社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2008－SLDM－137 (10)
2008 / 11 / 17

暗号回路における動的に構造変化するセキュアスキャンアーキテクチャ

跡部 浩士† 奈良 竜太† 史 又華† 戸川 望† 柳澤 政生†
大附 辰夫†

† 早稲田大学大学院基幹理工学研究科 情報理工学専攻
〒 169–8555 東京都新宿区新大久保 3–4–1
Tel:03–5286–3392, Fax:03–3204–4875
E-mail: †atobe@yanagi.comm.waseda.ac.jp

あらまし スキャンテストはスキャンチェインを用いた手法で一般的かつ強力なテスト手法である．しかし，スキャンチェインは外部から回路内部の情報を取得できるため，暗号回路においては有効な攻撃手段となりえる．本稿ではスキャンベース攻撃に対するセキュアスキャンアーキテクチャを提案する．スキャンチェイン内のランダムな場所にインバータを挿入し，スキャンチェインの構造を複雑にする防御手法が提案されているが，回路設計時にインバータを挿入する場所が固定されてしまうため，その特徴を利用し攻撃される可能性がある．したがって，設計した後にもスキャンチェインの構造を動的に変化させる必要があると考えられる．我々はラッチを用いて過去の FF の状態を利用することで次のスキャン FF への出力を変化させる状態依存スキャン FF(SDSFF) を提案する．このスキャン FF を用いることでスキャンチェインの構造を動的に変化させることが可能であり，コントローラを必要としないため面積オーバーヘッドも少ない．AES 暗号回路に提案手法を実装し，評価を行った．
キーワード スキャンベース攻撃，セキュアスキャンアーキテクチャ，スキャンチェイン，AES 暗号

Dynamically Variable Secure Scan Architecture against Scan-based Side Channel Attack on Cryptography LSIs

Hiroshi ATOBE†, Ryuta NARA†, Youhua SHI†, Nozomu TOGAWA†, Masao YANAGISAWA†, and Tatsuo OHTSUKI†

† Dept. of Computer Science and Engineering, Waseda University
3–4–1 Okubo, Shinjuku, Tokyo 169–8555, Japan
Tel:03–5286–3392, Fax:03–3204–4875
E-mail: †atobe@yanagi.comm.waseda.ac.jp

Abstract Scan test is a powerful and popular test technique because it can control and observe the internal states of the circuit under test. However, scan chains would be used to discover the internals of crypto hardware, which presents a significant security risk of information leakage. An interesting design-for-test technique by inserting inverters into the internal scan chains to complicate the scan structure has been recently presented. Unfortunately, it still carries the potential of being attacked through statistical analysis of the information scanned out from chips. Therefore, in this paper we propose secure scan architecture, called dynamic variable secure scan, against scan-based side channel attack. The modified scan flip-flops are state-dependent, which could cause the output of each SDSFF to be inverted or not so as to make it more difficult to discover the internal scan architecture. We made an analysis on an AES implementation to show the effectiveness of the proposed method and discussed how our approach is resistant to scan-based side channel attack.
Key words Scan-based attack, Secure scan architecture, Scan chain, AES

1. まえがき

高品質なLSIチップを提供するには，製造したチップを個々に検査するテスト工程が重要である．近年では設計自動化ツールの利用や，プロセスの微細化の影響により，回路規模が爆発的に増大している．そのような大規模集積回路のテストは，故障の検査をすべき項目が増大するため，回路を設計するときからテストを考慮することが必要である．このための方式として，設計段階でテスト専用の回路を用意しておき，外部ピンから直接制御や観測を行うスキャンテストが利用されている．スキャンテスト方式では回路内のFF(Flip-Flop)を結線し，FFの内部状態を操作・取り出し可能にしておくことで，故障検出率が高く効率的なテストを実現とするものである．

スキャンチェインは回路内のFFの情報にアクセスする事が出来るため，例えば暗号回路の場合，得られた情報を解析することで秘密鍵などの秘密情報が解読される可能性がある．レイアウト次第によりスキャンチェインの結線順序はランダムであるため，解析は容易ではない．しかし，スキャンチェインの結線順序という問題を解決し，スキャンチェインの特徴を用いたスキャンベース攻撃が提案された[6],[7]．スキャンベース攻撃はサイドチャネル攻撃の1つであり，他のサイドチャネル攻撃の手法に比べ短い時間で秘密鍵が解読可能なため，非常に強力な攻撃手法である．

