{(M, N)\}), P', Q') \in \mathcal{R}$.

A word on open hedged bisimulation

- We have defined an open variant of late hedged bisimulation, following Sangiorgi's idea of open bisimulation in the pi calculus.
- The idea is to move the instantiation of input names before the transitions take place.
- For instance, the input clause roughly becomes

$$(\sigma, \rho) \triangleright_B se \quad \begin{array}{ccccc} P & P\sigma & \xrightarrow{a} & (x)P' & P' \\ | & & & & | \\ Q & Q\rho & \xrightarrow{b} & (y)Q' & Q' \end{array}$$

A symbolic LTS

- *Idea* : record without checking the conditions needed to enable transitions.

$$\text{S-INPUT} \frac{}{E(x).P \xrightarrow[\{\{E:\mathbf{N}\}\}]{\mathbf{e}_a(E)} (x)P}$$

$$\text{S-OUTPUT} \frac{}{\overline{E}\langle F \rangle.P \xrightarrow[\{\{E:\mathbf{N}\},\{F:\mathbf{M}\}\}]{\overline{\mathbf{e}_a(E)}} \langle \mathbf{e}_a(F) \rangle P}$$

Abstract (or symbolic) evaluation of expressions :

$$\begin{array}{ll}
 \mathbf{e}_a(a) & := a & \text{if } a \in \mathbf{N} \\
 \mathbf{e}_a(\text{Enc}_F^s E) & := \text{Enc}_{\mathbf{e}_a(F)}^s \mathbf{e}_a(E) \\
 \mathbf{e}_a((E . F)) & := (\mathbf{e}_a(E) . \mathbf{e}_a(F)) \\
 \mathbf{e}_a(\text{Dec}_F^s E) & := E_1 & \text{if } \mathbf{e}_a(E) = \text{Enc}_{E_2}^s E_1 \\
 & \text{Dec}_{\mathbf{e}_a(F)}^s \mathbf{e}_a(E) & \text{otherwise} \\
 \mathbf{e}_a(\pi_1(E)) & := E_1 & \text{if } \mathbf{e}_a(E) = (E_1 . E_2) \\
 & \pi_1(\mathbf{e}_a(E)) & \text{otherwise} \\
 \mathbf{e}_a(\pi_2(E)) & := E_2 & \text{if } \mathbf{e}_a(E) = (E_1 . E_2) \\
 & \pi_2(\mathbf{e}_a(E)) & \text{otherwise}
 \end{array}$$

$$\text{S-INPUT} \frac{}{E(x).P \xrightarrow[\{\{E:\mathbf{N}\}\}]{e_a(E)} (x)P}$$

$$\text{S-OUTPUT} \frac{}{\overline{E}\langle F \rangle.P \xrightarrow[\{\{E:\mathbf{N}\},\{F:\mathbf{M}\}\}]{\overline{e_a(E)}} \langle e_a(F) \rangle P}$$

$$\text{S-GUARD} \frac{P \xrightarrow[c]{\mu} A}{\phi P \xrightarrow[c \& \{\phi\}]{\mu} A}$$

$$\text{S-CLOSE-L} \frac{P \xrightarrow[c_1]{E} F \quad Q \xrightarrow[c_2]{\overline{E'}} C}{P \mid Q \xrightarrow[\{\{E=E'\}\} \& c_1 \& c_2]{\tau} F \bullet C}$$

$$\text{S-INPUT} \frac{}{E(x).P \xrightarrow[\{\{E:\mathbf{N}\}\}]{e_a(E)} (x)P}$$

$$\text{S-OUTPUT} \frac{}{\overline{E}\langle F \rangle.P \xrightarrow[\{\{E:\mathbf{N}\},\{F:\mathbf{M}\}\}]{\overline{e_a(E)}} \langle e_a(F) \rangle P}$$

$$\text{S-GUARD} \frac{P \xrightarrow[c]{\mu} A}{\phi P \xrightarrow[c \& \{\phi\}]{\mu} A}$$

$$\text{S-CLOSE-L} \frac{P \xrightarrow[c_1]{E} F \quad Q \xrightarrow[c_2]{\overline{E'}} C}{P \mid Q \xrightarrow[\{\{E=E'\}\} \& c_1 \& c_2]{\tau} F \bullet C}$$

$$\text{S-RES} \frac{P \xrightarrow[c]{\mu} A}{(\nu z) P \xrightarrow[\nu_+(z,c)]{\mu} (\nu z) A} \quad z \notin n(\mu)$$

Plan

1 The spi calculus

2 ... in Coq

3 Proofs

Why formalize in Coq ?

