「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 22 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、昨年開発した順序回路におけるソフトエラー伝搬確率計算アルゴリズムの高速化を行った。適用可能な最大規模の例題に対して数十倍の高速化を達成している。また、近似回路を用いた回路の多重化を行うことで、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合成手法を開発した。組合せ回路のロジックマスキング効果の解析手法に関しても、回路規模に比例した手間で近似値を見積もる手法を開発した。

タイミングエラーに関しては、NBTI（Negative Bias Temperature Instability）起因の経年劣化を予防するメモリを検討した。レジスタファイルに用いられる SRAM で、スタティックノイズマージンを 25%改善出来ている。まずシミュレーションにより NBTI 起因劣化の特徴を調査した。それに基づき、劣化の度合いを小さくできるメモリアーキテクチャを提案した。続いて評価を行い上述の効果を確認した。また、タイミングエラーを予報するカナリア・フリップフロップについては実用性確認のための設計を実施中である。

情報セキュリティに関しては、システムの実装方式の不備を突くサイドチャネル攻撃の一つであるスキャンベース攻撃に対する防御法について研究を行った。スキャンベース攻撃の防御策であるノンスキャン設計（すべての FF でスキャン FF を用いない）とパーシャルスキャン設計（一部の FF のみでスキャン FF を用いる）をそれぞれ RSA 暗号回路に適用し、さらにテスタビリティを向上させる技術を開発し適用することによって、セキュリティとテスタビリティの両方を満たしていることを確認した。

§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. LSI の搭載し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　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. LSI の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

(4)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　大学院工学研究科情報・知能工学系　准教授)(主たる共同研究者)

②研究項目

1. 電源電圧値とソフトエラー率の関係の明示
2. チップ面積、性能、消費エネルギー、及び信頼性の間に存在するトレードオフの関係を考慮した VLSI 設計技術及び CPU アーキテクチャ技術の提案

§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)

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 の搭載し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

前年度と同様に以下に示すようなサブテーマごとに研究・開発を行った。

(1-1) 論理回路・RT レベル

今年度は「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」、「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」、「大規模回路に適用可能な組合せ回路のロジックマスキング評価手法」の3つのテーマに関して研究を行った。

「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」に関しては、昨年までに開発した手法を高速化した。従来の単純な手法で連立方程式を解くと、フリップフロップ数 20 程度の回路に対して約 9 万秒を要したが、状態遷移の依存性に着目して連立方程式を変形・分割する改良版の厳密アルゴリズムを開発した。改良版のアルゴリズムでは前述の例題を約 2,000 秒で解いている [12)]。

「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」に関しては、三重化を行った回路から冗長性を取り除くことで、僅かなソフトエラー耐性の低下で面積削減を行う論理合成手法を提案した。キーとなるアイデアは、もとの論理関数より面積の小さな近似関数を2つ用いて擬似的な三重化回路を構成することである [2)]。

「大規模回路に適用可能な組合せ回路のロジックマスキング評価手法」に関しては、論理ゲートで発生したソフトエラーのパルスが論理的なマスキング効果で消滅する確率の悲観的な見積り手法を開発した。厳密な見積りでは回路規模の 2 乗に比例する計算量を必要とすることが知られており、実用的ではない。今回、開発した手法は回路規模に比例する計算量で処理できる [13)]。

(1-2) アーキテクチャレベル

シルバコ社のデバイスシミュレータ及び Synopsys 社の回路シミュレータを用いて、電源電圧値及び空間的多重度を変更した際の遅延時間、消費エネルギー、及びクロックサイクル当りの failure 数を調査した。遅延時間の増加を許容できる場合、電源電圧値及び空間的多重度を適宜

決定することにより、ソフトエラー耐性及び低消費エネルギー性を両立できることを実験的に確認した。

キャッシュメモリ量がシステムのソフトエラー耐性に影響を与える点に着目し、特定用途向けシステムの設計制約下においてマルチコア CPU を合成する設計手法を検討した。キャッシュメモリ量を最適化し、実行中に生じるソフトエラー数を最小化するマルチコア CPU 合成技術を提案した [8]。また、マイクロプロセッサの命令系列における参照の局所性に着目し、マイクロプロセッサの制御信号誤り検出手法を提案した [4],[15]。

(1-3) 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

(1-1)、(1-2)の研究成果のアウトプットとして、これらの技術を用いた、ディペンダブル LSI の設計フローおよびツールチェインの開発を行っている。今年度は現在開発中の各々のツールの機能強化を行った。ツールの統合化に関しては、セルレベルのソフトエラーのモデル化ツールと、論理レベルのソフトエラー確率の計算ツールに関しては連携させる目処が立ったが、順序回路におけるエラー確率の計算へのインターフェイスが未定である。これは、起こりうるすべてのエラー状態を明示的に列挙するとフリップフロップ数の指数乗の記憶量および計算量を必要とするためであり、今後の課題となっている。

