

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第6566576号
(P6566576)

(45) 発行日 令和1年8月28日(2019.8.28)

(24) 登録日 令和1年8月9日(2019.8.9)

(51) Int.Cl. F I
G O 6 F 21/56 (2013.01) G O 6 F 21/56

請求項の数 15 (全 31 頁)

<p>(21) 出願番号 特願2016-560230 (P2016-560230) (86) (22) 出願日 平成27年11月17日(2015.11.17) (86) 国際出願番号 PCT/JP2015/082223 (87) 国際公開番号 W02016/080380 (87) 国際公開日 平成28年5月26日(2016.5.26) 審査請求日 平成30年11月1日(2018.11.1) (31) 優先権主張番号 特願2014-233953 (P2014-233953) (32) 優先日 平成26年11月18日(2014.11.18) (33) 優先権主張国・地域又は機関 日本国(JP)</p> <p>(出願人による申告)平成26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</p>	<p>(73) 特許権者 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 日本国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</p> <p style="text-align: right;">最終頁に続く</p>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

(54) 【発明の名称】 ハードウェアトロイの検出方法、ハードウェアトロイの検出プログラム、およびハードウェアトロイの検出装置

(57) 【特許請求の範囲】

【請求項1】

集積回路のネットリスト中のハードウェアトロイを検出する検出方法であって、前記ハードウェアトロイの存在を示すトロイネットを含む既知ネットリストと、前記トロイネットを含まない既知ネットリストとの両方を含む複数の既知ネットリストに基づき、前記トロイネットの有無を判断するための条件を設定する条件設定工程と、前記条件に基づき、被検ネットリストとしての前記集積回路のネットリストを評価し、得られた評価結果から前記被検ネットリスト中のトロイネットの有無を判断する判断工程とを備えることを特徴とする検出方法。

【請求項2】

前記複数の既知ネットリストのそれぞれは、端子間ネットによって接続された一群の回路によって構成される構成ネットを少なくとも一つ含む集合ネットを、少なくとも一つ有し、前記被検ネットリストは、端子間ネットによって接続された一群の回路によって構成される構成ネットを少なくとも一つ含む集合ネットを、少なくとも一つ有し、前記条件設定工程は、前記複数の既知ネットリストのそれぞれについて、前記集合ネットに含まれる前記構成ネットの形態を基に、前記トロイネットを含む可能性がある構成ネットを対照ネットとして、前記複数の既知ネットリストから選択し、前記対照ネットにそれぞれ付与されるスコアに基づく条件設定を含み、

前記判断工程は、

前記被検ネットリストの中から前記対照ネットを検索し、前記検索された対照ネットのスコアを基に前記被検ネットリストの評価データを生成し、前記評価データと、前記設定された条件とを比較して、前記被検ネットリスト中のトロイネットの有無を判断することを特徴とする請求項 1 記載の検出方法。

【請求項 3】

前記スコアは、

前記複数の既知ネットリストの中で、ハードウェアトロイを含む前記既知ネットリストにのみ含まれる前記対照ネットの方が、ハードウェアトロイを含まない前記既知ネットリストにも含まれる前記対照ネットより大きく設定され、

10

前記条件設定工程は、

前記複数の既知ネットリストのそれぞれについて、含まれる集合ネット毎に対照ネットのスコアを加算して合計スコアを得、前記合計スコアのうち、前記複数の既知ネットリスト中で最も大きいスコアを前記複数の既知ネットリストの最大スコアとし、前記ハードウェアトロイを含む前記既知ネットリストの最大スコアを基に最大スコア閾値を設定する条件設定を含み、

前記判断工程は、

前記被検ネットリストに含まれる集合ネット毎に対照ネットのスコアを加算して合計スコアを得、前記合計スコアのうち、前記被検ネットリスト中で最も大きいスコアを前記被検ネットリストの最大スコアとし、前記被検ネットリストの前記最大スコアが前記最大スコア閾値以上のとき、前記被検ネットリストにトロイネットが存在すると判断することを特徴とする請求項 2 記載の検出方法。

20

【請求項 4】

前記条件設定工程は、

前記複数の既知ネットリストのそれぞれについて、前記最大スコアを有する集合ネットの数である最大スコアネット数を求め、前記ハードウェアトロイを含む前記既知ネットリストの最大スコアネット数を基に最大スコアネット数閾値を設定する条件設定を含み、

前記判断工程は、

前記最大スコアが前記最大スコア閾値未満の場合、

前記被検ネットリスト中で、前記最大スコアを有する集合ネットの数である最大スコアネット数を求め、前記被検ネットリストの前記最大スコアが前記最大スコア閾値未満であって、前記被検ネットリストの最大スコアネット数が、前記最大スコアネット数閾値より大きいとき、前記被検ネットリストにトロイネットが存在しないと判断することを特徴とする請求項 3 記載の検出方法。

30

【請求項 5】

前記条件設定工程は、

前記複数の既知ネットリスト中、前記最大スコアを有する集合ネットが、所定時間内に一定値を出力するクロック数を求め、前記ハードウェアトロイを含む既知ネットリストのクロック数と前記ハードウェアトロイを含まない既知ネットリストのクロック数とを基に最大一定サイクル数閾値を設定する条件設定をさらに含み、

40

前記判断工程は、

前記被検ネットリスト中、前記最大スコアを有する集合ネットが、所定時間内に一定値を出力するクロック数をさらに求め、前記被検ネットリストの最大スコアが前記最大スコア閾値未満であって、前記被検ネットリスト最大スコアネット数が、前記最大スコアネット数閾値以下であり、かつ、前記被検ネットリストについてのクロック数が前記最大一定サイクル数閾値以上の場合に、前記ハードウェアトロイが存在すると判断することを特徴とする請求項 4 記載の検出方法。

【請求項 6】

集積回路のネットリスト中のハードウェアトロイを検出する処理をコンピュータに実行させるための検出プログラムであって、

50

前記ハードウェアトロイの存在を示すトロイネットを含む既知ネットリストと、前記トロイネットを含まない既知ネットリストとの両方を含む複数の既知ネットリストに基づき、前記トロイネットの有無を判断するための条件を設定する条件設定工程と、前記条件に基づき、被検ネットリストとしての前記集積回路のネットリストを評価し、得られた評価結果から前記被検ネットリスト中のトロイネットの有無を判断する判断工程とを含む処理をコンピュータに実行させることを特徴とする検出プログラム。

【請求項 7】

前記複数の既知ネットリストのそれぞれは、端子間ネットによって接続された一群の回路によって構成される構成ネットを少なくとも一つ含む集合ネットを、少なくとも一つ有し、

10

前記被検ネットリストは、端子間ネットによって接続された一群の回路によって構成される構成ネットを少なくとも一つ含む集合ネットを、少なくとも一つ有し、

前記条件設定工程は、

前記複数の既知ネットリストのそれぞれについて、前記集合ネットに含まれる前記構成ネットの形態を基に、前記トロイネットを含む可能性がある構成ネットを対照ネットとして、前記複数の既知ネットリストから選択し、前記対照ネットにそれぞれ付与されるスコアに基づく条件設定を含み、

前記判断工程は、

前記被検ネットリストの中から前記対照ネットを検索し、前記検索された対照ネットのスコアを基に前記被検ネットリストの評価データを生成し、前記評価データと、前記設定された条件とを比較して、前記被検ネットリスト中のトロイネットの有無を判断することを特徴とする請求項 6 記載の検出プログラム。

20

【請求項 8】

前記スコアは、

前記複数の既知ネットリストの中で、ハードウェアトロイを含む前記既知ネットリストにのみ含まれる前記対照ネットの方が、ハードウェアトロイを含まない前記既知ネットリストにも含まれる前記対照ネットより大きく設定され、

前記条件設定工程は、

前記複数の既知ネットリストのそれぞれについて、含まれる集合ネット毎に対照ネットのスコアを加算して合計スコアを得、前記合計スコアのうち、前記複数の既知ネットリスト中で最も大きいスコアを前記複数の既知ネットリストの最大スコアとし、前記ハードウェアトロイを含む前記既知ネットリストの最大スコアを基に最大スコア閾値を設定する条件設定を含み、

30

前記判断工程は、

前記被検ネットリストに含まれる集合ネット毎に対照ネットのスコアを加算して合計スコアを得、前記合計スコアのうち、前記被検ネットリスト中で最も大きいスコアを前記被検ネットリストの最大スコアとし、前記被検ネットリストの前記最大スコアが前記最大スコア閾値以上のとき、前記被検ネットリストにトロイネットが存在すると判断することを特徴とする請求項 7 記載の検出プログラム。

【請求項 9】

40

前記条件設定工程は、

前記複数の既知ネットリストのそれぞれについて、前記最大スコアを有する集合ネットの数である最大スコアネット数を求め、前記ハードウェアトロイを含む前記既知ネットリストの最大スコアネット数を基に最大スコアネット数閾値を設定する条件設定を含み、

前記判断工程は、

前記最大スコアが前記最大スコア閾値未満の場合、

前記被検ネットリスト中で、前記最大スコアを有する集合ネットの数である最大スコアネット数を求め、前記被検ネットリストの前記最大スコアが前記最大スコア閾値未満であって、前記被検ネットリストの最大スコアネット数が、前記最大スコアネット数閾値より大きいとき、前記被検ネットリストにトロイネットが存在しないと判断する

50

ことを特徴とする請求項 8 記載の検出プログラム。

【請求項 10】

前記条件設定工程は、

前記複数の既知ネットリスト中、前記最大スコアを有する集合ネットが、所定時間内に一定値を出力するクロック数を求め、前記ハードウェアトロイを含む既知ネットリストのクロック数と前記ハードウェアトロイを含まない既知ネットリストのクロック数とを基に最大一定サイクル数閾値を設定する条件設定をさらに含み、

前記判断工程は、

前記被検ネットリスト中、前記最大スコアを有する集合ネットが、所定時間内に一定値を出力するクロック数をさらに求め、前記被検ネットリストの最大スコアが前記最大スコア閾値未満であって、前記被検ネットリスト最大スコアネット数が、前記最大スコアネット数閾値以下であり、かつ、前記被検ネットリストについてのクロック数が前記最大一定サイクル数閾値以上の場合に、前記ハードウェアトロイが存在すると判断する

