Computer Security Symposium 2019
21 - 24 October 2019

Low-latency ブロック暗号に適した線形層の設計

阪本　光星[1,a)]　峯松　一彦[2]　五十部　孝典[1,3]

概要：FSE 2018 において Alfarano らはブロック暗号 Midori-128 の word 置換が active Sbox 評価と拡散性能において最適であることを示した．本研究では Midori-128 の word 置換を bit 置換に置き換えることにより拡散性能、Active Sbox 評価の観点で更に優れた線形層を示す．まず、Midori-128 の 3 ラウンドの拡散性能を上回る 2.5 ラウンドの拡散性能を持つ bit 置換のクラスを示す．次に、Midori-128 と同じ 3 ラウンドの拡散性能を持ち、Active Sbox 評価によって Midori の 13 ラウンドを上回る 12 ラウンドで安全性を達成可能な bit 置換を示す．置換部の変更のみであるため，Midori-128 とハードウェアのサイズは同じである．

キーワード：Low-latency ブロック暗号, 拡散性能, Active Sbox, MILP, bit 置換

Design of Permutation Layers in Low-latency Block Ciphers

Kosei Sakamoto[1,a)]　Kazuhiko Minematsu[2]　Takanori Isobe[1,3]

Abstract: In FSE 2018, Alfarano et al. showed that a word permutation of Midori-128 is optimal in term of full diffusion property and the minimal number of active Sboxes. In this paper, by replacing the word permutation to the bit permutation, we explore more efficient permutation in term of full diffusion property and the number of active Sboxes. First, we show a class of bit permutations that achieves 2.5 round full diffusion property while Midori-128 requires 3 round. Next, we show a class of bit permutations that achieves 3 round full diffusion property as Midori-128, and 12 round security by active S-box which exceeds 13 round security of Midori-128.

Keywords: Low-latency block cipher, full diffusion property, Active Sbox, MILP, bit permutation

1. はじめに

IoT 社会の発達にともない，より少ない遅延で暗号化を行う 128 bit Low-latency ブロック暗号が必要とされている．これまで行われてきた Low-latency ブロック暗号の研究の中で，Sbox とマトリックスについては十分な検討が行われているが，128 bit ブロックでの線形層における最適な置換の検討は十分に行われていない [2–4]．ASIACRYPT 2015 において，Banik らは低電力，低遅延な軽量ブロック暗号 Midori-128 [3] を提案した．Midori-128 は 2 つの 4 bit Sbox から構成される 8 bit Sox と分岐数 4 の 4×4 バイナリマトリックスを使用することで，word 置換で 3 ラウンドの順方向/逆方向の拡散性能を実現し，Active Sbox 評価において，13 ラウンドで差分/線形攻撃に対して安全な暗号である．FSE 2018 において，Alfarano らにより，Active Sbox 評価の観点で Midori-128 に使用されている置換が word 置換において最適であることが示された [1]．最適な置換の検討はラウンド数の削減に直結するため，Low-latency ブロック暗号の設計において非常に重要である．

本稿では 128 bit Low-latency ブロック暗号の線形層における最適な置換の検討を行う．具体的には，Alfarano らが検討していない bit 置換について検討し，拡散性能と MILP

[1] 兵庫県立大学
University of Hyogo
[2] 日本電気株式会社
NEC Corporation
[3] 情報通信研究機構
National Institute of Information and Communications Technology
[a)] k.sakamoto0728@gmail.com

による Active Sbox 評価において Midori-128 より優れた構成を提案する．結果として，4 bit Sbox と 4×4 バイナリマトリックスからなる 128bit ブロック暗号の構成において最適な拡散性能は順方向/逆方向で 2.5 ラウンドであることを示し，実際に 2.5 ラウンドの拡散性能を達成する bit 置換のクラスを示す．次に，順方向/逆方向で Midori-128 と同じ 3 ラウンドの拡散性能を実現し Active Sbox 評価において Midori-128 より少ない 12 ラウンドで差分/線形攻撃に対して安全な構造を発見した．ハードウェアにおいては，word 置換と bit 置換にはゲートサイズの違いはないため，提案する構成は Midori-128 より軽量性，Low-latency の観点で優れている．

本稿の構成は以下の通りである．まず第 2 章で本研究に関する予備知識である拡散性能と MILP による Active Sbox 評価について説明する．第 3 章で Midori-128 の構成を説明し，第 4 章で本研究で検討を行う構成について説明する．第 5 章と第 6 章で最適な拡散性能を持つ置換とその置換の MILP による Active Sbox 評価について述べ，第 7 章で Midori-128 より最適な構成を示し，第 8 章でまとめを述べる．

2. 準備

本章では，本研究に関する予備知識として，拡散性能，Active Sbox による差分/線形攻撃に対する安全性の評価，混合整数線形計画法 (Mixed Integer Linear Programing, MILP) を用いた Active Sbox 数の評価方法 [7] について説明する．

2.1 拡散性能

拡散性能はブロック暗号の安全性を保障する上で重要な性質である．特に，不能差分攻撃，Integral 攻撃などの代表的な攻撃法に対する安全性において非常に大きな影響を持つ．そのためブロック暗号を設計する際は，拡散性能が最適となるよう設計することが望まれる．

