ISSN 2186-5647

2-21

AES 暗号回路におけるトロイ設計の影響評価

日大生産工（院）○荻田 英実　日大生産工　細川 利典
九大　吉村 正義

1. はじめに

近年，大規模集積回路(Large Scale Integration circuits:LSI)は，社会情報基盤技術(infrastructure:インフラ)や，信用に関する情報を保持するシステムにおいて使用される．それゆえ，LSI の信頼性が社会に与える影響は大きくなってきている[1].

近年 LSI の製造は，海外工場に委託されることが多い[1]．製造コストが安い国に外注することにより，製造コストの削減が図られる．しかしながら，外注により LSI の製造に関与する組織や人が増加することにより，LSI の信頼性の低下が懸念される．

LSI の信頼性に関する問題の一つとして，攻撃者による LSI の設計および製造工程への攻撃がある[1,2]．本論文において攻撃者とは，LSI に対して攻撃を行う者，あるいは攻撃により得られた情報を悪用する者と定義する．外注の増加，および外注先の企業の多様化に伴い，外注先における LSI に対する攻撃は容易になってきている[1].

LSI の設計，製造過程における攻撃の一例として，トロイ回路の混入がある[1]．トロイ回路とは，攻撃者が設定した特定の条件をトリガーとして，攻撃を行う回路である．トロイ回路攻撃により，LSI が組み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，回路破壊といった脅威にさらされる[1,2]．トロイ回路の特徴として，以下の 3 点がある．

- トロイ回路の挿入の前後において，もとの回路の物理的な外観は損なわれない．
- 製造された LSI の入出力動作は，トロイ回路挿入がある場合においても，正規の設計仕様を満たす．
- トロイ回路が攻撃を行うのは，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 LSI の設計仕様上，使用されない入力パターンが利用されることが多い．

以上より，一般的な LSI 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]．現在では製品に混入したトロイ回路を検出するための様々な研究が行われている[2].

本論文では，128 ビットの暗号鍵に対応した AES(Advanced Encryption Standard)暗号回路[3,4]に対してトロイ回路を挿入し，その影響を評価する．また，トロイ回路攻撃により得た情報を利用し，AES の暗号鍵を逆算するアルゴリズムを提案する．

2. トロイ回路

2-1.トロイ回路

トロイ回路とは，LSI の設計もしくは製造段階において攻撃者により挿入される特定条件下で任意の回路に対して攻撃動作を行う回路のことである．トロイ回路は一般的に，起動条件の判定を行うトリガー部と攻撃動作を行うペイロード部から成る[5,6].

トリガー部とは，もとの回路の状態や信号線の値が，攻撃者の設定したトロイ回路の起動条件を満たすかを判定する回路である．起動条件の一例としては，回路内のカウンタが特定の値になる，対象信号線に特定の制御値が入力されるなどがある[6,7].

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動作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，動作する[6,7].

2-2.トロイ回路の検出手法

トロイ回路検出の従来法の 1 つとして，電力解析を用いた手法がある．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指標とした[1].

トロイ回路が起動条件を満たすと，通常の回路とは異なる消費電力影響が現れる．しかしながら，回路の消費電力影響は，もと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小さくなる．また，消費電力を指標とする場合，回路動作時の微小なノイズや，回路自身の製造ばらつきも問題となる．これらの要因により，単純電力解析を用い，消費電力を指標としてトロイ回路を検出することは困難になる．

Agrawal らは，製造ばらつきや回路動作時の微少なノイズの影響を低減するために，測定した消費電力に対する主成分分析として，Karhunen-Loeve(KL)展開法を用いた．Agrawal らはばらつきがあり，トロイ回路が混入していない複数個の回路に対して，消費電力を測定した．その測定値に対して KL 展開を用いて消費電力の特徴を分析し，トロイ回路を判別する指標とした．これにより，製造ばらつきを含む回路においても，トロイ回路検出が可能になった．

本論文では，消費電力影響，並びに面積影響を抑え、従来手法でも検出が困難なトロイ回路の実装を目指す．

3. AES 暗号回路

3-1.AES 暗号

AES 暗号とは，2001 年にアメリカ国立標準技術研究所(National Institute of Standards and Technology:NIST)で規格化された共通鍵暗号方式の暗号である[3,4].

