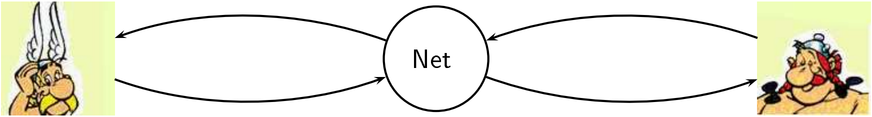
Spécification et Vérification de protocoles cryptographiques

Steve Kremer

Laboratoire Spécification et Vérification
ENS Cachan

Première partie I

Introduction (informelle) aux Protocoles Cryptographiques



Protocole

↪ règles décrivant des échanges de messages

But

↪ sécuriser les communications : *secret, authentification, anonymat ...*

Applications

↪ téléphonie mobile, vote électronique, homebanking, commerce électronique, . . .

Protocoles Cryptographiques

Protocole

↪ règles décrivant des échanges de messages

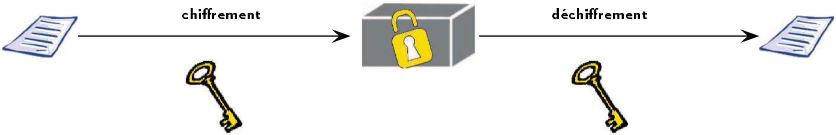
But

↪ sécuriser les communications : *secret, authentification, anonymat* ...

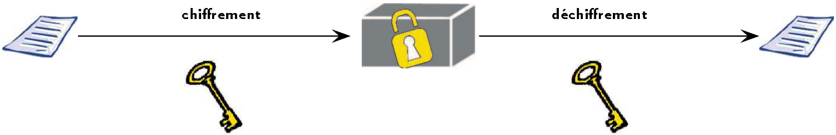
Applications

↪ téléphonie mobile, vote électronique, homebanking, commerce électronique, ...

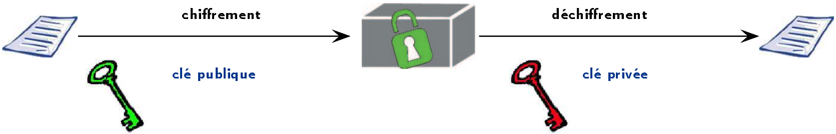
- Chiffrement à clé symétrique



- Chiffrement à clé symétrique

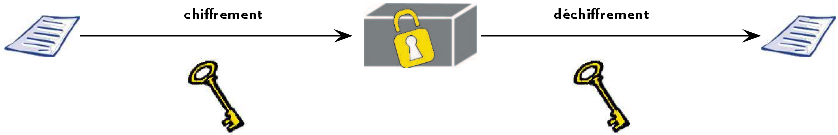


- Chiffrement à clé asymétrique



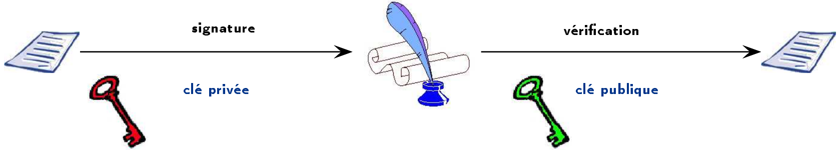
Chiffrement et Signature numérique

- Chiffrement à clé symétrique



- Chiffrement à clé asymétrique

- Signature numérique



Le protocole de paiement par carte bleue

1. L'acheteur introduit sa CB
2. Le commerçant saisit le montant m de la transaction
3. Le terminal authentifie la carte
4. L'acheteur entre son code
5. Si $m > 100$ EUR (et dans seulement 20% des cas)
   - Le terminal demande l'authentification de la carte à la banque
   - La banque donne l'autorisation

Le protocole de paiement par CB en détails

4 acteurs : la Banque, l'Acheteur, la Carte et le Terminal

- La Banque possède
  - une clé de signature K_B^{-1}
  - une clé de vérification K_B
  - une clé secrète pour chaque carte bancaire K_{CB}
- La Carte possède
  - Data : nom, prénom, numéro de carte, date de validité
  - Valeur de signature $VS = \{hash(\text{Data})\}_{K_B^{-1}}$
  - clé secrète K_{CB}
- le Terminal possède la clé de vérification K_B des signatures de la banque

