Théories de l'intrus pour la vérification des protocoles cryptographiques

Vincent Bernat

LSV, CNRS & ENS de Cachan, UMR 8643

7 juin 2006

Protéger ses communications

Applications nécessitant la confidentialité

- Achats sur Internet
- Réseaux sans fil (wifi)
- Transactions bancaires
- Communications téléphoniques (GSM)

Une solution pour protéger ses communications : la cryptographie.

Protéger ses communications

Applications nécessitant la confidentialité

- Achats sur Internet
- Réseaux sans fil (wifi)
- Transactions bancaires
- Communications téléphoniques (GSM)

Une solution pour protéger ses communications : la cryptographie.

Cryptographie classique

Chiffrer signifie rendre un message inintelligible à celui qui ne dispose pas de la clef nécessaire.

Déchiffrer signifie rendre un message chiffré sous sa forme originale en utilisant la clef prévue à cet effet.

Décrypter consiste à retrouver le message d'origine sans connaître la clef nécessaire à cette opération.

Le chiffrement permet donc de protéger des communications. Il existe de multiples techniques pour réaliser ce chiffrement. Il existe aussi des attaques !

Cryptographie classique

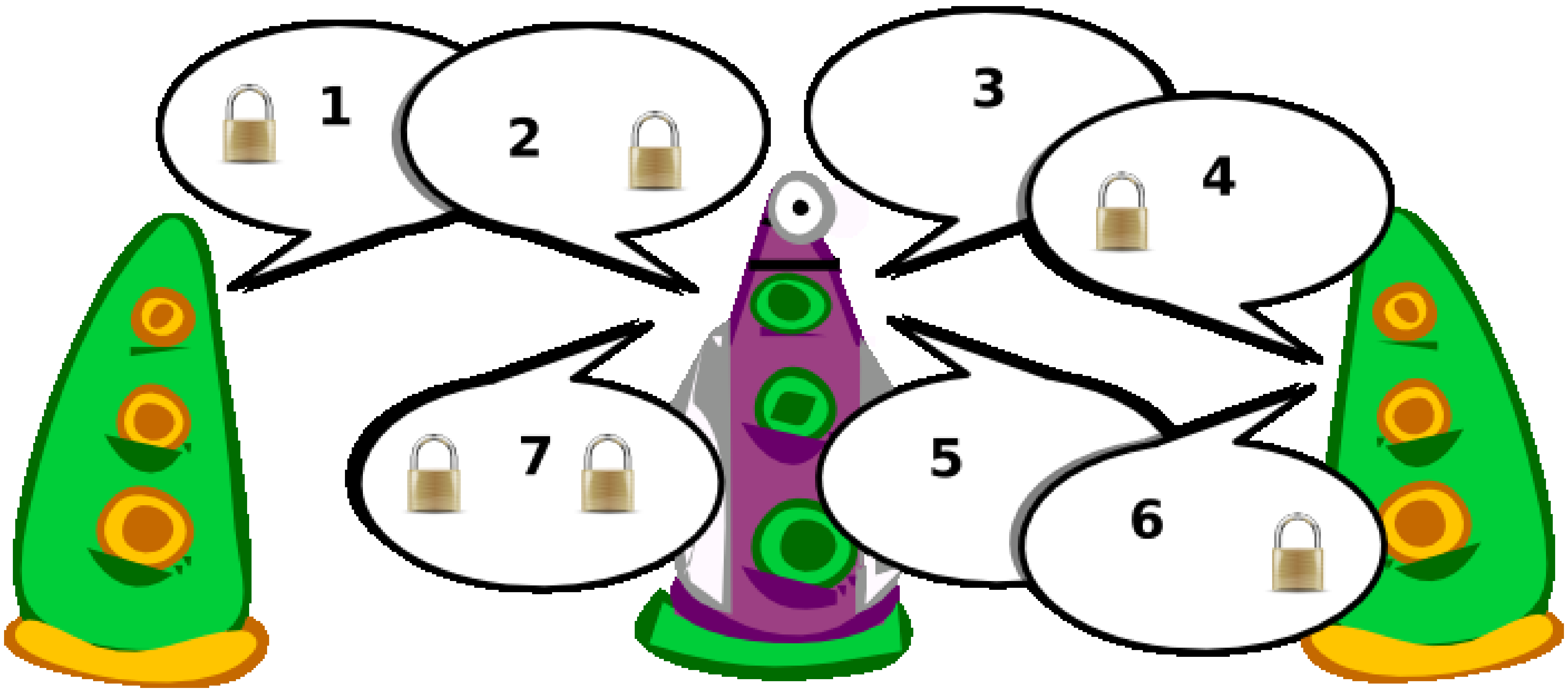
Chiffrer signifie rendre un message inintelligible à celui qui ne dispose pas de la clef nécessaire.

Déchiffrer signifie rendre un message chiffré sous sa forme originale en utilisant la clef prévue à cet effet.

Décrypter consiste à retrouver le message d'origine sans connaître la clef nécessaire à cette opération.

Le chiffrement permet donc de protéger des communications. Il existe de multiples techniques pour réaliser ce chiffrement. Il existe aussi des attaques !

Protocole cryptographique



Un protocole cryptographique est un ensemble de règles pour échanger des messages en utilisant des primitives cryptographiques.

Abstraction des messages

- Les primitives cryptographiques sont idéalisées : ce sont des boîtes noires.
- Les messages sont des termes échangés entre des acteurs.
- L'opération de chiffrement du message m par la clef k est écrite $\{m\}_k$.
- On utilise des nonces qui sont des constantes tirées aléatoirement impossibles à deviner : N_A.

Il est possible de trouver des attaques contre des protocoles sans utiliser d'attaques contre le chiffrement.

Abstraction des messages

- Les primitives cryptographiques sont idéalisées : ce sont des boîtes noires.
- Les messages sont des termes échangés entre des acteurs.
- L'opération de chiffrement du message m par la clef k est écrite $\{m\}_k$.
- On utilise des nonces qui sont des constantes tirées aléatoirement impossibles à deviner : N_A.

Il est possible de trouver des attaques contre des protocoles sans utiliser d'attaques contre le chiffrement.

Abstraction des messages

- Les primitives cryptographiques sont idéalisées : ce sont des boîtes noires.
- Les messages sont des termes échangés entre des acteurs.
- L'opération de chiffrement du message m par la clef k est écrite $\{m\}_k$.
- On utilise des nonces qui sont des constantes tirées aléatoirement impossibles à deviner : N_A.

Il est possible de trouver des attaques contre des protocoles sans utiliser d'attaques contre le chiffrement.

Abstraction des messages

- Les primitives cryptographiques sont idéalisées : ce sont des boîtes noires.
- Les messages sont des termes échangés entre des acteurs.
- L'opération de chiffrement du message m par la clef k est écrite $\{m\}_k$.
- On utilise des nonces qui sont des constantes tirées aléatoirement impossibles à deviner : N_A.

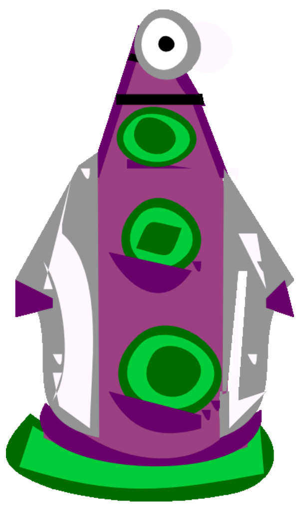
Il est possible de trouver des attaques contre des protocoles sans utiliser d'attaques contre le chiffrement.

Abstraction des messages

- Les primitives cryptographiques sont idéalisées : ce sont des boîtes noires.
- Les messages sont des termes échangés entre des acteurs.
- L'opération de chiffrement du message m par la clef k est écrite $\{m\}_k$.
- On utilise des nonces qui sont des constantes tirées aléatoirement impossibles à deviner : N_A.

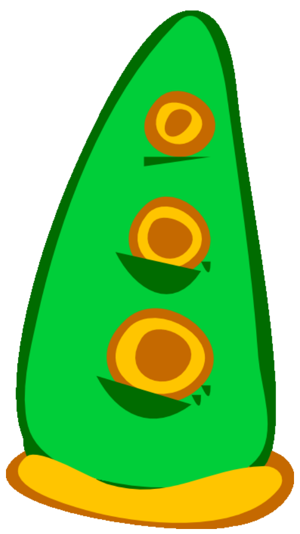
Il est possible de trouver des attaques contre des protocoles sans utiliser d'attaques contre le chiffrement.

Un exemple : Needham-Schroeder



Alice

$$\begin{array}{ll} A \to B & \{A, N_A\}_{\mathrm{pub}(B)} \\ B \to A & \{N_A, N_B\}_{\mathrm{pub}(A)} \\ A \to B & \{N_B\}_{\mathrm{pub}(B)} \end{array}$$

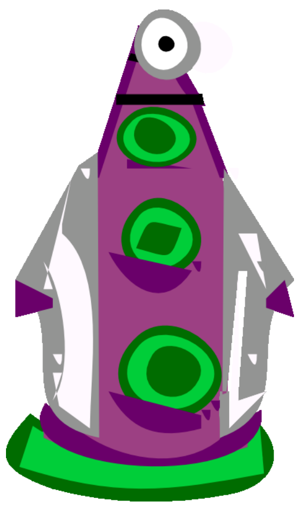


Bob

N_B est-il un secret entre les deux acteurs ?

