On -1-differential uniformity of ternary APN power functions

Haode Yan

Abstract

Very recently, a new concept called multiplicative differential and the corresponding c-differential uniformity were introduced by Ellingsen *et al*. A function $F(x)$ over finite field $\mathrm{GF}(p^n)$ to itself is called c-differential uniformity δ, or equivalent, $F(x)$ is differentially (c,δ) uniform, when the maximum number of solutions $x \in \mathrm{GF}(p^n)$ of $F(x+a)-F(cx)=b$, $a,b,c \in \mathrm{GF}(p^n)$, $c \neq 1$ if $a=0$, is equal to δ. The objective of this paper is to study the -1-differential uniformity of ternary APN power functions $F(x)=x^d$ over $\mathrm{GF}(3^n)$. We obtain ternary power functions with low -1-differential uniformity, and some of them are almost perfect -1-nonlinear.

Index Terms

c-differentials, differential uniformity, almost perfect c-nonlinearity

I. Introduction

Differential cryptanalysis ([4], [5]) is one of the most fundamental cryptanalytic approaches targeting symmetric-key primitives. Such a cryptanalysis approach has attracted a lot of attention because it was proposed to be the first statistical attack for breaking the iterated block ciphers [4]. The security of cryptographic functions regarding differential attacks was widely studied in the past 30 years. This type of security is quantified by the so-called *differential uniformity* of the substitution box (S-box) used in the cipher [26]. In [3], a new type of differential was proposed. The authors utilized modular multiplication as a primitive operation, which extends the type of differential cryptanalysis. It is necessary to start the theoretical analysis of an (output) multiplicative differential. Motivated by practical differential cryptanalysis, Ellingsen *et al.* recently coined a new concept called *multiplicative differential* and the corresponding c-differential uniformity ([16]).

Definition 1. *Let* $\mathrm{GF}(p^n)$ *denote the finite field with* p^n *elements, where* p *is a prime number and* n *is a positive integer. For a function* F *from* $\mathrm{GF}(p^n)$ *to itself,* $a,c \in \mathrm{GF}(p^n)$*, the (multiplicative)* c *derivative of* F *with respect to* a *is define as*

$$ {}_cD_aF(x) = F(x+a) - cF(x), \text{ for all } x. $$

For $b \in \mathrm{GF}(p^n)$*, let* ${}_c\Delta_F(a,b) = \#\{x \in \mathrm{GF}(p^n) : F(x+a)-cF(x)=b\}$*. We call* ${}_c\Delta_F = \max\{{}_c\Delta_F(a,b) : a,b \in \mathrm{GF}(p^n), \text{and } a \neq 0 \text{ if } c=1\}$ *the* c*-differential uniformity of* F*. If* ${}_c\Delta_F = \delta$*, then we say* F *is differentially* (c,δ)*-uniform.*

If the c-differential uniformity of F equals 1, then F is called a perfect c-nonlinear (PcN) function. PcN functions over odd characteristic finite fields are also called c-planar functions. If the c-differential uniformity of F is 2, then F is called an almost perfect c-nonlinear (APcN) function. It is easy to see that, for $c=1$ and $a \neq 0$, the c-differential uniformity becomes the usual differential uniformity, and the PcN and APcN functions become perfect nonlinear (PN) function and almost perfect nonlinear function (APN) respectively. These functions are of great significance in both theory and practical applications. For even characteristic finite fields, APN functions have the lowest differential uniformity. Known APN functions over even characteristic finite fields were presented in [1], [12], [13], [14], [17], [22], [23], [25]. For the

H. Yan is with the School of Mathematics, Southwest Jiaotong University, Chengdu, 610031, China (e-mail: hdyan@swjtu.edu.cn)

TABLE I
POWER FUNCTIONS $F(x)=x^d$ OVER GF(p^n) WITH LOW c-DIFFERENTIAL UNIFORMITY

p	d	condition	${}_c\Delta_F$	References
any	2	$c\neq 1$	2	[16]
any	p^n-2	$c=0$	1	[16]
2	2^n-2	$c\neq 0$, $\mathrm{Tr_n}(c)=\mathrm{Tr_n}(c^{-1})=1$	2	[16]
2	2^n-2	$c\neq 0$, $\mathrm{Tr_n}(c)=0$ or $\mathrm{Tr_n}(c^{-1})=0$	3	[16]
odd	p^n-2	$c=4$, $c=4^{-1}$ or $\chi(c^2-4c)=\chi(1-4c)=-1$	2	[16]
odd	p^n-2	$c\neq 0,4,4^{-1}$, $\chi(c^2-4c)$=1 or $\chi(1-4c)=1$	3	[16]
3	$(3^k+1)/2$	$c=-1$, $n/\gcd(k,n)=1$	1	[16]
odd	$(p^2+1)/2$	$c=-1$, n odd	1	[6]
odd	p^2-p+1	$c=-1$, $n=3$	1	[6]
2	2^k+1	$c\neq 1$, $\gcd(k,n)=1$	3	[27]
odd	p^k+1	$1\neq c\in \mathrm{GF}(p)$, $\gcd(k,n)=1$	2	[27]
odd	$(p^k+1)/2$	$c=-1$, $k/\gcd(k,n)$ is even	1	[27]
3	$(3^k+1)/2$	$c=-1$, k odd, $\gcd(k,n)=1$	2	[27]
any	$(2p^n-1)/3$	$c\neq 1$, $p^n\equiv 2 (\mathrm{mod}\ 3)$	≤ 3	[27]
odd	$(p^n+1)/2$	$c\neq \pm 1$	≤ 4	[27]
odd	$(p^n+1)/2$	$c\neq \pm 1$, $\chi(\frac{1-c}{1+c})=1$, $p^n\equiv 1(\mathrm{mod}\ 4)$	≤ 2	[27]
>3	$(p^n+3)/2$	$c=-1$, $p^n\equiv 3(\mathrm{mod}\ 4)$	≤ 3	[27]
>3	$(p^n+3)/2$	$c=-1$, $p^n\equiv 1(\mathrm{mod}\ 4)$	≤ 4	[27]
odd	$(p^n-3)/2$	$c=-1$	≤ 4	[27]

- $\mathrm{Tr_n}(\cdot)$ denotes the absolute trace mapping from GF(2^n) to GF(2).
- $\chi(\cdot)$ denotes the quadratic multiplicative character on GF(p^n)*.

known results on PN and APN functions over odd characteristic finite fields, the readers are referred to [8], [15], [10], [11], [19], [20], [24], [28], [29].

