ISSN 2186-5647

2-51

FPGA を用いた AES 暗号回路におけるトロイ回路設計の実装評価

日大生産工　○坊屋鋪　知拓　日立ソリューションビジネス　荻田　英実
日大生産工　細川　利典　九大(院)　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，海外の工場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，設計の一部のみ自社で行い，その他の設計は他社に，製造は製造コストの安い国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．その結果として VLSI の信頼性の低下が懸念されている．

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 の設計および製造工程への攻撃がある[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，あるいは攻撃により得られた情報を悪用するものと定義する．

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]．攻撃方法としては，攻撃者が設定した特定の条件をトリガー条件として，攻撃を行う．トロイ回路による攻撃により，VLSI が組込まれた製品やシステムは，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[2,3]．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．
- トロイ回路が発動するのは，限られたトリガー条件下のみである．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パターン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[2,3]．現在では製品に混入したトロイ回路を検出するためのさまざまな研究が行われている[3]．しかしながら，現在トロイ回路に対する有効な検出方法が提案されていないだけでなく，それぞれの手法

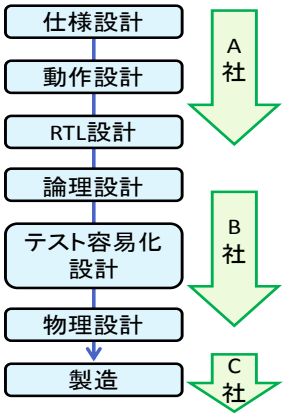

図 1. VLSI 設計フロー

のトロイ回路検出能力を測る適切なベンチマーク回路が存在しない．このことより本論文では，AES(Advanced Encryption Standard)暗号回路[4]に対してトロイ回路を設計する．そして設計した回路を，FPGA(Field-Programmable Gate Array)を用いて実装し，面積，故障検出率，鍵逆算時間などの評価を行う．なお本論文で取り扱う AES 暗号回路[4]は，図 1 に示す VLSI 設計フローの仕様設計から RTL(Register Transfer Level)設計までをファブレスメーカーA 社が担当し，論理設計から物理設計を専門企業 B 社が請け負う．B 社が作成した物理設計をもとに，ファウンドリ C 社が VLSI の製造を行うものと仮定する．

2　トロイ回路

2.1　トロイ回路

トロイ回路とは，VLSI の設計及び製造段階において，悪意ある攻撃者により挿入される悪意ある回路である．トロイ回路は，特定の条件下で正規の回路に対して攻撃を行う．トロイ回路は一般的に，発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]．

トリガー部では回路入力に対し，攻撃者の設定したトリガー条件に一致するか否かを判定する．[7,8]

ペイロード部とは，もとの回路に対して，機密情報の漏洩や回路機能の無効化，あるいは回路破壊などの攻撃

An Evaluation of Hardware Trojan Implementation on AES Cipher Circuit using FPGA
Tomohiro BOUYASHIKI, Amy OGITA, Toshinori HOSOKAWA, and Masayoshi YOSHIMURA

を実行する回路である．ペイロード部はトリガー部で設定された起動条件を満たす場合のみ，攻撃を実行する[7,8].

3. トロイ回路設計

3.1 トロイ回路混入の前提

A 社は自社で顧客の要求定義から RTL 設計までを行う．その後，RTL 設計を行った回路データを，専門業者 B 社に渡す．B 社は，A 社から渡された回路データをもとに，論理設計後，テスト容易化設計を行い，物理設計を行う．その後，B 社は物理設計が完了した回路データを依頼主である A 社に納品する．A 社は，B 社から納品された回路データを検証し，その後，回路データを C 社に渡し，製造を依頼する．このような流れで，VLSI の設計，製造フローが進むものとする．

3.2 VLSI 製造フローにおけるトロイ回路混入

3.1 節で述べた設計，製造フローに対し，攻撃者が攻撃を仕掛けることを考える．本論文では，論理設計から物理設計を担当する B 社において，攻撃者がテスト容易化設計の過程でトロイ回路を混入すると仮定する．

