Verification of Security Protocols in presence of Equational Theories with Homomorphism

Stéphanie Delaune

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

February, 13, 2006
Cryptographic Protocols (1)

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

...
Encryption

Symmetric Encryption

Encryption

Decryption
Encryption

Symmetric Encryption

[Diagram showing symmetric encryption process with an arrow from encryption to decryption, and a key icon representing the shared secret key.]

Asymmetric Encryption

[Diagram showing asymmetric encryption process with an arrow from encryption to decryption, and icons for public key and private key.]
Dolev-Yao Intruder Model

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

<table>
<thead>
<tr>
<th>Rule</th>
<th>Premises</th>
<th>Conclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Axiom (A)</td>
<td>$u \in T$</td>
<td>$T \vdash u$</td>
</tr>
<tr>
<td>Pairing (P)</td>
<td>$T \vdash u$, $T \vdash v$</td>
<td>$T \vdash \langle u, v \rangle$</td>
</tr>
<tr>
<td>Unpairing (UL)</td>
<td>$T \vdash \langle u, v \rangle$</td>
<td>$T \vdash u$</td>
</tr>
<tr>
<td>Unpairing (UR)</td>
<td>$T \vdash \langle u, v \rangle$</td>
<td>$T \vdash v$</td>
</tr>
<tr>
<td>Encryption (E)</td>
<td>$T \vdash u$, $T \vdash v$</td>
<td>$T \vdash {u}_v$</td>
</tr>
<tr>
<td>Decryption (D)</td>
<td>$T \vdash {u}_v$, $T \vdash v^{-1}$</td>
<td>$T \vdash u$</td>
</tr>
</tbody>
</table>

**Perfect Cryptography Assumption**

No way to obtain knowledge about $u$ from $\{u\}_v$ without knowing $v^{-1}$
Needham-Schroeder’s Protocol (1978)

- $A \rightarrow B : \{A, N_a\}_{\text{pub}(B)}$
- $B \rightarrow A : \{N_a, N_b\}_{\text{pub}(A)}$
- $A \rightarrow B : \{N_b\}_{\text{pub}(B)}$
Needham-Schroeder’s Protocol (1978)

\[ A \rightarrow B : \{A, Na\}_{pub(B)} \]
\[ B \rightarrow A : \{Na, Nb\}_{pub(A)} \]
\[ A \rightarrow B : \{Nb\}_{pub(B)} \]
Needham-Schroeder’s Protocol (1978)

\[
\begin{align*}
A & \rightarrow B : \{A, N_a\}_{\text{pub}(B)} \\
B & \rightarrow A : \{N_a, N_b\}_{\text{pub}(A)} \\
\bullet A & \rightarrow B : \{N_b\}_{\text{pub}(B)}
\end{align*}
\]
Needham-Schroeder’s Protocol (1978)

\[ A \rightarrow B : \{ A, N_a \}_{\text{pub}(B)} \]
\[ B \rightarrow A : \{ N_a, N_b \}_{\text{pub}(A)} \]
\[ A \rightarrow B : \{ N_b \}_{\text{pub}(B)} \]
Needham-Schroeder’s Protocol (1978)

\[
\begin{align*}
A & \rightarrow B : \quad \{A, N_a\}_{\text{pub}(B)} \\
B & \rightarrow A : \quad \{N_a, N_b\}_{\text{pub}(A)} \\
A & \rightarrow B : \quad \{N_b\}_{\text{pub}(B)}
\end{align*}
\]

Questions

- Is \(N_b\) secret between \(A\) and \(B\) ?
- When \(B\) receives \(\{N_b\}_{\text{pub}(B)}\), does this message really comes from \(A\) ?
Needham-Schroeder’s Protocol (1978)

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

Questions

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

A → B : \{A, N_a\}_{\text{pub}(B)}
B → A : \{N_a, N_b\}_{\text{pub}(A)}
A → B : \{N_b\}_{\text{pub}(B)}
Man in the Middle Attack

\[ \{A, N_a\}_{\text{pub}(I)} \rightarrow \{A, N_a\}_{\text{pub}(B)} \]

Agent A \quad \text{Intrus I} \quad \text{Agent B}

A \rightarrow B : \{A, N_a\}_{\text{pub}(B)}
B \rightarrow A : \{N_a, N_b\}_{\text{pub}(A)}
A \rightarrow B : \{N_b\}_{\text{pub}(B)}
Man in the Middle Attack

Agent A

Intrus I

Agent B

\[
\begin{align*}
\text{Agent A} & : \{A, N_a\}_{\text{pub}(A)} \\
\text{Intrus I} & : \{N_a, N_b\}_{\text{pub}(I)} \\
\text{Agent B} & : \{A, N_a\}_{\text{pub}(B)}
\end{align*}
\]

\[
\begin{align*}
A & \rightarrow B : \{A, N_a\}_{\text{pub}(B)} \\
B & \rightarrow A : \{N_a, N_b\}_{\text{pub}(A)} \\
A & \rightarrow B : \{N_b\}_{\text{pub}(B)}
\end{align*}
\]
Man in the Middle Attack

\[
\begin{align*}
\text{Agent } A & \quad \{A, N_a\}_{\text{pub}(I)} \\
& \quad \{N_a, N_b\}_{\text{pub}(A)} \\
& \quad \{N_b\}_{\text{pub}(I)} \\
\text{Intrus } I \\n& \quad \{A, N_a\}_{\text{pub}(B)} \\
& \quad \{N_a, N_b\}_{\text{pub}(A)} \\
& \quad \{N_b\}_{\text{pub}(B)} \\
\text{Agent } B & \quad \{A, N_a\}_{\text{pub}(B)} \\
& \quad \{N_a, N_b\}_{\text{pub}(A)} \\
& \quad \{N_b\}_{\text{pub}(B)}
\end{align*}
\]

\[
\begin{align*}
A & \rightarrow B : \{A, N_a\}_{\text{pub}(B)} \\
B & \rightarrow A : \{N_a, N_b\}_{\text{pub}(A)} \\
A & \rightarrow B : \{N_b\}_{\text{pub}(B)}
\end{align*}
\]
Man in the Middle Attack

\[ \{A, N_a\}_{pub(I)} \quad \{N_a, N_b\}_{pub(A)} \quad \{N_b\}_{pub(I)} \]

