Unicyclic strong permutations

Claude Gravel1 · Daniel Panario2 · David Thomson2

Received: 10 September 2018 / Accepted: 1 July 2019 / Published online: 19 July 2019
© Springer Science+Business Media, LLC, part of Springer Nature 2019

Abstract
In this paper, we study some properties of a certain kind of permutation σ over \(\mathbb{F}_2^n\), where \(n\) is a positive integer. The desired properties for σ are: (1) the algebraic degree of each component function is \(n - 1\); (2) the permutation is unicyclic; (3) the number of terms of the algebraic normal form of each component is at least \(2^{n-1}\). We call permutations that satisfy these three properties simultaneously unicyclic strong permutations. We prove that our permutations σ always have high algebraic degree and that the average number of terms of each component function tends to \(2^{n-1}\). We also give a condition on the cycle structure of σ. We observe empirically that for \(n\) even, our construction does not provide unicyclic permutations. For \(n\) odd, \(n \leq 11\), we conduct an exhaustive search of all σ given our construction for specific examples of unicyclic strong permutations. We also present some empirical results on the difference tables and linear approximation tables of σ.

Keywords Boolean functions · Finite fields · Permutations · Algebraic degree · Differential uniformity · Walsh spectra

Mathematics Subject Classification (2010) 11T06 · 11T71

1 Notation, facts and definitions

Let \(n\) be a positive integer. Denote by \(\mathbb{F}_2\) and \(\mathbb{F}_{2^n}\) the finite fields of 2 and \(2^n\) elements, respectively, and denote by \(\mathbb{F}_2^n\) the vector space of dimension \(n\) over \(\mathbb{F}_2\).
Let $N = \{0, 1, \ldots, n - 1\}$, let $a = (a_0, \ldots, a_{n-1})$ and for $I \subseteq N$ denote by $a_I = \prod_{i \in I} a_i$. The algebraic normal form of the Boolean function $\varphi(a)$ on the $n$ variables $a = (a_0, \ldots, a_{n-1})$ is the unique representation of $f$ in $\mathbb{F}_2[a_0, \ldots, a_{n-1}]/(a_0^2 - a_0, \ldots, a_{n-1}^2 - a_{n-1})$ of the form

$$\varphi(a) = \sum_{I \in \mathcal{P}(N)} x_I a_I, \quad x_I \in \{0, 1\},$$

where $\mathcal{P}(N)$ denotes the power set of $N$. The algebraic degree of $\varphi$ is the minimum degree of the nonzero terms of the ANF of $\varphi$. Moreover, the algebraic degree of any vectorial Boolean function $\varphi(a) = (\varphi_0(a), \ldots, \varphi_{n-1}(a))$ is the maximum algebraic degree of the component functions $\varphi_0, \ldots, \varphi_{n-1}$.

Let $\mathcal{I}_n$ be the set of irreducible polynomials of degree $n$ over $\mathbb{F}_2$ and let $Q \in \mathcal{I}_n$. For $a = (a_0, \ldots, a_{n-1}) \in \mathbb{F}_2^n$, we denote by $P_a$ the polynomial associated canonically to $a$

$$P_a(X) = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} \in \mathbb{F}_2[X]/(Q).$$

For $a \in \mathbb{F}_2^n$, $t \in [1, 2^n - 2]$ and $0 \leq j \leq n - 1$, we denote by $\varphi_{j,t}$ the boolean functions such that

$$\varphi_{j,t}(a) = \left(\sum_{i=0}^{n-1} a_i X^i \right) \mod Q.$$  

We define a permutation $\sigma$ on $\mathbb{F}_2^n$ as the concatenation of several maps

$$\sigma : \mathbb{F}_2^n \rightarrow \mathbb{F}_2[X]/(Q) \rightarrow \mathbb{F}_2[X]/(Q) \rightarrow \mathbb{F}_2^n$$

$$a \mapsto P_a(X) \mod Q \mapsto \varphi_{j,t}(a) = \left(\sum_{i=0}^{n-1} \varphi_{j,i}(a) X^i \right) \mod Q.$$  

It is necessary and sufficient that $\gcd(t, 2^n - 1) = 1$ for $\sigma$ to define a permutation on $\mathbb{F}_2^n$, so that the $t$-th power map defines a permutation of $\mathbb{F}_2^n$. For the remainder of this section, we assume that $\gcd(t, 2^n - 1) = 1$ and drop the subscript $t$ from $\varphi_{j,t}$.

We are interested in several properties of boolean functions. We are primarily concerned with boolean functions that have high algebraic degree for resilience against algebraic attacks and that have a large number of terms in their ANF [4, 5, 12]. When the vector of boolean functions $\varphi_j$ represents a permutation, entries of the difference and linear approximation tables [4, 5, 10, 14] of it, the cycle structure and the period [7, 8, 15], the number of bits required to describe, or generate, it [1, 15] and the possibility to generate it on the fly [3] are also interesting properties. As permutations, they should be comprised of a single cycle for resilience against potential Fourier-like attacks in non-commutative symmetric groups. To be considered strong for cryptographic purposes, candidate functions should also exhibit resilience against linear [13] and differential cryptanalysis [11].

**Definition 1** A permutation $\sigma$ on $n$ bits is a **unicyclic strong permutation** if it satisfies the following 3 properties:

1. the algebraic degree of $\varphi_j$ is $n - 1$ for all $0 \leq j \leq n - 1$;
2. $\sigma$ has one cycle of length $2^n$; and
3. the number of terms in the expressions $\varphi_j$ is at least $2^n - 1$ for all $j$.

Our goal in this work is to find permutations that simultaneously satisfy the properties $\mathbb{P}1$, $\mathbb{P}2$ and $\mathbb{P}3$ from Definition 1; that is, our goal is to construct unicyclic strong permutations. Property $\mathbb{P}1$ (algebraic degree) is important to prevent algebraic attacks. Property
\(\mathcal{P}2\) (unicyclicity) is to avoid short cycles in general and to avoid decomposability of attacks onto smaller permutations induced by the cycle structure. Property \(\mathcal{P}3\) (number of terms) is important to prevent algebraic attacks like linearization, exploiting hidden structures, optimization/SAT based attacks and so on. We also observe that to be considered strong for cryptographic purposes, candidate functions should exhibit resilience against linear [11] and differential cryptanalysis [2].

We present our construction of unicyclic strong permutations in Section 2, and in Section 3, we give results on Properties \(\mathcal{P}1, \mathcal{P}2,\) and \(\mathcal{P}3\) for our construction. In Section 4 we give some empirical results for our permutations. We observe experimentally that our construction only provides unicyclic permutations for \(n\) odd; so far we are unaware of a theoretical justification excluding the cases when \(n\) is even. Although our focus in this paper is to introduce permutations satisfying Properties \(\mathcal{P}1, \mathcal{P}2\) and \(\mathcal{P}3\), as already mentioned, before they can be suggested for practical use they must be found to have good resilience against linear and differential cryptanalysis. Some empirical results on the linearity and differential uniformity of such functions are also presented in Section 4.

2 Strong permutations

In this section, we define a permutation \(\sigma\) as the composition of \(n\) permutations \(\sigma_k, k = 0, 1, \ldots, n - 1\). Although we are not formally defining a cipher, we find it helpful to think of \(\sigma_k\) as round functions, for example as the rounds of a substitution-permutation network. Our precise selection of \(\sigma_k\) is motivated both by perturbations and as generalizations of the inverse function used in the S-boxes of the Advanced Encryption Standard (AES) [6]. We define and present some basic facts about the permutations \(\sigma_k\). In Section 3, we analyze local properties of \(\sigma_k\) to derive results on Properties \(\mathcal{P}1, \mathcal{P}2,\) and \(\mathcal{P}3\) for \(\sigma\).

Throughout the remainder of this paper, since \(2^n - 2^k - 1 \equiv -2^k \mod 2^n - 1\), we often use \(-2^k\) to denote this power. We also assume that all calculations in the finite field defined with modulus \(Q\) are given by canonical residues after reduction modulo \(Q\). In calculations we often suppress the \((\mod Q)\).

