ブロック暗号 LED の高階差分特性

井上 祐輔 †　　五十嵐 保隆 ‡　　金子 敏信 †

† 東京理科大学
278-8510 千葉県野田市山崎 2641
{j7312609@ed, kaneko@ee}.noda.tus.ac.jp

‡ 鹿児島大学
890-8580 鹿児島県鹿児島市郡元 1-21-24
igarashi@eee.kagoshima-u.ac.jp

あらまし　本稿ではブロック暗号 LED の高階差分特性について報告する。LED は AES を縮小した SPN 構造を持ち、4 ビット S-box で構成される。この LED において、4 階差分で 3 段まで、16 階差分で 4 段まで、32 階差分で 5 段まで達する高階差分特性を発見した。前 2 者は AES において知られる、8 階差分で 3 段まで、32 階差分で 4 段まで達する高階差分特性に対応している。

Higher Order Differential Properties of the LED Block Cipher

Yusuke Inoue†　　Yasutaka Igarashi‡　　Toshinobu Kaneko†

†Tokyo University of Science
2641 Yamazaki, Noda, Chiba 278-8510, JAPAN
{j7312609@ed, kaneko@ee}.noda.tus.ac.jp

‡Kagoshima University
1-21-24 Korimoto, Kagoshima, Kagoshima 890-8580, JAPAN
igarashi@eee.kagoshima-u.ac.jp

Abstract　In this paper, we report new higher order differential properties of the LED block cipher. LED has a AES-like structure with 4-bit S-boxes. We found a 4th order differential property for three rounds, a 16th order differential property for four rounds, and a 32nd order differential property for five rounds on LED. The 4th order and 16th order properties correspond to an 8th order differential property for three rounds and a 32th order differential property for four rounds on AES.

1　序論

LED は Guo らによって提案された 64 ビットブロック暗号である。CHES 2011 において初めて発表 [1] された後、Cryptology ePrint Archive において修正版が公表されている [2]。LED は AES を縮小したような SPN 構造を持ち、4 ビット S-box で構成される。本稿ではブロック暗号 LED の高階差分特性について報告する。この LED において、4 階差分で 3 段まで、16 階差分で 4 段まで達する高階差分特性を発見した。これらは AES において知られる、8 階差分で 3 段まで、32 階差分で 4 段まで達する高階差分特性に対応している。さらに、10 階差分で 4 段まで、32 階差分で 5 段まで達する高階差分特性を発見した。これらに対応する AES の特性は知られていない。

2　LED の構造

LED のブロック長は 64 ビットであり、鍵長は 64 から 128 ビットの間で自由に選択できる。

データ攪拌部における段関数の数は鍵長によって変わり、64 ビットでは 32 個、65 ビット以上では 48 個となる。全体構造を図 1 に示す。

段関数は AddConstants、SubCells、ShiftRows、MixColumnsSerial で構成され、4 段毎に秘密鍵より生成された副鍵が排他的論理和される。

2.1 データ攪拌部

ここては、64 ビットの内部状態を 4 ビットデータ s_i に分けて 4×4 の行列で表現する。

$$\begin{bmatrix} s_0 & s_1 & s_2 & s_3 \\ s_4 & s_5 & s_6 & s_7 \\ s_8 & s_9 & s_{10} & s_{11} \\ s_{12} & s_{13} & s_{14} & s_{15} \end{bmatrix}$$

