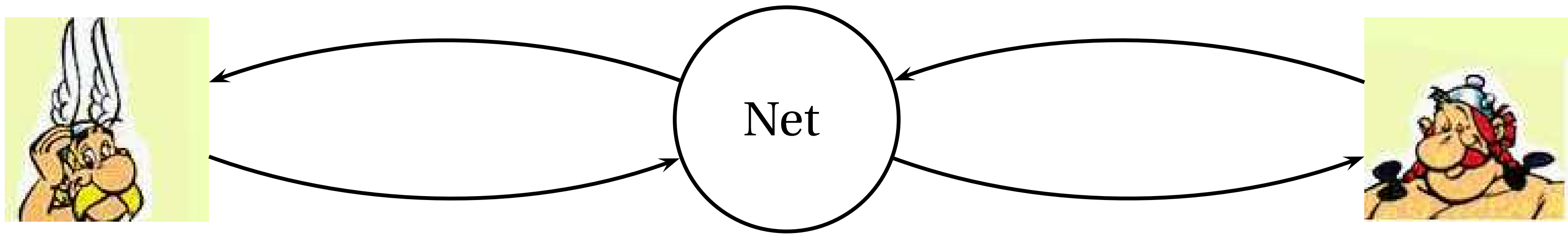
The Finite Variant Property: How to Get Rid of Some Algebraic Properties

Hubert Comon-Lundh[1], **Stéphanie Delaune**[1,2]

[1] LSV, CNRS UMR 8643, ENS de Cachan

[2] France Télécom R&D

Motivation: Cryptographic Protocols



Protocol

↪ rules of message exchanges

Goal

↪ secure communications: *secrecy, authentication, anonymity* ...

Applications

↪ mobile phone, e-voting, e-commerce, ...

Motivation: Cryptographic Protocols

Protocol

↪ rules of message exchanges

Goal

↪ secure communications: *secrecy, authentication, anonymity* ...

Applications

↪ mobile phone, e-voting, e-commerce, ...

Motivation: Security Problem

Protocol rules $\mathcal{P}$

$$\mathtt{enc}(x, k2) \;\Rightarrow\; \mathtt{enc}(\mathtt{dec}(x, k1), k2)$$

Motivation: Security Problem

Protocol rules $\mathcal{P}$

$$\texttt{enc}(x, k2) \;\Rightarrow\; \texttt{enc}(\texttt{dec}(x, k1), k2)$$

Intruder theory $\mathcal{I}$

$$\frac{u \quad v}{\texttt{enc}(u, v)} \qquad \frac{u \quad v}{\texttt{dec}(u, v)}$$

+ initial knowledge: $\texttt{enc}(s, k1), k2$

Motivation: Security Problem

Equational theory E

$$\texttt{dec}(\texttt{enc}(x,y),y) = x$$

Protocol rules $\mathcal{P}$

$$\texttt{enc}(x, k2) \;\Rightarrow\; \texttt{enc}(\texttt{dec}(x, k1), k2)$$

Intruder theory $\mathcal{I}$

$$\frac{u \quad v}{\texttt{enc}(u, v)} \qquad \frac{u \quad v}{\texttt{dec}(u, v)}$$

+ initial knowledge: $\texttt{enc}(s, k1)$, $k2$

Motivation: Security Problem

Equational theory E

$$\mathtt{dec}(\mathtt{enc}(x,y),y) = x$$

Protocol rules $\mathcal{P}$

$$\mathtt{enc}(x, k2) \;\Rightarrow\; \mathtt{enc}(\mathtt{dec}(x, k1), k2)$$

Intruder theory $\mathcal{I}$

$$\frac{u \quad v}{\mathtt{enc}(u, v)} \qquad \frac{u \quad v}{\mathtt{dec}(u, v)}$$

+ initial knowledge: $\mathtt{enc}(s, k1)$, $k2$

Description of the attack on $\mathcal{P}$ with $\mathcal{I}$, E:

Motivation: Security Problem

Equational theory E

$$\texttt{dec}(\texttt{enc}(x,y),y) = x$$

Protocol rules $\mathcal{P}$

$$\texttt{enc}(x, k2) \;\Rightarrow\; \texttt{enc}(\texttt{dec}(x, k1), k2)$$

Intruder theory $\mathcal{I}$

$$\frac{u \quad v}{\texttt{enc}(u, v)} \qquad \frac{u \quad v}{\texttt{dec}(u, v)}$$

