2020-09-17

Characters, Weil sums and c-differential uniformity with an application to the perturbed Gold function

Stnic, Pantelimon; Riera, Constanza; Tkachenko, Anton

ArXiv

Stnic, Pantelimon, Constanza Riera, and Anton Tkachenko. "Characters, Weil sums and c-differential uniformity with an application to the perturbed Gold function." Cryptography and Communications (2021): 1-17.
http://hdl.handle.net/10945/67565

Characters, Weil sums and c-differential uniformity with an application to the perturbed Gold function

Pantelimon Stănică [1]

Constanza Riera[2], Anton Tkachenko[2]

[1]Applied Mathematics Department,
Naval Postgraduate School, Monterey, USA; pstanica@nps.edu
[2]Department of Computer Science,
Electrical Engineering and Mathematical Sciences,
Western Norway University of Applied Sciences, 5020 Bergen, Norway;
{csr, atk}@hvl.no

September 17, 2020

Abstract

Building upon the observation that the newly defined [12] concept of c-differential uniformity is not invariant under EA or CCZ-equivalence [13], we showed in [22] that adding some appropriate linearized monomials increases the c-differential uniformity of the inverse function, significantly, for some c. We continue that investigation here. First, by analyzing the involved equations, we find bounds for the uniformity of the Gold function perturbed by a single monomial, exhibiting the discrepancy we previously observed on the inverse function. Secondly, to treat the general case of perturbations via any linearized polynomial, we use characters in the finite field to express all entries in the c-Differential Distribution Table (DDT) of an (n, n)-function on the finite field $\mathbb{F}_{p^n}$, and further, we use that method to find explicit expressions for all entries of the c-DDT of the perturbed Gold function (via an arbitrary linearized polynomial).

Keywords: Boolean and p-ary functions, c-differentials, differential uniformity, perfect and almost perfect c-nonlinearity, perturbations
MSC 2020: 06E30, 11T06, 94A60, 94C10.

1 Introduction and basic definitions

Motivated by the challenge of [3], who extended the differential attack on some ciphers by using a new type of differential, we defined in [12] a new differential and difference distribution table, in any characteristic, along with the corresponding perfect/almost perfect c-nonlinear functions, etc., (unbeknown to us, and developed independently, this is a generalization of the recent [1] concept of quasi planarity: a quasi planar function is simply a perfect c-nonlinear function for $c = -1$). We later extended the notion of boomerang connectivity table in [19] and characterized some of the known perfect nonlinear functions and the inverse function through this new concept. In [12, 13, 18, 24] various characterizations of the c-differential uniformity were found, and some of the known perfect and almost perfect nonlinear functions have been investigated. An approach on boomerang uniformity based upon Weil sums and characters was developed in [20]. We will take a similar approach in this paper on c-differential uniformity, which has the advantage of providing some character expressions for all entries in the c-Differential Distribution Table (defined below).

While we only introduce here only some needed notation on Boolean (binary, $p = 2$) and p-ary functions (where p is an odd prime), the reader can consult [4, 5, 6, 11, 17, 23] for more on cryptographic Boolean functions and their properties.

Let p be a prime number and n be a positive integer n. We let $\mathbb{F}_{p^n}$ be the finite field with p^n elements, and $\mathbb{F}_{p^n}^* = \mathbb{F}_{p^n} \setminus \{0\}$ be the multiplicative group; for $a \neq 0$, we often write $\frac{1}{a}$ to mean the inverse of a in the multiplicative group. We let $\mathbb{F}_p^n$ be the n-dimensional vector space over $\mathbb{F}_p$. We use $\#S, \bar{S}$ to denote the cardinality of a set S, respectively, the complement of S in a superset (usually, $\mathbb{F}_{p^n}$), which will be clear from the context. Also, for a complex number z, we denote by $\bar{z}$ its complex conjugate.

We call a function from $\mathbb{F}_{p^n}$ (or $\mathbb{F}_p^n$) to $\mathbb{F}_p$ a *p-ary function* on n variables. For positive integers n and m, any map $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ (or, $\mathbb{F}_p^n \to \mathbb{F}_p^m$) is called a *vectorial p-ary function*, or *(n, m)-function*. When $m = n$, F can be uniquely represented as a univariate polynomial over $\mathbb{F}_{p^n}$ of the form $F(x) = \sum_{i=0}^{p^n-1} a_i x^i$, $a_i \in \mathbb{F}_{p^n}$, whose *algebraic degree* is then the largest Hamming weight of the exponents i with $a_i \neq 0$. We let $\mathrm{Tr}_n : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be the absolute trace function, given by $\mathrm{Tr}_n(x) = \sum_{i=0}^{n-1} x^{p^i}$. Also, $\mathrm{Tr}_d(x) = \sum_{i=0}^{\frac{n}{d}-1} x^{p^{di}}$ is the relative trace from $\mathbb{F}_{p^n} \to \mathbb{F}_{p^d}$, where $d \,|\, n$.

For a p-ary (n, m)-function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$, and $c \in \mathbb{F}_{p^m}$, the (*multi-*

plicative) *c-derivative* of F with respect to $a \in \mathbb{F}_{p^n}$ is the function

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

For an (n,n)-function F, and $a, b \in \mathbb{F}_{p^n}$, we let the entries of the c-Difference Distribution Table (c-DDT) be defined by $_c\Delta_F(a,b) = \#\{x \in \mathbb{F}_{p^n} : F(x+a) - cF(x) = b\}$. We call the quantity

$$\delta_{F,c} = \max\{_c\Delta_F(a,b) \, : \, a, b \in \mathbb{F}_{p^n}, \text{ and } a \neq 0 \text{ if } c = 1\}$$

the *c-differential uniformity* of F. If $\delta_{F,c} = \delta$, then we say that F is differentially (c,δ)-uniform (or that F has c-uniformity δ). If $\delta = 1$, then F is called a *perfect c-nonlinear* (*PcN*) function (certainly, for $c = 1$, they only exist for odd characteristic p; however, as proven in [12], there exist PcN functions for $p = 2$, for all $c \neq 1$). If $\delta = 2$, then F is called an *almost perfect c-nonlinear* (*APcN*) function. When we need to specify the constant c for which the function is PcN or APcN, then we may use the notation c-PN, or c-APN. It is easy to see that if F is an (n,n)-function, that is, $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, then F is PcN if and only if $_cD_aF$ is a permutation polynomial. For $c = 1$, we recover the classical derivative, PN, APN, etc., differential uniformity and DDT.

The rest of the paper is organized as follows. Section 2 gives bounds for the c-differential uniformity for the Gold function perturbed by a single monomial. Section 3 gives a general theorem describing the entries of the c-DDT via characters in the finite field. Section 4 investigates c-DDT entries for a perturbation via an arbitrary linearized monomial of the Gold function, for p odd. Section 5 completes the investigation and does the same for p even. Section 7 concludes the paper.

2 Perturbations of the Gold function via a linearized monomial

We shall be using, throughout the paper, the following lemma.

Lemma 1 ([7, 12])**.** *Let p, t, n be integers greater than or equal to 1 (we take $t \leq n$, though the result can be shown in general). Let $d = \gcd(n,t), e =$*

$\gcd(n, 2t)$. *Then,*

$$\gcd(2^t + 1, 2^n - 1) = \frac{2^e - 1}{2^d - 1}, \text{ and if } p > 2, \text{ then,}$$
$$\gcd(p^t + 1, p^n - 1) = 2, \text{ if } \frac{n}{d} \text{ is odd,}$$
$$\gcd(p^t + 1, p^n - 1) = p^d + 1, \text{ if } \frac{n}{d} \text{ is even.}$$

We showed in [12] that the inverse function is PcN for $c = 0$, and it is 2 or 3 depending upon the parameter c (we found precisely those conditions). In [22] we showed that adding x^{2^d} to x^{2^n-2}, where d is the largest nontrivial divisor of n, increases the mentioned c-differential uniformity from 2 or 3 (for $c \neq 0, 1$) to $\geq 2^d + 2$ (in the case of the inverse function as used in the Advanced Encryption Function (AES) it is 18). This discrepancy is rather surprising and prompts an investigation into other well-behaved, under classical differential uniformity, vectorial functions.

