

修士論文

意図的な電磁妨害下における逐次比較型 ADC 出力の 真正性評価に関する研究

江頭 智也

奈良先端科学技術大学院大学

先端科学技術研究科

情報理工学プログラム

主指導教員: 林 優一 教授

情報セキュリティ工学研究室 (情報科学領域)

令和 2 年 3 月 13 日提出

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

江頭 智也

審査委員：

林 優一	教授	（主指導教員, 情報科学領域）
岡田 実	教授	（副指導教員, 情報科学領域）
安本 慶一	教授	（副指導教員, 情報科学領域）
藤本 大介	助教	（副指導教員, 情報科学領域）

意図的な電磁妨害下における逐次比較型 ADC 出力の 真正性評価に関する研究*

江頭 智也

内容梗概

実世界のセンシングにより得られる情報を物理層で処理する ADC (Analog to Digital Converter) の出力値が改ざんされた場合、出力データを用いて処理を行う上位レイヤのサービス全ての信頼性を著しく低下させる新たな脅威となり得る。ADC は基準電圧とアナログ入力電圧の比較により、アナログ値をデジタル値に変換しているため、機器外部から意図的な電磁妨害によって基準電圧やアナログ入力電圧の値が変動した場合、ADC の有効ビット数が著しく低下し、ADC 出力の真正性が失われる可能性がある。

本論文では、意図的な電磁妨害が ADC の出力に与える影響を評価するために、ADC の有効ビット数に着目し、ADC 出力の真正性を評価する。具体的には、汎用的な ADC を搭載した評価ボードを用い、評価ボードに接続された電源線に正弦波を印加し、ADC の有効ビット数を指標として真正性を評価する。さらに、実験結果に基づき、意図的な電磁妨害時にも真正性の保障されたデータを出力可能となる対策技術についても議論を行う。

キーワード

逐次比較型 ADC, 意図的な電磁妨害, 有効ビット数

*奈良先端科学技術大学院大学 先端科学技術研究科 修士論文, 令和 2 年 3 月 13 日.

Evaluation of Authenticity of Successive Approximation Analog to Digital Converter Output under Intentional Electromagnetic Interference*

Tomoya Egashira

Abstract

An analog to digital converter (ADC) is an important device which processes data obtained by sensing information from the real world at the physical layer. If the output value of the ADC is falsified by the external impacts, the reliability of all upper layers which use the output data from the ADC can be significantly affected and degraded. The ADC converts an analog value into a digital value by comparing a reference voltage and an analog input voltage. Therefore, when the value of the reference voltage or the analog input voltage fluctuates due to intentional electromagnetic interference (IEMI) from outside the device, effective number of bits of the ADC may be significantly reduced, and the authenticity of the AD conversion data may be lost. Therefore, a threat to ADC based on the IEMI can cause severe security issues.

In this study, evaluation of the IEMI impacts on the ADC is conducted. Impacts of the IEMI on the ADC are analyzed by evaluating the effective number of bits (ENOB). Experimental validation is conducted by applying sine waves which are a source of an IEMI to the power line connected to a general-purpose ADC evaluation board. By applying the external noise via a power line connected to the power plane of the evaluation board, the injected noise propagates

*Master's Thesis, Graduate School of Science and Technology, Nara Institute of Science and Technology, March 13, 2020.

along with the power/ground network of the evaluation board and affects the ADC causing performance degradation. Then, the authenticity is evaluated by monitoring the changes in ENOB of the ADC when the external noise is injected. Finally, based on the experimental results, I suggested how to counter ADC IEMI threats.

Keywords:

Successive Approximation Register - Analog to digital converter, Intentional electromagnetic interference, Effective number of bits

目次

図目次	v
第 1 章 序論	1
1.1 研究の背景	1
1.2 研究の目的	3
1.3 本論文の構成	4
第 2 章 意図的な電磁妨害に対する有効ビット数を用いた逐次比較型 ADC 出力の真正性評価手法の提案	5
2.1 SAR-ADC の変換原理	5
2.2 SAR-ADC の変換原理に基づく ADC 出力の改ざん手法の提案	7
2.3 有効ビット数による ADC 出力の真正性の評価	9
第 3 章 意図的な電磁妨害に対する有効ビット数を用いた逐次比較型 ADC 出力の真正性の評価	11
3.1 実験環境	11
3.2 実験結果	13
3.2.1 意図的な電磁妨害による基準電圧とアナログ入力電圧の変動	13
3.2.2 時間領域および周波数領域での妨害電磁波の注入の検証	14
3.2.3 周波数掃引・振幅固定による有効ビット数の評価	15
3.2.4 周波数固定・振幅掃引による有効ビット数の評価	16
3.3 対策技術の検討	17
3.4 まとめ	18
第 4 章 結論	19
謝辞	20
参考文献	21
発表リスト	23

図目次

1.1	計測機器のデータフロー	2
1.2	センサを搭載した機器内部の変換部への攻撃の可能性	3
2.1	AD 変換の概念図	6
2.2	SAR-ADC の回路構成	6
2.3	SAR-ADC のデータを改ざんする手法の原理	8
2.4	FFT による妨害信号成分の注入を検討する手法の原理	9
2.5	妨害電磁波の注入による有効ビット数の減少	10
3.1	実験セットアップの外観	12
3.2	ADC を搭載した評価ボードと制御ボード	12
3.3	実験セットアップのブロック図とパラメタ	12
3.4	基準電圧とアナログ入力電圧の変動	13
3.5	基準電圧とアナログ入力電圧の差分の波形	14
3.6	基準電圧とアナログ入力電圧の差分に含まれる周波数成分	14
3.7	周波数掃引・振幅値固定における有効ビット数の低下	15
3.8	周波数固定・振幅値掃引における有効ビット数の低下	16

第 1 章 序論

1.1 研究の背景

近年、外界の物理状態を測定するセンサが開発・普及しており、スマートフォンや自動車、スマートウォッチなど、これまでセンサが搭載されていなかった機器へのセンサの搭載が進んでいる [1]。これらのセンサは、角度・距離・温度などのデータを計測し、機器の動作情報、人の情報、環境情報などの情報をセンサ情報として収集する。収集されたセンサ情報は後段の回路に送られ、システムはセンサから送られたデータを基に処理を決定し、サービスの活用や機器の動作の決定に利用している。このデータの計測・活用の中で、活用側であるシステムは暗号技術などによってそのセキュリティが保証されている。一方で、センサでのデータの計測段階への攻撃によって、データの真正性が低下した場合、システム側で真正性の低下したデータの蓄積・解析が行われ、システムの信頼性が低下する可能性がある。そのため、自律制御、自動運転、ロボット、医療機器や社会インフラなどのあらゆるシステムに利用されるセンシング機器において、センサの情報が改ざんされると、機器やシステムが誤動作を起こし、人命・身体・社会システムの深刻な危険につながる大きな脅威となる可能性がある。以上の理由から、センサを対象とした物理的な攻撃に対する、計測段階でのデータの真正性の検討が求められる。

