Une Comparaison entre Deux Méthodes de Preuve de Sécurité

Duong Hieu Phan David Pointcheval

***Abstract*— In this paper, we compare two methods for security proofs - a formal method, and the method by reduction from the complexity theory. A modification of the Otway-Rees protocol is proposed to show out a difference between the two methods : the exchanged key is provably secure in the sense of the BAN logic but it is not when we analyze it by reduction. The difference is due to a limitation of BAN logic, which has not been noticed before, that it does not consider the relation between different ciphertexts. Note that in the original Otway-Rees protocol, under the hypothesis of semantic security of the symmetric encryption scheme, we prove the semantic security of the exchanged key which is a similar result to the one obtained with BAN logic.**

Keywords: theorical computer science, complexity theory, formal methods, security proofs, reductions, BAN logic.

Resumé : Dans cet article, nous comparons deux méthodes de preuve de sécurité : une méthode formelle et la méthode par réduction au sens de la théorie de la complexité. Une modification du protocole Otway-Rees est proposée pour montrer une différence entre ces deux méthodes : la clé échangée est montrée sûre avec la logique BAN, alors qu'elle ne l'ai pas lorsque nous analysons le schéma selon la méthode par réduction. Cette différence montre une limitation de la logique BAN qui n'était pas connue, à savoir qu'elle ne considère pas les relations possibles entre différents chiffrés. Remarquons que dans le protocole original Otway-Rees, sous l'hypothèse de la sécurité sémantique du schéma de chiffrement symétrique, nous prouvons la sécurité sémantique de la clé échangée, qui est un résultat similaire à celui obtenu suite à une analyse par la logique BAN.

Mots-clés : informatique théorique, théorie de la complexité, méthodes formelles, preuves de sécurité, réductions, logique BAN.

I. Introduction

La sécurité des protocoles cryptographiques repose sur la sécurité des primitives cryptographiques (hypothèses algorithmiques) et sur l'absence de failles dans la construction, l'agencement de ces primitives. Les preuves de sécurité ont pour objectif de montrer l'impossibilité de " casser " le protocole sans contredire les hypothèses algorithmiques.

Ces preuves de sécurité sont techniquement très intéressantes, mais également très importantes d'un point de vue pratique. Elles permettent en effet de montrer que les schémas utilisés en pratique ne présentent pas de failles, mais aussi de préciser les paramètres convenables pour garantir le niveau de sécurité souhaité. Ainsi, les organismes de normalisation réclament-ils désormais une preuve de sécurité avant de normaliser un protocole cryptographique.

Deux approches rigoureuses distinctes ont vu le jour, depuis une quinzaine d'années, dans des communautés très différentes : l'une repose sur les méthodes formelles, par déduction logique avec des règles de réécriture; l'autre se place dans le contexte de la théorie de la complexité, avec la réduction d'un problème difficile à une attaque du protocole.

Le principal avantage des méthodes formelles (que nous illustrons avec la logique BAN[3]) est qu'elles permettent la construction automatique de preuve. Cependant, ces méthode nécessitent la formalisation du protocole en formules logiques (la phase d'idéalisation du protocole) qui ne reflètent pas exactement le protocole original. Il y a donc eu de nombreuses attaques [6] sur cette phase dans le cadre de la logique BAN. Un autre inconvénient de ces méthodes est qu'elles ne tiennent pas compte des aspects arithmétiques (ou alors les règles de déduction deviendraient trop comliquées), donc il est possible que des attaques passent au travers de ces preuves en utilisant des relations arithmétiques simples entre des messages. En revanche, la méthode de preuve par réduction a un grand avantage puisqu'elle considère les aspects réels : les moyens des attaquants, les niveaux de sécurité, ...

Dans cet article, nous faisons une comparaison entre ces deux méthodes. Nous montrons la sécurité sémantique de la clé échangée du protocole Otway-Rees par réduction sous l'hypothèse que le schéma de chiffrement utilisé dans le protocole soit sémantiquement sûr. Ce résultat correspond bien au résultat de Burrows *et al.*[3] avec la logique BAN. Pourtant, nous proposons une modification du protocole Otway-Rees dans laquelle ces deux méthodes donnent des résultats différents : une attaque qui utilise la relation des messages est détectée par l'analyse par réduction mais elle peut passer au travers de la logique BAN.