Le protocole de paiement par CB

Le terminal lit la CB	1. $C \rightarrow T$: Data, $\{hash(\text{Data})\}_{K_B^{-1}}$
Le terminal demande le code	2. $T \rightarrow A$: *code secret ?* 3. $A \rightarrow C$: 1234 4. $C \rightarrow T$: *ok*
Le terminal contacte la banque	5. $T \rightarrow B$: *auth ?* 6. $B \rightarrow T$: 4567614283453621394 56 7. $T \rightarrow C$: 456761428345362139456 8. $C \rightarrow T$: $\{456761428345362139456\}_{K_{CB}}$ 9. $T \rightarrow B$: $\{456761428345362139456\}_{K_{CB}}$ 10. $B \rightarrow T$: *ok*

Failles de la Carte Bleue

La sécurité est initialement assurée par :

- le fait que les cartes sont difficilement réplicables
- le secret des clés et du protocole

Mais :

- faille cryptographique : la taille des clés (1988) de 320 bits est trop courte
- faille logique : pas de lien entre le code secret à 4 chiffres et l'authentification
- réplicabilité des cartes

Failles de la Carte Bleue

La sécurité est initialement assurée par :

- le fait que les cartes sont difficilement réplicables
- le secret des clés et du protocole

Mais :

- faille cryptographique : la taille des clés (1988) de 320 bits est trop courte
- faille logique : pas de lien entre le code secret à 4 chiffres et l'authentification
- réplicabilité des cartes

En 1998, Serge Humpich crée la “Yescard” !

La Yescard

$$\begin{array}{llcll}
1. & C & \rightarrow & T: & \text{Data}, \{hash(\text{Data})\}_{K_B^{-1}} \\
2. & T & \rightarrow & A: & code\ secret\ ? \\
3. & A & \rightarrow & C: & 1234 \\
4. & C & \rightarrow & T: & ok
\end{array}$$

La Yescard

$$\begin{array}{lllll} 1. & C & \rightarrow & T: & \text{Data}, \{hash(\text{Data})\}_{K_B^{-1}} \\ 2. & T & \rightarrow & A: & \textit{code secret ?} \\ 3. & A & \rightarrow & C': & 2345 \\ 4. & C' & \rightarrow & T: & ok \end{array}$$

Remarque :

Il y a toujours quelqu'un à débiter !

La Yescard

$$\begin{array}{llcll} 1. & C & \rightarrow & T: & \text{Data}, \{hash(\text{Data})\}_{K_B^{-1}} \\ 2. & T & \rightarrow & A: & code\ secret\ ? \\ 3. & A & \rightarrow & C': & 2345 \\ 4. & C' & \rightarrow & T: & ok \end{array}$$

Remarque :

Il y a toujours quelqu'un à débiter !

Yescard de Serge Humpich : Ajout d'une fausse signature sur une fausse carte

$$\begin{array}{llcll} 1. & C & \rightarrow & T: & \text{XXXX}, \{hash(\text{XXXX})\}_{K_B^{-1}} \\ 2. & T & \rightarrow & A: & code\ secret\ ? \\ 3. & A & \rightarrow & C: & 0000 \\ 4. & C & \rightarrow & T: & ok \end{array}$$

Protocole de Needham-Schroeder (1978)

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

Protocole de Needham-Schroeder (1978)

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

Protocole de Needham-Schroeder (1978)

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

Protocole de Needham-Schroeder (1978)

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

Questions

- Est-ce que N_b est un secret partagé entre A et B ?
- Quand B reçoit $\{N_b\}_{\mathrm{pub}(B)}$, ce message provient-il réellement de A ?

Protocole de Needham-Schroeder (1978)

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

Questions

- Est-ce que N_b est un secret partagé entre A et B ?
- Quand B reçoit $\{N_b\}_{\mathsf{pub}(B)}$, ce message provient-il réellement de A ?

Une attaque sur ce protocole a été trouvée 17 ans après sa publication !

