Decomposing Linear Layers

Christof Beierle[1], Patrick Felke[2], Gregor Leander[1] and Sondre Rønjom[3,4]

[1] Faculty of Computer Science, Ruhr University Bochum, Bochum, Germany,
firstname.lastname@rub.de
[2] University of Applied Sciences Emden-Leer, Emden, Germany,
patrick.felke@hs-emden-leer.de
[3] Nasjonal Sikkerhetsmyndighet (NSM), Oslo, Norway
[4] University of Bergen, Bergen, Norway, sondre.ronjom@uib.no

Abstract. There are many recent results on reverse-engineering (potentially hidden) structure in cryptographic S-boxes. The problem of recovering structure in the other main building block of symmetric cryptographic primitives, namely, the linear layer, has not been paid that much attention so far. To fill this gap, in this work, we develop a systematic approach to decomposing structure in the linear layer of a substitution-permutation network (SPN), covering the case in which the specification of the linear layer is obfuscated from applying secret linear transformations to the S-boxes. We first present algorithms to decide whether an $ms \times ms$ matrix with entries in a prime field $\mathbb{F}_p$ can be represented as an $m \times m$ matrix over the extension field $\mathbb{F}_{p^s}$. We then study the case of recovering structure in MDS matrices by investigating whether a given MDS matrix follows a Cauchy construction. As an application, for the first time, we show that the 8×8 MDS matrix over $\mathbb{F}_{2^8}$ used in the hash function Streebog is a Cauchy matrix.

Keywords: finite field · matrix · substitution-permutation network · MDS · Cauchy

1 Introduction

Different from the naive expectation, quite often and for various reasons, a cryptanalyst or user of a (symmetric) cryptographic primitive is not aware of the full documentation of its design. In some cases, the designers do publish the specification, but miss out documenting the design rationale explaining the reason for choosing each building block. The most prominent example is the Data Encryption Standard (DES) [PUB77], standardized in 1977, for which the S-boxes have been (secretly) designed to resist differential cryptanalysis [Cop94], a cryptanalytic technique that became known to the public only several years later [BS90]. As more recent examples, we mention the block cipher families Simon and Speck designed by the US National Security Agency (NSA) [BSS+13] and the Russian hash function standard Streebog [Fed12]. In the latter, the 8-bit S-box π is just given as a plain look-up table and the linear layer employs a 64×64 matrix L with entries in $\mathbb{F}_2$ and it is not explained in any more detail in the specification. In more severe cases, even the specification of the cryptographic algorithm is not made public and (in the best case) the user or cryptanalyist only has access to a device or software in which the algorithm is implemented. Examples include the stream cipher A5/1 used for GSM encryption [BGW99] and the stream ciphers GEA/1 and GEA/2 for GPRS encryption [BDL+21], but there are also block ciphers of that kind, e.g., Skipjack [Nat98, BBD+98] or Chiasmus [STW13].[1] Another example is ransomware. Via obfuscation techniques, the cryptographic algorithms

[1] Those algorithms became public through reverse-engineering, declassification, or anonymous sources.

are hidden to bypass virus scanners. Hence, the analyst has to deal with the problem of figuring out the original specification of the employed cryptographic algorithm, once identified with techniques as in, e.g., [KPK+20], with the goal to break it and recover the data without paying the ransom.

In the case where the specification is secret or otherwise obfuscated, before any cryptanalysis could be made, the whole cryptographic algorithm has to first be reverse-engineered from the device or software. What results after such a process is not a well-written design specification, but rather some more or less complicated program code, which does not reveal the precise specifications of the cryptographic building blocks that the designers chose.

While this is true for all designs, we are focusing on substitution-permutation networks (SPNs) and are interesed in particular to find structure that is induced by defining linear layers over extension fields. In the case of SPNs, a natural limitation is that the S-box within an SPN can only be recovered up to some linear transformations in the input and the output and for each such S-box one obtains a different linear layer. In Figure 1 we depict the original design, and two variants of obfuscated linear layers that might occur.

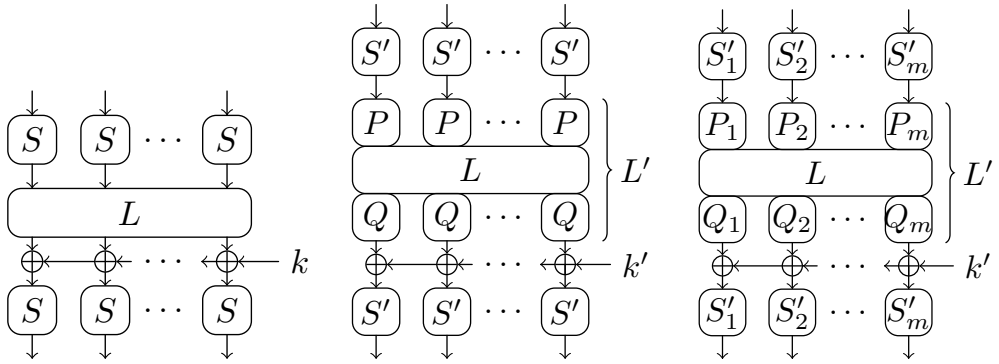

Figure 1: A keyed round function of an SPN with one additional S-box layer (left), an alternative representation of the round with $S' = P^{-1} \circ S \circ Q^{-1}$ (middle), and an alternative representation of the round with $S'_i = P_i^{-1} \circ S \circ Q_i^{-1}$ (right).

This obfuscation makes the above task of recovering structure harder, not only computationally, but also as we are not sure what the "correct" representation should be.[2]

In the case of *S-boxes*, there are lots of recent results on this problem, see [BP15, BPU16, PUB16, PU16, BPT19]. To name one specific result in this area, Perrin [Per19] has shown that the S-box π of Streebog has the interesting property of mapping multiplicative cosets to additive cosets of $\mathbb{F}_{2^4}^*$. Although no attack has been found exploiting this fact, such a result negatively affects the trust in the algorithm: Why did the designers intend to have such a property in the first place without making it public? Obviously, to fully understand the cryptographic strength of an algorithm, analyzing only the S-box is not enough and one has to study the interaction with the linear layer (see also the discussion in [Per19] for the case of Streebog). For reverse-engineering structure in *linear layers*, not much previous work has been done. In [KK13], Kazymyrov and Kazymyrova have shown that the transpose of the 64×64 binary matrix L used in Streebog can be represented as an 8×8 MDS matrix with entries in the extension field $\mathbb{F}_{2^8}$. In their method, they only focused on representing $\mathbb{F}_{2^8}$ as a quotient $\mathbb{F}_2[X]/(p)$ for p being an irreducible polynomial in $\mathbb{F}_2[X]$ of degree 8. More precisely, for all such irreducible polynomials p, they converted

[2] This could also be the case if the specification was made public by the designers, namely when they chose to obfuscate a (potentially hidden) structure by applying linear transformations to the input and output of the S-boxes.

all 8×8 submatrices to an element of the finite field and finally checked the MDS property of the resulting matrix.

In this work, we develop a systematic approach to decomposing structure in the linear layer of a block cipher or cryptographic permutation, also covering the case in which the specification of the linear layer is *obfuscated* from applying linear transformations to the S-boxes.

1.1 Our Contribution and Results

Let p be a prime and m, s be positive integers, $s > 1$. In Section 3, we start by investigating whether a given (non-obfuscated) $ms \times ms$ matrix with entries in the prime field $\mathbb{F}_p$ can be represented as an $m \times m$ matrix over the extension field $\mathbb{F}_{p^s}$ (Theorem 1 and Algorithm 2). Compared to the case where $\mathbb{F}_{p^s}$ is represented as the polynomial ring $\mathbb{F}_p[X]$ modulo an irreducible polynomial of degree s, we work with *matrix representations* of $\mathbb{F}_{p^s}$, which allows for a much more general choice of basis. Being of independent interest, at the core of our method is an algorithm that runs in time complexity of $\mathcal{O}(n \log p^s + ns^4 \log p \log\log p^s)$ elementary field operations (suppose we know the prime factorization of $p^s - 1$) and decides whether the matrix algebra $\mathbb{F}_p[A_1, \ldots, A_n]$ with $A_1, \ldots, A_n \in \mathrm{GL}(s, \mathbb{F}_p)$ is a field isomorphic to (a subfield of) $\mathbb{F}_{p^s}$ (Theorem 2). Since the algorithm needs to compute multiplicative orders of elements in $\mathrm{GL}(s, \mathbb{F}_p)$ as a subroutine, we need an oracle for the prime factorization of $p^s - 1$. However, that requirement is not a limitation for the parameters we consider in practice.

In Sections 4.1 and 4.2, we then study the case in which the specification of the linear layer (i.e., the $ms \times ms$ matrix under consideration) is obfuscated from applying secret linear transformations to the S-boxes (i.e., applying block-diagonal matrices with entries in $\mathrm{GL}(s, \mathbb{F}_p)$ in the input and the output). Interestingly, the complexity for recovering a matrix representation over $\mathbb{F}_{p^s}$ (if it exists) is comparable to the complexity of doing so in the non-obfuscated case (Theorems 3 and 5 and Algorithms 3 and 4).

In Section 5, we then study the problem of decomposing structure in a given MDS matrix; more precisely, we decide whether an MDS matrix over a finite field follows a Cauchy construction. As an application, we show in Section 6 how our methods can be applied to the linear layer of Streebog. For the first time, we show that the MDS matrix used in Streebog follows such a Cauchy construction.

2 Preliminaries

We recall some properties and relations about finite fields and matrix spaces and we fix the notation used in the remainder of this article. Thereby, we assume that the reader is familiar with basic facts about these objects. We denote by $\mathrm{Mat}(n, \mathbb{F}_p)$ the set of $n \times n$ matrices with coefficients in $\mathbb{F}_p$. A block diagonal matrix of the form

$$\begin{bmatrix} M_1 & 0 & \ldots & 0 \\ 0 & M_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & M_k \end{bmatrix}$$

will be denoted by $M_1 \oplus M_2 \oplus \cdots \oplus M_k$. If $M_1 = M_2 = \cdots = M_k$, we will also write $M^{\oplus k}$. By $\mathbb{N}$ we denote the natural numbers with 0 included.

Throughout this work, let p be a prime. For a positive integer s, it is well known that there exists exactly one finite field with p^s elements up to isomorphism, and we usually denote it by $\mathbb{F}_{p^s}$ and talk about *the* finite field with p^s elements. There are two typical representations of this field. The first, and most common, way is to fix

an irreducible polynomial $q \in \mathbb{F}_p[X]$ of degree s and represent the elements in $\mathbb{F}_{p^s}$ as elements in $\mathbb{F}_p[X]/(q)$. The second way is to use a *matrix representation*. Thereby a matrix $A \in \mathrm{Mat}(s, \mathbb{F}_p)$ is chosen with irreducible minimal polynomial q of degree s. The matrix algebra $\mathbb{F}_p[A] \coloneqq \{\sum_{i=0}^{m} r_i A^i | r_i \in \mathbb{F}_p, m \geq 0\}$ is isomorphic to $\mathbb{F}_p[X]/(q)$ and therefore a representation of $\mathbb{F}_{p^s}$ (see [War94]). In this way, the multiplicative group of the field can be represented as a subgroup of $\mathrm{GL}(s, \mathbb{F}_p)$, i.e., the group of all invertible $s \times s$ matrices with coefficients in $\mathbb{F}_p$. Together with the zero-matrix, this then defines a field with the addition being the usual matrix addition. Below, we briefly give a specific construction based on this second approach. For more details, we refer to [War94], Section 2.5 of [LN94], Section 7.2 of [HJ20], and also to [BKL16].

Let $\alpha \in \mathbb{F}_{p^s}$ be a non-zero element of the finite field (using an arbitrary field representation). Then, multiplication by α is an invertible linear mapping in $\mathbb{F}_{p^s}$. As $\mathbb{F}_{p^s}$ is isomorphic as a vector space to $\mathbb{F}_p^s$ by choosing an $\mathbb{F}_p$-basis, there exist an isomorphism by $\Phi \colon \mathbb{F}_{p^s} \to \mathbb{F}_p^s$.

