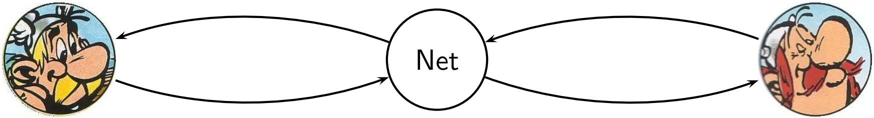
Verification of Security Protocols in presence of Equational Theories with Homomorphism

Stéphanie Delaune

France Télécom, division R&D,
LSV CNRS & ENS Cachan

March, 13, 2006

Cryptographic Protocols (1)



- **Protocol**: rules of message exchanges
- **Goal**: secure communications

Cryptographic Protocols (1)

- **Protocol**: rules of message exchanges
- **Goal**: secure communications

Presence of an attacker

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

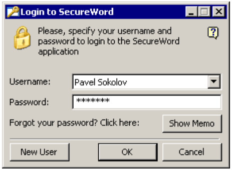
Cryptographic Protocols (2)

Credit Card

Electronic Vote

Electronic Purse

Secure Access



Electronic Signature

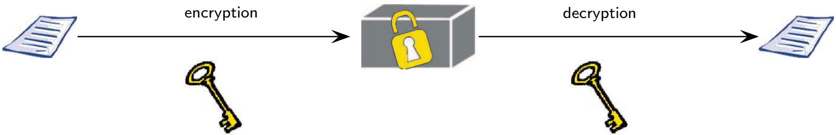
Goals

- **Secrecy**: May an intruder learn some secret message between two honest participants ?
- Authentication: Is the agent Alice really talking to Bob ?

Goals

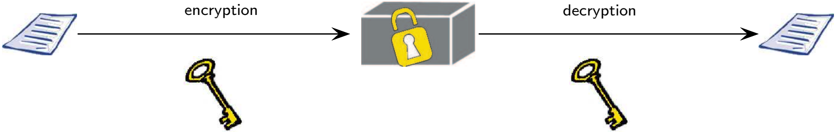
- **Secrecy**: May an intruder learn some secret message between two honest participants ?
- Authentication: Is the agent Alice really talking to Bob ?
- Fairness: Alice and Bob want to sign a contract. Alice initiates the protocol. May Bob obtain some advantage ?
- Privacy: Alice participate to an election. May a participant learn something about the vote of Alice ?
- Receipt-Freeness: Alice participate to an election. Does Alice gain any information (a receipt) which can be used to prove to a coercer that she voted in a certain way ?
- ...

Symmetric Encryption



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) $\dfrac{T \vdash \{u\}_v \quad T \vdash v^{-1}}{T \vdash u}$

Perfect Cryptography Assumption

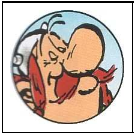
No way to obtain knowledge about u from $\{u\}_v$ without knowing v^{-1}

Needham-Schroeder's Protocol (1978)

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

Needham-Schroeder's Protocol (1978)

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

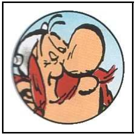


Needham-Schroeder's Protocol (1978)

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

Needham-Schroeder's Protocol (1978)

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



Needham-Schroeder's Protocol (1978)

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

Questions

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

Needham-Schroeder's Protocol (1978)

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

Questions

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

Attack

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

Man in the Middle Attack

Agent A

Intrus I

Agent B

Attack

- involving 2 sessions in parallel,
- an honest agent has to initiate a session with I.

$$
\begin{array}{lll}
A \to B & : & \{A, N_a\}_{\mathrm{pub}(B)} \\
B \to A & : & \{N_a, N_b\}_{\mathrm{pub}(A)} \\
A \to B & : & \{N_b\}_{\mathrm{pub}(B)}
\end{array}
$$

Man in the Middle Attack

$\{A, N_a\}_{\mathrm{pub}(I)}$ → $\{A, N_a\}_{\mathrm{pub}(B)}$ →

Agent A

Intrus I

Agent B

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

Man in the Middle Attack

$\{A, N_a\}_{\mathrm{pub}(I)} \longrightarrow$

$\longleftarrow \{N_a, N_b\}_{\mathrm{pub}(A)}$

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

$\longleftarrow \{N_a, N_b\}_{\mathrm{pub}(A)}$

Agent A | Intrus I | Agent B

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

Man in the Middle Attack

$\{A, N_a\}_{\mathrm{pub}(I)} \longrightarrow$

$\longleftarrow \{N_a, N_b\}_{\mathrm{pub}(A)}$

$\{N_b\}_{\mathrm{pub}(I)} \longrightarrow$

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

$\longleftarrow \{N_a, N_b\}_{\mathrm{pub}(A)}$

$\{N_b\}_{\mathrm{pub}(B)} \longrightarrow$

Agent A

Intrus I

Agent B

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

Man in the Middle Attack

$\xrightarrow{\{A, N_a\}_{\mathrm{pub}(I)}}$

$\xleftarrow{\{N_a, N_b\}_{\mathrm{pub}(A)}}$

$\xrightarrow{\{N_b\}_{\mathrm{pub}(I)}}$

$\xrightarrow{\{A, N_a\}_{\mathrm{pub}(B)}}$

$\xleftarrow{\{N_a, N_b\}_{\mathrm{pub}(A)}}$

$\xrightarrow{\{N_b\}_{\mathrm{pub}(B)}}$

Agent A | Intrus I | Agent B

Attack

- the intruder knows N_b,
- When B finishes his session (apparently with A), A has never talked with B.

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

Tatebayashi, Matsuzaki, Newman (TMN)

Protocol Description

A, B, S	:	principal
Ka, Kb	:	fresh symkey
pub, priv	:	principal $\rightarrow$ key (keypair)

A $\rightarrow$ S	:	B, $\{$Ka$\}$pub(S)
S $\rightarrow$ B	:	A
B $\rightarrow$ S	:	A, $\{$Kb$\}$pub(S)
S $\rightarrow$ A	:	B, Kb $\oplus$ Ka

Tatebayashi, Matsuzaki, Newman (TMN)

Protocol Description

A, B, S	:	principal
Ka, Kb	:	fresh symkey
pub, priv	:	principal $\rightarrow$ key (keypair)

$$
\begin{array}{lcl}
A \rightarrow S & : & B, \{Ka\}pub(S) \\
S \rightarrow B & : & A \\
B \rightarrow S & : & A, \{Kb\}pub(S) \\
S \rightarrow A & : & B, Kb \oplus Ka
\end{array}
$$

RSA Encryption:

$$
m \xrightarrow[\text{public key: } (n,\ e)]{\text{encryption}} c = m^e \bmod n \xrightarrow[\text{private key: } (n,\ d)]{\text{decryption}} c^d \bmod n = m
$$

Tatebayashi, Matsuzaki, Newman (TMN)

Protocol Description

A, B, S	:	principal
Ka, Kb	:	fresh symkey
pub, priv	:	principal $\rightarrow$ key (keypair)

