様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２７ 年　 ６ 月 １６ 日現在

機関番号：３２６８９
研究種目：基盤研究(C)
研究期間：2012～2014
課題番号：２４５６０４２１

研究課題名（和文）故障利用攻撃を検出できる耐タンパー暗号回路設計に関する研究

研究課題名（英文）Cryptosystem design which detects side-channel attacks

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

交付決定額（研究期間全体）：（直接経費）　　4,200,000円

研究成果の概要（和文）：近年、情報技術の進歩から暗号回路中の秘密鍵を解読する攻撃の成功により、暗号LSI回路に保存される機密情報の窃取など脅威が高まっている。暗号回路では、本来の暗号化・復号化機能に加えて、内部の秘密情報の不正読出しや機能の改変を防止する耐タンパー設計技術が求められている。そこで本研究では、近年提案された故障利用攻撃のメカニズムを解明し、このような攻撃を自動検出できる暗号LSI回路設計技術を確立した。この提案技術を利用することで、既存研究と比較して面積オーバーヘッドを削減し、かつ故障利用攻撃に対する耐性を高める。

研究成果の概要（英文）：As LSI technologies have advanced, design-for-test techniques have become essential to LSI designers. Particularly, scan-path test using scan chains, one of design-for-test techniques, makes test design much easier. A scan chain connects flip-flops in an LSI in series and enables LSI designers to set and observe these flip-flops easily. There are numerous researches on side-channel attacks utilizing information exploited from the physical implementation of a cryptosystem, for example, power consumption and timing information. A scan-based side-channel attack retrieves the secret information by utilizing scan chains. In this attack, the secret information inside the cryptosystem is
retrieved by analyzing scanned data obtained from its scan chain scheme during cryptographic processing. We demonstrate that the secret key can be retrieved successfully from the SASEBO-GII, side-channel attack standard evaluation board.

研究分野：工学

キーワード：暗号回路　ＬＳＩ設計　故障利用攻撃　耐タンパ性

１．研究開始当初の背景

情報セキュリティ技術は、情報化社会を支える重要な技術であり、中でも暗号技術は最も重要な基盤技術の一つである。90 年代後半から、暗号アルゴリズムが実装された暗号回路に対する物理的な様々な攻撃法（内部情報の不正な取得を試みること）が提案され、情報セキュリティに対する新たな脅威となってきた。特に、暗号回路の処理時間や消費電力といったいわゆるサイドチャネル情報を解析する“サイドチャネル攻撃”と呼ばれる攻撃法は、強力な攻撃法として注目されている。したがって、暗号回路には数学的な安全性だけでなく、実装面での安全性（耐タンパー性）も求められる。安全な実装を実現するためには、高度な耐タンパー評価・対策技術が不可欠である。

故障利用攻撃手法は、サイドチャネル攻撃の一つであり、一般的には外部からの異常な電力供給や強力なレーザ光を照射することにより、意図的にエラーを発生させて、それを基に鍵などの解読の手掛かりを得る攻撃方法である。故障利用攻撃に関する研究（攻撃の一例を図１に示す）は、90 年代後半に始まってから、多くの研究者によって絶えずに続けられている。たとえば、古いものでは文献[1]、新しいのものでは文献[2]などがある。

そこで、故障利用攻撃に対する耐性を持つ暗号 LSI 回路設計の要求が高まっている。このような故障利用攻撃の対策手法は、国内外でいくつか見られ、例えば文献[3]や[4]などがある(図２参照)。しかし、これらの研究はいずれも、回路動作中にフォールトを自動検出するため、回路面積オーバーヘッドが増大し、かつ、フォールト検出率が良くならないという本質的な問題点がある。

本研究課題に関連して、申請者は自らの研究（下記の業績を参照）によって、「スキャンベースサイドチャネル攻撃」、「耐タンパー設計・テスト技術」及びそれらを実現させる「LSI 暗号回路設計」の 3 つのテーマについて研究開発を行ってきた。ここまでの研究成果はすでに、原著論文として LSI 設計技術関連の論文誌で最も権威が高い TVLSI（IEEE Transactions on Very Large Scale Integration Systems）と TCAD (IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems) にて掲載されるなど国内外で極めて高く評価さ