2.1 Permutations from perturbations

For a positive integer \(n\), let \(Q \in \mathcal{I}_n\) and let \(b \in \mathbb{F}_2^n\) with \(P_b(X) \in \mathbb{F}_2[X]\) be its canonical representation. Our main idea is the construction of a permutation \(\sigma\) as a composition of permutations

\[
\sigma = \sigma_{n-1} \cdots \sigma_1 \sigma_0
\]

of a special form. Each \(\sigma_k\) is a modified power map, as in (2): for \(k = 0, 1, \ldots, n - 1\), we define \(\sigma_k\) as

\[
\sigma_k: \mathbb{F}_2^n \longrightarrow \mathbb{F}_2[X]/(Q) \longrightarrow \mathbb{F}_2[X]/(Q) \longrightarrow \mathbb{F}_2^n,
\]

\[
a \longmapsto P_a(X) \pmod{Q} \longmapsto (\tilde{P}_a(X) + P_b(X))^t_k \pmod{Q} \longmapsto c,
\]

where \(t_k \in [1, 2^n - 2]\) and \(c = \sigma_k(a)\) is the coefficient vector of the residue of \((P_a(X) + P_b(X))^t_k \pmod{Q}\).

The novelty in \(\sigma_k\) is the addition of a fixed polynomial \(P_b \in \mathbb{F}_2[X]/(Q)\), that we call a perturbation polynomial, to the input of a power map as in (1). In effect, this performs a fixed bit flip for the inputs to the power maps. If \(n = 8\), \(Q(X) = X^8 + X^4 + X^3 + X + 1\)
(Rijndael’s polynomial) and $t \equiv -1 \pmod{255}$, with no perturbation under repeated $t$-th powers we obtain only cycles of length 2. However, we find experimentally that for exactly half of all perturbations $b \in \mathbb{F}_2^n$ the permutation

$$(P_a(X) + P_b(X))^{-1}$$

is unicyclic. We discuss more experimental results in Section 4.

### 2.2 Expanded form of a strong permutation

In this section, we prove that for all perturbation vectors $b \in \mathbb{F}_2^n$ and for all $Q \in \mathcal{I}_n$, the expansion of $(P_a(X) + P_b(X))^{-2k} \pmod{Q}$ for $0 \leq k \leq n - 1$ contains $2^{n-1}$ terms of the form $P_j^i(X)P_b^{-j}(X)$. The values of $j$ yielding nonvanishing terms are given in Proposition 1.

**Proposition 1** For $0 \leq k \leq n - 1$, the number of products of the form $P_j^i(X)P_b^{-j}(X)$ in the binomial expansion of $(P_a(X) + P_b(X))^{-2k}$ is $2^{n-1}$. Values of $j$ yielding non-vanishing terms are the integers in $\{0, 1, \ldots, 2^n - 1\}$ that are congruent to $0, \ldots, 2^k - 1$ modulo $2^{k+1}$.

**Proof** We have

$$(P_a(X) + P_b(X))^{-2k} = \sum_{j=0}^{2^n-2^k-1} \binom{2^n-2^k-1}{j} P_j^i(X)P_b^{-j-2^k-1}(X)$$

$$= P_b^{-2k}(X) \sum_{j=0}^{2^n-2^k-1} \binom{2^n-2^k-1}{j} P_j^i(X)P_b^{-j}(X).$$

Denote by $R_k$ the set containing the values of $0 \leq j \leq 2^n - 2^k - 1$ such that

$$\binom{2^n-2^k-1}{j} \equiv 1 \pmod{2}.$$ 

For any positive integer $t$, let $\nu_2(t)$ be the largest power of 2 dividing $t$. By examining the parity of binomial coefficients, $R_k$ is the set of $j$’s such that

$$\nu_2 \left( \binom{2^n-2^k-1}{j} \right) = \nu_2 \left( \binom{2^n-2^k-1-j}{j} \right) + \nu_2(j).$$

We have for $0 \leq k \leq n - 1$ that

$$R_k = \left\{ j \in \mathbb{N} \mid 0 \leq j \leq 2^n - 2^k - 1, \ j \equiv 0, 1, \ldots, 2^k - 1 \pmod{2^{k+1}} \right\}$$

$$= \left\{ j \in \mathbb{N} \mid j = 2^{k+1}q + r, \ q = 0, \ldots, 2^n-2^k-1, \ r = 0, \ldots, 2^k - 1 \right\}$$

$$= \bigoplus_{q=0}^{2^{n-k-1}-1} R_{k,q},$$

where $R_{k,q} = \{ j \in \mathbb{N} \mid 0 \leq j \leq 2^n - 1, \ j = 2^{k+1}q + r, \text{ and } r = 0, \ldots, 2^k - 1 \}$. Since $|R_{k,q}| = 2^k$ and all $R_{k,q}$ are disjoint, then $|R_k| = 2^{n-1}$ for all $0 \leq k \leq n - 1$. \qed
2.3 Composition identity

We state an observation that relates permutations as elements of the symmetric group with a bijection over a finite field.

Remark 1 From the definition of the permutations $\sigma_k$, we observe that

$$\left( P_{\sigma_k(a)}(X) \right)^{2^j} = P_{\sigma_{(k+j) \pmod{n}}(a)}(X).$$

The next proposition concerning the permutations $\sigma_k$ provides a cyclically repeated forward-and-backward type composition.

Proposition 2 For an even integer $m \geq 2$ and integers $k_j$ such that $0 \leq k_j \leq n-1$ for $0 \leq j \leq m$, let $\ell$ be defined by

$$\ell = \left( \sum_{j=0}^{m} k_j (-1)^j \pmod{2} \right) \pmod{n}.$$ 

Then,

$$\sigma_{km}^{-1} \sigma_{km-1}^{-1} \cdots \sigma_{k_2}^{-1} \sigma_{k_1}^{-1} \sigma_{k_0} = \sigma_\ell.$$

Proof For some irreducible polynomial $Q$, perturbation $P_b$ and by the definition of the $\sigma_k$’s, if $0 \leq k \leq n-1$ and $u, v \in \mathbb{F}_n^2$ are such that $v = \sigma_k(u)$, then

$$P_v(X) = P_{\sigma_k(u)}(X) = (P_u(X) + P_b(X))^{-2^k} = P_{\sigma_{-2^k}(X) + P_b(X)},$$

$$P_u(X) = P_{\sigma_{-2^k}(X) + P_b(X)}(X) + P_b(X) = P_{\sigma_{-1}(X)}(X).$$

Let $c_0, c_1 \in \mathbb{F}_n^2$ be defined by

$$P_{\sigma_{k_0}(a)}(X) = (P_a(X) + P_b(X))^{-2^{k_0}} = P_{c_0}(X),$$

$$P_{\sigma_{k_1}^{-1}(c_0)}(X) = P_{\sigma_{k_1}^{-1}(c_0)}(X) + P_b(X)$$

$$= \left((P_a(X) + P_b(X))^{-2^{k_0}}\right)^{-2^{n-k_1}} + P_b(X)$$

$$= (P_a(X) + P_b(X))^{-2^{k_0} \cdot 2^{n-k_1}} + P_b(X)$$

$$= (P_a(X) + P_b(X))^{2^{k_0-k_1} + P_b(X)} = P_{c_1}(X),$$

and

$$P_{\sigma_{k_2}(c_1)}(X) = (P_{c_1}(X) + P_b(X))^{-2^{k_2}} = \left((P_a(X) + P_b(X))^{2^{k_0-k_1}}\right)^{-2^{k_2}}$$

$$= (P_a(X) + P_b(X))^{-2^{k_0-k_1} + k_2}.$$
Corollary 1 With the same notation as in Proposition 2, for any integer $\ell \geq 0$, 
\[
\sigma_{k_{2i+2}} \left( \sigma_{k_{2i+1}}^{-1} \sigma_{k_{2i}} \cdots \sigma_{k_1} \sigma_{k_0} \right)^{\ell} (a) = \sigma_{(k_{2i+2}+t)} \pmod{n} (a),
\]
where 
\[
t = \ell \sum_{j=0}^{i} (k_{2j} - k_{2j+1}).
\]

3 Properties of strong permutations

In this section, we analyze properties of the permutations $\sigma$ introduced in (3). In particular, we address the algebraic degree, cycle structure and average number of terms in the algebraic normal form of $\sigma$ that are related to Properties $P_1$, $P_2$ and $P_3$ of Definition 1, respectively.

Remark 2 We observe that algebraic normal forms are invariant under permutation of inputs. Hence, to prove Properties $P_1$ and $P_3$ for $\sigma = \sigma_{n-1} \cdots \sigma_1 \sigma_0$, it is enough to prove them for the final permutation $\sigma_{n-1}$ in the composition.

In Sections 3.1 and 3.3, we prove a stronger result than we need given Remark 2 and we show the main results in these sections hold for all $\sigma_k$, $k = 0, \ldots, n-1$.

