Lightweight Multiplication in $GF(2^n)$ with Applications to MDS Matrices

Christof Beierle(✉), Thorsten Kranz, and Gregor Leander

Horst Görtz Institute for IT Security, Ruhr-Universität Bochum, Bochum, Germany
{christof.beierle,thorsten.kranz,gregor.leander}@rub.de

Abstract. In this paper we consider the fundamental question of optimizing finite field multiplications with one fixed element. Surprisingly, this question did not receive much attention previously. We investigate which field representation, that is which choice of basis, allows for an optimal implementation. Here, the efficiency of the multiplication is measured in terms of the number of XOR operations needed to implement the multiplication. While our results are potentially of larger interest, we focus on a particular application in the second part of our paper. Here we construct new MDS matrices which outperform or are on par with all previous results when focusing on a round-based hardware implementation.

Keywords: Finite fields · Multiplication · XOR-count · Lightweight cryptography · MDS matrices · Block cipher

1 Introduction

Many cryptographic schemes build on finite fields as their underlying mathematic structure. In almost all cases, the schemes can be designed without having to specify a concrete representation of the finite field in advance. However, when finally being implemented in practice, one necessarily has to choose a particular representation of the finite field, basically as bit strings. In general, this choice does not influence the security of the scheme, but might well influence the performance of the resulting implementation. In this work we focus on this choice of field representations and derive theoretical results on how to choose an optimal field representation with respect to multiplication with fixed field elements. Before going into details, we elaborate on this setup in the special case of symmetric cryptography.

Symmetric Cryptographic Primitives. Build the back-bone of virtually any secure communication today. Block ciphers and hash functions can be seen as the workhorses in cryptography, used for encrypting and authenticating the largest part of the workload.

Today, we are in the comfortable situation of having at hand a choice of strong block ciphers and hash functions that seem secure against even the strongest

M. Robshaw and J. Katz (Eds.): CRYPTO 2016, Part I, LNCS 9814, pp. 625–653, 2016.
DOI: 10.1007/978-3-662-53018-4_23

adversaries with practically unlimited computational resources. Moreover, those primitives are based on rather well-understood design principles that allow to construct efficient, simple and easy to analyze ciphers. Especially in the case of substitution-permutation (SP) networks, following the seminal ideas of AES [9] and its predecessor SQUARE [8], arguing the security of ciphers against the two most powerful generic attacks, that is differential- and linear attacks [6,23], became significantly easier. In an SP-network the cipher (or the cryptographic permutation) consists of a number of almost identical rounds, each of which consists of a layer of S-boxes and an $\mathbb{F}_2$-linear layer to mix those parts.

One of the most important design strategies for those primitives is the so-called wide-trail strategy, initiated in [7], that aims at lower bounding the number of active S-boxes. Here, for a given linear or differential trail, an S-box is called active if its input-mask (resp. input-difference) is non-zero. The main observations of the wide-trail strategy is that it is actually the linear layer that is to a large extent responsible for the security of the primitive against linear and differential attacks. Moreover, the wide-trail strategy allows a natural decoupling of the design choice for a linear layer and an S-box.

Interestingly, for the linear layer not many general constructions are known. Two basic approaches can be identified. On the one hand, an ad-hoc approach, where lower bounding the number of active S-boxes requires computer-aided tools that search (sometimes heuristically) for optimal trails. This approach is used e.g. for Serpent [5] or Keccak [4]. On the other hand, a code-based approach, where the linear layers are chosen in such a way that they correspond to good (often locally optimal) linear codes. This is, most prominently, the case for AES where a Maximum Distance Separable (MDS) code is implemented via the MixColumns operation.

Even in the theoretically better circumstantiated code-based approach many fundamental questions are left open. Here, when using an MDS matrix for (parts of) the linear layer, the main challenge is to choose an MDS matrix that is most suitable for an efficient implementation. As those MDS matrices are usually defined over a finite field with characteristic two, i.e. $\mathbb{F}_{2^n}$, one important and so far almost unstudied question is the choice of an $\mathbb{F}_2$-basis of $\mathbb{F}_{2^n}$ and its impact on the implementation efficiency.

From a design point of view, one has to choose a linear layer given as a mapping on $\mathbb{F}_{2^n}^b$ and an $\mathbb{F}_2$-basis of $\mathbb{F}_{2^n}$ to concretely specify the primitive. This is actually a very natural separation of the design of the cipher and its specification (and thus implementation) on bit level. As nicely explained in [10] by introducing RIJNDAEL-GF this separation is probably most obvious for AES itself, but in principle possible for any cipher. Following [10], the choice of basis is to a large extent independent of the design and the security of the cipher. However, the choice of basis might have a significant impact on the efficiency of the cipher on certain platforms.

For software implementations, depending on the details, the choice of basis is either irrelevant (in e.g. a table-based implementation) or hard to capture (in e.g. a bit-sliced implementation) as the efficiency might depend on the exact

instructions offered by a given platform. For hardware implementations, one has to distinguish between a serial implementation or a round-based implementation. As the round-based implementation seems most relevant in practice (cf. [27]), we mainly focus on this use-case here. Surprisingly, compared to a serial hardware implementation, the case of a round-based hardware implementation has attracted less attention so far.

For a round-based hardware implementation, the impact of the choice of basis already becomes apparent when focusing on how to implement the multiplication with one given element α in $\mathbb{F}_{2^n}$. For different choices of bases, the efficiency of implementations of the resulting $\mathbb{F}_2$-linear mappings differs significantly. Thus, the very fundamental task we study in the first part of the paper is:

For a given element $\alpha \in \mathbb{F}_{2^n}$ find a basis such that multiplication by α can be implemented most efficiently.[1]

It is worth pointing out that the related question of how to efficiently multiply *two* arbitrary field elements has been studied extensively in the past.

While the above question is of independent interest, with potentially very different applications, we use our results for designing efficient linear layers. Thus, in the second part, we will give several constructions of MDS matrices. Echoing the above, the construction of our MDS matrices are independent of the choice of the basis – actually to a large extent independent of the field size as well.

The combination of the first part, i.e. how to choose a basis that allows for an optimal implementation, and the second part, i.e. the construction of MDS matrices, finally results in implementations of MDS matrices that are more efficient for a large variety of parameters than the best matrices discussed so far in literature.

Thus, this application serves as a nice example were an improved understanding on how to choose the field representation immediately leads to improved results. This is even more interesting as the construction of efficient MDS matrices has been an active field of research recently.

1.1 Related Work

In particular the construction of efficient serial MDS matrices is a well-studied subject. Considering serial implementations of MDS matrices is based on the initial idea of Guo, Peyrin, and Poschmann used in the design of PHOTON [13] and later in the block cipher LED [14]. In a nutshell the idea is not to implement an MDS matrix directly, but rather implement a matrix A such that A^k is MDS for some small k. When considering a hardware implementation, it reduces the chip area if implementing A is significantly cheaper than A^k. The circuit implementing A is then iterated k times, which does not increase its size significantly. This basic idea has been further generalized and improved in a series of subsequent papers. In [24,30] the authors focus on even more efficient

[1] Note that the choice of basis is of course not restricted to choosing different irreducible polynomials to represent the finite field.

choices for A by considering additive, i.e. $\mathbb{F}_2$-linear MDS codes. Their approach uses symbolic computations in order to derive general conditions on how to choose the matrix entries independent of the dimension.

In [31] Xu et al. furthermore took into account the cost of implementing the inverse matrix. At FSE 2014, in [2] Augot and Finiasz improved significantly upon the efficiency of the search algorithm of [24], allowing them to search for MDS matrices of much larger dimension than previously possible.

For a round-based implementation, less work has been done so far. The authors of [27] focus on MDS matrices that have an efficient implementation (in terms of the XOR-count) and put special emphasis on involutory MDS matrices, i.e. MDS matrices that are their own inverse. They derive several constructions and rather efficient search methods for MDS matrices meeting their goals. Very recently, Liu and Sim [21] improved upon some of those results by characterizing equivalences in circulant (and circulant-like) MDS matrices and thus further reduced the search space. In both works, in order to improve the efficiency for a given MDS matrix defined over a finite field, the authors considered different representations of the underlying finite fields by running through all possible irreducible polynomials of the given degree. However, in view of the question of how to choose an optimal basis, this corresponds to investigating only a small subset of all possible bases. Work on investigating the XOR-count distribution for other than the polynomial bases has been done very recently in [25].

Also recently, Li and Wang constructed circulant involutory $\mathbb{F}_2$-linear MDS matrices [19]. While it was already known that circulant MDS matrices over a finite field cannot be involutory [15], they have shown their existence in the additive case. Independently, the authors of [21] have shown the existence of left-circulant involutory MDS matrices over finite fields.

1.2 Our Contribution

After fixing our notation and recalling basic facts in Sect. 2, in the first part of the paper we focus on the question on how to find an optimal implementation of the multiplication by a given field element α (cf. Sect. 3). Here efficiency is measured in terms of the number of XOR operations needed to implement the corresponding binary matrix. Note that this metric differs from the XOR-count used in [27]. In [27] the XOR-count of an $n \times n$ matrix M was defined as the number of ones in M minus n. However, the number of (additional) ones in a matrix does not necessarily correspond to the number of XOR operations needed for implementation. Thus, while the number of ones in M is certainly an easier to handle metric, in our opinion it is more appropriate to consider the actual number of XOR operations as the efficiency metric. Note that this improved notion was also discussed in [16]. For technical reasons, we focus on the number of XOR operations without temporary registers, i.e. in-place XOR operations. One of our main results in this first part of the paper is, that for a non-trivial element α one can find a basis such that the resulting matrix can be implemented with one XOR operation if and only if the characteristic polynomial of α is an irreducible trinomial. Note that an XOR-count equal to one in our notion

coincides with the definition of the XOR-count in [27]. The interesting part here is that the condition on the characteristic polynomial is not only sufficient but also necessary. As an immediate consequence, one cannot hope to implement the multiplication by any element $\alpha \neq 1$ in $\mathbb{F}_{2^8}^*$ with one XOR only. This follows by the above and the well-known fact that there are no irreducible trinomials of degree 8 [28].

We furthermore show that, for any given basis, there are at most two (non-trivial) elements α and β such that the multiplication with those elements can be implemented with one XOR operation. In fact, β is necessarily the multiplicative inverse of α.

While the weight of the (irreducible) characteristic polynomial of an element α clearly gives an upper bound of the number of XOR operations needed to implement the corresponding multiplication, we show that this bound is in general not tight in the case were the characteristic polynomial is of weight larger than three.

In particular, for all elements $\alpha \in \mathbb{F}_{2^n}^*$ with $n \leq 8$ we present an optimal representation such that the multiplication with α can be implemented with a minimal number of XOR operations. For all those elements α, that are not contained in a proper subfield of $\mathbb{F}_{2^n}$, the multiplication can be implemented with at most 3 XOR operations (and often with two only). Those results are given in Tables 3, 4, 5, 6 and 7 and cover the cases which are most relevant for symmetric cryptography. Interestingly, and maybe counter-intuitive, multiplication with non trivial elements in a proper subfield turns out to be among the most expensive in all the cases explored here.

Moreover, for all $n \leq 2048$ for which no irreducible trinomial of degree n exists, we present one element $\alpha \in \mathbb{F}_{2^n}$ such that multiplication by α requires two XOR operations, cf. Table 8. Those results are proven optimal by the above mentioned necessary and sufficient condition.

In the second part of the paper (cf. Sect. 4) we present several (circulant) matrices. Entries in those matrices are represented as powers of a generic field element α. By symbolically computing all minors, i.e. the determinants of all square submatrices, we derive a list of polynomials in $\mathbb{F}_2[\alpha]$. Now, whenever α is chosen such that it is not a root of any of those polynomials, the matrix is MDS. One nice consequence of this approach is that, as the degree of those polynomials is limited, our matrices are MDS for almost all elements in $\mathbb{F}_{2^n}$ as soon as n is large enough, i.e. larger than the maximal degree of those polynomials.

Finally, the first and second part are combined in Sect. 4.2 to result in the most efficient MDS matrices in terms of the XOR-count known so far. A summary of our results and comparison with previous work is given in Tables 1 and 2, respectively. The main observation here is that if multiplication by α can be implemented with t XOR operations, then multiplication by $\alpha^{\pm i}$ for $i \geq 0$ can be implemented with at most $t \cdot i$ XOR operations.[2] Thus, by simply mini-

[2] It is exactly this part where considering only in-place XOR operations becomes very helpful, as otherwise multiplication by α and by α^{-1} might differ in their XOR-count.

mizing the sum of the (absolute) exponents for our circulant MDS matrices, we immediately reduce the XOR-count.

As an interesting side result, we like to point out that the *XOR-count per bit actually decreases with increasing field size*.[3] For example, our 4×4 MDS matrices have a per bit XOR-count of $3 + \frac{3}{n}$, or $3 + \frac{6}{n}$ in the case that no irreducible trinomial of degree n exists.

Thus, even so reducing the number of XOR operations has already received considerable attention recently, this part nicely shows that our improved understanding of how to choose an optimal basis allows us to easily improve upon known constructions. Note that such improvements are possible independent from which XOR-count definition is used, that is, we were able to improve existing results also in the old XOR-count definition by changing the basis. For example, we found an element in $\mathbb{F}_{2^8}$ with only 2 additional non-zero entries which directly improves the results of [27].

Finally, in Sect. 5 we give a perspective on non-linear, additive MDS matrices. In particular, we point out that while there exists no $\alpha \in \mathbb{F}_{2^8}$ (resp. $\mathbb{F}_{2^{13}}$, $\mathbb{F}_{2^{16}}$) which can be implemented with only one XOR operation, there does exist an 8×8 (resp. 13×13, 16×16) binary matrix, that can be used in place for the multiplication by α in the above mentioned 4×4 matrix to result in an additive MDS matrix with reduced cost.[4] Again, the idea of considering the entries of the matrix as powers of a single field element is beneficial as the conditions for the matrix to be MDS remain basically unchanged.

We conclude the paper by pointing to some interesting questions for future investigations.

