2-to-1 functions as subfunctions of APN permutations

Valeriya Idrisova

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

BFA-2018, Loen, Norway

Definitions

A *vectorial Boolean function* is an arbitrary mapping F from $\mathbb{F}_2^n$ into $\mathbb{F}_2^m$. Every vectorial function can be represented as set of m *coordinate* Boolean functions in n variables: $F = (f_1, ..., f_m)$.

A vectorial function F from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$ is called *2-to-1 function* if it's vector of values consists of 2^{n-1} different elements and F takes every value twice.

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

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

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.

Definitions

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)*. These notions were introduced by K. Nyberg [1]. It is also known that APN functions were investigated by V. Bashev and B. Egorov in USSR.

[1] Nyberg K. Differentially uniform mappings for cryptography // Eurocrypt 1993, Lecture Notes in Computer Science, 1994 V. 765. P. 55–64.

The Big APN problem

One of the most interesting problems in this area is constructing bijective APN functions in even dimensions. There was a conjecture that such functions do not exist (it was proved for $n = 4$), but in 2009 J.F.Dillon et al.[2] presented the first APN permutation for n = 6.

This question is still open for the greater dimensions and it is referred as **"The Big APN problem"**.

[2] McQuistan M. T., Wolfe A. J., Browning K. A., Dillon J. F. An apn permutation in dimension six.// American Mathematical Society, 2010 V. 518. P. 33–42.

$(n-1)$-subfunctions

Consider an arbitrary vectorial Boolean function $F = (f_1, \dots, f_n)$ from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$.

The vectorial Boolean function F_j' from $\mathbb{F}_2^n$ to $\mathbb{F}_2^{n-1}$ is called an $(n-1)$-*subfunction* of F if $F_j' = (f_1, \dots, f_{j-1}, f_{j+1}, \dots, f_n)$ for some $j \in \{1, \dots, n\}$.

We can consider any $(n-1)$-subfunction F_j' from $\mathbb{F}_2^n$ to $\mathbb{F}_2^{n-1}$ as a vectorial function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ that can take values only from the set $\{0, \dots, 2^{n-1}-1\}$ and, thus, is isomorphic to F_j'.

Let us consider a 2-to-1 function that takes values from $\{0, \ldots, 2^{n-1} - 1\}$. We denote the set of such 2-to-1 functions in n variables through $\mathcal{T}_n$.

Let us note that any $(n-1)$-subfunction of a bijective vectorial function is a function from $\mathcal{T}_n$.

Proposition 1. Let F be an APN permutation in n variables. Then any of its $(n-1)$-subfunction is a differentially 4-uniform function from $\mathcal{T}_n$.

$(n-1)$-subfunctions as admissible sequences

An algorithm for searching 2-to-1 APN functions that are potentially EA-equivalent to permutations was presented [3]. That algorithm based upon constructing of special symbol sequences.

Consider the vector of values of an arbirtrary 2-to-1 vectorial function. The definition of an APN function implies certain restrictions on its structure. In particular, for any non-zero $a \in \mathbb{F}_2^n$ and any different x_1 and x_2 from $\mathbb{F}_2^n$ such that $x_1 + a \neq x_2$ the following relation holds $F(x_1 + a) + F(x_1) \neq F(x_2 + a) + F(x_2)$.

[3] Idrisova V.On an algorithm generating 2-to-1 APN functions and its applications to "the big APN problem"// Cryptography and Communications, 2018, published online.

Symbol sequences, satisfying the restrictions mentioned above, are called *admissible*.

For example, the sequence $\alpha\ \alpha\ \beta\ \beta\ \theta\ \epsilon\ \theta\ \epsilon$ is not admissible, since for $a = 001$ holds $F(000+001)+F(000) = \alpha+\alpha = 000$ and $F(010+001)+F(010) = \beta+\beta = 000$, that contradicts these restrictions.

We observed that vectors of values of all 2-to-1 functions corresponded to their $(n-1)$-subfunctions can be obtained from 2-to-1 admissible sequences.

Proposition 2. Let F be an APN permutation in n variables. Then the 2-to-1 symbol sequence corresponding to the vector of values for any $(n-1)$-subfunction of F is an admissible sequence.

$(n-1)$-subfunctions of APN permutations

According to the Proposition 2 every APN permutation can be derived from a 2-to-1 differential 4-uniform function obtained from an admissible sequence.

If such function is given, we need to check all possible coordinate Boolean functions f such that the permutation constructed from $(n-1)$-subfunction and this function is APN. Generally, we need to check $2^{2^{n-1}}$ Boolean functions in order to the find necessary coordinate function.

