

修士論文

モータ制御信号への電気的外乱印加が スマートロック動作に与える影響評価に関する研究

中尾 文香

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。

中尾 文香

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）
小笠原 司 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）

モータ制御信号への電気的外乱印加が スマートロック動作に与える影響評価に関する研究*

中尾 文香

内容梗概

スマートロックシステムは認証と暗号化によりセキュリティが確保されている。一方、これらのセキュリティが確保される範囲は開閉動作を担うモータ制御部までは含んでおらず、制御信号が電気的外乱により、盗聴・改ざんされ、強制的に施錠/開錠される可能性がある。本研究では、こうした脅威を評価するため、スマートロックシステムの施錠/開錠に必要なモータ制御部を抽出した単純な評価系を構築し、外部からの電気的な外乱を与えることにより、施錠/開錠に関わる制御信号の改ざん可能性を評価する。また、評価結果に基づき、電気的な外乱に耐性を有する制御部の設計法について議論する。

キーワード

スマートロック, モータ制御通信, 電気的外乱

*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.

Study on Electric Disturbance Impacts on Motor Control Signal to Generate Smart Lock Malfunction*

Ayaka Nakao

Abstract

The security of the smart lock system is secured by verification and encryption processes. On the other hand, the range in which the security is ensured does not include the motor control unit which is responsible for opening and closing operations. As a result, there is a possibility that control signals can be intercepted and tampered by the electric disturbance, which can forcibly locked/unlocked the door with smart lock. In this study, in order to evaluate these threats, we proposed evaluation system that extracts the motor control unit which is required for locking / unlocking the smart lock system. Then, an electrical disturbance is injected to the proposed evaluation system to lock / unlock the smart lock system to evaluate the possibility of tampering of control signals related to unlocking. In addition, based on the evaluation results, a method of designing a control unit that is resistant to the electrical disturbance is proposed.

Keywords:

Smart Lock, Motor Control Communication, Electrical Disturbance

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

目次

図目次		v
第 1 章	序論	1
1.1	研究背景	1
1.2	本研究の目的	4
1.3	本論文の構成	5
第 2 章	スマートロック機器内部の信号改ざんに関する評価のための対象 の分類と故障注入法の提案	6
2.1	電磁波を用いたスマートロック機器外部からの信号改ざんの検討 .	6
2.2	スマートロックに用いられるモータドライバの分類	9
2.3	スマートロック機器内部の信号改ざんに関する故障注入法の提案 .	15
第 3 章	スマートロック機器内部の信号改ざんに関する故障注入実験	17
3.1	データ通信型モータドライバに対する故障注入実験	17
3.1.1	データ通信型モータドライバに対する故障注入実験の実験 セットアップ	18
3.1.2	データ通信型モータドライバに対する故障注入実験の実験 結果	19
3.2	2 信号タイミング型モータドライバに対する故障注入実験	21
3.2.1	2 信号タイミング型モータドライバに対する故障注入実験 の実験セットアップ	22
3.2.2	2 信号タイミング型モータドライバに対する故障注入実験 の実験結果	23
3.3	考察・対策	25
第 4 章	結論	29
謝辞		30

参考文献	31
発表リスト	34

図目次

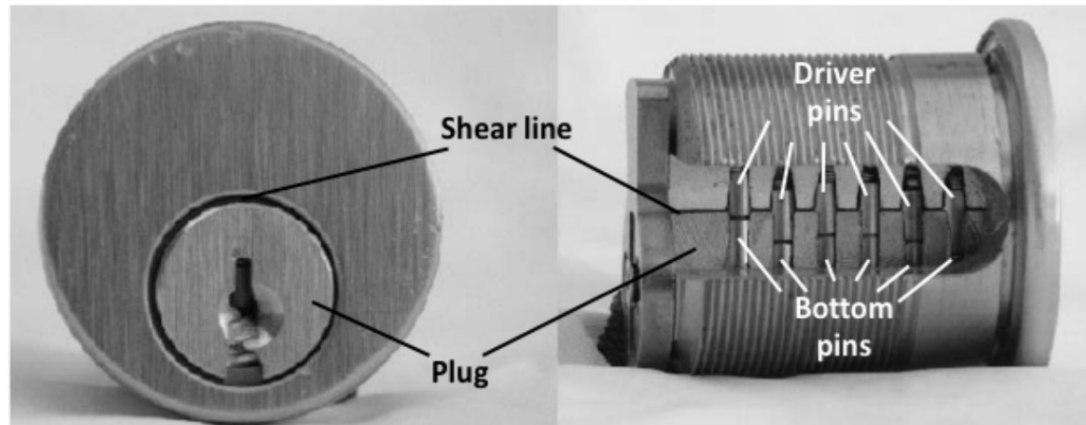
1.1	ピンタンプラー錠	2
1.2	スマートロックシステムの構成のブロック図	3
2.1	電磁波の伝達特性を用いた特定箇所への注入アプローチの概念図	7
2.2	電磁波注入による電気信号の改ざんの仕組み	9
2.3	データ通信型モータドライバの開錠信号例	11
2.4	2 信号タイミング型モータドライバの開錠信号例	13
2.5	3 信号タイミング型モータドライバの開錠信号例	14
3.1	データ通信型モータドライバの制御信号への故障注入実験のブ ロック図	18
3.2	パルスジェネレータの回路図	18
3.3	データ通信型モータドライバの制御信号への故障注入実験の外観	19
3.4	パルス波注入時のクロック信号波形	20
3.5	パルス波注入後のモータ電圧の変化	21
3.6	2 信号タイミング型モータドライバの制御信号への故障注入実験の ブロック図	22
3.7	2 信号タイミング型モータドライバの制御信号への故障注入実験の 外観	23
3.8	強制的に開錠が確認された際のモータドライバ信号線に発生した 電圧の時間応答波形	25

第 1 章 序論

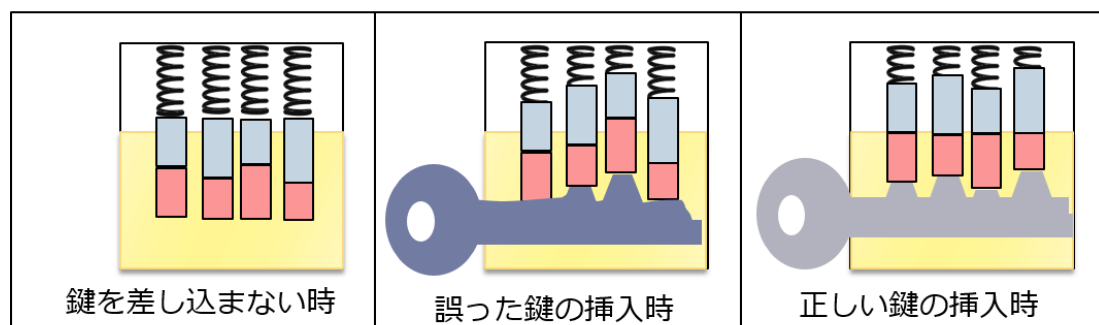
1.1 研究背景

古代から所有物や自分自身を他人から守るために鍵が用いられてきた。その始まりは紀元前の蝶番から始まり、鍵は時代が進むにつれ利便性を高めつつ脆弱性をなくす努力が施され、今では様々な鍵の種類が日常で使われている [1]。鍵のセキュリティの安全性で重要な点は、第三者の施錠/開錠が不可能である点である。一般的に、扉の物理鍵として用いられている鍵としてピンタンプラー錠がある。この鍵の構造と仕組みを図 1.1 に示す。外筒と内筒の 2 重管構造になっており、内筒が回転することで施錠/開錠される。内筒には鍵を差し込むための細長い穴が空いており、キーウェイと呼ばれる。鍵とキーウェイは不正な開錠が行われないように凹凸が付けられており、施錠/開錠の際に鍵穴の形状と鍵のブレード部分の溝が合わないと差し込めない仕組みである。キーウェイの上部にはピンが 5・6 本並んでおり、ピンは上部のドライバーピンと下部のキーピンに分けられる。ドライバーピンと外筒は押しバネで繋がれており、鍵を差し込んでいない状態ではこのバネの力でドライバーピンが内筒まで食い込み、内筒が回転しないようになっている。鍵が正常に差し込まれた場合、差し込まれた鍵のブレード部の鍵山がピンを上下させ、ドライバーピンとキーピンの切れ目が内筒と外筒の境界線上に並ぶと内筒を回転させることができ、施錠/開錠が可能となる。この物理鍵のセキュリティの安全性担保は、鍵穴ごとに作られる特有のキー溝が物理鍵に適合すること、鍵山がドライバーピンとキーピンの切れ目を内筒と外筒の境界線上に並べることが可能であることに依存する。つまり、これらを満たす物理鍵でないと施錠/開錠が出来ず、他の扉と同じ鍵は存在しない。また、複製する際も鍵の個々の特有な情報が必要なため、複製元となる物理鍵を用意する必要があり、基本的に第三者が施錠/開錠が出来ない点で、セキュリティが担保されている。しかし、この鍵の問題点としては、所有者の物理鍵の紛失や貸し出しにより、第三者が鍵を入手することで、物理鍵の複製や扉内部への侵入が可能となる点である。また、近年では、カメラの高解像度化やコンピュータ技術の向上などの技術の発展により、鍵の写った画像から、その鍵特有の溝や形などを推定することで、立体モデルを生成し、そのモデルを用いて 3D プリンター

で造形することで鍵の複製が可能であり、第三者に鍵を施錠/開錠される脅威についても報告されている [2]。



(a) ピンタンプラー錠の内部構造と名称 [2]