2 Preliminaries

If p is a prime, we denote the *finite field with p elements* by $\mathbb{F}_p$ and the *extension field with p^n elements* by $\mathbb{F}_{p^n}$, respectively. In this work, we consider binary fields, thus $p = 2$. Although there exists up to isomorphism only one finite field for every possible order, we are interested in the specific representation. For instance, if $q \in \mathbb{F}_2[x]$ is an irreducible polynomial of degree n, then $\mathbb{F}_{2^n} \cong \mathbb{F}_2[x]/(q)$ where (q) denotes the ideal generated by q. The multiplicative group of some field K is denoted by K^*. By the term *matrix*, we refer to matrices with entries in $\mathbb{F}_2$. In general, the ring of $n \times n$ matrices over a field K will be denoted by $\mathrm{Mat}_n(K)$. The symbol $\mathbf{0}_n$ will denote the *zero matrix* and I_n will be the *identity matrix*. As a third important type of matrix in $\mathrm{Mat}_n(\mathbb{F}_2)$, we introduce $E_{i,j}$ which consist of all zeros except in the i-th row of the j-th column for $i, j \in \{1, \ldots, n\}$. We denote a block diagonal matrix consisting of d matrix blocks A_k as $\bigoplus_{k=1}^{d} A_k$. By $\mathrm{wt}(A)$, we denote the number of non-zero entries of a matrix A. Analogously, $\mathrm{wt}(q)$ denotes the number of non-zero coefficients of a polynomial q.

[3] This is also true for the constructions given in [30], but does not hold for the subfield (or code-interleaving) construction.

[4] Note that the authors of [19] recently constructed a similar 32×32 $\mathbb{F}_2$-linear MDS matrix.

2.1 Some Basic Facts About Linear Transformations

We next recall some basics about finite fields and matrix representations. For more background the reader is referred to e.g. [20, Sect. 2.5] and [29]. Let $V \cong K^n$ be a finite-dimensional vector space over the field K. Every linear mapping $f : V \to V$ can be described as $v \mapsto A_B v$ by a left-multiplication with a matrix $A_B \in \mathrm{Mat}_n(K)$. This representation is dependent on the choice of the basis B for V. For instance, if $B = \{b_1, \ldots b_n\}$, the j-th column of A_B consists of the coefficients $a_{1,j}, \ldots, a_{n,j}$ of $f(b_j) = \sum_{i=1}^{n} a_{i,j} b_i$. Thus, changing the basis from B to B' results in a different matrix representation of f. This transformation is called the *change of basis* transformation, which is simply a conjugation of A_B. Thus, $A_{B'} = T A_B T^{-1}$ using an invertible matrix T. In this case, A_B and $A_{B'}$ are are called *similar* (resp. *permutation-similar* if T is a permutation matrix).

There is a natural way of representing the elements in a finite field with characteristic p as vectors with coefficients in $\mathbb{F}_p$. In the following, we consider the representation of the multiplication by α by a matrix as described in the following diagram.

$$\begin{array}{ccc} \mathbb{F}_{2^n} & \xrightarrow{\cdot\alpha} & \mathbb{F}_{2^n} \\ \Big\downarrow{\scriptstyle \Phi_B} & & \Big\uparrow{\scriptstyle \Phi_B^{-1}} \\ \mathbb{F}_2^n & \xrightarrow{M_{\alpha,B}} & \mathbb{F}_2^n \end{array}$$

The bijection Φ_B maps elements $\alpha \in \mathbb{F}_{2^n}$ to its vectorial representation over $\mathbb{F}_2$ with regard to a basis B (and Φ_B^{-1} vice versa). $M_{\alpha,B}$ denotes the $n \times n$ matrix representing (left-) multiplication by the element α. For different bases B and B', one can obtain $M_{\alpha,B'}$ from $M_{\alpha,B}$ by the change of basis transformation, in particular $M_{\alpha,B'} = T M_{\alpha,B} T^{-1}$ for an invertible T. We denote similarity of matrices with the relation symbol $\sim$, (resp. $\sim_\pi$ for permutation-similarity). The *characteristic polynomial* of a matrix A is defined as $\chi_A := \det(\lambda I - A) \in \mathbb{F}_2[\lambda]$ and the *minimal polynomial* is denoted by m_A. Recall that the minimal polynomial is the (monic) polynomial p of least degree, such that $p(A) = \mathbf{0}_n$. It is a well-known fact that the minimal polynomial divides the characteristic polynomial, thus $\chi_A(A) = \mathbf{0}_n$. As the minimal polynomial and the characteristic polynomial are actually properties of the underlying linear mapping, similar matrices have the same characteristic and the same minimal polynomial.

A special type of matrix, that will play an important role in the following is the companion matrix of a polynomial. For a polynomial

$$q = x^n + q_{n-1}x^{n-1} + \cdots + q_1 x + q_0 \in \mathbb{F}_2[x]$$

of degree n, the *companion matrix* of q is defined as

$$C_q = \begin{pmatrix} 0 & & & q_0 \\ 1 & 0 & & q_1 \\ & \ddots & \ddots & \vdots \\ & & 1 & 0\ q_{n-2} \\ & & & 1\ q_{n-1} \end{pmatrix}.$$

It is known from linear algebra that the characteristic polynomial and the minimal polynomial of C_q are equal to q itself, i.e. $\chi_{C_q} = m_{C_q} = q$. In addition, any matrix A is similar to a companion matrix if and only if its characteristic polynomial coincides with its minimal polynomial. In particular, C_q is exactly the *rational canonical form* [11, Sect. 12.2] of A in this case.

2.2 The XOR-Count and the Cycle Normal Form

The *XOR-count* of a field element was already studied in [17,27]. In the formal definition in [27], an invertible n-dimensional matrix A has an *XOR-count* of t if and only if A can be written as a permutation matrix with t additional non-zero entries. Formally, $A = P + \sum_{k=1}^{t} E_{i_k,j_k}$ and $\mathrm{wt}(A) = n + t$. Although all matrices of that structure can be implemented with at most t XOR operations (not necessarily without temporary registers), the construction does not contain all possible matrices which are realizable with at most t XOR operations. For instance, there are matrices with three additional non-zero entries such that the result of their defining linear function can be computed with just two additions. As an example, consider

$$\begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} = \begin{pmatrix} v_1 + v_3 \\ (v_1 + v_3) + v_2 \\ v_3 \end{pmatrix}.$$

In the following, we provide an alternative definition which includes the cases described above.

Definition 1. *An invertible matrix A has an* XOR-count *of t, denoted $\mathrm{wt}_{\oplus}(A) = t$, if t is the minimal number such that A can be written as*

$$A = P \prod_{k=1}^{t} (I + E_{i_k,j_k})$$

with $i_k \neq j_k$ for all k.

Note that if a matrix can be represented in the form $P \prod_{k=1}^{t} (I + E_{i_k,j_k})$, the number of factors $(I + E_{i_k,j_k})$ clearly gives an upper bound on the actual XOR-count. It is worth pointing out that the definition above just counts the number of XOR operations without using temporary registers. Those are technically

somewhat easier to handle. However, this restriction does not make a difference for matrices with XOR-count less or equal to 2, which we are most concerned about in in the following. In general, allowing temporary registers might well reduce the number of XOR operations needed for an implementation.

Our definition coincides with the one from [27] for the case that $t = 1$, that is, for matrices of XOR-count 1. For other cases, the number of additional non-zero entries can increase. We will often consider $t = 2$ within this work. By evaluating the product, it follows that any A with $\mathrm{wt}_{\oplus}(A) = 2$ is of the form

$$A = \begin{cases} P + P(E_{i_1,j_1} + E_{i_2,j_2}) & \text{iff } i_2 \neq j_1 \\ P + P(E_{i_1,j_1} + E_{i_2,j_2} + E_{i_1,j_2}) & \text{iff } i_2 = j_1. \end{cases}$$

The XOR-count is invariant under permutation-similarity. Moreover, naturally in the setting not allowing temporary registers, the XOR-count is invariant under taking the inverse. This is summarized and formally proven in the following Lemma and Corollary.

Lemma 1. *If* $A \sim_\pi A'$, *then* $\mathrm{wt}_{\oplus}(A) = \mathrm{wt}_{\oplus}(A')$.

Proof. Let $A' = QAQ^{-1}$ where Q is the permutation matrix representing the permutation $\sigma \in S_n$. Let $I + E_{i_k,j_k}$ be a factor in the XOR-count representation of $A = P\prod_{k=1}^{t}(I+E_{i_k,j_k})$ where $t = \mathrm{wt}_{\oplus}(A)$. Then the following identity holds:

$$(I + E_{i_k,j_k})Q^{-1} = Q^{-1} + E_{i_k,\sigma^{-1}(j_k)} = Q^{-1}(I + E_{\sigma(i_k),\sigma^{-1}(j_k)}).$$

One is able to commute Q^{-1} to the front before the first factor by proceeding for all of the t factors and finally obtain

$$A' = QPQ^{-1}\prod_{k=1}^{t}(I + E_{\sigma(i_k),\sigma^{-1}(j_k)}).$$

It follows that $\mathrm{wt}_{\oplus}(A') \leq \mathrm{wt}_{\oplus}(A)$. By reverting the above steps we obtain $\mathrm{wt}_{\oplus}(A) \leq \mathrm{wt}_{\oplus}(A')$. □

Corollary 1. *If* $\mathrm{wt}_{\oplus}(A) = t$, *then also* $\mathrm{wt}_{\oplus}(A^{-1}) = t$.

Proof. We show that A^{-1} is permutation-similar to a matrix with an XOR-count of t.

$$\left(P\prod_{k=1}^{t}(I + E_{i_k,j_k})\right)^{-1} = \prod_{k=t}^{1}(I + E_{i_k,j_k})P^{-1} \sim_\pi P^{-1}\prod_{k=t}^{1}(I + E_{i_k,j_k})$$

□

Later, we would like to be able to exhaustively search over all matrices with low XOR-count for a given dimension n. Since the number of permutation matrices (which is $n!$) rapidly increases with n, an exhaustive search will quickly become infeasible if we do not restrict the structure of P. By a well-known fact from combinatorics, one is able to assume P to be in a specific form.

Lemma 2. *For any permutation matrix P of dimension n, it is*

$$P \sim_\pi \bigoplus_{k=1}^{d} C_{x^{m_k}+1}$$

for some m_k with $\sum_{k=1}^{d} m_k = n$ and $m_1 \geq \cdots \geq m_d \geq 1$.

Proof. It is well-known that two permutations with the same cycle type are conjugate [11, Chapter 4.3, Proposition 11]. That is, given the permutations $\sigma, \tau \in S_n$ as

$$\sigma = (s_1, s_2, \ldots, s_{d_1})(s_{d_1+1}, \ldots, s_{d_2}) \ldots (s_{d_{m-1}+1}, \ldots, s_{d_m})$$
$$\tau = (t_1, t_2, \ldots, t_{d_1})(t_{d_1+1}, \ldots, t_{d_2}) \ldots (t_{d_{m-1}+1}, \ldots, t_{d_m})$$

in cycle notation, one can find some $\pi \in S_n$ such that $\pi\sigma\pi^{-1} = \tau$. This π operates as a relabeling of indices.

Let σ in the form above be the permutation defined by P. Now, there exits a permutation π such that $\pi\sigma\pi^{-1} = (d_1, 1, 2, \ldots, d_1 - 1)(d_2, d_1 + 1, d_1 + 2, \ldots, d_2 - 1) \ldots (d_m, d_{m-1} + 1, d_{m-1} + 2, \ldots, d_m - 1)$. If Q denotes the permutation matrix defined by π, one obtains QPQ^{-1} in the desired form. □

We say that any permutation matrix of this structure is in *cycle normal form*. The cycle normal form of P is denoted by $C(P)$. Up to permutation-similarity, we can always assume that the permutation matrix P of a given matrix with XOR-count t is in cycle normal form, as stated in the following corollary.

Corollary 2.

$$P \prod_{k=1}^{t} (I + E_{i_k, j_k}) \;\sim_\pi\; C(P) \prod_{k=1}^{t} (I + E_{\sigma(i_k), \sigma^{-1}(j_k)})$$

for some permutation $\sigma \in S_n$.

3 Efficient Multiplication in Finite Fields

In this section, we first present some theoretic results towards understanding the structure of matrices $M_{\alpha,B}$ representing (left-) multiplication by some finite field element $\alpha \in \mathbb{F}_{2^n}^*$. The parameter B indicates a basis of $\mathbb{F}_{2^n}$ considered as an n-dimensional vector space over $\mathbb{F}_2$. The XOR-count of $M_{\alpha,B}$ is indeed depending on the choice of the basis B. As described in Corollary 2, we can assume a certain normal form for matrices with an XOR-count of t.

Not every (invertible) matrix is a representation of a field multiplication. For example, an obvious condition for that, is that the multiplicative order of the matrix divides $2^n - 1$. In order to understand exactly which matrices indeed represent multiplication with some field element α, Theorem 1 below gives a characterization that allows to efficiently decide when a given matrix corresponds

to multiplication by a field element. The crucial part is the minimal polynomial of α. It is a property of the linear mapping

$$f_\alpha : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}, \beta \mapsto \alpha\beta$$

and is invariant under changing the specific representation of f_α to $\beta \mapsto M_{\alpha,B}\beta$.

Theorem 1. *Let $A \in \mathrm{Mat}_n(\mathbb{F}_2) \setminus \{\mathbf{0}_n\}$. Then $A = M_{\alpha,B}$ for some element $\alpha \in \mathbb{F}_{2^n}^*$ with respect to some basis B if and only if m_A is irreducible.*

Proof. As described in [29], the ring generated by some matrix A defines a field of order 2^n if and only if the characteristic polynomial χ_A is irreducible. This is the case since $\chi_A(A) = 0$ and thus A is the root of an irreducible polynomial of degree n. One can see that $\mathbb{F}_2(A) = \{\sum_{i=0}^{n-1} \alpha_i A^i \mid \alpha_i \in \mathbb{F}_2\}$ since it must contain all sums of powers of A. However, for $\mathbb{F}_2(A)$ being a field it is not necessary that A has an irreducible characteristic polynomial. It can be possible that A generates a subfield $\mathbb{F}_{2^m}$ of $\mathbb{F}_{2^n}$. As we show now, this is the case if and only if the minimal polynomial of α is irreducible and has degree m.

