Analyzing Permutations for AES-like Ciphers: Understanding ShiftRows†

Christof Beierle[1], Philipp Jovanovic[2], Martin M. Lauridsen[3], Gregor Leander[1⋆], and Christian Rechberger[3]

[1] Horst Görtz Institute for IT Security, Ruhr-Universität Bochum, Germany
{christof.beierle, gregor.leander}@rub.de
[2] Fakultät für Informatik und Mathematik, Universität Passau, Germany
jovanovic@fim.uni-passau.de
[3] DTU Compute, Technical University of Denmark, Denmark
{mmeh, crec}@rub.de

Abstract. Designing block ciphers and hash functions in a manner that resemble the AES in many aspects has been very popular since Rijndael was adopted as the Advanced Encryption Standard. However, in sharp contrast to the `MixColumns` operation, the security implications of the way the state is permuted by the operation resembling `ShiftRows` has never been studied in depth.

Here, we provide the first structured study of the influence of `ShiftRows`-like operations, or more generally, word-wise permutations, in AES-like ciphers with respect to diffusion properties and resistance towards differential- and linear attacks. After formalizing the concept of guaranteed trail weights, we show a range of equivalence results for permutation layers in this context. We prove that the trail weight analysis when using arbitrary word-wise permutations, with rotations as a special case, reduces to a consideration of a specific normal form. Using a mixed-integer linear programming approach, we obtain optimal parameters for a wide range of AES-like ciphers, and show improvements on parameters for Rijndael-192, Rijndael-256, PRIMATEs-80 and Prøst-128. As a separate result, we show for specific cases of the state geometry that a seemingly optimal bound on the trail weight can be obtained using cyclic rotations only for the permutation layer, i.e. in a very implementation friendly way.

Keywords: AES, AES-like, differential cryptanalysis, linear cryptanalysis, diffusion, optimization, mixed-integer linear programming

1 Introduction

Since 2000 with the standardization of Rijndael [14] as the Advanced Encryption Standard (AES), an astonishing number of new primitives using components similar to the AES have seen the light of day. Examples of such include, but are not limited to, block ciphers 3D [22], ANUBIS [4], LED [19], mCrypton [24] and PRINCE [11], as well as hash functions like WHIRLPOOL [3], ECHO [7], Grøstl [17], LANE [21], PHOTON [18], Twister [16] and components of CAESAR candidates PAEQ [10], PRIMATEs [1], Prøst [23] and STRIBOB [28]. This can largely be attributed to the seminal wide-trail design strategy [15] which was introduced along with Rijndael and its predecessor SQUARE [12] for the first time.

The wide-trail strategy is an elegant way of ensuring good diffusion properties and at the same time allow designers to easily give bounds on the resistance towards differential- and linear cryptanalysis. Additionally, another advantage is that it decouples the choice of the non-linear layer and the linear layer to a large extent. In a nutshell, any good S-box combined with any good linear layer will result in a cipher resistant against linear- and differential attacks.

For AES-like ciphers, including all the above mentioned designs, the linear layer itself is composed of two parts: one resembles the AES `MixColumns` operation and the other resembles

⋆ The work of Gregor Leander was funded by the BMBF UNIKOPS project
† This is an extended version of [5] which appeared at CT-RSA 2015

the AES `ShiftRows` operation. The `MixColumns`-like operation is a matrix multiplication of the columns of the state and the `ShiftRows`-like operation is a permutation of the words of the state.

For the former, the criteria are well understood. All that is required here is that this operation has a suitably high branch number. In short, the branch number corresponds to the minimal sum of the number of active S-boxes in an input/output column, provided an active input column (and the number of active S-boxes is the essential tool for bounding the success probability of linear- and differential attacks). In stark contrast, for the operation resembling `ShiftRows`, the situation is significantly less clear. Basically, the `ShiftRows`-like operation highly influences the number of active S-boxes when considering more than two rounds only. Understanding the bounds for more than two rounds is crucial for many good designs. With a well-chosen `ShiftRows`-like operation it is usually possible to derive much stronger bounds for more rounds than the trivial bound one gets by multiplying the two-round bound by half the number of rounds.

In the case of the AES (and others including [7, 10, 11]) one uses a so-called superbox argument to prove strong bounds on four rounds of the cipher. For others, the problem is modelled as a mixed-integer linear programs like in [1, 23, 27] which allows the computation of bounds for an (in principle) arbitrary number of rounds *for a given choice of the* `ShiftRows`-like operation. However, no structured approach for analyzing the influence of the `ShiftRows`-like operation on the security of the cipher has been undertaken previously. The results so far remain ad-hoc and specific to a given choice of parameters. Considering the large number of designs following this approach, this shortcoming is quite surprising and unsatisfactory from a scientific perspective. In particular, the choices made are often not optimal and not based on an adequate understanding of the implications.

Our Contribution. In this paper, we develop a structured approach to analyzing the permutation layer, i.e. the generalized `ShiftRows`-like operation, for AES-like ciphers with respect to diffusion and resistance towards differential- and linear cryptanalysis. For this, we start by defining a general framework for AES-like ciphers. Note that we do not restrict to the case where permutation is identical in all rounds but we allow for different choices of the permutation in different rounds. Moreover, we first consider arbitrary word-wise permutations and later restrict ourselves to word-wise rotations of the rows. The latter have the appeal of being efficiently implementable on many modern CPUs. Our following analysis consists of two parts.

First, and as a core contribution to a structured approach, we simplify the problem by introducing the notion of equivalent permutation parameters. It is intuitively clear that many choices of the permutation will lead to the same behavior of the cipher. One such example is changing the order of the rotation constants for the `ShiftRows` operation in the AES, i.e. rotate the first row by 3, the second by 2, and so on. We will make this intuition precise and, as will be shown below, discover more involved examples of the above.

The notion of equivalence will imply the same lower bound on the number of guaranteed active S-boxes. This is interesting theoretically, as it allows to simplify the problem. For example, we prove that a general permutation can never yield better results than a permutation that operates on the rows individually. Furthermore, using this notion of equivalence, we derive a normalized representation of any word-wise rotation of the rows. This allows to significantly reduce the problem domain and thus the search space for a computational approach.

In the second part of our analysis, we use this normalized representation in a combination with solving mixed-integer linear programs using the IBM ILOG CPLEX library [20]. The source code for this part is available as [6]. This results in optimal parameter suggestions for a wide range of AES-like ciphers. In particular, it allows us to suggest improved parameters for Rijndael-192, Rijndael-256, PRIMATEs-80 and Prøst-128 on this front, see Table 1 for details.

Finally, given our extensive experimental results, we conjecture an optimal lower bound on the number of active S-boxes possible for specific cases of the state geometry. Those parameters are such that they allow for an iterative version of the superbox argument mentioned above. We also provide a permutation which guarantees this conjectured optimal bound. In contrast to prior work, e.g. ECHO and PAEQ, this permutation layer is generic and, more importantly, realized with *cyclic row rotations only*. Thus, it allows for an easy and efficient implementation.

Outline. In Section 2 we give notation and define what we mean by AES-like ciphers. Then, in Section 3, we introduce, besides diffusion, the concept of guaranteed active S-boxes as a measure of the resistance against differential- and linear attacks. Section 4 provides reductions in order to identify equivalent permutation parameters for AES-like ciphers. We thereby also introduce the normal form of rotation matrices, considering only cyclic rotations of the state rows. Section 5 copes with modelling the problem using a mixed-integer linear programming approach in order to calculate optimal bounds for given state dimensions. In this context, some practical examples for rotation parameters are provided. Finally, Section 6 continues with a theoretic analysis of special cases of the state dimension and presents (conjectured) optimal solutions to the main criteria. We conclude the paper in Section 7.

2 Preliminaries

We use $\mathbb{F}_{q^r}$ to denote the finite field of size q^r with q prime. We use $\mathbb{Z}_n$ to interchangeably denote the group of integers modulo n and the set $\{0, 1, \ldots, n-1\}$. We refer to binary strings in $\mathbb{F}_2^m$ as *words*. We refer to $M \times N$ matrices with word entries as *states*. For a state X we use X_i to denote the ith row of X, and $X_{i,j}$ denotes word in the jth column of X_i. Let F be a function operating on states and let $\oplus$ be bitwise addition. For words x, x' we use the term *difference* to denote $x \oplus x'$, and let the notion extend to states where the differences are word-wise. For input states x, x' to F, we refer to $x \oplus x'$ and $F(x) \oplus F(x')$ as the *input difference* and *output difference*, respectively. For an $M \times N$ difference X, we use the symbol with a tilde on top, e.g. $\tilde{X}$, to denote the *activity pattern* of X, an $M \times N$ matrix over $\mathbb{F}_2$ where $\tilde{X}_{i,j} = 1$ if $X_{i,j} \neq 0$ and $\tilde{X}_{i,j} = 0$ otherwise. For $a, b \in \mathbb{F}_2^m$ we let $\langle a, b \rangle = \bigoplus_{i=0}^{m-1} a_i \cdot b_i$ denote the inner product of a and b, where subscript i denotes the ith bit. We extend this inner product to states, s.t. for $X, Y \in (\mathbb{F}_2^m)^{M \times N}$ we have $\langle X, Y \rangle = \bigoplus_{i \in \mathbb{Z}_M, j \in \mathbb{Z}_N} \langle X_{i,j}, Y_{i,j} \rangle$.

2.1 AES-like Ciphers

With the increasing popularity of the AES since its standardization, dozens of new ciphers that follow what we refer to as an *AES-like* design have seen the light of day. We describe formally our notion of AES-like ciphers in Definition 1.

Definition 1. *An* AES-like cipher *is a block cipher E_K which is parametrized by a fixed key K, the state dimension $M \times N$, the word size m, the number of rounds T and a permutation parameter $\pi = (\pi_0, \ldots, \pi_{T-1})$, where each π_t is a permutation on $\mathbb{Z}_M \times \mathbb{Z}_N$. It is composed of round functions $\mathcal{R}_i$, s.t. $E_K = \mathcal{R}_{T-1} \circ \cdots \circ \mathcal{R}_0$. Each round function is composed of the following bijective transformations on states, s.t. $\forall t \in \mathbb{Z}_T : \mathcal{R}_t = \texttt{AddRoundKey}_t \circ \texttt{Permute}_{\pi_t} \circ \texttt{MixColumns}_t \circ \texttt{SubBytes}$:*

1. `SubBytes` *substitutes each word of the state according to one or several S-boxes $S : \mathbb{F}_2^m \to \mathbb{F}_2^m$.*
2. $\texttt{MixColumns}_t$ *applies, in round t, for all columns $j \in \mathbb{Z}_N$ left-multiplication by an $M \times M$ matrix $\texttt{M}_j^t \in (\mathbb{F}_2^m)^{M \times M}$:*

$$\texttt{MixColumns}_t : (\mathbb{F}_2^m)^{M \times N} \to (\mathbb{F}_2^m)^{M \times N}$$
$$\forall j \in \mathbb{Z}_N : (X_{0,j}, \ldots, X_{M-1,j})^T \mapsto \texttt{M}_j^t \cdot (X_{0,j}, \ldots, X_{M-1,j})^T,$$

where multiplication in $\mathbb{F}_2^m$ is defined by an arbitrary irreducible polynomial over $\mathbb{F}_2$ of degree m.

