Problem 6. «8-bit S-box»

Permutations S of the set $\{0,1\}^n$ or $\mathbb{F}_2^n$ are usually called *n-bit S-boxes*. We will focus on the following cryptographic properties of S-boxes:

1. **The (minimal) algebraic degree** of S, denoted by $\deg(S)$, is the minimum of algebraic degrees of all component functions of S.
2. **The nonlinearity of** S, denoted by $\mathrm{nl}(S)$, is the minimal Hamming distance between all component functions of S and the set of all affine functions.
3. **The differential uniformity** of S, denoted by $\mathrm{du}(S)$ is the maximal number of solutions of the equation $S(x) \oplus S(x \oplus \alpha) = \beta$ for any nonzero vector α and any vector β.
4. **The (graph) algebraic immunity** of S, denoted by $\mathrm{ai}(S)$, is the minimal algebraic degree of all nonzero Boolean functions f in $2n$ variables such that $f(x,y) = 0$ for any $x \in \mathbb{F}_2^n$ and $y = S(x)$.

In modern symmetric cryptography, S-boxes of dimension $n = 8$ are probably the most popular. For example, such an S-box is used in the AES block cipher. The characteristics of S_{AES}:

$$(\deg, \mathrm{nl}, \mathrm{du}, \mathrm{ai})(S_{\mathrm{AES}}) = (7, 112, 4, 2).$$

The value $\mathrm{ai}(S_{\mathrm{AES}}) = 2$ means that S_{AES} (and the whole AES) can be compactly described by quadratic equations. This can be a weakness in the context of algebraic attacks.

Imposing the restrictions $(\deg, \mathrm{ai})(S) = (7, 3)$ (optimal values), we need to maximize $\mathrm{nl}(S)$ and minimize $\mathrm{du}(S)$. The current best result [1,2] is

$$(\deg, \mathrm{nl}, \mathrm{du}, \mathrm{ai})(S) = (7, 108, 6, 3).$$

Problem for a special prize! You need to improve this result:

find an 8-bit S with $\mathrm{nl}(S) > 108$ and/or $\mathrm{du}(S) < 6$ while preserving $\deg(S) = 7$ and $\mathrm{ai}(S) = 3$.

Remark. Let us recall the relevant definitions.

1. A Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ can be uniquely represented in the *algebraic normal form* (ANF) in the following way: $f(x) = \bigoplus_{I \in \mathcal{P}(N)} a_I \big(\prod_{i \in I} x_i\big)$, where $\mathcal{P}(N)$ is the power set of $N = \{1, \ldots, n\}$ and $a_I \in \mathbb{F}_2$.
2. The *algebraic degree* of f is degree of its ANF: $\deg(f) = \max\{|I| : \ a_I \neq 0, \ I \in \mathcal{P}(N)\}$.
3. Boolean functions of the algebraic degree not more than 1 are called *affine*.
4. The Hamming distance between Boolean functions f and g is the number of vectors $x \in \mathbb{F}_2^n$ such that $f(x) \neq g(x)$.
5. A function $S : \mathbb{F}_2^n \to \mathbb{F}_2^n$ can be given as $S = (s_1, \ldots, s_n)$, where s_i is a Boolean function; a nontrivial linear combination of $s_1, \ldots, s_n$ is a *component* function of S.

[1] R.A. de la Cruz Jimènez. Generation of 8-Bit S-Boxes Having Almost Optimal Cryptographic Properties Using Smaller 4-Bit S-Boxes and Finite Field Multiplication. In: Lange T., Dunkelman O. (eds) Progress in Cryptology – LATINCRYPT 2017. LNCS, 2019, vol 11368, pp 191–206.

[2] D. B. Fomin. New classes of 8-bit permutations based on a butterfly structure. Math. vopr. kript. 2019, vol 10(2), pp 169–180. https://ctcrypt.ru/files/files/2018/09_Fomin.pdf.