If m_A is not irreducible, $\mathbb{F}_2(A)$ is not a field and thus A cannot represent a field multiplication. Let now m_A be irreducible. The characteristic polynomial χ_A is necessarily a power of m_A, since both of these polynomials share the same irreducible factors. So, $\chi_A = (m_A)^d$ for some positive integer d. Both d and $\deg(m_A)$ divide n. Because of the irreducibility of m_A, the rational canonical form of A consists of d blocks of C_{m_A}. Thus, we obtain the similarity

$$A \sim \bigoplus_{k=1}^{d} C_{m_A}.$$

Since $\chi_{C_{m_A}} = m_A$, the matrix A defines a multiplication with some element in a subfield of $\mathbb{F}_{2^n}$. □

Note that, any field element α is, up to its conjugates $\alpha, \alpha^2, \alpha^{2^2}, \ldots, \alpha^{2^{n-1}}$, uniquely identified by its minimal polynomial. For every field element α, the minimal polynomial m_α is exactly the minimal polynomial m_A of a matrix A representing multiplication with α. Furthermore, two matrices $A, A' \in \mathrm{Mat}_n(\mathbb{F}_2)$ with the same irreducible minimal polynomial are similar. Thus, given a matrix A, identifying the element α such that $A = M_{\alpha,B}$ is equivalent to computing the (irreducible) minimal polynomial of A.

The main question is which field elements can be implemented with a minimal number of XOR operations, or in particular, what is the minimal XOR-count for a given (non-trivial) field element $\alpha \in \mathbb{F}_{2^n}^*$. Trivially, multiplication with $\alpha = 1$ can be implemented with zero additions since $M_{1,B} = I_n$ for all bases B. On the other hand, if the XOR-count is 0, the element is equal to 1. In a first place, we thus aim for an XOR-count of 1 whenever possible. By a simple observation, this optimal result can be realized if the minimal polynomial of α is a trinomial of degree n.

Example 1. Let the field with 2^n elements be represented as $\mathbb{F}_{2^n} = \mathbb{F}_2[x]/(q)$ for an irreducible q of degree n. For the (left-) multiplication with x in the canonical basis $B = \{1, x, x^2, \ldots, x^{n-1}\}$, it is $M_{x,B} = C_q$. Thus, $\mathrm{wt}_\oplus(M_{x,B}) = \mathrm{wt}(q) - 2$ and the XOR-count of $M_{x,B}$ equals 1 if q is a trinomial.

Since our approach is about finding any (non-trivial) element $\alpha \in \mathbb{F}_{2^n}^*$ such that multiplication with α can be implemented with minimal additions, this fact implies that we cannot hope to improve upon the implementation costs if there exists an irreducible trinomial of degree n. However, for several n, including the interesting case where n is a multiple of 8, there does not exist such a trinomial [28]. The question is what happens for these cases. As one of our main results, we show that the condition on the minimal polynomial is not only sufficient but also necessary.

3.1 Characterizing Elements with Optimal XOR-Count

In this section, we prove the converse of the fact described in Example 1, namely the necessary condition on the minimal (resp. characteristic) polynomial of α resulting in an XOR-count of 1.

Theorem 2. *Let $\alpha \in \mathbb{F}_{2^n}$. Then there exists a matrix A with $\mathrm{wt}_\oplus(A) = 1$ such that $A = M_{\alpha,B}$ for some basis B if and only if m_α is a trinomial of degree n.*

Proof. Let $M_{\alpha,B}$ represent multiplication by some element $\alpha \in \mathbb{F}_{2^n}$ with respect to the basis $B = \{b_1, \ldots, b_n\}$ and let further $\mathrm{wt}_\oplus(M_{\alpha,B}) = 1$. We show that the characteristic polynomial $\chi_{M_{\alpha,B}}$ is a trinomial and coincides with m_α. Since the XOR-count is 1, we can assume w.l.o.g. that $M_{\alpha,B} = P + E_{i,j}$ such that $P = \bigoplus_{k=1}^{l} C_{x^{m_k}+1}$ is in cycle normal form. We first show that $l = 1$. Suppose $l > 1$, then, depending on $E_{i,j}$, the matrix $M_{\alpha,B}$ is either in upper or lower triangular form consisting of at least two diagonal blocks. Since one of them must be of the form C_{x^m+1}, the polynomial x^m+1 must divide the characteristic polynomial $\chi_{M_{\alpha,B}}$. Since further $(x+1) \mid (x^m+1)$, the minimal polynomial of α is necessarily a multiple of $x+1$. This is a contradiction since $\alpha \neq 1$ and m_α must be irreducible. Hence, $M_{\alpha,B}$ is permutation-similar to $C_{x^n+1} + E_{i,j}$. It is further $i \neq j+1 \mod n$ since otherwise $M_{\alpha,B}$ would be singular.

We now investigate how α operates on the basis elements $b_k \in B$. Considering the structure of $M_{\alpha,B}$, we obtain the following list of equations.

$$
\begin{aligned}
\alpha b_1 &= b_2 \\
&\vdots \\
\alpha b_{j-1} &= b_j \\
\alpha b_j &= b_{j+1} + b_i \\
\alpha b_{j+1} &= b_{j+2} \\
&\vdots \\
\alpha b_n &= b_1.
\end{aligned}
$$

By defining $\gamma := b_{j+1}$, one can express every basis element b_k as a power of α multiplied by γ. In particular,

$$b_{j+k \mod n} = \alpha^{k-1}\gamma \tag{1}$$

for $k \in \{1, \ldots, n\}$. Combining this observation with the identity $\alpha b_j = b_{j+1} + b_i$, one obtains

$$\alpha^n \gamma = \gamma + \alpha^t \gamma \tag{2}$$

for some exponent $t \neq 0$. Since $\gamma \neq 0$, the field element α is a root of the trinomial $p = x^n + x^t + 1$. It is left to show that p is exactly the minimal polynomial of α. Suppose that $m_\alpha = x^m + \sum_{k=0}^{m-1} c_k x^k$ with constants $c_k \in \{0, 1\}$ and $m < n$. By multiplying $m_\alpha(\alpha)$ with γ, one obtains

$$\alpha^m \gamma = \sum_{k=0}^{m-1} c_k \alpha^k \gamma$$

and thus $b_{t_m} = \sum_{k=0}^{m-1} c_k b_{t_k}$ for some basis elements b_{t_k}. We are now able to express one basis element b_{t_k} as a sum of other elements from B which is contradictory to the linear independence of the basis. Hence, $\deg(m_\alpha) = n$ and thus $m_\alpha = p$ which finally proves the theorem. □

Note that the polynomial p is exactly the characteristic polynomial of $M_{\alpha,B}$ since it must be a monic multiple of m_α having degree n. An alternative way of proving that the characteristic polynomial of a matrix $C_{x^n+1} + E_{i,j}$ is a trinomial is given in Appendix A. As a simple corollary one obtains that any $\alpha \in \mathbb{F}_{2^n}^*$ with an XOR-count of 1 cannot be contained in a proper subfield.

Corollary 3. *Let $\alpha \in \mathbb{F}_{2^n}^* \setminus \{1\}$ and let further $\deg(m_\alpha) < n$, indicating that α lies in a proper subfield of $\mathbb{F}_{2^n}$. Then, any matrix $M_{\alpha,B}$ representing multiplication by a field element α with respect to some basis B has $\mathrm{wt}_\oplus(M_{\alpha,B}) > 1$.*

This result implies that building MDS layers using a block interleaving construction [1], also called subfield construction in [17], almost always results in suboptimal implementation costs. Note that specific instances of this construction are also implicitly used in the AES, LS-Designs [12] and the hash function Whirlwind [3].

Now let α be an element with XOR-count 1. From Corollary 1 we know that α^{-1} has the same XOR-count. Next, we show that there do not exist any further elements with an XOR-count equal to 1.

Theorem 3. *For any given basis B of $\mathbb{F}_{2^n}$, there exist at most two field elements α and α^{-1} with $\mathrm{wt}_\oplus(M_{\alpha,B}) = \mathrm{wt}_\oplus(M_{\alpha^{-1},B}) = 1$.*

Proof. Let $\alpha \in \mathbb{F}_{2^n}^*$ with $\mathrm{wt}_\oplus(M_{\alpha,B}) = 1$ for the basis $B = \{b_1, \ldots, b_n\}$. We show that for any $\beta \in \mathbb{F}_{2^n}$ with $\mathrm{wt}_\oplus(M_{\beta,B}) = 1$ it holds that $\beta = \alpha^{\pm 1}$.

Since w.l.o.g. $M_{\alpha,B}$ can be assumed to be of the form $C_{x^n+1} + E_{i,j}$, we know that (1) and (2) hold. We further know that $M_{\beta,B}$ is of the form $P + E_{i',j'}$ and thus there exist $l, m \in \{1, \ldots, n\}$ with $l \neq m$ and $\beta b_{j+l \mod n} = b_{j+m \mod n}$. Using Eq. (1), we can write $\beta = \alpha^{m-l} =: \alpha^s$ where $s \in \{-(n-1), \ldots, n-1\}$. We directly see that $s \neq 0$. It remains to show that $-1 \leq s \leq 1$.

Assume $s \geq 2$. We use Eqs. (1) and (2) to obtain

$$\beta b_{j+(n-s+1) \mod n} = \alpha^n \gamma = \gamma + \alpha^t \gamma = b_{j+1 \mod n} + b_{j+t+1 \mod n}.$$

Since $0 < t < n$, it holds that $b_{j+1 \mod n} \neq b_{j+t+1 \mod n}$ and thus the according column contains an additional 1. For the next column, we have

$$\begin{aligned} \beta b_{j+(n-s+2) \mod n} &= \alpha^{n+1}\gamma = \alpha\gamma + \alpha^{t+1}\gamma \\ &= \begin{cases} b_{j+2 \mod n} + b_{j+t+2 \mod n}, & \text{for } t < n-1 \\ b_{j+2 \mod n} + b_{j+1 \mod n} + b_{j \mod n}, & \text{for } t = n-1 \end{cases} \end{aligned}$$

Hence, this column also contains at least one additional 1 which is contradictory to the XOR-count of 1.

For $-s \geq 2$ we can construct the same contradiction by considering β^{-1}. □

We now understand the structure of field elements α that can be implemented with a single addition. One might think that also for the other cases, the weight of the minimal polynomial of α strictly lower-bounds XOR-count as $\mathrm{wt}(m_\alpha) - 2$. As we will see next, this is not the case.

3.2 Experimental Search for Optimal XOR-Counts

Surprisingly, we often can improve the XOR-count, compared to using the companion matrix for multiplication, if the weight of the minimal polynomial is greater than 3. For instance, if m_α is an irreducible pentanomial, that is of weight 5, of degree n there often exists a basis B such that $\mathrm{wt}_\oplus(M_{\alpha,B}) = 2$. Indeed, for all $n \leq 2048$ for which no irreducible trinomial of degree n exists, we found some element $\alpha \in \mathbb{F}_{2^n}^*$ with an XOR-count of 2 for some basis B. For every such dimension, we present an example of such a matrix in Table 8. Thus, for all practically relevant fields, we are able to identify an element such that multiplication can be implemented with one or two XOR operations. By Theorem 2, these results are proven to be optimal.

Moreover, as fields of small size are most interesting for SP-networks, we investigated those in full detail. For the fields $\mathbb{F}_{2^4}$, $\mathbb{F}_{2^5}$, $\mathbb{F}_{2^6}$, $\mathbb{F}_{2^7}$ and $\mathbb{F}_{2^8}$ we present the optimal XOR-count for each non-trivial element α in Tables 3, 4, 5, 6 and 7, respectively. The main observation is that each element which is not contained in a proper subfield can be implemented with at most 3 additions. Furthermore, whenever an XOR-count of 2 is possible, the minimal polynomial of α is a pentanomial in all those cases. However, a more thorough characterization of elements with non-optimal XOR-count is left as an open problem (see Sect. 6 for more details).

Those results are based on a search. Since we are only interested in matrices up to similarity (due to the change of basis), we just need to consider all matrices in the normal form described in Corollary 2. This will exhaust all possibilities of similarity classes for a given XOR-count t. In particular, the search space is reduced from $n!(n(n-1))^t$ to only $p(n)(n(n-1))^t$ where $p(n)$ denotes the number of partitions of n, which is exactly the number of possible cycle normal forms of dimension n. This allows us to exhaustively search over all similarity classes up to $t = 3$ XOR operations for the fields of small size. The key-point here is that, instead of searching for an optimal basis for a given field element, we generated all matrices with small XOR-count and used Theorem 1 in order to check which field element (if any) the given matrix corresponds to.

In order to identify a single lightweight element for larger field sizes, we identified conditions in which cases the characteristic polynomial of a matrix with XOR-count 2 has weight 5, cf. Theorem 4 below. During the search, one only has to check for irreducibility. This allows to compute the results presented in Table 8 extremely fast, that is within a couple of minutes on a standard PC. The proof of Theorem 4 is given in Appendix A.

Theorem 4. *Let $M = C_{x^n+1} + E_{i_1,j_1} + E_{i_2,j_2}$ such that the following relations hold:*

$$i_1 < j_1 \neq n, \quad i_2 > j_2 + 1, \quad i_1 \leq j_2, \quad i_2 \leq j_1, \quad j_1 - (i_1 - 1) \neq n, \quad n - (j_1 - i_1) \neq i_2 - j_2$$

The characteristic polynomial of M is a pentanomial of degree n. In particular

$$\chi_M = \lambda^n + \lambda^{n+i_1-j_1+i_2-j_2-2} + \lambda^{n+i_1-j_1-1} + \lambda^{i_2-j_2-1} + 1.$$

4 Constructing Lightweight MDS Matrices

Our goal is now to construct lightweight MDS matrices. We use the results obtained in the previous sections and restrict our search to circulant matrices and entries with low XOR-count. This simplifies checking the MDS property and computing an upper bound of the XOR-count of the whole matrix. The complexity of our algorithm enables us to easily search for MDS matrices up to dimension 8. Our construction is generic and works for all finite fields $\mathbb{F}_{2^m}$ with $m > b$ for a given bound b.

