An Introduction to the Applied Pi Calculus
Part I

Naipeng Dong
SaToSS

March 9, 2010

Outline

Introduction

- A language for describing and analyzing security protocols
- Why applied pi calculus:
  - Intuitive process syntax
  - Wide variety of cryptographic primitives

Outline

Syntax

- A signature Σ consists of a finite set of function symbols

Syntax

- A signature Σ consists of a finite set of function symbols

$$\Sigma_H = \{\mathsf{true}, \mathsf{fst}, \mathsf{snd}, \mathsf{hash}, \mathsf{pk}, \mathsf{getmsg}, \mathsf{pair}, \mathsf{sdec}, \mathsf{senc}, \mathsf{adec}, \mathsf{aenc}, \mathsf{sign}, \mathsf{checksign}, \ldots\}$$

Syntax

- A signature Σ consists of a finite set of function symbols

$$\Sigma_H = \{\text{true}, \text{fst}, \text{snd}, \text{hash}, \text{pk}, \text{getmsg}, \text{pair}, \text{sdec}, \text{senc}, \text{adec}, \text{aenc}, \text{sign}, \text{checksign}, \ldots\}$$

- Term

$L, M, N, T, U, V ::=$	terms
$a, b, c, \ldots, k, \ldots, m, n, \ldots, s$	name
x, y, z	variable
$g(M_1, \ldots, M_l)$	function application

Syntax

- Equational theories are typically specified by equational rules that are closed by variable substitution

$$\begin{array}{rcl} \mathsf{fst}(\mathsf{pair}(x,y)) & = & x \\ \mathsf{snd}(\mathsf{pair}(x,y)) & = & y \\ \mathsf{sdec}(x,\mathsf{senc}(x,y)) & = & y \\ \mathsf{adec}(x,\mathsf{aenc}(\mathsf{pk}(x),y)) & = & y \\ \mathsf{getmsg}(\mathsf{sign}(x,y)) & = & y \\ \mathsf{checksign}(\mathsf{pk}(x),\mathsf{sign}(x,y)) & = & \mathsf{true} \end{array}$$

Syntax

- Equational theories are typically specified by equational rules that are closed by variable substitution

$$
\begin{array}{lcl}
\mathsf{fst}(\mathsf{pair}(x,y)) & = & x \\
\mathsf{snd}(\mathsf{pair}(x,y)) & = & y \\
\mathsf{sdec}(x,\mathsf{senc}(x,y)) & = & y \\
\mathsf{adec}(x,\mathsf{aenc}(\mathsf{pk}(x),y)) & = & y \\
\mathsf{getmsg}(\mathsf{sign}(x,y)) & = & y \\
\mathsf{checksign}(\mathsf{pk}(x),\mathsf{sign}(x,y)) & = & \mathsf{true}
\end{array}
$$

e.g.reasoning with equational theories

$$\mathsf{sdec}(k,\mathsf{senc}(k,L)) =_E L$$
$$\mathsf{pair}(M,N) =_E \mathsf{pair}(\mathsf{sdec}(k,\mathsf{senc}(k,\mathsf{fst}(\mathsf{pair}(M,N)))),N)$$

Syntax

- Equational theories are typically specified by equational rules that are closed by variable substitution

$$
\begin{array}{lcl}
\mathsf{fst}(\mathsf{pair}(x,y)) & = & x \\
\mathsf{snd}(\mathsf{pair}(x,y)) & = & y \\
\mathsf{sdec}(x,\mathsf{senc}(x,y)) & = & y \\
\mathsf{adec}(x,\mathsf{aenc}(\mathsf{pk}(x),y)) & = & y \\
\mathsf{getmsg}(\mathsf{sign}(x,y)) & = & y \\
\mathsf{checksign}(\mathsf{pk}(x),\mathsf{sign}(x,y)) & = & \mathsf{true}
\end{array}
$$

e.g.reasoning with equational theories

$$\mathsf{sdec}(k,\mathsf{senc}(k,L)) =_E L$$

$$\mathsf{pair}(M,N) =_E \mathsf{pair}(\mathsf{sdec}(k,\mathsf{senc}(k,\mathsf{fst}(\mathsf{pair}(M,N)))),N)$$

Syntax

- Equational theories are typically specified by equational rules that are closed by variable substitution

$$
\begin{array}{lcl}
\mathsf{fst}(\mathsf{pair}(x,y)) & = & x \\
\mathsf{snd}(\mathsf{pair}(x,y)) & = & y \\
\mathsf{sdec}(x,\mathsf{senc}(x,y)) & = & y \\
\mathsf{adec}(x,\mathsf{aenc}(\mathsf{pk}(x),y)) & = & y \\
\mathsf{getmsg}(\mathsf{sign}(x,y)) & = & y \\
\mathsf{checksign}(\mathsf{pk}(x),\mathsf{sign}(x,y)) & = & \mathsf{true}
\end{array}
$$

e.g.reasoning with equational theories

$$\mathsf{sdec}(k,\mathsf{senc}(k,L)) =_E L$$
$$\mathsf{pair}(M,N) =_E \mathsf{pair}(\mathsf{sdec}(k,\mathsf{senc}(k,\mathsf{fst}(\mathsf{pair}(M,N)))),N)$$

Syntax

- Equational theories are typically specified by equational rules that are closed by variable substitution

$$\begin{array}{lcl} \mathsf{fst}(\mathsf{pair}(x,y)) & = & x \\ \mathsf{snd}(\mathsf{pair}(x,y)) & = & y \\ \mathsf{sdec}(x,\mathsf{senc}(x,y)) & = & y \\ \mathsf{adec}(x,\mathsf{aenc}(\mathsf{pk}(x),y)) & = & y \\ \mathsf{getmsg}(\mathsf{sign}(x,y)) & = & y \\ \mathsf{checksign}(\mathsf{pk}(x),\mathsf{sign}(x,y)) & = & \mathsf{true} \end{array}$$

e.g.reasoning with equational theories

$$\mathsf{sdec}(k,\mathsf{senc}(k,L)) =_E L$$

$$\mathsf{pair}(M,N) =_E \mathsf{pair}(\mathsf{sdec}(k,\mathsf{senc}(k,\mathsf{fst}(\mathsf{pair}(M,N)))),N)$$

Syntax

- Equational theories are typically specified by equational rules that are closed by variable substitution

$$
\begin{array}{rcl}
\mathsf{fst}(\mathsf{pair}(x,y)) & = & x \\
\mathsf{snd}(\mathsf{pair}(x,y)) & = & y \\
\mathsf{sdec}(x,\mathsf{senc}(x,y)) & = & y \\
\mathsf{adec}(x,\mathsf{aenc}(\mathsf{pk}(x),y)) & = & y \\
\mathsf{getmsg}(\mathsf{sign}(x,y)) & = & y \\
\mathsf{checksign}(\mathsf{pk}(x),\mathsf{sign}(x,y)) & = & \mathsf{true}
\end{array}
$$

e.g.reasoning with equational theories

$$\mathsf{sdec}(k,\mathsf{senc}(k,L)) =_E L$$
$$\mathsf{pair}(M,N) =_E \mathsf{pair}(\mathsf{sdec}(k,\mathsf{senc}(k,\mathsf{fst}(\mathsf{pair}(M,N)))),N)$$

Syntax

- Equational theories are typically specified by equational rules that are closed by variable substitution

$$\begin{aligned}
\mathsf{fst}(\mathsf{pair}(x,y)) &= x \\
\mathsf{snd}(\mathsf{pair}(x,y)) &= y \\
\mathsf{sdec}(x,\mathsf{senc}(x,y)) &= y \\
\mathsf{adec}(x,\mathsf{aenc}(\mathsf{pk}(x),y)) &= y \\
\mathsf{getmsg}(\mathsf{sign}(x,y)) &= y \\
\mathsf{checksign}(\mathsf{pk}(x),\mathsf{sign}(x,y)) &= \mathsf{true}
\end{aligned}$$

e.g.reasoning with equational theories

$$\mathsf{sdec}(k,\mathsf{senc}(k,L)) =_E L$$

$$\mathsf{pair}(M,N) =_E \mathsf{pair}(\mathsf{sdec}(k,\mathsf{senc}(k,\mathsf{fst}(\mathsf{pair}(M,N)))),N)$$

Syntax

- Process

$P, Q, R ::=$	plain porcesses
0	null process
$P \mid Q$	parallel composition
$!P$	replication
$\nu n.P$	name restriction
if $M = N$ then P else Q	conditional
$in(u, x).P$	message input
$out(u, N).P$	message output

Syntax

- Process

$P, Q, R ::=$	plain porcesses
0	null process
$P \mid Q$	parallel composition
$!P$	replication
$\nu n.P$	name restriction
if $M = N$ then P else Q	conditional
$in(u, x).P$	message input
$out(u, N).P$	message output

Syntax

- Process

$P, Q, R ::=$	plain porcesses
0	null process
$P \| Q$	parallel composition
$!P$	replication
$\nu n.P$	name restriction
if $M = N$ then P else Q	conditional
$in(u, x).P$	message input
$out(u, N).P$	message output

Syntax

- Process

$P, Q, R ::=$	plain porcesses
0	null process
$P \mid Q$	parallel composition
$!P$	replication
$\nu n.P$	name restriction
if $M = N$ then P else Q	conditional
$in(u, x).P$	message input
$out(u, N).P$	message output

Syntax

- Process

$P, Q, R ::=$	plain porcesses
0	null process
$P \mid Q$	parallel composition
$!P$	replication
$\nu n.P$	name restriction
if $M = N$ then P else Q	conditional
$in(u, x).P$	message input
$out(u, N).P$	message output

Syntax

- Process

$P, Q, R ::=$	plain porcesses
0	null process
$P \mid Q$	parallel composition
$!P$	replication
$\nu n.P$	name restriction
if $M = N$ then P else Q	conditional
$in(u, x).P$	message input
$out(u, N).P$	message output

Syntax

- Process

$P, Q, R ::=$	plain porcesses
0	null process
$P \mid Q$	parallel composition
$!P$	replication
$\nu n.P$	name restriction
if $M = N$ then P else Q	conditional
$in(u, x).P$	message input
$out(u, N).P$	message output

Syntax

- Extended process

$A, B, C ::=$	extended porcesses	
P		plain process
$A \vert B$		parallel composition
$\nu n.A$		name restriction
$\nu x.A$		variable restriction
$\{M/x\}$		active substitution

Syntax

- Extended process

$A, B, C ::=$	extended porcesses
P	plain process
$A \mid B$	parallel composition
$\nu n.A$	name restriction
$\nu x.A$	variable restriction
$\{M/x\}$	active substitution

Syntax

- Extended process

$A, B, C ::=$	extended porcesses
P	plain process
$A \vert B$	parallel composition
$\nu n.A$	name restriction
$\nu x.A$	variable restriction
$\{M/x\}$	active substitution

- Example

$\overline{c}\langle M\rangle.P \xrightarrow{\nu x.\overline{c}\langle x\rangle} P|\{M/x\}$

Active substitution : $P|\{M/x\}$

Syntactic substitution : $P\{M/x\}$

Syntax

- Extended process

$$
\begin{array}{lll}
A, B, C ::= & & \text{extended porcesses} \\
& P & \quad \text{plain process} \\
& A|B & \quad \text{parallel composition} \\
& \nu n.A & \quad \text{name restriction} \\
& \nu x.A & \quad \text{variable restriction} \\
& \{M/x\} & \quad \text{active substitution}
\end{array}
$$

- Example

  $\overline{c}\langle M\rangle.P \xrightarrow{\nu x.\overline{c}\langle x\rangle} P|\{M/x\}$

  Active substitution : $P|\{M/x\} \equiv P\{M/x\}|\{M/x\}$

  Syntactic substitution : $P\{M/x\}$

Syntax

- Extended process

A, B, C ::=	extended porcesses	
P		plain process
$A \mid B$		parallel composition
$\nu n.A$		name restriction
$\nu x.A$		variable restriction
$\{M/x\}$		active substitution

- Example

$\overline{c}\langle M \rangle.P \xrightarrow{\nu x.\overline{c}\langle x \rangle} P|\{M/x\}$

Active substitution : $P|\{M/x\}|Q \equiv P\{M/x\}|\{M/x\}|Q\{M/x\}$

Syntactic substitution : $P\{M/x\}|Q$

Syntax

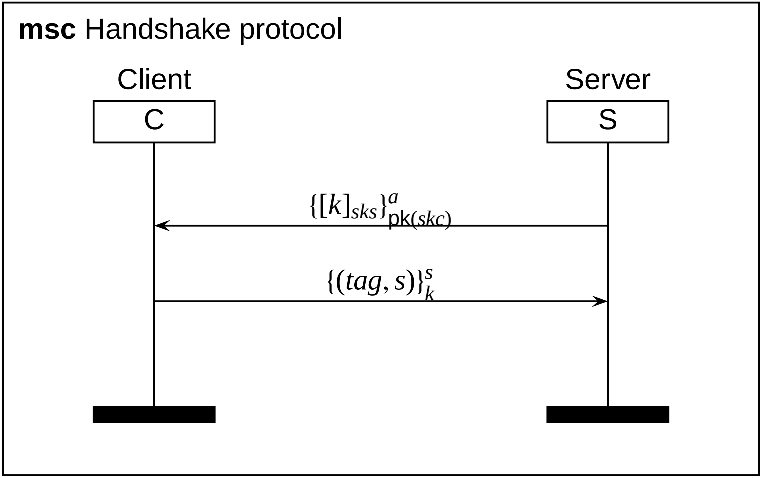
- Extended process

$$\begin{array}{lll} A, B, C ::= & & \text{extended porcesses} \\ & P & \text{plain process} \\ & A|B & \text{parallel composition} \\ & \nu n.A & \text{name restriction} \\ & \nu x.A & \text{variable restriction} \\ & \{M/x\} & \text{active substitution} \end{array}$$

- Example
  $\overline{c}\langle M\rangle.P \xrightarrow{\nu x.\overline{c}\langle x\rangle} P|\{M/x\}$
  Active substitution : $P|\{M/x\}|Q \equiv P\{M/x\}|\{M/x\}|Q\{M/x\}$
  Syntactic substitution : $P\{M/x\}|Q$
- $\nu x.(\{M/x\}|P)$ corresponds exactly to let $x = M$ in P

