様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２４年　５月１５日現在

機関番号：３２６８９
研究種目：基盤研究（C）
研究期間：2009～2011
課題番号：21560370
研究課題名（和文）　暗号処理向け組み込みＬＳＩとそのテスト設計環境の構築

研究課題名（英文）　Design Methods for Crypto LSI Implementations and Testing

研究代表者
柳澤　政生（ YANAGISAWA　MASAO ）
早稲田大学・理工学術院・教授
研究者番号：30170781

研究成果の概要（和文）：通信ネットワークの普及やディジタル回路技術の発達に伴って，情報の安全性確保や不正処理の防止のために暗号処理 LSI が使われている．通常，LSI では製造時の検査や動作テストを行うために，スキャンチェインと呼ばれるテスト用回路と信号線が用意されるが,暗号回路ではこれが不正な情報取得の糸口となる可能性がある.そこで本研究では，テスト目的での利用を可能としながら内部情報の解析を防ぐ SD-SFF (State Dependent Scan Flip Flop: 状態依存スキャンフリップフロップ) という機構を提案する．この提案テスト回路を利用することで，製造時のコスト増加を抑えながら機密性の高い暗号通信を可能とする．

研究成果の概要（英文）：Scan test has been widely adopted as a default testing technique among most LSI designs, including crypto cores.　However, these scan chains might be used as a ``side channel" to recover the secret keys from the hardware implementations of cryptographic algorithms.　In this research, we propose SD-SFF (State Dependent Scan Flip Flop) which significantly improves the security with ignorable design requirements for crypto hardware implementations.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００９年度	1,400,000	420,000	1,820,000
２０１０年度	1,000,000	300,000	1,300,000
２０１１年度	1,200,000	360,000	1,560,000
年度			
年度			
総　計	3,600,000	1,080,000	4,680,000

研究分野：工学
科研費の分科・細目：電気電子工学、電子デバイス・電子機器
キーワード：ＬＳＩ設計、テスト容易化設計，スキャンチェイン，暗号処理ＬＳＩ，スキャンベース攻撃，SD-SFF

１．研究開始当初の背景

研究開発当初では，インターネットが普及し，インターネットを通じて，クレジットカードの番号など重要な情報をやり取りすることが多かった．インターネットでは，盗聴や改ざんなどデータが危険にさらされるため，情報セキュリティは非常に重要である．

情報セキュリティの一つとして，データの暗号化技術が考えられる．データを暗号化して送受信するため，第３者にデータを盗聴されたとしても，情報の漏洩を防ぐことができる．そのような情報セキュリティへの意識の高まりから，暗号処理 LSI が重要性を増している．ルーターなどのネットワーク機器では

暗号回路を搭載することでセキュリティを高めており，また近年数多く発行されているICカードにおいても,暗号化してデータを送受信するため暗号回路を実装しているものが多い.

一方で,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，製造コストを抑えるためには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フリップフロップ(FF, 記憶素子)を全て結線し（図１参照），必要に応じてその状態を操作・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．回路を内部から直接制御できるため非常に強力なテスト手法であり，製品として出回っているLSIのほぼ全てにおいて利用されている.

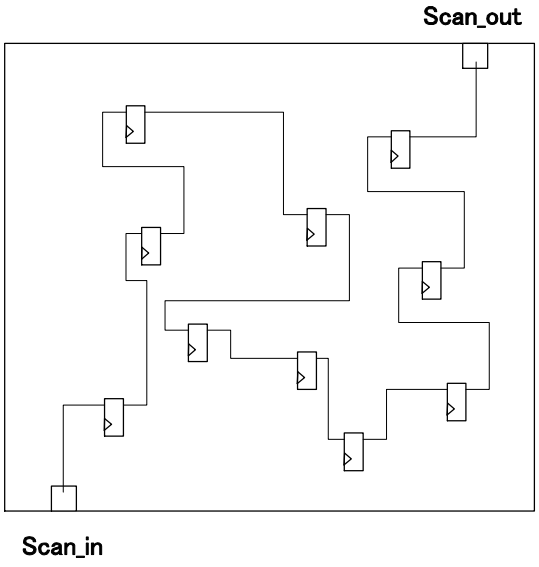

図１　スキャンチェイン

暗号回路においてもこのスキャンチェイン方式は用いられているが，スキャンチェインは回路内の情報に直接アクセスする事が出来るため，暗号回路の場合，内部の秘密情報が漏洩する可能性がある．本研究ではこのスキャンチェインの弱点を克服することを目的としている．スキャンチェイン内に図２のような回路をランダムに挿入することで,その挿入位置を知っている者にしかスキャンチェインを利用不可能にし，暗号回路の安全性を高めることができる.

