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　Ｃ－７－１

令和元年度科学研究費助成事業（科学研究費補助金）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　基盤研究(A)(一般)　　２．課題番号　19H01104

３．研究課題名　情報漏えいを引き起こす電磁波の計測困難化を実現する機器設計手法の開拓

４．研究期間　令和元年度～令和４年度　　５．領域番号・区分　－

６．研究実績の概要

本年度は、情報機器からの電磁波を通じた情報漏えいを評価する技術の開発を行った。情報機器からの電磁波を通じた情報の漏えいは特定の周波数（漏えいチャネル）で発生しており、この周波数において観測される放射電磁波に対して信号処理を施すことで情報の取得が可能となる。一方、情報機器から放射される電磁波は、非常に広い周波数で生じており、周波数毎に機器内部の実行される処理情報が得られるかを情報の復元まで行って確認する場合、多大な時間を要する。本年度は、電磁波を通じた情報漏えいモデルを機器内部で繰り返し実行される処理に着目して構築し、情報端末から放射される周波数毎に復調処理を施し、復調された信号に含まれる周波数を識別子として、漏えいチャネルを特定する手法を開発した。開発した手法は従来の評価手法に比べ、評価時間を1/100程度に短縮した。また、漏えいが発生している周波数帯に着目し、情報を漏えいさせる電磁波の強度をアクティブにコントロールできることを基礎実験により確認した。

７．キーワード

電磁波セキュリティ　サイドチャネル攻撃　電磁環境　暗号・認証

８．現在までの進捗状況

区分　（2）おおむね順調に進展している。

理由

本年度は、情報機器からの電磁波を通じた情報漏えいを評価する技術の開発を行い、その有効性も確認しており、当初の計画を達成している。また、次年度から着手予定であった電磁界シミュレーションを用いた漏えい評価技術の基礎検討も前倒しして開発を進め、基礎的な成果は当該分野における主要な国際会議・論文誌に採択されている。

日本学術振興会に紙媒体で提出する必要はありません。

９．今後の研究の推進方策

今後は、情報機器からの電磁波を通じた情報漏えい評価技術の精度向上を行うと共に、電磁界シミュレーション技術を用いた機器設計情報に基づく漏えい評価技術の開発を進める予定である。開発するシミュレーション技術は、汎用的な計算機で実行可能であることを目標とする。そのため、実験に基づいて抽出されたパラメタの中から、漏えい周波数を決定する支配的な要素を抽出し、シミュレーションに反映させる予定である。

１０．研究発表（令和元年度の研究成果）

〔雑誌論文〕　計3件（うち査読付論文　3件／うち国際共著論文　2件／うちオープンアクセス　1件）

１．著者名 林優一	４．巻 13
２．論文標題 ハードウェアに潜む電磁波セキュリティの脅威とその対策	５．発行年 2019年
３．雑誌名 電子情報通信学会 基礎・境界ソサイエティ Fundamentals Review	６．最初と最後の頁 28-37
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1587/essfr.13.1_28	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 Young Woo Kim, Daisuke Fujimoto, Hikaru Nishiyama, Daehwan Lho, Hyunwook Park, Joungho Kim and Yuichi Hayashi	４．巻 2019
２．論文標題 Statistical Analysis of Simultaneous Switching Output (SSO) Impacts on Steady State Output Responses and Signal Integrity	５．発行年 2019年
３．雑誌名 2019 12th International Workshop on the Electromagnetic Compatibility of Integrated Circuits (EMC Compo)	６．最初と最後の頁 138-140
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/EMCCompo.2019.8919652	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 Youngwoo Kim , Daisuke Fujimoto, Shugo Kaji, Shinpei Wada, HyunwookPark, Daehwan Lho, Joungho Kim, and Yuichi Hayashi	４．巻 2020
２．論文標題 Statistical Eye-Diagram Estimation Method Considering Power/Ground Noise Induced by Simultaneous Switching Output (SSO) Buffers	５．発行年 2020年
３．雑誌名 IEEE Transactions on Electromagnetic Compatibility	６．最初と最後の頁 1-11
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TEMC.2020.2975202	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5件（うち招待講演　4件／うち国際学会　3件）

1．発表者名 Y.Hayashi
2．発表標題 Introduction to Electromagnetic Information Security
3．学会等名 2019 Symposia on VLSI Technology and Circuits（招待講演）（国際学会）
4．発表年 2019年

1．発表者名 林優一
2．発表標題 IoT時代に求められるハードウェアセキュリティ
3．学会等名 EMC Sapporo & APEMC 2019 市民セミナー（招待講演）
4．発表年 2019年

1．発表者名 林優一
2．発表標題 EMCとセキュリティ ~電磁波によるセキュリティ低下の問題とその対策~
3．学会等名 EMCユーザ会議 2019（招待講演）
4．発表年 2019年

1．発表者名 Y.Hayashi
2．発表標題 Introduction：Application of EMC Methodology to Information Security　Evaluations/Countermeasures/Education
3．学会等名 2019 IEEE International Symposium on EMC+SIPI（招待講演）（国際学会）
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。

２版

１．発表者名 Youngwoo Kim , Yu-ichi Hayashi, Fujimoto Daisuke, Hyunwook Park,and Joungho Kim
２．発表標題 Statistical Signal/Power Integrity Analysis of High-BandwidthMemory (HBM) Interposer Channel considering SSO Noise and Data Coding
３．学会等名 DesignCon 2020（国際学会）
４．発表年 2020年

〔図書〕　計0件

１１．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）

１２．科研費を使用して開催した国際研究集会

計0件

１３．本研究に関連して実施した国際共同研究の実施状況

―

１４．備考

―