

# The Spi-calculus: Syntax and Operational Semantics

## Messages:

$x, y, z$	variables
$m, n, k, l, c, d, e$	names
$M, N, K, L ::=$	message
$x$	variable
$n$	name
$(M_1, \dots, M_n)$	tuple
$\{M\}_K$	$M$ encrypted with symmetric key $K$
$\{\! M \!\}_K$	$M$ encrypted with asymmetric key $K$
$\#(M)$	hash of $M$
$\text{Enc}(K)$	encryption key of asymmetric key $K$
$\text{Dec}(K)$	decryption key of asymmetric key $K$

## Processes:

$O, P, Q, R ::=$	process
stop	inactivity
out $L M; P$	output message $M$ on channel $L$
inp $L x; P$	input $x$ from channel $L$ (binding $x$ in $P$ )
$P \mid Q$	parallel composition
if $M = N$ then $P$	conditional
$!P$	replication
new $n; P$	generating name $n$ (binding $n$ in $P$ )
split $M$ is $(x_1, \dots, x_n); P$	splitting tuple $M$ (binding $x_1, \dots, x_n$ in $P$ )
decrypt $M$ is $\{x\}_K; P$	symmetrically decrypting $M$ (binding $x$ in $P$ )
decrypt $M$ is $\{\! x \!\}_{K^{-1}}; P$	asymmetrically decrypting $M$ (binding $x$ in $P$ )

For better readability, we often omit **stop**. E.g., we write  $\text{out } L M;$  instead of  $\text{out } L M; \text{stop}$ .

## Structural Congruence, $P \equiv Q$ :

$P \mid \text{stop} \equiv P$	(Struct Stop)
$P \mid Q \equiv Q \mid P$	(Struct Comm)
$(P \mid Q) \mid R \equiv P \mid (Q \mid R)$	(Struct Assoc)
$!P \equiv P \mid !P$	(Struct Repl)
$n$ not free in $P \Rightarrow P \mid \text{new } n; Q \equiv \text{new } n; (P \mid Q)$	(Struct New)

These rules may be applied anywhere in processes.

## Step Relation, $P \rightarrow Q$ :

$P \equiv P', P' \rightarrow Q', Q' \equiv Q \Rightarrow P \rightarrow Q$	(Step Equiv)
---	--------------

$P \rightarrow P' \Rightarrow P \mid Q \rightarrow P' \mid Q$	(Step Par)
$P \rightarrow P' \Rightarrow \text{new } n; P \rightarrow \text{new } n; P'$	(Step New)
$\text{out } c \ M; P \mid \text{inp } c \ x; Q \rightarrow P \mid \{M/x\}Q$	(Step IO)
$\text{if } M = M \text{ then } P \rightarrow P$	(Step Cond)
$\text{split } (M_1, \dots, M_n) \text{ is } (x_1, \dots, x_n); P \rightarrow \{M_1, \dots, M_n/x_1, \dots, x_n\}P$	(Step Split)
$\text{decrypt } \{M\}_K \text{ is } \{x\}_K; P \rightarrow \{M/x\}P$	(Step SDecrypt)
$\text{decrypt } \{M\}_{\text{Enc}(K)} \text{ is } \{x\}_{\text{Dec}(K)^{-1}}; P \rightarrow \{M/x\}P$	(Step ADecrypt)

---