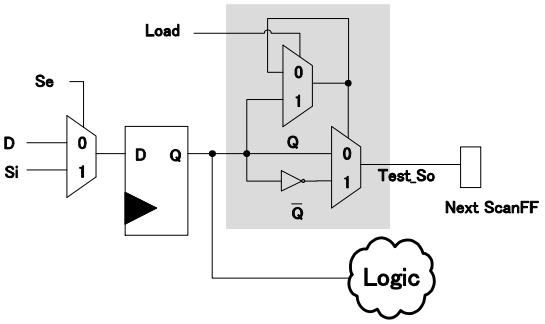

図２　提案手法（SD-SFF）

２．研究の目的

広帯域な通信ネットワークの普及やディジタル回路技術の発達に伴って，情報の安全性確保や不正処理の防止のためにあらゆる場所で暗号処理 LSI が使われている．通常，LSI では製造時の検査や動作テストを行うために，スキャンチェインと呼ばれるテスト用回路と信号線が用意されるが，暗号回路ではこれが不正な情報取得の糸口となってしまう可能性が指摘されている．そこで本研究では，テスト目的での利用を可能としながら内部情報の解析を防ぐ図２の SD-SFF (State Dependent Scan Flip Flop: 状態依存スキャンフリップフロップ) という機構を提案する．この提案テスト回路を利用することで，製造時のコスト増加を抑えながらより機密性の高い暗号通信を行うことができる.

提案するテスト用回路とそれを用いたテスト方式について，実装・シミュレーションを行うことでコストと効果について定量的に評価を行う．明らかにするのは，提案するテスト用回路を用いることによる(1) 回路面積の増加量，(2) 内部情報漏洩率の低下量と(3) 提案回路を用いたテスト方式の 3 点である.

まず，提案手法ではスキャンチェインに図２の回路を組み込むため，回路面積の増加が予想される．これについて評価を行うため，AES, DES, RSA など複数の暗号回路を対象として提案回路を組み込んだ回路を EDA ツールを用いて設計・実装し，これによる面積増加量について評価を行う.

次に，提案手法の効果については，先に実装した暗号回路と通常の暗号回路に対してそれぞれシミュレーション上で複数の方法を用いて秘密情報の取得を試みる実験を行い，提案回路を用いることで攻撃に対する耐性が何%上昇するかを測定する.

最後に，この実装結果を元に提案回路をもちいた場合のスキャンテスト方式について具体的な手順を検討する．通常のスキャンチェインと比較してテストパターンの生成方

法が複雑になることが予想されるため，テストパターンの自動生成アルゴリズムについて提案を行い，これによるテスト時間・テスト精度への影響についてシミュレーションによる評価を行う．

３．研究の方法

提案回路を暗号処理 LSI 上に実装して評価することと，これを用いたテスト方式について考察することを平行して進める．前者では既存のルータ・IC カード等で利用されている暗号処理 LSI について広く調査を行い，攻撃（内部情報の不正な取得を試みること）方法について調査及び提案を行う．さまざまな暗号処理 LSI について攻撃シミュレーションを行うことで提案手法の有効性を検証する．また，テスト方式については既存のスキャンテスト方式をもとに変更を行う．より安全性の高い暗号処理 LSI を実現するという観点から，テストの容易性や故障検出率の高さだけではなく，安全性に対する評価を並行して行う．

具体的な方法は以下の通りである．

(1) スキャンチェインを用いた暗号処理 LSI への攻撃方法についての調査・分析

スキャンチェインを用いた攻撃方法については既にいくつかの提案がなされている．後に提案手法の性能評価で用いるため，これについて調査を行う．加えて，新しい攻撃方法についても考案し，提案を行っていく．

