CRYPTANALYSE PAR CANAUX AUXILIAIRES

le 1 avril 2008 de 10h15 à 12h00

ENS Rennes Amphithéâtre
Plan d'accès

Intervention de Pierre-Alain Fouque, maître de conférences à l'ENS Ulm. Séminaire du département Informatique et télécommunications.

Ces dernières années, de nouvelles attaques très efficaces ont été mises au point contre certaines implémentations de systèmes cryptographiques fonctionnant sur une carte à puce ou dans un processeur embarqué.

Après une introduction à la cryptographie et à la cryptanalyse par canaux auxiliaires, je détaillerai certaines attaques contre les systèmes de chiffrement RSA et DES. Ces attaques montrent qu'il ne suffit pas d'utiliser un algorithme très sûr pour avoir un système sûr. Enfin, ces attaques sont très efficaces car elles permettent de retrouver très rapidement des clés secrètes contrairement à beaucoup d'attaques académiques qui ne mettent pas réellement en danger les applications.

THÉMATIQUE(S)

Formation, Recherche - Valorisation

CONTACT

Claude Jard

Mise à jour le 12 septembre 2019

CONTACT

Raphaël Truffet

ARCHIVES