修士論文

IC 周囲に分布するノイズの振幅値変化に着目した電磁波解析攻撃検知手法に関する研究

和田 慎平

2019 年 3 月 15 日

奈良先端科学技術大学院大学
情報科学研究科

本論文は奈良先端科学技術大学院大学情報科学研究科に
修士 (工学) 授与の要件として提出した修士論文である。

和田 慎平

審査委員：

林 優一 教授　（主指導教員）
岡田 実 教授　（副指導教員）
安本 慶一 教授　（副指導教員）
藤本 大介 助教　（副指導教員）

IC 周囲に分布するノイズの振幅値変化に着目した電磁波解析攻撃検知手法に関する研究*

和田 慎平

内容梗概

近年、暗号モジュールから漏えいする電磁波を利用し秘密鍵を推定する電磁波解析攻撃の脅威が指摘されており、多くの機器が脅威の対象となっている。こうした脅威に対する従来の対策は、暗号アルゴリズム毎に個別の対策の検討が必要となるほか、測定技術の進歩により無効化される可能性があり抜本的な対策となっていない。そこで本論文では、電磁波解析攻撃時に測定フェーズで実行されるプロービングを、暗号モジュールの実装された IC 周囲に分布するノイズを観測することで検知する手法を提案する。本手法は攻撃の過程で必ず実行される測定フェーズの検出を行うことから、暗号アルゴリズムに依存せず多様な機器に適用できる可能性がある。本論文では、前述の手法を実現するために、IC 内部の ADC により IC 周囲のノイズ測定を可能とする実験セットアップを構築すると共に、本セットアップを用いて、プロービングにより生ずるノイズ波形の振幅値の変化を攻撃の兆候として検知可能であることを実験的に示した。

キーワード

サイドチャネル攻撃, 電磁波解析攻撃, 電磁情報セキュリティ, 攻撃検知

*奈良先端科学技術大学院大学 情報科学研究科 修士論文, 2019 年 3 月 15 日.

A Study on Detection Method of Electromagnetic Analysis Attack Using the Change in Amplitude of Noise Around IC*

Shinpei Wada

Abstract

In recent years, electromagnetic analysis (EMA) attacks, which reveal the secret key information of cryptographic module by analyzing the EM radiation from the module, have been reported, and many devices may be a target of this type of threat. The conventional countermeasure methods, however, are specific to each cryptographic algorithm and may not be effective owing to changes or developments in measurement technology. In this paper, a countermeasure against EMA attack is proposed that detects the change in noise amplitude around the IC caused by probing. The proposed method may be applied to many devices independent of cryptographic algorithms because it detects the probe which the attacker used in the EMA attack. The author designed an experimental setup to realize the above mentioned method. The experimental results show that the change in noise amplitude by probing can be detected with the proposed method.

Keywords:

Side-channel Attacks, Electromagnetic Analysis Attack, EM Information Security, Attack Detection

*Master's Thesis, Graduate School of Information Science, Nara Institute of Science and Technology, March 15, 2019.

目 次

図 目 次

表 目 次

1. はじめに

現代の情報化社会においては、IC カード、スマートフォンや PC などの情報機器が普及しており、個人利用やビジネスなどの様々な領域で情報通信が利用されている。このような状況下では、情報セキュリティを確保することが課題であり、機密情報の秘匿や改ざん防止に用いられる暗号は、情報通信を利用する上で欠かすことのできない基盤技術となっている。一方で近年では、暗号アルゴリズムを実装した機器である暗号モジュールに対する物理攻撃の存在が指摘されている。

本章では、現代暗号の安全性、暗号モジュールに対する物理攻撃、電磁波解析攻撃への従来対策とその問題点および本研究の目的について述べる。

1.1 計算量で保証される現代暗号の安全性

インターネットなどの通信路上で転送されるデータの内容を第三者から秘匿すること、データの改ざんを防止することを目的に、 AES (Advanced Encryption Standard) [1] や RSA (Rivest-Shamir-Adelman) [2] などの暗号が利用されている。これらの暗号は暗号化・復号化の手順 (暗号アルゴリズム、復号アルゴリズム) が一般に公開されており、NIST などの評価機関やセキュリティ分野の研究者らにより十分な安全性評価がなされている。

暗号に対する理論上の攻撃モデルを図 1 に示す。現代暗号はデータの送信者が暗号鍵と暗号アルゴリズムを用いて平文を暗号化し通信路へ転送する。また、暗号文の受信者は復号鍵と復号アルゴリズムを用いて、転送されてきた暗号文を平文に復号する。暗号に対する理論上の攻撃モデルでは、悪意ある第三者 (攻撃者) が通信路上を転送される暗号文を解読し、盗聴や改ざんを行うことが想定されている。しかし暗号文の解読には暗号鍵または復号鍵が必要であるが、暗号処理に用いられる鍵は 128, 192, 256 bit などの長さとなるため、実際に鍵解析を行い暗号文を解読することは困難であると考えられてきた。すなわち、現代暗号の安全性は鍵解析のための計算量の大きさにより保証されていることになる。

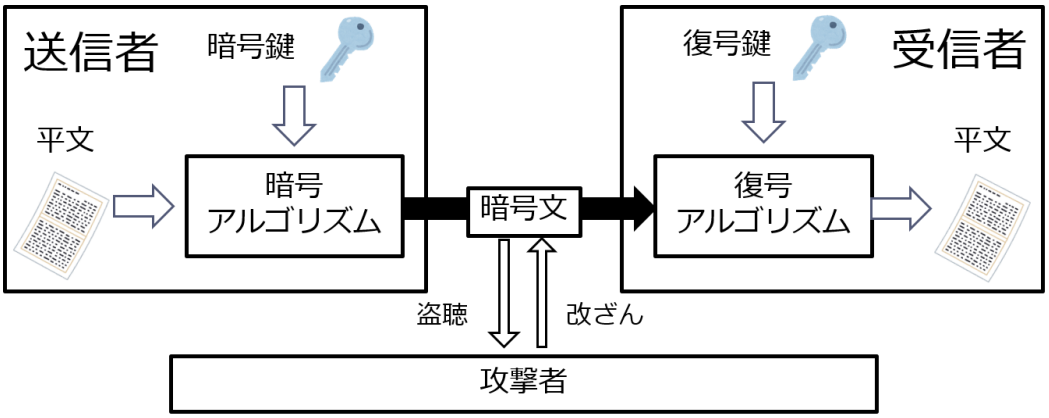


図 1　暗号に対する理論上のモデル

1.2　暗号モジュールに対する物理攻撃

実際の情報システムで暗号を利用する際には、暗号アルゴリズムをソフトウェアまたはハードウェアとして実装した暗号モジュールが利用される。そのため、攻撃者は暗号モジュール内部の回路動作に伴った物理的な情報を測定することも可能である。その結果、攻撃対象の範囲が暗号処理途中の中間データまで拡大し、計算量的に十分安全性が保証されている暗号でも解読される可能性がある。

