ANTOINE JOUX REÇOIT LE PRIX GÖDEL POUR "UNE JOLIE IDÉE" EN CRYPTOGRAPHIE

En 2000, Antoine Joux a eu « une très jolie idée ». Il a inventé un système de calcul qui ouvre de nouvelles perspectives à la cryptographie.

La cryptographie, c'est l'élaboration de codes mathématiques nécessaires à tous les cryptages de nos transactions sur Internet et à la sécurisation de nos données. Le 3 juin 2013, cet article de 2000 vaut au chercheur du laboratoire Prism (UVSQ) le prix Gödel, qu'il va recevoir à Palo Alto, en Californie.

Le monde de la cryptographie se divise en deux catégories : ceux qui ont un message crypté à faire passer en toute sécurité, les cryptographes ; et ceux qui s'acharnent à le déchiffrer : les cryptanalystes. La « jolie idée » d'Antoine Joux, chercheur au Prism, est d'avoir utilisé de manière constructive (c'est-à-dire pour fabriquer un système de chiffrement) un outil mathématique, nommé couplage, qu'on utilisait jusque-là en cryptanalyse (pour casser des codes existants). Cette année, le prix Gödel récompense conjointement deux articles: celui où Antoine Joux présente son idée et celui de Dan Boneh et Matt Franklin, deux Américains qui l'ont utilisée pour résoudre un problème qui persistait depuis 1984.

Depuis cette date, l'outil du couplage a servi à élaborer beaucoup de choses, dont des méthodes anti-piratage pour les contenus multimédia : ce qu'on appelle le « traçage de traîtres » en anglais, soit une manière de retrouver qui, parmi les abonnés à une chaîne cryptée, a revendu illégalement ses vidéos à d'autres utilisateurs. « Le même signal chiffré est envoyé à tout le monde, mais chaque décodeur le déchiffre de manière différente. En voyant comment le décodeur a déchiffré la vidéo envoyée, on sait à qui il

appartient » explique Antoine Joux.

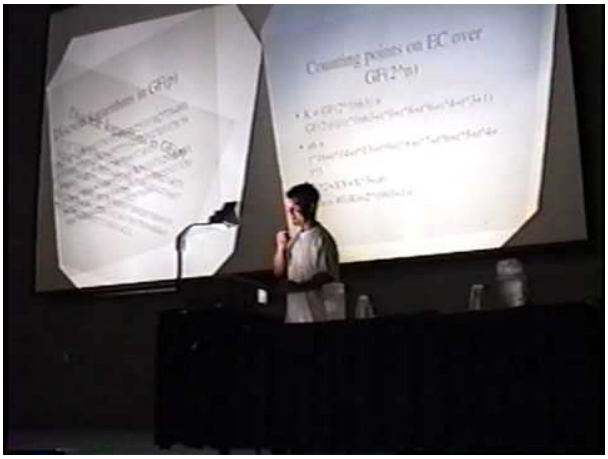
« Une nouvelle branche de la cryptographie »

« Dès 2000, nous avions senti qu'Antoine avait eu une idée brillante », remarque son collègue Louis Goubin, professeur d'informatique et responsable du master Secrets. «Mais il a fallu treize ans pour confirmer que citation après citation, colloque après colloque, son idée a donné naissance à une nouvelle branche de la cryptographie. » Chaque année depuis 1993, deux associations récompensent un ou plusieurs article(s) majeur(s) avec le prix Gödel : l'Association européenne pour l'informatique théorique (EATCS en anglais) et le Pôle algorithmique et informatique théorique de l'Association pour la machinerie informatique (ACM-Sigact).

Au moment où il a publié cet article, Antoine Joux dirigeait la branche scientifique de la Direction centrale de la sécurité des systèmes d'informations, sous le contrôle direct du Premier ministre. Professeur associé au laboratoire Prism (UVSQ) depuis 2004, ce polytechnicien est le deuxième chercheur français à remporter le prix Gödel, après Géraud Sénizergues en 2002.

Course au record de calcul

En 2013, Antoine Joux a découvert un nouvel algorithme de calcul qui montre, en particulier, que certaines façons de faire des couplages ne sont pas sûres. « On pourrait avoir l'impression qu'il remet en cause son propre travail, mais il faut plutôt considérer ces recherches comme les crash-test ou les tests de soufflerie qu'on fait subir aux nouvelles voitures », explique Louis Goubin. Ces tests permettent de détecter les utilisations des couplages trop faciles à décrypter, et ainsi de faire des choix éclairés dans la construction de systèmes de chiffrement.



Ce nouvel algorithme a relancé la course au record de calcul de logarithmes discrets, l'un des deux grands problèmes à la base de la cryptographie. En août 2012, avec les algorithmes de la génération précédente, quatre chercheurs japonais avaient réussi à déchiffrer un code de 923 bits de longueur en 750 000 heures de calcul. L'algorithme d' Antoine Joux permet d'aller bien au-delà : le 24 décembre 2012, il déchiffre un code de 1175 bits. Le 19 février, une équipe de chercheurs irlandais atteint les 1971 bits. Antoine Joux les double le 22 mars avec 4080 bits ; le 11 avril, ils reprennent la main, avec 6120 bits. Le 21 mai enfin, Antoine Joux déchiffre un code de 6168 bits, à peine plus long mais beaucoup plus proche de la réalité des codes utilisés.

Mais ce dernier record n'a nécessité que 550 heures de calcul. La course va donc probablement continuer. Ces nouveaux algorithmes vont-il réussir à remettre en cause toute la méthode cryptographique du logarithme discret ? Pour le moment, la question reste ouverte. Mais au cas où le problème du logarithme discret s'effondrerait complètement, les autres chercheurs du laboratoire Prism travaillent à inventer de nouvelles solutions de cryptage.

INFORMATIONS COMPLÉMENTAIRES

> Lire le communiqué de presse de l'ACM (en anglais)
> Pour les spécialistes et les courageux : consulter l'article qui a valu le prix Gödel à Antoine Joux : *A One-round protocol of tripartite Diffie-Hellman*

Contact :
Clara Tomasini, *chargée de communication éditoriale*
Tél. : 01 39 25 79 58
clara.tomasini@uvsq.fr