



---

# RAPPORT TECHNIQUE EVA

---

## Les syntaxes et la sémantique du langage de spécification EVA

**Date** : 16 Novembre 2001  
**Auteurs** : Jean Goubault-Larrecq  
**Titre** : Les syntaxes et la sémantique du langage de spécification EVA  
**Rapport No. / Version** : 3/2

**TRUSTED LOGIC S.A.**  
5 rue du Bailliage  
78000 Versailles, France  
[www.trusted-logic.fr](http://www.trusted-logic.fr)

**Laboratoire Spécification Vérification**  
CNRS UMR 8643, ENS Cachan  
61, avenue du président-Wilson  
94235 Cachan Cedex, France  
[www.lsv.ens-cachan.fr](http://www.lsv.ens-cachan.fr)

**Laboratoire Verimag**  
CNRS UMR 5104,  
Univ. Joseph Fourier, INPG  
2 av. de Vignate,  
38610 Gières, France  
[www-verimag.imag.fr](http://www-verimag.imag.fr)



## Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>Format d'échange</b>	<b>1</b>
<b>3</b>	<b>Syntaxe concrète</b>	<b>3</b>
3.1	Lexèmes . . . . .	3
3.2	La grammaire concrète . . . . .	4
3.3	Les arbres de syntaxe concrète . . . . .	6
3.4	Analyse syntaxique . . . . .	7
<b>4</b>	<b>Syntaxe abstraite</b>	<b>12</b>
4.1	Grammaire . . . . .	12
4.2	Traduction de LAEVA en PEVA . . . . .	14
4.2.1	Traduction des termes . . . . .	14
4.2.2	Déclarations . . . . .	16
4.2.3	Composition de messages . . . . .	17
4.2.4	Décomposition de message . . . . .	18
4.2.5	Compilation des patterns . . . . .	19
4.2.6	Compilation des messages . . . . .	20
4.2.7	Déclarations de sessions . . . . .	22
4.2.8	Formules . . . . .	22
4.2.9	Spécifications . . . . .	24
<b>5</b>	<b>Sémantique</b>	<b>25</b>
5.1	Valeurs . . . . .	25
5.2	Formalisation de l'intrus . . . . .	25
5.3	Actions . . . . .	27
5.4	Processus . . . . .	28
5.5	Formules . . . . .	29
5.6	Validité . . . . .	31

## 1 Introduction

Ce document rapide a pour but de définir les syntaxes concrètes et abstraites, ainsi que la sémantique, du langage du projet EVA. Il fait suite à un document [JLM01] sur la syntaxe concrète et un autre [GL01] sur la syntaxe abstraite et sa sémantique.

## 2 Format d'échange

Les différents outils du projet s'échangent les informations par des fichiers textuels, dont le contenu sont des termes du premier ordre écrits dans une syntaxe lispienne. C'est le cas notamment des fichiers en `.evl` contenant les arbres syntaxiques produits par l'analyseur syntaxique `evaparse` et pris en entrée par le traducteur `evatrans`. (L'analyse syntaxique est décrite en section 3.) C'est aussi le cas des fichiers d'extension `.cpl` contenant la syntaxe abstraite EVA, sur laquelle est définie la sémantique, des protocoles traduits par l'outil `evatrans`. (Cette syntaxe abstraite est définie en section 4, la sémantique étant le sujet de la section 5.) L'architecture actuelle des outils EVA est donnée en figure 1.

Les termes du premier ordre sont soit des variables, soit des constantes entières, soit des applications.

On notera dans la suite les termes du premier ordre comme suit. Une variable, par exemple de nom "abc", sera notée `'abc'`. Un entier, par exemple 12, sera noté en décimal. Une application d'un symbole  $f$  à une liste d'arguments  $t_1, \dots, t_n$ , sera notée  $f(t_1, \dots, t_n)$ . En particulier, une constante (le cas  $n = 0$ ) sera notée  $f()$ . Les symboles de fonctions sont des suites non vides de caractères quelconques, sauf "n",

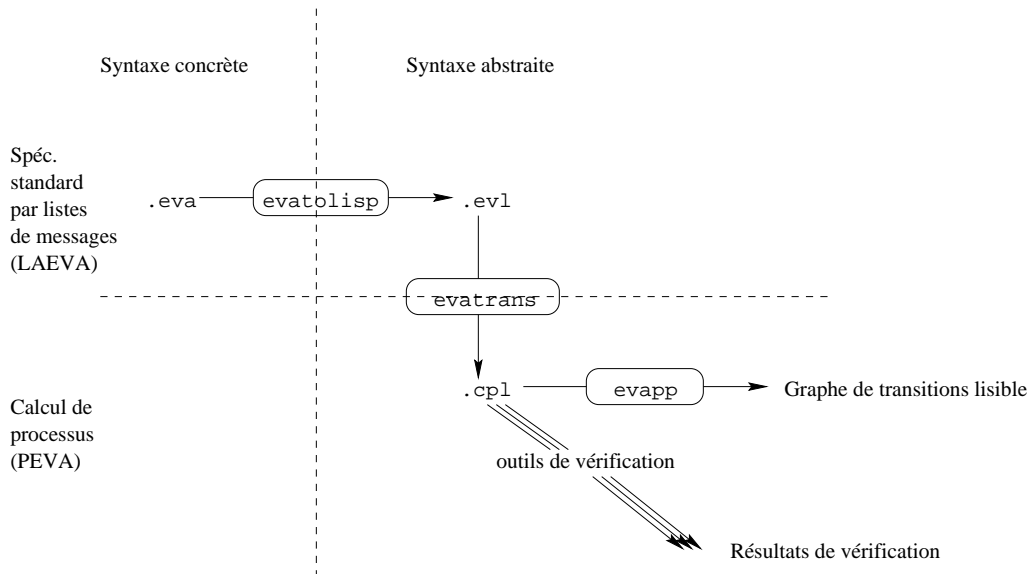


Figure 1: L'architecture EVA

l'espace, la tabulation, le retour chariot, le saut de ligne, et les parenthèses ouvrantes et fermantes. De plus, le symbole spécial 'line' est réservé.

Un terme Lisp est soit une variable, représentée par la chaîne des caractères de son nom entre guillemets (les caractères spéciaux et les guillemets étant notées avec la notation C classique utilisant le backslash \), soit une constante entière, notée en décimal, soit une application d'un symbole  $f$  à  $n$  termes Lisp  $t_1, \dots, t_n$ , notée  $(f t_1 \dots t_n)$ , soit une information de position textuelle (`line t l1 n1 l2 n2 N`), où  $t$  est un terme Lisp,  $l_1, n_1, l_2, n_2$  sont des constantes entières, et  $N$  est une chaîne de caractères. Cette dernière notation indique que le terme  $t$  correspond à une information issue du fichier de nom  $N$  (pour peu que  $N$  ne soit pas la chaîne vide, auquel cas les autres paramètres entiers sont sans signification), comprise entre les positions décrites par la ligne  $l_1$  et la colonne  $n_1$  d'une part, et la ligne  $l_2$  et la colonne  $n_2$  d'autre part. Les lignes sont numérotées à partir de 1, les colonnes à partir de 0.

La relation entre termes Lisp et termes du premier d'ordre est donnée par une fonction d'effacement  $E$  qui efface les appels à `line`:

$$\begin{aligned}
 E(x) &= x && \text{(identificateurs)} \\
 E(n) &= n && \text{(constantes entières)} \\
 E((f t_1 \dots t_n)) &= f(E(t_1), \dots, E(t_n)) \\
 E(\text{line } t \ l_1 \ n_1 \ l_2 \ n_2 \ N) &= E(t)
 \end{aligned}$$

La bibliothèque `lisp.cmxa` est une bibliothèque OCaml permettant de lire et d'écrire des termes Lispiens. Le type des termes lispiens est défini dans `lisp.mli` comme suit:

```

type term = VAR of string
          | INT of int
          | APP of string * term list
          | LINE of term * int * int * int * int * string;;
    
```

La fonction de lecture `lispread` est décrite dans `lispread.mli` comme suit:

```

exception LispNoFunction
exception LispUnexpectedFunction of string
exception LispRParen
    
```

```
val lispread : in_channel -> Term.term
```

Les exceptions mentionnées sont lancées en cas d'erreur de formatage du fichier lu: `LispNoFunction` lorsqu'une parenthèse ouvrante n'est pas suivie d'un symbole de fonction, `LispUnexpectedFunction` lorsqu'un symbole de fonction (passé en paramètre) a été découvert non précédé d'une parenthèse ouvrante, `LispRParen` lorsqu'une parenthèse fermante superflue a été rencontrée. Finalement, la fonction

```
lispwrite : in_channel -> Term.term -> unit
```

est fournie qui écrit un terme lispien dans un fichier.

De même, la bibliothèque `lispin.ml` est une bibliothèque `HimML` remplissant le même but. Le type des termes lispieus est défini dans `term_h.ml` comme suit:

```
type lineinfo = [| first_line : int,  
                  first_column : int,  
                  last_line : int,  
                  last_column : int,  
                  in_file : string  
                |];
```

```
datatype term = VAR of string  
              | INT of int  
              | APP of string * term list  
              | LINE of term * lineinfo;
```

Le fichier `lispin_h.ml` définit ensuite les fonctions `lispread` et `lispwrite`, éponymes des fonctions ci-dessus, par:

```
type 'a inlstream = [| get : int -> string,  
                      getline : unit -> string,  
                      ... : 'a ]|;
```

```
extern val lispread : 'a inlstream -> term;  
extern val lispwrite : 'a outstream -> term -> unit;
```

Noter qu'on aurait pu aussi choisir un format XML ici. L'inter-traduction ne semble pas devoir demander beaucoup d'efforts.

### 3 Syntaxe concrète

Il s'agit de la syntaxe comprise par l'outil `evatolisp`, qui est un shell-script construit au-dessus du programme `C evatrans`. Cet outil a pour but d'effectuer l'analyse syntaxique de fichiers EVA, en langage LAEVA et d'extension standard `.eva`, et de ressortir un arbre syntaxique, dans une syntaxe lispienne. Ce shell-script appelle le préprocesseur `C /lib/cpp/` dans le but de fournir l'inclusion de fichiers (par `#include`) et les macros (par `#define`).

#### 3.1 Lexèmes

**id** Un *identificateur* est une suite non vide de caractères alpha-numériques (de A à Z, de a à z, de 0 à 9, ou `_`), dont le premier est une lettre (entre A et Z ou entre a et z). Les identificateurs dénotent typiquement les variables, les noms de principaux.

**int** Un *entier littéral* est une suite non vide de chiffres entre 0 et 9.

**label** Une *étiquette* est un identificateur ou un entier suivi immédiatement d'un point, sans aucun autre caractère entre les deux. Les étiquettes servent à dénoter les étapes dans un protocole.

string Une *chaîne littérale* est une suite de caractères entre guillemets ". Le backslash \ est un caractère spécial, et sert à former des suites de caractères difficiles à écrire autrement: \n est un saut de ligne (ASCII 10), \t une tabulation (ASCII 9), \r un retour chariot (ASCII 13), \b un son de cloche (ASCII 7), \f un saut de page (ASCII 12). De plus, un backslash suivi de 1 à 3 chiffres octals dénote le code ASCII correspondant en octal; par exemple, \012 est synonyme de \n. À part cela, un backslash suivi d'un caractère représente ce caractère, de sorte que \" dénote le caractère guillemet.

Les commentaires, dans le style de ceux de C++ ou de Java, sont introduits par les symboles // (commentaire se poursuivant jusqu'en bout de ligne) ou /\* (commentaire se poursuivant jusqu'au prochain \*/, sans imbrication). Ceci est géré par le préprocesseur C /lib/cpp, qui est appelé par evatolisp.

Les mots-clés réservés sont:

```
alias  assume  axiom  case  claim
hash  keypair  knows  secret  session  switch
->    =>      ==     :=     &&     ||
*E    *A      *U     *W     *S     *B
*F    *G      *P     *Q     *N
:     (       )     ,     =     ~
{     }       [     ]     %
*     !       @     false  true
```

plus le symbole spécial eof dénotant la fin de fichier.

' , '	associatif à droite
'=>'	associatif à droite
'  ' '*U' '*W' '*S' '*B'	associatif à droite
'&&'	associatif à droite
'!' '*E' '*A' '*F' '*G' '*P' '*Q' '*N'	non associatifs

Figure 2: Priorités

Les priorités sont données en figure 2, qui liste les opérateurs de plus forte priorité — ceux qui lient plus fort — en bas.

### 3.2 La grammaire concrète

La syntaxe concrète des fichiers de spécification EVA est donnée par la grammaire qui suit. On utilise la notation  $[X]$  pour signifier toute chaîne reconnue par  $X$  ou la chaîne vide,  $X^*$  pour dénoter toute concaténation, possiblement vide, de chaînes reconnues par  $X$ , et  $X^+$  pour toute concaténation non vide. La notation 'abc' dénote le littéral correspondant (ici, abc). Les espaces, tabulations, sauts de lignes et de pages, retours chariots sont ignorés.

spec ::= id declaration* block session* assumptions claims eof		spécification EVA
declaration ::= typing-declaration   'keypair' [encryption-algorithm] id ' , ' id ['(' type-list ')']   'alias' id '=' term   ids ':' alias' id '=' term   id 'knows' tuple   'axiom' term '=' term [quantification]		déclaration de types déclaration de paires de clés asymétriques déclaration d'alias global déclaration d'alias locaux connaissances initiales axiome global
typing-declaration ::= ids ':' type   id '(' type-list ')' : type ['hash']		types d'identificateurs types de fonctions
quantification ::= '[' typing-declarations ']'		quantification universelle
typing-declarations ::= typing-declaration ( , ' typing-declaration)*		

ids	::=	id (',' id)*	liste d'identificateurs (non vide)
type	::=	id	type non fonctionnel
type-list	::=	[non-empty-type-list]	liste de types
non-empty-type-list	::=	type (',' type)*	liste de types non vide

block	::=	{' message* '}	bloc: protocole ou sous-protocole
message	::=	label id '->' id ':' term	envoi/réception de message
		id ':' id equals-or-assign-op	
		atomic-term-or-ciphertext	test d'égalité/affectation
		block	sous-protocole
		'switch' term '{' case* '}'	conditionnelle
equals-or-assign-op	::=	'=='   ':='	
case	::=	'case' term ':' message*	branche de conditionnelle

term	::=	tuple	terme
tuple	::=	atomic-term-or-ciphertext	
		(',' atomic-term-or-ciphertext)*	<i>n</i> -uplet
term-list	::=	(' [tuple] ')	liste parenthésée de termes
atomic-term-or-ciphertext	::=	atomic-term	terme atomique
		{' term '}_ atomic-term	
		[encryption-algorithm]	chiffrement
		[' term ']._ atomic-term	
		[encryption-algorithm]	signature
		atomic-term '%' atomic-term	schizo-notation de Lowe
		atomic-term-or-ciphertext '@' label id	terme placé
atomic-term	::=	id term-list	appel de fonction
		id	identificateur
		(' term ')	
		(' )'	<i>n</i> -uplet vide
encryption-algorithm	::=	'^' atomic-term	invocation d'algorithme

session	::=	[label] 'session' ['*{' ids '}]	instantiation de session
		[principals] assignments	
principals	::=	[' ['^'] ids ']	liste de principaux inclus/exclus
assignments	::=	assignment (',' assignment)*	substitution
assignment	::=	id '=' atomic-term-or-ciphertext	liaison de valeur

assumptions	::=	'assume' properties	hypothèses
claims	::=	'claim' properties	propriétés à prouver
properties	::=	property (' , ' property)*	liste de propriétés
property	::=	id term-list	proposition atomique
		label id '@' label	point de programme
		label id '(' term ')'	origine de message
		'secret (' term ')'	secret de message
		'true'	vrai
		'false'	faux
		property '&&' property	conjonction
		property ' ' property	disjonction
		property '=>' property	implication
		'!' property	négation
		(' property ')	
		'*E' property	sur un chemin
		'*A' property	sur tous les chemins
		'*F' property	à un instant futur
		'*G' property	à tous les instants futurs
		'*P' property	à un instant passé
		'*Q' property	à tous les instants passés
		'*N' property	dorénavant
		property '*U' property	until
		property '*W' property	waiting-for (until faible)
		property '*S' property	since
		property '*B' property	before (since faible)

### 3.3 Les arbres de syntaxe concrète

Les spécifications concrètes EVA (.eva) obéissant à cette syntaxe sont traduites par `evatolisp` en un terme du premier ordre (écrit en syntaxe lispienne dans un fichier d'extension .evl).