3. $\texttt{Permute}_{\pi_t}$ *permutes, in round t, the words within the state due to a given permutation π_t. We use the notation that for a position $(i,j) \in \mathbb{Z}_M \times \mathbb{Z}_N$ in the state, $\pi_t(i,j)$ gives the new position of that word under the permutation π_t:*

$$\texttt{Permute}_{\pi_t} : (\mathbb{F}_2^m)^{M \times N} \to (\mathbb{F}_2^m)^{M \times N}$$
$$\forall i \in \mathbb{Z}_M, \forall j \in \mathbb{Z}_N : X_{i,j} \mapsto X_{\pi_t(i,j)}.$$

4. $\texttt{AddRoundKey}_t$ *performs word-wise XOR to the state using the t^{th} round key.*

Subsequently, we omit the $\texttt{AddRoundKey}_t$ operation of Definition 1 from consideration, as it does not affect diffusion properties nor resistance towards differential- and linear cryptanalysis of the AES-like cipher. Note also, that for generality we consider in Definition 1 an arbitrary word permutation $\texttt{Permute}_{\pi_t}$, while later we will, for efficiency reasons, resrict ourselves to row-wise rotations of the words as in the `ShiftRows` operations of the AES.

3 Diffusion and Resistance to Differential/Linear Cryptanalysis

In this paper, we are concerned with two security aspects of an AES-like cipher, namely diffusion on the one hand and resistance against differential- and linear attacks on the other hand. We formally define our notations for both criteria in the following.

3.1 Diffusion

The first definition of diffusion is attributed to Shannon [29]. Informally, diffusion is about complicating the relationship between the ciphertext bits and plaintext bits. When designing a cipher, it is desirable to obtain what we call *full diffusion* after as few rounds as possible and indeed the number of rounds chosen for the cipher is often determined by exactly this number.

Definition 2 (Diffusion degree). *For a function $F : \mathbb{F}_2^\ell \to \mathbb{F}_2^n$, we define the* diffusion degree *$d(F)$ for F as the fraction of bits in the image under F that depend on* each bit *of the pre-image, i.e.*

$$d(F) = \frac{1}{n} \cdot \sharp \left\{ j \in \mathbb{Z}_n \mid \forall i \in \mathbb{Z}_\ell : \exists x \in \mathbb{F}_2^\ell : F(x^{(i)})_j \neq F(x)_j \right\},$$

where $F(x)_j$ denotes the jth bit of $F(x)$ and $x^{(i)}$ denotes the element x with the ith bit flipped. We say that F obtains full diffusion *when $d(F) = 1$.*

Definition 3 (Diffusion-optimality). *Fix the state dimensions $M \times N$. Consider a permutation sequence π for an AES-like cipher which obtains full diffusion after t rounds. We say that π is* diffusion-optimal *if there exists no $\pi' \neq \pi$ which obtains full diffusion after $t' < t$ rounds.*

3.2 Differential/Linear Cryptanalysis

Differential- and linear cryptanalysis were pioneered by Biham and Shamir [8, 9] and Matsui [26], respectively, to attack the DES. In a differential attack an attacker tries to predict the difference of the state after several rounds when plaintexts with a given difference are processed. In linear cryptanalysis, the attacker tries to find biased linear Boolean equations involving plaintext-, key- and ciphertext bits. Common to both attacks is that they are based on trails (or characteristics). The probability (resp. correlation) of those trails can be upper bounded by lower bounding the number of active S-boxes in any trail. Here, an S-box is active

in a given trail if it has a non-zero input difference (resp. mask). In general, if p is the largest probability (resp. correlation) for the S-box to satisfy a differential- or linear property, and any trail has at least k active S-boxes, then the trail property holds with probability (resp. correlation) at most p^k. This way of ensuring resistance against linear and differential attacks is the basis of the wide-trail-strategy as introduced by Daemen and Rijmen in [15]. The second important merit of the wide-trail starategy is that it allows to treat the S-box and the linear-layer as black boxes as long as they fulfill certain conditions. In our work, we follow both aspects of this philosophy. The designer is interested in having the lightest trail as heavy as possible. Indeed, knowing this probability is essential when determining the number of rounds for the cipher in the design phase. We give definitions of trails and trail weights in the following.

Definition 4 (Trail and trail weight). *For an AES-like cipher E_K using m-bit words and state dimension $M \times N$, a T-round* trail *is a $(T+1)$-tuple $(X^0, \ldots, X^T) \in \left((\mathbb{F}_2^m)^{M\times N}\right)^{T+1}$ and the* weight *of the trail is defined as*

$$\sum_{t\in\mathbb{Z}_T} \sum_{i\in\mathbb{Z}_M} \sum_{j\in\mathbb{Z}_N} \tilde{X}^t_{i,j}.$$

A pair of inputs $x, x' \in (\mathbb{F}_2^m)^{M\times N}$ is said to follow the differential trail $(X^0, \ldots, X^T)$ *over T rounds if and only if $X^0 = x \oplus x'$ and*

$$\forall t \in \{1, \ldots, T\} : X^t = (\mathcal{R}_{t-1} \circ \cdots \circ \mathcal{R}_0)(x) \oplus (\mathcal{R}_{t-1} \circ \cdots \circ \mathcal{R}_0)(x').$$

We say that a differential trail is valid *for E_K if and only if there exists at least one input pair which follows the trail.*

If $(\alpha^0, \ldots, \alpha^T)$ is a T-round linear trail, we say that the trail is valid *if and only if its correlation is non-zero, i.e. if*

$$\prod_{t\in\mathbb{Z}_T} \mathbf{C}_{\mathcal{R}_t}(\alpha^t, \alpha^{t+1}) \neq 0,$$

where, for $t \in \mathbb{Z}_T$, $\mathbf{C}_{\mathcal{R}_t}(\alpha^t, \alpha^{t+1})$ is the correlation over round $\mathcal{R}_t$ using input mask α^t and output mask α^{t+1}. This quantity is defined by

$$\mathbf{C}_{\mathcal{R}_t}(\alpha^t, \alpha^{t+1}) = 2 \Pr_x\big[\langle x, \alpha^t\rangle = \langle \mathcal{R}_t(x), \alpha^{t+1}\rangle\big] - 1.$$

Note from Definition 4 that the weight of a trail corresponds exactly to the number of active S-boxes over those T rounds. In the remainder of this work, we concentrate on the differential case. However, the results apply equally to linear trails as well.

Definition 5 (Branch number). *For a linear automorphism $\theta : (\mathbb{F}_2^m)^M \to (\mathbb{F}_2^m)^M$, the* differential branch number *B_θ is defined as*

$$B_\theta = \min_{\substack{x,x'\in(\mathbb{F}_2^m)^M \\ x\neq x'}} \left\{ \sum_{i\in\mathbb{Z}_M} \tilde{X}_i + \tilde{Y}_i \right\}, \qquad X = x \oplus x', Y = \theta(x) \oplus \theta(x').$$

In the context of an AES-like cipher E_K, we say E_K has branch number B_θ if and only if it is the largest integer s.t. left multiplication by any of the M_j^t used in the $\texttt{MixColumns}_t$ operation has branch number at least B_θ.

In order to calculate a useful lower bound on the number of active S-boxes in an efficient way, we focus on the $\texttt{Permute}_{\pi_t}$ part of the round function. The `SubBytes` operation will be considered as using an arbitrary S-box $S : \mathbb{F}_2^m \to \mathbb{F}_2^m$, and the analysis will be independent of

the specifc instance of S. Each of the $\mathtt{M}_j^t$ matrices used in the `MixColumns` operation will be considered as black-box linear operations, under the requirement that the AES-like cipher has branch number B_θ. A formal definition of that idea is given in the following. For a T-round permutation parameter $\pi = (\pi_0, \ldots, \pi_{T-1})$, let $\widetilde{\mathrm{AES}}_{M,N}(\pi, B_\theta)$ denote the set of all $M \times N$ AES-like ciphers over T rounds with branch number B_θ using $\pi_0, \ldots, \pi_{T-2}$ in the first $T-1$ rounds. The reason for not including π_{T-1} is that our proofs in the following use the fact that for different permutation sequences we can re-model one AES-like cipher into another, up to the last round, and up to changing `MixColumns` operations (but maintaining the branch number).

Definition 6. *We say that the sequence of permutations $\pi = (\pi_0, \ldots, \pi_{T-1})$* tightly guarantees *$k$ active S-boxes for branch number B_θ if and only if there is a valid trail of weight k for some $E_K \in \widetilde{\mathrm{AES}}_{M,N}(\pi, B_\theta)$ and there is no valid trail of weight $k' < k$, $k' > 0$, for some $E'_K \in \widetilde{\mathrm{AES}}_{M,N}(\pi, B_\theta)$. We denote this property by $\pi \xrightarrow{B_\theta} k$.*

Definition 7 (Trail-optimality). *A sequence of permutations $\pi = (\pi_0, \ldots, \pi_{T-1})$ with $\pi \xrightarrow{B_\theta} k$ is said to be* trail-optimal *if there exists no $\pi' = (\pi'_0, \ldots, \pi'_{T-1})$ s.t. $\pi' \xrightarrow{B_\theta} k'$ where $k' > k$.*

Appendix A provides a proof that the number of tightly guaranteed active S-boxes is really independent of the specific S-box instantiations. From Definition 6, it follows that the number of guaranteed active S-boxes is always a lower bound for the actual minimum number of active S-boxes in any concrete instantiation of an AES-like cipher.

4 Equivalent Permutations: Simplifying the Problem

In this section, we present a range of results which simplifies the problem of identifying good permutation parameters π for AES-like ciphers by showing when different permutation parameters are equivalent w.r.t. resistance towards differential- and linear attacks. Obviously, for a fixed branch number, many different π will tightly guarantee the same number of active S-boxes. Thus, identifying conditions under which two different permutation sequences $\pi \neq \pi'$ tightly guarantee the same bound is significant: for a theoretical understanding, this approach simplifies the problem while for a computer-aided search for a good π parameter, this significantly reduces the search space. In Definition 8, we specify what it means for two permutation sequences to be equivalent.

Definition 8 (Equivalence of permutation sequences). *Two permutation sequences π, π', for a T-round cipher, are said to be* equivalent*, denoted $\pi \sim \pi'$, if and only if for all possible branch numbers B_θ, the equality $\widetilde{\mathrm{AES}}_{M,N}(\pi, B_\theta) = \widetilde{\mathrm{AES}}_{M,N}(\pi', B_\theta)$ holds. Intuitively, this means that for all AES-like ciphers using π, there is an AES-like cipher using π' which it is functionally identical to, up until the last round.*

We remark that, using this notion of equivalence, one can transform each cipher E_K using π into a cipher E'_K using π' such that $E_K = \tau \circ E'_K$ for a permutation τ on the state words. Thus, equivalence will imply the same number of tightly guaranteed active S-boxes for all possible fixed branch numbers B_θ.

