# 論文の概要

1　申 請 者

防衛大学校　小菅　悠久

2　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

3　論文の概要（博士：400 字～2,000 字程度）

情報インフラの発展にともない，安全な通信環境を保証する暗号技術は重要度を増している．また，IoT 技術等の普及に伴い暗号の用途が多様化しているため，暗号は用途に合わせた安全性や実装を考えて設計，評価する必要がある．目的に応じて様々な暗号が存在するが，大量のデータの暗号化に用いられるブロック暗号に注目する．ブロック暗号は平文を一定の大きさに区切り，鍵を用いて出力をランダム化する関数を繰り返すことで暗号文を出力する．この関数の繰り返し回数を段数とよぶ．

暗号の評価は安全性と実装性に分けられる．安全性の評価では，暗号のアルゴリズムが安全性に関する要件を満たしているかを確認する．安全性評価として一般的な選択平文攻撃に注目し，その 1 つである Integral 攻撃を研究する．Integral 攻撃では暗号化処理の過程で生じる Integral 特性から攻撃可能段数を導出する．攻撃可能段数よりも余分に段数を設定することで，既知及び未知の攻撃への対策となる．本論文では攻撃者に優位な Integral 特性を高速に探索する手法を提案する．

実装性の評価については高速性等とともに，サイドチャネル攻撃耐性が評価される．サイドチャネル攻撃において形式的評価を行う研究がある．形式的評価は未知攻撃への対策となり，サイドチャネル情報のモデル化(漏洩モデル)を行なう．各漏洩モデルにおいて，攻撃が実行困難となる条件である測定回数等のパラメータを理論的に導出する．評価対象においてこのパラメータを用いて対策を行なうことで，未知のサイドチャネル攻撃への対策となる．本論文ではランダム漏洩モデル及び 1 ビットアクセス漏洩モデルに注目し，これらにおいて有効な差分バイアス攻撃及びサイドチャネル Cube 攻撃を研究する．

本論文では上記の 3 種類の攻撃法に対する耐性評価手法を提案する．耐性評価の結果，安全性に関するパラメータを得る．このパラメータを反映することで安全な暗号アルゴリズム及びその実装を設計できる．安全性の評価ではパラメータとして攻撃可能段数を導出し，実装性の評価では攻撃が実行困難となる条件をパラメータとして導出する．なお，本論文の提案手法はブロック暗号の設計・評価のフレームワークの一部となる．このフレームワークが確立されることで，安全性及び実装性の基準を満たすブロック暗号の開発が容易になる．

4　キーワード

「ブロック暗号」，「選択平文攻撃」，「サイドチャネル攻撃」