A Proof of the Beierle-Kranz-Leander's Conjecture related to Lightweight Multiplication in $\mathbb{F}_{2^n}$

Sihem Mesnager[1], Kwang Ho Kim[2,3], Dujin Jo[4], Junyop Choe[2], Munhyon Han[2], and Dok Nam Lee[2]

[1] LAGA, Department of Mathematics, University of Paris VIII and Paris XIII, CNRS and Telecom ParisTech, France smesnager@univ-paris8.fr
[2] Institute of Mathematics, State Academy of Sciences, Pyongyang, DPR Korea
[3] PGItech Corp., Pyongyang, DPR Korea
[4] Rason Senior Middle School No.1, Rason, DPR Korea

Abstract. Lightweight cryptography is an important tool for building strong security solutions for pervasive devices with limited resources. Due to the stringent cost constraints inherent in extremely large applications, the efficient implementation of cryptographic hardware and software algorithms is of utmost importance to realize the vision of generalized computing.
In CRYPTO 2016, Beierle, Kranz and Leander have considered lightweight multiplication in $\mathbb{F}_{2^n}$. Specifically, they have considered the fundamental question of optimizing finite field multiplications with one fixed element and investigated which field representation, that is which choice of basis, allows for an optimal implementation. They have left open a conjecture related to two XOR-count. Using the theory of linear algebra, we prove in the present paper that their conjecture is correct. Consequently, this proved conjecture can be used as a reference for further developing and implementing cryptography algorithms in lightweight devices.

Keywords: Lightweight cryptography · constant multiplication · Hamming weight · XOR-count · cycle normal form.

1 Introduction

The current pervasive computing age has lead to an increased demand for security for applications ranging from RFIDs and smart cards to mobile devices. Lightweight cryptography is an important tool for building strong security solutions for pervasive devices with limited resources. These devices implement lightweight ciphers which are reliable and require low power and low computations. The lightweight cipher should be designed with fast encryption speed and minimal use of resources. Due to the stringent cost constraints inherent in these extremely large applications, the efficient implementation of cryptographic hardware and software algorithms is of utmost importance to realize the vision

of generalized computing. However, the computer complexity inherent in encryption algorithms poses a major challenge. Two interesting surveys on lightweight cryptography can be found in [5] and [6]. In 2016, Beierle, Kranz and Leander [1] have considered Lightweight Multiplication in $\mathbb{F}_{2^n}$. Specifically, they have considered the fundamental question of optimizing finite field multiplications with one fixed element and investigated which field representation, that is which choice of basis, allows for an optimal implementation.

In this paper, the field $\mathbb{F}_{2^n}$ is considered as the n-dimensional vector space over the prime field $\mathbb{F}_2$, and given a basis B, every element of this vector space is uniquely represented as a $\mathbb{F}_2$-linear combination of elements in the basis B. In particular, a multiplication by a fixed element $\alpha \in \mathbb{F}_{2^n}$ becomes a linear transformation over the field $\mathbb{F}_{2^n}$ and this can be identified with a $n \times n$ matrix with entries in $\mathbb{F}_2$. As this representation of a matrix differs according to the choice of basis of $\mathbb{F}_{2^n}$, an efficiency of the multiplication with a fixed element in $\mathbb{F}_{2^n}$ depends on the choice of the field representations, that is, the choice of $\mathbb{F}_2$-basis of $\mathbb{F}_{2^n}$. The particular field representation has a tremendous impact on the efficiency of the multiplication. Here the efficiency of the multiplication is measured by the number of XOR operations needed to implement the multiplication.

In [1], Beierle et al. focused more specifically on the optimal implementation of multiplications with one given element over the field $\mathbb{F}_{2^n}$ and proposed a novel definition of XOR-count to evaluate the efficiency of the multiplication, which is more appropriate to consider the actual number of XOR operations than the definition of the XOR-count proposed in [4]. Note that this improved notion was first introduced by Jean et al. [7].

Considering the field representation with optimal implementation of the multiplication by a fixed element α in $\mathbb{F}_{2^n}$, they present a remarkable result that the multiplication by an element over $\mathbb{F}_{2^n}$ can be implemented with only one XOR-count if and only if the minimal polynomial of the element is a trinomial of degree n. As a generalization, they propose an open problem stated as follows:

Conjecture (Conjecture 1 of [1]): For an element $\alpha \in \mathbb{F}_{2^n}$ with two XOR-count, the minimal polynomial m_α is of Hamming weight 5.

This open conjecture was based on their computer search to find optimal bases for small fields of dimension smaller or equal to eight. Their search results showed that the converse statement of the conjecture is wrong.

In this paper, we prove the above conjecture. The remainder of this paper is organized as follows. In Section 2, we introduce some notation and definitions, and provide some propositions which are useful for the later proofs. In Section 3 we prove that the conjecture is correct.

2 Preliminaries

In this section, we introduce some notations and definitions. We also survey some useful results in [1] for discussions in next sections. Note that our description in this section closely follows the one given in [1].