スキャンベース攻撃に対する防御手法は大きく2パターンに分けられる．1つめは，専用のコントローラでスキャンチェインを用いることが出来ないようにすることで保護する方法であり，テストコントローラが必要になるがセキュリティは比較的柔軟に設定することが出来る[1],[4],[7]．しかし，テストコントローラを回路毎に再設計する必要があることや，テストコントローラ自身の面積オーバーヘッドが大きいという欠点がある．2つめは，スキャンチェインを利用することが可能だとしても攻撃者にとって解読できない情報にする手法である[2],[5]．スキャンチェインの入力と出力を回路内部で暗号化するような手法であるため，それが解読されてしまう危険性は高くなる欠点はあるが，基本的にテストコントローラは不必要で面積オーバーヘッドが小さい．回路毎に再設計を行うことなくツールなど自動でセキュアスキャンチェインを構築することが可能であり，IP(知的財産)などにも適応しやすいため，1つめの手法に比べ有意である．

2つめの手法の一つに，スキャンチェイン内のランダムな場所にインバータを挿入し，スキャンチェインの構造を複雑にする防御手法が提案されている[5]．しかし，インバータを挿入する場所が回路設計時に固定され以後変わることがないため，文献[3]の攻撃手法により，安全性が脅かされている．

こうした背景から，設計をした後にもスキャンチェインの構造を動的に変化させることで，スキャンベース攻撃に対する耐性を持つセキュアスキャンアーキテクチャを提案する．我々はラッチを用いて過去のFFの状態を利用し，次のスキャンFFへの出力を変化させる状態依存スキャンFF(SDSFF)を提案する．この提案するスキャンFFをスキャンチェインに導入すると各スキャンFFの出力値がラッチの値により変化するため，我々はスキャンチェインの構造が動的に変化すると定義する．防御対象となる回路に合わせ安全性を柔軟に変更でき，コントローラを必要としないため面積オーバーヘッドが少ないという特徴をもつ．

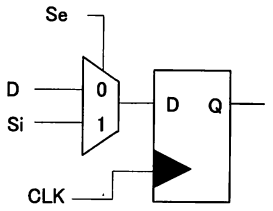

図1　スキャンFF.

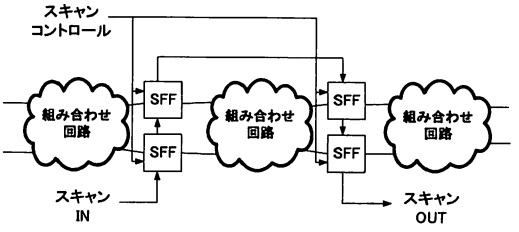

図2　スキャンチェイン.

本稿の構成は以下の通りである：第2節で関連研究について説明する．第3節で暗号回路におけるスキャンベース攻撃に耐性を持つセキュアスキャンアーキテクチャについて提案する．第4節で結果を示し，第5節でまとめる．

2. 関連研究

本節ではスキャンベース攻撃，スキャンベース攻撃に対する防御手法をついてまとめる．

2.1 スキャンベース攻撃

スキャンベース攻撃は，サイドチャネル攻撃の一つであり，スキャンテストで用いられるスキャンチェインを利用した攻撃手法である．スキャンテストでは，回路内のFFをスキャンFF(図1)に変更し，それらを結んだスキャンチェイン(図2)を用いて，回路内部の情報を直接制御，観測することでテストを行う．暗号処理回路に対して，スキャンベース攻撃により秘密情報を取得できることが示されている．テストを行うときと同様に，攻撃者はScan in，Capture，Scan outの操作を順に繰り返し行い，秘密鍵を解析するための情報を取得する．

Scan in：　テストモードで回路内のFFに任意の値を挿入する．

Capture：　システムモードで通常の処理を行う．

Scan out：　テストモードで回路内のFFの値を観測する．

文献[6],[7]では，入力の一部分を変えると，それに対応する部分だけ保存される値が変わることを利用して中間値が保存されるレジスタを特定し，ある入力で実行したときに，そのレジスタに保存された値の関係から秘密鍵を解読する．この攻撃手

法に対する防御手法は多く提案されている [1], [2], [4], [5], [7].

