(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2017-146777
(P2017-146777A)
(43)公開日　平成29年8月24日(2017.8.24)

(51)Int.Cl.	F I	テーマコード（参考）
G06F 21/56 (2013.01)	G06F 21/56	

審査請求 未請求　請求項の数 5　ＯＬ　（全 14 頁）

(21)出願番号　特願2016-27994(P2016-27994)
(22)出願日　平成28年2月17日(2016.2.17)

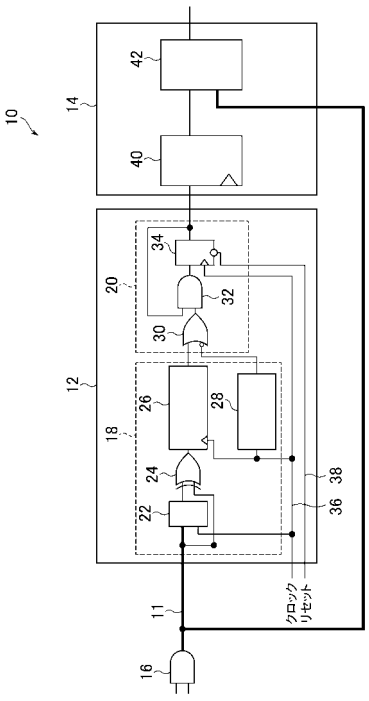
（出願人による申告）平成２８年度、総務省、戦略的情報通信研究開発推進事業、産業技術力強化法第１９条の適用を受ける特許出願

(71)出願人　899000068
学校法人早稲田大学
東京都新宿区戸塚町１丁目１０４番地
(74)代理人　100137800
弁理士　吉田　正義
(74)代理人　100148253
弁理士　今枝　弘充
(74)代理人　100148079
弁理士　梅村　裕明
(74)代理人　100158241
弁理士　吉田　安子
(72)発明者　戸川　望
東京都新宿区戸塚町１丁目１０４番地　学校法人早稲田大学内

最終頁に続く

(54)【発明の名称】集積回路の正常化方法、正常化回路、及び集積回路

(57)【要約】
【課題】ハードウェアトロイが存在していても正常に集積回路を動作させることができる集積回路の正常化方法、正常化回路及び集積回路を提供する。
【解決手段】正常化回路１０は、疑トロイネット１１に挿入され、認証部１２と、無効化部１４とを備え、前記認証部１２は、遷移カウンタ２６とクロックカウンタ２８とを有し、前記疑トロイネット１１の出力の遷移回数が、所定のクロック数において予め定められた閾値未満の場合、前記疑トロイネット１１をトロイネットであるとの判定結果を前記無効化部１４に出力し、前記無効化部１４は、前記トロイネットの出力を無効化する無効化素子４２を有することを特徴とする。
【選択図】図１



【特許請求の範囲】
【請求項１】
ハードウェアトロイに接続されている疑いのある疑トロイネットを含む集積回路を正常に動作させる正常化方法であって、
前記疑トロイネットの遷移回数が、所定のクロック数において予め定められた閾値未満の場合、前記疑トロイネットをトロイネットであると判定する工程と、
前記トロイネットの出力を無効化する工程と
を備えることを特徴とする正常化方法。
【請求項２】
前記遷移回数の閾値が３、前記クロック数の閾値が３２であることを特徴とする請求項１記載の正常化方法。
【請求項３】
ハードウェアトロイに接続されている疑いのある疑トロイネットを含む集積回路を正常に動作させる正常化回路であって、
前記疑トロイネットに挿入され、認証部と、無効化部とを備え、
前記認証部は、遷移カウンタとクロックカウンタとを有し、前記疑トロイネットの出力の遷移回数が、所定のクロック数において予め定められた閾値未満の場合、前記疑トロイネットをトロイネットであるとの判定結果を前記無効化部に出力し、
前記無効化部は、前記トロイネットの出力を無効化する無効化素子を有する
ことを特徴とする正常化回路。
【請求項４】
前記遷移回数の閾値が３、前記クロック数の閾値が３２であることを特徴とする請求項３記載の正常化回路。
【請求項５】
請求項３または請求項４の正常化回路を含むことを特徴とする集積回路。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、集積回路の正常化方法、正常化回路、及び集積回路に関し、特にハードウェアトロイが埋め込まれた集積回路を正常化する方法、正常化回路、及び集積回路に関する。
【背景技術】
【０００２】
近年、半導体業界においては、外部業者が情報処理装置に用いられる集積回路の製造に関わるようになったことから、集積回路の安全性が問題視されるようになっている。本来意図されていない機能（ハードウェアトロイ、以下「ＨＴ」とも記す。）を集積回路に埋め込むことが、第三者である外部業者において容易になったためであり、こうしたハードウェアトロイを検出することが求められている。
【０００３】
一般的には、ハードウェアトロイを検出するには、対象となる集積回路のハードウェアトロイに関する情報が必要とされてきた。ハードウェアトロイを含まない健全な設計データを利用して、ハードウェアトロイを検出する方法が提案されている（例えば、非特許文献１参照）。例えば、製造段階において挿入されたトロイの有無は、トロイが挿入されていない健全なチップと、トロイが挿入されたチップとの間で、物理的な重さや電力量、あるいは電磁波などについての差分をとることによって判断することができる。
【０００４】
ハードウェアトロイは、集積回路の製造段階のみならず設計段階においても埋め込まれる可能性がある。設計データに対して、ハードウェアトロイの個所を一度活性化させた後、その部分を無効化させるアプローチが提案されている（例えば非特許文献１）。
【先行技術文献】

