Утверждение 5. Пусть $g(x+2y) = a(x,y) + 2b(x,y)$, где $x, y \in \mathbb{Z}_2^n$ и a, b — булевы функции от $2n$ переменных, является бент-функцией. Тогда функция $g'(x+2y) = 3a(x,y)+2b(x,y)$ также является кватернарной бент-функцией от $n \geqslant 1$ переменных.

Отметим, что утверждение верно и в обратную сторону.

ЛИТЕРАТУРА

1. *Matsui M.* Linear cryptanalysis method for DES cipher // Eurocrypt'1993. LNCS. 1994. V. 765. P. 386–397.
2. *Adams C.* Constructing symmetric ciphers using the CAST design procedure // Design, Codes, and Cryptography. 1997. V. 12. No. 3. P. 283–316.
3. *Hell M., Johansson T., Maximov A., and Meier W.* A stream cipher proposal: Grain-128 // IEEE Intern. Symp. Inform. Theory. Seattle, WA, 2006. P. 1614–1618.
4. *Tokareva N.* Bent Functions: Results and Applications to Cryptography. Acad. Press, Elsevier, 2015. 230 p.
5. *Kumar P. V., Scholtz R. A., and Welch L. R.* Generalized bent functions and their properties // J. Combin. Theory. 1985. V. 40. No. 1. P. 90–107.
6. *Solé P. and Tokareva N.* Connections Between Quaternary and Binary Bent Functions // Cryptology ePrint Archive, Report 2009/544. `http://eprint.iacr.org/`.
7. *Solé P. and Tokareva N.* On quaternary and binary bent functions // Прикладная дискретная математика. Приложение. 2009. № 1. С. 16–18.

UDC 519.7 DOI 10.17223/2226308X/13/11

ON A SECONDARY CONSTRUCTION OF QUADRATIC APN FUNCTIONS[1]

K. V. Kalgin, V. A. Idrisova

Almost perfect nonlinear functions possess the optimal resistance to the differential cryptanalysis and are widely studied. Most known constructions of APN functions are obtained as functions over finite fields $\mathbb{F}_{2^n}$ and very little is known about combinatorial constructions in $\mathbb{F}_2^n$. We consider how to obtain a quadratic APN function in $n+1$ variables from a given quadratic APN function in n variables using special restrictions on new terms.

Keywords: *vectorial Boolean function, APN function, quadratic function, secondary construction.*

Let us recall some definitions. Let $\mathbb{F}_2^n$ be the n-dimensional vector space over $\mathbb{F}_2$. A function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, where n and m are integers, is called a *vectorial Boolean function*. If $m = 1$, such a function is called *Boolean*. Every vectorial Boolean function F can be represented as a set of m *coordinate functions* $F = (f_1, \ldots, f_m)$, where f_i is a Boolean function in n variables. Any vectorial function F can be represented uniquely in its *algebraic normal form* (ANF):

$$F(x) = \sum_{I \in \mathcal{P}(N)} a_I \left(\prod_{i \in I} x_i\right),$$

where $\mathcal{P}(N)$ is a power set of $N = \{1, \ldots, n\}$ and $a_I \in \mathbb{F}_2^m$. The *algebraic degree* of a given function F is the degree of its ANF: deg $(F) = \max\{|I| : a_I \neq 0, I \in \mathcal{P}(N)\}$. If algebraic

[1]The work was carried out within the framework of the state contract of the Sobolev Institute of Mathematics (project no. 0314-2019-0017) and supported by RFBR (projects no. 18-07-01394, 20-31-70043) and Laboratory of Cryptography JetBrains Research.

degree of a function F is not more than 1, then F is called *affine*. If for an affine function F it holds $F(\mathbf{0}) = \mathbf{0}$, then F is called *linear*. If algebraic degree of a function F is equal to 2, then F is called *quadratic*. Two vectorial functions F and G are *extended affinely equivalent* (*EA-equivalent*) if $F = A_1 \circ G \circ A_2 + A$, where A_1, A_2 are affine permutations on $\mathbb{F}_2^n$ and A is an affine function. 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

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

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 is, 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 [1]. APN fuctions draw attention of many researchers, but there is still a significant list (see, for example, [2–4]) of important open questions. We are especially interested how to find new constructions of APN functions in vector space $\mathbb{F}_2^n$, since almost all the known constructions of this class are found only as polynomials over the finite fields, and to the best of our knowledge, only a few approaches to such combinatorial constructions was proposed [5, 6].

Since EA-equivalence preserves APNness, it is always possible to omit linear and constant terms in the algebraic normal form of a given APN function. Further we will consider quadratic vectorial Boolean functions that have only quadratic terms in their ANF. The following theorem gives a necessary condition on the ANF of a given APN function.

Theorem 1 [7]. Let $F = (f_1, \ldots, f_n)$ be an APN function in n variables. Then every quadratic term $x_i x_j$, where $i \neq j$, appears at least in one coordinate function of F.