3.1 $P_1$–algebraic degree

For ease of notation, define $\xi_{j,k} = \varphi_{j,2^{n-2^k}-1}$ for all $j, k$ in order to match the notation from (1). In this section, we show that $\xi_{j,k}$ have high algebraic degree for all $j, k$.

Theorem 1 Let 
\[
P_{a}^{2^{n-2^k}-1}(X) = \sum_{j=0}^{n-1} \xi_{j,k}(a)X^j.
\]
Then the algebraic degree of $\xi_{j,k}$ is $n - 1$ for all $j, k$.

Proof We proceed by induction on $k$. First, let $P_a(X) = a_0 + \cdots + a_{n-1}X^{n-1}$. For $0 \leq k \leq n - 1$, and $0 \leq j \leq n - 1$, we define $\lambda_{j,k}(a)$ as the boolean function which is the coefficient of $X^j$ in the expression of $P_a^{2^k}(X)$. For $k = 0$, we have $\lambda_{j,0}(a) = a_j$, and for $k = 1$, we have 
\[
P_a^2(X) = \left( \sum_{j=0}^{n-1} a_j X^j \right)^2 = \sum_{j=0}^{n-1} a_j X^{2j} = \sum_{j=0}^{n-1} \lambda_{j,1}(a)X^j.
\]
The $\lambda_{j,1}$ are linear boolean functions with respect to $a$, since reduction (mod $Q$) does not increase the degree of the coefficient monomials. Now for $k \geq 1$, if there are linear functions $\lambda_{j,k-1}$ such that 
\[
P_a^{2^k-1}(X) = \sum_{j=0}^{n-1} \lambda_{j,k-1}(a)X^j,
\]
then
\[ P_a^{2k}(X) = P_a^{2k-1}(X) P_a^{2k-1}(X) = \sum_{j=0}^{n-1} \lambda_{j,k-1}(a) X^{2j} = \sum_{j=0}^{n-1} \lambda_{j,k}(a) X^j, \]
where \( \lambda_{j,k} \) are linear boolean functions with respect to \( a \).

Let \((\ell_0, \ldots, \ell_{n-1})\) be a permutation of \((0, 2, 2^2, \ldots, 2^{n-1})\), and observe that \(\sum_{j=0}^{n-1} \ell_j = 2^n - 2\), then
\[ P_a^{2(2^n-2)}(X) = \left( \sum_{j=0}^{n-1} \lambda_{j,k}(a) X^j \right)^{2^n-2} = \sum_{j=0}^{n-1} \ell_j \prod_{j=0}^{n-1} \lambda_{j,k}(a) X^j \ell_j \]
\[ = \sum_{j=0}^{n-1} \ell_j (2^n-2) = \sum_{j=0}^{n-1} \xi_{j,k}(a) X^j, \]
where without loss of generality we choose \( \ell_0 = 0 \), the sum extends over \((\ell_0, \ldots, \ell_{n-1})\) such that \(\ell_0 + \cdots + \ell_{n-1} = 2^n - 2\), and \( \xi_{j,k}(a) \) have degrees \( n - 1 \) with respect to \( a \) for all \( j, k \). Moreover,
\[ v_2((2^n-2)! ) = \sum_{j=1}^{2^{n-2}} v_2(j) = \sum_{j=1}^{2^{n-1}-1} v_2(j) = \sum_{j=1}^{2^{n-1}-1} (1 + v_2(j)) \]
\[ = 2^{n-1} - 1 + \sum_{j=1}^{2^{n-1}-1} v_2(j) = 2^{n-1} - 1 + \sum_{j=1}^{2^{n-1}-2} v_2(j) \]
\[ = 2^{n-1} - 1 + v_2((2^{n-1}-2)! ) = 2^{n-1} - n + v_2((2^{n-1})! ) \]
\[ = 2^n - (n + 1) = \sum_{j=1}^{n-1} v_2((2^j)! ) , \]
and therefore the multinomial coefficient is odd. Hence the algebraic degree is \( n - 1 \). \( \square \)

**Remark 3** We observe that since Theorem 1 holds for all \( a \in \mathbb{F}_2^n \), the algebraic degrees of \( \xi_{j,k} \) corresponding to \((P_a(X) + P_b(X))^{2^n-2k-1} = (P_{a+b}(X))^{2^n-2k-1} \) are \( n - 1 \) for all perturbations \( b \in \mathbb{F}_2^n \) of \( a \).

### 3.2 \( 2\)-period and cycle structure

In this section, we show that the cycle structure of \( \sigma_k \) depends only on the perturbation polynomial, and moreover we show that only \( \sigma_0 \) can be unicyclic for some perturbation.

**Theorem 2** Let \( \ell \geq 0, 0 \leq k \leq n - 1, 1 \leq j \leq \ell, \) and \( P_b \) be any perturbation. Let
\[ M_j = \begin{bmatrix} 0 & 1 \\ 1 & P_b^{2jk} \end{bmatrix}, \]
and consider \( \ell \) for which
\[ \prod_{j=1}^{\ell} M_j = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \]
For a large enough positive integer $L$, the period of $\sigma_k$ is contained in the sequence of positive integers $\ell \leq L$ satisfying (4) and

$$k\ell \equiv 0 \pmod{n}.$$  \hfill (5)

**Proof** As before, let $Q \in \mathbb{F}_2[X]$ be an irreducible polynomial of degree $n$, $P_b$ be a non-zero polynomial, and for $0 \leq k \leq n - 1$, let the bijections $\sigma_k$ be defined by the rule

$$P_a(X) \mapsto (P_a(X) + P_b(X))^{-2k} \pmod{Q}.$$  

For an arbitrary $a \in \mathbb{F}_2^n$, $\ell \geq 0$, and $0 \leq k \leq n - 1$, we define

$$P_{\sigma_\ell^k}(a)(X) = N_\ell(X)D_{\ell}^{-1}(X)$$

$$= \left(P_{\sigma_\ell^{-1}^k}(a)(X) + P_b(X)\right)^{-2k},$$

where $N_\ell \in \mathbb{F}_2[X]$, and $D_\ell \in \mathbb{F}_2[X]$, $D_\ell \neq 0$. We note that the case $\ell = 0$ corresponds to the identity permutation, and $N_0(X) = P_a(X)$, and $D_0(X) = 1$.

Reminiscent to the theory of continued fractions over fields of characteristic 0, we have for $\ell > 0$ that

$$\frac{N_\ell(X)}{D_\ell(X)} = \left(\frac{N_{\ell-1}(X)}{D_{\ell-1}(X)} + P_b(X)\right)^{-2k}.$$  \hfill (6)

From now on and for readability, we drop the argument $X$ for the elements $N_\ell$, $D_\ell$ and $P_b$. We recall that the period of a permutation $\tau$ is the smallest positive integer $m$ such that $\tau^m$ is the identity permutation.

From (6), we have for $\ell > 0$ that

$$N_\ell = D_{\ell-1}^{2k},$$

$$D_\ell = N_{\ell-1}^{2k} + P_b^{2k}D_{\ell-1}^{2k}.$$  

Equivalently in matrix notation:

$$\begin{bmatrix} \ell \\ 1 \end{bmatrix} = \left(\prod_{j=1}^{\ell} \begin{bmatrix} 0 & 1 \\ 1 & P_b^{2kj} \end{bmatrix}\right) \begin{bmatrix} N_0^{2^k} \\ D_0^{2^k} \end{bmatrix}.$$  

For $j \geq 0$, let $M_j \in \mathbb{F}_2[X]^{2 \times 2}$ be

$$M_j = \begin{bmatrix} 0 & 1 \\ 1 & P_b^{2^k} \end{bmatrix}.$$  

We have $P_a^{2^y} = P_a^{2^y \pmod{n}}$, $N_\ell^{2^k} = N_\ell^{2^k \pmod{n}}$, and $D_\ell^{2^k} = D_\ell^{2^k \pmod{n}}$, for any $a$. We obtain the cycle structure and the period from the values $\ell \leq L$ such that (4) and (5) are satisfied, with $L$ sufficiently large. \hfill \Box

**Remark 4** The matrices $M_j$, and thus the product $M_1M_2 \cdots M_\ell$ only depend on the perturbation. As a consequence, the period is independent from the input $a$. 

- Springer
Corollary 2 Only $\sigma_0$ can be unicyclic.