II. Analyse d'un protocole par la logique BAN

La logique BAN [3] a été proposée en 1989 comme une méthode formelle pour analyser des protocoles d'authentification. Comme pour décrire un système formel, on présente d'abord les notations, puis les règles de déduction de la logique BAN. Les notations de la logique BAN décrivent les notions dans le protocole cryptographique : les symboles P, Q, R représentent les participants; X, Y les aléas; K les clés; $P \models X$ (P *croit* X) exprime que P fonctionne en supposant que X est vrai, $P \succ X$ (P *a dit* X) exprime que P a envoyé un message contenant X à un moment quelconque, $P \overset{K}{\leftrightarrow} Q$

Phan Duong Hieu, École Normale Supérieure, Department d'Informatique, 45 rue d'Ulm, 75230 Paris Cedex 05, France (Email: duong.hieu.phan@ens.fr)
David Pointcheval, École Normale Supérieure, Department d'Informatique, 45 rue d'Ulm, 75230 Paris Cedex 05, France (Email: david.pointcheval@ens.fr).

exprime que K est une bonne clé partagée entre P et Q, c'est-à-dire exceptés P et Q ou un participant crédible par P et Q, personne ne connaît K; ... Pour le raisonnement, les auteurs ont donné les postulats comme la "*message meaning rule* :

$$\frac{P \models P \overset{K}{\leftrightarrow} Q, P \triangleleft \{X\}_K}{P \models Q \succ X}$$

qui signifie que si P croit en la clé K partagée avec Q et s'il voit le message X chiffré sous cette clé K, alors P croit que Q a dit X. Pour analyser un protocole, on doit d'abord transformer le protocole réel en protocole formel contenant des formules logiques, puis donner les hypothèses de l'état initial (l'état initial et les croyances des différents participants au début d'une session d'exécution du protocole), enfin, on attache les formules logiques à chaque étape du protocole et on déduit les assertions de croyance (exécutées par chaque participant) en utilisant les règles de déduction. Remarquons que les règles de déductions impliquent des hypothèses sur les primitives utilisées dans le protocole (par exemple, le schéma de chiffrement est parfaitement sûr).

III. Analyse d'un protocole par réduction

On remarque d'abord qu'un attaquant tout puissant, ou bien un attaquant non-limité dans le temps, peut effectuer une recherche exhaustive pour balayer tous les cas possibles et il peut casser le protocole. Donc, pour analyser la sécurité des protocoles, il nous faut donner des *notions de sécurité* [1], des *hypothèses algorithmiques* et il nous faut aussi préciser les informations accessibles à l'attaquant, les *moyens* dont il dispose [1], [5]. Avec une preuve par réduction, sous des hypothèses algorithmiques précises, on montre la sécurité des protocoles. Pour cela, on considère un attaquant qui peut casser le protocole, puis on utilise cet attaquant pour construire une attaque contre une des hypothèses algorithmiques.

A. Notions de sécurité du chiffrement symétrique

D'abord, on précise des notations utilisées par la suite :

Coins : l'ensemble des séquences infinies
$\mathcal{M}$: espace des messages
$\mathcal{K}$: espace des clés
$\mathcal{C}$: espace des chiffrés $= \{0,1\}^\star$

Définition 1 *Un schéma de chiffrement symétrique $\mathcal{S} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ est défini par 3 algorithmes:*

$\mathcal{G}$: $\quad \mathsf{Coins} \to \mathcal{K}$
$\mathcal{E}$: $\quad \mathcal{K} \times \mathcal{M} \times \mathsf{Coins} \to \mathcal{C}$
$\mathcal{D}$: $\quad \mathcal{K} \times \mathcal{C} \to \mathcal{M} \bigcup \{\perp\}$

Un schéma de chiffrement symétrique $\mathcal{S} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ est dit *déterministe* si $\mathcal{E}$ est déterministe, c'est-à-dire :

$$\mathcal{E} : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$$

On appelle $\mathcal{E}$ algorithme de chiffrement, $\mathcal{D}$ algorithme de déchiffrement et $\mathcal{G}$ algorithme de génération de clés. Il faut que $\mathcal{D}(\mathcal{E}(K, m, r)) = m$ pour tout $K \in \mathcal{K}, m \in \mathcal{M}, r \in \mathsf{Coins}$. Dans les schémas de chiffrement, $\mathcal{D}(K, c) = \perp$ est utilisé dans le cas où c n'est le chiffré d'aucun message m sous la clé K.

