ISSN 2186-5647

2-58

信号未遷移情報に基づくトロイ検出法

日大生産工(院)　○坊屋舗 知拓　　日大生産工　細川 利典
京産大　吉村 正義

1 はじめに

近年，超大規模集積回路(Very Large Scale Integrated circuits: VLSI)の製造および設計は，人件費や製造コストの削減のため，外部に業務委託することが多くなってきている[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外注することにより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の製造および設計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者とは，VLSIに対して悪意ある回路を組込む者，あるいは攻撃によって得られた情報を悪用する者と定義する．業務委託の増加，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]．

VLSIの設計，製造過程における攻撃の一例として，トロイ回路の挿入が考えられる[1]．トロイ回路が組込まれた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]．トロイ回路の特徴には以下の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，トロイ回路挿入があった場合においても，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]．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]．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が正常回路である保証にはならない[2]．

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[3]．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路が軍用機から発見されたことを公表している[4]．他にも2008年のIEEE Spectrum[5]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，対策の需要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[1]．しかしながら，現在提案されているトロイ回路検出手法の多くは，製造段階や物理レベルの設計時に対するものである．しかしながら，近年の委託先企業の多様化に伴い，下流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手法の需要が高まっている[6]．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

Hardware Trojan Detection Method
A Based on Information of Nontransitional Lines.
Tomohiro BOUYASHIKI, Toshinori HOSOKAWA, and Masayoshi YOSHIMURA

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．

2　トロイ回路

2.1 トロイ回路概要

トロ回路とは，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[7]．

2.2 トリガー部

トリガー部で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．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，ctrl=0，INT=0がトリガー条件となる．

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．

3　信号未遷移情報を用いたトロイ検出法

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パターンを利用する．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，トロイ回路の一部である疑いがある[8]．
提案手法では，信号未遷移情報を利用してトロイ回路の検出および挿入箇所の特定を行う．

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．本手法では，テスト容易化設計時に挿入されたトロイ回路のうち，委託元企業(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．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．

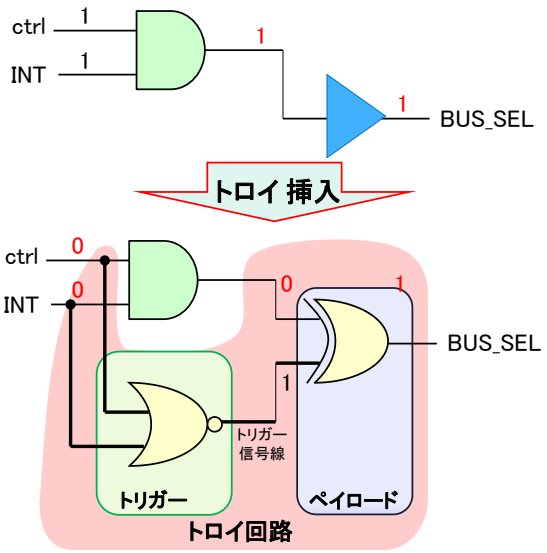

図 1. トロイ回路例

3.2 定義(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動作において，信号値が常にV(V∈{0,1})である未遷移信号線の集合をSとする．
Sの信号線l (l∈S)に$\bar{V}$の信号値を設定し，正当化する入力系列が生成できる時，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．

3.3 トロイ判定法

図2に提案するトロイ判定法の全体フローを記す．

(Step1)
テスト容易化設計後の論理回路に対し，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)
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固定値信号線に設定し正当化を行う．正当化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RTL回路に入力し，出力期待値を計算する．

(Step4)
Step2で生成したトロイ回路検出用入力系列をテスト容易化設計後の論理回路に入力し，出力応答を計算する．

(Step5)
Step3で計算した出力期待値とStep4で計算した出力応答を比較する．

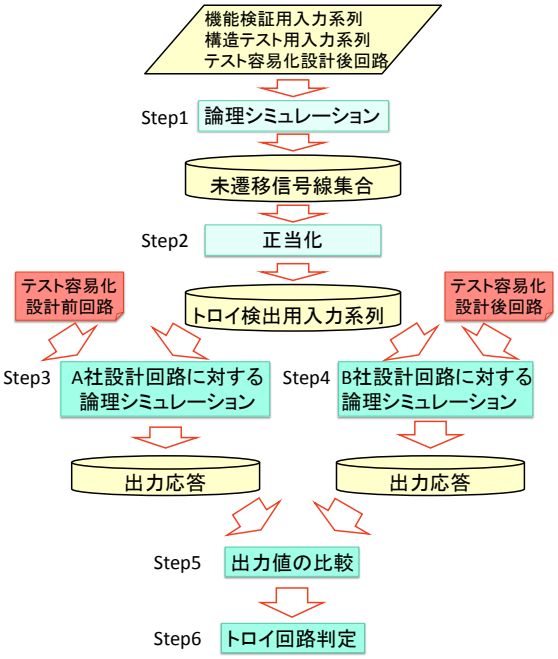

図 2. 提案手法フロー

(Step6)

