VLSI 設計工程時における未遷移信号線情報に基づいたトロイ回路検出法

坊屋舗知拓[†1]　細川利典[†2]　吉村正義[†3]

近年， VLSI の設計の一部を他の企業に委託するケースが増加し，VLSI の信頼性が低下している．VLSI の設計段階で，攻撃者によってトロイ回路が挿入される危険性がある．機能検証やテストでは，挿入されたトロイ回路を検出することが困難である．本論文では，受け入れ検証時の未遷移信号線と未設定値に基づくトロイ回路検出法を提案する．未遷移信号線の値を未設定値にするためのテスト生成を実行し，テスト生成できた信号線をトロイ回路の一部の信号線である可能性が高いマリシャスラインとして判定する．提案した方法を AES 暗号回路やベンチマーク回路に適用した結果，判定したマリシャスライン集合中にトロイ回路が含まれていたことを示す．

A Hardware Trojan Circuit Detection Method Based on Information of Non-transition Lines at VLSI Design Stages

TOMOHIRO BOUYASHIKI[†1]　TOSHINORI HOSOKAWA[†2]
MASAYOSHI YOSHIMURA[†3]

Recently, the increased utilization of outsourcing services for a part of designing VLSIs might reduce reliability of VLSIs. There is a risk that hardware Trojan circuits are inserted into VLSIs by attackers at design stages. It is difficult to detect Trojan circuits by functional verification and testing. In this paper, we propose a hardware Trojan circuit detection method based on a pair of non-transition lines and unset values generated as the results of acceptance verification. A test generation to set a non-transition line to an unset value is performed and lines with test sequences are identified as malicious lines which are suspected of Trojan circuits. The proposed method is applied to AES encryption circuit and benchmark circuits. Experimental results show that Trojan Circuits was included in the identified malicious line set.

1. はじめに

近年，超大規模集積回路(Very Large Scale Integrated circuits: VLSI)の設計および製造は，人件費や製造コストの削減のため，外部への業務委託が増加している[1]．自社で設計から製造まで行うよりも，上流の設計のみ自社で行い，下流の設計および製造はコストの安い外部企業に委託することによりVLSIの設計・製造コストの削減を図っている．しかしながら，業務委託を行うことによりVLSIの設計および製造に関与する組織や人物が増加し，業務の管理が困難となる．その結果として，VLSIの信頼性の低下が懸念される．

VLSIの信頼性に関する問題の一つとして，悪意あるエンジニア(攻撃者)によるVLSIの設計および製造への攻撃がある[1]．本論文において攻撃とは，VLSIにトロイ回路を挿入することと定義する．また攻撃者とは，VLSIに対して悪意ある回路を組込む者，あるいはトロイ回路によって得られた情報を悪用する者と定義する．外部へ業務委託するケースの増加，および委託先企業の多様化に伴い，委託先企業におけるVLSIに対する攻撃は容易になっている[1].

†1 日本大学大学院 生産工学研究科
Graduate School of Industrial Technology, Nihon University
†2 日本大学 生産工学部
College of Industrial Technology, Nihon University
†3 京都産業大学コンピュータ理工学部
College of Faculty of Computer Science and Engineering, Kyoto Sangyo University

トロイ回路が組み込まれたVLSIは，正常な機能の無効化，機密情報の漏洩や改ざん，回路破壊などの脅威にさらされる[1][2]．トロイ回路の特徴として以下の3点が挙げられる．

- トロイ回路挿入の前後において，元の回路の物理的な外観は損なわれない．
- 設計されたVLSIの入出力動作は，トロイ回路が路挿入された場合においても，正規の設計仕様を満たす．
- トロイ回路が起動するのは，限られた条件下(トリガー条件の充足)のみである．トリガー条件としてはVLSIの設計仕様上，使用されていない入力系列が利用されるケースが多い．

以上より，一般的なVLSIの機能検証やテストでは，トロイ回路の検出が困難である[1][2].

