様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　５ 年　 ６ 月　 ９ 日現在

機関番号：１１３０１
研究種目：基盤研究(B)（一般）
研究期間：2017～2020
課題番号：１７Ｈ０１７５１

研究課題名（和文）意図的電磁妨害による故障注入攻撃への電磁セキュリティ工学的対策の体系化

研究課題名（英文）Systematization of electromagnetic security engineering countermeasure against fault-injection attacks caused by intentional electromagnetic interference

研究代表者
曽根　秀昭（Sone, Hideaki）

東北大学・データシナジー創生機構・特任教授

研究者番号：４０１３４０１９

交付決定額（研究期間全体）：（直接経費）　　14,400,000円

研究成果の概要（和文）：情報通信機器への意図的な電磁妨害IEMIへの対策のため4つの課題を解いた。
妨害特性を決定するパラメタ及び被妨害コンポーネントについて、FPGAで故障時刻や内部の電気的変化を高精度に観測可能な環境構成を構築した。妨害によるIC内部からの出力を分析して故障が発生しやすい印加タイミングに関するリスク評価の知見を得た。妨害耐性評価について故障注入時の計測波形の解析に基づく手法を示し、波形の分解能は秘密鍵の取得性を向上させない知見を得て、また、放射電磁波情報漏えいを抑制可能な2値画像の設計を提案した。電磁妨害メカニズムに関し、暗号機器の処理の故障注入時刻を判定し秘密鍵解析リスクを評価する手法を実証した。

研究成果の学術的意義や社会的意義
情報通信機器への意図的な電磁妨害(IEMI)のうち電力電磁環境と比べ3桁ほど小さい数V程度の意図的な電磁妨害による電磁的情報セキュリティの分野は本課題のチームが創って国内外で研究活動を先導している。暗号機器に非侵襲に一時的な故障を注入し、その誤り出力から暗号化の秘密鍵情報を取得できる。すなわち、機器の可用性は損なわず、機密性・完全性のみを低下させる脅威である。
本課題では、FPGAなどの暗号機器へのIEMI攻撃について妨害受容特性とメカニズムに迫ったもので、リスク評価と妨害特性評価の手法を示し、評価測定の方法を提案しており、電磁的情報セキュリティ対策に意義深い。

研究成果の概要（英文）：Problems on countermeasures against intentional electromagnetic interference on information communication equipment are discussed.
Analysis of output from an FPGA under IEMI attack gave an idea of risk assessment on attack timing to cause failure. Also a method to measure waveforms under IEMI failure for tolerance evaluation and effect of amplitude resolution of the waveform were proposed. Based on analysis on mechanism of electromagnetic interference, a new method to evaluate the risk of secret key analysis by determining the time of failure injection on processing of a cryptographic equipment. Also an design of binary image which can suppress image information leakage by electromagnetic radiation.

研究分野：情報通信工学

キーワード：情報システム　情報セキュリティ　電子デバイス・機器　暗号・認証等　耐タンパー技術　電磁情報セキュリティ　ハードウェアセキュリティ

様　式　C－１９、F－１９－１、Z－１９（共通）

１．研究開始当初の背景

情報通信機器への意図的な電磁妨害(IEMI)は、一般に機器の機能停止や破壊に至らせて可用性を奪うものである。この IEMI は電子機器の電磁波に対する耐性を遙かに上回る大電力電磁環境(HPEM)を手段とする。この脅威に対し、メカニズム解析や対策技術の議論が IEEE Electromagnetic Compatibility (EMC) Society を中心に行われており、また国際電気標準会議(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」、「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。

一方で、研究代表者らのグループは、HPEM と比べ 3 桁ほど小さい数 V 程度の意図的な電磁妨害による電磁的情報セキュリティの分野を創り、国内外で研究活動を先導している。この脅威は、暗号機器に非侵襲に一時的な故障を注入し、その故障に起因する誤り出力から暗号化の秘密鍵情報を取得できるものである。すなわち、機器の動作は保ちつつ、一部の処理のみに意図的に誤りを生じさせて、可用性は損なわず、機密性・完全性のみのセキュリティを低下させる手法であり、情報セキュリティの新たな脅威である。電磁的情報セキュリティの脅威への対策には第一段で述べた大電力電磁波の IEMI とは異なる取組みが必要である。

