ISSN 2186-5647



2-31

# トロイトレラント向けIP回路設計

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，半導体集積技術の発展に伴い，設計される超大規模集積回路(Very Large Scale Integrated circuits: VLSI)は大規模・高集積化の一途をたどっている．これに伴いVLSI設計に必要な時間的資源および人的資源も増加の一途をたどっており，問題視されている．それゆえ，回路内を機能ブロック単位で再利用可能な形にまとめ，他の製品でも再利用可能にする設計法(Intellectual Property Core:IPコア)が用いられるようになった．IPコアを用いた設計を行うことで過去に設計した既存開発製品を再利用するだけでなく，自社製品をIPコア単位で他社に提供することが可能になる．さらに外部企業が提供しているIPコアを購入し，自社回路に組み込むことでVLSIの開発期間および人的資源を削減することが可能となる．しかしながら，購入したIPコアを自社設計回路に組み込む行為はVLSIの設計に関与する組織や人物が増加するため，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み込む者，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．近年では，IPコアを提供するIPコアベンダーの増加およびIPコアを用いた回路設計の一般化に伴い，IPコアベンダーによるVLSIに対する攻撃は容易になっている[2].

VLSIの設計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].

近年VLSIの発展に伴い，旅客機や自動車などの人命に関わる重要なシステム(ミッションクリティカルなシステム)に組み込まれるようになった．ミッションクリティカルなシステムにトロイ回路が挿入されたIPコアを組み込んだ場合，社会的な問題に発展する恐れがある．

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[6]．しかしながら，ステルス性の高いトロイ回路[9]を完全に識別することは困難である．このことより本論文では，トロイ回路が挿入された場合でも異常な動作を実現させない設計(トロイトレラント設計)法を提案する．なお本論文では，他社が設計したRTL回路をIPコアと仮定し議論する．またRTL回路の設計には動作合成技術を利用するものとする．

## 2 動作合成

本章では動作合成について説明する．動作合成[10]とは，C言語などによって記述された動作記述から，Verilog-HDLなどのハードウェア記述言語によって記述されたRTL(Register Transfer Level)回路を生成する技術である．動作合成では，入力された動作記述に対し，グラフ生成，スケジューリング，バインディング，

---

Hardware Trojan Tolerant IP Circuit Designs

Tomohiro BOYASHIKI, Toshinori HOSOKAWA, and Masayoshi YOSHIMURA

RTL回路記述生成の順で処理を行う. 一般的なRTL回路は, データパス部とコントローラ部によって構成されており, データパス部では演算処理を担っている. コントローラ部では, 要求された機能を実現するためのデータパスに対する制御を担っている.

## 3 トロイ回路

### 3.1 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[7].

### 3.2 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.

### 3.3 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.

### 3.4 RTL 回路に対するトロイ回路

RTL 回路に対するトロイ回路攻撃では, トリガー部とペイロード部をそれぞれコントローラ部とデータパス部に分割して挿入することが可能である. 近年, コントローラ部とデータパス部から構成される RTL 回路を対象にテスト生成を行う研究が行われている[10]. 回路仕様上, 起こりえない制御信号がコントローラから入力された場合に起動するペイロード部をデータパス部に挿入することで, トロイ回路の機能を隠ぺい可能であることが予想される. コントローラ部にトリガー部を挿入することで, 特定の状態時に特定の入力を外部より入力することで, トロイ回路を起動

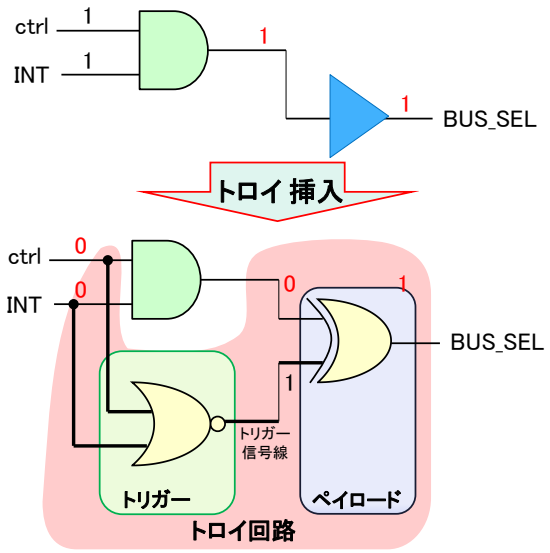


図1. トロイ回路例

させることが可能となり, 偶発的にトロイ回路が起動する確率が低下し, 検出困難なトロイ回路となることが予想される. したがって, ペイロード部とトリガー部を分割して, それぞれコントローラ部とデータパス部に挿入することで, トロイ回路の検出はより困難となることが予想される.

