暗号モジュールの電源ノイズと情報漏洩に関する研究

藤本，大介

(Degree)
博士（工学）

(Date of Degree)
2014-03-25

(Date of Publication)
2015-03-01

(Resource Type)
doctoral thesis

(Report Number)
甲第6104号

(URL)
https://hdl.handle.net/20.500.14094/D1006104

（別紙様式 3）

論文内容の要旨

氏　名　藤本　大介

専　攻　情報科学専攻

論文題目（外国語の場合は，その和訳を併記すること.）

暗号モジュールの電源ノイズと情報漏洩に関する研究

指導教員　永田　真

（注）2，000 字～4，000 字でまとめること.

近年，モバイル PC，携帯電話，スマートカードの普及により，個人情報を持つ携帯デバイスがますます増加している．これらの携帯デバイスに含まれる秘密情報を保護するためには，暗号化を行い，鍵を持たない他者からは解読できない形式にする必要がある．暗号化に使用されるアルゴリズムは現実的な時間で数学的に暗号解読が不可能である必要があり，規格の制定の際には多くの研究者によって，暗号化を破る攻撃が行われ安全性の評価が行われている．

しかし，数学的に安全であるアルゴリズムであっても実際に LSI 上に実装した場合，暗号化処理中に放射される電磁波や，消費電流量が漏れ情報として流出してしまう．これらの漏れ情報をサイドチャネル情報と言い，サイドチャネル情報を用いた暗号化回路攻撃手法をサイドチャネル攻撃と言う．暗号化回路が消費する電流による電圧変動を観測し攻撃する Differential Power Analysis(DPA)が提案されている．暗号化回路の消費電流量は回路の動作に依存するため，大量の消費電流波形を収集できれば，回路内部の動作が予測でき秘密鍵が特定されてしまう危険性がある．DPA に代表される電力解析攻撃は電源電圧変動波形を取得するためのオシロスコープと波形を処理する計算機のみで構成でき，非常に安価なため脅威となっている．標準暗号として用いられている AES(Advanced Encryption Standard)であっても対策を施さずに回路実装を行った場合は電力解析攻撃によって秘密鍵が取得できることが報告されている．

そのため，電力解析攻撃に対する対策を設計段階で評価することは重要である．電力解析攻撃は内部データ遷移に依存するため多くの対策は入力データに依存しない遷移回数の論理を構築することで実現される．しかしながら，実際には論理セル間の遅延の差，消費電流のアンバランス，配線負荷のアンバランスなどからサイドチャネル情報が漏洩してしまう．そのため，物理デバイスレベルでの暗号化回路の消費電流シミュレーションを行うことが求められている．しかし，電力解析攻撃の評価のためには 1 万波形以上ものシミュレーションが必要であり，既存の回路シミュレータを用いるのは現実的ではない．

一方で，製造後の測定評価において，現在では実際に攻撃が行われる時と同様に評価ボード上に電源電圧取得端子を設けて電源ノイズ波形を取得し電力解析攻撃ができないかを評価する手法が一般的である．しかし，チップ外部で得られる波形はボードの設計に大きく依存し，攻撃者がより高精度に電源ノイズを取得できる場合については対策ができていない．

また，暗号化回路の電力解析攻撃への耐性を評価する際に必要な電源ノイズの波形数が評価時間に大きく関わる．対策された暗号化デバイスであっても取得可能な時間で数十万波形を集めれば攻撃が可能になる場合があるためである．しかし暗号デバイスを設計するうえで数十万波形をシミュレーション，測定することは困難である．

（氏名：　藤本　大介　　NO.2　　）

本研究では，暗号化回路における電力解析攻撃への安全性評価技術として，物理デバイスレベルでの高速なシミュレーション，チップ内部での電源ノイズ波形取得技術，電力解析攻撃評価時に必要な波形を削減する技術を提案することを目標とする．

まず，シミュレーション技術においてはCMOS回路における消費電流が寄生容量の充電過程で発生するメカニズムに着目し，時系列的に充電される静電容量の列に置き換えてシミュレーションする容量充電モデルを提案する．静電容量の計算にはあらかじめ論理セルごとに遷移時に流れる電流を抽出しておき，高速であるデジタルシミュレーションと組み合わせる事で実現した．容量充電モデルによるシミュレーションによる電力解析攻撃の結果は実際のデバイスでの傾向とよく一致することを確認した．レイアウト情報を含む消費電流シミュレーションにおいてレイアウト情報を含まない回路シミュレータでの結果に対して200倍の高速化を達成した．

