« CONTRIBUTIONS À LA CONCEPTION ET ANALYSE DES SCHÉMAS DE CHIFFREMENT COMPLÈTEMENT HOMOMORPHE » PAR FRANCISCO VIAL PRADO

Discipline : Informatique / Laboratoire de recherche LMV - Laboratoire de Mathématiques de Versailles

Résumé :
Les schémas de Chiffrement Complètement Homomorphe (FHE) permettent de manipuler des données chiffrées avec grande flexibilité : ils rendent possible l'évaluation de fonctions à travers les couches de chiffrement. Depuis la découverte du premier schéma FHE en 2009 par Craig Gentry, maintes recherches ont été effectuées pour améliorer l'efficacité, atteindre des nouveaux niveaux de sécurité, et trouver des applications et liens avec d'autres domaines de la cryptographie. Dans cette thèse, nous avons étudié en détail ce type de schémas. Nos contributions font état d'une nouvelle attaque de récuperation des clés au premier schéma FHE, et d'une nouvelle notion de sécurité en structures hierarchiques, évitant une forme de trahison entre les usagers tout en gardant la flexibilité FHE. Enfin, on décrit aussi des implémentations informatiques. Cette recherche a été effectuée au sein du Laboratoire de Mathématiques de Versailles

avec le Prof. Louis Goubin.

Abstract:
Fully Homomorphic Encryption schemes allow public processing of encrypted data. Since the groundbreaking discovery of the first FHE scheme in 2009 by Craig Gentry, an impressive amount of research has been conducted to improve efficiency, achieve new levels of security, and describe real applications and connections to other areas of cryptography. In this Dissertation, we first give a detailed account on research these past years. Our contributions include a key-recovery attack on the ideal lattices FHE scheme and a new conception of hierarchic encryption, avoiding at some extent betrayal between users while maintaining the flexibility of FHE. We also describe some implementations. This research was done in the Laboratoire de Mathématiques de Versailles, under supervision of Prof. Louis Goubin.

INFORMATIONS COMPLÉMENTAIRES

M. Louis GOUBIN, Professeur, université de Versailles-Saint-Quentin-en-Yvelines - Directeur de these
M. Fabien LAGUILLAUMIE, Professeur, ENS Lyon - Rapporteur
M. Duong HIEU-PHAN, Professeur, Université de Limoges - Rapporteur
Mme Aline GOUGET, Ingénieur, Gemalt - Examinateur
M. Pascal PAILLIER, Ingénieur, CryptoExperts - Examinateur
M. Daniel AUGOT, Directeur de recherche, Centre Inria-Saclay - Examinateur
M. Carlos AGUILAR MELCHOR, Maître de conférences, Université de Toulouse - Examinateur
Mme Malika IZABACHèNE, Researcher, CEA List - Examinateur

Contact : DSR - Service FED : theses@uvsq.fr