論文の内容の要旨

論文題目　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）

氏　名　杉田　誠

様々な暗号アルゴリズムに対する安全性評価手法を提案する。従来、暗号の安全性評価は限られた専門家以外には実行不可能であったが、本提案手法により専門家以外でも容易に安全性評価を行うことを可能にした。更に非専門家が新たに安全な暗号を設計するための設計手法も与えた。また提案手法の有効性を示すため、従来広く知られているアルゴリズムの安全性評価を行い、その有効性を実証した。

対称鍵暗号やハッシュ関数には大きく分けて、次の２つのクラスの解読法が知られている。１つは差分解読法、線形解読法、トランケイテッド差分解読法、不能差分解読法に代表される統計的手法に基づく解読法であり、もう１つは XL、XSL、グレブナー解読法に代表される代数的解読法である。ここで差分解読法は１９９１年に Biham, Shamir により提案された解読法であり、線形解読法は三菱電機の松井氏により１９９４年に提案された解読法である。差分解読法については選択平文攻撃（解読者に都合のよい平文を自由に選んだ後に暗号に入力し、得られた暗号文と元の平文のペアを複数利用して鍵を推定する解読法）で、線形解読法については既知平文攻撃（既知の平文を暗号に入力し、得られた暗号文と平文のペアを複数利用して鍵を推定する解読法）であり、共に DES（従来の米国標準暗号）の解読に成功し、暗号解読における歴史的な成果とされている。またグレブナー基底アルゴリズムは１９７９年に Buchberger によって提案された連立方程式の一般的な計算アルゴリズムであり、XL、XSL アルゴリズムはその改良アルゴリズムとしてそれぞれ２０００年と２００２年にフランスの Courtois らにより提案された解読法である。XSL により現在世界標準暗号となりつつある AES(Advanced Encryption Standard) が解読可能である、という主張が２００２年になされ、暗号研究者以外にも世界的な注目を集めていた。

本論文ではこれらの解読法を現在世界で用いられている様々な暗号に適用し、その有効性を検証した。特に世界的に広く知られているブロック暗号 Camellia, E2, AES の差分解読法、トランケイテッド差分解読法、不能差分解読による暗号解析の手法を提案し、それら解読法に対して安全な暗号を設計するための設計手法も提案した。また XL, XSL とグレブナー基底アルゴリズムの関係について明らかにし、XSL が実はグレブナー基底アルゴリズムの一部であり、全てがグレブナー基底計算帰着しているため、この方法により AES を解読するのは困難であることを明らかにした。最後に統計的手法と代数的手法を組み合わせることにより、近年解読法が発表され社会化している SHA-1 の差分解読法による解析も行い、衝突計算の詳細を世界で初めて明らかにした。

Chapter 2 ではブロック暗号 Camellia のトランケイテッド差分解読法、不能差分解読法に対する安全性評価を行った。ブロック暗号 Camellia は NTT と三菱電機により提案されたブロック暗号で、全ての暗号解読法に対して安全性を保証可能な暗号として提案された。Camellia は１２８ビットブロックサイズを入力とし、鍵長については１２８ビットと２５６ビットの可変であり AES と同様の仕様となっている。また全ての演算がワード単位の演算によって構成されている。Camellia の主要な構造は、Feistel 構造と呼ばれる従来の世界標準であった DES 等で用いられた段構造を踏襲し、各段中のラウンド関数と呼ばれる関数として、バイト単位の表置換（Substitution）とバイト単位の線形変換（Permutation）を合成した SP の２層構造を採用している。Camellia は現在 ISO/IEC JTC 1/SC27 で世界標準として採用されており、他にも NESSIE (New European Schemes for Signature, Integrity and Encryption), CRYPTREC (CRYPTography Research & Evaluation Committee of Japan), ISO, IETF, SSL 等で標準として採用されている。ブロック暗号 Camellia は AES 公募に NTT によって応募され不採用となった E2 の改良版であり、大きな変更点はラウンド関数が従来 SPS（Substitution, Permutation, Substitution）の３層構造であったものを SP（Substitution, Permutation）構造に変更した点にあり、更に６段ごとに挿入されている FL 関数により安全性が高められている。