Spec ::= spec (Declarations, Block, Sessions, Assumptions, Claims)

Declarations ::= declare (Declaration\*)  
 Declaration ::= Typing-declaration  
 | keypair (Encryption-algorithm, id, id, Type)  
 | alias (id, Term)  
 | local-alias (id, Term, id\*)  
 | knows (id, Term)  
 | axiom (Term, Term, Typing-declaration\*)  
 Typing-declaration ::= type (id, Type)  
 Type ::= id  
 | function (id, id\*)  
 | one-way-function (id, id\*)

```

Block ::= block (Message*)
Message ::= comm (label, id, id, Term)
          | equals (id, id, Term)
          | assign (id, id, Term)
          | Block
          | switch (Term, Case*)
Case ::= case (Term, Message*)
Term ::= id
       | tuple (Term*)
       | crypt (Term, Term, Encryption-algorithm)
       | sign (Term, Term, Encryption-algorithm)
       | percent (Term, Term)
       | locate (label, id, Term)
       | apply (id, Term*)
Encryption-algorithm ::= vanilla ()
                       | Term
Sessions ::= sessions (Session*)
Session ::= session (label, Principals, Assignment*)
          | session-repeat (Private, label, Principals, Assignment*)
Private ::= private (id*)
Principals ::= principals-only (id*)
            | principals-except (id*)
Assignment ::= bind (id, Term)
Assumptions ::= assume (Property*)
Claims ::= claim (Property*)
Property ::= prop (id, Term*)
           | at (label, id, label)
           | owns (label, id, Term)
           | secret (Term)
           | and (Property*)
           | or (Property*)
           | implies (Property, Property)
           | not (Property)
           | E (Property)
           | A (Property)
           | F (Property)
           | G (Property)
           | P (Property)
           | Q (Property)
           | N (Property)
           | U (Property, Property)
           | W (Property, Property)
           | S (Property, Property)
           | B (Property, Property)
    
```

### 3.4 Analyse syntaxique

La correspondance entre syntaxe concrète et arbres de syntaxe concrète est décrite par la série de règles de grammaires suivante, écrite dans le style de *yacc*. Cette série de règles reprend et enrichit la grammaire de la section 3.2. La notation  $\epsilon$  dénote la suite vide; la virgule (par exemple dans  $\$1$ ,  $\$3$ ) dénote la concaténation de suites, sachant que tout terme est implicitement converti en une liste; si un terminal ou un non-terminal apparaît en position  $n$  en partie droite de règle, sa valeur est  $\$n$ ; s'il dénote une liste (par exemple s'il apparaît sous une astérisque), alors  $\$n^*$  dénote la suite de toutes les valeurs obtenus par le terminal ou le non-terminal dans la liste. La notation  $(\dots)_{x \in \$n^*}$  dénote la suite des  $\dots$  lorsque  $x$  parcourt

(dans l'ordre) les éléments de la suite  $\$n^*$ .

Les règles d'analyse syntaxique sont alors donnés sous la forme illustrée par la règle principale pour spec ci-dessous; chaque côté droit d'une règle de grammaire est associé à un calcul de \$\$, la valeur du côté gauche, sous forme d'un terme construit à partir des valeurs \$1, \$2, ..., des terminaux et non-terminaux du côté droit.

$$\begin{array}{l}
 \text{spec} ::= \text{id declaration}^* \text{ block session}^* \\
 \qquad \qquad \text{assumptions claims eof} \\
 \hline
 \text{\$\$} = \text{spec} (\text{declare} (\text{\$2}^*), \text{\$3}, \text{sessions} (\text{\$4}^*), \text{\$5}, \text{\$6}) \\
 \\
 \text{declaration} ::= \frac{\text{typing-declaration}}{\text{\$\$} = \text{\$1}} \\
 \qquad \qquad \qquad | \frac{\text{'keypair' opt-encryption-algorithm} \\
 \qquad \qquad \qquad \text{id ',' id opt-keypair-arg-type}}{\text{\$\$} = \text{keypair} (\text{\$2}, \text{\$3}, \text{\$5}, \text{\$6})} \\
 \qquad \qquad \qquad | \frac{\text{'alias' id '=' term}}{\text{\$\$} = \text{alias} (\text{\$2}, \text{\$4})} \\
 \qquad \qquad \qquad | \frac{\text{ids ':' alias' id '=' term}}{\text{\$\$} = \text{local-alias} (\text{\$3}, \text{\$5}, \text{\$1}^*)} \\
 \qquad \qquad \qquad | \frac{\text{id 'knows' tuple}}{\text{\$\$} = (\text{knows} (\text{\$1}, x))_{x \in \text{\$3}^*}} \\
 \qquad \qquad \qquad | \frac{\text{'axiom' term '=' term opt-quantification}}{\text{\$\$} = \text{axiom} (\text{\$2}, \text{\$4}, \text{\$5}^*)} \\
 \\
 \text{typing-declaration} ::= \frac{\text{ids ':' type}}{\text{\$\$} = (\text{type} (x, \text{\$3}))_{x \in \text{\$1}^*}} \\
 \qquad \qquad \qquad | \frac{\text{id '(' type-list ')' : type}}{\text{\$\$} = \text{type} (\text{\$1}, \text{function} (\text{\$5}, \text{\$3}^*))} \\
 \qquad \qquad \qquad | \frac{\text{id '(' type-list ')' : type 'hash'}}{\text{\$\$} = \text{type} (\text{\$1}, \text{one-way-function} (\text{\$5}, \text{\$3}^*))} \\
 \\
 \text{opt-quantification} ::= \frac{}{\text{\$\$} = \epsilon} \\
 \qquad \qquad \qquad | \frac{\text{quantification}}{\text{\$\$} = \text{\$1}} \\
 \\
 \text{quantification} ::= \frac{\text{'[' typing-declarations ']'}}{\text{\$\$} = \text{\$2}} \\
 \\
 \text{typing-declarations} ::= \frac{\text{typing-declaration (',' typing-declaration)^*}}{\text{\$\$} = \text{\$1}, \text{\$3}^*} \\
 \\
 \text{ids} ::= \frac{\text{id (',' id)^*}}{\text{\$\$} = \text{\$1}, \text{\$3}^*} \\
 \\
 \text{type} ::= \frac{\text{id}}{\text{\$\$} = \text{\$1}} \\
 \\
 \text{type-list} ::= \frac{}{\text{\$\$} = \epsilon} \\
 \qquad \qquad \qquad | \frac{\text{non-empty-type-list}}{\text{\$\$} = \text{\$1}} \\
 \\
 \text{non-empty-type-list} ::= \frac{\text{type (',' type)^*}}{\text{\$\$} = \text{\$1}, \text{\$3}^*} \\
 \\
 \text{opt-keypair-arg-type} ::= \frac{}{\text{\$\$} = \text{'number'}} \\
 \qquad \qquad \qquad | \frac{\text{'(' type-list ')'}}{\text{\$\$} = \text{one-way-function} (\text{'number'}, \text{\$2}^*)}
 \end{array}$$

block	::=	$\{\text{' message* '}\}$
		$$$ = \text{block} (\$2^*)$
message	::=	label id $\text{'->'}$ id $\text{':'}$ term
		$$$ = \text{comm} (\$1, \$2, \$4, \$6)$
		id $\text{':'}$ id $\text{'='}$ atomic-term-or-ciphertext
		$$$ = \text{equals} (\$1, \$3, \$5)$
		id $\text{':'}$ id $\text{':=}'$ atomic-term-or-ciphertext
		$$$ = \text{assign} (\$1, \$3, \$5)$
		block
		$$$ = \$1$
		$\text{'switch'}$ term $\{\text{' case* '}\}$
		$$$ = \text{switch} (\$2, \$4^*)$
case	::=	$\text{'case'}$ term $\text{':'}$ message*
		$$$ = \text{case} (\$2, \$4^*)$

		term ::= atomic-term-or-ciphertext
		$$$ = \$1$
		atomic-term-or-ciphertext $\text{' ,'}$ tuple
		$$$ = \text{tuple} (\$1, \$3^*)$
		tuple ::= atomic-term-or-ciphertext ( $\text{' ,'}$ atomic-term-or-ciphertext)*
		$$$ = \$1, \$3^*$
		term-list ::= $\text{'('}$
		$$$ = \epsilon$
		$\text{'('}$ tuple $\text{'}'}$
		$$$ = \$2$
atomic-term-or-ciphertext	::=	atomic-term
		$$$ = \$1$
		$\{\text{' term '}\}_-$ atomic-term opt-encryption-algorithm
		$$$ = \text{crypt} (\$2, \$4, \$5)$
		$[\text{' term '}]_-$ atomic-term opt-encryption-algorithm
		$$$ = \text{sign} (\$2, \$4, \$5)$
		atomic-term $\text{'\%'}$ atomic-term
		$$$ = \text{percent} (\$1, \$3)$
		atomic-term-or-ciphertext $\text{'@'}$ label id
		$$$ = \text{locate} (\$3, \$4, \$1)$
atomic-term	::=	id term-list
		$$$ = \text{apply} (\$1, \$2^*)$
		id
		$$$ = \$1$
		$\text{'('}$ term $\text{'}'}$
		$$$ = \$2$
		$\text{'('}$
		$$$ = \text{tuple} ()$
encryption-algorithm	::=	$\text{'^'}$ atomic-term
		$$$ = \$2$
opt-encryption-algorithm	::=	$$$ = \text{vanilla} ()$
		encryption-algorithm
		$$$ = \$1$

session	::=	<u>opt-label 'session' opt-principals assignments</u>
		\$\$ = session (\$1, \$3, \$4*)
		<u>opt-label 'session*' {' ids '}' opt-principals assignments</u>
		\$\$ = session-repeat (private (\$3*), \$1, \$5, \$6*)
opt-label	::=	<u>\$\$ = some fresh label (intentionally left unspecified).</u>
		<u>label</u>
		\$\$ = \$1
opt-principals	::=	<u>\$\$ = principals-except ()</u>
		<u>principals</u>
		\$\$ = \$1
principals	::=	<u>'[ ' ids ' ]'</u>
		\$\$ = principals-only (\$2*)
		<u>'[ ^' ids ' ]'</u>
		\$\$ = principals-except (\$2*)
assignments	::=	<u>assignment ( ' , ' assignment )*</u>
		\$\$ = \$1, \$3*
assignment	::=	<u>id '=' atomic-term-or-ciphertext</u>
		\$\$ = bind (\$1, \$3)

assumptions	::=	<u>'assume' properties</u>
		$$$ = \text{assume} (\$2^*)$
claims	::=	<u>'claim' properties</u>
		$$$ = \text{claim} (\$2^*)$
properties	::=	<u>property (' , ' property)*</u>
		$$$ = \$1, \$3^*$
property	::=	<u>id term-list</u>
		$$$ = \text{prop} (\$1, \$2^*)$
		<u>label id '@' label</u>
		$$$ = \text{at} (\$1, \$2, \$4)$
		<u>label id '(' term ')'</u>
		$$$ = \text{owns} (\$1, \$2, \$4)$
		<u>'secret (' term ')'</u>
		$$$ = \text{secret} (\$2)$
		<u>'true'</u>
		$$$ = \text{and} ()$
		<u>'false'</u>
		$$$ = \text{or} ()$
		<u>property '&amp;&amp;' property</u>
		$$$ = \text{and} (\$1, \$3)$
		<u>property ' '  property</u>
		$$$ = \text{or} (\$1, \$3)$
		<u>property '=&gt;' property</u>
		$$$ = \text{implies} (\$1, \$3)$
		<u>'!' property</u>
		$$$ = \text{not} (\$2)$
		<u>(' property ')'</u>
		$$$ = \$2$
		<u>'*E' property</u>
		$$$ = \text{E} (\$2)$
		<u>'*A' property</u>
		$$$ = \text{A} (\$2)$
		<u>'*F' property</u>
		$$$ = \text{F} (\$2)$
		<u>'*G' property</u>
		$$$ = \text{G} (\$2)$
		<u>'*P' property</u>
		$$$ = \text{P} (\$2)$
		<u>'*Q' property</u>
		$$$ = \text{Q} (\$2)$
		<u>'*N' property</u>
		$$$ = \text{N} (\$2)$
		<u>property '*U' property</u>
		$$$ = \text{U} (\$1, \$3)$
		<u>property '*W' property</u>
		$$$ = \text{W} (\$1, \$3)$
		<u>property '*S' property</u>
		$$$ = \text{S} (\$1, \$3)$
		<u>property '*B' property</u>
		$$$ = \text{B} (\$1, \$3)$

## 4 Syntaxe abstraite

La syntaxe abstraite d'un protocole EVA est produite à partir d'un fichier de spécification concrète (en `.evl`) par le traducteur `evatrans`. Ce dernier fournit une traduction qui est encore une fois un terme, dans un langage qui sera appelée PEVA.

### 4.1 Grammaire

La grammaire de PEVA est donnée par l'ensemble des termes de type `Spec`, décrits comme suit.

Une spécification PEVA, d'abord, est la donnée de déclarations d'identificateurs (Types), d'alias globaux (Values), d'axiomes (Axioms), d'hypothèses (Assumptions), de formules à prouver (Claims), et d'un programme (System). Ce dernier est une composition parallèle de processus, décrits plus bas.

<code>Spec</code>	<code>::= compiled-spec (Types, Values, Axioms, System, Assumptions, Claims)</code>	protocole EVA, syntaxe abstraite
<code>Types</code>	<code>::= types (Type-declaration*)</code>	déclarations d'identificateurs
Type-declaration	<code>::= type (id, Type)</code>	déclaration d'identificateur
<code>Values</code>	<code>::= values (Alias*)</code>	déclarations d'alias
<code>Alias</code>	<code>::= alias (id, Term)</code>	déclaration d'alias
<code>Axioms</code>	<code>::= axioms (Axiom*)</code>	listes d'axiomes
<code>Axiom</code>	<code>::= axiom (Term, Term, Type, Type-declaration*)</code>	axiome (lhs, rhs, type, variables quantifiées)
<code>System</code>	<code>::= system (Process*)</code>	Le système (composition parallèle de processus)
<code>Assumptions</code>	<code>::= assume (Formula*)</code>	Hypothèses
<code>Claims</code>	<code>::= claim (Formula*)</code>	Formules à prouver
<code>Type</code>	<code>::= id</code>	type d'ordre 1
	<code>  function (id, id*)</code>	type de fonction
	<code>  one-way-function (id, id*)</code>	type de fonction one-way

Un processus PEVA peut être soit un processus simple, décrit par un graphe de transitions, soit un processus en multi-session parallèle, qui est un nombre non borné de processus simples décrits par le même graphe de transitions (les *copies*), mis en parallèle. Les transitions sont données comme une liste de triplets (source, cible, action). Les actions sont décrites plus bas. Dans le cas de processus en multi-session parallèle, `Privates` contient la liste des identificateurs qui contiennent des valeurs possiblement différentes d'une copie à l'autre; les autres identificateurs sont partagés entre les copies. Finalement, chaque processus vient avec une liste de connaissances (`Know`), qui sert à faire le lien entre expressions LAEVA et identificateurs correspondants à ces expressions dans les processus PEVA.

<code>Process</code>	<code>::= process (id, state, Know, Transition*)</code>	processus simple (nom, label de départ, connaissances, transitions)
	<code>  repeat-process (Privates, id, state, Know, Transition*)</code>	processus en multi-session parallèle (vars privées, nom, départ, connaissances, transitions)
<code>Transition</code>	<code>::= trans (state, state, Action)</code>	transition (source, cible, action)
<code>state</code>	<code>::= label</code>	état visible
	<code>  '%label</code>	état interne
<code>Know</code>	<code>::= knows (As*)</code>	connaissances
<code>As</code>	<code>::= as (Term, Term)</code>	terme connu sous la forme: terme
<code>Privates</code>	<code>::= private (id*)</code>	liste de variables privées
<code>Action</code>	<code>::= new (Pattern)</code>	création de nonce
	<code>  let (Pattern, Term)</code>	pattern-matching
	<code>  recv (Pattern)</code>	réception de message
	<code>  send (Term)</code>	émission de message
	<code>  skip ()</code>	action nulle

Term ::=	id	variable
	crypt (Term, Term, Term)	chiffrement (algo, texte, clé)
	tuple (Term*)	<i>n</i> -uplet
	d (Term)	conversion *D* → number
	p (Term)	conversion principal → number
	a (Term)	conversion *algo* → number
	sa (Term)	conversion sym_algo → *algo*
	aa (Term)	conversion asym_algo → *algo*
	vanilla ()	algorithme symétrique par défaut
	apply (id, Term*)	application de fonction définie
	hash-apply (id, Term*)	application de fonction one-way
	apply-pubk (Term, id, Term*)	appl. de constructeur de clé publique
	hash-apply-pubk (Term, id, Term*)	(algo, constructeur, arguments)
	apply-privk (Term, id, Term*)	appl. de constructeur de clé publique one-way
	hash-apply-privk (Term, id, Term*)	(algo, constructeur, arguments)
	lambda-pubk (Term, id)	appl. de constructeur de clé privée
	lambda-privk (Term, id)	(algo, constructeur, arguments)
		appl. de constructeur de clé privée one-way
		(algo, constructeur, arguments)
		partie publique de clé (algo, clé)
		partie privée de clé (algo, clé)

Pattern ::=	id	variable
	exact (Term)	constante littérale
	crypt (Term, Pattern, Term)	déchiffrement (algo, texte, clé)
	apply (id, Pattern*)	application de constructeur
	tuple (Pattern*)	<i>n</i> -uplet
	d (Pattern)	extraction number → *D*
	p (Pattern)	extraction number → principal
	a (Pattern)	extraction number → *algo*
	sa (Pattern)	extraction *algo* → sym_algo
	aa (Pattern)	extraction *algo* → asym_algo
	vanilla ()	algorithme symétrique par défaut
	apply-pubk (Term, id, Pattern*)	appl. de constructeur de clé publique
	apply-privk (Term, id, Pattern*)	(algo, constructeur, arguments)
		appl. de constructeur de clé privée
		(algo, constructeur, arguments)

Form ::=	prop (id, Term*)	formule atomique
	at (label, id, label)	point de programme
	owns (label, id, Term)	origine de messages
	secret (Term)	secret de messages
	not (Form)	négation
	and (Form*)	conjonction
	or (Form*)	disjonction
	implies (Form, Form)	implication
	E (Form)	il existe un chemin
	A (Form)	pour tout chemin
	F (Form)	dans un futur
	G (Form)	dans tout futur
	P (Form)	dans un passé
	Q (Form)	dans tout passé
	N (Form)	dorénavant
	U (Form, Form)	until
	W (Form, Form)	until faible
	S (Form, Form)	since
	B (Form, Form)	since faible

## 4.2 Traduction de LAEVA en PEVA

### 4.2.1 Traduction des termes

On définit d'abord un jugement  $\rho, \sigma, \ell \vdash t \Rightarrow_{\text{term}} u : \tau$ , où  $t, u \in \text{Term}$ ,  $\tau \in \text{Type}$ ,  $\rho : \text{id} \rightarrow \text{Type}$  est un environnement de types,  $\sigma : \text{id} \rightarrow \text{Term}$  est une substitution,  $\ell : [\text{label} \times \text{id} \rightarrow \text{Term} \rightarrow \text{Term}]$ . On note  $[A]$  le type des éléments de  $A$ , en union disjointe avec un élément spécial  $- \notin A$ ; il s'agit du type " $A$  optionnel". La notation  $A \rightarrow B$  désigne l'espace des fonctions (partielles) de  $A$  vers  $B$ . Le domaine de  $f : A \rightarrow B$  est noté  $\text{dom } f$ . La fonction vide est notée  $\{\}$ , et  $f + g$  dénote la fonction qui à  $x \in \text{dom } g$  associe  $g(x)$ , et à  $x \in \text{dom } f \setminus \text{dom } g$  associe  $f(x)$ .