Agent A

\[ \{A, N_a\}_{pub(B)} \quad \{N_a, N_b\}_{pub(A)} \quad \{N_b\}_{pub(B)} \]

Intrus I

Agent B

**Attack**

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

A → B : \(\{A, N_a\}_{pub(B)}\)
B → A : \(\{N_a, N_b\}_{pub(A)}\)
A → B : \(\{N_b\}_{pub(B)}\)
### Protocol Description

<table>
<thead>
<tr>
<th>Role</th>
<th>Action</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>A, B, S</td>
<td>A → S</td>
<td>B, {Ka}pub(S)</td>
</tr>
<tr>
<td></td>
<td>S → B</td>
<td>A</td>
</tr>
<tr>
<td></td>
<td>B → S</td>
<td>A, {Kb}pub(S)</td>
</tr>
<tr>
<td></td>
<td>S → A</td>
<td>B, Kb ⊕ Ka</td>
</tr>
</tbody>
</table>

**Variables:**
- A, B, S : principal
- Ka, Kb : fresh symkey
- pub, priv : principal → key (keypair)
**Protocol Description**

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

<table>
<thead>
<tr>
<th>Message</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>A $\rightarrow$ S</td>
<td>B, ${Ka}pub(S)$</td>
</tr>
<tr>
<td>S $\rightarrow$ B</td>
<td>A</td>
</tr>
<tr>
<td>B $\rightarrow$ S</td>
<td>A, ${Kb}pub(S)$</td>
</tr>
<tr>
<td>S $\rightarrow$ A</td>
<td>B, $Kb \oplus Ka$</td>
</tr>
</tbody>
</table>

**RSA Encryption:**

Encryption: $c = m^e \mod n$

Decryption: $c^d \mod n = m$

Public key: $(n, e)$

Private key: $(n, d)$
Protocol Description

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

A → S : B, \{Ka\}pub(S)
S → B : A
B → S : A, \{Kb\}pub(S)
S → A : B, Kb ⊕ Ka

RSA Encryption:

\[ m \xrightarrow{\text{encryption}} c = m^e \mod n \xrightarrow{\text{decryption}} c^d \mod n = m \]

Public key: (n, e)
Private key: (n, d)

Homomorphism property:

\[ \{x \times y\} \text{pub}(S) = \{x\} \text{pub}(S) \times \{y\} \text{pub}(S) \]
Some Interesting Equational Theories

**homomorphism axiom** \((h)\): \( h(x + y) = h(x) + h(y) \)

1. **Associativity, Commutativity** \((AC)\):
   
   \[
   (x + y) + z = x + (y + z), \\
   x + y = y + x
   \]

2. **Exclusive or** \((ACUN)\):
   
   \[
   x + 0 = x \quad (U), \\
   x + x = 0 \quad (N)
   \]

3. **Abelian groups** \((AG)\):
   
   \[
   x + 0 = x \quad (U), \\
   x + I(x) = 0 \quad (Inv)
   \]
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) \[ u \in T \quad \frac{}{T \vdash_E u} \]

(UL) \[ T \vdash_E \langle u, v \rangle \quad \frac{}{T \vdash_E u} \]

(UR) \[ T \vdash_E \langle u, v \rangle \quad \frac{}{T \vdash_E v} \]

(C) \[ T \vdash_E u_1 \ldots T \vdash_E u_n \quad \text{with } f \in \mathcal{F} \]

(D) \[ T \vdash_E \{u\}_v \quad T \vdash_E v \quad \frac{}{T \vdash_E u} \]

(Eq) \[ T \vdash_E u \quad u =_E v \quad \frac{}{T \vdash_E v} \]

Intruder deduction problem (ID)

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

OUTPUT: Does there exist an \( E \)-proof of \( T \vdash_E s \)?
Example:

- \( T = \{ a + b, \{ h(a) \}_k, k \} \)
- \( s = h(b) \)
- \( E = ACUNh \)
Intruder Deduction Problem

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

\[
P = \begin{cases} 
  a + b \in T & \frac{a + b \in T}{T \vdash_E a + b} (A) \\
  h(a + b) \in T & \frac{T \vdash_E h(a + b)}{T \vdash_E h(a + b)} (C) \\
  \{ h(a) \}_k \in T & \frac{\{ h(a) \}_k \in T}{T \vdash_E \{ h(a) \}_k} (A) \\
  k \in T & \frac{T \vdash_E k}{T \vdash_E h(a)} \quad (A) \\
  k \in T & \frac{T \vdash_E h(a)}{T \vdash_E h(a) + h(a)} (C) \\
  h(a + b) \in T & \frac{h(a + b) \in T}{T \vdash_E h(a + b)} (C) \\
  h(\text{C}) & \frac{T \vdash_E h(\text{C})}{T \vdash_E h(a + b) + h(a)} (C) \\
\end{cases}
\]
Example: \[ T = \{a + b, \{h(a)\}_k, k\} \]

\[ s = h(b) \]

\[ E = ACUNh \]

\[
\begin{align*}
T & \vdash_E a + b & \text{(A)} \\
T & \vdash_E \{h(a)\}_k & \text{(A)} \\
T & \vdash_E k & \text{(A)} \\
T & \vdash_E h(a) & \text{(D)} \\
T & \vdash_E h(a + b) & \text{(C)} \\
T & \vdash_E h(a + b) + h(a) & \text{(C)} \\
\end{align*}
\]

\[ h(a + b) + h(a) =_E h(b) \]

\[ T \vdash_E h(b) \]
Some Existing Results

Complexity of the Intruder Deduction Problem

- without any equational theory (Dolev-Yao model): \textbf{PTIME-complete}
- with an equational theory
  - Results of Chevalier \textit{et al.} 2003

\begin{tabular}{|c|c|c|}
  \hline
  \textbf{AC} & \textbf{ACUN} & \textbf{AG} \\
  \hline
  NP & & \textbf{PTIME} \\
  \hline
\end{tabular}

