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

ブロック暗号 RAGHAV の高階差分特性
Higher Order Differential Property of Block Cipher RAGHAV

芝山直喜 *　　五十嵐保隆 †
Naoki Shibayama　　Yasutaka Igarashi

キーワード ブロック暗号，RAGHAV，高階差分特性，暗号解析

あらまし

RAGHAV[1] は 2021 年に Bansod によって提案された 64 ビットブロック暗号であり，鍵長は 80 ビット及び 128 ビットをサポートしている．なお，ラウンド数は 31 である．これまでに安全性の自己評価において，線形攻撃，差分攻撃，Biclique 攻撃及び零相関攻撃等は脅威とはならないだろうと述べられているが，高階差分攻撃 [2] に対する耐性は未知である．本稿では，RAGHAV の構造に着目することにより，フルラウンドの高階差分特性を発見した．これより，フルラウンドの RAGHAV に対する乱数識別攻撃が可能である．

参考文献

[1] G.Bansod, “RAGHAV : A new low power S-P network encryption design for resource constrained environment,” https://eprint.iacr.org/2021/364.pdf, 2021.

[2] X.Lai, “Higher Order Derivatives and Differential Cryptanalysis,” Communications and Cryptography, pp.227–233, Kluwer Academic Publishers, 1994.

* 航空自衛隊 〒 162-8804 東京都新宿区市谷本村町 5-1. Japan Air Self-Defense Force, 5-1, Ichigayahonmuracho, Shinjuku-Ku, Tokyo 162–8804, Japan.
† 東京理科大学 〒 278-8510 千葉県野田市山崎 2641. Tokyo University of Science, 2641, Yamazaki, Noda, Chiba 278–8510 Japan.