IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2018, No. 2, pp. 20–47. DOI:10.13154/tosc.v2018.i2.20-47

ShiftRows Alternatives for AES-like Ciphers and Optimal Cell Permutations for Midori and Skinny

Gianira N. Alfarano[1], Christof Beierle[2], Takanori Isobe[3], Stefan Kölbl[4] and Gregor Leander[2]

[1] University of Zurich, Zurich, Switzerland
gianiranicoletta.alfarano@math.uzh.ch
[2] Horst Görtz Institute for IT Security, Ruhr-Universität Bochum, Bochum, Germany
christof.beierle@rub.de, gregor.leander@rub.de
[3] University of Hyogo, Hyogo, Japan
takanori.isobe@ai.u-hyogo.ac.jp
[4] Cybercrypt, Hellerup, Denmark
stek@mailbox.org

Abstract. We study possible alternatives for ShiftRows to be used as cell permutations in AES-like ciphers. As observed during the design process of the block cipher Midori, when using a matrix with a non-optimal branch number for the MixColumns operation, the choice of the cell permutation, i.e., an alternative for ShiftRows, can actually improve the security of the primitive. In contrast, when using an MDS matrix it is known that one cannot increase the minimum number of active S-boxes by deviating from the ShiftRows-type permutation.

However, finding the optimal choice for the cell permutation for a given, non-optimal, MixColumns operation is a highly non-trivial problem. In this work, we propose techniques to speed up the search for the optimal cell permutations significantly. As case studies, we apply those techniques to Midori and Skinny and provide possible alternatives for their cell permutations. We finally state an easy-to-verify sufficient condition on a cell permutation, to be used as an alternative in Midori, that attains a high number of active S-boxes and thus provides good resistance against differential and linear attacks.

Keywords: Block Cipher · Midori · Skinny · AES · ShiftRows · Differential Cryptanalysis · Linear Cryptanalysis · Active S-boxes · Matsui's Algorithm · Diffusion

1 Introduction

The Advanced Encryption Standard (AES) [18] can certainly be considered to be the most important block cipher in practice. Besides that, due to its simple and elegant structure, the AES (and its predecessor SQUARE [10]) have influenced a large variety of cryptographic primitives that build upon its general design ideas. In particular, many block-cipher and hash-function designs start with the initial design structure of the AES and tweak it with respect to one or more parts in order to fulfill their requirements. Examples of such designs include, but are not limited to, Anubis [3], LED [13], mCrypton [15], Midori [2], Photon [12], Prince [8], Qarma [1], Skinny and Mantis [6], and Whirlpool [4].

Interestingly, even though AES and its general design have been studied for over 20 years now, still new ideas pop up in this area and raise interesting questions. One of the more recent ideas was presented in 2015 with the block cipher Midori. Midori, which is the Japanese word for *green*, is a lightweight cipher that aims at minimizing the energy

Licensed under Creative Commons License CC-BY 4.0.
Received: 2017-09-01, Revised: 2018-03-01, Accepted: 2018-05-01, Published: 2018-06-07

consumption of encryption. While Midori follows the general outline of the AES, almost all components are modified in order to reach the goal of minimizing energy.

In particular, the authors decided to change the MixColumns operation in a way that it applies multiplication with a *binary matrix with branch number 4*, compared to the non-binary MixColumns operation in the AES with branch number 5. This has the benefit of significantly reducing the energy consumption of this operation. However, the downside is that, *a priori*, the number of active S-boxes reduces. More precisely, while for AES we have at least 25 active S-boxes in any (linear or differential) four-round trail, moving to a branch number of 4 reduces this number to 16. This follows from the *four-round propagation theorem* (Section 9.5. in [11]), a powerful theoretical argument of the *wide-trail strategy* [9]. Indeed, the wide-trail strategy is one of the major design principles of the AES and allows for obtaining useful, and *mathematical provable*, bounds on the minimum number of active S-boxes. For states of quadric dimension and under the usage of a MixColumns operation with optimal branch number, it was shown in [7] that one cannot increase the minimum number of active S-boxes when substituting the ShiftRows operation by another, arbitrary, cell permutation. Therefore, the interesting, and maybe unexpected, observation made by the designers of Midori is that actually substituting ShiftRows can significantly increase the number of active S-boxes if a MixColumns operation with non-optimal branch number is employed. Indeed, by using a different cell permutation, the authors of Midori managed to increase the minimum number of active S-boxes, e.g., from 20 to 30 for 6 rounds. On top, changing the cell permutation does not come at any additional cost, at least when considering hardware implementations. Later in 2016, Todo and Aoki analyzed which binary matrices lead to an improved number of active S-boxes for the classical ShiftRows permutation [20].

The interesting and important question raised by the designers of Midori is what the optimal choice of the cell permutation, used as a substitute for ShiftRows, actually is. The difficulty in answering this question comes from the fact that the four-round propagation theorem is not capable of proving better bounds than one obtains by just iterating four-round trails. In other words, with our current knowledge we are not able to theoretically analyze those improved bounds on the number of active S-boxes, but rather have to rely on computer search techniques like Matsui's algorithm [16] or techniques based on Mixed-Integer Linear Programming (MILP) [17]. Quite some progress has been made on those tools in recent years, especially in the area of MILP (e.g. [19]). For a given cell permutation, even for a higher number of rounds, it is still possible to compute (bounds on) the number of active S-boxes within reasonable time using a single core of a standard PC. However, there is a huge choice of possible permutations to be considered – roughly $2^{44.25}$ in the case of Midori – which immediately renders the naive approach of simply testing them all very inefficient.

The designers of Midori overcome this problem by heuristically reducing the search space of all cell permutations to be considered. However, it stayed unclear if, by this reduction, we actually exclude the best possible cell permutations. Interestingly, in the design document of Midori [2], some conditions are given under which a permutation leads to an optimal number of active S-boxes. Unfortunately, those conditions are given without a proof or an intuition. Moreover, as we will see later, those conditions do not guarantee an optimal number of active S-boxes for *all* number of rounds *simultaneously*.

Thus, the final goal is clearly to gain some theoretical insight on what exactly characterizes the optimal cell permutations. However, as already mentioned, this seems out of reach with our current knowledge. We then focus on the task of computationally finding the best permutations among *all permutations*, i.e., *without any restriction on the search space*.

1.1 Our Contribution

The starting point of our work is the simple, but useful, observation given in Section 3, i.e., for any AES-like cipher, there are several cell permutations which basically lead to the same cipher. More precisely, if two cell permutations p and p' differ only by conjugation with a permutation that commutes with the MixColumns operation, the entire two ciphers differ only by a permutation on the plaintext and ciphertext and a corresponding permutation of the round keys. This immediately implies that in particular, the ciphers have the same cryptographic resistance against any attack that does not involve details about the key-scheduling algorithm. Especially, the bounds on the number of active S-boxes are necessarily the same.

For our task of finding the best permutation, this means that we have to check only one of those cell permutations, p or p'. More formally, we show that being equal up to conjugation with a permutation that commutes with a given MixColumns operation actually defines an equivalence relation (see Definition 4) on the set of all possible permutations. We then have to check only one representative of each possible equivalence class.

This naturally leads to the task of classifying cell permutations with respect to this notion of equivalence. Again, when approaching this task in a naive manner, it quickly turns very inefficient. In order to keep it still manageable, we first study a weakened notion of equivalence, which allows us to significantly simplify the classification algorithm. We furthermore give an easy to verify condition on when this a priori weakened equivalence notion coincides with the equivalence notion mentioned above. This will be part of Section 3.

The MixColumns operations used in Midori and Skinny then serve as case studies for our general approach (see Section 4 and Section 5). Focusing on Midori is especially interesting for the following two reasons. First, the MixColumns operation fulfills the sufficient condition for which the weaker notion of equivalence coincides with the stronger notion of equivalence we are actually interested in. This allows the simplified classification mentioned above. Second, as we will explain in detail, the number of different equivalence classes is especially small for Midori. Indeed, our algorithm reveals that there are only about $2^{21.7}$ equivalence classes. Thus, compared to checking $2^{44.5}$ possible permutations, we gain a speed-up factor of more than 2^{22}. All in all, this allows us to compare the actual best cell permutation with respect to active S-boxes – *without any restriction on the search space* – with the one actually used in Midori. For Skinny, we also have the beneficial property that the weakened notion of equivalence coincides with the stronger notion. However, compared to Midori, there are much more distinct equivalence classes ($\approx 2^{39.66}$). Due to the increased search space, we therefore only focus on permutations with diffusion properties as least as good as the original Skinny permutation, i.e., attaining full cell diffusion after 6 rounds both in forward and backward direction.

We computed the bounds on the minimum number of active S-boxes up to 40 rounds using Matsui's approach. As it turns out, the original cell permutation used in Midori does indeed give optimal bounds for any number of rounds ranging from 1 to 11, with the remarkable exception of 9. For 9 rounds, there exist four permutations (up to equivalence) that provide a higher number of active S-boxes than the one used in Midori. Moreover, from 13 rounds onwards and up to 40 rounds, the original Midori permutation is never the optimal one. Therefore, there is actually no single permutation that achieves the optimal bound for all number of rounds simultaneously. It is also worth noticing that the number of optimal permutations varies when considering different number of rounds. Those results are visualized in Figure 3. Our analysis indicates that the conditions on optimal cell permutations given by the Midori designers (see [2, pp. 15-16]) do not precisely characterize the properties one wants to achieve. For Skinny, we obtained similar results. Of all permutations with diffusion as least as good as the original Skinny permutation, the original Skinny permutation is optimal for most of the number of rounds up to 26. From

27 rounds onwards and up to 40 rounds, it is never optimal. Those results are visualized in Figure 4.

It is worth remarking that the ciphers mCrypton and Mantis apply the same MixColumns operation than Midori. This suggests that our findings are not limited to Midori, but may instead be useful for future cipher designs. Especially if a new lightweight cipher similar to Midori or Skinny has to be designed, the designers can now easily pick a cell permutation that suits their security goals – *depending on the size of the S-boxes and their cryptographic properties*. To make it easier for designers, we provide a comprehensive list of optimal cell permutations in Appendix C.1 and C.2

Besides computer-aided results, one would also like to obtain a more theoretical understanding of which cell permutations lead to high bounds on the minimum number of active S-boxes. Basically, for AES-like ciphers, we know the *four-round propagation theorem* as an elegant way to understand the best possible bounds on the minimum number of active S-boxes over four rounds. With a more complex argument, in [14], the authors formally proved that AES-128 guarantees high bounds on the minimum number of active S-boxes in the related-key setting. In a similar manner, we finally provide a *theoretical* argument on when a cell permutation, to be used as an alternative in Midori, attains a high number of active S-boxes (in the single-key model). More precisely, we give an easy-to-verify condition on a cell permutation to attain 28 active S-boxes over 6 rounds.

Parts of this work already appeared in the PhD thesis [5].

2 Preliminaries

In this work, we consider AES-like *substitution-permutation networks* (SPNs) as depicted in Figure 1. Generally speaking, the SPN transforms an $m \times n$ state of the form

$$\begin{bmatrix} a_0 & a_m & \cdots & a_{(n-1)m} \\ a_1 & a_{m+1} & \cdots & a_{(n-1)m+1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m-1} & a_{m+(m-1)} & \cdots & a_{nm-1} \end{bmatrix},$$

where each $a_i \in \mathbb{F}_{2^s}$ for a given word size s. The SPN follows an iterative structure in which a certain pre-defined round function is iterated several times. In an *SP block cipher*, this iteration is interleaved with the addition of round-dependent keys in $\mathbb{F}_{2^s}^{m \times n}$. For simplicity, we will omit this round-key addition in the following, as we are focusing only on the cryptographic properties of the round function.[1]

We focus on a special kind of round function as described in Definition 1, which resembles the structure applied in the AES. We further restrict to the case that a binary $\mathbb{F}_{2^s}$-linear MixColumns operation is employed, i.e., the $m \times m$ matrix representing the linear MixColumns transformation contains only the values 0 and 1 in $\mathbb{F}_{2^s}$ as its coefficients. We give a formal definition of this AES-like round structure in the following. It is important to note that many recently proposed lightweight designs fit into this notion, e.g., Midori [2] or Skinny [6].

Definition 1. An *AES-like round* is a permutation $\mathsf{R}_{S,p,\mathbf{M}} : \mathbb{F}_{2^s}^{mn} \to \mathbb{F}_{2^s}^{mn}$ which is parametrized by the state dimension $m \times n$, the word size s, a permutation $S : \mathbb{F}_{2^s} \to \mathbb{F}_{2^s}$, an $m \times m$ matrix $\mathbf{M}$ with (binary) coefficients in $\mathbb{F}_{2^s}$, and a permutation p on $\mathbb{Z}_{mn}$. In particular, the round function $\mathsf{R}_{S,p,\mathbf{M}}$ is composed of the bijective transformations SB, $\mathsf{Permute}_p$ and $\mathsf{Mix}_{\mathbf{M}}$ operating on $m \times n$ states, such that $\mathsf{R}_{S,p,\mathbf{M}} = \mathsf{Mix}_{\mathbf{M}} \circ \mathsf{Permute}_p \circ \mathsf{SB}$:

[1] Analyzing a cipher w.r.t. the most common attacks, i.e., differential and linear cryptanalysis, is usually done under the assumption of adding independent and uniformly distributed round keys after each round.

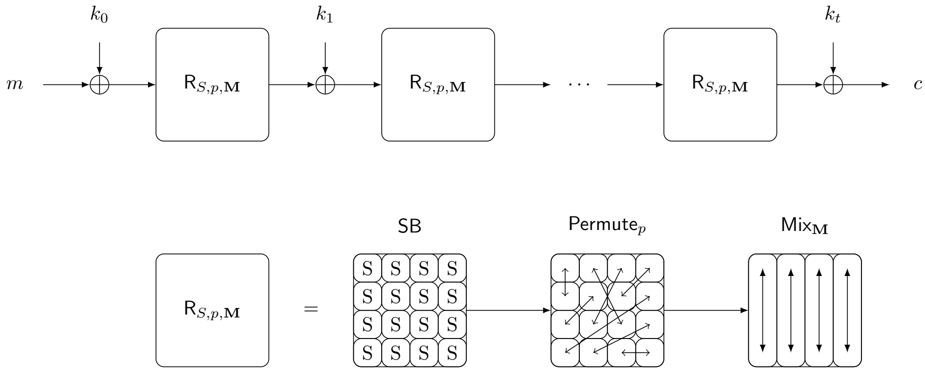

k_0
k_1
k_t
m
$\mathsf{R}_{S,p,\mathbf{M}}$
$\mathsf{R}_{S,p,\mathbf{M}}$
$\cdots$
$\mathsf{R}_{S,p,\mathbf{M}}$
c
SB
Permute$_p$
Mix$_{\mathbf{M}}$
$\mathsf{R}_{S,p,\mathbf{M}}$
=
S S S S
S S S S
S S S S
S S S S

Figure 1: The iterative structure of a substitution-permutation cipher using an AES-like round for a 4 × 4 state.

1. SB is a parallel application of the S-box $S : \mathbb{F}_{2^s} \to \mathbb{F}_{2^s}$ to all $m \cdot n$ cells of the state.

$$\mathsf{SB} : (\mathbb{F}_{2^s})^{mn} \to (\mathbb{F}_{2^s})^{mn}$$
$$\forall i \in \mathbb{Z}_m, \forall j \in \mathbb{Z}_n : a_{mj+i} \mapsto S(a_{mj+i}) \ .$$

2. Permute$_p$ permutes the cells of the state by the permutation p, i.e.,

$$\mathsf{Permute}_p : (\mathbb{F}_{2^s})^{mn} \to (\mathbb{F}_{2^s})^{mn}$$
$$\forall i \in \mathbb{Z}_m, \forall j \in \mathbb{Z}_n : a_{mj+i} \mapsto a_{p(mj+i)} \ .$$

3. Mix$_{\mathbf{M}}$ applies left-multiplication by the $m \times m$ matrix $\mathbf{M}$ to all columns $j \in \mathbb{Z}_n$ of the state, i.e.,

$$\mathsf{Mix}_{\mathbf{M}} : (\mathbb{F}_{2^s})^{mn} \to (\mathbb{F}_{2^s})^{mn}$$
$$\forall j \in \mathbb{Z}_n : [a_{mj+0}, \ldots, a_{mj+(n-1)}]^\top \mapsto \mathbf{M} \cdot [a_{mj+0}, \ldots, a_{mj+(n-1)}]^\top \ .$$

We denote by $\mathcal{S}_{mn}$ the set of all cell permutations on an $m \times n$ state. In the following, we give the AES-like rounds of Midori64 and Skinny as examples.