- Results of Lafourcade, Lugiez and Treinen 2005

\begin{tabular}{|c|c|c|}
  \hline
  \textbf{AC\textit{h}} & \textbf{ACUN\textit{h}} & \textbf{AG\textit{h}} \\
  \hline
  NP-complete & & \textbf{EXPTIME} \\
  \hline
\end{tabular}

\[\rightarrow \textbf{PTIME} \text{ in the } \textbf{binary case}\]
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:

   $$T \vdash u \text{ is derivable } \iff T \vdash_E u \text{ is derivable}$$

2. A locality result (notion due to Mc Allester, 1993), i.e.:

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

3. A one-step deducibility result:

   $\rightarrow$ to ensure that we can test that a deduction step is valid
**Exclusive Or Example**

**Inference System:**

\[
\frac{T \vdash u_1 \ldots T \vdash u_n}{T \vdash u_1 + \ldots + u_n} \quad (M_E)
\]
Exclusive Or Example

1. Inference System:

\[
\frac{T \vdash u_1 \ldots T \vdash u_n}{T \vdash u_1 + \ldots + u_n} (M_E)
\]

2. Notion of Subterms: (no partial sum)

**Example:** \( t = \{a_1 + a_2 + a_3\}_b \)

\[
St_E(t) = \{t, a_1 + a_2 + a_3, b, a_1, a_2, a_3\}
\]
Exclusive Or Example

1. Inference System:
   \[ T \vdash u_1 \ldots T \vdash u_n \]
   \[ T \vdash u_1 + \ldots + u_n \downarrow \]
   \[ (M_E) \]

2. Notion of Subterms: (no partial sum)
   \[ \text{Example: } t = \{a_1 + a_2 + a_3\}_b \]
   \[ St_E(t) = \{t, a_1 + a_2 + a_3, b, a_1, a_2, a_3\} \]

3. One-Step Deducibility of \((M_E)\):
   \[ \rightarrow \text{solvability of a system of linear equations over } \mathbb{Z}/2\mathbb{Z}: A \cdot Y = b. \]
   \[ \text{Example: } T = \{a_1 + a_2, a_2 + a_3 + a_4\} \text{ and } s = a_1 + a_3 + a_4 \]

\[ A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \\ 0 & 1 \end{pmatrix} \quad b = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} \]
How to Deal with Homomorphism?

\[ h(x + y) \rightarrow h(x) + h(y) \]

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

\[
\frac{T \vdash u}{T \vdash h(u)} \quad \frac{T \vdash u_1 \ldots T \vdash u_n}{T \vdash u_1 + \ldots + u_n}
\]
How to Deal with Homomorphism?

\[ h(x + y) \rightarrow h(x) + h(y) \]

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

  \[
  \frac{T \vdash u}{T \vdash h(u)} \quad \frac{T \vdash u_1 \ldots \ldots T \vdash u_n}{T \vdash u_1 + \ldots + u_n}
  \]

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

\[ h(x + y) \rightarrow h(x) + h(y) \]

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

\[
\begin{align*}
T \vdash u & \quad T \vdash u_1 \ldots \quad T \vdash u_n \\
T \vdash h(u) & \downarrow \quad T \vdash u_1 + \ldots + u_n & \downarrow
\end{align*}
\]

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

- **My approach**

\[
\begin{align*}
T \vdash u_1 \ldots \quad T \vdash u_n \\
T \vdash C[u_1, \ldots, u_n] & \downarrow
\end{align*}
\]

with \( C \) an E-context
How to Deal with Homomorphism?

\[ h(x + y) \rightarrow h(x) + h(y) \]

- **Approach of Lafourcade et al. 2005**
  
  \[
  \frac{T \vdash u}{T \vdash h(u) \downarrow} \quad \frac{T \vdash u_1 \ldots T \vdash u_n}{T \vdash u_1 + \ldots + u_n \downarrow}
  \]

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

- **My approach**

  \[
  \frac{T \vdash u_1 \ldots T \vdash u_n}{T \vdash C[u_1, \ldots, u_n] \downarrow}
  \]

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

\[
\begin{align*}
(A) & \quad u \in T \quad \frac{}{T \vdash u} \\
(UL) & \quad T \vdash \langle u, v \rangle \quad \frac{}{T \vdash u} \\
(UR) & \quad T \vdash \langle u, v \rangle \quad \frac{}{T \vdash v} \\
(C^-) & \quad T \vdash u_1 \ldots T \vdash u_n \quad \frac{}{T \vdash f(u_1, \ldots, u_n)} \\
(D) & \quad T \vdash \{u\}_v \quad T \vdash v \quad \frac{}{T \vdash u} \\
(M_E) & \quad T \vdash u_1 \ldots T \vdash u_n \quad \frac{}{T \vdash C[u_1, \ldots, u_n]} \\
\end{align*}
\]

with \( f \in \mathcal{F} \setminus \text{sig}(E) \)

with \( C \) an E-context
Intruder Deduction Capabilities

\[
\frac{u \in T}{T \vdash u}
\quad
\frac{T \vdash u_1 \ldots T \vdash u_n}{T \vdash f(u_1, \ldots, u_n)} \quad \text{with } f \in \mathcal{F} \setminus \text{sig}(E)
\]

\[
\frac{T \vdash \langle u, v \rangle}{T \vdash u}
\quad
\frac{T \vdash \{u\}_v}{T \vdash v}
\quad
\frac{T \vdash u_1 \ldots T \vdash u_n}{T \vdash C[u_1, \ldots, u_n]}
\quad \text{with } C \text{ an E-context}
\]

