日本学術振興会に紙媒体で提出する必要はありません。

様　式　Ｆ－７－４

科学研究費助成事業（学術研究助成基金助成金）実績報告書（研究実績報告書）

機関番号	１４６０３

所属研究機関名称		奈良先端科学技術大学院大学
研究代表者	部局	先端科学技術研究科
	職	教授
	氏名	林　優一

１．研究種目名　国際共同研究加速基金（国際共同研究強化(A)）　２．課題番号　16KK0006

３．研究課題名　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）

４．補助事業期間　平成２９年度～令和元年度

５．主たる外国機関と海外共同研究者の状況

渡航先国名	渡航先外国機関名	主な海外共同研究者所属部局・職・氏名	渡航期間
ベルギー	KU Leuven	ESAT・Professor・Ingrid Verbauwhede	2017.09.07～2017.10.06 2017.10.13～2017.10.24 2017.11.02～2017.12.19 2018.01.04～2018.01.24 2018.02.09～2018.03.24 2018.05.20～2018.06.11 2019.01.03～2019.01.19 2019.06.12～2019.06.27 2020.01.02～2020.01.14
		合計（小計）	224日

６．研究実績の概要

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、「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」を目指している。本年度は以下2項目について重点的に研究を遂行した。

(1) 高精度な電磁界計測及びシミュレーションに基づく電磁妨害メカニズムの解明：これまで構築した評価環境に対する高精度な電磁界計測と電磁界シミュレーションの双方を用いて妨害電磁波の伝搬を高時間分解能で解析し、電磁妨害時に生ずる暗号モジュール及び乱数生成器のセキュリティ低下メカニズムを検討した。

(2) 意図的な電磁妨害により機器から生ずる情報漏えいリスク評価手法の確立と対策技術の開発：前項で得られたメカニズムに基づき、意図的な電磁妨害により暗号デバイスから発生する故障の種類の分類を行った。また、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した。さらに、メカニズムに基づき、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。

７．キーワード

情報学　情報セキュリティ　サイドチャネル攻撃　故障利用解析　意図的電磁妨害

8．研究発表

〔雑誌論文〕　計5件（うち査読付論文　5件／うち国際共著　4件／うちオープンアクセス　0件）

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	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	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	6．最初と最後の頁 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	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 －

日本学術振興会に紙媒体で提出する必要はありません。

1．著者名 Beckers Arthur、Kinugawa Masahiro、Hayashi Yuichi、Fujimoto Daisuke、Balasch Josep、Gierlichs Benedikt、Verbauwhede Ingrid	4．巻 11833
2．論文標題 Design Considerations for EM Pulse Fault Injection	5．発行年 2020年
3．雑誌名 International Conference on Smart Card Research and Advanced Applications. Springer	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） https://doi.org/10.1007/978-3-030-42068-0_11	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3件（うち招待講演　1件／うち国際学会　1件）

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 Yuichi Hayashi
2．発表標題 EM Information Leakage Threat Caused by Low-power IEMI and Hardware Trojan
3．学会等名 The 2019 IEEE International Symposium on EMC+SIPI（招待講演）（国際学会）
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 2019年

日本学術振興会に紙媒体で提出する必要はありません。

４版

〔図書〕　計0件

９．研究成果による産業財産権の出願・取得状況

計0件（うち出願0件／うち取得0件）

１０．科研費を使用して開催した国際研究集会

計0件

１１．備考

―