研究代表者らはこれまで、暗号機器から放射される情報を含む漏えい電磁波による機密性・完全性低下の問題に取り組み、電磁放射の主要因であるコモンモード電流による情報漏えいメカニズムを解明し、また情報漏えいの評価法として複雑な解析を要せず放射スペクトルのみに着目した情報漏えいの評価法を確立してきた。こうした知見を基に、漏えい電磁波による機密性・完全性低下の問題で着目した漏えい電磁波について、意図的な電磁妨害による機密性・完全性低下の問題では、その伝搬方向を逆向きに捉えることで情報漏えいメカニズムの把握や対策技術の確立が可能と着想して、この研究計画に至った。

２．研究の目的

本研究は、意図的な電磁波妨害による情報機器の故障により引き起こされ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す。具体的には以下の課題に沿って取り組む。

(1)情報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と被妨害コンポーネントを特定し、以下の基盤とする。

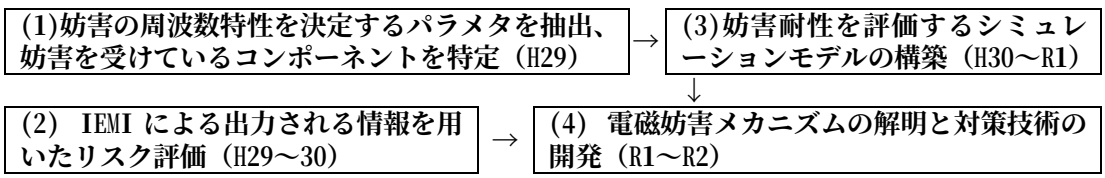
(2)意図的な電磁波妨害によって生ずる情報漏えいのリスク評価を行う。

(3)機器の設計時に妨害電磁波への故障耐性を評価可能なシミュレーションモデルを構築する。

(4)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、標記の研究目的を達成する。

３．研究の方法

IEMI による情報システムのセキュリティ低下メカニズムの解明と対策技術の開発を目指し、妨害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 4 つの課題を解く。



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

情報システム・機器への IEMI による意図的な故障の発生は、注入する妨害波の周波数に依存する。故障を引き起こしやすい周波数の妨害波を機器外部から印加し、機器上を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。

課題(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の既存の解析手法の適用可能性や、その際の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する。

課題(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
　課題(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。

課題(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
　課題(3)で実装したシミュレーションモデルを用い、妨害電磁波の伝搬を FDTD 法により高時間分解能で解析し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、シミュレーション上で評価しながら、課題(2)の結果を併せて、対策技術を開発する。

　これら４つの課題は互いに関連するので独立した課題あるいは取り組みではないが、これらを核として本研究を実施した。また、研究計画を実施した際に予期しなかった困難や当初計画よりも優れた検討項目に気づくことがあり、その際に当初の研究計画・予算を変更して実施した。

４．研究成果

課題１
　平成 29 年度に、課題１への取り組みとして、IC への意図的な電磁妨害を評価するための環境を構築し、また、IC に故障を引き起こし易い妨害周波数を決定するパラメタ及び印加タイミングの抽出について、実施した。
　評価環境の構築では、意図的電磁妨害によるセットアップタイム違反の発生を想定し、故障を引き起こした要因を特定するため、FPGA を搭載したテストボードを用いて、遅延時間が極めて長い加算回路を評価回路として FPGA に実装し、これを用いて故障が生じたタイミングをモニタリングすると共に、既存設備である電磁界計測装置システムを改良して用いて、低ノイズで高精度に IC 内部の電気的な変化をモニタリング可能な環境を構築した。
なお、当初計画していた課題１の内容のうち、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ための研究開発については、ほかの拡張した課題を優先させることにして、実施から外した。
　これらの環境構築は実験的検討の基盤であり、早期に整備した効果は大きく、当初予定した成果を得られた。