A $\rightarrow$ S	:	B, $\{$Ka$\}$pub(S)
S $\rightarrow$ B	:	A
B $\rightarrow$ S	:	A, $\{$Kb$\}$pub(S)
S $\rightarrow$ A	:	B, Kb $\oplus$ Ka

RSA Encryption:

$$m \xrightarrow[\text{public key: } (n,\ e)]{\text{encryption}} c = m^e \bmod n \xrightarrow[\text{private key: } (n,\ d)]{\text{decryption}} c^d \bmod n = m$$

Homomorphism property : $\{x \times y\}pub(S) = \{x\}pub(S) \times \{y\}pub(S)$

Some Interesting Equational Theories

homomorphism axiom (h): $\mathsf{h}(x+y) = \mathsf{h}(x) + \mathsf{h}(y)$

1. **Associativity, Commutativity** (AC):

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

2. **Exclusive or** (ACUN):

$$x+0 = x \quad (\mathsf{U}), \qquad x+x = 0 \quad (\mathsf{N})$$

3. **Abelian groups** (AG):

$$x+0 = x \quad (\mathsf{U}), \qquad x+\mathsf{I}(x) = 0 \quad (\mathsf{Inv})$$

Outline of the talk

1. Introduction
2. Passive Intruder (may read every messages sent on the network)
   - Intruder Deduction Problem
   - Some Existing Results
   - How to deal with Homomorphisms?
3. Active Intruder (may intercept and send new messages)
   - Trace Reachability Problem
   - Some Existing Results
   - Equational Theories ACUNh and AGh
4. Conclusion and Future Works

Outline of the talk

1 Introduction

2 Passive Intruder (may read every messages sent on the network)
- Intruder Deduction Problem
- Some Existing Results
- How to deal with Homomorphisms?

3 Active Intruder (may intercept and send new messages)
- Trace Reachability Problem
- Some Existing Results
- Equational Theories ACUNh and AGh

4 Conclusion and Future Works

Intruder Deduction Problem

Intruder Deduction Capabilities

(A) $\dfrac{u \in T}{T \vdash_{\mathsf{E}} u}$ (C) $\dfrac{T \vdash_{\mathsf{E}} u_1 \;\ldots\; T \vdash_{\mathsf{E}} u_n}{T \vdash_{\mathsf{E}} f(u_1, \ldots, u_n)}$ with $f \in \mathcal{VF}$

(UL) $\dfrac{T \vdash_{\mathsf{E}} \langle u, v \rangle}{T \vdash_{\mathsf{E}} u}$ (D) $\dfrac{T \vdash_{\mathsf{E}} \{u\}_v \quad T \vdash_{\mathsf{E}} v}{T \vdash_{\mathsf{E}} u}$

(UR) $\dfrac{T \vdash_{\mathsf{E}} \langle u, v \rangle}{T \vdash_{\mathsf{E}} v}$ (**Eq**) $\dfrac{T \vdash_{\mathsf{E}} u \quad u =_{\mathsf{E}} v}{T \vdash_{\mathsf{E}} v}$

Intruder deduction problem (ID)

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

OUTPUT: Does there exist an E-proof of $T \vdash_{\mathsf{E}} s$?

Intruder Deduction Problem

Example:

- $T = \{a + b, \ \ \{h(a)\}_k, \ \ k\}$
- $s = h(b)$
- $\mathsf{E} = \mathsf{ACUNh}$

Intruder Deduction Problem

Example:

- $T = \{a + b, \ \{h(a)\}_k, \ k\}$
- $s = h(b)$
- $\mathsf{E} = \mathsf{ACUNh}$

$$\mathbf{P} = \left\{ \dfrac{\dfrac{\dfrac{a+b \in T}{T \vdash_{\mathsf{E}} a+b}\,(A)}{T \vdash_{\mathsf{E}} h(a+b)}\,(C) \quad \dfrac{\dfrac{\{h(a)\}_k \in T}{T \vdash_{\mathsf{E}} \{h(a)\}_k}\,(A) \quad \dfrac{k \in T}{T \vdash_{\mathsf{E}} k}\,(A)}{T \vdash_{\mathsf{E}} h(a)}\,(D)}{T \vdash_{\mathsf{E}} h(a+b) + h(a)}\,(C) \right.$$

Intruder Deduction Problem

Example:

- $T = \{a + b, \ \ \{h(a)\}_k, \ \ k\}$
- $s = h(b)$
- $\mathsf{E} = \mathsf{ACUNh}$

$$\mathbf{P} = \left\{ \dfrac{\dfrac{\dfrac{a+b \in T}{T \vdash_{\mathsf{E}} a+b}\,(A)}{T \vdash_{\mathsf{E}} h(a+b)}\,(C) \quad \dfrac{\dfrac{\{h(a)\}_k \in T}{T \vdash_{\mathsf{E}} \{h(a)\}_k}\,(A) \quad \dfrac{k \in T}{T \vdash_{\mathsf{E}} k}\,(A)}{T \vdash_{\mathsf{E}} h(a)}\,(D)}{T \vdash_{\mathsf{E}} h(a+b) + h(a)}\,(C) \right.$$

$$\dfrac{\mathbf{P} \qquad h(a+b) + h(a) =_E h(b)}{T \vdash_{\mathsf{E}} h(b)}\,(\mathbf{Eq})$$

Some Existing Results

Complexity of the Intruder Deduction Problem

- without any equational theory (Dolev-Yao model): **PTIME-complete**
- with an equational theory
  - Results of Chevalier *et al.* 2003

AC	ACUN	AG
NP	PTIME	

  - Results of Lafourcade, Lugiez and Treinen 2005

AC**h**	ACUN**h**	AG**h**
NP-complete	**EXPTIME**	

$\longrightarrow$ PTIME in the **binary case**

Sketch of Proof

Let T be a set of terms and u a term (in normal forms)

1. An effective inference system ($\vdash$) such that:

   $$T \vdash u \text{ is derivable} \Leftrightarrow T \vdash_{\mathsf{E}} u \text{ is derivable}$$

2. A locality result (notion due to Mc Allester, 1993), *i.e.*:
   A minimal proof P of $T \vdash u$ only contains terms in $St_{\mathsf{E}}(T \cup \{u\})$.

