IET Information Security

Comment

ISSN 1751-8709
Received on 1st March 2018
Accepted on 10th January 2019
E-First on 29th April 2019
doi: 10.1049/iet-ifs.2018.5062
www.ietdl.org

Research on highly non-linear plateaued functions

Tianfeng Sun[1] ✉, *Bin Hu*[1], *Yang Yang*[1]

[1] *Information Science and Technology Institute, High-Tech zone, Zheng Zhou, People's Republic of China*

✉ *E-mail: enjoy2152013@163.com*

Abstract: Here, the authors correct the proof in the reference when explaining that the produced plateaued functions have no non-zero linear structures. Moreover, a new class of plateaued functions with the best algebraic degree is given.

1 Introduction

It is well-known that Boolean functions play an important role in the design of cryptography, coding theory, and so on [1]. To satisfy the requirements in applications, Boolean functions should have good cryptographic properties such as balancedness, high algebraic degree, high non-linearity, resiliency order, and so on. There exist constraint relations among the cryptographic properties such as algebraic degree and resiliency order, non-linearity, and resiliency order [2].

The notion of plateaued function was first introduced in [3], which provides some examples of good trade-off among all the properties needed in applications. Therefore, the study of plateaued function becomes necessary and important, but our knowledge on them is not at a level corresponding to their importance.

As for the primary construction of plateaued functions, we can refer to the reference [3–6]. As for the second construction and other constructions, they are also important to obtain plateaued functions approaching or achieving the best trade-off among the cryptographic properties. These constructions can be seen in [7–10].

The organisation of this paper is as follows. Some basic concepts and notions are presented in Section 2. It is shown that there exist faults in the proof of theorem in [1] and a complete proof is given in Section 3. In Section 4, a new class of plateaued functions is proposed. It is proved that these functions are balanced, have high non-linearity, no non-zero linear structures, and the best algebraic degree. Finally, Section 5 concludes the paper.

2 Preliminaries

Let F_2^n be the n-dimensional vector space over the finite field F_2. A Boolean function of n variables is a function from F_2^n into F_2. We denote the set of all n-variable Boolean functions by $\boldsymbol{B}_n$. The addition of integers over R is denoted by $+$ and Σ_i, and over F_2 by $\oplus$ and $\oplus_i$.

Any $f \in \boldsymbol{B}_n$ can be uniquely represented as a multivariate polynomial over F_2, called algebraic normal form (ANF),

$$f(x_1, x_2, \ldots, x_n) = \bigoplus_{u \in F_2^n} \lambda_u \left(\prod_{i=1}^{n} x_i^{u_i} \right)$$

where $\lambda_u \in F_2, u = (u_1, u_2, \cdots, u_n)$. The algebraic degree of f, denoted by deg(f), is the maximal value of $wt(u)$ such that $\lambda_u \neq 0$, where $wt(u)$ denotes the Hamming weight of u. Another basic representation of a Boolean function $f(x_1, \ldots, x_n)$ is by the output column of its truth table, i.e. a binary string of length 2^n,

$$[f(0, \ldots, 0, 0), f(0, \ldots, 0, 1), \ldots, f(1, \ldots, 1, 0), f(1, \ldots, 1, 1)]$$

A Boolean function is affine if there exists no term of degree strictly >1 in the ANF. An affine function with the constant term equal to zero is called a linear function.

Many properties of Boolean function can be deduced from its Walsh spectra, which is defined to be the set of the distinct values of the Walsh transform. The Walsh transform of $f \in \boldsymbol{B}_n$ is an integer valued function over F_2^n defined by

$$W_f(\omega) = \sum_{x \in F_2^n} (-1)^{f(x) \oplus \omega \cdot x}$$

where '·' denotes the standard dot product of two vectors. It satisfies Parseval's relation:

$$\sum_{w \in F_2^n} W_f(\omega)^2 = 2^{2n} \tag{1}$$

The non-linearity of a Boolean function $f \in \boldsymbol{B}_n$, denoted by N_f, is defined as the distance to the set of all affine functions, that is,

$$N_f = \min_{\omega \in F_2^n, a \in F_2} \#\{x \in F_2^n : f(x) \neq \omega \cdot x \oplus a\}$$

