AIMS Mathematics, 9(7): 17590–17605.
DOI:10.3934/math.2024855
Received: 30 January 2024
Revised: 21 March 2024
Accepted: 25 March 2024
Published: 22 May 2024

https://www.aimspress.com/journal/Math

Research article

Construction of a cryptographic function based on Bose-type Sidon sets

Julian Osorio*, **Carlos Trujillo and Diego Ruiz**

Department of Mathematics, Universidad del Cauca, Cauca, Colombia

* **Correspondence:** Email: rosorio@unicauca.edu.co.

Abstract: Sidon sets have several applications in mathematics and in real-world problems, including the generation of secret keys in cryptography, error-correcting codes, and the physical problem of compression of signals in telecommunications. In particular, in cryptography, the design of cryptographic functions with optimal properties like nonlinearity and differential uniformity plays a fundamental role in the development of secure cryptographic systems. Based on the construction of Bose-type Sidon sets, in this paper we present the construction of a new cryptographic function with good properties of nonlinearity and differential uniformity.

Keywords: cryptography; linearity; differential uniformity; Sidon sets; APN functions
Mathematics Subject Classification: Primary: 43A46, 11T71; Secondary: 12E20

1. Introduction

The security of the block cipher in symmetric cryptography, is based, in some cases, on vectorial Boolean functions $\mathbb{F}_2^n \to \mathbb{F}_2^m$ called *substitution boxes* (S-Box), which satisfy the properties of high *nonlinearity* and low *differential uniformity* that make those functions resistant to the linear cryptanalysis and differential cryptanalysis introduced by Mitsuru Matsui in [1], and Eli Biham and Adi Shamir in [2], respectively. The main ideas in those cryptanalyses are (i) to approximate the vectorial Boolean function by using affine functions, and (ii) to analyze how the differences in the input can affect the resulting difference in the output. Functions with high nonlinearity and low differential uniformity are highly resistant to the two cryptanalysis methods mentioned above. The notion of nonlinearity and differential uniformity can be generalized to algebraic structures other than $\mathbb{F}_2^n$, which allow us to talk about the nonlinearity and differential uniformity of functions between any two finite Abelian groups.

The designing and construction of cryptographic functions resistant to attacks is a complex task, and often based on algebraic methods, random generation, and heuristic designs [3–6]. Each of these methods has advantages and disadvantages over most of the desirable properties of a cryptographic function; for instance, with algebraic constructions, we analyze what properties the functions satisfy,

but with heuristic designs, we obtain functions with several properties from their construction [7]. However, if we consider an application from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, then there are 2^{m2^n} functions; that is, there exist many even in a few variables, which implies a hard problem in a computational search. The abundance of vectorial Boolean functions suggests to us that it is usually impossible to solve the problem of the construction of "good" cryptographic functions using only computational searching, and so it is necessary to introduce more effective methods to design new and better vectorial Boolean functions that can be efficiently implemented in electronic devices [3].

Functions between two Abelian finite groups A and B with the same cardinality and the smallest possible nonlinearity are called *perfect nonlinear (PN) functions*. These functions are related to Sidon sets (a subset of an additive group with the property that all sums of two elements in this set are different), since a function is APN if and only if its associated graph is a Sidon set in the product group $A \times B$. This is one of the reasons we focus on an algebraic construction to introduce new cryptographic functions that arise from the construction of a finite Sidon set due to Bose [8]. The main contribution of this paper is the construction of a new set of functions with good linear and differential properties based on the construction of Sidon sets. This set of functions is 2-to-1, that is, functions in which each output value has zero or two possible preimages [9]. We know that 2-to-1 functions play an important role in cryptography because they can be used to create reversible functions that are not 1-to-1, which can make it harder for attackers to break encryption schemes or find collisions in hash functions [10, 11]. Moreover, they are often used in the construction of APN functions, bent functions, and binary linear codes [12–14].

The remainder of this paper is as follows: Section 2 introduces definitions related to differential uniformity and nonlinearity in Abelian groups. Section 3 presents the construction of our function and some of its properties, including differential uniformity and symmetry. We then illustrate its linearity, and list the number of functions that exist for each $n \in \mathbb{N}$ based on our construction. Finally, Section 4 presents some conclusions and future research directions.

2. Perfect nonlinear functions and nonlinearity

The resistance of functions to cryptanalysis is characterized by two quantities: (i) *nonlinearity*, which measures the resistance of a function to linear cryptanalysis, and (ii) *differential uniformity*, which measures the resistance of a function to differential cryptanalysis. So, we want to construct cryptographic functions with optimal nonlinearity and differential uniformity properties, concepts introduced in this section.

Let A and B denote two non-empty Abelian groups.

Definition 2.1. *Let $f : A \to B$ be a function and let $a \in A$. The derivative of f in a is the function*

$$\begin{aligned} D_a f : A &\to B \\ x &\mapsto f(x+a) - f(x). \end{aligned}$$

A differential of f with input difference a and output difference b is given by

$$f(x+a) - f(x) = b. \tag{2.1}$$

The number of solutions to (2.1) is denoted by $\delta(a, b)$, that is

$$\delta(a,b) = |\{x \in A : \ f(x+a) - f(x) = b\}|.$$

Now, if Δ_f denotes the positive integer

$$\Delta_f = \max_{\substack{a\in A\setminus\{0\}\\ b\in B}} \delta(a,b),$$

then f is said to be *differentially* Δ_f-*uniform*. Note that $\Delta_f \geq |A|/|B|$. In particular, if $\Delta_f = |A|/|B|$, then f is called a *perfect nonlinear* (PN) function [15]. Note also that if $|A| = |B|$, then $\Delta_f = 1$, which implies that (2.1) has one solution. We know that PN functions do not exist in fields of characteristic 2, since if x satisfies $f(x + a) - f(x) = b$, then so does $x + a$. This is the reason for introducing the following definition:

Definition 2.2. *A function f is an almost perfect nonlinear (APN) function if $\Delta_f = 2|A|/|B|$.*

In particular, note that if $|A| = |B|$, then $\Delta_f = 2$, that is, (2.1) has at most two solutions [15].

If we consider a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ of n variables, then the nonlinearity $\mathcal{NL}(f)$ of f is the minimum *Hamming Distance** between f and all affine functions $\varphi_a(x) = a \cdot x + c$, with $a \in \mathbb{F}_2^n$ and $c \in \mathbb{F}_2$. That is

$$\mathcal{NL}(f) = \min_{a\in\mathbb{F}_2^n} d(f, \varphi_a).$$

However, an equivalent concept to nonlinearity that uses a special case of the discrete Fourier transform called the Walsh transform (or Walsh–Hadamard transform) is a useful tool when we want to study the nonlinearity of a function.

Now, consider $A = \mathbb{Z}_q$ and $B = \mathbb{Z}_r$ for the q and r integers. Let $\omega_q \in \mathbb{C}$ and $\omega_r \in \mathbb{C}$ denote the $q-$th and $r-$th roots of unity in $\mathbb{C}$. The expression $x \mapsto \omega_q^{ax}$ defines a character in $\mathbb{Z}_q$ for all $a \in \mathbb{Z}_q$. Similarly, the set of characters in $\mathbb{Z}_r$ for all $b \in \mathbb{Z}_r$ is defined by $y \mapsto \omega_r^{by}$ [15].