Because of the strong resistance to differential attacks and the low implementation cost in a hardware environment, power function $F(x)=x^d$ (i.e., monomials) with low differential uniformity can serve as a good candidate for the design of S-boxes. Moreover, power functions with low differential uniformity may also introduce some unsuitable weaknesses within a cipher [2], [21], [9], [7]. For instance, a differentially 4-uniform power function, which is extended affine EA-equivalent to the inverse function $x\mapsto x^{2^n-2}$ over GF(2^n) with even n, is employed in the AES (advanced encryption standard). A nature question one would ask is whether the power functions have good c-differential properties. In [16], the authors studied the c-differential uniformity of the well-known inverse function $F(x)=x^{p^n-2}$ over GF(p^n) for both even and odd prime p. It was shown that $F(x)$ is PcN when $c=0$, $F(x)$ is APcN with some conditions of c and $F(x)$ is differentially $(c,3)$-uniform otherwise. This result illustrates that PcN functions can exist for $p=2$. For PcN functions $x^{\frac{3^k+1}{2}}$ over GF(3^n) and $c=-1$, a sufficient and necessary condition was presented in [16]. In [6], it was shown that for odd p, n and $c=-1$, $x^{\frac{p^2+1}{2}}$ over GF(p^n) and x^{p^2-p+1} over GF(p^3) are PcN functions. In [27], it was proved that the Gold function over even characteristic finite field is differentially $(c,3)$-uniform for $c\neq 1$. Some PcN and APcN functions were also obtained. Moreover, for c-differential uniformity of power function $F(x)=x^d$ over GF(p^n) with $c\neq 1$, the following lemma was introduced.

Lemma 1 ([27]). *Let $F(x)=x^d$ be a power function over* GF(p^n). *Then*

$$ {}_c\Delta_F=\max\big\{\ \{{}_c\Delta_F(1,b):b\in \mathrm{GF}(p^n)\}\cup\{\gcd(d,p^n-1)\}\ \big\}.$$

As summarized in Table I, $c=-1$ is a very special case and sometimes the -1-differential uniformity is lower than c-differential uniformity for other $c\in \mathrm{GF}(p^n)$. The perfect -1-nonlinear function was also called quasi-planar function [6]. In this paper, we study the -1-differential uniformity of $F(x)$ when $F(x)$ is a ternary APN power function. Lemma 1 indicates that to determine the -1-differential uniformity of

TABLE II
RESULTS IN THIS PAPER

p	d	condition	${}_c\Delta_F$
3	$(3^{\frac{n+1}{2}}-1)/2$	$c=-1$, $n\equiv 1 \pmod 4$	≤ 2
3	$(3^{\frac{n+1}{2}}-1)/2+(3^n-1)/2$	$c=-1$, $n\equiv 3 \pmod 4$	≤ 2
3	$(3^{n+1}-1)/8$	$c=-1$, $n\equiv 1 \pmod 4$	≤ 2
3	$(3^{n+1}-1)/8+(3^n-1)/2$	$c=-1$, $n\equiv 3 \pmod 4$	≤ 2
3	$(3^{\frac{n+1}{2}}-1)/2$	$c=-1$, $n\equiv 3 \pmod 4$	≤ 4
3	$(3^{\frac{n+1}{2}}-1)/2+(3^n-1)/2$	$c=-1$, $n\equiv 1 \pmod 4$	≤ 4
3	$(3^{n+1}-1)/8$	$c=-1$, $n\equiv 3 \pmod 4$	≤ 4
3	$(3^{n+1}-1)/8+(3^n-1)/2$	$c=-1$, $n\equiv 1 \pmod 4$	≤ 4
3	$(3^{\frac{n+1}{4}}-1)(3^{\frac{n+1}{2}}+1)$	$c=-1$, $n\equiv 3 \pmod 4$	≤ 4
3	$(3^n+1)/4+(3^n-1)/2$	$c=-1$, n odd	≤ 4

power functions, the following -1-differential equation needs to be studied.

$$\Delta(x)=(x+1)^d+x^d=b.$$

Let $\delta(b)=\#\{x\in \mathrm{GF}(3^n) \mid \Delta(x)=b\}$. The maximum value of $\{\delta(b) \mid b\in \mathrm{GF}(3^n)\}$ plays an important role in studying the -1-differential uniformity of $F(x)$. In the rest of this paper, we consider several classes of ternary APN power functions. It turns out that they are with low -1-differential uniformity, and some of them are almost perfect -1-nonlinear. The results in this paper are shown in Table II.

II. C-DIFFERENTIAL UNIFORMITY OF $x^{\frac{3^{\frac{n+1}{2}}-1}{2}}$ OVER $\mathrm{GF}(3^n)$

In this section, let $F(x)=x^d$ be a power function over $\mathrm{GF}(3^n)$, where $n\equiv 1 \pmod 4$ and $d=\frac{1}{2}(3^{\frac{n+1}{2}}-1)$. It was proved in [15] that $F(x)$ is an APN function. We consider the -1-differential uniformity of $F(x)$ as follows.

Theorem 2. *Let $F(x)=x^d$ be a power function over $\mathrm{GF}(3^n)$, where $n\equiv 1 \pmod 4$ and $d=\frac{1}{2}(3^{\frac{n+1}{2}}-1)$. We have ${}_{-1}\Delta_F\leq 2$.*

Proof: Let $m=\frac{n+1}{2}$. Note that $2(3^m+1)d-3(3^n-1)=2$ and d is odd when $n\equiv 1 \pmod 4$, then $\gcd(d,3^n-1)=1$, i.e., $F(x)$ is a permutation on $\mathrm{GF}(3^n)$. For $b\in \mathrm{GF}(3^n)$, we consider the -1-differential equation

$$\Delta(x)=(x+1)^d+x^d=b. \tag{1}$$

Let $u_{x+1}=(x+1)^d$ and $u_x=x^d$. For $x\neq 0$, note that

$$u_x^{3^m+1}=x^{\frac{3^{n+1}-1}{2}}=\chi(x)x. \tag{2}$$

Herein and hereafter, let χ denote the quadratic multiplicative character on $\mathrm{GF}(3^n)^*$. Let $x\in \mathrm{GF}(3^n)\setminus\{0,-1\}$ be a solution of (1) for fixed $b\in \mathrm{GF}(3^n)$, then $u_x,u_{x+1}\neq 0$. Taking the (3^m+1)th power on both sides of $u_{x+1}=-u_x+b$, we have

$$bu_x^{3^m}+b^{3^m}u_x=-\chi(x+1)(x+1)+\chi(x)x+b^{3^m+1}. \tag{3}$$

For equation (3), we distinguish the following four cases.

Case I. $\chi(x+1)=\chi(x)=1$.

In this case, we have $bu_x^{3^m}+b^{3^m}u_x=b^{3^m+1}-1$ from (3). Since the mapping $u_x\mapsto bu_x^{3^m}+b^{3^m}u_x$ is bijective on $\mathrm{GF}(3^n)$, we can find a unique u_x. Because $F(x)$ is a permutation, a unique x can be found from the u_x. This case has at most one solution.

Case II. $\chi(x+1)=\chi(x)=-1$.