For every $f \in \boldsymbol{B}_n$, the non-linearity N_f and its Walsh transform satisfy the relation:

$$N_f = 2^{n-1} - \frac{1}{2} \max_{\omega \in F_2^n} \left| W_f(\omega) \right| \tag{2}$$

Due to Parseval's relation (1), N_f is upper bounded by $2^{n-1} - 2^{n/2-1}$. This bound is tight for every n even and the functions achieving it are called bent.

A Boolean function $f \in \boldsymbol{B}_n$ is balanced if its output column in the truth table contains an equal number of 0 and 1, i.e. $W_f(0) = 0$ or $wt(f) = 2^{n-1}$.

A Boolean function $f \in \boldsymbol{B}_n$ is said to be plateaued if its Walsh spectra $\{W_f(\omega) : \omega \in F_2^n\} \subseteq \{0, \pm 2^r\}$ for some $n/2 \leq r \leq n$. We call 2^r the amplitude of plateaued function and define the set $S(f) = \{\omega \in F_2^n : W_f(w) \neq 0\}$.

For any Boolean function $f \in \boldsymbol{B}_n$, we say that it has a linear structure $a \in F_2^n$ if the value $f(x \oplus a) \oplus f(x)$ is constant for all $x \in F_2^n$. Obviously, $(0, \cdots, 0)$ is always a linear structure, so we usually study non-zero linear structure only. Having any non-zero linear structures is a bad cryptographic property for f.

The autocorrelation function of $f \in \boldsymbol{B}_n$ is an integer valued function over F_2^n defined by

$$\Delta_f(a) = \sum_{x \in F_2^n} (-1)^{f(x) \oplus f(x \oplus a)}$$

It is obvious that $a \in F_2^n$ is a linear structure of f if and only if $\Delta_f(a) = \pm 2^n$.

It is well known that for any $f \in \boldsymbol{B}_n$ and $a \in F_2^n$,

$$\Delta_f(a) = \frac{1}{2^n} \sum_{x \in F_2^n} W_f(x)^2 (-1)^{a \cdot x} \tag{3}$$

The following lemma, given in [11] where bent functions were first introduced, is a main lemma of the paper.

Lemma 1: Let $f(x_1, \dots, x_n) \in \boldsymbol{B}_n$, then the function $f(x_1, \dots, x_n) \oplus \bigoplus_{i=1}^{n} x_i x_{i+n}$ is a bent function in $2n$ variables.

3 Correction of the proof in the reference [1]

In [1], the author puts forward a class of plateaued functions defined as follows.

Definition 1: Let $d \geq 3$, $k \geq 1$, and $f_k(x) = f_{k,d}(x_1, \dots, x_{2dk-1}) \in \boldsymbol{B}_{2dk-1}$, which is given by

$$f_k(x) = \bigoplus_{i=1}^{k} x_{di-(d-1)} x_{di-(d-2)} \cdots x_{di} \oplus \bigoplus_{i=1}^{dk-1} x_i x_{i+dk} \tag{4}$$

When explaining that f_k has no non-zero linear structures, the author mentions that 'since $S(f_k)$ is so large this is impossible unless $a = 0$ '. This is not the right reason why f_k has no non-zero linear structures. Indeed, for most Boolean functions f whose $S(f)$ is large, they can still have non-zero linear structures. Here are two examples.

Example 1: Let $f \in \boldsymbol{B}_3$ be a plateaued function of amplitude 2^2 and

$$f(x_1, x_2, x_3) = x_1 x_3 \oplus x_2 x_3 \oplus x_1 \oplus x_2$$

We have $S(f) = \{(000), (001), (110), (111)\}$. For every $\omega \in S(f)$, we have $\omega \cdot (110) = 0$, then the vector (110) is a linear structure of f.

