様式 C-19

科学研究費補助金研究成果報告書

平成２３年５月２４日現在

機関番号：１７１０２
研究種目：若手研究（B）
研究期間：2008～2010
課題番号：20700050
研究課題名（和文）　安全性と製造検査容易性の両立したＬＳＩ設計方法の研究法の研究

研究課題名（英文）　A study of LSI design method with balance security and testability
研究代表者
吉村 正義（YOSHIMURA MASAYOSHI）
九州大学・大学院システム情報科学研究院・助教
研究者番号：９０４５２８２０

研究成果の概要（和文）：LSI(大規模集積回路)の信頼性の項目である安全性と製造検査容易性は両立が困難である。まず安全性を阻害する要因を明確にした。次に，安全性を阻害しない範囲で製造検査容易性を向上する技術を開発した。この 2 つの技術に基づいて、LSI の安全性と製造検査容易性を両立させる設計手法を構築した。秘密情報が含まれる 3 種類の標準的な暗号回路に対して、この設計手法を適用し、効果を確認した。

研究成果の概要（英文）：It is difficult to balance with security and testability of LSIs.
We showed factors which destroy security of LSIs. DFT (design for testability) techniques which increase testability and do not decrease security were proposed. A LSI design method was constructed by techniques. This method is applied to three cipher LSIs. Experimental results show three cipher LSIs have security and testability.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００８年度	1,400,000	420,000	1,820,000
２００９年度	700,000	210,000	910,000
２０１０年度	1,000,000	300,000	1,300,000
総　計	3,100,000	930,000	4,030,000

研究分野：総合領域
科研費の分科・細目：情報学・計算機システム・ネットワーク
キーワード：VLSI 設計技術，設計自動化

１．研究開始当初の背景

LSI（大規模集積回路）は、情報通信技術の基幹的部品として、経済、交通、通信、教育などの多くの社会インフラシステムの中で広く用いられている。我々は LSI を用いた社会インフラシステムを用いて日常生活を行っているため、日常生活の安定性は LSI の信頼性の強弱によって大きく左右される。また LSI をキーデバイスとする IC カードや情報機器には、電子マネーのような貨幣や映画や音楽などの著作権に代表される大きな価値を持つ権利を認証するために用いられる暗号鍵などの価値に関する情報が搭載されている。これにより、LSI の信頼性や安全性は、個人や会社などの団体の財産に直接関係するものとなっている。これらの情報を搭載する LSI には、利用者やシステムの運用者が安心して利用できる技術の搭載が求められる。しかし従来、安全性に関する研究と、信頼性に関する研究は個々に議論されていた。そこで本研究では、LSI に搭載されている秘密情報の安全性と LSI の製造検査における信

頼性の両方を確保する技術の確立を目指す。九州大学では平成17年度から全学共通ICカード導入プロジェクトを実施しており、LSIに搭載されている秘密情報の安全性が必要なシステムの実証実験を行っている。この実験を通じて、LSIに求められる安全性の要件を、システム仕様、LSIの設計仕様、LSIの製造検査における信頼性などの点から検討し、仕様を決定した。本研究では、これらの仕様策定の経験に基づき、LSIに搭載されている秘密情報の安全性とLSIの製造検査における信頼性の両方を確保するLSI設計技術の確立を目指す。

LSIの製造技術における微細加工の進展に伴い、LSIの回路規模の飛躍的増大にしている。回路規模の増大につれ、物理的故障の検査の困難性の増加に対する検査容易化設計や検査系列の自動生成方法などの対応策の研究、悪意を持った攻撃による安全性の低下に対するセキュリティ性能の向上対策の研究などは、それぞれ個々に様々な研究が行われている。しかし、いずれもいくつかの条件を設定し、個々の問題ごとに対する対策を検討しているものである。例えば、製造検査容易性を向上させるために導入するスキャンパスは、設計検証や揺らぎの解析などにも利用できるが、一方で、回路の中の情報を観測制御する機構であるため、暗号鍵や秘密情報を盗むための大きな抜け道とすることが可能である。ここで、製造検査容易性とは、LSIの検査容易化設計とその設計を生かした製造検査時に用いる高品質な検査系列を自動生成が可能であり、LSIの製造品質に対する信頼性を保つことができる性質のこととする。単純にスキャンパスを適用すると、LSIの安全性が損なわれるが、スキャンパスを適用しない場合、LSIの信頼性が損なわれてしまう。この安全性と製造検査容易性の相反する性質を両立する設計技術を確立することは、LSIが社会基盤に広く用いられている現状において、LSI設計技術の研究者に対する課題である。

