

Verification of cryptographic protocols with algebraic properties

Stéphanie Delaune

France Télécom R&D,

Laboratoire Spécification et Vérification, CNRS & INRIA & ENS Cachan

June 20, 2006



Cryptographic protocols

- small programs designed to **secure** communication
- use **cryptographic primitives** (e.g. encryption, hash function, . . .)

Cryptographic protocols

- small programs designed to **secure** communication
- use **cryptographic primitives** (e.g. encryption, hash function, ...)



Symmetric encryption



Cryptographic primitives

Symmetric encryption



Asymmetric encryption



How cryptographic protocols can be attacked?

Breaking encryption



How cryptographic protocols can be attacked?

Breaking encryption



Logical attack



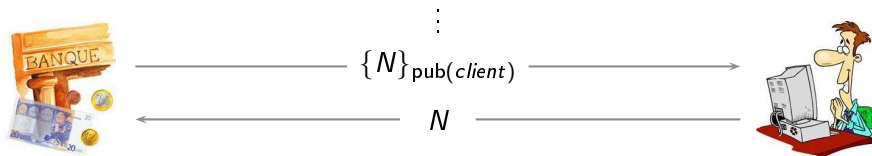
Logical attacks - What is it?

Electronic bank transfer



Logical attacks - What is it?

Electronic bank transfer



Logical attacks - What is it?

Electronic bank transfer



— $\{N\}_{\text{pub}(\text{client})}$ →



Logical attacks - What is it?

Electronic bank transfer



Logical attacks - What is it?

Electronic bank transfer



Logical attacks - What is it?

Electronic bank transfer



Logical attacks

- can be mounted even assuming **perfect** cryptography,
↪ **replay attack**, **man-in-the middle attack**, ...
- are **numerous**, see SPORE, Security Protocols Open REpository
↪ <http://www.lsv.ens-cachan.fr/spore/>
- **subtle** and **hard to detect** by “eyeballing” the protocol

Symbolic approach

- **messages** are represented by **terms** rather than bit-strings
 - ↦ $\{m\}_k$ encryption of the message m with key k ,
 - ↦ $\langle m_1, m_2 \rangle$ pairing of messages m_1 and m_2 , ...
- **attacker** controls the network and can perform **specific actions**

Symbolic approach

- **messages** are represented by **terms** rather than bit-strings
 - ↦ $\{m\}_k$ encryption of the message m with key k ,
 - ↦ $\langle m_1, m_2 \rangle$ pairing of messages m_1 and m_2 , ...
- **attacker** controls the network and can perform **specific actions**

Relevance of the approach

- **numerous** attacks have already been obtained,
- **soundness results** already exist, e.g. [Micciancio & Warinschi'04]
- allows us to perform **automatic** verification

Difficulties of the verification

Presence of an attacker ...



Presence of an attacker ...

who controls the communication network:

- may **read** every message sent on the network
- may **intercept** and **send** new messages



Presence of an attacker ...

who controls the communication network:

- may **read** every message sent on the network
- may **intercept** and **send** new messages



who has deduction capabilities (e.g. the standard Dolev-Yao model)

- encryption, decryption if he knows the decryption key,
- pairing, projection

Presence of an attacker ...

who controls the communication network:

- may **read** every message sent on the network
- may **intercept** and **send** new messages



who has deduction capabilities (*e.g.* the standard Dolev-Yao model)

- encryption, decryption if he knows the decryption key,
- pairing, projection

Security problem for an **unbounded** number of sessions is **undecidable**.

Presence of an attacker ...

who controls the communication network:

- may **read** every message sent on the network
- may **intercept** and **send** new messages



who has deduction capabilities (*e.g.* the standard Dolev-Yao model)

- encryption, decryption if he knows the decryption key,
- pairing, projection

Security problem for a **fixed** number of sessions is **decidable**.

Why?

- some **attacks are missed** when cryptographic primitives are **abstracted** as perfect black boxes.
Example: WEP protocol
- the **executability** of some protocols relies explicitly on **algebraic properties**.

Why?

- some **attacks are missed** when cryptographic primitives are **abstracted** as perfect black boxes.
Example: WEP protocol
- the **executability** of some protocols relies explicitly on **algebraic properties**.

How to take into account algebraic properties?

- 1 by modelling algebraic properties as an **equational theory E**,
- 2 by **extending** the deduction capabilities of the attacker

Some existing results

In 2003, results are **numerous** but deal with a **particular** equational theory.

Dolev-Yao ($E = \emptyset$)

[Amadio & Lugiez, 00], [Rusinowitch & Turuani, 01]

Exclusive or

[Comon & Shmatikov, 03], [Chevalier *et al.*, 03], [Comon & Cortier, 03]

Abelian group

[Comon & Shmatikov, 03], [Millen & Shmatikov, 03]

CBC encryption

[Chevalier *et al.*, 03]

...

