平成 20 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）、を対象として、エラー要因の解析・モデル化と対策技術の開発を行っている。ソフトエラーに関しては、信頼性の向上を目的としたマルチプロセッサシステム向けタスクスケジューリング手法と論理レベルのソフトエラー解析ツールの開発を行った。タイミングエラーに関しては、冗長な FF を用いてタイミングエラーを予報する方式の開発を行い、基礎的な実験データの収集を行った。情報セキュリティに関しては、LSI のテスト容易化のために用いられているスキャン FF 方式がセキュリティホールになっている問題を指摘し、一部の FF の読み出し・書き込み機能を制限することで、情報漏洩の危険性を低下させる手法を開発した。今後、これらの個別技術の開発と並行して、設計階層および対象となるエラー要因を統合的に扱う総合的な設計フローの開発を目指す。

2. 研究実施内容（文中にある参照番号は 4.(1)に対応する）

さまざまな種類のエラー(製造故障、ソフトエラー、タイミングエラー、設計誤り、不完全な仕様に基づく誤り、悪意のある攻撃など)に対して、統一的な視点からディジタル VLSI システムのディペンダビリティを確保するための設計技術の確立を目指して、 ディペンダビリティの解析と対策回路の合成を行う EDA ツールを核とした、ディペンダブル LSI 向け設計フロー(図 1)を構築する。現在は具体的なエラー要因として、1) ソフトエラー、2)タイミングエラー、3)外部からの悪意のある攻撃、の 3 点に着目して、これら個別の問題から、エラーのモデル化・解析、ツール構築、フロー構築へと展開する。

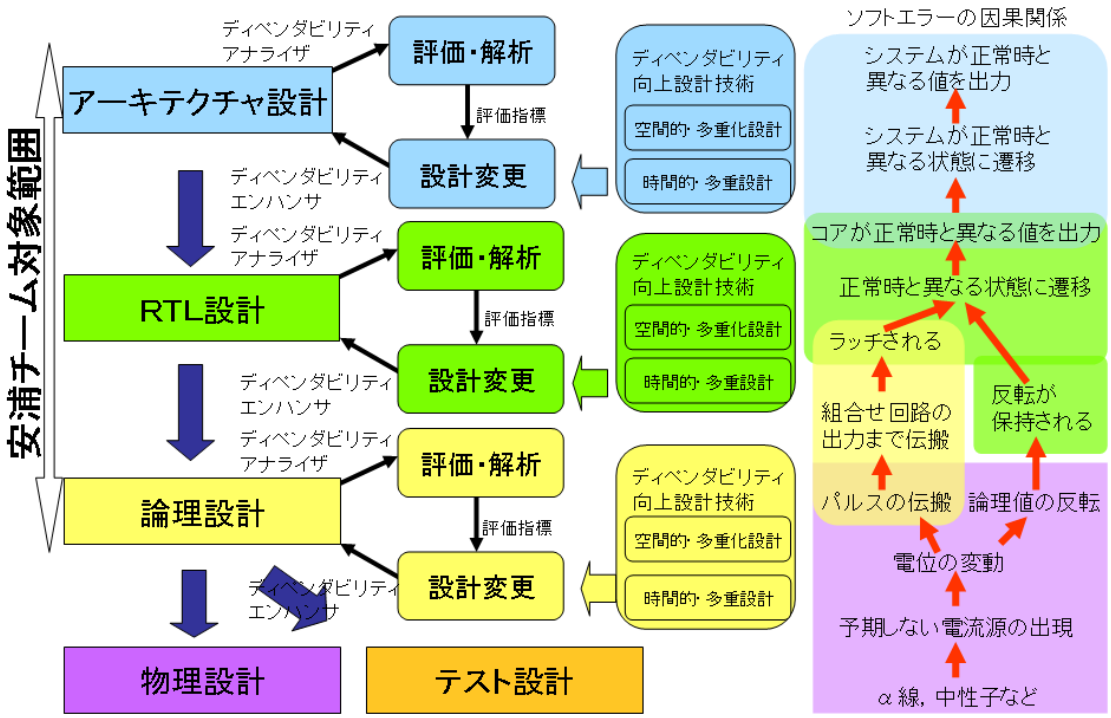

図 1 ディペンダブル VLSI 向け設計フロー

［ソフトエラー］

現状では、デバイスレベルや回路レベルにおいてソフトエラーの振る舞いを解析する手法はいくつか提案されている。論理レベルやアーキテクチャレベルにおいては、計算時間と精度の両方の要求を満たす実用的な手法は確率しているとは言い難い。