課題２
　平成 29 年度に課題１の成果である評価環境と電磁妨害評価の成果を基にして、IEMI による故障発生の有無は注入周波数に大きく依存することから、課題２の取り組みとして機器への妨害電磁波の注入効率を決定するパラメタを抽出するために、伝導及び放射雑音をカバーする連続波及びパルス波を IC に注入できる装置を整備した。これを用いて、課題３の計画を前倒しさせて、注入した信号の伝搬の様子を前述したモニタリング環境を用いて観測し、IC 内部の妨害電磁波の強度分布と、各測定点における伝達関数を求めた。
　さらに、上述により得られた周波数及び時間領域の計測結果を基に妨害波の伝達効率を決定する素子配置や配線パターンを抽出すると共に、意図的な電磁妨害より生ずる IC 内部の評価回路からの故障を示すデータ出力を観測することで、故障が発生しやすい妨害波の印加タイミングに関するリスク評価について基礎的な知見を得た。
　得られた知見を実アプリケーションである暗号デバイスに応用し、得られた知見の汎用性を示したものであり、こうした結果は当該分野において最も権威有る論文誌（IEEE Transaction on Electromagnetic Compatibility）への採録が決定して Early Access に掲載された。
　平成 29 年度に課題 2 への取り組みとして、故障注入により出力される誤り暗文を用いたリスク評価のためのパルス発生器を用いて意図的な機器妨害による故障発生のビット変化パターンの評価を実施したが、位相の影響などの高精度な故障解析を行うための波形計測蓄積において、波形計測オシロスコープから転送するデータ量が当初想定していた以上に大幅に増大したので研究計画を変更した。平成 30 年度にかけて測定環境の充実として計測波形の保存のための計測設備の整備を行い、故障時ビット変化パターンの大量データからの分析に基づく評価手法に取り組んだ。成果に基づき研究手法を改善して、意図的電磁妨害による故障注入について位相の影響の成果を得られた。これを故障注入により出力される誤り暗文を用いたリスク評価の計測設備と総合的に運用することで、機器妨害時のビット変化パターンについてより詳細な評価を行えるようになった。
　また、実システムは出力を直接観測することが困難な場合が多いため、故障発生時に漏えいする電磁情報から誤り出力を推定する手法についても開発を進めて、平成 31（令和元）年度の課題 3 の拡張に結びついた。これを優先するために、当初計画の課題２に含まれていた、他のブロック暗号・ストリーム暗号についての解析は進捗を見送った。

課題３
　平成 30 年度に、課題３の電磁妨害耐性の評価シミュレーション手法の開発について、課題 2 の計測波形の解析評価の成果から、出力する誤り暗文のビット変化パターンの解析に基づくよ

りも、故障注入時の計測波形の解析に基づく評価を発展させることにより優れた手法が可能になるとの知見を得て、計測波形に基づく評価手法の開発を選択すべきであるとの方針を得て、研究計画を変更した。

また、研究計画の実施中に成果に基づき研究手法を改善して、機器の配線・配置や部品・基板など素子を含む物理構造を扱う時間領域差分モデルに基づいて、配線接続部の条件が信号伝達特性と妨害耐性に与える影響、あるいは情報機器からの画像情報の電磁的漏えいを含めて検討課題を追加して、配線の物理構造のモデルと妨害耐性の評価を行える簡易モデルを提案するなど新たな成果を得た。また、実システムでは機器が相互に接続され構成されることから、相互接続が生じた場合の妨害耐性の評価についても検討を行った。

これらの成果は国際及び国内の研究会合で報告して隣接分野の研究者との議論を行った。

令和元（平成 31）年度に、電磁妨害による暗号機器への故障注入攻撃について、意図的な電磁妨害による故障注入の注入する周波数や位相などによって出力される誤り暗文に発生するビット誤りの変化について、暗号処理と関連付けて分析する手法を発展させ、暗号処理に誤りが混入したタイミングを判定し、暗号機器への故障利用攻撃による秘密鍵の解析可能性リスクを評価する手法を実証した。

また、平成 30 年度に課題２の成果に基づいて課題３に関連して検討を行った、出力が直接観測出来ない場合に適用可能なサイドチャネル情報を用いた誤りバイト推定手法の高精度化のために、サイドチャネル情報の計測手法について詳細な検討を行い、課題３を拡張した。具体的には、暗号モジュールを対象とし、故障注入時に生ずるサイドチャネル波形の時間領域における振幅方向の計測分解能に着目し、解析に適した分解能を選択するためにこれまでに研究グループが知見を蓄積してきた秘密鍵解析手法を応用し、課題３を拡張して実験的検討を進めた。

