Cryptanalyse de PRESENT avec peu de données

María Naya-Plasencia (PRISM, UVSQ), Bastien Vayssière (PRISM, UVSQ)

13 juillet 2012

PRESENT est un chiffrement par blocs ultra-léger proposé en 2007 par Bogdanov et al. Une série de cryptanalyses ont fourni des résultats sur ce chiffrement. Elles nécessitent un grand nombre de clairs/chiffrés, proche de la totalité des paires. Les travaux de Bouillaguet et al. sur un petit nombre de tours d'AES et une petite quantité de paires, présentés à Crypto 2011, nous ont alors amené à nous poser la question : pour PRESENT, à partir d'une seule paire, jusqu'à combien de tours peut-on retrouver la clé plus rapidement que la recherche exhaustive ? Dans ce contexte, c'est la méthode d'attaque meet-in-the-middle qui paraît pertinente.

Pour PRESENT 80-bit, nous présentons une attaque sur 6 tours, utilisant cette méthode, et une attaque sur 7 tours, où l'on gagne un tour en utilisant un crible sur les transitions possibles par les SBoxes au lieu d'une recherche de collision partielle au milieu.

Pour ces deux attaques, nous avons réalisé une implémentation simplifiée qui suppose 48 bits de clés connus et retrouve les 32 bits de clé restant, plus rapidement que leur recherche exhaustive. Les complexités obtenues ont confirmé nos résultats théoriques.

Pour PRESENT 128-bit, nous décrivons une attaque sur 9 tours par une méthode similaire à celle utilisée pour 7 tours de PRESENT 80-bit.

Nous avons calculé la borne supérieure sur le nombre de tours qui pourraient être attaqués avec nos méthodes. Cette analyse nous donne un maximum de 7 tours attaquables à partir d'une paire pour PRESENT 80-bit, et un maximum de 9 tours attaquables pour PRESENT 128-bit,ce qui correspond à nos attaques.

Nous présentons ainsi la première cryptanalyse de PRESENT pour un petit nombre de clairs/chiffrés, et les limites de cette cryptanalyse, en l'illustrant avec trois attaques dont deux ont été testées avec des implémentations simplifiées.