大量生産されたVLSIのうち，数個を分解・解析(リバースエンジニアリング)し，仕様書と比較することでトロイ回路を検出することは可能である[1][2]．しかしながら，リバースエンジニアリングは分析コストが非常に高価である上に，その手法の性質上，一度分析を実行した回路は製品として使用不可能となる．仮に分析対象としたVLSIにトロイ回路の混入がなかったとしても，分析を行わなかった他のVLSIが正常回路であるという保証にはならない[3].

現在報告されているトロイ回路による被害例として，2012 年にアメリカの半導体メーカーである Actel / Microsemi が販売している FPGA(Field-Programmable Gate Array)内に，暗号化に使用する共通鍵を外部へ流出するトロイ回路が組み込まれていた[4]．また同年に，米上院軍事委員会が発表したレポートでは，約100万個もの疑わしい回

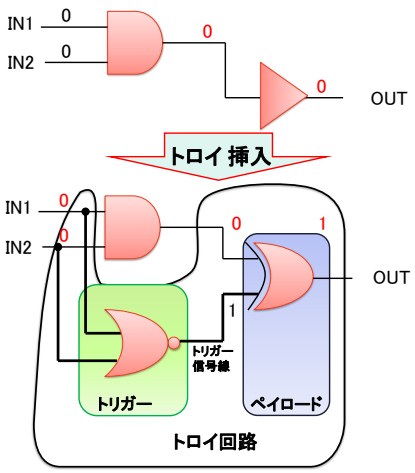

図1. トロイ回路例

路が軍用機から発見されたことを公表している[5]. 他にも2008年のIEEE Spectrum[6]によると, シリア防空システムにもトロイ回路が挿入された疑いがあることが報告されている. 以上の事例より, 近年ではトロイ回路攻撃の脅威が顕在化してきていると言える. したがって, 今後トロイ回路攻撃に対する対策の必要性が高まると予想される.

現在ではVLSIに挿入されたトロイ回路を検出するために, 様々な研究が行われている[2]. 現在提案されているトロイ回路検出法の多くは, 製造段階や物理レベルの設計時を想定した手法である. しかしながら, 近年の委託先企業の多様化に伴い, 物理設計におけるトロイ回路検出法だけでなく, 上流の設計におけるトロイ回路検出法の需要が高まっている[7]. このことより本論文では, VLSI製造フローのテスト容易化設計, 論理設計, 物理設計を外部へ委託した際に挿入されたトロイ回路を検出する手法を提案する.

本論文の構成は, 第2章において, 一般的なトロイ回路の概要について述べる. 第3章では信号未遷移情報を用いたトロイ回路検出法について述べる. 第4章では提案手法を用いたトロイ回路検出の実験結果を述べる. 第5章で本論文のまとめと今後の課題について述べる.

2. トロイ回路

2.1 トロイ回路概要

トロイ回路とは, VLSIの設計および製造段階において, 攻撃者により挿入される悪意ある回路である. 図1にトロイ回路の例を示す. トロイ回路は一般に, 起動条件の判定を行うトリガー部と攻撃を行うペイロード部から構成される[8].

2.2 トリガー部

トリガー部は攻撃者が設定したトロイ回路の起動条件を満たすか否かを判定する回路である. トリガー部では, 起動条件を満たした場合にペイロード部に対し, トリガー信号を送信する. トリガー部には, 記憶素子(Flip Flop: FF)を含んでいない組合せ回路トリガーと FF を組込むことで特定の入力系列が入力された場合のみトリガー信号を送信する順序回路トリガーの 2 種類が存在する[10]. 図 1 では, トロイ回路内の NOR ゲートがトリガー部に該当し, IN1=0, IN2=0 がトリガー条件となる. なお, 図 1 のトリガー部は回路内に FF が存在しないため, 組合せ回路トリガー部に分類される.

2.3 ペイロード部

ペイロード部ではトリガー部よりトリガー信号を受信した場合に, 攻撃対象回路に対し攻撃を行う回路である. 攻撃とは, 攻撃者が設定したトロイ回路機能を実行することである. トロイ回路による攻撃はトロイ回路を設計する際に攻撃者が任意に決定することができる. 図 1 では, トロイ回路内の XOR ゲートがペイロード部に該当し, トリガー信号が入力された場合出力を反転させる攻撃を行う.

