A decision procedure for proving trace equivalence (Work in progress)

V. Cheval, H. Comon-Lundh, S. Delaune

LSV, Project SECSI

10 December 2010

Context

Automatic procedure for proving security properties on protocol

Context

Automatic procedure for proving security properties on protocol

Trace properties

- Examples : simple secret, authentication, . . .
- All traces of a protocol has to satisfy a certain property.
- Lot of previous works on those security properties.
- Tools already exists (example : ProVerif, Maude-NPA,. . .)

Context

Automatic procedure for proving security properties on protocol

Trace properties

- Examples : simple secret, authentication, ...
- All traces of a protocol has to satisfy a certain property.
- Lot of previous works on those security properties.
- Tools already exists (example : ProVerif, Maude-NPA,...)

Equivalence properties

- Examples : strong secret, dictionnary attacks, anonymity, ...
- Express the indistinguishability of two protocols
- Theoretical results (Baudet, Chevalier, Rusinowitch, ...)
- No general tool implemented

Related works

Huttel (2002)

- Only spi-calculus (fixed primitives)
- Untractable implementation (multi-exponential complexity)
- Doesn't handle trace properties.

Cortier, Delaune (2009) + Baudet (2005) or Chevalier,Rusinowitch (2009)

- Bounded number of sessions
- Infinitely many traces are represented by constraint systems
- Observational equivalence of processes $\Leftrightarrow$ symbolic equivalence of constraint systems
- Algorithm for the symbolic equivalence of positive constraint systems when the equational theory is given by a subterm convergent rewriting system.

Related works : ProVerif

Blanchet, Abadi, Fournet (2008)

- Unbounded number of sessions
- Diff-equivalence : Observational equivalence between two process with the same structure but different messages.
- Very efficient
- Possibility of false attacks. Doesn't always terminate

ProVerif extension

ProSwapper (see the talk of Ben Smyth)

Examples

Minimum benchmark

Two examples we want our algorithm to prove :

- Privacy for the Private authentication protocol (Abadi and Fournet, 2004)
- Unlinkability for the E-Passport protocol (Arapinis, Chothia, Ritter and Ryan, CSF 2010)

We'll explain why the existing tools cannot handle them.

Private authentication protocol

Informal representation

$$\begin{array}{lll} 0. & A \longrightarrow B : & \mathsf{aenc}(\langle N_a, \mathsf{p}(A)\rangle, \mathsf{p}(B)) \\ 1. & B \longrightarrow A : & \mathsf{aenc}(\langle N_a, N_b, \mathsf{p}(B)\rangle, \mathsf{p}(A)) \end{array}$$

Role A : $P_A(a, b)$

$\nu N_a.\ \overline{c}\langle \mathsf{aenc}(\langle N_a, \mathsf{p}(a)\rangle, \mathsf{p}(b))\rangle.\ c(x)$

Role B : $P_B(b, a)$

$c(x)$. let $desc = \mathsf{adec}(x, b)$ in
let $n_a = \mathsf{proj}_1(desc)$ and $pub_a = \mathsf{proj}_2(desc)$ in
if $pub_a = \mathsf{p}(a)$
then $\nu N_b.\ \overline{c}\langle \mathsf{aenc}(\langle n_a, N_b, \mathsf{p}(b)\rangle, \mathsf{p}(a))\rangle$
else $\nu K.\ \overline{c}\langle \mathsf{aenc}(K, \mathsf{p}(a))\rangle$

Private authentication protocol

$$\overline{c}\langle \mathsf{p}(a)\rangle.\overline{c}\langle \mathsf{p}(a')\rangle.\overline{c}\langle \mathsf{p}(b)\rangle \mid P_A(a,b) \mid P_B(b,a)$$
$$\approx$$
$$\overline{c}\langle \mathsf{p}(a)\rangle.\overline{c}\langle \mathsf{p}(a')\rangle.\overline{c}\langle \mathsf{p}(b)\rangle \mid P_A(a',b) \mid P_B(b,a')$$

Role A (a,b)	Intruder	Role B (b,a)

Private authentication protocol

$$\overline{c}\langle \mathsf{p}(a)\rangle.\overline{c}\langle \mathsf{p}(a')\rangle.\overline{c}\langle \mathsf{p}(b)\rangle \mid P_A(a,b) \mid P_B(b,a)$$
$$\approx$$
$$\overline{c}\langle \mathsf{p}(a)\rangle.\overline{c}\langle \mathsf{p}(a')\rangle.\overline{c}\langle \mathsf{p}(b)\rangle \mid P_A(a',b) \mid P_B(b,a')$$