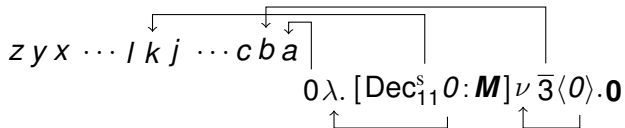
- *Dream* :
extract a certified (correct by construction) bisimulation checker.
- Validate hand-written proofs.
- Provide an interactive framework to reason formally about cryptographic protocols within the spi calculus model.
- It's fun !

Representation of binders

- There exist several techniques to encode binders :
 - ▶ de Bruijn indices
 - ▶ locally nameless
 - ▶ higher-order abstract syntax
 - ▶ nominal
- We have chosen de Bruijn representation.

de Bruijn representation

Representation of $a(x).[Dec_k^s x : \mathbf{M}](\nu l) \bar{b}\langle l \rangle. \mathbf{0}$:



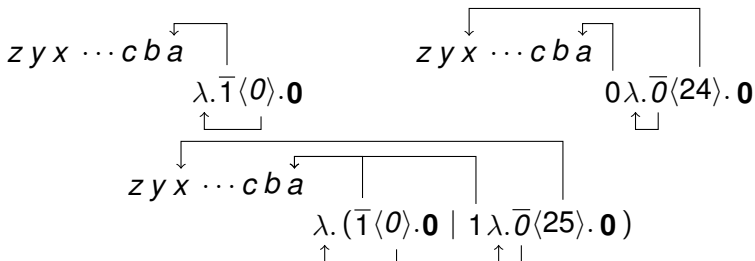
Operations on de Bruijn indices

- Parametrised by the binding depth d
- $\text{mem}_d(i, t)$ returns **true** iff i is free in t
- $\text{lift}_d(k, t)$ makes room for k new binders in t

Used in parallel composition of an agent and a process :

$$\begin{aligned}
 (\lambda.P) \mid Q &::= \lambda.(P \mid \text{lift}_0(1, Q)) \\
 (\nu^k \langle F \rangle P) \mid Q &::= \nu^k \langle F \rangle (P \mid \text{lift}_0(k, Q))
 \end{aligned}$$

For instance :



- $\text{swap}_d(k, t)$ makes a circular permutation of the k first indices in t
- $\text{low}_d(t)$ removes the first index
- Used in restriction of an agent :

$$\begin{aligned} \nu(\lambda.P) &:= \lambda.\nu \text{swap}_0(1, P) \\ \nu(\nu^k \langle F \rangle P) &:= \nu^{k+1} \langle F \rangle P && \text{if } \text{mem}_k(0, F) = \mathbf{true} \\ &:= \nu^k \langle \text{low}_k(F) \rangle \nu \text{swap}_0(k, P) && \text{otherwise} \end{aligned}$$

- $\text{lsubst}_d(k, \bar{E}, t)$ substitutes the $|\bar{E}|$ first indices with the corresponding expression of \bar{E} in t . The k first indices are bound in \bar{E} .

$$(\lambda.P) \bullet (\nu^k \langle F \rangle Q) := \nu^k (\text{lsubst}_0(k, F, P) | Q)$$

Concretely in Coq

- We have several types :
names, messages, expressions, guards, processes, agents.
- These “de Bruijn” operations should be defined for each of these types, i.e. :

```

Definition name_lift
  (d:nat) (k:nat) (x:name) : name := ...
Definition message_lift ...
Definition expression_lift ...
Definition formula_lift ...
Definition process_lift ...
Definition agent_lift ...