2.4 トロイ回路検出困難性

トロイ回路の検出は大きく 2 種類に分類することができる. 一つは製造工程時におけるトロイ回路の検出法である. 製造工程におけるトロイ回路検出法では, トロイ回路の挿入による物理的な特徴(消費電力や面積など)を観測することにより検出する手法[1]である. 二つ目は, 設計工程時におけるトロイ回路の検出法である. 設計工程時におけるトロイ回路検出法では, 回路構造などを解析することでトロイ回路の検出を行う[8].

現在 VLSI の設計および製造工程において, トロイ回路を考慮した検証は行われていない. それゆえに, 通常の機能検証およびテスト工程時においてトロイ回路の検出を行っている. しかしながら, トロイ回路は一般的に機能検証中やテスト中に使用されない入力系列をトリガー条件として設定される. したがって, トロイ回路が挿入された VLSI に対して機能検証およびテストを実行しても, トロイ回路は不活性化状態を維持する. このため, 設計工程時にトロイ回路による影響を観測することは困難である. また, 多くのトロイ回路は VLSI 全体の面積に対して, 物理的に微小なサイズで設計される. このため, トロイ回路の挿入による物理的な影響は微小なものとなる. 以上の理由よりトロイ回路を製造時および設計時に検出することは困難である.

2.5 従来手法

現在提案されているトロイ回路検出手法として, VLSI の物理的な特徴に着目したサイドチャネルベースのトロイ回路検出手法[1]と, VLSI の論理に着目したトロイ回路検出手法[8]がある.

前者の手法の 1 つとして, 電力解析を用いた手法[1]や論理合成技術を用いたトロイ回路検出法[8]がある. Agrawal らは, 回路を動作させた際に発生する消費電力に着目し, 回路内にトロイ回路が挿入されたか否かを判定するための

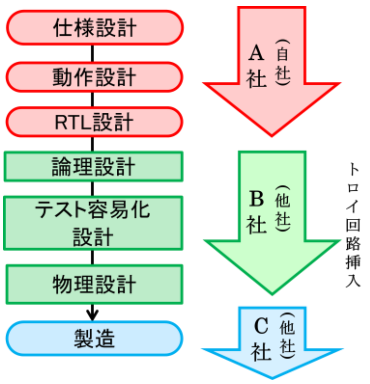

図 2. VLSI 製造フロー

指標とした[1]．トロイ回路が動作すると，通常の回路とは異なる消費電力量となる．しかしながら，トロイ回路による消費電力量の増加に伴う影響度は，元の回路面積に対してトロイ回路が占める割合が小さいほど，微小なものとなる．また消費電力を指標とする場合，回路自体の特性ばらつきや，回路動作時の微小なノイズも問題となる．Agrawal らは，これらの問題を主成分分析(PCA:principal component analysis)を用いることで改善した[1].

Zhang らは設計工程時に，回路内のトロイ回路の疑いがある部分に対して，商用論理合成ツールを用いた再論理合成を実行することで，トロイ回路の検出および無効化を行う"VeriTrust"法を提案している[8].

大屋らは，回路内のスイッチング確率を計算することでトロイ回路の検出を行う手法を提案している[11].

本提案手法では，既存の手法[1]のような製造後のVLSIに対するトロイ回路検出法ではなく，文献[8]同様に設計工程におけるトロイ回路検出法である．文献[8]ではトロイ回路の疑いのあるコーンを取り除くような再論理合成を行うことで，トロイ回路を検出するのに対し，本提案手法ではATPG(Automatic Test Pattern Generator)ツールを用いて，トロイ回路を活性化させるテスト系列を生成し，生成されたテスト系列を用いてトロイ回路の解析を行う．

3. 信号未遷移情報を用いたトロイ回路検出法

一般的にトロイ回路は，自身の存在を隠蔽するために，設計仕様上使用されていない入力系列をトリガー条件に利用する．なぜなら，設計仕様上で使用されている入力系列をトリガー条件とした場合，機能検証中にトロイ回路が起動し，トロイ回路を容易に検出することができるため，攻撃者はこれを回避するように設計する．したがって，機能検証及び，テスト時に一度も論理値が変化しない信号線は，トロイ回路の一部(トリガー信号線)である疑いがある[8].

