Antoine Joux, Prix Gödel 2013

Jacques Stern [1]

Antoine Joux est Professeur associé à l'Université de Versailles Saint-Quentin-en-Yvelines et chercheur au sein de l'équipe cryptographie du laboratoire PRISM (UVSQ/CNRS). Le 3 juin 2013, il a reçu 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).



Le prix Gödel 2013 a été décerné à Antoine Joux, Dan Boneh et Matt Franklin. C'est à la fois une juste reconnaissance de la profondeur des travaux d'Antoine Joux et de ses deux collègues, une véritable fierté pour la communauté des informaticiens français et, pour moi, la source d'une très grande joie. Antoine est en effet le premier de mes élèves qui a fait une thèse en cryptographie, au sein du Laboratoire d'informatique de l'École normale que nous avons rejoint pour ainsi dire ensemble. Je me souviens des heures passées en discussions autour de concepts mathématiques et d'implantations informatiques : Antoine avait déjà cette capacité étonnante de penser l'algorithmique de manière native, alors que, pour ceux venant d'une génération antérieure, il avait fallu un long apprentissage passant par l'étude des travaux des fondateurs. Les noms des fondateurs les plus emblématiques, Gödel et Turing, ont d'ailleurs été donnés aux deux grands prix internationaux d'informatique et ces prix sont allés tous deux cette année à des cryptologues, marquant ainsi la vitalité de cette discipline.

1. Professeur à l'École normale supérieure.

Paradoxe de ce prix Gödel : Antoine, Dan et Matt n'ont absolument pas travaillé ensemble mais ils ont, de part et d'autre de l'Atlantique, fait faire à la cryptologie deux pas de géant, qui ont permis, une fois mis bout à bout, de résoudre une conjecture ancienne et d'ouvrir un nouveau chapitre de la discipline. La conjecture avait été énoncée par Adi Shamir en 1984 lors du congrès Eurocrypt organisé à la Sorbonne, à quelques pas des lieux où Antoine a préparé sa thèse. Simple coïncidence bien sûr ! C'était huit ans après l'article de Whit Diffie et Marty Hellman *New Directions in Cryptology* [2], imaginant la cryptologie asymétrique et six ans après les travaux de Ron Rivest, Adi Shamir et Len Adleman, en donnant le premier exemple, le célèbre système RSA [8]. Comme on l'enseigne aujourd'hui dès le lycée, cette cryptologie permet de chiffrer un message à l'aide d'une clé publique accessible à tous ; le destinataire légitime seul peut reconstituer le message clair à l'aide d'une autre clé, appelée clé privée, mathématiquement reliée à la première, mais gardée quant à elle secrète. Dans le système RSA, la clé privée est choisie en premier et la clé publique s'en déduit. Il est donc impossible pour un utilisateur de choisir cette dernière a priori, par exemple en prenant son adresse mail ou son numéro de sécurité sociale. La conjecture de Shamir portait précisément sur l'existence de systèmes cryptographiques asymétriques dotés de cette propriété. C'est cette conjecture que les travaux de Joux, Boneh et Franklin ont résolue par l'affirmative et la branche de la cryptologie qu'ils ont ouverte a naturellement pris le nom de cryptologie fondée sur l'identité.

Pour comprendre les contributions des uns et des autres, il faut rappeler que Diffie et Hellman n'étaient pas parvenus à proposer un système asymétrique et qu'il avait fallu attendre l'invention de RSA pendant deux ans. Toutefois, ils avaient pu réaliser une fonctionnalité très proche : l'échange public de clé. Un tel échange se joue entre deux participants, chacun annonçant une donnée publique liée mathématiquement à des quantités gardées secrètes. Au terme de l'échange, les deux joueurs ont en commun une clé secrète commune, calculée à partir de leurs secrets respectifs et des données publiques. Il faut rappeler aussi que les recherches actives pour trouver d'autres exemples que le système RSA avaient conduit à l'utilisation des courbes elliptiques, comme proposé par Neil Koblitz [6] et Victor Miller [7] en 1985. Il faut rappeler enfin que certaines de ces courbes avaient été reconnues comme présentant des faiblesses, celles pour lesquelles on pouvait définir une opération dotée de propriétés algébriques remarquables, introduite dans les travaux d'André Weil dans les années 1940 et qui a depuis reçu le nom de couplage de Weil.