これまでに、暗号モジュール動作時に生ずる消費電力などのサイドチャネル情報を測定することで、モジュール内部の秘密鍵を解析する物理攻撃が報告されている [3–11]。暗号モジュールに対する物理攻撃は、モジュール加工の有無により侵襲攻撃と非侵襲攻撃に大別される。侵襲攻撃には、モジュールパッケージを開封した上で、光学顕微鏡で暗号モジュールの回路構造を解析したり、マイクロプローブで内部信号を観測する攻撃などがある [3]。侵襲攻撃では暗号モジュール内部の秘密鍵を扱う回路の情報を直接観測することができ、秘密鍵情報を比較的容易に取得することが可能であるが、高価なセットアップと高度な専門知識が必要であり実行可能な攻撃者は限られている。一方で、非侵襲攻撃には暗号モジュールの加工は行わず、暗号処理時におけるモジュールの消費電力や漏えい電磁波などを外部から測定し、秘密鍵情報を取得する攻撃がある [4–11]。特に、非侵襲攻撃の一種である電磁波解析攻撃は暗号処理を行う回路に関する高度な知識を必要

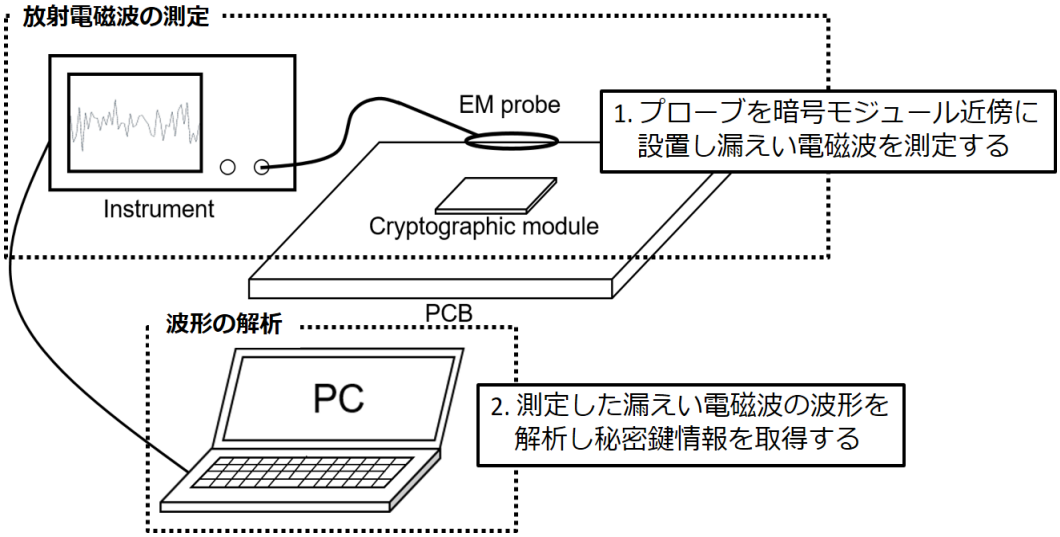


図 2 電磁波解析攻撃の攻撃例

とせず、オシロスコープと PC などの比較的安価なセットアップで攻撃可能である。さらに IC カードなどの耐タンパー性の保証された機器でも脅威の対象となり得るため電磁波解析攻撃への対策が求められている。

1.3 電磁波解析攻撃への従来対策とその問題

電磁波解析攻撃の攻撃例を図 2 に示す。電磁波解析攻撃では、まず攻撃者が暗号処理時に生ずるモジュールからの漏えい電磁波を測定する (測定フェーズ)。続いて、PC などの機器を用いて測定波形を統計的に解析し秘密鍵の推定を行う (解析フェーズ)。これまでに、電磁波解析攻撃への対策手法として測定波形の解析を困難化することに着目したアルゴリズム・回路レベルでの対策手法が提案されている [12–17] 。文献 [12, 13] ではモジュール内部で処理されるデータに乱数によるマスクをかけることで、選択関数 [7] に用いられる中間データの値をランダム化し、漏えい電磁波を用いた鍵解析を困難化する手法が提案されている。また、文献 [14] では CMOS 回路のゲート遷移回数を一定化することでモジュール動作時の消費電力を一定化し、モジュール内部のデータと漏えい電磁波との依存

関係を隠蔽する手法が提案されている。この他にも暗号処理にランダムな遅延を発生させる手法 [15] など様々な対策手法が提案されている。しかし、これらの対策手法は解析フェーズの困難化を目的としているため、暗号アルゴリズム毎に対策手法の有効性が変化する可能性、測定波形の解析手法が高度化した場合に無効化される可能性があり抜本的な対策とはなっていない。

一方で、電磁波解析攻撃では解析フェーズの前に必ず測定フェーズを実行する必要がある。そのため、漏えい電磁波の測定を困難化することで測定波形の解析を未然に防ぐことが可能となり、暗号アルゴリズムに依存せず電磁波解析攻撃全般に適用可能な対策を実現できる可能性がある。また、暗号モジュールからの漏えい電磁波の測定はプローブを用いて行われるが、周囲の電磁界を侵襲せずに電磁界測定を行なうのは物理法則上困難である [18]。そのため、暗号モジュール周囲の電磁環境の変化を観測可能ならば、プローブを用いた測定の兆候を検知可能となり、測定フェーズの実行を困難化できる可能性がある。

1.4 本研究の目的

本研究では、プローブを利用した漏えい電磁波の測定 (プロービング) により IC 周囲に分布するノイズの振幅値が変化する事象を利用した電磁波解析攻撃検知手法を提案し、その実現可能性を示すことを目的とする。そのために、提案手法を実現するための前提について議論した後に、IC 周囲のノイズを測定する機能を実装した機器を用いて、提案手法の実現可能性を確認するための基礎検討を行う。

1.5 本論文の構成

本論文の構成は以下の通りである。2 章では、電磁波解析攻撃への対策として、基板上のノイズ波形の振幅値変化を観測する手法について述べ、電磁波解析攻撃を検知するシステムについて説明する。3 章では、IC 周囲のノイズを測定する機能を実装したマイコンにより、提案手法の実現可能性を確認するための基礎検討を行う。4 章では、3 章で得られた実験結果をもとに発生した事象に対する考察