(b) ピンタンプラー錠の仕組み

図 1.1 ピンタンプラー錠

そうした状況の中、近年身の回りのあらゆるものがインターネットにつながる、モノのインターネット (IoT: Internet of Things) 技術の普及により、従来の物理鍵の問題点を解決する新しいデバイスであるスマートロックシステムが登場した。スマートロックシステムの施錠/開錠に用いられる構成を図 1.2 に示す。スマートロックシステムは、スマートキーと呼ばれる個々の鍵に紐づいた秘密情報を保持するデバイスと、扉に取り付けられたスマートロック本体で構成される。スマート

ロック本体は、スマートキーとの無線通信を行い、スマートキーの操作に基づいて物理鍵を施錠/開錠する。スマートロック本体で施錠/開錠の動作に関わる部分は通信部、処理部、駆動部に大別される。通信部はスマートキーと無線通信を行い、処理部では通信部から受け取ったデータを用いてスマートキーの認証を行い、施錠/開錠の制御を行う。駆動部は処理部からの命令に基づいて、物理的にドアのサムターンなどを回すためにモータを駆動する。スマートロックシステムは、従来の物理鍵を使用する方法とは異なり、鍵を電子データとすることで、従来の鍵の問題であった物理鍵の紛失や複製の危険性を排除する可能性がある。また、スマートロックシステムは、電子データを用いていることから、鍵の施錠/開錠のみならず、電子データの使用履歴から人の出入りの追跡や、スマートキーの全地球測位システム (GPS: Global Positioning System, Global Positioning Satellite) 等を用いることでスマートキーの操作なしスマートロックとの距離によって施錠/開錠が出来るハンズフリーや、特定の人に対し鍵を期限付きで共有するなど、様々な機能を付与することが可能な機器も流通している [3]。上記で述べた利便性の向上から、スマートロックシステムは急速に普及が進みつつある [4]。

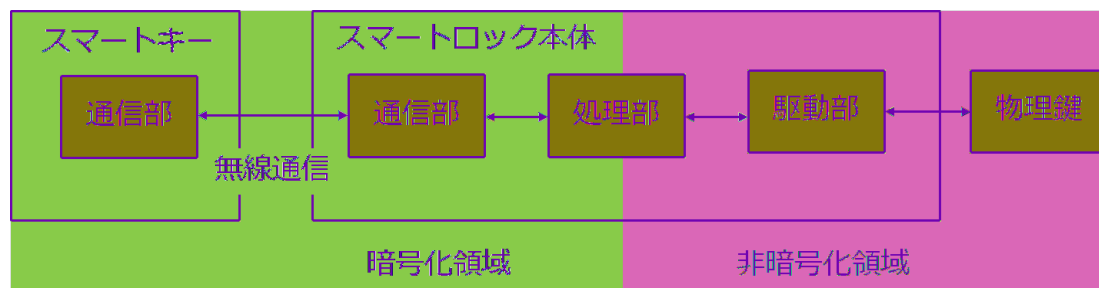


図 1.2 スマートロックシステムの構成のブロック図

しかし、スマートロックには従来の物理鍵とは別の問題点が存在する。スマートロックは、電子データを扱うことでセキュリティ安全性を担保しているため、電子データを第三者に盗聴、改ざんされると施錠/開錠が可能となる。通信部とスマートキー間の無線通信では、Bluetooth や Wi-Fi などの通信プロトコルに従ってデータは暗号化されている [5][6]。また、処理部ではスマートキーの認証や他の機能からのデータを基にスマートロック全体の制御を行うため、演算機能を持つ集積回路

(IC: Integrated Circuit) が用いられる。演算機能を持つ IC は実装方法によって、暗号アルゴリズムのハードウェアの実装が可能であるため [7]、通信部と処理部の間の通信においてもデータが暗号化されている可能性がある。

暗号化されている通信においては、第三者による改ざんがなされた場合でも、復号時に検出が可能なため、無効な命令信号であることを判断することが可能である。また、通信部と処理部の間の通信が暗号化されていない場合でも、スマートロック本体は正しい鍵による施錠/開錠命令か否かの認証を行う。そのため、正規のユーザのみがもつ秘密情報が漏えいしない限り、第三者が施錠/開錠命令を発行することは困難であり、この部分に対する攻撃により、スマートロックが強制的に施錠/開錠される可能性は少ないと考えられる。

一方、下位レイヤーである物理層の IC 間の通信では、データの暗号化や認証が行われていないことが多い [8][9][10][11]。これは、機器内部で完結した通信路であることや、駆動部に搭載されるモータドライバ IC は、高い電圧をモータへ出力する機能に特化しており、演算機能を有するものが少ないためである。このような通信路においては、攻撃者が通信路に流れている信号を解析可能であり、同じ信号を生成できる可能性がある。改ざんされた信号を注入された場合、データ認証が行われないため、駆動部は改ざんされた信号に基づいて動作を行う。また、スマートロックの内部信号の改ざんは、電氣的な外乱を与えることで可能であると考えられる。つまり、スマートロックはモータを駆動源として施錠/開錠を行うため、電氣的な外乱によるモータの制御信号の改ざんによって、強制的に鍵を施錠/開錠される可能性がある。よって、正規のユーザのみがもつ秘密情報を第三者が保持していなくても、スマートロック本体内部の IC のプロトコルを解析することで、施錠/開錠できる可能性があり、鍵としてのセキュリティの安全性が担保されないため、重要な問題である。

1.2 本研究の目的

前節では、スマートロックに対して、無線通信やソフトウェアが安全に実装されていた場合において、モータの制御信号等が暗号化されていないことから、施錠/開錠されるリスクがあることに着目し、重要な問題であることを示した。

本研究では、スマートロック機器外部から注入された電気的外乱による、施錠/開錠の可能性の評価を目的とする。具体的には、施錠/開錠される脅威について評価するために、スマートロックシステムの施錠/開錠に必要な要素を抽出した評価系を構築し、外部からの電気的な外乱を与えることにより、施錠/開錠に関わる制御信号の改ざん可能性について評価する。また、実験結果に基づき、電気的な外乱に耐性を有する制御部の設計法について議論する。

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、電磁波を用いたスマートロック機器外部からの信号改ざんについて検討し、モータドライバを制御信号の特徴ごとに分類をする。続いて、その特徴別分類を行ったモータドライバごとに、スマートロック機器内部の信号改ざんに関する故障注入法について提案する。第3章では、スマートロックシステムに対し、第2章で提案した故障注入法を用いて、施錠/開錠の可能性について評価を行う。また、得られた結果から、対策手法として制御部の設計法について検討を行う。第4章では本論文のまとめを行う。

第 2 章 スマートロック機器内部の信号改ざんに関する 評価のための対象の分類と故障注入法の提案

本章では、電磁波を用いたスマートロック機器外部からの信号改ざんについて検討し、モータドライバを制御信号の特徴ごとに分類を行う。最後にその特徴別分類を行ったモータドライバごとにスマートロック機器内部の信号改ざんに関する故障注入法について提案する。

2.1 電磁波を用いたスマートロック機器外部からの信号改ざんの 検討

本節では、スマートロックの内部信号の改ざんを引き起こす手法について検討する。まず、スマートロック本体は扉の内側に設置されることが多いことから、機器を破壊せずに内部に開錠信号を入力することが求められる。破壊せずに内部に信号を入力するには、機器本体やドアもしくは空間を通じて機器内部の電気信号に影響を与える手法が必要である。機器内部の電気信号に影響を与える方法としてレーザー光を用いた攻撃 [12][13] が報告されているが、外側から扉の内側に設置されたスマートロックにレーザーを到達させることは扉の材質やスマートロック本体の金属やプラスチックのカバーにより遮断されるため困難である。

それに対して、電磁波を用いた手法では、扉やスマートロック本体カバーなどの障害物に遮断されることなくスマートロックに到達、または扉の金属部やスマートロック機器の金属部に伝搬し、機器の内部信号に到達する可能性がある。さらに、機器内部の IC 間の線路長等に依存する伝搬特性を用いることで特定の電気信号に対して電気的変動を直接発生させるため効率的な注入が期待できる。機器外部から到来する電磁波は、機器に接続されたケーブルや電源線に電圧を誘起して機器に誤動作（一時的な故障）を引き起こすことが知られている。機器外部から到来する電磁波は、図 2.1 に示すように機器の各部位に到達するまでの減衰率が異なる。つまり、特定のモジュールに到達するまでの減衰率が少なく、他の機能への妨害が小さい周波数を選択することで特定のモジュールに対して一時的な故障を注入することが可能である。また伝搬特性は注入する位置で観測される放射電磁波の周波数成分

と密接に関係していることが多く、その周波数成分から伝達特性の良い周波数を推定できる可能性が高い [14]。つまり、プローブとスマートロック内部の対象とする通信路までの伝達特性の良い周波数を推定することで電磁波を注入出来る可能性がある。