Example 1 (Midori64)**.** For the 64-bit version of the Midori block cipher, we have $\mathsf{R}_{S,p,\mathbf{M}} : \mathbb{F}_{2^4}^{16} \to \mathbb{F}_{2^4}^{16}$. The state is represented as a 4 × 4 matrix of words a_i of length $s = 4$ bit by

$$\begin{bmatrix} a_0 & a_4 & a_8 & a_{12} \\ a_1 & a_5 & a_9 & a_{13} \\ a_2 & a_6 & a_{10} & a_{14} \\ a_3 & a_7 & a_{11} & a_{15} \end{bmatrix} .$$

The round function is composed of the following consecutive operations:

SubCell (SB). The S-box $S : \mathbb{F}_{2^4} \to \mathbb{F}_{2^4}$ employed in the SB operation is given in Table 1.

ShuffleCell (Permute$_p$) operates on the cells of the state. In particular, it transforms the state as

$$\begin{bmatrix} a_0 & a_4 & a_8 & a_{12} \\ a_1 & a_5 & a_9 & a_{13} \\ a_2 & a_6 & a_{10} & a_{14} \\ a_3 & a_7 & a_{11} & a_{15} \end{bmatrix} \mapsto \begin{bmatrix} a_0 & a_{14} & a_9 & a_7 \\ a_{10} & a_4 & a_3 & a_{13} \\ a_5 & a_{11} & a_{12} & a_2 \\ a_{15} & a_1 & a_6 & a_8 \end{bmatrix} .$$

Table 1: The 4-bit S-box used in Midori64. We give the values for x and $S(x)$ as elements in $\mathbb{F}_2^s$ with respect to the natural basis, e.g., `b` represents the vector $(1,0,1,1)$.

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S(x)$	c	a	d	3	e	b	f	7	8	9	1	5	0	2	4	6

This corresponds to the permutation

$$p = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 0 & 10 & 5 & 15 & 14 & 4 & 11 & 1 & 9 & 3 & 12 & 6 & 7 & 13 & 2 & 8 \end{pmatrix} \in \mathcal{S}_{16} \,.$$

MixColumns (Mix$_\mathbf{M}$). The matrix

$$\mathbf{M} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \in \mathrm{GL}(4, \mathbb{F}_{2^4})$$

is applied to every column of the state.

Midori64 applies the round function $\mathsf{R}_{S,p,\mathbf{M}}$ 16 times in total (where the last round omits the ShuffleCell and MixColumns operation). □

Example 2 (Skinny64)**.** As for Midori64, the round function of Skinny in its 64-bit version is given as $\mathsf{R}_{S,p,\mathbf{M}} : \mathbb{F}_{2^4}^{16} \to \mathbb{F}_{2^4}^{16}$ and the state is represented in the same way as for Midori64. The round function is composed of the following consecutive operations:

SubCells (SB). The S-box $S : \mathbb{F}_{2^4} \to \mathbb{F}_{2^4}$ employed in the SB operation is given in Table 2.

Table 2: The 4-bit S-box used in Skinny64 in its natural basis representation.

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S(x)$	c	6	9	0	1	a	2	b	3	8	5	d	4	e	7	f

ShiftRows (Permute$_p$) applies a cyclic rotation to the right on each of the rows of the state. In particular, it transforms the state as

$$\begin{bmatrix} a_0 & a_4 & a_8 & a_{12} \\ a_1 & a_5 & a_9 & a_{13} \\ a_2 & a_6 & a_{10} & a_{14} \\ a_3 & a_7 & a_{11} & a_{15} \end{bmatrix} \mapsto \begin{bmatrix} a_0 & a_4 & a_8 & a_{12} \\ a_{13} & a_1 & a_5 & a_9 \\ a_{10} & a_{14} & a_2 & a_6 \\ a_7 & a_{11} & a_{15} & a_3 \end{bmatrix} .$$

This corresponds to the permutation

$$p = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 0 & 13 & 10 & 7 & 4 & 1 & 14 & 11 & 8 & 5 & 2 & 15 & 12 & 9 & 6 & 3 \end{pmatrix} \in \mathcal{S}_{16} \,.$$

MixColumns (Mix). The matrix

$$\mathbf{M} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix} \in \mathrm{GL}(4, \mathbb{F}_{2^4})$$

is applied to every column of the state.

Depending on the size of the tweakey state (64, 128, or 196 bit), Skinny64 applies the round function $\mathsf{R}_{S,p,\mathbf{M}}$ 32, 36, or 40 times in total, respectively. □

2.1 Active S-boxes and Differential Cryptanalysis

The goal of differential cryptanalysis is to find a correlation between the difference of plaintext pairs and the corresponding output difference which holds with high probability. In order to estimate the probability of such a correlation we observe *trails* of differences through the round function.

Definition 2 (Differential Trail (see [11]))**.** Let E be an AES-like cipher with round function $\mathsf{R}_{S,p,\mathbf{M}}$ operating on a state of dimension $m \times n$ with word size s. A t-round *trail* is a $(t+1)$-tuple $(X^{(0)}, \ldots, X^{(t)}) \in ((\mathbb{F}_{2^s})^{mn})^{t+1}$. The *weight* of the differential trail is defined as

$$\sum_{r \in \mathbb{Z}_t} \sum_{i \in \mathbb{Z}_m} \sum_{j \in \mathbb{Z}_n} \tilde{X}^{(r)}_{mj+i} ,$$

where $\tilde{X}^{(r)}_{mj+i} \in \{0,1\} \subseteq \mathbb{Z}$ such that $\tilde{X}^{(r)}_{mj+i} = 1$ if and only if $X^{(r)}_{mj+i} \neq 0$. A pair of inputs $x, x' \in (\mathbb{F}_{2^s})^{mn}$ is said to *follow the differential trail* $(X^{(0)}, \ldots, X^{(t)})$ over t rounds if and only if $X^{(0)} = x + x'$ and

$$\forall r \in \{1, \ldots, t\} : X^{(r)} = \mathsf{R}^r_{S,p,\mathbf{M}}(x) + \mathsf{R}^r_{S,p,\mathbf{M}}(x') .$$

We say that a differential trail is *valid* for E if and only if there exists an input pair that follows the trail.

As the only non-linear operation in the round function is S, the probability that an input pair follows this trail is directly related to the weight of the trail. We refer to any S-box which has a non-zero difference in the trail as an *active S-box*. In order to show resistance of a cipher against differential cryptanalysis, it is important to find a good bound on the minimum weight, resp. number of active S-boxes, in any valid (non-zero) trail.

Definition 3 (Branch Number (see [11]))**.** For an $\mathbb{F}_{2^s}$-linear transformation L, the *branch number* $\mathcal{B}_L$ is defined as

$$\mathcal{B}_L = \min_{a \neq 0} \{wt(a) + wt(L(a))\} ,$$

where $wt(x)$ is the number of non-zero words in x.

The MixColumns layer of Midori has a branch number of 4. It has the further interesting property that the number of possible transitions is highly limited. See Figure 10 in Appendix A for a detailed overview of the possible transitions. For the MixColumns matrix of Skinny, the branch number is only 2 and the possible transitions are even more restricted (see Figure 11 in Appendix A).

Note that for analyzing the resistance against *linear cryptanalysis*, one has to evaluate the minimum number of active S-boxes for the MixColumns matrix $(\mathbf{M}^{-1})^\top$, where $^\top$ denotes the transpose of the matrix. As for Midori we have $\mathbf{M} = (\mathbf{M}^{-1})^\top$, the bounds on the minimum number of active S-boxes are the same both with regard to linear and differential cryptanalysis. However, for Skinny, this is not the case and the resistance against linear cryptanalysis has to be evaluated separately. Throughout this paper, we only concentrate on differential cryptanalysis.

In the remainder of this work, we will also consider diffusion properties of cell permutations. We say that a cell permutation attains *full diffusion after r rounds* if, after r rounds, every cell of the internal state depends on every cell of the input state.

3 Classifying Cell Permutations

When designing a new block cipher, besides choosing a cryptographically strong S-box, a crucial goal of the designer is to choose an appropriate linear layer in order to maximize diffusion properties and prevent against differential and linear attacks. In the notion of AES-like ciphers, the linear layer is fully specified by a matrix $\mathbf{M} \in \mathrm{GL}(m, \mathbb{F}_{2^s})$ corresponding to the MixColumns operation and by a cell permutation $p \in \mathcal{S}_{mn}$. A natural designer's approach is to first select the matrix $\mathbf{M}$ and then choose the cell permutation that maximizes the minimum number of active S-boxes. Indeed, one of the major novelties of the Midori design was to show that the choice of a specific type of cell permutation, in combination with the appropriate MixColumns matrix, can guarantee a much higher number of guaranteed active S-boxes, compared to just applying a simple ShiftRows-like operation as it was done in the AES.

In order to reduce the search space of all permutations in $\mathcal{S}_{mn}$, it is crucial to identify under which conditions two permutations lead to the same cryptographic properties. In particular, we base our work on the following simple observation: If we consider a permutation $p \in \mathcal{S}_{mn}$, then any permutation that is obtained from p by conjugation with some $\vartheta \in \mathcal{S}_{mn}$ for which $\mathsf{Mix}_{\mathbf{M}} \circ \mathsf{Permute}_{\vartheta} = \mathsf{Permute}_{\vartheta} \circ \mathsf{Mix}_{\mathbf{M}}$ lead to the same cryptographic properties. In other words, the SP cipher instantiated with the AES-like round $\mathsf{R}_{S,\vartheta \circ p \circ \vartheta^{-1},\mathbf{M}}$ is just a permuted version of the SP cipher instantiated with $\mathsf{R}_{S,p,\mathbf{M}}$ (under a permutation of the round keys), whenever the permutation matrix of ϑ commutes with the matrix corresponding to the operation $\mathsf{Mix}_{\mathbf{M}}$. This fact is illustrated in Figure 2. Overall, this motivates the notion of $\mathbf{M}$-equivalence as defined in the following. For given state dimensions m, n, we will denote the set of all cell permutations ϑ for which $\mathsf{Permute}_{\vartheta}$ commutes with $\mathsf{Mix}_{\mathbf{M}}$ by $\mathcal{T}(\mathbf{M})$.

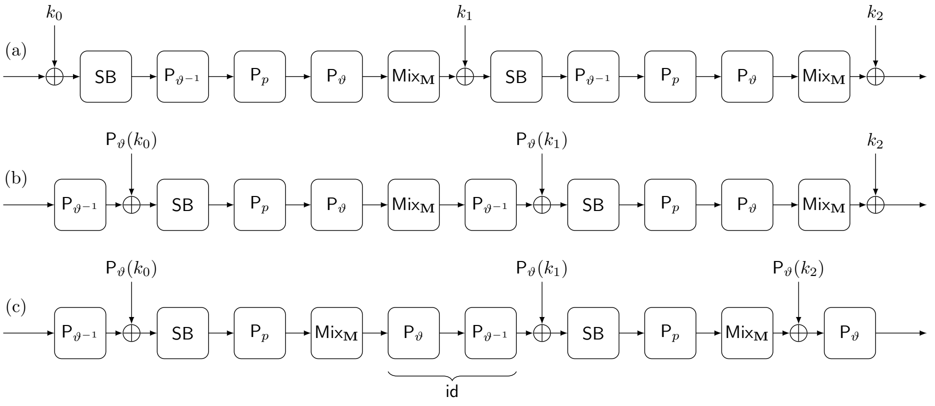

k_0
k_1
k_2
(a)
SB
$\mathsf{P}_{\vartheta^{-1}}$
P_p
P_ϑ
$\mathsf{Mix}_{\mathbf{M}}$
$\mathsf{P}_\vartheta(k_0)$
$\mathsf{P}_\vartheta(k_1)$
k_2
(b)
$\mathsf{P}_\vartheta(k_0)$
$\mathsf{P}_\vartheta(k_1)$
$\mathsf{P}_\vartheta(k_2)$
(c)
id

Figure 2: This illustration shows how equivalent permutations lead to the same cipher upto permutation of the input, the output and the round keys. One can easily see that cipher (a) is the same as cipher (b) by using the fact that the S-box layer commutes with the cell-permutation layer. The ciphers (b) and (c) are the same since $\mathsf{Permute}_{\vartheta}$ (here denoted as P_{ϑ} for short) commutes with $\mathsf{Mix}_{\mathbf{M}}$.

Definition 4 ($\mathbf{M}$-equivalence)**.** Let $\mathbf{M} \in \mathrm{GL}(m, \mathbb{F}_{2^s})$ be an $m \times m$ matrix with binary coefficients. We say that two permutations $p, p' \in \mathcal{S}_{mn}$ are $\mathbf{M}$-equivalent, if there exists a permutation $\vartheta \in \mathcal{T}(\mathbf{M})$ such that $p' = \vartheta \circ p \circ \vartheta^{-1}$. We write $p \sim p'$ for two $\mathbf{M}$-equivalent permutations p and p'.

Note that $\mathcal{T}(\mathbf{M})$ is a subgroup of $\mathcal{S}_{mn}$ which implies that the relation $\sim$ is symmetric, reflexive and transitive. Thus, $\sim$ is indeed an equivalence relation on $\mathcal{S}_{mn}$.

If p and p' are $\mathbf{M}$-equivalent permutations, by definition there exists a permutation ϑ such that

$$\mathsf{R}_{S,p',\mathbf{M}} = \mathsf{Permute}_{\vartheta} \circ \mathsf{R}_{S,p,\mathbf{M}} \circ \mathsf{Permute}_{\vartheta^{-1}} \ .$$

It is important to note that this can be extended for an arbitrary number of rounds. In particular, for any $t \in \mathbb{N}$, we have

$$\mathsf{R}^{t}_{S,p',\mathbf{M}} = \mathsf{Permute}_{\vartheta} \circ \mathsf{R}^{t}_{S,p,\mathbf{M}} \circ \mathsf{Permute}_{\vartheta^{-1}} \ .$$

Thus, if any cryptanalysis is done independently of the actual specification of the round keys, the corresponding ciphers share *the same cryptographic properties*. This holds in particular for the case of differential and linear cryptanalysis. $\mathbf{M}$-equivalent permutations lead to the same bound on the minimum number of active S-boxes.

For given $m, n \in \mathbb{N}$ and $\mathbf{M} \in \mathrm{GL}(m, \mathbb{F}_{2^s})$ with binary coefficients, we aim for classifying all permutations in $\mathcal{S}_{mn}$ up to $\mathbf{M}$-equivalence. As described above, such a classification would allow us to check only a single representative of each equivalence class for its cryptographic properties and it thus may significantly reduce the complexity of finding the best cell permutation. However, there is a difficulty in achieving this classification. Namely, for an arbitrary $\mathbf{M}$, it is not obvious how to efficiently determine $\mathcal{T}(\mathbf{M})$ and to separate all permutations into their equivalence classes. In order to reach our goal, we therefore first consider a weaker notion of $\mathbf{M}$-equivalence and describe an algorithm to enumerate all permutations up to this weak equivalence. Later, we will see that, for certain choices of $\mathbf{M}$, this weak equivalence coincides with the general notion of $\mathbf{M}$-equivalence. Fortunately, this approach allows us to finally classify all cell permutations upto $\mathbf{M}$-equivalence in its stronger notion for the case of Midori and Skinny.