Electronic purse protocol

EP



$(\text{priv}, \text{pub}) = (s, b^s)$

choose a ticket (n, b^n)

⋮



Server

Electronic purse protocol

EP



$(\text{priv}, \text{pub}) = (s, b^s)$

choose a ticket (n, b^n) \longrightarrow $\text{hash}(b^n, \text{Msg}) \longrightarrow$

⋮



Server

Electronic purse protocol

EP



$(\text{priv}, \text{pub}) = (s, b^s)$

choose a ticket (n, b^n) $\xrightarrow{\text{hash}(b^n, \text{Msg})}$

debit

\xleftarrow{c}

⋮



Server

Electronic purse protocol

EP



$(priv, pub) = (s, b^s)$

choose a ticket (n, b^n)

⋮

→ hash(b^n, Msg) →

← c ←

debit

→ $\underbrace{n - s \times c}_y, Msg$ →

$(b^s)^c \times b^{n-s \times c} \stackrel{?}{=} b^n$
 credit
 ⋮



Server

Electronic purse protocol

EP



$$(\text{priv}, \text{pub}) = (s, b^s)$$

choose a ticket (n, b^n)

$$\text{hash}(b^n, \text{Msg}) \longrightarrow$$

$$\longleftarrow c$$

debit

$$\text{Msg} \longrightarrow \underbrace{n - s \times c}_y$$

$$(b^s)^c \times b^{n-s \times c} \stackrel{?}{=} b^n$$

credit

⋮



Server

Equational theory

$$\text{AG} \left\{ \begin{array}{l} x + (y + z) = (x + y) + z \\ x + y = y + x \\ x + 0 = x \\ x + -(x) = 0 \end{array} \right. \quad \text{AC} \left\{ \begin{array}{l} x \times (y \times z) = (x \times y) \times z \\ x \times y = y \times x \\ b(x + y) = b(x) \times b(y) \\ \exp(b(x), y) = b(x \times y) \end{array} \right.$$

Generic results

- Decision procedures for **public-collapsing theories**
 - ↪ allowing us to deal with variants of the Dolev-Yao model
- The **finite variant property**
 - ↪ allowing us to get rid of some algebraic properties

Particular equational theories: ACUNh and AGh

- **Passive attacker**: **PTIME** decision procedure
 - ↪ improving existing results
 - ↪ allowing us to deal with active case
- **Active attacker**: **decidability** and **undecidability** results

1 Modelisation

- Passive attacker: intruder deduction problem
- Active attacker: insecurity problem (bounded number of sessions)

2 Verification

- Public-collapsing equational theories
- How to deal with more complex equational theories?
- Some particular equational theories: ACh, ACUNh et AGh

1 Modelisation

- Passive attacker: intruder deduction problem
- Active attacker: insecurity problem (bounded number of sessions)

2 Verification

- Public-collapsing equational theories
- How to deal with more complex equational theories?
- Some particular equational theories: ACh, ACUNh et AGh

Dolev-Yao inference system – \mathcal{I}_{DY}

$$\frac{u \in \mathcal{T}}{T \vdash u} \quad (\text{A})$$

$$\frac{T \vdash u_1 \ \dots \ T \vdash u_n}{T \vdash f(u_1, \dots, u_n)} \text{ with } f \in \mathcal{VF} \quad (\text{C})$$

$$\frac{T \vdash \langle u, v \rangle}{T \vdash u} \quad (\text{Proj}_1)$$

$$\frac{T \vdash \langle u, v \rangle}{T \vdash v} \quad (\text{Proj}_2)$$

$$\frac{T \vdash \{u\}_v \quad T \vdash v^{-1}}{T \vdash u} \quad (\text{D})$$

Modelisation of the intruder

Dolev-Yao inference system – \mathcal{I}_{DY}

$$\frac{u \in \mathcal{T}}{T \vdash u} \quad (\text{A})$$

$$\frac{T \vdash u_1 \ \dots \ T \vdash u_n}{T \vdash f(u_1, \dots, u_n)} \text{ with } f \in \mathcal{VF} \quad (\text{C})$$

$$\frac{T \vdash \langle u, v \rangle}{T \vdash u} \quad (\text{Proj}_1)$$

$$\frac{T \vdash \langle u, v \rangle}{T \vdash v} \quad (\text{Proj}_2)$$

$$\frac{T \vdash \{u\}_v \quad T \vdash v^{-1}}{T \vdash u} \quad (\text{D})$$

$$(\text{Eq}) \quad \frac{T \vdash u}{T \vdash v} \quad u =_{\mathbf{E}} v$$

Modelisation of the intruder

Dolev-Yao inference system – \mathcal{I}_{DY}

$$\frac{u \in \mathcal{T}}{T \vdash u} \quad (\text{A})$$

$$\frac{T \vdash u_1 \ \dots \ T \vdash u_n}{T \vdash f(u_1, \dots, u_n)} \text{ with } f \in \mathcal{VF} \quad (\text{C})$$