【非特許文献】
【０００５】
【非特許文献１】M. Hicks, M. Finnicum, S. T. King, M. M. Martin, and J. M. Smith, “Overcoming an untrusted computing base: detecting and removing malicious hardware automatically,” in Proc. Symposium on Security and Privacy (SP), 2010, pp. 159-172
【発明の概要】
【発明が解決しようとする課題】
【０００６】
しかしながら、上記非特許文献１のように、ハードウェアトロイの個所を一度活性化させた後、その部分を無効化させるアプローチをとる場合、滅多に動作しないように設計されたハードウェアトロイは、動作させる方法を知ることはできないため、ハードウェアトロイを動作させることが困難であるという問題がある。また、だれが、いつ、どこでハードウェアトロイを作成し、埋め込んだのか不明であるから、集積回路に埋め込まれているハードウェアトロイを全て検出することは非常に困難であり、ハードウェアトロイに対するセキュリティ上の懸念を完全に解消することは期待できない。
【０００７】
そこで本発明は、ハードウェアトロイが存在していても正常に集積回路を動作させることができる正常化方法、正常化回路、及び集積回路を提供することを目的とする。
【課題を解決するための手段】
【０００８】
本発明に係る正常化方法は、ハードウェアトロイに接続されている疑いのある疑トロイネットを含む集積回路を正常に動作させる正常化方法であって、前記疑トロイネットの遷移回数が、所定のクロック数において予め定められた閾値未満の場合、前記疑トロイネットをトロイネットであると判定する工程と、前記トロイネットの出力を無効化する工程とを備えることを特徴とする。
【０００９】
本発明に係る正常化回路は、ハードウェアトロイに接続されている疑いのある疑トロイネットを含む集積回路を正常に動作させる正常化回路であって、前記疑トロイネットに挿入され、認証部と、無効化部とを備え、前記認証部は、遷移カウンタとクロックカウンタとを有し、前記疑トロイネットの出力の遷移回数が、所定のクロック数において予め定められた閾値未満の場合、前記疑トロイネットをトロイネットであるとの判定結果を前記無効化部に出力し、前記無効化部は、前記トロイネットの出力を無効化する無効化素子を有することを特徴とする。
【００１０】
本発明に係る集積回路は、上記正常化回路を含むことを特徴とする。
【発明の効果】
【００１１】
本発明によれば、疑トロイネットのうち、正常ネットの出力はそのままとし、トロイネットの出力のみを無効化することにより、ハードウェアトロイを含む集積回路を正常に動作させることができる。
【図面の簡単な説明】
【００１２】
【図１】本実施形態に係る正常化回路の構成を示すブロック図である。
【図２】疑トロイネットの説明に供するブロック図である。
【図３】疑トロイネットを認証する処理手順を示すフローチャートである。
【図４】正常ネットの出力と正常化回路の出力の変化を示すタイミングチャートであり、（Ａ）疑トロイネットの出力信号、（Ｂ）第３記憶素子からの処理信号、（Ｃ）処理結果信号である。
【図５】トロイネットの出力と正常化回路の出力の変化を示すタイミングチャートであり

、（Ａ）疑トロイネットの出力信号、（Ｂ）第３記憶素子からの処理信号、（Ｃ）処理結果信号である。

【発明を実施するための形態】

【００１３】

以下、図面を参照して本発明の実施形態について詳細に説明する。

【００１４】

集積回路は、複数の各種素子を含む回路で構成される。集積回路が備えるネットリストは、集積回路に含まれる各種素子や回路同士を接続する配線（以下、「ネット」いう。）の一覧を記述した設計データである。ネットは、問題のない正常なネット（以下、「正常ネット」という。）のみから構成されることが理想的である。

【００１５】

集積回路がハードウェアトロイを含む場合、集積回路にはさらにハードウェアトロイ回路が挿入される。ハードウェアトロイ回路は、ペイロード回路、トリガー回路を含む。ハードウェアトロイ回路は、ハードウェアトロイに含まれている特定のネットであるトロイネットが、ペイロード回路、トリガー回路、またはこれら２つの回路の間に存在する。本明細書では、トロイネットである可能性があるネットを疑トロイネットという。

【００１６】

本発明者らは、特願２０１４－２３３９５３において、ネットリストに含まれる疑トロイネットの中からトロイネットであることが明白なネットを検出する手法を確立している。疑トロイネットの中から明白なトロイネットを検出することによって、ハードウェアトロイの危険性を低減することができる。しかしながら、明白なトロイネットがないとしても疑トロイネットの中には、正常ネットの他にトロイネットが含まれている可能性がある。集積回路が備えるネットリスト中に疑トロイネットが存在している限り、当該集積回路は信頼性が高いとはいえない。

