IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 27, 2021, accepted July 12, 2021, date of publication July 16, 2021, date of current version August 5, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3097914

On the Parity of Power Permutations

PINAR ÇOMAK[1] AND FERRUH ÖZBUDAK[2]
[1]Ericsson Research, 34367 İstanbul, Turkey
[2]Department of Mathematics, Institute of Applied Mathematics, Middle East Technical University, 06800 Ankara, Turkey
Corresponding author: Pinar Çomak (pinar.comak@ericsson.com)

ABSTRACT Side-channel analysis (SCA) attacks and many countermeasures to foil these attacks have been the subject of a large body of research. Different masking schemes have been proposed as countermeasures, one of which is Threshold Implementation (TI), which carries proof of security against DPA even in the presence of glitches. At the same time, it requires a smaller area and uses much less randomness than the other secure masking methods. One of the methods to have an efficient TI of high degree S-boxes is the decomposition method. Our goal in this paper is to analyze the nonlinear components of symmetric cryptographic algorithms. To minimize the area of the protected implementation of cryptographic algorithms, we show the conditions to decompose the substitutions boxes, which are permutations, of high algebraic degree into the ones of lower degree. To find the conditions, we target the decomposition of permutations into quadratic or cubic permutations by considering the power permutations and their parities, which help us determine whether the higher degree permutations are decomposable power permutations or not. Finally, the decomposition results about the finite fields and corresponding lower degree power permutations are presented.

INDEX TERMS Masking, quadratic and cubic permutations, decomposition, symmetric group.

I. INTRODUCTION

Nowadays, side-channel analysis (SCA) is a hot topic for researchers. The most common analysis, differential power analysis (DPA), exploits the correlations between instantaneous power consumption and the cryptographic algorithm's intermediate values.

Several countermeasures are being studied to prevent SCA attacks. One of the secure-proven methods, Threshold implementation (TI), is a Boolean masking technique that randomizes an algorithm's intermediate values and is based on secret sharing and multi-party computation. In [1], TI sharings of all 3×3 and 4×4 substitution boxes (S-box) with 3, 4 or 5 shares are presented. Recall that S-boxes used in many symmetric key algorithms are usually non-linear permutations over a finite field.

One needs at least $d + 1$ shares in order to share a permutation with algebraic degree d [2]. The area requirements of permutations using a different number of shares are well-investigated [3]. To limit the area increase of the protected implementations, we need to keep the number of shares as low as possible.

The associate editor coordinating the review of this manuscript and approving it for publication was Muhammad Imran Tariq.

It is shown that the decrease in the number of shares has a direct impact on the area requirements. In order to achieve this by applying TI with the minimal possible number of shares, one can decompose permutations of higher algebraic degree into lower degree permutations.

In this paper, we focus on the decomposition method, which is described in the literature [4]. In that paper, the conditions to obtain quadratic and cubic permutations over the finite fields $\mathbb{F}_{2^n}$ for values of n between 3 and 16 using Carlitz's Theorem are determined. Then in [5], the decomposition of permutations in $Sym(\mathbb{F}_{2^n})$ for $3 \leq n \leq 31$ is investigated. Also, the decomposition process of permutation is reduced to a modular arithmetic problem, as in this paper. Stafford's Theorem [6], which is stated in Section II, has made us consider the power permutations and their parities in order to investigate when a permutation over a finite field can be decomposed into permutations of lower degree. In Section III, we dive more into the parity of permutations, and then we prove a special case of decomposability of permutations over some finite fields satisfying certain conditions. In Section IV, we provide many lemmas and corollaries that we present our techniques leading us to find the cycle structures and parities of permutations. The cycle structure of power permutation was also studied in [7]. We give the

results from a different point of view, which is much better in computational complexity than the previous ones.

II. PRELIMINARIES

Let $\mathbb{F}_q$ be the finite field $GF(q)$ with $q = 2^n$ elements and $Sym(\mathbb{F}_q)$ denote its symmetric group. We find the values of n such that permutations in $Sym(\mathbb{F}_q)$ can be written as a composition of lower algebraic degree permutations. For the definition of algebraic degree and detailed information on symmetric groups, we refer to [8] and [9], respectively.

A polynomial $f \in \mathbb{F}_q[x]$ is called a *permutation polynomial* of $\mathbb{F}_q$ if the function $f : \mathbb{F}_q \to \mathbb{F}_q$ given by $c \mapsto f(c)$ is a permutation, i.e., f is 1-1 and onto. Given a permutation ψ in $Sym(\mathbb{F}_q)$, there exists the unique permutation polynomial representing ψ. We refer the reader [8], [10]–[14], and [15] for a rigorous information.

Lemma 2.1 [16]: For any function $\psi : \mathbb{F}_q \to \mathbb{F}_q$ there exists a unique polynomial $f \in \mathbb{F}_q[x]$ of degree at most $q-1$ such that the associated polynomial function $f : c \to f(c)$ satisfies $\psi(c) = f(c)$ for all $c \in \mathbb{F}_q$.

Consequently, all permutations considered in this paper are of degrees $\leq q-1$. We recall the following well-known theorem.

Theorem 2.2 [16]: The monomial x^k is a permutation polynomial of $\mathbb{F}_q$ if and only if $gcd(k, q-1) = 1$.

We will refer to permutations induced by monomials x^k as power permutations. The *(algebraic) degree* of a power permutation x^k is defined to be equal to $wt(k)$, where $wt(k)$ denotes the Hamming weight of the n-bit vector corresponding to the binary expansion of k in [8], or equivalently $2-adic$ notation of the number k.

