Low c-Differential Uniformity for the Gold Function Modified on a Subfield

Pantelimon Stănică

1 Introduction and Basic Definitions

In [10], we defined a multiplier differential and difference distribution table (in any characteristic). There seems to be quite a bit of interest in this new notion, as it opens the possibility for a modification of the differential attack. Using this concept, we extended the notion of the Boomerang Connectivity Table in [22]. In this paper, we investigate the c-differential uniformity for the Gold function, modified on a subfield.

As customary, n is a positive integer, p is a prime number, $\mathbb{F}_{p^n}$ is the finite field with p^n elements, and $\mathbb{F}_{p^n}^* = \mathbb{F}_{p^n} \setminus \{0\}$ is the multiplicative group (for $a \neq 0$, $\frac{1}{a}$ means the inverse of a in the multiplicative group of the corresponding finite field). We let $\mathbb{F}_p^n$ be the n-dimensional vector space over $\mathbb{F}_p$. We use $\#S$ to denote the cardinality of a set S and $\bar{z}$, for the 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 $\mathbb{F}_{p^n}$ (using some identification, via a basis, of the finite field with the vector space) 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 $a_i \neq 0$.

Given a p-ary function f, the derivative of f with respect to $a \in \mathbb{F}_{p^n}$ is the p-ary function $D_a f(x) = f(x + a) - f(x)$, for all $x \in \mathbb{F}_{p^n}$, which can be naturally extended to vectorial p-ary functions.

The next concept can be defined for general (n, m)-functions, though in this paper we only consider $m = n$. For an (n, n)-function F, and $a, b \in \mathbb{F}_{p^n}$, we let $\Delta_F(a, b) = \#\{x \in \mathbb{F}_{p^n} : F(x + a) - F(x) = b\}$. We call the quantity $\delta_F = \max\{\Delta_F(a, b) : a, b \in \mathbb{F}_{p^n}, a \neq 0\}$ the *differential uniformity* of F. If $\delta_F = \delta$, then

P. Stănică (✉)
Applied Mathematics Department, Naval Postgraduate School, Monterey, USA
e-mail: pstanica@nps.edu

P. Stănică et al. (eds.), *Security and Privacy*, Lecture Notes in Electrical Engineering 744,
https://doi.org/10.1007/978-981-33-6781-4_11

we say that F is differentially δ-uniform. If $\delta = 1$, then F is called a *perfect nonlinear* (*PN*) function, or *planar* function. If $\delta = 2$, then F is called an *almost perfect nonlinear* (*APN*) function. It is well known that PN functions do not exist if $p = 2$.

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

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

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

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

the *c-differential uniformity* of F (see [2] for a particular case). If $\delta_{F,c} = \delta$, then we say that F is differentially (c, δ)-uniform (or that F has c-uniformity δ, or for short, *F is δ-uniform c-DDT*). 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 [10], 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. 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.

This concept has been picked up quickly by the community and a flurry of papers started appearing [1, 17, 21–24, 27–29]. It is the purpose of this paper to investigate the c-differential uniformity for a subfield-modified (concept defined below) Gold function in the binary case. These affine modifications are occurring in many papers (see [12–14, 18–20, 26, 30], to cite just a few works).

The reader can consult [4–6, 8, 16, 25] for more on Boolean and p-ary (p is an odd prime) functions beyond what we have introduce here.

We will only consider the $p = 2$ case in this note. Given $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, and a divisor of n, say $s \,|\, n$, a fixed $t \in \mathbb{F}_{2^s}$, we let G be the $\mathbb{F}_{2^s}$-modification of F defined by

$$ G(x) = F(x) + t\left(x^{2^s} + x\right)^{2^n-1} + t = \begin{cases} F(x) + t & \text{if } x \in \mathbb{F}_{2^s} \\ F(x) & \text{if } x \notin \mathbb{F}_{2^s}. \end{cases} $$

In this paper, we consider the $\mathbb{F}_{2^s}$-modification of the Gold function only, so, $G(x) = x^{2^k+1} + t\left(x^{2^s} + x\right)^{2^n-1} + t$, $1 \leq k < n$, $\gcd(k, n) = 1$, $s \,|\, n$, $t \in \mathbb{F}_{2^s}$.

