審査の結果の要旨

論文提出者氏名　　盛合 志帆

本論文は「Design and Analysis of Block Ciphers (ブロック暗号の設計と解析に関する研究)」と題し、①安全な共通鍵ブロック暗号を設計する上で不可欠な解析・強度評価技術の改良と、②高い安全性と性能を兼ね備えた共通鍵ブロック暗号の設計法について検討している。安全な共通鍵ブロック暗号を設計するために、既知の暗号解読法に対する定量的な強度(安全性)を厳密かつ効率的に評価することが不可欠となっている。本論文では、代表的な暗号解読法に対する強度評価手法を改良するのに有効ないくつかの手法を示すとともに、これらの解析手法をもとに設計した新しい共通鍵ブロック暗号を提案している。本論文は「Introduction」を含め7章からなり、第2章から第4章までが Part I「ブロック暗号の解析」、第5章が Part II「ブロック暗号の設計」という構成となっている。

第1章は「Introduction(序論)」で、本研究の動機となる共通鍵ブロック暗号の動向について整理し、本研究の対象である共通鍵ブロック暗号とその代表的な解読法について述べている。

第2章は「Improving the Search Algorithm for the Best Linear Expression(最良線形特性探索アルゴリズムの改良)」と題し、ブロック暗号に対する最も汎用的かつ強力な攻撃法である、線形解読法及び差分解読法に対する強度指標を計算するアルゴリズムの改良手法を示している。このアルゴリズムは最大線形(差分)特性確率をもつ候補を探索する最適化問題であるが、事前処理により探索不要な候補を効果的に枝刈りできる手法を示した。これにより探索計算量は大幅に削減され、実際にFEAL暗号の強度評価に適用した事例では、従来アルゴリズムでは3ヶ月近く必要であった計算を3日未満で計算可能としている。

第3章は「Improved Higher Order Differential Attack(高階差分攻撃の改良)」と題し、ブロック暗号に対する代数的攻撃法の一つである高階差分攻撃の解読計算量を削減させる手法を提案している。従来法では全ての鍵候補に対して全数探索を行っていた部分を、鍵に関するブール多項式の連立方程式を立て、これを連立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。これにより高階差分攻撃に必要な解読計算量は大幅に削減され、強度指標を見直す必要が示された。一例として、カナダ政府標準暗号であるCAST暗号ファミリーの一つが現実的な計算量で解読できることが示された。

第4章は「Efficient Interpolation Attack(効率的な補間攻撃法)」と題し、ラグランジュ補間に基づく代数的攻撃である、補間攻撃法に対する強度指標の厳密な評価法を示している。補間攻撃法では、平文と暗号文の間に成り立つ代数関係式に含まれる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代数関係式の次数をもとにして項数を評価していたため、解読計算量を過大評価してしまう場合があるという問題点があった。本論文では、数

式処理システムを用いて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することにより、この問題を解決している。

第5章は「Design of Camellia: the 128-bit Block Cipher (128 ビットブロック暗号 Camellia)」と題し、高い安全性と性能を兼ね備えた 128 ビットブロック暗号 Camellia(カメリア)を提案している。安全性に関しては、これまでに知られている暗号解読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十分なマージンをもつよう設計されている。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まで対応できる柔軟性を目指している。Camellia は現在までに、CRYPTREC(暗号技術評価委員会)による評価に基づき、電子政府推奨暗号として認定されたほか、EU の暗号評価プロジェクト NESSIE でも、米国政府標準暗号 AES と並ぶ推奨暗号として高い評価を受けている。

最後に第7章は「Conclusion (結論)」で、本研究で得られた成果をまとめている。

以上これを要するに、本論文は、共通鍵ブロック暗号の解析と設計に関する体系的な研究をなしており、共通鍵ブロック暗号の強度評価技術に関して世界的にも高いレベルの成果を含み、かつ安全な共通鍵ブロック暗号の設計技術の進歩に貢献したという点で、電子情報工学、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(工学)の学位請求論文として合格と認められる。