2.1.1 AddConstants

次の定数が排他的論理和される。ただし、ks_i は鍵長依存の定数、rc_i は段依存の定数である。

$$\begin{bmatrix} 0 \oplus (\mathrm{ks}_7||\mathrm{ks}_6||\mathrm{ks}_5||\mathrm{ks}_4) & (\mathrm{rc}_5||\mathrm{rc}_4||\mathrm{rc}_3) & 0 & 0 \\ 1 \oplus (\mathrm{ks}_7||\mathrm{ks}_6||\mathrm{ks}_5||\mathrm{ks}_4) & (\mathrm{rc}_2||\mathrm{rc}_1||\mathrm{rc}_0) & 0 & 0 \\ 2 \oplus (\mathrm{ks}_3||\mathrm{ks}_2||\mathrm{ks}_1||\mathrm{ks}_0) & (\mathrm{rc}_5||\mathrm{rc}_4||\mathrm{rc}_3) & 0 & 0 \\ 3 \oplus (\mathrm{ks}_3||\mathrm{ks}_2||\mathrm{ks}_1||\mathrm{ks}_0) & (\mathrm{rc}_2||\mathrm{rc}_1||\mathrm{rc}_0) & 0 & 0 \end{bmatrix}$$

2.1.2 SubCells

各々の 4 ビットデータ s_i を 4 ビット入出力の非線形関数 (S-box) に適用する。これは AES における SubBytes 変換と対応する。

2.1.3 ShiftRows

内部状態の i 行目を 4 ビット単位で $i-1$ 回右回転シフトする。

2.1.4 MixColumnsSerial

内部状態の各列ベクトルを次の行列と乗算したものに置き換える。ただし、この計算における乗算は $\mathrm{GF}(2^4)$ 上の乗算であり、既約多項式は $X^4 + X + 1$ である。これは AES における MixColumns 変換と対応する。

$$\begin{pmatrix} 0\mathrm{x}4 & 0\mathrm{x}1 & 0\mathrm{x}2 & 0\mathrm{x}2 \\ 0\mathrm{x}8 & 0\mathrm{x}6 & 0\mathrm{x}5 & 0\mathrm{x}6 \\ 0\mathrm{xb} & 0\mathrm{xe} & 0\mathrm{xa} & 0\mathrm{x}9 \\ 0\mathrm{x}2 & 0\mathrm{x}2 & 0\mathrm{xf} & 0\mathrm{xb} \end{pmatrix}$$

3 高階差分攻撃

高階差分攻撃は Knudsen によって提案された高階差分の性質を利用した攻撃法である [3]。

3.1 高階差分

平文 $P \in \mathrm{GF}(2)^l$ と鍵 $K \in \mathrm{GF}(2)^m$ を入力とし、$H \in \mathrm{GF}(2)^n$ と出力する関数 $E'(P;K) = H$ の d 階差分は、1 次独立な d 個のベクトル A と、これによって張られる $\mathrm{GF}(2)^d$ 上の部分空間 $V^{(d)}$ を用いて、式 (1) のように定義する。

$$\Delta^{(d)}_{V^{(d)}} E'(P;K) = \bigoplus_{A \in V^{(d)}} E'(P \oplus A;K) \quad (1)$$

以降、$\Delta^{(d)}_{V^{(d)}}$ を $\Delta^{(d)}$ と表記する。$E'(P;K)$ の P に関するブール代数式が N 次のとき、$\Delta^{(d)} E'(P;K)$ は任意の鍵に対し次の性質を持つ。

$$\Delta^{(N+1)} E'(P;K) = 0 \quad (2)$$

3.2 飽和特性

飽和特性型の高階差分特性をデータの集合により表記する。N ビットデータの集合 $\{X_j | X_j \in \{0,1\}^N, 0 \le j < 2^N\}$ の性質として、次の 4 通りを定義する。ただし、Y_i は $X = i$ の出現度数である。

- Constant(C): if $\forall_{i,j}, X_i = X_j$
- All(A): if $\forall_{i,j}, i \neq j \Leftrightarrow X_i \neq X_j$
- Even/Odd(D): if $\forall_i, Y_i \equiv 0 (\mathrm{mod}\ 2)$ or $Y_i \equiv 1 (\mathrm{mod}\ 2)$
- Balance(B): if $\bigoplus_i X_i = 0$