Proof Recall that $0 \leq k < n$. To have a single cycle of maximal length, (4) must be satisfied with $\ell = 2^n$. If $\ell = 2^n$, then (5) is only satisfied when $k = 0$. □

Remark 5 Empirically, for a fixed $n$, the proportion of perturbation polynomials leading to unicyclic $\sigma_0$’s is the same for all irreducible polynomials. For instance, we checked experimentally that if $n = 2^\kappa$ with $\kappa \in \{1, 2, 3, 4\}$, then this proportion is one half.

3.3 $\mathbb{F}_3$–average number of terms

We focus on the third property of a unicyclic strong permutation: the number of terms in the algebraic normal forms of its coordinate functions. For a positive integer $t$, its Hamming weight is the number of ones in its binary expansion. For $0 \leq t < 2^n - 1$ with Hamming weight $h$, the expansion of $P_a(X)^t$ cannot have more than $2^{h+1} - 1$ monomials. In our case, $h = n - 1$ since we consider powers $2^n - 2^k - 1$, and therefore the maximum number of terms is $2^n - 1$.

In this section we give an asymptotic result that states that the average number of terms in the algebraic normal forms of all $\sigma_k$ is $2^n - 1$, where the average is taken over all irreducibles $Q(X) \in \mathbb{F}_2[x]$ of degree $n$. In order for the permutation $\sigma = \sigma_{n-1} \cdots \sigma_1 \sigma_0$ from (3) to be considered unicyclic strong, all of its component functions must have numbers of terms greater than this average.

We require an assumption on the distribution of the coefficients of irreducible polynomials over $\mathbb{F}_2$ in order to give our main result of this section.

Assumption 1 Let $n > 0$ and let $1 \leq j \leq n - 1$. The number of irreducible polynomials of degree $n$ over $\mathbb{F}_2$ with coefficient of $X^j$ fixed to either 0 or to 1 tends to $1/2$ as $n$ tends to $\infty$.

As justification for the assumption, we recall the famous Hansen-Mullen conjecture [9], which was first proven by Wan [16, Theorem 1.6].

Theorem 3 Let $q$ be a prime power, let $m$ and $n$ be positive integers with $m \geq n \geq 1$ and let $a \in \mathbb{F}_q$ with $a \neq 0$ if $n = 1$. If either $m \geq 36$ or $q > 19$, then there is a monic irreducible polynomial in $\mathbb{F}_q[X]$ of the form $g(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + 1$, with $a_{n-1} = a$.

Theorem 3 is a result on existence of irreducible polynomials with a given coefficient fixed to any value. Assumption 1 is a reflection of the observation that the result does not depend on the fixed value $a$ for $n > 1$.

We can be more precise than this first-order heuristic. Theorem 3 was proven using character sum techniques. The main technique is to construct a characteristic function for a given quantity, extract the leading term from the trivial character, and apply an estimation (for example, the Weil bound) on the remaining sums to get an expression for the error term. Existence is guaranteed as long as the error term is dominated by the main term.

Wan’s proof essentially states that the main term is estimated by $\pi_m/(q - 1)$, where $\pi_m$ is the number of irreducible polynomials of degree $m$ over $\mathbb{F}_q$. The details are out of scope of this work. Wan’s result applies particularly well when $m$ is large with respect to $n$, and when $q$ is large. If $q$ is large, then $q - 1 \approx q$, which supports (a generalization of) Assumption 1.
1. Unfortunately, in our particular case \( q = 2 \), so we further justify Assumption 1 with experiments; see Appendix A.

**Theorem 4** For \( n > 0 \), and \( 0 \leq k \leq n - 1 \), let

\[
P_a^{2^n - 2^k - 1}(X) = \sum_{j=0}^{n-1} \xi_{j,k}(a) X^j.
\]

Using Assumption 1, the number of terms in the algebraic normal form of \( \xi_{j,k} \) tends to \( 2^n - 1 \).

**Proof** We have

\[
(P_a(X))^{2^n - 2^k - 1} = \left( \sum_{i=0}^{n-1} a_i X^i \right)^{2^n - 2^k - 1} = \left( \sum_{i=0}^{n-1} a_i X^i \right)^{(2^n - 2^k)2^k}
\]

\[
= \left( \sum_{i=0}^{n-1} a_i X^{2^k i} \right)^{2^n - 2^k} = \left( \sum_{i=0}^{n-1} \lambda_{i,k}(a) X^i \right)^{2^n - 2^k}
\]

\[
= \sum_{\ell_0, \ldots, \ell_{n-1}} \left( \ell_0, \ldots, \ell_{n-1} \right)^{2^n - 2^k} \prod_{j=0}^{n-1} \lambda_{j,k}^{\ell_j}(a) X^{\ell_j}.
\]

As in the proof of Theorem 1, let \( (\ell_0, \ldots, \ell_{n-1}) \) be one of the \( n! \) permutations of \((0, 2, \ldots, 2^n - 1)\) and observe that \( \sum_{j=0}^{n-1} \ell_j = 2^n - 2 \). For convenience, let \( \Upsilon \) be the set of vectors of integers for which the multinomial coefficient is odd, and denote by \( [P(X)]_i (\text{mod } Q) \) the coefficient of \( X^i \) in the expression of \( P \) (mod \( Q \)). Then,

\[
(P_a(X))^{2^n - 2^k - 1} = \sum_{\ell \in \Upsilon} \prod_{j=0}^{n-1} \lambda_{j,k}^{\ell_j}(a) \sum_{i=0}^{n-1} [X^{\sum_{j=0}^{n-1} \ell_j}]_i X^i
\]

\[
= \sum_{i=0}^{n-1} \left( \sum_{\ell \in \Upsilon} \prod_{j=0}^{n-1} \lambda_{j,k}^{\ell_j}(a) [X^{\sum_{j=0}^{n-1} \ell_j}]_i \right) X^i = \sum_{i=0}^{n-1} \xi_{i,k}(a) X^i,
\]

where

\[
\xi_{i,k}(a) = \sum_{\ell \in \Upsilon} \prod_{j=0}^{n-1} \lambda_{j,k}^{\ell_j}(a) [X^{\sum_{j=0}^{n-1} \ell_j}]_i.
\]

The quantities \( \ell_j \) are distinct powers of two and only one of \( \ell_j \) is zero. Hence \( \lambda_{j,k}^{\ell_j}(a) = \lambda_{j,k} \) when \( \ell_j \neq 0 \), and \( \lambda_{j,k}^{\ell_j}(a) = 1 \) when \( \ell_j = 0 \). By Assumption 1, for an arbitrary \( \ell \in \Upsilon \), the coefficient \([X^{\sum_{j=0}^{n-1} \ell_j}]_i \) (mod \( Q \)) is equally likely to be 0 or 1 as \( Q \) runs over \( \mathcal{I}_n \) and \( n \) is large. Then the average number of terms in the algebraic normal form of \( \xi_{i,k} \) is \( 2^n - 1 \). □

**Remark 6** As in Remark 3, we observe that Theorem 4 holds for all \( a \in \mathbb{F}_2^n \), and hence also for all perturbations of \( a \).
4 Empirical results on strong permutations

In this section, we present some empirical results on the compositions $\sigma = \sigma_{n-1} \cdots \sigma_0$. In Section 4.1, we give some experimental results on the proportions of strong permutations of small degrees. In Sections 4.2 and 4.3, we give some empirical analysis of the difference table and the linear approximation table for some particular $\sigma$.

4.1 Permutations satisfying properties $P_2$ and $P_3$

By Section 3.1, the algebraic degree of all $\sigma$ defined as in (3) is $n - 1$ for all $\sigma$. Since Sections 3.2 and 3.3 do not give guarantees on Properties $P_2$ and $P_3$ holding, we present some empirical results on permutations satisfying these properties.

We recall from Section 2.1, for $n = 8$, $Q(X) = X^8 + X^4 + X^3 + X + 1$ (Rijndael’s polynomial) and $t \equiv -1 \pmod{255}$, that exactly half of the possible perturbations lead to a unicyclic permutation. Empirical observations suggest that if $n = 2^{\kappa}$ for some $\kappa$ and $t \equiv -1 \pmod{2^{n-1}}$, then there are exactly $2^{n-1}$ unicyclic permutations given by the rule

$$P_a(X) \mapsto (P_a(X) + P_b(X))^{-1} \pmod{Q}.$$ 

When $\kappa = 1, 2, 3,$ and 4, we empirically verified that the proportion of perturbation polynomials for an arbitrary representation that lead to unicyclic permutations is exactly one half. We stop at $\kappa = 4$ given our computational resources, noting that when $\kappa = 5$, there are approximately $2^{27}$ irreducible polynomials and $2^{32}$ perturbation polynomials yielding approximately $2^{59}$ pairs for which the cycle structure must be found.

