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?

- ...
Encryption

Symmetric Encryption

encryption → decryption

Stéphanie Delaune (FT R&D, LSV)  Verification of Security Protocols  March, 13, 2006
Encryption

Symmetric Encryption

Asymmetric Encryption

Stéphanie Delaune (FT R&D, LSV)
Dolev-Yao Intruder Model

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

Axiom (A)

\[ u \in T \]
\[ \frac{\vdash u}{\vdash T} \]

Pairing (P)

\[ T \vdash \langle u, v \rangle \]
\[ \frac{\vdash u \quad \vdash v}{\vdash T} \]

Unpairing (UL)

\[ T \vdash \langle u, v \rangle \]
\[ \frac{\vdash u}{\vdash T} \]

Unpairing (UR)

\[ T \vdash \langle u, v \rangle \]
\[ \frac{\vdash v}{\vdash T} \]

Encryption (E)

\[ T \vdash u \quad T \vdash v \]
\[ \frac{\vdash \{u\}_v}{\vdash T} \]

Decryption (D)

\[ T \vdash \{u\}_v \quad T \vdash v^{-1} \]
\[ \frac{\vdash u}{\vdash T} \]

Perfect Cryptography Assumption

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

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

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

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

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

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

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

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

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

Stéphanie Delaune (FT R&D, LSV)
Needham-Schroeder’s Protocol (1978)

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

Questions

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

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

Questions

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

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

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

Agent A \quad Intrus I \quad Agent B

\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

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

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

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

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

Agent A  Intrus I  Agent B

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

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

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

Agent A

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

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

\[ \{N_b\}_{\text{pub}(I)} \]

Intrus I

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

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

\[ \{N_b\}_{\text{pub}(B)} \]

Agent B

Attack

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

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

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

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

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

public key: (n, e)  
private key: (n, d)
Protocol Description

A, B, S : principal
Ka, Kb : fresh symkey
pub, priv : principal \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:

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

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

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

\[
x + 0 = x \quad (U), \quad x + x = 0 \quad (N)
\]

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

\[
x + 0 = x \quad (U), \quad x + I(x) = 0 \quad (Inv)
\]
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) $\frac{u \in T}{T \vdash_E u}$

(C) $\frac{T \vdash_E u_1 \ldots T \vdash_E u_n}{T \vdash_E f(u_1, \ldots, u_n)}$ with $f \in \mathcal{VF}$

(UL) $\frac{T \vdash_E \langle u, v \rangle}{T \vdash_E u}$

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

(UR) $\frac{T \vdash_E \langle u, v \rangle}{T \vdash_E v}$

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

Intruder deduction problem (ID)

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

**OUTPUT**: Does there exist an $E$-proof of $T \vdash_E s$?
Intruder Deduction Problem

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

\[
P = \begin{cases} 
 a + b \in T \quad (A) \\
 T \vdash_E a + b \\
\hline
 T \vdash_E \{h(a)\}_k \quad (A) \\
 k \in T \\
\hline
 T \vdash_E k \quad (A) \\
\hline
\end{cases} 
\]

\[
\begin{align*}
 T \vdash_E \{h(a)\}_k & \quad (A) \\
\hline
 T \vdash_E h(a) \\
\hline
 T \vdash_E h(a + b) + h(a) \quad (C)
\end{align*}
\]
Example:

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

\[
P = \begin{align*}
\frac{a + b \in T}{T \models_E a + b} & \quad (A) \\
\frac{T \models_E a + b}{T \models_E h(a + b)} & \quad (C) \\
\frac{\{ h(a) \}_k \in T}{T \models_E \{ h(a) \}_k} & \quad (A) \\
\frac{k \in T}{T \models_E k} & \quad (A) \\
\frac{T \models_E h(a)}{T \models_E h(a) + h(a)} & \quad (D) \\
\frac{T \models_E h(a + b) + h(a)}{T \models_E h(a + b)} & \quad (C)
\end{align*}
\]

\[
P \quad \frac{h(a + b) + h(a) =_E h(b)}{T \models_E h(b)} & \quad (Eq)
\]
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
    
    \[
    \begin{array}{|c|c|c|}
    \hline
    \text{AC} & \text{ACUN} & \text{AG} \\
    \hline
    \text{NP} & \text{PTIME} & \text{} \\
    \hline
    \end{array}
    \]

