Colloquium d'Informatique
de Sorbonne Université

Cryptographie reposant sur les réseaux : sécurité quantique et au-delà

Damien Stehlé

CryptoLab

Amphi 43

4, place Jussieu
75005 Paris
Métro Jussieu

20 Juin 2023
à 18h00

Un ordinateur quantique de grande taille sera capable de casser efficacement une très grande proportion des protocoles cryptographiques qui garantissent aujourd'hui la confidentialité et la sécurité des données. La cryptographie post-quantique vise à obtenir des constructions alternatives qui sont sûres face à des adversaires quantiques, tout en ne requérant que des calculs classiques de la part des utilisateurs honnêtes. Dans la présentation, je me concentrerai sur les cryptosystèmes reposant sur les réseaux euclidiens, qui fournissent l'approche la plus aboutie en cryptographie post-quantique. Je présenterai également un des sujets les plus actifs. en cryptographie reposant sur les réseaux, à savoir le chiffrement homomorphe.

Damien Stehlé est le directeur scientifique de CryptoLab, une startup travaillant sur le chiffrement homomorphe. Il a obtenu son doctorat à l'Université Nancy 1 en 2005. Il a ensuite été chargé de recherche au CNRS, puis professeur au département d'informatique de l'ENS de Lyon de 2012 à 2023. Il étudie les aspects algorithmiques des réseaux euclidiens et leurs applications en cryptographie. Il est co-auteur du protocole de chiffrement Kyber et du protocole de signature Dilithium, qui ont été sélectionnés par le NIST (Institut américain des normes et de la technologie) comme futurs standards de la cryptographie post-quantique.

contact : colloquium@lip6.fr

https://www.lip6.fr/colloquium/
Vidéo disponible sur le site

cnrs

LIP6

SCIENCES SORBONNE UNIVERSITÉ