Theorem

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

\( T \vdash u \) is derivable \( \iff \) \( T \vdash_E u \) is derivable
Locality

**Notion of Subterms**

→ **Generalization** of the notion used in the Exclusive Or case

**Examples:**

Let \( t_1 = h^2(a) + b + c \). \[ S_{t_E}(t_1) = \{ t_1, a, b, c \} \]

Let \( t_2 = h(\langle a, b \rangle) + c \). \[ S_{t_E}(t_2) = \{ t_2, \langle a, b \rangle, a, b, c \} \]
**Locality**

**Notion of Subterms**

→ **Generalization** of the notion used in the Exclusive Or case

**Examples:**

Let \( t_1 = h^2(a) + b + c. \) \( St_E(t_1) = \{ t_1, a, b, c \} \)

Let \( t_2 = h(⟨a, b⟩) + c. \) \( St_E(t_2) = \{ t_2, ⟨a, b⟩, a, b, c \} \)

**Locality Result**

**Lemma**

*A minimal proof \( P \) of \( T \vdash u \) only contains terms in \( St_E(T \cup \{ u \}). \)*
The only critical rule is \( (M_E) \).

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

\[ \rightarrow \text{solvability of a system of linear equations over } \mathbb{N}[h], \mathbb{Z}/2\mathbb{Z}[h] \text{ or } \mathbb{Z}[h] \text{ (depending on } E) \].

Example: \((ACUNh)\)

\[ T = \{ t_1, t_2, t_3 \} \text{ and } s = a_1 + h^2(a_1). \]

\[ t_1 = a_1 + h(a_1) + h^2(a_1), \quad t_2 = a_2 + h^2(a_1), \quad t_3 = h(a_2) + h^2(a_1). \]

\[ A = \begin{pmatrix} 1 + h + h^2 & h^2 & h^2 \\ 0 & 1 & h \end{pmatrix} \quad b = \begin{pmatrix} 1 + h^2 \\ 0 \end{pmatrix} \]

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).
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

Given a protocol $P$, an intruder theory $I$, 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

Definition

- A constraint is a sequent of the form $T \vdash u$ where $T$ is a finite set of terms and $u$ is a term ($T$ and $u$ are not necessarily ground).
- A system of constraints is a sequence of constraints. A solution to a system $C$ of constraints is a substitution $\sigma$ such that:

  for every $T \vdash u \in C$ there exists a proof of $T\sigma \vdash u\sigma$
Symbolic Constraint Solving Approach

**Definition**

- A **constraint** is a sequent of the form $T \vdash u$ where $T$ is a finite set of terms and $u$ is a term ($T$ and $u$ are not necessarily ground).
- A **system of constraints** is a sequence of constraints. A solution to a system $C$ of constraints is a substitution $\sigma$ such that:

  $$\text{for every } T \vdash u \in C \text{ there exists a proof of } T\sigma \vdash u\sigma$$

Which constraint systems are particularly interesting for us?

→ **Well-defined** constraint systems:
  - monotonicity
  - origination property (satisfies by the class of deterministic protocols)
# Needham-Schroeder’s Example (1)

## Protocol

<table>
<thead>
<tr>
<th>Role $A$ ($x_a, x_b$):</th>
<th>$\nu n_a$.</th>
<th>$\rightarrow$</th>
<th>${x_a, n_a}_{pub(x_b)}$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>${n_a, x_n b}_{pub(x_a)}$</td>
<td>$\rightarrow$</td>
<td>${x_n b}_{pub(x_b)}$</td>
</tr>
</tbody>
</table>

| Role $B$ ($y_b$):       | $\nu n_b$. | $\{y_a, y_n a\}_{pub(y_b)}$ | $\rightarrow$ | $\{y_n a, n_b\}_{pub(y_a)}$ |

Stéphanie Delaune (FT R&D, LSV)
Needham-Schroeder’s Example (1)

Protocol

\[ \text{Role}_A (x_a, x_b): \quad \nu n_a. \begin{align*}
\{ n_a, x_{n_b} \} & \quad \text{pub}(x_a) \quad \rightarrow \quad \{ x_{n_b} \} \quad \text{pub}(x_b) \\
\{ n_a, x_{n_b} \} & \quad \text{pub}(x_a) \quad \rightarrow \quad \{ x_{n_b} \} \quad \text{pub}(x_b)
\end{align*} \]

\[ \text{Role}_B (y_b): \quad \nu n_b. \begin{align*}
\{ y_a, y_{n_a} \} & \quad \text{pub}(y_b) \quad \rightarrow \quad \{ y_{n_a}, n_b \} \quad \text{pub}(y_a) \\
\{ y_a, y_{n_a} \} & \quad \text{pub}(y_b) \quad \rightarrow \quad \{ y_{n_a}, n_b \} \quad \text{pub}(y_a)
\end{align*} \]

We consider \( \text{Role}_A (a, I) \) and \( \text{Role}_B (b) \) (running in parallel).

Instanciation

\[ \begin{align*}
\{ n_a, x_{n_b} \} \quad \text{pub}(a) & \quad \rightarrow \quad \{ a, n_a \} \quad \text{pub}(I) \\
\{ y_a, y_{n_a} \} \quad \text{pub}(b) & \quad \rightarrow \quad \{ y_{n_a}, n_b \} \quad \text{pub}(y_a)
\end{align*} \]
### Protocol

**Role\(_A\) \((x_a, x_b)\):**

\[ \nu n_a. \quad \{ n_a, x_{n_b} \} \text{pub}(x_a) \rightarrow \{ x_{n_b} \} \text{pub}(x_b) \]

**Role\(_B\) \((y_b)\):**

\[ \nu n_b. \quad \{ y_a, y_{n_a} \} \text{pub}(y_b) \rightarrow \{ y_{n_a}, n_b \} \text{pub}(y_a) \]

We consider **Role\(_A\)(a, I)** and **Role\(_B\)(b)** (running in parallel).