```

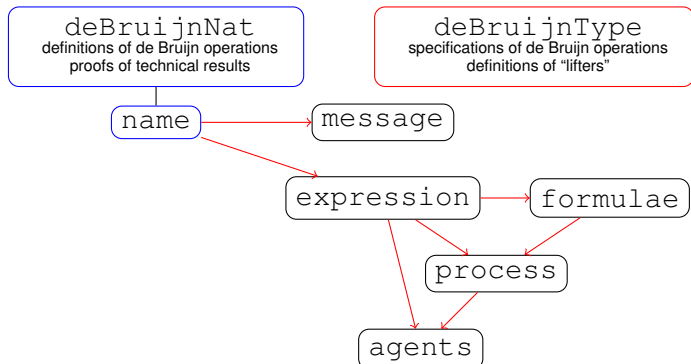
and similarly for the other operations.

- Moreover, several (about 60) facts hold for these operations.
For instance, we have :

$$\forall d, d', k, k', x : \text{swap}_{d+k+d'}(k', \text{lift}_d(k, x)) = \text{lift}_d(k, \text{swap}_{d+d'}(k', x))$$

Abstracting de Bruijn indices

- Not scalable and tedious.
- Instead, define and specify all these operations on names
- and lift them to other types thanks to “good” iterators.
- In practice :



Asbtracting the LTS

- There are several LTS to define.
- Some properties are shared (for instance, structural congruence preserves the semantics)
- These LTS all follow the same pattern.
- Instead of defining each LTS separately, we make a functor and thus defer the definition of the semantics to the definitions of the semantics of actions.

Actions

We rely on a set of actions \mathcal{A} and several functions to manipulate them :

- $\text{mkSil} : \mathcal{A}$ (silent)
- $\text{mkInp} : \mathbf{E} \rightarrow \mathcal{A} \cup \{\perp\}$ (input)
- $\text{mkOutp} : \mathbf{E} \times \mathbf{E} \rightarrow (\mathcal{A} \times \mathbf{E}) \cup \{\perp\}$ (output)
- $\text{mkRes} : \mathcal{A} \rightarrow \mathcal{A} \cup \{\perp\}$ (restriction)
- $\text{mkIf} : \mathbf{F} \times \mathcal{A} \rightarrow \mathcal{A} \cup \{\perp\}$ (guard)
- $\text{mkInt} : \mathcal{A} \times \mathcal{A} \rightarrow \mathcal{A} \cup \{\perp\}$ (interact)

The functor that defines an LTS

$$\text{SILENT} \frac{}{\tau.P \xrightarrow{\text{mkSil}} P} \qquad \text{INPUT} \frac{\text{mkInp}(E) = \alpha \in \mathcal{A}}{E\lambda.P \xrightarrow{\alpha} \lambda.P}$$

$$\text{OUTPUT} \frac{\text{mkOutp}(E, F) = (\alpha, M) \in \mathcal{A} \times \mathbf{E}}{\bar{E}\langle F \rangle.P \xrightarrow{\alpha} \langle M \rangle P}$$

$$\text{CLOSE-L} \frac{P \xrightarrow{\alpha} F \quad Q \xrightarrow{\beta} C \quad \text{mkInt}(\alpha, \beta) = \gamma \in \mathcal{A}}{P | Q \xrightarrow{\gamma} F \bullet C}$$

$$\text{RES} \frac{P \xrightarrow{\alpha} A \quad \text{mkRes}(\alpha) = \beta \in \mathcal{A}}{\nu P \xrightarrow{\beta} \nu A}$$

$$\text{IFTHEN} \frac{P \xrightarrow{\alpha} P' \quad \text{mkIf}(\phi, \alpha) = \beta \in \mathcal{A}}{\phi P \xrightarrow{\beta} P'}$$

$$\text{PAR-L} \frac{P \xrightarrow{\alpha} A}{P | Q \xrightarrow{\alpha} A | Q}$$

$$\text{SUM-L} \frac{P \xrightarrow{\alpha} A}{P + Q \xrightarrow{\alpha} A}$$

$$\text{REP-ACT} \frac{P \xrightarrow{\alpha} A}{!P \xrightarrow{\alpha} A | !P}$$

$$\text{REP-CLOSE} \frac{P \xrightarrow{\alpha} F \quad P \xrightarrow{\beta} C \quad \text{mkInt}(\alpha, \beta) = \gamma \in \mathcal{A}}{!P \xrightarrow{\gamma} (F \bullet C) | !P}$$

Plan

- 1 The spi calculus
- 2 ... in Coq
- 3 Proofs**

Structural congruence preserves the semantics

- $P \equiv Q$ iff P and Q represents intuitively the same process.
For instance, $(\mathbf{P}, +, \mathbf{0})$ and $(\mathbf{P}, |, \mathbf{0})$ are monoids.
- We extend this definition to agents.
- A classical result is

Theorem

If $P \equiv Q$ and $P \xrightarrow{\mu} A$ then there exists B such that $A \equiv B$ and $Q \xrightarrow{\mu} B$.

