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　 ７ 日現在

機関番号：１５３０１
研究種目：基盤研究(B)（一般）
研究期間：2019～2022
課題番号：１９Ｈ０４１１０

研究課題名（和文）信号対雑音比に基づく暗号ハードウェアへのサイドチャネル攻撃対策設計手法の開発

研究課題名（英文）Design method development of side-channel attack countermeasures for cryptographic hardware based on signal-to-noise ratio of electromagnetic leakage

研究代表者

五百旗頭　健吾（Iokibe, Kengo）

岡山大学・自然科学学域・助教

研究者番号：１０４２０４９９

交付決定額（研究期間全体）：（直接経費）　　12,300,000円

研究成果の概要（和文）：標準ブロック暗号であるAESのFPGA実装を評価対象として、サイドチャネル漏洩の信号対雑音比(SN比)に基づき、暗号実装のサイドチャネル攻撃(SCA)耐性設計手法確立に向けた検討を行った。まず、サイドチャネル漏洩のSN比同定法を提案し、暗号回路内のサイドチャネル漏洩源を暗号回路の設計情報より同定する手法を確立した。さらにSN比に基づいてサイドチャネル漏洩経路の伝達係数を設計することでSCA耐性を制御する可能性を示した。

研究成果の学術的意義や社会的意義
測定に基づくサイドチャネル攻撃に対する安全性評価については実用化された方法があるが、評価結果から設計へとシームレスに接続された手法はまだ確立されていない。IoT時代に入り、情報セキュリティの重要性が増している中において、サイドチャネル攻撃耐性設計手法の確立することは、限られた製品設計開発期間において高いセキュリティ性能を実現するために不可欠な技術であり社会的意義は大きい。また、古典的な電気回路学や電磁気学の知識と新しい暗号理論を融合する、暗号ハードウェア設計手法の開発は学術的にも新しく、価値の大きな成果となり得る。

研究成果の概要（英文）：We have studied the design of side-channel attack (SCA) resistant cryptographic implementations based on the signal-to-noise ratio (SN ratio) of side-channel leakage, using an FPGA implementation of the standard block cipher AES as an evaluation target. First, we proposed a method for identifying the signal-to-noise ratio of side-channel leakage and established a method for identifying the sources of side-channel leakage in cryptographic circuits from the design information of the cryptographic circuit. Furthermore, we showed the possibility of controlling SCA resistance by designing transfer coefficients of side-channel leakage paths based on the signal-to-noise ratio.

研究分野：電磁情報セキュリティ

キーワード：サイドチャネル攻撃　暗号　情報セキュリティ　IoT　信号対雑音比

１．研究開始当初の背景

IoT 機器において、十分な情報セキュリティ性能を実現するため暗号機能の実装が不可欠となっている。それと相まって、暗号の実装ハードウェアから漏洩する電磁ノイズ等の物理的な挙動を利用するサイドチャネル攻撃(SCA)が高度化しその脅威が高まっている。それと同時に、SCA 対策技術の開発も進んでいる。IoT 機器に暗号機能をハードウェア実装する場合、製品サイクルの早い IoT 機器において十分な SCA 耐性を実現する上での現在の課題は、SCA 対策の設計手法が未確立という点にある。SCA 対策の設計手法開発のためには、暗号回路の設計情報に基づく SCA 耐性予測を実現し、その予測に基づき設計目標を設定することが不可欠である。また設計目標とする指標にはプリント回路基板などのハードウェア設計と親和性の高い物理量を使用する必要がある。なぜなら、一般にハードウェア設計者が暗号技術や SCA について十分な知識を有する可能性は低い。そこでハードウェア設計と親和性の高い物理量によって設計指標を定めることで、暗号技術や SCA の知識を必要とせずに SCA 対策設計を実現できる。

２．研究の目的

研究代表者らは暗号回路の設計情報である HDL データに基づき SCA 耐性を予測する手法を検討してきた。その中で、暗号回路から漏洩するサイドチャネル波形の信号対雑音比(SN 比)と SCA 耐性の関係が解析式に従うことを示し[1]、その関係式を SN 比の実測やシミュレーションにより同定できることを示している[2]。SN 比はアナログ回路の伝達特性と親和性があり、ハードウェア設計者に馴染みのある量である。そこで、本研究では SN 比を指標として要求される SCA 耐性を実現する暗号ハードウェア設計手法を開発する。

