「ディペンダブル VLSI システムの基盤技術」
平成 19 年度採択研究代表者

平成 23 年度
実績報告

安浦　寛人

九州大学　大学院システム情報科学研究院・教授（副学長）

統合的高信頼化設計のためのモデル化と検出・訂正・回復技術

§1. 研究の概要

ディペンダビリティをコスト・性能・消費電力と同じような設計指標として位置づけ、VLSI システムの設計フローの中でシステム全体のディペンダビリティを他の指標とのトレードオフを考えながら最適化する設計技術を開発する。ディペンダビリティの評価指標の定義、それを設計の各段階で見積もる技術、ディペンダビリティの向上技術と設計中に組み込む技術、設計を最適化する技術を開発し、統合した設計フローを構築する。

1. チーム全体の研究の概要

豊橋技術科学大学グループは、主たる共同研究者の転属に伴い、平成 23 年度開始時に九州大学松永グループにマージした。

①本研究の背景、社会や産業に存在する問題と本研究の課題

LSI（大規模集積回路）は、情報通信技術の基幹的部品として、多くの社会システム（行政、経済、交通、通信、産業などの社会インフラ）の中で大量にかつ広範に利用されており、我々の生活は LSI の機能、性能、信頼性に大きく依存（depend）するようになっている。このような LSI においては、自然界の雑音や経年変化に起因する物理的な故障、設計の不備や利用法の誤りなど人的なミスに起因する障害、悪意ある攻撃者による攻撃など種々の障害要因に対して、利用者やシステムの運用者が安心して利用できる LSI を供給する技術の確立が求められている。

LSI のディペンダビリティの向上をはかるための一般的な対策として考えられるのは、LSI の機能を空間的または時間的に多重化することであり、実際、高度なディペンダビリティが必要とされるシステムでは導入されている場合もある。一方、多重化そのものは LSI システムの性能やコストに悪影響を与える場合が多く、通常の評価尺度と相反している。ところが、現時点ではディペンダビリティに関する標準的な指標というものは存在していないため、製品開発において、どの程度のディペンダビリティのためにどの程度の性能やコストを犠牲にすればよいのか、というトレードオフを客観的に考慮することが難しいという問題点がある。また、複雑な LSI システムの設計は、アーキテクチャレベル、レジスタ転送レベル、論理回路レベル、電子回路レベル、レイアウトレベルと階層的に行われ、この階層化に基づく設計フローが確立し、設計ツールや検証ツールが整備されている。しかし、これらの設計フローと自然に連携できるディペンダビリティの評価尺度や評価手法についても十分に検討がなされていない。

本研究チームでは、既存の設計フローと整合性を持ったディペンダブルな LSI システムの設計手法とフローおよびその為の設計ツール群を開発するために、具体的な事例として、(a) 中性子線等に起因するソフトエラー、(b) 素子の製造ばらつきや経年劣化によるタイミングエラー、(c) 悪意ある攻撃による回路内の機密データの漏洩を対象として取り上げ、原因となる物理的な現象からシステム全体のディペンダビリティを評価し、向上させる設計フローと必要なツールを構築する。これらの事例に対する研究を通じて、既存の階層設計との整合性を考慮し、一般的なディペンダブル VLSI の設計フローとツール群の開発指針を明確にすることを目指す。

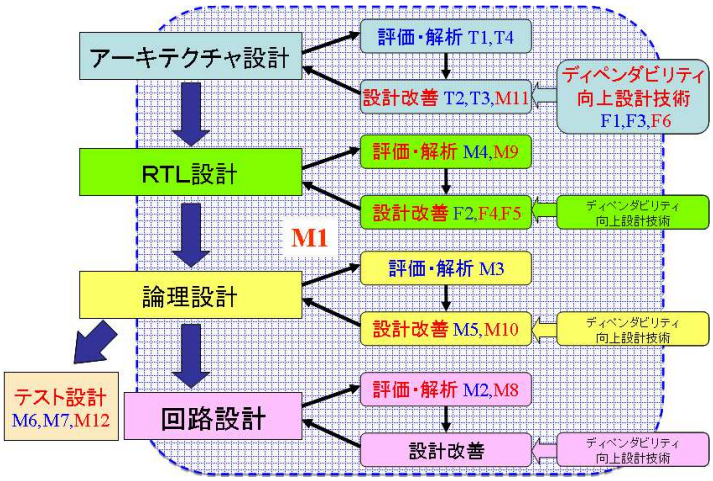
②本研究チームの達成目標

中性子線等に起因するソフトエラー、素子の製造ばらつきや経年劣化によるタイミングエラー、悪意ある攻撃による回路内の機密データの漏洩の3つの事例を対象とした各設計レベルにおけるディペンダビリティの評価指

標、見積もり技術、向上技術などを開発し、設計フローとツールを構築する。
　これらの研究開発を通じて、一般的なディペンダビリティの評価指標の定義、それを設計の各段階で見積もる技術、ディペンダビリティの向上技術と設計中に組み込む技術、設計を最適化する技術の開発、統合した設計フローの構築に対する基本的な方針を明確にする。

③本研究のアプローチ
　研究開始後の、領域代表やアドバイザーとの議論に従い、本研究は下記のようなアプローチで進める。
1) 具体的な事例として、ディペンダビリティに対する新しい問題として指摘されている下記の課題を対象とする。
　(a) 中性子線等に起因するソフトエラー
　(b) 素子の製造ばらつきや経年劣化によるタイミングエラー
　(c) 悪意ある攻撃による回路内の機密データの漏洩
　特に、ソフトエラーに関する問題に注力し、ソフトエラー対策に対応する設計フローとそのためのツールチェインの基本技術の構築に注力する。また、物理現象に関する専門家と協力して、物理レベルからシステムレベルまでの一貫したソフトエラーのディペンダビリティに対する影響を明らかにする。

