早稲田大学大学院 基幹理工学研究科

博 士 論 文 概 要

論 文 題 目

暗号集積回路に対するスキャンベース
サイドチャネル攻撃に関する研究
Scan-based side-channel attacks on
cryptographic integrated circuits
using scan signatures

申 請 者

藤代	美佳
Mika	FUJISHIRO

情報理工・情報通信専攻 情報システム設計研究

2015 年 12 月

近年ではICTの発展によりあらゆる情報をデータとして扱うようになり，扱う情報の価値は大きくなっている．情報の改ざん，漏洩が多発する中，想定される攻撃対象は金銭や個人情報から社会インフラまで及び，人身や国家の安全性をも揺るがす事態になっている．そのため多種多様な攻撃を想定したセキュアなシステムの構築が必要である．Suicaやクレジットカード等のスマートカードは，交通，金融，行政等多くの分野において日常的によく使われている．また2016年1月にはマイナンバーカードの導入が決定している.これらスマートカードに対し，ハードウェアの特性を利用したサイドチャネル攻撃の危険性が指摘されている．今日では情報を確実に保護するためには暗号技術だけでなくハードウェアの特性も考慮しなければならない．スマートカードは価値・機密性が高い情報を扱うため，機密情報を確実に保護する安全な暗号集積回路の設計が求められており，暗号技術とハードウェアの特性のセキュリティの研究は必須である．

安全な暗号集積回路を設計するためには,回路の脆弱性を解明する必要がある．これまでに暗号集積回路に対する多様な攻撃が検討されており，テスト用のスキャンチェインを利用したスキャンベース攻撃の危険性が指摘されている．スキャンチェインはLSI中のレジスタを直列に接続し，外部からレジスタを直接制御・観測可能にしたテスト技術である．スキャンチェインから取得したレジスタの値をスキャンデータといい，スキャンデータ上の値と実際のレジスタとの対応関係は設計者以外には分からない．スキャンベース攻撃では，スキャンデータとレジスタの対応関係を求めることが最大の鍵となる．スキャンベース攻撃における従来手法はスキャンチェインに接続されたレジスタが特定の構成になっていることを前提としている場合が多い．しかし，通常LSI上のスキャンチェインは様々な回路のレジスタを接続している．このように攻撃手法が特定の条件下でのみ有効であっても，スキャンベース攻撃の危険性を完全には指摘しきれていない．脆弱性を解明するためには，攻撃手法が有効になる条件を限定せず，現実的な条件を設定した上で攻撃手法を検討すべきである．

本論文では暗号集積回路のセキュア設計を目的としている．安全な暗号集積回路は,「強固な暗号アルゴリズム」を「情報を漏えいしない適切な仕組みで実装」していることが求められるため,「暗号アルゴリズム」の数理的な性質・脆弱性と「実装法」における脆弱性を評価する．ストリーム暗号，ブロック暗号アルゴリズムを実装した暗号集積回路に対してスキャンチェインの構造に依存しないスキャンベース攻撃手法を提案することで，暗号集積回路の「暗号アルゴリズム」における脆弱性,「実装法」における脆弱性を指摘する．多様な攻撃を想定することで暗号集積回路における脆弱性を解明し，防御設計における必要十分条件を明らかにすることができる．

本論文は6章で構成される．

第1章では本論文の背景，意義，概要を示す．

第 2 章ではサイドチャネル攻撃に関する研究を紹介する．暗号アルゴリズムの特性だけでなくハードウェアの特性を利用したサイドチャネル攻撃が注目されている．既存研究として，暗号 LSI の消費電力を計測，解析する差分電力解析を扱った Kocher らの手法，McEvoy らの手法，Belaid らの手法，桶屋らの手法がある．故障を発生させることで得られた出力を利用するフォールト解析攻撃に関する研究として，Boneh らの手法，Biham らの手法がある．スキャンベース攻撃においてはストリーム暗号に対する手法として，Agrawal らの手法，Liu らの手法，Mukhopadhyay らの手法がある．またブロック暗号に対する手法として Yang らの手法，奈良らの手法，小寺らの手法がある．