More precisely, we construct circulant matrices with entries of the form $\alpha^{\pm i}$ where α is an element in $\mathbb{F}_{2^m}$. Choosing entries of this form enables us to easily upper-bound the XOR-count of the elements since

$$\mathrm{wt}_{\oplus}(x^{\pm k}) \leq k \, \mathrm{wt}_{\oplus}(x).$$

This can be easily seen by using Corollary 1 and the fact that α^k can be implemented by k times implementing α. We want to keep the size of the finite field over which the matrix is defined generic. Thus, we choose the matrix entries from a subgroup of the *field of fractions* of the polynomial ring $\mathbb{F}_2[x]$, denoted $\mathrm{Quot}(\mathbb{F}_2[x])$. That is, every element is of the form

$$\frac{x^s + a_{s-1}x^{s-1} + \cdots + a_1 x + a_0}{x^t + b_{t-1}x^{t-1} + \cdots + b_1 x + b_0}.$$

More precisely, and as mentioned above, we restrict our search to elements from $\langle x \rangle$ which is the multiplicative subgroup of $\mathrm{Quot}(\mathbb{F}_2[x])$ generated by x. Our search works by constructing MDS conditions for an $n \times n$ matrix M with entries in $\langle x \rangle$. This approach later allows us to substitute the indeterminate x by any $\alpha \in \mathbb{F}_{2^m}$ that fulfills all of the conditions given below. In this context, we let $M(\alpha) \in \mathrm{Mat}_n(\mathbb{F}_{2^m})$ denote the matrix obtained by substituting x with $\alpha \in \mathbb{F}_{2^m}$.

We define the *weight* of some circulant matrix with entries in $\langle x \rangle$ as the sum of the absolute values of the exponents in its first row, that is, the number of times α has to be applied *per row*. Then, for a given dimension, we are interested in finding the lightest matrix M which can be made MDS for as many finite fields as possible. Note that the higher priority here was to find a lightweight matrix. Thus, there might exist matrices which can be made MDS for even more fields, but with a probably higher cost.

MDS Conditions. Note that a matrix is MDS, if and only if all its square submatrices are invertible [22, page 321, Theorem 8]. Thus, given a matrix $M \in \mathrm{Mat}_n(\mathrm{Quot}(\mathbb{F}_2[x]))$, we compute the determinants of all square submatrices (called *minors*) of M in order to check the MDS property. This way one obtains a list of conditions (polynomials in $\mathbb{F}_2$) for a matrix to be MDS. Since the determinant of a matrix with elements from a field is an element of the field itself, all of these determinants can be represented as the fraction of two polynomials. Thus, M is MDS if and only if the numerator of all minors is non-zero. One can decompose the numerators into their irreducible factors and collect all of them in a set T. This set now defines the MDS conditions. In particular, $M(\alpha)$ is MDS if and only if α is not a root of any of these irreducible polynomials in T, that is, iff $m_\alpha \notin T$. This trivially holds for $m > \max_{p \in T}\{\deg(p)\}$ and any $\alpha \in \mathbb{F}_{2^m}$ which is not contained in a proper subfield. In general, if α is not contained in a proper subfield, the necessary and sufficient condition for the existence of an MDS matrix $M(\alpha)$ is that not all irreducible polynomials of degree m are contained in T. We note that there exists a value b which lower bounds the field size for which M can always be made MDS. That is, for all $t > b$, there exists an irreducible polynomial of degree t which is not in T.

4.1 Generic Lightweight MDS Matrices

We now present some results obtained by the approach described above. Given the restrictions, these matrices achieve the smallest weight, i.e. the smallest sum of (absolute) exponents of x. Later, we will use these generic matrices to build concrete instantiations of $n \times n$ MDS matrices $M(\alpha)$ for $n \in \{2, 3, \ldots, 8\}$ over a finite field $\mathbb{F}_{2^m}$ with $m > b$. We note that the given results are not necessarily the only possible constructions with the smallest weight.

We also present the conditions for the matrix to be MDS, that is, the irreducible polynomials that must not be equal to m_α. However, since the number of conditions rapidly increases with the dimension of the matrix, we refrain from presenting a complete list for dimensions 6 to 8. Instead, we give the SageMath

Listing 1.1. Sage code for computing the set T.

```
P.<x> = GF(2)[]
K = FractionField(P)

def mds_equations(M):
    R = [P(x)]
    for i in range(len(M.rows())+1)[1:]:
        L = M.minors(i)
        for l in L:
            if (l != 0):
                F = list(l.numerator().factor())
                for f in F:
                    R.append(f[0])
            else:
                return
    return list(set(R))
```

source code that was used to compute the set T of irreducible polynomials in Listing 1.1.

2×2 **and** 3×3 **matrices.** The matrices

$$\mathrm{circ}(1, \alpha) = \begin{pmatrix} 1 & \alpha \\ \alpha & 1 \end{pmatrix}$$

and

$$\mathrm{circ}(1, 1, \alpha) = \begin{pmatrix} 1 & 1 & \alpha \\ \alpha & 1 & 1 \\ 1 & \alpha & 1 \end{pmatrix}$$

are MDS for all $\alpha \neq 0, 1$.

4×4 **matrices.** For $m > 3$, there exists an $\alpha \in \mathbb{F}_{2^m}$ such that the matrix $\mathrm{circ}(1, 1, \alpha, \alpha^{-2})$ is MDS. More precisely, the matrix is MDS iff α is not a root of any of the following polynomials:

$$\begin{aligned} x \\ x + 1 \\ x^2 + x + 1 \\ x^3 + x + 1 \\ x^3 + x^2 + 1 \\ x^4 + x^3 + x^2 + x + 1 \\ x^5 + x^2 + 1 \end{aligned}$$

5×5 **matrices.** For $m > 3$, there exists an $\alpha \in \mathbb{F}_{2^m}$ such that the matrix $\mathrm{circ}(1, 1, \alpha, \alpha^{-2}, \alpha)$ is MDS. More precisely, the matrix is MDS iff α is not a root of any of the following polynomials:

$$\begin{aligned} x \\ x+1 \\ x^2+x+1 \\ x^3+x+1 \\ x^3+x^2+1 \\ x^4+x+1 \\ x^4+x^3+1 \end{aligned}$$

6×6 **matrices.** For $m > 5$, there exists an $\alpha \in \mathbb{F}_{2^m}$ such that the matrix $\mathrm{circ}(1, \alpha, \alpha^{-1}, \alpha^{-2}, 1, \alpha^3)$ is MDS.
7×7 **matrices.** For $m > 5$, there exists an $\alpha \in \mathbb{F}_{2^m}$ such that the matrix $\mathrm{circ}(1, 1, \alpha^{-2}, \alpha, \alpha^2, \alpha, \alpha^{-2})$ is MDS.
8×8 **matrices.** For $m > 7$, there exists an $\alpha \in \mathbb{F}_{2^m}$ such that the matrix $\mathrm{circ}(1, 1, \alpha^{-1}, \alpha, \alpha^{-1}, \alpha^3, \alpha^4, \alpha^{-3})$ is MDS.

4.2 Instantiating Lightweight MDS Matrices

We now combine the efficient multiplication in finite fields from Sect. 3 with our construction of MDS matrices. That is, the presented generic MDS matrices are instantiated with elements α with low XOR-count.

In a matrix multiplication every element is computed as the sum over multiplications. The according XOR-count was already discussed in [17,27]. For our matrices, the total number of XOR operations needed *per row* is upper bounded by

$$(n-1)m + w \cdot \mathrm{wt}_{\oplus}(\alpha).$$

Here, $(n-1)m$ XORs are the static part which comes from summing over the multiplication results and w is the weight as defined above. The *overhead* of $w \cdot \mathrm{wt}_{\oplus}(\alpha)$ XORs is needed for multiplying with the single elements. The static part cannot be changed by fast multiplication. Therefore, this overhead is the part that has to be minimized.

The cost per bit for the whole matrix is given by

$$\frac{n((n-1)m + w\,\mathrm{wt}_{\oplus}(\alpha))}{nm} = n - 1 + \frac{w\,\mathrm{wt}_{\oplus}(\alpha)}{m}.$$

One can notice that it decreases for larger field sizes.

For each of the matrices M described in Sect. 4.1, Table 1 presents choices for α such that $M(\alpha)$ is MDS. Note that concrete instantiations are only given up to the field size $m = 13$. The reason is that for larger m, all possible C_p with

Table 1. Optimal instantiations of the generic MDS matrices for $2 \leq n \leq 8$. In each cell, the first entry describes the minimal polynomial of $\alpha \in \mathbb{F}_2^m$ and the second entry describes the overhead of the instantiated $n \times n$ matrix $M(\alpha)$. The trinomial $x^m + x^a + 1$ is denoted by (a) and the pentanomial $x^m + x^a + x^b + x^c + 1$ is denoted by (a, b, c).

n	m											
	2	3	4	5	6	7	8	9	10	11	12	13
2	(1), 1	(1), 1	(1), 1	(2), 1	(1), 1	(1), 1	(6,5,1), 2	(1), 1	(3), 1	(2), 1	(3), 1	(10,9,1), 2
3	(1), 1	(1), 1	(1), 1	(2), 1	(1), 1	(1), 1	(6,5,1), 2	(1), 1	(3), 1	(2), 1	(3), 1	(10,9,1), 2
4	-	-	(1), 3	(3), 3	(1), 3	(1), 3	(6,5,1), 6	(1), 3	(3), 3	(2), 3	(3), 3	(10,9,1), 6
5	-	-	(3,2,1), 8	(2), 4	(1), 4	(1), 4	(6,5,1), 8	(1), 4	(3), 4	(2), 4	(3), 4	(10,9,1), 8
6	-	-	-	-	(1), 7	(1), 7	(6,5,1), 14	(1), 7	(3), 7	(2), 7	(3), 7	(10,9,1), 14
7	-	-	-	-	(1), 8	(1), 8	(6,5,1), 16	(1), 8	(3), 8	(2), 8	(3), 8	(10,9,1), 16
8	-	-	-	-	-	-	(6,5,2), 26	(8), 13	(3), 13	(2), 13	(3), 13	(10,9,1), 26

p as an irreducible degree-m polynomial of weight 3 are valid choices. If no such trinomial exists, one can choose $M_{\alpha,B}$ as in Table 8.

Table 2 compares the results presented in this section to the best constructions known so far. It turned out that our construction of the 4×4 MDS matrix in $\mathbb{F}_{2^4}$ is identical to the $\mathbb{F}_2$-linear matrix constructed in [19,21]. We stress that our construction leads to the lightest MDS matrices known, improving the results described in [21,27] for 8×8 MDS matrices in $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$ respectively. This is also the case when considering an unrolled implementation of the serial implementations in [30]. Unrolled variants of their implementations have an XOR-count that is slightly larger than ours. Moreover, and more importantly, the circuit depth is considerably increased due to the optimization with respect to a serial implementation.

Table 2. Comparison of our results with the (non-involutory) $\mathbb{F}_{2^m}$-linear MDS matrices from [27, Sect. 6.2], [19,21] by overhead. a: In these constructions, the XOR-count is measured by counting the number of additional 1's in the corresponding matrix.

(n,m)	Our construction	Construction in [27][a]	Construction in [21][a]	Construction in [19][a]
(4,4)	3	5	3	3
(4,8)	6	10	8	
(8,8)	26	40	30	

Note that our results in Table 2 are measured by the XOR-count from Definition 1 while the results from [19,21,27] use the old XOR-count definition. Additionally to these results, our understanding of how to choose an optimal basis can also be used to improve existing results in the old XOR-count definition. For example, we can represent the 8×8 MDS matrix in $\mathbb{F}_{2^8}$ from [21] with 28 additional ones instead of 30 by change of basis.

5 Generalizing the MDS Property

Here, following e.g. [30], we consider a generalization to additive MDS codes in order to improve efficiency.

There are some dimensions for which no field element with an XOR-count of 1 exists, for instance $m = 8$. However, especially this dimension is very important since lots of block cipher designs are byte oriented. One would wish to have some element α with $\mathrm{wt}_{\oplus}(\alpha) = 1$. A way of solving this problem is to not restrict to field elements. Instead, α can be chosen to be some other matrix in the ring $R = \mathrm{Mat}_m(\mathbb{F}_2)$. Given an $n \times n$ matrix M with elements in $\mathrm{Quot}(\mathbb{F}_2[x])$, the substitution $M(\alpha)$ now consists of elements in a commutative ring with unity, which is the subring of R generated by α. In general, given a commutative ring with unity R, one can define the determinant $\det_R : \mathrm{Mat}_n(R) \to R$ in a similar way than for matrices over fields. As described in [18, pp. 212–215], any $A \in \mathrm{Mat}_n(R)$ is invertible if and only if $\det_R(A)$ is a unit in R. We now define the MDS property for matrices over a commutative ring.

Definition 2. *Let R be a commutative ring with unity. A matrix $M \in \mathrm{Mat}_n(R)$ is* MDS *if and only if for every $1 \leq s \leq n$, any $s \times s$ submatrix of M is invertible.*

For checking the MDS property in our case, we use a well-known fact about block matrices.

Theorem 5 (Theorem 1 in [26]). *Let K be a field and let R be a commutative subring of $\mathrm{Mat}_m(K)$ for some integer m. For any matrix $M \in \mathrm{Mat}_d(R)$, it is*

$$\det(M) = \det(\det_R(M)),$$

where $\det(M)$ is the determinant of M considered as $M \in \mathrm{Mat}_{dm}(K)$.

As an implication, $M(\alpha)$ is MDS if and only if $p(\alpha)$ is invertible for all $p \in T$, if and only if $\det(p(\alpha)) \neq 0$ for all $p \in T$.

2×2 and 3×3 matrices. Given $M = \mathrm{circ}(1, x)$ (resp. $M = \mathrm{circ}(1, 1, x)$), one has to make sure that both x and $x + 1$ are invertible for M to be MDS. This is the case if x is substituted by the companion matrix C_{x^m+x+1} for $m \geq 2$. Thus, $M(C_{x^m+x+1})$ is MDS and each entry has an XOR-count of 1.

4×4 matrices. The MDS conditions are more complex than above. So, we only present some improvements for $m \in \{8, 13, 16\}$. The matrix $M = \mathrm{circ}(1, 1, \alpha, \alpha^{-2})$ is MDS for

$$\alpha \in \{C_{x^8+x^2+1}, C_{x^{13}+x+1}, C_{x^{16}+x+1}\}.$$

Note that a similar matrix for $m = 8$ was recently constructed in [19].

6 Conclusion and Open Problems

We presented a study of optimal multiplication bases with respect to the XOR-count. When applied to MDS matrices those lead to very efficient round-based implementations. We expect our results to be applied in other domains as well.