Syntax

- Example



Syntax

- Signature

$$\Sigma_H = \{\mathsf{true}, \mathsf{fst}, \mathsf{snd}, \mathsf{pk}, \mathsf{getmsg}, \mathsf{pair}, \mathsf{sdec}, \mathsf{senc}, \mathsf{adec}, \mathsf{aenc}, \mathsf{sign}, \mathsf{checksign}\}$$

Syntax

- Signature

$$\Sigma_H = \{\text{true}, \text{fst}, \text{snd}, \text{pk}, \text{getmsg}, \text{pair}, \text{sdec}, \text{senc}, \text{adec}, \text{aenc}, \text{sign}, \text{checksign}\}$$

- Equantional theory

$$\begin{aligned}
\text{fst}(\text{pair}(x, y)) &= x \\
\text{snd}(\text{pair}(x, y)) &= y \\
\text{sdec}(x, \text{senc}(x, y)) &= y \\
\text{adec}(x, \text{aenc}(\text{pk}(x), y)) &= y \\
\text{getmsg}(\text{sign}(x, y)) &= y \\
\text{checksign}(\text{pk}(x), \text{sign}(x, y)) &= \text{true}
\end{aligned}$$

Syntax

- Processes

$$P \triangleq \nu sk_S.\nu sk_C.\nu s.$$
$$\text{let } pk_S = \text{pk}(sk_S) \text{ in let } pk_C = \text{pk}(sk_C) \text{ in}$$
$$(\overline{c}\langle pk_S\rangle | \overline{c}\langle pk_C\rangle | !P_S | !P_C)$$

Syntax

- Processes

$$P \triangleq \nu sk_S.\nu sk_C.\nu s.$$
$$\text{let } pk_S = \mathrm{pk}(sk_S) \text{ in let } pk_C = \mathrm{pk}(sk_C) \text{ in}$$
$$(\bar{c}\langle pk_S\rangle | \bar{c}\langle pk_C\rangle | !P_S | !P_C)$$

Syntax

- Processes

$$P \triangleq \nu sk_S.\nu sk_C.\nu s.$$
$$\text{let } pk_S = \text{pk}(sk_S) \text{ in let } pk_C = \text{pk}(sk_C) \text{ in}$$
$$(\overline{c}\langle pk_S\rangle | \overline{c}\langle pk_C\rangle | !P_S | !P_C)$$

Syntax

- Processes

$$P \triangleq \nu sk_S.\nu sk_C.\nu s.\ \text{let } pk_S = \text{pk}(sk_S) \text{ in let } pk_C = \text{pk}(sk_C) \text{ in } (\bar{c}\langle pk_S\rangle | \bar{c}\langle pk_C\rangle | !P_S | !P_C)$$

Syntax

- Processes

$$P \triangleq \nu sk_S.\nu sk_C.\nu s.$$
$$\text{let } pk_S = \text{pk}(sk_S) \text{ in let } pk_C = \text{pk}(sk_C) \text{ in}$$
$$(\bar{c}\langle pk_S\rangle | \bar{c}\langle pk_C\rangle | !P_S | !P_C)$$

$$P_S \triangleq c(x\_pk).\nu k.\bar{c}\langle \text{aenc}(x\_pk, \text{sign}(sk_S, k))\rangle.$$
$$c(z).\text{if fst}(\text{sdec}(k, z)) = tag \text{ then } Q$$

Syntax

- Processes

$$P \triangleq \nu sk_S.\nu sk_C.\nu s.$$
$$\text{let } pk_S = \text{pk}(sk_S) \text{ in let } pk_C = \text{pk}(sk_C) \text{ in}$$
$$(\overline{c}\langle pk_S\rangle | \overline{c}\langle pk_C\rangle | !P_S | !P_C)$$

$$P_S \triangleq c(x\_pk).\nu k.\overline{c}\langle \text{aenc}(x\_pk, \text{sign}(sk_S, k))\rangle.$$
$$c(z).\text{if fst}(\text{sdec}(k, z)) = tag \text{ then } Q$$

Syntax

- Processes

$$P \triangleq \nu sk_S.\nu sk_C.\nu s.$$
$$\text{let } pk_S = \text{pk}(sk_S) \text{ in let } pk_C = \text{pk}(sk_C) \text{ in}$$
$$(\bar{c}\langle pk_S\rangle | \bar{c}\langle pk_C\rangle | !P_S | !P_C)$$

$$P_S \triangleq c(x\_pk).\nu k.\bar{c}\langle \text{aenc}(x\_pk, \text{sign}(sk_S, k))\rangle.$$
$$c(z).\text{if fst}(\text{sdec}(k, z)) = tag \text{ then } Q$$

Syntax

- Processes

$$P \triangleq \nu sk_S.\nu sk_C.\nu s.$$
$$\text{let } pk_S = \text{pk}(sk_S) \text{ in let } pk_C = \text{pk}(sk_C) \text{ in}$$
$$(\bar{c}\langle pk_S\rangle | \bar{c}\langle pk_C\rangle | !P_S | !P_C)$$

$$P_S \triangleq c(x\_pk).\nu k.\bar{c}\langle \text{aenc}(x\_pk, \text{sign}(sk_S, k))\rangle.$$
$$c(z).\text{if fst}(\text{sdec}(k, z)) = tag \text{ then } Q$$

Syntax

- Processes

$$P \triangleq \nu sk_S.\nu sk_C.\nu s.$$
$$\text{let } pk_S = \text{pk}(sk_S) \text{ in let } pk_C = \text{pk}(sk_C) \text{ in}$$
$$(\bar{c}\langle pk_S\rangle | \bar{c}\langle pk_C\rangle | !P_S | !P_C)$$

$$P_S \triangleq c(x\_pk).\nu k.\bar{c}\langle \text{aenc}(x\_pk, \text{sign}(sk_S, k))\rangle.$$
$$c(z).\text{if fst}(\text{sdec}(k, z)) = tag \text{ then } Q$$

$$P_C \triangleq c(y).\text{let } y' = \text{adec}(sk_C, y) \text{ in}$$
$$\text{let } y\_k = \text{getmsg}(y') \text{ in}$$
$$\text{if checksign}(pk_S, y') = \text{true then}$$
$$\bar{c}\langle \text{senc}(y\_k, \text{pair}(tag, s))\rangle$$

Syntax

- Processes

$$P \triangleq \nu sk_S.\nu sk_C.\nu s.$$
$$\text{let } pk_S = \text{pk}(sk_S) \text{ in let } pk_C = \text{pk}(sk_C) \text{ in}$$
$$(\overline{c}\langle pk_S\rangle | \overline{c}\langle pk_C\rangle | !P_S | !P_C)$$

$$P_S \triangleq c(x\_pk).\nu k.\overline{c}\langle \text{aenc}(x\_pk, \text{sign}(sk_S, k))\rangle.$$
$$c(z).\text{if fst}(\text{sdec}(k, z)) = tag \text{ then } Q$$

$$P_C \triangleq c(y).\text{let } y' = \text{adec}(sk_C, y) \text{ in}$$
$$\text{let } y\_k = \text{getmsg}(y') \text{ in}$$
$$\text{if checksign}(pk_S, y') = \text{true then}$$
$$\overline{c}\langle \text{senc}(y\_k, \text{pair}(tag, s))\rangle$$

Syntax

- Processes

$$
\begin{aligned}
P &\triangleq \nu sk_S.\nu sk_C.\nu s.\\
&\quad \text{let } pk_S = \mathsf{pk}(sk_S) \text{ in let } pk_C = \mathsf{pk}(sk_C) \text{ in}\\
&\quad (\overline{c}\langle pk_S\rangle | \overline{c}\langle pk_C\rangle | !P_S | !P_C)\\
P_S &\triangleq c(x\_pk).\nu k.\overline{c}\langle \mathsf{aenc}(x\_pk, \mathsf{sign}(sk_S, k))\rangle.\\
&\quad c(z).\text{if } \mathsf{fst}(\mathsf{sdec}(k, z)) = tag \text{ then } Q\\
P_C &\triangleq c(y).\text{let } y' = \mathsf{adec}(sk_C, y) \text{ in}\\
&\quad \text{let } y\_k = \mathsf{getmsg}(y') \text{ in}\\
&\quad \text{if } \mathsf{checksign}(pk_S, y') = \mathsf{true} \text{ then}\\
&\quad \overline{c}\langle \mathsf{senc}(y\_k, \mathsf{pair}(tag, s))\rangle
\end{aligned}
$$

Syntax

- Processes

$$P \triangleq \nu sk_S.\nu sk_C.\nu s.$$
$$\text{let } pk_S = \text{pk}(sk_S) \text{ in let } pk_C = \text{pk}(sk_C) \text{ in}$$
$$(\overline{c}\langle pk_S\rangle | \overline{c}\langle pk_C\rangle | !P_S | !P_C)$$

$$P_S \triangleq c(x\_pk).\nu k.\overline{c}\langle \text{aenc}(x\_pk, \text{sign}(sk_S, k))\rangle.$$
$$c(z).\text{if fst}(\text{sdec}(k, z)) = tag \text{ then } Q$$

$$P_C \triangleq c(y).\text{let } y' = \text{adec}(sk_C, y) \text{ in}$$
$$\text{let } y\_k = \text{getmsg}(y') \text{ in}$$
$$\text{if checksign}(pk_S, y') = \text{true then}$$
$$\overline{c}\langle \text{senc}(y\_k, \text{pair}(tag, s))\rangle$$

Outline

Operational semantics

- Structural equivalence

PAR – 0	A	$\equiv$	$A\|0$
PAR – A	$A\|(B\|C)$	$\equiv$	$(A\|B)\|C$
PAR – C	$A\|B$	$\equiv$	$B\|A$
REPL	$!P$	$\equiv$	$P\|!P$
NEW – 0	$\nu n.0$	$\equiv$	0
NEW – c	$\nu u.\nu w.A$	$\equiv$	$\nu w.\nu u.A$
NEW-PAR	$A\|\nu u.B$	$\equiv$	$\nu u.(A\|B)$
			$where u \notin fv(A) \cup fn(A)$
ALIAS	$\nu x.\{M/x\}$	$\equiv$	0
SUBST	$\{M/x\}\|A$	$\equiv$	$\{M/x\}\|A\{M/x\}$
REWRITE	$\{M/x\}$	$\equiv$	$\{N/x\}$
			where $M =_E N$

Operational semantics

- Structural equivalence

PAR – 0	A	$\equiv$	$A \mid 0$
PAR – A	$A \mid (B \mid C)$	$\equiv$	$(A \mid B) \mid C$
PAR – C	$A \mid B$	$\equiv$	$B \mid A$
REPL	$!P$	$\equiv$	$P \mid !P$
NEW – 0	$\nu n.0$	$\equiv$	0
NEW – c	$\nu u.\nu w.A$	$\equiv$	$\nu w.\nu u.A$
NEW-PAR	$A \mid \nu u.B$	$\equiv$	$\nu u.(A \mid B)$
			$where u \notin fv(A) \cup fn(A)$
ALIAS	$\nu x.\{M/x\}$	$\equiv$	0
SUBST	$\{M/x\} \mid A$	$\equiv$	$\{M/x\} \mid A\{M/x\}$
REWRITE	$\{M/x\}$	$\equiv$	$\{N/x\}$
			where $M =_E N$

Operational semantics

- Structural equivalence

$$
\begin{array}{lrcl}
\text{PAR}-0 & A & \equiv & A|0 \\
\text{PAR}-A & A|(B|C) & \equiv & (A|B)|C \\
\text{PAR}-C & A|B & \equiv & B|A \\
\text{REPL} & !P & \equiv & P\,|!P \\
\\
\text{NEW}-0 & \nu n.0 & \equiv & 0 \\
\text{NEW}-c & \nu u.\nu w.A & \equiv & \nu w.\nu u.A \\
\text{NEW-PAR} & A|\nu u.B & \equiv & \nu u.(A|B) \\
 & & & where u \notin fv(A) \cup fn(A) \\
\\
\text{ALIAS} & \nu x.\{M/x\} & \equiv & 0 \\
\color{red}{\text{SUBST}} & \color{red}{\{M/x\}|A} & \color{red}{\equiv} & \color{red}{\{M/x\}|A\{M/x\}} \\
\text{REWRITE} & \{M/x\} & \equiv & \{N/x\} \\
 & & & \text{where } M =_E N
\end{array}
$$

Operational semantics

- Structural equivalence

PAR – 0	A	$\equiv$	$A\|0$
PAR – A	$A\|(B\|C)$	$\equiv$	$(A\|B)\|C$
PAR – C	$A\|B$	$\equiv$	$B\|A$
REPL	$!P$	$\equiv$	$P\|!P$
NEW – 0	$\nu n.0$	$\equiv$	0
NEW – c	$\nu u.\nu w.A$	$\equiv$	$\nu w.\nu u.A$
NEW-PAR	$A\|\nu u.B$	$\equiv$	$\nu u.(A\|B)$
			$where u \notin fv(A) \cup fn(A)$
ALIAS	$\nu x.\{M/x\}$	$\equiv$	0
SUBST	$\{M/x\}\|A$	$\equiv$	$\{M/x\}\|A\{M/x\}$
REWRITE	$\{M/x\}$	$\equiv$	$\{N/x\}$
			where $M =_E N$

Operational semantics

- Internal reduction

COMM	$\overline{c}\langle x\rangle.P \mid c(x).Q \rightarrow P \mid Q$
THEN	if $N = N$ then P else $Q \rightarrow P$
ELSE	if $L = M$ then P else $Q \rightarrow Q$

Operational semantics

- Internal reduction

COMM	$\overline{c}\langle x\rangle.P \mid c(x).Q \;\rightarrow\; P \mid Q$
THEN	if $N = N$ then P else $Q \;\rightarrow\; P$
ELSE	if $L = M$ then P else $Q \;\rightarrow\; Q$

