Cryptanalyse du schéma de chiffrement par bloc AES
Thématique : Sécurité/cryptologie

Laboratoire : IRISA
Ville : Rennes
Équipe : Inria Cidre
Directeur de stage : Pierre-Alain Fouque, `Pierre-Alain.Fouque@ens.fr`
Directeur du laboratoire : Jean-Marc Jézéquel

Présentation générale du domaine

La cryptanalyse de primitives symétriques par bloc est un domaine actuellement très actif. Pendant plus d'une dizaine d'année, aucune attaque n'a été rapportée contre l'AES et depuis 3 ans, de nouvelles attaques [4, 3] utilisant soient un modèle très fort (related-key model) ou des variantes d'attaque par le milieu sont apparues [5]. Ces dernières attaques permettent d'attaquer tous les tours de l'AES utilisant 128 bits de clé et ont été publiées à la conférence Asiacrypt 2011.

Objectifs du stage

L'inconvénient principal des dernières attaques est qu'elles demandent une quantité de données et de temps tellement grande que personne ne peut les mettre en oeuvre. Par conséquent, il existe dans la littérature, de nombreuses attaques dont personne ne sait si elles fonctionnent réellement ou non. Un objectif du stage est de bien comprendre comment fonctionnent ces attaques contre AES et de proposer une méthode pour vérifier si les principes de l'attaque fonctionnent en pratique. Plusieurs pistes peuvent être envisagées : la première consiste à réduire le nombre de tours et à adapter l'attaque pour que sa complexité soit raisonnable en pratique (cela a été fait dans [2] par exemple pour les attaques dans le modèle fort). La seconde idée est que ces attaques se décomposent en une partie recherche exhaustive et une autre partie et donc, si on suppose qu'on connaît une partie de la clé, est-ce que le reste de l'attaque fonctionne comme c'est indiqué dans l'article. Enfin, il est possible dans le cas de l'AES de définir une version sur 48 bits au lieu de 128 bits et de tester l'attaque dans ce cas. Si le temps le permet, on pourra aussi étudier si ces attaques peuvent s'appliquer à d'autres primitives de schémas de chiffrement ou d'autres schémas utilisant AES comme les schémas de MAC (Pelican-MAC [6]) ou le stream-cipher LEX [1].

Compétences espérées

Il est souhaitable que l'étudiant ait suivi un cours de cryptographie (mais de bonne compétence en algorithmique suffisent) et sache programmer en C par exemple.

Références

[1] Biryukov, A. : Design of a new stream cipher-lex. In Robshaw, M.J.B., Billet, O., eds. : The eSTREAM Finalists. Volume 4986 of Lecture Notes in Computer Science. Springer (2008) 48–56

[2] Biryukov, A., Dunkelman, O., Keller, N., Khovratovich, D., Shamir, A. : Key recovery attacks of practical complexity on aes-256 variants with up to 10 rounds. In Gilbert, H., ed. : EUROCRYPT. Volume 6110 of Lecture Notes in Computer Science., Springer (2010) 299–319

[3] Biryukov, A., Khovratovich, D. : Related-key cryptanalysis of the full aes-192 and aes-256. In Matsui, M., ed. : ASIACRYPT. Volume 5912 of Lecture Notes in Computer Science., Springer (2009) 1–18

[4] Biryukov, A., Khovratovich, D., Nikolic, I. : Distinguisher and related-key attack on the full aes-256. In Halevi, S., ed. : CRYPTO. Volume 5677 of Lecture Notes in Computer Science., Springer (2009) 231–249

[5] Bogdanov, A., Khovratovich, D., Rechberger, C. : Biclique cryptanalysis of the full aes. IACR Cryptology ePrint Archive **2011** (2011) 449

[6] Dunkelman, O., Keller, N., Shamir, A. : Alred blues : New attacks on aes-based mac's. IACR Cryptology ePrint Archive **2011** (2011) 95