拡散性能については FSE 2010 において洲崎らが詳しく説明している [9]．ブロック長が b bit のブロック暗号の入力平文を $(a_0, a_1, \cdots, a_{b-1}) \in \{0,1\}^1$ とする．拡散性能はある入力平文の a_x のみに差分を立て，その差分が b bit 全てに到達するラウンド数で定義される DR_x の最大値である DR_{max} によって評価される．DR_{max} は以下の式で定義される．

$$DR_{max} = \max_{x=0,\cdots,b-1} DR_x$$

DR_{max} は平文に 1 bit の差分を与えたときの拡散性能である暗号化方向 (順方向) と暗号文に 1 bit の差分を与えたときの拡散性能である復号方向 (逆方向) を評価する必要がある．順方向と逆方向の両方において，より少ないラウンドの拡散性能，すなわち，より小さい DR_{max} を持つほど不能差分攻撃などに対する安全性は向上する．したがって，より小さい DR_{max} を持つほど，拡散性能は良い．

2.2 Active Sbox による差分/線形攻撃の安全性の評価

差分/線形攻撃はブロック暗号に対する最も基本的な攻撃法である．b bit ブロック暗号 f についての差分/線形攻撃に対する安全性の評価を行う場合，以下の式で定義される差分確率 (DP_f) と線形確率 (LP_f) を導出し，それらの最大値である最大差分/線形確率を用いて評価する．なお，Δx と Δy は入力/出力差分，Γx と Γy は入力/出力マスクである．

$$DP_f(\Delta x, \Delta y) = \frac{\#\{x \in \{0,1\}^b | f(x) \oplus f(x \oplus \Delta x) = \Delta y\}}{2^b}$$

$$LP_f(\Gamma x, \Gamma y) = \left(2\frac{\#\{x \in \{0,1\}^b | x \bullet \Gamma x = f(x) \bullet \Gamma y\}}{2^b} - 1\right)^2$$

比較的ブロック長 b が小さい場合，最大差分/線形確率を求めることは容易であるが，現在提案されている多くのブロック暗号が持つブロック長 64/128 bit においては現実的な時間で最大差分/線形確率を導出することはできない．そこで，実際の評価の際は最大差分/線形確率の近似値として最大差分/線形特性確率 (DCP_{fmax} / LCP_{fmax}) が用いられる．これらは各ラウンドの差分/線形特性確率 (DP_f / LP_f) の積で定義される．

$$DCP_f = \prod_{R=1}^{r} DP_f(\Delta x_R, \Delta x_{R+1})$$

$$LCP_f = \prod_{R=1}^{r} LP_f(\Gamma x_R, \Gamma x_{R+1})$$

$$DCP_{fmax} = \max_{\substack{\Delta x_1 \neq 0 \\ \Delta x_2, \ldots, \Delta x_{r+1}}} DCP_f$$

$$LCP_{fmax} = \max_{\substack{\Gamma x_1 \neq 0 \\ \Gamma x_2, \ldots, \Gamma x_{r+1}}} LCP_f$$

一般的に差分/線形攻撃に対する安全性の評価を行う際，Active Sbox による安全性の評価が行われる．Sbox への入力差分/マスクが非 0 であるとき，その Sbox を Active Sbox と呼ぶ．差分/線形特性確率は系全体の Active Sbox の最大差分/線形確率の積で抑えられる．遷移する可能性のあるすべての差分/線形マスクのパスを考慮し，Active Sbox 数の下界を評価することで，差分特性確率の上界を評価することができる．一般的に，ブロック暗号に含まれる Active Sbox の数を保証する方法には 2 種類ある．1 つは証明などで示された Active Sbox 数の下界を用いる方法，もう 1 つは探索アルゴリズムにより，Active Sbox 数の下界を評価する方法である．本稿では 2 つ目の探索アルゴリズムにより，Active Sbox 数の下界を評価する方法を用いる．

2.3 混合整数線形計画法を用いた安全性の評価

混合整数線形計画法 (Mixed Integer Linear Programming，MILP) では，ある変数に対して線形式で与えられる制約式の下，線形式で与えられる目的関数を最適化 (最大化もしくは最小化) する変数の値を探索する．Mouha らが提案した手法 [7] では，まず暗号内部の各演算を線形式で表現し，制約式として与える．そして目的関数として Active Sbox の合計数を与え，最小化することにより Active Sbox の最小数を得る．本稿では MILP ソルバーとして Gurobi Optimizer [5] を用い，Mouha らと同様の手法を用いて，安全性の評価を行う．

3. ブロック暗号 Midori-128

ブロック暗号 Midori-128 [3] は ASIACRYPT 2015 において，Banik らが提案した低電力，低遅延な軽量ブロック暗号である．

3.1 Midori-128 の仕様

Midori-128 は 16 分割の SPN 構造を持つブロック暗号であり，ブロック長は 128 bit，鍵長が 128 bit，ラウンド数は 20 である．ラウンド関数は 8 bit Sbox，word 置換，Mixcolumn，Addkey で構成されている．Midori-128 のラウンド関数について説明する．平文，暗号文，鍵を $(M, C, K) \in \{0,1\}^{128}$ とする．平文，暗号文，鍵は以下の式の通り，8 bit の word に分割される．

$$
\begin{aligned}
M &= (M_0, M_1, M_2, \cdots, M_{15}), & M_i &\in \{0,1\}^8 \\
C &= (C_0, C_1, C_2, \cdots, C_{15}), & C_i &\in \{0,1\}^8 \\
K &= (K_0, K_1, K_2, \cdots, K_{15}), & K_i &\in \{0,1\}^8
\end{aligned}
$$

r ラウンドにおける中間値を $(X_0^r, \cdots, X_{15}^r) \in \{0,1\}^8$，ラウンド鍵を $(RK_0^r, \cdots, RK_{15}^r) \in \{0,1\}^8$ とする．Midori-128 のラウンド関数のアルゴリズムを図 2，ラウンド関数を図 1に示す．

