超ディペンダブルプロセッサの研究

坂井 修一
情報理工学系研究科電子情報学専攻

あらまし コンピュータシステムにとって処理速度･消費電力とともに重要なことがディペンダビリティである。われわれはマイクロプロセッサを対象として、ＬＳＩ内にディペンダビリティ機能を組み込み、高性能・省電力･ディペンダビリティの３者をバランス良く向上させるプロセッサアーキテクチャの研究を行っている。今年度は、プロセッサコアの最適化、ソフトエラー検出機構、プログラムの挙動の盗み見防止方式、暗号回路について提案し、基本設計を行った。さらに、これらの有効性について、シミュレーションなどによって検証した。

1. はじめに

コンピュータシステムにとって処理速度・消費電力とともに重要なことがディペンダビリティ[13]である。ここでは、ディペンダビリティを安全性と信頼性の両方からなる性質とする。本研究ではマイクロプロセッサレベルでのディペンダビリティを対象とし、プロセッサLSI内部にディペンダビリティ機能を組み込んで、性能とディペンダビリティの両面を向上させるプロセッサアーキテクチャ（コデザインを含む）の研究を行う。

本年度はその３年目として、プロセッサコアの最適化、ソフトエラー検出機構、プログラムの挙動の盗み見防止方式、暗号回路について提案し、基本設計を行った。さらに、これらの有効性について、シミュレーションなどによって検証した。

2. 超ディペンダブルプロセッサ

ここで研究開発を進めている超ディペンダブルプロセッサを図１に示す。

本プロセッサは、命令実行部にマルチスレッド冗長実行などのディペンダブル実行機能をもたせ、さらに

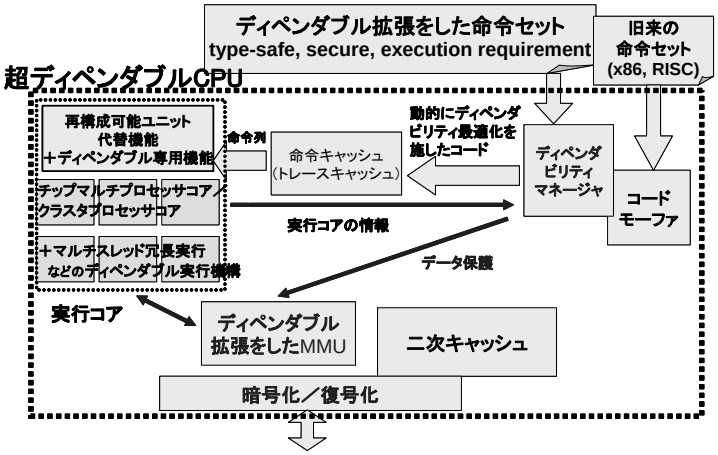


図１． 超ディペンダブルプロセッサ

実行コアにリコンフィギュラブルユニットを組み込むことで、故障時の代替機能の提供や命令実行部との機能分散を行っている。また、安全性をあげるために、外部バスの入出力は暗号化して行う。ディペンダブルなコード生成のためにはコンパイラ最適化や実行時最適化が施され、全体がディペンダビリティマネージャで管理される。