2) 既存の階層設計の各レベルにおいて下記の課題を解決する。特に、物理現象のレベルからシステムレベルまでの因果関係を明確にリンクさせ、各階層でのディペンダビリティに関する現象の抽象化の在り方を検討する。
　(ア) 階層設計の各レベルにおけるディペンダビリティの評価指標の定義
　(イ) 各レベルにおけるそれぞれの抽象度でディペンダビリティを効率良くかつできるだけ正確に見積もる技術
　(ウ) 各レベルにおけるディペンダビリティの向上技術とそれを大規模な設計中に組み込む技術
　(エ) コストや性能、消費電力等の制約要件とのトレードオフを考慮し、設計全体を最適化する技術
　(オ) 個々のツールを統合した設計フローの構築



(M1～M12、F1～F6、T1～T4 は§4 の成果番号)
図1　設計フローとツールチェイン

3) これらの具体事例に対する研究開発を通じて、一般的なディペンダビリティの評価指標の定義、それを設計の各段階で見積もる技術、ディペンダビリティの向上技術と設計中に組み込む技術、設計を最適化する技術の開発、統合した設計フローの構築に対する基本的な方針を明確にする。また、当初予定していたテストベッドによる実証実験は、費用対効果を考えて中止する。

④研究実施方法
1) 本研究チーム運営の方針、研究グループ間の分担・協力関係
　4 つ(平成 23 年度から 3 つ)のグループが密接に連携をしながら、研究を進めている。九州大学安浦グループがチーム全体のとりまとめを行い、ソフトエラー、タイミングエラー、機密データの漏洩について、それぞれのグループが得意とする設計段階に対応する具体的な研究を行っている。
・ソフトエラーについては、松永グループが中心となり RT(Register Transfer)レベルおよび論理レベルを主として担当し、豊橋技術科学大学グループ(平成 23 年度開始時に九州大学松永グループにマージ)と福岡大学グループが CPU や FPGA のアーキテクチャレベルに対応する。また、神戸大学の吉本チームのメモリに関する研究とも強く連携している。
・タイミングエラーについては、福岡大学グループが中心となり、他グループも議論に加わって研究を進めている。
・機密データの漏洩については、九州大学松永グループと安浦グループで研究を進めている。

すべてのグループが参加する会議（テレビ会議を利用）を2週間に1回程度の頻度で開催するとともに、合宿形式の研究検討会を年に1回ないし2回開催している。

2) 領域外部の企業等との連携

ソフトエラーに関しては、当初A社からの実問題の相談を受けて、具体的な研究に取り組んだ。最終的には、相手方の問題解決にはつながっていないが、現場からの問題の提示は、研究の方針を決める上で大いに役立った。

現在、B社と、デバイスレベルと回路レベルのソフトエラーモデルの整合性を取る問題で意見交換を重ねており、共同研究への発展も検討している。九州大学大学院総合理工学研究院の原子核物理の研究者渡辺幸信教授ともソフトエラーに関する情報交換を行っている。

3) 領域内他研究チームとの連携関係

神戸大学の吉本チームと密接な共同研究体制を取っている。本チームが論理回路中心、吉本チームがメモリ中心という分担で、モデルや評価ツールの共通化などの協力体制を構築し、頻繁な情報交換を行っている。

また、アーキテクチャレベルにおいて、東京大学の坂井チームと情報交換を行っている。フリップフロップの回路構造とセルレイアウトについては、小野寺チームの小林教授と意見交換を行っている。

2. 研究グループの研究の概要

豊橋技術科学大学グループを九州大学松永グループにマージしたため、今年度から安浦チームは3グループ構成となった。

(1) 九州大学安浦グループ

①本研究グループの研究課題、ならびに所属する研究チームの課題との関係

本グループの研究課題は、「統合的高信頼化設計のためのモデル化と検出・訂正・回復技術」であり、本領域の最終目標の一つであるVLSIが搭載している価値や信用を守るための設計技術の確立のために、各グループの研究課題を統合し、一般化して、本領域全体への位置づけを明確にする。領域全体の研究方針への提案や、他のチームとの連携方針等を検討し、本チーム内の各グループにおける研究課題やアプローチに対して適切なアドバイスを行う。

②本研究グループの達成目標

中性子線等に起因するソフトエラー、素子の製造ばらつきや経年劣化によるタイミングエラー、悪意ある攻撃による回路内の機密データの漏洩の 3 つの事例を対象とした各設計レベルにおけるディペンダビリティの評価指標、見積もり技術、向上技術などの開発に関する基本的な指針を明示する。さらに、一般的なディペンダビリティの評価指標の定義、それを設計の各段階で見積もる技術、ディペンダビリティの向上技術と設計中に組み込む技術、設計を最適化する技術の開発、統合した設計フローの構築への道筋を明らかにし、VLSIが搭載している価値や信用を守るための設計技術の確立を目指す。

③研究のアプローチ

各グループ間の研究活動を調整し、本チームにおける具体的な研究対象に対する各グループの研究成果を統合し、一般的なディペンダビリティの評価指標の定義、それを設計の各段階で見積もる技術、ディペンダビリティの向上技術と設計中に組み込む技術、設計を最適化する技術の開発、統合した設計フローの構築に対する基本的な方針として一般化する。

④研究実施方法

1) 本研究チーム運営の方針、研究グループ間の分担・協力関係

定期的にチーム全体の情報交換の会議を主催し、チーム間の研究活動の調整を行うとともに、領域に対するチーム全体の方針をまとめる。また、チーム内のグループの研究活動が円滑に進むように環境整備を行う。