+ initial knowledge: $\texttt{enc}(s, k1)$, $k2$

Description of the attack on $\mathcal{P}$ with $\mathcal{I}$, E:

$$\texttt{enc}(s, k1) \qquad k2$$

Motivation: Security Problem

Equational theory E

$$\texttt{dec}(\texttt{enc}(x,y),y) = x$$

Protocol rules $\mathcal{P}$

$$\texttt{enc}(x, k2) \Rightarrow \texttt{enc}(\texttt{dec}(x, k1), k2)$$

Intruder theory $\mathcal{I}$

$$\frac{u \quad v}{\texttt{enc}(u, v)} \qquad \frac{u \quad v}{\texttt{dec}(u, v)}$$

+ initial knowledge: $\texttt{enc}(s, k1)$, $k2$

Description of the attack on $\mathcal{P}$ with $\mathcal{I}$, E:

$$\frac{\texttt{enc}(s, k1) \qquad k2}{\texttt{enc}(\texttt{enc}(s, k1), k2)}$$

Motivation: Security Problem

Equational theory E

$$\mathtt{dec}(\mathtt{enc}(x,y),y) = x$$

Protocol rules $\mathcal{P}$

$$\mathtt{enc}(x, k2) \;\Rightarrow\; \mathtt{enc}(\mathtt{dec}(x, k1), k2)$$

Intruder theory $\mathcal{I}$

$$\frac{u \quad v}{\mathtt{enc}(u, v)} \qquad \frac{u \quad v}{\mathtt{dec}(u, v)}$$

+ initial knowledge: $\mathtt{enc}(s, k1)$, $k2$

Description of the attack on $\mathcal{P}$ with $\mathcal{I}$, E:

$$\frac{\mathtt{enc}(s, k1) \qquad k2}{\mathtt{enc}(\mathtt{enc}(s, k1), k2)} \quad \Rightarrow_{\mathcal{P}} \quad \mathtt{enc}(\mathtt{dec}(\mathtt{enc}(s, k1), k1), k2)$$

Motivation: Security Problem

Equational theory E

$$\mathtt{dec}(\mathtt{enc}(x,y),y) = x$$

Protocol rules $\mathcal{P}$

$$\mathtt{enc}(x, k2) \;\Rightarrow\; \mathtt{enc}(\mathtt{dec}(x, k1), k2)$$

Intruder theory $\mathcal{I}$

$$\frac{u \quad v}{\mathtt{enc}(u, v)} \qquad \frac{u \quad v}{\mathtt{dec}(u, v)}$$

+ initial knowledge: $\mathtt{enc}(s, k1)$, $k2$

Description of the attack on $\mathcal{P}$ with $\mathcal{I}$, E:

$$\frac{\mathtt{enc}(s, k1) \qquad k2}{\mathtt{enc}(\mathtt{enc}(s, k1), k2)} \;\Rightarrow_{\mathcal{P}}\; \mathtt{enc}(\mathtt{dec}(\mathtt{enc}(s, k1), k1), k2)$$

$$=_E$$

$$\mathtt{enc}(s, k2)$$

Motivation: Security Problem

Equational theory E

$$\mathtt{dec}(\mathtt{enc}(x,y),y) = x$$

Protocol rules $\mathcal{P}$

$$\mathtt{enc}(x, k2) \;\Rightarrow\; \mathtt{enc}(\mathtt{dec}(x, k1), k2)$$

Intruder theory $\mathcal{I}$

$$\frac{u \quad v}{\mathtt{enc}(u, v)} \qquad \frac{u \quad v}{\mathtt{dec}(u, v)}$$

+ initial knowledge: $\mathtt{enc}(s, k1)$, $k2$

Description of the attack on $\mathcal{P}$ with $\mathcal{I}$, E:

$$\frac{\mathtt{enc}(s, k1) \qquad k2}{\mathtt{enc}(\mathtt{enc}(s, k1), k2)} \;\Rightarrow_{\mathcal{P}}\; \mathtt{enc}(\mathtt{dec}(\mathtt{enc}(s, k1), k1), k2)$$

$$=_E$$

$$\frac{\mathtt{enc}(s, k2) \qquad k2}{\mathtt{dec}(\mathtt{enc}(s, k2), k2)}$$

Motivation: Security Problem

Equational theory E

$\mathtt{dec}(\mathtt{enc}(x,y),y) = x$

Protocol rules $\mathcal{P}$

$\mathtt{enc}(x, k2) \;\Rightarrow\; \mathtt{enc}(\mathtt{dec}(x, k1), k2)$

Intruder theory $\mathcal{I}$

$$\frac{u \quad v}{\mathtt{enc}(u, v)} \qquad \frac{u \quad v}{\mathtt{dec}(u, v)}$$

