Computer Security Symposium 2016
11 - 13 October 2016

ブロック暗号Midori64の特異な3階差分特性(Ⅱ)

高橋 勇介[1]　五十嵐 保隆[1]　金子 敏信[1]

概要：Midori64 は Banik らが 2015 年に提案した秘密鍵長 128 ビットの SPN 型 64 ビットブロック暗号アルゴリズムである．高階差分攻撃は Lai が提案した暗号攻撃手法である．暗号化関数のブール多項式の代数次数に着目した攻撃法であり，共通鍵暗号アルゴリズム全般に広く適用できる攻撃法である．本稿では，この攻撃で利用できる複数種類の特異な 3 階差分特性の発見とその理論解析を報告する．

キーワード：ブロック暗号，Midori64，高階差分攻撃，ブール多項式

The particular third-order differential characteristics of Midori64 block cipher(Ⅱ)

Yusuke Takahashi[1]　Yasutaka Igarashi[1]　Toshinobu Kaneko[1]

Abstract: Midori64 proposed by Banik et al. in 2015 is an SPN-type block cipher with 128-bit secret key. The higher-order differential characteristics of the boolean polynomial of encryption function can be exploited for cryptanalysis. In this paper, we show a variety of the particular third-order differential characteristics of Midori64 block cipher, and theoretically analyze the characteristics.

Keywords: Block Cipher, Midori64, Higher-order differential attack, Boolean polynomial

1. まえがき

Midori64 は Banik らが 2015 年に提案した秘密鍵長 128 ビットの SPN 型 64 ビットブロック暗号アルゴリズムである．高階差分攻撃は Lai が提案した暗号攻撃手法である．暗号化関数のブール多項式の代数次数に着目した攻撃法であり，共通鍵暗号アルゴリズム全般に広く適用できる攻撃法である．本稿では，この攻撃で利用できる複数種類の特異な 3 階差分特性の発見とその理論解析を報告する．尚，本稿で特異とは，一般的には，高階差分値が不定となる箇所で不定とならずに，(高階差分値)=0，つまり，バランス特性が出現することを意味している．

2. Midori64 のデータ撹拌部

図 1 に 10 段構成の Midori64 のデータ撹拌部を示す．R 関数 9 個と S 関数 1 個で構成されている．K_0, K_1 はそれぞれ次式で表される 64 ビットの鍵であり，$K_2 = K_0 \oplus K_1$ である．

$$K_i = k_0^i \parallel k_1^i \parallel ... \parallel k_{15}^i, (i = 0, 1, 2), \quad k_j^i \in \{0,1\}^4, (j = 0, 1, ..., 15). \tag{1}$$

$x \parallel y$ は 2 つのデータ x と y の連結を表す．RC_i は i 段目のラウンド定数を表すが，詳細は重要ではないので省略する．図 2 にラウンド関数 R を示す．その構成要素は 3 層から成り，1 つ目は 16 並列の 4 ビット入出力 S-box から成る S 層であり，2 つ目は，4 ビット単位のデータの入れ替え処理である SC 層であり，3 つ目は，要素の値が 4 ビットである次式で示される 4×4 行列 M の 4 並列から成る M 層である．行列 M と，その逆行列 M^{-1} を次式に示す．

$$M = M^{-1} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}. \tag{2}$$

[1] 東京理科大学大学院
Tokyo University of Science

S-box は次数 3 の全単射の非線形関数である．式 (3) から式 (6) に代数式展開を示す．x_i を S-box の入力，y_i を出力とし，x_3, y_3 を最上位ビットとし，x_0, y_0 を最下位ビットとする．

$$y_3 = x_0x_1x_3 \oplus x_1x_2x_3 \oplus x_0x_1 \oplus x_1x_3 \oplus x_2x_3 \oplus 1, \quad (3)$$

$$y_2 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_1x_2x_3 \oplus x_0x_3 \oplus x_0 \oplus x_3 \oplus 1, \quad (4)$$

$$y_1 = x_0x_2 \oplus x_0x_3 \oplus x_2x_3 \oplus x_0 \oplus x_2, \quad (5)$$

$$y_0 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_1x_2x_3 \oplus x_0x_2 \oplus x_0x_3 \oplus x_1. \quad (6)$$

SC 層と行列 M は線形関数である．図 1 の S 関数の構造は図 2 において SC 層と M 層を削除した S 層のみの構造となっている．

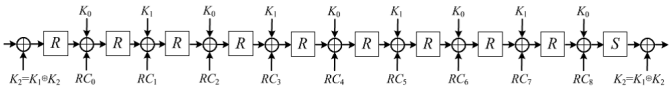

図 1 10 段構成の Midori64 のデータ撹拌部
Fig. 1 Data mixing part of Midori64 consisting of 10 round functions.

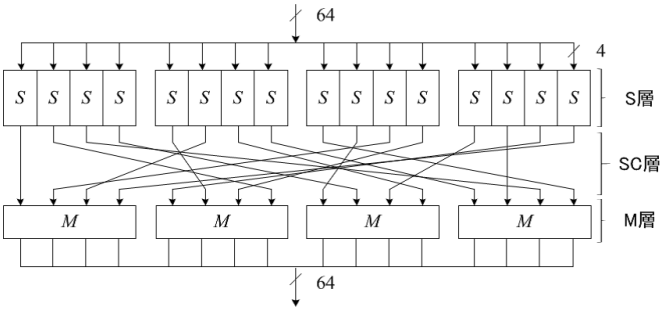

図 2 ラウンド関数 R
Fig. 2 Round function R.

