様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２８ 年　 ５ 月 ２４ 日現在

機関番号：１１３０１
研究種目：基盤研究(B)（一般）
研究期間：2013～2015
課題番号：２５２８９０６８

研究課題名（和文）意図的な電磁妨害による故障利用攻撃に対抗する環境電磁工学的対策技術の開発

研究課題名（英文）Development of EMC Countermeasure against fault injection based attack and intentional electromagnetic interference

研究代表者

曽根　秀昭（SONE, Hideaki）

東北大学・サイバーサイエンスセンター・教授

研究者番号：４０１３４０１９

交付決定額（研究期間全体）：（直接経費）　　13,100,000円

研究成果の概要（和文）：本研究は、暗号機器の故障を引き起こす妨害電磁波伝搬を周波数および時間領域で計測し、妨害波の伝達効率を決定する物理的なパラメタ及び妨害を受けているコンポーネントを特定すると同時に、意図的な電磁波妨害によって生ずる情報漏えいのリスク評価を行った。さらに、妨害波の伝達効率を決定する物理パラメタに基づき、汎用的な機器の設計時に妨害電磁波に対する耐性を評価可能なシミュレーションモデルを構築すると共に、シミュレーションによる妨害電磁波伝搬の高精度な解析に基づき機器に故障が引き起こされるメカニズムを明らかにした。メカニズムとリスク評価の結果に基づき対策技術を提案した。

研究成果の概要（英文）：This research project presented a new type of transient fault injection based on IEMI that causes information leakage from cryptographic modules without disrupting their operation. Moreover, the mechanism of IEMI fault injection is explained from the viewpoint of Electromagnetic Compatibility (EMC): We demonstrate the consequence of the mechanism through experiments and full wave simulations. Based on the mechanism, we proposed electric-level countermeasures against this kind of fault injection attacks.

研究分野：情報通信工学

キーワード：電気機器工学　情報通信工学　電気・電磁環境　電磁的情報セキュリティ　暗号　故障利用攻撃　環境電磁工学　意図的電磁妨害

１．研究開始当初の背景

近年，情報通信機器への意図的な電磁妨害(IEMI)によって、機器の機能停止や回路素子を破壊することで機器の可用性を奪う脅威が指摘されている。IEMI は電子機器の電磁波に対する耐性の許容値を遙かに上回る大電力電磁環境(HPEM)を手段とする。IEMI の脅威に対し，国際電気標準会議(IEC)および国際電気通信連合(ITU) では「放射 HPEM 環境」を「ピーク電界強度が 100V/m 以上」として、「伝導 HPEM 環境」を「電圧レベル 1kV を越えるケーブルや電線に結合または注入される大電力電磁電流及び電圧」として定義し、規格策定を進めている。

しかし、これらの破壊的な IEMI と異なって、暗号処理などの情報機器の機密性を奪うことは、HPEM ではなく、はるかに低レベルの電磁妨害波でも可能性があって、従来の IEMI 対策とは異なる問題として対策を考える必要がある。

２．研究の目的

本研究では、IEMI による情報漏えいのメカニズム解明と対策技術の開発を目指し、妨害電磁波の伝搬特性を決定するパラメタの抽出から対策技術の開発までの下記 4 項目を目的とした。

(1) 故障を引き起こす妨害周波数を決定するパラメタ抽出と電磁妨害先コンポーネントの特定

故障を引き起こしやすい周波数で妨害波を機器外部から印可し、機器上に妨害波が伝搬する様子を周波数及び時間領域で観測し、妨害電磁波の周波数特性を決定するパラメタを抽出する。また、機器上の妨害周波数の伝搬強度分布から、妨害を受けているコンポーネントを特定する。

(2) IEMI による意図的な電磁妨害によって機器から出力される情報を用いたリスク評価

リスク評価として、IEMI による故障注入時に出力される任意のビットに誤りが生じた暗号文へ、既存の解析手法の適用可能性や解読時間を計測する。また、新たな解析手法についても検討を行うと共に、他のブロック暗号・ストリーム暗号についても解析を検討しリスク評価する。