(2)LSI 製造で用いられているテスト方式についての調査・分析

既存のスキャンチェイン以外のテスト方式についてもその精度・コストを調査し分析を行う．この結果を用いて，後に提案 SD-SFF を用いた際のテスト方式を評価する．

(3) 暗号処理 LSI への SD-SFF の実装

AES，DES，RSA など広く利用されている暗号処理について，既存の暗号処理 LSI について調査を行い，それらに対して提案する SD-SFF を組み込んで実装を行う．この際に，面積や消費電力の増加など，提案手法を適用したことで起こったコスト増加についての見積もりを行う．また，回路規模やアルゴリズムとコスト増加の間に一定の関連性があればそれを洗い出し，コストの事前見積もりを可能にする．

(4) シミュレーションによる SD-SFF の性能評価

提案手法を実装した暗号処理 LSI に対して，(1)で収集した攻撃手法を用いた攻撃シミュレーションを行い，SD-SFF を挿入していないものと比較して攻撃への耐性がどれだけ向上したか測定する．また，SD-SFF の挿入数と耐性の間の関連性についても調査する．

(5) システムボードの設計，製作

暗号処理マルティメディア処理 LSI を搭載するシステムボードを設計，製作する．製作したボード上で各機能の動作確認を行い，実記上で実際にテスト作業・攻撃実験を試行することでシミュレーション結果の検証を行う．

４．研究成果

スキャンチェインを用いた暗号処理 LSI への攻撃方法についての調査・分析を行い、各種暗号方式対する攻撃手法を提案するとともに、安全にスキャンテストを行うために SF-SFF を用いた対策手法に関して研究した。

(1) 共通鍵暗号方式 AES、公開鍵暗号方式の一種である楕円曲線暗号に対するスキャンチェインを用いた鍵解読手法を提案した。前者における提案手法は、従来手法では不可能であった暗号処理回路以外の回路がスキャンチェインに含まれている場合でも鍵を解読することができ、さらに解析に必要な入力数を約 42%に削減することに成功した。後者において、163 ビットの鍵長を持つ楕円曲線暗号処理回路の秘密鍵を平均 29 個の入力から取得したスキャンデータを解析するだけで実現できることを示した。公開鍵暗号方式に対するスキャンチェインを利用した鍵解読攻撃は世界初である。

(2) (1)の結果から、提案したスキャンチェインを用いた鍵解読手法を効率的に防ぐことを目的とした SD-SFF の研究・実装、およびシミュレーションによる SD-SFF の評価を行った。スキャンチェインを構成するレジスタの間に SD-SFF を挿入することで、スキャンデータを動的に反転・非反転させ、スキャンデータを解析されることを防ぐことができる。従来の防御手法と異なり、攻撃手法を効率的に防ぐことができるため、従来手法よりも面積を縮小できることを確認した。

(3) サイドチャネル攻撃用標準評価基板である SASEBO-GII を使用したスキャンベース攻撃の実機実験に関する研究を主として行ったことに特徴がある。SASEBO-GII の FPGA に AES 暗号回路とテスト用のロジック解析回路を組み込み、暗号処理中の内部信号を取得・解析することで、FPGA に実装された暗号回路の秘密鍵を復元できることを示した。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 4 件）

① Youhua Shi, Nozomu Togawa, Masao Yanagisawa, and Tatsuo Ohtsuki, ``Rubust Secure Scan Design against Scan-Based Differential Cryptanalysis,” IEEE Trans. on Very Large Scale Integration (VLSI) Systems, 査読有り，vol. 20, no.1, 2012 年 1 月，

pp. 176-181
DOI: 10.1109/TVLSI

② Ryuta Nara, Nozomu Togawa, Masao Yanagisawa and Tatsuo Ohtsuki, ``Scan vulnerability in elliptic curve cryptosystems,'' IPSJ Trans. on System LSI Design Methodology, 査読有, vol.4, 2011 年 2 月, pp.47-59
https://www.jstage.jst.go.jp/article/ipsjtsldm/4/0/4_0_47/_article