This case has at most one solution. The discussion is similar to that of Case I and we omit it.

Case III. $\chi(x+1)=1,\chi(x)=-1$. From (3), we have $bu_x^{3^m}+b^{3^m}u_x=x+b^{3^m+1}-1$ in this case, and then we have

$$(u_x+b)^{3^m+1}=-b^{3^m+1}-1 \tag{4}$$

by (2). If there are two distinct solutions in this case, namely x_3 and x_3', then u_{x_3} and $u_{x_3'}$ satisfy (4) with $\chi(x_3+1)=\chi(x_3'+1)=1$ and $\chi(x_3)=\chi(x_3')=-1$. Consequently $(u_{x_3}+b)^{3^m+1}=(u_{x_3'}+b)^{3^m+1}$ can be obtained from (4). Then we have $u_{x_3}+b=-(u_{x_3'}+b)$ since $\gcd(3^m+1,3^n-1)=2$ and $x_3\neq x_3'$, which leads to $u_{x_3}=b-u_{x_3'}=u_{x_3'+1}$. However, the above conclusion contradicts to $\chi(u_{x_3})=\chi(x_3)=-1$ and $\chi(u_{x_3'+1})=\chi(x_3'+1)=1$. We conclude that Case III has at most one solution.

Case IV. $\chi(x+1)=-1,\chi(x)=1$. In this case we have $bu_x^{3^m}+b^{3^m}u_x=-x+b^{3^m+1}+1$ from (3), and then

$$(u_x+b)^{3^m+1}=-b^{3^m+1}+1 \tag{5}$$

by (2). Similar to Case III, we can obtain that this case has at most one solution.

Next we will prove that for fixed b, (1) cannot have solution in Case I and Case II simultaneously. Otherwise, suppose that x_1 and x_2 are solutions of (1) in Case I and Case II with $\chi(x_1+1)=\chi(x_1)=1$ and $\chi(x_2+1)=\chi(x_2)=-1$ respectively. Then we have $bu_{x_1}^{3^m}+b^{3^m}u_{x_1}=b^{3^m+1}-1$ and $bu_{x_2}^{3^m}+b^{3^m}u_{x_2}=b^{3^m+1}+1$, where u_{x_1} and u_{x_2} we defined before. Now we have $b(u_{x_1}+u_{x_2})^{3^m}+b^{3^m}(u_{x_1}+u_{x_2})=-b^{3^m+1}$ and the consequent $u_{x_1}+u_{x_2}=b$. From (1), we can obtain $u_{x_2}=u_{x_1+1}$, which contradicts to $\chi(u_{x_2})=\chi(x_2)=-1$ and $\chi(u_{x_1+1})=\chi(x_1+1)=1$. Therefore, we conclude that (1) has at most one solution in Cases I and II for fixed $b\in \mathrm{GF}(3^n)$.

Then we prove that for fixed b, (1) cannot have solution in Case III and Case IV simultaneously. Otherwise, suppose that x_3 and x_4 are solutions of (1) in Case III and Case IV with $\chi(x_3+1)=1$, $\chi(x_3)=-1$ and $\chi(x_4+1)=-1,\chi(x_4)=1$ respectively. Then x_3 and x_4 satisfy (4) and (5) respectively. By the sum of (4) and (5), we have

$$(u_{x_3}+b)^{3^m+1}+(u_{x_4}+b)^{3^m+1}=b^{3^m+1}. \tag{6}$$

Taking the 3^mth power on both sides of (6), we have

$$(u_{x_3}+b)^{3^m+3}+(u_{x_4}+b)^{3^m+3}=b^{3^m+3} \tag{7}$$

since $3^m(3^m+1)=3^{n+1}+3^m=3^m+3+3(3^n-1)$. From (6) and (7), we have $(u_{x_3}+b)^{3^m+3}+(u_{x_4}+b)^{3^m+3}=b^2(u_{x_3}+b)^{3^m+1}+b^2(u_{x_4}+b)^{3^m+1}$, that is

$$-(u_{x_3}+b)^{3^m+1}u_{x_3}(b-u_{x_3})=(u_{x_4}+b)^{3^m+1}u_{x_4}(b-u_{x_4}). \tag{8}$$

Note that $b-u_{x_3}=u_{x_3+1}$ and $b-u_{x_4}=u_{x_4+1}$, the left-hand side of (8) is a square element and the right-hand side of (8) is a nonsquare element. Then $u_{x_3}+b=u_{x_4}+b=0$ can be obtained, i.e. $u_{x_3}=u_{x_4}$, which contradicts to $\chi(u_{x_3})=\chi(x_3)=-1$ and $\chi(u_{x_4})=\chi(x_4)=1$. We conclude that (1) has at most one solution in Cases III and IV for fixed $b\in \mathrm{GF}(3^n)$.

From the above discussions, (1) has at most two solutions in $\mathrm{GF}(3^n)\setminus\{0,-1\}$. One can be easily calculate that $\Delta(0)=1$ and $\Delta(-1)=-1$. For $b=1$ and $b=-1$, it can be verified that $\Delta(x)=1$ and $\Delta(x)=-1$ has no solution in $\mathrm{GF}(3^n)\setminus\{0,-1\}$, i,e, $\delta(1)=\delta(-1)=1$. Then we obtain $\delta(b)\leq 2$ for any b, which leads to ${}_{-1}\Delta_F\leq 2$ by Lemma 1 and $\gcd(d,3^n-1)=1$.

■

For $n\equiv 3 \pmod 4$, we can also get power functions with low -1-differential uniformity.

Theorem 3. *Let $F(x)=x^d$ be a power function over $\mathrm{GF}(3^n)$, where $n\equiv 3 \pmod 4$ and $d=\frac{1}{2}(3^{\frac{n+1}{2}}-1)$. We have ${}_{-1}\Delta_F\leq 4$.*

Proof: The proof is similar to that of Theorem 2. We give a sketch here. In this case, $\gcd(d,3^n-1)=2$. With the notation we used before, equations (1), (2) and (3) also hold. Let $x\in \mathrm{GF}(3^n)\setminus\{0,-1\}$ be a solution of (3) for fixed $b\in \mathrm{GF}(3^n)$, four cases are considered as follows.

Case I. $\chi(x+1)=\chi(x)=1$.

In this case, We have $bu_x^{3^m}+b^{3^m}u_x=b^{3^m+1}-1$ from (3). Since the mapping $u_x \mapsto bu_x^{3^m}+b^{3^m}u_x$ is bijective on GF(3^n), we can find a unique u_x. Then a unique x can be found for $\chi(x)=1$. This case has at most one solution.

Case II. $\chi(x+1)=\chi(x)=-1$.

Similar to Case I, this case has at most one solution.