2) 領域外部の企業等との連携
チームを代表して関連する企業との交渉の窓口となる。積極的に連携対象の企業を探す。

3) 領域内他研究チームとの連携関係
チームを代表して関連する他の研究チームとの交渉の窓口となる。

(2)九州大学松永グループ

①本研究グループの研究課題、ならびに所属する研究チームの課題との関係
課題は以下のとおりである。

1. 論理・RT レベルのソフトエラー耐性解析ツールの開発
論理レベルでは、論理ゲートで発生したソフトエラーが記憶素子に取り込まれて異常動作となる確率を計算するための、ソフトエラー発生および伝搬のモデル化およびその解析アルゴリズムの検討を行う。
RT レベルでは、論理レベルの回路におけるソフトエラーの挙動を抽象度が一段上の RT レベルで解析することによって、より大規模かつ複雑な LSI に対するソフトエラー耐性の解析を行うアルゴリズムの検討を行う。
2. ソフトエラー耐性を考慮した論理合成アルゴリズムの研究
与えられた論理回路に冗長性を付加することでソフトエラー耐性を高めつつ、冗長性の付加にともなう面積や遅延、消費電力などのオーバーヘッドを削減する論理合成アルゴリズムの研究を行う。
3. CPU のソフトエラー耐性解析ツールの開発
CPU を用いたシステムの SEU(Single Event Upset)に対する脆弱性を測定する技術を開発する。さらに、CPU 中の組合せ回路で生じるソフトエラー、すなわち SET(Single Event Transient)に着目したソフトエラー耐性評価技術について研究を行う。集積回路の微細化が進むと、SET 起因の信頼性低下が SEU 起因の信頼性低下に匹敵するようになり、SET に対する脆弱性を見積もる技術が必要となるからである。
4. VLSI が搭載している価値や信用を守るための設計技術の確立
悪意のある攻撃に対する防御手法の提案を行う。さらに個々の防御手法の比較を行うために防御手法を適用した LSI に対するディペンダビリティの定量化手法の検討を行う。さらに個々の防御手法によるディペンダビリティの対費用効果を数値化することも合わせて目標とする。

このうち 1～3 はチーム全体の研究課題である中性子起因のソフトエラーに対してディペンダブルな LSI を設計するためのフローの確立およびそのための設計ツールの開発に対応している。4 は、悪意のある攻撃をエラーの対象としている。このエラーのモデルに対するモデル化、指標化を行う。

②本研究グループの達成目標
1～3 に関しては、論理レベルの回路や RT レベルの回路を入力として、対象の回路のソフトエラー耐性(SER: Soft Error Rate)を計算するツールのプロトタイプ版の開発を行うこと、およびソフトエラー耐性を設計制約や設計指標として考慮する設計フローの妥当性と関連する EDA ツールの実用性を評価することを目標としている。4 に関しては、悪意のある攻撃のモデル化および指標化を行うことと、ディペンダビリティを評価するツールを開発することを目標としている。

③研究のアプローチ
1. 論理・RT レベルのソフトエラー耐性解析ツールの開発
デバイスシミュレータおよび回路シミュレータを利用して、論理レベルより抽象度の低いレベルにおけるソフトエラー発生確率のモデル化を行い、そのモデルに対してある程度、精度の保証が可能な論理レベルにおけるソフトエラー発生確率のモデル化を行う。平行して、中性子照射の加速実験の結果との比較を行ってモデルの妥当性評価を行う。
一方、RT レベルの回路を、制御回路(有限状態機械)とデータパス(演算器系回路)に分解し、その各々に適した解析アルゴリズムの開発を行う。制御回路に関する解析はまず厳密アルゴリズムの開発を行い、続いてより大規模な回路に適用可能な近似アルゴリズムの開発を行う。データパスに関しては、内部の論理

回路の構造に起因するソフトエラーがどのようなパタンで出力に現れるかを確率的にモデル化することで、演算器系回路内部の論理回路を考慮せずに LSI 全体のソフトエラー解析が行えるようにする。モデル化の妥当性評価のために、超並列の計算機サーバーや GPGPU などの計算機資源を使って莫大な論理シミュレーションを行う。

2. ソフトエラー耐性を考慮した論理合成アルゴリズムの研究
　信頼性と冗長性の付加によるオーバーヘッドのトレードオフを考慮するためには大まかに2つのアプローチが考えられる。一つはオリジナルの回路に対してだんだんと冗長性を付加することで信頼性を向上させるやりかたであり、もう一つは多重化された回路から冗長性を削除してゆくことでオーバーヘッドを減らすやりかたである。多くの場合、オリジナルの回路に対して数桁の信頼性の向上が要求されるので前者のやり方は現実ではない。そこで、三重化された回路を初期回路として、許容できる範囲内で信頼性を落としつつ、回路量を削減する手法の検討を行う。

3. CPU のソフトエラー耐性解析ツールの開発
　メモリデバイス中における SEU に着目したソフトエラー耐性評価技術に関する研究から着手する。次に SET を対象としたソフトエラー耐性評価技術について研究を進め、テクノロジノードに依存することなく、CPU のソフトエラー耐性を解析・評価するツールを開発する。

4. VLSI が搭載している価値や信用を守るための設計技術の確立
　まず悪意のある攻撃手法をスキャンベース攻撃とし、攻撃対象回路を DES（Data Encryption Standard）暗号回路として、エラーのモデル化、および指標化を行う。具体的には、攻撃の要因を明確化し、防御手法の提案および種々の防御手法に対する機密情報の漏えいのしにくさを定量化する手法の検討を行う。さらに攻撃対象回路を拡張し、定量化する手法の一般化をめざす。

④研究実施方法

研究チーム内の各グループとは月に数回程度、定期的なミーティングを行っている。基本的にツール開発は本研究グループ内で行っているが、デバイスレベルのソフトエラー発生のメカニズムのモデル化のための情報共有を目的として、神戸大学吉本チームと定期的に打ち合わせを行っている。また、より下位レベルのシミュレーションツールに関する情報共有を九州大学大学院総合理工学研究院渡辺幸信教授と行っている。