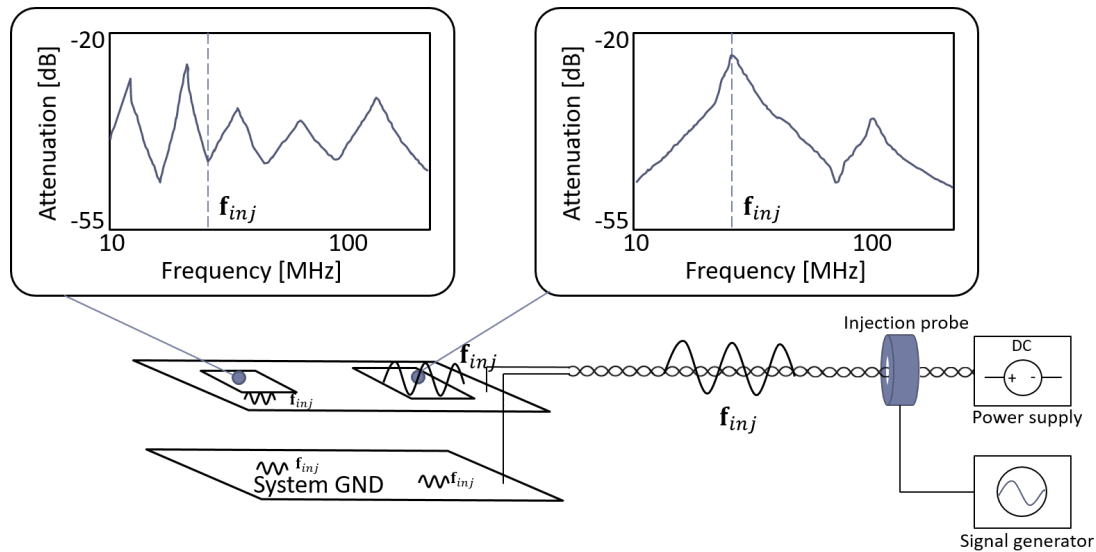
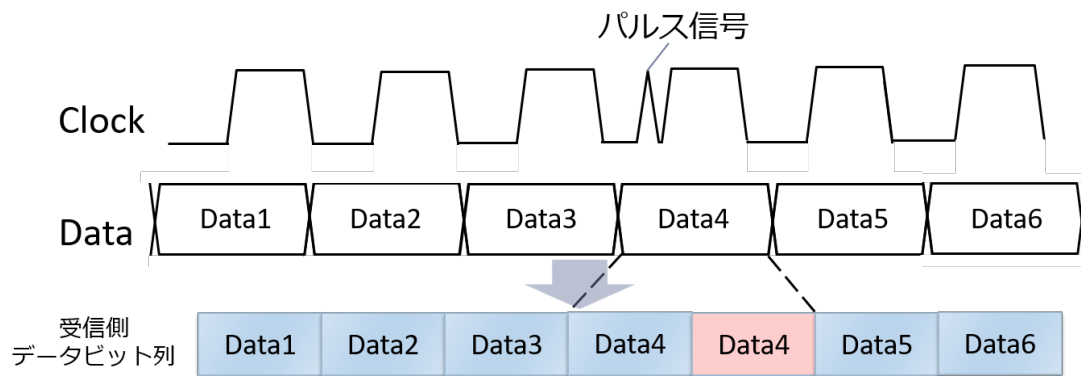


図 2.1 電磁波の伝達特性を用いた特定箇所への注入アプローチの概念図

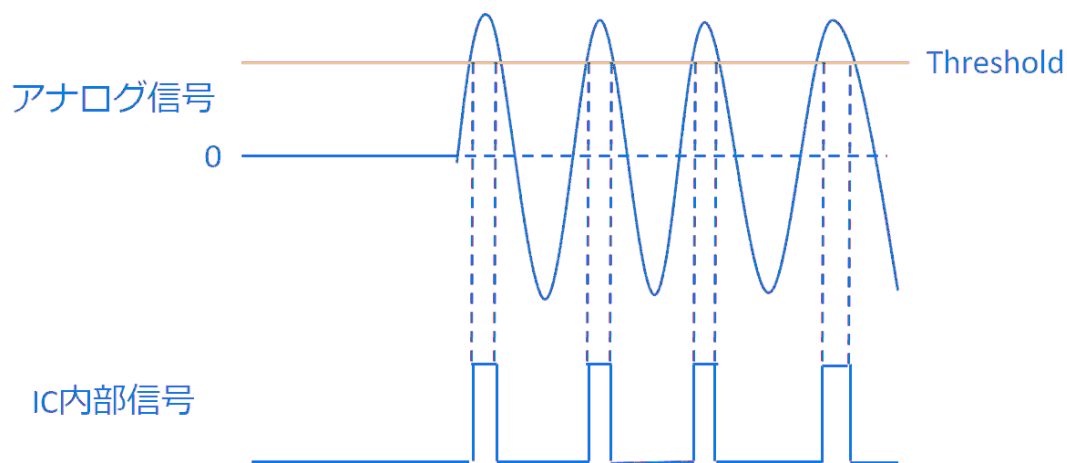
電磁波を用いた故障注入法として、瞬間的な変動を引き起こすパルス波を用いる手法 [15][16] と連続正弦波を用いる手法 [17] が存在する。パルス波を注入する手法では、図 2.2(a) のような信号列に電位変動を注入することが可能である。例えば、クロック信号にパルス波を重畳させることでデータの読み取り位置を変更することや、本来一度しか読めないデータを重複して読み取りさせることなどが考えられる。それにより、送信されているデータを改ざんすることが可能である。一方で、パルス波は短い変動であるため、注入した電位変動が IC の性能上読み取れない場合は有効な手法ではない。連続正弦波を注入する手法では、図 2.2(b) のように信号線に対して連続的に電位変動を発生させる。連続的な電位変動は、IC の入力回路によりアナログ信号からあるしきい値で 1/0 のデジタル信号に変換されるため、しきい値を超えるような振幅の信号を重畳することで、本来 0 となっている信号に対

して 1 を一定時間入力することが可能である。その時間は、入力する連続正弦波の周期と振幅および対象 IC のしきい値に依存する。

上記より、スマートロックの処理部と駆動部の間もしくは駆動部内の通信路に、パルス波もしくは連続正弦波を用いて信号の改ざんを行った際、その電気信号が正規の制御信号であると駆動部が認識すれば強制的に施錠/開錠することが可能であると推測できる。処理部と駆動部の通信路としては、処理部の IC とモータドライバ間の通信路、駆動部内の通信路としてはモータドライバとモータ間の通信路が一般的に考えられる。上述の 2 つの通信路を注入対象とした場合、モータの駆動電圧は処理部からの電気信号の電圧に比べて高電圧であることから、電磁波注入によりモータ駆動電圧に電位変動を発生させるためには処理部の IC とモータドライバの通信路へ注入するより高い電位変動を発生させる電磁波が必要となる。そこで、今回は、比較的発生させる電位変動が小さい処理部の IC とモータドライバ間の通信路への注入について検討する。また、第三者による攻撃として施錠ではなく開錠が行われると考えられるため、以降は開錠についてのみ述べる。



(a) パルス波



(b) 連続正弦波

図 2.2 電磁波注入による電気信号の改ざんの仕組み

2.2 スマートロックに用いられるモータドライバの分類

市場に流通するスマートロックのモータドライバへの制御信号には規格が存在しておらず、モータの駆動に用いられるモータドライバへの制御信号には様々な方式が存在する [8][9][10][11]。そこで、本節では、スマートロックに使用されるモータドライバを制御信号の特徴別に分類する。

スマートロックに用いられるモータドライバへの動作命令は正転、逆転、停止といった複数の動作が存在するため 1 つの信号線で通信を行うことは困難であり、複

数の信号線を使うものが多い。モータの機能は正転、逆転、停止と惰走の4つであり、モータドライバに直接データを送信することや表 2.1 に示した例のようにモータドライバへ信号を入力する信号線 (Input) の High/Low を 2 つ組み合わせることでモータの機能を実現することが可能である。また信号線の本数が増えるにつれて、処理部とモータドライバ間で使われる信号線の増加のコストや信号の複雑化などにより汎用性が低くなる。すなわち、モータドライバの汎用性の観点から以下の 3 種類に分類できる。

1. クロック信号とデータ信号を用いて制御データを通信し制御するデータ通信型 [8]
2. 2 本の信号線を用いてそれぞれの High/Low を組み合わせることにより正転/逆転/停止/惰走を割り当てる 2 信号タイミング型 [9]
3. 3 本の信号線の信号タイミングを組み合わせることによって回転の向きや角度、停止の動作を決定する 3 信号タイミング型 [10][11]

上記の 3 種類のモータドライバの制御信号を調査し、その特徴を示す。

表 2.1 入力 High/Low の組み合わせによる動作原理の一例

Input1	Input2	機能
High	Low	正転
Low	High	逆転
High	High	停止
Low	Low	惰走

データ通信型のモータドライバは、処理部の IC との通信でデータビットを送信するデータ信号線とタイミングを同期するクロックを送信するクロック信号線を用いて通信を行う。今回はデータ信号線とクロック信号線を 1 本ずつ、合計 2 本の信号線を用いて通信を行う I^2C (Inter-Integrated Circuit) 通信を例に検討を行う。 I^2C 通信を行うモータドライバとして DRV8830 [8] を用意し、モータを駆動する際に処理部の IC からモータドライバへ流れる信号例を図 2.3 に示す。通信のデータレートは 400 kbps であった。図 2.3 に示すように、クロック信号の区切りから 3 つのブロックに分けることができる。1 ブロック目は通信するデバイスのスレーブアドレスを示し、2 ブロック目はサブアドレスを示し、3 ブロック目はデータ部分でモータの出力電圧や動作を示す。モータの動作は、データ部分の下位 2 bit の 1/0 の組み合わせで、表 2.2 で示したように決定する。