Any permutation can be represented as a composition of disjoint cycles. A cycle is a set of elements in a permutation that switch an element with one another. A cycle with two elements is called a *transposition*. Any permutation can be written as a product of such transpositions. There is no unique way to express a permutation using transpositions; however, their number is either always odd or always even, depending on the permutation. This number corresponds to the parity or the sign of the permutation.

Recall that *Euler's totient function* $\phi(q-1)$ which counts the number of positive integers up to $q-1$ that are relatively prime to $q-1$.

A. COMPOSITION OF PERMUTATIONS

The permutations $\tau_{a,b}$ defined by $x \mapsto ax + b$ for $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$ are called affine permutations. The set $Aff(\mathbb{F}_q) = \{\tau_{a,b} \mid a \in \mathbb{F}_q^*, b \in \mathbb{F}_q\}$ is clearly closed under composition and inversion, hence it is a subgroup of $Sym(\mathbb{F}_q)$.

If there exists a permutation φ, such that φ and $Aff(\mathbb{F}_q)$ together generate $Sym(\mathbb{F}_q)$, then every element ψ of $Sym(\mathbb{F}_q)$ is of the form

$$\psi = \tau_1 \circ \varphi \circ \tau_2 \cdots \circ \varphi \circ \tau_k$$

for some affine permutations $\tau_1, \tau_2, \ldots, \tau_k$. If φ can be decomposed as

$$\varphi = Q_1 \circ Q_2 \circ \ldots Q_m,$$

where Q_i's are permutations of degree d, then ψ is a composition of permutations of degree d

$$\psi = (\tau_1 \circ Q_1) \circ Q_2 \circ \cdots \circ Q_m \circ (\tau_2 \circ Q_1) \circ Q_2 \circ \cdots \circ Q_m \\ \cdots \circ (\tau_{k-1} \circ Q_1) \circ Q_2 \circ \ldots (Q_m \circ \tau_k).$$

Thus, in order to show that every permutation in $Sym(\mathbb{F}_q)$ can be decomposed into permutations of degree d, it is sufficient to show that

- there exists a permutation φ, which can be decomposed into permutations of degree d, and
- φ generates $Sym(\mathbb{F}_q)$ together with $Aff(\mathbb{F}_q)$.

It was shown that every permutation could be written as a composition of affine permutations and the power permutation x^{q-2}, for $q = 5$ by Betti and for $q = 7$ by Dickson, [17]. Later on, Carlitz proved that, for any q, every transposition (0α) can be generated by affine polynomials and the monomial x^{q-2}, where α denotes a fixed non-zero number in $\mathbb{F}_q$, by considering the polynomial:

$$g(x) = -\alpha^2\Big(\big((x-\alpha)^{q-2} + \frac{1}{\alpha}\big)^{q-2} - \alpha\Big)^{q-2}$$

where $g(0) = \alpha$, $g(\alpha) = 0$ and $g(\beta) = \beta$ for $\beta \neq 0, \beta \neq \alpha$. Explanations how the polynomial is constructed are given in [18]. Since every permutation can be written as a composition of transpositions, we have the following.

Theorem 2.3 [19]: The group $Sym(\mathbb{F}_q)$ is generated by the affine permutations and the power permutation x^{q-2}.

In [4], the authors investigated when the power permutation $x^{q-2} = x^{-1}$ for $3 \leq n \leq 16$ can be decomposed into quadratic (or cubic) permutations and found those with a minimum decomposition length. The authors proved that every permutation in $Sym(\mathbb{F}_q)$ can be decomposed into quadratic permutations whenever n is not divisible by 4 and into cubic permutations when n is divisible by 4.

In this paper, we extend this result for larger n values using the following generalization of Carlitz's result. In [6], Stafford generalized the previous result to all power maps with the following result. Namely, instead of using power permutation x^{q-2} (i.e., inverse map), it suffices to use any power permutation x^k under some conditions.

Theorem 2.4 [6]: Let $\mathbb{F}_q$ be the finite field where $q = 2^n$ and let $1 < k < q-2$ be an integer relatively prime to $q-1$. If k is not a power of 2 and the power permutation x^k is an odd permutation, then $Sym(\mathbb{F})$ is generated by the affine permutations $Aff(\mathbb{F}_q)$ and the power permutation x^k.

Suppose we can write a power permutation x^k, which satisfies Stafford's conditions, as a composition of quadratic (or cubic) permutations. In that case, every permutation in $Sym(\mathbb{F}_q)$ can be written as a composition of quadratic (or cubic) permutations.

We aim to find low degree odd permutations x^k over a finite field $\mathbb{F}_{2^n}$ using Stafford's result.

III. PARITY

Recall that transposition is a cycle of length 2. A transposition is odd, and so is any cycle of even length, as it can be written as a product of an odd number of transpositions.

A. ANALYTIC APPROACH

We show how to determine analytically the parity of a power permutation. Let α be a primitive element of the finite field $\mathbb{F}_q$. Then we can write

$$\mathbb{F}_q = \{0, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^{q-2}, \alpha^{q-1} = 1\}$$

Consider the power permutation x^k in $Sym(\mathbb{F}_q)$. That is,

$$x^k : \begin{pmatrix} 0 & \alpha^1 & \alpha^2 & \alpha^3 & \ldots & \alpha^{q-2} & 1 \\ 0 & \alpha^k & \alpha^{2k} & \alpha^{3k} & \ldots & \alpha^{k(q-2)} & 1 \end{pmatrix}$$

In order to determine whether or not the power permutation x^k is odd, it is sufficient to determine its cycle structure. Notice that the elements 0 and 1 are fixed points of x^k and we discard them. We begin writing x^k as a composition of disjoint cycles. The first cycle is of the form

$$[\alpha] = (\alpha^1, \alpha^k, \alpha^{k^2}, \ldots, \alpha^{k^{N_1-1}})$$

where the length of cycle decomposition N_1 is the least positive integer such that

$$k^{N_1} \equiv 1 \ (mod\ q-1).$$

That is, N_1 is the order of k in the multiplicative group $\mathbb{Z}^*_{q-1}$. For the second cycle, if exists, we take the first α^j not included in this cycle and consider $(\alpha^j, \alpha^{kj}, \alpha^{k^2 j}, \ldots)$.

