



Task 7. «A special parameter»

In differential cryptanalysis of block ciphers a special parameter P is used to measure the diffusion strength. In this task we study its properties.

Let n, m be positive integer numbers. Let $a = (a_1, \dots, a_m)$ be a vector, where a_i are elements of the finite field \mathbb{F}_{2^n} . Denote by $\text{wt}(a)$ the number of nonzero coordinates a_i , $i = 1, \dots, m$, and call this number the *weight* of a .

We say that $a, b \in \mathbb{F}_{2^n}^m$ represent *states*. The sum of two states a, b is defined as $a + b = (a_1 + b_1, \dots, a_m + b_m)$.

Thus, the *special parameter* P of a function $\varphi : \mathbb{F}_{2^n}^m \rightarrow \mathbb{F}_{2^n}^m$ is given by

$$P(\varphi) = \min_{a, b, \text{ such that } a \neq b} \{ \text{wt}(a + b) + \text{wt}(\varphi(a) + \varphi(b)) \}.$$

- Rewrite (simplify) the definition of $P(\varphi)$ when the function φ is linear (recall that a function ℓ is linear if for any x, y it holds $\ell(x + y) = \ell(x) + \ell(y)$).
- Rewrite the definition of $P(\varphi)$ in terms of linear codes, when the linear transformation φ is given by a $m \times m$ matrix M over \mathbb{F}_{2^n} , i. e. $\varphi(x) = M \cdot x$.
- Let φ be an arbitrary function. Find a tight upper bound for $P(\varphi)$ as a function of m .
- Can you give an example of the function φ with the maximal possible value of P ?