A decision procedure for proving symbolic equivalence

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

LSV, ENS Cachan, CNRS, INRIA, France

19 July 2010

Example

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

Example

$$
\begin{array}{lll}
0. & A \longrightarrow B : & \{\langle N_a, \mathrm{pk}(sk_a)\rangle\}_{\mathrm{pk}(sk_b)} \\
1. & B \longrightarrow A : & \{\langle N_a, \langle N_b, \mathrm{pk}(sk_b)\rangle\rangle\}_{\mathrm{pk}(sk_a)}
\end{array}
$$

Security property : Anonymity

The identity of the principal A cannot be revealed to the attacker.

Example

$$
\begin{array}{lll}
0. & A \longrightarrow B : & \{\langle N_a, \mathrm{pk}(sk_a)\rangle\}_{\mathrm{pk}(sk_b)} \\
1. & B \longrightarrow A : & \{\langle N_a, \langle N_b, \mathrm{pk}(sk_b)\rangle\rangle\}_{\mathrm{pk}(sk_a)}
\end{array}
$$

Security property : Anonymity

The identity of the principal A cannot be revealed to the attacker.

Formally

$$
c(\mathrm{pk}(sk_a)).c(\mathrm{pk}(sk_{a'})).c(\mathrm{pk}(sk_b)) \mid P_A(a, b) \mid P_B(b, a)
$$

$$
\approx
$$

$$
c(\mathrm{pk}(sk_a)).c(\mathrm{pk}(sk_{a'})).c(\mathrm{pk}(sk_b)) \mid P_A(a', b) \mid P_B(b, a')
$$

Goal

Automatic procedure to prove equivalence properties

Previous works

- Huttel (2002)
- Blanchet, Abadi, Fournet (2008) : ProVerif
- Cortier, Delaune (2009) + Baudet (2005)
- Chevalier,Rusinowitch (2009)
- ...

Dolev-Yao

Rewrite rules

- $\mathsf{dec}(\mathsf{enc}(x, y), y) \to x$
- $\mathsf{adec}(\mathsf{aenc}(x, \mathsf{pk}(y)), y) \to x$
- $\mathsf{check}(\mathsf{sign}(x, y), \mathsf{pk}(y)) \to x$
- $\pi_1(\langle x, y \rangle) \to x$ and $\pi_2(\langle x, y \rangle) \to y$

Constraint system

$$
\begin{array}{lll}
0. & A \longrightarrow B : & \{\langle N_a, \mathrm{pk}(sk_a)\rangle\}_{\mathrm{pk}(sk_b)} \\
1. & B \longrightarrow A : & \{\langle N_a, \langle N_b, \mathrm{pk}(sk_b)\rangle\rangle\}_{\mathrm{pk}(sk_a)}
\end{array}
$$

Constraint system

$$
\begin{array}{lll}
0. & A \longrightarrow B : & \{\langle N_a, \mathrm{pk}(sk_a)\rangle\}_{\mathrm{pk}(sk_b)} \\
1. & B \longrightarrow A : & \{\langle N_a, \langle N_b, \mathrm{pk}(sk_b)\rangle\rangle\}_{\mathrm{pk}(sk_a)}
\end{array}
$$

For each interleaving, one constraint system.

Constraint System :

$$
\begin{array}{l}
\mathrm{pk}(k_a), \mathrm{pk}(k_b), \{\langle n_a, \mathrm{pk}(k_a)\rangle\}_{\mathrm{pk}(k_{\boldsymbol{b}})} \vdash \{\langle x, y\rangle\}_{\mathrm{pk}(k_{\boldsymbol{b}})} \\
\mathrm{pk}(k_a), \mathrm{pk}(k_b), \{\langle n_a, \mathrm{pk}(k_a)\rangle\}_{\mathrm{pk}(k_{\boldsymbol{b}})}, \{\langle x, n_b, \mathrm{pk}(k_b)\rangle\}_y \vdash \{\langle n_a, z, \mathrm{pk}(k_b)\rangle\}_{\mathrm{pk}(k_{\boldsymbol{a}})}
\end{array}
$$