本研究で開発する設計手法の特長は、目標とする SCA 耐性を、SN 比を指標として定量的に設定できることにある。既存の SCA 耐性評価法は、図 1 の(既存 A)のように、試作した暗号ハードウェアに対して実際に SCA を実行する方法、あるいは(既存 B)のように、統計学の検定手法により規定の SCA 耐性を満足しているかどうかを検定する方法の２つである。前者は試作ハードウェアの SCA 耐性は判定できるが、規定レベルを実現するための設計目標値を設定できない。後者は試作ハードウェアが SCA 耐性の目標レベルを満足しているか満足していないかのみを判定でき、やはり設計指標の目標値は設定できない。それに対し、本研究では、設計情報に基づくシミュレーションより SN 比に対する SCA 耐性の変化を表す曲線を決定し、規定の SCA 耐性を実現する SN 比の目標値を設定可能な、つまり、適切な設計目標を設定でき、要求仕様に対して過不足のない SCA 耐性設計を実現できる設計手法の開発を目的とした。

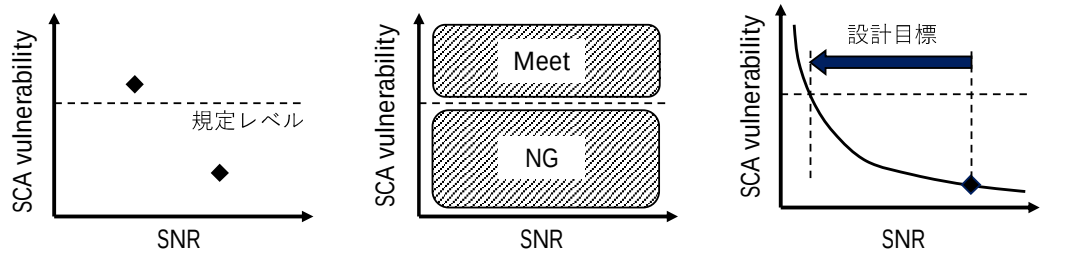


図 1　本研究で開発する設計手法と従来の安全性評価手法の比較

３．研究の方法

(1)　暗号アルゴリズムと実装ハードウェア

本研究では国際標準暗号の一つである AES (Advanced Encryption Standard)をサイドチャネル攻撃対象の暗号アルゴリズムとした。AES は IoT 機器、車載機器、ネットワーク機器、および各種コンピュータと幅広く実用されている。また AES 以外のブロック暗号でも AES と類似のアルゴリズムが採用されており、AES を評価対象とすることで汎用性の高い SCA 耐性設計手法の確立につながる。

AES では 128、192、および 256 ビットの 3 種類の長さの秘密鍵が使用される。いずれの鍵長に対しても SCA は可能であるが、実験効率を上げるため、本研究では最も短い 128 ビットの

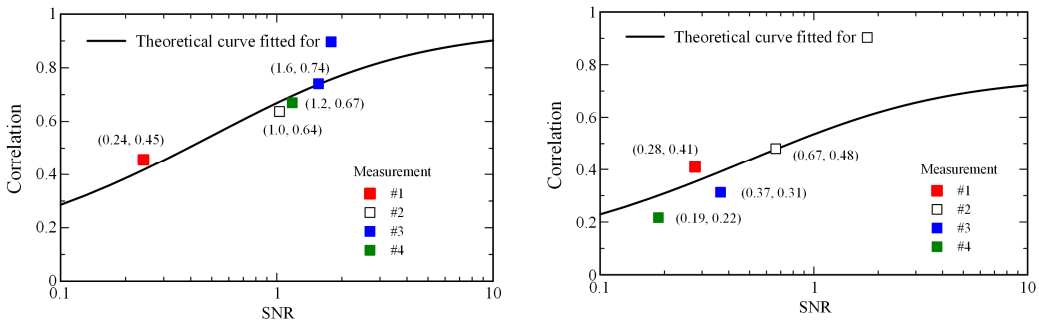
図 2　攻撃対象とした暗号モジュール

秘密鍵を使用した。

AES-128 アルゴリズムの SCA 耐性を評価するため、AES-128 を FPGA に実装した。Altera 社の Cyclone V シリーズの FPGA を搭載した評価用プリント回路基板を、攻撃対象の暗号モジュールとして使用した。暗号モジュールの外観を図 2 に示す。AES-128 を実装した FPGA、およびその電源系回路に実装されるデカップリングキャパシタ (C79-C82) の実装位置も示している。

