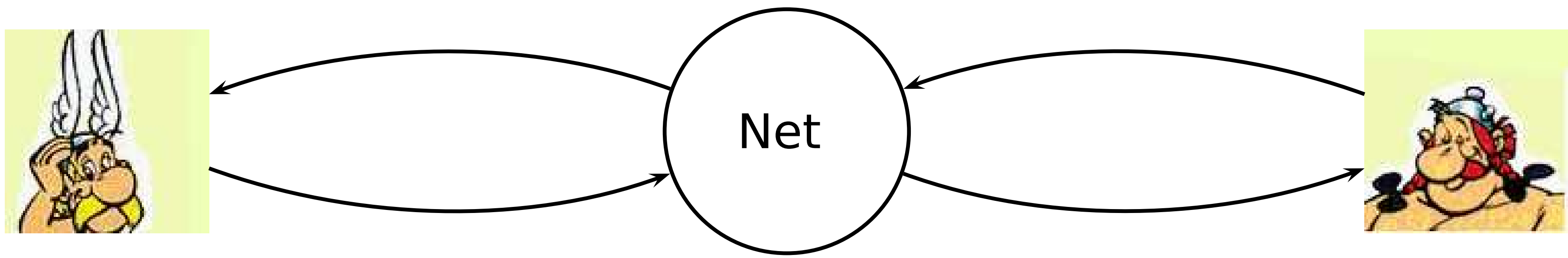
Verification of Cryptographic Protocols in Presence of Algebraic Properties

Stéphanie Delaune

LSV, CNRS UMR 8643, ENS de Cachan

France Télécom R&D

Cryptographic Protocols



Protocol

↪ rules of message exchanges

Goal

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

Applications

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

Cryptographic Protocols

Protocol

↪ rules of message exchanges

Goal

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

Applications

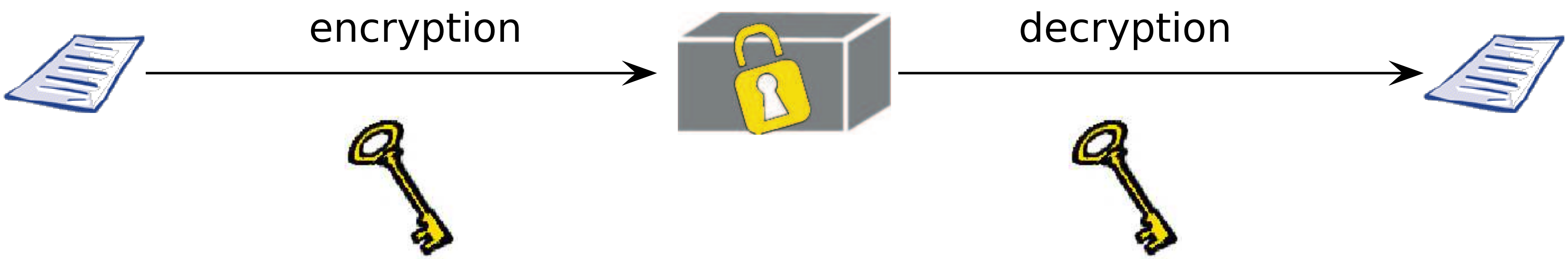
↪ mobile phone, e-voting, e-commerce, ...

Goals

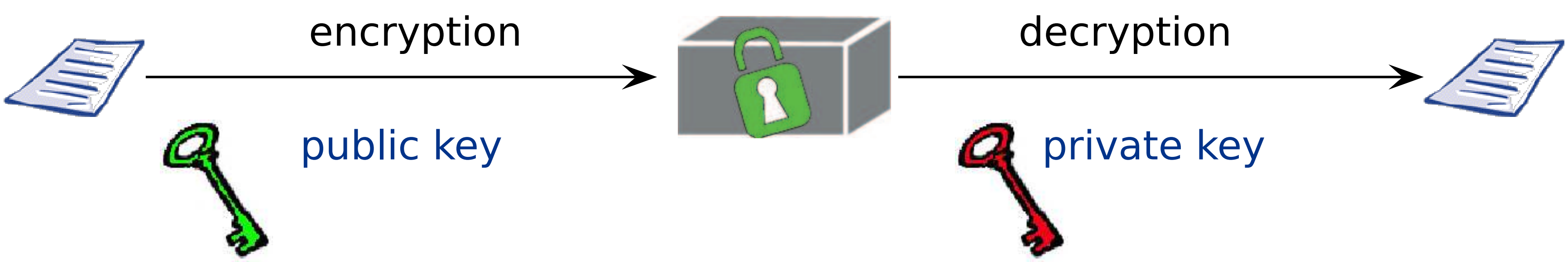
- **Secrecy**: May an intruder learn some secret message between two honest participants ?
- **Authentication**: Is the agent Alice really talking to Bob ?
- **Privacy**: Alice participate to an election. May a participant learn something about the vote of Alice ?
- **Fairness**: Alice and Bob want to sign a contract. Alice initiates the protocol. May Bob obtain some advantage ?