In the result of this section we see that simply adding a linearized monomial to the Gold function increases significantly the maximum value in its c-differential spectrum size. In the following, we take p prime, $n \geq 4$ an integer, and $0 \leq t < n$ an integer such that $a^{p^k - p^t + 1} + 1$ has a root (and consequently, $\gcd(p^k - p^t + 1, p^n - 1)$ roots) in the field $\mathbb{F}_{p^n}$.

Theorem 2. *Let p be a prime number, $n \geq 4$, $F(x) = x^{p^k+1}$ be the Gold function on $\mathbb{F}_{p^n}$, and $1 \neq c \in \mathbb{F}_{p^n}$, $1 \leq k < n$ with $\gcd(k, n) = d \geq 1$ and $\frac{n}{\gcd(n,k)} \geq 3$. Then, the c-differential uniformity, $\delta_{G,c}$, of $G(x) = F(x) + x^{p^t}$ satisfies $\gcd(p^k - p^t + 1, p^n - 1) + 1 \leq \delta_{G,c} \leq \max\{p^k + 1, p^t\}$; if $G(x) = F(x) + x$, or $G(x) = F(x) + x^{p^k}$, then $p^{\gcd(n,k)} + 1 \leq \delta_{G,c} \leq p^k + 1$.*

Proof. Let $G(x) = x^{p^k+1} + x^{p^t}$. The c-differential uniformity equation for G for $c \in \mathbb{F}_{p^n}$ at $(a, b) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$ is

$$(x + a)^{p^k+1} + (x + a)^{p^t} - cx^{p^k+1} - cx^{p^t} = b. \tag{1}$$

If $a = 0$, the equation becomes

$$x^{p^k+1} + x^{p^t} - \frac{b}{1 - c} = 0.$$

Surely, if $b = 0$, then $x = 0$ and $x^{p^k - p^t + 1} + 1 = 0$. The latter equation (under our assumption) has $\gcd(p^k - p^t + 1, p^n - 1)$ solutions. However, if $b \neq 0$, the equation is not easy to handle, unless t has some special forms, which are dealt with below.

We continue with $G(x) = x^{p^k+1} + x$ and use the c-differential uniformity equation of G for $c \in \mathbb{F}_{p^n}$ at $(a, b) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$ from (1), which, when $t = 0$ becomes

$$(1-c)x^{p^k+1} + ax^{p^k} + (1 + a^{p^k} - c)x + a^{p^k+1} + a - b = 0. \tag{2}$$

Clearly, $\delta_{G,c} \leq p^k + 1$. We now find a lower bound. If $a = 0$, the equation becomes

$$x^{p^k+1} + x - \frac{b}{1-c} = 0.$$

If $b = 0$, then $x = 0$ and $x^{p^k} + 1 = 0$. The latter equation has a unique solution, since $\gcd(p^k, p^n - 1) = 1$. Thus, if $a = 0$, we have two solutions for (2). If $b \neq 0$, we use the transformation $x = \frac{b}{1-c}y$ and obtain

$$y^{p^k+1} - By + B = 0, \tag{3}$$

where $B = \left(\frac{1-c}{b}\right)^{p^k}$. We now use [2, Theorem 5.6]. We let $Q = p^{\gcd(n,k)}$, so $\mathbb{F}_Q = \mathbb{F}_{p^n} \cap \mathbb{F}_{p^k}$, $m = [\mathbb{F}_{p^n} : \mathbb{F}_Q] = \frac{n}{\gcd(n,k)}$. By [2, Theorem 5.6], we know that there are $\dfrac{Q^{m-1} - Q}{Q^2 - 1}$, $\dfrac{Q^{m-1} - 1}{Q^2 - 1}$, for m even, respectively odd, values of B such that Equation (3) has $Q + 1$ solutions. Let T be the set of all such B. For any $B \in T$, we let $b \neq 0$ be random and $c = 1 - b(B)^{p^{-k}}$. For such choices of parameters, we do get $p^{\gcd(n,k)} + 1$ solutions, and so, $\delta_{G,c} \geq p^{\gcd(n,k)} + 1$.

We next assume that $a \neq 0$ (while we do not need to consider this case to show our claim, we do treat it here, just to point out that the c-DDT may have other entries, not only on the first row, with large values). We now remove the coefficient of x^{p^k} with the transformation

$$x \mapsto \frac{ca^{p^k+1} - bc + b}{(1-c)\left(a^{p^k} - \left(\frac{a}{1-c}\right)^{p^k} + c\left(\frac{a}{1-c}\right)^{p^k} - c + 1\right)}x - \frac{a}{1-c}$$

and Equation (1) becomes (3), where now,

$$B = \frac{(a_1 - e^{p^k})^{p^k+1}}{(b_1 - ea_1)^{p^k}},\ e = \frac{a}{1-c}, a_1 = 1 + \frac{a^{p^k}}{1-c}, b_1 = \frac{a + a^{p^k+1} - b}{1-c}. \tag{4}$$

By [2, Theorem 5.6], again we have $p^{\gcd(n,k)} + 1$ solutions for (3), for B belonging to a set T of cardinality $|T| = \dfrac{Q^{m-1} - Q}{Q^2 - 1}$, $|T| = \dfrac{Q^{m-1} - 1}{Q^2 - 1}$, for

m even, respectively odd. Clearly, for a, b, c such that (4) holds (there is no need to check if their existence, since we know they do, from the first part of the proof), then again we have ${}_c\Delta_G(a,b) \geq p^{\gcd(n,k)} + 1$, and thus $\delta_{G,c} \geq p^{\gcd(n,k)} + 1$ for those values of c.

We next continue with $G(x) = x^{p^k+1} + x^{p^k}$. Equation (1) is now

$$x^{p^k+1} + \left(1 + \frac{a}{1-c}\right) x^{p^k} + \frac{a^{p^k}}{1-c}x + \frac{a^{p^k+1} + a^{p^k} - b}{1-c} = 0. \tag{5}$$

If $c = a + 1$, this equation is now

$$x^{p^k+1} - a^{p^k-1}x + \left(\frac{b}{a} - a^{p^k} - a^{p^k-1}\right) = 0,$$

which is equivalent to $x^{p^k+1} - Bx + B = 0$, where $B = \dfrac{a^{p^{2k}-1}}{\left(\frac{b}{a} - a^{p^k} - a^{p^k-1}\right)^{p^k}}$, and this equation can be treated via [2, Theorem 5.6], as well (observe that, regardless of what $B \neq 0$ is, we can always find a, b such that the previous identity holds: for example, we can take $b = a^{p^k}$, and so, $B = \frac{1}{(-1)^{p^k} a}$). If $c \neq a + 1$, as we did for the first claim, we remove the coefficient of x^{p^k} by using a transformation

$$x \mapsto \frac{ca^{p^k+1} - bc + b}{(1-c)\left(a^{p^k} - \left(\frac{a}{1-c} + 1\right)^{p^k} + c\left(\frac{a}{1-c} + 1\right)^{p^k}\right)}x - \frac{a}{1-c} - 1$$

and Equation (5) becomes $x^{p^k+1} - Bx + B = 0$, where

$$B = \frac{(a_1 - e^{p^k})^{p^k+1}}{(b_1 - ea_1)^{p^k}},\ e = 1 + \frac{a}{1-c}, a_1 = \frac{a^{p^k}}{1-c}, b_1 = \frac{a^{p^k+1} + a^{p^k} - b}{1-c}, \tag{6}$$

enabling us to use, yet again, [2, Theorem 5.6], to infer ${}_c\Delta_G(a,b) \geq p^{\gcd(n,k)} + 1$, and consequently, $\delta_{G,c} \geq p^{\gcd(n,k)} + 1$. The theorem is shown. □

3 Characters and c-differential uniformity

We showed in [20] a general theorem expressing the entries in the c-Boomerang Connectivity Table (for all $c \neq 0$) in terms of double Weil sums. There is no reason why that is not developed for the c-DDT, and we shall do that below. We first show a general theorem that gives *all* entries of the c-DDT for

any function in terms of characters of the corresponding finite field (we will also include $c = 1$ in our analysis, since the use of characters does not seem to be a method of choice for classical computation of the DDT). For the convenience of the reader, we will go through the proof, although it follows in general lines the characters computation for the entries of the boomerang connectivity table method of [20].

