様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　３０　年　　５　月　１６　日現在

機関番号：　３４３０４
研究種目：　基盤研究(C)（一般）
研究期間：　2015～2017
課題番号：　１５Ｋ００００８６

研究課題名（和文）製造過程でのトロイ回路混入を検知するLSI設計技術に関する研究

研究課題名（英文）Study on LSI design technology to detect Trojan circuit inserted during manufacturing process

研究代表者

吉村　正義（YOSHIMURA, Masayoshi）

京都産業大学・コンピュータ理工学部・准教授

研究者番号：９０４５２８２０

交付決定額（研究期間全体）：（直接経費）　　3,400,000円

研究成果の概要（和文）：社会情報基盤において、トロイLSI は正常な機能の無効化、機密情報の漏洩や改ざんを引き起こす恐れがある。しかし製造されたLSI にトロイ回路が含まれないことを保証する手段が存在しない。そこで、トロイLSIの市場への流出の対策として、真正なLSI とトロイLSI を判別する技術の確立する必要がある。
研究成果は、(1)製造されたLSI 内部で網羅的に回路構造の情報を生成する手法の開発，(2) 出力された回路構造の情報を保護する仕組みの検討の2点である。これらによって、真正なLSI の設計データに基づいて、製造されたLSI にトロイ回路が含まれるかを区別できる仕組みの基盤技術を確立した。

研究成果の概要（英文）：In a social information infrastructure system in which a large number of LSIs are used, Trojan LSIs might cause invalidation of normal functions, leakage or tampering of confidential information. However, there is no means to guarantee that the manufactured LSI does not contain a Trojan circuit. From the aspect of safety and security as well as economics, we have worked on establishing a technology to distinguish authentic LSI and Trojan LSI as a measure to prevent Trojan LSI.
Two main research topics are as follows. (1) development of a method for generating comprehensive information on the circuit structure within the manufactured LSI, and (2) study on a mechanism for protecting the information of the output circuit structure. By achieving these research topics, we established the basic technology of a mechanism that can distinguish whether the manufactured LSIs are authentic LSIs or Trojan LSIs based on the design data of authentic LSI.

研究分野：　情報工学

キーワード：　トロイ回路　トロイ検査用回路　応答圧縮器　パタン生成器　論理的回路分割　回路構造情報　情報の保護

１．研究開始当初の背景

大規模集積回路（LSI）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情報基盤システムの中で用いられている。そのため LSI の信頼性は社会情報基盤の信頼性や安全性を大きく左右する。LSI を製造する工程が社外や海外に移されており、製造された LSI の信頼性が課題となっている。これらの課題の一つとして、外観を似せた模造 LSI や、ある一部分だけ仕様と異なる回路(以下トロイ回路) を含む LSI(以下トロイ LSI)が市場に存在することが報告されている[1]。

真正な LSI と、真正でない模造 LSI やトロイ LSI を判別する必要がある。しかし、真正の LSI とトロイ LSI の判別は困難である。困難な点は主に二つ存在する。一つはトロイ LSI は真正な LSI とほぼ同一の測定結果が得られるため、判別が困難な点である。もう一つは、そもそもどの LSI が真正な LSI であるかを同定することである。

トロイ回路が混入される行程は、主に設計と製造の二つである。製造工程で混入されるケースは、一部の LSI に混入される場合とすべての LSI に混入されるケース場合がある。一部の LSI に混入される場合は、真正な LSI が存在する。しかし分業化されている設計工程で混入された場合や製造工程ですべての LSI にトロイ回路が混入された場合は、真正な LSI が存在しない。真正な LSI が存在しない場合、真正 LSI とトロイ LSI を比較しトロイ LSI を特定する手法は実施できない。

真正な LSI が同定されている前提の下で、トロイ LSI の特定方法が多数提案されている。特定方法は真正な LSI とトロイ LSI の両方を様々な項目に対して測定を行い、その測定結果を統計的に比較し、異なる項目を同定することによって、異なる項目が測定された LSI をトロイ LSI と判断する手順で実施される。現在、この真正な LSI との比較による方法は、消費電力、ノイズや表面温度など、とても小さな規模の回路の違いによって影響される項目を測定することで、小規模なトロイ LSI であっても、高精度にトロイ LSI を特定できることが報告されている。

