On a relationship between Gold and Kasami functions and other power APN functions

Nikolay S. Kaleyski

University of Bergen

(joint work with Lilya Budaghyan, Marco Calderini and Claude Carlet

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.

Composing power functions with a linear polynomial

- denote by $P_i(x)$ the power function x^i over $\mathbb{F}_{2^n}$;
- consider the composition $P_i \circ L \circ P_j$ for some linear (n, n)-function L;
- we look for i, j, L for which $P_i \circ L \circ P_j$ is APN;
- exclude trivial cases when L is a linear monomial;
- at first consider L with coefficients in $\mathbb{F}_2$ and only take one i, j from each cyclotomic coset;
- exhaustive search for $4 \leq n \leq 9$.

Observations in the odd case

Proposition

For an odd $n = 3s \pm r, 3s \geq r$ *and* $\gcd(3s, r) = 1$, *and for* $L_i^{\mu}(x) = \mu x^{2^i} + x$, *we have*

$$G_s \circ L_{2s}^{\mu} \circ G_r^{-1}(x) = \begin{cases} A^{\mu} \circ K_s^{-1}(x^{2^{3s}}) + \mu^{2^s} x^{2^{3s}} & n = 3s + r \\ A^{\mu} \circ K_s^{-1}(x) + \mu^{2^s} x^{2^s} & n = 3s + r, \end{cases}$$

where $A^{\mu}(x) = \mu^{2^s+1} x^{2^{2s}} + \mu x^{2^s} + x$, $\mu \in \mathbb{F}_{2^n}$, G_i *is the Gold function* $G_i(x) = x^{2^i+1}$, G_i^{-1} *is its compositional inverse, and* $K_s^{-1}(x) = x^{(2^s+1)/(2^{3s}+1)}$ *is the inverse of the Kasami function* $K_s(x) = x^{(2^{3s}+1)/(2^s+1)}$.

- in other words, (the inverse of) a Kasami power function can be obtained by composing two Gold functions with a linear polynomial;
- experimental data reveals similar patterns in the odd case;
- similar proposition for $G_s \circ L_{n-2s}^{\mu} \circ G_r^{-1}(x)$, which also gives the inverse of a Kasami function.

Observations in the odd case (2)

Proposition

Let $n = 2m + 1$ for an arbitrary natural m. Denoting again $L_i^\mu(x) = \mu x^{2^i} + x$, we have for any $1 \leq i \leq n - 1$

$$G_i \circ L_{2i}^\mu \circ G_i^{-1}(x) = A_i^\mu(x) + \mu^{2^i} K_i(x),$$

where $A_i^\mu(x) = \mu^{2^s+1} x^{2^{2s}} + \mu x^{2^s} + x$ is as before.

- in this case, the parameter i of the Gold function does not depend on the dimension n;
- a similar proposition can be given for $G_i \circ L_{n-2i}^\mu \circ G_i^{-1}(x)$, which once again leads to a Kasami power function.

Observations in the odd case (3)

- let $n = 2t + 1$;
- for $L = x^{2^t} + x$, we have
$$(G_t^{-1} \circ L \circ G_t)(x) = (x^{2^t+1} + x^{2^{2t}+2^t})^{2^{t+1}\cdot(2^{t+1}-1)};$$
- for $L = x^{2^{t+1}} + x$, we have also
$$(G_t^{-1} \circ L \circ G_t)(x) = (x^{2^t+1} + x^{2^{2t+1}+2^{t+1}})^{2^{t+1}\cdot(2^{t+1}-1)};$$
- similarly, for $L = x^2 + x$ and $I(x) = x^{2^{2t}-1}$, we have
$$(I \circ L \circ I)(x) = (x^{2^{2t}-1} + x^{2^{2t+1}-2})^{2^{2t}-1};$$
- for $L = x^{2^{2t}} + x$, we have
$$(I \circ L \circ I)(x) = (x^{2^{2t}-1} + x^{2^{4t}-2^{2t}})^{2^{2t}-1};$$
- this exhausts the observed cases for odd dimension.

Observations in the even case

- let $n = 2m$ with $3 \nmid m$;
- let $l_n = \frac{2^{n-1}+1}{3}$, $L(x) = x^{2^{n-2}} + x^{2^{n-4}} + x$ and $1 \leq i \leq 2^n - 2$;
- then we have
$$P_i \circ L \circ P_{l_n}(x) = P_i \circ L_1 \circ L_2(x)$$
where $L_1(x) = x + x^4 + x^{16}$ and $L_2(x) = x^{2^{n-5}}$ are linear permutations;
- similar results for $L(x) = x^{2^{n-2}} + x^4 + x$ when $3 \nmid m$, $L(x) = x^{2^{n-4}} + x^{2^{n-6}} + x$ when $7 \nmid m$;
- the divisibility assumption guarantees that L_1 and L_2 are permutations;
- these observations exhaust all observed cases for even dimension;
- allowing L to have coefficients in $\mathbb{F}_{2^2}$ still gives the same cases.

Future work

- consider a larger set of linear polynomials L;
- apply the construction to functions with a more complicated structure;
- use the "decomposition" of power functions as a proof technique.