SOME STUDIES ON c-DIFFERENTIAL UNIFORMITY OF THE SWAPPED INVERSE FUNCTION

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF APPLIED MATHEMATICS
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

BETÜL ÜNVER

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
CRYPTOGRAPHY

SEPTEMBER 2021

Approval of the thesis:

SOME STUDIES ON c-DIFFERENTIAL UNIFORMITY OF THE SWAPPED INVERSE FUNCTION

submitted by **BETÜL ÜNVER** in partial fulfillment of the requirements for the degree of **Master of Science in Cryptography Department, Middle East Technical University** by,

Prof. Dr. A. Sevtap Selçuk Kestel _____
Director, Graduate School of **Applied Mathematics**

Prof. Dr. Ferruh Özbudak _____
Head of Department, **Cryptography**

Prof. Dr. Ferruh Özbudak _____
Supervisor, **Cryptography, METU**

Examining Committee Members:

Assoc. Prof. Dr. Murat Cenk
Institute of Applied Mathematics, METU _____

Prof. Dr. Ferruh Özbudak
Institute of Applied Mathematics, METU _____

Assist. Prof. Dr. Eda Tekin
Department of Mathematics, Karabük University _____

Date: _____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: BETÜL ÜNVER

Signature :

ABSTRACT

SOME STUDIES ON c-DIFFERENTIAL UNIFORMITY OF THE SWAPPED INVERSE FUNCTION

ÜNVER, Betül
M.S., Department of Cryptography
Supervisor : Prof. Dr. Ferruh Özbudak

September 2021, 33 pages

Lately, Ellingsen et al in [5] created a new concept by making minor changes on the old concept of (multiplicative) differential. This new definition which has potential to be capable of extending differential cryptanalysis in a completely new way is named as c-differential and brought with it the concept of c-differential uniformity. We examlify that how some known functions' behaviour, especially inverse function, would be under this extended differential. The main purpose of this thesis is to observe how the swapped inverse function, which is one of the variety of ways to modify the binary inverse function, impacts the function's c-differential uniformity. In this thesis, we proposed a new theorem including the new characterization of the $(0, \alpha)$-swapped inverse function in even characteristic under this new concept, $x^{2^n-2} + x^{2^n-1}/\alpha + (x-\alpha)^{2^n-1}/\alpha$ on F_{2^n}, and reached two conclusions for all $c \neq 1$: we prove that its c-differential uniformity value can take 1,2,3 and 4 and attains its maximum value 4 under two special conditions satisfied by the trace mapping.

Keywords: c-DDT, c-differential uniformity, c-PN, c-APN, swapping function , swapped inverse function

ÖZ

DEĞİŞTİRİLEN TERS FONKSİYONUN C-DİFERANSİYEL TEKDÜZELİĞİ ÜZERİNE BAZI ÇALIŞMALAR

ÜNVER, Betül
Yüksek Lisans, Kriptografi Bölümü
Tez Yöneticisi : Prof. Dr. Ferruh Özbudak

Eylül 2021, 33 sayfa

Son zamanlarda, Ellingsen ve diğerleri [5]'de eski (çarpımsal) diferansiyel kavramı üzerinde küçük değişiklikler yaparak yeni bir kavram yarattılar. Diferansiyel kriptanalizi tamamen yeni bir şekilde genişletme potansiyeline sahip olan bu yeni tanım, c-diferansiyel olarak adlandırılmış ve beraberinde c-diferansiyel tekdüzelik kavramını getirmiştir. Bilinen bazı fonksiyonların davranışlarının, özellikle ters fonksiyonun, bu genişletilmiş diferansiyel altında nasıl olacağını inceleyeceğiz. Bu tezin temel amacı, ikili ters fonksiyonu değiştirmenin çeşitli yollarından biri olan değiş tokuş edilen ters fonksiyonun, fonksiyonun c-diferansiyel tekdüzeliğini nasıl etkilediğini gözlemlemektir. Bu tezde, çift karakteristikli $(0, \alpha)$-değiştirilmiş ters fonksiyonu için, $x^{2^n-2} + x^{2^n-1}/\alpha + (x-\alpha)^{2^n-1}/\alpha$ F_{2^n} üzerinde , bu yeni kavram altında çift karakteristikli yeni karakterizasyonunu içeren yeni bir teorem önerdik ve tüm $c \neq 0$ için iki sonuca ulaştık: onun c-diferansiyel tekdüzelik değerinin 1,2,3 ve 4'ü alabileceğini ve trace bağıntı tarafından sağlanan iki özel koşul altında maksimum değeri olan 4'e ulaştığını kanıtladık.

Anahtar Kelimeler: c-DDT, c-diferansiyel tekdüzeliği, c-PN, c-APN, takas fonksiyonu, değiştirilen ters fonksiyonu

ACKNOWLEDGMENTS

At first, I am sincerely in dept to my advisor Prof. Dr. Ferruh Özbudak for his quidance, continuous support and unlimited thrust at every stage of this study. He always there to meet and provide me new and challenging ideas and inspirational comments.

I am grateful to my dear thesis defense committee members Assoc. Prof. Dr. Murat Cenk, Assist. Prof. Dr. Eda Tekin for their time and effort.

I thanks to my friends for their encouragement and patience for my frequent absences throughout the research. I would like to express my deepest thanks to my close friends Mehtap Fidan and Mehmet Arda Çolak for their keen friendship and morale support at my desperte times. It is great to know that I will have such wonderful pals for the rest of my life.

Finally but the most, I send endless thanks to my mother and brother very special for me.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

S-box	Substitution Box
Tr	Trace Mapping
DDT	Difference Distribution Table
APN	Almost Perfect Nonlinear
PN	Perfect Nonlinear
c-DDT	c-Difference Distribution Table
cAPN	c-Almost Perfect Nonlinear
cPN	c-Perfect Nonlinear
APcN	c-Almost Perfect Nonlinear
PcN	c-Perfect Nonlinear

CHAPTER 1

INTRODUCTION

We now live in a data-driven society, and in most situations, businesses acquire and keep sensitive personal and non-personal data, which cyber criminals can exploit. Cryptography, when used correctly and with the right tactics, can help protecting this sensitive data from cyber attacks and threat actors. In other words, it aims to ensure safe communication against malicious third-parties. Cryptography includes mathematical principles and a sequence of rule-based logical operations known as algorithms to make messages complex and hard to decipher. Block ciphers are symmetric-key algorithms for cryptography that use the same cryptographic keys for both the encryption and decryption by dividing the data into blocks.

The security of block ciphers against differential attacks has attracted a lot of attention and been the research topic for the last 30 years. In order for a cryptosystem to be considered "secure", it must be subjected to rigorous testing by the security community. How resistant a block cipher to an attack depends on a cryptographic properties of a Boolean function which is used in block ciphers. Because of this reason, the crucial cryptographic properties of Boolean function are considered in the process of designing and evaluating secure block cipher.

Differential cryptanalysis is the first statistical attack to analyze the security of a block cipher structure, proposed back in the late 1980s by Biham and Shamir [3]. Its publication allows a great deal of studies which analyzed the security provided by various types of functions in the matter of differential attack. This attack made a significant contribution to the development of stronger encryption methods thanks to

mathematical idea behind it.

1.1 Motivation and Problem Definition

1.1.1 DDT and c-DDT

When a vectorial function is put to use as an S-box nonlinear part in a block cipher, its differential uniformity measures the function's contribution to differential cryptanalysis resistance. For this purpose, a table also known as the difference distribution table (DDT) was formed for S-box to show the total number of solutions of equations $S(x \oplus a) \oplus S(x) = b$ for every input a and output b. It is a method to represent the differential behavior of a function.

Example: Consider the lookup table of 5x5 S-box and determine its differential behavior using DDT. The DDT for this S-box is given in Table 1.1.

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S(x)	8	15	5	10	2	11	6	13	13	10	5	7	9	11	1	15

The Appendix A contains a detailed table showing the results from the equation $S(x \oplus a) \oplus S(x) = b$ for all input a and corresponding output value b, allowing us to derive this DDT for S-box in this example. The maximum value which is 10 in this Difference Distribution Table of this S-box is called its differential uniformity. If the differential uniformity of a function equals to 2, then it has better resistance to differential attacks. This means that these functions have high security in cryptography and they are called APN functions.

Ellingsen et al. [5] reconstructed a brand new notion an crucial criteria for functions and their resistances based on the notion DDT. They are called this new table as c-DDT whose its maximum entry gives c-differential uniformity. There are block ciphers that use the multiplication operation as a primitive, so this extended notion could be intriguing from a practical standpoint for these ciphers. Thanks to this new concept, differential cryptanalysis have chance to gain a different point of view and some existing ciphers were cryptanalyzed with it.

Table 1.1: Differential Distribution Table (DDT) of S-Box

a \ b	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	32	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
1	-	-	4	-	2	-	-	6	2	4	2	4	-	-	2	6
2	-	-	2	2	4	2	2	-	8	-	-	-	-	6	4	2
3	-	-	4	-	-	2	4	6	-	2	6	-	2	2	-	4
4	-	2	-	4	6	-	2	2	8	2	4	-	-	2	-	-
5	-	4	2	6	-	-	4	4	2	-	2	-	4	2	2	-
6	6	2	2	-	2	2	2	4	2	-	-	-	6	-	4	-
7	-	2	2	-	2	2	-	-	2	2	2	2	2	-	6	8
8	4	2	4	2	-	10	-	2	2	-	-	2	-	2	2	-
9	-	2	8	-	2	-	-	-	-	6	4	-	4	2	2	2
10	2	-	-	4	2	-	4	-	4	-	2	4	2	6	-	2
11	-	-	4	-	6	-	2	4	-	-	4	-	2	4	2	4
12	-	4	2	4	4	2	-	-	2	-	4	4	-	4	-	2
13	2	2	4	2	4	-	6	-	4	2	2	2	2	-	-	-
14	4	4	2	2	-	6	2	4	-	2	-	2	4	-	-	-
15	2	-	-	2	2	2	-	4	-	-	4	-	4	2	8	2

We looked into a few well-known almost perfect nonlinear functions.

There are some criteria for permutation functions to use them as the S-boxes in block ciphers. Besides the high algebraic degree and high nonlinearity, they must have low differential uniformity. Power functions require lower implementation costs in hardware. We focus on their analysis under this new differential. We especially studied on the inverse function through this new multiplicative notions, one of the class of power functions. This thesis includes new results on swapped form of them.

1.2 The Outline of the Thesis

The following is the structure of the thesis:

- Some of the fundamental primitives, notations, and definitions about topic and an important lemma which will highly help at some points during the thesis are in Chapter 2.