### Instanciation

\[ \begin{align*}
\{ n_a, x_{n_b} \} \text{pub}(a) & \rightarrow \{ x_{n_b} \} \text{pub}(I) \\
\{ y_a, y_{n_a} \} \text{pub}(b) & \rightarrow \{ y_{n_a}, n_b \} \text{pub}(y_a)
\end{align*} \]

Initial intruder’s knowledge: \( T_0 = \{ a, b, I, \text{pub}(a), \text{pub}(b), \text{pub}(I), \text{priv}(I) \} \)

Secret: \( n_b \)
### Needham-Schroeder’s Example (1)

#### Protocol

**Role**\(_A\) \((x_a, x_b):\)

\[\nu n_a. \quad \{n_a, x_{n_b}\}_{\text{pub}(x_a)} \rightarrow \{x_{n_b}\}_{\text{pub}(x_b)}\]

**Role**\(_B\) \((y_b):\)

\[\nu n_b. \quad \{y_a, y_{n_a}\}_{\text{pub}(y_b)} \rightarrow \{y_{n_a}, n_b\}_{\text{pub}(y_a)}\]

We consider **Role**\(_A\)(\(a, I\)) and **Role**\(_B\)(\(b\)) (running in parallel).

#### Instanciation

<table>
<thead>
<tr>
<th>Step</th>
<th>Initial Knowledge</th>
<th>Final Knowledge</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>({a, n_a, x_{n_b}}_{\text{pub}(I)})</td>
<td>({a, n_a}_{\text{pub}(I)})</td>
</tr>
<tr>
<td>2</td>
<td>({y_a, y_{n_a}}_{\text{pub}(b)})</td>
<td>({y_{n_a}, n_b}_{\text{pub}(y_a)})</td>
</tr>
<tr>
<td>3</td>
<td>({n_a, x_{n_b}}_{\text{pub}(a)})</td>
<td>({x_{n_b}}_{\text{pub}(I)})</td>
</tr>
</tbody>
</table>

Initial intruder’s knowledge: \(T_0 = \{a, b, I, \text{pub}(a), \text{pub}(b), \text{pub}(I), \text{priv}(I)\}\)

Secret: \(n_b\)
### Instanciation

<table>
<thead>
<tr>
<th>Step</th>
<th>Equation</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>${a, n_a}_{pub(I)}$</td>
<td>${a, n_a}_{pub(I)}$</td>
</tr>
<tr>
<td>2</td>
<td>${y_a, y_{n_a}}_{pub(b)}$</td>
<td>${y_{n_a}, n_b}<em>{pub(y</em>{a})}$</td>
</tr>
<tr>
<td>3</td>
<td>${n_a, x_{n_b}}_{pub(a)}$</td>
<td>$x_{n_b}_{pub(I)}$</td>
</tr>
</tbody>
</table>

### Constraints System (well-defined)
Instanciation

1 \rightarrow \{a, n_a\}_{pub(I)}

2 \{y_a, y_{n_a}\}_{pub(b)} \rightarrow \{y_{n_a}, n_b\}_{pub(y_a)}

3 \{n_a, x_{n_b}\}_{pub(a)} \rightarrow \{x_{n_b}\}_{pub(I)}

Constraints System (well-defined)

\[ T_0, \{a, n_a\}_{pub(I)} \]
Instanciation

1. \( \{a, n_a\} \text{pub}(I) \rightarrow \{a, n_a\} \text{pub}(I) \)

2. \( \{y_a, y_{n_a}\} \text{pub}(b) \rightarrow \{y_{n_a}, n_b\} \text{pub}(y_a) \)

3. \( \{n_a, x_{n_b}\} \text{pub}(a) \rightarrow \{x_{n_b}\} \text{pub}(I) \)

Constraints System (well-defined)

\[ T_0, \{a, n_a\} \text{pub}(I) \models \{y_a, y_{n_a}\} \text{pub}(b) \]
Instanciation

\[
\begin{align*}
1 & \quad \rightarrow \quad \{a, n_a\}_{\text{pub}(l)} \\
2 & \quad \{y_a, y_{n_a}\}_{\text{pub}(b)} \quad \rightarrow \quad \{y_{n_a}, n_b\}_{\text{pub}(y_a)} \\
3 & \quad \{n_a, x_{n_b}\}_{\text{pub}(a)} \quad \rightarrow \quad \{x_{n_b}\}_{\text{pub}(l)}
\end{align*}
\]

Constraints System (well-defined)

\[
\begin{align*}
T_0, \{a, n_a\}_{\text{pub}(l)} & \mid\!
\mid \{y_a, y_{n_a}\}_{\text{pub}(b)} \\
T_0, \{a, n_a\}_{\text{pub}(l)}, \{y_{n_a}, n_b\}_{\text{pub}(y_a)}
\end{align*}
\]
Instanciation

1 \[ \{a, n_a\}^{\text{pub}(I)} \rightarrow \{a, n_a\}^{\text{pub}(I)} \]

2 \[ \{y_a, y_{n_a}\}^{\text{pub}(b)} \rightarrow \{y_{n_a}, n_b\}^{\text{pub}(y_a)} \]

3 \[ \{n_a, x_{n_b}\}^{\text{pub}(a)} \rightarrow \{x_{n_b}\}^{\text{pub}(I)} \]

