Texte : Sebastián Escalón. Photo : © CNRS DR7 - Vanessa Cusimano

Damien Stehlé

Chercheur en informatique

Vers une cryptographie invulnérable

« Mon travail consiste à concevoir des algorithmes, des méthodes permettant de faire certains calculs le plus vite possible. » Plus précisément, Damien Stehlé travaille sur les réseaux euclidiens, c'est-à-dire des arrangements réguliers de points dans l'espace. La disposition des atomes dans un cristal, ou tout simplement un carrelage, en sont des exemples. Les algorithmes que développe ce jeune chercheur permettent de trouver rapidement une représentation mathématique simple et exploitable des réseaux. Ces travaux ont de nombreuses applications dans des domaines tels que les télécommunications, l'arithmétique des ordinateurs, mais aussi en cryptographie, le domaine de spécialité de ce scientifique. Après un doctorat à l'université Nancy 1, Damien Stehlé entre au CNRS en 2006, au Laboratoire de l'informatique du parallélisme. C'est là qu'il développe ses idées et combine des méthodes venues de plusieurs branches des mathématiques — algèbre, théorie des nombres, arithmétique flottante — pour étudier et développer des systèmes de cryptographie à base de réseaux. Potentiellement, ceux-ci pourraient devenir les plus sûrs jamais conçus. « On a coutume de dire que cette cryptographie résisterait même à l'ordinateur quantique. » Damien Stehlé est aujourd'hui professeur à l'ENS de Lyon.

Laboratoire de l'informatique du parallélisme (LIP), CNRS / ENS de Lyon / Université Claude Bernard Lyon 1 / Inria, Lyon
www.ens-lyon.fr/LIP