一方、どの LSI が真正な LSI であるかの同定方法は、未だ解決されておらず，この課題の解決に取り組む。

２．研究の目的

トロイ LSI は、トロイ LSI が混入した社会情報基盤システム全体の正常な機能の無効化、機密情報の漏洩や改ざんを引き起こす恐れがある。またトロイ LSI の市場への流出は、流出させた組織の信頼性を大きく損なう。しかし製造された LSI にトロイ回路が含まれていないことを保証する手段がそもそも存在しない。よって、安全安心の面のみならず経済的な面からも、トロイ LSI の市場への流出への対策が必要である。そのため、真正な LSI とトロイ LSI を判別する技術の確立を本研究の目的とする。

３．研究の方法

真正な設計データに基づいて、トロイ LSI を特定する手法を提案する。本提案は製造された LSI 内部で網羅的に回路構造の情報を生成する手法と出力用の情報された情報の復号化を保護する仕組みの二つから構成される。

真正な設計データと製造された LSI が一致しているかを調べるために、製造された LSI の内部構造の情報を網羅的に出力することを考える。この出力された内部情報と真正な設計データを比較することで、製造された LSI にトロイ回路が含まれていないかを判断する。LSI の内部構造に関する情報を効率よくかつ網羅的に出力することは難しい。

LSI は順序回路であり、順序回路は入力系列の集合、出力系列の集合、状態集合、初期状態集合、状態遷移関数、および出力関数の 6 つ組で定義される。これらの情報を出力するために、LSI 製造後に行われる製造検査用に実装されているスキャン設計を利用する。製造検査では、製造された LSI に欠陥が発生しているかの判断をするために、多くの LSI にはスキャン設計が適用されている。このスキャン設計は、内部の記憶素子をシフトレジスタ状に接続し、外部入力ピンと外部出力ピンに接続し、内部の記憶素子の値を可制御、可観測にすることができる。このスキャン設計で実装された機能を用いることで、順序回路の入力系列の集合と、出力系列の集合、初期状態集合、状態集合の 4 つを観測・制御することができる。残り 2 つの状態遷移関数と出力関数について考える。状態遷移関数は、入力と現状態から次状態を決定し、出力関数は入力と現状態から出力値を決定する。すべての状態に対して、次状態および出力を確認することで、状態遷移関数と出力関数を確認することができる。しかし、LSI は記憶素子の数が多いため、状態数が指数的に増加し、全状態に対して次状態や出力を確認することは難しい。一方、トロイ回路を検出されにくくするために、攻撃者は状態と入力の組み合わせのごく特定の少数の場合のみ動作する箇所にトロイ回路を挿入していることが報告されている。そのため、真正な LSI と判断するために、すべての状態に対して網羅的に確認する必要がある。

そこで製造された LSI 内部で回路構造の情報を網羅的に生成する手法として、すべての状態を網羅的に確認するために、論理的に状態を分割し、分割された状態の全状態数を大幅に削減する。分割された状態ごとに全状態の状態遷移関数と出力関数を確認する。また分割した状態ごとに、全状態において状態

遷移関数と出力関数の情報を得るために、網羅的に入力を印加し、次状態の状態と出力値の観測を効率化する回路を追加する。

次に、出力用の情報された情報の復号化を保護する仕組みについて説明する。製造された LSI 内部の回路構造の情報は、知的財産などの秘密情報が含まれている。その情報を第三者が容易に得られることは問題となる。そこで回路内で符号化し、符号化された情報のみを出力させる。出力された情報は、復号鍵をもつ設計者などが解読できる仕組みを導入する。

４．研究成果

研究成果は次の 2 点である。
(1) 製造された LSI 内部で網羅的に回路構造の情報を生成する手法の開発
(2) 出力された回路構造の情報を保護する仕組みの検討

これらの研究目標を達成することにより、真正な LSI の設計データに基づいて、製造された LSI が真正な LSI かトロイ LSI かを区別できる仕組みの確立に貢献した。

個々の詳細な研究成果について述べる。まずは、製造された LSI 内部で網羅的に回路構造の情報の生成手法の開発についてである。網羅的に回路構造の情報を生成するために、回路を論理的に分割し、分割した回路ごとに網羅的に入力を印加し、その入力に対する応答をすべて観測することで回路構造の情報を得ることができる。

