S-Box: Quadratic Equations with its Quadratic Items

Let F be a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$, and define

$$AI(F) = \min\{\deg g \mid 0 \neq g \in \mathbb{B}_n, g(gr(F)) = 0\}$$

as the algebraic immunity of F, where $gr(F) = \{(x, F(x)) \mid x \in \mathbb{F}^n\} \subseteq \mathbb{F}^{2n}$. The number of linear independent equations in input and output bits of F with the degree of algebraic immunity of F is denoted as $NU(F)$.

We present the low degree description of the S-box. The algebraic immunity of S-box is 2, and the number of independent implicit equations of input and output variables with the degree of algebraic immunity of 2 is 19. Denote

$$(x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}) = S(x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7).$$

We give the coefficient vectors of 19 equations as follows in the order of terms

$$1,\ x_i, i = 0, \ldots 15,\ x_i x_j, i = 0, \ldots 15, j = i + 1 \ldots 15.$$

$equation_0$:
111101111111010110110000000000011111100000010100000000000011110010000
01000000000010000000001000000001000000011000101101101001010101101011;

$equation_1$:
000000000000000010000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000;

$equation_2$:
000000000000000000000000000000010000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000;

$equation_3$:
000000000000000000000000000000000000000000000100000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000;

$equation_4$:
000000000000000000000000000000000000000000000000000000000010000000000

00000000000000000000000000000000000000000000000000000000000000000000;

$equation_5$:
000000000000000000000000000000000000000000000000000000000000000000000
01000000000000000000000000000000000000000000000000000000000000000000;

$equation_6$:
000000000000000000000000000000000000000000000000000000000000000000000
00000000000010000000000000000000000000000000000000000000000000000000;

$equation_7$:
000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000001000000000000000000000000000000000000000000000;

$equation_8$:
000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000001000000000000000000000000000000000000;

$equation_9$:
000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000010000000000000000000000000000;

$equation_{10}$:
000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000001000000000000000000000;

$equation_{11}$:
000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000001000000000000000;

$equation_{12}$:
000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000010000000000;

$equation_{13}$:
100010000000001100000000000000001000000001000000000010000000000000000
00000000000000000000000000000000000000000000000010100000000100000000;

$equation_{14}$:
000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000001000000;

$equation_{15}$:
011111111111011000110000000000000111100001010000000010000001110010000
00000000000000000000000000000000000000001000100111000001000000100000;

$equation_{16}$:
000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000001000;

$equation_{17}$:
000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000010;

$equation_{18}$:
000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000001.

The independent implicit equations which fully describe the S-box are

$$equation_0 = 0,\ equation_0 \oplus equation_i = 0,\ i = 1, \ldots, 18.$$

They totally contain 38 quadratic items.