UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES

PREUVES DE SÉCURITÉ EN CRYPTOGRAPHIE SYMÉTRIQUE À L'AIDE DE LA TECHNIQUE DU COUPLING PAR RODOLPHE LAMPE

Présentée par : Rodolphe Lampe Discipline : informatique Laboratoire : PRISM

Résumé :
Dans cette thèse, on s'intéresse à des schémas de chiffrement par blocs, c'est-à-dire que le chiffrement (et le déchiffrement) envoie un bloc de n bits sur un bloc de n bits. Il y a essentiellement deux grandes structures utilisées pour un schéma de chiffrement par blocs : la structure de Feistel (utilisée pour le DES) et la structure SPN (utilisée pour l'AES). L'étude de la sécurité de ces différents structures et schémas a permis de nombreuses avancées autant pratiques que théoriques. Nous présentons dans cette thèse des preuves de sécurité pour le schéma d'Even-Mansour itéré, le schéma paramétrable CLRW et le schéma de Feistel à clés alternées. Ces preuves utilisent une technique probabiliste, appelée coupling, introduite en cryptographie en 2002 par Mironov. Nous présentons cette technique dans le cadre des probabilités, puis la façon d'utiliser le coupling pour prouver la sécurité des schémas cités précédemment. Nous présentons également une étude de la sécurité du schéma d'Even-Mansour à deux tours pour certaines minimisations (même clés de tours ou même permutations internes par exemple) et, pour conclure, une comparaison des différentes techniques d'indistinguabilité.

soutenance de thèse

Abstract :
In this thesis, we study blockciphers, meaning that the encryption (and decryption) sends a block of n bits on a block of n bits. There is essentially two main structures used for a blockcipher: the Feistel structure (used for DES) and the SPN structure (used for AES). The study of the security of these structures and schemes has led to many practical and theoretical advances. We present in this thesis proofs of security for the iterated Even-Mansour scheme, the tweakable blockcipher CLRW and the key-alternating Feistel cipher. These proofs use a probabilistic technique, called coupling, introduced in cryptography in 2002 by Mironov. We present this technique in the context of probabilities, then we present how to use the coupling to prove the security for the schemes mentioned above. We also present an analysis of the security of the Even-Mansour cipher with two rounds and some properties (same round keys or same internal permutations for example) and, finally, we compare the different techniques to prove indistinguishability.

Membres du jury :

Jean-Sébastien CORON, Maître de Conférences, Habilité à Diriger des Recherches, à l'Université du Luxembourg/Département Informatique - Luxembourg (Grand-Duché de Luxembourg) - Rapporteur
David NACCACHE, Professeur des Universités, à l'ENS/Département d'Informatique - Paris - Rapporteur
Jacques PATARIN, Professeur des Universités, à l'Université de Versailles Saint-Quentin-en-Yvelines/Laboratoire Parallélisme Réseaux Systèmes Modélisation (PRISM) - Versailles - Directeur de thèse
Louis GOUBIN, Professeur des Universités, à l'Université de Versailles Saint-Quentin-en-Yvelines/Laboratoire Parallélisme Réseaux Systèmes Modélisation (PRISM) - Versailles - Examinateur
Antoine JOUX, Professeur Associé, à l'Université Pierre et Marie Curie/Laboratoire d'Informatique de Paris 6 (LIP6) - Paris - Examinateur
David POINTCHEVAL, Directeur de Recherche, au CNRS/Département d'Informatique de l'ENS - Paris - Examinateur
Yannick SEURIN, Chercheur, à l'ANSSI - Saulx-les-Chartreux - Examinateur

Dernière mise à jour de cette page : 27 novembre 2014