(3) 汎用的な機器設計時に妨害電磁波への耐性を評価可能なシミュレーションモデルの構築

(1)に基づいて得られたパラメタと妨害先のコンポーネントを含むシミュレーションモデルを実装する。モデルは(1)の実験結果により得られた S パラメタや伝達関数などを正確に再現できているかを確認しながら進める。また、モデルは一般的な PC で計算可能な簡素なものを目指す。

(4) シミュレーションに基づく電磁妨害メカニズムの解明と対策技術の開発

(3)で実装したシミュレーションモデルを用い、FDTD 法により妨害電磁波の伝搬を高時間分解能で解析・可視化することにより電磁妨害メカニズムを解明する。得られたメカニズムを基に、配線パターンなどの幾何的な形状及び、EMC 分野で開発されたノイズ抑制素子を効果的に組み合わせ、それを逐次シミュレーション上で評価しながら、(2)の結果を併せつつ対策技術を開発する。

３．研究の方法

本研究では、上述の研究目的を 3 年間で達成することを目指す。平成 25 年度は機器の故障を引き起こし易い妨害周波数を決定するパラメタを S パラメタや伝達関数を基に抽出すると共に、電磁妨害を受けるコンポーネントを特定する。さらに、IEMI による故障注入により機器から出力される任意のビットに誤りが生じた暗号文に対して秘密鍵情報の漏えいリスク評価を行う。平成 26 年度は前年度のパラメタ抽出とリスク評価を継続すると共に、計測結果に基づく暗号機器設計時に妨害電磁波への耐性を評価可能な、汎用的シミュレーションモデルの構築を行う。平成 27 年度は、シミュレーションモデルの高精度化を図ると共に、シミュレーションモデルを用いて、妨害電磁波伝搬を高時間分解能で計算し、時系列で可視化することで、IEMI による機密性・完全性低下のメカニズムを解明する。得られたメカニズムとリスク評価の結果を基に対策技術の開発を行う。

４．研究成果

各年度において、交付申請書の研究実施計画各項目に対応して以下の項目について研究を行って成果を得た。

平成 25 年度

(1) 故障を引き起こす妨害周波数を決定するパラメタ抽出と電磁妨害先コンポーネントの特定

故障を引き起こしやすい周波数で妨害波を機器外部から印可し、機器上に妨害波が伝搬する様子を周波数及び時間領域で観測し、妨害電磁波の周波数特性を決定するパラメタを抽出した。また、機器上の妨害周波数の伝搬強度分布から、妨害を受けているコンポーネントを特定した。

(2) IEMI による意図的な電磁妨害によって機器から出力される情報を用いたリスク評価

リスク評価として、IEMI による故障注入時に出力される任意のビットに誤りが生じた暗号文へ、既存の解析手法の適用可能性や解読時間を計測した。また、注入するレベル、及び周波数を変化させ、出力される暗号文の誤りビット数に変化が生ずることを基礎実験より明らかにし、Differential Fault Analysis (DFA)により鍵の取得が可能であることを示した。

さらに、電磁妨害の影響を受けないカードを用いた暗号プロトコルの開発も進めた。

これらの研究を実施するために、実験環境として電磁界数値解析システムと供試デバイスなどを整備し、また、研究成果の公表として国内外の研究会合に参加した。

上述の研究成果は高く評価され、環境電磁工学分野においては、国内学会（2013 電子情報通信学会ソサイエティ大会）で招待講演を行うと共に、情報セキュリティ分野の国際会議（ IWSEC (International Workshop on Security)2013）においても招待され講演を行っている。