本提案手法は，トリガー信号線の論理値を反転させることにより，トロイ回路を無理やり起動させることでトロイ回路の検出を実現する．図3に示すようにトリガー信号線の論理値が反転するような入力系列TPを生成し，得られたTPを入力する．トロイ回路が挿入されていた場合，通常時と異なる出力応答が観測されることが予想される．したがって，外部出力系列またはFF値が異なる場合は，VLSIに対してトロイ回路が挿入されたと判定する．なお， 未遷移信号線に対しトロイ回路と考えられる信号線数を絞り込むために，固定値を反転させた影響が外部出力またはFFへ伝搬することが可能な未遷移信号線のみをトリガー信号線の候補とする．

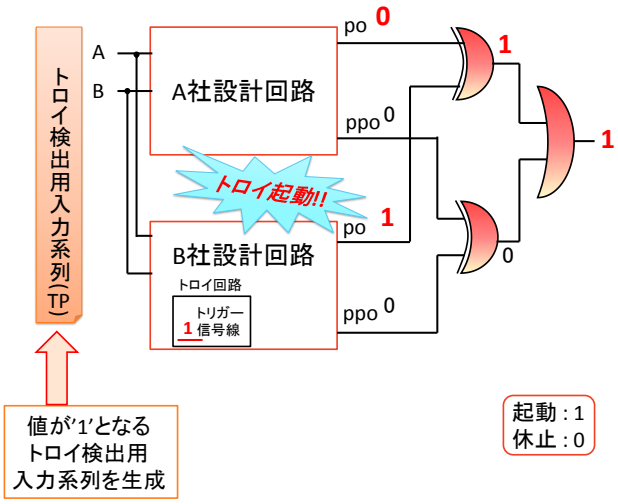

図3.提案手法基本概念

3.1 前提条件

提案手法は，業務委託時に挿入されたトロイ回路を検出することを目的としている．

本論文で取り扱うトロイ回路は，図 2 に示す仕様設計から RTL(Register Transfer Level)設計までを A 社で行い，論理設計から物理設計までを専門企業 B 社に業務委託する．その後 B 社が物理設計した回路データをファウンドリ C 社に渡し，製造を委託する．なお本論文では，B 社が委託業務を行う過程で A 社が設計した回路部に対してトロイ回路攻撃を仕掛けることを仮定している．A 社では B 社より受け取った回路データに対し，機能検証用入力系列とテスト用入力系列を用いて受け入れ検証を実行する．この際にトロイ回路は起動しないものとする．

本手法では，業務委託時に挿入されたトロイ回路のうち，A 社が設計した機能に対して攻撃を行うトロイ回路を検出対象とする(例: A 社回路内の機密情報の流出，A 社設計機能の停止など)．A 社では，自社で設計した機能の出力期待値を計算することができるものとする．

3.2 マリシャスライン

機能検証用入力系列及びテスト用入力系列に対する受け入れ検証時において，信号値v($v\in\{0,1\}$)の遷移回数が一定値以下である信号線を未遷移信号線と定義する．未遷移信号線の集合をSとする．

S の信号線 l ($l\in S$)に¬v の信号値を設定し，その影響を任意の FF もしくは外部出力へ伝搬可能な入力系列が生成できる時，信号線 l をマリシャスラインと定義する．マリシャスラインはトロイ回路の疑いがある信号線である．マリシャスラインに対する入力系列はトロイ回路検出用の入力系列である．

表 1. 未遷移信号線数(AES 暗号回路[9])

	機能検証用入力系列(Vin)	テスト用入力系列(Tin)	受け入れ検証全体
全信号線数	41,963	41,963	41,963
遷移信号線数	35,784	41,928	41,946
未遷移信号線数 L	6,179	35	17
未遷移信号線割合	14.72%	0.08%	0.04%
実行時間(秒)	4838	185	5023