計測段階の脅威は、(1) 計測値の完全性 (Integrity) の低下、(2) 計測の可用性 (Availability) の低下に大別されると考えられる。(1) 計測値の完全性 (Integrity) の低下は、計測の真正性を低下させることによって、実測値とは異なる計測結果を出力させるような攻撃により引き起こされる。(2) 計測の可用性 (Availability) の低下は、計測機器への物理的な破壊を含めた計測自体を停止させる攻撃により引き起こされる。これらの脅威を引き起こす計測段階での攻撃を検討するため、図 1.1 に、センサ入力部で収集した情報が ADC (Analog-to-digital converter) を経由して後段のプロセッサやマイクロコントローラで処理されるまでのデータフローを示す。まず、データ収集部において、センサ入力部が計測対象に対して物理情報の測定を行い、収集した計測値を電気的なアナログ情報へと変換する。そして、アンプにて信号を増幅し、変換部の ADC へとデータが送信される。次に、データ変換部

の ADC においてアナログ信号をデジタル信号へと変換する。最後に、データ処理部の CPU において信号処理が行われ、後段のシステムへとデータが送信される。

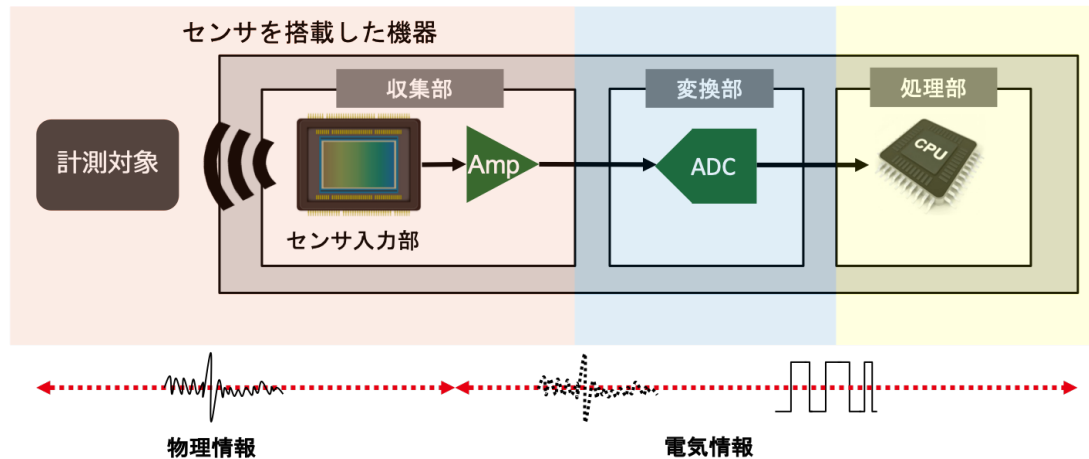


図 1.1 計測機器のデータフロー

このデータフローにおけるハードウェアレベルでの攻撃として、まず物理情報の収集段階である、センサ入力部への攻撃が考えられる。これまでの計測セキュリティ領域での研究において、センサ入力部への攻撃の検討事例として、LIDAR (Light Detection And Ranging) へのなりすまし攻撃 [2] やジャイロセンサへのジャミング [3] が検討されている。これらの研究では、センサの計測原理に基づく攻撃の実現可能性とメカニズム・対策技術が検討されており、センサが収集する計測値の真正性に関するセキュリティが議論されている。また、複数のセンサや異種のセンサを搭載することにより、精度の向上やコスト削減を図ったセンサフュージョンが開発・検討されており、センサフュージョンにより計測がロバストになれば、センサ攻撃への耐性が向上すると期待されている [4]。

しかし、図 1.2 で示すように、センサ入力部を中心とするデータ収集部への攻撃の対策が実装された機器に対して、データ変換部でデータが改ざんされた場合、後段のシステムに実測値とは異なるデータが送られ、システムの信頼性が低下する可能性がある。

データ変換部に対する攻撃により、センサ入力部が取得した計測値と異なる値が出力された場合、後段のシステムが本来のデータとは異なるデータを受け取り、従

来のセンサ入力部への攻撃と同様の脅威となる可能性がある。そのため、これまでのセンサ入力部への攻撃の実現可能性とメカニズム・対策技術の検討だけでなく、データ変換部における攻撃の可能性とメカニズム・対策技術の検討が必要となる。データ変換部の ADC はアナログ情報をデジタル情報へと変換する回路であり、多くの計測機器に搭載されている。そのため、ADC に対する物理的な攻撃によって、ADC 出力が変化した場合、後段のシステムの信頼性が低下する新たな脅威となる可能性がある。

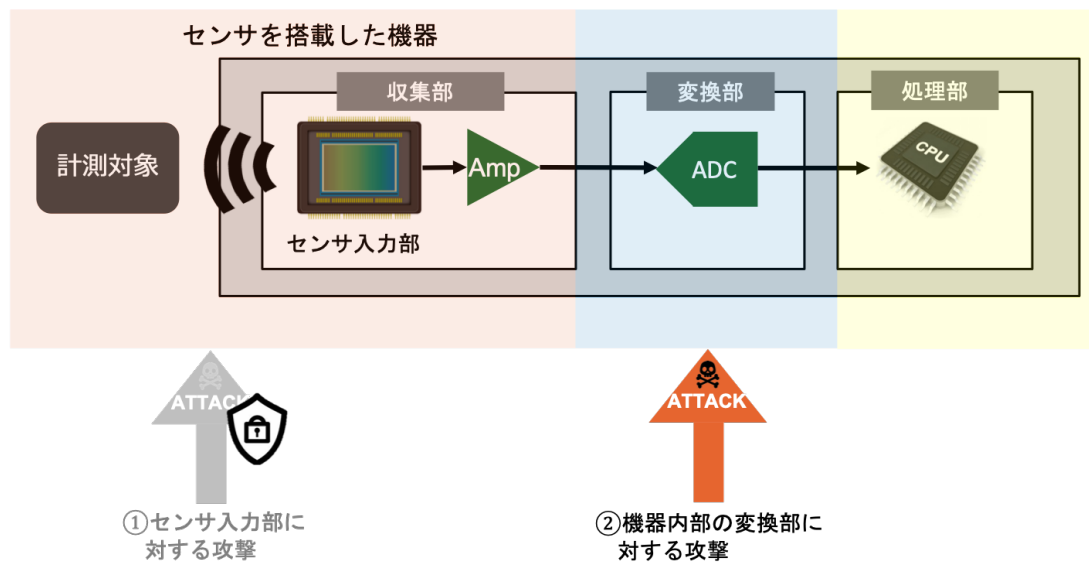


図 1.2 センサを搭載した機器内部の変換部への攻撃の可能性

1.2 研究の目的

これまで、計測機器のセンサ入力部に対する物理的な攻撃による計測値の完全性の低下や計測の可用性の低下が報告されており、攻撃の実現可能性の検討と対策技術の提案がなされている。しかし、センサ入力部への物理的な攻撃への対策が実装された機器において、センサ入力部の後段であるデータの変換部の ADC を対象とした物理的な攻撃により、ADC 出力の真正性が低下した場合、システムの信頼性が低下する可能性がある。そのため、物理的な攻撃により ADC 出力の真正性が低

