早稲田大学大学院 基幹理工学研究科

博士論文審査報告書

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

2016 年　　2 月

暗号システムを搭載した集積回路に対するサイドチャネル攻撃とは，集積回路の消費電力や熱・光等のサイドチャネル情報を利用することで，暗号集積回路内部の秘匿情報を取り出すことを言う．近年，各種交通系 IC カードやクレジットカード等，スマートカードの急速な普及・拡大に伴い，サイドチャネル攻撃が現実的な脅威として大きな注目を浴びている．サイドチャネル攻撃の一つとしてスキャンベースサイドチャネル攻撃（以下，スキャンベース攻撃と呼ぶ）がある．一般に集積回路はテスト設計を容易化するため，集積回路内部に存在する記憶素子の全部あるいは一部をスキャンチェインと呼ばれる信号線によって直列に接続し，集積回路外部から記憶素子の中身を観測・制御することを可能とする．スキャンチェインによって，製造された集積回路が設計通りに正しく動作するかテストすることができる.ところがスキャンチェインの出力を悪用することによって，第三者が記憶素子内部の状態を知ることができ，結果的に暗号集積回路内部の秘匿情報を取り出すことができる．スキャンチェインは集積回路中の記憶素子をランダムに接続しており，そのためスキャンチェインの設計者以外には記憶素子の接続順が不明である．スキャンベース攻撃では，いかにスキャンチェインから取り出されるデータ（これをスキャンデータと呼ぶ）と個別の記憶素子との対応関係を知ることができるかが大きな問題となる．

スキャンベース攻撃が 10 年程度前に初めて報告されて以降，スキャンベース攻撃の大部分は，スキャンチェインの構造に何らかの制約を課すことで，スキャンデータと記憶素子との対応関係を求めている．ところが，通常一つの集積回路内部には，暗号回路だけでなく，暗号を用いた各種演算回路や制御回路・マイクロプロセッサ等さまざまな回路ブロックが存在し，スキャンチェインはこれらに含まれる記憶要素をランダムに接続している．スキャンベース攻撃による暗号集積回路の脆弱性を解明するためには,スキャンチェインに特定の条件を仮定せず,より一般的なスキャンチェイン構造のもと，さまざまな暗号システムに対してスキャンベース攻撃の可能性を解明し，その結果として，暗号システムとその実装に関する脆弱性を解明する必要がある．

以上のような背景のもと，本論文では，ストリーム暗号，ブロック暗号，ハッシュといったさまざまな暗号システムとこれを実装した集積回路を取り上げ，一般的な構造を想定したスキャンチェインのもと，スキャンベース攻撃アルゴリズムを提案し，現実的な条件下でこれら暗号集積回路のスキャンベース攻撃の可能性を論じている．

本論文は 6 章から構成される．以下では，各章の概要を述べ，評価を加える．

第 1 章では，本論文の背景と目的および概要をまとめ，著者の研究の位置付けを明らかにしている．

第 2 章では，暗号集積回路に対する電力差分攻撃，フィールド解析攻撃，スキャンベース攻撃等さまざまなサイドチャネル攻撃を紹介している．

第３章では，ストリーム暗号の代表例としてストリーム暗号評価プロジェクト推奨暗号 Trivium を取り上げ,スキャンベース攻撃アルゴリズムを提案している．ここで，スキャンデータと Trivium 暗号回路の内部状態レジスタとの対応関係の解明が大きな課題となる．著者は，多数の入力信号を Trivium 暗号回路に入力したとき,各内部状態レジスタの値の変化が内部状態レジスタ特有の性質を持ち(これをスキャンシグニチャと呼ぶ),スキャンデータとスキャンシグニチャとを比較することで，スキャンデータ中の各内部状態レジスタ位置を正確に知ることができることを見い出した．提案アルゴリズムはこの性質を利用することで内部状態レジスタの値を特定し，その後，現在から過去の内部状態レジスタの値を復元することを示した．その結果，ストリーム暗号が持つキーストリーム値を全て復元し，最終的に元の平文を復元することができる．評価実験の結果，現実的な構造を持つスキャンチェインから得られたスキャンデータを利用しても，高々0.139 秒でスキャンデータと Trivium 暗号回路の内部状態レジスタとの対応関係が解明され，この結果を利用することで，平文が復元可能であることを確認している．

第４章では，ブロック暗号として LED 暗号を取り上げ，LED 暗号回路のスキャンベース攻撃アルゴリズムを提案している．提案アルゴリズムは，LED 暗号の秘密鍵の解読が 0 番目の副鍵の解読と実質的に等価であることを基本とする．この際，0 番目の副鍵のビットパタンが部分要素に分割できることを利用する．部分要素の全ビットパタンのスキャンシグニチャを生成し，これをスキャンデータと比較する.比較の結果,一致したものが実際の部分要素として解読可能となる．この操作を繰り返すことで最終的に LED 暗号の秘密鍵を復元できる．評価実験の結果，0.290 秒で 64 ビットの秘密鍵，0.468 秒で 128 ビットの秘密鍵を復元できることを確認している．

第５章では，第４章で提案された LED 暗号のためのスキャンベース攻撃アルゴリズムをハッシュ関数の一つ HMAC-PGV へのスキャンベース攻撃に拡張している．評価実験の結果，実際に HMAC-PGV へのスキャンベース攻撃が可能であり，ハッシュ関数中の秘密鍵を知らずとも任意のメッセージのハッシュ値を得られることを示した．

第６章では，本論文の成果の総括を行っている．

以上が本論文の概要であるが，本論文は，ストリーム暗号，ブロック暗号，ハッシュといったさまざまな暗号とこれを実装した集積回路に焦点を当て，一般的な構造を想定したスキャンチェインのもと，スキャンベース攻撃アルゴリズムを提案している．また評価実験の結果，これら暗号システムについて実際のスキャンベース攻撃の可能性を論じている．

これらの成果は，高度情報通信社会を支える重要な基盤情報技術たる情報セキュリティの発展に寄与するところが大である．よって本論文は博士（工学）の学位論文として価値あるものと認める．

2016 年 2 月

審査員　主査	早稲田大学教授	博士(工学)早稲田大学	戸川　望
	早稲田大学教授	工学博士(早稲田大学)	柳澤政生
	早稲田大学教授	工学博士(京都大学)	木村晋二
	早稲田大学准教授	博士(情報科学)早稲田大学	森　達哉