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

Lilya Budaghyan, Marco Calderini, Claude Carlet, Nikolay Kaleyski
University of Bergen

Among vectorial Boolean functions, power functions, i.e. mappings of the form $x \mapsto x^k$ for some k over the finite field $\mathbb{F}_{2^n}$, are some of the most extensively studied from the point of view of their cryptographic properties. The Gold functions $G_i(x) = x^{2^i+1}$ and Kasami functions $K_i(x) = x^{2^{2i}-2^i+1}$ are of particular interest, in part due to their being Almost Perfect Nonlinear (APN) over any finite field $\mathbb{F}_{2^n}$ with $\gcd(i, n) = 1$ and thus providing optimal resistance to differential cryptanalysis. Furthermore, for odd dimensions n, all power APN functions, and the Gold and Kasami power functions in particular, are permutations. These functions have been known since at least the 70's, and as such constitute some of the earliest known examples of APN mappings.

We present a new relation between the Gold and Kasami functions in the case of odd n, in which the composition of a Kasami function or the inverse of one with a linear polynomial may be obtained by composing a Gold function G_s and the inverse G_r^{-1} with a linear polynomial L in the form $G_s \circ L \circ G_r^{-1}$. In particular, the inverse K_i^{-1} can be decomposed (up to addition and composition with linear polynomials) as $G_s \circ L \circ G_r^{-1}$ for any s, r such that $n = 3s \pm r$, $3s \geq r$ and $\gcd(3s, r) = 1$. Similarly, K_i may be obtained (up to addition and composition with linear polynomials) by composing $G_i \circ L \circ G_i^{-1}$. We generalize this approach to the composition $F_1 \circ L \circ F_2$ of any two power functions, $F_1(x) = x^i$ and $F_2(x) = x^j$ with a linear polynomial L, and obtain experimental results and further observations on the possibility of obtaining APN functions by combining two power functions in this manner.