
Narrowing Based Constraint Solving for the Verification of Security Protocols*

Stéphanie Delaune

France Télécom R&D

Florent Jacquemard

INRIA Research Unit Futurs

LSV CNRS UMR 8643

work supported by the national project PROUVÉ 03V360

Our Result & Plan

Result

An NP decision procedure for the resolution of sets of **equations** and **deduction constraints** $s_1, \dots, s_m \vdash t$ **modulo** some collapsing equational theories.

Plan

1. Definition & Motivations (security protocols verification)
2. Syntactic procedure & Properties
3. Related works, extensions

Deduction Constraints

Given:

- a signature Σ partitioned into Σ_v (*visible / public symbols*) and Σ_p (*private symbols*),
- a TRS \mathcal{R} ,
- a set $T \subseteq \mathcal{T}(\Sigma)$ of ground terms,

$\mathcal{D}_{\mathcal{R}}(T)$ is the smallest (w.r.t. \subseteq) set of ground terms s.t.:

1. $T \subseteq \mathcal{D}_{\mathcal{R}}(T)$
2. $\forall f \in \Sigma_v, \forall t_1, \dots, t_n \in \mathcal{D}_{\mathcal{R}}(T), f(t_1, \dots, t_n) \in \mathcal{D}_{\mathcal{R}}(T)$
3. $\mathcal{D}_{\mathcal{R}}(T)$ is closed under $\xleftarrow{*}_{\mathcal{R}}$

	Deduction Constraint	Equation
	$s_1, \dots, s_n \Vdash t$	$s = t$
\mathcal{R} -solution	$t\sigma \in \mathcal{D}_{\mathcal{R}}(s_1\sigma, \dots, s_n\sigma)$	$s\sigma \xleftarrow{*}_{\mathcal{R}} t\sigma$

Application

Verification of the unsecurity of cryptographic protocols in systems with:

- a bounded number of honest participants communicating,
- an attacker controlling the communication network,
and whose capacities of deduction are modeled by \Vdash .
- [D. Dolev, A.C. Yao 1983]
assymmetric cryptography: $ae(_, _), ad(_, _), pub(_) \in \Sigma_v$ $_^{-1} \in \Sigma_p$
 $ad(ae(x, y), y^{-1}) \rightarrow x, \quad ad(ae(x, y^{-1}), y) \rightarrow x, \quad y^{-1^{-1}} \rightarrow y$
symmetric cryptography: $se(_, _), sd(_, _) \in \Sigma_v$, $sd(se(x, y), y) \rightarrow x$
pairs: $p(_, _), \pi_1(_), \pi_2(_) \in \Sigma_v$, $\pi_i(p(x_1, x_2)) \rightarrow x_i, i = 1, 2.$
- The problem is NP-complete in the model of Dolev-Yao.
[M. Rusinowitch, M. Turuani 2001].
- Problem NP-complete in the model of Dolev-Yao + equations for
exclusive or, Diffie-Hellman exponentiation...
[Y. Chevalier, R. Kuester, M. Rusinowitch, M. Turuani 2003].

Application (2)

Our procedure provides:

- a generic method to solve the unsecurity problem for a whole class of equational theories (but not XOR or DH exponent).

Generic procedure in [H. Comon, R. Treinen 2003],
for the decision of $s_1, \dots, s_n \Vdash t$ when s_1, \dots, s_n, t are ground,
in class of theories containing e.g. homomorphism
 $se(p(x_1, x_2), y) = p(se(x_1, y), se(x_2, y))$.

- the use of destructor symbols (ad, sd, π_1, π_2) and equations in protocol specifications.

This gives improved expressiveness and permits to capture more attacks [J. Millen 2003], [C. Lynch, C. Meadows 2004].

Example: Denning and Sacco Protocol (1981)

Exchange of a signed symmetric key K .

Protocol messages:

0. $A \rightarrow B : p(A, ae(ae(K, pub(A)^{-1}), pub(B)))$
1. $B \rightarrow A : se(S, K)$

A's process:

`new K.send(p(A, ae(ae(K, pub(A)^{-1}), pub(B)))).recv(x).record(sd(x, K))`

B's process:

`new S.recv(y).send(se(S, π2(ad(ad(π2(y), pub(B)^{-1}), pub(π1(y))))))`

Example: Denning and Sacco Protocol (1981)

Exchange of a signed symmetric key K .