+ initial knowledge: $\mathtt{enc}(s, k1)$, $k2$

Description of the attack on $\mathcal{P}$ with $\mathcal{I}$, E:

$$\frac{\mathtt{enc}(s, k1) \qquad k2}{\mathtt{enc}(\mathtt{enc}(s, k1), k2)} \;\Rightarrow_{\mathcal{P}}\; \mathtt{enc}(\mathtt{dec}(\mathtt{enc}(s, k1), k1), k2)$$

$$=_E$$

$$\frac{\mathtt{enc}(s, k2) \qquad k2}{\mathtt{dec}(\mathtt{enc}(s, k2), k2)}$$

$$=_E$$

$$s$$

Motivation: Security Problem

Equational theory E

$$\mathtt{dec}(\mathtt{enc}(x,y),y) = x$$

$$\mathcal{P}: \quad \mathtt{enc}(x, k2) \Rightarrow \mathtt{enc}(\mathtt{dec}(x, k1), k2)$$

$$\mathcal{I}: \quad \frac{u \quad v}{\mathtt{enc}(u, v)} \qquad \frac{u \quad v}{\mathtt{dec}(u, v)}$$

Motivation: Security Problem

Equational theory E

$$\texttt{dec}(\texttt{enc}(x,y),y) \rightarrow x$$

$\mathcal{P}$: $\texttt{enc}(x, k2) \Rightarrow \texttt{enc}(\texttt{dec}(x, k1), k2)$ $\mathcal{I}$: $\dfrac{u \quad v}{\texttt{enc}(u, v)}$ $\dfrac{u \quad v}{\texttt{dec}(u, v)}$

Motivation: Security Problem

Equational theory E

$$\mathtt{dec}(\mathtt{enc}(x,y),y) \rightarrow x$$

$\mathcal{P}: \quad \mathtt{enc}(x, k2) \Rightarrow \mathtt{enc}(\mathtt{dec}(x, k1), k2)$ $\qquad \mathcal{I}: \quad \dfrac{u \quad v}{\mathtt{enc}(u, v)} \qquad \dfrac{u \quad v}{\mathtt{dec}(u, v)}$

$\mathcal{P}_1: \quad \mathtt{enc}(x, k2) \Rightarrow \mathtt{enc}(\mathtt{dec}(x, k1), k2)$

Motivation: Security Problem

Equational theory E

$$\mathtt{dec}(\mathtt{enc}(x,y),y) \rightarrow x$$

$\mathcal{P}:\quad \mathtt{enc}(x, k2) \;\Rightarrow\; \mathtt{enc}(\mathtt{dec}(x, k1), k2)$

$\mathcal{I}$: $\dfrac{u \quad v}{\mathtt{enc}(u, v)} \qquad \dfrac{u \quad v}{\mathtt{dec}(u, v)}$

$\mathcal{P}_1:\quad \mathtt{enc}(x, k2) \;\Rightarrow\; \mathtt{enc}(\mathtt{dec}(x, k1), k2)$

$\mathcal{P}_2:\quad \mathtt{enc}(\mathtt{enc}(x, k1), k2) \;\Rightarrow\; \mathtt{enc}(x, k2)$

Motivation: Security Problem

Equational theory E

$$\mathtt{dec}(\mathtt{enc}(x,y),y) \rightarrow x$$

$\mathcal{P}$: $\mathtt{enc}(x, k2) \Rightarrow \mathtt{enc}(\mathtt{dec}(x, k1), k2)$

$\mathcal{I}$: $\dfrac{u \quad v}{\mathtt{enc}(u, v)}$ $\qquad$ $\dfrac{u \quad v}{\mathtt{dec}(u, v)}$

$\mathcal{P}_1$: $\mathtt{enc}(x, k2) \Rightarrow \mathtt{enc}(\mathtt{dec}(x, k1), k2)$

$\mathcal{P}_2$: $\mathtt{enc}(\mathtt{enc}(x, k1), k2) \Rightarrow \mathtt{enc}(x, k2)$

$\mathcal{I}_{var}$: $\dfrac{\mathtt{enc}(u, v) \quad v}{u}$

Motivation: Security Problem

Equational theory E

$$\mathtt{dec}(\mathtt{enc}(x,y),y) \rightarrow x$$

$$\mathcal{P}: \quad \mathtt{enc}(x, k2) \Rightarrow \mathtt{enc}(\mathtt{dec}(x, k1), k2)$$

$$\mathcal{I}: \quad \frac{u \quad v}{\mathtt{enc}(u, v)} \qquad \frac{u \quad v}{\mathtt{dec}(u, v)}$$

$$\mathcal{P}_1: \quad \mathtt{enc}(x, k2) \Rightarrow \mathtt{enc}(\mathtt{dec}(x, k1), k2)$$

$$\mathcal{P}_2: \quad \mathtt{enc}(\mathtt{enc}(x, k1), k2) \Rightarrow \mathtt{enc}(x, k2)$$

$$\mathcal{I}_{var}: \frac{\mathtt{enc}(u, v) \quad v}{u}$$

Attack on $\mathcal{P}$ with $\mathcal{I}$, E $\quad \Leftrightarrow \quad$ $\exists i$. Attack on $\mathcal{P}_i$ with $\mathcal{I} \cup \mathcal{I}_{var}$, $\emptyset$

Summary

Goal:
Investigate the finite variant property for equational theories, which are relevant to cryptographic protocols verification.

