先端科学技術研究科　修士論文要旨

所属研究室 （主指導教員）	情報セキュリティ工学 （林　優一　（教授））		
学籍番号	2311067	提出日	令和 7年 1月 22日
学生氏名	大貫　和基		
論文題目	サイドチャネル情報を用いた故障利用解析の高度化に関する研究		

要旨

暗号モジュールに対する故障利用解析は、外乱を用いて暗号処理に一時的な故障を誘発する「故障注入」とその結果得られる誤り出力から秘密鍵を導出する「秘密鍵解析」の2つから成る。秘密鍵解析は特定の条件を満たす誤り出力が得られたことを仮定しているため、故障注入の段階では条件を満たす誤り出力の発生が求められる。これまで前述の条件を満たすために故障注入手法が提案されてきたが、その多くは物理的な侵襲や改変が前提となるため、開封検知や筐体保護機構を備えた機器は脅威の対象外とされてきた。これに対し、暗号モジュール外部から非侵襲に電磁波を印加して故障を誘発する手法が提案され、物理的アクセスが制限される環境でも故障注入が可能となっている。しかし、故障を発生させるタイミングを制御することが難しく、秘密鍵解析に適した誤り出力の取得が困難という課題があった。本研究では、暗号処理中の内部回路の動作情報がサイドチャネル情報として外部に漏えいする点に着目し、故障発生時に生じるサイドチャネル情報の変化を利用して誤り出力を分類する手法を検討する。これにより適用可能な解析手法を拡張し高度な秘密鍵解析が可能となると考えられる。提案手法を用いた実験の結果、故障注入で得られた誤り出力の中から秘密鍵解析に有効なものを選別できること、さらに従来法では適用困難であった解析手法に必要な誤り出力を取得可能になることを明らかにした。