technicolor

Marc Joye, *HDR*
Technicolor
175 S. San Antonio Road
Los Altos, CA 94022, USA
email : marc.joye@technicolor.com

Objet : Mémoire d'habilitation de Duong Hieu Phan

Los Altos, le 18 octobre 2014

Madame, Monsieur,

Le mémoire d'habilitation à diriger des recherches (HDR) de Duong Hieu Phan porte sur la diffusion chiffrée et le traçage de traîtres (en anglais, « broadcast encryption » et « traitor tracing »). Ces deux primitives cryptographiques présentent la particularité qu'un même message chiffré est destiné à un grand nombre d'utilisateurs. Cette configuration, différente de la configuration usuelle point à point, pose un certain nombre de défis au niveau de la mise en œuvre et des modèles de sécurité.

Les techniques de diffusion chiffrée et de traçage de traîtres apportent des solutions complémentaires. De façon simplifiée, la diffusion chiffrée s'assure que seuls les utilisateurs autorisés puissent accéder au contenu en clair avec une clé de déchiffrement qui leur est propre. Le traçage de traîtres, quant à lui, dissuade les utilisateurs de partager leurs moyens de déchiffrement en permettant, par exemple, de remonter à un des utilisateurs ayant participé à la construction d'un décodeur pirate. Ces techniques cryptographiques sont largement utilisées en pratique, principalement dans les domaines de la distribution de contenus numériques (sur support physique) ou de la télévision à péage, ou encore dans les systèmes de géo-localisation. Les travaux de Duong Hieu Phan visent à améliorer l'efficacité et la sécurité de tels systèmes.

Le mémoire offre un aperçu très complet et récent des différentes techniques connues à ce jour. Il contient un nombre important de contributions originales de l'auteur, obtenues seul ou en collaboration avec d'autres chercheurs. L'ensemble de ces contributions sont reprises en annexe. La partie principale du mémoire est organisée en quatre chapitres.

1. Le premier chapitre présente de façon succincte les primitives de diffusion chiffrée et de traçage de traîtres ainsi que les notions de sécurité associées.

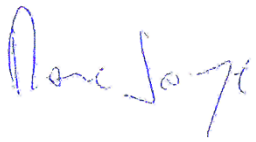
2. Essentiellement, deux familles de schémas existent. Le deuxième chapitre s'intéresse aux constructions dites combinatoires, lesquelles s'appuient sur des structures de type arbre ou à base de codes ; le but étant de pouvoir supporter les fonctionnalités de traçage et/ou de révocation.
3. Le troisième chapitre étudie les approches purement algébriques et introduit, dans un second temps, des approches hybrides (combinatoire et algébrique). Plusieurs schémas reposant sur diverses hypothèses cryptographiques dans certains modèles de sécurité sont présentés.
4. Enfin le dernier chapitre liste plusieurs problèmes ouverts et suggère plusieurs voies de recherche dans la continuité du mémoire, visant à améliorer certaines caractéristiques des schémas existants.

Duong Hieu Phan est un très bon chercheur, de niveau international. Il publie régulièrement, y compris dans les conférences phares de son domaine. Certains de ses travaux ont été primés ou ont donné lieu à des dépôts de brevets. Il a à plusieurs reprises été invité à présenter ses résultats lors de séminaires ou de congrès. En outre, Duong Hieu Phan a participé à plusieurs conférences internationales en tant qu'organisateur ou que membre du comité de programme. Il est un expert reconnu dans son domaine et maîtrise les techniques cryptographiques sous-jacentes.

Ainsi, au vu des nombreuses et substantielles contributions apportées par ce mémoire, j'émets sans réserve un avis très favorable à la soutenance.

Je vous prie d'agréer, Madame, Monsieur, mes salutations les meilleures.

Cordialement,



Marc Joye
Technicolor Fellow

Technicolor R&D France Snc
975, avenue des Champs Blancs – CS 17616
35576 Cesson-Sévigné cedex, France
tél. : +33 (0)2 99 27 30 00 - fax : +33 (0)2 99 27 30 01
www.technicolor.com

SNC au capital de 152 000 euros
Siège social : 1-5, rue Jeanne d'Arc
92130 Issy-les-Moulineaux, France
341 399 558 R.C.S. de Nanterre