On Equivalence of Known Families of APN Functions in Small Dimensions

Bo Sun
University of Bergen
Bergen, Norway
Bo.Sun@uib.no

***Abstract*—In this extended abstract, we computationally check and list the CCZ-inequivalent APN functions from infinite families on $\mathbb{F}_{2^n}$ for n from 6 to 11. These functions are selected with simplest coefficients from CCZ-inequivalent classes. This work can simplify checking CCZ-equivalence between any APN function and infinite APN families.**

I. Introduction

A cryptosystem is the system provides encryption and decryption. Algorithms, protocols, keys are the fundamental components in any cryptosystem. Algorithms impact how the encryption and decryption take place and they encompass symmetric algorithms and asymmetric algorithms. Symmetric algorithms use same keys for encryption and decryption, while asymetrric algorithms use different keys. DES, AES, and blowfish are well known symmetric algorithms. Symmetric algorithms are the oldest and most used algorithms among cryptosystems. Symmetric algorithms have two main types, one is block cipher which encrypts fixed-size blocks at a time and the other one is stream cipher which encrypts one bit or byte at a time.

One critical component in symmetric block cipher is substitution-box (S-box). Substitution substitutes some values to other values instead. The design of S-boxes in symmetric block cipher is based on Claude Elwood Shannon's theory about designing secure cryptosystems. Shannon is called the father of contemporary cryptography. In particular, he theoretically deduced that both confusion and diffusion should be present in a computationally secure cryptosystem. Confusion is for making the relation between ciphertext and keys as complex as possible. Diffusion is for spreading the influence of any bit of plaintext over ciphertext as much as possible.

S-boxes provide confusion for symmetric block cipher cryptosystems. They take some number of bits of input from one finite field and transform them into output from other finite field. The reasons that S-boxes are the most critical components in symmetric block cipher are as following: 1) They are the only nonlinear components in block cipher; 2) They provide confusion to block cipher; 3) There is strong connection between cryptographic attacks and certain properties of S-boxes.

II. Preliminaries

For positive integers n and m, a Boolean function f is a function from finite filed $\mathbb{F}_{2^n}$ to finite filed $\mathbb{F}_2$. Likewise, a function F is a vectorial Boolean function if it is from finite filed $\mathbb{F}_{2^n}$ to another finite filed $\mathbb{F}_{2^m}$. Any vectorial boolean function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ can be represented by m Boolean functions as $F(x_1, x_2, ..., x_n) = \{f_1(x_1, x_2, ..., x_n), ..., f_m(x_1, x_2, ..., x_n)\}$. $f_1, f_2...f_m$ are called coordinate functions of F and each of them has n variables. Any nonzero linear combination of the coordinate functions is called a component function of F. The mathematical nature of S-boxes is represented by vectorial Boolean functions.

As we mentioned, there is close connection between successfulness of many attacks on symmetric block cipher and certain properties of S-boxes (or vectorial Boolean functions). Two most well known and powerful attacks on block cipher are linear attacks and differential attacks. Linear attacks try to find the linear relationship between plaintext and ciphertext in order to deduce keys. Nonlinearity of S-boxes (defined below) can measure the resistance of block cipher to linear attacks. Differential attacks study how the difference of input can impact the difference of output. The differential uniformity of S-boxes (defined below) define the resistibility to differential attacks. Correspondingly, algebraic degree of S-boxes matters with the resistance to high order differential attacks. The low degree multivariate equation of S-boxes influences the resistance to algebraic attacks. The univariate polynomial degree of S-boxes measures the ability against interpolation attacks. There are also other attacks, the resistance to those attacks highly depend on one or more properties of S-boxes. In this extended abstract, we will only focus on nonlinearity, differential uniformity and algebraic degree of S-boxes.