For $\sigma = \sigma_{n-1} \cdots \sigma_0$, $n$ even, and $n \leq 30$, we conducted an exhaustive search over all irreducible polynomials and all perturbation vectors and found no unicyclic permutations. We conjecture that this continues to hold.

Conjecture 1 If $n$ is even, then the composition $\sigma = \sigma_{n-1} \cdots \sigma_0$ is not unicyclic.

In Table 1, we run exhaustively through all pairs of irreducible and perturbation polynomials and count for a given perturbation how many irreducible polynomials lead to a unicyclic permutation $\sigma$. For brevity, we report only the minimum and maximum ratios of the number of irreducibles per perturbation.

Let $J_n$ be the number of irreducible polynomials of degree $n$ such that, for the fixed perturbation polynomial $P_b(X) = X^{n-1} + 1$, the permutation $\sigma$ from (3) is unicyclic. Table 2 shows exhaustive results for the ratio $J_n/I_n$ for odd $n \leq 25$. We also sampled randomly 4000 irreducible polynomials of degree 33 among which 483 led to unicyclic permutations, and thus resulting in an estimation of $|J_{33}|/|I_{33}| \approx 0.12075$.

Based on the experimental evidence in Tables 1 and 2, we make the following conjecture.

| Table 1 | Min-max ratios of unicyclic permutations of degree $n$ |
|---------|---------------------------------|
| $n = 7$  | $n = 9$  | $n = 11$ |
| Min     | 2       | Min      | 14 |
| Max     | 14      | Max      | 49 |
| $|I_7|/|I_9|$ | 18      | $|I_{11}|$ | 186 |
Table 2  Ratios $\mathcal{J}_n/\mathcal{I}_n$ when $P_b(X) = 1 + X^{n-1}$

| $n$ | $|\mathcal{J}_n|$ | $|\mathcal{I}_n|$ | $|\mathcal{J}_n|/|\mathcal{I}_n|$ |
|-----|------------------|------------------|------------------|
| 3   | 1                | 2                | 0.5              |
| 5   | 2                | 6                | 0.333333         |
| 7   | 6                | 18               | 0.333333         |
| 9   | 10               | 56               | 0.178571         |
| 11  | 30               | 186              | 0.16129          |
| 13  | 87               | 630              | 0.138095         |
| 15  | 259              | 2182             | 0.118698         |
| 17  | 1130             | 7710             | 0.146563         |
| 19  | 3805             | 27594            | 0.137892         |
| 21  | 12551            | 99858            | 0.125688         |
| 23  | 46290            | 364722           | 0.126919         |
| 25  | 153976           | 1342176          | 0.114721         |

Conjecture 2  For odd values of $n$, and $P_b$ not constant,

$$\lim \inf_{n \to \infty} \frac{|\mathcal{J}_n|}{|\mathcal{I}_n|} \neq 0.$$  

In order for a permutation $\sigma$ to be “strong”, its component functions must all have at least $2^{n-1}$ terms (that is, it must also satisfy Property P3). We expect that this property is quite rare, a rough approximation based on Theorem 4 gives that as $n$ grows, roughly $1/2^n$ of all component functions will have at least $2^{n-1}$ terms. So, we expect roughly $1/2^n$ unicyclic permutations to be strong.

Table 3 tabulate the results of an exhaustive search for the total number of unicyclic permutations constructed as in (3) for $n = 7, 9, 11$ (the search is currently running for $n = 13$).

4.2 Examples of difference tables

The difference table of a function is a crucial tool in analyzing its resilience against differential cryptanalysis [2]. Let $f: \mathbb{F}_2^n \to \mathbb{F}_2^n$, and index the rows and columns of a $2^n \times 2^n$ table $D_f$ with the elements of $\mathbb{F}_2^n$. For $(c, d) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$, the entry at row $c$ and column $d$ of $D_f$ is the number of pre-images $a \in \mathbb{F}_2^n$ of the expression $f(a + c) + f(a) = d$; that is,

$$D_f(c, d) = \sum_{a \in \mathbb{F}_2^n} \mathbb{I} \{f(a + c) + f(a) = d\},$$

Table 3  Proportions of unicyclic permutations that are “strong”

| $n$ | Unicyclic | Strong |
|-----|-----------|--------|
| 7   | 756       | 5      |
| 9   | 5040      | 3      |
| 11  | 61380     | 21     |
| 13  | unknown   | $\geq 10$ |
Differentials over all unicyclic permutations for \( n = 7, 9, 11 \)

| \( n = 7 \) | \( n = 9 \) | \( n = 11 \) |
|-----------------|-----------------|-----------------|
| \( |I_7| = 18 \) | \( |I_9| = 56 \) | \( |I_{11}| = 186 \) |
| \( |T_7| = 756 \) | \( |T_9| = 5040 \) | \( |T_{11}| = 61380 \) |

| Differentials | Counts | Differentials | Counts | Differentials | Counts |
|---------------|--------|---------------|--------|---------------|--------|
| 0             | 6545700| 0             | 673216992| 0             | 129465640194|
| 2             | 5541102| 2             | 636750576| 2             | 127302770628|
| 4             | 292572 | 4             | 11137392 | 4             | 676155942 |
| 6             | 6174   | 6             | 95760   | 6             | 1751376 |
| 128           | 756    | 512           | 5040    | 2048          | 61380  |

where \( \mathbb{I}\{\cdot\} \) denotes the indicator function of 0. The maximum entry of \( \mathcal{D}_f \) is the differential uniformity of \( f \), and it is desirable for resilience against differential cryptanalysis to have differential uniformity as small as possible.

In fields of characteristic 2 the differential uniformity of a function is always at least 2. Functions with differential uniformity equal to 2 are almost perfect nonlinear (APN). The inverse function \( x \mapsto x^{2^{n-2}} \) is APN when \( n \) is odd, and otherwise has differential uniformity 4; see [5, Section 3.1.7].

We present summaries of difference tables for \( n = 7, n = 9, \) and \( n = 11 \). See Appendix B for more statistics. In Table 4, \( n \) refers to the degree, \( |I_n| \) to the number of irreducible polynomial of degree \( n \), and \( |T_n| \) to the number of pairs that lead to a unicyclic permutation. We count the number of unicyclic compositions \( \sigma_{n-1} \cdots \sigma_0 \) for possible differentials, and only nonzero counts are reported. The trivial counts for the maximal differential value of \( 2^n \) are also reported.

We note that for a given \( n \) the sum over all counts divided by \( T_n \) is always equal to \( 2^n \). In our experiments, for \( n \leq 13 \) the maximum entry in the difference table is at most 6. Moreover, the differential 6 occurs rarely. For \( n = 15 \), Example 1 from Appendix B shows a unicyclic permutation that is nearly APN except for a degenerate hyperplane.

Table 5 Distribution of Walsh coefficients over all unicyclic permutations with \( n = 7 \)

| Coefficients | Counts | Coefficients | Counts |
|--------------|--------|--------------|--------|
| −32          | 378    | 4            | 1367226|
| −28          | 17136  | 8            | 1288224|
| −24          | 140238 | 12           | 1185786|
| −20          | 486864 | 16           | 881622 |
| −16          | 864360 | 20           | 478674 |
| −12          | 1202796| 24           | 139482 |
| −8           | 1282176| 28           | 15750  |
| −4           | 1366344| 32           | 378    |
| 0            | 1668114| 128          | 756    |
4.3 Examples of linear approximation tables

The Walsh spectrum of a function is a crucial tool in analyzing its resilience against linear cryptanalysis \[11\]. Let \( f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n \) and let \( c, d \in \mathbb{F}_2^n \times \mathbb{F}_2^n \). The Walsh coefficient \( W_f(c, d) \) of \( f \) at \( c, d \) is given by

\[
W_f(c, d) = \sum_{a \in \mathbb{F}_2^n} (-1)^{a \cdot c + d \cdot f(a)},
\]

where \( \cdot \) denotes the usual scalar product. The values of the Walsh coefficients measure the distance between a given function and the set of affine functions, and hence the table containing the Walsh coefficients is sometimes called the linear approximation table. Similarly to the difference table, we highlight the largest entry (in magnitude) in the linear approximation table, and call this the linearity of \( f \).

