

Some APN functions CCZ-equivalent to Gold functions and EA-inequivalent to power functions over \mathbb{F}_{2^n} (constructed in [1])

Functions	Conditions	d°
$x^{2^i+1} + (x^{2^i} + x + \text{tr}_n(1) + 1)\text{tr}(x^{2^i+1} + x \text{tr}_n(1))$	$n \geq 4$ $\gcd(i, n) = 1$	3
$[x + \text{tr}_{n/3}(x^{2(2^i+1)} + x^{4(2^i+1)}) + \text{tr}(x)\text{tr}_{n/3}(x^{2^i+1} + x^{2^{2^i}(2^i+1)})]^{2^i+1}$	$6 n$ $\gcd(i, n) = 1$	4
$x^{2^i+1} + \text{tr}_{n/m}(x^{2^i+1}) + x^{2^i} \text{tr}_{n/m}(x) + x \text{tr}_{n/m}(x)^{2^i}$ $+ [\text{tr}_{n/m}(x)^{2^i+1} + \text{tr}_{n/m}(x^{2^i+1}) + \text{tr}_{n/m}(x)]^{\frac{1}{2^i+1}} (x^{2^i} + \text{tr}_{n/m}(x)^{2^i} + 1)$ $+ [\text{tr}_{n/m}(x)^{2^i+1} + \text{tr}_{n/m}(x^{2^i+1}) + \text{tr}_{n/m}(x)]^{\frac{2^i}{2^i+1}} (x + \text{tr}_{n/m}(x))$	$m \neq n$ n odd $m n$ $\gcd(i, n) = 1$	$m + 2$

References

- [1] Lilya Budaghyan, Claude Carlet, and Alexander Pott. New classes of almost bent and almost perfect nonlinear polynomials. *IEEE Transactions on Information Theory*, 52(3):1141–1152, 2006.