2.1 Notation and basic facts

For a prime p, 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 a 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 0_n will denote the *zero matrix* and I_n will be the *identity matrix*. $E_{i,j} \in \mathrm{Mat}_n(\mathbb{F}_2)$ denotes the matrix which consists of all zeros except in the i-th row of the j-th column for $i, j \in \{1, \ldots, n\}$. Also, $A^{(i,j)} \in Mat_n(\mathbb{F}_2)$ denotes the $(n-1) \times (n-1)$ submatrix of A formed by deleting the i-th row and j-th column of A. In addition, $A^{(i_1,j_1)(i_2,j_2)}$ stands for $\left(A^{(i_1,j_1)}\right)^{(i_2,j_2)}$ and when $i_1 \neq i_2$ and $j_1 \neq j_2$, $A^{(i_1,j_1),(i_2,j_2)}$ denotes the $(n-2) \times (n-2)$ submatrix obtained by deleting the i_1, i_2-th rows and j_1, j_2-th columns in A. We denote a block diagonal matrix consisting of d matrix blocks A_k as $\bigoplus_{k=1}^{d} A_k$. If P is a matrix with only one non-zero in each row and each column, then P is called a *permutation matrix*. The characteristic polynomial of a matrix A is defined as $\chi_A :=\det(A+\lambda I) \in \mathbb{F}_2[\lambda]$ and the minimal polynomial is denoted by m_A. Recall that the minimal polynomial is the (monic) polynomial p of least degree, such that $p(A) = 0_n$. It is a well-known fact that the minimal polynomial divides the characteristic polynomial, thus $\chi_A(A) = 0_n$. 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. 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. For a polynomial of degree n

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

the *companion matrix* of q is defined as

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

Now, it is well known that $\chi_{C_q} = m_{C_q} = q$.

For any two matrix A and A' in $\mathrm{Mat}_n(\mathbb{F}_2)$, if $A' = TAT^{-1}$ for some invertible $T \in \mathrm{Mat}_n(\mathbb{F}_2)$ then A and A' are called *similar* (resp. *permutation-similar* if T is a permutation matrix) and denoted by $A \sim B$ (resp. $A \sim_\pi B$ for permutation-similarity).

The field $\mathbb{F}_{2^n}$ can be considered as the n-dimensional vector space over the field $\mathbb{F}_2$, and given a basis B, every element of this vector space is uniquely

represented as a $\mathbb{F}_2$-linear combination of elements in the basis B. In particular, a multiplication by a fixed element $\alpha \in \mathbb{F}_{2^n}$ becomes a linear transformation over the field $\mathbb{F}_{2^n}$ and this can be identified with a $n \times n$ matrix with entries in $\mathbb{F}_2$. This matrix depends on the choice of basis of $\mathbb{F}_{2^n}$, which is denoted by $M_{\alpha,B}$. For any two bases B and B', there is a invertible matrix T called the *matrix of basis transformation* such that $M_{\alpha,B} = TM_{\alpha,B'}T^{-1}$.

2.2 XOR-count and some useful propositions

In [4], it is considered that $A \in \mathrm{Mat}_n(\mathbb{F}_2)$ has an XOR-count of t if and only if A can be written as $A = P + \sum_{k=1}^{t} E_{i_k,j_k}$. However the such construction does not reflect all possible matrices which can be implemented with at most t XOR operations. Authors of [1] provided a tight definition for XOR-count.

Definition 1 ([1]). *If t is the minimal number such that an invertible matrix 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, A has XOR-count of t, denoted by $wt_{\oplus}(A) = t$, where P is a permutation matrix.

In the above definition, note that the number of factors $(I + E_{i_k,j_k})$ gives an upper bound on the actual XOR-count. In other words, if A can be written as $A = P \prod_{k=1}^{t}(I + E_{i_k,j_k})$, i.e. $\mathrm{wt}_{\oplus}(A) = t$ then the multiplication represented by A can be implemented with at most t XOR operations.

Given $\alpha \in \mathbb{F}_{2^n}$, an XOR-count of α is defined as the minimal XOR-count of matrices $M_{\alpha,B}$ represented the multiplication by α with respect to any basis B.

Below, we introduce some propositions presented in [1] with their proofs.

Proposition 2 ([1]). *If $A \sim_{\pi} A'$ then $wt_{\oplus}(A) = wt_{\oplus}(A')$.*

Proof. Let $wt_{\oplus}(A) = t$ and $A' = QAQ^{-1}$ for a permutation matrix Q which represents the permutation $\sigma \in S_n$. Then $A = P \prod_{k=1}^{t}(I + E_{i_k,j_k})$ and we have $A' = QPQ^{-1} \prod_{k=1}^{t}(I + E_{\sigma(i_k),\sigma^{-1}(j_k)})$ since $(I + E_{i_k,j_k})Q^{-1} = Q^{-1} + E_{i_k,\sigma^{-1}(j_k)} = Q^{-1}(I + E_{\sigma(i_k),\sigma^{-1}(j_k)})$. It follows that $wt_{\oplus}(A') \leq wt_{\oplus}(A)$ and by reverting the above steps we obtain $wt_{\oplus}(A) \leq wt_{\oplus}(A')$. □

Proposition 3 ([1]). $wt_{\oplus}(A) = wt_{\oplus}(A^{-1})$.

