平成 19 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 システムのディベ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．

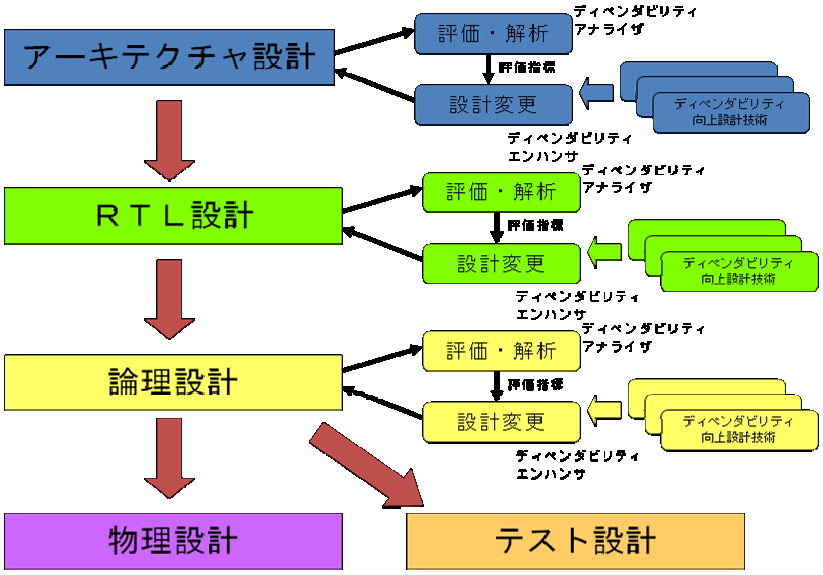

図 1　ディペンダブル LSI 向け設計フロー

[ソフトエラー]

協力企業との情報交換および現象の解析や，メモリデバイスのソフトエラー率測定法(JEDEC JESD89A，JEITA などの業界標準)に関する調査，および，加速試験やフィールド試験などの測定法の調査や，国際会議における技術動向の調査を踏まえて基本的な方針の策定を行った．現状では，デバイスレベル，回路レベル，論理レベル，アーキテクチャレベル，システムレベルなどさまざまな階層でソフトエラーの対策のアイデアが提案されているが，基幹サーバーシステムなどのいくつかの例外を除いては、それを統合的に組み合わせた構成法は確立していない．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向けタスクスケジューリング手法の開発

ソフトエラー耐性の異なる複数のプロセッサ間で実行するタスクをうまく割り当てることで，タスクの実行に関するリアルタイム制約を満たしつつ，エラー耐性が最大になるようなタスクスケジューリングを求める手法を開発した[4]．

- 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の効果を解析するためのツールの開発を行った．重複して計算される部分回路を極力減らすヒューリスティックにより従来技術より 1.5～2 倍程度の高速化を達成している．

[タイミングエラー]

従来は，タイミングに関して最悪の仮定のもとで回路が正しく動くことを保証して設計を行っていたが，テクノロジの微細化に伴い考慮すべきマージンが増大し，適切な設計を行うことが困難になっている．そこで，設計時の制約を緩くして動作時にリアルタイムにタイミングエラーを検知する手法の確立を目指している．今年度は，機能的には等価だが動作タイミングをずらした二つのFFの挙動から組み合わせ回路のタイミングエラーを予報する方式の開発を行った．FF間のタイミングのずれを大きくすれば，タイミングエラーの見逃しは少なくなるが，高速に動作させることが難しくなる．一方，タイミングのずれを小さくすれば，タイミングエラーの見逃しが多くなる．いくつかの例題でこれらの間のトレードオフを測定した．今後これらの知見をもとに実用的な設計手法の構築を行う．

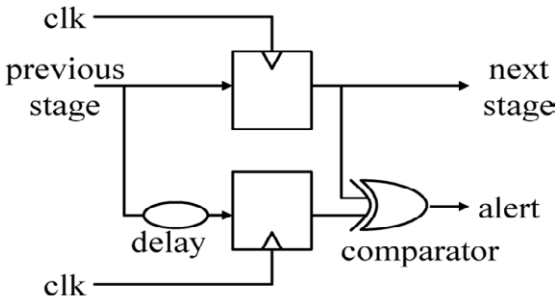

図 2　タイミングエラー予報回路

[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開発した.DES アルゴリズムのハードウェア実装例に対して本手法を適用し，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，書き込みをすべて禁止した場合には十分なテストパタンを生成することはできなかったが，読み出しと書き込みの制限を適切に設定することで，実用的なテストカバー率を満たすテストパタンが生成できる事を確認した．今後，他の例題に対して摘要を行い，制限をかける FF の選択法などの一般化を行っていく．また，一部の FF の読み出し，書き込みの制限が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も行う．

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、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)「豊橋技術科学大学」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] Makoto Sugihara, Tohru Ishihara, and Kazuaki Murakami, ``Architectural-level soft-error modeling for estimating reliability of computer systems'', IEICE Transactions on Electronics, Vol.E90-C, No.10, pp.1983-1991, Oct. 2007.

[2] Taeko Matsunaga and Yusuke Matsunaga, ``Timing-Constrained Area Minimization Algorithm for Parallel Prefix Adders'', IEICE Trans. Fundamentals, Vol.E90-A, No.12, pp.2770-2777, Dec. 2007.

[3] Mohammad Mesbah Uddin, Yasunobu Nohara, Daisuke Ikeda, and Hiroto Yasuura, ``A Multi-Application Smart Card System with Authentic Post-Issuance Program Modification'', IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E91-A, No.1, pp.229-235, Jan. 2008.

[4] M. Sugihara, T. Ishihara, and K. Murakami, "Reliable cache architectures and task scheduling for multiprocessor systems," to appear in IEICE Transactions on Electronics, April 2008.