- Example

$$\overline{c}\langle M\rangle.P \mid c(x).Q$$

Operational semantics

- Internal reduction

COMM	$\overline{c}\langle x\rangle.P \mid c(x).Q \;\rightarrow P \mid Q$
THEN	if $N = N$ then P else $Q \;\rightarrow P$
ELSE	if $L = M$ then P else $Q \;\rightarrow\; Q$

- Example

$$\overline{c}\langle M\rangle.P \mid c(x).Q$$

$$\overline{c}\langle M\rangle.P \mid c(x).Q \equiv \nu x.(\overline{c}\langle x\rangle.P \mid c(x).Q \mid \{M/x\})$$ ALIAS

Operational semantics

- Internal reduction

COMM	$\overline{c}\langle x\rangle.P \mid c(x).Q \;\rightarrow\; P \mid Q$
THEN	if $N = N$ then P else $Q \;\rightarrow\; P$
ELSE	if $L = M$ then P else $Q \;\rightarrow\; Q$

- Example

$$\overline{c}\langle M\rangle.P \mid c(x).Q$$

$$\overline{c}\langle M\rangle.P \mid c(x).Q \equiv \nu x.(\overline{c}\langle x\rangle.P \mid c(x).Q \mid \{M/x\}) \qquad \text{ALIAS}$$

$$\nu x.(\overline{c}\langle x\rangle.P \mid c(x).Q \mid \{M/x\}) \rightarrow \nu x.(P \mid Q \mid \{M/x\}) \qquad \text{COMM}$$

Operational semantics

- Internal reduction

COMM	$\overline{c}\langle x\rangle.P \mid c(x).Q$	$\rightarrow P \mid Q$
THEN	if $N = N$ then P else Q	$\rightarrow P$
ELSE	if $L = M$ then P else Q	$\rightarrow Q$

- Example

$\overline{c}\langle M\rangle.P \mid c(x).Q$	
$\overline{c}\langle M\rangle.P \mid c(x).Q \equiv \nu x.(\overline{c}\langle x\rangle.P \mid c(x).Q \mid \{M/x\})$	ALIAS
$\nu x.(\overline{c}\langle x\rangle.P \mid c(x).Q \mid \{M/x\}) \rightarrow \nu x.(P \mid Q \mid \{M/x\})$	COMM
$\nu x.(P \mid Q \mid \{M/x\}) \equiv P \mid Q \mid \{M/x\}$	NEW-PAR

Operational semantics

- Internal reduction

COMM	$\overline{c}\langle x\rangle.P \mid c(x).Q \rightarrow P \mid Q$
THEN	if $N = N$ then P else $Q \rightarrow P$
ELSE	if $L = M$ then P else $Q \rightarrow Q$

- Example

$\overline{c}\langle M\rangle.P \mid c(x).Q$	
$\overline{c}\langle M\rangle.P \mid c(x).Q \equiv \nu x.(\overline{c}\langle x\rangle.P \mid c(x).Q \mid \{M/x\})$	ALIAS
$\nu x.(\overline{c}\langle x\rangle.P \mid c(x).Q \mid \{M/x\}) \rightarrow \nu x.(P \mid Q \mid \{M/x\})$	COMM
$\nu x.(P \mid Q \mid \{M/x\}) \equiv P \mid Q \mid \{M/x\}$	NEW-PAR
$\overline{c}\langle M\rangle.P \mid c(x).Q \rightarrow P \mid Q \mid \{M/x\}$	

Operational semantics

- Labelled reduction allows us to reason about processes that interact with the environment

Operational semantics

- Labelled reduction allows us to reason about processes that interact with the environment
- Labelled semantics

$$A \xrightarrow{\alpha} B$$

α is a label of the form $c(M), \overline{c}\langle u\rangle, \nu u.\overline{c}\langle u\rangle$
u is either achannel name or a variable of base type

Operational semantics

- Labelled reduction allows us to reason about processes that interact with the environment
- Labelled semantics

$$A \xrightarrow{\alpha} B$$

  α is a label of the form $c(M), \overline{c}\langle u\rangle, \nu u.\overline{c}\langle u\rangle$
  u is either achannel name or a variable of base type
- Example

$$A \xrightarrow{c(M)} B$$

Operational semantics

- Labelled reductions

IN	$c(x).P \xrightarrow{c(M)} P\{M/x\}$
OUT-ATOM	$\overline{c}\langle u\rangle.P \xrightarrow{\overline{c}\langle u\rangle} P$
OPEN-ATOM	$\dfrac{A \xrightarrow{\overline{c}\langle u\rangle} A' \qquad u \neq c}{\nu u.A \xrightarrow{\nu u.\overline{c}\langle u\rangle} A'}$
SCOPE	$\dfrac{A \xrightarrow{\alpha} A' \qquad u \text{ does not occur in } \alpha}{\nu u.A \xrightarrow{\alpha} \nu u.A'}$
PAR	$\dfrac{A \xrightarrow{\alpha} A' \qquad \mathrm{bv}(\alpha) \cap \mathrm{fv}(B) = \mathrm{bn}(\alpha) \cap \mathrm{fn}(B) = \emptyset}{A \mid B \xrightarrow{\alpha} A' \mid B}$
STRUCT	$\dfrac{A \equiv B \qquad B \xrightarrow{\alpha} B' \qquad B' \equiv A'}{A \xrightarrow{\alpha} A'}$

Operational semantics

- Labelled reductions

IN	$c(x).P \xrightarrow{c(M)} P\{M/x\}$
OUT-ATOM	$\bar{c}\langle u\rangle.P \xrightarrow{\bar{c}\langle u\rangle} P$
OPEN-ATOM	$\dfrac{A \xrightarrow{\bar{c}\langle u\rangle} A' \qquad u \neq c}{\nu u.A \xrightarrow{\nu u.\bar{c}\langle u\rangle} A'}$
SCOPE	$\dfrac{A \xrightarrow{\alpha} A' \qquad u \text{ does not occur in } \alpha}{\nu u.A \xrightarrow{\alpha} \nu u.A'}$
PAR	$\dfrac{A \xrightarrow{\alpha} A' \qquad \text{bv}(\alpha) \cap \text{fv}(B) = \text{bn}(\alpha) \cap \text{fn}(B) = \emptyset}{A \mid B \xrightarrow{\alpha} A' \mid B}$
STRUCT	$\dfrac{A \equiv B \qquad B \xrightarrow{\alpha} B' \qquad B' \equiv A'}{A \xrightarrow{\alpha} A'}$

Operational semantics

- Labelled reductions

IN	$c(x).P \xrightarrow{c(M)} P\{M/x\}$
OUT-ATOM	$\overline{c}\langle u\rangle.P \xrightarrow{\overline{c}\langle u\rangle} P$
OPEN-ATOM	$\dfrac{A \xrightarrow{\overline{c}\langle u\rangle} A' \quad u \neq c}{\nu u.A \xrightarrow{\nu u.\overline{c}\langle u\rangle} A'}$
SCOPE	$\dfrac{A \xrightarrow{\alpha} A' \quad u \text{ does not occur in } \alpha}{\nu u.A \xrightarrow{\alpha} \nu u.A'}$
PAR	$\dfrac{A \xrightarrow{\alpha} A' \quad \mathrm{bv}(\alpha) \cap \mathrm{fv}(B) = \mathrm{bn}(\alpha) \cap \mathrm{fn}(B) = \emptyset}{A \mid B \xrightarrow{\alpha} A' \mid B}$
STRUCT	$\dfrac{A \equiv B \quad B \xrightarrow{\alpha} B' \quad B' \equiv A'}{A \xrightarrow{\alpha} A'}$

Operational semantics

- Labelled reductions

IN $$c(x).P \xrightarrow{c(M)} P\{M/x\}$$

OUT-ATOM $$\overline{c}\langle u\rangle.P \xrightarrow{\overline{c}\langle u\rangle} P$$

OPEN-ATOM $$\frac{A \xrightarrow{\overline{c}\langle u\rangle} A' \quad u \neq c}{\nu u.A \xrightarrow{\nu u.\overline{c}\langle u\rangle} A'}$$

SCOPE $$\frac{A \xrightarrow{\alpha} A' \quad u \text{ does not occur in } \alpha}{\nu u.A \xrightarrow{\alpha} \nu u.A'}$$

PAR $$\frac{A \xrightarrow{\alpha} A' \quad \mathrm{bv}(\alpha) \cap \mathrm{fv}(B) = \mathrm{bn}(\alpha) \cap \mathrm{fn}(B) = \emptyset}{A|B \xrightarrow{\alpha} A'|B}$$

STRUCT $$\frac{A \equiv B \quad B \xrightarrow{\alpha} B' \quad B' \equiv A'}{A \xrightarrow{\alpha} A'}$$

Operational semantics

- Labelled reductions

IN $$c(x).P \xrightarrow{c(M)} P\{M/x\}$$

OUT-ATOM $$\overline{c}\langle u\rangle.P \xrightarrow{\overline{c}\langle u\rangle} P$$

OPEN-ATOM $$\frac{A \xrightarrow{\overline{c}\langle u\rangle} A' \qquad u \neq c}{\nu u.A \xrightarrow{\nu u.\overline{c}\langle u\rangle} A'}$$

SCOPE $$\frac{A \xrightarrow{\alpha} A' \qquad u \text{ does not occur in } \alpha}{\nu u.A \xrightarrow{\alpha} \nu u.A'}$$

PAR $$\frac{A \xrightarrow{\alpha} A' \qquad \text{bv}(\alpha) \cap \text{fv}(B) = \text{bn}(\alpha) \cap \text{fn}(B) = \emptyset}{A|B \xrightarrow{\alpha} A'|B}$$

STRUCT $$\frac{A \equiv B \qquad B \xrightarrow{\alpha} B' \qquad B' \equiv A'}{A \xrightarrow{\alpha} A'}$$

Operational semantics

- Labelled reductions

IN $$c(x).P \xrightarrow{c(M)} P\{M/x\}$$

OUT-ATOM $$\overline{c}\langle u\rangle.P \xrightarrow{\overline{c}\langle u\rangle} P$$

OPEN-ATOM $$\frac{A \xrightarrow{\overline{c}\langle u\rangle} A' \qquad u \neq c}{\nu u.A \xrightarrow{\nu u.\overline{c}\langle u\rangle} A'}$$

SCOPE $$\frac{A \xrightarrow{\alpha} A' \qquad u \text{ does not occur in } \alpha}{\nu u.A \xrightarrow{\alpha} \nu u.A'}$$

PAR $$\frac{A \xrightarrow{\alpha} A' \qquad \text{bv}(\alpha) \cap \text{fv}(B) = \text{bn}(\alpha) \cap \text{fn}(B) = \emptyset}{A|B \xrightarrow{\alpha} A'|B}$$

STRUCT $$\frac{A \equiv B \qquad B \xrightarrow{\alpha} B' \qquad B' \equiv A'}{A \xrightarrow{\alpha} A'}$$

Operational semantics

- Labelled reductions

IN	$c(x).P \xrightarrow{c(M)} P\{M/x\}$
OUT-ATOM	$\overline{c}\langle u\rangle.P \xrightarrow{\overline{c}\langle u\rangle} P$
OPEN-ATOM	$\dfrac{A \xrightarrow{\overline{c}\langle u\rangle} A' \qquad u \neq c}{\nu u.A \xrightarrow{\nu u.\overline{c}\langle u\rangle} A'}$
SCOPE	$\dfrac{A \xrightarrow{\alpha} A' \qquad u \text{ does not occur in } \alpha}{\nu u.A \xrightarrow{\alpha} \nu u.A'}$
PAR	$\dfrac{A \xrightarrow{\alpha} A' \qquad \mathrm{bv}(\alpha) \cap \mathrm{fv}(B) = \mathrm{bn}(\alpha) \cap \mathrm{fn}(B) = \emptyset}{A \mid B \xrightarrow{\alpha} A' \mid B}$
STRUCT	$\dfrac{A \equiv B \qquad B \xrightarrow{\alpha} B' \qquad B' \equiv A'}{A \xrightarrow{\alpha} A'}$

Operational semantics

- Labelled reductions

IN	$c(x).P \xrightarrow{c(M)} P\{M/x\}$
OUT-ATOM	$\overline{c}\langle u\rangle.P \xrightarrow{\overline{c}\langle u\rangle} P$
OPEN-ATOM	$\dfrac{A \xrightarrow{\overline{c}\langle u\rangle} A' \quad u \neq c}{\nu u.A \xrightarrow{\nu u.\overline{c}\langle u\rangle} A'}$
SCOPE	$\dfrac{A \xrightarrow{\alpha} A' \quad u \text{ does not occur in } \alpha}{\nu u.A \xrightarrow{\alpha} \nu u.A'}$
PAR	$\dfrac{A \xrightarrow{\alpha} A' \quad \text{bv}(\alpha) \cap \text{fv}(B) = \text{bn}(\alpha) \cap \text{fn}(B) = \emptyset}{A \mid B \xrightarrow{\alpha} A' \mid B}$
STRUCT	$\dfrac{A \equiv B \quad B \xrightarrow{\alpha} B' \quad B' \equiv A'}{A \xrightarrow{\alpha} A'}$

Operational semantics

$$\frac{}{\overline{c}\langle x\rangle.P \xrightarrow{\overline{c}\langle x\rangle} P} \quad \text{OUT-ATOM}$$

$$\frac{\overline{c}\langle x\rangle.P \xrightarrow{\overline{c}\langle x\rangle} P}{\overline{c}\langle x\rangle.P \,|\{M/x\} \xrightarrow{\overline{c}\langle x\rangle} P \,|\{M/x\}} \quad \text{PAR}$$

$$\frac{\overline{c}\langle x\rangle.P \,|\{M/x\} \xrightarrow{\overline{c}\langle x\rangle} P \,|\{M/x\}}{\overline{c}\langle M\rangle.P \equiv \nu x.(\overline{c}\langle x\rangle.P \,|\{M/x\}) \xrightarrow{\nu x.\overline{c}\langle x\rangle} P \,|\{M/x\} \equiv P \,|\{M/x\}} \quad \text{OPEN-ATOM}$$

$$\frac{\overline{c}\langle M\rangle.P \equiv \nu x.(\overline{c}\langle x\rangle.P \,|\{M/x\}) \xrightarrow{\nu x.\overline{c}\langle x\rangle} P \,|\{M/x\} \equiv P \,|\{M/x\}}{\overline{c}\langle M\rangle.P \xrightarrow{\nu x.\overline{c}\langle x\rangle} P \,|\{M/x\}} \quad \text{STRUCT}$$

