要 旨

秘密分散法に基づく
ファイル保管コマンドの実装

舟橋釈仁

データを分散暗号化する理論に秘密分散法 (SSS: Secret Sharing Scheme) がある．SSS は RAID 同様にデータを分散保管する方法で, RAID にはない高い対障害性と秘匿性を持っている．本研究の目的は SSS を実装し対障害性と秘匿性を与えるシステムを作成することである．第一の目標として SSS の一つである Shamir の (k, n) 閾値 SSS に基づく `ssar` コマンドを UNIX 上に実装した．性能測定を行ったところ, 用途によっては十分実用になることが判明した．現在の実装では暗号化の単位であるブロック長は 2Byte が限界であり、これを大きくするためには原始根を求める計算を高速に行う必要があることが判明した．

キーワード　秘密分散法, 対障害性, 秘匿性, RAID5

Abstract

Implementation of an archive command using Secret Sharing Scheme

FUNAHASHI Sekiji

Secret Sharing Scheme, or SSS, is a scheme of cryptology, that distributes of data . SSS is scheme of data storage same as RAID, which have against obstacle property and secrecy property The purpose of this research is to creating system which give data against obstacle property and secrecy property First target is to implement an encrypt/decrypt command which is `ssar` on UNIX based on SSS . It turns out that the command is useful in some applications because of a performance result of the command. Block size limits of crypt unit is 2 Byte on this implement. In order to block size enlarge It need to high transaction of seeking primitive root.

key words SSS , opposite obstacle nature, Secrecy nature, RAID5, Shamir, k, nthreshold SSS, sssar