文献 [3] では，中間値が保存されているレジスタを特定する必要はなく，秘密鍵に依存した中間値の 1 ビットが，スキャンチェイン内のレジスタに保存されているかどうかを各レジスタにおいて判定することで秘密鍵を解読する．いくつかの入力パターンで，秘密鍵に依存した中間値がスキャンチェイン内の注目するレジスタに保存されている場合，秘密鍵と相関がある確率が高いことを利用し秘密鍵を攻撃する．

2.2 スキャンベース攻撃に対する防御手法

スキャンベース攻撃に対する防御手法は大きく 2 種類に分けられる．

防御手法 1： 専用のコントローラで制限をかけ，攻撃者にスキャンチェインを利用させない手法．

防御手法 2： スキャンチェインを利用することはできるが，攻撃者には解読できない情報にする手法．

「システムモードからテストモードへ」,「テストモードからシステムモードへ」，モードジャンプが行われるときに回路の安全性が脅かされることになる．そのため防御手法 1 は，専用のコントローラによりモードジャンプを制限することで，スキャンベース攻撃を防御する [2], [4].

文献 [2] では，スキャンチェインの中にスパイスキャン FF(スパイ SFF) を用いて，スキャンチェインがテストモードになったことを自動的に検知することができ，自動的にツールでスパイ SFF を挿入することが可能であるため，導入が簡単である．しかし，検出しかできないため，別に防御手法を考える必要がある．

文献 [4] では，M 個の長さ N の鍵が，決められた N 個の FF に，テストを始める前の間にテストベクタとして入力されたときのみ，スキャンアウトが許可される．キーに用いられる N 個の FF の選択はランダムで，システムデザイン時に決定される．指定された鍵が入力されない限り，スキャンアウトされる値は'0' のみに制限する．つまり，Nbit の鍵が M 回特定の順序で入力されない限りユーザは内部情報を得ることが出来ない．Nbit の鍵を攻撃者が当てる確率は $1/2^N$ で，M 回入力を行うため，最終的な確率は $1/2^{MN}$ である．また，M もしくは N を任意に決めることができるため，安全性を柔軟に選択することが可能である．しかし，入力された鍵を M 回判定するためのコントローラを設計する必要があり，面積オーバーヘッドは大きいものになる．

防御手法 1 は，専用のコントローラが必要になるが，セキュリティは比較的柔軟に設定することができる．しかし，テストコントローラを回路毎に再設計する必要があることや，テストコントローラ自身の面積オーバーヘッドが大きいという欠点がある．

防御手法 2 では，スキャンインとスキャンアウトされるデータを回路設計者にしかわからないようにすることで，攻撃者にとって意味のない情報にする [1], [5], [7].

文献 [1] では，システムモードからテストモードへ，テストモードからシステムモードへモードジャンプを行うことを基本的には全て制限することで秘密情報を保護するが，このままでは本来のテストも行えなくなるため，イネーブルツリーでモードジャンプを許可する例外を用意する．スキャンチェインの中のいくつかのスキャン FF からの出力が，回路設計時に決めたパターンになっているときのみモードジャンプを許可する手法である．しかし，テストコントローラを回路毎に新たに設計しなおす必要があり，面積オーバーヘッドも大きい．

文献 [5] では，全スキャン FF の数の半分インバータをランダムにスキャンチェイン内に挿入することにより，スキャンチェインの構造を複雑にし，スキャンアウトされた値を解読させないようにすることで，秘密情報を保護する．全スキャン FF の数を n とすると，各スキャン FF ごとインバータが挿入される場合と，されない場合の 2 パターンができるため，スキャンチェインのとり得る構造は 2^n パターンになる．つまり，攻撃者がスキャンチェインの構造を当てる確率は $1/2^n$ となり，現実的な時間では解読されないため，安全であると言える．テストコントローラが不必要であるため，面積や回路設計時に掛かるオーバーヘッドはとても小さく，ツールなどで自動的に防御対策を行うことが容易に実現できる．しかし，各ビットごと出力が固定されているという問題がある．インバータを挿入する場所が回路設計時に固定され以後変わることがないため，各ビットごとに考えると，値がそのまま出力されるか反転されて出力されるかのどちらか一方である．文献 [3] の攻撃手法では，スキャンチェイン全体の構造や中間値が保存されているレジスタの一部分の場所さえ特定する必要がなく，スキャンチェイン内のレジスタの 1 ビットのみに着目するため，この問題は致命的である．