3. 高階差分

本節では図 3 の一般的な暗号回路モデルを例にして高階差分の定義を示し，高階差分の性質のうち，本稿に関係する事項及びその性質を利用した攻撃方程式について一般的に述べる．高階差分の詳細な性質に関しては文献 [1] を参照されたい．

3.1 定義

図 3 の E_1, E_2 はそれぞれ暗号化関数の構成要素を表し，$K_1 \in GF(2)^p, K_2 \in GF(2)^q$ はそれぞれ p ビット，q ビットの暗号化鍵を表す．$P = (p_1, p_2, ..., p_n)$ と $\Delta P \in GF(2)^n$ はそれぞれ n ビットの平文と平文差分を表す．$H \in GF(2)^m$ は m ビットの E_1 出力を表す．$C(P \oplus \Delta P) \in GF(2)^l$ は

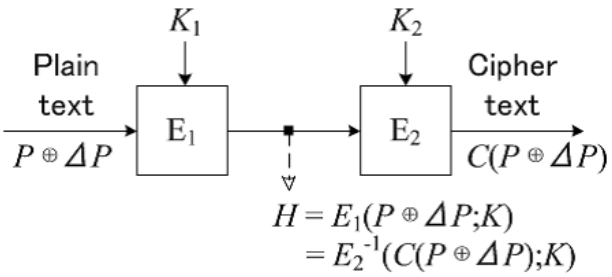

図 3 一般的な暗号回路モデル
Fig. 3 A general model of encryption circuit.

平文 $(P \oplus \Delta P)$ に対応する l ビットの出力暗号文を表す．$V^{(i)}$ は $GF(2)^n$ の i 次元部分空間を表す．$V^{(i)}$ に関する $E_1(P; K_1)$ の i 階差分 $\Delta^{(i)}E_1(P; K_1)$ は次式で定義される．

$$\Delta^{(i)}E_1(P; K_1) \equiv \sum_{\Delta P \in V^{(i)}}^{\oplus} E_1(P \oplus \Delta P; K_1). \quad (7)$$

ここで $\sum^{\oplus}$ は XOR による総和を表す．

3.2 性質

今，$E_1(P; K_1)$ の P に関するブール代数次数が $N(\leq n)$ ならば，次式のように N 階差分 $\Delta^{(N)}E_1(P; K_1)$，$(N+1)$ 階差分 $\Delta^{(N+1)}E_1(P; K_1)$ はそれぞれ P と K_1 に依存せずに，定数，ゼロになる性質をもつ．

$$\Delta^{(N)}E_1(P; K_1) = const, \quad (8)$$

$$\Delta^{(N+1)}E_1(P; K_1) = 0. \quad (9)$$

3.3 飽和特性

N ビットデータ X の集合 $\{X_j | X_j \in \{0,1\}^N, 0 \leq j \leq 2^N - 1\}$ の性質の表記として次に挙げる表記を用いる．

Constant(C) : $\forall_{i,k}; X_i = X_k$
All(A) : $\forall_{i,k}; i \neq k \rightarrow X_i \neq X_k$
Balance-0(B) : $\sum_i^{\oplus} X_i = 0$
Balance-1($\overline{\text{B}}$) : $\sum_i^{\oplus} X_i = 1$
Unknown(U) : 不定値

U のみは攻撃に利用できない特性であるが，それ以外の 4 つの特性は攻撃に利用できる．

4. Midori64 の 3 階差分特性

4.1 差分の入力パターン

入力平文 64 ビットの左端の最上位 4 ビット (x_3, x_2, x_1, x_0) に着目し，3 階差分の全ての入力パターン，つまり 3 次元部分空間を次式に従って考える．

$$\begin{pmatrix} x_3 \\ x_2 \\ x_1 \\ x_0 \end{pmatrix} = \vec{V} \begin{pmatrix} t_2 \\ t_1 \\ t_0 \end{pmatrix}. \quad (10)$$

ここで，$\vec{V} = (\vec{v_i}, \vec{v_j}, \vec{v_k})$ であり，$\vec{v_i}, \vec{v_j}, \vec{v_k}$ は互いに独立である GF(2) 上の 4 次元縦ベクトルを表す．$(t_2, t_1, t_0)^t$ は，$(0,0,0)^t$ から $(1,1,1)^t$ までの全 8 通りの値を取る 3 次元ベクトルである．$()^t$ は行列の転置を表す．$(\vec{v_i}, \vec{v_j}, \vec{v_k})$ の候補として次に示す 15 個のベクトルが存在する．

$$\vec{v_1} = (0,0,0,1)^t, \tag{11}$$
$$\vec{v_2} = (0,0,1,0)^t, \tag{12}$$
$$\vec{v_3} = (0,0,1,1)^t, \tag{13}$$
$$\vec{v_4} = (0,1,0,0)^t, \tag{14}$$
$$\vec{v_5} = (0,1,0,1)^t, \tag{15}$$
$$\vec{v_6} = (0,1,1,0)^t, \tag{16}$$
$$\vec{v_7} = (0,1,1,1)^t, \tag{17}$$
$$\vec{v_8} = (1,0,0,0)^t, \tag{18}$$
$$\vec{v_9} = (1,0,0,1)^t, \tag{19}$$
$$\vec{v_{10}} = (1,0,1,0)^t, \tag{20}$$
$$\vec{v_{11}} = (1,0,1,1)^t, \tag{21}$$
$$\vec{v_{12}} = (1,1,0,0)^t, \tag{22}$$
$$\vec{v_{13}} = (1,1,0,1)^t, \tag{23}$$
$$\vec{v_{14}} = (1,1,1,0)^t, \tag{24}$$
$$\vec{v_{15}} = (1,1,1,1)^t. \tag{25}$$

実際には互いに異なる 3 次元部分空間を与える $\vec{V}$ は次に示す 15 通りである．

$$\vec{V} = \begin{pmatrix} * & * & * \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \tag{26}$$
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & * & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \tag{27}$$
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & * \\ 0 & 0 & 1 \end{pmatrix}, \tag{28}$$
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}. \tag{29}$$

ここで，$*$ 印は 0 または 1 のどちらの値も取ることができることを表す．従って，式 (25)，(26)，(27)，(28) はそれぞれ 8 通り，4 通り，2 通り，1 通りの計 15 通りとなっている．これら 15 通りの $\vec{V}$ とそれに対応する (x_3, x_2, x_1, x_0) の集合を (例えば (1,0,1,1) を B と表記し，16 進数としてまとめて表記している) 表 1 に示す．

表 1 4 次元空間における 3 階差分の入力パターン
Table 1 Input patterns of the 3rd-order differential in 4-dimensional space.

