On Decompositions of Permutations in Quadratic Functions

Samuele Andreoli[1], Enrico Piccione[1], Lilya Budaghyan[1], Pantelimon Stănică[2], and Svetla Nikova[1,3]

[1]University of Bergen, Norway, {name.surname}@uib.no
[2]Naval Postgraduate School, Applied Mathematics Department, Monterey, CA 93955, USA, pstanica@nps.edu
[3]KU Leuven, Belgium, {name.surname}@esat.kuleuven.be

Abstract

The algebraic degree of a vectorial Boolean function is one of the main parameters driving the cost of its hardware implementation. Thus, finding decompositions of functions into sequences of functions of lower algebraic degrees has been explored to reduce the cost of implementations. In this paper, we consider such decompositions of permutations over $\mathbb{F}_{2^n}$. We prove the existence of decompositions using quadratic and linear power permutations for all permutations when $2^n - 1$ is a prime, and we prove the non-existence of such decompositions for power permutations of differential uniformity strictly lower than 16 when $4|n$. We also prove that any permutation admits a decomposition into quadratic power permutations and affine permutations of the form $ax + b$ if $4 \nmid n$. Furthermore, we prove that any permutation admits a decomposition into cubic power permutations and affine permutations. Finally, we present a decomposition of the PRESENT S-Box using the power permutation x^7 and affine permutations.

Keywords— power function, vectorial Boolean function, decomposition, permutation

1 Introduction

Vectorial Boolean functions are one of the fundamental building blocks of many cryptographic primitives. For instance, symmetric ciphers where permutations are used as S-Boxes. The permutations used in cryptographic primitives are usually quite complex and have a high algebraic degree. Unfortunately, a high algebraic degree is one of the main factors driving the area requirements in hardware implementations, especially when side-channel countermeasures such as Threshold Implementations [NRR06] are employed. Thus, decompositions of permutations into sequences of functions of low algebraic degree is a useful tool to reduce the area requirements of hardware implementations. For instance, the circuit can be composed of Threshold Implementations of those functions with low algebraic degree as it was done in [Pic+23] for the AES S-box. There are many examples in the literature of searches for such decompositions, for instance in [Bil+12], or [Bil+15]. These early works are carried out with the goal of constructing secure implementations, thus focusing on particular S-Boxes, or being limited to very low dimensions.

An important step towards a general treatment of the problem of finding decompositions was taken in [NNR19], where an algorithm for searching decompositions of the inverse power function into quadratic and linear power functions was presented. Using the algorithm, decompositions into quadratic or cubic power permutations of the inverse power function over $\mathbb{F}_{2^n}$ were found for $3 \leq n \leq 16$. The existence of a decomposition can then be extended to any permutation using Carlitz Lemma [Car53]. The result of [NNR19] was later extended in [Pet23] to n up to 32, and by using a different number theoretical analysis for all odd $n \leq 250$ in [LSS23]. In the last two papers, the existence of a decomposition of the inverse into quadratic power permutations for some infinite family of values of n was also proven.

Another approach to the search of decompositions tries to get rid of the middleman that is the inverse power function. Using a generalization of the Carlitz Lemma presented by Stafford [Sta98, Theorem 1], one can show that it is possible to decompose any permutation over $\mathbb{F}_{2^n}$ into odd power permutations and affine permutations. The problem of finding decompositions into permutations of low algebraic degrees can then be reduced to studying the parity of power permutations. A first important step in this direction was taken in [ÇÖ21], where the existence of odd quadratic power permutations for all n not doubly even up to $n = 127$ is proven.

Our contribution

Our contributions touch on both kinds of decompositions mentioned above.

In the first place, we focus on decompositions of power permutations into sequences of power permutations of lower algebraic degree. We show that any power permutation, including the inverse function, can be decomposed into quadratic power permutations when $2^n - 1$ is a Mersenne prime, a family of values of n that is conjectured to be infinite. Moreover, we prove that no power permutation with differential uniformity lower than 16 can be decomposed into quadratic power permutations when n is divisible by 4.

In the second place, we consider decompositions of any permutation into power permutations of lower algebraic degree, and affine permutations of the form $ax + b$. We use the Zolotoroff-Frobenius Lemma to show a link between the parity of a power permutation x^k and its Jacobi Symbol $\left(\frac{k}{2^n-1}\right)$. We use this link to show that all permutations can be decomposed into quadratic power permutations and affine permutations of the form $ax + b$ if and only if n is not divisible by 4. Moreover, we show that all permutations can be decomposed into cubic power permutations and affine permutations.

Finally, we find a decomposition of the PRESENT S-Box into quadratic power permutations and affine permutations.

2 Preliminaries

2.1 Vectorial Boolean functions

A vectorial Boolean function over the vector space (over the two element field $\mathbb{F}_2$) $\mathbb{F}_2^n$ (respectively, the finite field $\mathbb{F}_{2^n}$ dimension n over $\mathbb{F}_2$) is a function from $\mathbb{F}_2^n$ (respectively, $\mathbb{F}_{2^n}$) to itself. Further, it is called a permutation if it is also bijective. A vectorial Boolean function F over $\mathbb{F}_{2^n}$ is uniquely represented as a univariate polynomial, $F(x) = \sum_{i=0}^{2^n-1} c_i x^i$ where $c_i \in \mathbb{F}_{2^n}$, called the *univariate representation.* The algebraic degree of F, denoted by $\mathrm{d}^\circ(F)$, is equal to the maximum Hamming weight of the binary expansion of the exponents i of the terms of the polynomial $F(x)$ such that $c_i \neq 0$. The function F is called affine, quadratic, or cubic if the algebraic degree of F is respectively 1, 2, or 3. A function F is called linear if it is affine and $F(0) = 0$.

The differential uniformity of a function F over $\mathbb{F}_2^n$ is the positive integer

$$\delta_F = \max_{a,b \in \mathbb{F}_2^n,\, a \neq 0} \delta_F(a,b),$$

where

$$\delta_F(a,b) = |\{x \in \mathbb{F}_2^n \mid F(x+a) + F(x) = b\}|.$$

The function F is called almost perfect nonlinear (APN) if $\delta_F = 2$. The function F is called δ-uniform if $\delta \geq \delta_F$. We refer to Table 1 in [Bud+22] for a survey of known families of APN power functions, which are tabulated in Table 1. It has been observed by Dobbertin in [Car21, Proposition 165] that any APN power function x^d over $\mathbb{F}_{2^n}$ is such that $\gcd(d, 2^n - 1) = 1$ (hence, x^d is a permutation) if n is odd and $\gcd(d, 2^n - 1) = 3$ (hence, x^d is 3-to-1). Moreover, we consider 4−differential uniform power functions in Table 2.

Family	Exponent	Conditions	Alg. Degree
Gold	$2^i + 1$	$gcd(i,n) = 1$	2
Kasami	$2^{2i} - 2^i + 1$	$gcd(i,n) = 1$	$i + 1$
Welch	$2^t + 2 + 1$	$n = 2t + 1$	3
Niho	$2^t + 2^{\frac{t}{2}} - 1$ $2^{\frac{3t+1}{2}} + 2^t - 1$	$n = 2t + 1$, t even $n = 2t + 1$, t odd	$t/2 + 1$ $t + 1$
Inverse	$2^n - 2$	$n = 2t + 1$	$n - 1$
Dobbertin	$2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$	$n = 5t$	$t + 3$

Table 1: Known APN power functions over $\mathbb{F}_2^n$

Two functions F and G over $\mathbb{F}_{2^n}$ are called affine equivalent if $F = A_1 \circ G \circ A_2$ where A_1 and A_2 are affine permutations. More generally, F and G are called extended affine (EA) equivalent if F is affine equivalent to $G + A$ for some affine function A. Still more generally, F and G are called CCZ equivalent if there exists an affine permutation of $\mathbb{F}_{2^n}^2$ mapping $\{(x, F(x)) \colon x \in \mathbb{F}_{2^n}\}$ to $\{(x, G(x)) \colon x \in \mathbb{F}_{2^n}\}$. A particular case of CCZ equivalence is between any permutation and its compositional inverse. If a notion is preserved by affine (respectively, EA, CCZ) equivalence, we shall say that it is affine (respectively EA, CCZ) invariant. A power function over $\mathbb{F}_{2^n}$ is a function F with univariate representation of the form $F(x) = x^d$ for some positive integer

Family	Exponent	Conditions	Alg. Degree	References
Gold*	2^i+1	$gcd(i,n)=2$	2	[Gol68]
Kasami*	$2^{2i}-2^i+1$	$gcd(i,n)=2$	$i+1$	[Kas71]
B-L	$2^{2t}+2^t+1$	$n=4t$, t odd	3	[BL10]
Inverse	2^n-2	$n=2t$	$n-1$	[Nyb93]

Table 2: Known 4-uniform power functions over $\mathbb{F}_2^n$
$*$ Permutation if and only if $n=2t$, t odd.

