【 4 】

氏　　名	小菅　悠久
学位の種類	博　士（工学）
学位記番号	第　５８１　号
認定課程名	防衛大学校理工学研究科後期課程
学位授与年月日	平成 30 年 3 月 18 日
論文題目	選択平文攻撃及びサイドチャネル攻撃に対するブロック暗号の耐性評価手法
審査担当専門委員	（主査）九州大学教授　竹内　純一
	慶應義塾大学教授　天野　英晴
	電気通信大学教授　阪口　豊

審　査　の　結　果　の　要　旨

情報インフラの発展にともない，暗号技術の重要性は増し続けている．本研究では，大量のデータの処理に向いたブロック暗号に着目し，以下のように三種類の攻撃手法に対する強度の評価を行ったものである．

第一に，最も一般的な攻撃法である選択平文攻撃の 1 つである Integral 攻撃について，効率的な攻撃アルゴリズムを提案している．Integral 攻撃とは，平文集合が与えられたもとで，暗号演算回路のノードのうち Integral 特性が成立するノードの出力を利用して秘密鍵の推定を行う．そのため，Integral 特性をもつノードをいかに効率よく発見する探索アルゴリズムを用いるかが重要である．既知の攻撃法ではノードの探索に平文の長さの指数時間必要であるのに対し，本研究では多項式時間で動作するアルゴリズムを提案し，飛躍的に効率的な攻撃を可能とした．また，これを用いた強度評価の例を示している．

第二に，機器に実装された暗号に対する攻撃手法であるサイドチャネル攻撃について，その安全性を評価するための枠組みであるランダム漏洩モデル(RL (Random Leakage))の提案と，差分バイアス攻撃の一種である DBA-PM を改良した DBA-KE を提案し，それら攻撃法を AES-128 に適用した場合の攻撃耐性を評価した．その結果，DBA-KE による攻撃が防ぐための漏洩データ量に対する条件を導いた．第三に，同様にサイドチャネル攻撃について，SCCA-PM を改良した攻撃法である SCCA-KE を提案し，1 ビットアクセス漏洩モデル(1AL（1-bit Accessed Leakage）モデル）のもとでの評価を行った．その結果，漏洩に基づく攻撃を防ぐことができる中間値の段数等を明らかにした．これにより，SCCA-KE

を防ぐために付加すべき雑音電力の条件を得ることに成功した．

以上要するに，本研究は，暗号強度評価を目的に，選択平文攻撃とサイドチャネル攻撃の新たな手法を提案し，それぞれの手法が従来より強い攻撃手法であることを示すことで，従来より精密な強度評価を実現し，強い暗号アルゴリズムの開発に貢献するものである．よって学術的価値は高く，博士(工学)として合格と判断した．