2 The c-Differential Uniformity of the Subfield Modified Gold Function

We will now state and prove our result for the c-differential uniformity of the binary $\mathbb{F}_{2^s}$-modification of the Gold function $F(x) = x^{2^k+1}$, $\gcd(n, k) = 1$, which is known to be APN under $\gcd(n, k) = 1$ (it is differentially 4-uniformity when $n \equiv 2 \pmod 4$ and $\gcd(n, k) = 2$).

Theorem *Let $G(x) = x^{2^k+1} + t\left(x^{2^s} + x\right)^{2^n-1} + t$ be the $\mathbb{F}_{2^s}$-modification of the Gold function, $1 \le k < n$, $\gcd(k, n) = 1$, $s \mid n$, $t \in \mathbb{F}_{2^s}$. Then, for $c \neq 1$, the c-differential uniformity of G is $\delta_{G,c} \le 9$.* □

Proof There is no need to consider $c = 0$ for the c-differential uniformity, since we can easily show that G is a permutation, and we argue that below. We assume that $G(x_1) = G(x_2)$, for some $x_1, x_2 \in \mathbb{F}_{2^n}$. If both $x_1, x_2 \notin \mathbb{F}_{2^s}$, then we get $x_1^{2^k+1} + t = x_2^{2^k+1} + t$, implying that $x_1 = x_2$ from the invertibility of F. If $x_1 \in \mathbb{F}_{2^s}$, $x_2 \in \mathbb{F}_{2^n}$, then $x_2^{2^k+1} = x_1^{2^k+1} + t \in \mathbb{F}_{2^s}$, implying that $x_2 \in \mathbb{F}_{2^s}$, as well, which is a contradiction. If none of x_1, x_2 are in $\mathbb{F}_{2^s}$, then again $x_1^{2^k+1} = x_2^{2^k+1}$, implying that $x_1 = x_2$.

From here on, we assume that $c \neq 0, 1$. The c-differential equation $G(x + a) - cG(x) = b$ of G at $a, b \in \mathbb{F}_{2^n}$ is

$$(x+a)^{2^k+1} + t\left((x+a)^{2^s} + (x+a)\right)^{2^n-1} + t + cx^{2^k+1} + ct\left(x^{2^s} + x\right)^{2^n-1} + ct = b,$$

which is equivalent to

$$(1+c)x^{2^k+1} + ax^{2^k} + a^{2^k}x + t\left(x^{2^s} + x + a^{2^s} + a\right)^{2^n-1} + ct\left(x^{2^s} + x\right)^{2^n-1} + a^{2^k+1} + t(1+c) + b = 0.$$

Case 1. Let $a \in \mathbb{F}_{2^s}$, $x \in \mathbb{F}_{2^s}$. By expanding the first term, the above equation transforms into

$$(1+c)x^{2^k+1} + x^{2^k}a + a^{2^k}x + a^{2^k+1} + t(1+c)\left(x^{2^s} + x\right)^{2^n-1} + t(1+c) + b = 0.$$

Since $x \in \mathbb{F}_{2^s}$, the equation becomes (when divided by a^{2^k+1} and by relabeling $\frac{x}{a} \mapsto x$)

$$x^{2^k+1} + \frac{1}{1+c}x^{2^k} + \frac{1}{1+c}x + d = 0, \qquad (1)$$

where $d = \frac{a^{2^k+1}+t(1+c)+b}{(1+c)a^{2^k+1}}$. If $d = 0$, then $x = 0$ is a solution. The cofactor, with the relabeling $\frac{1}{x} \mapsto x$, becomes