Definition 2.3. *The Walsh–Hadamard transform of $f : \mathbb{Z}_q \to \mathbb{Z}_r$ at $a \in \mathbb{Z}_q$ and $b \in \mathbb{Z}_r$ is defined as*

$$\hat{f}(a,b) = \sum_{x\in A} \omega_r^{bf(x)} \overline{\omega}_q^{ax},$$

where $\overline{\omega}_q$ is the complex conjugate of ω_q.

For the different possible parameter values (a, b), this formula compares every constant multiple of f against every linear function ax; the greatest value is indicative of the closeness of f to such a linear function, so the Walsh–Hadamard transform helps us measure the nonlinearity of a function f according to the following definition:

Definition 2.4. *The linearity of a function $f : \mathbb{Z}_q \to \mathbb{Z}_r$ is defined by*

$$\mathcal{L}(f) = \max_{\substack{0\leq a<q\\ 0<b<r}} |\hat{f}(a,b)|.$$

From [16], we know that if $f : \mathbb{Z}_q \to \mathbb{Z}_r$, then $\sqrt{q} \leq \mathcal{L}(f) \leq q$. Functions that reach the lower bound have optimal linearity and are called *bent functions*.

Definition 2.5. *Let $f : \mathbb{Z}_q \to \mathbb{Z}_r$. We define the nonlinearity of f by*

$$\mathcal{NL}(f) = \frac{|\mathbb{Z}_q| - \mathcal{L}(f)}{|\mathbb{Z}_r|} = \frac{q - \mathcal{L}(f)}{r}.$$

*The Hamming Distance between f and g is $d(f,g) = |\{x \in \mathbb{F}_2^n;\ f(x) \neq g(x)\}|$.

Note that nonlinearity actually measures the distance between f and all linear affine functions. Furthermore, also that $\mathcal{NL}(f) = 0$ if and only if f is an affine linear function. It is clear that a bijection and its inverse have the same nonlinearity [16].

Finally, from [17], we know that a function $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$, with $n \geq 2m$ and n even, is perfect nonlinear if and only if it is bent.

3. The construction

In this section, we present the construction of our function, which is based on the construction of Sidon sets due to Bose [8].

Let G denote an additive group. A set $A \subseteq G$ is a *Sidon set* in G if, for all $a, b, c, d \in A$, we have

$$a + b = c + d \;\Rightarrow\; \{a, b\} = \{c, d\}.$$

That is, A is a Sidon set if all the sums of two elements of A are different. Since $a+b = c+d$ if and only if $a - c = d - b$, Sidon sets can also be defined as those with the property that all nonzero differences of pairs of elements are distinct. In particular, the construction of Sidon sets due to Bose is as follows [8].

Theorem 3.1. *Let $q = p^n$ with p a prime number and $n \in \mathbb{N}$. Let $(\mathbb{F}_q, +, \cdot)$ be the finite field with q elements, and $\mathbb{F}_{q^2}$ be an algebraic extension of degree two over $\mathbb{F}_q$. If θ is a primitive element of $\mathbb{F}_{q^2}$, then*

$$\mathcal{B}_q(\theta) = \log_\theta(\theta + \mathbb{F}_q) := \{\log_\theta(\theta + a) : a \in \mathbb{F}_q\} \tag{3.1}$$

is a Sidon set in $\mathbb{Z}_{q^2-1}$ with q elements.

From [18], we know that the set $\theta + \mathbb{F}_q$ is a Sidon set with q elements in the multiplicative group $\mathbb{F}_{q^2}^*$. Furthermore, we know that isomorphisms preserve the Sidon property, so using the discrete logarithm in base θ, we verify that set the $\mathcal{B}_q(\theta)$ is a Sidon set with q elements in the group $\mathbb{Z}_{q^2-1}$, which illustrates a proof of Theorem 3.1.

Example 3.1. *Let $q = 2^4$. If we take the primitive element θ over $\mathbb{F}_2$ such that $\theta^8 + \theta^4 + \theta^3 + \theta^2 + 1 = 0$, then we can construct the Sidon set in $\mathbb{Z}_{255}$ given by*

$$\mathcal{B}_{2^4}(\theta) = \{1, 3, 16, 25, 41, 48, 62, 90, 145, 146, 157, 165, 217, 223, 227, 253\}.$$

According to the work in [18], we know that $\mathcal{B}_q(\theta)$ satisfies the following properties, where $[1, q]$ denotes the set of integers $\{1, \ldots, q\}$.

Proposition 3.1. *If $\mathcal{B}_q(\theta)$ is the set in (3.1), then*

B1) If $b \in \mathcal{B}_q(\theta)$, then $b \not\equiv 0 \bmod (q + 1)$.

B2) If $a, b \in \mathcal{B}_q(\theta)$ and $a \neq b$, then $a \not\equiv b \bmod (q + 1)$.

B3) $\mathcal{B}_q(\theta) \bmod (q + 1) := \{a \bmod (q + 1) : a \in \mathcal{B}_q(\theta)\} = [1, q]$.

Proof. We verify property B2) by contradiction. Suppose $a \equiv b \bmod (q + 1)$, that is, there exists $n \in \mathbb{Z}$ such that $a - b = n(q + 1)$. Note that θ^{q+1} generates $\mathbb{F}_q^*$, so $\theta^{a-b} = \theta^{n(q+1)} \in \mathbb{F}_q^*$. Now, let $a, b \in \mathcal{B}_q(\theta)$, there exist $k_1, k_2 \in \mathbb{F}_q$ with $k_1 \neq k_2$, such that $a = \log_\theta(\theta + k_1)$ and $b = \log_\theta(\theta + k_2)$, implying

that $\theta^a = \theta + k_1$ and $\theta^b = \theta + k_2$. Thus, $\theta^{a-b} = (\theta + k_1)/(\theta + k_2)$. Since $\theta^{a-b} \in \mathbb{F}_q^*$, there exists $c \in \mathbb{F}_q^*$ such that $(\theta + k_1)/(\theta + k_2) = c$. So, $(1 - c)\theta = ck_2 - k_1$. Because $c \neq 1$, then $\theta = (ck_2 - k_1)(1 - c)^{-1} \in \mathbb{F}_q^*$, which is a contradiction. □

Proposition 3.1 means that for each $x \in [1, q]$, we can find a unique $b \in \mathcal{B}_q(\theta)$ such that $b \bmod (q + 1) = x$, i.e., there exists a bijective relationship between the sets $[1, q]$ and $\mathcal{B}_q(\theta) \bmod (q+1)$.

The authors in [19, 20] describe the following relationship between Sidon sets and APN functions: A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is APN if and only if the set $\mathcal{G}_F = \{(x, F(x)) : x \in \mathbb{F}_2^n\}$ is a Sidon set in the group $(\mathbb{F}_2^n \times \mathbb{F}_2^n, +)$. It is common to refer to $\mathcal{G}_F$ as the graph of F. This relationship gives us an idea of how to construct cryptographic functions from known constructions of Sidon sets on finite Abelian groups, that is, we take Sidon sets in one dimension and try to put them in two dimensions via some transformation that preserves the Sidon property; in particular, we use the isomorphism guaranteed by the Chinese remainder theorem to put the set $\mathcal{B}_q(\theta)$ in two dimensions.