Example 2: More generally, for any given $i \neq j \in \{1, \dots, n\}$ (n odd), if we let $f \in \boldsymbol{B}_n$ be a plateaued function of amplitude $2^{(n+1)/2}$ and $S(f) = \{\omega \in F_2^n : \omega_i = \omega_j\}$, obviously, $\#S(f) = 2^{n-1}$, then for every $\omega \in S(f)$, we have $\omega \cdot \alpha = 0$ where $\alpha \in F_2^n$, $\alpha_i = \alpha_j = 1$ and $\alpha_k = 0$ for $k \neq i, j$. Thus, the vector α is a linear structure of f.

Now, we give a complete proof in the following two theorems.

Theorem 1: Let the function f_k be defined by (4) and the set

$$\Omega = \{e_1, \dots, e_{dk-1}, e_{dk+1}, \dots, e_{2dk-1}, (1, \dots, 1)\}$$

where e_i has its only non-zero value 1 at position i, then $\Omega \subset S(f_k)$.

Proof: Let the function

$$pk(x) = \bigoplus_{i=1}^{k} x_{di-(d-1)} x_{di-(d-2)} \cdots x_{di}$$

$$q_{dk-1}(x) = \bigoplus_{i=1}^{dk-1} x_i x_{i+dk}$$

Then for any $a = (a_1, \dots, a_{2dk-1}) \in \Omega$, we have

$$\begin{aligned} W_{f_k}(a) &= \sum_{x \in F_2^{2dk-1}} (-1)^{p_k(x) \oplus q_{dk-1}(x) \oplus a \cdot x} \\ &= \sum_{x \in F_2^{2dk-1}, x_{dk}=0} (-1)^{p_k(x) \oplus q_{dk-1}(x) \oplus a' \cdot x'} + (-1)^{a_{dk}} \\ &\quad \times \sum_{x \in F_2^{2dk-1}, x_{dk}=1} (-1)^{p_{k-1}(x) \oplus q_{dk-1}(x) \oplus a' \cdot x' \oplus x_{dk-(d-1)} \cdots x_{dk-1}} \\ &\triangleq W_1 + (-1)^{a_{dk}} W_2 \end{aligned}$$

, where

$$\begin{aligned} a' \cdot x' = a_1 \cdot x_1 \oplus \cdots \oplus a_{dk-1} \cdot x_{dk-1} \oplus a_{dk+1} \cdot x_{dk+1} \\ \oplus \cdots \oplus a_{2dk-1} \cdot x_{2dk-1}. \end{aligned}$$

According to Lemma 1, $p_{k-1}(x) \oplus q_{dk-1}(x)$ and $p_{k-1}(x) \oplus q_{dk-1}(x) \oplus x_{dk-(d-1)} \cdots x_{dk-1}$ are bent functions in $2dk-2$ variables, then $W_1 = \pm 2^{dk-1}$ and $W_2 = \pm 2^{dk-1}$.

Let $(y_1, y_2, y_3, y_4) \in F_2^{2dk-2}$, where $y_1 = (x_1, \dots, x_{dk-d})$, $y_2 = (x_{dk-(d-1)}, \dots, x_{dk-1})$, $y_3 = (x_{dk+1}, \dots, x_{2dk-d})$ and $y_4 = (x_{2dk-(d-1)}, \dots, x_{2dk-1})$. We divide the set into two sets $\Omega \setminus \{(1, \cdots 1)\}$ and $\{(1, \cdots 1)\}$.

