Exercises on Cryptographic Boolean functions

Anne Canteaut, March 2025

Exercise 1. (Walsh spectrum of quadratic functions).

1. Let f be a Boolean function of n variables. For any $a \in \mathbf{F}_2^n$, the derivative of f with respect to a is the n-variable Boolean function $D_a f : x \mapsto f(x+a)+f(x)$. The set $\mathsf{LS}(f)$ of all $a \in \mathbf{F}_2^n$ such that $D_a f$ is constant is named the *linear space of* f. It can be decomposed into $\mathsf{LS}_0(f) = \{a \in \mathsf{LS}(f) : D_a f = 0\}$ and $\mathsf{LS}_1(f) = \{a \in \mathsf{LS}(f) : D_a f = 1\}$.
   - Prove that $\mathsf{LS}(f)$ is a linear subspace of $\mathbf{F}_2^n$.
   - Prove that the subset $\mathsf{LS}_0(f)$ is a linear subspace of $\mathsf{LS}(f)$.
   - Prove that $\mathsf{LS}_1(f)$ is either empty or is of the form $\alpha + \mathsf{LS}_0(f)$ for some $\alpha \in \mathbf{F}_2^n$.
2. Let f be a Boolean function of n variables. Prove that, for any $a \in \mathbf{F}_2^n$,
$$\mathcal{E}^2(f+\varphi_a) = \sum_{b \in \mathbf{F}_2^n} (-1)^{a \cdot b} \mathcal{E}(D_b f) \ . \tag{1}$$
3. Let f a Boolean function of n variables with degree 2.
   - Using (1), prove that f is balanced if and only if there exists $\alpha \in \mathbf{F}_2^n$ such that $D_\alpha f = 1$.
   - Prove that, for any $a \in \mathbf{F}_2^n$,
   $$\mathcal{E}(f+\varphi_a) \in \{0, \pm 2^{\frac{n+k}{2}}\}$$
   where k is the dimension of $\mathsf{LS}(f)$.

Exercise 2. (Linear approximation table of a 5-bit Sbox)
The following table is the linear approximation table of a 5-bit Sbox S. Its entry at Row a and Column b is the value $\mathcal{E}(S_b + \varphi_a)$.

