An extension of the avalanche criterion in the context of c-differentials

Pål Ellingsen[1], Constanza Riera[1], Pantelimon Stănică[2], Anton Tkachenko[1]

[1]*Department of Computer Science, Electrical Engineering and Mathematical Sciences, Western Norway University of Applied Sciences, 5020 Bergen, Norway; {pel, csr, atk}@hvl.no*

[2]*Department of Applied Mathematics, Naval Postgraduate School, Monterey, CA 93943–5216, USA; pstanica@nps.edu*

Keywords: Boolean, p-ary functions, c-differentials, Walsh transform, differential uniformity, perfect and almost perfect c-nonlinearity, Strict Avalanche Criterion.

Abstract: The Strict Avalanche Criterion (SAC) is a property of vectorial Boolean functions that is used in the construction of strong S-boxes. We generalize in this paper the concept of SAC in the realm of finite fields, to address possible c-differential attacks. We define the concepts of c-Strict Avalanche Criterion (c-SAC) and c-Strict Avalanche Criterion of order m (c-SAC(m)), and generalize results of (Li and Cusick, 2005). We also find out, computationally, that the new definition is not equivalent to the existing concepts of c-bent$_1$-ness (Stănică et al., 2020), nor (for $n = m$) PcN-ness (Ellingsen et al., 2020).

1 INTRODUCTION

A Substitution-box (S-Box) is one of the most important elements that are used to provide attack resistance to block encryption algorithms. An S-box performs substitution on its input symbols, and together with permutations, they are typically used to obscure the relationship between the plaintext, the key and the ciphertext of an encryption algorithm. The attack resistance of an S-box depends on many different factors, but one of the more important ones is the ability of the S-box to induce a significant change in the output of the box from a small change in the input. This is called the avalanche effect. In general, if an S-box does not have this avalanche effect, it will result in a lack of randomization in the algorithm that may be used as part of an attack on the algorithm. A primary strategy for attacking cryptographic algorithms with weak randomization properties are the so-called differential attacks (Biham and Shamir, 1991), (Biham and Shamir, 2012). The *Strict Avalanche Criterion* (*SAC*) is a more refined property of S-boxes derived from the general avalanche property. SAC was introduced in (Webster and Tavares, 1985) in the context of S-boxes, described by vectorial Boolean functions, as follows: a vectorial Boolean function satisfies SAC if and only if whenever a single input bit of a coordinate is complemented, each of its output bits changes with probability $1/2$; i.e. given $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ ($\mathbb{F}_2$ is the two-element field and $\mathbb{F}_2^k$ is a vector space of dimension k over $\mathbb{F}_2$), the function $F = (F_1, \ldots, F_m)$ satisfies SAC if and only if the probability $Prob(F_i(\mathbf{x} \oplus \mathbf{e}_i) \oplus F_i(\mathbf{x}) = 1) = \frac{1}{2}$, $\forall i = 1, \ldots, m$, where $\mathbf{e}_i$ is the standard basis vector with 1 in component i and 0 in all other components. In general, SAC is a well-studied Boolean functions characteristic (Forré, 1990) (Cao et al., 2015), which is often used to design S-boxes in order to reach optimal security properties, for example (Kim et al., 1991)(Gupta and Sarkar, 2004).

The paper (Ellingsen et al., 2020) gives a definition to the concept of c-differential uniformity, that may leave ciphers vulnerable to differential cryptanalysis. This concept has also been explored further for power functions with good properties for S-box design in (Hasan et al., 2021), (Stănică and Geary, 2021), (Mesnager et al., 2021), to cite only a few papers among the many that appeared in a short time on the topic. In this paper, we extend the Strict Avalanche Criterion to address new attacks that might stem from such use of the c-differential.

Surely, the Strict Avalanche Criterion can be defined for (vectorial or single output) Boolean and p-ary functions. Throughout this paper, we will take the primitive root of unity, $\zeta = \zeta_p = e^{\frac{2\pi i}{p}}$, for any prime p.

Definition 1. (Li and Cusick, 2005) *Let $wt(a)$ be the Hamming weight of $a \in \mathbb{F}_p^n$, that is, the number of nonzero components of a. Then,*

(i) $f : \mathbb{F}_p^n \to \mathbb{F}_p$ *fulfills the* Strict Avalanche Criterion (SAC) *if and only if* $Prob(f(x+a) - f(x) = b) = \frac{1}{p}$, $\forall a \in \mathbb{F}_p^n, b \in \mathbb{F}_p, wt(a) = 1$. *Equivalently, f fulfills SAC if and only if*

$$\sum_{x \in \mathbb{F}_p^n} \zeta^{f(x+a)-f(x)} = 0,\ \forall a \in \mathbb{F}_p^n, wt(a) = 1.$$

(ii) *For vectorial p-ary functions, this is defined componentwise: a vectorial p-ary function* $F = (F_0, \dots, F_{m-1}) : \mathbb{F}_p^n \to \mathbb{F}_p^m$ *fulfills the* Strict Avalanche Criterion *if and only if* $Prob(F_i(x+a) - F_i(x) = b) = \frac{1}{p}$, $\forall i = 0,\dots,m-1, \forall a \in \mathbb{F}_p^n, b \in \mathbb{F}_p$, $wt(a) = 1$. *Equivalently, F fulfills SAC if and only if* $, \forall i = 0,\dots,m-1$,

$$\sum_{x\in\mathbb{F}_p^n} \zeta^{F_i(x+a)-F_i(x)} = 0,\ \forall a \in \mathbb{F}_p^n, wt(a) = 1.$$

In this paper, we present a new form of Strict Avalanche Criterion based on c-differentials (as defined in (Ellingsen et al., 2020)), and extend the results of (Li and Cusick, 2005) to this new criterion. We need first to rewrite the definition of SAC in the context of finite fields, since the new criterion is more naturally defined in that context.

Let g be a generator of the finite field $\mathbb{F}_{p^k}$. For any k, we use the identification $M_g : \mathbb{F}_p^k \to \mathbb{F}_{p^k}$, defined as $M_g((x_0,\dots,x_{k-1})) = x_0 + x_1 g + \cdots + x_{k-1} g^{k-1}$. Then, $wt(\alpha) = 1$ if and only if $M_g(\alpha) = \alpha_t g^t$ for some $t = 0,\dots,k-1$, $\alpha_t \in \mathbb{F}_p^*$. The components of a vectorial p-ary function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ are $\mathrm{Tr}_m(bF(x))$, where $\mathrm{Tr}_m : \mathbb{F}_{p^m} \to \mathbb{F}_p$ is the absolute trace function, given by $\mathrm{Tr}_m(x) = \sum_{i=0}^{m-1} x^{p^i}$ (we will denote it by Tr, if the dimension is clear from the context). So, it is natural to define the Strict Avalanche Criterion relating it to the derivative of F[1]:

Definition 2. *Let* $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ *a p-ary* (n,m)*-function. Let g be a generator of* $\mathbb{F}_{p^n}$*. We say that F fulfills SAC if and only if*

$$\sum_{x\in\mathbb{F}_p^n} \zeta^{\mathrm{Tr}_m(b(F(x+a)-F(x)))} = 0, \text{ for all } b \in \mathbb{F}_{p^m}^*, a = a_t g^t,$$

for some $t = 0,\dots,k-1$, $a_t \in \mathbb{F}_p^*$.