Summary

Goal:
Investigate the finite variant property for equational theories, which are relevant to cryptographic protocols verification.

Application:
Reduce the decidability of a problem in E into a (supposedly) simpler theory E':

- security problem
- disunification problem

Summary

Goal:
Investigate the finite variant property for equational theories, which are relevant to cryptographic protocols verification.

Application:
Reduce the decidability of a problem in E into a (supposedly) simpler theory E':

- security problem
- disunification problem

How to do this ?
Given a theory E, find a splitting of E in $(\mathcal{R}, E')$ such that:

- $\mathcal{R}$ is an E'-convergent rewrite system for E,
- $(\mathcal{R}, E')$ has the finite variant property

Roadmap of the Talk

I) Another Caracterisation of the Property

- Preliminaries
- Finite Variant Property
- Boundedness Property

II) Proving Boundedness

- Sufficient Criteria (1)
- Difficulties with Non-Orientable Axioms
- Abelian Group Theory
- Sufficient Criteria (2)
- Diffie-Hellman Theory

III) Proving Non-Boundedness

- ACUNh Theory

Roadmap of the Talk

I) Another Caracterisation of the Property

- Preliminaries
- Finite Variant Property
- Boundedness Property

II) Proving Boundedness

- Sufficient Criteria (1)
- Difficulties with Non-Orientable Axioms
- Abelian Group Theory
- Sufficient Criteria (2)
- Diffie-Hellman Theory

III) Proving Non-Boundedness

- ACUNh Theory

Preliminaries

Equational Rewriting (w.r.t $E'\backslash\mathcal{R}$)

$s \rightarrow_{E'\backslash\mathcal{R}} t$ iff $\exists p \in Pos(s)$ $\exists\sigma$ such that $s|_p =_{E'} l\sigma$ and $t = s[r\sigma]_p$

Equational Narrowing (w.r.t $E'\backslash\mathcal{R}$)

$s \leadsto_{E'\backslash\mathcal{R}} t$ iff $\exists p \in Pos(s)$ $\exists\sigma$ such that $(s|_p)\sigma =_{E'} l\sigma$ and $t = s[r\sigma]_p$

Preliminaries

Equational Rewriting (w.r.t $E'\backslash\mathcal{R}$)

$$s \rightarrow_{E'\backslash\mathcal{R}} t \quad \text{iff} \quad \exists p \in Pos(s)\ \exists\sigma \text{ such that } s|_p =_{E'} l\sigma \text{ and } t = s[r\sigma]_p$$

Equational Narrowing (w.r.t $E'\backslash\mathcal{R}$)

$$s \rightsquigarrow_{E'\backslash\mathcal{R}} t \quad \text{iff} \quad \exists p \in Pos(s)\ \exists\sigma \text{ such that } (s|_p)\sigma =_{E'} l\sigma \text{ and } t = s[r\sigma]_p$$

Lifting Lemma

Let E' be a regular presentation for which a unification algorithm exists.
Let $\mathcal{R}$ be an E'-convergent rewriting system.
Let $\mathcal{D}$ a derivation starting from $s_1 = t_1\theta_1$ (θ_1 normalized):

$$\begin{tikzcd}
\mathcal{D}: & s_1 \arrow[r, "p_1"] & {}_{E'\backslash\mathcal{R}}\ s_2 \arrow[r, "p_2"] & {}_{E'\backslash\mathcal{R}} \cdots \arrow[r, "p_n"] & {}_{E'\backslash\mathcal{R}}\ s_n \\
& t_1 \arrow[u, bend left, "\theta_1"] \arrow[r, rightsquigarrow, "p_1"] & {}_{E'\backslash\mathcal{R}}\ t_2 \arrow[u, bend left, "\theta_2"] \arrow[r, rightsquigarrow, "p_2"] & {}_{E'\backslash\mathcal{R}} \cdots \arrow[r, rightsquigarrow, "p_n"] & {}_{E'\backslash\mathcal{R}}\ t_n \arrow[u, bend left, "\theta_n"]
\end{tikzcd}$$

with $\theta_1, \ldots, \theta_n$ normalized substitutions.

Finite Variant Property

Let $\mathcal{R}$ be an E'-convergent rewrite system for E.