L'environnement  $\rho$  est décrit par les déclarations de type, et  $\sigma$  par les déclarations d'alias'. La composante  $\ell$  est liée aux déclarations 'knows', et sera commentée plus loin.

Le jugement  $\rho, \sigma, \ell \vdash t \Rightarrow_{\text{term}} u : \tau$  décrit sous quelles conditions le terme  $t$  de la syntaxe concrète se traduit en le terme  $u$  de la syntaxe abstraite, de type  $\tau$ .

$$\frac{x \in \text{dom } \rho \quad x \in \text{dom } \sigma}{\rho, \sigma, - \vdash x \Rightarrow_{\text{term}} \sigma(x) : \rho(x)} \quad (1)$$

$$\frac{x \in \text{dom } \rho \quad x \notin \text{dom } \sigma}{\rho, \sigma, - \vdash x \Rightarrow_{\text{term}} x : \rho(x)} \quad (2)$$

Noter que les variables ne sont valides que lorsque  $\ell = -$ . Si  $\ell \neq -$ , on exige que toutes les variables soient dans la portée d'un locate (règle (15)).

$$\frac{\rho, \sigma, \ell \vdash t \Rightarrow_{\text{term}} t' : \text{number} \quad \rho, \sigma, \ell \vdash k \Rightarrow_{\text{term}} k' : \text{number} \quad \rho, \sigma, \ell \vdash a \Rightarrow_{\text{term}} a' : \text{number}}{\rho, \sigma, \ell \vdash \text{crypt}(t, k, a) \Rightarrow_{\text{term}} \text{crypt}(a', t', k') : \text{number}} \quad (3)$$

Noter que l'ordre des arguments est différent en LAEVA et PEVA. En PEVA, l'algorithme  $a'$  vient en premier: pour toutes les fonctions de nature cryptographique, il est convenu que l'algorithme de chiffrement vienne toujours en premier argument en PEVA.

$$\frac{\rho, \sigma, \ell \vdash t \Rightarrow_{\text{term}} t' : \text{number} \quad \rho, \sigma, \ell \vdash k \Rightarrow_{\text{term}} k' : \text{number} \quad \rho, \sigma, \ell \vdash a \Rightarrow_{\text{term}} a' : \text{number}}{\rho, \sigma, \ell \vdash \text{sign}(t, k, a) \Rightarrow_{\text{term}} \text{crypt}(a', t', k') : \text{number}} \quad (4)$$

Noter que toute signature est traduite sous forme d'un chiffrement en PEVA.

$$\frac{\rho, \sigma, \ell \vdash t_1 \Rightarrow_{\text{term}} u_1 : \text{number} \dots \rho, \sigma, \ell \vdash t_n \Rightarrow_{\text{term}} u_n : \text{number}}{\rho, \sigma, \ell \vdash \text{tuple}(t_1, \dots, t_n) \Rightarrow_{\text{term}} \text{tuple}(u_1, \dots, u_n) : \text{number}} \quad (5)$$

$$\frac{}{\rho, \sigma, \ell \vdash \text{vanilla}() \Rightarrow_{\text{term}} \text{vanilla}() : \text{sym\_algo}} \quad (6)$$

Les termes `lambda-pubk(...)` et `lambda-privk(...)` désignent des parties publiques et privées respectivement de clés asymétriques. Elles ont des types *fonctionnels*, c'est-à-dire de la forme `fonction`( $\tau_{res}, \tau_1, \dots, \tau_n$ ) ou `one-way-fonction`( $\tau_{res}, \tau_1, \dots, \tau_n$ ).

$$\frac{\rho, \sigma, \ell \vdash a \Rightarrow_{\text{term}} a' : *algo* \quad \rho, \sigma, \ell \vdash f \Rightarrow_{\text{term}} f' : \tau \quad f' \in \text{id} \quad \tau \text{ type fonctionnel}}{\rho, \sigma, \ell \vdash \text{lambda-pubk}(a, f) \Rightarrow_{\text{term}} \text{lambda-pubk}(a', f') : \tau} \quad (7)$$

$$\frac{\rho, \sigma, \ell \vdash a \Rightarrow_{\text{term}} a' : *algo* \quad \rho, \sigma, \ell \vdash f \Rightarrow_{\text{term}} f' : \tau \quad f' \in \text{id} \quad \tau \text{ type fonctionnel}}{\rho, \sigma, \ell \vdash \text{lambda-privk}(a, f) \Rightarrow_{\text{term}} \text{lambda-privk}(a', f') : \tau} \quad (8)$$

$$\frac{\rho, \sigma, \ell \vdash f \Rightarrow_{\text{term}} f' : \text{fonction}(\tau_{res}, \tau_1, \dots, \tau_n) \quad f' \in \text{id} \quad \rho, \sigma, \ell \vdash t_1 \Rightarrow_{\text{term}} u_1 : \tau_1 \dots \rho, \sigma, \ell \vdash t_n \Rightarrow_{\text{term}} u_n : \tau_n}{\rho, \sigma, \ell \vdash \text{apply}(f, t_1, \dots, t_n) \Rightarrow_{\text{term}} \text{apply}(f', u_1, \dots, u_n) : \tau_{res}} \quad (9)$$

$$\frac{\rho, \sigma, \ell \vdash f \Rightarrow_{\text{term}} f' : \text{one-way-fonction}(\tau_{res}, \tau_1, \dots, \tau_n) \quad f' \in \text{id} \quad \rho, \sigma, \ell \vdash t_1 \Rightarrow_{\text{term}} u_1 : \tau_1 \dots \rho, \sigma, \ell \vdash t_n \Rightarrow_{\text{term}} u_n : \tau_n}{\rho, \sigma, \ell \vdash \text{apply}(f, t_1, \dots, t_n) \Rightarrow_{\text{term}} \text{hash-apply}(f', u_1, \dots, u_n) : \tau_{res}} \quad (10)$$

$$\frac{\rho, \sigma, \ell \vdash f \Rightarrow_{\text{term}} \text{lambda-pubk}(a, f') : \text{fonction}(\tau_{res}, \tau_1, \dots, \tau_n) \quad \rho, \sigma, \ell \vdash t_1 \Rightarrow_{\text{term}} u_1 : \tau_1 \dots \rho, \sigma, \ell \vdash t_n \Rightarrow_{\text{term}} u_n : \tau_n}{\rho, \sigma, \ell \vdash \text{apply}(f, t_1, \dots, t_n) \Rightarrow_{\text{term}} \text{apply-pubk}(a, f', u_1, \dots, u_n) : \tau_{res}} \quad (11)$$

$$\frac{\rho, \sigma, \ell \vdash f \Rightarrow_{\text{term}} \text{lambda-pubk}(a, f') : \text{one-way-fonction}(\tau_{res}, \tau_1, \dots, \tau_n) \quad \rho, \sigma, \ell \vdash t_1 \Rightarrow_{\text{term}} u_1 : \tau_1 \dots \rho, \sigma, \ell \vdash t_n \Rightarrow_{\text{term}} u_n : \tau_n}{\rho, \sigma, \ell \vdash \text{apply}(f, t_1, \dots, t_n) \Rightarrow_{\text{term}} \text{hash-apply-pubk}(a, f', u_1, \dots, u_n) : \tau_{res}} \quad (12)$$

$$\frac{\rho, \sigma, \ell \vdash f \Rightarrow_{\text{term}} \text{lambda-privk}(a, f') : \text{fonction}(\tau_{res}, \tau_1, \dots, \tau_n) \quad \rho, \sigma, \ell \vdash t_1 \Rightarrow_{\text{term}} u_1 : \tau_1 \dots \rho, \sigma, \ell \vdash t_n \Rightarrow_{\text{term}} u_n : \tau_n}{\rho, \sigma, \ell \vdash \text{apply}(f, t_1, \dots, t_n) \Rightarrow_{\text{term}} \text{apply-privk}(a, f', u_1, \dots, u_n) : \tau_{res}} \quad (13)$$

$$\frac{\rho, \sigma, \ell \vdash f \Rightarrow_{\text{term}} \text{lambda-privk}(a, f') : \text{one-way-fonction}(\tau_{res}, \tau_1, \dots, \tau_n) \quad \rho, \sigma, \ell \vdash t_1 \Rightarrow_{\text{term}} u_1 : \tau_1 \dots \rho, \sigma, \ell \vdash t_n \Rightarrow_{\text{term}} u_n : \tau_n}{\rho, \sigma, \ell \vdash \text{apply}(f, t_1, \dots, t_n) \Rightarrow_{\text{term}} \text{hash-apply-privk}(a, f', u_1, \dots, u_n) : \tau_{res}} \quad (14)$$

Les termes de la forme `locate`(*session*, *principal*, *t*) sont traités par le jugement (15). Il utilise un jugement auxiliaire `known`  $\vdash t \Rightarrow_{loc} u$ , qui traduit par quel terme *u* le terme *t* est interprété dans le contexte où les termes *s* de dom *known* doivent être vus comme `known`(*s*), où `known` : Term  $\rightarrow$  Term.

$$\frac{\rho, \sigma, - \vdash t \Rightarrow_{\text{term}} u : \tau \quad \ell \neq - \quad (p, s) \in \text{dom } \ell \quad \ell(p, s) \vdash u \Rightarrow_{loc} v}{\rho, \sigma, \ell \vdash \text{locate}(s, p, t) \Rightarrow_{\text{term}} \text{located}(s, p, v) : \tau} \quad (15)$$

$$\frac{t \in \text{dom } \text{known}}{\text{known} \vdash t \Rightarrow_{loc} \text{known}(t)} \quad (16)$$

$$\frac{f(t_1, \dots, t_n) \notin \text{dom } \text{known} \quad \text{known} \vdash t_1 \Rightarrow_{loc} u_1 \dots \text{known} \vdash t_n \Rightarrow_{loc} u_n}{\text{known} \vdash f(t_1, \dots, t_n) \Rightarrow_{loc} f(u_1, \dots, u_n)} \quad (17)$$

Finalement, on dispose de coercions automatiques:

$$\frac{\rho, \sigma, \ell \vdash t \Rightarrow_{\text{term}} u : *D*}{\rho, \sigma, \ell \vdash t \Rightarrow_{\text{term}} \mathbf{d}(u) : \mathbf{number}} \quad (18)$$

$$\frac{\rho, \sigma, \ell \vdash t \Rightarrow_{\text{term}} u : \mathbf{principal}}{\rho, \sigma, \ell \vdash t \Rightarrow_{\text{term}} \mathbf{p}(u) : \mathbf{number}} \quad (19)$$

$$\frac{\rho, \sigma, \ell \vdash t \Rightarrow_{\text{term}} u : *algo*}{\rho, \sigma, \ell \vdash t \Rightarrow_{\text{term}} \mathbf{a}(u) : \mathbf{number}} \quad (20)$$

$$\frac{\rho, \sigma, \ell \vdash t \Rightarrow_{\text{term}} u : \mathbf{sym\_algo}}{\rho, \sigma, \ell \vdash t \Rightarrow_{\text{term}} \mathbf{sa}(u) : *algo*} \quad (21)$$

$$\frac{\rho, \sigma, \ell \vdash t \Rightarrow_{\text{term}} u : \mathbf{asym\_algo}}{\rho, \sigma, \ell \vdash t \Rightarrow_{\text{term}} \mathbf{aa}(u) : *algo*} \quad (22)$$

On notera qu'il n'existe pas de jugement de la forme  $\rho, \sigma, \ell \vdash \mathbf{percent}(\dots) \Rightarrow_{\text{term}} u : \tau$ : les termes utilisant la notation ‘%’ sont illégaux. Les pourcents sont traités par un autre mécanisme (voir plus loin).

#### 4.2.2 Déclarations

Les déclarations  $d$  s'élaborent en un environnement de types  $\rho : \text{id} \rightarrow \text{Type}$ , une substitution globale  $\sigma : \text{id} \rightarrow \text{Term}$ , des substitutions locales à chaque rôle  $\theta : \text{id} \rightarrow \text{id} \rightarrow \text{Term}$ , des déclarations de connaissances  $\kappa : \text{id} \rightarrow \text{Term} \rightarrow \text{Term}$ , une par rôle, un ensemble  $\alpha \in \mathbb{P}(\text{Term} \times \text{Term} \times \text{Type} \times (\text{id} \rightarrow \text{Type}))$  d'axiomes (un axiome est formé de deux termes  $s$  et  $t$ , d'un type  $\tau$ , et d'un environnement  $x_1 : \tau_1, \dots, x_n : \tau_n$ , et signifie  $\forall x_1 : \tau_1, \dots, x_n : \tau_n. s = t : \tau$ ).

On utilisera les abréviations suivantes pour les composantes  $\theta$  et  $\kappa$ . On note  $\{p_i \mapsto x \mapsto \tau \mid 1 \leq i \leq n\}$  la fonction curriée  $\{p_i \mapsto \{x \mapsto \tau\} \mid 1 \leq i \leq n\}$ . La notation  $+$  est adaptée aux composantes  $\theta$  en définissant  $\theta + \theta'$  comme étant la fonction qui à  $p \in \text{dom } \theta \setminus \text{dom } \theta'$  associe  $\theta(p)$ , à  $p \in \text{dom } \theta' \setminus \text{dom } \theta$  associe  $\theta'(p)$ , et à  $p \in \text{dom } \theta \cap \text{dom } \theta'$  associe  $\theta(p) + \theta'(p)$ .

On note  $S$  le sextuplet  $(\rho, \sigma, \theta, \kappa, \alpha, v)$ , où  $v$  est un ensemble d'id auxiliaire, qui servira à éviter la circularité dans les définitions d'alias. On notera aussi “ $\rho$  of  $S$ ”, “ $\sigma$  of  $S$ ”, etc., la composante correspondante de  $S$ . De façon symétrique à ces projections, les injections “ $\rho$  in  $S$ ”, “ $\sigma$  in  $S$ ”, etc., dénoteront respectivement  $(\rho, \{\}, \{\}, \{\}, \{\}, \emptyset)$ ,  $(\{\}, \sigma, \{\}, \{\}, \{\}, \emptyset)$ , etc. La notation  $+$  est étendue aux sextuplets composante par composante, de sorte que, par exemple,  $S + (\rho \text{ in } S)$ , où (le premier)  $S$  est  $(\rho_1, \sigma_1, \theta_1, \kappa_1, \alpha_1, v_1)$ , est  $(\rho_1 + \rho, \sigma_1, \theta_1, \kappa_1, \alpha_1, v_1)$ . On abrégera ceci le plus souvent en  $S + \rho$ , laissant “in  $S$ ” implicite. Ces conventions sont aussi celles de la sémantique de Standard ML ([MTH90], section 4.3).

