Problem 10. «APN + Involutions»

Alice wants to construct a block cipher with heavy use of **involutions** as its subcomponents; this minimizes difference in the algorithms for encryption and decryption. She knows that **almost perfect nonlinear permutations** (**APN permutations**) are the best choice of subcomponents to resist attacks based on differential technique. She wants to construct a set of APN permutations that are involutions for every $n \geqslant 2$.

Alice also knows that any involution can be expressed as the product of disjoint **transpositions**. So, she decides to study the following involution

$$g = \prod_{i=1}^{d} (\alpha_i, {\alpha'}_i),$$

where $\{\alpha_i, {\alpha'}_i\} \cap \{\alpha_j, {\alpha'}_j\} = \emptyset$ for all $i, j \in \{1, ..., d\}$, $i \neq j$, $1 \leqslant d \leqslant 2^{n-1}$.

Alice needs your help to get APN permutations among such involutions g. Find answers to the following questions!

Q1 Let

$$\Lambda(g) = \{\alpha_i \oplus {\alpha'}_i : \ i = 1, ..., d\}, \qquad \widehat{\Lambda}(g) = [\alpha_i \oplus {\alpha'}_i : \ i = 1, ..., d],$$
$$\mathrm{B}(g) = \{x \oplus y : \ \{x, y\} \subseteq \mathrm{FixP}(g), \ x \neq y\}, \quad \widehat{\mathrm{B}}(g) = [x \oplus y : \ \{x, y\} \subseteq \mathrm{FixP}(g), \ x \neq y],$$

where $\mathrm{FixP}(g)$ is the set of all **fixed points** of g, i. e. $\mathrm{FixP}(g) = \{x \in \mathbb{F}_2^n : \ g(x) = x\}$.

Suppose that g is an APN permutation. Get necessary conditions for multisets $\widehat{\Lambda}(g)$, $\widehat{\mathrm{B}}(g)$ and sets $\Lambda(g)$, $\mathrm{B}(g)$. Prove that if your conditions are not satisfied, then g is not an APN permutation.

Q2 Let

$$\mathrm{d}_{a,b}(g) = |\{x \in \mathbb{F}_2^n : \ g(x \oplus a) \oplus g(x) = b\}|, \quad a, b \in \mathbb{F}_2^n.$$

Let g be an involution and APN. Find $\mathrm{d}_{a,a}(g)$ for each nonzero $a \in \mathbb{F}_2^n$.

Q3 Can you get the nontrivial upper bound on $|\mathrm{FixP}(g)|$?

Q4 Let M_n be the set of all n-bit involutions that are APN permutations.

(a) Can you find the cardinality of M_n for $n = 2, 3, 4$?

(b) Can you find the cardinality of M_n for $n = 5$?

(c) Bonus problem (extra scores, a special prize!)
Let $n \geqslant 6$. Can you get the lower and the upper bounds for the cardinality of M_n? Can you describe involutions from M_n? Can you suggest constructions for involutions from M_n?

Note that the mapping $x \mapsto x^{-1}$ in the Galois field $GF(2^n)$ belongs to M_n for odd $n \geqslant 3$.

Turn to the next page.

Remark. Let us recall the relevant definitions.

- $\mathbb{F}_2^n$ is the vector space of dimension over $\mathbb{F}_2 = \{0, 1\}$.
- A vector $x \in \mathbb{F}_2^n$ has the form $x = (x_1, ..., x_n)$, where $x_i \in \mathbb{F}_2$. For two vectors $x, y \in \mathbb{F}_2^n$ their sum is $x \oplus y = (x_1 \oplus y_1, ..., x_n \oplus y_n)$, where $\oplus$ stands for XOR operation.
- Let $\widehat{X} = \left[x_1, ..., x_d\right]$ be a multiset with the underlying set $\mathbb{F}_2^n$, where $x_1, ..., x_d \in \mathbb{F}_2^n$.
  Note that all elements in a set are distinct. Unlike a set, a multiset allows for multiple instances for each of its elements.
- A **permutation** s is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ such that $s(x) \neq s(y)$ for all $x, y \in \mathbb{F}_2^n$, $x \neq y$.
- An **involution** s is a permutation that is its own inverse, $s^2(x) = s(s(x)) = x$ for all $x \in \mathbb{F}_2^n$.
- For any different vectors $\alpha, \beta \in \mathbb{F}_2^n$, a permutation s is called a **transposition** if $s(\alpha) = \beta$, $s(\beta) = \alpha$ and $s(x) = x$ for all $x \in \mathbb{F}_2^n \setminus \{\alpha, \beta\}$; it is denoted by $s = (\alpha, \beta)$.
- A permutation s is called **APN** (Almost Perfect Nonlinear) if, for every nonzero $a \in \mathbb{F}_2^n$ and every $b \in \mathbb{F}_2^n$, the equation $s(x \oplus a) \oplus s(x) = b$ has at most 2 solutions.