B社とはソフトエラーのデバイスシミュレーションおよび照射実験などに関する意見交換を定期的に行っている。

（3）福岡大学グループ

①本研究グループの研究課題、ならびに所属する研究チームの課題との関係

§１．１．① で説明されている、ディペンダブルな LSI システムの設計手法を確立するために、本研究グループはアーキテクチャレベルにおける検討を担当している。§１．１．③ 2) に掲げられている（ウ）各レベルにおけるディペンダビリティの向上技術をアーキテクチャレベルで考案し、それを大規模な設計中に組み込む技術の考案が課題である。それらを設計フローおよび設計ツールに統合するためには、§１．１．③ 2) に掲げられている（ア）階層設計の各レベルにおけるディペンダビリティの評価指標の定義も課題であり、ディペンダビリティ向上技術のモデル化にも取り組んでいる。§１．１．③ 1) で述べられている（a）中性子等に起因するソフトエラーと（b）素子の製造ばらつきや経年劣化によるタイミングエラーを対象とし、アーキテクチャレベルにおいてそれらのエラーのモデル化と指標化を行い、エラーの検出技術とオンライン訂正技術の提案を行う。また、§１．１．③ 2) に掲げられているように、（エ）コストや性能、消費電力等の制約条件とのトレードオフを考慮し、設計全体を最適化するため、ディペンダビリティにおける対費用効果を数値化することも併せて目標とする。

②本研究グループの達成目標

1)タイミングエラーとソフトエラーに関するエラーのモデル化・指標化≪a,b、ア,ウ≫、2)タイミングエラー検出回路設計技術の実用化≪b、ウ≫、3)耐ソフトエアラー・プロセッサアーキテクチャの構築≪a、ウ≫、の三つを達成目標として掲げている。≪≫は、§１．１．③ の（a）～（c）、（ア）～（オ）との対応を示す。

具体的には以下を目標とする。

・ タイミングエラーの振る舞いをアーキテクチャ設計レベルでモデル化するための指標の検討を継続する。

・ ソフトエアラーに関して、性能・電力とディペンダビリティのレンジの違いを考慮出来る指標を策定する。
・ 策定されたタイミングエラーを動的に検出するための回路方式について、回路設計とレイアウト設計を実施し、チップ面積に与える影響を調査する。
・ NBTI（Negative Bias Temperature Instability）等に起因するタイミングエラーを回避する技術について検討する。

③研究のアプローチ

§1．1．② で説明されている設計フローとツールの構築を実現するためには、ディペンダビリティ向上技術とディペンダビリティ評価指標の、両方の開発が必要である。前者については、空間的冗長性を利用してソフトエラーを検出するマルチコアアーキテクチャ、様々な要因で発生するタイミングエラーを予報可能なカナリア・フリップフロップ、そして NBTI 起因経年劣化故障を予防可能なメモリ・アーキテクチャを提案してきた。後者については、前述のマルチコアアーキテクチャを対象に、性能・消費電力・信頼性の間のトレードオフを考察できる評価指標の考案に取り組んできた。本グループでは、まずアイデア出しから始め、様々なシミュレーションを実施することで問題の把握、解決法の考案と評価を行う。いずれの提案も VLSI における基本構成要素（フリップフロップ、SRAM）を対象とした技術であり、適用対象は広範囲に渡る。カナリア・フリップフロップについては小野寺チームが展開研究を実施されている。彼らの論文にも書かれているように、類似研究の Razor がタイミングエラーを検出するのに対し、カナリア・フリップフロップはエラーを予報するという独創性を持つため、プロセッサだけでなくあらゆるディジタル回路に適用可能であり、エラーからの回復回路も必要としないという優位性を持っている。

④研究実施方法

研究チーム内の各グループとは、定期的な研究ミーティングおよび研究合宿を行っている。外部との連携については、これまでに坂井チームとの議論、小野寺チームとの意見交換や、領域アドバイザーのご厚意でC社とD社の研究者・技術者との意見交換を実施してきた。

§2. 研究実施体制

（1）九州大学安浦グループ

①研究分担グループ長：安浦　寛人（九州大学　大学院システム情報科学研究院　教授）（研究代表者）

②研究項目

1. 各グループ間の研究活動を調整し、本チームにおける具体的な研究対象に対する各グループの研究成果を統合し、統合した設計フローの構築に対する基本的な方針として一般化する。
2. 定期的にチーム全体の情報交換の会議を主催し、チーム間の研究活動の調整を行うとともに、領域に対するチーム全体の研究方針をまとめる。
3. チームを代表して関連する研究機関・企業や領域内の他の研究チームとの研究協力交渉の窓口となる。

（2）九州大学松永グループ

①研究分担グループ長：松永　裕介（九州大学　大学院システム情報科学研究院　准教授）（主たる共同研究者）

②研究項目

1. 論理・RT レベルのソフトエラー耐性解析ツールの開発
2. ソフトエラー耐性を考慮した論理合成アルゴリズムの研究
3. CPU のソフトエラー耐性解析ツールの開発
4. VLSI が搭載している価値や信用を守るための設計技術の確立

（3）福岡大学グループ

①研究分担グループ長：佐藤　寿倫（福岡大学　工学部　教授）（主たる共同研究者）

②研究項目

1. タイミングエラーとソフトエラーに関するエラーのモデル化・指標化
2. タイミングエラー検出回路設計技術の実用化
3. 耐ソフトエラー・プロセッサアーキテクチャの構築

§3. 研究実施内容

(文中に番号がある場合は(4－1)に対応する)

(1)研究の成果と自己評価

【平成 22 年度までの成果】

成果 M2.「ソフトエラーのパルス幅ごとの確率モデル生成方法」(九州大学松永グループ)