Note that if $q = 2^n$, then we have that $\gcd(q + 1, q - 1) = 1$, and so by the Chinese remainder theorem, we have that $\mathbb{Z}_{q^2-1}$ is isomorphic to $\mathbb{Z}_{q+1} \times \mathbb{Z}_{q-1}$. So if $\mathcal{B}_q(\theta)$ is a Sidon set given by (3.1), then each element $b \in \mathcal{B}_q(\theta)$ can be represented as an ordered pair in $\mathbb{Z}_{q+1} \times \mathbb{Z}_{q-1}$ as follows:

$$(b \bmod (q + 1), b \bmod (q - 1)). \tag{3.2}$$

According to Proposition 3.1, B3), note that if we run b in $\mathcal{B}_q(\theta)$, then the set of first coordinates of pair (3.2) coincides with the set $[1, q]$; it allows us to define a set of functions with a common domain $[1, q]$, which, when endowed with the sum modulo q, can be identified with $\mathbb{Z}_q$, that is $([1, q], +_{\bmod q}) \equiv \mathbb{Z}_q$. The co-domain of this set of functions is obtained by reducing the set $\mathcal{B}_q(\theta)$ modulo $q - 1$, as indicated by the second coordinate of the pair (3.2). This set of functions is our main contribution to this work, and they have, in particular, properties of symmetry, good differential uniformity, and good nonlinearity. Moreover, since Proposition 3.1 is valid for all q, we observe that if $q = p^n$ with $p > 2$, then the construction of these functions is still valid and their properties are preserved, except for good nonlinearity.

Definition 3.1. *Let $\mathcal{B}_q(\theta)$ be a Sidon set defined by (3.1). Identify the set $[1, q]$ with the group $\mathbb{Z}_q$ and consider $\mathcal{B}_q(\theta) \bmod (q - 1) \subseteq \mathbb{Z}_{q-1}$. Define the function $f_q : \mathbb{Z}_q \to \mathbb{Z}_{q-1}$ as*

$$f_q(x) = b \bmod (q - 1), \tag{3.3}$$

for $b \in \mathcal{B}_q(\theta)$ such that $b \bmod (q + 1) = x$.

We denote the range of f_q as the sequence $R(f_q) = [f_q(x)]$. The function f_q can be constructed based on the following procedure, where step 2 is valid because of Proposition 3.1, B2).

Step 1. Take $x \in \mathbb{Z}_q$.

Step 2. Find the unique $b \in \mathcal{B}_q(\theta)$ such that $b \equiv x \bmod (q + 1)$.

Step 3. Take $f_q(x) = b \bmod (q - 1)$.

Note that b depends on x, so we can denote b as b_x. In this way, the diagram in Figure 1 illustrates the procedure described above.

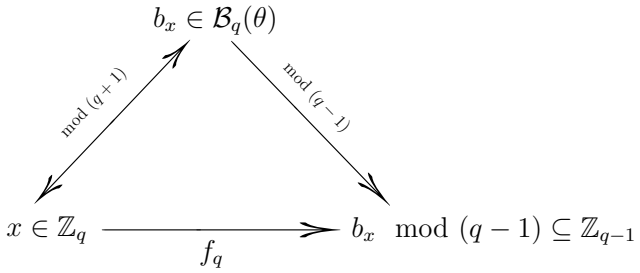


Figure 1. Diagram for function $f_q : \mathbb{Z}_q \to \mathbb{Z}_{q-1}$.

Example 3.2. *Let*

$$\mathcal{B}_{2^4}(\theta) = \{1, 3, 16, 25, 41, 48, 62, 90, 145, 146, 157, 165, 217, 223, 227, 253\}$$

be the Sidon set in Example 3.1. We construct the function $f_{16} : \mathbb{Z}_{16} \to \mathbb{Z}_{15}$ *as follows:*

- *If* $x = 1$, *then* $b = 1 \in \mathcal{B}_{2^4}(\theta)$ *satisfies* $1 \bmod 17 = 1$, *which implies that* $f_{16}(1) = 1 \bmod 15 = 1$.
- *If* $x = 2$, *then* $b = 223 \in \mathcal{B}_{2^4}(\theta)$ *is the unique element that satisfies* $223 \bmod 17 = 2$, *which implies that* $f_{16}(2) = 223 \bmod 15 = 13$.
- *If* $x = 3$, *then* $b = 3 \in \mathcal{B}_{2^4}(\theta)$ *satisfies* $3 \bmod 17 = 3$, *and so* $f_{16}(3) = 3 \bmod 15 = 3$.
- *If* $x = 4$, *then* $b = 157 \in \mathcal{B}_{2^4}(\theta)$ *is the unique element that satisfies* $157 \bmod 17 = 4$, *which implies that* $f_{16}(4) = 157 \bmod 15 = 7$.
- *We repeat the above procedure for the other elements of* $\mathbb{Z}_{16}$.

Figure 2 illustrates the function $f_{16} : \mathbb{Z}_{16} \to \mathbb{Z}_{15}$ *with a range given by*

$$R(f_{16}) = [1, 13, 3, 7, 0, 2, 11, 10, 10, 11, 2, 0, 7, 3, 13, 1].$$

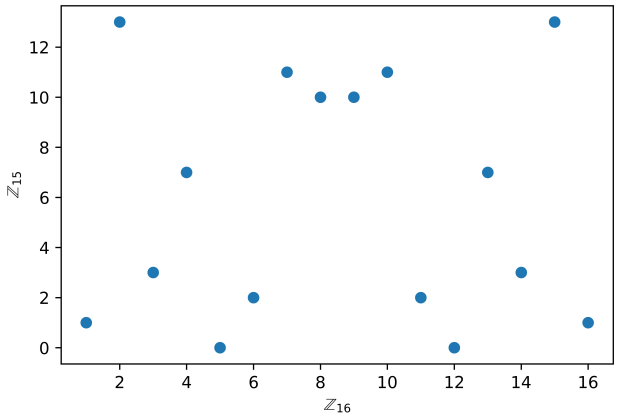


Figure 2. Function f_{16} associated with the Sidon set $\mathcal{B}_{2^4}(\theta)$.

Note that we take $0 := 16$ in $\mathbb{Z}_{16}$, so Figure 2 shows a clear symmetry in the range of the function f_{16}. In general, we have the following result:

Theorem 3.2. *If $f_q : \mathbb{Z}_q \to \mathbb{Z}_{q-1}$ is the function defined in (3.3), then for all $x \in \mathbb{Z}_q$ we have*

i) $f_q(x) = f_q(q + 1 - x)$.

ii) $f_q((q + 1)/2 + x) = f_q((q + 1)/2 - x)$ *for $p > 2$ (i.e., f_q is symmetric with respect to $x = (q + 1)/2$).*

Proof. i) Let $x, q + 1 - x \in [1, q]$. Assume that

$$f_q(x) = r \equiv b_1 \bmod (q - 1),$$
$$f_q(1 - x) = s \equiv b_2 \bmod (q - 1),$$

with $b_1, b_2 \in \mathcal{B}_q(\theta)$. According to the definition of f_q, we know that

$$b_1 \equiv x \bmod (q + 1),$$
$$b_2 \equiv q + 1 - x \bmod (q + 1).$$

Consider the following two cases:

Case 1. If $b_1 = b_2$, then $q + 1 - x \equiv x \bmod (q + 1)$. Since $1 \leq x, q + 1 - x \leq q < q + 1$ we have that $q + 1 - x = x$, or $x = (q + 1)/2$ (only for q odd), which implies $f_q(x) = f_q(q + 1 - x)$, that is, $r = s$.

