Proving computational security using Avispa

Véronique Cortier
LORIA, équipe Cassis, Nancy

FormaCrypt, 30 novembre 2007

This work is part of the PhD thesis of Heinrich Hördegen

Objective

Obtaining computational guarantees with an automatic tool Avispa, using existing transfer results

Theorem (Cortier-Kuesters-Kremer-Warinschi)

If a protocol Π *satisfies symbolically a property* ϕ*, then* Π *satisfies the property computationally :*

$$\Pi \models^s \phi \implies \Pi \models^c \phi.$$

Both secrecy and authentication properties can be considered. The cryptographic primitives are :

- Either asymmetric encryption and signatures
- Or asymmetric encryption and hashes (in which case the symbolic secrecy property has to be reinforced).

Approach

Difficulty : The term algebra used in the previous theorem is much richer than the algebra used in Avispa and other existing tools.

→ Proposition of 4 term algebras

→ Transfer of security properties

→ Implementation of the module CryptoSec in Avispa

Term algebras

	Pair $\langle \_ , \_ \rangle$	symmetric encryption $\{\!\|\_\|\!\}_\_$	asymmetric encryption $\{\_\}_\_$	Signatures $hash(\_)$	hash $[\_]_\_$	probabilistic symbols [1]
T^{lhs}	+	+	+	+	+	+
T^{hs}	+	+	+	+	+	−
T^{h}	+	+	+	+	−	−
T	+	+	+	−	−	−

[1] Symb. prob. : $\{\!\|\_\|\!\}^{\sim}_\_$, $\{\_\}^{\sim}_\_$, $[\_]^{\sim}_\_$

Common encoding between term algebra

Protocol specifiers commonly use tricks to encode a protocol of an algebra into a smaller algebra.

- Hash functions : $hash(m) \longrightarrow \{m\}_{\mathsf{dk}(h)}$
- Signatures : $[m]_{\mathsf{sk}(a)} \longrightarrow \{m\}_{\mathsf{dk}(a)}$
- probabilistic primitives :
  Probabilistic symbols $\longrightarrow$ Deterministic symbols

Relating the term algebra (1)

Function $lhs \longrightarrow hs$

We introduce a function $\overline{\cdot}^{lhs \longrightarrow hs} : T^{lhs} \longrightarrow T^{hs}$ *that erases labels.*

$$\overline{\{m\}^{ag(1)}_{ek(a)}}^{lhs \longrightarrow hs} = \{m\}_{ek(a)}$$

Relating the term algebra (1)

Function $lhs \longrightarrow hs$

We introduce a function $\overline{\cdot}^{lhs \longrightarrow hs} : T^{lhs} \longrightarrow T^{hs}$ *that erases labels.*

$$\overline{\{m\}^{\mathsf{ag}(1)}_{\mathsf{ek(a)}}}^{lhs \longrightarrow hs} = \{m\}_{\mathsf{ek}(a)}$$

Function $hs \longrightarrow h$

We introduce a function $\overline{\cdot}^{hs \longrightarrow h} : T^{hs} \longrightarrow T^{h}$ *that replaces signatures with asymmetric encryption with private keys.*

$$\overline{[m]_{\mathsf{sk(a)}}}^{hs \longrightarrow h} = \{m\}_{\mathsf{dk}(a)}$$

Relating the term algebra (2)

Function $h \longrightarrow \_$

We introduce a function $\overline{\cdot}^{h \longrightarrow \_} : T^h \longrightarrow T$ *that replaces hash with asymmetric encryption with the public key of an idle agent* h.

$$\overline{hash(m)}^{h \longrightarrow \_} = \{m\}_{\mathsf{ek}(h)}$$

Four corresponding logics

Logic	Term algebra
$\mathcal{L}_2^{lhs}$	T^{lhs}
$\mathcal{L}_2^{hs}$	T^{hs}
$\mathcal{L}_2^{h}$	T^{h}
$\mathcal{L}_2$	T

Notation : $\mathcal{L}_2^\star$ denotes any of the logic with $\star \in \{lhs, hs, h, \_\}$.