成果 M3.「ソフトエラーに起因するパルスのラッチ確率の計算モデル」(九州大学松永グループ)

成果 M4.「順序回路におけるソフトエラー伝搬確率の厳密な計算アルゴリズム」(九州大学松永グループ)

成果 M5.「ソフトエラー耐性と面積オーバーヘッドのトレードオフを考慮した論理合成手法」(九州大学松永グループ)

成果 T1.「SEU に対する脆弱性を見積もるシミュレーション技術」(九州大学松永グループ)

成果 T2.「CPU の動作モードにより性能と信頼性のトレードオフを図る技術」(九州大学松永グループ)

成果 T3.「マルチコア CPU の heterogeneity によって性能と信頼性のトレードオフを図る設計技術」(九州大学松永グループ)

成果 T4.「制御信号系列における誤りを検出する動的シグネチャ検査技術」[1)] (九州大学松永グループ)

成果 M6.「スキャンベース攻撃に対する攻撃のモデル化と防御手法」(九州大学松永グループ)

成果 M7.「スキャンベース攻撃に対する防御手法の定量的評価」(九州大学松永グループ)

成果 F1.「耐ソフトエラー・マルチコアアーキテクチャとその評価指標」[19)] (福岡大学グループ)

成果 F2.「カナリア・フリップフロップの置換え位置決定手法」[12),13)] (福岡大学グループ)

成果 F3.「NBTI 起因の経年劣化故障を予防するメモリ・アーキテクチャ」[2)] (福岡大学グループ)

【平成 23 年度の成果】

成果 M1.「ソフトエラーを考慮した設計フローとツールチェイン」(九州大学松永グループ)

①内容

ソフトエラー耐性の解析や、ソフトエラー耐性を向上させる設計を行うための設計フローとそれに関わる EDA のツールチェインの基本概念の提案を行った。あわせて、各設計階層においてソフトエラーの挙動をどのようにモデル化すべきかの指針の検討を行った。提案するツールチェインを図2に示す。この設計フローのインターフェースに従って個々のツール開発を行っている。

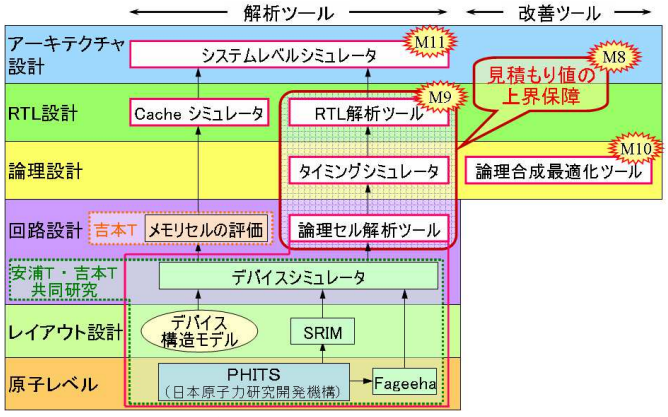


図2 ツールチェイン

②有用性

ソフトエラーの放射線物理レベルの挙動から、デバイスレベル、回路レベル、論理レベル、RT レベルにおける挙動までさまざまなレベルにおいて一貫した指標化を行うことで、各設計階層間で整合性のとれた設計を行うことが可能となる。また、各設計階層におけるソフトエラー対応の EDA ツールのインターフェースを規定することで、個々の要素技術の開発が行えるようになる。

③優位比較

既存研究では、一つの設計階層におけるソフトエラーのモデル化のみを行っているものがほとんどであり、実際の設計フローへの適用を考慮した統合的なツールチェインの提案は皆無である。

成果 M8.「ソフトエラー率の上界を保証する効率的な近似計算手法」(九州大学松永グループ)

①内容

組合せ回路のソフトエラー率を厳密に計算するためには、回路中の各ゲートで発生したパルスが外部出力に伝搬する確率を計算する必要があり、一つのゲートに対する確率計算の手間が回路規模に比例するため、全体で回路規模の2乗に比例した計算の手間を必要とする。今回、複数のゲートに対する確率計算を一度に行うことで、回路規模に比例した手間で全体の確率計算を行う近似アルゴリズムを開発した[5),10),20)]。

②有用性
　組合せ回路に対するソフトエラー率計算を高速に行うことができる。
③優位比較
　回路規模の2乗に比例する手間を必要とする厳密アルゴリズムは数万～数十万ゲート規模の回路に対しては実用的ではない。一方、既存手法として回路規模に比例した手間で近似計算を行うアルゴリズムも提案されているが、こちらは厳密に計算した値に対して過小にも過大にもぶれる可能性がある。対して本手法は常に厳密な値に対する過大見積もりとなる性質があるため、ソフトエラー率の近似値としてより実用的である。

成果 M9.「順序回路のソフトエラー耐性評価用厳密アルゴリズム」(九州大学松永グループ)
①内容
　順序回路中のソフトエラーの影響が外部に伝搬する確率を厳密に計算するアルゴリズムを開発した。今年度は今までの成果を論文にまとめ、発表を行った[14),21),23)]。
②有用性
　一般的な順序回路に対する厳密なソフトエラー耐性の評価が行える。
③優位比較
　現時点で、本手法と同様のエラー伝搬確率を計算するアルゴリズムは知られていない。他の近似計算アルゴリズムで求められる確率が厳密な確率とどの程度の誤差があるかを評価するためにも本手法の意義は大きい。