また、信頼性のためにかけられるコストも限られているので、各設計階層においてどれだけのエラー耐性を確保すればよいかというトレードオフ問題を考えなければならない。今後、この基本方針にそって、各階層におけるエラー動作のモデル化、解析技術、対策用の EDA 技術の確立を行う。今年度は以下の項目について開発を行った。

－ ソフトエラー耐性を考慮したマルチプロセッサ合成技術の開発

ソフトエラー耐性制約及び実時間制約を考慮し、マルチプロセッサのチップ面積を最小化するマルチプロセッサ合成技術に関する研究を行った。

－ 論理レベルのソフトエラー耐性解析ツールの開発

組み合わせ論理回路の構造によってソフトエラーの影響の伝搬が阻害されるロジックマスキング効果の解析ツールの高速化を行った。既存の高速な近似解析ツールの数倍～十数倍程度の計算時間で厳密な解析を行うことが可能となっている。また、既存の近似解析ツールでは外部出力寄りの一部の回路を多重化したような回路の解析時に非常に大きな計算誤差を含むことを明らかにした。

今後、厳密手法の更なる高速化は難しいと思われるので、より精度の高い高速な近似手法の

検討を行う。

－ 信頼性／性能／電力間のトレードオフを考慮できるアーキテクチャの検討

マルチコアプロセッサ上でソフトエラーを検出できるアーキテクチャを検討しているが、ソフトエラー耐性を備えるだけではなく性能と電力への影響を考察している。シミュレーションによる初期評価の結果、信頼性の尺度が曖昧なためにトレードオフ検討が困難であることが判明した。早急に信頼性を図る尺度を定義することが必要である。

［タイミングエラー］

・タイミング違反回避 FF の実用性に関する検討

チップ面積に与える影響の調査と、タイミング違反を見逃す可能性の調査である。前者については、必要となるタイミング違反回避 FF の数を抑える方式を検討した。二つの商用プロセッサの回路情報を用いて評価したところ、いずれの場合もチップ面積の増加は 10%程度に抑えられることが確認出来た。後者については、桁上げ保存加算器を用いて調査した結果、非常に小さな確率ではあるがタイミング違反を見逃す可能性があることが確認された。この問題を回避する方策の検討が必要である。