NB: Given a p-ary (n,m)-function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$, the derivative of F with respect to $a \in \mathbb{F}_{p^n}$ is the function

$$D_a F(x) = F(x+a) - F(x), \text{ for all } x \in \mathbb{F}_{p^n}.$$

Using this notation, fulfills SAC if and only if

$$\sum_{x\in\mathbb{F}_p^n} \zeta^{\mathrm{Tr}_m(bD_aF(x))} = 0, \text{ for all } b \in \mathbb{F}_{p^m}^*, a = a_t g^t \in \mathbb{F}_{p^n}^*,$$

for some $t = 0,\dots,k-1$, $a_t \in \mathbb{F}_p^*$.

Remark 1. *Note that Definition 2 is more restrictive than Definition 1. The reason for this is that, while in the usual definition (Definition 1) the output components are considered independently, in Definition 2 the condition is for the derivative as a single object; in fact, for* $n = m$*, the condition of Definition 2 is equivalent to all derivatives* $D_aF(x)$ *(for* $a = a_t g^t$*) being permutation polynomials (see* (Lidl and Niederreiter, 1997, Theorem 7.7))*, and, in fact, as Lemma 1 shows (taking* $c = 1$*), Definition 2 is equivalent to the balancedness of the derivative itself. For example, the function* $F : \mathbb{F}_2^2 \to \mathbb{F}_2^2$ *defined by* $F(x_0,x_1) = (x_0x_1, x_0x_1)$ *fulfills SAC according to Definition 1, since, for each component, the derivatives with respect to* $a = (0,1)$ *and* $a = (1,0)$ *are balanced. However, if we map the function* $F : \mathbb{F}_2^2 \to \mathbb{F}_2^2$ *to the function* $F' : \mathbb{F}_4 \to \mathbb{F}_4$ *by applying the map* M_g *to its input and output we see that* F' *has values* $F'(0) = 0, F'(g) = 0, F'(1) = 0, F'(g^2) = g^2$*. It is easy to see that neither derivative* $D_1F'(x)$ *nor* $D_gF'(x)$ *are permutation polynomials. Thus,* F' *does not fulfill SAC under Definition 2. Furthermore, while there exist functions* $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ *that fulfill SAC under Definition 1 (at any rate, for even dimension), there exists no function* $F' : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *that fulfills SAC under Definition 2, since* $F'(x+a) - F'(x)$ *has the same values for x and* $x+a$*, and can therefore never be a permutation. However, it is not an empty definition, if* $m \neq n$*, as we see below.*

Example 1. *The function* $F : \mathbb{F}_4 \to \mathbb{F}_2$ *defined by its values* $F(0) = 0, F(g) = 0, F(1) = 0, F(g^2) = 1$ *fulfills SAC under Definition 1, since here* $b = 1$, $a = 1$ *or* $a = g$*, and*

$$\sum_{x\in\mathbb{F}_4} (-1)^{\mathrm{Tr}_1(bD_1F(x))} = \sum_{x\in\mathbb{F}_4} (-1)^{D_1F(x)} = 0$$

and

$$\sum_{x\in\mathbb{F}_4} (-1)^{\mathrm{Tr}_1(bD_gF(x))} = \sum_{x\in\mathbb{F}_4} (-1)^{D_gF(x)} = 0.$$

We recall below the differential extension from (Ellingsen et al., 2020), in the context of finite fields.

Definition 3. (Ellingsen et al., 2020) *Given a p-ary* (n,m)*-function* $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$*, and* $c \in \mathbb{F}_{p^m}$*, the (multiplicative) c-derivative of F with respect to* $a \in \mathbb{F}_{p^n}$ *is the function*

$${}_cD_aF(x) = F(x+a) - cF(x), \text{ for all } x \in \mathbb{F}_{p^n}.$$

(Note that, if $c = 1$*, then we obtain the usual derivative, and, if* $c = 0$ *or* $a = 0$*, then we obtain a shift (input, respectively, output) of the function.)*

It is natural to consider then an extension of the Strict Avalanche Criterion (SAC) using this new derivative.

[1] We have not found a definition for SAC in the finite fields context in the literature, though we do not claim that this is necessarily new.

2 THE C-STRICT AVALANCHE CRITERION (C-SAC)

In this section, we extend the Strict Avalanche Criterion (SAC) to address new attacks that might stem from the use of the c-differential.

Definition 4. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ be a p-ary (n,m)-function. We say that F fulfills the c-Strict Avalanche Criterion (c-SAC) if and only if* $\sum_{x\in\mathbb{F}_p^n} \zeta^{\mathrm{Tr}_m(b(F(x+a)-cF(x)))} = \sum_{x\in\mathbb{F}_p^n} \zeta^{\mathrm{Tr}_m(bF(x+a))-\mathrm{Tr}_m(cbF(x))} = 0$*, for all* $b \in \mathbb{F}_{p^m}^*$, $a = a_t g^t \in \mathbb{F}_{p^n}^*$*, for some* $t = 0,\ldots,k-1$, $a_t \in \mathbb{F}_p^*$.

In (Stănică et al., 2020), for $F \in \mathcal{B}_{n,p}^m$ (the set of all functions from $\mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$) and fixed $c \in \mathbb{F}_{2^m}$, we define the *c-crosscorrelation* at $u \in \mathbb{F}_{p^n}, b \in \mathbb{F}_{p^m}$ by

$$_c\mathcal{C}_{F,G}(u,b) = \sum_{x\in\mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_m(b(F(x+u)-cG(x)))}$$

and the corresponding *c-autocorrelation* at $u \in \mathbb{F}_{p^n}$, $_c\mathcal{C}_F(u,b) = {}_c\mathcal{C}_{F,F}(u,b)$.

Using this, we say that for $F \in \mathcal{B}_{n,p}^m$ and fixed $c \in \mathbb{F}_{2^m}$, F fulfills the c-Strict Avalanche Criterion (c-SAC) if and only if $_c\mathcal{C}_F(a,b) = 0$, $\forall b \in \mathbb{F}_{p^m}^*$, $a = a_t g^t \in \mathbb{F}_{p^n}^*$ for some $t = 0,\ldots,k-1$, $a_t \in \mathbb{F}_p^*$.