Definition 5 (weak $\mathbf{M}$-equivalence)**.** Let $\mathcal{P}_{\rightleftharpoons}$ denote the set of all cell permutations that permute whole columns of the state and let $\mathcal{P}_{\updownarrow}$ be the set of cell permutations that operate independently on the columns of the state. Formally,

$$\mathcal{P}_{\rightleftharpoons} := \{p \in \mathcal{S}_{mn} \mid \exists \sigma \in \mathcal{S}_n : \forall i \in \mathbb{Z}_m, j \in \mathbb{Z}_n : mj + i \overset{p}{\mapsto} m\sigma(j) + i\} \ .$$

$$\mathcal{P}_{\updownarrow} := \{p \in \mathcal{S}_{mn} \mid \exists \sigma_0, \dots, \sigma_{n-1} \in \mathcal{S}_m : \forall i \in \mathbb{Z}_m, j \in \mathbb{Z}_n : mj + i \overset{p}{\mapsto} mj + \sigma_j(i)\} \ .$$

Then, we say that a cell permutation p is weakly $\mathbf{M}$-equivalent to a cell permutation p', written $p \sim_w p'$, if there exists a cell permutation $\vartheta \in \mathcal{T}(\mathbf{M})$ of the form $\vartheta = \pi \circ \phi$, with $\pi \in \mathcal{P}_{\rightleftharpoons}$ and $\phi \in \mathcal{P}_{\updownarrow}$ such that $p' = \vartheta \circ p \circ \vartheta^{-1}$.

Again, since $\{\vartheta \in \mathcal{T}(\mathbf{M}) \mid \vartheta = \pi \circ \phi \text{ with } \pi \in \mathcal{P}_{\rightleftharpoons} \text{ and } \phi \in \mathcal{P}_{\updownarrow}\}$ is a subgroup of $\mathcal{S}_{mn}$, the relation $\sim_w$ is indeed an equivalence relation. Further, $p \sim_w p'$ trivially implies $p \sim p'$. For an equivalence class $[p]_{\sim_w}$, we consider the *smallest* permutation (in lexicographic ordering $\prec$) as its canonical representative. For a given $\mathbf{M}$, we will describe an algorithm that enumerates a representative of each equivalence class.

3.1 Structure Matrix of a Cell Permutation

Let $p \in \mathcal{S}_{mn}$ be a cell permutation on an $m \times n$ state. We define *the structure matrix of* p as the $n \times n$ matrix $\mathbf{A}_p$ s.t. $\mathbf{A}_{p_{i,j}}$ contains the number of cells of column i that are permuted to column j. Formally,

$$\mathbf{A}_{p_{i,j}} = |\{k \in \mathbb{Z}_{mn} \mid k = mi + r \text{ for } r \in \mathbb{Z}_m \text{ and } mi + r \overset{p}{\mapsto} mj + r' \text{ with } r' \in \mathbb{Z}_m\}| \ .$$

Example 3.

$$\begin{bmatrix} 0 & 4 & 8 & 12 \\ 1 & 5 & 9 & 13 \\ 2 & 6 & 10 & 14 \\ 3 & 7 & 11 & 15 \end{bmatrix} \overset{p}{\mapsto} \begin{bmatrix} 4 & 0 & 13 & 1 \\ 5 & 6 & 14 & 2 \\ 11 & 9 & 8 & 3 \\ 15 & 12 & 7 & 10 \end{bmatrix} , \qquad \mathbf{A}_p = \begin{pmatrix} 0 & 1 & 0 & 3 \\ 2 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 2 & 0 \end{pmatrix}$$

□

Note that an $n \times n$ matrix is a valid structure matrix for some permutation if and only if the sum of each column as well as the sum of each row adds up to m. Let now $\sigma \in \mathcal{S}_n$ be a permutation of $\mathbb{Z}_n$. For an $n \times n$ matrix $\mathbf{A}$, we define $\mathbf{A}^\sigma$ as the $n \times n$ matrix that is obtained from $\mathbf{A}$ by both permuting the rows and the columns according to σ. Formally,

$$\forall i, j \in \mathbb{Z}_n : \mathbf{A}^\sigma_{i,j} \coloneqq \mathbf{A}_{\sigma(i),\sigma(j)} \ .$$

We now define an equivalence relation $\sim$ on $n \times n$ structure matrices as

$$\mathbf{A} \sim \mathbf{B} \quad :\Leftrightarrow \quad \exists \sigma \in \mathcal{S}_n : \mathbf{B} = \mathbf{A}^\sigma \ .$$

The following proposition explains how the weak $\mathbf{M}$-equivalence of permutations and equivalence of their corresponding structure matrices are related.

Proposition 1. *Let $m, n \in \mathbb{N}$ and let $\mathbf{M} \in \mathrm{GL}(m, \mathbb{F}_{2^s})$ with binary coefficients.*

1. *If $p \sim_w p'$ for two $p, p' \in \mathcal{S}_{mn}$, then $\mathbf{A}_p \sim \mathbf{A}_{p'}$.*
2. *Let $\mathbf{A} \sim \mathbf{B}$ for two valid $n \times n$ structure matrices of permutations in $\mathcal{S}_{mn}$. Then, for any permutation $p \in \mathcal{S}_{mn}$ that has $\mathbf{A}$ as structure matrix, there exist a permutation $p' \in \mathcal{S}_{mn}$ that has $\mathbf{B}$ as structure matrix such that $p \sim_w p'$.*

Proof. 1. Let $p \sim_w p'$. Then, by definition there exists permutations $\pi \in \mathcal{P}_{\leftrightarrows}$ and $\phi \in \mathcal{P}_{\updownarrow}$ such that $p' = \pi \circ \phi \circ p \circ \phi^{-1} \circ \pi^{-1}$. Clearly, $\mathbf{A}_p = \mathbf{A}_{\phi \circ p \circ \phi^{-1}}$. Let now be $\sigma \in \mathcal{S}_n$ chosen such that, for all $i \in \mathbb{Z}_m$ and $j \in \mathbb{Z}_n$, $mj + i \overset{\pi}{\mapsto} m\sigma(j) + i$. Then, for all $i \in \mathbb{Z}_m$ and $j \in \mathbb{Z}_n$, it is

$$(\mathbf{A}_{p'})_{i,j} = (\mathbf{A}_{p' \circ \pi})_{\sigma^{-1}(i),j} = (\mathbf{A}_{\pi^{-1} \circ p' \circ \pi})_{\sigma^{-1}(i),\sigma^{-1}(j)} = (\mathbf{A}_{\phi \circ p \circ \phi^{-1}})_{\sigma^{-1}(i),\sigma^{-1}(j)} \ .$$

This shows that $\mathbf{A}_{p'} = \mathbf{A}^{\sigma^{-1}}_{\phi \circ p \circ \phi^{-1}} = \mathbf{A}^{\sigma^{-1}}_p$.

2. Let $p \in \mathcal{S}_{mn}$ such that $\mathbf{A}_p = \mathbf{A}$. By definition of the equivalence between $\mathbf{A}$ and $\mathbf{B}$, there exist a $\sigma \in \mathcal{S}_n$ such that $\mathbf{A}^\sigma_p = \mathbf{B}$. With the same observation as above, it follows that there exists a $\pi \in \mathcal{P}_{\leftrightarrows}$ such that $\mathbf{A}^\sigma_p = \mathbf{A}_{\pi \circ p \circ \pi^{-1}}$. This means that $\pi \circ p \circ \pi^{-1}$ has structure matrix $\mathbf{B}$. Now, since $\mathsf{Permute}_\pi$ commutes with $\mathsf{Mix}_\mathbf{M}$, we have $\pi \circ p \circ \pi^{-1} \sim_w p$.

□

This result (2) implies that, in order to characterize permutations upto weak $\mathbf{M}$-equivalence, it is enough to separate all valid structure matrices into their equivalence classes, pick a representative of each class and search for all permutations (upto weak $\mathbf{M}$-equivalence) that fulfill the respective structure matrix.

3.2 Search Algorithm

Algorithm 1 for enumerating all permutations upto weak $\mathbf{M}$-equivalence for a given structure matrix $\mathbf{A}$ works as follows. We start with an $m \times n$ cell permutation p_{start} which is undefined at any position (this is represented by a -1 value). Then, we apply EnumerateRecursive to p_{start}. After each call, the permutation is extended by another column until it is completely defined. Note that it can only be extended by a column which meets the requirements given by the structure matrix $\mathbf{A}$ (see line 12 of Algorithm 1). Only if the new extended permutation leads to a smallest representative of an equivalence class, the algorithm will proceed with this permutation.[2] This is checked in line 14. Since we

[2] We use the approach of constructing the permutations in a column-wise manner from their structure matrices as we expect that iterating through *all* permutations and checking whether they are the smallest representatives would be less efficient.

only concentrate on a single structure matrix, checking if p is the smallest representative can be done with at most $|\mathcal{P}_{\updownarrow}|$ iterations.

After the algorithm terminates, it outputs a list of cell permutations that contains *at least one* representative of each equivalence class. However, it can contain more than one representative. As a last step, for each p in this list, it is therefore required to check if p is the smallest permutation w.r.t. conjugation by all $\pi \circ \phi$ with $\phi \in \mathcal{P}_{\updownarrow}$ and $\pi \in \mathcal{P}_{\leftrightarrows}$ that leave the structure matrix of p invariant. In other words, it is to check if p is smaller than any permutation $\pi \circ \phi \circ p \circ \phi^{-1} \circ \pi^{-1}$, where $\phi \in \mathcal{P}_{\updownarrow}$ and $\pi \in \mathcal{P}_{\leftrightarrows}$ such that $\mathbf{A}_p = \mathbf{A}_p^\sigma$ for the $\sigma \in \mathcal{S}_n$ corresponding to the permutation π.

Algorithm 1 Enumerate all permutations upto weak **M**-equivalence for a given structure matrix **A**

```
procedure EnumeratePermutations($\mathbf{A}$)
    $R \leftarrow \{\}$
    $p_{\text{start}} = \begin{bmatrix} -1 & \dots & -1 \\ \vdots & \ddots & \vdots \\ -1 & \dots & -1 \end{bmatrix}$
    EnumerateRecursive($\mathbf{A}, 0, p_{\text{start}}$)
    return $R$
end procedure

procedure EnumerateRecursive($\mathbf{A}, j, p$)
    if $j \geq n$ then
        return
    end if
    for $q = [q_0, \dots, q_{m-1}]^\top$ corresponding to $\mathbf{A}_{\cdot,j}$ do
        $p_{\text{new}} = $ Extend($p, q$)
        if $p_{\text{new}}$ is permutation and $\nexists p' \in [p]_{\sim_w} : p' \prec p$ then
            if $p_{\text{new}}$ is complete then
                $R \leftarrow R \cup \{p_{\text{new}}\}$
            else
                return EnumerateRecursive($\mathbf{A}, j+1, p_{\text{new}}$)
            end if
        end if
    end for
end procedure

procedure Extend($p, q$)
    for $j \in \{0, \dots, n-1\}$ do
        if $p_{\cdot,j} = [-1, \dots, -1]^\top$ then
            $p_{\cdot,j} \leftarrow q$
            return $p$
        end if
    end for
end procedure
```

3.3 The Difference between Weak M-Equivalence and M-Equivalence

In this section, we outline the relations between weak **M**-equivalence and the stronger notion of **M**-equivalence. The following proposition describes a sufficient condition on the matrix **M** such that the notions of weak **M**-equivalence and **M**-equivalence are the same.

Proposition 2. *Let* $\mathbf{M} \in \mathrm{GL}(m, \mathbb{F}_{2^s})$ *be an* $m \times m$ *matrix with binary coefficients and let* $\mathcal{G}$ *be the directed graph with* m *vertices that has* $\mathbf{M}$ *as its adjacency matrix. Then, if* $\mathcal{G}$ *is a strongly connected directed graph, the notion of* $\mathbf{M}$*-equivalence coincides with the notion of weak* $\mathbf{M}$*-equivalence.*

Proof. Let ϑ be a cell permutation in $\mathcal{T}(\mathbf{M})$. We can write any cell position $k \in \{0, \ldots, mn-1\}$ of an $m \times n$ state uniquely as $k = m \cdot \mathsf{Block}(k) + \mathsf{Index}(k)$, where $0 \leq \mathsf{Index}(k) < m$. We now have to show that, for all $k, k' \in \{0, \ldots, mn-1\}$, $\mathsf{Block}(k) = \mathsf{Block}(k')$ implies $\mathsf{Block}(\vartheta(k)) = \mathsf{Block}(\vartheta(k'))$. In that case, ϑ can be written as $\pi \circ \phi$ with $\pi \in \mathcal{P}_{\leftrightarrows}$ and $\phi \in \mathcal{P}_{\updownarrow}$.

We can represent the operation $\mathsf{Mix}_{\mathbf{M}}$, operating on the whole $m \times n$ state as the $mn \times mn$ binary block-diagonal matrix which consists of n blocks of the $m \times m$ matrix $\mathbf{M}$, i.e.,

$$\mathsf{Mix}_{\mathbf{M}} = \begin{pmatrix} \mathbf{M} & & & \\ & \mathbf{M} & & \\ & & \ddots & \\ & & & \mathbf{M} \end{pmatrix} =: (b_{i,j})_{i,j \in \{0,\ldots,mn-1\}} \in \mathrm{GL}(mn, \mathbb{F}_{2^s}).$$

Thereby, $b_{i,j}$ denotes the entry in row i and column j of $\mathsf{Mix}_{\mathbf{M}}$. Since the permutation matrix of ϑ has to commute with $\mathsf{Mix}_{\mathbf{M}}$, we necessarily have the property that $b_{i,j} = b_{\vartheta(i),\vartheta(j)}$ for all $i, j \in \{0, \ldots, mn-1\}$. Let now $k, k' \in \{0, \ldots, mn-1\}$. By the block-diagonal structure of the matrix $\mathsf{Mix}_{\mathbf{M}}$, it is

$$b_{k,k'} = 1 \Leftrightarrow \left(\mathsf{Block}(k) = \mathsf{Block}(k') \text{ and } \mathsf{Index}(k') \in T_{\mathsf{Index}(k)}\right),$$

where $T_i := \{j \in \{0, \ldots, m-1\} \mid \mathbf{M}_{i,j} = 1\}$. Since $b_{k,k'} = b_{\vartheta(k),\vartheta(k')}$, we have that, for all $k, k' \in \{0, \ldots, mn-1\}$,

$$\left(\mathsf{Block}(k) = \mathsf{Block}(k') \text{ and } \mathsf{Index}(k') \in T_{\mathsf{Index}(k)}\right) \Rightarrow \mathsf{Block}(\vartheta(k)) = \mathsf{Block}(\vartheta(k')). \quad (1)$$

Let now $k, k' \in \{0, \ldots, mn-1\}$ with $\mathsf{Block}(k) = \mathsf{Block}(k')$ and not necessarily $\mathsf{Index}(k') \in T_{\mathsf{Index}(k)}$. If $\mathcal{G}$ is a strongly connected directed graph, then for each pair of vertices (v, v') there exists a path from v to v'. Since $\mathcal{G}$ is the directed graph that has $\mathbf{M}$ as its adjacency matrix, this means that, for all $v, v' \in \{0, \ldots, m-1\}$, there exists $v^{(0)}, \ldots, v^{(t)} \in \{0, \ldots, m-1\}$ with $v = v^{(0)}$, $v' = v^{(t)}$ and

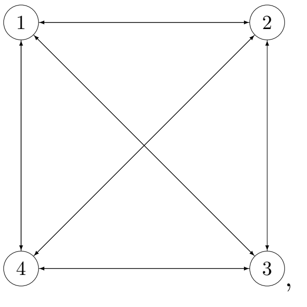
$$\forall i \in \{0, \ldots, t-1\} : v^{(i+1)} \in T_{v^{(i)}}.$$

We obtain that there exists $k^{(0)}, \ldots, k^{(t)} \in \{0, \ldots, mn-1\}$ s.t. $k = k^{(0)}$, $k' = k^{(t)}$, $\mathsf{Block}(k^{(i)}) = \mathsf{Block}(k^{(j)})$ for all $i, j \leq t$, and

$$\forall i \in \{0, \ldots, t-1\} : \mathsf{Index}(k^{(i+1)}) \in T_{\mathsf{Index}(k^{(i)})}.$$

But then, from Equation 1, $\mathsf{Block}(\vartheta(k^{(i)}))$ must be the same for all $k^{(i)}$ and, in particular, $\mathsf{Block}(\vartheta(k)) = \mathsf{Block}(\vartheta(k'))$. □

Example 4. Let $\mathbf{M}$ be the MixColumns matrix applied in Midori. Then, the directed graph $\mathcal{G}$ with m vertices having adjacency matrix $\mathbf{M}$ can be given as

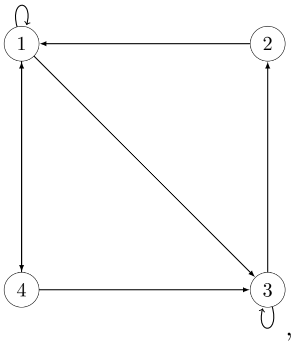


,

which is a strongly connected directed graph. □

Corollary 1. *For the* Midori *MixColumns matrix* $\mathbf{M}$*, the notion of weak* $\mathbf{M}$*-equivalence coincides with the notion of* $\mathbf{M}$*-equivalence.*

Example 5. Let $\mathbf{M}$ be the MixColumns matrix applied in Skinny. Then, the directed graph $\mathcal{G}$ with m vertices having adjacency matrix $\mathbf{M}$ can be given as



,

which is a strongly connected directed graph. □

Corollary 2. *For the* Skinny *MixColumns matrix* $\mathbf{M}$*, the notion of weak* $\mathbf{M}$*-equivalence coincides with the notion of* $\mathbf{M}$*-equivalence.*

4 Case Study – The Best Cell Permutations for Midori

Midori operates on an $m \times n$ state with $m = n = 4$, using a word size of $s = 4$ for the 64-bit block-size version and $s = 8$ for the 128-bit version, respectively. For such state dimensions, there are 501 possible structure matrices upto equivalence (as described in Section 3.1). The Midori MixColumns operation $\mathsf{Mix}_{\mathbf{M}}$ has the useful property that $\mathsf{Permute}_{\phi}$ commutes with $\mathsf{Mix}_{\mathbf{M}}$ for all 24^4 possible permutations $\phi \in \mathcal{P}_{\updownarrow}$.