- This theorem constitutes a good crash test for our formalization.
- With our definitions, we show

Theorem

If the set of actions \mathcal{A} and the functions mkSil , mkInp , \dots satisfy some conditions, then if $P \equiv Q$ and $P \xrightarrow{\alpha} A$ then there exist β and B such that $A \equiv B$, $Q \xrightarrow{\beta} B$ and $\alpha = \beta$.

- This theorem constitutes a good crash test for our formalization.
- With our definitions, we show

Theorem

If the set of actions \mathcal{A} and the functions mkSil , mkInp , \dots satisfy some conditions, then if $P \equiv Q$ and $P \xrightarrow{\alpha} A$ then there exist β and B such that $A \equiv B$, $Q \xrightarrow{\beta} B$ and $\alpha = \beta$.

- Thanks to our formalization, we have noticed that this result does not hold for the symbolic LTS!

Indeed let $P := (\nu x) x(z). \mathbf{0}$ and $Q := \bar{y}\langle k \rangle. \mathbf{0}$.

We have $P \mid Q \equiv (\nu x) (x(z). \mathbf{0} \mid \bar{y}\langle k \rangle. \mathbf{0})$.

$P \mid Q$ cannot perform any internal transition whereas

$$(\nu x) (x(z). \mathbf{0} \mid \bar{y}\langle k \rangle. \mathbf{0}) \xrightarrow[\text{(\nu x) } \{[x: \mathbf{N}], [y: \mathbf{N}], [x=y], [k: \mathbf{M}]\}]{\tau} (\nu x) (\mathbf{0} \mid \mathbf{0})$$

Back to the analysis

- We defined the analysis $\mathcal{A}(h)$ as being the smallest hedge that is closed by $\text{analz}(\cdot)$.
- In Coq, this requires some work to show that this definition makes sense.
- To show the existence, we exhibit a multiset that strictly decreases.
- Fortunately, the CoLoR library shows that multiset ordering is well-founded.

A small example of bisimulation

- Define $P(c, M) := (\nu k) \bar{c} \langle \text{Enc}_k^s M \rangle. \mathbf{0}$ where $k \notin \{c\} \cup n(M)$.
- We show that for any c, M and N we have $P(c, M) \sim_{\text{LH}}^h P(c, N)$ where $h = \mathcal{I}(\{(c, c), (M, M), (N, N)\})$.
- In Coq : $P(c, M) := \nu \overline{\text{lift}_0(1, c)} \langle \text{Enc}_0^s \text{lift}_0(1, M) \rangle. \mathbf{0}$.
- We exhibit a late hedged bisimulation.

$$\begin{aligned} \mathcal{R} := & \{ (h_0(c, M, N), P(c, M), P(c, N)) \} \\ & \cup \{ (h_1(c, M, N, k, k), \mathbf{0}, \mathbf{0}) \mid k \notin n(h_0(c, M, N)) \} \\ & \cup \{ (h_0(c, N, M), P(c, N), P(c, M)) \} \\ & \cup \{ (h_1(c, N, M, k, k), \mathbf{0}, \mathbf{0}) \mid k \notin n(h_0(c, N, M)) \} \end{aligned}$$

where

$$\begin{aligned} h_0(c, M, N) &:= \mathcal{I}(\{(c, c), (M, M), (N, N)\}) \\ h_1(c, M, N, k, l) &:= h_0 \cup \{ (\text{Enc}_k^s M, \text{Enc}_k^s N) \} \end{aligned}$$

A variant

- Define $Q(c, M, M') = (\nu k) \bar{c}\langle \text{Enc}_k^s M \rangle . \bar{c}\langle \text{Enc}_k^s M' \rangle . \mathbf{0}$ where $k \notin \{c\} \cup n(M, M')$.
- We show that for any c, M, N and N' , if $N \neq N'$ then there is no hedge h such that $(c, c) \in h$ (i.e. the channel c is known by the attacker) and $Q(c, M, M) \sim_{\text{LH}}^h Q(c, N, N')$.
- The proof proceeds by contradiction.

$$h' := \mathcal{I}(h \cup \{\text{Enc}_k^s M, \text{Enc}_l^s N\})$$

$$h'' := \mathcal{I}(h' \cup \{\text{Enc}_k^s M, \text{Enc}_l^s N'\})$$

At some point, we have that h'' is consistent. This implies necessarily that $N = N'$.