4.1 Equivalences for Permutation Sequences π

In order to prove the reduction to a normalized form on the round permutations, we show a range of observations in the following. Firstly, Lemma 9 is a combinatorial result on permutations on Cartesian products.

Lemma 9 (Representation of permutations on cartesian products). *Every permutation π_t on the words of an $M \times N$ state can be represented as $\pi_t = \gamma' \circ \phi \circ \gamma$ where γ, γ' are permuting the words within the columns and ϕ is permuting the words within the rows.*

Proof. Let $T_A, T_B, T_C, T_D \in (\mathbb{Z}_M \times \mathbb{Z}_N)^{M \times N}$ s.t. $T_{A_{i,j}} = (i, j)$ and let T_B, T_C and T_D be defined by the following diagram:

$$T_A \xrightarrow{\gamma} T_B \xrightarrow{\phi} T_C \xrightarrow{\gamma'} T_D.$$

To show the result, we let $T_D = \pi_t(T_A)$ and show how to construct the permutations such that $T_D = (\gamma' \circ \phi \circ \gamma)(T_A)$. We first observe the following two properties which must hold:

1. T_B must be a matrix where, within each column $j \in \mathbb{Z}_N$, it holds that i) the second coordinate of each point is equal to j, because γ only permutes within each column of T_A and ii) the set of first coordinates cover all of $\mathbb{Z}_M$, because T_B is a permutation of $\mathbb{Z}_M \times \mathbb{Z}_N$.
2. T_C must be a matrix where, for each column $j \in \mathbb{Z}_N$, the points in column j of T_C are the same as those in column j of T_D. This is required because otherwise going between T_C and T_D using a permutation operating in each column, is impossible.

If we can determine a matrix T_B with property (1) and a row permutation ϕ s.t. $T_C = \phi(T_B)$ has property (2), we are clearly done, because T_A and T_D can be obtained from T_B respectively T_C by applying a permutation on the columns.

For a matrix $A \in (\mathbb{Z}_M \times \mathbb{Z}_N)^{M \times N}$, let $Q(A)$ be an $N \times N$ matrix for which $Q(A)_{i,j}$ is the number of occurences of $j \in \mathbb{Z}_N$ in the second coordinate of the points in column $i \in \mathbb{Z}_N$ of A. As $Q(T_B)$ and $Q(T_C)$ are both magic squares of weight M, one can decompose $Q(T_C)$ into a sum of M permutation matrices by the Birkhoff-von Neumann Theorem (see e.g. [2, p. 164]), and thus

$$Q(T_C) = P_0 + \cdots + P_{M-1}.$$

Let ϕ be a permutation within each row, defined by applying P_i to row $i \in \mathbb{Z}_M$. Then $Q(\phi(T_B)) = Q(T_C)$.

What is left to show is that there exists a column permutation T_B of T_A s.t. the first coordinates in each column j of T_C is correct, given the fixed permutation ϕ. To see this, consider the case where T_C requires a point (a, b) to be in column j. Clearly, (a, b) is in column b of both T_A and T_B. Now, let P_i be such that it moves *some* point in position (a', b) of T_B from column b to column j of T_C. If $(a', b) = (a, b)$, then (a, b) does not need to be moved within column b from T_A to T_B by γ, but if $(a', b) \neq (a, b)$, one can use γ to move (a, b) to (a', b) so it ends up in column j of T_C. As each point (a, b) will only be present once in T_C, it can be moved once between T_A and T_B and never moved again. This procedure holds for all points (a, b), and as such the result follows.[1] □

Lemma 10 (Equivalence under permutations within columns). *Let $\pi = (\pi_0, \ldots, \pi_{T-1})$ be a permutation sequence for an AES-like cipher E_K and let γ, γ' be arbitrary permutations on the words within the columns of a state. Then, $\forall t \in \mathbb{Z}_T : \pi \sim (\pi_0, \ldots, \gamma' \circ \pi_t \circ \gamma, \ldots, \pi_{T-1})$. In particular, the number of tightly guaranteed active S-boxes is invariant under inserting permutations, before and after any π_t, which act on the columns of the state separately.*

Proof. Fix the branch number B_θ and let $E_K \in \widetilde{\mathrm{AES}}_{M,N}(\pi, B_\theta)$. We consider any round $t \in \mathbb{Z}_T$.

We first show that $\pi \sim \pi' = (\pi_0, \ldots, \pi_t \circ \gamma, \ldots, \pi_{T-1})$. Let E'_K be like E_K but using permutation sequence π', with rounds denoted $\mathcal{R}'_t, t \in \mathbb{Z}_T$. Thus, $E'_K \in \widetilde{\mathrm{AES}}_{M,N}(\pi', B_\theta)$. It holds that

$$\mathcal{R}'_t = \texttt{Permute}_{\pi_t} \circ \texttt{Permute}_\gamma \circ \texttt{MixColumns}_t \circ \texttt{SubBytes}.$$

Since γ operates on the columns separately, one can define

$$\texttt{MixColumns}'_t = \texttt{Permute}_\gamma \circ \texttt{MixColumns}_t,$$

[1] Thanks to John Steinberger who had the idea for this proof.

which in turn is a linear layer for an AES-like cipher with the same branch number, and we have

$$\mathcal{R}'_t = \texttt{Permute}_{\pi_t} \circ \texttt{MixColumns}'_t \circ \texttt{SubBytes}.$$

Now, E'_K is a cipher which uses the permutation sequence π and thus $E'_K \in \widetilde{\text{AES}}_{M,N}(\pi, B_\theta)$. The other inclusion follows the same way by applying γ^{-1}. For showing the case of $\pi' = (\pi_0, \ldots, \gamma' \circ \pi_t, \ldots, \pi_{T-1})$, the argument is parallel. By combining the two, the result follows. □

As an easy result, one obtains Theorem 11, which we state without proof. Note that a permutation sequence is called *ρ-alternating*, written $\pi = (\pi_0, \ldots, \pi_{\rho-1})_T$, if it repeats the same ρ permutations alternatingly.

Theorem 11 (Reduction to permutations on the rows). *Let $\pi = (\pi_0, \ldots, \pi_{\rho-1})_T$ be a ρ-alternating permutation sequence. Then one can construct a $\pi' = (\pi'_0, \ldots, \pi'_{\rho-1})_T$ with $\pi \sim \pi'$, s.t. for each $t \in \mathbb{Z}_\rho$, it holds that π'_t permutes only the words in each row of the state.*

4.2 Equivalences for Rotation Matrices σ

While we have, until this point, focused on AES-like ciphers with arbitrary word-wise permutations $\texttt{Permute}_{\pi_t}$ as part of the round function, such general permutations are not suitable for designs of cryptographic primitives. To that end, we limit ourselves from this point on to AES-like ciphers where the permutation operation of the round function *cyclically rotates each row of the state from left-to-right* using a rotation matrix as specified in Definition 12.

Definition 12 (Rotation matrix). *Consider an AES-like cipher where the permutation operation in the round function consists of cyclic word-wise rotations of each state row. For such a cipher, we define a* rotation matrix *as a matrix $\sigma \in \mathbb{Z}_N^{\rho \times M}$, where ρ is a positive integer, such that*

1. *If $\rho = T$, then $\sigma_{t,i}$ denotes the rotation amount for row $i \in \mathbb{Z}_M$ in round t, and*
2. *If $\rho < T$, then we have the further requirement that the rotation constants alternate, such that $\sigma_{k,i}$ denotes the rotation amount for row $i \in \mathbb{Z}_M$ in rounds t where $t \equiv k \bmod \rho$,*

where, without loss of generality, we let the rotation direction be left-to-right.

As rotation matrices are a special case of arbitrary permutations, we remark that the notion of equivalence includes these as well. We simplify our notion of an AES-like cipher to only use row-wise rotations in the permutation part of each $\mathcal{R}_t$. In particular, we substitue the $\texttt{Permute}_{\pi_t}$ operation by

$$\begin{aligned} &\texttt{ShiftRows}_{\sigma_t} : (\mathbb{F}_2^m)^{M \times N} \to (\mathbb{F}_2^m)^{M \times N} \\ &\forall i \in \mathbb{Z}_M, \forall j \in \mathbb{Z}_N : X_{i,j} \mapsto X_{i,j+\sigma_{t \bmod \rho,i} \bmod N}. \end{aligned}$$

Lemma 13 (Equivalence under re-ordering of row entries). *Let $\sigma \in \mathbb{Z}_N^{\rho \times M}$ be a rotation matrix and let $\vartheta_0, \ldots, \vartheta_{\rho-1}$ be arbitrary, independent permutations on the ρ rows of σ. Define σ' s.t. $\forall t \in \mathbb{Z}_\rho : \sigma'_t = \vartheta_t(\sigma_t)$. Then $\sigma \sim \sigma'$.*

Proof. This directly follows from Lemma 10, as using σ'_t is equivalent to using $\gamma' \circ \sigma_t \circ \gamma$ for appropriate permutations γ' and γ on the state columns. □

Lemma 14 (Equivalence under row-wise constant addition). *Let $\sigma \in \mathbb{Z}_N^{\rho \times M}$ be a rotation matrix and let $c_0, \ldots, c_{\rho-1} \in \mathbb{Z}_N$. Define a rotation matrix σ' where $\forall t \in \mathbb{Z}_\rho, \forall i \in \mathbb{Z}_M$: $\sigma'_{t,i} = \sigma_{t,i} + c_t \bmod N$. Then $\sigma \sim \sigma'$.*

