Algorithme de recherche de plus grand espace vectoriel inclus

Université de Versailles Saint-Quentin en Yvelines

2019

Résumé En cryptographie symétrique, il peut s'avérer utile d'identifier des structures, notamment des espaces vectoriels, afin de pouvoir mener à bien certaines attaques (cube atacks, division property), ou de comprendre plus précisément les objets que l'on utilise.

Objectifs L'idée de ce projet consiste à implanter l'algorithme de Léo Perrin pour la recherche de plus grand espace vectoriel (affine) inclus dans un ensemble quelconque d'éléments.

De plus, l'algorithme étant relativement simple, il est demandé à l'étudiant de réfléchir à des astuces pour améliorer l'algorihtme, afin que celui-ci fonctionne sur de grandes tailles.

Prérequis Algèbre.

Références `https://eprint.iacr.org/2019/528.pdf`