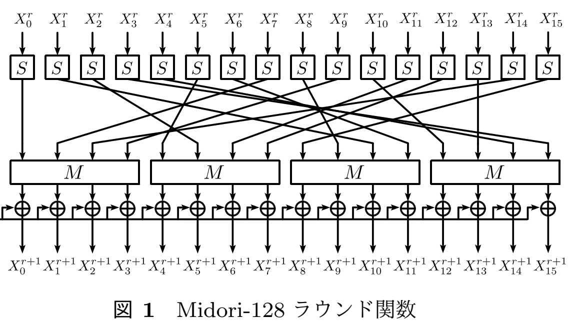

図 1　Midori-128 ラウンド関数

ここで π は表 1に示す word 置換である．また，S，M は以下で説明する 8 bit Sbox，Mixcolumn の演算である．

Sbox　図 3に使用している 8 bit Sbox の一例を示す．内部では 4 bit Sbox が並列に接続されており，その入出力に bit 置換が使用されている．4 bit Sbox の最大差分/線形確率は共に 2^{-2} であり，任意の入力差分に対して確率的に出力 4 bit 全てに差分が拡散する Full diffusion 性を有する．また，4 bit Sbox，bit 置換は共に自分自身をその逆として持つ写像である Involution 性を有している．したがって，8 bit Sbox 全体としても Involution 性を有している．Midori-128 では Full diffusion 性と Involution 性を有する 4 bit Sbox と bit 置換から構成される 4 種類の 8 bit Sbox を使用している．

Algorithm Midori-128 ラウンド関数

for $i \leftarrow 0$ to 15
　do $X_i^1 \leftarrow M_i \oplus K_i$
for $r \leftarrow 1$ to 19
　for $i \leftarrow 0$ to 15
　　$X_i^r \leftarrow S(X_i^r)$
　　$X_{\pi i}^r \leftarrow X_i^r$
　for $h \leftarrow 0$ to 4
　　$(X_{4i}^r, X_{4i+1}^r, X_{4i+2}^r, X_{4i+3}^r)$
　　　$\leftarrow M(X_{4i}^r, X_{4i+1}^r, X_{4i+2}^r, X_{4i+3}^r)$
　for $i \leftarrow 0$ to 15
　　$X_i^{r+1} \leftarrow X_i^r \oplus RK_i^r$
for $i \leftarrow 0$ to 15
　$X_i^r \leftarrow S(X_i^r)$
for $i \leftarrow 0$ to 15
　$C_i \leftarrow X_i^r \oplus K_i$

図 2　Midori-128 のラウンド関数アルゴリズム

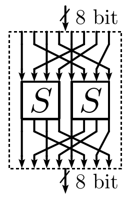

図 3　Midori-128 の 8 bit Sbox の一例

Mixcolumn　Mixcolumn の演算は Sbox と同様に Involution 性を有するバイナリマトリックスを使用している．Mixcolumn の入力を $(x_0, x_1, x_2, x_3) \in \{0,1\}^8$，出力を $(y_0, y_1, y_2, y_3) \in \{0,1\}^8$ とする．Mixcolumn における演算は以下の式の通りである．

$$
M = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}
$$

$$
\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}
\begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix}
=
\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{pmatrix}
$$

3.2 Midori-128 の拡散性能と Active Sbox 数

Midori-128 の拡散性能と Active Sbox の最小数について述べる．Midori-128 に使用されている 8 bit Sbox は最大差分/線形確率が 2^{-2} である 4 bit Sbox から構成されている．したがって，Active Sbox 評価において 64 の Active Sbox を保証すれば差分/線形攻撃に対して安全である．Midori-128 は 13 ラウンドで Active Sbox の最小数が 64 に達し，差分/線形攻撃に対して耐性を持つ．拡散性能につ

表 1　Midori-128 word 置換

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\pi\ (x)$	0	10	5	15	14	4	11	1	9	3	12	6	7	13	2	8

いては順方向/逆方向ともに $DP_{max} = 3$ である．また，FSE 2018 において，Alfarano らにより，Active Sbox 評価の観点で Midori-128 に使用されている置換が word 置換において最適であることが示されている [1].

4.　検討する Low-latency ブロック暗号の構成

本節では検討を行う Low-latency ブロック暗号の構成について説明する．そして，その構成を等価変形し，MILP を用いた Active Sbox 評価を適用可能にする方法について説明する．

4.1　全体構造

図 5に検討を行う 128 bit ブロック暗号の r ラウンドにおけるラウンド関数を示す．P は検討する置換であり，r ラウンドにおけるラウンド鍵を RK^r，Sbox を S^r_n，バイナリマトリックスを M^r_m とする．ここで，$n\ (0 \leq n \leq 31)$ は Sbox の位置，$m\ (0 \leq m \leq 7)$ はマトリックスの位置である．以下に Sbox，Mixcolumn について説明する．

Sbox　Midori-128 と同様に Full diffusion 性と Involution 性を有する 4 bit Sbox を使用する．

Mixcolumn　Midori-128 と同様に Involution 性を有する 4×4 バイナリマトリックス M を使用する．M^r_m の入力 16 bit を $(Mi^r_{8m}, Mi^r_{8m+1}, \cdots Mi^r_{8m+15}) \in \{0,1\}^1$，出力 16 bit を $(Mo^r_{8m}, Mo^r_{8m+1}, \cdots Mo^r_{8m+15}) \in \{0,1\}^1$ とする．ここで，図 4にマトリックスの入出力 bit と入出力 nibble の関係を示す．

本研究では，図 5に示す構成について Alfarano らが検討していない bit 置換の検討を行い，拡散性能と Active Sbox 評価の観点で Midori-128 より優れている構成を提案する．