The nonlinearity of any vectorial Boolean function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ is the minimum hamming distance between all nonzero linear Boolean functions over $\mathbb{F}_{2^n}$ and component functions of F. The nonlinearity $N(F)$ can also be represented by Walsh transofrm. Walsh transform λ_F is defined as:

$$\lambda_F(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{b \cdot F(x) + a \cdot x}, a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^m}^*,$$

and corresponding Walsh spectrum is the set as following:

$$\{\lambda_F(a,b) : a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^m}^*\}.$$

Then the nonlinearity of F equals:

$$N(F) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^m}^*} |\lambda_F(a,b)|.$$

ISSN 2305-7254

TABLE I
KNOWN APN POWER FUNCTIONS x^d ON $\mathbb{F}_{2^n}$

Functions	Exponents d	Conditions	Proven
Gold	2^i+1	$\gcd(i,n)=1$	[7], [8]
Kasami	$2^{2i}-2^i+1$	$\gcd(i,n)=1$	[9], [10]
Welch	2^t+3	3	[11]
Niho	$2^t+2^{\frac{t}{2}}-1$, t even $2^t+2^{\frac{3t+1}{2}}-1$, t odd	$n=2t+1$	[12]
Inverse	$2^{2t}-1$	$n=2t+1$	[13], [8]
Dobbertin	$2^{4i}+2^{3i}+2^{2i}+2^i-1$	$n=5i$	[14]

TABLE II
FAMILIES OF APN POLYNOMIAL FUNCTIONS ON $\mathbb{F}_{2^n}$

N°	Functions	Conditions	References
1-2	$x^{2^s+1}+\alpha^{2^k-1}x^{2^{ik}+2^{mk+s}}$	$n=pk$, $\gcd(k,p)=\gcd(s,pk)=1$, $p\in\{3,4\}$, $i=sk \bmod p$, $m=p-i$, $n\geq 12$, α primitive in $\mathbb{F}_{2^n}^*$	[15]
3	$x^{2^{2i}+2^i}+bx^{q+1}+cx^{q(2^{2i}+2^i)}$	$q=2^m$, $n=2m$, $\gcd(i,m)=1$, $\gcd(2^i+1,q+1)\neq 1, cb^q+b\neq 0$, $c\notin\{\lambda^{(2^i+1)(q-1)},\lambda\in\mathbb{F}_{2^n}\}, c^{q+1}=1$	[16]
4	$x(x^{2^i}+x^q+cx^{2^iq})$ $+x^{2^i}(c^qx^q+sx^{2^iq})+x^{(2^i+1)q}$	$q=2^m, n=2m, \gcd(i,m)=1$, $c\in\mathbb{F}_{2^n}, s\in\mathbb{F}_{2^n}\setminus\mathbb{F}_q$, $X^{2^i+1}+cX^{2^i}+c^qX+1$ is irreducible over $\mathbb{F}_{2^n}$	[16]
5	$x^3+a^{-1}\mathrm{tr}_1^n(a^3x^9)$	$a\neq 0$	[17], [18]
6	$x^3+a^{-1}\mathrm{tr}_3^n(a^3x^9+a^6x^{18})$	$3\|n$, $a\neq 0$	[17]
7	$x^3+a^{-1}\mathrm{tr}_3^n(a^6x^{18}+a^{12}x^{36})$	$3\|n$, $a\neq 0$	[17]
8-10	$ux^{2^s+1}+u^{2^k}x^{2^{-k}+2^{k+s}}+$ $vx^{2^{-k}+1}+wu^{2^k+1}x^{2^s+2^{k+s}}$	$n=3k$, $\gcd(k,3)=\gcd(s,3k)=1$, $v,w\in\mathbb{F}_{2^k}, vw\neq 1$, $3\|(k+s)$, u primitive in $\mathbb{F}_{2^n}^*$	[19]
11	$\alpha x^{2^s+1}+\alpha^{2^k}x^{2^{k+s}+2^k}+$ $\beta x^{2^k+1}+\sum_{i=1}^{k-1}\gamma_i x^{2^{k+i}+2^i}$	$n=2k$, $\gcd(s,k)=1$, s,k odd, $\beta\notin\mathbb{F}_{2^k}, \gamma_i\in\mathbb{F}_{2^k}$, α not a cube	[19], [20]

The higher is the nonlinearity $N(F)$, the better is the resistance of F to linear attacks. There is a universal upper bound of nonlinearity for any vectorial Boolean function.