Let G be the Gauss' sum $G(\psi, \chi) = \sum_{z \in \mathbb{F}_q^*} \psi(z)\chi(z)$, where χ, ψ, are additive, respectively, multiplicative characters of $\mathbb{F}_q$, $q = p^n$. Below, we let $\chi_1(a) = \exp\left(\frac{2\pi i \mathrm{Tr}_n(a)}{p}\right)$ be the principal additive character, and $\psi_k\left(g^\ell\right) = \exp\left(\frac{2\pi i k\ell}{q-1}\right)$ be the k-th multiplicative character of $\mathbb{F}_q$, $0 \leq k \leq q-2$.

Theorem 3. *Let $F(x)$ be an arbitrary function on $\mathbb{F}_q$, $q = p^n$, p a prime number, and $c \in \mathbb{F}_q^*$. Then, the c-Differential Distribution Table entry at (a, b) is given by*

$$ {}_c\Delta_F(a,b) = 1 + \frac{1}{q} \sum_{\alpha \in \mathbb{F}_q^*} \chi_1(-b\alpha) \sum_{x \in \mathbb{F}_q} \chi_1\left(\alpha\left(F(x+a) - cF(x)\right)\right). $$

Proof. Recall that ${}_c\Delta_F(a,b)$ is the number of solutions in $\mathbb{F}_q$, $q = p^n$, for the equation

$$ F(x+a) - cF(x) = b. \tag{7} $$

As done in [20], we know that the number $\mathcal{N}(b)$ of of solutions $(x_1, \ldots, x_n) \in \mathbb{F}_q^n$, for $b \in \mathbb{F}_{p^m}$ fixed, of an equation $f(x_1, \ldots, x_n) = b$ is

$$ \begin{aligned} \mathcal{N}(b) &= \frac{1}{q} \sum_{x_1,\ldots,x_n \in \mathbb{F}_q} \sum_{\alpha \in \mathbb{F}_q} \chi_1\left(\alpha\left(f(x_1,\ldots,x_n) - b\right)\right) \\ &= \frac{1}{q} \sum_{x_1,\ldots,x_n \in \mathbb{F}_q} \sum_{\chi \in \widehat{\mathbb{F}_q}} \chi(f(x_1,\ldots,x_n))\overline{\chi(b)}, \end{aligned} $$

where $\widehat{\mathbb{F}_q}$ is the set of all additive characters of $\mathbb{F}_q$, and χ_1 is the principal additive character of $\mathbb{F}_q$. For our Equation (7), we see that the number of solutions for some a, b fixed is therefore

$$ \begin{aligned} \mathcal{N}_{a,b;c} &= \frac{1}{q} \sum_{x \in \mathbb{F}_q} \sum_{\alpha \in \mathbb{F}_q} \chi_1\left(\alpha\left(F(x+a) - cF(x) - b\right)\right) \\ &= \frac{1}{q} \sum_{\alpha \in \mathbb{F}_q} \chi_1(-b\alpha) \sum_{x \in \mathbb{F}_q} \chi_1\left(\alpha F(x+a)\right) \chi_1\left(-\alpha c F(x)\right). \end{aligned} $$

Splitting, based on $\alpha = 0$ and $\alpha \neq 0$, we write

$$
\begin{aligned}
{}_c\Delta_F(a,b) &= 1 + \frac{1}{q} \sum_{\alpha \in \mathbb{F}_q^*} \chi_1(-b\alpha) \sum_{x \in \mathbb{F}_q} \chi_1\left(\alpha F(x+a) - \alpha c F(x)\right) \\
&= 1 + \frac{1}{q} \sum_{\alpha \in \mathbb{F}_q^*} \chi_1(-b\alpha) U_\alpha,
\end{aligned}
$$

where $U_\alpha := \sum_{x \in \mathbb{F}_q} \chi_1\left(\alpha F(x+a) - \alpha c F(x)\right)$. □

Corollary 4. *For all $c \in \mathbb{F}_q$, if $a = 0$, then*

$$
U_\alpha = \sum_{x \in \mathbb{F}_q} \chi_1\left(\alpha(1-c)F(x)\right),
$$

and so,

$$
{}_c\Delta_F(0,b) = 1 + \frac{1}{q} \sum_{\alpha \in \mathbb{F}_q^*} \chi_1(-b\alpha) \sum_{x \in \mathbb{F}_q} \chi_1\left(\alpha(1-c)F(x)\right).
$$

4 Entries of the c-DDT for the perturbed Gold function via a linearized polynomial, p odd

We now take the particular case of the Gold function $F(x) = x^{p^k+1}$ on $\mathbb{F}_q$, $1 \leq k < n$, $q = p^n$, p prime, $n \geq 2$, perturbed by any linearized polynomial $P(x) = \sum_{i=0}^{n-1} a_i x^{p^i}$, that is, $G(x) = x^{p^k+1} + \sum_{i=0}^{n-1} a_i x^{p^i}$. We fix $c \in \mathbb{F}_q$ (for $c = 1$ many of the expressions will simplify significantly, since the term $(1-c)P(x)$ below will disappear) but we kept that case for completeness, since we do not believe there was ever a complete description for the DDT of the Gold function (surely, in this case, in terms of characters). For every $\alpha \in \mathbb{F}_q^*$, we let $A_\alpha = \alpha(1-c)$, $P^*(x) = \sum_{i=0}^{n-1} ((1-c)a_i)^{p^{n-i}} x^{p^{n-i}}$ be the linearized c-companion polynomial for P, and $B_\alpha = \sum_{i=0}^{n-1} (a_i')^{p^{n-i}}$, where $a_i' = \alpha(1-c)a_i = A_\alpha a_i$, for all $0 \neq i \neq k$, $a_0' = \alpha\left(a^{p^k} + (1-c)a_0\right) = A_\alpha a_0 + \alpha a^{p^k}$ and $a_k' = \alpha(a + (1-c)a_k) = A_\alpha a_k + \alpha a$.

We next expand

$$
G(x+a) - cG(x) = (1-c)x^{p^k+1} + a^{p^k}x + ax^{p^k} + (1-c)P(x) + a^{p^k+1} + P(a).
$$

Thus, using Theorem 3 and the fact that $\chi_1(y^p) = \chi_1(y)$, for all $y \in \mathbb{F}_q$, implying $\chi_1(a_i' x^{p^i}) = \chi_1((a_i')^{p^{n-i}} x)$, we get

$$
{}_c\Delta_G(a,b) = 1 + \frac{1}{q} \sum_{\alpha \in \mathbb{F}_q^*} \chi_1(-b\alpha) U_\alpha,
$$

where (we use the notation $P'(a) = P(a) + a^{p^k+1}$)

$$\begin{aligned}
U_\alpha &= \sum_{x\in\mathbb{F}_q} \chi_1\left(\alpha G(x+a) - \alpha c G(x)\right) \\
&= \sum_{x\in\mathbb{F}_q} \chi_1\left(\alpha\left((1-c)x^{p^k+1} + a^{p^k}x + ax^{p^k} + (1-c)P(x) + P'(a)\right)\right) \\
&= \chi_1(\alpha P'(a)) \sum_{x\in\mathbb{F}_q} \chi_1\left(\alpha(1-c)x^{p^k+1}\right)\chi_1\left(\alpha\left(ax^{p^k} + a^{p^k}x + (1-c)P(x)\right)\right) \\
&= \chi_1(\alpha P'(a)) \sum_{x\in\mathbb{F}_q} \chi_1\left(A_\alpha x^{p^k+1} + B_\alpha x\right).
\end{aligned}$$

Therefore,

$${}_c\Delta_G(a,b) = 1 + \frac{1}{q}\sum_{\alpha\in\mathbb{F}_q^*} \chi_1\left(\alpha(P'(a)-b)\right) \sum_{x\in\mathbb{F}_q} \chi_1\left(A_\alpha x^{p^k+1} + B_\alpha x\right).$$

For general c and a fixed, we now let $X_a \subseteq \mathbb{F}_q^*$ be defined by (the second formulation is obtained by raising the first one to the p^k power)

$$\begin{aligned}
X_a &= \left\{\alpha\in\mathbb{F}_q^* \,:\, \alpha a^{p^k} + \alpha^{p^{-k}} a^{p^{-k}} + P^*(\alpha) = 0\right\} \\
&= \left\{\alpha\in\mathbb{F}_q^* \,:\, \alpha^{p^k} a^{p^{2k}} + \alpha a + (P^*(\alpha))^{p^k} = 0\right\}.
\end{aligned} \tag{8}$$

(This is the set of α's such that $B_\alpha = 0$.)