- Chapter 3 relates to analysis of c-differential uniformity of well-known functions such as Gold/Kasami and power functions. There are some information on

what the swapping of a function is and a formula on how it can be obtained. After giving detailed information about swapped inverse function, $(0, 1)$-swapped inverse function and its c-differential uniformity are following this.

- Chapter 4 details our study on $(0, \alpha)$-swapped inverse function and involves a theorem which includes the results of all works in it.
- Section 5 concludes the paper and provides comprehensive detailed information about the entire thesis and future works.

CHAPTER 2

PRELIMINARY TO THE SUBJECT

In this chapter, some of the fundamental primitives, notations, and definitions will be given to help the reader to get sufficient theoretical background information about subject.

2.0.1 Notations

From now on, S-box will equally mean a vectorial Boolean function $S : F_2^n \rightarrow F_2^n$. Functions in this form were used in this thesis. The focus is on cryptographic differential properties of extended dimensions of Boolean functions. This section includes only some required notations related to the objects of thesis. Before giving main required definitions, generally accepted meanings to some signs and notations in the finite field is as follows:
Assume that p is a prime number, let m, n are positive integers and $\mathbb{F}_{p^n}$ denotes the finite field throughout the thesis. Obviously, it has p^n elements. If the element zero is removed from this field, then the new group is denoted as the same notation but with asteriks, $\mathbb{F}_{p^n}^*$. It denotes the multiplicative finite field. $\frac{1}{\alpha}$ means the inverse of the nonzero element α in the multiplicative group of mentioned finite field); if a finite field with bigger dimension is considered, the notation will be $\mathbb{F}_p^n$ or $\mathbb{F}_{p^n}$. It denotes the vector space with n-dimensional on $\mathbb{F}_p$. The following two functions type are most crucial for S-boxes used in block ciphers: any map from $\mathbb{F}_{p^n}$ (or $\mathbb{F}_p^n$) to $\mathbb{F}_p$ (i.e, f: $\mathbb{F}_{p^n} \rightarrow \mathbb{F}_p$) with n variables is named as a p-ary Boolean function; a function $F : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^m}$ (or, $F : \mathbb{F}_p^n \rightarrow \mathbb{F}_p^m$) is named as a vectorial p-ary Boolean function. In other words, it is simply denoted as (n, m)-function.

Definition 1. *(Derivative of f) Let f be a p-ary function, the following*

$$D_\alpha f(x) = f(x+\alpha) - f(x), \textit{for all } x \in \mathbb{F}_{p^n} \tag{2.1}$$

is also a p-ary function. It represents the derivative of f at the point $\alpha \in \mathbb{F}_{p^n}$. The derivative of a vectorial Boolean function F at the same point α can easily obtain from above definition on the derivative of f.

Definition 2. *(the entries of Difference Distribution Table) Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be a vectorial function, let α,b $\in \mathbb{F}_{p^n}$,*

$$\#\{x \in \mathbb{F}_{p^n} : D_\alpha F(x) = F(x+\alpha) - F(x) = b\} = \Delta_F(\alpha, b)$$

This definition can be defined for general vectorial Boolean function, i.e for the function F in the form of (n,m). We give this definition for the case when m=n since we consider m=n through the thesis.

Definition 3. *(Differential Uniformity of F)*

$$max\{\Delta_F(a,b) : \alpha, b \in \mathbb{F}_{p^n}, \alpha \neq 0\} = \delta_F \tag{2.2}$$

The above mathematical definition says basically that the maximum entry in Difference Distribution Table gives us the differential uniformity of F. In other words, the maximum entry at DDT refers to exactly δ. If $\Delta_F \leq \delta$ (or, $\delta_F = \delta$), then this function is called differential uniformity-δ function.

- Name this function as planar function, shortly PN or a perfect nonlinear if this number is equivalent to 1.
- Name this function as shortly APN or an almost perfect nonlinear if this number is equivalent to 2.
  (Note that there is not any function with differential 1-uniformity in even characterictic.)

There are some criteria for these functions in order to resist differential attacks. Their differential uniformity should be very low in term of their resistance besides other good cryptological properties.

Definition 4. *((multiplicative) c-derivative of F)*
Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ *be a vectorial map. Let* $\alpha, b \in \mathbb{F}_{p^n}$. *Assume that* c *be an element from the field* $\mathbb{F}_{p^m}$. *The (multiplicative) c-derivative of this function at the point* $\alpha \in \mathbb{F}_{p^n}$ *is the following mapping:*

$$F(x+\alpha) - cF(x) = {}_cD_\alpha F(x) \text{ for all } x \in \mathbb{F}_{p^n} \tag{2.3}$$

For c=1, the above definition will be exactly identical to the definition on standard derivative of function at the same point.

Definition 5. *(the c-Difference Distribution Table's entries) Let* $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ *be a vectorial map. Let* $\alpha, b \in \mathbb{F}_{p^n}$. *Assume that* c *be an element from the field* $\mathbb{F}_{p^m}$.

$$\#\{x \in \mathbb{F}_{p^n} : {}_cD_\alpha F(x) = F(x+\alpha) - cF(x) = b\} = {}_c\Delta_F(\alpha, b)$$

Definition 6. *(c-Differential Uniformity of F)*

$$max\{{}_c\Delta_F(\alpha, b) \quad | \quad \alpha, b \in \mathbb{F}_{p^n}, \alpha \neq 0 \text{ if c=1}\} = \delta_{F,c} \tag{2.4}$$

Definition 7. *(Trace map) Let* $Tr_{F/K}$ *be a map s.t* $Tr_{F/K} : \mathbb{F}_{q^n} \to \mathbb{F}_q$ *and* $x \in \mathbb{F}_{q^n}$, *the trace of x over* $\mathbb{F}_q$ *is defined by*

$$Tr_{F/K}(x) = x + x^p + x^{p^2} + ... + x^{p^{n-1}}$$

Consider the following properties of the trace map:

- $Tr_{F/K}(l+k) = Tr_{F/K}(l) + Tr_{F/K}(k)$ for all $s, t \in F$;
- $Tr_{F/K}$ is a linear transformation.
- $Tr_{F/K}(cs) = cTr_{F/K}(s)$ for all $c \in K$, $s \in F$
- $Tr_{F/K}(c) = tc$ for all $c \in K$
- $Tr_{F/K}(s^q) = Tr_{F/K}(s)$ for all $s \in$ F

In this thesis, we will use additive form of Hilbert's Theorem 90. It says the following:

Definition 8. *(Hilbert's Theorem 90) Let G be a Galois group. Let K/F be an extension. Assume G=$<\rho>$. Then for $\alpha \in \mathbb{K}$*

$$\alpha = \rho(\beta) - \beta \quad \textit{if and only if} \quad Tr_{\mathbb{K}/\mathbb{F}}(\alpha) = 0, \quad \textit{for some } \beta \in \mathbb{K}$$

This thesis is based on finding how many solutions satisfying the given equations according to characteristic of the field in the thesis and enumerating them.

Lemma 1.

1. *Let $0 \neq c \in \mathbb{F}_{2^n}^*$ and let $d \in \mathbb{F}_{2^n}^*$. Consider the equation $x^2+cx+d = 0$, it has two solutions in $\mathbb{F}_{2^n}$ if $Tr\left(\frac{c}{d^2}\right) = 0$. If this condition is not hold, then it has no solution in this field. If a is not equivalent to 0 and b is equivalent to zero, it has only one solution. (see [2]).*

2. *Let $0 \neq c \in \mathbb{F}_{p^n}^*$ and let $d \in \mathbb{F}_{p^n}^*$. Consider $cx^2 + dx + e = 0$, p is a prime number except 2. There exists two solutions for this equation in $\mathbb{F}_{p^n}$ if and only if $d^2 - 4ce$ is nonzero square in $\mathbb{F}_{p^n}$. If this discriminant is zero square, then it has only one solution in this field. (see [12]).*

3. *Let $c \in \mathbb{F}_{2^n}^*$ and let $0 \neq d \in \mathbb{F}_{2^n}^*$. Consider the equation $x^3 + cx + d = 0$. (Let u_1, u_2 be the solutions for the equation $u^2 + du + c^3 = 0$).*

   (i) $Tr(1) = Tr(c^3/d^2)$ and u_1, u_2 are cubes in $\mathbb{F}_{2^n}$ for both even and odd n $\iff$ there are three solutions for this equation in the field of even characteristic;

   (ii) $Tr(1) \neq Tr(c^3/d^2)$ $\iff$ it has only one solution in the field of even characteristic ;

   (iii) u_1, u_2 are not cubes in this field for even n and in $\mathbb{F}_2^{2^n}$ for odd n and $Tr(1) = Tr(c^3/d^2)$ $\iff$ there is no solution in the field of even characteristic. (see [12]).

CHAPTER 3

C-DIFFERENTIAL UNIFORMITY

3.0.1 c-Differential Uniformity of Power Functions

Power permutations are a good possible choice for cryptography because they are usually less expensive to implement in hardware enviroment. Power functions' resilience to the typical differential attack attracted attention. They led to prompted more investigation on them. A detailed Table 3.4 is displayed by Riera et al. in [10], placed the end of this section. The idea of calculating their c-differential uniformity is coming from the following concept. Firstly, one need to look at the entries of c-Difference Distribution Table of power functions for $\alpha = 1$, which is ${}_{\mathrm{c}}\Delta_F(1, b)$. Secondly, the entries of c-Difference Distribution Table of power functions for $\alpha = 0$ should be calculated, which is ${}_{\mathrm{c}}\Delta_F(0, b)$. The second one is exactly corresponding to $gcd(d, p^n - 1)$. After calculating these two c-differential at the point 0 and 1, then the maximum value of their union gives the entries of c-Difference Distribution Table for this power functions, which are given in the paper [14].

The following idea is very useful to calculate the gratest common divisor in above explanation, which is coming from the paper [14].

There are three different answers for the gratest common divisor of $p^k + 1$ and $p^n - 1$: If the finite field is on the even characteristic, then

$gcd(p^k + 1, p^n - 1)$ equals to $\frac{2^{gcd(2k,n)-1}}{2^{gcd(k,n)-1}}$; $\frac{n}{gcd(n,k)}$ is odd, then $gcd(p^k + 1, p^n - 1)$ equals to 2; if it is even, the greatest common divisor equals to $p^{gcd(k,n)+1}$.

