FPGAベース並列マシンRASHの改良検討 ～RASH2のハードウェア構成～

1ZB−01

浅見廣愛†，飯田全広‡，佐藤裕幸†，中島克人†，森伯郎†
†三菱電機（株），‡三菱電機エンジニアリング（株）

1　はじめに

近年、FPGA(Field Programmable Gate Array)は、最新デバイステクノロジの適用により高速化・大規模化の進展が著しく、その利便性・柔軟性と処理性能の高さから、特に信号処理や画像処理等の分野で幅広く利用されている。我々はFPGAの特性に注目し、複数のFPGAを使用した可変構造型計算機として、FPGAベース並列マシンRASH(Reconfigurable Architecture based on Scalable Hardware)を開発し[1]、DES(Data Encryption Standard)を始めとする秘密鍵暗号の鍵探索処理が高速に行えることを実証した[2]。また、合成開口レーダ(SAR, Synthetic Aperture Radar)の画像再生処理への適用検討等を行った[3]。

デバイステクノロジの進歩によりFPGAは更に大規模・高速化しており、従来より大きなデータを高速に処理可能になった。これらの新たなデバイスを用いることで、RASHの大幅な性能向上が期待できる。そこで、RASHでの適用事例を踏まえて、必要とされる機能を追加するためにハードウェアの構成等に改良を行い、新たなデバイスを適用してRASHの検討を行ったので報告する。

2　RASHの構成

RASHはCompactPCI(Peripheral Component Interconnect)基板を使用した演算ボードを基本構成要素としている。演算ボードには、1石10万ゲート規模相当のSRAMタイプのFPGAである、ALTERA社のFLEX10K100A-1(240ピンQFP)が8個搭載されている（図1参照)。

各FPGA間は32bitの信号線でメッシュ／リング状に接続されている。これにより、2石以上のFPGAを使用して1つの機能を実現するような場合や、機能ブロック間の処理データをパイプライン的に流すような構成も可能となる。このような用途を考慮して各FPGAには共通のグローバルクロックが供給される。また、各FPGAでの独立した処理を可能にするために各々のFPGAには個別にローカルクロックが供給される。グローバルクロックおよびローカルクロックは約4.9MHzから60MHzの16種類から選択できる。

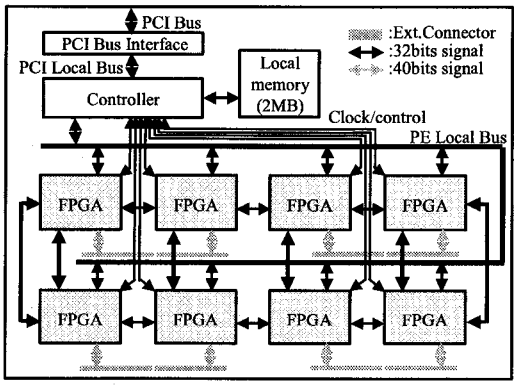

図1　RASHのボード構成

また、各FPGAはコントローラとバス接続(32bit)されており、コントローラには演算ボードに搭載されたPCIバスインタフェース回路と2MBのSRAMのローカルメモリが接続されている。FPGAの回路情報はローカルメモリを経由してロードされる。ローカルメモリ上に複数種類の回路情報を常駐させることができ、1つのFPGA当り190ms程度で再構成が可能である。

また、演算ボードの各FPGAからは直接40bitずつの信号線が拡張ボードコネクタに接続されており、ドータカードを増設することで様々な機能拡張が可能である。

3　RASH2のハードウェア構成

RASH2の演算ボードの構成を図2に示す。また、現行RASHとRASH2の主な相違点を表1に示す。

RASH2の演算ボードではフルサイズのPCI基板をカットしたもの(260mm×106.8mm)を使用し、Xilinx社のFPGAであるVirtex2000E-6を4個搭載した構成とした。RASH2では市販のPC等にも搭載できるようPCI基板を採用し、PCIインタフェースを制御用FPGA内部に構成して32bitPCIと64bitPCIの両方に対応できるようにした。Virtex2000E等の大容量FPGAを1枚の基板に多数搭載した場合、消費電力が膨大になる。このため、RASH2ではFPGAを4個とした。

A Study on the Improvement of FPGA-based Parallel Machine "RASH" - Hardware of RASH2 -
Hiroai Asami, Masahiro Iida, Hiroyuki Sato, Katsuto Nakajima, Hakuro Mori
Mitsubishi Electric Corporation & Mitsubishi Electric Engineering Co.,LTD.
5-1-1 Ofuna, Kamakura, Kanagawa 247-8501, Japan

