2-to-1 functions as subfunctions of APN permutations[1]

Valeriya Idrisova[2,3]

[2]Sobolev Institute of Mathematics, Novosibirsk, Russia
[3]Novosibirsk State University, Novosibirsk, Russia

E-mail: vitkup@math.nsc.ru

Abstract. Our talk is devoted to the longstanding problem of APN permutation existence for even number of variables. This problem is referred to as "the Big APN problem" and it is stated as Problem 3.7 in [1]. Let us recall some definitions. Let F be a vectorial Boolean function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. For vectors $a, b \in \mathbb{F}_2^n$, where $a \neq 0$, consider the value

$$\delta(a,b) = \big|\{\ x \in \mathbb{F}_2^n \ \big|\ F(x+a) + F(x) = b\}\big|.$$

Denote by Δ_F the following value:

$$\Delta_F = \max_{a \neq \mathbf{0},\ b \in \mathbb{F}_2^n} \delta(a,b).$$

Then F is called *differentially* Δ_F*-uniform* function. The smaller the parameter Δ_F the better the resistance of a cipher containing F as an S-box to differential cryptanalysis. For the vectorial functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ the minimal possible value of Δ_F is equal to 2. In this case the function F is called *almost perfect nonlinear (APN)*. This notion was introduced by K. Nyberg in [3]. The vectorial Boolean function F_j' from $\mathbb{F}_2^n$ to $\mathbb{F}_2^{n-1}$ is called an $(n-1)$-*subfunction* of function $F = (f_1, \ldots, f_n)$ if $F_j' = (f_1, \ldots, f_{j-1}, f_{j+1}, \ldots, f_n)$ for some $j \in \{1, \ldots, n\}$.

At BFA-2017 an algorithm for searching 2-to-1 APN functions that are potentially EA-equivalent to permutations was presented [2]. That algorithm based upon constructing of special symbol sequences that are called admissible. In this work we considered 2-to-1 functions that are isomorphic to $(n-1)$-subfunctions of APN permutations and studied their differential properties. We proved that any such 2-to-1 function is differentially 4-uniform and its vector of values has a structure of an admissble sequence. Therefore, corresponding $(n-1)$-subfunction of an APN permutation can be derived by that algorithm as well. We can check all possible coordinate Boolean functions f such that the bijective function constructed from derived $(n-1)$-subfunction and this function is APN. So, this fact allows us to search for new APN permutations.

Keywords. APN function, Permutation, Subfunction.

References

[1] Carlet C.: Open Questions on Nonlinearity and on APN Functions. Arithmetic of Finite Fields, Lecture Notes in Computer Science. 9061, 83–107 (2015).
[2] Idrisova V. On APN functions EA-equivalent to permutations // Abstracts of the 2nd International Workshop on Boolean Functions and their Applications (BFA) (2017).
[3] Nyberg K.: Differentially uniform mappings for cryptography. Advances in Cryptography, EUROCRYPT'93, Lecture Notes in Computer Science, vol. 765, pp.55-64 (1994).

[1]The author was supported by the Russian Foundation for Basic Research (projects 18-31-00374 and 18-07-01394)