令和元（平成 31）年度に、故障注入攻撃への耐性の評価と情報機器の電磁妨害耐性・情報漏えいの評価手法について計画を実施したほか、さらにサイドチャネル波形の計測分解の影響や画像情報信号方式による電磁的情報漏えいの評価にも課題を拡張して知見を得た。機器設計時における電磁的情報漏えいと電磁妨害耐性を評価可能な汎用的な電磁界シミュレーション手法の開発について、実験に基づき暗号モジュール等と線路それぞれに対して行った妨害耐性評価結果の結合による情報通信機器の電磁的情報漏えい耐性の評価の開発を検討した。情報機器からの画像情報の電磁的漏えいについて、機器の物理的構造モデルと画像情報信号表現の影響の実験的評価を行って、対策を提案した。また、妨害波の機器内部への伝搬を効率的にコントロールするために、これまでに開発してきた配線接続部における信頼性モデルを適用する評価を取りまとめた。

令和 2 年度には、前年度の暗号機器の電磁妨害耐性の評価手法開発において、誤り暗文の分析のための波形計測が高分解能である場合でも取得性が制限される結果を得たため、高分解能計測の影響について、リスク評価の追加実験と評価手法の再検討を実施した上で研究計画を変更し、情報機器の放射電磁波情報漏えいの対策開発と情報漏えい抑制対策の検討を追加で実施した。

また、令和２年度に、出力が直接観測出来ない場合に適用可能なサイドチャネル情報を用いた誤りバイト推定手法の高精度化のために、サイドチャネル情報の計測手法について詳細な検討を行った。具体的には、暗号モジュールを対象とし、誤り暗文の分析のための故障注入時に生ずるサイドチャネル波形の時間領域における波形計測が高分解能でも取得性が制限される結果を得たため、計画を見直し、計測分解能の影響を再検討する実験的検討を進めた結果、波形取得の分解能を高めた条件でも秘密鍵の取得性は向上しないことを明らかにした。

機器設計時における電磁的情報漏えいと電磁妨害耐性を評価可能な汎用的な電磁界シミュレーション手法の開発について、実験に基づき暗号モジュール等と線路それぞれに対して行った妨害耐性評価結果の結合による情報通信機器の電磁的情報漏えい耐性を検討した。

情報機器からの画像情報の電磁的漏えいについて、機器の物理的構造モデルと画像情報信号表現の影響を考慮した実験的評価により、画像の傍受により生じるリスクの評価手法を提案し、放射電磁波情報漏えいを抑制可能な 2 値画像の設計を提案した。また、高解像度の映像情報を扱う機器内の信号伝送と情報漏えいの関係に着目し、漏えい電磁波の強度とその発生タイミングの推定結果から漏えい源のモデルを生成する手法を提案し、その有効性を確認した。また、妨害波の機器内部への伝搬を効率的にコントロールするために、これまでに開発してきた相互接続部における信頼性モデルを適用する評価を取りまとめた。

課題３では新しい検討項目を取り入れてかなり拡張したので、実験により得られる S パラメタや伝達関数などが正確かの検証や、一般的な PC で計算可能な簡素なモデルの構築については、優先度を見送ることとした。

これらの成果を当該分野における権威ある国際会議で多数の報告に結び付けた。これらの成果は国際及び国内の研究会合で報告して隣接分野の研究者との議論を行った。

課題４

令和元年度から令和 2 年度にかけて、電磁妨害による暗号機器への故障注入攻撃について、注入信号の周波数や位相などによって出力される誤り暗文に発生するビット誤りの変化について、暗号処理と関連付けて分析する手法を発展させ、暗号処理に誤りが混入したタイミングを判定し、暗号機器への故障利用攻撃による秘密鍵の解析可能性リスクを評価する手法を実証した。

また、配線パターンなどの幾何的な形状及び、EMC 対策用ノイズ抑制素子の組み合わせによる対策技術を検討した。課題３として拡張した検討項目のうち、機器の物理的構造モデルと画像情報信号表現の影響を考慮した実験的評価から、これらについて対策技術を考案した。

５．主な発表論文等

〔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 Nakamura Ko、Hayashi Yu-Ichi、Mizuki Takaaki、Sone Hideaki	４．巻 Early Access
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	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27件（うち招待講演　1件／うち国際学会　1件）