第 3 章ではストリーム暗号に対するスキャンベース攻撃手法を提案し，評価する．ストリーム暗号評価プロジェクトで推奨暗号に認定された Trivium を対象にスキャンベース攻撃手法を提案する．Trivium は 3 本のシフトレジスタから構成され，内部の演算はビット同士の AND 演算と XOR 演算のみであるため，構造が単純で高速に動作する．秘密鍵 K(80bit)と IV(initialization vector: 初期化ベクトル)(80bit)により 288 個の内部状態レジスタが初期化され，内部状態を更新しながらキーストリームのビットを生成する．Trivium の性質上，攻撃者が解読対象の暗号文を出力した直後の Trivium LSI の内部状態値を取得した場合，過去のいかなる内部状態も算出でき，キーストリームを復元できる．得られたキーストリームと暗号文を順に排他的論理和することで元の平文を取得できる．暗号文から平文への復元は，いかに暗号文が出力された直後の内部状態値を取得するかに還元される．そこでストリーム暗号 LSI に任意の秘密鍵と IV を入力できることを利用する．秘密鍵と IV の値を入力ペアとして多数用意し，各入力に対し Trivium LSI を数サイクル動作させるとき，ある 1 ビットレジスタの入力に対する値の変化，動作させたサイクル数に対する値の変化は，そのレジスタ固有の値になる．この固有の値をスキャンシグネチャと呼ぶ．Trivium の内部状態レジスタに対しそれぞれスキャンシグネチャをシミュレータで計算しておき，同様の条件下で実際の LSI 回路から取得したスキャンデータと比較することでレジスタとスキャンデータ上のビットの対応を解析できる．この手法では，スキャンデータに Trivium のレジスタ以外のレジスタの値が含まれていても，高々1 ビットの値の変化にのみ着目しているため，内部状態レジスタのビットの位置を特定できる．スキャンデータのビット対応が一度求まれば，Trivium LSI が暗号文を出力した直後のスキャンデータから Trivium の内部状態レジスタの各値を求められる．Trivium の内部状態レジスタ値が求まれば，過去の内部状態，キーストリームを復元でき，Trivium LSI が出力した暗号文と排他的論理和することで，平文を復元できる．評価実験により，提案手法はスキャンデータに他の回路のビットが含まれていても，ビット対応解析可能と確認した．また，Trivium の内部状態レジスタ 288 個のビット対応解析には，特定の入力を設定してキーストリーム生成フ

ェーズからサイクル毎にスキャンデータを 13 個取得すれば良く，解析時間は 0.139 秒で済み，最も効率的に求められることを確認した．

第 4 章ではブロック暗号に対するスキャンベース攻撃手法を提案し，評価する．攻撃対象とするブロック暗号 LED は 64 ビットから 128 ビットの秘密鍵を用いて副鍵を生成し，分割・転置を実行するラウンド処理と副鍵との排他的論理和を繰り返す．演算処理単位は 4 ビットであり，各 4 ビットを 1 要素とする．秘密鍵長が 64 ビットの場合，秘密鍵を解読するためには 0 番目の副鍵 SK^0 を解読すればよい．LED の性質より，ラウンド処理実行前の値の任意の 1 要素はラウンド処理実行後の値の 4 つの要素に影響を及ぼしており，他の要素とは独立である．また，ラウンド処理実行後の値の任意の 1 要素はラウンド処理実行前の値の 4 つの要素に依存しており，他の要素とは独立の関係にある．これらの関係より 0 番目の要素のみ異なり，他の要素は等しい 2 つの平文を LED 暗号 LSI に入力し，1 ラウンド目処理後の値をスキャンデータとして取得し，排他的論理和する時，4 つの要素，つまり，ある 16 個のビットは副鍵 SK^0 の中の 0 番目の要素(4 ビット)のみに依存した値になる．よって，副鍵 SK^0 の 0 番目の要素の全パターンについて，これら 16 個のビットのスキャンシグネチャを求め，スキャンデータと比較することで，副鍵 SK^0 の 0 番目の要素を解読できる．同様に，副鍵 SK^0 の他の要素についてもこれらの手法で解読可能である．提案手法は，スキャンチェインに他の回路が含まれていても解読可能で，スキャンチェイン長，秘密鍵長に非依存である．スキャンチェイン長が 3 万ビット以上の場合には副鍵 SK^0 を 2 要素ずつ順番に求めればよい．また，秘密鍵長が 64 ビットより大きい場合，提案手法を用いて SK^0, 1 番目の副鍵 SK^1 を同様に順に求めることで判明する．計算機実験では，提案手法を用いて平均 73 個の平文で 64 ビットの秘密鍵を 0.290 秒で復元可能と確認した．また平均 145 個の平文で 128 ビットの秘密鍵を 0.468 秒で復元可能と確認した．スキャンチェインに他の回路が含まれていることを想定し，スキャンデータにランダムなビット値を付加してスキャンチェイン長を 13 万ビット程度まで変化させた場合にも，137 個の平文を用いて副鍵 SK^0 を 2 要素ずつ順番に求めることで，64 ビットの秘密鍵を 2 時間半程度で解読できることを確認した．