Solution of a constraint system

$$\mathsf{pk}(k_a),\ \mathsf{pk}(k_b),\ \{\langle n_a, \mathsf{pk}(k_a)\rangle\}_{\mathsf{pk}(k_{\boldsymbol{b}})} \vdash \{\langle x, y\rangle\}_{\mathsf{pk}(k_{\boldsymbol{b}})}$$

$$\mathsf{pk}(k_a),\ \mathsf{pk}(k_b),\ \{\langle n_a, \mathsf{pk}(k_a)\rangle\}_{\mathsf{pk}(k_{\boldsymbol{b}})},\ \{\langle x, n_b, \mathsf{pk}(k_b)\rangle\}_y \vdash \{\langle n_a, z, \mathsf{pk}(k_b)\rangle\}_{\mathsf{pk}(k_{\boldsymbol{a}})}$$

Solution of a constraint system

$$
\begin{array}{lccccc}
 & ax_1 & ax_2 & ax_3 & ax_4 & \\
X_1 & \mathsf{pk}(k_a), & \mathsf{pk}(k_b), & \{\langle n_a, \mathsf{pk}(k_a)\rangle\}_{\mathsf{pk}(k_b)} & & \vdash \{\langle x, y\rangle\}_{\mathsf{pk}(k_b)} \\
X_2 & \mathsf{pk}(k_a), & \mathsf{pk}(k_b), & \{\langle n_a, \mathsf{pk}(k_a)\rangle\}_{\mathsf{pk}(k_b)}, & \{\langle x, n_b, \mathsf{pk}(k_b)\rangle\}_y & \vdash \{\langle n_a, z, \mathsf{pk}(k_b)\rangle\}_{\mathsf{pk}(k_a)}
\end{array}
$$

A solution

- $\sigma = \{x \mapsto n_a \ ; \ y \mapsto \mathsf{pk}(k_a) \ ; \ z \mapsto n_b\}$, and
- $\theta = \{X_1 \mapsto ax_3 \ ; \ X_2 \mapsto ax_4\}$.

Static equivalence

Static equivalence : $\phi \sim \phi'$

Given two sequences of terms ϕ, ϕ', the intruder cannot distinguish them.

- $\forall (\xi, \xi') \in \Pi^2, \xi\phi\downarrow = \xi'\phi\downarrow \Leftrightarrow \xi\phi'\downarrow = \xi'\phi'\downarrow$
- $\forall \xi \in \Pi, \xi\phi\downarrow$ is a message $\Leftrightarrow \xi\phi'\downarrow$ is a message

Static equivalence

Static equivalence : $\phi \sim \phi'$

Given two sequences of terms ϕ, ϕ', the intruder cannot distinguish them.

- $\forall (\xi, \xi') \in \Pi^2, \xi\phi\downarrow = \xi'\phi\downarrow \Leftrightarrow \xi\phi'\downarrow = \xi'\phi'\downarrow$
- $\forall \xi \in \Pi, \xi\phi\downarrow$ is a message $\Leftrightarrow \xi\phi'\downarrow$ is a message

Example 1

- $\phi_1 = a,\ \{a\}_b,\ b$
- $\phi_2 = a,\ \{c\}_b,\ b$

Static equivalence

Static equivalence : $\phi \sim \phi'$

Given two sequences of terms ϕ, ϕ', the intruder cannot distinguish them.

- $\forall (\xi, \xi') \in \Pi^2, \xi\phi\downarrow = \xi'\phi\downarrow \Leftrightarrow \xi\phi'\downarrow = \xi'\phi'\downarrow$
- $\forall \xi \in \Pi, \xi\phi\downarrow$ is a message $\Leftrightarrow \xi\phi'\downarrow$ is a message

Example 1 : Non-equivalent

- $\phi_1 = a,\ \{a\}_b,\ b$ $\quad \mathrm{dec}(ax_2, ax_3)\phi_1\downarrow = a = ax_1\phi_1\downarrow$
- $\phi_2 = a,\ \{c\}_b,\ b$ $\quad \mathrm{dec}(ax_2, ax_3)\phi_2\downarrow = c \neq ax_1\phi_2\downarrow$

Static equivalence

Static equivalence : $\phi \sim \phi'$

Given two sequences of terms ϕ, ϕ', the intruder cannot distinguish them.