We repeat this procedure until we exhaust all elements.

Since a cycle is even if and only if its length is odd, we should count how many disjoint cycles there are of even length to determine if x^k is odd. Notice that this idea reduces the problem of checking the parity of x^k to a modular arithmetic problem.

B. SPECIAL CASE

The idea in III-A reveals a straightforward theorem below:

Theorem 3.1: Let x^k be a power permutation in $Sym(\mathbb{F}_q)$ of degree d. Assume that $q-1$ is an odd prime number and k is a primitive root of the multiplicative group $\mathbb{Z}^*_{q-1}$. Then every permutation in $Sym(\mathbb{F}_q)$ can be decomposed into permutations of degree d.

Proof 1: Since k is a primitive root of $\mathbb{Z}^*_{q-1}$, the least positive integer i such that $k^i \equiv 1 \ (mod\ q-1)$ is $q-2$. Therefore, the cycle decomposition of x^k is

$$(\alpha^1, \alpha^k, \alpha^{k^2}, \ldots, \alpha^{k^{q-3}})$$

Since the length of this cycle is even, the permutation x^k is odd and hence it generates $Sym(\mathbb{F}_q)$ together with $Aff(\mathbb{F}_q)$ by Theorem 2.4. Consequently, every permutation in $Sym(\mathbb{F}_q)$ can be decomposed into permutations of degree d.

The specific instances of this theorem can be seen for the permutations defined over the finite fields $\mathbb{F}_q$, where $q = 2^n$ and $n = 3, 5, 7, 13, 17, 19, \ldots$ (i.e., the exponents of some Mersenne primes) with $k = 3$.

IV. CYCLE DECOMPOSITION OF PERMUTATIONS

Assume that, using the exhaustive procedure described previously, the permutation x^k can be written in cycle decomposition notation, with disjoint cycles as

$$\underbrace{(\alpha^1, \alpha^k, \alpha^{k^2}, \ldots, \alpha^{k^{N_1-1}})}_{N_1\text{-many elements}} \ldots \underbrace{(\alpha^m, \alpha^{mk}, \ldots, \alpha^{mk^{N_m-1}})}_{N_m\text{-many elements}} \ldots$$

under the assumption that α^m is not included in the previous cycles.

Notation 4.1: We shall denote the length of the cycle $[\alpha^m]$ by N_m. Equivalently, N_m is the minimum positive integer such that $mk^{N_m} \equiv m \mod (q-1)$. In addition, in the case m is a proper divisor of $q-1$, N_m is the order of k in the multiplicative group $(\mathbb{Z}_{q-1/m})^\times$. In general, for any m, N_m is the order of k in the multiplicative group $(\mathbb{Z}_{q-1/\gcd(q-1,m)})^\times$. Throughout the paper, we consider the divisor m's, the subscripts are from $\{1, 2, \cdots, q-2\}$ and unless otherwise indicated, "divisor" is used instead of "proper divisor" in these cases.

Let k be a positive integer less than $q-2$ and relatively prime to $q-1$. Let d be the algebraic weight of k where x^k is a power permutation in $Sym(\mathbb{F}_q)$. For a divisor m of $q-1$, let N_m be the order of k in $(\mathbb{Z}_{q-1/m})^\times$, where $(\mathbb{Z}_{q-1/m})^\times$ is the multiplicative group consisting of invertible elements of $\mathbb{Z}_{q-1/m}$. Then, x^k is odd if and only if N_1 is even and $|S|$ is odd where $S = \{m \mid N_m \text{ is even}\}$.

A. ON THE LENGTH OF THE CYCLES

In this subsection, we start with a useful lemma to show some relations between the lengths of certain cycles of some elements in $\mathbb{F}_q$ in cycle decomposition of the power permutation x^k.

Lemma 4.2: $N_{ms} | N_s$ for all m, s.

Proof 2: Recall that N_s is the minimum positive integer satisfying $\alpha^{sk^{N_s}} = \alpha^s$. So, if we take the m^{th}-power of both sides, we get that

$$\alpha^{msk^{N_s}} = \alpha^{ms}$$

On the other hand, α^{ms} is in the cycle $(\alpha^{ms}, \alpha^{msk}, \alpha^{msk^2}, \ldots, \alpha^{msk^{N_{ms}-1}})$ and so

$$\alpha^{msk^{N_{ms}}} = \alpha^{ms}$$

where N_{ms} is the minimum positive integer satisfying this. Let $N_s = qN_{ms} + r$ for some integers q, r with $0 \le r < N_{ms}$. Assume that $r \neq 0$. Then we have that

$$\begin{aligned} \alpha^{msk^{N_s}} &= \alpha^{ms} \\ \alpha^{msk^{qN_{ms}+r}} &= \alpha^{ms} \\ \alpha^{msk^{qN_{ms}}k^r} &= \alpha^{ms} \\ \left(\alpha^{msk^{qN_{ms}}}\right)^{k^r} &= \alpha^{ms} \\ \left(\left(\ldots\left(\alpha^{msk^{N_{ms}}}\right)^{k^{N_{ms}}}\ldots\right)^{k^{N_{ms}}}\right)^{k^r} &= \alpha^{ms} \end{aligned}$$

where we iteratively exponentiate q times to the power $k^{N_{ms}}$. However, since we have $\alpha^{msk^{N_{ms}}} = \alpha^{ms}$, one obtains that

$\alpha^{msk^r} = \alpha^{ms}$, which contradicts the minimality of N_{ms}. Thus $r = 0$ and so $N_{ms}|N_s$.

