Generalized Binomial APN Functions

Nikolay S. Kaleyski

University of Bergen

(joint work with Lilya Budaghyan and Tor Helleseth)

Background and Notation

- *Vectorial Boolean Function*, or (n, m)-function: $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$;
- substitution of sequences of n bits with sequences of m bits;
- core component of cryptographic algorithms;
- resistance to cryptanalysis depends on properties of the function;
- $n = m$;
- finite field interpretation: $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$;
- unique representation as a univariate polynomial

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

Background and Notation (2)

- *algebraic degree* $\deg(F)$: maximum binary weight of exponent with non-zero coefficient in univariate representation;
- ... high algebraic degree $\implies$ resistance to *higher order differential attacks*;
- *differential uniformity* Δ_F: largest number of solutions x to the equation
$$D_aF(x) = F(x) + F(a + x) = b$$
for $a, b \in \mathbb{F}_{2^n}$, $a \neq 0$;
- ... low differential uniformity $\implies$ resistance to *differential attacks*;
- ... $\Delta_F \geq 2$ for any $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$;
- ... when $\Delta_F = 2$, F is called *almost perfect nonlinear (APN)*;
- other desirable properties: nonlinearity, boomerang uniformity, bijectivity, etc.

Background and Notation (3)

- the number of (n, n)-functions is huge, so they are classified with respect to equivalence relations which preserve the properties of interest;
- two (n, n)-functions F and G are *EA-equivalent* if $G = A_1 \circ F \circ A_2 + A$ where A_1, A_2, A are affine (n, n)-functions and A_1, A_2 are permutations;
- F and G are *CCZ-equivalent* if there is an affine permutation $\mathcal{L}$ of $\mathbb{F}_{2^n}^2$ which maps the graph $G_F = \{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$ of F to the graph G_G of G;
- EA-equivalence is a special case of CCZ-equivalence, and the latter is strictly more general;
- CCZ-equivalence preserves i.a. differential uniformity, so e.g. APN functions are classified up to CCZ-equivalence;
- deciding equivalence of two given functions is computationally difficult in general;
- can be resolved by the isomorphism of linear codes associated to the functions, which can take a long time for high dimensions;
- equivalence can sometimes be disproved by invariants: Walsh spectrum, Γ-rank, Δ-rank, etc.

Status quo of APN functions

- APN functions introduced by K. Nyberg in 1993[1];
- since then, there are six known infinite families of monomial APN functions[2]:

Family	Exponent	Conditions	$\deg(x^d)$
Gold	2^i+1	$\gcd(i,n)=1$	2
Kasami	$2^{2i}-2^i+1$	$\gcd(i,n)=1$	$i+1$
Welch	2^t+3	$n=2t+1$	3
Niho	$2^t+2^{t/2}-1, t$ even	$n=2t+1$	$(t+2)/2$
	$2^t+2^{(3t+1)/2}-1, t$ odd		$t+1$
Inverse	$2^{2t}-1$	$n=2t+1$	$n-1$
Dobbertin	$2^{4i}+2^{3i}+2^{2i}+2^i-1$	$n=5i$	$i+3$

- the table is conjectured complete.

[1] Nyberg 1994.

[2] Beth and Ding 1994; Dobbertin 1999a,b, 2001; Gold 1968; Janwa and Wilson 1993; Kasami 1971; Nyberg 1994.

Status quo of APN functions (2)

- Eight infinite families of quadratic polynomials[3]:

N°	Functions	Conditions
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 $\mathbb{F}_{2^n}^*$
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. $x^{q+1}=1$
C4	$x^3+a^{-1}\mathrm{Tr}_n(a^3x^9)$	$a\neq 0$
C5	$x^3+a^{-1}\mathrm{Tr}_n^3(a^3x^9+a^6x^{18})$	$3\|n, a\neq 0$
C6	$x^3+a^{-1}\mathrm{Tr}_n^3(a^6x^{18}+a^{12}x^{36})$	$3\|n, a\neq 0$
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 $\mathbb{F}_{2^n}^*$
C10	$(x+x^{2^m})^{2^k+1}+u'(ux+u^{2^m}x^{2^m})^{(2^k+1)2^i}+u(x+x^{2^m})(ux+u^{2^m}x^{2^m})$	$n=2m, m\geqslant 2$ even, $\gcd(k,m)=1$ and $i\geqslant 2$ even, u primitive in $\mathbb{F}_{2^n}^*, u'\in\mathbb{F}_{2^m}$ not a cube
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 [7]

- 470, resp. 8157 new quadratic APN functions found over $\mathbb{F}_{2^7}$, resp. $\mathbb{F}_{2^8}$ using matrix methods[4];
- sporadic APN binomial over $\mathbb{F}_{2^{10}}$[5]: first example of an APN function CCZ-inequivalent to a power function, conjectured by Bierbrauer not to belong to any infinite family.

