**SCIS 2022** 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

# Fibonacci 数列を利用した S-box 及び転置関数による AES への有効性調査
# A Study on the behavior of functions using Fibonaacci for AES

阿部友美 *　　五十嵐保隆 *
Tomomi Abe　　Yasutaka Igarashi

**キーワード**　AES、Fibonacci 数列、Integral 特性、差分特性、MILP

## 1　はじめに

2000 年に Rijndael が NIST により AES として選定されて以来、様々な攻撃や改良が提案されている [1]。その中で、Kamsiah Mohamed らにより、Fibonacci 数列を利用した S-box と Fibonacci Spiral を利用した転置関数が提案され、AES の構成要素として有効であると報告されている [2, 3]。しかし、ショートカット攻撃耐性について評価をされていなかったため、本稿では MILP(混合整数線形計画法) を用いて Integral 特性及び差分特性を調査する。

## 2　Mohamed らに提案された S-box 及び転置関数

提案された S-box は Fibobacci 数 $F_n$、$n$ の素因数 $P$、$P$ の重複度で最大のべき数 $a$ を使用する。アフィン変換後、定数 $C = 0x63$、$F_n$、$P^a$ を排他的論理和したものを出力する。提案された転置関数は、図 1 に示すように Fibonacci Spiral を利用した転置順序になる。

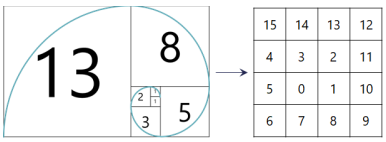


図 1: fibonacci spiral を利用した転置関数

## 3　MILP を利用した特性調査

Integral 攻撃は 2002 年に Knudsen らによって提案され、差分攻撃は 1990 年に Biham らによって提案された暗号解読手法である。また近年、MILP を用いて特性の伝搬を調査する手法が提案されている。特性が現れるラウンド数が多い程、鍵探索の効率が向上するため、弱い暗号となる。

* 東京理科大学大学院　理工学研究科　電気工学専攻 Dept. of Electrical Engineering, Graduate School of Science and Technology, Tokyo University of Science

## 4　調査結果

従来の AES、AES に提案された転置関数を適用させたもの、AES に提案された S-box を適用させたものの 3 通りの特性探索を行った。Integral 特性の結果を表 1 に示す。 4 階差分において、転置関数適用型 AES は特性

表 1: Integral 特性が現れた最大ラウンド数

| 入力 | 従来 AES | 転置関数適用 | S-box 適用 |
|---|---|---|---|
| 4 階差分 | 2 | 4 | 2 |
| 8 階差分 | 4 | 4 | 2 |
| 12 階差分 | 4 | 4 | 3 |

が悪化した。8 階、12 階差分において S-box 適用型 AES は最大ラウンド数が小さくなった。また、差分特性については、3 ラウンドで従来の AES はアクティブな S-box が 16 個となり、差分特性確率が $2^{-126}$ に対し、提案転置関数を適用した AES はアクティブな S-box が 9 個、差分特性確率が $2^{-56}$ となった。

## 5　まとめ

8 階、12 階差分において提案された S-box は従来の AES より特性を改善し、有効に機能することがわかった。一方で、提案された転置関数は従来の shiftrows より有効に機能していない。しかし、mixcolumn における積の順序を交換して調査したところ、1 ラウンドだけ特性が向上したことから、提案された転置関数は AES 以外のブロック暗号ではショートカット攻撃耐性に有効となる可能性がある。

## 参考文献

[1] Jie Cui,Liusheng Huang,Hong Zhong, Chinchen Chang,Wei Yang,“AN IMPROVED AES S-BOX AND ITS PERFORMANCE ANALYSIS ,”International Journal of Innovative Computing, Information and Control Volume 7, Number 5(A), May 2011 pp. 2291–2302

[2] Kamsiah Mohamed,Fakariah Hani Hj. Mohd Ali,Suriyani Ariffin,“A New Design of Permutation Function Using Spiral Fibonacci in Block Cipher,”International Journal of Advanced Trends in Computer Science and Engineering,volume9,No.1.3,2020,pp445-450

[3] Kamsiah Mohamed,Fakariah Hani Hj. Mohd Ali,Suriyani Ariffin,Nur Hafiza Zakaria,Mohd Nazran Mohammed Pauzi“An Improved AES S-box Based on Fibonacci Numbers and Prime Factor,”International Journal of Network Security, Vol.20, No.6, PP.1206-1214, Nov. 2018

[4] L. Knudsen , D. Wagner,“Integral cryptanalysis,” FSE 2002. LNCS, vol. 2365, pp. 112–127. Springer, Heidelberg, 2002.