Résolution de contraintes et recherche d'attaque pour un nombre borné de sessions

Hubert Comon-Lundh

5 février 2004

1 Rappel des règles de déduction de l'intrus

$\mathcal{F}$ est un alphabet contenant des constantes, les symboles binaires $\{\_\}_\_$ et $<\_,\_>$. On se limite ici et dans toute la suite au cas du chiffrement symétrique.

Les règles standard de déduction de l'intrus sont alors données dans la figure 1

Les règles **P**, **C** ont appelées *règles de composition*. Les règles **UL, UR, D** sont appelées *règles de décomposition*.

Si t est un terme, on note $\mathsf{St}(t)$ l'ensemble des sous-termes de t. Si T est un ensemble de termes, $\mathsf{St}(T) = \bigcup_{t \in T} \mathsf{St}(t)$.

On rappelle alors le résultat de localité :

Lemme 1 *Si $T \vdash u$ est prouvable à l'aide des règles de la figure 1, alors il en existe une preuve dont tous les noeuds sont de la forme $T \vdash v$ avec $v \in \mathsf{St}(T, u)$. De plus, si la dernière règle appliquée est une décomposition, on a même, pour tous les noeuds $T \vdash v$, $v \in \mathsf{St}(T)$.*

2 Le système de contraintes

2.1 Syntaxe

Un ensemble (conjonction) d'expressions $T \Vdash u$ où T est un ensemble de termes et u un terme (dans la suite T est appelé "membre gauche de contrainte" et u "membre droit de

$$\mathbf{C}\quad \frac{T \vdash u \quad T \vdash v}{T \vdash \{u\}_v} \qquad\qquad \mathbf{P}\quad \frac{T \vdash u \quad T \vdash v}{T \vdash < u, v >}$$

$$\mathbf{UL}\quad \frac{T \vdash < u, v >}{T \vdash u} \qquad\qquad \mathbf{UR}\quad \frac{T \vdash < u, v >}{T \vdash v}$$

$$\mathbf{D}\quad \frac{T \vdash \{u\}_v \quad T \vdash v}{T \vdash u} \qquad\qquad \mathbf{A}\quad \frac{}{T \vdash u}\ \text{Si } u \in T$$

FIG. 1 – Règles de déduction de l'intrus

R_1	$T \Vdash u$	$\rightsquigarrow$	$\top$	Si $T \cup \{x \mid T' \Vdash x \in C, T' \subseteq T, T' \neq T\} \vdash u\}$
R_2	$C \wedge T \Vdash u$	$\rightsquigarrow_\sigma$	$C\sigma \wedge T\sigma \Vdash u\sigma$	Si $\sigma = mgu(t,u)$, $t \in \mathsf{St}(T), t \neq u$, t, u non variable
R_3	$C \wedge T \Vdash u$	$\rightsquigarrow_\sigma$	$C\sigma \wedge T\sigma \Vdash u\sigma$	Si $\sigma = mgu(t_1,t_2)$, $t_1, t_2 \in \mathsf{St}(T), t_1 \neq t_2$, t_1, t_2 non variable
R_4	$T \Vdash \{u\}_v$	$\rightsquigarrow$	$T \Vdash u \wedge T \Vdash v$	
R_5	$T \Vdash < u, v >$	$\rightsquigarrow$	$T \Vdash u \wedge T \Vdash v$	
R_6	$T \Vdash u$	$\rightsquigarrow$	$\perp$	Si $T = \emptyset$ ou bien $Var(T,u) = \emptyset$ et $T \not\vdash u$

FIG. 2 – Règles de simplification des contraintes

contrainte") et tels que :
- Les membres gauches de contrainte sont totalement ordonnés par inclusion
- Si $T \Vdash u \in C$ et $x \in Var(T)$, alors

$$T_x = \min\{T' \mid T' \Vdash v \in C, x \in Var(v)\}$$

existe et $T_x \subseteq T, T_x \neq T$.

$\top$ désigne la conjonction vide de contraintes. $\perp$ désigne la contrainte insatisfaisable.

2.2 Sémantique

Une substitution close σ est solution d'une contrainte C ssi, pour tout $T \Vdash u \in C$, $T\sigma \vdash u\sigma$ est dérivable (par les règles de déduction de l'intrus).