平成 26 年度

(1) 汎用的な暗号機器設計時に妨害電磁波への耐性を評価可能なシミュレーションモデルの構築

故障を引き起こし易い妨害周波数を決定するパラメタを基に、基板上の電磁界分布などの実測結果を確認しながら暗号機器設計時に耐性を評価可能とする基礎的なシミュレーションモデルを構築した。また、故障を引き起こしやすい妨害電磁波の周波数を決定するパラメタを抽出して、基板上の電磁界分布と各点における S パラメタ及び伝達関数などの実測を行いつつ、汎用的なシミュレーションモデルの基礎を得た。

(2) 電磁妨害メカニズム解明と対策技術の開発

故障注入に必要な妨害電磁波は正弦波の場合にインパルスより 20 倍小さいという基礎検討から、機器内部で共振が生じるモデルを用いて、妨害波が伝搬し共振する時間領域現象を可視化することでメカニズムを解明した。また、意図的な電磁妨害に対して耐性の高い暗号プロトコルの開発を進めて、電磁妨害の影響を受けないカード組を用いた暗号プロトコルの開発を進め、その成果のひとつは IEICE Trans. Fundamentals 誌に掲載されることが決定した。

さらに、計測、リスク評価及び耐性評価モデルの結果を取りまとめ、成果の発表を行った。

平成 27 年度

(1) 汎用的な暗号機器設計時に妨害電磁波への耐性を評価可能なモデルの構築

前年度に抽出した故障を引き起こし易い妨害電磁波の周波数を決定するパラメタを基に、電磁界シミュレーションモデルを構築すると共に、シミュレーションのみでは評価が困難な複雑な電子機器にも適用可能な妨害電磁波評価回路を設計した。そして、シミュレーション及び評価回路をベースに暗号機器設計時に妨害電磁波への耐性を評価可能とする汎用的なモデルを構築した。モデルの構築は、基板上の電磁界分布、各点における S パラメタ及び伝達関数などの実測に得られた各種結果と比較し、妥当性を確認した。

(2) 電磁妨害メカニズム解明と対策技術の開発

妨害波の機器上伝搬を時間領域で可視化すると共に、故障時に暗号機器から出力される誤りを計測することで、妨害波は暗号モジュール内部で分配されるクロック信号に重畳し、セットアップタイム違反を引き起こすことで故障が引き起こされていることを明らかにした。また、本メカニズムに基づき、電源線を利用した故障注入手法に対しては、暗号機器への妨害波の伝搬を抑制するためフェライトコアなどの安価で機器に容易に適用可能な EMC 対策手法が有効であることを示唆した。

(3)意図的な電磁妨害に高い耐性のある暗号プロトコルの開発

意図的な電磁妨害に耐性のある物理的暗号システムの一つとして、前年度に引き続きカードを用いた暗号プロトコルの開発を進め、情報漏えいを防止する物理的ケースを導入することにより効率的なプロトコルを構築した。

５．主な発表論文等

〔雑誌論文〕（計４件）

① 林優一，本間尚文，水木敬明，青木孝文，曽根秀昭，周波数領域における暗号モジュールに対する電磁波解析の効率化，電気学会論文誌 A(査読有)，135，2015，515-521，DOI:10.1541/ieejfms.135.515

② Takuya Nishida, Yu-ichi Hayashi, Takaaki Mizuki, Hideaki Sone, Securely Computing Three-Input Functions with Eight Cards, IEICE Trans. Fundamentals（査読有），E98-A，2015，1145-1152，DOI:10.1587/transfun.E98.A.1145

③ 林優一，本間尚文，水木敬明，青木孝文，

曽根秀昭，暗号モジュールに対する意図的な電磁妨害による故障発生メカニズムに関する基礎的検討，電気学会論文誌 A(査読有)，135，2015，276-281，DOI:10.1541/ieejfms.135.276

④ Y. Hayashi, T. Mizuki and H. Sone, Investigation of Noise Interference due to Connector Contact Failure in a Coaxial Cable, IEICE Trans. Electronics（査読有）, E97-C, 2014, 900-903, DOI: 10.1587/transele.E97.C. 900

