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	2011218	提出日	令和 4年 1月 23日
学生氏名	橋本　律紀		
論文題目	リングオシレータベースの真性乱数生成器に対する周波数注入攻撃耐性評価システムの提案		

要旨

リングオシレータ（RO）ベースの真性乱数生成器（TRNG）に特定の電磁波を照射することで出力の乱数性低下を引き起こす周波数注入攻撃が報告されている。従来研究では、ROの発振周波数の高調波の印加によるTRNGの乱数性低下が示されている。さらに最近の研究では、発振周波数の有理数倍などの比をもつ周波数においてもROのエントロピーが低下することが報告されており、周波数注入攻撃への耐性評価を行う周波数範囲は拡大している。さらに、TRNGの乱数性低下を引き起こすための注入周波数は300 kHz 以下の精度で決定することが求められるため、広い周波数範囲の探索が求められる。そこで、本論文では、攻撃によって出力ビットに生じる周期性の変化を指標として、こうした広範囲の周波数帯から攻撃が成立する周波数を探索可能な攻撃耐性評価システムを提案する。本提案システムを用いた評価の結果、ROの発振周波数の高調波以外の周波数注入においても乱数性低下が発生することが確認され、こうした周波数に対しても耐性を有する設計が必要であることを明らかにした。