Using this, multiplication by α can be written as the mapping $\Phi^{-1} \circ A_\alpha \circ \Phi$, where $A_\alpha \in \mathrm{GL}(s, \mathbb{F}_p)$, as the following commutative diagram illustrates. Here, by abuse of notation, A_α denotes the mapping $x \mapsto A_\alpha x$.

$$\begin{array}{ccc} \mathbb{F}_{p^s} & \xrightarrow{\cdot\alpha} & \mathbb{F}_{p^s} \\ \Big\downarrow{\scriptstyle \Phi} & & \Big\uparrow{\scriptstyle \Phi^{-1}} \\ \mathbb{F}_p^s & \xrightarrow{A_\alpha \in \mathrm{GL}(s, \mathbb{F}_p)} & \mathbb{F}_p^s \end{array}$$

Note that the matrix A_α depends on the choice of basis. In the same way, the multiplication by 0 in the finite field can be written as $\Phi^{-1} \circ \mathbf{0} \circ \Phi$ with $\mathbf{0}$ being the $s \times s$ zero-matrix. It becomes obvious that the set $\{A_\alpha \mid \alpha \in \mathbb{F}_{p^s}^*\} \subseteq \mathrm{GL}(s, \mathbb{F}_p)$, together with the zero-matrix defines a field with p^s elements by using the usual multiplication and addition of matrices. Changing the choice-of-basis transformation Φ corresponds to changing the matrices A_α up to similarity. In other words, for each matrix $M \in \mathrm{GL}(s, \mathbb{F}_p)$, the field $\{A_\alpha \mid \alpha \in \mathbb{F}_{p^s}^*\} \cup \{\mathbf{0}\}$ is isomorphic to $\{M A_\alpha M^{-1} \mid \alpha \in \mathbb{F}_{p^s}^*\} \cup \{\mathbf{0}\}$. As we will heavily use this wording in the remainder of the work, we explicitly define it.

Definition 1. Any set of matrices $\mathcal{M} \subseteq \mathrm{GL}(s, \mathbb{F}_p) \cup \{\mathbf{0}\}$ that, together with the natural matrix operations, forms the field $\mathbb{F}_{p^s}$ is called a *matrix representation of* $\mathbb{F}_{p^s}$.

The most simple matrix representation of $\mathbb{F}_{p^s}$ can be given as $\langle T_q \rangle \cup \{\mathbf{0}\} = \{T_q^i \mid i = 0, \ldots, p^s - 2\} \cup \{\mathbf{0}\}$, where T_q is the *companion matrix* of a primitive polynomial $q = X^s + \sum_{i=0}^{s-1} q_i X^i \in \mathbb{F}_p[X]$ of degree s, defined as

$$T_q \coloneqq \begin{bmatrix} 0 & 0 & \ldots & 0 & -q_0 \\ 1 & 0 & \ldots & 0 & -q_1 \\ 0 & 1 & \ldots & 0 & -q_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -q_{s-1} \end{bmatrix}.$$

Indeed, T_q corresponds to multiplication with a field element with minimal polynomial q. We are going to use the following, more general, lemma which gives a criterion when a matrix algebra is a field. It is a well known result, see also [War94] or [BKL16, Theorem 1]. We still provide a proof for completeness.

Lemma 1. *Let $A \in \mathrm{GL}(s, \mathbb{F}_p)$. Then, the matrix algebra $\mathbb{F}_p[A]$ is a field of order p^t with $t \mid s$ if and only if the minimal polynomial of A is irreducible.*

Proof. Let us denote by m_A the minimal polynomial of A with $t \coloneqq \deg(m_A)$. If m_A is reducible, it can be easily seen that $\mathbb{F}_p[A]$ is not a field. Indeed, we could write m_A as a product of two non-constant polynomials $P = \sum_{i=0}^{d_P} p_i X^i \in \mathbb{F}_p[X]$ and $Q = \sum_{i=0}^{d_Q} q_i X^i \in \mathbb{F}_p[X]$ with $d_P + d_Q = t$. If $\mathbb{F}_p[A]$ would be a field, then $m_A(A) = P(A) \cdot Q(A) = 0$ implies $P(A) = 0$ or $Q(A) = 0$, contradicting to the fact that m_A is the non-constant monic polynomial of least degree with $m_A(A) = 0$.

If m_A is irreducible, the ideal (m_A) is a maximal ideal in $\mathbb{F}_p[X]$. Moreover by definition of the minimal polynomial, the ideal (m_A) is the kernel of the surjective ring homomorphism $f \colon \mathbb{F}_p[X] \to \mathbb{F}_p[A], \sum_{i=0}^{m} r_i X^i \mapsto \sum_{i=0}^{m} r_i A^i$. Hence, we have $\mathbb{F}_p[X]/(m_A) \cong \mathrm{Im}(f) = \mathbb{F}_p[A]$ by the isomorphism theorem for rings and thus $\mathbb{F}_p[A]$ is a field. □

Remark 1. Note that we did not impose any restriction on the degree of m_A. If the degree of m_A is strictly smaller than s, then A is an element of a proper subfield of $\mathbb{F}_{p^s}$.

Clearly, if the matrix algebra generated by $A \in \mathrm{GL}(s, \mathbb{F}_p)$ is a field, the cyclic group $\langle A \rangle \coloneqq \{A^i \mid i \geq 0\}$ is isomorphic to a subgroup of $\mathbb{F}_{p^s}^*$. A matrix representation of a finite field of characteristic p is more general than the representation of the field as $\mathbb{F}_p[X]/(q)$, where q is an irreducible polynomial. Indeed, not every matrix representation is of the form $\langle T_q \rangle \cup \{\mathbf{0}\}$. A counterexample is the matrix representation

$$\mathcal{M} = \left\langle \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \right\rangle \cup \{\mathbf{0}\}$$

of $\mathbb{F}_{2^4}$, which does not contain any companion matrix (or a transpose of it). To summarize, any matrix A which is similar to T_q yields a field isomorphic to $\mathbb{F}_p[X]/(q)$ and vice versa.

3 Decomposing Matrices

In this section, the problem we are studying is how to algorithmically decide whether a given $ms \times ms$ matrix over $\mathbb{F}_p$ can be represented as a matrix over the extension field $\mathbb{F}_{p^s}$. Let us first formally define our terminology.

Definition 2. Let s, m be positive integers and let $n = s \cdot m$. Let $A \in \mathrm{Mat}(n, \mathbb{F}_p)$ and $A_{i,j} \in \mathrm{Mat}(s, \mathbb{F}_p), 1 \leq i, j \leq m$ such that $A = [A_{i,j}]_{1 \leq i,j \leq m}$. We say that A *can be represented as a matrix over* $\mathbb{F}_{p^s}$, if there exists a matrix representation $\mathcal{M}$ of $\mathbb{F}_{p^s}$ such that $\{A_{i,j} \mid 1 \leq i, j \leq m\} \subseteq \mathcal{M}$.

We then have the following result. Note that we exclude the case of $A = \mathbf{0}$ in the statement of the theorem. Clearly, the zero-matrix can trivially be represented over an extension field.

Theorem 1. *Let s, m be positive integers and let $n = s \cdot m$. Let $A \in \mathrm{Mat}(n, \mathbb{F}_p) \setminus \{\mathbf{0}\}$ with $A = [A_{i,j}]_{1 \leq i,j \leq m}$ for $A_{i,j} \in \mathrm{Mat}(s, \mathbb{F}_p)$. Then, A can be represented as a matrix over $\mathbb{F}_{p^s}$ if and only if the following two conditions hold:*

1. *For each $i, j \in \{1, \ldots, m\}$, we have $A_{i,j} \in \mathrm{GL}(s, \mathbb{F}_p) \cup \{\mathbf{0}\}$.*
2. *The multiplicative group generated by $\{A_{i,j} \mid 1 \leq i, j \leq m\} \setminus \{\mathbf{0}\}$ is cyclic and generated by an element $\alpha \in \mathrm{GL}(s, \mathbb{F}_p)$ with irreducible minimal polynomial.*

Proof. We define $S \coloneqq \{A_{i,j} \mid 1 \leq i,j \leq m\} \setminus \{\mathbf{0}\}$. Since we have $A \neq \mathbf{0}$, the set S is not empty. Let us assume that A can be represented as a matrix over $\mathbb{F}_{p^s}$. By definition, there exists a matrix representation $\mathcal{M}$ of $\mathbb{F}_{p^s}$ such that $S \subseteq \mathcal{M} \setminus \{\mathbf{0}\}$. Since $\mathcal{M}$ is a field, we have $\mathcal{M} \setminus \{\mathbf{0}\}$ being a cyclic group, hence each element in S is invertible and $\langle S \rangle$ is a cyclic subgroup of $\mathcal{M} \setminus \{\mathbf{0}\}$. Let α be a generator of $\langle S \rangle$. Since $\mathbb{F}_p[\alpha] \subseteq \mathcal{M}$ and $\mathcal{M}$ is a finite field, $\mathbb{F}_p[\alpha]$ is a finite integral domain and therefore a field (see, e.g., [LN94]). By Lemma 1, the element α has an irreducible minimal polynomial.

Let us now assume that $\langle S \rangle = \langle \alpha \rangle$ for $\alpha \in \mathrm{GL}(s, \mathbb{F}_p)$ with irreducible minimal polynomial. By Lemma 1, the matrix algebra generated by α is a field, so the group $\langle \alpha \rangle$ is a subgroup of $\mathbb{F}_{p^s}^*$. □

On deciding whether a subgroup of $\mathrm{GL}(s, \mathbb{F}_p)$ is a subgroup of $\mathbb{F}_{p^s}^*$. The problem we face now is to algorithmically decide whether a subgroup G of $\mathrm{GL}(s, \mathbb{F}_p)$ generates a subgroup of the multiplicative group of $\mathbb{F}_{p^s}$, i.e., to decide whether G is cyclic and generated by an element with irreducible minimal polynomial (see Condition 2 of Theorem 1). If this is the case, we also want to find the generator of G. This problem can be solved by using only elementary group theory. We first recall the following fundamental lemma on cyclic groups.

Lemma 2 (See, e.g., Thm. 1.6.17 of [HJ20])**.** *Let $G = \langle \alpha \rangle$ be a finite cyclic group of order n and let d be a divisor of n. Then, there exists a unique subgroup of G of order d, i.e., $\langle \alpha^{\frac{n}{d}} \rangle$.*

Another well-known group-theoretic result is that, if G is an Abelian group containing elements of finite orders k_1 and k_2, then G contains an element of order $\mathrm{lcm}(k_1, k_2)$ (see, e.g., Thm. 1.6.21 of [HJ20]). For the special case of cyclic groups (which are always Abelian), this result allows to give a generator quite easily, as we formulate below. Lemma 3 and the corresponding lines 8–15 in Algorithm 1 are mathematical folklore, we still provide a proof for completeness.

Lemma 3. *Let $G = \langle A_1, A_2 \rangle$ be a finite cyclic group with k_1 and k_2 being the multiplicative order of A_1 and A_2, respectively. Let h_1, h_2 be coprime positive integers such that $h_1 h_2 = \mathrm{lcm}(k_1, k_2)$ and, for $i \in \{1, 2\}$, h_i divides k_i. Then, $G = \langle A_1^{k_1/h_1} \cdot A_2^{k_2/h_2} \rangle$.*

Proof. Let $G' \coloneqq \langle A_1^{k_1/h_1} \cdot A_2^{k_2/h_2} \rangle$. Since $A_1^{k_1/h_1} \cdot A_2^{k_2/h_2}$ is an element of order $h_1 h_2$ (Lem. 1.6.19 of [HJ20]), the order of G' is equal to $\mathrm{lcm}(k_1, k_2)$. Hence, by Lemma 2, G' contains unique subgroups S_1, S_2 of order k_1 and k_2, respectively. Since G' is a subgroup of G and G is cyclic, S_1 (resp., S_2) is also the unique subgroup of G of order k_1 (resp., k_2). Hence, both A_1 and A_2 must be in G'. □

Note that from the prime factorizations of k_1 and k_2, it is easy to compute elements h_1 and h_2 that fulfill the conditions of Lemma 3, see ll. 8–15 in Algorithm 1. Applying Lemma 3 iteratively allows to find a generator of a cyclic group $G = \langle A_1, \ldots, A_n \rangle$.