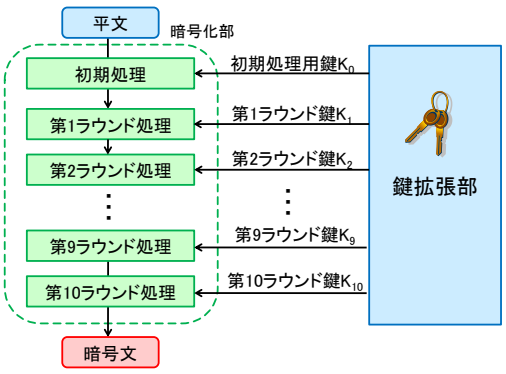

図 1. AES の暗号化処理の概要

Evaluation of the Effect for Hardware Trojan Designs in AES Encryption Circuits

Amy OGITA, Toshinori HOSOKAWA, and Masayoshi YOSHIMURA

AES は平文サイズが 128 ビットで固定される．鍵のサイズは 128，192，256 ビットの 3 種類が用意されているが，本論文では鍵長が 128 ビットの AES を扱う．

AES において，鍵と平文を EXOR 演算やシフト演算によって暗号化する処理をラウンド処理と呼ぶ．AES は，ラウンド処理を繰り返すことにより，暗号文を生成する．ラウンド処理で使用する鍵は，鍵拡張部を用いてラウンドごとに変化させる．図 2 に AES の暗号化処理の概要を示す．128 ビット鍵対応の AES はラウンド処理を 10 回繰り返すことにより，平文を暗号化する．

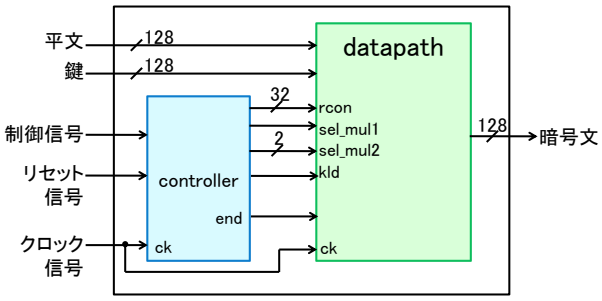

図 2. AES 暗号回路実装概要

3-2.AES 暗号回路

本論文において使用する AES 暗号回路の構成概要を図 2 に，データパスおよびコントローラをそれぞれ図 3，4 に示す．

AES 暗号回路は，暗号化処理を実行する前に，リセット信号に'1'を入力し，リセット処理を行う．リセット処理は，データパス内の信号線に初期値を入力する．

リセット処理実行後，リセット信号に'0'を，制御信号に'1'を入力すると，平文，鍵を入力として AES の暗号化処理を開始する．

暗号化処理は図 4 に示す状態遷移図の状態 ST2 から状態 ST11 の間行われる．そして，最終状態 ST12 で暗号文が出力され，暗号化処理が終了する．

4. トロイ回路設計

4-1.トロイ回路混入の前提

LSI の製造は，1 つのメーカー内で設計から販売までの全工程を行う場合もあるが，設計，製造，販売，それぞれの業務に特化した企業が各工程を分担することもある．本論文では図 5 に示すように，A 社が仕様設計から論理設計までを，B 社がテスト容易化設計からレイアウト設計を，C 社が製造業務をそれぞれ担当するものとする．

A 社は自社で顧客の要求仕様から 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 社に納入する．A 社は，B 社から納品される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，LSI の設計，製造フローが進むものとする．