3. A one-step deducibility result:
   $\rightarrow$ to ensure that we can test that a deduction step is valid

Exclusive Or Example

1. Inference System: $$\frac{T \vdash u_1 \ \ldots \ T \vdash u_n}{T \vdash u_1 + \ldots + u_n \downarrow} \ (\mathsf{M_E})$$

Exclusive Or Example

1. Inference System: $$\frac{T \vdash u_1 \;\; \ldots \;\; T \vdash u_n}{T \vdash u_1 + \ldots + u_n \downarrow} \; (\mathsf{M_E})$$
2. Notion of Subterms: (no partial sum)
   Example: $t = \{a_1 + a_2 + a_3\}_b$

$$St_{\mathsf{E}}(t) = \{t, a_1 + a_2 + a_3, b, a_1, a_2, a_3\}$$

Exclusive Or Example

1. Inference System:
$$\frac{T \vdash u_1 \;\; \ldots \;\; T \vdash u_n}{T \vdash u_1 + \ldots + u_n \downarrow}\;(\mathsf{M_E})$$
2. Notion of Subterms: (no partial sum)
Example: $t = \{a_1 + a_2 + a_3\}_b$
$$St_{\mathsf{E}}(t) = \{t, a_1 + a_2 + a_3, b, a_1, a_2, a_3\}$$
3. One-Step Deducibility of $(\mathsf{M_E})$:
$\longrightarrow$ solvability of a system of linear equations over $\mathbb{Z}/2\mathbb{Z}$: $A \cdot Y = b$.
Example: $T = \{a_1 + a_2, a_2 + a_3 + a_4\}$ and $s = a_1 + a_3 + a_4$

$$A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \\ 0 & 1 \end{pmatrix} \qquad b = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}$$

How to Deal with Homomorphism ?

$$h(x+y) \to h(x) + h(y)$$

- **Approach of Lafourcade et al. 2005**

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

How to Deal with Homomorphism ?

$$h(x+y) \to h(x) + h(y)$$

- **Approach of Lafourcade et al. 2005**

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

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

How to Deal with Homomorphism ?

$$\mathsf{h}(x+y) \to \mathsf{h}(x) + \mathsf{h}(y)$$

- **Approach of Lafourcade et al. 2005**

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

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

- **My approach**

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

How to Deal with Homomorphism ?

$$\mathsf{h}(x + y) \rightarrow \mathsf{h}(x) + \mathsf{h}(y)$$

- **Approach of Lafourcade et al. 2005**

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

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

- **My approach**

$$\frac{T \vdash u_1 \; \ldots \; T \vdash u_n}{T \vdash C[u_1, \ldots, u_n]\downarrow} \text{ with } C \text{ an E-context}$$

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

My Inference System

Intruder Deduction Capabilities

(A) $\dfrac{u \in T}{T \vdash u}$

(C$^-$) $\dfrac{T \vdash u_1 \ \ldots \ T \vdash u_n}{T \vdash f(u_1, \ldots, u_n)}$ with $f \in \mathcal{F} \setminus sig(E)$

(UL) $\dfrac{T \vdash \langle u, v\rangle}{T \vdash u}$

(D) $\dfrac{T \vdash \{u\}_v \quad T \vdash v}{T \vdash u}$

(UR) $\dfrac{T \vdash \langle u, v\rangle}{T \vdash v}$

($\mathbf{M_E}$) $\dfrac{T \vdash u_1 \ \ldots \ T \vdash u_n}{T \vdash C[u_1, \ldots, u_n]\downarrow}$ with C an E-context

My Inference System

Intruder Deduction Capabilities

(A) $\dfrac{u \in T}{T \vdash u}$

(C⁻) $\dfrac{T \vdash u_1 \ \ldots \ T \vdash u_n}{T \vdash f(u_1, \ldots, u_n)}$ with $f \in \mathcal{F} \setminus sig(E)$

(UL) $\dfrac{T \vdash \langle u, v \rangle}{T \vdash u}$

(D) $\dfrac{T \vdash \{u\}_v \quad T \vdash v}{T \vdash u}$

(UR) $\dfrac{T \vdash \langle u, v \rangle}{T \vdash v}$

($\mathbf{M_E}$) $\dfrac{T \vdash u_1 \ \ldots \ T \vdash u_n}{T \vdash C[u_1, \ldots, u_n]\downarrow}$ with C an E-context

Theorem

Let T be a set of terms and u a term (in normal forms). We have:

$$T \vdash u \text{ is derivable} \Leftrightarrow T \vdash_{\mathsf{E}} u \text{ is derivable}$$

Locality

Notion of Subterms

$\longrightarrow$ Generalization of the notion used in the Exclusive Or case

Examples:

Let $t_1 = h^2(a) + b + c$. $\quad St_{\mathsf{E}}(t_1) = \{t_1, a, b, c\}$

Let $t_2 = h(\langle a, b\rangle) + c$. $\quad St_{\mathsf{E}}(t_2) = \{t_2, \langle a, b\rangle, a, b, c\}$

Locality

Notion of Subterms

$\longrightarrow$ Generalization of the notion used in the Exclusive Or case

Examples:

Let $t_1 = h^2(a) + b + c$. $\quad St_{\mathsf{E}}(t_1) = \{t_1, a, b, c\}$

Let $t_2 = h(\langle a, b\rangle) + c$. $\quad St_{\mathsf{E}}(t_2) = \{t_2, \langle a, b\rangle, a, b, c\}$

Locality Result

Lemma

A minimal proof P of $T \vdash u$ only contains terms in $St_{\mathsf{E}}(T \cup \{u\})$.

One-Step-Deducibility (1/2)

The only critical rule is $(\mathsf{M_E})$.
$\rightarrow$ solvability of a system of linear equations over $\mathbb{N}[h]$, $\mathbb{Z}/2\mathbb{Z}[h]$ or $\mathbb{Z}[h]$ (depending on E).

One-Step-Deducibility (1/2)

The only critical rule is ($\mathsf{M_E}$).
$\rightarrow$ solvability of a system of linear equations over $\mathbb{N}[h]$, $\mathbb{Z}/2\mathbb{Z}[h]$ or $\mathbb{Z}[h]$ (depending on E).

Example: (ACUNh)
$T = \{t_1, t_2, t_3\}$ and $s = a_1 + h^2(a_1)$.
$t_1 = a_1 + h(a_1) + h^2(a_1), \qquad t_2 = a_2 + h^2(a_1), \qquad t_3 = h(a_2) + h^2(a_1).$

$$A = \begin{pmatrix} 1+h+h^2 & h^2 & h^2 \\ 0 & 1 & h \end{pmatrix} \qquad b = \begin{pmatrix} 1+h^2 \\ 0 \end{pmatrix}$$

The equation $A \cdot Y = b$ has a solution over $\mathbb{Z}/2\mathbb{Z}[h]$: $Y = (1+h, h, 1)$.

$$C = x_1 + h(x_1) + h(x_2) + x_3$$

One-Step-Deducibility (2/2)

Complexity of solving linear equations:

- over $\mathbb{N}[h]$: NP-complete
- over $\mathbb{Z}/2\mathbb{Z}[h]$: PTIME [Kaltofen *et al.*, 1987]
- over $\mathbb{Z}[h]$: PTIME
  1. thanks to [Aschenbrenner, 2004], $A \cdot Y = b$ has a solution iff there is one such that each component of Y has a degree polynomially bounded by the degrees and the coefficients which appear in A and b.
  2. reduce the problem to the solvability of an enormous (but polynomial) system of linear equations over $\mathbb{Z}$ (PTIME).