  - Results of Lafourcade, Lugiez and Treinen 2005
    
    \[
    \begin{array}{|c|c|c|}
    \hline
    \text{ACH} & \text{ACUNh} & \text{AGh} \\
    \hline
    \text{NP-complete} & \text{EXPTIME} & \text{} \\
    \hline
    \end{array}
    \]

  \[\rightarrow \text{PTIME in the binary case}\]
Let $T$ be a set of terms and $u$ a term (in normal forms)

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

   $T \vdash u$ is derivable $\iff T \vdash_{E} u$ 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:
   $\to$ to ensure that we can test that a deduction step is valid
Exclusive Or Example

Inference System:

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

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

\[ St_E(t) = \{t, a_1 + a_2 + a_3, b, a_1, a_2, a_3\} \]
Inference System:
\[ \frac{T \vdash u_1 \ldots T \vdash u_n}{T \vdash u_1 + \ldots + u_n} \text{(M_E)} \]

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

One-Step Deducibility of \( \text{(M_E)} \):
\( \rightarrow \) 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 \( s = a_1 + a_3 + a_4 \)
\[ A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \\ 0 & 1 \end{pmatrix} \quad b = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} \]
How to Deal with Homomorphism?

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

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

  \[
  \begin{align*}
  T \vdash u & \quad T \vdash u_1 \ldots T \vdash u_n \\
  T \vdash h(u) \downarrow & \quad T \vdash u_1 + \ldots + u_n \downarrow
  \end{align*}
  \]
How to Deal with Homomorphism?

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

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

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

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

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

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

  \[ T \vdash u \quad T \vdash u_1 \ldots T \vdash u_n \]

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

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

- **My approach**

  \[ T \vdash u_1 \ldots T \vdash u_n \]

  \[ T \vdash C[u_1, \ldots, u_n] \]

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

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

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

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

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

- **My approach**

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

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

(A) \[ \frac{u \in T}{T \vdash u} \]

(B) \[ \frac{T \vdash \langle u, v \rangle}{T \vdash u} \]

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

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

(M\textsubscript{E}) \[ \frac{T \vdash u_1 \ldots T \vdash u_n}{T \vdash C[u_1, \ldots, u_n]} \quad \text{with } C \text{ an E-context} \]
Intruder Deduction Capabilities

(A) \[ \frac{u \in T}{T \vdash u} \]  

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

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

(D) \[ \frac{T \vdash \{u\}_v}{T \vdash u} \]

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

(M\textsubscript{E}) \[ \frac{T \vdash u_1 \ldots T \vdash u_n}{T \vdash C[u_1, \ldots, u_n]} \text{ with } C \text{ an E-context} \]

Theorem

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

\[ T \vdash u \text{ is derivable } \iff T \vdash_{E} u \text{ is derivable} \]
Notion of Subterms

→ Generalization of the notion used in the Exclusive Or case

Examples:

Let $t_1 = h^2(a) + b + c$. \hspace{1cm} St_E(t_1) = \{t_1, a, b, c\}

Let $t_2 = h(\langle a, b \rangle) + c$. \hspace{1cm} St_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 \( t_2 = h(\langle a, b \rangle) + c \). \( St_E(t_2) = \{ t_2, \langle a, b \rangle, a, b, c \} \)

Locality Result

Lemma

A minimal proof \( P \) of \( T \vdash u \) only contains terms in \( St_E(T \cup \{ u \}) \).
The only critical rule is \((M_E)\).
\[
\rightarrow \text{solvability of a system of linear equations over } \mathbb{N}[h], \mathbb{Z}/2\mathbb{Z}[h] \text{ or } \mathbb{Z}[h]\]
(depending on \(E\)).
One-Step-Deducibility (1/2)

The only critical rule is \((M_E)\).
\(\rightarrow\) 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 \(s = a_1 + h^2(a_1)\).
\(t_1 = a_1 + h(a_1) + h^2(a_1), \quad t_2 = a_2 + h^2(a_1), \quad t_3 = h(a_2) + h^2(a_1)\).