Proof. Using the fact that the matrix $I + E_{i,j}$ with $i \neq j$ is an involution and Proposition 2, we get the result.
$\left(P \prod_{k=1}^{t}(I + E_{i_k,j_k})\right)^{-1} = \prod_{k=t}^{1}(I + E_{i_k,j_k})P^{-1} \sim_{\pi} P^{-1} \prod_{k=t}^{1}(I + E_{i_k,j_k})$. □

Proposition 4 ([1]). *For any n-dimensional permutation matrix P,*

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

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 [3]. That is, given the permutations $\sigma, \tau \in S_n$ as

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

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 $\pi\sigma\pi^{-1} = (d_1, 1, 2, \ldots, d_1 - 1)(d_2, d_1 + 1, d_1 + 2, \ldots, d_2 - 1) \cdots (d_m, d_{m-1} + 1, d_{m-1} + 2, \ldots, d_m - 1)$. 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 5 ([1]).

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

for some permutation $\sigma \in S_n$. *Here, we note that* $\sigma(i_k) \neq \sigma^{-1}(j_k)$ *from the invertibility of the given matrix.*

The following theorem which is a main theoretical result of [1] characterizes elements with a lowest XOR-count over $\mathbb{F}_{2^n}$.

Theorem 6 ([1]). *Let* $\alpha \in \mathbb{F}_{2^n}$. *Then* $wt_\oplus(M_{\alpha,B}) = 1$ *for some basis* B *if and only if* m_α *is a trinomial of degree* n.

The theorem shows that one cannot hope to implement the constant multiplication with only one XOR-count over fields $\mathbb{F}_{2^n}$ for such n that there is no any irreducible trinomial of degree n, for example, multiple of 8. For extension fields of such degree, we can expect the XOR-count of 2 as optimal implementation. In below, a conjecture suggested by authors of [1] is introduced.

Conjecture 7 (Conjecture 1 of [1]). If $\mathrm{wt}_\oplus(M_{\alpha,B}) = 2$ for some basis B then m_α is of weight smaller or equal to 5.

Note that the converse of the conjectured statement is wrong as seen in Tables of [1].

3 A proof of the conjecture

In this section, we will prove that the conjecture is correct. The following theorem, which is a major task of this work, formalizes the conjecture again.

Theorem 8. *Conjecture 7 is true: if* $wt_{\oplus}(M_{\alpha,B}) = 2$ *for some basis* B *then* m_α *is of weight smaller or equal to 5.*

As a preliminary for proving, we provide some necessary facts and brief computations.

Proposition 9. *Elements with the same minimal polynomial have the same XOR-count.*

Proof. Let α, β be different roots of irreducible polynomial $f(x) \in \mathbb{F}_2[x]$ of degree m and let $B = \{b_1, \ldots, b_m\}$ be a $\mathbb{F}_2$-basis of $\mathbb{F}_{2^m}$ such that $\mathrm{wt}_{\oplus}(\alpha)$=$\mathrm{wt}_{\oplus}(M_{\alpha,B})$, i.e. which gives the lowest XOR-count for the multiplication with α. And let $\sigma \in Gal(\mathbb{F}_{2^m}/\mathbb{F}_2)$ map α to β. From the definition of the matrix of the linear transformation,

$$\begin{pmatrix} \alpha b_1 \\ \vdots \\ \alpha b_m \end{pmatrix} = M_{\alpha,B} \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$$

and by the action of σ, we have

$$\begin{pmatrix} \beta\sigma(b_1) \\ \vdots \\ \beta\sigma(b_m) \end{pmatrix} = M_{\alpha,B} \begin{pmatrix} \sigma(b_1) \\ \vdots \\ \sigma(b_m) \end{pmatrix},$$

which shows that $M_{\alpha,B} = M_{\beta,\sigma(B)}$ since $\sigma(B) = \{\sigma(b_1), \ldots, \sigma(b_m)\}$ is also a basis of $\mathbb{F}_{2^m}$. Thus $\mathrm{wt}_{\oplus}(\beta) \leq \mathrm{wt}_{\oplus}(\alpha)$. Similarly, we can also get $\mathrm{wt}_{\oplus}(\alpha) \leq \mathrm{wt}_{\oplus}(\beta)$. □

Proposition 10. *Let* $\alpha \in \mathbb{F}_{2^n}$ *be algebraic element of degree* m*, i.e.* $\mathbb{F}_2(\alpha) = \mathbb{F}_{2^m} \subset \mathbb{F}_{2^n}$ *and let* B *be any basis of* $\mathbb{F}_{2^n}$ *over* $\mathbb{F}_2$*. Then* $\chi_{M_{\alpha,B}} = (m_\alpha)^d$*, where* $d = n/m$*.*