The following corollary follows immediately from Lemma 4.2.

Corollary 4.3: We have that $N_m|N_1$ for all m.

The next lemma gives us a stronger result under some conditions.

Lemma 4.4: Let ρ be a divisor of $q-1$ and suppose that $\gcd\left(t, \frac{q-1}{\rho}\right) = 1$. Then $N_{\rho t} = N_\rho$.

Proof 3: Recall that, by the definition of N_ρ, we have that $\alpha^{\rho k^{N_\rho}} = \alpha^\rho$. It follows that $\alpha^{\rho(k^{N_\rho}-1)} = 1$ in $\mathbb{F}_q$. As the order of α in the multiplicative group $\mathbb{F}_q^*$ is $q-1$, we have that

$$q-1|\rho(k^{N_\rho}-1).$$

Moreover, N_ρ is the least positive integer satisfying this relation. Similarly, we know that $\alpha^{\rho t k^{N_{\rho t}}} = \alpha^{\rho t}$ and so $\alpha^{\rho t(k^{N_{\rho t}}-1)} = 1$ in $\mathbb{F}_q$. As before, we have that $q-1|\rho t(k^{N_{\rho t}}-1)$ and so $\frac{q-1}{\rho}|t(k^{N_{\rho t}}-1)$. Since $\gcd\left(t, \frac{q-1}{\rho}\right) = 1$, one can see

$$q-1|\rho(k^{N_{\rho t}}-1).$$

By the minimality of N_ρ, we have that $N_\rho|N_{\rho t}$. Otherwise, after applying the division algorithm to $N_{\rho t}$ and N_ρ as before, and we would obtain $0 < r < N_\rho$ such that $\alpha^{\rho k^r} = \alpha^\rho$ which is equivalent to $q-1|\rho(k^r-1)$. By Lemma 4.2, we also know that $N_{\rho t}|N_\rho$. Hence

$$N_{\rho t} = N_\rho.$$

Again we present an immediate corollary which follows from the Lemma 4.4.

Corollary 4.5: In particular, we have that if $\gcd(t, q-1) = 1$, then $N_t = N_1$.

As one can deduce from the Lemma 4.4, the Euler totient function defined above in Section II, is needed in order to be able to count the number of a part of elements within the cycle of the same length.

B. THE NUMBER OF DISTINCT CYCLES

Let ρ be a divisor of $q-1$. In this subsection, it will be proven that the corresponding cycles are all distinct for a given divisor, and the counting of elements appearing in the cycle decomposition of a permutation is completely done.

Notation 4.6: Set $K_\rho = \phi\left(\frac{q-1}{\rho}\right)$. Let W_ρ denote the set of as $W_\rho = \{t : \gcd\left(t, \frac{q-1}{\rho}\right) = 1 \text{ and } 1 \le t < \frac{q-1}{\rho}\}$. Note that $|W_\rho| = \phi\left(\frac{q-1}{\rho}\right) = K_\rho$. We enumerate the elements of W_ρ as $W_\rho = \{t_1, t_2, \ldots, t_{K_\rho}\}$. Then, for a divisor ρ of $q-1$, we define the list L_ρ of cycles as the following list:

$$\begin{aligned}
[\alpha^{\rho t_1}] &= (\alpha^{\rho t_1}, \alpha^{\rho t_1 k}, \alpha^{\rho t_1 k^2}, \ldots, \alpha^{\rho t_1 k^{N_\rho-1}}) \\
[\alpha^{\rho t_2}] &= (\alpha^{\rho t_2}, \alpha^{\rho t_2 k}, \alpha^{\rho t_2 k^2}, \ldots, \alpha^{\rho t_2 k^{N_\rho-1}}) \\
&\vdots \\
[\alpha^{\rho t_{K_\rho}}] &= (\alpha^{\rho t_{K_\rho}}, \alpha^{\rho t_{K_\rho} k}, \alpha^{\rho t_{K_\rho} k^2}, \ldots, \alpha^{\rho t_{K_\rho} k^{N_\rho-1}}) \qquad (\star)
\end{aligned}$$

Observe that each of these cycles has length N_ρ, since $\gcd(t, \frac{q-1}{\rho}) = 1$ implies that the length of $[\alpha^{\rho t}]$ is the same as the length of $[\alpha^\rho]$, as stated in the Lemma 4.4.

Some of the cycles in $(\star)$ may be identical. Let U_ρ denote the number of *distinct* cycles in this list. In the following lemma we determine U_ρ.

Lemma 4.7: Let ρ be a divisor of $q-1$ and U_ρ denote the number of *distinct* cycles in the list $(\star)$, which is the list determined by ρ as explained above. We have

$$U_\rho = \frac{K_\rho}{N_\rho}$$

where K_ρ and N_ρ is defined in Notation 4.6 and 4.1, respectively.