$$\frac{T \vdash \langle u, v \rangle}{T \vdash u} \quad (\text{Proj}_1)$$

$$\frac{T \vdash \langle u, v \rangle}{T \vdash v} \quad (\text{Proj}_2)$$

$$\frac{T \vdash \{u\}_v \quad T \vdash v^{-1}}{T \vdash u} \quad (\text{D})$$

$$(\text{Eq}) \quad \frac{T \vdash u}{T \vdash v} \quad u =_{\mathbf{E}} v$$

Notation: $(\mathcal{I}, \mathbf{E})$ denote the inference system made up of:

- the inference rules of \mathcal{I} , and
- the rule (Eq) for the equational theory \mathbf{E}

Intruder deduction problem (ID)

Let \mathcal{I} be an inference system and \mathcal{E} an equational theory.

INPUT: a finite set of terms T , a term s (the secret).

OUTPUT: Does there exist a proof of $T \vdash s$ in $(\mathcal{I}, \mathcal{E})$?

Intruder deduction problem (ID)

Let \mathcal{I} be an inference system and \mathbf{E} an equational theory.

INPUT: a finite set of terms T , a term s (the secret).

OUTPUT: Does there exist a proof of $T \vdash s$ in $(\mathcal{I}, \mathbf{E})$?

Example:

$$\mathcal{I} = \mathcal{I}_{\text{DY}}$$

$$\mathbf{E} = \{ \{ \{ x \}_y \}_z = \{ \{ x \}_z \}_y \}$$

$$T = \{ \{ \{ a \}_{k_1}, k_2 \}$$

$$s = \{ \{ a \}_{k_2} \}_{k_1}$$

$$\frac{\frac{\{ a \}_{k_1} \in T}{T \vdash \{ a \}_{k_1}} \text{(A)} \quad \frac{k_2 \in T}{T \vdash k_2} \text{(A)}}{T \vdash \{ \{ a \}_{k_1} \}_{k_2}} \text{(C)} \\ \frac{}{T \vdash \{ \{ a \}_{k_2} \}_{k_1}} \text{(Eq)}$$

1 Modelisation

- Passive attacker: intruder deduction problem
- Active attacker: insecurity problem (bounded number of sessions)

2 Verification

- Public-collapsing equational theories
- How to deal with more complex equational theories?
- Some particular equational theories: ACh, ACUNh et AGh

Denning-Sacco protocol

$A \rightarrow B : \langle A, \{ \{ \langle B, K \rangle \}_{\text{priv}(A)} \}_{\text{pub}(B)} \rangle$

$B \rightarrow A : \{ S \}_K$

Denning-Sacco protocol

$$A \rightarrow B : \langle A, \{ \{ \langle B, K \rangle \}_{\text{priv}(A)} \}_{\text{pub}(B)} \rangle$$
$$B \rightarrow A : \{ S \}_K$$

Modelisation with pattern-matching – $E = \emptyset$

$$R_B(z_B) := \nu s . \text{recv}(\langle x_A, \{ \{ \langle z_B, x_K \rangle \}_{\text{priv}(x_A)} \}_{\text{pub}(z_B)} \rangle);$$
$$\text{send}(\{ s \}_{x_K})$$

Denning-Sacco protocol

$$A \rightarrow B : \langle A, \{\{\langle B, K \rangle\}_{\text{priv}(A)}\}_{\text{pub}(B)} \rangle$$
$$B \rightarrow A : \{S\}_K$$

Modelisation with pattern-matching – $E = \emptyset$

$$R_B(z_B) := \nu s . \text{recv}(\langle x_A, \{\{\langle z_B, x_K \rangle\}_{\text{priv}(x_A)}\}_{\text{pub}(z_B)} \rangle);$$
$$\text{send}(\{s\}_{x_K})$$

Modelisation with equality tests

$$E = \begin{cases} \text{dec}(\{x\}_{\text{pub}(y)}, \text{priv}(y)) = x \\ \text{proj}_i(\langle x_1, x_2 \rangle) = x_i & i = 1, 2 \\ \dots \end{cases}$$

$$R_B(z_B) := \nu s . \text{recv}(x);$$
$$z_B = \text{proj}_1(\text{dec}(\text{dec}(\text{proj}_2(x), \text{priv}(z_B)), \text{pub}(\text{proj}_1(x))));$$
$$\text{send}(\{s\}_{\text{proj}_2(\text{dec}(\text{dec}(\text{proj}_2(x), \text{priv}(z_B)), \text{pub}(\text{proj}_1(x))))})$$