En outre, toute substitution satisfait $\top$ et aucune ne satisfait $\perp$.

2.3 Règles de simplification des contraintes

Ces règles sont données dans la figure 2. On y note $T \vdash u$ lorsque $T \vdash u$ est dérivable en utilisant les règles de l'intrus. En particulier, cela signifie que, pour toute substitution σ, $T\sigma \vdash u\sigma$ est dérivable.

La relation $\rightsquigarrow$ est indicée par une substitution σ dont le domaine est contenu dans les variables libres de la contrainte ; $(C, \theta) \rightsquigarrow (C', \theta\sigma)$ si $C \rightsquigarrow_\sigma C'$. La deuxième composante de la paire n'est là que pour garder en mémoire la séquence de substitutions appliquée à la contrainte. A l'origine, θ est l'identité. Lorsque la substitution n'est pas précisée, c'est l'identité par défaut.

3 Propriétés des règles de simplification de contraintes

3.1 Correction

Tout d'abord les deux conditions dans la définition syntaxique des contraintes sont invariantes.

Lemme 2 *Les règles transforment une contrainte en une contrainte.*

Preuve
Le fait que les membres gauches sont totalement ordonnés est invariant par transformation car

$$T \subseteq T' \Rightarrow T\sigma \subseteq T'\sigma$$

Reste la deuxième condition à vérifier. Soit $C \rightsquigarrow_\sigma C'$, et, pour tout $T \Vdash u \in C$, $x \in Var(T)$, $T_x = \min\{T' \mid T' \Vdash v \in C, x \in Var(v)\}$, $T_x \subseteq T$, $T_x \neq T$.

Si C' est obtenu à partir de C par l'une des règles R_1, R_5, R_6, alors, si $T \Vdash u \in C'$, et $x \in Var(u)$, il existe un terme v contenant u comme sous-terme tel que $T \Vdash v \in C$ et $\min\{T' \mid T' \Vdash w \in C', x \in Var(w)\} \subseteq T_x$, ce qui montre que la propriété voulue est préservée.

Considérons maintenant le cas des règles R_2, R_3 :

$$C_1 \wedge T \Vdash u \rightsquigarrow_\sigma C_1\sigma \wedge T\sigma \Vdash u\sigma$$

On pose

$$T'_x = \begin{cases} \min\{T_y\sigma \mid x \in Var(y\sigma)\} & \text{Si l'ensemble est non vide} \\ T_x & \text{Sinon} \end{cases}$$

Si $T'\sigma \Vdash v\sigma \in C'$ avec $x \in Var(v\sigma)$, alors

- Ou bien x n'est pas introduite par σ et

$$T_x \subseteq T', T_x \neq T' \Rightarrow T_x\sigma \subseteq T'\sigma, T_x\sigma \neq T'\sigma \Rightarrow T'_x \subseteq T'\sigma, T'_x \neq T'\sigma$$

- Ou bien $\exists y \in Var(v)$, $x \in Var(y\sigma)$. Dans ce cas, $T_y \subseteq T', T_y \neq T'$ et donc $T'_x \subseteq T_y\sigma \subseteq T'\sigma$ et $T_y\sigma \neq T'\sigma$.

Dans tous les cas, $T'_x \subseteq T'\sigma$ et $T'_x \neq T'\sigma$.

Par ailleurs, $T'_x \Vdash w \in C'$ avec $x \in Var(w)$ dans les deux cas de construction.

$\square$

Lemme 3 (Correction) *Si $C \rightsquigarrow_\sigma C'$, alors pour toute solution θ de C', $\sigma\theta$ est une solution de C.*