Case 2. If $b_1 \neq b_2$, then there are $k_1, k_2 \in \mathbb{F}_q$ with $k_1 \neq k_2$ such that

$$b_1 = \log_\theta(\theta + k_1),$$
$$b_2 = \log_\theta(\theta + k_2),$$

that is

$$b_1 - b_2 = \log_\theta(\theta + k_1) - \log_\theta(\theta + k_2) = \log_\theta\left(\frac{\theta + k_1}{\theta + k_2}\right).$$

Let $\gamma := \theta^{b_1 - b_2} = \frac{\theta + k_1}{\theta + k_2}$. Note that $\gamma \neq 1$, since otherwise $k_1 = k_2$. Moreover, $\gamma \notin \mathbb{F}_q^*$ because θ is a primitive element over $\mathbb{F}_q$ of degree two, so $\gamma \in \mathbb{F}_{q^2}^* \setminus \mathbb{F}_q^*$. Because $\mathbb{F}_q^*$ and $\left\langle \theta^{q-1} \right\rangle$ (the group generated by θ^{q-1}) are two subgroups of $\mathbb{F}_{q^2}^*$ that only intersect at 1 if q is even or ± 1 if q is odd, and because $\gamma \notin \mathbb{F}_q^*$, we have that $\gamma \in \left\langle \theta^{q-1} \right\rangle$. Therefore, there exists $t \in \mathbb{Z}$ such that $\gamma = \theta^{t(q-1)}$, from which $\theta^{b_1 - b_2} = \theta^{t(q-1)}$. Since $b_1 - b_2 \equiv r - s \bmod (q - 1)$, then $b_1 - b_2 = n(q - 1) + (r - s)$ for some $n \in \mathbb{Z}$, implying that

$$\theta^{n(q-1)+(r-s)} = \theta^{t(q-1)},$$

from which $n(q-1)+(r-s) \equiv t(q-1) \bmod (q^2-1)$, that is, $(r-s) \equiv 0 \bmod (q-1)$. Because $0 \leq r, s < q-1$ we have that $r = s$.
ii) Is similar to the proof of i). □

Now, we know in $\mathbb{Z}_q$ that $-x = q - x$, so in $\mathbb{Z}_{q+1}$ and for $b_1, b_2 \in \mathcal{B}_q(\theta)$, we have

$$b_1 \bmod (q + 1) + b_2 \bmod (q + 1) = x + 1 + q - x = 0$$

in $\mathbb{Z}_{q+1}$. That is, $b_1 + b_2 \equiv 0 \bmod (q+1)$ and $b_1 - b_2 \equiv 0 \bmod (q-1)$. The following corollary formalizes this property, in which the system of congruences is a particular case of the multivariable Chinese Remainder theorem.

Corollary 3.1. *For a given $x \in \mathcal{B}_q(\theta)$, there exist a $y \in \mathcal{B}_q(\theta)$ not necessarily different from x such that*

$$\begin{cases} x + y & \equiv & 0 \bmod (q+1) \\ x - y & \equiv & 0 \bmod (q-1). \end{cases}$$

Example 3.3. *Let*

$$\mathcal{B}_{2^4}(\theta) = \{1, 3, 16, 25, 41, 48, 62, 90, 145, 146, 157, 165, 217, 223, 227, 253\}$$

be the Sidon set in Example 3.1. Table 1 illustrates Corollary 3.1.

Table 1. Illustration of Corollary 3.1.

$x + y \equiv 0 \bmod 17$	$x - y \equiv 0 \bmod 15$
16 + 1	16 − 1
48 + 3	48 − 3
145 + 25	145 − 25
146 + 41	146 − 41
227 + 62	227 − 62
165 + 90	165 − 90
217 + 157	217 − 157
253 + 223	253 − 223

Note that Theorem 3.2 establishes that $f_q(x)$ is symmetric and consequently a 2-to-1 function according to the next definition [9].

Definition 3.2. *Let A and B be two finite sets, and let f be a mapping from A to B. Function f is called a 2-to-1 mapping if one of the following two cases holds:*

i) $|A|$ is even, and for any $b \in B$, it has either 2 or 0 preimages of f.

ii) $|A|$ is odd, and for all but one $b \in B$, it has either 2 or 0 preimages of f, and the exception element has exactly one preimage.

From Theorem 3.2, i), note that the conditions of Definition 3.2 are satisfied, and from Theorem 3.2, ii), the exception element is $2^{-1} \bmod q = \frac{q+1}{2}$. It implies the next corollary.

Corollary 3.2. *For all prime numbers p and all $n \in \mathbb{N}$, the function f_q is 2-to-1.*

One important property in cryptographic applications is low differentiability, since functions with low differential uniformity are resistant to differential attacks [2]. Fortunately, the function f_q has this property, as we demonstrate in the following theorem.

Theorem 3.3. *For all prime numbers p and all $n \in \mathbb{N}$, the function f_q is differentially 2-uniform.*

Proof. Let $a \in \mathbb{Z}_q \setminus \{0\}$ and $b \in \mathbb{Z}_{q-1}$. Consider the equation

$$f_q(x + a) - f_q(x) = b. \tag{3.4}$$

From the definition of f_q we know that there exist $b_1, b_2 \in \mathcal{B}_q(\theta)$ such that

$$b_1 \bmod (q+1) = x + a,$$
$$b_2 \bmod (q+1) = x,$$

which implies that $b_1 + b_2 \equiv 2x + a \bmod (q+1)$, and so there exists $m \in \mathbb{N}$ such that

$$b_1 + b_2 = (q+1)m + 2x + a. \tag{3.5}$$

Note also from the definition of f_q that

$$f_q(x+a) = b_1 \bmod (q-1),$$
$$f_q(x) = b_2 \bmod (q-1),$$

so (3.4) is equivalent to $b_1 - b_2 \equiv b \bmod (q-1)$, that is, there exists $n \in \mathbb{N}$ such that

$$b_1 - b_2 = (q-1)n + b, \tag{3.6}$$

and thus, from (3.5) and (3.6), we have

$$2x = (q-1)n - (q+1)m + 2b_2 + b - a.$$

That is

$$2x \equiv -2m + 2b_2 + b - a \bmod (q-1). \tag{3.7}$$

So far, we have proved that (3.4) is equivalent to (3.7). Next, to show that (3.4) has at most 2 solutions, we consider the following cases for q:

1) If $q = 2^n$, then $\gcd(2, q-1) = 1$, and so (3.7) has one solution.