下するかを評価し、ADC 出力の真正性を低下させる物理的な攻撃に対する対策技術の提案を行う。

1.3 本論文の構成

本論文の構成は以下の通りである。

第 2 章では、まず、本研究の対象となる SAR-ADC (Successive Approximation Register Analog-to-digital converter) の AD 変換の原理を述べる。次に、SAR-ADC の変換原理に基づき、意図的な電磁妨害を用いた ADC 出力の真正性の低下を引き起こす手法を提案する。そして、有効ビット数を用いた ADC 出力の真正性の評価手法を提案する。

第 3 章では、第 2 章で提案した手法を用いて、SAR-ADC を搭載した評価ボードの電源線に対して、意図的な電磁妨害を行う。機器内部の電圧変動を観測するとともに、ADC の出力値から有効ビット数を算出することによって、第 2 章で提案した手法により、有効ビット数が低下することを示す。

第 4 章では、本論文をまとめる。

第 2 章 意図的な電磁妨害に対する有効ビット数を用いた逐次比較型 ADC 出力の真正性評価手法の提案

本章では、まず、高分解能で小型化や低消費電力化が可能であることから計測機器において最も普及している SAR-ADC の AD 変換の原理について説明する。続いて、変換原理に基づき、ADC 出力の真正性を低下させる物理的な攻撃手法の検討を行う。最後に、有効ビット数を用いた、物理攻撃による ADC 出力の真正性低下の評価について論ずる。

2.1 SAR-ADC の変換原理

本節では、攻撃の実現可能性について検討する SAR-ADC の AD 変換の原理について説明する。

IoT (Internet of Things) エッジノードを中心として計測機器に搭載される ADC は、小型かつ低消費電力であること、および高分解能であることが求められ、SAR-ADC が多く用いられている。SAR-ADC は、図 2.1 に示すように、二分探索のアルゴリズムを用いており、一つの比較器を繰り返し使用するため回路規模が小さく、小型化が可能である [6]。さらに、回路に占めるデジタル回路の比率が高いため、微細化することで低消費電力化が可能である。

図 2.2 に示すように、SAR-ADC は一般的に、サンプル・ホールド回路、コンパレータ、DAC(Digital-to-Analog Converter)、そして SAR およびそれらの制御回路で構成される。以下に変換アルゴリズムを示す。まず、アナログ入力電圧 (V_{IN}) がトラック/ホールド上で保持される。二分探索アルゴリズムを実行するために、 N ビットのレジスタは最初に中間スケールに設定される。これによって、DAC 出力 (V_{DAC}) を ADC に供給される基準電圧 (V_{REF}) の半分である $V_{REF}/2$ に設定する。その後、 V_{IN} が V_{DAC} 以上か以下であるかを決定するために、比較が実行される。 $V_{IN} > V_{DAC}$ の場合、コンパレータは 1 を出力し、 N ビットレジスタの MSB は 1 を維持する。逆に、 $V_{IN} < V_{DAC}$ の場合、コンパレータは 0 を出力し、レジスタの MSB (Most Significant Bit) は 0 にクリアされる。SAR 制御ロジックは、その後、次のビットダウンに移行し、そのビットを 1 に設定して、次の比較を行う。

このシーケンスは LSB（Least Significant Bit）まで続く。

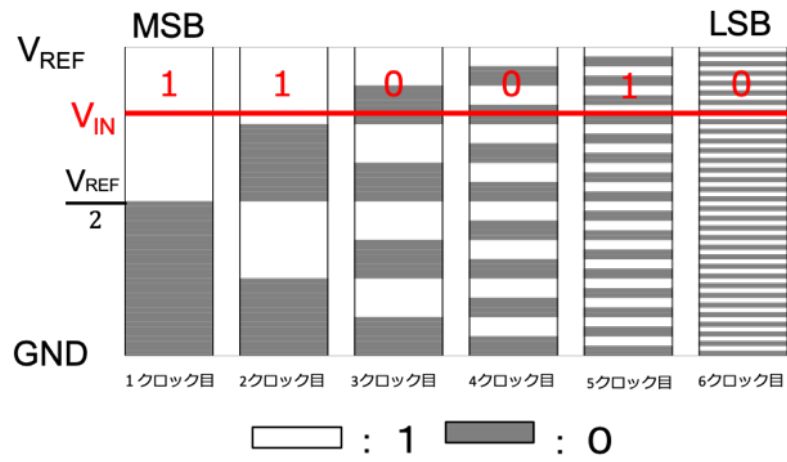


図 2.1 AD 変換の概念図

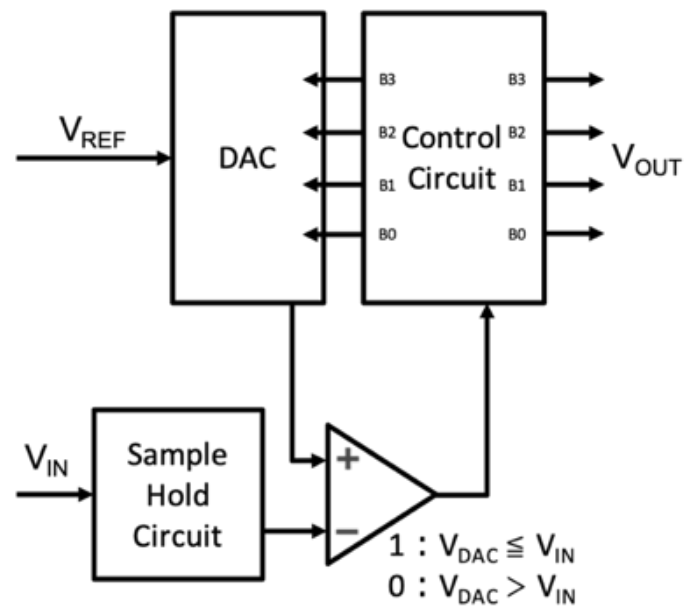


図 2.2 SAR-ADC の回路構成

2.2 SAR-ADC の変換原理に基づく ADC 出力の改ざん手法の提案

本節では、ADC 出力の改ざんの可能性を検討するために、逐次比較型の AD 変換原理に基づく、ADC 出力の真正性を低下させる手法を検討する。

変換原理に基づく手法として、機器内部で生成される基準電圧を含め、内部の電圧を変動させることによって出力値を変動させる手法の検討が必要となる。機器内部の電気信号に影響を与える手法として、レーザー光の照射による攻撃 [5] が報告されているが、機器の筐体により遮断され、機器内部の ADC 回路まで到達させることは困難である。一方で、電磁波の印加による手法 [8] は、筐体を侵襲することなく、機器内部の回路に電気的変動を直接発生させるため効率的に注入できる可能性がある。以上の理由から、本研究では電磁波を用いた意図的な電磁妨害が ADC の出力に与える影響について検討する。

