要 旨

DDMP における SSS の研究
—連立一次方程式の求解—

宗石 真人

秘匿性と対障害性という特徴を持った暗号技術に秘密分散法 (SSS: Secret Sharing Scheme) がある。データを分散保管できるという利点があるが、計算量が大きいため処理時間がかかるという欠点もある。本研究の目的は並列処理などに優れたデータ駆動型プロセッサ (DDMP: Data-Driven Multimedia Processors) に SSS を実装することで処理時間の軽減を図ることである。そのために必要となる機能の一つである連立一次方程式の求解プログラムを作成した。ガウスの掃き出し法による求解プログラムを作成することにより、DDMP 上で連立一次方程式の求解が行えるようになった。しかしパイプライン処理ができないという問題点があり、それを改善するには新しいアルゴリズムの作成が必要であることが判明した。

キーワード　秘密分散法、データ駆動型プロセッサ、ガウスの掃き出し法、パイプライン処理

Abstract

SSS on DDMP
find the solution of simultaneous linear equations

Masato Muneishi

Secret Sharing Scheme, or SSS, is cryptographic technology which has against obstacle property and secrecy property. SSS have the benefit of decentralized administration of data, and it has suffer from the disadvantage of require processing time to large calculation amount. The purpose of this research is to arrange interest processing time by mount SSS in Data-Driven Multimedia Processors, or DDMP, parallel processing what have you of top caliber. I create program to find the solution of simultaneous linear equations in function of SSS. To create find the solution of simultaneous linear equations by Gauss elimination method could find the solution of simultaneous linear equations in DDMP.

key words SSS,DDMP,Gauss elimination method,pipeline processing