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 LBC-IoT に対する MILP を用いた線形攻撃耐性評価
MILP-Based Linear Attack on Lightweight Block Cipher "LBC-IoT"

安士 颯真 * 五十嵐 保隆 *
Soma Yasushi Yasutaka Igarashi

キーワード 軽量ブロック暗号 LBC-IoT 線形攻撃 MILP

概要

軽量ブロック暗号 LBC-IoT[1] は、2021 年に Rabie A. Ramadan らによって提案された IoT デバイス向けの暗号である。この暗号は IoT デバイス向けの暗号のため、エネルギー効率が高い暗号化方式で、ハードウェアの実装面積が小さく抑えられているのが特徴である。LBC-IoT のブロックサイズは 32 bits,鍵長 80 bits,ラウンド数 32 rounds の Feistel 構造である。本稿では、MILP を用いた線形特性の探索により、23 rounds を線形特性確率2^{-30}で伝搬する線形パスを発見した。これにより LBC-IoT において 26 rounds で鍵回復が可能であることを示す。また、鍵回復に必要なデータ量は2^{30}、計算量は$2^{56.9}$となった。

軽量ブロック暗号 LBC-IoT

軽量ブロック暗号 LBC-IoT はブロックサイズ 32bits, 鍵長 80bits,ラウンド数 32 rounds の Feistel 構造である。LBC-IoT の 1 段分の構造を図 1 に示す。

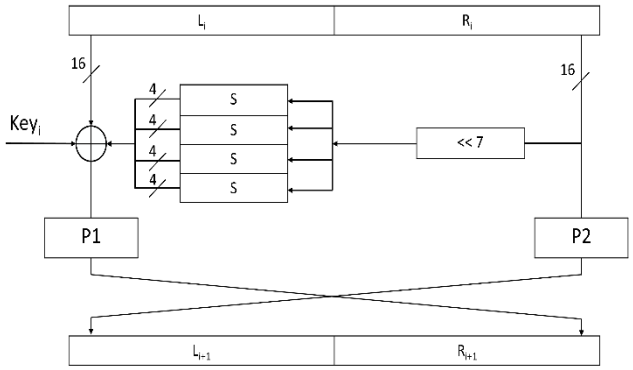

図 1 軽量ブロック暗号 LBC-IoT の 1 段分の構成

LBC-IoT は$i = 1,2, \cdots 32$段目において、左巡回シフト（記号≪）、4-bit S-box（記号S）、16-bit 段鍵（記号Key_i）、16 bits 単位の bit-permutation（記号$P1, P2$）、排他的論理和（記号⊕）で構成される。

MILP を用いた線形パスの探索

軽量ブロック暗号 LBC-IoT の線形パスを MILP を用いて探索した。結果として 23 rounds を線形特性確率2^{-30}で伝搬する線形パスを発見した。発見した線形パスを表 1 に示す。この特性により 26 rounds で鍵回復が可能であることを示す。

表 1 23 rounds を確率2^{-30}で伝搬する線形パス
段数の 0 は平文入力部を表す

段数	線形マスク (16 進数)	段数	線形マスク (16 進数)
0	0040 C001	12	0040 0001
1	0000 0001	13	0000 0001
2	0040 0000	14	0040 0000
3	0040 0001	15	0040 0001
4	0000 0001	16	0000 0001
5	0040 0000	17	0040 0000
6	0040 0001	18	0040 0001
7	0000 0001	19	0000 0001
8	0040 0000	20	0040 0000
9	0040 0001	21	0040 0001
10	0000 0001	22	0000 0001
11	0040 0000	23	0040 0000

参考文献

[1] Rabie A. Ramadan, Bassam W. Aboshosha, Kusum Yadav1, Ibrahim M. Alseadoon, Munawar J. Kashout and Mohamed Elhoseny "LBC-IoT: Lightweight Block Cipher for IoT Constraint Devices" CMC, 2021, vol.67, no.3, pp. 3563-3579

* 東京理科大学 〒278-8510 千葉県野田市山崎 2641
Tokyo University of Science, 2641 Yamazaki, Noda, 278-8510