Proof. Since $\chi_{M_{\alpha,B}}$ is independent of the choice of the basis, it is sufficient that we consider about a specified basis. As a such basis, we can construct as follows: let's take the polynomial basis $\{1, \alpha, \alpha^2, \ldots, \alpha^m\}$ of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$ and the polynomial basis $\{1, \beta, \beta^2, \ldots, \beta^d\}$ of $\mathbb{F}_{2^n}$ over $\mathbb{F}_{2^m}$. Now, $B = \{1, \alpha, \ldots, \alpha^m;\ \beta, \beta\alpha, \ldots, \beta\alpha^m;\ \ldots\ ;\ \beta^d, \beta^d\alpha, \ldots, \beta^d\alpha^m\}$ becomes a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ and, with respect to this basis, we have $M_{\alpha,B} = \bigoplus_{k=1}^{d} C_{m_\alpha}$. Thus $\chi_{M_{\alpha,B}} = (\chi_{C_{m_\alpha}})^d = (m_\alpha)^d$. □

Proposition 11. *Let* $f \in \mathbb{F}_2[x]$ *be a irreducible polynomial and suppose that* $wt(f) \geq 5$*. Then* $wt(f^d) \geq 5$ *for any integer* $d \geq 1$*.*

Proof. Let $f(x) = x^{n_1} + x^{n_2} + \cdots + x^{n_k} + 1$, where $n_1 > n_2 > \cdots > n_k \geq 1$ and $k \geq 4$. Since $\mathrm{wt}(f^2) = \mathrm{wt}(f)$, we can assume that d is odd. Then $f(x)^d = (x^{n_1} + x^{n_2} + \cdots + x^{n_k} + 1)^d = x^{dn_1} + dx^{(d-1)n_1+n_2} + \cdots + dx^{n_k} + 1$. Since d is odd, $\mathrm{wt}(f^d) \geq 4$. Considering that f is irreducible, $f(1) = 1$ and so $f(1)^d = 1$. Thus $\mathrm{wt}(f^d)$ is a odd and we obtain $\mathrm{wt}(f^d) \geq 5$. □

Proposition 12. *(i) The matrix $I + E_{i,j}$ with $i \neq j$ is a involution, i.e. $(I + E_{i,j})^{-1} = I + E_{i,j}$, and $\det(I + E_{i,j}) = 1$.*
(ii) For any matrix $A \in \mathrm{Mat}_n(\mathbb{F}_2)$, $\det(A + E_{i,j}) = \det(A) + \det(A^{(i,j)})$.
(iii) For any integer $i, j \in \{1, 2, \ldots, n\}$,

$$\det\left((C_{x^n+1} + \lambda I)^{(i,j)}\right) = \begin{cases} \lambda^{i-j-1} & (i > j) \\ \lambda^{n+i-j-1} & (i \leq j) \end{cases}. \tag{1}$$

Furthermore, the determinant of a matrix $(C_{x^n+1} + \lambda I)^{(i_1,j_1)(i_2,j_2)}$ is zero or λ^k for some integer $k \geq 0$.

Proof. (i) and (ii) of the proposition are trivial from the fundamental properties of matrix theory.
(iii) We define the $m \times m$ matrices H_m^λ and S_m^λ as the following:

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

If $i \leq j$ then the matrix $(C_{x^n+1} + \lambda I)^{(i,j)}$ has the following form:

$$U = \begin{pmatrix} H_{i-1}^\lambda & & \\ & S_{j-i}^\lambda & 1 \\ & & H_{n-j}^\lambda \end{pmatrix}$$

and $\det(C_{x^n+1} + \lambda I)^{(i,j)} = \det(H_{i-1}^\lambda) \cdot \det(S_{j-i}^\lambda) \cdot \det(H_{n-j}^\lambda) = \lambda^{n-j+i-1}$.

If $i > j$ then, by moving the first row to the last row in the matrix $(C_{x^n+1} + \lambda I)^{(i,j)}$ without the change of the determinant, we get the following matrix:

$$V = \begin{pmatrix} S_{j-1}^\lambda & & \\ & H_{i-j-1}^\lambda & \\ \lambda & & S_{n-i+1}^\lambda \end{pmatrix}.$$

Thus, $\det(C_{x^n+1} + \lambda I)^{(i,j)} = \det V = \lambda^{i-j-1}$.

Now we consider $\det U^{(k,l)}$ and $\det V^{(k,l)}$ in order to evaluate the determinant of the matrix $(C_{x^n+1} + \lambda I)^{(i,j)(k,l)}$.

