Rapport de thèse d'habilitation

Jean-Sébastien Coron

Ceci est un rapport sur la thèse d'habilitation de Duong Hieu Phan intitulée "Some Advances in Broadcast Encryption and Traitor Tracing".

1 Commentaires

Dans le chapitre d'introduction, le candidat rappelle les deux objectifs essentiels du chiffrement multi-utilisateurs: le contrôle d'accès qui permet de restreindre la diffusion du message confidentiel à un sous-ensemble d'utilisateurs (broadcast encryption), et la détection des traîtres qui a pour but de décourager les utilisateurs de partager leur clef de déchiffrement, sachant que cela pourra être détecté (traitor tracing). Le chiffrement multi-utilisateurs est une primitive de base dans le domaine de la télévision à péage. Dans ce domaine comme dans le reste de la cryptographie, l'utilisation de primitives à sécurité prouvée est bien sûr essentielle.

Cela signifie qu'il faut définir convenablement la sécurité du chiffrement multi-utilisateur. Le candidat rappelle ainsi au premier chapitre les principales notions de sécurité. Le candidat rappelle aussi les principaux schémas de broadcast et de traitor tracing. Ces schémas peuvent être différenciés en deux classes: les schémas combinatoires et les schémas algébriques.

Dans le chapitre deux, l'auteur considère les schémas combinatoires et commence par rappeler les constructions existantes à base d'arbre, en particulier la construction de Naor, Naor et Lopspiech [NLL01] dans le modèle "subset-cover". L'auteur rappelle aussi les schémas basés sur les codes, en particulier la construction de Tardos. Enfin, l'auteur décrit un nouveau schéma, publié avec Hung Q. Ngo et David Pointcheval dans le journal Algorithmica.

Dans le chapitre trois, l'auteur considère les schémas algébriques ainsi qu'une combinaison algébrique et combinatoire. En particulier le schéma de Boneh, Gentry et Waters [BGW05] est le premier à avoir proposé un schéma de broadcast à clef publique complètement résistant à la collusion avec une taille de chiffré constante.

Le candidat décrit d'abord des extension au schéma BGW, en particulier un schéma de broadcast avec la propriété "inclusive-exclusive" permettant au schéma de spécifier efficacement soit les utilisateurs pouvant déchiffrer, soit les utilisateurs révoqués. Le candidat décrit également une extension de BGW pour le chiffrement multi-canal, utile dans le contexte de la télévision à péage; l'article a été publié dans la conférences ASIACCS 13. Le candidat introduit ensuite le premier schéma de traitor tracing basé sur les réseaux, avec une sécurité basée sur une variante du problème LWE. L'article a été publié dans la conférence CRYPTO 2014. Enfin l'auteur propose un schéma de traitor tracing avec une expansion du chiffré optimale, en étendant la méthode de Kiayias-Yung pour combiner des méthodes combinatoires et

des méthode algébriques. Ces constructions ont été publiées dans les conférences ISC 2007 et LATINCRYPT 2012.

Enfin, au chapitre 4, le candidat décrit de nouveaux modèles de sécurité pour le chiffrement broadcast. En particulier le candidat décrit un nouveau modèle d'attaquants collaborant de manière publique en publiant une partie de leurs secrets, sans risque d'être tracés; le candidat décrit ainsi plusieurs attaques de ce type contre des schémas existants, ainsi que des contre-mesures possibles. L'article a été publié lors de la conférence Eurocrypt 2009.

2 Avis

La thèse est très bien rédigée et rend bien compte des nombreuses contributions du candidat dans le domaine de la cryptographie. Plusieurs de ces contributions ont fait l'objet de publications lors des conférences EUROCRYPT et CRYPTO, les deux plus importantes du domaine.

En conclusion, j'émets un avis très favorable pour la soutenance de cette thèse d'habilitation.

Rueil, le 18 octobre 2014
Jean-Sébastien Coron
Professeur-associé à l'Université du Luxembourg.