Next, we let

$$\begin{aligned}
S_\alpha &= \sum_{x\in\mathbb{F}_q} \chi_1\left(A_\alpha x^{p^k+1} + B_\alpha x\right) \\
T_{a,b} &= \sum_{\alpha\in\mathbb{F}_q^*} \chi_1(\alpha(P'(a)-b)) S_\alpha.
\end{aligned}$$

With these notations, we thus obtain

$$\begin{aligned}
T_{a,b} &= \sum_{\alpha\in X_a} \chi_1(\alpha(P'(a)-b)) \sum_{x\in\mathbb{F}_q} \chi_1\left(A_\alpha x^{p^k+1}\right) \\
&\quad + \sum_{\alpha\in\bar{X}_a} \chi_1(\alpha(P'(a)-b)) \sum_{x\in\mathbb{F}_q} \chi_1\left(A_\alpha x^{p^k+1} + B_\alpha x\right) \\
&=: T_1 + T_2.
\end{aligned}$$

We let $\eta = \psi_{(q-1)/2}$ be the quadratic character of $\mathbb{F}_q$ and for some $A, B \in \mathbb{F}_q$, $1 \le k < n$, $d = \gcd(n,k)$, we let $\mathscr{S}_k(A,B) = \sum_{x\in\mathbb{F}_q} \chi_1\left(Ax^{p^k+1} + Bx\right)$. We now use [7, Theorem 1 and 2] (we simplify the original statement).

Theorem 5 ([7])**.** *Let $q = p^n$, $1 \le k < n, d = \gcd(n,k)$. The following statements hold*:

(1) *When $\frac{n}{d}$ is even ($n = 2m$), then*

$$\mathscr{S}_k(A,0) = \begin{cases} (-1)^{\frac{m}{d}}\, p^m & \text{if } A^{\frac{q-1}{p^d+1}} \neq (-1)^{\frac{m}{d}} \\ (-1)^{\frac{m}{d}+1}\, p^{m+d} & \text{if } A^{\frac{q-1}{p^d+1}} = (-1)^{\frac{m}{d}}. \end{cases}$$

(2) *When $\frac{n}{d}$ is odd, then*

$$\mathscr{S}_k(A,0) = \begin{cases} (-1)^{n-1}\sqrt{q}\,\eta(A) & \text{if } p \equiv 1 \pmod 4 \\ (-1)^{n-1}\imath^n\sqrt{q}\,\eta(A) & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Therefore, with $A = A_\alpha, B = B_\alpha = 0$ (c is fixed), and even $\frac{n}{d}$ (so, $n = 2m$), we obtain

$$\begin{aligned} T_1 = (-1)^{\frac{m}{d}} p^m \sum_{\substack{\alpha\in X_a \\ A_\alpha^{\frac{q-1}{p^d+1}} \neq (-1)^{\frac{m}{d}}}} & \chi_1(\alpha(P'(a)-b)) \\ + (-1)^{\frac{m}{d}+1}\, p^{m+d} \sum_{\substack{\alpha\in X_a \\ A_\alpha^{\frac{q-1}{p^d+1}} = (-1)^{\frac{m}{d}}}} & \chi_1(\alpha(P'(a)-b)). \end{aligned} \tag{9}$$

Observe that the equation $A_\alpha^{\frac{q-1}{p^d+1}} = (-1)^{\frac{m}{d}}$ is equivalent to $\alpha^{\frac{q-1}{p^d+1}} = (-1)^{\frac{m}{d}}(1-c)^{-\frac{q-1}{p^d+1}}$. With

$$\begin{aligned} W_a &= \left\{ \alpha \in X_a \,:\, A_\alpha^{\frac{q-1}{p^d+1}} \neq (-1)^{\frac{m}{d}} \right\} \\ \Sigma &= \sum_{\alpha\in X_a} \chi_1(\alpha(P'(a)-b)), \\ \Sigma_1 &= \sum_{\alpha\in X_a\setminus W_a} \chi_1(\alpha(P'(a)-b)), \end{aligned}$$

the sum (9) becomes (for even $\frac{n}{d}$)

$$\begin{aligned} T_1 &= (-1)^{\frac{m}{d}} p^m \left(\Sigma - \Sigma_1\right) + (-1)^{\frac{m}{d}+1} p^{m+d} \Sigma_1 \\ &= (-1)^{\frac{m}{d}} p^m \, \Sigma + (-1)^{\frac{m}{d}+1} p^m \, \Sigma_1 \left(p^d + 1\right). \end{aligned}$$

We now consider the case of odd $\frac{n}{d}$. Recall the definition of the Gauss sum

$$G(\psi, \chi) = \sum_{\alpha \in \mathbb{F}_q^*} \psi(\alpha)\chi(\alpha),$$

where ψ, χ are some multiplicative, respectively, additive characters of $\mathbb{F}_q$. We also define an incomplete Gauss sum on a set $U \subseteq \mathbb{F}_q^*$ to be $G_U(\psi, \chi) = \sum_{\alpha \in U} \psi(\alpha)\chi(\alpha)$.

Next, when $\frac{n}{d}$ is odd, c fixed, and $A = A_\alpha, B = B_\alpha = 0, \epsilon_p = 1$, if $p \equiv 1 \pmod 4$, respectively, $\epsilon_p = \imath^n$, if $p \equiv 3 \pmod 4$, then

$$\begin{aligned} T_1 &= (-1)^{n-1} \epsilon_p \sqrt{q} \, \eta(1-c) \sum_{\alpha \in X_a} \chi_1(\alpha(P'(a) - b)) \eta(\alpha) \\ &= (-1)^{n-1} \epsilon_p \sqrt{q} \, \eta(1-c) G_{X_a}(\eta, \chi_{P'(a)-b}). \end{aligned}$$

If $\alpha \in \bar{X}_a$ (so, $B_\alpha \neq 0$), we shall make use of the following result from [8] (we make slight changes in notations and combine various results).

Theorem 6 ([8])**.** *Let $q = p^n$, $n \geq 2$, p an odd prime, $1 \leq k < n$, $d = \gcd(n, k)$. Let $f(x) = A^{p^k} x^{p^{2k}} + Ax$, for some nonzero A. The following statements hold*:

(1) *If f is a permutation polynomial over $\mathbb{F}_q$, and x_0 is the unique element such that $f(x_0) = -B^{p^k}, B \neq 0$, then*:

(*i*) *If $\frac{n}{d}$ is odd, then*

$$\mathscr{S}_k(A, B) = \begin{cases} (-1)^{n-1} \sqrt{q} \, \eta(-A) \, \overline{\chi_1(A x_0^{p^k+1})} & \text{if } p \equiv 1 \pmod 4 \\ (-1)^{n-1} \imath^{3n} \sqrt{q} \, \eta(-A) \, \overline{\chi_1(A x_0^{p^k+1})} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

(the solution is $x_0 = -\frac{1}{2} \sum_{j=0}^{\frac{n}{d}-1} (-1)^j A^{-\frac{p^{(2j+1)k}+1}{p^k+1}} B^{p^{(2j+1)k}}$).