Définition 2 *Un schéma de chiffrement symétrique $\mathcal{S} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ est dit $\epsilon-$sémantiquement sûr face à un adversaire $\mathcal{A}$ si:*

$$\mathsf{Adv}^{\mathsf{ind}}_{\mathcal{S}}(\mathcal{A}) \overset{\mathsf{def}}{=} \left| 2 \times \Pr_{b,r} \begin{bmatrix} m_0, m_1 \leftarrow \mathcal{A}_1, K \leftarrow \mathcal{K}, \\ c = \mathcal{E}(K, m_b, r), \\ b' = \mathcal{A}_2(m_0, m_1, c) : b' = b \end{bmatrix} - 1 \right|$$

est inférieur à ϵ.
Un schéma de chiffrement symétrique est dit $(t, \epsilon)-$ sémantiquement sûr si :

$$\mathsf{Adv}^{\mathsf{ind}}_{\mathcal{S}}(t) \overset{\mathsf{def}}{=} \underset{|\mathcal{A}| \leq t}{\mathrm{Max}}(\mathsf{Adv}^{\mathsf{ind}}_{\mathcal{S}}(\mathcal{A})) \leq \epsilon.$$

B. Les moyens d'un attaquant contre le chiffrement symétrique

Contrairement au chiffrement asymétrique où un attaquant peut chiffrer tout message de son choix, dans le contexte symétrique, l'accès à l'algorithme de chiffrement sous la clé K (avec la restriction de ne pas l'utiliser sur m_0 et m_1 dans le cas déterministe) donne à l'attaquant des informations puisqu'il ne connaît pas la clé sécrète. Cette attaque est appelée attaque à *clairs choisis* (ou *chosen-plaintext attack* - CPA). Dans certains cas, l'attaquant peut avoir accès à l'algorithme de déchiffrement sous la clé K (avec la restriction de ne pas l'utiliser sur le challenge). Cette attaque est appelée attaque à *chiffrés choisis* - CCA. On note le $\mathsf{CPA}/\mathsf{CCA}$ l'attaque qui donne accès à la fois à l'algorithme de chiffrement et à l'algorithme de déchiffrement sous la clé K.

C. Mise en accord de clé

Une notion de sécurité que l'on doit examiner est celle de la confidentialité de la clé échangée dans un tel protocole. Pour cela, on suppose d'abord que l'attaquant contrôle le réseau et tous les messages échangés. Il peut de plus interagir avec les participants en leur posant une $\mathsf{Test-query}$: quand il pose une $\mathsf{Test-query}$ à un des deux participants (A, par exemple) qui a accepté le protocole, on choisit un bit β aléatoire, si β = 0 on retourne K_0-la clé obtenue dans le protocole, si $\beta = 1$ on retourne K_1-une chaîne aléatoire. On note $\mathrm{Prot}(K)$ le protocole dans lequel la clé échangée reçoit la valeur K.

Définition 3 *La clé échangée dans un protocole de mise en accord de clé est dite ϵ - sémantiquement sûre face à un adversaire $\mathcal{A}$ si:*

$$\mathsf{Adv}^{\mathsf{ind}}_{P}(\mathcal{A}) \overset{\mathsf{def}}{=} \left| 2 \times \Pr_{b,r} \begin{bmatrix} K_0, K_1 \leftarrow \mathcal{K}, \beta \leftarrow \{0,1\} \\ K_\beta \leftarrow \mathsf{Test-query}, \\ \beta' = \mathcal{A}(\mathrm{Prot}(K_0), K_\beta) : \beta' = \beta \end{bmatrix} - 1 \right|$$

est inférieur à ϵ.
La clé échangée dans un protocole de mise en accord de clé est dite $(t, \epsilon)-$sémantiquement sûre si:

$$\mathsf{Adv}^{\mathsf{ind}}_{P}(t) \overset{\mathsf{def}}{=} \underset{|\mathcal{A}| \leq t}{\mathrm{Max}}(\mathsf{Adv}^{\mathsf{ind}}_{P}(\mathcal{A})) \leq \epsilon.$$

Maintenant, on donne la définition de l'authentification mutuelle, une notion de sécurité également importante pour un protocole d'échange de clé authentifiée. Le but est qu'après chaque session, le participant qui accepte la clé échangée veut s'assurer que son partenaire l'accepte aussi. Puisqu'il est impossible d'obtenir à la fois que "A accepte implique B accepte" et que "B accepte implique A accepte", on change un peu le but. Intuitivement, un participant *accepte* lorsque toutes les étapes sont consistantes et lui permettent d'extraire la clé partagée. Un participant *termine* le protocole s'il n'y a plus de message à échanger [2]. Les définitions exactes de ces deux notions sont introduites pour chaque protocole.