１．発表者名 Birukawa, Ryota, Mizuki, Takaaki, Sone, Hideaki, Hayashi, Yuichi
２．発表標題 A Practical Evaluation Method for EM Information Leakage by Using Audible Signal
３．学会等名 2019 Joint International Symposium on Electromagnetic Compatibility and Asia-Pacific International Symposium on Electromagnetic Compatibility, Sapporo (EMC Sapporo & APEMC 2019)
４．発表年 2019年

１．発表者名 Aihara, Kenji, Hayashi, Yuichi, Mizuki, Takaaki, Sone, Hideaki
２．発表標題 Study on the Influence of Contact Surfaces Roughness on High-Frequency Signal Transmission Characteristics
３．学会等名 2019 Joint International Symposium on Electromagnetic Compatibility and Asia-Pacific International Symposium on Electromagnetic Compatibility, Sapporo (EMC Sapporo & APEMC 2019)
４．発表年 2019年

１．発表者名 Takenouchi, Mitsuki, Saga, Naoto, Hayashi, Yuichi, Mizuki, Takaaki, Sone, Hideaki
２．発表標題 A Method for Distinguishing Faulty Bytes in Cryptographic Device Using EM Information Leakage
３．学会等名 2019 Joint International Symposium on Electromagnetic Compatibility and Asia-Pacific International Symposium on Electromagnetic Compatibility, Sapporo (EMC Sapporo & APEMC 2019)
４．発表年 2019年

１．発表者名
Ryota Birukawa, Yu-ichi Hayashi, Takaaki Mizuki, Hideaki Sone

２．発表標題
A study on an Effective Evaluation Method for EM Information Leakage without Reconstructing Screen

３．学会等名
2019 International Symposium on Electromagnetic Compatibility - EMC EUROPE

４．発表年
2019年

１．発表者名
内海航平，林優一，水木敬明，曽根秀昭

２．発表標題
サイドチャネル波形の計測分解能が相関電力解析に与える影響

３．学会等名
計測自動制御学会東北支部55周年記念学術講演会

４．発表年
2019年

１．発表者名
竹之内光樹，篠田悠斗，林優一，水木敬明，曽根秀昭

２．発表標題
印加位相を考慮した意図的電磁妨害による故障注入手法に関する検討

３．学会等名
計測自動制御学会東北支部55周年記念学術講演会

４．発表年
2019年

１．発表者名
Ryota Birukawa, Yu-ichi Hayashi, Takaaki Mizuki, Hideaki Sone

２．発表標題
A Study on an Efficient Evaluation Method for EM Information Leakage by Changing Display Color (from SCIS 2019)

３．学会等名
The 14th International Workshop on Security (IWSEC 2019)（招待講演）

４．発表年
2019年

１．発表者名
内海航平，林　優一，水木敬明，曽根秀昭

２．発表標題
サイドチャネル波形の計測分解能が秘密鍵の取得性に与える影響

３．学会等名
2019年電子情報通信学会ソサイエティ大会

４．発表年
2019年

１．発表者名
内海航平，林　優一，水木敬明，曽根秀昭

２．発表標題
サイドチャネル波形の計測分解能が秘密鍵の取得性に与える影響の測定

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
2019年

１．発表者名
竹之内 光樹，林優一，水木敬明，曽根秀昭

２．発表標題
暗号ハードウェアにおける意図的な電磁妨害による故障発生に関する研究

３．学会等名
IEEE EMC Society Sendai Chapter 学生研究発表会

４．発表年
2020年

１．発表者名
尾留川 良太，林優一，水木敬明，曽根秀昭

２．発表標題
画面情報の制御による情報機器からの電磁情報漏えいの効率的評価に関する研究

３．学会等名
IEEE EMC Society Sendai Chapter 学生研究発表会

４．発表年
2020年

１．発表者名
神津 岳志，林優一，水木敬明，曽根秀昭

２．発表標題
漏えい電磁波からの画面再構成に関する検討

３．学会等名
IEEE EMC Society Sendai Chapter 学生研究発表会

４．発表年
2020年

１．発表者名
Naoto Saga, Takuya Itoh, Yu-ichi Hayashi, Takaaki Mizuki, Hideaki Sone

２．発表標題
Study on the effect of clock rise time on fault occurrence under IEMI

３．学会等名
2018 IEEE International Symposium on Electromagnetic Compatibility and 2018 IEEE Asia-PacificSymposium on Electromagnetic Compatibility (EMC/APEMC)

