Chiffrement totalement homomorphe

Antoine Joux, prix Gödel, Chaire de Crypto, Sorbonne Université
Invité

Abstract:

Dans cet exposé, nous expliquerons les principes du chiffrement homomorphe et montrerons comment il est possible de réaliser cette fonctionnalité d'apparence inaccessible.
Puis, nous examinerons la mise en pratique de la méthode qui malgré d'énormes progrès, reste extrêmement couteuse pour l'essentiel des applications.