様　式　Ｆ－１９－２

科学研究費助成事業　　研究成果報告書

令和　２ 年　 ９ 月　 ８ 日現在

機関番号：１４６０３
研究種目：国際共同研究加速基金（国際共同研究強化）
研究期間：2017～2019
課題番号：１６ＫＫ０００６

研究課題名（和文）意図的な電磁妨害によるフォールト攻撃に対抗するレイヤ縦断型対策技術の開発（国際共同研究強化）

研究課題名（英文）Development of countermeasure methods based on combinations of layered security against fault attacks by intentional electromagnetic interference(Fostering Joint International Research)

研究代表者

林　優一（Hayashi, Yuichi）

奈良先端科学技術大学院大学・先端科学技術研究科・教授

研究者番号：６０５５１９１８

交付決定額（研究期間全体）：（直接経費）　　10,300,000円
渡航期間：　　８ヶ月

研究成果の概要（和文）：本研究では、IoTデバイスなどにもその組み込みが加速している暗号モジュールに対して実行される最も強力な実装攻撃の１つである電磁波妨害を用いた故障利用攻撃に焦点をあて、研究代表者の有する下位レイヤの知見と国際共同研究機関であるKU Leuvenの有する上位レイヤの知見を有機的に結合させ、上述した攻撃に対する抜本的な対策技術の開発を行った。

研究成果の学術的意義や社会的意義
実装攻撃に関しては攻撃が多様化しており、セキュアな暗号モジュール設計や、学会などで示される新たな解析法や対策法を実装するためには、プロトコルレベルの知識から、暗号モジュールを実装するハードウェア設計の知識に至るレイヤを縦断した幅広い知識が要求される。一方、各レイヤに関する知見は単一の分野でのカバーは難しく、分野間の連携が必要となることから、研究代表者の有する下位レイヤの知見と国際共同研究機関であるKU Leuvenの有する上位レイヤの知見を有機的に結合させ、上述した攻撃に対する抜本的な対策技術の開発を行った。

研究成果の概要（英文）：We focus on threats of fault injection attacks using intentional electromagnetic interference, which is one of the most powerful implementation attacks against cryptographic modules that are increasingly being embedded in IoT devices. By combining the lower-layers knowledge of us and the upper-layers knowledge of KU Leuven, we have developed drastic countermeasure methods against fault injection attacks.

研究分野：情報セキュリティ

キーワード：故障利用解析　サイドチャネル攻撃　意図的電磁妨害　電磁情報セキュリティ

様　式　Ｆ－１９－２

１．研究開始当初の背景

タッチスクリーンを搭載したスマートホン、タブレットなどのスマートデバイスの急激な普及に伴い、その利便性から私的な空間のみならず第 3 者が存在する公共の空間においても個人的な情報を閲覧・入力する機会が増加している。一方で、タッチスクリーン型の端末は、従来の PC などと異なり、スクリーン上に表示されるソフトウェアキーボードで入力操作を行うため、入力したキーとその入力先が同一画面に表示される。そのため、画面を盗み見されるとそれらの情報が同時に知られてしまうことになる。特にソフトウェアキーボードでは、ユーザに通知する目的で押下したキーを色の反転やポップアップにより強調表示するため、パスワード入力時などの入力した文字が伏せ字になる場合でも、タッチしたキーの情報とその入力先の情報から、何をどこに入力したのかを判別できる。さらに、こうした情報が電磁波を通じて漏えいした場合には、盗視の痕跡を残さずに情報を取得できる可能性があり、重大なセキュリティリスクをもたらす可能性がある。しかし、デバイス自体の消費電力が小さいことから、情報を含んだ放射電磁界強度も相対的に弱く、さらに、移動しながら利用されることが多いことから、電磁波を介した盗み見（電磁的画面盗視）の対象としては見なされず、その危険性に関する十分な検討はなされていなかった。

本研究代表者のグループはプロファイリングや信号処理技術を用いることにより、可搬性のある装置による電磁的画面盗視の脅威がタブレット端末に存在することを明らかにした。これまでの電磁的画面盗視では主に、据え置き型のディスプレイが対象とされ、盗視のための装置は一般に大がかりとなり、屋内や車内に設置されて使用されることが想定されてきたため、ディスプレイから漏えいする電磁波が装置に到達する前に、信号レベルを背景雑音以下に減衰させることで盗み見を防止するゾーニングという概念の下に対策がとられてきた。しかし、本研究代表者が明らかにした新たな脅威は、これまでの前提条件を覆すものであり、従来の電磁的画面盗視とは異なる対策が求められることから、スマートホンやタブレットなどのスマートデバイスにおける電磁情報漏えい評価及び対策技術の確立を目指し研究を遂行してきた。