Proof. We split the proof into two cases: i) $T \leq \rho$ and ii) $T > \rho$. Consider first $T \leq \rho$. If $T < \rho$, one can add constants to $\sigma_T, \ldots, \sigma_{\rho-1}$, since these are never used anyway. Thus, let us consider $T = \rho$. We give a proof by induction that one can add independent constants $c_t, \ldots, c_{T-1}$ to $\sigma_t, \ldots, \sigma_{T-1}$ to obtain an equivalent rotation matrix σ', and proceed by induction on t. Clearly, one can add a constant to σ_{T-1} to obtain an equivalent σ', since the set $\widetilde{\mathrm{AES}}_{M,N}(\sigma, B_\theta)$ does not cover the use of σ_{T-1}. Assuming the statement holds for $t, \ldots, T-1$, we now prove that it is possible to add a constant c_{t-1} to σ_{t-1} as well. Using the notation that $\mathtt{SR} = \mathtt{ShiftRows}$, $\mathtt{MC} = \mathtt{MixColumns}$, $\mathtt{SB} = \mathtt{SubBytes}$ and $\mathtt{RS}_k$ is a rotation of the whole state by k positions, we have

$$\begin{aligned}\mathcal{R}_t \circ \mathcal{R}_{t-1} &= (\mathtt{SR}_{\sigma_t} \circ \mathtt{MC}_t \circ \mathtt{SB}) \circ (\mathtt{RS}_{-c_{t-1}} \circ \mathtt{RS}_{c_{t-1}}) \circ (\mathtt{SR}_{\sigma_{t-1}} \circ \mathtt{MC}_{t-1} \circ \mathtt{SB}) \\ &= \mathtt{SR}_{\sigma_t} \circ \mathtt{RS}_{-c_{t-1}} \circ \mathtt{RS}_{c_{t-1}} \circ \mathtt{MC}_t \circ \mathtt{RS}_{-c_{t-1}} \circ \mathtt{SB} \circ (\mathtt{RS}_{c_{t-1}} \circ \mathtt{SR}_{\sigma_{t-1}} \circ \mathtt{MC}_{t-1} \circ \mathtt{SB}),\end{aligned}$$

since $\mathtt{RS}_{-c_{t-1}}$ commutes with $\mathtt{SB}$. Now, since $\mathtt{RS}_{c_{t-1}} \circ \mathtt{MC}_t \circ \mathtt{RS}_{-c_{t-1}} =: \mathtt{MC}'_t$ defines a (just rotated) linear column mixing and since $\mathtt{SR}_{\sigma_t}$ commutes with $\mathtt{RS}_{-c_{t-1}}$, we have

$$\mathcal{R}_t \circ \mathcal{R}_{t-1} = (\mathtt{RS}_{-c_{t-1}} \circ \mathtt{SR}_{\sigma_t} \circ \mathtt{MC}'_t \circ \mathtt{SB}) \circ (\mathtt{RS}_{c_{t-1}} \circ \mathtt{SR}_{\sigma_{t-1}} \circ \mathtt{MC}_{t-1} \circ \mathtt{SB}),$$

and we see that by adding c_{t-1} to σ_{t-1} and $-c_{t-1}$ to σ_t we obtain an equivalent σ'. The result now follows by induction, since the addition of $-c_{t-1}$ to σ_t can be undone by the induction assumption.

For the case $T > \rho$, let H be a $T \times M$ matrix where $H_t = \sigma_k$ when $t \equiv k \bmod \rho$. For a T-round AES-like cipher E_K, H and σ are clearly equivalent rotation matrices. From the above, it follows we can add c_t to row t of H, $t \in \mathbb{Z}_T$, and obtain an equivalent H'. In particular, adding the same c_k to all rows t where $t \equiv k \bmod \rho$, we obtain H' which is equivalent to σ, and has the property that $H'_i = H'_j$ if $i \equiv j \bmod \rho$, and in particular the first ρ rows of H' equals σ' and the result follows. □

Theorem 15 (Equivalence for rotation matrices). *Given a rotation matrix $\sigma \in \mathbb{Z}_N^{\rho \times M}$, one can obtain an equivalent matrix $\sigma' \in \mathbb{Z}_N^{\rho \times M}$ for which the following holds simultaneously*

1. *Each row $\sigma'_t, t \in \mathbb{Z}_\rho$, is lexicographically ordered,*
2. *For all $t \in \mathbb{Z}_\rho$ it holds that $\sigma'_{t,0} = 0$ and*
3. *For all $t \in \mathbb{Z}_\rho$ it holds that $\sigma'_{t,1} \leq \frac{N}{2}$.*

Proof. Points (1) and (2) follow directly from Lemma 13 and 14, respectively. For point (3), let us assume w.l.o.g that (1) and (2) hold and consider the case where $M \geq 2$ and consider the element $\sigma_{t,1}$ from some row σ_t. If $\sigma_{t,1} > \frac{N}{2}$, we add $-\sigma_{t,1} \bmod N$ and the result follows from Lemmas 13 and 14. □

Besides Theorem 15, we heuristically suggest a search for optimal rotation matrices to restrict itself to matrices where all entries in a row are different, i.e. $\forall t \in \mathbb{Z}_\rho : \sigma_{t,j} = \sigma_{t,j'} \Leftrightarrow j = j'$, as equal entries in some σ_t are redundant w.r.t. the diffusion properties of the cipher. Moreover, when N is even, we require that σ contains at least one odd entry, because otherwise even-numbered columns never mix with odd-numbered columns. We refer to a rotation matrix which satisfies these properties, plus properties (1) – (3) of Theorem 15, as the *normal form* of its equivalence class of rotation matrices.

5 Mixed-Integer Linear Programming and Experimental Results

One advantage of modeling the S-boxes and linear layers as black boxes is that one easily can compute useful lower bounds on the number of guaranteed active S-boxes using a mixed-integer linear programming approach. We describe this approach next.

5.1 The Problem as a Mixed Integer Linear Program

In the following, we describe the mixed-integer linear program which models the problem of determining the tightly guaranteed trail weight under a given rotation matrix $\sigma \in \mathbb{Z}_N^{\rho \times M}$. We give the parameters, decision variables, the constraints and the target optimization as Model 1. This formulation is similar to that of Mouha et al. [27]. We note that Model 1 is specified for the case where each $\mathtt{M}_j^t$ used in the $\mathtt{MixColumns}_t$ operation is an MDS matrix, as this is usually what is applied in designs. If, on the other hand, non-MDS matrices are deployed, the model can be easily modified to cover these cases as well, at the cost of a slightly more complicated model. Theorem 16 formalizes how Model 1 provides us with the sought bound.

Theorem 16. *The solution of Model 1 is always a lower bound on the number of tightly guaranteed active S-boxes for an AES-like cipher with branch number B_θ and rotation matrix σ. If the branch number is optimal for the given dimensions and a linear mixing layer with this branch number exists (and the word length $m > \log_2(M+2)$), this provides a tight bound.*

Proof. This follows from Corollary 27 in Appendix A. □

Theorem 16 shows in particular that one can not hope to improve the bounds in a generic way for the case of AES-like ciphers using MDS matrices. That is to say that any argument to improve upon the bounds provided by the model will necessarily be a non-black box argument. Thus, in the spirit of the wide-trail strategy, one cannot improve upon those bounds.

Model 1: MILP model for determining the guaranteed trail weight using a fixed rotation matrix

Parameters

Name	Domain	Description
M	$\mathbb{Z}_+$	Number of rows in state
N	$\mathbb{Z}_+$	Number of columns in state
T	$\mathbb{Z}_+$	Number of rounds
ρ	$\mathbb{Z}_+$	Number of rows in rotation paramter σ
B_θ	$\mathbb{Z}_+$	Branch number of `MixColumns`
σ	$\mathbb{Z}_N^{\rho \times M}$	Rotation parameter

Decision variables

Name	Domain	Index domain	Description
$\tilde{X}_{i,j}^t$	$\mathbb{F}_2$	$i \in \mathbb{Z}_M, j \in \mathbb{Z}_N, t \in \mathbb{Z}_T \cup \{T\}$	$\tilde{X}_{i,j} = 1$ if and only if the word in position (i,j) is active before round $\mathcal{R}_t$
a_j^t	$\mathbb{F}_2$	$j \in \mathbb{Z}_N, t \in \mathbb{Z}_T$	Auxilliary variable; $a_j^t = 1$ if and only if column j has an active word before round $\mathcal{R}_t$

Minimize

$$\sum_{t \in \mathbb{Z}_T} \sum_{i \in \mathbb{Z}_M} \sum_{j \in \mathbb{Z}_N} \tilde{X}_{i,j}^t$$

subject to

$$\sum_{i \in \mathbb{Z}_M} \sum_{j \in \mathbb{Z}_N} \tilde{X}_{i,j}^0 \geq 1 \qquad (1)$$

$$\forall j \in \mathbb{Z}_N, \forall t \in \mathbb{Z}_T : \quad \sum_{i \in \mathbb{Z}_M} \tilde{X}_{i,j}^t + \tilde{X}_{i,(j+\sigma_t \mod \rho, i)}^{t+1} \mod N \geq B_\theta \cdot a_j^t \qquad (2)$$

$$\forall i \in \mathbb{Z}_M, \forall j \in \mathbb{Z}_N, \forall t \in \mathbb{Z}_T : \quad a_j^t \geq \tilde{X}_{i,j}^t \qquad (3)$$

5.2 Experimental Results

A part of our contribution is a wide range of optimal choices of rotation matrices for various state geometries $M \times N$, ρ and number of rounds T. For all our experiments, we concentrated on the case of MDS $\texttt{MixColumns}_t$ layers, i.e. AES-like ciphers with optimal branch number. Using the heuristic approach from Section 4.2, i.e. by brute-forcing the normal form of each equivalence class of rotation matrices, we provide optimal solutions for the analyzed cases as per Theorem 16. The full table of results is given in Appendix B.

We highlight in Table 1 results which suggest improvements for some existing AES-like primitives. We see that, in some cases, direct replacement of σ yields better bounds, while in other cases, one must increase ρ to obtain better bounds.

Table 1. Improvements for existing AES-like primitives. An entry $(\rho_P, \mathcal{B}_P)/(\rho_M, \mathcal{B}_M)$ gives ρ and the number of tightly guaranteed S-boxes $\mathcal{B}$ in a T-round trail for the *primitive* (subscript P) and the *modified primitive* (subscript M), respectively. The † symbol indicates results where only diffusion-optimal σ were tested, which means actual obtainable bounds may be higher.

Primitive	$T = 5$	$T = 6$	$T = 7$	$T = 8$	$T = 10$	$T = 12$
Rijndael-192	–	$(1, 42)/(1, 45)$	$(1, 46)/(1, 48)$	$(1, 50)/(1, 57)$	–	$(1, 87)/(1, 90)$
Rijndael-256	–	$(1, 50)/(2, 55)$	–	–	$(1, 85)/(2, 90)$	$(1, 105)/(2, 111)$
PRIMATEs-80	$(1, 54)/(2, 56)$	–	–	–	–	–
Prøst-128	–	$(2, 85)/(2, 90)^\dagger$	$(2, 96)/(2, 111)^\dagger$	–	–	–

Among our findings are tight bounds which are not a multiple of the branch number for an even number of rounds. This implies that there exists some MDS linear mixing layers such that the lightest valid trail contains a two-round subtrail of weight more than B_θ. Thus, some optimal trails have non-optimal transitions locally.

6 Optimal Solutions

In this section we describe, for special cases of the state geometry, optimal solutions with respect to both our main criteria, i.e. with respect to diffusion properties on one hand and resistance towards differential/linear attacks on the other hand.

6.1 Diffusion-Optimal Rotation Matrices

Under the assumptions that each S-box $S : \mathbb{F}_2^m \to \mathbb{F}_2^m$ and each $\mathtt{M}_j^t$ matrix has the property that each output bit depends on each input bit, we describe in the following a way of tracking the diffusion properties for an AES-like cipher E_K. Let z be an arbitrary fixed bit of an input to E_K. When, in the beginning of a round, a single bit in a column depends on z, then each bit in the column will depend on z after applying $\texttt{MixColumns} \circ \texttt{SubBytes}$. Thus, with fixed parameters M, N and σ, determining how many rounds t are required to obtain full diffusion reduces to answering how many rounds are required to have at least one bit depending on z in each column: if this is obtained after t' rounds then full diffusion is obtained after $t = t' + 1$ rounds. This is formalized in the following.