Below two examples are coming from two items of Theorem 3 from the paper [10]. We have proved both of them in detail as in the following way:

Example 1: Let $H : \mathbf{F}_{p^n} \to \mathbf{F}_{p^n}$ be a mapping such that $H(x) = x^d$. Let c is not equivalent to 1. If d equals to two, then H becomes almost perfect c-nonlinear function under the condition constructed for c.
By Definition 2.4, taking $d = 2$, the c-differential equation for $H(x) = x^2$ is By Definition 2.3, the (multiplicative) c-derivative of x^2 at the point $\alpha \in \mathbb{F}_{p^n}$ is

$$\begin{aligned} b = {}_{\mathrm{c}}D_{\alpha}H(x) = (x+\alpha)^2 - x^2 &= x^2 + 2\alpha x + \alpha^2 - cx^2 \\ &= (1-c).x^2 + 2\alpha x + \alpha^2 \end{aligned}$$

Since we are free to choose b, taking $b = 0$, By Lemma 1, $Tr(\frac{1-c}{4})$ equals to 0 if and only if there are 2 zeros for the this equation with second order , of course under the assumption $c \neq 1$, hence F is APcN function for $d = 2$.

Example 2: For c$\neq$1, the c-differential uniformity of $H(x) = x^{10} - vx^6 - v^2x^2$ over $\mathbf{F}_{3^n}$ is ${}_{\mathrm{c}}\Delta_H$ is greater than or equal to 2.

The c-differential equation ${}_{\mathrm{c}}D_{\alpha}H(x) = b$ for $H(x) = x^{10} - vx^6 - v^2x^2$ on $\mathbf{F}_3^n$ is as follows:

$$\begin{aligned} b &= (x+\alpha)^{10} - v(x+\alpha)^6 - v^2(x+\alpha)^2 - c(x^{10} - vx^6 - u^2x^2) \\ &= x^{10} + x^9\alpha + x\alpha^9 - v(x^6 + 2x^3\alpha^3 + \alpha^6) - v^2(x^3 + 2x\alpha^2 + \alpha^3) \\ &- c(x^{10} - vx^6 - v^2x^2) \\ &= (1-c)x^{10} + v\alpha^3x^3 + v(c-1)x^6 + \alpha x^9 \\ &+ (\alpha^9{+}^2)x + \alpha^{10} - v^2\alpha^2 - v\alpha^6 + v^2(c-1)x^2 \end{aligned}$$

When α is taken as 0, above equation becomes $b = (c-1)(-x^{10} + vx^6 + v^2x^2)$. As one can be seen that when x equals to 1 then it is a solution for the map H under the condition that c is not equal to 1 and $b = 0$. Hence, $1 \to {}_{\mathrm{c}}\Delta_H(0,0)$. This equations has two solutions, which are $x = 1, 2$ under $c \neq 1$ and $b = (c-1)(-1+v+v^2)$. Thus, $2 \to {}_{\mathrm{c}}\Delta_H\big(\alpha, (c-1)(-1+u+u^2)\big)$. As a result, this equation takes the value 2 a maximal c-differential uniformity. So, ${}_{\mathrm{c}}\Delta_H\big(\alpha, (c-1)(-1+v+v^2)\big) \geq 2$.

Since the function in Example 2 is the generalized formula, if $u = \pm 1$ for the special case, the equation becomes $H(x) = \pm x^6 - x^2 + x^{10}$ on $\mathbf{F}_{3^n}$. The following Table 3.1 shows the behavior for both functions when they are subjected to new notion of c-differential uniformity, by way of c-differential derivative.

Table 3.1: When $c \in \mathbf{F}_{3^n} \setminus \{0, 1\}$, $H(x) = x^{10} \pm x^6 - x^2$ on characteristic p=3 [4]

n	$H(x) = x^6 - x^2 + x^{10}$	$H(x) = -x^6 - x^2 + x^{10}$
11	10	10
9	10	10
7	10	10
5	6	6
3	4	4
2	2	2
1	2	2

We have already proved that its c-differential uniformity of H should be at least 2 in Example 2, as seen in the rows of the table. It equals to n+1 for n=1,3,5 and equals to 10 for $n \geq 7$, from [4].

3.0.2 c-Differential Uniformity for Gold/Kasami Function

We will consider two specific functions which are Gold and Kasami functions seen their mathematical formulas over $\mathbf{F}_{2^n}$ in the Table 3.2

Table 3.2: APN families that have been identified [9].

	Exponent	Condition
Dobbertin	-1+$2^{2s} + 2^{3s} + 2^s$+2^{4s}	$5s = n$
Niho	$2^s - 2^{\frac{s}{2}} - 1$ $2^s - 2^{\frac{3s+1}{2}} - 1$	$n = 2s + 1$, $s\ even$ $n = 2s + 1$, $s\ odd$
Inverse	$2^s - 2$	$s\ odd$
Kasami	$-2^s + 2^{2s} + 1$	$gcd(s, n) = 1$
Welch	$2^s + 3$	$n = 2s + 1$
Gold	$2^s + 1$	$gcd(s, n) = 1$

Note that, for $s = 1$, the Kasami function $K(x) = x^{2^{2s}-2^s+1}$ and the Gold function $G(x) = x^{2^s+1}$ are identical on characteristic 2, which is x^3, it can be easily obtained from Table 3.2.

- If r is selected as 1 to investigate their c-differential uniformity, this value equals to 2 when $n \geq 2$; equals to 3 when $n \geq 3$ for both functions. The proof for $n \geq 3$ is as follows:

  Proof. By Definition 2.3, the (multiplicative) c-derivative of $K(x) = x^3$ at the point $1 \in \mathbb{F}_{2^n}$ will become like in the following:

  $$\begin{aligned} &= (x+1)^3 + c.x^3 \\ &= x^3 + 3x^2 + 3x + 1 - c.x^3 \\ &= (1+c).x^3 + x^2 + x + 1 = {}_{\mathrm{c}}D_1K(x) \end{aligned}$$

  By Definition 2.4, taking b=1, the c-differential equation for $K(x) = x^3$

  $${}_{\mathrm{c}}\Delta_K(\alpha, b) = \#\{x \in \mathbb{F}_{2^n} : {}_{\mathrm{c}}D_1K(x) = 1\}$$

  The equation $(1+c).x^3 + x + 1 + x^2 = 1$ becomes $(1 + (1+c)x^2 + x)x = 0$. It is obvious that $x = 0$ is a trivial solution. By Lemma 1, $Tr(1+c)$ is equivalent to zero $\iff$ the quadratic equations $(1+c)x^2 + x + 1 = 0$ has two zeros. (Assuming $0 \neq= \gamma^2 + \gamma + 1 = c$ where γ is a primitive root of $\mathbb{F}_{2^n}$). Consequently, three solutions are coming from quadratic equations and $x = 0$ for $b = {}_{\mathrm{c}}D_\alpha K(x)$. Thus, the c-differential uniformity of Gold/Kasami function equals to 3 when $s = 1$. □

Note that, for $s = 2$, the Kasami renders $K(x) = x^5$. Gold function G turns into $G(x) = x^{13}$ over $\mathbf{F}_{2^n}$, respectively, from Table 3.2.

- If s is selected as 2, it allows us to obtain Table 3.3 below which shows their maximal c-differential uniformity for some n-values.

Table 3.3: c-differential for K(x) and G(x), r=2 [5].

n and $s = 2$	for Gold	for Kasami
8	5	5
7	3	3
6	5	5
5	3	3
4	5	5
3	3	3
2	4	4
1	2	2

The fact that c-differential uniformity of Kasami/Gold functions equals to 3 in the field of prime characteristic except for 2. (When n and s are relatively prime). It equals to 5 when p is even, which can be seen from the Table 3.3, for a proof see [5]. A number of well-known power functions and their differential spectrum are shown below in the Table 3.4 coming from the paper [4]. As one can see that they are quite low.

Table 3.4: c-differential uniformity which belongs to known power functions on $\mathbf{F}_{p^n}$ [10].

p	d	condition	${}_c\Delta_F$	Refs
any	2	$c \neq 1$	2	[5]
any	p^n-2	$c=0$	1	[5]
2	2^n-2	$c\neq 0, Tr_n(c)=Tr_n(c^{-1})=1$	2	[5]
2	2^n-2	$c\neq 0, Tr_n(c)=0$ or $\mathrm{Tr}_n(c^{-1})=0$	3	[5]
odd	p^n-2	$c=4,4^{-1}$, or $\mu(c^2-4c)=-1$ and $\mu(1-4c)=-1$	2	[5]
odd	p^n-2	$c\neq 4,4^{-1}$,$\mu(c^2-4c)=1$ or $\mu(1-4c)=1$	3	[5]
3	$(3^k+1)/2$	$c=-1, n/gcd(k,n)=1$	1	[5]
odd	$(p^2+1)/2$	$c=-1$, n odd	1	[1]
odd	p^2-p+1	$c=-1, n=3$	1	[1]
odd	$p^4-(p-2)p^2+(p-1)p+1$	$c=-1, n=5$	1	[6]
odd	$(p^5+1)/(p+1)$	$c=-1, n=5$		[6]
odd	$(p-1)p^6+p^5+(p-1)p^4+p^3+p^2+p$	$c=-1, n=7$	1	[6]
odd	$(p^7+1)/(p+1)$	$c=-1, n=7$	1	[6]
any	p^k+1	$c\neq 1\in \mathbb{F}_{p^{gcd(n,k)}}$	$p^{gcd(n,k)+1}$	[10]-Thm 3
2	2^k+1	$c\neq 1$, $\frac{n}{gcd(n,k)}\geq 3$ (n odd) $\frac{n}{gcd(n,k)}\geq 4$ (n even)	$2^{gcd(n,k)+1}$	[10]-Thm 4
odd	$(p^2+1)/2$	$c=1$	≤ 4	[8]
odd	$(p^2+1)/2$	$c=-1$	$p^{gcd(n,k)+1}$	[10]-Thm 6
odd	$(p^2+1)/2$	$c\neq \mp 1$	≤ 4	[10]-Thm 9
odd	$(p^2+1)/2$	$c\neq \mp 1$, $\mu(\frac{1-c}{1+c})=1$ $p^n\equiv 1(\mod 4)$	≤ 4	[10]-Thm 9
3	$\frac{3^n+3}{2}$	$c=-1$, n even	2	[10]-Thm 10
>3	$(p^n+3)/2$	$p^n\equiv 3(\mod 4), c\neq -1$	≤ 3	[10]-Thm 11
>3	$(p^n+3)/2$	$p^n\equiv 1(\mod 4), c\neq -1$	≤ 4	[10]-Thm 11
3	3^n-3	$c=1, n>1$ odd	2	[7]
3	3^n-3	$c=1, n>2, n\equiv 2(\mod 4)$	4	[13]
3	3^n-3	$c=1, n>2, n\equiv 0(\mod 4)$	5	[13]
3	3^n-3	$c=-1, n>2, n\equiv 0(\mod 4)$	6	[10]-Thm 12
3	3^n-3	$c=-1, n>2, n0(\mod 4)$	4	[10]-Thm 12
3	3^n-3	$c=0$	2	[10]-Thm 12
3	3^n-3	$c\neq 0,-1$	≤ 5	[10]-Thm 12
odd	$(p^n-3)/2$	$c=-1$	≤ 4	[10]-Thm 15
any	$(2p^n-1)/3$	$p^n 2(\mod 3)$	≤ 3	[10]-Thm 16

The next section is related to c-differential uniformity of inverse function form of x^{p^n-2} on F_{p^n} for all characteristics, which is a family class of permutation functions as it can be seen from the below Table 3.4.