- $\forall (\xi, \xi') \in \Pi^2, \xi\phi\downarrow = \xi'\phi\downarrow \Leftrightarrow \xi\phi'\downarrow = \xi'\phi'\downarrow$
- $\forall \xi \in \Pi, \xi\phi\downarrow$ is a message $\Leftrightarrow \xi\phi'\downarrow$ is a message

Example 1 : Non-equivalent

- $\phi_1 = a,\ \{a\}_b,\ b \qquad \mathrm{dec}(ax_2, ax_3)\phi_1\downarrow = a = ax_1\phi_1\downarrow$
- $\phi_2 = a,\ \{c\}_b,\ b \qquad \mathrm{dec}(ax_2, ax_3)\phi_2\downarrow = c \neq ax_1\phi_2\downarrow$

Example 2 :

- $\phi_1 = a,\ \{a\}_b$
- $\phi_2 = a,\ \{c\}_b$

Static equivalence

Static equivalence : $\phi \sim \phi'$

Given two sequences of terms ϕ, ϕ', the intruder cannot distinguish them.

- $\forall (\xi, \xi') \in \Pi^2, \xi\phi\downarrow = \xi'\phi\downarrow \Leftrightarrow \xi\phi'\downarrow = \xi'\phi'\downarrow$
- $\forall \xi \in \Pi, \xi\phi\downarrow$ is a message $\Leftrightarrow \xi\phi'\downarrow$ is a message

Example 1 : Non-equivalent

- $\phi_1 = a,\ \{a\}_b,\ b \qquad \mathrm{dec}(ax_2, ax_3)\phi_1\downarrow = a = ax_1\phi_1\downarrow$
- $\phi_2 = a,\ \{c\}_b,\ b \qquad \mathrm{dec}(ax_2, ax_3)\phi_2\downarrow = c \neq ax_1\phi_2\downarrow$

Example 2 : Equivalent

- $\phi_1 = a,\ \{a\}_b$
- $\phi_2 = a,\ \{c\}_b$

Symbolic equivalence

$C \approx_s C'$

Two constraint system C and C' are in symbolic equivalence iff :

- for all $(\theta, \sigma) \in \mathrm{Sol}(C)$,there exists σ' such that $(\theta, \sigma') \in \mathrm{Sol}(C')$ and $\phi\sigma \sim \phi'\sigma'$
- for all $(\theta, \sigma') \in \mathrm{Sol}(C')$, there exists σ such that $(\theta, \sigma) \in \mathrm{Sol}(C)$, and $\phi\sigma \sim \phi'\sigma'$

Example 1

$$\begin{array}{ll} a, b & \vdash x \\ a, b, \{x\}_k & \vdash \{a\}_k \end{array}$$

$$\begin{array}{ll} a, b & \vdash x \\ a, b, \{a\}_k & \vdash \{a\}_k \end{array}$$

Example 1

$$\begin{array}{ll} a, b & \vdash x \\ a, b, \{x\}_k & \vdash \{a\}_k \end{array}$$

$$\begin{array}{ll} a, b & \vdash x \\ a, b, \{a\}_k & \vdash \{a\}_k \end{array}$$

Non-equivalent

The substitution $\theta = \{X_1 \mapsto ax_2,\ X_2 \mapsto ax_3\}$ is only a solution for the second constraint system with $\sigma = \{x \mapsto b\}$, and

Example 2

$$\begin{array}{ll} \{n_a\}_k, & \vdash \{x\}_k \\ \{n_a\}_k,\ \{f(x)\}_k,\ k & \vdash \{f(n_a)\}_k \end{array}$$

$$\begin{array}{ll} \{n_a\}_k, & \vdash \{x\}_k \\ \{n_a\}_k,\ \{f(x)\}_k,\ k' & \vdash \{f(n_a)\}_k \end{array}$$

Example 2

$$\begin{array}{ll} \{n_a\}_k, & \vdash \{x\}_k \\ \{n_a\}_k,\ \{f(x)\}_k,\ k & \vdash \{f(n_a)\}_k \end{array}$$

$$\begin{array}{ll} \{n_a\}_k, & \vdash \{x\}_k \\ \{n_a\}_k,\ \{f(x)\}_k,\ k' & \vdash \{f(n_a)\}_k \end{array}$$

Non-equivalent

- A solution : $\sigma = \sigma' = \{x \mapsto n_a\}$, and $\theta = \{X_1 \mapsto ax_1,\ X_2 \mapsto ax_2\}$
- $\phi\sigma \not\sim \phi'\sigma' : \xi = f(\mathsf{dec}(ax_1, ax_3)), \xi' = \mathsf{dec}(ax_2, ax_3)$