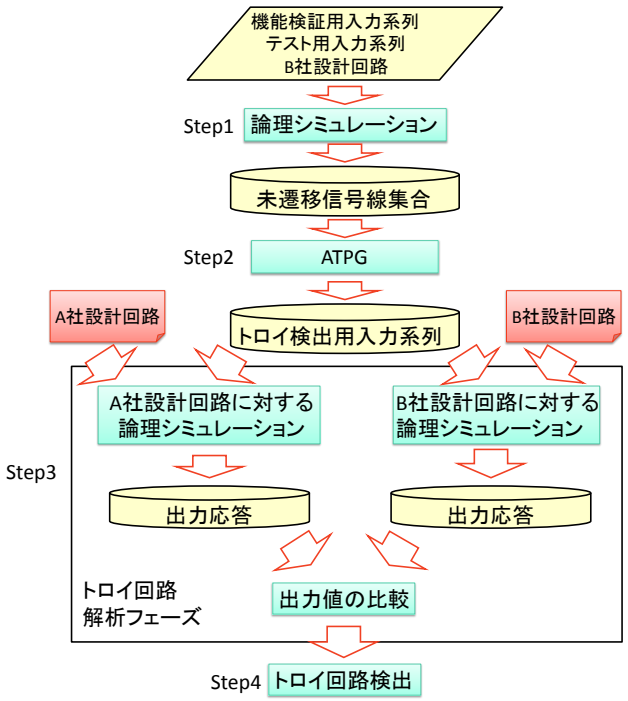

図4. 提案手法フロー

3.3 トロイ回路検出法

図4に受け入れ検証における提案するトロイ回路検出法の全体フローを記す.

(Step1)
B社が設計した論理回路に対し，機能検証用入力系列とテスト用入力系列を用いて論理シミュレーションを実行し未遷移信号線集合を生成する.

(Step2)
Step2では，Step1で生成した未遷移信号線集合に含まれる各未遷移信号線に対し，固定値と反対の論理値を未遷移信号線に設定し，その影響を外部出力またはFFに伝搬させるためのテスト系列を生成する．このテスト系列生成処理は，未遷移信号線*l*(固定値v)のv縮退故障のATPGと同じである．ATPGに成功した未遷移信号線をマリシャスラインとし，トロイ回路検出用入力系列を得る.

(Step3)
Step2で生成したトロイ回路検出用入力系列を用いてマリシャスライン*l*がトロイ回路の一部であるか否かを解析する．なお，本ステップにおける解析手段は実行者に一任するものとする．本論文では，Step2で生成されたトロイ回路検出用入力系列をA社が設計した回路に対して入力し，得られた出力応答PO1とB社が設計した回路に対して入力し，得られた出力応答PO2を比較することで，マリシャスライン*l*がトロイ回路の一部であるか解析する．マリシャスライン*l*がトリガー信号線であった場合，B社が設計した回路内のトロイ回路が起動するために，出力応答PO1とPO2が異なる値となる.

(Step4)
Step4 の結果，値が一致しない場合において，そのマリシャスラインをトロイ回路と判定する．値が一致した場合において，そのマリシャスラインはトロイ回路ではないと判定する.

4. 実験結果

本章では提案手法を用いたトロイ回路検出の実験結果を示す．本実験で使用するトロイ回路は，文献[9]で提案されているAES暗号回路に対して機密情報を外部出力へ流出するトロイ回路とWebサイト”trust-HUB”で配布されているベンチマークトロイ回路[12]を使用する．なお本実験で使用したマシンスペックは，CPUがIntel Core i7-4790，メモリは8GBのものを使用している

4.1 AES 暗号回路の実験結果

図5に文献[9]のトロイ回路の概要図を示す．図5に示す回路では，機能検証時および，テストモード時にトロイ回路は起動されないように設計されている．トロイ回路の起動条件は，特定の状態で特定の値を外部入力より印加した時のみ，トリガー部よりトリガー信号として論理値'1'がペイロード部へ送信されトロイ回路が起動する．トロイ回路が起動された場合，ペイロード部より連続する2つの暗号化途中データを外部へ流出する．攻撃者は得られた2つの暗号化途中データを利用して，共通鍵の逆算を行う.