(1) $a \in \Omega \setminus \{(1, \cdots 1)\}$ For any $a \in \Omega \setminus \{(1, \cdots 1)\}$, we have

$$\begin{aligned} W_2 &= \sum_{x \in F_2^{2dk-1}, (y_2, x_{dk}) \neq (1, \cdots, 1)} (-1)^{p_{k-1}(x) \oplus q_{dk-1}(x) \oplus a' \cdot x'} \\ &\quad - \sum_{x \in F_2^{2dk-1}, (y_2, x_{dk}) = (1, \dots, 1)} (-1)^{p_{k-1}(x) \oplus q_{dk-1}(x) \oplus a' \cdot x'} \\ &= \sum_{x \in F_2^{2dk-1}, x_{dk}=1} (-1)^{p_{k-1}(x) \oplus q_{dk-1}(x) \oplus a' \cdot x'} \\ &\quad -2 \sum_{x \in F_2^{2dk-1}, (y_2, x_{dk}) = (1, \dots, 1)} (-1)^{p_{k-1}(x) \oplus q_{dk-1}(x) \oplus a' \cdot x'} \\ &= \sum_{x \in F_2^{2dk-1}, x_{dk}=1} (-1)^{p_{k-1}(x) \oplus q_{dk-1}(x) \oplus a' \cdot x'} \\ &\quad -2 \sum_{x \in F_2^{2dk-1}, (y_2, x_{dk}) = (1, \dots, 1)} (-1)^{r(x)} \end{aligned}$$

where $r(x) = p_{k-1}(x) \oplus q_{dk-d}(x) \oplus x_{2dk-(d-1)} \oplus \cdots \oplus x_{2dk-1} \oplus a' \cdot x'$. Since $d \geq 3, d-1 \geq 2 > 1 = wt(a) = wt(a')$, we have $r(x)$ is balanced. Thus, we have

$$\begin{aligned} W_2 &= \sum_{x \in F_2^{2dk-1}, x_{dk}=1} (-1)^{p_{k-1}(x) \oplus q_{dk-1}(x) \oplus a' \cdot x'} \\ &= \sum_{x \in F_2^{2dk-1}, x_{dk}=0} (-1)^{p_{k-1}(x) \oplus q_{dk-1}(x) \oplus a' \cdot x'} \\ &= W_1 \end{aligned}$$

and $W_{f_k}(a) = W_1 + W_2 = \pm 2^{dk}$.

(2) $a = (1, \dots, 1)$ Let $g(y_1, y_3) \in B_{2d-2}$, $h(y_2, y_4) \in B_{2d-2}$ and

$$\begin{aligned} g(y_1, y_3) &= p_{k-1}(x) \oplus q_{dk-d}(x) \\ h(y_2, y_4) &= x_{dk-(d-1)} \oplus \cdots \oplus x_{dk-1} \oplus x_{2dk-(d-1)} \oplus \cdots \\ &\quad \oplus x_{2dk-1} \oplus \bigoplus_{i=dk-(d-1)}^{dk-1} x_i x_{i+dk} \end{aligned}$$

Then, we have

$$
\begin{aligned}
W_1 = &\sum_{(y_1, y_3) \in F_2^{2dk-2d}} (-1)^{g(y_1, y_3) \oplus x_1 \oplus \cdots \oplus x_{dk-d} \oplus x_{dk+1} \oplus \cdots \oplus x_{2dk-1}} \\
&\times \sum_{(y_2, y_4) \in F_2^{2d-2}} (-1)^{h(y_2, y_4)}
\end{aligned}
$$

$$
\begin{aligned}
W_2 = &\sum_{(y_1, y_3) \in F_2^{2dk-2d}} (-1)^{g(y_1, y_3) \oplus x_1 \oplus \cdots \oplus x_{dk-d} \oplus x_{dk+1} \oplus \cdots \oplus x_{2dk-1}} \\
&\times \sum_{(y_2, y_4) \in F_2^{2d-2}} (-1)^{h(y_2, y_4) \oplus x_{dk-(d-1)} \cdots x_{dk-1}}
\end{aligned}
$$