3.0.3 c-Differential Behaviors of Inverse Functions

The inverse permutations are in the form of x^{2^n-2} in even characteristic. The following is their c-differential uniformity in all characteristic
The following two theorems are from the article [4].

3.0.3.1 The Inverse Function in Even Characteristic

When the finite field has characteristic 2, the following theorem shows these functions' differential behaviors under the notion of c:

Theorem 1. *[4] Let F be the inverse function s.t.* $F(x) = x^{2^n-2}$. *Assume that c be an element from the field* $\mathbb{F}_{2^n}$*:*

(i) P is c-planar function if c equals to zero (it means that P is a permutation polynomial).

(ii) P is c-almost perfect nonlinear if c is not equal to 0, $Tr(c)$ *equals to zero and* $Tr(1/c)$ *equals to 1.*

(iii) $\delta_{P,c} = 3$ *if c is not equal to 0,* $Tr(1/c)$ *equals to zero or* $Tr(c)$ *equals to 0*

Proof (i): The first step is constructing the equation ${}_c\Delta_P = b$ as

$$(x+\alpha)^{2^n-2} + cx^{2^n-2} = b \tag{3.1}$$

For α, b $\in \mathbb{F}_{2^n}$, when c=0, $(x+\alpha)^{2^n-2} = b$ ($\star$). When α equals to 1, then it becomes $x^{2^n-2} = b$, which is $x = \frac{1}{b}$. As a result, there is at most one solution which belongs to ($\star$) in the case of $\alpha = 0$. Hence ${}_c\Delta_P(0, \frac{1}{b}) = 1$. (Shortly, without computing, this proof can be explained with the fact that it has one solution because of permutation features of map P. □

Proof (ii) and (iii): For α, b $\in \mathbb{F}_{2^n}$, when c is not equivalent to 0, if α equals to zero, 3.1 renders $b = (1+c)x^{2^n-2}$, which has one zero: Since if b equals to 0, then $x = 0$ is only one zero; if x equals to 1, then $b = c+1$. Hence, $1 \to {}_c\Delta_P(0, 1+c)$; if $x \neq 0, 1$, then multiply equation with x, it turns into $xb = (c+1)x^{2^n-1}$, which means $x = \frac{1+c}{b}$, which has only one solution. From here on, we will suppose that $a \neq 0$. Case 1: $a = 1$, $b = 0$, the equation 3.1 becomes $(x+1)^{2^n-2}$+c$x^{2^n-2} = 0$ ($\star\star$). It is obvious that $x = 0$ is not solution. $x = 1$ is also not a solution in this case. Since $x \neq 0, 1$, we have only one solution which is $x = \frac{c}{c+1}$ since the equation ($\star\star$) turns to $x = (1+x)c$ by multiplying both sides of the equation ($\star$) by x(x+1). Case 2: a equals to one and b equals to 1, the equation 3.1 becomes $(x+1)^{2^n-2}$+c$x^{2^n-2} = 1$. While $x = 0$ is not a solution, $x = 1$ is a solution for this equation. So, $1 \to {}_c\Delta_F(1, 1)$. Multiplying it by $x+1$ and x, then it turns into $x + c(x+1) = x(x+1)$ which means $0 = c + cx + x^2$. From Lemma 1, there is two solutions $\iff Tr(\frac{c}{c^2}) = Tr(\frac{1}{c}) = 0$. Therefore, $2 \to {}_c\Delta_F(1, 1)$ under $Tr(\frac{1}{c}) = 0$. As a result, ${}_c\Delta_F(1, 1) = 3$. (This partially completes item (iii) in the Theorem under $Tr(\frac{1}{c}) = 0$). If $1 = Tr(\frac{1}{c})$, only one solution occurs for it. Case 3: $bisnotequaltozerooroneand\alpha$ equals to 1, the equation 3.1 turns into $b = cx^{2^n-2} + (x+1)^{2^n-2}+$. There is only one solution which is 1, x should not be zero. In the case that x is not equal to zero or one, multiplying by x and $x+1$, the equation turns into $x^2+(\frac{b+c+1}{b})x+\frac{b}{c} = 0$, which has two solutions under $b+c+1 \neq 0$ if and only if $Tr\big(\frac{cb}{(b+c+1)^2}\big) = 0$. Taken $b = c \neq 0, 1$, $0 = Tr(c^2) = Tr(c)$. All in all, adding all solutions, there are three zeros under the assumption of $Tr(c) = 0$. (This completely proves the item (iii) in the Theorem under the assumption of $Tr(c) = 0$). Taken $b \neq c \neq 0, 1$, (Clearly, $x = 0$ and $x = 1$ do not satisfy the equation). We now control whether two solutions exist or not from trace notion except $x = 0, 1$. The equation has only one solution in the case that c is not equal to one and b is equal to zero. (we did it in Case 1); otherwise $0 = Tr\big(\frac{bc}{b^2+c^2+1}\big)$ if and only there are two solutions. As one can see, the case of $1 = Tr(c)$ and $1 = Tr(\frac{1}{c})$ sufficient to show , since otherwise, we showed that three solutions occur. After now on, we claimed that one can always find $b \neq 0$ such that $Tr\big(\frac{bc}{b^2+c^2+1}\big) = 0$ in odd case or even case:
When n is odd, It can be argued that there is k s.t

$$\frac{1}{c} + 1 = \frac{1+c}{c} = \frac{ct}{c^2+1+t^2},$$

It converts to $0 = c^2t + (c+1)t^2 + (c+1)^3$, means $0 = t^2 + \frac{c^2}{c+1}t + (c+1)^2$, from Lemma $1(i)$, $0 = Tr\big(\frac{(c+1)^2}{c^4/(c+1)^2}\big) = Tr(\frac{c+1}{c}) = Tr\big(\frac{(c+1)^4}{c^4}\big) = Tr(1 + \frac{1}{c})$ if and only if there is two zeros. We know that $Tr_n(\frac{1}{c}) = 1$. In addition to this, because n odd n, $0 = Tr(1)$ then $0 = Tr(\frac{1}{c} + 1)$. We proved that there exists such a solution k since t satisfies the trace condition. There is two roots satisfying c-differential equation in odd case.

For even n, we now take the equation that

$$\frac{tc}{t^2 + c^2 + 1} = 1 + c + \frac{1}{c}$$

equals $t^2 + \frac{c^2}{1+c+c^2}t + (c+1)^2 = 0$. $0 = Tr\big(\frac{(c+1)^2}{c^4/(c+c^2+1)^2}\big) = Tr\big(\frac{(c^2+c+1)(c+1)}{c^2}\big) = Tr(\frac{c^3+1}{c^2}) = Tr(c) + Tr(\frac{1}{c^2}) = Tr(c) + Tr_(\frac{1}{c})$ if and only if there is two zeros, which is exactly true. When we take b as such solution t, then the trace condition holds. So, the c-differential equation has two solutions in even case. Since we got the results ${}_c\Delta_P(1, b) = 2$. desired in item (ii) of the theorem thanks to above first three cases, then we do not need to regard the Case 4, a and b are not equal to 0 or 1, which gives us the equation itself, $(x + a)^{2^n-2} + cx^{2^n-2} = b$.

□

Normally, PN only exist when p is odd for $c = 1$. However, Theorem $1(i)$ shows that there exists PcN functions for even characteristic, for all $c \neq 1$.

3.0.3.2 The Inverse Function in Odd Characteristic

When the finite field has odd characteristic, the following theorem shows these functions' differential behaviors under the notion of c. For each set Z, $[Z]^2$ in below theorem means the squares in this set.

Theorem 2. *[4]: Let P be the inverse function s.t. $P(x) = x^{2^n-2}$. Assume that c be an element from the field $\mathbb{F}_{p^n}$. Let p be odd prime :*

(i) P is c-planar function if c equals to zero (it means that P is a permutation polynomial).

(ii) $\delta_{P,c} = 3$ *if c is not equal to* $(-4c + c^2), \frac{1}{4}, 0, 4$ *is a square in the set* $[F_{p^n}]^2$*, or* $(-4c + 1)$ *is a square in* $[F_{p^n}]^2$*,*

(iii) $\delta_{P,c} = 2$ *if c is equal to*$\frac{1}{4}$ *or 4.*

(iv) P is c-almost perfect nonlinear if c is not equal to zero, $(-4c+c^2)$ *is not square in* $[F_{p^n}]^2$ *and* $(-4c + 1)$ *is not square in* $[F_{p^n}]^2$

Proof (i): We display first the c-differential equation at a

$$(x + \alpha)^{p^n-2} - cx^{p^n-2} = b \tag{3.2}$$

When c is equal to 0, the proof is as similar as in the even case since if b is equal to 0, $\alpha = x$ is merely one solution; if not, the equation $1 = b(x + \alpha)$ has only one root. There is only one solution for a,b $\in \mathbb{F}_{2^n}$, so F is PcN. □

