審査の結果の要旨

論文提出者氏名　　杉田　誠

本論文は「Security Evaluation of Cryptographic Algorithms by Statistical and Algebraic Methods（統計的及び代数的手法に基づく暗号アルゴリズムの安全性評価）」と題し，安全な暗号アルゴリズムを構成する上で不可欠な安全性評価手法に関し，理論的評価手法として代表的な統計的手法と代数的手法の二つについて論じたものである．安全な暗号アルゴリズムを構成する上で理論的評価手法は必須であるが，実際に暗号アルゴリズムを設計する場合には，さらに，この安全性評価手法に対して安全に構成するための設計指針を立てることが重要となる．本論文は，これらの問題に対し，有効な解決策を示したものであり，「Introduction」を含め5章からなる．

第1章は「Introduction（序論）」で，本研究の背景を明らかにした上で，研究の動機と目的について言及し，研究の位置付けについて整理している．

第2章は「Security analysis of block ciphers（ブロック暗号の安全性）」と題して，ブロック暗号 Camellia の打切り差分解読法，不能差分解読法に対する安全性評価を行った．このブロック暗号 Camellia に対して Matrix-method という打切り差分確率の計算方法を新たに提案し，この手法と Camellia についての固有の性質とを融合して，FL 関数と呼ばれる部分を削除し簡略化した9段 Camellia について打切り差分と呼ばれる計測値に統計的偏りがあることを示した．さらに7段で不能差分についても統計的偏りを発見した．

第3章は「Security analysis of polynomial based cryptographic algorithms by algebraic attack – Relation between the XL algorithm and Grobner Basis Algorithms（多変数多項式暗号アルゴリズムの代数的攻撃による安全性解析 – XL 法とグレブナー基底法の関係」と題し，最近 Courtois らが提案し話題となった XL 法と従来から知られていたグレブナー基底法との関係を明らかにしている．まず，XL 法が扱う連立方程式のクラスに対し，これを解くことが既約グレブナー基底を計算することと等価であることを示し，XL 法が実は既知の高速グレブナー基底計算法 F4を冗長にしたものに過ぎないことを証明した．さらに，暗号学的に重要な GF(2)上のグレブナー基底計算プログラムの世界最高速実装を実現した．また，このプログラムをグリッドコンピュータ上にも実装して Toyocrypt というストリーム暗号の世界初の解読に成功した．

第4章は「Security analysis of hash function – Finding new differential patterns of SHA-1 and improvement of Wang's message modification technique（ハッシュ関数の安全性解析 – SHA-1 の新しい差分パターンの発見と Wang のメッセージ修正手法の改良」と題し，最近中国の Wang によって攻撃が発表され，暗号学会のみならず情報セキュリティの世界で大問題となっているハッシュ関数 SHA-1 の解読法の技術的詳細について解析した．従来 Wang の衝突発見法の

概略については明らかにされているものの，解析に用いる差分パスの発見方法，メッセージ修正手法と呼ばれる衝突発見確率を劇的に向上させる技術の詳細は明らかにされていなかった．ここでは2つの有効な差分パスを組み合わせることによってさらに有効な差分パスを構成する手法について提案し，この方法によりWang の差分パスを含む有効な差分パスが発見可能であることを示した．またメッセージ修正手法が実質的にグレブナー基底計算に帰着することを示した．さらに基底計算における項の消去順序に工夫を加えることで，代数的手法に基づくメッセージ修正に成功し，その技術的詳細を世界で初めて明らかにした．

最後に第5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，本論文は，Camellia，多変数多項式暗号，SHA-1など暗号アルゴリズムに対する理論的安全性評価手法を提案するとともに，安全な暗号アルゴリズムの設計指針を明示したものであり，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．