A 社は AES 暗号回路のテスト容易化設計を B 社に依頼する．このとき，A 社はスキャンベース攻撃[9,10]を避けるため，テスト容易化設計手法として，スキャンベースの組込み自己テスト(Built In Self Test:BIST)機能[6]の設計を依頼する．本論文において，スキャンベース BIST を動作させるために使用されるテスト専用の機能をテストモードと定義する．

一般に BIST は，疑似ランダムパターン生成部(Pseudo-Random Pattern Generator:PRPG)として線形帰還シフトレジスタ(Linear Feedback Shift Register:LFSR)，テスト対象回路(Circuit Under Test:CUT)として AES 回路，応答圧縮器として多入力シグネチャレジスタ(Multiple Input Signature Register: MISR)で構成されている．

3.3 テストモードを利用したトロイ回路の検出困難性

B 社が物理設計済みの回路データを納品する際に，A 社はテストモードを使用しない状態における回路機能の等価性と，テストモードを使用する場合の故障検出率のみを検証すると予想される．ここで，A 社が要求した通りの故障検出率を満たしている場合，A 社は B 社が論理物理設計した回路の機能を詳細に検証せず，製造工程へ進む．このため，トロイ回路が混入される危険性を A 社が想定していない場合，トロイ回路を検出することは困難である．

3.4 トロイ回路仕様

本節では B 社が挿入したトロイ回路について説明する．本論文で述べているトロイ回路は，AES 暗号方式が一定のラウンド処理を繰り返し，暗号化を行う点を利用している．なお, AES 暗号回路から出力される暗号文を RK_{11} とし，ラウンド処理が x(x は任意の整数)回実行されたあとに生成されるデータを RK_{x+1} とする．暗号文 RK_{11} が出力されたあとにラウンド処理が x 回実行された場合，生成されるデータは $RK_{11+(x+1)}$ となる．

- ペイロード部

ペイロード部では，暗号化処理終了後に回路内でラウンド処理を継続し，データ $RK_{11+(x+1)}$ を出力する機能を実装している．攻撃者は出力されたデータ $RK_{11+(x+1)}$ を用いて，AES 暗号回路内で使用されている共通鍵を導出する．

- トリガー部

トリガー部では暗号化終了後，テストモードの起動条件を満たした場合，トロイ回路を起動させる信号をペイロード部へ送る．

3.5 鍵逆算アルゴリズム

攻撃者はトロイ回路攻撃により，データ $RK_{11+(x+1)}$ と，1 ラウンド分処理数が異なるデータ $RK_{11+(x+2)}$ を得る．攻撃者は $RK_{11+(x+1)}$ と $RK_{11+(x+2)}$ を用いて当該するラウンドのラウンド鍵を逆算する．攻撃者は入手したラウンド鍵と，正規の暗号文を用いて初期鍵(共通鍵)を算出する．[4]

4. テスト容易化設計

本章では，B 社が設計するテスト容易化設計でのスキャンベース BIST 構造のについて述べる．

4.1 BIST 概要

B 社において設計される BIST 回路は，LFSR，フェーズシフタ，MISR，比較器，テストコントローラで構成されている．

テストモード実行時にテストコントローラでは，外部より入力された初期シード値を LFSR へ送る．次に LFSR で生成された疑似ランダムテストパターンをフェ

表 1. フェーズシフタの有無による故障検出率

トロイ無			トロイ有		
	LFSR	フェーズシフタ		LFSR	フェーズシフタ
故障検出率	98.72%	99.95%	故障検出率	98.72%	99.94%
検出故障数	108398	109741	検出故障数	108458	109801
総故障数	109,800		総故障数	109,866	

ーズシフタ[2]により，エンコードする．エンコードしたテストパターンは，CUT(AES 暗号回路)内のスキャンパスを経由して CUT 内のフリップフロップ(Flip Flop:FF)に設定される. テストパターンが CUT 内の全ての FF に設定された状態で，CUT 内の組合せ回路部で，通常動作を実行する．その後，再び LFSR で生成された疑似ランダムテストパターンを CUT 内の全ての FF に設定する．なお, このときスキャンパスより出力された値を, MISR に取り込む.