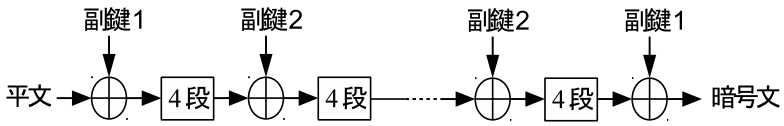

図 1: LED の全体構造

2^l 個の l ビット幅の集合 $\{X_j\}$ の性質が A のとき、$\mathrm{A}_{(l)}$ と表記する。さらに l ビットを分割し、m 個の $k_0, k_1, \cdots, k_{m-1}$(ただし、$\sum_{i=0}^{m-1} k_i = l$) ビットデータに表現する場合、次のように表す。

$$\mathrm{A}_{(l)} = (\mathrm{A}^0_{(k_0)}\mathrm{A}^1_{(k_1)}\cdots\mathrm{A}^{m-1}_{(k_{m-1})})$$

また、2^N 個の k ビットデータ X の性質として次を定義する。

- all(a): if $\forall_i, Y_i = 2^{N-k}$

上記以外の N ビットデータ X の集合の性質を Unknown(U) とする。

特性 C, A, D, B, a においては高階差分が 0 となる。

3.3 攻撃方程式

$r-1$ 段目出力において式 (2) の性質が現れる暗号に対する攻撃を考える。暗号文と r 段目の鍵 K_r を用いて $r-1$ 段目出力を求める関数を F とすると、次の方程式を解くことにより、正しい K_r を求められる。ただし $\mathcal{C}$ は 2^d 組の暗号文である。

$$\bigoplus_{C\in\mathcal{C}} F(C; K_r) = 0 \qquad (3)$$

式 (3) を攻撃方程式という。この方程式は K_r が正しいときは必ず成り立ち、K_r が誤っているときは 2^{-n}(n は $r-1$ 段目出力のビット長) の確率で成り立つ。

4 LED の高階差分特性

計算機実験により、LED 各段の出力において高階差分が式 (2) の性質を示すか否か (高階差分特性) を調査し、次に示す結果を得た。

4.1 AES の高階差分特性に対応する特性

次に示す特性は Ferguson らの論文 [4] において示された AES の高階差分特性と同じ飽和特性構造のものである。

4.1.1 4 階差分

16 個ある 4 ビットデータのいずれか 1 つに $\mathrm{A}_{(4)}$ を入力すれば、3 段目出力の 4 階差分が 0 となる。一例を図 2 に示す。

この特性は AES において 8 階差分で 3 段まで達する既知の高階差分特性に対応している。

4.1.2 16 階差分

1 段目の MixColumnsSerial への入力において内部状態の 1 列分が $\mathrm{A}_{(16)}$ となるように変数を選べば、4 段目出力の 16 階差分が 0 となる。一例を図 3 に示す。