General idea

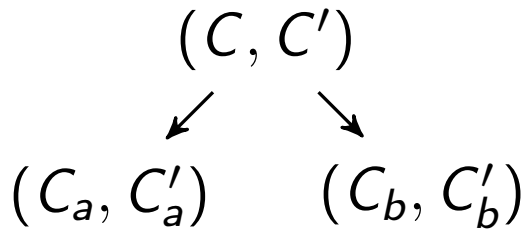
- Input : two constraint systems : C and C'
- Problem : is $C \approx_s C'$?
- Reduce the problem to a finite conjunction of constraint systems equivalence :

$$C_1 \approx_s C'_1 \wedge \ldots \wedge C_n \approx_s C'_n$$

- Decidability of each $C_i \approx_s C'_i$ has to be trivial

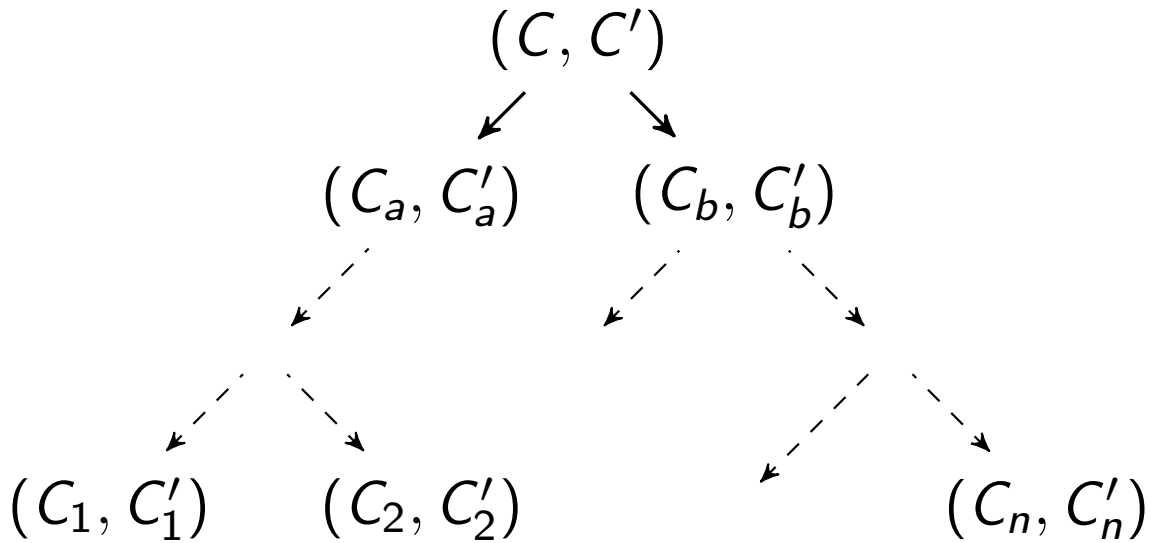
The algorithm

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



The algorithm

- 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.

Main result

Theorem

Our set of rules is :

- complete,
- sound
- and terminates

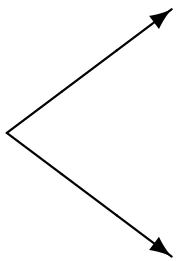
for the problem of deciding the symbolic equivalence of constraint systems.

