早稲田大学大学院情報生産システム研究科

博士論文審査報告書

論　文　題　目

Research on Performance Enhancement for Electromagnetic Analysis and Power Analysis in Cryptographic LSI

申　請　者

Hongying LIU

情報生産システム工学専攻

マルチメディアシステム研究

2012 年 11 月

近年、ユーザ認証や秘密情報の保管などに様々な暗号化デバイス、例えば、スマートカード、無線タグ、投票計算機、暗号コプロセッサなどが、広く使われている。その一方で、暗号をアルゴリズムの面から解析するだけではなく、電磁波や電力等の物理的な漏洩を解析するサイドチャンネル解析が出現し、暗号化デバイスの安全性を確保する手法の確立が重要な課題となってきた。

多くのサイドチャンネル解析のなかで、電磁波解析や電力解析は多くの研究成果が公開されており、比較的安価に解析環境を構築することができるため、セキュリティ分野では注目を集める重要な課題となっている。また、サイドチャンネル解析から暗号化デバイスを守るための耐タンパー技術の研究や実用的に安全なLSI設計も多数行われてきている。電磁波解析と電力解析は暗号化デバイスに対するサイドチャネル攻撃の耐タンパー性（防護力）を評価する際の基礎となる技術であることから多くの研究がなされてきた。

しかし、従来提案された解析手法を実際に適用する際には、下記のような問題が存在する。(1) 電磁波サイドチャンネル解析では、Le (IEEE TIFS07)がガウシアンノイズに対するノイズの低減の手法を提案したが、非ガウシアンノイズに対する良い手法がまだ知られていない。(2) Brier (CHES04)が提案したハミング距離漏洩モデルは一般的に有効とされるが、具体的なデバイスに適用するためにGlitch(回路の中に不均一なパス遅延が論理ゲートへ入力されることで起きる不必要な信号転移)電力の消費を考慮した改善をすべきである。(3) 電磁波解析には漏洩位置を高い精度で求めることが必要となるが、Sauvage (ACM TRTS09)が提案した統計的検定に基づいた検出方法は正確な位置を特定することができない。

これらの問題があるため、従来手法は電磁波解析と電力解析のパフォーマンス（正確な暗号鍵を低演算量で求めること）の低下を招いている。パフォーマンスを向上させることができれば、暗号解析の時間を短縮することができ、暗号の耐タンパー性能をより正確に測定できる。それにより、より安全性の高い暗号化デバイスの開発が可能となる。

本論文の目的は、電磁波解析と電力解析のパフォーマンスを向上させる新しい手法を提案することである。電磁波解析と電力解析のパフォーマンスの向上にはノイズの低減、正確な漏洩のモデルの構築、及び有効な統計手法の適用という３つの課題を解決することが重要である。本論文では、これらの課題に対する有効な手法として、以下の３つの内容を提案している。

(1) 電磁波サイドチャンネル情報のノイズ低減問題を解決するために、相関ノイズ(Correlated Noise) と同期ノイズ (Simultaneous Noise) を取り上げ、ノイズの電磁波解析への影響を下げる効率的なアルゴリズムを提案している。

(2) Glitch電力の消費を考慮するために、Switching Glitch漏洩モデルを新たに提案し、電磁波解析と電力解析のパフォーマンスを向上させている。

(3) 漏洩位置を高い精度で求めるために、ニアフィールドスキャンに基づいた瞬時信号分散を利用した新たな漏洩測定方法を提案し、電磁波解析のパフォーマンスを向上させている。

本論文は以下の章で構成される。

第 1 章[Introduction]では、暗号のサイドチャンネル解析手法を紹介し、特に、電力解析と電磁波解析の説明を行い、現在までに発表された解析技術を紹介し、本論文の位置づけと目的を述べている。

第 2 章[Correlated Noise Reduction for EMA]では、暗号の電磁波解析で発生する相関ノイズを取り上げ、ノイズの電磁波解析への影響を低下させる効率的な 3 つのアルゴリズムを提案している。相関ノイズはクロックネットワークから発生される電磁波が暗号化モジュールに干渉することが原因で引き起こされるものであり、ノイズと暗号化信号の間には強い相関性が現れる。ノイズの周波数バンドと暗号信号の周波数バンドが重なっているために、Pelletier (NIST 05) によって提案された離散ウェーブレット変換手法では、ノイズを信号から分離できない。実機での測定とシミュレーションを行うことで、ノイズと暗号化信号では、ノイズのクロック信号のエッジ分散が大きいことがわかった。この特徴を利用して、S-SVD(Single-sample singular value decomposition)法、M-SVD(Multi-sample singular value decomposition)法、A.Subt.(Averaged Subtraction) 法の 3 種の方法を提案している。S-SVD 法と M-SVD 法は、混合信号中からエッジ分散値の大きいクロック信号をサンプリングし、相関ノイズを分離する方法である。A.Subt.法は、信号サンプリング時に背景信号を分離する方法である。これらの手法を AES 暗号が FPGA と ASIC に実装されているボード上で実験を行った。Pelletier (NIST 05)のノイズ削減方法は SNR 値が平均で 2.45dB であったが、提案した 3 つの方法は夫々、14.49dB、 21.58dB、8.08dB となる結果が得られ、相関ノイズの影響を低下させることが確認でき、提案した手法の有効性を示すことができている。