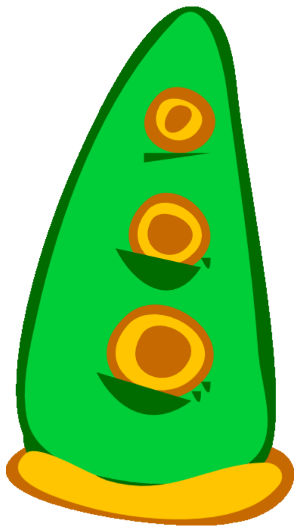
Ce protocole date de 1978. Une attaque a été trouvée en 1995 par G. Lowe !

Un exemple : Needham-Schroeder



Alice

$$\begin{array}{ll} A \rightarrow B & \{A, N_A\}_{\mathrm{pub}(B)} \\ B \rightarrow A & \{N_A, N_B\}_{\mathrm{pub}(A)} \\ A \rightarrow B & \{N_B\}_{\mathrm{pub}(B)} \end{array}$$

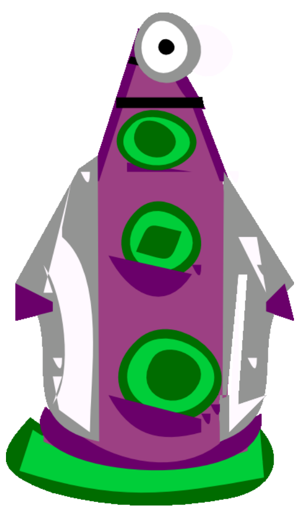


Bob

N_B est-il un secret entre les deux acteurs ?

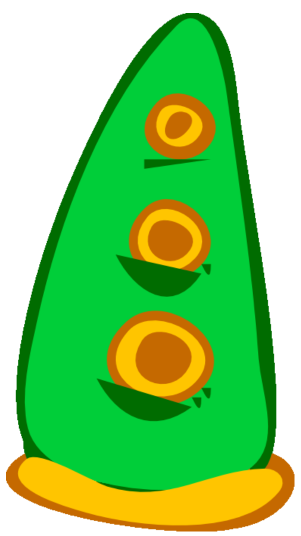
Ce protocole date de 1978. Une attaque a été trouvée en 1995 par G. Lowe !

Un exemple : Needham-Schroeder



Alice

$$
\begin{array}{ll}
A \to B & \{A, N_A\}_{\mathrm{pub}(B)} \\
B \to A & \{N_A, N_B\}_{\mathrm{pub}(A)} \\
A \to B & \{N_B\}_{\mathrm{pub}(B)}
\end{array}
$$



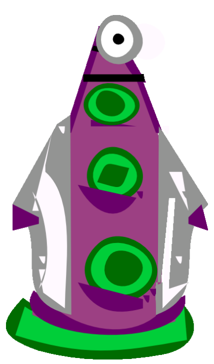
Bob

N_B est-il un secret entre les deux acteurs ?
Ce protocole date de 1978. Une attaque a été trouvée en 1995 par G. Lowe !

Une attaque sur Needham-Schroeder

- $A \to I \quad \{A, N_A\}_{\mathrm{pub}(I)}$
- $I \to A \quad \{N_A, N_I\}_{\mathrm{pub}(A)}$
- $A \to I \quad \{N_I\}_{\mathrm{pub}(I)}$

- $A \to B \quad \{A, N_A\}_{\mathrm{pub}(B)}$
- $B \to A \quad \{N_A, N_B\}_{\mathrm{pub}(A)}$
- $A \to B \quad \{N_B\}_{\mathrm{pub}(B)}$



Alice

$A \to I \quad \{A, N_A\}_{\mathrm{pub}(I)}$

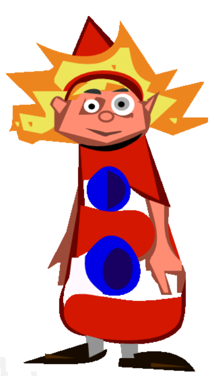
$I(A) \to B \quad \{A, N_A\}_{\mathrm{pub}(B)}$

$B \to I(A) \quad \{N_A, N_B\}_{\mathrm{pub}(A)}$

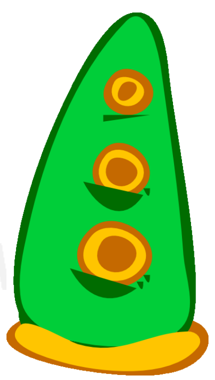
$I \to A \quad \{N_A, N_B\}_{\mathrm{pub}(A)}$

$A \to I \quad \{N_B\}_{\mathrm{pub}(I)}$

$I(A) \to B \quad \{N_B\}_{\mathrm{pub}(B)}$



Intrus

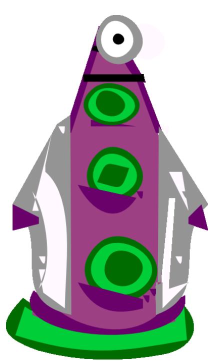


Bob

Une attaque sur Needham-Schroeder

- $A \to I \quad \{A, N_A\}_{\mathrm{pub}(I)}$
- $I \to A \quad \{N_A, N_I\}_{\mathrm{pub}(A)}$
- $A \to I \quad \{N_I\}_{\mathrm{pub}(I)}$

- $A \to B \quad \{A, N_A\}_{\mathrm{pub}(B)}$
- $B \to A \quad \{N_A, N_B\}_{\mathrm{pub}(A)}$
- $A \to B \quad \{N_B\}_{\mathrm{pub}(B)}$

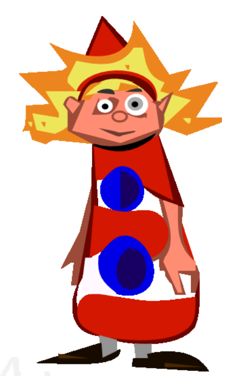


Alice

$A \to I \quad \{A, N_A\}_{\mathrm{pub}(I)}$

$I \to A \quad \{N_A, N_B\}_{\mathrm{pub}(A)}$

$A \to I \quad \{N_B\}_{\mathrm{pub}(I)}$

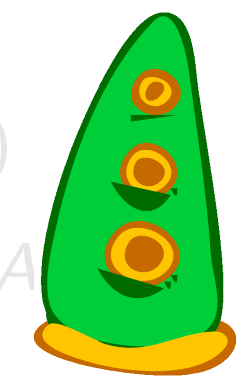


Intrus

$I(A) \to B \quad \{A, N_A\}_{\mathrm{pub}(B)}$

$B \to I(A) \quad \{N_A, N_B\}_{\mathrm{pub}(A)}$

$I(A) \to B \quad \{N_B\}_{\mathrm{pub}(B)}$

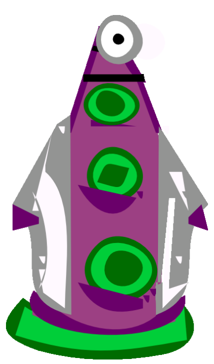


Bob

Une attaque sur Needham-Schroeder

- ★ $A \to I \quad \{A, N_A\}_{\mathrm{pub}(I)}$
- ★ $I \to A \quad \{N_A, N_I\}_{\mathrm{pub}(A)}$
- ★ $A \to I \quad \{N_I\}_{\mathrm{pub}(I)}$

- ★ $A \to B \quad \{A, N_A\}_{\mathrm{pub}(B)}$
- ★ $B \to A \quad \{N_A, N_B\}_{\mathrm{pub}(A)}$
- ★ $A \to B \quad \{N_B\}_{\mathrm{pub}(B)}$

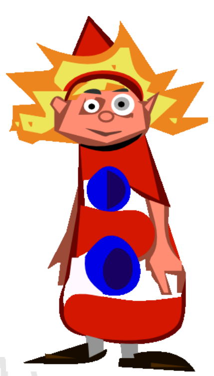


Alice

$A \to I \quad \{A, N_A\}_{\mathrm{pub}(I)}$

$I \to A \quad \{N_A, N_B\}_{\mathrm{pub}(A)}$

$A \to I \quad \{N_B\}_{\mathrm{pub}(I)}$

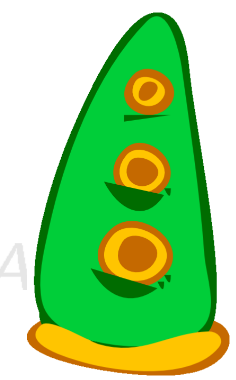


Intrus

$I(A) \to B \quad \{A, N_A\}_{\mathrm{pub}(B)}$

$B \to I(A) \quad \{N_A, N_B\}_{\mathrm{pub}(A)}$

$I(A) \to B \quad \{N_B\}_{\mathrm{pub}(B)}$

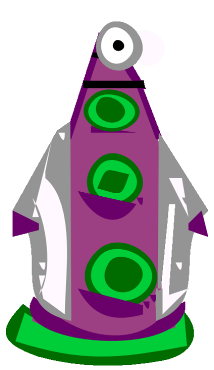


Bob

Une attaque sur Needham-Schroeder

- $A \rightarrow I \quad \{A, N_A\}_{\mathrm{pub}(I)}$
- $I \rightarrow A \quad \{N_A, N_I\}_{\mathrm{pub}(A)}$
- $A \rightarrow I \quad \{N_I\}_{\mathrm{pub}(I)}$