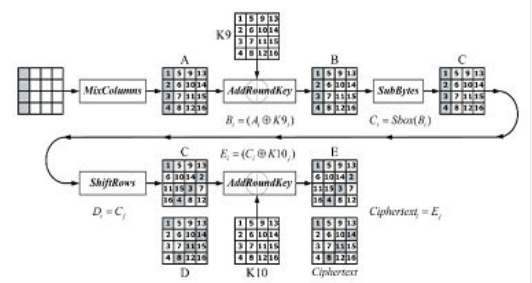
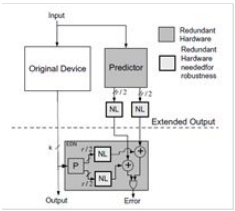
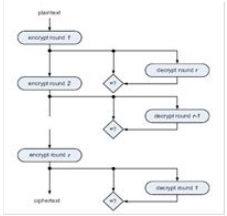


図１．暗号回路への故障利用攻撃の一例

れている。また、国内外を問わず、これまで故障利用攻撃を自動検出できる暗号 LSI 回路設計技術に関する報告は極めて少なく、その意味において、本研究は、先駆的な研究であると考えられる。





(a) Fault-tolerant architecture [3]
(b) Enc/Dec-based Concurrent Fault Detection [4]

図２．既存のフォールト検出 AES 設計

２．研究の目的

近年、情報技術の進歩から暗号回路中の秘密鍵を解読する攻撃の成功により、暗号 LSI 回路に保存される機密情報の窃取など脅威が高まっている。暗号回路では、本来の暗号化・復号化機能に加えて、内部の秘密情報の不正読出しや機能の改変を防止する耐タンパー設計技術が求められている。そこで本研究では、近年提案された故障利用攻撃のメカニズムを解明し、このような攻撃を自動検出できる暗号 LSI 回路設計技術を確立することを目的とする。この提案技術を利用することで、既存研究と比較して面積オーバーヘッドを削減し、かつ故障利用攻撃に対する耐性を高めることを目標とする。

３．研究の方法

最初の年度は、主に暗号回路における故障利用攻撃のメカニズムについての考察、ならびに、DPA 対策を施した暗号回路と未対策の回路の故障利用攻撃の耐性についての考察を行う。前者では既存の故障利用攻撃手法について広く調査を行い、解析方法について調査及び提案を行う。後者では、さまざまな暗号処理 LSI 回路について攻撃シミュレーションを行うことで故障利用攻撃の耐性を考察する。また、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、DPA 対策を施した暗号回路と未対策の暗号回路における故障利用攻撃に対する安全性の評価を行う。具体的な方法は以下の通りである。

(1) 暗号回路における故障利用攻撃のメカニズムの考察

故障利用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。まず、既存の故障利用攻撃手法について広く調査を行い、解析方法について調査を行う。加えて、新しい故障利用攻撃方法についても考案し、提案を行っていく。

(2) 暗号 LSI 回路における故障利用攻撃の耐性の考察・評価

さまざまな共通鍵ブロック暗号回路にお

ける攻撃シミュレーションを行うことで故障利用攻撃の耐性を考察する。また、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、DPA 対策を施した暗号回路と未対策の回路の故障利用攻撃に対する安全性の評価を行う。

本研究では、共通鍵ブロック暗号回路は 128/192/256 bit 鍵の AES を対象とする。AES 回路の実装方法としては、①S-box を 1 段の PPRM 論理で実装した AES、②LUT をベースにした AES、③合成体による S-box を用いた AES、④合成体による S-box をベースにして DPA 対策である WDDL を施した AES、⑤Dual Sbox を用いた AES および⑥Parity ベースにした AES の全 6 種類の AES の実装方法を対象として、故障利用攻撃を行い、各実装方法における故障利用攻撃に対する安全性の評価を行う。