Modelisation with equality tests

- allows us to consider inference system **without pattern-matching**

$$\frac{T \vdash x_1 \quad \dots \quad T \vdash x_n}{T \vdash f(x_1, \dots, x_n)} \quad f \in \mathcal{VF} \qquad \frac{T \vdash u}{T \vdash v} \quad u =_{\mathbf{E}} v$$

Modelisation with equality tests

- allows us to consider inference system **without pattern-matching**

$$\frac{T \vdash x_1 \quad \dots \quad T \vdash x_n}{T \vdash f(x_1, \dots, x_n)} \quad f \in \mathcal{VF} \qquad \frac{T \vdash u}{T \vdash v} \quad u =_{\mathbf{E}} v$$

- equality tests allow us to model some protocols in a more **natural way** (e.g. Electronic purse)

Modelisation with equality tests

- allows us to consider inference system **without pattern-matching**

$$\frac{T \vdash x_1 \quad \dots \quad T \vdash x_n}{T \vdash f(x_1, \dots, x_n)} \quad f \in \mathcal{VF} \qquad \frac{T \vdash u}{T \vdash v} \quad u =_{\mathbf{E}} v$$

- equality tests allow us to model some protocols in a more **natural way** (e.g. Electronic purse)

↔ Equality tests **can** easily **be encoded** by using **pattern-matching**

Modelisation with equality tests

- allows us to consider inference system **without pattern-matching**

$$\frac{T \vdash x_1 \quad \dots \quad T \vdash x_n}{T \vdash f(x_1, \dots, x_n)} \quad f \in \mathcal{VF} \qquad \frac{T \vdash u}{T \vdash v} \quad u =_{\mathbf{E}} v$$

- equality tests allow us to model some protocols in a more **natural way** (e.g. Electronic purse)

↔ Equality tests **can** easily **be encoded** by using **pattern-matching**

Modelisation with pattern-matching seems to be **more expressive**.

Examples: Let $+$ be an associative and commutative operator

- $\text{recv}(x + x); \text{send}(x), \quad \text{recv}(x + x + x); \text{send}(x), \dots$
- $\text{recv}(x + \{x\}_k); \text{send}(x)$

Insecurity problem (bounded number of sessions)

Let \mathcal{I} be an inference system and \mathbf{E} an equational theory.

INPUT: a finite set R_1, \dots, R_m of instances of roles,
a finite set T_0 of terms (initial intruder knowledge),
a term s (the secret)

OUTPUT: Does there exist an **interleaving** of R_1, \dots, R_m
runnable from T_0 in $(\mathcal{I}, \mathbf{E})$ at the end of which

- the intruder knowledge is T , and
- $T \vdash s$ in $(\mathcal{I}, \mathbf{E})$?

Security properties (**trace properties**): *e.g.* secrecy, some kinds of authentication properties, ...

System of deducibility constraints with pattern-matching

recv(u_1); send(v_1)
...
recv(u_n); send(v_n)

$$\mathcal{C} = \left\{ \begin{array}{l} T_0 \Vdash u_1 \\ \dots \\ T_0, v_1, \dots, v_n \Vdash s \end{array} \right.$$

System of deducibility constraints with pattern-matching

$$\begin{array}{l} \text{recv}(u_1); \text{send}(v_1) \\ \dots \\ \text{recv}(u_n); \text{send}(v_n) \end{array} \quad \mathcal{C} = \left\{ \begin{array}{l} T_0 \Vdash u_1 \\ \dots \\ T_0, v_1, \dots, v_n \Vdash s \end{array} \right.$$

System of simple deducibility constraints with equality tests

$$\begin{array}{l} \text{recv}(x_1); \mathcal{E}_1; \text{send}(v_1) \\ \dots \\ \text{recv}(x_n); \mathcal{E}_n; \text{send}(v_n) \end{array} \quad \mathcal{C} = \left\{ \begin{array}{l} T_0 \Vdash x_1 \\ \dots \\ T_0, v_1, \dots, v_n \Vdash x_{n+1} \end{array} \right. \wedge \begin{array}{l} \mathcal{E}_1 \\ \dots \\ x_{n+1} = s \end{array}$$

System of deducibility constraints with pattern-matching

$$\begin{array}{l} \text{recv}(u_1); \text{send}(v_1) \\ \dots \\ \text{recv}(u_n); \text{send}(v_n) \end{array} \quad \mathcal{C} = \left\{ \begin{array}{l} T_0 \Vdash u_1 \\ \dots \\ T_0, v_1, \dots, v_n \Vdash s \end{array} \right.$$