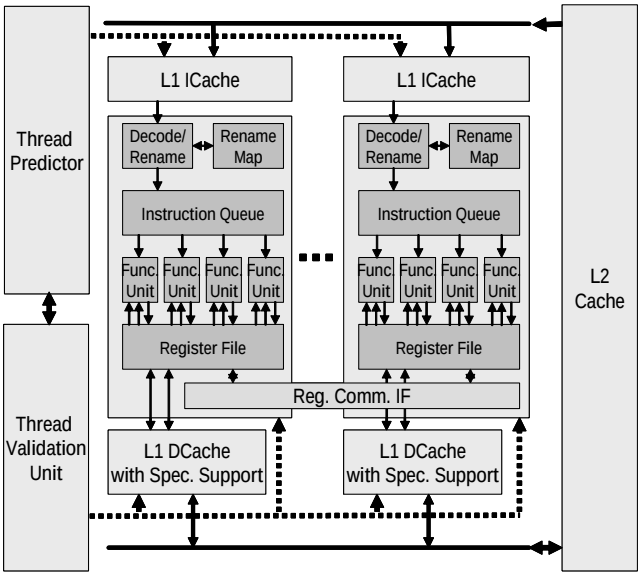
3. プロセッサコアの最適化

現在、プロセッサコアとして、チップマルチプロセ

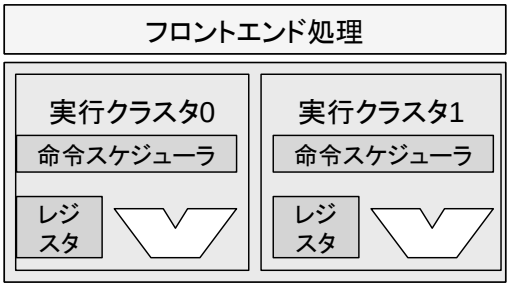
ッサとクラスタ型プロセッサを考えている（図２）。

チップマルチプロセッサに関する今年度の貢献は、投機的マルチスレッディングを行うさいのキャッシュコヒーレンスプロトコルの新規提案と検証[4][6][12]である。これによって、バスに放送機構をもたせたチップマルチプロセッサでは、提案した更新型プロトコルが有利であることが示された。

クラスタ型プロセッサでは、命令ステアリング方式[1][2][7]とメモリフォワーディング方式[3][5][8][9]について提案・評価した。前者では、データ生成命令と消費命令の命令間距離を用いるステアリング方式を提案し、シミュレータを用いた評価の結果，従来方式に比べて， 9.2%性能が向上することを確認した。後者では、分散投機メモリフォワーディングを用いてメモリオーバヘッドが低減されることがわかった。



(a)チップマルチプロセッサ



(b)クラスタ型プロセッサ

図２　プロセッサコア

4. ソフトエラー検出機構

放射線などによるソフトエラーを防止するために、パイプラインレジスタを２重化し、クロックの位相を少しずらして結果の差分をとることで、これを検知する方式を考案し、回路設計を行って評価した（図３）[11]。

実際に 0.18μm ルールのもとでこの方式の 32 ビット乗算器（5 段）を設計したところ、従来の回路と比べて面積増 19.3%、電力増 7.6%、クロック周期増 6.4%で実現できることが示された（表１）。

5. 盗み見防止機構

プロセッサの外部バスが盗み見されることを想定し、外部バスに出すデータを暗号化し、アドレスを乱数化する方式の研究を行った。特に後者について、プロセッサが外部メモリに書き込むたびにアドレス変換を行うことで空間的局所性を秘匿する方式（図４）を提案・評価した。ベンチマーク SpecInt2000 を用いた評価の結果、本方式を導入することによってアドレ

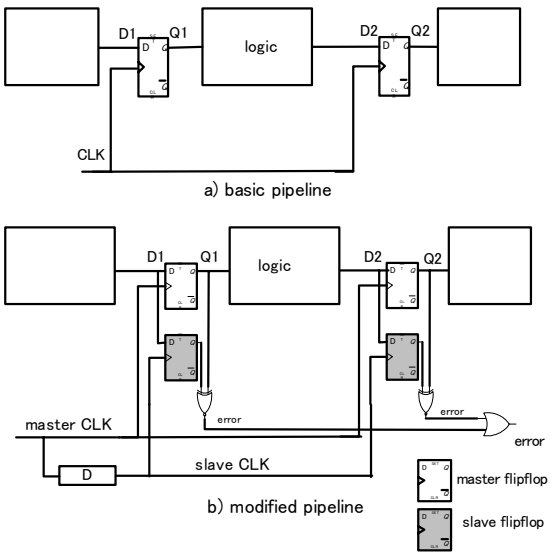


図３．ソフトエラー検出機構

スが乱数化され、またこれによる性能低下は平均で数%～十数%に過ぎず、この方式の有効性が示された（図５）。

6. 暗号回路

公開鍵暗号 RSA の回路を２種類考案・評価した。

1 つはモンゴメリ乗算を用いるものである。現在の主流である右向きアレイ法は1回のべき乗演算で行われる乗算が指数のビット数の約1.25倍の回数であり、膨大な記憶領域を必要とする。われわれは左向きアレイ法を用いて2つの乗算器を用いてべき乗演算を行う方式を提案した（図６）。その結果、記憶領域の使用を抑え、指数のビット数回の乗算でべき乗演算が行えることを確認した