10

ことを特徴とする請求項 9 記載の検出プログラム。

【請求項 11】

集積回路のネットリスト中のハードウェアトロイを検出する検出装置であって、

前記ハードウェアトロイの存在を示すトロイネットを含む既知ネットリストと、前記トロイネットを含まない既知ネットリストとの両方を含む複数の既知ネットリストに基づき、前記トロイネットの有無を判断するための条件を設定する条件設定手段と、

前記条件に基づき、被検ネットリストとしての前記集積回路のネットリストを評価し、得られた評価結果から前記被検ネットリスト中のトロイネットの有無を判断する判断手段とを備えることを特徴とする検出装置。

20

【請求項 12】

前記複数の既知ネットリストのそれぞれは、端子間ネットによって接続された一群の回路によって構成される構成ネットを少なくとも一つ含む集合ネットを、少なくとも一つ有し、

前記被検ネットリストは、端子間ネットによって接続された一群の回路によって構成される構成ネットを少なくとも一つ含む集合ネットを、少なくとも一つ有し、

前記条件設定手段は、

前記複数の既知ネットリストのそれぞれについて、前記集合ネットに含まれる前記構成ネットの形態を基に、前記トロイネットを含む可能性がある構成ネットを対照ネットとして、前記複数の既知ネットリストから選択し、前記対照ネットにそれぞれ付与されるスコアに基づく条件設定を含み、

30

前記判断手段は、

前記被検ネットリストの中から前記対照ネットを検索し、前記検索された対照ネットのスコアを基に前記被検ネットリストの評価データを生成し、前記評価データと、前記設定された条件とを比較して、前記被検ネットリスト中のトロイネットの有無を判断する

ことを特徴とする請求項 11 記載の検出装置。

【請求項 13】

前記スコアは、

前記複数の既知ネットリストの中で、ハードウェアトロイを含む前記既知ネットリストにのみ含まれる前記対照ネットの方が、ハードウェアトロイを含まない前記既知ネットリストにも含まれる前記対照ネットより大きく設定され、

40

前記条件設定手段は、

前記複数の既知ネットリストのそれぞれについて、含まれる集合ネット毎に対照ネットのスコアを加算して合計スコアを得、前記合計スコアのうち、前記複数の既知ネットリスト中で最も大きいスコアを前記複数の既知ネットリストの最大スコアとし、前記ハードウェアトロイを含む前記既知ネットリストの最大スコアを基に最大スコア閾値を設定する条件設定を含み、

前記判断手段は、

50

前記被検ネットリストに含まれる集合ネット毎に対照ネットのスコアを加算して合計スコアを得、前記合計スコアのうち、前記被検ネットリスト中で最も大きいスコアを前記被検ネットリストの最大スコアとし、前記被検ネットリストの前記最大スコアが前記最大スコア閾値以上のとき、前記被検ネットリストにトロイネットが存在すると判断することを特徴とする請求項 1 2 記載の検出装置。

【請求項 1 4】

前記条件設定手段は、

前記複数の既知ネットリストのそれぞれについて、前記最大スコアを有する集合ネットの数である最大スコアネット数を求め、前記ハードウェアトロイを含む前記既知ネットリストの最大スコアネット数を基に最大スコアネット数閾値を設定する条件設定を含み、

10

前記判断手段は、

前記最大スコアが前記最大スコア閾値未満の場合、

前記被検ネットリスト中で、前記最大スコアを有する集合ネットの数である最大スコアネット数を求め、前記被検ネットリストの前記最大スコアが前記最大スコア閾値未満であって、前記被検ネットリストの最大スコアネット数が、前記最大スコアネット数閾値より大きいとき、前記被検ネットリストにトロイネットが存在しないと判断する

ことを特徴とする請求項 1 3 記載の検出装置。

【請求項 1 5】

前記条件設定手段は、

前記複数の既知ネットリスト中、前記最大スコアを有する集合ネットが、所定時間内に一定値を出力するクロック数を求め、前記ハードウェアトロイを含む既知ネットリストのクロック数と前記ハードウェアトロイを含まない既知ネットリストのクロック数とを基に最大一定サイクル数閾値を設定する条件設定をさらに含み、

20

前記判断手段は、

前記被検ネットリスト中、前記最大スコアを有する集合ネットが、所定時間内に一定値を出力するクロック数をさらに求め、前記被検ネットリストの最大スコアが前記最大スコア閾値未満であって、前記被検ネットリスト最大スコアネット数が、前記最大スコアネット数閾値以下であり、かつ、前記被検ネットリストについてのクロック数が前記最大一定サイクル数閾値以上の場合に、前記ハードウェアトロイが存在すると判断する

ことを特徴とする請求項 1 4 記載の検出装置。

30

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、ハードウェアトロイの検出方法、ハードウェアトロイの検出プログラム、およびハードウェアトロイの検出装置に関する。

【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きている。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。）を集積回路に挿入することが、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。

40

【0003】

一般的には、ハードウェアトロイを検出するには、対象となる情報処理装置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。

50

【 0 0 0 4 】

しかしながら、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挿入される可能性がある。設計段階では、製造段階の場合のような差分をとることができず、ハードウェアトロイに関する情報なしにトロイを検出する技術は未だ得られていないのが現状である。

【 0 0 0 5 】

図 1 4 に示すように、ハードウェアトロイ (H T) 回路 4 6 が存在する回路 4 0 においては、例えば通常回路 4 2 を接続する通常ネット 4 4 の一部 4 8 にトリガー回路 4 6 b が接続され、通常ネット 4 4 の他の一部 4 9 にペイロード回路 4 6 a が接続されている。ペイロード回路 4 6 a は、本来意図されていない機能を有し、トリガー回路 4 6 b はペイロード回路 4 6 a を起動する。こうしたペイロード回路 4 6 a とトリガー回路 4 6 b とによって、H T 回路 4 6 が構成される。

10

【 0 0 0 6 】

回路 4 0 から H T 回路 4 6 を完全に排除することができれば、ハードウェアトロイの危険性を完全に排除することが可能となる。

【 先行技術文献 】

【 非特許文献 】

【 0 0 0 7 】

【 非特許文献 1 】 B. Cha and S. K. Gupta, "Trojan detection via delay measurement s: a new approach to select paths and vectors to maximize effectiveness and minimize cost," in Proc. Design, Automation and Test in Europe (DATE), 2013, pp. 12 65-1270

20

【 発明の概要 】

【 発明が解決しようとする課題 】

【 0 0 0 8 】

しかしながら、H T 回路 4 6 は必ずしも明確に存在せずに通常ネット 4 4 に融合していることもあり、H T 回路 4 6 を区別して回路 4 0 から完全に区別することは極めて困難である。

【 0 0 0 9 】

本発明は以上の点を考慮してなされたもので、集積回路のハードウェアトロイに関する情報を用いずに、ハードウェアトロイを検出する検出方法、ハードウェアトロイの検出プログラム、およびハードウェアトロイの検出装置を提供することを目的とする。

30

【 課題を解決するための手段 】

【 0 0 1 0 】

本発明に係るハードウェアトロイの検出方法は、集積回路のネットリスト中のハードウェアトロイを検出する検出方法であって、前記ハードウェアトロイの存在を示すトロイネットを含む既知ネットリストと、前記トロイネットを含まない既知ネットリストとの両方を含む複数の既知ネットリストに基づき、前記トロイネットの有無を判断するための条件を設定する条件設定工程と、前記条件に基づき、被検ネットリストとしての前記集積回路のネットリストを評価し、得られた評価結果から前記被検ネットリスト中のトロイネットの有無を判断する判断工程とを備えることを特徴とする。

40

【 0 0 1 1 】

上記検出方法においては、前記複数の既知ネットリストのそれぞれは、端子間ネットによって接続された一群の回路によって構成される構成ネットを少なくとも一つ含む集合ネットを、少なくとも一つ有し、前記被検ネットリストは、端子間ネットによって接続された一群の回路によって構成される構成ネットを少なくとも一つ含む集合ネットを、少なくとも一つ有し、前記条件設定工程は、前記複数の既知ネットリスト中のそれぞれについて、前記集合ネットに含まれる前記構成ネットの形態を基に、前記トロイネットを含む可能性がある構成ネットを対照ネットとして、前記複数の既知ネットリストから選択し、前記対照ネットにそれぞれ付与されるスコアに基づく条件設定を含み、前記判断工程は、前記

50

被検ネットリストの中から前記対照ネットを検索し、前記検索された対照ネットのスコアを基に前記被検ネットリストの評価データを生成し、前記評価データと、前記設定された条件とを比較して、前記被検ネットリスト中のトロイネットの有無を判断することができる。

【0012】

前記スコアは、前記複数の既知ネットリストの中で、ハードウェアトロイを含む前記既知ネットリストにのみ含まれる前記対照ネットの方が、ハードウェアトロイを含まない前記既知ネットリストにも含まれる前記対照ネットより大きく設定され、前記条件設定工程は、前記複数の既知ネットリストのそれぞれについて、含まれる集合ネット毎に対照ネットのスコアを加算して合計スコアを得、前記合計スコアのうち、前記複数の既知ネットリスト中で最も大きいスコアを前記複数の既知ネットリストの最大スコアとし、前記ハードウェアトロイを含む前記既知ネットリストの最大スコアを基に最大スコア閾値を設定する条件設定を含み、前記判断工程は、前記被検ネットリストに含まれる集合ネット毎に対照ネットのスコアを加算して合計スコアを得、前記合計スコアのうち、前記被検ネットリスト中で最も大きいスコアを前記被検ネットリストの最大スコアとし、前記被検ネットリストの前記最大スコアが前記最大スコア閾値以上のとき、前記被検ネットリストにトロイネットが存在すると判断することができる。

