Task 5. «Super-Sboxes for AES: differential characteristics»

Special Prize from the Program Committee!

Let $\mathbb{F}_{256}$ be the finite field of 256 elements and α be a primitive element (it means that for any nonzero $x \in \mathbb{F}_{256}$ there exists $i \in \mathbb{N}$ such that $x = \alpha^i$). Let $\mathbb{F}_{256}^4$ be the vector space of dimension 4 over $\mathbb{F}_{256}$. Thus, any element $x \in \mathbb{F}_{256}^4$ is $x = (x_1, x_2, x_3, x_4)$, where $x_i \in \mathbb{F}_{256}$. An arbitrary function from $\mathbb{F}_{256}^4$ to $\mathbb{F}_{256}^4$ can be considered as the set of 4 coordinate functions from $\mathbb{F}_{256}^4$ to $\mathbb{F}_{256}$. Define the following auxiliary functions $F_4, M : \mathbb{F}_{256}^4 \to \mathbb{F}_{256}^4$:

$$F_4(x_1, x_2, x_3, x_4) = (x_1^{254}, x_2^{254}, x_3^{254}, x_4^{254});$$

$$M(x_1, x_2, x_3, x_4) = (x_1, x_2, x_3, x_4) \times \begin{bmatrix} \alpha+1 & 1 & 1 & \alpha \\ \alpha & \alpha+1 & 1 & 1 \\ 1 & \alpha & \alpha+1 & 1 \\ 1 & 1 & \alpha & \alpha+1 \end{bmatrix}.$$

Consider the function $G : \mathbb{F}_{256}^4 \to \mathbb{F}_{256}^4$ that is a combination of F_4 and M:

$$G(x_1, x_2, x_3, x_4) = F_4(M(F_4(x_1, x_2, x_3, x_4))).$$

Find the number of solutions of the equation $G(x + a) = G(x) + b$, where parameters a and b run all nonzero values from $\mathbb{F}_{256}^4$.

Foundation of the problem. J. Daemen and V. Rijmen, the designers of AES (Rijndael), have introduced the Super-Sbox representation of two rounds of AES in order to study differential properties. The function G can be considered as a simplified Super-Sbox model of two rounds of AES. To study resistance of AES to differential cryptanalysis, we welcome you to start with differential characteristics of the function G.