Remark 2. *Note that, for $n = m$, the Perfect c-Nonlinear (PcN) class defined in* (Ellingsen et al., 2020) *is a subclass of the set of functions fulfilling c-SAC, and, in general, its generalization, the c-bent$_1$ class, defined in* (Stănică et al., 2020)*, is a subclass of c-SAC. However, as we show in Section* 5*, these subclasses are strict, and we can find examples of* (n,n)*-vectorial p-ary functions that fulfill c-SAC for some c but are not PcN* (*which, for $n = m$, is equivalent to c-bent$_1$*) *for that value of c, for both even and odd characteristics.*

3 THEORETICAL RESULTS ON THE C-STRICT AVALANCHE CRITERION

Note that, as in the classical case, the correlation condition and the balancedness are equivalent[2]:

Lemma 1. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ a p-ary (n,m)-function. Then, F fulfills c-SAC if and only if all the traces of multiples of c-differentials with respect to any a of p-ary weight* 1 *are balanced, i.e.* $\mathrm{Tr}_m({}_cD_a bF(x))$ *is balanced, for all $b \in \mathbb{F}_{p^m}^*$, $a = a_t g^t \in \mathbb{F}_{p^n}^*$, for some $t = 0,\ldots,k-1$, $a_t \in \mathbb{F}_p^*$.*

Proof. We follow the proof of (Stănică et al., 2020, Theorem 2.5), and include it here for the convenience of the reader.

With $c \in \mathbb{F}_{p^n}$ constant, for every $u \in \mathbb{F}_{p^n}, b \in \mathbb{F}_{p^m}$, $0 \le j \le p-1$, we let $S_{j,c}^{u,b} = \{x \in \mathbb{F}_{p^n} \,|\, \mathrm{Tr}_m(b(F(x+u)-cF(x))) = j\}$. We will use below that the order of the cyclotomic polynomial of index p^m is $\phi(p^m) = p^{m-1}(p-1)$.

First, recall that the p^k-cyclotomic polynomial is $\phi_{p^k}(x) = 1 + x^{p^{k-1}} + x^{2p^{k-1}} + \cdots + x^{(p-1)p^{k-1}}$. In particular, we deduce that $\zeta_p^{p-1} = -(1+\zeta_p+\cdots+\zeta_p^{p-2})$. If $u \in \mathbb{F}_{p^n}^*$ such that $u = u_t g^t$ for some $t = 0,\ldots,k-1$, $u_t \in \mathbb{F}_p^*$, $b \in \mathbb{F}_{p^m}^*$, and F fulfills c-SAC, then

$$\begin{aligned}0 ={}_c\mathcal{C}_F(u,b) &= \sum_{x\in\mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_m(b(F(x+u)-cF(x)))}\\ &= \sum_{j=0}^{p-1} |S_{j,c}^{u,b}|\zeta_p^j = \sum_{j=0}^{p-2}\left(|S_{j,c}^{u,b}| - |S_{p-1,c}^{u,b}|\right)\zeta_p^j.\end{aligned}$$

The extension $\mathbb{Q} \overset{p-1}{\hookrightarrow} \mathbb{Q}(\zeta_p)$ has degree $p-1$ and the elements in following set $\left\{\zeta_p^j \,|\, 0 \le j \le p-2\right\}$ are linearly independent in $\mathbb{Q}(\zeta_p)$ over $\mathbb{Q}$, therefore the coefficients in the displayed expression are zero, that is, that for all $0 \le j \le p-2$, $|S_{j,c}^{u,b}| = |S_{p-1,c}^{u,b}|$. Summarizing, for any $0 \le j \le p-1$, the cardinality of the set $S_{j,c}^{u,b}$ is independent of j, and so, for all $c,b,u \ne 0$ fixed, the function $x \mapsto \mathrm{Tr}_m(b(F(x+u)-cF(x))$ is balanced for all $u = u_t g^t$ for some $t = 0,\ldots,k-1$, $u_t \in \mathbb{F}_p^*$, $b \in \mathbb{F}_{p^m}^*$.

If $x \mapsto \mathrm{Tr}_m(b(F(x+u)-cF(x))$ is balanced, by reversing the argument, we find that f fulfills c-SAC. ☐

This means that F fulfills c-SAC if and only if any of the following equivalent conditions are fulfilled:

1. $_c\mathcal{C}_F(a,b) = 0$ $\forall b \in \mathbb{F}_{p^m}^*$, $a = a_t g^t \in \mathbb{F}_{p^n}^*$, for some $t = 0,\ldots,k-1$, $a_t \in \mathbb{F}_p^*$.
2. the function $x \mapsto \mathrm{Tr}_m(b(F(x+a)-cF(x))$ is balanced, for all $b \in \mathbb{F}_{p^m}^*$, $a = a_t g^t \in \mathbb{F}_{p^n}^*$, for some $t = 0,\ldots,k-1$, $a_t \in \mathbb{F}_p^*$.

The (vectorial) Walsh transform $\mathcal{W}_F(a,b)$ of an (n,m)-function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ at $a \in \mathbb{F}_p^n, b \in \mathbb{F}_p^m$ is the Walsh-Hadamard transform of its component function $\mathrm{Tr}_m(bF(x))$ at a, that is,

$$\mathcal{W}_F(a,b) = \sum_{x\in\mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_m(bF(x))-\mathrm{Tr}_n(ax)}.$$

[2]Note that, as stated before, for the case $n = m$, this result is given in (Lidl and Niederreiter, 1997, Theorem 7.7).

We can extend Lemma 3.3 of (Li and Cusick, 2005), using (Stănică et al., 2020, Lemma 2.2) (the proof follows directly from (Stănică et al., 2020, Lemma 2.2) and it is omitted):

Lemma 2. *We have* $h(u,b) = {}_cC_F(u,b)$ *if and only if* $\sum_{u\in\mathbb{F}_{p^n}} h(u,b)\zeta_p^{-\mathrm{Tr}_n(ux)} = \mathcal{W}_F(x,b)\overline{\mathcal{W}_F(x,bc)}$.

This implies that:

Lemma 3. *Let* $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ *a* p*-ary* (n,m)*-function. Then,* F *satisfies* c*-SAC if and only if* $\sum_{y\in\mathbb{F}_{p^n}} \mathcal{W}_F(y,b)\overline{\mathcal{W}_F(y,bc)}\zeta_p^{\mathrm{Tr}_n(ay)} = 0, \quad \forall b \in \mathbb{F}^*_{p^m}, a = a_t g^t \in \mathbb{F}^*_{p^n}$, *for some* $t = 0,\ldots,k-1$, $a_t \in \mathbb{F}^*_p$.