Case III. $\chi(x+1)=1,\chi(x)=-1$. We have $bu_x^{3^m}+b^{3^m}u_x=x+b^{3^m+1}-1$ from (3), and then we have $(u_x+b)^{3^m+1}=-b^{3^m+1}-1$ by (2). We can obtain two u_x's since $\gcd(d,3^n-1)=2$ and the consequent two x's for given $\chi(x)$. This case has at most two solutions.

Case IV. $\chi(x+1)=-1,\chi(x)=1$.

Similar to Case III, this case has at most two solutions.

One can similarly prove that for fixed b, (1) cannot have solution in Case III and Case IV simultaneously. By discussions as above, we know that (1) has at most four solutions in GF(3^n)$\setminus\{0,-1\}$. We have $\Delta(0)=\Delta(-1)=1$. For $b=1$, one can easily verify that $\Delta(x)=1$ has no solution in GF(3^n)$\setminus\{0,-1\}$, i.e., $\delta(1)=2$. Then we obtain $\delta(b)\leq 4$ for any b, this leads to ${}_{-1}\Delta_F\leq 4$ by Lemma 1 and $\gcd(d,3^n-1)=2$. ■

For $d'=d+\frac{3^n-1}{2}$, we have the following corollary.

Corollary 4. *Let $F'(x)=x^{d'}$ be a power function over* GF(3^n)*, where n is an odd integer and $d'=\frac{3^{\frac{n+1}{2}}-1}{2}+\frac{3^n-1}{2}$. We have ${}_{-1}\Delta_{F'}\leq 2$ when $n\equiv 3 \pmod 4$ and ${}_{-1}\Delta_{F'}\leq 4$ when $n\equiv 1 \pmod 4$.*

Proof: It can be calculated that $\gcd(d',3^n-1)\leq 2$. First we consider $n\equiv 3 \pmod 4$, i.e., $3n\equiv 1 \pmod 4$. By Theorem 2,

$$(x+1)^{\frac{3^{\frac{3n+1}{2}}-1}{2}}+x^{\frac{3^{\frac{3n+1}{2}}-1}{2}}=b \tag{9}$$

has at most two solutions in GF(3^{3n}) for any $b\in$ GF(3^{3n}). Since $(3^n-1)|\frac{3^{\frac{3n+1}{2}}-1}{2}-d'$, equation (9) becomes $(x+1)^{d'}+x^{d'}=b$ any $x,b\in$ GF(3^n). Therefore, this equation has at most two solutions in GF(3^n), i.e., ${}_{-1}\Delta_{F'}\leq 2$. The other case can be proved similarly and we omit the details. ■

III. -1-DIFFERENTIAL UNIFORMITY OF $x^{\frac{3^{n+1}-1}{8}}$ OVER GF(3^n)

In this section, let $F(x)=x^d$ be a power function over GF(3^n), where $n\equiv 1 \pmod 4$ and $d=\frac{3^{n+1}-1}{8}$. It was proved in [15] that $F(x)$ is an APN function. We consider the -1-differential uniformity of $F(x)$ as follows.

Theorem 5. *Let $F(x)=x^d$ be a power function over* GF(3^n)*, where $n\equiv 1 \pmod 4$ and $d=\frac{3^{n+1}-1}{8}$. We have ${}_{-1}\Delta_F\leq 2$.*

Proof: Note that $\gcd(d,3^n-1)=1$, $F(x)$ is a permutation on GF(3^n). For $b\in$ GF(3^n), we consider the c-differential equation

$$\Delta(x)=(x+1)^d+x^d=b. \tag{10}$$

Let $u_{x+1}=(x+1)^d$ and $u_x=x^d$. For $x\neq 0$, note that

$$u_x^4=x^{4d}=\chi(x)x. \tag{11}$$

Let $x\in$ GF(3^n)$\setminus\{0,-1\}$ be a solution of (10) for fixed $b\in$ GF(3^n), then $u_x,u_{x+1}\neq 0$. Taking the 4th power on both sides of $u_{x+1}=-u_x+b$, we have

$$bu_x^3+b^3u_x=-\chi(x+1)(x+1)+\chi(x)x+b^4. \tag{12}$$

For (12), we distinguish the following four cases.

Case I. $\chi(x+1)=\chi(x)=1$.

In this case, we have $bu_x^3+b^3u_x=b^4-1$ from (12). Since the mapping $u_x\mapsto bu_x^3+b^3u_x$ is bijective on GF(3^n), we can find a unique u_x. Because $F(x)$ is a permutation, a unique x can be found from the u_x. This case has at most one solution.

Case II. $\chi(x+1)=\chi(x)=-1$.

This case has at most one solution. The discussion is similar to that of Case I and we omit it.

Case III. $\chi(x+1)=1,\chi(x)=-1$. From (12), we have $bu_x^3+b^3u_x=x+b^4-1$ in this case, and then we have

$$(u_x+b)^4=-b^4-1 \tag{13}$$

by (11). If there are two distinct solutions in this case, namely x_3 and x_3', then u_{x_3} and $u_{x_3'}$ satisfy (13) with $\chi(x_3+1)=\chi(x_3'+1)=1$ and $\chi(x_3)=\chi(x_3')=-1$. Consequently $(u_{x_3}+b)^4=(u_{x_3'}+b)^4$ can be obtained from (13). Then we have $u_{x_3}+b=-(u_{x_3'}+b)$ since $x_3\neq x_3'$, which leads to $u_{x_3}=b-u_{x_3'}=u_{x_3'+1}$. However, the above conclusion contradicts to $\chi(u_{x_3})=\chi(x_3)=-1$ and $\chi(u_{x_3'+1})=\chi(x_3'+1)=1$. We conclude that Case III has at most one solution.

Case IV. $\chi(x+1)=-1,\chi(x)=1$. In this case we have $bu_x^3+b^3u_x=-x+b^4+1$ from (12), and then

$$(u_x+b)^4=-b^4+1 \tag{14}$$

by (11). Similar to Case III, we can obtain that this case has at most one solution.

Next we will prove for fixed b, (10) cannot have solutions in Case I and Case II simultaneously. Otherwise, suppose that x_1 and x_2 are solutions of (10) in Case I and Case II with $\chi(x_1+1)=\chi(x_1)=1$ and $\chi(x_2+1)=\chi(x_2)=-1$ respectively. Then we have $bu_{x_1}^3+b^3u_{x_1}=b^4-1$ and $bu_{x_2}^3+b^3u_{x_2}=b^4+1$, where u_{x_1} and u_{x_2} we defined before. Now we have $b(u_{x_1}+u_{x_2})^3+b^3(u_{x_1}+u_{x_2})=-b^4$ and the consequent $u_{x_1}+u_{x_2}=b$. From (10), we can obtain $u_{x_2}=u_{x_1+1}$, which contradicts $\chi(u_{x_2})=\chi(x_2)=-1$ and $\chi(u_{x_1+1})=\chi(x_1+1)=1$. Therefore, we conclude that (10) has at most one solution in Cases I and II for fixed $b\in$ GF(3^n).