(3) 故障利用攻撃対策手法の検討

上記の考察・評価の結果により、AES 暗号回路における故障利用攻撃対策手法を検討する。

2 年目以降では、「故障利用攻撃を自動検出できる暗号 LSI 回路設計手法」、並びに「サイドチャネル攻撃用標準評価ボード（SASEBO）上で提案手法を実装・評価」に関する研究を取り組む。具体的は、以下の手順で研究を遂行する。

(4) 故障利用攻撃を自動検出できる暗号 LSI 回路設計

AES の処理では、SubBytes, ShiftRows, MixColumns, AddRoundKey の各操作を順に行い、これを 1 ラウンドとする。そのうち、SubBytes とは非線形の bit 転置であり、各 Byte 単位で bit 転置が行なわれる。他の三つの操作が線形である。線形の部分では Parity check でフォールト検出ができる。非線形の部分では、冗余ロジックを用いて故障を検出できる。そこで、本研究では、AES の処理を線形と非線形の部分を分けて、それぞれでフォールト検出処理を行い、故障利用攻撃を自動検出できる暗号 LSI 回路の設計を提案する。(2)で述べた 6 種類の AES 実装方法に対して提案する故障利用攻撃自動検出回路を組み込んで実装を行う。

(5) シミュレーションによる提案手法の性能評価

提案手法を実装した暗号処理 LSI に対して、(1)で調査した故障利用攻撃手法を用いた攻撃シミュレーションを行い、提案手法と対策のないものの故障利用攻撃への耐性を比較する。

(6) サイドチャネル攻撃用標準評価ボード（SASEBO）上で提案手法の実装・評価

サイドチャネル攻撃用標準評価ボード（SASEBO）を利用し、実ボード上で提案手法を実装し、電源電圧・クロック周波数を変更することにより故障利用攻撃を行い、提案手法の有効性・コストを評価する。

(7) 故障利用攻撃を自動修正できる暗号 LSI 回路設計の検討

暗号処理中、故障利用攻撃を自動検出できるだけではなく、フォールト検出した場合には、Single Error を修正できる回路の設計に関する研究も検討する。

４．研究成果

初年度は、まず、暗号回路における故障利用攻撃のメカニズムについての考察、ならびに、DPA 対策を施した暗号回路と未対策の回路の故障利用攻撃の耐性についての考察を行った。前者では既存の故障利用攻撃手法について広く調査を行い、解析方法について調査および考察を行った。後者では、さまざまな暗号処理 LSI 回路について攻撃シミュレーションを行うことで故障利用攻撃の耐性を考察した。また、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、DPA 対策を施した暗号回路と未対策の暗号回路における故障利用攻撃に対する安全性の評価を行った。具体的な成果のうち、主な成果を以下に示す。

攻撃手法として、Camellia 暗号回路に対するスキャンベース攻撃手法を提案した。Camellia は共通ブロック暗号であり、AES よりも高い暗号攻撃耐性を持ち、AES と同等の処理性能を持つ暗号アルゴリズムである。提案手法では、複数の平文を LSI に入力したときに取得したスキャンデータのある 1 ビットの列データに着目することで、Camellia の等価鍵を解読し、秘密鍵を復元できることを示した。また、スキャンチェインのレジスタ長を 1024 ビットとした場合でも、30 個の平文を用いることで秘密鍵を解読できることを示した。

故障利用攻撃の耐性に関して、鍵ベース構成の State Dependent Scan Flip Flop を用いた暗号回路へのセキュアスキャンアーキテクチャを提案した。提案手法では、従来手法と比べ、オンラインテストが可能になることで、テスト容易性が向上する一方で、スキャンベース攻撃に対する安全性は維持している。実験結果により、提案手法は様々な暗号回路において有効性があることを示した。また、クロックグリッチを利用した故障攻撃に対するカウンタ用いた耐タンパ AES 暗号回路を提案した。