Theorem 2. *Let $A_1, A_2, \ldots, A_n \in \mathrm{GL}(s, \mathbb{F}_p)$ and let $G = \langle A_1, A_2, \ldots, A_n \rangle$. Algorithm 1 returns a generator $\alpha \in \mathrm{GL}(s, \mathbb{F}_p)$ of G with irreducible minimal polynomial if and only if G is cyclic and generated by an element with irreducible minimal polynomial. Otherwise, it returns $\perp$. If we know the prime factorization of $p^s - 1$, the time complexity of Algorithm 1 is in $\mathcal{O}(n \log p^s + n s^4 \log p \log\log p^s)$ elementary field operations.*

Proof. If G is cyclic and generated by an element with irreducible minimal polynomial, G is a subgroup of $\mathbb{F}_{p^s}^*$, hence the order of G divides $p^s - 1$ and the minimal polynomial of each generator is irreducible. In particular, it suffices to compute an arbitrary generator of G. By Lemma 3, the element α computed in Algorithm 1 is a generator of G. Because its

minimal polynomial is irreducible, the matrix algebra $\mathbb{F}_p[\alpha]$ is a field of extension degree at most s over $\mathbb{F}_p$. Hence, $A_1, \ldots, A_n$ are all in the linear span of $\{1, \alpha, \alpha^2, \ldots, \alpha^{s-1}\}$.

If G is not cyclic, the elements $A_1, \ldots, A_n$ do not lie all in a finite field, so clearly Algorithm 1 would return $\perp$ when checking whether $A_1, \ldots, A_n \in \mathbb{F}_p[\alpha]$ in line 21 (if it did not return $\perp$ already before). If G is cyclic, but not generated by an element with irreducible minimal polynomial, Algorithm 1 returns $\perp$ in line 19.

Let us now analyze the time complexity. In each of the $n-1$ iterations of the main loop (ll. 2–17), we need to perform one multiplication, four exponentiations, and two computations of the multiplicative order of elements in $\mathrm{GL}(s, \mathbb{F}_p)$. Further, we need to compute two prime factorizations of integers dividing $p^s - 1$. Let $p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r}$ be the prime factorization of $p^s - 1$. The two prime factorizations in line 7 can be obtained by computing $\gcd(p_i^{c_i}, k_j)$ for $i \in \{1, \ldots, r\}$ and $j \in \{1, 2\}$. Note that the number of prime factors r is in $\mathcal{O}(\log p^s)$. The time complexity of a matrix multiplication and exponentiation is in $\mathcal{O}(s^3)$ and $\mathcal{O}(s^3 \log s)$ elementary field operations, respectively. Let $A \in \mathrm{GL}(s, \mathbb{F}_p)$ have multiplicative order dividing $p^s - 1$. By knowing the factorization of $p^s - 1$, computing $\mathrm{ord}(A)$ can be done in time complexity of $\mathcal{O}(s^4 \log p \log\log p^s)$ elementary field operations, see [O'B11, Theorem 2.2] and [CL95]. Hence, the time complexity of the main loop is in $\mathcal{O}(n \log p^s + n s^4 \log p \log\log p^s)$ elementary field operations. The complexity of the steps outside of the main loop can be neglected. More precisely, the computation of the minimal polynomial of α can be done with $\mathcal{O}(s^3)$ elementary field operations (see [Sto98]) and for checking whether $A_1, \ldots, A_n \in \mathbb{F}_p[\alpha]$, we need to solve n linear systems of s^2 equations and s unknowns over $\mathbb{F}_p$. □

There are various ways to optimize the implementation of Algorithm 1 further. For instance, we could add a step at the beginning which checks whether the degrees of all minimal polynomials $m_{A_i}, i = 1, \ldots, n$ divide s. If we know beforehand that $G = \langle A_1, A_2, \ldots, A_n \rangle$ is cyclic, we could use a probabilistic algorithm (e.g., Algorithm 4.80 in [VOMV96]) to find a generator of G.

Remark 2. Algorithm 1 is general enough to even work if all of the $A_1, \ldots, A_n$ lie in different proper subfields of $\mathbb{F}_{p^s}$. Note that, once we encounter one element with multiplicative order $p^s - 1$ in line 6 of Algorithm 1, we could skip the rest of the computation and directly perform the check in line 21 for that particular element. In particular, constructing a potential generator by means of Lemma 3 is not needed if one of the A_i has multiplicative order $p^s - 1$. Further, if one of the matrices $A_1, \ldots, A_n \in \mathrm{GL}(s, \mathbb{F}_p)$ (say A_1) has an irreducible minimal polynomial of degree s and if we are not interested in finding the generator α, but just want to know whether $A_1, \ldots, A_n$ are contained in a field $\mathbb{F}_p[\alpha]$, we could take $\alpha \coloneqq A_1$ and directly perform the check in line 21 for α. However, we would not necessarily have $G = \langle \alpha \rangle$.

Algorithm 2 takes as input a non-zero matrix $A \in \mathrm{Mat}(n, \mathbb{F}_p)$ and positive integers m, s with $n = s \cdot m$ and outputs (if it exists) a representation of A as

$$\left[\alpha^{N(i,j)}\right]_{1 \le i,j \le m} \coloneqq \begin{bmatrix} \alpha^{N(1,1)} & \alpha^{N(1,2)} & \ldots & \alpha^{N(1,m)} \\ \alpha^{N(2,1)} & \alpha^{N(2,2)} & \ldots & \alpha^{N(2,m)} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{N(m,1)} & \alpha^{N(m,2)} & \ldots & \alpha^{N(m,m)} \end{bmatrix} \tag{1}$$

with $\alpha \in \mathcal{M} \setminus \{\mathbf{0}\}$ for a matrix representation $\mathcal{M}$ of $\mathbb{F}_{p^s}$ and, for each $i, j \in \{1, \ldots, m\}$, $N(i, j) \in \mathbb{N} \cup \{\infty\}$. We define $\alpha^\infty \coloneqq \mathbf{0}$.

The running time of this algorithm is dominated by solving m^2 discrete logarithms over $\mathbb{F}_{p^s}^*$ in order to recover the exponents $N(i, j)$ for $i, j \in \{1, \ldots, m\}$ (this step could be omitted if the exponents are not needed). For the parameters $s = m = 8$ and $p = 2$, our implementation recovers the field representation within less than a second when running

Algorithm 1 ComputeGenerator

Input: Matrices $A_1, A_2, \ldots, A_n \in \mathrm{GL}(s, \mathbb{F}_p)$.

Output: A generator α of $G \coloneqq \langle A_1, A_2, \ldots, A_n \rangle$ if G is cyclic and generated by an element of irreducible minimal polynomial, $\perp$ otherwise.

$\alpha \leftarrow A_1$
for $i = 2, \ldots, n$ **do**
  if $\alpha^{p^s-1} \neq 1$ or $A_i^{p^s-1} \neq 1$ **then** ▷ One of the orders of α, A_i does not divide $p^s - 1$
    Return $\perp$
  end if
  $k_1 \leftarrow \mathrm{ord}(\alpha), \quad k_2 \leftarrow \mathrm{ord}(A_i)$
  Compute the prime factorizations $k_1 = p_1^{d_1} \cdot p_2^{d_2} \cdot \cdots \cdot p_r^{d_r}$ and $k_2 = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_r^{e_r}$
  $h_1 \leftarrow 1, \quad h_2 \leftarrow 1$
  for $j = 1, \ldots, r$ **do**
    if $d_j \geq e_j$ **then**
      $h_1 \leftarrow h_1 \cdot p_j^{d_j}$
    else
      $h_2 \leftarrow h_2 \cdot p_j^{e_j}$
    end if
  end for ▷ h_1 and h_2 fulfill the conditions of Lemma 3
  $\alpha \leftarrow \alpha^{k_1/h_1} \cdot A_i^{k_2/h_2}$
end for
if the minimal polynomial of α is not irreducible **then**
  Return $\perp$
end if
for $i = 1, \ldots, n$ **do** ▷ We check whether $A_1, \ldots, A_n$ are elements of the field $\mathbb{F}_p[\alpha]$
  if $A_i \notin \mathrm{Span}(1, \alpha, \alpha^2, \ldots, \alpha^{s-1})$ **then**
    Return $\perp$
  end if
end for
Return α

Algorithm 2 MatrixDecomposition

Input: Positive integers m, s and a matrix $A \in \mathrm{Mat}(m \cdot s, \mathbb{F}_p) \setminus \{\mathbf{0}\}$.

Output: A representation of A as $\left[\alpha^{N(i,j)}\right]_{1 \leq i,j \leq m} \in \mathrm{Mat}(m, \mathbb{F}_{p^s})$ if it exists, $\perp$ otherwise.

$\mathcal{S} \leftarrow []$
for each $s \times s$ block $A_{i,j}$ in A **do**
  if $A_{i,j}$ is non-zero **then**
    if $A_{i,j}$ is not invertible **then**
      Return $\perp$ ▷ Non-zero field elements need to be invertible
    end if
    Append $A_{i,j}$ to $\mathcal{S}$
  end if
end for
$\alpha \leftarrow$ ComputeGenerator($\mathcal{S}$)
if $\alpha = \perp$ **then** ▷ The group generated by $\mathcal{S}$ is not a subgroup of $\mathbb{F}_{p^s}^*$
  Return $\perp$
end if
Return A as $\left[\alpha^{N(i,j)}\right]_{1 \leq i,j \leq m}$ ▷ We need to solve m^2 dlogs over $\mathbb{F}_{p^s}^*$ to recover the exponents

on a PC. Applying the algorithm to the linear layer used in Streebog, we directly obtain the representation given in Section 6.

4 Decomposing an Obfuscated Matrix

A designer of an SPN using an S-box S (m times in parallel) and a linear layer L for its round function (as depicted in Figure 1 (left)) could try to hide the structure of the linear layer L, most importantly the property whether L has a representation over an extension field $\mathbb{F}_{p^s}$, by publishing a different *representation* of the round. In particular, the designer could select a linear layer $L' = Q^{\oplus m} \circ L \circ P^{\oplus m}$ for some invertible linear mappings P, Q aligned with the S-boxes and then cancel the application of those mappings P and Q by selecting an S-box S' which is linear equivalent to S, see Figure 1 (middle). If one allows to represent a round function with multiple distinct S-boxes, instead of restricting to a single pair (P, Q) a designer could even choose $P_1, \dots, P_m, Q_1, \dots, Q_m$ and define $L' = (Q_1 \oplus \cdots \oplus Q_m) \circ L \circ (P_1 \oplus \cdots \oplus P_m)$, see Figure 1 (right). The resulting ciphers are the same as the original one, up to linear permutations in the input and output, and up to the addition of different round keys. It is worth remarking that the most important cryptographic properties of L are not affected by changing to L'. In particular, if L is MDS, so is L' (see [WLTZ21, Prop. 6]). However, what is affected is the property whether the linear layer can or cannot be represented over an extension field $\mathbb{F}_{p^s}$. The same situation is often encountered when reverse engineering some proprietary cipher on hardware or included in binaries of a software, e.g., in ransomware. Therefore, we study the problem how to decide whether such *obfuscated* linear layers can be represented over an extension field $\mathbb{F}_{p^s}$, and if they can, how to recover an according representation. Section 4.1 deals with the case of hiding the structure of L by using a single pair of invertible linear mappings (P, Q) (as depicted in Figure 1 (middle)), and Section 4.2 analyzes the case where L is hidden as depicted in Figure 1 (right). In both cases, it turns out that the recovery of a representation over an extension field is not more complex than the recovery of such a representation in the non-obfuscated case.

4.1 Simple Obfuscation

Let s, m be positive integers and let $n = s \cdot m$. The problem we are studying now is, given a matrix $B \in \mathrm{Mat}(n, \mathbb{F}_p)$, decide whether there exists matrices $P, Q \in \mathrm{GL}(s, \mathbb{F}_p)$ and a matrix $A \in \mathrm{Mat}(n, \mathbb{F}_p)$ which can be represented as a matrix over $\mathbb{F}_{p^s}$ such that

$$B = \begin{bmatrix} Q & 0 & \dots & 0 \\ 0 & Q & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & Q \end{bmatrix} \cdot A \cdot \begin{bmatrix} P & 0 & \dots & 0 \\ 0 & P & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & P \end{bmatrix}. \tag{2}$$

If such a representation as given in (2) exists, our goal is to recover P, Q, a matrix representation $\mathcal{M}$ of $\mathbb{F}_{p^s}$, and to find $\alpha \in \mathcal{M} \backslash \{\mathbf{0}\}$ and exponents $N(i,j), i, j = 1, \dots, m$ with $N(i,j) \in \mathbb{N} \cup \{\infty\}$ such that A can be represented as in (1). Note that such a representation (if it exists) is not unique. For instance, up to a change of basis transformation of the coefficients in A, we can without loss of generality assume that Q is the identity matrix. In the following, let us denote by $A_{i,j}$ and $B_{i,j}, i, j = 1, \dots, m$ the $s \times s$ blocks of A and B, respectively, i.e., $A = [A_{i,j}]_{1 \le i,j \le m}$ and $B = [B_{i,j}]_{1 \le i,j \le m}$. We have the following result.