Proof (ii), (iii) and (iv): For a, b $\in \mathbb{F}_{p^n}$, when $c \neq 0$, if $a = 0$, the equation 3.2 becomes $(1 + c)x^{p^n-2} = b(\star)$, which has at most one solution as in the case of $p = 2$. We will suppose that $a \neq 0$ after now on, assuming that $a = 1$, then we need to consider the equation $(x + 1)^{p^n-2} - cx^{p^n-2} = b$. Case 1: $b = 0$, the equation 3.2 becomes $(x + 1)^{p^n-2} - cx^{p^n-2} = 0$. It is obvious that $x = 0$ and $x = -1$ are not solutions for this equation. When $x \neq 0, -1$, by multiplying both sides of the equation $(\star)$, we have only one solution which is $x = \frac{c}{1-c}$ as in the even case. Case 2: $b = 1$, the equation 3.2 becomes $(x + 1)^{p^n-2} - cx^{p^n-2} = 1$. It has one solutions: $x = 0$ because $1 - c.0 = 1$, always true; $x = -1$, $0 - c.(-1) = 1$, a contradiction. When $x \neq 0, -1$, then the equation $x - c.(x + 1) = x(x + 1)$ is occured by multiplying $x(x + 1)$, which equals $x^2 + cx + x = 0$. By Lemma $1(ii)$, the discriminant becomes $d_1 = c^2 - 4c$ for this equation; it has two solutions if $d_1 \neq 0$ and unique solution if $d_1 = 0$. As a result, we get three solutions for the equation if $0 \neq d_1 \in [\mathbf{F}_{p^n}]^2$ and two solutions if $d_1 = 0$ with prior $x = 0$. (Here we get $x = -2$ as second solution since $c = 4$ $(\star)$ in this case, $x^2 + 4x + 4 = 0$). Case 3: $b \neq 0, 1$, $x = 0$ is not a solution since $1 - 0 = b$ which is a contradiction and $x = -1$ is a solution for the equation 3.2. We next suppose that $x \neq 0, -1$, 3.2 becomes $x - c(x + 1) = bx(x + 1)$. Assume $b = c \neq 0, 1$, then it renders $cx^2 + (2c - 1)^x + c = 0$ which is equivalent to $x^2 + (2 - \frac{1}{c}) + 1 = 0$. By Lemma $1(ii)$,

the discriminant becomes $d_2 = (2 - \frac{1}{c})^2 - 4c = \frac{1-4c}{c^2}$ for this equation; it has two solutions if $d_2 \neq 0$ and unique solution if $d_2 = 0$. Therefore, we get three solutions for the equation if $1 - 4c \neq 0$ ($c \neq 0$ from assumption) and two solutions if $d_1 = 0$ with prior $x = -1$ under the condition of $c = \frac{1}{4}$ ($\star\star$). Actually, the proof is done for (iii) because we got desired results in Theorem at ($\star$) and ($\star\star$).

Assume $b \neq 0, 1$. The equation 3.2 has no solution at $x = 0$ and $x = -1$. When $x \neq 0, -1$ multiplying the equation by $x(x+1)$ gives us the equation $x - c(x+1) = bx(x+1)$, derived at the beginning of this case. It equals to $x^2 + \left(\frac{b+c-1}{b}\right)x + \frac{c}{b}$. By Lemma 1($ii$), the discriminant becomes $d_3 = (b + c - 1/b)^2 - 4b/c$, that is $(b + c - 1)^2 = 4bc$ for this equation; it has two solutions if and only if $0 \neq d_3 = (b + c - 1)^2 - 4bc \in [\mathbf{F}_{p^n}]^2$ and one solution if and only if $d_3 = 0$.

When $c = -1$, $p = 3$ and $n = 2$, some b which satisfies this equation $(b + c + 1)^2 - 4bc = 0$ will occur only under this conditions. Now we claim that there exits b such that $(b + c + 1)^2 - 4bc \neq 0$ under the condition $c \neq -1$, $b \neq 0, 1, c$, $p \neq 3$ and $n \neq 2$.

When $c \neq -2, 2, 4$, taken b as $\frac{1}{2}(c - 2) \neq 0$, then the equation becomes
$(b + c + 1)^2 - 4bc = \frac{1}{4}(c - 4)^2 \neq 0$:

Now we will do some finite field constructions to make the proof more clear and understandable:

1. $p = 3$ and $n = 2$, if the primitive polynomial is $x^2 - x - 1$, then let β be the root of it. So, we can express the field as $\mathbf{F}_{3^2} = \frac{\mathbf{F}_3[x]}{<x^2-x-1>} = \mathbf{F}_3(\beta)$
2. $p = 5$ and $n = 2$, if the primitive polynomial is $x^2 - x + 2$, then let β be the root of it. So, we can express the field as $\mathbf{F}_{5^2} = \frac{\mathbf{F}_5[x]}{<x^2-x+2>} = \mathbf{F}_5(\beta)$.

When $c = 2$ or $c = 4$, p is not equal to 3 and 5, taken b as $2(c + 1)$, then the equation becomes $(b + c + 1)^2 - 4bc = (1 - c)^2 \neq 0$.

If $c = 2$ and $p = 3$, then the equation becomes $(b + c + 1)^2 - 4bc = b^2 + 1$: If $n > 2$, taken b as $\beta - \frac{1}{\beta}$, where β is a primitive root over $\mathbf{F}_{3^n}$. So, $b^2 + 1 = (\beta + \frac{1}{\beta})^2 \neq 0$. The equation 3.2 has two or fewer solutions; if $n = 2$, from Case 1: $d_1 = 2^2 - 4.2 = 2 = (\beta + 1)^2 \in [\mathbf{F}_{3^n}]^2 \neq 0$. Thus, 3.2 has at most two solutions which means its c-differential uniformity is 3. If $c = 2$, and $p = 5$, from Case 1: $d_1 = 2^2 - 4.2 = 1 = 1^2 \in [\mathbf{F}_{5^n}]^2 \neq 0$. It has at most two solutions which means its c-differential uniformity is again 3.

If $c = 4$ and $p = 3$, c equals to 1 in the modulo $p = 3$, which is a contradiction with our assumption. If $c = 4$ and $p = 5$, then the equation becomes $(b + c + 1)^2 - 4bc = b^2 + 4$: If $n > 2$, taken b as $\beta - \frac{1}{\beta}$, where β is a primitive root over $\mathbf{F}_{5^n}$. So, $b^2 + 4 = (2\beta + 2)^2 \neq 0$ when $b = \beta + 3 \neq 0, 1, -1$. When $c = -2$, from Case 3: $d_2 = (2 - \frac{1}{2})^2 - 4 = \frac{25}{4} - 4 = (\frac{3}{2})^2 \in [F_{5^2}]^2$. The equation has 3 solutions for $p \neq 3$, $d_2 \neq 0$. If p is equal to 3, then c would be -2, which is 1. This case is out of this theorem because it corresponds to usual derivative. All in all, the equation 3.2 has at most 3 solutions, so its c-differential uniformity is ≤ 3. This result proves the second item in Theorem 2.

□

3.0.3.3 c-Differential Uniformity of Modification of Inverse Function

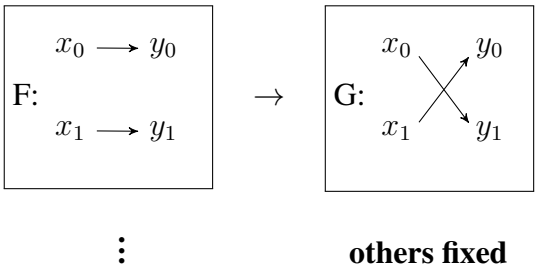
There are lots of ways constructed to modify the inverse functions in the previous studies under this new differential concept. They are examined c-differential behaviour of this modified version of the inverse function. For instance, adding some appropriate linearized monomials is one of these ways. One can observed that there is an increase in the value of their c-differential uniformity. The following theorem is achieved by Stanica and Geary in the paper [12].

Theorem 3. *Let $n \geq 4$, $F(x) = x^{2^n 2}$ be the inverse function on $\mathbb{F}_2^n$ and $1 \neq c \in \mathbb{F}_2^n$. Then, if n is even, the c-differential uniformity of $G(x) = F(x) + x$ is $\delta_{G,c} = 5$, for some c; if n is odd, there exist c such that $\delta_{G,c} = 4, 5$. Moreover, if $G(x) = F(x) + x^2$ and n is even, then there exists c such that $\delta_{G,c} = 5$; if n is odd and there exists a such that $Tr(\frac{a^2}{a^2+a+1}) = Tr(\frac{a^4}{(a+1)^5}) = 0$, , then $\delta_{G,c} = 5$ for some c.*
$\big($for example, $c = 1 + \frac{1}{(a^3+a^2+1)^{\frac{1}{2}}}\big)$

3.0.3.4 Swapped Inverse Function

The study area of this thesis is based on inverse functions which is one of the class of power functions. Another way to modify the inverse function is swapping two output points.

Consider a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and two points $x_0 \neq x_1 \in \mathbb{F}_{2^n}$,



From the scheme, as one can see that $G : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is a function such that $G(x_0) = y_1$, $G(x_1) = y_0$ and fixes remaining all values unlike the function F does, such that $F(x_0) = y_0$, $F(x_1) = y_1$. The new function G is a modified version of the original function F by changing two output points. Therefore, the function G is called the $\{x_0, x_1\}$-swapping of F, denoted by $G_{x_0x_1}$. It is formulated on $\mathbb{F}_{2^n}$ in the paper [11] as follows:

$$G_{x_0x_1} = F(x) + \big((x + x_0)^{p^n-1} + (x + x_1)^{p^n-1}\big)(y_0 + y_1)$$

More generally, we give its more general formula valid for all characterictic as follows:

$$G_{x_0x_1} = F(x) - \big((x - x_0)^{p^n-1} - (x - x_1)^{p^n-1}\big)(y_0 + y_1) \tag{3.3}$$

Throughout the thesis, we will symbolize it shortly by G if it won't cause confusion. In this thesis, we consider the (0,1)-swapping and the (0,α)-swapping of the inverse function $F = x^{2n-2}$. The following two sections are about these two modified version of inverse function and their c-differential uniformity.

3.0.3.5 The c-Differential Uniformity of the (0,1)-Swapped Inverse Function

For the inverse function $F(x) = x^{2^n-2}$ on $\mathbb{F}_{2^n}$, and two points $x_0 \neq x_1 \in \mathbb{F}_{2^n}$ such that $x_0 = 0$ and $x_1 = 1$. (Note that $F(0) = 0$ and $F(1) = 1$). One can obtained that its (0,1)-output swapping of inverse function by using the generalized formula

3.3 defined in the beginning of the Chapter 3 is the following way:

$$\begin{aligned} G_{0,1} &= x^{2^n-2} - \left((x-0)^{2^n-1} - (x-1)^{2^n-1}\right)(0+1) \\ &= x^{2^n-2} + x^{2^n-1} + (x-1)^{2^n-1} \end{aligned}$$

As one can see $G(0) = 1$, $G(1) = 0$ and for any α in $\mathbb{F}_{2^n}$ $G(\alpha) = \frac{1}{\alpha}$ like in the function F s.t. $F(\alpha) = \frac{1}{\alpha}$. (other elements are fixed). The following theorem is related to the c-differential uniformity of this swapped function G, coming from the article [11]. The given theorem leads our studies.

