

Antoine Joux lauréat du Prix Gödel

Écrit par Administrator

Lundi, 03 Juin 2013 12:02 - Mis à jour Lundi, 03 Juin 2013 12:16

Le prix Gödel 2013 créé par l'European Association for Theoretical Computer Science (EATCS) et le Pôle Algorithmique et Informatique théorique de l'ACM (SIGACT) de l'Association for Computing Machinery (ACM) a été attribué aux trois chercheurs en cryptographie : Dan Boneh, Matt Franklin et Antoine Joux. Ces chercheurs ont réalisé des travaux remarquables sur les couplages sur les courbes elliptiques à usage de la cryptographie. Antoine Joux est un cryptographe français chercheur au sein du laboratoire PRISM. Il a par ailleurs réalisés de nombreux travaux dans d'autres domaines de la cryptographie, notamment sur les attaques des fonctions de hachage, sur les attaques du logarithme discret sur les corps finis etc.