System of simple deducibility constraints with equality tests

$$\begin{array}{l} \text{recv}(x_1); \mathcal{E}_1; \text{send}(v_1) \\ \dots \\ \text{recv}(x_n); \mathcal{E}_n; \text{send}(v_n) \end{array} \quad \mathcal{C} = \left\{ \begin{array}{l} T_0 \Vdash x_1 \\ \dots \\ T_0, v_1, \dots, v_n \Vdash x_{n+1} \end{array} \right. \quad \wedge \quad \begin{array}{l} \mathcal{E}_1 \\ \dots \\ x_{n+1} = s \end{array}$$

Solution of a constraint system in $(\mathcal{I}, \mathcal{E})$

A substitution σ such that:

- for every $T \Vdash u \in \mathcal{C}$, $T\sigma \vdash u\sigma$ in $(\mathcal{I}, \mathcal{E})$
- for every $u = v \in \mathcal{C}$, $u\sigma =_{\mathcal{E}} v\sigma$

System of deducibility constraints with pattern-matching

$$\begin{array}{l} \text{recv}(u_1); \text{send}(v_1) \\ \dots \\ \text{recv}(u_n); \text{send}(v_n) \end{array} \quad \mathcal{C} = \left\{ \begin{array}{l} T_0 \Vdash u_1 \\ \dots \\ T_0, v_1, \dots, v_n \Vdash s \end{array} \right.$$

System of simple deducibility constraints with equality tests

$$\begin{array}{l} \text{recv}(x_1); \mathcal{E}_1; \text{send}(v_1) \\ \dots \\ \text{recv}(x_n); \mathcal{E}_n; \text{send}(v_n) \end{array} \quad \mathcal{C} = \left\{ \begin{array}{l} T_0 \Vdash x_1 \\ \dots \\ T_0, v_1, \dots, v_n \Vdash x_{n+1} \end{array} \right. \wedge \begin{array}{l} \mathcal{E}_1 \\ \dots \\ x_{n+1} = s \end{array}$$

Well-formed constraint system

- **monotonicity**: intruder never forgets information
- **origination** stable by **substitution** and **normalisation**: due to the fact that we consider “deterministic” protocols

1 Modelisation

- Passive attacker: intruder deduction problem
- Active attacker: insecurity problem (bounded number of sessions)

2 Verification

- Public-collapsing equational theories
- How to deal with more complex equational theories?
- Some particular equational theories: ACh, ACUNh et AGh

1 Modelisation

- Passive attacker: intruder deduction problem
- Active attacker: insecurity problem (bounded number of sessions)

2 Verification

- **Public-collapsing equational theories**
- How to deal with more complex equational theories?
- Some particular equational theories: ACh, ACUNh et AGh

Definition

A **public-collapsing** equational theory is a theory that can be represented by a **convergent** rewriting system \mathcal{R} and each rule $\ell \rightarrow r \in \mathcal{R}$ satisfies:

- 1 r is a **variable** or a **ground term**,
- 2 if $\text{head}(\ell) \in \mathcal{VF}$, then under each public symbol in ℓ , there is r .

Examples:

- **Dolev-Yao**: $\text{dec}(\{x\}_y)y = x$, $\text{proj}_i(\langle x_1, x_2 \rangle) = x_i$ ($i = 1, 2$)
- **Asymmetric encryption**: $\text{dec}(\{x\}_y, y^{-1}) = x$, $x^{-1^{-1}} = x$
- **Inverse-key**: $\{\text{dec}(x, y)\}_y = x$
- **Probabilistic encryption**: $\text{dec}(\text{enc}(x, y, z), y) = x$
- ...

Let $\mathcal{I}_{\mathcal{V}\mathcal{F}}$ be an inference system and \mathbf{E} a public-collapsing equational theory.

Theorem (intruder deduction problem)

ID is decidable in *polynomial time* for the inference system $(\mathcal{I}_{\mathcal{V}\mathcal{F}}, \mathbf{E})$.

Let $\mathcal{I}_{\mathcal{V}\mathcal{F}}$ be an inference system and \mathbf{E} a public-collapsing equational theory.

Theorem (intruder deduction problem)

*ID is decidable in **polynomial time** for the inference system $(\mathcal{I}_{\mathcal{V}\mathcal{F}}, \mathbf{E})$.*

Theorem (insecurity problem)

*The problem of the satisfiability of a simple and well-formed constraint system with equality tests in $(\mathcal{I}_{\mathcal{V}\mathcal{F}}, \mathbf{E})$ is **NP-complete**.*

1 Modelisation

- Passive attacker: intruder deduction problem
- Active attacker: insecurity problem (bounded number of sessions)

2 Verification

- Public-collapsing equational theories
- How to deal with more complex equational theories?
- Some particular equational theories: ACh, ACUNh et AGh

The finite variant property

Goal

This property allows us (for many equational theories):

- to **get rid** of some algebraic properties,
- to **reduce** the equational theory to the **empty theory** or **AC**.