Theorem 4. *[11] Let n $\leq$ 2 be a positive integer, 0,1 $\neq$ c $\in \mathbb{F}_{p^n}$ and F: $\mathbb{F}_{p^n} \to \mathbb{F}_{2^n}$ be the inverse function defined by $F(x) = x^{2^n-2}$ and G be its $(0,1)$-swapping. If $n = 2$, then ${}_c\Delta_G(a,b) \leq 1$; if $n = 3$, then ${}_c\Delta_G(a,b) \leq 3$. If n $\geq$ 4, and for any a,b $\in \mathbb{F}_{p^n}$, the c-DDT entries satisfy ${}_c\Delta_G(a,b) \leq 4$ (all [1,2,3,4] c-DDT entries occur). Furthermore, ${}_c\Delta_G(a,b)$ =4 (so, the c-differential uniformity of G is $\delta_{F,c} = 4$) if and only if any of the conditions happen:*

(i) For a $\in \mathbb{F}_{2^n}^*$ with $Tr\left(\frac{a}{a+1}\right) = 0$, $b = \frac{1}{a+1}$ and $c = \frac{1}{a^2+a}$, then ${}_c\Delta_G(a, \frac{1}{a+1}) = 4$

(ii) For a $\in \mathbb{F}_{2^n}^*$ with $Tr\left(\frac{a}{(a+1)^2}\right) = 0$, $b = \frac{1}{a^2}$ and $c = \frac{a+1}{a^2}$ then, ${}_c\Delta_G(a, \frac{1}{a^2}) = 4$

Proof. See [11]. □

As we know that this theorem is about c-DDT entries of $\{0,1\}$-swapped form of a inverse function F in characteristic 2 and gives us two results. Firstly, it provides some bounds for c-DDT entries of swapped inverse function G according to changing n variables. Secondly it gives maximum value that c-DDT entries will attain under two specific conditions i and ii.

Based on Theorem 4, the c-differential uniformity of the $(0,\alpha)$-swapped inverse function will be discussed in details in the next Chapter.

CHAPTER 4

C-DIFFERENTIAL UNIFORMITY OF {0,α}- SWAPPED INVERSE FUNCTION

We work on the same function $F(x) = x^{2^n-2}$ on $\mathbb{F}_{2^n}$. As you know that above theorem is on $\{0,1\}$-swapping of this function , we focus on $\{0,\alpha\}$-swapping of it and we analyze its c-differential uniformity case by case throughout next two sections.

4.1 Preparation for Thesis Work

Before going into more detail, we need to prepare the equation used in the proof and analyzed. In Chapter 3, we created a formula to get the swapped function G that would allow us to construct this equation.

$$G(x) = x^{2^n-2} + \frac{x^{2^n-1}}{\alpha} + \frac{(x-\alpha)^{2^n-1}}{\alpha} \tag{4.1}$$

(Observe that while $F(0) = 0$ and $F(\alpha) = \frac{1}{\alpha}$ and $F(\beta) = \frac{1}{\beta}$ for any β in $\mathbb{F}_{2^n}$, $G(0) = \frac{1}{\alpha}$, $G(\alpha) = 0$ and $G(\beta) = \frac{1}{\beta}$ for any β, other elements are fixed.)

We can now construct the equation whose solutions gives us the entries of the c-DDT of G by using the definition below

$${}_c\Delta_G(a,b) = \#\{x \in \mathbb{F}_{p^n} : {}_cD_aG(x) = G(x+a) - c.G(x) = b\} \tag{4.2}$$

The equation to be actively used and analyzed in the proof is as follows:

$$
\begin{aligned}
{}_{\mathrm{c}}\Delta_G(a,b) = (x+a)^{2^n-2} - \frac{(x+a)^{2^n-1}}{\alpha} + \frac{(x-\alpha+a)^{2^n-1}}{\alpha} \\
+c.\left(x^{2^n-2} - \frac{x^{2^n-1}}{\alpha} + \frac{(x-\alpha)^{2^n-1}}{\alpha}\right) = b
\end{aligned}
\tag{4.3}
$$

4.2 An Approach to Thesis Work and The Results

After now on we extend above Theorem 4 related to c-differential uniformity of $\{0,1\}$-swapped inverse function to $\{0,\alpha\}$-swapped inverse function by using the idea behind this theorem. The obtained theorem and its proof in thesis study is as follows:

Theorem 5. *Let n $\leq$ 2 be a positive integer, 0,1 $\neq$ c $\in \mathbb{F}_{2^n}$ and F: $\mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be the inverse function defined by $F(x) = x^{2^n-2}$ and G be its $(0,\alpha)$-swapping. While $n \geq 5$, ${}_c\Delta_G(a,b)$ =4 (so, the c-differential uniformity of G is $\delta_{F,c} = 4$) if and only if any of the conditions happen:*

(i) For a $\in \mathbb{F}_{2^n}^*$ with $Tr\left(\frac{a}{a+\alpha}\right) = 0$, $b = \frac{1}{a+\alpha}$ and $c = \frac{\alpha^2}{a^2+a\alpha}$, then ${}_c\Delta_G(a, \frac{1}{a+\alpha}) = 4$

(ii) For a $\in \mathbb{F}_{2^n}^*$ with $Tr\left(\frac{a}{\alpha^2.(a+1)^2}\right) = 0$, $b = \frac{\alpha}{a^2}$ and $c = \frac{\alpha^2+\alpha.a}{a^2}$, then ${}_c\Delta_G(a, \frac{\alpha}{a^2}) = 4$

Proof. The proof is done for $n = 2, 3, 4$ in Theorem 4. So, we now assume n $\geq$ 5.

For a,b $\in \mathbb{F}_{2^n}$, we consider the c-differential equation (4.3). If a=0, then (4.3) becomes Solve for a sphere:

$$
\begin{aligned}
b &= x^{2^n-2} - \frac{x^{2^n-1}}{\alpha} + \frac{(x-\alpha)^{2^n-1}}{\alpha} + c.\left(x^{2^n-2} - \frac{x^{2^n-1}}{\alpha} + \frac{(x-\alpha)^{2^n-1}}{\alpha}\right) \\
&= (1+c)G(x)
\end{aligned}
$$

Since G is also a permutation, then there exists a unique solution x, regardless of what c$\neq$ 1, b$\in \mathbb{F}_{2^n}$. Thus, ${}_{\mathrm{c}}\Delta_G(0,b) = 1$. From now on, we will assume that a$\neq$ 0

Case 1. *Let a=*α*,* $b = 0$*. Then* (4.3) *becomes*

$$(x+\alpha)^{2^n-2} - \frac{(x+\alpha)^{2^n-1}}{\alpha} + \frac{x^{2^n-1}}{\alpha}$$
$$+c.\left(x^{2^n-2} - \frac{x^{2^n-1}}{\alpha} + \frac{(x-\alpha)^{2^n-1}}{\alpha}\right) = 0$$

Surely, $x = 0$ *is a solution if and only if* $\frac{1}{\alpha} - \frac{1}{\alpha} + 0 + c.\big(0 + 0 + \frac{1}{\alpha}\big) = 0$*, that is,* $c = 0$ *unless* $\alpha \neq 0, 1$*, a contradiction. If* $x = \alpha$*, then* $0 - 0 + \frac{1}{\alpha} + c.\big(\frac{1}{\alpha} - \frac{1}{\alpha} + 0\big) = 0$*, so* $\frac{1}{\alpha} = 0$ *, a contradiction . If* $x \neq 0, \alpha$*, then multiplying displayed equation by* $x(x+\alpha)$*, renders* $x + c.(x+\alpha) = 0$*, and so,* $x = \frac{c\alpha}{1+c}$*, which implies 1 →* ${}_c\Delta_G(\alpha, 0)$*.*

Case 2. *Let a=*α*, b=*α*. Then* (4.3) *becomes*

$$(x+\alpha)^{2^n-2} - \frac{(x+\alpha)^{2^n-1}}{\alpha} + \frac{x^{2^n-1}}{\alpha}$$
$$+c.\left(x^{2^n-2} - \frac{x^{2^n-1}}{\alpha} + \frac{(x-\alpha)^{2^n-1}}{\alpha}\right) = \alpha$$

If $x = 0$ *in* (4.3)*, then we must* $\frac{1}{\alpha} - \frac{1}{\alpha} + 0 + c.\big(0 + 0 + \frac{1}{\alpha}\big) = \alpha$*, so* $c = \alpha^2$*. This is a solution. If* $x = \alpha$*, then* $0 - 0 + \frac{1}{\alpha} + c.\big(\frac{1}{\alpha} - \frac{1}{\alpha} + 0\big) = \alpha$*, so* $\frac{1}{\alpha} = \alpha$*, which means* $\alpha^2 = 1$*, that is* $\alpha = 1$*, a contradiction . If* $x \neq 0, \alpha$*, then multiplying displayed equation by* $x(x+\alpha)$*, gives us*

$$x + c.(x+\alpha) = \alpha.x.(x+\alpha)\text{, that is, } \alpha.x^2 + (\alpha^2 + 1 + c).x + c.\alpha = 0$$

to apply Lemma 1 to this equation, firstly divide this equation by α*, and convert it to the desired form by Lemma 1. By Lemma 1, under* $\frac{\alpha^2+c+1}{\alpha} \neq 0$*, has two distinct solutions if and only if* $Tr\big(\frac{c.\alpha^2}{(\alpha^2+c+1)^2}\big) = 0$*, therefore, we have 3 →* ${}_c\Delta_G(\alpha, \alpha)$ *(including the prior x=0), under this conditions, and a contribution of 2, otherwise.*

Case 3. *Let a=*α*,* $b \neq 0, \alpha$*. Then* (4.3) *becomes*

$$(x+\alpha)^{2^n-2} - \frac{(x+\alpha)^{2^n-1}}{\alpha} + \frac{x^{2^n-1}}{\alpha}$$
$$+c.\left(x^{2^n-2} - \frac{x^{2^n-1}}{\alpha} + \frac{(x-\alpha)^{2^n-1}}{\alpha}\right) = b$$

If $x = 0$ *in* (4.3)*, then we must have* $\frac{1}{\alpha} - \frac{1}{\alpha} + 0 + c.\big(0 + 0 + \frac{1}{\alpha}\big) = b$*, so* $b = \frac{c}{\alpha}$*. which means that is a solution. So, 1 →* ${}_c\Delta_G(\alpha, \frac{c}{\alpha})$*. If* $x = \alpha$*, then* $0 - 0 + \frac{1}{\alpha} + c.\big(\frac{1}{\alpha} - \frac{1}{\alpha} + 0\big) = b$*, so* $\frac{1}{\alpha} = b$*, which means that this is also a solution since* $\alpha \neq 0, 1$ *and* $\alpha^2 \neq 1$*. If* $x \neq 0, \alpha$*, then multiplying displayed equation by* $x(x+\alpha)$*, gives us*

$$x + c.(x + \alpha) = b.x.(x + \alpha), \text{ that is, } b.x^2 + (b.\alpha + 1 + c).x + c.\alpha = 0$$