最後に MISR の応答圧縮結果が期待値と一致するか比較器を用いて検証する.

4.2 LFSR 回路

B 社が設計した LFSR はテストコントローラから入力されたテストモード信号が真である場合，テストコントローラから入力された初期シード値を設定する．なお，B 社が設計した BIST 回路では，スキャンチェーン数を 16 本に設定していたため，LFSR も 16 ビットのものを使用する.

4.3 フェーズシフタ

LFSR で生成される疑似ランダムパターンには一定の規則性が存在する．フェーズシフタは XOR ゲートを追加することで，規則性を緩和する回路である.

4.4 CUT 回路

本論文では，B 社は CUT 内のスキャンパス数を 16 本に設定している．また，テスト実行時に平文と秘密鍵の入力を LFSR から行うため, 外部入力と LFSR 入力を切り替えるマルチプレクサが組み込まれている.

4.5 MISR 回路

MISR 回路では，テストコントローラより入力される MISR 制御信号が真である場合, CUT 回路のスキャンパスより出力される値を圧縮し，圧縮された符号を比較器に出力する.

表 2. トロイ回路挿入の有無による面積の比較

	面積(ゲート数)
BIST回路全体 (トロイなし)	27237
BIST回路全体 (トロイあり)	27291

4.6 比較器

比較器では，MISR 出力と期待値を比較する．MISR 回路の圧縮結果が期待値と一致した場合，真を，一致しない場合は，偽を出力する.

4.7 テストコントローラ

テストコントローラ回路では，BIST 回路内の各モジュールへ制御信号を出力している.

5. 実験結果

AES 暗号回路に対する BIST 回路を Verilog-HDL で設計，FPGA で実装し，トロイ回路の影響と鍵逆算時間の評価実験を行った．本実験では, ALTERA 社の Signal Tap Ⅱ[5]を使用し回路内を観測した.

図 2 と図 3 は，FPGA の出力結果を示している．図 2 は，トロイ回路が起動していない場合に出力されている暗号文を示している．一方，図 3 は，図 2 の状態で，トロイ回路を起動した場合の出力を示している．図 3 出力 dout より，共通鍵を算出するのに必要な情報が出力されていることがわかる．このことより，本論文で述べているトロイ回路を AES 暗号回路に組み込むことで, 共通鍵を逆算するために必要な情報を不正入手することが可能であることが言える．図 4 に示すグラフは，3.5 節で説明したラウンド処理回数 x の変化による共通鍵逆算にかかる計算時間の変化をグラフにまとめたものである．本実験で使用した鍵逆算アルゴリズムは，ラウンド処理回数を x，AES 暗号化処理を A とした場合，$O(xA^x)$の計算量であるため図 4 のグラフは指数関数となった.

次に表 1 は LFSR 単体で生成された疑似ランダムテストパターンにおける故障検出率と，フェーズシフタを付加した場合の故障検出率を示している．トロイ回路の有無に関わらず，フェーズシフタを追加することにより故障検出率は向上した．また，トロイ回路挿入による故障検出率は 0.01%の増加と微小であるため，故障検出率によるトロイ回路の検出は困難である.

次に本実験で設計した AES 暗号回路の面積評価結果を表 2 に示す．2.2 節で述べたトロイ回路を検出する従来法[1]では，トロイ回路を検出する指標として消費電力

BIST_TOP:bist|dout	3925841D02DC09FBDC118597196A0B32h
BIST_TOP:bist|BIST_CONTROL:control|trigger	
BIST_TOP:bist|din	3243F6A8885A308D313198A2E0370734h
BIST_TOP:bist|key	2B7E151628AED2A6ABF7158809CF4F3Ch

