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

令和　５ 年　 ６ 月 ２１ 日現在

機関番号：３４３０４
研究種目：基盤研究(C)（一般）
研究期間：2018～2022
課題番号：１８Ｋ１１２２８

研究課題名（和文）IPコア内のトロイ回路を特定するLSI設計技術に関する研究

研究課題名（英文）Research on LSI design methods to identify Trojan circuits in IP cores

研究代表者
吉村　正義（Yoshimura, Masayoshi）

京都産業大学・情報理工学部・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）：LSIの設計データであるIPコアに含まれる恐れのあるトロイ回路を検出する技術について開発を行った．動作中にあまり用いられれない内部状態において起動するトロイ回路は検出しずらい．このあまり用いられれない状態を検出するために，SATソルバーとモンテカルロツリー探索を用いた手法を開発した．小規模と中規模なベンチマーク回路に対しては比較的短時間で精度良く目的となる状態を特定できた．一方，大規模なベンチマーク回路に対する探索時間は長かった．

研究成果の学術的意義や社会的意義
情報化社会において，LSIは基盤となる部品であり，LSIの信頼性や安全性が損なわれると，情報化社会の信頼性安全性にも大きな影響を与える．本研究は，LSIの信頼性と安全性をLSI設計レベルで高める技術である．本研究は，LSIの設計段階において，LSIに悪意のある回路が含まれていないかの判定に用いられる．LSIへの悪意のある回路の混入を防ぐことで，情報化社会の信頼性と安全性の向上に貢献する．

研究成果の概要（英文）：We have developed a technique to detect trojan circuits that may be included in IP cores, which are LSI design data. Trojan circuits that are activated in states that are rarely used during operation are difficult to detect in the LSI desgin phases. To detect these states, we developed a method using a SAT solver and Monte Carlo tree search. For small and medium benchmark circuits, we were able to identify these states with high accuracy in a relatively short time. On the other hand, search times for large benchmark circuits were long.

研究分野：コンピュータサイエンス

キーワード：トロイ回路　ブラックボックス　ホワイトボックス　SATソルバー　モンテカルロツリーサーチ　入力系列生成

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

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広く用いられている．そのため LSI の信頼性・安全性は社会情報基盤の信頼性や安全性を大きく左右する．この LSI の回路規模は年々増大しており，そのため LSI を設計するコストや期間が増加している．この LSI を設計するコストの削減や期間を短縮するために，第三者が設計した LSI の設計データ(以下 IP コア)の利用が増えてきている．LSI の設計者は求められる機能を持つ IP コアを自らの LSI に組み込むことで，求められる機能を容易に追加することができる．

しかし，この第三者の IP コアの提供者が設計した IP コアには，LSI の設計者が求めている機能とは別の隠された機能が含まれている恐れがある．LSI の設計データである IP コアは大規模で複雑なデータであるため，LSI の設計者が求めている機能の有無は確認できるが，LSI の設計者が求めていない機能の有無を確認することは難しい．一般に，何かを存在しないことを確認する方が，何かが存在することを確認するより難しい．

この IP コアはデジタルデータとして提供されるため，LSI の設計者は，契約した自らの LSI に IP コアを容易に組み込めるという利点がある．その一方で，デジタルデータであるため，契約外の別の LSI の設計データにも流用することが容易である．この流用を防ぐ手法の一つとして，IP コアの提供者はより流用が容易な抽象度の高い設計データを内部でブラックボックス化して提供し，抽象度の低い設計データをホワイトボックス化して提供する手法がある．IP コアの提供者は，抽象度の低いホワイトボックス化された設計データに，IP コア固有の特徴的な設計データを含めている．IP コア固有の特徴的な設計データは，本来の機能には一切影響させず，また他の IP コアにはない設計データである．IP コア固有の特徴的な設計データは密に他の設計データと関連しているため，IP コア固有の特徴的な設計データのみを取り除くことは難しい．よって，製造された LSI にこの IP コアのホワイトボックス化された詳細な設計データによる部分を含んでいると，IP コアを使用したことを特定できる．このような仕組みを用いることで，IP コアの提供側は IP コアの流用を防ぎつつ，IP コアの設計データの使用を確認することができる．