Proof. By (Stănică et al., 2020, Lemma 2.2), $\sum_{y\in\mathbb{F}_{p^n}} \mathcal{W}_F(y,b)\overline{\mathcal{W}_F(y,bc)}\zeta_p^{\mathrm{Tr}_n(ay)} = \mathcal{C}_F(a,b)$. The result follows. □

Let $U,T : \mathbb{F}_{p^n}\times\mathbb{F}_{p^n} \to \mathbb{C}$. We define the left convolution by $(U\star T)(x,y) = \sum_{z\in\mathbb{F}_{p^n}} U(x-z,y)T(z,y)$. Let $F,G : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$. Then, it is easy to show that

$$(\mathcal{W}_F \star \mathcal{W}_G)(a,b) = p^n\mathcal{W}_{F+G}(a,b)$$

and so,

$$(\mathcal{W}_F \star \mathcal{W}_{-F})(a,b) = \begin{cases} p^{2n} & \text{if } a = 0\\ 0 & \text{if } a \neq 0.\end{cases}$$

We will show below that the c-SAC is preserved by extended-affine (EA) equivalence, where EA-equivalence is defined as follows:

Definition 5. (Canteaut and Perrin, 2019) *Two functions* $F,G : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ *are extended-affine equivalent (EA-equivalent) if and only if there exist* $\alpha \in \mathbb{F}^*_{p^m}$, $e \in \mathbb{F}_{p^m}$, $\beta \in \mathbb{F}^*_{p^n}$, $d \in \mathbb{F}_{p^n}$ *such that* $G(x) = \alpha F(\beta x+d)+e$.

The next theorem is a generalization of Theorems 3.6 and 3.7 of (Li and Cusick, 2005).

Theorem 1. *The* c*-SAC is preserved under the EA-equivalence.*

Proof. We need to prove that F satisfies c-SAC if and only if $G(x) = \alpha F(\beta x+d)+e$ satisfies c-SAC, where $\alpha \in \mathbb{F}^*_{p^m}$, $e \in \mathbb{F}_{p^m}$, $\beta \in \mathbb{F}^*_{p^n}$, $d \in \mathbb{F}_{p^n}$. Thus, G satisfies c-SAC if and only if $\sum_{x\in\mathbb{F}_p^n} \zeta^{\mathrm{Tr}_m(b(G(x+a)-cG(x)))} = 0$, $\forall b \in \mathbb{F}^*_{p^m}$, $a = a_t g^t \in \mathbb{F}^*_{p^n}$, for some $t = 0,\ldots,k-1$, $a_t \in \mathbb{F}^*_p$. Calling $y = \beta x+d$, we have that

$$\sum_{x\in\mathbb{F}_p^n} \zeta_p^{\mathrm{Tr}_m(b(G(x+a)-cG(x)))} =$$
$$= \sum_{x\in\mathbb{F}_p^n} \zeta_p^{\mathrm{Tr}_m(b(\alpha F(\beta x+d+a)+e-c(\alpha F(\beta x+d)+e))}$$
$$= \zeta_p^{\mathrm{Tr}_m(b(1-c)e)} \sum_{y\in\mathbb{F}_p^n} \zeta_p^{\mathrm{Tr}_m(b\alpha(F(y+a)-cF(y)))}.$$

The theorem follows. □

For the next result, which generalizes Theorem 3.8 of (Li and Cusick, 2005), we need to introduce some notations. Let $n = n_1+n_2$, and g,g_1,g_2 be generators of $\mathbb{F}_{p^n}, \mathbb{F}_{p^{n_1}}, \mathbb{F}_{p^{n_2}}$, respectively. Then, we can write any element z of $\mathbb{F}_{p^n}$ as $z = x_0 + x_1 g + \cdots + x_{n_1-1}g^{n_1-1} + y_0 g^{n_1} + y_1 g^{n_1+1} + \cdots + y_{n_2} g^{n_1+n_2-1}$. We define then $\sigma_1 : \mathbb{F}_{p^n} \to \mathbb{F}_{p^{n_1}}$ as $\sigma_1(z) = x_0 + x_1 g_1 + \cdots + x_{n_1-1} g_1^{n_1-1}$ and $\sigma_2 : \mathbb{F}_{p^n} \to \mathbb{F}_{p^{n_2}}$ as $\sigma_2(z) = y_0 + y_1 g_2 + \cdots + y_{n_2-1} g_2^{n_1-1}$. It is easy to see that σ_1 and σ_2 are linear over $\mathbb{F}_p$.

Theorem 2. *Let* F *be an* (n_1,m)*-vectorial* p*-ary function, and* G *be an* (n_2,m)*-vectorial* p*-ary function. We define an* (n,m)*-vectorial* p*-ary function by* $H(z) = F(\sigma_1(z)) + G(\sigma_2(z))$. *Then,* H *fulfills SAC if and only if both* F *and* G *fulfill SAC.*

Proof. We write

$$\sum_{z\in\mathbb{F}_p^n} \zeta_p^{\mathrm{Tr}_m(b(H(z+a)-cH(z)))} =$$
$$\sum_{z\in\mathbb{F}_p^n} \zeta_p^{\mathrm{Tr}_m(b(F(\sigma_1(z+a))-cF(\sigma_1(z))))} \zeta_p^{\mathrm{Tr}_m(b(G(\sigma_2(z+a))-cF(\sigma_2(z))))}.$$

Now, $\sigma_i(z+a) = \sigma_i(z)+\sigma_i(a)$. Since $a = a_t g^t$ for some $t = 0,\ldots,k-1$, $a_t \in \mathbb{F}^*_p$, we have that either $\sigma_1(a) = 0$ or $\sigma_2(a) = 0$. Without loss of generality, we let $\sigma_2(a) = 0$. Then, denoting $x = \sigma_1(x), \alpha = \sigma_1(a) = a_t g_1^t$, we have

$$\sum_{z\in\mathbb{F}_p^n} \zeta_p^{\mathrm{Tr}_m(b(H(z+a)-cH(z)))} = p^{n_2} \sum_{x\in\mathbb{F}_p^{n_1}} \zeta_p^{\mathrm{Tr}_m(b(F(x+\alpha)-cF(x)))}.$$

The autocorrelation of H with respect to a is zero if and only if the autocorrelation of F with respect to α is zero.

Taking into account the two cases, $\sigma_1(a) = 0$ or $\sigma_2(a) = 0$, the theorem follows. □

Definition 6. *Function* $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ *is called* $\frac{1}{p}$*-*c*-independent in its* x *input if and only if for any* $c,b,x \in \mathbb{F}_{p^n}$, $\alpha \in \mathbb{F}_p$ *and* $a = a_t g^t, t = 0,1\ldots,k-1, a_t \in F^*_p$, *the probability* $Prob(Tr(bF(x+a)) = Tr(bcF(x)) + \alpha) = \frac{1}{p}$.

In order to connect it to the c-SAC condition, we can say that, if the function F is $\frac{1}{p}$-c-independent in all components, then it is c-SAC, meaning that $\sum_{x\in\mathbb{F}_{p^n}} \zeta^{\mathrm{Tr}_m(bF(x+a))-\mathrm{Tr}_m(cbF(x))} = 0$.