Role A (a,b)

Intruder

$M_1 = \mathsf{p}(a)$
$M_2 = \mathsf{p}(a')$
$M_3 = \mathsf{p}(b)$

Role B (b,a)

Private authentication protocol

$$\overline{c}\langle \mathsf{p}(a)\rangle.\overline{c}\langle \mathsf{p}(a')\rangle.\overline{c}\langle \mathsf{p}(b)\rangle \mid P_A(a,b) \mid P_B(b,a)$$
$$\approx$$
$$\overline{c}\langle \mathsf{p}(a)\rangle.\overline{c}\langle \mathsf{p}(a')\rangle.\overline{c}\langle \mathsf{p}(b)\rangle \mid P_A(a',b) \mid P_B(b,a')$$

Role A (a,b)	Intruder	Role B (b,a)
	$M_1 = \mathsf{p}(a)$ $M_2 = \mathsf{p}(a')$ $M_3 = \mathsf{p}(b)$	
$\xrightarrow{\{\langle N_a, \mathsf{p}(a)\rangle\}_{\mathsf{p}(b)}}$		

Private authentication protocol

$$\overline{c}\langle \mathsf{p}(a)\rangle.\overline{c}\langle \mathsf{p}(a')\rangle.\overline{c}\langle \mathsf{p}(b)\rangle \mid P_A(a,b) \mid P_B(b,a)$$
$$\approx$$
$$\overline{c}\langle \mathsf{p}(a)\rangle.\overline{c}\langle \mathsf{p}(a')\rangle.\overline{c}\langle \mathsf{p}(b)\rangle \mid P_A(a',b) \mid P_B(b,a')$$

Role A (a,b)

Intruder

Role B (b,a)

$M_1 = \mathsf{p}(a)$
$M_2 = \mathsf{p}(a')$
$M_3 = \mathsf{p}(b)$

$\xrightarrow{\{\langle N_a, \mathsf{p}(a)\rangle\}_{\mathsf{p}(b)}}$

$\xrightarrow{\{\langle N_i, M_1\rangle\}_{M_3}}$

Private authentication protocol

$$\overline{c}\langle \mathsf{p}(a)\rangle.\overline{c}\langle \mathsf{p}(a')\rangle.\overline{c}\langle \mathsf{p}(b)\rangle \mid P_A(a,b) \mid P_B(b,a)$$
$$\approx$$
$$\overline{c}\langle \mathsf{p}(a)\rangle.\overline{c}\langle \mathsf{p}(a')\rangle.\overline{c}\langle \mathsf{p}(b)\rangle \mid P_A(a',b) \mid P_B(b,a')$$

Role A (a,b)

Intruder

Role B (b,a)

$M_1 = \mathsf{p}(a)$
$M_2 = \mathsf{p}(a')$
$M_3 = \mathsf{p}(b)$

$\xrightarrow{\{\langle N_a, \mathsf{p}(a)\rangle\}_{\mathsf{p}(b)}}$

$\xrightarrow{\{\langle N_i, M_1\rangle\}_{M_3}}$

$x = \{\langle N_i, \mathsf{p}(a)\rangle\}_{\mathsf{p}(b)}$

Private authentication protocol

$$\overline{c}\langle \mathrm{p}(a)\rangle.\overline{c}\langle \mathrm{p}(a')\rangle.\overline{c}\langle \mathrm{p}(b)\rangle \mid P_A(a,b) \mid P_B(b,a)$$
$$\approx$$
$$\overline{c}\langle \mathrm{p}(a)\rangle.\overline{c}\langle \mathrm{p}(a')\rangle.\overline{c}\langle \mathrm{p}(b)\rangle \mid P_A(a',b) \mid P_B(b,a')$$

Role A (a,b)

Intruder

Role B (b,a)

$M_1 = \mathrm{p}(a)$
$M_2 = \mathrm{p}(a')$
$M_3 = \mathrm{p}(b)$

$\xrightarrow{\{\langle N_a, \mathrm{p}(a)\rangle\}_{\mathrm{p}(b)}}$

$\xrightarrow{\{\langle N_i, M_1\rangle\}_{M_3}}$

$x = \{\langle N_i, \mathrm{p}(a)\rangle\}_{\mathrm{p}(b)}$
Verify key succeeds
$\mathrm{p}(a) = \mathrm{p}(a)$