$$x^{2^k} + x + (c+1) = 0.$$

We now need to investigate the number of solutions of this linearized polynomial. We rewrite (simplifying some parameters) a result from [7, 15]. Let $f(z) = z^{p^k} - Az - B$ in $\mathbb{F}_{p^n}$, $g = \gcd(n,k)$, $m = n/\gcd(n,k)$, and $\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_{p^g}}$ be the relative trace from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^g}$. For $0 \le i \le m-1$, we define $t_i = \frac{p^{nm}-p^{n(i+1)}}{p^n-1}$, $\alpha_0 = A$, $\beta_0 = B$. If $m > 1$, then, for $1 \le r \le m-1$, we let $\alpha_r = A^{\frac{p^{k(r+1)}-1}{p^k-1}}$ and $\beta_r = \sum_{i=0}^{r} A^{s_i} B^{p^{ki}}$, where $s_i = \frac{p^{k(r+1)}-p^{k(i+1)}}{p^k-1}$, for $0 \le i \le r-1$ and $s_r = 0$. The trinomial f has no roots in $\mathbb{F}_{p^n}$ if and only if $\alpha_{m-1} = 1$ and $\beta_{m-1} \ne 0$. If $\alpha_{m-1} \ne 1$, then it has a unique root, namely $x = \beta_{m-1}/(1-\alpha_{m-1})$, and, if $\alpha_{m-1} = 1$, $\beta_{m-1} = 0$, it has p^g roots in $\mathbb{F}_{p^n}$ given by $x + \delta\tau$, where $\delta \in \mathbb{F}_{p^g}$, τ is fixed in $\mathbb{F}_{p^n}$ with $\tau^{p^k-1} = a$ (that is, a (p^k-1)-root of a), and, for any $e \in \mathbb{F}_{p^n}^*$ with $\mathrm{Tr}_g(e) \ne 0$, then $x = \dfrac{1}{\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_{p^g}}(e)} \displaystyle\sum_{i=0}^{m-1} \left(\sum_{j=0}^{i} e^{p^{kj}} \right) A^{t_i} B^{p^{ki}}$.

For our prior case, $p = 2$, $A = 1$, $B = c+1$, $m = n$, $g = 1$, and so, $\alpha_{n-1} = 1$, $\beta_{n-1} = \sum_{i=0}^{n-1} (c+1)^{2^{ki}}$. Thus, if $\beta_{n-1} \ne 0$, we have no roots, and if $\beta_{n-1} = 0$, we have 3 roots (we added the previous 0 root to the count). We make the observation that these roots can belong to $\mathbb{F}_{2^s}$ if we force $c \in \mathbb{F}_{2^s}$, and we take $e \in \mathbb{F}_{2^s}$ in the formula above.

If $d \ne 0$, taking $y = x + (c+1)^{-1}$ we obtain

$$y^{2^k+1} + \frac{1}{1+c}\left(1 + \frac{1}{(1+c)^{2^k-1}}\right) y + d + \frac{1}{(c+1)^2} = 0.$$

Now, let $y = \alpha z$, where $\alpha = \left(\frac{1}{1+c} + \frac{1}{(1+c)^{2^k}}\right)^{2^{-k}} = 1 + \frac{1}{(1+c)^{2^{-k}}}$ (the 2^k-root exists since $\gcd(2^k, 2^n-1) = 1$). The previous equation becomes

$$z^{2^k+1} + z + \beta = 0, \tag{2}$$

where $\beta = \dfrac{d(1+c)^2+1}{\alpha^{2^k+1}(1+c)^2} = \dfrac{ca^{2^k+1} + t(1+c)^2 + b(1+c)}{a^{2^k+1}\alpha^{2^k+1}(1+c)^2}$. Assuming $\beta \ne 0$, we will be using some results of [11] (see also [3, 9]), under $\gcd(n,k) = 1$. By [11] [Theorem 1], we know that Eq. (2) has either none, one or three solutions in $\mathbb{F}_{2^n}$. In fact, the distribution of these cases for n odd (respectively, n even) is (denoting by M_ℓ the amount of equations of type (2) with ℓ solutions)

$$M_0 = \frac{2^n+1}{3},\ M_1 = 2^{n-1}-1,\ M_3 = \frac{2^{n-1}-1}{3},\ \text{for } n \text{ odd},$$
$$M_0 = \frac{2^n-1}{3},\ M_1 = 2^{n-1},\ M_3 = \frac{2^{n-1}-2}{3},\ \text{for } n \text{ even}.$$