We present summaries of linear approximation tables for \( n = 7, n = 9, \) and \( n = 11 \). See Appendix B for more statistics. In Tables 5, 6, and 7, \( n \) refers to the degree, \(|\mathcal{L}_n|\) to the number of irreducible polynomial of degree \( n \), and \(|\mathcal{T}_n|\) to the number of pairs that lead to a unicyclic permutation. We count the number of unicyclic compositions \( \sigma_{n-1} \cdots \sigma_0 \) for possible correlations, and only nonzero counts are reported. The trivial maximal or minimal values \( \pm 2^n \) are also reported as a check.

We observe that the Walsh coefficients of our unicyclic permutations are tightly compacted around 0, especially in comparison to a uniform random permutation as in Appendix B. As expected, the weighted average of the Walsh coefficients is 0.

| Table 6 | Distribution of Walsh coefficients over all unicyclic permutations with \( n = 9 \) |
|----------|--------------------------------------------------|
| \( n = 9 \) |                                                                                           |
| \(|\mathcal{L}_9| = 56 \) |                                                                                           |
| \(|\mathcal{T}_9| = 5040 \) |                                                                                           |
| Coefficients | Counts | Coefficients | Counts |
| --- | --- | --- | --- |
| \(-60\) | 504 | \(4\) | 72997848 |
| \(-56\) | 35784 | \(8\) | 73843056 |
| \(-52\) | 668304 | \(12\) | 75178152 |
| \(-48\) | 4377744 | \(16\) | 72959544 |
| \(-44\) | 14541912 | \(20\) | 64853208 |
| \(-40\) | 29371104 | \(24\) | 60175080 |
| \(-36\) | 42948864 | \(28\) | 57930768 |
| \(-32\) | 52182648 | \(32\) | 52175592 |
| \(-28\) | 58134888 | \(36\) | 42539112 |
| \(-24\) | 60220944 | \(40\) | 29639736 |
| \(-20\) | 64415736 | \(44\) | 14436576 |
| \(-16\) | 72875880 | \(48\) | 4386816 |
| \(-12\) | 75241656 | \(52\) | 689976 |
| \(-8\) | 73638432 | \(56\) | 50904 |
| \(-4\) | 73057824 | \(512\) | 5040 |
| 0 | 77632128 |
Table 7  Distribution of Walsh coefficients over all unicyclic permutations with \( n = 11 \)

| Coefficients | Counts | Coefficients | Counts |
|--------------|--------|--------------|--------|
| -108         | 10230  | 4            | 7190926842 |
| -104         | 777480 | 8            | 7251819894 |
| -100         | 17145480 | 12       | 7065347545 |
| -96          | 141090114 | 16      | 7134428598 |
| -92          | 572151624 | 20      | 7557831930 |
| -88          | 1386917928 | 24     | 7312983018 |
| -84          | 2406924630 | 28     | 6648708198 |
| -80          | 3331962150 | 32     | 6391800162 |
| -76          | 3885243516 | 36     | 6449828814 |
| -72          | 4243987110 | 40     | 6482409318 |
| -68          | 4616684444 | 44     | 6421456932 |
| -64          | 4985688708 | 48     | 6359592030 |
| -60          | 5358269400 | 52     | 6104515164 |
| -56          | 5710862718 | 56     | 5702230644 |
| -52          | 6099580212 | 60     | 5362862670 |
| -48          | 6361061058 | 64     | 4989750018 |
| -44          | 6425397528 | 68     | 4611074292 |
| -40          | 6479716782 | 72     | 4247581932 |
| -36          | 6449734698 | 76     | 3887400000 |
| -32          | 6387153696 | 76     | 3887400000 |
| -28          | 6649688232 | 80     | 3331630698 |
| -24          | 7306112550 | 84     | 2405177346 |
| -20          | 7567429716 | 88     | 1384610040 |
| -16          | 7135218354 | 92     | 571769022 |
| -12          | 7062515790 | 96     | 140161230 |
| -8           | 7246246590 | 100    | 17010444 |
| -4           | 7188592356 | 104    | 789756 |
| 0            | 7406442252 | 108    | 16368 |
|              |         | 2048    | 61380  |

5 Conclusion

In this paper, we give permutations over \( \mathbb{F}_2^n \) that simultaneously satisfy at least three properties of interest in cryptography: high algebraic degree and large number of terms in the algebraic normal forms of their component functions, and maximal cycle size. Experimentally, we also find that these permutations have properties that may indicate good resistance against linear and differential cryptanalysis.

It would be interesting to study the distributions of the coefficients of the difference table and linear approximation table of strong unicyclic permutations. Other future work includes determining conditions under which our composition from Section 4 is unicyclic; this would imply a proof of Conjecture 2 and would likely explain the dichotomy in the cycle structures between odd and even degrees. Another path for future work is to obtain analytic conditions for when a unicyclic permutation has large number of terms in the algebraic normal forms of its component functions.
Acknowledgments  The authors are grateful for the very careful reviews and the constructive suggestions received from the referees.

Appendix A: Empirical evidence for Assumption 1

In Tables 8, 9, 10, and 11, the column entitled \(i\) refers to the coefficients of \(X^i\) of an irreducible polynomial of degree \(d\). The column entitled “Ratios” gives the ratios of the number of irreducible polynomials of degree \(d\) with a \(X^i\) term.

Table 8  Average proportions by terms of irreducible polynomials

| \(d = 2\) | \(d = 3\) | \(d = 4\) | \(d = 5\) |
|-----------|-----------|-----------|-----------|
| \(i\)     | Ratios    | \(i\)     | Ratios    | \(i\)     | Ratios    | \(i\)     | Ratios    |
| 1         | 1.000000  | 1         | 0.500000  | 1         | 0.666667  | 1         | 0.500000  |
| 2         | 0.500000  | 2         | 0.333333  | 2         | 0.666667  | 2         | 0.666667  |
| 3         | 0.666667  | 3         | 0.666667  | 3         | 0.666667  | 3         | 0.666667  |

Table 9  Average proportions by terms of irreducible polynomials (continued)

| \(d = 6\) | \(d = 7\) | \(d = 8\) | \(d = 9\) |
|-----------|-----------|-----------|-----------|
| \(i\)     | Ratios    | \(i\)     | Ratios    | \(i\)     | Ratios    | \(i\)     | Ratios    |
| 1         | 0.555556  | 1         | 0.500000  | 1         | 0.533333  | 1         | 0.500000  |
| 2         | 0.444444  | 2         | 0.500000  | 2         | 0.533333  | 2         | 0.464286  |
| 3         | 0.333333  | 3         | 0.500000  | 3         | 0.600000  | 3         | 0.517857  |
| 4         | 0.444444  | 4         | 0.500000  | 4         | 0.533333  | 4         | 0.517857  |
| 5         | 0.555556  | 5         | 0.500000  | 5         | 0.600000  | 5         | 0.517857  |
| 6         | 0.500000  | 6         | 0.533333  | 6         | 0.533333  | 6         | 0.517857  |
| 7         | 0.533333  | 7         | 0.533333  | 7         | 0.533333  | 7         | 0.464286  |
| 8         |           |           |           |           |           |           | 8         | 0.500000  |

Table 10  Average proportions by terms of irreducible polynomials (continued)

| \(d = 10\) | \(d = 11\) | \(d = 12\) | \(d = 13\) |
|-----------|-----------|-----------|-----------|
| \(i\)     | Ratios    | \(i\)     | Ratios    | \(i\)     | Ratios    | \(i\)     | Ratios    |
| 1         | 0.515152  | 1         | 0.500000  | 1         | 0.507463  | 1         | 0.500000  |
| 2         | 0.515152  | 2         | 0.500000  | 2         | 0.492537  | 2         | 0.507937  |
| 3         | 0.484848  | 3         | 0.500000  | 3         | 0.507463  | 3         | 0.507937  |
| 4         | 0.474747  | 4         | 0.516129  | 4         | 0.498507  | 4         | 0.500000  |
| 5         | 0.494949  | 5         | 0.516129  | 5         | 0.477612  | 5         | 0.512698  |
| 6         | 0.474747  | 6         | 0.516129  | 6         | 0.504478  | 6         | 0.495238  |
| 7         | 0.484848  | 7         | 0.516129  | 7         | 0.477612  | 7         | 0.495238  |
| 8         | 0.515152  | 8         | 0.500000  | 8         | 0.498507  | 8         | 0.512698  |
| 9         | 0.515152  | 9         | 0.500000  | 9         | 0.507463  | 9         | 0.500000  |
| 10        | 0.500000  | 10        | 0.492537  | 10        | 0.507937  |
| 11        | 0.507463  | 11        | 0.507937  |
| 12        |           | 12        | 0.500000  |

\[ \text{Cryptography and Communications (2019) 11:1211–1231} \]
In order to make this article concise, we jump from degree 13 to 26 up to 29 inclusively.