- $A \rightarrow B \quad \{A, N_A\}_{\mathrm{pub}(B)}$
- $B \rightarrow A \quad \{N_A, N_B\}_{\mathrm{pub}(A)}$
- $A \rightarrow B \quad \{N_B\}_{\mathrm{pub}(B)}$

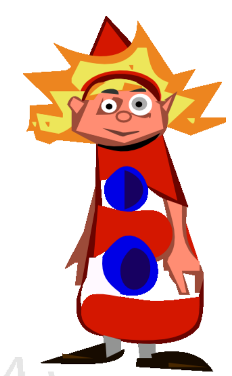


Alice

$A \rightarrow I \quad \{A, N_A\}_{\mathrm{pub}(I)}$

$I \rightarrow A \quad \{N_A, N_B\}_{\mathrm{pub}(A)}$

$A \rightarrow I \quad \{N_B\}_{\mathrm{pub}(I)}$

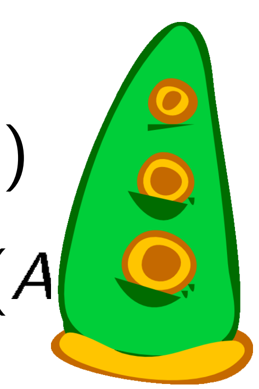


Intrus

$I(A) \rightarrow B \quad \{A, N_A\}_{\mathrm{pub}(B)}$

$B \rightarrow I(A) \quad \{N_A, N_B\}_{\mathrm{pub}(A)}$

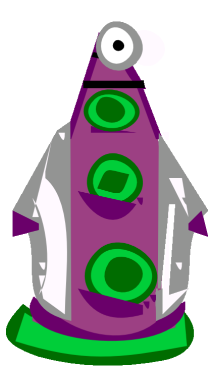
$I(A) \rightarrow B \quad \{N_B\}_{\mathrm{pub}(B)}$



Bob

Une attaque sur Needham-Schroeder

★	$A \to I$	$\{A, N_A\}_{\mathrm{pub}(I)}$	★	$A \to B$	$\{A, N_A\}_{\mathrm{pub}(B)}$
★	$I \to A$	$\{N_A, N_I\}_{\mathrm{pub}(A)}$	★	$B \to A$	$\{N_A, N_B\}_{\mathrm{pub}(A)}$
★	$A \to I$	$\{N_I\}_{\mathrm{pub}(I)}$	★	$A \to B$	$\{N_B\}_{\mathrm{pub}(B)}$

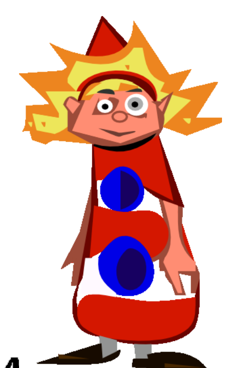


Alice

$A \to I \quad \{A, N_A\}_{\mathrm{pub}(I)}$

$I \to A \quad \{N_A, N_B\}_{\mathrm{pub}(A)}$

$A \to I \quad \{N_B\}_{\mathrm{pub}(I)}$

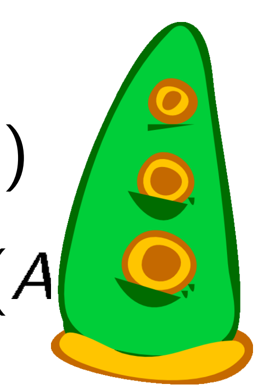


Intrus

$I(A) \to B \quad \{A, N_A\}_{\mathrm{pub}(B)}$

$B \to I(A) \quad \{N_A, N_B\}_{\mathrm{pub}(A)}$

$I(A) \to B \quad \{N_B\}_{\mathrm{pub}(B)}$

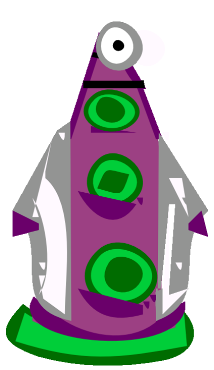


Bob

Une attaque sur Needham-Schroeder

- $A \to I \quad \{A, N_A\}_{\mathrm{pub}(I)}$
- $I \to A \quad \{N_A, N_I\}_{\mathrm{pub}(A)}$
- $A \to I \quad \{N_I\}_{\mathrm{pub}(I)}$

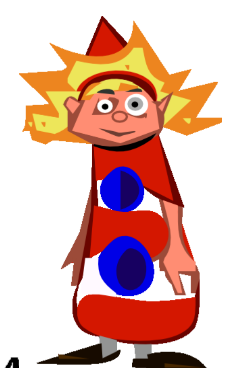
- $A \to B \quad \{A, N_A\}_{\mathrm{pub}(B)}$
- $B \to A \quad \{N_A, N_B\}_{\mathrm{pub}(A)}$
- $A \to B \quad \{N_B\}_{\mathrm{pub}(B)}$


Alice

$A \to I \quad \{A, N_A\}_{\mathrm{pub}(I)}$

$I \to A \quad \{N_A, N_B\}_{\mathrm{pub}(A)}$

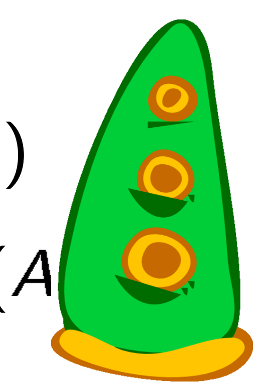
$A \to I \quad \{N_B\}_{\mathrm{pub}(I)}$


Intrus

$I(A) \to B \quad \{A, N_A\}_{\mathrm{pub}(B)}$

$B \to I(A) \quad \{N_A, N_B\}_{\mathrm{pub}(A)}$

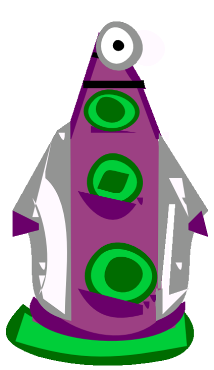
$I(A) \to B \quad \{N_B\}_{\mathrm{pub}(B)}$


Bob

Une attaque sur Needham-Schroeder

- $A \to I \quad \{A, N_A\}_{\mathrm{pub}(I)}$
- $I \to A \quad \{N_A, N_I\}_{\mathrm{pub}(A)}$
- $A \to I \quad \{N_I\}_{\mathrm{pub}(I)}$

- $A \to B \quad \{A, N_A\}_{\mathrm{pub}(B)}$
- $B \to A \quad \{N_A, N_B\}_{\mathrm{pub}(A)}$
- $A \to B \quad \{N_B\}_{\mathrm{pub}(B)}$



Alice

$A \to I \quad \{A, N_A\}_{\mathrm{pub}(I)}$

$I \to A \quad \{N_A, N_B\}_{\mathrm{pub}(A)}$

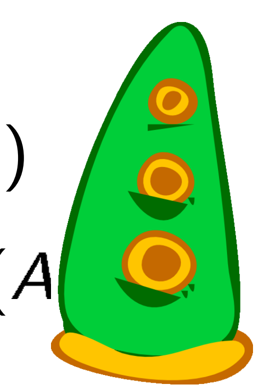
$A \to I \quad \{N_B\}_{\mathrm{pub}(I)}$

Intrus

$I(A) \to B \quad \{A, N_A\}_{\mathrm{pub}(B)}$

$B \to I(A) \quad \{N_A, N_B\}_{\mathrm{pub}(A)}$

$I(A) \to B \quad \{N_B\}_{\mathrm{pub}(B)}$



Bob

L'intrus de Dolev-Yao

Capacités de l'intrus :

- Contrôler le réseau
  - lire tout message y circulant
  - détruire un message
  - Injecter un message
- Cryptographie parfaite
  - chiffrer un message
  - déchiffrer un message s'il connaît la clef

Ce modèle d'intrus date de 1981.

L'intrus de Dolev-Yao

Capacités de l'intrus :

- Contrôler le réseau
  - lire tout message y circulant
  - détruire un message
  - Injecter un message
- Cryptographie parfaite
  - chiffrer un message
  - déchiffrer un message s'il connaît la clef

Ce modèle d'intrus date de 1981.

L'intrus de Dolev-Yao

Capacités de l'intrus :

- Contrôler le réseau
  - lire tout message y circulant
  - détruire un message
  - Injecter un message
- Cryptographie parfaite
  - chiffrer un message
  - déchiffrer un message s'il connaît la clef

Ce modèle d'intrus date de 1981.