Logics $\mathcal{L}_2^\star$

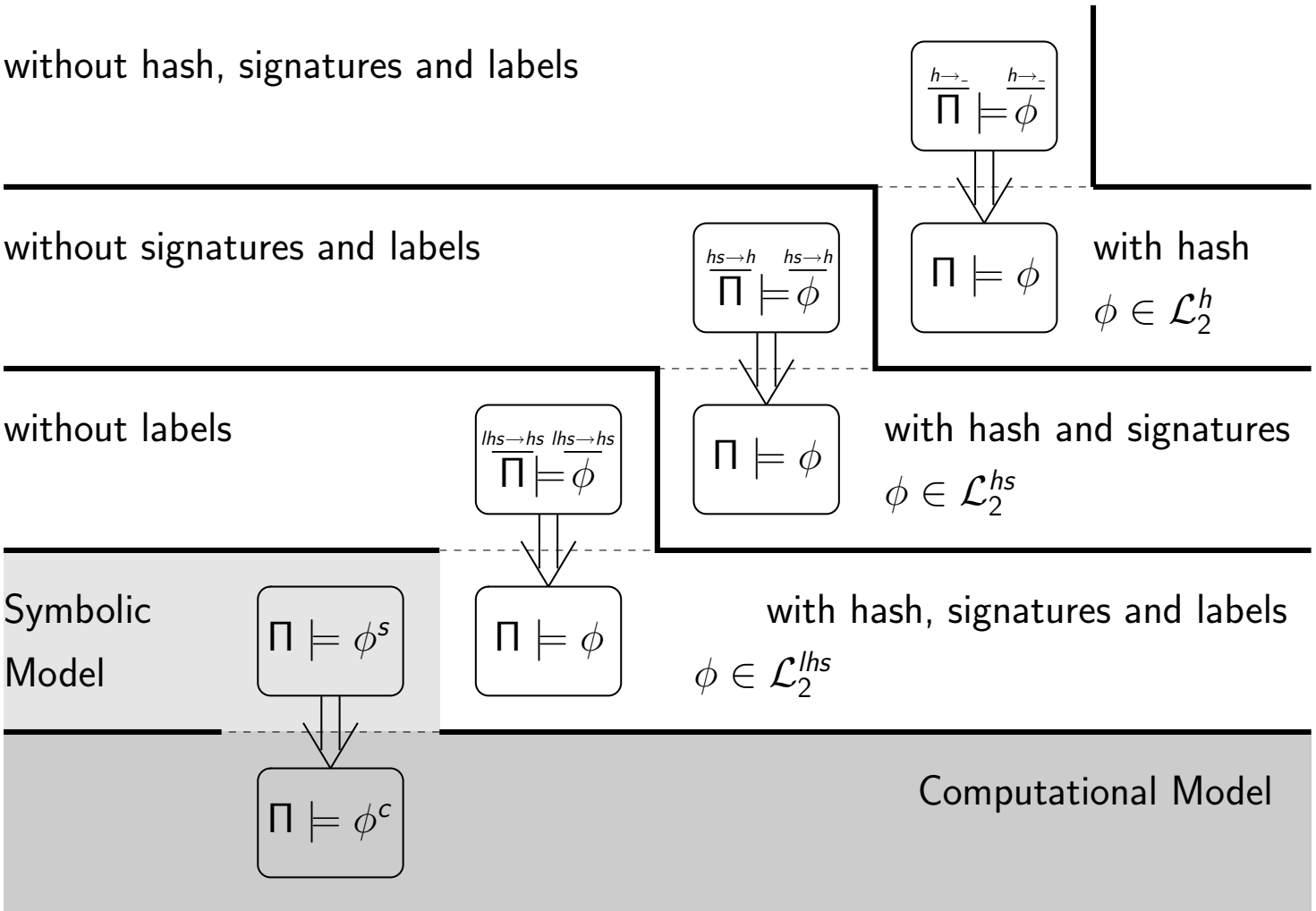
Syntax of formula of $\mathcal{L}_2^\star$

$$F ::= NC(a) \mid \neg NC(a) \mid (u_1 = u_2) \mid (m_1 \neq m_2) \mid F \wedge F \mid F \vee F \mid \forall \mathcal{LS}_{i,p}.\varsigma\ F \mid \exists \mathcal{LS}_{i,p}.\varsigma\ F$$