2) If $q = p^n$ and $p \neq 2$, then $\gcd(2, q-1) = 2$, but note that $2|(-2m+2b_2+b-a)$ if and only if $2|(b-a)$. So it is sufficient to find $b \in \mathbb{Z}_{q-1}$ and $a \in \mathbb{Z}_q \setminus \{0\}$ such that $b - a$ is an even number to guarantee that (3.7) has exactly two solutions.

□

3.1. Enumeration of the functions f_q

Note that the function f_q depends on the Sidon set $\mathcal{B}_q(\theta)$ given in (3.1); thus, if we want to count the functions f_q we must first count the sets $\mathcal{B}_q(\theta)$. Note also that for a fixed $q = p^n$, the construction of the Sidon set $\mathcal{B}_q(\theta)$ depends on a primitive element $\theta \in \mathbb{F}^*_{q^2}$, so we can wonder about the behavior of these sets when we vary the primitive element within the field. We have the following:

Theorem 3.4. *If α and θ are conjugates, then $\mathcal{B}_q(\theta) = \mathcal{B}_q(\alpha)$.*

Proof. If α and θ are conjugates, then $\alpha = \theta^{p^i}$ for some $i \in \{1, \ldots, 2n-1\}$. Let $\log_\alpha(\alpha + a) \in \mathcal{B}_q(\alpha)$. Since α^{q+1} generates $\mathbb{F}^*_{p^n}$ there exists $m \in \mathbb{Z}$ such that $a = \alpha^{m(q+1)} = \theta^{m(q+1)p^i}$, thus

$$\log_\alpha(\alpha + a) = \log_{\theta^{p^i}}(\theta^{p^i} + \theta^{m(q+1)p^i})$$

$$= \log_{\theta^{p^i}}(\theta + \theta^{m(q+1)})^{p^i}$$
$$= p^i \cdot \log_{\theta^{p^i}}(\theta + \theta^{m(q+1)}). \tag{3.8}$$

Note that θ^{q+1} also generates $\mathbb{F}_{p^n}^*$, so $b := \theta^{m(q+1)} \in \mathbb{F}_{p^n}^*$. If we apply the base interchange formula on the right side of (3.8), then

$$\begin{aligned} p^i \cdot \log_{\theta^{p^i}}(\theta + \theta^{m(q+1)}) &= p^i \cdot \log_{\theta^{p^i}} \theta \cdot \log_\theta(\theta + b) \\ &= p^i (p^i)^{-1} \cdot \log_\theta(\theta + b) \\ &= \log_\theta(\theta + b). \end{aligned}$$

Therefore, $\log_\alpha(\alpha + a) \in \mathcal{B}_q(\theta)$, which implies that $\mathcal{B}_q(\alpha) \subseteq \mathcal{B}_q(\theta)$. Now, because $|\mathcal{B}_q(\alpha)| = |\mathcal{B}_q(\theta)|$, we have that $\mathcal{B}_q(\alpha) = \mathcal{B}_q(\theta)$. □

Computational calculations indicate that the reciprocal of Theorem 3.4 is valid, but its proof is strongly related to the theory of multipliers on relative difference sets, of which we do not know the solution. So we conjecture the following:

Conjecture 3.1. *If $\mathcal{B}_q(\theta) = \mathcal{B}_q(\alpha)$, then α and θ are conjugates.*

Theorem 3.4 helps us to establish an upper bound for the number of different Bose-type Sidon sets that exist for each $p \geq 2$ and $n \geq 1$, and since the construction of our set of functions depends on these sets, it will also help us to establish an upper bound for the number of different functions f_q that exist.

Theorem 3.5. *Let $q = p^n$. For each $p \geq 2$ and each $n \in \mathbb{N}$, there exist at most $\varphi(q^2 - 1)/2n$ different Sidon sets $\mathcal{B}_q(\theta)$.*

Proof. Note that, if θ is a primitive element of $\mathbb{F}_{q^2}$ over $\mathbb{F}_p$, then its $2n$ conjugates $\theta, \theta^p, \ldots, \theta^{p^{2n-1}}$ are also primitives, so from Theorem 3.4, it generates the same Sidon set $\mathcal{B}_q(\theta)$. Furthermore, because there are $\varphi(q^2 - 1)$ primitive elements in $\mathbb{F}_{q^2}$ (φ is Euler's phi function), we have that actually there exist $\varphi(q^2 - 1)/2n$ different primitive elements that are not conjugated to each other, thus these primitive elements generate at most $\varphi(q^2 - 1)/2n$ different Sidon sets $\mathcal{B}_q(\theta)$. □

Note that if Conjecture 3.1 is true, then we obtain the equality in Theorem 3.5 since the $\varphi(q^2 - 1)/2n$ different primitive elements not conjugate with each other would generate exactly $\varphi(q^2 - 1)/2n$ sets $\mathcal{B}_q(\theta)$.

Lemma 3.1. *Let $p > 2$ and θ be a primitive element of $\mathbb{F}_{p^2}$. If $c = \frac{p^2-1}{2} + p$, then $\theta^c = \theta + b$ for some $b \in \mathbb{F}_p \setminus \{0\}$.*

Proof. Note that $\gcd(c, p^2 - 1) = 1$, so θ^c is another primitive element of $\mathbb{F}_{p^2}$, implying that $\theta^c = a\theta + b$ for some $a, b \in \mathbb{F}_p \setminus \{0\}$. Note also that $\theta^c = -\theta^p$, from which $\theta^p = -a\theta - b$, and so $\theta^p + \theta = (1 - a)\theta - b$. Because $\theta^p + \theta \in \mathbb{F}_p$, we have $a = 1$. □

Theorem 3.6. *Let $p > 2$ and $t \leq \varphi(p^2 - 1)/2$. Let $\mathcal{A} = \{\mathcal{B}_p(\theta_i) : i = 1, \ldots, t\}$ be the collection of the t different Bose-type Sidon sets. For each $\mathcal{B}_p(\theta_i) \in \mathcal{A}$ there exist $\mathcal{B}_p(\theta_j) \in \mathcal{A}$, with $i \neq j$ such that*

$$\mathcal{B}_p(\theta_i) \bmod (p - 1) = \mathcal{B}_p(\theta_j) \bmod (p - 1).$$