(2) サイドチャネル攻撃手法

ブロック暗号に対する SCA 手法として代表的な相関電力解析 (CPA) を使用した。CPA はブロック暗号に対する SCA 手法として最も強力であると考えられ、CPA に対する耐性を評価することにより、あらゆる SCA に対する耐性を保証することを想定している。



(a) 模擬漏洩波形の場合　　(b) 実測漏洩波形の場合

図 3 同定されたサイドチャネル漏洩の SN 比の検証

4．研究成果

(1) サイドチャネル漏洩の SN 比同定[3][4]

サイドチャネル漏洩は 4 つの成分で構成されている。一つは攻撃者が注目する暗号処理の中間値と相関のある成分(信号成分)、残りの三成分は無相関な成分(ノイズ成分)である。SN 比の同定には信号成分と、ノイズ成分のうち暗号化されるデータに依存して変化する 2 成分の和をそれぞれ同定する必要がある。そこで、信号成分を発生させず、ノイズ成分だけを発生させる特殊な平文セットを作成し、サイドチャネル漏洩波形より信号成分とノイズ成分を分離することを試みた。

標準ブロック暗号 AES を対象とした検証の結果、提案した平文セットを用いた提案法により、模擬的な漏洩波形の SN 比を精度良く同定できた。実測した漏洩波形に対しても実用的な精度で SN 比を同定できた。図 3 は同定された SN 比の評価結果を示している。図 3 の各グラフには、同定した SN 比に加えて SN 比と相関係数の関係を表す理論曲線を示している。ここで言う相関係数は攻撃者が注目する中間値と漏洩波形の変化の相関係数であり、高い相関はサイドチャネル漏洩強度が高いことを意味する。相関係数が異なる 4 条件で同定された SN 比のうち一つの条件で理論曲線にフィッティングし、残りの 3 条件が理論曲線と一致するかどうかを確認した。その結果、いずれも理論曲線と良い一致を示した。この結果より、提案手法によりサイドチャネル漏洩の SN 比を実用的な精度で動的できることを確認した。

なお、実測波形では模擬波形より誤差が大きい。その原因について検証し、攻撃者が注目する中間値を算出時より前に実行される演算によって発生するノイズ成分が影響しているとの示唆を得た。したがって、その影響を排除する平文セットを作成することにより、SN 比の同定精度の向上が可能である。

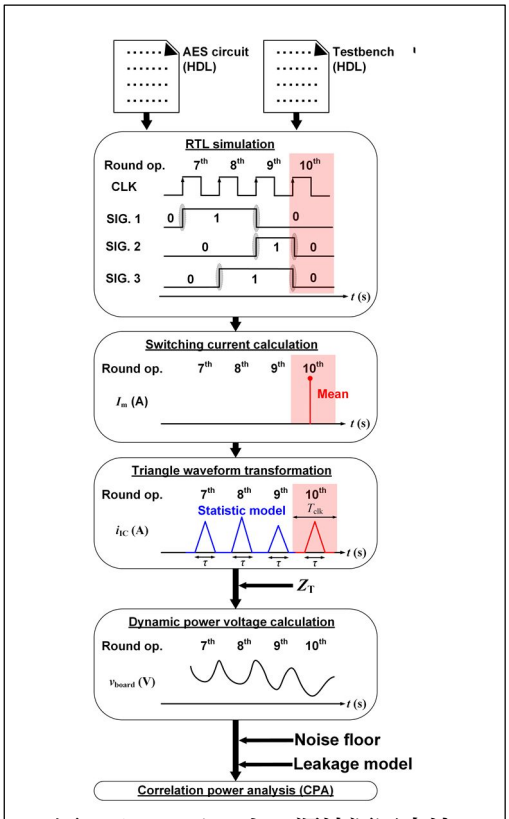
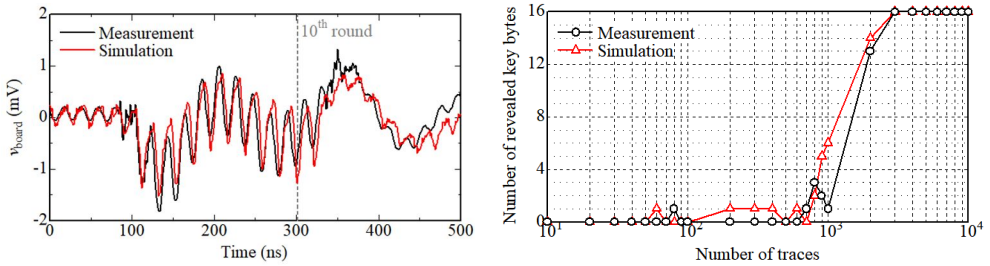