測定手法においては，従来チップ内の電源ノイズ観測に用いられてきたオンチップ診断技術であるオンチップモニタリング技術を応用した．チップ内での電源ノイズ観測のために暗号化回路とオンチップモニタを搭載したチップを試作し，チップ内外での電源ノイズの変化を評価した．結果，チップ外へは高周波成分が出て行かないことという知見を得た．一方で，対策を施さない場合低周波成分にサイドチャネル情報が重畳することをつきとめた．この結果より，高周波成分に対する評価はチップ内における測定が必要であることが言える．

暗号化回路の評価時の波形数が膨大である問題については，回路開発者は秘密情報を持っているという利点を活かし，評価したい電力解析攻撃に合わせて暗号化デバイスからサイドチャネル情報が漏れやすい入力を生成する手法を提案する．この手法を用いることでワーストケースでの攻撃が成功できるかが評価できる．実際にシミュレーション，測定において1万波形を用いても攻撃できない電力解析攻撃対策実装を評価し，4000波形程度で鍵の取得ができサイドチャネル情報が漏れているという結果を得た．この結果は1万波形より波形数を増やすと秘密情報を取得されてしまう可能性を示唆し，評価を1万波形で終了してしまうと評価として不十分であることを意味する．この評価の効率化手法により設計・製造時のサイドチャネル漏洩評価にかかる時間が大幅に削減される．

今後，暗号化回路を搭載したデバイスはますます増加する．そこで安全な暗号回路を設計する技術がより重要になる．本論文で提案した，シミュレーション技術は設計時の時背評価を可能にする．測定技術は製造後デバイスのより強固な評価となりうる．評価技術はシミュレーション，測定両者においてテスト時間を短縮する．これらの技術は安全な暗号回路のデザインフローを構築する上で有用である．

（別紙１）　　論文審査の結果の要旨

氏名	藤本 大介		
論文題目	暗号モジュールの電源ノイズと情報漏洩に関する研究		
審査委員	区　分	職　名	氏　　名
	主　査	教　授	有木　康雄
	副　査	教　授	鳩野　逸生
	副　査	教　授	永田　真
	副　査		
	副　査		印

要　　旨

暗号モジュールにおけるサイドチャネル攻撃は、安全・安心な社会に向けた電子情報システムにおける具体的な脅威となっている。暗号アルゴリズムはVLSIシステムに実装されることによりはじめて実用されることから、暗号モジュールの集積回路開発において、高い安全性を獲得することが必須である。しかしながら、実デバイスを対象にしたサイドチャネル情報の収集に係るコストは小さく、大量のデータを比較的短時間で得られることに対して、暗号モジュール集積回路の設計段階におけるサイドチャネル情報のシミュレーションには物理メカニズムを適切に含む必要があり、サイドチャネル情報漏洩を設計品質の定量的指標として捉えることがたいへん困難である。そこで本研究では、暗号モジュールの集積回路における電源ノイズに着目し、サイドチャネル情報漏洩の高速シミュレーションと、攻撃対策手法の導入評価に関する工学的な解決法を与えることを目的とした。

本論文では、暗号モジュールの電源ノイズと情報漏洩に関して、電源ノイズをサイドチャネル情報の担体とした情報漏洩メカニズムの実験的理解と、容量充電モデルによる高速シミュレーション手法の開発、およびサイドチャネル攻撃対策を施した暗号モジュールの導入評価に適したシミュレーションおよび実験手段、について研究成果をまとめている。本論文に論じられている研究成果の一部は、組込みシステムにおける暗号プロセッサの物理攻撃に対する安全性評価に関する産官学連携研究プロジェクトによるものであり、社会的要請への学術貢献および実用性を意識した工学成果であることに特徴がある。

本論文では、暗号モジュールの電源ノイズと情報漏洩に関して、以下の3つの研究課題について論じている。すなわち、

(1)　暗号モジュールのVLSI実装における電力解析攻撃の高速シミュレーション手法
(2)　暗号モジュールのVLSI実装における回路近傍電源ノイズの測定と攻撃手法
(3)　暗号モジュールのVLSI実装における電力解析攻撃への耐性評価手法