Proof 4: Since $\gcd(k, q-1) = 1$ and $\gcd\left(t_i, \frac{q-1}{\rho}\right) = 1$, following from $\forall t_i \in W_\rho$, we have that $\gcd\left(t_i k, \frac{q-1}{\rho}\right) = 1$, which implies that $t_i k \mod (\frac{q-1}{\rho})$ is also in the set W_ρ. Hence, one can see that $\alpha^{\rho t_i}$ is counted in at least N_ρ different cycles in the list $\star$. As this holds for any $t \in W_\rho$, we conclude that $N_\rho|K_\rho$ and

$$U_\rho \le \frac{K_\rho}{N_\rho}.$$

We claim that $U_\rho \ge \frac{K_\rho}{N_\rho}$ for every divisor ρ of $q-1$. Assume to the contrary that, for some divisor ρ of $q-1$, we have that $U_\rho < \frac{K_\rho}{N_\rho}$. Then, since every element of $\mathbb{F}_q^*$ is contained in some cycle of this form for some divisor ρ of $q-1$, we would have

$$|\mathbb{F}_q^*| \le \sum_{\rho|q-1} U_\rho N_\rho < \sum_{\rho|q-1} \frac{K_\rho}{N_\rho} N_\rho = \sum_{\rho|q-1} \phi\left(\frac{q-1}{\rho}\right) = q-1$$

which is a contradiction. Hence, $U_\rho = \frac{K_\rho}{N_\rho}$ for every divisor ρ of $q-1$.

Remark 4.8: Note that it is possible to have two distinct divisors ρ_1 and ρ_2 of $q-1$ such that $N_{\rho_1} = N_{\rho_2}$. Therefore, U_{ρ_1} might be strictly less than the number of all cycles of length N_{ρ_1}.

To make it more precise, we give the following toy example for a power permutation defined in a finite field $\mathbb{F}_{2^n}$ with a small value of n because of the cycles being easy to compute.

Example 4.9: Consider the power permutation x^5 over $\mathbb{F}_{2^6}$. So $q-1 = 63 = 3^2 7$. Let $\rho_1 = 1$, $\rho_2 = 3$, $\rho_3 = 7$, $\rho_4 = 9$ and $\rho_5 = 21$, the proper divisors of 63.

- For $\rho_1 = 1$, $W_1 = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20, 22, 23, 25, 26, 29, 31, 32, 34, 37, 38, 40, 41, 43, 44, 46, 47, 50, 52, 53, 55, 58, 59, 61, 62\}$, i.e. the numbers coprime to 63. The distinct cycles in L_1 by computing the cycles of α^{t_i} where $t_i \in W_1$ are:
  - $[\alpha] = (\alpha, \alpha^5, \alpha^{25}, \alpha^{62}, \alpha^{58}, \alpha^{38})$
  - $[\alpha^2] = (\alpha^2, \alpha^{10}, \alpha^{50}, \alpha^{61}, \alpha^{53}, \alpha^{13})$
  - $[\alpha^4] = (\alpha^4, \alpha^{20}, \alpha^{37}, \alpha^{59}, \alpha^{43}, \alpha^{26})$
  - $[\alpha^8] = (\alpha^8, \alpha^{40}, \alpha^{11}, \alpha^{55}, \alpha^{23}, \alpha^{52})$

TABLE 1. K_ρ, N_ρ and U_ρ values for given ρ.

	K_ρ	N_ρ	U_ρ
$\rho = 1$	36	6	6
$\rho = 3$	12	6	2
$\rho = 7$	6	6	1
$\rho = 9$	6	6	1
$\rho = 21$	2	2	1

- $[\alpha^{16}] = (\alpha^{16}, \alpha^{17}, \alpha^{22}, \alpha^{47}, \alpha^{46}, \alpha^{41})$
- $[\alpha^{19}] = (\alpha^{19}, \alpha^{32}, \alpha^{34}, \alpha^{44}, \alpha^{31}, \alpha^{29})$

Note that it is not necessary to compute the cycle $[\alpha^5]$ separately since it is nothing but $[\alpha]$. Clearly it is seen that all elements α^{t_i} satisfying $t_i \in W_1$ are spanned above. 36 elements of $\mathbb{F}_{2^6} \setminus \{0, 1\}$ are located in a cycle. There are 6 different cycles, which confirms with Lemma 4.7 as the values of the total number of elements, $K_1 = \phi(63) = 36$, the number of elements in one cycle $N_1 = 6$ and the number of distinct cycles $U_1 = 6$ in the list L_1.

– For $\rho_2 = 3$, $W_3 = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$. Check the cycles of $\alpha^{3\,t_i}$ where $t_i \in W_3$.
  - $[\alpha^3] = (\alpha^3, \alpha^{15}, \alpha^{12}, \alpha^{60}, \alpha^{48}, \alpha^{51})$
  - $[\alpha^6] = (\alpha^6, \alpha^{30}, \alpha^{24}, \alpha^{57}, \alpha^{33}, \alpha^{39})$

  Again all elements α^{t_i} satisfying $t_i \in W_3$ are spanned. Another 12 elements of $\mathbb{F}_{2^6} \setminus \{0, 1\}$ are located in a cycle.

We continue to apply the same procedure to the rest of divisors with less details. resume

– For $\rho_3 = 7$, $W_7 = \{1, 2, 4, 5, 7, 8\}$ and the only cycle is:
  - $[\alpha^7] = (\alpha^7, \alpha^{35}, \alpha^{49}, \alpha^{56}, \alpha^{28}, \alpha^{14})$
– For $\rho_4 = 9$, $W_9 = \{1, 2, 3, 4, 5, 6\}$ and there is again one cycle:
  - $[\alpha^9] = (\alpha^9, \alpha^{45}, \alpha^{36}, \alpha^{54}, \alpha^{18}, \alpha^{27})$
– For $\rho_5 = 21$, $W_{21} = \{1, 2\}$ and the cycle:
  - $[\alpha^{21}] = (\alpha^{21}, \alpha^{42})$

One can see that each element of $\mathbb{F}_{2^6}$ appears exactly once in the distinct cycles listed above. The values of K_ρ, N_ρ and U_ρ are given together with the divisors ρ, in the Table 1, where $K_\rho = \phi\left(\frac{q-1}{\rho}\right)$, N_ρ is order of k in $(\mathbb{Z}_{q-1/\rho})^\times$ and $U_\rho = \frac{K_\rho}{N_\rho}$.