表 1 に AES 暗号回路[9]に対する未遷移信号線集合の評価結果を示す．本実験では，機能検証用入力系列として，

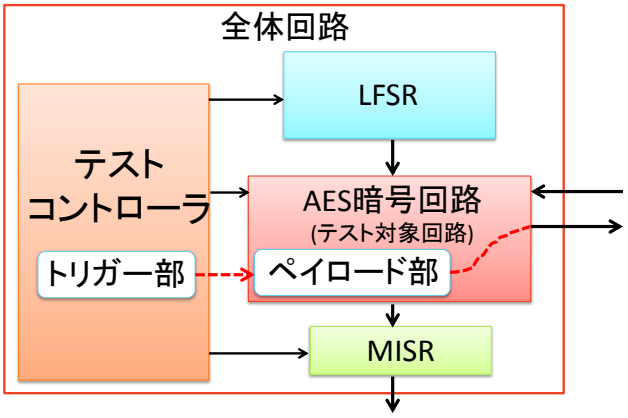

図5. 実験回路概要図(BIST設計後AES暗号回路)

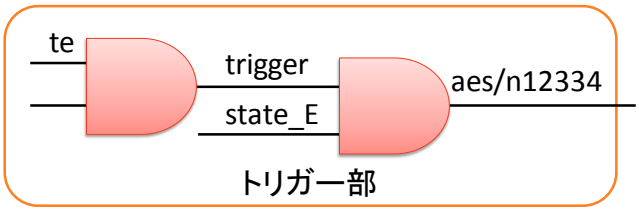

図6. トロイ判定信号線(BIST)

表 2. マリシャスライン数(文献[9])

全未遷移信号線数	マリシャスライン数	実験時間(秒)
17	10	9629

表 3. トロイ判定信号線(文献[9])

マリシャスライン数	トロイ判定信号線数	実行時間(秒)
10	2	5

表 4. ベンチマーク回路実験結果

回路名	全体信号線数	非遷移信号線	実行時間(s)	非遷移信号線の割合	マリシャスライン数	実行時間(s)	トロイ判定信号線数	実行時間(s)
s35932_T100	20481	23	162	0.11%	19	921	1	2
s35932_T200	20477	17	187	0.08%	17	596	3	2
s35932_T300	20506	22	222	0.11%	**0**	**1154**	**0**	**2**
s38417_T100	20628	55	212	0.27%	54	1063	13	7
s38417_T200	20633	63	213	0.31%	62	1150	18	9
s38417_T300	20665	91	212	0.44%	**0**	**1933**	**0**	**2**
s38584_T200	51395	2870	142	4.50%	1462	18530	320	26
b15_T100	29452	1404	6	4.77%	63	2744	58	1
b15_T200	29452	1401	5	4.77%	65	2758	64	1

表 5. ベンチマーク回路(変更)実験結果

回路名	全体信号線数	非遷移信号線	実行時間(s)	非遷移信号線の割合	マリシャスライン数	実行時間(s)	トロイ判定信号線数	実行時間(s)
s35932_T300_B	20509	23	253	0.11%	23	725	6	1
s38417_T300_B	20667	92	212	0.45%	36	1683	36	1

50,000 通りの共通鍵と平文の組み合わせを検証する入力系列 Vin とテストモードを起動するテスト用入力系列 Tin の 2 種類の系列を用いた．実験結果より機能検証用入力系列を使用した場合は，回路全体の信号線数 41,963 本のうち，14.72%の 6,179 本の信号線が未遷移信号線と判定された．テスト用の入力系列を使用した場合，全信号線のうち，約 0.08%の 35 本の信号線が未遷移信号線と判定された．これら 2 つの入力系列を用いてシミュレーションを実行した結果，未遷移信号線集合と判定された信号線は全信号線の約 0.04%の 17 本となった．