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

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

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

Trace Reachability Problem

Given a protocol $\mathcal{P}$, an intruder theory $\mathcal{I}$, an equational theory $\mathcal{E}$, 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

recv\( (u_1) \); send\( (v_1) \)
recv\( (u_2) \); send\( (v_2) \)
\vdots
recv\( (u_n) \); send\( (v_n) \)

Constraint system

\[ T_0 \vdash u_1 \]
\[ T_0, v_1 \vdash u_2 \]
\vdots
\[ T_0, v_1, v_2, \ldots, v_{n-1} \vdash u_n \]
\[ T_0, v_1, v_2, \ldots, v_{n-1}, v_n \vdash s \]

Solution to a constraint system

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 \( T\sigma \vdash u\sigma \) in \( (\mathcal{I}, \mathcal{E}) \).
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 $ACh$.***
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>AC</th>
<th>ACUN</th>
<th>AG</th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td>NP [CKRT03] Decidable [CLS03]</td>
<td>Decidable [Shm04]</td>
</tr>
</tbody>
</table>

- with homomorphism

<table>
<thead>
<tr>
<th>ACh</th>
<th>ACUNh</th>
<th>AGh</th>
</tr>
</thead>
<tbody>
<tr>
<td>Undecidable</td>
<td>?</td>
<td>?</td>
</tr>
</tbody>
</table>
The trace reachability problem is **decidable** for the theory **ACUNh**.
New Results

**Theorem [Delaune, Lafourcade, Lugiez and Treinen’05]**
The trace reachability problem is **decidable** for the theory **ACUNh**.

**Theorem [Delaune’06]**
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
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]

<table>
<thead>
<tr>
<th>ACh</th>
<th>ACUNh</th>
<th>AGh</th>
</tr>
</thead>
<tbody>
<tr>
<td>NP-complete</td>
<td></td>
<td>PTIME-(complete)</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>Decidable</td>
<td>Undecidable</td>
</tr>
</tbody>
</table>
Other kinds of homomorphisms

- homomorphic encryption
- commutating homomorphic encryption
Other kinds of homomorphisms \textit{Lafourcade, Lugiez & Treinen}

- homomorphic encryption
- commutating homomorphic encryption

Towards a generic result \textit{Bernat, Comon-Lundh & Delaune}

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

1. \textbf{Reduce} the equational theory to a simpler one, \textit{i.e.} $\emptyset$ or AC.
   \rightarrow \text{Finite Variant Property}

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

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

**Role**<sub>A</sub> \((x_a, x_b)\):
\[
\nu n_a. \rightarrow \{x_a, n_a\}_{pub(x_b)}
\]
\[
\{n_a, x_{n_b}\}_{pub(x_a)} \rightarrow \{x_{n_b}\}_{pub(x_b)}
\]

**Role**<sub>B</sub> \((y_b)\):
\[
\nu n_b. \{y_a, y_{n_a}\}_{pub(y_b)} \rightarrow \{y_{n_a}, n_b\}_{pub(y_a)}
\]
**Needham-Schroeder’s Example (1)**

### Protocol

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{Role}_A (x_a, x_b)$:</td>
<td>$\nu n_a.$ \rightarrow {x_a, n_a}<em>{\text{pub}(x_b)}$  \rightarrow {x</em>{n_b}}_{\text{pub}(x_b)}</td>
</tr>
<tr>
<td>${n_a, x_{n_b}}_{\text{pub}(x_a)}$</td>
<td>$\rightarrow {x_{n_b}}_{\text{pub}(x_b)}$</td>
</tr>
<tr>
<td>$\text{Role}_B (y_b)$:</td>
<td>$\nu n_b.$ \rightarrow {y_{n_a}, n_b}_{\text{pub}(y_a)}$</td>
</tr>
<tr>
<td>${y_a, y_{n_a}}_{\text{pub}(y_b)}$</td>
<td>$\rightarrow {y_{n_a}, n_b}_{\text{pub}(y_a)}$</td>
</tr>
</tbody>
</table>