Operational semantics

$$\frac{}{\overline{c}\langle x\rangle.P \xrightarrow{\overline{c}\langle x\rangle} P} \quad \text{OUT-ATOM}$$

$$\frac{\overline{c}\langle x\rangle.P \xrightarrow{\overline{c}\langle x\rangle} P}{\overline{c}\langle x\rangle.P \mid \{M/x\} \xrightarrow{\overline{c}\langle x\rangle} P \mid \{M/x\}} \quad \text{PAR}$$

$$\overline{c}\langle M\rangle.P \equiv \nu x.(\overline{c}\langle x\rangle.P \mid \{M/x\}) \xrightarrow{\nu x.\overline{c}\langle x\rangle} P \mid \{M/x\} \equiv P \mid \{M/x\} \quad \text{OPEN-ATOM}$$

$$\frac{\overline{c}\langle M\rangle.P \equiv \nu x.(\overline{c}\langle x\rangle.P \mid \{M/x\}) \xrightarrow{\nu x.\overline{c}\langle x\rangle} P \mid \{M/x\} \equiv P \mid \{M/x\}}{\overline{c}\langle M\rangle.P \xrightarrow{\nu x.\overline{c}\langle x\rangle} P \mid \{M/x\}} \quad \text{STRUCT}$$

Operational semantics

$$\frac{}{\overline{c}\langle x\rangle.P \xrightarrow{\overline{c}\langle x\rangle} P} \quad \text{OUT-ATOM}$$

$$\frac{\overline{c}\langle x\rangle.P \xrightarrow{\overline{c}\langle x\rangle} P}{\overline{c}\langle x\rangle.P \mid \{M/x\} \xrightarrow{\overline{c}\langle x\rangle} P \mid \{M/x\}} \quad \text{PAR}$$

$$\frac{\overline{c}\langle x\rangle.P \mid \{M/x\} \xrightarrow{\overline{c}\langle x\rangle} P \mid \{M/x\}}{\overline{c}\langle M\rangle.P \equiv \nu x.(\overline{c}\langle x\rangle.P \mid \{M/x\}) \xrightarrow{\nu x.\overline{c}\langle x\rangle} P \mid \{M/x\} \equiv P \mid \{M/x\}} \quad \text{OPEN-ATOM}$$

$$\frac{\overline{c}\langle M\rangle.P \equiv \nu x.(\overline{c}\langle x\rangle.P \mid \{M/x\}) \xrightarrow{\nu x.\overline{c}\langle x\rangle} P \mid \{M/x\} \equiv P \mid \{M/x\}}{\overline{c}\langle M\rangle.P \xrightarrow{\nu x.\overline{c}\langle x\rangle} P \mid \{M/x\}} \quad \text{STRUCT}$$

Operational semantics

$$\frac{}{\bar{c}\langle x\rangle.P \xrightarrow{\bar{c}\langle x\rangle} P} \quad \text{OUT-ATOM}$$

$$\frac{\bar{c}\langle x\rangle.P \mid \{M/x\} \xrightarrow{\bar{c}\langle x\rangle} P \mid \{M/x\}}{\bar{c}\langle M\rangle.P \equiv \nu x.(\bar{c}\langle x\rangle.P \mid \{M/x\}) \xrightarrow{\nu x.\bar{c}\langle x\rangle} P \mid \{M/x\} \equiv P \mid \{M/x\}} \quad \begin{array}{l}\text{PAR}\\ \text{OPEN-ATOM}\end{array}$$

$$\frac{}{\bar{c}\langle M\rangle.P \xrightarrow{\nu x.\bar{c}\langle x\rangle} P \mid \{M/x\}} \quad \text{STRUCT}$$

Operational semantics

$$\frac{}{\overline{c}\langle x\rangle.P \xrightarrow{\overline{c}\langle x\rangle} P} \quad \text{OUT-ATOM}$$

$$\frac{\overline{c}\langle x\rangle.P \mid \{M/x\} \xrightarrow{\overline{c}\langle x\rangle} P \mid \{M/x\}}{} \quad \text{PAR}$$

$$\frac{\overline{c}\langle M\rangle.P \equiv \nu x.(\overline{c}\langle x\rangle.P \mid \{M/x\}) \xrightarrow{\nu x.\overline{c}\langle x\rangle} P \mid \{M/x\} \equiv P \mid \{M/x\}}{\overline{c}\langle M\rangle.P \xrightarrow{\nu x.\overline{c}\langle x\rangle} P \mid \{M/x\}} \quad \begin{array}{l}\text{OPEN-ATOM}\\ \text{STRUCT}\end{array}$$

Operational semantics

$$\frac{}{\bar{c}\langle x\rangle.P \xrightarrow{\bar{c}\langle x\rangle} P} \quad \text{OUT-ATOM}$$

$$\frac{\bar{c}\langle x\rangle.P \xrightarrow{\bar{c}\langle x\rangle} P}{\bar{c}\langle x\rangle.P \mid \{M/x\} \xrightarrow{\bar{c}\langle x\rangle} P \mid \{M/x\}} \quad \text{PAR}$$

$$\frac{\bar{c}\langle M\rangle.P \equiv \nu x.(\bar{c}\langle x\rangle.P \mid \{M/x\}) \xrightarrow{\nu x.\bar{c}\langle x\rangle} P \mid \{M/x\} \equiv P \mid \{M/x\}}{\bar{c}\langle M\rangle.P \xrightarrow{\nu x.\bar{c}\langle x\rangle} P \mid \{M/x\}} \quad \text{OPEN-ATOM / STRUCT}$$

Operational semantics

$$\frac{}{\bar{c}\langle x\rangle.P \xrightarrow{\bar{c}\langle x\rangle} P} \quad \text{OUT-ATOM}$$

$$\frac{\bar{c}\langle x\rangle.P \mid \{M/x\} \xrightarrow{\bar{c}\langle x\rangle} P \mid \{M/x\}}{} \quad \text{PAR}$$

$$\frac{\bar{c}\langle M\rangle.P \equiv \nu x.(\bar{c}\langle x\rangle.P \mid \{M/x\}) \xrightarrow{\nu x.\bar{c}\langle x\rangle} P \mid \{M/x\} \equiv P \mid \{M/x\}}{\bar{c}\langle M\rangle.P \xrightarrow{\nu x.\bar{c}\langle x\rangle} P \mid \{M/x\}} \quad \begin{array}{l}\text{OPEN-ATOM}\\ \text{STRUCT}\end{array}$$

Operational semantics

$$\dfrac{\dfrac{\dfrac{}{\bar{c}\langle x\rangle.P \xrightarrow{\bar{c}\langle x\rangle} P}\ \text{OUT-ATOM}}{\bar{c}\langle x\rangle.P \mid \{M/x\} \xrightarrow{\bar{c}\langle x\rangle} P \mid \{M/x\}}\ \text{PAR}}{\dfrac{\bar{c}\langle M\rangle.P \equiv \nu x.(\bar{c}\langle x\rangle.P \mid \{M/x\}) \xrightarrow{\nu x.\bar{c}\langle x\rangle} P \mid \{M/x\} \equiv P \mid \{M/x\}}{\bar{c}\langle M\rangle.P \xrightarrow{\nu x.\bar{c}\langle x\rangle} P \mid \{M/x\}}\ \text{STRUCT}}\ \text{OPEN-ATOM}$$

Operational semantics

$$\frac{}{\bar{c}\langle x\rangle.P \xrightarrow{\bar{c}\langle x\rangle} P} \quad \text{OUT-ATOM}$$

$$\frac{}{\bar{c}\langle x\rangle.P \,|\, \{M/x\} \xrightarrow{\bar{c}\langle x\rangle} P \,|\, \{M/x\}} \quad \text{PAR}$$

$$\frac{\bar{c}\langle M\rangle.P \equiv \nu x.(\bar{c}\langle x\rangle.P \,|\, \{M/x\}) \xrightarrow{\nu x.\bar{c}\langle x\rangle} P \,|\, \{M/x\} \equiv P \,|\, \{M/x\} \quad \text{OPEN-ATOM}}{\bar{c}\langle M\rangle.P \xrightarrow{\nu x.\bar{c}\langle x\rangle} P \,|\, \{M/x\}} \quad \text{STRUCT}$$

Operational semantics

$$\frac{}{\overline{c}\langle x\rangle.P \xrightarrow{\overline{c}\langle x\rangle} P} \quad \text{OUT-ATOM}$$

$$\frac{\overline{c}\langle x\rangle.P \xrightarrow{\overline{c}\langle x\rangle} P}{\overline{c}\langle x\rangle.P \mid \{M/x\} \xrightarrow{\overline{c}\langle x\rangle} P \mid \{M/x\}} \quad \text{PAR}$$

$$\overline{c}\langle M\rangle.P \equiv \nu x.(\overline{c}\langle x\rangle.P \mid \{M/x\}) \xrightarrow{\nu x.\overline{c}\langle x\rangle} P \mid \{M/x\} \equiv P \mid \{M/x\} \quad \text{OPEN-ATOM}$$

$$\frac{\overline{c}\langle M\rangle.P \equiv \nu x.(\overline{c}\langle x\rangle.P \mid \{M/x\}) \xrightarrow{\nu x.\overline{c}\langle x\rangle} P \mid \{M/x\} \equiv P \mid \{M/x\}}{\overline{c}\langle M\rangle.P \xrightarrow{\nu x.\overline{c}\langle x\rangle} P \mid \{M/x\}} \quad \text{STRUCT}$$

Operational semantics

$$\frac{}{\overline{c}\langle x\rangle.P \xrightarrow{\overline{c}\langle x\rangle} P} \quad \text{OUT-ATOM}$$

$$\frac{\overline{c}\langle x\rangle.P \xrightarrow{\overline{c}\langle x\rangle} P}{\overline{c}\langle x\rangle.P \,|\, \{M/x\} \xrightarrow{\overline{c}\langle x\rangle} P \,|\, \{M/x\}} \quad \text{PAR}$$

$$\overline{c}\langle M\rangle.P \equiv \nu x.(\overline{c}\langle x\rangle.P \,|\, \{M/x\}) \xrightarrow{\nu x.\overline{c}\langle x\rangle} P \,|\, \{M/x\} \equiv P \,|\, \{M/x\} \quad \text{OPEN-ATOM}$$

$$\frac{}{\overline{c}\langle M\rangle.P \xrightarrow{\nu x.\overline{c}\langle x\rangle} P \,|\, \{M/x\}} \quad \text{STRUCT}$$

Outline

Secrecy

- A closed process P preserves the secrecy of M if and only if $P|Q$ does not output M on c for any adversary Q and any $c \in \text{fn(A)}$
- example

$$\begin{aligned} I \triangleq\ & c(y\_pk).\overline{c}\langle \mathsf{pk}(sk_M)\rangle.c(x). \\ & \overline{c}\langle \mathsf{aenc}(y\_pk, \mathsf{adec}(sk_M, x))\rangle.c(z). \\ & \overline{c}\langle \mathsf{snd}(\mathsf{sdec}(\mathsf{getmsg}(\mathsf{adec}(sk_M, x)), z))\rangle \end{aligned}$$

Secrecy

- A closed process P preserves the secrecy of M if and only if $P|Q$ does not output M on c for any adversary Q and any $c \in \mathrm{fn(A)}$
- example

$$\begin{aligned} I \triangleq\ & c(y\_pk).\bar{c}\langle \mathrm{pk}(sk_M)\rangle.c(x). \\ & \bar{c}\langle \mathrm{aenc}(y\_pk, \mathrm{adec}(sk_M, x))\rangle.c(z). \\ & \bar{c}\langle \mathrm{snd}(\mathrm{sdec}(\mathrm{getmsg}(\mathrm{adec}(sk_M, x)), z))\rangle \end{aligned}$$

Secrecy

- A closed process P preserves the secrecy of M if and only if $P|Q$ does not output M on c for any adversary Q and any $c \in$ fn(A)
- example

$$\begin{array}{rcl} I & \triangleq & c(y\_pk).\overline{c}\langle \mathsf{pk}(sk_M)\rangle.c(x). \\ & & \overline{c}\langle \mathsf{aenc}(y\_pk, \mathsf{adec}(sk_M, x))\rangle.c(z). \\ & & \overline{c}\langle \mathsf{snd}(\mathsf{sdec}(\mathsf{getmsg}(\mathsf{adec}(sk_M, x)), z))\rangle \end{array}$$

Secrecy

- A closed process P preserves the secrecy of M if and only if $P|Q$ does not output M on c for any adversary Q and any $c \in \text{fn}(A)$
- example

$$
\begin{aligned}
I \triangleq\ & c(y\_pk).\overline{c}\langle \text{pk}(sk_M)\rangle.c(x). \\
& \overline{c}\langle \text{aenc}(y\_pk, \text{adec}(sk_M, x))\rangle.c(z). \\
& \overline{c}\langle \text{snd}(\text{sdec}(\text{getmsg}(\text{adec}(sk_M, x)), z))\rangle
\end{aligned}
$$

Secrecy

- A closed process P preserves the secrecy of M if and only if $P|Q$ does not output M on c for any adversary Q and any $c \in \mathrm{fn}(A)$
- example

$$
\begin{aligned}
I \quad \triangleq \quad & c(y\_pk).\overline{c}\langle \mathrm{pk}(sk_M)\rangle.c(x). \\
& \overline{c}\langle \mathrm{aenc}(y\_pk, \mathrm{adec}(sk_M, x))\rangle.c(z). \\
& \overline{c}\langle \mathrm{snd}(\mathrm{sdec}(\mathrm{getmsg}(\mathrm{adec}(sk_M, x)), z))\rangle
\end{aligned}
$$