Protocol messages:

0. $A \rightarrow B : p(A, ae(ae(K, pub(A)^{-1}), pub(B)))$
1. $B \rightarrow A : se(S, K)$

A's process:

`new K.send(p(A, ae(ae(K, pub(A)^{-1}), pub(B)))).recv(x).record(sd(x, K))`

B's process:

`new S.recv(y).send(se(S, π2(ad(ad(π2(y), pub(B)^{-1}), pub(π1(y))))))`

Attack against 1 agent, playing role B ($IK = 0, A, B, pub(A), pub(B)$):

$$\{ IK \Vdash y; IK, se(S, π2(ad(ad(π2(y), pub(B)^{-1}), pub(π1(y)))))) \Vdash x'; x' = S \}$$

Solution: $\{ y = p(A, ae(0, pub(B))), x' = S \}$.

$$se(S, π2(ad(ad(π2(y), pub(B)^{-1}), pub(π1(y)))))) \downarrow_{\mathcal{R}} \underbrace{se(S, π2(ad(0, pub(A))))}_{\in \mathcal{D}_{\mathcal{R}}(IK)} \stackrel{\text{UNIF}}{\sim} 2^{004 - 6}$$

Amended Denning Sacco Protocol (Lowe 1996)

Protocol messages:

- 
0. $A \rightarrow B : p(A, ae(ae(p(A, p(B, K)), pub(A)^{-1}), pub(B)))$
 1. $B \rightarrow A : se(S, K)$

A's process:

`new K.send($p(A, ae(ae(p(A, p(B, K)), pub(A)^{-1}), pub(B))))$).recv(x).record($sd(x, K)$)`

B's process:

`new S.recv(y).if $\pi_1(y) = \pi_1(\pi_1(ad(ad(\pi_2(y), pub(B)^{-1}), pub(\pi_1(y))))))$`
 `then if $\pi_1(\pi_2(ad(ad(\pi_2(y), pub(B)^{-1}), pub(\pi_1(y)))))) = B$`
 `then send($se(S, \pi_2(\pi_2(ad(ad(\pi_2(y), pub(B)^{-1}), pub(\pi_1(y))))))$)`
 `else abort`
 `else abort`

Public Collapsing Theories

Definition: A TRS \mathcal{R} is *public-collapsing* iff for every rule $\ell \rightarrow r \in \mathcal{R}$,

1. $r \in vars(\ell)$ or $r \in \mathcal{T}(\Sigma_v) \downarrow_{\mathcal{R}}$ and $r \neq \ell$,
2. if $\ell = f(\ell_1, \dots, \ell_n)$ with $f \in \Sigma_v$, then
for all $i \leq n$, and all subterm $g(t_1, \dots, t_m)$ of ℓ_i with $g \in \Sigma_v$,
either $g(t_1, \dots, t_m) \in \mathcal{T}(\Sigma_v) \downarrow_{\mathcal{R}}$, or there exists $j \leq m$ such that $t_j = r$.

Example: $sd(se(x, y), y) \rightarrow x$, $ad(ae(x, y), y^{-1}) \rightarrow x$,
 $ad(ae(x, y^{-1}), y) \rightarrow x$, $y^{-1^{-1}} \rightarrow y$, $check(x, ad(x, y^{-1}), y) \rightarrow ok$.

Public Collapsing Theories

Definition: A TRS \mathcal{R} is *public-collapsing* iff for every rule $\ell \rightarrow r \in \mathcal{R}$,

1. $r \in vars(\ell)$ or $r \in \mathcal{T}(\Sigma_v) \downarrow_{\mathcal{R}}$ and $r \neq \ell$,
2. if $\ell = f(\ell_1, \dots, \ell_n)$ with $f \in \Sigma_v$, then
for all $i \leq n$, and all subterm $g(t_1, \dots, t_m)$ of ℓ_i with $g \in \Sigma_v$,
either $g(t_1, \dots, t_m) \in \mathcal{T}(\Sigma_v) \downarrow_{\mathcal{R}}$, or there exists $j \leq m$ such that $t_j = r$.

Example: $sd(se(x, y), y) \rightarrow x$, $ad(ae(x, y), y^{-1}) \rightarrow x$,
 $ad(ae(x, y^{-1}), y) \rightarrow x$, $y^{-1^{-1}} \rightarrow y$, $check(x, ad(x, y^{-1}), y) \rightarrow ok$.

Theorem: Given $s_1, \dots, s_n, t \in \mathcal{T}(\Sigma)$ ground terms, $t \in \mathcal{D}_{\mathcal{R}}(s_1, \dots, s_n)$ is decidable in PTIME if \mathcal{R} is convergent and public-collapsing.

