



LE SCHÉMA D'EVEN-MANSOUR PARAMÉTRABLE : PREUVES DE SÉCURITÉ À L'AIDE DE LA TECHNIQUE DES COEFFICIENTS H PAR BENOÎT-MICHEL COGLIATI

Présentée par : Benoît-Michel Cogliati Discipline : informatique Laboratoire : LMV

Résumé :
Les algorithmes de chiffrement par blocs paramétrables constituent une généralisation des algorithmes de chiffrement par blocs classiques qui, en plus d'une clé et d'un message à chiffrer ou déchiffrer, admettent un paramètre additionnel, nommé tweak en anglais. Le rôle de ce paramètre additionnel est d'apporter une variabilité à l'algorithme de chiffrement, sans qu'il soit nécessaire de changer la clé ou de garder le tweak secret. Ce dernier doit également pouvoir être contrôlé par l'adversaire sans dégradation de la sécurité. Dans cette thèse nous nous intéressons à une classe particulière d'algorithmes de chiffrement par blocs, les algorithmes de chiffrement par blocs à clé alternée. Plus précisément, nous étudions la sécurité du schéma d'Even-Mansour, qui constitue une abstraction de la structure de ces algorithmes dans le modèle de la permutation aléatoire, et cherchons à rendre ce schéma paramétrable tout en conservant de fortes garanties de sécurité. À cette fin, nous introduisons une nouvelle construction générique,

baptisée
TEM, qui remplace les clés de tours de la construction d'Even-Mansour par une valeur qui dépend de la clé et du tweak, et en étudions la sécurité dans deux cas : lorsque le mixage de la clé et du tweak est linéaire ou lorsqu'il est très non-linéaire. Nos preuves de sécurité utilisent la technique des coefficients H, introduite par Jacques Patarin dans sa thèse de doctorat, qui permet de transformer des problèmes cryptographiques en problèmes combinatoires sur des groupes finis.

Abstract :
Tweakable block ciphers are a generalization of classical block ciphers which, in addition to a key and a plaintext or a ciphertext, take an additionnal parameter called a tweak. The goal of this new parameter is to bring variability to the block cipher without needing to change the key or to keep the tweak secret. The tweak should also be adversarially controllable without sacrificing security. In this thesis we study a particular class of block ciphers, namely key-alternating ciphers. More precisely, we study the security of the Even-Mansour scheme, which is an abstraction of these ciphers in the random permutation model, and seek to bring tweakability to this scheme while keeping strong security guarantees. To this end, we introduce a new generic construction, dubbed TEM, which replaces the round keys from the Even-Mansour construction by a value depending on both the key and the tweak, and study its security in two cases: when the tweak and key mixing is linear or highly non-linear. Our security proofs rely on the H-coefficients technique, a technique introduced by Jacques Patarin in his PhD thesis which transforms cryptographic problems into combinatorial problems in finite groups.

INFORMATIONS COMPLÉMENTAIRES

M. Jacques PATARIN, Professeur des Universités, Université de Versailles-Saint-Quentin-en-Yvelines - Laboratoire LMV - Directeur de these
M. Pierre-Alain FOUQUE, Professeur des Universités, Université de Rennes I - Rapporteur
M. David NACCACHE, Professeur, ENS Paris - Rapporteur
M. Jean-Sébastien CORON, Professeur assistant, Université de Luxembourg - Examinateur
M. Louis GOUBIN, Professeur des Universités, Université de Versailles Saint-Quentin-en-Yvelines - Laboratoire LMV - Examinateur
Mme Aline GOUGET, Ingénieur de recherche, Gemalto - Examinateur
Mme Valérie NACHEF, Maître de conférences, Université de Cergy-Pontoise -

Examinateur

M. Yannick SEURIN, Ingénieur de recherche, ANSSI - Examinateur

Contact : dredval service FED : theses@uvsq.fr