



LA VÉRIFICATION FORMELLE APPLIQUÉE AUX PROTOCOLES CRYPTOGRAPHIQUES

le 27 septembre 2016 15h30 - 17h00

ENS Rennes, Salle du conseil
[Plan d'accès](#)

Dans le cadre d'un séminaire du département Informatique et télécommunications : Intervention de Stéphanie Delaune, directrice de recherche (DR) CNRS à l'IRISA, membre de l'équipe EMSEC qui s'intéresse à la sécurité et la cryptographie embarquées.



Cet exposé présentera la problématique de la sécurité des protocoles cryptographiques et l'application à ce domaine des techniques de logique mathématique et de vérification automatique / assistée.

Résumé

Les protocoles cryptographiques sont les algorithmes et programmes qui permettent d'établir une communication sécurisée. Ils sont fragiles et sont le principal point d'entrée pour les attaques de sécurité, comme le montreront quelques exemples. Ils sont aussi très difficiles à analyser. La preuve formelle est de plus en plus vue comme le meilleur moyen (voire le seul) d'assurer le bon fonctionnement de ces protocoles. Elle demande souvent la mise en œuvre de techniques très élaborées.

<https://www.irisa.fr/fr/equipes/emsec>

THÉMATIQUE(S)

Formation, Recherche - Valorisation

CONTACT

[David Cachera & François Schwarzentruber](#)

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](#)