Secrecy

- A closed process P preserves the secrecy of M if and only if $P|Q$ does not output M on c for any adversary Q and any $c \in$ fn(A)
- example

$$
\begin{aligned}
I \quad \triangleq \quad & c(y\_pk).\overline{c}\langle \mathrm{pk}(sk_M)\rangle.c(x). \\
& \overline{c}\langle \mathrm{aenc}(y\_pk, \mathrm{adec}(sk_M, x))\rangle.c(z). \\
& \overline{c}\langle \mathrm{snd}(\mathrm{sdec}(\mathrm{getmsg}(\mathrm{adec}(sk_M, x)), z))\rangle
\end{aligned}
$$

Secrecy

- A closed process P preserves the secrecy of M if and only if $P|Q$ does not output M on c for any adversary Q and any $c \in$ fn(A)
- example

$$
\begin{aligned}
I \quad \triangleq \quad & c(y\_pk).\overline{c}\langle \mathrm{pk}(sk_M)\rangle.c(x). \\
& \overline{c}\langle \mathrm{aenc}(y\_pk, \mathrm{adec}(sk_M, x))\rangle.c(z). \\
& \overline{c}\langle \mathrm{snd}(\mathrm{sdec}(\mathrm{getmsg}(\mathrm{adec}(sk_M, x)), z))\rangle
\end{aligned}
$$

Secrecy

- A closed process P preserves the secrecy of M if and only if $P|Q$ does not output M on c for any adversary Q and any $c \in$ fn(A)
- example

$$\begin{aligned} I \quad \triangleq \quad & c(y\_pk).\overline{c}\langle \mathrm{pk}(sk_M)\rangle.c(x). \\ & \overline{c}\langle \mathrm{aenc}(y\_pk, \mathrm{adec}(sk_M, x))\rangle.c(z). \\ & \overline{c}\langle \mathrm{snd}(\mathrm{sdec}(\mathrm{getmsg}(\mathrm{adec}(sk_M, x)), z))\rangle \end{aligned}$$

$$C[\_] \triangleq \nu sk_S.\nu sk_C.\nu s.(\_|!P_S|!P_C)$$

Secrecy

- A closed process P preserves the secrecy of M if and only if $P|Q$ does not output M on c for any adversary Q and any $c \in \text{fn(A)}$
- example

$$\begin{aligned} I \triangleq\ & c(y\_pk).\overline{c}\langle \text{pk}(sk_M)\rangle.c(x). \\ & \overline{c}\langle \text{aenc}(y\_pk, \text{adec}(sk_M, x))\rangle.c(z). \\ & \overline{c}\langle \text{snd}(\text{sdec}(\text{getmsg}(\text{adec}(sk_M, x)), z))\rangle \end{aligned}$$

$$C[\_] \triangleq \nu sk_S.\nu sk_C.\nu s.(\_|!P_S|!P_C)$$

$$P \equiv C[\overline{c}\langle pk_S\rangle|\overline{c}\langle pk_C\rangle|P_S|P_C]$$

Secrecy

$$
\begin{aligned}
P\,|I \quad \rightarrow \quad & C[\bar{c}\langle \mathsf{pk}(sk_S)\rangle | \bar{c}\langle pk_C\rangle \\
& |c(x\_pk).\nu k.\bar{c}\langle \mathsf{aenc}(x\_pk, \mathsf{sign}(sk_S, k))\rangle. \\
& c(z).\mathsf{if}\ \mathsf{fst}(\mathsf{sdec}(k, z)) = tag\ \mathsf{then}\ Q \\
& |c(y).\mathsf{if}\ \mathsf{checksign}(\mathsf{pk}(sk_S), \mathsf{adec}(sk_C, y)) = \mathsf{true}\ \mathsf{then} \\
& \bar{c}\langle \mathsf{senc}(\mathsf{getmsg}(\mathsf{adec}(sk_C, y)), \mathsf{pair}(tag, s))\rangle \\
& |c(y\_pk).\bar{c}\langle \mathsf{pk}(sk_M)\rangle.c(x). \\
& \bar{c}\langle \mathsf{aenc}(\mathsf{pk}(sk_C), \mathsf{adec}(sk_M, x))\rangle.c(z). \\
& \bar{c}\langle \mathsf{snd}(\mathsf{sdec}(\mathsf{getmsg}(\mathsf{adec}(sk_M, x)), z))\rangle]
\end{aligned}
$$

Secrecy

$$
\begin{aligned}
P\,|I \quad \rightarrow \quad & C[\overline{c}\langle \mathsf{pk}(sk_S)\rangle | \overline{c}\langle pk_C\rangle \\
& | c(x\_pk).\nu k.\overline{c}\langle \mathsf{aenc}(x\_pk, \mathsf{sign}(sk_S, k))\rangle. \\
& c(z).\text{if } \mathsf{fst}(\mathsf{sdec}(k, z)) = tag \text{ then } Q \\
& | c(y).\text{if } \mathsf{checksign}(\mathsf{pk}(sk_S), \mathsf{adec}(sk_C, y)) = \mathsf{true} \text{ then} \\
& \overline{c}\langle \mathsf{senc}(\mathsf{getmsg}(\mathsf{adec}(sk_C, y)), \mathsf{pair}(tag, s))\rangle \\
& | c(y\_pk).\overline{c}\langle \mathsf{pk}(sk_M)\rangle.c(x). \\
& \overline{c}\langle \mathsf{aenc}(\mathsf{pk}(sk_C), \mathsf{adec}(sk_M, x))\rangle.c(z). \\
& \overline{c}\langle \mathsf{snd}(\mathsf{sdec}(\mathsf{getmsg}(\mathsf{adec}(sk_M, x)), z))\rangle]
\end{aligned}
$$

Secrecy

$$
\begin{aligned}
P\,|I \quad \rightarrow \quad & C[\overline{c}\langle \mathsf{pk}(sk_S)\rangle | \overline{c}\langle pk_C\rangle \\
& |c(x\_pk).\nu k.\overline{c}\langle \mathsf{aenc}(x\_pk, \mathsf{sign}(sk_S, k))\rangle. \\
& c(z).\mathsf{if}\ \mathsf{fst}(\mathsf{sdec}(k, z)) = tag\ \mathsf{then}\ Q \\
& |c(y).\mathsf{if}\ \mathsf{checksign}(\mathsf{pk}(sk_S), \mathsf{adec}(sk_C, y)) = \mathsf{true}\ \mathsf{then} \\
& \overline{c}\langle \mathsf{senc}(\mathsf{getmsg}(\mathsf{adec}(sk_C, y)), \mathsf{pair}(tag, s))\rangle \\
& |c(y\_pk).\overline{c}\langle \mathsf{pk}(sk_M)\rangle.c(x). \\
& \overline{c}\langle \mathsf{aenc}(\mathsf{pk}(sk_C), \mathsf{adec}(sk_M, x))\rangle.c(z). \\
& \overline{c}\langle \mathsf{snd}(\mathsf{sdec}(\mathsf{getmsg}(\mathsf{adec}(sk_M, x)), z))\rangle]
\end{aligned}
$$

Secrecy

$$
\begin{aligned}
P \,|\, I \quad \rightarrow \quad & C[\bar{c}\langle \mathsf{pk}(sk_S)\rangle | \bar{c}\langle pk_C\rangle \\
& | c(x\_pk).\nu k.\bar{c}\langle \mathsf{aenc}(x\_pk, \mathsf{sign}(sk_S, k))\rangle. \\
& c(z).\mathsf{if}\ \mathsf{fst}(\mathsf{sdec}(k, z)) = tag\ \mathsf{then}\ Q \\
& | c(y).\mathsf{if}\ \mathsf{checksign}(\mathsf{pk}(sk_S), \mathsf{adec}(sk_C, y)) = \mathsf{true}\ \mathsf{then} \\
& \bar{c}\langle \mathsf{senc}(\mathsf{getmsg}(\mathsf{adec}(sk_C, y)), \mathsf{pair}(tag, s))\rangle \\
& {\color{red} | c(y\_pk).\bar{c}\langle \mathsf{pk}(sk_M)\rangle.c(x).} \\
& {\color{red} \bar{c}\langle \mathsf{aenc}(\mathsf{pk}(sk_C), \mathsf{adec}(sk_M, x))\rangle.c(z).} \\
& {\color{red} \bar{c}\langle \mathsf{snd}(\mathsf{sdec}(\mathsf{getmsg}(\mathsf{adec}(sk_M, x)), z))\rangle]}
\end{aligned}
$$

Secrecy

$$
\begin{aligned}
P\,|I \quad \rightarrow \quad & C[\overline{c}\langle \mathsf{pk}(sk_S)\rangle | \overline{c}\langle pk_C\rangle \\
& |c(x\_pk).\nu k.\overline{c}\langle \mathsf{aenc}(x\_pk, \mathsf{sign}(sk_S, k))\rangle. \\
& c(z).\mathsf{if}\ \mathsf{fst}(\mathsf{sdec}(k, z)) = tag\ \mathsf{then}\ Q \\
& |c(y).\mathsf{if}\ \mathsf{checksign}(\mathsf{pk}(sk_S), \mathsf{adec}(sk_C, y)) = \mathsf{true}\ \mathsf{then} \\
& \overline{c}\langle \mathsf{senc}(\mathsf{getmsg}(\mathsf{adec}(sk_C, y)), \mathsf{pair}(tag, s))\rangle \\
& |c(y\_pk)\overline{c}\langle \mathsf{pk}(sk_M)\rangle.c(x). \\
& \overline{c}\langle \mathsf{aenc}(\mathsf{pk}(sk_C), \mathsf{adec}(sk_M, x))\rangle.c(z). \\
& \overline{c}\langle \mathsf{snd}(\mathsf{sdec}(\mathsf{getmsg}(\mathsf{adec}(sk_M, x)), z))\rangle]
\end{aligned}
$$

Secrecy

$$
\begin{aligned}
P \,|\, I \quad \rightarrow \quad & C[\overline{c}\langle \mathsf{pk}(sk_S)\rangle \\
& |c(x\_pk).\nu k.\overline{c}\langle \mathsf{aenc}(x\_pk, \mathsf{sign}(sk_S, k))\rangle. \\
& c(z).\mathsf{if}\ \mathsf{fst}(\mathsf{sdec}(k, z)) = tag\ \mathsf{then}\ Q \\
& |c(y).\mathsf{if}\ \mathsf{checksign}(\mathsf{pk}(sk_S), \mathsf{adec}(sk_C, y)) = \mathsf{true}\ \mathsf{then} \\
& \overline{c}\langle \mathsf{senc}(\mathsf{getmsg}(\mathsf{adec}(sk_C, y)), \mathsf{pair}(tag, s))\rangle \\
& |\overline{c}\langle \mathsf{pk}(sk_M)\rangle.c(x). \\
& \overline{c}\langle \mathsf{aenc}(\mathsf{pk}(sk_C), \mathsf{adec}(sk_M, x))\rangle.c(z). \\
& \overline{c}\langle \mathsf{snd}(\mathsf{sdec}(\mathsf{getmsg}(\mathsf{adec}(sk_M, x)), z))\rangle]
\end{aligned}
$$

Secrecy

$$
\begin{array}{llll}
1. & P \,|\, I & \rightarrow & C[\bar{c}\langle \mathsf{pk}(sk_S)\rangle \\
 & & & |c(x\_pk).\nu k.\bar{c}\langle \mathsf{aenc}(x\_pk, \mathsf{sign}(sk_S, k))\rangle. \\
 & & & c(z).\mathsf{if}\ \mathsf{fst}(\mathsf{sdec}(k, z)) = tag\ \mathsf{then}\ Q \\
 & & & |c(y).\mathsf{if}\ \mathsf{checksign}(\mathsf{pk}(sk_S), \mathsf{adec}(sk_C, y)) = \mathsf{true}\ \mathsf{then} \\
 & & & \bar{c}\langle \mathsf{senc}(\mathsf{getmsg}(\mathsf{adec}(sk_C, y)), \mathsf{pair}(tag, s))\rangle \\
 & & & |\bar{c}\langle \mathsf{pk}(sk_M)\rangle.c(x). \\
 & & & \bar{c}\langle \mathsf{aenc}(\mathsf{pk}(sk_C), \mathsf{adec}(sk_M, x))\rangle.c(z). \\
 & & & \bar{c}\langle \mathsf{snd}(\mathsf{sdec}(\mathsf{getmsg}(\mathsf{adec}(sk_M, x)), z))\rangle]
\end{array}
$$

Secrecy

$$
\begin{array}{lll}
2. \quad P \,|\, I & \rightarrow & C[\overline{c}\langle \mathsf{pk}(sk_S)\rangle \\
& & |\nu k.\overline{c}\langle \mathsf{aenc}(\mathsf{pk}(sk_M)), \mathsf{sign}(sk_S, k))\rangle. \\
& & c(z).\mathsf{if}\ \mathsf{fst}(\mathsf{sdec}(k, z)) = tag\ \mathsf{then}\ Q \\
& & |c(y).\mathsf{if}\ \mathsf{checksign}(\mathsf{pk}(sk_S), \mathsf{adec}(sk_C, y)) = \mathsf{true}\ \mathsf{then} \\
& & \overline{c}\langle \mathsf{senc}(\mathsf{getmsg}(\mathsf{adec}(sk_C, y)), \mathsf{pair}(tag, s))\rangle \\
& & |c(x). \\
& & \overline{c}\langle \mathsf{aenc}(\mathsf{pk}(sk_C), \mathsf{adec}(sk_M, x))\rangle.c(z). \\
& & \overline{c}\langle \mathsf{snd}(\mathsf{sdec}(\mathsf{getmsg}(\mathsf{adec}(sk_M, x)), z))\rangle]
\end{array}
$$

Secrecy

$$
\begin{aligned}
2.\quad P \,|\, I \quad \rightarrow \quad & C[\overline{c}\langle \mathsf{pk}(sk_S)\rangle \\
& |\nu k.\overline{c}\langle \mathsf{aenc}(\mathsf{pk}(sk_M), \mathsf{sign}(sk_S, k))\rangle. \\
& c(z).\mathsf{if}\ \mathsf{fst}(\mathsf{sdec}(k, z)) = tag\ \mathsf{then}\ Q \\
& |c(y).\mathsf{if}\ \mathsf{checksign}(\mathsf{pk}(sk_S), \mathsf{adec}(sk_C, y)) = \mathsf{true}\ \mathsf{then} \\
& \overline{c}\langle \mathsf{senc}(\mathsf{getmsg}(\mathsf{adec}(sk_C, y)), \mathsf{pair}(tag, s))\rangle \\
& |c(x). \\
& \overline{c}\langle \mathsf{aenc}(\mathsf{pk}(sk_C), \mathsf{adec}(sk_M, x))\rangle.c(z). \\
& \overline{c}\langle \mathsf{snd}(\mathsf{sdec}(\mathsf{getmsg}(\mathsf{adec}(sk_M, x)), z))\rangle]
\end{aligned}
$$