Implementation

`www.lsv.ens-cachan.fr/~cheval/programs/index.php`

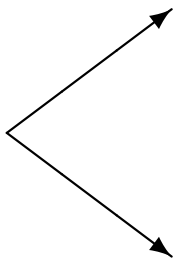
Example 1

$$\begin{cases} a,\ b \vdash \{a\}_b \\ c,\ d \vdash \{x\}_c \end{cases}$$



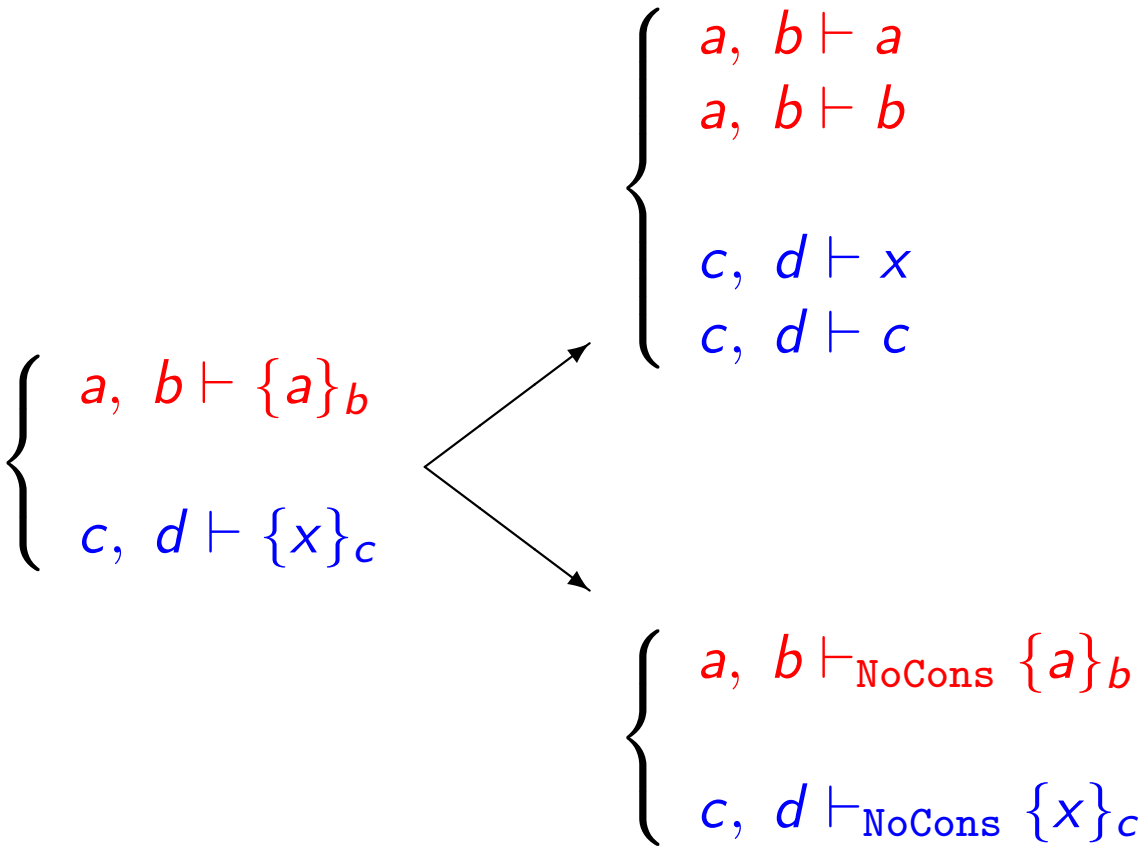
Example 1

$$\left\{\begin{array}{l} a,\ b \vdash \{a\}_b \\ \\ c,\ d \vdash \{x\}_c \end{array}\right.$$



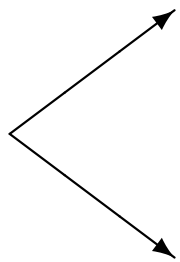
$$\left\{\begin{array}{l} a,\ b \vdash a \\ a,\ b \vdash b \\ \\ c,\ d \vdash x \\ c,\ d \vdash c \end{array}\right.$$

Example 1


$\left\{ \begin{array}{l} a,\ b \vdash \{a\}_b \\ \\ c,\ d \vdash \{x\}_c \end{array} \right.$
$\left\{ \begin{array}{l} a,\ b \vdash a \\ a,\ b \vdash b \\ \\ c,\ d \vdash x \\ c,\ d \vdash c \end{array} \right.$
$\left\{ \begin{array}{l} a,\ b \vdash_{\texttt{NoCons}} \{a\}_b \\ \\ c,\ d \vdash_{\texttt{NoCons}} \{x\}_c \end{array} \right.$