LSI の設計の上流段階では，ブラックボックス化されたデータを用いて，IP コアの機能を確認する．また IP コアの機能の確認とともに，LSI 全体の機能を確認する．LSI の設計の下流段階では，ホワイトボックスである詳細な設計データを用いて，LSI の詳細な設計をすすめる．この段階では，LSI 設計の抽象度が低いため，LSI 全体の機能を確認することは難しく，LSI や IP コアの一部分の機能の確認のみを行う．

IP コアの提供者は，ブラックボックス化された機能確認用の設計データとホワイトボックス化された詳細な物理設計用の設計データの二つを LSI の設計者に提供する．これら 2 つを提供することで，LSI 設計者の設計コストや期間の削減し，IP コアの設計データの流用を防ぐ．

しかし，LSI 設計者は，ブラックボックス化された機能確認用の設計データとホワイトボックス化された詳細な物理設計用の設計データとの機能が同一であることを確認できない．ブラックボックス化された機能確認用の設計データに含まれていない機能がホワイトボックス化された詳細な物理設計用の設計データに含まれている恐れがある．また私の知りうる限り，ブラックボックス化された機能確認用の設計データに含まれていない機能がホワイトボックス化された詳細な物理設計用の設計データに含まれていないことを確認する手法はないため，LSI 設計者は，自らが IP コアを用いて設計した LSI にトロイ回路が混入していないことを保証できない．

２．研究の目的

本研究の目的はこのブラックボックス化された機能確認用の設計データに含まれていない機能がホワイトボックス化された詳細な物理設計用の設計データに含まれていないことを示す手法を開発することである．

そこで，本研究では，ブラックボックス化された設計データと変換されたホワイトボックス化された機能確認用の設計データとの等価性を検証する手法を開発する．ブラックボックス化された順序回路とホワイトボックス化された順序回路の等価性を検証し，余分な機能が含まれていないことを明らかにし，IP コアにトロイ回路が含まれていないことを示す．

３．研究の方法

本提案は，ブラックボックス化された設計データと変換されたホワイトボックス化された機能確認用の設計データとの等価性を検証する手法を開発する．この二つの設計データに対して，同じ入力，同じ内部状態に対して，異なる出力が存在しなければ，二つの設計データは等価であるといえる．そこで，本研究では，まず内部状態を特徴ごとに二つに分類し，それぞれの特徴に応じ同じ入力，同じ内部状態に対して，異なる出力が存在するかを求める．つまり，本研究は動作中に用いられる内部状態とあまり用いられない内部状態に分類する手法と分類した内部状態ごとに二つの設計データが異なる出力を探索する手法の二つから構成される．

本研究では，ブラックボックス化された設計データと変換されたホワイトボックス化された

機能確認用の設計データとの等価性を検証する手法を開発する．ブラックボックス化された順序回路とホワイトボックス化された順序回路の等価性を検証し，余分な機能が含まれていないことを明らかにし，IP コアにトロイ回路が含まれていないことを示す