Secrecy

3. $P \mid I \quad \rightarrow \quad \nu k.C[\overline{c}\langle \mathsf{pk}(sk_S)\rangle$
$\mid c(z).\mathsf{if}\ \mathsf{fst}(\mathsf{sdec}(k,z)) = tag\ \mathsf{then}\ Q$
$\mid c(y).\mathsf{if}\ \mathsf{checksign}(\mathsf{pk}(sk_S), \mathsf{adec}(sk_C, y)) = \mathsf{true}\ \mathsf{then}$
$\overline{c}\langle \mathsf{senc}(\mathsf{getmsg}(\mathsf{adec}(sk_C, y)), \mathsf{pair}(tag, s))\rangle$
$\mid \overline{c}\langle \mathsf{aenc}(\mathsf{pk}(sk_C), \mathsf{adec}(sk_M,$
$\mathsf{aenc}(\mathsf{pk}(sk_M), \mathsf{sign}(sk_S, k)))) \rangle.c(z).$
$\overline{c}\langle \mathsf{snd}(\mathsf{sdec}(\mathsf{getmsg}(\mathsf{adec}(sk_M,$
$\mathsf{aenc}(\mathsf{pk}(sk_M), \mathsf{sign}(sk_S, k)))), z))\rangle]$

Secrecy

$$
\begin{aligned}
3.\quad P \mid I \quad \rightarrow \quad & \nu k.C[\overline{c}\langle \mathsf{pk}(sk_S)\rangle \\
& | c(z).\text{if } \mathsf{fst}(\mathsf{sdec}(k,z)) = tag \text{ then } Q \\
& | c(y).\text{if } \mathsf{checksign}(\mathsf{pk}(sk_S), \mathsf{adec}(sk_C, y)) = \mathsf{true} \text{ then} \\
& \overline{c}\langle \mathsf{senc}(\mathsf{getmsg}(\mathsf{adec}(sk_C, y)), \mathsf{pair}(tag, s))\rangle \\
& | \overline{c}\langle \mathsf{aenc}(\mathsf{pk}(sk_C), \mathsf{adec}(sk_M, \\
& \mathsf{aenc}(\mathsf{pk}(sk_M), \mathsf{sign}(sk_S, k)))))\rangle.c(z). \\
& \overline{c}\langle \mathsf{snd}(\mathsf{sdec}(\mathsf{getmsg}(\mathsf{adec}(sk_M, \\
& \mathsf{aenc}(\mathsf{pk}(sk_M), \mathsf{sign}(sk_S, k)))), z))\rangle]
\end{aligned}
$$

Secrecy

4. $P \mid I \quad \rightarrow \quad \nu k.C[\overline{c}\langle \mathsf{pk}(sk_S)\rangle$

$|c(z).\mathsf{if}\ \mathsf{fst}(\mathsf{sdec}(k,z)) = tag\ \mathsf{then}\ Q$

$|\mathsf{if}\ \mathsf{checksign}(\mathsf{pk}(sk_S), \mathsf{adec}(sk_C, \mathsf{aenc}(\mathsf{pk}(sk_C),$
$\quad \mathsf{adec}(sk_M, \mathsf{aenc}(\mathsf{pk}(sk_M), \mathsf{sign}(sk_S, k)))))) = \mathsf{truethen}$

$\overline{c}\langle \mathsf{senc}(\mathsf{getmsg}(\mathsf{adec}(sk_C, \mathsf{aenc}(\mathsf{pk}(sk_C),$
$\quad \mathsf{adec}(sk_M, \mathsf{aenc}(\mathsf{pk}(sk_M), \mathsf{sign}(sk_S, k)))))), \mathsf{pair}(tag, s))\rangle$

$|c(z).$

$\overline{c}\langle \mathsf{snd}(\mathsf{sdec}(\mathsf{getmsg}(\mathsf{adec}(sk_M, \mathsf{aenc}(\mathsf{pk}(sk_M),$
$\mathsf{sign}(sk_S, k)))), z))\rangle]$

Secrecy

$$
\begin{aligned}
4.\quad P \,|\, I \quad \rightarrow \quad & \nu k.C[\overline{c}\langle \mathsf{pk}(sk_S)\rangle \\
& |c(z).\mathsf{if\ fst}(\mathsf{sdec}(k,z)) = tag \mathsf{\ then\ } Q \\
& |\mathsf{if\ checksign}(\mathsf{pk}(sk_S), \mathsf{adec}(sk_C, \mathsf{aenc}(\mathsf{pk}(sk_C), \\
& \quad \mathsf{adec}(sk_M, \mathsf{aenc}(\mathsf{pk}(sk_M), \mathsf{sign}(sk_S, k)))))) = \mathsf{truethen} \\
& \overline{c}\langle \mathsf{senc}(\mathsf{getmsg}(\mathsf{adec}(sk_C, \mathsf{aenc}(\mathsf{pk}(sk_C), \\
& \quad \mathsf{adec}(sk_M, \mathsf{aenc}(\mathsf{pk}(sk_M), \mathsf{sign}(sk_S, k)))))), \mathsf{pair}(tag, s))\rangle \\
& |c(z). \\
& \overline{c}\langle \mathsf{snd}(\mathsf{sdec}(\mathsf{getmsg}(\mathsf{adec}(sk_M, \mathsf{aenc}(\mathsf{pk}(sk_M), \\
& \mathsf{sign}(sk_S, k)))), z))\rangle]
\end{aligned}
$$

Secrecy

$$
\begin{aligned}
4.\quad P \,|\, I \quad \rightarrow \quad & \nu k.C[\bar{c}\langle \mathsf{pk}(sk_S)\rangle \\
& |c(z).\mathsf{if}\ \mathsf{fst}(\mathsf{sdec}(k, z)) = tag\ \mathsf{then}\ Q \\
& |\mathsf{if}\ \mathsf{checksign}(\mathsf{pk}(sk_S), \mathsf{adec}(sk_C, \mathsf{aenc}(\mathsf{pk}(sk_C), \\
& \quad \mathsf{adec}(sk_M, \mathsf{aenc}(\mathsf{pk}(sk_M), \mathsf{sign}(sk_S, k)))))) = \mathsf{truethen} \\
& \bar{c}\langle \mathsf{senc}(\mathsf{getmsg}(\mathsf{adec}(sk_C, \mathsf{aenc}(\mathsf{pk}(sk_C), \\
& \quad \mathsf{adec}(sk_M, \mathsf{aenc}(\mathsf{pk}(sk_M), \mathsf{sign}(sk_S, k)))))), \mathsf{pair}(tag, s))\rangle \\
& |c(z). \\
& \bar{c}\langle \mathsf{snd}(\mathsf{sdec}(\mathsf{getmsg}(\mathsf{adec}(sk_M, \mathsf{aenc}(\mathsf{pk}(sk_M), \\
& \mathsf{sign}(sk_S, k)))), z))\rangle]
\end{aligned}
$$

Secrecy

$$
\begin{aligned}
5.P\,|\,I \quad \equiv \quad & \nu k.C[\overline{c}\langle \mathsf{pk}(sk_S)\rangle \\
& |c(z).\text{if } \mathsf{fst}(\mathsf{sdec}(k,z)) = tag \text{ then } Q \\
& |\text{if } \textcolor{red}{\mathsf{true}} = \mathsf{true} \text{ then} \\
& \overline{c}\langle \mathsf{senc}(\textcolor{red}{k}, \mathsf{pair}(tag, s))\rangle \\
& |c(z).\overline{c}\langle \mathsf{snd}(\mathsf{sdec}(k,z))\rangle]
\end{aligned}
$$

Secrecy

$$
\begin{aligned}
5.\quad P \mid I \quad \equiv \quad & \nu k.C[\overline{c}\langle \mathsf{pk}(sk_S)\rangle \\
& \mid c(z).\mathsf{if}\ \mathsf{fst}(\mathsf{sdec}(k,z)) = tag\ \mathsf{then}\ Q \\
& \mid \mathsf{if}\ \mathsf{true} = \mathsf{true}\ \mathsf{then} \\
& \overline{c}\langle \mathsf{senc}(k, \mathsf{pair}(tag, s))\rangle \\
& \mid c(z).\overline{c}\langle \mathsf{snd}(\mathsf{sdec}(k,z))\rangle]
\end{aligned}
$$

Secrecy

$$6. \quad P \,|\, I \quad \rightarrow \quad \nu k.C[\overline{c}\langle \mathsf{pk}(sk_S)\rangle \\ |c(z).\text{if } \mathsf{fst}(\mathsf{sdec}(k,z)) = tag \text{ then } Q \\ |\overline{c}\langle \mathsf{snd}(\mathsf{sdec}(k, \mathsf{senc}(k, \mathsf{pair}(tag, s))))\rangle]$$

Secrecy

$$6.\quad P\,|\,I \;\rightarrow\; \nu k.C[\overline{c}\langle \mathsf{pk}(sk_S)\rangle \\ |c(z).\text{if } \mathsf{fst}(\mathsf{sdec}(k,z)) = tag \text{ then } Q \\ |\overline{c}\langle \mathsf{snd}(\mathsf{sdec}(k,\mathsf{senc}(k,\mathsf{pair}(tag,s))))\rangle]$$

Secrecy

$$7. \quad P \,|\, I \quad \equiv \quad \nu k.C[\overline{c}\langle \mathsf{pk}(sk_S)\rangle$$
$$|c(z).\text{if } \mathsf{fst}(\mathsf{sdec}(k, z)) = \mathit{tag} \text{ then } Q$$
$$|\overline{c}\langle s\rangle]$$

Outline

Correspondence properties

- Relationships between events
- Expressed as “if an event e has been executed then event e' has been previously executed”
- Events: message outputs $\overline{f}\langle M\rangle$
- Correspondence property: a formula of the form: $\overline{f}\langle M\rangle \leadsto \overline{g}\langle N\rangle$

Correspondence properties

$$P \triangleq \nu sk_S.\nu sk_C.\nu s.$$
$$\text{let } pk_S = \mathsf{pk}(sk_S) \text{ in let } pk_C = \mathsf{pk}(sk_C) \text{ in}$$
$$(\overline{c}\langle pk_S\rangle | \overline{c}\langle pk_C\rangle | !P_S | !P_C)$$

$$P_S \triangleq c(x\_pk).\nu k.\overline{startedS}\ \langle pair(x\_pk, k)\rangle$$
$$\overline{c}\langle \mathsf{aenc}(x\_pk, \mathsf{sign}(sk_S, k))\rangle.$$
$$c(z).\text{if } \mathsf{fst}(\mathsf{sdec}(k, z)) = tag \text{ then}$$
$$\overline{completedS}\ \langle pair(k, \mathsf{eq}(x\_pk, pk_C))\rangle.Q$$

$$P_C \triangleq c(y).\text{let } y' = \mathsf{adec}(sk_C, y) \text{ in let} y\_k = \mathsf{getmsg}(y') \text{ in}$$
$$\overline{startedC}\ \langle y\_k\rangle$$
$$\text{if } \mathsf{checksign}(pk_S, y') = \mathsf{true} \text{ then}$$
$$\overline{c}\langle \mathsf{senc}(y\_k, \mathsf{pair}(tag, s))\rangle$$
$$\overline{completedC}\ \langle pair(pk_C, y\_k)\rangle$$

Correspondence properties

- Authentication Example
  $\overline{completeC}\,\langle \text{pair}(x, y)\rangle \rightsquigarrow \overline{startedS}\,\langle \text{pair}(x, y)\rangle$
- Validity of corresondence property:
  Let E be an equational theory, and A_0 an extended process. We say that A_0 satisfies the correspondence property $\bar{f}\langle M\rangle \rightsquigarrow \bar{g}\langle N\rangle$ if for all excution paths
  $A_0 \rightarrow * \xrightarrow{\alpha_1}\rightarrow *A_1 \rightarrow * \xrightarrow{\alpha_2}\rightarrow * \ldots \rightarrow * \xrightarrow{\alpha_n}\rightarrow *A_n$
  and all index $i \in \mathbb{N}$, substitution α and variable e such that $\alpha_i = \nu e.\bar{f}\langle e\rangle$ and $e\varphi(A_i) =_E M_\alpha$, there exists $j \in \mathbb{N}$ and e' such that $\alpha_j = \nu e'.\bar{g}\langle e'\rangle$, $e'\varphi(A_j) =_E N_\alpha$ and $j < i$

Correspondence properties

$$
\begin{aligned}
P = \quad & C[\bar{c}\langle \mathsf{pk}(sk_S)\rangle | \bar{c}\langle pk_C\rangle \\
& | c(x\_pk).\nu k.\overline{startedS}\langle pair(x\_pk, k)\rangle \\
& \bar{c}\langle \mathsf{aenc}(x\_pk, \mathsf{sign}(sk_S, k))\rangle. \\
& c(z).\mathsf{if}\ \mathsf{fst}(\mathsf{sdec}(k, z)) = tag\ \mathsf{then} \\
& \overline{completedS}\langle pair(k, \mathsf{eq}(x\_pk, pk_C))\rangle.Q \\
& | c(y). \\
& \mathsf{let}\ y' = \mathsf{adec}(sk_C, y)\ \mathsf{in} \\
& \mathsf{let}\ y\_k = \mathsf{getmsg}(y')\ \mathsf{in} \\
& \overline{startedC}\langle y\_k\rangle \\
& \mathsf{if}\ \mathsf{checksign}(pk_S, y') = \mathsf{true}\ \mathsf{then} \\
& \bar{c}\langle \mathsf{senc}(y\_k, \mathsf{pair}(tag, s))\rangle \\
& \overline{completedC}\langle pair(pk_C, y\_k)\rangle]
\end{aligned}
$$