Our investigations leave many possibilities for future research. While we have been able to characterize exactly which field elements can be implemented with one XOR operation only, the general case is still open. For small fields of dimension smaller or equal to eight, we were able to compute the optimal bases with the help of an exhaustive computer search. However, for larger dimensions, this approach turns quickly inefficient and more insight would be needed. As a first step, we conjecture the following statement.

Conjecture 1. If $\mathrm{wt}_{\oplus}(M_{\alpha,B}) = 2$, then m_α is of weight smaller or equal to 5.

Note that the converse of the conjectured statement is (unlike the case of trinomials) wrong. As can be seen in Table 7, there exist a pentanomial of degree 8 which cannot be implemented with two XOR operations only. Beyond that, our intuition is that the larger the weight of the minimal polynomial, the larger the gap between the most efficient multiplication and the efficiency of multiplying by means of the companion matrix. Quantifying and demonstrating such a statement is an interesting and challenging open problem. Another interesting question is to get an improved understanding of how to most efficiently multiply with elements in proper subfields. More specifically, as a generalization of Corollary 3, one may ask the following question.

Question 1. Is the most efficient way to multiply with a subfield element given by multiplying in the subfield d times, where d is the extension degree of the field when viewed as an extension of the subfield. More precisely, given an $\alpha \in \mathbb{F}_{2^m}^* \subset \mathbb{F}_{2^n}^*$ in a proper subfield of dimension $m = \frac{n}{d}$ and let $M_{\alpha \in \mathbb{F}_{2^m}, B'}$ be the multiplication matrix in $\mathbb{F}_{2^m}$ with an optimal XOR-count. Is $M_{\alpha \in \mathbb{F}_{2^n}, B} = \bigoplus_{k=1}^{d} M_{\alpha \in \mathbb{F}_{2^m}, B'}$ a matrix with the lowest possible XOR-count for multiplication with $\alpha \in \mathbb{F}_{2^n}$? In particular, is $\mathrm{wt}_{\oplus}(M_{\alpha \in \mathbb{F}_{2^n}, B}) = d\,\mathrm{wt}_{\oplus}(M_{\alpha \in \mathbb{F}_{2^m}, B'})$?

Finally, for MDS matrices, it should be noted that we *locally* achieve the optimal solution. What would be needed to finally settle the search for lightweight matrices is a global optimal solution. That is for a given dimension, find an MDS matrix that can be implemented with the minimal number of XOR operations.

Finally, when optimizing for software, similar questions can be phrased and investigating solutions that are valid for more than one specific platform is a challenging research topic.

Acknowledgements. We would like to thank Thomas Peyrin for some valuable discussions on the notion of the XOR-count. We would also like to thank Gottfried Herold. This work was partly supported by the DFG Research Training Group GRK 1817 Ubicrypt and by the BMBF Project UNIKOPS (01BY1040).

A Proofs

In the following, we present an alternative way of proving the fact that the characteristic polynomial of some matrix $M = C_{x^n+1} + E_{i,j}$ with $\mathrm{wt}_{\oplus}(M) = 1$ is a trinomial of degree n. This is true in general, even if M does not represent a multiplication with a field element.

Lemma 3. *For $M = C_{x^n+1} + E_{i,j}$ with $\mathrm{wt}(M) = n + 1$, the characteristic polynomial χ_M of M is a trinomial of degree n.*

Proof. It is to compute $\chi_M = \det(\lambda I_n - M) = \det(\lambda I_n + C_{x^n+1} + E_{i,j})$. If $j = n$, then $M = C_{x^n+x^{i-1}+1}$ and $\chi_M = \lambda^n + \lambda^{i-1} + 1$ is a trinomial of degree n. Thus, w.l.o.g. one can assume $j < n$. To compute the determinant we use Laplace's formula by expanding along the n-th column. One obtains

$$\chi_M = \det\left(\begin{pmatrix} 1 & \lambda & & & \\ & 1 & \lambda & & \\ & & \ddots & \ddots & \\ & & & 1 & \lambda \\ & & & & 1 \end{pmatrix} + E_{i-1,j}\right) + \lambda \det\left(\begin{pmatrix} \lambda & & & & \\ 1 & \lambda & & & \\ & \ddots & \ddots & & \\ & & 1 & \lambda & \\ & & & 1 & \lambda \end{pmatrix} + E_{i,j}\right),$$

where $E_{0,j} := \mathbf{0}$ and $E_{n,j} := \mathbf{0}$. Both of these remaining matrices are of dimension $(n-1) \times (n-1)$. We now distinguish three cases:

(i) $i < j$: The additional 1 lies in the upper triangle of M. Now, χ_M reduces to $\chi_M = 1 + \lambda \det(\lambda I_{n-1} + C_{x^{n-1}} + E_{i,j}))$. In order to compute the remaining determinant, we keep on expanding along the last column for $n-1-j$ times until the additional 1 is located in the rightmost column. We now obtain the determinant of a companion matrix. Thus,

$$\begin{aligned} \chi_M &= 1 + \lambda^{n-j} \det(\lambda I_j + C_{x^j+x^{i-1}}) \\ &= 1 + \lambda^{n-j}(\lambda^j + \lambda^{i-1}) = \lambda^n + \lambda^{n-j+i-1} + 1. \end{aligned}$$

(ii) $i = j$: In this case, the additional 1 lies on the main diagonal of M and

$$\chi_M = 1 + \lambda(\lambda^{n-2}(\lambda + 1)) = \lambda^n + \lambda^{n-1} + 1.$$

(iii) $i > j$: The additional 1 lies in the lower triangle of M. Because of the structure of M, it is further $i > (j + 1)$. Defining the $m \times m$ matrix S_m^λ as

$$S_m^\lambda := \begin{pmatrix} 1 & \lambda & & & \\ & 1 & \lambda & & \\ & & \ddots & \ddots & \\ & & & 1 & \lambda \\ & & & & 1 \end{pmatrix},$$

the characteristic polynomial of M reduces to $\chi_M = \det(S^\lambda_{n-1}+E_{i-1,j})+\lambda^n$. We expand along the last row of $S^\lambda_{n-1} + E_{i-1,j}$ for $n-i$ times and get $\chi_M = \det(S^\lambda_{i-1} + E_{i-1,j}) + \lambda^n$.

Now, the additional 1 lies in the last row of the remaining $(i-1)\times(i-1)$-dimensional matrix. The goal is now to shift this 1 to the first column. This is done by expanding $j-1$ times along the first column. We now obtain $\chi_M = \det(S^\lambda_{i-j}+E_{i-j,1})+\lambda^n$ and the additional 1 is in the lower left corner of the matrix. As a last step, we expand along the first column for one more time and finally get

$$\begin{aligned}\chi_M &= \lambda^n + \det(S^\lambda_{i-j} + E_{i-j,1}) = \lambda^n + \det(\lambda I_{i-j-1} + C_{x^{i-j-1}}) + 1\\ &= \lambda^n + \lambda^{i-j-1} + 1.\end{aligned}$$

We now present the proof of Theorem 4 which makes use of Lemma 3. □

Theorem 4. *Let $M = C_{x^n+1} + E_{i_1,j_1} + E_{i_2,j_2}$ such that the following relations hold:*

$$i_1 < j_1 \neq n, \quad i_2 > j_2 + 1, \quad i_1 \leq j_2, \quad i_2 \leq j_1, \quad j_1 - (i_1 - 1) \neq n, \quad n - (j_1 - i_1) \neq i_2 - j_2$$

The characteristic polynomial of M is a pentanomial of degree n. In particular

$$\chi_M = \lambda^n + \lambda^{n+i_1-j_1+i_2-j_2-2} + \lambda^{n+i_1-j_1-1} + \lambda^{i_2-j_2-1} + 1.$$

Proof. The first two conditions ensure that M has exactly one additional non-zero entry in the upper and one in the lower triangle (not on the main diagonal). Since $j_1, j_2, i_2 \neq n$, we can expand along the last column and obtain

$$\chi_M = \det(S^\lambda_{n-1} + E_{i_1-1,j_1} + E_{i_2-1,j_2}) + \lambda \det(\lambda I_{n-1} + C_{x^{n-1}} + E_{i_1,j_1} + E_{i_2,j_2}).$$

For simplicity, we define $A := S^\lambda_{n-1} + E_{i_1-1,j_1} + E_{i_2-2,j_2}$ and $B := \lambda I_{n-1} + C_{x^{n-1}} + E_{i_1,j_1} + E_{i_2,j_2}$. In order to compute the latter part, we "push" the additional non-zero entry from the upper triangle to the top-right corner by first expanding $n-1-j_1$ times along the last column and then expanding $i_1 - 1$ times along the first row. The condition $i_2 \leq j_1$ ensures that E_{i_2,j_2} will not be eliminated from expanding along the last column and the condition $i_1 \leq j_2$ ensures that E_{i_2,j_2} will not be eliminated from expanding along the first row. Using Lemma 3, one obtains

$$\begin{aligned}\lambda \det(B) &= \lambda\lambda^{n-1-j_1}\lambda^{i_1-1}\det(\lambda I_{j_1-i_1+1} + C_{x^{j_1-i_1+1}+1} + E_{i_2-i_1+1,j_2-i_1+1})\\ &= \lambda^{n-1-j_1+i_1}(\lambda^{j_1-i_1+1} + \lambda^{i_2-i_1+1-j_2+i_1-1-1} + 1)\\ &= \lambda^n + \lambda^{n+i_1-j_1+i_2-j_2-2} + \lambda^{n+i_1-j_1-1}.\end{aligned}$$

For $\det(A)$, we proceed similar to case (iii) in Lemma 3. We first expand $j_2 - 1$ times along the first column in order to get the additional non-zero value from the lower triangle to the leftmost column. Because of the condition $i_1 \leq j_2$, this elimintates E_{i_1-1,j_1}. Now, one can expand $n - j_2 - (i_2 - j_2)$ times along the last row, until the remaining additional non-zero entry lies in the lower left corner of the remaining matrix. We finally expand along the first column one more time and obtain

$$\det(A) = \det(S^{\lambda}_{n-j_2} + E_{i_2-j_2,1}) = \det(S^{\lambda}_{i_2-j_2} + E_{i_2-j_2,1}) = \lambda^{i_2-j_2-1} + 1.$$

The last two assumptions make sure that all of the five coefficients of $\det(A) + \lambda \det(B)$ are distinct such that χ_M is indeed a pentanomial. □

B Minimal XOR-Counts in $\mathbb{F}_{2^n}$

Table 3. Minimal XOR-counts for all elements in $\mathbb{F}^*_{2^4}$.

Minimal polynomial m_α	Min $\mathrm{wt}_\oplus(\alpha)$	Matrix
$x+1$	0	I
x^2+x+1	2	$C_{m_\alpha} \oplus C_{m_\alpha}$
x^4+x+1	1	C_{m_α}
x^4+x^3+1	1	C_{m_α}
$x^4+x^3+x^2+x+1$	2	$C_{x^4+1} + E_{2,2} + E_{3,4}$

Table 4. Minimal XOR-counts for all elements in $\mathbb{F}^*_{2^5}$.

Minimal polynomial m_α	Min $\mathrm{wt}_\oplus(\alpha)$	Matrix
$x+1$	0	I
x^5+x^2+1	1	C_{m_α}
x^5+x^3+1	1	C_{m_α}
$x^5+x^3+x^2+x+1$	2	$C_{x^5+1} + E_{2,4} + E_{4,2}$
$x^5+x^4+x^2+x+1$	2	$C_{x^5+1} + E_{2,2} + E_{3,5}$
$x^5+x^4+x^3+x+1$	2	$C_{x^5+1} + E_{2,3} + E_{3,1} + E_{3,3}$
$x^5+x^4+x^3+x^2+1$	2	$C_{x^5+1} + E_{2,2} + E_{3,4}$

Table 5. Minimal XOR-counts for all elements in $\mathbb{F}_{2^6}^*$.

Minimal polynomial m_α	Min $\mathrm{wt}_\oplus(\alpha)$	Matrix
$x+1$	0	I
x^2+x+1	3	$C_{m_\alpha} \oplus C_{m_\alpha} \oplus C_{m_\alpha}$
x^3+x+1	2	$C_{m_\alpha} \oplus C_{m_\alpha}$
x^3+x^2+1	2	$C_{m_\alpha} \oplus C_{m_\alpha}$
x^6+x+1	1	C_{m_α}
x^6+x^3+1	1	C_{m_α}
$x^6+x^4+x^2+x+1$	2	$(C_{x^4+1} \oplus C_{x^2+1})(I + E_{1,5} + E_{5,4})$
$x^6+x^4+x^3+x+1$	2	$C_{x^6+1} + E_{2,3} + E_{4,6}$
x^6+x^5+1	1	C_{m_α}
$x^6+x^5+x^2+x+1$	2	$C_{x^6+1} + E_{2,2} + E_{3,6}$
$x^6+x^5+x^3+x^2+1$	2	$C_{x^6+1} + E_{2,2} + E_{3,5}$
$x^6+x^5+x^4+x+1$	2	$C_{x^6+1} + E_{2,3} + E_{3,1} + E_{3,3}$
$x^6+x^5+x^4+x^2+1$	2	$(C_{x^4+1} \oplus C_{x^2+1})(I + E_{1,5} + E_{6,1} + E_{6,5})$

Table 6. Minimal XOR-counts for all elements in $\mathbb{F}_{2^7}^*$.

