École doctorale : École doctorale de mathématiques et informatique de Bordeaux, ED-39

Unité de recherche : Institut de Mathématiques (IMB) - Université Bordeaux 1 et CNRS, UMR 5251

Équipe : Théorie des nombres et algorithmique arithmétique

Localisation : Institut de Mathématiques de Bordeaux

Directeur : Gilles Zémor

Courriel : `Gilles.Zemor@math.u-bordeaux1.fr`

Sujet de thèse : Étude de la combinatoire des schémas de révocation et d'identification.

Description :

Les problèmes étudiés sont motivés par l'application cryptographique des schémas de diffusion chiffrée (broadcast encryption). La situation est celle où le diffuseur émet un message chiffré par une fonction qui admet un nombre important de fonctions de déchiffrement différentes. Chaque fonction de déchiffrement est associée à un utilisateur potentiel, et l'on souhaite intégrer au schéma une capacité de révocation, c'est-à-dire interdire l'accès au message à un sous-ensemble choisi d'utilisateurs tout en autorisant l'accès aux utilisateurs restants.

Un tel schéma peut être réalisé par une famille de parties d'un ensemble fini (destiné à être un ensemble de clés) possédant des bonnes propriétés de recouvrement. Chaque utilisateur dispose d'une de ces parties, c'est-à-dire d'un petit ensemble de clés. Chaque message diffusé est chiffré avec une clé de session, laquelle est elle même chiffrée plusieurs fois avec des clés différentes ; les différents chiffrés de la clé de session constituent l'en-tête du message. Au moins une des clés de chaque utilisateur autorisé doit lui permettre d'accéder à la clé de session.

Du point de vue combinatoire, l'en-tête est une partie d'un ensemble (de clés) qui intersecte toutes les parties associées à chaque utilisateur autorisé et dont l'intersection avec celles des utilisateurs révoqués est vide. Si l'on souhaite pouvoir révoquer t utilisateurs quelconques sans pénaliser un autre utilisateur, il s'agit notamment d'assurer qu'une quelconque partie de la famille n'est jamais incluse dans la réunion de t autres parties. Le système est, en particulier, d'autant plus efficace que l'ensemble sous-jacent est petit et la famille grande.

Les ensembles de parties possédant cette propriété ont été étudiés par le passé dans différents contextes, et remontent aux travaux de Kautz et Singleton (Non random binary superimposed codes, 1964) puis Erdös Frankl Füredi (Families of finite sets in which the no set is covered by the union of r others, 1985). Ces structures trouvent par ailleurs des applications, certaines récentes, dans le domaine du «group testing» entre autres.

Dans le cadre de la révocation apparaît cependant une préoccupation supplémentaire, à savoir celle de la taille de l'en-tête : celle-ci donne lieu à des problèmes combinatoires originaux. L'étude portera sur de nouvelles manières d'engendrer des bons schémas combinatoires de révocation. D'autres schémas de révocation pourront être envisagés. Il sera également opportun d'étudier les relations avec le problème voisin de l'identification ou du pistage des pirates (traitor tracing).

Connaissances et compétences :

Des connaissances préalables en cryptographie, ainsi qu'en codage correcteur d'erreurs seront utiles. Un goût pour les mathématiques combinatoires et les probabilités discrètes est souhaité.