Encryption

- **Symmetric** Encryption



- **Asymmetric** Encryption



Dolev-Yao Intruder Model

u, v terms
T a finite set of terms (intruder's knowledge)

Axiom (A)	$\dfrac{u \in T}{T \vdash u}$	*Pairing* (*P*)	$\dfrac{T \vdash u \quad T \vdash v}{T \vdash \langle u, v \rangle}$
Unpairing (*UL*)	$\dfrac{T \vdash \langle u, v \rangle}{T \vdash u}$	*Unpairing* (*UR*)	$\dfrac{T \vdash \langle u, v \rangle}{T \vdash v}$
Encryption (*E*)	$\dfrac{T \vdash u \quad T \vdash v}{T \vdash \{u\}_v}$	*Decryption* (*D*)	$\dfrac{T \vdash \{u\}_v \quad T \vdash v^{-1}}{T \vdash u}$

$\hookrightarrow$ **Perfect Cryptography Assumption**

no way to obtain knowledge about u from $\{u\}_v$ without knowing v^{-1}

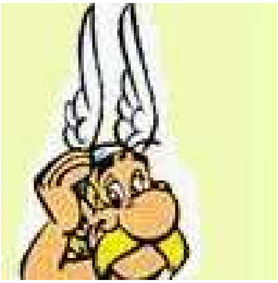
Needham-Schroeder's Protocol (1978)

- $A \rightarrow B: \{A, N_a\}_{pub(B)}$

  $B \rightarrow A: \{N_a, N_b\}_{pub(A)}$

  $A \rightarrow B: \{N_b\}_{pub(B)}$

Needham-Schroeder's Protocol (1978)



$$A \longrightarrow B: \quad \{A, N_a\}_{pub(B)}$$

- $B \longrightarrow A: \quad \{N_a, N_b\}_{pub(A)}$

$$A \longrightarrow B: \quad \{N_b\}_{pub(B)}$$

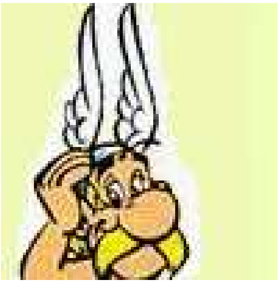
Needham-Schroeder's Protocol (1978)

$$A \rightarrow B : \{A, N_a\}_{pub(B)}$$

$$B \rightarrow A : \{N_a, N_b\}_{pub(A)}$$

- $A \rightarrow B : \{N_b\}_{pub(B)}$

Needham-Schroeder's Protocol (1978)



$$\begin{array}{rcrr} A & \rightarrow & B: & \{A, N_a\}_{pub(B)} \\ B & \rightarrow & A: & \{N_a, N_b\}_{pub(A)} \\ A & \rightarrow & B: & \{N_b\}_{pub(B)} \end{array}$$

Questions

- Is N_b secret between A and B ?
- When B receives $\{N_b\}_{pub(B)}$, does this message really comes from A ?

Needham-Schroeder's Protocol (1978)

$$\begin{array}{rcrr} A & \rightarrow & B: & \{A, N_a\}_{pub(B)} \\ B & \rightarrow & A: & \{N_a, N_b\}_{pub(A)} \\ A & \rightarrow & B: & \{N_b\}_{pub(B)} \end{array}$$

Questions

- Is N_b secret between A and B ?
- When B receives $\{N_b\}_{pub(B)}$, does this message really comes from A ?

An attack was found 17 years after its publication ! [Lowe 96]

Roadmap of the Talk

I) Secrecy Problem

- Results in the Dolev-Yao Intruder Model
- Relaxing the Perfect Cryptographic Assumption

II) My Contribution: How to Get Rid of Algebraic Properties?