[3] Bracken et al. 2011; Budaghyan, Calderini, et al. 2018; Budaghyan and Carlet 2008; Budaghyan, Carlet, and Leander 2008, 2009a,b; Zhou and Pott 2013.
[4] Yu, Wang, and Li 2014.
[5] Edel, Kyureghyan, and Pott 2006.

Expanding $x^3 + \beta \cdot x^{36}$

- the binomial $B(x) = x^3 + \beta \cdot x^{36}$ over $\mathbb{F}_{2^{10}}$, where β is the primitive element of $\mathbb{F}_{2^2}$;
- compare with $x^3 + w \cdot x^{258}$ over $\mathbb{F}_{2^{12}}$ which was extended into *two* infinite families;
- we attempt to "expand" it to another APN function by adding terms;
- $B(x)$ cannot be expanded to an APN trinomial;
- we do find quadrinomials containing $B(x)$ which are APN, for example:
  - $x^3 + \beta \cdot x^{36} + \beta^2 \cdot x^{96} + x^{129}$;
  - $x^3 + \beta \cdot x^{36} + x^{96} + x^{129}$;
  - $x^3 + \beta \cdot x^{36} + \beta \cdot x^{80} + x^{520}$;
  - etc.
- remaining quadrinomials equivalent to $B(x)$ (allowing us to represent $B(x)$ as a quadrinomial) or to one of the quadrinomials above;
- above quadrinomials inequivalent as witnessed by Γ-rank.

Expanding $x^3 + \beta \cdot x^{36}$ (2)

- the general form is $C(x) = x^3 + \beta \cdot x^{2^i+1} + \beta^2 \cdot (x^3)^{2^k} + (x^{2^i+1})^{2^k}$;
- $0 \leq i, k \leq n-1$;
- the APN-ness of C is characterized by a system of two equations in two variables a, x;
- depending on the parity of k, we get two different systems of equations;
- C is APN if the associated system has only $x \in \mathbb{F}_2$ as solutions for any $a \neq 0$;
- it remains to select a value of i for which the system has no solutions.

Expanding $x^3 + \beta \cdot x^{36}$ (3)

- if $i = m - 2 = n/2 - 2$, then the even system only has trivial solutions;
- for example, $C(x) = x^3 + \beta \cdot x^{36} + \beta^2 \cdot x^{96} + x^{129}$ has $i = 3 = 10/2 - 2$ and $k = 4$
- proof by contradiction: the equalities together imply that β is a cube, which cannot be true unless $3 \nmid m$;
- for $n = 10$, $C(x)$ has Γ-rank 166068, which is distinct from that of $x^3, x^9, x^3 + \mathrm{Tr}(x^9)$ and $x^3 + \alpha^{-1} \cdot \mathrm{Tr}(\alpha^3 \cdot x^9)$;
- Γ-ranks of representatives from other families are being computed;
- note that $C(x)$ cannot be CCZ-equivalent to x^{57} (Kasami) or x^{339} (Dobbertin);
- $C(x)$ is inequivalent to any known family according to *Magma* via code isomorphism.

Expanding $x^3 + \beta \cdot x^{36}$ (4)

- for $i = m + 2 = n/2 + 2$, the odd system only has trivial solutions, and the odd and even functions are equivalent;
- functions for $i = m - 2$ and different even k, resp. $i = m + 2$ and different odd k are equivalent;
- empirically, if $i = (m-2)^{-1} \mod n$, resp. $i = (m+2)^{-1} \mod n$ for k even, resp. k odd, then the system also has only trivial solutions;
- these "inverse" functions are equivalent between themselves, but inequivalent to the previous ones (or to any other known APN function).