Correspondence properties

$$
\begin{aligned}
P = \quad & C[\overline{c}\langle \mathsf{pk}(sk_S)\rangle | \overline{c}\langle pk_C\rangle \\
& | c(x\_pk).\nu k.\overline{startedS}\langle pair(x\_pk, k)\rangle \\
& \overline{c}\langle \mathsf{aenc}(x\_pk, \mathsf{sign}(sk_S, k))\rangle. \\
& c(z).\mathsf{if}\ \mathsf{fst}(\mathsf{sdec}(k, z)) = tag\ \mathsf{then} \\
& \overline{completedS}\langle pair(k, \mathsf{eq}(x\_pk, pk_C))\rangle.Q \\
& | c(y). \\
& \mathsf{let}\ y' = \mathsf{adec}(sk_C, y)\ \mathsf{in} \\
& \mathsf{let}\ y\_k = \mathsf{getmsg}(y')\ \mathsf{in} \\
& \overline{startedC}\langle y\_k\rangle \\
& \mathsf{if}\ \mathsf{checksign}(pk_S, y') = \mathsf{true}\ \mathsf{then} \\
& \overline{c}\langle \mathsf{senc}(y\_k, \mathsf{pair}(tag, s))\rangle \\
& \overline{completedC}\langle pair(pk_C, y\_k)\rangle]
\end{aligned}
$$

Correspondence properties

$$
\begin{aligned}
P = \quad & C[\overline{c}\langle \mathsf{pk}(sk_S)\rangle | \overline{c}\langle pk_C\rangle \\
& | c(x\_pk).\nu k.\overline{startedS}\langle pair(x\_pk, k)\rangle \\
& \overline{c}\langle \mathsf{aenc}(x\_pk, \mathsf{sign}(sk_S, k))\rangle. \\
& c(z).\mathsf{if}\ \mathsf{fst}(\mathsf{sdec}(k, z)) = tag\ \mathsf{then} \\
& \overline{completedS}\langle pair(k, \mathsf{eq}(x\_pk, pk_C))\rangle.Q \\
& | c(y). \\
& \mathsf{let}\ y' = \mathsf{adec}(sk_C, y)\ \mathsf{in} \\
& \mathsf{let}\ y\_k = \mathsf{getmsg}(y')\ \mathsf{in} \\
& \overline{startedC}\langle y\_k\rangle \\
& \mathsf{if}\ \mathsf{checksign}(pk_S, y') = \mathsf{true}\ \mathsf{then} \\
& \overline{c}\langle \mathsf{senc}(y\_k, \mathsf{pair}(tag, s))\rangle \\
& \overline{completedC}\langle pair(pk_C, y\_k)\rangle]
\end{aligned}
$$

Correspondence properties

$$
\begin{aligned}
P = \quad & C[\overline{c}\langle \mathsf{pk}(sk_S)\rangle | \overline{c}\langle pk_C\rangle \\
& | c(x\_pk).\nu k.\overline{startedS}\langle pair(x\_pk, k)\rangle \\
& \overline{c}\langle \mathsf{aenc}(x\_pk, \mathsf{sign}(sk_S, k))\rangle. \\
& c(z).\text{if } \mathsf{fst}(\mathsf{sdec}(k, z)) = tag \text{ then} \\
& \overline{completedS}\langle pair(k, \mathsf{eq}(x\_pk, pk_C))\rangle.Q \\
& | c(y). \\
& \text{let } y' = \mathsf{adec}(sk_C, y) \text{ in} \\
& \text{let } y\_k = \mathsf{getmsg}(y') \text{ in} \\
& \overline{startedC}\langle y\_k\rangle \\
& \text{if } \mathsf{checksign}(pk_S, y') = \text{true then} \\
& \overline{c}\langle \mathsf{senc}(y\_k, \mathsf{pair}(tag, s))\rangle \\
& \overline{completedC}\langle pair(pk_C, y\_k)\rangle]
\end{aligned}
$$

Correspondence properties

1. $$
\begin{array}{ll}
P \xrightarrow{\nu y_pk.\overline{c}\langle y_pk\rangle} & C[\overline{c}\langle \mathsf{pk}(sk_S)\rangle | \{\mathsf{pk}(sk_C)/y_pk\} \\
& | c(x_pk).\nu k.\overline{startedS}\langle pair(x_pk, k)\rangle \\
& \overline{c}\langle \mathsf{aenc}(x_pk, \mathsf{sign}(sk_S, k))\rangle. \\
& c(z).\mathsf{if}\ \mathsf{fst}(\mathsf{sdec}(k, z)) = tag\ \mathsf{then} \\
& \overline{completedS}\langle pair(k, \mathsf{eq}(x_pk, pk_C))\rangle.Q \\
& | c(y). \\
& \mathsf{let}\ y' = \mathsf{adec}(sk_C, y)\ \mathsf{in} \\
& \mathsf{let}\ y_k = \mathsf{getmsg}(y')\ \mathsf{in} \\
& \overline{startedC}\langle y_k\rangle \\
& \mathsf{if}\ \mathsf{checksign}(pk_S, y') = \mathsf{true}\ \mathsf{then} \\
& \overline{c}\langle \mathsf{senc}(y_k, \mathsf{pair}(tag, s))\rangle \\
& \overline{completedC}\langle pair(pk_C, y_k)\rangle]
\end{array}
$$

Correspondence properties

1. $$P \xrightarrow{\nu y\_pk.\bar{c}\langle y\_k\rangle} \begin{array}{l} C[\bar{c}\langle \mathsf{pk}(sk_S)\rangle | \{\mathsf{pk}(sk_C)/y\_pk\} \\ | c(x\_pk).\nu k.\overline{startedS}\langle pair(x\_pk, k\rangle \\ \bar{c}\langle \mathsf{aenc}(x\_pk, \mathsf{sign}(sk_S, k))\rangle. \\ c(z).\mathsf{if\ fst}(\mathsf{sdec}(k, z)) = tag \mathsf{\ then} \\ \overline{completedS}\langle pair(k, \mathsf{eq}(x\_pk, pk_C))\rangle.Q \\ | c(y). \\ \mathsf{let\ } y' = \mathsf{adec}(sk_C, y) \mathsf{\ in} \\ \mathsf{let\ } y\_k = \mathsf{getmsg}(y') \mathsf{\ in} \\ \overline{startedC}\langle y\_k\rangle \\ \mathsf{if\ checksign}(pk_S, y') = \mathsf{true\ then} \\ \bar{c}\langle \mathsf{senc}(y\_k, \mathsf{pair}(tag, s))\rangle \\ \overline{completedC}\langle pair(pk_C, y\_k)\rangle] \end{array}$$

Correspondence properties

1. $P \xrightarrow{\nu y\_pk.\overline{c}\langle y\_k\rangle}$ $C[\overline{c}\langle \mathsf{pk}(sk_S)\rangle | \{\mathsf{pk}(sk_C)/y\_pk\}$
$| c(x\_pk).\nu k.\overline{startedS}\langle pair(x\_pk, k)\rangle$
$\overline{c}\langle \mathsf{aenc}(x\_pk, \mathsf{sign}(sk_S, k))\rangle.$
$c(z).\text{if } \mathsf{fst}(\mathsf{sdec}(k, z)) = tag \text{ then}$
$\overline{completedS}\langle pair(k, \mathsf{eq}(x\_pk, pk_C))\rangle.Q$
$| c(y).$
$\text{let } y' = \mathsf{adec}(sk_C, y) \text{ in}$
$\text{let } y\_k = \mathsf{getmsg}(y') \text{ in}$
$\overline{startedC}\langle y\_k\rangle$
$\text{if } \mathsf{checksign}(pk_S, y') = \mathsf{true} \text{ then}$
$\overline{c}\langle \mathsf{senc}(y\_k, \mathsf{pair}(tag, s))\rangle$
$\overline{completedC}\langle pair(pk_C, y\_k)\rangle]$

Correspondence properties

2. $\xrightarrow{c(\mathsf{pk}(sk_M))}$

$$
\begin{array}{l}
C[\overline{c}\langle \mathsf{pk}(sk_S)\rangle | \{\mathsf{pk}(sk_C)/y\_pk\} \\
|\nu k.\overline{startedS}\langle pair(x\_pk, k)\rangle \\
\overline{c}\langle \mathsf{aenc}(x\_pk, \mathsf{sign}(sk_S, k))\rangle. \\
c(z).\mathsf{if}\ \mathsf{fst}(\mathsf{sdec}(k, z)) = tag\ \mathsf{then} \\
\overline{completedS}\langle pair(k, \mathsf{eq}(x\_pk, pk_C))\rangle.Q \\
|c(y). \\
\mathsf{let}\ y' = \mathsf{adec}(sk_C, y)\ \mathsf{in} \\
\mathsf{let}\ y\_k = \mathsf{getmsg}(y')\ \mathsf{in} \\
\overline{startedC}\langle y\_k\rangle \\
\mathsf{if}\ \mathsf{checksign}(pk_S, y') = \mathsf{true}\ \mathsf{then} \\
\overline{c}\langle \mathsf{senc}(y\_k, \mathsf{pair}(tag, s))\rangle \\
\overline{completedC}\langle pair(pk_C, y\_k)\rangle]
\end{array}
$$

Correspondence properties

2. $\xrightarrow{c(\mathsf{pk}(sk_M))}$

$$
\begin{array}{l}
C[\overline{c}\langle \mathsf{pk}(sk_S)\rangle | \{\mathsf{pk}(sk_C)/y\_pk\} \\
|\nu k.\overline{startedS}\langle pair(x\_pk, k)\rangle \\
\overline{c}\langle \mathsf{aenc}(x\_pk, \mathsf{sign}(sk_S, k))\rangle. \\
c(z).\text{if } \mathsf{fst}(\mathsf{sdec}(k, z)) = tag \text{ then} \\
\overline{completedS}\langle pair(k, \mathsf{eq}(x\_pk, pk_C))\rangle.Q \\
|c(y). \\
\text{let } y' = \mathsf{adec}(sk_C, y) \text{ in} \\
\text{let } y\_k = \mathsf{getmsg}(y') \text{ in} \\
\overline{startedC}\langle y\_k\rangle \\
\text{if } \mathsf{checksign}(pk_S, y') = \mathsf{true} \text{ then} \\
\overline{c}\langle \mathsf{senc}(y\_k, \mathsf{pair}(tag, s))\rangle \\
\overline{completedC}\langle pair(pk_C, y\_k)\rangle]
\end{array}
$$

Correspondence properties

3. $\xrightarrow{\nu e_1.\overline{startedS}\langle e_1\rangle}$

$$
\begin{aligned}
&\nu k.C[\overline{c}\langle \mathsf{pk}(sk_S)\rangle|\{\mathsf{pk}(sk_C)/y\_pk\}\\
&|\{pair(\mathsf{pk}(sk_M),k)/e_1\}\\
&|\overline{c}\langle \mathsf{aenc}(x\_pk,\mathsf{sign}(sk_S,k))\rangle.\\
&c(z).\mathsf{if\ fst}(\mathsf{sdec}(k,z)) = tag\ \mathsf{then}\\
&\overline{completedS}\langle pair(k,\mathsf{eq}(x\_pk,pk_C))\rangle.Q\\
&|c(y).\\
&\mathsf{let}\ y' = \mathsf{adec}(sk_C,y)\ \mathsf{in}\\
&\mathsf{let}\ y\_k = \mathsf{getmsg}(y')\ \mathsf{in}\\
&\overline{startedC}\langle y\_k\rangle\\
&\mathsf{if\ checksign}(pk_S,y') = \mathsf{true\ then}\\
&\overline{c}\langle \mathsf{senc}(y\_k,\mathsf{pair}(tag,s))\rangle\\
&\overline{completedC}\langle pair(pk_C,y\_k)\rangle]
\end{aligned}
$$

Correspondence properties

3. $\xrightarrow{\nu e_1.\overline{startedS}\langle e_1\rangle}$ $\nu k.C[\overline{c}\langle \mathsf{pk}(sk_S)\rangle | \{\mathsf{pk}(sk_C)/y\_pk\}$
$|\{pair(\mathsf{pk}(sk_M), k)/e_1\}$
$|\overline{c}\langle \mathsf{aenc}(x\_pk, \mathsf{sign}(sk_S, k))\rangle.$
$c(z).\text{if } \mathsf{fst}(\mathsf{sdec}(k, z)) = tag \text{ then}$
$\overline{completedS}\langle pair(k, \mathsf{eq}(x\_pk, pk_C))\rangle.Q$
$|c(y).$
$\text{let } y' = \mathsf{adec}(sk_C, y) \text{ in}$
$\text{let } y\_k = \mathsf{getmsg}(y') \text{ in}$
$\overline{startedC}\langle y\_k\rangle$
$\text{if } \mathsf{checksign}(pk_S, y') = \text{true then}$
$\overline{c}\langle \mathsf{senc}(y\_k, \mathsf{pair}(tag, s))\rangle$
$\overline{completedC}\langle pair(pk_C, y\_k)\rangle]$

Correspondence properties

4. $\xrightarrow{\nu x.\overline{c}\langle x\rangle}$

$$
\begin{aligned}
&\nu k.C[\overline{c}\langle \mathsf{pk}(sk_S)\rangle | \{\mathsf{pk}(sk_C)/y\_pk\} \\
&|\{pair(\mathsf{pk}(sk_M), k)/e_1\} \\
&|\{aenc(\mathsf{pk}(sk_M), sign(sk_S, k))/x\} \\
&|c(z).\text{if } \mathsf{fst}(\mathsf{sdec}(k, z)) = tag \text{ then} \\
&\overline{completedS}\langle pair(k, \mathsf{eq}(\mathsf{pk}(sk_M), \mathsf{pk}_{sk_C}))\rangle.Q \\
&|c(y). \\
&\text{let } y' = \mathsf{adec}(sk_C, y) \text{ in} \\
&\text{let } y\_k = \mathsf{getmsg}(y') \text{ in} \\
&\overline{startedC}\langle y\_k\rangle \\
&\text{if } \mathsf{checksign}(pk_S, y') = \mathsf{true} \text{ then} \\
&\overline{c}\langle \mathsf{senc}(y\_k, \mathsf{pair}(tag, s))\rangle \\
&\overline{completedC}\langle pair(pk_C, y\_k)\rangle]
\end{aligned}
$$