Constraints System (well-defined)

\[ T_0, \{a, n_a\}^{\text{pub}(I)} \vdash \{y_a, y_{n_a}\}^{\text{pub}(b)} \]
\[ T_0, \{a, n_a\}^{\text{pub}(I)}, \{y_{n_a}, n_b\}^{\text{pub}(y_a)} \vdash \{n_a, x_{n_b}\}^{\text{pub}(a)} \]
Needham-Schroeder’s Example (2)

### Instanciation

<table>
<thead>
<tr>
<th></th>
<th>[ { y_a, y_{na} }^{\text{pub}(b)} \rightarrow { y_{na}, n_b }^{\text{pub}(y_a)} ]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>[ { a, n_a }^{\text{pub}(l)} \rightarrow { y_{na}, n_b }^{\text{pub}(y_a)} ]</td>
</tr>
<tr>
<td>2</td>
<td>[ { n_a, x_{nb} }^{\text{pub}(a)} \rightarrow { x_{nb} }^{\text{pub}(l)} ]</td>
</tr>
</tbody>
</table>

### Constraints System (well-defined)

\[
\begin{align*}
T_0, \{ a, n_a \}^{\text{pub}(l)} & \vdash \{ y_a, y_{na} \}^{\text{pub}(b)} \\
T_0, \{ a, n_a \}^{\text{pub}(l)}, \{ y_{na}, n_b \}^{\text{pub}(y_a)} & \vdash \{ n_a, x_{nb} \}^{\text{pub}(a)} \\
T_0, \{ a, n_a \}^{\text{pub}(l)}, \{ y_{na}, n_b \}^{\text{pub}(y_a)}, \{ x_{nb} \}^{\text{pub}(l)} & \vdash \{ a, n_a \}^{\text{pub}(l)}
\end{align*}
\]
Needham-Schroeder’s Example (2)

Instanciation

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

Constraints System (well-defined)

\[
T_0, \{a, n_a\}_{pub(I)} \vdash \{y_a, y_{n_a}\}_{pub(b)}
\]
\[
T_0, \{a, n_a\}_{pub(I)} \vdash \{y_{n_a}, n_b\}_{pub(y_a)} \vdash \{n_a, x_{n_b}\}_{pub(a)}
\]
\[
T_0, \{a, n_a\}_{pub(I)} \vdash \{y_{n_a}, n_b\}_{pub(y_a)} \vdash \{x_{n_b}\}_{pub(I)} \vdash n_b
\]
Instanciation

\begin{align*}
1 & \quad \rightarrow \quad \{a, n_a\}_{\text{pub}(I)} \\
2 & \quad \{y_a, y_{n_a}\}_{\text{pub}(b)} \quad \rightarrow \quad \{y_{n_a}, n_b\}_{\text{pub}(y_a)} \\
3 & \quad \{n_a, x_{n_b}\}_{\text{pub}(a)} \quad \rightarrow \quad \{x_{n_b}\}_{\text{pub}(I)}
\end{align*}

Constraints System (well-defined)

\begin{align*}
T_0, \{a, n_a\}_{\text{pub}(I)} & \models \{y_a, y_{n_a}\}_{\text{pub}(b)} \\
T_0, \{a, n_a\}_{\text{pub}(I)}, \{y_{n_a}, n_b\}_{\text{pub}(y_a)} & \models \{n_a, x_{n_b}\}_{\text{pub}(a)} \\
T_0, \{a, n_a\}_{\text{pub}(I)}, \{y_{n_a}, n_b\}_{\text{pub}(y_a)}, \{x_{n_b}\}_{\text{pub}(I)} & \models n_b
\end{align*}

Solution

\[\sigma = \{y_{n_a} \mapsto n_a, \; x_{n_b} \mapsto n_b, \; y_a \mapsto a\}\]
What Happens by Adding an Equational Theory $E$?

Unification Problem modulo $E$

**INPUT**: Given 2 terms $u[x_1, \ldots, x_n]$ and $v[x_1, \ldots, x_n]$

**OUTPUT**: Yes iff there exists a substitution

$$\sigma = \{x_1 \mapsto M_1, \ldots, x_n \mapsto M_n\}$$

such that $u\sigma =_E v\sigma$. 

Stéphanie Delaune (FT R&D, LSV)
What Happens by Adding an Equational Theory $E$?

Unification Problem modulo $E$

**INPUT:** Given 2 terms $u[x_1, \ldots, x_n]$ and $v[x_1, \ldots, x_n]$

**OUTPUT:** Yes iff there exists a substitution

$$\sigma = \{ x_1 \mapsto M_1, \ldots, x_n \mapsto M_n \}$$

such that $u\sigma =_E v\sigma$.

Protocol

1. $x_1, \ldots, x_n \rightarrow \{u[x_1, \ldots, x_n], v[x_1, \ldots, x_n]\}_{Kab}$
2. $\{x, x\}_{Kab} \rightarrow$ secret

$\text{secret}$ is secret $\iff u$ and $v$ have no $E$-unifier
What Happens by Adding an Equational Theory $E$?

**Unification Problem modulo $E$**

**INPUT:** Given 2 terms $u[x_1, \ldots, x_n]$ and $v[x_1, \ldots, x_n]$  

**OUTPUT:** Yes iff there exists a substitution  

$$\sigma = \{x_1 \mapsto M_1, \ldots, x_n \mapsto M_n\}$$  

such that $u\sigma =_E v\sigma$.