$(\vec{v_i}, \vec{v_j}, \vec{v_k})$	(x_3, x_2, x_1, x_0) の集合
$(\vec{v_4}, \vec{v_2}, \vec{v_1})$	{0, 1, 2, 3, 4, 5, 6, 7}
$(\vec{v_4}, \vec{v_2}, \vec{v_9})$	{0, 9, 2, B, 4, D, 6, F}
$(\vec{v_4}, \vec{v_{10}}, \vec{v_9})$	{0, 9, A, 3, 4, D, E, 7}
$(\vec{v_{12}}, \vec{v_2}, \vec{v_9})$	{0, 9, 2, B, C, 5, E, 7}
$(\vec{v_4}, \vec{v_{10}}, \vec{v_1})$	{0, 1, A, B, 4, 5, E, F}
$(\vec{v_{12}}, \vec{v_{10}}, \vec{v_1})$	{0, 1, A, B, C, D, 6, 7}
$(\vec{v_{12}}, \vec{v_2}, \vec{v_1})$	{0, 1, 2, 3, C, D, E, F}
$(\vec{v_{12}}, \vec{v_{10}}, \vec{v_9})$	{0, 9, A, 3, C, 5, 6, F}
$(\vec{v_8}, \vec{v_2}, \vec{v_1})$	{0, 1, 2, 3, 8, 9, A, B}
$(\vec{v_8}, \vec{v_2}, \vec{v_5})$	{0, 5, 2, 7, 8, D, A, F}
$(\vec{v_8}, \vec{v_6}, \vec{v_1})$	{0, 1, 6, 7, 8, 9, E, F}
$(\vec{v_8}, \vec{v_6}, \vec{v_5})$	{0, 5, 6, 3, 8, D, E, B}
$(\vec{v_8}, \vec{v_4}, \vec{v_1})$	{0, 1, 4, 5, 8, 9, C, D}
$(\vec{v_8}, \vec{v_4}, \vec{v_3})$	{0, 3, 4, 7, 8, B, C, F}
$(\vec{v_8}, \vec{v_4}, \vec{v_2})$	{0, 2, 4, 6, 8, A, C, E}

4.2 3 階差分の出力結果

表 1 の 15 通りの 3 階差分の入力に対する，各段の飽和特性を表 2 から表 16 に示す．これは鍵と平文の基準値をランダムに 20000 回設定した時のシミュレーション結果である．C，B，U はそれぞれ 4 ビット分の特性をまとめて表している．さらに，B_x^n は B 特性を持つビットを n ビット，x 特性を持つビットを $(4-n)$ ビット含む 4 ビットの特性を表す．

表 2 $\vec{V} = (\vec{v_4}, \vec{v_2}, \vec{v_1})$ の 3 階差分特性
Table 2 The third-order differential characteristics of Midori64 with $\vec{V} = (\vec{v_4}, \vec{v_2}, \vec{v_1})$.

出現位置	$\vec{V} = (\vec{v_4}, \vec{v_2}, \vec{v_1})$ の特性
入力	($\mathrm{B}_{\mathrm{C}}^3$CCC CCCC CCCC CCCC)
1 段目出力	($\mathrm{CB}_{\mathrm{B}}^2\mathrm{B}_{\mathrm{B}}^2\mathrm{B}_{\mathrm{B}}^2$ CCCC CCCC CCCC)
2 段目出力	(CCCC $\mathrm{B}_{\mathrm{U}}^1\mathrm{B}_{\mathrm{U}}^1\mathrm{B}_{\mathrm{U}}^1$C $\mathrm{B}_{\mathrm{U}}^1\mathrm{CB}_{\mathrm{U}}^1\mathrm{B}_{\mathrm{U}}^1$ $\mathrm{B}_{\mathrm{U}}^1\mathrm{B}_{\mathrm{U}}^1\mathrm{CB}_{\mathrm{U}}^1$)

表 3 $\vec{V} = (\vec{v_4}, \vec{v_2}, \vec{v_9})$ の 3 階差分特性
Table 3 The third-order differential characteristics of Midori64 with $\vec{V} = (\vec{v_4}, \vec{v_2}, \vec{v_9})$.

出現位置	$\vec{V} = (\vec{v_4}, \vec{v_2}, \vec{v_9})$ の特性
入力	(BCCC CCCC CCCC CCCC)
1 段目出力	($\mathrm{CB}_{\mathrm{B}}^3\mathrm{B}_{\mathrm{B}}^3\mathrm{B}_{\mathrm{B}}^3$ CCCC CCCC CCCC)
2 段目出力	(CCCC UUUC UCUU UUCU)
3 段目出力	($\mathrm{B}_{\mathrm{U}}^1\mathrm{B}_{\mathrm{U}}^1\mathrm{B}_{\mathrm{U}}^1\mathrm{B}_{\mathrm{U}}^1$ $\mathrm{B}_{\mathrm{U}}^1\mathrm{B}_{\mathrm{U}}^1\mathrm{B}_{\mathrm{U}}^1\mathrm{B}_{\mathrm{U}}^1$ $\mathrm{B}_{\mathrm{U}}^1\mathrm{B}_{\mathrm{U}}^1\mathrm{B}_{\mathrm{U}}^1\mathrm{B}_{\mathrm{U}}^1$ $\mathrm{B}_{\mathrm{U}}^1\mathrm{B}_{\mathrm{U}}^1\mathrm{B}_{\mathrm{U}}^1\mathrm{B}_{\mathrm{U}}^1$)

表 4 $\vec{V}=(\vec{v_4},\vec{v_{10}},\vec{v_9})$ の 3 階差分特性

Table 4 The third-order differential characteristics of Midori64 with $\vec{V}=(\vec{v_4},\vec{v_{10}},\vec{v_9})$.

出現位置	$\vec{V}=(\vec{v_4},\vec{v_{10}},\vec{v_9})$ の特性
入力	(BCCC CCCC CCCC CCCC)
1 段目出力	($\mathrm{CB}^3_{\mathrm{B}}\mathrm{B}^3_{\mathrm{B}}\mathrm{B}^3_{\mathrm{B}}$ CCCC CCCC CCCC)
2 段目出力	(CCCC UUUC UCUU UUCU)

表 5 $\vec{V}=(\vec{v_{12}},\vec{v_2},\vec{v_9})$ の 3 階差分特性

Table 5 The third-order differential characteristics of Midori64 with $\vec{V}=(\vec{v_{12}},\vec{v_2},\vec{v_9})$.

