



# フリップチップ半導体デバイスの高電圧パルス注入によるビット反転の誘発と解析に関する研究

弘原海, 拓也

---

(Degree)

博士 (科学技術イノベーション)

(Date of Degree)

2025-03-25

(Resource Type)

doctoral thesis

(Report Number)

甲第9251号

(URL)

<https://hdl.handle.net/20.500.14094/0100496532>

※ 当コンテンツは神戸大学の学術成果です。無断複製・不正使用等を禁じます。著作権法で認められている範囲内で、適切にご利用ください。



(別紙様式 3)

## 論文内容の要旨

氏 名 弘原海 拓也

---

専 攻 科学技術イノベーション専攻

---

論文題目 (外国語の場合は、その和訳を併記すること。)

フリップチップ半導体デバイスの高電圧パルス注入によるビット反転の誘発と解析  
に関する研究

指導教員 永田 真

---

(氏名：弘原海 拓也 NO.1)

近年、機密情報のデジタル化が進展する中でサイバー攻撃による被害が深刻化しており、セキュリティ技術の重要性が改めて認識されている。従来、セキュリティは暗号技術によって確保されてきた。暗号技術は「アルゴリズム」と「鍵」によって構成されており、アルゴリズムは一般に公開されることで安全性が検証され、鍵を隠匿することで暗号化通信が実現される。このため、鍵の管理が非常に重要であり、暗号処理や鍵管理を専門に担うハードウェアセキュリティモジュール（HSM）の利用により、鍵管理をサーバーシステムから分離し、サイバー攻撃に対して堅牢なシステムを構築することが可能である。

しかし、攻撃者が HSM に接近することが可能な環境下では、暗号処理に伴って放射される電磁波や熱を解析するサイドチャネル攻撃や、意図的に回路に故障を引き起こす故障注入攻撃などの物理攻撃によって、暗号鍵の推測が可能であることが知られている。このため、高度なセキュリティが要求されるアプリケーションにおいて、物理攻撃耐性の重要性が議論されるようになってきた。

本研究では、HSM をはじめとする電子デバイスのセキュリティ向上を目的に、物理攻撃の検知および解析を行う高感度なオンチップ電圧測定回路技術を開発した。また、フリップチップ実装した半導体集積回路（IC）の裏面から高電圧パルスを印加する故障注入攻撃手法に着目し、チップ内部で引き起こされる現象をシミュレーションと実測で評価し、セキュリティ脆弱性の要因となるビット反転現象のメカニズムを明らかにした。さらに、デジタルデータ管理における物理攻撃耐性の必要性に加え、デジタル主権の確保といった社会的背景を踏まえ、サーバー用途の国産 HSM の開発および事業化可能性についても検討した。

第1章では、情報技術の進展に伴い、機密情報のデジタルデータ化が進む一方で、サイバー攻撃による被害が深刻化している現状を述べた。一般的には、暗号技術によってデジタルデータが保護されるが、暗号化データと鍵情報が同一のサーバー上に展開される場合、セキュリティホールを突いた攻撃によって暗号化データと鍵情報が同時に窃取される危険性がある。この問題に対応するため、暗号処理を専門に担う HSM の利用が広がっている。HSM をサーバーシステムに組み込むことで、暗号鍵がサーバー上に直接展開されるリスクを排除し、機密情報の漏えいを抑制できる。

一方で、HSM 自体が物理攻撃の対象となり得る課題が浮上している。特に、クラウド環境では、クラウド事業者が管理する顧客のサーバーや HSM に物理的に接近可能である状況がセキュリティ上の問題となる。米国では、政府向けクラウドの管理者を市民権保持者に限定する部分的な対策を講じているが、十分な対策とは言えない。このため、米国大手クラウド事業者は、物理攻撃耐性を備えた HSM を利用し、セキュアなクラウドシステムを提供する高セキュリティサービスを展開している。これにより、クラウド事業者自身による物理攻撃を防ぎ、顧客に対して付加価値のあるセキュリティソリューションを提供している。このような背景を踏まえ、本研究では HSM を含む電子デバイスの物理攻撃耐性を強化すること

を目的とした。

続いて、現代における物理攻撃手法の特徴を整理し、物理攻撃耐性技術の開発に向けた技術的課題を提起した。暗号鍵の解読難度を高める暗号アルゴリズムの開発のみでは対策が不十分であり、暗号解読に繋がる物理情報の漏えいや回路の故障発生を低減する擾乱耐性の半導体設計技術、さらに攻撃を検知して暗号鍵を迅速にゼロ化する技術が不可欠であることを指摘した。