**Protocol**

1. $x_1, \ldots, x_n \rightarrow \{u[x_1, \ldots, x_n], v[x_1, \ldots, x_n]\}_Kab$
2. $\{x, x\}_Kab \rightarrow \text{secret}$

$\text{secret}$ is secret $\iff$ $u$ and $v$ have no $E$-unifier

**Undecidability Result**

Unification Problem **undecidable** in $E$  

⇓  

Trace Reachability Problem **undecidable** in $E$ (bounded nb of sessions)
Some Existing Results

Trace Reachability Problem (bounded number of sessions)

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

<table>
<thead>
<tr>
<th></th>
<th>AC</th>
<th>ACUN</th>
<th>AG</th>
</tr>
</thead>
<tbody>
<tr>
<td>without</td>
<td>?</td>
<td>NP [CKRT03] Decidable [CLS03]</td>
<td>Decidable [Shm04]</td>
</tr>
</tbody>
</table>

- **with** homomorphism

<table>
<thead>
<tr>
<th></th>
<th>AC(h)</th>
<th>ACUN(h)</th>
<th>AG(h)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Undecidable</td>
<td>?</td>
<td>?</td>
</tr>
</tbody>
</table>
The trace reachability problem is \textit{decidable} for the theory \textit{ACUNh}.
The trace reachability problem is **decidable** for the theory **ACUNh**.

The trace reachability problem is **undecidable** for the theory **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
A **new approach** to deal with Homomorphism allowing to:

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

### Passive Intruder [Delaune’05]

<table>
<thead>
<tr>
<th>ACh</th>
<th>ACUNh</th>
<th>AGh</th>
</tr>
</thead>
<tbody>
<tr>
<td>NP-complete</td>
<td><strong>PTIME-(complete)</strong></td>
<td></td>
</tr>
</tbody>
</table>

### Active Intruder

[Delaune, Lafourcade, Lugiez and Treinen’05] & [Delaune’06]

<table>
<thead>
<tr>
<th>ACh</th>
<th>ACUNh</th>
<th>AGh</th>
</tr>
</thead>
<tbody>
<tr>
<td>Undecidable</td>
<td><strong>Decidable</strong></td>
<td>Undecidable</td>
</tr>
</tbody>
</table>
Future Works

Others kind of homomorphisms Lafourcade, Lugiez & Treinen

- homomorphic encryption
- commutating homomorphic encryption
Others kind 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 $C$ in $(I, E)$

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

\[ C \text{ solvable in } (I,E) \iff \exists C' \in \text{var}(C). \quad C' \text{ solvable in } (\text{var}(I), E') \]

2. Find sufficient conditions on the inference system to ensure decidability of the problem in $(\text{var}(I), E')$. 
Procedure in the case of ACUNh (1)

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

1. From $\models$ constraints to $\models_1$ (one-step) constraints
   → Generalisation of the locality result to non-groun terms

2. From $\models_1$ constraints to $\models M_E$ constraints
   → ACUNh-unification is decidable and finitary

3. Abstract subterms by constants
   → this abstraction preserves the well-definedness of the system
First Part:
Reduce the problem to the solvability of a (well-defined) system of $\models_{ME}$ constraints on the reduced signature ($\{0, h, \oplus\}$ and constants).

1. From $\models$ constraints to $\models_1$ (one-step) constraints
   → Generalisation of the locality result to non-ground terms

2. From $\models_1$ constraints to $\models_{ME}$ constraints
   → ACUNh-unification is decidable and finitary

3. Abstract subterms by constants
   → this abstraction preserves the well-definedness of the system

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

Example: $C = \left\{ \begin{array}{l}
a + h(a) \quad \models_{ME} a + h^3(X_1) \\
a + h(a); b + X_1 \quad \models_{ME} b + h^4(a)\end{array} \right\}$
Procedure in the case of ACUNh (2)

Second Part:

\[ C = \left\{ \begin{array}{l}
  a + h(a) \\
  a + h(a); \ b + X_1 \\
  a + h^3(X_1) \\
  b + h^4(a)
\end{array} \right\} \models_{ME} \]
Procedure in the case of ACUNh (2)

Second Part:

\[ C = \begin{cases} 
  a + h(a) & \vdash_{ME} a + h^3(X_1) \\
  a + h(a); \ b + X_1 & \vdash_{ME} b + h^4(a) 
\end{cases} \]

A Solution is: \( X_1 \mapsto h^4(a) \)
Procedure in the case of ACUNh (2)

Second Part:

\[ C = \left\{ \begin{array}{c} a + h(a) \\ a + h(a); \ b + X_1 \\ a + h(a) \end{array} \right\} \models_{M_E} \left\{ \begin{array}{c} a + h^3(X_1) \\ b + h^4(a) \end{array} \right\} \]

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

Indeed,

\[ a + h(a) \quad h(a) + h^2(a) \quad \ldots \quad h^6(a) + h^7(a) \]

\[ \overbrace{\quad a + h^7(a) \quad} \]

\[ a + h^7(a) \]
Procedure in the case of ACUNh (2)

Second Part:

\[ C = \left\{ \begin{array}{ll} a + h(a) & \vdash_{M_E} a + h^3(X_1) \\ a + h(a); b + X_1 & \vdash_{M_E} b + h^4(a) \end{array} \right\} \]

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:

\[ C = \begin{cases} 
  a + h(a) & \vdash_{\text{ME}} \, a + h^3(X_1) \\
  a + h(a); \, b + X_1 & \vdash_{\text{ME}} \, b + h^4(a) 
\end{cases} \]

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:

\[ C = \begin{cases} 
  a + h(a) \\ 
  a + h(a); \ b + X_1 \\
\end{cases} \quad \Vdash_{\mathcal{M}_E} \quad \begin{cases} 
  a + h^3(X_1) \\
  b + h^4(a) \\
\end{cases} \]

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 \( Q_{\text{max}} \).