The cycle structure of the power permutation x^5 over $\mathbb{F}_{2^6}$ can be represented as $[\langle 6, 10\rangle, \langle 2, 1\rangle]$, which means there are 10 different cycles of length 6 and there is 1 cycle of length 2. The cycles of the elements 0 and 1 are not listed in this notation.

In brief, we can give a summary of lemmas and some corresponding examples specific to x^5 defined over $\mathbb{F}_{2^6}$. By the Lemma 4.2, $N_9|N_3$ and $N_{21}|N_7$ etc, where $N_9 = 6$, $N_3 = N_7 = 6$, $N_{21} = 2$. By the Corollary 4.3, $N_\rho|N_1 = 6$ for all divisors ρ. By the Lemma 4.4, $N_{18} = N_9$ since $\gcd(2, 7) = 1$, i.e. $\gcd\left(t, \frac{q-1}{\rho}\right) = 1$. By the Corollary 4.5, $N_2 = N_1$ since $\gcd(2, 63) = 1$. Also as mentioned in the Remark 4.8, one can see that there are some cycles of same length for the elements placed in different lists, for example $N_3 = N_7$. By the Lemma 4.7, we cover all elements in $\mathbb{F}_{2^6}$.

From its cycle structure, one can say that x^5 defined over $\mathbb{F}_{2^6}$ has odd parity since there are odd-many cycles of even length. Afterward, we will decide the parity of a permutation without computing the cycle structure of it.

Corollary 4.10: If N_1 is odd, then permutation is even.

Proof 5: N_1 is odd implies N_m's are all odd, for any $1 \leq m \leq q-2$, since $N_m|N_1$ by Corollary 4.3. Hence regardless of their number of cycles, it forms a even permutation.

Therefore, using Lemma 4.4 and the Lemma 4.7, we arrive at our main Theorem.

Theorem 4.11: Let k be a positive integer less than $q-2$ and relatively prime to $q-1$. Let d be the algebraic weight of k where x^k is a power permutation in $Sym(\mathbb{F}_q)$. For a divisor m of $q-1$, let N_m be the order of k in $(\mathbb{Z}_{\frac{q-1}{m}})^\times$, where $(\mathbb{Z}_{\frac{q-1}{m}})^\times$ is the multiplicative group consisting of invertible elements of $\mathbb{Z}_{\frac{q-1}{m}}$. Then, x^k is odd if and only if N_1 is even and $|S|$ is odd where $S := \{m \mid N_m \text{ is even}\}$.

With the help of this theorem, we can determine the parity of a given power permutation as well as its cycle structure. In the literature, the cycle structure of power permutation ψ_k was also given by Ahmad, in [7] as follows:

Theorem 4.12: Let m be any positive integer. Then x^k has a cycle of length m if and only if $q-1$ has a divisor t such that k belongs to the exponent m modulo t. The exact number T_m of such cycles is

$$T_m = \sum_{e \in C_m} \phi(e)$$

where $C_m = \{t : t|d_m \text{ and } k \text{ belongs to } m \text{ modulo } t$, where $d_m = gcd(k^m - 1, q-1)\}$ and ϕ is Euler's totient function.

By using our method, from a different point of view than the one in [7], which is described in Section IV and which will be described in the following algorithms in detail, one can obtain the cycle structure of a power permutation with a better computational complexity. Moreover, our method gives information also about the parity of the permutation much faster, see the Section V.

V. ALGORITHMS

In order to determine that a permutation is even or not, we provide the following algorithm:

By the algorithm 1, one can determine that the permutation is odd if the count is odd; otherwise, it is even.

Besides, to write the cycle structure of a monomial using our method, we provide the algorithm 2.

Since $q = 2^n$, the number of digits of q, equally $\log(q)$, or $\log(q-1)$ when required, equals to n. First we need to find the divisors of the number $q-1$. This can be done by factorizing having the complexity $\mathcal{O}(exp((64/9)^{1/3} n^{1/3} (\ln(n))^{2/3}))$ with the Generalized Number Field Sieve. The number of divisors are bounded from above with $n^{1/3}$. Then, it will be computed the order of k in $\mathbb{Z}^\times_{q-1/\rho}$, having the complexity

Algorithm 1 The Parity of a Power Permutation x^k

Input: k and $q-1$ such that $gcd(k, q-1) = 1$, count $= 0$
Output: Parity of x^k

```
N_1 ⇐ ord_{Z^×_{q-1}}(k)
if N_1 is odd then
    Print "The permutation is even"
    Stop
else
    while ρ is a proper divisor of q − 1 do
        N_ρ ⇐ ord_{(Z_{q-1/ρ})^×}(k)
        if N_ρ is even then
            U_ρ ⇐ φ((q−1)/ρ)/N_ρ
            if U_ρ is odd then
                count ⇐ count + 1
            end if
        end if
    end while
end if
if count is odd then
    print "The permutation is odd"
else
    print "The permutation is even"
end if
```

Algorithm 2 The Cycle Structure of a Power Permutation x^k

Input: k and $q-1$ such that $gcd(k, q-1) = 1$, count $= 0$, List[a][2], where a is the number of divisors
Output: Cycle Structure of x^k

```
while ρ is a divisor of q − 1 do
    N_ρ ⇐ ord_{Z^×_{q-1}/ρ}(k)
    U_ρ ⇐ φ((q−1)/ρ)/N_ρ
    for i ⇐ 0 to count do
        if N_ρ in List[i][0] then
            List[i][1] ⇐ List[i][1] + U_ρ
            break i
        else
            count ⇐ count + 1
            List[count][0] ⇐ N_ρ
            List[count][1] ⇐ U_ρ
        end if
    end for
end while
print "The cycle structure is:" List[a][2]
```

$\mathcal{O}(\sqrt{N_\rho}) < \mathcal{O}(2^{n/2})$ with Pollard's Rho algorithm. The Euler totient function of $q-1/\rho$ has the complexity $\mathcal{O}(2^{n/2})$ and dividing it by N_ρ for each divisor ρ has relatively small complexity.