これに対し、本研究課題では、電磁波によるセキュリティ低下評価技術を、電磁気学の相反定理から、逆向きの電磁気現象である妨害電磁波により引き起こされるセキュリティ低下の問題に応用する。具体的には、IoT デバイスなどにもその組み込みが加速している暗号モジュールに対して実行される最も強力な実装攻撃の１つである電磁波妨害を用いた故障利用攻撃に焦点をあてる。そして、研究代表者の有する下位レイヤの知見と国際共同研究機関である KU Leuven の有する上位レイヤの知見を有機的に結合させ、上述した攻撃に対する抜本的な対策技術の開発を目指す。

２．研究の目的

本研究では、電磁波によるセキュリティ低下評価技術を、電磁気学の相反定理から、逆向きの電磁気現象である妨害電磁波により引き起こされるセキュリティ低下の問題に応用する。具体的には、IoT デバイスなどにもその組み込みが加速している暗号モジュールに対して実行される最も強力な実装攻撃の１つである電磁波妨害を用いた故障利用攻撃に焦点をあてる。そして、研究代表者の有する下位レイヤの知見と国際共同研究機関である KU Leuven の有する上位レイヤの知見を有機的に結合させ、上述した攻撃に対する抜本的な対策技術の開発を目指す。

３．研究の方法

本研究では、暗号集積回路・実装攻撃・対策に関する世界的な権威である Ingrid Verbauwhede 教授と Verbauwhede 教授が所属する COSIC（暗号理論・プロトコルに関する著名な研究者が在籍）のメンバが有する知見と研究代表者が有する電磁界計測及びシミュレーション技術・信号処理技術、及び物理レイヤの対策技術に関する知見を融合させ研究を遂行する。また、KU Leuven 滞在中に実施する研究は、環境電磁工学・電子回路工学などに関する実験やディスカッションが必要となる可能性があるため、Telecom ParisTech（フランス）の Jean-Luc Danger 教授（Digital Electronic Systems 所属), University of Twente(オランダ)の Frank Leferink 教授（Electrical Engineering 所属）など、これまでヨーロッパ地域で研究代表者と交流のある研究者の協力を適宜得る。

４．研究成果

本研究では、暗号集積回路・実装攻撃・対策に関する世界的な権威である Ingrid Verbauwhede 教授と Verbauwhede 教授が所属する KU Leuven COSIC のメンバが有する知見と研究代表者が有する電磁界計測及びシミュレーション技術・信号処理技術、及び物理レイヤの対策技術に関する知見を融合させ、以下のように研究を遂行した。

まず、高い再現性を有する意図的な電磁妨害による暗号モジュールへの故障注入評価環境の構築のために、妨害電磁波の時間領域・周波数領域において異なる特性を有する連続波とパルス波を想定した評価セットアップを構築した。また、ターゲットとしては情報通信機器の機密性確保に欠くことができない暗号モジュール及び乱数生成器を選択し実装を行った。

そして、意図的な電磁妨害によりターゲットから生ずる誤り出力に対する解析手法を開発するために、汎用的な暗号モジュールに対して、故障差分攻撃(Differential Fault Analysis: DFA)などの従来手法に適用できる誤り出力が出現するか否かについて、妨害を受けた際に生ず

る暗号モジュールからの漏えい電磁波を時間領域で計測し、その外形を用いて誤りが発生した時刻を分類し、秘密鍵解析の可能性を検討した。また、乱数生成器に対しても、乱数生成時に機器外部に漏えいするサイドチャネル情報の振幅確立分布を計測することで、乱数性の低下を検出可能な手法を開発した。

また、多くのデバイスに適用可能な非侵襲な故障注入手法として、意図的な電磁妨害に着目し、注入する電磁波の周波数・振幅・位相を変化させ、暗号処理に対して非同期に注入した場合にも特定の処理に誤りを発生させる故障注入手法を開発した。

さらに、上記で構築した評価環境及び電磁界計測及びシミュレーションを用いて暗号モジュール及び乱数生成器にデバイスに印加した妨害電磁波の伝搬を高時間分解能で解析し、電磁妨害によるセキュリティ低下のメカニズムについて検討を行った。

続いて、前項で検討したメカニズムに基づき、電磁波を用いた非侵襲なフォールト注入時に暗号デバイスから発生する故障の種類の分類を行った。これに続いて、意図的な電磁妨害により暗号機器から生ずる情報漏えいのリスク評価手法を提案すると共に、情報セキュリティ及び環境電磁工学両分野の知見を融合させ上位レイヤに実装されるアルゴリズムに依存しない対策技術の開発に取り組んだ。

