



Chip-Package System Level Countermeasure Methodologies against Side-Channel Leakage Problems

門田, 和樹

(Degree)

博士 (科学技術イノベーション)

(Date of Degree)

2024-03-25

(Date of Publication)

2025-03-01

(Resource Type)

doctoral thesis

(Report Number)

甲第8965号

(URL)

<https://hdl.handle.net/20.500.14094/0100490190>

※ 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 _____ 門田 和樹 _____

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。)

Chip-Package System Level Countermeasure

Methodologies against Side-Channel Leakage Problems

サイドチャネル漏洩問題に対するチップ・パッケージ・システムレベルの対策手段

指導教員 _____ 永田 真 _____

(注) 2, 000 字～4, 000 字

情報通信技術の発展により実現が進められている高度情報化社会では、デジタルデータの活用がもたらす社会的インパクトが大きく増大している。これはデジタルデータが不正に取得される、悪用されることにより、企業や個人、社会全体が受ける経済的、社会的損失が拡大するということを意味している。そのため、高度情報化社会においては、セキュリティ技術を用いてデジタルデータを不正取得や悪用から保護することが不可欠となっている。デジタルデータの保護には暗号技術が用いられるが、暗号技術を電子デバイスに実装した際にはデバイスの脆弱性を利用する物理攻撃がハードウェアセキュリティの脅威として存在する。中でも、暗号回路動作中に副次的に生じる消費電流、電磁波などのサイドチャネル情報を解析することで秘密情報を解読するサイドチャネル攻撃は、比較的安価、容易に攻撃可能であり、さらに実製品への攻撃事例も報告しているため非常に大きな脅威となっている。そのため、サイドチャネル攻撃による秘密情報の漏洩（サイドチャネル漏洩）への対策が急務となっている。

本論文では1つ（もしくは複数）のチップとパッケージを含むシステムに必要な機能を集約し実現したチップ・パッケージシステムにおいて、サイドチャネル漏洩を抑制する対策技術について論じる。サイドチャネル漏洩を対策するためには、サイドチャネル漏洩の原因となる電源ノイズの振る舞いの正確な理解と、対策手法の構築が重要となる。そこで、本論文では、サイドチャネル漏洩の原因となる電源ノイズの高分解能評価技術、サイドチャネル漏洩を抑制するパッケージング技術、サイドチャネル漏洩シミュレーションによる対策技術の3つの技術によりチップ・パッケージシステムレベルでのサイドチャネル漏洩対策手段の実現を検討した。

はじめに、サイドチャネル漏洩の原因となる電源ノイズの高分解能評価技術として、オンチップモニタ回路とシミュレーションを用いてシステムオンチップ(SoC)や3次元積層集積回路(3DIC)などの大規模デバイス内のダイナミック電圧ドロップ波形を評価した。オンチップモニタ回路による正確な電源ノイズ波形取得により、取得した電源ノイズ波形から算出したチップ内のノードのスイッチング数と、論理シミュレーションにより事前に算出したスイッチング数が高い精度で一致した。この技術はサイドチャネル漏洩の原因となる暗号回路の電源ノイズの振る舞いの理解に貢献する。また、電力供給を平坦化・安定化させるために、信号出力を生成せずにバックグラウンドでトグルを生成し、電力を消費する回路の診断にも応用可能である。

サイドチャネル漏洩を抑制するパッケージング技術としては、裏面埋設配線による電源供給網を三次元積層チップに適用する電源ノイズ抑制技術を提案した。この裏面埋設配線はシリコン基板の裏面に Cu 配線を埋め込む裏面埋設配線により電源供給網を形成することで、低い並列配線抵抗、裏面埋設配線とシリコン基板間の寄生容量を実現し、電源ノイズを低減する技術である。提案手法によりダイナミック電圧ドロップを抑制し、電圧変動にお

いて約 59%の低減を実現した。このノイズ低減効果によるサイドチャネル抑制効果は統計的有意性を表すt値を用いて評価し、従来実装と比較して 14 倍のサイドチャネル漏洩の抑制を確認した。

続いて、サイドチャネル漏洩対策のためのシミュレーション技術として、暗号コア解析に向けたトランジスタレベルの高精度サイドチャネル漏洩シミュレーション手法と、大規模回路向けに精度の低下を最小限に抑えつつ高速化を実現するシミュレーション手法を構築した。シミュレーションによるサイドチャネル漏洩評価が可能になった場合には、設計者は製造前にサイドチャネル漏洩耐性を評価し、求める耐性レベルに到達していなかった場合には即時に修正を施すことが可能となるため、サイドチャネル漏洩耐性シミュレーションは非常に重要である。しかし、シミュレーションの正確さや速度の面で課題が存在するため実用レベルには到達していない。そこで、暗号コアレベルの正確なシミュレーションではトランジスタレベルでのシミュレーションによるサイドチャネル漏洩評価における偽陽性が発生する課題を発見し、擬陽性を回避するシミュレーション手法の構築を行った。また、SoC レベルでのシミュレーションでは近年の回路規模の増大に伴うシミュレーション時間の増加が課題となる中、精度を維持しつつ高速化を実現するシミュレーション手法を提案した。提案手法を用いることにより、3 時間で 1 万波形取得が可能であり、さらにチップ内におけるサイドチャネル漏洩強度の分布についてのシミュレーション結果が実測と高い精度で一致することを確認した。