Attaque sur Needham-Schroeder

Agent A

Intruder I

Agent B

$$
\begin{array}{ccccl}
A & \longrightarrow & B & : & \{N_a, A\}_{\mathsf{pub}(B)} \\
B & \longrightarrow & A & : & \{N_a, N_b\}_{\mathsf{pub}(A)} \\
A & \longrightarrow & B & : & \{N_b\}_{\mathsf{pub}(B)}
\end{array}
$$

Attaque sur Needham-Schroeder

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

Agent A

Intruder I

Agent B

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

Attaque sur Needham-Schroeder

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

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

Agent A | Intruder I | Agent B

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

Attaque sur Needham-Schroeder

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

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

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

Agent A — Intruder I — Agent B

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

Attaque sur Needham-Schroeder

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

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

Agent A | Intruder I | Agent B

- $$\begin{array}{lcll} A & \longrightarrow & B & : \{N_a, A\}_{\text{pub}(B)} \\ B & \longrightarrow & A & : \{N_a, N_b\}_{\text{pub}(A)} \\ A & \longrightarrow & B & : \{N_b\}_{\text{pub}(B)} \end{array}$$

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

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

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

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

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

Agent A

Intruder I

Agent B

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

Attaque sur Needham-Schroeder

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

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

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

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

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

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

Agent A Intruder I Agent B

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

Attaque sur Needham-Schroeder

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

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

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

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

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

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

Agent A | Intruder I | Agent B

Réponses

- Est-ce que N_b est un secret partagé entre A et B ?
  $\hookrightarrow$ Non

Attaque sur Needham-Schroeder

Agent A

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

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

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

Intruder I

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

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

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

Agent B

Réponses

- Est-ce que N_b est un secret partagé entre A et B ?
  $\hookrightarrow$ Non
- Quand B reçoit $\{N_b\}_{\mathrm{pub}(B)}$, ce message provient-il réellement de A ?
  $\hookrightarrow$ Non

Attaque sur Needham-Schroeder

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

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

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

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

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

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

Agent A — Intruder I — Agent B

Réponses

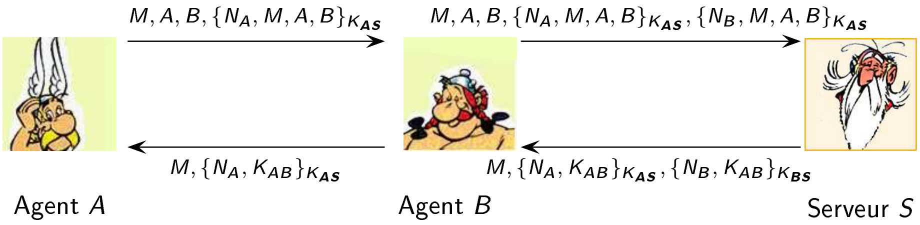
- Est-ce que N_b est un secret partagé entre A et B ?
  $\hookrightarrow$ Non
- Quand B reçoit $\{N_b\}_{\text{pub}(B)}$, ce message provient-il réellement de A ?
  $\hookrightarrow$ Non

Remarque : les algorithmes de chiffrement n'ont pas été cassés
$\hookrightarrow$ Attaque sur la logique du protocole

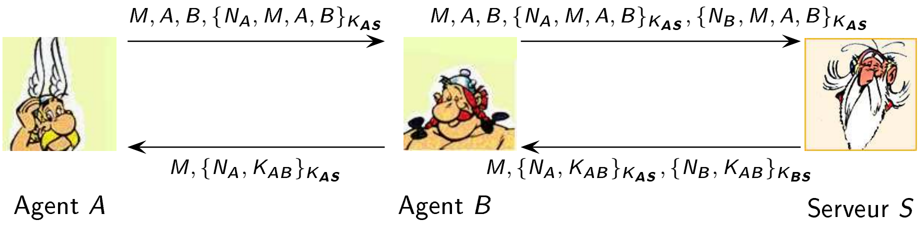
‘Man-in-the-middle’ et SSH

```
$ ssh -o stricthostkeychecking=ask ssh-server.example.com
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
23:00:20:83:de:02:95:f1:e3:34:be:57:3f:cf:2c:e7.
Please contact your system administrator.
Add correct host key in /home/xahria/.ssh/known_hosts to get rid of this message.
Offending key in /home/xahria/.ssh/known_hosts:8
RSA host key for localhost has changed and you have requested strict checking.
Host key verification failed.
```

Le protocole d'Otway-Rees



Le protocole d'Otway-Rees



But : une clé partagée entre A et B (et S)

Mais : il existe une attaque de confusion de type

$\xrightarrow{M, A, B, \{N_A, M, A, B\}_{K_{AS}}}$

$\xleftarrow[M, \{N_A, K_{AB}\}_{K_{AS}}]{}$

Agent A

$\xrightarrow{M, A, B, \{N_A, M, A, B\}_{K_{AS}}, \{N_B, M, A, B\}_{K_{AS}}}$

$\xleftarrow[M, \{N_A, K_{AB}\}_{K_{AS}}, \{N_B, K_{AB}\}_{K_{BS}}]{}$

Agent B

Serveur S

But : une clé partagée entre A et B (et S)