4.2　MILP による Active Sbox 評価が可能な bit 置換への変換

本研究では図 5の構成に関して MILP を用いた Active Sbox の最小数の探索を行う．

一般的に，MILP による Active Sbox の評価を行う際，評価を行うブロック暗号の線形層の置換が word/nibble 置換で構成されている場合，word/nibble サイズの切詰差分/線形マスクによる評価を行うことにより，短時間で Active Sbox の最小数を探索することができる．しかし，bit 置換においては，入力空間と制約式の数が word/nibble 置換の評価と比べ急激に増加することから，現実的な時間で Active Sbox の最小数を探索することができない．そこで，bit 置換の検討を行う際，現実的な時間で MILP による Active Sbox 評価を可能にするために，図 5の構成を，図 6に示す構成に変換する．

図 5で示した 1 ラウンドあたりのラウンド関数を E，図 6で示した 1 ラウンドあたりのラウンド関数を E_c，nibble 置換を P_n，bit 置換を P_b，Sbox を S，Mixcolumn を M とする．図 5と図 6はそれぞれ $E = M \circ P \circ S$ と $E_c = M \circ P_b \circ S \circ P_n$ と表現される．ここで，P を $P = P_b \circ P_n$ を満たす bit 置換 P_b と nibble 置換 P_n に分解すると $E = M \circ P_b \circ P_n \circ S$ と表現される．E と E_c における S は 4 bit Sbox であるため，nibble 置換 P_n に対して $P_n \circ S = S \circ P_n$ が成立する．したがって $E = M \circ P_b \circ S \circ P_n$ となり，$E = E_c$ の等価変形が成立する．

本研究では bit 置換の検討を行う際，図 7に示す 2 種類の bit 置換 P_{b1} と P_{b2} について MILP による Active Sbox 評価を行い，最適な nibble 置換 P_{n1} と P_{n2} の探索を行う．拡散性能を向上するために，P_{b1} は任意の $(S^r_{4m}, S^r_{4m+1}, S^r_{4m+2}, S^r_{4m+3})$ に 1 bit 以上の Active bit が入力されたとき，M^r_m の出力 4 nibble が全て Active になりえる．P_{b2} は任意の $(S^r_{8l}, S^r_{8l+1}, S^r_{8l+2}, S^r_{8l+3}, S^r_{8l+4}, S^r_{8l+5}, S^r_{8l+6}, S^r_{8l+7})$ に 1 bit 以上の Active bit が入力されたとき，(M^r_{2l}, M^r_{2l+1}) の出力 8 nibble が全て Active になりえる．ここで，$l\ (0 \leq l \leq 3)$ は 2 組のマトリックス M の位置であり，P_{b1} における nibble 置換が P_{n1}，P_{b2} における nibble 置換が P_{n2} である．また，P_{n1} と P_{n2} の入力をそれぞれ $(s_m, \cdots, s_{m+3})$ と $(s_{8l}, \cdots, s_{8l+7})$ とする．この bit 置換 P_{b1} と P_{b2} を使用することにより，Sbox，bit 置換，Mixcolumn を 1 つの演算 $SBM = M \circ P_{b1} \circ S$ と $SBM' = M \circ P_{b1} \circ S$ と見なすことができる．したがって，ラウンド関数を $E_c = SBM \circ P_{n1}$，$E_c = SBM' \circ P_{n2}$ とみなすことができ，nibble サイズの切詰差分での MILP による Active Sbox 評価が可能となる．このとき，最適な nibble 置換 P_n の探索空間は P_{b1} と P_{b2} のそれぞれにおいて 32! $(\approx 2^{117.66})$ となる．

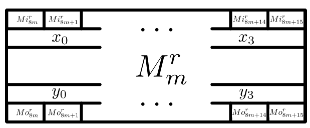

図 4　マトリックスの入出力 bit と入出力 nibble の関係

5.　拡散性能の観点における最適な置換の検討

本章では図 4で述べた構成について，拡散性能の観点で最適な置換の検討を行う．まず，図 5の P が任意の bit 置換である構成及び P が任意の nibble 置換である構成と図

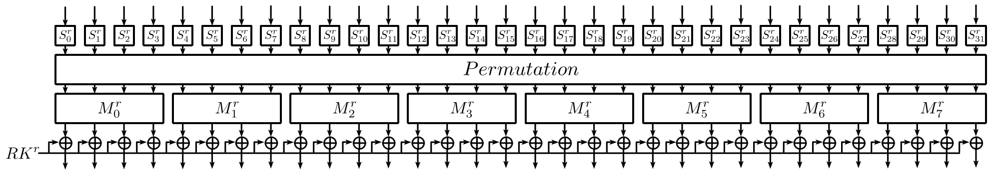

図 5　検討する 128 bit ブロック暗号の構成

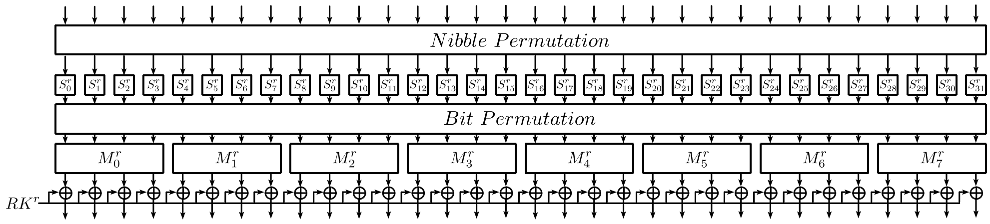

図 6　等価変形後の図 5

6の bit 置換 P_{b1} と P_{b2} の構成における最適な拡散性能について考察する．次に P_{b1} と P_{b2} の構成に対して MILP による Active Sbox 評価が可能である 2.5 ラウンドの拡散性能を持つ置換のクラスと，Midori-128 と同じ 3 ラウンドの拡散性能を持つ置換のクラスを示す．