L'intrus de Dolev-Yao

Capacités de l'intrus :

- Contrôler le réseau
  - lire tout message y circulant
  - détruire un message
  - Injecter un message
- Cryptographie parfaite
  - chiffrer un message
  - déchiffrer un message s'il connaît la clef

Ce modèle d'intrus date de 1981.

L'intrus de Dolev-Yao

Capacités de l'intrus :

- Contrôler le réseau
  - lire tout message y circulant
  - détruire un message
  - Injecter un message
- Cryptographie parfaite
  - chiffrer un message
  - déchiffrer un message s'il connaît la clef

Ce modèle d'intrus date de 1981.

L'intrus de Dolev-Yao

Capacités de l'intrus :

- Contrôler le réseau
  - lire tout message y circulant
  - détruire un message
  - Injecter un message
- Cryptographie parfaite
  - chiffrer un message
  - déchiffrer un message s'il connaît la clef

Ce modèle d'intrus date de 1981.

L'intrus de Dolev-Yao

Capacités de l'intrus :

- Contrôler le réseau
  - lire tout message y circulant
  - détruire un message
  - Injecter un message
- Cryptographie parfaite
  - chiffrer un message
  - déchiffrer un message s'il connaît la clef

Ce modèle d'intrus date de 1981.

L'intrus de Dolev-Yao

Capacités de l'intrus :

- Contrôler le réseau
  - lire tout message y circulant
  - détruire un message
  - Injecter un message
- Cryptographie parfaite
  - chiffrer un message
  - déchiffrer un message s'il connaît la clef

Ce modèle d'intrus date de 1981.

Raffinement du modèle de l'intrus

Actuellement, de nombreuses applications nécessitent un modèle d'intrus disposant de capacités supplémentaires :

- sécurisation d'un réseau sans-fil (WEP)
- porte-monnaie électronique
- vote électronique
- vidéo à la demande

La modélisation de l'intrus est différente dans chacune de ces applications.

Raffinement du modèle de l'intrus

Actuellement, de nombreuses applications nécessitent un modèle d'intrus disposant de capacités supplémentaires :

- sécurisation d'un réseau sans-fil (WEP)
- porte-monnaie électronique
- vote électronique
- vidéo à la demande

La modélisation de l'intrus est différente dans chacune de ces applications.

Raffinement du modèle de l'intrus

Actuellement, de nombreuses applications nécessitent un modèle d'intrus disposant de capacités supplémentaires :

- sécurisation d'un réseau sans-fil (WEP)
- porte-monnaie électronique
- vote électronique
- vidéo à la demande

La modélisation de l'intrus est différente dans chacune de ces applications.

Raffinement du modèle de l'intrus

Actuellement, de nombreuses applications nécessitent un modèle d'intrus disposant de capacités supplémentaires :

- sécurisation d'un réseau sans-fil (WEP)
- porte-monnaie électronique
- vote électronique
- vidéo à la demande

La modélisation de l'intrus est différente dans chacune de ces applications.

Objectif

- Prendre en paramètre la théorie de l'intrus dans le cadre de la vérification automatique des protocoles et traiter de manière uniforme les cas nombre fixe et non borné de sessions.

Des résultats de vérification automatique

- Problème de déduction de l'intrus : [Comon-Lundh, Treinen, 2003]
- Problème de sécurité :

Intrus de Dolev-Yao : [Amadio, Lugiez, 2000] et [Rusinowitch, Turuani, 2001]
Cas du « ou exclusif » : [Chevalier, Küsters, Rusinowitch, Turuani, 2003] et [Comon-Lundh, Shmatikov, 2003]
« ou exclusif » et homomorphisme : [Delaune, Lafourcade, Lugiez, Treinen, 2006]
Diffie-Hellman : [Chevalier, Küster, Rusinowitch, Turuani, 2003]
CBC et camouflage : [Cortier, Rusinowitch, Zalinescu, 2005]
Chiffrement probabiliste et attaques par dictionnaire : [Delaune, Jacquemard, 2004]

Des résultats de vérification automatique

- Problème de déduction de l'intrus : [Comon-Lundh, Treinen, 2003]
- Problème de sécurité :

  Intrus de Dolev-Yao : [Amadio, Lugiez, 2000] et [Rusinowitch, Turuani, 2001]

  Cas du « ou exclusif » : [Chevalier, Küsters, Rusinowitch, Turuani, 2003] et [Comon-Lundh, Shmatikov, 2003]

  « ou exclusif » et homomorphisme : [Delaune, Lafourcade, Lugiez, Treinen, 2006]

  Diffie-Hellman : [Chevalier, Küster, Rusinowitch, Turuani, 2003]

  CBC et camouflage : [Cortier, Rusinowitch, Zalinescu, 2005]

  Chiffrement probabiliste et attaques par dictionnaire : [Delaune, Jacquemard, 2004]

Plan

1. Cas passif : introduction
2. Protocoles comme capacité supplémentaire de l'intrus
3. Théorème de normalisation
4. Algorithme de décision

Plan

L'intrus passif

L'intrus passif peut observer les messages qui circulent sur le réseau. Cependant, il ne peut pas les modifier ou en envoyer.
Il dispose d'un système de règles d'inférences pour déduire des termes dont le but est de construire des preuves menant à un secret s.

Système d'inférence de Dolev-Yao

$$\frac{T \vdash m_1 \qquad T \vdash m_2}{T \vdash \langle m_1, m_2 \rangle} \qquad \frac{T \vdash \langle m_1, m_2 \rangle}{T \vdash m_1} \qquad \frac{T \vdash \langle m_1, m_2 \rangle}{T \vdash m_2}$$

$$\frac{T \vdash m \qquad T \vdash k}{T \vdash \{m\}_k} \qquad \frac{T \vdash \{m\}_k \qquad T \vdash k}{T \vdash m} \qquad \frac{m \in T}{T \vdash m}$$

L'intrus passif

L'intrus passif peut observer les messages qui circulent sur le réseau. Cependant, il ne peut pas les modifier ou en envoyer.
Il dispose d'un système de règles d'inférences pour déduire des termes dont le but est de construire des preuves menant à un secret s.

Système d'inférence de Dolev-Yao

$$\frac{T \vdash m_1 \qquad T \vdash m_2}{T \vdash \langle m_1, m_2 \rangle} \qquad \frac{T \vdash \langle m_1, m_2 \rangle}{T \vdash m_1} \qquad \frac{T \vdash \langle m_1, m_2 \rangle}{T \vdash m_2}$$

$$\frac{T \vdash m \qquad T \vdash k}{T \vdash \{m\}_k} \qquad \frac{T \vdash \{m\}_k \qquad T \vdash k}{T \vdash m} \qquad \frac{m \in T}{T \vdash m}$$

Problème du secret

Le problème de déductibilité du secret est généralement décidable grâce à une propriété de sous-formule [Comon-Lundh, Treinen, 2003] appelée localité selon [McAllester, 1993].

Théorème (Localité)

Pour toute preuve Π de $T \vdash s$ dans le système d'inférence de Dolev-Yao, il existe une preuve Π' de $T \vdash s$ telle que :

- *si Π' termine par un chiffrement ou un appariement, alors Π' n'utilise que des sous-termes de $T \cup \{s\}$*
- *sinon, Π' n'utilise que des sous-termes de T*

Problème du secret

Le problème de déductibilité du secret est généralement décidable grâce à une propriété de sous-formule [Comon-Lundh, Treinen, 2003] appelée localité selon [McAllester, 1993].

Théorème (Localité)

Pour toute preuve Π de $T \vdash s$ dans le système d'inférence de Dolev-Yao, il existe une preuve Π' de $T \vdash s$ telle que :

- *si Π' termine par un chiffrement ou un appariement, alors Π' n'utilise que des sous-termes de $T \cup \{s\}$*
- *sinon, Π' n'utilise que des sous-termes de T*

Preuve du théorème de localité

On procède par récurrence sur la taille de la preuve.

- Cas de base :

$$\frac{}{T, u \vdash u}$$

  u est bien sous-terme de T, u.

- Cas récursif. On examine la dernière règle.
  1. Chiffrement ou appariement :

  $$\frac{T \vdash m \qquad T \vdash k}{T \vdash \{m\}_k}$$

  m et k sous-termes de $\{m\}_k$
  2. Déchiffrement ou projection :

  $$\frac{T \vdash \{m\}_k \qquad T \vdash k}{T \vdash m}$$

  $\{m\}_k$ provient soit d'une décomposition, soit d'un chiffrement. Dans le second cas, on dispose d'une preuve plus courte de

Preuve du théorème de localité

On procède par récurrence sur la taille de la preuve.

- Cas de base :

$$\frac{}{T, u \vdash u}$$

  u est bien sous-terme de T, u.

- Cas récursif. On examine la dernière règle.
  1. Chiffrement ou appariement :

  $$\frac{T \vdash m \qquad T \vdash k}{T \vdash \{m\}_k}$$

  m et k sous-termes de $\{m\}_k$

  2. Déchiffrement ou projection :

  $$\frac{T \vdash \{m\}_k \qquad T \vdash k}{T \vdash m}$$

Preuve du théorème de localité

On procède par récurrence sur la taille de la preuve.