物理攻撃対策技術の開発においては、IC チップ内外における物理現象を精密に把握することが極めて重要である。例えば、漏えいを低減するためには電磁波や温度が攻撃者に観測される過程を詳細に理解する必要がある。また、故障注入攻撃に対する対策では、攻撃者がどの程度意図した動作タイミングや回路位置に故障を誘発できるかを把握し、回路設計やレイアウトに反映させることが求められる。しかし、I/O パッドを介さないチップレベルの故障注入攻撃では、外乱が回路へ結合するモデルが複雑であることから従来の回路シミュレーションのみでは説明することが困難であり、最適な検知回路技術の開発やレイアウト最適化手法の確立には至っていない。

このため、本研究ではフリップチップ実装 IC の裏面に対する電圧パルス印加に着目し、故障発生の局所性と故障のメカニズムを明らかにし、検知や防御に対する対策指針を示すことを研究の目標と定めた。

第2章では、物理攻撃の検知と解析のための広帯域オンチップ電圧測定技術として、SAR ADC（逐次比較型 AD 変換器）を活用した回路設計技術を提案した。本技術では、物理攻撃に伴うチップ内の電圧変動の変化を正確に捕捉するために、広帯域でリアルタイムかつ高解像度な波形観測を実現する回路技術を開発した。65 nm CMOS プロセスを用いて試作チップを製作し、実験によりプリント基板上のプロロービング攻撃検知の有効性を実証した。さらに、故障注入による IC チップ内の現象を解析するためにも利用が可能であり、第3章における実験でも使用された。

第3章では、フリップチップ実装 IC のシリコン基板裏面に高電圧パルスを照射した際の IC チップ内の電圧変動を解析した。三次元電磁界シミュレーションを活用し、基板内での電圧分布とその広がりモデル化して解析を行った。また、第2章で開発したオンチップ測定回路を組み込んだ試作チップを用いて実験を行い、シミュレーション結果を実測で検証した。

これにより、電圧注入位置がチップ内における電圧変動の局所性に与える影響を明らかにし、さらにシリコン基板厚みに依存して局所性が変化することを発見した。この結果から、近年半導体集積回路の高密度化を目的とした 3D パッケージング技術におけるチップ厚の薄化の傾向によって、セキュリティ脆弱性を生む可能性を示唆した。

(氏名：弘原海 拓也 NO.3)

第4章では、フリップチップ実装 IC の裏面に対する電圧注入攻撃によるビット反転現象をシミュレーションと実測によって明らかにした。第3章で明らかにしたように、電圧注入位置に応じてシリコン基板の電圧が局所的に変動する。その際にデバイス領域に存在する pn 接合間に形成されるダイオード構造に電流が流れ、後段のゲート容量を充電することによって、双安定状態のデータが反転するメカニズムを明らかにした。この現象は、シミュレーションと実験の両面から検証し、攻撃耐性向上のための回路設計や検知回路の配置などに新たな視点を示した。

第5章では、本研究の成果を基に、国産 HSM の開発および事業化の可能性について検討した。この事業化アイデアでは、サーバーシステムに設置される HSM に対して物理攻撃耐性が求められる背景に加え、他国の干渉を受けない自国の機密情報保護という「デジタル主権」の重要性に着目している。

物理攻撃耐性を備えた HSM は、そのセキュリティ特性上、ハードウェアやファームウェアの構成がブラックボックス化されるのが一般的である。このため、海外製 HSM を利用する場合、導入国において内部構成を確認する手段が存在せず、セキュリティ上の懸念が生じるという課題がある。一方、国産 HSM を使用する場合、日本国内における法的な開示請求を通じて内部構成の透明性を担保できる点が、利用者にとって信頼性を向上させる要素となる。さらに、国内で製造された HSM であれば、その物理攻撃耐性のレベルを日本国内で評価・把握することが可能であり、セキュリティ上の信頼性が高まる。

HSM のセキュリティレベルを判断する指標の一つである米国政府のセキュリティ製品調達基準「FIPS 140」では、サーバー用途かつ物理攻撃耐性を持つ HSM において、日本製品の登録がない現状がある。これにより、デジタル主権を満たす国産の HSM は事実上存在していない。この課題を解決するため、本事業では、FIPS 140 を満たすことで標準的な物理攻撃耐性を示すと同時に、独自の物理攻撃検知システムを組み込むことで、高い物理攻撃耐性を実現し、競争力を確保することを差別化要因とし、事業を検討した。