図 4 サイドチャネル漏洩源同定法



(a) 漏洩波形　　(b) 解読された暗号鍵の byte 数

図 5 同定した漏洩源を用いたサイドチャネル漏洩シミュレーション

(2) 設計情報に基づくサイドチャネル漏洩源同定[5][6]

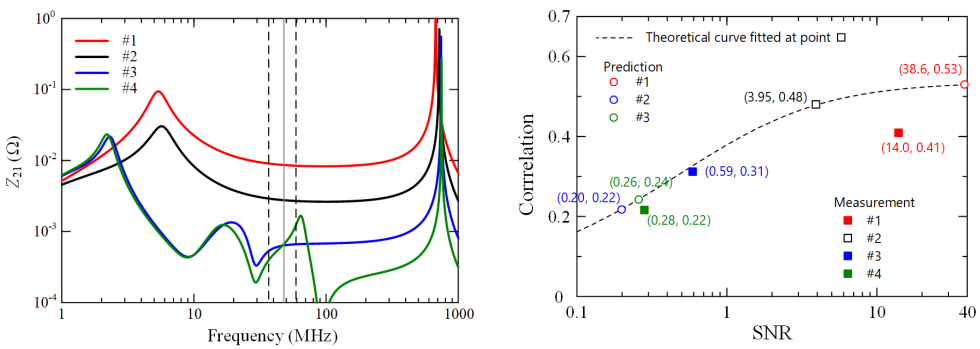
製品設計の段階、つまり製品試作前に SCA 耐性設計をするためには、設計情報に基づきサイドチャネル漏洩の SN 比を同定する必要がある。その実現のためにはサイドチャネル漏洩を暗号回路の設計情報より同定する必要がある。そこで、FPGA 実装した AES 回路を検討対象として、FPGA 内部のサイドチャネル漏洩源を、レジスタ転送レベルのロジックシミュレーションに基づき同定する手法を構築した。

図 4 に示すように AES 回路の設計情報である HDL ファイルを入力としてロジックシミュレーションより FPGA の消費電力と関係するスイッチング電流を算出し、その電流波形を三角波パルスで近似することで漏洩源を同定した。さらに漏洩源からサイドチャネル漏洩の観測ポートへの伝達関数より、サイドチャネル漏洩を予測した。

図 5(a)は予測したサイドチャネル漏洩波形(赤)であり、実測波形(黒)とよく一致している。さらに同様の漏洩波形を 10000 平文に対して算出し、サイドチャネル解析を実行した。その結果を図 5(b)に示している。横軸がサイドチャネル解析に用いた波形数を表しており、縦軸が解読された鍵ブロックの数(byte 数)を表している。シミュレーション(赤)と実測(黒)の曲線はよく一致しており、どちらも 700 波形付近で解読された byte 数が急激に増加し始め、3000 波形で全 16 bytes が解読されている。この結果より、暗号回路内に発生するサイドチャネル漏洩源を、暗号回路の設計情報より精度良く同定する手法を確立した。

(3) SN 比に基づく暗号モジュールのサイドチャネル攻撃耐性設計法[7]

サイドチャネル漏洩源の漏洩強度と要求されるサイドチャネル漏洩強度との比率を求め、それを SN 比低減量の目標値としてサイドチャネル漏洩経路を設計することで、要求される SCA 耐性を実現可能かどうか検討した。図 2 に示したデカップリングキャパシタ C79－C82 の実装状態を変更することでサイドチャネル漏洩経路の伝達インピーダンスを図 6(a)のように変化させた。#2 を基準とし、伝達インピーダンスが大きい#1、および小さい#3 と#4 の 3 通りの状態について、SN 比より CPA による攻撃結果である相関係数を予測した。その結果、図 6(b)に示すように、#4 については SN 比より予測した相関係数が実測結果と一致した。その一方で、#1 および#3 については、誤差のある結果となった。つまり、SN 比に基づき SCA 耐性を予測する、つまり、SCA 耐性を設計できる可能性を示唆する結果を得られたと同時に、改善の必要性も確認された。