4-2.トロイ回路仕様

4-1 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に乗じて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[8,9]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[10]の追加を依頼する．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．

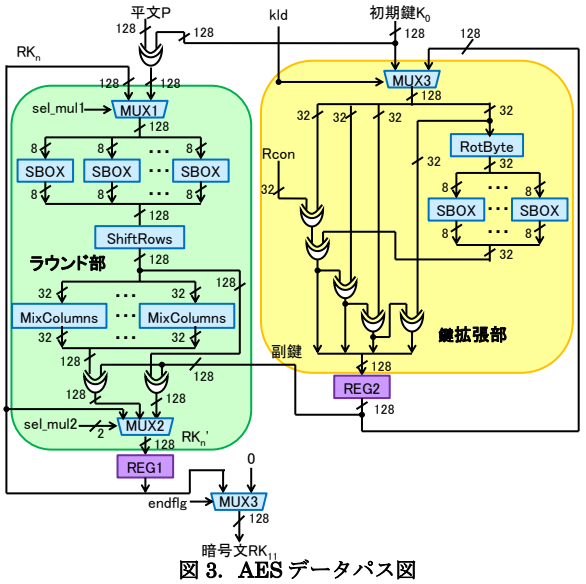

図 3. AES データパス図

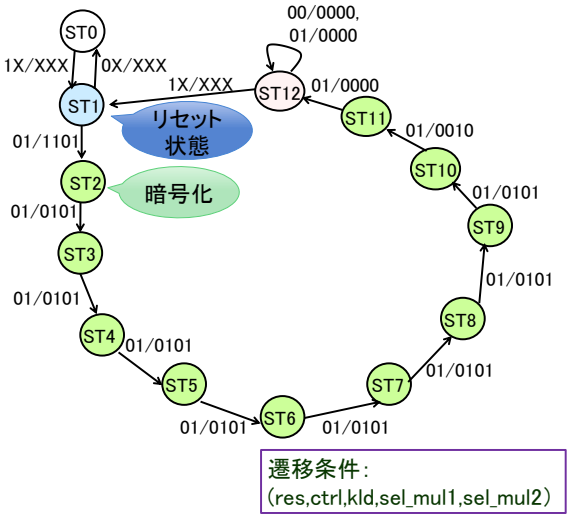

図 4. AES コントローラ図

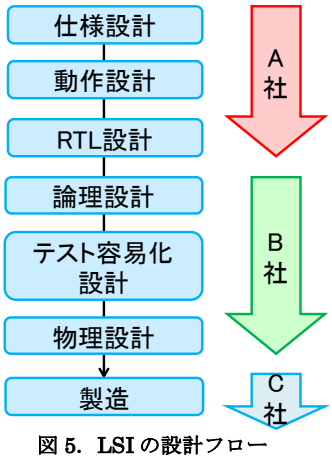

図 5. LSI の設計フロー

4-3. トロイ回路仕様

AES 暗号回路から出力される暗号文を RK_{11}，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．

トロイ回路のペイロード部として，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する．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る暗号鍵を導出する．

トロイ回路のトリガー条件としては，暗号化処理終了後，テストモードが起動する場合を条件に設定する．

AES 暗号回路のデータパス部に対して挿入されたトロイ回路を図 6 に示す．暗号文を格納するレジスタ REG1 に接続されたマルチプレクサ MUX2 に対してトロイ回路を挿入する．図 6 の破線部分で囲われた箇所がトロイ回路である．

図 3，4 より AES 暗号回路は，暗号化処理が完了する状態 ST12 において暗号文 RK_{11} を出力する．このとき，回路のテストモードを利用する際に用いられる制御信号”TE”に’1’を入力すると，図 6 のトロイ回路部において，マルチプレクサ MUX2 の制御信号 sel_mul2 に”01”が入力される．これにより，マルチプレクサ MUX2 は $RK_{11+(x+1)}$’に MixColumns モジュールの演算結果を出力する．マルチプレクサ MUX3 を制御する信号線”endflg”は，暗号化処理終了後においてアクティブであり，$RK_{11+(x+1)}$を選択する．以上より，MixColumns モジュールの演算が再開されると同時に，その演算結果がデータ $RK_{11+(x+1)}$として回路の外部出力に出力される．

