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－７－３

科学研究費助成事業（学術研究助成基金助成金）実施状況報告書（研究実施状況報告書）（平成２９年度）

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	情報科学研究科
	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）　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～平成３１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
		合計（小計）	155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、以下2項目について重点的に研究を遂行した。

(1)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：故障注入評価環境の構築は、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。

(2)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の開発：暗号モジュールに対しては、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、秘密鍵が解析される可能性を検討した。また、乱数生成器については、乱数生成時に生ずる放射スペクトルのパターンを周波数領域で計測することにより、妨害時に生ずるスペクトルの変化から乱数性の低下を検出可能な手法を開発した。

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．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

今年度実施した研究では、当初計画した成果が得られている。すなわち、(1)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および(2)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の開発について、既に以下の結果が得られている。

(1)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：故障注入評価環境の構築は、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た。

(2)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の開発：暗号モジュールに対しては、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、秘密鍵が解析される可能性を検討した。また、乱数生成器については、乱数生成時に生ずる放射スペクトルのパターンを周波数領域で計測することにより、妨害時に生ずるスペクトルの変化から乱数性の低下を検出可能な手法を開発した。

９．今後の研究の推進方策

現時点では研究を遂行する上での大きな問題点はないため、今後も研究計画にしたがって研究を遂行して行く予定である。具体的には以下の2項目について研究を引き続き遂行していく。

(1) 高精度な電磁界計測や電磁界シミュレーションなどに基づく電磁妨害メカニズムの解明： 高精度な電磁界計測や時間領域差分などの電磁界シミュレーションを用いてターゲットに伝搬する妨害電磁波を高時間分解能で解析し、それらを可視化することにより、時間領域・周波数領域双方の結果を用いて電磁妨害メカニズムを解明する。

(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：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を分類し、観測された誤り出力に適した解析手法の開発を行う。また、妨害の受けやすさを設計時に推定可能な計測手法についても開発を行う。これら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抜本的な対策技術を開発する。

１０．研究発表（平成２９年度の研究成果）

〔雑誌論文〕　計1件（うち査読付論文　1件／うち国際共著　0件／うちオープンアクセス　0件）

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 －

〔学会発表〕　計4件（うち招待講演　2件／うち国際学会　1件）

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

〔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．備考

―