Preuve

Pour les règles R_4, R_5, ceci résulte des capacités de construction de l'intrus. Pour les règles R_2, R_3, cela résulte des définitions. Considérons la règle R_1. Il s'agit de montrer que toute solution de C est aussi solution de $T \Vdash u$. Par la condition d'application de la règle, si σ est une solution de C, $T\sigma \cup \{x\sigma \mid T' \Vdash x \in C, T' \subseteq T, T' \neq T\} \vdash u\sigma$ est dérivable. Mais $T' \Vdash x \in C$ entraîne que $T'\sigma \vdash x\sigma$ est dérivable et, comme $T' \subseteq T$, $T\sigma \vdash x\sigma$ est dérivable : pour tout $z \in \{x \mid T' \Vdash x \in C, T' \subseteq T, T' \neq T\}$, $T\sigma \vdash z\sigma$ est dérivable. Donc $T\sigma \cup \{x\sigma \mid T' \Vdash x \in C, T' \subseteq T, T' \neq T\} \vdash u\sigma$ entraine $T\sigma \vdash u\sigma$. $\square$

3.2 Terminaison et formes résolues

Lemme 4 (Terminaison) *Les règles de simplification se terminent.*

Preuve

Il suffit de remarquer que la mesure suivante de C décroît strictement par application des règles : $I(C) = (nbv(C), |C|)$ où $nbv(C)$ est le nombre de variables de C et $|C|$ est la somme des tailles des membres droits de la contrainte. Les paires sont ordonnées lexicographiquement. Aucune règle n'introduit de variable et les conditions des règles R_2, R_3 imposent une décroissance stricte de $nbv(C)$. Pour les 4 autres règles la deuxième composante décroit. $\square$

Une contrainte est en *forme résolue* si toutes les contraintes sont de la forme $T \vdash x$ où x est une variable.

Lemme 5 *Toute forme résolue distincte de $\perp$ possède au moins une solution.*

Preuve
Soit T_0 le plus petit des membres gauches pour l'inclusion. T_0 est non vide et ne contient que des termes sans variable, par propriété des contraintes. Soit $t_0 \in T_0$. La substitution qui associe t_0 à toutes les variables libres de la forme résolue est une solution puisque T_0 est contenu dans tous les membres gauches. $\square$

3.3 Complétude

On montre d'abord un résultat légèrement plus fort que la localité. Si $T_1 \subseteq \ldots \subseteq T_k$, on dira qu'une preuve de $T_i \vdash u$ est *minimale à gauche* si, pour tout $j \leq i$ tel que $T_j \vdash u$ est prouvable, c'est aussi une preuve de $T_j \vdash u$. (Autrement dit, une preuve est minimale à gauche si ses feuilles sont dans un ensemble T_j d'indice minimal). Une preuve de $T_i \vdash u$ est *simple* si

1. Aucune branche ne contient deux fois le même noeud
2. Toutes les sous-preuves sont minimales à gauche
3. Si la dernière règle appliquée est une composition, alors tous les noeuds de la preuve sont de la forme $T_i \vdash v$ avec $v \in \mathsf{St}(T_i, u)$
4. Si la dernière règle appliquée est une décomposition, alors tous les noeuds de la preuve sont de la forme $T_i \vdash v$ avec $v \in \mathsf{St}(T_i)$

Lemme 6 *Pour toute séquence $T_1 \subseteq \ldots \subseteq T_k$, tout indice i et tout terme u, si $T_i \vdash u$ est prouvable, alors il en existe une preuve simple.*

Preuve
On prouve, par récurrence sur la paire (i, n) que, s'il existe une preuve de $T_i \vdash u$ de taille n, il en existe une preuve simple.

Dans le cas où $i = 0$, c'est le lemme de localité.

Sinon, s'il existe un $j < i$ tel que $T_j \vdash u$ est prouvable, il suffit d'appliquer l'hypothèse de récurrence.

Sinon, on applique l'hypothèse de récurrence aux deux sous preuves immédiates de la preuve de $T_i \vdash u$. La condition 2 des preuves simples est satisfaite par construction. La condition 1 pourrait ne pas être satisfaite dans le cas où $T_i \vdash u$ est un noeud interne de la preuve. Mais dans ce cas, il suffit de considérer une (sous-)preuve de $T_i \vdash u$ qui ne contient pas $T_i \vdash u$ comme noeud interne ; par hypothèse de récurrence elle satisfait les 4 conditions.