Variant

t' is a variant of a term t iff $\exists\theta$ such that $t' = t\theta\downarrow$ (w.r.t. $E'\backslash\mathcal{R}$)

S is a complete set of variants of t iff $\forall\sigma.\exists t' \in S.\exists\theta$ such that $t\sigma\downarrow =_{E'} t'\theta$.

Finite Variant Property

Let $\mathcal{R}$ be an E'-convergent rewrite system for E.

Variant

t' is a variant of a term t iff $\exists\theta$ such that $t' = t\theta\downarrow$ (w.r.t. $E'\backslash\mathcal{R}$)

S is a complete set of variants of t iff $\forall\sigma.\exists t' \in S.\exists\theta$ such that $t\sigma\downarrow =_{E'} t'\theta$.

EXAMPLE:

$$\mathcal{R} = \left\{ \begin{array}{rcl} x + 0 & \rightarrow & x \\ x + x & \rightarrow & 0 \\ x + (x + y) & \rightarrow & y \end{array} \right. \qquad\qquad E' = AC$$

Let $t = x + f(x + y)$ and $\sigma_0 = \{x \mapsto f(z) + z;\ \ y \mapsto f(z)\}$.

- $t\sigma_0\downarrow = z \quad\Rightarrow\quad z$ is a variant of t,
- $\forall\sigma, (x + f(x + y))\sigma\downarrow =_{AC} z\theta$ for some $\theta \quad\Rightarrow\quad \{z\}$ is complete.

Boundedness Property

Finite Variant Property – $(\mathcal{R}, E')$ has the finite variant property if:
For every term t, there exists a finite and complete set of variants of t

Boundedness Property

Finite Variant Property – $(\mathcal{R}, E')$ has the finite variant property if:
For every term t, there exists a finite and complete set of variants of t

$\Updownarrow$ **when E' is regular (Lifting Lemma)**

Boundedness Property – $(\mathcal{R}, E')$ has the boundedness property if:
For every term t, there is an integer n such that

$$\forall \sigma.\ t(\sigma\downarrow) \xrightarrow{\leq n}_{E' \backslash \mathcal{R}} (t\sigma)\downarrow$$

Roadmap of the Talk

I) Another Caracterisation of the Property

- Preliminaries
- Boundedness Property
- Finite Variant Property

II) Proving Boundedness

- Sufficient Criteria (1)
- Difficulties with Non-Orientable Axioms
- Abelian Group Theory
- Sufficient Criteria (2)
- Diffie-Hellman Theory

III) Proving Non-Boundedness

- ACUNh Theory

Sufficient Criteria (1)

Proposition:
If (basic) narrowing terminates for $\mathcal{R}$ then $(\mathcal{R}, \emptyset)$ satisfies the boundedness property.

Sufficient Criteria (1)

Proposition:
If (basic) narrowing terminates for $\mathcal{R}$ then $(\mathcal{R}, \emptyset)$ satisfies the boundedness property.

Axiomatized Dolev-Yao Theory (DYT)
The classical Dolev-Yao model with explicit destructors.

$$
\begin{array}{rcll}
\pi_i(\langle x_1, x_2 \rangle) & = & x_i & \text{for } i = 1, 2 \\
\mathtt{dec}(\mathtt{enc}(x, y), y^{-1}) & = & x & \\
x^{-1^{-1}} & = & x &
\end{array}
$$

Sufficient Criteria (1)

Proposition:
If (basic) narrowing terminates for $\mathcal{R}$ then $(\mathcal{R}, \emptyset)$ satisfies the boundedness property.

Axiomatized Dolev-Yao Theory (DYT)
The classical Dolev-Yao model with explicit destructors.

$$
\begin{array}{rcll}
\pi_i(\langle x_1, x_2 \rangle) & \rightarrow & x_i & \text{for } i = 1, 2 \\
\texttt{dec}(\texttt{enc}(x, y), y^{-1}) & \rightarrow & x & \\
{x^{-1}}^{-1} & \rightarrow & x & \\
\texttt{dec}(\texttt{enc}(x, y^{-1}), y) & \rightarrow & x &
\end{array}
$$

Corollary: $(\mathcal{R}_{\mathrm{DYT}}, \emptyset)$ has the boundedness property.