One-Step-Deducibility (2/2)

Complexity of solving linear equations:

- over $\mathbb{N}[h]$: NP-complete
- over $\mathbb{Z}/2\mathbb{Z}[h]$: PTIME [Kaltofen *et al.*, 1987]
- over $\mathbb{Z}[h]$: PTIME
  1. thanks to [Aschenbrenner, 2004], $A \cdot Y = b$ has a solution iff there is one such that each component of Y has a degree polynomially bounded by the degrees and the coefficients which appear in A and b.
  2. reduce the problem to the solvability of an enormous (but polynomial) system of linear equations over $\mathbb{Z}$ (PTIME).

Result [Delaune'05]

(ID) is PTIME-complete for ACUNh and AGh.

Outline of the talk

1. Introduction

2. Passive Intruder (may read every messages sent on the network)
   - Intruder Deduction Problem
   - Some Existing Results
   - How to deal with Homomorphisms?

3. Active Intruder (may intercept and send new messages)
   - Trace Reachability Problem
   - Some Existing Results
   - Equational Theories ACUNh and AGh

4. Conclusion and Future Works

Trace Reachability Problem

Trace Reachability 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

- unbounded number of sessions: undecidable
- bounded number of sessions: NP-complete [RT01]

Symbolic Constraint Solving Approach

Protocol rules

$$\begin{array}{c} \mathrm{recv}(u_1)\ ;\mathrm{send}(v_1) \\ \mathrm{recv}(u_2)\ ;\mathrm{send}(v_2) \\ \vdots \\ \mathrm{recv}(u_n)\ ;\mathrm{send}(v_n) \end{array}$$

Constraint system

$$\begin{array}{rcl} T_0 & \Vdash & u_1 \\ T_0, v_1 & \Vdash & u_2 \\ & \vdots & \\ T_0, v_1, v_2, \ldots, v_{n-1} & \Vdash & u_n \\ T_0, v_1, v_2, \ldots, v_{n-1}, v_n & \Vdash & s \end{array}$$

Solution to a constraint system

A solution to a system $\mathcal{C}$ of constraints is a substitution σ such that:

for every $T \Vdash u \in \mathcal{C}$ there exists a proof of $T\sigma \vdash u\sigma$ in $(\mathcal{I}, \mathrm{E})$.

Details

What Happens by Adding an Equational Theory E ?

Undecidability Result

Unification Problem undecidable in E

$\Downarrow$

Trace Reachability Problem undecidable in E (bounded nb of sessions)

What Happens by Adding an Equational Theory E ?

Undecidability Result

Unification Problem undecidable in E

$\Downarrow$

Trace Reachability Problem undecidable in E (bounded nb of sessions)

Corollary

The trace reachability problem is undecidable for the theory ACh.

Trace Reachability Problem (bounded number of sessions)

- without any equational theory (Dolev-Yao model): **NP-complete**
- with an equational theory
  - AC-like theories

AC	ACUN	AG
?	NP [CKRT03] Decidable [CLS03]	Decidable [Shm04]

  - with homomorphism

AC**h**	ACUN**h**	AG**h**
Undecidable	**?**	**?**

New Results

Theorem [Delaune, Lafourcade, Lugiez and Treinen'05]

The trace reachability problem is decidable for the theory ACUNh.

Details

New Results

Theorem [Delaune, Lafourcade, Lugiez and Treinen'05]

The trace reachability problem is decidable for the theory ACUNh.

▸ Details

Theorem [Delaune'06]

The trace reachability problem is undecidable for the theory AGh.

▸ Details

Outline of the talk

1. Introduction
2. Passive Intruder (may read every messages sent on the network)
   - Intruder Deduction Problem
   - Some Existing Results
   - How to deal with Homomorphisms?
3. Active Intruder (may intercept and send new messages)
   - Trace Reachability Problem
   - Some Existing Results
   - Equational Theories ACUNh and AGh
4. Conclusion and Future Works

Conclusion

A new approach to deal with Homomorphism allowing to:

- improve some existing complexity results
- obtain new decidability and undecidability results

Passive Intruder [Delaune'05]

ACh	ACUNh	AGh
NP-complete	**PTIME-(complete)**	

Active Intruder
[Delaune,Lafourcade,Lugiez and Treinen'05] & [Delaune'06]

ACh	ACUNh	AGh
Undecidable	**Decidable**	Undecidable

Future Works

Other kinds of homomorphisms Lafourcade, Lugiez & Treinen

- homomorphic encryption
- commutating homomorphic encryption

Future Works

Other kinds of homomorphisms Lafourcade, Lugiez & Treinen

- homomorphic encryption
- commutating homomorphic encryption

Towards a generic result Bernat, Comon-Lundh & Delaune

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

1. Reduce the equational theory to a simpler one, *i.e.* $\emptyset$ or AC.
   $\rightarrow$ Finite Variant Property

   $$\mathcal{C} \text{ solvable in } (\mathcal{I},\mathcal{E}) \quad \Leftrightarrow \quad \exists\, \mathcal{C}' \in \mathit{var}(\mathcal{C}).\ \mathcal{C}' \text{ solvable in } (\mathit{var}(\mathcal{I}),\, \mathcal{E}')$$

2. Find sufficient conditions on the inference system to ensure decidability of the problem in $(\mathit{var}(\mathcal{I}),\, \mathcal{E}')$.

Needham-Schroeder's Example (1)

Protocol

$$\begin{array}{llrcl}
\mathit{Role}_A\ (x_a,\ x_b): & \nu n_a. & & \longrightarrow & \{x_a, n_a\}_{\mathsf{pub}(x_b)} \\
 & & \{n_a, x_{n_b}\}_{\mathsf{pub}(x_a)} & \longrightarrow & \{x_{n_b}\}_{\mathsf{pub}(x_b)} \\
 & & & & \\
\mathit{Role}_B\ (y_b): & \nu n_b. & \{y_a, y_{n_a}\}_{\mathsf{pub}(y_b)} & \longrightarrow & \{y_{n_a}, n_b\}_{\mathsf{pub}(y_a)}
\end{array}$$

Needham-Schroeder's Example (1)

Protocol

$$
\begin{array}{llrcl}
Role_A\ (x_a, x_b): & \nu n_a. & & \rightarrow & \{x_a, n_a\}_{\mathrm{pub}(x_b)} \\
 & & \{n_a, x_{n_b}\}_{\mathrm{pub}(x_a)} & \rightarrow & \{x_{n_b}\}_{\mathrm{pub}(x_b)} \\
 & & & & \\
Role_B\ (y_b): & \nu n_b. & \{y_a, y_{n_a}\}_{\mathrm{pub}(y_b)} & \rightarrow & \{y_{n_a}, n_b\}_{\mathrm{pub}(y_a)}
\end{array}
$$

We consider $Role_A(a, I)$ and $Role_B(b)$ (running in parallel).

