平成 21 年度
実績報告

「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

安浦　寛人

九州大学　大学院システム情報科学研究院・教授

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. 研究実施の概要

今年度は、ソフトエラー、タイミングエラー、外部からの悪意のある攻撃（情報セキュリティ）を対象に、エラー要因の解析・モデル化と対策技術の開発を行った。

ソフトエラーに関しては、順序回路におけるエラー伝搬の振る舞いを確率的モデルでモデル化し、エラー率を推定する手法の開発を行った。また、FPGAを用いて実装されるシステムにおいて、構成データのリロードによりシステムに対するエラー耐性を高める技術の開発を行った。また、神戸大学の吉本チームと共同で、論理セルおよびSRAMのソフトエラー率解析のためのシミュレーション環境の基盤整備を行った。今後、チップ試作と照射実験を行い、シミュレーションモデルの妥当性検証を行う予定である。個々の技術の開発・評価を加速させるとともに、LSI システム全体の設計フローに組み込める形で統合化を行うことが今後の課題である。

タイミングエラーに関しては、NBTI(Negative Bias Temperature Instability)起因のタイミングエラーを軽減する SRAM アーキテクチャを検討し、シミュレーションにより評価した。また、回路中の各 FF に対して、遅延変動に関する頑強度の解析法を検討した。今後、ツール化を視野に入れた解析モデルの構築を目指す。

情報セキュリティに関しては、回路のセキュリティの定量化のためのモデルを構築した。具体的には DES と呼ばれる暗号回路に対して、スキャンベース攻撃に対する機密情報の漏洩のしにくさを相互情報量で定量化するモデルを提案した。今後はそのモデルを他の暗号回路へ応用し、防御手法を適用した回路の面積やテスタビリティとのトレードオフで評価する。

§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、教授)

②研究項目

1. LSI に搭載されている価値や信用を守るための設計技術の確立

(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、准教授)

②研究項目

1. 論理レベルのソフトエラー耐性解析ツールの開発
2. RT レベルのソフトエラー耐性解析ツールの開発
3. 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
4. LSI に搭載され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、教授)

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

(4)「豊橋科学技術大学」グループ

①研究分担グループ長:杉原　真(豊橋技術科学大学、准教授)

②研究項目

1. ソフトエラーに関するエラーのモデル化・指標化
2. 信頼性と低消費エネルギー性との間に存在するトレードオフの関係の明示

§3. 研究実施内容

(文中に番号がある場合は§4(4－1)に対応する)

本研究では、ディペンダビリティを考慮した LSI の設計を行う工学的な枠組みとしての設計フローの確立およびツールチェインの開発を行う。現在、対象として考えているテーマは以下のとおりである。

(1) ソフトエラー対策を考慮した設計技術の確立

(2) 回路のさまざまなばらつきを考慮した設計技術の確立

(3) LSI に搭載されている価値や信用を守るための設計技術の確立

以下に、各テーマ毎の当該年度の研究実施内容を記す。

(1) ソフトエラー対策を考慮した設計技術の確立

ソフトエラーに対する信頼性の指標としてはVLSIやシステム全体に対するソフトエラー率が考えられるが、個々のデバイスにおけるソフトエラー率から全体のソフトエラー率を厳密に算出することは計算量的に非常に困難であり、現実的ではない。そこで、設計の各階層においてソフトエラーの振る舞いの適切なモデル化を行い、解析ツール(アナライザ)および合成・最適化ツール(エンハンサ)の開発を進めた。

(1-1) 論理回路・RT レベル

内部に記憶を持つ順序回路内部でソフトエラーが起きた場合、ソフトエラーの影響が直接、外部出力に現れるとは限らず、数クロックサイクル後に影響が顕在化する場合がある。そのため順序回路に対するソフトエラーの振る舞いを厳密に解析することは計算量的に困難な問題である。今年度は順序回路を確率的に動作するマルコフモデルとみなしてソフトエラーの影響が外部に伝搬する確率を求める厳密アルゴリズムと近似手法の開発を行った。

厳密アルゴリズムで解決すべき問題はソフトエラーが起きた状態から到達可能な状態の全列挙である。フリップフロップ数が 10 程度の順序回路でも単純な方法では 100 万状態を調べなければならずほとんど不可能であった。これを二分決定グラフと呼ばれる論理関数を効率よく処理するデータ構造を用いることでフリップフロップ数が17～18程度の回路に対して適用可能な厳密アルゴリズムを開発した。