- Motivations
- Finite Variant Property, Boundedness Property
- Proving Boundedness

Roadmap of the Talk

I) Secrecy Problem
- Results in the Dolev-Yao Intruder Model
- Relaxing the Perfect Cryptographic Assumption

II) My Contribution: How to Get Rid of Algebraic Properties?
- Motivations
- Finite Variant Property, Boundedness Property
- Proving Boundedness

Secrecy Problem (Example)

Protocol rules $\mathcal{P}$

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

Secrecy Problem (Example)

Protocol rules $\mathcal{P}$

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

Intruder theory $\mathcal{I}$

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

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

Secrecy Problem (Example)

Equational theory E

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

Protocol rules $\mathcal{P}$

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

Intruder theory $\mathcal{I}$

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

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

Secrecy Problem (Example)

Equational theory E

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

Protocol rules $\mathcal{P}$

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

Intruder theory $\mathcal{I}$

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

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

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

Secrecy Problem (Example)

Equational theory E

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

Protocol rules $\mathcal{P}$

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

Intruder theory $\mathcal{I}$

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

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

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

$$\mathrm{enc}(s, k1) \quad k2$$

Secrecy Problem (Example)

Equational theory E

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

Protocol rules $\mathcal{P}$

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

Intruder theory $\mathcal{I}$

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

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

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

$$\frac{\mathrm{enc}(s,k1) \quad k2}{\mathrm{enc}(\mathrm{enc}(s,k1),k2)}$$

Secrecy Problem (Example)

Equational theory E

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

Protocol rules $\mathcal{P}$

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

Intruder theory $\mathcal{I}$

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

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

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

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

Secrecy Problem (Example)

Equational theory E

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

Protocol rules $\mathcal{P}$

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

Intruder theory $\mathcal{I}$

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

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

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

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

$$=_E$$

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

Secrecy Problem (Example)

Equational theory E

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

Protocol rules $\mathcal{P}$

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

Intruder theory $\mathcal{I}$

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

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

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

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

$$=_E$$

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

Secrecy Problem (Example)

Equational theory E

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

Protocol rules $\mathcal{P}$

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

Intruder theory $\mathcal{I}$

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

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

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

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

$$=_E$$

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

$$=_E$$

$$s$$

Secrecy Problem

Secrecy Problem

Given a protocol $\mathcal{P}$, an intruder theory $\mathcal{I}$, an equational theory E, a secret data s and an initial intruder's knowledge T_0, does there exist a running sequence of protocol rules such that:

- at the end, the intruder's knowledge is T,
- s is deducible from T

Results in the Dolev-Yao Intruder Model

- infinite number of sessions: undecidable
- finite number of sessions: NP-complete [RT01]

Roadmap of the Talk

I) Secrecy Problem

- Results in the Dolev-Yao Intruder Model
- Relaxing the Perfect Cryptographic Assumption

II) My Contribution: How to Get Rid of Algebraic Properties?

- Motivations
- Finite Variant Property, Boundedness Property
- Proving Boundedness

New Kind of Intruder Model

Intruder = Inference System $\mathcal{I}$ + Equational Theory E

Example:

- **Inference System** $\mathcal{I}$

$$\text{Dolev-Yao Intruder Model} \quad + \quad (Xor) \quad \frac{T \vdash u \quad T \vdash v}{T \vdash u \oplus v}$$

- **Equational Theory** E

$$\begin{array}{rcll} x \oplus 0 & = & x & \text{Unit} \\ x \oplus x & = & 0 & \text{Nilpotence} \\ x \oplus (y \oplus z) & = & (x \oplus y) \oplus z & \text{Associtivity} \\ x \oplus y & = & y \oplus x & \text{Commutativity} \end{array}$$

Some Existing Results

	Secrecy Problem (finite number of sessions)
Exclusive or theory $x \oplus x = 0$ $x \oplus 0 = x$ + Assoc. and Commut. of $\oplus$	Decidable / NP-complete [CLS03] / [CKRT03]
Abelian group theory $x \times I(x) = 1$ $x \times 1 = x$ + Assoc. and Commut. of $\times$	Decidable [Shm04]
Diffie-Hellman theory $exp(x, 1) = x$ $exp(exp(x, y), z) = exp(x, y \times z)$ + Abelian group for $\times$	Decidable / NP-complete [Shm04] /[CKRT03]

Roadmap of the Talk

I) Secrecy Problem

- Results in the Dolev-Yao Intruder Model
- Relaxing the Perfect Cryptographic Assumption

II) My Contribution: How to Get Rid of Algebraic Properties?

- Motivations
- Finite Variant Property, Boundedness Property
- Proving Boundedness

Motivation

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':

- secrecy problem
- disunification problem

Motivation: Example

Equational theory E

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

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

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

Motivation: Example

Equational theory E

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

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

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

Motivation: Example

Equational theory E

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

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

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

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

Motivation: Example

Equational theory E

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

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

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

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

Motivation: Example

Equational theory E

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

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

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

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

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

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

Motivation: Example

Equational theory E

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

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

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

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

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

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

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

Roadmap of the Talk

I) Secrecy Problem

- Results in the Dolev-Yao Intruder Model
- Relaxing the Perfect Cryptographic Assumption

II) My Contribution: How to Get Rid of Algebraic Properties?

