6ZA
6A-05

高速演算用 FPGA アーキテクチャ

天沼 佳幸 (筑波大学), 宮田 耕自 (同),
丸山 勉 (同), 星野 力 (同)

1 はじめに

Field Programmable Gate Array(FPGA) は，近年の目覚ましい集積回路技術の発展にともない高集積化や高速化が進んでいる．それにより，様々な計算問題を並列，パイプライン処理を施して FPGA 上に回路を構成できるようになった．構成した回路は，多くの計算問題において，汎用マイクロプロセッサに比べ大幅な高速計算が可能であることが確認されている．

しかし，既存の FPGA には次のような問題がある．32bit 程度のデータの演算速度が非常に遅い．基本セル (1bit 演算を行う) ごとに書き換えデータが必要であるため，書き換えデータ量が多く，回路を書き換えるために多くの時間を費やす．ハードウェア記述言語 (HDL) を用いたハードウェアの設計がソフトウェアのプログラミングのように簡単ではない．

本稿では，これらの問題を解決し様々な計算に対して高速演算を可能とする，高速演算用 FPGA アーキテクチャを提案する．

2 高速演算用 FPGA アーキテクチャ

2.1 アーキテクチャの構成

高速演算用アーキテクチャの構想を図 1に示す．

このアーキテクチャは，32bit のデータ幅の 2 項演算を行う ALU と，演算結果を受け取るレジスタを基本セルとしている．また，基本セル間を接続するネットワークも 32bit 幅とする．

このようなアーキテクチャにパイプライン，並列化を施した回路を構成することにより，汎用マイクロプロセッサを凌ぐ高速演算を実現する．

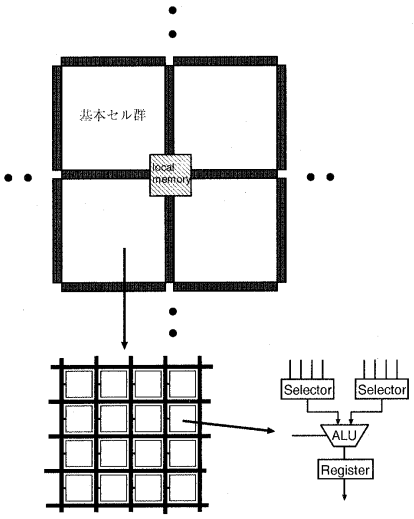

図 1: 高速演算用 FPGA アーキテクチャの構想

2.2 アーキテクチャの狙い

図 1の様な構成にすることにより，次のような効果を狙う．

まず，データ幅を 32bit にすることで，多 bit の演算における動作速度の低下を防ぐ．このことにより，動作速度の向上が得られる．

次に，ハードウェアを構成する際，アーキテクチャへの書き換えは 32bit の演算単位での指定となるため，従来の FPGA に比べはるかに少ない情報量で済む．そのため，回路構成に要する時間を大幅に短縮することができる．

最後に，アーキテクチャへのマッピングを自動で行うコンパイラの開発を考えた場合，C 言語などで書かれたプログラムが，固定長のデータに対して四則演算などの限られた種類の演算を繰り返しているため，このようなアーキテクチャの方がアルゴリズムを容易にマッピングすることができる．

A FPGA architecture for high speed computation
Yoshiyuki Amanuma (University of Tsukuba)
Kouji Miyata, Tsutomu Maruyama, Tsutomu Hoshino

3 暗号アルゴリズム

アーキテクチャの有効性を示すため，暗号アルゴリズムのハードウェア化を検証した．

今回ハードウェア化を行った暗号アルゴリズムは，RC5という共通鍵暗号である．RC5暗号アルゴリズムの，平文1ブロックから，暗号文1ブロックを生成する処理を図2に示す．

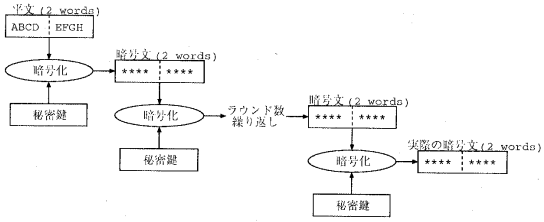

図 2: 暗号ブロックの生成

RC5はワード長，鍵長，ラウンド数が任意であり，今回作成したハードウェアは，ワード長32bit，鍵長64bit，ラウンド数12とした．

図2で生成された暗号ブロックが，そのまま暗号文として成り立つものをECBモードと言い，また，直前の暗号ブロックと排他的論理和をとってから暗号文とするものをCBCモードと言う．

図3に，ECBモードとCBCモードを示す．

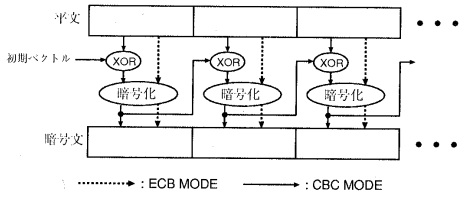

図 3: ECB，CBCモード

4 性能評価

RC5のEBC，CBCモードのソフトウェアとの速度比較，また，CAST-256という暗号アルゴリズムの速度比較も行った．計算時間は，実際にFPGAに構成したハードウェアから計算に必要なクロック数を求め，動作周波数を100MHzとして算出した．

表 1: 速度比較

	ソフトウェア	ハードウェア	速度向上比
RC5(ECB)	16.18ms	0.21ms	77.0
RC5(CBC)	18.26ms	3.65ms	5.0
CAST256	9.252ms	0.976ms	9.5

暗号処理を行ったデータは3.2Kbyteである．ソフトウェアはPentiumII 450MHzプロセッサマシンで実行した．

ECBモードでは，平文間のデータ依存がないため，充分なパイプライン処理を施して回路を作成することができたが，CBCモード，CAST256では，データ依存やメモリアクセスの問題があるため，充分なパイプライン処理を施すことができなかった．

このように本稿が提案するアーキテクチャは，パイプライン処理が有効な計算問題に対しては，大幅な高速計算が可能であることがわかる．また，従来のFPGAではほとんど高速化が望めない，多bit演算を多用し，パイプライン処理がほとんど有効でない計算問題に対しても，ある程度の高速化が望めることがわかった．

5 おわりに

今後，本稿で述べたアーキテクチャに有効であると思われるアルゴリズムのハードウェア化を行い，アーキテクチャの評価をしながら具体的なアーキテクチャの実現をめざす．また，C言語からアーキテクチャへマッピングを行うコンパイラ方式の開発を行う．

6 参考文献

[1] 宮田 耕自 (1999) : FPGAによるCPUアクセラレータ，情報処理学会第58回全国大会講演論文集，127-128

[2] 越智 裕之 (1999) : フィールドプログラマブルアキュムレータアレイFPAccA model 1.0 チップの設計と評価，情報処理学会論文詩，vol.40 1717-1725

[3]http://www.netpassport.or.jp/ wejhsk/rc5/rc5sec2.html : RC5 Algorithm