この特性は AES において 32 階差分で 4 段まで達する既知の高階差分特性に対応している。

4.2 新しい高階差分特性

次に示す特性は AES において同じ飽和特性構造のものが未確認の特性である。

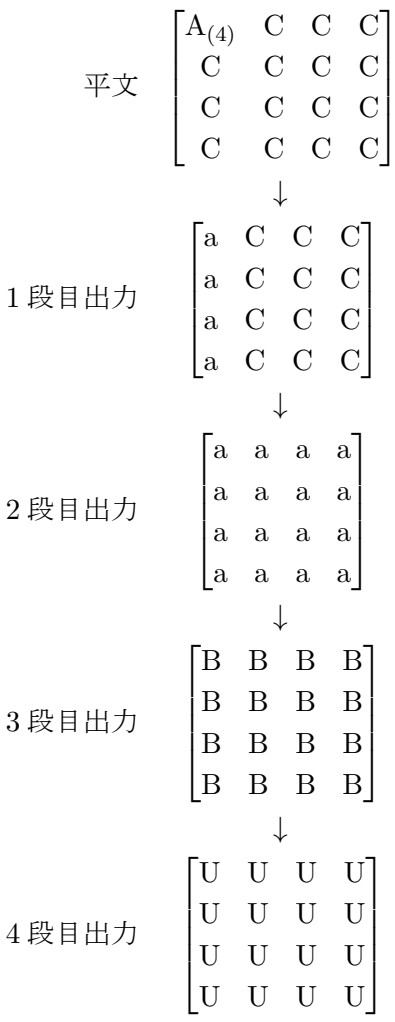

図 2: 4 階差分

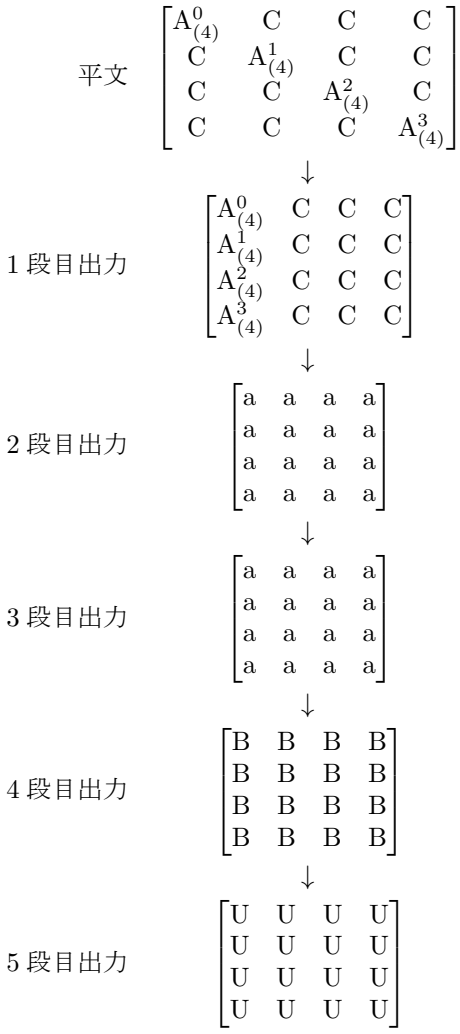

図 3: 16 階差分

4.2.1 10 階差分

4.1.2 節の特性が現れる 4 変数において、いずれか 2 変数を $A^i_{(4)}$ から $A^i_{(1)}$ に変えても、4 段目出力の 10 階差分は 0 となる。一例を図 4 に示す。

4.2.2 32 階差分

1 段目の MixColumnsSerial への入力において内部状態の 2 列分が $A_{(32)}$ となるように変数を選べば、5 段目出力の 32 階差分が 0 となる。一例を図 5 に示す。

4.3 変形 LED の高階差分特性

AES においては 1 段毎に鍵加算を行うのに対し、LED では 4 段毎に鍵加算を行うことから、鍵加算の頻度が少ないことによって LED の高階差分特性が AES よりも多い段に達するものとなっている可能性が考えられる。そこで、LED を 1 段毎に鍵加算を行うように変形したものについても 4.1〜4.2 節の特性が現れるか調査したところ、同じ特性が得られた。従って、4.2 節の特性が現れたのは鍵加算の頻度によるものではない。