If we again divide both sides of this equation by b to apply Lemma 1 on it, then we can get two distinct solutions if and only if $Tr = \left(\frac{c.\alpha.b}{(b.\alpha+c+1)^2}\right) = 0$ *(of course, as long as* $\frac{b.\alpha+c+1}{b} \neq 0$*). Thus, if* $b = \frac{c}{\alpha}$*, and* $Tr(c) = 0$ *(since* $Tr(c^2) = 0$*), then 3* $\rightarrow {}_c\Delta_G(\alpha, \frac{c}{\alpha})$ *If* $b = \frac{c}{\alpha}$ *and* $Tr(c) = 1$ *then 1* $\rightarrow {}_c\Delta_G(\alpha, c)$*. If* $b \neq \frac{c}{\alpha}$*, and* $Tr = \left(\frac{c.\alpha.b}{(b.\alpha+c+1)^2}\right) = 0$*, then 2* $\rightarrow {}_c\Delta_G(\alpha, b)$*.*

Case 4. *Let* $a, b \neq 0, \alpha$*. Then the equation* (4.3) *would remain in its original form. All variables are active without any substitution. The equation we will examine is as follows:*

$$(x+a)^{2^n-2} - \frac{(x+a)^{2^n-1}}{\alpha} + \frac{(x-\alpha+a)^{2^n-1}}{\alpha} + c.\left(x^{2^n-2} - \frac{x^{2^n-1}}{\alpha} + \frac{(x-\alpha)^{2^n-1}}{\alpha}\right) = b$$

If $x = 0$ *in* (4.3)*, then we must have* $\frac{1}{a} - \frac{1}{\alpha} + \frac{1}{\alpha} + c.\left(0 + 0 + \frac{1}{\alpha}\right) = b$*, implies* $b = \frac{1}{a} + \frac{c}{\alpha}$*. Therefore, 1* $\rightarrow {}_c\Delta_G(a, \frac{1}{a} + \frac{c}{\alpha})$*. If* $x = \alpha$ *in* (4.3)*, then we must have* $\frac{1}{\alpha+a} - \frac{1}{\alpha} + \frac{1}{\alpha} + c.\left(\frac{1}{\alpha} - \frac{1}{\alpha} + 0\right) = b$*, implies* $b = \frac{1}{\alpha+a}$*. Hence, 1* $\rightarrow {}_c\Delta_G(a, \frac{1}{\alpha+a})$*. If* $x = a$*, then* $0 - 0 + \frac{1}{\alpha} + c.\left(\frac{1}{a} - \frac{1}{\alpha} + \frac{1}{\alpha}\right) = b$*, implies* $b = \frac{1}{\alpha} + \frac{c}{a}$*. Thus, 1* $\rightarrow {}_c\Delta_G(a, \frac{1}{\alpha} + \frac{c}{a})$*. If* $x = a + \alpha$ *in* (4.3)*, then we must have* $\frac{1}{\alpha} - \frac{1}{\alpha} + 0 + c.\left(\frac{1}{a+\alpha} - \frac{1}{\alpha} + \frac{1}{\alpha}\right) = b$*, implies* $b = \frac{c}{a+\alpha}$*. Therefore, 1* $\rightarrow {}_c\Delta_G(a, \frac{c}{a+\alpha})$*.*
Now assuming that $x = 0, \alpha, a, \alpha + a$*, multiplying Equation* (4.3) *by x.(x+a) and dividing by b renders*

$$x + c.(x + a) = b.x.(x + a), \text{ that is, } x^2 + \left(\frac{a.b+1+c}{b}\right).x + \frac{a.c}{b} = 0$$

By Lemma 1, under $\frac{a.b+1+c}{b} \neq 0$*. This equation has two distinct solutions if and only if* $Tr\left(\frac{a.b.c}{(a.b+c+1)^2}\right) = 0$

Now, we will do some calculations to determine the largest contributions to ${}_c\Delta_G(a, b)$*: As one can see, we got 4 conditions and we need to check whether there is a overlapped among them by equalizing the pairs. If we pair these conditions , 6 states would occur to examine.*

Four conditions are as follows:

(i) $x = 0$, *1* $\to {}_c\Delta_G(a, \frac{1}{a} + \frac{c}{\alpha})$

(ii) $x = \alpha$, *1* $\to {}_c\Delta_G(a, \frac{1}{\alpha+a})$

(iii) $x = a$, *1* $\to {}_c\Delta_G(a, \frac{1}{\alpha} + \frac{c}{a})$

(iv) $x = a + \alpha$, *1* $\to {}_c\Delta_G(a, \frac{c}{a+\alpha})$

Pairing and equalizing above conditions:

- *If* $b = \frac{1}{a} + \frac{c}{\alpha} = \frac{1}{\alpha+a}$, *that is,* $\alpha^2 = \alpha ac + a^2 c$
  $\big($*so,* $b = \frac{1}{a}$ *and* $c = \frac{\alpha^2}{\alpha.a+a^2}\big)$ *and* $Tr = \big(\frac{a.b.c}{(a.b+c+1)^2}\big) = Tr\big(\frac{a^2}{(\alpha+a)^2}\big) = Tr\big(\frac{a}{a+\alpha}\big) = 0$, *then 2* $\to {}_c\Delta_G(a, \frac{1}{\alpha+a})$
- *If* $b = \frac{1}{\alpha} + \frac{c}{\alpha} = \frac{1}{\alpha} + \frac{c}{a}$ *(so,* $c = 1$*), a contradiction.*
- *If* $b = \frac{1}{a} + \frac{c}{\alpha} = \frac{c}{\alpha+a}$, *that is,* $\alpha^2 + \alpha.a = a^2.c$
  (so, $b = \frac{\alpha}{a^2}$ *and* $c = \frac{\alpha^2+\alpha.a}{a^2}$*) and* $Tr\big(\frac{\alpha^2 a}{(a+\alpha)^3}\big) = 0$,
  then 4 $\to {}_c\Delta_G(a, \frac{\alpha}{a^2})$
- *If* $b = \frac{1}{\alpha+a} = \frac{1}{\alpha} + \frac{c}{a}$, *that is,* $a^2 = c.(\alpha^2 + \alpha.a)$
  (so, $b = \frac{1}{\alpha+a}$ *and* $c = \frac{a^2}{\alpha^2+\alpha.a}$*) and* $Tr = \big(\frac{a.b.c}{(a.b+c+1)^2}\big) = Tr\big(\frac{a^3}{(a^2+\alpha^2)^2}\big) = 0$,
  then 4 $\to {}_c\Delta_G(a, \frac{1}{\alpha+a})$
- *If* $b = \frac{1}{\alpha+a} = \frac{c}{\alpha+a}$ *(so,* $c = 1$*), a contradiction.*
- *If* $b = \frac{1}{\alpha} + \frac{c}{a} = \frac{c}{\alpha+a}$, *that is,* $\alpha^2.c = a^2 + \alpha.a$
  (so $b = \frac{a}{\alpha^2}$ *and* $c = \frac{a^2+\alpha.a}{\alpha^2}$*) and* $Tr = \big(\frac{a.b.c}{(a.b+c+1)^2}\big) = Tr\big(\frac{a^3}{(a^2.(a+\alpha)}\big) = 0$,
  then 4 $\to {}_c\Delta_G(a, \frac{a}{\alpha^2})$

Table 4.1: Results after pairing 6 states

States	conditions	c	b	a	$Tr\big(\frac{abc}{ab+c+1}\big)$	# of solutions
$x = 0 \wedge x = \alpha$	$\frac{1}{a} + \frac{c}{\alpha} = \frac{1}{\alpha+a}$	$\frac{\alpha^2}{\alpha.a+a^2}$	$\frac{1}{a}$	a	$Tr\big(\frac{a}{a+\alpha}\big)$	2
$x = 0 \wedge x = a$	$\frac{1}{\alpha} + \frac{c}{\alpha} = \frac{1}{\alpha} + \frac{c}{a}$	1	x	x	x	2
$x = 0 \wedge x = a + \alpha$	$\frac{1}{a} + \frac{c}{\alpha} = \frac{c}{\alpha+a}$	$\frac{\alpha^2+\alpha.a}{a^2}$	$\frac{\alpha}{a^2}$	a	$Tr\big(\frac{\alpha^2 a}{(a+\alpha)^3}\big)$	2
$x = \alpha \wedge x = a$	$b = \frac{1}{\alpha+a} = \frac{1}{\alpha} + \frac{c}{a}$	$\frac{a^2}{\alpha^2+\alpha.a}$	$\frac{1}{\alpha+a}$	a	$Tr\big(\frac{a^3}{(a^2+\alpha^2)^2}\big)$	2
$x = \alpha \wedge x = a + \alpha$	$\frac{1}{\alpha+a} = \frac{c}{\alpha+a}$	1	x	x	x	2
$x = a \wedge x = a + \alpha$	$\frac{1}{\alpha} + \frac{c}{a} = \frac{c}{\alpha+a}$	$c = \frac{a^2+\alpha.a}{\alpha^2})$	$\frac{a}{\alpha^2}$	a	$Tr\big(\frac{a^3}{(a^2.(a+\alpha)}\big)$	2

As one can see, we reached values $[1, 2, 3, 4]$ as c-DDT entries from cases. We proved that the c-differential uniformity is less than or equal to 4. Next, we claim that $(0, \alpha)$-swapped inverse function attains its maximum value 4 under some conditions: Since State 1 and State 6 collide with one other, we get just 2 solutions under $Tr\big(\frac{a}{a+\alpha}\big) = 0$ (observe that $Tr(\frac{1}{c}) = Tr(\frac{a}{\alpha}) + Tr(\frac{a^2}{\alpha^2}) = 0$). Therefore, $4 \rightarrow {}_{\mathrm{c}}\Delta_G(a, \frac{1}{\alpha+a})$ (including the prior in condition 1 and condition 2). Based on the same procedure, we get 2 solutions from State 3 and State 4 under $Tr\left(\frac{a}{\alpha^2.(a+1)^2}\right) = 0$. Hence, $4 \rightarrow {}_{\mathrm{c}}\Delta_G(a, \frac{\alpha}{a^2})$. We cannot get any solution from State 2 and State 5 because of $c \neq 1$. The value 4 will occur when we found parameters from the combinations of the previous four conditions. We reached 4 solutions under the conditions $Tr\big(\frac{a}{a+\alpha}\big) = 0$ and $Tr\left(\frac{a}{\alpha^2.(a+1)^2}\right) = 0$. This proves the first and second conditions in Theorem 5.