を行い、実験結果から考えられるプローブ接近の判別方法と攻撃検知精度を低下させる可能性について論ずる。5 章では本論文のまとめを述べる。

2. IC 周囲の電磁環境の変化を観測するための手法

本章では、電磁波解析攻撃においてプロービングが実行されているときに発生する、IC 周囲に分布するノイズの振幅値変化について論じ、その事象を利用することで電磁波解析攻撃を検知する手法を提案する。続いて、提案する電磁波解析攻撃検知手法を実現するシステムの例を示し、提案手法を実現するための前提について論ずる。

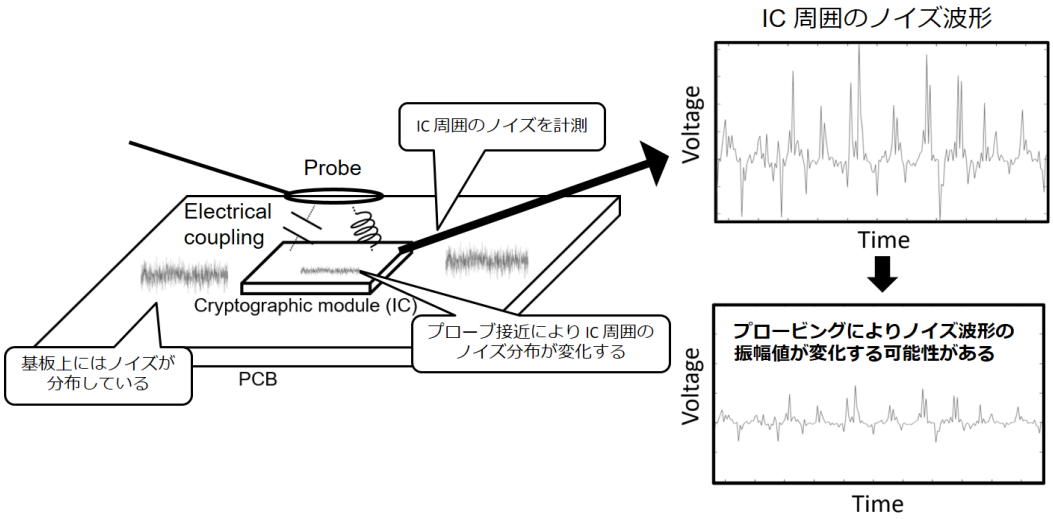


図 3　プロービングによるノイズ波形の振幅値変化

2.1　ノイズの振幅値測定に基づく電磁環境の変化の観測

提案手法のアイディアを図 3 に示す。電磁波解析攻撃では、攻撃者が暗号モジュールからの漏えい電磁波を測定した後に、その測定波形を統計的に解析することで秘密鍵の推定が行われる。特に、暗号モジュール近傍で漏えい電磁波を測定することが可能な場合には、漏えい電磁波以外の雑音信号の影響を低く抑えられるため、高精度に漏えい電磁波を測定することが可能となる。一方で暗号モジュール近傍にプローブが設置される状況下では、プローブと暗号モジュールを

搭載した IC や基板上の配線などとの間に電磁界結合が生じ 、それに伴い IC 周囲の電磁環境が変化する。例えば、プロービングにより IC からの漏えい電磁波を測定した場合には、プローブと IC または周辺配線などとの間に電磁界結合が生じ、IC 周囲に分布するノイズの振幅値に変化が生ずる。このノイズの振幅値変化を暗号モジュール側で観測することが可能ならば、電磁波解析攻撃の兆候として検知し漏えい電磁波の測定を困難化することができる。そこで本研究では、暗号モジュール近傍で実行される電磁波解析攻撃を対象に、IC 周囲のノイズを測定し、その測定波形の振幅値から暗号モジュール近傍で実行される電磁波解析攻撃を検知する手法を提案する。本手法は、プローブが周囲の電磁界を侵襲することなく測定を行なうのは困難であるという現象に基づいている。そのため、暗号モジュール近傍でのプロービングによる漏えい電磁波の測定を必要とする攻撃全般に適用可能な対策を実現できる可能性がある。

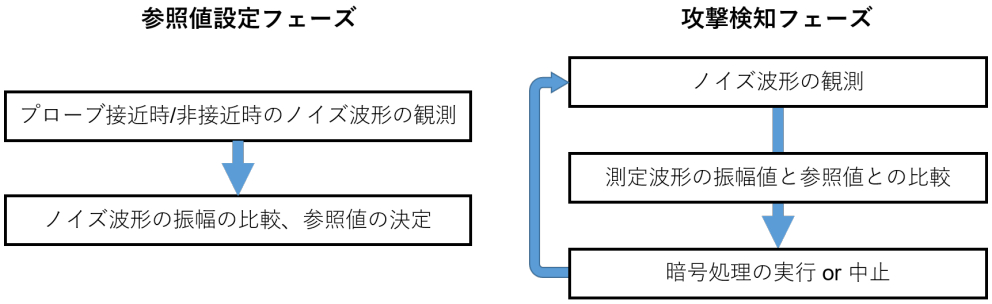


図 4　ノイズの振幅値測定に基づく攻撃検知システムの例

2.2　攻撃検知手法を実現するための前提

提案手法を実装したノイズの振幅値測定に基づく攻撃検知システムの例を図 4 に示す。IC 周囲のノイズ波形の振幅値変化を観測し電磁波解析攻撃の兆候 (プローブの設置) を検知するためには、参照値を設定し攻撃が実行されていることを判定するシステムが必要である。そのため、攻撃検知システムは参照値を設定するフェーズ (参照値設定フェーズ) と電磁波解析攻撃を検知するフェーズ (攻撃

検知フェーズ) に大きく分けられる。参照値設定フェーズでは、プローブが IC へ接近するときと接近しないときのノイズを測定し、それぞれの状況下で観測された波形の振幅値を比較することで参照値の設定を行う。攻撃検知フェーズでは、暗号モジュールに暗号処理を実行させる直前にノイズの測定を行ない、その振幅値と参照値を比較することで攻撃検知を行う。

上述の攻撃検知システムを実現するためには、IC 周囲に分布するノイズを測定するための ADC が必要である。市場に出回っている多くの IC には内部に ADC が実装されているため、利用している IC に未使用の端子と ADC があるならば IC 周囲のノイズを測定することが可能となる。但し、プローブの有無により振幅値が変化する周波数を ADC で観測可能であること、プローブの有無によって IC 周囲に分布するノイズの振幅値にどのような変化が生じるか明らかであることが前提となる。そこで、 3 章において IC 周囲に分布するノイズを IC 内部の ADC により測定することで、提案手法が実現可能か検討する。