Applying Algorithm 1 can be done efficiently (up to a few days on a standard pc) and thus, all cell permutations can be enumerated upto $\mathbf{M}$-equivalence. One finally obtains $3,413,774 \approx 2^{21.7}$ distinct equivalence classes. Out of those, $14,022$ permutations correspond to the all-1 structure matrix, i.e.,

$$\mathbf{A_1} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} .$$

Note that having the above structure matrix, containing only coefficients of value 1, is necessary for a cell permutation to achieve optimal diffusion, i.e., full diffusion after three rounds. Moreover, we can state the following as a necessary and sufficient condition. The proof is given in Appendix B.

Proposition 3. *Let* $p \in \mathcal{S}_{16}$ *be a cell permutation on a* 4×4 *state and let* $\mathbf{M}$ *be the MixColumns matrix of* Midori*. The corresponding AES-like cipher instantiated with* p *and* $\mathbf{M}$ *(and also its inverse) achieves full diffusion after 3 rounds if and only if both* p *and* p^2 *have* $\mathbf{A_1}$ *as their structure matrix.*

For each of the $3,413,774$ distinct cell permutations p, we want to evaluate the cryptographic properties of the corresponding cipher that is obtained by substituting the original cell permutation of Midori by p. In particular, we would like to compute an exact lower bound on the minimum number of active S-boxes.

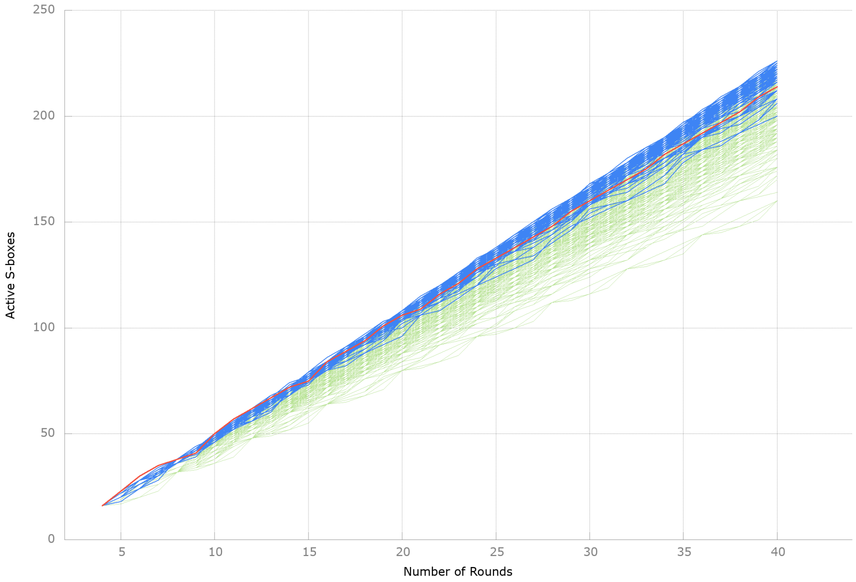


Figure 3: Bounds on the number of active S-boxes for the original Midori permutation (red), the permutations which reach at least once the optimal bound for $9 \leq r \leq 40$ (blue) and all permutations which have an all-1 structure matrix (green). We did not consider permutations guaranteeing only 40 or less active S-boxes over 10 rounds, so *optimal* refers to the best bound over all permutations that have more than 40 active S-boxes over 10 rounds.

Note that it is not clear that all permutations which lead to an optimal number of active S-boxes have the all-1 structure matrix. In fact, out of the 2218 optimal classes for 8 rounds, 162 do not have the all-1 structure matrix. However, this was the only number of rounds for which we observed this kind of behavior.

4.1 Computing the Minimum Number of Active S-boxes

There are several ways to compute exact lower bounds on the minimum number of active S-boxes for a given number of rounds in designs like Midori, for instance Matsui's algorithm [16] or MILP [17].

In order to find the exact bounds, we applied Matsui's algorithm[3] on all of the $2^{21.7}$ candidates. It turned out to be significantly more efficient than the MILP approach due to the highly-limited valid MixColumns transitions (see Figure 10). The most interesting observation is that the Midori cell permutation is in fact *not optimal for all number of rounds simultaneously*. In particular, there are four permutations upto equivalence that guarantee 44 active S-boxes for 9 rounds, while the permutation used in Midori only guarantees 41. We illustrated our results in Figure 3 and provide a selection of cell permutations that lead to optimal bounds on the number of active S-boxes in Appendix C.1.

In the case of Midori, the designers looked at a subset of cell permutations $\mathcal{S}_{\text{opt}}$ (which they called *optimal cell permutations*) by first filtering all row-based permutations according to Condition 1 and then applying a column permutation for which Condition 2 or Condition 3 holds. We recall those conditions as stated in [2, pp. 15-16].

- **Condition 1**: After applying a cell-permutation once and twice, each input cell in a column is mapped into a cell in the different column.

[3] You can find our implementation of the algorithm at https://github.com/kste/matsui.

- **Condition 2**: After applying a cell-permutation twice and twice inversely, each input cell in a column is mapped into a cell in the same row.
- **Condition 3**: After applying a cell-permutation once and three times inversely, each input cell in a column is mapped into a cell in the same row.

For our optimal cell permutations for 9 rounds (and all permutations in this equivalence class), we checked whether any of them contains a member in $\mathcal{S}_{\text{opt}}$. This is not the case, so it shows that these conditions are neither strictly necessary nor sufficient to maximize the number of active S-boxes.

5 Case Study – The Best Cell Permutations for Skinny

The lightweight block cipher Skinny has a similar structure as Midori, i.e., a 4×4 state using a word size of $s = 4$ for the 64-bit block-size version and $s = 8$ for the 128-bit version. However, Skinny uses a ShiftRows permutation and the MixColumns matrix is very sparse.

In order to find the best cell permutations for Skinny, we first used a similar approach as described in Algorithm 1 to obtain all permutations up to $\mathbf{M}$-equivalence. The difference to the case of Midori is that only for $24 = 4!$ permutations p, the operation $\mathsf{Permute}_p$ commutes with the $\mathsf{Mix}_{\mathbf{M}}$ operation. Those are exactly the 24 permutations in $\mathcal{P}_{\rightleftharpoons}$. Therefore, we did not use the separation into different structure matrices as we did for Midori. Instead, we iterated through all 16! permutations and checked which of them are canonical representatives of their equivalence class, i.e., which are the smallest by conjugation with all permutations in $\mathcal{P}_{\rightleftharpoons}$. The number of equivalence classes is $\approx 2^{39.66}$ and it took about 23.8 CPU days on an Intel Xeon E5-2660 to find all classes. To further reduce the number of permutations to consider, we filtered them by the minimum number of rounds required to reach full diffusion in forward and backward direction. We limited it to either requiring at most 6 rounds in both directions or less than 6 rounds in at least one direction to reach full diffusion. Note that the original Skinny permutation required 6 rounds for full diffusion in both directions. We found that there exist slightly better permutations with regard to diffusion in the sense that they require 5 rounds in forward direction and 6 rounds in backward direction. However, they do not lead to optimal bounds on the number of active S-boxes.

After the diffusion filtering, there were still 2,726,526 permutations left. For all of those permutations, we found the minimum number of active S-boxes up to 40 rounds using Matsui's algorithm. This process took approximately 2937 CPU days. The results are summarized in Figure 4 and Appendix C.2.

6 Proof on the Minimum Number of Active S-boxes for the Midori Cell Permutation

The designers of Midori did not provide a theoretical proof why their cell permutation guarantees a much higher number of active S-boxes compared to the ShiftRows permutation. In this section, we formally prove that any non-trivial six-round trail in Midori has at least 28 active S-boxes. In particular, we show a much stronger result which states a simple sufficient condition on the cell permutation p.

Proposition 4. *Let $p \in \mathcal{S}_{16}$ be a cell permutation on a 4×4 state and let $\mathbf{M}$ be the MixColumns matrix of* Midori*. If p, p^2 and p^3 have $\mathbf{A_1}$ as their structure matrix, the corresponding AES-like cipher instantiated with p and $\mathbf{M}$ guarantees at least 28 active S-boxes over 6 rounds.*

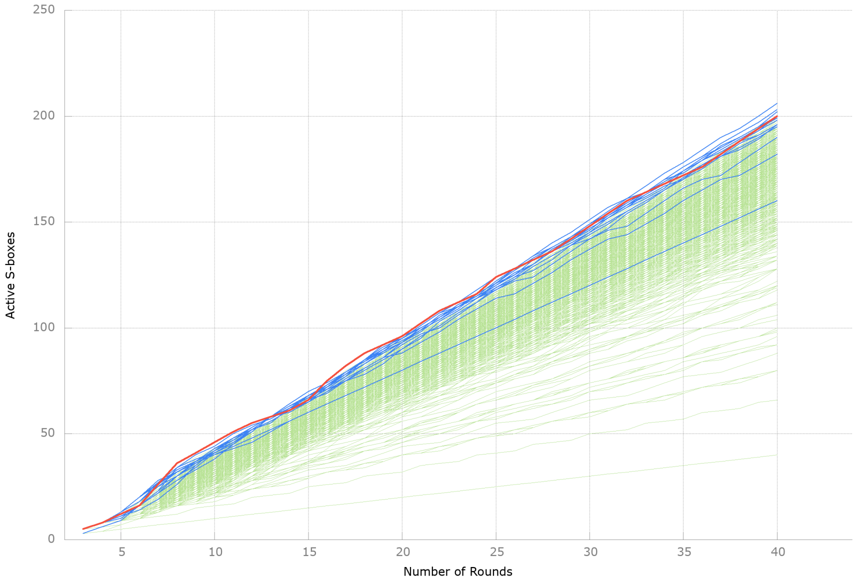


Figure 4: Bounds on the number of active S-boxes for the original Skinny permutation (red), the permutations which reach at least once the optimal bound for $7 \leq r \leq 40$ after filtering them for diffusion (blue) and a random sample of 10000 permutations after filtering them for diffusion (green). There might be permutations attaining better bounds, but having worse diffusion.

Proof. The corresponding six-round AES-like cipher can be equivalently expressed as the three-round SP cipher $\mathsf{SE}_{\mathsf{K},3}$ using the *Super S-box* representation.[4] An S-layer consists of $\mathsf{SB} \circ \mathsf{Mix}_{\mathbf{M}} \circ \mathsf{SB}$, which is regarded as four column-wise 16-bit functions (aka. *Super S-boxes*) $\mathsf{F}\colon \mathbb{F}_{(2^4)^4} \to \mathbb{F}_{(2^4)^4}$, and a P-layer consists of $\mathsf{Permute}_p \circ \mathsf{Mix}_{\mathbf{M}} \circ \mathsf{Permute}_p$. Let an input state of an i-th round of $\mathsf{SE}_{\mathsf{K},3}$ be denoted as IS_{i-1}, and let an internal state before the first $\mathsf{Permute}_p$, $\mathsf{Mix}_{\mathbf{M}}$, and the the second $\mathsf{Permute}_\mathsf{p}$ of an i-th round be denoted as $IS_{i-1}^{(a)}$, $IS_{i-1}^{(b)}$, and $IS_{i-1}^{(c)}$, respectively. Figure 5 illustrates this three-round equivalent SP cipher $\mathsf{SE}_{\mathsf{K},3}$, where the last P-layer is omitted (since it does not affect the number of active S-boxes of $\mathsf{SE}_{\mathsf{K},3}$).

If p, p^2 and p^3 have $\mathbf{A_1}$ as its structure matrix, each input cell in a column is mapped into different columns after applying $\mathsf{Permute}_p$, $\mathsf{Permute}_{p^2}$ and $\mathsf{Permute}_{p^3}$, respectively. Since the branch number of $\mathbf{M}$ is 4 and p has $\mathbf{A_1}$ as its structure matrix, any two rounds of $\mathsf{SE}_{\mathsf{K},3}$ have at least 4 active Super S-boxes, and each Super S-box has at least 4 active S-boxes. Thus, $\mathsf{SE}_{\mathsf{K},3}$ has at least 5 active Super S-boxes (20 active S-boxes) over 3 rounds. To prove that $\mathsf{SE}_{\mathsf{K},3}$ has at least 28 active S-boxes, we will show that there is no valid (non-zero) trail with 5 or 6 active Super S-boxes that attains less than 28 active S-boxes. A valid trail with 5 active Super S-boxes would necessarily be of the form $(1 \to 3 \to 1)$ and, for 6 active Super S-boxes, there are only the four possible cases $(1 \to 3 \to 2)$, $(1 \to 4 \to 1)$, $(2 \to 2 \to 2)$, and $(2 \to 3 \to 1)$. Since p^{-1}, p^{-2}, and p^{-3} also have $\mathbf{A_1}$ as their structure matrix, if the trail of $(1 \to 3 \to 2)$ does not exist, the trail of $(2 \to 3 \to 1)$ does not exist as well and so we only have to consider the four other cases. For a state IS_i, we define $w_{as}[IS_i] := (n_0, n_1, n_2, n_3, n_4)$, where n_j is the number of columns having j active cells in IS_i. For instance, if there are two columns having three active cells, one column having two active cells, and the remaining one column having one active cell in the state IS_2, we have $w_{as}[IS_2] = (0, 1, 1, 2, 0)$.

[4] We omit the key addition for simplicity as it does not change the activity pattern of a trail.

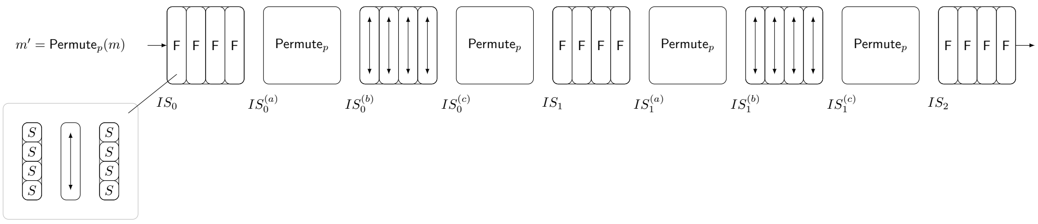


Figure 5: The three-round Super S-box SP cipher $\mathsf{SE}_{\mathsf{K},3}$: An equivalent representation of the six-round AES-like cipher employing a cell permutation p and the MixColumns matrix of Midori.