Difficulties with Non-Orientable Axioms

Lifting of Innermost Derivation $\not\Rightarrow$ Basic Narrowing Sequence [Viola01]

$$\mathcal{R}_+ = \left\{\; x + 0 \to x \quad ; \quad x + x \to 0 \quad ; \quad x + (x + y) \to y \;\right\}$$

Let $t = x_1 + x_2$ and $\sigma = \{x_1 \mapsto a + b,\;\; x_2 \mapsto a + b\}$.
Consider the following innermost derivation (w.r.t. $\to_{AC\backslash\mathcal{R}_+}$):

$$\mathcal{D} : \quad \underbrace{(a + b) + (a + b)}_{t\sigma} \quad \xrightarrow{\Lambda}_{x+(x+y)\to y} \quad b + b \quad \xrightarrow{\Lambda}_{x+x\to 0} \quad 0$$

$\Rightarrow$ $\mathcal{D}$ **is not basic** (i.e. not based on $\bar{O}(t)$)

Even worse: Basic AC-Narrowing is not complete [See our paper]

Difficulties with Non-Orientable Axioms

Lifting of Innermost Derivation $\not\Rightarrow$ Basic Narrowing Sequence [Viola01]

$$\mathcal{R}_+ = \left\{ \; x + 0 \to x \quad ; \quad x + x \to 0 \quad ; \quad x + (x + y) \to y \; \right\}$$

Let $t = x_1 + x_2$ and $\sigma = \{x_1 \mapsto a + b, \;\; x_2 \mapsto a + b\}$.
Consider the following innermost derivation (w.r.t. $\to_{AC\backslash\mathcal{R}_+}$):

$$\mathcal{D}: \quad \underbrace{(a+b)+(a+b)}_{t\sigma} \quad \xrightarrow{\Lambda}_{x+(x+y)\to y} \quad b + b \quad \xrightarrow{\Lambda}_{x+x\to 0} \quad 0$$

$\Rightarrow$ $\mathcal{D}$ **is not basic** (i.e. not based on $\bar{O}(t)$)

Even worse: Basic AC-Narrowing is not complete [See our paper]

Non termination of Basic AC-Narrowing
for many relevant equational theories

EXAMPLE: Abelian Group Theory

Abelian Group Theory (1)

$$\begin{aligned} x \times x^{-1} &= 1 \\ x \times 1 &= x \end{aligned} \qquad\qquad \begin{aligned} x \times (y \times z) &= (x \times y) \times z \\ x \times y &= y \times x \end{aligned}$$

Abelian Group Theory (1)

Classical presentation of $\mathcal{AG}$:

$$\mathcal{R}_\times = \left\{ \begin{array}{rcl} x \times x^{-1} & \rightarrow & 1 \\ x \times 1 & \rightarrow & x \\ x^{-1^{-1}} & \rightarrow & x \\ 1^{-1} & \rightarrow & 1 \\ (x \times y)^{-1} & \rightarrow & x^{-1} \times y^{-1} \\ x \times (y \times x^{-1}) & \rightarrow & y \end{array} \right.$$

$$\begin{array}{rcl} x \times (y \times z) & = & (x \times y) \times z \\ x \times y & = & y \times x \end{array}$$

Abelian Group Theory (1)

Classical presentation of $\mathcal{AG}$:

$$\mathcal{R}_\times = \left\{ \begin{array}{rcl} x \times x^{-1} & \rightarrow & 1 \\ x \times 1 & \rightarrow & x \\ {x^{-1}}^{-1} & \rightarrow & x \\ 1^{-1} & \rightarrow & 1 \\ (x \times y)^{-1} & \rightarrow & x^{-1} \times y^{-1} \\ x \times (y \times x^{-1}) & \rightarrow & y \end{array} \right.$$

$$\begin{array}{rcl} x \times (y \times z) & = & (x \times y) \times z \\ x \times y & = & y \times x \end{array}$$

Problem
This presentation does **not** satisify the **boundedness property**.

Abelian Group Theory (1)

Classical presentation of $\mathcal{AG}$:

$$\mathcal{R}_\times = \left\{ \begin{array}{rcl} x \times x^{-1} & \rightarrow & 1 \\ x \times 1 & \rightarrow & x \\ {x^{-1}}^{-1} & \rightarrow & x \\ 1^{-1} & \rightarrow & 1 \\ (x \times y)^{-1} & \rightarrow & x^{-1} \times y^{-1} \\ x \times (y \times x^{-1}) & \rightarrow & y \end{array} \right.$$

$$\begin{array}{rcl} x \times (y \times z) & = & (x \times y) \times z \\ x \times y & = & y \times x \end{array}$$

Problem
This presentation does **not** satisify the **boundedness property**.