(*ii*) *If $\frac{n}{d}$ is even, then $n = 2m$, $A^{\frac{q-1}{p^d+1}} \neq (-1)^{\frac{m}{d}}$ and*

$$\mathscr{S}_k(A, B) = (-1)^{\frac{m}{d}} p^m \, \overline{\chi_1(A x_0^{p^k+1})}.$$

(2) *If f is not a permutation polynomial, then, for $B \neq 0$, $\mathscr{S}_k(A,B) = 0$, unless, $f(x) = -B^{p^k}$ has a solution x_0 (this can only happen if $\frac{n}{d}$ is even with $n = 2m$, and $A^{\frac{q-1}{p^d+1}} = (-1)^{\frac{m}{d}}$), in which case*

$$\mathscr{S}_k(A,B) = (-1)^{\frac{m}{d}+1} p^{m+d} \overline{\chi_1(A x_0^{p^k+1})}.$$

Let $A = A_\alpha = \alpha(1-c)$, $B = B_\alpha = \sum_{i=0}^{n-1} (a_i')^{p^{n-i}} \neq 0$ (so, $\alpha \in \bar{X}_a$), where $a_i' = A_\alpha a_i$, for all $0 \neq i \neq k$, $a_0' = \alpha a^{p^k} + A_\alpha a_0$, $a_k' = \alpha a + A_\alpha a_k$, and $L_\alpha(x) = A_\alpha^{p^k} x^{p^{2k}} + A_\alpha x$. It is known [25] that a linearized polynomial of the form $L(x) = x^{p^r} + \gamma x \in \mathbb{F}_{p^n}$ is a permutation polynomial (PP) if and only if $(-1)^{n/e} \gamma^{(p^n-1)/(p^e-1)} \neq 1$, where $e = \gcd(n,r)$. It follows that in our case, with $e = \gcd(n,2k)$, L_α is a PP if and only if

$$1 \neq (-1)^{\frac{n}{e}} A_\alpha^{(p^k-1)\frac{p^n-1}{p^e-1}}.$$

From Theorem 6, if $\frac{n}{d}$ is odd, $\alpha \in \bar{X}_a$ and L_α is a PP (that is, the above displayed condition holds), then (x_α is the solution to $L_\alpha(x) = B_\alpha^{p^k}$)

$$\begin{aligned} S_\alpha &= \sum_{x \in \mathbb{F}_q} \chi_1\left(A_\alpha x^{p^k+1} + B_\alpha\right) \\ &= (-1)^{n-1} \mu_p \sqrt{q}\, \eta(-A_\alpha)\, \overline{\chi_1(A_\alpha x_\alpha^{p^k+1})}, \end{aligned}$$

where $\mu_p = 1$, if $p \equiv 1 \pmod 4$, and $\mu_p = i^{3n}$, if $p \equiv 3 \pmod 4$. Recall the incomplete Gauss sum on a set $U \subseteq \mathbb{F}_q^*$, namely $G_U(\psi,\chi) = \sum_{\alpha \in U} \psi(\alpha)\chi(\alpha)$. Thus, when $\frac{n}{d}$ is odd and $V_a = \{\alpha \in \bar{X}_a : A_\alpha^{(p^k-1)\frac{p^n-1}{p^e-1}} \neq (-1)^{\frac{n}{e}}\}$, then, denoting by $T_2|_{V_a}$ the restriction function T_2 computed only on V_a, and using [16, Theorem 5.12 (i)] (with $\delta_\alpha = P'(a) - b - (1-c)x_\alpha^{p^k+1}$)

$$\begin{aligned} T_2|_{V_a} &= (-1)^{n-1} \mu_p \sqrt{q}\, \eta(c-1) \\ &\quad \times \sum_{x \in V_a} \eta(\alpha)\, \chi_1(\alpha(P'(a) - b - (1-c)x_\alpha^{p^k+1})) \\ &= (-1)^{n-1} \mu_p \sqrt{q}\, \eta(c-1) G_{V_a}(\eta, \chi_{\delta_\alpha}). \end{aligned}$$

Observe that when $\frac{n}{d}$ is odd, then $e = \gcd(n,2k) = \gcd(n,k) = d$ (this is equivalent to $2^\ell \| n$ and $2^\ell \| k$ for some integer ℓ, where $2^\ell \| n$ means that ℓ is the 2-valuation of n, that is the exact power of 2 dividing n), then,

$$A_\alpha^{(p^k-1)\frac{p^n-1}{p^e-1}} = \left(A_\alpha^{\frac{p^k-1}{p^e-1}}\right)^{p^n-1} = 1,$$

so, L_α is always a PP (observe that $\frac{n}{d}$ is odd). If that is the case ($2^\ell \| n$ and $2^\ell \| k$ for some integer ℓ), then,

$$T_2 = (-1)^{n-1}\mu_p\sqrt{q}\,\eta(c-1)G_{V_a}(\eta, \chi_{\delta_\alpha}).$$

We now consider the case of $\frac{n}{d}$ being even, so $e = 2d$. If L_α is a PP, and thus, $A_\alpha^{\frac{p^n-1}{p^d+1}} \neq (-1)^{\frac{n}{2d}}$, then ($x_\alpha$ is the solution to $L_\alpha(x) = B_\alpha^{p^k}$)

$$S_\alpha = (-1)^{\frac{m}{d}} p^m \chi_1\left(-A_\alpha x_\alpha^{p^k+1}\right),$$

and when L_α is not a PP (thus, $A_\alpha^{\frac{p^n-1}{p^d+1}} = (-1)^{\frac{n}{2d}}$), but a solution x_α exists to $L_\alpha(x) = B_\alpha^{p^k}$ – we will call this, condition $(\mathcal{P})$, then

$$S_\alpha = (-1)^{\frac{m}{d}+1} p^{m+d} \chi_1\left(-A_\alpha x_\alpha^{p^k+1}\right),$$

As before, we let $V_a = \left\{\alpha \in \bar{X}_a \,:\, A_\alpha^{\frac{p^n-1}{p^d+1}} \neq (-1)^{\frac{n}{2d}}\right\}$. Putting the previous results together, for even $\frac{n}{d}$, we get

$$\begin{aligned} T_2 = (-1)^{\frac{m}{d}} p^m \sum_{\alpha \in V_a} \chi_1\left(\alpha\left(P'(a) - b + (c-1)x_\alpha^{p^k+1}\right)\right) \\ + (-1)^{\frac{m}{d}+1} p^{m+d} \sum_{\substack{\alpha \in \bar{X}_a \setminus V_a \\ \alpha \text{ satisfies } (\mathcal{P})}} \chi_1\left(\alpha\left(P'(a) - b + (c-1)x_\alpha^{p^k+1}\right)\right). \end{aligned}$$

We thus have shown the following theorem. Let $P(x) = \sum_{i=0}^{n-1} a_i x^{p^i}$ be a linearized polynomial. Recall that for $1 \leq k < n$ and $c \in \mathbb{F}_q$, $\alpha \in \mathbb{F}_q^*$, $d = \gcd(n,k), e = \gcd(n,2k)$, we let $P'(a) = P(a) + a^{p^k+1}$, $A_\alpha = \alpha(1-c)$, $B_\alpha = \sum_{i=0}^{n-1}(a_i')^{p^{n-i}}$, where $a_i' = A_\alpha a_i$, for all $0 \neq i \neq k$, $a_0' = \alpha a^{p^k} + A_\alpha a_0$ and $a_k' = \alpha(a + (1-c)a_k)$. Further, for fixed $a \in \mathbb{F}_q$,

$$\begin{aligned} X_a &= \left\{\alpha \in \mathbb{F}_q^* \,:\, \alpha a^{p^k} + \alpha^{p^{-k}} a + P^*(\alpha) = 0\right\}, \\ V_a &= \left\{\alpha \in \bar{X}_a \,:\, A_\alpha^{\frac{p^n-1}{p^d+1}} \neq (-1)^{\frac{n}{2d}}\right\}, \\ W_a &= \left\{\alpha \in X_a \,:\, A_\alpha^{\frac{q-1}{p^d+1}} \neq (-1)^{\frac{n}{2d}}\right\}, \end{aligned}$$

$$\Sigma = \sum_{\alpha \in X_a} \chi_1(\alpha(P'(a) - b)),$$
$$\Sigma_1 = \sum_{\alpha \in X_a \setminus W_a} \chi_1(\alpha(P'(a) - b)).$$