最後に、これらの技術を活用した事業計画として、シミュレーションを用いた物理攻撃耐性評価技術の事業化について検討した。社会背景と顧客課題を踏まえて、高い物理攻撃耐性を備えた暗号モジュール搭載半導体 IC チップ設計事業を提案し、提案事業の事業環境を分析した。分析の結果、物理攻撃への脅威が強く普及していない現段階においては、事業開始段階において物理攻撃の脅威を顧客に認識させることが非常に重要であることが明らかになった。脅威を認識させることに成功し、最初の顧客にサービスを利用してもらうことが出来れば、その後はシミュレーション技術について継続的に研究開発を行い、新規参入障壁を高めることで事業規模拡大が見込まれる。

氏名	門田 和樹		
論文 題目	Chip-Package System Level Countermeasure Methodologies against Side-Channel Leakage Problems (サイドチャネル漏洩問題に対するチップ・パッケージ・システムレベルの対策手段)		
審査委員	区 分	職 名	氏 名
	主 査	教 授	永田 真
	副 査	教 授	川口 博
	副 査	准教授	三木 拓司
	副 査	准教授	福家 信洋

要 旨

情報通信技術(ICT)分野において、デジタルデータの流通や利活用の一般化が進んでおり、その安全・安心な利用環境の提供は現代の社会生活において最も重要な技術領域の一つと考えられる。一般に、セキュリティシステムでは暗号化・復号を適正に利用することによりデジタルデータの機密性・完全性・可用性を確保するが、これに対して、悪意ある第三者は、暗号化・復号の機能を実現する半導体チップ等のセキュリティモジュールの動作状態におけるサイドチャネル情報を利用して秘密情報を奪取する、すなわちサイドチャネル攻撃の可能性を探索している。半導体技術の進展とともに、暗号化・復号のハードウェア実装において、高度なサイドチャネル漏洩耐性を具備する技術が開発されてきた。しかしながら、攻撃者も高度な解析手段を見出しており、暗号モジュールの危殆化を防ぐ多層的な防御手段が必要である。

本研究は、半導体チップとパッケージを含むハードウェアシステムにおいて、半導体集積回路の動作に伴い不可避に発生する消費電流あるいは放射される電磁波によるサイドチャネル漏洩の問題に着目し、これを解析・抑制あるいは検知する回路技術やシミュレーション技術を総合的に創出するものである。

本論文では、半導体チップにおけるサイドチャネル漏洩の問題に着目し、チップ・パッケージ・システムレベルの対策手段を実現する設計・構築・評価技術(先端IT分野)および半導体チップの設計事業(アントレプレナーシップ分野)について纏めている。サイドチャネル漏洩のメカニズムを半導体集積回路の動作と紐づけて深く理解し、サイドチャネル漏洩を引き起こす電流変動や電磁放射について半導体チップ内部や近傍空間における多元的な物理モデルにより表現する手段を与え、さらには数百万ゲートを超える大規模集積システムの半導体チップにおけるサイドチャネル漏洩の可能性をシミュレーションにより定量的かつ効果的に予測する道筋を示すとともに、本研究の開発技術を、高い物理攻撃耐性を備えた暗号モジュール搭載半導体チップ設計事業として社会実装する道筋についてイノベーションストラテジーを構築している。

本論文では、半導体チップにおけるサイドチャネル漏洩の問題に対して、チップ・パッケージ・システムレベルで対策する手段を確立すべく、次に示す5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を用いたサイドチャネル漏洩の半導体チップその場評価技術
- (2) 裏面埋設金属配線パッケージングによる電源ノイズの低減とサイドチャネル漏洩の抑制技術
- (3) 暗号モジュールのトランジスタレベルシミュレーションによるサイドチャネル漏洩対策の評価技術
- (4) セキュア半導体チップにおける電源電流シミュレーションとサイドチャネル漏洩の評価技術
- (5) 物理攻撃耐性を備えた暗号モジュール搭載半導体チップ設計事業に関するイノベーション戦略である。