③ Ryuta Nara, Kei Satoh, Masao Yanagisawa, Tatsuo Ohtsuki, and Nozomu Togawa, ``Scan-based side-channel attack against RSA cryptosystems using scan signatures,'' IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences, 査読有, vol. E93-A, no.12, 2010 年 12 月, pp. 2481-2489
http://search.ieice.org/bin/summary.php?id=e93-a_12_2481&category=A&year=2010&lang=E&abst=

④ Ryuta Nara, Nozomu Togawa, Masao Yanagisawa, and T. Ohtsuki, ``A Scan-Based Attack Based on Discriminators for AES Cryptosystems,'' IEICE Trans. Fundamentals, 査読有, vol. E92-A, no. 12, 2009, pp. 3229-3237
http://search.ieice.org/bin/summary.php?id=e92-a_12_3229&category=A&year=2009&lang=E&abst=

〔学会発表〕(計 10 件)

① 小寺博和、柳澤政生、戸川望, ``スキャンシグネチャを利用した Triple DES に対するスキャンベース攻撃の実装実験,'' 暗号と情報セキュリティシンポジウム (SCIS) 2012, 2012 年 2 月 1 日, 金沢

② 小寺博和、柳澤政生、戸川望, ``スキャンシグネチャを用いた Triple DES に対するスキャンベース攻撃手法,'' 電子情報通信学会システム LSI 設計技術研究会, 2011 年 11 月 28 日, 宮崎

③ 小寺博和、柳澤政生、戸川望, ``スキャンチェイン構造に依存しない DES に対するスキャンベース攻撃,'' 情報処理学会システム LSI 設計技術研究会, 2011 年 10 月 25 日, 仙台

④ 奈良竜太、柳澤政生、大附辰夫、戸川望, ``SASEBO-GII を使用した AES に対するスキャンベース攻撃の実装実験,'' 2011 年暗号と情報セキュリティシンポジウム (SCIS2011), 2011 年 1 月 25 日, 小倉

⑤ 奈良竜太、戸川望、柳澤政生、大附辰夫, ``RSA 暗号に対するスキャンベース攻撃の評価実験,'' 電子情報通信学会 2010 ソサイエティ大会, 2010 年 9 月 14-17 日, 大阪

⑥ Youhua Shi, Nozomu Togawa, Masao Yanagisawa and Tatsuo Ohtsuki, ``Constant-scan-based attack and its countermeasure for crypto hardware implementations,'' 情報処理学会 DA シンポジウム 2010, 2010 年 9 月 2-3 日, 愛知県豊橋市

⑦ Ryuta Nara, Hiroshi Atobe, Youhua Shi, Nozomu Togawa, Masao Yanagisawa and Tatsuo Ohtsuki, ``State-dependent Changeable Scan Architecture against Scan-based Side Channel Attacks,'' IEEE ISCAS 2010, 2010 年 5 月-6 月, Paris, France

⑧ 奈良竜太、佐藤圭、戸川望、柳澤政生、大附辰夫, ``RSA 暗号に対するスキャンベース攻撃,'' 第 23 回 回路とシステム軽井沢ワークショップ, 2010 年 4 月 19-20 日, 軽井沢

⑨ Ryuta Nara, Nozomu Togawa, Masao Yanagisawa, and T. Ohtsuki, ``Scan-Based Attack against Elliptic Curve Cryptosystems,'' IEEE 15th Asia and South Pacific Design Automation Conference (ASP-DAC 2010), 2010 年 1 月 20 日, 台湾 台北

⑩ 奈良竜太, 戸川 望, 柳澤政生, 大附辰夫, ``楕円曲線暗号に対するスキャンベース攻撃,'' 情報処理学会 DA シンポジウム 2009, 2009 年 8 月 26 日, 石川県

６．研究組織

(1)研究代表者
柳澤 政生 (YANAGISAWA MASAO)
早稲田大学・理工学術院・教授
研究者番号：30170781

(3)連携研究者
奈良 竜太 (NARA RYUTA)
早稲田大学・理工学術院・助手
研究者番号：30547047
史 又華 (SHI YOUHUA)
早稲田大学・理工学術院・助教
研究者番号：70409655