It means any vectorial Boolean function's nonlinearity is lower or equal than this uppper bound. The bound is $2^{n-1}-2^{\frac{n}{2}-1}$ for any vectorial Boolean function $F:\mathbb{F}_{2^n}\to\mathbb{F}_{2^m}$. Functions which achieve this bound are called bent functions. Since bent functions have the highest nonlinearity, so they are optimal against linear attacks. Bent functions only exist when n is even and $m\leq n/2$. When $n=m$ and n is odd, the upper bound is smaller and changes to $N(F)\leq 2^{n-1}-2^{\frac{n-1}{2}}$. Functions which achieve this bound when n is odd are Almost Bent(AB) functions. When $n=m$ and n is even, it is conjectured that the bound is $N(F)\leq 2^{n-1}-2^{\frac{n}{2}}$.

A vectorial Boolean functions $F:\mathbb{F}_{2^n}\to\mathbb{F}_{2^m}$ is differential δ-uniform if the equations

$$F(x+a)-F(x)=b,\qquad \forall a\in\mathbb{F}_{2^n}^*,\quad \forall b\in\mathbb{F}_{2^m},$$

have at most δ solutions. The lower is the differential uniformity, the better is the resistance to differential attacks. Differential uniformity δ has lower bound if $n\neq m$ as $\delta\geq 2^{(n-m)}$. Functions achieve this bound are Perfect Non-linear(PN) functions. A function is PN if and only if it is bent. Since bent functions have highest nonlinearity, thus PN (or bent functions) have highest nonlinearity and lowest uniformity. When $n=m$, the functions with lowest possible differential uniformity are Almost Perfect Nonlinear (APN) functions which are 2-uniform. Every AB function is APN, but the converse is not true. Any vectorial Boolean function $F:\mathbb{F}_2^n\to\mathbb{F}_2^m$ can be represented by its Algebraic Normal Form (ANF) as follow:

$$F(x_1,...,x_n)=\sum_{u\in\mathbb{F}_2^n}a_u\prod_{i=1}^{n}x_i^{u_i},\ \ a_u\in\mathbb{F}_2^m,\ \ u=(u_1,...,u_n).$$

The degree of F - $d^\circ(F)$ is the degree of its ANF. F is affine if $d^\circ(F)\leq 1$ and it is quadratic if $d^\circ(F)=2$. If $n=m$, F can be represented as univariate polynomial over $\mathbb{F}_{2^n}$:

$$F(x)=\sum_{i=0}^{2^n-1}c_ix^i,\quad c_i\in\mathbb{F}_{2^n}.$$

We denote tr_m^n as the trace functions from $\mathbb{F}_{2^n}\to\mathbb{F}_{2^m}$:

$$\mathrm{tr}_m^n(x)=x+x^{2^m}+x^{2^{2m}}+\cdots+x^{2^{(n/m-1)m}},$$

TABLE III
CCZ-INEQUIVALENT APN FUNCTIONS OVER $\mathbb{F}_{2^n}$ FROM THE KNOWN APN CLASSES ($6 \leq n \leq 11$ AND a PRIMITIVE IN $\mathbb{F}_{2^n}$)