Instanciation

$$
\begin{array}{rcl}
 & \rightarrow & \{a, n_a\}_{\mathrm{pub}(I)} \\
\{n_a, x_{n_b}\}_{\mathrm{pub}(a)} & \rightarrow & \{x_{n_b}\}_{\mathrm{pub}(I)} \\
 & & \\
\{y_a, y_{n_a}\}_{\mathrm{pub}(b)} & \rightarrow & \{y_{n_a}, n_b\}_{\mathrm{pub}(y_a)}
\end{array}
$$

Needham-Schroeder's Example (1)

Protocol

$Role_A\ (x_a, x_b)$: $\nu n_a.$ $\quad \rightarrow \quad \{x_a, n_a\}_{\mathrm{pub}(x_b)}$

$\{n_a, x_{n_b}\}_{\mathrm{pub}(x_a)} \quad \rightarrow \quad \{x_{n_b}\}_{\mathrm{pub}(x_b)}$

$Role_B\ (y_b)$: $\nu n_b.$ $\{y_a, y_{n_a}\}_{\mathrm{pub}(y_b)} \quad \rightarrow \quad \{y_{n_a}, n_b\}_{\mathrm{pub}(y_a)}$

We consider $Role_A(a, I)$ and $Role_B(b)$ (running in parallel).

Instanciation

$\rightarrow \quad \{a, n_a\}_{\mathrm{pub}(I)}$

$\{n_a, x_{n_b}\}_{\mathrm{pub}(a)} \quad \rightarrow \quad \{x_{n_b}\}_{\mathrm{pub}(I)}$

$\{y_a, y_{n_a}\}_{\mathrm{pub}(b)} \quad \rightarrow \quad \{y_{n_a}, n_b\}_{\mathrm{pub}(y_a)}$

Initial intruder's knowledge: $T_0 = \{a, b, I, \mathrm{pub}(a), \mathrm{pub}(b), \mathrm{pub}(I), \mathrm{priv}(I)\}$

Secret: n_b

Needham-Schroeder's Example (1)

Protocol

$$
\begin{array}{llrcl}
Role_A\ (x_a, x_b): & \nu n_a. & & \rightarrow & \{x_a, n_a\}_{\mathrm{pub}(x_b)} \\
 & & \{n_a, x_{n_b}\}_{\mathrm{pub}(x_a)} & \rightarrow & \{x_{n_b}\}_{\mathrm{pub}(x_b)} \\
 & & & & \\
Role_B\ (y_b): & \nu n_b. & \{y_a, y_{n_a}\}_{\mathrm{pub}(y_b)} & \rightarrow & \{y_{n_a}, n_b\}_{\mathrm{pub}(y_a)}
\end{array}
$$

We consider $Role_A(a, I)$ and $Role_B(b)$ (running in parallel).

Instanciation

$$
\begin{array}{lrcl}
\mathbf{1} & & \rightarrow & \{a, n_a\}_{\mathrm{pub}(I)} \\
\mathbf{3} & \{n_a, x_{n_b}\}_{\mathrm{pub}(a)} & \rightarrow & \{x_{n_b}\}_{\mathrm{pub}(I)} \\
 & & & \\
\mathbf{2} & \{y_a, y_{n_a}\}_{\mathrm{pub}(b)} & \rightarrow & \{y_{n_a}, n_b\}_{\mathrm{pub}(y_a)}
\end{array}
$$

Initial intruder's knowledge: $T_0 = \{a, b, I, \mathrm{pub}(a), \mathrm{pub}(b), \mathrm{pub}(I), \mathrm{priv}(I)\}$

Secret: n_b

Needham-Schroeder's Example (2)

Instanciation

$$
\begin{array}{llcl}
\mathbf{1} & & \rightarrow & \{a, n_a\}_{\mathrm{pub}(I)} \\
\mathbf{2} & \{y_a, y_{n_a}\}_{\mathrm{pub}(b)} & \rightarrow & \{y_{n_a}, n_b\}_{\mathrm{pub}(y_a)} \\
\mathbf{3} & \{n_a, x_{n_b}\}_{\mathrm{pub}(a)} & \rightarrow & \{x_{n_b}\}_{\mathrm{pub}(I)}
\end{array}
$$

Constraints System

Back

Needham-Schroeder's Example (2)

Instanciation

1		$\rightarrow$	$\{a, n_a\}_{\mathrm{pub}(I)}$
2	$\{y_a, y_{n_a}\}_{\mathrm{pub}(b)}$	$\rightarrow$	$\{y_{n_a}, n_b\}_{\mathrm{pub}(y_a)}$
3	$\{n_a, x_{n_b}\}_{\mathrm{pub}(a)}$	$\rightarrow$	$\{x_{n_b}\}_{\mathrm{pub}(I)}$

Constraints System

$$T_0, \{a, n_a\}_{\mathrm{pub}(I)}$$

Back

Needham-Schroeder's Example (2)

Instanciation

$$
\begin{array}{llcl}
\mathbf{1} & & \rightarrow & \{a, n_a\}_{\mathrm{pub}(I)} \\
\mathbf{2} & \{y_a, y_{n_a}\}_{\mathrm{pub}(b)} & \rightarrow & \{y_{n_a}, n_b\}_{\mathrm{pub}(y_a)} \\
\mathbf{3} & \{n_a, x_{n_b}\}_{\mathrm{pub}(a)} & \rightarrow & \{x_{n_b}\}_{\mathrm{pub}(I)}
\end{array}
$$

Constraints System

$$T_0, \{a, n_a\}_{\mathrm{pub}(I)} \Vdash \{y_a, y_{n_a}\}_{\mathrm{pub}(b)}$$

▸ Back

Needham-Schroeder's Example (2)

Instanciation

$$\begin{array}{llcl} \mathbf{1} & & \rightarrow & \{a, n_a\}_{\mathrm{pub}(I)} \\ \mathbf{2} & \{y_a, y_{n_a}\}_{\mathrm{pub}(b)} & \rightarrow & \{y_{n_a}, n_b\}_{\mathrm{pub}(y_a)} \\ \mathbf{3} & \{n_a, x_{n_b}\}_{\mathrm{pub}(a)} & \rightarrow & \{x_{n_b}\}_{\mathrm{pub}(I)} \end{array}$$

Constraints System

$$\begin{array}{l} T_0, \{a, n_a\}_{\mathrm{pub}(I)} \Vdash \{y_a, y_{n_a}\}_{\mathrm{pub}(b)} \\ T_0, \{a, n_a\}_{\mathrm{pub}(I)}, \{y_{n_a}, n_b\}_{\mathrm{pub}(y_a)} \end{array}$$

Back

Needham-Schroeder's Example (2)

Instanciation

$$
\begin{array}{llcl}
\mathbf{1} & & \rightarrow & \{a, n_a\}_{\mathrm{pub}(I)} \\
\mathbf{2} & \{y_a, y_{n_a}\}_{\mathrm{pub}(b)} & \rightarrow & \{y_{n_a}, n_b\}_{\mathrm{pub}(y_a)} \\
\mathbf{3} & \{n_a, x_{n_b}\}_{\mathrm{pub}(a)} & \rightarrow & \{x_{n_b}\}_{\mathrm{pub}(I)}
\end{array}
$$