Theorem 3. *If* $\mathcal{W}_F(x,b)\overline{\mathcal{W}_F(-x,bc)} = \mathcal{W}_F(x+z,b)\overline{\mathcal{W}_F(-x-z,bc)}$ *for any* $z = \sum_{i=0}^{n-1} a_i g^i$, *so that* $a \in \mathbb{F}_p$ *and* g*, a generator of the field,* $z \in I_{i_1 i_2\ldots i_m} = \left\{a_0 g^0 + \cdots + a_{n-1}g^{n-1} \mid a_i \neq 0 \Longrightarrow i \in \{i_0,\ldots,i_{m-1}\}\right\}$, *then* $F(x)$ *is* $\frac{1}{p}$*-*c*-independent in the input coordinates* $a_{i_0}, a_{i_1},\ldots,a_{i_n-1}$.

Proof. Let $x' \in \mathbb{F}_{p^n}$, $x' = \sum_{i=0}^{n-1} a'_i g^i$, and

$$S_{x'} = \{x \in \mathbb{F}_{p^n} \mid x' = \sum_{i=0}^{n-1} a'_i g^i = x'_m\},$$

so that,

$$\mathbb{F}_{p^n} = \bigcup_{x' \in GF(p)^m} S_{x'}, \quad S_{x'_1} \cap S_{x'_2} = \emptyset \Longleftrightarrow x'_1 \neq x'_2.$$

By the hypothesis of the theorem, we can write:

$$\sum_{x \in S_{x'}} \mathcal{W}_F(x,b)\overline{\mathcal{W}_F(-x,bc)} = \sum_{x \in S_{x'+z'}} \mathcal{W}_F(x,b)\overline{\mathcal{W}_F(-x,bc)},$$

for any $x', z' \in \mathbb{F}_{p^n}$. Now let $x' = a_0 g^0 + x''$, so that $x'' = \sum_{i=1}^{n-1} a_i g^i$ and $a_0 = 0$, or for short notation $x' = (0, x'')$, and the same for $z' = (j, z''), z'' \in I_{i_2 \dots i_m}, 1 \leq j \leq p-1$, will be

$$\sum_{x \in S_{(0,x'')}} \mathcal{W}_F(x,b)\overline{\mathcal{W}_F(-x,bc)} = \sum_{x \in S_{(j,x''+z'')}} \mathcal{W}_F(x,b)\overline{\mathcal{W}_F(-x,bc)},$$

for any $x'', z'' \in \mathbb{F}(p^{n-1})$. Thus,

$$\sum_{x'' \in F_{p^{n-1}}} \sum_{x \in S_{(0,x'')}} \mathcal{W}_F(x,b)\overline{\mathcal{W}_F(-x,bc)} = \sum_{x'' \in F_{p^{n-1}}} \sum_{x \in S_{(j,x''|z'')}} \mathcal{W}_F(x,b)\overline{\mathcal{W}_F(-x,bc)}$$

and

$$\sum_{x: x_{i_1}=0} \mathcal{W}_F(x,b)\overline{\mathcal{W}_F(-x,bc)} = \sum_{x: x_{i_1}=j} \mathcal{W}_F(x,b)\overline{\mathcal{W}_F(-x,bc)},$$

for $j \in 1, 2 \dots, p-1$.

That means that $f(x)$ is $\frac{1}{p}$-c-independent in the i_1 input and the other components can be obtained in the same way. □

4 THE *C*-STRICT AVALANCHE CRITERION OF HIGHER ORDER

Given a function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^l}$, we fix a set of indices $I = \{j_1, \dots, j_m\}$, and define a restriction of F, by fixing the coordinates corresponding to the indices in I, that is, the restriction's input is written as $x = \sum_{i \notin I} a_i g^i + \sum_{j \in I} a_j g^j$, where $a_j \in \mathbb{F}_p$ are chosen to be constants. Then we can define the *c-Strict Avalanche Criterion of order m (c-SAC(m))* as follows.

Definition 7. *Let F be an (n,m)-vectorial p-ary function. Then, the function $F(x)$ satisfies the c-*Strict Avalanche Criterion of order m (c-SAC(m)) *if for m chosen constant inputs, the corresponding restriction of $F(x)$ satisfies c-SAC.*

Theorem 4. *If a function $F(x)$ satisfies c-SAC(m), it also satisfies c-SAC $(m-1)$, for $1 \leq m \leq n-1$.*

Proof. First we introduce the function $F_{I c_{j_1} \dots c_{j_m}}^{z_{j_1} \cdots z_{j_m}}(x)$, which is obtained from the function $F(x)$ by fixing a_j to a constant y_j. So the input of the F_I will be of the form $x = \sum_{i \notin I} a_i g^i + \sum_{j \in I} a_j g^j$, where $I = \{j_1 \dots j_m\}$ is a set of indices of fixed elements for $F_I(x)$.

Thus, $I = \{j_1, \dots, j_m\}$ is a set of indices of fixed elements for $F(x)$, where $x = \sum_{i \notin I} a_i g^i + \sum_{j \in I} a_j g^j$, and $z_j = a_j g^j = y_j g^j$ where $y_j \in \mathbb{F}_p$ are fixed constants.

Then, $F(x)$ can be written as $F_{c_{j_1} \dots c_{j_m}}^{z_{j_1} \cdots z_{j_m}}(x)$, obtained from $F(x)$ by fixing a_j to constant y_j, and $\alpha_i = u_i g^i$, $u_i \in \mathbb{F}_p, i \notin I$. We next consider:

$$M = \sum_{x' = \sum_{i \notin I} a_i g^i, a_i \in F_p} \zeta^{\mathrm{Tr}(bF_{c_{j_1} \dots c_{j_m}}^{z_{j_1} \cdots z_{j_m}}(x+\alpha)) - \mathrm{Tr}(bcF_{c_{j_1} \dots c_{j_m}}^{z_{j_1} \cdots z_{j_m}}(x))}.$$

Now, let $x = \sum_{i \notin I} a_i g^i + \sum_{j \in I \setminus \{j_l\}} a_j g^j + \delta g^{j_l}$, where δ is an element extracted from the set I corresponding to g^{j_l}, so the function will be of the form $F_{c_{j_1} \dots c_{j_{l-1}}, c_{j_{l+1}} \dots c_{j_m}, \delta}^{z_{j_1} \dots z_{j_{l-1}}, z_{j_{l+1}} \dots z_{j_m}, z_{j_l}}$, which, for brevity, it will be denoted $F_{c_{j_1} \dots c_{j_m}, \delta}^{z_{j_1} \dots z_{j_m} z_{j_l}}$. Next,

$$M = \sum_{\delta=0}^{p-1} \sum_{\substack{x' = \sum_{i \notin I} a_i g^i, \\ a_i \in F_p}} \zeta^{\mathrm{Tr}(bF_{c_{j_1} \dots c_{j_m}, \delta}^{z_{j_1} \dots z_{j_m} z_{j_l}}(x+\alpha)) - \mathrm{Tr}(cbF_{c_{j_1} \dots c_{j_m}, \delta}^{z_{j_1} \dots z_{j_m} z_{j_l}}(x))}.$$