On définit un jugement de la forme  $S \vdash d \Rightarrow_{\text{decl}} S'$ , qui définit comment une déclaration  $d$  modifie le contexte  $S$  en le contexte  $S'$ .

$$\frac{x \notin \text{dom}(\sigma \text{ of } S) \quad \rho = \{x \mapsto \tau\}}{S \vdash \mathbf{type}(x, \tau) \Rightarrow_{\text{decl}} S + \rho} \quad (23)$$

Certaines règles, dont la suivante, doivent créer des identificateurs  $z$  frais; informellement, “frais” signifie non présents dans la spécification LAEVA d'entrée, et différents de tous les identificateurs frais créés précédemment<sup>1</sup>. On ne précisera pas plus formellement la notion, ce qui compliquerait inutilement les règles.

$$\frac{\begin{array}{l} x, y \notin \text{dom } \sigma \quad x \neq y \quad \rho \text{ of } S, \sigma \text{ of } S, - \vdash a \Rightarrow_{\text{term}} a' : *algo* \quad z \in \text{id frais} \\ \rho = \{z \mapsto *D*, x \mapsto \mathbf{number}, y \mapsto \mathbf{number}\} \\ \sigma = \{x \mapsto \mathbf{hash\_apply\_pubk}(a', **asymk**, z), \\ y \mapsto \mathbf{hash\_apply\_privk}(a', **asymk**, z)\} \end{array}}{S \vdash \mathbf{keypair}(a, x, y, \mathbf{number}) \Rightarrow_{\text{decl}} S + \rho + \sigma} \quad (24)$$

<sup>1</sup> `evatrans` crée ces identificateurs de la forme ‘ $\_xn$ ’, ou ‘ $\_kn$ ’, ou ‘ $\_kpn$ ’, ou ‘ $\_swn$ ’, ou en concaténant à un identificateur LAEVA un tiret ‘-’ et un entier  $n$ . Formellement, ce ne sont pas des id.

$$\begin{array}{c}
 x, y \notin \text{dom } \sigma \quad x \neq y \quad \rho \text{ of } S, \sigma \text{ of } S, - \vdash a \Rightarrow_{\text{term}} a' : * \text{algo} * \quad z \in \text{id frais} \\
 \tau = \text{one-way-function}(\text{number}, \tau_1, \dots, \tau_n) \\
 \rho = \{z \mapsto \tau, x \mapsto \tau, y \mapsto \tau\} \\
 \sigma = \{x \mapsto \text{lambda-pubk}(a', z), y \mapsto \text{lambda-privk}(a', z)\} \\
 \hline
 S \vdash \text{keypair}(a, x, y, \tau) \Rightarrow_{\text{decl}} S + \rho + \sigma
 \end{array} \tag{25}$$

On note  $\text{fv}(u)$  l'ensemble des variables libres du terme  $u$ . L'ensemble  $v$  of  $S$  collectionne toutes les variables apparaissant libres dans un terme déjà mentionné. On vérifie que  $x$  n'est pas dans  $v$ , ce qui interdit tout alias circulaire.

$$\begin{array}{c}
 x \notin \text{dom}(\sigma \text{ of } S) \cup \bigcup_{r \in \text{dom}(\kappa \text{ of } S)} \text{dom}((\kappa \text{ of } S)(r)) \quad x \notin v \\
 x \in \text{dom}(\rho \text{ of } S) \implies \tau = (\rho \text{ of } S)(x) \\
 \rho \text{ of } S, \sigma \text{ of } S, - \vdash t \Rightarrow_{\text{term}} u : \tau \quad x \notin \text{fv}(u) \\
 \rho = \{x \mapsto \tau\} \quad \sigma = \{x \mapsto u\} \quad v = \text{fv}(u) \\
 \hline
 S \vdash \text{alias}(x, t) \Rightarrow_{\text{decl}} S + \rho + \sigma + v
 \end{array} \tag{26}$$

$$\begin{array}{c}
 x \notin \text{dom}(\sigma \text{ of } S) \cup \bigcup_{r \in \text{dom}(\kappa \text{ of } S)} \text{dom}((\kappa \text{ of } S)(r)) \quad x \notin v \\
 x \in \text{dom}(\rho \text{ of } S) \implies \tau = (\rho \text{ of } S)(x) \\
 \rho \text{ of } S, \sigma \text{ of } S, - \vdash t \Rightarrow_{\text{term}} u : \tau \quad x \notin \text{fv}(u) \\
 (\rho \text{ of } S)(p_1) = \text{principal}, \dots, (\rho \text{ of } S)(p_n) = \text{principal} \\
 \rho = \{x \mapsto \tau\} \quad \theta = \{p_i \mapsto x \mapsto u \mid 1 \leq i \leq n\} \quad v = \text{fv}(u) \\
 \hline
 S \vdash \text{local-alias}(x, t, p_1, \dots, p_n) \Rightarrow_{\text{decl}} S + \rho + \theta + v
 \end{array} \tag{27}$$

$$\begin{array}{c}
 (\rho \text{ of } S)(p) = \text{principal} \quad \rho \text{ of } S, \sigma \text{ of } S, - \vdash t \Rightarrow_{\text{term}} u : \tau \\
 \kappa = \{p \mapsto u \mapsto u\} \quad v = \{p\} \cup \text{fv}(u) \\
 \hline
 S \vdash \text{knows}(p, t) \Rightarrow_{\text{decl}} S + \kappa + v
 \end{array} \tag{28}$$

$$\begin{array}{c}
 \rho \text{ of } S + \{x_1 \mapsto \tau_1, \dots, x_n \mapsto \tau_n\}, \sigma \text{ of } S, - \vdash s \Rightarrow_{\text{term}} u : \tau \\
 \rho \text{ of } S + \{x_1 \mapsto \tau_1, \dots, x_n \mapsto \tau_n\}, \sigma \text{ of } S, - \vdash t \Rightarrow_{\text{term}} v : \tau \\
 \alpha = \{(u, v, \tau, \{x_1 \mapsto \tau_1, \dots, x_n \mapsto \tau_n\})\} \quad v = \text{fv}(u) \cup \text{fv}(v) \\
 \hline
 S \vdash \text{axiom}(s, t, \text{type}(x_1, \tau_1), \dots, \text{type}(x_n, \tau_n)) \Rightarrow_{\text{decl}} S + \alpha + v
 \end{array} \tag{29}$$

### 4.2.3 Composition de messages

Le jugement  $\rho, \text{known} \vdash t \Rightarrow_{\text{comp}} al, t', \text{known}'$ , où  $\rho : \text{id} \rightarrow \text{Type}$ ,  $\text{known}, \text{known}' : \text{Term} \rightarrow \text{Term}$ ,  $t, t' \in \text{Term}$ ,  $al \in \text{Action}^*$ , décrit comment l'on peut fabriquer un message  $t$  dans un environnement de types  $\rho$  et un état de connaissances  $\text{known}$ . Le résultat est un message  $t'$ , une liste d'actions  $al$  (typiquement des créations de nonces par `new`), et un nouvel état de connaissances  $\text{known}'$ .

$$\begin{array}{c}
 t \in \text{dom } \text{known} \\
 \hline
 \rho, \text{known} \vdash t \Rightarrow_{\text{comp}} \epsilon, \text{known}(t), \text{known}
 \end{array} \tag{30}$$

Toute variable non connue est compilée comme la création d'un nonce (si son type est `number`), ou d'une paire de clés (si son type est `*D*`; ce sera le cas pour les  $z$  des règles (24) et (25))

$$\begin{array}{c}
 x \notin \text{dom } \text{known} \quad \rho(x) = \text{number} \quad z \in \text{id frais} \\
 \hline
 \rho, \text{known} \vdash x \Rightarrow_{\text{comp}} \text{new}(z), \text{d}(z), \text{known} + \{x \mapsto \text{d}(z)\}
 \end{array} \tag{31}$$

$$\begin{array}{c}
 x \notin \text{dom } \text{known} \quad \rho(x) = *D* \quad z \in \text{id frais} \\
 \hline
 \rho, \text{known} \vdash x \Rightarrow_{\text{comp}} \text{new}(z), z, \text{known} + \{x \mapsto z\}
 \end{array} \tag{32}$$

$$\begin{array}{c}
 f(t_1, \dots, t_n) \notin \text{dom } \text{known} \\
 \rho, \text{known} \vdash t_1 \Rightarrow_{\text{comp}} al_1, t'_1, \text{known}_1 \quad \dots \quad \rho, \text{known}_{n-1} \vdash t_n \Rightarrow_{\text{comp}} al_n, t'_n, \text{known}_n \\
 \hline
 \rho, \text{known} \vdash f(t_1, \dots, t_n) \Rightarrow_{\text{comp}} al_1 \dots al_n, f(t'_1, \dots, t'_n), \text{known}_n
 \end{array} \tag{33}$$

#### 4.2.4 Décomposition de message

On définit maintenant un jugement  $\rho, known \vdash t \Rightarrow_{\text{dec}} pat, known'$  qui définit comment un terme  $t$  attendu par un principal sera compilé comme un pattern  $pat$ . On rappelle le jugement  $known \vdash t \Rightarrow_{loc} u$  défini par les règles (16) et (17).

D'abord, un terme que l'on peut fabriquer est compilé en un pattern **exact**.

$$\frac{known \vdash t \Rightarrow_{loc} u}{\rho, known \vdash t \Rightarrow_{\text{dec}} \text{exact}(u), known} \quad (34)$$

Notons  $known \vdash t \not\Rightarrow_{loc} u$  le jugement signifiant que  $known \vdash t \Rightarrow_{loc} u$  est faux pour tout  $u$ .

$$\frac{x \in \text{id} \quad z \in \text{id frais} \quad known \vdash x \not\Rightarrow_{loc} z}{\rho, known \vdash x \Rightarrow_{\text{dec}} z, known + \{x \mapsto z\}} \quad (35)$$

Le déchiffrement correspond au pattern-matching des termes de la forme  $\text{crypt}(\dots)$ . On distingue deux cas, selon que l'algorithme de chiffrement  $a$  est symétrique (règle (36)) ou asymétrique (règle (37)).

$$\frac{\begin{array}{l} known \vdash \text{crypt}(a, t, k) \not\Rightarrow_{loc} \quad known \vdash a \Rightarrow_{loc} a' \quad a' = \mathbf{a}(\mathbf{sa}(a_0)) \\ known \vdash k \Rightarrow_{loc} k' \quad \rho, known \vdash t \Rightarrow_{\text{dec}} pat, known' \end{array}}{\rho, known \vdash \text{crypt}(a, t, k) \Rightarrow_{\text{dec}} \text{crypt}(a', pat, k'), known'} \quad (36)$$

Pour le déchiffrement asymétrique, on pose :

$$\begin{aligned} Inv = \{ & \text{hash-apply-pubk} \mapsto \text{hash-apply-privk}, \\ & \text{hash-apply-privk} \mapsto \text{hash-apply-pubk}, \\ & \text{apply-pubk} \mapsto \text{apply-privk}, \\ & \text{apply-privk} \mapsto \text{apply-pubk} \} \end{aligned}$$

$$\frac{\begin{array}{l} known \vdash \text{crypt}(a, t, k) \not\Rightarrow_{loc} \quad known \vdash a \Rightarrow_{loc} a' \quad a' = \mathbf{a}(\mathbf{aa}(a_0)) \\ known \vdash k \Rightarrow_{loc} k' \quad k' = f(a', t_1, \dots, t_n) \\ f \in \text{dom } Inv \quad f' = Inv(f) \quad k^{-1} = f'(a', t_1, \dots, t_n) \\ \rho, known \vdash t \Rightarrow_{\text{dec}} pat, known' \end{array}}{\rho, known \vdash \text{crypt}(a, t, k) \Rightarrow_{\text{dec}} \text{crypt}(a', pat, k^{-1}), known'} \quad (37)$$

On notera que le premier argument de  $f$  dans  $k'$  doit être exactement le même algorithme de chiffrement  $a'$  que celui utilisé pour le chiffrement (le premier argument de  $\text{crypt}$ ).

$$\frac{\begin{array}{l} known \vdash \text{apply}(f, t_1, \dots, t_n) \not\Rightarrow_{loc} \quad f \in \text{id} \\ \rho, known \vdash t_1 \Rightarrow_{\text{dec}} pat_1, known_1 \quad \dots \quad \rho, known_{n-1} \vdash t_n \Rightarrow_{\text{dec}} pat_n, known_n \end{array}}{\rho, known \vdash \text{apply}(f, t_1, \dots, t_n) \Rightarrow_{\text{dec}} \text{apply}(f, pat_1, \dots, pat_n), known_n} \quad (38)$$

$$\frac{\begin{array}{l} known \vdash \text{apply-pubk}(f, t_1, \dots, t_n) \not\Rightarrow_{loc} \quad known \vdash a \Rightarrow_{loc} a' \quad f \in \text{id} \\ \rho, known \vdash t_1 \Rightarrow_{\text{dec}} pat_1, known_1 \quad \dots \quad \rho, known_{n-1} \vdash t_n \Rightarrow_{\text{dec}} pat_n, known_n \end{array}}{\rho, known \vdash \text{apply-pubk}(a, f, t_1, \dots, t_n) \Rightarrow_{\text{dec}} \text{apply-pubk}(a, f, pat_1, \dots, pat_n), known_n} \quad (39)$$

$$\frac{\begin{array}{l} known \vdash \text{apply-privk}(f, t_1, \dots, t_n) \not\Rightarrow_{loc} \quad known \vdash a \Rightarrow_{loc} a' \quad f \in \text{id} \\ \rho, known \vdash t_1 \Rightarrow_{\text{dec}} pat_1, known_1 \quad \dots \quad \rho, known_{n-1} \vdash t_n \Rightarrow_{\text{dec}} pat_n, known_n \end{array}}{\rho, known \vdash \text{apply-privk}(a, f, t_1, \dots, t_n) \Rightarrow_{\text{dec}} \text{apply-privk}(a, f, pat_1, \dots, pat_n), known_n} \quad (40)$$

On note que l'on ne peut pas faire de pattern-matching sur des messages commençant par `hash-apply`, `hash-apply-pubk`, `hash-apply-privk` (on ne peut pas inverser les fonctions `hash`). On interdit aussi le pattern-matching sur `lambda-pubk` et `lambda-privk` (ce qui permettrait de récupérer la partie privée à

partir de sa partie publique et réciproquement). Les cas `crypt`, `apply`, `apply-pubk`, `apply-privk` sont aussi exclus, car traités dans les règles ci-dessus.

$$\begin{array}{c}
 \textit{known} \vdash f(t_1, \dots, t_n) \not\equiv_{loc} \\
 f \notin \{\text{hash-apply}, \text{hash-apply-pubk}, \text{hash-apply-privk}, \\
 \text{crypt}, \text{apply}, \text{apply-pubk}, \text{apply-privk}, \\
 \text{lambda-pubk}, \text{lambda-privk}\} \\
 z \in \text{id frais} \\
 \hline
 \rho, \textit{known} \vdash f(t_1, \dots, t_n) \Rightarrow_{\text{dec}} z, \textit{known} + \{f(t_1, \dots, t_n) \mapsto z\}
 \end{array} \quad (41)$$

#### 4.2.5 Compilation des patterns

Il existe deux façon de compiler l'attente d'un message sur un canal, correspondant à un pattern  $pat$ . La première façon, qui est la façon par défaut pour `evatrans`, est de compiler simplement l'action `recv(pat)`. Ceci est la règle (42).

$$\frac{}{\vdash pat \Rightarrow_{\text{recv}} \text{recv}(pat)} \quad (42)$$

Le jugement ici est de la forme  $\vdash pat \Rightarrow_{\text{recv}} al$ , où  $pat \in \text{Pattern}$ , et  $al \in \text{Action}^*$ .

Lorsque l'option `-d` est fournie à `evatrans`, ce jugement est défini de sorte à compiler une liste d'actions de reconnaissance de patterns élémentaires, qui sont des variables, ou de la forme `exact(t)`, ou de la forme  $f(x_1, \dots, x_n)$ , où les  $x_i$  ne sont plus des patterns généraux mais des variables. Le jugement est alors défini par les règles suivantes. On note  $x_{pat}$  une variable fraîche si  $pat$  n'est pas une variable, et la variable  $pat$  elle-même sinon.

$$\frac{x_{pat} \vdash pat \Rightarrow_{\text{brk}} al}{\vdash pat \Rightarrow_{\text{recv}} al.\text{recv}(x_{pat})} \quad (43)$$

Le jugement auxiliaire  $x \vdash pat \Rightarrow_{\text{brk}} al$  est défini par les règles suivantes.

$$\frac{x_{pat} \vdash pat \Rightarrow_{\text{brk}} al}{x \vdash \text{crypt}(a, pat, k) \Rightarrow_{\text{brk}} al.\text{let}(\text{crypt}(a, x_{pat}, k), x)} \quad (44)$$

Noter dans les règles suivantes qu'on effectue le pattern-matching de gauche à droite. C'est un choix arbitraire qui se retrouve dans la sémantique (section 5).

$$\frac{x_{pat_1} \vdash pat_1 \Rightarrow_{\text{brk}} al_1 \quad \dots \quad x_{pat_n} \vdash pat_n \Rightarrow_{\text{brk}} al_n}{x \vdash \text{apply-pubk}(a, f, pat_1, \dots, pat_n) \Rightarrow_{\text{brk}} al_1.\dots.al_n.\text{let}(\text{apply-pubk}(a, f, x_{pat_1}, \dots, x_{pat_n}), x)} \quad (45)$$

$$\frac{x_{pat_1} \vdash pat_1 \Rightarrow_{\text{brk}} al_1 \quad \dots \quad x_{pat_n} \vdash pat_n \Rightarrow_{\text{brk}} al_n}{x \vdash \text{apply-privk}(a, f, pat_1, \dots, pat_n) \Rightarrow_{\text{brk}} al_1.\dots.al_n.\text{let}(\text{apply-privk}(a, f, x_{pat_1}, \dots, x_{pat_n}), x)} \quad (46)$$

$$\frac{}{x \vdash \text{exact}(t) \Rightarrow_{\text{brk}} \text{let}(\text{exact}(t), x)} \quad (47)$$

On note ici que `let(exact(t), u)` est juste le test d'égalité  $t==u$ .

$$\frac{f \notin \{\text{crypt}, \text{apply-pubk}, \text{apply-privk}, \text{exact}\} \quad x_{pat_1} \vdash pat_1 \Rightarrow_{\text{brk}} al_1 \quad \dots \quad x_{pat_n} \vdash pat_n \Rightarrow_{\text{brk}} al_n}{x \vdash f(pat_1, \dots, pat_n) \Rightarrow_{\text{brk}} al_1.\dots.al_n.\text{let}(f(x_{pat_1}, \dots, x_{pat_n}), x)} \quad (48)$$

$$\frac{}{x \vdash x \Rightarrow_{\text{brk}} \epsilon} \quad (49)$$

#### 4.2.6 Compilation des messages

On utilise ici un jugement  $R, S, \gamma, src, tgt, ls \vdash m \Rightarrow_{\text{code}} \gamma', S', ls'$ , où  $R \in \mathbb{P}(\text{id})$  est l'ensemble des noms de rôles participant au protocole,  $S$  et  $S'$  sont des contextes comme décrits en section 4.2.2,  $src, tgt \in \text{state}$ ,  $ls, ls' \in \mathbb{P}(\text{state})$ ,  $m \in \text{Message}$ ,  $\gamma, \gamma' \in \text{id} \rightarrow \mathbb{P}(\text{state} \times \text{state} \times \text{Action})$  est une famille de graphes indexés par des noms de principaux. Les graphes sont des ensembles de transitions. De plus, tous les états de  $\gamma$  sont dans  $ls'$ .

