

# Sujet de stage de recherche / M2

## Titre

Modélisation des clefs de l'intrus

## Encadrants

Hubert Comon-Lundh & Véronique Cortier

*Tél* : 01 47 40 75 47 & 03 83 59 30 55

*Email* : [comon@lsv.ens-cachan.fr](mailto:comon@lsv.ens-cachan.fr) & [cortier@loria.fr](mailto:cortier@loria.fr)

## Description du sujet

Les propriétés de sécurité du chiffrement (qu'il soit symétrique ou asymétrique) sont définies à partir d'une moyenne des succès d'un intrus sur l'espace des clefs. Autrement dit, elles disent que l'intrus a peu de chances de réussir lorsque la clef est tirée en utilisant l'algorithme de génération de clefs, mais ne disent rien d'un éventuel succès de l'attaquant lorsqu'il utilise des clefs qu'il construit d'une autre manière.

Le sujet du stage est de spécifier, dans un modèle symbolique style Dolev-Yao, cette capacité de l'attaquant : en fonction de messages déjà obtenus, il doit pouvoir construire une clefs (sans utiliser l'algorithme de génération de clefs) qui possède des propriétés de son choix. Cette spécification devra être correcte d'un point de vue calculatoire : elle devra être satisfaite typiquement par des schémas de chiffrements réputés IND-CCA.

La deuxième étape du stage est de mettre au point un algorithme de décision de la déductibilité et peut-être de l'existence d'attaque en un nombre borné de sessions dans la ligne de [CLCZ09], pour ce nouvel ensemble de capacités de l'intrus.

Enfin, en perspective, la correction dans le modèle calculatoire devra être étendue au cas d'un attaquant actif, étendant par exemple le résultat de [CLC08]

## Références

- [CLC08] Hubert Comon-Lundh and Véronique Cortier. Computational soundness of observational equivalence. In *Proc. ACM Conf. Computer and Communication Security (CCS)*, <https://hal.inria.fr/inria-00274158>, 2008.

- [CLCZ09] Hubert Comon-Lundh, Véronique Cortier, and Eugen Zlinescu. Deciding security properties of cryptographic protocols. application to key cycles. *Transaction on Computational Logic*, 2009. To appear. A preliminary version is available at <http://arxiv.org/abs/0708.3564>.