Following the definition of the c-SAC all internal p-sums are equal to zero, since the function satisfies c-SAC(m). Therefore, for $M = 0$, the function satisfies the c-SAC($m-1$), since every $F_{c_{j_1} \dots c_{j_m}}^{z_{j_1} \dots z_{j_m}}$ satisfies c-SAC. □

5 COMPUTATIONAL RESULTS AND ANALYSIS

This section displays a partial list of functions of type $F : \mathbb{F}_{2^3} \to \mathbb{F}_{2^3}$ and $F : \mathbb{F}_{3^2} \to \mathbb{F}_{3^2}$ that fulfill c-SAC but are not PcN (which, for $n=m$, is equivalent to c-bent$_1$), for the values of c given in the list. It is interesting to note that all functions of type $F:\mathbb{F}_{2^2}\to\mathbb{F}_{2^2}$ we found that fulfilled c-SAC were PcN for those values of c.

As argued before, for $p=2$ there are no (n,n)-functions that are c-SAC for $c=1$. We do, however, find examples of (n,n)-functions that fulfill c-SAC for $c=1$ for $p=3$. We note that these are PN (perfect nonlinear). Below, g denotes a primitive element in the considered field.

5.1 Even characteristic

The following functions $F:\mathbb{F}_{2^3}\to\mathbb{F}_{2^3}$ fulfill c-SAC for $c\in\{g,g^2,g^2+g+1,g^2+1\}$:

1. $(g^2+1)x^6+(g+1)x^5+(g+1)x^4+(g^2+g)x^3+x^2+g^2x$;
2. $gx^6+x^5+gx^4+(g^2+g+1)x^3+(g+1)x^2+(g+1)x$;
3. $g^2x^6+(g^2+g+1)x^5+x^4+(g^2+g)x^3+(g^2+g)x^2+(g^2+1)x$;
4. $(g^2+g+1)x^6+gx^5+x^4+x^3+(g^2+g)x^2+(g^2+1)x$;
5. $(g^2+g+1)x^6+(g^2+g)x^5+g^2x^3+(g^2+1)x^2+(g^2+g+1)x$;
6. $(g^2+g)x^6+(g+1)x^5+g^2x^4+gx^3+gx^2+g^2x$;
7. $g^2x^6+(g^2+1)x^5+gx^4+x^3+g^2x^2$;
8. $(g^2+g)x^6+(g+1)x^5+(g^2+1)x^4+gx^3+(g+1)x^2+(g^2+g+1)x$;
9. $g^2x^6+(g^2+1)x^5+(g^2+1)x^4+x^3+(g+1)x^2+(g^2+g+1)x$;
10. $gx^6+(g^2+g)x^5+(g+1)x^4+(g+1)x^3+x^2+g^2x$;
11. $(g^2+g+1)x^6+gx^5+(g+1)x^4+x^3+x^2+g^2x$;
12. $(g^2+g)x^6+(g+1)x^5+(g^2+g)x^4+gx^3+(g^2+1)x^2+(g^2+1)x$;
13. $gx^6+x^5+(g^2+g+1)x^3+g^2x^2+gx$;
14. $x^6+(g^2+1)x^5+(g^2+g+1)x^4+(g^2+g)x^3+(g^2+g)x^2+(g^2+g+1)x$;
15. $(g^2+1)x^6+(g+1)x^5+(g^2+1)x^4+(g^2+g)x^3+gx^2+x$;
16. $(g^2+g+1)x^6+gx^5+(g^2+g)x^4+x^3+(g^2+g+1)x^2+(g^2+g+1)x$;
17. $gx^6+x^5+x^4+(g^2+g+1)x^3+(g^2+g)x^2+(g^2+1)x$;
18. $(g^2+1)x^6+(g+1)x^5+x^4+(g^2+g)x^3+(g^2+g)x^2+(g^2+1)x$;
19. $(g^2+g+1)x^6+g^2x^5+(g^2+g+1)x^4+(g+1)x^3+x^2+(g^2+1)x$;
20. $x^6+(g^2+1)x^5+(g^2+1)x^4+(g^2+g)x^3+(g+1)x^2+(g^2+g+1)x$;
21. $(g^2+g)x^6+x^5+(g+1)x^4+(g^2+1)x^3+(g^2+g)x^2+(g^2+g)x$;
22. $(g^2+g+1)x^6+g^2x^5+(g^2+1)x^4+(g+1)x^3+(g+1)x^2+(g^2+g+1)x$;
23. $gx^6+(g^2+g+1)x^5+x^4+(g^2+1)x^3+gx^2$;
24. $(g+1)x^6+g^2x^5+(g^2+g+1)x^4+x^3+g^2x^2+(g^2+g)x$;
25. $x^6+(g+1)x^5+(g^2+g)x^4+g^2x^3+(g^2+1)x$;
26. $(g^2+g)x^6+gx^5+(g^2+g)x^4+g^2x^3+(g^2+1)x^2+(g^2+g+1)x$;
27. $(g^2+1)x^6+(g^2+g+1)x^5+(g^2+g+1)x^4+(g+1)x^3+g^2x^2+(g^2+g)x$.

The following functions $F:\mathbb{F}_{2^3}\to\mathbb{F}_{2^3}$ fulfill c-SAC for $c\in\{g,g+1,g^2+g,g^2+1\}$:

1. $(g^2+g)x^6+gx^5+(g^2+1)x^4+g^2x^3+g^2x^2+(g+1)x$;
2. $(g^2+1)x^6+(g^2+g+1)x^5+g^2x^4+(g+1)x^3+(g^2+1)x^2+gx$;
3. $(g+1)x^6+(g^2+1)x^5+(g^2+g+1)x^4+(g^2+g+1)x^3+gx^2+(g^2+g+1)x$;
4. $(g^2+g)x^6+gx^5+g^2x^4+g^2x^3+(g^2+1)x^2+gx$;
5. $(g+1)x^6+(g^2+1)x^5+x^4+(g^2+g+1)x^3+(g^2+g)x^2+(g^2+1)x$;
6. $gx^6+(g^2+g)x^5+x^4+(g+1)x^3+(g^2+g)x^2+(g^2+1)x$;
7. $(g^2+1)x^6+(g^2+g+1)x^5+(g+1)x^4+(g+1)x^3+x$.
8. $x^6+(g^2+g)x^5+g^2x^4+(g^2+g+1)x^3+(g^2+g+1)x^2+(g^2+1)x$;
9. $g^2x^6+gx^5+(g^2+g+1)x^4+(g^2+1)x^3+g^2x^2+(g^2+g)x$;
10. $(g^2+1)x^6+g^2x^5+gx^4+gx^3+(g^2+g)x^2+gx$;
11. $x^6+(g^2+g)x^5+(g^2+g+1)x^4+(g^2+g+1)x^3+g^2x^2+(g^2+g)x$;
12. $(g^2+1)x^6+g^2x^5+(g+1)x^4+gx^3+x^2+g^2x$;
13. $(g^2+g)x^6+x^5+(g+1)x^4+(g^2+1)x^3+x^2+g^2x$;
14. $g^2x^6+gx^5+(g^2+1)x^4+(g^2+1)x^3+(g+1)x$;
15. $(g+1)x^6+x^5+x^4+gx^3+(g^2+g+1)x$;
16. $(g^2+g+1)x^6+g^2x^5+(g+1)x^3+(g^2+1)x^2+(g+1)x$;
17. $(g^2+g)x^6+x^5+g^2x^4+(g^2+1)x^3+gx^2$;