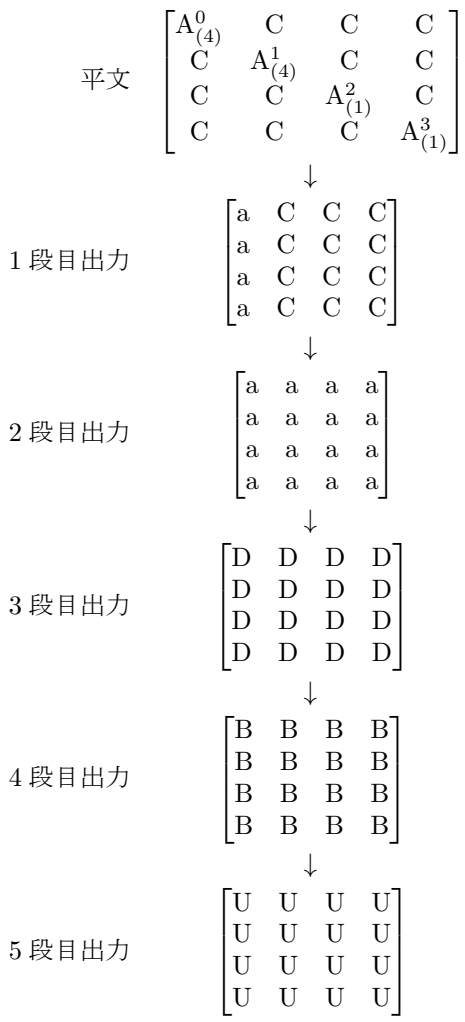

図 4: 10 階差分

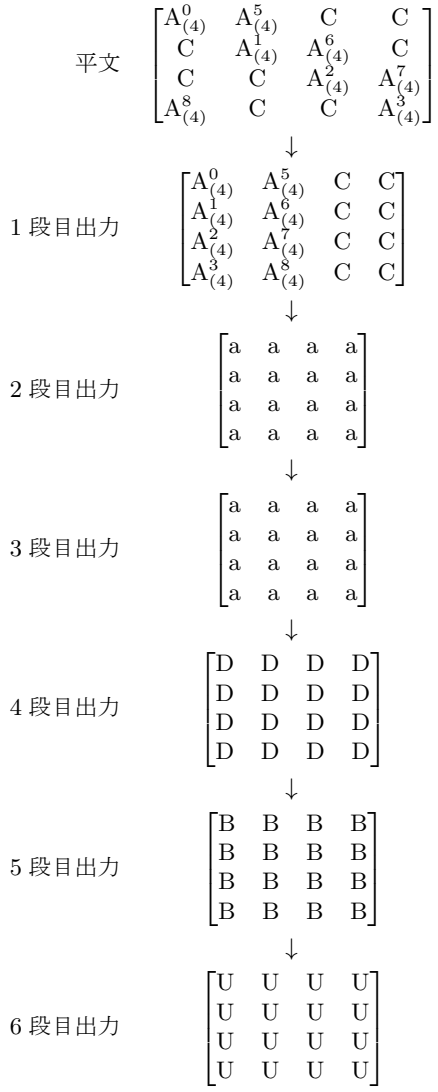

図 5: 32 階差分

5 LED に対する高階差分攻撃

これまでに示した高階差分特性を用いて、7 段・11 段 LED に対して攻撃することができる。なお、攻撃可能段数が 4 段おきとなっているのは、副鍵が 4 段毎に加算されているためである。

5.1 7 段 LED に対する攻撃

4.1.1 節の特性を用いることにより 7 段 LED に対して攻撃が可能である。手順は次の通りである (図 6)。

1. 4.1.1 節の特性が現れるように 2^4 組の平文を攻撃対象の 7 段 LED に入力し、2^4 組の暗号文を得る。
2. 暗号文に 3 段 LED の逆関数を適用する。
3. 2. の出力に MixColumnsSerial の逆関数を適用する。
4. 3. の出力を 4 ビット毎に分割し、その内のいずれか 1 つについて 4 ビットの鍵を推定し、排他的論理和する。
5. 4. の結果に S-box の逆関数を適用する。
6. 5. の結果を全て排他的論理和する。その結果、0 にならなければ 4. において推定した鍵は偽の鍵である。

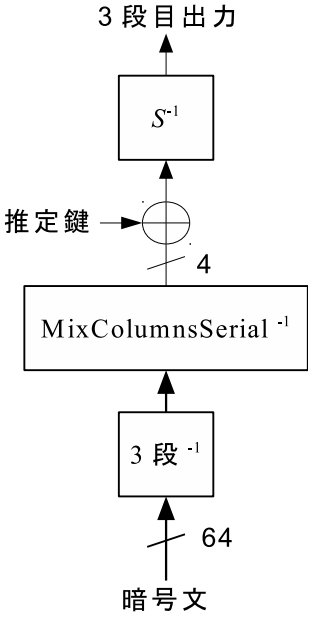

図 6: 7 段 LED に対する攻撃

7. 4.〜6. を全ての 4 ビット鍵で試行する。その結果、鍵候補がただ 1 つ残ればその鍵が真の鍵である。鍵候補が複数残った場合は平文を変え、鍵候補が 1 つになるまで 1.〜7. を繰り返す。