Case of (1 → 3 → 1 or 1 → 3 → 2): We consider only the case $w_{as}[IS_0^{(a)}] = (0,1,0,0,0)$. Otherwise, i.e., if the active column of $IS_0^{(a)}$ has two, three, or four active cells, it would lead to 4 active Super S-boxes in the second round (see description of the case $(1 \to 4 \to 1)$ and Figure 7). If $w_{as}[IS_0^{(a)}]$ is $(0,1,0,0,0)$, then $w_{as}[IS_1^{(a)}]$ becomes $(0,0,0,3,0)$, since one active cell leads to three active cells by $\mathbf{M}$, and three active cells are mapped into different columns by $\mathsf{Permute}_p$ as shown in Figure 6. The four cells of the blank column in $IS_1^{(a)}$ (yellow cells in Figure 6) are mapped into different columns in $IS_1^{(b)}$ by $\mathsf{Permute}_p$, and the three inactive cells of the remaining three column in $IS_1^{(a)}$ (blue cells in Figure 6), which come from a single column of $IS_0^{(c)}$, are mapped into different columns in $IS_1^{(b)}$ due to the property of p^2. Thus, $w_{as}[IS_1^{(b)}]$ must be $(0,0,3,1,0)$. After applying $\mathbf{M}$, if there would be a column with three or four active cells in $IS_1^{(c)}$, we would have three or four active Super S-boxes in the third round due to the property of p. So, we only focus on the case where two active cells remain two active cells, and three active cells become one active cell by $\mathbf{M}$, namely $w_{as}[IS_1^{(c)}] = (0,1,3,0,0)$ (see the possible transitions depicted in Figure 10). In this case, the two sets of three inactive cells that come from a single column of $IS_0^{(c)}$ and $IS_1^{(a)}$, respectively, remain in $IS_1^{(c)}$ (blue and yellow cells in Figure 6). According to the property of p^2 and p^3, the three inactive cells in each set are mapped into different columns in IS_2. Furthermore, the remaining three inactive cells in $IS_1^{(c)}$ (white cells in Figure 6) are also mapped into different columns. Thus, there must be 4 active columns in IS_2. Therefore, there is no valid trail of the form $(1 \to 3 \to 1)$ or $(1 \to 3 \to 2)$.

Case of (1 → 4 → 1): We start with three states of $IS_0^{(a)}$ in which a single column of $IS_0^{(a)}$ has two, three, or four active cells, i.e.,

$$w_{as}[IS_0^{(a)}] \in \{(0,0,1,0,0),(0,0,0,1,0),(0,0,0,0,1)\} \ .$$

We will see that those lead to 4 active Super S-boxes in the second round. To show the impossibility of a trail of the form $(1 \to 4 \to 1)$ with less than 28 active S-boxes, we use a miss-in-the-middle approach between IS_1 and $IS_1^{(a)}$. We will first investigate possible values of $w_{as}[IS_1]$ that are derived from the three start states of $w_{as}[IS_0^{(a)}]$.

- $w_{as}[IS_0^{(a)}] = (0,0,1,0,0)$: $w_{as}[IS_0^{(c)}]$ becomes $(0,0,0,2,0)$ by the deterministic transition of one to three active S-boxes of $\mathbf{M}$, and the property of p. Since the two sets of four inactive cells in a blank column (yellow cells in the top of

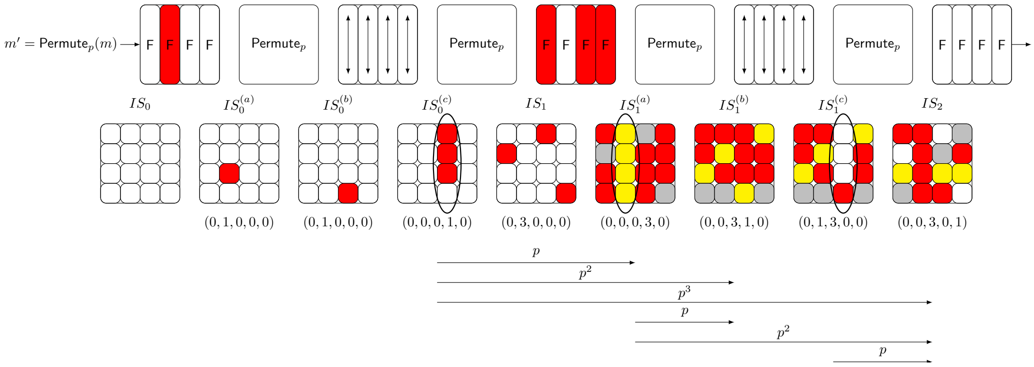


Figure 6: A differential trail of the form $(1 \rightarrow 3 \rightarrow 1)$ or $(1 \rightarrow 3 \rightarrow 2)$ in $\mathsf{SE}_{\mathsf{K},3}$, where $\mathsf{Permute}_p$ is instantiated by the original cell permutation of Midori.

Figure 7) are mapped into different columns by $\mathsf{Permute}_p$, and the two inactive cells of the remaining two columns (blue cells in the top of Figure 7) are mapped to different columns due to the property of p^2, we have $w_{as}[IS_1] = (0, 2, 2, 0, 0)$.

- $w_{as}[IS_0^{(a)}] = (0, 0, 0, 1, 0)$: $w_{as}[IS_0^{(c)}]$ becomes $(0, 0, 0, 3, 0)$. Since the four inactive cells in a blank column (yellow cells) are mapped into different columns by $\mathsf{Permute}_p$, and the three inactive cells of the remaining three columns (blue cells) are mapped into different columns, we have $w_{as}[IS_1] = (0, 0, 3, 1, 0)$.
- $w_{as}[IS_0^{(a)}] = (0, 0, 0, 0, 1)$: $w_{as}[IS_0^{(c)}]$ becomes $(0, 0, 0, 4, 0)$. Since the four inactive cells of four columns (blue cells) are mapped into different columns, we have $w_{as}[IS_1] = (0, 0, 0, 4, 0)$.

Thus, $w_{as}[IS_1] \in \{(0, 2, 2, 0, 0), (0, 0, 3, 1, 0), (0, 0, 0, 4, 0)\}$. Since p^{-1}, p^{-2}, and p^{-3} also have $\mathbf{A_1}$ as their structure matrix and since $\mathbf{M}$ is an involution, we also have $w_{as}[IS_1^{(a)}] \in \{(0, 2, 2, 0, 0), (0, 0, 3, 1, 0), (0, 0, 0, 4, 0)\}$ when it is inversely computed from the three start states of $w_{as}[IS_2] \in \{(0, 0, 1, 0, 0), (0, 0, 0, 1, 0), (0, 0, 0, 0, 1)\}$. According to the possible transitions of $\mathbf{M}$ (see Figure 10), valid transitions are only

$$w_{as}[IS_1] = (0, 0, 3, 1, 0) \rightarrow w_{as}[IS_1^{(a)}] = (0, 0, 3, 1, 0) \ ,$$
$$w_{as}[IS_1] = (0, 0, 0, 4, 0) \rightarrow w_{as}[IS_1^{(a)}] = (0, 0, 0, 4, 0) \ .$$

- $w_{as}[IS_1^{(a)}] = (0, 0, 3, 1, 0)$: According to the property of $\mathbf{M}$ (see Figure 10), the positions of the two active cells in three columns of IS_1 and $IS_1^{(a)}$ are the same. Thus, two sets of three inactive cells that come from a single column of $IS_0^{(a)}$ and $IS_0^{(c)}$, respectively, remain in $IS_1^{(a)}$ (blue and yellow cells in the middle of Figure 6), and the three inactive cells in each set are mapped into different columns in $IS_1^{(b)}$ by the property of p^2 and p^3. In this case, $w_as[IS_1^{(b)}]$ can never become $(0, 0, 0, 3, 0)$, which would be necessary for a trail of this form. Thus, such a trail is invalid.
- $w_{as}[IS_1^{(a)}] = (0, 0, 0, 4, 0)$: Since this trail has $24 (= 4 \times 3 \times 2)$ active S-boxes in the Super S-boxes in the second round, the number of active S-boxes is at least $32\ (\ = 24 + 4 + 4)$.

Therefore, there is no valid trail of $(1 \rightarrow 4 \rightarrow 1)$ attaining less than 28 active S-boxes.

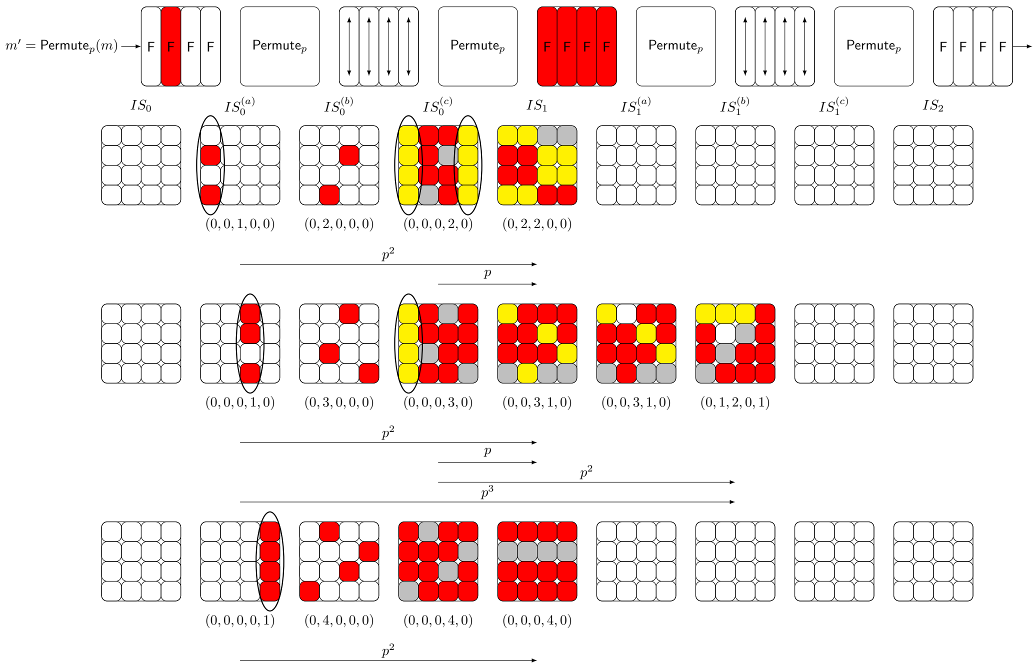


Figure 7: Differential trails of the form $(1 \to 4 \to 1)$ in $\mathsf{SE}_{\mathsf{K},3}$, where $\mathsf{Permute}_p$ is instantiated by the original cell permutation of Midori.

Case of (2 → 2 → 2): We focus on the four start states in which the two active columns of $IS_0^{(a)}$ have the same number of active cells, i.e.,

$$w_{as}[IS_0^{(a)}] \in \{(0,2,0,0,0),(0,0,2,0,0),(0,0,0,2,0),(0,0,0,0,2)\} .$$

If the number of active cells of the two active columns is different, $IS_0^{(b)}$ would have at least one column having only one active cell. This would lead to more than 3 active Super S-boxes in the second round as shown in Figure 8. To show the impossibility of a trail of the form $(2 \to 2 \to 2)$ with less than 28 active S-boxes by a miss-in-the-middle approach, we will investigate possible values of $w_{as}[IS_1]$ that are derived from the four start states of $w_{as}[IS_0^{(a)}]$.

- $w_{as}[IS_0^{(a)}] = (0,2,0,0,0)$: After applying $\mathsf{Permute}_p$, we have $w_{as}[IS_0^{(b)}] \in \{(0,2,0,0,0),(0,0,1,0,0)\}$. If $w_{as}[IS_0^{(b)}] = (0,2,0,0,0)$, one active cell of a column in $IS_0^{(b)}$ leads to 3 active Super S-boxes as discussed before. In the case of $w_{as}[IS_0^{(b)}] = (0,0,1,0,0)$, only if the two active cells of the active column in $w_{as}[IS_0^{(b)}]$ remain two active cells in $w_{as}[IS_0^{(c)}]$, it leads to 2 active Super S-boxes as shown in the top of Figure 9. Otherwise, i.e., if two active cells become four active cells by $\mathbf{M}$, it causes 4 active Super S-boxes by $\mathsf{Permute}_p$. Thus, $w_{as}[IS_1] = (0,2,0,0,0)$.
- $w_{as}[IS_0^{(a)}] = (0,0,2,0,0)$: We have

  $$w_{as}[IS_0^{(b)}] \in \{(0,0,2,0,0),(0,2,1,0,0),(0,4,0,0,0)\} .$$

  If $w_{as}[IS_0^{(b)}]$ is $(0,2,1,0,0)$ or $(0,4,0,0,0)$, one active cell of a column in $IS_0^{(b)}$ causes 3 active Super S-boxes. $w_{as}[IS_0^{(b)}] = (0,0,2,0,0)$ must become

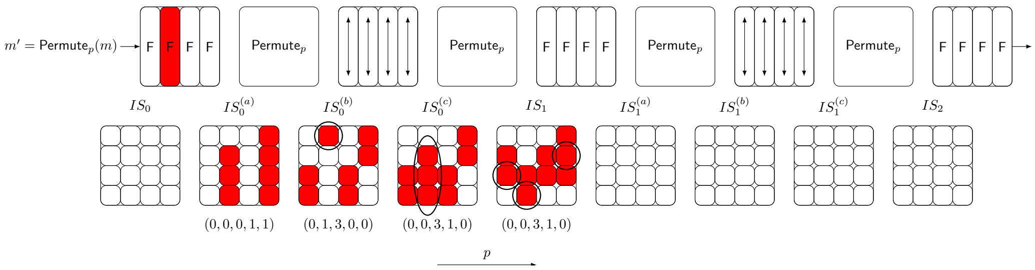


Figure 8: A differential trail of the form $(2 \to 2 \to 2)$ in $\mathsf{SE}_{\mathsf{K},3}$, where the number of active cells of two active columns in $IS_0^{(a)}$ is different and where $\mathsf{Permute}_p$ is instantiated by the original cell permutation of Midori.

$w_{as}[IS_0^{(c)}] = (0,0,2,0,0)$ after applying $\mathbf{M}$, otherwise it leads to four active Super S-boxes. Due to the property of p, $w_{as}[IS_1]$ must be $(0,0,2,0,0)$.

- $w_{as}[IS_0^{(a)}] = (0,0,0,2,0)$: We have $w_{as}[IS_0^{(b)}] \in \{(0,0,3,0,0),(0,2,2,0,0)\}$. If $w_{as}[IS_0^{(b)}]$ is $(0,2,2,0,0)$, one active cell of a column in $IS_0^{(b)}$ would lead to 3 active Super S-boxes. $w_{as}[IS_0^{(b)}] = (0,0,3,0,0)$ becomes $w_{as}[IS_0^{(c)}] = (0,0,3,0,0)$ after applying $\mathbf{M}$, otherwise four active cells in $IS_0^{(c)}$ would lead to four active Super S-boxes. Since the four inactive cells of each blank column in $IS_0^{(a)}$ (blues cell in the bottom of Figure 9) are mapped into different columns in $w_{as}[IS_1]$ by the property of p^2, and the remaining two inactive cells in $IS_0^{(c)}$ (yellow cells in the bottom of Figure 9) are mapped into different columns in $w_{as}[IS_1]$ by $\mathsf{Permute}_p$, we have $w_{as}[IS_1] = (0,2,2,0,0)$, which causes four active Super S-boxes.
- $w_{as}[IS_0^{(a)}] = (0,0,0,0,2)$: There are at least $12(= 4 \times 2 + 2 \times 2)$ active S-boxes in the first round. Thus $\mathsf{SE}_{\mathsf{K},3}$ has at least $28(= 12 + 2 \times 4 + 2 \times 4)$ active S-boxes.

