Cryptographie appliquée à base de courbes elliptiques

Bruno Martin
Bruno.Martin@unice.fr

17 février 2015

Nombre d'étudiants souhaités : 1-2

Description du sujet

Les outils récents de sécurité des réseaux utilisent de plus en plus de cryptographie à base de courbes elliptiques. Que ce soit pour engendrer des suites pseudo-aléatoires, pour des protocoles de mise en accord de clé à la Diffie-Hellman ou pour réaliser des signatures numériques. D'un point de vue pratique, on se concentrera sur deux aspects de la cryptographie à base de courbes elliptiques :

— la génération de suites pseudo-aléatoires ;
— l'utilisation de ces courbes par `ssh`.

Dans un premier temps, il s'agira de comprendre les bases (informatiques) de l'utilisation des courbes elliptiques en cryptographie.

Pour le premier point, on tentera de comprendre l'article *The Mathematics Community and the NSA* de M. Wertheimer, Notices of the AMS, 2015 qui porte sur une polémique récente autour d'une brèche connue dans un générateur de suites pseudo-aléatoires.

Pour le second, on cherchera à expliquer la raison pour laquelle les versions récentes de `ssh` utilisent deux standards distincts (et deux implémentations) basés sur de la cryptographie à base de courbes elliptiques : ECDSA et ED25519.

Lieu

Département d'informatique, Université Nice Sophia Antipolis

Prérequis

Connaissances en algèbre, intérêt pour la cryptographie appliquée.

Informations complémentaires