４．研究成果

研究成果は次の 2 点である．
(1) トリガー状態と推測される状態の探索手法
(2) トリガー推測状態へ遷移する入力系列生成方法

これらの研究成果により，ブラックボックス化された IP コアにトロイ回路が含まれているか否かを検証する仕組みの確立に貢献した．

個々の研究成果について述べる．
まずはトリガー状態と推測される状態の探索手法である．まずは内部状態を「初期状態から到達可能な状態」と「初期状態から到達不可能な状態」の 2 つの状態に分類する手法について開発を行った．ここで「動作中に用いられる内部状態とあまり用いられない内部状態」はいずれも，「初期状態から到達可能な状態」である．まずこれらに含まれない「初期状態から到達不可能な状態」の特定を行なった．これらの初期状態から到達不可能な状態をすべて特定するのではなく，到達不可能な一部の状態を特定し，その特定された状態から他の到達不可能な状態を特定する手法の開発を行い，プログラムを作成した．この手法によって，多くの到達不可能な状態を特定できるようになった．さらに本研究の対象となる回路の作成であるトロイが含まれた回路とそうでない回路を作成した．それぞれ RTL とゲートレベルの回路を作成した．このトロイ回路は，順序回路であり，通常動作では到達しないまたは到達しにくい状態において，トロイ回路のトリガー回路が起動する回路である．これらの設計したトロイ回路に対して，考案したアルゴリズムを実装したプログラムを適用し，トロイ回路を起動する状態を特定できるかを確かめる評価実験を行なった．小規模な回路では，内部状態を列挙し，動作中に用いられる状態とあまり用いられない内部状態に分類できた．一方，中規模から大規模な回路ではすべての状態を列挙できなかったため，状態の分類も行うことができなかった．
さらに中規模から大規模回路向けにトロイ回路のトリガーに用いられる可能性の高い内部状態をモンテカルロツリーサーチを用いて探索する手法」について開発を行った．トロイ回路のトリガーに用いられる可能性の高い内部状態の探索は，大規模回路な回路において処理時間が指数的に増大するため困難である．そこで今年度は統計的な探索手法であるモンテカルロツリーサーチを用いて，通常動作では到達しにくい状態として，状態確率が 0 ではないが低い状態を求める手法を開発した．開発した手法を小規模から大規模なベンチマーク回路に適用し性能について評価を行った．小規模な回路では，状態確率が 0 ではないが低い状態を正確に求められた．また中規模な回路では，従来の手法より短時間で状態確率が 0 ではないが低い状態を正確に特定できることがわかった．次に大規模回路向けに処理時間を削減することを目的として，モンテカルロツリー探索と簡易な状態確率見積もりを組合せた手法を開発した．簡易な状態確率の見積もり結果によって，あらかじめ状態確率がある閾値以上と見積もられる状態を求め，モンテカルロツリー探索の対象となる状態から除去し，大規模な回路における探索時間の短縮を図った．簡易な状態確率の見積もり手法として，今回はランダムパタンシミュレーションによる各状態への遷移確率を用いた．中規模，大規模なベンチマーク回路による実験の結果，精度よくトリガー状態を特定できた．また中規模な回路での探索時間を大幅に削減することができた．一方，大規模な回路では探索時間を要した．簡易な状態確率の見積もり手法も含めて，大規模な回路に対する改善が必要である．

次にトリガー状態へ遷移する入力系列の生成方法についてである．初期状態からトリガー状態への状態遷移する入力系列はブラックボックス化された IP コアへ入力され，同じ入力系列を入力されたホワイトボックスの IP コアと異なる振る舞いをするかによってトロイ回路の有無を検証する．この入力系列の生成は，2 つの手法を開発した．
一つは SAT ソルバーを用いる手法であり，もう一つはモンテカルロツリーサーチを用いたトリガー状態探索の結果を利用する方法である．まず SAT ソルバーを用いる手法について説明する．ホワイトボックス IP コアの回路に対する時間展開モデルを生成し，最終時刻の状態をトリガー状態と推定される状態に設定し，初期状態もしくは初期状態から到達可能な状態のいずれかの状態を開始時刻の状態として，設定する．このモデルを CNF 式に変換し，SAT ソルバーを用いて，解を探索する．もし解が得られれば，この解がトリガー状態への入力系列となる．解が得られない場合は，時間展開モデルの時間展開数を増加させ，開始時刻の状態と最終時刻の状態を設定し，モデルを更新する．解が得られるまで，モデルの更新と SAT ソルバーでの探索を繰り返

す.