出現位置	$\vec{V}=(\vec{v_{12}},\vec{v_2},\vec{v_9})$ の特性
入力	(BCCC CCCC CCCC CCCC)
1 段目出力	($\mathrm{CB}^2_{\mathrm{B}}\mathrm{B}^2_{\mathrm{B}}\mathrm{B}^2_{\mathrm{B}}$ CCCC CCCC CCCC)
2 段目出力	(CCCC UUUC UCUU UUCU)

表 6 $\vec{V}=(\vec{v_4},\vec{v_{10}},\vec{v_1})$ の 3 階差分特性

Table 6 The third-order differential characteristics of Midori64 with $\vec{V}=(\vec{v_4},\vec{v_{10}},\vec{v_1})$.

出現位置	$\vec{V}=(\vec{v_4},\vec{v_{10}},\vec{v_1})$ の特性
入力	(BCCC CCCC CCCC CCCC)
1 段目出力	($\mathrm{CB}^2_{\mathrm{B}}\mathrm{B}^2_{\mathrm{B}}\mathrm{B}^2_{\mathrm{B}}$ CCCC CCCC CCCC)
2 段目出力	(CCCC UUUC UCUU UUCU)

表 7 $\vec{V}=(\vec{v_{12}},\vec{v_{10}},\vec{v_1})$ の 3 階差分特性

Table 7 The third-order differential characteristics of Midori64 with $\vec{V}=(\vec{v_{12}},\vec{v_{10}},\vec{v_1})$.

出現位置	$\vec{V}=(\vec{v_{12}},\vec{v_{10}},\vec{v_1})$ の特性
入力	(BCCC CCCC CCCC CCCC)
1 段目出力	($\mathrm{CB}^3_{\mathrm{B}}\mathrm{B}^3_{\mathrm{B}}\mathrm{B}^3_{\mathrm{B}}$ CCCC CCCC CCCC)
2 段目出力	(CCCC UUUC UCUU UUCU)

表 8 $\vec{V}=(\vec{v_{12}},\vec{v_2},\vec{v_1})$ の 3 階差分特性

Table 8 The third-order differential characteristics of Midori64 with $\vec{V}=(\vec{v_{12}},\vec{v_2},\vec{v_1})$.

出現位置	$\vec{V}=(\vec{v_{12}},\vec{v_2},\vec{v_1})$ の特性
入力	(BCCC CCCC CCCC CCCC)
1 段目出力	($\mathrm{CB}^3_{\mathrm{B}}\mathrm{B}^3_{\mathrm{B}}\mathrm{B}^3_{\mathrm{B}}$ CCCC CCCC CCCC)
2 段目出力	(CCCC UUUC UCUU UUCU)
3 段目出力	($\mathrm{B}^1_{\mathrm{U}}\mathrm{B}^1_{\mathrm{U}}\mathrm{B}^1_{\mathrm{U}}\mathrm{B}^1_{\mathrm{U}}$ $\mathrm{B}^1_{\mathrm{U}}\mathrm{B}^1_{\mathrm{U}}\mathrm{B}^1_{\mathrm{U}}\mathrm{B}^1_{\mathrm{U}}$ $\mathrm{B}^1_{\mathrm{U}}\mathrm{B}^1_{\mathrm{U}}\mathrm{B}^1_{\mathrm{U}}\mathrm{B}^1_{\mathrm{U}}$ $\mathrm{B}^1_{\mathrm{U}}\mathrm{B}^1_{\mathrm{U}}\mathrm{B}^1_{\mathrm{U}}\mathrm{B}^1_{\mathrm{U}}$)

表 9 $\vec{V}=(\vec{v_{12}},\vec{v_{10}},\vec{v_9})$ の 3 階差分特性

Table 9 The third-order differential characteristics of Midori64 with $\vec{V}=(\vec{v_{12}},\vec{v_{10}},\vec{v_9})$.

出現位置	$\vec{V}=(\vec{v_{12}},\vec{v_{10}},\vec{v_9})$ の特性
入力	(BCCC CCCC CCCC CCCC)
1 段目出力	($\mathrm{CB}^2_{\mathrm{B}}\mathrm{B}^2_{\mathrm{B}}\mathrm{B}^2_{\mathrm{B}}$ CCCC CCCC CCCC)
2 段目出力	($\mathrm{CCCC\,B}^1_{\mathrm{U}}\mathrm{B}^1_{\mathrm{U}}\mathrm{B}^1_{\mathrm{U}}\mathrm{C\,B}^1_{\mathrm{U}}\mathrm{CB}^1_{\mathrm{U}}\mathrm{B}^1_{\mathrm{U}}$ $\mathrm{B}^1_{\mathrm{U}}\mathrm{B}^1_{\mathrm{U}}\mathrm{CB}^1_{\mathrm{U}}$)

表 10 $\vec{V}=(\vec{v_8},\vec{v_2},\vec{v_1})$ の 3 階差分特性

Table 10 The third-order differential characteristics of Midori64 with $\vec{V}=(\vec{v_8},\vec{v_2},\vec{v_1})$.

出現位置	$\vec{V}=(\vec{v_8},\vec{v_2},\vec{v_1})$ の特性
入力	($\mathrm{B}^3_{\mathrm{C}}$CCC CCCC CCCC CCCC)
1 段目出力	($\mathrm{CB}^1_{\mathrm{B}}\mathrm{B}^1_{\mathrm{B}}\mathrm{B}^1_{\mathrm{B}}$ CCCC CCCC CCCC)
2 段目出力	($\mathrm{CCCC\,B}^2_{\mathrm{U}}\mathrm{B}^2_{\mathrm{U}}\mathrm{B}^2_{\mathrm{U}}\mathrm{C\,B}^2_{\mathrm{U}}\mathrm{CB}^2_{\mathrm{U}}\mathrm{B}^2_{\mathrm{U}}$ $\mathrm{B}^2_{\mathrm{U}}\mathrm{B}^2_{\mathrm{U}}\mathrm{CB}^2_{\mathrm{U}}$)

表 11 $\vec{V}=(\vec{v_8},\vec{v_2},\vec{v_5})$ の 3 階差分特性

Table 11 The third-order differential characteristics of Midori64 with $\vec{V}=(\vec{v_8},\vec{v_2},\vec{v_5})$.