5.1　最適な拡散性能

図 5の P が任意の bit 置換である構成及び P が任意の nibble 置換である構成と図 6の bit 置換 P_{b1} と P_{b2} の構成について暗号内部の Active bit 数について検討を行う．本稿では，注目する bit/nibble に差分がある場合，その bit/nibble は Active であるという．表 2に順方向における各操作 (Sbox，Mixcolumn) 後の Active bit 数の上界を示し，表 3に逆方向における各操作 (Mixcolumn，Sbox) 後の Active bit 数の上界を示す．ここで，表 2と表 3は Active bit 数の上界を見積るので Sbox については入力 1 Active bit に対して出力 4 Active bit を保証する．また Mixcolumn については入力 1 Active bit に対して出力 3 Active bit 以上を保証する．なお，置換に関しては操作の前後で Active bit 数は変化しないので省略する．

表 2　各操作後の Active bit 数の上界 (順方向)

r	操作	bit 置換	nibble 置換	P_{b1}	P_{b2}
-	平文差分	1	1	1	1
1	Sbox	4	4	4	4
1	Mixcolumn	12	12	12	20
2	Sbox	48	12	16	32
2	Mixcolumn	120	36	48	80
3	Sbox	**128**	36	64	**128**
3	Mixcolumn	**128**	100	**128**	**128**

表 2と表 3より，図 5の任意の bit 置換において最適な拡散性能は順方向/逆方向でそれぞれ $DP_{max} = 2.5$ と $DP_{max} = 2.5$ である．また，図 5の任意の nibble 置換において，Midori-128 が持つ $DP_{max} = 3$ の順方向/逆方向の拡散性能を上回る構成は存在しない．

表 3　各操作後の Active bit 数の上界 (逆方向)

r	操作	bit 置換	nibble 置換	P_{b1}	P_{b2}
-	暗号文差分	1	1	1	1
1	Sbox	4	4	4	4
1	Mixcolumn	12	12	12	12
2	Sbox	36	12	16	32
2	Mixcolumn	112	36	48	96
3	Sbox	**128**	100	64	**128**
3	Mixcolumn	**128**	100	**128**	**128**

5.2　P_{b1} における最適な拡散性能を持つ P_{n1} の検討

図 6の P_{b1} の構成について順方向/逆方向ともに $DP_{max} = 3$ を満たす P_{n1} の検討を行う．本稿では，図 7の P_{b1} と P_{b2} について P_{n1} と P_{n2} に入力されるステート $(s_1, s_2 \cdots, s_{31})$ を 4×8 の行と列からなるステートとし，nibble 置換 P_{n1} と P_{n2} はこれらをシャッフルする．図 8に 4×8 のステート $(s_1, s_2 \cdots, s_{31})$ を示す．

ここで，P_{b1} における順方向と逆方向の拡散性能が $DP_{max} = 3$ を達成するための P_{n1} の必要十分条件は以下の通りである．

順方向 $DP_{max} = 3$ 必要十分条件　図 6の構成における P_{b1} について，順方向の拡散性能が $DP_{max} = 3$ を達成するための nibble 置換 P_{n1} の必要十分条件は，任意の 1 bit の入力差分に対して各 $S^3_{4m}, S^3_{4m+1}, S^3_{4m+2}, S^3_{4m+3}$ が少なくとも 2 つ以上 Active となる nibble 置換を使用することである．

逆方向 $DP_{max} = 3$ 必要十分条件　図 6の P_{b1} の構成について，逆方向の拡散性能が $DP_{max} = 3$ を達成するための nibble 置換 P_{n1} の必要十分条件は，任意の 1 bit の出力差分に対して各 M^{r-2}_m の出力 4 nibble が少なくとも 2 つ以上 Active となる nibble 置換を使用することである．

これら両方の必要十分条件を満たす P_{n1} の条件を条件 1. に示す．

条件 1.　図 8において，全ての列について重複のない任意の 2 列の全 8 ステートが P_{n1} を適用後，1 ステートず

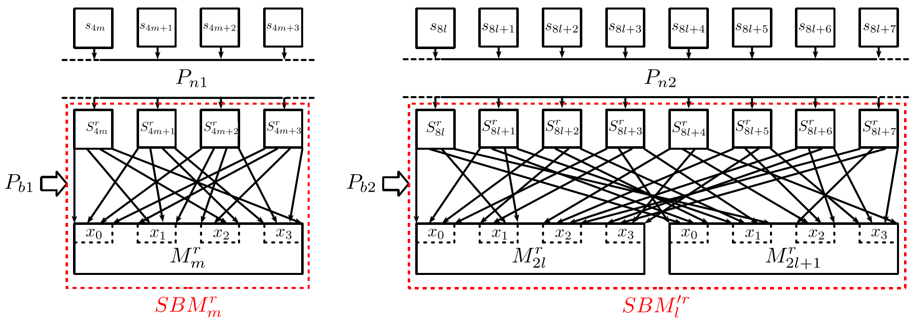

図 7　bit 置換 P_{b1}，P_{b2}

表 4　nibble 置換 $P_{n1'}$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$P_{n1'}(x)$	0	4	8	12	16	20	24	28	1	5	9	13	17	21	25	29
x	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$P_{n1'}(x)$	2	6	10	14	18	22	26	30	3	7	11	15	19	23	27	31