【００１７】

（全体構成）

図１に示す正常化回路１０は、疑トロイネット１１に挿入され、当該疑トロイネット１１のうち認証されなかったネット、すなわちトロイネットの出力を無効化することにより、集積回路（図示しない）を正常に動作させる。疑トロイネット１１は、疑トロイゲートを通じてハードウェアトロイに接続されている。

【００１８】

疑トロイネット１１の一例について、図２を参照して説明する。疑トロイゲートとしてＡＮＤ回路１６と、当該ＡＮＤ回路１６の入力として６個以上のＡＮＤ回路４６ａ～４６ｎが接続されている場合、ＡＮＤ回路１６の出力であるネットは、疑トロイネット１１である。その他の疑トロイネット１１の例は、上記特願２０１４－２３３９５３に記載されている。

【００１９】

正常化回路１０（図１）は、認証部１２と、無効化部１４とを備える。認証部１２は、監視モジュール１８と、管理モジュール２０とを有する。監視モジュール１８は、疑トロイネット１１の出力を監視し、その結果を管理モジュール２０へ出力する。監視モジュール１８は、第１記憶素子２２と、遷移判別素子２４と、遷移カウンタ２６と、クロックカウンタ２８とを含む。

【００２０】

第１記憶素子２２は、入力に疑トロイネット１１が接続され、クロック入力にクロック信号線が接続されており、出力が遷移判別素子２４の一方の入力に接続されている。第１記憶素子２２は、疑トロイネット１１からの出力信号とクロック信号線からのクロック信号とが入力され、１クロック前の疑トロイネット１１からの出力信号を、遷移判別素子２４に出力する。第１記憶素子２２は、フリップフロップで構成される。

【００２１】

遷移判別素子２４は、一方の入力に第１記憶素子２２の出力が接続され、他方の入力に

疑トロイネット１１が接続されており、出力が遷移カウンタ２６の入力に接続されている。遷移判別素子２４は、第１記憶素子２２から入力される１クロック前の疑トロイネット１１の出力と、現在のクロックの疑トロイネット１１の出力が異なる場合、疑トロイネット１１の出力が遷移したと判別し、Ｈレベルの遷移信号を出力する。一方、遷移判別素子２４は、第１記憶素子２２から入力される１クロック前の疑トロイネット１１の出力と、現在のクロックの疑トロイネット１１の出力が同じ場合、疑トロイネット１１の出力が遷移しなかったと判別し、Ｌレベルの遷移信号を出力する。遷移判別素子２４は、ＸＯＲ（排他的論理和）ゲートで構成される。

【００２２】

遷移カウンタ２６は、入力に遷移判別素子２４の出力が接続され、クロック入力にクロック信号線が接続されており、出力が管理モジュール２０へ接続されている。遷移カウンタ２６は、遷移判別素子２４から入力されるＨレベルの遷移信号をクロック毎にカウントし、当該遷移信号の数（以下、遷移回数という）に応じた遷移回数信号を出力する。すなわち遷移カウンタ２６は、遷移回数が、所定の閾値（$2^{M}-1$）未満の場合、遷移回数信号をＬレベルに保持し、所定の閾値（$2^{M}-1$）以上になった場合、遷移回数信号をＨレベルに変化させる。ここでＭは、遷移カウンタ２６のビット数である。

【００２３】

クロックカウンタ２８は、入力にクロック信号線が接続されており、出力が管理モジュール２０へ接続されている。クロックカウンタ２８は、クロック数に応じたクロック数信号を出力する。すなわちクロックカウンタ２８は、クロック数が所定の閾値2^{N}未満の場合、クロック数信号をＬレベルに保持し、クロック数が所定の閾値2^{N}以上になった場合クロック数信号をＨレベルに変化させる。ここでＮは、クロックカウンタ２８のビット数である。

【００２４】

管理モジュール２０は、認証素子３０と、管理値出力素子３２と、第２記憶素子３４とを含む。管理モジュール２０は、監視モジュール１８から出力された疑トロイネット１１の出力の監視結果に基づき、当該疑トロイネット１１のからの出力を有効化するか又は無効化するかを管理する。

【００２５】

認証素子３０は、一方の入力に遷移カウンタ２６の出力が接続され、他方の入力にクロックカウンタ２８の出力が接続されており、出力が管理値出力素子３２の入力に接続されている。認証素子３０は、遷移カウンタ２６からの遷移回数信号が入力され、クロックカウンタ２８からのクロック数信号が反転された状態で入力される。認証素子３０は、クロック数信号がＬレベル（反転された状態がＨレベル）のとき、Ｈレベルの認証信号を出力する。認証素子３０は、クロック数信号がＨレベル（反転された状態がＬレベル）に変化したとき、遷移回数信号がＨレベルであれば、疑トロイネット１１を正常ネットであると認証し、認証信号をＨレベルに保持する。一方、認証素子３０は、クロック数信号がＨレベル（反転された状態がＬレベル）であって、遷移回数信号がＬレベルの場合、疑トロイネット１１を認証せず、トロイネットであると判別し、Ｌレベルの認証信号を出力する。認証素子３０は、ＯＲ（論理和）ゲートで構成される。