前節の SAR-ADC における変換原理を踏まえ、機器外部の電源線から意図的な電磁妨害を行い、SAR-ADC の値を改ざんする手法を提案する。SAR-ADC の出力は、2.1 節に示した通り、基準電圧とアナログ入力電圧との間で逐次的に比較を行い、その電位差によって出力値が決定される。そのため、基準電圧とアナログ入力電圧の間の電位差が電気的な外乱により変動した場合、正規の出力値とは異なる値が出力される可能性がある。

機器外部の電源線から電磁妨害を行い SAR-ADC のデータを改ざんする手法の原理を図 2.3 に示す。

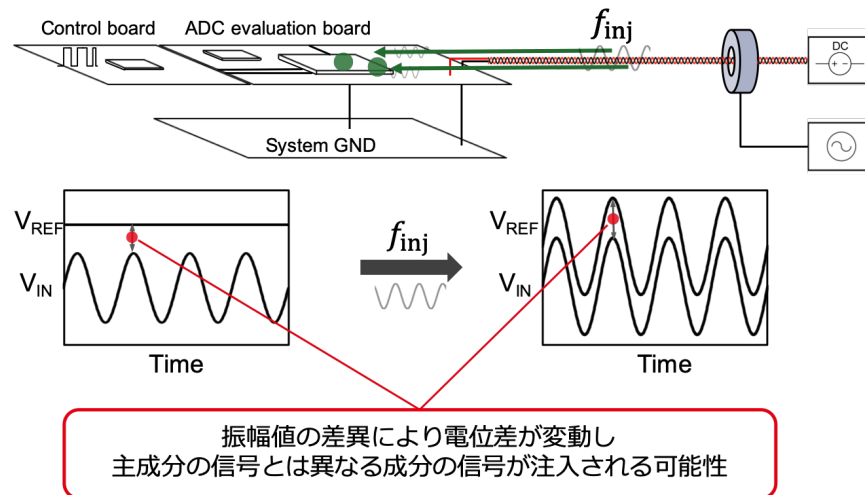


図 2.3 SAR-ADC のデータを改ざんする手法の原理

意図的な電磁妨害によって、ターゲットとなる ADC の評価ボードの遠方から、電源線を通して特定の周波数で正弦波を印加する。電源線に対して妨害電磁波を印加した場合、基板全体に電磁波が分布することで電圧変動が生じ、基準電圧およびアナログ入力電圧においても変動が生じる。この基準電圧およびアナログ入力電圧の変動において、その振幅値は電磁妨害を行う照射源からの伝達関数によって決定される。伝達関数は周囲の IC や素子の実装の違いなどにより異なるため、伝達関数の差異から、基準電圧とアナログ入力電圧においても異なる振幅値で信号が伝播し、伝達関数に応じて基準電圧とアナログ入力電圧の変動に差異が生じると考えられる。本手法では、この特性を利用して、基準電圧に到達するまでの伝達関数とアナログ入力電圧に到達するまでの伝達関数が大きく異なる周波数帯を選択することにより、意図的にアナログ入力電圧と基準電圧の間の電位差に変動を起こし、ADC から出力されるデータを改ざんする。AD 変換において出力値は、基準電圧とアナログ入力電圧の電位差によって決定されることから、基準電圧とアナログ入力電圧が異なる振幅値で変動した場合、主成分の信号とは異なる成分の信号が注入される可能性がある。

主成分の信号とは異なる成分の信号が注入されているかを検証する手法の原理を図 2.4 に示す。

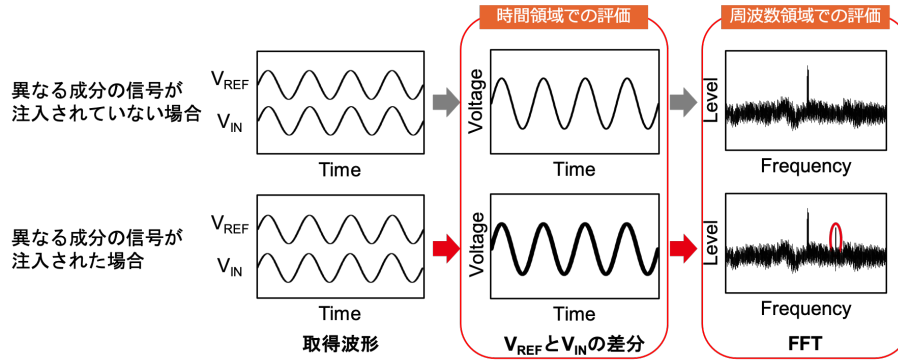


図 2.4 FFT による妨害信号成分の注入を検討する手法の原理

電磁妨害時における基準電圧とアナログ入力電圧の差分を算出し、この差分を FFT 解析することにより周波数領域で評価する。FFT 解析により、電磁妨害に用いた周波数帯にスペクトルが観測された場合、主成分の信号とは異なる成分の信号が注入されていると判断することができる。

2.3 有効ビット数による ADC 出力の真正性の評価

ADC 出力の真正性、つまり ADC 出力の変化を評価する指標として、外部からのノイズによる出力値の変化は有効ビット数で評価される。そのため、本研究では、ADC 出力の真正性を評価する指標として有効ビット数（ENOB: Effective Number of Bits）を用いる。ENOB は雑音や誤差の影響を考慮した際に、十分な精度が得られるビットを示し、ENOB により保証されていないビットは、出力値が変化する可能性がある。そのため、攻撃により ENOB が減少した場合、アナログ入力信号を変換する能力が低下し、センサ入力部において測定した実測値とは異なる値が出力され、後段のシステムへと送られる可能性がある。