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

### Instanciation

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>${n_a, x_{n_b}}_{\text{pub}(a)}$</td>
</tr>
<tr>
<td>${y_a, y_{n_a}}_{\text{pub}(b)}$</td>
</tr>
</tbody>
</table>
Needham-Schroeder’s Example (1)

Protocol

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

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

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

Instanciation

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

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

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

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

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

### Constraints System
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

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

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

1 \[ \{ a, n_a \} \text{pub}(I) \]
2 \[ \{ y_a, y_{na} \} \text{pub}(b) \rightarrow \{ y_{na}, n_b \} \text{pub}(y_a) \]
3 \[ \{ n_a, x_{nb} \} \text{pub}(a) \rightarrow \{ x_{nb} \} \text{pub}(I) \]

Constraints System

\[ T_0, \{ a, n_a \} \text{pub}(I) \vdash \{ y_a, y_{na} \} \text{pub}(b) \]
\[ T_0, \{ a, n_a \} \text{pub}(I), \{ y_{na}, n_b \} \text{pub}(y_a) \]
### Instanciation

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

2. \[ \{y_a, y_n_a\} \overset{\text{pub}(b)}{\rightarrow} \{y_n_a, n_b\} \overset{\text{pub}(y_a)}{\rightarrow} \{x_n_b\} \overset{\text{pub}(I)}{\rightarrow} \{x_n_b\} \]

### Constraints System

\[
T_0, \{a, n_a\} \overset{\text{pub}(I)}{\vdash} \{y_a, y_n_a\} \quad \text{pub}(b) \\
T_0, \{a, n_a\} \overset{\text{pub}(I)}{\vdash} \{y_n_a, n_b\} \overset{\text{pub}(y_a)}{\vdash} \{n_a, x_n_b\} \overset{\text{pub}(a)}{\rightarrow} \{x_n_b\} \overset{\text{pub}(I)}{\rightarrow} \{x_n_b\} 
\]
### Instanciation

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>${a, n_a}$</td>
<td>$\rightarrow \quad {a, n_a}_{pub(I)}$</td>
</tr>
<tr>
<td>2</td>
<td>${y_a, y_{na}}$</td>
<td>$\rightarrow \quad {y_{na}, n_b}_{pub(y_a)}$</td>
</tr>
<tr>
<td>3</td>
<td>${n_a, x_{nb}}$</td>
<td>$\rightarrow \quad {x_{nb}}_{pub(I)}$</td>
</tr>
</tbody>
</table>

### Constraints System

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

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

2  \{ya, yna\}_{\text{pub}(b)}  \rightarrow  \{yna, nb\}_{\text{pub}(ya)}

3  \{na, xn_b\}_{\text{pub}(a)}  \rightarrow  \{xn_b\}_{\text{pub}(I)}

Constraints System

\begin{align*}
T_0, \{a, na\}_{\text{pub}(I)}  &\models  \{ya, yna\}_{\text{pub}(b)} \\
T_0, \{a, na\}_{\text{pub}(I)}, \{yna, nb\}_{\text{pub}(ya)}  &\models  \{na, xn_b\}_{\text{pub}(a)} \\
T_0, \{a, na\}_{\text{pub}(I)}, \{yna, nb\}_{\text{pub}(ya)}, \{xn_b\}_{\text{pub}(I)}  &\models  nb
\end{align*}
Instanciation

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

2 \{ya, yn\}_{pub(b)} \rightarrow \{yn, nb\}_{pub(ya)}

3 \{na, xn\}_{pub(a)} \rightarrow \{xn\}_{pub(I)}

Constraints System

\[ T_0, \{a, na\}_{pub(I)} \vdash \{ya, yn\}_{pub(b)} \]
\[ T_0, \{a, na\}_{pub(I)}, \{yn, nb\}_{pub(ya)} \vdash \{na, xn\}_{pub(a)} \]
\[ T_0, \{a, na\}_{pub(I)}, \{yn, nb\}_{pub(ya)}, \{xn\}_{pub(I)} \vdash nb \]