文献 [7] では，ミラーキーレジスタを用いて，テストモードのときには秘密情報がスキャンチェインにロードされないように分離し，暗号処理を実行しているデータパスとコントロールパスを独立させることにより，秘密情報を保護する．しかし，保護したい情報の保存される FF の数と同じだけ余分にミラーキーレジスタを追加する必要があるため，面積オーバーヘッドが大きい．

防御手法 2 の特徴はスキャンチェインの出力を回路内部で暗号化するような手法であるため，その情報から解読される可能性はあるが，基本的にテストコントローラは不必要で面積オーバーヘッドが小さい．回路毎に再設計を行うことなくツールなど自動でセキュアスキャンチェインを構築することが可能であり，IP などにも適応しやすい．

3. 提案手法

文献 [5] の手法の各ビットごとに出力が固定されてしまう問題を改良し，文献 [3] の攻撃手法に耐性を持つスキャンアーキテクチャを提案する．文献 [3] の攻撃手法はスキャンチェインの構造が固定されたものである場合に有効であるため，設計した後にもスキャンチェインの構造が動的に変化する手法を提案する．文献 [3] の攻撃手法から防御するため，ラッチを用いて過去の FF の状態を利用し，次のスキャン FF への出力を変化させる状態依存スキャン FF(SDSFF: State-Dependent Scan FF) を提案する．スキャンチェイン内の FF のいくつかを，提案す

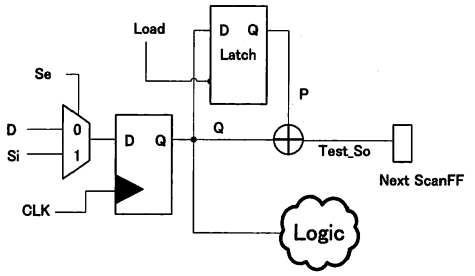

図 3 提案するスキャン FF.

表 1 提案するスキャン FF の出力.

Q の値	P の値	次のスキャン FF への出力
0	0	0
0	1	1
1	0	1
1	1	0

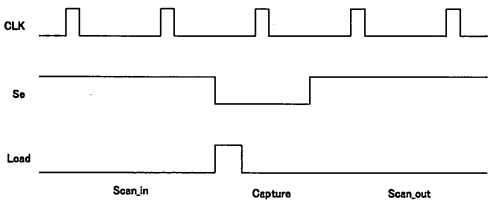

図 4 タイミング.

るスキャン FF に置き換えることにより，スキャンベース攻撃に耐性を持つセキュアスキャンアーキテクチャを構築する．

提案するスキャン FF を図 3 に示す．FF で保存されている値と P を XOR した値が，次のスキャン FF への出力になり，P の値が演算処理中に変わることでスキャンチェインの出力を変化させる．P と Q，次のスキャン FF への出力の関係を表 1 に示す．文献 [3] の攻撃手法で着目するレジスタの値が，P の値により動的に変化するため，攻撃耐性をもつ．

テストモードからシステムモードへモードジャンプが行われるときに Load 信号により P を更新することで，スキャン FF の出力を動的に変化させる．Se 信号とクロック信号，Load 信号の関係を図 4 に示す．Se 信号が '0' のときシステムモード，'1' のときテストモードとする．

Se 信号は '1' の間は，クロックが入力されるごとに 1 つずつスキャンシフトが行われ，データをスキャンチェインに入力している状態である．スキャンインを行った後は，Se 信号を '0' にしシステムモードに移行するが，この際に Load 信号が一度だけ '1' になり，システムモードで処理を行ったときの値がラッチに保存される．次のクロックで FF には実行結果が保存されているので，Se 信号を '1' にし，スキャンチェインのデータを観測する．P の値がテストモードからシステムモードへ移行する際に更新されるため，スキャンチェインの構造が固定されることがない．

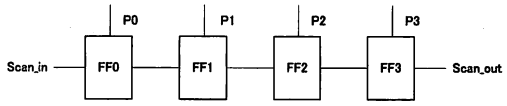

図 5 提案するスキャンアーキテクチャのモデル.