出現位置	$\vec{V}=(\vec{v_8},\vec{v_2},\vec{v_5})$ の特性
入力	(BCCC CCCC CCCC CCCC)
1 段目出力	(CBBB CCCC CCCC CCCC)
2 段目出力	($\mathrm{CCCC\,B}^1_{\mathrm{U}}\mathrm{B}^1_{\mathrm{U}}\mathrm{B}^1_{\mathrm{U}}\mathrm{C\,B}^1_{\mathrm{U}}\mathrm{CB}^1_{\mathrm{U}}\mathrm{B}^1_{\mathrm{U}}$ $\mathrm{B}^1_{\mathrm{U}}\mathrm{B}^1_{\mathrm{U}}\mathrm{CB}^1_{\mathrm{U}}$)
3 段目出力	($\mathrm{B}^1_{\mathrm{U}}\mathrm{B}^1_{\mathrm{U}}\mathrm{B}^1_{\mathrm{U}}\mathrm{B}^1_{\mathrm{U}}$ $\mathrm{B}^1_{\mathrm{U}}\mathrm{B}^1_{\mathrm{U}}\mathrm{B}^1_{\mathrm{U}}\mathrm{B}^1_{\mathrm{U}}$ $\mathrm{B}^1_{\mathrm{U}}\mathrm{B}^1_{\mathrm{U}}\mathrm{B}^1_{\mathrm{U}}\mathrm{B}^1_{\mathrm{U}}$ $\mathrm{B}^1_{\mathrm{U}}\mathrm{B}^1_{\mathrm{U}}\mathrm{B}^1_{\mathrm{U}}\mathrm{B}^1_{\mathrm{U}}$)

表 12 $\vec{V}=(\vec{v_8},\vec{v_6},\vec{v_1})$ の 3 階差分特性

Table 12 The third-order differential characteristics of Midori64 with $\vec{V}=(\vec{v_8},\vec{v_6},\vec{v_1})$.

出現位置	$\vec{V}=(\vec{v_8},\vec{v_6},\vec{v_1})$ の特性
入力	(BCCC CCCC CCCC CCCC)
1 段目出力	($\mathrm{CB}^1_{\mathrm{B}}\mathrm{B}^1_{\mathrm{B}}\mathrm{B}^1_{\mathrm{B}}$ CCCC CCCC CCCC)
2 段目出力	($\mathrm{CCCC\,B}^2_{\mathrm{U}}\mathrm{B}^2_{\mathrm{U}}\mathrm{B}^2_{\mathrm{U}}\mathrm{C\,B}^2_{\mathrm{U}}\mathrm{CB}^2_{\mathrm{U}}\mathrm{B}^2_{\mathrm{U}}$ $\mathrm{B}^2_{\mathrm{U}}\mathrm{B}^2_{\mathrm{U}}\mathrm{CB}^2_{\mathrm{U}}$)

表 13 $\vec{V}=(\vec{v_8},\vec{v_6},\vec{v_5})$ の 3 階差分特性

Table 13 The third-order differential characteristics of Midori64 with $\vec{V}=(\vec{v_8},\vec{v_6},\vec{v_5})$.

出現位置	$\vec{V}=(\vec{v_8},\vec{v_6},\vec{v_5})$ の特性
入力	(BCCC CCCC CCCC CCCC)
1 段目出力	(CBBB CCCC CCCC CCCC)
2 段目出力	($\mathrm{CCCC\,B}^2_{\mathrm{U}}\mathrm{B}^2_{\mathrm{U}}\mathrm{B}^2_{\mathrm{U}}\mathrm{C\,B}^2_{\mathrm{U}}\mathrm{CB}^2_{\mathrm{U}}\mathrm{B}^2_{\mathrm{U}}$ $\mathrm{B}^2_{\mathrm{U}}\mathrm{B}^2_{\mathrm{U}}\mathrm{CB}^2_{\mathrm{U}}$)

表 14 $\vec{V}=(\vec{v_8},\vec{v_4},\vec{v_1})$ の 3 階差分特性

Table 14 The third-order differential characteristics of Midori64 with $\vec{V}=(\vec{v_8},\vec{v_4},\vec{v_1})$.

出現位置	$\vec{V}=(\vec{v_8},\vec{v_4},\vec{v_1})$ の特性
入力	($\mathrm{B}^3_{\mathrm{C}}$CCC CCCC CCCC CCCC)
1 段目出力	(CBBB CCCC CCCC CCCC)
2 段目出力	($\mathrm{CCCC\,B}^3_{\mathrm{U}}\mathrm{B}^3_{\mathrm{U}}\mathrm{B}^3_{\mathrm{U}}\mathrm{C\,B}^3_{\mathrm{U}}\mathrm{CB}^3_{\mathrm{U}}\mathrm{B}^3_{\mathrm{U}}$ $\mathrm{B}^3_{\mathrm{U}}\mathrm{B}^3_{\mathrm{U}}\mathrm{CB}^3_{\mathrm{U}}$)
3 段目出力	(UUUU UUUU UUUU UUUU)
4 段目出力	($\mathrm{B}^1_{\mathrm{U}}$UUU UUUU UUUU UUUU)

表 15 $\vec{V}=(\vec{v_8},\vec{v_4},\vec{v_3})$ の 3 階差分特性

Table 15 The third-order differential characteristics of Midori64 with $\vec{V}=(\vec{v_8},\vec{v_4},\vec{v_3})$.