もう一つはモンテカルロツリーサーチの結果を利用する手法である．モンテカルロツリーサーチでは，ルートノードの状態から遷移可能な状態を順々にたどり，目的となる状態に到達するまで繰り返す．即ち，モンテカルロツリーサーチを用いて，得られたトリガー状態はルートノードから到達可能な状態遷移も自明である．この状態遷移を行う入力系列が検証用の入力系列となる．

これらの研究成果により，ブラックボックス化された IP コアにトロイ回路が含まれているか否かを検証する仕組みの確立に貢献した．

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計23件（うち招待講演　0件／うち国際学会　11件）

１．発表者名 Kyohei Iizuka, Toshinori Hosokawa, Hiroshi Yamazaki and Masayoshi Yoshimura
２．発表標題 An Additional State Transition Insertion Method to Improve Transition Fault Coverage for Controllers
３．学会等名 IEEE The　Workshop on RTL and High Level Testing 2021（国際学会）
４．発表年 2021年

１．発表者名 三浦　怜，細川利典，山崎紘史，吉村正義，　新井雅之
２．発表標題 低消費電力指向多重目標故障テスト生成法
３．学会等名 第6回 Winter Workshop on Safety
４．発表年 2021年

１．発表者名 飯塚恭平，細川利典，山崎紘史，吉村正義
２．発表標題 無効状態を含んだコントローラの遷移故障検出率向上指向状態割当て法
３．学会等名 ディペンダブルコンピューティング研究会
４．発表年 2022年

１．発表者名 徐　浩豊，細川利典，山崎紘史，新井雅之，吉村正義
２．発表標題 論理故障テスト並列化のための制御信号のドントケア割当て法
３．学会等名 ETNET2022
４．発表年 2022年

１．発表者名
Toshinori HOSOKAWA, Kenichiro MISAWA, Hiroshi YAMAZAKI, Masayoshi YOSHIMURA, Masayuki ARAI

２．発表標題
A Low Capture Power Oriented X-Identification-Filling Co-Optimization Method

３．学会等名
2020 IEEE 26th International Symposium on On-Line Testing and Robust System Design (IOLTS)（国際学会）

４．発表年
2020年

１．発表者名
浅見竜輝・細川利典・吉村正義・新井雅之

２．発表標題
テストパターン数削減のためのゲート網羅故障の多重目標故障テスト生成法

３．学会等名
SWoPP2020

４．発表年
2020年

１．発表者名
辻川敦也・細川利典・吉村正義

２．発表標題
機能等価な有限状態機械生成に基づく面積削減指向コントローラ拡大法

３．学会等名
SWoPP2020

４．発表年
2020年

１．発表者名
Ryuki Asami, Toshinori Hosokawa, Masayoshi Yoshimura and Masayuki Arai

２．発表標題
A Multiple Target Test Generation Method for Gate-Exhaustive Faults to Reduce the Number of Test Patterns Using Partial MaxSAT

３．学会等名
2020 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)（国際学会）

４．発表年
2020年

１．発表者名
浅見竜輝・細川利典・山崎紘史・吉村正義・新井雅之

２．発表標題
RTLハードウェア要素のテストスケジューリング情報を用いた多重目標故障テスト生成法

３．学会等名
ディペンダブルコンピューティング研究会

４．発表年
2021年

１．発表者名
飯塚恭平・細川利典・山崎紘史・吉村正義

２．発表標題
レジスタ転送レベルにおける非スキャンベースフィールドテスタビリティに基づく制御信号のドントケア割当て法

３．学会等名
ディペンダブルコンピューティング研究会

４．発表年
2021年

１．発表者名
飯塚恭平・細川利典・山崎紘史・吉村正義

２．発表標題
コントローラの遷移故障検出率向上のためのコントローラ拡大法

３．学会等名
ETNET2021

４．発表年
2021年

１．発表者名
辻川敦也・細川利典・吉村正義

２．発表標題
レジスタ転送レベルにおけるアンチSATに基づく論理暗号化法

３．学会等名
ETNET2021

４．発表年
2021年

１．発表者名
Yuki Takeuchi, Toshinori Hosokawa, Hiroshi Yamazaki, and Masayoshi Yoshimura