and

$$
\begin{aligned}
&\sum_{(y_2, y_4) \in F_2^{2d-2}} (-1)^{h(y_2, y_4) \oplus x_{dk-(d-1)} \cdots x_{dk-1}} \\
&= \sum_{y_4 \in F_2^{d-1}, y_2 \neq 1(1, \cdots, 1)} (-1)^{h(y_2, y_4)} \\
&\quad - \sum_{y_4 \in F_2^{d-1}, y_2 = 1(1, \cdots, 1)} (-1)^{h(y_2, y_4)} \\
&= \sum_{(y_2, y_4) \in F_2^{2d-2}} (-1)^{h(y_2, y_4)} \\
&\quad -2 \sum_{y_4 \in F_2^{d-1}, y_2 = 1(1, \cdots, 1)} (-1)^{h(y_2, y_4)} \\
&= \prod_{j = dk-(d-1)}^{dk-1} \sum_{(x_j, x_{j+dk}) \in F_2^2} (-1)^{x_j x_{j+dk} \oplus x_j \oplus x_{j+dk}} \\
&\quad -2 \prod_{j = dk-(d-1)}^{dk-1} \sum_{(x_j, x_{j+dk}) \in F_2} (-1)^{x_j x_{j+dk} \oplus 1 \oplus x_{j+dk}} \\
&= (-1)^{d-1} 2^{d-1} - 2(-1)^{d-1} 2^{d-1} \\
&= -(-1)^{d-1} 2^{d-1} \\
&= -\sum_{(y_2, y_4) \in F_2^{2d-2}} (-1)^{h(y_2, y_4)}
\end{aligned}
$$

Hence, $W_1 = -W_2$ and $W_{f_k} = W_1 - W_2 = \pm 2^{dk}$.

To sum up, we have $\Omega \subset S(f_k)$. □

Theorem 2: Let the function f_k be defined by (4), then f_k has no non-zero linear structures.

Proof: According to Parseval's relation (1), we have $\#S(f_k) = 2^{2dk-2}$. Let $a \in F_2^{2dk-1}$ be a linear structure of f_k, it follows from the (3) that

$$
\Delta_{f_k}(a) = \frac{2^{2dk}}{2^{2dk-1}} \sum_{u \in S(f_k)} (-1)^{u \cdot a} = 2 \sum_{u \in S(f_k)} (-1)^{u \cdot a}
$$

then we have a is a linear structure of f_k if and only if for every $u \in S(f_k)$, the value $u \cdot a$ is constant (0 or 1). From the reference [1], we know that $(0, \ldots, 0) \in S(f_k)$. Hence, we have a is a linear structure of f_k if and only if for every $u \in S(f_k)$, $u \cdot a = 0$.

According to Theorem 1, $\Omega \subset S(f_k)$. It is obvious that Ω is a basis of F_2^{2dk-1}. Hence, if for every $u \in S(f_k)$, $u \cdot a = 0$, then for every $u \in \Omega$, $u \cdot a = 0$ and we have $a = (0, \ldots, 0)$.

Thus, f_k has no non-zero linear structures. □

Remark 1: From the proof, we can see that the right reason why f_k has no non-zero linear structures is that there exist $2dk - 1$ linearly independent vectors in $S(f_k)$.

4 Improvement of highly non-linear plateaued functions in the reference [1]

It is known that for a plateaued function $f \in \boldsymbol{B}_n$ of amplitude $2^{n - r/2}$, $\deg(f) \le r/2 + 1$ [12]. The algebraic degree of the plateaued functions constructed in [1] is d but not dk. When $k \ge 2$, the algebraic degree is not the best. Here is an improvement.

Theorem3: Let $d \ge 3$, $k \ge 1$ and $h_k(x) = h_{k,d}(x_1, \ldots, x_{2dk-1}) \in \boldsymbol{B}_{2dk-1}$, which is given by

$$
h_k(x) = x_1 \cdots x_{dk} \oplus \bigoplus_{i=1}^{dk-1} x_i x_{i+dk} \tag{5}
$$

Then h_k is a plateaued function of amplitude 2^{dk} and has no non-zero linear structures. In addition, $\deg(h_k) = dk$, $W_{h_k}(0, \ldots, 0) = 2^{dk}$, and $h_k \oplus \bigoplus_{i=1}^{dk-1} x_{i+dk}$ is balanced.