Then, for $n \geq 3$, $c \neq 0, 1$, and $\gcd(n, k) = 1$, and since β is linear on b, this implies that, for any β and any a, c, we can find b such that $\beta = \dfrac{ca^{2^k+1} + b(1-c)}{\alpha^{2^k+1}(1-c)^2}$, so the maximum (attainable, if they happen to be in $\mathbb{F}_{2^s}$) number of solutions for (1) in this case is 3.

Case 2. Let $a \in \mathbb{F}_{2^s}$, $x \notin \mathbb{F}_{2^s}$. Then our equation becomes (when divided by a^{2^k+1} and relabeling $\frac{x}{a} \mapsto x$)

$$x^{2^k+1} + \frac{1}{1+c}x^{2^k} + \frac{1}{1+c}x + \frac{a^{2^k+1}+b}{(1+c)a^{2^k+1}} = 0. \quad (3)$$

Arguing as above we get that the maximum number of solutions is, yet again, 3, if $b \neq a^{2^k+1}$.

Case 3. Let $a \notin \mathbb{F}_{2^s}$, $x \in \mathbb{F}_{2^s}$. As in the first case, by expanding the first term, the above equation transforms into

$$(1+c)x^{2^k+1} + ax^{2^k} + a^{2^k}x + a^{2^k+1} + tc + b = 0,$$

which, as before, is equivalent to

$$x^{2^k+1} + \frac{1}{1+c}x^{2^k} + \frac{1}{1+c}x + d = 0,$$

with $d = \frac{a^{2^k+1}+tc+b}{(c+1)a^{2^k+1}}$. A similar analysis as in the prior case renders a maximum of 3 solutions.

Case 4. Let $a \notin \mathbb{F}_{2^s}$, $x \notin \mathbb{F}_{2^s}$, and $x + a \in \mathbb{F}_{2^s}$. The c-differential equation of G becomes

$$(1+c)x^{2^k+1} + ax^{2^k} + a^{2^k}x + a^{2^k+1} + t + b = 0,$$

which resembles the prior equations, and so, by appropriate substitutions and arguing similarly, we infer that it has a maximum of 3 solutions.

Case 5. Let $a \notin \mathbb{F}_{2^s}$, $x \notin \mathbb{F}_{2^s}$, and $x + a \notin \mathbb{F}_{2^s}$. The relevant equation is then

$$(1+c)x^{2^k+1} + ax^{2^k} + a^{2^k}x + a^{2^k+1} + b = 0,$$

which, as we got used by now, renders a maximum of 3 solutions. The theorem is shown. □

3 Concluding Remarks

In this paper, we find the c-differential uniformity of the $\mathbb{F}_{2^s}$-modification of the Gold function on $\mathbb{F}_{2^n}$, $s \mid n$, and show that its c-differential uniformity is less than or equal to 9. As we saw already, investigating questions on c-differential uniformity by this method is not a simple matter, mostly because the obtained equations need to be solved over finite fields and not many techniques have been developed for that purpose. In spite of that, it would be interesting to find other classical PN/APN functions and study their properties through the new differential. It will also be worthwhile to check into the general p-ary versions of the results from this paper, as well as other modifications of the Gold, the inverse, or other PN/APN functions.