18. $x^6+(g^2+1)x^5+gx^4+(g^2+g)x^3+(g^2+g+1)x^2+x$;
19. $(g^2+g+1)x^6+g^2x^5+gx^4+(g+1)x^3+(g^2+g+1)x^2+x$;
20. $(g^2+1)x^6+(g+1)x^5+gx^4+(g^2+g)x^3+(g^2+g)x^2+(g^2+g+1)x$;
21. $gx^6+x^5+(g^2+g)x^4+(g^2+g+1)x^3+gx^2+(g+1)x$;
22. $(g^2+g+1)x^6+gx^5+x^4+x^3+(g+1)x^2+x$;
23. $(g^2+1)x^6+(g+1)x^5+(g^2+g)x^4+(g^2+g)x^3+gx^2+(g+1)x$;
24. $(g^2+1)x^6+(g^2+g+1)x^5+(g^2+g)x^4+(g+1)x^3+(g+1)x^2+(g^2+g)x$;
25. $gx^6+x^5+(g^2+g+1)x^4+(g^2+g+1)x^3+g^2x$.

The following functions $F:\mathbb{F}_{2^3}\to\mathbb{F}_{2^3}$ fulfill c-SAC for $c\in\{g^2,g+1,g^2+g,g^2+g+1\}$:

1. $gx^6+(g^2+g+1)x^5+g^2x^4+(g^2+1)x^3+x^2+(g^2+g+1)x$;
2. $(g+1)x^6+g^2x^5+gx^4+x^3+(g^2+g+1)x^2+x$;
3. $x^6+(g+1)x^5+(g+1)x^4+g^2x^3+(g+1)x^2+gx$;
4. $gx^6+(g^2+g+1)x^5+gx^4+(g^2+1)x^3+(g^2+g+1)x^2+x$;
5. $x^6+(g+1)x^5+x^4+g^2x^3+(g^2+g)x^2+(g^2+1)x$;
6. $(g^2+1)x^6+g^2x^5+x^4+gx^3+(g^2+g)x^2+(g^2+1)x$;
7. $(g+1)x^6+g^2x^5+(g^2+g)x^4+x^3+g^2x^2$;
8. $g^2x^6+gx^5+(g^2+g+1)x^4+(g^2+1)x^3+(g^2+g+1)x^2+gx$;
9. $(g^2+g)x^6+gx^5+(g^2+g+1)x^4+g^2x^3+(g+1)x^2+gx$;
10. $(g^2+1)x^6+(g^2+g+1)x^5+(g^2+g)x^4+(g+1)x^3+gx^2+(g+1)x$;
11. $(g+1)x^6+(g^2+1)x^5+(g^2+1)x^4+(g^2+g+1)x^3+(g^2+1)x^2+(g^2+g)x$;
12. $(g^2+g)x^6+gx^5+(g^2+g)x^4+g^2x^3+gx^2+(g+1)x$;
13. $(g+1)x^6+(g^2+1)x^5+(g+1)x^4+(g^2+g+1)x^3+x^2+g^2x$;
14. $g^2x^6+(g^2+g+1)x^5+(g+1)x^4+(g^2+g)x^3+x^2+g^2x$;
15. $(g^2+1)x^6+(g^2+g+1)x^5+x^4+(g+1)x^3+(g^2+g+1)x^2$;
16. $(g^2+g+1)x^6+(g^2+g)x^5+gx^4+g^2x^3+gx^2+(g^2+g)x$;
17. $g^2x^6+(g^2+g+1)x^5+(g^2+g)x^3+(g+1)x^2+(g^2+1)x$;
18. $(g^2+g+1)x^6+(g^2+g)x^5+g^2x^4+g^2x^3+(g^2+1)x^2+gx$;
19. $(g+1)x^6+x^5+g^2x^4+gx^3+(g^2+1)x^2+gx$;
20. $(g+1)x^6+x^5+(g^2+g)x^4+gx^3+g^2x^2+x$;
21. $(g^2+g+1)x^6+(g^2+g)x^5+(g+1)x^4+g^2x^3+x^2+g^2x$;
22. $g^2x^6+(g^2+g+1)x^5+(g^2+g+1)x^4+(g^2+g)x^3+(g^2+g+1)x^2+(g+1)x$;
23. $(g+1)x^6+x^5+(g+1)x^4+gx^3+x^2+g^2x$;
24. $g^2x^6+(g^2+g+1)x^5+g^2x^4+(g^2+g)x^3+(g^2+1)x^2+gx$;
25. $gx^6+(g^2+g)x^5+g^2x^4+(g+1)x^3+(g^2+1)x^2+gx$.

5.2 Odd characteristic

The following functions $F:\mathbb{F}_{3^2}\to\mathbb{F}_{3^2}$ all fulfill c-SAC and are PcN for $c=1$, in addition to the values of c displayed.

For $c\in\{g,2g,2g+2\}$:

1. $(g+2)x^6+gx^4+x^3+(2g+1)x^2+2gx$;
2. $2x^6+2x^4+(g+1)x^3+2x^2+2gx$;
3. $(2g+2)x^6+(2g+2)x^4+x^3+(2g+2)x^2+gx$;
4. $(g+1)x^6+x^4+gx^3+(2g+2)x^2+x$;
5. $gx^6+(2g+1)x^4+(2g+1)x^3+2gx^2+2x$;
6. $(g+1)x^6+(g+1)x^4+(g+1)x^3+(g+1)x^2$;
7. $gx^6+gx^4+gx^2+2gx$;
8. $gx^6+(2g+1)x^4+2x^3+2gx^2$;
9. $(g+1)x^6+x^4+(g+2)x^3+(2g+2)x^2$;
10. $x^6+(2g+2)x^4+2x^3+2x^2+gx$;
11. $(g+2)x^6+2gx^4+gx^3+(2g+1)x^2+2x$;
12. $2x^6+2x^4+gx^3+2x^2+(2g+2)x$;
13. $gx^6+gx^4+gx^3+gx^2$;
14. $(g+1)x^6+x^4+(2g+2)x^2+gx$;
15. $gx^6+gx^4+x^3+gx^2+(g+2)x$;
16. $(g+2)x^6+2gx^4+(g+1)x^3+(2g+1)x^2+(2g+1)x$;
17. $2gx^6+(g+2)x^4+gx^2+(2g+2)x$;
18. $2x^6+2x^4+(2g+2)x^3+2x^2+(g+2)x$;
19. $x^6+(2g+2)x^4+(g+2)x^3+2x^2+(2g+2)x$;
20. $2x^6+(2g+2)x^4+x^2+2gx$.

