Differential equivalence of APN functions: results and open problems[1]

Anastasiya Gorodilova*,**

*Sobolev Institute of Mathematics, Novosibirsk, Russia
**Novosibirsk State University, Novosibirsk, Russia

E-mail: gorodilova@math.nsc.ru

Abstract. This work is devoted to APN functions. Recall that a function F from $\mathbb{F}_2^n$ to itself is called *almost perfect nonlinear* (APN) if for any $a, b \in \mathbb{F}_2^n$, $a \neq \mathbf{0}$, equation $F(x) + F(x + a) = b$ has at most 2 solutions.

The problem considered is how to classify APN functions under the differential equivalence. We call two functions *differentially equivalent* [2] if their associated Boolean functions are equal. The *associated Boolean function* $\gamma_F(a, b)$ in $2n$ variables of a function F on $\mathbb{F}_2^n$ was defined by C. Carlet, P. Charpin, V. Zinoviev in 1998 as follows: it takes value 1 iff $a \neq \mathbf{0}$ and equation $F(x) + F(x + a) = b$ has solutions. To describe the differential equivalence class of a given APN function is an open problem of great interest: it is stated as Problem 3.11 in [1].

We started to investigate the problem by considering what affine functions do not change the associated Boolean function when adding to a given quadratic APN function. Surprisingly, we got that there are only 2^{2n} *trivial* such affine functions for almost all known quadratic APN functions in small number of variables n up to 8 (there are only three exceptional cases up to EA-equivalence). Moreover, we formulated a conjecture: if two quadratic APN functions F and G are differentially equivalent, then $F + G$ is affine. This conjecture was proved for $n \leqslant 6$.

Also, we theoretically found the first infinitive family of APN functions having nontrivial differential equivalence class by studying the APN Gold functions. Namely, the APN Gold function $F(x) = x^{2^k+1}$ with $k = n/2 - 1$ and $n = 4t$ has exactly $2^{2n+n/2}$ affine functions that lead to differentially equivalent to F functions when adding to F.

As well, new properties of the associated Boolean functions of quadratic APN functions were obtained and a new notion of *linear spectrum* of a quadratic APN function was studied.

Keywords: almost perfect nonlinear function, differential equivalence, APN Gold function, linear spectrum.

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] Gorodilova A. On differential equivalence of APN functions // Cryptology ePrint Archive, Report 2017/907 (2017).

[1] The author was supported by the Russian Foundation for Basic Research (projects 18-31-00479, 18-07-01394).