論 文 内 容 の 要 旨

博士論文題目

暗号モジュールから生ずるサイドチャネル情報の計測困難化手法に関する研究

Countermeasure Methodology Preventing Electromagnetic Measurement against Side-channel Attacks

氏　　名　　和田 慎平

（論文内容の要旨）

電子機器に対する情報セキュリティ確保のために、暗号技術が重要な役割を果たしている。近年では、暗号処理の高速化などを目的に、暗号アルゴリズムを専用のモジュール（暗号モジュール）に実装し、利用する機会が増加している。一方で、暗号モジュールの動作に伴って生ずる電磁放射を計測・解析し、秘密鍵情報を解読する電磁波解析が現実的な脅威となっている。電磁波解析には暗号アルゴリズム毎に様々な解析手法が存在し、それぞれの解析手法に対し、秘密鍵解読の困難化に着目した対策手法がこれまで議論されてきた。電磁波解析は暗号モジュールから生ずる漏えい電磁界の計測に基づいて解析が実行されるため、漏えい電磁界の計測を困難化することで、暗号モジュールに実装されるアルゴリズムに依存しない対策手法を実現できる可能性がある。

漏えい電磁界の計測を困難化する対策手法の実現には、（１）電磁界計測が実行され得る秘密情報漏えい位置の特定、（２）特定した位置における電磁界計測検知が課題となる。本論文では、（１）に関して、暗号機器上に分布する電界・磁界それぞれの網羅的な計測に基づく秘密情報漏えい位置の特定手法を提案し、電界支配・磁界支配で秘密情報が漏えいする位置を明らかにした。続いて（２）に関して、秘密情報を含む電界・磁界が放射される位置での計測を困難化するための手法として、計測位置周辺における電磁環境の変化に着目した電磁界計測検知手法を提案した。

これにより、秘密情報を含む電界・磁界が漏えいする機器の物理構造を考慮し、その周辺電磁環境の変化を暗号モジュール内部から検知することで、秘密情報漏えいを引き起こす電磁界計測の困難化が可能であることを示した。

氏　名	和田 慎平

（論文審査結果の要旨）

本研究では、暗号モジュールに対する電磁波解析攻撃への対策として、攻撃時に避けることができない漏えい電磁界の計測を困難化することに着目した対策手法を提案した。

本論文の主な成果は以下に要約される。

1. 暗号機器上で漏えい電磁界による秘密情報漏えいが生ずる位置を特定するために、機器上での電磁界分布の計測に基づく秘密情報漏えい位置特定手法を提案し、その有効性を実証した。
2. 提案した秘密情報漏えい位置特定手法に基づき、秘密情報漏えいが生ずる暗号機器の物理構造を明らかにした。
3. 周辺電磁環境の変化をパッシブおよびアクティブにセンシングすることで、電磁波解析攻撃時に実行されるプロービングを検知可能であることを示し、漏えい電磁界の計測を困難化することにより、実装される暗号アルゴリズムに依存しない汎用的な対策手法を実現可能であることを示した。

以上の様に、本研究は攻撃者が電磁気学の基本法則上回避困難な対策を実現しており、情報セキュリティ分野に与えるインパクトは少なくない。よって本研究は、博士（工学）の学位論文としての価値があるものと認める。