## 4 トロイトレラント指向設計法

本章では委託先企業から納品されたVLSI設計データに対して, トロイ回路が挿入された場合を想定してRTL回路のコントローラ部を変更することにより起動不可能なトロイ回路に変更する手法を説明する.

### 4.1 前提条件

本提案手法では, 自社が要件定義した内容を基に委託先企業がRTL回路設計する際にトロイ回路が挿入されることを想定してる. それゆえ, 本手法では, 以下の情報を自社は持っているものと仮定する.

- 通常機能時のコントローラから出力される制御信号系列
- テストモード時のコントローラから出力される制御信号系列
- RTL回路(コントローラ+データパス)

### 4.2 提案手法

一般的にコントローラから出力される制御信号はデータパスの動作に必要な部分だけがケアビットとなり, その動作を実現させるために必要ない制御信号線の出力値はドントケア

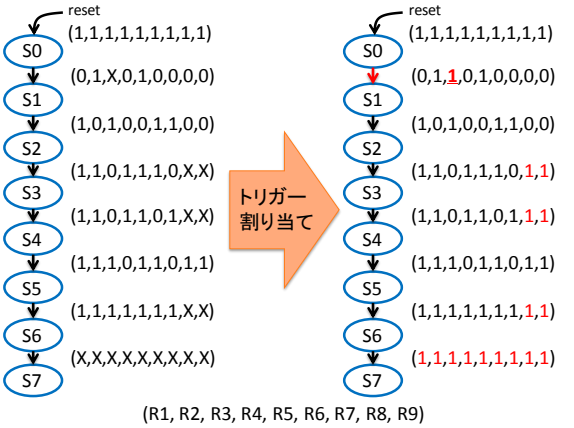


**図2.トロイトリガー挿入済み FFTコントローラ出力信号**

となる．トロイ回路攻撃を行う攻撃者にとって，ドントケアの制御信号はトロイ回路の起動を制御するトリガー条件に利用することが容易である．それゆえ，本来ドントケアである制御信号に対してケアビットが割当てられていた場合，何らかの意図があるものと推測することができる．本提案手法では，RTLコントローラのドントケアにケアビットが割当てられていた場合，トロイ回路の起動に利用するトリガー信号であると仮定し，制御信号線を反転させることで，起動不可能なトロイ回路に変更する．

## 5 実験結果

本章ではトロイ回路が挿入されたRTL回路に対して，本提案手法を用いて再設計した結果を示す．本実験で使用するベンチマーク回路は，FFT(フーリエ変換)の動作記述を使用する．挿入したトロイ回路の攻撃内容としては，動作合成により生成されたRTL回路の出力系列を変更する機能を実装した．

図2にFFT回路のコントローラ部が出力する制御信号の一部を示す．本実験で挿入したトロイ回路は，状態S0から状態S1に遷移する際に出力する，制御信号R3の'X'を利用してトリガー信号をデータパス部へ送信する．本実験では，トリガー信号を隠ぺいするために，攻撃者はトリガー信号と無関係な'X'に対しても何らかのケアビットを割当てるものとする．

図3にトロイ回路起動時に影響を受ける部分を抜粋したFFT回路のデータパス部を示す．正常回路における状態S1の機能動作は，図3に示す外部入力Fの値がMUX7経由でレジスタR3に取り込まれ，外部へ出力される．トロイ回路が起動した場合，外部入力Fの値が外部へ出力されるべき時刻で不定値が出力される設計を行った．