５．主な発表論文等

〔雑誌論文〕　計10件（うち査読付論文　10件／うち国際共著　6件／うちオープンアクセス　1件）

１．著者名 S. Osuka, D. Fujimoto, Y. Hayashi, N. Homma, A. Beckers, J. Balasch, B. Gierlichs and I. Verbauwhede	４．巻 99
２．論文標題 EM Information Security Threats Against RO-Based TRNGs: The Frequency Injection Attack Based on IEMI and EM Information Leakage	５．発行年 2018年
３．雑誌名 IEEE Transactions on Electromagnetic Compatibility	６．最初と最後の頁 1-7
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TEMC.2018.2844027	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 N. Saga, T. Itoh, Y. Hayashi, T. Mizuki, and H. Sone	４．巻 99
２．論文標題 Study on the effect of clock rise time on fault occurrence under IEMI	５．発行年 2018年
３．雑誌名 2018 IEEE International Symposium on Electromagnetic Compatibility and 2018 IEEE Asia-Pacific Symposium on Electromagnetic Compatibility	６．最初と最後の頁 9-9
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ISEMC.2018.8394009	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Y. Hayashi, N. Homma	４．巻 E102.B
２．論文標題 Introduction to Electromagnetic Information Security	５．発行年 2019年
３．雑誌名 IEICE Transactions on Communications	６．最初と最後の頁 40-50
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transcom.2018EBI0001	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Y. Hayashi, I. Verbauwhede, W. A. Radasky	４．巻 99
２．論文標題 Introduction to EM information security for IoT devices	５．発行年 2018年
３．雑誌名 2018 IEEE International Symposium on Electromagnetic Compatibility and 2018 IEEE Asia-Pacific Symposium on Electromagnetic Compatibility (EMC/APEMC), Singapore, 2018	６．最初と最後の頁 735-738
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ISEMC.2018.8393878	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 Ko Nakamura, Yuichi Hayashi, Takaaki Mizuki, Hideaki Sone	4．巻 印刷中
2．論文標題 Information Leakage Threats for Cryptographic Devices Using IEMI and EM Emission	5．発行年 2017年
3．雑誌名 IEEE Transactions on Electromagnetic Compatibility 1	6．最初と最後の頁 1-8
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TEMC.2017.2766139	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Arthur Beckers, Josep Balasch, Benedikt Gierlichs, Saki Osuka, Masahiro Kinugawa, Daisuke Fujimoto, Yuichi Hayashi, Ingrid Verbauwhede	4．巻 99
2．論文標題 Characterization of EM Faults on ATmega328p	5．発行年 2019年
3．雑誌名 2019 Joint International Symposium on Electromagnetic Compatibility and Asia-Pacific International Symposium on Electromagnetic Compatibility (EMC Sapporo & APEMC 2019)	6．最初と最後の頁 820-823
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 Saki Osuka, Daisuke Fujimoto, Naofumi Homma, Arthur Beckers, Josep Balasch, Benedikt Gierlichs, Ingrid Verbauwhede, Yuichi Hayashi	4．巻 99
2．論文標題 Fundamental Study on Randomness Evaluation Method of RO-Based TRNG Using APD	5．発行年 2019年
3．雑誌名 2019 Joint International Symposium on Electromagnetic Compatibility and Asia-Pacific International Symposium on Electromagnetic Compatibility (EMC Sapporo & APEMC 2019)	6．最初と最後の頁 244-244
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 Yuichi Hayashi, William Radasky	4．巻 99
2．論文標題 Electromagnetic Information Security Demanded by Social Infrastructure Constructed by Information Devices	5．発行年 2019年
3．雑誌名 2019 Joint International Symposium on Electromagnetic Compatibility and Asia-Pacific International Symposium on Electromagnetic Compatibility (EMC Sapporo & APEMC 2019)	6．最初と最後の頁 788-788
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 Mitsuki Takenouchi, Naoto Saga, Yuichi Hayashi, Takaaki Mizuki, Hideaki Sone	４．巻 99
２．論文標題 A Method for Distinguishing Faulty Bytes in Cryptographic Device Using EM Information Leakage	５．発行年 2019年
３．雑誌名 2019 Joint International Symposium on Electromagnetic Compatibility and Asia-Pacific International Symposium on Electromagnetic Compatibility (EMC Sapporo & APEMC 2019)	６．最初と最後の頁 669-669
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 A. Beckers, M.Kinugawa, Y. Hayashi, D. Fujimoto, J. Balasch, B. Gierlichs, & I. Verbauwhede	４．巻 99
２．論文標題 Design Considerations for EM Pulse Fault Injection	５．発行年 2019年
３．雑誌名 In: International Conference on Smart Card Research and Advanced Applications. Springer, Cham, 2019.	６．最初と最後の頁 176-192
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