Then we prove for fixed b, (10) cannot have solutions in Case III and Case IV simultaneously. Otherwise, suppose that x_3 and x_4 are solutions of (10) in Case III and Case IV with $\chi(x_3+1)=1,\chi(x_3)=-1$ and $\chi(x_4+1)=-1,\chi(x_4)=1$ respectively. Then x_3 and x_4 satisfy (13) and (14) respectively. By the sum of (13) and (14), we have $(u_{x_3}+b)^4+(u_{x_4}+b)^4=b^4$, that is,

$$(u_{x_3}^2-bu_{x_3}+u_{x_4}^2-bu_{x_4}+b^2)^2=-u_{x_3}(b-u_{x_3})u_{x_4}(b-u_{x_4}). \tag{15}$$

Note that $b-u_{x_3}=u_{x_3+1}$ and $b-u_{x_4}=u_{x_4+1}$, the right-hand side of (15) is a nonzero nonsquare element, which is a contradiction. We conclude that (10) has at most one solution in Cases III and IV for fixed $b\in$ GF(3^n). From the above discussions, (10) has at most two solutions in GF(3^n)$\setminus\{0,-1\}$.

One can easily calculate that $\Delta(0)=1$ and $\Delta(-1)=-1$. For $b=1$ and $b=-1$, it can be verified that $\Delta(x)=1$ and $\Delta(x)=-1$ has no solution in GF(3^n)$\setminus\{0,-1\}$, i,e, $\delta(1)=\delta(-1)=1$. Then we obtain $\delta(b)\leq 2$ for any b, this leads to ${}_{-1}\Delta_F\leq 2$ by Lemma 1 and $\gcd(d,3^n-1)=1$.

■

For $n\equiv 3 \pmod 4$ and $d'=d+\frac{3^n-1}{2}$, we list the following theorems without proof.

Theorem 6. *Let $F(x)=x^d$ be a power function over* GF(3^n)*, where $n\equiv 3 \pmod 4$ and $d=\frac{3^{n+1}-1}{8}$. We have ${}_{-1}\Delta_F\leq 4$.*

Corollary 7. *Let $F'(x)=x^{d'}$ be a power function over* GF(3^n)*, where n is an odd integer and $d'=\frac{3^{n+1}-1}{8}+\frac{3^n-1}{2}$. We have ${}_{-1}\Delta_{F'}\leq 2$ when $n\equiv 3 \pmod 4$ and ${}_{-1}\Delta_{F'}\leq 4$ when $n\equiv 1 \pmod 4$.*

IV. -1-DIFFERENTIAL UNIFORMITY OF $x^{(3^{\frac{n+1}{4}}-1)(3^{\frac{n+1}{2}}+1)}$ OVER GF(3^n)

In [29], the authors studied the power function $F(x)=x^d$ over GF(3^n), where $n\equiv 3 \pmod 4$ and $d=(3^{\frac{n+1}{4}}-1)(3^{\frac{n+1}{2}}+1)$. It was shown that x^d is an APN function. In what follows, we discuss the -1-differential uniformity of $F(x)$.

Theorem 8. *Let $F(x)=x^d$ be a power function over* GF(3^n)*, where $n\equiv 3 \pmod 4$, $d=(3^m-1)(3^{2m}+1)$ and $m=\frac{n+1}{4}$. Then ${}_{-1}\Delta_F \leq 4$.*

Proof: Note that d is an even number and $\gcd(d,3^n-1)=2$. For $b\in$ GF(3^n), we consider equation

$$\Delta(x)=(x+1)^d+x^d=b. \tag{16}$$

It is easy to see that $\Delta(0)=\Delta(-1)=1$, and (16) has no solution when $b=0$. Let $x\in$ GF$(3^n)\setminus\{0,-1\}$ be a solution of (16) for some given $b\in$ GF$(3^n)^*$. Denote by $u_{x+1}=(x+1)^d$ and $u_x=x^d$. Since $\frac{3^m+1}{2}\cdot d=\frac{3^{n+1}-1}{2}\equiv 1+\frac{3^n-1}{2} \pmod{3^n-1}$, we have ${u_x}^{\frac{3^m+1}{2}}=\chi(x)x$ and ${u_{x+1}}^{\frac{3^m+1}{2}}=\chi(x+1)(x+1)$. One can easily see that if u_x and $\chi(x)$ are given, x can be determined uniquely.

Let $\xi\in$ GF$(3^{2n})\setminus\{0,\pm 1\}$ such that $\frac{u_x}{b}=\xi+\frac{1}{\xi}-1=\frac{(\xi+1)^2}{\xi}$, then we have $\frac{u_{x+1}}{b}=-\xi-\frac{1}{\xi}-1=-\frac{(\xi-1)^2}{\xi}$ by (16). Moreover, we can obtain $\chi(x)x={u_x}^{\frac{3^m+1}{2}}=(\frac{b(\xi+1)^2}{\xi})^{\frac{3^m+1}{2}}$ and $\frac{b(\xi+1)^2}{\xi}=x^d=(\frac{b(\xi+1)^2}{\xi})^{\frac{3^m+1}{2}\cdot d}$. Similarly, $-\frac{b(\xi-1)^2}{\xi}=(x+1)^d=(-\frac{b(\xi-1)^2}{\xi})^{\frac{3^m+1}{2}\cdot d}$. Then ξ satisfies $-(\frac{\xi+1}{\xi-1})^2=(\frac{\xi+1}{\xi-1})^{(3^m+1)d}$, i.e., $(\frac{\xi+1}{\xi-1})^{3(3^n-1)}=-1$. This with $\xi\in$ GF(3^{2n}) leads to $\xi^{3^n+1}=1$. In the following, we discuss equation (16) in two cases.

Case 1. $\chi(x+1)=\chi(x)$.

In this case, ${u_{x+1}}^{\frac{3^m+1}{2}}-{u_x}^{\frac{3^m+1}{2}}=\chi(x+1)(x+1)-\chi(x)x=\chi(x)$. That is,

$$(-\frac{b(\xi-1)^2}{\xi})^{\frac{3^m+1}{2}}-(\frac{b(\xi+1)^2}{\xi})^{\frac{3^m+1}{2}}=\chi(x).$$

We deduce the following equation

$$(-1)^{\frac{3^m+1}{2}}(\xi-1)^{3^m+1}-(\xi+1)^{3^m+1}=\chi(x)b^{-\frac{3^m+1}{2}}\xi^{\frac{3^m+1}{2}}. \tag{17}$$

Two subcases are considered as follows.