なお，MUX2 の制御信号の値と出力値の関係は表 1 に示す通りである．また，図 3，4 におけるマルチプレクサ MUX2 の制御信号と出力信号線の対応は，最右端から制御信号が”00”の場合の出力，”01”の場合の出力，”10”の場合の出力である．

表 1．MUX2 の割り当て表

sel_mul2	出力値
00	x回目のラウンド処理により生成されるデータ($RK_{11+(x+1)}$')
01	MixColumnsモジュールの演算結果
10	ShiftRowsモジュールの演算結果
11	0

4-4．鍵逆算アルゴリズム

攻撃者はトロイ回路攻撃により得たデータを用いて，秘密鍵を算出する．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キーを逆算する．攻撃者は入手したラウンドキーと，正規の暗号文を用いて図 6 において初期鍵 K_0 と定義される秘密鍵を算出する．

AES 暗号回路から得たデータ $RK_{11+(x+1)}$および $RK_{11+(x+2)}$を用いて，初期鍵 K_0 を導出するアルゴリズムのフローチャートを図 7 に示す．

(step1)：AES 暗号回路を動作させ，暗号文 RK_{11} を得る．

(step2)：トロイ回路攻撃により，データ $RK_{11+(x+1)}$および $RK_{11+(x+2)}$(x は任意の値)を AES 暗号回路から出力する．

(step3)：式 1 を用いて 11+(x+1)ラウンド目のラウンドキー $K_{11+(x+1)}$を導出する．

$$K_{11+(x+1)} = R_{11+(x+1)} \oplus RK_{11+(x+2)} \quad \text{...(式 1)}$$

トロイ回路が攻撃を行うことにより，AES 暗号回路は再度，暗号化処理を実行する状態になる．式 1 中の $R_{11+(x+1)}$は，トロイ回路攻撃により取得したデータ $RK_{11+(x+1)}$を図 6 のラウンド部に入力することで得られる．図 6 のラウンド部では，文献 [4] で述べられている "SubBytes"，"ShiftRows"，"MixColumns"，"AddRoundKey"という 4 つの暗号化処理が実行される．