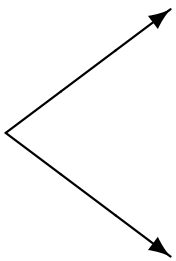
Example 2

$$\begin{cases} a,\ b \vdash \{a\}_b \\ c,\ d \vdash c \end{cases}$$



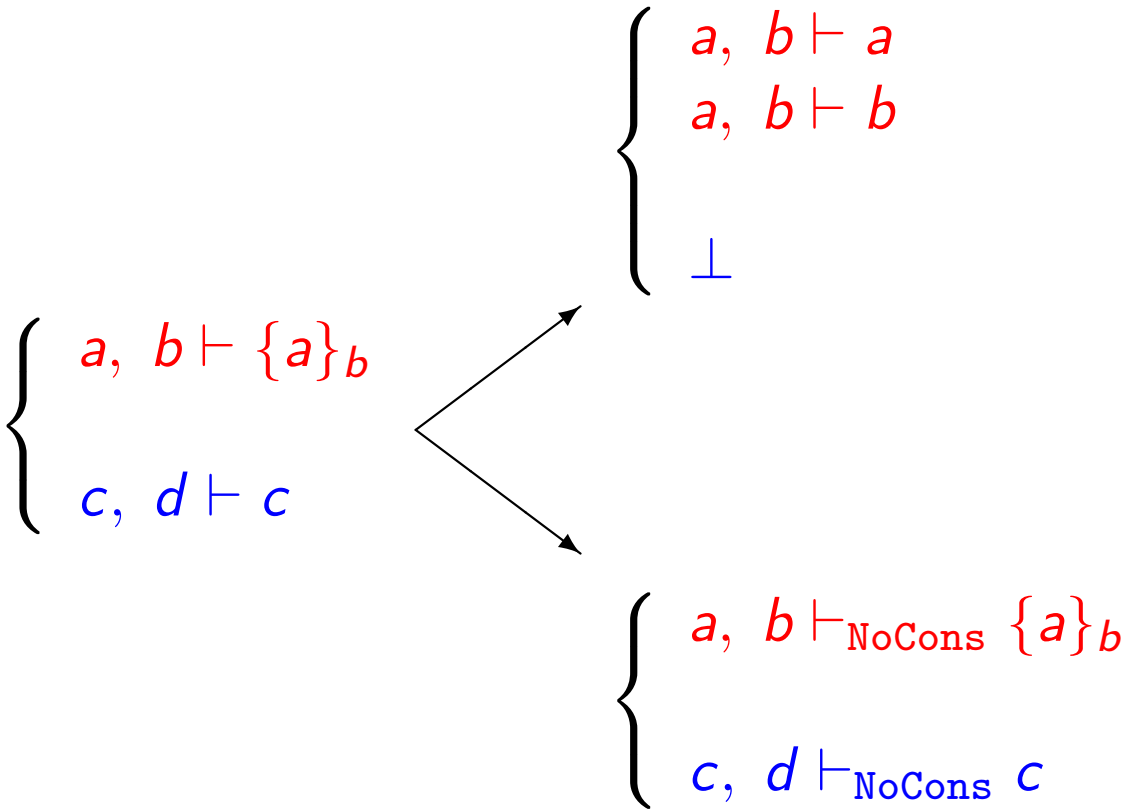
Example 2

$$\left\{ \begin{array}{l} a,\ b \vdash \{a\}_b \\ \\ c,\ d \vdash c \end{array} \right.$$



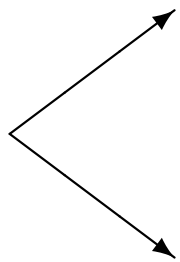
$$\left\{ \begin{array}{l} a,\ b \vdash a \\ a,\ b \vdash b \\ \\ \\ \bot \end{array} \right.$$

Example 2


$a,\ b \vdash \{a\}_b$
$c,\ d \vdash c$
$a,\ b \vdash a$
$a,\ b \vdash b$
$\bot$
$a,\ b \vdash_{\texttt{NoCons}} \{a\}_b$
$c,\ d \vdash_{\texttt{NoCons}} c$

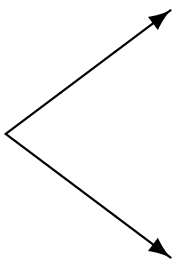
Example 3

$$\begin{cases} a,\ b \vdash \{a\}_b \\ c,\ d \vdash x \end{cases}$$



Example 3

$$\left\{\begin{array}{l} a,\ b \vdash \{a\}_b \\ \\ c,\ d \vdash x \end{array}\right.$$



$$\left\{\begin{array}{l} a,\ b \vdash a \\ a,\ b \vdash b \\ \\ c,\ d \vdash x_1 \\ c,\ d \vdash x_2 \\ x = \{x_1\}_{x_2} \end{array}\right.$$