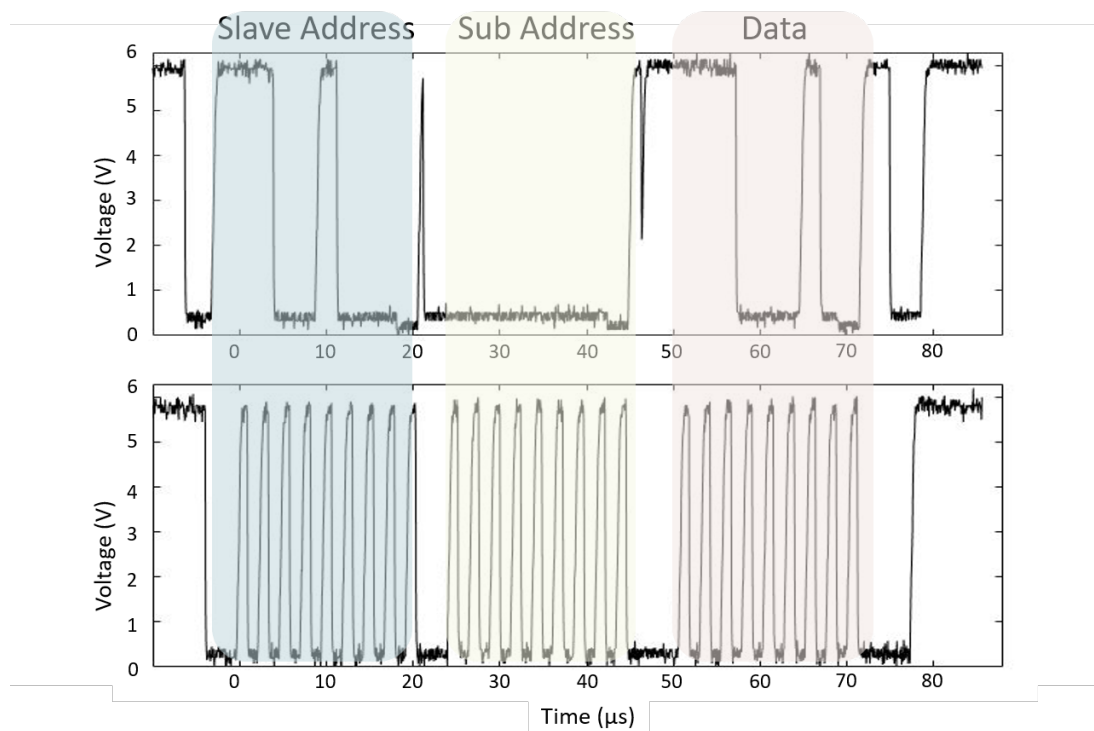


図 2.3 データ通信型モータドライバの開錠信号例

表 2.2 データ通信型モータドライバの動作原理 [8]

Data1	Data2	Output1	Output2	機能
0	0	開放	開放	スタンバイ/惰走
0	1	Low	High	逆転
1	0	High	Low	正転
1	1	High	High	ブレーキ

2 信号タイミング型のモータドライバは、表 2.3 のように 2 本の信号線の 1/0 を組み合わせることで、正転/逆転/停止といった動作決定を行う。このようなモータドライバとして L9110 [9] を用意し、モータを駆動する際に処理部の IC からモータドライバへ流れる信号例を図 2.4 に示し、モータの動作決定を表 2.3 に示す。2 本ある信号線のうち、一方の信号線の入力信号が High で、もう一方が Low であればモータが回転する仕組みである。

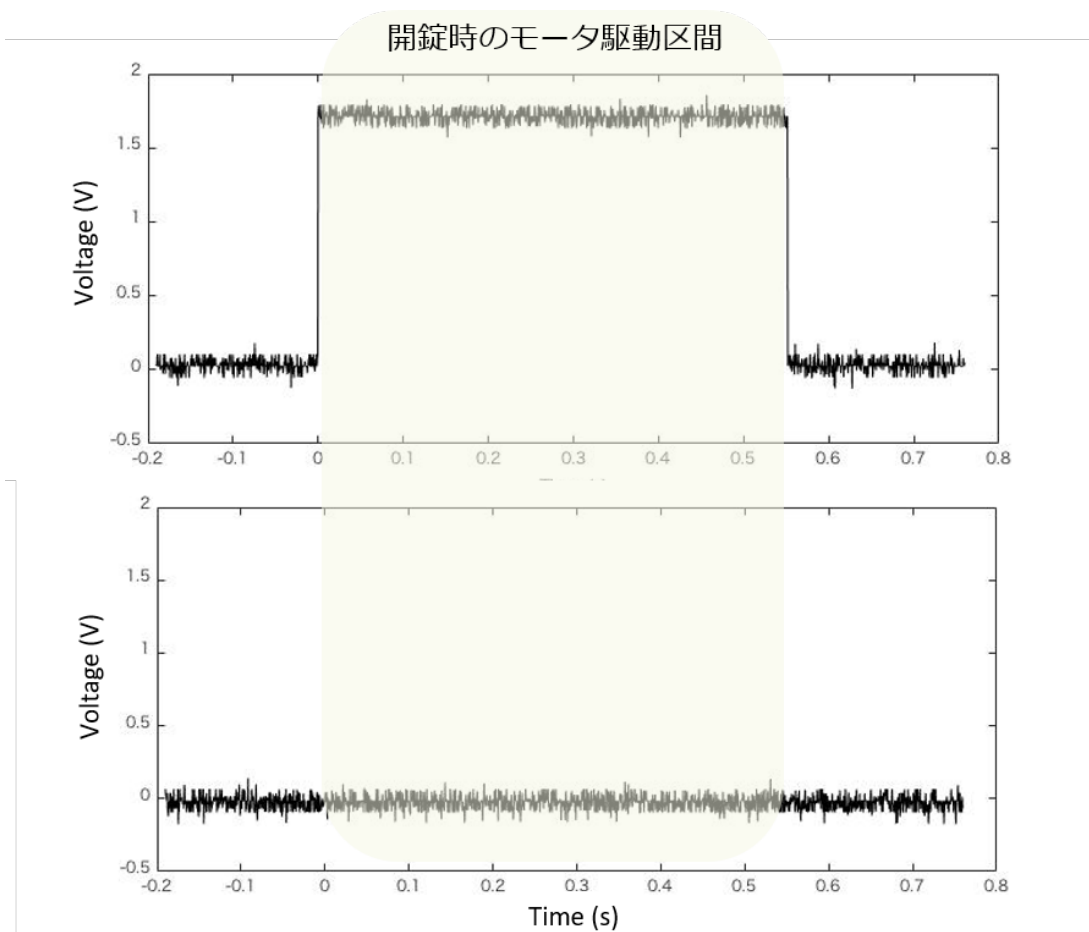


図 2.4 2 信号タイミング型モータドライバの開錠信号例

表 2.3 2 信号タイミング型モータドライバの動作原理 [9]

Input1	Input2	Output1	Output2	機能
Low	Low	Low	Low	ブレーキ
Low	High	Low	High	逆転
High	Low	High	Low	正転
High	High	Low	Low	ブレーキ

3 信号タイミング型モータドライバは、2 信号タイミング型モータドライバの仕組みに信号線を 1 本追加することで、正転/逆転/停止の動作命令のみならず回転速度や角度などより多くの制御信号を通信することが可能である。このようなモータドライバを用意し、モータを駆動する際に処理部の IC からモータドライバへ流れる信号例を図 2.5 に示し、モータの動作決定を表 2.4 に示す。パワーセーブ端子 (PS) が Low の時、Input に関わらずモータの出力を開放する。複数の信号線の High/Low を組み合わせることで駆動や停止を示している。

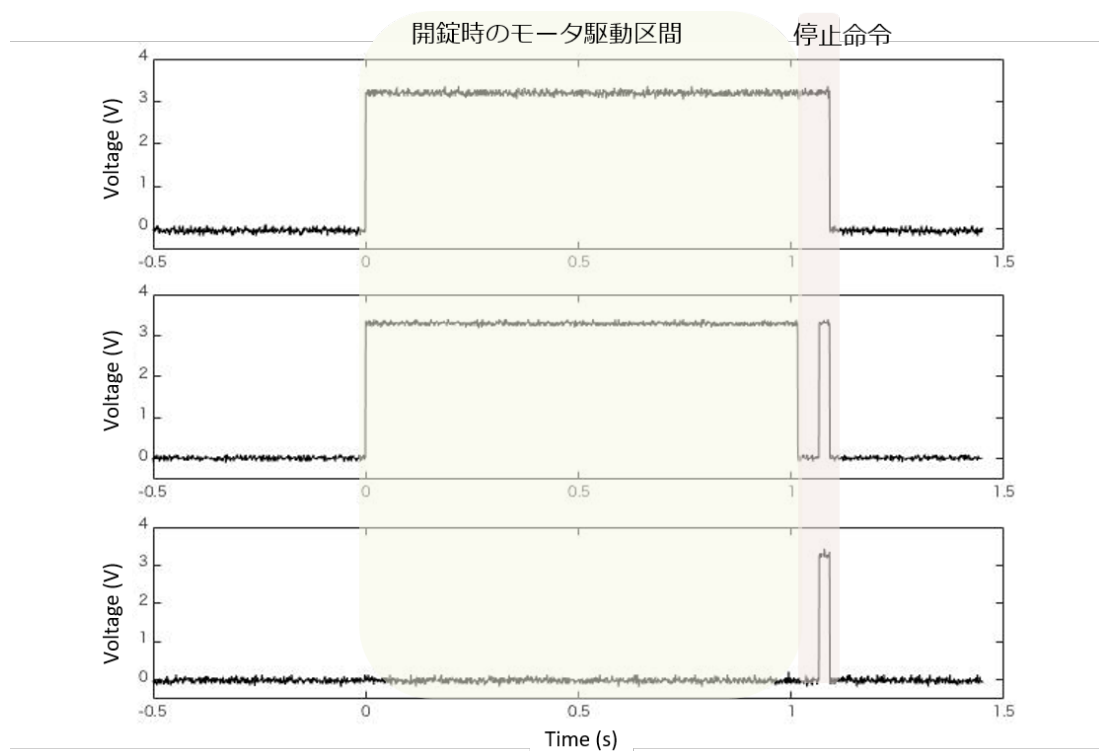


図 2.5 3 信号タイミング型モータドライバの開錠信号例

表 2.4 3 信号タイミング型モータドライバの動作原理 [10]

PS	Input1	Input2	Output1	Output2	機能
Low	High or Low	High or Low	開放	開放	全回路スタンバイ
High	Low	Low	開放	開放	待機
High	High	Low	High	Low	正転
High	Low	High	Low	High	逆転
High	High	High	Low	Low	ブレーキ