次に ENOB を算出する流れについて説明する。ENOB は、下記で示すように、ADC の主要なパフォーマンス要因である SINAD（Signal-to-Noise And Distortion）によって直接導出される [9]。

$$ENOB = \frac{SINAD - 1.76}{6.02} \quad (2.3.1)$$

SINAD は信号対雑音および歪み特性であり、SNR (Signal-to-Noise Ratio) 特性と THD (Total Harmonic Distortion) 特性を総合して、表したものである。したがって SINAD は下記で示す式で定義され、 P_S は信号電力、 P_{ND} は雑音電力と歪み電力の合計を表す。

$$SINAD = 10 \log \frac{P_s}{P_{ND}} \quad (2.3.2)$$

本研究では、上記の式から算出された有効ビット数を用いて、SAR-ADC 出力の真正性を評価する。

続いて、意図的な電磁妨害により、ENOB が低下するメカニズムについて説明する。図 2.5 に示すように、意図的な電磁妨害により、ナイキスト周波数までの帯域においてノイズが注入された場合、信号と歪みの総電力が増加することで SINAD が低下し、有効ビット数が減少する。そのため、伝達関数の差異から、効率良く妨害電磁波が注入され、妨害電磁波の振幅値が大きくなった場合、有効ビット数が大きく減少することが考えられる。

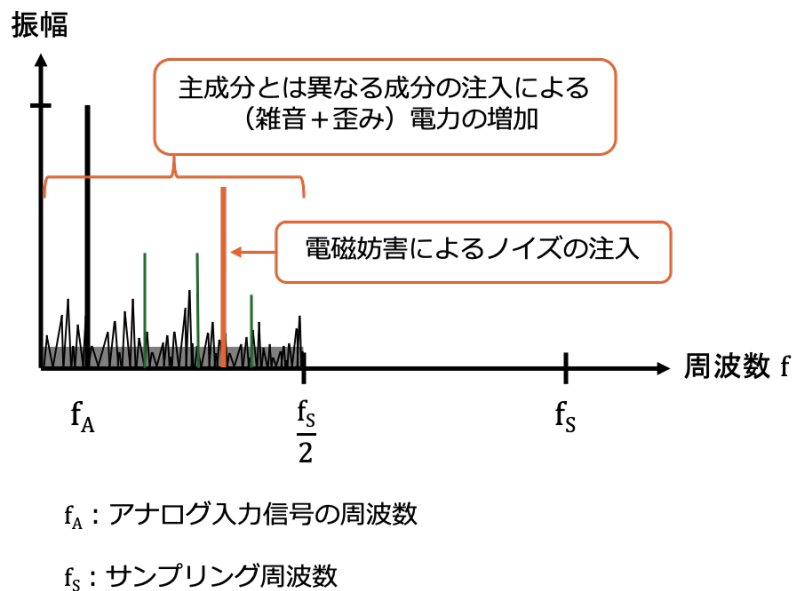


図 2.5 妨害電磁波の注入による有効ビット数の減少

第 3 章 意図的な電磁妨害に対する有効ビット数を用いた逐次比較型 ADC 出力の真正性の評価

3.1 実験環境

図 3.1, 図 3.2, 図 3.3 に本実験のセットアップを示す。ファンクションジェネレータ（エヌエフ回路設計ブロック WF1968）よりアナログ信号として交流電圧を生成し、ADC でデジタル値に変換し、出力値を PC で観測する。本実験ではアナログデバイス社の AD7091R という 12 bit の ADC が搭載された評価ボード、および、評価ボードを制御する SDP-CB1Z という制御ボードを使用した。AD7091R は、基準電圧端子に対して外部から基準電圧を供給しない場合、2.5 V の内蔵基準電圧を生成する。本実験では、この 2.5 V の基準電圧とファンクションジェネレータより入力した 1.25 V の交流電圧で AD 変換を行った。

ADC を搭載した評価ボードへの電源の供給は安定化電源（TEXIO PA36-3B）より 5.0 V を出力しツイストペアケーブルを通して行った。また、意図的な電磁妨害の手法として、シグナルジェネレータ（KEYSIGHT N5181B）から、任意の周波数と強度を設定した正弦波を発生させ、インジェクションプローブ（Fischer Custom Communications, Inc F140）を通して電源線に印加した。これにより、評価ボードの内部で生成される基準電圧とアナログ入力電圧をそれぞれの伝達効率に応じて変動させ、その振幅値の差異によって、正規の電位差とは異なる電位差を生じさせる。

また、基準電圧およびアナログ入力電圧は ADC 評価ボード上のそれぞれのピンより、オシロスコープ（KEYSIGHT DSOS204A）にて測定した。

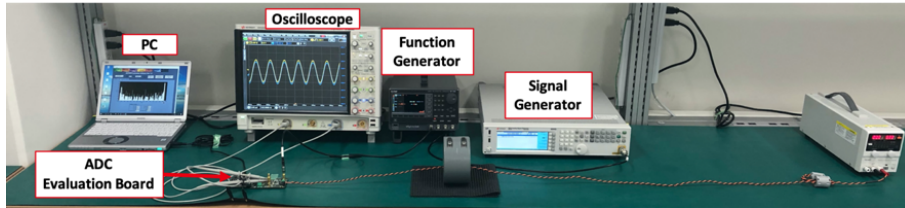


図 3.1 実験セットアップの外観

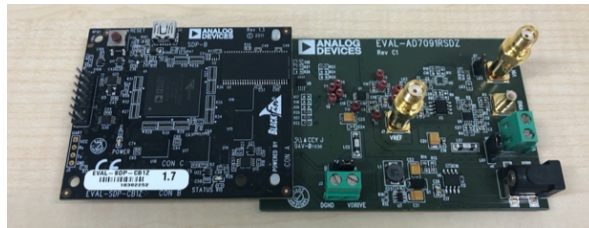


図 3.2 ADC を搭載した評価ボードと制御ボード

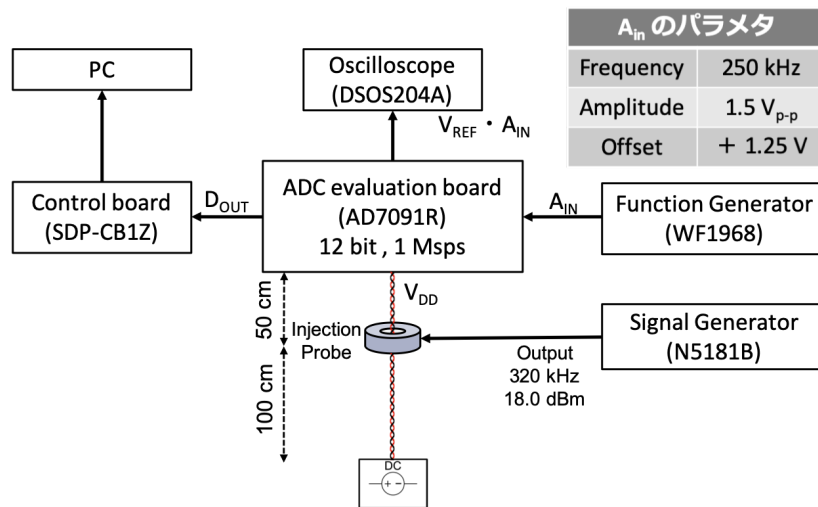


図 3.3 実験セットアップのブロック図とパラメタ

3.2 実験結果

3.2.1 意図的な電磁妨害による基準電圧とアナログ入力電圧の変動

電磁妨害の強度を 18.0 dBm で固定し、100 kHz～490 kHz の範囲で 10kHz ステップで周波数を掃引した中で、最も有効ビット数が低下した 320 kHz における基準電圧とアナログ入力電圧の変動の測定結果を図 3.4 に示す。