This property motivated us to suggest the following construction of quadratic APN functions. Let $G = (g_1, \ldots, g_n)$ be a quadratic APN-function in n variables. Consider vectorial function $F = (f_1, \ldots, f_n, f_{n+1})$ in $n+1$ variables such that

$$\begin{aligned} f_1 &= g_1 + \sum_{i=1}^{n} \alpha_{1,i} x_i x_{n+1}, \\ &\ldots \\ f_n &= g_n + \sum_{i=1}^{n} \alpha_{n,i} x_i x_{n+1}, \\ f_{n+1} &= g_{n+1} + \sum_{i=1}^{n} \alpha_{n+1,i} x_i x_{n+1}, \end{aligned} \tag{1}$$

where $\alpha_{1,i} \ldots, \alpha_{n+1,i} \in \mathbb{F}_2$ for $i = 1, \ldots, n$ and $g_{n+1} = \sum\limits_{1\leqslant j<k\leqslant n} \beta_{j,k} x_j x_k$ for some fixed $\beta_{j,k} \in \mathbb{F}_2$. Note that if $\alpha_{1,i}, \ldots, \alpha_{n,i}$ are such that each term $x_i x_{n+1}$ appears at least in one of the coordinate functions $f_1, \ldots, f_n$, then the necessary condition of Theorem 1 is held for the constructed function F.

Each quadratic vectorial function G in n variables can be considered as a symmetric matrix $\mathcal{G} = (g_{ij})$, where each element $g_{ij} \in \mathbb{F}_2^n$ is a vector of coefficients corresponding to term $x_i x_j$ in the algebraic normal form of G and all diagonal elements g_{ii} are null. It is necessary to mention that these matrices are essentially the same as so-called QAM matrices that were used in [8, 9] to construct and classify a lot of new quadratic APN functions over finite fields. Using these matrices, the APN property can be formulated in the following way:

Proposition 1. Let $\mathcal{G}$ be the matrix that corresponds to quadratic vectorial function G. Then function G is APN if and only if $x\,(\mathcal{G} \cdot a) \neq 0$ for all $x \neq a$, where $a, x \in \mathbb{F}_2^n$ and $a \neq \mathbf{0}$.

In terms of matrices, the construction (1) can be considered as an extension of a given $\mathcal{G}$ with an extra bit that represents g_{n+1} in every element and an extra pair of row and column that represents a set of new terms $x_i x_{n+1}$.

Consider a quadratic APN function G and the corresponding $n \times n$ matrix $\mathcal{G}$. Denote the vector of nonzero coefficients as $\alpha = (\alpha_1, \ldots, \alpha_n)$. Let us fix g_{n+1} and construct $(n+1) \times (n+1)$ matrix $\mathcal{F}$ by adding $(\alpha_1, \ldots, \alpha_n, 0)$ as the last column and the last row and adding new bit to every element according to the choice of g_{n+1}. Let us denote as $\mathcal{G}'$ the submatrix (f_{ij}) of $\mathcal{F}$, such that $i, j < n+1$. Let $\langle X \rangle$ denote the linear span of X and F be the quadratic vectorial function corresponding to the constructed matrix $\mathcal{F}$.

Theorem 2. A function F is APN if and only if $\alpha \cdot a'$ does not belong to $\langle \mathcal{G}' \cdot a' \rangle$ for all $a' \in \mathbb{F}_2^n$, $a' \neq \mathbf{0}$.

Theorem 2 shows how to choose new coefficients $\alpha_{1,i} \ldots, \alpha_{n+1,i} \in \mathbb{F}_2$ in the construction (1) such that an obtained function F is APN. When $n = 3, 4$ and 5, for APN functions that are representatives of EA classes, all possible classes of quadratic APNs are obtained for $4, 5$ and 6 variables from the classification [10] and large variety of classes for constructing functions in 6 and 7 variables.

REFERENCES

1. *Nyberg K.* Differentially uniform mappings for cryptography. EUROCRYPT'93, LNCS, 1994, vol. 765, pp. 55–64.
2. *Carlet C.* Open questions on nonlinearity and on APN Functions. WAIFI 2014, LNCS, 2015, vol. 9061, pp. 83–107.
3. *Glukhov M. M.* O priblizhenii diskretnykh funktsiy lineynymi funktsiyami [On the approximation of discrete functions by linear functions]. Matematicheskie Voprosy Kriptografii, 2016, vol. 7, no. 4, pp. 29–50. (in Russian)
4. *Tuzhilin M. E.* Pochti sovershennye nelineynye funktsii [APN-functions]. Prikladnaya Diskretnaya Matematika, 2009, no. 3(5), pp. 14–20. (in Russian)
5. *Gorodilova A. A.* Characterization of almost perfect nonlinear functions in terms of subfunctions. Discrete Math. Appl., 2016, vol. 26, iss. 4, pp. 193–202.
6. *Idrisova V. A.* On an algorithm generating 2-to-1 APN functions and its applications to "the big APN problem". Cryptogr. Commun., 2019, no. 11, pp. 21–39.
7. *Beth T. and Ding C.* On almost perfect nonlinear permutations. EUROCRYPT'93, LNCS, 1993, vol. 765, pp. 65–76.
8. *Yu Y., Wang M., and Li Y.* A matrix approach for constructing quadratic APN functions. Des. Codes Cryptogr., 2014, no. 73, pp. 587–600.
9. *Yu Y., Kaleyski N. S., Budaghyan L., and Li Y.* Classification of Quadratic APN Functions with Coefficients in GF(2) for Dimensions up to 9. IACR Cryptol. ePrint Arch.: 1491, 2019.
10. *Brinkmann M. and Leander G.* On the classification of APN functions up to dimension five. Des. Codes Cryptogr., 2008, vol. 49, iss. 1–3, pp. 273–288.