【００２６】

管理値出力素子３２は、一方の入力に認証素子３０の出力が接続され、他方の入力に管理モジュール２０の出力が接続されており、出力が第２記憶素子３４に接続されている。なお、管理モジュール２０の出力は、初期段階では、Ｈレベルである。管理値出力素子３２は、認証素子３０からの認証信号が、ＨレベルであればＨレベルの管理値信号、ＬレベルであればＬレベルの管理値信号を出力する。管理値出力素子３２は、ＡＮＤ（論理積）ゲートで構成される。

【００２７】

第２記憶素子３４は、入力に管理値出力素子３２が接続され、クロック入力にクロック信号線が接続され、リセット入力にリセット信号線が接続されており、出力が無効化部１

４に接続されている。第２記憶素子３４は、管理値出力素子３２からの管理値信号を保持すると共に、管理値信号に応じた指示信号を出力する。なお指示信号は、初期段階においてＨレベルとする。第２記憶素子３４は、当該管理値信号がＬレベルであればＬレベルの指示信号を出力する。このように第２記憶素子３４は、Ｌレベルの管理値信号を受信し、疑トロイネット１１をトロイネットであると判別すると、その結果を管理値出力素子３２へフィードバックする。これにより、管理モジュール２０は、トロイネットであるとの判別結果を保持する。一方、第２記憶素子３４は、管理値信号がＨレベルであれば、指示信号をＨレベルのまま出力する。第２記憶素子３４は、リセット信号が入力されると、保持していた管理値信号を消去する。第２記憶素子３４は、揮発性のフリップフロップで構成される。

【００２８】

第２記憶素子３４の出力を管理値出力素子３２にフィードバックすることでトロイネットの判別結果が保存されるが、認証後もクロックが供給されて遷移カウンタ２６とクロックカウンタ２８が動作し、認証素子３０の値が遷移する可能性がある。そこで、管理値出力素子３２に管理モジュール２０の出力を接続することで、一度トロイネットと判定した後は認証素子３０の値に関わらず、管理モジュール２０がトロイネットの判別を保持し続けることが可能になる。

【００２９】

無効化部１４は、第３記憶素子４０と、無効化素子４２とを含む。第３記憶素子４０は、入力された指示信号を保持すると共に、当該指示信号に応じた処理信号を出力する。処理信号は、疑トロイネット１１の定常状態における出力信号のレベルによって選択される。本実施形態では、疑トロイネット１１の定常状態における出力信号がＬレベルである場合について説明する。この場合、第３記憶素子４０は、疑トロイネット１１が正常ネットであり第２記憶素子３４からＨレベルの指示信号が入力されると、処理信号をＨレベルのまま保持する。一方、第３記憶素子４０は、疑トロイネット１１がトロイネットであり第２記憶素子３４からＬレベルの指示信号が入力されると、処理信号をＬレベルに変化させる。なお、疑トロイネット１１の定常状態は、シミュレーションにより集積回路を動作させることで得られる。第３記憶素子は、不揮発性のフリップフロップで構成されるのが好ましい。

【００３０】

無効化素子４２は、一方の入力に第３記憶素子４０が接続され、他方の入力に疑トロイネット１１が接続されている。無効化素子４２は、第３記憶素子４０からの処理信号がＨレベルであれば、疑トロイネット１１からの出力信号と同じレベルの処理結果信号を出力する。一方、無効化素子４２は、第３記憶素子４０からの処理信号がＬレベルの場合、疑トロイネット１１からの出力信号が、定常状態のＬレベルからＨレベルに遷移したとき、Ｌレベルの処理結果信号を出力することで、疑トロイネット１１の出力を無効化する。無効化素子４２は、定常状態における疑トロイネット１１の出力信号がＬレベルのとき、ＡＮＤ（論理積）ゲートで構成される。

【００３１】

（認証処理）

次に、認証部１２における認証処理手順について、図３を参照して説明する。認証部１２は、本図に示す認証処理手順の開始ステップＲＴ１から入ってステップＳＰ１へ移る。ステップＳＰ１において認証部１２は、疑トロイネット１１からの出力信号が遷移したか否かを判定する。ステップＳＰ１において肯定結果が得られると、このことは疑トロイネット１１からの出力信号がＨレベルからＬレベル、又はＬレベルからＨレベルへ遷移したことを表しており、このとき認証部１２はステップＳＰ２へ移る。

【００３２】

ステップＳＰ２において認証部１２は、遷移カウンタ２６に１を加え、ステップＳＰ３へ移る。

【００３３】

一方、ステップＳＰ１において否定結果が得られると、このことは疑トロイネット１１からの出力信号がＨレベルのまま、又はＬレベルのままであることを表しており、このとき認証部１２はステップＳＰ３へ移る。