２．研究の目的

LSIに搭載されている秘密情報の安全性とLSIの製造検査における信頼性の両方を確保するLSIの設計技術および設計支援技術の確立を目指す。LSI設計時において、秘密情報の安全性と製造検査の品質を算出する技術などを開発する。これらの技術は秘密情報の機能を実現するLSIアーキテクチャ、アルゴリズム、設計支援技術、製造検査技術などの幅広い観点から構築する必要がある。
具体的な研究目標は、下記のとおりである。
(1) LSIのアーキテクチャにおける秘密情報の安全性を阻害する要因を明確化する。
(2) 秘密情報の安全性を維持しつつ、製造検査容易性を推定および計測し、製造検査容易性を高める設計技術を確立する。
(3) (2)の製造検査容易性を高める計技術を適用したLSIに対する検査系列自動生成技術を開発する。
(4) 秘密情報の安全性と製造検査における信頼性の両方を確保するLSIの設計フローを確立する。

製造検査容易性の推定は、検査系列の生成を行わずにLSIの検査容易化設計を行った時点で、実施するものである。一般に製造検査容易性は検査系列を用いて評価が行われるが、本研究では、秘密情報の安全性を維持するために、製造検査容易性とトレードオフを行う必要があるため、処理時間を要する検査系列生成を行わずに、製造検査容易性を評価する必要がある。また従来の検査容易化設計と異なる設計を行うため、対応した検査系列の自動生成技術が必要となる。さらに検査系列自動生成技術の観点から、安全性を維持しつつより製造検査容易性を高める検査容易化技術の開発を行う。本研究は、LSIの設計段階において、LSIに搭載されている秘密情報の安全性とLSIの製造検査における信頼性をあらかじめ見通し、確保することを考えることが最大の特徴である。LSIのアーキテクチャ設計という早期の設計段階から、安全性と製造検査容易性に関して検討と評価を行い、相反する性質の両立をはかることによって、高度な安全性が必要とされる社会インフラシステムの構築の基礎となる研究である。

３．研究の方法

４つの研究目標に対して、それぞれ以下のような計画に沿って研究を推進する。

(1) 秘密情報の安全性を阻害する要因の明確化
秘密情報が搭載されるLSIにおいて、安全性を担保する回路のアーキテクチャを抽出し、まずアーキテクチャのどの構成要素が秘密情報の秘匿に貢献しているかの解析および評価を行う。具体的には標準的な暗号回路であるAESを例にとり、AESの暗号アルゴリズムを実現するアーキテクチャを複数検討する。アーキテクチャごとに、どの回路要素が暗号化に貢献しているかを求め、さらにフルスキャン設計されたときの秘密情報の保持性について評価を行う。さらに通常のフルスキャン設計のおいて同時に与えられる可制御性や可観測性を、それぞれのレジスタにおいていずれか１つを付与された場合において、どの程度安全性を阻害するかの検討を行う。

(2) 製造検査容易性を推定および計測技術の確立

秘密情報を保持するために、まず(1)で検討したアーキテクチャの当該部分をノンスキャン設計とした回路に対しての製造検査容易性に対する評価を行う。具体的には、順序回路故障シミュレータを用いて、検査用のパタンを入力し、評価指標のひとつである故障検出率を求める。検査用のパタンとして、動作検査用の検査系列およびランダムに生成した検査系列を用いる。
さらにノンスキャンだけでなく、フルスキャン設計のおいて同時に与えられる可制御性や可観測性を、それぞれ FF に 1 つずつ与えた設計に関する製造検査容易性の計測を行う。具体的な回路構成方法としては、可制御性のみを与える場合は、スキャンアウトピンを有しないスキャンパス設計やテスト時の値設定用のセット/リセット端子の追加設計、制御用のテストポイント設計方法などを検討している。また可観測性のみを与える場合は、スキャンインピンを有しないスキャンパス設計や観測用のテストポイント設計方法などを検討している。これらの両立するための技術の検討および評価を行う。

(3) 検査系列自動生成技術開発

可制御性と可観測性を 1 つずつ与えた場合に対しての検査系列の生成技術の開発を行う。まず可制御性と可観測性を 1 つずつ与えた場合のモデル化を行い、回路構成の実現方法において、どの程度検査系列の生成難易度が変化するかの評価を行う。具体的には、検査系列の難易度を示すテスタビリティメジャの値の測定と、実際に検査系列生成を行い、個々の故障に対する生成難易度の評価を行う。