機能検証用入力系列と比較して，未遷移信号線数はテスト用入力系列を用いた方が，少ないことが実験結果よりわかる．この理由の一因として，機能検証用入力系列を用いた場合，AES 暗号回路部に含まれる信号線のみ遷移が発生するのに対し，テスト用入力系列を用いた場合，テストコントローラ部，テストパターン生成器部，応答圧縮器部に含まれる信号線も遷移したためであると推測される．

表2にAES暗号回路[9]に対するトロイ検出用入力系列の評価結果を示す．本実験では，トロイ検出用入力系列生成にATPGアルゴリズムを使用した．ATPGにおけるバックトラックリミットは，最大展開時間数25で実行し，トロイ回路検出用入力系列を生成した．実験結果より，全未遷移信号線のうち10本の信号線がトロイ検出用入力系列生成に成功した．よって，この10本の信号線をマリシャスラインと判定する．

表 3 に AES 暗号回路[9]に対するトロイ回路判定結果を示す．本実験では，テスト容易化設計後の回路とテスト容易化設計前の回路に対して，生成されたマリシャスラインに対する入力系列を与え，得られた出力応答を比較することでトロイ回路の判定を行っている．実験結果より，10 本のマリシャスラインのうち，2 本のマリシャスラインがトロイ回路と判定された．本実験でトロイ回路と判定された 2 本の信号線は図 6 に示す信号線"trigger"と信号線"aes/n12334"である．信号線"trigger"は外部入力より，特定の値を印加した時のみ値が'1'となる．信号線"aes/n12334"は，特定の状態(state_E = 1)で特定の値を外部より印加(trigger = 1)した時に値が'1'となる．なお両信号線は図 5 に示すトリガー部の信号線である．信号線"aes/n12334"の出力はペイロード部に接続されており，本信号線がトリガー信号線の役割を果たしていた．また，本信号線は，シミュレーション中は値が'0'で固定されており，トロイ回路が起動する際には論理値が'1'となった．

4.2 ベンチマーク回路実験結果

trust-HUB で配布されているトロイ回路に対して本提案手法を用いた実験結果を示す．なお trust-HUB で配布されているトロイ回路に対する A 社設計回路に相当する回路を入手することができなかったため，提案手法の一部を変更している．トロイ回路の特徴の 1 つに，異なるベンダが提供している IP(Intellectual Property)コアにトロイ回路が挿入されていた場合，それらのトロイ回路のトリガー条件が一

致する可能性は極めて稀である[10]ことが一般に知られている．このため本実験では，図 4 の Step3 においてテスト容易化設計前回路に代わって，異なるベンダが提供する IP コアを使用する．

表 4 に trust-HUB で配布されている **9** 個のベンチマーク回路に対する実験結果を示す．本実験では，各ベンチマーク回路に対する機能検証用入力系列として，s35932 系回路には 77 系列のランダムパターン, s38417 系回路には 50,000 系列のランダムパターンを使用した．実験結果より s35932_T300 と s38417_T300 以外の全てのベンチマーク回路に対して本提案手法を用いたトロイ回路検出に成功した．トロイ検出に成功したベンチマーク回路は，全てトリガー条件を満たした場合，外部出力および疑似外部出力の値を変化させるのに対し，トロイ検出に失敗した s35932_T300 と s38417_T300 は，トリガー条件を満たした場合リングオシレータが起動する構造となっていた．その結果，図 4 の Step3 において出力応答を比較しても，トロイ回路の影響を観測することができなかったと考えられる．表 5 にトロイ回路の検出に失敗した s35932_T300 と s38417_T300 に対してマルチプレクサを挿入し，リングオシレータの値を外部へ出力する仕様に変更した回路，s35932_T300_B と s38417_T300_B に対する実験結果を示す．実験結果より両回路のトロイ検出に成功した．このことより，提案手法では外部出力および疑似外部出力を変更しない物理的な攻撃(遅延攻撃，IR ドロップ)を行うトロイ回路の検出が不可能であり，論理的な攻撃を行うペイロード部を実装したトロイ回路のみを検出することができると言える．また実験結果より，最も実行時間が長い回路においても，最大で約 5 時間と現実的な時間でトロイ回路の検出に成功した．