□

CHAPTER 5

CONCLUSION AND FUTURE WORKS

The behavior of the functions has attracted considerable interest, not just in terms of the usual derivative, but also in terms of the new differential notion. As the main conclusion of this thesis is about how the functions' behaviour against differential attacks under this new definitions. It is thought that differential cryptanalysis can take a different approach under this new concept. We especially concentrate on permutations because they are of particular significance to cryptography. Indeed, such functions are strong candidates for side-channel resistant functions due to their low multiplicative differential.

In introduction and preliminary part of the thesis, sufficient theoretical background information about subject and some neccessary lemmas used throughout thesis are given.

We presented some examples related to c-differential uniformity of some known functions such as Gold/Kasami, power, especially inverse functions. In accordance with this purpose, we analyze two Theorem 1 and 2 about the c-differential uniformity of inverse function in even, respectively, odd characteristic and we gave a broad proof in an explanatory way both of them. After giving deep analysis on the inverse function and their differential behaviours under this new notion, we also adapted a formula suggested by Stanica in [11] on even characteristic to odd characteristic. This formula allows to swap two outputs of a vectorial Boolean function. Based on Stanica's study on the c-differential uniformity of $\{0,1\}$-binary swapped inverse function $F(x) = 2^{n-2}$ on F_{2^n}, we firstly construct c-differential equation for $\{0,\alpha\}$-output

swapped inverse function and proposed a theorem to the c-differential uniformity of it and proved it case by case throughout the Chapter 4.

One can see that this theorem is about c-DDT entries of $\{0, \alpha\}$-swapped form of a inverse function F in characteristic 2 and gives us two results. Firstly, it provides some bounds for c-DDT entries of $\{0, \alpha\}$-swapped inverse function G according to changing n variables. In other words, we proved that its c-differential uniformity is less than or equal to 4. Secondly, it gives maximum value 4 that c-DDT entries attain under two specific conditions satisfied by trace mapping.

This overall analysis in Chapter 4 raises some important open questions. One of them is that whether there is any simple modification of the inverse function, $F(x) = x^{2^n-2}$ on F_{2^n}, based on two outputs swapping such as $\{0, 1+\alpha\}$, $\{1, \alpha\}$ or $\{\alpha, \beta\}$ for α,$\beta \in F_{2^n}$; whether there is any modification of the inverse function based on three outputs swapping such as $\{0, 1, \alpha\}$, for instance like $G(0) = \alpha$, $G(1) = 0$ and $G(\alpha) = \frac{1}{\alpha}$, or all these works can be searched for characteristic 3. All these are worthwhile to study their properties through the new differential. In addition to these, the c-differential uniformity of other AP/APN functions can be researched under this new multiplication.

REFERENCES

[1] D. Bartoli and M. Timpanella, On a generalization of planar functions, Journal of Algebraic Combinatorics, 52, pp. 187–213, 2020.

[2] E. Berlekamp, H. Rumsey, and G. Solomon, On the solution of algebraic equations over finite fields, Inf. Control., 10, pp. 553–564, 1967.

[3] E. Biham and A. Shamir, Differential cryptanalysis of des-like cryptosystems, in A. J. Menezes and S. A. Vanstone, editors, *Advances in Cryptology-CRYPTO' 90*, pp. 2–21, Springer Berlin Heidelberg, Berlin, Heidelberg, 1991, ISBN 978-3-540-38424-3.

[4] P. Ellingsen, P. Felke, C. Riera, P. Stanica, and A. Tkachenko, c-differentials, multiplicative uniformity and (almost) perfect c-nonlinearity, 2019.

[5] P. Ellingsen, P. Felke, C. Riera, P. Stănică, and A. Tkachenko, c-differentials, multiplicative uniformity, and (almost) perfect c-nonlinearity, IEEE Transactions on Information Theory, 66(9), pp. 5781–5789, 2020.

[6] S. U. Hasan, M. Pal, C. Riera, and P. Stănică, On the c-differential uniformity of certain maps over finite fields, Des. Codes Cryptogr., 89, pp. 221–239, 2021.

[7] T. Helleseth, C. Rong, and D. Sandberg, New families of almost perfect nonlinear power mappings, IEEE Trans. Inf. Theory, 45, pp. 475–485, 1999.

[8] T. Helleseth and D. Sandberg, Some power mappings with low differential uniformity, Applicable Algebra in Engineering, Communication and Computing, 8, pp. 363–370, 1997.

[9] L. Kölsch, On ccz-equivalence of the inverse function, arXiv:2008.08398, 2020.

[10] C. Riera and P. Stănică, Some c-(almost) perfect nonlinear functions, ArXiv, abs/2010.10023, 2020.

[11] P. Stănică, Low c-differential and c-boomerang uniformity of the swapped inverse function, Discret. Math., 344, p. 112543, 2021.

[12] P. Stănică and A. Geary, The c-differential behavior of the inverse function under the ea-equivalence, Cryptography and Communications, pp. 1–12, 2021.

[13] Y. Xia, X. Zhang, C. Li, and T. Helleseth, The differential spectrum of a ternary power mapping, Finite Fields Their Appl., 64, p. 101660, 2020.

[14] H. Yan and Z. Zhou, Power functions over finite fields with low c-differential uniformity, ArXiv, abs/2003.13019, 2020.

Appendix A

SOME APPENDICES

Figure A.1: for $\alpha = 0, 1, 2, 3$

x	S(x)	x⊕0	S(x⊕0)	β=S(x⊕0)⊕S(x)	x⊕1	S(x⊕1)	β=S(x⊕1)⊕S(x)	x⊕2	S(x⊕2)	β=S(x⊕2)⊕S(x)	x⊕3	S(x⊕3)	β=S(x⊕3)⊕S(x)
0	8	0	8	0	1	15	7	2	5	13	3	10	2
1	15	1	15	0	0	8	7	3	10	5	2	5	10
2	5	2	5	0	3	10	15	0	8	13	1	15	10
3	10	3	10	0	2	5	15	1	15	5	0	8	2
4	2	4	2	0	5	11	9	6	6	4	7	13	15
5	11	5	11	0	4	2	9	7	13	6	6	6	13
6	6	6	6	0	7	13	11	4	2	4	5	11	13
7	13	7	13	0	6	6	11	5	11	6	4	2	15
8	13	8	13	0	9	10	7	10	5	8	11	7	10
9	10	9	10	0	8	13	7	11	7	13	10	5	15
10	5	10	5	0	11	7	2	8	13	8	9	10	15
11	7	11	7	0	10	5	2	9	10	13	8	13	10
12	9	12	9	0	13	11	2	14	1	8	15	15	6
13	11	13	11	0	12	9	2	15	15	4	14	1	10
14	1	14	1	0	15	15	14	12	9	8	13	11	10
15	15	15	15	0	14	1	14	13	11	4	12	9	6

Figure A.2: for $\alpha = 4, 5, 6, 7$

x⊕8	S(x⊕8)	β=S(x⊕8)⊕S(x)	x⊕9	S(x⊕9)	β=S(x⊕9)⊕S(x)	x⊕10	S(x⊕10)	β=S(x⊕10)⊕S(x)	x⊕11	S(x⊕11)	β=S(x⊕11)⊕S(x)
8	13	5	9	10	2	10	5	13	11	7	15
9	10	5	8	13	2	11	7	8	10	5	10
10	5	0	11	7	2	8	13	8	9	10	15
11	7	13	10	5	15	9	10	0	8	13	7
12	9	11	13	11	9	14	1	3	15	15	13
13	11	0	12	9	2	15	15	4	14	1	10
14	1	7	15	15	9	12	9	15	13	11	13
15	15	2	14	1	12	13	11	6	12	9	4
0	8	5	1	15	2	2	5	8	3	10	7
1	15	5	0	8	2	3	10	0	2	5	15
2	5	0	3	10	15	0	8	13	1	15	10
3	10	13	2	5	2	1	15	8	0	8	15
4	2	11	5	11	2	6	6	15	7	13	4
5	11	0	4	2	9	7	13	6	6	6	13
6	6	7	7	13	12	4	2	3	5	11	10
7	13	2	6	6	9	5	11	4	4	2	13

Figure A.3: for $\alpha = 8, 9, 10, 11$

x⊕8	S(x⊕8)	β=S(x⊕8)⊕S(x)	x⊕9	S(x⊕9)	β=S(x⊕9)⊕S(x)	x⊕10	S(x⊕10)	β=S(x⊕10)⊕S(x)	x⊕11	S(x⊕11)	β=S(x⊕11)⊕S(x)
8	13	5	9	10	2	10	5	13	11	7	15
9	10	5	8	13	2	11	7	8	10	5	10
10	5	0	11	7	2	8	13	8	9	10	15
11	7	13	10	5	15	9	10	0	8	13	7
12	9	11	13	11	9	14	1	3	15	15	13
13	11	0	12	9	2	15	15	4	14	1	10
14	1	7	15	15	9	12	9	15	13	11	13
15	15	2	14	1	12	13	11	6	12	9	4
0	8	5	1	15	2	2	5	8	3	10	7
1	15	5	0	8	2	3	10	0	2	5	15
2	5	0	3	10	15	0	8	13	1	15	10
3	10	13	2	5	2	1	15	8	0	8	15
4	2	11	5	11	2	6	6	15	7	13	4
5	11	0	4	2	9	7	13	6	6	6	13
6	6	7	7	13	12	4	2	3	5	11	10
7	13	2	6	6	9	5	11	4	4	2	13

Figure A.4: for $\alpha = 12, 13, 14, 15$

x⊕12	S(x⊕12)	β=S(x⊕12)⊕S(x	x⊕13	S(x⊕13)	β=S(x⊕13)⊕S(x)	x⊕14	S(x⊕14	β=S(x⊕14)⊕S(x)	x⊕15	S(x⊕15)	β=S(x⊕15)⊕S(x)
12	9	1	13	11	3	14	1	9	15	15	7
13	11	4	12	9	6	15	15	0	14	1	14
14	1	4	15	15	10	12	9	12	13	11	14
15	15	5	14	1	11	13	11	1	12	9	3
8	13	15	9	10	8	10	5	7	11	7	5
9	10	1	8	13	6	11	7	12	10	5	14
10	5	3	11	7	1	8	13	11	9	10	12
11	7	10	10	5	8	9	10	7	8	13	0
4	2	15	5	11	6	6	6	11	7	13	0
5	11	1	4	2	8	7	13	7	6	6	12
6	6	3	7	13	8	4	2	7	5	11	14
7	13	10	6	6	1	5	11	12	4	2	5
0	8	1	1	15	6	2	5	12	3	10	3
1	15	4	0	8	3	3	10	1	2	5	14
2	5	4	3	10	11	0	8	9	1	15	14
3	10	5	2	5	10	1	15	0	0	8	7