Definition 17 (Sumset). *Let G be an additive group and let $A, B \subset G$. We define the* sumset *written $A + B$ as $A + B = \{a + b \mid a \in A, b \in B\}$, where the sum is over G. We write kA for the sumset $A + A + \cdots + A$ with k terms.*

Theorem 18. *Consider an AES-like cipher with fixed parameters M, N, ρ and σ. Let w.l.o.g. z denote a bit in the word $X_{0,0}$ for an input X. Let $\alpha(T) = (\alpha(T)_0, \ldots, \alpha(T)_{\rho-1})$ be a vector where α_i, $0 \leq i < \rho$, equals the number of times σ_i is used in a* $\texttt{ShiftRows}$ *operation during T*

rounds of the cipher. Then, after T rounds, the indices of columns which contain bits depending on z are given by the sumset $\alpha(T)_0\sigma_0 + \alpha(T)_1\sigma_1 + \cdots + \alpha(T)_{\rho-1}\sigma_{\rho-1}$, where addition is over $\mathbb{Z}_N$.

Proof. Let $S_{-1} = \{0\}$. We recursively define $S_t = \{v + s \mid s \in S_{t-1}, v \in \sigma_{t \bmod \rho}\}$ for $t \geq 0$, where addition is in $\mathbb{Z}_N$. Note that the set S_t corresponds exactly to the sumset $\alpha(t)_0\sigma_0 + \cdots + \alpha(t)_{\rho-1}\sigma_{\rho-1}$. Clearly, $S_0 = \{v \mid v \in \sigma_0\}$ is the set of indices of columns that contain words depending on z after round $\mathcal{R}_0$. Now, assume that S_t are the column indices which contain some word depending on z after $\mathcal{R}_t$. Then, after applying $\texttt{MixColumns}_{t+1}$, *all* words in columns $j \in S_t$ depend on z. Now, when we apply $\texttt{ShiftRows}_{\sigma_{t+1 \bmod \rho}}$, the words depending on z are moved exactly to the indices given in S_{t+1}, and thus the result is obtained by induction. □

Corollary 19. *Consider an AES-like cipher with fixed parameters M, N, ρ and σ. If t' is the smallest positive integer s.t. the sumset $\alpha(t')_0\sigma_0 + \cdots + \alpha(t')_{\rho-1}\sigma_{\rho-1}$ over $\mathbb{Z}_C$ generates all of $\mathbb{Z}_N$, then the cipher obtains full diffusion after $t = t' + 1$ rounds.*

Proof. The proof follows from Theorem 18. Note that we chose the input bit z from the word $X_{0,0}$. If it would be chosen from an arbitrary word $X_{i,j}$, the corresponding sumset would be just shifted by a constant c. However, these are the same sumsets for all possible c, since they generate all of Z_N. □

Theorem 20. *When $N = M^\rho$, a diffusion-optimal rotation matrix is $\sigma \in \mathbb{Z}_N^{\rho \times M}$ s.t. $\sigma_{t,i} = i \cdot M^t$ for $(t, i) \in \mathbb{Z}_\rho \times \mathbb{Z}_M$ or any σ' where the rows of σ are permuted. These obtain full diffusion after $\rho + 1$ rounds.*

Proof. The set of indices of columns containing a word depending on z after ρ rounds is given by the sumset $\sigma_0 + \cdots + \sigma_{\rho-1}$ over $\mathbb{Z}_N$. This sumset has $M^\rho = N$ sums, and thus equals $\mathbb{Z}_N$ if and only if no two sums in the sumset are equal. To see why this is the case, consider constructing M-adic numbers using the sums in the sumset. We pick exactly one element from each row of σ and add them. As the elements in row t are $\sigma_t = \begin{pmatrix} 0M^t & 1M^t & \cdots & (M-1)M^t \end{pmatrix}$, the choice for the sum from σ_t is the t^{th} least significant digit in the M-adic representation of that number. In other words, the rows of σ form a base for the M-adic number system, and we can form any number up to $\sum_{t=0}^{\rho-1}(M-1)M^t = N - 1$ with it. Since M^ρ elements cannot be generated using less than ρ parameters in the sumset, the diffusion-optimaltiy of σ follows. □

6.2 Trail-Optimal Solutions

In this section, we first state Theorem 21, which is of particular interest because of the large number of AES-like ciphers with square geometry. Considering its statement, square states can be understood quite well. We also give a conjecture on the optimality of guaranteed trail weights for $M \times M^n$ AES-like ciphers over 2^{n+1} rounds and give a construction which matches the conjectured bound.

Theorem 21 (Optimality for square geometries). *Let σ be a rotation matrix in normal form operating on a square state of dimension $M \times M$. Then the number of tightly guaranteed active S-boxes is invariant under increasing ρ. In particular, any σ has $\sigma \sim \begin{pmatrix} 0 & 1 & \cdots & M-1 \end{pmatrix}$. Furthermore, assuming the existence of at least one MDS linear layer and the word length $m > \log_2(M+2)$, we have $\sigma \xrightarrow{M+1} k(M+1)^2$ over $4k$ rounds for all $k \in \mathbb{N}$.*

Proof. As for any $\rho > 1$, each row σ_t of a rotation matrix σ in normal form will equal $\begin{pmatrix} 0 & 1 & \cdots & M-1 \end{pmatrix}$, or any permutation hereof, this is equivalent to having $\rho = 1$ by Lemma 13. In order to prove the second statement, we first apply the Four-Round Propagation Theorem [15, Theorem 3] of the AES in a repeated manner, which provides the stated $k(M+1)^2$ as a lower bound. It is left to argue that there is a valid $4k$-round trail of weight $k(M+1)^2$

for some E_K using the specific parameters. Therefore, we first define a four-round trail X of weight $(M+1)^2$ as

$$X := \left(\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \iddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 1 \\ \vdots & \vdots & \iddots & \vdots \\ 0 & 1 & \cdots & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \iddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \right).$$

By repeating this structure k times, one can define a $4k$-round trail of weight $k(M+1)^2$. For the validity of this trail for some E_K, one can see that it is obtainable by only using the identity as the S-box and existing mixing steps, applying Corollary 27 in Appendix A. □

Theorem 21 implies that a designer who wants to improve upon the bound for a square dimension necessarily has to choose a rotation parameter σ consisting of at least one σ_t which breaks the normal form structure. Intuitively, this would not only provide a worse bound but also worse diffusion properties. However, giving an argument for the trail-optimality considering all possible rotation matrices (resp. permutations) seems to be quite difficult.

For the special case of a hypercubed geometry, we give Conjecture 22.

Conjecture 22. Given the state dimension $M \times M^n$ for an AES-like cipher, then a trail-optimal choice of the permutation sequence π over 2^{n+1} rounds yields $\pi \xrightarrow{M+1} (M+1)^{n+1}$.

The Superbox Argument. The superbox argument is a commonly used proof technique to lower bound on the number of active S-boxes in an AES-like cipher over a certain number of rounds. It has been used for the AES but also for ECHO [7] and PAEQ [10].

One uses the fact that for a clever choice of the rotation matrix, the round operations can be commuted such that some part of the encryption first works locally, in parallel, on parts of the state which we call *superboxes*. Next the superboxes are combined using state-wide operations which effectively mix the superboxes together, only to split the state into superboxes again, working with the localized operations. Such a large structure is referred to as a *megabox*, and covers four rounds of the cipher.

One can show that if a superbox has active input, there are at least B_θ active S-boxes in the first two rounds inside this superbox. Now, with the right choice of rotation matrix, the operation that combines the superboxes again imply that for the next two rounds, the total number of active superboxes is at least B_θ. From this, one obtains a four-round lower bound of B_θ^2.

This concept, which is the idea behind the Four-Round Propagation Theorem [15, Theorem 3], can be easily generalized by iteration for appropriate dimensions of state in the AES-like cipher, and with an appropriately chosen rotation matrix. We stress, however, that choosing the rotation matrix correctly for the given state dimension is of paramount importance to assuring the argument that one has e.g. B_θ active superboxes in a megabox (or equivalently for higher dimensions).

As mentioned, in Theorem 23, we give a construction which achieves the bound given in the conjecture above. Note that (especially for a cubed state dimension) this approach is not new in itself. Our main point here is that, in clear distinction to prior work such as [10, 13], we present an efficient way of implementing this idea by using cyclic rotations only. For a better visualization, Example 24 illustrates this construction for $M = 4$ and $n = 3$.

Theorem 23 (2^{n+1}-Round Propagation Theorem). *There exists a rotation matrix $\sigma \in \mathbb{Z}_{M^n}^{2^n \times M}$, such that every (non-zero) valid 2^{n+1}-round trail over all $E_K \in \widetilde{\mathrm{AES}}_{M,M^n}(\sigma, B_\theta)$ has a weight of at least B_θ^{n+1}. The rotations can be described as*

$$\begin{aligned} &\forall j \in \mathbb{Z}_n \quad : \sigma_{2^{n-j}-2} = \sigma_{2^{n-j}-1} = \begin{pmatrix} 0 & M^j & 2M^j & \cdots & (M-1)M^j \end{pmatrix} \\ &\forall j \in \mathbb{Z}_{n-1} : \forall i \in \mathbb{Z}_{2^{n-(j+1)}} \quad \sigma_i = \sigma_{2^{n-j}-3-i}. \end{aligned}$$

Proof. For $n = 1$, the statement is precisely the Four-Round Propagation Theorem of the AES. Therefore, we first prove the theorem for the eight-round case, thus for $n = 2$. We need to show that

$$\sigma := \begin{pmatrix} 0 & M & 2M & \cdots & (M-1)M \\ 0 & M & 2M & \cdots & (M-1)M \\ 0 & 1 & 2 & \cdots & M-1 \\ 0 & 1 & 2 & \cdots & M-1 \end{pmatrix} \xrightarrow{B_\theta} \mathcal{B}$$

over eight rounds for a $\mathcal{B} \geq B_\theta^3$. For the proof, we rely on a straightforward generalization of the Four-Round Propagation Theorem to the dimension one higher than the standard AES, as described previously. In particular, if one can partition the $M \times M^2$ state into M sub-states of M columns each (i.e. consider them as $M \times M$ sub-states), such that in four consecutive rounds, the `ShiftRows` operating in the first and second rounds shifts each such sub-state as if using the vector $(0\ 1\ \cdots\ M-1)$, with respect to considering that particular $M \times M$ sub-state, then the number of guaranteed active S-boxes in each such sub-state over four rounds it at least B_θ^2 (assuming a non-zero input difference). Note that the rotations of the third and fourth round have no impact on the four-round trail weight.

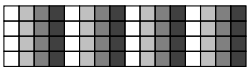

Fig. 1. Positions of the 4 independent sets of columns in a 4×16 state

Using the σ specified, the first four rounds of E_K satisfies this property when the M sub-states of size $M \times M$ are taken to be every Mth column of the state, as indicated for a 4×16 state in Figure 1. The same thing holds when considering the last four rounds separately.