Proof. Let θ^i be a primitive element such that $\mathcal{B}_p(\theta^i) \in \mathcal{A}$ and $c = \frac{p^2-1}{2} + p$. Take $j = ic$ and note that $\mathcal{B}_p(\theta^j) \in \mathcal{A}$ because θ^j is also a primitive element; moreover, $\mathcal{B}_p(\theta^j) \neq \mathcal{B}_p(\theta^i)$ since otherwise θ^j and θ^i would be conjugates, which is not possible. Now, from Lemma 3.1, we have that

$$\theta^j = (\theta^i)^c = \theta^i + b \tag{3.9}$$

for some $b \in \mathbb{F}_p \setminus \{0\}$. Now, if $\log_{\theta^j}(\theta^j + k_0) \in \mathcal{B}_p(\theta^j)$ for some $k_0 \in \mathbb{F}_p$, then from (3.9) we have that

$$\begin{aligned}\log_{\theta^j}(\theta^j + k_0) &= \log_{\theta^j}(\theta^i + b + k_0)\\ &= \log_{\theta^j}(\theta^i + k_1)\end{aligned}$$

for $k_1 \in \mathbb{F}_p$. If we apply the base interchange formula, then

$$\begin{aligned}\log_{\theta^j}(\theta^j + k_0) &= \log_{\theta^j}\theta^i \cdot \log_{\theta^i}(\theta^i + k_1)\\ &= j^{-1}i \cdot \log_{\theta^i}(\theta^i + k_1)\\ &= c^{-1} \cdot \log_{\theta^i}(\theta^i + k_1),\end{aligned}$$

so

$$c\log_{\theta^j}(\theta^j + k_0) = \log_{\theta^i}(\theta^i + k_1),$$

that is

$$c\log_{\theta^j}(\theta^j + k_0) \in \mathcal{B}_p(\theta^i).$$

This implies that $c\mathcal{B}_p(\theta^j) \subseteq \mathcal{B}_p(\theta^i)$, and because $|c\mathcal{B}_p(\theta^j)| = |\mathcal{B}_p(\theta^i)|$, we have proof that $c\mathcal{B}_p(\theta^j) = \mathcal{B}_p(\theta^i)$, and so $\mathcal{B}_p(\theta^j) \bmod (p-1) = \mathcal{B}_p(\theta^i) \bmod (p-1)$. □

Note again that if Conjecture 3.1 is true, then we could guarantee uniqueness in the set $\mathcal{B}_p(\theta^j) \in \mathcal{A}$. The objective of this section was to count the functions f_q, so, in the following theorem, we establish an upper bound for the number of functions for $q = 2^n$ and $q = p$.

Theorem 3.7. *Let $q = p^n$ with $n \in \mathbb{N}$. For $p = 2$, there exist at most $\varphi(q^2-1)/2n$ different functions f_q, and for $p > 2$ and $n = 1$, there exist at most $\varphi(p^2-1)/4$ different functions f_p.*

Proof. If $p = 2$, then by the Chinese remainder theorem we have that $\mathbb{Z}_{q^2-1}$ is isomorphic to $\mathbb{Z}_{q+1} \times \mathbb{Z}_{q-1}$ (denoted by $\mathbb{Z}_{q^2-1} \equiv \mathbb{Z}_{q+1} \times \mathbb{Z}_{q-1}$), and because Sidon's property is preserved under isomorphism [18], from (3.2) we have that

$$\mathcal{B}_q(\theta) \equiv \Big(\mathcal{B}_q(\theta) \bmod (q+1), \mathcal{B}_q(\theta) \bmod (q-1)\Big) = (\mathrm{dom}(f_q), \mathrm{ran}(f_q)),$$

and the result follows from Theorem 3.5.

Now, if $p > 2$ and $n = 1$, then we simply put the set $\mathcal{B}_p(\theta)$ in the group $\mathbb{Z}_{p+1} \times \mathbb{Z}_{p-1}$ as

$$\Big(\mathcal{B}_p(\theta) \bmod (p+1), \mathcal{B}_p(\theta) \bmod (p-1)\Big) = (\mathrm{dom}(f_p), \mathrm{ran}(f_p)),$$

and the result follows from Theorem 3.5 and Theorem 3.6. □

Example 3.4. *Note that if $q = 2^n$, then $gdc(q-1, q+1) = 1$, and $\varphi(q^2-1)/2n = \varphi(q-1)\varphi(q+1)/2n$, which facilitates the counting of the functions f_q. For instance, for $q = 2^4$, there exists $\varphi(15)\varphi(17)/8 = 16$ different functions given by*

[1, 13, 3, 7, 0, 2, 11, 10, 10, 11, 2, 0, 7, 3, 13, 1], [1, 7, 12, 4, 3, 14, 11, 13, 13, 11, 14, 3, 4, 12, 7, 1],
[1, 4, 14, 10, 2, 0, 6, 7, 7, 6, 0, 2, 10, 14, 4, 1], [1, 0, 8, 13, 11, 14, 5, 9, 9, 5, 14, 11, 13, 8, 0, 1],
[1, 2, 9, 4, 6, 3, 12, 8, 8, 12, 3, 6, 4, 9, 2, 1], [1, 7, 2, 4, 8, 9, 6, 13, 13, 6, 9, 8, 4, 2, 7, 1],
[1, 12, 14, 4, 11, 8, 2, 3, 3, 2, 8, 11, 4, 14, 12, 1], [1, 13, 8, 7, 5, 12, 6, 10, 10, 6, 12, 5, 7, 8, 13, 1],
[1, 10, 5, 13, 14, 3, 6, 4, 4, 6, 3, 14, 13, 5, 10, 1], [1, 4, 9, 10, 12, 5, 11, 7, 7, 11, 5, 12, 10, 9, 4, 1],
[1, 5, 3, 13, 6, 9, 0, 14, 14, 0, 9, 6, 13, 3, 5, 1], [1, 14, 0, 10, 6, 12, 9, 2, 2, 9, 12, 6, 10, 0, 14, 1],
[1, 9, 5, 10, 11, 2, 14, 12, 12, 14, 2, 11, 10, 5, 9, 1], [1, 3, 2, 7, 11, 5, 8, 0, 0, 8, 5, 11, 7, 2, 3, 1],
[1, 10, 0, 13, 9, 8, 11, 4, 4, 11, 8, 9, 13, 0, 10, 1], [1, 8, 12, 7, 6, 0, 3, 5, 5, 3, 0, 6, 7, 12, 8, 1].

From [21, Chapter 18], we know that $\limsup \varphi(n)/n = 1$, which means that the order of $\varphi(n)$ is nearly n, that is,

$$\frac{\varphi(q^2 - 1)}{2n} \approx \frac{q^2 - 1}{2n}.$$

So for $p = 2$ and n sufficiently large, we conclude that there exist approximately $2^{2n}/2n$ functions f_q. Moreover, from [21, Theorem 328], we know that the function $\varphi(n)$ satisfies

$$\liminf_{n\to\infty} \frac{\varphi(n)}{\frac{n}{\log\log n}} = e^{-\gamma}, \tag{3.10}$$

where γ is the Euler–Mascheroni constant. So for $q = 2^n$, (3.10) implies that $\varphi(q^2 - 1)/2n$ is bounded below by

$$\frac{2^{2n}}{2ne^{\gamma}\log\log 2^{2n}},$$

this expression is equivalent to

$$\frac{2^{2n}}{(2e^{\gamma} + \varepsilon_n)n\log n}$$

with $\varepsilon_n \to 0$ when $n \to \infty$. Hence, for $q = 2^n$, we have that the number of functions f_q is at least