D'abord, on traite des envois de messages (fonction `comm`). Pour traiter de la notation ‘%’, on pose:

$$\begin{aligned} split_1(\text{percent}(s, t)) &= s \\ split_2(\text{percent}(s, t)) &= t \\ split_i(x) &= x \quad (1 \leq i \leq 2) \\ split_i(f(t_1, \dots, t_n)) &= f(split_i(t_1), \dots, split_i(t_n)) \quad (1 \leq i \leq 2) \end{aligned}$$

Le prédicat  $pure(t)$ , quant à lui, est vrai si et seulement si  $t$  ne contient pas de sous-terme commençant par `percent`.

On note  $[g(a)]$  la fonction  $g(a)$  si  $a \in \text{dom } g$ , la fonction vide  $\{\}$  sinon. On note d'autre part, pour toute liste  $al = a_1 \dots a_n$  d'actions ( $n \geq 1$ ), et tout graphe  $G$ ,  $G + (src \xrightarrow{al} tgt)$  tout graphe dont les transitions sont celles de  $\gamma$  plus les  $(st_{i-1}, a_i, st_i)$ ,  $1 \leq i \leq n$ , où  $st_0 = src$ ,  $st_n = tgt$ , et les  $st_i$ ,  $1 \leq i < n$ , sont des états dans  $\text{state} \setminus \text{label}$ , distincts deux à deux et frais (distincts de tout autre label apparaissant dans  $G$  ou un autre graphe). Lorsque  $n = 0$ , on étend cette notation pour dénoter  $G + (src \xrightarrow{\text{skip}()} tgt)$ . On note enfin  $\gamma + \{p_1 \mapsto (src_1 \xrightarrow{al_1} tgt_1), \dots, p_n \mapsto (src_n \xrightarrow{al_n} tgt_n)\}$  la fonction qui à  $p \in \text{dom } \gamma \setminus \{p_1, \dots, p_n\}$  associe  $\gamma(p)$ , à  $p_i$  associe  $[\gamma(p_i)] + (src_i \xrightarrow{al_i} tgt_i)$  si  $1 \leq i \leq n$ .

$$\begin{array}{c} lab \in \text{label} \setminus ls \quad s \neq r \quad s, r \in \text{dom } R \\ t_1 = split_1(m) \quad t_2 = split_2(m) \quad pure(t_1) \quad pure(t_2) \\ \rho \text{ of } S, (\sigma \text{ of } S) + [(\theta \text{ of } S)(s)], - \vdash t_1 \Rightarrow_{\text{term}} u_1 : \text{number} \\ \rho \text{ of } S, [(\kappa \text{ of } S)(s)] \vdash u_1 \Rightarrow_{\text{comp}} al_1, v_1, known_1 \\ \rho \text{ of } S, (\sigma \text{ of } S) + [(\theta \text{ of } S)(r)], - \vdash t_2 \Rightarrow_{\text{term}} u_2 : \text{number} \\ \rho \text{ of } S, [(\kappa \text{ of } S)(r)] \vdash u_2 \Rightarrow_{\text{dec}} pat, known_2 \\ x_{pat} \vdash pat \Rightarrow_{\text{brk}} al_2 \\ \kappa = \{s \mapsto known_1, r \mapsto known_2\} \\ \gamma' = \gamma + \{s \mapsto (src \xrightarrow{al_1 \cdot \text{send}(v_1)} tgt), r \mapsto (src \xrightarrow{al_2} tgt)\} + \{p \mapsto (src \xrightarrow{\text{skip}()} tgt) \mid p \in R \setminus \{s, r\}\} \\ \hline R, S, \gamma, src, tgt, ls \vdash \text{comm}(lab, s, r, m) \Rightarrow_{\text{code}} \gamma', S + \kappa, ls \cup \{lab\} \end{array} \quad (50)$$

On note que  $lab$  n'est pas en réalité utilisé dans cette règle. En pratique, `evatrans` a une politique de création de labels qui fait que  $src$  vaudra toujours  $lab$  ici.

Dans la règle (50), il n'est pas spécifié qu'il faille vérifier que les axiomes  $\alpha$  of  $S$  impliquent que  $u_1 = u_2$ . Le traducteur `evatrans` émet cependant un warning s'il n'arrive pas à prouver cette égalité, à l'aide d'un prouveur incomplet mais terminant en temps polynomial.

$$\begin{array}{c} R, S, \gamma, src, lab_1, ls \vdash m_1 \Rightarrow_{\text{code}} \gamma_1, S_1, ls_1 \quad \dots \\ R, S_{n-1}, \gamma_{n-1}, lab_{n-1}, tgt, ls_{n-1} \vdash m_n \Rightarrow_{\text{code}} \gamma_n, S_n, ls_n \\ lab_1, \dots, lab_{n-1} \in \text{label frais} \\ \hline R, S, \gamma, src, tgt, ls \vdash \text{block}(m_1, \dots, m_n) \Rightarrow_{\text{code}} \gamma_n, S_n, ls_n \end{array} \quad (51)$$

$$\begin{array}{c}
 p \in \text{dom } R \\
 \rho \text{ of } S, (\sigma \text{ of } S) + [(\theta \text{ of } S)(p)], - \vdash x \Rightarrow_{\text{term}} s : \text{number} \\
 \rho \text{ of } S, (\sigma \text{ of } S) + [(\theta \text{ of } S)(p)], - \vdash t \Rightarrow_{\text{term}} u : \text{number} \\
 \rho \text{ of } S, [(\kappa \text{ of } S)(s)] \vdash u \Rightarrow_{\text{comp}} al, v, \text{known} \\
 \kappa = \{p \mapsto \text{known}\} \\
 al' = al.\text{let}(\text{exact}(s), u) \\
 \hline
 \gamma' = \gamma + \{p \mapsto (src \xrightarrow{al'} tgt)\} + \{p' \mapsto (src \xrightarrow{\text{skip}()} tgt) \mid p' \in R \setminus \{p\}\} \\
 R, S, \gamma, src, tgt, ls \vdash \text{equals}(p, x, t) \Rightarrow_{\text{code}} \gamma', S + \kappa, ls
 \end{array} \tag{52}$$

$$\begin{array}{c}
 p \in \text{dom } R \\
 z \in \text{id frais} \\
 \rho \text{ of } S, (\sigma \text{ of } S) + [(\theta \text{ of } S)(p)], - \vdash t \Rightarrow_{\text{term}} u : \text{number} \\
 \rho \text{ of } S, [(\kappa \text{ of } S)(s)] \vdash u \Rightarrow_{\text{comp}} al, v, \text{known} \\
 \kappa = \{p \mapsto \text{known} + \{x \mapsto z\}\} \\
 al' = al.\text{let}(z, u) \\
 \hline
 \gamma' = \gamma + \{p \mapsto (src \xrightarrow{al'} tgt)\} + \{p' \mapsto (src \xrightarrow{\text{skip}()} tgt) \mid p' \in R \setminus \{p\}\} \\
 R, S, \gamma, src, tgt, ls \vdash \text{assign}(p, x, t) \Rightarrow_{\text{code}} \gamma', S + \kappa, ls
 \end{array} \tag{53}$$

$$\begin{array}{c}
 z \in \text{id frais} \\
 R_0 = \{ \begin{array}{l} p \mapsto (\text{known}, al.\text{let}(z, v)) \\ \mid \exists u. \\ \rho \text{ of } S, (\sigma \text{ of } S) + [(\theta \text{ of } S)(p)], - \vdash t \Rightarrow_{\text{term}} u : \text{number} \\ \rho \text{ of } S, [(\kappa \text{ of } S)(p)] \vdash u \Rightarrow_{\text{comp}} al, v, \text{known} \} \\
 c_1 = \text{case}(t_1, u_{11}, \dots, u_{1m_1}) \quad \dots \\
 c_n = \text{case}(t_n, u_{n1}, \dots, u_{nm_n}) \\
 lab, lab_1, \dots, lab_n \in \text{label frais} \end{array} \\
 \gamma_0 = \gamma + \{p \mapsto (src \xrightarrow{al} lab) \\
 \mid p \in \text{dom } R_0, (\text{known}, al) = R_0(p)\} \\
 + \{p \mapsto (lab \xrightarrow{\text{let}(\text{exact}(v), z)} lab_i) \\
 \mid p \in \text{dom } R_0, 1 \leq i \leq n, (\text{known}, al) = R_0(p), \text{known} \vdash t_i \Rightarrow_{loc} v\} \\
 \kappa = \{p \mapsto \text{known} \mid p \in \text{dom } R_0, (\text{known}, al) = R_0(p)\} \quad S_0 = S + \kappa \\
 \text{dom } R_0, S_0, \gamma_0, lab_1, tgt, ls \vdash \text{block}(u_{11}, \dots, u_{1m_1}) \Rightarrow_{\text{code}} \gamma_1, S_1, ls_1 \quad \dots \\
 \text{dom } R_0, S_{n-1}, \gamma_{n-1}, lab_n, tgt, ls_{n-1} \vdash \text{block}(u_{n1}, \dots, u_{nm_n}) \Rightarrow_{\text{code}} \gamma_n, S_n, ls_n \\
 \hline
 \gamma' = \gamma_n + \{p \mapsto (src \xrightarrow{\text{skip}()} tgt) \mid p \in R \setminus \text{dom } R_0\} \\
 R, S, \gamma, src, tgt, ls \vdash \text{switch}(t, c_1, \dots, c_n) \Rightarrow_{\text{code}} \gamma', S_n, ls_n
 \end{array} \tag{54}$$

On forme le jugement  $S \vdash m \Rightarrow_{\text{msgs}} start, \gamma, S'$ , où  $m \in \text{Message}$ ,  $\gamma \in \text{id} \rightarrow \mathbb{P}(\text{state} \times \text{state} \times \text{Action})$  et  $start \in \text{state}$  est l'état de départ de tous les graphes. On définit la fonction  $roles(m)$ , qui calcule l'ensemble des noms de rôles utilisés dans le protocole  $m$ :

$$\begin{array}{l}
 roles(\text{comm}(lab, s, r, t)) = \{s, r\} \\
 roles(\text{equals}(p, x, t)) = \{p\} \\
 roles(\text{assign}(p, x, t)) = \{p\} \\
 roles(\text{block}(t_1, \dots, t_n)) = roles(t_1) \cup \dots \cup roles(t_n) \\
 roles(\text{switch}(t, c_1, \dots, c_n)) = roles(c_1) \cup \dots \cup roles(c_n) \\
 roles(\text{case}(t, t_1, \dots, t_n)) = roles(t) \cup \dots \cup roles(t_n) \\
 \\
 \hline
 \frac{roles(m), S, \{\}, start, \text{end.}, \{\text{end.}\} \vdash m \Rightarrow_{\text{code}} \gamma, S', ls'}{S \vdash m \Rightarrow_{\text{msgs}} start, \gamma, S'}
 \end{array} \tag{55}$$

### 4.2.7 Déclarations de sessions

On définit un jugement  $\rho, \sigma \vdash ss \Rightarrow_{\text{sess}} \zeta$ , où  $\rho : \text{id} \rightarrow \text{Type}$ ,  $\sigma : \text{id} \rightarrow \text{Term}$ ,  $ss \in \text{Sessions}$ ,  $\zeta : \text{label} \rightarrow [\mathbb{P}(\text{id})] \times (\text{id} \rightarrow \text{Term}) \times \mathbb{P}(\text{id})$ , qui précompile les déclarations de sessions:  $\zeta$  associe à chaque identificateur de session un triplet formé d'un ensemble optionnel d'identificateurs (les variables privées, déclarées par `private`, des multi-sessions parallèles, si présent; si absent, c'est une mono-session), d'une substitution (les affectations de termes aux variables), et d'un ensemble d'identificateurs (l'ensemble des rôles présents dans la session).

$$\frac{\begin{array}{c} \zeta_0 = \{\} \\ \rho, \sigma, \zeta_0 \vdash s_1 \Rightarrow_{\text{ses}} \zeta_1 \quad \dots \\ \rho, \sigma, \zeta_{n-1} \vdash s_n \Rightarrow_{\text{ses}} \zeta_n \end{array}}{\rho, \sigma \vdash \text{sessions}(s_1, \dots, s_n) \Rightarrow_{\text{sess}} \zeta_n} \quad (56)$$

On utilise le jugement auxiliaire  $\rho, \sigma, \zeta \vdash s \Rightarrow_{\text{ses}} \zeta'$ , où  $s \in \text{Session}$ . Ce jugement est lui-même défini en fonction de deux autres jugements auxiliaires  $\rho, \sigma, \sigma' \vdash b_1, \dots, b_n \Rightarrow_{\text{bind}} \sigma'$  et  $\vdash ps \Rightarrow_{\text{princ}} prs$ .

$$\frac{\begin{array}{c} lab \in \text{label} \setminus \text{dom } \zeta \\ \vdash ps \Rightarrow_{\text{princ}} prs \\ \rho, \sigma, \{\} \vdash b_1, \dots, b_n \Rightarrow_{\text{bind}} \sigma' \end{array}}{\rho, \sigma, \zeta \vdash \text{session}(lab, ps, b_1, \dots, b_n) \Rightarrow_{\text{ses}} \zeta + \{lab \mapsto (-, \sigma', prs)\}} \quad (57)$$

Rappelons que l'on note  $-$  un champ option absent.

$$\frac{\begin{array}{c} x_1, \dots, x_n \in \text{id} \\ pr = \text{private}(x_1, \dots, x_m) \\ lab \in \text{label} \setminus \text{dom } \zeta \\ \vdash ps \Rightarrow_{\text{princ}} prs \\ \rho, \sigma, \{\} \vdash b_1, \dots, b_n \Rightarrow_{\text{bind}} \sigma' \end{array}}{\rho, \sigma, \zeta \vdash \text{session-repeat}(pr, lab, ps, b_1, \dots, b_n) \Rightarrow_{\text{ses}} \zeta + \{lab \mapsto (\{x_1, \dots, x_m\}, \sigma', prs)\}} \quad (58)$$

$$\frac{x_1, \dots, x_n \in \text{id}}{\vdash \text{principals-only}(x_1, \dots, x_n) \Rightarrow_{\text{princ}} \{x_1, \dots, x_n\}} \quad (59)$$

$$\frac{x_1, \dots, x_n \in \text{id}}{\vdash \text{principals-except}(x_1, \dots, x_n) \Rightarrow_{\text{princ}} \text{id} \setminus \{x_1, \dots, x_n\}} \quad (60)$$

$$\frac{}{\rho, \sigma, \sigma' \vdash \epsilon \Rightarrow_{\text{bind}} \sigma'} \quad (61)$$

$$\frac{\begin{array}{c} x \in \text{dom } \rho \setminus (\text{dom } \sigma \cup \text{dom } \sigma') \\ \rho, \sigma, - \vdash t \Rightarrow_{\text{term}} u : \rho(x) \\ u \in \text{id} \setminus \text{dom } \sigma' \end{array}}{\frac{\rho, \sigma, \sigma' + \{x \mapsto u\} \vdash b_2, \dots, b_n \Rightarrow_{\text{bind}} \sigma''}{\rho, \sigma, \sigma' \vdash \text{bind}(x, t), b_2, \dots, b_n \Rightarrow_{\text{bind}} \sigma''}} \quad (62)$$

On note que  $u$  est contraint à être une variable, et non n'importe quel terme.

### 4.2.8 Formules

On définit un jugement  $\rho, \sigma, \ell, \tilde{\gamma} \vdash F \Rightarrow_{\text{form}} F'$ , où  $\rho : \text{id} \rightarrow \text{Type}$ ,  $\sigma : \text{id} \rightarrow \text{Term}$ ,  $\ell : \text{label} \times \text{id} \rightarrow \text{Term} \rightarrow \text{Term}$ ,  $\tilde{\gamma} : \text{label} \times \text{id} \rightarrow \mathbb{P}(\text{state} \times \text{state} \times \text{Action})$ , et  $F, F' : \text{Form}$ .