Les conditions 3 et 4 sont satisfaites, par minimalité de la preuve, comme dans la preuve du lemme de localité. $\square$

Si C est une contrainte, on dira que le membre gauche T_i est *minimal non résolu* si, pour tout T_j tel que $T_j \subseteq T_i$, $T_j \neq T_i$ et $T_j \Vdash u_j \in C$, u_j est une variable. Dans ce cas, on note $T_i' = T_i \cup \{x \mid T_j \Vdash x \in C, T_j \subseteq T_i, T_j \neq T_i\}$.

Lemme 7 *Soit C une contrainte et σ une solution de C. Soit T_i un membre gauche minimal non résolu de C.*

Si $T_i\sigma \vdash u$ a une preuve simple dont la dernière règle est une décomposition ou un axiome, alors il existe $t \in \mathsf{St}(T_i)$, t non variable, tel que $u = t\sigma$.

Preuve
Soit $T_i\sigma \vdash u$ une preuve simple. On suppose de plus i minimal sans perte de généralité. On procède alors par récurrence sur la preuve.

Cas 1 : la dernière règle est un axiome . Dans ce cas, $u \in T_i\sigma$. Donc il existe $t \in T_i$ tel que $t\sigma = u$. Si t était une variable, comme $T_t \subseteq T_i$ et $T_t \neq T_i$ par définition du système de contraintes et que $T_t \Vdash v \in C$ avec $x \in Var(v)$, on aurait, par hypothèse du lemme, $T_t \Vdash t \in C$ et donc, comme σ est solution de C, $T_t\sigma \vdash t\sigma$ prouvable. Autrement dit $T_t\sigma \vdash u$ prouvable, ce qui contredit la minimalité de i. Donc t n'est pas variable, ce qui termine ce cas.

cas 2 : la dernière règle est un déchiffrement .

$$\frac{T_i\sigma \vdash \{u\}_v \quad T_i\sigma \vdash v}{T_i\sigma \vdash u}$$

Par simplicité de la preuve (propriété 1), la dernière règle appliquée pour obtenir $T_i\sigma \vdash \{u\}_v$ est une règle de décomposition ou un axiome. Donc, par hypothèse de récurrence, il existe un terme non variable $t \in \mathsf{St}(T_i)$ tel que $t\sigma = \{u\}_v\sigma$. Comme t n'est pas une variable, t ne peut-être qu'un chiffrement : $t = \{t_1\}_{t_2}$. De plus, $t_1\sigma = u$. t_1 ne peut pas être une variable, pour les mêmes raisons que dans le cas 1 (minimalité de i et hypothèses sur le système de contraintes). On a donc un terme t_1 non variable, $t_1 \in \mathsf{St}(T_i)$ (puisque $\{t_1\}_{t_2} \in \mathsf{St}(T_i)$) tel que $t_1\sigma = u$, ce qui termine ce cas.

Cas 3 : la dernière règle est une projection . Par exemple une projection gauche (le cas de la projection droite est identique).

$$\frac{T_i\sigma \vdash < u, v >}{T_i\sigma \vdash u}$$

Comme dans le cas précédent, la dernière règle appliquée pour obtenir $T_i\sigma \vdash < u, v >$ ne peut être qu'une règle de décomposition ou un axiome. Par hypothèse de récurrence, il existe donc un terme non variable $t \in \mathsf{St}(T_i)$ tel que $t\sigma =< u, v >$. Comme dans le cas précédent, $t =< t_1, t_2 >$ et $t_1\sigma = u\sigma$. Comme précédemment, t_1 n'est pas une variable, ce qui termine ce cas.

$\square$

Lemme 8 *Soit C une contrainte et σ une solution de C. Soit T_i un membre gauche minimal non résolu de C.*

Si T_i ne contient pas deux sous-termes distincts non variables qui sont unifiables, alors

$$\left.\begin{array}{r} T_i\sigma \vdash u\sigma \textit{prouvable} \\ u \in \mathsf{St}(T_i), u \textit{ non variable} \end{array}\right\} \Rightarrow T_i' \vdash u \textit{est prouvable}$$

Preuve
On considère (ce qui est possible d'après le lemme 6) une preuve simple de $T_i\sigma \vdash u\sigma$. On prouve alors le lemme par récurrence sur cette preuve.