2.3 スマートロック機器内部の信号改ざんに関する故障注入法の提案

1.1 節で述べたように、スマートロックシステムの非暗号化領域では攻撃者が容易に通信路に流れる信号を解析可能であり、開錠信号を生成可能である。つまり、第三者が機器外部から開錠信号を何らかの方法を用いて入力することが出来れば、セキュリティを担保している上位レイヤーの実装によらず、スマートロックを強制的に開錠できる可能性がある。また、2.1 節ではスマートロックの内部信号の改ざんを引き起こす手法として電磁波が有効であることを示し、前節の 2.2 節ではモータドライバを制御通信方式から 3 種類に分類を行った。

本節では、電磁波を用いたスマートロック機器内部の信号改ざんに関する故障注入法について、2.2 節で分類を行ったモータドライバごとにそれぞれ提案を行う。

データ通信型モータドライバは、データ信号にクロック信号を同期させることで制御データを通信するモータドライバである。そのデータ通信型モータドライバを用いたスマートロック機器を強制的に開錠するためには、図 2.3 に示した信号と同様に、2 本の信号線に対してクロック信号とデータ信号を生成する必要がある。連続正弦波を注入した際は、クロック信号を生成可能であると考えられるが、同時に意味のあるデータ信号の生成は困難であると考えられるため、開錠の可能性は低いと考えられる。一方、パルス波を本来の通信されている信号のクロック信号に重畳することで、機器の内部信号をシフトさせ改ざんすることが可能であると考えられるが、この手法には制約が存在する。制約の 1 つ目として、パルス波を注入した信

号がオーバークロックによるデータシフトで開錠命令となる必要がある。また制約の2つ目として、通信されるデータとパルス波の注入タイミングを同期し注入する必要がある。

2信号タイミング型モータドライバは、2本の信号線のうち一方の信号線に1が入力されることで駆動する仕組みである。その2信号タイミング型モータドライバを強制的に開錠するには、開錠方向の駆動命令を入力する信号線に1となるような信号の注入により開錠が可能となる。パルス波では連続した1を生成することは困難であるが、連続正弦波を注入することで制御信号線に電位変動を発生させて、1と認識させることが可能であると考えられる。つまり、連続正弦波を用いることで第三者がモータを強制的に駆動させ開錠を行う可能性がある。

3信号タイミング型モータドライバは、複数の信号線のHigh/Lowを組み合わせることで駆動する仕組みである。その3信号タイミング型のモータドライバに対して強制的な開錠を行うためには、継続的な信号生成が必要である。つまり、2信号タイミング型と同じく連続正弦波を注入し継続的な電気信号を生成することで開錠する可能性がある。しかし、2信号タイミング型と異なり、どれか1つの信号線に電磁波が注入された場合や、3つすべての信号線に電磁波が注入された場合は開錠が発生せず、また生成する信号も複雑であるため、第三者が電磁波を注入することで強制的に開錠する可能性は低いと考えられる。

第 3 章 スマートロック機器内部の信号改ざんに関する故障注入実験

本章では、2 章で提案したスマートロック機器内部の信号改ざんに関する故障注入法の実現可能性を実験によって示す。また、得られた結果から、対策手法として制御部の設計法について検討する。

故障注入法の実験をするにあたり、モータドライバの選択を行う。3 信号タイミング型モータドライバは、2 信号タイミング型モータドライバと通信方法が類似しており、想定される故障注入法も同じであった。しかし 3 信号タイミング型への攻撃は、注入する信号線が複数であること、開錠信号が複雑であることから、2 信号タイミング型に比べて困難であると考えられる。そのため、本研究では、パルス波による故障注入実験の対象としてデータ通信型、連続正弦波による故障注入実験の対象として 2 信号タイミング型モータドライバを選択し、それぞれの故障注入法でスマートロックシステムの機器内部信号の改ざんされ開錠される可能性について検討する。

3.1 データ通信型モータドライバに対する故障注入実験

本節では、データ通信型モータドライバに対し、2 章で述べた故障注入法を用いて実験する。

2.3 節で述べたように、データ通信型は開錠される可能性があるが、様々な制約が存在する。市場に流通するデータ通信型のモータドライバを用いたスマートロックを抽出して調査したところ、モータドライバへ常時通信している信号の中にパルス波を入れることで開錠命令に書き換わる信号が存在しなかった。しかし、モータドライバへ常時通信される信号によっては開錠される可能性があるため、本論文ではモデル環境を構築し、パルス波注入により機器内部の信号が改ざんされ開錠される可能性について検証した。

3.1.1 データ通信型モータドライバに対する故障注入実験の実験セットアップ

データ通信型モータドライバに対する故障注入実験を行うために、実験セットアップを構築した。実験セットアップのブロック図を図 3.1 に、図 3.1 内のパルスジェネレータについては図 3.2 に詳細を示す。また、図 3.3 に実験セットアップの外観図を示す。モータドライバは実際のスマートロックシステムに用いられていた DRV8830 を用いた。FPGA からモータドライバへ I^2C 通信を模擬して停止信号を送信した。その信号を基に、モータドライバはモータへ停止命令を送信する。制御命令が送信されるタイミングと同期した信号をパルスジェネレータへ入力し、パルスジェネレータ内のコイルからパルス波が注入される。 I^2C 通信の信号波形とモータの電圧値をオシロスコープで観測し、パルス波が信号線に注入されることによって制御命令が改ざんされモータが駆動させる可能性を検討する。

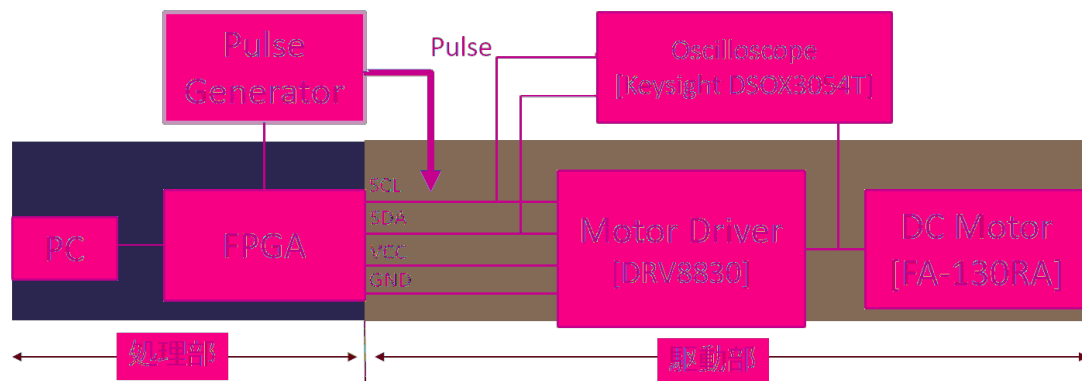


図 3.1 データ通信型モータドライバの制御信号への故障注入実験のブロック図

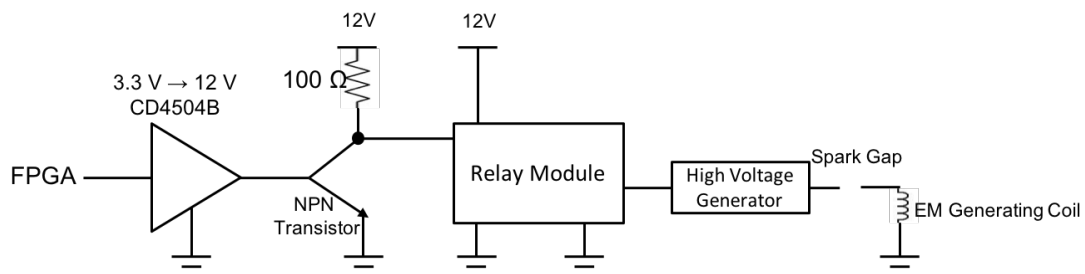


図 3.2 パルスジェネレータの回路図

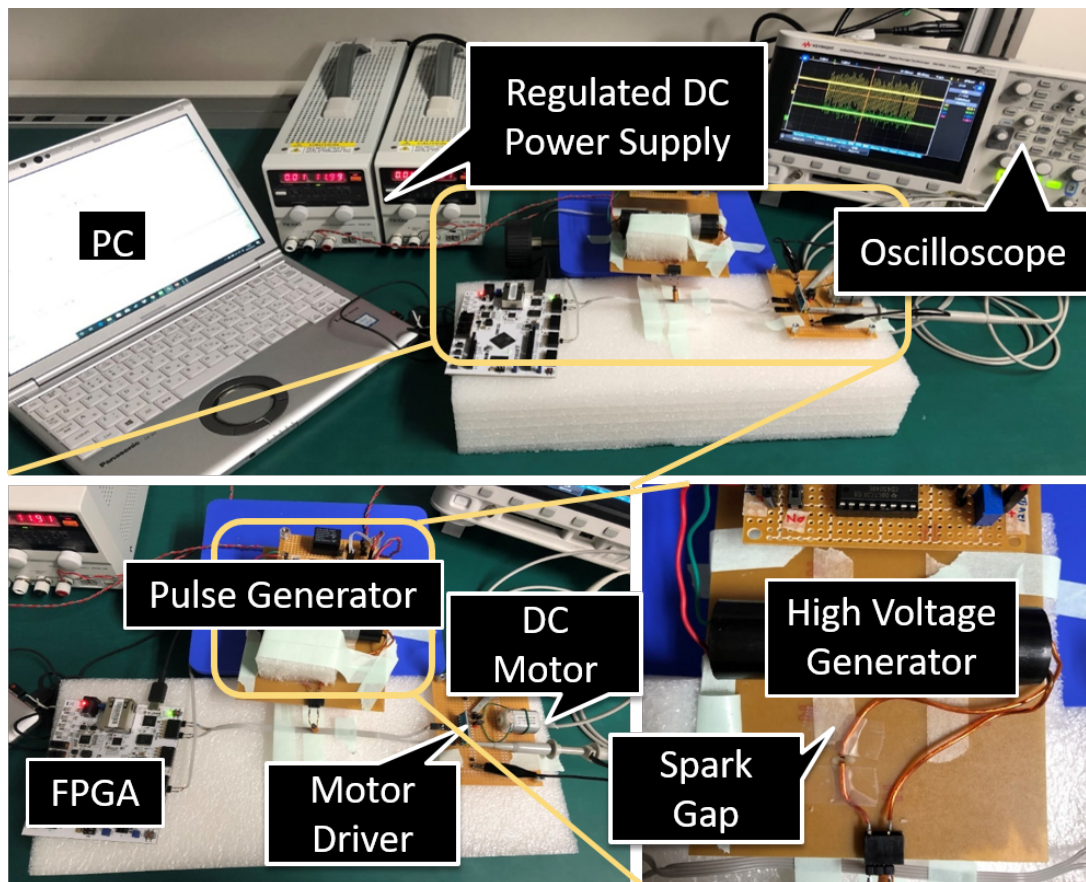
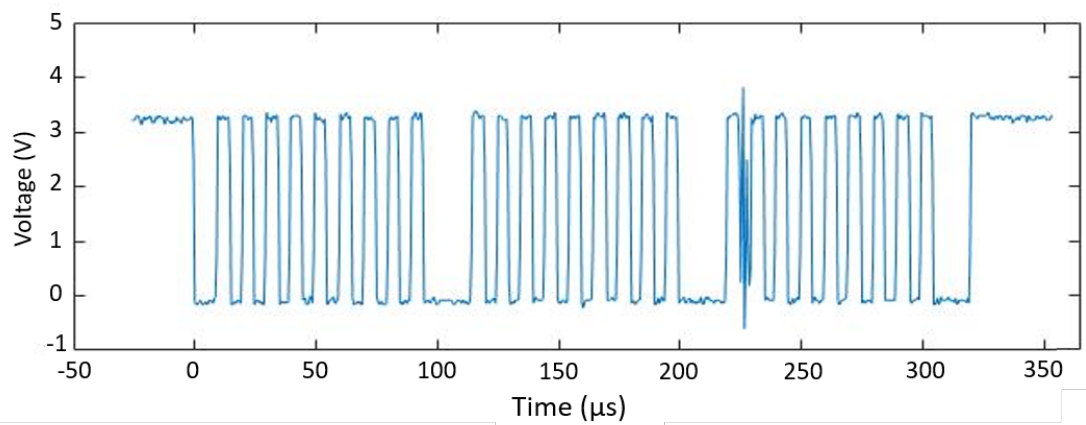