If the (k,l)-entry of U belongs to a diagonal block matrix H^λ or S^λ of the matrix, then $\det U^{(k,l)}$ is λ^d for some integer $d \geq 0$. If the entry belongs to an upper part of diagonal blocks of U, then $\det U = \det(U + E_{k,l})$ and thus

$\det U^{(k,l)} = \det(U + E_{k.l}) - \det U = 0$. In the case that the (k,l)-entry of U belongs to a lower part of diagonal blocks, if the k-th row and l-th column of U cross to the blocks H^{λ}_{n-j} and H^{λ}_{i-1} respectively, then $\det U^{(k,l)} = \lambda^d$ for some integer $d \geq 0$ because the matrix obtained by moving the first row to the last row in $U^{(k,l)}$ becomes a block diagonal matrix with H^{λ} or S^{λ} form as diagonal blocks. Otherwise, since

$$\det U^{(k,l)} = \det \begin{pmatrix} H^{\lambda}_{i-1} & \\ & S^{\lambda}_{j-i} \end{pmatrix}^{(k,l)} \cdot \det H^{\lambda}_{n-j}$$

or

$$\det U^{(k,l)} = \det H^{\lambda}_{i-1} \cdot \det \begin{pmatrix} S^{\lambda}_{j-i} & \\ & H^{\lambda}_{n-j} \end{pmatrix}^{(k',l')},$$

and

$$\det \begin{pmatrix} H^{\lambda}_{i-1} & \\ & S^{\lambda}_{j-i} \end{pmatrix}^{(k,l)} = \det \begin{pmatrix} S^{\lambda}_{j-i} & \\ & H^{\lambda}_{n-j} \end{pmatrix}^{(k',l')} = 0,$$

we obtain $\det U^{(k,l)} = 0$.

In the similar way, we can also obtain the same result for $\det V^{(k,l)}$. Therefore $\det(C_{x^n+1} + \lambda I)^{(i,j)(k,l)}$ is zero or λ^d for some integer $d \geq 0$. □

Corollary 13. *The characteristic polynomial of the matrix $C_{x^n+1}(I + E_{i,j})$ is a trinomial. Precisely,*

$$\det\Big(C_{x^n+1}(I + E_{i,j}) + \lambda I\Big) = \begin{cases} \lambda^n + \lambda^{i-j} + 1 & (i > j) \\ \lambda^n + \lambda^{n+i-j} + 1 & (i \leq j) \end{cases}. \tag{2}$$

Proof.

$$\begin{aligned} \chi_M &= \det(C_{x^n+1}(I + E_{i,j}) + \lambda I) \\ &= \det(C_{x^n+1} + \lambda(I + E_{i,j})) \quad \text{(by Proposition 12, (i))} \\ &= \det((C_{x^n+1} + \lambda I) + \lambda E_{i,j}) \\ &= \det(C_{x^n+1} + \lambda I) + \lambda \det\Big((C_{x^n+1} + \lambda I)^{(i,j)}\Big) \quad \text{(by Proposition 12, (ii))} \\ &= \begin{cases} \lambda^n + 1 + \lambda^{i-j} & (i > j) \\ \lambda^n + 1 + \lambda^{n+i-j} & (i \leq j) \end{cases} \quad \text{(by Proposition 12, (iii)).} \end{aligned}$$

□

Let $\alpha \in \mathbb{F}_{2^n}^*$ be given. As mentioned in Section 2, by using a cycle normal form, the matrix $M_{\alpha,B}$ representing the multiplication with α can be written as follows:

$$M_{\alpha,B} = \left(\bigoplus_{k=1}^{s} C_{x^{m_k}+1}\right) \prod_{k=1}^{t} (I + E_{i_k,j_k}), \tag{3}$$

where $\sum_{k=1}^{s} m_k = n$ and $m_1 \geq \cdots \geq m_s \geq 1$, and $i_k \neq j_k$ for all k.

Lemma 14. *Let $\alpha \in \mathbb{F}_{2^n}^*$ and $\alpha \neq 1$. If $\mathrm{wt}_{\oplus}(M_{\alpha,B}) = 2$, then the number of blocks in the cycle normal form is less or equal to 2, i.e. $s \leq 2$.*

Proof. Since $\mathrm{wt}_{\oplus}(M_{\alpha,B}) = 2$, we have $M_{\alpha,B} = \left(\bigoplus_{k=1}^{s} C_{x^{m_k}+1}\right)(I + E_{i_1,j_1})(I + E_{i_2,j_2})$. In general, the matrix $A(I+E_{i,j})$ can be obtained by adding the i-th column of A to j-th column of A. Thus $M_{\alpha,B}$ can be obtained by changing at most two columns, i.e. j_1-th column and j_2-th column, in the matrix $\bigoplus_{k=1}^{s} C_{x^{m_k}+1}$. If we suppose that $s \geq 3$, then neither j_1 nor j_2-th column crosses at least one block $C_{x^{m_k}+1}$ in the matrix. Thus $\chi_{M_{\alpha,B}}$ is divided by $\chi_{C_{x^{m_k}+1}} = x^{m_k} + 1$ and so by $x + 1$. Since $\chi_{M_{\alpha,B}} = (m_\alpha)^d$ for some integer d (from Proposition 10), we get $m_\alpha = x + 1$ which contradicts to $\alpha \neq 1$. □

Proof of Theorem 8. Let $\mathbb{F}_2(\alpha) = \mathbb{F}_{2^m} \subset \mathbb{F}_{2^n}$ and let the XOR-count of α be two, that is $\mathrm{wt}_{\oplus}(M_{\alpha,B}) = 2$ for some basis B of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. From Lemma 14, $M_{\alpha,B}$ can be represented by either

$$M_{\alpha,B} = C_{x^n+1}(I + E_{i_1,j_1})(I + E_{i_2,j_2}) \tag{4}$$

or

$$M_{\alpha,B} = \left(C_{x^{m_1}+1} \bigoplus C_{x^{m_2}+1}\right)(I + E_{i_1,j_1})(I + E_{i_2,j_2}), \tag{5}$$

where $m_1 + m_2 = n$ and $m_1 \geq m_2 \geq 1$.