Si la dernière règle est un axiome. alors ou bien $u \in T$ et le lemme est prouvé, ou bien il existe un terme $t \in T_i$ distinct de u tel que $t\sigma = u\sigma$. Par simplicité de la preuve, t ne peut pas être une variable (si t est une variable, $T_t \Vdash t \in C$ et donc $T_t\sigma \vdash u\sigma$ est prouvable). Il en résulte que T_i contient deux sous-termes distincts non variables et unifiables (t et u).

Si la dernière règle est un déchiffrement.

$$\frac{T_i\sigma \vdash \{u\sigma\}_v \quad T_i\sigma \vdash v}{T_i\sigma \vdash u\sigma}$$

Par minimalité de la preuve (propriété 1 de la simplicité), la dernière règle appliquée pour obtenir $T_i\sigma \vdash \{u\sigma\}_v$ ne peut être qu'un axiome ou une décomposition. On peut donc appliquer le lemme 7 : il existe un terme t non variable de $\mathsf{St}(T_i)$ tel que $t\sigma = \{u\sigma\}_v$. Comme t n'est pas une variable, $t = \{t_1\}_{t_2}$. On a alors $t_1\sigma = u\sigma$. De plus, t_1 lui-même n'est pas une variable, par simplicité de la preuve (autrement on aurait une preuve de $T_{t_1}\sigma \vdash u\sigma$). Comme t_1, u sont deux sous-termes non variables de T_1, par hypothèse du lemme, $t_1 = u$. De plus, par hypothèse de récurrence, $T'_i \vdash \{u\}_{t_2}$ est prouvable.

Si maintenant t_2 n'est pas une variable, comme $t_2\sigma = v$ et $T_i\sigma \vdash t_2\sigma$, $t_2 \in \mathsf{St}(T_i)$, par hypothèse de récurrence, $T'_i \vdash t_2$ est prouvable. Alors $T'_i \vdash u$ est prouvable :

$$\frac{T'_i \vdash \{u\}_{t_2} \quad T'_i \vdash t_2}{T'_i \vdash u}$$

Si t_2 est une variable, alors $t_2 \in T'_i$ et donc $T'_i \vdash u$ est prouvable.

Si la dernière règle est une projection . Le cas est semblable au précédent (en plus simple)

Si la dernière règle est une règle de composition. Par exemple, une paire (le cas du chiffrement est semblable).

$$\frac{T_i\sigma \vdash u_1 \quad T_i\sigma \vdash u_2}{T_i\sigma \vdash u\sigma}$$

u n'est pas une variable et appartient à $\mathsf{St}(T_i)$, donc $u =< t_1, t_2 >$ avec $t_1\sigma = u_1$, $t_2\sigma = u_2$. Si t_1 (resp. t_2) n'est pas une variable, par hypothèse de récurrence et puisque $t_1 \in \mathsf{St}(T_i)$ et $T_i\sigma \vdash t_1\sigma$ est dérivable, il en résulte que $T'_i \vdash t_1$ est dérivable (resp. $T'_i \vdash t_2$ est dérivable). Si par contre t_1 est une variable (resp. t_2 est une variable) alors $t_1 \in T'_i$ (resp. $t_2 \in T'_i$) et donc, dans tous les cas, $T'_i \vdash t_1$ et $T'_i \vdash t_2$ sont dérivables. Il en est donc de même pour $u =< t_1, t_2 >$.

$\square$

Lemme 9 *Si σ est une solution de C et C n'est pas en forme résolue, alors il existe une contrainte C' et des substitutions θ, τ telles que $C \rightsquigarrow_\theta C'$, τ est une solution de C' et $\sigma = \theta\tau$.*

Preuve

Comme C n'est pas en forme résolue, il existe un membre droit minimal T_i tel que $T_i \Vdash u \in C$

et $u \notin X$. Comme σ est une solution de C, $T_i\sigma \vdash u\sigma$ est prouvable, donc prouvable par une preuve simple d'après le lemme 6. On envisage alors les différents cas de règle appliquée en dernier dans une telle preuve :

Cas 1 : la dernière règle est une composition Par exemple, une paire (le cas est identique pour un chiffrement) :

$$\frac{T\sigma \vdash v_1 \quad T\sigma \vdash v_2}{T\sigma \vdash u\sigma}$$

et $u\sigma =< v_1, v_2 >$. Comme u n'est pas une variable, $u =< u_1, u_2 >$ et $u_1\sigma = v_1$, $u_2\sigma = v_2$. En appliquant alors la règle R_5 à C, on obtient $T \vdash u_1 \wedge T \vdash u_2$, dont σ est à nouveau une solution.

