要 旨

DDMP における SSS の研究
—除算プログラムの実装—

川畑 淳史

今日、情報の電子化に伴い、膨大な量の情報が存在している。そのため機器の故障や災害によるデータの消失、情報の漏洩を防ぐことができる情報保管手法が必要とされてきている。

その最適な方法の一つとして、秘密分散法 SSS(Secret Sharing Scheme) が存在する。これは高い秘匿性と対障害性をもつ優れたデータ保管方法だが、秘密分散法は演算量が多く、処理に時間がかかるという問題があった。これまではこの秘密分散法を 2 の拡大体の演算を行うことで処理時間の向上を実現した [5][7]。

本研究では、データ駆動型プロセッサである DDMP 上で SSS を実装することでさらなる高速化を目指し、その上で必要になる除算プログラムの分析と実装をした。

キーワード　秘密分散法、2 の拡大体、DDMP、データ駆動型プロセッサ

Abstract

SSS on DDMP

—Development of the division program—

Today, a huge amount of information exists along with computerization of information. Therefore, the method that can keep infomation efficiently has been attached to importance and one of the best methods is SSS.

This is an excellent data storage method have against obstacle property and secrecy property but it's takes a lot of time to process because the amount of the operation is large. Up to now, we have used an expansion body of 2 to shorten the procesing time.

In this paper, we aim to improve the processing speed of SSS more further by mounting SSS on DDMP that is data-driven processor. Our purpose is to analyze and implement a division program in that process.

key words SSS, Data-Driven Processor