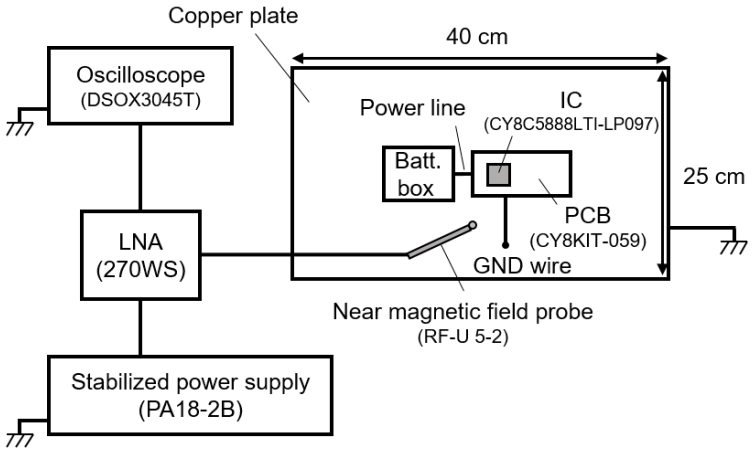
3. 提案手法の実現可能性を確認するための基礎検討

本章では、基板上で観測されるノイズの時間領域における振幅値変化を IC (マイコン) 内部に実装された ADC で観測し、提案手法の実現可能性を検討する。本実験では、最初に、プローブを IC へ接近させたときに ADC で観測されるノイズの時間領域波形の振幅値が有意に変化することを示す。続いて、ノイズの振幅値変化を評価するための指標を検討し、最後に、本章の実験環境下において ADC で測定したノイズ波形の振幅値情報から、プローブの接近を検知できる距離を検討することで提案手法の実現可能性を確認する。

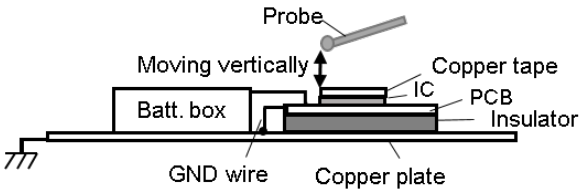
3.1 実験環境

図 5 に実験セットアップを示す。ここでは、攻撃者のセットアップをオシロスコープ (Keysight DSOX3054T)、 安定化電源 (TEXIO PA18-2B)、ローノイズアンプ (COSMOWAVE LNA270WS) と磁界プローブ (Langer EMV RF- U 5-2) と仮定する。また、攻撃対象となる機器はマイコンボード (Cypress CY8KIT-059) とする。ここでは、マイコンボードからの電源ノイズの影響を抑えるため、電池ボックスによりマイコンへ電源を供給させる。また、本実験ではマイコン内部の ADC により IC 周囲のノイズを測定するため、マイコンの GND を規定する必要がある。そのため攻撃対象となる機器は、オシロスコープおよび安定化電源が接続された電源タップの GND へ接続された銅板 (縦 25 cm、横 40 cm) の中央に設置し、マイコンの GND を銅板と短絡させた。

また、本研究では攻撃者が精度よく IC からの漏えい電磁波を測定可能であることを想定する。攻撃者の磁界プローブは図 6 に示す通り、プローブの先端を貫く磁界を取得するため、実験では攻撃者が上述の磁界プローブを IC チップ直上に接近させ、IC からの磁界を測定することを想定する。図 7 にマイコン周辺のノイズを測定するための ADC 回路のブロック図を示す。提案手法には、攻撃を検知するためにプローブの有無によって有意な変化が現れる周波数帯とその周波数帯を観測可能な ADC が必要となる。本実験では、測定環境に依存せず機器の内外で観測可能な商用周波数 (60 Hz) を検知に用いる周波数帯として選択する。



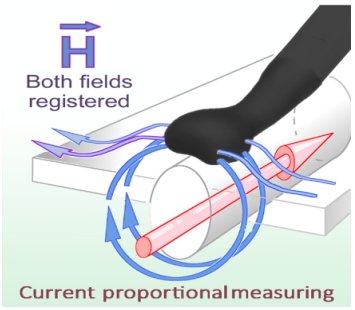
(a) 上面図



(b) 側面図

図 5　実験セットアップ

(a) 磁界プローブの形状



(b) プローブが取得する磁界
(www.langer-emv.de)

図 6　攻撃者の磁界プローブ

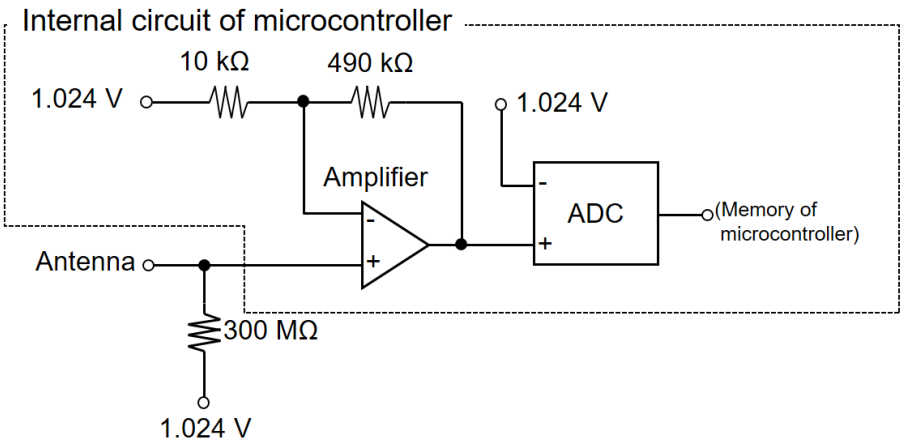


図 7　IC 内部の ADC 回路のブロック図

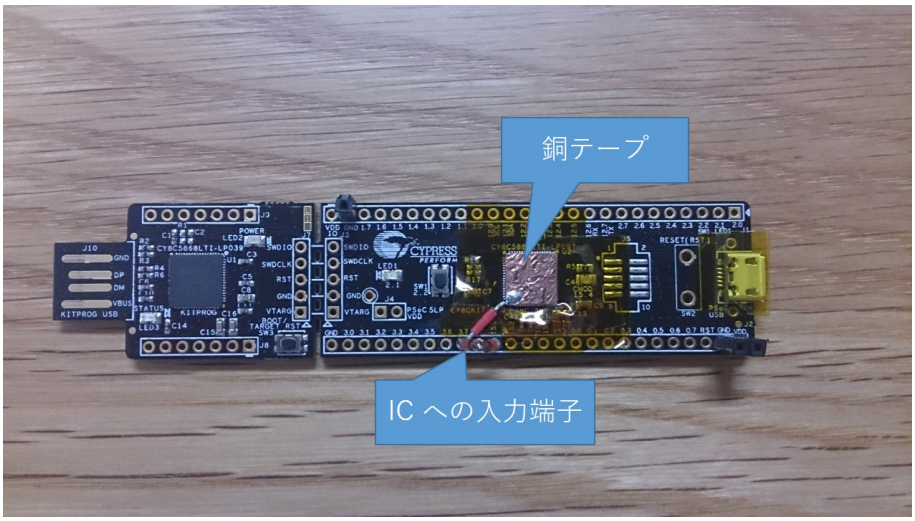


図 8　攻撃対象のマイコンボード

表 1 ADC の電磁界測定性能

パラメータ	値
サンプルレート	2.0 kHz
測定一回のサンプルサイズ	20,000 points
ADC への入力電圧範囲	0 – 2.048 V
電圧分解能	16 bit (1LSB = 31.25 μ V)
参照電圧	1.024 V
増幅器の倍率	約 50 倍