$d < 2^n-1$. Two power functions x^{d_1} and x^{d_2} are called cyclotomic equivalent if $d_1 \equiv 2^j d_2 \pmod{2^n-1}$, or $d_1 d_2 \equiv 2^j \pmod{2^n-1}$ if $\gcd(d_2, 2^n-1)=1$, for some $0 \le j \le n-1$. It is known that two power functions are cyclotomic equivalent, if and only if they are CCZ equivalent [Dem18; Dem22].

2.2 Quadratic residues and permutations

We give some preliminaries on quadratic residues. We use [Wei20, Chapter 8] as a reference, but the reader can use any of her/his preferred algebraic number theory book.

Let p be an odd prime. We say that an integer a is a *quadratic residue* modulo p if the equation $x^2 \equiv a \pmod p$ has solutions and otherwise we say that a is a *quadratic non-residue* modulo p. We denote by $\left(\frac{a}{p}\right)$ the Legendre symbol of a over p, defined as $\left(\frac{a}{p}\right)=1$ if a is a quadratic residue modulo p, $\left(\frac{a}{p}\right)=-1$ if a is a quadratic non-residue modulo p, and $\left(\frac{a}{p}\right)=0$ if $\gcd(a,p)>1$. The Legendre symbol can be explicitly computed using Euler's Criterion [Wei20, Theorem 8.5], as $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$. Using Euler's Criterion, it is immediate to see that the symbol is (completely) multiplicative, that is, $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, and that $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$ if $a \equiv b \pmod p$. Moreover, we have a specific result for $a=2$, that

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}, \tag{1}$$

see for instance [Wei20, Theorem 8.10]. The Legendre symbol also satisfies one last property, crucial for its computation, Gauss' Quadratic Reciprocity Law [Wei20, Theorem 8.22]. Let p and q be distinct odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}. \tag{2}$$

The Legendre symbol is extended to the *Jacobi symbol* that allows the denominator to be any odd positive integer n. Let $n = p_1^{e_1} \dots p_\ell^{e_\ell}$ be its prime factorization, then the Jacobi symbol of a over n is defined as

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \cdots \left(\frac{a}{p_\ell}\right)^{e_\ell}.$$

It follows immediately from the definition that the Jacobi symbol shares many of the properties of the Legendre symbol, such as Gauss' Quadratic Reciprocity Law, being multiplicative, Gauss' Lemma, and its corollary. Moreover, it is also multiplicative in the denominator, so that $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$. However, while the Legendre symbol $\left(\frac{a}{p}\right)$ is equal to -1 if and only if a is a quadratic non-residue modulo p, for a composite n we can only say that if $\left(\frac{a}{n}\right) = -1$, then a is a quadratic non-residue for at least one of the prime factors of n.

We denote as $(\mathrm{Sym}(\mathbb{F}_{2^n}), \circ)$ the group of all permutations F over $\mathbb{F}_{2^n}$. A permutation $T \in \mathrm{Sym}(\mathbb{F}_{2^n})$ is called a *transposition* if there exists $\alpha, \beta \in \mathbb{F}_{2^n}$ such that $T(\alpha) = \beta$, $T(\beta) = \alpha$, and $T(x) = x$ for all $x \in \mathbb{F}_{2^n} \setminus \{\alpha, \beta\}$. Every permutation $F \in \mathrm{Sym}(\mathbb{F}_{2^n})$ can be written as a composition of transpositions $F = T_1 \circ \cdots \circ T_\ell$, for some transpositions $T_1, \ldots, T_\ell$ [Wei20, Proposition 8.12]. Such writing is not unique, but given two decompositions of F of length ℓ_1 and ℓ_2, then $\ell_1 \equiv \ell_2 \pmod 2$. Then, we can define $\mathrm{sgn}(F)$ to be equal to $(-1)^\ell$, where ℓ is the length of a decomposition of F into transpositions [Wei20, Theorem 8.14]. We say that F is even if $\mathrm{sgn}(F) = 1$, while we say that F is odd otherwise.

We are now ready to give a useful characterization of the Jacobi symbol using the parity of some permutations over $\mathbb{Z}_{2^n-1}$. This result was first used by Zolotareff in [Zol72] to give an alternate proof of Gauss' Quadratic Reciprocity Law for the Legendre symbol. It was then extended by Frobenius in [Fro14] to the Jacobi symbol, and this is the result we shall use.

Lemma 2.1 (Zolotareff-Frobenius Lemma [Fro14])**.** *Let a, b be positive integers such that $b \geq 3$ odd and $\gcd(a, b) = 1$. Let $\sigma_a\colon \mathbb{Z}_b \to \mathbb{Z}_b$ be the multiplication map $x \mapsto ax$. Then $\mathrm{sgn}(\sigma_a) = \left(\frac{a}{b}\right)$.*

A more recent and simpler proof of the Zolotareff-Frobenius Lemma [Fro14] can be found in [DS76].

3 On the existence of a decomposition into quadratic power permutations

Let $\mathbb{Z}_N$ be the ring of integers modulo N, we will denote as $U(\mathbb{Z}_N)$ the multiplicative group of integers k modulo N such that $\gcd(k, N) = 1$, that is the set of invertible elements in $\mathbb{Z}_N$. For any integer n, we define the set $\mathcal{Q}_n$ as the multiplicative subgroup of $U(\mathbb{Z}_{2^n-1})$ generated by all the residues $d \in U(\mathbb{Z}_{2^n-1})$ with Hamming weight in their binary expansion at most 2.

Theorem 3.1. *Let n be odd. The APN exponents Gold, Kasami, and Niho for $n \equiv 1 \pmod 4$ all belong to $\mathcal{Q}_n$.*

Proof. Referring to Table 1, each of the exponents mentioned can be written as products of quadratic exponents and inverse of quadratic exponents as in [Bud+22], that all belong to $\mathcal{Q}_n$. □

3.1 The case $2^n - 1$ prime

The following folklore result (see [FV03] for reference) gives a necessary and sufficient condition on N to determine if $U(\mathbb{Z}_N)$ is cyclic.

Proposition 3.1. *Let N be a positive integer. Then $U(\mathbb{Z}_N)$ is cyclic if and only if $N \in \{2, 4, p^\ell, 2p^\ell\}$ where p is an odd prime.*

Note, however, that $N = 2^n - 1$ is odd, so it is not equal to 2, 4, or $2p^\ell$ where p is an odd prime. We are going to prove that $2^n - 1 \neq p^\ell$ for $\ell \geq 2$. The following theorem is also known as the Catalan's conjecture, proven to be true in 2002 by P. Mihăilescu.

Theorem 3.2 ([Bil04])**.** *Let a, b, x, y be positive integers such that $x > 1, y > 1, a > 1$ and $b > 1$. Then the only solution to the equation*

$$x^a - y^b = 1$$

is $x = 3$, $y = 2$, $a = 2$, $b = 3$.

