LA CRYPTOGRAPHIE DES COURBES ELLIPTIQUES

le 27 novembre 2018 de 15h30 à 16h30

ENS Rennes Amphithéâtre

Conférence de Reynald Lercier (Rennes 1) dans le cadre des conférences d'initiation à la recherche du département Mathématiques.

Résumé : La difficulté supposée du logarithme discret défini par des courbes elliptiques, ou ses variantes les hypothèses Diffie-Hellman calculatoires ou décisionnelles, ont inspiré de nombreux schémas cryptographiques depuis maintenant une trentaine d'année. Des résultats de Shoup, d'abord en 1997 sur la difficulté prouvée de ces problèmes lorsque considérés en toute généricité, ensuite en 1998 sur l'existence de schémas de chiffrement asymétriques efficaces et prouvés sûrs face à des attaquants adaptatifs, ont permis, parmi d'autres, d'apporter une assise théorique remarquable à cette cryptographie. Dans cet exposé, nous en rappelons les grandes étapes, de la naissance jusqu'à, en phase avec les préoccupations du moment, l'avènement des schémas résistant à l'informatique quantique.

Page web de Reynald Lercier

THÉMATIQUE(S)

Formation, Recherche - Valorisation

Mise à jour le 12 novembre 2018

À LIRE AUSSI

Et si on mélangeait des équations différentielles avec un peu de probas ?

Quelques équations des biomathématiques

Parcimonie et problèmes inverses

DOCUMENTATION

Vous souhaitez recevoir plus d'information sur l'ENS Rennes, vous pouvez pour cela remplir le formulaire de demande de documentation.

CONFÉRENCES D'INITIATION À LA RECHERCHE

Ces conférences, organisées à destination des élèves de première et deuxième années, sont ouvertes à tous. Elles sont l'occasion de découvrir la recherche contemporaine en mathématiques au travers de questions actuelles exposées par des chercheurs reconnus.

Programme complet des conférences d'initiation à la recherche