最後に、第6章では、第1章から第4章で得られた研究成果と第5章における事業化検討を総括した。本研究は、ハードウェアセキュリティ分野における基盤技術の進展に寄与し、学術的意義と産業応用の可能性を示した。また、本研究における物理攻撃への対策技術が、セキュリティと経済安全保障の双方を強化するものであることを明らかにした。

|          |                                             |     |       |       |
|----------|---------------------------------------------|-----|-------|-------|
| 氏名       | 弘原海 拓也                                      |     |       |       |
| 論文<br>題目 | フリップチップ半導体デバイスの高電圧パルス注入によるビット反転の誘発と解析に関する研究 |     |       |       |
| 審査委員     | 区 分                                         | 職 名 | 氏 名   | 署 名   |
|          | 主 査                                         | 教 授 | 永田 真  | 永田 真  |
|          | 副 査                                         | 教 授 | 川口 博  | 川口 博  |
|          | 副 査                                         | 准教授 | 三木 拓司 | 三木 拓司 |
|          | 副 査                                         | 准教授 | 福家 信洋 | 福家 信洋 |

## 要 旨

情報通信技術(ICT)分野において、自動運転、機械翻訳、物質創製などの応用に資する大規模データの流通や利活用の展開とともに、先進的な自律処理や知能処理を担う半導体デバイスの高度化が進展している。現代の社会生活において、安全・安心な半導体デバイスの提供は重要な技術領域の一つである。一般に、セキュリティとして暗号化・復号の機能により機密性・完全性・可用性を確保し、セーフティとして状態遷移の冗長化や多重化によりフェイルセーフを実現する。しかしながら、近年、ハードウェアセキュリティ分野では半導体デバイスに対する能動的な攻撃が幅広く議論されており、とくに、デジタル回路の論理ビットを意図的に変更するアクティブ攻撃の脅威が調べられている。暗号処理過程のビット変更による誤った暗号文を解析することで秘密鍵を特定する手法、ロックステップ等の状態保持におけるビット変更によるシステム誤動作の誘発など、セキュリティとセーフティを脅かす攻撃について、半導体デバイスレベルの理解と対策が急務になっている。

本研究では、半導体製品に普及の進むフリップチップパッケージングを考慮して、半導体デバイスのアクティブ攻撃、とりわけ、半導体チップ裏面における高電圧パルス注入法に着目し、空間・時間分解能の高い実験技術・観測技術および論理ビット反転現象を解析するシミュレーション技術を創出する。また、本研究の成果に係るイノベーション戦略として、半導体デバイスにおける高度な物理攻撃耐性の獲得とセキュリティ機能の中核として暗号処理や鍵管理を担うハードウェアセキュリティモジュール(HSM)の構築について産業応用の視点から探求する。

本論文では、フリップチップ半導体デバイスの高電圧パルス注入によるビット反転の誘発と解析に関して、オンチップのその場観測・解析手段とチップレベルのシミュレーション技術(先端IT分野)および攻撃耐性の高い半導体デバイスによるHSM事業(アントレプレナーシップ分野)について纏めている。シリコン基板裏面の高電圧パルス注入によるビット反転の誘発メカニズムを半導体デバイスおよび半導体集積回路の動作と紐づけて深く理解し、高電圧パルス注入器と半導体デバイスの結合およびパルス伝搬を物理モデルにより表現する手段を与え、さらに論理状態を保持するレジスタの回路動作とパルス干渉をシミュレーションによりビット反転現象を定量的に解析する道筋を示すとともに、本研究の開発技術を、高度な物理攻撃耐性を具備する半導体デバイスおよびHSMの構築に応用し、事業化・社会実装する道筋についてイノベーション戦略を構築している。

本論文では、フリップチップ半導体デバイスの高電圧パルス注入によるビット反転の誘発と解析に関して、オンチップのその場観測・解析手段とチップレベルのシミュレーション技術およびHSMへの応用事業を確立すべく、次に示す4つの課題について論じている。すなわち、

- (1) オンチップ電圧モニタリングの広帯域化と物理攻撃のその場観測・検知と解析技術
- (2) フリップチップ半導体デバイスのシリコン基板における高電圧パルス結合とパルス伝搬の解析技術
- (3) 高電圧パルス注入攻撃によるビット反転現象のシミュレーション技術
- (4) 高度な物理攻撃耐性を具備する半導体デバイスおよびHSMの事業化に関するイノベーション戦略である。