La découverte d'Antoine Joux procède d'un étonnant changement de perspective : utiliser le couplage non pour monter une attaque mais pour profiter de ses propriétés algébriques afin d'obtenir de nouvelles fonctionnalités. Par un choix extrêmement fin des paramètres, il a montré qu'il y avait bien un espace à l'abri des attaques connues, pour développer ces fonctionnalités et il en a donné un premier exemple en 2000 : l'échange triparti à la Diffie-Hellman [4]. Dans cet échange ce sont non plus

deux mais trois joueurs qui construisent une clé secrète commune après avoir diffusé chacun une unique annonce.

Le second pas vers la solution de la conjecture de Shamir résulte là encore, d'un surprenant changement de perspective opéré cette fois par Dan Boneh et Matt Franklin [1]. En 1984, Taher El Gamal avait montré comment rendre l'échange de clé de Diffie-Hellman dissymétrique pour en faire un cryptosystème à clé publique [3] ; un des joueurs – celui disposant de la clé secrète – restait stable, tandis que ceux qui lui adressaient des messages créaient des quantités secrètes éphémères. C'était un peu faire jouer Kasparov aux échecs contre le reste du monde ! Pour passer de l'échange triparti à un cryptosystème fondé sur l'identité, il faut ajouter un arbitre. Cet arbitre reste immuable ; Kasparov et les autres grands maîtres en reçoivent une clé dérivée de leur identité et ils jouent alors avec le reste du monde. Cependant, chaque partie, prise isolément, se joue à trois suivant les règles proposées par Antoine Joux. Ceux qui trouvent – sans doute à juste titre - l'analogie peu éclairante sont invités à lire les articles d'Antoine Joux *A One-Round Protocol for Tripartite Diffie-Hellman* [5] et de Boneh-Franklin *Identity-Based Encryption from the Weil Pairing* [1]. Ils y reconnaîtront le talent respectif des auteurs et ils verront la filiation entre les deux textes. Cette filiation est d'ailleurs avérée : en montant à la tribune du congrès Crypto durant l'été 2001, Dan a dit en souriant : je vais utiliser une hypothèse algorithmique nouvelle mais, d'une part, elle m'est utile et, d'autre part, un chercheur l'a utilisée avant moi. Ce chercheur c'était Antoine naturellement. Quant à l'hypothèse algorithmique, elle affirme qu'il est difficile de calculer la valeur d'un couplage de Weil, même en disposant d'autres valeurs du couplage prises sur des arguments liés par des relations algébriques simples. Comme indiqué plus haut, l'utilisation de cette hypothèse a véritablement ouvert un nouveau domaine de recherche.

Le prix Gödel est attribué pour une contribution en particulier et non pour un ensemble de travaux. Toutefois, je ne peux terminer sans mentionner que le registre d'Antoine n'est pas limité au couplage de Weil : il a notamment montré comment calculer explicitement des collisions pour certaines fonctions de hachage et il détient plusieurs records sur le calcul de logarithmes discrets. Dans les deux cas il a su combiner avec élégance idées mathématiques et calculs massifs. Pour conclure, je livre au lecteur une observation faite sur le site *Mathematics Genealogy Project* [2] : en notant DT la fonction qui associe à un chercheur son directeur de thèse, on a DT^5(Joux) = DT(Weil). Simple coïncidence encore ! Ou peut-être plus : bien que leur science soit plus récente, les membres de la communauté des informaticiens sont, au même titre que les collègues d'autres disciplines, les héritiers d'une tradition scientifique d'excellence. Le prix décerné à Antoine Joux fait honneur à cette tradition.

2. `http://genealogy.math.ndsu.nodak.edu/`

Références

[1] D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. Proc. CRYPTO '2001, *Lecture Notes in Comput. Sci.* **2139**, 213-–229 (2001).

[2] W. Diffie and M. Hellman. New Directions in Cryptology. *IEEE Trans. Inform. Theory* **22**, 644–654 (1976).

[3] T. El Gamal. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. Proc. CRYPTO '1984, *Lecture Notes in Comput. Sci.* **196**, 10–18 (1985).

[4] A. Joux. A One Round Protocol for Tripartite Diffie-Hellman. Proc. ANTS-IV, *Lecture Notes in Comput. Sci.* **1838**, 385–394 (2000).

[5] A. Joux. A One Round Protocol for Tripartite Diffie-Hellman. *J. Cryptology* **17**, 263–276 (2004).

[6] N. Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation* **48**, 203–209 (1987).

[7] V. Miller. Uses of elliptic curves in cryptography. Proc. CRYPTO '1985, *Lecture Notes in Comput. Sci.* **218**, 417–426 (1986).

[8] R. Rivest, A. Shamir and L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM* **21**, no. 2, 120–126 (1978).