Example: \( Q_{\text{max}} = h^3 \)

Another solution is: \( z[1, 1] = 1 + h + h^2 \) and \( X_1 \mapsto a \).
Second Part:
Reduce the problem to the satisfaisability of a set of intruder deduction problems (ground constraints)

4 From $\models_{M_E}$ constants to ground $\models_{M_E}$ constraints
   - solvable system admits small ($< Q_{max}$) defining contexts variables
   - determine value of the variables ($X_1, \ldots X_n$) from the values of the defining contexts variables

5 Check satisfaisability of ground $\models_{M_E}$ constants: PTIME.
Abelian groups + homomorphism (AGh):

\[ h(x + y) = h(x) + h(y) \]

\[ (x + y) + z = x + (y + z) \]
\[ x + y = y + x \]
\[ x + 0 = x \]
\[ x + -(x) = 0 \]
Abelian groups + homomorphism (AGh):

\[ h(x + y) = h(x) + h(y) \]

\[
(x + y) + z = x + (y + z) \quad x + 0 = x \\
x + y = y + x \quad x + -(x) = 0
\]

1. **First Part:** As in the ACUNh case, we can reduce the problem to the solvability of a (well-defined) system of \( \models_{\text{ME}} \) constraints on the reduced signature.
Trace Reachability Problem for AGh

Abelian groups + homomorphism (AGh):

\[ h(x + y) = h(x) + h(y) \]

\[
(x + y) + z = x + (y + z) \quad x + 0 = x \\
x + y = y + x \quad x + -(x) = 0
\]

First Part: As in the ACUNh case, we can reduce the problem to the solvability of a (well-defined) system of \( \models_{ME} \) constraints on the reduced signature.

Second Part: Contrary to the ACUNh case, satisfaisability of (well-defined) \( \models_{ME} \) constraints on the reduced signature is undecidable for AGh.
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 $\mathbb{Z}$?
Reduction of the Hilbert’s 10\textsuperscript{th} problem

Hilbert’s 10\textsuperscript{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 $t = 4a + 3h^2(a) - 3b$. $N(a, t) = 4$ and $N(b, t) = -3$. 
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.

A first part $C_1$ ensures that:

$\sigma$ solution of $C_1 \Rightarrow \mathcal{N}(a, X_i'\sigma) = \mathcal{N}(a, X_i\sigma)^2$

All the terms in $C_1$ are of the form $h^k(\ldots)$ with $k \geq p$. 
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 $C_1$ ensures that:

   $\sigma$ solution of $C_1 \Rightarrow \mathcal{N}(a, X_i' \sigma) = \mathcal{N}(a, X_i \sigma)^2$

   All the terms in $C_1$ are of the form $h^k(\ldots)$ with $k \geq p$.

2. A second part $C_2$ (one constraint per equation) is built as follows:

   1. $x_i = m \quad \mapsto \quad .. ; \quad h^{p-1}(X_i) + c_1 \quad \parallel \quad h^{p-1}(ma) + c_1$
   2. $x_i + x_j = x_k \quad \mapsto \quad .. ; \quad h^{p-2}(X_i + X_j) + c_2 \quad \parallel \quad h^{p-2}(X_k) + c_2$
   3. $x_i = x_j^2 \quad \mapsto \quad .. ; \quad h^{p-3}(X_i) + c_3 \quad \parallel \quad h^{p-3}(X_j') + c_3$
$X_1$, $X'_1$, and $Y_1$ are variables.

$$\begin{align*}
C_1 := \{ & h^3(a) \vdash h^3(X_1) \\
& h^3(a) \vdash h^3(X'_1) \\
& h^2(b); h^3(a) \vdash h^2(Y_1) \\
& h(a + b); h^2(b); h^3(a) \vdash h(X_1 + Y_1) \\
& X_1 + b; h(a + b); h^2(b); h^3(a) \vdash X'_1 + Y_1 \}
\end{align*}$$

Let $\sigma$ be a solution of $C_1$. We have:
\( X_1, X'_1 \) and \( Y_1 \) are variables.

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

Let \( \sigma \) be a solution of \( \mathcal{C}_1 \). We have:

\( X_1\sigma \) and \( X'_1\sigma \) contains no occurrences of \( b, h(b), h^2(b), \ldots \)
$X_1, X'_1$ 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 $\sigma$ be a solution of $\mathcal{C}_1$. We have:

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

$$C_1 := \begin{cases} 
  h^3(a) \vdash h^3(X_1) \\
  h^3(a) \vdash h^3(X'_1) \\
  h^2(b); h^3(a) \vdash h^2(Y_1) \\
  h(a + b); h^2(b); h^3(a) \vdash h(X_1 + Y_1) \\
  X_1 + b; h(a + b); h^2(b); h^3(a) \vdash X'_1 + Y_1
\end{cases}$$

Let $\sigma$ be a solution of $C_1$. We have:

- $X_1 \sigma$ and $X'_1 \sigma$ contains no occurrences of $b$, $h(b)$, $h^2(b)$, ...
- $\mathcal{N}(a, Y_1 \sigma) = 0$,
- $\mathcal{N}(a, X_1 \sigma) = \mathcal{N}(b, Y_1 \sigma)$
Let $\sigma$ be a solution of $C_1$. We have:

- $X_1 \sigma$ and $X'_1 \sigma$ contains no occurrences of $b$, $h(b)$, $h^2(b)$, ...
- $N(a, Y_1 \sigma) = 0$,
- $N(a, X_1 \sigma) = N(b, Y_1 \sigma)$
- $N(a, X'_1 \sigma) = N(a, X_1 \sigma) \times N(b, Y_1 \sigma)$
$X_1$, $X'_1$ and $Y_1$ are variables.

\[
C_1 := \begin{cases} 
\h_3(a) \vdash \h_3(X_1) \\
\h_3(a) \vdash \h_3(X'_1) \\
\h_2(b); \ h_3(a) \vdash \h_2(Y_1) \\
h(a + b); \ h_2(b); \ h_3(a) \vdash \h(X_1 + Y_1) \\
X_1 + b; \ h(a + b); \ h_2(b); \ h_3(a) \vdash X'_1 + Y_1
\end{cases}
\]

Let $\sigma$ be a solution of $C_1$. We have:

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

Hence, we have $N(a, X'_1\sigma) = N(a, X_1\sigma) \times N(a, X_1\sigma)$