第 3 章[Simultaneous Noise Reduction for EMA]では、電磁波サイドチャンネル解析での同期ノイズを削減するアルゴリズムを提案している。電磁波サイドチャンネル解析では、攻撃への有効な防御手段として、複数の暗号化モジュールを同時に動かすことがある。これにより、同期ノイズが発生し解析が困難になる。Le (IEEE TIFS07)は 4 次累積率 (Cumulant) を用い、ガウスノイズに対しては有効な解析が可能であることを示したが、非ガウスノイズに対しては効果的な解析ができないことが課題であると指摘されている。本論文では、非ガウスノイズに対して、Hyvarinen が提案した FastICA アルゴリズム(IEEE Tran.NN,1999)を用いて、混合信号の中から単一暗号化信号を抽出した後に、相関係数判定と暗号信号の振幅を再生成するという SR (Source Recovery) 法を提案している。SR 法は、同期ノイズを効率良く削減でき、正確に暗号鍵を解析することができるため、SR を適用しない方法と比べて、正確な鍵を検出するために必要な信号の数を 47.8%まで減らすことができることを実験で確かめている。電磁波解析のパフォーマンスを大幅に上げることができる手法を開発したことは学術的に高く評価できる。

第 4 章[The Switching Glitch Leakage Model for EMA and PA]では、電磁

波解析と電力解析のパフォーマンスを向上させるために新たな漏洩モデルを提案している。Brier (CHES 04)が提案したハミング距離漏洩モデルは暗号解析手法のなかで広く利用されてきたが、Glitch が引き起こすエネルギー消費は考慮されていない。多くの場合、Glitch のエネルギー消費は CMOS 回路の動的動作エネルギーの 20%から 40%を占めるため、Glitch を考慮しない従来の電磁波解析と電力解析手法ではパフォーマンスの劣化が起こる。本論文では回路中のデータに依存する論理回路の反転と暗号化演算時の Glitch 消費も考慮した Switching Glitch モデルを提案している。従来のハミング距離漏洩モデルと比較したところ、電力解析では正確な鍵を検出するに必要な信号の数が 24.5%減少し、電磁波解析では 17.1%減少することが確認された。パフォーマンスを向上することが可能となっており、学術的にも、実用的にも高く評価できる。

第 5 章[A Novel Leakage Localization Method for EMA]では、電磁波解析のパフォーマンスを上げるために、新しい漏洩定位方法を提案している。電磁波の放射は局所的特性を持ち、秘密情報が暗号化デバイスの複数の位置から漏洩するため、暗号解析をする前に電磁波解析をする最適な位置を特定することは困難であり、信号を取得し解析を行いながら位置を見つけることとなる。Sauvage (ACM TRTS09)の方法は計測値の最大値に着目した方法を採用しており、局所的に最適値を早く検出できるが、広域の多くのデータに依存する電磁漏洩の場合は検出が困難である。本論文ではプローブの近傍箇所から取得した電磁波放射信号に対して、信号の分散値と中央値の差分値が同一になることを利用して、暗号化モジュールの漏洩を識別する方法を提案している。実際に磁場プローブを作り、ASIC 化された AES 暗号が搭載されたボード上で提案手法の性能を測定している。実験の結果、Sauvage の手法と比べて正確な漏洩位置を特定化する率が 48.6%向上することが確かめられ、その有効性を高く評価できる。

第 6 章[Conclusion]では本論文をまとめ、本研究成果を総括している。

以上、電磁波解析と電力解析問題において、様々なノイズが発生する環境下で、正確な暗号鍵を低演算量で求める問題に対して新しい手法を提案しその有効性を示しており、学術的な貢献のみならず、実用面でも有効な研究成果であると評価できる。
よって本論文は博士（工学）の学位論文として価値あるものと認める。

2012 年 10 月 23 日

審査員

主査 早稲田大学　教授　工学博士　（早稲田大学）　後藤　敏
早稲田大学　教授　博士（工学）（大阪大学）　吉村　猛
早稲田大学　教授　博士（工学）（早稲田大学）　戸川　望
日本電気株式会社主席研究員　博士（工学）（中央大学）角尾幸保