Private authentication protocol

$$\overline{c}\langle \mathsf{p}(a)\rangle.\overline{c}\langle \mathsf{p}(a')\rangle.\overline{c}\langle \mathsf{p}(b)\rangle \mid P_A(a,b) \mid P_B(b,a)$$
$$\approx$$
$$\overline{c}\langle \mathsf{p}(a)\rangle.\overline{c}\langle \mathsf{p}(a')\rangle.\overline{c}\langle \mathsf{p}(b)\rangle \mid P_A(a',b) \mid P_B(b,a')$$

Role A (a,b)

Intruder

Role B (b,a)

$M_1 = \mathsf{p}(a)$
$M_2 = \mathsf{p}(a')$
$M_3 = \mathsf{p}(b)$

$\xrightarrow{\{\langle N_a, \mathsf{p}(a)\rangle\}_{\mathsf{p}(b)}}$

$\xrightarrow{\{\langle N_i, M_1\rangle\}_{M_3}}$

$x = \{\langle N_i, \mathsf{p}(a)\rangle\}_{\mathsf{p}(b)}$
Verify key succeeds
$\mathsf{p}(a) = \mathsf{p}(a)$

$\xleftarrow{\{\langle N_i, N_b, \mathsf{p}(b)\rangle\}_{\mathsf{p}(a)}}$

Private authentication protocol

$$\overline{c}\langle \mathrm{p}(a)\rangle.\overline{c}\langle \mathrm{p}(a')\rangle.\overline{c}\langle \mathrm{p}(b)\rangle \mid P_A(a,b) \mid P_B(b,a)$$
$$\approx$$
$$\overline{c}\langle \mathrm{p}(a)\rangle.\overline{c}\langle \mathrm{p}(a')\rangle.\overline{c}\langle \mathrm{p}(b)\rangle \mid P_A(a',b) \mid P_B(b,a')$$

Role A (a,b)		Intruder		Role B (b,a)
		$M_1 = \mathrm{p}(a)$ $M_2 = \mathrm{p}(a')$ $M_3 = \mathrm{p}(b)$		
	$\xrightarrow{\{\langle N_a, \mathrm{p}(a)\rangle\}_{\mathrm{p}(b)}}$			
			$\xrightarrow{\{\langle N_i, M_1\rangle\}_{M_3}}$	
				$x = \{\langle N_i, \mathrm{p}(a)\rangle\}_{\mathrm{p}(b)}$ Verify key succeeds $\mathrm{p}(a) = \mathrm{p}(a)$
			$\xleftarrow{\{\langle N_i, N_b, \mathrm{p}(b)\rangle\}_{\mathrm{p}(a)}}$	
		$M_4 = \{\langle N_i, N_b, \mathrm{p}(b)\rangle\}_{\mathrm{p}(a)}$		

Private authentication protocol

$$\overline{c}\langle \mathrm{p}(a)\rangle.\overline{c}\langle \mathrm{p}(a')\rangle.\overline{c}\langle \mathrm{p}(b)\rangle \mid P_A(a,b) \mid P_B(b,a)$$
$$\approx$$
$$\overline{c}\langle \mathrm{p}(a)\rangle.\overline{c}\langle \mathrm{p}(a')\rangle.\overline{c}\langle \mathrm{p}(b)\rangle \mid P_A(a',b) \mid P_B(b,a')$$

Role A (a',b)	Intruder	Role B (b,a')

Private authentication protocol

$$\overline{c}\langle \mathsf{p}(a)\rangle.\overline{c}\langle \mathsf{p}(a')\rangle.\overline{c}\langle \mathsf{p}(b)\rangle \mid P_A(a,b) \mid P_B(b,a)$$
$$\approx$$
$$\overline{c}\langle \mathsf{p}(a)\rangle.\overline{c}\langle \mathsf{p}(a')\rangle.\overline{c}\langle \mathsf{p}(b)\rangle \mid P_A(a',b) \mid P_B(b,a')$$

Role A	Intruder	Role B
(a',b)		(b,a')
	$M_1 = \mathsf{p}(a)$	
	$M_2 = \mathsf{p}(a')$	
	$M_3 = \mathsf{p}(b)$	

