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

Rocca と AEGIS ファミリーのラウンド関数の安全性評価
Security Evaluation for Round Functions of Rocca and AEGIS Families

竹内 信幸 * 阪本 光星 † 五十部 孝典 * ‡§
Nobuyuki Takeuchi Kosei Sakamoto Takanori Isobe

キーワード 認証暗号，ラウンド関数，Active S-box，Integral 攻撃，MILP

あらまし

SAC 2013 において Wu らは AES-NI を用いたソフトウェアで非常に高速な認証暗号 AEGIS-128/128L/256 を提案した [3]．FSE 2016 において Jean らは AEGIS の構成一般化を行い，いくつかの効率的な構成案を示した [1]．ToSC 2021 で，阪本らは Jean らの構成をさらに拡張し，Beyond 5G 向け認証暗号 Rocca を提案した [2]．

本稿では，混合整数線形計画法を用いて差分攻撃及び Integral 攻撃について，AEGIS と Rocca の初期化関数について安全性評価を行う．差分攻撃に対しては，Rocca と AEGIS-128/128L/256 はそれぞれ 6 ラウンド，4/3/6 ラウンドで Active-Sbox 評価で安全であることを示す．Integral 攻撃に関しては，Rocca においては 6 ラウンド，AEGIS-128/128L/256 においては 6/5/7 ラウンドの Integral 識別子を発見した．さらに，Rocca に加え，Jean らのラウンド関数をベースにした Permutation についての安全性解析も行う．

参考文献

[1] Jérémy Jean and Ivica Nikolic. Efficient design strategies based on the AES round function. In Thomas Peyrin, editor, *Fast Software Encryption - 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers*, volume 9783 of *Lecture Notes in Computer Science*, pages 334–353. Springer, 2016.

[2] Kosei Sakamoto, Fukang Liu, Yuto Nakano, Shinsaku Kiyomoto, and Takanori Isobe. Rocca: An efficient aes-based encryption scheme for beyond 5g. *IACR Trans. Symmetric Cryptol.*, 2021(2):1–30, 2021.

[3] Hongjun Wu and Bart Preneel. AEGIS: A fast authenticated encryption algorithm. In Tanja Lange, Kristin E. Lauter, and Petr Lisonek, editors, *Selected Areas in Cryptography - SAC 2013 - 20th International Conference, Burnaby, BC, Canada, August 14-16, 2013, Revised Selected Papers*, volume 8282 of *Lecture Notes in Computer Science*, pages 185–201. Springer, 2013.

* 兵庫県立大学大学院情報科学研究科，〒 650-0047 兵庫県神戸市中央区港島南町 7-1-28，University of Hyogo, 7-1-28, Minatojimaminami-cho, Chuo-ku, Kobe-shi, Hyogo, 650-0047, Japan.
† 兵庫県立大学応用情報科学研究科, 〒 650-0047 兵庫県神戸市中央区港島南町 7-1-28, University of Hyogo, 7-1-28, Minatojimaminami-cho, Chuo-ku, Kobe-shi, Hyogo, 650-0047, Japan.
‡ 国立研究開発法人情報通信研究機構，〒 184-8795 東京都小金井市貫井北町 4-2-1, NICT, 4-2-1, Nukui-Kitamachi, Koganei-shi, Tokyo, 184-8795, Japan.
§ 国立研究開発法人科学技術振興機構, 〒 102-0076 東京都千代田区五番町 7, PRESTO, 7, Gobancho, Chiyoda-ku, Tokyo, 102-0076 Japan.