要 旨

DDMP における SSS の研究
—効率的な SSS の提案—

近藤 喜昭

データを保管する手法の一つとして, 秘密分散法 (SSS: Secret Sharing Scheme) がある. データ保管には秘匿性と対障害性が求められる. SSS はこの両方の性質を併せ持っており, データ保管手法に適していると言える. しかし SSS はこうした特徴を持つ一方で処理時間が長いと言う問題点がある. 本研究の目的は, この問題に対してノイマン型プロセッサから脱却し, データ駆動型プロセッサ上で実装することによる改善策の提案である. アーキテクチャを逐次処理型から並列処理型へ移行することで処理時間を短縮し, これまで以上の高速化を行う. データ駆動型プロセッサ上で動作させるため, SSS のアルゴリズムを Data Flow Graph で記述し, シミュレータの上で実際に数値を与えてその処理にかかった時間を計測した. 結果を検討してみると, 元のデータを分割して符号化する処理は高速化することが出来たが, 復号の処理はそれまでの処理時間を越えられなかったということがわかった.

キーワード　秘密分散法, 秘匿性, 対障害性, データ駆動型プロセッサ

Abstract

SSS on DDMP
—Approach of effective SSS—

KONDO Yoshiaki

Secret Sharing Scheme (SSS) is a scheme for one of the data storage. Data storage scheme is required high security and strong for disaster. SSS satisfies these two conditions. But SSS have a problem that take for long calculation time. This paper aim at to suggestion of speed up it by adapting a data driven processor. Until now, it was the mainstream to use von Neumann type processor, but this processor is sequential processing. Data driven processor is characterized by parallel computation and effective pipeline processing. So we improve the calculation time by this two characteristics.

We implement a program of SSS algorithm written by Data Flow Graph. Data flow graph is a things to describe program to work on data driven processor. And we simulate the program by the simulator. As a result, encryption time is shortened. But decryption time became slow.

key words Secret Sharing Scheme, Data Driven Multimedia Processor, Data Flow Graph