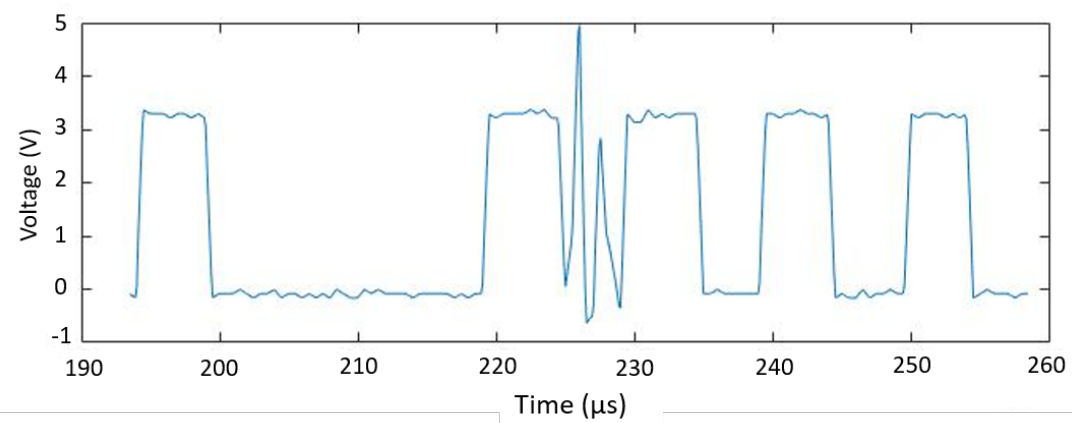
図 3.3 データ通信型モータドライバの制御信号への故障注入実験の外観

3.1.2 データ通信型モータドライバに対する故障注入実験の実験結果

実験環境を用いてパルス波を注入することで、図 3.4 に示すクロック信号の生成を確認した。また、図 3.5(a) にこのパルス波が注入された時のクロック信号、図 3.5(b) にモータの電圧値を示す。本実験では、モータの制御用信号としてパルス幅変調 (PWM: Pulse Width Modulation) 制御を用いた。パルス波注入後、モータの電圧値が変化し PWM 制御が停止から駆動に変化したことから、パルス波を用いることで制御信号が改ざんされ、特定の信号に対して開錠命令を発行することが可能であることを確認した。

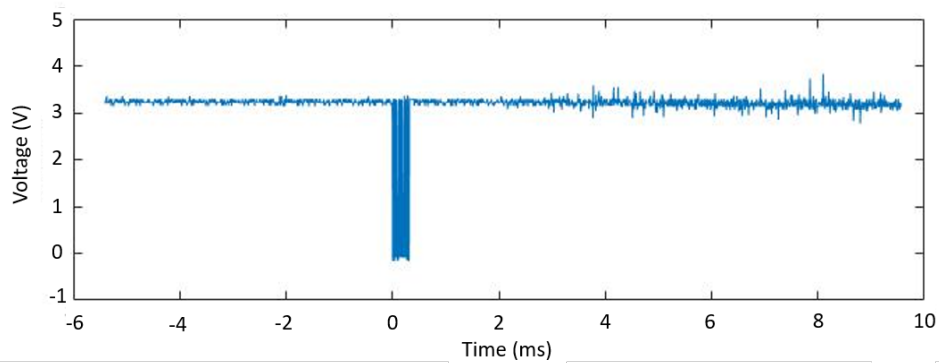


(a) クロック信号全体の信号波形

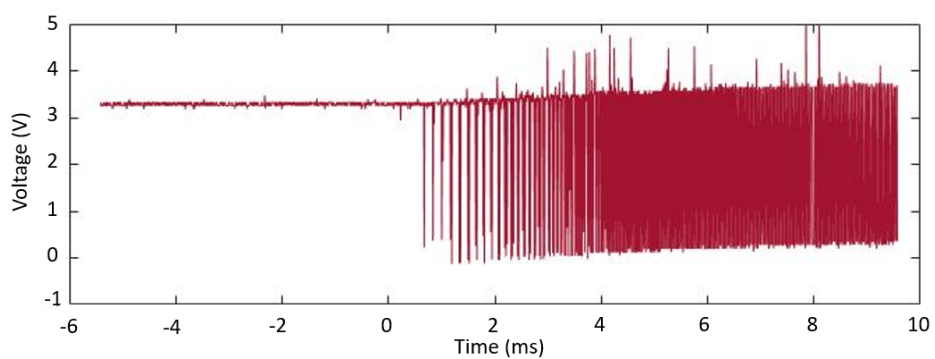


(b) パルス波周辺の信号波形

図 3.4 パルス波注入時のクロック信号波形



(a) クロック信号波形



(b) モータ電圧の信号波形

図 3.5 パルス波注入後のモータ電圧の変化

3.2 2 信号タイミング型モータドライバに対する故障注入実験

本節では、市場に流通するスマートロックの中で、2 信号型モータドライバを用いたスマートロックを用意し、2 章で述べた故障注入法を用いて評価を行う。

3.2.1 2 信号タイミング型モータドライバに対する故障注入実験の実験セットアップ

2 信号タイミング型モータドライバに対する故障注入実験を行うために、実験セットアップを構築した。実験セットアップのブロック図を図 3.6 に示し、実験セットアップの外観図を図 3.7 を示す。機器への攻撃を実施する際は機器外部から電磁波を注入する必要がある。しかし、本研究は外部から注入された信号による開錠の可能性の評価であり、実証実験ではない。そのため、今回の実験は、再現性のため効率的に配線に対して電磁波を重畳させる必要があり、電磁両立性 (EMC: Electromagnetic Compatibility) のイミュニティ試験 [18] でも用いられるインジェクションプローブを用い、モータドライバの開錠に使用される信号線をボード上から引き出し、その線に対して電磁波注入を行った。0.1 MHz から 1 GHz の間で注入する電磁波の周波数を掃引させ、注入した電磁波により信号線の電位変動が発生したかをオシロスコープで観測を行った。