Minimal polynomial m_α	Min $\mathrm{wt}_\oplus(\alpha)$	Matrix
$x+1$	0	I
x^7+x+1	1	C_{m_α}
x^7+x^3+1	1	C_{m_α}
$x^7+x^3+x^2+x+1$	2	$C_{x^7+1} + E_{2,6} + E_{4,2}$
x^7+x^4+1	1	C_{m_α}
$x^7+x^4+x^3+x^2+1$	2	$(C_{x^4+1} \oplus C_{x^3+1})(I + E_{1,5} + E_{5,3})$
$x^7+x^5+x^2+x+1$	2	$(C_{x^5+1} \oplus C_{x^2+1})(I + E_{1,6} + E_{6,5})$
$x^7+x^5+x^3+x+1$	2	$C_{x^7+1} + E_{2,3} + E_{4,7}$
$x^7+x^5+x^4+x^3+1$	2	$(C_{x^4+1} \oplus C_{x^3+1})(I + E_{1,5} + E_{7,2})$
$x^7+x^5+x^4+x^3+x^2+x+1$	3	$C_{x^7+1} + E_{2,3} + E_{4,6} + E_{4,7}$
x^7+x^6+1	1	C_{m_α}
$x^7+x^6+x^3+x+1$	2	$(C_{x^6+1} \oplus C_{x^1+1})(I + E_{1,7} + E_{7,4})$
$x^7+x^6+x^4+x+1$	2	$(C_{x^6+1} \oplus C_{x^1+1})(I + E_{1,7} + E_{7,3})$
$x^7+x^6+x^4+x^2+1$	2	$C_{x^7+1} + E_{2,4} + E_{4,1} + E_{4,4}$
$x^7+x^6+x^5+x^2+1$	2	$(C_{x^5+1} \oplus C_{x^2+1})(I + E_{1,6} + E_{7,1} + E_{7,6})$
$x^7+x^6+x^5+x^3+x^2+x+1$	3	$C_{x^7+1} + E_{2,2} + E_{2,3} + E_{4,7}$
$x^7+x^6+x^5+x^4+1$	2	$C_{x^7+1} + E_{2,2} + E_{3,4}$
$x^7+x^6+x^5+x^4+x^2+x+1$	3	$C_{x^7+1} + E_{2,2} + E_{3,4} + E_{3,7}$
$x^7+x^6+x^5+x^4+x^3+x^2+1$	3	$C_{x^7+1} + E_{2,2} + E_{2,3} + E_{4,6}$

Table 7. Minimal XOR-counts for all elements in $\mathbb{F}_{2^8}^*$.

Minimal polynomial m_α	Min $\mathrm{wt}_\oplus(\alpha)$	Matrix
$x+1$	0	I
x^2+x+1	4	$\bigoplus_{k=1}^{4} C_{m_\alpha}$
x^4+x+1	2	$C_{m_\alpha} \oplus C_{m_\alpha}$
x^4+x^3+1	2	$C_{m_\alpha} \oplus C_{m_\alpha}$
$x^4+x^3+x^2+x+1$	4	$\bigoplus_{k=1}^{2}(C_{x^4+1} + E_{2,2} + E_{3,4})$
$x^8+x^4+x^3+x+1$	2	$C_{x^8+1} + E_{2,6} + E_{4,2}$
$x^8+x^4+x^3+x^2+1$	3	C_{m_α}
$x^8+x^5+x^3+x+1$	2	$(C_{x^5+1} \oplus C_{x^3+1})(I + E_{1,6} + E_{6,5})$
$x^8+x^5+x^3+x^2+1$	2	$C_{x^8+1} + E_{2,6} + E_{5,2}$
$x^8+x^5+x^4+x^3+1$	2	$(C_{x^5+1} \oplus C_{x^3+1})(I + E_{1,6} + E_{6,2})$
$x^8+x^5+x^4+x^3+x^2+x+1$	3	$C_{x^8+1} + E_{2,5} + E_{2,7} + E_{4,2}$
$x^8+x^6+x^3+x^2+1$	2	$(C_{x^6+1} \oplus C_{x^2+1})(I + E_{1,7} + E_{8,5})$
$x^8+x^6+x^4+x^3+x^2+x+1$	3	$C_{x^8+1} + E_{2,3} + E_{4,7} + E_{4,8}$
$x^8+x^6+x^5+x+1$	2	$C_{x^8+1} + E_{2,4} + E_{4,2}$
$x^8+x^6+x^5+x^2+1$	2	$(C_{x^6+1} \oplus C_{x^2+1})(I + E_{1,7} + E_{7,2})$
$x^8+x^6+x^5+x^3+1$	2	$C_{x^8+1} + E_{2,3} + E_{4,6}$
$x^8+x^6+x^5+x^4+1$	3	C_{m_α}
$x^8+x^6+x^5+x^4+x^2+x+1$	3	$C_{x^8+1} + E_{2,3} + E_{2,4} + E_{5,8}$
$x^8+x^6+x^5+x^4+x^3+x+1$	3	$C_{x^8+1} + E_{2,3} + E_{2,5} + E_{6,8}$
$x^8+x^7+x^2+x+1$	2	$C_{x^8+1} + E_{2,2} + E_{3,8}$
$x^8+x^7+x^3+x+1$	2	$(C_{x^7+1} \oplus C_{x+1})(I + E_{1,8} + E_{8,5})$
$x^8+x^7+x^3+x^2+1$	2	$C_{x^8+1} + E_{2,2} + E_{3,7}$
$x^8+x^7+x^4+x^3+x^2+x+1$	3	$C_{x^8+1} + E_{2,2} + E_{3,6} + E_{3,8}$
$x^8+x^7+x^5+x+1$	2	$(C_{x^7+1} \oplus C_{x+1})(I + E_{1,8} + E_{8,3})$
$x^8+x^7+x^5+x^3+1$	2	$(C_{x^5+1} \oplus C_{x^3+1})(I + E_{1,6} + E_{8,1} + E_{8,6})$
$x^8+x^7+x^5+x^4+1$	2	$C_{x^8+1} + E_{2,2} + E_{3,5}$
$x^8+x^7+x^5+x^4+x^3+x^2+1$	3	$C_{x^8+1} + E_{2,2} + E_{3,5} + E_{3,7}$
$x^8+x^7+x^6+x+1$	2	$C_{x^8+1} + E_{2,3} + E_{3,1} + E_{3,3}$
$x^8+x^7+x^6+x^3+x^2+x+1$	3	$C_{x^8+1} + E_{2,2} + E_{2,3} + E_{4,8}$
$x^8+x^7+x^6+x^4+x^2+x+1$	3	$(C_{x^6+1} \oplus C_{x^2+1})(I + E_{1,7} + E_{7,3} + E_{7,8})$
$x^8+x^7+x^6+x^4+x^3+x^2+1$	3	$C_{x^8+1} + E_{2,2} + E_{2,3} + E_{4,7}$
$x^8+x^7+x^6+x^5+x^2+x+1$	3	$C_{x^8+1} + E_{2,2} + E_{3,4} + E_{3,8}$
$x^8+x^7+x^6+x^5+x^4+x+1$	3	$C_{x^8+1} + E_{2,3} + E_{3,1} + E_{3,3} + E_{8,3}$
$x^8+x^7+x^6+x^5+x^4+x^2+1$	3	$C_{x^8+1} + E_{2,2} + E_{2,5} + E_{6,7}$
$x^8+x^7+x^6+x^5+x^4+x^3+1$	3	$C_{x^8+1} + E_{2,2} + E_{2,3} + E_{4,6}$

Table 8. For each $n \leq 2048$ for which no irreducible trinomial of degree n exists, this table presents a matrix of the form $C_{x^n+1}+E_{i_1,j_1}+E_{i_2,j_2}$ with irreducible characteristic pentanomial. Such a matrix is represented as a 4-tuple (i_1, j_1, i_2, j_2). In all cases, the characteristic polynomial is equal to $\lambda^n+\lambda^{n+i_1-j_1+i_2-j_2-2}+\lambda^{n+i_1-j_1-1}+\lambda^{i_2-j_2-1}+1$.