10

【0013】

また、前記条件設定工程は、前記複数の既知ネットリストのそれぞれについて、前記最大スコアを有する集合ネットの数である最大スコアネット数を求め、前記ハードウェアトロイを含む前記既知ネットリストの最大スコアネット数を基に最大スコアネット数閾値を設定する条件設定を含み、前記判断工程は、前記最大スコアが前記最大スコア閾値未満の場合、前記被検ネットリスト中で、前記最大スコアを有する集合ネットの数である最大スコアネット数を求め、前記被検ネットリストの前記最大スコアが前記最大スコア閾値未満であって、前記被検ネットリストの最大スコアネット数が、前記最大スコアネット数閾値より大きいとき、前記被検ネットリストにトロイネットが存在しないと判断することができる。

20

【0014】

さらに、前記条件設定工程は、前記複数の既知ネットリスト中、前記最大スコアを有する集合ネットが、所定時間内に一定値を出力するクロック数を求め、前記ハードウェアトロイを含む既知ネットリストのクロック数と前記ハードウェアトロイを含まない既知ネットリストのクロック数とを基に最大一定サイクル数閾値を設定する条件設定をさらに含み、前記判断工程は、前記被検ネットリスト中、前記最大スコアを有する集合ネットが、所定時間内に一定値を出力するクロック数をさらに求め、前記被検ネットリストの最大スコアが前記最大スコア閾値未満であって、前記被検ネットリスト最大スコアネット数が、前記最大スコアネット数閾値以下であり、かつ、前記被検ネットリストについてのクロック数が前記最大一定サイクル数閾値以上の場合に、前記ハードウェアトロイが存在する判断することができる。

30

【0015】

本発明に係るハードウェアトロイの検出プログラムは、集積回路のネットリスト中のハードウェアトロイを検出する処理をコンピュータに実行させるための検出プログラムであって、前記ハードウェアトロイの存在を示すトロイネットを含む既知ネットリストと、前記トロイネットを含まない既知ネットリストとの両方を含む複数の既知ネットリストに基づき、前記トロイネットの有無を判断するための条件を設定する条件設定工程と、前記条件に基づき、被検ネットリストとしての前記集積回路のネットリストを評価し、得られた評価結果から前記被検ネットリスト中のトロイネットの有無を判断する判断工程とを含む処理をコンピュータに実行させることを特徴とする。

40

【0016】

本発明に係るハードウェアトロイの検出装置は、集積回路のネットリスト中のハードウェアトロイを検出する検出装置であって、前記ハードウェアトロイの存在を示すトロイネ

50

ットを含む既知ネットリストと、前記トロイネットを含まない既知ネットリストとの両方を含む複数の既知ネットリストに基づき、前記トロイネットの有無を判断するための条件を設定する条件設定手段と、前記条件に基づき、被検ネットリストとしての前記集積回路のネットリストを評価し、得られた評価結果から前記被検ネットリスト中のトロイネットの有無を判断する判断手段とを備えることを特徴とする。

【発明の効果】

【0017】

本発明によれば、公知ネットリストの既知情報に基づいて得られた条件に基づき、被検ネットリスト中のトロイネットの有無を判断することにより、公知ネットリストと種類が異なるネットリストを有する集積回路にハードウェアトロイが含まれるか否かを判断することができる。したがって本発明によれば、対象となる集積回路の、ハードウェアトロイが挿入されていない健全なネットリストやハードウェアトロイに関する公知情報を用いずに、上記集積回路にハードウェアトロイが含まれるか否かを判断することができる。

10

【図面の簡単な説明】

【0018】

【図1】本実施形態のハードウェアトロイ検出装置の使用状態を示す図である。

【図2】本実施形態のハードウェアトロイ検出装置の構成を示すブロック図である。

【図3】Case 1の対照ネットを示す説明図である。

【図4】Case 2の対照ネットを示す説明図である。

【図5】Case 3の対照ネットを示す説明図である。

20

【図6】Case 4の対照ネットを示す説明図である。

【図7】Case 5の対照ネットを示す説明図である。

【図8】Case 6の対照ネットを示す説明図である。

【図9】Case 7の対照ネットを示す説明図である。

【図10】Case 8の対照ネットを示す説明図である。

【図11】Case 9の対照ネットを示す説明図である。

【図12】最大一定サイクル数を説明する図である。

【図13】ネットリスト中のハードウェアトロイの有無を判断する比較判定の処理手順を示すフローチャートである。

【図14】ハードウェアトロイ（HT）回路を模式的に説明する図である。

30

【発明を実施するための形態】

【0019】

1. 全体構成

以下、図面を参照して本発明の実施の形態を詳述する。図1に示すように情報処理装置10は、ハードウェアトロイ検出装置（以下、「検出装置」という。）20に接続される。これにより、情報処理装置10が備えるネットリスト（以下、「被検ネットリスト」という。）が検出装置20に入力され得る。被検ネットリストは、情報処理装置10に含まれる各種回路同士を接続する配線の一覧を記述した設計データである。被検ネットリストは、情報処理装置を構成する回路の階層に合わせて構築された階層を有し、最上位層である集合ネットと、当該集合ネットの下位層である構成ネットを備える。集合ネット及び構成ネットは、情報処理装置の規模に応じて1つ以上設けられる。構成ネットは、回路の端子間を繋ぐ配線（以下、「端子間ネット」という。）によって接続された一群の回路によって構成される。

40

【0020】

本図に示す情報処理装置10は、端子間ネットである通常ネット44で接続された通常回路42で構成される。情報処理装置10がハードウェアトロイを含む場合、さらにHT回路46が挿入される。HT回路46は、ペイロード回路46a、トリガー回路46bを含む。HT回路46は、ハードウェアトロイに含まれている特定の端子間ネットであるトロイネットが、ペイロード回路46a、トリガー回路46b、またはこれら2つの回路の間に存在する。情報処理装置10の被検ネットリストには、端子間ネットとして、通常ネ

50

ット44と、トロイネットとが含まれる。

【0021】

図2に示すように、検出装置20は、検出装置20の各種機能を統括的に制御する制御手段24、条件設定手段26、および判断手段28が、制御バス22を介して接続されている。

【0022】

制御手段24は、予め格納されている基本プログラムなどの各種プログラムを読み出して、これら各種プログラムに従って、検出装置20全体を制御するようになされている。

【0023】

条件設定手段26は、対照ネット取得部26aと、第1の閾値設定部26bと、第2の閾値設定部26cと、条件設定部26dとから構成される。条件設定手段26は、被検ネットリスト中におけるトロイネットの有無を判断するための基準を、トロイネットの有無が既知である公知のネットリスト(以下、「公知ネットリスト」という。)から取得し、得られた基準に基づいてトロイネットの有無を判断するための閾値および条件を設定する。なお、実施の形態では、既知ネットリストとして公知ネットリストを使用しているが、必ずしも既知ネットリストが公知である必要はない。トロイネットの有無が既知であれば、公知でなくても構わない。

10

【0024】

判断手段28は、第1の評価データ生成部28aと第2の評価データ生成部28bと比較判定部28cとから構成される。判断手段28は、情報処理装置10の被検ネットリストを、条件設定手段26で設定された基準で評価して、得られた評価結果(評価データ)を条件設定手段26で設定された閾値を含む条件で判定する。こうして、情報処理装置10の被検ネットリスト中のトロイネットの有無を判断することによってハードウェアトロイを検出する。

20

【0025】

(1) 条件設定手段

次に、条件設定手段26の各部について説明する。

【0026】

(対照ネット取得部)

対照ネット取得部26aは、端子間ネットに関する情報が公開されているゲートレベルの公知ネットリストに基づき、トロイネットの特徴を抽出する。対照ネット取得部26aは、例えばネットワークを介して情報記録サーバーに接続し、公知ネットリストを、情報記録サーバーからランダムに複数個ダウンロードして、これらを図示しない記憶部に記憶する。

30

【0027】

公知ネットリストは、例えば米国のサイト(Trust-HUB)に公開されているベンチマークのネットリストを利用することができる。すなわち、公開されているベンチマークの中から、ランダムに複数、例えば10個選択してもよい。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。

40

【0028】

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。ベンチマークは、端子間ネットで接続されたゲート、フリップフロップ、加算器などのセルを含むいくつかのサブモジュールからなる。

【0029】

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)および端子間ネット数が既知である。下記表1に示す10個のベンチマークのうちでは、7個が“HT-inserted”であり、3個が“HT-free”である。ベンチマークには、ハードウェアトロイに含まれているトロイネット(以下、「公知トロイネット」という。)の名称、種類およびその存在箇所といった情報も、ネットリスト中に明ら

50

かにされている。

【 0 0 3 0 】

【 表 1 】

ベンチマーク	タイプ	ネット数
b19	HT-free	108,332
EthernetMAC10GE	HT-free	103,206
s35932	HT-free	6,423
EthernetMAC10GE-T700	HT-inserted	103,220
RS232-T1000	HT-inserted	311
s15850-T100	HT-inserted	2,456
s38417-T100	HT-inserted	5,819
s38584-T200	HT-inserted	7,580
vga_lcd-T100	HT-inserted	70,162
wb_conmax-T100	HT-inserted	22,197

10

20

【 0 0 3 1 】

対照ネット取得部 2 6 a は、公知ネットリストに基づき、トロイネットである可能性がある端子間ネット（以下、「疑トロイネット」という。）を見出す。すなわち、疑トロイネットは、公知ネットリストの集合ネットに含まれる構成ネットの形態、すなわち各種回路の組み合わせや個数等から見出すことができる。疑トロイネットを含む構成ネットを対照ネットと呼ぶ。例えば、上記表 1 に示した 1 0 個のベンチマークから、図 3 ~ 1 1 に示す 9 個の対照ネットを見出すことができる。図 3 ~ 1 1 中、LSLG(little switching logic gate)は、AND回路、NAND回路、OR回路、NORゲート回路を意味する。図中の太線が疑トロイネットである。ハードウェアトロイは動作し難く制御性が高いため、特定の条件のみ動作する。すなわち、ハードウェアトロイは、スイッチング確率が低い。図 3 ~ 1 1 に示したCase 1 ~ 9の対照ネットはいずれも、こうした特徴を含むものである。Case 1 ~ 9の各対照ネットについて以下に説明する。

30

【 0 0 3 2 】

Case 1 (図 3) においては、1st LSLGの入力として2nd LSLGの出力が含まれている。2nd LSLGの入力の数が 6 以上であれば、1st LSLGの出力の端子間ネットが疑トロイネットである。2nd LSLGは、入力の数が 2 つの 2 入力のものに限定されず、3 入力または 4 入力のものでもよい。