Définition 4 *Un protocole d'échange de clé garantit l'authentification mutuelle si aucun attaquant ne peut contrefaire le rôle d'un participant. Plus précisément, lorsqu'un participant termine en acceptant, son partenaire a nécessairement accepté.*

IV. Analyse du protocole Otway-Rees

Otway et Rees ont proposé un protocole d'échange de clé en 1987 [7]. Ce protocole met en œuvre deux participants et un serveur. Il est intéressant en raison du petit nombre de messages échangés. On présente le protocole ci-dessous, A et B sont deux participants, S est le serveur. K_{as} est la clé secrète que A partage avec S, K_{bs} est la clé secrète que B partage avec S. N_a, N_b et M sont des aléas générés par A et B. Le serveur S génère K_{ab} qui deviendra la clé de session partagée entre A et B.

Message 1	$A \rightarrow B$	:	$M, A, B, \{N_a, M, A, B\}_{K_{as}}$
Message 2	$B \rightarrow S$	:	$M, A, B, \{N_a, M, A, B\}_{K_{as}}$, $\{N_b, M, A, B\}_{K_{bs}}$
Message 3	$S \rightarrow B$	:	$M, \{N_a, K_{ab}\}_{K_{as}}, \{N_b, K_{ab}\}_{K_{bs}}$
Message 4	$B \rightarrow A$	:	$M, \{N_a, K_{ab}\}_{K_{as}}$

A. Analyse par la logique BAN

Les auteurs ont montré

$$A \models A \overset{K_{ab}}{\leftrightarrow} B \qquad B \models A \overset{K_{ab}}{\leftrightarrow} B$$

Avec cette conclusion, A et B savent que K_{ab} est une bonne clé partagée mais l'un ne sait pas si l'autre connaît effectivement cette clé. Cette conclusion montre la sécurité de la clé échangée mais elle ne montre pas si le protocole garantit l'authentifition mutuelle, qui exige que lorsqu'un participant termine avec une clé, son partenaire connaît également cette clé [2].

B. Analyse par réduction

Théorème 1 *La clé échangée dans le protocole Otway-Rees est sémantiquement sûre sous l'hypothèse que le schéma de chiffrement utilisé dans protocole soit sémantiquement sûr selon des attaques à clairs et chiffrés choisis:*

$$\mathsf{Adv}_P^{\mathsf{ind}}(\mathcal{A}) \leq 2N \cdot \mathsf{Adv}_{\mathcal{S}}^{\mathsf{ind-cpa/cca}}(t)$$

Proof: On utilise des jeux successifs (cette méthode a été introduite et développée ces deux dernières années [9], [4]) dans lesquels on transforme à chaque étape la distribution de probabilité pour réduire le problème de la sécurité sémantique de la clé échangée au problème de la sécurité du schéma de chiffrement supposé sémantiquement sûr.

Game_0 : Le protocole est réalisé avec les clés K_{ab}^i ($i = \overline{1, N}$) choisies aléatoirement par S pour N sessions éventuellement simultanées. On note Prot(K_{ab}^i) le protocole correspondant à la session i. L'attaquant "casse" la clé de la session t en posant la $\mathsf{Test-query}$ à un oracle (soit A, soit B) et il reçoit K_β (β est choisi aléatoirement, $K_1 = K_{ab}^t$ et $K_0 = K'_{ab}$ choisie aléatoirement). L'attaquant doit déterminer si K_β est égale à K_{ab}^t ou pas, il retourne son choix β'. Avec probabilité (ϵ+1)/2, $\beta' = \beta$ (plus clairement, $\beta' = (K_\beta = K_{ab}^t)$). On note cet événement S_0 ainsi que S_i dans les jeux Game_i ci-dessous : Pr[S_0] = (ϵ + 1)/2.

Game_1 : On choisit aléatoirement i et on suppose que l'attaquant veut casser la clé K_{ab}^i(que l'on note K_{ab}) du protocole Prot(K_{ab}^i) (que l'on note par clarté Prot(K_{ab})). On stoppe les exécutions où la session i n'est pas testée et on retourne β' aléatoire. La probabilité que cette session soit justement celle choisie par l'attaquant est 1/N. Alors:

$$\begin{aligned}
\Pr[S_1] &= \Pr[\beta = \beta'] \\
&= \Pr[\beta = \beta' \wedge i \neq t] \\
&\quad + \Pr[\beta = \beta' \wedge i = t] \\
&= \Pr[i \neq t].\Pr[\beta = \beta' | i \neq t] \\
&\quad + \Pr[i = t].\Pr[\beta = \beta' | i = t] \\
&= \frac{N-1}{N} \cdot \frac{1}{2} + \frac{1}{N} \cdot \frac{\epsilon + 1}{2} \\
&= \frac{1}{2} + \frac{\epsilon}{2N}.
\end{aligned}$$

Game_2 : On modifie encore un peu ce jeu. Les clés K_{ab} et K'_{ab} ainsi que β sont choisis aléatoirement dès le début du jeu : $K_{ab}, K'_{ab} \overset{R}{\leftarrow} \mathcal{K}$, $\beta \overset{R}{\leftarrow}$ {0,1} : Pr[S_2] = Pr[S_1].