また、60 Hz のノイズを IC 内部に効率的に誘導するため、IC チップ上面に銅テープを設置し IC への入力に接続させている (図 8)。さらに、ノイズ波形の振幅変動を感度良く測定するため、ADC の入力回路に増幅率が約 50 である増幅器を設置する。ADC の入力電圧の範囲は 0 – 2.048 V であり、ADC 入力 (図 7 における ADC の正入力) の直流成分が 1.024 V ならば、測定波形は ADC の測定レンジの中心が直流成分となり、ADC の測定レンジを最大限使って振幅を評価することができる。 ADC 入力の直流成分を 1.024 V にするために、300 MΩ の抵抗を用いて 1.024 V の参照電圧へ接続し固定する。ADC のサンプルレートは IC 周囲のノイズに含まれる 60 Hz の商用周波数帯の測定を行う上で十分な 2.0 kHz に設定し、測定一回に付き 20,000 ポイント (= 10 sec) を取得し評価を行う。また、本実験で用いた ADC の電圧分解能は 16 bit (1 LSB = 31.25 μV) である。

3.2 プローブの有無によるノイズ波形の振幅値変化の観測

IC 内部の ADC でプローブあり/なしの状況下における IC 周囲のノイズをそれぞれ測定し、磁界プローブの接近により観測される ノイズの時間領域波形の振幅が変化することを示す。ここでは、攻撃者が IC からの漏えい電磁波を最も高精度に測定可能である状況を想定する。そのため、図 5(b) におけるプローブ — IC 間の垂直方向の距離が 0 cm であるときをプローブありの状況とし、磁界プローブが IC 周囲に存在しないときをプローブなしの状況とする。本実験では

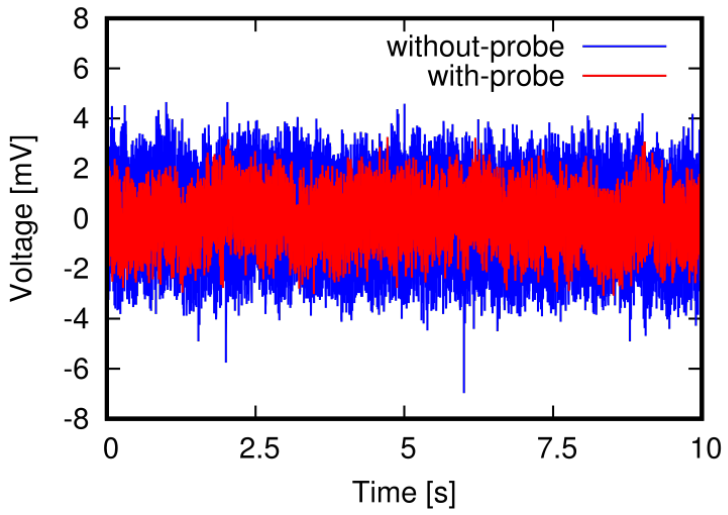


図 9　プローブの有無による IC 周囲のノイズ波形の変化

プローブあり/なし、それぞれの状況下で ADC による IC 周囲のノイズの測定を一回ずつ行い、プローブの有無により測定波形にどのような変化が生じるか調査する。

プローブあり/なしのそれぞれの状況下で観測されたノイズの時間領域波形を図 9 に示す。グラフには、”with-probe”、”without-probe”がそれぞれプローブあり/なしの状況下での測定波形を示している。横軸は測定時間、縦軸は ADC の出力 (電圧値) を示している。この結果から、プローブの設置により、IC 内部から観測されるノイズの時間領域波形の振幅値が減少する傾向が確認できる。つまり、本実験環境では磁界プローブが IC 近傍へ配置されることにより、IC 周囲に分布するノイズの振幅値が減少することが明らかとなった。

3.3　ノイズ波形の振幅値変化を評価するための指標

提案手法ではノイズ波形の振幅値変化からプローブを検知するが、ノイズ波形は時間的な揺らぎを持っているため、測定波形の振幅値のみを用いて評価することは難しい。そのため、ノイズ波形の振幅値変化を利用し攻撃検知を行うために

は、測定波形の振幅値を評価するための指標が必要となる。本実験では、測定波形の振幅値との相関があり、ノイズの電力として利用される分散値 (式 (1)) が、本実験環境におけるノイズ波形の振幅値変化の評価に利用可能か検討する。

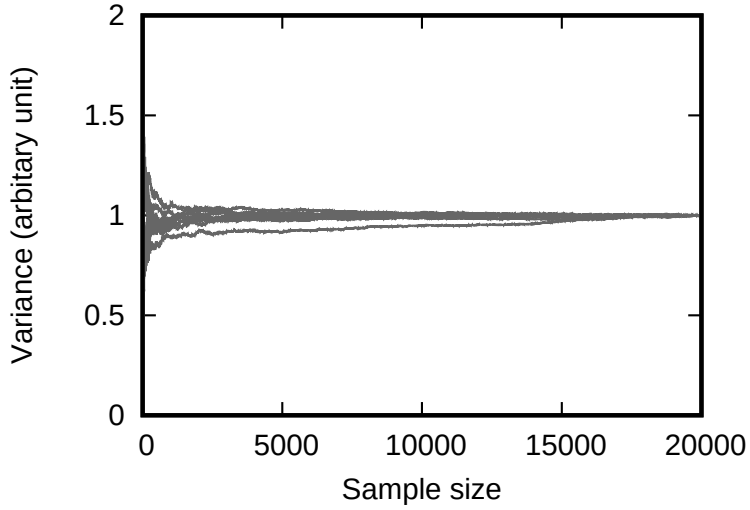
$$s^2 = \frac{1}{n-1}\sum_{i=1}^{n}(x_i - \bar{x})^2 \tag{1}$$