We also define an incomplete Gauss sum on a set $U \subseteq \mathbb{F}_q^*$, namely, $G_U(\psi, \chi) = \sum_{\alpha \in U} \psi(\alpha)\chi(\alpha)$, and $\delta_\alpha = P'(a) - b - (1-c)x_\alpha^{p^k+1}$, where x_α is the solution of the equation $L_\alpha(x) = B_\alpha^{p^k}$ (we called this, condition $(\mathcal{P})$). Let also, $\mu_p = 1$, if $p \equiv 1 \pmod 4$, and $\mu_p = i^{3n}$, if $p \equiv 3 \pmod 4$.

Theorem 7. *Let $F(x) = x^{p^k+1}$ (p is an odd prime, $n \geq 2$, and $k < n$) be the Gold function, $P(x) = \sum_{i=0}^{n-1} a_i x^{p^i}$ be a linearized polynomial and $c \in \mathbb{F}_{p^n}$. Then, the c-Differential Distribution Table entries of $G(x) = F(x) + P(x)$ at $a, b \in \mathbb{F}_{p^n}$ are given by ${}_c\Delta_G(a,b) = 1 + p^{-n}T_{a,b}$, where:*

(i) Let $\frac{n}{d}$ be even, $n = 2m$. Then

$$T_{a,b} = (-1)^{\frac{m}{d}} p^m \Sigma + (-1)^{\frac{m}{d}+1} p^m \Sigma_1 \left(p^d - 1\right) + (-1)^{\frac{m}{d}} p^m \sum_{\alpha \in V_a} \chi_1(\alpha\delta_\alpha) + (-1)^{\frac{m}{d}+1} p^{m+d} \sum_{\substack{\alpha \in \bar{X}_a \setminus V_a \\ \alpha \text{ satisfies } (\mathcal{P})}} \chi_1(\alpha\delta_\alpha).$$

(ii) Let $\frac{n}{d}$ be odd. Then

$$T_{a,b} = (-1)^{n-1}\mu_p p^{\frac{n}{2}}\, \eta(1-c) G_{X_a}(\eta, \chi_{P'(a)-b}) + (-1)^{n-1}\mu_p p^{\frac{n}{2}}\, \eta(c-1) G_{V_a}(\eta, \chi_{\delta_\alpha}).$$

The following corollary is immediate.

Corollary 8. *With the notations of Theorem 7, we have:*

(i) If $\frac{n}{d}$ is even, then

$${}_c\Delta_G(a,b) \leq 1 + p^{-\frac{n}{2}}|X_a| + p^{-\frac{n}{2}}(p^d-1)|X_a \setminus W_a| + p^{-\frac{n}{2}}|V_a| + p^{-\frac{n}{2}+d}|\bar{X}_a \setminus V_a|.$$

(ii) If $\frac{n}{d}$ is even, then

$${}_c\Delta_G(a,b) \leq 1 + p^{-\frac{n}{2}}\left(|X_a| + |V_a|\right).$$

Remark 9. *We can bring more light into Equation* (8)*, if we were to consider it as an equation in* a*, not* α*. We know* [25] *that a linearized polynomial of the form* $L(x) = x^{p^r} + \gamma x \in \mathbb{F}_{p^n}$ *is a permutation polynomial if and only if the relative norm* $N_{\mathbb{F}_{p^n}/\mathbb{F}_{p^d}}(\gamma) \neq 1$*, that is,* $(-1)^{n/d}\gamma^{(p^n-1)/(p^d-1)} \neq 1$*, where* $d = \gcd(n, r)$*. In our case,* $r = 2k$ *and* $\gamma = \alpha^{1-p^k}$ *(the condition can be written in terms of* γ*, or* γ^{-1}*), and so, for fixed* $\alpha \neq 0$ *if* $\alpha^{p^k}x^{p^{2k}} + \alpha x$ *is a PP (that is,* $1 \neq (-1)^{\frac{n}{e}}\alpha^{\frac{p^n-1}{p^k+1}}$*), there is a unique root* a *of the above equation.*

We can also do the general case, when perhaps the previous linearized polynomial is not a PP, by using [10]*. With* $t = \frac{n}{\gcd(2k,n)}$*, and the notations of* [10]*, we let*

$$
\begin{aligned}
\alpha_{t-1} :&= (-\alpha^{1-p^k})^{1+p^{2k}+\cdots+p^{2k(t-1)}} = (-1)^t\alpha^{\frac{1-p^{2kt}}{p^k+1}},\\
\beta_{t-1} :&= \sum_{i=0}^{t-2}(-\alpha^{1-p^k})^{\sum_{j=i}^{t-2}p^{2k(j+1)}}\left(-\frac{P^*(\alpha)}{\alpha}\right)^{p^{2ki}} + \left(-\frac{P^*(\alpha)}{\alpha}\right)^{p^{2k(t-1)}}\\
&= \sum_{i=0}^{t-2}(-1)^{t-i}\alpha^{\frac{p^{2k(i+1)}-p^{2kt}}{p^k+1}}\left(\frac{P^*(\alpha)}{\alpha}\right)^{p^{2ki}} - \left(\frac{P^*(\alpha)}{\alpha}\right)^{p^{2k(t-1)}}\\
&= \sum_{i=0}^{t-2}(-1)^{t-i}\alpha^{\frac{p^{2k(i+1)}-p^{2kt}}{p^k+1}-p^{2ki}}(P^*(\alpha))^{p^{2ki}} - \left(\frac{P^*(\alpha)}{\alpha}\right)^{p^{2k(t-1)}}\\
&= \alpha^{\frac{-p^{2kt}}{p^k+1}}\sum_{i=0}^{t-2}(-1)^{t-i}\left(\alpha^{\frac{p^{2k}}{p^k+1}-1}P^*(\alpha)\right)^{p^{2ki}} - \left(\frac{P^*(\alpha)}{\alpha}\right)^{p^{2k(t-1)}}\\
&= (-1)^t\alpha^{\frac{-p^{2kt}}{p^k+1}}\sum_{i=0}^{t-1}(-1)^{i}\left(\alpha^{\frac{p^{2k}}{p^k+1}-1}P^*(\alpha)\right)^{p^{2ki}}.
\end{aligned}
$$

(*Though the final expressions are in* $\mathbb{F}_q$*, we regard the various terms in this last identity to belong in an extension of* $\mathbb{F}_q$*, otherwise a factor like* $\alpha^{\frac{p^{2k}}{p^k+1}-1}$ *makes little sense, for some* α*'s.*)

By [10]*, if* $\alpha_{t-1} = 1$ *and* $\beta_{t-1} \neq 0$*, there are no solutions* a *for Equation* (8)*; if* $\alpha_{t-1} = 1$ *and* $\beta_{t-1} = 0$*, there are* p^d *solutions; and, if* $\alpha_{t-1} \neq 1$*, there is one solution.*

5 Entries of the c-DDT for the perturbed Gold function via a linearized polynomial, p even

Here $q = 2^n$. We let as before $\mathscr{S}_k(A,B) = \sum_{x\in\mathbb{F}_q} \chi_1\left(Ax^{p^k+1} + Bx\right)$, and A_α, B_α defined as in the previous section. In this case, using [9], we have that, if $\frac{n}{d}$ is odd, where $d = \gcd(n,k)$,

$$\mathscr{S}_k(A_\alpha, B_\alpha) = \begin{cases} 0 & \text{if } \mathrm{Tr}_n(B_\alpha C_\alpha^{-1}) \neq 1 \\ \pm 2^{\frac{n+d}{2}} & \text{if } \mathrm{Tr}_n(B_\alpha C_\alpha^{-1}) = 1. \end{cases}$$

where C_α is the only element such that $C_\alpha^{2^k+1} = A_\alpha$ (by Lemma 1, $\gcd(2^k+1, 2^n-1) = 1$, when $\frac{n}{d}$ is odd).

