

様 式 F-7-2

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）

所属研究機関名称		奈良先端科学技術大学院大学	機関番号	14603
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(B) (特設分野研究) 2. 課題番号 18KT0050

3. 研究課題名 センシング情報の真正性を保証する物理層におけるトラスト基盤の確立

4. 補助事業期間 平成30年度～令和2年度

5. 研究実績の概要

本研究では、実世界センシングにより得られる情報の真正性を保証するために（１）センサ入力部におけるデータの改ざんに対抗するためにセンサ周囲の電磁界を認証情報として用い、データの真正性を保証する技術を開発すると共に（２）センサ内部及びデータ伝送時の改ざんに対抗するため、機器内部の電磁界分布をモニタリングすることで改ざんの予兆を検出すると共にデータの真正性を保証する技術を開発した。また、（３）センサを搭載したデバイス自体を置き換えて値を改ざんする脅威に対し、センシングデバイスが有する物理特性を認証情報として用い、デバイスの真正性を保証する技術の開発を行った。具体的には、環境電磁波を認証情報としたセンサ入力部に対するデータ改ざん検出技術の開発を行うためにデータ改ざんの検出に利用でき、かつ攻撃者による書き換えが困難な周波数帯を環境電磁波から選択するための計測環境を構築すると共に、改ざんを検出する具体的なアルゴリズムは、漏えい電磁波から統計的に情報抽出を行う手法を応用した。また、改ざん検出を行うセンシングのカテゴリ分けを行い、センシング方式に適した改ざん検出周波数の選定法についても検討を行った。機器内部の電磁界分布センシングによるデータ改ざん検出技術の開発に関してはセンシング後のデータ改ざんを発生させるオーバークロック、IRドロップ、グリッド挿入をリアルタイムにモニタリング可能な環境を構築した。また、データ変換時に生ずる電磁的な特徴量を用いたセンサ認証技術の開発についてもセンサ自体が攻撃者により付け替えられることを想定し、部品の実装ばらつきにより生ずる機器周囲に放射される電磁界スペクトルの差を認証に用いる技術を開発した。さらに、センサ内部及びデータ伝送時の改ざんに対抗するため、フルデジタルで構成され、機器内外の環境電磁波をセンシングし、攻撃の予兆を検出する技術の開発を行った。

6. キーワード

電磁波セキュリティ 計測セキュリティ 真正性保証 故障利用解析

7. 研究発表

〔雑誌論文〕 計4件（うち査読付論文 3件／うち国際共著 2件／うちオープンアクセス 0件）

1. 著者名 Beckers Arthur, Kinugawa Masahiro, Hayashi Yuichi, Balasch Josep, Verbauwhede Ingrid	4. 巻 2020
2. 論文標題 Design and Evaluation of a Spark Gap Based EM-fault Injection Setup	5. 発行年 2020年
3. 雑誌名 2020 IEEE International Symposium on Electromagnetic Compatibility & Signal/Power Integrity	6. 最初と最後の頁 523-526
掲載論文のDOI (デジタルオブジェクト識別子) 10.1109/EMCSI38923.2020.9191455	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

3 版

1. 著者名 Kinugawa Masahiro, Hayashi Yuichi	4. 巻 2020
2. 論文標題 Possibility of Injecting Malicious Instructions from Legitimate Communication Channels by IEMI	5. 発行年 2020年
3. 雑誌名 2020 IEEE International Symposium on Electromagnetic Compatibility & Signal/Power Integrity	6. 最初と最後の頁 527-527
掲載論文のDOI (デジタルオブジェクト識別子) 10.1109/EMCSI38923.2020.9191669	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 Yuichi Hayashi, William A. Radasky	4. 巻 2020
2. 論文標題 Introduction to Measurement Methods for Electromagnetic Information Security	5. 発行年 2020年
3. 雑誌名 2020 IEEE International Symposium on Electromagnetic Compatibility & Signal/Power Integrity	6. 最初と最後の頁 1-1
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 Shinoda Yuto, Takenouchi Mitsuki, Hayashi Yu-ichi, Mizuki Takaaki, Sone Hideaki	4. 巻 2020
2. 論文標題 Measurement on Effect of Controlled Wave Phase in EM Fault Injection Attack	5. 発行年 2020年
3. 雑誌名 2020 International Symposium on Electromagnetic Compatibility	6. 最初と最後の頁 1-5
掲載論文のDOI (デジタルオブジェクト識別子) 10.1109/EMCEUROPE48519.2020.9245847	査読の有無 無
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 —

〔学会発表〕 計4件（うち招待講演 0件／うち国際学会 0件）

1. 発表者名 鍛冶秀伍, 藤本大介, 林優一
2. 発表標題 意図的な電磁妨害時に生ずる情報漏えいの基礎評価
3. 学会等名 電子情報通信学会・環境電磁工学研究会
4. 発表年 2020年

1. 発表者名 鍛冶秀伍, 藤本大介, 衣川昌宏, 林優一
2. 発表標題 意図的に引き起こされる電磁的情報漏えい評価法の検討 ～ デジタル出力回路のインピーダンス変化に着目した評価 ～
3. 学会等名 電子情報通信学会・ハードウェアセキュリティ研究会
4. 発表年 2020年

1. 発表者名 鍛冶秀伍, 藤本大介, 林優一
2. 発表標題 複数の周波数印加による電磁的情報漏えい誘発に関する検討
3. 学会等名 2021年暗号と情報セキュリティシンポジウム(SCIS2021)
4. 発表年 2021年

1. 発表者名 上田浩行, 鍛冶秀伍, 藤本大介, キムヨンウ, 林優一
2. 発表標題 接触境界の表面粗さとトルク値がコネクタ高周波特性に与える影響に関する基礎検討
3. 学会等名 電子情報通信学会・機構デバイス研究会
4. 発表年 2020年

〔図書〕 計0件

8. 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）

9. 科研費を使用して開催した国際研究集会

計0件

10. 本研究に関連して実施した国際共同研究の実施状況

—

11. 備考

—