Implantation d'un algorithme de calcul de forme canonique rationnelle

Université de Versailles Saint-Quentin en Yvelines

2019

Résumé Certaines notions d'algèbre telles que la forme canonique rationnelle des matrices semblaient ne pas avoir d'impact en cryptographie. Rien n'est moins vrai, et comprendre en détail l'effet des applications linéaires peu s'avérer utile en cryptographie.

Objectifs Le but de ce projet consiste à implanter les deux algorithmes décrits succintement par Daniel Augot et Paul Camion en 1994 dans l'article intitulé "Forme de Frobenius et vecteurs cycliques".

Le but consistera à trouver un vecteur cyclique d'une matrice lorsque le polynôme caractéristique est sans facteurs multiples, puis d'implanter le calcul de la forme rationnelle canonique.

Prérequis Connaissances en algèbre et corps finis.

Références Wikipedia

`https://www.semanticscholar.org/paper/Forme-de-Frobenius-et-vecteurs-cycliques-Augot-Camio`
`2fcf847de2f4d6559c1a37323548a16664fc7a5d`

Utilisation en cryptographie :

`https://eprint.iacr.org/2017/463.pdf`