成果 M10.「多項加算回路の自動合成手法」(九州大学松永グループ)
①内容
　乗算回路の最終段として用いられる多項加算回路を自動合成するアルゴリズムの開発を行った。通常は3入力2出力のキャリーセーブアダーを組合せて多項加算回路を構成するが、本手法ではより入力数の多いGPC(Generalized Parallel Counter)を基本回路として構成することで、遅延時間や消費電力をより自由にコントロールすることが可能となっている[4),11),16)]。
②有用性
　ソフトエラー耐性を考慮した論理合成システムの中で演算系回路を自動合成するために用いる。
③優位比較
　多項加算器の自動合成手法はあまり研究されておらず、また、LUT 型 FPGA を対象にしたものは極めてすくない。本手法は現実的な計算時間で遅延時間や消費電力のトレードオフを考慮した設計を自動で行うもので実用的である。

成果 M11.「スクラッチパッドメモリを用いた組込みシステムの高信頼化技術」(九州大学松永グループ)
①内容
　キャッシュメモリおよび主記憶からなる記憶階層を持つ組込みシステムに、エラー訂正機構を有するスクラッチパッドメモリ(SPM)を付加したシステム(図3)を対象として、信頼性と高速性を両立するコンパイル技術の開発を行った[15)]。キャッシュメモリ、特にL1 キャッシュメモリには高速性が要求され、エラー訂正機構によるアクセスレイテンシの増加が許容されない場合が多い。本研究においては、L1 キャッシュレベルと同等の高速性を実現するメモリとして、エラー訂正機構を有するスクラッチパッドメモリを用い、高速性と信頼性を両立するシステムアーキテクチャを提案した。特定用途向けシステムを対象とし、プログラムとその入力に対して実行プロファイルを取得し、命令およびデータの脆弱性を抽出し、抽出された脆弱性をもとに、脆弱な命令・データはスクラッチパッドメモリに、それ以外を主記憶に配置するコンパイル技術の提案を行った。

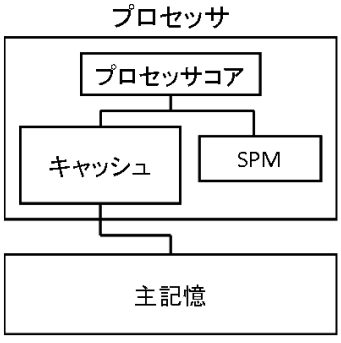


図3　スクラッチパッドメモリを付加した組込みシステム

②有用性
　高度な信頼性を要求される製品群においては、しばしば多額のコストを費やし、製品開発がなされるが、本研究で対象とする製品は、中度の信頼性を要求される製品を対象とするものである。組込みシステム開発においては、高速性や低消費電力性とともに、低価格性が追及される。低価格性を実現するためには、汎用部品を使用することが望ましい。本技術が対象とするシステムは汎用部品から構成でき、製造コストの抑制することが可能である。

③優位比較

2010 年に Lee らは高信頼な小容量キャッシュと低信頼な大容量キャッシュを併用するシステム構成を提案している。Lee らのアプローチにおける「高信頼な小容量キャッシュ」は、我々のアプローチにおける「高信頼なスクラッチパッドメモリ」に相当する。しかしながら、キャッシュは、データを格納する RAM に加えて、タグを格納するテーブル、タグ比較器、および、セットアソシアティブキャッシュであればセレクタから構成され、RAM で構成されるスクラッチパッドメモリと比べて面積効率が低い。同程度の性能、および信頼性であれば、我々のアプローチのほうが低価格に同等のシステムを構築することができる。

成果 M12.「指紋画像による認証アルゴリズムの性能と信頼度の見積もり手法」(九州大学松永グループ)

①内容

機密情報を保持する VLSI のアプリケーションとして、IC カードや携帯型デバイスを用いた生体認証に着目する。個人認証に用いられる情報は、サーバーだけでなくクライアント側にも保持される場合があり、特に生体認証に用いられる身体的特徴に関する登録情報は変更が困難であるため、漏洩しないことが求められる。認証の高速化・高精度化のための様々なアルゴリズムにおいて、何が秘匿すべき情報かを明らかにすることで、機密情報の漏洩しにくさと、漏洩した情報から個人を特定できる可能性によって信頼度を定義することができる。認証アルゴリズムの評価指標として、処理時間や精度に加えて、この信頼度を考える。

本年度は、まず、一般的な個人認証プロトコルについて，個人を特定する情報をサーバーに渡さない手法を提案した [3]。また、具体的に、指紋画像による個人識別のアルゴリズムについて、機密情報の漏洩対策が処理時間や精度に与える影響を見積もった。まず、指紋画像の分類による個人識別の高速化について、既存手法の比較を行い [6),17),18)]、処理時間と認証精度の関係を明らかにした。生体認証に用いる情報そのものに比べ、分類に用いる粗い情報は漏洩による個人特定の可能性は低い。そこで、クライアントが保持する情報を分類のための情報のみにすることで、信頼度の向上が期待できる。一方、クライアントが保持する情報を分類のための情報のみとすることによって、認証精度が低下するため、新たに高速かつ高精度な分類方法を提案した [8),24)]。

②有用性

生体情報による個人識別を含む認証は、社会基盤システムとして広く普及しつつあり、高速化・高精度化そのものが求められている。本研究では、その 2 つの観点に加え、生体情報の漏洩についての信頼度を考慮している。ここで得た指標間の関係によって、認証のための情報をシステムのどの部分に保持し、どれだけ漏洩対策を施すかによって決まる認証システムの信頼度を見積もることができる。

③優位比較

生体情報の漏洩による危険性は Ratha らによって指摘され、一方向の変換による解決方法が提案されている。しかし、認証システムの信頼度を定式化する研究は、調査を行った範囲では見つかっていない。

成果 F4.「カナリア・フリップフロップの置換え位置決定手法の評価」(福岡大学グループ)

①内容

DesignCompiler の出力する Verilog-HDL ネットリストに対してカナリア・フリップフロップの置換え位置決定手法を適用するツールを構築した。東芝よりライセンス購入した MeP プロセッサの RTL を論理合成した後のネットリストに対し、本ツールを用いて提案手法を適用した。さらに配置配線を行い、チップ全体の面積を見積もった。