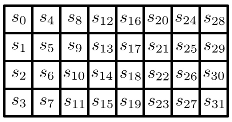

図 8　4×8 のステート

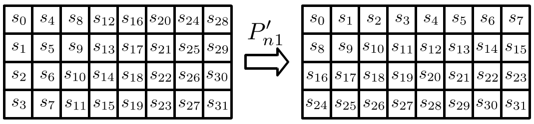

図 9　nibble 置換 P'_{n1}

つ全 8 列の任意の行に写像される．

表 4と図 9に条件 1. を満たす P'_{n1} の一例を示す．図 6の P_{b1} の構成において，条件 1. を満たす順方向/逆方向の拡散性能が $DP_{max} = 3$ である P_{n1} の総数は $\binom{8}{2} \times \binom{6}{2} \times \binom{4}{2} \times \binom{2}{2} \times (8!)^4$ $(\approx 2^{73.50})$ である．

5.3　P_{b2} における最適な拡散性能を持つ P_{n2} の検討

図 6の P_{b2} の構成ついて順方向/逆方向ともに $DP_{max} = 2.5$ を満たす P_{n2} の検討を行う．

ここで，P_{b2} における順方向と逆方向の拡散性能が $DP_{max} = 2.5$ を達成するための P_{n2} の必要十分条件は以下の通りである．

順方向 $DP_{max} = 2.5$ 必要十分条件　図 6の構成における P_{b2} について，順方向の拡散性能が $DP_{max} = 2.5$ を達成するための nibble 置換 P_{n2} の必要十分条件は，任意の 1 bit の入力差分に対して各 $S^2_{8l}, S^2_{8l+1}, S^2_{8l+2}, S^2_{8l+3}, S^2_{8l+4}, S^2_{8l+5}, S^2_{8l+6}, S^2_{8l+7}$ が少なくとも 1 つ以上 Active となる nibble 置換を使用することである．

逆方向 $DP_{max} = 2.5$ 必要十分条件　図 6の構成における P_{b2} について，逆方向の拡散性能が $DP_{max} = 2.5$ を達成するための nibble 置換の必要十分条件は，任意の 1 bit の出力差分に対して各 $(M^{r-2}_{2l}, M^{r-2}_{2l+1})$ の出力 8 nibble のうち少なくとも 1 つ以上 Active となる nibble 置換を使用することである．

これら両方の必要十分条件を満たす P_{n2} の条件を条件 2. に示す．

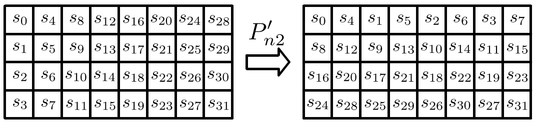

図 10　nibble 置換 P'_{n2}

条件 2.　図 8のにおいて，各 $(2l, 2l+1)$ 列の全 8 ステートについて P_{n2} を適用後，各 $(2l, 2l+1)$ 列内の任意の列と行に少なくとも 1 ステート以上が写像される．

表 5と図 10に条件 2. を満たす P'_{n2} の一例を示す．図 6の P_{b2} の構成において，条件 2. を満たす順方向/逆方向の拡散性能が $DP_{max} = 2.5$ である P_{n2} の総数は $({}_8P_4 \times 4! \times 8 \times 7 \times 6 \times 5)^4$ $(\approx 2^{104.05})$ である．

6.　Active Sbox 評価における最適な置換の検討

本章では，条件 1. と条件 2. を満たす P_{n1} と P_{n2} について MILP による nibble サイズの Active Sbox 評価 [7] を行い，Midori-128 を上回る，12 ラウンド以下で Active Sbox の最小数が 64 を上回る構成を探索する．まず，P_{b1} と P_{b2} の構成における MILP による nibble サイズの切詰差分/線形マスクの伝搬モデルのモデリング方法について説明する．そして条件 2. を満たす P_{n2} の構成の MILP による Active Sbox 数の上界を示すことにより，Acive Sbox 評価の観点で Midori-128 を上回ることがないことを示す．最後に，条件 1. を満たす P_{n1} の構成において，MILP による Active Sbox 評価の観点で Midori-128 を上回る 12 ラウンドで Active Sbox の最小数が 64 に達する構成を示す．なお，本研究で検討する構造では，MILP 評価における nibble

表 5　nibble 置換 $P_{n2'}$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$P_{n1'}(x)$	0	8	16	24	4	12	20	28	1	9	17	25	5	13	21	29
x	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$P_{n1'}(x)$	2	10	18	26	6	14	22	30	3	11	19	27	7	15	23	31

表 6　P_{b2}，P_{n2} の構成について各ラウンドごとの active Sbox の最小数 ($DP_{max} = 2.5$)

ラウンド	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
AS	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60	**64**

サイズの切詰差分/線形マスクの伝搬は等価であるため，以降では区別しない．

6.1　差分伝搬のモデリング方法

一般的に，SPN 構造の MILP による nibble サイズの切詰差分の伝搬のモデリングを行う際，差分が遷移する可能性がある操作 (Sbox，置換，Mixcolumn) の入出力に変数を与える．そして，各ラウンドの Sbox，置換，Mixcolumn をそれらの変数を用いて制約式として与え，Sbox の入力に与えた変数を最小化することにより Active Sbox の最小数を得る．本研究では，図 6の評価を行うため，図 7の各 nibble 置換，MBS，MBS' の入出力に変数を与える．そして，それらの演算についての制約式を与え，Sbox の入力に与えた変数を最小化することにより，Active Sbox の最小数を得る．P_{b1} と P_{b2} における MBS と MBS' の制約式についてそれぞれ説明する．