n	N°	Functions	Families from Tables I,II	Relation to [22]
6	6.1	x^3	Gold	Table 5: N°1.1
	6.2	$x^6 + x^9 + a^7x^{48}$	N°3	5: N°1.2
	6.3	$ax^3 + a^4x^{24} + x^{17}$	N°8-10	5: N°2.3
7	7.1	x^3	Gold	Table 7 : N°1.1
	7.2	x^5	Gold	7 : N°3.1
	7.3	x^9	Gold	7 : N°4.1
	7.4	x^{13}	Kasami	7 : N°5.1
	7.5	x^{57}	Kasami	7 : N°6.1
	7.6	x^{63}	Inverse	7 : N°7.1
	7.7	$x^3 + \mathrm{tr}_1^7(x^9)$	N°5	7 : N°1.2
8	8.1	x^3	Gold	Table 9 : N°1.1
	8.2	x^9	Gold	9 : N°1.2
	8.3	x^{57}	Kasami	9 : N°7.1
	8.4	$x^3 + x^{17} + a^{48}x^{18} + a^3x^{33} + ax^{34} + x^{48}$	N°4	9 : N°2.1
	8.5	$x^3 + \mathrm{tr}_1^8(x^9)$	N°5	9 : N°1.3
	8.6	$x^3 + a^{-1}\mathrm{tr}_1^8(a^3x^9)$	N°5	9 : N°1.5
9	9.1	x^3	Gold	
	9.2	x^5	Gold	
	9.3	x^{17}	Gold	
	9.4	x^{13}	Kasami	
	9.5	x^{241}	Kasami	
	9.6	x^{19}	Welch	
	9.7	x^{255}	Inverse	
	9.8	$x^3 + \mathrm{tr}_1^9(x^9)$	N°5	
	9.9	$x^3 + \mathrm{tr}_3^9(x^9 + x^{18})$	N°6	
	9.10	$x^3 + \mathrm{tr}_3^9(x^{18} + x^{36})$	N°7	
10	10.1	x^3	Gold	
	10.2	x^9	Gold	
	10.3	x^{57}	Kasami	
	10.4	x^{339}	Dobbertin	
	10.5	$x^6 + x^{33} + a^{31}x^{192}$	N°3	
	10.6	$x^{72} + x^{33} + a^{31}x^{258}$	N°3	
	10.7	$x^3 + \mathrm{tr}_1^{10}(x^9)$	N°5	
	10.8	$x^3 + a^{-1}\mathrm{tr}_1^{10}(a^3x^9)$	N°5	
11	11.1	x^3	Gold	
	11.2	x^5	Gold	
	11.3	x^9	Gold	
	11.4	x^{17}	Gold	
	11.5	x^{33}	Gold	
	11.6	x^{13}	Kasami	
	11.7	x^{57}	Kasami	
	11.8	x^{241}	Kasami	
	11.9	x^{993}	Kasami	
	11.10	x^{35}	Welch	
	11.11	x^{287}	Niho	
	11.12	x^{1023}	Inverse	
	11.13	$x^3 + \mathrm{tr}_1^{11}(x^9)$	N°5	

and we write tr_1^n when $m = 1$.

There are three equivalence relations of vectorial Boolean functions which keep the uniformity (APN-ness) and nonlinearity (AB-ness) the same. They are affine-equivalence, Extended Affine (EA)-equivalence and Carlet-Charpin-Zinoview (CCZ)-equivalence. CCZ-equivalence is more general than EA-equivalence and EA-equivalence is more general than affine-equivalence.

For example, if two vectorial Boolean functions are affine-equivalent, they are also EA and CCZ-equivalent, however if two functions are CCZ-equivalent, they may not be affine or EA-equivalent. In particular, CCZ-equivalence doesn't preserve the algebraic degree, but affine and EA-equivalence do. Two vectorial Boolean functions F,F': $\mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ are affine-equivalent if $F' = A_1 \circ F \circ A_2$. Likewise, they are EA-equivalent if $A_1 \circ F \circ A_2 + A$, which A_1 is affine permuation on $\mathbb{F}_{2^m}$, A_2 is affine permutation on $\mathbb{F}_{2^n}$, A is affine functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$.

F and F' are called CCZ-equivalent if there exists affine permutation L on $\mathbb{F}_2^n \times \mathbb{F}_2^m$, which makes $\mathcal{L}(G_F) = G_{F'}$, where $G_F = \{(x, F(x)) : x \in \mathbb{F}_2^n\} \subset \mathbb{F}_2^n \times \mathbb{F}_2^m$, $G'_F = \{(x, F'(x)) : x \in \mathbb{F}_2^n\} \subset \mathbb{F}_2^n \times \mathbb{F}_2^m$.