2 年度目における具体的な成果のうち、主な成果を以下に示す。

“Scan-based Attack against DES and Triple DES Cryptosystems Using Scan Signatures”では、共通鍵暗号 DES ならびに Triple DES に対するスキャンシグネチャを用いたスキャンベース攻撃手法を提案した。提案手法では、暗号 LSI に複数の平文を入力したときのスキャンデータの特定ビット列に着目し、対応するレジスタの変化を観察することで秘密鍵を解読する。提案手法では、多くても 43 個の平文で秘密鍵を解読するという結果が得られた。

“Scan-based Attack against Trivium Stream Cipher Independent of Scan Structure”では、スキャンチェインの構造に依存しないTriviumへのスキャンベース攻撃手法を提案した。提案手法では、1ビットレジスタ値の入力・動作サイクル数に対する変化がそのレジスタ固有の値になることを利用し、スキャンチェインの構造を求める。計算機実験の結果、高々1個の入力ペア、13サイクルでTriviumの内部状態を復元でき、元の平文を復元することができた。

“Secure Scan Design with Dynamically Configurable Connection”では、安全性とテスト容易性を両立するセキュアスキャン・アーキテクチャを提案した。提案手法では、スキャンチェインをサブチェインに分割し、サブチェイン毎に接続順を仮想的に動的に変化させる。攻撃者はサブチャインの接続順の予測が困難であるが、テスト者は接続順を予測、操作可能であることで、安全性とテスト容易性を両立させる。AES暗号回路に提案手法を実装した結果、面積オーバーヘッドが0.5%と微小なことを示した。

最終年度における具体的な成果のうち、主な成果を以下に示す。

スマートカード等において利用される軽量ブロック暗号にLED暗号があり、LED暗号へのスキャンベース攻撃が報告されている。しかし、この手法ではLED暗号の鍵長を64ビットとしており、他の鍵長を考慮していないため、他の鍵長の場合、秘密鍵を解読できないという問題点がある。本研究では、LED暗号の鍵長が64ビットより大きい場合のスキャンベース攻撃手法を提案した。計算機実験により、暗号回路のみをスキャンチェインに含む場合、提案手法を用いて、平均145個の平文で128ビットの秘密鍵を復元可能であることがわかり、その有効性を示した。

また、サイドチャネル攻撃用標準評価ボード（SASEBO-GII）上にLED暗号回路ならびに提案手法を実装した結果、16×16の平文を入力に対して、すべてのスキャンデータを9.48秒で得られることを示した、また、提案手法により、0.218秒で64ビットの秘密鍵を解読できることを示した。

近年、暗号回路への攻撃手法として、故障解析が脅威となっている。回路への故障の発生方法には、レーザー照射やで電圧変動、クロックグリッチなどの方法があるが、実装や制御の容易性から、クロックグリッチが注目されている。対策手法として、回路を三重化して比較する空間冗長化手法や、同じ処理を2回行って比較する時間冗長化手法が存在する。しかし、これらの手法は面積オーバーヘッド、あるいは、時間オーバーヘッドが大きいという問題点がある。本研究では、故障解析の誘因となるクロックグリッチを高速に自動検出可能で、かつ、面積オーバーヘッドを4.9%に抑えたAES暗号回路を提案した。

＜引用文献＞

[1] P. Dusart, G. Letourneux, and O. Vivolo, “Differential Fault Analysis on AES,” Proc. Int’l Conf. Applied Cryptography and Network Security (ACNS ’03), pp. 293-306, Oct. 2003.

[2] P. Derbez, P. Fouque and D. Leresteux, “Meet-in-the-Middle and Impossible Differential Fault Analysis on AES,” Cryptographic Hardware and Embedded Systems (CHES ’11), Springer Lecture Notes in Computer Science, Vol. 6917, pp.274-291, Sep. 2011.