Mais : il existe une attaque de confusion de type

$\xrightarrow{M, A, B, \{N_A, M, A, B\}_{K_{AS}}}$

$\xleftarrow{M, \{N_A, M, A, B\}_{K_{AS}}}$

Confusion entre la clé partagé K_{AB} et le triplet M, A, B

Deuxième partie II

Les modèles à la Dolev-Yao : adversaire passif

Vérification des protocoles "à la Dolev-Yao"

En 1978, Needham et Schroeder évoquent le besoin de vérification formelle de protocoles
En 1982, Dolev et Yao formalisent les bases de ce qu'on appelle aujourd'hui le modèle "Dolev-Yao"

- un intrus ayant un contrôle total du réseau :
  - l'intrus peut intercepter tout message
  - l'intrus peut modifier tout message
  - l'intrus peut insérer des nouveaux messages calculés à partir de sa connaissance
- primitive cryptographique parfaite :
  - idéalisation de la cryptographie : algèbre de termes
  - par exemple, l'unique façon de déchiffrer un message est de connaître la clé de déchiffrement
- le protocole a
  - un nombre arbitraire de participants
  - un nombre arbitraire de sessions parallèles
  - des messages de taille arbitraire

Dans un premier temps : adversaire passif (écoute tous les messages)

Modélisation des messages par des termes

Définition (signature)

Une signature est un couple $(\mathcal{F}, Ar)$. $\mathcal{F}$ est un ensemble fini de symboles de fonctions et $Ar : \mathcal{F} \to \mathbb{N}$ est une fonction associant une arité à chaque élément de $\mathcal{F}$.
L'ensemble des fonctions d'arité p est noté $\mathcal{F}_p = \{f \in \mathcal{F} \mid Ar(f) = p\}$.
En particulier l'ensemble $\mathcal{F}_0$ est l'ensemble des constantes.

Exemple

Soit $\mathcal{F} = \{\mathbf{enc}, \mathbf{pair}, \mathbf{k}_1, \mathbf{k}_2, \mathbf{0}, \mathbf{1}\}$

$Ar(\mathbf{enc}) = Ar(\mathbf{pair}) = 2$
$Ar(\mathbf{k}_1) = Ar(\mathbf{k}_2) = Ar(\mathbf{0}) = Ar(\mathbf{1}) = 0$

On notera également $\mathcal{F} = \{\mathbf{enc}/2, \mathbf{pair}/2, \mathbf{k}_1/0, \mathbf{k}_2/0, \mathbf{0}/0, \mathbf{1}/0\}$

Termes

Définition (Termes)

Soit une signature $(\mathcal{F}, Ar)$ et un ensemble de variables $\mathcal{X}$, tels que $\mathcal{X} \cap \mathcal{F} = \emptyset$. L'ensemble des termes sur la signature $(\mathcal{F}, Ar)$ et les variables $\mathcal{X}$, noté $\mathcal{T}(\mathcal{F}, \mathcal{X})$, est le plus petit ensemble tel que

- $\mathcal{X} \subseteq \mathcal{T}(\mathcal{F}, \mathcal{X})$
- $\mathcal{F}_0 \subseteq \mathcal{T}(\mathcal{F}, \mathcal{X})$
- $f(t_1, \ldots, t_n) \subseteq \mathcal{T}(\mathcal{F}, \mathcal{X})$ si $f \in \mathcal{F}_n$, $n > 0$, $t_1, \ldots, t_n \in \mathcal{T}(\mathcal{F}, \mathcal{X})$

Exemple

Soit $\mathcal{F} = \{\mathbf{enc}/2, \mathbf{pair}/2, \mathbf{k_1}/0, \mathbf{k_2}/0, \mathbf{0}/0, \mathbf{1}/0\}$ et $\mathcal{X} = \{x, y, z\}$.

$\mathbf{pair}(x, \mathbf{1})$, $\mathbf{enc}(\mathbf{pair}(y, z), \mathbf{k_1})$ et $\mathbf{enc}(\mathbf{0}, \mathbf{k_1})$ sont des termes dans $\mathcal{T}(\mathcal{F}, \mathcal{X})$

$\mathbf{pair}(\mathbf{0}, \mathbf{1})$, $\mathbf{enc}(\mathbf{0}, \mathbf{k_1})$ sont des termes dans $\mathcal{T}(\mathcal{F})$, i.e., des termes clos

On utilisera également les notations $\{\_\}_\_$ pour $\mathbf{enc}(\_, \_)$ et $\langle \_, \_ \rangle$ pour $\mathbf{pair}(\_, \_)$.