- Cas de base :

$$\frac{}{T, u \vdash u}$$

u est bien sous-terme de T, u.

- Cas récursif. On examine la dernière règle.

1. Chiffrement ou appariement :

$$\frac{T \vdash m \qquad T \vdash k}{T \vdash \{m\}_k}$$

m et k sous-termes de $\{m\}_k$

2. Déchiffrement ou projection :

$$\frac{T \vdash \{m\}_k \qquad T \vdash k}{T \vdash m}$$

$\{m\}_k$ provient soit d'une décomposition, soit d'un chiffrement. Dans le second cas, on dispose d'une preuve plus courte de m.

Preuve du théorème de localité

On procède par récurrence sur la taille de la preuve.

- Cas de base :

$$\frac{}{T, u \vdash u}$$

  u est bien sous-terme de T, u.

- Cas récursif. On examine la dernière règle.
  1. Chiffrement ou appariement :

  $$\frac{T \vdash m \qquad T \vdash k}{T \vdash \{m\}_k}$$

     m et k sous-termes de $\{m\}_k$
  2. Déchiffrement ou projection :

  $$\frac{T \vdash \{m\}_k \qquad T \vdash k}{T \vdash m}$$

     $\{m\}_k$ provient soit d'une décomposition, soit d'un chiffrement. Dans le second cas, on dispose d'une preuve plus courte de m.

Preuve du théorème de localité

On procède par récurrence sur la taille de la preuve.

- Cas de base :

$$\frac{}{T, u \vdash u}$$

  u est bien sous-terme de T, u.
- Cas récursif. On examine la dernière règle.
  1. Chiffrement ou appariement :

  $$\frac{T \vdash m \qquad T \vdash k}{T \vdash \{m\}_k}$$

     m et k sous-termes de $\{m\}_k$
  2. Déchiffrement ou projection :

  $$\frac{T \vdash \{m\}_k \qquad T \vdash k}{T \vdash m}$$

     $\{m\}_k$ provient soit d'une décomposition, soit d'un chiffrement. Dans le second cas, on dispose d'une preuve plus courte de m.

Preuve du théorème de localité

$$
\dfrac{\dfrac{\dfrac{\Pi_1}{T \vdash m} \quad \dfrac{\Pi_2}{T \vdash k}}{T \vdash \{m\}_k} \quad \dfrac{\Pi_3}{T \vdash k}}{T \vdash m} \quad \rightarrow \quad \dfrac{\Pi_1}{T \vdash m}
$$

Objectif

- Prendre en paramètre la théorie de l'intrus dans le cadre de la vérification automatique des protocoles et traiter de manière uniforme les cas nombre fixe et non borné de sessions.
- Généraliser la propriété de localité à l'intrus actif : les règles de protocole s'ajoutent au pouvoir de l'intrus.

Plan

Inclure les règles de protocole dans le pouvoir de l'intrus

Le protocole de Needham-Schroeder est décrit suivant ce formalisme :

« Alice »

	réception		émission
1.		$\longrightarrow$	$\{A, N_A\}_{\mathrm{pub}(B)}$
2.	$\{N_A, x\}_{\mathrm{pub}(A)}$	$\longrightarrow$	$\{x\}_{\mathrm{pub}(B)}$

« Bob »

	réception		émission
1.	$\{y, z\}_{\mathrm{pub}(B)}$	$\longrightarrow$	$\{z, N_B\}_{\mathrm{pub}(y)}$
2.	$\{N_B\}_{\mathrm{pub}(B)}$	$\longrightarrow$	

Si $u \longrightarrow v$ est une règle de protocole, pour tout σ :

$$\frac{T \vdash u\sigma}{T \vdash v\sigma}$$

Il n'y a pas de contrôle sur σ. Difficile d'obtenir la localité.

Inclure les règles de protocole dans le pouvoir de l'intrus

Le protocole de Needham-Schroeder est décrit suivant ce formalisme :

« Alice »

	réception		émission
1.		$\longrightarrow$	$\{A, N_A\}_{\mathrm{pub}(B)}$
2.	$\{N_A, x\}_{\mathrm{pub}(A)}$	$\longrightarrow$	$\{x\}_{\mathrm{pub}(B)}$

« Bob »

	réception		émission
1.	$\{y, z\}_{\mathrm{pub}(B)}$	$\longrightarrow$	$\{z, N_B\}_{\mathrm{pub}(y)}$
2.	$\{N_B\}_{\mathrm{pub}(B)}$	$\longrightarrow$	

Si $u \longrightarrow v$ est une règle de protocole, pour tout σ :

$$\frac{T \vdash u\sigma}{T \vdash v\sigma}$$

Il n'y a pas de contrôle sur σ. Difficile d'obtenir la localité.

Inclure les règles de protocole dans le pouvoir de l'intrus

Le protocole de Needham-Schroeder est décrit suivant ce formalisme :

« Alice »

	réception		émission
1.		$\longrightarrow$	$\{A, N_A\}_{\mathrm{pub}(B)}$
2.	$\{N_A, x\}_{\mathrm{pub}(A)}$	$\longrightarrow$	$\{x\}_{\mathrm{pub}(B)}$

« Bob »

	réception		émission
1.	$\{y, z\}_{\mathrm{pub}(B)}$	$\longrightarrow$	$\{z, N_B\}_{\mathrm{pub}(y)}$
2.	$\{N_B\}_{\mathrm{pub}(B)}$	$\longrightarrow$	

Si $u \longrightarrow v$ est une règle de protocole, pour tout σ :

$$\frac{T \vdash u\sigma}{T \vdash v\sigma}$$

Il n'y a pas de contrôle sur σ. Difficile d'obtenir la localité.

Notre approche : utiliser des séquents contraints

Dans [Rusinowitch, Turuani, 2001], σ est bornée par une propriété de sous-formule. Notre approche consiste alors à conserver σ à part.

$$\frac{T \vdash u\sigma}{T \vdash v\sigma} \quad \rightarrow$$

L'intrus peut également instancier des termes :

$$\frac{T \vdash x \;\; [\![x = u \wedge E]\!]}{T \vdash u \;\; [\![x = u \wedge E]\!]}\,\mathcal{I}$$

Les règles de base sont étendues aux séquents contraints :

$$\frac{T \vdash m \;\; [\![E_1]\!] \quad T \vdash k \;\; [\![E_2]\!]}{T \vdash \{m\}_k \;\; [\![E_1 \wedge E_2]\!]}\,\mathcal{S}$$

Cela comprend l'axiome :

$$\frac{m \in T}{T \vdash m \;\; [\![]\!]}$$

Notre approche : utiliser des séquents contraints

Dans [Rusinowitch, Turuani, 2001], σ est bornée par une propriété de sous-formule. Notre approche consiste alors à conserver σ à part.

$$\frac{T \vdash u\sigma}{T \vdash v\sigma} \quad \rightarrow \quad \frac{T \vdash u \;\; [\![\sigma]\!]}{T \vdash v \;\; [\![\sigma]\!]}$$

L'intrus peut également instancier des termes :

$$\frac{T \vdash x \;\; [\![x = u \wedge E]\!]}{T \vdash u \;\; [\![x = u \wedge E]\!]}\,\mathcal{I}$$

Les règles de base sont étendues aux séquents contraints :

$$\frac{T \vdash m \;\; [\![E_1]\!] \quad T \vdash k \;\; [\![E_2]\!]}{T \vdash \{m\}_k \;\; [\![E_1 \wedge E_2]\!]}\,\mathcal{S}$$

Cela comprend l'axiome :

$$\frac{m \in T}{T \vdash m \;\; [\![]\!]}$$

Notre approche : utiliser des séquents contraints

Dans [Rusinowitch, Turuani, 2001], σ est bornée par une propriété de sous-formule. Notre approche consiste alors à conserver σ à part.

$$\frac{T \vdash u\sigma}{T \vdash v\sigma} \quad \rightarrow \quad \frac{T \vdash w \ \llbracket E \rrbracket}{T \vdash v \ \llbracket E \wedge u = w \rrbracket}\,\mathcal{P}$$

L'intrus peut également instancier des termes :

$$\frac{T \vdash x \ \llbracket x = u \wedge E \rrbracket}{T \vdash u \ \llbracket x = u \wedge E \rrbracket}\,\mathcal{I}$$

Les règles de base sont étendues aux séquents contraints :

$$\frac{T \vdash m \ \llbracket E_1 \rrbracket \quad T \vdash k \ \llbracket E_2 \rrbracket}{T \vdash \{m\}_k \ \llbracket E_1 \wedge E_2 \rrbracket}\,\mathcal{S}$$

Cela comprend l'axiome :

$$\frac{m \in T}{T \vdash m \ \llbracket\rrbracket}$$

Notre approche : utiliser des séquents contraints

Dans [Rusinowitch, Turuani, 2001], σ est bornée par une propriété de sous-formule. Notre approche consiste alors à conserver σ à part.

