論文の内容の要旨

論文題目： **Design and Analysis of Block Ciphers**

ブロック暗号の設計と解析に関する研究

氏　　名： 盛合　志帆

暗号は、今やインターネットや携帯電話をはじめ、社会生活のインフラストラクチャーに必要不可欠な技術となっている。共通鍵ブロック暗号（以下、ブロック暗号）はその中でも高速な暗号化・復号処理が特徴で、秘匿の機能のみならず、擬似乱数生成やメッセージ認証コードのビルディングブロックとして利用されるなど、重要な役割を担っている。

多くの公開鍵暗号が、素因数分解問題や離散対数問題といった計算量的に困難な問題に基づいて設計され、その安全性について理論的に帰着関係が示されているのに対し、公開鍵暗号の１０００倍、１００００倍もの速度が要求されるブロック暗号については、このような安全性が証明できる設計法は知られていない。よって、ブロック暗号を設計するには、想定されるあらゆる解読法に対する安全性を評価する必要がある。ブロック暗号の設計と解析（強度評価）は車の両輪のような関係で、安全なブロック暗号の設計には、既知の解読法に関する知識と強度評価技術が不可欠となっている。

本論文では、まず、ブロック暗号に対する強度評価において最も重要な解読法、すなわち差分解読法、線形解読法、高階差分攻撃法、補間攻撃法に対する強度評価手法の改良について述べる。

差分解読法及び線形解読法については、これらの解読法に対する強度評価指標をより効率的に計算することが可能になり、現実的な時間で強度評価が行なえるようになった。例えば、これまで数ヶ月必要であった評価計算を 3 日未満で実行可能となった。

高階差分攻撃法及び補間攻撃法については、これらの解読法に対する強度評価指標をよ

り正確に計算することが可能になり、より厳密に安全性を評価できるようになった。例えば、従来の評価法では、解読には鍵の全数探索よりも多い計算量が必要であるため安全であると予想されていた暗号が、本改良により、実際はそれよりも少ない計算量で解読可能であることが示された。

本論文では、また、このような強度評価技術をもとに設計した 128 ビットブロック暗号 Camellia について述べる。特に安全性と性能を両立させるための設計指針と強度評価結果について述べている。

本論文の主な成果は以下の通りである。

最良線形特性及び最良差分特性探索の改良：線形解読法及び差分解読法を用いてブロック暗号を解読するのに必要な計算量の下限を見積もるために、最良線形特性及び最良差分特性を導出する必要がある。本論文では、最良線形特性や最良差分特性を探索するアルゴリズムを改良する方法を示した。本改良では、各段でとりうる線形確率及び差分確率の値の組を探索パターンとして導入し、前処理により不必要な探索候補を効果的に枝刈りすることで探索計算量の削減が可能となった。従来、松井によって示されていた探索アルゴリズムではＦＥＡＬ暗号の８段最良線形特性を求めるのに３ヶ月近く必要であることが試算されていたが、改良アルゴリズムでは３日以内で求めることができるようになった。さらに、この探索により計算されたＦＥＡＬの最大線形特性確率は、従来 Biham らにより示されていた予測値より大きいこと、ＦＥＡＬの仕様となっている 32 段では線形解読法に必要な計算量は鍵の全数探索よりも少なく、線形解読法に対し十分な安全性をもつことが示された。

高階差分攻撃法の解読計算量削減：ブロック暗号に対する代数的攻撃法の一つとして高階差分攻撃が知られているが、本論文では従来よりも解読計算量を削減させる新しい高階差分攻撃法を提案する。Jakobsen と Knudsen によって示された高階差分攻撃では、攻撃対象である最終段の鍵を求めるのに、全ての鍵候補に対して全数探索を行っていた。しかし、高階差分攻撃が可能となる条件下では、最終段の鍵に関する代数方程式を立て、これを一次方程式に変換して現実的な計算量で解くことができることに注目した。これにより大幅に解読計算量が削減できる。この攻撃法をカナダ政府標準暗号として有名なＣＡＳＴ暗号ファミリーの一つに適用したところ、2^{17} 組の選択平文とそれに対応する暗号文を用いて 2^{25} 回以下のラウンド関数の計算に要する計算量で解読できることが分かった。

補間攻撃法の解読計算量削減：補間攻撃法は、ラグランジェ補間公式を利用して暗号アルゴリズムを復元する代数的攻撃法の一つである。本論文では補間攻撃法に必要な平文-暗

号文数及び計算量の上限をより厳密に与える強度評価方法を提案する。補間攻撃法では、平文と暗号文の間に成り立つ多項式表現や有理式表現等の代数関係式の項数が強度評価指標となることが知られている。しかし、従来の評価方法ではこの多項式表現や有理式表現の次数をもとにして項数を評価していたため、補間攻撃に必要な計算量を過大評価してしまう傾向にあった。本論文では、数式処理システムを用いることによりこの問題を解決した。すなわち、実際の多項式表現や有理式表現に含まれる項数を厳密に評価し、かつ攻撃に有利な少ない項数をもつ多項式表現を選択することが可能となった。

128 ビットブロック暗号 *Camellia* の設計：Camellia は高い安全性と性能を兼ね備えることを目標に設計された 128 ビットブロック暗号である。安全性に関しては、これまでに知られているあらゆる攻撃法に対する十分な安全性と、将来の解読法の進歩に耐えるよう十分なマージンをもつよう設計を行った。性能に関しては、ソフトウェア実装・ハードウェア実装の両方に適し、低コストのＩＣカードから高速ネットワークのサーバーまで対応できる柔軟性を目指した。現在のところ、ソフトウェアでの最適化実装では Pentium III(1.13GHz)上で 471Mbps の暗号化速度、ハードウェア小型化実装では 0.18μm CMOS ASIC ライブラリを用いて 6.26K ゲートという世界最小クラスを実現している。Camellia は 2000 年にＮＴＴと三菱電機で共同開発されて以来、現在までに、日本電子政府推奨暗号リスト案に採用されているほか、ＩＳＯ／ＩＥＣ、ＥＵ　ＮＥＳＳＩＥプロジェクト、ＩＥＴＦ、Ｗ３Ｃ、ＴＶ－Ａｎｙｔｉｍｅ　Ｆｏｒｕｍ等の国際標準機関において規格化が検討されている。