(a) 漏洩経路の伝達インピーダンス　　(b)予測結果

図 6　SN 比に基づく SCA 耐性予測

＜引用文献＞

[1] Y. Yano, T. Teshima, K. Iokibe, Y. Toyota, “Signal-to-Noise Ratio Measurements of Side-Channel Traces for Establishing Low-Cost Countermeasure Design,” 2017 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC 2017), WE-PM-7-2, pp. 93-95, Seoul, Korea, 2017.

[2] K. Iokibe, T. Teshima, Y. Yano, and Y. Toyota, “Extension of signal-to-noise ratio measurement method to byte-by-byte side-channel attack,” In Proceedings of the 2018 IEEE International Symposium on Electromagnetic Compatibility and 2018 IEEE Asia-Pacific Symposium on Electromagnetic Compatibility (EMC/APEMC), pp. 745-748, Singapore, June 2018.

[3] Y. Yano, T. Teshima, K. Iokibe, and Y. Toyota, "Experimental Identification of Relationship between Leakage Trace SNR and Correlation Coefficient in Differential Power Analysis," 2019 Joint International Symposium on Electromagnetic Compatibility and Asia-Pacific International Symposium on Electromagnetic Compatibility, Sapporo(EMC Sapporo & APEMC 2019), FriAM1C.4, pp. 797-800, Sapporo, Japan, Jun. 3-7, 2019.

[4] K. Iokibe, M. Himuro, and Y. Toyota, "A Study for Improving Signal-to-Noise Ratio Measurement Method in Side-Channel Information Leakage of Cryptographic Hardware," 2022 IEEE International Symposium on Electromagnetic Compatibility, Signal & Power Integrity (EMC+SIPI 2022), pp. 294-298, Spokane, USA, Aug. 1-5, 2022.

[5] Y. Yano, K. Iokibe, T. Teshima, Y. Toyota, T. Katashita, and Y. Hori, "Evaluation of Side-channel Leakage Simulation by Using EMC Macro-model of Cryptographic Devices," IEICE Transactions on Communications, Vol. E104-B, No. 2, pp. 178-186, Feb. 2021.

[6] M. Himuro, K. Iokibe, and Y. Toyota, "FPGA Switching Current Modeling Based on Register Transfer Level Logic Simulation for Power Side-channel Attack Prediction," 2022 International Symposium on Electromagnetic Compatibility (EMC Europe 2022), pp. 172-177, Gothenburg, Sweden, Sep. 5-8, 2022.

[7] K. Iokibe, M. Himuro, and Y. Toyota, "A Study for Low Calculation Cost Side-Channel Resistance Prediction Based on Transfer Impedance of Leakage Path," 2021 Asia Pacific International Symposium on Electromagnetic Compatibility (APEMC), SS-02-03, Sep.27-30, 2021 (Online).