On note que  $\ell \neq -$  ici. Ceci impose que les termes  $t_i$  soient équipés d'annotations `locate` permettant de savoir, au moins pour toute variable libre de  $t_i$ , dans quel principal elle doit être consultée.

$$\frac{P \in \text{id} \quad \rho, \sigma, \ell \vdash t_1 \Rightarrow_{\text{term}} u_1 : \text{number} \quad \dots \quad \rho, \sigma, \ell \vdash t_n \Rightarrow_{\text{term}} u_n : \text{number}}{\rho, \sigma, \ell, \tilde{\gamma} \vdash \text{prop}(P, t_1, \dots, t_n) \Rightarrow_{\text{form}} \text{prop}(P, u_1, \dots, u_n)} \quad (63)$$

Dans la règle suivante,  $\tilde{\gamma}(s, p)$  est un graphe  $G$ . On définit  $\text{states } G$  comme étant l'ensemble  $\{src, tgt \mid (src \xrightarrow{a} tgt) \in G\}$  des sommets de  $G$ .

$$\frac{(s, p) \in \text{dom } \ell \quad (s, p) \in \text{dom } \tilde{\gamma} \quad lab \in \text{states}(\tilde{\gamma}(s, p)) \cup \{\text{end.}\}}{\rho, \sigma, \ell, \tilde{\gamma} \vdash \text{at}(s, p, lab) \Rightarrow_{\text{form}} \text{at}(s, p, lab)} \quad (64)$$

$$\frac{(s, p) \in \text{dom } \ell \quad \rho, \sigma, \ell \vdash t \Rightarrow_{\text{term}} u : \text{number}}{\rho, \sigma, \ell, \tilde{\gamma} \vdash \text{owns}(s, p, t) \Rightarrow_{\text{form}} \text{owns}(s, p, u)} \quad (65)$$

$$\frac{\rho, \sigma, \ell \vdash t \Rightarrow_{\text{term}} u : \text{number}}{\rho, \sigma, \ell, \tilde{\gamma} \vdash \text{secret}(t) \Rightarrow_{\text{form}} \text{secret}(s, p, u)} \quad (66)$$

$$\frac{\rho, \sigma, \ell, \tilde{\gamma} \vdash F \Rightarrow_{\text{form}} F' \quad \rho, \sigma, \ell, \tilde{\gamma} \vdash G \Rightarrow_{\text{form}} G'}{\rho, \sigma, \ell, \tilde{\gamma} \vdash \text{implies}(F, G) \Rightarrow_{\text{form}} \text{implies}(F', G')} \quad (67)$$

$$\frac{\rho, \sigma, \ell, \tilde{\gamma} \vdash F_1 \Rightarrow_{\text{form}} F'_1 \quad \dots \quad \rho, \sigma, \ell, \tilde{\gamma} \vdash F_n \Rightarrow_{\text{form}} F'_n}{\rho, \sigma, \ell, \tilde{\gamma} \vdash \text{and}(F_1, \dots, F_n) \Rightarrow_{\text{form}} \text{and}(F'_1, \dots, F'_n)} \quad (68)$$

$$\frac{\rho, \sigma, \ell, \tilde{\gamma} \vdash F_1 \Rightarrow_{\text{form}} F'_1 \quad \dots \quad \rho, \sigma, \ell, \tilde{\gamma} \vdash F_n \Rightarrow_{\text{form}} F'_n}{\rho, \sigma, \ell, \tilde{\gamma} \vdash \text{or}(F_1, \dots, F_n) \Rightarrow_{\text{form}} \text{or}(F'_1, \dots, F'_n)} \quad (69)$$

$$\frac{\rho, \sigma, \ell, \tilde{\gamma} \vdash F \Rightarrow_{\text{form}} F'}{\rho, \sigma, \ell, \tilde{\gamma} \vdash \text{not}(F) \Rightarrow_{\text{form}} \text{not}(F')} \quad (70)$$

$$\frac{\rho, \sigma, \ell, \tilde{\gamma} \vdash F \Rightarrow_{\text{form}} F'}{\rho, \sigma, \ell, \tilde{\gamma} \vdash \text{E}(F) \Rightarrow_{\text{form}} \text{E}(F')} \quad (71)$$

$$\frac{\rho, \sigma, \ell, \tilde{\gamma} \vdash F \Rightarrow_{\text{form}} F'}{\rho, \sigma, \ell, \tilde{\gamma} \vdash \text{A}(F) \Rightarrow_{\text{form}} \text{A}(F')} \quad (72)$$

$$\frac{\rho, \sigma, \ell, \tilde{\gamma} \vdash F \Rightarrow_{\text{form}} F'}{\rho, \sigma, \ell, \tilde{\gamma} \vdash \text{F}(F) \Rightarrow_{\text{form}} \text{F}(F')} \quad (73)$$

$$\frac{\rho, \sigma, \ell, \tilde{\gamma} \vdash F \Rightarrow_{\text{form}} F'}{\rho, \sigma, \ell, \tilde{\gamma} \vdash \text{G}(F) \Rightarrow_{\text{form}} \text{G}(F')} \quad (74)$$

$$\frac{\rho, \sigma, \ell, \tilde{\gamma} \vdash F \Rightarrow_{\text{form}} F'}{\rho, \sigma, \ell, \tilde{\gamma} \vdash \text{P}(F) \Rightarrow_{\text{form}} \text{P}(F')} \quad (75)$$

$$\frac{\rho, \sigma, \ell, \tilde{\gamma} \vdash F \Rightarrow_{\text{form}} F'}{\rho, \sigma, \ell, \tilde{\gamma} \vdash \text{Q}(F) \Rightarrow_{\text{form}} \text{Q}(F')} \quad (76)$$

$$\frac{\rho, \sigma, \ell, \tilde{\gamma} \vdash F \Rightarrow_{\text{form}} F'}{\rho, \sigma, \ell, \tilde{\gamma} \vdash \text{N}(F) \Rightarrow_{\text{form}} \text{N}(F')} \quad (77)$$

$$\frac{\rho, \sigma, \ell, \tilde{\gamma} \vdash F \Rightarrow_{\text{form}} F' \quad \rho, \sigma, \ell, \tilde{\gamma} \vdash G \Rightarrow_{\text{form}} G'}{\rho, \sigma, \ell, \tilde{\gamma} \vdash \text{U}(F, G) \Rightarrow_{\text{form}} \text{U}(F', G')} \quad (78)$$

$$\frac{\rho, \sigma, \ell, \tilde{\gamma} \vdash F \Rightarrow_{\text{form}} F' \quad \rho, \sigma, \ell, \tilde{\gamma} \vdash G \Rightarrow_{\text{form}} G'}{\rho, \sigma, \ell, \tilde{\gamma} \vdash \text{W}(F, G) \Rightarrow_{\text{form}} \text{W}(F', G')} \quad (79)$$

$$\frac{\rho, \sigma, \ell, \tilde{\gamma} \vdash F \Rightarrow_{\text{form}} F' \quad \rho, \sigma, \ell, \tilde{\gamma} \vdash G \Rightarrow_{\text{form}} G'}{\rho, \sigma, \ell, \tilde{\gamma} \vdash \text{S}(F, G) \Rightarrow_{\text{form}} \text{S}(F', G')} \quad (80)$$

$$\frac{\rho, \sigma, \ell, \tilde{\gamma} \vdash F \Rightarrow_{\text{form}} F' \quad \rho, \sigma, \ell, \tilde{\gamma} \vdash G \Rightarrow_{\text{form}} G'}{\rho, \sigma, \ell, \tilde{\gamma} \vdash \text{B}(F, G) \Rightarrow_{\text{form}} \text{B}(F', G')} \quad (81)$$

### 4.2.9 Spécifications

Si  $\sigma$  est une substitution, et  $t$  est un terme, on note  $t\sigma$  le résultat de l'application de la substitution  $\sigma$  à  $t$ :

$$\begin{aligned} x\sigma &= x & \text{si } x \in \text{id} \setminus \text{dom } \sigma \\ x\sigma &= \sigma(x) & \text{si } x \in \text{dom } \sigma \\ f(t_1, \dots, t_n)\sigma &= f(t_1\sigma, \dots, t_n\sigma) \end{aligned}$$

Noter que la substitution s'effectue aussi à travers les patterns. Ceci n'est correct que si la substitution  $\sigma$  remplace des variables par des variables. Ceci est assuré par la règle (62).

On étend cette notation: si  $G$  est un graphe ( $G = \gamma(p)$  dans la règle (82) ci-dessous),  $G\sigma$  est le graphe dont les transitions sont les  $\text{src} \xrightarrow{t\sigma} \text{tgt}$ , lorsque  $(\text{src} \xrightarrow{t} \text{tgt})$  parcourt les transitions de  $G$ . De même, si  $\text{known} : \text{Term} \xrightarrow{\sim} \text{Term}$  ( $\text{known} = (\kappa \text{ of } S)(p)$  dans la règle (82) ci-dessous),  $\text{known}\sigma$  est la fonction qui à  $t \in \text{dom } \text{known}$  associe  $\text{known}(t)\sigma$ .

$$\begin{aligned} S_0 &= \{\text{**asymk**} \mapsto \text{one-way-function}(*D*, \text{number})\} \text{ in } S \\ ds &= \text{declare}(d_1, \dots, d_n) \\ S_0 \vdash d_1 &\Rightarrow_{\text{decl}} S_1 \\ &\dots \\ S_{n-1} \vdash d_n &\Rightarrow_{\text{decl}} S_n \\ S_n \vdash m &\Rightarrow_{\text{msgs}} \text{start}, \gamma, S \\ \rho \text{ of } S, \sigma \text{ of } S \vdash ss &\Rightarrow_{\text{sess}} \zeta \\ \tilde{\gamma} &= \{(s, p) \mapsto \gamma(p)\sigma \mid s \in \text{dom } \zeta, (\text{privs}, \sigma, \text{prs}) = \zeta(s), p \in \text{dom } \gamma \cap \text{prs}\} \\ \ell &= \{(s, p) \mapsto (\kappa \text{ of } S)(p)\sigma \mid s \in \text{dom } \zeta, (\text{privs}, \sigma, \text{prs}) = \zeta(s), p \in \text{dom}(\kappa \text{ of } S) \cap \text{prs}\} \\ rp &= \{(s, p) \mapsto \text{privs} \mid s \in \text{dom } \zeta, (\text{privs}, \sigma, \text{prs}) = \zeta(s), \text{privs} \neq -, p \in \text{dom } \gamma \cap \text{prs}\} \\ as &= \text{assume}(F_1, \dots, F_p) \\ \rho \text{ of } S, \sigma \text{ of } S, \ell, \tilde{\gamma} \vdash F_1 &\Rightarrow_{\text{form}} F'_1 \\ &\dots \\ \rho \text{ of } S, \sigma \text{ of } S, \ell, \tilde{\gamma} \vdash F_p &\Rightarrow_{\text{form}} F'_p \\ as' &= \text{assume}(F'_1, \dots, F'_p) \\ cs &= \text{claim}(G_1, \dots, G_q) \\ \rho \text{ of } S, \sigma \text{ of } S, \ell, \tilde{\gamma} \vdash G_1 &\Rightarrow_{\text{form}} G'_1 \\ &\dots \\ \rho \text{ of } S, \sigma \text{ of } S, \ell, \tilde{\gamma} \vdash G_q &\Rightarrow_{\text{form}} G'_q \\ cs' &= \text{claim}(G'_1, \dots, G'_q) \\ \hline \vdash \text{spec}(ds, m, ss, as, cs) &\Rightarrow_{\text{spec}} \rho \text{ of } S, \sigma \text{ of } S, \alpha \text{ of } S, \text{start}, \tilde{\gamma}, \ell, rp, as', cs' \end{aligned} \tag{82}$$

Pour tout  $\rho : \text{id} \xrightarrow{\sim} \text{Type}$ , on définit de façon sous-déterminée un terme  $\text{Types}(\rho)$  tel que  $\text{Types}(\rho)$  est de la forme  $\text{types}(\text{type}(x_1, \tau_1), \dots, \text{type}(x_n, \tau_n))$ , avec  $\rho = \{x_1 \mapsto \tau_1, \dots, x_n \mapsto \tau_n\}$ ,  $x_1, \dots, x_n$  étant disjointes deux à deux.

De même, pour tout  $\sigma : \text{id} \xrightarrow{\sim} \text{Term}$ , on définit  $\text{Values}(\sigma)$  comme étant n'importe quel terme  $\text{values}(\text{alias}(x_1, t_1), \dots, \text{alias}(x_n, t_n))$  tel que  $\sigma = \{x_1 \mapsto t_1, \dots, x_n \mapsto t_n\}$ ,  $x_1, \dots, x_n$  étant disjointes deux à deux.

Pour tout  $\alpha \in \mathbb{P}(\text{Term} \times \text{Term} \times \text{Type} \times (\text{id} \xrightarrow{\sim} \text{Type}))$ , on pose  $\text{Axioms}(\alpha)$  n'importe quel terme de la forme  $\text{axioms}(\text{axiom}(s_1, t_1, \tau_1, l_1), \dots, \text{axiom}(s_n, t_n, \tau_n, l_n))$ , où  $\alpha = \{(s_1, t_1, \tau_1, \rho_1), \dots, (s_n, t_n, \tau_n, \rho_n)\}$ ,  $\text{Types}(\rho_1) = \text{types}(l_1), \dots, \text{Types}(\rho_n) = \text{types}(l_n)$ . (Où l'on a supposé que  $l_1, \dots, l_n$  étaient des listes de Type-declaration.)

Pour tout  $\text{known} : \text{Term} \xrightarrow{\sim} \text{Term}$ ,  $\text{Know}(\text{known})$  est un terme de la forme  $\text{knows}(\text{as}(s_1, t_1), \dots, \text{as}(s_n, t_n))$ , où  $\text{known} = \{s_1 \mapsto t_1, \dots, s_n \mapsto t_n\}$ .

Pour tout graphe  $G \in \mathbb{P}(\text{state} \times \text{state} \times \text{Action})$ ,  $\text{Trans}(G)$  est toute liste de la forme  $\text{trans}(\text{src}_1, \text{tgt}_1, a_1), \dots, \text{trans}(\text{src}_n, \text{tgt}_n, a_n)$ , où  $G = \{(\text{src}_1, \text{tgt}_1, a_1), \dots, (\text{src}_n, \text{tgt}_n, a_n)\}$ .

Deux graphes  $G$  et  $G'$  sont *équivalents* modulo l'état  $\text{start}$ , ce que l'on notera  $G \equiv_{\text{start}} G'$ , si et seulement s'ils vérifient exactement les mêmes formules d'état closes (cf. section 5.5) en l'état  $\text{start}$ . Ceci

permet de remplacer un graphe  $G$  par un graphe  $G'$  plus simple mais ayant le même comportement. Par exemple,  $\text{evatrans}$  élimine les états inaccessibles depuis  $\text{start}$ , et les transitions  $\text{skip}()$  si possible<sup>2</sup>.

Pour tout  $ps \in \mathbb{P}(\text{id})$ , on définit  $\text{Privates}(ps)$  comme étant tout terme  $\text{private}(x_1, \dots, x_n)$ , avec  $ps = \{x_1, \dots, x_n\}$ .

Pour tout  $\tilde{\gamma} : \text{label} \times \text{id} \rightarrow \mathbb{P}(\text{state} \times \text{state} \times \text{Action})$ ,  $\ell : \text{label} \times \text{id} \rightarrow \text{Term} \rightarrow \text{Term}$ ,  $rp : \text{label} \times \text{id} \rightarrow \mathbb{P}(\text{id})$ , et  $\text{start} \in \text{state}$ , on pose  $\text{System}(\text{start}, \tilde{\gamma}, \ell, rp) = \text{system}(\pi_1, \dots, \pi_n)$ , où  $\pi_1, \dots, \pi_n$  sont  $n$  processus construits comme suit. Énumérons  $\text{dom } \tilde{\gamma} \cup \text{dom } \ell$  sous la forme  $\{(s_1, p_1), \dots, (s_n, p_n)\}$ . Pour chaque  $i$ ,  $1 \leq i \leq n$ , posons  $N_i = s_i.p_i$ , la concaténation du nom de session  $s_i$  et du nom de processus  $p_i$ . Posons  $\text{known}_i = [\ell(s_i, p_i)]$  (cf. section 4.2.6 pour la notation  $[g(a)]$ ),  $k_i = \text{Know}(\text{known}_i)$ ; posons encore  $G_i = [\tilde{\gamma}(s_i, p_i)]$ ,  $g_i = \text{Trans}(G'_i)$ , où  $G'_i$  est n'importe quel graphe tel que  $G_i \equiv_{\text{start}} G'_i$ . Alors  $\pi_i$  est  $\text{process}(N_i, \text{start}, k_i, g_i)$  si  $rp(s, p) = -$ , et est  $\text{repeat-process}(\text{Privates}(rp(s, p)), N_i, \text{start}, k_i, g_i)$  sinon.

Le résultat de la traduction d'une spécification LAEVA  $\text{spec}$  en PEVA réussit si et seulement si on peut dériver:

$$\vdash \text{spec} \Rightarrow_{\text{spec}} \rho, \sigma, \alpha, \text{start}, \tilde{\gamma}, \ell, rp, as, cs$$

Ce résultat est alors le terme:

$$\text{compiled-spec}(\text{Types}(\rho), \text{Values}(\sigma), \text{Axioms}(\alpha), \text{System}(\text{start}, \tilde{\gamma}, \ell, rp), as, cs)$$

## 5 Sémantique

### 5.1 Valeurs

Étant donné un ensemble d'axiomes  $\alpha \in \mathbb{P}(\text{Term} \times \text{Term} \times \text{Type} \times (\text{id} \rightarrow \text{Type}))$ , on définit la relation d'équivalence  $\approx_\alpha$  sur  $\text{Term}$  comme étant la plus petite qui vérifie tous les axiomes de  $\alpha$ . Par vérifier les axiomes de  $\alpha$ , on entend que  $s\sigma \approx_\alpha t\sigma$  pour tout axiome  $(s, t, \tau, \rho) \in \alpha$ , pour toute substitution  $\sigma$  de domaine inclus dans  $\text{dom } \rho$ .

On notera que cette définition ignore les types  $\tau$  ainsi que ceux donnés par  $\rho$ . La restriction de  $\approx_\alpha$  aux termes bien typés est identique à la relation souhaitée, qui ne quantifierait que sur les substitutions bien typées et respectant les types donnés par  $\rho$ . (Ceci dépend du fait qu'aucun de nos types n'est vide, car contenant une infinité de variables.) Cette dernière notion est un peu plus compliquée à définir, car dépendant aussi d'un environnement de typage global; d'où son abandon.

Dans la suite, au lieu de raisonner sur la structure quotient  $\text{Term}/\approx_\alpha$ , on raisonnera sur des termes. Toutes les constructions (sauf  $\text{FST}(t)$  dans la règle (100)) seront invariantes par  $\approx_\alpha$ .