【００３４】

ステップＳＰ３において認証部１２は、クロックカウンタ２８に１を加え、ステップＳＰ４へ移る。

【００３５】

ステップＳＰ４において認証部１２は、クロックカウンタ２８の値が2^N以上か否か判定する。ステップＳＰ４において肯定結果が得られると、このことはクロック数が所定の閾値に達したことを表しており、このとき認証部１２はステップＳＰ５へ移る。一方、ステップＳＰ４において否定結果が得られると、認証部１２はステップＳＰ１へ戻り、クロックカウンタ２８の値が2^Nに達するまで、ステップＳＰ１からステップＳＰ３の処理ループを繰り返す。

【００３６】

ステップＳＰ５において認証部１２は、遷移カウンタ２６の値が（2^M-1）以上か否かを判定する。ステップＳＰ５において肯定結果が得られると、このことは遷移回数が所定の閾値に達したことを表しており、このとき認証部１２はステップＳＰ６へ移る。

【００３７】

ステップＳＰ６において認証部１２は、疑トロイネット１１を正常ネットであると認証し、ステップＳＰ８へ移り、認証処理手順を終了する。

【００３８】

一方、ステップＳＰ５において否定結果が得られると、認証部１２はステップＳＰ７へ移る。ステップＳＰ７において認証部１２は、疑トロイネット１１を正常ネットであるとは認証せず、すなわちトロイネットであると判別し、ステップＳＰ８へ移り、認証処理手順を終了する。

【００３９】

（動作及び効果）

次に上記のように構成された正常化回路１０の動作及び効果について説明する。まず、正常化回路１０を挿入すべき集積回路中の疑トロイネット１１を検出する。疑トロイネット１１を検出する方法については、上述の通り、特願２０１４－２３３９５３に記載の方法を用いることができる。

【００４０】

次いで、正常化回路１０は、検出された集積回路中の疑トロイネット１１に挿入される。すなわち、正常化回路１０は、疑トロイネット１１を切断し、その端部同士の間に挿入される。集積回路中に疑トロイネット１１が複数存在する場合には、それぞれの疑トロイネット１１毎に正常化回路１０が挿入される。

【００４１】

疑トロイネット１１に接続された正常化回路１０は、疑トロイネット１１からの出力信号を監視する。具体的には、認証部１２が、クロック数と、疑トロイネット１１からの出力信号の遷移回数とをカウントし、クロック数と遷移回数とが所定の閾値に達したか否かを判別する。本実施形態の場合、クロック数の閾値は2^N、遷移回数の閾値は（2^M-1）である。因みに、賢いハードウェアトロイは滅多に動作しないように設計されているので、所定のクロック数において、疑トロイネット１１からの出力信号の遷移回数が閾値に達した場合、監視モジュール１８は、当該疑トロイネット１１を問題のない正常ネットであると判別する。この場合、正常化回路１０は、当該疑トロイネット１１の出力信号を、そのまま出力する。

【００４２】

一方、所定のクロック数において、疑トロイネット１１からの出力信号の遷移回数が閾値に達しなかった場合、監視モジュール１８は、当該疑トロイネット１１をトロイネットであると判別する。この場合、正常化回路１０は、トロイネットの出力信号を、無効化す

る。
【００４３】
ここで図４を参照して、疑トロイネット１１が正常ネットである場合について説明する。Ｎが３、Ｍが２と仮定する。この場合、クロック数の閾値は８、遷移回数の閾値は３となる。本図は、正常ネットの出力と正常化回路の出力の変化を示すタイミングチャートであり、（Ａ）疑トロイネットの出力信号、（Ｂ）第３記憶素子からの処理信号、（Ｃ）処理結果信号を示し、横軸はクロック数を示す。
【００４４】
図４（Ａ）に示すように、疑トロイネット１１の出力信号は、クロック数が８になるまでの間（同図▼印）に４回遷移しているので、遷移回数は閾値の３以上である。したがって認証部１２は、当該疑トロイネット１１を正常ネットであると認証する。これにより無効化部１４は、第３記憶素子４０から出力する処理信号をＨレベルに保持することで（図４（Ｂ））、当該疑トロイネット１１からの出力信号と同じレベルの処理結果信号を出力する（図４Ｃ））。
【００４５】
一方、図５を参照して、疑トロイネット１１がトロイネットである場合について説明する。本図は、トロイネットの出力と正常化回路の出力の変化を示すタイミングチャートであり、（Ａ）疑トロイネットの出力信号、（Ｂ）第３記憶素子からの処理信号、（Ｃ）処理結果信号を示し、横軸はクロック数を示す。図５（Ａ）に示すように、クロック数が８になるまでの間（同図▼印）における疑トロイネット１１の遷移回数は１回であるので、遷移回数は閾値３未満である。したがって認証部１２は、当該疑トロイネット１１をトロイネットであると判別する。これにより無効化部１４は、第３記憶素子４０から出力する処理信号をＬレベルに変化させ（図５（Ｂ））、当該疑トロイネット１１からの出力信号が定常状態のＬレベルからＨレベルに遷移したとき、Ｌレベルの処理結果信号を出力する（図５（Ｃ））。これにより、疑トロイネット１１からの出力は、無効化される。
【００４６】
このようにして正常化回路１０は、疑トロイネット１１のうち、正常ネットの出力はそのままとし、トロイネットの出力のみを無効化することにより、ハードウェアトロイを含む集積回路を正常に動作させることができる。
【００４７】
正常化回路１０は、認証部１２と無効化部１４を備えるだけの簡単な構成で、上記の効果を得ることができる。
【００４８】
正常化回路１０は、第２記憶素子３４と第３記憶素子４０とを有するので、演算に遅延が生じた場合でも安全に動作することができる。
【００４９】
上記のような正常化回路１０は、外部業者によって設計された集積回路の設計データ中に、トロイネットであると断定できないネットを含むネットリストが存在する場合に、ユーザ側で当該ネットに挿入される使い方が想定される。
【００５０】
また認証部１２を含む検査装置を、集積回路を設計するＣＡＤ（computer-aided design）装置と一体化し、外部業者によって設計された集積回路の設計データを検査し、必要に応じ正常化回路１０を自動的に挿入することとしてもよい。
【００５１】
さらにＦＰＧＡ（field-programmable gate array）中に予め正常化回路１０を複数挿入しておき、検査結果に基づき正常化回路１０に配線をすることとしてもよい。
【００５２】
既知のネットリストを用いて、本実施形態に係る正常化回路１０が、疑トロイネット１１に含まれる正常ネットとトロイネットとを区別できる上記閾値を、シミュレーションにより求める。既知ネットリストは、米国のサイト（Trust-HUB）に公開されているベンチ

