論文の内容の要旨

論文題目　Linear Cryptanalysis of Block Ciphers
（ブロック暗号の線形解読法）

氏名　松井　充

本論文では、ブロック暗号（block cipher）の新しい暗号解読手法である線形解読法（linear cryptanalysis）の提案と、線形解読法に対して安全性が保証された新しいブロック暗号の提案をおこなう。

第１章では、本論文を通して用いられる用語の説明と、暗号解読の定義づけがおこなわれる。具体的には、本論文では、固定された秘密鍵のもとで平文が連続的に暗号化されている通信路において、平文と暗号の情報から秘密鍵を、秘密鍵の総当り解読よりも少ない計算量で解読するのが、解読者の目標である。またこのような解読を許さないようなブロック暗号を、安全なブロック暗号であると定義する。これはブロック暗号の安全性に関する最も一般的な考え方である。さらに本章では、米国標準暗号 DES（Data Encryption Standard）の成立の背景と、そのアルゴリズムの詳細について図示する。

第２章では、線形解読法の概念を、DES を具体例として説明する。線形解読法の原理は、暗号アルゴリズムを線形近似することにより、複雑なアルゴリズムを簡易化して、もとのアルゴリズムのかわりにこれを解読するというものである。この簡易化されたアルゴリズムは確率的なものなので、解読結果は正しい鍵を示しているとは限らない。しかし、もと

のアルゴリズムと、近似されたアルゴリズムの差は、情報量、すなわち平文と暗号文のペアの数で補われ、解読者に得られた情報量が多ければ多いほど、解読結果の確からしさも向上する。本章ではこのアルゴリズム近似の方法論を、DES の最小の非線形コンポーネントである SBOX からはじめ、アルゴリズム全体に拡大してゆく方向で述べる。ここで複数の近似式を重ねることにより得られる近似式の成立確立を簡単に計算するための方法（Piling-up Lemma）を証明する。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す。

第３章では、第２章の結果を拡張し、計算機による初めての DES 解読実験を行うことが目標である。１６段の DES のうち、中間１４段を近似することにより、ひとつの式から１３ビットの秘密鍵を導出することを目指す。さらにまた同じ確率で成立する式が２種類あるため、合計２６ビットの導出が可能である。計算機実験にさきだち、解読効率を見積もるため、８段に縮小した DES による解読実験をおこない、この結果から、DES は 2 の 43 乗程度の既知平文と対応する暗号文のペアがあれば、８０％以上の確率で解読が成功するとの結果を得た。１６段の 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ー（PA-RISC 99MHz）によって行われ、50 日間で正しい鍵に到達した。

第４章では、DES アルゴリズムに対して、もっとも良い近似式を探索するアルゴリズムを提案する。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近似式を完全な形でもとめることは、現実的には計算量的に困難である。しかし DES のように小さい SBOX をもつブロック暗号の場合は、最良近似式を現実的な時間で完全に決定することができる。本章ではこの２重再帰アルゴリズムを記述する。次にこのアルゴリズムを用いて、DES の 8 個の SBOX の順序を変更した場合に差分解読法ならびに線形解読法に対する強度がどのように変化するかを実験した。この結果、DES の SBOX のならびは、差分解読法に対してほぼ最強のものであることが判明した。このことは DES 設計者が、設計当時にすでに差分解読法を知っていたことを示している。一方線形解読法に対しては、DES の SBOX のならびは非常に弱い部類に属している。すなわち SBOX の順序を変更するだけで、DES は線形解読法に対する暗号強度を増すことができることを示す。

第５章では、差分解読法と線形解読法に対する証明可能安全性を議論する。証明可能安全とは、差分解読法や線形解読法に対する安全性の指標となる、差分確率あるいは線形確率が十分小さいことを数学的に証明することができるブロック暗号をさす。本章では差分解読法と線形解読法に対する証明可能安全性の評価式は完全にたがいに双対的な形で書き下すことができることをしめす。また証明可能安全性をみたすさまざまなブロック暗号の構成原理を提案する。そのひとつは F 関数の位置を変更することにより並列処理性能の向上であり、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を提案する。これら

の構造により、暗号設計者はブロック暗号設計の大きな自由度をえることができる。すなわち、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を示す。

第６章では、差分解読法と線形解読法に対する証明可能安全なブロック暗号 MISTY を提案する。MISTY は第５章で示した、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り、その再帰構造は３階層から構成される。最上位の構成の違いから、MISTY1 と MISTY2 という２つの具体的なアルゴリズムに分類される。MISTY はハードウエアでの小型化、高速化を狙うために算術演算を用いず、論理演算とテーブルだけでアルゴリズム全体が作られている。またテーブルはハードウエアでの小型化のため、論理ゲートの組み合わせで全体が簡単に構成できるように設計を行った。この結果 MISTY は最小６キロゲートでアルゴリズム全体を構成することができる。現在 MISTY の設計技術は以下の標準で採用されており、世界中で幅広く用いられている。

CRYPTREC 推薦暗号	（日本の電子政府のための暗号技術検討委員会）
NESSIE 推薦暗号	（欧州における産学共同暗号評価プロジェクト）
ISO/IEC 18033	（国際標準機構におけるブロック暗号国際標準）

第三世代携帯電話 W-CDMA 必須標準暗号
第二世代携帯電話 GSM 標準暗号