Proposition 3.2. *Let n be a positive integer, p an odd prime, and $\ell \geq 2$. Then $2^n - 1 \neq p^\ell$.*

Proof. Suppose $2^n - 1 = p^\ell$, then $(x, y, a, b) = (2, p, n, \ell)$ is a solution to the equation

$$x^a - y^b = 1,$$

but this is in contradiction with Theorem 3.2. □

Corollary 3.1. *Let n be a positive integer. Then $U(\mathbb{Z}_{2^n-1})$ is cyclic if and only if $2^n - 1$ is prime.*

Remark 3.1. *It is easy to observe that if $n = pq$ is composite, then $2^n - 1$ has $2^p - 1$ and $2^q - 1$ as factors. On the other hand, if n is prime, then $2^n - 1$ might also be prime, called a Mersenne prime. For instance, we have that $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 31$, $2^7 - 1 = 127$ are all primes. The fact that n is prime is not a sufficient condition, and the first counterexample is $2^{11} - 1 = 23 \cdot 89$. It is not known if the set of Mersenne primes is finite or infinite.*

Suppose that $2^n - 1$ is prime. If we can find an element d of weight 2 that is a generator of $U(\mathbb{Z}_{2^n-1})$, we can use that to decompose any power permutation over $\mathbb{F}_{2^n}$. For this, we need to find a d such that $\left(\frac{d}{2^n-1}\right) = -1$ because then $d^{\frac{2^n-2}{2}} \equiv -1 \pmod{2^n - 1}$ by Euler's criterion, and this implies that d has order $2^n - 2$ that is the order of $U(\mathbb{Z}_{2^n-1})$.

Proposition 3.3. *Let $n \geq 3$ be such that $2^n - 1$ is a prime, then we have that*

1. $\left(\frac{3}{2^n-1}\right) = -1$.
2. $\left(\frac{5}{2^n-1}\right) = -1$ *if and only if* $n \equiv 3 \pmod 4$.

Proof. Since $2^n - 1$ is prime, then n is an odd prime. Since $n \geq 3$, we have that $2^n - 1 \equiv 3 \pmod 4$ and

$$\left(\frac{3}{2^n - 1}\right) = -\left(\frac{2^n - 1}{3}\right)$$

by (2).

Observe that $2^n \equiv 2 \pmod 3$ because n is odd and

$$\left(\frac{2^n - 1}{3}\right) = (2^n - 1)^{(3-1)/2} = 2^n - 1 \equiv 1 \pmod 3$$

by Euler's criterion. So we must have that $\left(\frac{3}{2^n-1}\right) = -1$ and therefore 3 is a primitive root modulo $2^n - 1$.

Considering now 5, surely $5 \equiv 1 \pmod 4$, and so

$$\left(\frac{5}{2^n-1}\right) = \left(\frac{2^n-1}{5}\right).$$

Since $2^2 \equiv -1 \pmod 5$, we have that $2^n \equiv -2 \pmod 5$ if $n \equiv 3 \pmod 4$ and $2^n \equiv 2 \pmod 5$ if $n \equiv 1 \pmod 4$. So we have that

$$(2^n-1)^{(5-1)/2} = (2^n-1)^2 = \begin{cases} 1 \pmod 5 & \text{if } n \equiv 1 \pmod 4, \\ -1 \pmod 5 & \text{if } n \equiv 3 \pmod 4. \end{cases}$$

Therefore, 5 is a primitive root modulo $2^n - 1$ if and only if $n \equiv 3 \pmod 4$. □

Theorem 3.3. *Let $n > 2$ such that $2^n - 1$ is a prime, then $\mathcal{Q}_n = U(\mathbb{Z}_{2^n-1})$ and it is a cyclic group generated by 3. Moreover, if $n \equiv 3 \pmod 4$ then it is also generated by 5.*

Proof. It is known that $U(\mathbb{Z}_{2^n-1})$ is a cyclic group of order $2^n - 2$ since $\mathbb{Z}_{2^n-1}$ is a field. By Proposition 3.3, we have that 3 is a generator of the cyclic group $U(\mathbb{Z}_{2^n-1})$. Since the group generated by 3 is contained in $\mathcal{Q}_n$ and $\mathcal{Q}_n \subseteq U(\mathbb{Z}_{2^n-1})$, we have that $\mathcal{Q}_n = U(\mathbb{Z}_{2^n-1})$. If $n \equiv 3 \pmod 4$, we have that 5 is a generator of $U(\mathbb{Z}_{2^n-1})$ by Proposition 3.3. □

Corollary 3.2. *Let n be a positive integer such that $2^n - 1$ is prime. Then, any power permutation x^d over $\mathbb{F}_{2^n}$ can be decomposed into quadratic power functions by repeated compositions of x^3, or alternatively x^5 if $n \equiv 3 \pmod 4$.*

3.2 Non-existence of decomposition into quadratics for some power permutations in doubly even dimension

Let n be a positive integer. Observe the following:

1. If $n \neq 2^k$, then there exists $1 \leq i \leq n-1$ such that $\frac{n}{\gcd(i,n)}$ is odd and therefore $2^i + 1 \in \mathcal{Q}_n$.
2. If $n = 2^k$, then $\mathcal{Q}_n$ is a cyclic group generated by 2 of order n.

Let k be a positive integer such that k divides n. For any x^d power permutations over $\mathbb{F}_{2^n}$, we have that x^d restricted to $\mathbb{F}_{2^k}$ is a power permutation x^e where $e = d \pmod{2^k - 1}$. Then, the algebraic degree of x^e over $\mathbb{F}_{2^k}$ is lower or equal than the algebraic degree of x^d over $\mathbb{F}_{2^n}$. Indeed, if $x^d = x^{d_0} x^{2^k d_1} x^{2^{2k} d_2} \ldots x^{2^{n-k} d_{n/k-1}}$ then we can rewrite the algebraic degree over $\mathbb{F}_{2^k}$ as

$$\mathrm{d}^\circ(x^{d_0} x^{2^k d_1} x^{2^{2k} d_2} \ldots x^{2^{n-k} d_{n/k-1}}) \leq \mathrm{d}^\circ(x^{d_0}) + \mathrm{d}^\circ(x^{d_1}) + \ldots + \mathrm{d}^\circ(x^{d_{n/k-1}}),$$

since $x^{2^k} = x$ over $\mathbb{F}_{2^k}$. Since $\mathrm{d}^\circ(x^{d_i}) = \mathrm{w}(d_i)$, then the sum of the degrees is equal to the sum of the weights, which is equal to $\mathrm{w}(d)$ because of how we split d. Thus, $\mathrm{d}^\circ(x^e) \leq \mathrm{d}^\circ(x^d)$. Moreover, there is a natural surjective homomorphism from $\mathcal{Q}_n$ to $\mathcal{Q}_k$ induced by the surjective homomorphism from $U(\mathbb{Z}_{2^n-1})$ to $U(\mathbb{Z}_{2^k-1})$ that maps $d \in U(\mathbb{Z}_{2^n-1})$ to $e \equiv d \pmod{2^k - 1}$. So we have that $\mathcal{Q}_k$ is isomorphic to a subgroup of $\mathcal{Q}_n$. As a consequence, we have the following lemma for the case $k = 4$.

Lemma 3.1. *Let n be a positive integer such that $n \equiv 0 \pmod 4$. Let d be a positive integer such that $\gcd(d, 2^n - 1) = 1$ and $d \pmod{2^4 - 1}$ is not a power of 2. Then $d \notin \mathcal{Q}_n$.*

Proof. It follows from the fact that for any $d \in \mathcal{Q}_n$, we have that $e \in \mathcal{Q}_4$ where $e \equiv d \pmod{2^4 - 1}$. Indeed, $\mathcal{Q}_4$ is a cyclic group generated by 2. □

Theorem 3.4. *Let n be a positive integer such that $n \equiv 0 \pmod 4$. For any $d \in \mathcal{Q}_n$ with $\gcd(d, 2^n - 1) = 1$, the power permutation x^d has differential uniformity at least 16. In particular, the inverse function cannot be decomposed in quadratic power functions in dimension n.*

Proof. Let $d \notin \mathcal{Q}_n$, then Lemma 3.1 we have that $F(x) = x^d$ defined over $\mathbb{F}_{2^n}$ is linear over $\mathbb{F}_{2^4}$. Therefore, for any $x \in \mathbb{F}_{2^4}$ we have that

$$(x+1)^d + x^d = x^d + 1 + x^d = 1$$

and so $\delta_F(1,1) \geq 16$. Therefore, $\delta_F \geq 16$. Since the inverse function is 4-uniform, it cannot be decomposed in quadratic power functions. □

4 On decompositions using power permutations and affine permutations

Stafford proved in [Sta98, Theorem 1] that if $\pi_k = x^k$ is an odd permutation, then $\mathrm{Sym}(\mathbb{F}_{2^n})$ is generated by π_k and the affine permutations $\tau_{a,b} = ax + b$, for $a \in \mathbb{F}_{2^n} \setminus \{0\}, b \in \mathbb{F}_{2^n}$. This means that we can write any permutation in $\mathrm{Sym}(\mathbb{F}_{2^n})$ as

$$\pi = \tau_{a_1,b_1} \circ \pi_k \circ \tau_{a_2,b_2} \circ \pi_k \circ \ldots \circ \pi_k \circ \tau_{a_l,b_l}, \tag{3}$$

for an appropriate choice of $a_1, \ldots, a_l$ and $b_1, \ldots, b_l$, which is clearly a decomposition of π as a sequence of affine permutations and the power permutation π_k. Thus, the problem of proving the existence of decompositions can be reduced to studying the parity of power permutations over $\mathbb{F}_{2^n}$.

