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	2111196	提出日	令和 5年 1月 19日
学生氏名	芳賀　陸雄		
論文題目	サイドチャネル攻撃を考慮したRNSを用いた公開鍵暗号実装に関する研究		

要旨

公開鍵暗号方式は長いビット長での剰余乗算が必要であるため，大きい値を小さな値の集合に分割して並列計算が可能なResidue Number System(RNS)表現を用いた実装が乗算器サイズの小面積化と高速化の観点から注目されている．
一方で，暗号実装では性能に加えて実装安全性としてサイドチャネル攻撃対策も考慮する必要があり，演算を上回る消費電力をノイズとして発生させることで演算の消費電力をハイディングするアーキテクチャレベルでの対策法が知られている．ハイディングによる対策では，2種類の演算をそれぞれSignal，Noiseとした時のSignal-to-Noise Ratio(SNR)が大きいほどノイズとして発生させる必要のある消費電力も大きくなることが課題となっている．
本論文では，並列計算が可能なRNS表現を用いた公開鍵暗号方式の実装において，並列数によりSNRが変化することを明らかにし，性能と電力解析攻撃耐性の両立を行う並列数の選択法を示す．