Example 3

$$\left\{\begin{array}{l} a,\ b \vdash \{a\}_b \\ \\ c,\ d \vdash x \end{array}\right.$$

$$\left\{\begin{array}{l} a,\ b \vdash a \\ a,\ b \vdash b \\ \\ c,\ d \vdash x_1 \\ c,\ d \vdash x_2 \\ x = \{x_1\}_{x_2} \end{array}\right.$$

$$\left\{\begin{array}{l} a,\ b \vdash_{\texttt{NoCons}} \{a\}_b \\ \\ c,\ d \vdash_{\texttt{NoCons}} x \end{array}\right.$$

Termination problem

$$\begin{cases} a & \vdash & \{x_1\}_{x_2} \\ a, b & \vdash & x_1 \end{cases}$$

$$\begin{cases} a & \vdash & y_1 \\ a, b & \vdash & \{y_1\}_{y_2} \end{cases}$$

$\longrightarrow$

$$\begin{cases} a & \vdash & x_1 \\ a & \vdash & x_2 \\ a, b & \vdash & x_1 \end{cases}$$

$$\begin{cases} a & \vdash & z_1 \\ a & \vdash & z_2 \\ a, b & \vdash & \{\{z_1\}_{z_2}\}_{y_2} \end{cases}$$

with $y_1 \stackrel{?}{=} \{z_1\}_{z_2}$

Termination problem

$$\begin{cases} a & \vdash & x_1 \\ a & \vdash & x_2 \\ a, b & \vdash & x_1 \end{cases}$$

$$\begin{cases} a & \vdash & z_1 \\ a & \vdash & z_2 \\ a, b & \vdash & \{\{z_1\}_{z_2}\}_{y_2} \end{cases}$$
with $y_1 \stackrel{?}{=} \{z_1\}_{z_2}$

$\longrightarrow$

$$\begin{cases} a & \vdash & \{t_1\}_{t_2} \\ a & \vdash & x_2 \\ a, b & \vdash & t_1 \\ a, b & \vdash & t_2 \end{cases}$$
with $x_1 \stackrel{?}{=} \{t_1\}_{t_2}$

$$\begin{cases} a & \vdash & z_1 \\ a & \vdash & z_2 \\ a, b & \vdash & \{z_1\}_{z_2} \\ a, b & \vdash & y_2 \end{cases}$$
with $y_1 \stackrel{?}{=} \{z_1\}_{z_2}$

Termination problem

$$\begin{cases} a & \vdash & \{x_1\}_{x_2} \\ a, b & \vdash & x_1 \end{cases}$$

$$\begin{cases} a & \vdash & \{t_1\}_{t_2} \\ a & \vdash & x_2 \\ a, b & \vdash & t_1 \\ a, b & \vdash & t_2 \end{cases}$$

with $x_1 \stackrel{?}{=} \{t_1\}_{t_2}$

$$\begin{cases} a & \vdash & y_1 \\ a, b & \vdash & \{y_1\}_{y_2} \end{cases}$$

$$\begin{cases} a & \vdash & z_1 \\ a & \vdash & z_2 \\ a, b & \vdash & \{z_1\}_{z_2} \\ a, b & \vdash & y_2 \end{cases}$$

with $y_1 \stackrel{?}{=} \{z_1\}_{z_2}$

Termination problem

$$\begin{cases} a & \vdash & \{x_1\}_{x_2} \\ a, b & \vdash & x_1 \end{cases}$$

$$\begin{cases} a & \vdash & \{t_1\}_{t_2} \\ a & \vdash & x_2 \\ a, b & \vdash & t_1 \\ a, b & \vdash & t_2 \end{cases}$$

with $x_1 \stackrel{?}{=} \{t_1\}_{t_2}$

$$\begin{cases} a & \vdash & y_1 \\ a, b & \vdash & \{y_1\}_{y_2} \end{cases}$$

$$\begin{cases} a & \vdash & z_1 \\ a & \vdash & z_2 \\ a, b & \vdash & \{z_1\}_{z_2} \\ a, b & \vdash & y_2 \end{cases}$$

with $y_1 \stackrel{?}{=} \{z_1\}_{z_2}$

There exists a strategy on the rules which terminates

Future Works

Decision procedure for symbolic equivalence

- disequation
- set of constraint systems
- more cryptographic primitives

Future Works

Decision procedure for symbolic equivalence

- disequation
- set of constraint systems
- more cryptographic primitives

Decision procedure for trace equivalence

- else branch
- non deterministc protocol