



# 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

Séminaires 2020-2021  
Séminaires 2019-2020  
Séminaires 2018-2019  
Séminaires 2017-2018  
Séminaires 2016-2017  
Séminaires 2015-2016  
Séminaires 2014-2015  
Séminaires 2013-2014  
Séminaires 2012-2013  
Séminaires 2011-2012  
Séminaires 2010-2011  
Séminaires 2009-2010  
Séminaires 2008-2009  
Séminaires 2007-2008  
Séminaires 2006-2007  
Séminaires 2005-2006  
Séminaires 2004-2005  
Séminaires 2003-2004  
Séminaires 2002-2003