出現位置	$\vec{V}=(\vec{v_8},\vec{v_4},\vec{v_3})$ の特性
入力	(BCCC CCCC CCCC CCCC)
1 段目出力	($\mathrm{CB}^1_{\overline{\mathrm{B}}}\mathrm{B}^1_{\overline{\mathrm{B}}}\mathrm{B}^1_{\overline{\mathrm{B}}}$ CCCC CCCC CCCC)
2 段目出力	(CCCC $\mathrm{B}^2_{\mathrm{U}}\mathrm{B}^2_{\mathrm{U}}\mathrm{B}^2_{\mathrm{U}}$C $\mathrm{B}^2_{\mathrm{U}}\mathrm{CB}^2_{\mathrm{U}}\mathrm{B}^2_{\mathrm{U}}$ $\mathrm{B}^2_{\mathrm{U}}\mathrm{B}^2_{\mathrm{U}}\mathrm{CB}^2_{\mathrm{U}}$)

表 16 $\vec{V}=(\vec{v_8},\vec{v_4},\vec{v_2})$ の 3 階差分特性

Table 16 The third-order differential characteristics of Midori64 with $\vec{V}=(\vec{v_8},\vec{v_4},\vec{v_2})$.

出現位置	$\vec{V}=(\vec{v_8},\vec{v_4},\vec{v_2})$ の特性
入力	($\mathrm{B}^3_{\mathrm{C}}$CCC CCCC CCCC CCCC)
1 段目出力	($\mathrm{CB}^1_{\overline{\mathrm{B}}}\mathrm{B}^1_{\overline{\mathrm{B}}}\mathrm{B}^1_{\overline{\mathrm{B}}}$ CCCC CCCC CCCC)
2 段目出力	(CCCC $\mathrm{B}^2_{\mathrm{U}}\mathrm{B}^2_{\mathrm{U}}\mathrm{B}^2_{\mathrm{U}}$C $\mathrm{B}^2_{\mathrm{U}}\mathrm{CB}^2_{\mathrm{U}}\mathrm{B}^2_{\mathrm{U}}$ $\mathrm{B}^2_{\mathrm{U}}\mathrm{B}^2_{\mathrm{U}}\mathrm{CB}^2_{\mathrm{U}}$)

4.3 S-box 入出力における特異な 3 階差分特性の伝播

表 2 から表 16 より，S-box の入力に対して，一般とは異なる特異な S-box 出力特性を観測した．その特異な特性をまとめて詳細な 1 ビット単位で表 17 に示す．$(\vec{v_i},\vec{v_j},\vec{v_k})^r$ は $(\vec{v_i},\vec{v_j},\vec{v_k})$ を用いた時の r 段目の S-box の入出力特性を表している．例えば，通番 1 では 2 段目の S-box の入出力特性を表している．

表 17 Midori64 の S-box の特異な 3 階差分特性

Table 17 The particular third-order differential characteristics of S-box of Midori64.

通番	$\vec{V}$	入力特性	出力特性
1	$(\vec{v_4},\vec{v_2},\vec{v_1})^2,(\vec{v_{12}},\vec{v_{10}},\vec{v_9})^2$	(B$\overline{\mathrm{B}}$B$\overline{\mathrm{B}}$)	(BUUU)
2	$(\vec{v_8},\vec{v_4},\vec{v_1})^2$	(BBBB)	(UBBB)
3	$(\vec{v_4},\vec{v_2},\vec{v_9})^3,(\vec{v_{12}},\vec{v_2},\vec{v_1})^3,$ $(\vec{v_8},\vec{v_4},\vec{v_1})^4$	(UUUU)	(UUBU)
4	$(\vec{v_8},\vec{v_6},\vec{v_5})^2$	(BBBB)	(BUBU)
5	$(\vec{v_8},\vec{v_2},\vec{v_1})^2,(\vec{v_8},\vec{v_6},\vec{v_1})^2$	($\overline{\mathrm{B}}$$\overline{\mathrm{B}}B\overline{\mathrm{B}}$)	(UBBU)
6	$(\vec{v_8},\vec{v_2},\vec{v_5})^2$	(BBBB)	(UUBU)
7	$(\vec{v_8},\vec{v_4},\vec{v_1})^2$	(BBCB)	(UBBB)
8	$(\vec{v_8},\vec{v_4},\vec{v_3})^2,(\vec{v_8},\vec{v_4},\vec{v_2})^2$	($\overline{\mathrm{B}}$$\overline{\mathrm{B}}B\overline{\mathrm{B}}$)	(UUBB)
9	$(\vec{v_8},\vec{v_2},\vec{v_5})^3$	(UUBU)	(UUBU)

今までの一般的な高階差分特性では，S-box の入力部に 1 ビットでも A 特性にはなっていない B 特性 (つまり，A 特性には含まれない B 特性) や $\overline{\mathrm{B}}$ 特性，U 特性が出現した場合，その出力部の特性は全て U であり，U 以外の特性は出現しなかった．今回は表 17 に示すように，一般とは異なる特異な 3 階差分特性が観測された．例えば，通番 3 では，入力 4 ビット全てが U 特性であるにも関わらず，その出力の内 1 ビットについては B 特性が出現している．

5. 特異な 3 階差分の経路モデル

表 17 に示した特異な特性を理論的に検証するには図 4 に示した経路モデルにおける $X^i=(x^i_3,x^i_2,x^i_1,x^i_0)$，$Y^i=(y^i_3,y^i_2,y^i_1,y^i_0)$ のブール多項式を解析し，3 次項 $t_2t_1t_0$ の係数を導出すれば十分である．例えば表 17 の通番 1 は実際に図 4 の X^2,Y^2 の特性に対応し，通番 9 は X^3,Y^3 の特性に対応している．P は平文 64 ビットの最上位 4 ビット表す．J は 4 ビットの段鍵を表し，K,L,M は 4 ビットの段鍵と差分の影響しないパスからの定数を加算した結果を表す．

$$J=(j_3,j_2,j_1,j_0), \tag{30}$$
$$K=(k_3,k_2,k_1,k_0), \tag{31}$$
$$L=(l_3,l_2,l_1,l_0), \tag{32}$$
$$M=(m_3,m_2,m_1,m_0), \tag{33}$$

とすると，x^i_j,y^i_j は入力変数 t_2,t_1,t_0 の 3 元，鍵変数 16 元の計 19 元の多項式として表現できる．図 4 の X^i と Y^i の関係は式 (3) から (6) で与えられる．

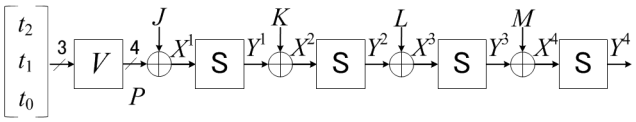

図 4 特異な 3 階差分の経路モデル

Fig. 4 Path model of the third-order differential characteristics.

