Task 2. «An APN Permutation»

Special Prize from the Program Committee!

Suppose we have a mapping F from $\mathbb{F}_2^n$ to itself (recall that $\mathbb{F}_2^n$ is the vector space of all binary vectors of length n). This mapping is called a **vectorial Boolean function in n variables**. Such functions are used, for example, as S-boxes in block ciphers and should have special cryptographic properties. In this task we consider the following two properties and the problem of combining them.

- A function F in n variables is a **permutation** if for all distinct vectors $x, y \in \mathbb{F}_2^n$ it has distinct images, i. e. $F(x) \neq F(y)$.
- A function F in n variables is called **Almost Perfect Nonlinear** (APN) if for any nonzero vector $a \in \mathbb{F}_2^n$ and any vector $b \in \mathbb{F}_2^n$ an equation $F(x) \oplus F(x \oplus a) = b$ has at most 2 solutions. Here $\oplus$ is the coordinate-wise sum of vectors modulo 2.

Try to find an APN permutation in 8 variables or prove that it doesn't exist.

History of the problem. The question «Does there exist an APN permutation in even number of variables?» has been studied for more that 20 years. If the number of variables is odd, APN permutations exist as it was proved by K. Nyberg (1994). It is known that for 2 and 4 variables the answer is «No». But for 6 variables J.F. Dillon and K. Browning, M. McQuistan, A.J Wolfe have found such a function in 2009! You can see it bellow:

$$G = \left(\begin{array}{cccccccccccccccc} 0 & 54 & 48 & 13 & 15 & 18 & 53 & 35 & 25 & 63 & 45 & 52 & 3 & 20 & 41 & 33 \\ 59 & 36 & 2 & 34 & 10 & 8 & 57 & 37 & 60 & 19 & 42 & 14 & 50 & 26 & 58 & 24 \\ 39 & 27 & 21 & 17 & 16 & 29 & 1 & 62 & 47 & 40 & 51 & 56 & 7 & 43 & 44 & 38 \\ 31 & 11 & 4 & 28 & 61 & 46 & 5 & 49 & 9 & 6 & 23 & 32 & 30 & 12 & 55 & 22 \end{array} \right).$$

This function is presented as the list of its values, i. e. $G(0) = 0$, $G(4) = 15$, $G(16) = 59$ and so on. For brevity we use integers instead of binary vectors. A binary vector $x = (x_1, \ldots, x_n)$ corresponds to an integer $k_x = x_1 \cdot 2^{n-1} + x_2 \cdot 2^{n-2} + \ldots + x_{n-1} \cdot 2 + x_n$.

Thus, you are welcome to study the next case, $n = 8$.