マークの中から、ランダムに６個選択する。ベンチマークには、トロイネットを含むとされているベンチマーク（HT-inserted）とトロイネットを含まないとされているベンチマーク（HT-free）とが含まれる。

【００５３】

Trust-HUBにおけるベンチマークは、ゲートレベルのネットリストが公開されている。下記表１に示されるように、これらのベンチマークは、ハードウェアトロイの有無（HT-inserted／HT-free）、ネット数、および疑トロイネット数が既知である。下記表１に示す６個のベンチマークのうちでは、２個が“HT-free”であり、４個が“HT-inserted”である。

【００５４】

【表１】

ベンチマーク	HTの有無	ネット数	疑トロイネット数
s15850	HT-free	2,429	5
s38417	HT-free	5,807	2
s38417-T100	HT-inserted	5,819	3
s38417-T200	HT-inserted	5,822	1
s38584-T300	HT-inserted	9,110	1
vga_lcd-T100	HT-inserted	70,157	2

【００５５】

各ベンチマークに含まれる疑トロイネットは、下記表２に示されるようにネット名、およびタイプ（正常ネットまたはトロイネット）も、ネットリスト中に明らかにされている。

【００５６】

【表２】

ベンチマーク	ネット名	タイプ
s15850	n1132	ノーマルネット
	n1440	ノーマルネット
	n1494	ノーマルネット
	n1509	ノーマルネット
	n1546	ノーマルネット
s38417	g25489	ノーマルネット
	n2401	ノーマルネット
s38417-T100	Tj_Trigger	トロイネット
	Tj_OUT1234	トロイネット
	Tj_OUT5678	トロイネット
s38417-T200	Tj_OUT1234	トロイネット
s38584-T300	Trigger_out	トロイネット
vga_lcd-T100	Tj_Trigger	トロイネット
	Tj_OUT1	トロイネット

【００５７】
上記表２に示されるように、“HT-free”であるとされているベンチマーク（s15850、s38417）に含まれている疑トロイネットは、いずれも正常ネットである。一方、“HT-inserted”であるとされているベンチマーク（s38417-T100、s38417-T200、s38584-T300、vga_lcd-T100）に含まれている疑トロイネットは、いずれもトロイネットである。
【００５８】
正常ネットおよびトロイネットのいずれであるかが既知の疑トロイネットに対し、Ｍ（正数）とＮ（２以上の正数）とを組み合わせて、パラメーター（Ｍ，Ｎ）を設定する。
【００５９】
ベンチマークに対して、論理シミュレータを用いてクロック数2^{N}だけ疑トロイネットを監視して、遷移回数をカウントする。カウントされた遷移回数が（$2^{M}-1$）以上の場合、疑トロイネットは正常ネットであると認証される。（Ｍ，Ｎ）の組み合わせを変更して、全ての疑トロイネットについて、認証結果と既知情報とが一致するか否かを調べる。
【００６０】
例えば、上記表１に示した６個のベンチマークについては、下記表３に示すような結果が得られる。
【００６１】