【 0 0 3 3 】

Case 2 (図 4) は、Case 1 の特別な場合であり、Case 1 より動作し難い。1st LSLGの入力として2nd LSLGの出力を含み、この2nd LSLGの入力の数が 1 6 個以上の場合、または2nd LSLGの入力として3rd LSLGの出力を含み、この3rd LSLGの入力の数が 1 6 個以上の場合、2nd LSLGの出力を入力として含む1st LSLGの出力の端子間ネットが疑トロイネットである。

40

【 0 0 3 4 】

Case 3 (図 5) は、MUX (multiplexer) の選択信号の端子間ネットが疑トロイネットである。

【 0 0 3 5 】

Case 4 (図 6) においては、ADDER (半加算器または全加算器) の出力を入力としても

50

つセルを2nd any cellとし、2nd any cellの出力を入力としてもつセルを1st any cellとする。この場合、1st any cellの入力および出力の端子間ネットは、全て疑トロイネットである。全ての2nd any cellにADDERが接続されている必要はなく、図示するように1つの2nd any cellにADDERが接続されていれば、このCase 4に該当する。

【 0 0 3 6 】

Case 5 (図7) は、FF (フリップフロップ) を含むサブモジュールの主出力の端子間ネットが疑トロイネットである。

【 0 0 3 7 】

Case 6 (図8) においては、他のネットを介さずに、“0” または “1” がFFに直接入力されており、特殊なケースである。このようなFFの出力およびクロックの端子間ネットは、疑トロイネットである。

10

【 0 0 3 8 】

Case 7 (図9) においては、FFのクロックがCase 2の端子間ネット (疑トロイネット) である。Case 2のネットは極めて動き難いので、このようなFFの入力、出力、およびクロックの端子間ネットの全ては、疑トロイネットである。

【 0 0 3 9 】

Case 8 (図10) においては、構成ネットより下位のサブモジュールネットの数が22000以上のサブモジュールにおいて、任意セルの入力の端子間ネットの一つが主入力であり、もう一つはCase 2の端子間ネット (疑トロイネット) である。この場合、Case 2の疑トロイネットは、真のトロイネット (以下「真トロイネット」という。) である可能性がより高い。

20

【 0 0 4 0 】

Case 9 (図11) においては、スキャンモードとノーマルモードとを制御するTEST-SE信号の否定信号がセルに入力されている。こうしたセルの入力および出力の端子間ネットは、疑トロイネットである。

【 0 0 4 1 】

上記対照ネットには、疑トロイネットが真トロイネットである可能性の高さに適応したスコアが付与される。スコアは、疑トロイネットが真トロイネットである可能性の高さを反映できるように設定する。すなわち、“HT-inserted” の公知ネットリストのみに含まれている対照ネットは、“HT-inserted” および “HT-free” の両方の公知ネットリストに

30

【 0 0 4 2 】

含まれている対照ネットよりも、真トロイネットを含む可能性が高いので、大きなスコアが与えられる。

例えば、上記表1に示した10個のベンチマークのネットリストと前述の9個の対照ネット (Case 1~9) とを比較したところ、Case 6~9の対照ネットは、7個の “HT-inserted” のベンチマークのみに存在することが確認された。残りのCase 1~5の対照ネットは、7個の “HT-inserted” のベンチマークおよび3個の “HT-free” のベンチマークの全てに確認された。Case 1~5の対照ネットは、疑トロイネットを有しているにもかかわらず、Case 1~5の対照ネットが含まれている公知ネットリストのうち3個は “HT-free” である。すなわち、Case 6~9の対照ネットのほうが、Case 1~5の対照ネットよりも真トロイ

40

【 0 0 4 3 】

ネットを含む可能性が高いといえる。このような真トロイネットを含む可能性の高さを反映して、Case 1~5の対照ネットのスコアを1と設定し、Case 6~9の対照ネットのスコアを2と設定する。真トロイネットを含む可能性の高さを反映した所定の大きさのスコアを付与することにより、対照ネットは、被検ネットリスト中のトロイネットの有無を判断するための基準となる。

【 0 0 4 4 】

以上のとおり、対照ネット取得部26aは、公知ネットリストから対照ネットを取得し、真トロイネットを含む可能性の高さを反映した所定の大きさのスコアを対照ネットに付与し、これを図示しない記憶部に記憶する。

50

(第1の閾値設定部)

第1の閾値設定部26bは、第1の閾値としての最大スコア閾値(T_{score})(T_{score} は正数)および最大スコアネット数閾値(T_{number})(T_{number} は正数)を選択する。

【0045】

最大スコア閾値(T_{score})は、最大スコア(X_{score})の中から選択される。最大スコア(X_{score})は、集合ネットに含まれる対照ネットのスコアを加算した合計スコアのうち、公知ネットリスト中で最も大きいスコアとする。

【0046】

最大スコアネット数閾値(T_{number})は、最大スコアネット数(X_{number})の中から選択される。最大スコアネット数(X_{number})は、公知ネットリスト中の最大スコア(X_{score})を有する集合ネット(以下、「最大スコアネット」という。)の数とする。

10

【0047】

具体的には、第1の閾値設定部26bは、記憶部から受け取った“HT-inserted”の公知ネットリストおよび“HT-free”の公知ネットリスト中の各集合ネットに含まれる構成ネットのそれぞれを、対照ネットと比較する。第1の閾値設定部26bは、構成ネットが対照ネットと一致する場合、当該対照ネットのスコアを集合ネット毎に加算する。この集合ネット毎に加算されたスコアを合計スコアと呼ぶ。合計スコアのうち、公知ネットリスト中、最も大きいスコアを最大スコア(X_{score})、最大スコア(X_{score})を有する集合ネットを最大スコアネットとする。また、第1の閾値設定部26bは、公知ネットリスト中の最大スコアネットの数を最大スコアネット数(X_{number})とする。

20

【0048】

第1の閾値設定部26bは、最大スコアネットと、記憶部に記憶された公知トロイネットの情報を比較して、最大スコアネット中に公知トロイネットが含まれる公知ネットリストを抽出する。第1の閾値設定部26bは、公知トロイネットが含まれる公知ネットリストのうち、最大スコア(X_{number})の最も小さい値を選択して1を加えた値を最大スコア閾値(T_{score})として図示しない記憶部に記憶する。

【0049】

例えば、上記表1に示した10個のベンチマークを前述の9個の対照ネット(Case1~9)と比較し、各ベンチマークのネットリストについて確認された対照ネットの数を下記表2にまとめる。

30

【0050】

【表 2】

	Case 1	Case 2	Case 3	Case 4	Case 5	Case 6	Case 7	Case 8	Case 9
b19	598	38	1108	16586	130	0	0	0	0
EthernetMAC10GE	344	55	2595	417	193	0	0	0	0
s35932	0	0	0	0	420	0	0	0	0
Ethernet MAC10GE-T700	347	56	2595	417	193	3	3	0	0
RS232-T1000	11	2	2	0	12	0	0	0	0
s15850-T100	80	11	1	0	160	2	4	0	3
s38417-T100	206	4	0	0	206	0	0	0	0
s38584-T200	112	4	4	87	405	0	0	0	0
vga_lcd-T100	19	0	1954	168	209	0	0	0	0
wb_conmax-T100	466	55	0	0	1516	0	0	1	0

10

20

【 0 0 5 1 】

各ベンチマークの集合ネット毎に合計スコアを算出し、その最大値を最大スコア (X_{score}) とし、最大スコア (X_{score}) を有する集合ネットを最大スコアネットとする。上述したとおり、Case 1~5のスコアは1であり、Case 6~9のスコアは2である。例えば、Case 1~9の対照ネットのうちの1つも含まない集合ネットは、合計スコアが0であり、Case 1の対照ネットを1つ含む集合ネットの合計スコアは1である。また、Case 1の対照ネットを1つとCase 6の対照ネットを1つ含む集合ネットの合計スコアは3である。

【 0 0 5 2 】

得られた結果を、最大スコアネットの内容(通常ネット/トロイネット)とともに下記表3にまとめる。ここで、表3中の最大スコアネットの内容は、公知トロイネットの情報に基づくものである。

30

【 0 0 5 3 】

【表 3】

ベンチマーク	最大スコア (X_{score})	最大スコアネット数 (X_{number})	最大スコアネットの内容
b19	2	73	通常ネットのみ
EthernetMAC10GE	2	55	通常ネットのみ
s35932	1	420	通常ネットのみ
EthernetMAC10GE-T700	6	1	トロイネットのみ
RS232-T1000	2	2	トロイネットのみ
s15850-T100	6	1	トロイネットのみ
s38417-T100	2	5	通常ネットとトロイネット
s38584-T200	3	1	トロイネットのみ
vga_lcd-T100	2	2	トロイネットのみ
wb_conmax-T100	4	1	トロイネットのみ

10

20

【0054】

上記表 3 に示されるように、最大スコア (X_{score}) が 3 以上のベンチマーク (Ethernet (登録商標) MAC10GE-T700、s15858-T100、s38584-T200、wb_conmax-T100) において、最大スコアネットに含まれている対照ネットは全てトロイネットである。ベンチマーク (RS 232-T1000、s38417-T100、vga_lcd-T100) に示されているように、最大スコア (X_{score}) が 2 の最大スコアネットにも公知トロイネットが含まれている。公知トロイネットを含む最大スコアネットの最大スコアの値は、2 が最小である。最大スコアの最小値に 1 を加えた値 (最小値 + 1) を、最大スコア閾値 (T_{score}) とする。すなわち、最大スコア (X_{score}) の値が最大スコア閾値 (T_{score}) 以上であれば、最大スコアネットにトロイネットが含まれる可能性が高いといえる。表 3 の例では、最大スコア閾値 (T_{score}) は 3 である。

30

【0055】

なお、本実施の形態では、上述のような手法で最大スコア閾値 (T_{score}) を求めたが、他の手法により最大スコア閾値 (T_{score}) を求めることも可能である。例えば、最大スコアネットに含まれている対照ネットが全てトロイネットとなる最小の値を、最大スコア閾値 (T_{score}) とするなどの手法が挙げられる。