〔学会発表〕（計３６件）

① 佐藤友哉，林優一，水木敬明，曽根秀昭，接触不良による接触点部分のインダクタンス値推定手法，電子情報通信学会総合大会，2016 年 03 月 15 日～2016 年 03 月 18 日，九州大学（福岡県・福岡市）

② 中村 紘，林 優一，水木敬明，曽根秀昭，サイドチャネル情報への相関解析を用いた暗号処理時刻推定，電子情報通信学会総合大会，2016 年 03 月 15 日～2016 年 03 月 18 日，九州大学（福岡県・福岡市）

③ Akihiro Nishimura, Takuya Nishida, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone, Five-Card Secure Computations Using Unequal Division Shuffle , Theory and Practice of Natural Computing (TPNC 2015) (国際学会), 2015 年 12 月 15 日～2015 年 12 月 16 日，ミエレス（スペイン）

④ Megumi Saito, Yu-ichi Hayashi, Takaaki Mizuki, Hideaki Sone, Fundamental study on randomized processing in cryptographic IC using variable clock against Correlation Power Analysis, EMC Compo 2015 - 10th International Workshop on the Electromagnetic Compatibility of Integrated Circuits (国際学会), 2015 年 11 月 10 日～2015 年 11 月 13 日，エディンバラ（イギリス）

⑤ Tomoya Sato, Yu-ichi Hayashi, Takaaki Mizuki and Hideaki Sone, Estimation of Inductance at Surface Structure in Contact Surfaces of Coaxial Connector, 電子情報通信学会技術研究報告, IS-EMD2015, 2015 年 11 月 06 日，東北大学（宮城県・仙台市）

⑥ 佐藤友哉，林優一，水木敬明，曽根秀昭，接触不良によるインダクタンス値増大の定量的評価に関する検討，電子情報通信学会ソサイエティ大会，2015 年 09 月 11 日，東北大学（宮城県・仙台市）

⑦ Ko Nakamura, Yu-ichi Hayashi, Naofumi Homma, Takaaki Mizuki, Takafumi Aoki, Hideaki Sone, Method for estimating fault injection time on cryptographic devices from EM leakage , 2015 IEEE International Symposium on Electromagnetic Compatibility (国際学会), 2015 年 08 月 16 日～2015 年 08 月 22 日，ドレスデン（ドイツ）

⑧ 中村紘，林優一，本間尚文，水木敬明，青木孝文，曽根 秀昭，暗号モジュールからの漏えい電磁波を用いた故障タイミング特定手法の実行可能性に関する検討，電子情報通信学会技術研究報告, 2015 年 07 月 02 日，機械振興会館（東京都・港区）

⑨ M. Saito, Y. Hayashi, T. Mizuki, and H. Sone, Effect of Clock Frequencies on EM Information Leakage from Cryptographic Devices，電子情報通信学会技術研究報告, 2015 年 06 月 26 日，バンコク（タイ）

⑩ Yu-ichi Hayashi, Naofumi Homma, Takaaki Mizuki, Takafumi Aoki, Hideaki Sone , Fundamental Study on Fault Occurrence Mechanisms by Intentional Electromagnetic Interference Using Impulses , 2015 Asia-Pacific Symposium on Electromagnetic Compatibility (APEMC2015) (国際学会), 2015 年 05 月 29 日，台北（台湾）

⑪ 佐藤友哉，林優一，水木敬明，曽根秀昭，接触不良による接触点の減少とインダクタンス値増加の関係，電子情報通信学会総合大会，2015 年 03 月 12 日，立命館大学(滋賀県・草津市)

⑫ 中村紘，林優一，水木敬明，曽根秀昭，漏洩電磁波の観測に基づく故障タイミング特定手法に関する検討，電子情報通信学会総合大会，2015 年 03 月 11 日，立命館大学(滋賀県・草津市)