【表３】

ベンチマーク	ネット名	M=1 N=2	M=1 N=3	M=2 N=3	M=1 N=4	M=2 N=4	M=3 N=4	M=1 N=5	M=2 N=5	M=3 N=5	M=4 N=5	M=1 N=6	M=2 N=6	M=3 N=6	M=4 N=6	M=5 N=6
s15850	n1132	↘	↘	FP	↘	↘	FP	↘	↘	FP	FP	↘	↘	FP	FP	FP
	n1440	↘	↘	FP	↘	↘	↘	↘	↘	↘	↘	↘	↘	↘	↘	↘
	n1491	↘	↘	FP	↘	FP	FP	↘	↘	↘	FP	↘	↘	↘	↘	FP
	n1509	↘	↘	FP	↘	FP	FP	↘	↘	↘	FP	↘	↘	↘	↘	FP
	n1546	↘	↘	FP	↘	FP	FP	↘	↘	↘	FP	↘	↘	↘	↘	FP
s38417	g25489	FP	FP	FP	FP	FP	FP	↘	↘	FP	FP	↘	↘	↘	↘	↘
	n2401	FP	FP	FP	↘	↘	FP	↘	↘	↘	FP	↘	↘	↘	↘	FP
s38417-T100	Tj_Trigger	FN	FN	↘	FN	↘	↘	FN	↘	↘	↘	FN	↘	↘	↘	↘
	Tj_OUT1234	FN	FN	↘	FN	↘	↘	FN	↘	↘	↘	FN	↘	↘	↘	↘
	Tj_OUT5678	FN	FN	↘	FN	↘	↘	FN	↘	↘	↘	FN	↘	↘	↘	↘
s38417-T200	Tj_OUT1234	↘	↘	↘	↘	↘	↘	↘	↘	↘	↘	↘	↘	↘	↘	↘
s38584-T300	Trigger_out	↘	↘	↘	↘	↘	↘	↘	↘	↘	↘	↘	↘	↘	↘	↘
vga_lcd-T100	Tj_Trigger	↘	↘	↘	↘	↘	↘	↘	↘	↘	↘	↘	↘	↘	↘	↘
	Tj_OUT1	↘	↘	↘	↘	↘	↘	↘	↘	↘	↘	↘	↘	↘	↘	↘

【００６２】

上記表３においては、チェックマークは、既知情報と一致した正しい認証結果が得られることを示している。ＦＮはトロイネットを誤って正常ネットと認証し有効化した結果、ＦＰは正常ネットを誤ってトロイネットと判別し無効化した結果を示す。正常化回路は、（Ｍ，Ｎ）が（２，５）の場合、既知情報と一致した正しい認証結果を得ることができる。

【００６３】

さらに、上記のシミュレーションにより得られた（Ｍ，Ｎ）が（２，５）の閾値を用い、ハードウェアトロイを含むベンチマーク（RS232-T1000、Ethernet（登録商標）MAC10GE-T700）に正常化回路を挿入し、当該正常化回路がトロイネットの出力を無効化することができるか、シミュレーションにて検証する。RS232-T1000に含まれるトロイネットは、iRECEIVER_CTRLと、iCTRLであり、正常化回路は、シミュレーションの結果、これらのトロイネットの出力を正確に無効化することができた。この場合、正常化回路を挿入したことによる面積オーバーヘッドは約２０％、遅延オーバーヘッドは０であった。

【００６４】

またEthernet（登録商標）MAC10GE-T700に含まれるトロイネットは、Tj_OUTClockであり、正常化回路は、シミュレーションの結果、これらのトロイネットの出力を正確に無効化することができた。この場合、正常化回路を挿入したことによる面積オーバーヘッドは約０．０５％、遅延オーバーヘッドは０であった。

【００６５】

（変形例）

本発明は上記実施形態に限定されるものではなく、本発明の趣旨の範囲内で適宜変更することが可能である。

【００６６】

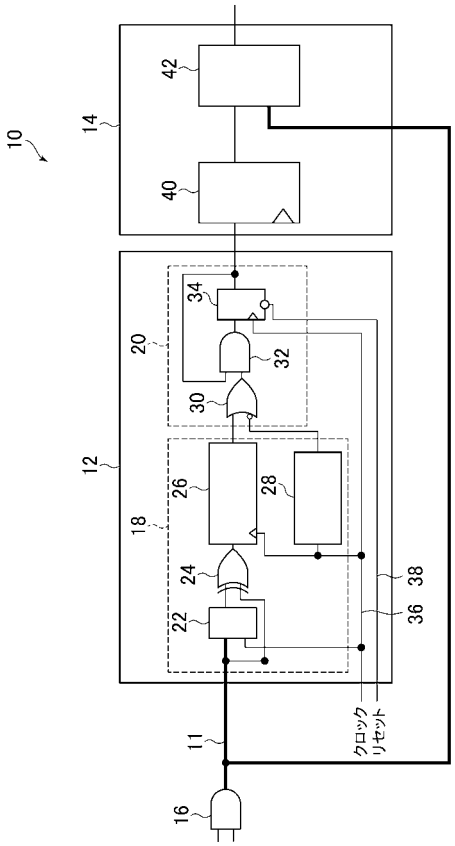
上記実施形態では、トロイネットの定常状態における出力信号がＬレベルの場合について説明したが、本発明はこれに限られず、トロイネットの定常状態における出力信号がＨレベルの場合も適用できる。この場合、第３記憶素子４０は、疑トロイネット１１が正常ネットであり第２記憶素子３４からＨレベルの指示信号が入力されると、Ｌレベルの処理信号を出力する。一方、第３記憶素子４０は、疑トロイネット１１がトロイネットであり第２記憶素子３４からＬレベルの指示信号が入力されると、Ｈレベルの処理信号を出力する。無効化素子４２は、処理信号がＬレベルであれば、疑トロイネット１１からの出力信号と同じレベルの処理結果信号を出力する。一方、無効化素子４２は、処理信号がＨレベルの場合、疑トロイネット１１からの出力信号がＨレベルからＬレベルに遷移したとき、Ｈレベルの処理結果信号を出力することで、疑トロイネット１１の出力を無効化する。このように定常状態における疑トロイネット１１の出力信号がＨレベルのとき、無効化素子４２はＯＲ（論理和）ゲートで構成される。