$\boldsymbol{P_{b1}}$　図 7の P_{b1} の構成を Sbox，P_{b1}，バイナリマトリックスから構成される 4 nibble 入力，4 nibble 出力の 1 つの演算 SBM_m^r とみなし，新たに制約式を与える．このとき，[8] と同様の方法を用いることで，SBM_m^r の制約式は 21 の不等式で表現される．したがって，r ラウンドにおけるラウンド関数全体の制約式は P_{n1}，SBM_m^r の制約式から構成することができる．

$\boldsymbol{P_{b2}}$　図 7の P_{b2} の構成を Sbox，P_{b2}，バイナリマトリックスから構成される 8 nibble 入力，8 nibble 出力の 1 つの演算 $SBM_l'^r$ とみなし，新たに制約式を与える．本稿では，bit 置換と Mixcolumn の制約式から $SBM_l'^r$ の制約式を構成する．ここで，bit 置換については，Full diffusion 性を持つ各 $S_{8l}^r, S_{8l+1}^r, S_{8l+2}^r, S_{8l+3}^r, S_{8l+4}^r, S_{8l+5}^r, S_{8l+6}^r, S_{8l+7}^r$ の各出力 4 bit が M_{2l}^r, M_{2l+1}^r の入力 4 nibble のそれぞれ 2 nibble に入力されていることから，各 $S_{8l}^r, S_{8l+1}^r, S_{8l+2}^r, S_{8l+3}^r, S_{8l+4}^r, S_{8l+5}^r, S_{8l+6}^r, S_{8l+7}^r$ についてそれぞれ 1 nibble 入力，4 nibble 出力の演算とみなすことができる．この演算は 6 の不等式で表現される．また，バイナリマトリックス M については 13 の制約式で表現される [6]．よって，$SBM_l'^r$ は $6 \times 8 + 13 + 13 = 74$ の制約式で表現される．したがって，r ラウンドにおけるラウンド関数全体の制約式は P_{n2}，$SBM_l'^r$ の制約式から構成することができる．

6.2　$\boldsymbol{P_{b2}}$ の構成についての Active Sbox の最小数の上界

本節では条件 2. を満たす，P_{b2} と P_{n2} の構成について MILP による Active Sbox 評価による各ラウンドごとの Active Sbox の最小数の上界を示す．ここで，条件 2. を満たす，P_{b2} と P_{n2} の構成について 1 ラウンドにおける，Active Sbox 数について以下の命題を与える．

命題 1.　条件 2. を満たす P_{b2}，P_{n2} の構成について，特定の 2 組の $\{(S_{8l}^1, S_{8l+1}^1, S_{8l+2}^1, S_{8l+3}^1), (S_{8l+4}^1, S_{8l+5}^1, S_{8l+6}^1, S_{8l+7}^1)\}$ のそれぞれが 1 Active，すなわち合計で 4 Active である場合，以降のラウンドについて 1 ラウンドにおける Active Sbox の最小数の上界は 4 となる．

証明　$(S_{8l}^r, S_{8l+1}^r, S_{8l+2}^r, S_{8l+3}^r)$ と $(S_{8l+4}^r, S_{8l+5}^r, S_{8l+6}^r, S_{8l+7}^r)$ のそれぞれが 1 以上 Active である場合，$(M_{2l}^r,\ M_{2l+1}^R)$ の出力 8 nibble は合計して 1 Active 以上となる任意の Active nibble をとりえる．また，条件 2. より，各 (M_{2l}^r, M_{2l+1}^r) の出力 8 nibble は各 $(S_{8l}^{r+1}, S_{8l+1}^{r+1}, S_{8l+2}^{r+1}, S_{8l+3}^{r+1}, S_{8l+4}^{r+1}, S_{8l+5}^{r+1}, S_{8l+6}^{r+1}, S_{8l+7}^{r+1})$ に少なくとも 1 つ以上必ず接続されている．したがって，各ラウンドにおいて，2 組の $(M_{2l}^r,\ M_{2l+1}^r)$ の出力 nibble が 2 組の $\{(S_{8l}^{r+1}, S_{8l+1}^{r+1}, S_{8l+2}^{r+1}, S_{8l+3}^{r+1}), (S_{8l+4}^{r+1}, S_{8l+5}^{r+1}, S_{8l+6}^{r+1}, S_{8l+7}^{r+1})\}$ のそれぞれに接続されている $(M_{2l}^r,\ M_{2l+1}^r)$ と $\{(S_{8l}^{r+1}, S_{8l+1}^{r+1}, S_{8l+2}^{r+1}, S_{8l+3}^{r+1}), (S_{8l+4}^{r+1}, S_{8l+5}^{r+1}, S_{8l+6}^{r+1}, S_{8l+7}^{r+1})\}$ が必ず存在する．よって，条件 2. を満たす P_{b2}，P_{n2} の構成について，特定の 2 組の $\{(S_{8l}^1, S_{8l+1}^1, S_{8l+2}^1, S_{8l+3}^1), (S_{8l+4}^1, S_{8l+5}^1, S_{8l+6}^1, S_{8l+7}^1)\}$ のそれぞれが 1 Active，すなわち合計で 4 Active である場合，以降のラウンドについて 1 ラウンドにおける Active Sbox の最小数の上界は 4 となる．

命題 1. より，条件 2. を満たす P_{b2}，P_{n2} の構成について各ラウンドごとの Active Sbox の最小数の上界を表 6に示す．表 6より，条件 2. を満たす，P_{b2}，P_{n2} の構成について Active sbox 評価の観点で Midori-128 を上回る構成は存在しない．