5. おわりに

本論文では，信号未遷移情報を用いたトロイ回路検出法を提案した．実験結果より文献 [9]で提案されたAES暗号回路に挿入したトロイ回路の検出に成功した．また"trust-HUB"で配布されているベンチマーク回路に対し，提案手法を用いた結果，トロイ回路検出の成否は，ペイロード部の機能に依存することが判明した．トロイ回路検出に失敗した理由としては，トロイ検出用入力系列に対して外部出力および疑似外部出力の値のみを比較することでトロイ検出を実行することによると予想される．したがって，図4のStep3(トロイ回路解析フェーズ)時に出力応答値を比較するだけでなく，微小遅延が発生するか，消費電力が以上に上昇するかなどの解析を行うことで，物理的な攻撃を行うトロイ回路の検出も可能となることが予想される．よって今後の課題は，トロイ回路検出条件を改良することで，論理的な攻撃を行うトロイ回路だけでなく，物理的な攻撃を行うトロイ回路の検出も可能にすることが挙げられる．

また，今後はトロイ回路の検出だけでなく，トロイ回路の検出が容易に行えるVLSIの設計手法の考案なども行っていく予定である．

謝辞　本研究は一部，日本学術振興会科学技術研究補助金基盤(C)(課題番号 26330071,15K06086)の研究助成による．

参考文献

1) Dakshi Agrawal, Selcuk Baktır, Deniz Karakoyunlu, Pankaj Rohatgi and Berk Sunar, "Trojan Detection using IC Fingerprinting, " 2007 IEEE Symposium on Security and Privacy, pp.296-310, 2007.

2) 木村雅秀, Phil Keys，内田泰, "その電子部品，ホンモノですか？," 日経エレクトロニクス, pp.29-50, April 2010.

3) S. Skorobogatov and C. Woods, "Breakthrough silicon scanning discovers backdoor in military chip," In Proc, International conference on Cryptographic Hardware and Embedded Systems, pp.23-40, 2012.

4) Inquiry into counterfeit electronic parts in the department of defense supply chain, "Committee Armed Services," United States Senate, May 2012. http://www.levin.senate.gov/download/?id=24b3f08d-02a3-42d0-bc75-5f673f3a8c93.

5) S. Adee, "the hunt for the kill switch," IEEE Spectrum, vol.45, no.5, pp.34-39, May 2008.

6) Mainak Banga and Michael S. Hsiao, "Trusted RTL: Trojan detection methodology in pre-silicon designs,", Hardware-Oriented Security and Trust(HOST), 2010 IEEE International Symposium, pp. 56-59.

7) Yier Jin, Nathan Kupp and Yiorgos Makris, "Experi-ences in Hard-ware Trojan Design and Implementation," 2009 IEEE International Workshop on Hard-ware-Oriented Security and Trust, pp.50-57 2009.

8) Jie Zhang, Feng Yuan, Lingxiao Wei, Zelong Sun, and Qiang Xu, "VeriTrust: verification for hardware trust. ", Proceedings of the 50th Annual Design Automation Conference, ACM, 2013. No.61.

9) M. Yoshimura, A. Ogita, and T. Hosokawa, “A smart Trojan circuit and smart attack method in AES encryption circuits”, IEEE International Symposium on Defect and Fault Tolerance in VLIS and Nanotechnology Systems, pp.278 – 283, 2013.

10) Cui, Xiaotong, et al. "High-Level Synthesis for Run-Time Hardware Trojan Detection and Recovery," Proceedings of The 51st Annual Design Automation Conference on Design Automation Conference. ACM, pp.1 - 6, 2014.

11) OYA, Masaru, et al. “A score-based classification method for identifying hardware-trojans at gate-level netlists.” In: Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition. EDA Consortium, 2015. p. 465-470.

12) Trust-Hub Website. https://www.trust-hub.org/tags/benchmark