COUNTER-EXAMPLE
Let $t = x^{-1}$ and $\sigma = \{x \mapsto a_0 \times \ldots \times a_n\}$.

$$\underbrace{(a_0 \times \ldots \times a_n)^{-1}}_{t\sigma} \underbrace{\rightarrow_{AC\backslash\mathcal{R}_\times} \cdots \rightarrow_{AC\backslash\mathcal{R}_\times} \cdots \rightarrow}_{\text{at least } n \text{ steps}} \underbrace{a_0^{-1} \times \ldots \times a_n^{-1}}_{t\sigma\downarrow}$$

Abelian Group Theory (2)

Unusual Presentation of $\mathcal{AG}$: [Lankford]

$$\mathcal{R}'_\times = \left\{ \begin{array}{rclrcl} x \times 1 & \rightarrow & x & {x^{-1}}^{-1} & \rightarrow & x \\ 1^{-1} & \rightarrow & 1 & (x^{-1} \times y)^{-1} & \rightarrow & x \times y^{-1} \\ x \times x^{-1} & \rightarrow & 1 & x \times (x^{-1} \times y) & \rightarrow & y \\ x^{-1} \times y^{-1} & \rightarrow & (x \times y)^{-1} & x^{-1} \times (y^{-1} \times z) & \rightarrow & (x \times y)^{-1} \times z \\ (x \times y)^{-1} \times y & \rightarrow & x^{-1} & (x \times y)^{-1} \times (y \times z) & \rightarrow & x^{-1} \times z \end{array} \right.$$

Proposition:
$\mathcal{R}'_\times$ is an AC-convergent rewrite system for $\mathcal{AG}$

Abelian Group Theory (2)

Unusual Presentation of $\mathcal{AG}$: [Lankford]

$$\mathcal{R}'_\times = \left\{ \begin{array}{rclrcl} x \times 1 & \rightarrow & x & {x^{-1}}^{-1} & \rightarrow & x \\ 1^{-1} & \rightarrow & 1 & (x^{-1} \times y)^{-1} & \rightarrow & x \times y^{-1} \\ x \times x^{-1} & \rightarrow & 1 & x \times (x^{-1} \times y) & \rightarrow & y \\ x^{-1} \times y^{-1} & \rightarrow & (x \times y)^{-1} & x^{-1} \times (y^{-1} \times z) & \rightarrow & (x \times y)^{-1} \times z \\ (x \times y)^{-1} \times y & \rightarrow & x^{-1} & (x \times y)^{-1} \times (y \times z) & \rightarrow & x^{-1} \times z \end{array} \right.$$

Proposition:
$\mathcal{R}'_\times$ is an AC-convergent rewrite system for $\mathcal{AG}$

Remark:
Basic AC-Narrowing does not terminate

$\Rightarrow$ $(\mathcal{R}'_\times, AC)$ satisfies the **boundedness property**

Sufficient Criteria (2)

Lemma:
If for each function symbol f, there is an integer c_f such that

$t_1, \ldots, t_n$ in normal forms $\Rightarrow$ $f(t_1, \ldots, t_n) \xrightarrow{\leq c_f}_{E' \backslash \mathcal{R}} f(t_1, \ldots, t_n)\downarrow$

then $(\mathcal{R}, E')$ satisfies the boundedness property.

Sufficient Criteria (2)

Lemma:
If for each function symbol f, there is an integer c_f such that

$t_1, \ldots, t_n$ in normal forms $\Rightarrow$ $f(t_1, \ldots, t_n) \xrightarrow{\leq c_f}_{E' \backslash \mathcal{R}} f(t_1, \ldots, t_n)\downarrow$
then $(\mathcal{R}, E')$ satisfies the boundedness property.

EXAMPLE: Abelian Group Theory

Let t_1 and t_2 terms in normal forms (w.r.t $AC \backslash \mathcal{R}'_\times$), we have:

- $t_1{}^{-1} \xrightarrow{\leq 1} (t_1{}^{-1})\downarrow$
- $t_1 \times t_2 \xrightarrow{\leq 2} (t_1 \times t_2)\downarrow$

Diffie-Hellman Theory

Presentation of the Diffie-Hellman Theory $\mathcal{DH}$

$$\mathcal{R}_{\mathcal{DH}} = \mathcal{R}'_{\times} \cup \left\{ \begin{array}{rcl} \mathtt{exp}(x, 1) & \rightarrow & x \\ \mathtt{exp}(\mathtt{exp}(x, y), z) & \rightarrow & \mathtt{exp}(x, y \times z) \end{array} \right.$$

Proposition:
$\mathcal{R}'_{\mathcal{DH}}$ is an AC-convergent rewrite system for $\mathcal{DH}$

Diffie-Hellman Theory

Presentation of the Diffie-Hellman Theory $\mathcal{DH}$

$$\mathcal{R}_{\mathcal{DH}} = \mathcal{R}'_{\times} \cup \left\{ \begin{array}{rcl} \mathtt{exp}(x, 1) & \rightarrow & x \\ \mathtt{exp}(\mathtt{exp}(x, y), z) & \rightarrow & \mathtt{exp}(x, y \times z) \end{array} \right.$$

Proposition:
$\mathcal{R}'_{\mathcal{DH}}$ is an AC-convergent rewrite system for $\mathcal{DH}$