【0056】

上記表 3 によれば、公知トロイネットを含む最大スコアネット数 (X_{number}) は比較的小さく、その値は最大でも 5 である。これに対して、通常ネットのみを含む最大スコアネット数 (X_{number}) は大きく、その値は最小でも 55 である。最大スコア (X_{score}) が高いほど最大スコアネット数 (X_{number}) は減少し、最大スコア (X_{score}) が低いほど最大スコアネット数 (X_{number}) は増加する。

40

【0057】

したがって、最大スコアネット数 (X_{number}) が十分に大きなネットリストは、トロイネットを含まない“HT-free”である可能性が高いと判断する。上記表 3 によれば、公知トロイネットを含む最大スコアネットのうち、最大スコアネット数 (X_{number}) の最も大きな値は、ベンチマーク (s38417-T100) の 5 である。

【0058】

この場合、ベンチマーク (s38417-T100) の最大スコアネット数 (X_{number}) である 5 を、最大スコアネット数閾値 (T_{number}) とする。すなわち、最大スコアネット数 (X_{number}) が最大スコアネット数閾値 (T_{number}) 以下であれば、最大スコアネットにトロイネット

50

トが含まれる可能性が高いといえる。こうして、最大スコアネット数閾値 (T_{number}) が選択される。

【0059】

以上のとおり、第1の閾値設定部26bは、対照ネットと公知トロイネットの情報を比較することにより、最大スコア閾値 (T_{score}) と最大スコアネット数閾値 (T_{number}) とを選択して第1の閾値として取得し、これを図示しない記憶部に記憶する。

【0060】

(第2の閾値設定部)

第2の閾値設定部26cは、公知ネットリストにおける最大スコアネットについて最大一定サイクル数 (X_{cycle}) を生成し、第2の閾値としての最大一定サイクル数閾値 (T_{cycle}) (T_{cycle} は正数) を選択する。具体的には、第2の閾値設定部26cは、最大スコア (X_{score}) が最大スコア閾値 (T_{score}) 未満の最大スコアネットに対して、論理シミュレータと呼ばれる既存のソフトウェア (例えばVCS (登録商標)) でランダムデータを入力して1Mクロック間における値の変化をシミュレートし、一定値を出力する最長のクロック数を最大一定サイクル数 (X_{cycle}) として得て、これを図示しない記憶部に記憶する。

10

【0061】

第2の閾値設定部26cは、得られた最大一定サイクル数 (X_{cycle}) のなかから、最小の値を最大一定サイクル数閾値 (T_{cycle}) として選択する。

【0062】

例えば、図12に示すように、1Mクロック間で一定値を出力する最長のクロック数を、最大一定サイクル数 (Max constant cycles) として定義する。最大一定サイクル数が高いほど、最大スコアネットはトロイネットを含む可能性が高くなる。これは、次のように説明される。トロイネットは動作し難く制御性が高いため、トロイネットが存在する場合には、長期間にわたって一定値が出力されることが予測される。この点に着目し、所定のクロック間で一定値が出力されるサイクル数 (最大一定サイクル数) によって、最大スコアネットにトロイネットが含まれるか否かを判断する。

20

【0063】

下記表4には、ベンチマーク (RS232-T1000、s38417-T100、およびvga_lcd-T100) について、最大一定サイクル数 (X_{cycle}) を公知トロイネットの名称とともにまとめる。下記表4に示した3個のベンチマークは、上記表3に示したとおり最大スコア (X_{score}) が2で、最大スコアネットにトロイネットが含まれている。

30

【0064】

【表4】

ベンチマーク	トロイネット名	最大一定サイクル数 (X_{cycle})
RS232-T1000	iRECEIVER_CTRL	999,999
	iCTRL	999,999
s38417-T100	Tj_Trigger	999,997
	Tj_OUT1234	999,997
	Tj_OUT5678	999,996
vga_lcd-T100	Tj_Trigger	999,999
	Tj_OUT1	999,999

40

【0065】

上記表4によれば、ベンチマーク (RS232-T1000、s38417-T100、およびvga_lcd-T100) は全て、最大スコアネットの最大一定サイクル数 (X_{cycle}) が999,996サイクル以上である。このことから、最大一定サイクル数 (X_{cycle}) が999,996サイクル以上の最大スコア

50

ネットにはトロイネットが含まれていると判断して、999,996サイクルを最大一定サイクル数閾値 (T_{cycle}) とする。すなわち最大一定サイクル数閾値 (T_{cycle}) (999,996サイクル) は、公知トロイネットを含む最大スコアネットについての最大一定サイクル数 (X_{cycle}) の最小値である。

【0066】

なお、上記表3, 4からは、最大一定サイクル数 (X_{cycle}) が999,996サイクル以上の場合には、最大スコアネットに公知トロイネットが含まれていることがわかる。その一方、下記表5に示すように、最大一定サイクル数 (X_{cycle}) が999,996サイクル以上の最大スコアネットに通常ネットが含まれていることも確認された。

【0067】

【表5】

ベンチマーク	最大スコア (X_{score})	最大一定サイクル数が999,996 以上の最大スコアネットの数	最大スコアネット の内容
b19	2	59	通常ネットのみ
EthernetMAC10GE	2	10	通常ネットのみ
s35932	1	0	該当せず
RS232-T1000	2	2	トロイネットのみ
s38417-T100	2	3	トロイネットのみ
vga_lcd-T100	2	2	トロイネットのみ

【0068】

上記表5に示されるとおり、最大スコア (X_{score}) が1のベンチマーク (s35932) には、最大一定サイクル数 (X_{cycle}) が999,996サイクル以上の最大スコアネットは存在しない。ベンチマーク (b19およびEthernetMAC10GE) は、いずれも最大スコア (X_{score}) が2で、最大スコアネットに含まれているのは通常ネットのみである。公知トロイネットが含まれていないにもかかわらず、ベンチマーク (b19およびEthernetMAC10GE) には、最大一定サイクル数 (X_{cycle}) が999,996サイクル以上の最大スコアネットが存在している。そのような最大スコアネットの数は、それぞれ59および10である。

【0069】

最大スコア (X_{score}) と最大一定サイクル数 (X_{cycle}) とを用いても、公知トロイネットの有無は必ずしも正確に判断されていない。これは、回路の規模 (端子間ネット数) が関連しているものと推測される。上記表1に示されるように、ベンチマーク (s35932) の端子間ネット数は6,423であり、ベンチマーク (b19およびEthernetMAC10GE) の端子間ネット数は、それぞれ108,332および103,206である。こうした端子間ネット数からわかるように、ベンチマーク (s35932) は小規模回路であり、ベンチマーク (b19およびEthernetMAC10GE) は大規模回路である。最大スコア (X_{score}) および最大一定サイクル数 (X_{cycle}) に加えて、最大スコアネット数 (X_{number}) を用いることによって、小規模回路のみならず、大規模回路に対しても誤検出なく正確にトロイネットを検出できる。

【0070】

以上のとおり、第2の閾値設定部26cは、最大一定サイクル数閾値 (T_{cycle}) を第2の閾値として取得して、これを図示しない記憶部に記憶する。

【0071】

(条件設定部)

条件設定部26dは、最大スコア閾値 (T_{score})、最大スコアネット数閾値 (X_{number})

10

20

30

40

50

)、および最大一定サイクル数閾値 (X_{cycle}) を記憶部から受け取って、これらの閾値を用いて、トロイネットの有無について、記憶されている公知ネットリストのハードウェアトロイの有無 (HT-inserted / HT-free) と一致した結果が得られる条件を設定する。トロイネットの有無を判断する条件は、以下の (A) , (B) である。いずれかの条件を満たす場合には、トロイネットが存在する。

(A) 最大スコア (X_{score}) が最大スコア閾値 (T_{score}) (T_{score} は正数) 以上

(B) 最大スコア (X_{score}) が最大スコア閾値 (T_{score}) (T_{score} は正数) 未満、最大スコアネット数 (X_{number}) が最大スコアネット数閾値 (T_{number}) (T_{number} は正数) 以下、かつ最大一定サイクル数 (X_{cycle}) が最大一定サイクル数閾値 (T_{cycle}) (T_{cycle} は正数) 以上

【0072】

例えば、上記表1に示した10個のベンチマークについては、トロイネットが存在するのは、次のいずれかの場合である。

(a) 最大スコア (X_{score}) が3以上

(b) 最大スコア (X_{score}) が3未満、最大スコアネット数 (X_{number}) が5以下、かつ最大一定サイクル数 (X_{cycle}) が999,996サイクル以上

【0073】

上記表1に示した10個のベンチマークについて、条件(a) , (b) と各ベンチマークについての既知情報のハードウェアトロイの有無 (HT-free / HT-inserted) とを、下記表6にまとめる。下記表6においては、条件(a) または条件(b) を満たしていれば “ ” としている。なお、「条件(a) または条件(b) 」を、「条件(a / b) 」と記載する。

【0074】

【表6】

ベンチマーク	条件		タイプ
	a	b	
b19	—	—	HT-free
EthernetMAC10GE	—	—	HT-free
s35932	—	—	HT-free
EthernetMAC10GE-T700	○		HT-inserted
RS232-T1000		○	HT-inserted
s15850-T100	○		HT-inserted
s38417-T100		○	HT-inserted
s38584-T200	○		HT-inserted
vga_lcd-T100		○	HT-inserted
wb_conmax-T100	○		HT-inserted

【0075】

“HT-free” である3個のベンチマークは、条件(a / b) を満たしていない。一方、“HT-inserted” である7個のベンチマークは、条件(a / b) を満たしており、条件(a / b) による判定はベンチマークの既知の情報によるハードウェアトロイの有無 (HT-free / HT-inserted) と完全に一致している。このように検出装置10は、最大スコア閾値 (T_{score})、最大スコアネット数閾値 (T_{number})、および最大一定サイクル数閾値 (T_{cy}

10

20

30

40

50

T_{cycle})に基づいたトロイネットの有無を決定する条件 (a / b) を用いて判定することによって、ベンチマークが “HT-free” および “HT-inserted” のいずれであるかを正しく識別できる。