提案するスキャン FF がスキャンチェインに導入されることにより，スキャンチェインの構造が動的に変わり，各 FF の値は毎回違う変化を伴い出力される．テスト設計者は，ラッチに保存されている P の値を知っているため，スキャンアウトされた値を解読することができるが，攻撃者は P の値を知らないため，スキャンアウトで観測された値がどのように変化したものなのか分からず，解読することができない．図 5 の提案手法のモデルを用い，P の値を "0101" とした例を表 2 に示し，ステップごとに解説する．図 5 での FF は全て提案するスキャン FF である．Scan in は次のクロックサイクルでスキャンチェインに入力するデータを示し，Scan out はスキャンチェインから出力されるデータである．

P の値が '1' のとき値が反転するため，表 2 の第 1 クロックサイクルの P の状態の場合，P1 と P3 を通るとき値が変わる．スキャンチェインに入力する値は "$S_0S_1S_2S_3$" であるが，P1 と P3 を通るときに値が反転するため，FF には "$S_0\bar{S}_1S_2S_3$" が保存される．同様に，FF に保存されている値 "$D_0D_1D_2D_3$" をスキャンアウトすると，"$\bar{D}_0\bar{D}_1D_2D_3$" が出力される．第 6 クロックサイクルでは，FF に保存されていた値が次の P の値になり，システムモードで実行された値が FF に保存される．

FF1 を中心に考えると P1 の値は，スキャンアウトの際に FF0 と FF1 の値に影響を与え，スキャンインの際に FF2 と FF3 の値に影響を与える．このように，スキャンインとスキャンアウトを行う際，各 P の値によってデータが変化する．

4. 結　　果

提案手法を AES 暗号回路に実装した．回路の設計にはハードウェア記述言語の一つである Verilog-HDL を使用し，Synopsys 社の Design Compilier Z-2007.03-SP4 を用いて制約なしで論理合成を行った．また，セルライブラリには STARC (注1) (90[nm]) の設計ルールを用いた．

スキャンチェイン内の全スキャン FF の数を n とすると，全てのスキャン FF，$\frac{n}{2}$，$\frac{n}{4}$，$\frac{n}{8}$，$\frac{n}{12}$，$\frac{n}{16}$ の数だけ既存のスキャン FF を提案するスキャン FF に置き換えた場合の面積結果を表 3 に示す．実装した回路において，スキャンチェインにより結ばれたスキャン FF の全数は 716 であるため，順に 716，358，179，90，60，45 となる．提案するスキャン FF へ置き換える数が増えることに面積は単調増加をしていることが示されてい

(注1)：STARC[90nm] ライブラリは東京大学大規模集積システム設計教育研究センターを通し，株式会社半導体理工研究センター (STARC) の協力で開発されたものである．

表 2　図 5 を用いたテストの例.

Clock Cycle		P0	P1	P2	P3	Scan in	FF0	FF1	FF2	FF3	Scan out
1st						S_0	D_3	D_2	D_1	D_0	–
2nd						S_1	S_0	D_3	$\bar{D}_2$	D_1	$\bar{D}_0$
3rd	Scan shift	0	1	0	1	S_2	S_1	S_0	$\bar{D}_3$	$\bar{D}_2$	$\bar{D}_1$
4th						S_3	S_2	S_1	$\bar{S}_0$	$\bar{D}_3$	D_2
5th						–	S_3	S_2	$\bar{S}_1$	$\bar{S}_0$	D_3
6th	Capture	S_3	S_2	$\bar{S}_1$	$\bar{S}_0$	–	D'_3	D'_2	D'_1	D'_0	–

表 3　AES 暗号回路での実装結果.

	No Scan	Normal Scan	文献 [5]	Proposed					
Modified Scan FFs	–	–	358	716	358	179	90	60	45
Area[gates]	19030	19594	19863	22812	21205	20400	19999	19864	19797
Area Overhead[gates]	–	0	269(1.4%)	3218(16%)	1611(8.2%)	806(4.1%)	405(2.1%)	270(1.4%)	203(1.0%)

表 4　文献 [5] との安全性比較.