もう 1 つは SRT 除算を用いるものであり、高基数の剰余除算器を設計することで、モンゴメリ乗算に匹敵する面積速度比が得られることがわかった。

７．まとめ

本年度は、ディペンダブルプロセッサの要素技術として、プロセッサコアの最適化、ソフトエラー防止機構、プログラムの挙動の盗み見防止方式、暗号回路について提案し、基本設計を行った。さらに、これらの有効性について、シミュレーションなどによって検証した。

今後は、ディペンダビリティ制御機構の研究開発、ディペンダブル要素技術と実行コアとの融合、性能・電力とのトレードオフ、コンパイラの設計が課題となる。

発表文献

[1] 服部 直也, 高田 正法, 岡部 淳, 入江 英嗣, 坂井 修一, 田中 英彦:「クリティカルパス情報を用いた分散命令発行型マイクロプロセッサ向けステアリング方式」、情報処理学会論文誌コンピューティング

表１．ソフトエラー検出回路の面積・電力・性能

	Original multiplier	Modified multiplier	Overhead
Area	0.264 mm^2	0.315 mm^2	19.3 %
Power	1.18 W	1.27 W	7.6%
Timing	4.5 ns|22.5 ns	4.58 ns|23.94 ns	1.7%| 6.4%

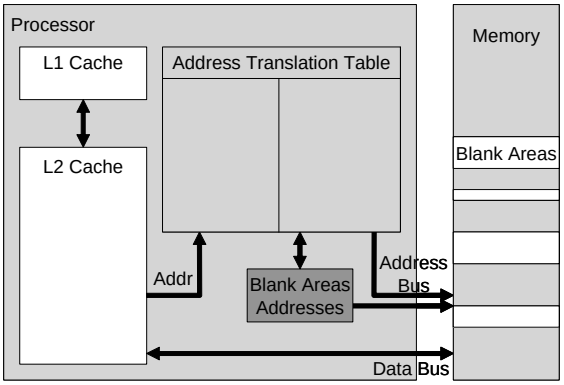


図４．アドレス秘匿機構

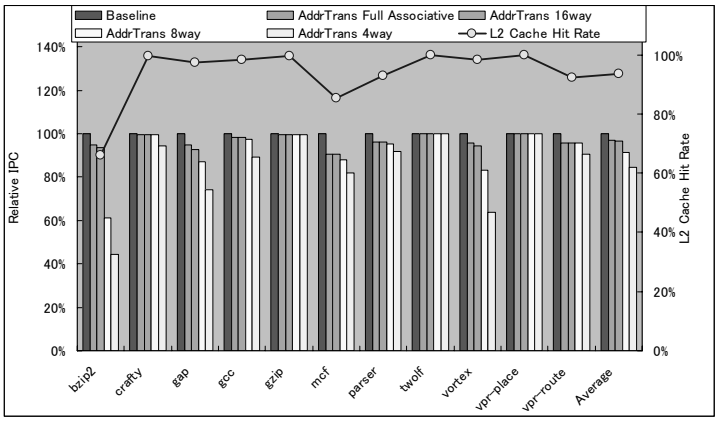


図５．動的アドレス変換によるプログラムの特性秘匿（評価結果）

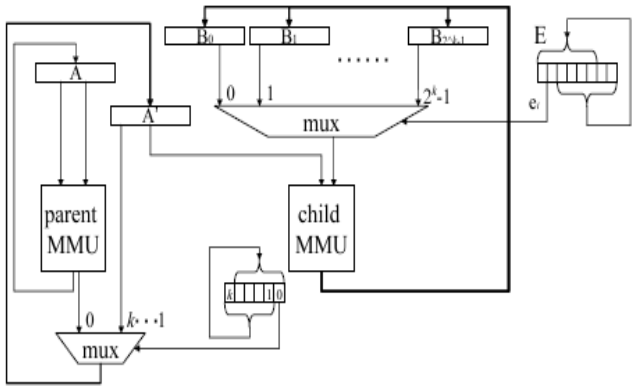


図６．左向きアレイ法によるべき乗回路

システム(ACS 6), Vol.45, No.SIG6, pp.12-22, May, 2004.
[2]服部 直也, 高田 正法, 岡部 淳, 入江 英嗣, 坂井 修一, 田中 英彦:「発行時間差に基づいた命令ステアリング方式」情報処理学会論文誌コンピューティングシステム(ACS 7), Vol.45, No.SIG11, pp.80-93, Oct, 2004.
[3]入江 英嗣, 服部 直也, 高田 正法, 坂井 修一, 田中 英彦:「クラスタ型プロセッサのための分散投機メモリフォワーディング」、情報処理学会論文誌コンピューティングシステム(ACS 7), Vol.45, No.SIG11, pp.94-104, Oct, 2004.
[4] Niko Demus Barli, Luong Dinh Hung, Hideyuki Miura, Chitaka Iwama, Daisuke Tashiro, Shuichi Sakai, Hidehiko Tanaka: "Cache Coherence Strategies for Speculative Multithreding CMPs: Characterization and Performance Study"、情報処理学会論文誌コンピューティングシステム(ACS 7), Vol.45, No.SIG11, pp.119-132, Oct, 2004.
[5] Hidetsugu Irie, Naoya Hattori, Masanori Takada, Naoya Hatta, Takashi Toyoshima, Shota Watanabe and Shuichi Sakai: "Steering and Forwarding Techniques for Reducing Memory Communication on Clustered Microarchitecture"、8th International Workshop on Innovative Architecture for Future Generation High-Performance Processors and Systems (IWIA2005)", at OAFU, Hawaii, Jan, 2005.