6.3　$\boldsymbol{P_{b1}}$ の構成についての Active Sbox 評価

P_{b1} と P_{n1}' の構成について，各ラウンドにおける Active Sbox の最小数を表 7に示す．なお，本研究では MILP による 9 ラウンド以降の Active Sbox 数の探索は不可能であっ

表 **7**　P_{b1}，$P_{n1'}$ の構成についての各ラウンドにおける Active Sbox の最小数

ラウンド	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
AS 数	1	4	7	16	20	32	36	44	-		-	**64**	-	72	-	88

表 **8**　各構成についての拡散性能および，各ラウンドにおける Active Sbox 数の比較

構成	拡散性能	ラウンド	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Midori-128	$DC_{max} = 3$	AS 数	-	-	-	16	23	30	35	38	41	50	57	62	**67**	72	75	84
P_{b1}，$P_{n1'}$	$DC_{max} = 3$	AS 数	1	4	7	16	20	32	36	44	-	-	-	**64**	-	72	-	88
P_{b2}，P_{n2}	$DC_{max} = 2.5$	AS 数	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60	**64**

ため，9 ラウンド以降の Active Sbox 数は $r/2$ ラウンドの結果を 2 倍したものである．

P_{b1} と P'_{n1} の構成は 12 ラウンドで Active Sbox の最小数が 64 に達する．これは Active Sbox 評価の観点において Midori-128 の 13 ラウンドを上回る．

7. 各構成の比較検討

本章では，拡散性能，Active Sbox 評価の観点で Midori-128，P_{b1} と P'_{n1} の構成，P_{b2} と P_{n2} の構成の比較を行い，より最適な構成を決定する．

Midori-128，P_{b1} と P'_{n1} の構成，P_{b2} と P_{n2} の構成における拡散性能と各ラウンドごとの Active Sbox の最小数を表 8に示す．

拡散性能の観点において，より最適な構成は $DP_{max} = 2.5$ を満たす P_{b2} と P_{n2} の構成であるが，Active Sbox 評価の観点において，Midori-128，P_{b1} と P'_{n1} の構成と比べると大きく劣る．したがって，拡散性能と Active Sbox 評価両方の観点においてより最適な構成は $DP_{max} = 3$ と 12 ラウンドで Active Sbox の最小数が 64 に達する P_{b1} と P'_{n1} の構成である．

8. まとめ

本稿では 4 bit Sbox，バイナリマトリックスを持つ 128 bit Low-latency ブロック暗号の線形層について拡散性能，Active Sbox 評価の観点でより最適な bit 置換の検討を行った．bit 置換を評価する際，bit 置換を 2 つの置換に分割することにより，特定の bit 置換に対して MILP による Active Sbox 評価を可能とした．結果として Midori-128 と同等の拡散性能を持ち，Active Sbox 評価の観点では Midori-128 を上回る 12 ラウンドで差分/線形攻撃に対して安全な構成を発見した．

謝辞

本研究は科研費 19H02141 の助成を受けたものです．

参考文献

[1] Gianira N. Alfarano, Christof Beierle, Takanori Isobe, Stefan Kölbl, and Gregor Leander. Shiftrows alternatives for aes-like ciphers and optimal cell permutations for midori and skinny. *IACR Trans. Symmetric Cryptol.*, 2018(2):20–47, 2018.

[2] Roberto Avanzi. The QARMA block cipher family. almost MDS matrices over rings with zero divisors, nearly symmetric even-mansour constructions with non-involutory central rounds, and search heuristics for low-latency s-boxes. *IACR Trans. Symmetric Cryptol.*, 2017(1):4–44, 2017.

[3] Subhadeep Banik, Andrey Bogdanov, Takanori Isobe, Kyoji Shibutani, Harunaga Hiwatari, Toru Akishita, and Francesco Regazzoni. Midori: A block cipher for low energy. In *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part II*, pages 411–436, 2015.

[4] Julia Borghoff, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Knezevic, Lars R. Knudsen, Gregor Leander, Ventzislav Nikov, Christof Paar, Christian Rechberger, Peter Rombouts, Søren S. Thomsen, and Tolga Yalçin. PRINCE - A low-latency block cipher for pervasive computing applications - extended abstract. In *Advances in Cryptology - ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings*, pages 208–225, 2012.

[5] Gurobi Optimization Inc. Gurobi optimizer 6.5. Official webpage, `http://www.gurobi.com/`, 2015.

[6] AmirHossein E. Moghaddam and Zahra Ahmadian. New automatic search method for truncated-differential characteristics: Application to midori, skinny and craft. Cryptology ePrint Archive, Report 2019/126, 2019. `https://eprint.iacr.org/2019/126`.

[7] Nicky Mouha, Qingju Wang, Dawu Gu, and Bart Preneel. Differential and linear cryptanalysis using mixed-integer linear programming. In *Information Security and Cryptology - 7th International Conference, Inscrypt 2011, Beijing, China, November 30 - December 3, 2011. Revised Selected Papers*, pages 57–76, 2011.

[8] Peng Wang Kexin Qiao Xiaoshuang Ma Ling Song Siwei Sun, Lei Hu. Automatic security evaluation and (related-key) differential characteristic search: Application to simon, present, lblock, des(l) and other bit-oriented block ciphers. Cryptology ePrint Archive, Report 2013/676, 2013. `https://eprint.iacr.org/2013/676`.

[9] Tomoyasu Suzaki and Kazuhiko Minematsu. Improving the generalized feistel. In *Fast Software Encryption, 17th International Workshop, FSE 2010, Seoul, Korea, February 7-10, 2010, Revised Selected Papers*, pages 19–39, 2010.