②有用性

置換える必要のあるフリップフロップは全体の 2%未満であり、チップ面積の増加は約 6%に過ぎないことを確認した [22)]。提案手法を用いるオーバーヘッドは十分小さく、実用化の見通しが立った。

③優位比較

ミシガン大学と ARM のグループは同様の技術である Razor フリップフロップを採用したチップ試作を行っており、やや後塵を拝しているが、フリップフロップ置換えツールについては報告例を知らず、優位にある。

成果 F5.「カナリア・フリップフロップの回路構造の改良」(福岡大学グループ)

①内容

カナリア・フリップフロップの消費電力を削減する新たな回路構造を考案した。

②有用性

従来のフリップフロップと比較して、カナリア・フリップフロップは平均 2.7 倍の電力を消費することが見積もられた。トランジスタ数を削減する最適化を行い、回路構造を改良した。その結果、平均で約 8%の電力削減が可能

になった[22)]。
③優位比較
同様のフリップフロップを採用してプロセッサコア全体の消費電力を削減する報告は多いが、フリップフロップの電力を削減する研究については報告例を知らない。この点で優位に立っている。

成果 F6.「カナリア・フリップフロップによるマルチコアプロセッサの電力削減の評価」(福岡大学グループ)
①内容
カナリア・フリップフロップを用いた消費電力削減手法をマルチコアプロセッサに適用し、効果を評価した。
②有用性
カナリア・フリップフロップを用いた消費電力削減手法は、これまでシングルコア上での評価しか行われていなかった。クアッドコアプロセッサに適用し、20%強の削減効果を確認した[7)]。
③優位比較
マルチコアでの評価報告は未だなされておらず、優位に立っている。

その他の成果
デバイスレベルのソフトエラー発生のメカニズムのモデル化のための情報共有を目的として、神戸大学吉本チームと定期的に打ち合わせを行っているが、それに関する吉本チームの研究成果発表に共同研究者として加わった[9)]。

(2)上記(1)のうち、特筆すべき成果
(1) 特に顕著な成果(科学や技術の新しい分野の展望など)
・成果 M1.「ソフトエラーを考慮した設計フローとツールチェイン」(九州大学松永グループ)
・成果 M8.「ソフトエラー率の上界を保証する効率的な近似計算手法」(九州大学松永グループ)
・成果 M11.「スクラッチパッドメモリを用いた組込みシステムの高信頼化技術」(九州大学松永グループ)
・成果 M12.「指紋画像による認証アルゴリズムの性能と信頼度の見積もり手法」(九州大学松永グループ)
・成果 F5.「カナリア・フリップフロップの回路構造の改良」(福岡大学グループ)

(2) 当初計画で想定外であった重要・新規な展開
なし

§4. 成果発表等

(4－1)原著論文発表
●論文詳細情報

1. Makoto Sugihara, "A Dynamic Continuous Signature Monitoring Technique for Reliable Microprocessors," IEICE Trans. Electron., Vol.E94-C, No.4, pp.477-486, Apr. 2011. (DOI: 10.1587/transele.E94.C.477)
2. Yuji Kunitake, Toshinori Sato and Hiroto Yasuura, "Short Term Cell-Flipping Technique for Mitigating SNM Degradation Due to NBTI," IEICE Trans. Electron., Vol.E94-C, No.4, pp.520-529, Apr. 2011. (DOI: 10.1587/transele.E94.C.520)
3. Toru Nakamura, Shunsuke Inenaga, Daisuke Ikeda, Kensuke Baba and Hiroto Yasuura, "Password Based Anonymous Authentication with Private Information Retrieval," Journal of Digital Information Management, Vol.9, No.2, pp.72-78, Apr. 2011. (DOI: 不明)
4. Taeko Matsunaga, Shinji Kimura and Yusuke Matsunaga, "Synthesis of GPC-based Compressor Trees Targeting Delay and Power Aware Implementation on FPGAs," Proc. 20th International Workshop on Logic and Synthesis 2011 (IWLS 2011), pp.1-8, UC San Diego, CA, USA, June 2011. (DOI: 不明)
5. Taiga Takata and Yusuke Matsunaga, "A Robust CODC-based Heuristic to Extract Observability Don't Care Set," Proc. 20th International Workshop on Logic and Synthesis 2011 (IWLS 2011), pp.105-111, UC San Diego, CA, USA, June 2011. (DOI: 不明)
6. Ali Ismail Awad and Kensuke Baba, "Fingerprint Singularity Detection: a Comparative Study," Second

International Conference on Software Engineering and Computer Systems (ICSECS 2011), Kuantan, Malaysia, June 2011. published in the "Software Engineering and Computer Systems, Communications in Computer and Information Science, Vol.179, pp.122-132, Springer-Verlag, June 2011." (DOI: 不明)