⑬ 佐々木匠，林優一，水木敬明，曽根秀昭，暗号機器への入力データの選択による漏えい電磁波解析の効率化に関する検討，計測自動制御学会東北支部 50 周年記念学術講演会，20 14 年 12 月 12 日，東北大学(宮城県・仙台市)

⑭ 小林瑞樹，林優一，水木敬明，曽根秀昭，暗号器に対するタイミングを制御した意図的な電磁妨害による故障注入に関する検討，計測自動制御学会東北支部 50 周年記念学術講演会，2014 年 12 月 12 日，東北大学(宮城県・仙台市)

⑮ 中村紘，林優一，水木敬明，曽根秀昭，漏洩電磁波計測に基づく暗号機器の故障タイミング特定手法，計測自動制御学会東北支部 50 周年記念学術講演会，2014 年 12 月 12 日，東北大学(宮城県・仙台市)

⑯ 佐藤友哉，林優一，水木敬明，曽根秀昭，電磁界シミュレーションを用いたコネクタ接触不良部における電流路の解析，計測自動制御学会東北支部 50 周年記念学術講演会，2014 年 12 月 12 日，東北大学(宮城県・仙台市)

⑰ T. Sato, Y. Hayashi, T. Mizuki, and H. Sone, Fundamental Study on a Mechanism of Increased Inductance due to Connector Contact Failure, 電子情報通信学会技術研究報告，2014 年 11 月 30 日，千歳市文化センター (北海道・千歳市)

⑱ 西田拓也, 林優一, 水木敬明, 曽根秀昭, カード組を用いた任意の論理関数の安全な計算について, コンピュータセキュリティシンポジウム 2014, 2014 年 10 月 24 日, 札幌コンベンションセンター(北海道・札幌市)

⑲ 小林瑞樹, 林優一, 本間尚文, 水木敬明, 青木孝文, 曽根秀昭, タイミングを制御した意図的な電磁妨害が暗号機器の内部動作に与える影響に関する検討, 電子情報通信学会技術研究報告, 2014 年 10 月 23 日, 秋田県立大学(秋田県・由利本荘市)

⑳ H. Sone, Y. Hayashi, T. Mizuki, Analysis of EM Emission from Cryptographic Devices, URSI General Assembly and Scientific Symposium(招待講演), 2014 年 08 月 19 日, 北京（中国）

㉑ Takuya Nishida, Secure Three-Input Majority Computation Using a Deck of Cards, The 9th International Workshop on Security, IW SEC2014 (招待講演), 2014 年 08 月 14 日, 弘前大学(青森県・弘前市)

㉒ Y. Hayashi, N. Homma, T. Mizuki, T. Aoki, H. Sone, Precisely Timed IEMI Fault Injection Synchronized with EM Information Leakage, IEEE International Symposium on Electromagnetic Compatibility (招待講演), 2014 年 08 月 07 日, ローリー(アメリカ)

㉓ 中村紘, 林優一, 本間尚文, 水木敬明, 青木孝文, 曽根秀昭, サイドチャネル情報を用いた故障発生タイミング特定手法の実現可能性に関する検討, 電子情報通信学会技術研究報告, 2014 年 07 月 10 日, 機械振興会館(東京都・港区)

㉔ Tomoya Sato, Yu-ichi Hayashi, Takaaki Mizuki, Hideaki Sone, Simulation-based Analysis of Inductance at Loosened Connector Contact Boundary, The 27th International Conference on Electrical Contacts, 2014 年 06 月 26 日, ドレスデン（ドイツ)

㉕ 中村紘, 林優一, 本間尚文, 水木敬明, 青木孝文, 曽根秀昭, 暗号モジュールにおけるサイドチャネル情報を用いた故障発生タイミング特定手法, 電子情報通信学会技術研究報告, 2014 年 06 月 20 日, 神戸大学(兵庫県・神戸市)