For $c\in\{g+1,2g+1,g+2\}$:

1. $(2g+1)x^6+2gx^4+2x^3+(g+2)x^2+(g+2)x$;
2. $x^6+x^4+(2g+2)x^3+x^2+(g+2)x$;

3. $2gx^6 + (2g+1)x^4 + 2gx^3 + gx^2 + (g+1)x$;
4. $(2g+1)x^6 + 2gx^4 + x^3 + (g+2)x^2 + 2gx$;
5. $(2g+2)x^6 + 2x^4 + 2x^3 + (g+1)x^2 + (g+2)x$;
6. $2gx^6 + (g+2)x^4 + 2x^3 + gx^2$;
7. $(2g+2)x^6 + (2g+2)x^4 + (g+2)x^3 + (2g+2)x^2 + 2x$;
8. $2gx^6 + 2gx^4 + (g+2)x^3 + 2gx^2 + (g+1)x$;
9. $2x^6 + (g+1)x^4 + 2gx^3 + x^2$;
10. $2x^6 + (2g+2)x^4 + x^3 + x^2 + (g+2)x$;
11. $2gx^6 + (g+2)x^4 + gx^3 + gx^2 + x$;
12. $(2g+2)x^6 + 2x^4 + 2gx^3 + (g+1)x^2 + (2g+2)x$;
13. $2x^6 + (2g+2)x^4 + (2g+1)x^3 + x^2$;
14. $2gx^6 + (2g+1)x^4 + (2g+1)x^3 + gx^2 + (2g+2)x$;
15. $(g+1)x^6 + x^4 + 2gx^3 + (2g+2)x^2 + 2x$;
16. $x^6 + (g+1)x^4 + 2x^2 + 2gx$;
17. $2gx^6 + 2gx^4 + gx^3 + 2gx^2$;
18. $2x^6 + (g+1)x^4 + x^2 + (g+2)x$;
19. $(2g+1)x^6 + gx^4 + (2g+2)x^3 + (g+2)x^2 + 2gx$;
20. $2gx^6 + (g+2)x^4 + (2g+1)x^3 + gx^2 + 2x$.

6 CONCLUSION AND FUTURE WORK

In this paper, we have generalized the concept of Strict Avalanche Criterion (SAC) in the realm of finite fields to address possible c-differential attacks. Further, we have defined the concepts of c-Strict Avalanche Criterion (c-SAC) and c-Strict Avalanche Criterion of order m (c-SAC(m)), and generalized results of (Li and Cusick, 2005). By computing and checking functions of the given type, we have also shown that the new definition is not equivalent to the existing concepts of c-bent$_1$-ness (Stănică et al., 2020), nor (for $n = m$) PcN-ness (Ellingsen et al., 2020). It would of interest to find, theoretically, classes of functions that fulfill c-SAC or c-SAC(m) for large n and m, and to find other properties satisfied by c-SAC functions, as well as devise a practical attack on particular S-boxes using these concepts. Finally, for small examples, all functions that we found that fulfilled 1-SAC for $n = m$ were PN. It would be worth investigating to find either a function which fulfills 1-SAC but is not PN, or a proof that this cannot happen.

REFERENCES

Biham, E. and Shamir, A. (1991). Differential cryptanalysis of DES-like cryptosystems. *J. Cryptology*, 4(1):3–72.

Biham, E. and Shamir, A. (2012). *Differential cryptanalysis of the Data Encryption Standard*. Springer Science & Business Media.

Canteaut, A. and Perrin, L. (2019). On CCZ-equivalence, extended-affine equivalence, and function twisting. *Finite Fields & Applic.*, 56:209–246.

Cao, Z., Chen, F., Chen, B., and Zhang, X. (2015). Research on the balanced boolean functions satisfying strict avalanche criterion. *International Conference on Computational Science and Computational Intelligence (CSCI)*, pages 680–684.

Ellingsen, P., Felke, P., Riera, C., Stănică, P., and Tkachenko, A. (2020). *C*-differentials, multiplicative uniformity and (almost) perfect c-nonlinearity. *IEEE Trans. Inform. Theory*, 66:5781–5789.

Forré, R. (1990). The strict avalanche criterion: Spectral properties of boolean functions and an extended definition. *Adv. in Crypt. – Crypto '88, Springer-Verlag, LNCS 403*, pages 450–468.

Gupta, K. C. and Sarkar, P. (2004). Construction of perfect nonlinear and maximally nonlinear multiple-output boolean functions satisfying higher order strict avalanche criteria. *IEEE Trans. Inform. Theory*, (11):2886–2893.

Hasan, S. U., Pal, M., Riera, C., and Stănică, P. (2021). On the c-differential uniformity of certain maps over finite fields. *Designs, Codes, and Crypt.*, 89:221–239.

Kim, K., Matsumoto, T., and Imai, H. (1991). A recursive construction method of *S*-boxes satisfying strict avalanche criteria. *Adv. in Crypt. – Crypto '90, LNCS 537*, pages 565–574.

Li, Y. and Cusick, T. W. (2005). Strict avalanche criterion over finite fields. *J. Math. Cryptology*, 1:65–78.

Lidl, J. R. and Niederreiter, H. (1997). *Finite Fields (Ed. 2), Encycl. Math. Appl., vol.20*. Cambridge Univ. Press, Cambridge, London, 2nd edition.

Mesnager, S., Riera, C., Stanica, P., Yan, H., and Zhou, Z. (2021). Investigations on c-(almost) perfect nonlinear functions. *https://arxiv.org/abs/2010.10023*.

Stănică, P., Gangopadhyay, S., Geary, A., Riera, C., and Tkachenko, A. (2020). *C*-differential bent functions and perfect nonlinearity. *https://arxiv.org/abs/2006.12535*.

Stănică, P. and Geary, A. (2021). The c-differential behavior of the inverse function under the *EA*-equivalence. *Cryptogr. Commun.*, 13:295–306.

Webster, A. F. and Tavares, S. E. (1985). On the design of S-boxes. In *Adv. in Crypt. – Crypto '85, Springer-Verlag, LNCS 218*, pages 523–534. Springer, Berlin, Heidelberg.