[3] K. Kulikowski, M. Karpovsky, E. Taubin, "Robust Codes and Robust, Fault Tolerant Architectures of the Advanced Encryption Standard," Journal of Systems Architecture, Vol. 53, No. 2, pp. 139-149, Feb. 2007

[4] T. Malkin, F. Standaert, M. Yung, “A Comparative Cost/Security Analysis of Fault Attack Countermeasures,” Springer Lecture Notes in Computer Science, Vol. 4236, pp. 159-172, Sep. 2006.

５．主な発表論文等

〔雑誌論文〕（計 4件）

① Mika Fujishiro, Masao Yanagisawa, and Nozomu Togawa, “Scan-based side-channel attack on the LED block cipher using scan signatures,” IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences, 査読有, vol. E97-A, no. 12, 2014, pp. 2434-2442
DOI: 10.1587/transfun.E97.A.2434

② Mika Fujishiro, Masao Yanagisawa, and Nozomu Togawa, “Scan-based attack against trivium stream cipher using scan signatures,” IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences, 査読有, vol. E97-A, no. 7, 2014, pp. 1444-1451
DOI: 10.1587/transfun.E97.A.1444

③ Hirokazu Kodera, Masao Yanagisawa, and Nozomu Togawa, “Scan-based Attack against DES and Triple DES Cryptosystems Using Scan Signatures,” IPSJ Journal of Information Processing, 査読有, vol. 21, no. 3, 2013, pp.572-579
DOI: 10.2197/ipsjjip.21.572

④ Youhua Shi, Nozomu Togawa, and Masao Yanagisawa, “Scan-Based Attack on AES through Round Registers and Its Countermeasure,” IEICE Transactions on Fundamentals, 査読有, vol. 95-A, no. 12, 2012, pp. 2338-2346
10.1587/transfun.E95.A.2338

〔学会発表〕（計　7 件）

① Huiqian Jiang, Mika Fujishiro, Masao Yanagisawa, and Nozumu Togawa, “Scan-Based Side-Channel Attack Implementation Evaluation on the LED cipher using SASEBO-GII,” SASIMI2015, March 17, 2015, Yilan, Taiwan

② Huiqian Jiang, Mika Fujishiro, Hirokazu Kodera, Masao Yanagisawa, and Nozomu Togawa, “Scan-Based Side-Channel Attack on Camellia Cipher Using Scan Signatures,” Asia Pacific Conference on Circuits and Systems (APCCAS 2014), November 19, 2014, Ishigaki, Japan

③ Yuta Atobe, Youhua Shi, Masao Yanagisawa, and Nozomu Togawa, “Secure Scan Design with Dynamically Configuravle Connection,” Proc. 2013 IEEE 19th Pacific Rim International Symposium on Dependable Computing, Dec. 2-4, 2013, Vancouver, Canada

④ Mika Fujishiro, Masao Yanagisawa, and Nozomu Togawa, “Scan-based Attack against Trivium Stream Cipher Independent of Scan Structure,” ASICON 2013, Oct. 28-31, 2013, Shenzhen, China

⑤ Yuta Atobe, Youhua Shi, Masao Yanagisawa, and Nozomu Togawa, “State Dependent Scan Flip-Flop with Key-Based Configuration against Scan-Based Side Channel Attack on RSA Circuit,” 2012 IEEE Asia Pacific Conference on Circuits and Systems (2012 APCCAS), Dec. 5, 2012, Kaohsiung, Taiwan

⑥ Hirokazu Kodera, Masao Yanagisawa, and Nozomu Togawa, “Scan-Based Attack Against DES Cryptosystems Using Scan Signatures,” 2012 IEEE Asia Pacific Conference on Circuits and Systems (2012 APCCAS), Dec. 5, 2012, Kaohsiung, Taiwan

⑦ Yuta Atobe, Youhua Shi, Masao Yanagisawa, and Nozomu Togawa, “Dynamically Changeable Secure Scan Architecture against Scan-Based Side Channel Attack,” 2012 International SoC Design Conference (ISOCC 2012), Nov. 6, 2012, Jeju, Korea

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