32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	16	0	-16	0	16	0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	16	0	0	0	-16	0	0	0	16	0	0	0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	-16	0	0	0	16	0	0	0	0	0	16	0	0	0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	16	0	0	0	0	0	0	0	-16	0	0	0	0	0	0	0	16	0	0	0	0	0	0	0	16	0	0	0
0	8	0	8	0	8	0	-8	0	-8	0	-8	0	-8	0	8	0	8	0	8	0	8	0	-8	0	8	0	8	0	8	0	-8
0	0	-16	0	0	0	0	0	0	0	16	0	0	0	0	0	0	0	0	0	0	0	16	0	0	0	0	0	0	0	16	0
0	8	0	-8	0	-8	0	-8	0	-8	0	8	0	8	0	8	0	8	0	8	0	-8	0	8	0	8	0	8	0	-8	0	8
0	0	0	0	0	0	0	0	16	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-16	16	0	0	0	0	0	0
0	0	0	0	0	0	0	0	8	8	-8	-8	8	8	8	8	0	0	0	0	0	0	0	0	8	-8	-8	8	8	-8	8	-8
0	0	8	8	0	0	8	8	0	0	8	8	0	0	-8	-8	0	0	-8	8	0	0	-8	8	0	0	-8	8	0	0	8	-8
0	0	8	8	0	0	8	8	-8	-8	0	0	8	8	0	0	0	0	8	-8	0	0	8	-8	-8	8	0	0	8	-8	0	0
0	0	0	0	-16	0	0	0	0	0	0	0	0	16	0	0	0	0	0	0	16	0	0	0	0	0	0	0	0	16	0	0
0	-8	0	-8	0	-8	0	8	8	0	8	0	8	0	-8	0	0	8	0	8	0	8	0	-8	8	0	8	0	8	0	-8	0
0	0	8	8	0	0	-8	8	0	0	-8	-8	0	0	-8	8	0	0	-8	8	0	0	8	8	0	0	8	-8	0	0	8	8
0	-8	8	0	0	8	8	0	8	0	0	-8	-8	0	0	-8	0	8	8	0	0	-8	8	0	8	0	0	8	-8	0	0	8
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	16	-16	16	16	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-16	0	16	0	0	16	0	16	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8	8	8	-8	-8	-8	-8	8	8	8	8	-8	8	8	8	-8
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8	-8	-8	-8	-8	8	8	8	8	8	-8	8	8	8	-8	8
0	0	0	0	8	-8	8	8	0	0	0	0	8	-8	8	8	0	0	0	0	8	-8	8	8	0	0	0	0	-8	8	-8	-8
0	8	0	8	-8	0	8	0	0	8	0	8	-8	0	8	0	0	8	0	8	-8	0	8	0	0	-8	0	-8	8	0	-8	0
0	0	0	0	8	8	8	-8	0	0	0	0	8	8	8	-8	-8	-8	-8	8	0	0	0	0	8	8	8	-8	0	0	0	0
0	8	0	8	8	0	-8	0	0	8	0	8	8	0	-8	0	-8	0	8	0	0	-8	0	-8	8	0	-8	0	0	8	0	8
0	0	0	0	0	0	0	0	-16	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	16	16	0	0	0	0
0	0	0	0	0	0	0	0	8	-8	-8	8	8	-8	8	-8	0	0	0	0	0	0	0	0	-8	-8	8	8	8	8	8	8
0	0	-8	8	0	0	-8	8	0	0	-8	8	0	0	8	-8	8	8	0	0	8	8	0	0	8	8	0	0	-8	-8	0	0
0	0	8	-8	0	0	8	-8	-8	8	0	0	8	-8	0	0	8	8	0	0	8	8	0	0	0	0	-8	-8	0	0	8	8
0	0	0	0	8	-8	8	8	0	0	0	0	-8	8	8	8	0	0	0	0	-8	8	-8	-8	0	0	0	0	-8	8	8	8
0	8	0	8	-8	0	8	0	8	0	8	0	0	-8	0	8	0	-8	0	-8	8	0	-8	0	8	0	8	0	0	-8	0	8
0	0	-8	8	8	8	0	0	0	0	8	-8	8	8	0	0	8	8	0	0	0	0	-8	8	-8	-8	0	0	0	0	-8	8
0	8	8	0	8	0	0	-8	8	0	0	8	0	8	-8	0	8	0	0	-8	0	8	8	0	0	-8	8	0	-8	0	0	-8

1. Is S a permutation?
2. Is S a power function?
3. Find a lower bound on the degree of S.
4. Prove that S^{-1} has degree 2. More generally, prove that if all Walsh coefficients of a Boolean function f are divisible by 2^ℓ, then $\deg f \leq (n+1) - \ell$.

Exercise 3. (Degree of the composition of Sboxes)

1. Let us consider the 4-bit Sbox defined by the following table:

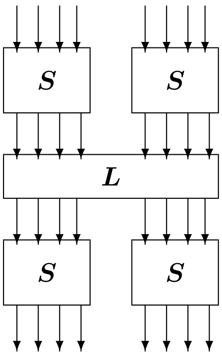
x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S(x)$	f	e	b	c	6	d	7	8	0	3	9	a	4	2	1	5
$S_1(x)$	1	0	1	0	0	1	1	0	0	1	1	0	0	0	1	1
$S_2(x)$	1	1	1	0	1	0	1	0	0	1	0	1	0	1	0	0
$S_3(x)$	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1
$S_4(x)$	1	1	1	1	0	1	0	1	0	0	1	1	0	0	0	0

