

## Résumé de la thèse - Véronique Cortier

Avec le développement des réseaux de communication, le besoin d'assurer la confidentialité et l'authenticité des messages échangés a considérablement augmenté. Les protocoles cryptographiques sont des règles d'échange entre les points du réseau, ils permettent de sécuriser les communications. Ils sont utilisés par exemple dans les distributeurs de billets, les abonnements aux chaînes de télévision payantes, la téléphonie mobile, le commerce électronique. Ils utilisent des primitives cryptographiques comme le chiffrement symétrique et asymétrique, le hachage et le « ou » exclusif bit à bit sur les messages. On suppose en général que ces échanges de messages ont lieu sur des canaux publics, en présence d'un ou plusieurs intrus qui ont une capacité de mémorisation infinie. De tels intrus peuvent ainsi intercepter tous les messages émis sur le réseau et en envoyer de nouveaux. La seule restriction sur le pouvoir de ces intrus est qu'ils ne peuvent déchiffrer un message uniquement s'ils possèdent l'inverse de la clef. Ils ne sont donc pas capables de « casser » les clefs de chiffrements. Malgré la concision de la description de ces protocoles, ils sont très difficiles à vérifier. Ainsi, G. Lowe a découvert que le protocole de Needham-Schroeder avait une faille, 18 ans après sa publication.

Mon travail au cours de la thèse s'articule autour de trois axes :

- l'étude et la comparaison des modèles de protocoles cryptographiques ;
- l'étude de classes décidables de protocoles cryptographiques, permettant pour certaines d'affaiblir l'hypothèse du chiffrement parfait ;
- l'aide à la vérification pratique des protocoles par un résultat de réduction sur le nombre de participants et le développement d'un outil de preuve.

**Modèles.** J'ai introduit un nouveau modèle de protocoles cryptographiques sous forme de clauses de Horn qui permet de les représenter dans toute leur généralité : chiffrement symétrique et asymétrique, clefs composées, hachage... Ce modèle présente deux avantages. D'une part, il est plus général que la plupart des modèles basés sur des systèmes de transitions. J'ai ainsi montré que ce modèle est strictement plus général que le modèle présenté par J. Millen et H. Rueß. D'autre part, il permet de réutiliser toutes les techniques classiques déjà développées en logique du premier ordre (stratégies de résolution, arbres sémantiques...)

Par ailleurs, j'ai apporté quelques éléments de réponse en ce qui concerne la comparaison de deux notions très différentes du secret. Dans la plupart des modèles, le secret est exprimé sous forme d'une propriété d'accessibilité : « il existe une trace valide telle que l'intrus connaît la donnée supposée secrète ». Or, dans le cadre du spi-calcul, le secret est modélisé par une équivalence observationnelle entre deux processus. Intuitivement, un protocole préserve le secret si l'on ne peut pas distinguer ce protocole d'un protocole « témoin » ne contenant pas de secret. J'ai montré comment relier la notion de secret exprimée sous forme d'accessibilité à la notion de secret exprimée sous forme d'équivalence observationnelle. Ce résultat a deux principaux intérêts. D'un point de vue conceptuel, il permet de mieux comprendre le lien entre ces deux propriétés de secret. En outre, il permet de développer une méthode de preuve de l'équivalence observationnelle entre processus. Je prouve dans ce cadre le secret du protocole de Needham-Schroeder-Lowe pour un nombre arbitraire de sessions. À ma connaissance, c'est la première fois que la preuve de ce protocole est apportée pour une propriété d'équivalence observationnelle.

**Classes décidables.** Il existe de très nombreux protocoles cryptographiques et chacun d'entre eux a presque toujours plusieurs variantes. J'ai donc cherché à développer des classes décidables de protocoles cryptographiques afin d'obtenir des méthodes automatiques de vérification. Des résultats satisfaisants existaient déjà dans le cadre d'un nombre borné de sessions. Cependant, les protocoles sont utilisés en réalité un nombre arbitraire de fois. Aussi, je me suis intéressée à des classes décidables pour un nombre non borné de sessions.

Le problème du secret d'un protocole peut se ramener à un problème de satisfaction d'un ensemble de clauses. Aussi, j'ai introduit un nouveau fragment décidable (pour la satisfaction) de clauses. Ce fragment est une variante étendue aux termes fonctionnels clos d'un des fragments présentés par Fermüller *et al.* Ce résultat permet d'exhiber une classe décidable de protocoles qui permet de modéliser la majorité des protocoles réels à condition d'abstraire les nonces par un nombre fini de constantes. Il a été étendu (dans un article à paraître dans TCS) au cas où plusieurs copies sont possibles sous une hypothèse de non entrelacement et où les données *basiques* (agents, nonces ou clefs) peuvent être copiées arbitrairement.

J'ai ensuite affaibli l'hypothèse du chiffrement parfait en tenant compte des propriétés algébriques du « ou » exclusif. J'ai alors montré que mon résultat de décision pouvait s'étendre aux protocoles utilisant le « ou » exclusif en exhibant une extension décidable du fragment de clauses considéré précédemment.

**Vérification pratique des protocoles.** Avec Jon Millen et Harald Rueß, j'ai mis au point la description de leur modèle en PVS et j'ai prouvé, à l'aide de PVS, le secret des protocoles de Needham-Schroder-Lowe et d'Otway-Rees. Ce travail a été le point de départ de la mise au point d'une procédure automatique de preuve du secret pour les protocoles. Cette procédure consiste à décomposer les messages en « morceaux » élémentaires puis à faire une recherche en arrière sur le système de transitions modélisant le protocole. Elle est correcte mais incomplète : la preuve du secret d'un protocole peut échouer même si celui-ci ne comporte pas de faille. Cette procédure a été programmée en *Ocaml* (environ 2000 lignes de code) et apporte une représentation visuelle en cas d'échec de preuve qui permet souvent de reconstituer une véritable attaque. L'outil résultant de l'implémentation de cette procédure se nomme Securify et peut être utilisé en ligne depuis la page web suivante :

<http://www-eva.imag.fr/fournitures1.html>. Il prend en entrée la spécification d'un protocole cryptographique en langage EVA et fait la preuve que le protocole préserve les secrets demandés. Le langage EVA est un langage de spécification commun à plusieurs outils, développé dans le cadre du projet RNTL EVA. En cas d'échec de preuve, l'outil fournit une sortie graphique qui permet d'analyser le protocole et de retrouver des attaques. Il a en particulier permis de vérifier le secret de très nombreux protocoles cryptographiques.

D'autre part, j'ai montré que pour une classe très générale de protocoles cryptographiques et de propriétés de sécurité, il est toujours suffisant de considérer  $b$  agents où  $b$  ne dépend que de la propriété de sécurité : s'il existe une attaque avec  $n$  agents, alors il existe une attaque avec  $b$  agents. En pratique,  $b$  est le plus souvent égal à 2 ou 3. Un tel résultat était souvent utilisé sans justification dans les outils de vérification. J'ai mis en évidence les hypothèses nécessaires à ce résultat. En particulier, le nombre minimal d'agents nécessaire à une attaque dépend de la possibilité d'un agent à se parler à lui-même et du nombre d'agents impliqués explicitement dans la propriété de sécurité étudiée. Un tel résultat permet de limiter l'espace des recherches lors de la recherche d'attaques à l'aide d'outils. Il permet également de restreindre sans perte de généralité la recherche de classes décidables de protocoles.