Therefore, $w_{as}[IS_1]$ should be $(0,2,0,0,0)$ or $(0,0,2,0,0)$. Since p^{-1}, p^{-2}, and p^{-3} also have $\mathbf{A_1}$ as their structure matrix and since $\mathbf{M}$ is an involution, $w_{as}[IS_1^{(a)}]$ should also be $(0,2,0,0,0)$ or $(0,0,2,0,0)$ in the backward direction. According to the possible transitions of $\mathbf{M}$ (see Figure 10), a valid transition is only

$$w_{as}[IS_1] = (0,0,2,0,0) \to w_{as}[IS_1^{(a)}] = (0,0,2,0,0) \,.$$

In the forward direction, this trail always follows the transition of two active cells to two active cells in $\mathbf{M}$. According to the property of $\mathbf{M}$ (see Figure 10), the position of two active cells does not change after applying $\mathbf{M}$ in this transition. Thus, the positions of active cells are controlled by only three operations of $\mathsf{Permute}_p$ in these rounds. Due to the property of p, p^2 and p^3, all four active cells must be mapped to different columns in $IS_1^{(b)}$. More precisely, as shown in the middle of Figure 9, the property of p, p^2 and p^3 ensures that the cell indexed by A must not be in the same column of cells indexed by B, D, and C, respectively, in $IS_1^{(b)}$. The other cells indexed by B, C, D are also ensured by these properties. Since $IS_1^{(b)}$ must be $(0,4,0,0,0)$, which causes at least 3 active Super S-boxes in the third round, there is no valid trail of the form $(2 \to 2 \to 2)$ with less than 28 active S-boxes.

Therefore, there is no valid (non-trivial) trail attaining less than 28 active S-boxes. □

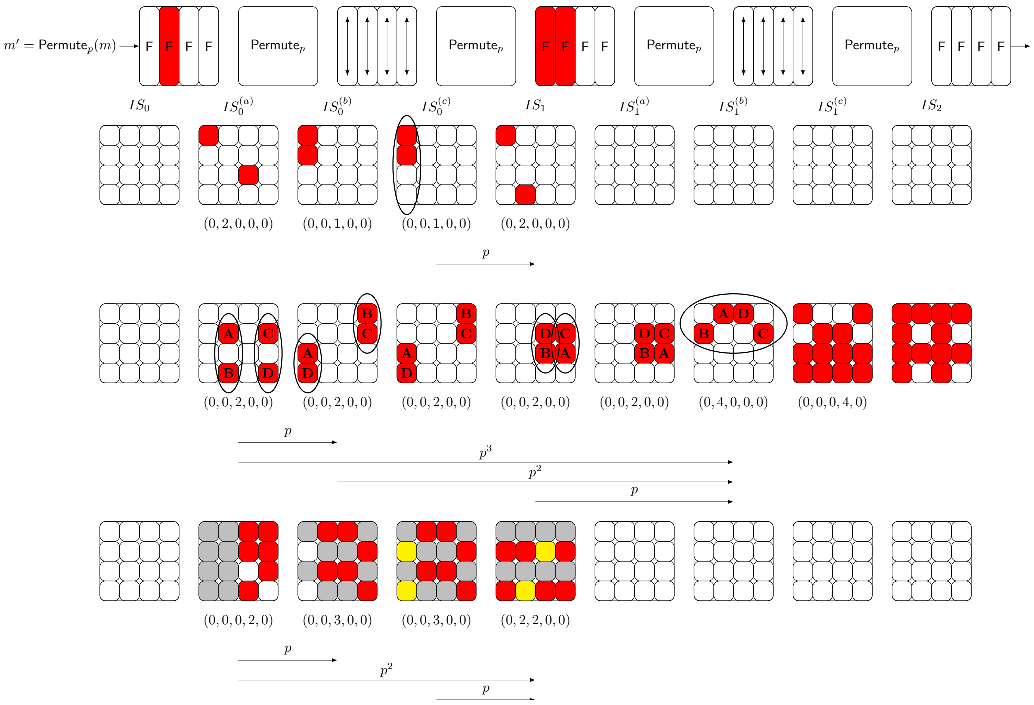


Figure 9: Differential trails of the form$(2 \to 2 \to 2)$ in $\mathsf{SE}_{\mathsf{K},3}$, where $\mathsf{Permute}_p$ is instantiated by the original cell permutation of Midori.

7 Conclusion

In this work, we showed that it is feasible to classify *all* cell permutations for ciphers like Midori and Skinny and to find the optimal cell permutations with respect to diffusion and the minimum number of active S-boxes. We showed how the full search space can be reduced by classifying all the cell permutations up to a reasonable notion of equivalence.

We determined the exact bounds on the minimum number of active S-boxes using Matsui's approach. We provided several new permutations which can achieve a higher number of active S-boxes as the original cell permutations used in those primitives. Note that we only considered active S-boxes with regard to *differential cryptanalysis*. For Midori, the number of active S-boxes with regard to linear cryptanalysis is actually the same. For Skinny, the bounds for linear cryptanalysis have to be computed separately. For that, one could also use our implementation of Matsui's algorithm.

Overall, we think the methods presented in this work will be particular useful for future designers as they allow to explore the whole design space for cell permutations. Moreover, for the particular MixColumns operations used in Skinny and Midori, designers could now easily pick the cell permutation that best suit their security goals, depending on the their choice of S-box.

References

[1] R. Avanzi. The QARMA block cipher family. *IACR Trans. Symm. Cryptol.*, 2017(1):4–44, 2017.

[2] S. Banik, A. Bogdanov, T. Isobe, K. Shibutani, H. Hiwatari, T. Akishita, and F. Regazzoni. Midori: A block cipher for low energy. In T. Iwata and J. H. Cheon, editors, *ASIACRYPT 2015, Part II*, volume 9453 of *LNCS*, pages 411–436. Springer, Heidelberg, Nov. / Dec. 2015.

[3] P. S. Barreto and V. Rijmen. The ANUBIS Block Cipher. NESSIE submission, 2000. http://www.larc.usp.br/~pbarreto/AnubisPage.html.

[4] P. S. Barreto and V. Rijmen. The Whirlpool Hashing Function. NESSIE submission, 2000. http://www.larc.usp.br/~pbarreto/WhirlpoolPage.html.

[5] C. Beierle. *Design and analysis of lightweight block ciphers: a focus on the linear layer*. Doctoral thesis, Ruhr-Universität Bochum, Universitätsbibliothek, 2018.

[6] C. Beierle, J. Jean, S. Kölbl, G. Leander, A. Moradi, T. Peyrin, Y. Sasaki, P. Sasdrich, and S. M. Sim. The SKINNY family of block ciphers and its low-latency variant MANTIS. In M. Robshaw and J. Katz, editors, *CRYPTO 2016, Part II*, volume 9815 of *LNCS*, pages 123–153. Springer, Heidelberg, Aug. 2016.

[7] C. Beierle, P. Jovanovic, M. M. Lauridsen, G. Leander, and C. Rechberger. Analyzing permutations for AES-like ciphers: Understanding ShiftRows. In K. Nyberg, editor, *CT-RSA 2015*, volume 9048 of *LNCS*, pages 37–58. Springer, Heidelberg, Apr. 2015.

[8] J. Borghoff, A. Canteaut, T. Güneysu, E. B. Kavun, M. Knežević, L. R. Knudsen, G. Leander, V. Nikov, C. Paar, C. Rechberger, P. Rombouts, S. S. Thomsen, and T. Yalçin. PRINCE - A low-latency block cipher for pervasive computing applications - extended abstract. In X. Wang and K. Sako, editors, *ASIACRYPT 2012*, volume 7658 of *LNCS*, pages 208–225. Springer, Heidelberg, Dec. 2012.

[9] J. Daemen. *Cipher and hash function design strategies based on linear and differential cryptanalysis*. PhD thesis, Doctoral Dissertation, March 1995, KU Leuven, 1995.

[10] J. Daemen, L. R. Knudsen, and V. Rijmen. The block cipher Square. In E. Biham, editor, *FSE'97*, volume 1267 of *LNCS*, pages 149–165. Springer, Heidelberg, Jan. 1997.

[11] J. Daemen and V. Rijmen. *The design of Rijndael: AES-the advanced encryption standard*. Springer-Verlag Berlin Heidelberg, 2002.

[12] J. Guo, T. Peyrin, and A. Poschmann. The PHOTON family of lightweight hash functions. In P. Rogaway, editor, *CRYPTO 2011*, volume 6841 of *LNCS*, pages 222–239. Springer, Heidelberg, Aug. 2011.

[13] J. Guo, T. Peyrin, A. Poschmann, and M. J. B. Robshaw. The LED block cipher. In B. Preneel and T. Takagi, editors, *CHES 2011*, volume 6917 of *LNCS*, pages 326–341. Springer, Heidelberg, Sept. / Oct. 2011.

[14] K. Khoo, E. Lee, T. Peyrin, and S. M. Sim. Human-readable proof of the related-key security of aes-128. *IACR Trans. Symm. Cryptol.*, 2017(2):59–83, 2017.

[15] C. H. Lim and T. Korkishko. mCrypton - a lightweight block cipher for security of low-cost RFID tags and sensors. In J. Song, T. Kwon, and M. Yung, editors, *WISA 05*, volume 3786 of *LNCS*, pages 243–258. Springer, Heidelberg, Aug. 2006.

[16] M. Matsui. On correlation between the order of S-boxes and the strength of DES. In A. D. Santis, editor, *EUROCRYPT'94*, volume 950 of *LNCS*, pages 366–375. Springer, Heidelberg, May 1995.

[17] N. Mouha, Q. Wang, D. Gu, and B. Preneel. Differential and linear cryptanalysis using mixed-integer linear programming. In C.-K. Wu, M. Yung, and D. Lin, editors, *Information Security and Cryptology*, volume 7537 of *LNCS*, pages 57–76. Springer Berlin Heidelberg, 2012.

[18] PUB FIPS. 197: Advanced encryption standard (AES). *National Institute of Standards and Technology*, 2001. Available online at `http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf`.

[19] S. Sun, L. Hu, P. Wang, K. Qiao, X. Ma, and L. Song. Automatic security evaluation and (related-key) differential characteristic search: Application to SIMON, PRESENT, LBlock, DES(L) and other bit-oriented block ciphers. In P. Sarkar and T. Iwata, editors, *ASIACRYPT 2014, Part I*, volume 8873 of *LNCS*, pages 158–178. Springer, Heidelberg, Dec. 2014.

[20] Y. Todo and K. Aoki. Wide trail design strategy for binary MixColumns - enhancing lower bound of number of active S-boxes. In M. Manulis, A.-R. Sadeghi, and S. Schneider, editors, *ACNS 16*, volume 9696 of *LNCS*, pages 467–484. Springer, Heidelberg, June 2016.

A MixColumns Propagation in Midori and Skinny

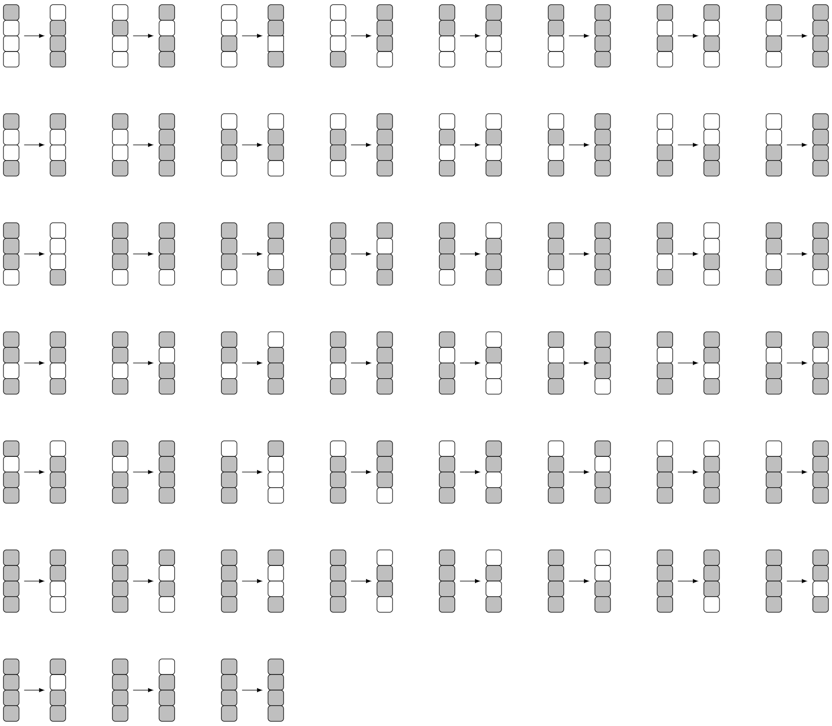


Figure 10: All possible transitions from active nibbles in a column to active nibbles after applying the Midori MixColumns matrix.

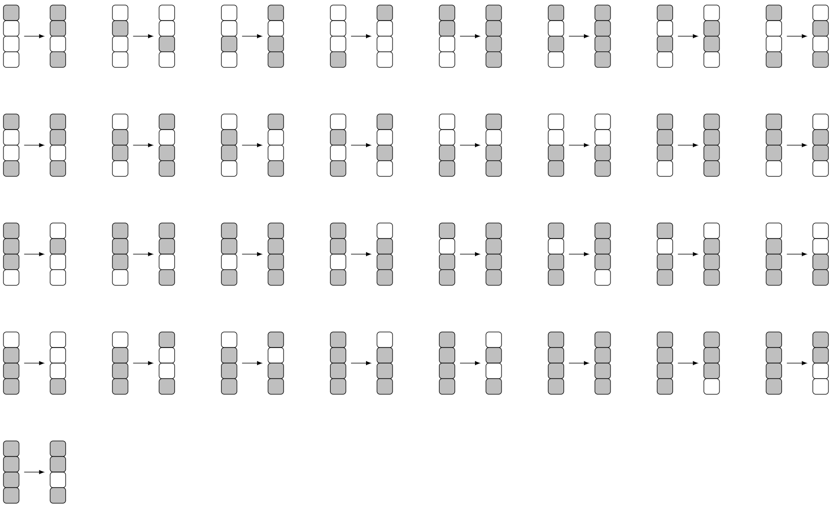


Figure 11: All possible transitions from active nibbles in a column to active nibbles after applying the Skinny MixColumns matrix.

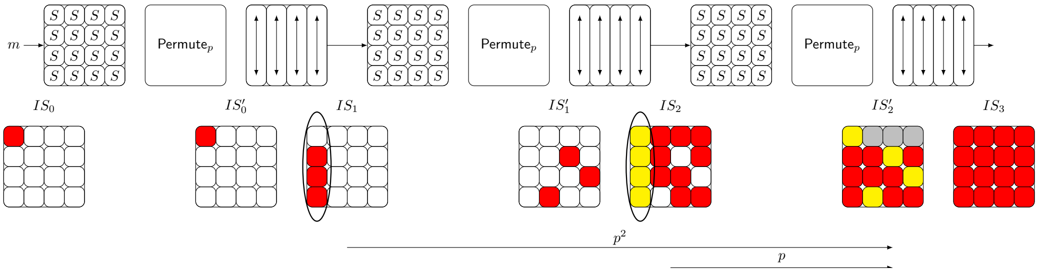


Figure 12: The diffusion property over three rounds of the AES-like cipher employing the MixColumns matrix of Midori and a cell permutation p that fulfills the condition that p and p^2 both have $\mathbf{A_1}$ as their structure matrix.

B Proof of Proposition 3

Let the input state of the i-th round be IS_{i-1} and let the internal state before $\mathsf{Mix}_{\mathsf{M}}$ of the i-th round be IS'_{i-1} as shown in Figure 12. If both p and p^2 have $\mathbf{A_1}$ as their structure matrix, each input cell in a column is mapped into different columns after applying both $\mathsf{Permute}_p$ and $\mathsf{Permute}_p \circ \mathsf{Permute}_p$.

We fix a single cell in IS_0 for which we analyze the propagation of the dependencies in the subsequent states. We refer to the cells that depend on this single cell as *active* cells. The active cell in IS_0 activates three cells of a single column in IS_1 after applying $\mathbf{M}$. According to the property of p, those three cells are permuted into different columns in IS'_1 and then activate 9 cells in IS_2 after applying $\mathbf{M}$, where three columns have 3 active cells and the remaining column does not have any active cell (we call it a *blank column*). In the third round, the four cells of the blank column in IS_2 (yellow cells in Figure 12) are mapped into four different columns after applying $\mathsf{Permute}_p$. In addition, each inactive cell of the remaining three columns in IS_2 (blue cells) is mapped into a different column in IS'_2 due to the property of p^2 (those inactive cells all come from a single column in IS_1). Therefore, IS'_2 has three columns with 2 active cells and one column with 3 active cells. Since 2 and 3 active cells in a column affect all cells in a corresponding column after applying $\mathbf{M}$, all 16 cells in IS_3 become active. Thus, if both p and p^2 have $\mathbf{A_1}$ as their structure matrix, it achieves the three-round full diffusion.

