List of APN polynomials

In the following we report the list of quadratics APN polynomials which are inequivalent to power functions and that can produce APN functions inequivalent to each other.

Table 1: Known classes of quadratic APN polynomial over $\mathbb{F}_{2^n}$ CCZ-inequivalent to power functions

N°	Functions	Conditions	Proven
C1-C2	$x^{2^s+1}+u^{2^k-1}x^{2^{ik}+2^{mk+s}}$	$n=pk$, $\gcd(k,3)$=$\gcd(s,3k)$=1, $p\in\{3,4\}$, $i=sk \bmod p$, $m=p-i$, $n\geq 12$, u primitive in $\mathbb{F}_{2^n}^*$	[6]
C3	$sx^{q+1}+x^{2^i+1}+x^{q(2^i+1)}$ $+cx^{2^iq+1}+c^qx^{2^i+q}$	$q=2^m$, $n=2m$, $\gcd(i,m)$=1, $c\in\mathbb{F}_{2^n}$, $s\in\mathbb{F}_{2^n}\setminus\mathbb{F}_q$, $X^{2^i+1}+cX^{2^i}+c^qX+1$ has no solution x s.t. $x^{q+1}=1$	[5]
C4	$x^3+a^{-1}Tr_n(a^3x^9)$	$a\neq 0$	[7]
C5	$x^3+a^{-1}Tr_n^3(a^3x^9+a^6x^{18})$	$3\|n$, $a\neq 0$	[8]
C6	$x^3+a^{-1}Tr_n^3(a^6x^{18}+a^{12}x^{36})$	$3\|n$, $a\neq 0$	[8]
C7-C9	$ux^{2^s+1}+u^{2^k}x^{2^{-k}+2^{k+s}}+$ $vx^{2^{-k}+1}+wu^{2^k+1}x^{2^s+2^{k+s}}$	$n=3k$, $\gcd(k,3)$=$\gcd(s,3k)$=1, $v,w\in\mathbb{F}_{2^k}$, $vw\neq 1$, $3\|(k+s)$ u primitive in $\mathbb{F}_{2^n}^*$	[2]
C10	$(x+x^{2^m})^{2^k+1}+$ $u'(ux+u^{2^m}x^{2^m})^{(2^k+1)2^i}+$ $u(x+x^{2^m})(ux+u^{2^m}x^{2^m})$	$n=2m$, $m\geq 2$ even, $\gcd(k,m)=1$ and $i\geq 2$ even u primitive in $\mathbb{F}_{2^n}^*$, $u'\in\mathbb{F}_{2^m}$ not a cube	[11]
C11	$a^2x^{2^{2m+1}+1}+b^2x^{2^{m+1}+1}+ax^{2^{2m}+2}$ $+bx^{2^m+2}+(c^2+c)x^3$	$n=3m$, m odd $L(x)=ax^{2^{2m}}+bx^{2^m}+cx$ satisfies the conditions in Lemma 8 of [3]	[3]

- For n odd all these families are AB. However, only the functions of the family C1, with n odd, are provably permutations. In particular, this implies that these binomials and the Gold AB monomials are the only two known crooked functions.
- In [10] the author introduced the APN trinomials $x^{2^k+1}+tr_m^n(x)^{2^k+1}$ with $n=2m=4t$, $\gcd(k,n)=1$. Here tr_m^n denotes the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$. It was conjectured that this family was inequivalent to power functions, but in [9] it is shown that such a function is affine equivalent to the Gold function $x^{2^{m-k}+1}$.
- The family of APN multinomials from [1] is contained in the family C4 (see [4]).
- The family of APN trinomials from [5] is contained in the family C4 (see [4]).

References

[1] Bracken, C., Byrne, E., Markin, N., McGuire, G.: *New Families of Quadratic Almost Perfect Nonlinear Trinomials and Multinomials*. Finite Fields and Their Applications 14(3), 703–714 (2008)

[2] C. Bracken, E. Byrne, N. Markin, and G. McGuire, *A Few More Quadratic APN Functions*, Cryptography and Communications, 3(1), 2011, pp. 43-53.

[3] Budaghyan L., Calderini M., Carlet C., Coulter R., Villa I., *On Isotopic Construction of APN Functions*. SETA 2018.

[4] Budaghyan L., Calderini M., Villa I., *On relations between CCZ- and EA-equivalences*. BFA 2018.

[5] Budaghyan, L., Carlet, C.: *Classes of Quadratic APN Trinomials and Hexanomials and Related Structures*. IEEE Trans. Inform. Theory 54(5), 2354-2357 (2008)

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

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

[8] L. Budaghyan, C. Carlet, and G. Leander, *On a construction of quadratic APN functions*, Proceedings of IEEE Information Theory workshop ITW'09, Oct. 2009, pp. 374-378.

[9] Budaghyan L., Helleseth T., Li N., Sun B., *Some Results on the Known Classes of Quadratic APN Functions*. In: El Hajji S., Nitaj A., Souidi E. (eds) Codes, Cryptology and Information Security. C2SI 2017. Lecture Notes in Computer Science, vol 10194. Springer, Cham (2017)

[10] Göloğlu, F.: *Almost Perfect Nonlinear Trinomials and Hexanomials*. Finite Fields and Their Applications 33, 258?282 (2015)

[11] Y. Zhou and A. Pott. *A New Family of Semifields with 2 Parameters*. Advances in Mathematics, 234:43-60, 2013.