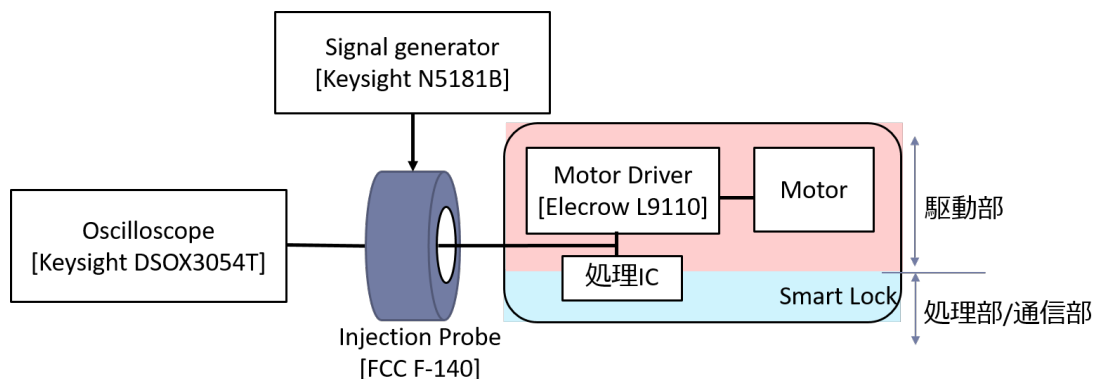


図 3.6 2 信号タイミング型モータドライバの制御信号への故障注入実験のブロック図

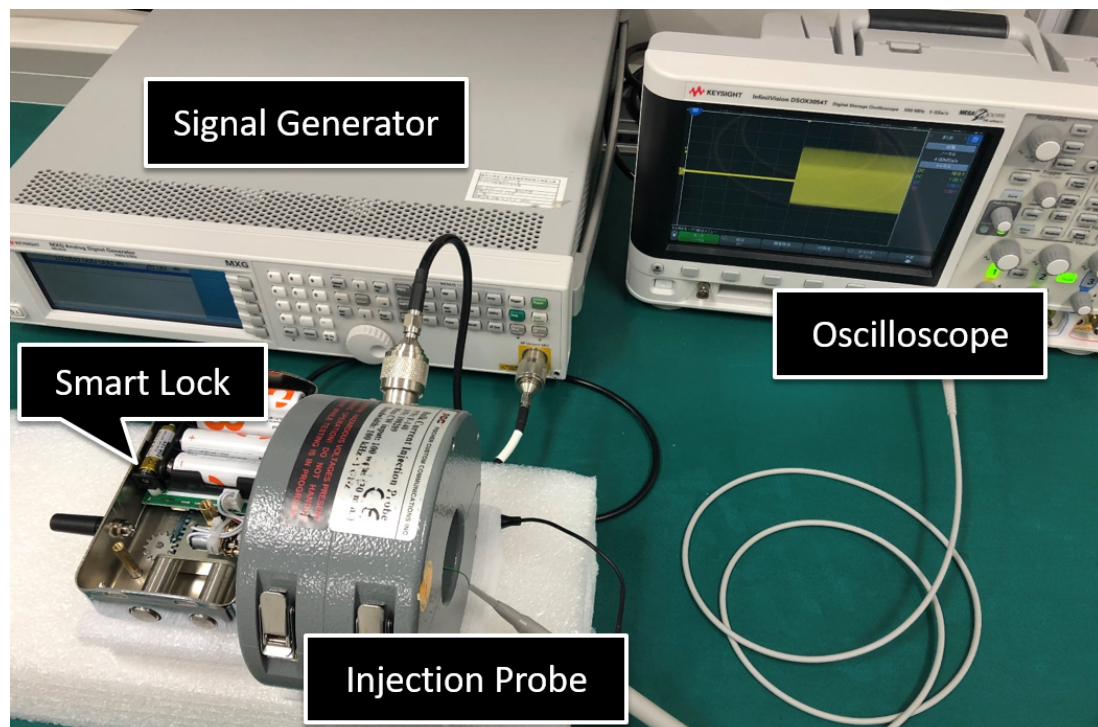


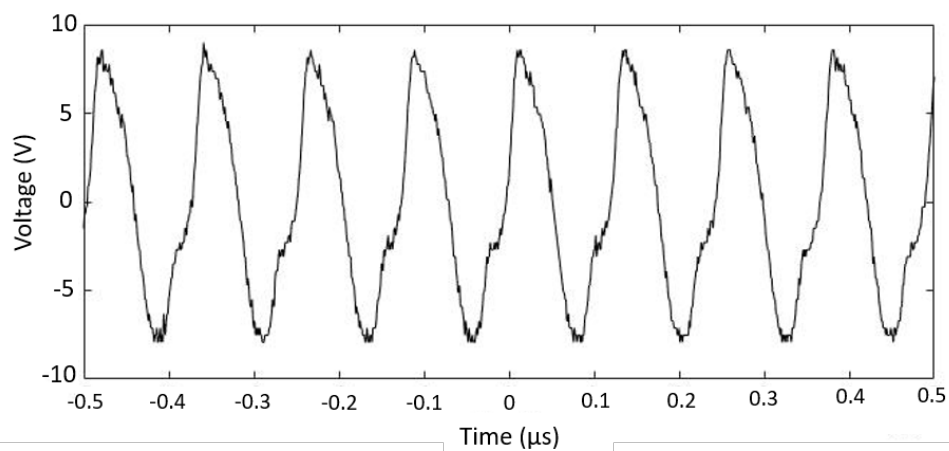
図 3.7 2 信号タイミング型モータドライバの制御信号への故障注入実験の外観

3.2.2 2 信号タイミング型モータドライバに対する故障注入実験の実験結果

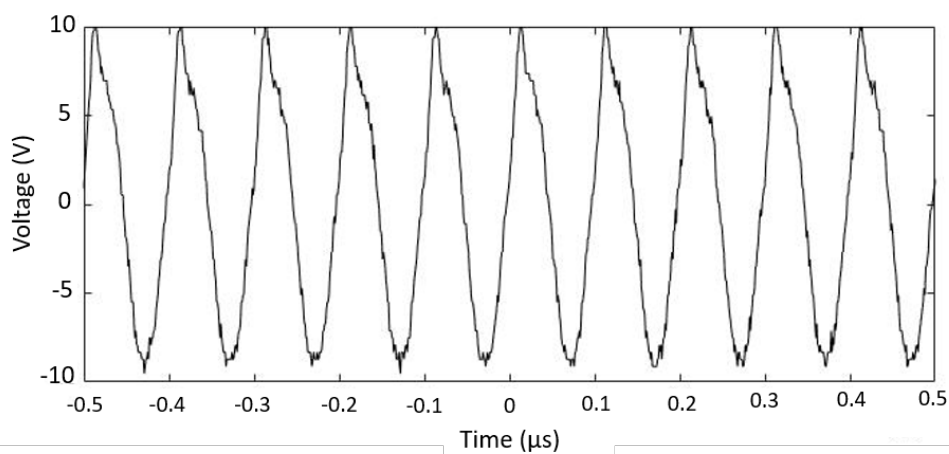
実験セットアップを用いて連続正弦波の注入実験を行った結果、表 3.1 のように 8 MHz から 11 MHz の間でのみスマートロックの開錠が確認された。最も低い信号強度で攻撃が成功した 8 MHz を注入時に制御信号線に発生した電位変動を図 3.8(a)、最も高い信号強度が必要だった 11 MHz の注入時に制御信号線に発生した電位変動を図 3.8(b) に示す。表 3.1 の発生した電位変動は、観測した電圧の最大値と最小値の差分である。この実験により、今回用いたスマートロックシステムは強制的に開錠可能であることを示した。

表 3.1 開錠が確認された電磁波の周波数と信号強度と信号線に発生した電位変動の関係

周波数 (MHz)	信号強度 (dBm)	発生した電位変動 (V)
8	23.6	14.7
9	24.2	16.3
10	24.8	17.5
11	30	18.2



(a) 8 MHz の連続正弦波注入時



(b) 11 MHz の連続正弦波注入時

図 3.8 強制的に開錠が確認された際のモータドライバ信号線に発生した電圧の時間応答波形

3.3 考察・対策

3.1 節により、データ通信型モータドライバを用いたスマートロックシステムでは、特定の制御命令であれば、機器外部からパルス波を注入することで第三者が強

制的に開錠することが可能であり、脆弱性が存在することが示された。今回用いたモータドライバにはシュミットトリガが設定されており、VCC の 0.7 倍で 1 を判定するしきい値が設定されている。設定されている VCC は 3.5 V であり、2.45 V がしきい値であることがわかる。注入されたパルス波は図 3.5(b) より、2 つともしきい値を超えているが、モータの回転方向と送信したデータ信号から 1 つのみデータがシフトしていることが確認できた。つまり、モータドライバは 1 が連続した時間の短い 2 つ目に発生したパルス波を認識出来なかったと考えられる。

3.2 節により、2 信号タイミング型モータドライバを用いたスマートロックシステムでは、連続正弦波を注入することで第三者が強制的に開錠される可能性が示された。今回の実験では、モータドライバへの入力信号線を基板から引き出し、その信号線に連続正弦波の注入を行った。注入された連続正弦波は、IC の入出力部に存在するダイオード等でコモンモードノーマルモード変換が発生したため信号線に注入されたと考えられる [19][20][21]。今回用いたモータドライバの正規信号は 1.8 V であるが、マージンをもってしきい値を 1.6 V とし、入力信号のしきい値を越えた部分を 1 とする。連続正弦波注入時に 1 が連続した時間と 1 の時間全体における比率である Duty 比を表 3.2 に示す。Duty 比はすべての周波数でほぼ同等であった。このことから、少なくともモータを回転させるために必要な 1 の信号の時間比率に限度が存在する。また、周波数が上がるにつれて、攻撃に必要な電位変動が大きくなるといえる。今回使用した機器の最大出力電力が 30 dBm であったため、11 MHz より高い周波数では攻撃の検討が不可能であったが、電力を上げることで攻撃出来る可能性がある。

モータドライバに 1 が入力されてから実際にモータを動かすための信号が生成されるまでには時間遅延が発生するため、その期間 1 が連続して入力され続けることが必要である。本実験では、11 MHz における 39.5 ns が最小であり、それ以上の周波数やそれ以下の振幅ではこの数値を下回り攻撃が成立しなかったため、この数値がモータを動作させるために必要な連続した 1 の時間の下限であると考えられる。

表 3.2 開錠が確認された電磁波の周波数と信号強度と信号線に発生した電位変動の関係

周波数 (MHz)	1 が連続した時間 (ns)	Duty 比
8	55.5	0.441
9	48.5	0.436
10	42.5	0.433
11	39.5	0.441

一方で、電磁波を機器に注入した場合、機器の電気的特性により信号の減衰率を決める伝達特性が周波数によって異なる [22]。今回の実験では、8 MHz より低い周波数及び 11 MHz より高い周波数において、制御信号線に重畳する電圧変動が急激に小さくなっており、伝達特性が悪いことが原因で注入が困難であったと考えられる。

本論文の実験結果から、スマートロックシステムには無線通信やソフトウェアが安全に実装されていた場合でも、モータドライバへの制御信号に対して電磁波を注入することによって、開錠される脆弱性が存在することが示された。