５．主な発表論文等

〔雑誌論文〕　計6件（うち査読付論文　6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 Yusuke Yano, Kengo Iokibe, Toshiaki Teshima, Yoshitaka Toyota, Toshihiro Katashita, and Yohei Hori	４．巻 E104-B
２．論文標題 Evaluation of Side-channel Leakage Simulation by Using EMC Macro-model of Cryptographic Devices	５．発行年 2021年
３．雑誌名 IEICE Transactions on Communications	６．最初と最後の頁 178-186
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transcom.2020EBP3015	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 Yusuke Yano, Toshiaki Teshima, Kengo Iokibe, and Yoshitaka Toyota	４．巻 -
２．論文標題 Experimental Identification of Relationship between Leakage Trace SNR and Correlation Coefficient in Differential Power Analysis	５．発行年 2019年
３．雑誌名 2019 Joint International Symposium on Electromagnetic Compatibility and Asia-Pacific International Symposium on Electromagnetic Compatibility	６．最初と最後の頁 797-800
掲載論文のDOI（デジタルオブジェクト識別子） 10.23919/EMCSapporo/APEMC44270.2019.9320847	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 Kengo Iokibe, Tomonobu Kan, Yoshitaka Toyota	４．巻 -
２．論文標題 A Study on Evaluation Board Requirements for Assessing Vulnerability of Cryptographic Modules to Side-Channel Attacks	５．発行年 2020年
３．雑誌名 2020 IEEE International Symposium on Electromagnetic Compatibility & Signal/Power Integrity (EMCSI)	６．最初と最後の頁 528-531
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/EMCSI38923.2020.9191655	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 Kengo Iokibe, Masaki Himuro, Yoshitaka Toyota	４．巻 -
２．論文標題 A Study for Low Calculation Cost Side-Channel Resistance Prediction Based on Transfer Impedance of Leakage Path	５．発行年 2021年
３．雑誌名 2021 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC)	６．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/APEMC49932.2021.9597127	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 Kengo Iokibe, Masaki Himuro, and Yoshitaka Toyota	４．巻 -
２．論文標題 A Study for Improving Signal-to-Noise Ratio Measurement Method in Side-Channel Information Leakage of Cryptographic Hardware	５．発行年 2022年
３．雑誌名 2022 IEEE International Symposium on Electromagnetic Compatibility & Signal/Power Integrity (EMCSI)	６．最初と最後の頁 294-298
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/EMCSI39492.2022.9889660	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 Masaki Himuro, Kengo Iokibe, and Yoshitaka Toyota	４．巻 -
２．論文標題 FPGA Switching Current Modeling Based on Register Transfer Level Logic Simulation for Power Side-channel Attack Prediction	５．発行年 2022年
３．雑誌名 2022 International Symposium on Electromagnetic Compatibility (EMC Europe)	６．最初と最後の頁 172-177
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/EMCEurope51680.2022.9900948	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9件（うち招待講演　1件／うち国際学会　1件）

１．発表者名 日室雅貴，五百旗頭健吾，豊田啓孝
２．発表標題 実機のサイドチャネル攻撃耐性評価を目的とした時間・周波数領域相関電力解析
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 2021年

１．発表者名 日室雅貴，五百旗頭健吾，豊田啓孝
２．発表標題 動的 FPGA 電源電流の RTL 解析に基づく電力解析攻撃への耐性予測
３．学会等名 2022年度 暗号と情報セキュリティシンポジウム (SCIS2022)
４．発表年 2022年

１．発表者名
下田洸平，日室雅貴，五百旗頭健吾，豊田啓孝

２．発表標題
FPGA実装したAES回路の模擬スイッチング電流波形に基づくサイドチャネル情報漏洩帯域の考察

３．学会等名
2022年暗号と情報セキュリティシンポジウム（SCIS 2022）

４．発表年
2022年

１．発表者名
菅智信，五百旗頭健吾，豊田啓孝

２．発表標題
暗号ICの電力解析攻撃耐性評価基板に対する要求仕様の検討 ～PDNの伝達インピーダンスの漏洩強度への寄与～

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，HWS2020-25

４．発表年
2020年

１．発表者名
五百旗頭健吾，矢野佑典，豊田啓孝

２．発表標題
電源系デカップリングによるサイドチャネル攻撃対策効果の伝達インピーダンスに基づく予測の試み

３．学会等名
電子情報通信学会環境電磁工学研究会，EMCJ2019-85，pp．23-28

４．発表年
2020年

１．発表者名
竹﨑彬隼，五百旗頭健吾，豊田啓孝

２．発表標題
サイドチャネル攻撃耐性設計を目的とした相関係数と波形数の関係式の検証

３．学会等名
2020年暗号と情報セキュリティシンポジウム(SCIS2020)予稿集，3E2-2

４．発表年
2020年

１．発表者名
下田浩平，日室雅貴，五百旗頭健吾，豊田啓孝

２．発表標題
プリント回路基板のグラウンド分割で生じたコモンモード電流によるサイドチャネル情報漏洩

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
2023年

１．発表者名
Kengo Iokibe

２．発表標題
Countermeasures and Leakage Simulation of Power Side-Channel Attacks

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

１．発表者名
坂上達哉，日室雅貴，五百旗頭健吾，豊田啓孝

２．発表標題
対策設計を目的とした機械学習を用いたサイドチャネル攻撃における暗号情報漏洩タイミングの感度分析による特定

３．学会等名
2022年度(第73回)電気・情報関連学会中国支部連合大会

４．発表年
2022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

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