実験結果より、正弦波の印加によって、基準電圧とアナログ入力電圧のどちらも変動を確認できた。これは、コモンモードで注入された正弦波が不平衡インピーダンスで終端された線路において、終端ではノーマルモードへと変換されたことによると考えられる [10]。基準電圧とアナログ入力電圧がそれぞれの伝達関数に応じて異なる振幅値で変動した場合、主成分とは異なる成分の信号が注入された可能性がある。そのため、基準電圧とアナログ入力電圧の差分を算出することにより（1）時間領域での評価を行い、基準電圧とアナログ入力電圧の差分を FFT 解析することにより（2）周波数領域での評価を行う。

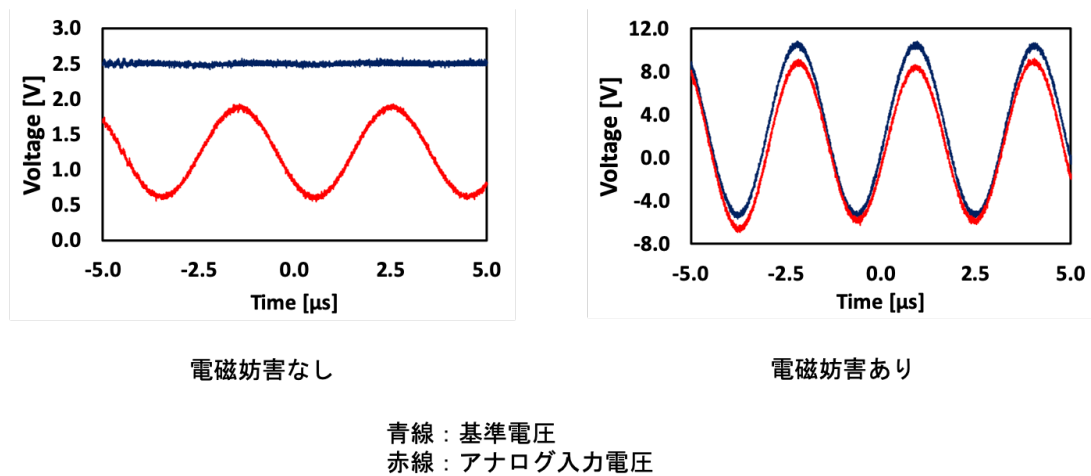


図 3.4 基準電圧とアナログ入力電圧の変動

3.2.2 時間領域および周波数領域での妨害電磁波の注入の検証

(1) 時間領域での評価として、基準電圧とアナログ入力電圧の差分を計算した結果を図 3.5 に示す。時間領域での評価では、電磁妨害により、主成分の信号に妨害電磁波が重畳していることを確認できた。

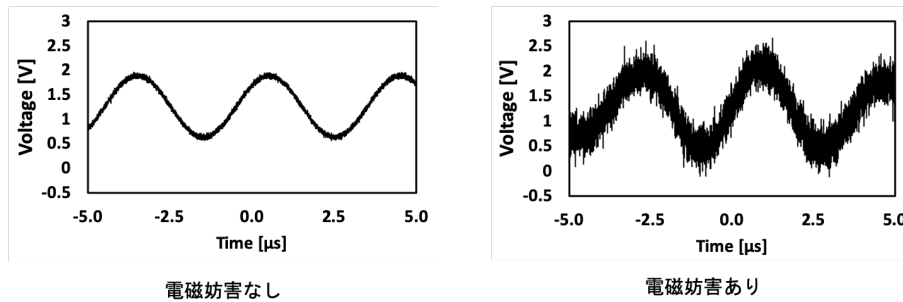


図 3.5 基準電圧とアナログ入力電圧の差分の波形

アナログ入力信号において本来の信号とは異なる成分が注入された可能性があることから、2 章で示した通り、(2) 周波数領域での評価として、基準電圧とアナログ入力電圧の差分を算出し FFT 解析を行った。基準電圧とアナログ入力電圧の差分を FFT した結果を図 3.6 に示す。実験結果より、基準電圧とアナログ入力電圧の差分の周波数成分において、電磁妨害に用いた 320 kHz の周波数帯でスペクトルを確認できた。これにより、基準電圧とアナログ入力電圧までの伝達関数の違いにより電位差が生じ、アナログ入力である主信号とは異なる成分の妨害電磁波の注入を確認できた。

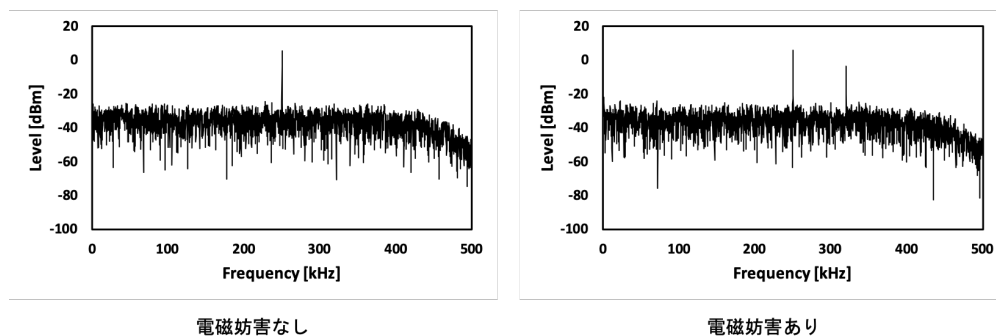


図 3.6 基準電圧とアナログ入力電圧の差分に含まれる周波数成分

3.2.3 周波数掃引・振幅固定による有効ビット数の評価

2.3 で示した式より意図的な電磁妨害を行っていない時の有効ビット数を算出し、その値は 10.27 であった。本実験では、この値との差分をとることにより意図的な電磁妨害によって何ビット低下したかを算出した。印加する周波数を掃引し振幅を固定した際の有効ビット数の低下を図 3.7 に示す。