Game_3 :On remplace les chiffrements et déchiffrements avec la clé K_{as} et la clé K_{bs} par les couples d'oracles $(\mathcal{E}_{as}, \mathcal{D}_{as})$ et $(\mathcal{E}_{bs}, \mathcal{D}_{bs})$ respectivement. En utilisant ces oracles, l'attaquant retourne son choix β' : Pr[S_3] = Pr[S_2].

Game_4 : On choisit aléatoirement une valeur b : $b \overset{R}{\leftarrow} \{0, 1\}$.

- Si b = 0, on simule Prot(K_{ab}), l'attaquant retourne β' : Pr[S_4] = Pr[$\beta' = \beta$], ou bien Pr[S_4] = Pr[$b \bigoplus \beta' = \beta$].
- si b = 1, on simule Prot(K'_{ab}), l'attaquant retourne β' : Pr[S_4] = Pr[$\beta' = \neg(\beta)$] (puisque $K_0 = K'_{ab}$ et Pr[S_4] = Pr[$\beta' = (K_\beta = K'_{ab})$]), ou bien Pr[$S_4$] = Pr[$b \bigoplus \beta' = \beta$].

On combine ces deux cas et on définit $b' = b \bigoplus \beta'$. On note S'_4 l'événement $b' = \beta$, alors :

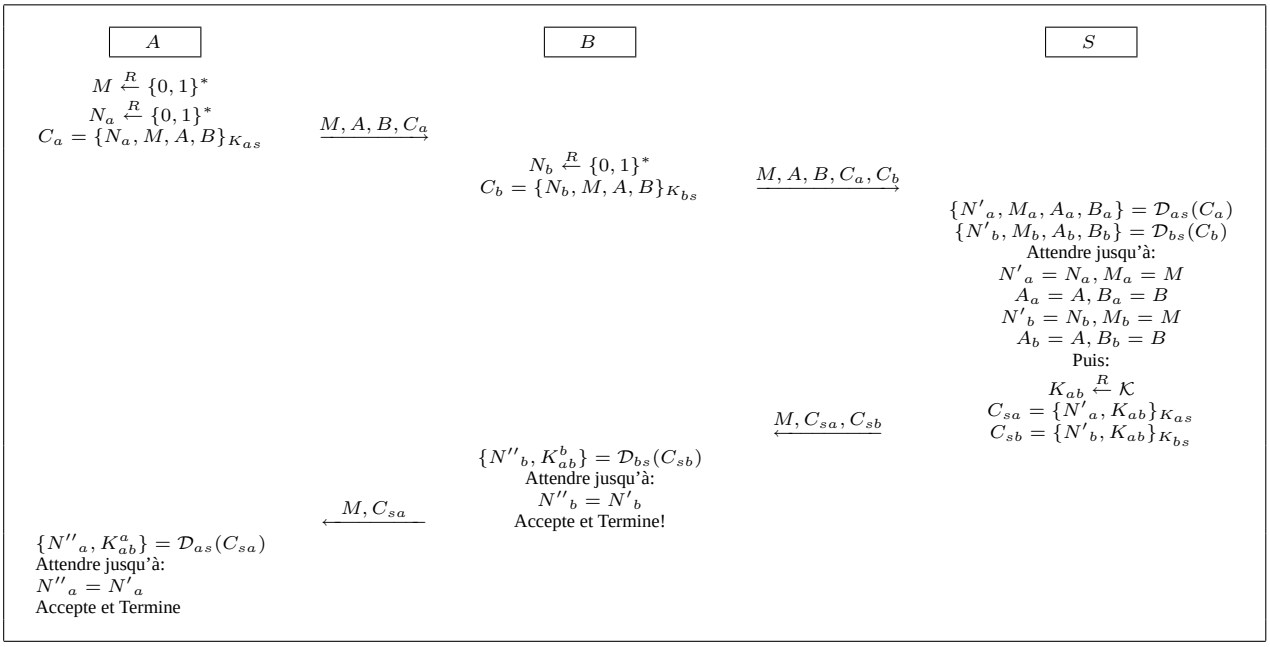

Fig. 1. L'action des participants dans le Protocole d'Otway-Rees

$$\begin{aligned}\Pr[S'_4] &= \Pr[b' = \beta] = \Pr[b = \beta \bigoplus \beta'] \\ &= \Pr[\beta = \beta' | b = 0] \cdot \Pr[b = 0] \\ &\quad + \Pr[\beta' = \neg(\beta) | b = 1] \cdot \Pr[b = 1] \\ &= \Pr[S_4].\end{aligned}$$

