Copyright© 2022 The Institute of Electronics,
Information and Communication Engineers

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

# 軽量ブロック暗号 DLBCA に対する MILP を用いた Integral 攻撃
# Integral attack on lightweight block cipher DLBCA using MILP

廣見　紗妃 *　　五十嵐　保隆 †
Saki Hiromi　　Yasutaka Igarashi

**キーワード**　軽量ブロック暗号, DLBCA, Integral 攻撃, MILP

## あらまし

DLBCA は 2017 年に S.AlDabbagh によって提案された Feistel 構造を持つ軽量ブロック暗号である。鍵長 80 ビット、ブロック長 32 ビット、段鍵 32 ビット、段数 15 段である。[1]

提案論文には差分攻撃については脅威を示さないと記載されていた。しかし、Integral 攻撃については評価が記載されておらず、第三者による安全性評価も行われていない。そこで本稿では、Integral 特性を MILP (Mixed Integer Linear Programming)[2]を利用して探索し、得られた特性を用いて、8 段に対しての鍵回復に必要な平文数、計算量を算出した。

## ブロック暗号 DLBCA

DLBCA は 4bit S-Box を用いた非線形処理(Substitution)、BitRotation、排他的論理和、線形処理(Permutation)で構成されている。１段分の構造を以下の図１に示す。

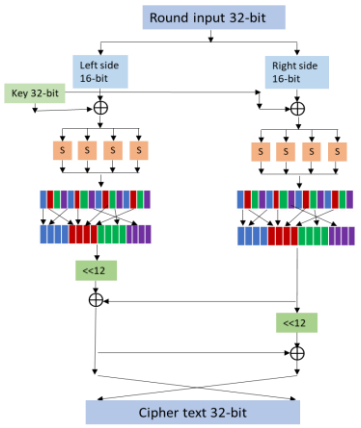


図１：DLBCA１段分の構造

## MILP を用いた Integral 特性探索

目的関数および制約条件は線形であり、変数の全てまたは一部が整数に制限される数理最適化問題を混合整数線形計画法(Mixed Integer Linear Programming) と呼ぶ。解析の結果、31 階差分において 6 段の特性を発見した。

## Integral 特性を利用した鍵回復

31 階差分において発見した特性を用い鍵回復に必要な計算量・平文数を算出した。

表１：鍵回復に必要な計算量・平文数

| 暗号化計算量 | 必要な平文数 |
|---|---|
| $2^{69}$ | $2^{31}$ |

## 参考文献

[1] Sufyan Salim Mahmood AlDabbagh"Design 32-bit Lightweight Block Cipher Algorithm(DLBCA)", International Journal of Computer Applications(0975–8887) Volume 166–No.8, May 2017

[2] Z.Xiang, W.Zhang, Z.Bao, and D.Lin "Applying MILP Method to Searching Integral Distinguishers Based on Division Property for 6 Lightweight Block Ciphers" Advances in Cryptology –ASIACRYPT 2016 (2016)

*東京理科大学理工学研究科電気工学専攻，〒278-8510 千葉県野田市山崎 2641 ,7321501@ed.tus.ac.jp

† 東京理科大学理工学研究科電気工学専攻，〒278-8510 千葉県野田市山崎 2641