### 5.2 Formalisation de l'intrus

Le jugement  $E \vdash_\alpha t$  définit les conditions sous lesquelles un terme  $t$  (de type `number`) est déductible par l'intrus, lorsque l'intrus a acquis les termes (de type `number`) de l'ensemble de termes  $E$ . Il est paramétré par un ensemble d'axiomes  $\alpha$ , qui est utilisé dans la règle ( $\approx_\alpha$ ). Encore une fois, on raisonne en réalité sur des termes non typés.

$$\frac{}{E, t \vdash_\alpha t} (Ax) \quad \frac{E \vdash_\alpha t \quad t \approx_\alpha t'}{E \vdash_\alpha t'} (\approx_\alpha)$$

<sup>2</sup>Formellement, l'implémentation actuelle est non conforme à la spécification (ce document). En effet, la condition d'équivalence implique qu'on ne puisse pas renommer, supprimer ou rajouter d'état visible (dans label, ne commençant pas par '\*'), puisque le prédicat `at` permet de tester la présence en un état visible. Or `evatrans` remplace deux transitions de la forme  $\text{lab} \xrightarrow{\text{skip}()} \text{lab}' \xrightarrow{a} \text{lab}''$  par une transition  $\text{lab} \xrightarrow{a} \text{lab}''$ , supprimant l'état inaccessible  $\text{lab}'$ , même s'il était visible. Il est facile de corriger le code pour tenir compte de ce bug. Il n'est cependant pas clair que ce soit souhaitable, et une relation moins fine que  $\equiv_{\text{start}}$  ou une logique moins finie que celle proposée est probablement ce qu'il faudrait définir.

$$\begin{array}{c}
 \frac{E \vdash_{\alpha} t \quad E \vdash_{\alpha} k}{E \vdash_{\alpha} \text{crypt}(a, t, k)} (\text{Crypt}I) \quad \frac{E \vdash_{\alpha} \text{crypt}(a(\text{sa}(a_0)), t, k) \quad E \vdash_{\alpha} k}{E \vdash_{\alpha} t} (\text{Crypt}E/\text{sym}) \\
 \\
 \frac{E \vdash_{\alpha} \text{crypt}(a(\text{aa}(a_0)), t, k) \quad k = f(a(\text{aa}(a_0)), t_1, \dots, t_n) \quad f \in \text{dom } \text{Inv} \quad f' = \text{Inv}(f) \quad k^{-1} = f'(a(\text{aa}(a_0)), t_1, \dots, t_n)}{E \vdash_{\alpha} k^{-1}} (\text{Crypt}E/\text{asym}) \\
 \hline
 E \vdash_{\alpha} t
 \end{array}$$

Dans la règle (*CryptI*), noter que l'intrus n'a pas besoin de connaître l'algorithme de chiffrement  $a$ : on suppose que l'intrus connaît *tous* les algorithmes de chiffrement. La règle (*CryptE/sym*) traite du déchiffrement par des algorithmes à clés symétriques, la règle (*CryptE/asym*) du déchiffrement par algorithmes à clés asymétriques; *Inv* est définie en section 4.2.4. On notera que l'intrus n'a aucune règle pour déchiffrer un chiffrement mal typé, de la forme  $\text{crypt}(a, t, k)$  où  $a$  n'est ni de la forme  $a(\text{sa}(a_0))$  ni de la forme  $a(\text{aa}(a_0))$ ; de même si  $a$  est de la seconde forme mais  $k$  n'est pas de la forme  $f(a', t_1, \dots, t_n)$  avec  $f \in \text{Inv}$ , ou bien est de cette forme mais avec  $a \neq a'$ .

$$\frac{E \vdash_{\alpha} t_1 \quad \dots \quad E \vdash_{\alpha} t_n}{E \vdash_{\alpha} \text{tuple}(t_1, \dots, t_n)} (\text{Tuple}I) \quad \frac{E \vdash_{\alpha} \text{tuple}(t_1, \dots, t_n)}{E \vdash_{\alpha} t_i} (\text{Tuple}E_i) (1 \leq i \leq n)$$

L'intrus connaît tous les algorithmes de chiffrement:

$$\frac{}{E \vdash_{\alpha} a(a_0)} (\text{Alg}I)$$

$$\frac{E \vdash_{\alpha} t_1 \quad \dots \quad E \vdash_{\alpha} t_n}{E \vdash_{\alpha} \text{apply}(f, t_1, \dots, t_n)} (\text{App}I) \quad \frac{E \vdash_{\alpha} \text{apply}(f, t_1, \dots, t_n)}{E \vdash_{\alpha} t_i} (\text{App}E_i) (1 \leq i \leq n)$$

$$\frac{E \vdash_{\alpha} t_1 \quad \dots \quad E \vdash_{\alpha} t_n}{E \vdash_{\alpha} \text{hash-apply}(f, t_1, \dots, t_n)} (\text{HApp}I)$$

$$\frac{E \vdash_{\alpha} t_1 \quad \dots \quad E \vdash_{\alpha} t_n}{E \vdash_{\alpha} \text{apply-pubk}(a, f, t_1, \dots, t_n)} (\text{AppPub}I) \quad \frac{E \vdash_{\alpha} \text{apply-pubk}(a, f, t_1, \dots, t_n)}{E \vdash_{\alpha} t_i} (\text{AppPub}E_i) (1 \leq i \leq n)$$

$$\frac{E \vdash_{\alpha} t_1 \quad \dots \quad E \vdash_{\alpha} t_n}{E \vdash_{\alpha} \text{hash-apply-pubk}(a, f, t_1, \dots, t_n)} (\text{HAppPub}I)$$

$$\frac{E \vdash_{\alpha} t_1 \quad \dots \quad E \vdash_{\alpha} t_n}{E \vdash_{\alpha} \text{apply-privk}(a, f, t_1, \dots, t_n)} (\text{AppPriv}I) \quad \frac{E \vdash_{\alpha} \text{apply-privk}(a, f, t_1, \dots, t_n)}{E \vdash_{\alpha} t_i} (\text{AppPriv}E_i) (1 \leq i \leq n)$$

$$\frac{E \vdash_{\alpha} t_1 \quad \dots \quad E \vdash_{\alpha} t_n}{E \vdash_{\alpha} \text{hash-apply-privk}(a, f, t_1, \dots, t_n)} (\text{HAppPriv}I)$$

Il n'y a aucune différence entre partie publique et partie privée des clés, d'un point de vue formelle. La différence est uniquement une différence d'intention. Il n'y a aucune règle sur les  $\text{lambda-pubk}$  et les  $\text{lambda-privk}$ , qui ne fournissent pas des termes de type `number`.

Pour traiter du prédicats `owns`, on a un second jugement  $E; \Omega \vdash A \ni_{\alpha} t$ , où  $A$  est censé être un principal honnête ou l'intrus,  $t$  est un terme de type `number`,  $E$  est un ensemble de termes de type `number`,

et  $\Omega$  est une fonction qui à tout principal honnête associe un ensemble de termes, censé être l'ensemble des termes qu'il a lui-même fabriqués (à l'exclusion de ceux qu'il retransmet).

Formellement,  $A \in P \cup \{I\}$ , où l'ensemble  $P$  des principaux est défini comme l'union disjointe de  $\text{id}$  et de  $\text{id} \times \mathbb{N}$ , et  $I \notin P$  désigne l'intrus,  $t \in \text{Term}$ ,  $\Omega : P \rightarrow \mathbb{P}(\text{Term})$ , et l'on a les règles:

$$\frac{t \in \Omega(A)}{E; \Omega \vdash A \ni_{\alpha} t} \text{ (Creator)} \quad \frac{E; \Omega \vdash A \ni_{\alpha} t \quad t \approx_{\alpha} t'}{E; \Omega \vdash A \ni_{\alpha} t'} (\approx_{\alpha}) \quad \frac{E \vdash_{\alpha} t}{E; \Omega \vdash I \ni_{\alpha} t} \text{ (Intruder)}$$

### 5.3 Actions

On définit la sémantique des actions par un jugement  $E; D, C, \sigma \vdash_{\alpha} a \Rightarrow_{\text{act}} E'; D', C', \sigma'$ , où  $E, E' \in \mathbb{P}(\text{Term})$  (ensembles de termes connus de l'intrus),  $D, D' \in \mathbb{P}(\text{Term})$  (ensembles de données, de type  $*D*$ , déjà créées dans le passé),  $C, C' \in \mathbb{P}(\text{Term})$  (ensembles de données créés par le processus),  $\sigma, \sigma' : \text{id} \rightarrow \text{Term}$ . Dans le cas d'une action  $\text{recv}$  ou  $\text{let}$ , on utilise un jugement auxiliaire  $\sigma; t \vdash_{\alpha} \text{pat} \Rightarrow_{\text{match}} \sigma'$ , où  $\sigma, \sigma' : \text{id} \rightarrow \text{Term}$ ,  $t \in \text{Term}$ ,  $\text{pat} \in \text{Pattern}$ .

$$\frac{x \in \text{id}}{\sigma; t \vdash_{\alpha} x \Rightarrow_{\text{match}} \sigma + \{x \mapsto t\}} \quad (83)$$

$$\frac{u\sigma \approx_{\alpha} t}{\sigma; t \vdash_{\alpha} \text{exact}(u) \Rightarrow_{\text{match}} \sigma} \quad (84)$$

$$\frac{a\sigma \approx_{\alpha} a(\text{sa}(a_0)) \quad t \approx_{\alpha} \text{crypt}(a\sigma, t_1, k\sigma) \quad \sigma; t_1 \vdash_{\alpha} \text{pat} \Rightarrow_{\text{match}} \sigma'}{\sigma; t \vdash_{\alpha} \text{crypt}(a, \text{pat}, k) \Rightarrow_{\text{match}} \sigma'} \quad (85)$$

$$\frac{\begin{array}{l} a\sigma \approx_{\alpha} a(\text{aa}(a_0)) \quad k\sigma \approx_{\alpha} f(a\sigma, s_1, \dots, s_n) \\ f \in \text{dom } \text{Inv} \quad f' = \text{Inv}(f) \quad k^{-1} = f'(a\sigma, s_1, \dots, s_n) \\ t \approx_{\alpha} \text{crypt}(a\sigma, t_1, k^{-1}) \\ \sigma; t_1 \vdash_{\alpha} \text{pat} \Rightarrow_{\text{match}} \sigma' \end{array}}{\sigma; t \vdash_{\alpha} \text{crypt}(a, \text{pat}, k) \Rightarrow_{\text{match}} \sigma'} \quad (86)$$

On rappelle que  $\text{Inv}$  est définie en section 4.2.4.

Pour les patterns qui ont plusieurs sous-patterns en arguments, on effectue le pattern-matching de gauche à droite. C'est un choix arbitraire.

$$\frac{\begin{array}{l} t \approx_{\alpha} \text{apply}(f, t_1, \dots, t_n) \\ \sigma; t_1 \vdash_{\alpha} \text{pat}_1 \Rightarrow_{\text{match}} \sigma_1 \\ \dots \\ \sigma_{n-1}; t_n \vdash_{\alpha} \text{pat}_n \Rightarrow_{\text{match}} \sigma_n \end{array}}{\sigma; t \vdash_{\alpha} \text{apply}(f, \text{pat}_1, \dots, \text{pat}_n) \Rightarrow_{\text{match}} \sigma_n} \quad (87)$$

$$\frac{\begin{array}{l} t \approx_{\alpha} \text{tuple}(t_1, \dots, t_n) \\ \sigma; t_1 \vdash_{\alpha} \text{pat}_1 \Rightarrow_{\text{match}} \sigma_1 \\ \dots \\ \sigma_{n-1}; t_n \vdash_{\alpha} \text{pat}_n \Rightarrow_{\text{match}} \sigma_n \end{array}}{\sigma; t \vdash_{\alpha} \text{tuple}(\text{pat}_1, \dots, \text{pat}_n) \Rightarrow_{\text{match}} \sigma_n} \quad (88)$$

$$\frac{t \approx_{\alpha} \text{d}(t_1) \quad \sigma; t_1 \vdash_{\alpha} \text{pat} \Rightarrow_{\text{match}} \sigma'}{\sigma; t \vdash_{\alpha} \text{d}(\text{pat}) \Rightarrow_{\text{match}} \sigma'} \quad (89)$$

$$\frac{t \approx_{\alpha} \text{p}(t_1) \quad \sigma; t_1 \vdash_{\alpha} \text{pat} \Rightarrow_{\text{match}} \sigma'}{\sigma; t \vdash_{\alpha} \text{p}(\text{pat}) \Rightarrow_{\text{match}} \sigma'} \quad (90)$$

$$\frac{t \approx_{\alpha} \text{a}(t_1) \quad \sigma; t_1 \vdash_{\alpha} \text{pat} \Rightarrow_{\text{match}} \sigma'}{\sigma; t \vdash_{\alpha} \text{a}(\text{pat}) \Rightarrow_{\text{match}} \sigma'} \quad (91)$$

$$\frac{t \approx_\alpha \text{sa}(t_1) \quad \sigma; t_1 \vdash_\alpha \text{pat} \Rightarrow_{\text{match}} \sigma'}{\sigma; t \vdash_\alpha \text{sa}(\text{pat}) \Rightarrow_{\text{match}} \sigma'} \quad (92)$$

$$\frac{t \approx_\alpha \text{aa}(t_1) \quad \sigma; t_1 \vdash_\alpha \text{pat} \Rightarrow_{\text{match}} \sigma'}{\sigma; t \vdash_\alpha \text{aa}(\text{pat}) \Rightarrow_{\text{match}} \sigma'} \quad (93)$$

$$\frac{t \approx_\alpha \text{vanilla}()}{\sigma; t \vdash_\alpha \text{vanilla}() \Rightarrow_{\text{match}} \sigma} \quad (94)$$

$$\frac{\begin{array}{c} t \approx_\alpha \text{apply-pubk}(a, f, t_1, \dots, t_n) \\ \sigma; t_1 \vdash_\alpha \text{pat}_1 \Rightarrow_{\text{match}} \sigma_1 \\ \dots \\ \sigma_{n-1}; t_n \vdash_\alpha \text{pat}_n \Rightarrow_{\text{match}} \sigma_n \end{array}}{\sigma; t \vdash_\alpha \text{apply-pubk}(a, f, \text{pat}_1, \dots, \text{pat}_n) \Rightarrow_{\text{match}} \sigma_n} \quad (95)$$

$$\frac{\begin{array}{c} t \approx_\alpha \text{apply-privk}(a, f, t_1, \dots, t_n) \\ \sigma; t_1 \vdash_\alpha \text{pat}_1 \Rightarrow_{\text{match}} \sigma_1 \\ \dots \\ \sigma_{n-1}; t_n \vdash_\alpha \text{pat}_n \Rightarrow_{\text{match}} \sigma_n \end{array}}{\sigma; t \vdash_\alpha \text{apply-privk}(a, f, \text{pat}_1, \dots, \text{pat}_n) \Rightarrow_{\text{match}} \sigma_n} \quad (96)$$

On passe maintenant aux actions elles-mêmes. En premier, **new** crée une nouvelle donnée (de type  $*D*$ , normalement). Cette donnée étant créée par le principal courant, on l'ajoute aussi à  $C$ .

$$\frac{t \notin D \quad \sigma; t \vdash_\alpha \text{pat} \Rightarrow_{\text{match}} \sigma'}{E; D, C, \sigma \vdash_\alpha \text{new}(\text{pat}) \Rightarrow_{\text{act}} E; D \cup \{t\}, C \cup \{t\}, \sigma'} \quad (97)$$

$$\frac{\sigma; t \vdash_\alpha \text{pat} \Rightarrow_{\text{match}} \sigma'}{E; D, C, \sigma \vdash_\alpha \text{let}(\text{pat}, t) \Rightarrow_{\text{act}} E; D, C, \sigma'} \quad (98)$$

La réception de message opère en acceptant n'importe quel message que l'intrus peut fabriquer:

$$\frac{E \vdash_\alpha t \quad \sigma; t \vdash_\alpha \text{pat} \Rightarrow_{\text{match}} \sigma'}{E; D, C, \sigma \vdash_\alpha \text{recv}(\text{pat}) \Rightarrow_{\text{act}} E; D, C, \sigma'} \quad (99)$$

L'envoi de message consiste à ajouter le message qui est la valeur de  $t$  dans  $\sigma$ , soit  $t\sigma$ , à l'ensemble des messages  $E$  connus par l'intrus. On ajoute aussi à  $C$  tous les messages créés par le principal courant à l'aide du terme  $t$ . Par convention, il s'agit des valeurs de tous les sous-termes non variables  $u$  de  $t$  dans  $\sigma$ . On note  $FST(t)$  l'ensemble de tous les sous-termes non variables de  $t$ . (Noter que cette notion n'est pas définie modulo  $\approx_\alpha$ .)

$$\frac{}{E; D, C, \sigma \vdash_\alpha \text{send}(t) \Rightarrow_{\text{act}} E \cup \{t\sigma\}; D, C \cup \{u\sigma \mid u \in FST(t)\}, \sigma} \quad (100)$$

$$\frac{}{E; D, C, \sigma \vdash_\alpha \text{skip}() \Rightarrow_{\text{act}} E; D, C, \sigma} \quad (101)$$

## 5.4 Processus

Étant donnés  $\tilde{\gamma} : \text{label} \times \text{id} \rightarrow \mathbb{P}(\text{state} \times \text{state} \times \text{Action})$ ,  $rp : \text{label} \times \text{id} \rightarrow \mathbb{P}(\text{id})$ , et  $\text{start} \in \text{state}$ , on définit l'ensemble des principaux actifs comme étant l'ensemble des  $s.p$ , où  $(s, p) \in \text{dom } \tilde{\gamma}$  tels que  $rp(s, p) = -$  (pour les rôles en mono-session), union l'ensemble des  $(s.p, n)$ , où  $(s, p) \in \text{dom } \tilde{\gamma}$  tels que  $rp(s, p) \neq -$ , et  $n \in \mathbb{N}$  (rôles en multi-session parallèle). En tout état de cause, les principaux sont dans l'ensemble  $P = \text{id} \cup \text{id} \times \mathbb{N}$ .