Syntactic Basic Procedure

$$\frac{\frac{\frac{\frac{\mathcal{P} \cup \{e[f(u_1, \dots, u_n)]\}; \mathcal{C}; \sigma}{\mathcal{P} \cup \{e[r]\}; \mathcal{C}\eta; \sigma\eta \cup \eta} \text{N}}{\mathcal{P} \cup \{s = t\}; \mathcal{C}; \sigma} \cup \\ \frac{\mathcal{P} \cup \{c\}; \mathcal{C}; \sigma}{\mathcal{P}; \mathcal{C} \cup \{c\sigma\}; \sigma} \text{B}}{\mathcal{P}; \mathcal{C}; \sigma} \text{VE}}{\mathcal{P}; \mathcal{C} \cup \{s_1, \dots, s_n \Vdash t\}; \sigma} \text{G}$$

Narrowing

e equation or deduction constraint,
 $f(\ell_1, \dots, \ell_n) \rightarrow r \in \mathcal{R}$ (fresh variant),
 $\eta = mgu(f(\ell_1, \dots, \ell_n)\sigma, f(u_1, \dots, u_n)\sigma)$

Syntactic Unification

$\eta = mgu(s\sigma, t\sigma)$

Blocking

c deduction constraint

Variable Elimination

$x \in vars(\mathcal{C}), t \in st(\mathcal{C}) \setminus vars(\mathcal{C}), x \notin t$

Ground

$t \in \mathcal{D}_R(s_1, \dots, s_n)$

Results

Theorem Given a convergent and public-collapsing TRS \mathcal{R} , the application of the inferences of the constraint solving system to $\mathcal{P}; \emptyset; \emptyset$

- terminates (and the depth, branching deg. and dag-size of nodes of the derivation tree are polynomial in $\|\mathcal{P}\| + \|\mathcal{R}\|$),
- is correct,
- is complete.

Results

Theorem Given a convergent and public-collapsing TRS \mathcal{R} , the application of the inferences of the constraint solving system to $\mathcal{P}; \emptyset; \emptyset$

- terminates (and the depth, branching deg. and dag-size of nodes of the derivation tree are polynomial in $\|\mathcal{P}\| + \|\mathcal{R}\|$),
- is correct,
- is complete.

Lemma (completeness) Let σ be a minimal (w.r.t. \ll) \mathcal{R} -solution of a *well-formed* set \mathcal{C} of deduction constraints s.t. all the terms in $\mathcal{C}\sigma$ are in \mathcal{R} -NF. For all $x \in \text{vars}(\mathcal{C})$, there exists $t \in \text{st}(\mathcal{C}) \setminus \text{vars}(\mathcal{C})$ such that $t\sigma = x\sigma$.

Results

Theorem Given a convergent and public-collapsing TRS \mathcal{R} , the application of the inferences of the constraint solving system to $\mathcal{P}; \emptyset; \emptyset$

- terminates (and the depth, branching deg. and dag-size of nodes of the derivation tree are polynomial in $\|\mathcal{P}\| + \|\mathcal{R}\|$),
- is correct,
- is complete.

Lemma (completeness) Let σ be a minimal (w.r.t. \ll) \mathcal{R} -solution of a *well-formed* set \mathcal{C} of deduction constraints s.t. all the terms in $\mathcal{C}\sigma$ are in \mathcal{R} -NF. For all $x \in \text{vars}(\mathcal{C})$, there exists $t \in \text{st}(\mathcal{C}) \setminus \text{vars}(\mathcal{C})$ such that $t\sigma = x\sigma$.

Corollary For \mathcal{R} convergent and public-collapsing,
the \mathcal{R} -solvability of *well formed* sets of equations and DC is NP

Corollary Protocol insecurity in presence of explicit destructors and \mathcal{R} convergent and public-collapsing is NP.

Further Works

Automatic proof of static non-equivalences $\not\approx_s$.

$$\sigma \not\approx_s \sigma' \quad \text{iff} \quad \exists s, t \text{ s.t. } s\sigma =_{\mathcal{R}} t\sigma \text{ and } s\sigma' \neq_{\mathcal{R}} t\sigma'$$

Extension of the procedure to AC;
XOR theory with AC(+) and the public-collapsing rules:

$$\begin{aligned} x + x &\rightarrow 0 \\ x + 0 &\rightarrow x \\ x + x + y &\rightarrow y \end{aligned}$$

Semantical methods with constrained tree automata, using results of regularity preservation under rewriting.