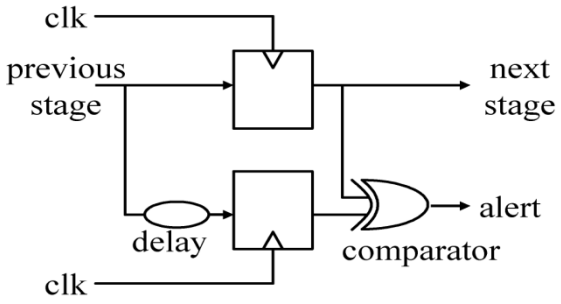

図 2 タイミングエラー予報回路

［テスト容易性とセキュリティのトレードオフの検討］

通常の VLSI は製造時故障の検査を容易にするためにスキャン方式を採用している。このスキャン方式を用いることで、テスト時には回路中の全ての FF の値を読み書きすることが可能となっている。これは暗号用 LSI のようにチップ内部に秘密情報を保持している場合には、重大なセキュリティホールとなりうることが分かっている。そこで一部の FF に対して、スキャンによる読み出し、書き込みの一方もしくは両方を制限する事で、チップ内部に保持している秘密情報が漏洩する危険を下げる手法を、DES アルゴリズムのハードウェア実装例に対して適用し、テスト容易性の評価を行ったところ、秘密情報に関係する FF の読み出し、実用的なテストカバー率を満たすことがわかったが、セキュリティの評価尺度が明確ではなった。そこで本年度は、H19 年度に提案した手法に対するセキュリティの指標のモデル化とそのモデルを用いたセキュリティ評価を行った。セキュリティ指標のモデル化は、スキャン方式によって得られる情報から秘密情報の候補数がどの程度絞り込めるかという尺度を用いて行った。そのモデル化を用いてセキュリティの尺度を評価した結果、提案した防御法では秘密情報の候補数が絞り込めないことがわかった。今後、防御法に対して秘密情報の漏洩に対してどれだけ効果的かを定量的に評価する方法の確立を行う。

［実証実験］

フィールド試験のためにイベントの発生確率と回路規模に関する詳細な検討を行ったところ、試作予定の回路規模では有意の観測結果を得るための実験期間が研究期間を超える可能性が高いので試作を断念した。また、デバイス／素子レベルのソフトエラー研究者との交流を行いデータや事例を分析した。

一方、ソフトエラーの影響を回路／システムレベルで見積もるための解析に大量のシミュレーションが必要となるので、計算パワーの増強を計った。

－ 学内外の IC カード等を利用したフィールド実験からの情報の収集と解析

IC カードによる認証実験で発生した各種障害情報を収集した。原因は、システムレベルからデバイスレベルまで広範にわたっており、メーカーや運用者に解析をしてもらっている。結果は、本研究のためのフィールドデータとして今後利用する計画である。

なお、次年度からは IC カードが学内の正式サービスとなるので、実験は今年で終了する。引き続き、障害データの供給は受けいれる体制は整える。

3. 研究実施体制

(1)「九州大学」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、教授）

②研究項目

1. タイミングエラー、ソフトエラー、人為的攻撃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
3. ツールチェインの開発
4. 実証実験

(2)「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、講師）

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

4. 研究成果の発表等

（1） 論文発表 （原著論文）

1. M. Sugihara, T. Ishihara, and K. Murakami, ″Reliable cache architectures and task scheduling for multiprocessor systems,″ IEICE Transactions on Electronics, Vol. E91-C, No. 4, pp. 410-417, April 2008.
2. 佐藤 寿倫, 舟木 敏正, ``マルチコアプロセッサのための電力・性能間トレードオフを考慮したディペンダビリティ選択法'',情報処理学会論文誌, Vol.49, No.6, pp.2005-2015, June 2008.

3. 佐藤 寿倫, 国武 勇次,``ばらつき耐性を持つカナリア FF を利用したデザインマージン削減による省電力化'', 情報処理学会論文誌, Vol.49, No.6, pp.2029-2042, June 2008.
4. 渡辺 慎吾, 橋本 昌宜, 佐藤 寿倫, ″タイミング歩留まり改善を目的とする演算カスケーディング″, 情報処理学会論文誌コンピューティングシステム, Vol.1, No.2, pp.12-21, Aug. 2008.
5. Toshinori Sato, ``A Simple Mechanism for Collapsing Instructions under Timing Speculation'', IEICE Transactions on Electronics, Vol.E91-C, No.9, pp.1394-1401, September 2008.
6. M. Sugihara, ″Reliability inherent in heterogeneous multiprocessor systems and task scheduling for ameliorating their reliability,″ to appear in IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E92-A, No. 4, April 2009
7. Yuji Kunitake, Kazuhiro Mima, Toshinori Sato, Hiroto Yasuura, ″Enhancements of a Circuit-level Timing Speculation Technique and their Evaluations Using a Co-simulation Environment″, IEICE Transactions on Electronics, pp.483-491, E92-C, No.4, April 2009.

(2) 特許出願

平成 20 年度 国内特許出願件数：0 件（CREST 研究期間累積件数：0 件）