References

1. Bartoli D, Calderini M, On construction and (non)existence of c-(almost) perfect nonlinear functions. https://arxiv.org/abs/2008.03953
2. Bartoli D, Timpanella M (2020) On a generalization of planar functions. J. Algebr Comb 52:187–213
3. Bluher AW (2004) On $x^{q+1} + ax + b$. Finite Fields Appl 10(3):285–305
4. Budaghyan L (2014) Construction and analysis of cryptographic functions. Springer
5. Carlet C (2010) Boolean functions for cryptography and error correcting codes. In: Crama Y, Hammer P (eds) Boolean methods and models. Cambridge University Press, Cambridge, pp 257–397
6. Carlet C (2010) Vectorial Boolean functions for cryptography. In: Crama Y, Hammer P (eds) Boolean methods and models. Cambridge University Press, Cambridge, pp 398–472
7. Coulter RS, Henderson M (2004) A note on the roots of trinomials over a finite field. Bull Austral Math Soc 69:429–432
8. Cusick TW, Stănică P (2017) Cryptographic Boolean functions and applications, 2nd edn. Academic Press, San Diego, CA
9. Dobbertin H, Felke P, Helleseth T, Rosendahl P (2006) Niho type cross-correlation functions via Dickson polynomials and Kloosterman sums. IEEE Trans Inf Theory 52(2):613–627
10. Ellingsen P, Felke P, Stănică CRP, Tkachenko A (2020) C-differentials, multiplicative uniformity and (almost) perfect c-nonlinearity. IEEE Trans Inf Theory 66(9):5781–5789
11. Helleseth T, Kholosha A (2008) On the equation $x^{2^\ell+1} + x + a = 0$ over $GF(2^k)$. Finite Fields Appl 14:159–176
12. Kaleyski NS (2019) Changing APN functions at two points. Cryptogr Commun 11(6):1165–1184
13. Li K, Qu L, Sun B, Li C (2019) New results about the boomerang uniformity of permutation polynomials. IEEE Trans Inf Theory 65(11):7542–7553
14. Li Y, Wang M, Yu Y, Constructing differentially 4-uniform permutations over $GF(2^{2k})$ from the inverse function revisited. https://eprint.iacr.org/2013/731
15. Liang J (1978) On the solutions of trinomial equations over finite fields. Bull Cal Math Soc 70:379–382
16. Mesnager S (2016) Bent functions: fundamentals and results. Springer
17. Mesnager S, Riera C, Stănică P, Yan H, Zhow Z (2020) Investigations on c-(almost) perfect nonlinear functions, manuscript
18. Peng J, Tan CH (2017) New differentially 4-uniform permutations by modifying the inverse function on subfields. Cryptogr Commun 9:363–378
19. Qu L, Tan Y, Tan CH, Li C (2013) Constructing differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$ via the switching method. IEEE Trans Inf Theory 59(4):4675–4686
20. Qu L, Tan Y, Li C, Gong G (2016) More constructions of differentially 4-uniform permutations on $\mathbb{F}_{2^{2k}}$. Des Codes Cryptogr 78:391–408
21. Riera C, Stănică P, Investigations on c-(almost) perfect nonlinear functions. https://arxiv.org/abs/2004.02245

22. Stănică P (2020) Investigations on c-boomerang uniformity and perfect nonlinearity. https://arxiv.org/abs/2004.11859
23. Stănică P (2020) 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
24. Stănică P, Geary A, The c-differential behavior of the inverse function under the EA-*equivalence*. Cryptogr Commun. https://arxiv.org/abs/2006.00355
25. Tokareva N (2015) Bent functions. In: Results and applications to cryptography. Academic Press, San Diego, CA
26. Yu Y, Wang M, Li Y (2013) Constructing differentially 4 uniform permutations from known ones. Chin J Electron 22(3):495–499
27. Yan H, Mesnager S, Zhou Z, Power functions over finite fields with low c-differential uniformity. https://arxiv.org/pdf/2003.13019.pdf
28. Wu Y, Li N, Zeng X, New Pc N and APc N functions over finite fields. https://arxiv.org/abs/2010.05396
29. Zha Z, Hu L, Some classes of power functions with low c-differential uniformity over finite fields. https://arxiv.org/abs/2008.12183
30. Zha Z, Hu L, Sun S (2014) Constructing new differentially 4-uniform permutations from the inverse function. Finite Fields Appl 25:64–78