(1-4) 実験

神戸大学吉本チームと共同で、デバイスシミュレータを用いてソフトエラーの振る舞いを解析する手法を検討した。具体的には、デバイスシミュレータに付随する簡易モデルよりも正確なモデルを用いて中性子起因の電荷分布を指定するプログラムを実装した。その他、さまざまなシミュレーション実験を通して、ソフトエラーの振る舞いの特徴抽出を行っている [14]。

(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

タイミングエラーを予報するカナリア・フリップフロップと、NBTI 起因の経年劣化を予防するメモリを検討している。

カナリア FF に関しては、前年度までの成果をまとめ、国際会議で発表した [10]。実用性を確認するために回路設計とレイアウト設計を実施中である。そのアプリケーションについては、マルチコアでの利用時に設計マージンを削減できることを確認している [7]。

経年劣化予防メモリについては、劣化の特徴調査、アーキテクチャの提案、そしてその評価を行った。NBTI 起因でトランジスタの動作速度が低下するとSRAM セルのスタティックノイズマージンが悪化し、SRAM が誤動作する恐れがある。NBTI には回復モードがあるので、それと劣化との関係をシミュレーションにより調査した。Stress 期間には閾値電圧が劣化するが、Recovery 期間には劣化が回復する。Stress 期間と Recovery 期間の割合や切り替り頻度と劣化の度合いの関係を調査した。その結果に基づき、SRAM が保持している値を反転して回復モードを利用するアーキテクチャを提案した。提案方式を評価してレジスタファイルでの有効性を確認した。また、性能

や消費電力への影響の観点から既存方式と比較し、メモリの特徴に応じて提案方式と既存方式を使い分けることが有効であることを見出した [3]。スタティックノイズマージンについては 25%改善できることを確認している [16]。

(3) LSI の搭載し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り、これらの情報の漏えいや改ざんを防ぐこともディペンダブル VLSI の要件である。安浦チームでは、システムの実装方式の不備を突くサイドチャネル攻撃と認証プロトコルに対する攻撃に対して、それぞれの防御手法について研究を行っている。

サイドチャネル攻撃に関しては、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経由で LSI 内部の秘密情報を漏洩させる攻撃(スキャンベース攻撃)に対する防御法について研究を行っている。前年度までに確立した秘密情報の漏洩のしにくさを表すモデル [5]を用いて、スキャンベース攻撃の防御策であるノンスキャン設計(すべての FF でスキャン FF を用いない)とパーシャルスキャン設計(一部の FF のみでスキャン FF を用いる)をそれぞれ RSA 暗号回路に適用し、セキュリティとテスタビリティに関して評価した。いずれの回路もセキュリティは保たれているが、テスタビリティは不足したため、セキュリティを保ちつつ、テスタビリティを向上させる技術を開発し適用することによって、セキュリティとテスタビリティの両方を満たしていることを確認した [1),6),9)]。

認証プロトコルに対する防御手法としては、今年度はユーザとサービス提供者間に認証手続きを行う第三者機関(中央機関)が存在するモデルにおいて、秘密情報の漏えいを防ぐ認証モデルを提案した [11),17)]。

§4. 成果発表等

(4－1) 原著論文発表

●論文詳細情報

1. Masayoshi Yoshimura, Hiroshi Ogawa, Toshinori Hosokawa and Koji Yamazaki, "Evaluation of Transition Untestable Faults Using a Multi-Cycle Capture Test Generation Method," Proc. 13th IEEE Symposium on Design and Diagnostics of Electronic Circuits and Systems, Vol.1, pp.273-276, Vienna, Austria, Apr. 2010. (DOI: 10.1109/DDECS.2010.5491771)
2. Shoji Harada, Masayoshi Yoshimura and Yusuke Matsunaga, "TMR based Error Correction Method Considering Trade-off between Area and Soft-Error Tolerance," Proc. 19th International Workshop on Logic and Synthesis 2010, pp.69-75, University of California Irvine, CA, USA, June 2010. (DOI: 不明)
3. Yuji Kunitake, Toshinori Sato and Hiroto Yasuura, "A Case Study of Short Term

Cell-Flipping Technique for Mitigating NBTI degradation on Cache," Proc. 2nd Asia Symposium on Quality Electronic Design, pp.301-307, Penang, Malaysia, Aug. 2010. (DOI: 10.1109/ASQED.2010.5548256)