Constraints System

$$
\begin{array}{l}
T_0, \{a, n_a\}_{\mathrm{pub}(I)} \Vdash \{y_a, y_{n_a}\}_{\mathrm{pub}(b)} \\
T_0, \{a, n_a\}_{\mathrm{pub}(I)}, \{y_{n_a}, n_b\}_{\mathrm{pub}(y_a)} \Vdash \{n_a, x_{n_b}\}_{\mathrm{pub}(a)}
\end{array}
$$

Back

Needham-Schroeder's Example (2)

Instanciation

$$
\begin{array}{llcl}
\mathbf{1} & & \rightarrow & \{a, n_a\}_{\mathrm{pub}(I)} \\
\mathbf{2} & \{y_a, y_{n_a}\}_{\mathrm{pub}(b)} & \rightarrow & \{y_{n_a}, n_b\}_{\mathrm{pub}(y_a)} \\
\mathbf{3} & \{n_a, x_{n_b}\}_{\mathrm{pub}(a)} & \rightarrow & \{x_{n_b}\}_{\mathrm{pub}(I)}
\end{array}
$$

Constraints System

$$
\begin{array}{l}
T_0, \{a, n_a\}_{\mathrm{pub}(I)} \Vdash \{y_a, y_{n_a}\}_{\mathrm{pub}(b)} \\
T_0, \{a, n_a\}_{\mathrm{pub}(I)}, \{y_{n_a}, n_b\}_{\mathrm{pub}(y_a)} \Vdash \{n_a, x_{n_b}\}_{\mathrm{pub}(a)} \\
T_0, \{a, n_a\}_{\mathrm{pub}(I)}, \{y_{n_a}, n_b\}_{\mathrm{pub}(y_a)}, \{x_{n_b}\}_{\mathrm{pub}(I)}
\end{array}
$$

Back

Needham-Schroeder's Example (2)

Instanciation

$$\begin{array}{llcl}
\mathbf{1} & & \rightarrow & \{a, n_a\}_{\mathrm{pub}(I)} \\
\mathbf{2} & \{y_a, y_{n_a}\}_{\mathrm{pub}(b)} & \rightarrow & \{y_{n_a}, n_b\}_{\mathrm{pub}(y_a)} \\
\mathbf{3} & \{n_a, x_{n_b}\}_{\mathrm{pub}(a)} & \rightarrow & \{x_{n_b}\}_{\mathrm{pub}(I)}
\end{array}$$

Constraints System

$$\begin{array}{l}
T_0, \{a, n_a\}_{\mathrm{pub}(I)} \Vdash \{y_a, y_{n_a}\}_{\mathrm{pub}(b)} \\
T_0, \{a, n_a\}_{\mathrm{pub}(I)}, \{y_{n_a}, n_b\}_{\mathrm{pub}(y_a)} \Vdash \{n_a, x_{n_b}\}_{\mathrm{pub}(a)} \\
T_0, \{a, n_a\}_{\mathrm{pub}(I)}, \{y_{n_a}, n_b\}_{\mathrm{pub}(y_a)}, \{x_{n_b}\}_{\mathrm{pub}(I)} \Vdash n_b
\end{array}$$

Back

Needham-Schroeder's Example (2)

Instanciation

$$
\begin{array}{llcl}
\mathbf{1} & & \to & \{a, n_a\}_{\mathrm{pub}(I)} \\
\mathbf{2} & \{y_a, y_{n_a}\}_{\mathrm{pub}(b)} & \to & \{y_{n_a}, n_b\}_{\mathrm{pub}(y_a)} \\
\mathbf{3} & \{n_a, x_{n_b}\}_{\mathrm{pub}(a)} & \to & \{x_{n_b}\}_{\mathrm{pub}(I)}
\end{array}
$$

Constraints System

$$
\begin{array}{l}
T_0, \{a, n_a\}_{\mathrm{pub}(I)} \Vdash \{y_a, y_{n_a}\}_{\mathrm{pub}(b)} \\
T_0, \{a, n_a\}_{\mathrm{pub}(I)}, \{y_{n_a}, n_b\}_{\mathrm{pub}(y_a)} \Vdash \{n_a, x_{n_b}\}_{\mathrm{pub}(a)} \\
T_0, \{a, n_a\}_{\mathrm{pub}(I)}, \{y_{n_a}, n_b\}_{\mathrm{pub}(y_a)}, \{x_{n_b}\}_{\mathrm{pub}(I)} \Vdash n_b
\end{array}
$$

Solution

$$\sigma = \{y_{n_a} \mapsto n_a, \quad x_{n_b} \mapsto n_b, \quad y_a \mapsto a\}$$

Back

Procedure in the case of ACUNh (1)

First Part:

Reduce the problem to the solvability of a (well-defined) system of $\Vdash_{M_\mathsf{E}}$ constraints on the reduced signature ($\{0, h, \oplus\}$ and constants).

1. From $\Vdash$ constraints to $\Vdash_1$ (one-step) constraints
   $\longrightarrow$ Generalisation of the locality result to non-groun terms
2. From $\Vdash_1$ constraints to $\Vdash_{M_\mathsf{E}}$ constraints
   $\longrightarrow$ ACUNh-unification is decidable and finitary
3. Abstract subterms by constants
   $\longrightarrow$ this abstraction preserves the well-definedness of the system

Procedure in the case of ACUNh (1)

First Part:
Reduce the problem to the solvability of a (well-defined) system of $\Vdash_{M_E}$ constraints on the reduced signature ($\{0, h, \oplus\}$ and constants).

1 From $\Vdash$ constraints to $\Vdash_1$ (one-step) constraints
$\rightarrow$ Generalisation of the locality result to non-groun terms

2 From $\Vdash_1$ constraints to $\Vdash_{M_E}$ constraints
$\rightarrow$ ACUNh-unification is decidable and finitary

3 Abstract subterms by constants
$\rightarrow$ this abstraction preserves the well-definedness of the system

Now, we have to solve $\Vdash_{M_E}$ constraint systems on a reduced signature:

Example :
$$\mathcal{C} = \begin{cases} a + h(a) & \Vdash_{\mathrm{M_E}} \quad a + h^3(X_1) \\ a + h(a);\ b + X_1 & \Vdash_{\mathrm{M_E}} \quad b + h^4(a) \end{cases}$$

Procedure in the case of ACUNh (2)

Second Part:

$$\mathcal{C} = \begin{cases} a + h(a) & \Vdash_{\mathsf{M_E}} \quad a + h^3(X_1) \\ a + h(a);\ b + X_1 & \Vdash_{\mathsf{M_E}} \quad b + h^4(a) \end{cases}$$

Procedure in the case of ACUNh (2)

Second Part:

$$\mathcal{C} = \begin{cases} a + h(a) & \Vdash_{\mathsf{M_E}} \quad a + h^3(X_1) \\ a + h(a);\ b + X_1 & \Vdash_{\mathsf{M_E}} \quad b + h^4(a) \end{cases}$$