(step4)：データ $RK_{11+(x+1)}$を暗号化する際，用いられるラウンドキー $K_{11+(x)}$を，式 2 を用いて導出する．

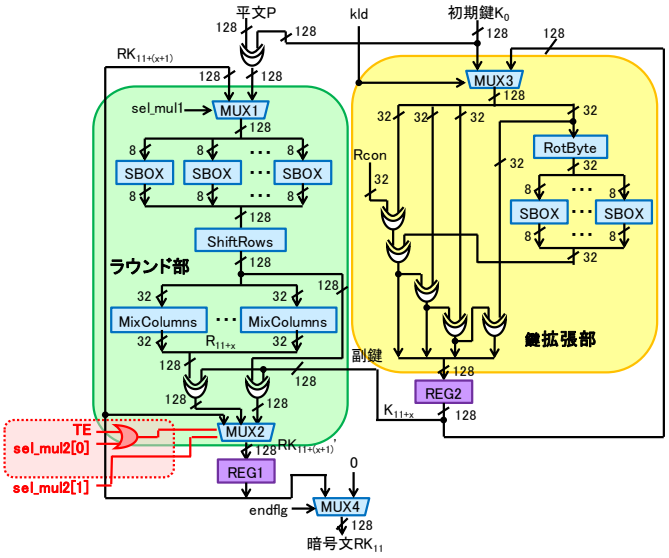

図 6．トロイ回路実装

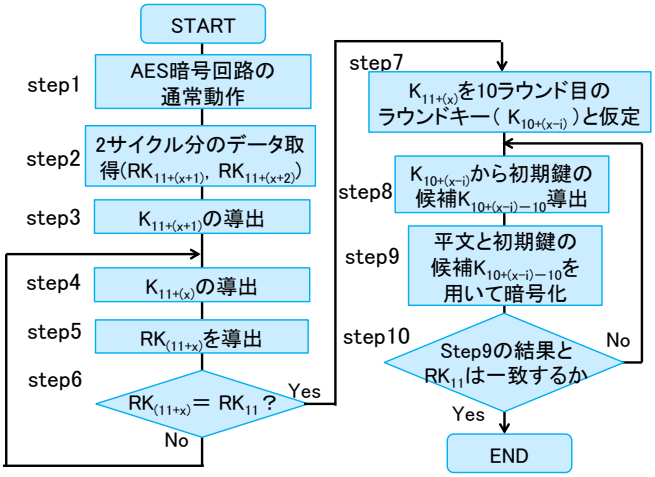

図 7．暗号鍵逆算アルゴリズム

$$K_{11+(x)} = KeyExp^{-1}(K_{11+(x+1)}) \quad \text{...(式 2)}$$

関数 $KeyExp^{-1}$は，AES 復号時に用いられる暗号鍵の逆算を行う関数である[3]．

(step5)：step4 で導いたラウンドキー $K_{11+(x)}$，およびデータ $RK_{11+(x+1)}$を用いて，1 ラウンド前に AES 暗号回路内で使用されるデータ $RK_{(11+x)}$を式 3 より導出する．

$$RK_{(11+x)} = Round^{-1}(RK_{11+(x+1)}, K_{11+(x)}) \quad \text{...(式 3)}$$

関数 $Round^{-1}$は AES 復号時に用いられるラウンド処理データの逆算を行う関数である[5]．

(step6)：step5 で導いたデータ $RK_{(11+x)}$と暗号文 RK_{11} を比較する．比較したデータが一致しない場合は step4 に戻り，$K_{11+(x)}$を入力として式 2 を用いて 1 つ前のラウンドキーを導出する．また，導出したラウンドキーで $K_{11+(x)}$を更新する．比較したデータが一致する場合は step7 に進む．

(step7)：ラウンドキー $K_{11+(x)}$を 10 ラウンド目に使用されるラウンドキー $K_{10+(x-i)}$($0 \leqq i \leqq x-10$)と仮定する．

(step8)：ラウンドキー $K_{10+(x-i)}$，式 2 を用いて初期鍵の候補 $K_{10+(x-i)-10}$ を導出する．

(step9)：平文 P と step8 で導いた初期鍵の候補 $K_{10+(x-i)-10}$

を用いて AES の暗号化処理を行う．

(step10)：step9 の暗号化結果と暗号文 RK_{11} を比較する．結果が不一致の場合，step8 で使用したラウンドキー$K_{10+(x-i)}$を入力として式 2 を実行し，ラウンドキー$K_{10+(x-i)}$を更新する．ラウンドキー更新後，step8 に戻る．比較結果が一致した場合，step8 で導出した $K_{10+(x-i)-10}$が初期鍵である．

5. 評価実験

3 章で設計した AES 暗号回路に対し，4 章で設計したトロイ回路を組み込み，評価実験を行った．トロイ回路の有無による回路影響の比較を表 2，表 3 に示す．

表 2 のトグル回数とは，論理シミュレーションを実行した際に各信号線の値の遷移が起きた回数の総数である．2-2 節で述べたトロイ回路を検出する従来法[2]では，トロイ回路を検出する指標として消費電力を用いる．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．このため，各信号線の値の遷移回数を測定することにより，消費電力の影響を評価できる．表 2 より，トロイ回路挿入により AES 暗号回路の面積，信号線数は 0.01%増加した．また，信号線のトグル回数はトロイ回路挿入の有無に関わらず，同等な値が得られた．