$$\frac{T \vdash u\sigma}{T \vdash v\sigma} \quad \rightarrow \quad \frac{T \vdash w \;\; [\![E]\!]}{T \vdash v \;\; [\![E \wedge u = w]\!]}\,\mathcal{P}$$

L'intrus peut également instancier des termes :

$$\frac{T \vdash x \;\; [\![x = u \wedge E]\!]}{T \vdash u \;\; [\![x = u \wedge E]\!]}\,\mathcal{I}$$

Les règles de base sont étendues aux séquents contraints :

$$\frac{T \vdash m \;\; [\![E_1]\!] \quad T \vdash k \;\; [\![E_2]\!]}{T \vdash \{m\}_k \;\; [\![E_1 \wedge E_2]\!]}\,\mathcal{S}$$

Cela comprend l'axiome :

$$\frac{m \in T}{T \vdash m \;\; [\![]\!]}$$

Notre approche : utiliser des séquents contraints

Dans [Rusinowitch, Turuani, 2001], σ est bornée par une propriété de sous-formule. Notre approche consiste alors à conserver σ à part.

$$\frac{T \vdash u\sigma}{T \vdash v\sigma} \quad \rightarrow \quad \frac{T \vdash w \;\; [\![E]\!]}{T \vdash v \;\; [\![E \wedge u = w]\!]}\,\mathcal{P}$$

L'intrus peut également instancier des termes :

$$\frac{T \vdash x \;\; [\![x = u \wedge E]\!]}{T \vdash u \;\; [\![x = u \wedge E]\!]}\,\mathcal{I}$$

Les règles de base sont étendues aux séquents contraints :

$$\frac{T \vdash m \;\; [\![E_1]\!] \qquad T \vdash k \;\; [\![E_2]\!]}{T \vdash \{m\}_k \;\; [\![E_1 \wedge E_2]\!]}\,\mathcal{S}$$

Cela comprend l'axiome :

$$\frac{m \in T}{T \vdash m \;\; [\![]\!]}$$

Notre approche : utiliser des séquents contraints

Dans [Rusinowitch, Turuani, 2001], σ est bornée par une propriété de sous-formule. Notre approche consiste alors à conserver σ à part.

$$\frac{T \vdash u\sigma}{T \vdash v\sigma} \quad \rightarrow \quad \frac{T \vdash w \ \llbracket E \rrbracket}{T \vdash v \ \llbracket E \wedge u = w \rrbracket}\mathcal{P}$$

L'intrus peut également instancier des termes :

$$\frac{T \vdash x \ \llbracket x = u \wedge E \rrbracket}{T \vdash u \ \llbracket x = u \wedge E \rrbracket}\mathcal{I}$$

Les règles de base sont étendues aux séquents contraints :

$$\frac{T \vdash m \ \llbracket E_1 \rrbracket \quad T \vdash k \ \llbracket E_2 \rrbracket}{T \vdash \{m\}_k \ \llbracket E_1 \wedge E_2 \rrbracket}\mathcal{S}$$

Cela comprend l'axiome :

$$\frac{m \in T}{T \vdash m \ \llbracket\rrbracket}$$

Correction et complétude

Théorème

$T \vdash s \; [\![E]\!]$ est déductible et E satisfaisable si et seulement s'il existe une attaque contre le secret s sur le protocole.

Nous travaillons avec un nombre fixe ou non borné de sessions.

Correction et complétude

Théorème

$T \vdash s \ \llbracket E \rrbracket$ est déductible et E satisfaisable si et seulement s'il existe une attaque contre le secret s sur le protocole.

Nous travaillons avec un nombre fixe ou non borné de sessions.

Plan

Énoncé dans le cas de Dolev-Yao

Dans le cas de Dolev-Yao, il est possible d'étendre le théorème de localité ainsi :

Théorème (Normalisation dans le cas de Dolev-Yao)

Il existe une fonction F tel que pour tout protocole V et tout ensemble de termes T, $T \vdash s\ [\![E]\!]$ est déductible et E satisfaisable si et seulement s'il existe une preuve n'utilisant que des séquents $T \vdash u\ [\![E']\!]$ où :

- *$u \in F(V, T, s)$ si u est issu d'une composition et $u \in F(V, T)$ sinon*
- *E' est constitué d'égalités entre termes de $F(V, T)$.*

La preuve se fait par récurrence sur la taille de $T \vdash s\ [\![E]\!]$. On discrimine sur la dernière règle.

Énoncé dans le cas de Dolev-Yao

Dans le cas de Dolev-Yao, il est possible d'étendre le théorème de localité ainsi :

Théorème (Normalisation dans le cas de Dolev-Yao)

Il existe une fonction F tel que pour tout protocole V et tout ensemble de termes T, $T \vdash s \ \llbracket E \rrbracket$ est déductible et E satisfaisable si et seulement s'il existe une preuve n'utilisant que des séquents $T \vdash u \ \llbracket E' \rrbracket$ où :

- *$u \in F(V, T, s)$ si u est issu d'une composition et $u \in F(V, T)$ sinon*
- *E' est constitué d'égalités entre termes de $F(V, T)$.*

La preuve se fait par récurrence sur la taille de $T \vdash s \ \llbracket E \rrbracket$. On discrimine sur la dernière règle.

Règle de protocole

$$\frac{T \vdash w \ [\![E]\!]}{T \vdash v \ [\![E \wedge u = w]\!]}$$

- v est sous-terme de V donc dans $F(V,T)$.
- si w est dans $F(V,T)$, l'hypothèse de récurrence suffit pour conclure.
- sinon, w est issu de compositions et on peut alors remplacer certains sous-termes de w, liés à une variable de u, par $\star$ pour obtenir une preuve de $T \vdash w' \ [\![E']\!]$ où $w' \in F(V,T)$.

Exemple avec $w = \{\{a\}_b\}_c$, $u = \{x\}_c$ et $\{a\}_b \notin F(V,T)$:

$$\frac{\dfrac{T \vdash a \ [\![E_1]\!] \quad T \vdash b \ [\![E_2]\!]}{T \vdash \{a\}_b \ [\![\ldots]\!]} \qquad T \vdash c \ [\![E_3]\!]}{T \vdash \{\{a\}_b\}_c \ [\![\ldots]\!]} \quad \rightarrow \quad \frac{T \vdash \star \ [\![\ldots]\!] \quad T \vdash c \ [\![E_3]\!]}{T \vdash \{\star\}_c \ [\![\ldots]\!]}$$

Règle de protocole

$$\frac{T \vdash w \;\; [\![E]\!]}{T \vdash v \;\; [\![E \wedge u = w]\!]}$$

- v est sous-terme de V donc dans $F(V, T)$.
- si w est dans $F(V, T)$, l'hypothèse de récurrence suffit pour conclure.
- sinon, w est issu de compositions et on peut alors remplacer certains sous-termes de w, liés à une variable de u, par $\star$ pour obtenir une preuve de $T \vdash w' \;\; [\![E']\!]$ où $w' \in F(V, T)$.

Exemple avec $w = \{\{a\}_b\}_c$, $u = \{x\}_c$ et $\{a\}_b \notin F(V, T)$:

$$\frac{\dfrac{T \vdash a \;\; [\![E_1]\!] \quad T \vdash b \;\; [\![E_2]\!]}{T \vdash \{a\}_b \;\; [\![\ldots]\!]} \qquad T \vdash c \;\; [\![E_3]\!]}{T \vdash \{\{a\}_b\}_c \;\; [\![\ldots]\!]} \rightarrow \frac{T \vdash \star \;\; [\![\ldots]\!] \quad T \vdash c \;\; [\![E_3]\!]}{T \vdash \{\star\}_c \;\; [\![\ldots]\!]}$$

Règle de protocole

$$\frac{T \vdash w \ \ \llbracket E \rrbracket}{T \vdash v \ \ \llbracket E \wedge u = w \rrbracket}$$

- v est sous-terme de V donc dans $F(V, T)$.
- si w est dans $F(V, T)$, l'hypothèse de récurrence suffit pour conclure.
- sinon, w est issu de compositions et on peut alors remplacer certains sous-termes de w, liés à une variable de u, par $\star$ pour obtenir une preuve de $T \vdash w' \ \ \llbracket E' \rrbracket$ où $w' \in F(V, T)$.

Exemple avec $w = \{\{a\}_b\}_c$, $u = \{x\}_c$ et $\{a\}_b \notin F(V, T)$:

$$\frac{\dfrac{T \vdash a \ \ \llbracket E_1 \rrbracket \quad T \vdash b \ \ \llbracket E_2 \rrbracket}{T \vdash \{a\}_b \ \ \llbracket \ldots \rrbracket} \qquad T \vdash c \ \ \llbracket E_3 \rrbracket}{T \vdash \{\{a\}_b\}_c \ \ \llbracket \ldots \rrbracket} \rightarrow \frac{T \vdash \star \ \ \llbracket \ldots \rrbracket \quad T \vdash c \ \ \llbracket E_3 \rrbracket}{T \vdash \{\star\}_c \ \ \llbracket \ldots \rrbracket}$$

Règle de protocole

$$\frac{T \vdash w \;\; [\![E]\!]}{T \vdash v \;\; [\![E \wedge u = w]\!]}$$

- v est sous-terme de V donc dans $F(V, T)$.
- si w est dans $F(V, T)$, l'hypothèse de récurrence suffit pour conclure.
- sinon, w est issu de compositions et on peut alors remplacer certains sous-termes de w, liés à une variable de u, par $\bigstar$ pour obtenir une preuve de $T \vdash w' \;\; [\![E']\!]$ où $w' \in F(V, T)$.