Solution

\[ \sigma = \{ya_n \mapsto na, \ xn_n \mapsto nb, \ ya \mapsto a\} \]
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-ground 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

Stéphanie Delaune (FT R&D, LSV)  Verification of Security Protocols  March, 13, 2006  34 / 1
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-ground 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

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

**Example:**
\[ C = \begin{cases} 
  a + h(a) & \models_{M_E} a + h^3(X_1) \\
  a + h(a); b + X_1 & \models_{M_E} b + h^4(a) 
\end{cases} \]
Second Part:

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

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

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

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

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

Indeed,

$$a + h(a) \quad h(a) + h^2(a) \quad \ldots \quad h^6(a) + h^7(a) \quad a + h^7(a)$$
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: \( X_1 \mapsto h^4(a) \)

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:

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

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 \( Q_{\text{max}} \).
Procedure in the case of ACUNh (2)

Second Part:

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

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 \( X_1 \mapsto a \).
Second Part:
Reduce the problem to the satisfaisability of a set of intruder deduction problems (ground constraints)

4. From $\vdash_{M_E}$ constraints to ground $\vdash_{M_E}$ 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 $\vdash_{M_E}$ constraints: PTIME.
Abelian groups + homomorphism (AGh):

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

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

\[
x + y = y + x \quad x + -x = 0
\]
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.
Trace Reachability Problem for A\text{Gh}

Abelian groups + homomorphism (A\text{Gh}):

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

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

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

2. **Second Part:** Contrary to the A\text{CUNh} case, satisfaisability of (well-defined) \( \models_{M_E} \) constraints on the reduced signature is undecidable for A\text{Gh}.
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 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 $t = 4a + 3h^2(a) - 3b$. $N(a, t) = 4$ and $N(b, t) = -3$. 
Reduction of the Hilbert’s 10\textsuperscript{th} problem

Hilbert’s 10\textsuperscript{th} problem

\textbf{Input:} a set $S$ of equations of the form: $x_i = m$, $x_i + x_{i'} = x_j$, or $x_i^2 = x_j$.

\textbf{Output:} Does $S$ have a solution over $\mathbb{Z}$?

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

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

1. A first part $C_1$ ensures that:

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

   All the terms in $C_1$ are of the form $h^k(\cdot)$ 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:
   $$\sigma \text{ solution of } C_1 \implies \mathcal{N}(a, X'_i \sigma) = \mathcal{N}(a, X_i \sigma)^2$$
   All the terms in $C_1$ are of the form $h^k(\cdot)$ with $k \geq p$.

2. A second part $C_2$ (one constraint per equation) is built as follows:
   1. $x_i = m \leadsto \ldots; h^{p-1}(X_i) + c_1 \models h^{p-1}(ma) + c_1$
   2. $x_i + x_j = x_k \leadsto \ldots; h^{p-2}(X_i + X_j) + c_2 \models h^{p-2}(X_k) + c_2$
   3. $x_i = x_j^2 = \leadsto \ldots; h^{p-3}(X_i) + c_3 \models h^{p-3}(X'_j) + c_3$
$X_1$, $X'_1$ and $Y_1$ are variables.

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

Let $\sigma$ be a solution of $C_1$. We have:
$X_1$, $X'_1$ 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 occurences of $b$, $h(b)$, $h^2(b)$, ...
\(X_1, X'_1\) and \(Y_1\) are variables.

\[
\mathcal{C}_1 := \left\{ \begin{array}{l}
h^3(a) \vdash h^3(X_1) \\
h^3(a) \vdash h^3(X'_1) \\
h^2(b); \quad h^3(a) \vdash h^2(Y_1) \\
h(a + b); \quad h^2(b); \quad h^3(a) \vdash h(X_1 + Y_1) \\
X_1 + b; \quad h(a + b); \quad h^2(b); \quad h^3(a) \vdash X'_1 + Y_1 \end{array} \right. 
\]

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

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

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

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

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


$X_1$, $X'_1$ and $Y_1$ are variables.

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

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

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

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