Notations pour manipuler des termes

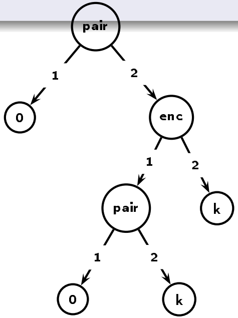
Définition (Positions)

L'ensemble des positions d'un terme t est un sous-ensemble de $\mathbb{N}_+^*$ (l'ensemble des suites finies d'entiers positifs non nuls). Il est défini inductivement comme

$$Pos(x) = \{\epsilon\} \quad (x \in \mathcal{X}) \qquad Pos(f(t_1, \ldots, t_n)) = \{\epsilon\} \cup_{1 \leq i \leq n} i \cdot Pos(t_i)$$

Exemple

Soit $t = \mathbf{pair}(\mathbf{0}, \mathbf{enc}(\mathbf{pair}(\mathbf{0}, \mathbf{k}), \mathbf{k}))$
$Pos(t) = \{\epsilon, 1, 2, 21, 22, 211, 212\}$



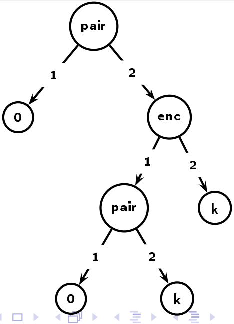
Notations pour manipuler des termes

Définition (Sous-termes)

Le sous-terme $t|_p$ de t à la position p ($p \in Pos(t)$) est

$$t\ |_\epsilon = t \qquad\qquad t\ |_{i\cdot p} = t_i\ |_p \ \text{ si } t = f(t_1, \ldots, t_n), f \in \mathcal{F}_n$$

On note $st(t) = \{t_p \mid p \in Pos(t)\}$ l'ensemble des sous-termes de t. On étend la notion de sous-termes à des ensembles de termes : $st(\{t_1, \ldots t_n\}) = \cup_{1 \leq i \leq n} st(t_i)$



Exemple

Soit $t = \mathbf{pair}(\mathbf{0}, \mathbf{enc}(\mathbf{pair}(\mathbf{0}, \mathbf{k}), \mathbf{k}))$
$t|_{21} = \mathbf{pair}(0, k)$
$st(t) = \{t, \mathbf{0}, \mathbf{enc}(\mathbf{pair}(\mathbf{0}, \mathbf{k}), \mathbf{k}), \mathbf{pair}(\mathbf{0}, \mathbf{k}), \mathbf{k}\}$

Taille (DAG) de termes

Définition (Taille d'un terme)

La taille d'un terme t, noté $\mid t \mid$ est défini de façon inductive

$$\begin{array}{rcl} \mid t \mid & = & 1 \text{ si } t \in \mathcal{F}_0 \cup \mathcal{X} \\ \mid f(t_1, \ldots, t_n) \mid & = & 1 + \sum_{i=1}^{n} \mid t_i \mid \text{ si } f \in \mathcal{F}_n \end{array}$$

Définition (Taille DAG d'un terme)

La taille DAG d'un terme t, noté $\mid t \mid_{DAG}$ est le nombre de sous-termes différents, i.e., $\mid t \mid_{DAG} = \mid st(t) \mid$ (où $\mid E \mid$ dénote la cardinalité de l'ensemble E).

On peut étendre ces deux notions de taille à des ensembles de termes

$$\mid \{t_1, \ldots, t_n\} \mid = \sum_{i=1}^{n} \mid t_i \mid$$

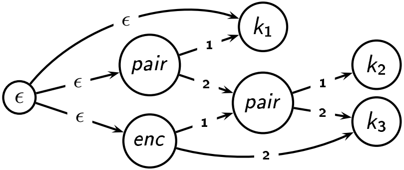
$$\mid \{t_1, \ldots, t_n\} \mid_{DAG} = \mid \bigcup_{i=1}^{n} st(t_i) \mid$$

Représentation compacte d'ensembles de termes

Des ensembles de termes peuvent être représentés de façon compacte par des DAGs avec partage maximal