Remark 4.1. *Note that, as stated in[Sta98, Theorem 1], the Alternating group, that is the group of even permutations over $\mathbb{F}_{2^n}$, is generated by any power permutation and affine permutations. A quadratic permutation over $\mathbb{F}_{2^n}$ exists if and only if n is not a power of 2. Then, even permutations admit a decomposition into quadratic power permutations and affine permutations if and only if n is not a power of 2.*

Some results on the parity of power permutations were presented in [ÇÖ21] where an algorithm to compute the parity of a power permutation over $\mathbb{F}_{2^n}$ was presented and used to justify the following conjecture.

Conjecture 4.1. *[ÇÖ21, Conjecture 6.3]*

- *For all n odd integers, the power permutation x^3 is odd over $\mathbb{F}_{2^n}$,*
- *for all $n \equiv 2, 3 \pmod 4$, the power permutation x^5 is odd over $\mathbb{F}_{2^n}$,*
- *for all n multiples of 4 and not a power of 2, all quadratic permutations are even over $\mathbb{F}_{2^n}$.*

In the next Lemma, we prove a relationship between the Jacobi symbol $\left(\frac{k}{2^n-1}\right)$ and the parity of the permutation x^k over $\mathbb{F}_{2^n}$. We will then use this result to prove the conjecture and give some further results on the parity of power permutation and the existence of decomposition in quadratic power permutation and affine permutations, as described by (3).

Lemma 4.1. *Let $n \geq 3$. A power permutation $\pi_k = x^k$ on $\mathbb{F}_{2^n}$ is odd if and only if the Jacobi symbol $\left(\frac{k}{2^n-1}\right) = -1$.*

Proof. This is a direct consequence of the Zolotareff-Frobenius Lemma. We briefly recall the statement of the lemma. Let k be an integer such that $\gcd(k, 2^n - 1) = 1$, then

$$\left(\frac{k}{2^n-1}\right) = \operatorname{sgn}(\sigma_k),$$

where σ_k is the permutation induced by the multiplication by k over $\mathbb{Z}_{2^n-1}$. First, note that since π_k is a permutation, $\gcd(k, 2^n - 1) = 1$, and $2^n - 1$ is an odd integer, meaning that we can apply the lemma. Now, let α be a primitive element of $\mathbb{F}_{2^n}$, we consider the isomorphism

$$\begin{aligned} \Psi_\alpha : \mathbb{Z}_{2^n-1} &\to \mathbb{F}_{2^n} \setminus \{0\} \\ b &\mapsto \alpha^b, \end{aligned}$$

and its inverse $\Psi_\alpha^{-1} : \mathbb{F}_{2^n} \setminus \{0\} \to \mathbb{Z}_{2^n-1}$. Note that Ψ_α depends on the choice of α, but this choice does not affect the proof. Here, for brevity, we drop the subscript α. We now consider $\bar{\pi}_k$, the restriction of π_k to $\mathbb{F}_{2^n} \setminus \{0\}$. Then, $\bar{\pi}_k = \Psi(\sigma_k(\Psi^{-1}(x)))$, because $\Psi(\sigma_k(\Psi^{-1}(x))) = \alpha^{bk} = x^k$ for any $x = \alpha^b \in \mathbb{F}_{2^n} \setminus \{0\}$. Finally, let $\sigma_k = T_1 \dots T_\ell$ be a decomposition of σ_k in transpositions. Since $\Psi \circ T \circ \Psi^{-1}$ is still a transposition for any transposition T, then

$$\bar{\pi}_k = \left(\Psi \circ T_1 \circ \Psi^{-1}\right) \dots \left(\Psi \circ T_\ell \circ \Psi^{-1}\right)$$

is a decomposition of $\bar{\pi}_k$ in transpositions. Since π_k is equal to the extension of $\bar{\pi}_k$ to $\mathbb{F}_{2^n}$ that fixes 0, then it also has the same decomposition in transpositions, and

$$\operatorname{sgn}(\pi_k) = \operatorname{sgn}(\bar{\pi}_k) = (-1)^\ell = \operatorname{sgn}(\sigma_k) = \left(\frac{k}{2^n-1}\right),$$

because of the Zolotareff-Frobenius lemma, concluding the proof. □

Lemma 4.1 gives us a tool to easily show that a particular power permutation is odd. This is quite useful in proving theoretical results by manipulating the appropriate Jacobi symbol. Moreover, this result also gives a more efficient way to compute the parity of a power permutation, reducing it to the computation of the Jacobi symbol $\left(\frac{k}{2^n-1}\right)$. Efficient algorithms exist for the computation of Jacobi symbols. For instance, [ES96, RS $k - ary$ algorithm] runs in sub-quadratic time $\mathcal{O}(n^2/\log(n))$, which is much faster than [ÇÖ21, Algorithm 1], which runs in $\mathcal{O}(2^{n/3}n^{2/3})$.

We now use Lemma 4.1 to prove [ÇÖ21, Conjecture 6.3]. Before starting, we give a couple of useful notions. First, let n be a positive integer, we denote by $\nu_2(n)$ the *dyadic valuation* of n, that is, the integer i such that $2^i | n$, but $2^{i+i} \nmid n$. Moreover, we give a small lemma, which will be useful for many of the following proofs.

Lemma 4.2. *Let $n \geq 2$. If $0 < i < n$, then*

$$\left(\frac{2^i+1}{2^n-1}\right) = (-1)^{\delta_1(i)} \left(\frac{2^n-1}{2^i+1}\right), \tag{4}$$

where δ_i is the Kronecker delta defined by

$$\delta_i(j) = \begin{cases} 1 & if\ i = j, \\ 0 & otherwise. \end{cases}$$

Moreover, if $0 < i < j < n$, then

$$\left(\frac{2^j+2^i+1}{2^n-1}\right) = (-1)^{\delta_1(i)} \left(\frac{2^n-1}{2^j+2^i+1}\right). \tag{5}$$

Proof. Equations (5) and (5) are a direct consequence of Gauss' Quadratic Reciprocity Law. Now, $2^n - 1 \equiv 3 \pmod 4$ for any $n \geq 2$. Equation (4) follows directly from the fact that $2^i + 1 \equiv 1 \pmod 4$ for any $i > 1$ and $2^1 + 1 \equiv 3 \pmod 4$ for $i = 1$. Similarly, Equation (5) follows directly from the fact that $2^j + 2^i + 1 \equiv 1 \pmod 4$ for any $i > 1$, while for $i = 1$, $2^j + 3 \equiv 3 \pmod 4$ because $j > i > 0$. □

We are now ready to prove the three points of [ÇÖ21, Conjecture 6.3]. We remember that this conjecture on the parity of power permutations is tied to the existence of decompositions for any permutation by [Sta98, Theorem 1].