The finite variant property

Goal

This property allows us (for many equational theories):

- to **get rid** of some algebraic properties,
- to **reduce** the equational theory to the **empty theory** or **AC**.

How to do this ?

Given a theory E , find a splitting of E in $\mathcal{R} \uplus E'$ such that:

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

Main application

Attack on P in $(\mathcal{I}, E) \Leftrightarrow \exists P' \in \mathcal{V}ariant(P)$. **Attack** on P' in $(\mathcal{V}ariant(\mathcal{I}), E')$.

Proposition 1

If **narrowing** terminates for \mathcal{R} then (\mathcal{R}, \emptyset) has the **finite variant property**.

Examples

- public-collapsing theories,
- blind signature, $\text{unblind}(\text{sign}(\text{blind}(x, y), z), y) = \text{sign}(x, z)$

Proposition 1

If **narrowing** terminates for \mathcal{R} then (\mathcal{R}, \emptyset) has the **finite variant property**.

Examples

- public-collapsing theories,
- blind signature, $\text{unblind}(\text{sign}(\text{blind}(x, y), z), y) = \text{sign}(x, z)$

Proposition 2

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

$$t_1, \dots, t_n \text{ in normal form} \Rightarrow f(t_1, \dots, t_n) \xrightarrow{\leq c_f}_{E' \setminus \mathcal{R}} f(t_1, \dots, t_n) \downarrow$$

then (\mathcal{R}, E') satisfies the **finite variant property**.

Examples

- Exclusive or, Abelian groups, Diffie-Hellman,
- Equational theory allowing to model electronic purse.

Abelian group theory

$$\begin{array}{ll} x + -(x) = 0 & \text{(Inv)} \\ x + 0 = x & \text{(U)} \end{array} \quad \begin{array}{ll} x + (y + z) = (x + y) + z & \text{(A)} \\ x + y = y + x & \text{(C)} \end{array}$$

Abelian group theory

$$x + -(x) = 0 \quad (\text{Inv}) \quad x + (y + z) = (x + y) + z \quad (\text{A})$$

$$x + 0 = x \quad (\text{U}) \quad x + y = y + x \quad (\text{C})$$

...

$$-(x + y) = -(x) + -(y)$$

Abelian group theory

$$x + -(x) \rightarrow 0 \quad (\text{Inv}) \quad x + (y + z) = (x + y) + z \quad (\text{A})$$

$$x + 0 \rightarrow x \quad (\text{U}) \quad x + y = y + x \quad (\text{C})$$

...

$$-(x + y) \rightarrow -(x) + -(y)$$

Abelian group theory

$$\begin{array}{ll} x + -(x) \rightarrow 0 & \text{(Inv)} \\ x + 0 \rightarrow x & \text{(U)} \end{array} \quad \begin{array}{ll} x + (y + z) = (x + y) + z & \text{(A)} \\ x + y = y + x & \text{(C)} \end{array}$$

...

$$-(x + y) \leftarrow -(x) + -(y)$$

Proposition

- 1 This rewrite system \mathcal{R} is AC-convergent
- 2 (\mathcal{R}, AC) satisfies the **finite variant property**

Abelian group theory

$$\begin{array}{ll} x + -(x) \rightarrow 0 & \text{(Inv)} \\ x + 0 \rightarrow x & \text{(U)} \end{array} \quad \begin{array}{ll} x + (y + z) = (x + y) + z & \text{(A)} \\ x + y = y + x & \text{(C)} \end{array}$$

...

$$-(x + y) \leftarrow -(x) + -(y)$$

Proposition

- 1 This rewrite system \mathcal{R} is AC-convergent
- 2 (\mathcal{R}, AC) satisfies the **finite variant property**