Exemple

$$T = \{ \quad pair(k_1, pair(k_2, k_3)), \\ enc(pair(k_2, k_3), k_3), k_1\}$$



$||T||_d$ dénote the la taille DAG de l'ensemble de termes T

Formellement, $(\mathcal{V}, \mathcal{E})$ est le DAG qui représente l'ensemble de termes T où

- $\mathcal{V} = st(T) \cup \{\epsilon\}$
- $\mathcal{E} = \{v_s \xrightarrow{i} v_e \mid v_s, v_e \in \mathcal{V}, v_s = f(t_1, \ldots, t_n), v_e = t_i\} \cup \{\epsilon \xrightarrow{\epsilon} v \mid v \in T\}$

Substitutions et unificateurs

Définition (Substitution)

Une substitution σ est une fonction de $X \subseteq \mathcal{X}$ (X fini) dans $\mathcal{T}(\mathcal{F}, \mathcal{X})$. On dénote $dom(\sigma)$ l'ensemble X et on étend les substitutions à des termes

$$\begin{array}{rcl} \sigma(x) & = & x \text{ si } x \notin dom(\sigma) \\ \sigma(f(t_1, \ldots, t_n)) & = & f(\sigma(t_1), \ldots, \sigma(t_n)) \end{array}$$

Définition (Unificateurs)

Deux termes s et t sont unifiables s'il existe une substitution σ, telle que $t\sigma = s\sigma$. σ est appelé l'unificateur.

Un unificateur de s et de t est appelé l'unificateur le plus général, noté $mgu(s, t)$ si

$$\forall \sigma.\ s\sigma = t\sigma \quad \exists \theta.\ \sigma = mgu(s, t)\theta$$

Définition (Règle et système d'inférence)

Une règle d'inférence est une règle de la forme

$$\frac{T_1 \quad \ldots \quad T_n}{T}\gamma$$

avec $T_1, \ldots, T_n, T \in \mathcal{T}(\mathcal{F}, \mathcal{X})$.

Un système d'inférence est un ensemble de règles d'inférence.

Exemple

Nous définissons le système d'inférence $\mathcal{I}_{DY}$:

$$\frac{x \quad y}{\langle x, y\rangle} \qquad \frac{x \quad y}{\{x\}_y} \qquad \frac{\langle x, y\rangle}{x} \qquad \frac{\langle x, y\rangle}{y} \qquad \frac{\{x\}_y \quad y}{x}$$

qui correspond aux capacités d'un intrus classique (appelé "intrus Dolev-Yao").

Dérivation : définition

Définition (Définition)

Un terme clos t est dérivable en une étape d'un ensemble de termes S par un système d'inférence $\mathcal{I}$, noté $S \vdash^1_{\mathcal{I}} t$ si

- $\dfrac{T_1 \quad \ldots \quad T_n}{T}\gamma \in \mathcal{I}$
- $\exists t_1, \ldots, t_n \in S$ et $\exists \sigma$, tels que $T_i\sigma = t_i$, $T\sigma = t$, $\gamma\sigma = \mathrm{true}$

Un terme t est dérivable d'un ensemble de termes S par un système d'inférence $\mathcal{I}$, noté $S \vdash_{\mathcal{I}} t$ si

- $t \in S$ ou
- $\exists t_1, \ldots, t_n$ tels que $t_n = t$ et $S \cup \{t_1, \ldots, t_i\} \vdash^1_{\mathcal{I}} t_{i+1}$

On appelle alors $\exists t_1, \ldots, t_n$ la preuve de dérivation.

Dérivation : exemple

Exemple

Soit $S = \{\{k_1\}_{k_2}, k_2, k_3\}$

$S \overset{?}{\vdash}_{\mathcal{I}_{DY}} \{k_2\}_{\{k_1\}_{k_3}}$

Dérivation : exemple

Exemple

Soit $S = \{\{k_1\}_{k_2}, k_2, k_3\}$

$S \overset{?}{\vdash}_{\mathcal{I}_{DY}} \{k_2\}_{\{k_1\}_{k_3}}$

La preuve de dérivation : $k_1, \{k_1\}_{k_3}, \{k_2\}_{\{k_1\}_{k_3}}$

$$\dfrac{\dfrac{}{k_2} \qquad \dfrac{\dfrac{\dfrac{}{\{k_1\}_{k_2}} \quad \dfrac{}{k_2}}{k_1} \qquad \dfrac{}{k_3}}{\{k_1\}_{k_3}}}{\{k_2\}_{\{k_1\}_{k_3}}}$$

Problème de décision et complexité

Définition (Problème de dérivation)

Soit S un ensemble de termes clos, $\mathcal{I}$ un système de dérivation et t un terme clos. Le problème de dérivation pour $S, \mathcal{I}, t$ est le suivant.
Données : $S, \mathcal{I}, t$
Question : $S \vdash_{\mathcal{I}} t$?