Theorem 3. *Let s, m be positive integers and let $n = s \cdot m$. For a matrix $B = [B_{i,j}]_{1 \le i,j \le m} \in \mathrm{Mat}(n, \mathbb{F}_p) \setminus \{\mathbf{0}\}$, Relation (2) holds for some $P, Q \in \mathrm{GL}(s, \mathbb{F}_p)$ and $A = [A_{i,j}]_{1 \le i,j \le m} \in \mathrm{Mat}(n, \mathbb{F}_p)$ that can be represented as a matrix over $\mathbb{F}_{p^s}$ if and only if the following conditions hold:*

1. *For each* $i, j \in \{1, \ldots, m\}$*, we have* $B_{i,j} \in \mathrm{GL}(s, \mathbb{F}_p) \cup \{\mathbf{0}\}$*.*
2. *There exists a block* $B_{k',\ell'} \in \mathrm{GL}(s, \mathbb{F}_p)$ *of* B *such that the group*

$$\langle B_{i,j} B_{k',\ell'}^{-1} \mid i, j = 1, \ldots, m \text{ and } B_{i,j} \in \mathrm{GL}(s, \mathbb{F}_p) \rangle \tag{3}$$

is cyclic and generated by an element $\alpha \in \mathrm{GL}(s, \mathbb{F}_p)$ *with irreducible minimal polynomial.*

Proof. We first show that if one of the two conditions does not hold, a representation as given in (2) does not exist. Indeed, if Condition 1 does not hold, there exists a block $A_{i,j}$ of A such that $A_{i,j}$ is neither invertible nor zero, which is a contradiction to the fact that A can be represented as a matrix over $\mathbb{F}_{p^s}$. If Condition 1 holds and Condition 2 does not hold, then by Lemma 1 there is a group $\mathcal{G}$ as defined in (3) such that the matrix algebra generated by $\mathcal{G}$ is not a field (note that a block $B_{k',\ell'} \in \mathrm{GL}(s, \mathbb{F}_p)$ exists as we assume that $B \neq \mathbf{0}$). Indeed, if $\mathcal{G}$ is not cyclic, it is not isomorphic to a subgroup of $\mathbb{F}_{p^s}^*$. If $\mathcal{G}$ is cyclic, but not generated by an element with irreducible minimal polynomial, we can directly apply Lemma 1. Hence, there exists a non-zero non-invertible element H of $\mathbb{F}_p[\mathcal{G}]$. Suppose that such an element H does not exist, $\mathbb{F}_p[\mathcal{G}]$ would be a finite division ring and therefore a field due to Wedderburn's theorem (see [Wit31]). Having a representation of B as

$$B = Q^{\oplus m} \cdot A \cdot P^{\oplus m}$$

with $A = [A_{i.j}]_{1 \leq i,j \leq m}$, we have $B_{i,j} = Q \cdot A_{i,j} \cdot P$ for any $i, j \in \{1, \ldots, m\}$, hence any element $B_{i,j} B_{k',\ell'}^{-1}$ is of the form $Q \cdot A_{i,j} A_{k',\ell'}^{-1} \cdot Q^{-1}$, and we can write $H = Q \cdot H' \cdot Q^{-1}$ with H' being a sum of elements of the form $A_{i,j}^t A_{k',\ell'}^{-t}$. But if H is not invertible, also H' is not invertible, a contradiction to the fact that A can be represented as a matrix over $\mathbb{F}_{p^s}$.

Let now both of the Conditions 1 and 2 hold. Let $B_{k',\ell'}$ be an invertible block of B such that

$$\langle B_{i,j} B_{k',\ell'}^{-1} \mid i, j = 1, \ldots, m \text{ and } B_{i,j} \in \mathrm{GL}(s, \mathbb{F}_p) \rangle = \langle \alpha \rangle$$

with α having an irreducible minimal polynomial. By Lemma 1, we have that $\langle \alpha \rangle \subseteq \mathcal{M} \backslash \{\mathbf{0}\}$ for a matrix representation $\mathcal{M}$ of $\mathbb{F}_{p^s}$. Let now $A \in \mathrm{Mat}(n, \mathbb{F}_p)$ be such that

$$B = A \cdot B_{k',\ell'}^{\oplus m},$$

which is a representation as in Relation (2) with Q being the identity and $P = B_{k',\ell'}$. For any $i, j \in \{1, \ldots, m\}$, we now have $B_{i,j} B_{k',\ell'}^{-1} = A_{i,j} = \alpha^{N(i,j)}$ with $N(i,j) \in \mathbb{N}$ if $B_{i,j}$ is invertible and $N(i,j) = \infty$ if $B_{i,j} = \mathbf{0}$. □

Algorithm 3 recovers α, P and $N(i,j) \in \mathbb{N} \cup \{\infty\}$ for $1 \leq i, j \leq m$ such that $A = [\alpha^{N(i,j)}]_{1 \leq i,j \leq m}$ (if it exists) and outputs $\perp$ otherwise (note that we assume without loss of generality Q to be the identity). Again, the running time is dominated by solving m^2 discrete logarithms over $\mathbb{F}_{p^s}^*$ for recovering the exponents $N(i,j)$ for $i, j \in \{1, \ldots, m\}$. For the parameters $s = m = 8$ and $p = 2$, our implementation recovers the field representation within a few seconds when running on a PC.

4.1.1 On the Degrees of Freedom by the Designer

Algorithm 3 recovers a simply-obfuscated matrix A with entries from a finite field $\mathbb{F}_{p^s}$ up to the simplification that, without loss of generality, it is assumed that Q is the identity matrix. In other words, it outputs only *one of several* possible solutions of the decomposition. When it comes to cryptanalysis or studying implementation properties of the whole primitive, it might be crucial to recover the original matrix A *chosen by designer* or at least a matrix A' which is "as close as possible" to A. In this section we

Algorithm 3 SimplyObfuscatedMatrixDecomposition

Input: Positive integers m, s and a matrix $B \in \mathrm{Mat}(m \cdot s, \mathbb{F}_p) \setminus \{\mathbf{0}\}$.

Output: A matrix $P \in \mathrm{GL}(s, \mathbb{F}_p)$ and $A \in \mathrm{Mat}(m \cdot s, \mathbb{F}_p)$ represented over $\mathbb{F}_{p^s}$ as $A = \left[\alpha^{N(i,j)}\right]_{1 \le i,j \le m} \in \mathrm{Mat}(m, \mathbb{F}_{p^s})$ such that $B = A \cdot P^{\oplus m}$ if it exists, $\perp$ otherwise.

$\mathcal{S} \leftarrow []$
for each $s \times s$ block $B_{i,j}$ in B **do**
  if $B_{i,j}$ is non-zero **then**
    if $B_{i,j}$ is not invertible **then**
      Return $\perp$ ▷ Non-zero field elements need to be invertible
    end if
    Append $B_{i,j}$ to $\mathcal{S}$
  end if
end for
Choose P as the first element in $\mathcal{S}$ ▷ An arbitrary element in $\mathcal{S}$ can be chosen
$\alpha \leftarrow$ ComputeGenerator($\{C \cdot P^{-1} \mid C \in \mathcal{S}\}$)
if $\alpha = \perp$ **then** ▷ The group generated by $\mathcal{S}P^{-1}$ is not a subgroup of $\mathbb{F}_{p^s}^*$
  Return $\perp$
end if
Return P and $A \coloneqq B \cdot (P^{-1})^{\oplus m}$ as $\left[\alpha^{N(i,j)}\right]_{1 \le i,j \le m}$ ▷ We need to solve m^2 dlogs over $\mathbb{F}_{p^s}^*$

will deal with this problem. The next lemma is crucial to settle it. Recall that for a (non-empty) subset $S = \{z_1, \ldots, z_t\} \subseteq \mathbb{F}_{p^s}$, the subfield of $\mathbb{F}_{p^s}$ obtained by adjoining S to $\mathbb{F}_p$ is $\mathbb{F}_p[S] \coloneqq \{\sum_{i=0}^{m} \sum_{j=1}^{t} r_{i,j} z_j^i \mid r_{i,j} \in \mathbb{F}_p, m \ge 0\}$.

Lemma 4. *Let $\mathcal{M}$ be a matrix representation of $\mathbb{F}_{p^s}$ and let $\alpha \in \mathcal{M}$ such that $\mathbb{F}_p[\alpha] = \mathbb{F}_{p^s}$, i.e., $1, \alpha, \ldots, \alpha^{s-1}$ defines a polynomial basis. If $Q_1 \alpha Q_1^{-1} = Q_2 \alpha^{p^k} Q_2^{-1}$ with $Q_1, Q_2 \in \mathrm{GL}(s, \mathbb{F}_p)$ and $0 \le k \le s-1$, then $Q_1 = Q_2 \beta F_k$ with $\beta \in \mathcal{M} \setminus \{\mathbf{0}\}$ and F_k being the representation matrix of the Frobenius automorphism $x \mapsto x^{p^k}$ with respect to the basis $1, \ldots, \alpha^{s-1}$.*

Proof. Let F_k denote the matrix representation of the Frobenius automorphism $x \mapsto x^{p^k}$ with respect to the basis $1, \alpha, \ldots, \alpha^{s-1}$. For $v \in \mathbb{F}_p^s$ and $A \in \mathrm{Mat}(s, \mathbb{F}_p)$ we denote by $A(v)$ the matrix-vector multiplication. The equation $Q_1 \alpha Q_1^{-1} = Q_2 \alpha^{p^k} Q_2^{-1}$ is equivalent to $\alpha = Q_1^{-1} Q_2 \alpha^{p^k} Q_2^{-1} Q_1$. We will now show that, for $L \in \mathrm{GL}(s, \mathbb{F}_p)$, the equation $\alpha = L \alpha^{p^k} L^{-1}$ holds if and only if $L = \beta' F_{s-k}$ for an element $\beta' \in \mathcal{M} \setminus \{\mathbf{0}\}$. The equation $\alpha = L \alpha^{p^k} L^{-1}$ is equivalent to $\alpha L = L \alpha^{p^k}$. Let $v \in \mathbb{F}_p^s$ be such that when applying the mapping α to v the image $\alpha(v)$ corresponds to α, i.e., v corresponds to 1 when both are considered as elements of $\mathcal{M}$ with respect to the basis $1, \alpha, \ldots, \alpha^{s-1}$. Hence, $L(\alpha^{p^k}(v))$ corresponds to applying $L(F_k \alpha)$, where we now consider by abuse of notation α as a vector in $\mathbb{F}_p^s$ with respect to $1, \alpha, \ldots, \alpha^{s-1}$. It follows that $\alpha(L(v)) = L(\alpha^{p^k})$. Note that $L(v)$ corresponds to an element $\beta' \in \mathcal{M}$. So $\alpha(L(v))$ is identical to $\beta'(\alpha)$. With $\alpha = L \alpha^{p^k} L^{-1}$, we also have $\alpha^i = L \alpha^{ip^k} L^{-1}, i = 0, \ldots, s-1$. In the same vein it follows that $\alpha^i(L(v)) = \beta'(\alpha^i) = L(\alpha^{ip^k})$ for $i = 0, \ldots, s-1$. As $1, \alpha, \ldots, \alpha^{s-1}$ forms a polynomial basis, it follows that $\beta' = L F_k$ and by composing with F_{s-k} from the right we finally have $L = \beta' F_{s-k}$.

Thus $Q_1^{-1} Q_2 = \beta' F_{s-k}$. It follows that $Q_2 F_k \beta'^{-1} = Q_1$. We have $F_k \beta'^{-1} = \beta'^{-p^k} F_k$. By setting $\beta \coloneqq \beta'^{-p^k}$ the result follows. □

The next theorem shows how close one can get to the original matrix A, given the simply-obfuscated matrix B.