Game_5 : comme ci-dessus, mais dans ce jeu, b sera le bit choisi par le challengeur pour évaluer la sécurité sémantique du schéma de chiffrement $\mathcal{S}$. D'où, la simulation qui utilise β mais plus b. Dans le jeu précédent, on voit que Pr[$b' = \beta$] = Pr[$b = \beta \bigoplus \beta'$]. Alors, on retourne maintenant $b'' = \beta \bigoplus \beta'$. On note cet événement S''_5 ainsi que S''_i dans les jeux ci-dessous. On a Pr[S''_5] = Pr[$b'' = b$] = Pr[$\beta \bigoplus \beta' = b$] = Pr[$S'_5$] = Pr[$S'_4$].

Game_6 : On ne modifie pas mais on récrit le jeu précédent. K_{ab}, $K'_{ab} \xleftarrow{R} \mathcal{K}$, $b \xleftarrow{R}$ {0,1}. On note $m_0 = \{N_a, K_{ab}\}, m'_0 = \{N_b, K_{ab}\}$ et $m_1 = \{N_a, K'_{ab}\}, m'_1 = \{N_b, K'_{ab}\}$. On reçoit dans les messages 3 et 4 le chiffrement d'un des deux couples (m_0, m'_0) et (m_1, m'_1) : $c = (\mathcal{E}_{as}(m_b), \mathcal{E}_{bs}(m'_b))$ et on évalue b'', Pr[S''_6] = Pr[S''_5].

Game_7 : On remplace les deux couples (m_0, m'_0) et (m_1, m'_1) par (m_1, m'_0) et (m_1, m'_1). La différence est l'avantage de distinguer $(\mathcal{E}_{as}(m_0), \mathcal{E}_{bs}(m'_0))$ et $(\mathcal{E}_{as}(m_1), \mathcal{E}_{bs}(m'_0))$. Pour ce dernier, on remplace les oracles $\mathcal{E}_{bs}$ et $\mathcal{D}_{bs}$ par les algorithmes de chiffrement et déchiffrement avec la clé K_{bs}. Ça ne change en rien le jeu, et l'avantage de distinguer $(\mathcal{E}_{as}(m_0), \mathcal{E}_{bs}(m'_0))$ et $(\mathcal{E}_{as}(m_1), \mathcal{E}_{bs}(m'_0))$, en utilisant les oracles $\mathcal{E}_{as}$, $\mathcal{E}_{bs}$, $\mathcal{D}_{as}$, $\mathcal{D}_{bs}$ est égal à l'avantage de distinguer $\mathcal{E}_{as}(m_0)$ et $\mathcal{E}_{as}(m_1)$ en utilisant les oracles $\mathcal{E}_{as}$ et $\mathcal{D}_{as}$. $|\Pr[\mathrm{S}''_7] - \Pr[\mathrm{S}''_6]| \leq \mathsf{Adv}^{\mathsf{ind-cpa/cca}}_{\mathcal{E}}(t)$.

Game_8 : On remplace les deux couples (m_1, m'_0) et (m_1, m'_1) par (m_1, m'_1) et (m_1, m'_1). La différence est l'avantage de distinguer $(\mathcal{E}_{as}(m_1), \mathcal{E}_{bs}(m'_0))$ et $(\mathcal{E}_{as}(m_1), \mathcal{E}_{bs}(m'_1))$. Pour ce dernier, on remplace les oracles $\mathcal{E}_{as}$ et $\mathcal{D}_{as}$ par les algorithmes de chiffrement et déchiffrement avec la clé K_{as}. Ça ne change en rien le jeu, et l'avantage de distinguer $(\mathcal{E}_{as}(m_1), \mathcal{E}_{bs}(m'_0))$ et $(\mathcal{E}_{as}(m_1), \mathcal{E}_{bs}(m'_1))$, en utilisant les oracles $\mathcal{E}_{as}$, $\mathcal{E}_{bs}$, $\mathcal{D}_{as}$, $\mathcal{D}_{bs}$ est égal à l'avantage de distinguer $\mathcal{E}_{bs}(m_0)$ et $\mathcal{E}_{bs}(m_1)$ en utilisant les oracles $\mathcal{E}_{bs}$ et $\mathcal{D}_{bs}$: $|\Pr[\mathrm{S}''_8] - \Pr[\mathrm{S}''_7]| \leq \mathsf{Adv}^{\mathsf{ind-cpa/cca}}_{\mathcal{E}}(t)$.
Cependant, dans ce dernier jeu Game_8, on doit distinguer $(\mathcal{E}_{as}(m_1), \mathcal{E}_{bs}(m'_1))$ et $(\mathcal{E}_{as}(m_1), \mathcal{E}_{bs}(m'_1))$ qui sont identiques, donc b est indépendant de la vue du simulateur, ainsi $\Pr[\mathrm{S}''_8] = \frac{1}{2}$.