A Solution is: $X_1 \mapsto h^4(a)$

Procedure in the case of ACUNh (2)

Second Part:

$$\mathcal{C} = \begin{cases} a + h(a) & \Vdash_{\mathsf{M_E}} \quad a + h^3(X_1) \\ a + h(a);\ b + X_1 & \Vdash_{\mathsf{M_E}} \quad b + h^4(a) \end{cases}$$

A Solution is: $X_1 \mapsto h^4(a)$

Indeed, $$\frac{a + h(a) \quad h(a) + h^2(a) \quad \dots \quad h^6(a) + h^7(a)}{a + h^7(a)}$$

Procedure in the case of ACUNh (2)

Second Part:

$$\mathcal{C} = \begin{cases} a + h(a) & \Vdash_{\mathsf{M_E}} \quad a + h^3(X_1) \\ a + h(a);\ b + X_1 & \Vdash_{\mathsf{M_E}} \quad b + h^4(a) \end{cases}$$

A Solution is: $X_1 \mapsto h^4(a)$

Contexts used to solve the both intruder deduction problems:

1. $z[1,1] = 1 + h + h^2 + \ldots + h^6$
2. $z[2,1] = 0$ and $z[2,2] = 1$

Procedure in the case of ACUNh (2)

Second Part:

$$\mathcal{C} = \begin{cases} a + h(a) & \Vdash_{\mathsf{M_E}} \quad a + h^3(X_1) \\ a + h(a);\ b + X_1 & \Vdash_{\mathsf{M_E}} \quad b + h^4(a) \end{cases}$$

A Solution is: $X_1 \mapsto h^4(a)$

Contexts used to solve the both intruder deduction problems:

1. $z[1,1] = 1 + h + h^2 + \ldots + h^6$
2. $z[2,1] = 0$ and $z[2,2] = 1$

Lemma

If such a constraint system has a solution, then there is one where defining context variables (in this example $z[1,1]$) are bounded by Q_{max} .

Procedure in the case of ACUNh (2)

Second Part:

$$\mathcal{C} = \begin{cases} a + h(a) & \Vdash_{\mathsf{M_E}} \quad a + h^3(X_1) \\ a + h(a);\ b + X_1 & \Vdash_{\mathsf{M_E}} \quad b + h^4(a) \end{cases}$$

A Solution is: $X_1 \mapsto h^4(a)$

Contexts used to solve the both intruder deduction problems:

1. $z[1,1] = 1 + h + h^2 + \ldots + h^6$
2. $z[2,1] = 0$ and $z[2,2] = 1$

Lemma

If such a constraint system has a solution, then there is one where defining context variables (in this example $z[1,1]$) are bounded by Q_{max} .

Example: $Q_{max} = h^3$
Another solution is: $z[1,1] = 1 + h + h^2$ and $X_1 \mapsto a$.

Procedure in the case of ACUNh (2)

Second Part:
Reduce the problem to the satisfaisability of a set of intruder deduction problems (ground constraints)

4. From $\Vdash_{\mathsf{M_E}}$ constaints to ground $\Vdash_{\mathsf{M_E}}$ constraints
   - solvable system admits small ($< Q_{max}$) defining contexts variables
   - determine value of the variables $(X_1, \dots X_n)$ from the values of the defining contexts variables
5. Check satisfaisability of ground $\Vdash_{\mathsf{M_E}}$ constaints: PTIME.

Back

Trace Reachability Problem for AGh

Abelian groups + homomorphism (AGh):

$$\mathsf{h}(x+y) = \mathsf{h}(x) + \mathsf{h}(y)$$

$$\begin{array}{rclcrcl}
(x+y)+z & = & x+(y+z) & \qquad & x+0 & = & x \\
x+y & = & y+x & & x+-(x) & = & 0
\end{array}$$

Trace Reachability Problem for AGh

Abelian groups + homomorphism (AGh):

$$\mathsf{h}(x+y) = \mathsf{h}(x) + \mathsf{h}(y)$$

$$\begin{array}{rclcrcl} (x+y)+z & = & x+(y+z) & \quad & x+0 & = & x \\ x+y & = & y+x & \quad & x+-(x) & = & 0 \end{array}$$

1. **First Part:** As in the ACUNh case, we can reduce the problem to the solvability of a (well-defined) system of $\Vdash_{\mathsf{M_E}}$ constraints on the reduced signature.

Trace Reachability Problem for AGh

Abelian groups + homomorphism (AGh):

$$h(x+y) = h(x) + h(y)$$

$$\begin{array}{rclcrcl} (x+y)+z & = & x+(y+z) & \quad & x+0 & = & x \\ x+y & = & y+x & \quad & x+-(x) & = & 0 \end{array}$$

1. **First Part:** As in the ACUNh case, we can reduce the problem to the solvability of a (well-defined) system of $\Vdash_{\mathrm{M_E}}$ constraints on the reduced signature.
2. **Second Part:** Contrary to the ACUNh case, satisfaisability of (well-defined) $\Vdash_{\mathrm{M_E}}$ constraints on the reduced signature is undecidable for AGh.

Reduction of the Hilbert's 10^{th} problem

Hilbert's 10^{th} problem

Input: a set S of equations of the form: $x_i = m$, $x_i + x_{i'} = x_j$, or $x_i^2 = x_j$.
Output: Does S have a solution over $\mathbb{Z}$?

Reduction of the Hilbert's 10^{th} problem

Hilbert's 10^{th} problem

Input: a set S of equations of the form: $x_i = m$, $x_i + x_{i'} = x_j$, or $x_i^2 = x_j$.
Output: Does S have a solution over $\mathbb{Z}$?

Example: Let $t = 4a + 3h^2(a) - 3b$. $\mathcal{N}(a, t) = 4$ and $\mathcal{N}(b, t) = -3$.

Reduction of the Hilbert's 10^{th} problem

Hilbert's 10^{th} problem

Input: a set S of equations of the form: $x_i = m$, $x_i + x_{i'} = x_j$, or $x_i^2 = x_j$.
Output: Does S have a solution over $\mathbb{Z}$?

Example: Let $t = 4a + 3h^2(a) - 3b$. $\mathcal{N}(a,t) = 4$ and $\mathcal{N}(b,t) = -3$.

Let n is the number of variables and p the number of equations.

1. A first part $\mathcal{C}_1$ ensures that:

$$\sigma \text{ solution of } \mathcal{C}_1 \Rightarrow \mathcal{N}(a, X_i'\sigma) = \mathcal{N}(a, X_i\sigma)^2$$

All the terms in $\mathcal{C}_1$ are of the form $h^k(..)$ with $k \geq p$.

Reduction of the Hilbert's 10th problem

Hilbert's 10th problem

Input: a set S of equations of the form: $x_i = m$, $x_i + x_{i'} = x_j$, or $x_i^2 = x_j$.
Output: Does S have a solution over $\mathbb{Z}$?