As we mentioned, EA-equivalences are special cases of CCZ-equivalences. There are some cases when they coincide:
1) Boolean functions [1];
2) Bent functions [2];
3) Two quadratic APN functions [3];
4) If a quadratic APN function is CCZ-equivalent to a power function then they are EA-equivalent [4];
5) For $n \geq 3$, two power APN functions are CCZ-equivalent if and only if they are EA-equivalent or one of them is EA-equivalent to the inverse of the other one [4].

In contrast, for functions from $\mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$, $m \geq 2$, CCZ-equivalence is different from EA-equivalence [5],[6].

III. Known Families of APN functions

Until now, there are 17 known infinite families of APN functions. Among them are 6 families of power functions.

A. Families of Power APN

Talbe I lists all the power APN functions on $\mathbb{F}_{2^n}$. Welch, Niho, Gold with n odd and Kasami with n odd are AB functions. Their Walsh spectra are $\{0, \pm 2^{(n+1)/2}\}$. In contrast, Inverse, Dobbertin, Gold with n even and Kasami with n even are not AB. When n is even, Gold and Kasami functions have the Walsh spectra $\{0, \pm 2^{n/2}, \pm 2^{(n+2)/2}\}$. For $n \leq 5$, all APN functions are CCZ-equivalent to power functions.

B. Families of APN Polynomials

Table II lists all the known families of APN polynomials. They are all quadratic. When n is odd, all these polynomials are AB functions.

IV. Simplification of known APN families

As we can see from Talbe I and Talbe II, there are many APN functions in each APN family. In particular, there are many coefficients and many parameters in the families of APN polynomials. For example, when $n = 10$, only family NO.3 in Table II already has 45012 APN functions. So it is very difficult to check the equivalence of a given APN function to both monomial and polynomial families.

Not only polynomial APN are complex to compare with, APN power functions are the same. In [21], they alleged that they have found a new APN family, but it was proved their result is affine equivalent to Gold family. These motivate us to simplify the families and make a list that for given n, all functions are CCZ-inequivalent. Taking family NO.3 for $n = 10$ for example to explain what we do. Firstly, we found all the value range for each parameter, then we found 45012 APN functions. Secondly, we compare all 45012 APN functions with each other, then we found two CCZ-inequivalent classes. Next, from each class, we choose one representative APN function with simplest coefficients. Fianlly, we check CCZ-equivalence between these two representatives with other families for $n = 10$. In the end, both two representatives are CCZ-inequivalent with other families. Thus, we put them into our table.

Table III contains all APN functions from $n = 6$ to $n = 11$ and they are CCZ-inequivalent between each other for given n. In the future, people can compare with this table for $n = 6$ to $n = 11$ instead of comparing with each function in every known APN family again. We also compare the result with the known APN functions from [22].

In addition, we observe that when n is odd and not divisible by 3, there is only one APN polynomial (up to CCZ-equivalence) provided by the known families of APN polynomials $x^3 + \mathrm{tr}_1^n(x^9)$.

V. Conclusion and future work

In this extended abstract, we check CCZ-equivalence for functions within known families of APN functions and compare them with each other. We present a list of CCZ-inequivalent APN functions for n from 6 to 11 provided by the known APN families. This work can facilitate to find new APN families for constructing more secure cryptosystems or for enriching knowledge in mathematics or other fields. In the future, we plan to extend the list for bigger n and try to find some rules behind the results.

References

[1] L.Budaghyan, C.Carlet, "CCZ-equivalence of single and multi output Boolean functions", *Post-proceedings of the 9-th International Conference on Finite Fields and Their Applications Fq'09, Contemporary Math.*, AMS, vol. 518, 2010, pp. 43-54.

[2] L. Budaghyan, C. Carlet, "CCZ-equivalence of bent vectorial functions and related constructions",*Designs, Codes and Cryptography*, vol 59(1), 2011, pp. 69-87.