上記の結果から、スマートロックシステムの対策手法として制御部の設計法について検討する。データ通信型モータドライバを用いたスマートロックシステムの対策としては、送信されるデータがパルス波注入によるデータのシフトで開錠可能となる信号を生成不可能にすることが有効的であると考ええる。今回の実験では、データのシフトは 1 つであったが、攻撃の可能性として複数パルス波が注入される可能性がある。そのため、制御命令にパルス波が注入された時のすべての組み合わせを考える必要があるが、時間やコストがかかる。しかし、パルス波が注入されデータがシフトするということは、データの 1/0 の偏りが大きくなることと等価であり、攻撃対象の信号データの 1/0 の偏りが制御命令よりも大きければ攻撃は不可能である。その点に着目することで、組み合わせの試行回数を減らすことが可能であり、データシフトが発生しても開錠命令にならない制御信号の実装が対策手法として考えられる。またパルス波は開錠に必要な信号より連続で 1 となる時間が短いため、そういった波形を除去できるフィルタを設置することも効果的であり、シュミットトリガやチャタリング防止を用いた対策手法も考えられる。シュミットトリガとは、高低のしきい値を設けることで、入力信号の揺らぎを除去するものである。し

かし、今回実験で用いたモータドライバにはシュミットトリガが設定されていたが、注入したパルス波を認識していた。これは、注入する電磁波によって発生した電位変動がしきい値を超えたため、対策として効果的ではない可能性がある。チャタリングとは、スイッチの ON/OFF の際に、複数の電氣的パルスが発生することである。チャタリング防止のローパスフィルタを用いることで、パルス波の高周波成分を除去すれば、入力される信号の振幅を IC の入力回路の感度がないレベルまで抑制できる可能性がある。

2 信号タイミング型モータドライバへの信号改ざんとして、連続正弦波を使用し、開錠の可能性を示した。開錠した際に注入された連続正弦波は、通常の信号より大きい振幅であり、それを検知する回路が有効であると考えられる。また、信号線への注入では、伝達特性の良い周波数帯で開錠が行われており、それを遮断するフィルタ回路 [23][24] が有効と考えられる。今回開錠が確認された周波数は 8 MHz から 11 MHz であったので、ローパスフィルタやバンドパスフィルタで遮断が可能と考えられる。

スマートロックシステム全体では、サムターンなどを回転させる駆動部に回転を観測するセンサを設置することで、処理部が意図しない開錠行為を検知することができ、攻撃を防ぐことが可能である。また、処理部と駆動部の IC を 1 チップ化することで対策出来る可能性もあるが、モータドライバはモータを駆動するために高電圧を出力する様に特化されているため、処理部の IC と合わせることは困難であり、汎用性がないため対策としては有効ではないと考えられる。すでに設置がされており、取り換えが困難なスマートロックには電磁波シールド [23][24] などで機器を覆うことが考えられる。

第 4 章 結論

本論文では、スマートロックに対して無線通信やソフトウェアが安全に実装されている場合においても、モータの制御信号等が暗号化されていないことから開錠される可能性があることに着目し、スマートロック機器外部から注入された電氣的外乱による開錠の可能性について検討した。

第 2 章においては、スマートロック機器外部からの内部信号の改ざん手法として電磁波を用いた故障注入が有効であることを論じ、モータドライバへの制御信号の特徴から 3 種類に分類した。データ通信型モータドライバにはパルス波を用いた、2 信号タイミング型モータドライバおよび 3 信号タイミング型モータドライバには連続正弦波を用いた開錠信号の改ざんの可能性を示した。また、スマートロック機器内部の信号改ざんに関する故障注入法を提案した。

第 3 章では、第 2 章で提案した故障注入法の実現可能性を実験によって示した。データ通信型モータドライバは特定の信号にパルス波を注入すること、2 信号タイミング型モータドライバは伝達特性の良い周波数の連続正弦波を注入することによって、スマートロック機器外部からの内部信号の改ざんが行われ開錠される可能性を示した。また、実験結果から、対策手法として制御部の設計法について議論し、開錠の危険性を抑制できる可能性を示唆した。

以上より、本論文では、非暗号化領域であるモータの制御信号等に電磁波を用いた故障注入を行うことで、無線通信やソフトウェアが安全に実装されていた場合においてもスマートロックが機器外部から開錠される可能性を示した。このことから、攻撃者が容易に接近し攻撃が可能なスマートロックに対しては、電磁波攻撃に対する制御部の設計が必要であることを明らかにした。

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科学領域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丁寧かつ熱心な御指導、御鞭撻を賜りました。ここに心より感謝申し上げます。

本学岡田実教授及び小笠原司教授には、研究を進めるにあたり有益なご助言・ご討論を頂き、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ご支援、ご助言を賜り、学会参加においても多大なご支援をいただきました。厚く御礼申し上げます。

本学 Youngwoo Kim 助教及び仙台高等専門学校衣川昌弘助教には、研究活動を進めるにあたり活発な議論を通じて多くの知識や示唆をいただきました。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。

最後に、日ごろの研究生活において様々な面でご協力いただきました、研究室の皆様がこの場を借りて深く感謝申し上げます。

参考文献

- [1] IPUSIRON, "ハッカーの学校 鍵あけの教科書," データハウス, 2016.
- [2] Benjamin Laxton, Kai Wang, and Stefan Savage, "Reconsidering Physical Key Secrecy: Teleduplication via Optical Decoding," Proceedings of the 2008 ACM Conference on Computer and Communications Security, CCS 2008, Alexandria, Virginia, USA, October 27-31, 2008.
- [3] Qrio, "Qrio Lock - カギが自由になる生活。," <https://qrio.me/smartlock/>.
- [4] Allied Market Research, "Smart Locks Market by Product Type (Deadbolts, Lever handles, Padlocks, and Others), Technology (Wi-Fi and Bluetooth), and End User (Commercial and Residential) - Global Opportunity Analysis and Industry Forecast, 2017-2023," 2017.
- [5] Symantec, "セキュリティレスポンス IoT(モノのインターネット)のセキュリティ問題," 2015.
- [6] Broadcom Corporation, "BCM20737 Single-Chip Bluetooth Low Energy-Only System-On-Chip with Support for Wireless Charging," datasheet, 2016.
- [7] 五百旗頭 健吾, 上竹 嘉紀, 手嶋 俊彰, 眞田 晃宏, 野上 保之, "市販マイコンモジュールを利用した暗号ハードウェアセキュリティ演習の開発," コンピュータソフトウェア, 2019, 36 巻, 1 号, p. 30-36, 2019.3.26.
- [8] TEXAS INSTRUMENTS, "DRV8830 Low-Voltage Motor Driver With Serial Interface," datasheet, 2015.
- [9] Elecrow, "L1190 Motor control driver chip," datasheet.
- [10] 東芝, "TB6612FNG Dual DC モータドライバ," datasheet, 2014.
- [11] ROHM, "ステッピングモータドライバーシリーズ スタンダード 36V 耐圧シリーズ ステッピングモータドライバ BD63940EFV,BD63960EFV," datasheet, 2014.
- [12] T. Sugawara, B. Cyr, S. Rampazzi, D. Genkin, and K. Fu, "Light Commands: Laser-Based Audio Injection Attacks on Voice-Controllable Systems," 2019.

- [13] J. Rodriguez, A. Baldomero, V. Montilla and J. Mujal, "LLFI: Lateral Laser Fault Injection Attack," 2019 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), Atlanta, GA, USA, 2019, pp. 41-47.
- [14] 林 優一, 菅原 健, 水木 敬明, 本間 尚文, 青木 孝文, 曾根 秀昭, "意図的な電磁妨害による暗号モジュールへの故障注入に関する検討," 電気学会研究会資料, EMC-11-17, pp. 53-57, 2011.
- [15] P. Maurine, "Techniques for EM Fault Injection: Equipments and Experimental Results," 2012 Workshop on Fault Diagnosis and Tolerance in Cryptography, Leuven, 2012, pp. 3-4.
- [16] S. Ordas, L. Guillaume-Sage and P. Maurine, "EM Injection: Fault Model and Locality," 2015 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), St. Malo, 2015, pp. 3-13.
- [17] Y. Hayashi, N. Homma, T. Mizuki, T. Aoki and H. Sone, "Transient IEMI Threats for Cryptographic Devices," IEEE Trans. on Electromagnetic Compatibility, vol. 55, pp. 140-148, 2013.
- [18] C. R. Paul, "Introduction to Electromagnetic Compatibility," K. Chang, ed., John Wiley & Sons, New York, 1992.
- [19] 鈴木 茂夫, "ノイズ対策は基本式を理解すれば必ず出来る!," 日刊工業新聞社, 2015.
- [20] 落合 政 司, "スイッチング電源におけるノイズの抑制対策," <https://kobaweb.ei.st.gunma-u.ac.jp/lecture/EMC20160926-1.pdf>.
- [21] International Rectifier, "高耐圧モノリシック IC で実現する 最新モータ・インバータの回路設計," <http://www.irf.com/technical-info/designtp/jpmotorinv.pdf>.
- [22] IEC 61000-4-6:2013 Electromagnetic compatibility (EMC) - Part 4-6: Testing and measurement techniques - Immunity to conducted disturbances, induced by radiofrequency fields.
- [23] International Telecommunication Union-Telecommunication Standardization Sector(ITU-T), "K.115: Mitigation methods against electromagnetic security threats," 2015.

- [24] International Telecommunication Union-Telecommunication Standardization Sector (ITU-T), "K.84: Test methods and guide against information leaks through unintentional electromagnetic emissions," 2011.

発表リスト

- [1] 中尾文香, 藤本大介, 林優一, "クロックグリッチ発生タイミングがモータ動作に与える影響に関する基礎検討," 2019 年電子情報通信学会ソサイエティ大会, A-20-6, 2019.9.12.
- [2] 藤本大介, 中尾文香, 林優一, "スマートロックに対する電磁波を用いた強制的な開錠の脅威," 2020 年暗号と情報セキュリティシンポジウム (SCIS2020), 2E2-5, 2020.