Conclusion

- We have formalized an “abstract” pi calculus

$$\begin{array}{l}
 P, Q ::= \mathbf{0} \mid P + Q \\
 \quad \mid P \mid Q \mid !P \\
 \quad \mid (\nu X) P \mid \tau.P \\
 \quad \mid E(x).P \mid \bar{E}\langle F \rangle.P \\
 \quad \mid \phi P
 \end{array}$$

- and have made two instantiations of this calculus :
monadic pi calculus and spi calculus.
- We have shown a general theorem about structural congruence.
- We have defined 3 LTS for the spi calculus and studied their properties.
We have thus fixed several errors in the handwritten proofs.
- We have formalized the hedges and then defined late hedged bisimulation in Coq.

Future work

- Continue the formalization until realizing our dream of having a correct-by-construction bisimulation checker.
- Test our de Bruijn “library” on other formalisms (POPLMark ?)
- Develop tactics to ease reasoning in Coq with our framework.

Thanks !
Questions ?

Bibliography

 [D. Sangiorgi](#)
A Theory of Bisimulation for the π -calculus.

 [M. Abadi and A. Gordon](#)
A Calculus for Cryptographic Protocols : The Spi Calculus

 [J. Borgström, S. Briaïs and U. Nestmann](#)
Symbolic Bisimulations in the Spi Calculus

 [S. Briaïs and U. Nestmann](#)
Open Bisimulation, Revisited

Operations on agents

- Pseudo-application :

If $F = (x)P$ is an abstraction and

$C = (\nu\tilde{z}) \langle M \rangle Q$ is a concretion (with $\{\tilde{z}\} \cap \text{fn}(P) = \emptyset$),

then $F \bullet C := (\nu\tilde{z}) (P\{M/x\} \mid Q)$

- Restriction :

$$(\nu x) P := (\nu x) P$$

$$(\nu x) ((y)P) := (y)(\nu x) P \quad \text{if } y \neq x$$

$$(\nu x) ((\nu\tilde{z}) \langle M \rangle P) := (\nu\tilde{z}) \langle M \rangle (\nu x) P \quad \text{if } y \notin \{\tilde{z}\} \text{ and } x \notin n(M)$$

$$(\nu x) ((\nu\tilde{z}) \langle M \rangle P) := (\nu x\tilde{z}) \langle M \rangle P \quad \text{if } y \notin \{\tilde{z}\} \text{ and } x \in n(M)$$

- Parallel composition :

$$((x)P) \mid Q := (x)(P \mid Q) \quad \text{if } x \notin \text{fn}(Q)$$

$$((\nu\tilde{z}) \langle M \rangle P) \mid Q := (\nu\tilde{z}) \langle M \rangle (P \mid Q) \quad \text{if } \{\tilde{z}\} \cap \text{fn}(Q) = \emptyset$$

Possible inputs

Let $h \in \mathbf{H}$, $(M, N) \in \mathbf{M} \times \mathbf{M}$

Let $B \subseteq \mathbf{N} \times \mathbf{N}$ a consistent hedge such that

- $\pi_1(B) \cap n(\pi_1(h)) = \emptyset$
- $\pi_2(B) \cap n(\pi_2(h)) = \emptyset$

i.e. the names of B are fresh component-wise w.r.t. those of h .

