別紙１

論文の内容の要旨

論文題目	Research on hardware-based hiding countermeasures against Power Analysis Attacks （和訳：電力解析攻撃に対するハードウェアベースの隠蔽対策に関する研究）
学位申請者	Dao Ba-Anh

近年、電力解析攻撃は、暗号デバイスのセキュリティに対する深刻な脅威として浮上している。これらの攻撃は、対応する暗号アルゴリズムの理論的弱点の分析に焦点を合わせるのではなく、物理的な実装によって引き起こされる意図しないデバイス内の情報のリークを利用する、サイドチャネル攻撃の一種に分類される。ここでいう意図しないリークとは、暗号デバイスが機密性の高い中間値を処理する際の、電力消費または電磁放射である。このリーク情報を解析することで、攻撃者は対応する暗号アルゴリズムの秘密鍵を取得する。

電力解析攻撃には多くの対策が提案されているが、マスキング対策と隠蔽対策の2つのグループに分類できる。マスキング対策は、暗号処理中の中間値を予測されないようにランダムにマスクする。一方、隠蔽対策は、中間値のリーク情報を低減するため、暗号デバイスの消費電力特性を変更する。マスキング対策は多くの場合、暗号処理が複雑となり、計算量が大幅に増加するため、スループット低下や実装コストの増加を引き起こす。さらに、ディープラーニングを利用した最先端の電力解析攻撃では、使用されているマスクに関する情報がなくてもマスキング対策を破れる可能性が示されている。

一方、隠蔽対策は暗号アルゴリズムの変更が不要ないため、一つのデバイスに複数のアルゴリズムを実装する際に、すべてに同様に適用することができる。また、マスキング対策よりもディープラーニングベースの電力解析攻撃への耐性が高いことも実験的に証明されている。概して、隠蔽対策はマスキング対策と比較して、ハードウェアコストや速度性能等のパフォーマンスに優れているが、実装のオーバーヘッドは依然として少なくない。

本論文は、電力解析攻撃への耐性が大きく実装が容易、かつ汎用性を有した2つの新しいハードウェアベースの隠蔽対策を提案している。最初の対策は、デバイス速度と消費電力の動的制御に広く用いられるSOTB（Silicon On Thin Buried Oxide）製造技術のバックゲートバイアス技術を利用するる。これにより特殊な回路を付加することなく、消費電力をランダム化することができる。2番目の対策は、暗号デバイスの動作周波数を動的に変更するランダム動的周波数スケーリ

ング対策である。提案手法を施した暗号デバイスをFPGAとASICで実装し、電力解攻撃実験を行った。その結果により、提案手法は、隠蔽対策よりも少ないハードウェアリソースで、高い耐性を有することが示された。

提案対抗策は、提案対抗策を適用する場合としない場合で、FPGAとASICの両方に実装された実際の暗号化デバイスに対して実際の電力分析攻撃を実行し評価する。評価において、最先端の電力分析攻撃のVector Leakage Assessment（TVLAリークテスト）、Correlation Power Analysis（CPA）攻撃やDeep Learning-based Sideチャネル攻撃（DL-SCA）などを実施した。実験結果により、提案対策は、特にハードウェアリソースの使用率の点で、他の隠蔽対策よりも優れていることが分かった。

別紙２

論文審査の結果の要旨

学位申請者氏名　Dao Ba-Anh

審査委員主査　範　公可

委員　石橋　孝一郎

委員　佐藤　証

委員　崎山　一男

委員　菅原　健

（*自筆署名の場合に限り、押印省略可）

第１章では、攻撃者は、暗号化デバイスの電力消費または電磁放射に関する漏洩情報を使用して、暗号化に必要な秘密鍵を抽出するサイドチャネル攻撃のサブセットである電力分析攻撃の概要について述べている。まず、電力分析攻撃の元のアイデア、基本原則、分類、および最先端の開発について述べ、それに続き、マスキング対策や隠蔽対策など、電力解析攻撃に対する一般的な既存の対策とそれらの長所と短所について比較している。最後に、研究の動機および主要な貢献の新しい隠蔽対策について述べている。

第２章では、関連研究として、暗号デバイスの電力波形の振幅および処理の時間に対する隠蔽対策について述べている。前者は暗号処理中の機密性の高いデータと電力振幅との相関を隠蔽し、後者は解析する機密データが処理される時間を隠蔽するものである。本論文では、これら振幅および時間ベースの隠蔽対策を提案している。

第３章では、評価手法の理論的背景とその手順について述べられている。これらの評価手法には、従来の差分電力解析攻撃、相関電力解析攻撃、ディープラーニングベースのサイドチャネル攻撃、およびテストベクトルリーク評価が含まれまる。

第４章では、電力解析攻撃に対する新しい対策として、バックゲートバイアスを用いる手法が提案されている。完全に空乏化したシリコンオンインシュレータ（FD-SOI）テクノロジは、バックゲートバイアス電圧の制御性は優れている。これにより、FD-SOIテクノロジで製造されたデバイスを、必要なアプリケーションに応じて、適切なバックゲートバイアスを用いて低消費電力または高性能に最適化できる。理論的な議論に続き、バックゲートバイアスによる暗号処理中の電力波形の小振幅化と、バイアスをランダムに変更するRandom Dynamic Back-gate Bias（RDBB）の2つの対策が提案されている．提案対策を施したAES-128暗号は65 nm STOB 32ビットRISC-Vマイクロコントローラに実装され、差分電力解析（DPA）攻撃が実施された。その結果、提案手法を施した実装はそれぞれ、16バイトの秘密鍵

全体の抽出に必要な電力トレース数を、従来手法の14.5倍および33.4倍に増加させるなど高い性能が示されている。

第５章では、暗号コンポーネントがシステム全体のハードウェアのごく一部であっても、複数の電力解析攻撃に対して脆弱であることが示されている。そして、複雑な暗号化SoCを電力解析攻撃から防御するランダム動的周波数スケーリング対策が提案され、CPA攻撃、DL-SCA攻撃、およびTVLAリークテストを通じてその有効性を検証している。提案対策を施したRISC-V SoCは、CPA攻撃に対して対策を施さない時よりも500万を超える電力トレースを増加させ、少なくとも2,593倍の改善であることが示された。TVLAリークテストに対しても500万の電力トレースで合格し、高度なDL-SCA攻撃への耐性も強化されることを明らかにしている。さらに、スペクトラム拡散技術や周波数領域分析を実施し、より厳密なセキュリティ評価も行われている。

第６章では、全体的な成果および課題が述べられ、将来の研究としてのいくつかの未解決のトピックが示されている。

本研究は工学における成果として、また情報化社会を支える基盤技術として産業にも大きな貢献が期待できる。よって、本論文は博士（工学）の学位論文として十分な価値を有するものと認める。