Private authentication protocol

$$\overline{c}\langle \mathsf{p}(a)\rangle.\overline{c}\langle \mathsf{p}(a')\rangle.\overline{c}\langle \mathsf{p}(b)\rangle \mid P_A(a,b) \mid P_B(b,a)$$
$$\approx$$
$$\overline{c}\langle \mathsf{p}(a)\rangle.\overline{c}\langle \mathsf{p}(a')\rangle.\overline{c}\langle \mathsf{p}(b)\rangle \mid P_A(a',b) \mid P_B(b,a')$$

Role A (a',b)

Intruder

Role B (b,a')

$M_1 = \mathsf{p}(a)$
$M_2 = \mathsf{p}(a')$
$M_3 = \mathsf{p}(b)$

$\xrightarrow{\{\langle N_a, \mathsf{p}(a')\rangle\}_{\mathsf{p}(b)}}$

Private authentication protocol

$$\overline{c}\langle \mathsf{p}(a)\rangle.\overline{c}\langle \mathsf{p}(a')\rangle.\overline{c}\langle \mathsf{p}(b)\rangle \mid P_A(a,b) \mid P_B(b,a)$$
$$\approx$$
$$\overline{c}\langle \mathsf{p}(a)\rangle.\overline{c}\langle \mathsf{p}(a')\rangle.\overline{c}\langle \mathsf{p}(b)\rangle \mid P_A(a',b) \mid P_B(b,a')$$

Role A (a',b)	Intruder	Role B (b,a')
	$M_1 = \mathsf{p}(a)$ $M_2 = \mathsf{p}(a')$ $M_3 = \mathsf{p}(b)$	

$\xrightarrow{\{\langle N_a, \mathsf{p}(a')\rangle\}_{\mathsf{p}(b)}}$

$\xrightarrow{\{\langle N_i, M_1\rangle\}_{M_3}}$

Private authentication protocol

$$\overline{c}\langle \mathrm{p}(a)\rangle.\overline{c}\langle \mathrm{p}(a')\rangle.\overline{c}\langle \mathrm{p}(b)\rangle \mid P_A(a,b) \mid P_B(b,a)$$
$$\approx$$
$$\overline{c}\langle \mathrm{p}(a)\rangle.\overline{c}\langle \mathrm{p}(a')\rangle.\overline{c}\langle \mathrm{p}(b)\rangle \mid P_A(a',b) \mid P_B(b,a')$$

Role A (a',b) | Intruder | Role B (b,a')

$$M_1 = \mathrm{p}(a)$$
$$M_2 = \mathrm{p}(a')$$
$$M_3 = \mathrm{p}(b)$$

$\xrightarrow{\{\langle N_a, \mathrm{p}(a')\rangle\}_{\mathrm{p}(b)}}$

$\xrightarrow{\{\langle N_i, M_1\rangle\}_{M_3}}$

$$x = \{\langle N_i, \mathrm{p}(a)\rangle\}_{\mathrm{p}(b)}$$

Private authentication protocol

$$\overline{c}\langle \mathsf{p}(a)\rangle.\overline{c}\langle \mathsf{p}(a')\rangle.\overline{c}\langle \mathsf{p}(b)\rangle \mid P_A(a,b) \mid P_B(b,a)$$
$$\approx$$
$$\overline{c}\langle \mathsf{p}(a)\rangle.\overline{c}\langle \mathsf{p}(a')\rangle.\overline{c}\langle \mathsf{p}(b)\rangle \mid P_A(a',b) \mid P_B(b,a')$$

Role A (a',b)	Intruder	Role B (b,a')
	$M_1 = \mathsf{p}(a)$ $M_2 = \mathsf{p}(a')$ $M_3 = \mathsf{p}(b)$	
$\xrightarrow{\{\langle N_a, \mathsf{p}(a')\rangle\}_{\mathsf{p}(b)}}$		
	$\xrightarrow{\{\langle N_i, M_1\rangle\}_{M_3}}$	
		$x = \{\langle N_i, \mathsf{p}(a)\rangle\}_{\mathsf{p}(b)}$ Verify key fails $\mathsf{p}(a) \neq \mathsf{p}(a')$