図 2. 通常モード出力

BIST_TOP:bist|dout	3183D18B80921B6632EDFF9CEDA6E1C8h 4D8EFDECBD640FC94E5BA70E37EE8159h
BIST_TOP:bist|BIST_CONTROL:control|trigger	
BIST_TOP:bist|din	3243F6A8885A308D313198A2E0370734h
BIST_TOP:bist|key	2B7E151628AED2A6ABF7158809CF4F3Ch

図 3. 通常モード出力(トロイ起動)

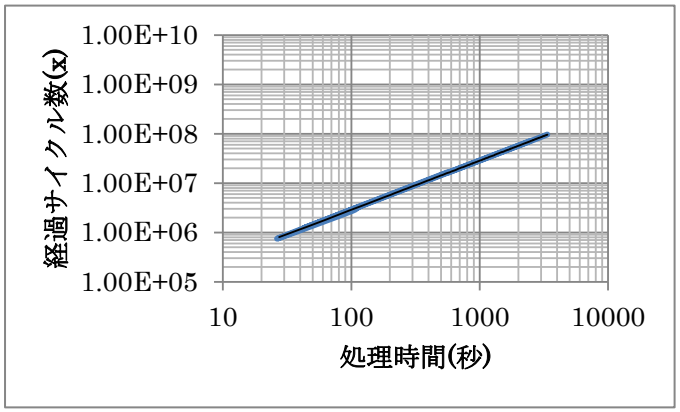

図 4. 鍵逆算処理時間

を用いる．一般に，回路の消費電力は各信号線の値の遷移回数に比例して増加する．このことより，回路内のゲート数を評価した結果, 増加率は約 0.198%と微小な増加に抑えることができた．

6. おわりに

本論文では, AES 暗号回路のテスト容易化設計として BIST 回路の設計および，テスト容易化設計を利用したトロイ回路の設計を行った．

提案したトロイ回路の面積は，もとの回路と比較して 0.2%以下の増加であった．このため，従来手法[1]によるトロイ回路の検出が困難であると予想される．

課題としては，挿入したトロイ回路の検出手法の提案が挙げられる．

7. 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] Janusz Rajski, Nagesh Tamarapalli, Jerzy Tyszer, "Automated Synthesis of Phase Shifters for Built-In Self-Test Applications",Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on (Volume:19 , Issue: 10)

[3] Mohammad Tehranipoor and Farinaz Koushanfar,"A Survey of Hardware Trojan Taxonomy and Detection, " IEEE Design & Test of Computers, pp.10-25, Jan/Feb. 2010.

[4] Masayoshi Yoshimura, Amy Ogita, and Toshinori Hosokawa, “An Estimation of Trojan Circuits on AES Encryption Circuits”, November 22th 2012 @WRTLT'12

[5] 小林優，”FPGA ボードで学ぶ組み込みシステム開発入門 ~Altera 編~”,技術評論社, 2011 年 10 月 25 日.

[6] M. Arai, S. Fukumoto, K. Iwasaki, T. Hiraide, T. Aikyo, "Test Data Compression Using TPG Recon-struction for BIST-Aided Test, " proc IEEE 6th Work-shop on RTL and High Level Testing(WRTLT' 05), 2005.

[7] Yier Jin, Nathan Kupp and Yiorgos Makris, "Experi-ences in Hard-ware Trojan Design and Implementa-tion, " 2009 IEEE International Workshop on Hard-ware-Oriented Security and Trust, 2009.

[8] X. Wang, M. Tehranipoor, and J. Plusquellic, "Detecting Malicious Inclusions in Secure Hardware: Challenges and Solutions, " Proc. IEEE Int’l Workshop Hardware Oriented Security and Trust (HOST 08), IEEE CS Press, pp. 15-19, 2008.

[9] B.Yang, K.wu, and R.Karri, "Secure scan: A de-sign-for-test architecture for crypto chips, " IEEE Transactions on Computer -Aided Design of Intergrat-ed Circuit and Systems, pp.2287-2293, October 2006.

[10] B.Yang, K.wu, and R.Karri, "Scan based side channel attack on dedicated hard ware implementations of Data Encryption Standard, " Proceedings of Interna-tional Test Conference 2004 (ITC’ 04), pp.339-344, 2004.