である。

暗号モジュールの電源ノイズと情報漏洩に関して、前項(1)では、CMOSデジタル回路の電源消費電流をコンパクトに表現する容量充電モデリング法を暗号モジュール集積回路に適用し、10,000以上の異なる入力平文パターンに対する暗号モジュールの動的な消費電流モデルを高速に生成し、電源ノイズをシミュレーションする手法を確立した。また、論理構造の異なる複数の秘密鍵(AES)方式暗号モジュールについて、実デバイスに対する電力解析攻撃と、本手法によるシミュレーション波形に対する電力解析攻撃を実施し、両者による攻撃の成立（秘密鍵の全バイト特定）を実証するとともに、シミュレーションにより効果的な攻撃評価が可能であることを明らかにした。前項(2)では、オンチップの電源ノイズ波形を収集するオンチップモニタ機構と複数の暗号モジュールを搭載したテストチップを開発し、チップ内ノイズ波形に

氏名	藤本 大介

よる電力解析攻撃が、従来のオンボードのノイズ波形による攻撃と同等あるいはそれ以上（少ない波形数による秘密鍵の全バイト特定が可能）であることを明らかにした。前項(3)では、サイドチャネル攻撃対策回路方式による暗号モジュールについて、その攻撃耐性を効果的に評価するための入力平文の選択手法を提案した。暗号モジュールの集積回路開発者が、既知の秘密鍵を前提に、効率的にサイドチャネル攻撃を行うことで、設計時点でサイドチャネル情報漏洩の程度を定量的に評価できるようにした。

いずれの課題においても、暗号モジュールの集積回路化におけるサイドチャネル情報漏洩のメカニズム解明および対策のあり方の追求に関し、電源ノイズのシミュレーション法ならびにオンチップモニタリング法の適用にとどまらず、暗号工学の考え方に立脚した理解と議論に努めている。暗号モジュールの安全性を、電源ノイズを担体としたサイドチャネル情報漏洩について設計時点で解析評価する手法を与えている点で、本論文における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。

第一章では、研究の背景と動機について述べている。暗号モジュールの VLSI 実装に関する技術動向について簡潔に述べると共に、さまざまなサイドチャネル攻撃技術に関する先行研究をまとめ、本研究による発展的な内容の位置づけを明らかにしている。

第二章では、暗号モジュールの VLSI 実装における電力解析攻撃の高速シミュレーション手法に関して、容量充電モデルを応用し、10,000 以上の入力平文に対する消費電流波形の導出を効率化する方法について論じている。

第三章では、暗号モジュールの VLSI 実装における回路近傍電源ノイズの測定と攻撃手法に関して、オンチップモニタと暗号モジュールを搭載したテストチップの構成法および評価システムの構築法を示すとともに、オンチップの電源ノイズならびにオンボードの電流ノイズに対するサイドチャネル攻撃と評価について論じている。

第四章では、暗号モジュールの VLSI 実装における電力解析攻撃への耐性評価手法に関して、サイドチャネル攻撃対策型の暗号モジュール集積回路におけるサイドチャネル漏洩評価に向けた選択平文の導出方法ならびに導入評価法について論じている。

第五章では、まとめと今後の展望を述べている。

以上のように、本研究は暗号モジュールの電源ノイズと情報漏洩に関して、容量充電モデルを用いた電源ノイズによるサイドチャネル情報漏洩のシミュレーション手法、およびオンチップモニタによるチップ内部の電源ノイズ波形取得を用いた高い能力の攻撃の実証と、攻撃対策版の導入評価、について具体的な提案と成果を得ている。今後の研究展開として、最先端デバイスによるサイドチャネル情報漏洩の評価やサイドチャネル情報漏洩を低減する新しい集積回路技術の開発への応用が期待できる。

本研究の成果は、査読付き学術論文２件、および国際会議論文４件に報告されている。

このように本研究は、暗号モジュールにおける電源ノイズを担体としたサイドチャネル情報漏洩の問題に対して、深い理解を導き、また効果的な対策を見極める工学的手段を与える成果であり、価値ある集積であると認める。提出された論文はシステム情報学研究科学位論文評価基準を満たしており、学位申請者の藤本大介は、博士（工学）の学位を得る資格があると認める。