Proof: Obviously, $\deg(h_k) = dk$. Let the function $q_{dk-1}(x) = \bigoplus_{i=1}^{dk-1} x_i x_{i+dk}$, then for any $a \in F_2^{2dk-1}$, we have (see equation below), where

$a' \cdot x' = a_1 \cdot x_1 \oplus \cdots \oplus a_{dk-1} \cdot x_{dk-1} \oplus a_{dk+1} \cdot x_{dk+1} \oplus \cdots.$
$\oplus a_{2dk-1} \cdot x_{2dk-1}$

According to Lemma 1, $q_{dk-1}(x)$ and $q_{dk-1}(x) \oplus x_1 \cdots x_{dk-1}$ are bent functions in $2dk - 2$ variables, then we have $W_{h_k}(a) \in \{0, \pm 2^{dk}\}$, that is, h_k is a plateaued function of amplitude 2^{dk}.

For $a = (0, \ldots, 0)$, we have (see (6)) .

Let $H_k = h_k \oplus \bigoplus_{i=1}^{dk-1} x_{i+dk}$, similarly to (6), we have (see equation below). Hence, H_k is balanced.

Finally, we have the set $\Omega \subset S(h_k)$ (the proof follows the same lines of reasoning as the proof of Theorem 1) and then similarly to Theorem 2, h_k has no non-zero linear structures. □

Remark 2: Compared with [1], Theorem 3 can construct plateaued functions of amplitude $2^{(n+1)/2}$ in n (odd) variables with the best algebraic degree. At the same time, other cryptographic properties can be remained.

5 Conclusion

Plateaued functions with good cryptographic properties have been widely used in cryptography and other fields. This paper corrects the proof in [1] and provides a new class of plateaued functions with the best algebraic degree.

6 Acknowledgment

This work was supported by National Natural Science Foundation of China under Grant N61502532.

$$
\begin{aligned}
W_{h_k}(a) &= \sum_{x \in F_2^{2dk-1}} (-1)^{x_1 \cdots x_{dk} \oplus q_{dk-1}(x) \oplus a \cdot x} \\
&= \sum_{x \in F_2^{2dk-1}, x_{dk} = 0} (-1)^{q_{dk-1}(x) \oplus a' \cdot x'} \\
&\quad + (-1)^{a_{dk}} \sum_{x \in F_2^{2dk-1}, x_{dk} = 1} (-1)^{q_{dk-1}(x) \oplus a' \cdot x' \oplus x_1 \cdots x_{dk-1}}
\end{aligned}
$$

$$
\begin{aligned}
W_{h_k}(0,\ldots,0) &= \sum_{x \in F_2^{2dk-1}} (-1)^{x_1 \cdots x_{dk} \oplus q_{dk-1}(x)} \\
&= \sum_{x \in F_2^{2dk-1}, x_{dk}=0} (-1)^{q_{dk-1}(x)} \\
&\quad + \sum_{x \in F_2^{2dk-1}, x_{dk}=0} (-1)^{x_1 \cdots x_{dk-1} \oplus q_{dk-1}(x)} \\
&= \sum_{x \in F_2^{2dk-1}, x_{dk}=0} (-1)^{q_{dk-1}(x)} \\
&\quad + \sum_{x \in F_2^{2dk-1}, x_{dk}=1, x_1 \cdots x_{dk-1}=0} (-1)^{q_{dk-1}(x)} \\
&\quad - \sum_{x \in F_2^{2dk-1}, x_{dk}=1, x_1 \cdots x_{dk-1}=1} (-1)^{q_{dk-1}(x)} \\
&= \sum_{x \in F_2^{2dk-1}, x_{dk}=0} (-1)^{q_{dk-1}(x)} + \sum_{x \in F_2^{2dk-1}, x_{dk}=1} (-1)^{q_{dk-1}(x)} \\
&\quad -2 \sum_{x \in F_2^{2dk-1}, x_{dk}=1, x_1 \cdots x_{dk-1}=1} (-1)^{q_{dk-1}(x)} \\
&= \sum_{x \in F_2^{2dk-1}} (-1)^{q_{dk-1}(x)} \\
&\quad -2 \sum_{(x_{1+dk}, \ldots, x_{2dk-1}) \in F_2^{dk-1}} (-1)^{x_{1+dk} \oplus \cdots \oplus x_{2dk-1}} \\
&= 2 \prod_{i=1}^{dk-1} \sum_{(x_i, x_{i+dk}) \in F_2^2} (-1)^{x_i x_{i+dk}} \\
&= 2^{dk}
\end{aligned} \tag{6}
$$