4. Makoto Sugihara, "Dynamic control flow checking technique for reliable microprocessors," Proc. 13th Euromicro Conf. on Digital System Design, pp. 232-239, Lille, France, Sep. 2010. (DOI: 10.1109/DSD.2010.81)
5. Masayoshi Yoshimura, Yuma Ito and Hiroto Yasuura, "An estimation of encryption LSI testability against scan-based attack," Proc. International Symposium on Communications and Information Technologies 2010 (ISCIT 2010), pp.727-731, Meiji University, Tokyo, Japan, Oct. 2010. (DOI: 10.1109/ISCIT.2010.5665083)
6. Toshinori Hosokawa, Yun Chen, LingLing Wan, Motohiro Wakazono and Masayoshi Yoshimura, "A Test Pattern Matching Method on BAST Architecture Using Don't Care Identification for Random Pattern Resistant Faults," Proc. International Symposium on Communications and Information Technologies 2010 (ISCIT 2010), pp.738-743, Meiji University, Tokyo, Japan, Oct. 2010. (DOI: 10.1109/ISCIT.2010.5665085)
7. Yoshimi Otsuka, Toshinori Sato, Takahito Yoshiki and Takanori Hayashida, "MultiCore Energy Reduction Utilizing Canary FF," Proc. International Symposium on Communications and Information Technologies 2010 (ISCIT 2010), pp.922-927, Meiji University, Tokyo, Japan, Oct. 2010. (DOI: 10.1109/ISCIT.2010.5665119)
8. Makoto Sugihara, "On Synthesizing a Reliable Mmultiprocessor for Embedded Systems," IEICE Trans. Fundamentals, Vol.E93-A, No.12, pp.2560-2569, Dec. 2010. (DOI: 10.1587/transfun.E93A.2560)
9. Toshinori Hosokawa, Teppei Hayakawa and Masayoshi Yoshimura, "A Comprehensive Functional Time Expansion Model Generation Method for Datapaths Using Controllers," Proc. 11th Workshop on RTL and High Level Testing (WRTLT 2010), pp.131-138, Shanghai, China, Dec. 2010. (DOI: 不明)
10. Yuji Kunitake, Toshinori Sato and Hiroto Yasuura, "A Replacement Strategy for Canary Flip-Flops," Proc. 16th IEEE Pacific Rim International Symposium on Dependable Computing, pp227-228, National Institute of Informatics, Tokyo, Japan, Dec. 2010. (DOI: 10.1109/PRDC.2010.46)
11. Toru Nakamura, Shunsuke Inenaga, Kensuke Baba, Daisuke Ikeda and Hiroto Yasuura, "An Anonymous Authentication Protocol with Single-database PIR," Australasian Information Security Conference 2011 (AISC 2011), pp.3-8, Vol.116, Perth, Australia, Jan. 2011. (DOI: 不明)
12. Masayoshi Yoshimura, Yusuke Akamine and Yusuke Matsunaga, "An SER

Analysis Method for Sequential Circuits," 7th Workshop on Silicon Errors in Logic - System Effects (SELSE7), University of Illinois, USA, Mar. 2011. (DOI: 不明)
13. Taiga Takata and Yusuke Matsunaga, "A Robust Algorithm for Pessimistic Analysis of Logic Masking Effects in Combinational Circuits," 7th Workshop on Silicon Errors in Logic - System Effects (SELSE7), University of Illinois, USA, Mar. 2011. (DOI: 不明)
14. S. Yoshimoto, T. Amashita, D. Kozuwa, T. Takata, M. Yoshimura, Y. Matsunaga, H. Yasuura, H. Kawaguchi and M. Yoshimoto, "A Multiple-Bit-Upset Tolerant 8T SRAM Cell Layout with Divided Wordline Structure," 7th Workshop on Silicon Errors in Logic - System Effects (SELSE7), University of Illinois, USA, Mar. 2011. (DOI: 不明)
15. Makoto Sugihara, "A Dynamic Continuous Signature Monitoring Technique for Reliable Microprocessors," to appear in IEICE Trans. Electron., Vol.E94-C, No.4, pp.477-486, Apr. 2011. (DOI: 10.1587/transele.E94.C.477)
16. Yuji Kunitake, Toshinori Sato and Hiroto Yasuura, "Short Term Cell-flipping Technique for Mitigating SNM Degradation Due to NBTI," to appear in IEICE Trans. Electron., Vol.E94-C, No.4, pp.520-529, Apr. 2011. (DOI: 10.1587/transele.E94.C.520)
17. Toru Nakamura, Shunsuke Inenaga, Daisuke Ikeda, Kensuke Baba and Hiroto Yasuura, "Password Based Anonymous Authentication with Private Information Retrieval, " to appear in Journal of Digital Information Management, Vol.9, No.2, pp.72-78, Apr. 2011. (DOI: 不明)

(4－2)知財出願

① 平成22年度特許出願件数(国内 1 件)
② CREST 研究期間累積件数(国内 1件)