1) The Case that $M_{\alpha,B} = C_{x^n+1}(I + E_{i_1,j_1})(I + E_{i_2,j_2})$

In this case we first show that the Hamming weight of the characteristic polynomial of $M_{\alpha,B}$ is less or equal to 5:

$$\begin{aligned}
\chi_{M_{\alpha,B}} &= \det(C_{x^n+1}(I + E_{i_1,j_1})(I + E_{i_2,j_2}) + \lambda I) \\
&= \det(C_{x^n+1}(I + E_{i_1,j_1}) + \lambda(I + E_{i_2,j_2})) \\
&= \det(C_{x^n+1}(I + E_{i_1,j_1}) + \lambda I + \lambda E_{i_2,j_2})) \\
&= \det(C_{x^n+1}(I + E_{i_1,j_1}) + \lambda I) + \lambda \det\left(\left(C_{x^n+1}(I + E_{i_1,j_1}) + \lambda I\right)^{(i_2,j_2)}\right) \\
&= \lambda^n + \lambda^{(n+)i_1-j_1} + 1 + \lambda \det\left(\left(C_{x^n+1} + \lambda I + E_{\sigma(i_1),j_1}\right)^{(i_2,j_2)}\right),
\end{aligned}$$

where σ is a permutation corresponding to C_{x^n+1}, which is defined as:

$$\sigma(i) = \begin{cases} i+1, & i \in \{1, \ldots, n-1\} \\ 1, & i = n \end{cases}.$$

If either $\sigma(i_1) = i_2$ or $j_1 = j_2$, then

$$\begin{aligned}
\phi(\lambda) :&= \det\left(\left(C_{x^n+1} + \lambda I + E_{\sigma(i_1),j_1}\right)^{(i_2,j_2)}\right) \\
&= \det\left(\left(C_{x^n+1} + \lambda I\right)^{(i_2,j_2)}\right) = \lambda^{(n+)i_2-j_2}
\end{aligned}$$

and otherwise, for some indices i' and j' in $\{1, \ldots, n-1\}$,

$$\begin{aligned}\phi(\lambda) &= \det\left(\left(C_{x^n+1} + \lambda I\right)^{(i_2,j_2)} + E_{i',j'}\right) \\ &= \det\left(\left(C_{x^n+1} + \lambda I\right)^{(i_2,j_2)}\right) + \det\left(\left(C_{x^n+1} + \lambda I\right)^{(i_2,j_2)(i',j')}\right),\end{aligned}$$

which is a binomial at most from Proposition 12, (iii). Thus the Hamming weight of $\chi_{M_{\alpha,B}}$ is smaller or equal to 5.

Next, we show that the extension degree of $\mathbb{F}_{2^n}$ over $\mathbb{F}_{2^m}$, that is $d = n/m$, is at most two in the case considered now.

Suppose that $d \geq 3$ in order to yield a contradiction. Then the minimal polynomial of α with coefficients in $\mathbb{F}_2$

$$m_\alpha = x^m + c_{m-1}x^{m-1} + \cdots + c_1 x + 1 \tag{6}$$

has a degree $m \leq \frac{n}{3}$ because $\chi_{M_{\alpha,B}} = (m_\alpha)^d$.

Let $B = \{b_1, b_2, \ldots, b_n\}$ be a basis which gives the form (4). Observing the each column of the matrix $M_{\alpha,B}$ that represents the multiplication with α, non-zero in the $k(\neq j_1, j_2)$-th column is only $(k+1)$-th entry. Thus we obtain the following a list of equalities with respect to the basis. (We assume $j_1 \leq j_2$ without loss of generality.)

$$\begin{aligned}\alpha b_1 &= b_2 \\ &\vdots \\ \alpha b_{j_1-1} &= b_{j_1} \\ \alpha b_{j_1+1} &= b_{j_1+2} \\ &\vdots \\ \alpha b_{j_2-1} &= b_{j_2} \\ \alpha b_{j_2+1} &= b_{j_2+2} \\ &\vdots \\ \alpha b_n &= b_1.\end{aligned} \tag{7}$$

Now, set $\beta := b_{j_1+1}$ and $\gamma := b_{j_2+1}$, then from (7), we obtain

$$\begin{aligned}(b_{j_1+1}, b_{j_1+2}, \ldots, b_{j_2}) &= (\beta, \alpha\beta, \ldots, \alpha^{j_2-j_1-1}\beta), \\ (b_{j_2+1}, \ldots, b_n, b_1, \ldots, b_{j_1}) &= (\gamma, \alpha\gamma, \ldots, \alpha^{n-(j_2-j_1)-1}\gamma).\end{aligned}$$