式 (1) における x_i は i 番目に出力された ADC の出力値であり、n はサンプルサイズである。本実験では、攻撃が行われていないときに IC 周囲に分布するノイズを IC 内部の ADC で測定し、ノイズの分散値がマイコンで取得可能なサンプルサイズの範囲で一定の値に収束するか確認する 。ここでは、プローブなしの状況下において測定を 10 回行い、各測定波形の分散値を出力する。

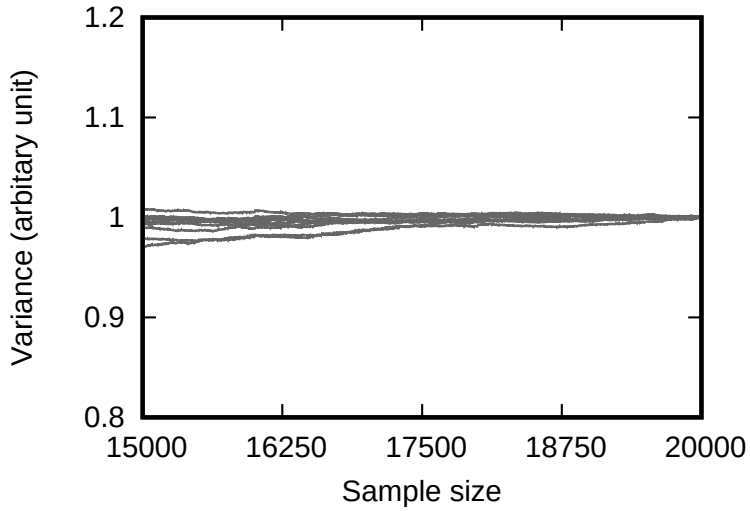
図 10 には、測定した 10 波形それぞれのサンプルサイズに対するノイズの分散値変化を示している。横軸が測定波形数、縦軸が分散値を示している。但し、縦軸の分散値はサンプルサイズが 20,000 のときの各分散値を平均化した値が 1 となるように正規化させている。この結果から、いずれの測定においてもサンプルサイズが 15,000 以上となると、正規化した分散値が 1 に近い値に収束していることが確認できる。また、サンプルサイズ 15,000 以上の部分を拡大すると (図 10(b))、サイズが 17,500 付近で限りなく 1 に近い範囲内に分散値が収束していることが確認できた。すなわち、マイコンメモリで保持可能なサンプルサイズで分散値が一定の範囲内に収束することが明らかとなり、ノイズの振幅値変化に分散値を利用できることが示された。

3.4 プローブ - IC 間の距離に応じたノイズ波形の分散値変化

本節では、提案手法によりプローブを検知できる距離に関する検討を行う。電磁波解析攻撃の特徴の一つは、攻撃者がプローブを任意の位置に 設置し電磁界測定を実行できることである。3.2 節で観測されたノイズ波形の振幅値変化は、プローブ ― IC 間の距離に依存するため、プローブが設置される位置によっては検知できない可能性がある。そこで本節では、図 5(b) におけるプローブ ― IC 間



(a) 全体図



(b) 拡大図

図 10 サンプルサイズに対するノイズ波形の分散値の変化

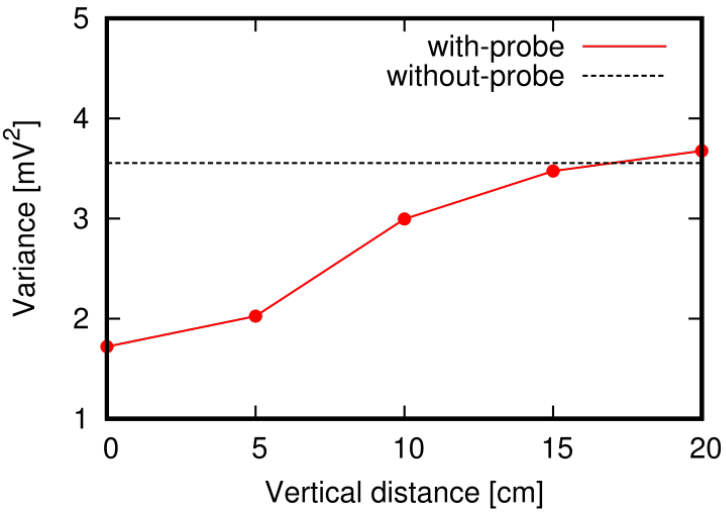


図 11　プローブ – IC 間の距離変化に対する分散値変化

の距離を垂直方向に変化させながらノイズを測定し、プローブを IC からある程度の距離まで離れた位置に設置されたとしても、提案手法によりプローブの検知が可能であるか検討する。本実験では、プローブ — IC 間の垂直方向の距離を 0 cm から増大させながらノイズを測定し、得られた分散値をプローブなしでの分散値と比較することで、プローブの有無を分散値により判別できる距離の限界値を検討する。ここでは、各状況下において 10 回ずつ測定を行う。比較に用いる分散値として、プローブなしの状況下では測定した 10 波形の中から、分散値が最小のものをプローブなしの分散値として選択する。また、プローブありの状況下では各距離で測定した 10 波形の中から分散値が最大のものを、その距離の分散値として選択する。本実験では、実験セットアップの周囲に設置されている機器の数を固定することで、周辺電磁環境の変化を可能な限り抑え、プローブの設置位置によるノイズ波形の分散値変化を評価する。

プローブなしで測定した波形の分散値、およびプローブ -— IC 間の各距離での分散値を図 11 に示す。このグラフでは ”with-probe” はプローブありの状況下で距離を変化させたときに測定された分散値を示し、”without-probe” はプローブなしの分散値を示している。この結果から、プローブ -— IC 間の距離が大き

表 2 検定に用いる 10 波形の分散値 (mV^2)

プローブあり (15 cm)	プローブなし
3.207215	3.554209
3.283236	3.603386
3.312685	3.642344
3.314555	3.676821
3.341589	3.685075
3.349032	3.715915
3.351418	3.883540
3.363204	3.944281
3.387586	4.091851
3.474882	4.384126

くなるにつれて、測定波形の分散値が大きくなることが確認できる。またプローブ – IC 間の距離が 15 cm から 20 cm へと変化したとき、プローブなしの分散値 (3.55 mV^2) を超える分散値が観測された。さらにプローブ – IC 間の距離が 16 cm の分散値を出力したところ、3.87 mV^2 となった。このことから、本実験環境ではプローブ – IC 間の距離が 15 cm 付近までが、提案手法によりプローブを検知できる範囲であると考えられる。