n		n		n		n		n		n		n		n	
8	(1,3,3,1)	237	(1,168,3,1)	451	(1,104,3,1)	659	(1,250,3,1)	869	(1,128,3,1)	1067	(1,960,5,1)	1274	(1,1176,3,1)	1480	(1,413,3,1)	1680	(1,645,3,1)	1867	(1,670,3,1)
13	(1,4,3,1)	240	(1,121,4,1)	452	(1,90,3,1)	661	(1,224,3,1)	872	(1,405,3,1)	1068	(1,54,3,1)	1275	(1,1265,3,1)	1483	(1,412,3,1)	1682	(1,5,3,1)	1868	(1,420,3,1)
16	(1,9,4,1)	243	(1,38,3,1)	453	(1,302,3,1)	664	(1,149,3,1)	874	(1,83,3,1)	1069	(1,338,3,1)	1277	(1,230,3,1)	1484	(1,41,3,1)	1683	(1,1278,3,1)	1869	(1,384,3,1)
19	(1,8,3,1)	245	(1,38,3,1)	454	(1,314,3,1)	666	(1,117,3,1)	875	(1,386,3,1)	1070	(1,228,3,1)	1280	(1,81,3,1)	1485	(1,1086,3,1)	1684	(1,730,3,1)	1872	(1,183,3,1)
24	(1,5,3,1)	246	(1,71,3,1)	456	(1,129,3,1)	667	(1,38,4,1)	877	(1,248,5,1)	1072	(1,789,4,1)	1283	(1,344,3,1)	1488	(1,1017,3,1)	1685	(1,816,3,1)	1874	(1,35,4,1)
26	(1,11,3,1)	248	(1,29,3,1)	459	(1,270,3,1)	669	(1,48,3,1)	878	(1,3,3,1)	1073	(1,362,3,1)	1285	(1,1174,3,1)	1491	(1,666,3,1)	1686	(1,72,3,1)	1875	(1,1386,3,1)
27	(1,3,3,1)	251	(1,24,3,1)	461	(1,170,3,1)	672	(1,567,3,1)	880	(1,11,3,1)	1074	(1,801,3,1)	1288	(1,379,3,1)	1493	(1,1002,3,1)	1688	(1,255,3,1)	1876	(1,1204,3,1)
32	(1,3,3,1)	254	(1,19,3,1)	464	(1,55,3,1)	674	(1,307,4,1)	883	(1,589,3,1)	1075	(1,142,3,1)	1290	(1,149,3,1)	1494	(1,620,3,1)	1690	(1,733,3,1)	1877	(1,628,3,1)
37	(1,16,4,1)	256	(1,157,3,1)	466	(1,451,3,1)	675	(1,225,3,1)	885	(1,512,3,1)	1076	(1,49,3,1)	1291	(1,302,3,1)	1496	(1,21,3,1)	1691	(1,26,3,1)	1880	(1,207,3,1)
38	(1,4,3,1)	259	(1,20,3,1)	467	(1,72,3,1)	677	(1,647,3,1)	886	(1,10,3,1)	1077	(1,706,4,1)	1292	(1,473,3,1)	1498	(1,223,3,1)	1693	(1,394,3,1)	1882	(1,399,4,1)
40	(1,14,3,1)	261	(1,12,3,1)	469	(1,188,3,1)	678	(1,312,3,1)	888	(1,501,3,1)	1080	(1,75,3,1)	1293	(1,212,3,1)	1499	(1,3,3,1)	1696	(1,19,3,1)	1883	(1,680,3,1)
43	(1,8,3,1)	262	(1,13,3,1)	472	(1,385,3,1)	680	(1,21,3,1)	891	(1,12,3,1)	1083	(1,92,3,1)	1296	(1,257,3,1)	1501	(1,1222,3,1)	1699	(1,404,3,1)	1885	(1,352,3,1)
45	(1,6,3,1)	264	(1,63,3,1)	475	(1,94,3,1)	681	(1,51,3,1)	893	(1,827,4,1)	1088	(1,3,3,1)	1299	(1,144,3,1)	1502	(1,5,3,1)	1701	(1,540,3,1)	1888	(1,905,3,1)
48	(1,21,3,1)	267	(1,182,3,1)	477	(1,286,4,1)	683	(1,104,3,1)	896	(1,87,3,1)	1091	(1,1026,3,1)	1301	(1,160,3,1)	1504	(1,559,3,1)	1702	(1,262,3,1)	1891	(1,280,3,1)
50	(1,7,3,1)	269	(1,64,3,1)	480	(1,273,5,1)	685	(1,172,3,1)	899	(1,64,3,1)	1093	(1,310,3,1)	1303	(1,380,3,1)	1506	(1,215,3,1)	1704	(1,1617,4,1)	1892	(1,440,3,1)
51	(1,12,3,1)	272	(1,165,3,1)	482	(1,115,3,1)	688	(1,149,3,1)	901	(1,504,4,1)	1096	(1,947,3,1)	1304	(1,391,3,1)	1507	(1,200,3,1)	1706	(1,843,3,1)	1893	(1,344,3,1)
53	(1,4,3,1)	275	(1,20,3,1)	483	(1,26,3,1)	691	(1,606,7,1)	904	(1,241,5,1)	1099	(1,644,3,1)	1307	(1,1200,3,1)	1509	(1,128,5,1)	1707	(1,150,3,1)	1894	(1,391,3,1)
56	(1,13,3,1)	277	(1,208,3,1)	485	(1,158,3,1)	693	(1,278,3,1)	907	(1,142,3,1)	1101	(1,474,3,1)	1309	(1,26,3,1)	1512	(1,381,3,1)	1709	(1,688,3,1)	1896	(1,1053,4,1)
59	(1,14,3,1)	280	(1,73,3,1)	488	(1,359,3,1)	696	(1,77,3,1)	909	(1,480,3,1)	1104	(1,515,3,1)	1312	(1,901,3,1)	1515	(1,14,3,1)	1712	(1,95,3,1)	1897	(1,80,3,1)
61	(1,4,3,1)	283	(1,154,3,1)	491	(1,477,3,1)	699	(1,360,3,1)	910	(1,8,3,1)	1107	(1,936,3,1)	1315	(1,508,3,1)	1517	(1,698,3,1)	1714	(1,1021,3,1)	1898	(1,241,3,1)
64	(1,61,3,1)	285	(1,158,3,1)	493	(1,20,3,1)	701	(1,238,3,1)	912	(1,627,3,1)	1109	(1,278,3,1)	1316	(1,204,3,1)	1520	(1,131,3,1)	1715	(1,250,3,1)	1899	(1,986,3,1)
67	(1,58,3,1)	288	(1,206,3,1)	496	(1,149,3,1)	703	(1,19,3,1)	914	(1,81,3,1)	1112	(1,35,3,1)	1317	(1,820,4,1)	1522	(1,985,3,1)	1717	(1,142,3,1)	1901	(1,230,3,1)
69	(1,42,4,1)	290	(1,96,3,1)	499	(1,40,3,1)	704	(1,195,5,1)	915	(1,320,3,1)	1114	(1,143,3,1)	1318	(1,109,3,1)	1523	(1,906,3,1)	1718	(1,242,3,1)	1904	(1,535,3,1)
70	(1,19,3,1)	291	(1,200,3,1)	501	(1,144,4,1)	706	(1,503,3,1)	917	(1,572,3,1)	1115	(1,328,3,1)	1320	(1,167,3,1)	1525	(1,602,3,1)	1720	(1,133,3,1)	1907	(1,780,3,1)
72	(1,15,5,1)	293	(1,16,3,1)	502	(1,245,3,1)	707	(1,376,3,1)	920	(1,535,3,1)	1117	(1,220,3,1)	1322	(1,405,3,1)	1528	(1,79,3,1)	1723	(1,322,3,1)	1909	(1,46,3,1)
75	(1,36,3,1)	296	(1,109,3,1)	504	(1,141,3,1)	709	(1,230,3,1)	922	(1,299,4,1)	1118	(1,168,3,1)	1323	(1,272,3,1)	1531	(1,910,3,1)	1725	(1,90,3,1)	1910	(1,266,3,1)
77	(1,47,3,1)	298	(1,55,3,1)	507	(1,429,6,1)	710	(1,17,3,1)	923	(1,52,4,1)	1120	(1,1043,3,1)	1325	(1,22,3,1)	1532	(1,66,3,1)	1727	(1,207,3,1)	1912	(1,157,3,1)
78	(1,23,3,1)	299	(1,116,3,1)	509	(1,10,3,1)	712	(1,455,3,1)	925	(1,859,3,1)	1123	(1,410,3,1)	1328	(1,917,3,1)	1533	(1,1160,3,1)	1728	(1,1227,3,1)	1914	(1,639,4,1)
80	(1,5,3,1)	301	(1,164,3,1)	510	(1,425,3,1)	713	(1,110,3,1)	928	(1,537,4,1)	1124	(1,424,3,1)	1330	(1,187,3,1)	1536	(1,39,3,1)	1730	(1,443,3,1)	1915	(1,40,3,1)
82	(1,47,5,1)	304	(1,109,3,1)	515	(1,236,3,1)	717	(1,448,4,1)	929	(1,51,3,1)	1125	(1,254,3,1)	1331	(1,978,3,1)	1538	(1,509,3,1)	1731	(1,338,3,1)	1916	(1,663,3,1)
83	(1,4,3,1)	306	(1,81,3,1)	517	(1,172,3,1)	720	(1,369,4,1)	931	(1,544,3,1)	1128	(1,21,3,1)	1333	(1,530,3,1)	1539	(1,30,3,1)	1732	(1,1250,3,1)	1917	(1,1026,3,1)
85	(1,16,3,1)	307	(1,192,4,1)	520	(1,331,3,1)	723	(1,414,3,1)	933	(1,264,3,1)	1131	(1,552,3,1)	1336	(1,97,3,1)	1541	(1,698,3,1)	1733	(1,128,3,1)	1920	(1,39,3,1)
88	(1,11,3,1)	309	(1,155,3,1)	523	(1,140,3,1)	725	(1,68,3,1)	934	(1,424,4,1)	1132	(1,52,3,1)	1339	(1,820,3,1)	1544	(1,411,3,1)	1736	(1,493,3,1)	1922	(1,497,3,1)
91	(1,8,3,1)	311	(1,25,3,1)	525	(1,328,4,1)	728	(1,393,3,1)	936	(1,23,3,1)	1133	(1,238,3,1)	1341	(1,732,3,1)	1546	(1,351,4,1)	1739	(1,420,3,1)	1923	(1,326,3,1)
96	(1,9,3,1)	312	(1,7,5,1)	528	(1,35,3,1)	731	(1,80,3,1)	939	(1,288,3,1)	1136	(1,957,3,1)	1342	(1,610,3,1)	1547	(1,62,3,1)	1741	(1,476,3,1)	1925	(1,210,3,1)
99	(1,78,3,1)	315	(1,50,3,1)	530	(1,17,3,1)	733	(1,310,3,1)	940	(1,8,3,1)	1139	(1,246,3,1)	1344	(1,185,3,1)	1549	(1,1220,3,1)	1744	(1,1183,3,1)	1928	(1,83,3,1)
101	(1,20,3,1)	317	(1,90,3,1)	531	(1,44,3,1)	734	(1,56,3,1)	941	(1,382,3,1)	1141	(1,196,3,1)	1346	(1,57,3,1)	1552	(1,325,3,1)	1747	(1,1402,3,1)	1930	(1,569,4,1)
104	(1,94,3,1)	320	(1,53,3,1)	533	(1,56,3,1)	736	(1,271,5,1)	944	(1,191,3,1)	1143	(1,191,3,1)	1347	(1,18,3,1)	1555	(1,404,3,1)	1749	(1,56,3,1)	1931	(1,3,3,1)
107	(1,44,4,1)	323	(1,120,3,1)	535	(1,104,3,1)	739	(1,286,3,1)	946	(1,469,3,1)	1144	(1,335,3,1)	1349	(1,138,5,1)	1557	(1,822,3,1)	1752	(1,1585,4,1)	1933	(1,940,3,1)
109	(1,20,3,1)	325	(1,244,3,1)	536	(1,117,3,1)	741	(1,18,3,1)	947	(1,16,3,1)	1147	(1,598,3,1)	1352	(1,595,3,1)	1560	(1,1027,5,1)	1754	(1,103,3,1)	1936	(1,1657,3,1)
112	(1,91,3,1)	326	(1,27,3,1)	539	(1,3,3,1)	744	(1,635,3,1)	949	(1,550,4,1)	1149	(1,902,5,1)	1355	(1,216,3,1)	1563	(1,198,3,1)	1755	(1,308,3,1)	1939	(1,110,3,1)
114	(1,33,3,1)	328	(1,237,4,1)	541	(1,364,5,1)	747	(1,548,3,1)	950	(1,154,3,1)	1150	(1,130,3,1)	1357	(1,302,5,1)	1565	(1,66,3,1)	1757	(1,988,3,1)	1941	(1,1262,3,1)
115	(1,32,3,1)	331	(1,8,3,1)	542	(1,50,3,1)	749	(1,316,3,1)	952	(1,573,4,1)	1152	(1,11,3,1)	1360	(1,485,3,1)	1568	(1,231,3,1)	1758	(1,213,3,1)	1942	(1,76,3,1)
116	(1,20,3,1)	334	(1,64,3,1)	544	(1,65,5,1)	752	(1,117,3,1)	955	(1,80,3,1)	1155	(1,8,3,1)	1363	(1,1018,3,1)	1571	(1,430,3,1)	1760	(1,273,3,1)	1944	(1,429,3,1)
117	(1,99,4,1)	335	(1,20,3,1)	546	(1,213,3,1)	755	(1,230,3,1)	957	(1,372,3,1)	1157	(1,328,3,1)	1365	(1,488,3,1)	1573	(1,112,3,1)	1761	(1,186,3,1)	1947	(1,216,3,1)
120	(1,15,3,1)	336	(1,35,3,1)	547	(1,302,4,1)	757	(1,751,3,1)	958	(1,80,3,1)	1160	(1,87,3,1)	1368	(1,533,3,1)	1574	(1,284,3,1)	1762	(1,277,3,1)	1949	(1,686,3,1)
122	(1,60,3,1)	338	(1,15,3,1)	548	(1,18,3,1)	760	(1,187,3,1)	960	(1,765,3,1)	1162	(1,451,3,1)	1370	(1,35,3,1)	1576	(1,131,3,1)	1763	(1,266,3,1)	1952	(1,205,3,1)
125	(1,18,3,1)	339	(1,20,3,1)	549	(1,304,4,1)	763	(1,334,3,1)	962	(1,213,3,1)	1163	(1,162,3,1)	1371	(1,528,3,1)	1579	(1,706,3,1)	1765	(1,458,3,1)	1954	(1,714,4,1)
128	(1,61,3,1)	341	(1,278,3,1)	552	(1,195,3,1)	764	(1,40,3,1)	963	(1,38,3,1)	1165	(1,32,3,1)	1373	(1,154,3,1)	1581	(1,1446,3,1)	1766	(1,423,3,1)	1955	(1,1256,4,1)
131	(1,36,3,1)	344	(1,85,3,1)	554	(1,191,3,1)	765	(1,216,3,1)	965	(1,88,3,1)	1168	(1,629,3,1)	1376	(1,151,3,1)	1584	(1,621,3,1)	1768	(1,157,3,1)	1957	(1,1486,3,1)
133	(1,28,3,1)	347	(1,10,3,1)	555	(1,10,4,1)	766	(1,161,3,1)	968	(1,319,3,1)	1171	(1,466,3,1)	1378	(1,611,4,1)	1587	(1,250,7,1)	1771	(1,518,3,1)	1960	(1,31,3,1)
136	(1,11,3,1)	349	(1,58,3,1)	557	(1,318,3,1)	768	(1,117,3,1)	970	(1,415,3,1)	1172	(1,288,3,1)	1379	(1,306,3,1)	1589	(1,128,7,1)	1773	(1,1352,3,1)	1963	(1,1504,3,1)
138	(1,53,3,1)	352	(1,125,3,1)	560	(1,25,3,1)	770	(1,547,3,1)	971	(1,346,3,1)	1173	(1,108,3,1)	1381	(1,1276,3,1)	1592	(1,1135,3,1)	1776	(1,469,3,1)	1965	(1,752,3,1)
139	(1,8,5,1)	355	(1,164,3,1)	562	(1,25,3,1)	771	(1,138,3,1)	973	(1,56,3,1)	1176	(1,57,3,1)	1382	(1,270,3,1)	1594	(1,821,3,1)	1779	(1,1046,3,1)	1968	(1,9,3,1)
141	(1,47,3,1)	356	(1,10,3,1)	563	(1,60,3,1)	773	(1,138,3,1)	974	(1,30,3,1)	1179	(1,56,3,1)	1384	(1,221,3,1)	1595	(1,192,3,1)	1781	(1,36,3,1)	1970	(1,649,3,1)
143	(1,19,3,1)	357	(1,266,3,1)	565	(1,178,3,1)	776	(1,569,3,1)	976	(1,715,3,1)	1181	(1,650,4,1)	1387	(1,140,3,1)	1597	(1,1150,3,1)	1784	(1,1481,3,1)	1971	(1,6,3,1)
144	(1,39,3,1)	360	(1,5,3,1)	568	(1,373,3,1)	779	(1,538,3,1)	978	(1,311,3,1)	1183	(1,701,3,1)	1389	(1,204,3,1)	1598	(1,289,3,1)	1786	(1,289,3,1)	1972	(1,849,3,1)
149	(1,40,3,1)	361	(1,25,3,1)	571	(1,10,4,1)	781	(1,278,3,1)	980	(1,369,3,1)	1187	(1,530,3,1)	1392	(1,1283,3,1)	1600	(1,529,3,1)	1787	(1,112,4,1)	1973	(1,1918,3,1)
152	(1,3,3,1)	363	(1,258,3,1)	572	(1,35,3,1)	784	(1,169,3,1)	981	(1,42,3,1)	1189	(1,136,3,1)	1394	(1,371,3,1)	1603	(1,134,3,1)	1789	(1,578,3,1)	1976	(1,361,3,1)
157	(1,50,3,1)	365	(1,294,3,1)	573	(1,6,3,1)	786	(1,387,3,1)	984	(1,917,5,1)	1192	(1,397,3,1)	1395	(1,380,3,1)	1605	(1,1328,5,1)	1792	(1,1001,4,1)	1978	(1,289,3,1)
158	(1,12,3,1)	368	(1,25,3,1)	576	(1,3,3,1)	787	(1,52,3,1)	987	(1,308,3,1)	1194	(1,153,3,1)	1397	(1,128,3,1)	1608	(1,273,3,1)	1794	(1,27,3,1)	1979	(1,1849,4,1)
160	(1,91,3,1)	371	(1,20,3,1)	578	(1,507,3,1)	788	(1,26,3,1)	989	(1,138,3,1)	1195	(1,962,3,1)	1400	(1,489,3,1)	1610	(1,561,3,1)	1795	(1,130,3,1)	1981	(1,1930,3,1)
163	(1,104,3,1)	373	(1,34,3,1)	579	(1,114,3,1)	789	(1,294,3,1)	992	(1,33,3,1)	1197	(1,12,3,1)	1403	(1,3,3,1)	1611	(1,506,3,1)	1796	(1,48,3,1)	1982	(1,260,3,1)
164	(1,18,3,1)	374	(1,38,3,1)	581	(1,318,3,1)	790	(1,269,3,1)	995	(1,558,5,1)	1200	(1,179,3,1)	1405	(1,658,3,1)	1613	(1,892,4,1)	1797	(1,8,3,1)	1984	(1,739,3,1)
166	(1,135,3,1)	376	(1,113,3,1)	584	(1,63,3,1)	792	(1,131,3,1)	997	(1,76,3,1)	1202	(1,788,5,1)	1406	(1,97,3,1)	1614	(1,138,3,1)	1800	(1,829,3,1)	1987	(1,196,3,1)
168	(1,21,3,1)	379	(1,8,3,1)	586	(1,469,3,1)	795	(1,450,3,1)	1000	(1,101,3,1)	1205	(1,590,5,1)	1408	(1,817,3,1)	1616	(1,801,3,1)	1803	(1,1158,3,1)	1989	(1,232,5,1)
171	(1,60,3,1)	381	(1,198,4,1)	587	(1,256,3,1)	796	(1,26,3,1)	1002	(1,225,3,1)	1208	(1,319,3,1)	1411	(1,634,3,1)	1619	(1,578,3,1)	1805	(1,1312,3,1)	1992	(1,177,3,1)
173	(1,32,3,1)	384	(1,195,3,1)	589	(1,70,3,1)	797	(1,336,3,1)	1003	(1,716,3,1)	1211	(1,686,3,1)	1413	(1,880,4,1)	1621	(1,852,4,1)	1808	(1,545,3,1)	1995	(1,710,3,1)
176	(1,19,3,1)	387	(1,102,3,1)	591	(1,95,3,1)	800	(1,523,3,1)	1004	(1,106,3,1)	1213	(1,664,3,1)	1416	(1,461,3,1)	1622	(1,158,3,1)	1811	(1,618,3,1)	1997	(1,366,3,1)
179	(1,10,3,1)	389	(1,38,3,1)	592	(1,241,3,1)	802	(1,47,4,1)	1005	(1,692,3,1)	1216	(1,709,3,1)	1418	(1,149,3,1)	1624	(1,1375,3,1)	1812	(1,702,3,1)	1998	(1,155,3,1)
181	(1,175,3,1)	392	(1,47,3,1)	595	(1,364,3,1)	803	(1,60,3,1)	1006	(1,40,3,1)	1219	(1,676,4,1)	1419	(1,324,3,1)	1626	(1,573,3,1)	1813	(1,14,3,1)	2000	(1,333,3,1)
184	(1,83,3,1)	395	(1,126,3,1)	597	(1,540,3,1)	805	(1,248,3,1)	1008	(1,521,3,1)	1221	(1,200,3,1)	1421	(1,496,3,1)	1627	(1,130,3,1)	1816	(1,83,3,1)	2002	(1,5,3,1)
187	(1,22,3,1)	397	(1,206,3,1)	598	(1,248,3,1)	808	(1,379,3,1)	1011	(1,330,3,1)	1222	(1,181,3,1)	1424	(1,323,3,1)	1629	(1,500,3,1)	1819	(1,926,3,1)	2003	(1,710,3,1)
188	(1,21,3,1)	398	(1,104,3,1)	600	(1,87,3,1)	811	(1,394,3,1)	1013	(1,296,3,1)	1224	(1,545,3,1)	1427	(1,1310,3,1)	1632	(1,791,3,1)	1821	(1,668,3,1)	2005	(1,1074,4,1)
189	(1,63,3,1)	400	(1,283,3,1)	603	(1,453,3,1)	813	(1,98,3,1)	1016	(1,131,3,1)	1227	(1,212,3,1)	1429	(1,400,3,1)	1635	(1,545,3,1)	1822	(1,856,3,1)	2008	(1,445,3,1)
190	(1,16,3,1)	403	(1,124,3,1)	605	(1,248,3,1)	816	(1,285,3,1)	1017	(1,261,3,1)	1229	(1,40,3,1)	1432	(1,1241,3,1)	1637	(1,90,3,1)	1824	(1,1125,4,1)	2011	(1,922,3,1)
192	(1,15,3,1)	405	(1,68,5,1)	608	(1,73,3,1)	819	(1,496,4,1)	1018	(1,937,3,1)	1232	(1,477,3,1)	1433	(1,484,3,1)	1640	(1,401,3,1)	1826	(1,335,3,1)	2012	(1,40,3,1)
195	(1,158,3,1)	408	(1,27,3,1)	611	(1,334,3,1)	821	(1,424,3,1)	1019	(1,3,3,1)	1235	(1,50,3,1)	1437	(1,380,3,1)	1643	(1,3,3,1)	1827	(1,1308,3,1)	2013	(1,108,3,1)
197	(1,126,3,1)	410	(1,117,3,1)	613	(1,368,4,1)	824	(1,233,3,1)	1021	(1,832,3,1)	1237	(1,380,3,1)	1439	(1,300,3,1)	1644	(1,221,3,1)	1829	(1,760,3,1)	2014	(1,170,3,1)
200	(1,53,3,1)	411	(1,108,7,1)	616	(1,597,4,1)	827	(1,680,3,1)	1024	(1,643,3,1)	1240	(1,826,3,1)	1440	(1,901,4,1)	1645	(1,176,3,1)	1832	(1,295,3,1)	2016	(1,645,3,1)
203	(1,3,3,1)	413	(1,36,3,1)	619	(1,118,3,1)	829	(1,560,3,1)	1027	(1,830,3,1)	1243	(1,34,3,1)	1443	(1,348,3,1)	1646	(1,68,3,1)	1834	(1,829,3,1)	2018	(1,178,3,1)
205	(1,176,3,1)	416	(1,87,3,1)	621	(1,344,3,1)	830	(1,60,3,1)	1032	(1,541,4,1)	1244	(1,46,3,1)	1445	(1,68,3,1)	1648	(1,1249,3,1)	1835	(1,1352,3,1)	2019	(1,1506,3,1)
206	(1,7,3,1)	419	(1,40,5,1)	624	(1,609,3,1)	832	(1,685,3,1)	1035	(1,208,5,1)	1245	(1,360,3,1)	1448	(1,93,3,1)	1651	(1,490,3,1)	1837	(1,1162,4,1)	2021	(1,102,3,1)
208	(1,197,4,1)	421	(1,20,7,1)	627	(1,377,3,1)	835	(1,92,3,1)	1037	(1,758,3,1)	1248	(1,327,3,1)	1450	(1,1183,3,1)	1653	(1,834,3,1)	1840	(1,409,3,1)	2024	(1,1949,4,1)
211	(1,113,3,1)	424	(1,359,3,1)	629	(1,268,3,1)	836	(1,8,3,1)	1040	(1,708,3,1)	1250	(1,313,3,1)	1451	(1,22,3,1)	1654	(1,1000,3,1)	1842	(1,305,3,1)	2027	(1,1980,3,1)
213	(1,24,3,1)	427	(1,22,3,1)	630	(1,80,3,1)	837	(1,542,3,1)	1040	(1,311,3,1)	1251	(1,38,3,1)	1453	(1,146,3,1)	1656	(1,179,3,1)	1843	(1,904,3,1)	2029	(1,4,3,1)
216	(1,11,3,1)	429	(1,18,3,1)	632	(1,117,3,1)	840	(1,173,3,1)	1043	(1,304,3,1)	1253	(1,318,3,1)	1456	(1,29,3,1)	1658	(1,801,3,1)	1845	(1,786,3,1)	2030	(1,337,3,1)
219	(1,201,3,1)	430	(1,49,3,1)	635	(1,60,3,1)	843	(1,200,3,1)	1045	(1,298,3,1)	1254	(1,56,3,1)	1459	(1,496,3,1)	1659	(1,446,3,1)	1848	(1,1077,3,1)	2032	(1,1479,5,1)
221	(1,80,3,1)	432	(1,117,5,1)	637	(1,386,6,1)	848	(1,243,3,1)	1046	(1,38,3,1)	1256	(1,605,3,1)	1461	(1,122,3,1)	1661	(1,156,3,1)	1850	(1,1015,4,1)	2035	(1,442,3,1)
222	(1,7,3,1)	434	(1,119,3,1)	638	(1,3,3,1)	851	(1,58,3,1)	1048	(1,539,3,1)	1258	(1,689,3,1)	1462	(1,913,3,1)	1662	(1,285,3,1)	1851	(1,720,3,1)	2037	(1,210,3,1)
224	(1,83,3,1)	435	(1,122,3,1)	640	(1,35,3,1)	853	(1,142,3,1)	1051	(1,12,4,1)	1259	(1,168,3,1)	1464	(1,1155,3,1)	1664	(1,135,3,1)	1852	(1,46,3,1)	2038	(1,1498,3,1)
226	(1,169,3,1)	437	(1,318,3,1)	643	(1,412,4,1)	854	(1,138,3,1)	1053	(1,1044,3,1)	1261	(1,640,3,1)	1467	(1,782,3,1)	1667	(1,1146,3,1)	1853	(1,906,3,1)	2040	(1,77,3,1)
227	(1,182,3,1)	440	(1,297,3,1)	644	(1,236,3,1)	856	(1,691,3,1)	1056	(1,891,3,1)	1262	(1,285,3,1)	1469	(1,164,4,1)	1669	(1,106,3,1)	1856	(1,861,3,1)	2042	(1,417,3,1)
229	(1,80,3,1)	442	(1,187,4,1)	645	(1,50,3,1)	859	(1,178,3,1)	1059	(1,260,3,1)	1264	(1,283,3,1)	1472	(1,83,3,1)	1670	(1,472,3,1)	1858	(1,1099,3,1)	2043	(1,398,3,1)
230	(1,3,3,1)	443	(1,48,3,1)	648	(1,626,3,1)	863	(1,92,3,1)	1061	(1,268,3,1)	1267	(1,800,4,1)	1474	(1,829,3,1)	1672	(1,881,4,1)	1859	(1,4,3,1)	2045	(1,1554,3,1)
232	(1,133,3,1)	445	(1,88,3,1)	653	(1,478,3,1)	864	(1,39,3,1)	1064	(1,351,3,1)	1269	(1,907,4,1)	1475	(1,68,3,1)	1675	(1,970,4,1)	1861	(1,398,3,1)	2046	(1,240,3,1)
235	(1,26,3,1)	448	(1,119,3,1)	656	(1,295,3,1)	867	(1,48,3,1)	1066	(1,401,3,1)	1272	(1,383,3,1)	1477	(1,140,3,1)	1677	(1,852,3,1)	1864	(1,61,3,1)	2048	(1,83,3,1)