Private authentication protocol

$$\overline{c}\langle \mathrm{p}(a)\rangle.\overline{c}\langle \mathrm{p}(a')\rangle.\overline{c}\langle \mathrm{p}(b)\rangle \mid P_A(a,b) \mid P_B(b,a)$$
$$\approx$$
$$\overline{c}\langle \mathrm{p}(a)\rangle.\overline{c}\langle \mathrm{p}(a')\rangle.\overline{c}\langle \mathrm{p}(b)\rangle \mid P_A(a',b) \mid P_B(b,a')$$

Role A (a',b)	Intruder	Role B (b,a')
	$M_1 = \mathrm{p}(a)$ $M_2 = \mathrm{p}(a')$ $M_3 = \mathrm{p}(b)$	
$\xrightarrow{\{\langle N_a, \mathrm{p}(a')\rangle\}_{\mathrm{p}(b)}}$		
	$\xrightarrow{\{\langle N_i, M_1\rangle\}_{M_3}}$	
		$x = \{\langle N_i, \mathrm{p}(a)\rangle\}_{\mathrm{p}(b)}$ Verify key fails $\mathrm{p}(a) \neq \mathrm{p}(a')$
	$\xleftarrow{\{K\}_{\mathrm{p}(a)}}$	

Private authentication protocol

$$\overline{c}\langle \mathsf{p}(a)\rangle.\overline{c}\langle \mathsf{p}(a')\rangle.\overline{c}\langle \mathsf{p}(b)\rangle \mid P_A(a,b) \mid P_B(b,a)$$
$$\approx$$
$$\overline{c}\langle \mathsf{p}(a)\rangle.\overline{c}\langle \mathsf{p}(a')\rangle.\overline{c}\langle \mathsf{p}(b)\rangle \mid P_A(a',b) \mid P_B(b,a')$$

Role A (a',b)		Intruder		Role B (b,a')
		$M_1 = \mathsf{p}(a)$ $M_2 = \mathsf{p}(a')$ $M_3 = \mathsf{p}(b)$		
	$\xrightarrow{\{\langle N_a, \mathsf{p}(a')\rangle\}_{\mathsf{p}(b)}}$			
			$\xrightarrow{\{\langle N_i, M_1\rangle\}_{M_3}}$	
				$x = \{\langle N_i, \mathsf{p}(a)\rangle\}_{\mathsf{p}(b)}$ Verify key fails $\mathsf{p}(a) \neq \mathsf{p}(a')$
			$\xleftarrow{\{K\}_{\mathsf{p}(a)}}$	
		$M_4 = \{K\}_{\mathsf{p}(a)}$		

Private authentication protocol : related works

Theoretical works

- Cannot be applied since there is some else branches.
- If the else branches are removed, there is an attack (Cortier, Delaune (2009))

ProVerif

- ProVerif accepts else branch;
- but this example doesn't satisfy the diff-equivalence.

E-Passport protocol : description

Passport (ke, km)		Reader
	$\xrightarrow{ke, km}_{\text{priv}}$	
	$\xleftarrow{Get\_C}$	
N_T		
	$\xrightarrow{N_T}$	
		N_R, K_R $E_1 = \{N_R, N_T, K_R\}_{ke}$ $M_1 = MAC_{km}(E_1)$
	$\xleftarrow{E_1, M_1}$	
Verify Mac (Error 6300) Verify N_T (Error 6A80) K_T $E_2 = \{N_T, N_R, K_T\}_{ke}$ $M_2 = MAC_{km}(E_2)$		
	$\xrightarrow{E_2, M_2}$	
		Verify Mac, Verify N_R

Unlinkability

An attacker cannot identify particular sessions which involved the same principal

Unlinkability

Unlinkability

An attacker cannot identify particular sessions which involved the same principal

Formally (Arapinis, Chothia, Ritter and Ryan, CSF 2010)

$$!Reader \mid !\nu ke.\ \nu km.!Pass(ke, km)$$
$$\approx$$
$$!Reader \mid !\nu ke.\ \nu km.Pass(ke, km)$$

$!Reader \mid !\nu ke.\ \nu km.!Pass(ke, km) \approx !Reader \mid !\nu ke.\ \nu km.Pass(ke, km)$