【 0 0 7 6 】

以上のとおり、条件設定部 2 6 d は、最大スコア閾値 (T_{score})、最大スコアネット数閾値 (T_{number})、および最大一定サイクル数閾値 (T_{cycle}) を用いてトロイネットの有無を判断する条件 (A) , 条件 (B) を設定し、これを図示しない記憶部に記憶する。

【 0 0 7 7 】

こうして、条件設定手段 2 6 は、トロイネットを含む可能性を反映した大きさのスコアが付与された複数の対照ネットを取得するとともに、第 1 の閾値としての最大スコア閾値 (T_{score}) (T_{score} は正数) および最大スコアネット数閾値 (T_{number}) (T_{number} は正数) と、第 2 の閾値としての最大一定サイクル数閾値 (T_{cycle}) (T_{cycle} は正数) を設定し、第 1 および第 2 の閾値を用いてトロイネットの有無を判断する条件を設定する。

【 0 0 7 8 】

条件設定手段 2 6 は、基準としての対照ネットを、閾値 (最大スコア閾値 (T_{score}) (T_{score} は正数)、最大スコアネット数閾値 (T_{number}) (T_{number} は正数)、最大一定サイクル数閾値 (T_{cycle}) (T_{cycle} は正数)) およびこれを用いて設定された条件とともに、図示しない記憶部に記憶する。記憶された基準、閾値および条件は、ネットリスト中のトロイネットの有無を判断するために判断手段 2 8 に送出される。

【 0 0 7 9 】

(2) 判断手段

次に、判断手段 2 8 について説明する。判断手段 2 8 は、情報処理装置 1 0 から被検ネットリストを取得し、当該被検ネットリストを記憶部から受け取った基準で評価する。判断手段 2 8 は、評価結果を評価データとして得、記憶部から受け取った条件で評価データを判定してハードウェアトロイの有無を判断する。

【 0 0 8 0 】

また、判断手段 2 8 は、公知ネットリストから抽出した基準としての対照ネットを、閾値 (最大スコア閾値 (T_{score}) (T_{score} は正数)、最大スコアネット数閾値 (T_{number}) (T_{number} は正数)、最大一定サイクル数閾値 (T_{cycle}) (T_{cycle} は正数)) および条件とともに図示しない記憶部から適宜受け取る。

【 0 0 8 1 】

(第 1 の評価データ生成部)

第 1 の評価データ生成部 2 8 a は、被検ネットリストについて、最大スコアネットに関する情報 (最大スコア (X_{score}) および最大スコアネット数 (X_{number})) を得る。被検ネットリストについての最大スコア (X_{score}) および最大スコアネット数 (X_{number}) は、条件設定手段 2 6 における第 1 の閾値設定部 2 6 b について説明した手順と同様の手順で得られる。

【 0 0 8 2 】

こうして、第 1 の評価データ生成部 2 8 a は、被検ネットリストについて最大スコア (X_{score}) と最大スコアネット数 (X_{number}) とを得て、これを第 1 の評価データとして図示しない記憶部に記憶する。記憶された第 1 の評価データは、比較判定部 2 8 c に送出される。第 1 の評価データは、被検ネットリストの中から対照ネットを検索し、検索された対照ネットのスコアを基に生成される。

【 0 0 8 3 】

(第 2 の評価データ生成部)

第 2 の評価データ生成部 2 8 b は、被検ネットリストにおける最大スコアネットについて、最大一定サイクル数 (X_{cycle}) を生成する。被検ネットリストについての最大一定サイクル数 (X_{cycle}) は、条件設定手段 2 6 における第 2 の閾値設定部 2 6 c について説明した手順と同様の手順で得られる。

【 0 0 8 4 】

10

20

30

40

50

こうして、第2のデータ生成部28bは、被検ネットリストについて最大一定サイクル数(X_{cycle})を得て、これを第2の評価データとして図示しない記憶部に記憶する。記憶された第2の評価データは、比較判定部28cに送出される。

【0085】

(比較判定部)

比較判定部28cにおいては、比較判定プログラムに従って比較判定処理が行われる。具体的には、比較判定部28cは、被検ネットリストから得た第1の評価データおよび第2の評価データを、第1の閾値および第2の閾値に基づいて得られた条件と比較し、被検ネットリストにトロイネットが含まれるか否かを判定する。以下、比較判定処理手順について図13を参照して説明する。

10

【0086】

比較判定処理にあたっては、図13に示す比較判定処理手順RT1の開始ステップから入って、ステップSP1に移る。

【0087】

比較判定部28cは、ステップSP1において、被検ネットリストの最大スコア(X_{score})が、最大スコア閾値(T_{score})以上であるか否かを判断する。ステップSP1において肯定結果が得られると、このことは、被検ネットリストがトロイネットを含み“HT-inserted”であることを表しており、このとき比較判定部28cはステップSP5へ移る。

【0088】

20

一方、ステップSP1において否定結果が得られると、比較判定部28cはステップSP2に移る。ステップSP2において比較判定部28cは最大スコアネット数(X_{number})が最大スコアネット数閾値(T_{number})以下であるか否かを判断する。ステップSP2において否定結果が得られると、このことは、被検ネットリストにはトロイネットは含まれておらず“HT-free”であることを表しており、このとき比較判定部28cはステップSP6へ移る。

【0089】

ステップSP2において肯定結果が得られると、比較判定部28cはステップSP3に移る。ステップSP3において比較判定部28cは最大一定サイクル数(X_{cycle})が最大一定サイクル数閾値(T_{cycle})以上であるか否かを判断する。ステップSP3において肯定結果が得られると、このことは、被検ネットリストがトロイネットを含み“HT-inserted”であることを表しており、このとき比較判定部28cはステップSP5へ移る。

30

【0090】

ステップSP3において否定結果が得られると、比較判定部28cはステップSP4へ移る。ステップSP4において比較判定部28cは、全ての最大スコアネットについて、最大一定サイクル数(X_{cycle})を最大一定サイクル数閾値(T_{cycle})と比較したか否かを判断する。

【0091】

ステップSP4において否定結果が得られると、このことは、最大一定サイクル数(X_{cycle})が最大一定サイクル数閾値(T_{cycle})と比較されていない最大スコアネットが残っていることを表しており、このとき比較判定部28cはステップSP3に戻る。

40

【0092】

ステップSP4において肯定結果を得ると、このことは被検ネットリストにはトロイネットは含まれておらず“HT-free”であることを表しており、ステップSP6へ移る。

【0093】

ステップSP5において比較判定部28cは、被検ネットリストがトロイネットを含むことを示す出力信号を生成して出力し、ステップSP7へ移り、比較判定処理手順RT1を終了する。

【0094】

またステップSP6において比較判定部28cは、被検ネットリストがトロイネットを

50

含まないことを示す出力信号を生成して出力し、ステップS P 7へ移り、比較判定処理手順R T 1を終了する。

【0095】

判断手段28は、比較判定部から得られた出力信号に基づき、判定結果を図示しない表示手段に出力する。表示手段は、出力信号に基づいた出力結果を表示する。

【0096】

2. 効果

上記構成において、検出装置20は、公知ネットリストから対照ネットを抽出し、さらに第1の閾値および第2の閾値を選択して、予め条件を設定する。そして検出装置20は、情報処理装置10の被検ネットリストを取得すると、当該被検ネットリストに対照ネットが含まれるか否かを判断する。被検ネットリストに対照ネットが含まれている場合、検出装置20は、当該対照ネットに基づき、第1の評価データおよび第2の評価データを生成する。検出装置20は、予め設定された条件に基づき、生成された第1の評価データおよび第2の評価データを評価し、これにより被検ネットリストにトロイネットが含まれるか否かを判断する。

10

【0097】

以上のとおり、本実施形態に係る検出装置20は、公知ネットリストの既知情報に基づいて得られた条件に基づき、被検ネットリスト中のトロイネットの有無を判断することにより、公知ネットリストと種類が異なるネットリストを有する情報処理装置10にハードウェアトロイが含まれるか否かを判断することができる。したがって検出装置20は、対象となる情報処理装置10の、ハードウェアトロイが挿入されていない健全なネットリストやハードウェアトロイに関する公知情報を用いずに、情報処理装置10にハードウェアトロイが含まれるか否かを判断することができる。

20

【0098】

一例として、上記表1に示した10個のベンチマークから、(Case 1~9)の9個の対照ネットが得られること、このときの最大スコア閾値(T_{score})、最大スコアネット数閾値(T_{number})、および最大一定サイクル数閾値(T_{cycle})は、それぞれ3、5、および99,996であること、さらに、閾値を用いてトロイネットの有無を判断する条件が以下のとおり設定されることを示した。

(a) 最大スコア(X_{score})が3以上

30

(b) 最大スコア(X_{score})が3未満、最大スコアネット数(X_{number})が5以下、かつ最大一定サイクル数(X_{cycle})が99,996サイクル以上

【0099】

こうしたハードウェアトロイの検出方法の一例を、被検ネットリストとして他の公知ネットリストに適用してトロイネットの有無を判断し、その結果を既知情報と比較することにより、本実施形態に係るハードウェアトロイの検出方法の正当性を確認した。

【0100】

他の公知ネットリストとしては、Trust-HUBで公開されている全ベンチマーク34個を用いた。Trust-HUBで公開されている全ベンチマーク34個のうち、“HT-inserted”のベンチマークは25個であり、“HT-free”のベンチマークは9個である。こうした34個のベンチマークを所定の基準で評価して、評価結果を所定の条件で判定した。

40

【0101】

まず、各ベンチマークに含まれている構成ネットを、上述の9個の対照ネット(Case 1~9)と比較した。各ベンチマークについて、含まれている対照ネットの数を求め、最大スコア(X_{score})および最大スコアネット数(X_{number})を得た。その結果を、対照ネットの数とともに下記表7, 8にまとめる。下記表7, 8には、上記表1に示した10個のベンチマークについての結果も併せて示した。