Now, due to the way the row shifting of the third round combines with the column mixing and row shifting of the fourth round, i.e. $\mathtt{SR}_{\sigma_3} \circ \mathtt{MC} \circ \mathtt{SB} \circ \mathtt{SR}_{\sigma_2}$, each $M \times M$ sub-state mixes completely with each of the $M \times M$ sub-states. As such, like in the Four-Round Propagation Theorem, the sum of active $M \times M$ sub-states from the third and fourth round is at least B_θ. Combining this observation with the generalized Four-Round Propagation Theorem, the result of $B_\theta \cdot B_\theta^2$ follows.

The general case is now obtained by induction. In order to do the iteration to $2^{(n+1)+1}$ rounds, one has to apply the 2^{n+1}-round propagation. □

Example 24. Let $M = 4$, $n = 3$ and $B_\theta = 5$. Then the state has geometry 4×64. The guaranteed trail weight of 625 over 16 rounds can be realized using the rotation matrix

$$\sigma = \begin{pmatrix} 0 & 16 & 32 & 48 \\ 0 & 16 & 32 & 48 \\ 0 & 4 & 8 & 12 \\ 0 & 4 & 8 & 12 \\ 0 & 16 & 32 & 48 \\ 0 & 16 & 32 & 48 \\ 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 \end{pmatrix}.$$

We remark that especially for higher dimensions, a rotation matrix following this construction is not of much practical interest as the diffusion properties are far from optimal. One open question is whether it is possible to obtain these bounds without using a rotation matrix which allows a proof using a superbox-like argument for general M. For the special case of $M = 2$ and $N = 4$, we found that

$$\sigma = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 2 & 1 & 1 \end{pmatrix}^T,$$

which contains no superbox structure, yields $\sigma \xrightarrow{3} 27$ over eight rounds.

7 Conclusion

For AES-like ciphers, the linear mixing layer, often denoted `MixColumns`, is very well understood: one typically chooses mixing layers defined by MDS matrices to obtain optimal branch numbers. In sharp contrast to this, no systematic approach has been conducted to understand how the word-wise permutation layer in such ciphers affects the diffusion properties and resistance towards differential- and linear attacks. With this work, we close that gap.

Specifically, we consider arbitrary word-wise permutations, with special focus on rotations due to their elegant implementation characteristics. We formalized the concept of AES-like ciphers, guaranteed trail weights and equivalence of permutation parameters and, using these formalizations, proved a range of results which reduces the consideration to a special normalized form.

These results are employed in practice by connecting it with mixed-integer linear programming models for determining the guaranteed trail weights. To that end, we give a range of optimal word-wise rotations and improve on existing parameters for Rijndael-192, Rijndael-256, PRIMATEs-80 and Prøst-128.

Using superbox-like arguments we are able, as a separate result, to show for specific state geometries that a seemingly optimal bound on the trail weight can be obtained using cyclic rotations only for the permutation layer, i.e. in a very implementation friendly way. Also coming out of our analysis is the observation that square state geometries are, in some sense, ideal when it comes to solving the problem of determining the best word-wise rotations, as there is just one solution which is optimal.

References

1. Elena Andreeva, Begül Bilgin, Andrey Bogdanov, Atul Luykx, Florian Mendel, Bart Mennink, Nicky Mouha, Qingju Wang, and Kan Yasuda. PRIMATEs. CAESAR Proposal, 2014. `http://competitions.cr.yp.to/round1/primatesv1.pdf`.
2. Armen S. Asratian, Tristan M. J. Denley, and Roland Häggkvist. *Bipartite Graphs and Their Applications*. Cambridge Tracts in Mathematics. Cambridge University Press, 1998.
3. Paolo S.L.M. Barreto and Vincent Rijmen. The Whirlpool Hashing Function. NESSIE submission, 2000. `http://www.larc.usp.br/~pbarreto/WhirlpoolPage.html`.
4. Paulo S.L.M. Barreto and Vincent Rijmen. The ANUBIS Block Cipher. NESSIE submission, 2000. `http://www.larc.usp.br/~pbarreto/AnubisPage.html`.
5. Christof Beierle, Philipp Jovanovic, Martin M. Lauridsen, Gregor Leander, and Christian Rechberger. Analyzing Permutations for AES-like Ciphers: Understanding ShiftRows. In Kaisa Nyberg, editor, *Topics in Cryptology - CT-RSA 2015, The Cryptographer's Track at the RSA Conference 2015, San Francisco, CA, USA, April 20-24, 2015. Proceedings*, volume 9048 of *Lecture Notes in Computer Science*, pages 37–58. Springer, 2015.
6. Christof Beierle, Philipp Jovanovic, Martin M. Lauridsen, Gregor Leander, and Christian Rechberger. Source code for experimental results, 2015. https://github.com/mmeh/understanding-shiftrows.
7. Ryad Benadjila, Olivier Billet, Henri Gilbert, Gilles Macario-Rat, Thomas Peyrin, Matt Robshaw, and Yannick Seurin. SHA-3 Proposal: ECHO, 2010. `http://crypto.rd.francetelecom.com/ECHO/`.
8. Eli Biham and Adi Shamir. Differential Cryptanalysis of DES-like Cryptosystems. In Alfred Menezes and Scott A. Vanstone, editors, *Advances in Cryptology - CRYPTO '90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990, Proceedings*, volume 537 of *Lecture Notes in Computer Science*, pages 2–21. Springer, 1990.
9. Eli Biham and Adi Shamir. *Differential Cryptanalysis of the Data Encryption Standard*. Springer, 1993.
10. Alex Biryukov and Dmitry Khovratovich. PAEQ. CAESAR Proposal, 2014. `http://competitions.cr.yp.to/round1/paeqv1.pdf`.
11. Julia Borghoff, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Knezevic, Lars R. Knudsen, Gregor Leander, Ventzislav Nikov, Christof Paar, Christian Rechberger, Peter Rombouts, Søren S. Thomsen, and Tolga Yalçin. PRINCE - A Low-Latency Block Cipher for Pervasive Computing Applications - Extended Abstract. In Xiaoyun Wang and Kazue Sako, editors, *Advances in Cryptology - ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings*, volume 7658 of *Lecture Notes in Computer Science*, pages 208–225. Springer, 2012.

12. Joan Daemen, Lars R. Knudsen, and Vincent Rijmen. The Block Cipher Square. In Eli Biham, editor, *Fast Software Encryption, 4th International Workshop, FSE '97, Haifa, Israel, January 20-22, 1997, Proceedings*, volume 1267 of *Lecture Notes in Computer Science*, pages 149–165. Springer, 1997.
13. Joan Daemen, Lars R. Knudsen, and Vincent Rijmen. Linear Frameworks for Block Ciphers. *Designs, Codes and Cryptography*, 22(1):65–87, 2001.
14. Joan Daemen and Vincent Rijmen. AES Proposal: Rjindael, 1998. `http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf`.
15. Joan Daemen and Vincent Rijmen. The Wide Trail Design Strategy. In Bahram Honary, editor, *Cryptography and Coding, 8th IMA International Conference, Cirencester, UK, December 17-19, 2001, Proceedings*, volume 2260 of *Lecture Notes in Computer Science*, pages 222–238. Springer, 2001.
16. Ewan Fleischmann, Christian Forler, Michael Gorski, and Stefan Lucks. Twister - A Framework for Secure and Fast Hash Functions. In Feng Bao, Hui Li, and Guilin Wang, editors, *Information Security Practice and Experience, 5th International Conference, ISPEC 2009, Xi'an, China, April 13-15, 2009, Proceedings*, volume 5451 of *Lecture Notes in Computer Science*, pages 257–273. Springer, 2009.
17. Praveen Gauravaram, Lars R. Knudsen, Krystian Matusiewicz, Florian Mendel, Christian Rechberger, Martin Schläffer, and Søren S. Thomsen. Grøstl – a SHA-3 Candidate, 2011. `http://www.groestl.info/`.
18. Jian Guo, Thomas Peyrin, and Axel Poschmann. The PHOTON Family of Lightweight Hash Functions. In Phillip Rogaway, editor, *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*, volume 6841 of *Lecture Notes in Computer Science*, pages 222–239. Springer, 2011.
19. Jian Guo, Thomas Peyrin, Axel Poschmann, and Matthew J. B. Robshaw. The LED Block Cipher. In Bart Preneel and Tsuyoshi Takagi, editors, *Cryptographic Hardware and Embedded Systems - CHES 2011 - 13th International Workshop, Nara, Japan, September 28 - October 1, 2011. Proceedings*, volume 6917 of *Lecture Notes in Computer Science*, pages 326–341. Springer, 2011.
20. IBM. *ILOG CPLEX Optimizer*, 1997-2014. `http://www-01.ibm.com/software/commerce/optimization/cplex-optimizer/`.
21. Sebastiaan Indesteege, Elena Andreeva, Christophe De Cannière, Orr Dunkelman, Emilia Käsper, Svetla Nikova, Bart Preneel, and Elmar Tischhauser. The LANE hash function. Submission to NIST, 2008. `http://www.cosic.esat.kuleuven.be/publications/article-1181.pdf`.
22. Jorge Nakahara Jr. 3D: A Three-Dimensional Block Cipher. In Matthew K. Franklin, Lucas Chi Kwong Hui, and Duncan S. Wong, editors, *Cryptology and Network Security, 7th International Conference, CANS 2008, Hong-Kong, China, December 2-4, 2008. Proceedings*, volume 5339 of *Lecture Notes in Computer Science*, pages 252–267. Springer, 2008.
23. Elif Bilge Kavun, Martin M. Lauridsen, Gregor Leander, Christian Rechberger, Peter Schwabe, and Tolga Yalçın. Prøst. CAESAR Proposal, 2014. `http://proest.compute.dtu.dk`.
24. Chae Hoon Lim and Tymur Korkishko. mCrypton - A Lightweight Block Cipher for Security of Low-Cost RFID Tags and Sensors. In JooSeok Song, Taekyoung Kwon, and Moti Yung, editors, *Information Security Applications, 6th International Workshop, WISA 2005, Jeju Island, Korea, August 22-24, 2005, Revised Selected Papers*, volume 3786 of *Lecture Notes in Computer Science*, pages 243–258. Springer, 2005.
25. Florence J. MacWilliams and Neil J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland Publishing Company, 2nd edition, 1978.
26. Mitsuru Matsui. Linear Cryptoanalysis Method for DES Cipher. In Tor Helleseth, editor, *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*, volume 765 of *Lecture Notes in Computer Science*, pages 386–397. Springer, 1993.
27. Nicky Mouha, Qingju Wang, Dawu Gu, and Bart Preneel. Differential and Linear Cryptanalysis Using Mixed-Integer Linear Programming. In Chuankun Wu, Moti Yung, and Dongdai Lin, editors, *Information Security and Cryptology - 7th International Conference, Inscrypt 2011, Beijing, China, November 30 - December 3, 2011. Revised Selected Papers*, volume 7537 of *Lecture Notes in Computer Science*, pages 57–76. Springer, 2011.
28. Markku-Juhani O. Saarinen. STRIBOBr1. CAESAR Proposal, 2014. `http://competitions.cr.yp.to/round1/stribobr1.pdf`.
29. Claude Shannon. Communication Theory of Secrecy Systems. *Bell System Technical Journal, Vol 28, pp. 656–715*, 1949.
30. Dominic J. A. Welsh. *Codes and cryptography*. Clarendon Press, 1988.