Further observations

- both $x^3 + \beta \cdot x^{36} + \beta^2 \cdot x^{96} + x^{129}$ and $x^3 + \beta \cdot x^{36} + x^{96} + x^{129}$ are 3-to-1 functions on $\mathbb{F}_{2^{10}}^*$;
- $x^3 + \beta \cdot x^{36} + \beta \cdot x^{80} + x^{520}$ is not, and has a different structure that does not appear to be easily generalizable;
- the quadrinomial can be seen as the sum of a composition of power functions with binomials, i.e. for $L_1(x) = x + \beta^2 \cdot x^{2^{n/2}}$ and $L_2(x) = x + \beta \cdot x^{2^{n/2}}$, we can write

$$C(x) = L_1(x^3) + \beta \cdot L_2(x^9) = L_1(x^3) + L_2(x^{9 \cdot 2^{n/2}})$$

or, in general,

$$C(x) = L_1(x^3) + \beta \cdot L_2(x^{2^{m-2}+1}) = L_1(x^3) + L_2(x^{(2^{m-2}+1) \cdot 2^{n/2}}).$$

- functions of the form $L_1(x^3) + L_2(x^9)$ have previously been studied for APN-ness by Budaghyan, Carlet and Leander; $C(x)$ is the first known case where $L_1(x) + L_2(x^3)$ is not a permutation.

Future work

- Prove APN-ness of $C(x)$ for the cases when $i = (m-2)^{-1}$ and $i = (m+2)^{-1}$;
- extended the other quadrinomials over $\mathbb{F}_{2^{10}}$ to APN families;
- find a more general form of the polynomials;
- find a general form of the construction;
- investigate invariants and other properties of the polynomials families.

- Beth, Thomas and Cunsheng Ding (1994). "On Almost Perfect Nonlinear Permutations". In: *EUROCRYPT '93 Workshop on the theory and application of cryptographic techniques on Advances in cryptology*, pp. 65–76.
- Bracken, Carl et al. (2011). "A Few More Quadratic APN Functions". In: *Cryptography and Communications* 3.1, pp. 43–53.
- Budaghyan, Lilya, Marco Calderini, et al. (2018). "On Isotopic Construction of APN Functions". In: *Sequences and their Applications (SETA) 2018*.
- Budaghyan, Lilya and Claude Carlet (2008). "Classes of Quadratic APN Trinomials and Hexanomials and Related Structures". In: *IEEE Transactions on Information Theory* 54.5, pp. 2354–2357.
- Budaghyan, Lilya, Claude Carlet, and Gregor Leander (2008). "Two Classes of Quadratic APN Binomials Inequivalent to Power Functions". In: *IEEE Transactions on Information Theory* 54.9, pp. 4218–4229.
- – (2009a). "Constructing New APN Functions from Known Ones". In: *Finite Fields and Their Applications* 15.2, pp. 150–159.

- Budaghyan, Lilya, Claude Carlet, and Gregor Leander (2009b). "On a Construction of Quadratic APN Functions". In: *2009 IEEE Information Theory Workshop*, pp. 374–378.
- Dobbertin, Hans (1999a). "Almost Perfect Nonlinear Power Functions on $GF(2^n)$: the Niho case". In: *Information & Computation* 151.1, pp. 57–72.
- – (1999b). "Almost Perfect Nonlinear Power Functions on $GF(2^n)$: the Welch case". In: *IEEE Transactions on Information Theory* 45.4, pp. 1271–1275.
- – (2001). "Almost Perfect Nonlinear Power Functions on $GF(2^n)$: A New Case for n Divisible by 5". In: *International Conference on Finite Fields and Applications*, pp. 113–121.
- Edel, Yves, Gohar Kyureghyan, and Alexander Pott (2006). "A new APN function which is not equivalent to a power mapping". In: *IEEE Transactions on Information Theory* 52.2, pp. 744–747.
- Gold, Robert (1968). "Maximal Recursive Sequences with 3-valued Recursive Cross-correlation Functions (Corresp.)" In: *IEEE Transactions on Information Theory* 14.1, pp. 154–156.

Janwa, Heeralal and Richard M Wilson (1993). "Hyperplane sections of Fermat varieties in P 3 in char. 2 and some applications to cyclic codes". In: *International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*. Springer, pp. 180–194.

Kasami, Tadao (1971). "The Weight Enumerators for Several Classes of Subcodes of the 2nd Order Binary Reed-Muller Codes". In: *Information & Computation* 18.4, pp. 369–394.

Nyberg, K. (1994). "Differentially Uniform Mappings for Cryptography". In: *Lecture Notes in Computer Science* 765, pp. 55–64.

Yu, Yuyin, Mingsheng Wang, and Yongqiang Li (2014). "A matrix approach for constructing quadratic APN functions". In: *Designs, codes and cryptography* 73.2, pp. 587–600.

Zhou, Yue and Alexander Pott (2013). "A new family of semifields with 2 parameters". In: *Advances in Mathematics* 234, pp. 43–60.