Table 11  Average proportions by terms of irreducible polynomials (continued)

| $d = 26$ | $d = 27$ | $d = 28$ | $d = 29$ |
|----------|----------|----------|----------|
| $i$      | Ratios   | $i$      | Ratios   | $i$      | Ratios   | $i$      | Ratios   |
| 1        | 0.500061 | 1        | 0.500000 | 1        | 0.500031 | 1        | 0.500000 |
| 2        | 0.500061 | 2        | 0.500000 | 2        | 0.499969 | 2        | 0.500031 |
| 3        | 0.499939 | 3        | 0.500092 | 3        | 0.500031 | 3        | 0.500031 |
| 4        | 0.500036 | 4        | 0.500118 | 4        | 0.500063 | 4        | 0.499945 |
| 5        | 0.500098 | 5        | 0.499878 | 5        | 0.499957 | 5        | 0.500007 |
| 6        | 0.499999 | 6        | 0.500101 | 6        | 0.499967 | 6        | 0.499954 |
| 7        | 0.500038 | 7        | 0.500101 | 6        | 0.500003 | 7        | 0.499999 |
| 8        | 0.499982 | 7        | 0.500219 | 8        | 0.500044 | 8        | 0.499960 |
| 9        | 0.500092 | 9        | 0.499944 | 9        | 0.499936 | 9        | 0.500074 |
| 10       | 0.499886 | 10       | 0.500054 | 10       | 0.500089 | 10       | 0.500139 |
| 11       | 0.500013 | 11       | 0.499764 | 11       | 0.499940 | 11       | 0.500091 |
| 12       | 0.499996 | 12       | 0.500161 | 12       | 0.499999 | 12       | 0.500012 |
| 13       | 0.499994 | 13       | 0.500063 | 13       | 0.499884 | 13       | 0.499931 |
| 14       | 0.499996 | 14       | 0.500063 | 14       | 0.499982 | 14       | 0.499990 |
| 15       | 0.500013 | 15       | 0.500161 | 15       | 0.499984 | 15       | 0.499990 |
| 16       | 0.499886 | 16       | 0.499764 | 16       | 0.499999 | 16       | 0.499931 |
| 17       | 0.500092 | 17       | 0.500054 | 17       | 0.499940 | 17       | 0.500012 |
| 18       | 0.499982 | 18       | 0.499944 | 18       | 0.500089 | 18       | 0.500091 |
| 19       | 0.500038 | 19       | 0.500219 | 19       | 0.499936 | 19       | 0.500139 |
| 20       | 0.499999 | 20       | 0.500101 | 20       | 0.500044 | 20       | 0.500074 |
| 21       | 0.500098 | 21       | 0.500101 | 21       | 0.500031 | 21       | 0.499960 |
| 22       | 0.500036 | 22       | 0.499878 | 22       | 0.499967 | 22       | 0.499999 |
| 23       | 0.499939 | 23       | 0.500118 | 23       | 0.499957 | 23       | 0.499954 |
| 24       | 0.500061 | 24       | 0.500092 | 24       | 0.500063 | 24       | 0.500007 |
| 25       | 0.500061 | 25       | 0.500000 | 25       | 0.500031 | 25       | 0.499945 |
| 26       | 0.500000 | 26       | 0.499969 | 26       | 0.500031 | 26       | 0.500031 |
| 27       | 0.500000 | 27       | 0.500031 | 27       | 0.500031 | 28       | 0.500000 |

Appendix B: Differentials and correlations

Example 1 gives two unicyclic permutations that are APN except for a fixed set of $2^{15}$ pairs giving differentials of size $2^{15}$.

Example 1  The following two examples give unicyclic permutations $\sigma$ that are APN aside from $2^{15}$ $(c, d)$ pairs each giving $2^{15}$ solutions to $\sigma(X \oplus c) \oplus \sigma(X) = d$. A summary of both
difference tables is given in Table 12. We present these examples for interest and further study, but we make no claims on their suitability for cryptography.

Table 12  Summary of the difference tables of two unicyclic strong permutations from (7) and (8)

| Differentials | Counts       |
|---------------|--------------|
| 0             | 1073250409   |
| 2             | 458647       |
| 32768         | 32768        |

\[
Q_1(X) = 1 + X + X^7 + X^{10} + X^{15} \quad (7) \\
P_{1,b}(X) = 1 + X^3 + X^5 + X^7 + X^{11} + X^{12} + X^{13} \\
Q_2(X) = 1 + X^2 + X^3 + X^7 + X^8 + X^{12} + X^{13} + X^{14} + X^{15} \quad (8) \\
P_{2,b}(X) = X^2 + X^5 + X^6 + X^7 + X^8 + X^{11} + X^{12} + X^{14}
\]

**Example 2** Let \( n = 17 \) and let \( Q \) and \( P_b \) be as follows,
\[
Q(X) = 1 + X + X^4 + X^8 + X^{11} + X^{12} + X^{13} + X^{14} + X^{15} + X^{16} + X^{17}, \\
P_b(X) = 1 + X^{16}.
\]

The difference table for \( \sigma \) defined with \( Q \) and \( P_b \) is

| Differentials | Counts       |
|---------------|--------------|
| 0             | 8591113477   |
| 2             | 8587642420   |
| 4             | 1113222      |
| 6             | 64           |
| 131072        | 1            |

**Example 3** Let \( n = 19 \) and let \( Q \) and \( P_b \) be as follows,
\[
Q(X) = 1 + X^5 + X^7 + X^8 + X^9 + X^{11} + X^{13} + X^{16} + X^{17} + X^{18} + X^{19}, \\
P_b(X) = 1 + X^{18}.
\]

The difference table for \( \sigma \) defined with \( Q \) and \( P_b \) is

| Differentials | Counts       |
|---------------|--------------|
| 0             | 137444193323 |
| 2             | 137428735987 |
| 4             | 4977558      |
| 6             | 75           |
| 524288        | 1            |

Example 4 gives a comparison of a particular unicyclic permutation with a uniformly randomly sampled permutation.
Example 4 Let $n = 15$ and let $Q$ and $P_b$ be as follows,

\[ Q(X) = 1 + X^3 + X^4 + X^5 + X^7 + X^{14} + X^{15}, \]

\[ P_b(X) = 1 + X^{14}. \]

The linear approximation table for $\sigma$ defined with $Q$ and $P_b$ is

| Coefficients | Counts   | Coefficients | Counts   |
|--------------|----------|--------------|----------|
| $-384$       | 6 (extreme) | $4$          | 7419616  |
| $-380$       | $146$    | $8$          | 7521798  |
| $\vdots$     | $\vdots$ | $12$         | 7751075  |
| $-12$        | 7748469  | $\vdots$    | $\vdots$ |
| $-8$         | 7519934  | 380          | 148      |
| $-4$         | 7416332  | 384          | 4 (extreme) |
| $0$          | 7486434  | 32768        | 1 (trivial) |

Comparing with a uniform random permutation, we obtain

| Coefficients | Counts   | Coefficients | Counts   |
|--------------|----------|--------------|----------|
| $-1088$      | 1 (extreme) | $4$          | 9464656  |
| $-1072$      | 1        | $\vdots$    | $\vdots$ |
| $\vdots$     | $\vdots$ | 380          | 1046219  |
| $-384$       | 998280   | 384          | 997790   |
| $-380$       | 1044401  | $\vdots$    | $\vdots$ |
| $\vdots$     | $\vdots$ | 1196         | 1        |
| $-4$         | 9465140  | 1252         | 1 (extreme) |
| $0$          | 9525299  | 32768        | 1 (trivial) |

Appendix C: An example with intermediate round computations

For $1 \leq i \leq n$, let

\[ P_{a^{(i)}}(X) = \left( P_{a^{(i-1)}}(X) + P_b(X) \right)^{-2^{i-1}}. \]

In Table 13, we give the sequence $a = a^{(0)} \rightarrow a^{(1)} \rightarrow \cdots \rightarrow a^{(n)}$; columns entitled $a^{(i)}$ contain the output of the partial computations $a^{(i)} = \sigma_{i-1} \sigma_{i-2} \cdots \sigma_0$. In each column, we give an underlined boldfaced entry that signifies a cycle that is not of maximal length up to the given column/round. For instance, after two rounds, we have a fixed point since $\sigma_1 \sigma_0(59) = 59$, and after four rounds we have a cycle of length three since $\sigma_3 \sigma_2 \sigma_1 \sigma_0(0) = 23, \sigma_3 \sigma_2 \sigma_1 \sigma_0(23) = 35$, and $\sigma_3 \sigma_2 \sigma_1 \sigma_0(35) = 0$.

