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

氏　　名　和田 慎平
研 究 室 名　情報セキュリティ工学研究室
主指導教員名　林 優一教授

内 容 梗 概（1ページ目に収めること）

高度情報化社会では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、暗号モジュールへの攻撃が行われており、中でもモジュールの動作に伴って生ずる電磁放射を解析し、秘密鍵情報を解読する電磁波解析が現実的な脅威として報告されている。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。一方で、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。

本研究では、秘密情報の漏えいを引き起こす電磁界の計測困難化を達成するための評価技術・メカニズム解明・対策技術の実現を目的とする。漏えい電磁界の計測を困難化する手法として、攻撃実行時における暗号モジュールでの処理停止や、ダミー処理の実行などの対策が挙げられることから、これらの対策を実現するためには、（1）電磁界計測が実行され得る秘密情報が漏えいする位置の特定、（2）特定した位置における電磁界計測実行の検知が課題となる。（1）に関しては、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背景雑音の時間的な振幅変動に着目した電磁界計測検知手法を提案し、秘密情報を含む電磁界の計測困難化を達成した。

本研究は、暗号モジュールからの漏えい電磁界による秘密情報漏えい評価技術として、機器上での電磁放射による秘密情報漏えい箇所特定手法を提案し、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明らかにすると共に、背景雑音の振幅変化に基づく電磁界計測検知手法を提案することで、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。