まず論理的に回路を分割するために追加するトロイ検査用回路に対する効率的な回路構成を求め、通常モード時とトロイ検査モード時の仕様を作成した。制御用の信号線を 1 本追加し、その信号線の 0/1 で通常モードとトロイ検査用モードを切り替える。次にトロイ回路検査用回路の構成について検討を行った。最終的には論理ゲート一つと制御用と観測用の信号線それぞれ 1 本ずつの構成となった。論理ゲートは挿入箇所の前段と後段の論理ゲートの種類によって決定できることがわかった。これらによって、最適なトロイ検査用回路の構成を決定した。

次にトロイ検査用回路の挿入箇所の探索手法についてである。網羅的に回路構造情報を出力するために、適切な箇所に回路を挿入する必要がある。まずは挿入箇所を貪欲法に基づいた手法を開発した。これは外部入力側からゲートを順々に調べ、そのゲートから到達可能な外部入力数が定められた数を超えている場合、そのゲートの入力側を挿入箇所とする手法である。次に貪欲法をベースにして、少し大域的に挿入箇所を探索する手法を開発した。また最後に回路を論理関数に変換し、論理関数を用いて回路を簡単化し、簡単化した回路に対して、挿入箇所を探索する手法を検討した。開発したこれらの手法を実装した。またトロイ検査モードにおいて、分割された回路ごとの外部入力数の上限が 32 となるようにトロイ検査用回路の挿入箇所を求めた。外部入力数の上限を 32 とした理由は、外部入力数が 32 の場合、網羅的な入力パタン数が 2^{32} (43 億)パタンとなり、LSI を 1GHz で動作させて、検査に約 4 秒かかるためである。4 秒は実際の検査にかかる時間としては現実的な時間の上限であると考える。この外部入力数の上限を 32 として、様々なベンチマーク回路に対して、トロイ検査用回路の挿入数を求めた。その結果、多くのベンチマーク回路は回路規模と挿入数が比例関係にあった。しかし b15 と b20 のように同じ規模の回路でも挿入数が 2 倍異なるものもあった。図 1 に結果のグラフを示す。図 1 はベンチマーク回路の信号線数とトロイ検査用回路の挿入数の関係を示したものである。

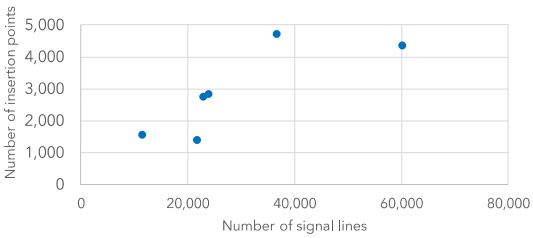

図 1 信号線数とトロイ検査用回路挿入数

網羅的に入力と状態を印加するためのパタン生成器について検討した。その結果、網羅的な入力を生成する回路として、LSI の製造検査などで使われている線形帰還フィードバックレジスタが適切であることがわかった。

印加された入力と状態に対する次状態を観測するための応答圧縮器について検討した。網羅的に入力パタンを印加するため、それらに対する応答も同じく膨大な数となる。全ての応答を回路に記憶することは膨大な容量が必要となるため、非常に困難である。また単純な応答圧縮器を用いた場合、トロイ回路の有無の判断を誤る場合がある。そこで判断を誤る確率を低下させる構成について検討した。検討した結果、全ての応答を一つの応答圧縮器へ入力する場合、分割した回路ごとに個々の応答圧縮器を作成し 1 対 1 対応させる場合は判断を誤る確率を低下させないことが判った。そこで、分割した回路数分だけ応答圧縮器を作成し、分割した回路からの応答の系列を時間方向に分割し、時間ごとに異なる応答圧縮器に入力する構成を検討した。この構成により、判断を誤る確率を低下させることが判った。

出力された回路構造の情報は外部から観測することが難しい情報であり、知的財産でもあるため、保護する仕組みが必要である。そこで応答圧縮器で圧縮された情報を単に

LSI から出力するのではなく、符号化を施す必要がある。どのような符号化が適切かについて検討を行った。検討した結果、論理暗号化やチップの認証などに用いる PUF に基づいた鍵を利用する暗号を用いることで、適切な符号化であることが判った。 この方式は正規の情報利用者である場合、PUF に基づいた鍵の値を知ることができるため、トロイ回路の有無を判別することができる。一方、非正規の利用者は PUF に基づいた鍵の値を知ることができないため、応答圧縮器の情報から LSI 中の回路の構成に関する情報を得ることができない。