このブロック暗号 Camellia に対して Matrix-method というトランケイテッド差分確率の計算方法を新たに提案し、この手法と Camellia について固有の性質とを融合して、FL 関数なしの場合に９段 Camellia でのトランケイテッド差分と呼ばれる統計的偏りがあることを示した。さらに７段で不能差分と呼ばれる別種の統計的偏りを発見した。従来トランケイテッド差分解読法においては６段、不能差分解読法においては５段までしか統計的偏りが発見されておらず、以後現在に至るまでにこれを上回る段数の統計的偏りは発見されていない。また実際の Camellia においては FL 関数があるため解読が不可能であることも示し、ブロック暗号 Camellia の安全性を示す根拠として世界中の標準化で本成果が参照されている。

Chapter 3 ではXLアルゴリズムと従来から知られていたグレブナー基底アルゴリズムとの関係を明らかにした。ブロック暗号AESは線形解読法、差分解読法の進展に伴うDESの安全性低下に伴い、米国NIST(National Institute of Standards and Technology)により新規に公募され、以後数年間に渡り世界中の研究者が参加した公開審査の後に制定されたブロック暗号である。AESは表置換(Substitution)とバイト単位の(GF(2^8)上の)線形変換(Permutation)が交互に重なったSPN(Substitusion and Permutation Network)と呼ばれる構造から成り立っており、各段が代数的に簡略な構造から成り立っているという特徴がある。Chapter 3 では、XLが扱っていた連立方程式のクラスに対し、連立方程式を解くことが既約グレブナー基底を計算することと一致することを証明した。さらにXLアルゴリズムが実はグレブナー基底アルゴリズムであり、既知の高速グレブナー基底計算アルゴリズムであるF4 を冗長にしたものに過ぎないことも証明した。

従来 XL アルゴリズムは完全なグレブナー基底アルゴリズムを計算する必要がないために高速であるという主張がなされていた。しかし Chapter 3 の結果は、XL アルゴリズムが与えられた連立方程式に対応する既約グレブナー基底を F4 アルゴリズムよりも冗長なアルゴリズムで計算しているに過ぎないことから、予想されていたよりも非効率的であることを示している。

さらにこれら理論的な検討に加え、世界最速のグレブナー基底計算プログラムである Magma を超える世界最高速実装に、暗号学的に重要である GF(2)上で成功した。さらに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。ここで Toyocrypt とは２０００年に公募された電子政府推奨暗号に応募された暗号の一つで、結局不採用となったものの、その後世界的な学会で代数的解読法を用いた理論的な解読法が発表され世界的に有名になったストリーム暗号である。

Chapter4 では、近年中国の Wang によって解読法が発表され、暗号学会のみならず PKI などの認証の世界でも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。

ハッシュ関数SHA-1 は最長 2^{64}のメッセージから１６０ビットのハッシュ値を出力する関数でPKI認証などあらゆる場面で最も広く用いられているハッシュ関数である。SHA-1 は米国NISTにより１９９５年にFederal Information Processing Standard (FIPS)という政府調達基準として標準化されている。

SHA-1 は Merkle/Dangard と呼ばれるメッセージ列に対して連鎖的にハッシュ値を計算する構造を有し、データ構造としては chaining value と呼ばれる１６０ビットのレジスタビットと５１２ビットの message block から構成され、chaining value の初期値 IV は固定されている。

具体的な処理としては、１６×３２ビットのメッセージから８０×３２ビットの拡大メッセージを線形変換により生成し、８０個の拡大メッセージを順々に chaining value に作用させていき、最後に得られた chaining condition が出力ハッシュ値となる。

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、Message Modification Technique 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等、大部分の詳細が明らかにされていなかった。Chapter4 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 の差分パスを含むクラスの有効な差分パスが発見可能であることを示した。また Message Modification Technique 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。さらに基底計算に必要な elimination order と呼ばれる変数の順序を導入することで、代数的手法に基づく Message Modification に成功し、その技術的詳細を世界で初めて明らかにした。さらに Wang による Sufficient Condition に Message Modification のための条件を追加した Advanced Sufficient Condition とうい条件を新規に導入し、衝突発見手法の視覚化に成功した。本手法を Wang により衝突パターンが実際に

発表されている５８段の簡略版の SHA-1 について実際にコンピュータ実装し、全ての Message Condition と 1-22 段の Chaining Value Condition 全てを満たすように Message Modification することに実際に成功し、その有効性を実証した。