



Versailles, le 30 mai 2013

Antoine Joux reçoit le prix Gödel pour son modèle en cryptographie

Chercheur au sein de l'équipe cryptographie du laboratoire PRISM, Parallélisme, réseaux, systèmes, modélisation (UVSQ/CNRS), Antoine Joux a élaboré un système de calcul innovant dans le domaine de la cryptographie basé sur le couplage. Le 3 juin 2013, il recevra avec deux autres scientifiques américains le prix Gödel, qui récompense des travaux remarquables d'informatique théorique, lors de l'ACM Symposium on the Theory of Computing, à Palo-Alto (Californie).



La cryptographie est un domaine à l'interface entre mathématiques et informatique, qui vise à élaborer les méthodes et les outils qui sous-tendent la sécurisation des données et des transactions sur Internet. Ce domaine se divise en deux sous-domaines : le premier cherche à créer des dispositifs adéquats, tandis que le second cherche à "casser" les dispositifs proposés par d'autres, en montrant qu'ils ne sont pas "sûrs".

En 2000, Antoine Joux a eu l'idée de détourner le couplage, qui était jusque là un outil réservé au domaine des mathématiques pures, pour en faire un nouvel outil de la cryptographie, devenu depuis incontournable dans chacun des deux sous-domaines de la cryptographie. L'irruption du couplage en cryptographie a permis d'y développer de nouvelles fonctionnalités, qui étaient impossibles à réaliser auparavant. Un exemple frappant de l'importance de ce nouvel outil est son utilisation contre le piratage des contenus multimédia. « *Le même signal chiffré est envoyé à tout le monde, mais chaque décodeur le déchiffre de manière différente. En observant comment le décodeur a déchiffré la vidéo envoyée, on peut déterminer à qui il appartient* » explique Antoine Joux. Ce procédé permet ainsi de retrouver, parmi les abonnés à une chaîne cryptée, celui qui a revendu illégalement ses vidéos à d'autres utilisateurs.

Le Prix Gödel

Nommé en l'honneur du logicien Kurt Gödel, le prix Gödel a été créé en 1992 par l'European Association for Theoretical Computer Science (EATCS) et le Pôle Algorithmique et Informatique théorique (SIGACT) de l'Association for Computing Machinery (ACM) pour honorer des travaux remarquables en informatique théorique.

Cette année, le prix Gödel est décerné à trois scientifiques : Antoine Joux pour son article « *A One Round Protocol for Tripartite Diffie-Hellman* » qui présente sa méthode fondée sur le couplage; Dan Boneh et Matt Franklin, deux chercheurs américains qui l'ont appliquée pour résoudre d'autres problèmes centraux en cryptographie.

Professeur associé au laboratoire PRISM (UVSQ/CNRS) depuis 2004, Antoine Joux est le deuxième chercheur français à remporter le prix Gödel, après Géraud Sénizergues en 2002.

CONTACT

Jennifer Mayeur – Responsable des relations presse
T : 01 39 25 78 70 — M : 06 60 09 17 50
jennifer.mayeur@uvsq.fr