Exemple avec $w = \{\{a\}_b\}_c$, $u = \{x\}_c$ et $\{a\}_b \notin F(V, T)$:

$$\frac{\dfrac{T \vdash a \;\; [\![E_1]\!] \quad T \vdash b \;\; [\![E_2]\!]}{T \vdash \{a\}_b \;\; [\![\ldots]\!]} \qquad T \vdash c \;\; [\![E_3]\!]}{T \vdash \{\{a\}_b\}_c \;\; [\![\ldots]\!]} \rightarrow \frac{T \vdash \bigstar \;\; [\![\ldots]\!] \quad T \vdash c \;\; [\![E_3]\!]}{T \vdash \{\bigstar\}_c \;\; [\![\ldots]\!]}$$

Règle de protocole

$$\frac{T \vdash w \ \ [\![E]\!]}{T \vdash v \ \ [\![E \wedge u = w]\!]}$$

- v est sous-terme de V donc dans $F(V,T)$.
- si w est dans $F(V,T)$, l'hypothèse de récurrence suffit pour conclure.
- sinon, w est issu de compositions et on peut alors remplacer certains sous-termes de w, liés à une variable de u, par $\bigstar$ pour obtenir une preuve de $T \vdash w' \ \ [\![E']\!]$ où $w' \in F(V,T)$.

Exemple avec $w = \{\{a\}_b\}_c$, $u = \{x\}_c$ et $\{a\}_b \notin F(V,T)$:

$$\frac{\dfrac{T \vdash a \ \ [\![E_1]\!] \quad T \vdash b \ \ [\![E_2]\!]}{T \vdash \{a\}_b \ \ [\![\ldots]\!]} \qquad T \vdash c \ \ [\![E_3]\!]}{T \vdash \{\{a\}_b\}_c \ \ [\![\ldots]\!]} \quad \rightarrow \quad \frac{T \vdash \bigstar \ \ [\![\ldots]\!] \quad T \vdash c \ \ [\![E_3]\!]}{T \vdash \{\bigstar\}_c \ \ [\![\ldots]\!]}$$

Règle d'instanciation

$$\frac{T \vdash x \ \llbracket x = u \wedge E \rrbracket}{T \vdash u \ \llbracket x = u \wedge E \rrbracket}$$

Après application de l'hypothèse de récurrence, deux cas peuvent se présenter :

1. On obtient une preuve de $T \vdash x \ \llbracket x = u \wedge E' \rrbracket$. Dans ce cas, on applique l'instanciation comme auparavant. $u \in F(V, T)$ par hypothèse de récurrence.
2. On obtient une preuve de $T \vdash x \ \llbracket x = \star \wedge E' \rrbracket$. Il nous faut chercher une preuve de $T \vdash u \ \llbracket x = \star \wedge E' \rrbracket$ d'une autre façon.

Règle d'instanciation

$$\frac{T \vdash x \ \llbracket x = u \wedge E \rrbracket}{T \vdash u \ \llbracket x = u \wedge E \rrbracket}$$

Après application de l'hypothèse de récurrence, deux cas peuvent se présenter :

1. On obtient une preuve de $T \vdash x \ \llbracket x = u \wedge E' \rrbracket$. Dans ce cas, on applique l'instanciation comme auparavant. $u \in F(V, T)$ par hypothèse de récurrence.
2. On obtient une preuve de $T \vdash x \ \llbracket x = \star \wedge E' \rrbracket$. Il nous faut chercher une preuve de $T \vdash u \ \llbracket x = \star \wedge E' \rrbracket$ d'une autre façon.

Règle d'instanciation

$$\frac{T \vdash x \ [\![x = u \wedge E]\!]}{T \vdash u \ [\![x = u \wedge E]\!]}$$

Après application de l'hypothèse de récurrence, deux cas peuvent se présenter :

1. On obtient une preuve de $T \vdash x \ [\![x = u \wedge E']\!]$. Dans ce cas, on applique l'instanciation comme auparavant. $u \in F(V, T)$ par hypothèse de récurrence.
2. On obtient une preuve de $T \vdash x \ [\![x = \bigstar \wedge E']\!]$. Il nous faut chercher une preuve de $T \vdash u \ [\![x = \bigstar \wedge E']\!]$ d'une autre façon.

Règle d'instanciation

$$\dfrac{\begin{array}{c}\dfrac{\begin{array}{c}T \vdash u \;\; [\![\ldots]\!] \\ \vdots\, \mathcal{C} \\ T \vdash w \;\; [\![\ldots]\!]\end{array}}{T \vdash v \;\; [\![x = u \wedge \ldots]\!]}\,\mathcal{P} \\ \vdots \\ T \vdash x \;\; [\![x = u \wedge \ldots]\!]\end{array}}{T \vdash u \;\; [\![x = u \wedge \ldots]\!]}\,\mathcal{I}
\quad \rightarrow \quad
\dfrac{\begin{array}{c}\dfrac{\begin{array}{c}T \vdash \star \;\; [\![\ldots]\!] \\ \vdots\, \mathcal{C} \\ T \vdash w[u \leftarrow \star] \;\; [\![\ldots]\!]\end{array}}{T \vdash v \;\; [\![x = \star \wedge \ldots]\!]}\,\mathcal{P} \\ \vdots \\ T \vdash x \;\; [\![x = \star \wedge \ldots]\!]\end{array}}{T \vdash \star \;\; [\![x = \star \wedge \ldots]\!]}\,\mathcal{I}$$

On dispose d'une preuve de u dans la preuve originale !

Règle d'instanciation

$$
\begin{array}{c}
\color{red}{T \vdash u \;\; \llbracket \ldots \rrbracket} \\
\vdots \; \mathcal{C} \\
\dfrac{T \vdash w \;\; \llbracket \ldots \rrbracket}{T \vdash v \;\; \llbracket x = u \wedge \ldots \rrbracket}\,\mathcal{P} \\
\vdots \\
\dfrac{T \vdash x \;\; \llbracket x = u \wedge \ldots \rrbracket}{T \vdash u \;\; \llbracket x = u \wedge \ldots \rrbracket}\,\mathcal{I}
\end{array}
\quad \rightarrow \quad
\begin{array}{c}
T \vdash \bigstar \;\; \llbracket \ldots \rrbracket \\
\vdots \; \mathcal{C} \\
\dfrac{T \vdash w[u \leftarrow \bigstar] \;\; \llbracket \ldots \rrbracket}{T \vdash v \;\; \llbracket x = \bigstar \wedge \ldots \rrbracket}\,\mathcal{P} \\
\vdots \\
\dfrac{T \vdash x \;\; \llbracket x = \bigstar \wedge \ldots \rrbracket}{T \vdash \bigstar \;\; \llbracket x = \bigstar \wedge \ldots \rrbracket}\,\mathcal{I}
\end{array}
$$

On dispose d'une preuve de u dans la preuve originale !

Généralisation à d'autres intrus

On souhaite généraliser le théorème précédent à des intrus disposant de capacités supplémentaires :

CBC L'intrus est capable d'obtenir le préfixe d'un chiffré :

$$\frac{T \vdash \{m_1, m_2\}_k}{T \vdash \{m_1\}_k}$$

Signature en aveugle L'intrus est capable d'effectuer des signatures en aveugle [Chaum, 1982] :

$$\frac{T \vdash \mathrm{sign}(\mathrm{blind}(m, r), sk) \qquad T \vdash r}{T \vdash \mathrm{sign}(m, sk)}$$

$$\frac{T \vdash \mathrm{blind}(m, r) \qquad T \vdash r}{T \vdash m}$$

$$\frac{T \vdash \mathrm{sign}(m, sk) \qquad T \vdash \mathrm{pk}(sk)}{T \vdash m}$$

Généralisation à d'autres intrus

On souhaite généraliser le théorème précédent à des intrus disposant de capacités supplémentaires :

CBC L'intrus est capable d'obtenir le préfixe d'un chiffré :

$$\frac{T \vdash \{m_1, m_2\}_k}{T \vdash \{m_1\}_k}$$

Signature en aveugle L'intrus est capable d'effectuer des signatures en aveugle [Chaum, 1982] :

$$\frac{T \vdash \mathrm{sign}(\mathrm{blind}(m, r), sk) \qquad T \vdash r}{T \vdash \mathrm{sign}(m, sk)}$$

$$\frac{T \vdash \mathrm{blind}(m, r) \qquad T \vdash r}{T \vdash m}$$

$$\frac{T \vdash \mathrm{sign}(m, sk) \qquad T \vdash \mathrm{pk}(sk)}{T \vdash m}$$

Indécidabilité

Dans le cas général, on peut montrer par réduction du problème de Post, que la recherche du secret en nombre fixe de sessions est indécidable.