続いて、プローブ – IC 間が 15 cm (プローブあり (15 cm)) の分散値とプローブなしの分散値に有意な差があるか確認する。プローブあり (15 cm)/なしで測定した 10 波形それぞれの分散値を表 2 に示す。ここでは、2 群の標本間の平均値に有意差があることを確認する。 Welch の t 検定を用いて、プローブあり (15 cm) の分散値とプローブなしの分散値が有意に異なるか確認する。本検定では、帰無仮説 H_0 を”プローブあり (15 cm) で得られた分散値の母平均は、プローブなしで得られた分散値の母平均と等しい” とする。また、対立仮説 H_1 を”プローブあり (15 cm) で得られた分散値の母平均は、プローブなしで得られた分散値の母平均とは異なる”とする。ここでの有意水準は 1 % とする。

表 3 検定結果

	プローブあり (15 cm)	プローブなし
平均	3.338540 mV^2	3.818155 mV^2
分散	0.004826	0.067806
標本数	10	10
自由度	10	
t 値	- 5.627640	
t 境界値	2.228139	
p 値	0.000219	

検定に用いる統計量 t は式 (2) のように定義される。

$$t = \frac{\bar{x_1} - \bar{x_2}}{\sqrt{\frac{s_1^2}{n_1} + \frac{s_2^2}{n_2}}} \tag{2}$$

ここでの $\bar{x_1}$、$\bar{x_2}$ はそれぞれプローブあり (15 cm)/なしで取得したサンプル (分散値) の平均であり、s_1^2、s_2^2 はその分散、n_1、n_2 はサンプル数を示している。

検定の結果を表 3 に示す。この結果から、$p = 2.2 \times 10^{-4} < 0.01$ となり有意水準 1 % で帰無仮説 H_0 を棄却し、対立仮説 H_1 を採択できることが分かる。すなわち、プローブあり (15 cm) の状況とプローブなしの状況で取得した分散値の平均に有意な差がみられたことから、本実験環境においては提案手法によりプローブを検知できる距離は 15 cm 付近までであることが示された。以上の結果から、ノイズ波形の分散値を測定することで、IC からある程度の距離まで離れた位置に設置されたプローブでも検知できることが明らかになった。

4. 考察

本章では、ADC で観測されるノイズ波形の振幅値変化の原因について考察し、続いて実験結果から考えられるプローブ接近を自動的に判別する方法および攻撃検知精度を低下させる可能性について論ずる。

4.1 ノイズ波形の振幅値変化の要因

3 章で得られた ADC 測定波形の振幅値変化に関する考察を行う。ノイズの振幅値が変化したのは、ADC の入力端子に接続された銅テープ (と ADC までの配線) とプローブとの間に相互インダクタンスまたは相互キャパシタンスが生じ、ADC の入力端子とプローブが電気的に結合したためである。プローブ -— IC 間に生ずる結合の大きさは、プローブまたは ADC への入力端子 (センサ) の大きさや形状に依存するため、多様なプローブに提案手法を適用するための要件を明らかにすることが必要である。また、IC 周囲に分布するノイズ波形の振幅値の大きさは、周囲に設置されている PC やディスプレイなどの機器や、人体の有無によっても変化する可能性がある。そのため、機器の設置箇所が変化しても、高精度にプローブを検知するための検討については今後の課題である。

4.2 プローブ接近の判別方法

3 章の実験では、プローブが接近することにより IC 内部の ADC で観測されるノイズ波形の振幅値 (分散値) が減少する傾向が得られた。このことからプローブの接近を回路内部で自動的に判定する方法として、観測される分散値に下限値を設け、その値を超えた場合に測定が実施されていると判定する方法が挙げられる。ただし、サンプルサイズや下限値の大きさと攻撃検知の精度はトレードオフの関係にある。また、提案手法を実装する機器の大きさによっては、プローブ以外の物体を誤検知する可能性もある。そのため、実システムへの導入には、サンプルサイズおよび下限値の設定方法について検討が必要である。

4.3 攻撃検知精度低下の可能性

4.3.1 ADC 入力インピーダンスの不正操作

提案手法では、基板上の IC 周囲におけるノイズ波形の振幅値変化を分散値により評価し、漏えい電磁波の測定に用いられるプローブを検知する 。ノイズの振幅値変化を感度良く観測するためには高い入力インピーダンスを有する ADC が必要である。もし攻撃者が ADC 回路の入力インピーダンスを操作可能ならば、ADC が有するノイズ波形の振幅値変化に対する感度を低下させ、攻撃検知機能を無効化することが考えられる。ADC 回路の入力インピーダンスを変化させる方法としては、例えば、入力端子を基板上の別の端子へ接続することなどが考えられる。一方で 、4.1 節で述べた通り入力インピーダンスが変化した場合は、ADC により観測されるノイズ波形が変化するため、不正なインピーダンスの操作は通常利用時に観測されるノイズ波形の振幅値と比較することで検知可能であると考えられる。また、提案手法を暗号機器へ実装する際に、ノイズを測定するための ADC 回路を他の回路と分離することでも、ADC 回路のインピーダンス変化を防ぐことができると考えられる。また、高インピーダンスの ADC 回路を機器へ実装すると、機器自体が周辺のノイズに対して脆弱になることも考えられる。この問題に対しては、攻撃検知用の回路を他の回路と分離させる、EMI 除去フィルタを設置するなどの手法により一定のノイズ耐性を確保することで対応できると考えられる。

4.3.2 ノイズ波形の意図的な操作

攻撃者に検知に利用する周波数を特定された場合、ADC で観測される波形の分散値が意図的に操作され、検知システムが無効化されることも考えられる。例えば、基板上に対し検知に用いる周波数の電磁波を照射することで、ノイズ波形の分散値が操作される可能性がある。そのため、提案手法を暗号システムへ導入する際には、測定波形の分散値の操作を検知するシステムを導入するなどの対応も併せて必要になると考えられる。

5. まとめ

本論文では、暗号モジュールへの電磁波解析攻撃の対策手法として、 IC 周囲に分布するノイズの振幅値に着目した攻撃検知手法を提案し、その実現可能性を議論するための基礎的な実験を行った。

2 章では、暗号モジュールを実装した IC 近傍でのプロービングにより生ずる IC 周囲のノイズ波形の振幅値変化に着目した電磁波解析攻撃検知手法および提案手法を実装した暗号システムについて論じた。