近似手法はある程度の精度を保ちつつより大きな回路に対して適用することを目的にしている。具体的には、正常な振る舞いをしている場合に取りうる状態の定常確率の見積もりと、エラーの影響が複数クロックにまたがって伝搬する確率の見積もりを工夫することで、厳密アルゴリズムよりはるかに少ない計算量で処理をできる。これらの順序回路に対するソフトエラーの振る舞いの解析手法に関しては、未だ確立した手法は存在していない。当研究グループで検討している手法の実用化の目途が立てば大きな貢献になると思われる。

部分的な冗長化を行うことで、面積・消費電力の増加を抑えつつ信頼性を向上させる手法に関しては、既存手法とはまったく異なったアプローチで、特定の入力ベクタに対してはエラー訂正を行わないことで訂正回路の面積を削減する手法を提案した。部分回路を 3 重化する既存手法では面積オーバーヘッドとソフトエラー耐性がほぼ比例するため効果的なトレードオフをとることが難しいが、提案手法ではごく一部の入力ベクタに対する耐性を落とすだけで訂正回路の面積を数分の 1 に縮小できる回路も確認されており、有効な手法と思われる。

信頼性を考慮した論理合成を実現するための基礎技術として、FPGAを対象にした論理合成技術の高性能化の研究[3],[6],[8],[12]および、算術演算回路の合成技術[7],[9],[13]の開発を行っている。FPGA 向け論理合成技術は既存研究と同程度の処理時間で 5%～10%程度の面積削減を実現している。算術演算回路に関しては、従来あまり自動合成対象ではなかった専用算術演算回

路の合成アルゴリズムを提案した。

(1-2)　アーキテクチャレベル

アーキテクチャ設計レベルでソフトエラー検出技術が提案されているが、ディペンダビリティの指標が曖昧なため設計階層を跨いだ効果を明らかにすることが困難である。そこで、まず、アーキテクチャ設計レベルでディペンダビリティを測るための指標を再定義するために AVF（Architectural Vulnerability Factor）を精査した。続いて、その指標に基づき、性能や消費電力とのトレードオフを検討できる指標を構築中である。性能や電力と比べてディペンダビリティのレンジが狭く、既存の EDP（Energy Delay Product）等を元に拡張するのでは不十分であることが判っている。

マルチコアプロセッサをベースにソフトエラーを検出可能なアーキテクチャの考案を検討していたが、ソフトエラー検出を目的とするだけではマルチコアアーキテクチャはオーバスペックであることを痛感した。アーキテクチャの洗練が必要であることが判明した。

(1-3)　メモリシステム

今年度は、高信頼性が要求される組込みシステム向けマルチコア CPU を自動合成する VLSI 設計技術に関する研究を遂行した[1],[10]。本年度の研究においては、SRAM が特に SEU (Single Event Upset)を生じやすい点を考慮し、信頼性制約（与えられたタスクセットを実行する間に生じる SEU 数の上限値）の下で、マルチコア CPU を構成する CPU コア数、CPU コア毎のキャッシュメモリのサイズ、タスクの CPU コアへの割り当て、及びタスクの実行開始時刻を最適に決定し、チップ面積を最小化する設計技術に関する提案を行った。また、フィージビリティスタディのために、マルチコア CPU を自動合成するソフトウェアの開発を行った。

また、FPGA 上に複数のモジュールを搭載するシステムにおいて、構成データをリロードすることにより構成データ上の SEU を除去する技術に関する研究を行った。モジュール毎に要求される信頼性が異なる仮定の下で、モジュール毎にリロード頻度を設定し、停止時間が最小となるモジュール配置手法の提案を行った。

(1-4)　ディペンダビリティを考慮した設計フローの確立およびツールチェイン開発

今年度は論理・RT レベル、アーキテクチャレベル、メモリシステムにおけるツールの機能強化および実用性の評価を行ったが、統合的な評価は例題となる適切なベンチマークがないなどの問題があり、進んでいない。今後早急にシステム全体としてのソフトエラー率評価が行える環境の構築を行う。