	文献 [5]	Proposed
既存の攻撃手法に対するとり得るパターン [通り]	2^n	2^n
文献 [3] の攻撃手法に対するとり得るパターン [通り]	×	2^i

る．提案手法は，スキャンパスに挿入するため，クリティカルパスなどに対するタイミングに影響を与えない．そのため，考慮すべきオーバーヘッドは面積である．面積増加として考えられる主要因は，前回の状態を保持するラッチと，次のスキャン FF への出力を変化させる XOR である．

文献 [5] の手法と面積オーバーヘッド，安全性について比較し，評価を行う．提案するスキャン FF へ置き換えた数と文献 [5] では，挿入するインバータの数をもとに比較する．面積オーバーヘッドは，Normal Scan での面積を基準にしている．

提案するスキャン FF へ置き換える数が 60 のとき文献 [5] の手法とほぼ同じ面積になり，それ以降は提案手法の面積が大きくなる．

安全性について比較をしたものを表 4 に示す．提案するスキャン FF の数をランダムに置き換えた場合と，文献 [5] でインバータの数をランダムに挿入した場合のスキャンチェインのとり得るパターンはともに 2^n 通りである．攻撃者がスキャンチェインの構造を特定する確率は $1/2^n$ となり，この確率が既存手法におけるスキャンベース攻撃に対する耐性である．

次に，文献 [3] の攻撃手法に対する防御耐性を評価する．文献 [5] の防御手法では，回路設計時に決められたスキャンチェインの構造から変化することがないため，文献 [3] の攻撃に対する耐性がない．提案するスキャン FF へ置き換えた数を i とすると，提案手法におけるスキャンチェインのとり得るパターンは 2^i 通りであるため，攻撃者がスキャンチェインの構造を特定する確率は $1/2^i$ となる．提案手法では，スキャン FF を置き換えた数だけ攻撃に対する耐性を高めることができるため，回路の用途に応じ，i の数を変更することで安全性を選択することが可能である．

5. むすび

状態依存スキャン FF を用いたセキュアスキャンアーキテクチャを提案した．スキャンベース攻撃はスキャンチェインの構造が動的に変化する場合，攻撃できなくなる点に着目し，ラッチを用いて過去の状態を保存し，その値を利用することでスキャンチェインの構造を動的に変化させる．安全性を評価した上で，AES 暗号回路に実装し有効性を確認した．今後の課題としては，より現実に近い形での検証するため，FPGA に実装し評価することや，自動化ツールへの導入等が考えられる．

文　献

[1] D. Hely, M. L. Flottes, F. Bancel, and B. Rouzeyre, "Test control for secure scan designs," in Proc. European Test Symposium 2005, pp. 190–195, May 2005.

[2] D. Hely, M. L. Flottes, F. Bancel, and B. Rouzeyre, "A secure scan design methodology," in Proc. Design, Automation and Test in Europe 2006, pp. 1–2, March 2006.

[3] 奈良竜太，戸川望，柳澤政生，大附辰夫，"周辺回路を含む AES-LSI へのスキャンベース攻撃，" 信学技報 システム LSI 設計技術研究会 2008, November 2008.

[4] S. Paul, R. S. Chakraborty, and S. bhunia "VIm-Scan: A low overhead scan design approach for protection of secret key in scan-based secure chips," in Proc. VLSI Test Symmposium 2007, pp. 455–460, May 2007.

[5] G. Senger, D. Mukhopadhyay, and D. R. Chowdhury, "Secured flipped scan-chain model for crypto-architecture," in Proc. Computer-Aided Design of Integrated Circuits and Systems, vol. 26, no. 11, pp. 2080–2084, November 2007.

[6] B. Yang, K. Wu, and R. Krri, "Scan based side channel attack on dedicated hardware implementations of data encryption standard," in Proc. International Test Conference 2004, pp. 339–344, 2004.

[7] B. Yang, K. Wu, and R. Krri, "Secure scan: A design-for-test architecture for crypto chips," in Proc. Design Automation Conference 2005, pp. 135–140, June 2005.