Intruder		Passport (ke, km)		Reader (ke, km)
			$\xleftarrow{Get\_C}$	
		N_T		
			$\xrightarrow{N_T}$	
				N_R, K_R $E_1 = \{N_R, N_T, K_R\}_{ke}$ $M_1 = MAC_{km}(E_1)$
			$\xleftarrow{E_1, M_1}$	
		$\vdots$		
	$\xrightarrow{Get\_C}$			
		N'_T		
	$\xleftarrow{N'_T}$			
Reply third msg	$\xrightarrow{E_1, M_1}$			
		Verify Mac succeeds Verify N'_T fails		
	$\xleftarrow{6A80}$			

E-Passport protocol : the attack

$!Reader \mid !\nu ke.\ \nu km.!Pass(ke, km) \approx !Reader \mid !\nu ke.\ \nu km.Pass(ke, km)$

Intruder		Passport (ke, km)		Reader (ke, km)
			$\xleftarrow{Get\_C}$	
		N_T		
			$\xrightarrow{N_T}$	
				N_R, K_R $E_1 = \{N_R, N_T, K_R\}_{ke}$ $M_1 = MAC_{km}(E_1)$
			$\xleftarrow{E_1, M_1}$	
		⋮		
		Passport (ke', km')		
	$\xrightarrow{Get\_C}$			
		N'_T		
	$\xleftarrow{N'_T}$			
Reply third msg	$\xrightarrow{E_1, M_1}$			
		Verify Mac fails		
	$\xleftarrow{6300}$			

E-Passport protocol : related works

Theoretical works

Cannot be applied since there is some else branches.

ProVerif

The example doesn't satisfy the diff-equivalence

Algorithm

Algorithm

Previous work : IJCAR '10

- Algorithm for proving the symbolic equivalence of couples of constraint systems
- Implemented and efficient
- Can be used for proving the trace equivalence of simple processes without else-branch : Cortier, Delaune (2009)

Work in progress

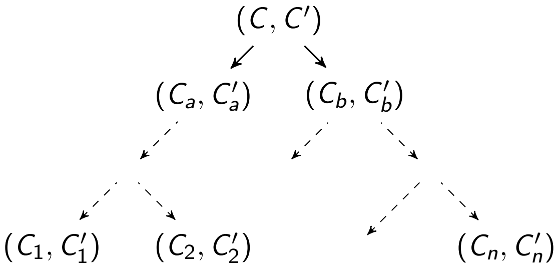
- Algorithm for proving the symbolic equivalence of constraint systems sets with disequation
- Extension to trace equivalence for a class of protocol including E-Passport and Private authentication protocol

- Set of rules.
- Each rule takes a couple of constraint system as input
- Each rule creates two couples of constraint system as output

$$
\begin{array}{ccc}
 & (C, C') & \\
\swarrow & & \searrow \\
(C_a, C'_a) & & (C_b, C'_b)
\end{array}
$$

IJCAR '10

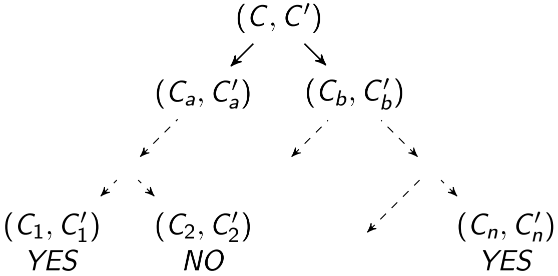
- Set of rules.
- Each rule takes a couple of constraint system as input
- Each rule creates two couples of constraint system as output



The application of the rules creates a binary tree where each node is a couple of constraint systems.

IJCAR '10

- Set of rules.
- Each rule takes a couple of constraint system as input
- Each rule creates two couples of constraint system as output



The application of the rules creates a binary tree where each node is a couple of constraint systems.

Symbolic equivalence of constraint systems sets

- We modified the rules such that they take a couple of constraint systems sets as input and output.
- We added some rules to deal with disequations.

The application of the rules creates a binary tree where each node is a couple of constraint systems sets.

The algorithm is implemented and is efficient but the proof isn't done yet

Trace equivalence of protocols

- Reduce the problem of trace equivalence of protocols to the problem of symbolic equivalence of constraint systems sets
- An algorithm is implemented and works with the Private authentication and E-Passport protocols;
- but it's not efficient : optimizations are needed
- No proof yet

Conclusion

- An algorithm for deciding trace equivalence has been implemented using the rules described in IJCAR '10
- First tool to work on both Private authentication protocol and E-Passport protocol
- Not efficient enough
- Lot of proofs are missing