要 旨

秘密分散法における効率的なアルゴリズム

庄田亜輝

コンピュータへの情報の保管には, 盗聴やデータ紛失などの危険がともなう. これらへの耐性を高め, 情報を安全に保管する方法のひとつとして秘密分散法がある. 本研究では, 秘密分散法を効率良く実行するためのアルゴリズムを検討する. 演算処理の高速化を目的として, 拡大体上での秘密分散法の実現とその演算処理方法の検討を行う.

キーワード　秘密分散法, (k, n) しきい値法, 有限体, 拡大体

Abstract

Efficient Algorithm for the Secred Sharing Scheme

Aki SHODA

Risk, such as eavesdropping and data loss, follows on storage of the information on a computer. The Secred Sharing Scheme(SSS) is one of the safty method of data conservation. In this paper, we consider efficent algorithm for the SSS. we conduct an investigation into SSS for the extension field $\boldsymbol{GF}(2^m)$ and method of calculation.

key words Secred Sharing Scheme(SSS), (k,n)threshold SSS, finite field, extension field