As expected, since the degree is even ($n = 6$), the resulting composition is not unicyclic although the initial round corresponding to $\sigma_0$ is unicyclic.
Table 13  Intermediate round computations for $P_b(X) = 1 + X^5$ and $Q(X) = 1 + X + X^4 + X^5 + X^6$

| $a$ | $a^{(1)}$ | $a^{(2)}$ | $a^{(3)}$ | $a^{(4)}$ | $a^{(5)}$ | $a^{(6)}$ | $a$ | $a^{(1)}$ | $a^{(2)}$ | $a^{(3)}$ | $a^{(4)}$ | $a^{(5)}$ | $a^{(6)}$ |
|-----|-----------|-----------|-----------|-----------|-----------|-----------|-----|-----------|-----------|-----------|-----------|-----------|-----------|
| 0   | 10        | 38        | 39        | 23        | 19        | 39        | 32     | 1         | 36        | 24        | 37        | 18        | 35        |
| 1   | 13        | 5         | 29        | 53        | 34        | 48        | 33     | 0         | 49        | 32        | 1         | 16        | 33        |
| 2   | 46        | 13        | 17        | 17        | 63        | 30        | 34     | 44        | 18        | 34        | 24        | 3         | 41        |
| 3   | 38        | 40        | 53        | 43        | 27        | 36        | 35     | 58        | 25        | 33        | 0         | 56        | 27        |
| 4   | 48        | 24        | 12        | 14        | 50        | 10        | 36     | 55        | 20        | 52        | 21        | 53        | 22        |
| 5   | 18        | 43        | 59        | 36        | 48        | 55        | 37     | 29        | 61        | 25        | 19        | 40        | 53        |
| 6   | 47        | 10        | 6         | 39        | 43        | 14        | 38     | 50        | 45        | 44        | 29        | 61        | 45        |
| 7   | 34        | 55        | 46        | 2         | 6         | 21        | 39     | 22        | 17        | 5         | 26        | 10        | 51        |
| 8   | 43        | 19        | 47        | 45        | 57        | 17        | 40     | 61        | 56        | 19        | 50        | 25        | 28        |
| 9   | 21        | 53        | 23        | 33        | 0         | 25        | 41     | 52        | 39        | 35        | 15        | 22        | 3         |
| 10  | 41        | 60        | 62        | 31        | 29        | 8         | 42     | 12        | 28        | 60        | 13        | 12        | 19        |
| 11  | 20        | 9         | 50        | 56        | 28        | 60        | 43     | 33        | 0         | 45        | 55        | 41        | 9         |
| 12  | 59        | 62        | 30        | 44        | 26        | 49        | 44     | 32        | 1         | 2         | 38        | 21        | 61        |
| 13  | 3         | 6         | 40        | 61        | 49        | 29        | 45     | 11        | 46        | 36        | 11        | 38        | 47        |
| 14  | 39        | 42        | 3         | 46        | 4         | 11        | 46     | 62        | 31        | 18        | 22        | 37        | 58        |
| 15  | 35        | 29        | 8         | 42        | 17        | 12        | 47     | 25        | 14        | 21        | 8         | 35        | 18        |
| 16  | 19        | 21        | 61        | 10        | 46        | 16        | 48     | 57        | 12        | 27        | 62        | 30        | 57        |
| 17  | 37        | 26        | 56        | 59        | 2         | 20        | 49     | 26        | 54        | 38        | 7         | 23        | 59        |
| 18  | 23        | 27        | 16        | 27        | 13        | 37        | 50     | 49        | 15        | 43        | 28        | 52        | 50        |
| 19  | 7         | 22        | 63        | 30        | 55        | 38        | 51     | 36        | 57        | 37        | 32        | 1         | 62        |
| 20  | 60        | 16        | 28        | 9         | 39        | 34        | 52     | 40        | 8         | 22        | 12        | 33        | 0         |
| 21  | 8         | 34        | 57        | 3         | 51        | 13        | 53     | 42        | 37        | 15        | 34        | 11        | 6         |
| 22  | 5         | 58        | 10        | 20        | 9         | 7         | 54     | 51        | 2         | 41        | 52        | 47        | 56        |
| 23  | 28        | 52        | 7         | 35        | 32        | 1         | 55     | 6         | 50        | 54        | 6         | 7         | 43        |
| 24  | 17        | 3         | 20        | 60        | 36        | 44        | 56     | 14        | 7         | 42        | 5         | 15        | 42        |
| 25  | 27        | 4         | 55        | 51        | 62        | 31        | 57     | 63        | 30        | 48        | 48        | 44        | 15        |
| 26  | 45        | 48        | 11        | 41        | 60        | 2         | 58     | 56        | 33        | 0         | 54        | 20        | 52        |
| 27  | 2         | 51        | 4         | 57        | 5         | 32        | 59     | 16        | 59        | 13        | 63        | 31        | 26        |
| 28  | 9         | 47        | 49        | 18        | 42        | 63        | 60     | 4         | 44        | 58        | 49        | 58        | 54        |
| 29  | 53        | 35        | 26        | 25        | 59        | 4         | 61     | 54        | 41        | 9         | 40        | 8         | 23        |
| 30  | 24        | 63        | 31        | 58        | 45        | 24        | 62     | 30        | 11        | 51        | 16        | 14        | 40        |
| 31  | 15        | 23        | 14        | 47        | 54        | 46        | 63     | 31        | 32        | 1         | 4         | 24        | 5         |

References

1. Bacher, A., Bodini, O., Hwang, H.-K., Tsai, T.-H.: Generating random permutations by coin tossing: Classical algorithms, new analysis, and modern implementation. ACM Trans. Algor. 13(2), 1–43 (2017)
2. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. J. Cryptol. 4(1), 3–72 (1991)
3. Brassard, G., Kannan, S.: The generation of random permutations on the fly. Inf. Process. Lett., 28(4) (1988)
4. Carlet, C.: Boolean functions for cryptography and error correcting codes. In: Crama, Y., Hammer, P.L. (eds.) Boolean Models and Methods in Mathematics, Computer Science, and Engineering, pp. 257–397. Cambridge University Press (2010). monography’s chapter
5. Carlet, C.: Vectorial boolean functions for cryptography. In: Crama, Y., Hammer, P.L. (eds.) Boolean Models and Methods in Mathematics, Computer Science, and Engineering, pp. 398–469. Cambridge University Press (2010). monography’s chapter
6. Daemen, J., Vincent, R.: The Design of Rijndael: AES-the Advanced Encryption Standard. Springer Science & Business Media (2013)
7. Flajolet, P., Odlyzko, A.M.: Random mapping statistics. In: Quisquater, J.-J., Vandewalle, J. (eds.) Advances in Cryptology — EUROCRYPT ’89, vol. 434, pp. 329–354. LNCS (1990)
8. Flajolet, P., Sedgewick, R.: Analytic Combinatorics, 1st edn. Cambridge University Press (2009)
9. Hansen, T., Mullen, G.L.: Primitive polynomials over finite fields. Math. Comput. 59(200), 639–643 (1992)
10. Xiao, G.-Z., Massey, L., James: A spectral characterization of correlation-immune combining functions. IEEE Trans. Inf. Theory 34(3), 569–571 (1988)
11. Matsui, M.: Linear cryptanalysis method for DES cipher. In: Workshop on the Theory and Application of of Cryptographic Techniques, pp. 386–397. Springer (1993)
12. Mullen, G.L., Panario, D.: Handbook of Finite Fields. Chapman & Hall/CRC (2013)
13. Nyberg, K.: Statistical and linear independence of binary random variables. Cryptology ePrint Archive Report 2017/432 (2017)
14. Siegenthaler, T.: Correlation-immunity of nonlinear combining functions for cryptographic applications. IEEE Trans. Info. Th. 30, 776–780 (1984)
15. Szpankowski, W.: Average Case Analysis of Algorithms on Sequences. Wiley (2001)
16. Wan, D.: Generators and irreducible polynomials over finite fields. Math. Comput. 66(219), 1195–1212 (1997)

Publisher’s note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.