x^i_j,y^i_j の多項式を解析し，その中の 3 次項 $t_2t_1t_0$ の係数を表 18 から表 31 にまとめて示す．$A^k_{i,j}$ は鍵変数と定数から成る i 元 j 次多項式で，k は通し番号である．表 18 から表 31 の中で 2 つの $A^{k_1}_{i,j},A^{k_2}_{i,j}$ があるとき，$k_1=k_2$ の場合は同一の i 元 j 次多項式を表し，$k_1\neq k_2$ の時は異なる i 元 j 次多項式を表している．表 17 と表 18 から表 31 を比べると分かることは，表 17 で特性が C や B となっているビットについては，そのビットのブール多項式の $t_2t_1t_0$ の係数が表 18 から表 31 ではゼロとなっている．これは $N=2$ について式 (9) が成立していることを示しており，計算機実験と理論解析の結果が一致していることを示している．表 17 で特性が $\overline{\mathrm{B}}$ となっているビットについては，そのビットのブール多項式の $t_2t_1t_0$ の係数が表 18 から 31 では 1 となっている．これは，$N=2$ について式 (8) が成立していることを示しており，計算機実験と理論解析の結果が一致していることを示している．また，表 17 で特性が U となっているビットについては，そのビットの $t_2t_1t_0$ の係数が鍵変数と定数の多項式になっている．これは，鍵や平文の基準値の選び方によって，$t_2t_1t_0$ の係数が 0 となったり 1 となったりして，これに応じてその 3 階差分値も 0 となったり，1 となったりして不定と成ることを表している．従って，これについても計算機実験と理論解析の結果が一致していることが分かる．

表 18 S-box 入出力ビットにおける 3 次項 $t_2t_1t_0$ の係数 (表 17 中の通番 1, $(\vec{v_4},\vec{v_2},\vec{v_1})^2$ に対応)

Table 18 The coefficients of the 3rd-degree term $t_2t_1t_0$ of input and output bits of S-box corresponding to Table 17, #1, $(\vec{v_4},\vec{v_2},\vec{v_1})^2$.

x_3^2	x_2^2	x_1^2	x_0^2	y_3^2	y_2^2	y_1^2	y_0^2
0	1	0	1	0	$A_{3,2}^0$	$A_{2,1}^1$	$A_{3,2}^2$

表 19 S-box 入出力ビットにおける 3 次項 $t_2t_1t_0$ の係数 (表 17 中の通番 1, $(\vec{v_{12}},\vec{v_{10}},\vec{v_9})^2$ に対応)

Table 19 The coefficients of the 3rd-degree term $t_2t_1t_0$ of input and output bits of S-box corresponding to Table 17, #1, $(\vec{v_{12}},\vec{v_{10}},\vec{v_9})^2$.

x_3^2	x_2^2	x_1^2	x_0^2	y_3^2	y_2^2	y_1^2	y_0^2
0	1	0	1	0	$A_{3,2}^3$	$A_{2,1}^4$	$A_{3,2}^5$

表 20 S-box 入出力ビットにおける 3 次項 $t_2t_1t_0$ の係数 (表 17 中の通番 2, $(\vec{v_8},\vec{v_4},\vec{v_1})^2$ に対応)

Table 20 The coefficients of the 3rd-degree term $t_2t_1t_0$ of input and output bits of S-box corresponding to Table 17, #2, $(\vec{v_8},\vec{v_4},\vec{v_1})^2$.

x_3^2	x_2^2	x_1^2	x_0^2	y_3^2	y_2^2	y_1^2	y_0^2
0	0	0	0	$A_{2,1}^6$	0	0	0

表 21 S-box 入出力ビットにおける 3 次項 $t_2t_1t_0$ の係数 (表 17 中の通番 3, $(\vec{v_4},\vec{v_2},\vec{v_9})^3$ に対応)

Table 21 The coefficients of the 3rd-degree term $t_2t_1t_0$ of input and output bits of S-box corresponding to Table 17, #3, $(\vec{v_4},\vec{v_2},\vec{v_9})^3$.

x_3^3	x_2^3	x_1^3	x_0^3	y_3^3	y_2^3	y_1^3	y_0^3
$A_{3,2}^7$	$A_{3,2}^7$	$A_{2,1}^8$	$A_{3,2}^7$	$A_{7,4}^9$	$A_{7,3}^{10}$	0	$A_{7,3}^{11}$

表 22 S-box 入出力ビットにおける 3 次項 $t_2t_1t_0$ の係数 (表 17 中の通番 3, $(\vec{v_{12}},\vec{v_2},\vec{v_1})^3$ に対応)

Table 22 The coefficients of the 3rd-degree term $t_2t_1t_0$ of input and output bits of S-box corresponding to Table 17, #3, $(\vec{v_{12}},\vec{v_2},\vec{v_1})^3$.

x_3^3	x_2^3	x_1^3	x_0^3	y_3^3	y_2^3	y_1^3	y_0^3
$A_{3,2}^{12}$	$A_{3,2}^{12}$	$A_{2,1}^{13}$	$A_{3,2}^{12}$	$A_{7,4}^{14}$	$A_{7,3}^{15}$	0	$A_{7,3}^{16}$

表 23 S-box 入出力ビットにおける 3 次項 $t_2t_1t_0$ の係数 (表 17 中の通番 3, $(\vec{v_8},\vec{v_4},\vec{v_1})^4$ に対応)

Table 23 The coefficients of the 3rd-degree term $t_2t_1t_0$ of input and output bits of S-box corresponding to Table 17, #3, $(\vec{v_8},\vec{v_4},\vec{v_1})^4$.

x_3^4	x_2^4	x_1^4	x_0^4	y_3^4	y_2^4	y_1^4	y_0^4
$A_{6,3}^{17}$	$A_{6,3}^{17}$	$A_{4,2}^{18}$	$A_{6,3}^{17}$	$A_{10,5}^{19}$	$A_{10,4}^{20}$	0	$A_{10,4}^{21}$