Theorem 4. *Let us be given a simply-obfuscated matrix $B = Q^{\oplus m} \cdot A \cdot P^{\oplus m} \neq \mathbf{0}$ with $P, Q \in \mathrm{GL}(s, \mathbb{F}_p)$, $A = \left[\gamma^{N(i,j)}\right]_{1 \leq i,j \leq m}, s > 1$. Thereby γ is the representation matrix for the multiplication with a primitive element of $\mathbb{F}_{p^s}^*$ with respect to a basis $\mathcal{B}$. Let $B_{k',\ell'} \in \mathrm{GL}(s, \mathbb{F}_p)$ and*

$$\mathcal{G} \coloneqq \langle B_{i,j} B_{k',\ell'}^{-1} \mid 1 \leq i, j \leq m \text{ and } B_{i,j} \in \mathrm{GL}(s, \mathbb{F}_p) \rangle = \langle \zeta \rangle$$

as in Equation (3) be such that $\mathbb{F}_p[\zeta]$ is a matrix representation of $\mathbb{F}_{p^s}$, i.e., $1, \zeta, \ldots, \zeta^{s-1}$ defines a polynomial basis. Then, for any *primitive element $g \in \mathbb{F}_{p^s}^*$, a companion matrix α of g and matrices $Q' = QL\beta_1 F_k$, $P' = P^{-1} L \beta_2 F_k$ can be computed from B, ζ such that*[3]

$$((Q'^{-1})^{\oplus m} \cdot B \cdot P'^{\oplus m}) = \left[\alpha^{p^{s-k}(dN(i,j)+c)}\right]_{1 \leq i,j \leq m},$$

where c is such that $\alpha^c = \beta_1^{-1}\beta_2$ and d such that $L\alpha^d L^{-1} = \gamma$. The complexity for this computation is $\mathcal{O}(s^{2 \cdot 3})$ elementary field operations, and the computation of one discrete logarithm with respect to g or α.

Proof. Let us choose a primitive element g of $\mathbb{F}_{p^s}^*$ and let α be its companion matrix. Let L denote the transition matrix from $1, g, \ldots, g^{s-1}$ to $\mathcal{B}$. As g and γ are primitive elements there exists an exponent d with $\gcd(d, p^s - 1) = 1$ such that $L\alpha^d L^{-1} = \gamma$. We have $\zeta = Q\gamma^{e' p^{k_1}} Q^{-1}$. It follows that $\alpha^{e' p^k} = L^{-1} \gamma^{d^{-1} e' p^k} L$, where d^{-1} is the multiplicative inverse of $d \mod (p^s - 1)$, and ζ can be re-written as $QL\alpha^{ep^k} L^{-1} Q^{-1}$ (where $e \coloneqq de'$). The exponent e is determined by considering the characteristic polynomial χ_ζ of ζ, which is identical to $\chi_{\gamma^{e'}}$ and computing a discrete logarithm with respect to g or α respectively. Moreover, p^k cannot be determined uniquely as a characteristic polynomial determines a zero only up to application of the Frobenius automorphism. By Lemma 4, the equation $\zeta = Q'\alpha^e Q'^{-1}$ has the solutions $Q' = QL\beta_1 F_k$, where β_1 is the representation matrix of the multiplication with a field element β_1 and F_k the representation matrix of the Frobenius automorphism $x \mapsto x^{p^k}$ with respect to $1, \ldots, g^{s-1}$. By solving the equation $\zeta Q' = Q'\alpha^e$ the matrices Q' can be computed with $s^{2 \cdot 3}$ arithmetic field operations.

Let $\zeta' \coloneqq B_{k',\ell'}^{-1} \cdot \zeta \cdot B_{k',\ell'}$. Then, $\zeta' = P^{-1}\gamma^{e' p^k} P$ and thus we can compute $P' = P^{-1} L \beta_2 F_k$ in the same vein. It follows that $(Q'^{-1})^{\oplus m} \cdot B \cdot P'^{\oplus} = A'$, where $A'_{i,j} = F_{s-k}\beta_1^{-1} L^{-1} A_{i,j} L \beta_2 F_k$. Thereby $L^{-1} A_{i,j} L$ is the representation matrix of $A_{i,j} = \gamma^{N(i,j)}$ with respect to the basis $1, g, \ldots, g^{s-1}$. Since $L\alpha^d L^{-1} = \gamma$, we have

$$\begin{aligned} F_{s-k}\beta_1^{-1} L^{-1} \gamma^{N(i,j)} L \beta_2 F_k &= F_{s-k} L^{-1} \gamma^{N(i,j)} L \beta_1^{-1} \beta_2 F_k \\ &= F_{s-k} \alpha^{dN(i,j)} \left(\beta_1^{-1}\beta_2\right) F_k = \alpha^{p^{s-k}(dN(i,j)+c)}. \end{aligned}$$

□

Note that with Algorithm 3 one can check if Theorem 4 is applicable and determine s. The element ζ can be found by using Algorithm 1. Then, Theorem 4 shows that one is able to recover a representation based on companion matrices, which might deal as a good enough substitute for the original matrix chosen by the designer to conduct, e.g., cryptanalysis or implementation optimization. However, if we are not interested in deriving such a representation based on companion matrices, we can omit the computation step of complexity $\mathcal{O}(s^{2 \cdot 3})$ and the computation of the discrete logarithm given in Theorem 4. Indeed, we can formulate the following corollary, which shows that, up to similarity, we can find A up to $(p^s - 1)^2$ possibilities.

[3] For an integer a, we define $a \cdot \infty = \infty + a = \infty$.

Corollary 1. *Let $s > 1$. Given a simply-obfuscated matrix $B = Q^{\oplus m} \cdot A \cdot P^{\oplus m} \neq \mathbf{0}$ with $P, Q \in \mathrm{GL}(s, \mathbb{F}_p)$ and where $A = \left[\gamma^{N(i,j)}\right]_{1 \leq i,j \leq m}$ for a primitive element $\gamma \in \mathbb{F}_{p^s}^*$. Let α be an* arbitrary *primitive element of $\mathbb{F}_{p^s}^*$. Let $B_{k',\ell'} \in \mathrm{GL}(s, \mathbb{F}_p)$ and*

$$\mathcal{G} \coloneqq \langle B_{i,j} B_{k',\ell'}^{-1} \mid 1 \leq i, j \leq m \text{ and } B_{i,j} \in \mathrm{GL}(s, \mathbb{F}_p) \rangle = \langle \zeta \rangle$$

as in Equation (3) be such that $1, \zeta, \ldots, \zeta^{s-1}$ defines a polynomial basis of $\mathbb{F}_{p^s}$. Then there exists $L \in \mathrm{GL}(s, \mathbb{F}_p)$ and $c, d \in \{0, 1, \ldots, p^s - 2\}$ such that $A = \left[L \alpha^{dN(i,j)+c} L^{-1}\right]_{1 \leq i,j \leq m}$.

4.2 Heavy Obfuscation

Again, let s, m be positive integers and let $n = s \cdot m$. The problem we are studying in this section is, given a matrix $B \in \mathrm{Mat}(n, \mathbb{F}_p)$, decide whether there exists matrices $P_1, P_2, \ldots, P_m \in \mathrm{GL}(s, \mathbb{F}_p)$ and $Q_1, Q_2, \ldots, Q_m \in \mathrm{GL}(s, \mathbb{F}_p)$, and a matrix $A \in \mathrm{Mat}(n, \mathbb{F}_p)$ which can be represented as a matrix over $\mathbb{F}_{p^s}$ such that

$$B = \begin{bmatrix} Q_1 & 0 & \ldots & 0 \\ 0 & Q_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & Q_m \end{bmatrix} \cdot A \cdot \begin{bmatrix} P_1 & 0 & \ldots & 0 \\ 0 & P_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & P_m \end{bmatrix}. \tag{4}$$

In the following, we restrict to the simpler case in which B (and therefore also A) does not contain a zero block, i.e., $\mathbf{0} \notin \{A_{i,j} \mid 1 \leq i, j \leq m\}$. This might be a reasonable assumption when having B as a linear layer of a block cipher or cryptographic permutation. For instance, in an MDS matrix, all square submatrices are invertible [MS77].

Again, a representation as in (4) (if it exists) is not unique. For instance, without loss of generality, we can assume that Q_1 is the identity matrix as changing Q_1 only applies a change-of-basis transformation to the elements of A. Our goal is to recover a matrix representation $\mathcal{M}$ of $\mathbb{F}_{p^s}$ and to find $\alpha \in \mathcal{M} \setminus \{\mathbf{0}\}$ and exponents $N(i,j), i, j = 1, \ldots, m$ with $N(i,j) \in \mathbb{N}$ such that A is given as in (1). Let us again denote by $A_{i,j}$ and $B_{i,j}, i, j = 1, \ldots, m$ the $s \times s$ blocks of A and B, respectively, i.e., $A = [A_{i,j}]_{1 \leq i,j \leq m}$ and $B = [B_{i,j}]_{1 \leq i,j \leq m}$. We have the following result.

Theorem 5. *Let s, m be positive integers and let $n = s \cdot m$. For a matrix $B = [B_{i,j}]_{1 \leq i,j \leq m} \in \mathrm{Mat}(n, \mathbb{F}_p)$ with $B_{i,j} \neq \mathbf{0}$ for all $i, j \in \{1, \ldots, m\}$, Relation (4) holds for some $P_1, P_2, \ldots, P_m$, $Q_1, Q_2, \ldots, Q_m \in \mathrm{GL}(s, \mathbb{F}_p)$ and $A = [A_{i,j}]_{1 \leq i,j \leq m} \in \mathrm{Mat}(n, \mathbb{F}_p)$ that can be represented as a matrix over $\mathbb{F}_{p^s}$ if and only if the following conditions hold:*

1. *For each $i, j \in \{1, \ldots, m\}$, we have $B_{i,j} \in \mathrm{GL}(s, \mathbb{F}_p)$.*
2. *The group*
$$\langle B_{1,1} B_{i,1}^{-1} B_{i,j} B_{1,j}^{-1} \mid i, j = 1, \ldots, m \rangle \tag{5}$$
is cyclic and generated by an element $\alpha \in \mathrm{GL}(s, \mathbb{F}_p)$ with irreducible minimal polynomial.

Proof. Having any representation of B as

$$B = (Q_1 \oplus Q_2 \cdots \oplus Q_m) \cdot A \cdot (P_1 \oplus P_2 \cdots \oplus P_m) \tag{6}$$

with $A = [A_{i.j}]_{1 \leq i,j \leq m}$, we have $B_{i,j} = Q_i \cdot A_{i,j} \cdot P_j$ for any $i, j \in \{1, \ldots, m\}$. If Condition 1 does not hold, there exists a block $A_{i,j}$ of A such that $A_{i,j}$ is neither invertible nor zero, which is a contradiction to the fact that A can be represented as a matrix over $\mathbb{F}_{p^s}$. If Condition 1 holds and Condition 2 does not hold, then by Lemma 1 the matrix algebra generated by the group $\mathcal{G}$ defined in (5) is not a field. Hence, there exists a non-zero

non-invertible element H of $\mathbb{F}_p[\mathcal{G}]$. Having a representation of B as given in Equation (6), any element $B_{1,1}B_{i,1}^{-1}B_{i,j}B_{1,j}^{-1}$ is of the form $Q_1 \cdot A_{1,1}A_{i,1}^{-1}A_{i,j}A_{1,j}^{-1} \cdot Q_1^{-1}$. In particular, we have $H = Q_1 \cdot H' \cdot Q_1^{-1}$ with H' being a sum of elements of the form $A_{1,1}^t A_{i,1}^{-t} A_{i,j}^t A_{1,j}^{-t}$. But if H is not invertible, also H' is not invertible, a contradiction to the fact that A can be represented as a matrix over $\mathbb{F}_{p^s}$.