Subcase 1.1. $\frac{3^m+1}{2}$ is even, i.e., m is odd. Then (17) becomes $\xi^{3^m}+\xi=\chi(x)b^{-\frac{3^m+1}{2}}\xi^{\frac{3^m+1}{2}}$. Let $t=\xi^{\frac{3^m-1}{2}}$, then $t_{1,2}=-\chi(x)b^{-\frac{3^m+1}{2}}\pm\sqrt{b^{-(3^m+1)}-1}$. Since m is odd, then $\gcd(m,2n)=1$ and $\gcd(\frac{3^m-1}{2},3^{2n}-1)=1$. We can obtain a unique ξ_1 from $\xi^{\frac{3^m-1}{2}}=t_1$ since $\gcd(\frac{3^m-1}{2},3^{2n}-1)=1$. For $t_2=t_1^{-1}$, we can also obtain a unique ξ_2 such that $\xi_2^{\frac{3^m-1}{2}}=t_2$. Note that $\xi_2=\xi_1^{-1}$ and they give the same u_x.

Subcase 1.2. $\frac{3^m+1}{2}$ is odd, i.e., m is even. Then (17) becomes $\xi^{3^m+1}+1=\chi(x)b^{-\frac{3^m+1}{2}}\xi^{\frac{3^m+1}{2}}$. Let $t=\xi^{\frac{3^m+1}{2}}$, then $t_{1,2}=-\chi(x)b^{-\frac{3^m+1}{2}}\pm\sqrt{b^{-(3^m+1)}-1}$. Since m is even, then $\gcd(m,2n)=2$ and $\gcd(\frac{3^m+1}{2},3^{2n}-1)=1$. We can obtain a unique ξ_1 from $\xi^{\frac{3^m+1}{2}}=t_1$ since $\gcd(\frac{3^m+1}{2},3^{2n}-1)=1$. For $t_2=t_1^{-1}$, we can also obtain a unique ξ_2 such that $\xi_2^{\frac{3^m+1}{2}}=t_2$. Note that $\xi_2=\xi_1^{-1}$ and they give the same u_x.

By discussions in the above two subcases, we conclude that one can obtain a unique u_x from given b and $\chi(x)$, and then we find at most one solution of (17) for each $\chi(x)$. This case has at most 2 solutions.

Case 2. $\chi(x+1)=-\chi(x)$.

In this case, ${u_{x+1}}^{\frac{3^m+1}{2}}+{u_x}^{\frac{3^m+1}{2}}=\chi(x+1)(x+1)+\chi(x)x=-\chi(x)$. That is,

$$(-\frac{b(\xi-1)^2}{\xi})^{\frac{3^m+1}{2}}+(\frac{b(\xi+1)^2}{\xi})^{\frac{3^m+1}{2}}=-\chi(x).$$

We deduce the following equation

$$(-1)^{\frac{3^m+1}{2}}(\xi-1)^{3^m+1}+(\xi+1)^{3^m+1}=-\chi(x)b^{-\frac{3^m+1}{2}}\xi^{\frac{3^m+1}{2}}. \tag{18}$$

We have following two subcases.

Subcase 2.1. $\frac{3^m+1}{2}$ is even. Then (18) becomes

$$\xi^{3^m+1}+1=\chi(x)b^{-\frac{3^m+1}{2}}\xi^{\frac{3^m+1}{2}}.$$

Let $t=\xi^{\frac{3^m+1}{2}}$, if $\chi(x)=1$, then $t_{1,2}=-b^{-\frac{3^m+1}{2}}\pm\sqrt{b^{-(3^m+1)}-1}$. Note that $t_2=t_1^{-1}$ and they give the same u_x's, we only consider t_1. Since $\frac{3^m+1}{2}$ is even, m is odd, then $\gcd(\frac{3^m+1}{2},3^n+1)=2$. We can obtain two solutions, namely $\pm\xi_1$, from $\xi^{\frac{3^m+1}{2}}=t_1$ since $\gcd(\frac{3^m+1}{2},3^n+1)=2$. If $\chi(x)=-1$, then $t_{3,4}=b^{-\frac{3^m+1}{2}}\pm\sqrt{b^{-(3^m+1)}-1}$. We only consider t_4, which satisfies $t_4=-t_1$. Similarly, we obtain another two ξ's, namely $\delta\xi_1$, $-\delta\xi_1$, where $\delta\in \mathrm{GF}(3^{2n})$ with $\delta^2=-1$. In this subcase, we get four distinct ξ's and each of them corresponds a possible solution of (16).

Subcase 2.2. $\frac{3^m+1}{2}$ is odd. Then (18) becomes

$$\xi^{3^m}+\xi=\chi(x)b^{-\frac{3^m+1}{2}}\xi^{\frac{3^m+1}{2}}.$$

Let $t=\xi^{\frac{3^m-1}{2}}$, if $\chi(x)=1$, then $t_{1,2}=-b^{-\frac{3^m+1}{2}}\pm\sqrt{b^{-(3^m+1)}-1}$. We only consider the equation $\xi^{\frac{3^m-1}{2}}=t_1$ since the solutions of another equation correspond the same u_x's. Since $\frac{3^m+1}{2}$ is odd, m is even, and $\gcd(\frac{3^m-1}{2},3^n+1)=4$. We obtain four solutions from $\xi^{\frac{3^m-1}{2}}=t_1$, namely $\xi_2,\delta\xi_2,-\xi_2,-\delta\xi_2$, where $\delta\in \mathrm{GF}(3^{2n})$ with $\delta^2=-1$. If $\chi(x)=-1$, then $t_{3,4}=b^{-\frac{3^m+1}{2}}\pm\sqrt{b^{-(3^m+1)}-1}$. We only consider t_4, which satisfies $t_4=-t_1$. If ξ_2' is a solution of $\xi^{\frac{3^m-1}{2}}=t_4=-t_1$, then $(\frac{\xi_2'}{\xi_2})^{\frac{3^m-1}{2}}=-1$. We obtain that $(\frac{\xi_2'}{\xi_2})^4=1$ from $\gcd(3^m-1,3^n+1)=4$, i.e., $\xi_2'=\delta^i\xi_2$, $0\le i\le 3$. That means $\xi^{\frac{3^m-1}{2}}=t_4$ cannot contribute new ξ's. We also obtain four distinct ξ's in this subcase.

Recall that $u_x=b(\xi+\frac{1}{\xi}-1)$, in the following we prove that ξ and $\delta\xi$ cannot contribute solutions of (16) simultaneously, where δ we defined before. More precisely, let $u_{x_1}=b(\xi+\frac{1}{\xi}-1)$ and $u_{x_2}=b(\delta\xi+\frac{1}{\delta\xi}-1)$, then we have

$$(u_{x_1}+b)^2+(u_{x_2}+b)^2=b^2((\xi+\frac{1}{\xi})^2+(\delta\xi+\frac{1}{\delta\xi})^2)=b^2.$$

The above identity can be rewritten as

$$(u_{x_1}+u_{x_2}+b)^2=-u_{x_1}u_{x_2},$$

which is a contradiction. That means each of subcases 2.1 and 2.2 has at most two solutions.