1 回の暗号化を S-box を 16×7 回参照するのと等価とすると、この攻撃に必要な計算量は 1 回の暗号化を単位として $\frac{2^4 \times (16 \times 3 + 2^4)}{16 \times 7} \approx 2^4$ である。

5.2 11 段 LED に対する攻撃

4.2.1 節の特性を用いることにより 11 段 LED に対して攻撃が可能である。手順は次の通りである (図 7)。

1. 4.2.1 節の特性が現れるように 2^{10} 組の平文を攻撃対象の 11 段 LED に入力し、2^{10} 組の暗号文を得る。
2. 暗号文に 3 段 LED の逆関数を適用する。

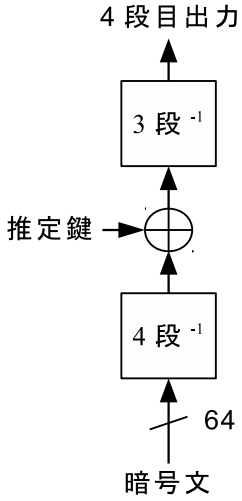

図 7: 11 段 LED に対する攻撃

3. 64 ビットの鍵を推定し、2. の出力に排他的論理和する。
4. 3. の結果に 4 段 LED の逆関数を適用する。
5. 4. の結果を全て排他的論理和する。その結果、0 にならなければ 3. において推定した鍵は偽の鍵である。
6. 3.〜5. を全ての 64 ビット鍵で試行する。その結果、鍵候補がただ 1 つ残ればその鍵が真の鍵である。鍵候補が複数残った場合は平文を変え、鍵候補が 1 つになるまで 1.〜6. を繰り返す。

1 回の暗号化を S-box を 16×11 回参照するのと等価とすると、この攻撃に必要な計算量は 1 回の暗号化を単位として $\frac{2^{10} \times (16 \times 3 + 2^{64} \times (16 \times 4))}{16 \times 11} \approx 2^{73}$ である。従ってこの攻撃が有効と言えるのは鍵長が 74 ビット以上のときである。

6 結論

本稿ではブロック暗号 LED の高階差分特性について述べた。LED には 4 階差分で 3 段まで、16 階差分で 4 段まで達する高階差分特性が

存在し、これらはAESにおける、8階差分で3段まで、32階差分で4段まで達する高階差分特性に対応している。他にも、10階差分で4段まで、32階差分で5段まで達する高階差分特性が存在する。これらと同様の特性をAESが持つかどうかを調べることは今後の課題である。また、これらの高階差分特性を利用することにより、7段LED、74〜128ビット鍵11段LEDを攻撃することが可能である。

参考文献

[1] Jian Guo, Thomas Peyrin, Axel Poschmann and Matt Robshaw, “The LED Block Cipher,” CHES 2011, LNCS vol.6917, pp.326-341, 2011.

[2] Jian Guo, Thomas Peyrin, Axel Poschmann and Matt Robshaw, “The LED Block Cipher,” Cryptology ePrint Archive, Report 2012/600, 2012.

[3] Lars R. Knudsen, ”Truncated and Higher Order Differentials,” FSE 1994, LNCS, vol.1008, pp.196-211, 1995.

[4] Niels Ferguson, John Kelsey, Stefan Lucks, Bruce Schneier, Mike Stay, David Wagner, and Doug Whiting, ”Improved Cryptanalysis of Rijndael,” FSE 2000, LNCS, vol.1978, pp.136-141, 2001.