[3] S. Yoshiara, "Equivalences of quadratic APN functions", *Journal of Algebraic Combinatorics*, vol.35(3), 2012, pp. 461-475.

[4] S. Yoshiara, "Equivalences of power APN functions with power or quadratic APN functions", *Journal of Algebraic Combinatorics*, vol.35(3), 2016, pp. 561-585.

[5] L. Budaghyan, C. Carlet, "CCZ-equivalence of single and multi-output Boolean functions", *Post-proceedings of the 9th International Conference on Finite Fields and Their Applications Fq'09, Contemporary Mathematics*, vol. 518, 2010, pp. 43-54.

[6] L. Budaghyan, T. Helleseth, "Planar functions and commutative semifields", *Tatra. Mt. Math. Publ.* vol.45,2010, pp. 15-45.

[7] R. Gold, "Maximal recursive sequences with 3-valued recursive cross-correlation functions", *IEEE Trans. Inform. Theory*, vol.14, 1986, pp. 154-156.

[8] K. Nyberg, "Differentially uniform mappings for cryptography", *Advances in Cryptography, EUROCRYPT'93*, LNCS, vol.765, 1994, pp. 55-64.

[9] H. Janwa, R. Wilson, "Hyperplane sections of Fermat varieties in P^3 in char. 2 and some applications to cyclic codes", *Proceedings of AAECC-10*, LNCS, vol. 673, 1993, pp. 180-194. Berlin: Springer-Verlag.

[10] T. Kasami, "The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes", *Inform. and Control*, vol.18, 1971, pp. 369-394.

[11] H. Dobbertin, "Almost perfect nonlinear power functions over $GF(2^n)$ the Welch case", *IEEE Trans. Inform. Theory*, vol.45, 1999, pp. 1271-1275.

[12] H. Dobbertin, "Almost perfect nonlinear power functions over $GF(2^n)$: the Niho case", *Inform. and Comput.*, vol.151, 1999, pp. 57-72.

[13] T. Beth, C. Ding, "On almost perfect nonlinear permutations", *Advances in Cryptology-EUROCRYPT'93*, LNCS, vol.765, 1993, pp. 65-76, New York: Springer-Verlag.

[14] H. Dobbertin, "Almost perfect nonlinear power functions over $GF(2^n)$: a new case for n divisible by 5", *Proceedings of Finite Fields and Applications Fq5*, 2000, pp. 113-121.

[15] L. Budaghyan, C. Carlet, G. Leander, "Two classes of quadratic APN binomials inequivalent to power functions", *IEEE Trans. Inform. Theory*, vol.54(9), 2008, pp. 4218-4229.

[16] L. Budaghyan, C. Carlet, "Classes of quadratic APN trinomials and hexanomials and related structures", *IEEE Trans. Inform. Theory*, vol.54(5), 2008, pp. 2354-2357.

[17] L. Budaghyan, C. Carlet, G. Leander, "Constructing new APN functions from known ones", *Finite Fields and Their Applications*, vol 15(2), 2009, pp. 150-159.

[18] L. Budaghyan, C. Carlet, G. Leander, "On a construction of quadratic APN functions", *IEEE Information Theory Workshop*, 2009, pp. 374-378.

[19] C. Bracken, E. Byrne, N.Markin, G. McGuire, "A few more quadratic APN functions", *Cryptography and Communications*, vol.3(1), 2011, pp. 43-53.

[20] C. Bracken, E. Byrne, N.Markin, G. McGuire, "New families of quadratic almost perfect nonlinear trinomials and multinomials", *Finite Fields and Their Applications*, vol.14(3), 2008, pp. 703-714.

[21] F. Göloğlu, "Almost perfect nonlinear trinomials and hexanomials", *Finite Fields and Their Applications*, vol.33, 2015, pp. 258-282.

[22] Y. Edel, A. Pott, "A new almost perfect nonlinear function which is not quadratic", *Advances in Mathematics of Communications*, vol.3(1), 2009, pp. 59-81.