Une configuration globale  $\mathfrak{G}$  du système est un quintuplet  $(E; D, \Omega, \Sigma, pc)$ , où  $E \in \mathbb{P}(\text{Term})$  est l'état de connaissance de l'intrus,  $D \in \mathbb{P}(\text{Term})$  est l'ensemble des données déjà créées,  $\Omega : \mathbb{P} \rightarrow \mathbb{P}(\text{Term})$  envoie chaque principal vers l'ensemble des termes qu'il a fabriqués,  $\Sigma : \mathbb{P} \rightarrow \text{id} \rightarrow \text{Term}$  envoie chaque principal vers un environnement  $\sigma$  contenant les valeurs de ses variables, et  $pc : \mathbb{P} \rightarrow \text{state}$  donne le point de programme courant de chaque principal.

Le système global évolue via la relation de transition  $\tilde{\gamma}, rp \vdash_{\alpha} \mathfrak{G} \Rightarrow_{\text{exec}} \mathfrak{G}'$ . On a d'abord le cas des principaux en mono-session:

$$\begin{array}{c} (p, s) \in \text{dom } \tilde{\gamma} \quad (p, s) \in \text{dom } rp \implies rp(p, s) = - \\ (pc \xrightarrow{a} pc') \in \tilde{\gamma}(p, s) \\ E; D, \Omega(p.s), \Sigma(p.s) \vdash_{\alpha} a \Rightarrow_{\text{act}} E'; D', C', \sigma' \\ \Omega' = \Omega + \{p.s \mapsto C'\} \quad \Sigma' = \Sigma + \{p.s \mapsto \sigma'\} \\ \hline \tilde{\gamma}, rp \vdash_{\alpha} E; D, \Omega, \Sigma, pc \Rightarrow_{\text{exec}} E'; D', \Omega', \Sigma', pc' \end{array} \quad (102)$$

Les principaux en multi-session évoluent comme une mise en parallèle d'un nombre infini de copies  $(p.s, n)$ ,  $n \in \mathbb{N}$ , du processus  $p.s$ :

$$\begin{array}{c} (p, s) \in \text{dom } \tilde{\gamma} \quad (p, s) \in \text{dom } rp \text{ et } rp(p, s) \neq - \quad n \in \mathbb{N} \\ (pc \xrightarrow{a} pc') \in \tilde{\gamma}(p, s) \\ E; D, \Omega(p.s, n), \Sigma(p.s, n) \vdash_{\alpha} a \Rightarrow_{\text{act}} E'; D', C', \sigma' \\ \Omega' = \Omega + \{(p.s, n) \mapsto C'\} \quad \Sigma' = \Sigma + \{(p.s, n) \mapsto \sigma'\} \\ \hline \tilde{\gamma}, rp \vdash_{\alpha} E; D, \Omega, \Sigma, pc \Rightarrow_{\text{exec}} E'; D', \Omega', \Sigma', pc' \end{array} \quad (103)$$

Une configuration *initiale* est telle que les états locaux de tous les processus sont à *start*. On impose de plus que la connaissance de l'intrus initiale  $E$ , ainsi que l'ensemble des termes déjà créés, contiennent un ensemble infini  $D_0$  de variables (dans *id*). On suppose de plus que  $\text{id} \setminus D_0$  est lui aussi infini. Cette astuce permet de modéliser la création de nonces et de clés par l'intrus, et remplace une règle qui énoncerait que  $E \vdash_{\alpha} t$  pour tout  $t \in D_0$ . On impose de plus qu'aucun principal n'ait initialement créé de donnée ( $\Omega(A) = \emptyset$ ) et que toute paire de copies d'un même principal en multi-session parallèle ait les mêmes valeurs pour leurs variables non privées.

$$\begin{array}{l} \text{Init}_{\text{start}, rp}(E; D, \Omega, \Sigma, pc) \iff E \supseteq D_0 \\ \text{et } D \supseteq D_0 \\ \text{et } \forall A \in \mathbb{P} \cdot (pc(A) = \text{start} \text{ et } \Omega(A) = \emptyset) \\ \text{et } \forall (s, p) \in \text{dom } rp \cap \text{dom } \Sigma \cdot rp(s, p) \neq - \implies \\ \quad \forall n, n' \in \mathbb{N} \cdot \forall x \in \text{dom } \Sigma(s, p, n) \setminus rp(s, p) \cdot \\ \quad x \in \text{dom } \Sigma(s, p, n') \text{ et } \Sigma(s, p, n)(x) = \Sigma(s, p, n')(x) \end{array}$$

Ainsi,  $\text{start}, \tilde{\gamma}, rp$  définissent un automate dont les états sont les configurations globales  $\mathfrak{G}$ , les transitions de  $\mathfrak{G}$  vers  $\mathfrak{G}'$  sont données par les instances dérivables de  $\tilde{\gamma}, rp \vdash_{\alpha} \mathfrak{G} \Rightarrow_{\text{exec}} \mathfrak{G}'$ , et les états initiaux sont ceux vérifiant  $\text{Init}_{\text{start}, rp}$ .

On note cet automate  $\mathcal{A}_{\text{start}, \tilde{\gamma}, rp}$ .

## 5.5 Formules

Un *chemin*  $\bar{\mathfrak{G}}$  dans un automate  $\mathcal{A}$ , partant de l'état  $\mathfrak{G}$ , est une suite infinie  $\mathfrak{G}_0, \mathfrak{G}_1, \dots, \mathfrak{G}_k, \dots$ , de configurations telles que  $\mathfrak{G}_0 = \mathfrak{G}$ , et pour tout  $i \in \mathbb{N}$ , soit  $\mathfrak{G}_i = \mathfrak{G}_{i+1}$  soit il existe une transition de  $\mathfrak{G}_i$  vers  $\mathfrak{G}_{i+1}$  dans  $\mathcal{A}$ . On note  $\bar{\mathfrak{G}}(k) = \mathfrak{G}_k$ , et  $\bar{\mathfrak{G}}(\geq k)$  le suffixe  $\mathfrak{G}_k, \mathfrak{G}_{k+1}, \dots, \mathfrak{G}_i, \dots$ . On remarque que l'on autorise le bégaiement ( $\mathfrak{G}_i = \mathfrak{G}_{i+1}$ ) sur les chemins, et même le bégaiement infini (pour tout  $i \geq k$ ,  $\mathfrak{G}_i = \mathfrak{G}_k$ ). De la sorte, il existe toujours un chemin partant de n'importe quel état.

Une formule  $F$  est évaluée sur un chemin  $\bar{\mathfrak{G}}$  à une position  $k \in \mathbb{N}$ . La logique d'EVA est, comme on le constatera, une variante de NCTL\* [LS95]. Il ne lui manque que les opérateurs "next-state" et "previous-state", et elle a une sémantique invariante par bégaiement par construction, ce qui en fait un lointain cousin de TLA [Lam94].

Pour tout  $(s, p) \in \text{dom } rp$ , on note  $(s.p)_{rp}$  le processus  $s.p$  si  $rp(s, p) = -$ , et  $(s.p, 0)$  sinon. Dans ce dernier cas,  $(s.p)_{rp}$  dénote donc la copie numéro 0 du processus en multi-session parallèle  $s.p$ .

L'interprétation  $I$  est une application de  $\text{id}$  vers  $\mathbb{P}(\text{Term}^*)$ , qui sert à interpréter les symboles de prédicats (premiers arguments de  $\text{prop}$ ). On suppose que  $I$  envoie 'equal's' vers l'ensemble  $\{(t, t) \mid t \in \text{Term}\}$ . (C'est la relation d'égalité.) Les interprétations des autres prédicats sont réservées, et pourront être définies ultérieurement.

Les termes  $t$  sont interprétés par la fonction  $\llbracket t \rrbracket \Sigma rp$  définie comme suit:

$$\llbracket \text{located}(s, p, t) \rrbracket \Sigma rp = t\sigma, \text{ avec } \sigma = \Sigma((s.p)_{rp}) \quad (104)$$

$$\llbracket f(t_1, \dots, t_n) \rrbracket \Sigma rp = f(\llbracket t_1 \rrbracket \Sigma rp, \dots, \llbracket t_n \rrbracket \Sigma rp) \quad (105)$$

où  $f \neq \text{located}$ . Cette fonction est partielle. Notamment  $\llbracket x \rrbracket \Sigma rp$  n'est pas définie lorsque  $x$  est une variable, et  $\llbracket \text{located}(s, p, t) \rrbracket \Sigma rp$  n'est pas définie lorsque  $(s.p)_{rp} \notin \text{dom } \Sigma$ . Les règles de typage assurent cependant que  $\llbracket t \rrbracket \Sigma rp$  sera toujours définie dans les cas où elle sera utilisée.

$$\bar{\mathfrak{G}}, k; I, rp \models_{\alpha} \text{prop}(P, t_1, \dots, t_n) \Leftrightarrow (\llbracket t_1 \rrbracket (\Sigma \text{ of } \bar{\mathfrak{G}}(k))rp, \dots, \llbracket t_n \rrbracket (\Sigma \text{ of } \bar{\mathfrak{G}}(k))rp) \in I(P) \quad (106)$$

$$\bar{\mathfrak{G}}, k; I, rp \models_{\alpha} \text{at}(s, p, lab) \Leftrightarrow pc \text{ of } \bar{\mathfrak{G}}(k)((s.p)_{rp}) = lab \quad (107)$$

$$\begin{aligned} \bar{\mathfrak{G}}, k; I, rp \models_{\alpha} \text{owns}(s, p, t) &\Leftrightarrow \forall A \in \mathbf{P} \cup \{\mathbf{I}\}. \\ &(E \text{ of } \bar{\mathfrak{G}}(k); \Omega \text{ of } \bar{\mathfrak{G}}(k) \vdash A \ni_{\alpha} \llbracket t \rrbracket (\Sigma \text{ of } \bar{\mathfrak{G}}(k))rp \\ &\implies A = (s.p)_{rp}) \end{aligned} \quad (108)$$

$$\bar{\mathfrak{G}}, k; I, rp \models_{\alpha} \text{secret}(t) \Leftrightarrow E \text{ of } \bar{\mathfrak{G}}(k) \not\vdash_{\alpha} \llbracket t \rrbracket (\Sigma \text{ of } \bar{\mathfrak{G}}(k))rp \quad (109)$$

$$\bar{\mathfrak{G}}, k; I, rp \models_{\alpha} \text{implies}(F, G) \Leftrightarrow (\bar{\mathfrak{G}}, k; I, rp \models_{\alpha} F) \implies (\bar{\mathfrak{G}}, k; I, rp \models_{\alpha} G) \quad (110)$$

$$\begin{aligned} \bar{\mathfrak{G}}, k; I, rp \models_{\alpha} \text{and}(F_1, \dots, F_n) &\Leftrightarrow (\bar{\mathfrak{G}}, k; I, rp \models_{\alpha} F_1) \\ &\text{et } \dots \text{ et } (\bar{\mathfrak{G}}, k; I, rp \models_{\alpha} F_n) \end{aligned} \quad (111)$$

$$\begin{aligned} \bar{\mathfrak{G}}, k; I, rp \models_{\alpha} \text{or}(F_1, \dots, F_n) &\Leftrightarrow (\bar{\mathfrak{G}}, k; I, rp \models_{\alpha} F_1) \\ &\text{ou } \dots \text{ ou } (\bar{\mathfrak{G}}, k; I, rp \models_{\alpha} F_n) \end{aligned} \quad (112)$$

$$\bar{\mathfrak{G}}, k; I, rp \models_{\alpha} \text{not}(F) \Leftrightarrow \bar{\mathfrak{G}}, k; I, rp \not\models_{\alpha} F \quad (113)$$

$$\bar{\mathfrak{G}}, k; I, rp \models_{\alpha} \mathbf{E}(F) \Leftrightarrow \exists \bar{\mathfrak{G}}' \cdot (\forall i \leq k \cdot \bar{\mathfrak{G}}'(i) = \bar{\mathfrak{G}}(i)) \text{ et } \bar{\mathfrak{G}}', k; I, rp \models_{\alpha} F \quad (114)$$

$$\bar{\mathfrak{G}}, k; I, rp \models_{\alpha} \mathbf{A}(F) \Leftrightarrow \forall \bar{\mathfrak{G}}' \cdot (\forall i \leq k \cdot \bar{\mathfrak{G}}'(i) = \bar{\mathfrak{G}}(i)) \implies \bar{\mathfrak{G}}', k; I, rp \models_{\alpha} F \quad (115)$$

$$\bar{\mathfrak{G}}, k; I, rp \models_{\alpha} \mathbf{F}(F) \Leftrightarrow \exists k' \geq k \cdot \bar{\mathfrak{G}}, k'; I, rp \models_{\alpha} F \quad (116)$$

$$\bar{\mathfrak{G}}, k; I, rp \models_{\alpha} \mathbf{G}(F) \Leftrightarrow \forall k' \geq k \cdot \bar{\mathfrak{G}}, k'; I, rp \models_{\alpha} F \quad (117)$$

$$\bar{\mathfrak{G}}, k; I, rp \models_{\alpha} \mathbf{P}(F) \Leftrightarrow \exists k' \leq k \cdot \bar{\mathfrak{G}}, k'; I, rp \models_{\alpha} F \quad (118)$$

$$\bar{\mathfrak{G}}, k; I, rp \models_{\alpha} \mathbf{Q}(F) \Leftrightarrow \forall k' \leq k \cdot \bar{\mathfrak{G}}, k'; I, rp \models_{\alpha} F \quad (119)$$

$$\bar{\mathfrak{G}}, k; I, rp \models_{\alpha} \mathbf{N}(F) \Leftrightarrow \bar{\mathfrak{G}}(\geq k), 0; I, rp \models_{\alpha} F \quad (120)$$

$$\begin{aligned} \bar{\mathfrak{G}}, k; I, rp \models_{\alpha} \mathbf{U}(F, G) &\Leftrightarrow \exists k' \geq k \cdot \\ &(\forall i \cdot k \leq i < k' \implies \bar{\mathfrak{G}}, i; I, rp \models_{\alpha} F) \\ &\text{et } \bar{\mathfrak{G}}, k'; I, rp \models_{\alpha} G \end{aligned} \quad (121)$$

$$\begin{aligned} \bar{\mathfrak{G}}, k; I, rp \models_{\alpha} \mathbf{W}(F, G) &\Leftrightarrow \forall k' \geq k \cdot \\ &(\forall i \cdot k \leq i < k' \implies \bar{\mathfrak{G}}, i; I, rp \not\models_{\alpha} G) \\ &\implies (\forall i \cdot k \leq i < k' \implies \bar{\mathfrak{G}}, i; I, rp \models_{\alpha} F) \end{aligned} \quad (122)$$

$$\begin{aligned} \bar{\mathfrak{G}}, k; I, rp \models_{\alpha} \mathbf{S}(F, G) &\Leftrightarrow \exists k' \leq k \cdot \\ &(\forall i \cdot k' < i \leq k \implies \bar{\mathfrak{G}}, i; I, rp \models_{\alpha} F) \\ &\text{et } \bar{\mathfrak{G}}, k'; I, rp \models_{\alpha} G \end{aligned} \quad (123)$$

$$\begin{aligned} \bar{\mathfrak{G}}, k; I, rp \models_{\alpha} \mathbf{B}(F, G) &\Leftrightarrow \forall k' \leq k \cdot \\ &(\forall i \cdot k' < i \leq k \implies \bar{\mathfrak{G}}, i; I, rp \not\models_{\alpha} G) \end{aligned} \quad (124)$$

$$\implies (\forall i \cdot k' < i \leq k \implies \bar{\mathfrak{G}}, i; I, rp \models_{\alpha} F)$$

## 5.6 Validité

Finalemnt, étant donné une spécification LAEVA  $spec$  telle que:

$$\vdash spec \Rightarrow_{spec} \rho, \sigma, \alpha, start, \tilde{\gamma}, \ell, rp, \mathbf{assume}(F_1, \dots, F_m), \mathbf{claim}(G_1, \dots, G_n)$$

on dit que  $spec$  est *valide* si et seulement si, définissant  $\mathcal{A}_{start, \tilde{\gamma}, rp}$  et  $Init_{start, rp}$  comme en section 5.4, alors pour tout chemin  $\bar{\mathfrak{G}}$  partant d'un état quelconque  $\mathfrak{G}$  satisfaisant  $Init_{start, rp}$  et tel que

$$\bar{\mathfrak{G}}, 0; I, rp \models_{\alpha} F_i$$

pour tout  $i, 1 \leq i \leq m$ , alors

$$\bar{\mathfrak{G}}, 0; I, rp \models_{\alpha} G_i$$

pour tout  $i, 1 \leq i \leq n$ .

## References

- [GL01] Jean Goubault-Larrecq. Langage de spécification de protocoles de EVA: syntaxe abstraite et sémantique. Technical Report EVA-2, LSV/CNRS UMR 8643 & ENS Cachan, July 2001.
- [JLM01] Florent Jacquemard and Daniel Le Métayer. Langage de spécification de protocoles de EVA: syntaxe concrète. Technical Report EVA-1, Trusted Logic S.A., July 2001. Version 3.14.
- [Lam94] Leslie Lamport. The temporal logic of actions. *ACM Transactions on Programming Languages and Systems*, 16(3):872–923, 1994.
- [LS95] François Laroussinie and Philippe Schnoebelen. A hierarchy of temporal logics with past. *Theoretical Computer Science*, 148(2):303–324, 1995.
- [MTH90] Robin Milner, Mads Tofte, and Robert Harper. *The Definition of Standard ML*. MIT Press, 1990.