   All its coordinates have degree 3:

$$\begin{aligned}
S_1(x_1,\ldots,x_4) &= 1 + x_1 + x_3 + x_4 + x_2x_3 + x_2x_4 + x_3x_4 + x_1x_3x_4 + x_2x_3x_4\\
S_2(x_1,\ldots,x_4) &= 1 + x_4 + x_1x_2 + x_1x_3 + x_1x_4 + x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4\\
S_3(x_1,\ldots,x_4) &= 1 + x_2 + x_4 + x_1x_2 + x_2x_3 + x_2x_4 + x_3x_4 + x_1x_2x_4 + x_1x_3x_4\\
S_4(x_1,\ldots,x_4) &= 1 + x_3 + x_4 + x_1x_3 + x_2x_4 + x_3x_4 + x_1x_3x_4 + x_2x_3x_4\ .
\end{aligned}$$

   - Give an upper bound on the degree of the 4-variable Boolean function corresponding to the product (S_1S_2).
   - Give an upper bound on the degree of the 4-variable Boolean function $(S_1S_2S_3)$.
   - Let δ_k denote the maximal degree of the product of k coordinates of S. Give an upper bound for each δ_k, $1 \leq k \leq 4$.
   - Prove that, for any n-bit bijective Sbox, $\delta_k = n$ if and only if $k = n$.

2. Give an upper bound on the degree of the following 2-round function



   Hint: first consider the degree of an 8-variable Boolean function

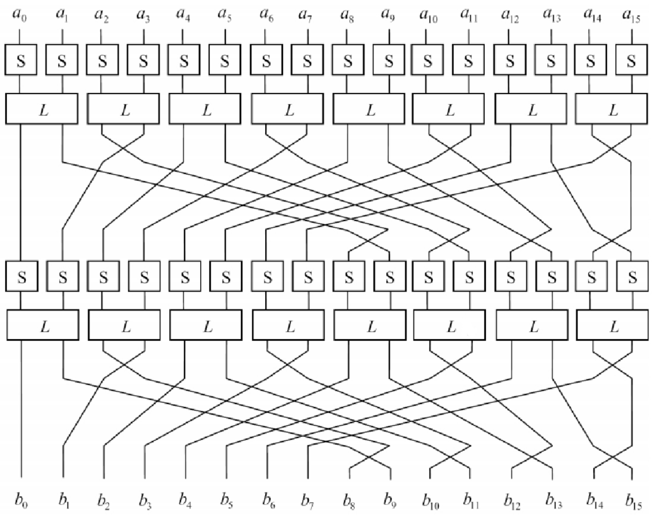
$$h(x_1,\ldots,x_8) := g(S(x_1,x_2,x_3,x_4), S(x_5,x_6,x_7,x_8))$$

   where g is an 8-variable Boolean function whose ANF consists of a single monomial of degree 3.

   More generally, it can be proved that, if F is an n-bit function defined by $F := (S,S,\ldots,S)$ with S an m-bit bijective Sbox, then, for any $G : \mathbf{F}_2^n \to \mathbf{F}_2^n$,

$$\deg(G \circ F) \leq n - \frac{n - \deg G}{m-1}\ .$$

3. Let us consider a cipher operating on 64-bit blocks, whose round function is defined as follows, where a_i and b_i denote 4-bit elements, S is a 4-bit Sbox and L an 8-bit linear function.



How many rounds are needed until the cipher reaches the highest possible degree?

Exercise 4. (Power permutations on $\mathbf{F}_{2^n}$, n even) Let n be an even integer, and s be an integer between 1 and $2^n - 1$.

1. Let α be a primitive element of $\mathbf{F}_{2^n}$ and $\beta = \alpha^{(2^n-1)/3}$. Prove that β is a solution of

$$(x+1)^s + x^s = 1$$

unless $s \bmod 3 = 0$.

2. Deduce that there is no power permutation on $\mathbf{F}_{2^n}$ when n even.