7. Toshinori Sato, Takahito Yoshiki and Takanori Hayashida, "Multicore Power Management Utilizing Error-Predicting Flip-flop," 4th International Workshop on Multi-Core Computing Systems (MuCoCoS 2011) in conjunction with International Conf. on Complex, Intelligent, and Software Intensive Systems (CISIS 2011), pp.606-611, Seoul, Korea, June 2011. (DOI: 10.1109/CISIS.2011.100)
8. Ali Ismail Awad and Kensuke Baba, "An Application for Singular Point Location in Fingerprint Classification," International Conference on Digital Information Processing and Communications (ICDIPC 2011), Ostrava, Czech Republic, July 7-9, 2011. published in the "Digital Information Processing and Communications, Communications in Computer and Information Science, Vol.188, pp.262-276, Springer-Verlag, July 2011." (DOI: 不明)
9. Shusuke Yoshimoto, Takuro Amashita, Daisuke Kozuwa, Taiga Takata, Masayoshi Yoshimura, Yusuke Matsunaga, Hiroto Yasuura, Hiroshi Kawaguchi and Masahiko Yoshimoto "Multiple-Bit-Upset and Single-Bit-Upset Resilient 8T SRAM Bitcell Layout with Divided Wordline Structure," Proc. 17th International On-Line Testing Symposium 2011 (IOLTS 2011), pp.151-156, Athens, Greece, July 2011. (DOI: 10.1109/IOLTS.2011.5993829)
10. Taiga Takata and Yusuke Matsunaga, "A Robust Algorithm for Pessimistic Analysis of Logic Masking Effects in Combinational Circuits," Proc. 17th International On-Line Testing Symposium 2011 (IOLTS 2011), pp.246-251, Athens, Greece, July 2011. (DOI: 10.1109/IOLTS.2011.5994537)
11. Taeko Matsunaga, Shinji Kimura and Yusuke Matsunaga, "Power and Delay Aware Synthesis of Multi-Operand Adders Targeting LUT-based FPGAs," Proc. International Symposium on Low Power Electronics and Design 2011 (ISLPED 2011), pp.217-222, Fukuoka Convention Center, Fukuoka, Japan, Aug. 2011. (DOI: 10.1109/ISLPED.2011.5993639)
12. Yuji Kunitake, Toshinori Sato, Hiroto Yasuura, and Takanori Hayashida, "A Selective Replacement Method for Timing-Error-Predicting Flip-Flops," Proc. 54th International Midwest Symposium on Circuits and Systems (MWSCAS), [P03_1006] 4 pages, Seoul, Korea, Aug. 2011. (DOI: 10.1109/MWSCAS.2011.6026267)
13. Yuji Kunitake, Toshinori Sato, Hiroto Yasuura, and Takanori Hayashida, "Possibilities to Miss Predicting Timing Errors in Canary Flip-flops," Proc. 54th International Midwest Symposium on Circuits and Systems (MWSCAS), [P16_1002] 4 pages, Seoul, Korea, Aug. 2011. (DOI: 10.1109/MWSCAS.2011.6026656)
14. Masayoshi Yoshimura, Yusuke Akamine and Yusuke Matsunaga, "A Soft Error Tolerance Estimation Method for Sequential Circuits," Proc. International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems 2011 (DFT 2011), pp.268-276, Vancouver, Canada, Oct. 2011. (DOI: 10.1109/DFT.2011.22)
15. 森本 喬, 小林 良太郎, 杉原 真, "スクラッチパッドメモリ搭載組込みシステムのソフトエラー耐性を向上するメモリオブジェクト配置手法," 情報処理学会組込みシステムシンポジウム 2011 (ESS2011), pp.12.1-12.10, 国立オリンピック記念青少年総合センター(東京都), Oct. 2011 . (DOI: 不明)
16. Taeko Matsunaga, Shinji Kimura and Yusuke Matsunaga, "Multi-Operand Adder Synthesis Targeting FPGAs," IEICE Trans. Fundamentals, Vol.E94-A, No.12, pp.2579-2586, Dec. 2011. (DOI: 10.1587/transfun.E94.A.2579)
17. Ali Ismail Awad and Kensuke Baba, "FingRF: A Generalized Fingerprints Research Framework," International Conference on Advances in Information Technology and Communication (AIT 2011), Amsterdam, Netherlands, Dec. 2011. published in the "Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, pp.1-6, Springer-Verlag, Dec. 2011." (DOI: 不明)
18. Ali Ismail Awad and Kensuke Baba, "Singular Point Detection for Efficient Fingerprint Classification," International Journal of New Computer Architectures and their Applications (IJNCAA), Vol.2, No.1, pp.1-7, SDIWC, Jan. 2012. (DOI: 不明)
19. Toshinori Sato, Hideki Mori, Rikiya Yano and Takanori Hayashida, "Importance of Single-Core Performance in the Multicore Era," 35th Australasian Computer Science Conference (ACSC 2012), pp.107-113, Melbourne, Australia, Jan. 2012. (DOI: なし)
20. Taiga Takata and Yusuke Matsunaga, "A Robust Algorithm for Pessimistic Analysis of Logic Masking Effects

in Combinational Circuits," IPSJ Trans. System LSI Design Methodology, Vol.5, pp.55-62, Feb. 2012. (DOI: 10.2197/ipsjtsldm.5.55)
21. Masayoshi Yoshimura, Yusuke Akamine and Yusuke Matsunaga, "An Exact Estimation Algorithm of Error Propagation Probability for Sequential Circuits," IPSJ Trans. System LSI Design Methodology, Vol.5, pp.63-70, Feb. 2012. (DOI: 10.2197/ipsjtsldm.5.63)
22. Ken Yano, Takahito Yoshiki, Takanori Hayashida and Toshinori Sato, "An Automated Design Approach of Dependable VLSI Using Improved Canary FF," 7th International Workshop on Unique Chips and Systems (UCAS-7), pp.34-39, New Orleans, Louisiana, USA, Feb. 2012. (DOI: なし)
23. Taiga Takata and Yusuke Matsunaga, "A Quantitative Analysis of Soft Error Propagation in Sequential Circuits," 8th Workshop on Silicon Errors in Logic - System Effects (SELSE8), University of Illinois, USA, Mar. 2012. (DOI: 不明)
24. Ali Ismail Awad and Kensuke Baba, "An Application of Singular Point Location in Fingerprint," International Journal of Digital Information and Wireless Communications (IJDIWC), SDIWC, in press. (DOI: 不明)

(4－2)知財出願

① 平成23年度特許出願件数(国内 0 件)
② CREST 研究期間累積件数(国内 1 件)