P-83

情報通信技術

AES 暗号と CIPHERUNICORN-A の S ボックスの比較

TECHNOLOGY SHOWCASE

■ はじめに

現代の情報化社会においては、インターネットを介した膨大なデータの送受信が日常的に行われており、通信の安全性を確保するための暗号技術の重要性が一層高まっている。特に、共通鍵暗号方式は高速かつ効率的な暗号化を可能にすることから、実用システムにおいて広く用いられている。代表的な共通鍵暗号として、2001 年にアメリカ国立標準技術研究所(NIST)によって次世代標準暗号方式として採用された AES(Advanced Encryption Standard)が挙げられる。AES は、Rijndael 暗号をもとに設計され、高い安全性と計算効率を兼ね備えた暗号として現在も広く利用されている。一方で、暗号解読技術の進展にともない、新たな暗号方式の設計と評価が継続的に求められている。CIPHERUNICORN-A は、日本電気株式会社(NEC)によって設計された共通鍵ブロック暗号であり、線形解読法や差分解読法に対して強い耐性を持つよう設計されている。そのラウンド関数には、撹拌の偏りを抑える工夫が施されており、2000 年当時には AES 最終候補に挙げられた 5 つの暗号方式よりも高い強度を有すると評価された。本研究では、この CIPHERUNICORN-A に用いられている S-box に着目し、その構造的特徴や安全性の評価を行う。特に、既存の AES 暗号に関する安全性評価研究で得られた知見を踏まえ、CIPHERUNICORN-A の S-box が持つ性質を解析することで、暗号方式の設計指針や今後の安全性評価の一助とすることを目的とする。

■ 活動内容

本研究では、共通鍵暗号におけるS-boxの特性に注目し、AES暗号とCIPHERUNICORN-AのS-boxを比較・分析した。暗号の安全性を評価するうえで重要となる「偏りの少ない出力分布」を検証し、S-box構造が暗号文の拡散性に与える影響を調べた。

1. 安全性の評価

偏りの評価にはカイ二乗検定を用いた。特定の平文集合を暗号化し、得られた暗号文を4bit単位で16進数表記に変換して各値(0〜F)の出現回数を計測した。観測度数と期待度数の差からχ^2値を算出し、自由度15・有意水準0.05のもとで棄却限界域を24.97と設定した。また、各S-boxを置換としてサイクル分解し、サイクル長や固定点の分布を解析することで、構造的な特徴を比較した。

2. 結果及び考察

	AES	S0	S1	S2	S3
Round1	52992.00	52992.00	52992.00	52992.00	52992.00
Round2	0.0	0.0	0.0	0.0	0.0
Round3	18.94	18.82	14.31	13.06	10.05
Round4	29.43	5.80	10.05	24.5	8.62
Round5	14.62	13.07	11.58	18.6	9.02
Round6	8.76	4.18	22.59	12.44	19.71
Round7	5.20	11.61	8.05	20.43	17.40
Round8	11.14	19.68	10.15	19.80	9.12
Round9	27.98	16.89	10.75	14.02	22.64
Round10	17.47	18.34	18.18	29.00	9.29

図1

実験の結果、平文を128bit(8bit×16個)とし、そのうち先頭の1箇所のみを00〜FFに変化させ、残りの15箇所をすべて00とした256通りの平文を生成し、暗号化鍵をすべて00で固定した場合、図1に示すように、全てのS-boxにおいてRound 2の時点で出力値が0となることが確認された。このことから、S-box単体では十分な拡散特性が得られないことが示唆された。さらに、AESとCIPHERUNICORN-AのS-box間でχ^2値に顕著な差は見られず、暗号全体の乱数性はS-box以外の変換との組み合わせによって実現されていると考えられる。

これらの結果から、暗号設計においてはS-boxの性能のみならず、他の構成要素との相互作用が安全性確保において重要な役割を果たすことが示された。

■ 関連情報等(特許関係、施設)

本研究はお茶の水女子大学人間文化創成研究科で行われたものである。

参考文献

[1] Johannes A.Buchman, “Introduction to cryptography”
[2] 日本電気株式会社,”暗号技術仕様書 CIPHERUNICORN-A”
[3] 古川早紀 “AES 暗号の MixColumn 変換が安全性に及ぼす影響”令和 4 年度卒業研究要項 2023

代表発表者 **丸山 真穂(まるやま まほ)**
所 属 **お茶の水女子大学大学院 人間文化創成科学研究科 理学専攻数学コース**
問合せ先 **〒112-8610 東京都文京区大塚 2-1-1**
TEL:070-3163-7579
E-mails:maruyamamaho.univ@gmail.com

■キーワード: (1)暗号理論
(2)共通鍵暗号
■共同研究者: 萩田真理子
(お茶の水女子大学)