(1-5)　実験

神戸大学の吉本チームと共同で、デバイスレベルでのソフトエラーの振る舞いのシミュレーション、および照射実験に関する情報収集と基盤技術の整備を行った。具体的には、デバイスシミュレータおよびソフトエラー専用シミュレータを導入し、中性子衝突によるソフトエラーの振る舞いを

解析する環境の整備を行った。本年度は，このシミュレーション環境の整備のための計算機サーバー、および関連ソフトウェアのライセンス購入に予算を重点的に配分した。

(2) 回路のさまざまなばらつきを考慮した設計技術の確立

個々のトランジスタの遅延ばらつきが論理回路でのタイミング違反に至る過程を評価するための指標を検討する。それを与えるための解析技術も重要である。特に遅延ばらつきに対する FF の頑強度の解析法を検討し、頑強度に基づいて FF をタイミング違反回避 FF に置換する処理を検討する。最終的にはツール化を視野に入れた解析モデルの構築を目指す。

NBTI（Negative Bias Temperature Instability）起因のタイミング違反に着目し、今年度は特に SRAM セルの NBTI 軽減アーキテクチャを検討した[14]。既存の経年劣化モデルを採用しているが、極めて簡易でありながら効果の高い方式を考案し、シミュレーションにより評価した。遅延ばらつきの評価環境については、アーキテクチャレベルで評価することの問題を整理し、アーキテクチャレベルとゲートレベルで協調して評価する環境を検討した[2]。

(3) LSI に搭載されている価値や信用を守るための設計技術の確立

最近は、電子マネーやカードキーのように LSI のハードウェアそのものとは別に LSI に付加的な価値や信用が与えられていることがある。このような LSI においては通常の故障やソフトエラーの対策以外に、外部から悪意のある攻撃の対策も講じる必要がある。悪意のある攻撃とその対策の具体的な例として、LSI の製造テストを行うために用意されているスキャンパスを経由した LSI 内部の機密情報を外部から取得しようとする攻撃と、その機密情報の外部への漏洩を防御する対策がある。今年度は DES と呼ばれる暗号回路に対して、機密情報の漏洩のしにくさを表す評価モデルを考案した。またこのモデルを用いて、既存の防御手法の有効性を定量的に比較評価した。さらにスキャンパスを用いないまたはスキャンパスを経由する箇所を削減する手法の検討として、多時刻の動作を考慮した順序回路に対するテスト方法の検討を行った。多時刻の動作を考慮すると、考慮しない場合より多くのテスト不能故障を同定できることがわかった[16]。

LSI の製造過程や実使用時に得られる様々なデータの統計的処理により、LSI における故障を検知または予測する手法について、関連研究の文献調査を行った。テスト技術に関する世界最大の会議である IEEE International Test Conference では、特にここ数年、テスト応答データの統計的処理により選別された異常値（outlier）を用いた技術についての論文の投稿が増加している。これらの技術について、実使用時に得られるデータへの応用を検討した。

LSI に価値や信用が付加されるシステムの例として、IC カードによる認証やアクセス制御システムを考え、鍵の概念を用いた場合のコストモデルを提案した[5]。また、悪意のある攻撃に対する対策として、IC カード内に固定された秘匿情報を持たない認証モデル[15]と、認証の際の問い合わせ内容からの情報漏洩を防ぐ認証モデルを提案した[4],[17]。また、信頼性が求められるシステムの一例として、学術情報等を恒久的に保存・管理するシステムの一形態を提案した[11]。

§4. 成果発表等

(4－1) 原著論文発表

- 論文詳細情報

[1] M. Sugihara, “Reliability inherent in heterogeneous multiprocessor systems and task scheduling for ameliorating their reliability,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E92-A, No. 4, pp. 1121-1128, April 2009. (10.1587/transfun.E92.A.1121)

[2] Yuji Kunitake, Kazuhiro Mima, Toshinori Sato and Hiroto Yasuura, “Enhancements of a Circuit-level Timing Speculation Technique and their Evaluations Using a Co-simulation Environment, ” IEICE Transactions on Electronics, Vol. E92-C, No. 4, pp.483-491, April 2009. (10.1587/transele.E92.C.483)

[3] Taiga Takata and Yusuke Matsunaga, “An efficient cut enumeration for depth-optimum technology mapping for LUT-based FPGAs,” ACM Great Lakes Symposium on VLSI, pp.351-356, May, 2009. (10.1145/1531542.1531622)