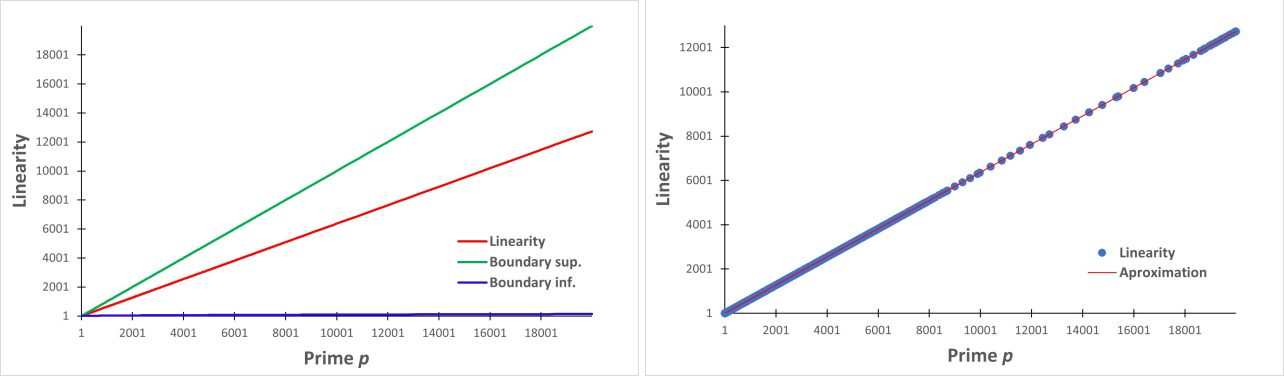
$$\frac{2^{2n}}{(2e^{\gamma} + \varepsilon_n)n\log n},$$

if n is large enough. For $p > 2$ and $n = 1$, similar formulas can be derived.

3.2. Simulation results

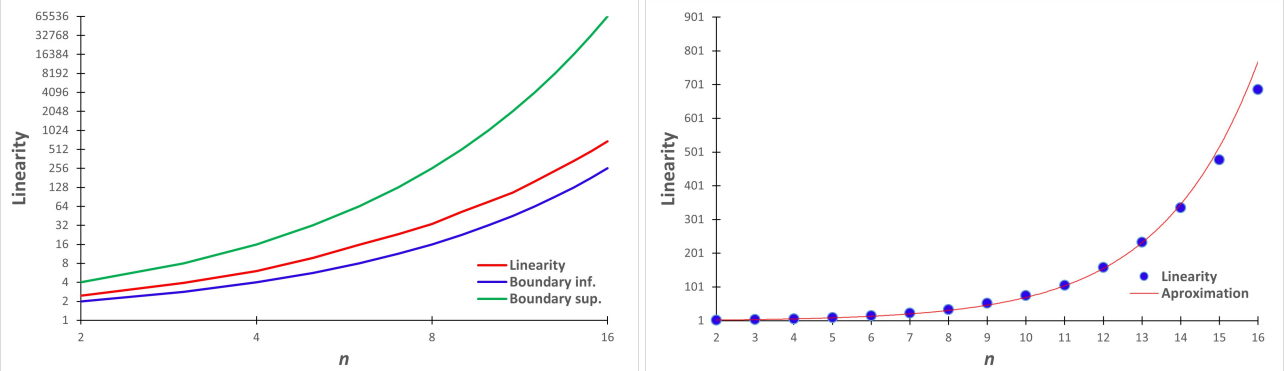
This section illustrates the linearity of f_q. We know for $\alpha \neq 0$ that $|\hat{f}_q(q-\alpha, (q-1)-\beta)| = |\hat{f}_q(\alpha, \beta)|$, which, together with Theorem 3.2, reduces by a factor of approximately 4 the number of points required to calculate the linearity of f_q. With this fact and the fast Fourier transform, we illustrate in Figures 3 and 4 the linearity of f_q for $q = p$ with $2 < p < 20000$ and $q = 2^n$ with $2 \leq n \leq 16$. Figure 3b illustrates that the approximation of linearity has a slope of around 0.64, which leads us to conjecture that the linearity of f_p is bounded below by an affine function that depends on p; unfortunately, this implies that $\mathcal{L}(f_p)$ would be asymptotically closer to the upper bound, that is, f_p is closer to being a linear function.

But when $q = 2^n$, our simulations show a more interesting behavior. For example, for values of $n \in \{4, 5, 6, 7, 8\}$, important in cryptographic applications, the linearity of f_{2^n} is closer to the lower bound, as shown in Figure 4a and Table 2, implying that f_{2^n} has high nonlinearity. Figure 4b illustrates, by means of an exponential regression with a coefficient of determination of $r^2 = 0.998$, that for values of n greater than 16, the behavior of the linearity of f_{2^n} tends to remain.



(a) Linearity vs. boundaries. **(b)** Linearity and approximation.

Figure 3. Behavior of the linearity of f_p for $2 < p < 20000$.



(a) Linearity vs. boundaries. **(b)** Linearity and approximation.

Figure 4. Behavior of the linearity of f_{2^n} for $2 \leq n \leq 16$.

Table 2. Linearity of f_{2^n} and lower and upper bounds of $\mathcal{L}(f_{2^n})$.

n	Lower bound	$\mathcal{L}(f_{2^n})$	Upper bound
4	4	6,00776721665963	16
5	5,65685425	9,76163585008853	32
6	8	15,7984554517002	64
7	11,3137085	23,1605616207365	128
8	16	33,7779991765064	256

Now, when we compare the cases $q = 2^n$ and $q = p$ with $p > 2$, we suspect that the loss of linearity for the second case is due to the fact that there is no an isomorphism between $\mathbb{Z}_{p^2-1}$ and $\mathbb{Z}_{p+1} \times \mathbb{Z}_{p-1}$. Furthermore, note that this behavior still remains when $q = p^n$ with $p > 2$ and $n > 1$.

4. Conclusions

Our contribution in this work is the construction of a new set of functions that are 2-to-1 functions and differentially 2-uniform, which, for the case $q = 2^n$, present an asymptotic behavior close to the trivial lower bound for its linearity, that is, the asymptotic nonlinearity of function f_q is high. The number of functions that exist for each n, with $p = 2$, is of the order $2^{2n}/2n$, and for $n = 1$ and $p > 2$, it is of the order $p^2/4$, so this set of functions grows rapidly as n and p increase, respectively.

Due to the particular way in which we define our function f_q, we cannot establish nontrivial bounds for its linearity, so this problem remains open. For instance, through linear and exponential regression, respectively, we conjecture that, i) for $q = p$, there exist two constants $0.5 < \alpha < 1$ and $0 < \beta < 0.5$ such that $\mathcal{L}(f_p) \geq \alpha p + \beta$, and ii) for $q = 2^n$, there exist two constants $\gamma > 1$ and $0 < \mu < 1$ such that $\mathcal{L}(f_{2^n}) \leq \gamma e^{\mu n}$. Moreover, note that in this work we emphasize the study of two cases; first, when $q = 2^n$ due to the isomorphism between $\mathbb{Z}_{q^2-1}$ and $\mathbb{Z}_{q+1} \times \mathbb{Z}_{q-1}$, and second, when $q = p$; but the case $q = p^n$ with $p > 2$ and $n > 1$ was not studied in detail, so it remains open to study what other properties the function f_{p^n} satisfies for this case. For instance, we conjecture from Theorem 3.7 that the number of functions f_q that exist for $q = p^n$ with $p > 2$ and $n > 1$ is equal to $\varphi(q^2 - 1)/4n$, but for proof of this, it is necessary to generalize Lemma 3.1 and Theorem 3.6 for that case.