In total, both Algorithm 1 and 2 have the complexity:

$$\mathcal{O}(exp((64/9)^{1/3}n^{1/3}(\ln(n))^{2/3})) + \mathcal{O}(n^{1/3}2^n) \approx \mathcal{O}(exp((64/9)^{1/3}n^{1/3}(\ln(n))^{2/3})).$$

In Ahmad's method, there are $q-1$ many choices in the beginning. Then the method calculates a greatest common divisor of $k^m - 1$ and $q-1$ which has complexity $\mathcal{O}(\log(n))$ and finds a divisor of that number with the same complexity as integer factorization then finds the order of k in $\mathbb{Z}_t^\times$ which has $\mathcal{O}(2^{n/2})$ and then Euler totient with $\mathcal{O}(2^{n/2})$ and their sum which has relatively small complexity. In overall it has:

$$\mathcal{O}((2^n-1)\log(n)exp((64/9)^{1/3}n^{1/3}(\ln(n))^{2/3})2^n).$$

VI. RESULTS

In this section, before stating our experimental result, it is given the following lemma, which helps us omit the search for quadratic power permutations in some finite fields.

Lemma 6.1: No quadratic power permutations exist for $n = 2^m$ in $\mathbb{F}_q$ with $q = 2^n$.

Proof 6: For a quadratic power permutation x^k, k should be of the form $k = 2^{j+i} + 2^j$ for some integers i, j with $i > 0$, i.e. the binary representation of quadratic k is $(0\cdots010\cdots010\cdots0)$ where 1's are in the $(j+i)^{th}$ and j^{th} positions from right. Clearly $k = 2^j(2^i+1)$. By Theorem 2.2, x^k being a permutation is equivalent to $gcd(k, q-1) = 1$. So we check whether $gcd(2^j(2^i+1), 2^{2^m}-1) = 1$. It is easily seen that $gcd(2^j(2^i+1), 2^{2^m}-1) = gcd(2^i+1, 2^{2^m}-1)$ and moreover, we have that

- If $gcd(2^i-1, 2^{2^m}-1) = 1$, then
$$\begin{aligned} gcd(2^i+1, 2^{2^m}-1) &= \text{gcd}(2^{2i}-1, 2^{2^m}-1) \\ &= 2^{gcd(2i,2^m)}-1 \\ &\neq 1. \end{aligned}$$
- If $gcd(2^i-1, 2^{2^m}-1) \neq 1$, then
$$\begin{aligned} gcd(2^i+1, 2^{2^m}-1) &= \frac{\text{gcd}(2^{2i}-1, 2^{2^m}-1)}{gcd(2^i-1, 2^{2^m}-1)} \\ &= \frac{2^{gcd(2i,2^m)}-1}{2^{gcd(i,2^m)}-1} \\ &= 2^{gcd(i,2^m)}+1 \\ &\neq 1. \end{aligned}$$

In both cases, since $gcd(k, q-1) \neq 1$, no quadratic power permutations exists in $\mathbb{F}_q$ with $q = 2^{2^m}$.

In this paper, we performed a search for quadratic and cubic power permutations for the values $3 \leq n \leq 141$ using the Algorithm 1 which follows from the Theorem 4.11, and also with the help of the Lemma 6.1.

We now state our experimental results.

Theorem 6.2: Let n be an integer such that $3 \leq n \leq 141$.

- If n is not divisible by 4, then every permutation in $Sym(\mathbb{F}_{2^n})$ can be written as a composition of quadratic and affine permutations.
- If n is divisible by 4, then every permutation in $Sym(\mathbb{F}_{2^n})$ can be written as a composition of cubic and affine permutations.
  - Moreover, if n is a power of 2, then every permutation in $Sym(\mathbb{F}_{2^n})$ can be written as a composition of x^{13} and affine permutations.

- $Sym(\mathbb{F}_{2^n})$ cannot be generated by the quadratic power permutations and the affine permutations.

One can find these decomposition results to any permutation in $GF(2^n)$ in [4] for the values $3 \leq n \leq 16$, and in [5] for the values $3 \leq n \leq 31$.

We performed a search for quadratic and cubic power permutations for various values of n, using C and MAGMA [20]. Based on the computational evidence, we conjecture the following:

Conjecture 6.3:

- For all $n \geq 1$, the power permutation x^3 is odd in $Sym(\mathbb{F}_{2^{2n+1}})$.
- For all $n \geq 1$, the power permutation x^5 is odd in $Sym(\mathbb{F}_{2^{4n+2}})$ and $Sym(\mathbb{F}_{2^{4n+3}})$.
- For all n which is a multiple of 4 and not a power of 2, all quadratic permutations of $\mathbb{F}_{2^n}$ are even.

VII. CONCLUSION

In this paper, we have provided two algorithms, one determining the parity and the other finding the cycle structure of a given power permutation. We also gave the complexities of the algorithms. The comparison with the previously known method showed that our approach is $2^n - 1$ times less complex. Using our method, we also extended the previous results: Any permutation on $\mathbb{F}_{2^n}$ where $3 \leq n \leq 141$ can be decomposed in quadratic permutations, when n is not divisible by 4 and in cubic permutations, otherwise. We have left some conjectures: "Are the power permutations x^3 and x^5 odd in $Sym(\mathbb{F}_{2^n})$ where n is not multiple of 4?" and "Are all quadratic power permutations even in $Sym(\mathbb{F}_{2^{4n}})$?".