Theorem 4.1. *Let $n \geq 3$. Then*

1. *x^3 is an odd permutation over $\mathbb{F}_{2^n}$ if and only if $n \equiv 1 \pmod 2$,*
2. *x^5 is an odd permutation over $\mathbb{F}_{2^n}$ if and only if $n \equiv 2, 3 \pmod 4$,*
3. *quadratic power permutations over $\mathbb{F}_{2^n}$ are even for any $n \equiv 0 \pmod 4$.*

Proof. To prove the first two points, we can directly prove that the Jacobi symbols $\left(\frac{3}{2^n-1}\right)$ and $\left(\frac{5}{2^n-1}\right)$ are always odd for the appropriate values of n. In particular, we use Lemma 4.2 to say that

$$\left(\frac{3}{2^n-1}\right) = -\left(\frac{2^n-1}{3}\right),$$

and that

$$\left(\frac{5}{2^n-1}\right) = \left(\frac{2^n-1}{5}\right).$$

Now, for $n = 2t = 1$, we have that $2^n - 1 = 2^{2t+1} - 1 = 2(4^t) - 1 \equiv 1 \pmod 3$, and

$$\left(\frac{3}{2^n-1}\right) = -\left(\frac{2^n-1}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

On the other hand, for $n = 4t+s$ with $1 \leq s \leq 3$ (s cannot be zero since otherwise x^5 is not a permutation), we have that $2^n-1 = 2^{4t+s}-1 = 2^s(4^{2t})-1 = 2^s(-1)^{2t}-1 \equiv 2^s-1 \pmod 5$, and

$$\left(\frac{2^n-1}{5}\right) = \left(\frac{2^s-1}{5}\right) = \left(\frac{5}{2^s-1}\right),$$

using Lemma 4.2 and Euler's Criterion. For $s = 1$, we have $\left(\frac{5}{2^s-1}\right) = \left(\frac{5}{1}\right) = 1$. For $s = 2$, we have $\left(\frac{5}{2^s-1}\right) = \left(\frac{5}{3}\right) = \left(\frac{-1}{3}\right) = -1$. For $s = 3$, we have $\left(\frac{5}{2^s-1}\right) = \left(\frac{5}{7}\right) = \left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{25-1}{8}} = -1$, because of Lemma 4.2 and (1). Using Lemma 4.1, we can conclude.

Let us consider the third point. We denote $n = 4t$ and start with some necessary conditions for a power function to be a permutation. Let us consider $x^{2^{i'}+1}$. This is a permutation if and only if $\frac{4t}{gcd(i',4t)}$ is odd, which is true if and only if $4|i'$. This means that from now on, we can assume $i' = 4i$ for some integer $i > 0$. Moreover, for $\frac{t}{gcd(i,t)}$ to be odd, we also need that $\nu_2(i) \geq \nu_2(t)$. Any other combination of i and t falls in the cases where the power function is not a permutation.

We now aim to prove that $\left(\frac{2^{4i}+1}{2^{4t}-1}\right) = 1$ for any i, t such that $0 < i < t$ and $\nu_2(i) \geq \nu_2(t)$, meaning that the Jacobi symbol must be either 1 or -1. First, note that using Lemma 4.2,

$$\left(\frac{2^{4i}+1}{2^{4t}-1}\right) = \left(\frac{2^{4t}-1}{2^{4i}+1}\right),$$

because $4i > 1$. To continue the proof, we first consider the case $i|t$, and then the more general case $t = is + r$, with $0 \leq r < i$.

Case $i|t$. Note that in this case $\nu_2(i) \leq \nu_2(t)$, so $\nu_2(i) = \nu_2(t)$. Therefore, We must have that $t = is$ for some odd integer $s > 0$. Then,

$$\left(\frac{2^{4t}-1}{2^{4i}+1}\right) = \left(\frac{(2^{4i})^s-1}{2^{4i}+1}\right),$$

and since $2^{4i} \equiv -1 \pmod{2^{4i}+1}$,

$$\left(\frac{(2^{4i})^s-1}{2^{4i}+1}\right) = \left(\frac{(-1)^s-1}{2^{4i}+1}\right) = \left(\frac{-2}{2^{4i}+1}\right) = \left(\frac{-1}{2^{4i}+1}\right)\left(\frac{2}{2^{4i}+1}\right),$$

using the fact that s is odd in the second equality, and the complete multiplicative property of the Jacobi symbol, for the third identity. Both factors are now easy to compute, as

$$\left(\frac{-1}{2^{4i}+1}\right) = (-1)^{2^{4i-1}} = 1, \text{ and } \left(\frac{2}{2^{4i}+1}\right) = (-1)^{\frac{(2^{4i}+1)^2-1}{8}} = 1,$$

where the second to last equality is due to Equation (1).

We therefore infer that $\left(\frac{2^{4i}+1}{2^{4t}-1}\right) = 1$.

Case $t = is + r$, with $0 \leq r < i$. We prove by induction on i that $\left(\frac{2^{4i}+1}{2^{4t}-1}\right) = 1$. For $i = 1$, this falls back on the case $i|t$, so it is trivially true for any t. Now, assume $\left(\frac{2^{4j}+1}{2^{4t}-1}\right) = 1$ for any $j < i$. If $r = 0$, we fall back to the case $i|t$, so we assume $r > 0$. Then,

$$\left(\frac{2^{4t}-1}{2^{4i}+1}\right) = \left(\frac{2^{4r}(2^{4i})^s-1}{2^{4i}+1}\right) = \left(\frac{2^{4r}(-1)^s-1}{2^{4i}+1}\right).$$

If s is even, then

$$\left(\frac{2^{4t}-1}{2^{4i}+1}\right) = \left(\frac{2^{4r}-1}{2^{4i}+1}\right) = \left(\frac{2^{4i}+1}{2^{4r}-1}\right), \tag{6}$$

where the second equality holds for Lemma 4.2. Since $r < i$, we can say that $i = s_1 r + r_1$, for some non-negative integers $s_1, r_1 < i$, and we can rewrite

$$\left(\frac{2^{4i}+1}{2^{4r}-1}\right) = \left(\frac{(2^{4r})^{s_1} 2^{4r_1}+1}{2^{4r}-1}\right) = \left(\frac{2^{4r_1}+1}{2^{4r}-1}\right),$$

because $2^{4r} \equiv 1 \pmod{2^{4r}-1}$. Now, note that this last symbol must be different from zero, otherwise, the original symbol would also be zero, and we restricted ourselves to cases where the symbol $\left(\frac{2^{4i}+1}{2^{4t}-1}\right)$ is either 1 or -1. Since the symbol cannot be zero, then $2^{4r_1}+1$ and $2^{4r}-1$ must be coprime, and then we are in one of the cases covered by the inductive hypothesis. Thus, $\left(\frac{2^{4r_1}+1}{2^{4r}-1}\right) = 1$, concluding the proof for s even.

On the other hand, if s is odd, then

$$\left(\frac{2^{4t}-1}{2^{4i}+1}\right) = \left(\frac{-2^{4r}-1}{2^{4i}+1}\right) = \left(\frac{2^{4i}+1-2^{4r}-1}{2^{4i}+1}\right) = \left(\frac{2^{4r}(2^{4(i-r)}-1)}{2^{4i}+1}\right).$$

Now, using the fact that the Jacobi symbol is multiplicative, we can rewrite

$$\left(\frac{2^{4r}(2^{4(i-r)}-1)}{2^{4i}+1}\right) = \left(\frac{2^{4r}}{2^{4i}+1}\right)\left(\frac{2^{4(i-r)}-1}{2^{4i}+1}\right) = \left(\frac{2^{4(i-r)}-1}{2^{4i}+1}\right),$$

where the second equality holds because

$$\left(\frac{2^{4r}}{2^{4i}+1}\right) = \left(\frac{2}{2^{4i}+1}\right)^{4r} = 1.$$

Using Lemma 4.2, we can rewrite

$$\left(\frac{2^{4(i-r)}-1}{2^{4i}+1}\right) = \left(\frac{2^{4i}+1}{2^{4(i-r)}-1}\right).$$

This is the same as the symbol in Equation (6), with the care of replacing r with $(i-r)$, because both r and $i-r$ are non-zero integers strictly lower than i. We can then rewrite the symbol as

$$\left(\frac{2^{4i}+1}{2^{4(i-r)}-1}\right) = \left(\frac{2^{4r_1}+1}{2^{4(i-r)}-1}\right) = 1,$$

using the same reasoning as above to justify the application of the inductive hypothesis. This concludes the proof for s odd, and also the induction.

