INTRODUCTION À LA CRYPTOGRAPHIE REPOSANT SUR LES RÉSEAUX EUCLIDIENS

le 26 janvier 2016 16h00

ENS Rennes, Salle du conseil
Plan d'accès

Intervention de Adeline Langlois (CNRS, IRISA, Rennes)
Séminaire du département Informatique et télécommunications.

La cryptographie reposant sur les réseaux Euclidiens est née dans les années 1990 avec les travaux d'Ajtai. Elle connaît aujourd'hui un essor rapide. Ses attraits sont sa simplicité et son efficacité potentielle, son apparente résistance aux attaques quantiques, et surtout ses preuves de sécurité sous des hypothèses très précises de difficulté algorithmique de problèmes assez bien compris. En effet, la plupart des constructions cryptographiques reposant sur les réseaux sont prouvées sûres sous l'hypothèse que certains problèmes algorithmiques portant sur les réseaux sont difficile à résoudre dans le pire des cas. Dans cet exposé, nous introduirons cette branche récente de la cryptographie. Nous définirons en particulier le problème "Learning With Errors" (LWE), et nous verrons un aperçu des constructions dont la sécurité repose sur ce problème.

THÉMATIQUE(S)

Formation, Recherche - Valorisation

CONTACT

David Cachera & François Schwarzentruber

Mise à jour le 9 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