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	2211132	提出日	令和 6年 1月 19日
学生氏名	佐藤　太一		
論文題目	複数のリングオシレータを用いた電磁波解析攻撃検知の高精度化に関する研究		

要旨

暗号モジュール外部の配線とプローブ間に生ずる容量結合をリングオシレータ（RO）を用いて計測し、電磁波解析攻撃を検出する手法が提案されている。一方、外来雑音などにより、暗号モジュール内部に電圧変動が生ずる環境においては、ROの電圧依存性からプローブの検出が困難であった。これに対し、本論文では暗号モジュール内部の電圧変動のみに感度を持つ、チップ内に閉じたROを用いて、プローブセンシング用のROの計測結果からチップ内部の電圧変動の影響を除去する手法を提案し、サイドチャネル攻撃が成立する範囲内にプローブが設置された場合も精度良く検知可能であることを示した。