表 24 S-box 入出力ビットにおける 3 次項 $t_2t_1t_0$ の係数 (表 17 中の通番 4, $(\vec{v_8},\vec{v_6},\vec{v_5})^2$ に対応)

Table 24 The coefficients of the 3rd-degree term $t_2t_1t_0$ of input and output bits of S-box corresponding to Table 17, #4, $(\vec{v_8},\vec{v_6},\vec{v_5})^2$.

x_3^2	x_2^2	x_1^2	x_0^2	y_3^2	y_2^2	y_1^2	y_0^2
0	0	0	0	0	$A_{2,1}^{22}$	0	$A_{2,1}^{22}$

表 25 S-box 入出力ビットにおける 3 次項 $t_2t_1t_0$ の係数 (表 17 中の通番 5, $(\vec{v_8},\vec{v_2},\vec{v_1})^2$ に対応)

Table 25 The coefficients of the 3rd-degree term $t_2t_1t_0$ of input and output bits of S-box corresponding to Table 17, #5, $(\vec{v_8},\vec{v_2},\vec{v_1})^2$.

x_3^2	x_2^2	x_1^2	x_0^2	y_3^2	y_2^2	y_1^2	y_0^2
1	1	0	1	$A_{3,2}^{23}$	0	0	$A_{2,1}^{24}$

表 26 S-box 入出力ビットにおける 3 次項 $t_2t_1t_0$ の係数 (表 17 中の通番 5, $(\vec{v_8},\vec{v_6},\vec{v_1})^2$ に対応)

Table 26 The coefficients of the 3rd-degree term $t_2t_1t_0$ of input and output bits of S-box corresponding to Table 17, #5, $(\vec{v_8},\vec{v_6},\vec{v_1})^2$.

x_3^2	x_2^2	x_1^2	x_0^2	y_3^2	y_2^2	y_1^2	y_0^2
1	1	0	1	$A_{3,2}^{25}$	0	0	$A_{2,1}^{26}$

表 27 S-box 入出力ビットにおける 3 次項 $t_2t_1t_0$ の係数 (表 17 中の通番 6, $(\vec{v_8},\vec{v_2},\vec{v_5})^2$ に対応)

Table 27 The coefficients of the 3rd-degree term $t_2t_1t_0$ of input and output bits of S-box corresponding to Table 17, #6, $(\vec{v_8},\vec{v_2},\vec{v_5})^2$.

x_3^2	x_2^2	x_1^2	x_0^2	y_3^2	y_2^2	y_1^2	y_0^2
0	0	0	0	$A_{2,1}^{27}$	$A_{2,1}^{27}$	0	$A_{2,1}^{27}$

表 28 S-box 入出力ビットにおける 3 次項 $t_2t_1t_0$ の係数 (表 17 中の通番 7, $(\vec{v_8},\vec{v_4},\vec{v_1})^2$ に対応)

Table 28 The coefficients of the 3rd-degree term $t_2t_1t_0$ of input and output bits of S-box corresponding to Table 17, #7, $(\vec{v_8},\vec{v_4},\vec{v_1})^2$.

x_3^2	x_2^2	x_1^2	x_0^2	y_3^2	y_2^2	y_1^2	y_0^2
0	0	0	0	$A_{2,1}^{28}$	0	0	0

表 29 S-box 入出力ビットにおける 3 次項 $t_2t_1t_0$ の係数 (表 17 中の通番 8, $(\vec{v_8}, \vec{v_4}, \vec{v_3})^2$ に対応)

Table 29 The coefficients of the 3rd-degree term $t_2t_1t_0$ of input and output bits of S-box corresponding to Table 17, #8, $(\vec{v_8}, \vec{v_4}, \vec{v_3})^2$.

x_3^2	x_2^2	x_1^2	x_0^2	y_3^2	y_2^2	y_1^2	y_0^2
1	1	0	1	$A_{3,2}^{29}$	$A_{2,1}^{30}$	0	0

表 30 S-box 入出力ビットにおける 3 次項 $t_2t_1t_0$ の係数 (表 17 中の通番 8, $(\vec{v_8}, \vec{v_4}, \vec{v_2})^2$ に対応)

Table 30 The coefficients of the 3rd-degree term $t_2t_1t_0$ of input and output bits of S-box corresponding to Table 17, #8, $(\vec{v_8}, \vec{v_4}, \vec{v_2})^2$.

x_3^2	x_2^2	x_1^2	x_0^2	y_3^2	y_2^2	y_1^2	y_0^2
1	1	0	1	$A_{3,2}^{31}$	$A_{2,1}^{32}$	0	0

表 31 S-box 入出力ビットにおける 3 次項 $t_2t_1t_0$ の係数 (表 17 中の通番 9, $(\vec{v_8}, \vec{v_4}, \vec{v_5})^3$ に対応)

Table 31 The coefficients of the 3rd-degree term $t_2t_1t_0$ of input and output bits of S-box corresponding to Table 17, #9, $(\vec{v_8}, \vec{v_4}, \vec{v_5})^3$.

x_3^3	x_2^3	x_1^3	x_0^3	y_3^3	y_2^3	y_1^3	y_0^3
$A_{2,1}^{33}$	$A_{2,1}^{33}$	0	$A_{2,1}^{33}$	$A_{5,3}^{34}$	$A_{3,2}^{35}$	0	$A_{3,2}^{36}$

6. 結論

計算機実験により得られた Midori64 の特異な 3 階差分特性をブール多項式を用いて解析し理論的に示した.

参考文献

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

[2] J.Daemen, L.R.Knudsen, and V.Rijmen, “ The block cipher SQUARE ”, FSE ’ 97, LNCS1267, pp.149–165, Springer–Verlag, 1997.

[3] N.Ferguson, J.Kelsey et al., “ Improved Cryptanalysis of Rijndael ”, Lecture Notes in Computer Science, vol.1978, pp.136–141, Springer, 2001

[4] Subhadeep Banik, Andrey Bogdanov, Takanori Isobe, Kyoji Shibutani, Harunaga Hiwatari, Toru Akishita, and Francesco Regazzoni, ”Midori : A Block Cipher for Low Energy ”, ASIACRYPT2015, Part II, LNCS 9453, pp.411–436, 2015