[4] Toru Nakamura, Shunsuke Inenaga, Daisuke Ikeda, Kensuke Baba and Hiroto Yasuura, “Anonymous Authentication Systems Based on Private Information Retrieval”, The First Conference on Networked Digital Technologies (NDT2009), pp.53--58, Jul, 2009.(/)

[5] Tomomi Yamasaki, Shunsuke Inenaga, Daisuke Ikeda and Hiroto Yasuura, “Modeling Costs of Access Control with Various Key Management Systems”, In Proc. The 2009 International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA’09), Vol.1, pp.676--682, Jul, 2009. (/)

[6] Taiga Takata and Yusuke Matsunaga, “Area Recovery under Depth Constraint for Technology Mapping for LUT-based FPGAs”, IPSJ Transactions on System LSI Design Methodology, Vol. 2, pp.200-211. Aug, 2009. (10.2197/ipsjtsldm.2.200)

[7] Taeko Matsunaga, Shinji Kimura and Yusuke Matsunaga, “Framework for Parallel Prefix Adder Synthesis Considering Switching Activities,” IPSJ Transactions on System LSI Design Methodology, Vol. 2, pp.212-221. Aug, 2009. (10.2197/ipsjtsldm.2.212)

[8] Taiga Takata and Yusuke Matsunaga, “A Power-aware Post-processing under depth constraint for LUT-based FPGA Technology Mapping”, Proc. of International Workshop on Logic and Synthesis 2009, pp.332-339, Aug, 2009. (/)

[9] Taeko Matsunaga, Shinji Kimura and Yusuke Matsunaga, “Multi-Operand Adder Synthesis on FPGAs using Generalized Parallel Counters”, Proc. of International Workshop on Logic and Synthesis 2009, pp.222-228, Aug, 2009. (/)

[10] M. Sugihara, “Heterogeneous multiprocessor synthesis under performance and reliability constraints,” Proc. EUROMICRO Conference on Digital System Design, pp. 333-340,

Patras, Greece, Aug, 2009.(10.1109/DSD.2009.217)

[11] Kensuke Baba, Eisuke Ito, Naomi Yoshimatsu, Nami Hoshiko and Kazuaki Murakami, “A Model of Publication of Scholarly Papers on Institutional Repositories”, DRF International Conference 2009 Conference Proceedings, Dec, 2009. (/)

[12] Taiga Takata and Yusuke Matsunaga, “ Efficient Cut Enumeration Heuristics for Depth-Optimum Technology Mapping for LUT-Based FPGAs”, IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E92-A No.12, pp.3268-3275, Dec, 2009. (10.1145/1531542.1531622)

[13] Taeko Matsunaga, Shinji Kimura and Yusuke Matsunaga, “Multi-Operand Adder Synthesis on FPGAs using Generalized Parallel Counters,” Proc. of 15th Asia and South Pacific Design Automation Conference 2010, pp.337-342, Taipei, Taiwan, Jan. 2010. (/)

[14] Yuji Kunitake, Toshinori Sato and Hiroto Yasuura, “Signal Probability Control for Relieving NBTI in SRAM Cells, ”11th International Symposium on Quality Electronic Design, pp660-666, San Jose, USA, March 2010. (/)

[15] Toru Nakamura, Shunsuke Inenaga, Daisuke Ikeda, Kensuke Baba and Hiroto Yasuura, “An Identifiable Yet Unlinkable Authentication System with Smart Cards for Multiple Services, ” The 2010 International Conference on Computational Science and Its Applications (ICCSA 2010), pp236-251, Vol.6019, No.4, LNCS, March 2010.

[16] Masayoshi Yoshimura, Hiroshi Ogawa, Toshinori Hosokawa and Koji Yamazaki, “Evaluation of Transition Untestable Faults Using a Multi-Cycle Capture Test Generation Method,”13th IEEE International Symposium on Design and Diagnostics of Electronic circuits & systems, Vienna, Austria, April 2010, accepted.

[17] Toru Nakamura, Shunsuke Inenaga, Daisuke Ikeda, Kensuke Baba and Hiroto Yasuura, “Password Based Anonymous Authentication with Private Information Retrieval”, Journal of Digital Information Management, in press.