We write $h \vdash_B (M, N)$ if

- $\forall (b_1, b_2) \in B : b_1 \in n(M) \vee b_2 \in n(N)$
- $(M, N) \in \mathcal{S}(h \cup B)$

A LTS that collects type constraints

$$\text{NC-SILENT} \frac{}{\tau.P \xrightarrow[\emptyset]{\tau} P} \quad \text{NC-INPUT} \frac{\mathbf{e}_c(E) = a \in \mathbf{N}}{E(x).P \xrightarrow[\{a\}]{a} (x)P}$$

$$\text{NC-OUTPUT} \frac{\mathbf{e}_c(E) = a \in \mathbf{N} \quad \mathbf{e}_c(F) = M \in \mathbf{M}}{\bar{E}\langle F \rangle.P \xrightarrow[\{a\}]{\bar{a}} \langle M \rangle P}$$

$$\text{NC-IFTHEN} \frac{P \xrightarrow[S]{\mu} A}{\phi P \xrightarrow[\text{Sunc}(\phi)]{\mu} A} \quad \mathbf{e}(\phi) = \mathbf{true}$$

where $\mathbf{nc}([E : \mathbf{N}]) := \{\mathbf{e}_c(E)\}$ and $\mathbf{nc}([E = F]) := \emptyset$.

Theorem

The two semantics are equivalent :

- 1 If $P \xrightarrow{\mu} A$ there exists $S \subseteq \mathbf{N}$ such that $P \xrightarrow[S]{\mu} A$.
- 2 If $P \xrightarrow[S]{\mu} A$ then $P \xrightarrow{\mu} A$.

Lemma

If $P \xrightarrow[S]{\mu} A$ and $\sigma : \mathbf{N} \rightarrow \mathbf{M}$ is a substitution such that $S\sigma \subseteq \mathbf{N}$ then
 $P\sigma \xrightarrow[S\sigma]{\mu\sigma} A\sigma$.

A symbolic LTS

- *Idea* : record without checking the conditions needed to enable transitions.
- A transition constraint has the form $(\nu \tilde{z}) \Phi$ where Φ is a finite set of guards and \tilde{z} is a finite set of names that occur in Φ , i.e. $\{\tilde{z}\} \subseteq n(\Phi)$
- Composition of constraints :
 - ▶ Conjunction of $c_1 = (\nu \tilde{z}_1) \Phi_1$ and $c_2 = (\nu \tilde{z}_2) \Phi_2$

$$c_1 \ \& \ c_2 := (\Phi_1 \cup \Phi_2)$$

- ▶ Restriction of name x .
If $c = (\nu \tilde{z}) \Phi$ and $x \notin \{\tilde{z}\}$:

$$\begin{aligned} \nu_+(x, c) &:= (\nu x \tilde{z}) \Phi && \text{if } x \in \text{fn}(c) \\ &:= c && \text{otherwise} \end{aligned}$$

Define $>_o$ as being the smallest precongruence on expressions that satisfies :

- $\pi_1 ((E_1 . E_2)) >_o E_1$ if $\mathbf{e}_c(E_2) \neq \perp$
- $\pi_2 ((E_1 . E_2)) >_o E_2$ if $\mathbf{e}_c(E_1) \neq \perp$
- $\text{Dec}_{E_2}^s \text{Enc}_{E_2}^s E_1 >_o E_1$ if $\mathbf{e}_c(E_2) \neq \perp$

Extend this relation to agents in :

- $A >_o^= B$ (A, B are concrete agents)
- $A >_o^e B$ (A is symbolic, B is concrete)

(two ways to handle concretions)

Theorem

Let $P, Q \in \mathbf{P}$ and assume that $P >_0 Q$.

- 1 If $P \xrightarrow[S]{\mu} A$ then $Q \xrightarrow[S]{\mu} B$ and $A >_0^= B$
- 2 If $Q \xrightarrow[S]{\mu} B$ then $P \xrightarrow[S]{\mu} A$ and $A >_0^= B$

Theorem

Let $P, Q \in \mathbf{P}$ and $\sigma : \mathbf{N} \rightarrow \mathbf{M}$ a substitution.

- 1 If $P \xrightarrow[c]{\mu_s} A$ and $\mathbf{e}(c\sigma) = \mathbf{true}$ then $P\sigma \xrightarrow[\mathbf{nc}(c\sigma)]{\mathbf{e}_c(\mu_s\sigma)} B$ with $A\sigma >_0^e B$
- 2 If $P\sigma \xrightarrow[S]{\mu} B$ then $P \xrightarrow[c]{\mu_s} A$ with $\mathbf{e}(c\sigma) = \mathbf{true}$, $\mathbf{nc}(c\sigma) = S$, $\mathbf{e}_c(\mu_s\sigma) = \mu$ and $A\sigma >_0^e B$