前項(1)では、半導体チップに高分解能のオンチップ電圧モニタ回路を搭載することで、暗号モジュールの動作テストモードにおいて、暗号化・復号の動作に由来する消費電流をチップ内部で観測し、サイドチャネル漏洩の発生を定量的に評価する手法を提案している。一般に、大規模集積システムの半導体チップにはマイクロプロセッサ等の汎用デジタル回路ブロックと暗号モジュールが混在している。半導体チップの通常の動作において暗号モジュールが単体で動作することは稀であり、その一方で、消費電力の制約あるいは極大化を回避する観点から全てのブロックが同時に動作することも一般的でない。そこで、半導体チップに論理ゲートのトグル率を可制御とするデジタル回路を搭載することにより、適正なバックグラウンド消費電力のもとで暗号モジュールの動作とサイドチャネル漏洩を評価する手法について詳述している。これに加えて、基本論理ゲートの消費電荷量を基本単位とする粒度で消費電流を評価できることも示している。

氏名	門田 和樹
前項(2)では、半導体チップの裏面に金属配線パターンを埋設形成し、これを半導体チップの表面に具備されたデジタル回路の金属配線とシリコン貫通ビアを経由して接続する先端パッケージング構造を提案している。半導体チップの裏面に形成される寄生容量により、デジタル回路の電源電流変動すなわち電源ノイズを効果的に低減でき、さらに、サイドチャネル漏洩を抑制できることを実験的に明らかにしている。 前項(3)では、暗号モジュールのサイドチャネル漏洩を対策するマスキングアーキテクチャについて、半導体チップを形成するトランジスタレベルの回路シミュレーションにより消費電流の高分解能波形を取得し、サイドチャネル漏洩の発生する可能性をt検定値により評価する手段を概説している。ここで、t検定値が回路シミュレーションの数値解析パラメータに強く依存する可能性を実験的に示唆するとともに、サイドチャネル漏洩の発生について偽陽性もしくは偽陰性を判断する必要性を示し、半導体チップの設計検証におけるサイドチャネル漏洩シミュレーションの適正な適用手段に関する新規の知見を提示している。 前項(4)では、大規模集積システムの半導体チップにおいて、数百万ゲート規模のデジタル回路における消費電流をパワーライブラリベースの電源電流シミュレーションにより効率的に導出する一般的な手段を概説している。当該手段の応用として、暗号モジュールと汎用デジタル回路の同時動作におけるサイドチャネル漏洩を評価する手法、さらには、半導体チップ内部においてサイドチャネル漏洩を発生する主要部分を特定する手法について提案するとともに、半導体チップの電源電流による近傍磁界の発生および電磁的なサイドチャネル漏洩の発生についてシミュレーション評価が可能であること、およびチップ・パッケージ・システムレベルにおけるサイドチャネル漏洩の探索に有意であることを実験的に明らかにしている。 前項(5)では、サイドチャネル漏洩に関するトランジスタレベルからチップ・パッケージ・システムレベルに至るシミュレーション技術を応用し、セキュリティ向け半導体チップの開発支援につながる設計事業の可能性についてイノベーションストラテジーを構築している。 いずれの課題においても、半導体チップにおけるサイドチャネル漏洩の問題を高機能・高密度・高性能な集積システムにおける物理事象として捉え、これを対策するため、回路技術とシミュレーション技術を核とした工学的手法を与えている。暗号モジュールのサイドチャネル漏洩による脆弱性の発現およびその対策に関する最先端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。 本論文の構成は以下のとおりである。 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。半導体チップにおけるサイドチャネル漏洩の問題を網羅的に指摘し、回路技術およびシミュレーション技術による対策手法の導出と適用方針について論じている。 第2章では、オンチップ電圧モニタリングを用いたサイドチャネル漏洩の評価技術について詳述している。 第3章では、裏面埋設金属配線を具備した先端パッケージングにおける電源ノイズの低減とサイドチャネル漏洩の抑制技術について詳述している。 第4章では、暗号モジュールのトランジスタレベルシミュレーションによるサイドチャネル漏洩対策の評価技術について詳述している。 第5章では、暗号モジュール搭載半導体チップにおける電源電流シミュレーションとサイドチャネル漏洩の評価技術について詳述している。 第6章では、サイドチャネル漏洩のシミュレーション技術を応用したセキュリティ半導体チップの設計事業に関するイノベーション戦略について概略を述べている。 第7章では、まとめと今後の展望を述べている。 本論文は、以上のように、サイドチャネル漏洩問題に対するチップ・パッケージ・システムレベルの対策手段に関し、暗号モジュールのアルゴリズム・アーキテクチャ・回路・パッケージングの技術階層において論じるとともに、これを対策する回路技術とシミュレーション技術を導出し、さらに、最先端半導体技術による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、セキュリティ向け半導体チップの開発を支援する設計事業の可能性を示し、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。 本研究の成果として、サイドチャネル漏洩問題に対するチップ・パッケージ・システムレベルの対策手段に関する深い理解を導き、また、半導体チップ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件と国際会議論文1件（いずれも公開資料）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。サイドチャネル漏洩問題に対するチップ・パッケージ・システムレベルの対策手段について、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門田 和樹は、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。	