- Motivations
- Finite Variant Property, Boundedness Property
- Proving Boundedness

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:

$$\mathcal{R} = \{\ \mathrm{dec}(\mathrm{enc}(x,y),y) \ \rightarrow \ x\ \} \qquad\qquad E' = \emptyset$$

Let $t = \mathrm{dec}(x, k_1)$ and $\sigma = \{x \mapsto \mathrm{enc}(z, k_1)\}$.

- $t\sigma = \mathrm{dec}(\mathrm{enc}(z, k_1), k_1) \rightarrow_{\mathcal{R}} z \quad \Rightarrow \quad z$ is a variant of t,
- $\forall\sigma, t\sigma\downarrow = z\theta$ 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** (typically AC)

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

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

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** (typically AC)

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

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

Example:

$$\mathcal{R} = \{\ \mathrm{dec}(\mathrm{enc}(x, y), y) \quad \rightarrow \quad x\ \} \qquad\qquad E' = \emptyset$$

$$t = \mathrm{dec}(x, k_1)$$

Roadmap of the Talk

I) Secrecy Problem

- Results in the Dolev-Yao Intruder Model
- Relaxing the Perfect Cryptographic Assumption

II) My Contribution: How to Get Rid of Algebraic Properties?

- Motivations
- Finite Variant Property, Boundedness Property
- Proving Boundedness

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.

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

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.

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

Key Inverse Theory (KIT)
The equations of DYT extending by:

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

Abelian Group Theory (1)

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

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 $\mathcal{AG}$:

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

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

Problem

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

Counter-Example

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

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

Abelian Group Theory (2)

Unusual Presentation of $\mathcal{AG}$: $\mathcal{R}'_\times$ [Lankford]

$$
\begin{array}{rcl}
x \times 1 & \to & x \\
1^{-1} & \to & 1 \\
x \times x^{-1} & \to & 1 \\
x^{-1} \times y^{-1} & \to & (x \times y)^{-1} \\
(x \times y)^{-1} \times y & \to & x^{-1}
\end{array}
\qquad
\begin{array}{rcl}
{x^{-1}}^{-1} & \to & x \\
(x^{-1} \times y)^{-1} & \to & x \times y^{-1} \\
x \times (x^{-1} \times y) & \to & y \\
x^{-1} \times (y^{-1} \times z) & \to & (x \times y)^{-1} \times z \\
(x \times y)^{-1} \times (y \times z) & \to & x^{-1} \times z
\end{array}
$$

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

Abelian Group Theory (2)

Unusual Presentation of $\mathcal{AG}$: $\mathcal{R}'_\times$ [Lankford]

$$
\begin{array}{rcl}
x \times 1 & \rightarrow & x \\
1^{-1} & \rightarrow & 1 \\
x \times x^{-1} & \rightarrow & 1 \\
x^{-1} \times y^{-1} & \rightarrow & (x \times y)^{-1} \\
(x \times y)^{-1} \times y & \rightarrow & x^{-1}
\end{array}
\qquad
\begin{array}{rcl}
{x^{-1}}^{-1} & \rightarrow & x \\
(x^{-1} \times y)^{-1} & \rightarrow & x \times y^{-1} \\
x \times (x^{-1} \times y) & \rightarrow & y \\
x^{-1} \times (y^{-1} \times z) & \rightarrow & (x \times y)^{-1} \times z \\
(x \times y)^{-1} \times (y \times z) & \rightarrow & x^{-1} \times z
\end{array}
$$

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

$\Rightarrow$ $(\mathcal{R}'_\times, AC)$ 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 $\Rightarrow$ $f(t_1, \ldots, t_n) \xrightarrow{\leq c_f}_{E' \setminus \mathcal{R}} f(t_1, \ldots, t_n)\!\downarrow$
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:

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

Others Equational Theories

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

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

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

Others Equational Theories

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

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

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

Presentation of the Xor Theory *ACUN*

$$\mathcal{R}_{+} = \left\{ \begin{array}{rcl} x+0 & \to & x \\ x+x & \to & 0 \\ x+(x+y) & \to & y \end{array} \right\}$$

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

Conclusion & Future Works

Conclusion

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

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

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

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

  $\Rightarrow$ solve the secrecy problem by reducing it to AC

Conclusion & Future Works

Conclusion

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

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

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

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

$\Rightarrow$ solve the secrecy problem by reducing it to AC

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 secrecy problem.