By discussions as above, we conclude that ${}_{-1}\Delta_F\le 4$. The proof is finished. ■

V. C-DIFFERENTIAL UNIFORMITY OF $x^{\frac{3^n+1}{4}+\frac{3^n-1}{2}}$ OVER $\mathrm{GF}(3^n)$

It was proved in [19] that the power function x^d is an APN function over $\mathrm{GF}(3^n)$, where n is an odd integer and $d=\frac{3^n+1}{4}+\frac{3^n-1}{2}$. The -1-differential uniformity is considered as follows.

Theorem 9. *Let $F(x)=x^d$ be a power function over $\mathrm{GF}(3^n)$, where n is odd and $d=\frac{3^n+1}{4}+\frac{3^n-1}{2}$. Then ${}_{-1}\Delta_F\le 4$.*

Proof: One can easily obtain that d is even and $\gcd(d,3^n-1)=2$. Note that $\chi(-1)=-1$ since n is odd. We consider the c-differential equation

$$\Delta(x)=(x+1)^d+x^d=b. \tag{19}$$

When $b=0$, (19) has no solution. For fixed $b\in\mathrm{GF}(3^n)^*$, let $x\in\mathrm{GF}(3^n)\setminus\{0,-1\}$ is a solution of (19), we distinguish the following four cases.

Case I. $\chi(x+1)=\chi(x)=1$. Let $x+1=\alpha^2$ and $x=\beta^2$ for $\alpha,\beta\in\mathrm{GF}(3^n)^*$, then $\alpha^2-\beta^2=1$. We can obtain $\chi(\alpha)\alpha+\chi(\beta)\beta=b$ from (19). We have

$$\beta^2+1=\alpha^2=(\chi(\alpha)\alpha)^2=(b-\chi(\beta)\beta)^2=b^2+b\chi(\beta)\beta+\beta^2.$$

One can obtain $\chi(\beta)\beta = b^{-1} - b$ and $x = \beta^2 = (\chi(\beta)\beta)^2 = (b^{-1} - b)^2$. This case has at most one solution.

Case II. $\chi(x+1) = \chi(x) = -1$. Let $x+1 = -\alpha^2$ and $x = -\beta^2$ for $\alpha, \beta \in \mathrm{GF}(3^n)^*$, then $\alpha^2 - \beta^2 = -1$. Similar to Case I, we can obtain $x = -(b + b^{-1})^2$. This case has at most one solution.

Case III. $\chi(x+1) = 1, \chi(x) = -1$. Let $x+1 = \alpha^2$ and $x = -\beta^2$ for $\alpha, \beta \in \mathrm{GF}(3^n)^*$, then $\alpha^2 + \beta^2 = 1$. We can obtain $\chi(\alpha)\alpha + \chi(\beta)\beta = b$ from (19). Let $\gamma = \chi(\beta)\beta$, which is a square element in $\mathrm{GF}(3^n)$. Then $\gamma^2 = \beta^2$ and γ satisfies $(b-\gamma)^2 + \gamma^2 = 1$, i.e.

$$\gamma^2 - b\gamma + 1 - b^2 = 0, \tag{20}$$

which is a quadratic equation on γ. Equation (20) has most two solutions, then we can obtain at most two x's since $x = \gamma^2$. This case has at most two solutions.

Case IV. $\chi(x+1) = -1, \chi(x) = 1$. Let $x+1 = -\alpha^2$ and $x = \beta^2$ for $\alpha, \beta \in \mathrm{GF}(3^n)^*$, then $\alpha^2 + \beta^2 = -1$. We can obtain $\chi(\alpha)\alpha + \chi(\beta)\beta = b$ from (19). Let $\gamma = \chi(\beta)\beta$, which is a square element in $\mathrm{GF}(3^n)$. Then $\gamma^2 = \beta^2$ and γ satisfies $(b-\gamma)^2 + \gamma^2 = -1$, i.e.

$$\gamma^2 - b\gamma - 1 - b^2 = 0, \tag{21}$$

which is a quadratic equation on γ. Equation (21) has most two solutions, then we can obtain at most two x's since $x = \gamma^2$. This case has at most two solutions.

Note that x is a solution of (19) if and only if $-x-1$ is a solution of (19). This implies that if Case III (the same for Case IV) has solutions, it must has two solutions. Next we prove that for fixed $b \in \mathrm{GF}(3^n)^*$, (19) cannot have solution in Case III and Case IV simultaneously. Suppose on the contrary that x_1, x_2 are distinct solutions of (19) for some given b in Case III, and x_3, x_4 are distinct solutions of (19) for the same b in Case IV. By the discussions above, each $x_i, 1 \le i \le 4$ corresponds to square element γ_i. Moreover, γ_1, γ_2 are the two solutions of (20), and γ_3, γ_4 are the two solutions of (21). They satisfy $\gamma_1 + \gamma_2 = \gamma_3 + \gamma_4 = b$, $\gamma_1\gamma_2 = 1 - b^2$ and $\gamma_3\gamma_4 = -1 - b^2$. We can obtain $\gamma_1^2 + \gamma_2^2 + \gamma_3^2 + \gamma_4^2 = (\gamma_1+\gamma_2)^2 + \gamma_1\gamma_2 + (\gamma_3+\gamma_4)^2 + \gamma_3\gamma_4 = 0$. Since $\gamma_4 \neq 0$, let $\delta_i = \gamma_i/\gamma_4$, $1 \le i \le 3$, then δ_1, δ_2 and δ_3 are square elements, and they satisfy $\delta_1 + \delta_2 - \delta_3 - 1 = 0$ and $\delta_1^2 + \delta_2^2 + \delta_3^2 + 1 = 0$. Replace by $\delta_3 = \delta_1 + \delta_2 - 1$, we have the following quadratic equation on δ_1.

$$\delta_1^2 - (\delta_2 - 1)\delta_1 + (\delta_2^2 - \delta_2 + 1) = 0.$$

The discriminate of the above quadratic equation is $\Delta = (\delta_2 - 1)^2 - (\delta_2^2 - \delta_2 + 1) = -\delta_2$, which is a nonzero nonsquare element in $\mathrm{GF}(3^n)$. It contradicts to $\delta_1 \in \mathrm{GF}(3^n)$. Then we proved that for $b \in \mathrm{GF}(3^n)^*$, (19) has at most 4 solutions in $\mathrm{GF}(3^n) \setminus \{0, -1\}$.