Dans le cas du chiffrement, il suffit de remplacer R_5 par R_4.

Cas 2 : la dernière règle est l'axiome ou une décomposition Dans ce cas, par le lemme 7, il existe un terme t non variable tel que $t \in \mathsf{St}(T_i)$ et $t\sigma = u\sigma$. Si $t \neq u$, alors on peut appliquer la règle R_2 à $T_i \Vdash u$, obtenant une contrainte qui satisfait aux conditions du lemme. Sinon, $u \in \mathsf{St}(T_i)$ et, d'après le lemme 8, ou bien on peut appliquer R_3, ou bien on peut appliquer R_1.

□

Lemme 10 *Toute contrainte qui n'est pas en forme résolue est réductible ou bien n'a pas de solution.*

Preuve
C'est une conséquence du lemme 9 : si C n'est pas en forme résolue et possède une solution, alors il est possible d'appliquer une règle à C. □

4 Décision en nombre borné de sessions

4.1 Le problème est dans co-NP

Étant données des instances (en nombre fixé) de chaque rôle, on commence par deviner un entrelacement des règles qui respecte l'ordre des règles dans chaque instance de rôle. Soient $u_1 \Rightarrow v_1, \ldots, u_n \Rightarrow v_n$ cet entrelacement (dans lequel les règles sans prémisse ou sans conclusion n'apparaissent pas). Il existe une attaque sur le protocole (avec les instances fixées) si et seulement si le système de contraintes suivant admet une solution :

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

Bien entendu, les variables apparaissant dans chaque instance de rôle ont été renommées de manière à ce qu'il n'y ait pas de conflit de nom. T_0 est l'ensemble (fini) des connaissances initiales de l'intrus qui comprend typiquement les noms des agents intervenant dans les instances de rôles considérées, les clefs privées et nonces des agents malhonnêtes et aussi les messages initiaux (règles sans prémisses) de chaque instance de rôle qui comprend un tel message.

Exemple du protocole de Denning-Sacco à clefs partagées

$$\begin{array}{lll} 1. & A \to S: & < A, B > \\ 2. & S \to A & \{<< B, N_{AB} >, < N_S, \{< N_{AB}, < A, N_S >>\}_{K_{BS}} >>\}_{K_{AS}} \\ 3. & A \to B & \{< N_{AB}, < A, N_S >>\}_{K_{BS}} \\ 4. & B \to A & \{S_{AB}\}_{N_{AB}} \end{array}$$

On suppose une instance du rôle A par a (honnête), une instance du rôle S par s (honnête), une instance du rôle B par b (honnête). Chaque rôle comporte une seule règle (en dehors de l'initialisation).

On a alors à entrelacer les règles :

$$\begin{array}{lrcl} s1. & < a, b > & \Rightarrow & \{<< b, N_{ab} >, < N_s, \{< N_{ab}, < a, N_s >>\}_{K_{bs}} >>\}_{K_{as}} \\ a1. & \{<< b, x >, < y, z >>\}_{K_{as}} & \Rightarrow & z \\ b1. & \{< x', < a, y' >>\}_{K_{bs}} & \Rightarrow & \{s_{ab}\}_{x'} \end{array}$$

