1 General Description

Suppose $\mathbb{F}_{2^n}$ is a finite field such that $n = 2m$, $q = 2^m$ and $gcd(k, n) = 1$.

Conjecture 1 *For some a_1, a_2 and $a_3 \in \mathbb{F}_{2^n}$ the function*

$$F_1(x) = x^{2^k+1} + a_1 x^{q+2^k} + a_2 x^{2^k q+1} + a_3 x^{(2^k+1)q}$$

is APN.

Remark 1 *Note that*

$$(F_1(x))^{2^{2m-k}} = x^{1+2^{2m-k}} + a_1 x^{q2^{2m-k}+1} + a_2 x^{2^m+2^{2m-k}} + a_3 x^{(1+2^{2m-k})q}.$$

We only need to consider the cases that $k \leq m$.

Remark 2 *Either a_1 or a_2 can be 0.*

Conjecture 2 *F_1 produces either 1 or $\phi(m)$ classes of APN functions up to EA/CCZ-equivalence.*

Theorem 1 *(proved) Suppose n is even, $gcd(k, n) = 1$ and g is a primitive element of $\mathbb{F}_{2^n}$. Then the function $F_1 = x^{2^k+1} + a_3 x^{(2^k+1)q}$, where $a_3 = \mathbb{F}_{2^n} \setminus \{1\} \cup \{g^{q-1} \mid i = \{1, 2, \ldots, q-1\}\}$, is APN.*

2 Special Cases

Suppose $\mathbb{F}_{2^n}$ is a finite field such that $hw(n) = 2$, $n = 2m$, $q = 2^m$ and $n = 2^s + 2^t$.

Conjecture 3 *For some a_1, a_2 and $a_3 \in \mathbb{F}_{2^n}$ the function*

$$\begin{aligned} F_2(x) &= x^{2^{s-1}+2^{t-1}} + a_1 x^{2^{s-1}q+2^{t-1}} + a_2 x^{2^{t-1}q+2^{s-1}} + a_3 x^{(2^{s-1}+2^{t-1})q} \\ &= x^m + a_1 x^{2^{s-1}q+2^{t-1}} + a_2 x^{2^{t-1}q+2^{s-1}} + a_3 x^{m \cdot q} \end{aligned}$$

is APN.

Remark 3 *Without loss of generality, we may assume $s \geq t$. Denoting $k = s - t$ and $y = x^{2^{t-1}}$, we get*

$$\begin{aligned} F_1(y) &= y^{2^k+1} + a_1 y^{q+2^k} + a_2 y^{2^k q+1} + a_3 y^{(2^k+1)q} \\ &= x^{2^{t-1}(2^k+1)} + a_1 x^{2^{t-1}(q+2^k)} + a_2 x^{2^{t-1}(2^k q+1)} + a_3 x^{2^{t-1}(2^k+1)q} \\ &= F_2(x). \end{aligned}$$

Thus, $F_1(x)$ and $F_2(x)$ have the same form. From the experiment result in A.4, $\gcd(2^s + 2^t, s - t)$ is not necessarily equal to 1 for $F_2(x)$ to be APN.

Conjecture 3 is also true if ether $a_1 = 0$, $a_2 = 0$ or $a_3 = 0$ (verified for $n = 6, 10$).

Observation 1 *F_2 is equivalent to F_1 for $n < 18$.*

Conjecture 4 *For $h = 1$ ($hw(n) = 1$) and $n > 2$ the function $F_2(x) = x^{2^{s-2}\cdot(1+2^m)}$ has $\delta = 2^{2^{s-1}}$.*

All monomials of F_2 preserve the property $x^d \pmod{x^{2^m} + x} = x^m$. In other words, $F_2(x) = cx^m \pmod{x^{2^m} + x}$.

Observation 2 *For $k = 1$ F_1 is equivalent to the function $F_3(x) = x^3 + a_1 x^{2+q} + a_2 x^{1+2q} + a_3 x^{3q}$.*

Observation 3 *The number of all possible APN functions of the form $x^3 + a_1 x^{10} + a_2 x^{17} + a_3 x^{24}$ (n=6, k=1) is 43174. That means $\frac{43174}{2^{18}} = 0.164$ or 16% of all possible functions. The probability that a random APN function CCZ-equivalent to permutation is 0.9643.*

A Examples of degrees of F_1 for several values of n

n	k	degrees	APN
4	$1,3$	$\{3,6,9,12\}$	+
6	$1,4$	$\{3,10,17,24\}$	+
	$2,5$	$\{5,12,33,40\}$	+
	3	$\{2,9,9,16\}$	-
8	$1,5$	$\{3,18,33,48\}$	+
	$2,6$	$\{5,20,65,80\}$	-
	$3,7$	$\{9,24,129,144\}$	+
10	$1,6$	$\{3,34,65,96\}$	+
	$2,7$	$\{5,36,129,160\}$	+
	$3,8$	$\{9,40,257,288\}$	+
	$4,9$	$\{17,48,513,544\}$	+
12	$1,7$	$\{3,66,129,192\}$	+
	$2,8$	$\{5,68,257,320\}$	-
	$3,9$	$\{9,72,513,576\}$	-
	$4,10$	$\{17,80,1025,1088\}$	-
	$5,11$	$\{33,96,2049,2112\}$	+

B Examples of degrees of F_2 for several values of n

n	degrees
6	$\{3,10,17,24\}$
10	$\{5,36,129,160\}$
12	$\{6,132,258,384\}$
18	$\{9,520,4097,4608\}$
20	$\{10,2056,8194,10240\}$
24	$\{12,16392,32772,49152\}$
34	$\{17,131088,2097153,2228224\}$
36	$\{18,524304,4194306,4718592\}$
40	$\{20,4194320,16777220,20971520\}$

C Examples of APN functions

Precomputed APN functions in the form of $F_1(x)$ are listed here. The results have the following format $[a, b, c, d]$, where $a = 1 = g^{2^n-1}, a_1 = g^b, a_2 = g^c, a_3 = g^d$ (note, $0 = 0$, and not g^0). File names consist of n, k and degrees (d_1, d_2, d_3, d_4). For example, the second line of "6_1_3-10-17-24.txt" describes the function $F_1(x) = x^3 + 0x^{10} + 0x^{17} + gx^{24} = x^3 + gx^{24}$ $(k = 1)$ over $\mathbb{F}_{2^6}$.

Remark 4 *Perhaps you have noticed that degrees are sorted in increasing order. A problem may occur when $d_i > 2^n - 1$. In this case the order changes. In other words, correspondence of coefficients depends on k.*