第 5 章では，ハッシュ関数の実装法 HMAC とハッシュ関数 PGV の性質とアルゴリズムを示し，HMAC-PGV へのスキャンベース攻撃手法を提案する．HMAC はハッシュ関数を 2 回実行するメッセージ認証コードである．ANSI, IETF ISO, NIST により標準化され，SSL, TLS, SSH, Ipsec 等に使われている．ハッシュ関数 PGV はブロック暗号を利用したハッシュ関数である．HMAC-PGV-f_1 に実装されたブロック暗号へのスキャンベース攻撃が可能な時，HMAC-PGV-f_1 に対してもスキャンベース攻撃可能である．ソフトウェアによる評価実験より，ハッシュに対してもスキャンベース攻撃可能なことを確認した．

第 6 章では本論文の内容をまとめ，今後の課題を示す．

早稲田大学　博士（工学）　学位申請　研究業績書

氏 名　　藤代　　美佳　　印

（2015 年　12 月現在）

種 類 別	題名、　発表・発行掲載誌名、　発表・発行年月、　連名者（申請者含む）
a. 論文：学術誌原著論文	[1] ○**M. Fujishiro**, M. Yanagisawa, and N. Togawa, “Scan-based side-channel attack on the LED block cipher using scan signatures,” *IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E97-A, no. 12, pp. 2434-2442, 2014. [2] ○**M. Fujishiro**, M. Yanagisawa, and N. Togawa, “Scan-based attack against trivium stream cipher using scan signatures,” *IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E97-A, no. 7, pp. 1444-1451, 2014. [3] H. Jiang, **M. Fujishiro**, H. Kodera, M. Yanagisawa, and N. Togawa, “Scan-based side-channel attack on the camellia block cipher using scan signatures,” *IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E98-A, no. 12, pp. 2547-2555, 2015.
c. 講演：国際会議（査読有り）	[4] ○**M. Fujishiro**, M. Yanagisawa, and N. Togawa, “Scan-based attack on the LED block cipher using scan signatures,” in *Proc. IEEE International Symposium on Circuits and Systems (ISCAS 2014)*, pp. 1460-1463, 2014. [5] ○**M. Fujishiro**, M. Yanagisawa, and N. Togawa, “Scan-based attack against trivium stream cipher independent of scan structure,” in *Proc. IEEE International Conference on ASIC (ASICON 2013)*, pp. 146-149, 2013. [6] 【招待論文】 **M. Fujishiro**, Y. Shi, M. Yanagisawa, and N. Togawa, “Scan-based side-channel attack against symmetric key ciphers using scan signatures,” in *Proc. IEEE Conference on Electron Devices and Solid-State Circuits (EDSSC 2015)*, pp. 309-312, 2015. [7] H. Jiang, **M. Fujishiro**, M. Yanagisawa, and N. Togawa, “Scan-based side-channel attack implementation evaluation on the LED cipher using SASEBO-GII,” in *Proc. Workshop on Synthesis And System Integration of Mixed Information Technologies (SASIMI 2015)*, pp. 433-434, 2015. [8] H. Jiang, **M. Fujishiro**, H. Kodera, M. Yanagisawa, and N. Togawa, “Scan-based side-channel attack on camellia cipher using scan signatures,” in *Proc. IEEE Asia Pacifc Conference on Circuits and Systems (APCCAS 2014)*, pp. 252-255, 2014.

Ｎｏ.2

早稲田大学　博士（工学）　学位申請　研究業績書

種 類 別	題名、　発表・発行掲載誌名、　発表・発行年月、　連名者（申請者含む）
c. 講演：国内学会（査読付き）	[9] **藤代美佳**, 柳澤政生, 戸川望, “ストリーム暗号 Trivium に対するスキャンチェインの構造に依存しないスキャンベース攻撃手法,” 第 26 回回路とシステムワークショップ論文集, pp. 442-447, 2013.
c. 講演：国内学会（査読無し）	[10] **藤代美佳**, 柳澤政生, 戸川望, “鍵長に依存しない LED 暗号に対するスキャンベース攻撃,” 情処研報, vol. 2015-SLDM-170, no. 47, pp. 149-154, 2015. [11] **藤代美佳**, 柳澤政生, 戸川望, “スキャンチェイン長に依存しない LED 暗号に対するスキャンベース攻撃, ” 信学技報, VLD2013-139, vol. 113, no. 454, pp. 31-36, 2014. [12] **藤代美佳**, 柳澤政生, 戸川望, “スキャンシグネチャを用いた LED 暗号へのスキャンベース攻撃, ” 信学技報, VLD2013-55, vol. 113, no. 235, pp. 47-52, 2013. [13] **藤代美佳**, 柳澤政生, 戸川望, “スキャンシグネチャを用いたストリーム暗号 Trivium へのスキャンベース攻撃手法,” 信学技報, VLD2013-8, vol. 113, no. 30, pp. 61-66, 2013.
e. その他（賞）	2014 年 8 月　DA シンポジウム 2014 アルゴリズムデザインコンテスト特別賞.