In [9], combining Lemma 4.3 and Theorem 4.6, we see further that: $\mathscr{S}_k(1,1) = \left(\frac{2}{n/d}\right)^d 2^{\frac{n+d}{2}}$, where $\left(\frac{2}{s}\right)$ is the Jacobi symbol, and $\mathscr{S}_k(A,B) = \chi_1(\gamma^{2^k+1}+\gamma)\mathscr{S}_k(1,1)$, with $B_\alpha C_\alpha^{-1} = \gamma^{2^{2k}} + \gamma + 1$, for some $\gamma \in \mathbb{F}_q$. In conclusion, for $\frac{n}{d}$ odd, with C_α and γ as before, and denoting by $W = \left\{\alpha : \mathrm{Tr}_n(B_\alpha C_\alpha^{-1}) = 1\right\}$ and $\Sigma_2 = \sum_{\alpha\in W} \chi_1(\alpha(P'(a)-b) + \gamma^{2^k+1} + \gamma)$, then

$${}_c\Delta_G(a,b) = 1 + \left(\frac{2}{n/d}\right)^d 2^{\frac{d-n}{2}} \Sigma_2.$$

For $\frac{n}{d}$ even, we use Theorem 5.3 of [9], which we cite here for the convenience of the reader.

Theorem 10 ([9])**.** *Let $B \in \mathbb{F}_q^*$, $q = 2^n$, g be a primitive element of $\mathbb{F}_q$, and suppose that $\frac{n}{d}$ is even so that $n = 2m$ for some integer m. Let $f(x) = A^{2^k}x^{2^{2k}} + Ax$. The following statements hold*:

(i) If $A \neq g^{t(2^d+1)}$ for some integer t then f is a PP. Let $x_0 \in \mathbb{F}_q$ be the unique element satisfying $f(x_0) = B^{2^k}$. Then,

$$\mathscr{S}_k(A,B) = (-1)^{\frac{m}{d}} 2^m \chi_1\left(Ax_0^{2^k+1}\right).$$

(ii) If $A = g^{t(2^d+1)}$ for some integer t then $\mathscr{S}_k(A,B) = 0$ unless the equation $f(x) = B^{2^k}$ is solvable. If the equation is solvable, with solution x_0, say, then

$$\mathscr{S}_k(A,B) = \begin{cases} (-1)^{\frac{m}{d}+1} 2^{m+d} \chi_1\left(Ax_0^{2^k+1}\right) & \text{if } \mathrm{Tr}_d(A) = 0 \\ (-1)^{\frac{m}{d}} 2^m \chi_1\left(Ax_0^{2^k+1}\right) & \text{if } \mathrm{Tr}_d(A) = 0. \end{cases}$$

Then, if $\frac{n}{d}$ is even, so that $n = 2m$, and denoting by

$$Y = \{\alpha : A_\alpha \neq g^{t(2^d+1)}\},$$
$$Z_1 = \{\alpha : A_\alpha = g^{t(2^d+1)}, f(x) = B_\alpha^{2^k} \text{ is solvable, and } \mathrm{Tr}_d(A_\alpha) \neq 0\},$$
$$Z_2 = \{\alpha : A_\alpha = g^{t(2^d+1)}, f(x) = B_\alpha^{2^k} \text{ is solvable, and } \mathrm{Tr}_d(A_\alpha) = 0\},$$

then

$${}_c\Delta_G(a,b) = 1 + (-1)^{\frac{m}{d}} 2^{-m} \left(\sum_{Y \cup Z_1} \chi_1 \left(A_\alpha x_\alpha^{2^k+1} + \alpha(P'(a) - b) \right) \right.$$
$$\left. -2^d \sum_{Z_2} \chi_1 \left(A_\alpha x_\alpha^{2^k+1} + \alpha(P'(a) - b) \right) \right).$$

Denoting further, for any set U, by $\Sigma_U = \sum_U \chi_1 \left(A_\alpha x_\alpha^{2^k+1} + \alpha(P'(a) - b) \right)$, then

$${}_c\Delta_G(a,b) = 1 + (-1)^{\frac{m}{d}} 2^{-m} \left(\Sigma_{Y \cup Z_1} - 2^d \Sigma_{Z_2} \right).$$

We have then proven the following theorem (with the above notations).

Theorem 11. *Let $G(x) = x^{2^k+1} + P(x)$ be a perturbation of the Gold function on $\mathbb{F}_{2^n}$ (of primitive element g), where P is a linearized polynomial, and $d = \gcd(n,k)$. For each $\alpha \in \mathbb{F}_{2^n}^*$, we let $f_\alpha(x) = A_\alpha^{2^k} x^{2^{2k}} + A_\alpha x$, where A_α, B_α are defined in Section 4. Then, the c-Differential Distribution Table entries of $G(x)$ at $a, b \in \mathbb{F}_{2^n}$ are given by:*

(i) If $\frac{n}{d}$ is odd, $C_\alpha = A_\alpha^{\frac{1}{2^k+1}}$, $B_\alpha C_\alpha^{-1} = \gamma^{2^{2k}} + \gamma + 1$, for some $\gamma \in \mathbb{F}_{2^n}$, $W = \left\{\alpha : \mathrm{Tr}_n(B_\alpha C_\alpha^{-1}) = 1\right\}$ and $\Sigma_2 = \sum_{\alpha \in W} \chi_1 \left(\alpha \left(P'(a) - b \right) + \gamma^{2^k+1} + \gamma \right)$,

$${}_c\Delta_G(a,b) = 1 + \left(\frac{2}{n/d} \right)^d 2^{\frac{d-n}{2}} \Sigma_2,$$

where $\left(\frac{2}{s}\right)$ is the Jacobi symbol.

(ii) If $\frac{n}{d}$ is even, so that $n = 2m$, and denoting by $Y = \left\{\alpha : A_\alpha \neq g^{t(2^d+1)}\right\}$, $Z_1 = \left\{\alpha : A_\alpha = g^{t(2^d+1)}, \mathrm{Tr}_d(A_\alpha) \neq 0, f_\alpha(x) = B_\alpha^{2^k} \text{ is solvable}\right\}$, $Z_2 = \left\{\alpha : A_\alpha = g^{t(2^d+1)}, \mathrm{Tr}_d(A_\alpha) = 0, f_\alpha(x) = B_\alpha^{2^k} \text{ is solvable}\right\}$, and, for any set U, letting $\Sigma_U = \sum_U \chi_1 \left(A_\alpha x_\alpha^{2^k+1} + \alpha(P'(a) - b) \right)$,

$${}_c\Delta_G(a,b) = 1 + (-1)^{\frac{m}{d}} 2^{-m} \left(\Sigma_{Y \cup Z_1} - 2^d \Sigma_{Z_2} \right).$$

The following corollary is immediate.