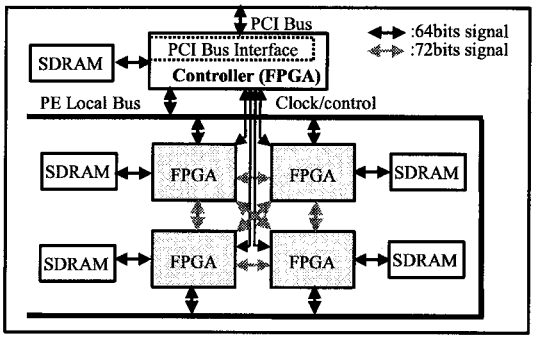

図 2 RASH2 の演算ボード構成

RASH2 でも、ボード上での構成は RASH と同様に、FPGA とコントローラがバス接続され、各 FPGA 間がメッシュ（リング）状に接続された構成になっている。各 FPGA とコントローラとのバス接続は 64bit に、各 FPGA 間を接続する信号線は 72bit に増やした。また、RASH と同様に、共通のグローバルクロックと、FPGA 個別のローカルクロックが供給される。また、各 FPGA には直接 64MByte の SDRAM が接続された構成にした。このように RASH2 では、内部バスや FPGA 間結線を強化してボード上のデータ転送性能を向上させた。また、メモリを強化することで、画像処理等の大容量のデータにも対応できるようにした。

4 演算性能の比較

RASH と RASH2 の性能を比較するため、DES 暗号回路を搭載した場合の解析性能の比較を行った。これを表 2 に示す。

RASH2 に関しては、EDA ツールを用いて、Virtex2000E 用の暗号回路を合成し、推定された動作周波数から、暗号解析性能を見積もった。FLEX10K100A 用の回路は Max+plusII を使用し、Virtex2000E 用には、論理合成には Synplify を使用し配置配線には Foundation3.3 を使用した。

論理合成の結果、Virtex2000E 上には DES 回路として F 関数 16 段の回路が 8 個搭載できた。この結果、ボード当りの性能を比較した場合、RASH2 では、RASH の約 7 倍の性能が得られた。DES 暗号回路では、FPGA 内部の RAM は使用せず、FF(flip-flop)と LUT(look up table)のみを使用する。FF のボード当りの総数比は 4 倍程度であるが、FPGA が大規模になったことにより、FPGA 内部の制御回路の占める割合が小さくなったため、このような高い性能が得られた。

また、FFT などのような内部 RAM や FPGA に直接接続した SDRAM を必要とする回路を使用した場合には、さらに高い性能が得られると予想される。一例として文献[3]に示した SAR 画像再生処理の検討結果を表 2 に示す。RASH2 と文献[3]に示した基板では、FPGA が異なる以外はほぼ同じ構成であり、RASH2 でも同等の性能が得られると考えられる。

表 1 RASH と RASH2 の構成比較

	RASH	RASH2
使用 FPGA	FLEX10K100A-1×8	Virtex2000E-6×4
FF 数／FPGA	4992 個	38400 個
FF 数／ボード	39K 個	150K 個
RAMbit 数／FPGA	24,576 個	1240K 個
RAMbit 数／ボード	192K 個	4960K 個
ボード形状	CompactPCI (6U)	PCI (Card Edge)
PCI Interface	PCI9080 (32bitPCI)	制御用 FPGA 内部に構成 (32/64bitPCI)
メモリ	SRAM 2MB	SDRAM64MB
内部バス	32bit 非同期バス	64bit 同期バス
内部結線	リング，メッシュ 各 32bit	リング，メッシュ 各 72bit
拡張 Interface	各 FPGA から 40bit	—

表 2 RASH と RASH2 の暗号解析性能比較

	RASH	RASH2
DES 暗号解析性能		
回路構成	F 関数 12 段×1	F 関数 16 段×8
動作周波数	39.5MHz	47.62MHz
使用率	90%	92%
性能／FPGA	29.6M 鍵／秒	408.8M 鍵／秒
性能／ボード	236.8M 鍵／秒	1.6G 鍵／秒
SAR 画像再生処理性能		
使用ボード数	6 枚	1 枚
処理時間	8 秒	1.3 秒

5 まとめ

以上、新デバイスを用いた RASH の改良検討について報告した。今回の検討結果を踏まえ、今後、詳細検討等を行う予定である。

参考文献

[1] 中島，他: “FPGA ベース並列マシン RASH の概要”，第 58 回情処全国大会，1H-08，1999-3.

[2] 浅見，他: “FPGA ベース並列マシン RASH での DES 暗号解析処理の改良”，情報処理学会論文誌：ハイパフォーマンスコンピューティングシステム，Vol.41,No.SIG 5(HPS 1), pp.50-57, 2000-8.

[3] 浅見，他: “FPGA ベース並列マシン RASH での SAR 画像再生処理の適用”，情報処理学会研究報告 2001-ARC-144(SWoPP2001), pp.19-24, 2001-8.