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...

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.