Codes correcteurs et cryptosystème de Mc Eliece

Auclair Pierre

14 mai 2014

Le cryptostème de Mc Eliece est un système de cryptage qui s'appuie sur la théorie des codes correcteurs. Il se situe à l'intersection des soucis de fiabilité et de sécurité de l'information. C'est pourquoi nous avons implémenté ce système en python dans le cadre du sujet transfert et échange.

Préliminaires

Codes correcteurs

Outils informatiques

Algorithmes supplémentaires

Codes de Goppa

Définition

Décodage

Implémentation

Mc Eliece

Principe

Sécurité

Mise en oeuvre

Références