One can easily check that $\Delta(0) = \Delta(-1) = 1$. For $b = 1$, it can be verified that $\Delta(x) = 1$ has no solution in the four cases, i.e., $\Delta(x) = 1$ has no solution in $\mathrm{GF}(3^n) \setminus \{0, -1\}$, $\delta(1) = 2$. This with the discussions above leads to ${}_{-1}\Delta_F \le 4$. ■

VI. CONCLUDING REMARKS

In this paper, we studied the -1-differential uniformity of ternary APN power functions. We obtain many classes of power functions with low -1-differential uniformity, and some of them are almost perfect -1-nonlinear. It is mentioned that in this paper we give the upper bound of the -1-differential uniformity of some power functions, it is better to study whether the equality holds. In this paper, we only studied $c = -1$, it is also good to study the c-differential properties for $\pm 1 \neq c \in \mathrm{GF}(3^n)$. Our future work is to find more power functions with low c-differential uniformity. This topic is widely open. Power functions with low usual differential uniformity are useful in sequences, coding theory, and combinatorial designs. It is worth finding the applications of power functions with low c-differential uniformity in such areas.

REFERENCES

[1] T. Beth and C. Ding, *On almost perfect nonlinear permutations*, in Advances in Cryptography. EUROCRYPT 93 (Lecture Notes in Computer Science). New York: Springer-Verlag, 1994, vol. 765, pp. 65-76.

[2] C. Blondeau, A. Canteaut and P. Charpin, "Differential properties of power functions", *Int. J. Inf. Coding Theory*, vol. 1, no. 2, pp. 149–170, 2010.

[3] N. Borisov, M. Chew, R. Johnson and D. Wagner, *Multiplicative Differentials*, In: Daemen J., Rijmen V. (eds) Fast Software Encryption. FSE 2002. Lecture Notes in Computer Science, vol 2365. Springer, Berlin, Heidelberg, 2002.

[4] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems", In Alfred Menezes and Scott A. Vanstone, editors, Advances in Cryptology-CRYPTO' 90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990, Proceedings, volume 537 of Lecture Notes in Computer Science, pages 2-21. Springer, 1990.

[5] E. Biham and A. Shamir. Differential Cryptanalysis of the Data Encryption Standard. Springer, 1993.

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

[7] A. Canteaut and M. Videau, "Degree of composition of highly nonlinear functions and applications to higher order differential cryptanalysis", in *Advances in Cryptology – EUROCRYPT 2002*, Springer, Berlin, 2002, vol. 2332, Lecture Notes in Comput. Sci., pp. 518–533.

[8] R. S. Coulter and R. W. Matthews, "Planar functions and planes of Lenz-Barlotti class II", Des. Codes Cryptogr., vol. 10, pp. 167-184, 1997.

[9] N. Courtois and J. Pieprzyk, "Cryptanalysis of block ciphers with overdefined systems of equations", in *Advances in Cryptology – ASIACRYPT 2002*, Springer, Berlin, 2002, vol. 2501, Lecture Notes in Comput. Sci., pp. 267–287.

[10] P. Dembowski and T. G. Ostrom, "Planes of order n with collineation groups of order n^2", *Math. Z.*, vol. 193, pp. 239-258, 1968.

[11] C. Ding and J. Yuan, "A new family of skew Paley-Hadamard difference sets", *J. Comb. Theory Ser. A*, vol. 113, pp. 1526-1535, 2006.

[12] H. Dobbertin, "Almost perfect nonlinear power functions on GF(2^n) : A new case for n divisible by 5", in Finite Fields and Applications, Augsburg, Germany, 1999, pp. 113-121.

[13] H. Dobbertin, "Almost perfect nonlinear power functions on GF(2^n) : The Welch case", *IEEE Trans. Inf. Theory*, vol. 45, no. 4, pp. 1271-1275, 1999.

[14] H. Dobbertin, "Almost perfect nonlinear power functions on GF(2^n) : The Niho case", *Inform. Comput.*, vol. 151, no. 1-2, pp. 57-72, 1999.

[15] H. Dobbertin, D. Mills, E.N. Muller, A. Pott and W. Willems, "APN functions in odd characteristic", *Discr. Math.*, vol. 267, pp. 95-112, 2003.

[16] P. Ellingsen, P. Felke, C. Riera, P. Stănică and A. Tkachenko, "C-differentials, multiplicative uniformity and (almost) perfect c-nonlinearity", *IEEE Trans. Inform. Theory*, 2020. To appear.

[17] R. Gold, "Maximal recursive sequences with 3-valued recursive crosscorrelation function", *IEEE Trans.Inf .Theory*, vol. 14, no. 1, pp. 154-156, 1968.

[18] T. Helleseth and A. Kholosha, "On the equation $x^{2^l+1}+x+a$ over GF(2^k)", *Finite Fields Appl.*, vol. 14, no. 1, pp. 159-176, 2008.

[19] T. Helleseth, C. Rong and D. Sandberg, "New families of almost perfect nonlinear power mappings", *IEEE Trans. Inform. Theory*, vol. 45. no. 2, pp. 475–485, 1999.

[20] T. Helleseth and D. Sandberg, "Some power mappings with low differential uniformity", *Appl. Algebra Engrg. Commun. Comput.*, vol. 8, pp. 363-370, 1997.

[21] T. Jakobsen and Lars R. Knudsen, "The interpolation attack on block ciphers", in *Fast Software Encryption – FSE 1997*, Springer, Berlin, 1997, vol. 1267, Lecture Notes in Comput. Sci., pp. 28–40.

[22] H. Janwa and R. M. Wilson, "Hyperplane sections of Fermat varieties in P3 in char. 2 and some applications to cyclic codes", in Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, vol. 673, pp. 180-194, 1993.

[23] T. Kasami, "The weight enumerators for several classes of subcodes of the 2nd order binary reed-muller codes", *Inform. Contr.*, vol. 18, pp. 369-394, 1971.

[24] E. Leducq, "New families of APN functions in characteristic 3 or 5", In: Arithmetic, Geometry, Cryptography and Coding Theory, Contemporary Mathematics, vol. 574, pp. 115-123, AMS 2012.

[25] K. Nyberg, "Differentially uniform mappings for cryptography", in Advances in Cryptography. EUR OCRYPT93 (Lecture Notes in Computer Science). New York: Springer-Verlag, 1994, vol. 765, pp. 55-64.

[26] K. Nyberg and L. Knudsen, "Provable security against differential cryptanalysis", in Proc. Advances in Cryptology-CRYPTO 92, 1993, vol. 740, Lecture Notes in Computer Science, pp. 566-574.

[27] H. Yan, S. Mesnager and Z. Zhou, "Power Functions over Finite Fields with Low c-Differential Uniformity", arXiv:2003.13019v3.

[28] Z. Zha and X, Wang, "Power functions with low uniformity on odd characteristic finite fields", *Sci. China Math.*, vol. 53, no. 8, pp. 1931-1940, 2010.

[29] Z. Zha and X. Wang, "Almost perfect nonlinear power functions in odd characteristic", *IEEE Trans. Inf. Theory*, vol. 57, no. 7, pp. 4826-4832, 2011.