㉖ Y. Hayashi, N. Homma, T. Mizuki, T. Aoki, H. Sone, Efficient Method for Estimating Propagation Area of Information Leakage via EM Field, 2014 International Symposium on Electromagnetic Compatibility, Tokyo, 2014 年 05 月 14 日, 学術総合センター(東京都・千代田区)

㉗ 佐藤友哉, 林優一, 水木敬明, 曽根秀昭, コネクタ接触不良部近傍の磁界分布に基づく電流路の推定, 2014 年電子情報通信学会総合大会, 2014 年 03 月 18 日, 新潟大学(新潟県・新潟市)

㉘ Takuya Nishida, Takaaki Mizuki, Hideaki Sone, Securely Computing the Three-Input Majority Function with Eight Cards, 2nd International Conference on the Theory and Practice of Natural Computing, TPNC 2013, Caceres, Spain, 2013 年 12 月 05 日, カセレス (スペイン)

㉙ Yu-ichi Hayashi, Remote fault-injection method with timing control based on leaked information, The 8th International Workshop on Security, IWSEC2013 (招待講演), 2013 年 11 月 19 日, 沖縄県市町村自治会館(沖縄県那覇市)

㉚ Yu-ichi Hayashi, Takaaki Mizuki, Hideaki Sone, Investigation of No ise Interference due to Connector Contact Failure in a Coaxial Cable, International Session on Electromechanical Devices IS-EMD2013, 2013 年 11 月 16 日, 武漢 （中国）

㉛ 小林瑞樹, 林優一, 本間尚文, 水木敬明, 青木孝文, 曽根秀昭, 漏えい情報を用いた注入タイミングを制御可能な暗号モジュール外部からの故障注入メカニズムに関する検討, 電子情報通信学会環境電磁工学研究会, 2013 年 10 月 25 日, 東北大学(宮城県・仙台市)

㉜ 西田拓也, 林優一, 水木敬明, 曽根秀昭, カードを用いた安全な三入力多数決の計算について, コンピュータセキュリティシンポジウム 2013, 2013 年 10 月 22 日, かがわ国際会議場(香川県・高松市)

㉝ 林優一, 本間尚文, 水木敬明, 青木孝文, 曽根秀昭, 意図的な電磁妨害による暗号デバイスからの情報漏えいの脅威とその対策, 2013 年電子情報通信学会ソサイエティ大会（招待講演) , 2013 年 09 月 19 日, 福岡工業大学(福岡県・福岡市)

㉞ 林優一, 本間尚文, 曽根秀昭, 安全・安心な情報通信社会を実現する電磁情報セキュリティ評価・対策技術, 2013 年電子情報通信学会ソサイエティ大会（招待講演) , 2013 年 09 月 19 日, 福岡工業大学（福岡県・福岡市）

㉟ 佐々木匠, 林優一, 水木敬明, 曽根秀昭, 暗号処理時に生ずる漏えい電磁信号とハミング距離の関係, 2013 年電子情報通信学会ソサイエティ大会, 2013 年 09 月 19 日, 福岡工業大学(福岡県・福岡市)

㊱ 小林瑞樹, 林優一, 本間尚文, 水木敬明, 青木孝文, 曽根秀昭, 漏えい電磁情報を用いた任意の処理への非侵襲な故障注入手法, 2013 年電子情報通信学会ソサイエティ大会, 2013 年 09 月 18 日, 福岡工業大学(福岡県・福岡市)

６．研究組織

(1)研究代表者

曽根　秀昭　（SONE, Hideaki）
東北大学・サイバーサイエンスセンター・教授
研究者番号：４０１３４０１９

(2)**研究分担者**
林　優一　（HAYASHI, Yu-ichi）
東北学院大学・工学部・准教授
研究者番号：６０５５１９１８

水木　敬明　（MIZUKI, Takaaki）
東北大学・サイバーサイエンスセンター・
准教授
研究者番号：９０３２３０８９