3 章では、提案手法の有効性を確認するための基礎検討を行った。 具体的には、まず電磁波解析攻撃を模擬した評価環境において、プローブを IC に接近させた際に、IC 内部の ADC で測定されるノイズの時間領域波形がどのように変化するのか調査した。続いて、ノイズの振幅値変化を評価するための指標を検討した。最後に、提案手法により検知可能なプローブの距離を検討するため、プローブ – IC 間の垂直方向の距離を変化させながら、測定される背景ノイズの振幅値変化を観測 した。さらに、提案手法でプローブを検知可能な距離と、攻撃者が IC からの漏えい電磁波を取得可能な距離との大小関係について検討した。その結果 (i) プローブ接近による IC 周囲のノイズ波形の振幅値減少を IC 内部の ADC により観測可能であること、(ii) サンプルサイズが 20,000 の場合には振幅値変化の評価に分散値が利用できること、(iii) IC からある程度離れた位置 (本実験環境では IC から 15 cm 程度の距離) に設置されたプローブを検知可能であることをそれぞれ確認した。

4 章では、3 章で観測されたノイズ波形の振幅値変化が発生した原因について考察し、また実験結果から考えられるプローブ接近を回路内部で自動的に判別する方法と攻撃検知精度を低下させる可能性について論じた。

以上より、IC 周囲に分布するノイズを測定することで電磁波解析攻撃におけるプロービングの兆候を検知し、 IC からの漏えい電磁波の測定を困難化させることができる可能性があることを示した。

謝辞

本論文は、奈良先端科学技術大学院大学情報科学研究科情報セキュリティ工学研究室での研究活動に基づいています。末筆になりますが、研究の遂行、論文の執筆にあたり御助言を頂いた皆様に深く感謝の意を表します。

主指導教員である林優一教授には、研究方針の策定から論文の執筆に至るまで貴重な御指導、御鞭撻を賜りました。厚く御礼申し上げます。

副指導教員である岡田実教授ならびに安本慶一教授には、審査会において研究の方針について御指導を賜りました。深く感謝申し上げます。

藤本大介助教には、日頃より研究活動に関する熱心な御指導を賜りました。深く感謝申し上げます。

仙台高等専門学校の衣川昌宏助教には、実験を行うにあたり多くの御指導を賜りました。深く感謝申しあげます。

情報セキュリティ工学研究室の学生の皆様には、日頃の研究室生活において様々な面でご協力を頂きました。感謝申し上げます。

最後に、学業生活を様々な面から支えてくれた家族に感謝致します。

参考文献

[1] FIPS P. 197. Advanced encryption standard (aes). *NIST. US Department of Commerce*, 2001.

[2] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, February 1978.

[3] Sergei P. Skorobogatov. Semi-invasive attacks – a new approach to hardware security analysis, 2005.

[4] Karine Gandolfi, Christophe Mourtel, and Francis Olivier. Electromagnetic analysis: Concrete results. In Çetin K. Koç, David Naccache, and Christof Paar, editors, *Cryptographic Hardware and Embedded Systems — CHES 2001*, pages 251–261, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg.

[5] Dakshi Agrawal, Bruce Archambeault, Josyula R. Rao, and Pankaj Rohatgi. The em side—channel(s). In Burton S. Kaliski, çetin K. Koç, and Christof Paar, editors, *Cryptographic Hardware and Embedded Systems - CHES 2002*, pages 29–45, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg.

[6] Michael Hutter, Stefan Mangard, and Martin Feldhofer. Power and em attacks on passive 13.56 mhz rfid devices. In Pascal Paillier and Ingrid Verbauwhede, editors, *Cryptographic Hardware and Embedded Systems - CHES 2007*, pages 320–333, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.

[7] Stefan Mangard, Maria Elisabeth Oswald, and Thomas Popp. *Power Analysis Attacks - Revealing the Secrets of Smart Cards*. Springer, 1 edition, 2007. XXIII, 337 S.

[8] Timo Kasper, David Oswald, and Christof Paar. Em side-channel attacks on commercial contactless smartcards using low-cost equipment. In Heung Youl

Youm and Moti Yung, editors, *Information Security Applications*, pages 79–93, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.

[9] François-Xavier Standaert. *Introduction to Side-Channel Attacks*, pages 27–42. Springer US, Boston, MA, 2010.

[10] Alessandro Barenghi, Gerardo Pelosi, and Yannick Teglia. Improving first order differential power attacks through digital signal processing. In *Proceedings of the 3rd International Conference on Security of Information and Networks*, SIN '10, pages 124–133, New York, NY, USA, 2010. ACM.

[11] D. Aboulkassimi, M. Agoyan, L. Freund, J. Fournier, B. Robisson, and A. Tria. Electromagnetic analysis (ema) of software aes on java mobile phones. In *2011 IEEE International Workshop on Information Forensics and Security*, pages 1–6, Nov 2011.

[12] C. H. Gebotys. A table masking countermeasure for low-energy secure embedded systems. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 14(7):740–753, July 2006.

[13] F. Poucheret, L. Barthe, P. Benoit, L. Torres, P. Maurine, and M. Robert. Spatial em jamming: A countermeasure against em analysis? In *2010 18th IEEE/IFIP International Conference on VLSI and System-on-Chip*, pages 105–110, Sep. 2010.

[14] K. Tiri and I. Verbauwhede. A logic level design methodology for a secure dpa resistant asic or fpga implementation. In *Proceedings Design, Automation and Test in Europe Conference and Exhibition*, volume 1, pages 246–251 Vol.1, Feb 2004.

[15] Jean-Sébastien Coron and Ilya Kizhvatov. An efficient method for random delay generation in embedded software. In Christophe Clavier and Kris Gaj, editors, *Cryptographic Hardware and Embedded Systems - CHES 2009*, pages 156–170, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.

[16] Emmanuel Prouff and Matthieu Rivain. Masking against side-channel attacks: A formal security proof. In Thomas Johansson and Phong Q. Nguyen, editors, *Advances in Cryptology – EUROCRYPT 2013*, pages 142–159, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

[17] Weize Yu, Orhun Aras Uzun, and Selçuk Köse. Leveraging on-chip voltage regulators as a countermeasure against side-channel attacks. In *Proceedings of the 52Nd Annual Design Automation Conference*, DAC '15, pages 115:1–115:6, New York, NY, USA, 2015. ACM.

[18] Clayton R. Paul. *Introduction to Electromagnetic Compatibility (Wiley Series in Microwave and Optical Engineering)*. Wiley-Interscience, New York, NY, USA, 2006.

著者発表論文

1. Shinpei Wada, Daisuke Fujimoto and Yu-ichi Hayashi, Detecting Electromagnetic Analysis Using the Distribution of Electromagnetic Noise, EMC Joint Workshop 2018, Daejon.

2. 和田 慎平, 藤本 大介, 林 優一, IC 周囲に分布する電磁雑音を用いた電磁波解析攻撃検知手法の検討, EMCJ 研究会 2018 年 12 月, デンソー.