A notion on S-boxes for a partial resistance to some integral attacks

Claude Carlet,

University of Bergen, Department of Informatics, 5005 Bergen, Norway

University of Paris 8, Department of Mathematics, 93526 Saint-Denis, France.

E-mail: `claude.carlet@gmail.com`,

A vectorial function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is called *kth-order sum-free* [1] if, for every k-dimensional affine subspace A of $\mathbb{F}_2^n$ (or of $\mathbb{F}_{2^n}$), we have $\sum_{x\in A} F(x) \neq 0$. This notion generalizes that of almost perfect nonlinearity [5] (which corresponds to $k = 2$) and it has some relation with the resistance to integral attacks (in cryptanalysis) of those block ciphers using F as a substitution box (S-box), by preventing the propagation of the division property [6] of k-dimensional affine spaces. In this talk, we shall show that this notion, which is rarely satisfied by vectorial functions, can be weakened while retaining the property that the S-boxes do not propagate the division property of k-dimensional affine spaces. This will lead us to the property of *kth-order t-degree-sum-freedom*, whose strength decreases when t increases, and which coincides with kth-order sum-freedom when $t = 1$. The condition for kth-order t-degree-sum-freedom is that, for every k-dimensional affine space A, there exists a non-negative integer j of 2-weight (i.e. Hamming weight of the binary expansion) at most t such that $\sum_{x\in A}(F(x))^j \neq 0$. We shall show, for a general kth-order t-degree-sum-free function F, that t can always be taken smaller than or equal to $\min(k, m)$ under some reasonable condition on F, and that it is larger than or equal to $\frac{k}{\deg(F)}$, where $\deg(F)$ is the algebraic degree of F (i.e. the degree of its multivariate representation over $\mathbb{F}_2$ called algebraic normal form). We shall also show two other lower bounds: one, that is often tighter, by means of the algebraic degree of the compositional inverse of F when F is a permutation, and another (valid for every vectorial function) by means of the algebraic degree of the indicator of the graph $\{(x, F(x)); x \in \mathbb{F}_2^n\}$ of the function. We shall study power functions $F(x) = x^d; x \in \mathbb{F}_{2^n}$, for which we shall prove upper bounds. We shall study in particular the multiplicative inverse function (used as an S-box in the AES), for which we shall characterize the kth-order t-degree-sum-freedom by the coefficients of the subspace polynomials of k-dimensional vector subspaces (deducing the exact value of t when k divides n) and we shall extend to kth-order t-degree-sum-freedom the result that it is kth-order sum-free if and only if it is $(n - k)$th-order sum-free.

References

[1] C. Carlet. Two generalizations of almost perfect nonlinearity. *Journal of Cryptology* 38(2), 2025 (Topical Collection on Advances in Boolean Functions with Applications in Cryptography). Available at Cryptology ePrint Archive 2024/841

[2] C. Carlet. On the vector subspaces of $\mathbb{F}_{2^n}$ over which the multiplicative inverse function sums to zero. Special issue in memory of Kai-Uwe Schmidt of *Designs, Codes and Cryptography* 93, no. 4, pp. 1237-1254, 2025. Available at Cryptology ePrint Archive 2024/1007.

[3] C. Carlet and X.-D. Hou. More on the sum-freedom of the multiplicative inverse function. Preprint, 2024.

[4] F. J. MacWilliams and N. J. Sloane. *The theory of error-correcting codes*, North Holland. 1977.

[5] K. Nyberg. Differentially uniform mappings for cryptography. *Proceedings of EUROCRYPT 1993, Lecture Notes in Computer Science* 765, pp. 55-64, 1994.

[6] Y. Todo. Structural evaluation by generalized integral property. *Proceedings of EUROCRYPT 2015, Lecture Notes in Computer Science* 9056, pp. 287-314, 2015.