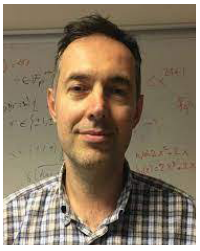
ACKNOWLEDGMENT

The authors are grateful to Burak Kaya from METU for his insightful and valuable conversations and Alexander Maximov from Ericsson for his useful comments on this manuscript.

REFERENCES

[1] B. Bilgin, S. Nikova, V. Nikov, V. Rijmen, and G. Stütz, "Threshold implementations of all 3 × 3 and 4 × 4 S-boxes," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.*, 2012, pp. 76–91.
[2] S. Nikova, C. Rechberger, and V. Rijmen, "Threshold implementations against side-channel attacks and glitches," in *Proc. Int. Conf. Inf. Commun. Secur.* Springer, 2006, pp. 529–545.
[3] B. Bilgin, "Threshold implementations: As countermeasure against higher-order differential power analysis," Ph.D. dissertation, Dept. Electr. Eng., Katholieke Universiteit Leuven, Leuven, Belgium, 2015.
[4] S. Nikova, V. Nikov, and V. Rijmen, "Decomposition of permutations in a finite field," IACR Cryptol. ePrint Arch., Tech. Rep., 2018, p. 103, vol. 2018.
[5] P. Çomak, S. Nikova, and V. Rijmen, "On decomposition of permutations," in *Cryptography and Information Security in the Balkans*. 2018.
[6] R. M. Stafford, "Groups of permutation polynomials over finite fields," *Finite Fields Their Appl.*, vol. 4, no. 4, pp. 450–452, Oct. 1998.
[7] S. Ahmad, "Cycle structure of automorphisms of finite cyclic groups," *J. Combinat. Theory*, vol. 6, no. 4, pp. 370–374, May 1969.
[8] C. Carlet, "Vectorial Boolean functions for cryptography," in *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, vol. 134. 2010, pp. 398–469.
[9] I. N. Herstein, *Abstract Algebra*. Upper Saddle River, NJ, USA: Prentice-Hall, 1996.
[10] G. L. Mullen and D. Panario, *Handbook of Finite Fields*. Boca Raton, FL, USA: CRC Press, 2013.
[11] A. H. Zahid, E. Al-Solami, and M. Ahmad, "A novel modular approach based substitution-box design for image encryption," *IEEE Access*, vol. 8, pp. 150326–150340, 2020, doi: 10.1109/ACCESS.2020.3016401.
[12] A. H. Zahid, A. M. Iliyasu, M. Ahmad, M. M. U. Shaban, M. J. Arshad, H. S. Alhadawi, and A. A. A. El-Latif, "A novel construction of dynamic S-box with high nonlinearity using heuristic evolution," *IEEE Access*, vol. 9, pp. 67797–67812, 2021, doi: 10.1109/ACCESS.2021.3077194.
[13] A. H. Zahid, H. Rashid, M. M. U. Shaban, S. Ahmad, E. Ahmed, M. T. Amjad, M. A. T. Baig, M. J. Arshad, M. N. Tariq, M. W. Tariq, M. A. Zafar, and A. Basit, "Dynamic S-box design using a novel square polynomial transformation and permutation," *IEEE Access*, vol. 9, pp. 82390–82401, 2021, doi: 10.1109/ACCESS.2021.3086717.
[14] A. H. Zahid, M. J. Arshad, and M. Ahmad, "A novel construction of efficient substitution-boxes using cubic fractional transformation," *Entropy*, vol. 21, no. 3, p. 245, 2019.
[15] A. H. Zahid and M. J. Arshad, "An innovative design of substitution-boxes using cubic polynomial mapping," *Symmetry*, vol. 11, no. 3, p. 437, 2019.
[16] R. Lidl and H. Niederreiter, "Finite fields: Encyclopedia of mathematics and its applications," *Comput. Math. Appl.*, vol. 33, no. 7, p. 136, 1997.
[17] L. E. Dickson, "The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group," *Ann. Math.*, vol. 11, no. 1/6, pp. 65–120, 1896.
[18] M. E. Zieve, "On a theorem of Carlitz," *J. Group Theory*, vol. 17, no. 4, pp. 667–669, Jul. 2014.
[19] L. Carlitz, "Permutations in a finite field," *Proc. Amer. Math. Soc.*, vol. 4, no. 4, p. 538, Apr. 1953.
[20] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system I: The user language," *J. Symbolic Comput.*, vol. 24, nos. 3–4, pp. 235–265, Sep. 1997.

PINAR ÇOMAK received the B.Sc. degree in mathematics and the M.Sc. and Ph.D. degrees in cryptography from Middle East Technical University (METU), in 2010, 2013, and 2020, respectively. She worked as a Research Assistant with METU. She has joined the 3GPP Security Working Group, Ericsson Research, İstanbul, Turkey, in 2019, as a Standardization Delegate. She has authored some international scientific journals and conference papers related to coding theory, computational algebra, cryptography, and software security.



FERRUH ÖZBUDAK received the B.Sc. degree in electrical and electronics engineering and the Ph.D. degree in mathematics from Bilkent University, Ankara, Turkey, in 1993 and 1997, respectively. He is currently a Professor with Middle East Technical University, Ankara. His research interests include algebraic curves, codes, sequences, cryptography, finite fields, and Galois rings.