Therefore, we can say that $\left(\frac{2^{4i}+1}{2^{4t}-1}\right) = 1$ for any i, t such that $0 < i < t$ and $\nu_2(i) \geq \nu_2(t)$, and using Lemma 4.1 we can say that $x^{2^{4i}+1}$ is an even permutation. In any other case, $\frac{4t}{gcd(i',4t)}$ is even, so $x^{2^{i'}+1}$ is not a permutation. □

Remark 4.2. *Note that this is a generalization of Theorem* 3.3 *to any odd n, as the Jacobi symbol is the same as the Legendre symbol when the modulus is prime. However, this new result does not allow a generalization of* 3.3*, since it requires the equivalence between an element being of maximal order, and its Legendre symbol having value -1. This strong connection is not present for the Jacobi symbol.*

Proving the conjecture allows the formulation of the following theorem on the existence of decompositions in quadratic and affine permutations.

Theorem 4.2. *Let $n \geq 3$. All permutations over $\mathbb{F}_{2^n}$ admit a decomposition in quadratic power permutations and affine permutations, if and only if $4 \nmid n$.*

Proof. In Theorem 4.1 we show the existence of an odd quadratic power permutation over $\mathbb{F}_{2^n}$ for any $4 \nmid n$. Using [Sta98, Theorem 1], we can say that $\mathrm{Sym}\,(\mathbb{F}_{2^n})$ is generated by affine permutations of the form $ax + b$ and by the quadratic power permutations π_3 and π_5 respectively when n is odd and when n is even, but not doubly even. This means that if $4 \nmid n$, then all permutations over $\mathbb{F}_{2^n}$ admit a decomposition in quadratic and affine permutations.

On the other hand, in the same Theorem 4.1, we also proved that all quadratic permutations on $\mathbb{F}_{2^n}$ are even if $4|n$. Moreover, all affine permutations $ax+b$ are even, as proved in the proof of [Sta98, Theorem 1], and also the Frobenius automorphism π_2 is even, since $\left(\frac{2}{2^n-1}\right) = (-1)^{\frac{(2^n-1)^2-1}{8}} = (-1)^{\frac{2^{2n}-2^{n+1}}{8}} = 1$ for any $n \geq 3$, using (1). Thus, all affine permutations over $\mathbb{F}_{2^n}$ are even. This means that if $4|n$, then all compositions of quadratic power permutations and affine permutations are even. We can then conclude that odd permutations do not admit a decomposition in quadratic and affine permutations when $4|n$. □

Corollary 4.1. *Any APN permutation in dimension $n \not\equiv 0 \pmod 4$ can be decomposed using quadratic power permutations and affine permutations.*

Remark 4.3. *Note that this is not a generalization of Corollary 3.2 to any permutation and n not divisible by 4. Indeed, the decompositions we are considering in this section do not use only power permutations, but also polynomial affine permutations.*

This result leads to one last question. Is it always possible to decompose a permutation using cubic power permutations and affine permutations when $4|n$? In order to answer this question, we first give a preliminary lemma proving that the cubic power permutation x^{13} is odd over $\mathbb{F}_{2^n}$ when $n = 4t$ and $t \not\equiv 0 \pmod 3$.

Proposition 4.1. *Let $n = 4t$, with $t \not\equiv 0 \pmod 3$. Then x^{13} is an odd permutation on $\mathbb{F}_{2^n}$.*

Proof. Using Lemma 4.1, we can say that x^{13} is odd if and only if $\left(\frac{13}{2^{4t}-1}\right) = -1$. Using Lemma 4.2, we have that

$$\left(\frac{13}{2^{4t}-1}\right) = \left(\frac{2^{4t}-1}{13}\right) = \left(\frac{3^t-1}{13}\right),$$

because $2^4 \equiv 3 \pmod{13}$. We now consider the two cases $t \equiv 1, 2 \pmod 3$.

Case $t \equiv 1 \pmod 3$, so that $t = 3s + 1$ for some integer s. Then

$$\left(\frac{3^t-1}{13}\right) = \left(\frac{3^{3s+1}-1}{13}\right) = \left(\frac{3(3^3)^s-1}{13}\right) = \left(\frac{2}{13}\right) = (-1)^{\frac{13^2-1}{8}} = -1,$$

where the third equality holds because $3^3 \equiv 1 \pmod{13}$, while the second last is due to Equation (1).

Case $t \equiv 2 \pmod 3$, so that $t = 3s + 2$ for some integer s. Then

$$\left(\frac{3^t-1}{13}\right) = \left(\frac{3^{3s+2}-1}{13}\right) = \left(\frac{9(3^3)^s-1}{13}\right) = \left(\frac{8}{13}\right) = \left(\frac{2}{13}\right)^3 = -1,$$

reusing the value for $\left(\frac{2}{13}\right)$ that we just found for the case $t = 1$.

Thus, combining the two cases, we show that $\left(\frac{13}{2^{4t}-1}\right) = -1$ for all $t \not\equiv 0 \pmod 3$. □

We are now ready to give our most general result on the existence of odd decompositions. In particular, we show that for any value of n, an odd decomposition always exists.

Theorem 4.3. *Let $n \geq 3$ be a positive integer, $n = 2^{\nu_2(n)}s$, so that s is odd. Then x^{k_n} is an odd power function, where*

- *$k_n = 2^{2s} + 2^s + 1$, for any n, except when $s = 1$ and $\nu_2(n)$ is an odd integer,*
- *$k_n = 13$, if $s = 1$ and $\nu_2(n)$ is an odd integer.*

Proof. First, we consider the exceptional case where $s = 1$ and $\nu_2(n)$ is odd. When n is fixed, for easy writing, we let $\nu_2(n) = \ell$. Then $2^\ell = 4 \cdot 2^{\ell-2}$, and $2^{\ell-2} \equiv 2 \pmod 3$, and 4.1 applies.

We can now assume that either $s = 1$ and ℓ is even, or $s > 1$. Next, we write

$$2^n - 1 = (2^s - 1)\left(2^{\left(2^\ell-1\right)s} + 2^{\left(2^\ell-2\right)s} + \cdots + 2^s + 1\right).$$

If $s = 1$ and ℓ is even, since the Jacobi symbol is completely multiplicative in one parameter (when the other parameter is fixed), it will be sufficient to show that

$$\left(\frac{2^{2s}+2^s+1}{2^s-1}\right) = \left(\frac{7}{1}\right) = 1 \text{ and } \left(\frac{7}{2^{\left(2^\ell-1\right)s} + \cdots + 2^s + 1}\right) = \left(\frac{7}{2^{2^\ell}-1}\right) = -1.$$

The first identity is immediate and the second follows (via Gauss' Quadratic Reciprocity Law) from

$$\left(\frac{7}{2^{2^\ell}-1}\right) = \left(\frac{2^{2^\ell}-1}{7}\right) = \left(\frac{1}{7}\right) = 1,$$

using the fact that $2^{2^\ell} \equiv 2 \pmod 7$, for even ℓ. The reason that this argument does not work for odd ℓ is because $2^{2^\ell} \equiv 4 \pmod 7$, for odd ℓ, and so, the second Jacobi symbol is then $\left(\frac{7}{2^{2^\ell}-1}\right) = \left(\frac{2^{2^\ell}-1}{7}\right) = \left(\frac{3}{1}\right) = 1$.

Let now $s \geq 2$. As above, it will be enough to show that the two Jacobi symbols satisfy

$$\left(\frac{2^{2s}+2^s+1}{2^s-1}\right) = -1 \text{ and } \left(\frac{2^{2s}+2^s+1}{2^{\left(2^\ell-1\right)s} + \cdots + 2^s + 1}\right) = 1.$$

Since $2^{2s} + 2^s + 1 \equiv 3 \pmod{2^s - 1}$, then

$$\left(\frac{2^{2s}+2^s+1}{2^s-1}\right) = \left(\frac{3}{2^s-1}\right) = -\left(\frac{2^s-1}{3}\right) = \left(\frac{1}{3}\right) = -1,$$

since s is odd and so, $2^s - 1 \equiv 1 \pmod 3$.