References

1. Albrecht, M.R., Driessen, B., Kavun, E.B., Leander, G., Paar, C., Yalçın, T.: Block ciphers – focus on the linear layer (feat. PRIDE). In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014, Part I. LNCS, vol. 8616, pp. 57–76. Springer, Heidelberg (2014)
2. Augot, D., Finiasz, M.: Direct construction of recursive MDS diffusion layers using shortened BCH codes. In: Cid, C., Rechberger, C. (eds.) FSE 2014. LNCS, vol. 8540, pp. 3–17. Springer, Heidelberg (2015)
3. Barreto, P., Nikov, V., Nikova, S., Rijmen, V., Tischhauser, E.: Whirlwind: a new cryptographic hash function. Des. Codes Crypt. **56**(2–3), 141–162 (2010)
4. Bertoni, G., Daemen, J., Peeters, M., Assche, G.: The Keccak reference. Submission to NIST (Round 3) (2011)
5. Biham, E., Anderson, R., Knudsen, L.R.: Serpent: a new block cipher proposal. In: Vaudenay, S. (ed.) FSE 1998. LNCS, vol. 1372, p. 222. Springer, Heidelberg (1998)
6. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. In: Menezes, A., Vanstone, S.A. (eds.) CRYPTO 1990. LNCS, vol. 537, pp. 2–21. Springer, Heidelberg (1991)
7. Daemen, J.: Cipher and hash function design strategies based on linear and differential cryptanalysis. Ph.D. thesis, Doctoral Dissertation, KU Leuven, March 1995
8. Daemen, J., Knudsen, L.R., Rijmen, V.: The block cipher SQUARE. In: Biham, E. (ed.) FSE 1997. LNCS, vol. 1267, pp. 149–165. Springer, Heidelberg (1997)
9. Daemen, J., Rijmen, V.: AES Proposal: Rijndael (1998). http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf
10. Daemen, J., Rijmen, V.: Correlation analysis in $GF(2^n)$. In: Advanced Linear Cryptanalysis of Block and Stream Ciphers. Cryptology and Information Security, pp. 115–131 (2011)
11. Dummit, D.S., Foote, R.M.: Abstract Algebra. Wiley, Hoboken (2004)
12. Grosso, V., Leurent, G., Standaert, F.-X., Varici, K.: LS-designs: bitslice encryption for efficient masked software implementations. In: Cid, C., Rechberger, C. (eds.) FSE 2014. LNCS, vol. 8540, pp. 18–37. Springer, Heidelberg (2015)
13. Guo, J., Peyrin, T., Poschmann, A.: The PHOTON family of lightweight hash functions. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 222–239. Springer, Heidelberg (2011)
14. Guo, J., Peyrin, T., Poschmann, A., Robshaw, M.: The LED block cipher. In: Preneel, B., Takagi, T. (eds.) CHES 2011. LNCS, vol. 6917, pp. 326–341. Springer, Heidelberg (2011)
15. Gupta, K.C., Ray, I.G.: Cryptographically significant MDS matrices based on circulant and circulant-like matrices for lightweight applications. Crypt. Commun. **7**(2), 257–287 (2015)
16. Jean, J., Peyrin, T., Sim, S.M.: Minimal implementations of linear and non-linear lightweight building blocks. Personal communication (2015)
17. Khoo, K., Peyrin, T., Poschmann, A.Y., Yap, H.: FOAM: searching for hardware-optimal SPN structures and components with a fair comparison. In: Batina, L., Robshaw, M. (eds.) CHES 2014. LNCS, vol. 8731, pp. 433–450. Springer, Heidelberg (2014)
18. Knapp, A.W.: Basic Algebra. Birkhäuser, Boston (2006)
19. Li, Y., Wang, M.: On the construction of lightweight circulant involutory MDS matrices. In: Fast Software Encryption (FSE), LNCS. Springer, Heidelberg (2016, to appear)

20. Lidl, R., Niederreiter, H.: Introduction to Finite Fields and Their Applications. Cambridge University Press, Cambridge (1994)
21. Liu, M., Sim, S.M.: Lightweight MDS generalized circulant matrices. In: Fast Software Encryption (FSE). LNCS. Springer, Heidelberg (2016, to appear)
22. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North-Holland Publishing Company, Amsterdam (1977)
23. Matsui, M.: Linear cryptanalysis method for DES cipher. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 386–397. Springer, Heidelberg (1994)
24. Sajadieh, M., Dakhilalian, M., Mala, H., Sepehrdad, P.: Recursive diffusion layers for block ciphers and hash functions. In: Canteaut, A. (ed.) FSE 2012. LNCS, vol. 7549, pp. 385–401. Springer, Heidelberg (2012)
25. Sarkar, S., Sim, S.M.: A deeper understanding of the XOR count distribution in the context of lightweight cryptography. In: Pointcheval, D., et al. (eds.) AFRICACRYPT 2016. LNCS, vol. 9646, pp. 167–182. Springer, Heidelberg (2016). doi:10.1007/978-3-319-31517-1_9
26. Silvester, J.R.: Determinants of block matrices. Math. Gaz. **84**(501), 460–467 (2000)
27. Sim, S.M., Khoo, K., Oggier, F., Peyrin, T.: Lightweight MDS involution matrices. In: Leander, G. (ed.) FSE 2015. LNCS, vol. 9054, pp. 471–493. Springer, Heidelberg (2015)
28. Swan, R.G.: Factorization of polynomials over finite fields. Pacific J. Math. **12**(3), 1099–1106 (1962)
29. Wardlaw, W.P.: Matrix representation of finite fields. Math. Mag. **67**(4), 289–293 (1994)
30. Wu, S., Wang, M., Wu, W.: Recursive diffusion layers for (lightweight) block ciphers and hash functions. In: Knudsen, L.R., Wu, H. (eds.) SAC 2012. LNCS, vol. 7707, pp. 355–371. Springer, Heidelberg (2013)
31. Xu, H., Zheng, Y., Lai, X.: Construction of perfect diffusion layers from linear feedback shift registers. IET Inf. Secur. **9**(2), 127–135 (2015)