

Master 1 de Cryptologie et Sécurité Informatique
Équipe-projet GRACE

Stage estival 2017

Rapport de stage

Étude du cryptosystème de Chor-Rivest

Rémi CLARISSE

Tuteurs : Daniel AUGOT et Luca DE FEO

Introduction

Dans l'article [1]

1 Présentation de l'Inria

Inria emploie 2 600 collaborateurs issus des meilleures universités mondiales, qui relèvent les défis des sciences informatiques et mathématiques. Inria est organisé en «équipes-projets» qui rassemblent des chercheurs aux compétences complémentaires autour d'un projet scientifique focalisé. Ce modèle ouvert et agile lui permet d'explorer des voies originales avec ses partenaires industriels et académiques. Inria répond ainsi aux enjeux pluridisciplinaires et applicatifs de la transition numérique. A l'origine de nombreuses innovations créatrices de valeur et d'emploi, Inria transfère vers les entreprises (start-up, PME et grands groupes) ses résultats et ses compétences, dans des domaines tels que la santé, les transports, l'énergie, la communication, la sécurité et la protection de la vie privée, la ville intelligente, l'usine du futur ...

1.1 Centre Inria Saclay - Île-de-France

À Paris-Saclay, Inria développe des recherches à fort impact sociétal pour inventer le monde de demain. Créé en 2008, le centre de recherche Inria Saclay - Île-de-France accueille 450 scientifiques et 100 membres des services d'appui à la recherche. Les scientifiques sont organisés en 31 équipes de recherche dont 26 sont communes avec des partenaires du plateau de Saclay. Le centre accueille également le Joint Lab Inria / Microsoft Research.

«Le centre Inria Saclay - Île-de-France est un acteur essentiel de la recherche en sciences du numérique sur le plateau de Saclay. Il porte les valeurs et les projets qui font l'originalité d'Inria dans le paysage de la recherche : l'excellence scientifique, le transfert technologique, les partenariats pluridisciplinaires avec des établissements aux compétences complémentaires aux nôtres, afin de maximiser l'impact scientifique, économique et sociétal d'Inria.»
Bertrand Braunschweig, directeur du centre Inria Saclay - Île-de-France.

Références

- [1] B. Chor and R. L. Rivest. **A Knapsack-Type Public Key Cryptosystem Based on Arithmetic in Finite Fields.** *IEEE Transactions on Information Theory*, 1988.