We now consider two cases, depending upon the parity of ℓ. If $\ell \equiv 0 \pmod 2$, then the number of terms in $2^{\left(2^\ell-1\right)s} + 2^{\left(2^\ell-2\right)s} + \cdots + 2^s + 1$ is congruent to 1 modulo 3, and so,

$$2^{\left(2^\ell-1\right)s} + 2^{\left(2^\ell-2\right)s} + \cdots + 2^s + 1 \equiv 1 \pmod{2^{2s} + 2^s + 1},$$

which implies (via Gauss' Quadratic Reciprocity Law and the fact that $s > 1$, and so $2^{2s} + 2^s + 1 \equiv 1 \pmod 4$) that the Jacobi symbol

$$\begin{aligned}\left(\frac{2^{2s} + 2^s + 1}{2^{\left(2^\ell - 1\right)s} + \cdots + 2^s + 1}\right) &= \left(\frac{2^{\left(2^\ell - 1\right)s} + \cdots + 2^s + 1}{2^{2s} + 2^s + 1}\right) \\ &= \left(\frac{1}{2^{2s} + 2^s + 1}\right) = 1.\end{aligned}$$

If $\ell \equiv 1 \pmod 2$, using the same argument on the number of terms as above, then

$$2^{\left(2^\ell - 1\right)s} + 2^{\left(2^\ell - 2\right)s} + \cdots + 2^s + 1 \equiv 2^s + 1 \pmod{2^{2s} + 2^s + 1},$$

which implies (again, via Gauss' Quadratic Reciprocity Law and using that $2^{2s} + 2^s + 1 \equiv 1 \pmod 4$, for $s > 1$) that the Jacobi symbol

$$\begin{aligned}\left(\frac{2^{2s} + 2^s + 1}{2^{\left(2^\ell - 1\right)s} + \cdots + 2^s + 1}\right) &= \left(\frac{2^{\left(2^\ell - 1\right)s} + \cdots + 2^s + 1}{2^{2s} + 2^s + 1}\right) \\ &= \left(\frac{2^s + 1}{2^{2s} + 2^s + 1}\right) = \left(\frac{2^{2s} + 2^s + 1}{2^s + 1}\right) \\ &= \left(\frac{2^{2s} + 2^s + 1}{2^s + 1}\right) = \left(\frac{1}{2^s + 1}\right) = 1.\end{aligned}$$

The theorem is therefore shown. □

Remark 4.4. *We note that in the case $n = 4t$ and t is odd, the power function x^{k_n} from Theorem* 4.3 *is the Bracken-Leander power function.*

Just as in the case of quadratic permutations, we can now formulate the following theorem on the existence of decompositions of permutations into cubic power permutations and affine permutations.

Theorem 4.4. *Let $n \geq 3$ be a positive integer. All permutations on $\mathbb{F}_{2^n}$ admit a decomposition in cubic power permutations and affine permutations.*

Proof. In Theorem 4.3 we show the existence of an odd cubic power permutation x^{k_n} over $\mathbb{F}_{2^n}$ for any n. Using [Sta98, Theorem 1], we can say that $\mathrm{Sym}\left(\mathbb{F}_{2^n}\right)$ is generated by affine pemrutations and by the cubic power permutation x^{k_n} for any value of n. Then, all permutations over $\mathbb{F}_{2^n}$ admit a decomposition in cubic power permutations and affine permutations. □

Finally, we give an alternative odd power permutation for some values of n. Although this is not necessary for our existence result, the power function x^7 is interesting as it can be computed with only two multiplications and two squarings in the finite field.

Proposition 4.2. *Let $n = 3t + 1$. Then x^7 is an odd permutation on $\mathbb{F}_{2^n}$.*

Proof. Once again, using Lemma 4.1, we can say that x^7 is odd if and only if $\left(\frac{7}{2^{3t+1}-1}\right) = -1$. Using Lemma 4.2, we have that

$$\left(\frac{7}{2^{3t+1} - 1}\right) = -\left(\frac{2^{3t+1} - 1}{7}\right).$$

Now, $2^{3t} \equiv (-1)^t \pmod 7$, so we have two cases.

Case t even.

$$\left(\frac{2^{3t+1}-1}{7}\right) = \left(\frac{(2(-1)^t-1)}{7}\right) = 1,$$

so the symbol $\left(\frac{7}{2^{3t+1}-1}\right) = -1$.

Case t odd.

$$\left(\frac{2^{3t+1}-1}{7}\right) = \left(\frac{2(-1)^t-1}{7}\right) = \left(\frac{4}{7}\right) = \left(\frac{2}{7}\right)^2 = 1,$$

so the symbol is once again $\left(\frac{7}{2^{3t+1}-1}\right) = -1$.

Thus, combining the two cases, we show that $\left(\frac{7}{2^{3t+1}-1}\right) = -1$ for all t. □

5 Computational search of Stafford-like decompositions

In this section, we give some observations on the computational search of decompositions of the form

$$\tau_{a_0,b_0} \circ \pi_k \circ \tau_{a_2,b_2}\pi_k \circ \ldots \circ \pi_k \circ \tau_{a_\ell,b_\ell}. \tag{7}$$

We then use them to decompose the PRESENT [Bog+07] S-Box into cubic power permutations and affine permutations. Note that the S-Box of PRESENT is also a cubic permutation, but it is not equivalent to a power function. Thus, decomposing it into affine permutations and cubic power permutations gives a different representation, that can be useful for implementations.

At first glance, the cost of exhaustively searching all possible decomposition of length ℓ would be the cost of iterating through ℓ pairs of a_i, b_i. However, we notice that if we consider two pairs a, b and c, d, we can rewrite

$$c(ax+b)^k + d = ca^k(x+ba^{-1})^k + d,$$

since a must be non-zero. Iterating this procedure, it is easy to see that if a decomposition of length ℓ exists, then we can always rewrite it as a decomposition where all a_i except a_ℓ are equal to 1. Then, we can replace τ_{a_i,b_i} with $\tau_{1,b_i} = x + b_i$ for any $0 \leq i < \ell$ in (7), obtaining a significant reduction of the search space. One further improvement can be achieved by relaxing our search to any function D in the affine equivalence class of the target function F. Note that this is usually not problematic, since finding a decomposition

$$D = \tau_{1,b_0} \circ \pi_k \circ \tau_{1,b_1} \circ \ldots \circ \tau_{1,b_{\ell-1}} \circ \pi_k \circ \tau_{a_\ell,b_\ell}$$

naturally yields a decomposition of the same length, where every term still has the same algebraic degree, since the composition of A and τ_{1,b_0} and the composition of B and τ_{a_ℓ,b_ℓ} are still affine functions. Then, it is justified to search for a decomposition up to affine equivalence. This has two advantages. On one hand, we do not have to brute force b_0, a_ℓ, b_ℓ, further reducing the search space. On the other hand, we now target an entire affine equivalence class, rather than a single function.

We target the PRESENT S-Box `C56B90AD3EF84712` using these observations. We use the cubic power permutation $\pi_7 = x^7$, since we proved in Proposition 4.2 that we can decompose any permutation in $\mathbb{F}_{2^4}$ using π_7. However, we remember that in $\mathbb{F}_{2^4}$ all cubic power permutations are affine equivalent so that the search result would be the same using any other cubic power permutation. The truth table we use for x^7 is `019EDB76F2C5A438`, obtained constructing $\mathbb{F}_{2^5}$ using the primitive polynomial $x^5 + x^2 + 1 \in \mathbb{F}_2[x]$. We find that the S-Box is not decomposable with 5 power permutations or less, while we find 2280 decompositions length 6. That is, we find 2280 combinations of $b_1, \ldots, b_5$ such that

$$\pi_7 \circ \tau_{1,b_1} \circ \pi_7 \circ \ldots \circ \pi_7 \circ \tau_{1,b_5} \circ \pi_7$$

is affine equivalent to the PRESENT S-Box F. We give a particular solution for the sake of exposition. Consider the affine transformations A and B with truth tables, respectively, `09B2F64D813A7EC5` and `62C815BF379D40EA`. Then we can rewrite $F = A \circ D \circ B$. Now, D can be decomposed using π_7 and XORs as

$$D = \pi_7 \circ \tau_{1,3} \circ \pi_7 \circ \tau_{1,4} \circ \pi_7 \circ \tau_{1,3} \circ \pi_7 \circ \tau_{1,3} \circ \pi_7 \circ \tau_{1,3} \circ \pi_7.$$

6 Conclusions

In this paper, we studied different methods to decompose a permutation into a sequence of permutations of lower algebraic degree with the aim to find useful decompositions for hardware implementations.