Il y a donc 6 entrelacements possibles. En fait, comme s1 ne comporte pas de variable, seuls les deux entrelacements entre a1 et b1 sont significatifs. Considérons l'entrelacement $(s1, a1, b1)$, ceci conduit aux contraintes :

$$\begin{array}{rcl} a, b, s, < a, b > & \Vdash & < a, b > \\ a, b, s, < a, b >, & & \\ \{<< b, N_{ab} >, < N_s, \{< N_{ab}, < a, N_s >>\}_{K_{bs}} >>\}_{K_{as}} & \Vdash & \{<< b, x >, < y, z >>\}_{K_{as}} \\ a, b, s, z, < a, b >, & & \\ \{<< b, N_{ab} >, < N_s, \{< N_{ab}, < a, N_s >>\}_{K_{bs}} >>\}_{K_{as}}, z & \Vdash & \{< x', < a, y' >>\}_{K_{bs}} \\ a, b, s, z, \{s_{ab}\}_{x'}, < a, b >, & & \\ \{<< b, N_{ab} >, < N_s, \{< N_{ab}, < a, N_s >>\}_{K_{bs}} >>\}_{K_{as}} & \Vdash & s_{ab} \end{array}$$

Théorème 1 *Le problème du secret pour un nombre borné de sessions est dans co-NP.*

Preuve
(sketch) On remarque tout d'abord, que, grâce au lemme 4, la simplification de contraintes se termine. D'autre part, grâce au lemme 9 et par récurrence sur la longueur de réduction, si la contrainte a une solution, alors il existe une forme résolue qui est atteinte par la réduction. Enfin, par le lemme **??**, les solutions de cette forme résolue sont aussi des solutions de la contrainte initiale et, par le lemme 5, la forme résolue a au moins une solution. En conclusion, il existe une attaque si et seulement s'il existe une dérivation finie $C \rightsquigarrow_\sigma^* C'$ où C' est en forme résolue. L'attaque est de plus donnée par $\sigma\tau$ où τ est une solution de C'.

Concernant la complexité. L'entrelacement, puis la séquence de réductions est devinée. Si les substitutions sont de plus non pas calculées, mais conservées sous forme résolue (de taille polynômiale), il n'est pas nécéssaire de les appliquer, car il n'est pas nécéssaire d'unifier avec les termes introduits par les substitutions, qui se trouvent déjà comme des sous-termes des membres gauches (cette partie mériterait d'être détaillée, cf paragraphe ci-dessous. On admettra le résultat). $\square$

Noter qu'en fait on a un résultat plus fort : *toutes* les attaques pour un entrelacement fixé sont obtenues en calculant les formes résolues de C et en composant pour chacune d'elles la substitution calculée le long de la dérivation avec une solution de la forme résolue.

4.2 Remarques sur le système de contraintes en vue d'une implantation

Tout d'abord, le résultat de complétude reste vrai si l'on applique les règles de résolution qu'à une contrainte qui a un membre gauche minimal (pour l'inclusion). Ensuite, certaines règles (R_1, R_5, R_6) préservent l'ensemble des solutions. Donc, lorsqu'on applique ces règles à une contrainte, il est inutile d'appliquer d'autres règles à la même contrainte.

En fin de compte, les seuls cas où il faut considérer plusieurs réductions à partir d'une même contrainte C sont ceux où, si T est un membre gauche minimal de C tel qu'il existe au moins une contrainte $T \Vdash u$ non résolue dans C, les règles R_1, R_5, R_6 ne sont applicables à aucune des contraintes $T \Vdash u$ de C. Dans ce cas, il faut choisir l'une de ces contraintes $T \Vdash u$ et lui appliquer les règles R_2, R_3, R_4 de toutes les manières possibles.

Remarquons aussi que, plutôt que d'appliquer les substitutions, on peut les conserver dans un système d'équations E en forme résolue, conservé avec la contrainte. La règle R_2, par exemple, devient alors :

$$C \wedge T \Vdash u, E \rightsquigarrow C \wedge T \Vdash u, E \wedge u = t$$

Si t, u sont non variables, t est un sous-terme de T et $u = t$ n'est pas une conséquence de E.

L'ensemble d'équations est maintenu en forme résolue (supposée satisfaisable). On prouve alors que les équations de E sont de la forme $x = t$ où t est un sous-terme d'un membre gauche de T (c'est un invariant des règles). Il en résulte qu'il n'est pas nécessaire de considérer les unificateurs avec les termes introduits par les substitutions : la version "basique" de la résolution de contraintes esquissée ci-dessus est complète.

5 Ajout du chiffrement asymétrique

Sera complété ultérieurement.