If $j_2 - j_1 > \frac{n}{2}$, then by multiplying β to both sides of (6) and substituting α, we obtain

$$\alpha^m\beta + c_{m-1} \cdot \alpha^{m-1}\beta + \cdots + c_1 \cdot \alpha\beta + \beta = 0,$$

which means that a sublist $(\beta, \alpha\beta, \ldots, \alpha^m\beta)$ of the list $(b_{j_1+1}, b_{j_1+2}, \ldots, b_{j_2})$ is linear dependent, this is contradictory to linear independence of basis. If

$j_2 - j_1 \leq \frac{n}{2}$ then by multiplying γ to both sides of (6) we also get a contradiction that a sublist $(\gamma, \alpha\gamma, \ldots, \alpha^m\gamma)$ of the list $(b_{j_2+1}, \ldots, b_n, b_1, \ldots, b_{j_1})$ is linear dependent.

Therefore, $d \leq 2$ and we have $\chi_{M_{\alpha,B}} = m_\alpha$ or $\chi_{M_{\alpha,B}} = (m_\alpha)^2$ from Proposition 10. Thus we obtain $\mathrm{wt}(m_\alpha) = \mathrm{wt}(\chi_{M_{\alpha,B}}) \leq 5$.

2) The case that $M_{\alpha,B} = (C_{x^{m_1}+1} \bigoplus C_{x^{m_2}+1})\,(I + E_{i_1,j_1})(I + E_{i_2,j_2})$

In this case, following the proof of Lemma 14, each of j_1 and j_2-th column of $M_{\alpha,B}$ has to cross the different blocks in the matrix. Without loss of generality, let j_1-th column cross the block $C_{x^{m_1}+1}$ and j_2-th one cross the block $C_{x^{m_2}+1}$, that is, we can assume that $j_1 \in \{1, \ldots, m_1\}$ and $j_2 \in \{m_1 + 1, \ldots, n\}$.

Setting $P := C_{x^{m_1}+1} \bigoplus C_{x^{m_2}+1}$, we have

$$\begin{aligned} \chi_{M_{\alpha,B}} &= \det\left(P(I + E_{i_1,j_1})(I + E_{i_2,j_2}) + \lambda I\right) \\ &= \det\left(P(I + E_{i_1,j_1}) + \lambda(I + E_{i_2,j_2})\right) \\ &= \det\left(P + \lambda I + E_{\sigma(i_1),j_1} + \lambda E_{i_2,j_2}\right), \end{aligned} \tag{8}$$

where σ is a permutation corresponding to P which is defined as

$$\sigma(i) = \begin{cases} 1 & \text{if } i = m_1, \\ m_1 + 1 & \text{if } i = n, \\ i + 1 & \text{otherwise.} \end{cases} \tag{9}$$

If both $\sigma(i_1)$ and i_2 are in $\{1, \ldots, m_1\}$ or both in $\{m_1 + 1, \ldots, n\}$, then from (8) $\chi_{M_{\alpha,B}} = (m_\alpha)^d$ is divided by $\chi_{C_{x^{m_2}+1}} = x^{m_2} + 1$ or $\chi_{C_{x^{m_1}+1}} = x^{m_1} + 1$, so by $x + 1$. Thus we get $m_\alpha = x + 1$, which is contradictory to $\alpha \neq 1$.

Now we consider two cases:

(i) If $\sigma(i_1) \in \{1, \ldots, m_1\}$ and $i_2 \in \{m_1 + 1, \ldots, n\}$, then we have

$$\begin{aligned} &\chi_{M_{\alpha,B}} = (m_\alpha)^d = \\ &= \det(C_{x^{m_1}+1} + \lambda I_{m_1} + E_{\sigma(i_1),j_1}) \cdot \det(C_{x^{m_2}+1} + \lambda I_{m_2} + \lambda E_{i_2-m_1,j_2-m_1}). \end{aligned}$$

Thus, $\det(C_{x^{m_1}+1} + \lambda I_{m_1} + E_{\sigma(i_1),j_1}) = (m_\alpha)^{d_1}$ for some integer d_1. From Corollary 13, the left side is at most a trinomial and by applying Proposition 11, we obtain $\mathrm{wt}(m_\alpha) < 5$.