The first direction we explored is the search for decompositions of the power permutations into power permutations of lower algebraic degrees. We showed that a decomposition of any power permutation into quadratic power permutations, including the inverse, always exists when $2^n - 1$ is a Mersenne prime, and that such a decomposition does not exist when n is doubly even and the target power permutation has differential uniformity lower than 16. The case when $2^n - 1$ is not prime and n is not divisible by 4 is still an open problem, though progress has been made [NNR19; Pet23; LSS23].

The second direction we explored is the search of decompositions using [Sta98, Theorem 1]. We have shown that any permutation on $\mathbb{F}_{2^n}$ can be decomposed as a sequence of affine permutations and quadratic power permutations when n is not doubly even. We have also shown that when n is doubly even, it is not possible to decompose odd permutations using only affine permutations and quadratic power permutations. We further prove that any permutation can be decomposed as a composition of affine permutations and cubic power permutations for any n.

Finally, we give an example of a decomposition of the PRESENT S-Box using cubic power permutations and affine permutations, but a more efficient search algorithm, and finding more instances of Stafford-like decompositions remain as open problems.

References

[Bil+12] B. Bilgin, S. Nikova, V. Nikov, V. Rijmen, and G. Stütz. “Threshold Implementations of All 3 ×3 and 4 ×4 S-Boxes”. In: *Cryptographic Hardware and Embedded Systems - CHES 2012 - 14th International Workshop, Leuven, Belgium, September 9-12, 2012. Proceedings.* Vol. 7428. LNCS. Springer, 2012, pp. 76–91. URL: `https://doi.org/10.1007/978-3-642-33027-8_5`.

[Bil+15] B. Bilgin, S. Nikova, V. Nikov, V. Rijmen, N. N. Tokareva, and V. Vitkup. "Threshold implementations of small S-boxes". In: *Cryptogr. Commun.* 7.1 (2015), pp. 3–33. URL: https://doi.org/10.1007/s12095-014-0104-7.

[Bil04] Y. F. Bilu. "Catalan's conjecture (after Mihăilescu)". en. In: *Séminaire Bourbaki : volume 2002/2003, exposés 909-923*. Astérisque 294. talk:909. Paris: Association des amis de Nicolas Bourbaki, Société mathématique de France, 2004, pp. 1–26. URL: http://www.numdam.org/item/SB_2002-2003__45__1_0/.

[Bog+07] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe. "PRESENT: An Ultra-Lightweight Block Cipher". In: *Cryptographic Hardware and Embedded Systems - CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings.* Vol. 4727. LNCS. Springer, 2007, pp. 450–466. URL: https://doi.org/10.1007/978-3-540-74735-2_31.

[BL10] C. Bracken and G. Leander. "A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree". In: *Finite Fields Their Appl.* 16.4 (2010), pp. 231–242. URL: https://doi.org/10.1016/j.ffa.2010.03.001.

[Bud+22] L. Budaghyan, M. Calderini, C. Carlet, D. Davidova, and N. S. Kaleyski. "On Two Fundamental Problems on APN Power Functions". In: *IEEE Trans. Inf. Theory* 68.5 (2022), pp. 3389–3403. URL: https://doi.org/10.1109/TIT.2022.3147060.

[Car21] C. Carlet. *Boolean functions for cryptography and coding theory.* Cambridge University Press, 2021.

[Car53] L. Carlitz. "Permutations in a finite field". In: *Proc. AMS* (1953), p. 538.

[ÇÖ21] P. Çomak and F. Özbudak. "On the Parity of Power Permutations". In: *IEEE Access* 9 (2021), pp. 106806–106812. URL: https://doi.org/10.1109/ACCESS.2021.3097914.

[Dem18] U. Dempwolff. "CCZ equivalence of power functions". In: *Des. Codes Cryptogr.* 86.3 (2018), pp. 665–692. ISSN: 0925-1022,1573-7586. URL: https://doi.org/10.1007/s10623-017-0350-8.

[Dem22] U. Dempwolff. "Correction to: CCZ equivalence of power functions". In: *Des. Codes Cryptogr.* 90.2 (2022), pp. 473–475. ISSN: 0925-1022,1573-7586. URL: https://doi.org/10.1007/s10623-021-00979-0.

[DS76] R. E. Dressler and E. E. Shult. "A simple proof of the Zolotareff-Frobenius theorem". In: *Proceedings of the American Mathematical Society* 54.1 (1976), pp. 53–54.

[ES96] S. M. Eikenberry and J. Sorenson. “Efficient Algorithms for Computing the Jacobi Symbol”. In: *Algorithmic Number Theory, Second International Symposium, ANTS-II, Talence, France, May 18-23, 1996, Proceedings*. Vol. 1122. LNCS. Springer, 1996, pp. 225–239. URL: https://doi.org/10.1007/3-540-61581-4_58.

[FV03] J. B. J. Fourier and I. M. Vinogradov. *Elements of Number Theory*. 2003.

[Fro14] G. F. Frobenius. *Über das quadratische Reziprozitätsgesetz I, II*. Königliche Akademie der Wissenschaften, 1914.

[Gol68] R. Gold. “Maximal recursive sequences with 3-valued recursive cross-correlation functions (Corresp.)” In: *IEEE Trans. Inf. Theory* 14.1 (1968), pp. 154–156. URL: https://doi.org/10.1109/TIT.1968.1054106.

[Kas71] T. Kasami. “The Weight Enumerators for Several Clauses of Subcodes of the 2nd Order Binary Reed-Muller Codes”. In: *Inf. Control.* 18.4 (1971), pp. 369–394. URL: https://doi.org/10.1016/S0019-9958(71)90473-6.

[LSS23] F. Luca, S. Sarkar, and P. Stănică. “Representing the inverse map as a composition of quadratics in a finite field of characteristic 2”. In: *arXiv* (2023). URL: https://arxiv.org/abs/2309.17424.

[NNR19] S. Nikova, V. Nikov, and V. Rijmen. “Decomposition of permutations in a finite field”. In: *Cryptogr. Commun.* 11.3 (2019), pp. 379–384. URL: https://doi.org/10.1007/s12095-018-0317-2.

[NRR06] S. Nikova, C. Rechberger, and V. Rijmen. “Threshold Implementations Against Side-Channel Attacks and Glitches”. In: *Information and Communications Security, 8th International Conference, ICICS 2006, Raleigh, NC, USA, December 4-7, 2006, Proceedings*. Vol. 4307. LNCS. Springer, 2006, pp. 529–545. URL: https://doi.org/10.1007/11935308_38.

[Nyb93] K. Nyberg. “Differentially Uniform Mappings for Cryptography”. In: *Advances in Cryptology - EUROCRYPT ’93, Workshop on the Theory and Application of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*. Vol. 765. LNCS. Springer, 1993, pp. 55–64. URL: https://doi.org/10.1007/3-540-48285-7_6.

[Pet23] G. Petrides. “On decompositions of permutation polynomials into quadratic and cubic power permutations”. In: *Cryptogr. Commun.* 15.1 (2023), pp. 199–207. URL: https://doi.org/10.1007/s12095-022-00600-8.

[Pic+23] E. Piccione, S. Andreoli, L. Budaghyan, C. Carlet, S. Dhooghe, S. Nikova, G. Petrides, and V. Rijmen. “An Optimal Universal Construction for the Threshold Implementation of Bijective S-Boxes”. In: *IEEE Trans. Inf. Theory* 69.10 (2023), pp. 6700–6710. URL: https://doi.org/10.1109/TIT.2023.3287534.

[Sta98] R. M. Stafford. “Groups of Permutation Polynomials over Finite Fields”. In: *Finite Fields and Their Applications* 4.4 (1998), pp. 450–452. ISSN: 1071-5797. URL: https://www.sciencedirect.com/science/article/pii/S1071579798902246.

[Wei20] M. Weissman. *An Illustrated Theory of Numbers*. Miscellaneous Books. American Mathematical Society, 2020. ISBN: 9781470463717. URL: https://books.google.no/books?id=ILH_DwAAQBAJ.

[Zol72] M. Zolotareff. “Nouvelle démonstration de la loi de réciprocité de Legendre”. fre. In: *Nouvelles annales de mathématiques : journal des candidats aux écoles polytechnique et normale* 11 (1872), pp. 354–362. URL: http://eudml.org/doc/98666.