２．発表標題
A Controller Augmentation Method to Improve Transition Fault Coverage for RTL Data-Paths

３．学会等名
2019 IEEE 25th International Symposium on On-Line Testing and Robust System Design (IOLTS)（国際学会）

４．発表年
2019年

１．発表者名
Toshinori Hosokawa, Hiroshi Yamazaki, Kenichiro Misawa, Masayoshi Yoshimura, Yuki Hirama, and Masavuki Arai

２．発表標題
A State Assignment Method to Improve Transition Fault Coverage for Controllers

３．学会等名
2019 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)（国際学会）

４．発表年
2019年

１．発表者名
Masayoshi Yoshimura, Yuki Takeuchi, Hiroshi Yamazaki and Toshinori Hosokawa

２．発表標題
A State Assignment Method to Improve Transition Fault Coverage for Controllers

３．学会等名
2019 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)（国際学会）

４．発表年
2019年

１．発表者名
Kenichiro Misawa, Toshinori Hosokawa, Hiroshi Yamazaki, Masayoshi Yoshimura, and Masayuki Arai

２．発表標題
A Don't Care Identification-Filling Co-Optimization Method for Low Capture Power Testing Using Partial MaxSAT

３．学会等名
The 20th Workshop on RTL and High-Level Testing (WRTLT ' 19)（国際学会）

４．発表年
2019年

１．発表者名
竹内勇希、細川利典、山崎紘史、吉村正義

２．発表標題
レジスタ転送レベルにおけるコントローラ拡大を用いた遷移故障検出率向上のためのテスト容易化設計

３．学会等名
DAシンポジウム2018

４．発表年
2018年

１．発表者名
Yuki Takeuchi, Toshinori Hosokawa, Hiroshi Yamazaki , Masayoshi Yoshimura

２．発表標題
A design for testability method to improve transition fault coverage using controller augmentation at register transfer level

３．学会等名
The Nineteenth Workshop on RTL and High Level Testing（国際学会）

４．発表年
2018年

１．発表者名
三澤健一郎・細川利典・山崎紘史・吉村正義

２．発表標題
キャプチャセーフテストベクトルの故障伝搬経路を模倣した低消費電力指向ドントケア判定法

３．学会等名
ディペンダブルコンピューティング研究会

４．発表年
2018年

１．発表者名
吉村正義・竹内勇希・細川利典・山崎紘史

２．発表標題
コントローラの遷移故障検出率向上のための状態割当て手法

３．学会等名
ディペンダブルコンピューティング研究会

４．発表年
2018年

１．発表者名
Toshinori Hosokawa, Hiroshi Yamazaki, Shun Takeda, Masayoshi Yoshimura

２．発表標題
A Test Register Assignment Method Based on Controller Augmentation to Reduce the Number of Test Patterns

３．学会等名
2018 IEEE 24th International Symposium on On-Line Testing And Robust System Design (IOLTS)（国際学会）

４．発表年
2018年

１．発表者名
Toshinori Hosokawa, Morito Niseki, Masayoshi Yoshimura, Hiroshi Yamazaki, Masayuki Arai, Hiroyuki Yotsuyanagi, Masaki Hashizume

２．発表標題
A Sequentially Untestable Fault Identification Method Based on n-Bit State Cube Justification

３．学会等名
2018 IEEE 24th International Symposium on On-Line Testing And Robust System Design (IOLTS)（国際学会）

４．発表年
2018年

１．発表者名
Sayuri Ochi, Hiroshi Yamazaki, Toshinori Hosokawa, Masayoshi Yoshimura

２．発表標題
A Capture Safe Static Test Compaction Method Based on Don't Cares

３．学会等名
2018 IEEE 24th International Symposium on On-Line Testing And Robust System Design (IOLTS)（国際学会）

４．発表年
2018年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	細川　利典 (Hosokawa Toshinori) (40373005)	日本大学・生産工学部・教授 (32665)	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関