Example: Let $t = 4a + 3h^2(a) - 3b$. $\mathcal{N}(a,t) = 4$ and $\mathcal{N}(b,t) = -3$.

Let n is the number of variables and p the number of equations.

1. A first part $\mathcal{C}_1$ ensures that:
$$\sigma \text{ solution of } \mathcal{C}_1 \Rightarrow \mathcal{N}(a, X_i'\sigma) = \mathcal{N}(a, X_i\sigma)^2$$
All the terms in $\mathcal{C}_1$ are of the form $h^k(..)$ with $k \geq p$.
2. A second part $\mathcal{C}_2$ (one constraint per equation) is built as follows:

$$
\begin{array}{lllll}
1.\ x_i = m & \rightsquigarrow & ..;\ h^{p-1}(X_i) + c_1 & \Vdash & h^{p-1}(ma) + c_1 \\
2.\ x_i + x_j = x_k & \rightsquigarrow & ..\ ;\ h^{p-2}(X_i + X_j) + c_2 & \Vdash & h^{p-2}(X_k) + c_2 \\
3.\ x_i = x_j^2 = & \rightsquigarrow & ..\ ;\ h^{p-3}(X_i) + c_3 & \Vdash & h^{p-3}(X_j') + c_3
\end{array}
$$

Encoding Product

X_1, X_1' and Y_1 are variables.

$$\mathcal{C}_1 := \left\{ \begin{array}{rrrrcl} & & & h^3(a) & \Vdash & h^3(X_1) \\ & & & h^3(a) & \Vdash & h^3(X_1') \\ & & h^2(b); & h^3(a) & \Vdash & h^2(Y_1) \\ & h(a+b); & h^2(b); & h^3(a) & \Vdash & h(X_1 + Y_1) \\ X_1 + b; & h(a+b); & h^2(b); & h^3(a) & \Vdash & X_1' + Y_1 \end{array} \right.$$

Let σ be a solution of $\mathcal{C}_1$. We have:

Encoding Product

X_1, X'_1 and Y_1 are variables.

$$\mathcal{C}_1 := \begin{cases} & & & h^3(a) & \Vdash & h^3(X_1) \\ & & & h^3(a) & \Vdash & h^3(X'_1) \\ & & h^2(b); & h^3(a) & \Vdash & h^2(Y_1) \\ & h(a+b); & h^2(b); & h^3(a) & \Vdash & h(X_1 + Y_1) \\ X_1 + b; & h(a+b); & h^2(b); & h^3(a) & \Vdash & X'_1 + Y_1 \end{cases}$$

Let σ be a solution of $\mathcal{C}_1$. We have:

- $X_1\sigma$ and $X'_1\sigma$ contains no occurences of b, $h(b)$, $h^2(b)$, ...

Encoding Product

X_1, X_1' and Y_1 are variables.

$$\mathcal{C}_1 := \begin{cases} & & & h^3(a) & \Vdash & h^3(X_1) \\ & & & h^3(a) & \Vdash & h^3(X_1') \\ & & h^2(b); & h^3(a) & \Vdash & h^2(Y_1) \\ & h(a+b); & h^2(b); & h^3(a) & \Vdash & h(X_1+Y_1) \\ X_1+b; & h(a+b); & h^2(b); & h^3(a) & \Vdash & X_1'+Y_1 \end{cases}$$

Let σ be a solution of $\mathcal{C}_1$. We have:

- $X_1\sigma$ and $X_1'\sigma$ contains no occurences of b, $h(b)$, $h^2(b)$, ...
- $\mathcal{N}(a, Y_1\sigma) = 0$,

Encoding Product

X_1, X'_1 and Y_1 are variables.

$$\mathcal{C}_1 := \left\{ \begin{array}{rrrrcl} & & & h^3(a) & \Vdash & h^3(X_1) \\ & & & h^3(a) & \Vdash & h^3(X'_1) \\ & & h^2(b); & h^3(a) & \Vdash & h^2(Y_1) \\ & h(a+b); & h^2(b); & h^3(a) & \Vdash & h(X_1 + Y_1) \\ X_1 + b; & h(a+b); & h^2(b); & h^3(a) & \Vdash & X'_1 + Y_1 \end{array} \right.$$

Let σ be a solution of $\mathcal{C}_1$. We have:

- $X_1\sigma$ and $X'_1\sigma$ contains no occurences of b, $h(b)$, $h^2(b)$, ...
- $\mathcal{N}(a, Y_1\sigma) = 0$,
- $\mathcal{N}(a, X_1\sigma) = \mathcal{N}(b, Y_1\sigma)$

Encoding Product

X_1, X'_1 and Y_1 are variables.

$$\mathcal{C}_1 := \left\{ \begin{array}{rrrrcl} & & & h^3(a) & \Vdash & h^3(X_1) \\ & & & h^3(a) & \Vdash & h^3(X'_1) \\ & & h^2(b); & h^3(a) & \Vdash & h^2(Y_1) \\ & h(a+b); & h^2(b); & h^3(a) & \Vdash & h(X_1 + Y_1) \\ X_1 + b; & h(a+b); & h^2(b); & h^3(a) & \Vdash & X'_1 + Y_1 \end{array} \right.$$

Let σ be a solution of $\mathcal{C}_1$. We have:

- $X_1\sigma$ and $X'_1\sigma$ contains no occurences of b, $h(b)$, $h^2(b)$, ...
- $\mathcal{N}(a, Y_1\sigma) = 0$,
- $\mathcal{N}(a, X_1\sigma) = \mathcal{N}(b, Y_1\sigma)$
- $\mathcal{N}(a, X'_1\sigma) = \mathcal{N}(a, X_1\sigma) \times \mathcal{N}(b, Y_1\sigma)$

Encoding Product

X_1, X_1' and Y_1 are variables.

$$\mathcal{C}_1 := \left\{ \begin{array}{rrrrcl} & & & h^3(a) & \Vdash & h^3(X_1) \\ & & & h^3(a) & \Vdash & h^3(X_1') \\ & & h^2(b); & h^3(a) & \Vdash & h^2(Y_1) \\ & h(a+b); & h^2(b); & h^3(a) & \Vdash & h(X_1+Y_1) \\ X_1+b; & h(a+b); & h^2(b); & h^3(a) & \Vdash & X_1'+Y_1 \end{array} \right.$$

Let σ be a solution of $\mathcal{C}_1$. We have:

- $X_1\sigma$ and $X_1'\sigma$ contains no occurences of b, $h(b)$, $h^2(b)$, ...
- $\mathcal{N}(a, Y_1\sigma) = 0$,
- $\mathcal{N}(a, X_1\sigma) = \mathcal{N}(b, Y_1\sigma)$
- $\mathcal{N}(a, X_1'\sigma) = \mathcal{N}(a, X_1\sigma) \times \mathcal{N}(b, Y_1\sigma)$

Hence, we have $\mathcal{N}(a, X_1'\sigma) = \mathcal{N}(a, X_1\sigma) \times \mathcal{N}(a, X_1\sigma)$

Back