L'inégalité triangulaire nous donne:

$$\begin{aligned}\frac{\epsilon}{2N} = \frac{\epsilon/N + 1}{2} - \frac{1}{2} &= |\Pr[\mathrm{S}_1] - \Pr[\mathrm{S}''_8]| \\ &\leq 2\mathsf{Adv}^{\mathsf{ind-cpa/cca}}_{\mathcal{S}}(t).\end{aligned}$$

■

Sous l'hypothèse de la sécurité sémantique du schéma de chiffrement, on déduit la sécurité sémantique de la clé K_{ab}.

Authentification mutuelle : On peut facilement montrer que le protocole ne garantit pas l'authentification mutuelle :

- L'attaquant peut prendre un ancien message 1 de A et le renvoyer à B, puis il retient le message 4 que B envoie à A. Bien que l'attaquant ne connaisse pas la clé commune K_{ab}, A ne la connaît pas non plus puisqu'il ne participe pas au protocole. Alors, B accepte la clé K_{ab} mais pas A. Ceci montre que l'attaquant peut casser l'authentification $A - B$.

- L'attaquant suit le protocole jusqu'au message 3, puis il retient le message 3 que S envoie à B. Il ne l'envoie pas à B mais il joue le rôle de B pour envoyer le message 4, qui est explicite dans le message 3 à A. Alors A accepte la clé K_{ab} sans savoir que B ne reçoit pas K_{ab}. Ceci montre que l'attaquant peut casser l'authentification $B - A$.

V. Analyse du protocole Otway-Rees modifié

Pour tenter de garantir l'authentification mutuelle, nous ajoutons au protocole Otway-Rees une phase de confirmation de la clé:

$$\begin{array}{lllll}
\textit{Message 1} & A \rightarrow B & : & M, A, B, \{N_a, M, A, B\}_{K_{as}} \\
\textit{Message 2} & B \rightarrow S & : & M, A, B, \{N_a, M, A, B\}_{K_{as}}, \\
 & & & \{N_b, M, A, B\}_{K_{bs}} \\
\textit{Message 3} & S \rightarrow B & : & M, \{N_a, K_{ab}\}_{K_{as}}, \\
 & & & \{N_a, N_b, K_{ab}\}_{K_{bs}} \\
\textit{Message 4} & B \rightarrow A & : & M, \{N_a, N_b, K_{ab}\}_{K_{as}}, \\
 & & & \{N_a, N_b\}_{K_{ab}} \\
\textit{Message 5} & A \rightarrow B & : & \{N_b\}_{K_{ab}}
\end{array}$$

A. Analyse par la logique BAN

Théorème 2 *La clé échangée dans le protocole d'Otway-Rees modifié est sûre et le protocole garantit l'authentification mutuelle.*

En fait, nous pouvons prouver que non seulement :

$$A \models A \overset{K_{ab}}{\leftrightarrow} B \qquad B \models A \overset{K_{ab}}{\leftrightarrow} B$$

mais aussi:

$$A \models B \models A \overset{K_{ab}}{\leftrightarrow} B$$

$$B \models A \models A \overset{K_{ab}}{\leftrightarrow} B$$

Ceci implique l'énoncé du théorème.

B. Analyse par réduction

Théorème 3 *La clé échangée dans le protocole d'Otway-Rees modifié n'est pas sémantiquement sûre même sous l'hypothèse que le schéma de chiffrement utilisé dans protocole soit sémantiquement sûr selon des attaques à clairs et chiffrés choisis ou même parfaitement sûr devant tout attaquant.*

Proof: Quand un attaquant reçoit un challenge K qui est soit la vraie clé K_{ab} utilisée dans le protocole, soit une fausse clé K' choisie aléatoirement, il peut déterminer avec un avantage non-négligible si K est la vraie clé ou une fausse clé. En effet, en utilisant la clé K, l'attaquant :

- déchiffre le message $\{N_a, N_b\}_{K_{ab}}$ dans le message 4, il obtient m_4.
- déchiffre le message $\{N_b\}_{K_{ab}}$ dans le message 5, il obtient m_5.
- si m_5 est un suffixe de m_4, alors il croit que K est justement la clé K_{ab} sinon, K est une fausse clé.