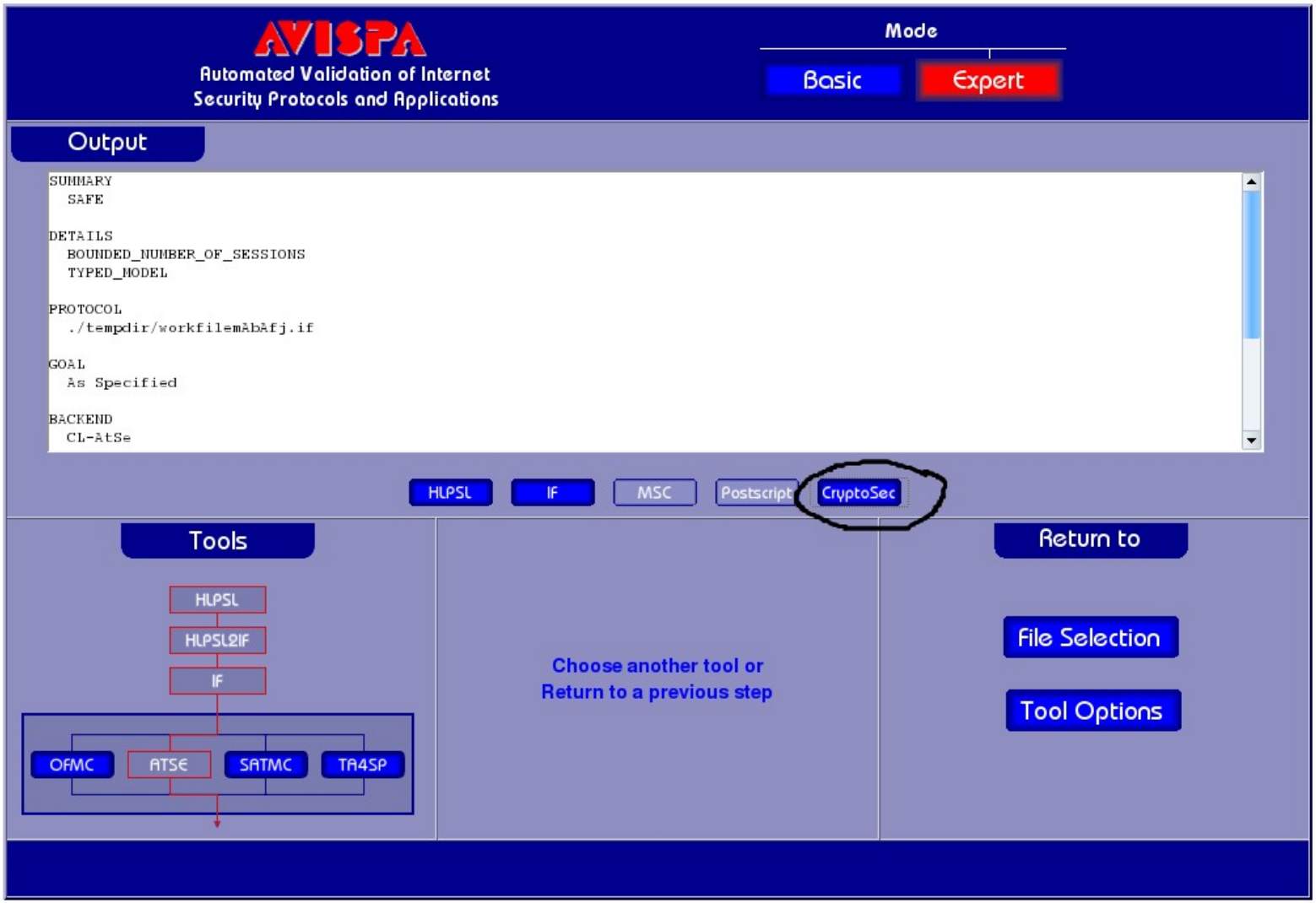
- *NC* predicate that tells whether an agent is corrupted,
- Equality tests only between invariant terms, that is terms that are unchanged by the projection functions
- Two quantification on local states of agents,
- No arbitrary negation.

$\longrightarrow$ Allow usual formulation of secrecy and authentication properties (with authentication on invariant terms).

Transfer Results



Avispa Interface : http ://www.loria.fr/hordegen/



CryptoSec output

```
The following properties
(weak authentication)
FOR ALL SESSIONS s OF ROLE alice AT STEP 2 THERE EXISTS A SESSION s' OF ROLE bob AT STEP 1
(s'(Nb) = s(Nb)) / (s'(B) = s(B)) / (s'(A) = s(A)) /  (s(B) = intruder)
FOR ALL SESSIONS s OF ROLE bob AT STEP 3 THERE EXISTS A SESSION s' OF ROLE alice AT STEP 0
(s'(Na) = s(Na)) / (s'(A) = s(A)) / (s'(B) = s(B)) /  (s(A) = intruder)

(replay protection)
FOR ALL SESSIONS s OF ROLE alice AT STEP 2 FOR ALL SESSIONS s' OF ROLE alice AT STEP 2
 (s(Nb) = s'(Nb))   (s(A) = s'(A))   (s(B) = s'(B))  (s(Session) = s'(Session))  (s(B) =
intruder)
FOR ALL SESSIONS s OF ROLE bob AT STEP 3 FOR ALL SESSIONS s' OF ROLE bob AT STEP 3
 (s(Na) = s'(Na))   (s(B) = s'(B))   (s(A) = s'(A))  (s(Session) = s'(Session))  (s(A) =
intruder)

are guaranteed computationally under the assumption of - an IND-CCA secure encryption scheme, -
hash fonctions in the random oracle model.

See transfer theorem [1] and the translation result of [2].

[1] Cortier, V., Kremer, S., Küsters, R. and Warinschi, B. (2006). Computationally sound
symbolic secrecy in the presence of hash functions. In Proc. 26th Conference on Foundations of
Software Technology and Theoretical Computer Science (FSTTCS'06), volume 4337 of Lecture Notes
in Computer Science, Springer-Verlag.
[2] Cortier, V., Hördegen, H., and Warinschi, B. (2006). Explicit randomness is not necessary
when modeling probabilistic encryption. Technical raport 5928, INRIA.
```

Experiences

The protocols of the AVISPA library have been analyzed.

Total number of protocols in the library	84
with only asymmetric encryption and hashes	12
computationally sound	9