(ii) If $i_2 \in \{1, \ldots, m_1\}$ and $\sigma(i_1) \in \{m_1 + 1, \ldots, n\}$, then we have

$$
\begin{aligned}
\chi_{M_{\alpha,B}} &= \det(P+\lambda I+E_{\sigma(i_1),j_1})+\lambda\det\left((P+\lambda I+E_{\sigma(i_1),j_1})^{(i_2,j_2)}\right)\\
&= \det(C_{x^{m_1}+1}+\lambda I)\cdot\det(C_{x^{m_2}+1}+\lambda I)+\\
&\qquad +\lambda\det\left((P+\lambda I)^{(i_2,j_2)}\right)+\lambda\det\left((P+\lambda I)^{(i_2,j_2),(\sigma(i_1),j_1)}\right)\\
&= (\lambda^{m_1}+1)(\lambda^{m_2}+1)+\lambda\Big(\det(P+\lambda I+E_{i_2,j_2})-\det(P+\lambda I)\Big)+\\
&\qquad +\lambda\det\left((P+\lambda I)^{(i_2,j_1),(\sigma(i_1),j_2)}\right)\\
&= (\lambda^{m_1}+1)(\lambda^{m_2}+1)+\\
&\qquad +\lambda\det\left((C_{x^{m_1}+1}+\lambda I_{m_1})^{(i_2,j_1)}\right)\det\left((C_{x^{m_2}+1}+\lambda I_{m_2})^{(\sigma(i_1),j_2)}\right).
\end{aligned}
$$

Since the last term is a monomial by Proposition 12 (iii), we obtain

$$\mathrm{wt}(\chi_{M_{\alpha,B}})\leq 5. \tag{10}$$

On the other hand, if we suppose that $d\geq 3$ when $\chi_{M_{\alpha,B}}=(m_\alpha)^d$, then the minimal polynomial of α represented by (6) has a degree $m\leq\frac{n}{3}$. Let $B=\{b_1,\ldots,b_n\}$ be a basis generating the matrix (5). Then from the structure of the matrix $M_{\alpha,B}$, we obtain a list of equalities:

$$
\begin{aligned}
\alpha b_1 &= b_2\\
&\vdots\\
\alpha b_{j_1-1} &= b_{j_1}\\
\alpha b_{j_1+1} &= b_{j_1+2}\\
&\vdots\\
\alpha b_{m_1-1} &= b_{m_1}\\
\alpha b_{m_1} &= b_1.
\end{aligned}
$$

Setting $\gamma:=b_{j_1+1}$, we have

$$\{b_{j_1+1},\ldots,b_{m_1},b_1,\ldots,b_{j_1}\}=\{\gamma,\alpha\gamma,\alpha^2\gamma\ldots,\alpha^{m_1-1}\gamma\}.$$

By multiplying γ to both sides of (6) and substituting α, we get

$$\alpha^m\gamma+c_{m-1}\cdot\alpha^{m-1}\gamma+\cdots+c_1\cdot\alpha\gamma+\gamma=0, \tag{11}$$

Since $m\leq n/3$ and $m_1\geq n/2$ by conditions $m_1+m_2=n$ and $m_1\geq m_2$, the list $(\gamma,\alpha\gamma,\ldots,\alpha^m\gamma)$ is a sublist of the list $(b_1,b_2,\ldots,b_{m_1})$, which is linear dependent by (11). This is a contradiction. Thus, $d\leq 2$ and $\mathrm{wt}(m_\alpha)=\mathrm{wt}(\chi_{M_{\alpha,B}})\leq 5$. Consequently, Theorem 8 is proven completely. □

4 Conclusions

In CRTPTO 2016, a study of optimal multiplication bases with respect to the XOR- count has been presented in [1]. The authors have been able to characterize exactly which field elements can be implemented with one XOR operation only, the general case was left open. For small fields of dimension smaller or equal to eight, they were able to compute the optimal bases with the help of an exhaustive computer search. They have conjectured that for an element $\alpha \in \mathbb{F}_{2^n}$ with two XOR-count, the minimal polynomial m_α is of Hamming weight 5. In this paper we confirm the validity of this conjecture and prove it. The proved result can be used to improve the performance of the algorithms in lightweight cryptography.

References

1. Beierle, C., Kranz, T., Leander, G.: Lightweight multiplication in $GF(2^n)$ with application to MDS matrices. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016. LNCS, vol. 9814, pp. 625-653. Springer, Heidelberg (2016)
2. Daemen, J., Rijmen, V.: AES Proposal: Rjindael (1998) http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf.
3. Dummit, D.S., Foote, R.M.: Abstract Algebra. Wiley, Hoboken (2004)
4. 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)
5. Paar, C., Poschmann, A., Kumar, S., Eisenbarth, T., and Uhsadel, L.: A Survey of Lightweight-Cryptography Implementations. In IEEE Design and Test of Computers, vol. 24, pp. 522-533 (2007)
6. Pawar, S. V., Pattanshetti, T.R.: Lightweight-Cryptography: A Survey. In International Research Journal of Engineering and Technology (IRJET), Volume 05 Issue 05 (2018)
7. Jean, J., Peyrin, T., Sim , S. M., Tourteaux, J.: Optimizing Implementations of Lightweight Building Blocks. IACR Transactions on Symmetric Cryptology, pp. 130-168 Vol 4, 2017 (https://tosc.iacr.org/index.php/ToSC/article/view/806). Cryptology ePrint Archive 2017/101(https://eprint.iacr.org/2017/101)
8. Vaudenay, S.: On the need for multipermutations: Cryptanalysis of MD4 and SAFER. In: Preneel, B. (ed.) FSE 1994. LNCS, vol. 1008, pp. 286-297. Springer, Heidelberg (1994)