４．発表年
2018年

１．発表者名
Ryota Birukawa, Gentaro Tanabe, Yu-ichi Hayashi, Takaaki Mizuki, Hideaki Sone

２．発表標題
A study on an evaluation method for EM information leakage utilizing controlled image displaying

３．学会等名
2018 IEEE International Symposium on Electromagnetic Compatibility and 2018 IEEE Asia-Pacific Symposium on Electromagnetic Compatibility (EMC/APEMC)

４．発表年
2018年

１．発表者名
相原 健志，林 優一，水木 敬明，曽根 秀昭

２．発表標題
接触部の荷重が信号伝達特性に与える影響の測定法に関する検討

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
2018年

１．発表者名
竹之内光樹，林　優一，水木敬明，曽根秀昭

２．発表標題
意図的な電磁妨害による故障発生に印加位相が与える影響に関する検討

３．学会等名
電子情報通信学会2018年ソサイエティ大会

４．発表年
2018年

１．発表者名
相原健志，林　優一，水木敬明，曽根秀昭

２．発表標題
接触表面粗さが高周波伝達特性に与える影響に関する基礎的検討

３．学会等名
電子情報通信学会2018年ソサイエティ大会

４．発表年
2018年

１．発表者名
Kenji Aihara, Yu-ichi Hayashi, Takaaki Mizuki and Hideaki Sone

２．発表標題
Study on the Effect of Surface Condition on High-Frequency Transmission Characteristics

３．学会等名
電子情報通信学会機構デバイス研究会(IS-EMD2018)

４．発表年
2018年

１．発表者名
Naoto Saga, Yu-ichi Hayashi, Takaaki Mizuki and Hideaki Sone

２．発表標題
A Specification Method of Faulty Bytes in Cryptographic Module Using EM Information Leakage

３．学会等名
電子情報通信学会環境電磁工学研究会（EMCJWS2018）

４．発表年
2018年

１．発表者名
Mitsuki Takenouchi, Yu-ichi Hayashi, Takaaki Mizuki and Hideaki Sone

２．発表標題
Influence of IEMI considering injected signal phase on faulty outputs in a cryptographic module

３．学会等名
電子情報通信学会環境電磁工学研究会（EMCJWS2018）

４．発表年
2018年

１．発表者名
尾留川良太，林優一，水木敬明，曽根秀昭

２．発表標題
表示色の操作によるディスプレイからの電磁的情報漏えいの効率的な評価に関する検討

３．学会等名
2019年暗号と情報セキュリティシンポジウム(SCIS2019)

４．発表年
2019年

１．発表者名
杉本藍莉，藤本大介，林優一，水木敬明，曽根秀昭

２．発表標題
周波数選択による暗号機器の情報漏えい評価の効率化に関する検討

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
2017年

１．発表者名
田辺弦太郎，林優一，水木敬明，曽根秀昭

２．発表標題
表示画像の選択を用いた電磁情報漏えい評価手法に関する検討

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
2017年

１．発表者名
伊東拓哉，林優一，水木敬明，曽根秀昭

２．発表標題
意図的な電磁妨害による故障発生にクロック信号の立ち上がり時間が与える影響に関する検討

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
2017年

１．発表者名
田辺弦太郎，林優一，水木敬明，曽根秀昭

２．発表標題
描画情報の選択による放射電磁波制御を利用した情報漏えい評価手法の検討

３．学会等名
2017年電子情報通信学会ソサイエティ大会

４．発表年
2017年

１．発表者名
杉本藍莉，林優一，水木敬明，曽根秀昭

２．発表標題
周波数選択フィルタを用いた相関電力解析の評価の効率化に関する検討

３．学会等名
2017年電子情報通信学会ソサイエティ大会

４．発表年
2017年

１．発表者名
Naoto Saga, Yu-chi Hayashi, Takaaki Mizuki, and Hideaki Sone

２．発表標題
A Method of Fault Detection in Encryption Device Based on Leaked EM Information from Adder Circuit

３．学会等名
電子情報通信学会EMC Joint Workshop（国際学会）

４．発表年
2017年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	林　優一 (Hayashi Yuichi) (60551918)	奈良先端科学技術大学院大学・先端科学技術研究科・教授 (14603)	
研究分担者	水木　敬明 (Mizuki Takaaki) (90323089)	東北大学・サイバーサイエンスセンター・准教授 (11301)	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関