〔学会発表〕　計12件（うち招待講演　3件／うち国際学会　3件）

１．発表者名 大須賀彩希，藤本大介，本間尚文，Arthur Beckers，Josep Balasch，Benedikt Gierlichs，Ingrid Verbauwhede，林優一
２．発表標題 TRNG on-the-fly テストを実装したリングオシレータベースの乱数生成器への周波数注入攻撃
３．学会等名 2019年暗号と情報セキュリティシンポジウム（SCIS2019）
４．発表年 2019年

１．発表者名 大須賀彩希，藤本大介，本間尚文，Arthur Beckers，Josep Balasch，Benedikt Gierlichs，Ingrid Verbauwhede，林優一
２．発表標題 振幅確率分布を用いた真性乱数生成器の乱数性評価手法に関する基礎検討
３．学会等名 ハードウェアセキュリティフォーラム2018
４．発表年 2018年

１．発表者名
Saki OSUKA, Daisuke FUJIMOTO, Naofumi HOMMA, Arthur BECKERS, Josep BALASCH, Benedikt GIERLICHS, Ingrid VERBAUWHEDE, Yu-ichi HAYASHI

２．発表標題
Fundamental Study on Degradation of Randomness in TRNG due to Intentional Electromagnetic Interference

３．学会等名
EMC Joint Workshop 2018 Daejeon（国際学会）

４．発表年
2018年

１．発表者名
硲マーティン，衣川昌宏，藤本大介，林優一

２．発表標題
意図的な電磁波注入による漏えい情報の制御に関する基礎検討

３．学会等名
2018年電子情報通信学会ソサイエティ大会

４．発表年
2018年

１．発表者名
岡本拓実，藤本大介，林優一，本間尚文，Arthur Beckers，Josep Balasch，Benedikt Gierlichs，Ingrid Verbauwhede

２．発表標題
ガウス雑音を用いた暗号機器への意図的な電磁妨害に対する耐性評価手法

３．学会等名
ハードウェアセキュリティ研究会

４．発表年
2018年

１．発表者名
Y.Hayashi

２．発表標題
EM Information Leakage Threat Caused by Low-power IEMI and Hardware Trojan

３．学会等名
AMEREM2018（招待講演）（国際学会）

４．発表年
2018年

１．発表者名
Yuichi Hayashi

２．発表標題
EM Information Security Threats and Its Countermeasures

３．学会等名
EMC Beijing 2017（招待講演）（国際学会）

４．発表年
2017年

１．発表者名
林優一

２．発表標題
漏えい・妨害・改変の3つの視点からみた電磁情報セキュリティ

３．学会等名
IEEE EMC Society Sendai Chapter Colloquium（招待講演）

４．発表年
2017年

１．発表者名
鍛治秀伍，衣川昌宏，藤本大介，林優一

２．発表標題
HTを用いて局所的にイミュニティを低下させた電子機器へのデータ注入攻撃

３．学会等名
2018年暗号と情報セキュリティシンポジウム

４．発表年
2018年

１．発表者名
大須賀彩希，藤本大介，林優一，本間尚文，Arthur Beckers，Josep Balasch，Benedikt Gierlichs，Ingrid Verbauwhede

２．発表標題
サイドチャネル情報を用いた乱数生成器への非侵襲な周波数注入攻撃

３．学会等名
2018年暗号と情報セキュリティシンポジウム

４．発表年
2018年

1．発表者名 大須賀 彩希，藤本 大介，林 優一
2．発表標題 TERO-based TRNGに対する周波数注入攻撃時の出力ビット推定手法に関する基礎検討
3．学会等名 ハードウェアセキュリティ研究会
4．発表年 2019年

1．発表者名 岡本拓実，藤本大介，崎山一男，李 陽，林優一
2．発表標題 順序回路への故障注入に起因した不均一な頻度分布を持つ誤り出力を用いた故障利用解析
3．学会等名 ハードウェアセキュリティ研究会
4．発表年 2020年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

6．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
主たる渡航先の主たる海外共同研究者	ヴェルバウヘーデ　イングリッド (Verbauwhede Ingrid)	ルーベン・カトリック大学・ESAT・教授	
主たる渡航先の主たる海外共同研究者	バラッシュ　ジョセップ (Balasch Josep)	ルーベン・カトリック大学・ESAT・FWO Postdoc	
主たる渡航先の主たる海外共同研究者	ギエルス　ベネディクト (Gierlichs Benedikt)	ルーベン・カトリック大学・ESAT・FWO Postdoc	

６．研究組織（つづき）

	氏名 （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
主たる渡航先の主たる海外共同研究者	ベッカーズ　アーサー (Beckers Arthur)	ルーベン・カトリック大学・ESAT・FWO Postdoc	