

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

¹Symb. prob. : $\{-\}_-$, $\{-\}_-$, $[-]_-$

Common encoding between term algebra

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

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

Relating the term algebra (1)

Function $lhs \rightarrow hs$

We introduce a function $\frac{lhs \rightarrow hs}{\cdot} : T^{lhs} \rightarrow T^{hs}$ that erases labels.

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

Relating the term algebra (1)

Function $lhs \rightarrow hs$

We introduce a function $\frac{lhs \rightarrow hs}{\cdot} : T^{lhs} \rightarrow T^{hs}$ that erases labels.

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

Function $hs \rightarrow h$

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

$$\frac{hs \rightarrow h}{[m]_{sk(a)}} = \{m\}_{dk(a)}$$

Relating the term algebra (2)

Function $h \rightarrow _$

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

$$\frac{h \rightarrow _}{\text{hash}(m)} = \{m\}_{\text{ek}(h)}$$

Four corresponding logics

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

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

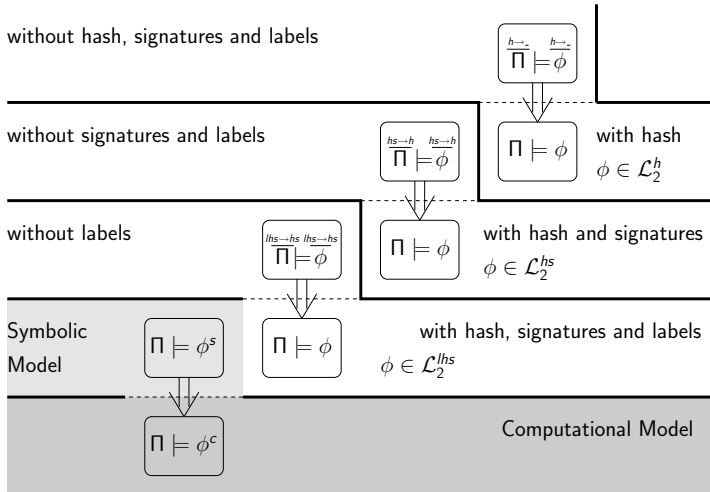
Logics \mathcal{L}_2^* Syntax of formula of \mathcal{L}_2^*

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

- 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.**

→ Allow usual formulation of secrecy and authentication properties (with authentication on invariant terms).

Transfer Results



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

The screenshot displays the Avispa web interface. At the top, the logo "AVISPA" is shown in red, with the text "Automated Validation of Internet Security Protocols and Applications" below it. To the right, there is a "Mode" selector with two buttons: "Basic" (blue) and "Expert" (red). Below this is a large "Output" window containing the following text:

```
SUMMARY
SAFE

DETAILS
BOUNDED_NUMBER_OF_SESSIONS
TYPED_MODEL

PROTOCOL
./tempdir/workfileabafj.if

GOAL
As Specified

BACKGROUND
CL-AtSe
```

Below the output window, there is a row of tool selection buttons: "HLPSP", "IF", "MSC", "Postscript", and "CryptoSec". The "CryptoSec" button is circled in black. To the left of the tool buttons is a "Tools" section with a flowchart showing the sequence of tools used: HLPSP, HLPSP/IF, IF, and then a group containing OMC, ATSE, SATMC, and TRASP. To the right of the tool buttons is a "Return to" section with three buttons: "Return to", "File Selection", and "Tool Options". In the center of the interface, there is a text prompt: "Choose another tool or Return to a previous step".

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 functions 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 report 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