AES 暗号と CIPHERUNICORN-A の S ボックスの比較

P83

丸山真穂

お茶の水女子大学　修士1年

研究の目的

現代の情報化社会では,インターネットを通じた膨大なデータのやりとりが日常化しており,高い安全性を持つ暗号技術の重要性がますます高まっている.これまでの研究室では,AES暗号の安全性評価に関する研究が行われてきた.
本研究では,CRYPTREC評価委員会の推奨候補暗号リストに掲載されているCIPHERUNICORN-AのS-boxを扱う.AESのS-boxと比較し,カイ二乗検定を用いて安全性を評価した.

AES

DES の安全性の低下にともない,アメリカ国立標準技術研究所によって DES に代わる新たな暗号方式としてRijndael 暗号がAES として選定された. 2001 年にアメリカ合衆国の標準規格 AES(Advanced Encryption Standard) として採用され, 世界中で広く使用されている.

入力　平文(*state*)《128bit》
暗号化鍵(*key*)《128bit/192bit/256bit》

出力　暗号文(*cipher*) 《128bit》

アルゴリズム

1. 暗号化鍵(*key*)を*KeyExpansion*関数を用いて11個に拡張する.
2. 平文(*state*)に対して*AddRoundKey*変換を施す.
3. 平文(*state*)に対して*SubByte*変換, *ShiftRow*変換, *MixColumn*変換, *AddRoundKey*変換を1サイクルとして1Roundから9Roundまで繰り返し行う.
4. 最終Roundのみ平文(*state*)に対して*SubByte*変換, *ShiftRow*変換, *AddRoundKey*変換を行う.

CHIPHERUNICORN-A

日本電気株式会社によって設計された共通鍵暗号. 線形解読法と差分解読法による解読を防ぐため, ラウンド関数において, 撹拌の偏りが現れないように設計されている.

入力　平文(*state*)《128bit》
暗号化鍵(*key*)《128bit/192bit/256bit》

出力　暗号文(*cipher*) 《128bit》

データブロック長 128 ビット、秘密鍵長 128 ビット，192 ビット，256 ビットのいずれかを利用できる Feistel 構造の暗号. ラウンド数は 16 段，初期/終期処理では拡大鍵の加算/減算を行う.

本流

1. 平文1ブロックを入力する.初期処理として拡大鍵加算をおこなう.
2. A3関数,定数乗算,Tn関数によって撹拌する.

一時鍵生成部

1. 拡大鍵と入力データを加算
2. 定数乗算,Tn関数を通過後生成した一時鍵を取り出す

検証方法

CIPHERUNICORN-A の4つのS-boxをAESのS-boxに置換して生成した平文を暗号化する.各暗号文について8bitをひとかたまり(16進数2桁)と見て, 振り分ける箱を256個(00～FF)に設定する. 平文 128bit を $8bit \times 16$ 個とし，この 16 個の中一カ所だけに各サイクルの互換となる値を入れ, それ以外は全て 00 として、16 通りの平文を生成する. 暗号化鍵は 00 のみで生成する. カイ二乗検定を行い,それぞれのカイ二乗値を比較する.

カイ二乗検定

偏りの度合いを確かめるために，カイ二乗検定を用いる. 観測度数と期待度数の差が大きいほど χ^2 値は大きくなるため，χ^2 値が大きいほど偏りが大きいと言える.

観測度数 暗号化した暗号文において，各条件で設定した箱に入る元の個数.

期待度数 設定した箱の元が等確率で現れた場合のそれぞれの個数.

$$\chi^2 = \sum_{i=0}^{m} \frac{(O_i - E_i)^2}{E_i}$$

O_i 観測度数

E_i 期待度数

m 事象数

今回は、ランダムに出現している場合と比較し、実際の暗号文が偏る確率が5%以下であるか否かを判断することとする. よって，自由度 15，有意水準 0.05 より，カイ二乗検定棄却限界域は 24.97 以下と設定する.

概要

暗号の安全性を考える上で,『偏りのある平文の集合が偏りの少ない暗号文の集合へ変換されること』が一つの焦点となる.特定の平文集合を暗号化し，出力された暗号文を 4bit ごとに分割して 16 進数で表記したものの，0 から F の出現回数をそれぞれ数える.そのうちある数字の出現回数が極端に多くなっているとき, 偏りがあるといえる. AES,CHIPHERUNICORN-A の各 S ボックスを置換とみなし, サイクル分解する. サイクル長が均一で, 固定点や短いサイクルが少ない S ボックスは, より均一な出力を生成し, 攻撃を困難にするのか比較する.

結果

平文の先頭に 00～FF の全通りを入力し, それ以外をすべて 0 とした場合、全ての S-box において Round 2 の時点で値が 0 になるという結果が得られた. また, 各 S-box において互換となる値に着目した場合でも, 最終ラウンドでのカイ二乗値に顕著な差は見られなかった. このことから,S-box 単体では十分な拡散特性が実現されず, その他の変換との組み合わせによって初めて効果的な混合が実現されていると考えられる. この結果は,S-box を含む暗号全体の設計における相互作用の重要性を示唆している.

今後の展望

今後は，CIPHERUNICORN-Aの各変換が暗号全体に与える影響や，S-boxに互換が含まれる場合に乱数性へ与える影響を中心に分析を進める. また，カイ二乗値が一度0になることで暗号全体へ与える影響を考察するとともに, CIPHERUNICORN-Aのプログラムを実装し, その特性を詳細に調査する予定である.

参考文献

[1] Johannes A. Buchmann, *Introduction to Cryptography*, Springer.

[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.