Proof (Proposition 2). Let t_1 and t_2 be terms in normal form, we have

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

$$x + 0 = x \quad (\text{U})$$

$$x + x = 0 \quad (\text{N})$$

$$h(x + y) = h(x) + h(y) \quad (\text{h})$$

$$x + (x + z) = (x + y) + z \quad (\text{A})$$

$$x + y = y + x \quad (\text{C})$$

$$x + 0 \rightarrow x$$

$$x + x \rightarrow 0$$

$$x + x + y \rightarrow y$$

$$h(0) \rightarrow 0$$

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

$$\mathcal{R}_2 : h(x) + h(y) \rightarrow h(x + y)$$

$$h(x) + h(y) + z \rightarrow h(x + y) + z$$

$$x + 0 \rightarrow x$$

$$x + x \rightarrow 0$$

$$x + x + y \rightarrow y$$

$$h(0) \rightarrow 0$$

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

$$\mathcal{R}_2 : h(x) + h(y) \rightarrow h(x + y)$$

$$h(x) + h(y) + z \rightarrow h(x + y) + z$$

Remark

(\mathcal{R}_1, AC) and (\mathcal{R}_2, AC) do **not** satisfy the **finite variant property**

$$x + 0 \rightarrow x$$

$$x + x \rightarrow 0$$

$$x + x + y \rightarrow y$$

$$h(0) \rightarrow 0$$

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

$$\mathcal{R}_2 : h(x) + h(y) \rightarrow h(x + y)$$

$$h(x) + h(y) + z \rightarrow h(x + y) + z$$

Remark

(\mathcal{R}_1, AC) and (\mathcal{R}_2, AC) do **not** satisfy the **finite variant property**

Proposition

There is **no** decomposition of ACUNh having the **finite variant property**.

1 Modelisation

- Passive attacker: intruder deduction problem
- Active attacker: insecurity problem (bounded number of sessions)

2 Verification

- Public-collapsing equational theories
- How to deal with more complex equational theories?
- Some particular equational theories: ACh, ACUNh et AGh

Intruder deduction problem [Lafourcade *et al.*, 05]

ACh	ACUNh	AGh
NP-complete	EXPTIME	

→ PTIME in the **binary case**

Insecurity problem (bounded number of sessions)

ACh	ACUNh	AGh
Undecidable	?	?

Intruder deduction problem in (\mathcal{I}, E)

Let T be a set of terms and u a term.

- 1 An **effective inference system** (\mathcal{I}', E') such that:

$$T \vdash u \text{ in } (\mathcal{I}, E) \Leftrightarrow T \vdash u \text{ in } (\mathcal{I}', E')$$

- 2 A **locality** result (notion due to [Mc Allester, 1993](#)), i.e.:
A minimal proof P of $T \vdash u$ contains only terms in $St_E(T \cup \{u\})$.
- 3 A **one-step deducibility** result:
→ to ensure that we can test that a deduction step is valid

How to deal with homomorphism ?

Approach of Lafourcade et al. 2005

$$\frac{T \vdash u}{T \vdash h(u) \downarrow} \qquad \frac{T \vdash u_1 \dots T \vdash u_n}{T \vdash (u_1 + \dots + u_n) \downarrow}$$

How to deal with homomorphism ?

Approach of Lafourcade et al. 2005

$$\frac{T \vdash u}{T \vdash h(u)\downarrow} \qquad \frac{T \vdash u_1 \dots T \vdash u_n}{T \vdash (u_1 + \dots + u_n)\downarrow}$$

- **advantage:** **one-step deducibility**, easy to prove
- **drawback:** **locality**, hard to prove for a “good” notion of subterms

How to deal with homomorphism ?

Approach of Lafourcade et al. 2005

$$\frac{T \vdash u}{T \vdash h(u)\downarrow} \quad \frac{T \vdash u_1 \dots T \vdash u_n}{T \vdash (u_1 + \dots + u_n)\downarrow}$$

- **advantage:** one-step deducibility, easy to prove
- **drawback:** locality, hard to prove for a “good” notion of subterms

My approach

$$(M_E) \frac{T \vdash u_1 \dots T \vdash u_n}{T \vdash C[u_1, \dots, u_n]\downarrow} \text{ with } C \text{ an E-context}$$

How to deal with homomorphism ?

Approach of Lafourcade et al. 2005

$$\frac{T \vdash u}{T \vdash h(u) \downarrow} \quad \frac{T \vdash u_1 \dots T \vdash u_n}{T \vdash (u_1 + \dots + u_n) \downarrow}$$

- **advantage:** **one-step deducibility**, easy to prove
- **drawback:** **locality**, hard to prove for a “good” notion of subterms

My approach

$$(M_E) \frac{T \vdash u_1 \dots T \vdash u_n}{T \vdash C[u_1, \dots, u_n] \downarrow} \text{ with } C \text{ an E-context}$$

- **advantage:** **locality**, easy to prove
- **drawback:** **one-step deducibility** seems difficult

How to deal with homomorphism ?