On the other hand, for three-round full diffusion, each column of IS'_2 must have at least two active cells, because one active cell in a column activates only three cells after applying $\mathbf{M}$. This implies that IS'_2 and IS_2 must have at least 8 active cells. Recall that a single active cell in IS_0 activates three cells of a single column in IS_1. Only if p ensures that each cell of a column in IS_1 is mapped into different columns after applying $\mathsf{Permute}_p$ in round two, it achieves 9 active cells in IS_2 by $\mathsf{Mix}_{\mathbf{M}}$. Otherwise, the number of active cells would be at most 7. Therefore, p must have $\mathbf{A_1}$ as its structure matrix. Furthermore, in the case of the a single active cell in IS_0, IS_2 must consist of three columns with 3 active cells and one blank column. Only if p ensures that each cell of a column in IS_1 is mapped into different columns after applying $\mathsf{Permute}_p \circ \mathsf{Permute}_p$, each column of IS'_2 has at least two active cells, which results in the full diffusion. Otherwise, there would exist a column having 0 or 1 active cell only. Therefore, the condition that p and p^2 have $\mathbf{A_1}$ as their structure matrix is also necessary to achieve three-round full diffusion.

Since p^{-1} and p^{-2} also have $\mathbf{A_1}$ as their structure matrix whenever p and p^2 have and since $\mathbf{M}$ is an involution, this holds also in the inverse direction. □

C Optimal Permutations

In C.1, we list *some* equivalence classes of permutations for the Midori MixColumns matrix that lead to optimal[5] bounds on the number of active S-boxes for *some* number of rounds between 9 and 40. We provide the actual bounds and the number of rounds for full diffusion in both forward and backward direction. Any optimal bound is emphasized in red. The first line represents the actual permutation used in the primitive. Note that, as the transpose of the MixColumns matrix is identical to the inverse of the matrix, those bounds are also valid for the case of linear cryptanalysis.

In C.2, we give a list of *all* equivalence classes of permutations for the Skinny MixColumns matrix that

- require at most 6 rounds for full diffusion in both forward and backward direction or require less than 6 rounds for full diffusion in at least one direction, and
- lead to optimal[6] bounds on the number of active S-boxes for *some* number of rounds between 7 and 40.

We provide the actual bounds and the number of rounds for full diffusion in both forward and backward direction. Any optimal bound is emphasized in red. The first line represents the actual permutation used in the primitive. Note that those bounds are not valid for the case of linear cryptanalysis.

[5] *Optimal* refers to the best bound over all permutations that have more than 40 active S-boxes over 10 rounds.

[6] *Optimal* refers to the best bound over all permutations that require at most 6 rounds for full diffusion in both forward and backward direction or require less than 6 rounds for full diffusion in at least one direction.

C.1 Midori

		Rounds																																			
$[\mathbf{p}]_\sim$	Diff	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
[0 4 8 12 5 9 3 13 14 1 6 11 10 7 15 2]	(3,3)	23	30	35	38	41	50	57	62	67	72	75	84	89	94	101	106	109	116	121	128	133	138	143	148	155	160	165	170	175	182	187	192	197	202	209	214
[1 4 8 12 2 6 13 9 10 5 14 0 15 3 11 7]	(3,3)	23	30	35	38	41	50	57	62	67	72	75	84	89	94	101	106	109	116	121	128	133	138	143	148	155	160	165	170	175	182	187	192	197	202	209	214
[0 4 8 12 5 9 1 13 10 14 6 3 15 2 11 7]	(3,3)	23	28	33	38	41	48	55	61	67	72	77	82	91	95	102	108	113	118	125	131	137	142	149	154	161	166	173	178	183	190	195	202	208	213	219	226
[0 4 8 12 9 1 5 13 14 10 3 6 7 15 11 2]	(3,3)	23	28	33	38	41	48	55	61	67	72	77	82	91	95	102	108	113	118	125	131	137	142	149	154	161	166	173	178	183	190	195	202	208	213	219	226
[0 4 8 12 5 2 9 13 10 14 6 3 15 7 1 11]	(3,3)	23	28	33	38	41	50	55	60	65	70	77	84	88	96	99	104	111	116	120	128	132	136	144	148	152	160	164	168	176	180	184	192	196	200	208	212
[0 4 8 12 5 2 9 13 14 6 3 10 11 15 7 1]	(3,3)	23	28	33	38	41	50	55	60	65	70	77	84	88	96	99	104	111	116	120	128	132	136	144	148	152	160	164	168	176	180	184	192	196	200	208	212
[0 4 8 12 5 9 3 13 10 6 14 1 15 2 11 7]	(3,3)	23	28	30	36	42	50	54	56	62	68	78	80	82	88	94	104	106	108	114	120	130	132	134	140	146	156	158	160	166	172	182	184	186	192	198	208
[0 4 8 12 5 9 3 13 14 2 7 10 11 6 1 15]	(3,3)	20	28	34	38	42	48	57	62	64	70	76	81	88	94	99	103	109	116	121	126	131	138	142	148	153	158	165	170	175	180	185	192	197	202	207	212
[0 4 8 12 9 1 7 13 14 10 3 6 5 2 11 15]	(3,3)	20	28	34	38	42	48	57	62	64	70	76	81	88	94	99	103	109	116	121	126	131	138	142	148	153	158	165	170	175	180	185	192	197	202	207	212
[0 4 8 12 9 1 7 13 14 10 5 2 6 3 15 11]	(3,3)	23	28	30	36	42	50	54	56	62	68	78	80	82	88	94	104	106	108	114	120	130	132	134	140	146	156	158	160	166	172	182	184	186	192	198	208
[0 4 8 12 9 2 5 13 14 6 3 10 7 15 11 1]	(3,3)	23	28	30	36	42	50	54	56	62	68	78	80	82	88	94	104	106	108	114	120	130	132	134	140	146	156	158	160	166	172	182	184	186	192	198	208
[1 4 8 12 2 6 13 9 10 7 3 14 15 0 5 11]	(3,3)	20	28	34	38	42	48	57	62	64	70	76	81	88	94	99	103	109	116	121	126	131	138	142	148	153	158	165	170	175	180	185	192	197	202	207	212
[1 4 8 12 9 0 7 13 2 6 11 14 15 10 3 5]	(3,3)	20	28	34	38	42	48	57	62	64	70	76	81	88	94	99	103	109	116	121	126	131	138	142	148	153	158	165	170	175	180	185	192	197	202	207	212
[0 4 8 12 2 6 9 13 7 14 3 11 5 15 10 1]	(4,4)	18	24	30	38	44	48	52	56	60	70	76	80	84	88	92	96	106	112	116	120	124	128	132	142	148	152	156	160	164	168	178	184	188	192	196	200
[0 4 8 12 2 6 9 13 10 3 7 14 11 1 5 15]	(4,4)	18	24	30	38	44	48	52	56	60	70	76	80	84	88	92	96	106	112	116	120	124	128	132	142	148	152	156	160	164	168	178	184	188	192	196	200
[1 4 8 12 2 6 13 9 5 10 0 14 3 15 7 11]	(4,4)	18	24	30	38	44	48	52	56	60	70	76	80	84	88	92	96	106	112	116	120	124	128	132	142	148	152	156	160	164	168	178	184	188	192	196	200
[1 4 8 12 5 9 2 13 0 14 6 10 3 15 7 11]	(4,4)	18	24	30	38	44	48	52	56	60	70	76	80	84	88	92	96	106	112	116	120	124	128	132	142	148	152	156	160	164	168	178	184	188	192	196	200
[0 4 8 12 2 6 9 13 14 7 3 10 15 5 1 11]	(4,4)	20	28	34	38	43	48	54	62	68	72	76	82	88	96	100	104	110	116	122	128	132	138	144	150	156	160	166	172	178	184	188	194	200	206	212	216
[1 4 8 12 5 2 9 13 14 7 3 10 11 15 6 0]	(4,4)	22	28	32	38	41	48	54	60	68	72	75	82	88	95	100	104	109	116	120	128	132	136	143	148	152	160	164	168	176	180	184	192	196	200	208	212
[0 4 8 12 2 5 9 13 7 1 10 14 11 15 6 3]	(4,4)	20	28	32	38	41	50	55	60	67	74	77	83	91	94	101	107	111	118	125	130	137	142	147	154	159	164	171	178	181	188	195	200	206	212	217	224
[0 4 8 12 2 5 9 13 7 1 10 14 15 11 3 6]	(4,4)	20	28	32	38	41	50	55	60	67	74	77	83	91	94	101	107	111	118	125	130	137	142	147	154	159	164	171	178	181	188	195	200	206	212	217	224
[0 4 8 12 2 6 9 13 7 1 10 14 11 15 5 3]	(4,4)	22	28	33	38	41	48	55	62	67	74	77	84	90	96	102	108	113	120	125	130	136	142	148	154	160	166	170	176	182	188	195	200	206	210	216	222
[0 4 8 12 2 6 13 9 5 1 10 14 15 11 3 7]	(4,4)	22	28	33	38	41	48	55	62	67	74	77	84	90	96	102	108	113	120	125	130	136	142	148	154	160	166	170	176	182	188	195	200	206	210	216	222
[0 4 8 12 5 9 1 13 7 10 2 14 11 15 3 6]	(4,4)	22	28	32	38	41	48	56	62	67	74	77	84	90	95	101	108	113	118	124	130	137	144	149	154	160	166	173	178	184	190	196	201	207	214	220	226
[0 4 8 12 5 9 1 13 14 10 2 6 7 3 15 11]	(4,4)	22	28	32	38	41	48	56	62	67	74	77	84	90	95	101	108	113	118	124	130	137	144	149	154	160	166	173	178	184	190	196	201	207	214	220	226
[0 4 8 12 5 2 9 13 7 14 1 10 15 11 3 6]	(4,4)	20	28	32	38	43	48	55	60	67	72	79	84	89	96	101	108	114	120	125	130	137	144	148	155	161	166	171	178	183	190	197	201	207	212	219	225
[0 4 8 12 5 2 9 13 10 1 14 7 11 15 6 3]	(4,4)	20	28	32	38	43	48	55	60	67	72	79	84	89	96	101	108	114	120	125	130	137	144	148	155	161	166	171	178	183	190	197	201	207	212	219	225
[0 4 8 12 5 9 1 13 14 3 6 10 7 15 11 2]	(4,4)	22	26	31	38	43	48	53	60	65	72	79	84	87	96	101	108	113	120	123	130	137	141	147	154	160	166	172	177	183	188	195	201	207	212	219	224
[0 4 8 12 5 9 1 13 14 6 2 10 7 3 15 11]	(4,4)	22	28	33	38	43	50	55	62	67	72	79	84	90	96	101	108	114	120	126	130	136	142	148	154	160	166	172	176	182	188	194	200	206	212	218	222
[0 4 8 12 5 9 1 13 14 10 6 2 7 15 11 3]	(4,4)	22	28	33	38	43	50	55	62	67	72	79	84	90	96	101	108	114	120	126	130	136	142	148	154	160	166	172	176	182	188	194	200	206	212	218	222
[0 4 8 12 5 9 1 13 14 10 6 3 15 7 2 11]	(4,4)	22	28	32	38	43	48	55	60	65	72	79	84	89	96	101	106	113	118	125	130	135	142	147	152	157	164	169	176	181	186	193	198	203	208	215	220
[0 4 8 12 5 9 1 13 14 10 7 3 6 15 2 11]	(4,4)	22	28	33	38	43	48	53	60	67	72	79	84	89	96	101	106	113	118	125	130	137	142	147	152	159	164	171	178	183	188	195	200	205	212	217	224
[0 4 8 12 5 9 2 13 14 3 6 10 15 1 7 11]	(4,4)	20	28	31	38	43	48	55	60	65	72	79	84	89	96	101	108	113	118	123	130	137	143	147	154	159	166	171	176	181	188	195	201	205	212	217	224
[0 4 8 12 5 9 2 13 14 3 7 11 6 15 1 10]	(4,4)	22	28	33	38	43	50	57	62	67	72	79	86	91	96	101	108	115	120	125	132	137	144	150	156	161	166	173	180	185	190	195	202	209	214	221	226
[0 4 8 12 5 9 3 13 7 14 1 11 15 10 2 6]	(4,4)	22	28	33	38	43	50	57	62	67	72	79	86	91	96	101	108	115	120	125	132	137	144	150	156	161	166	173	180	185	190	195	202	209	214	221	226
[0 4 8 12 5 9 3 13 14 6 2 10 11 1 15 7]	(4,4)	22	26	31	38	43	48	53	60	65	72	79	84	87	96	101	108	113	120	123	130	137	141	147	154	160	166	172	177	183	188	195	201	207	212	219	224
[0 4 8 12 9 1 5 13 14 3 7 10 11 15 2 6]	(4,4)	22	28	33	38	43	48	53	60	67	72	79	84	89	96	101	106	113	118	125	130	137	142	147	152	159	164	171	178	183	188	195	200	205	212	217	224
[0 4 8 12 9 1 5 13 14 10 6 3 11 7 15 2]	(4,4)	22	28	32	38	43	48	55	60	65	72	79	84	89	96	101	106	113	118	125	130	135	142	147	152	157	164	169	176	181	186	193	198	203	208	215	220
[0 4 8 12 9 2 7 13 6 10 3 14 11 15 5 1]	(4,4)	20	28	31	38	43	48	55	60	65	72	79	84	89	96	101	108	113	118	123	130	137	143	147	154	159	166	171	176	181	188	195	201	205	212	217	224
[1 4 8 12 0 6 9 13 3 10 7 14 15 2 5 11]	(4,4)	22	28	32	38	43	48	55	60	65	72	79	82	88	96	101	106	113	118	123	130	136	142	149	154	159	164	171	177	181	188	195	198	204	212	217	222
[1 4 8 12 0 6 9 13 3 14 7 10 15 2 11 5]	(4,4)	22	28	31	36	43	49	55	61	67	72	79	84	91	96	102	108	113	120	125	132	138	142	149	156	161	166	173	178	184	190	197	202	207	214	220	226
[1 4 8 12 0 6 9 13 5 10 14 3 2 15 11 7]	(4,4)	20	28	31	38	43	48	55	60	67	72	79	82	89	96	101	108	113	118	125	130	135	142	149	154	161	166	171	178	183	188	195	202	207	212	219	224
[1 4 8 12 0 6 9 13 5 14 2 10 15 7 3 11]	(4,4)	22	28	32	38	43	48	55	60	65	72	79	84	89	96	101	106	113	118	123	130	137	142	147	154	159	164	171	176	183	188	195	200	205	212	217	222
[1 4 8 12 0 6 9 13 7 10 3 14 2 15 5 11]	(4,4)	22	28	31	36	43	49	55	61	67	72	79	84	91	96	102	108	113	120	125	132	138	142	149	156	161	166	173	178	184	190	197	202	207	214	220	226
[0 4 8 12 2 5 9 13 7 14 1 11 10 6 3 15]	(4,4)	22	28	32	38	41	48	57	61	67	72	75	84	91	97	103	106	109	118	125	133	137	140	143	152	159	168	171	174	177	186	193	202	205	208	211	220
[0 4 8 12 2 5 9 13 14 1 7 11 10 6 3 15]	(4,4)	22	28	32	38	41	48	57	61	67	72	75	84	91	97	103	106	109	118	125	133	137	140	143	152	159	168	171	174	177	186	193	202	205	208	211	220
[0 4 8 12 5 9 1 13 10 2 14 7 15 11 3 6]	(4,4)	22	28	32	38	41	48	57	61	67	72	75	84	91	97	103	106	109	118	125	133	137	140	143	152	159	168	171	174	177	186	193	202	205	208	211	220
[0 4 8 12 5 9 3 13 10 1 14 7 15 11 2 6]	(4,4)	22	28	32	38	41	48	57	61	67	72	75	84	91	97	103	106	109	118	125	133	137	140	143	152	159	168	171	174	177	186	193	202	205	208	211	220
[0 4 8 12 9 1 5 13 14 10 2 7 6 11 15 3]	(4,4)	22	28	32	38	41	48	57	61	67	72	75	84	91	97	103	106	109	118	125	133	137	140	143	152	159	168	171	174	177	186	193	202	205	208	211	220
[0 4 8 12 9 3 5 13 14 10 1 7 6 11 15 2]	(4,4)	22	28	32	38	41	48	57	61	67	72	75	84	91	97	103	106	109	118	125	133	137	140	143	152	159	168	171	174	177	186	193	202	205	208	211	220
[0 4 8 12 2 6 9 13 10 14 5 3 7 1 11 15]	(4,4)	22	28	32	38	41	48	55	62	65	72	77	84	90	94	101	108	113	120	126	130	137	144	149	154	159	166	171	178	181	190	195	200	207	214	217	224
[0 4 8 12 2 6 13 9 7 3 10 14 11 15 5 1]	(4,4)	22	28	32	38	41	48	55	62	65	72	77	84	90	94	101	108	113	120	126	130	137	144	149	154	159	166	171	178	181	190	195	200	207	214	217	224
[0 4 8 12 2 6 13 9 7 10 14 1 11 3 15 5]	(4,4)	22	28	32	38	42	48	55	62	67	72	78	84	90	96	102	108	114	119	126	132	138	144	150	155	160	168	173	178	184	190	196	203	208	214	220	226
[0 4 8 12 2 6 13 9 14 1 7 10 5 15 3 11]	(4,4)	22	28	32	38	42	48	55	62	67	72	78	84	90	96	102	108	114	119	126	132	138	144	150	155	160	168	173	178	184	190	196	203	208	214	220	226
[0 4 8 12 2 6 13 9 7 10 1 14 5 15 11 3]	(4,4)	22	28	33	38	43	48	55	62	67	72	78	84	90	96	101	108	113	120	125	131	137	144	149	154	161	166	173	178	184	190	196	202	207	214	219	226
[0 4 8 12 2 6 13 9 10 1 7 14 15 3 11 5]	(4,4)	22	28	33	38	43	48	55	62	67	72	78	84	90	96	101	108	113	120	125	131	137	144	149	154	161	166	173	178	184	190	196	202	207	214	219	226
[0 4 8 12 1 6 9 13 7 3 10 14 15 5 2 11]	(4,4)	20	28	33	38	41	49	55	60	67	72	77	84	90	96	102	108	113	118	125	131	137	142	149	154	161	166	173	178	184	190	195	202	207	214	220	226
[0 4 8 12 1 6 9 13 14 7 3 10 5 2 11 15]	(4,4)	20	28	33	38	41	49	55	60	67	72	77	84	90	96	102	108	113	118	125	131	137	142	149	154	161	166	173	178	184	190	195	202	207	214	220	226
[0 4 8 12 2 5 9 13 7 10 1 14 11 3 15 6]	(4,4)	22	28	32	38	43	48	55	60	67	72	78	84	89	96	101	108	113	119	125	132	137	143	149	154	161	167	173	178	185	190	196	202	208	214	220	226
[0 4 8 12 2 5 9 13 10 1 7 14 6 15 3 11]	(4,4)	22	28	32	38	43	48	55	60	67	72	78	84	89	96	101	108	113	119	125	132	137	143	149	154	161	167	173	178	185	190	196	202	208	214	220	226