[6] Niko Demus Barli, Luong Dinh Hung, Hideyuki Miura, Chitaka Iwama, Daisuke Tashiro, Shuichi Sakai and Hidehiko Tanaka:"Cache Coherence Strategies for Speculative Multithreding CMPs: Characterization and Performance Study" 先進的計算基盤システムシンポジウム 2004(SACSIS2004), 於 札幌コンベンションセンター, Vol.2004, No.6, pp.111-120, May, 2004.(優秀若手論文賞受賞)
[7] 服部 直也, 高田 正法, 岡部 淳, 入江 英嗣, 坂井 修一, 田中 英彦: 「発行時間命令差に基づいた命令ステアリング方式」先進的計算基盤システムシンポジウム 2004(SACSIS2004), 於 札幌コンベンションセンター, Vol.2004, No.6, pp.167-176, May, 2004.
[8] 入江 英嗣, 服部 直也, 高田 正法, 坂井 修一, 田中 英彦:「クラスタ型プロセッサのための分散投機メモリフォワーディング」、先進的計算基盤システムシンポジウム 2004(SACSIS2004), 於 札幌コンベンションセンター, Vol.2004, No.6, pp.177-186, May, 2004.
[9] 入江 英嗣, 高田 正法, 坂井 修一:「メモリ依存予測を利用したフォワーディング局所化手法」情報処理学会報告 2004-ARC-159, 於 青森文化会館, Vol.2004, No.80, pp.49-54, Jul, 2004.
[10]Naoya Hatta, Niko Demus Barli, Chitaka Iwama, Luong Dinh Hung, Daisuke Tashiro, Shuichi Sakai and Hidehiko Tanaka: "Bus Serialization for Reducing Power Consumption"情報処理学会報告 2004-ARC-159, 於 青森文化会館, Vol.2004, No.80, pp.163-168, Jul, 2004.(若手プレゼンテーション賞受賞)
[11] Luong D. Hung, Masanori Takada, Yi Ge and Shuichi Sakai: "A Cost-effective Technique to Mitigate Soft Errors in Logic Circuits"、電子情報通信学会技術研究報告 VLD2004-49～60, 於 北九州国際会議場, Vol.104, No.477, pp.31-36, Dec, 2004.
[12]豊島 隆志, 田代 大輔, バルリ ニコ デムス, 坂井 修一:「メモリ投機を支援する CMP キャッシュコヒーレンスプロトコルの検討」情報処理学会報 2004-ARC-160, 於 北九州国際会議場, Vol.2004, No.123, pp.47-52, Dec, 2004.
[13]坂井修一:「スピードからディペンダビリティへ:プロセッサのこれから」情報処理学会関西支部大会（招待講演）論文集, 於 大阪大学中之島センター, Vol.H16, No.S-07, pp.143-148, Oct, 2004.