Théorème (Localité)

Soit $\mathcal{I}$ un système d'inférence, tel que pour tous termes clos $t_1, \ldots, t_n, t$ si $\{t_1, \ldots, t_n\} \vdash_{\mathcal{I}} t$ alors il existe une preuve de dérivation qui n'utilise que des sous-termes de $\{t_1, \ldots, t_n, t\}$.

Le problème de dérivation pour $S, \mathcal{I}, t$ est décidable en temps polynolmial en $|\{t_1, \ldots, t_n, t\}|_{DAG}$.

Rappel : Clauses de Horn propositionelles

Définition (Clause de Horn propositionelle)

Une clause de Horn propositionelle est une formule de la forme

$$p_1 \wedge \ldots \wedge p_n \longrightarrow p$$

Définition (Le problème Horn-SAT propositionel)

Données : Un ensemble de clauses de Horn propositionelles H

Question : Est-ce qu'il existe une valuation V telle que

$$\forall \phi \in H.\ V \models \phi$$

Théorème (Horn-SAT)

Horn-SAT propositionel est décidable en temps linéaire en $\mid H \mid$.

Preuve

Notons $S = st(\{t_1, \ldots, t_n, t\})$
Définissons l'ensemble des propositions $\{p_t \mid t \in S\}$ et l'ensemble des clauses de Horn

$$H = \left\{ \begin{array}{rll} \top & \rightarrow p_u & u \in \{t_1, \ldots t_n\} \\ p_{u_1}, \ldots, p_{u_n} & \rightarrow p_u & \dfrac{T_1, \ldots, T_n}{T}\gamma \in \mathcal{I} \\ & & \text{et } \exists \sigma. u_i = T_i\sigma, \gamma\sigma = \top, T\sigma = u \\ p_t & \rightarrow \bot & \end{array} \right\}$$

L'encodage est de sorte que $\{t_1, \ldots, t_n\} \vdash_{\mathcal{I}} t$ ssi H n'est pas satisfaisable.

Horn-SAT est décidable en temps linéaire en $\mid H \mid$ et $\mid H \mid$ est polynomial en $\mid \{t_1, \ldots, t_n\} \mid_{DAG}$. (Le degré est $max\{n \mid \dfrac{T_1, \ldots, T_n}{T}\gamma \in \mathcal{I}\}$)

Dolev-Yao est décidable en temps polynomial

Proposition (Décidabilité du système Dolev-Yao)

Le système d'inférence $\mathcal{I}_{DY}$ vérifie que pour tous termes clos $t_1, \ldots, t_n, t$ si $\{t_1, \ldots, t_n\} \vdash_{\mathcal{I}_{DY}} t$ alors il existe une preuve n'utilisant que des sous-termes de $\{t_1, \ldots, t_n, t\}$.

Preuve : Soit $u_1, \ldots, u_n$ une preuve de dérivation de $\{t_1, \ldots, t_n\} \vdash_{\mathcal{I}_{DY}} t$. On appelle $u_1, \ldots, u_n$ une preuve de composition si la dernière étape utilise la règle $\dfrac{x \quad y}{\langle x, y\rangle}$ ou $\dfrac{x \quad y}{\{x\}_y}$. Sinon, on parle de preuve de décomposition.

On prouve un lemme plus fort :
Pour tous termes clos $t_1, \ldots, t_n, t$ si $\{t_1, \ldots, t_n\} \vdash_{\mathcal{I}_{DY}} t$ alors il existe une preuve de taille minimale $u_1, \ldots, u_\ell$, telle que si $u_1, \ldots, u_\ell$ est

- une preuve de composition : $st(\{u_1, \ldots u_\ell\}) \subseteq st(\{t_1, \ldots, t_n, t\})$
- une preuve de décomposition : $st(\{u_1, \ldots u_\ell\}) \subseteq st(\{t_1, \ldots, t_n\})$

Preuve par induction sur la taille ℓ de la preuve.