Some ciphers, such as SAFER [22], use non-binary transformations with "high nonlinearity" and optimal differential uniformity, known in the literature as exponential Welch Costas (EWC) and logarithmic Welch Costas (LWC) functions [16, 23, 24]. Given that for the case $q = 2^n$, the characteristics of our function are similar to those of these functions, we raised concern about the possibility of using our function in a cipher like SAFER.

Author contributions

Julian Osorio: Writing – original draft, Writing – review & editing, Conceptualization, Formal analysis, Investigation; Carlos Trujillo: Conceptualization, Formal analysis, Investigation; Diego Ruiz: Writing – original draft, Writing – review & editing, Conceptualization, Formal analysis, Investigation. All authors have read and approved the final version of the manuscript for publication.

Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

Authors would like to thank the Universidad del Cauca for funding this paper, and the reviewers for the important feedback, which helped us to improve the quality of this paper. The first author would like to thank MINCIENCIAS (Colombia) for supporting his doctoral studies through "Convocatoria del fondo de ciencia, tecnología e innovación del sistema general de regalías para conformación de una lista de proyectos elegibles para ser viabilizados, priorizados y aprobados por el OCAD en el marco del programa de becas de excelencia doctoral del bicentenario (No. BB 2019 01)."

Conflict of interest

The authors declare no conflict of interest in this paper.

References

1. M. Matsui, A. Yamagishi, A New Method for Known Plaintext Attack of FEAL Cipher, in *Advances in Cryptology — EUROCRYPT' 92* (ed. Rueppel, R.A.), Springer Berlin Heidelberg, Berlin, Heidelberg, 1993, 81–91. https://doi.org/10.1007/3-540-47555-9_7
2. E. Biham, A. Shamir, *Differential Cryptanalysis of DES Variants*, *Differential Cryptanalysis of the Data Encryption Standard*, Springer New York, New York, NY, 1993, 33–77. https://doi.org/10.1007/978-1-4613-9314-6_4
3. L. Budaghyan, *Construction and Analysis of Cryptographic Functions*, Springer Publishing Company, Incorporated, 2015. https://doi.org/10.1007/978-3-319-12991-4
4. Y. Chen, L. Zhang, Z. Gong, W. Cai, Constructing Two Classes of Boolean Functions With Good Cryptographic Properties, *IEEE Access*, **7** (2019), 149657–149665. https://doi.org/10.1109/ACCESS.2019.2947367
5. C. Beierle, G. Leander, New Instances of Quadratic APN Functions, *IEEE T. Inform. Theory*, **68** (2022), 670–678. https://doi.org/10.1109/TIT.2021.3120698
6. L. Mariot, M. Saletta, A. Leporati, L. Manzoni, Heuristic search of (semi-) bent functions based on cellular automata, *Natural Computing*, **21** (2022), 377–391. https://doi.org/10.1007/s11047-022-09885-3
7. J. A. Clark, J. L. Jacob, S. Maitra, P. Stănică, Almost Boolean functions: the design of Boolean functions by spectral inversion, *Computational intelligence*, **20** (2004), 450–462. https://doi.org/10.1111/j.0824-7935.2004.00245.x
8. R. C. Bose, An affine analogue of Singer's theorem, *Journal of the Indian Mathematical Society*, **6** (1942), 1–15.
9. S. Mesnager, L. Qu, On Two-to-One Mappings Over Finite Fields, *IEEE T. Inform. Theory*, **65** (2019), 7884–7895. https://doi.org/10.1109/TIT.2019.2933832
10. N. Alamati, G. Malavolta, A. Rahimi, Candidate Trapdoor Claw-Free Functions from Group Actions with Applications to Quantum Protocols, *Theory of Cryptography* (eds. Kiltz, E., Vaikuntanathan, V.), Springer Nature Switzerland, Cham, 2022, 266–293. https://doi.org/10.1007/978-3-031-22318-1_10
11. T. Morimae, T. Yamakawa, Proofs of Quantumness from Trapdoor Permutations, *arXiv:2208.12390*, 2022. https://doi.org/10.48550/arXiv.2208.12390
12. D. Bartoli, M. Giulietti, M. Timpanella, Two-to-one functions from Galois extensions, *Discrete Appl. Math.*, **309** (2022), 194–201. https://doi.org/10.1016/j.dam.2021.12.008
13. V. Idrisova, On an algorithm generating 2-to-1 APN functions and its applications to "the big APN problem", *Cryptography and Communications*, **11** (2019), 21–39. https://doi.org/10.1007/s12095-018-0310-9

14. S. Mesnager, L. Qian, X. Cao, Further projective binary linear codes derived from two-to-one functions and their duals, *Designs, Codes and Cryptography*, **91** (2023), 719–746. https://doi.org/10.1007/s10623-022-01122-3

15. C. Blondeau, K. Nyberg, Perfect nonlinear functions and cryptography, *Finite Fields and Their Applications*, **32** (2015), 120–147. Special Issue: Second Decade of FFA. https://doi.org/10.1016/j.ffa.2014.10.007

16. K. Drakakis, V. Requena, G. McGuire, On the Nonlinearity of Exponential Welch Costas Functions, *IEEE T. Inform. Theory*, **56** (2010), 1230–1238. https://doi.org/10.1109/TIT.2009.2039164

17. F. Chabaud, S. Vaudenay, Links between differential and linear cryptanalysis, in *Advances in Cryptology — EUROCRYPT'94* (ed. A. De Santis), Springer Berlin Heidelberg, Berlin, Heidelberg, 1995, 356–365. https://doi.org/10.1007/BFb0053450

18. D. Ruiz, C. Trujillo, Y. Caicedo, New Constructions of Sonar Sequences, *International Journal of Basic & Applied Sciences*, **14** (2014), 12–16.

19. C. Carlet, S. Picek, On the exponents of APN power functions and Sidon sets, sum-free sets, and Dickson polynomials, *Adv. Math. Commun.*, **17** (2023), 1507–1525. https://doi.org/10.3934/amc.2021064

20. C. Carlet, S. Mesnager, On those multiplicative subgroups of $\mathbb{F}_{2^n}^*$ which are Sidon sets and/or sum-free sets, *J. Algebr. Comb.*, **55** (2022), 43–59. https://doi.org/10.1007/s10801-020-00988-7

21. G. H. Hardy, E. M. Wright, *An introduction to the theory of numbers*, 5th edition, Oxford university press, 1979.

22. J. L. Massey, Safer K-64: A Byte-Oriented Block-Ciphering Algorithm, in *Fast Software Encryption* (ed. R. Anderson), Springer Berlin Heidelberg, Berlin, Heidelberg, 1994, 1–17. https://doi.org/10.1007/3-540-58108-1_1

23. K. Drakakis, R. Gow and G. McGuire, APN permutations on $\mathbb{Z}_n$ and Costas arrays, *Discrete Appl. Math.*, **157** (2009), 3320–3326. https://doi.org/10.1016/j.dam.2009.06.029

24. R. M. Hakala, An upper bound for the linearity of Exponential Welch Costas functions, *Finite Fields and Their Applications*, **18** (2012), 855–862. https://doi.org/10.1016/j.ffa.2012.05.001

AIMS Press