UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES

"CRYPTANALYSE LINÉAIRE ET CONCEPTION DE PROTOCOLES D'AUTHENTIFICATION À SÉCURITÉ PROUVÉE" PAR JONATHAN ETROG

Présentée par : Monsieur Jonathan ETROG Discipline : Informatique Laboratoire : PRISM

soutenance de thèse

Cette thèse, restreinte au cadre de la cryptologie symétrique, s'intéresse à deux aspects séparés de la cryptologie : la protection des messages à l'aide d'algorithmes chiffrement et la protection de la vie privée à travers des protocoles d'authentification. La première partie concerne l'étude de la cryptanalyse linéaire et la seconde la conception de protocoles d'authentification à sécurité prouvée garantissant une forme forte d'intraçabilité.
Dans la première partie, nous nous intéressons à la cryptanalyse linéaire qui bien qu'introduite au début des années 90 a connu récemment un nouvel essor dû au développement de nouvelles variantes. Nous nous sommes à la fois intéressés à son aspect pratique et théorique. Dans un premier temps, nous présentons une cryptanalyse d'une version réduite de SMS4, algorithme utilisé dans le chiffrement du WiFi chinois puis nous introduisons la cryptanalyse multilinéaire et décrivons une nouvelle forme de cryptanalyse multilinéaire.
La deuxième partie concerne l'étude de protocoles d'authentification RFID respectant la vie privée. Nous définissons un modèle d'attaquant permettant de formaliser les notions de sécurité relatives à ces protocoles. Nous proposons ensuite deux protocoles réalisant chacun un compromis entre l'intraçabilité forte et la résistance aux attaques par déni de service et admettant des implantations à bas coût et établissons des preuves de sécurité dans le modèle standard pour ces deux protocoles.

Abstract :
This Ph.D, devoted to symmetric cryptography, addresses two separate aspects of cryptology. First, the protection of messages using encryption algorithms and, second, the protection of privacy through authentication protocols. The first part concerns the study of linear cryptanalysis while the second is devoted to the design of authentication protocols with proven security.
Although introduced in the early 90s, linear cryptanalysis has recently experienced a revival due to the development of new variants. We are both interested in its practical and theoretical aspects. First, we present a cryptanalysis of a reduced version of SMS4, the encryption algorithm used in WiFi in China then, second, we introduce multilinear cryptanalysis and describe a new form of multilinear cryptanalysis.
The second part of the thesis concerns the study of RFID authentication protocols respecting privacy. We define a model to formalize the notions of security for these protocols. Then we propose two protocols, each one performing a compromise between strong unlinkability and resistance to denial of service attacks, which allow low-cost implementations. We establish security proofs in the standard model for these two protocols.

Membres du jury :

Gildas AVOINE, Professeur, à l'Université Catholique de Louvain - Louvain-La-Neuve (Belgique) - Rapporteur
Anne CANTEAUT, Directeur de Recherche, à l'INRIA Rocquencourt - Le Chesnay - Rapporteur
Jacques PATARIN, Professeur des Universités, à l'Université de Versailles Saint-Quentin-en-Yvelines/Laboratoire Parallélisme, Réseaux, Système, Modélisation (PRISM) - Versailles - Directeur de thèse
Carlos CID, Directeur de Recherche, à l'Université de Londres Royal Holloway - Londres (Angleterre)- Examinateur
Henri GILBERT, Directeur de Recherche, à Orange Labs Division Recherche et Développement - Issy-les-Moulineaux - Examinateur
Vincent RIJMEN, Directeur de Recherche, à l'Université Catholique de Leuven/Laboratoire COSIC - Heverlee (Belgique) - Examinateur
Matt ROBSHAW, Directeur de Recherche, à Orange Labs Division Recherche et Développement - Issy-les-Moulineaux - Examinateur

Changer mon statut sur twitter
Partager sur 'Facebook
Partager sur 'Digg'
Partager sur 'LinkedIn'
Partager sur 'Viadeo'
Partager cette actualité sur :

Dernière mise à jour de cette page : 18 février 2013