審査の結果の要旨

論文提出者氏名　　松井　充

本論文は，「Linear Cryptanalysis of Block Ciphers（ブロック暗号の線形解読法）」と題し，個人のプライバシー保護や機密情報保護に用いられる暗号技術について，ブロック暗号の新しい暗号解読手法である線形解読法の提案と，米国標準暗号 DES の世界初の解読実験，ならびにこの線形解読法に対して安全性が保証された，新しい実用的なブロック暗号の提案をおこなっている．論文の構成は「Preliminaries」を含め７章からなる．

第１章は「Preliminaries（序論）」で，本研究の背景を明らかにした上で，ブロック暗号ならびに暗号の安全性の定義について言及し，研究の位置づけについて整理している．さらに本章では，米国標準暗号 DES の成立の背景と，そのアルゴリズムの詳細について記述している．

第２章は「Linear Cryptanalysis of the Data Encryption Standard（DES の線形解読法）」と題し，線形解読法の概念を，DES を具体例として説明している．線形解読法の原理は，複雑な暗号アルゴリズムを線形近似することにより簡易化し，もとのアルゴリズムのかわりにこの簡易化されたアルゴリズムを解読するという着想である．本章では，複数の近似式を重ねることにより得られる新しい近似式の成立確率を簡単に計算する公式（Piling-up Lemma）を証明し，結果として，DES は 56 ビットの鍵の全数探索よりも高速に解読可能であることを示している．

第３章は「The First Experimental Cryptanalysis of the Data Encryption Standard（DES の最初の解読実験）」と題し，計算機による世界で初めての DES 解読実験の詳細を述べている．本章では計算機実験にさきだち，簡易化した DES による解読実験をおこない，この結果から解読効率を見積っている．完全仕様の DES の計算機による解読は 12 台のワークステーションコンピュータによって行われ，50 日間で正しい鍵に到達したことが具体的に報告されている．

第４章は「How to Derive the Best Expression（最良表現の導出方法）」と題し，DES アルゴリズムに対して，もっとも効率の良い線形近似式を探索するアルゴリズムを提案している．一般に与えられたブロック暗号アルゴリズムに対して最良な線形近似式を完全な形で求めることは，計算量的に困難であるが，本章では DES のように小さい乱数表をもつブロック暗号の場合に，最良近似式を現実的な時間で完全に決定するアルゴリズムを示し，さらにこのアルゴリズムを用いて，DES 設計者が，設計当時にすでに差分解読法を知っていたが，線形解読法は知らなかったはずであるという強い証拠を示すことに成功している．

第５章は「Provable Security of Block Ciphers（ブロック暗号の証明可能安全性）」と題し，差分解読法と線形解読法に対して安全性が証明できるさまざまなブロック暗号の

構成原理を提案している．そのひとつは内部関数の位置を変更することによる並列処理性能の向上あり,もうひとつは再帰構造の導入である.さらに不等分分割構造の発明により，暗号設計者はブロック暗号設計の大きな自由度を得ることができること，すなわち，システムで要求されるさまざまなパラメータを組み合わせて，暗号設計ができるようになることが示されている．

第６章は「Design of Block Encryption Algorithm MISTY（ブロック暗号アルゴリズム MISTY の設計)」と題し，差分解読法と線形解読法に対する証明可能安全性をもつ具体的なブロック暗号 MISTY が提案されている．MISTY は第５章で示された，F 関数の新しい位置,再帰構造,不等分分割の３つの新提案をすべて含んだ新しいブロック暗号である．またハードウエアでの小型化・高速化のため，算術演算を用いず，論理演算とテーブルだけでアルゴリズム全体が構成されており，実用的な性能を実現している．

最後に第７章は「Conclusion（結言)」で，本研究の総括を行い，併せて将来展望について述べている．

以上これを要するに，本論文では，安全な暗号設計に必要な暗号評価手法としての暗号解読技術からはじめ，既存の暗号にはない特徴をもつ安全な暗号設計の指針と，具体的な暗号アルゴリズムを示したものであり，その技術は現在第三世代携帯電話の必須標準暗号として世界中で用いられており，電子情報学，特に情報セキュリティ工学上貢献するところが少なくない．

よって本論文は博士（情報理工学）の学位請求論文として合格と認められる．