Lemma:
Given t_1, t_2 terms in normal forms,

- ${t_1}^{-1} \xrightarrow{\leq 1} ({t_1}^{-1})\downarrow$
- $t_1 \times t_2 \xrightarrow{\leq 2} (t_1 \times t_2)\downarrow$
- $\mathtt{exp}(t_1, t_2) \xrightarrow{\leq 4} (\mathtt{exp}(t_1, t_2))\downarrow$

$\Rightarrow (\mathcal{R}'_{\mathcal{DH}}, AC)$ satisfies the **boundedness property**

Related Works

- **E. Viola** [ICTCS'01]
  E-unifiability via Narrowing

  $\hookrightarrow$ termination is ensured by a *narrowing bound*

- **C. Meadows and P. Narendran** [WITS'02]
  A unification algorithm for the group Diffie-Hellman protocol

  $\hookrightarrow$ compute a bound on the $\mathcal{R}_{exp}$-reduction steps

- **P. Narendran *et al.*** [LICS'93]
  On the unification problem for cartesian closed categories

  $\hookrightarrow$ notion of optimally reducing rewriting system

Roadmap of the Talk

I) Another Caracterisation of the Finite Variant Property

- Preliminaries
- Finite Variant Property
- Boundedness Property

II) Proving Boundedness

- Sufficient Criteria (1)
- Difficulties with Non-Orientable Axioms
- Abelian Group Theory
- Sufficient Criteria (2)
- Diffie-Hellman Theory

III) Proving Non-Boundedness

- ACUNh Theory

ACUNh Theory

$$
\begin{aligned}
x + x &= 0 \\
x + 0 &= x \\
h(x + y) &= h(x) + h(y)
\end{aligned}
$$

$$
\begin{aligned}
x + y &= y + x \\
x + (x + z) &= (x + y) + z
\end{aligned}
$$

ACUNh Theory

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

$$\mathcal{R}_1 : \quad h(x+y) \rightarrow h(x) + h(y)$$

$$
\begin{aligned}
\mathcal{R}_2 : \quad & h(x) + h(y) \rightarrow h(x+y) \\
& h(x) + h(y) + z \rightarrow h(x+y) + z
\end{aligned}
$$

ACUNh Theory

$$\begin{aligned} x + 0 &\to x \\ x + x &\to 0 \\ x + x + y &\to y \\ h(0) &\to 0 \end{aligned}$$

$$\mathcal{R}_1 : \quad h(x+y) \to h(x) + h(y)$$

$$\begin{aligned} \mathcal{R}_2 : \quad & h(x) + h(y) \to h(x+y) \\ & h(x) + h(y) + z \to h(x+y) + z \end{aligned}$$

$\Rightarrow$ $(\mathcal{R}_1, AC)$ and $(\mathcal{R}_2, AC)$ do **not** satisfy the **boundedness property**

ACUNh Theory

$$\begin{array}{rcl} x + 0 & \rightarrow & x \\ x + x & \rightarrow & 0 \\ x + x + y & \rightarrow & y \\ h(0) & \rightarrow & 0 \end{array} \qquad \begin{array}{ll} \mathcal{R}_1 : & h(x+y) \rightarrow h(x) + h(y) \\ & \\ \mathcal{R}_2 : & h(x) + h(y) \rightarrow h(x+y) \\ & h(x) + h(y) + z \rightarrow h(x+y) + z \end{array}$$

$\Rightarrow$ $(\mathcal{R}_1, AC)$ and $(\mathcal{R}_2, AC)$ do **not** satisfy the **boundedness property**

Theorem:
There is no decomposition $(\mathcal{R}, AC)$ of *ACUNh* which has the boundedness property.

Conclusion & Future Works

Conclusion

Reduce the decidability of the security problem in E to a smaller theory:

- **Sufficient Criteria 1**: termination of (basic) narrowing

$\Rightarrow$ solve the security problem by going back to the free model algebra

- **Sufficient Criteria 2**: it is satisfied by the $ACUN$, $\mathcal{AG}$ and $\mathcal{DH}$ theories

$\Rightarrow$ solve the security problem by reducing it to the AC equational theory

Conclusion & Future Works

Conclusion

Reduce the decidability of the security problem in E to a smaller theory:

- **Sufficient Criteria 1**: termination of (basic) narrowing

$\Rightarrow$ solve the security problem by going back to the free model algebra

- **Sufficient Criteria 2**: it is satisfied by the $ACUN$, $\mathcal{AG}$ and $\mathcal{DH}$ theories

$\Rightarrow$ solve the security problem by reducing it to the AC equational theory

Future Works

- Find a decidable criteria for establishing automatically the boundedness property of a theory,
- Find sufficient conditions on the intruder theory to ensure the decidability of the security problem,
- A Challenging Question: Does AC has the finite variant property ?