【符号の説明】

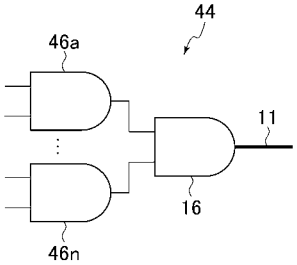
【００６７】

１０　正常化回路
１１　疑トロイネット
１２　認証部
１４　無効化部
２６　遷移カウンタ
２８　クロックカウンタ
４２　無効化素子

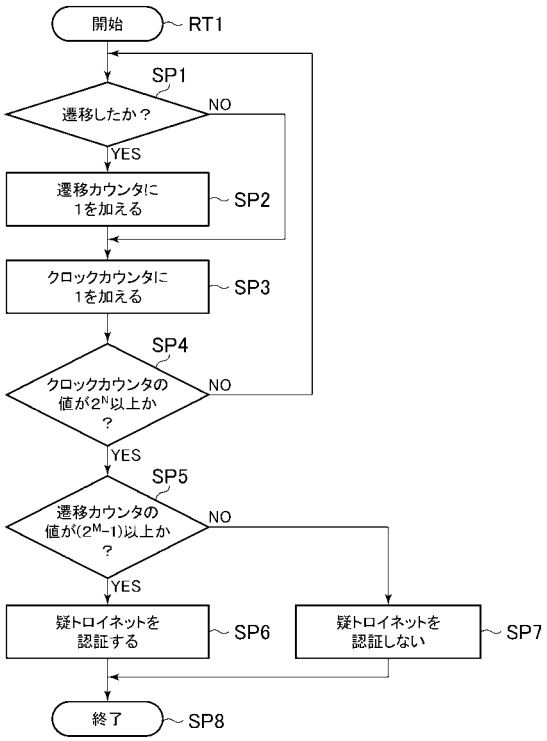
【図１】


10
14
42
40
12
20
34
32
30
18
26
28
24
22
38
36
クロック
リセット
11
16

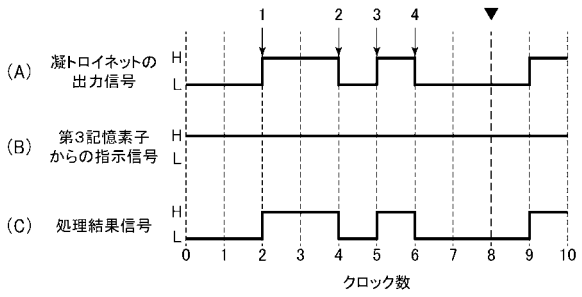
【図２】


44
46a
11
16
46n

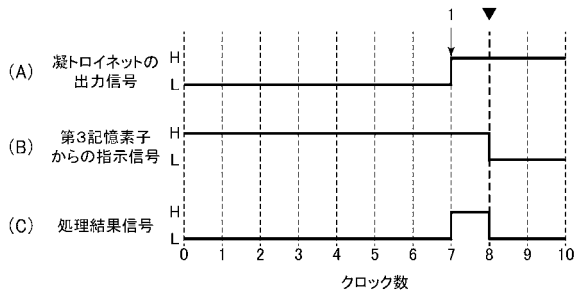
【図３】


開始
RT1
SP1
遷移したか？
NO
YES
遷移カウンタに
1を加える
SP2
クロックカウンタに
1を加える
SP3
SP4
クロックカウンタの
値が2^N以上か
？
NO
YES
SP5
遷移カウンタの
値が(2^M-1)以上か
？
NO
YES
疑トロイネットを
認証する
SP6
疑トロイネットを
認証しない
SP7
終了
SP8

【図４】


(A) 凝トロイネットの
出力信号
(B) 第3記憶素子
からの指示信号
(C) 処理結果信号
H
L
1
2
3
4
0 1 2 3 4 5 6 7 8 9 10
クロック数

【図５】


(A) 凝トロイネットの
出力信号
(B) 第3記憶素子
からの指示信号
(C) 処理結果信号
H
L
1
0 1 2 3 4 5 6 7 8 9 10
クロック数

フロントページの続き

(72)発明者　大屋　優
東京都新宿区戸塚町１丁目１０４番地　学校法人早稲田大学内