機器の電源線や通信路を伝わる伝導妨害波に関する EMC 基本規格 (CISPR16-2-1) で定められている 9 kHz から 30 MHz の周波数帯のうち、100 kHz からサンプリング定理を考慮し 490 kHz の範囲の中で 10 kHz ステップで変化させ、18 dBm の強度で印加した。ただし、アナログ入力電圧と同じ周波数である 250 kHz は有効ビットの算出ができないため対象外とした。

図 3.7 より周波数を掃引した場合、320 kHz で最も有効ビット数が低下し、5.69 ビットの低下が観測された。本実験結果より、基準電圧とアナログ入力電圧で大きく伝達効率が異なり、効率よく妨害電磁波が注入される周波数帯において、有効ビット数が大きく低下することが示された。また、有効ビット数の低下により計測機器のデータ変換部において ADC 出力の真正性が低下する可能性があることを示した。

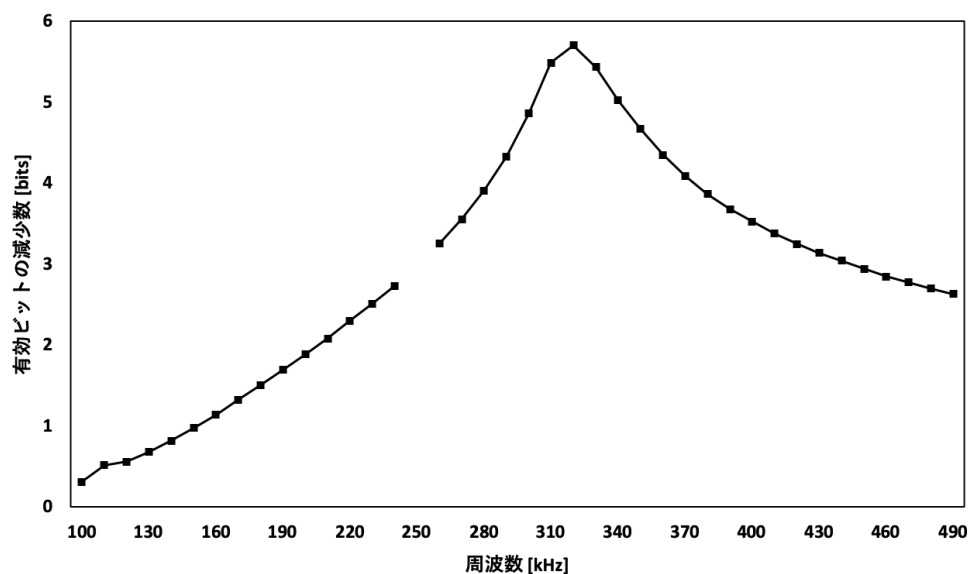


図 3.7 周波数掃引・振幅値固定における有効ビット数の低下

3.2.4 周波数固定・振幅掃引による有効ビット数の評価

周波数固定・振幅掃引における有効ビット数の低下を図 3.8 に示す。電磁妨害のパラメータは、周波数は 320 kHz で固定し、印加した妨害電磁波の強度は -20 dBm から 18 dBm まで 1 dBm ステップで掃引した。

図 3.8 より振幅値を掃引した場合は、電磁妨害の強度を上げることにより、有効ビット数が比例して減少することが観測された。本節では妨害電磁波の強度を -20 dBm から 18 dBm まで掃引し検証を行ったが、本実験結果より、より高い強度の妨害電磁波を印加することにより、より有効ビット数が減少すると考えられる。

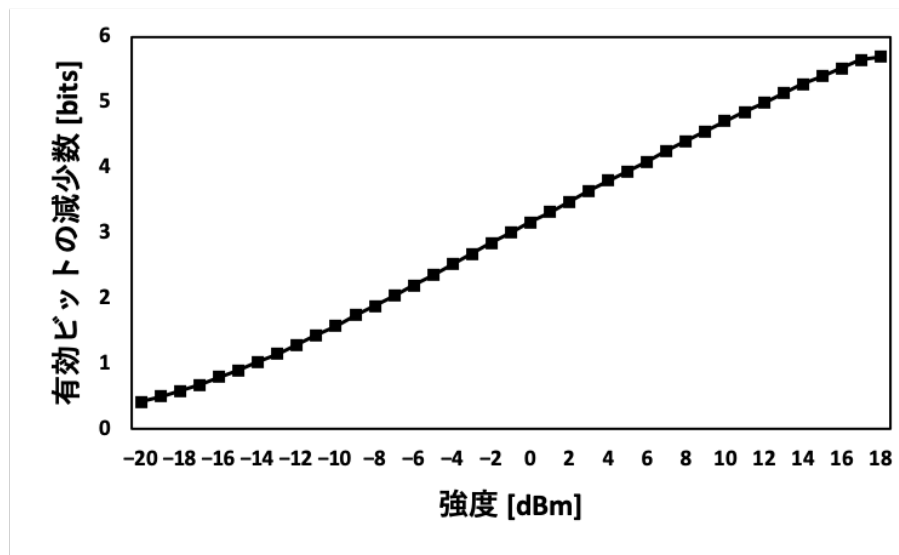


図 3.8 周波数固定・振幅値掃引における有効ビット数の低下

3.3 対策技術の検討

本節では、前節までに示した SAR-ADC に対する意図的な電磁妨害による脅威への対策技術として、妨害電磁波の伝達効率に着目した対策の検討を行う。

意図的な電磁妨害により ADC の有効ビット数を低下させるには、印加する正弦波の周波数と振幅の二つの条件を適切に設定することが必要である。伝達効率は周波数によって異なり、伝達効率の高い周波数の電磁波を印加することで、減衰が少なく効率よく伝達する。このことから、電磁波印加を利用した SAR-ADC への攻撃への対策を検討する方針として、デバイスの設計段階において、基準電圧とアナログ入力電圧の伝達効率が大きく異なる回路構成を避けることが求められる。しかし、回路設計段階において、回路を搭載する基板もしくはデバイスの設置環境全体の伝達効率を考慮することは困難である。そのため、現実的には回路設計後に基準電圧とアナログ入力電圧間の電位差の変動が大きく生じる周波数を評価し、その周波数帯において妨害電磁波を減衰させるフィルタをハードウェアの実装環境において付加する方法が考えられる。