On est donc amené à prendre certaines restrictions sur les règles de composition et décomposition.

Indécidabilité

Dans le cas général, on peut montrer par réduction du problème de Post, que la recherche du secret en nombre fixe de sessions est indécidable.
On est donc amené à prendre certaines restrictions sur les règles de composition et décomposition.

Restriction sur les compositions

Désormais, une règle de composition est de la forme :

$$\frac{T \vdash u_1 \ \llbracket E_1 \rrbracket \quad \dots \quad T \vdash u_n \ \llbracket E_n \rrbracket}{T \vdash f(u_1, \dots, u_n) \ \llbracket E_1 \wedge \dots \wedge E_n \rrbracket} \mathcal{C}$$

Restriction sur les décompositions

Les règles de décomposition sont de la forme :

$$\frac{T \vdash t_1 \ \llbracket E_1 \rrbracket \quad \dots \quad T \vdash t_n \ \llbracket E_n \rrbracket}{T \vdash t \ \llbracket E_1 \wedge \dots \wedge E_n \rrbracket} \mathcal{D}$$

Elles vérifient l'une des conditions suivantes :

1. chaque t_i est de profondeur au plus 1.
2. chaque t_i est de profondeur au plus 2 et pour chaque t_i de profondeur 2,
   - soit t est une variable de t_i,
   - soit t est un sous-terme de t_i et t est de profondeur 1,
   - soit $t_i = C[f(u_1, \dots, u_m)]$ et $t = C[u_j]$

Restriction sur les décompositions

Les règles de décomposition sont de la forme :

$$\frac{T \vdash t_1 \ \llbracket E_1 \rrbracket \quad \dots \quad T \vdash t_n \ \llbracket E_n \rrbracket}{T \vdash t \ \llbracket E_1 \wedge \dots \wedge E_n \rrbracket} \mathcal{D}$$

Elles vérifient l'une des conditions suivantes :

1. chaque t_i est de profondeur au plus 1.
2. chaque t_i est de profondeur au plus 2 et pour chaque t_i de profondeur 2,
   - soit t est une variable de t_i,
   - soit t est un sous-terme de t_i et t est de profondeur 1,
   - soit $t_i = C[f(u_1, \dots, u_m)]$ et $t = C[u_k]$

Restriction sur les décompositions

Les règles de décomposition sont de la forme :

$$\frac{T \vdash t_1 \ \llbracket E_1 \rrbracket \quad \ldots \quad T \vdash t_n \ \llbracket E_n \rrbracket}{T \vdash t \ \llbracket E_1 \wedge \ldots \wedge E_n \rrbracket}\ \mathcal{D}$$

Elles vérifient l'une des conditions suivantes :

1. chaque t_i est de profondeur au plus 1.
2. chaque t_i est de profondeur au plus 2 et pour chaque t_i de profondeur 2,
   - soit t est une variable de t_i,
   - soit t est un sous-terme de t_i et t est de profondeur 1,
   - soit $t_i = C[f(u_1, \ldots, u_m)]$ et $t = C[u_i]$

Restriction sur les décompositions

Les règles de décomposition sont de la forme :

$$\frac{T \vdash t_1 \;\; [\![E_1]\!] \quad \ldots \quad T \vdash t_n \;\; [\![E_n]\!]}{T \vdash t \;\; [\![E_1 \wedge \ldots \wedge E_n]\!]} \mathcal{D}$$

Elles vérifient l'une des conditions suivantes :

1. chaque t_i est de profondeur au plus 1.
2. chaque t_i est de profondeur au plus 2 et pour chaque t_i de profondeur 2,
   - soit t est une variable de t_i,
   - soit t est un sous-terme de t_i et t est de profondeur 1,
   - soit $t_i = C[f(u_1, \ldots, u_m)]$ et $t = C[u_i]$

Restriction sur les décompositions

Les règles de décomposition sont de la forme :

$$\frac{T \vdash t_1 \ \llbracket E_1 \rrbracket \quad \ldots \quad T \vdash t_n \ \llbracket E_n \rrbracket}{T \vdash t \ \llbracket E_1 \wedge \ldots \wedge E_n \rrbracket} \mathcal{D}$$

Elles vérifient l'une des conditions suivantes :

1. chaque t_i est de profondeur au plus 1.
2. chaque t_i est de profondeur au plus 2 et pour chaque t_i de profondeur 2,
   - soit t est une variable de t_i,
   - soit t est un sous-terme de t_i et t est de profondeur 1,
   - soit $t_i = C[f(u_1, \ldots, u_m)]$ et $t = C[u_i]$

Restriction sur les décompositions

Les règles de décomposition sont de la forme :

$$\frac{T \vdash t_1 \;\; [\![E_1]\!] \quad \ldots \quad T \vdash t_n \;\; [\![E_n]\!]}{T \vdash t \;\; [\![E_1 \wedge \ldots \wedge E_n]\!]} \mathcal{D}$$

Elles vérifient l'une des conditions suivantes :

1. chaque t_i est de profondeur au plus 1.
2. chaque t_i est de profondeur au plus 2 et pour chaque t_i de profondeur 2,
   - soit t est une variable de t_i,
   - soit t est un sous-terme de t_i et t est de profondeur 1,
   - soit $t_i = C[f(u_1, \ldots, u_m)]$ et $t = C[u_i]$

Théorème de normalisation

Théorème (Normalisation de preuve)

Pour tout intrus respectant la propriété de localité et dont les règles de composition et décomposition sont de la forme évoquée auparavant, il existe F tel que pour tout protocole V et tout ensemble de termes T, $T \vdash s\ [\![E]\!]$ est déductible et E satisfaisable si et seulement s'il existe une preuve n'utilisant que des séquents $T \vdash u\ [\![E']\!]$ où :

- $u \in F(V, T, s)$ *si* u *est issu d'une composition et* $u \in F(V, T)$ *sinon*
- E' *est constitué d'égalités entre termes de* $F(V, T)$.

Plan

Décision en nombre fixe de sessions

Le théorème de normalisation admet le corollaire suivant :

Théorème

S'il existe une attaque en nombre fixe de sessions contre le secret s sur le protocole alors il existe une preuve de cette attaque telle que tous les séquents sont dans un ensemble fini calculable.

Cela nous permet d'obtenir un algorithme de décision par énumération des séquents accessibles et recherche du secret s parmi eux.

Décision en nombre fixe de sessions

Le théorème de normalisation admet le corollaire suivant :

Théorème

S'il existe une attaque en nombre fixe de sessions contre le secret s sur le protocole alors il existe une preuve de cette attaque telle que tous les séquents sont dans un ensemble fini calculable.

Cela nous permet d'obtenir un algorithme de décision par énumération des séquents accessibles et recherche du secret s parmi eux.

Recherche d'attaque

Nous avons conçu un algorithme plus intelligent qui fonctionne également en nombre non borné de sessions et permet d'adopter une stratégie de recherche.

On effectue une recherche en arrière parmi les preuves en forme normale en construisant de manière paresseuse la contrainte.

Recherche d'attaque

Nous avons conçu un algorithme plus intelligent qui fonctionne également en nombre non borné de sessions et permet d'adopter une stratégie de recherche.

On effectue une recherche en arrière parmi les preuves en forme normale en construisant de manière paresseuse la contrainte.

Par rapport à l'existant

On retrouve le résultat de décision de [Rusinowitch, Turuani, 2001] dans le cas de Dolev-Yao.

On obtient un algorithme de décision en nombre fixe de sessions pour les signatures en aveugle.

Par rapport à l'existant

On retrouve le résultat de décision de [Rusinowitch, Turuani, 2001] dans le cas de Dolev-Yao.

On obtient un algorithme de décision en nombre fixe de sessions pour les signatures en aveugle.

Conclusion et perspectives

Contributions

- objectif atteint : extension des propriétés de localité au cas actif
- algorithme correct et complet pour un nombre fixe et non borné de sessions

Perspectives

- Réaliser une implantation de l'algorithme
- Généraliser le résultat principal en imposant moins de restrictions et en acceptant la théorie équationnelle AC

Conclusion et perspectives

Contributions

- objectif atteint : extension des propriétés de localité au cas actif
- algorithme correct et complet pour un nombre fixe et non borné de sessions

Perspectives

- Réaliser une implantation de l'algorithme
- Généraliser le résultat principal en imposant moins de restrictions et en acceptant la théorie équationnelle AC

Conclusion et perspectives

Contributions

- objectif atteint : extension des propriétés de localité au cas actif
- algorithme correct et complet pour un nombre fixe et non borné de sessions

Perspectives

- Réaliser une implantation de l'algorithme
- Généraliser le résultat principal en imposant moins de restrictions et en acceptant la théorie équationnelle AC

Conclusion et perspectives

Contributions

- objectif atteint : extension des propriétés de localité au cas actif
- algorithme correct et complet pour un nombre fixe et non borné de sessions

Perspectives

- Réaliser une implantation de l'algorithme
- Généraliser le résultat principal en imposant moins de restrictions et en acceptant la théorie équationnelle AC