$$
\begin{aligned}
W_{H_k}(0,\ldots,0) &= \sum_{x \in F_2^{2dk-1}} (-1)^{H_k(x)} \\
&= \sum_{x \in F_2^{2dk-1}} (-1)^{q_{dk-1}(x) \oplus \bigoplus_{i=1}^{dk-1} x_{i+dk}} \\
&\quad -2 \sum_{(x_{1+dk}, \ldots, x_{2dk-1}) \in F_2^{dk-1}} (-1)^{x_{1+dk} \oplus \cdots \oplus x_{2dk-1} \oplus \bigoplus_{i=1}^{dk-1} x_{i+dk}} \\
&= 2 \prod_{i=1}^{dk-1} \sum_{(x_i, x_{i+dk}) \in} (-1)^{x_i x_{i+dk} \oplus x_{i+dk}} - 2 \times 2^{dk-1} \\
&= 2 \times 2^{dk-1} - 2 \times 2^{dk-1} \\
&= 0
\end{aligned}
$$

7 References

[1] Cusick, T.W.: 'Highly nonlinear plateaued functions', *IET Inf. Sec.*, 2017, **11**, (2), pp. 78–81

[2] Carlet, C.: 'Partially-bent functions', *Des. Codes Cryptogr.*, 1993, **3**, (2), pp. 135–145

[3] Zheng, Y., Zhang, X.M.: 'Plateaued functions'. Int. Conf. on Information and Communications Security, Berlin, Heidelberg, November 1999, pp. 284–300

[4] Camion, P., Carlet, C., Charpin, P., *et al.*: 'On correlation-immune functions'. Int. Cryptology Conf. on Advances in Cryptology, California, USA, August 1991, pp. 86–100

[5] Carlet, C.: 'A large class of cryptographic boolean functions via a study of the marorana-McFarland construction'. Int. Cryptology Conf. on Advances in Cryptology, California, USA, August 2002, pp. 549–564

[6] Carlet, C., Prouff, E.: 'On plateaued functions and their construction'. Fast Software Encryption, Lund, Sweden, February 2003, pp. 54–73

[7] Wang, W.Q., Xiao, G.Z.: 'Decomposition and construction of plateaued functions', *Chin. J. Electron.*, 2009, **18**, (4), pp. 686–688

[8] Zhang, F.R., Carlet, C., Hu, Y.P., *et al.*: 'New secondary constructions of bent functions', *Adv. Math. Commun.*, 2012, **27**, (5), pp. 413–434

[9] Zhang, F.R., Carlet, C., Hu, Y.P., *et al.*: 'Secondary constructions of highly nonlinear boolean functions and disjoint spectra plateaued functions', *Inf. Sci.*, 2014, **283**, pp. 94–106

[10] Hyun, J.Y., Lee, J., Lee, Y.: 'Explicit criteria for construction of plateaued functions', *IEEE Trans. Inf. Theory*, 2016, **62**, (12), pp. 7555–7565

[11] Zheng, Y., Zhang, X.M.: 'On plateaued functions', *IEEE Trans. Inf. Theory*, 2001, **47**, (3), pp. 1215–1223

[12] Rothaus, O.: 'On 'bent' functions', *J. Comb. Theory*, 1976, **20**, (3), pp. 300–305