A Optimality of the Black-Box Model

One has to make sure that the definition of the tightly guaranteed active S-boxes is independent of the concrete S-box functions within the AES-like ciphers. This is shown in Lemma 25.

Lemma 25. *Let* $\theta : (\mathbb{F}_2^m)^M \to (\mathbb{F}_2^m)^M$ *be a linear automorphism with branch number* B_θ. *Let* $v = (v_1, \ldots, v_M) \in (\mathbb{F}_2^m)^M \setminus \{0\}$ *such that* $\theta(v) = w = (w_1, \ldots, w_M)$. *Then for all*

$a_1, \ldots, a_{2M} \in \mathbb{F}_2^m \setminus \{0\}$, *one can construct a linear automorphism* θ' *with branch number* B_θ *such that* $\theta'(a_1 v_1, \ldots, a_M v_M) = (a_{M+1} w_1, \ldots, a_{2M} w_M)$.

Proof. Let $G = [I \mid A]$ be the generator matrix in standard form of the linear $[2M, M, B_\theta]_m$-code C corresponding to θ. Now one can construct an equivalent code C' with the same minimal distance by multiplying every column of G by non-zero scalars $a_1, \ldots, a_{2M}$ [30, p. 54-55]. In order to obtain a generator matrix $G' = [I \mid A']$ of C' in standard form, one scales the rows by the non-zero values $a_1^{-1}, \ldots, a_M^{-1}$. This does not change the generated code and defines the new mixing $\theta'(x) = A'x$.

$$\begin{array}{c} \\ a_1^{-1} \\ \vdots \\ a_M^{-1} \end{array} \begin{array}{c} \begin{array}{cccccc} a_1 & \ldots & a_M & a_{M+1} & \ldots & a_{2M} \end{array} \\ \begin{pmatrix} 1 & & & & & \\ & \ddots & & & A' & \\ & & 1 & & & \end{pmatrix} \end{array}$$

If the matrix A was invertible, then A' is invertible as well since A' is obtained from A by scaling the rows and the columns. □

In order to prove Theorem 16, one will make use of the following two results.

Lemma 26. *Let* $\log_2(M+2) < m$ *and let* C *be a linear* $[2M, M]_m$*-code which is MDS. For every subset* $S \subseteq \{1, \ldots, 2M\}$ *with* $M+1 \leq |S| \leq 2M$*, there exists a vector* $v = (v_1, \ldots, v_{2M}) \in C$ *such that* $v_i \neq 0$ *if and only if* $i \in S$.

Proof. Define two subsets $S_1, S_2 \subseteq S$ such that $|S_1| = |S_2| = M+1$ and $S_1 \cup S_2 = S$. This is possible since $|S| \geq M+1$. From [25, p. 319, Theorem 4] it follows that there exists two vectors $v^{(1)} = (v_1^{(1)}, \ldots, v_{2M}^{(1)})$ and $v^{(2)} = (v_1^{(2)}, \ldots, v_{2M}^{(2)})$ in C such that $v_i^{(j)} \neq 0$ if and only if $i \in S_j$. Now, one can construct v as a linear combination $v := v^{(1)} + cv^{(2)}$ with $c \in \mathbb{F}_2^m$ as follows. Choose $c \neq 0$ such that for all non-zero components $v_i^{(1)}$ in $v^{(1)}$ the identity

$$c \cdot v_i^{(2)} \neq -v_i^{(1)}$$

holds. This is possible because of the field property of $\mathbb{F}_2^m$ and since $2^m > M+2$. □

Thus, given a concrete MDS transformation (which has a sufficiently large dimension), every activity pattern which fulfils the branch number property can be be realized. By applying Lemma 25, one obtains as a corollary:

Corollary 27. *Let* $\log_2(M+2) < m$ *and let* A *be an existing MDS matrix,* $A \in (\mathbb{F}_2^m)^{M \times M}$. *Then for all* $v, w \in (\mathbb{F}_2^m)^M$ *with* $\text{weight}(v) + \text{weight}(w) \geq M+1$*, there exists an MDS matrix* $A' \in (\mathbb{F}_2^m)^{M \times M}$ *such that* $w = A'v$.

B Search Results

Table 2 provides the results from our search for optimal rotation matrices. For $\rho \in \{1, 2, 3\}$ and a wide range of dimensions $M \times N$, number of rounds T and *some* trail-optimal choice of σ, we give the number of active S-boxes it tightly guarantees, denoted $\mathcal{B}$. Note that for $\rho = 2$ with the 4×16 and 4×32 geometries, entries marked with † are results restricted to diffusion-optimal σ due to the complexity of the model. As such, the optimal bound w.r.t. trail weights may be even higher.