【0102】

【 表 7 】

	Case 1	Case 2	Case 3	Case 4	Case 5	Case 6	Case 7	Case 8	Case 9	最大スコア (X_{score})	最大スコアネット数 (X_{number})
b19-T100	822	43	84	16701	131	0	0	0	0	3	1
b19-T200	822	43	84	16701	131	0	0	0	0	3	1
EthernetMAC10GE-T700	347	56	2595	417	193	3	3	0	0	6	1
EthernetMAC10GE-T710	347	56	2595	417	193	3	3	0	0	6	1
EthernetMAC10GE-T720	347	56	2595	417	193	3	3	0	0	6	1
EthernetMAC10GE-T730	347	56	2595	417	193	3	3	0	0	6	1
RS232-T1000	11	2	2	0	12	0	0	0	0	2	2
RS232-T1100	11	2	2	0	12	0	0	0	0	2	2
RS232-T1200	10	2	2	0	12	0	0	0	0	2	2
RS232-T1300	9	2	2	0	12	0	0	0	0	2	2
RS232-T1400	12	3	2	0	12	0	0	0	0	2	3
RS232-T1500	11	2	2	0	12	0	0	0	0	2	2
RS232-T1600	9	2	2	0	12	0	0	0	0	2	2
s15850-T100	80	11	1	0	160	2	4	0	3	6	1
s35932-T100	3	3	1	0	420	2	2	0	4	8	1
s35932-T200	3	3	0	0	420	0	0	0	4	4	3
s35932-T300	3	3	1	0	420	0	0	0	4	5	1
s38417-T100	206	4	0	0	206	0	0	0	0	2	5
s38417-T200	203	3	0	0	206	0	0	0	0	2	4
s38417-T300	206	4	0	0	206	4	4	0	0	6	1
s38584-T100	112	3	2	0	404	0	0	0	4	3	2
s38584-T200	112	4	4	87	405	0	0	0	0	3	1
s38584-T300	123	16	3	783	405	0	0	0	0	3	1
vga_lcd-T100	19	0	1954	168	209	0	0	0	0	2	2
wb_conmax-T100	466	55	0	0	1516	0	0	1	0	4	1

【 0 1 0 3 】

10

20

30

40

【表 8】

	Case 1	Case 2	Case 3	Case 4	Case 5	Case 6	Case 7	Case 8	Case 9	最大スコア (X_{score})	最大スコアネット数 (X_{number})
b19	598	38	1108	16586	130	0	0	0	0	2	77
EthernetMAC10GE	344	55	2595	417	193	0	0	0	0	2	55
RS232	5	0	2	0	12	0	0	0	0	1	19
s15850	68	5	0	0	160	0	0	0	0	2	5
s35932	0	0	0	0	420	0	0	0	0	1	420
s38417	199	1	0	0	206	0	0	0	0	2	2
s38584	110	3	2	0	404	0	0	0	0	2	9
vga_lcd	16	0	1954	161	209	0	0	0	0	1	2340
wb_conmax	455	52	0	0	1516	0	0	0	0	2	48

10

20

30

40

【 0 1 0 4 】

3 4 個の全てのベンチマークの最大スコア (X_{score}) および最大スコアネット数 (X_{num}) 50

ber) について、上述の条件 (a / b) を満たすか否かを調べ、その結果を既知情報によるハードウェアトロイの有無 (HT-free / HT-inserted) とともに下記表 9 にまとめる。下記表 9 には、前述の 10 個のベンチマークについての結果も併せて示した。下記表 9 においては、条件 (a / b) を満たしていれば、“ ” としている。

【 0 1 0 5 】

【表 9】

ベンチマーク	条件(a/b)	タイプ
b19-T100	○	HT-inserted
b19-T200	○	HT-inserted
EthernetMAC10GE-T700	○	HT-inserted
EthernetMAC10GE-T710	○	HT-inserted
EthernetMAC10GE-T720	○	HT-inserted
EthernetMAC10GE-T730	○	HT-inserted
RS232-T1000	○	HT-inserted
RS232-T1100	○	HT-inserted
RS232-T1200	○	HT-inserted
RS232-T1300	○	HT-inserted
RS232-T1400	○	HT-inserted
RS232-T1500	○	HT-inserted
RS232-T1600	○	HT-inserted
s15850-T100	○	HT-inserted
s35932-T100	○	HT-inserted
s35932-T200	○	HT-inserted
s35932-T300	○	HT-inserted
s38417-T100	○	HT-inserted
s38417-T200	○	HT-inserted
s38417-T300	○	HT-inserted
s38584-T100	○	HT-inserted
s38584-T200	○	HT-inserted
s38584-T300	○	HT-inserted
vga_lcd-T100	○	HT-inserted
wb_conmax-T100	○	HT-inserted
b19	—	HT-free
EthernetMAC10GE	—	HT-free
RS232	—	HT-free
s15850	—	HT-free
s35932	—	HT-free
s38417	—	HT-free
s38584	—	HT-free
vga_lcd	—	HT-free
wb_conmax	—	HT-free

10

20

30

40

【 0 1 0 6 】

上記表 9 には、34 個のベンチマーク全てについて、既知情報によるハードウェアトロ

50

イの有無 (HT-free / HT-inserted) と一致する結果が得られたことが示されている。上述のような基準および条件を用いることによって、“HT-inserted” の 25 個のベンチマーク全てにおいて、誤検出無しでトロイネットの一部を確実に検出することができた。

【 0 1 0 7 】

既存手法を用いた場合には、“HT-inserted” の 25 個全てのベンチマークについて、ハードウェアトロイを正確に検出することはできない。検出に成功したハードウェアトロイの数は、下記表 10 に示すように、既存手法 1 では 4 個であり、既存手法 2 では 8 個にとどまっている。しかも、既存手法の場合には、ペイロード回路やトリガー回路などの回路におけるハードウェアトロイの情報を、事前に知る必要がある。ここで、既存方法 1 は UCI による手法であり、既存方法 2 は Veri Trust による方法である。UCI は、回路検証中に活性化しない信号を特定し、その信号に対してマルチプレクサを挿入することで、ハードウェアトロイを検出する。Veri Trust は、回路検証中に活性化しない信号を特定し、その信号に対して観測性を高めることによりハードウェアトロイを検出する。

【 0 1 0 8 】

【表 1 0】

ベンチマーク	本手法	既存手法1	既存手法2
b19-T100	○	×	×
b19-T200	○	×	×
EthernetMAC10GE-T700	○	×	×
EthernetMAC10GE-T710	○	×	×
EthernetMAC10GE-T720	○	×	×
EthernetMAC10GE-T730	○	×	×
RS232-T1000	○	×	×
RS232-T1100	○	×	×
RS232-T1200	○	×	×
RS232-T1300	○	×	×
RS232-T1400	○	×	×
RS232-T1500	○	×	×
RS232-T1600	○	×	×
s15850-T100	○	○	○
s35932-T100	○	×	○
s35932-T200	○	○	○
s35932-T300	○	×	○
s38417-T100	○	○	○
s38417-T200	○	×	○
s38417-T300	○	○	○
s38584-T100	○	×	×
s38584-T200	○	×	○
s38584-T300	○	×	×
vga_lcd-T100	○	×	×
wb_conmax-T100	○	×	×

10

20

30

【 0 1 0 9】

以上のように、ハードウェアトロイの挿入されていないネットリストや、ハードウェアトロイに関する情報を用いずに、公知のネットリストから得られた基準および条件を用いることによって、ゲートレベルの被検ネットリストが“HT-free”および“HT-inserted”のいずれであるかを識別することが可能となった。しかも、上述の基準および条件を用いた場合には、既存手法を用いた場合よりも正確な識別結果が得られており、こうした点でも既存手法に対して優位性を有することが確認された。

40

【 0 1 1 0】

3. 他の実施の形態

なお、本発明は、本実施の形態に限定されるものではなく、本発明の要旨の範囲内で種々の変形実施が可能である。例えば、上述の実施形態においては、公知ネットリストとし

50

て所定のサイト（Trust-HUB）からダウンロードした所定の10個のベンチマークを用い、こうした公知ネットリストから9個の対照ネットを選択することを一例として説明したが、公知ネットリストの数および対照ネットの数はこれに限定されない。公知ネットリストの数は任意に設定して、ランダムに選択することができる。また、対照ネットの数や種類は、公知ネットリストの数や種類によって、変わり得るものである。

【0111】

また、実施形態においては、対照ネットのスコアとして1または2を例に挙げたが、公知ネットリストの種類や数に変更された場合には、各対照ネットのスコアの大きさも変わり得る。

【0112】

さらに、実施形態においては、被検ネットリスト中のハードウェアトロイの有無の判定に用いる最大スコア閾値および最大スコアネット数閾値の値は、それぞれ3および5に設定したが、これらの数値もまた、変わり得るものである。最大スコア閾値および最大スコアネット数閾値は、上述の実施形態に示したように、公知ネットリストとの比較に基づいて適宜設定することができる。必要に応じて、公知ネットリストとの比較に基づいて得られた閾値よりも、厳しい閾値を設定してもよい。

【0113】

また、トロイネットを含むか否かを判断する指標の一つとして、最大一定クロック数（1Mクロック間で一定値を出力する最長のクロック数）を用いたが、これに限定されるものではない。被検ネットリスト中に潜むトロイネットの可能性を示すものであれば、最大一定サイクル数以外の任意のパラメータを用いてもよい。そのような場合においても、上述した実施形態で説明したように、公知ネットリストとの比較に基づいて適切な閾値を設定することができる。

【0114】

公知ネットリストからトロイネットの有無を判断するための基準を得、この基準に基づいてトロイネットの有無を判断するための条件を設定し、得られた基準および条件を用いてゲートレベルの被検ネットリスト中のトロイネットの有無を判断することによってハードウェアトロイを検出することは、本発明の範囲内である。

【0115】

情報処理装置10を検出装置20に直接接続して、情報処理装置10の被検ネットリストを入力する場合について説明したが、被検ネットリストを得ることができれば、情報処理装置10を検出装置20に接続する形態に限定されない。

【0116】

また、上記実施形態の場合、ネットリストは情報処理装置10に含まれている場合について説明したが本発明はこれに限られない。情報処理装置10は、必ずしもネットリストを保持している必要はない。この場合、検出装置20はネットリストを記憶した記憶媒体や、ネットワーク上のサーバーなどからネットリストを取得してもよい。