Correspondence properties

4. $\xrightarrow{\nu x.\overline{c}\langle x\rangle}$ $\nu k.C[\overline{c}\langle \mathsf{pk}(sk_S)\rangle | \{\mathsf{pk}(sk_C)/y\_pk\}$
$|\{pair(\mathsf{pk}(sk_M), k)/e_1\}$
$|\{aenc(\mathsf{pk}(sk_M), sign(sk_S, k))/x\}$
$|c(z).\text{if } \mathsf{fst}(\mathsf{sdec}(k, z)) = tag \text{ then}$
$\overline{completedS}\langle pair(k, \mathsf{eq}(\mathsf{pk}(sk_M), \mathsf{pk}_{sk_C}))\rangle.Q$
$|c(y).$
$\text{let } y' = \mathsf{adec}(sk_C, y) \text{ in}$
$\text{let } y\_k = \mathsf{getmsg}(y') \text{ in}$
$\overline{startedC}\langle y\_k\rangle$
$\text{if } \mathsf{checksign}(pk_S, y') = \mathsf{true} \text{ then}$
$\overline{c}\langle \mathsf{senc}(y\_k, \mathsf{pair}(tag, s))\rangle$
$\overline{completedC}\langle pair(pk_C, y\_k)\rangle]$

Correspondence properties

5. $\xrightarrow{c(\mathrm{aenc}(y\_pk,\mathrm{adec}(sk_M,x)))}$

$$
\begin{aligned}
&\nu k.C[\overline{c}\langle \mathrm{pk}(sk_S)\rangle | \{\mathrm{pk}(sk_C)/y\_pk\} \\
&|\{pair(\mathrm{pk}(sk_M), k)/e_1\} \\
&|\{aenc(\mathrm{pk}(sk_M), sign(sk_S, k))/x\} \\
&|c(z).\text{if } \mathrm{fst}(\mathrm{sdec}(k, z)) = tag \text{ then} \\
&\overline{completedS}\langle pair(k, \mathrm{eq}(\mathrm{pk}(sk_M), \mathrm{pk}_{sk_C}))\rangle.Q \\
&|\text{let } y' = \mathrm{adec}(sk_C, \mathrm{aenc}(y\_pk, \mathrm{adec}(sk_M, x))) \text{ in} \\
&\text{let } y\_k = \mathrm{getmsg}(y') \text{ in} \\
&\overline{startedC}\langle y\_k\rangle \\
&\text{if checksign}(pk_S, y') = \text{true then} \\
&\overline{c}\langle \mathrm{senc}(y\_k, \mathrm{pair}(tag, s))\rangle \\
&\overline{completedC}\langle pair(pk_C, y\_k)\rangle]
\end{aligned}
$$

Correspondence properties

5. $\xrightarrow{c(\mathsf{aenc}(y\_pk,\mathsf{adec}(sk_M,x)))}$

$$
\begin{aligned}
&\nu k.C[\overline{c}\langle \mathsf{pk}(sk_S)\rangle | \{\mathsf{pk}(sk_C)/y\_pk\}\\
&|\{pair(\mathsf{pk}(sk_M),k)/e_1\}\\
&|\{aenc(\mathsf{pk}(sk_M),sign(sk_S,k))/x\}\\
&|c(z).\text{if } \mathsf{fst}(\mathsf{sdec}(k,z)) = tag \text{ then}\\
&\overline{completedS}\langle pair(k,\mathsf{eq}(\mathsf{pk}(sk_M),\mathsf{pk}_{sk_C}))\rangle.Q\\
&|\text{let } y' = \mathsf{adec}(sk_C,\mathsf{aenc}(y\_pk,\mathsf{adec}(sk_M,x))) \text{ in}\\
&\text{let } y\_k = \mathsf{getmsg}(y') \text{ in}\\
&\overline{startedC}\langle y\_k\rangle\\
&\text{if } \mathsf{checksign}(pk_S,y') = \text{true then}\\
&\overline{c}\langle \mathsf{senc}(y\_k,\mathsf{pair}(tag,s))\rangle\\
&\overline{completedC}\langle pair(pk_C,y\_k)\rangle]
\end{aligned}
$$

Correspondence properties

$$
\begin{array}{lll}
6. & \equiv & \nu k.C[\overline{c}\langle \mathsf{pk}(sk_S)\rangle | \{\mathsf{pk}(sk_C)/y\_pk\} \\
 & & |\{pair(\mathsf{pk}(sk_M), k)/e_1\} \\
 & & |\{aenc(\mathsf{pk}(sk_M), sign(sk_S, k))/x\} \\
 & & |c(z).\mathsf{if}\ \mathsf{fst}(\mathsf{sdec}(k, z)) = tag\ \mathsf{then} \\
 & & \overline{completedS}\langle pair(k, \mathsf{eq}(\mathsf{pk}(sk_M), \mathsf{pk}_{sk_C}))\rangle.Q \\
 & & |\overline{startedC}\langle k\rangle \\
 & & \mathsf{if}\ \mathsf{true} = \mathsf{true}\ \mathsf{then} \\
 & & \overline{c}\langle \mathsf{senc}(k, \mathsf{pair}(tag, s))\rangle \\
 & & \overline{completedC}\langle pair(pk_C, k)\rangle]
\end{array}
$$

Correspondence properties

$$
\begin{array}{lll}
6. & \equiv & \nu k.C[\overline{c}\langle \mathsf{pk}(sk_S)\rangle | \{\mathsf{pk}(sk_C)/y\_pk\} \\
 & & |\{pair(\mathsf{pk}(sk_M), k)/e_1\} \\
 & & |\{aenc(\mathsf{pk}(sk_M), sign(sk_S, k))/x\} \\
 & & |c(z).\mathsf{if}\ \mathsf{fst}(\mathsf{sdec}(k, z)) = tag\ \mathsf{then} \\
 & & \overline{completedS}\langle pair(k, \mathsf{eq}(\mathsf{pk}(sk_M), \mathsf{pk}_{sk_C}))\rangle.Q \\
 & & |\overline{startedC}\langle k\rangle \\
 & & \mathsf{if}\ \mathsf{true} = \mathsf{true}\ \mathsf{then} \\
 & & \overline{c}\langle \mathsf{senc}(k, \mathsf{pair}(tag, s))\rangle \\
 & & \overline{completedC}\langle pair(pk_C, k)\rangle]
\end{array}
$$

Correspondence properties

7. $\nu e_2.\overline{startedC}\langle e_2\rangle \longrightarrow$

$$
\begin{aligned}
&\nu k.C[\overline{c}\langle \mathsf{pk}(sk_S)\rangle | \{\mathsf{pk}(sk_C)/y\_pk\} \\
&|\{pair(\mathsf{pk}(sk_M), k)/e_1\} \\
&|\{aenc(\mathsf{pk}(sk_M), sign(sk_S, k))/x\} \\
&|c(z).\text{if fst(sdec}(k, z)) = tag \text{ then} \\
&\overline{completedS}\langle pair(k, \mathsf{eq}(\mathsf{pk}(sk_M), \mathsf{pk}_{sk_C}))\rangle.Q \\
&|\{k/e_2\} \\
&|\text{if true} = \text{true then} \\
&\overline{c}\langle \mathsf{senc}(k, \mathsf{pair}(tag, s))\rangle \\
&\overline{completedC}\langle pair(pk_C, k)\rangle]
\end{aligned}
$$

Correspondence properties

7. $\xrightarrow{\nu e_2.\overline{startedC}\langle e_2\rangle}$

$$
\begin{aligned}
&\nu k.C[\overline{c}\langle \mathsf{pk}(sk_S)\rangle | \{\mathsf{pk}(sk_C)/y\_pk\}\\
&|\{pair(\mathsf{pk}(sk_M), k)/e_1\}\\
&|\{aenc(\mathsf{pk}(sk_M), sign(sk_S, k))/x\}\\
&|c(z).\text{if } \mathsf{fst}(\mathsf{sdec}(k, z)) = tag \text{ then}\\
&\overline{completedS}\langle pair(k, \mathsf{eq}(\mathsf{pk}(sk_M), \mathsf{pk}_{sk_C}))\rangle.Q\\
&|\{k/e_2\}\\
&|\text{if true} = \text{true then}\\
&\overline{c}\langle \mathsf{senc}(k, \mathsf{pair}(tag, s))\rangle\\
&\overline{completedC}\langle pair(pk_C, k)\rangle]
\end{aligned}
$$

Correspondence properties

8. $\xrightarrow{\nu z.\overline{c}\langle z\rangle}$

$$
\begin{array}{l}
\nu k.C[\overline{c}\langle \mathrm{pk}(sk_S)\rangle | \{\mathrm{pk}(sk_C)/y\_pk\} \\
|\{pair(\mathrm{pk}(sk_M), k)/e_1\} \\
|\{aenc(\mathrm{pk}(sk_M), sign(sk_S, k))/x\} \\
|c(z).\mathrm{if\ fst}(\mathrm{sdec}(k, z)) = tag \mathrm{\ then} \\
\overline{completedS}\langle pair(k, \mathrm{eq}(\mathrm{pk}(sk_M), \mathrm{pk}_{sk_C}))\rangle.Q \\
|\{k/e_2\} \\
|\{\mathrm{senc}(k, \mathrm{pair}(tag, s))/z\} \\
|\overline{completedC}\langle pair(pk_C, k)\rangle]
\end{array}
$$

Correspondence properties

$$8. \xrightarrow{\nu z.\overline{c}\langle z\rangle} \nu k.C[\overline{c}\langle \mathsf{pk}(sk_S)\rangle | \{\mathsf{pk}(sk_C)/y\_pk\}$$
$$|\{pair(\mathsf{pk}(sk_M), k)/e_1\}$$
$$|\{aenc(\mathsf{pk}(sk_M), sign(sk_S, k))/x\}$$
$$|c(z).\text{if } \mathsf{fst}(\mathsf{sdec}(k, z)) = tag \text{ then}$$
$$\overline{completedS}\langle pair(k, \mathsf{eq}(\mathsf{pk}(sk_M), \mathsf{pk}_{sk_C}))\rangle.Q$$
$$|\{k/e_2\}$$
$$|\{\mathsf{senc}(k, \mathsf{pair}(tag, s))/z\}$$
$$|\overline{completedC}\langle pair(pk_C, k)\rangle]$$

Correspondence properties

9. $\xrightarrow{\nu e_3.\overline{completedC}\langle e_3\rangle}$

$$
\begin{aligned}
&\nu k.C[\overline{c}\langle \mathsf{pk}(sk_S)\rangle|\{\mathsf{pk}(sk_C)/y\_pk\}\\
&|\{pair(\mathsf{pk}(sk_M),k)/e_1\}\\
&|\{aenc(\mathsf{pk}(sk_M),sign(sk_S,k))/x\}\\
&|c(z).\mathsf{if}\ \mathsf{fst}(\mathsf{sdec}(k,z)) = tag\ \mathsf{then}\\
&\overline{completedS}\langle pair(k,\mathsf{eq}(\mathsf{pk}(sk_M),\mathsf{pk}_{sk_C}))\rangle.Q\\
&|\{k/e_2\}\\
&|\{\mathsf{senc}(k,\mathsf{pair}(tag,s))/z\}\\
&|\{\mathsf{pair}(\mathsf{pk}(sk_C),k)/e_3\}
\end{aligned}
$$

Correspondence properties

9. $\xrightarrow{\nu e_3.\overline{completedC}\langle e_3\rangle}$

$$\begin{aligned}&\nu k.C[\overline{c}\langle \mathsf{pk}(sk_S)\rangle | \{\mathsf{pk}(sk_C)/y\_pk\} \\ &| \{pair(\mathsf{pk}(sk_M), k)/e_1\} \\ &| \{aenc(\mathsf{pk}(sk_M), sign(sk_S, k))/x\} \\ &| c(z).\text{if } \mathsf{fst}(\mathsf{sdec}(k, z)) = tag \text{ then} \\ &\overline{completedS}\langle pair(k, \mathsf{eq}(\mathsf{pk}(sk_M), \mathsf{pk}_{sk_C}))\rangle.Q \\ &| \{k/e_2\} \\ &| \{\mathsf{senc}(k, \mathsf{pair}(tag, s))/z\} \\ &| \{\mathsf{pair}(\mathsf{pk}(sk_C), k)/e_3\}\end{aligned}$$

e_1 is $startedS$, e_3 is $completedC$

Correspondence properties

- Example

$$\overline{start}\langle n\rangle.\overline{complete}\langle n\rangle.\overline{complete}\langle n\rangle$$

$$\overline{complete}\ \langle x\rangle \rightsquigarrow \overline{start}\ \langle x\rangle$$

- Injective correspondence property: a formula of the form: $\overline{f}\langle M\rangle \rightsquigarrow\ inj\ \overline{g}\langle N\rangle$

Correspondence properties

- Validity of injective correspondence property:
  Let E be an equational theory, and A_0 an extended process. We say that A_0 satisfies the correspondence property $\overline{f}\langle M\rangle \rightsquigarrow inj\ \overline{g}\langle N\rangle$ if for all excution paths
  $A_0 \rightarrow * \xrightarrow{\alpha_1}\rightarrow *A_1 \rightarrow * \xrightarrow{\alpha_2}\rightarrow * \ldots \rightarrow * \xrightarrow{\alpha_n}\rightarrow *A_n$
  there exists a partial injective function
  $h : \{1, \ldots, n\} \rightarrow \{1, \ldots, n\}$ such that for all $i \in \{1, \ldots, n\}$, substitution α and variable e such that $\alpha_i = \nu e.\overline{f}\langle e\rangle$ and $e\varphi(A_i) =_E M_\alpha$, then the following conditions are satisfied: (1) $h(i)$ is defined; (2) $\alpha_{h(i)} = \nu e'.\overline{g}\langle e'\rangle$ for some e' such that $e'\varphi(A_{h(i)}) =_E N_\alpha$; and (3) $h(i) < i$.

Questions and comments

Questions and comments?