Utilisation des tests statistiques : LLR et χ^2 pour la cryptanalyse différentielle

Céline Blondeau

Aalto University, Finlande
celine.blondeau@aalto.fi

La cryptanalyse différentielle a été introduite en 1990 par Biham et Shamir. Cette attaque statistique exploite l'existence de différentielles ayant un comportement non-aléatoire. Celle-ci a été appliquée et généralisée dans le but de retrouver la clé d'un certain nombre de systèmes de chiffrement par blocs. Parmis les généralisations, peu d'études ont été faites dans le cas où l'on veux exploiter les propriétés de plusieurs différentielles avec différentes probabilités.

Parallèlement à la cryptanalyse différentielle, en 1993, Matsui introduit la cryptanalyse linéaire. En 2004, Biryukov *et al.* proposent une première généralisation de celle-ci exploitant l'information venant de plusieurs approximations linéaires. Quelques années plus tard, Cho, Hermelin et Nyberg introduisent la cryptanalyse linéaire multidimentionelle, étudient la complexité des tests LLR et χ^2 et l'appliquent à un certain nombre de systèmes de chiffrement.

En 2011, avec Gérard [2], nous avons étudié une généralisation de la cryptanalyse différentielle qui permet de distinguer les clés en utilisant une statistique simple qui regroupe l'information de toutes les différentielles collectées en un seul compteur sans tenir compte des variations entre les probabilités de ces différentielles.

Plus récemment [1], nous avons étudié différentes possibilités pour pouvoir appliquer les tests statistiques : LLR et χ^2 au contexte de la cryptanalyse différentielle. Ainsi nous avons étudié (en comparant la théorie à une batterie d'expérimentation) différents scenarios d'attaques. Dans la pratique l'obtention d'une bonne estimation des probabilités des différentielles reste encore un problème ouvert pour un certain nombre de système de chiffrement. Les attaques utilisant le test LLR ne fonctionnent alors que dans ce cas (bonne estimation des probabilités) et sont alors plus performantes (meilleure complexité en temps et en données) que celles utilisant le test χ^2. Dans le cas contraire une sous estimation des probabilités des différentielles nous donne une sous estimation de la complexité des attaques utilisant le test χ^2.

Dans le même temps, nous avons aussi étudié la différence entre des attaques qui utilisent un ensemble de différentielle et celles qui utilisent des différentielles tronquées. Ce second type d'attaque comporte alors un certain nombre d'avantages. Par exemple, le fait que toutes les différences en sortie peuvent être prises en compte dans l'analyse (par le biais de projections sur des sous ensembles) peut suivant les cas nous donner plus d'information et peut ainsi nous permettre de récupérer la clé avec une complexité en donnée moindre. Néanmoins, notamment par le fait que la complexité en mémoire de celle-ci est beaucoup plus importante que la précédante, suivant les contraintes imposées, le premier type d'attaque utilisant des différentielles simples peux rester d'une grande utilité.

Références

[1] Blondeau, C.,Gérard, B., Nyberg, K. : Multiple Differential Cryptanalysis using LLR and χ^2 Statistics In Visconti, I., ed. : *Conference on Security and Cryptography for Networks, SCN 2012.* Volume 7485 of *LNCS.*, Springer (2012)

[2] Blondeau, C., Gérard, B. : Multiple Differential Cryptanalysis : Theory and Practice. In Joux, A., ed. : *Fast Software Encryption - FSE 2011.* Volume 6733 of *LNCS.*, Springer (2011) 35 – 54