【符号の説明】

【0117】

- 10 情報処理装置
- 20 ハードウェアトロイ検出装置
- 22 制御バス
- 24 制御手段
- 26 条件設定手段
- 28 判断手段

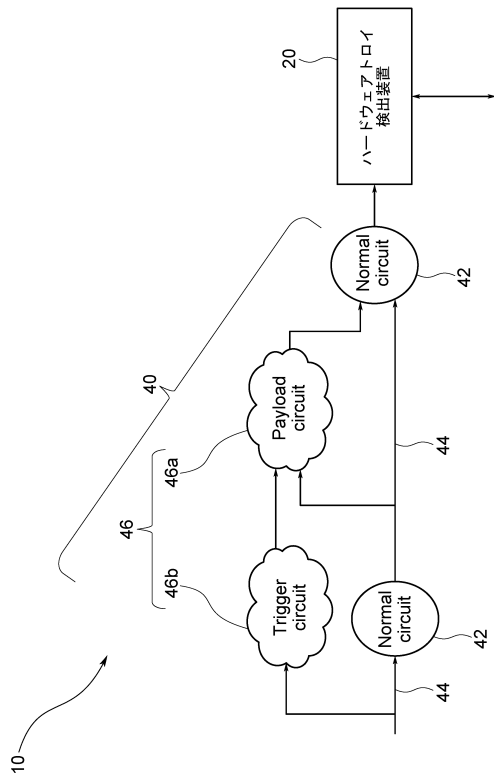
10

20

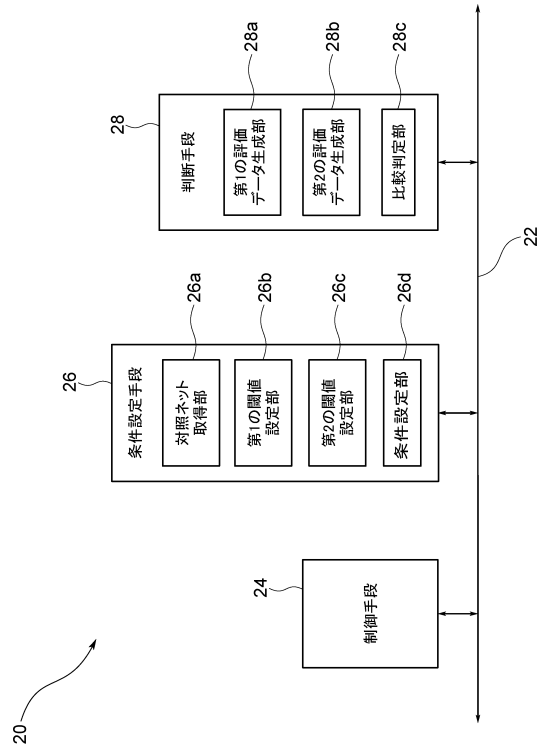
30

40

【 図 1 】

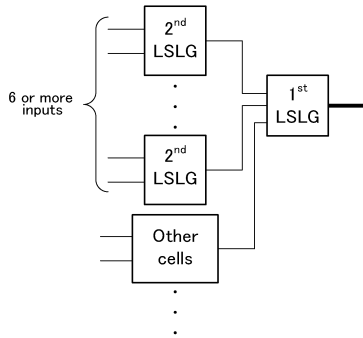


【 図 2 】



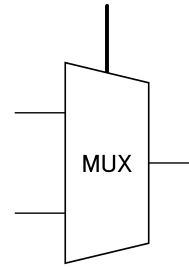
【 図 3 】

Case 1



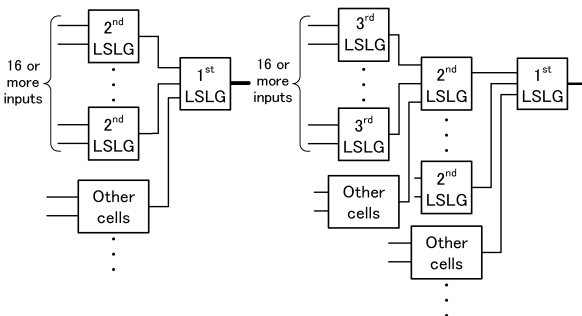
【 図 5 】

Case 3



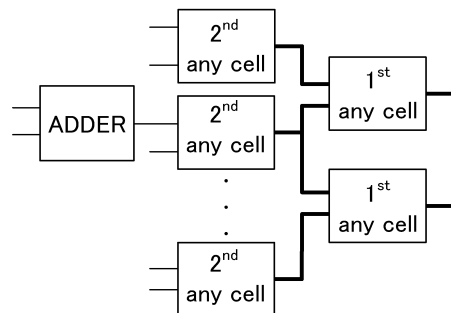
【 図 4 】

Case2



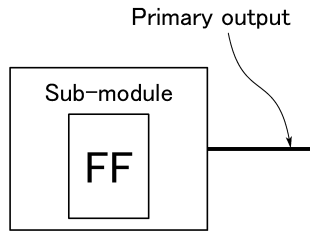
【 図 6 】

Case 4



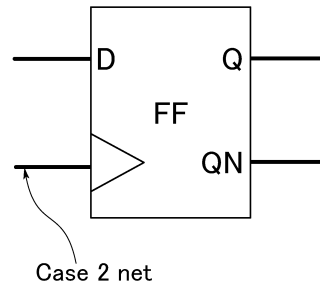
【 図 7 】

Case 5



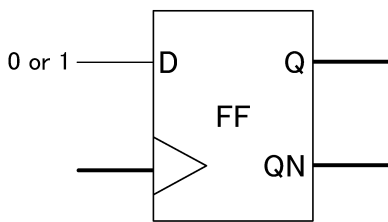
【 図 9 】

Case 7



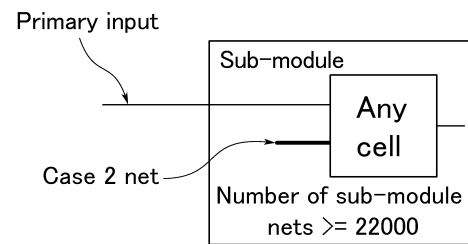
【 図 8 】

Case 6



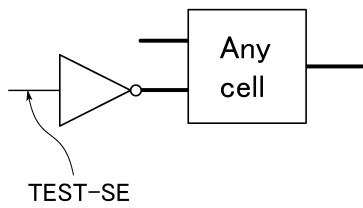
【 図 10 】

Case 8

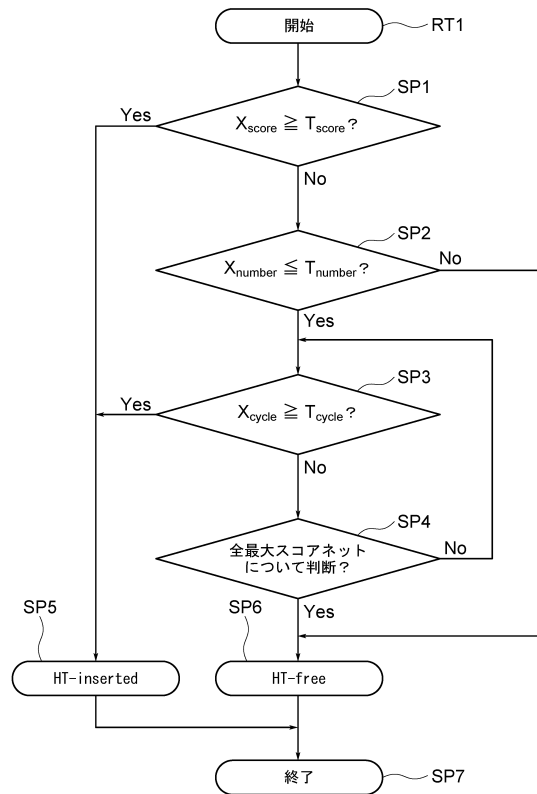


【 図 11 】

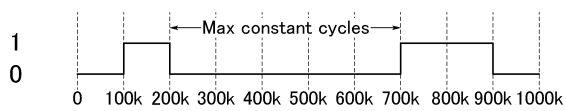
Case 9



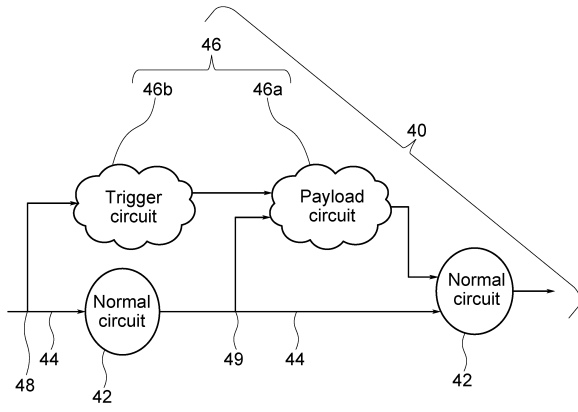
【 図 13 】



【 図 12 】



【 図 1 4 】



フロントページの続き

(72)発明者 大屋 優

日本国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

審査官 青木 重徳

(56)参考文献 中国特許出願公開第102662144(CN,A)

特開2012-207993(JP,A)

Mainak Banga, et al., Trusted RTL: Trojan Detection Methodology in Pre-Silicon Designs, IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 2010, 米国, IEEE, 2010年 6月13日, p.56-59

Yier Jin, et al., Experiences in Hardware Trojan Design and Implementation, IEEE International Workshop on Hardware-Oriented Security and Trust, 2009. HOST'09, 米国, IEEE, 2009年 7月27日, p.50-57

Jie Zhang, et al., VeriTrust: Verification for Hardware Trust, 2013 50th ACM/EDAC/IEEE Design Automation Conference (DAC), 米国, IEEE, 2013年 5月29日

Kan Xiao, et al., A Clock Sweeping Technique for Detecting Hardware Trojans Impacting Circuits Delay, IEEE Design & Test, 米国, IEEE, 2013年 3月 7日, Volume 30 Issue 2, p. 26-34

(58)調査した分野(Int.Cl., DB名)

G06F 21/56

JSTPlus/JMEDPlus/JST7580(JDreamIII)

IEEE Xplore