C.2 Skinny

		Rounds																																
[p]~	Diff	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
[0 5 10 15 4 9 14 3 8 13 2 7 12 1 6 11]	(6,6)	26	36	41	46	51	55	58	61	66	75	82	88	92	96	102	108	112	116	124	128	132	136	142	148	154	160	164	168	172	176	182	188	194	200
[4 1 10 15 12 5 2 11 0 9 14 7 8 13 6 3]	(6,6)	26	36	41	46	51	55	58	61	66	75	82	88	92	96	102	108	112	116	124	128	132	136	142	148	154	160	164	168	172	176	182	188	194	200
[4 9 2 15 0 13 6 11 12 5 10 3 8 1 14 7]	(6,6)	26	36	41	46	51	55	58	61	66	75	82	88	92	96	102	108	112	116	124	128	132	136	142	148	154	160	164	168	172	176	182	188	194	200
[4 9 14 3 8 13 2 7 12 1 6 11 0 5 10 15]	(6,6)	26	36	41	46	51	55	58	61	66	75	82	88	92	96	102	108	112	116	124	128	132	136	142	148	154	160	164	168	172	176	182	188	194	200
[0 1 6 11 4 5 14 3 8 9 2 15 12 13 10 7]	(6,6)	28	32	36	40	44	48	52	56	60	64	68	72	76	80	84	88	92	96	100	104	108	112	116	120	124	128	132	136	140	144	148	152	156	160
[0 5 10 15 4 1 14 11 12 9 2 7 8 13 6 3]	(6,6)	28	32	36	40	43	46	51	56	60	64	68	72	76	80	84	88	92	96	100	104	108	112	116	120	124	128	132	136	140	144	148	152	156	160
[4 5 2 11 8 9 6 15 12 13 10 3 0 1 14 7]	(6,6)	28	32	36	40	44	48	52	56	60	64	68	72	76	80	84	88	92	96	100	104	108	112	116	120	124	128	132	136	140	144	148	152	156	160
[4 5 10 3 8 9 14 7 12 13 2 11 0 1 6 15]	(6,6)	28	32	36	40	44	48	52	56	60	64	68	72	76	80	84	88	92	96	100	104	108	112	116	120	124	128	132	136	140	144	148	152	156	160
[4 5 10 15 0 1 14 11 12 13 6 3 8 9 2 7]	(6,6)	28	32	36	40	44	48	52	56	60	64	68	72	76	80	84	88	92	96	100	104	108	112	116	120	124	128	132	136	140	144	148	152	156	160
[4 9 2 15 0 13 10 7 12 1 6 11 8 5 14 3]	(6,6)	28	32	36	40	43	46	51	56	60	64	68	72	76	80	84	88	92	96	100	104	108	112	116	120	124	128	132	136	140	144	148	152	156	160
[0 7 8 13 12 1 6 9 10 3 14 5 2 11 4 15]	(6,6)	26	32	37	42	47	52	58	63	68	72	78	83	88	93	98	105	110	114	120	125	130	136	141	146	153	158	162	167	170	177	181	184	189	196
[0 7 8 15 10 13 2 5 6 1 14 9 12 11 4 3]	(6,6)	27	32	37	42	47	52	58	60	65	70	76	81	86	88	93	98	104	109	114	116	121	126	132	137	142	144	149	154	160	165	170	172	177	182
[0 1 4 9 6 11 2 15 10 7 14 3 12 13 8 5]	(6,6)	26	32	37	42	47	53	58	63	68	72	77	85	90	96	100	105	111	115	120	126	130	136	143	148	153	159	164	170	173	179	186	190	195	202
[0 1 4 9 8 7 2 15 6 3 12 5 10 11 14 13]	(6,6)	22	28	34	41	46	51	58	62	66	69	75	80	85	90	95	103	108	114	118	123	129	134	139	144	149	155	160	165	170	175	181	187	191	196
[0 1 4 9 14 11 2 7 12 13 10 5 6 15 8 3]	(6,6)	25	32	37	43	47	52	58	61	66	73	79	84	90	94	99	104	109	116	121	125	130	136	141	147	152	158	163	168	174	180	185	190	195	200
[0 1 4 11 2 9 12 13 6 3 8 5 14 7 10 15]	(6,6)	22	28	34	41	46	51	58	62	66	69	75	80	85	90	95	103	108	114	118	123	129	134	139	144	149	155	160	165	170	175	181	187	191	196
[0 1 4 11 10 7 14 5 12 9 2 13 6 3 8 15]	(6,6)	19	26	35	42	46	52	58	62	66	71	75	78	83	90	96	101	107	112	119	124	127	132	139	142	147	154	159	165	171	176	182	188	191	196
[0 1 4 11 10 9 6 15 8 7 2 13 14 3 12 5]	(6,6)	19	26	35	42	46	52	58	62	66	71	75	78	83	90	96	101	107	112	119	124	127	132	139	142	147	154	159	165	171	176	182	188	191	196
[0 1 6 11 2 15 8 5 14 3 4 9 12 13 10 7]	(6,6)	26	32	37	42	47	53	58	63	68	72	77	85	90	96	100	105	111	115	120	126	130	136	143	148	153	159	164	170	173	179	186	190	195	202
[0 1 6 11 4 5 2 15 12 13 10 7 8 9 14 3]	(6,6)	27	34	38	41	46	52	58	64	70	74	79	85	91	95	101	107	112	118	124	128	134	140	145	151	157	161	167	173	178	184	190	194	200	206
[0 1 6 11 12 13 4 9 14 3 10 5 2 7 8 15]	(6,6)	25	32	37	43	47	52	58	61	66	73	79	84	90	94	99	104	109	116	121	125	130	136	141	147	152	158	163	168	174	180	185	190	195	200
[0 1 6 11 12 13 10 7 8 9 14 3 4 5 2 15]	(6,6)	27	34	38	41	46	52	58	64	70	74	79	85	91	95	101	107	112	118	124	128	134	140	145	151	157	161	167	173	178	184	190	194	200	206
[2 5 10 13 8 15 0 7 4 3 12 11 14 9 6 1]	(6,6)	27	32	37	42	47	52	58	60	65	70	76	81	86	88	93	98	104	109	114	116	121	126	132	137	142	144	149	154	160	165	170	172	177	182
[2 7 8 13 0 5 10 15 12 9 6 3 14 11 4 1]	(6,6)	27	32	37	42	47	52	58	60	65	70	76	81	86	88	93	98	104	109	114	116	121	126	132	137	142	144	149	154	160	165	170	172	177	182
[2 7 8 15 6 3 12 11 0 1 10 13 4 5 14 9]	(6,6)	22	30	37	43	48	53	58	63	68	71	77	83	89	95	100	105	110	115	120	125	130	136	140	145	150	155	160	165	170	175	181	185	190	195
[2 7 10 15 0 1 4 9 12 13 8 5 14 11 6 3]	(6,6)	22	30	37	43	48	53	58	63	68	71	77	83	89	95	100	105	110	115	120	125	130	136	140	145	150	155	160	165	170	175	181	185	190	195
[4 1 8 13 10 15 0 7 6 3 12 9 2 5 14 11]	(6,6)	26	32	37	42	47	52	58	63	68	72	78	83	88	93	98	105	110	114	120	125	130	136	141	146	153	158	162	167	170	177	181	184	189	196
[4 3 10 13 12 9 0 7 2 11 14 5 6 15 8 1]	(6,6)	25	30	36	41	45	51	58	62	68	73	78	83	88	93	99	106	110	114	119	124	130	137	142	147	152	157	161	166	174	179	183	188	193	200
[4 3 10 13 12 9 0 7 6 1 8 15 2 5 14 11]	(6,6)	25	30	35	42	48	52	58	63	67	73	79	84	89	93	99	106	110	115	120	125	132	136	142	148	153	158	164	169	174	179	184	189	194	199
[4 3 10 13 14 7 0 9 2 5 12 11 6 15 8 1]	(6,6)	22	28	33	38	45	52	58	61	65	70	75	81	86	93	99	104	110	114	119	123	129	134	139	145	152	157	163	168	172	177	182	188	193	198
[4 3 10 15 8 13 6 1 14 5 2 11 0 7 12 9]	(6,6)	25	30	35	42	48	52	58	63	67	73	79	84	89	93	99	106	110	115	120	125	132	136	142	148	153	158	164	169	174	179	184	189	194	199
[4 5 2 11 12 13 10 3 0 1 6 15 8 9 14 7]	(6,6)	27	34	38	41	46	52	58	64	70	74	79	85	91	95	101	107	112	118	124	128	134	140	145	151	157	161	167	173	178	184	190	194	200	206
[4 5 8 1 14 3 10 7 12 13 0 9 6 11 2 15]	(6,6)	22	30	37	43	48	53	58	63	68	71	77	83	89	95	100	105	110	115	120	125	130	136	140	145	150	155	160	165	170	175	181	185	190	195
[4 5 8 13 0 1 12 9 14 11 2 7 10 15 6 3]	(6,6)	26	32	37	42	47	53	58	63	68	72	77	85	90	96	100	105	111	115	120	126	130	136	143	148	153	159	164	170	173	179	186	190	195	202
[4 5 10 1 14 7 0 11 12 13 2 9 6 15 8 3]	(6,6)	22	30	37	43	48	53	58	63	68	71	77	83	89	95	100	105	110	115	120	125	130	136	140	145	150	155	160	165	170	175	181	185	190	195
[4 5 10 3 12 13 2 11 0 1 14 7 8 9 6 15]	(6,6)	27	34	38	41	46	52	58	64	70	74	79	85	91	95	101	107	112	118	124	128	134	140	145	151	157	161	167	173	178	184	190	194	200	206
[4 5 10 15 0 1 14 11 2 7 8 13 6 3 12 9]	(6,6)	26	32	37	42	47	53	58	63	68	72	77	85	90	96	100	105	111	115	120	126	130	136	143	148	153	159	164	170	173	179	186	190	195	202
[4 9 0 13 2 15 6 11 14 3 8 5 10 7 12 1]	(6,6)	22	28	33	38	45	52	58	61	65	70	75	81	86	93	99	104	110	114	119	123	129	134	139	145	152	157	163	168	172	177	182	188	193	198
[4 9 2 15 14 3 8 5 12 1 10 7 6 11 0 13]	(6,6)	27	32	37	42	47	52	58	60	65	70	76	81	86	88	93	98	104	109	114	116	121	126	132	137	142	144	149	154	160	165	170	172	177	182
[4 11 0 9 10 13 6 1 14 3 12 5 2 7 8 15]	(6,6)	23	30	37	41	46	51	58	61	65	70	76	81	86	92	97	100	106	112	118	122	124	130	136	142	146	148	154	160	166	170	172	178	184	190
[4 11 0 15 2 13 6 9 14 5 8 3 10 7 12 1]	(6,6)	25	30	36	41	45	51	58	62	68	73	78	83	88	93	99	106	110	114	119	124	130	137	142	147	152	157	161	166	174	179	183	188	193	200
[4 11 2 9 10 13 0 7 14 3 12 5 6 15 8 1]	(6,6)	23	30	37	41	46	51	58	61	65	70	76	81	86	92	97	100	106	112	118	122	124	130	136	142	146	148	154	160	166	170	172	178	184	190
[0 5 11 2 8 13 3 10 12 9 7 14 4 1 15 6]	(6,6)	23	34	40	44	50	54	57	62	65	72	79	85	92	95	101	107	110	116	121	127	133	138	143	149	155	161	164	170	176	181	187	192	197	203
[0 5 11 6 8 13 3 14 12 9 7 10 4 1 15 2]	(6,6)	23	34	40	44	50	54	57	62	65	72	79	85	92	95	101	107	110	116	121	127	133	138	143	149	155	161	164	170	176	181	187	192	197	203
[0 7 8 15 12 1 4 9 2 13 10 5 14 11 6 3]	(6,6)	26	33	37	42	46	52	56	61	68	73	79	85	88	93	100	105	110	115	122	128	132	138	143	148	154	159	164	170	176	181	185	190	195	202
[2 7 8 15 6 3 12 11 0 5 10 13 4 1 14 9]	(6,6)	26	32	37	41	46	52	55	62	67	72	78	85	89	93	100	105	110	114	121	128	134	138	143	149	154	159	164	169	174	179	184	189	194	199
[2 7 10 15 12 1 4 9 0 13 8 5 14 11 6 3]	(6,6)	26	32	37	41	46	52	55	62	67	72	78	85	89	93	100	105	110	114	121	128	134	138	143	149	154	159	164	169	174	179	184	189	194	199
[4 1 10 13 14 7 0 11 12 5 2 9 6 3 8 15]	(6,6)	26	33	37	42	46	52	56	61	68	73	79	85	88	93	100	105	110	115	122	128	132	138	143	148	154	159	164	170	176	181	185	190	195	202
[4 9 12 1 10 15 2 7 6 3 14 11 8 5 0 13]	(6,6)	26	32	37	41	46	52	55	62	67	72	78	85	89	93	100	105	110	114	121	128	134	138	143	149	154	159	164	169	174	179	184	189	194	199
[4 9 14 1 10 7 0 15 6 11 12 3 8 5 2 13]	(6,6)	26	32	37	41	46	52	55	62	67	72	78	85	89	93	100	105	110	114	121	128	134	138	143	149	154	159	164	169	174	179	184	189	194	199