Let now both of the Conditions 1 and 2 hold. Let

$$\langle B_{1,1}B_{i,1}^{-1}B_{i,j}B_{1,j}^{-1} \mid i,j = 1,\dots,m\rangle = \langle \alpha \rangle$$

with α having an irreducible minimal polynomial. By Lemma 1, we have that $\langle \alpha \rangle \subseteq \mathcal{M}\backslash\{\mathbf{0}\}$ for a matrix representation $\mathcal{M}$ of $\mathbb{F}_{p^s}$. Let now $A \in \mathrm{Mat}(n, \mathbb{F}_p)$ be such that

$$B = (B_{1,1}B_{1,1}^{-1} \oplus B_{2,1}B_{1,1}^{-1} \cdots \oplus B_{m,1}B_{1,1}^{-1}) \cdot A \cdot (B_{1,1} \oplus B_{1,2} \oplus \cdots \oplus B_{1,m}),$$

i.e., for each $i,j \in \{1,\dots,m\}$, we define $A_{i,j} \coloneqq B_{1,1} \cdot B_{i,1}^{-1} \cdot B_{i,j} \cdot B_{1,j}^{-1}$. We now have that $A_{i,j} = \alpha^{N(i,j)}$ with $N(i,j) \in \mathbb{N}$. □

Algorithm 4 recovers $\alpha, Q_2, \dots, Q_m$, $P_1, P_2, \dots, P_m$ and $N(i,j) \in \mathbb{N}$ for $1 \le i,j \le m$ such that $A = [\alpha^{N(i,j)}]_{1\le i,j\le m}$ (if it exists) and outputs $\perp$ otherwise (note that we assume without loss of generality Q_1 to be the identity, denoted I_s). Again, the running time is dominated by solving m^2 discrete logarithms over $\mathbb{F}_{p^s}^*$ for recovering the exponents $N(i,j)$ for $i,j \in \{1,\dots,m\}$.

Algorithm 4 HeavyObfuscatedMatrixDecomposition

Input: Positive integers m, s and a matrix $B \in \mathrm{Mat}(m \cdot s, \mathbb{F}_p)$ with $B_{i,j} \neq \mathbf{0}$ for all $i,j \in \{1,\dots,m\}$.

Output: Matrices $P_1,\dots,P_m, Q_2,\dots,Q_m \in \mathrm{GL}(s,\mathbb{F}_p)$ and $A \in \mathrm{Mat}(m\cdot s, \mathbb{F}_p)$ represented over $\mathbb{F}_{p^s}$ as $A = \left[\alpha^{N(i,j)}\right]_{1\le i,j\le m} \in \mathrm{Mat}(m, \mathbb{F}_{p^s})$ such that $B = (I_s \oplus Q_2 \oplus \dots Q_m) \cdot A \cdot (P_1 \oplus \cdots \oplus P_m)$ if it exists, $\perp$ otherwise.

1: **for** each $s \times s$ block $B_{i,j}$ in B **do**
2: **if** $B_{i,j}$ is not invertible **then**
3: Return $\perp$ ▷ Non-zero field elements need to be invertible
4: **end if**
5: **end for**
6: **for** $i = 1,\dots,m$ **do**
7: $P_i \leftarrow B_{1,i}, \quad Q_i \leftarrow B_{i,1}B_{1,1}^{-1}$
8: **end for**
9: $\alpha \leftarrow$ ComputeGenerator$(\{Q_i^{-1}B_{i,j}P_j^{-1} \mid 1 \le i,j \le m\})$
10: **if** $\alpha = \perp$ **then**
11: Return $\perp$
12: **end if**
13: Return $P_1,\dots,P_m,Q_2,\dots,Q_m$ and

$$A \coloneqq (Q_1^{-1} \oplus Q_2^{-1} \oplus \cdots \oplus Q_m^{-1}) \cdot B \cdot (P_1^{-1} \oplus P_2^{-1} \oplus \cdots \oplus P_m^{-1}) \text{ as } \left[\alpha^{N(i,j)}\right]_{1\le i,j\le m}$$

▷ We need to solve m^2 dlogs over $\mathbb{F}_{p^s}^*$

4.2.1 On the Degrees of Freedom by the Designer

Again, as we already saw in the case of simple obfuscation, the decomposition of a heavy-obfuscated matrix B into $P_1,\dots,P_m,Q_1,\dots,Q_m$ and A is not unique. To precisely reveal the possible degrees of freedom, one can proceed in the same vein as in Theorem 4. Doing so yields the following theorem, which we state without proof.

Theorem 6. *Let us be given a heavily-obfuscated matrix B as in Relation (4) with $P_1, P_2, \ldots, P_m$, $Q_1, Q_2, \ldots, Q_m \in \mathrm{GL}(s, \mathbb{F}_p)$ and $A = [A_{i,j}]_{1 \leq i,j \leq m} \in \mathrm{Mat}(n, \mathbb{F}_p)$ that can be represented as a matrix over $\mathbb{F}_{p^s}$ and not containing a zero block, i.e. $A = \left[\gamma^{N(i,j)}\right]_{1 \leq i,j \leq m}$, $s > 1$ and $N(i,j) \in \mathbb{N}$ for $i, j \in \{1, \ldots, m\}$. Thereby γ is the representation matrix for the multiplication with a primitive element of $\mathbb{F}_{p^s}^*$ with respect to a basis $\mathcal{B}$. Let*

$$\mathcal{G} \coloneqq \langle B_{1,1} B_{i,1}^{-1} B_{i,j} B_{1,j}^{-1} \mid i, j = 1, \ldots m \rangle = \langle \zeta \rangle$$

be as in Equation (5) such that $\mathbb{F}_p[\zeta]$ is a matrix representation of $\mathbb{F}_{p^s}$, i.e., $1, \zeta, \ldots, \zeta^{s-1}$ defines a polynomial basis. Then, for any *primitive element $g \in \mathbb{F}_{p^s}^*$, a companion matrix α of g and matrices $Q_i' = Q_i L \beta_i F_{k_i}$, $P_i' = P_i^{-1} L \beta_i' F_{k_i}$ for $i = 1, \ldots, m$ can be computed from B, ζ such that*

$$(Q_1'^{-1} \oplus \cdots \oplus Q_m'^{-1}) \cdot B \cdot (P_1' \oplus \cdots \oplus P_m') = \left[\alpha^{p^{s-k_i}(dN(i,j)+c_i+c_j')}\right]_{1 \leq i,j \leq m},$$

where c_i, c_j' are such that $\alpha^{c_i} = \beta_i^{-1}$, $\alpha^{c_j'} = \beta_j'$ and d is such that $L\alpha^d L^{-1} = \gamma$. The complexity for this computation is $\mathcal{O}(ms^{2 \cdot 3})$ elementary field operations, and the computation of m discrete logarithms with respect to g or α.

Again, if we are not interested in deriving a representation based on companion matrices, we can omit the computation step of complexity $\mathcal{O}(ms^{2 \cdot 3})$ and the computation of the discrete logarithms. Indeed, we can formulate the following corollary.

Corollary 2. *Let $s > 1$. Given a heavily-obfuscated matrix $B = (Q_1 \oplus \cdots \oplus Q_m) \cdot A \cdot (P_1 \oplus \cdots \oplus P_m)$ with $P_i, Q_j \in \mathrm{GL}(s, \mathbb{F}_p)$ and where $A = \left[\gamma^{N(i,j)}\right]_{1 \leq i,j \leq m}$ with $N(i,j) \in \mathbb{N}$ for a primitive element $\gamma \in \mathbb{F}_{p^s}^*$, $i, j = 1, \ldots, m$. Let α be an* arbitrary *primitive element of $\mathbb{F}_{p^s}^*$. Let*

$$\mathcal{G} \coloneqq \langle B_{1,1} B_{i,1}^{-1} B_{i,j} B_{1,j}^{-1} \mid i, j = 1, \ldots m \rangle = \langle \zeta \rangle$$

be as in Equation (5) such that $1, \zeta, \ldots, \zeta^{s-1}$ defines a polynomial basis of $\mathbb{F}_{p^s}$. Then there exists $L \in \mathrm{GL}(s, \mathbb{F}_p)$ and $c_1, \ldots, c_m, c_1', \ldots, c_m', d \in \{0, 1, \ldots, p^s - 2\}$ and $k_1, \ldots, k_m \in \{0, \ldots, s-1\}$ such that $A = \left[L\alpha^{p^{k_i}(dN(i,j)+c_i+c_j')}L^{-1}\right]_{1 \leq i,j \leq m}$.

5 Recovering MDS Constructions – The Case of Cauchy Matrices

There are several ways to construct MDS matrices. If we are given an arbitrary MDS matrix over a finite field, e.g., by applying the decomposition methods described earlier, as a next step, it would be interesting to reveal how the actual matrix was constructed. In the following, we explain methods to algorithmically decide whether an (obfuscated) MDS matrix follows a *Cauchy construction* and to decompose the underlying structure.

5.1 Deciding Whether an MDS Matrix Is Cauchy

Cauchy matrices are of interest in symmetric cryptography as they yield MDS matrices in a very simple manner (see [RS85]). Cauchy matrices can be used to construct maximum distance separable (MDS) codes and are often used as linear layers in block cipher and hash function designs due to their optimal diffusion properties. Thus, given an MDS matrix recovered by one of our approaches, it is very natural to check if it is a Cauchy matrix and thereby revealing more structure of the possible design criteria. In this section we give an algorithm to do so.

Definition 3 (See, e.g., [RS85])**.** A matrix $A = [A_{i,j}]_{1 \le i,j \le m} \in \mathrm{Mat}(m, \mathbb{F}_{p^s})$ is called a *Cauchy matrix* if there exist two tuples $(u_1, \ldots, u_m), (v_1, \ldots, v_m), u_i, v_i \in \mathbb{F}_{p^s}$ such that, $u_1, \ldots, u_m, v_1, \ldots, v_m$ are pairwise distinct and $A_{i,j} = \frac{1}{u_i - v_j}$.

Remark 3. Obviously if $(u_1, \ldots, u_m), (v_1, \ldots, v_m)$ defines a Cauchy matrix A, so does $(u_1 + b, \ldots, u_m + b), (v_1 + b, \ldots, v_m + b)$ for every $b \in \mathbb{F}_{p^s}$. We will see that this way all possibilities to represent A are covered.

Let $A = \left[\alpha^{N(i,j)}\right]_{1 \le i,j \le m}$ be an MDS matrix, where $\alpha \in \mathbb{F}_{p^s}^*$ and $N(i,j) \in \mathbb{N}$. If A is a Cauchy matrix, by definition there exist $N(i) \in \mathbb{N} \cup \{\infty\}, i = 1, \ldots, m$ and $N'(j) \in \mathbb{N} \cup \{\infty\}, j = 1, \ldots, m$ such that $\alpha^{-N(i,j)} = \alpha^{N(i)} - \alpha^{N'(j)}$ for all $i, j = 1, \ldots, m$.

To detect whether A is a Cauchy matrix, we could derive a linear system with the $2m$ unknowns $\alpha^{N(i)}$ and $\alpha^{N'(j)}$ and m^2 equations. If the system has a solutions, we can afterwards (if needed)[4] reveal the exponents by computing $2m$ discrete logarithms.

The system of equations is of the form $l_{i,j} \coloneqq x_i - y_j - a_{i,j} = 0$, $1 \le i, j \le m$. The case $m = 1$ is trivial. Thus, we assume $m \ge 2$ in the following. Subtracting successively $l_{1,j} - l_{1,j+1}, j = 1, \ldots, m-1$ yields

$$\begin{array}{llll} -y_1 + y_2 - a_{1,1} + a_{1,2} & & & = 0 \\ & -y_2 + y_3 - a_{1,2} + a_{1,3} & & = 0 \\ \vdots & \ddots & \vdots & = 0 \\ \vdots & \vdots & & = 0 \\ & \cdots & -y_{m-1} + y_m - a_{1,m-1} + a_{1,m} & = 0 \end{array} . \tag{7}$$

Obviously y_m can be chosen as a free parameter. Once a value $b \in \mathbb{F}_{p^s}^*$ is assigned to y_m, the whole system is uniquely determined. Hence, if the system is solvable, the solution space is a 1-dimensional affine subspace, which can be split into $x_i = u_i + b, y_i = v_i + b, u_i, v_i, b \in \mathbb{F}_{p^s}^*$ and $v_m = 0$. The matrix A is a Cauchy matrix if and only if the system $(l_{i,j})_{1 \le i,j \le m}$ has a solution, where $u_1 + b, \ldots, u_m + b, v_1 + b, \ldots, v_m + b$ are pairwise distinct for a fixed and consequently all $b \in \mathbb{F}_{p^s}^*$.

We conclude the following result, which implies that writing an $m \times m$ MDS matrix as a Cauchy matrix, or showing that it is impossible, can be done with a complexity of $\mathcal{O}(m^2)$ arithmetic operations in $\mathbb{F}_{p^s}$.