Corollary 12. *With the notations of Theorem* 11*, we have*:

(*i*) *If* $\frac{n}{d}$ *is even, then*

$$ {}_c\Delta_G(a,b) \leq 1 + 2^{\frac{d-n}{2}} \left|\left\{\alpha : \mathrm{Tr}_n(B_\alpha C_\alpha^{-1}) = 1\right\}\right|.$$

(*ii*) *If* $\frac{n}{d}$ *is even, then*

$$ {}_c\Delta_G(a,b) \leq 1 + 2^{-\frac{n}{2}} \left(|Y \cup Z_1| + 2^d |Z_2|\right).$$

6 Computational results

In this section, we give the maximal c-differential uniformity over $\mathbb{F}_{2^n}$ for the concrete Gold perturbation $G(x) = x^{2^k+1} + x^{2^i} + x^{2^j}$, for $2 \leq n \leq 6$, and all $0 \leq i < j < n$, $1 \leq k < n$. We will also include (for comparison purposes) the c-differential uniformity (cDU) for the Gold function under the row 00 (in [18], the c-differential uniformity of the Gold function is completely described when $\gcd(n,k) = 1$ and also when $\gcd(n,k) > 1$, under some technical conditions). We shall denote by $\beta_G = \max_{c \neq 1} {}_c\beta_G$. For $n = 2$, $\beta_G = 3$, which the same as for the Gold function. From the tables below we see that the c-differential uniformity of the perturbation fluctuates, in some instances being three times as much, e.g, $n = 6, k = 1, (i,j) = (3,4)$. Furthermore, there are cases when it does decrease, e.g, $n = 6, k = 3, (i,j) = (2,3)$.

(i,j)	$k=1$	$k=2$
(0,0)	3	3
(0,1)	3	4
(0,2)	4	3
(1,2)	4	4

Table 1: Maximal c-differential uniformity β_G, for $n = 3$

7 Concluding remarks

In this paper we first show that a perturbation (it is known [13] that the c-differential uniformity is not invariant under EA or CCZ equivalence) of the Gold function via a linearized monomial has the property that its c-differential uniformity spectrum tends to increase significantly for some c.

(i,j)	$k=1$	$k=2$	$k=3$
(0,0)	3	5	3
(0,1)	3	5	4
(0,2)	4	5	6
(0,3)	6	5	3
(1,2)	4	5	5
(1,3)	6	5	4
(2,3)	5	5	6

Table 2: Maximal c-differential uniformity β_G, for $n = 4$

(i,j)	$k=1$	$k=2$	$k=3$	$k=4$
(0,0)	3	3	3	3
(0,1)	3	5	5	4
(0,2)	4	3	6	6
(0,3)	6	5	3	6
(0,4)	6	6	5	3
(1,2)	4	5	6	7
(1,3)	6	7	5	6
(1,4)	6	6	7	4
(2,3)	7	5	6	5
(2,4)	6	6	6	6
(3,4)	5	6	5	6

Table 3: Maximal c-differential uniformity β_G, for $n = 5$

(i,j)	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$
(0,0)	3	5	9	5	3
(0,1)	3	5	9	5	4
(0,2)	4	5	6	5	7
(0,3)	7	5	9	10	7
(0,4)	7	5	9	5	6
(0,5)	6	10	6	5	3
(1,2)	4	5	8	7	6
(1,3)	7	8	9	5	6
(1,4)	7	6	15	5	8
(1,5)	6	10	6	8	4
(2,3)	6	5	6	10	9
(2,4)	6	5	6	5	7
(2,5)	8	10	13	6	7
(3,4)	9	7	9	10	7
(3,5)	7	5	6	10	7
(4,5)	7	10	8	5	6

Table 4: Maximal c-differential uniformity β_G, for $n = 6$

We further propose a new approach for the computation of the c-DDT entries and the c-differential uniformity via characters in the finite field. We then apply our method for the Gold function perturbed by any linearized polynomial. It is the first such investigation providing exact expressions for the full c-DDT table (albeit, in terms of characters on the finite field). We provide detailed computations for the c-differential uniformity of a perturbation of the Gold function via linearized binomials, for small dimensions. We further propose here that one could look at perturbations of other PN/APN functions under EA-transformations and investigate their c-differential uniformity.

References

[1] D. Bartoli, M. Timpanella, *On a generalization of planar functions*, J. Algebr. Comb.(2019), https://doi.org/10.1007/s10801-019-00899-2.

[2] A. W. Bluher, *On* $x^{q+1} + ax + b$, Finite Fields Appl. 10 (3) (2004), 285–305.

[3] N. Borisov, M. Chew, R. Johnson, D. Wagner, *Multiplicative Differentials*, In: Daemen J., Rijmen V. (eds.), Fast Software Encryption, FSE 2002, LNCS 2365, pp. 17–33, Springer, Berlin, Heidelberg, 2002.

[4] L. Budaghyan, Construction and Analysis of Cryptographic Functions, Springer-Verlag, 2014.

[5] C. Carlet, *Boolean functions for cryptography and error correcting codes*, In: Y. Crama, P. Hammer (eds.), Boolean Methods and Models, Cambridge Univ. Press, Cambridge, pp. 257–397, 2010.

[6] C. Carlet, *Vectorial Boolean Functions for Cryptography*, In: Y. Crama, P. Hammer (eds.), Boolean Methods and Models, Cambridge Univ. Press, Cambridge, pp. 398–472, 2010.

[7] R. S. Coulter, *Explicit evaluations of some Weil sums*, Acta Arithmetica 83 (1998), 241–251.

[8] R. S. Coulter, *Further evaluations of Weil sums*, Acta Arithmetica 86 (1998), 217–226.

[9] R. S. Coulter, *On the evaluation of a class of Weil sums in characteristic* 2, New Zealand J. Math. 28 (1999), 171–184.

[10] R. S. Coulter, M. Henderson, *A note on the roots of trinomials over a finite field*, Bull. Austral. Math. Soc. 69 (2004), 429–432.

[11] T. W. Cusick, P. Stănică, Cryptographic Boolean Functions and Applications (Ed. 2), Academic Press, San Diego, CA, 2017.

[12] P. Ellingsen, P. Felke, C. Riera, P. Stănică, A. Tkachenko, *C-differentials, multiplicative uniformity and (almost) perfect c-nonlinearity*, IEEE Trans. Inf. Theory, 2020, https://doi.org/10.1109/TIT.2020.2971988.

[13] S.U. Hasan, M. Pal, C. Riera, P. Stănică, *On the c-differential uniformity of certain maps over finite fields*, https://arxiv.org/abs/2004.09436, 2020.

[14] P. A. Leonard, K. S. Williams, *Quartics over $GF(2^n)$*, Proc. AMS 36:2 (1972), 347–350.

[15] K. Li, L. Qu, B. Sun, C. Li, *New results about the boomerang uniformity of permutation polynomials*, IEEE Trans. Inf. Theory 65(11) (2019), 7542–7553.

[16] R. Lidl, H. Niederreiter, FiniteFields (Ed. 2), Encycl. Math. Appl., vol.20, Cambridge Univ. Press, Cambridge, 1997.

[17] S. Mesnager, Bent functions: fundamentals and results, Springer Verlag, 2016.

[18] C. Riera, P. Stănică, *Investigations on c-(almost) perfect nonlinear functions*, https://arxiv.org/abs/2004.02245, 2020.

[19] P. Stănică, *Investigations on c-boomerang uniformity and perfect nonlinearity*, https://arxiv.org/abs/2004.11859, 2020.

[20] P. Stănică, *Using double Weil sums in finding the Boomerang and the c-Boomerang Connectivity Table for monomial functions on finite fields*, https://arxiv.org/abs/2007.09553, 2020.

[21] P. Stănică, *Using double Weil sums in finding the Boomerang and the c-Boomerang Connectivity Table for monomial functions on finite fields*, https://arxiv.org/abs/2007.09553, 2020.

[22] P. Stănică, A. Geary, *The c-differential behavior of the inverse function under the EA-equivalence*, https://arxiv.org/abs/2006.00355.

[23] N. Tokareva, Bent Functions, Results and Applications to Cryptography, Academic Press, San Diego, CA, 2015.

[24] H. Yan, S. Mesnager, Z. Zhou, *Power Functions over Finite Fields with Low c-Differential Uniformity*, `https://arxiv.org/pdf/2003.13019.pdf`.

[25] Y. Zheng, Q. Wang, W. Wei, *On Inverses of Permutation Polynomials of Small Degree Over Finite Fields*, IEEE Trans. Inf. Theory 66:2 (2020), 914–922.