表 3 に示す回路のテスト容易性の比較結果は，疑似ランダムパターン 10000 個を入力として，Synopsis 社の TetraMax を用いて縮退故障を対象とした故障シミュレーションを実行した結果得られたものである．表 3 において，「故障検出率」は全故障に対する故障の検出率，「総故障数」は回路上に存在するすべての故障数，「検出故障数」は総故障数のうち，実験で使用した疑似ランダムパターンにより検出可能な故障の数，「未検出故障数」は疑似ランダムパターンにより検出できなかった故障の数を示す．表 3 より，総故障数，検出故障数はトロイ回路の有無により約 0.01%増加した．これは，表 2 に示す通り，トロイ回路挿入により回路の信号線数が増加したことによる影響であると考えられる．

表 2. トロイ回路挿入の有無による比較(1)：面積とトグル回数

	面積（ゲート数）	信号線数	トグル回数
AES暗号回路（トロイなし）	21565	37493	73534
AES暗号回路（トロイあり）	21568	37495	73534

表 3. トロイ回路挿入の有無による比較(2)：テスト容易性

トロイ	故障検出率	総故障数	検出故障数	未検出故障数
無	99.90	96762	96665	97
有	99.90	96772	96675	97

提案したトロイ回路は面積，トグル回数ともに，もとの AES 暗号回路と比較した場合の差異が 0.01%以下である．また，テスト容易性の面においてはトロイ回路の有無により大きな差異は現れなかった．このため，従来法[2]によるトロイ回路の検出が困難であると予想される．

6. おわりに

本論文では，AES 暗号回路に対して回路面積，消費電力，テスト容易性の面で影響が少ないトロイ回路設計を行った．また，トロイ回路攻撃により出力したデータを用い，AES 暗号回路で使用される秘密鍵を逆算する鍵逆算アルゴリズムを提案した．

鍵逆算アルゴリズムは検証の結果，x－10 回逆算処理を行うことで，AES の暗号化処理に使用される初期鍵 K_0の導出が可能である．なお，x は暗号文出力後からトロイ回路が AES 暗号回路上で動作するまでに経過したクロック数とする．

今後の課題としては，挿入したトロイ回路の評価結果を踏まえたトロイ回路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 using IC Fingerprinting", 2007 IEEE Symposium on Security and Privacy, pp.296-310, 2007.

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

[3] 神永正博，山田聖，渡邊高志，"Java で作って学ぶ暗号技術-RSA,AES,SHA の基礎から SSL まで"，森北出版，2008, pp. 115-142.

[4] National Institute of Standards and Technology, "Advanced Encryption Standard (AES)", FIPS PUB 197, Nov. 2001.

[5] H. Salmani, M. Tehranipoo and J. Plusquellic, "New Design Strategy for Improving Hardware Trojan Detection and Reducing Trojan Activation Time", 2009 IEEE International Workshop on Hardware-Oriented Security and Trust (HOST'09), pp.66-73, July 2009.

[6] Yier Jin, Nathan Kupp and Yiorgos Ma-kris, "Experiences in Hard-ware Trojan Design and Implementation", 2009 IEEE International Workshop on Hard-ware-Oriented Security and Trust, 2009.

[7] X. Wang, M. Tehranipoor, and J. Plusquellic, "Detecting Malicious Inclu-sions in Secure Hardware: Challenges and Solutions", Proc. IEEE Int'l Work-shop Hardware Oriented Security and Trust (HOST 08), IEEE CS Press, pp. 15-19, 2008.

[8] 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.

[9] 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.

[10] M. Arai, S. Fukumoto, K. Iwasaki, T. Hiraide, T. Aikyo, "Test Data Compression Using TPG Reconstruction for BIST-Aided Test", proc IEEE 6th Workshop on RTL and High Level Testing, 211-8588, 2005.