また、簡単な対策手法として、電源線やコミュニケーションケーブルにフェライトコアを巻き付け、妨害電磁波を含むノイズの機器内部への侵入を防ぐ方法が考えられる。

3.4 まとめ

本節では、第 2 章で論じた SAR-ADC 出力の真正性の低下を引き起こす物理攻撃の実現可能性を示すため、逐次比較型 ADC が搭載された評価ボードの遠方から意図的な電磁妨害を行った。有効ビット数を用いた評価により、攻撃者が電磁妨害波の周波数と振幅値を設定できる条件下において、最大で 5.69 ビットの低下が確認された。

本研究では、電源線を通じて、意図的な電磁妨害を行ったが、原理的にはアンテナを用いても同様に有効ビット数の低下を引き起こす可能性がある。また、本実験では ADC を搭載した評価ボードから 50 cm の位置から電磁波を印加したが、信号の減衰率を考慮して印加する電磁波のエネルギーを増大させることにより、より遠方からの攻撃も可能になると予想される。そのため、筐体で覆われた機器に搭載された ADC を対象とした場合においても、意図的な電磁妨害に対する適切な対策が必要であると考えられる。

第 4 章 結論

本論文では、物理的な攻撃により ADC 出力の真正性が低下するかを評価するために、意図的な電磁妨害を用いて機器に電圧変動を発生させることで、逐次比較型 ADC の有効ビット数の低下を誘発する手法を提案し、上述した目標を達成するために各章では以下について議論した。ADC の出力に影響を与える攻撃の実現可能性を検討するとともに、ADC の出力に与える影響を評価する手法を提案し、評価を行った。

第 2 章では、SAR-ADC の AD 変換原理に基づく、意図的な電磁妨害による攻撃の実現可能性を示した。また、有効ビット数を用いた ADC 出力の真正性の評価と意図的な電磁妨害が有効ビット数の低下を引き起こすメカニズムを示した。

第 3 章では、実験を通じて、意図的な電磁妨害により基準電圧とアナログ入力電圧が、それぞれの伝達関数に応じて異なる振幅値で変動することを基準電圧とアナログ入力電圧の差分を FFT 解析することにより示した。これにより、基準電圧とアナログ入力電圧間において、電位差に変動が発生し、有効ビット数が低下することを示した。また、有効ビット数の低下を引き起こす意図的な電磁妨害に対する対策として、フェライトコアやフィルタを用いた手法を提案した。

以上の議論より、本論文で提案した電源線に対する意図的な電磁妨害により、計測機器のデータ変換部である ADC において ADC 出力の真正性が低下し、新たな脅威となり得ることを示した。本論文では、評価ボードにおいて、基準電圧とアナログ入力電圧までの伝達関数が大きく異なる周波数で妨害電磁波を印加することにより、有効ビット数が低下することを示したが、ADC を搭載した実際のデバイスにおいて、ADC の実装に応じてより大きく有効ビット数が低下する可能性があることから、ADC の実装に応じて EMC 対策などを適用し、システムを運用することが求められると考えられる。

謝辞

本論文は、奈良先端科学技術大学院大学先端科学技術研究科情報セキュリティ工学研究室において研究を行ったものです。末筆ながら、本研究を行うにあたり、ご支援下さった皆様に深く感謝の意を表します。

本学林優一教授には、日頃の研究活動において熱心な御指導、御鞭撻さらに研究者発表の機会を賜りました。ここに心より感謝申し上げます。

本学岡田実教授および安本慶一教授には、研究を進めるにあたり有益な御助言・御討論を頂き、心より御礼申し上げます。

本学藤本大介助教には、研究方針の策定や、研究活動においての多くの御支援、御助言を賜り、学会参加においても多大な御支援をいただきました。厚く御礼申し上げます。

本学 Youngwoo Kim 助教には、本研究生生活の中で適切な御助言と細部にわたる御支援を賜りました。厚く御礼申し上げます。

仙台高等専門学校の衣川昌宏助教には、実験の御指導や御助言を賜りました、厚く御礼申し上げます。

本研究室秘書の石谷由美様には、学会参加のお手続きや研究室運営などをはじめ、様々な面でお世話になりました。深く感謝申し上げます。

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、家族には、2年間の学業生活を様々な面から支えて頂きました。心より感謝申し上げます。

参考文献

- [1] 次世代センサ協議会, “センシング技術の普及とこれからの社会,” <http://www.jisedaisensor.org/PDF/J30sensor.pdf>.
- [2] H. Shin, D. Kim, Y. Kwon, and Y. Kim, “Illusion and dazzle: Adversarial optical channel exploits against Li- dars for automotive applications,” Proc. Conference on Cryptographic Hardware and Embedded Systems (CHES 2017), 2017.
- [3] Y. Son, H. Shin, D. Kim, Y. Park, J. Noh, K. Choi, J. Choi, and Y. Kim, “Rocking drones with intentional sound noise on gyroscopic sensors,” Usenix Security, 2015.
- [4] Drew Davidson, Hao Wu, Robert Jellinek, Vikas Singh, and Thomas Ristenpart, “Controlling uavs with sensor input spoofing attacks,” In WOOT, 2016.
- [5] Loughry, “("Oops! Had the silly thing in reverse")- Optical injection attacks in through LED status indicators,” International Symposium on Electromagnetic Compatibility (EMC EUROPE), pp.376-382, 2019.
- [6] J. McCreary and P. R. Gray, “All-MOS charge redistribution analog-to-digital conversion techniques - Part I,” IEEEJ.Solid-State Circuits, vol.SC-10, no.6, pp.371-379, Dec. 1975. International Symposium on Electromagnetic Compatibility (EMC EUROPE), pp.376-382, 2019.
- [7] T. Sugawara, B. Cyr, S. Rampazzi, D. Genkin, and K. Fu, “Light Commands: Laser-Based Audio Injection Attacks on Voice-Controllable Systems,” 2019.
- [8] W. Radasky, C. Baum, and M. Wik, “Introduction to the special issue on high-power electromagnetics (HPEM) and intentional electromagnetic interference (IEMI),” IEEE Transactions on Electromagnetic Compatibility, Mar, 2004.
- [9] Shayan Taheri, Jie Lin and Jiann-Shiun Yuan, “Security Interrogation and Defense for SAR Analog to Digital Converte,” MDPI, Electronics,

volume6, issue2, 10.3390/electronics6020048.

- [10] 赤尾保男, 環境電磁工学の基礎, 社団法人電子情報通信学会, 1993.

発表リスト

[1] 江頭智也, 藤本大介, 林優一, “電磁照射を用いた逐次比較型 ADC の出力データ改ざん手法に関する研究,” ハードウェアセキュリティ夏のワークショップ, 2019.9.26.

[2] 江頭智也, 藤本大介, 林優一, “逐次比較型 ADC 出力の意図的な電磁妨害耐性評価環境の構築,” IEEE EMCS 仙台チャプタ 学生研究発表会, 2020.2.20.