On peut voir que la probabilité pour que l'attaquant retourne une fausse réponse est la probabilité, pour la clé $K's$ choisie aléatoirement, que le déchiffré par K_β de $\{N_b\}_{K_{ab}}$ soit un suffixe du déchiffré de $\{N_a, N_b\}_{K_{ab}}$. Il est évident que cette probabilité est négligeable quelle que soit la sécurité du schéma de chiffrement, sémantiquement sûr selon des attaques à clairs et chiffrés choisis ou parfaitement sûr devant tout attaquant. D'où le résultat. ■

Ce théorème nous donne un résultat tout à fait différent : la clé échangée n'est pas sémantiquement sûre (notion plus faible que la notion de sécurité parfaite prouvée par logique BAN) même sous l'hypothèse de la sécurité parfaite du schéma de chiffrement (exactement ce qui est supposé par logique BAN). Par conséquent, le protocole ne garantit pas l'authentification mutuelle.

En fait, on profite de la relation entre les messages $\{N_a, N_b\}_{K_{ab}}$ et $\{N_b\}_{K_{ab}}$ pour détecter la fausse clé. Tandis que pour la logique BAN, puisque ces deux messages sont considérés indépendants, la relation n'est pas détectée.

VI. Conclusions

Nous avons considéré deux méthodes d'analyse d'un protocole : méthode formelle avec la logique BAN et méthode d'analyse par réduction. Outre l'inconvénient de la perte d'information lors de la phase de formalisation (qui a été beaucoup analysée), une autre faiblesse des méthodes formelles que nous avons mise en évidence est qu'elles ne tiennent pas compte des propriété arithmétiques des attaques. Un des objectifs de notre travail dans l'avenir est de trouver un pont entre ces deux méthodes : une méthode qui permette de mener des analyses formelles similaires à celles usuellement faites avec les méthodes issues de la théorie de la complexité. Dans [8], nous avons proposé une extension de la logique BAN qui satisfait cette condition et qui permet d'analyser quelques protocoles plus complexes. Cependant, les règles de cette méthode sont compliquées ce qui rend difficile l'automatisation des preuves de sécurité.

References

[1] M. Bellare, A. Desai, E. Jokipii, and P. Rogaway. A concrete security treatment of symmetric encryption. In *Proceedings of 38th Annual Symposium on Foundations of Computer Science (FOCS 97)*. IEEE, 1997.

[2] M. Bellare and P. Rogaway. Entity Authentication and Key Distribution. In D. Stinson, editor, *Advances in Cryptology - Crypto 93 Proceedings*, volume LNCS 773, pages 232–249. Springer-Verlag, 1994.

[3] M. Burrows, M. Abadi, and R. Needham. A Logic of Authentication. *Proc. Cambridge Phil. Soc.*, 60:699–700, 1989.

[4] E. Fujisaki, T. Okamoto, D. Pointcheval, and J. Stern. RSA-OAEP is Secure under the RSA Assumption. In J. Kilian, editor, *Adv. in Cryptology – Proceedings of Crypto 2001*, volume LNCS 2139, pages 260–274. Springer-Verlag, 2001.

[5] J. Katz and M. Yung. Complete characterization of security notions for probabilistic private-key encryption. In *STOC 2000*, pages 245–254, 2000.

[6] W. Mao and C. Boyd. On a Limitation of BAN Logic. In *Advances in Cryptology - Proceedings of EUROCRYPT 93*, pages 240–247. Springer-Verlag, 1993.

[7] D. Otway and O. Rees. Efficient and Timely Mutual Authentication. *Operating Systems Review*, 21(1):8–10, 1987.

[8] D.H. Phan. *Une comparaison des preuves de sécurité*. Rapport de DEA, Ecole normale supérieure, juin 2002.

[9] V. Shoup. OAEP reconsidered. In J. Kilian, editor, *Adv. in Cryptology – Proceedings of Crypto 2001*, volume LNCS 2139, pages 239–259. Springer-Verlag, 2001.

PHAN Duong Hieu
Thésard en cryptographie au laboratoire d'informatique, École normale supérieur de Paris.

David POINTCHEVAL
Chargé de Recherche CNRS, chercheur en cryptographie au laboratoire d'informatique, École normale supérieur de Paris.