

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	2411079	提出日	令和 8年 1月 19日
学生氏名	金谷 祐輝		
論文題目	サイドチャネル情報を用いた故障感度解析の成立条件評価と鍵復元手法に関する研究		
要旨			
誤り暗号文を必要としない故障感度解析は、冗長化対策を回避できる強力な故障利用解析手法である。一方、故障注入検知時に出力を停止する外乱検出型対策の下では適用が困難となる。しかし、対策下でも故障による内部状態変化は完全には抑制されず、サイドチャネル情報として観測され得る。本研究では、この内部状態変化がサイドチャネル情報に反映されることを前提とした従来の攻撃概念について検討した。当該攻撃概念は理論上鍵復元が可能とされるが、実環境ではノイズや観測誤差により理想的前提が成立しにくく、実行可能性は十分に示されていない。そこで感度推定誤差を含むモデルを導入し、誤差分布と鍵復元成功率の関係から成立条件と限界を体系的に明らかにした。その結果、この攻撃概念には極めて高精度な感度推定が要求され、実環境におけるサイドチャネル解析では実現が容易ではないことを示した。次に、この結果に基づき、正常暗号文の特定バイト値に基づく平文分類により故障影響をバイト単位で分離し、鍵復元を実現する新手法を提案した。本手法は高精度な感度推定を必要としないため、実環境への適用が現実的である。実装実験により分離効果と特定条件下での鍵復元可能性を確認し、提案手法が誤り暗号文の取得を前提とせず出力停止環境でも解析を継続できることを明らかにした。			