Approach of Lafourcade et al. 2005

$$\frac{T \vdash u}{T \vdash h(u) \downarrow} \quad \frac{T \vdash u_1 \dots T \vdash u_n}{T \vdash (u_1 + \dots + u_n) \downarrow}$$

- **advantage:** **one-step deducibility**, easy to prove
- **drawback:** **locality**, hard to prove for a “good” notion of subterms

My approach

$$(M_E) \frac{T \vdash u_1 \dots T \vdash u_n}{T \vdash C[u_1, \dots, u_n] \downarrow} \text{ with } C \text{ an E-context}$$

- **advantage:** **locality**, easy to prove
- **drawback:** **one-step deducibility** seems difficult

reducible to the solvability of a **system of linear equations**
over $\mathbb{N}[X]$, $\mathbb{Z}/2\mathbb{Z}[X]$ or $\mathbb{Z}[X]$

How to deal with homomorphism ?

Approach of Lafourcade et al. 2005

$$\frac{T \vdash u}{T \vdash h(u) \downarrow} \quad \frac{T \vdash u_1 \dots T \vdash u_n}{T \vdash (u_1 + \dots + u_n) \downarrow}$$

- **advantage:** **one-step deducibility**, easy to prove
- **drawback:** **locality**, hard to prove for a “good” notion of subterms

My approach

$$(M_E) \frac{T \vdash u_1 \dots T \vdash u_n}{T \vdash C[u_1, \dots, u_n] \downarrow} \text{ with } C \text{ an E-context}$$

- **advantage:** **locality**, easy to prove
- **drawback:** **one-step deducibility** seems difficult

Theorem

*ID is **P-complete** for the inference system $(\mathcal{I}_{DY}, ACUNh)$ and (\mathcal{I}_{DY}, AGh) .*

Theorem

The problem of the satisfiability of a well-formed constraint system with pattern-matching in $(\mathcal{I}_{DY}, \text{ACUNh})$ is **decidable**.

Theorem

The problem of the satisfiability of a well-formed constraint system with pattern-matching in $(\mathcal{I}_{DY}, ACUNh)$ is **decidable**.

Procedure

- 1 from constraints $(T \Vdash u)$ to **one-step constraints** $(T \Vdash_1 u)$,
↪ generalisation of the locality result
- 2 from constraints $(T \Vdash_1 u)$ to **M_E -constraints** $(T \Vdash_{M_E} u)$,
↪ unification modulo ACUNh is decidable and finitary
- 3 **abstract** subterms by constants,

Theorem

The problem of the satisfiability of a well-formed constraint system with pattern-matching in $(\mathcal{I}_{DY}, ACUNh)$ is **decidable**.

Procedure

- 1 from constraints $(T \Vdash u)$ to **one-step constraints** $(T \Vdash_1 u)$,
↪ generalisation of the locality result
- 2 from constraints $(T \Vdash_1 u)$ to **M_E -constraints** $(T \Vdash_{M_E} u)$,
↪ unification modulo ACUNh is decidable and finitary
- 3 **abstract** subterms by constants,
- 4 from M_E -constraints $(T \Vdash_{M_E} u)$ to **ground** M_E -constraints,
↪ solvability of particular systems of quadratic equations
- 5 **check** satisfaisability of ground M_E -constraints.

Theorem

The problem of the satisfiability of a well-formed constraint system with pattern-matching in $(\mathcal{I}_{DY}, \text{AGh})$ is **undecidable**.

Theorem

The problem of the satisfiability of a well-formed constraint system with pattern-matching in $(\mathcal{I}_{DY}, \text{AGh})$ is **undecidable**.

Remarks

- solvability of well-formed M_E -constraints system on the **reduced signature** is already **undecidable**,
- reduction of Hilbert's 10th problem,
- the presence of **pattern-matching is crucial** to obtain **undecidability**.

Generic Results

- Decision procedures for **public-collapsing theories**
↔ allowing us to deal with variants of the Dolev-Yao model
- The **finite variant property**
↔ allowing us to get rid of some algebraic properties

Particular Equational Theories: ACUNh and AGh

- Intruder deduction problem:

ACh	ACUNh	AGh
NP-complete	PTIME-(complete)	

- Insecurity problem (bounded number of sessions):

ACh	ACUNh	AGh
Undecidable	Decidable	Undecidable

Complete the picture

Our problem is the satisfiability of a constraint system \mathcal{C} in $(\mathcal{I}, \mathbf{E})$

- 1 **Reduce** the equational theory to a simpler one, *i.e.* \emptyset or **AC**
→ **Finite Variant Property**
- 2 **Find** sufficient **conditions** on the inference system $\mathit{variant}(\mathcal{I})$ to ensure decidability of the problem in $(\mathit{variant}(\mathcal{I}), \mathbf{AC})$
- 3 **Implementation** of the approach

↔ This will allow us to solve the case study by a generic approach.

Other kinds of protocols and security properties

- Electronic **voting protocols**
- **Equivalence** based security properties