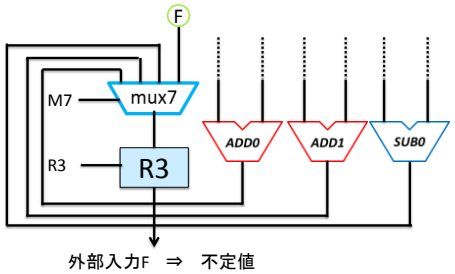


**図3.FFTデータパス抜粋図**

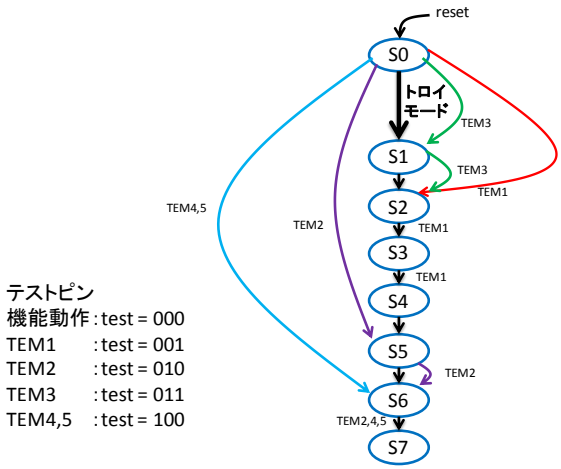


**図4.トロイトリガー挿入済み FFTコントローラ**

本実験に使用したFFT回路は文献[10]で提案された機能的k時間展開モデルによるテスト容易化設計が施されているものとする．図4にテスト容易化設計が施された，FFT回路のコントローラを示す．本実験で挿入したトロイ回路は，機能動作時にテスト容易化設計で追加したテストピンに，特定の値を入力することでトリガー信号をデータパスへ出力する．

図5では図上部より順に，クロック信号，正常回路の出力信号，図4のコントローラ部を用いて合成された回路の出力信号，提案手法を用いて生成されたコントローラ部を用いて合成された回路の出力信号を示している．図4のコントローラを用いた回路の出力信号は，トロイ回路の影響で，正常回路の出力信号と異なり，不定値を出力している．提案手法を用いたコントローラを用いた回路の出力信号は，トロイ回路が挿入されているにもかかわらず，正常な回路と等しい出力結果となった．以上の実験結果より，本提案手法を用いることでトロイ回路を起動不可能なものに変更することが可能であることが予想される．

## 6 おわりに

本論文では業務の一部を外部へ委託(または外部よりIPコアを購入)した際のトロイトレラ

ント性を考慮した，再設計手法の提案と検証を行った．実験結果より，FFTに挿入したトロイ回路の無効化に成功した．また、本提案手法ではケアビット割当てが行われた全ての制御信号を反転しており，低消費電力などを考慮した設計を破壊する恐れがある．したがって，今後の課題はケアビット反転の最小化や実験に使用するベンチマーク回路の追加，複雑なトロイ回路に対する実験などが挙げられる．

「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] 坊屋鋪知拓，細川利典，吉村正義，"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"，DA シンポジウム(2015):199-204.

[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.

[10] Yusuke Kodama, Jun Nishimaki, Tetsuya Masuda, Toshinori Hosokawa and Hideo Fujiwara, “ A Controller Augmentation Method to Generate Easily Testable Functionl k-Time Expansion Models for Data `Path Circuits”, The Ninth Workshop on RTL and High Level Testing(WRTLT’13).


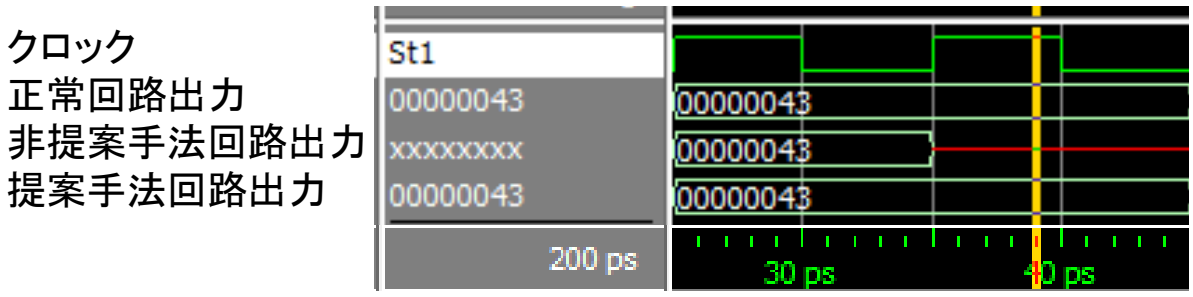


図 5. トロイトレラント指向設計シミュレーション結果