前項(1)では、オンチップ電圧モニタリングと物理攻撃の検知および解析技術に関して、逐次比較型アナログデジタル変換器(SAR-ADC)を広帯域する回路方式および設計法を追求した。また、物理攻撃に伴うチップ内での電圧変動の変化を高い確度でその場観測するため、広帯域・リアルタイムかつ高解像度な波形

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |        |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|
| 氏名                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 弘原海 拓也 |
| <p>取得をデュアルモード計測アルゴリズムにより実現し、また、オフチップのプリント基板におけるプロービング等の物理攻撃の検知について実験的に実証した。</p> <p>前項(2)では、フリップチップ半導体デバイスのシリコン基板裏面に高電圧パルス照射し、半導体チップ内の電圧変動を前項(1)によるオンチップ電圧モニタリングによりその場観測した。また、半導体チップの物理構造およびプロセスデータを取り込んだ三次元電磁界シミュレーションにより、シリコン基板内部のパルス伝搬による電圧分布の解析結果を得るとともに、その場観測データとの高い整合性を明らかにした。</p> <p>前項(3)では、フリップチップ半導体デバイスの高電圧パルス注入攻撃によるビット反転現象について、詳細実験と物理レベルシミュレーションにより、シリコン基板裏面の電圧注入位置に依存したシリコン基板の電圧が局所的に変動すること、および、半導体デバイスに寄生する pn ダイオードに順方向の電流が流れて後段のゲート容量を充電すること、を素過程として、論理ビットを保持するレジスタの双安定状態が反転するメカニズムを明らかにした。</p> <p>前項(4)では、本研究の成果に立脚して、高度な物理攻撃耐性を具備する半導体デバイスおよび HSM の事業化に関するイノベーション戦略を構築した。</p> <p>いずれの課題においても、最先端の半導体集積化システムのセキュリティとセーフティに関して、フリップチップ半導体デバイスのシリコン基板裏面高電圧パルス注入法に着目し、空間・時間分解能の高い実験技術・観測技術を導出するとともに、これによる論理ビット反転現象の物理メカニズムの理解について最新の知見を与えていることから、本論文における研究成果の工学的な価値は高いと考えられる。</p> <p>本論文の構成は以下のとおりである。</p> <p>第 1 章では、研究の背景と動機について述べるとともに、本研究の取組と成果の位置づけを明らかにしている。半導体技術に基づく HSM の構造をまとめ、物理攻撃を分類するとともに、セキュリティ脅威の問題を網羅的に指摘し、対策技術の必要性和導出と適用方針について論じている。</p> <p>第 2 章では、オンチップ電圧モニタリングの広帯域化と物理攻撃のその場観測・検知と解析技術について詳述している。</p> <p>第 3 章では、フリップチップ半導体デバイスのシリコン基板における高電圧パルス結合とパルス伝搬の解析技術について詳述している。</p> <p>第 4 章では、高電圧パルス注入攻撃によるビット反転現象のシミュレーション技術について詳述している。</p> <p>第 5 章では、高度な物理攻撃耐性を具備する半導体デバイスおよび HSM の事業化に関するイノベーション戦略について詳述している。</p> <p>第 6 章では、まとめと今後の展望を述べている。</p> <p>本論文は、以上のように、フリップチップ半導体デバイスの高電圧パルス注入によるビット反転の誘発と解析に関し、半導体チップ内部の電圧変動を高確度でその場観測するオンチップモニタリング、高電圧パルス注入、シリコン基板への結合と伝搬およびレジスタにおける論理ビット反転現象について探求し、テストチップを含む実証デバイスの構築と評価により具象的な議論を展開している。また、高度な物理攻撃耐性を具備する半導体デバイスおよび HSM の事業化の可能性を示し、先端 IT 分野における技術開発の方針を纏めていることから、科学技術イノベーションに向けた参考となることが期待できる。</p> <p>本研究の成果として、フリップチップ半導体デバイスの高電圧パルス注入によるビット反転の誘発と解析に関する深い理解を導き、また、セキュリティ半導体デバイス設計に応用する事業戦略の考え方を提示した。これらの成果は、査読付き学術論文 3 件（公開資料）および参考文献 1 件（イノベーションストラテジー研究成果書、抜粋を除き非公開資料）に報告されている。フリップチップ半導体デバイスの高電圧パルス注入によるビット反転の誘発と解析について、持続的な開発の基礎につながる工学的手段を与える成果であり、さらに科学技術イノベーションの観点からも価値ある集積であると認める。提出された論文は科学技術イノベーション研究科学学位論文評価基準を満たしており、よって学位申請者の弘原海 拓也は、博士（科学技術イノベーション）の学位を得る資格があると認める。</p> |        |