

Known Infinite Families of APN power functions x^d on \mathbb{F}_{2^n}

Functions	Exponents d	Conditions	$d^\circ(x^d)$	Proven
Gold	$2^t + 1$	$\gcd(i, n) = 1$	2	[5, 8]
Kasami	$2^{2^i} - 2^i + 1$	$\gcd(i, n) = 1$	$i + 1$	[6, 7]
Welch	$2^t + 3$	$n = 2t + 1$	3	[4]
Niho	$2^t + 2^{\frac{t}{2}} - 1, \quad t \text{ even}$ $2^t + 2^{\frac{3t+1}{2}} - 1, \quad t \text{ odd}$	$n = 2t + 1$	$(t + 2)/2$ $t + 1$	[3]
Inverse	$2^{2^t} - 1$	$n = 2t + 1$	$n - 1$	[1, 8]
Dobbertin	$2^{4^i} + 2^{3^i} + 2^{2^i} + 2^i - 1$	$n = 5i$	$i + 3$	[2]

References

- [1] Thomas Beth and Cunsheng Ding. On almost perfect nonlinear permutations. In *Workshop on the Theory and Application of Cryptographic Techniques*, pages 65–76. Springer, 1993.
- [2] H Dobbertin. Almost perfect nonlinear power functions over $\text{gf}(2^i \text{ sup}_i n_i / \text{sup}_i i)$: a new case for n divisible by 5. In *proceedings of: The fifth Conference on Finite Fields and Applications FQ5*, pages 113–121.
- [3] Hans Dobbertin. Almost perfect nonlinear power functions on $\text{gf}(2^n)$: the niho case. *Information and Computation*, 151(1-2):57–72, 1999.
- [4] Hans Dobbertin. Almost perfect nonlinear power functions on $\text{gf}(2^n)$: the welch case. *IEEE Transactions on Information Theory*, 45(4):1271–1275, 1999.
- [5] Robert Gold. Maximal recursive sequences with 3-valued recursive cross-correlation functions (corresp.). *IEEE transactions on Information Theory*, 14(1):154–156, 1968.
- [6] Heeralal Janwa and Richard M Wilson. 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*, pages 180–194. Springer, 1993.
- [7] Tadao Kasami. The weight enumerators for several classes of subcodes of the 2nd order binary reed-muller codes. *Information and Control*, 18(4):369–394, 1971.
- [8] Kaisa Nyberg. Differentially uniform mappings for cryptography. In *Workshop on the Theory and Application of Cryptographic Techniques*, pages 55–64. Springer, 1993.