Theorem 7. *Let $A = \left[\alpha^{N(i,j)}\right]_{1 \le i,j \le m}$ be an MDS matrix, where $\alpha \in \mathbb{F}_{p^s}^*$ and $N(i,j) \in \mathbb{N}$. Then, A is a Cauchy matrix if and only if, for all $i, j \in \{1, \ldots, m\}$, we can write $\alpha^{-N(i,j)} = u_i - v_j$ with*

1. *$u_i = \alpha^{-N(i,m)}$, $i = 1, \ldots, m$ and*
2. *$v_m = 0$ and $v_j = v_{j+1} + \alpha^{-N(1,j+1)} - \alpha^{-N(1,j)}$, $j = 1, \ldots, m-1$.*

Proof. From System (7), by setting $y_m = 0$, we obtain all the relations for v_m as described in 2. From the condition $\alpha^{-N(i,j)} = u_i - v_j$, for $j = m$, we obtain $\alpha^{-N(i,m)} = u_i$. □

Using those method, we show in Section 6 that the matrix used in the linear layer of Streebog is indeed a Cauchy matrix. To the best of our knowledge, this was not pointed out previously in the literature.

Remark 4. As we discussed in Sections 4.1 and 4.2, a recovered matrix A with entries from a finite field from a (simply- or heavily-) obfuscated matrix is not unique. Unfortunately, it might well be possible that the matrix chosen by the designer is of a Cauchy form, while the one recovered by our methods is not. In the case of having a simply-obfuscated

[4] If we are not interested in finding structure in the exponents, we could omit this step and just write the field elements in their matrix representation.

MDS matrix $B = Q^{\oplus m} \cdot A \cdot P^{\oplus m}$ with A being a matrix with entries in $\mathbb{F}_{p^s}$, Corollary 1 gives all $(p^s-1)^2$ possible solutions (up to applying the same similarity transformation to the entries of A) for A. Since applying the same similarity transformations to the entries of a Cauchy matrix does not affect the property of being a Cauchy matrix, we could decide whether there exist a solution for a Cauchy matrix A by simply brute-forcing all $(p^s-1)^2$ possible choices for the tuple (c,d) given in Corollary 1. This is feasible for usual parameters in block cipher constructions, i.e., $p=2, s \leq 8$.

In the case of heavy obfuscation, we have $(p^s-1)^{2m+1}s^m$ possible solutions for A, where m denotes the number of rows of A (see Corollary 2). The naive approach of brute forcing all those choices and check the Cauchy property quickly becomes infeasible, even for the parameters usually used in practice. For instance, in the case of $p=2, s=8, m=4$ (the parameters corresponding to an AES MixColumns operation), we would need to brute force roughly 2^{84} possibilities. In the next section, we will consider an alternative approach to solving that problem based on so-called *generalized Cauchy matrices*.

5.2 Detecting and Recovering Generalized Cauchy Matrices

In order to ease notation, in the following we use lower-case letters for matrices corresponding to field elements to distinguish them from general matrices. We need the notion of a *generalized Cauchy matrix*, defined as follows. Similarly to the notion of a Cauchy matrix as given in Definition 3, generalized Cauchy matrices are MDS.

Definition 4. [RS85] A matrix A over a field $\mathbb{F}_{p^s}$ with entries

$$A_{i,j} = \frac{u_i v_j}{x_i - y_j}$$

with $x_i, y_j \in \mathbb{F}_{p^s}, u_i, v_j \in \mathbb{F}_{p^s}^*$, $x_i - y_j \neq 0$ is called a *generalized Cauchy matrix*.

In Section 4.2 we introduced Algorithm 4 that tests if a heavily-obfuscated matrix can be represented over a field extension. The algorithm takes as input a matrix B and, if it is indeed representable over an extension field, computes a matrix representation for the field together with a decomposition of the matrix into a form

$$B = (Q'_1 \oplus \cdots \oplus Q'_m) \cdot G \cdot (P'_1 \oplus \cdots \oplus P'_m),$$

where G is over an extension field $\mathbb{F}_{p^s}$. Fortunately, if we want to test whether a matrix B corresponds to a heavily-obfuscated generalized Cauchy matrix, the matrix G determined by the algorithm is in fact also generalized Cauchy if the obfuscated matrix A is.

Theorem 8. *If $B = (Q_1 \oplus \cdots \oplus Q_m) \cdot A \cdot (P_1 \oplus \cdots \oplus P_m)$ is a heavily-obfuscated matrix representation of a generalized Cauchy matrix A over $\mathbb{F}_{p^s}$ with $Q_1, \ldots, Q_m, P_1, \ldots, P_m \in \mathrm{GL}(s, \mathbb{F}_p)$, then the matrix G returned by Algorithm 4 with entries*

$$G_{i,j} = B_{1,1} B_{i,1}^{-1} B_{i,j} B_{1,j}^{-1}$$

is also a generalized Cauchy matrix over $\mathbb{F}_{p^s}$.

Proof. By assumption, for $i,j \in \{1,\ldots,m\}$, we have $A_{i,j} = u_i v_j (x_i - y_j)^{-1}$ for elements $x_i, y_j \in \mathbb{F}_{p^s}, u_i, v_j \in \mathbb{F}_{p^s}^*$, thus $B_{1,1}B_{i,1}^{-1}B_{i,j}B_{1,j}^{-1} = Q_1(x_1-y_1)^{-1}(x_i-y_1)(x_i-y_j)^{-1}(x_1-y_j)Q_1^{-1}$ where the u_i, v_j cancel each other out in the product. Now if we let $u'_i = Q_1(x_1-y_1)^{-1}(x_i-y_1)Q_1^{-1}$ and $v'_j = Q_1(x_1-y_j)Q_1^{-1}$, $x'_i = Q_1 x_i Q_1^{-1}$ and $y'_j = Q_1 y_j Q_1^{-1}$ it follows that the entries of G are of the form

$$G_{i,j} = \frac{u'_i v'_j}{(x'_i - y'_j)}$$

and thus is a generalized Cauchy matrix over the field $\mathbb{F}_{p^s}$. □

Theorem 8 above shows the strength of Algorithm 4 described earlier. Not only does the algorithm discover a conjugate matrix representation of the field of the obfuscated matrix, it also directly provides a matrix for us which is generalized Cauchy if and only if the matrix that has been obfuscated was originally generalized Cauchy. Thus, in order to check whether a matrix is a heavily-obfuscated generalized Cauchy matrix, we can apply Algorithm 4 to determine a de-obfuscated matrix which then must be a generalized Cauchy matrix only involving field elements. Thus, the matrix G over $\mathbb{F}_{p^s}$ which is returned by Algorithm 4 will have entries of the form $G_{i,j} = \frac{u_i v_j}{x_i - y_j}$ where $x_i, y_j \in \mathbb{F}_{p^s}, u_i, v_j \in \mathbb{F}_{p^s}^*$.

From the definition of generalized Cauchy matrices there are $(p^s-1)^{2m-1}\prod_{i=0}^{2m-1}(p^s-i)$ parameters to choose from. However, not all of those matrices will be unique. There are many sets of choices of tuples $u, u', v, v', x, x', y, y' \in \mathbb{F}_{p^s}^m$ leading to the same fixed generalized Cauchy matrix. These equivalences provide some freedom when we want to determine whether a matrix G is indeed a generalized Cauchy. For instance, for any $h \in \mathbb{F}_{p^s}$ and $g_1, g_2, g \in \mathbb{F}_{p^s}^*$ with $g_1 g_2 = g$ such that $u'_i = u_i g_1, v'_j = v_j g_2, x'_i = g_1 g_2 (x_i + h)$ and $y'_j = g_1 g_2 (y_j + h)$, we have that

$$\frac{u'_i v'_j}{(x'_i - y'_j)} = \frac{u_i v_j}{(x_i - y_j)}$$

for all $1 \leq i, j \leq m$. Since an element $g \in \mathbb{F}_{p^s}^*$ can be expressed as a product $g_1 g_2 = g$ in $(p^s - 1)$ ways, while the number of shifts $h \in \mathbb{F}_{p^s}$ is exactly p^k, the above equivalences define $(p^s - 1)^2 p^s$ equivalent generalized Cauchy constructions.

5.3 Algorithm for Testing Generalized Cauchy

In this section we present an algorithm (Algorithm 5) that, given the output of Algorithm 4, tests whether a matrix over a field is generalized Cauchy by either returning a valid set of Cauchy-defining parameters $u, v, x, y \in \mathbb{F}_{p^s}^m$ or decides that it is not a generalized Cauchy matrix. The matrix G returned by Algorithm 4 has an especially nice form. Since the first row and first column are all ones, the entries of the generalized Cauchy matrix satisfy

$$u_i (x_i - y_1)^{-1} v_1 = u_1 (x_1 - y_j)^{-1} v_j = 1$$

for all $0 < i, j \leq m$. Now, from $G_{1,t} = u_1 v_t (x_1 - y_t)^{-1}$ and $G_{2,t} = u_2 v_t (x_2 - y_t)^{-1}$ we may derive a general relation

$$v_t = (G_{1,t}^{-1} u_1 - G_{2,t}^{-1} u_2)^{-1} (x_1 - x_2) = (u_1 - G_{2,t}^{-1} u_2)^{-1} (x_1 - x_2), \tag{8}$$

which is related to y_t via

$$y_t = x_1 - v_t G_{1,t}^{-1} u_1 = x_1 - v_t u_1.$$

Similarly, from $G_{t,1} = u_t v_1 (x_t - y_1)^{-1}$ and $G_{t,2} = u_t v_2 (x_t - y_2)^{-1}$ we can derive a relation

$$u_t = (v_2 G_{t,2}^{-1} - v_1 G_{t,1}^{-1})^{-1} (y_1 - y_2) = (v_2 G_{t,2}^{-1} - v_1)^{-1} (y_1 - y_2), \tag{9}$$

which is related to x_t by

$$x_t = v_1 G_{t,1}^{-1} u_t + y_1 = v_1 u_t + y_1.$$

Notice in particular that the values (u_t, x_t) or (v_t, y_t) only depend on the values of the matrix G together with a valid decomposition of the initial upper leftmost 2×2 square matrix. Thus consider the first upper leftmost 2×2 sub-matrix with entries

$$\begin{aligned} u_1 v_1 (x_1 - y_1)^{-1} &= 1 \\ u_1 v_2 (x_1 - y_2)^{-1} &= 1 \\ u_2 v_1 (x_2 - y_1)^{-1} &= 1 \\ u_2 v_2 (x_2 - y_2)^{-1} &= G_{2,2}. \end{aligned}$$

The equivalences explained in the previous subsection allows us to fix $u_1 = v_1 = 1$ and $x_1 = 0$. From the first equation we find that $y_1 = -1$. By simplifying (8) and (9) to

$$\begin{aligned} v_t &= (1 - G_{2,t}^{-1}(x_2 + 1))^{-1}(-x_2) \qquad y_t = -v_t \\ u_t &= (-y_2 G_{t,2}^{-1} - 1)^{-1}(-(1 + y_2)) \quad x_t = u_t - 1, \end{aligned}$$

we guess x_2 in the above and get $u_2 = x_2 + 1$, v_2 and $y_2 = -v_2$. In the case we guess x_2 such that $x_2 = G_{2,t} - 1$ or $y_2 = -G_{t,2}$ for any t, the algorithm fails. Thus, if we let $\mathcal{A} = \{G_{2,t} - 1 \,|\, 0 < t \leq m\}$ and $\mathcal{B} = \{-G_{t,2} \,|\, 0 < t \leq m\}$, we pick x_2 such that x_2 is not in $\mathcal{A}$ (nor among x_1, y_1) and such that the corresponding y_2 is not in $\mathcal{B}$ (nor among x_1, y_1, x_2). If this condition holds, we proceed and compute the rest of the u_i, v_i, x_i, y_i. The number of possible wrong choices for x_2 is exactly $2m - 1$ out of p^s. The complete procedure is presented in Algorithm 5 and requires first to use Algorithm 4 to recover a field representation and a matrix G.

Algorithm 5 ReverseGeneralizedCauchy

Input: An $m \times m$ matrix G over a field $\mathbb{F}_{p^s}$ returned by Algorithm 4.