(4) 安全性と製造検査容易性を確保する LSI の設計フロー

今年度は LSI 設計フローの検討を行う。特に、アーキテクチャの選択によって、製造検査容易性の定性的に求めることについて研究する。既存のアーキテクチャと製造検査容易性に関するクラスを定義して、定性的に整理する。

４．研究成果

４つの研究目標に対して、それぞれ以下のような研究を行った。

(1) 秘密情報の安全性を阻害する要因の明確化

まず秘密情報が搭載される LSI において、安全性を担保する回路のアーキテクチャを抽出し、まずアーキテクチャのどの構成要素が秘密情報の秘匿に貢献しているかの解析および評価を行った。具体的には標準的な暗号回路である AES を例にとって解析と評価を行った。次に同じく標準的な暗号回路である公開鍵暗号方式である DES と共通鍵方式の RSA に対しても同様の解析と評価を行った。

次に秘密情報が搭載される LSI において、安全性を定量的に測定するために、相互情報量を用いた尺度を提案した。その尺度に基づいて、安全性を阻害する要因を定量的に評価した。

最終的に秘密情報である鍵の値によって値が左右されることのある記憶素子がスキャンベース攻撃に対する安全性を阻害する要因であることが分かった。

(2) 製造検査容易性を推定および計測技術の確立

まず秘密情報を保持するために、1)で検討したアーキテクチャの当該部分をノンスキャン設計とした回路に対しての製造検査容易性に対する評価を行った。1)で検討したアーキテクチャの当該部分をノンスキャン設計とした回路に秘密保持性を維持しうる箇所にテストポイントを挿入した回路に対して、順序回路故障シミュレータを用いて、検査用のパタンを入力し、評価指標のひとつである故障検出率を求めた。DES、AES、RSA の 3 つの回路でそれぞれの手法に対して製造検査容易性が十分満たされていることを確認した。

(3) 検査系列自動生成技術開発

まず (2)で検討した回路に対しての製造検査容易性に対する評価を行った。具体的には、まず製造検査用の系列を作成する際の制約条件の抽出を行った。暗号回路に入力される制御系列をすべて列挙し、列挙された系列一つ一つを製造検査用の制約とした。個々の制約ごとに製造検査用の系列を作成した。次に製造検査容易性の評価尺度の一つである故障検出率を求めた。具体的には生成した製造検査用のパタンを入力して、順序回路故障シミュレータを用いて、故障検出率を求め、必要な故障検出率を満たしていることが解った。

(4) 安全性と製造検査容易性を確保する LSI の設計フロー

(1)(2)(3)の手順によって，安全性と製造検査容易性を両立させる LSI の設計フローとして確立することができた。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計０件）

〔学会発表〕（計 41 件）

(1) Masayoshi Yoshimura, An estimation of encryption LSI testability against scan-based attack, An estimation of encryption LSI testability against scan-based attack, October 28, 2010, Tokyo, Japan.
(2) Toshinori Hosokawa, A Comprehensive Functional Time Expansion Model Generation Method for Datapaths Using Controllers, 11th Workshop on RTL and High Level Testing, December 6, 2010, Shanghai, China.
(3) 早川 鉄平, RSA暗号回路の安全なテスト容易化設計，デザインガイア2009，2009年12月4日，高知市文化プラザ.
(4) 伊藤 侑磨，スキャンベース攻撃とその防御法に対する定量的なセキュリティ評価，デザインガイア2009，2009年12月3日，高知市文化プラザ.
(5) Masayoshi YOSHIMURA, Design For Testability Methods against Scan based Attacks, Joint Seminar on Advanced LSI Test Technology, December 1, 2008, Fukuoka, Japan.
(6) Kazuya Sugiki, A Test Generation Method for Datapath Circuits Using Functional Time Expansion Models, 9th Workshop on RTL and High Level Testing, November 28, 2008, Sapporo, Japan.
(7) 伊藤侑磨，暗号 LSI におけるテスタビリティとセキュリティに関する一考察，第５９回 FTC 研究会，2008 年 7 月 19 日，石川県羽咋市.
(8) 杉木一也，機能的時間展開モデルを用いたデータパスのテスト生成法，2008 年 7 月 19 日，石川県羽咋市.

〔図書〕（計０件）

〔産業財産権〕
○出願状況（計０件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計０件）

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等

６．研究組織
(1)研究代表者
吉村 正義 （YOSHIMURA MASAYOSHI）
九州大学・大学院システム情報科学研究院・助教
研究者番号：20700050

(2)研究分担者
なし （ ）

研究者番号：

(3)連携研究者
なし （ ）

研究者番号：