Step5の結果，値が一致しない場合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を使用する．図3に実験に使用したトロイ回路の概要図を示す．図3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しない．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．

表1に図2におけるStep1の実験結果を示す．本実験では，機能検証用入力系列として，共通鍵Aと平文Bを入力し暗号文Zを出力させる入力系列，テスト用入力系列として共通鍵Cと平文Dを入力しテストモードを起動する入力系列をそれぞれ1つずつ用意した．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，44.76%の18,784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1.04%の437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0.76%の18本となった．

機能検証用入力系列を使用した場合と比べてテスト用入力系列を使用した場合の方が未遷移信号線数が少ない理由の1つとしては，入力系列長に起因していると考えられる．本実験で使用した機能検証用入力系列長は15サイクルに対し，テスト用入力系列長は350,026サイクルである．このため単純にテスト用の入力系列の方が多くの信号線を遷移させる能力を有していたと推測される．

表2に図2におけるStep2の実験結果を示す．本実験では，正当化には決定論的アルゴリズムに基づく後方追跡を使用した．後方追跡はバックトラック数の上限を1,000回，最大展開時刻数50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本の信号線が正当化に成功した．よって，この正当化に成功した10本の信号線をマリシャスラインと判定する．

表3に図2におけるStep5の実験結果を示す．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4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3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，シミュレーション中は共に値が'0'で固定されていた．本来ならば，信号線"aes/n12334"のみが検出可能であるが，信号線"trigger"の正当化時に偶発的に信号線"state_E"の値が'1'になったため，トリガー部の一部である信号線"trigger"も検出することができたと考えられる．

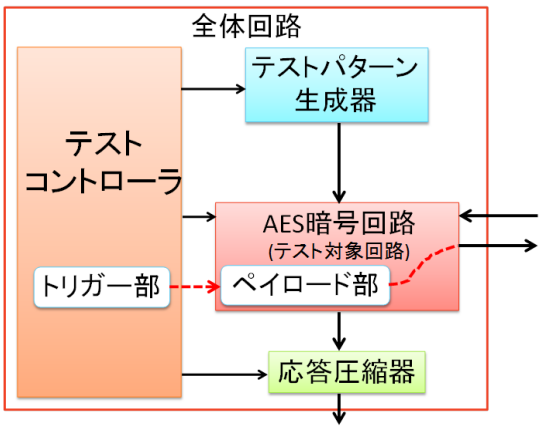

図 3. 実験回路概要図(BIST 設計 AES 回路)

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手法を提案した．実験結果より文献[9]で提案されたトロイ回路の検出に成功した．今後の課題として，様々なタイプのトロイ回路に対しても本手法が有効であるか否か評価する必要がある．

「参考文献」

[1] Dakshi Agrawal, Selcuk Baktır, Deniz Karakoyunlu, Pankaj Rohatgi and Berk Sunar, "Trojan Detection us-ing 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 Cyptographic 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. p.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.

表 1. 固定値信号線数

	機能検証用入力系列 (V_{in})	構造テスト用入力系列 (T_{in})	積集合 ($V_{in} \cap T_{in}$)
全信号線数	41, 963	41, 963	41, 963
遷移信号線数	23, 179	41, 526	41, 945
未遷移信号線数	18, 784	437	18
未遷移信号線割合	44. 76%	1. 04%	0. 76%

表 2. マリシャスライン数

全未遷移信号線数	マリシャスライン数
18	10

表 3. トロイ判定信号線

マリシャスライン数	トロイ判定信号線数
10	2

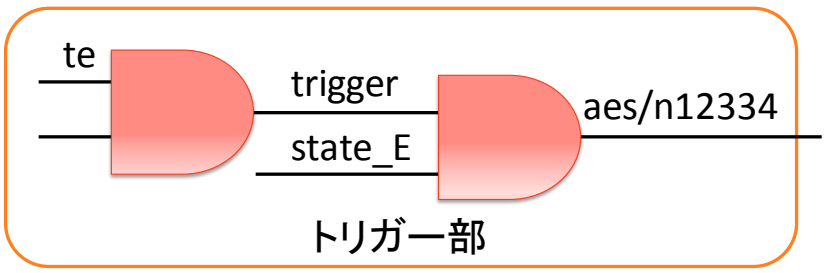

図 4. トロイ判定信号線