Table 2. Results for $M = 2, 3, 4, 5$

			$\rho=1$		$\rho=2$		$\rho=3$				$\rho=1$		$\rho=2$		$\rho=3$	
T	M	N	$\mathcal{B}$	σ	$\mathcal{B}$	σ	$\mathcal{B}$	σ	M	N	$\mathcal{B}$	σ	$\mathcal{B}$	σ	$\mathcal{B}$	σ
2	2	2	3	(0, 1)	3	(0, 1), (0, 1)	3	(0, 1), (0, 1), (0, 1)	4	4	5	(0, 1, 2, 3)	5	(0, 1, 2, 3), (0, 1, 2, 3)	5	(0, 1, 2, 3), (0, 1, 2, 3), (0, 1, 2, 3)
3			5	(0, 1)	5	(0, 1), (0, 1)	5	(0, 1), (0, 1), (0, 1)			9	(0, 1, 2, 3)	9	(0, 1, 2, 3), (0, 1, 2, 3)	9	(0, 1, 2, 3), (0, 1, 2, 3), (0, 1, 2, 3)
4			9	(0, 1)	9	(0, 1), (0, 1)	9	(0, 1), (0, 1), (0, 1)			25	(0, 1, 2, 3)	25	(0, 1, 2, 3), (0, 1, 2, 3)	25	(0, 1, 2, 3), (0, 1, 2, 3), (0, 1, 2, 3)
5			10	(0, 1)	10	(0, 1), (0, 1)	10	(0, 1), (0, 1), (0, 1)			26	(0, 1, 2, 3)	26	(0, 1, 2, 3), (0, 1, 2, 3)	26	(0, 1, 2, 3), (0, 1, 2, 3), (0, 1, 2, 3)
6			12	(0, 1)	12	(0, 1), (0, 1)	12	(0, 1), (0, 1), (0, 1)			30	(0, 1, 2, 3)	30	(0, 1, 2, 3), (0, 1, 2, 3)	30	(0, 1, 2, 3), (0, 1, 2, 3), (0, 1, 2, 3)
7			14	(0, 1)	14	(0, 1), (0, 1)	14	(0, 1), (0, 1), (0, 1)			34	(0, 1, 2, 3)	34	(0, 1, 2, 3), (0, 1, 2, 3)	34	(0, 1, 2, 3), (0, 1, 2, 3), (0, 1, 2, 3)
8			18	(0, 1)	18	(0, 1), (0, 1)	18	(0, 1), (0, 1), (0, 1)			50	(0, 1, 2, 3)	50	(0, 1, 2, 3), (0, 1, 2, 3)	50	(0, 1, 2, 3), (0, 1, 2, 3), (0, 1, 2, 3)
10			21	(0, 1)	21	(0, 1), (0, 1)	21	(0, 1), (0, 1), (0, 1)			55	(0, 1, 2, 3)	55	(0, 1, 2, 3), (0, 1, 2, 3)	55	(0, 1, 2, 3), (0, 1, 2, 3), (0, 1, 2, 3)
12			27	(0, 1)	27	(0, 1), (0, 1)	27	(0, 1), (0, 1), (0, 1)			75	(0, 1, 2, 3)	75	(0, 1, 2, 3), (0, 1, 2, 3)	75	(0, 1, 2, 3), (0, 1, 2, 3), (0, 1, 2, 3)
2	2	4	3	(0, 1)	3	(0, 1), (0, 1)	3	(0, 1), (0, 1), (0, 1)	4	6	5	(0, 1, 2, 3)	5	(0, 1, 2, 3), (0, 1, 2, 3)	5	(0, 1, 2, 3), (0, 1, 2, 3), (0, 1, 2, 3)
3			5	(0, 1)	5	(0, 1), (0, 1)	5	(0, 1), (0, 1), (0, 1)			9	(0, 1, 2, 3)	9	(0, 1, 2, 3), (0, 1, 2, 3)	9	(0, 1, 2, 3), (0, 1, 2, 3), (0, 1, 2, 3)
4			9	(0, 1)	9	(0, 1), (0, 1)	9	(0, 1), (0, 1), (0, 1)			25	(0, 1, 2, 3)	25	(0, 1, 2, 3), (0, 1, 2, 3)	25	(0, 1, 2, 3), (0, 1, 2, 3), (0, 1, 2, 3)
5			13	(0, 1)	13	(0, 1), (0, 1)	13	(0, 1), (0, 1), (0, 1)			34	(0, 1, 2, 3)	36	(0, 1, 2, 4), (0, 1, 2, 3)	37	(0, 1, 2, 3), (0, 1, 2, 4), (0, 1, 3, 4)
6			18	(0, 1)	18	(0, 1), (0, 1)	18	(0, 1), (0, 1), (0, 1)			45	(0, 1, 3, 4)	45	(0, 1, 3, 4), (0, 1, 3, 4)	45	(0, 1, 3, 4), (0, 1, 3, 4), (0, 1, 3, 4)
7			21	(0, 1)	22	(0, 1), (0, 2)	21	(0, 1), (0, 1), (0, 1)			48	(0, 1, 3, 4)	48	(0, 1, 3, 4), (0, 1, 3, 4)	48	(0, 1, 2, 3), (0, 1, 2, 3), (0, 1, 3, 4)
8			24	(0, 1)	24	(0, 1), (0, 1)	24	(0, 1), (0, 1), (0, 1)			57	(0, 1, 3, 4)	57	(0, 1, 3, 4), (0, 1, 3, 4)	57	(0, 1, 3, 4), (0, 1, 3, 4), (0, 1, 3, 4)
10			30	(0, 1)	30	(0, 1), (0, 1)	30	(0, 1), (0, 1), (0, 1)			72	(0, 1, 2, 3)	73	(0, 1, 2, 3), (0, 1, 2, 4)	74	(0, 1, 2, 3), (0, 1, 2, 3), (0, 1, 3, 4)
12			36	(0, 1)	36	(0, 1), (0, 1)	36	(0, 1), (0, 1), (0, 1)			90	(0, 1, 3, 4)	90	(0, 1, 3, 4), (0, 1, 3, 4)	90	(0, 1, 3, 4), (0, 1, 3, 4), (0, 1, 3, 4)
2	2	6	3	(0, 1)	3	(0, 1), (0, 1)	3	(0, 1), (0, 1), (0, 1)	4	8	5	(0, 1, 2, 3)	5	(0, 1, 2, 3), (0, 1, 2, 3)	5	(0, 1, 2, 3), (0, 1, 2, 3), (0, 1, 2, 3)
3			5	(0, 1)	5	(0, 1), (0, 1)	5	(0, 1), (0, 1), (0, 1)			9	(0, 1, 2, 3)	9	(0, 1, 2, 3), (0, 1, 2, 3)	9	(0, 1, 2, 3), (0, 1, 2, 3), (0, 1, 2, 3)
4			9	(0, 1)	9	(0, 1), (0, 1)	9	(0, 1), (0, 1), (0, 1)			25	(0, 1, 2, 3)	25	(0, 1, 2, 3), (0, 1, 2, 3)	25	(0, 1, 2, 3), (0, 1, 2, 3), (0, 1, 2, 3)
5			13	(0, 1)	13	(0, 1), (0, 1)	13	(0, 1), (0, 1), (0, 1)			41	(0, 1, 2, 4)	41	(0, 1, 2, 3), (0, 1, 3, 4)		
6			18	(0, 1)	21	(0, 1), (0, 2)	21	(0, 1), (0, 2), (0, 2)			50	(0, 1, 2, 4)	55	(0, 1, 2, 3), (0, 1, 3, 5)		
7			21	(0, 1)	29	(0, 2), (0, 1)	28	(0, 1), (0, 2), (0, 2)			58	(0, 1, 3, 4)	58	(0, 1, 2, 3), (0, 2, 3, 5)		
8			24	(0, 1)	33	(0, 1), (0, 2)	33	(0, 1), (0, 2), (0, 1)			65	(0, 1, 2, 4)	65	(0, 1, 2, 3), (0, 1, 3, 4)		
10			30	(0, 1)	39	(0, 1), (0, 2)	42	(0, 1), (0, 1), (0, 2)			85	(0, 1, 2, 4)	90	(0, 1, 2, 3), (0, 2, 3, 5)		
12			36	(0, 1)	45	(0, 1), (0, 2)	48	(0, 1), (0, 1), (0, 3)			105	(0, 1, 2, 4)	111	(0, 1, 2, 3), (0, 2, 3, 5)		
14											120	(0, 1, 2, 4)				
2	2	8	3	(0, 1)	3	(0, 1), (0, 1)	3	(0, 1), (0, 1), (0, 1)	4	10	5	(0, 1, 2, 3)	5	(0, 1, 2, 3), (0, 1, 2, 3)		
3			5	(0, 1)	5	(0, 1), (0, 1)	5	(0, 1), (0, 1), (0, 1)			9	(0, 1, 2, 3)	9	(0, 1, 2, 3), (0, 1, 2, 3)		
4			9	(0, 1)	9	(0, 1), (0, 1)	9	(0, 1), (0, 1), (0, 1)			25	(0, 1, 2, 3)	25	(0, 1, 2, 3), (0, 1, 2, 3)		
5			13	(0, 1)	13	(0, 1), (0, 1)	13	(0, 1), (0, 1), (0, 1)			41	(0, 1, 2, 4)	41	(0, 1, 2, 3), (0, 1, 3, 4)		
6			18	(0, 1)	21	(0, 1), (0, 2)	21	(0, 1), (0, 2), (0, 2)			60	(0, 1, 2, 4)	65	(0, 1, 2, 3), (0, 1, 4, 7)		
7			21	(0, 1)	29	(0, 1), (0, 3)	29	(0, 1), (0, 2), (0, 3)			70	(0, 1, 3, 4)	72	(0, 1, 2, 3), (0, 1, 4, 7)		
8			24	(0, 1)	39	(0, 1), (0, 3)	42	(0, 1), (0, 2), (0, 3)			80	(0, 1, 3, 4)	82	(0, 1, 5, 6), (0, 2, 5, 7)		
10			30	(0, 1)	51	(0, 1), (0, 3)	54	(0, 1), (0, 3), (0, 2)								
12			36	(0, 1)	56	(0, 1), (0, 3)	60	(0, 1), (0, 2), (0, 3)								
2	3	3	4	(0, 1, 2)	4	(0, 1, 2), (0, 1, 2)	4	(0, 1, 2), (0, 1, 2), (0, 1, 2)	4	12	5	(0, 1, 2, 3)	5	(0, 1, 2, 3), (0, 1, 2, 3)		
3			7	(0, 1, 2)	7	(0, 1, 2), (0, 1, 2)	7	(0, 1, 2), (0, 1, 2), (0, 1, 2)			9	(0, 1, 2, 4)	9	(0, 1, 2, 3), (0, 1, 2, 4)		
4			16	(0, 1, 2)	16	(0, 1, 2), (0, 1, 2)	16	(0, 1, 2), (0, 1, 2), (0, 1, 2)			25	(0, 1, 2, 3)				
5			17	(0, 1, 2)	17	(0, 1, 2), (0, 1, 2)	17	(0, 1, 2), (0, 1, 2), (0, 1, 2)			41	(0, 1, 3, 4)				
6			20	(0, 1, 2)	20	(0, 1, 2), (0, 1, 2)	20	(0, 1, 2), (0, 1, 2), (0, 1, 2)			65	(0, 1, 4, 5)				
7			23	(0, 1, 2)	23	(0, 1, 2), (0, 1, 2)	23	(0, 1, 2), (0, 1, 2), (0, 1, 2)			76	(0, 1, 4, 5)				
8			32	(0, 1, 2)	32	(0, 1, 2), (0, 1, 2)	32	(0, 1, 2), (0, 1, 2), (0, 1, 2)			92	(0, 1, 4, 5)				
10			36	(0, 1, 2)	36	(0, 1, 2), (0, 1, 2)	36	(0, 1, 2), (0, 1, 2), (0, 1, 2)								
12			48	(0, 1, 2)	48	(0, 1, 2), (0, 1, 2)	48	(0, 1, 2), (0, 1, 2), (0, 1, 2)								
2	3	6	4	(0, 1, 2)	4	(0, 1, 2), (0, 1, 2)	4	(0, 1, 2), (0, 1, 2), (0, 1, 2)	4	16	5	(0, 1, 2, 3)	5	(0, 1, 2, 3), (0, 1, 2, 3)		
3			7	(0, 1, 2)	7	(0, 1, 2), (0, 1, 2)	7	(0, 1, 2), (0, 1, 2), (0, 1, 2)			9	(0, 1, 2, 3)	9	(0, 1, 2, 3), (0, 1, 2, 3)		
4			16	(0, 1, 2)	16	(0, 1, 2), (0, 1, 2)	16	(0, 1, 2), (0, 1, 2), (0, 1, 2)			25	(0, 1, 2, 3)	$25^\dagger$	(0, 1, 2, 3), (0, 1, 2, 3)		
5			20	(0, 1, 2)	25	(0, 1, 2), (0, 1, 3)	25	(0, 1, 2), (0, 1, 3), (0, 1, 2)			41	(0, 1, 2, 4)				
6			24	(0, 1, 2)	36	(0, 1, 2), (0, 1, 3)	36	(0, 1, 3), (0, 1, 2), (0, 2, 3)			75	(0, 1, 4, 6)	$90^\dagger$	(0, 4, 10, 14), (0, 2, 11, 13)		
7			28	(0, 1, 2)	38	(0, 1, 2), (0, 1, 3)	40	(0, 1, 3), (0, 2, 3), (0, 1, 2)			100	(0, 1, 4, 6)	$111^\dagger$	(0, 1, 2, 3), (0, 3, 7, 11)		
8			32	(0, 1, 2)	41	(0, 1, 2), (0, 1, 3)	44	(0, 1, 2), (0, 1, 3), (0, 2, 3)			120	(0, 1, 4, 5)				
10			40	(0, 1, 2)	56	(0, 1, 2), (0, 1, 3)	56	(0, 1, 2), (0, 1, 3), (0, 2, 3)								
12			48	(0, 1, 2)	72	(0, 1, 2), (0, 1, 3)	72	(0, 1, 2), (0, 1, 3), (0, 2, 3)								
2	3	9	4	(0, 1, 2)	4	(0, 1, 2), (0, 1, 2)	4	(0, 1, 2), (0, 1, 2), (0, 1, 2)	4	32	5	(0, 1, 2, 3)	$5^\dagger$	(0, 1, 2, 3), (0, 1, 2, 3)		
3			7	(0, 1, 2)	7	(0, 1, 2), (0, 1, 2)	7	(0, 1, 2), (0, 1, 2), (0, 1, 2)			9	(0, 1, 2, 3)	$9^\dagger$	(0, 1, 2, 3), (0, 1, 2, 3)		
4			16	(0, 1, 2)	16	(0, 1, 2), (0, 1, 2)	16	(0, 1, 2), (0, 1, 2), (0, 1, 2)			25	(0, 1, 2, 3)	$25^\dagger$	(0, 1, 2, 3), (0, 1, 2, 3)		
5			25	(0, 1, 3)	25	(0, 1, 2), (0, 1, 3)	25	(0, 4, 8), (0, 4, 8), (0, 2, 8)			41	(0, 1, 2, 4)				
6			36	(0, 1, 3)	44	(0, 1, 2), (0, 2, 5)	44	(0, 1, 2), (0, 2, 4), (0, 3, 6)			75	(0, 1, 4, 6)				
7			42	(0, 1, 3)	53	(0, 1, 2), (0, 2, 5)	55	(0, 1, 2), (0, 2, 4), (0, 3, 6)								
8			48	(0, 1, 3)	60	(0, 1, 2), (0, 1, 4)	60	(0, 1, 2), (0, 1, 2), (0, 2, 5)								
10			60	(0, 1, 3)	69	(0, 1, 2), (0, 1, 4)										
12			72	(0, 1, 3)	92	(0, 1, 2), (0, 2, 5)	93	(0, 1, 2), (0, 2, 4), (0, 3, 6)								
2									5	8	6	(0, 1, 2, 3, 4)	6	(0, 1, 2, 3, 4), (0, 1, 2, 3, 4)		
3											11	(0, 1, 2, 3, 4)	11	(0, 1, 2, 3, 4), (0, 1, 2, 3, 4)		
4											36	(0, 1, 2, 3, 4)	36	(0, 1, 2, 3, 4), (0, 1, 2, 3, 4)		
5											54	(0, 1, 2, 3, 5)	56	(0, 1, 2, 3, 4), (0, 1, 3, 5, 6)		
6											62	(0, 1, 2, 3, 5)	62	(0, 1, 2, 3, 4), (0, 1, 2, 3, 5)		
7											67	(0, 1, 2, 3, 5)	67	(0, 1, 2, 3, 4), (0, 1, 2, 3, 5)		
8											72	(0, 1, 2, 3, 4)	72	(0, 1, 2, 3, 4), (0, 1, 2, 3, 4)		
9													95	(0, 1, 2, 3, 4), (0, 1, 2, 3, 5)		