Output: Return $\perp$ if G is not a generalized Cauchy matrix, or tuples $U, V, X, Y \in \mathbb{F}_{p^s}^m$ defining the generalized Cauchy matrix G

$x_1 = 0, y_1 = -1, u_1 = 1, v_1 = 1$
$\mathcal{A} \leftarrow \{G_{2,1} - 1, G_{2,2} - 1, \ldots, G_{2,m} - 1\}$
$\mathcal{B} \leftarrow \{-G_{1,2}, -G_{2,2}, \ldots, -G_{m,2}\}$
for $x_2 \in \mathbb{F}_{p^s}$ **do**
    if $x_2 \notin \mathcal{A} \cup \{x_1, y_1\}$ **then**
        $y_2 = (1 - G_{2,2}^{-1}(x_2 + 1))^{-1}(x_2)$
        if $y_2 \notin \mathcal{B} \cup \{x_1, x_2, y_1\}$ **then**
            $X = \{x_1, x_2\}$
            $Y = \{y_1, y_2\}$
            for $t = 3, \ldots, m$ **do**
                $y_t = x_2(1 - G_{2,t}^{-1}(x_2 + 1))^{-1}$
                $Y = Y \cup \{y_t\}$
                $x_t = (-1 - y_2)(-y_2 G_{t,2}^{-1} - 1)^{-1} - 1$
                $X = X \cup \{x_t\}$
            end for
            $U = \{\}$
            $V = \{\}$
            for $t = 1, \ldots, m$ **do**
                $U = U \cup \{X_t + 1\}$
                $V = V \cup \{-Y_t\}$
            end for
            Return U, V, X, Y
        end if
    end if
end for
Return $\perp$

6 Application to Streebog

Applying Algorithm 2 to the matrix used in Streebog yields

$$A := \begin{bmatrix} \gamma^{1} & \gamma^{64} & \gamma^{66} & \gamma^{39} & \gamma^{133} & \gamma^{249} & \gamma^{94} & \gamma^{135} \\ \gamma^{249} & \gamma^{84} & \gamma^{150} & \gamma^{0} & \gamma^{210} & \gamma^{1} & \gamma^{221} & \gamma^{32} \\ \gamma^{100} & \gamma^{16} & \gamma^{155} & \gamma^{15} & \gamma^{167} & \gamma^{36} & \gamma^{182} & \gamma^{57} \\ \gamma^{220} & \gamma^{174} & \gamma^{246} & \gamma^{217} & \gamma^{216} & \gamma^{17} & \gamma^{90} & \gamma^{198} \\ \gamma^{116} & \gamma^{188} & \gamma^{217} & \gamma^{246} & \gamma^{124} & \gamma^{127} & \gamma^{237} & \gamma^{206} \\ \gamma^{37} & \gamma^{129} & \gamma^{147} & \gamma^{243} & \gamma^{36} & \gamma^{167} & \gamma^{154} & \gamma^{89} \\ \gamma^{77} & \gamma^{66} & \gamma^{64} & \gamma^{238} & \gamma^{206} & \gamma^{3} & \gamma^{136} & \gamma^{124} \\ \gamma^{135} & \gamma^{230} & \gamma^{73} & \gamma^{137} & \gamma^{164} & \gamma^{32} & \gamma^{134} & \gamma^{1} \end{bmatrix}, \tag{10}$$

where

$$\gamma = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix},$$

which has minimal polynomial $q = X^8+X^6+X^5+X^4+1 \in \mathbb{F}_2[X]$. Note that $(\gamma^{32})^\top = T_q$, so by substituting γ by γ^{32} (and adapting the exponents accordingly) and transposing, we obtain the representation as recovered in [KK13]. Note that this is a consequence of Theorem 4, where we choose $\alpha = T_q$. Recall that by Theorem 4 there exist Q', P' such that $Q'^{-1}\gamma^{N(i,j)}P' = \alpha^{dN(i,j)+c}$. Indeed, $32 = 2^5$ is the application of the Frobenius automorphism $x \mapsto x^{2^5}$ and transposing a matrix is a similarity operation, i.e. $A_{i,j}^T = L^{-1}A_{i,j}L$ for a proper chosen matrix $L \in \mathrm{GL}(s, \mathbb{F}_p)$. Hence $A_{i,j}^T = L^{-1}\gamma^{N(i,j)}L = T_q^{2^{8-5}N(i,j)} = \alpha^{2^3N(i,j)}$ which gives as requested the above identity with $P' = Q' = L, d = 2^3$ and $c = 0$. It was remarked in [KK13], the decomposition method of Kazymyrov and Kazymyrova only worked if the matrix used in Streebog is transposed first.

6.1 Decomposition as a Cauchy Matrix

By applying the ideas described in Section 5.1, we can observe that Matrix (10) is a Cauchy matrix. Indeed, with

$$(u_1, u_2, u_3, u_4, u_5, u_6, u_7, u_8) = (\gamma^{120}, \gamma^{223}, \gamma^{198}, \gamma^{57}, \gamma^{49}, \gamma^{166}, \gamma^{131}, \gamma^{254})$$
$$(v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8) = (\gamma^{77}, \gamma^{82}, \gamma^{59}, \gamma^{220}, \gamma^{72}, \gamma^{209}, \gamma^{4}, 0),$$

we have $\gamma^{-N(i,j)} = u_i - v_j$ for all $i, j \in \{1, \ldots, 8\}$.

7 Conclusion

We presented algorithms to detect and recover the existence of structure induced by extension fields in matrices over finite fields. Surprisingly, while being a natural question in algorithmic algebra, even outside of cryptographic applications, we are not aware of previous solutions to this question.

Structure induced by extension fields is certainly most prominent in current designs and we exhaustively handled that case in our work. However, our work raises many questions on how to detect other types of structure in linear layers that we feel are worth being investigated in future works.

Acknowledgments

We thank Schloss Dagstuhl as this work was discussed at Dagstuhl-Seminar 22141 (symmetric cryptography).

This work was supported by the German Research Foundation (DFG) within the framework of the Excellence Strategy of the Federal Government and the States – EXC 2092 CaSa – 39078197.

References

[BBD+98] Eli Biham, Alex Biryukov, Orr Dunkelman, Eran Richardson, and Adi Shamir. Initial observations on Skipjack: Cryptanalysis of Skipjack-3XOR. In Stafford E. Tavares and Henk Meijer, editors, *Selected Areas in Cryptography '98, SAC'98, Proceedings*, volume 1556 of *LNCS*, pages 362–376. Springer, 1998.

[BDL+21] Christof Beierle, Patrick Derbez, Gregor Leander, Gaëtan Leurent, Håvard Raddum, Yann Rotella, David Rupprecht, and Lukas Stennes. Cryptanalysis of the GPRS encryption algorithms GEA-1 and GEA-2. In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology - EUROCRYPT 2021, Proceedings, Part II*, volume 12697 of *LNCS*, pages 155–183. Springer, 2021.

[BGW99] Marc Briceno, Ian Goldberg, and David Wagner. A pedagogical implementation of A5/1. https://cryptome.org/jya/a51-pi.htm (accessed July 22, 2022), 1999.

[BKL16] Christof Beierle, Thorsten Kranz, and Gregor Leander. Lightweight multiplication in $GF(2^n)$ with applications to MDS matrices. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016, Proceedings, Part I*, volume 9814 of *LNCS*, pages 625–653. Springer, 2016.

[BP15] Alex Biryukov and Léo Perrin. On reverse-engineering s-boxes with hidden design criteria or structure. In Rosario Gennaro and Matthew Robshaw, editors, *Advances in Cryptology - CRYPTO 2015, Proceedings, Part I*, volume 9215 of *LNCS*, pages 116–140. Springer, 2015.

[BPT19] Xavier Bonnetain, Léo Perrin, and Shizhu Tian. Anomalies and vector space search: Tools for s-box analysis. In Steven D. Galbraith and Shiho Moriai, editors, *Advances in Cryptology - ASIACRYPT 2019, Proceedings, Part I*, volume 11921 of *LNCS*, pages 196–223. Springer, 2019.

[BPU16] Alex Biryukov, Léo Perrin, and Aleksei Udovenko. Reverse-engineering the s-box of Streebog, Kuznyechik and STRIBOBr1. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology - EUROCRYPT 2016, Proceedings, Part I*, volume 9665 of *LNCS*, pages 372–402. Springer, 2016.

[BS90] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. In Alfred Menezes and Scott A. Vanstone, editors, *Advances in Cryptology - CRYPTO '90, 1990, Proceedings*, volume 537 of *LNCS*, pages 2–21. Springer, 1990.

[BSS+13] Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers. The SIMON and SPECK families of lightweight block ciphers. *IACR Cryptol. ePrint Arch.*, page 404, 2013.

[CL95] Frank Celler and Charles R. Leedham-Green. Calculating the order of an invertible matrix. In Larry Finkelstein and William M. Kantor, editors, *Groups and Computation, Proceedings of a DIMACS Workshop, 1995*, volume 28 of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, pages 55–60. DIMACS/AMS, 1995.

[Cop94] Don Coppersmith. The data encryption standard (DES) and its strength against attacks. *IBM journal of research and development*, 38(3):243–250, 1994.

[Fed12] Federal Agency on Technical Regulation and Metrology. Information technology – data security: Hash function. 2012.

[HJ20] Dirk Hachenberger and Dieter Jungnickel. *Topics in Galois fields*. Springer, 2020.

[KK13] Oleksandr Kazymyrov and Valentyna Kazymyrova. Algebraic aspects of the Russian hash standard GOST R 34.11-2012. *IACR Cryptol. ePrint Arch.*, page 556, 2013.

[KPK+20] Hyunji Kim, Jaehoon Park, Hyeokdong Kwon, Kyoungbae Jang, Seungju Choi, and Hwajeong Seo. Detecting block cipher encryption for defense against crypto ransomware on low-end internet of things. In Ilsun You, editor, *Information Security Applications - 21st International Conference, WISA 2020, Revised Selected Papers*, volume 12583 of *LNCS*, pages 16–30. Springer, 2020.

[LN94] Rudolf Lidl and Harald Niederreiter. *Introduction to finite fields and their applications*. Cambridge university press, 1994.

[MS77] Florence J. MacWilliams and Neil J. A. Sloane. *The theory of error correcting codes*, volume 16. Elsevier, 1977.

[Nat98] National Institute of Standards and Technology. Skipjack and KEA algorithms specifications, v2.0. https://csrc.nist.gov/Presentations/1998/Skipjack-and-KEA-Algorithm-Specifications (accessed July 2022, 2022), 1998.

[O'B11] Eamonn A. O'Brien. Algorithms for matrix groups. *London Math. Soc. Lecture Note Ser*, 388:297–323, 2011.

[Per19] Léo Perrin. Partitions in the s-box of Streebog and Kuznyechik. *IACR Trans. Symmetric Cryptol.*, 2019(1):302–329, 2019.

[PU16] Léo Perrin and Aleksei Udovenko. Exponential s-boxes: a link between the s-boxes of BelT and Kuznyechik/Streebog. *IACR Trans. Symmetric Cryptol.*, 2016(2):99–124, 2016.

[PUB77] PUB FIPS. 46: Data encryption standard. *National Institute of Standards and Technology*, 1977.

[PUB16] Léo Perrin, Aleksei Udovenko, and Alex Biryukov. Cryptanalysis of a theorem: Decomposing the only known solution to the big APN problem. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016, Proceedings, Part II*, volume 9815 of *LNCS*, pages 93–122. Springer, 2016.

[RS85] Ron M. Roth and Gadiel Seroussi. On generator matrices of MDS codes. *IEEE Trans. Inf. Theory*, 31(6):826–830, 1985.

[Sto98] Arne Storjohann. An $O(n^3)$ algorithm for the Frobenius normal form. In Volker Weispfenning and Barry M. Trager, editors, *Proceedings of the 1998 International Symposium on Symbolic and Algebraic Computation, ISSAC '98, 1998*, pages 101–105. ACM, 1998.

[STW13] Jan Schejbal, Erik Tews, and Julian Wälde. Reverse engineering of CHIASMUS from GSTOOL. Presentation at the Chaos Computer Club (CCC), slides available at https://fahrplan.events.ccc.de/congress/2013/Fahrplan/events/5307.html (accessed July 22, 2022), 2013.

[VOMV96] Paul C. Van Oorschot, Alfred J. Menezes, and Scott A. Vanstone. *Handbook of applied cryptography*. CRC press, 1996.

[War94] William P. Wardlaw. Matrix representation of finite fields. *Mathematics Magazine*, 67(4):289–293, 1994.

[Wit31] Ernst Witt. Über die Kommutativität endlicher Schiefkörper. *Abh. Math. Semin. Univ. Hambg.*, 8(413), 1931.

[WLTZ21] Shi Wang, Yongqiang Li, Shizhu Tian, and Xiangyong Zeng. Four by four MDS matrices with the fewest XOR gates based on words. *Adv. Math. Commun.*, 2021. https://doi.org/10.3934/amc.2021025.