Proposition 3. For any n vectorspace $\mathbb{F}_2^n$ can be represented as $\mathbb{F}_2^n = V_1 \cup V_2$, where $|V_i| = 2^{n-1}$, such that for every two vectors $v_1, w_1 \in V_1$ and for every two vectors $v_2, w_2 \in V_2$ holds $v_i + w_i \in V_2$.

Consider bijective function $F = (f_1, \dots, f_n)$. Let us fix k coordinates $f_{i_1}, \dots, f_{i_k}$. Given V_1, V_2 such that $\mathbb{F}_2^k = V_1 \cup V_2$, we can split $\mathbb{F}_2^n$ into subsets $\mathcal{F}_1$ and $\mathcal{F}_2$ defined as follows:

$$\mathcal{F}_i = \{(f_1(x), \dots, f_n(x)) \mid f_{i_1}(x), \dots, f_{i_k}(x) \in V_i, x \in \mathbb{F}_2^n\}$$

.

Given permutation F of $\mathbb{F}_2^n$, value k, sets V_1, V_2 such that $\mathbb{F}_2^k = V_1 \cup V_2$, indices $i_1, \ldots, i_k$ and index $j \notin \{i_1, \ldots, i_k\}$, let us define associated permutation $F^\star$ as follows:

$$F^\star(x) = \begin{cases} F(x), & \text{if } F(x) \in \mathcal{F}_1; \\ F(x) + e_j, & \text{if } F(x) \in \mathcal{F}_2. \end{cases}$$

Theorem 1. Permutation F is APN if and only if permutation $F^\star$ is APN.

Let S be a 2-to-1 vectorial differentially 4-uniform function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ with values from $\{0, \ldots, 2^{n-1} - 1\}$ that can be represented as a $(n-1)$-subfunction $S = (s_1, \ldots, s_{n-1})$.

Theorem 2. Let $nf(S)$ be the number of coordinate functions f such that function $H = S \cup f$ is an APN permutation. If $nf(S) \neq 0$ then $nf(S) \geqslant 2^n$.

Remark. Without loss of generality we can assume here $H = S \cup f = (s_1, \ldots, s_{n-1}, f)$.

The bound from Theorem 2 is exact for $n = 3, 5$ and all checked sporadic examples for $n = 6$.

On the algorithm

Let us suggest some ideas how to implement an algorithm of searching these Boolean functions for the given 2-to-1 function. If a $(n-1)$-subfunction $S = (s_1, \ldots, s_{n-1})$ is fixed, we can choose an arbitrary Boolean function f such that $H = S \cup f$ is a permutation.

Let us note that if there exists a Boolean function f' such that $H' = S \cup f'$ is an APN permutation, then f' can be derived by consequent swapping values of f that are corresponded to the same pair of coincided values of 2-to-1 function S.

If we enumerate pairs of coincided values of S, we can encode this swapping using binary vectors of length 2^{n-1}. We put 1 in i-th coordinate, if values of i-th pair were swapped and put 0 otherwise. So, all possible $2^{2^{n-1}}$ Boolean functions can be represented as sum

$$\sum_{j=0}^{2^{n-1}} \binom{2^{n-1}}{j} = 2^{2^{n-1}},$$

where $\binom{2^{n-1}}{j}$ is the number of Boolean functions obtained from f with j swaps.

For any vector v' with $wt(v') > 2^{n-2}$ corresponded Boolean function f' is equal to $f'' + \mathbf{1}$ for some function f'' with corresponded vector v'' such that $wt(v'') < 2^{n-2}$. So, if permutation $H' = S \cup f'$ is APN, permutation $H'' = S \cup f''$ is also APN, since H' and H'' are EA-equivalent. Therefore we can consider only vectors $v \in \mathbb{F}_2^{2^{n-1}}$ with $wt(v) \leqslant 2^{n-2}$.

Open problems

There left the following open questions:

1. Given differentially 4-uniform function S from $\mathcal{T}_n$ that can be considered as a $(n-1)$-subfunction, does there always exist Boolean function f such that $H = S \cup f$ is an APN permutation? It is interesting that there are no 2-to-1 differentially 4-uniform functions from $\mathcal{T}_n$ when $n = 4$.

2. We can consider the statement of Theorem 1 as a relationship of equivalence for APN permutations. How does this equivalence correlate with notions of EA- and CCZ-equivalence?

Thank you for your attention!