これらの 2 つの研究成果によって、真正な LSI の設計データに基づいて、製造された LSI が真正な LSI かトロイ LSI かを区別できる仕組みの基盤技術を確立した。

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 1 件）

① Masayoshi YOSHIMURA, Yoshiyasu TAKAHASHI, Hiroshi YAMAZAKI, and Toshinori HOSOKAWA, “A Don't Care Filling Method for Low Capture Power based on Correlation of FF Transitions Using SAT,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Volume E100.A (2017) Issue 12 Pages 2824-283.3(査読あり).

〔学会発表〕（計 9 件）

① Yoshinobu Okuda, Masayoshi Yoshimura, Kohei Ohyama, and Toshinori Hosokawa, “A Secure Design Method to Detect for Trojan Circuit inserted in Manufacturing Process,” DUHDe 2018 — 5th Workshop on Design Automation for Understanding Hardware Designs, 2018(査読あり).

② Shun Takeda, Toshinori Hosokawa, Hiroshi Yamazaki, and Masayoshi Yoshimura, “A Test Register Assignment Method to Reduce the Number of Test Patterns Using Controller Augmentation,” DUHDe 2018 – 5th Workshop on Design Automation for Understanding Hardware Designs, March 23, 2018, Dresden, Germany(査読あり).

③ Sayuri Ochi, Hiroshi Yamazaki, Toshinori Hosokawa, and Masayoshi Yoshimura, “A Low Power Oriented Static Test Compaction Method Based on Don't Care Bits,” IEEE The Eighteenth Workshop on RTLT and High Level Testing 2017, Dec. 1, 2017(査読あり).

④ Morito Niseki, Toshinori Hosokawa, Hiroshi Yamazaki, Masayuki Arai, Masayoshi Yoshimura, Hiroyuki Yotsuyanagi and Masaki Hashizume, “A Sequentially Untestable Fault Identification Method Based on State Cube Justification,” IEEE The Eighteenth Workshop on RTLT and High Level Testing 2017, Dec. 1, 2017(査読あり).

⑤ Toshinori Hosokawa, Shun Takeda, Hiroshi Yamazaki, and Masayoshi Yoshimura, “Controller augmentation and test point insertion at RTL for concurrent operational unit testing,” 2017 IEEE 23rd International Symposium on On-Line Testing and Robust System Design (IOLTS), Thessaloniki, Greece, 3-5 July 2017(査読あり).

⑥ Masayoshi Yoshimura, Tomohiro Bouyashiki, and Toshinori Hosokawa, “A Hardware Trojan Circuit Detection Method Using Activation Sequence Generations,” The 22nd IEEE Pacific Rim International Symposium on Dependable Computing, Christchurch, New Zealand, Jan. 22-25, 2017(査読あり).

⑦ Shun Takeda, Toshinori Hosokawa, Hiroshi Yamazaki and Masayoshi Yoshimura, “A Design for Testability Method at RTL for Concurrent Operational Unit Testing,” IEEE The Seventeenth Workshop on RTL and High Level Testing, Hiroshima, Japan, Nov. 24-25, 2016(査読あり).

⑧ Masayoshi Yoshimura, Tomohiro Bouyashiki and Toshinori Hosokawa, “A Sequence Generation Method to detect Hardware Trojan Circuits,” RTL and High Level Testing 2015, Bombay, India, Nov. 25, 2015(査読あり).

⑨ Masayoshi Yoshimura, Yoshiyasu Takahashi, Hiroshi Yamazaki and Toshinori Hosokawa, “A Don’t Care Filling Method to Reduce Capture Power based on Correlation of FF Transitions,” 24th IEEE Asian Test Symposium 2015, Bombay, India, Nov. 23, 2015(査読あり).

〔その他〕

ホームページ等

http://www.cc.kyoto-su.ac.jp/~myoshi

６．研究組織
(1)研究代表者
吉村　正義（YOSHIMURA, Masayoshi）
京都産業大学・コンピュータ理工部・准教授
研究者番号：90452820