# On the (Fast) Algebraic Immunity of Boolean Power Functions

DU Yusong[1*], WEI Baodian[2], ZHANG Fangguo[2] & ZHANG Huang[2]

[1]*School of Information Management, Sun Yat-sen University, Guangzhou* 510006*, China;*
[2]*School of Information Science and Technology, Sun Yat-sen University, Guangzhou* 510006*, China*

**Abstract** The (fast) algebraic immunity, including (standard) algebraic immunity and the resistance against fast algebraic attacks, has been considered as an important cryptographic property for Boolean functions used in stream ciphers. This paper is on the determination of the (fast) algebraic immunity of a special class of Boolean functions, called Boolean power functions. An $n$-variable Boolean power function $f$ can be represented as a monomial trace function over finite field $\mathbb{F}_{2^n}$, $f(x) = Tr_1^n(\lambda x^k)$, where $\lambda \in \mathbb{F}_{2^n}$ and $k$ is the coset leader of cyclotomic coset $C_k$ modulo $2^n - 1$. To determine the (fast) algebraic immunity of Boolean power functions one may need the arithmetic in $\mathbb{F}_{2^n}$, which may be not computationally efficient compared with the operations over $\mathbb{F}_2$. We prove that if $\lambda = \alpha^k$ and $\alpha$ is a primitive element of $\mathbb{F}_{2^n}$, or $k$ is co-prime to $2^n - 1$, then the (fast) algebraic immunity of Boolean power function $Tr_1^n(\lambda x^k)$ is the same as that of $Tr_1^n(x^k)$. This may help us determine the immunity of some Boolean power functions more efficiently. We show that Niho functions satisfy the co-prime condition, and verify that a number of odd variables Kasami functions also satisfy the co-prime condition.

**Keywords** Boolean function, Boolean power function, fast algebraic attacks, algebraic immunity

## 1 Introduction

Boolean functions used in stream ciphers, especially in the filter and combination generators of stream ciphers based on linear feedback shift registers, should have large algebraic immunity ($\mathcal{AI}$), in order to resist algebraic attacks [1, 2]. They should also have the resistance against fast algebraic attacks (FAA's), because Boolean functions with large algebraic immunity (even the maximum $\mathcal{AI}$) may not resist FAA's [3, 4, 5]. The *(fast) algebraic immunity*, including (standard) algebraic immunity and the resistance against fast algebraic attacks, is considered as an important cryptographic property for Boolean functions used in stream ciphers resisting both algebraic and fast algebraic attacks.

In resent years, more efforts have been made to study the (fast) algebraic immunity of Boolean functions, especially their resistance against FAA's. It was stated that almost all the symmetric Boolean functions including these functions with good algebraic immunity behave badly against FAA's [6]. However, Carlet-Feng function, a class of $n$-variable balanced Boolean functions with the maximum algebraic immunity as well as good nonlinearity [7], was proved to have almost optimal resistance and even optimal resistance against FAA's if $n = 2^s + 1$ exactly with positive integer $s$ [8]. Another class of even $n$-variable balanced Boolean functions with the maximum algebraic immunity and large nonlinearity, called Tang-Carlet function [9], was also proved to have almost optimal resistance [10]. Moreover, the immunity of some rotation symmetric Boolean functions against FAA's was also analyzed [11].

A special class of Boolean functions are called Boolean power functions. An $n$-variable Boolean power function $f$ can be represented as a monomial trace function over finite field $\mathbb{F}_{2^n}$, $f(x) = Tr_1^n(\lambda x^k)$, where $\lambda \in \mathbb{F}_{2^n}$ and $k$ is the coset leader of cyclotomic coset $C_k$ modulo $2^n - 1$. Boolean power functions are widely studied because of their interesting algebraic and combinatorial properties, and their applications in cryptography, coding theory and sequence design. The (fast) algebraic immunity of Boolean power

* Corresponding author (email: duyusong@mail.sysu.edu.cn)

functions also received attention, but mainly on their standard algebraic immunity. In 2006, Y. Nawaz et al. firstly studied the upper bound on the algebraic immunity of Boolean power functions. The upper bounds on the algebraic immunities of inverse functions, Kasami functions and Niho functions, which are typical Boolean power functions, were given respectively [12]. In 2008, V.V. Bayev further analyzed the lower bound on the algebraic immunity of inverse functions ($Tr_1^n(\lambda x^{-1})$, $\lambda \in \mathbb{F}_{2^n}$) [13]. In 2013, D. K. Dalai presented a new technique of computing algebraic immunity by using incidence matrices [14]. On the basis of his experiments, he conjectured the algebraic immunity of inverse functions exactly arrives at the upper bound given by Y. Nawaz et al. Then X. Feng et al. proved that Dalai's conjecture on the bound of inverse functions is correct [15]. They also demonstrated some weak properties of inverse functions against FAA's.

In this paper, we consider the determination of the (fast) algebraic immunity of Boolean power functions, not only their standard algebraic immunity but also their resistance against FAA's. For an $n$-variable Boolean power function $Tr_1^n(\lambda x^k)$ with $1 \neq \lambda \in \mathbb{F}_{2^n}$, to determine its (fast) algebraic immunity one may need the arithmetic in $\mathbb{F}_{2^n}$, which may be not computationally efficient compared with the operations over $\mathbb{F}_2$. Furthermore, the algebraic immunity of inverse function $Tr_1^n(\lambda x^{-1})$ was proven to be the same as that of $Tr_1^n(x^{-1})$ [12]. And thus the studies on inverse functions are essentially the studies on $Tr_1^n(x^{-1})$. We'd like to know whether other Boolean power functions have similar properties, so that one only needs to investigate the immunity of $Tr_1^n(x^k)$ no matter what $\lambda$ equals when he wants to get the knowledge on the immunity of $Tr_1^n(\lambda x^k)$. By discussing the generic method of determining the (fast) algebraic immunity of Boolean power functions, we obtain two sufficient conditions such that the (fast) algebraic immunity of Boolean power function $Tr_1^n(\lambda x^k)$ is the same as that of $Tr_1^n(x^k)$. One is that $\lambda = \alpha^k$ and $\alpha$ is a primitive element of $\mathbb{F}_{2^n}$, the other one is that $k$ is co-prime to $2^n - 1$. Obviously, inverse function $Tr_1^n(x^{-1})$ is a simple instant in the Boolean power functions satisfying the proposed co-prime condition. We also show that Niho functions and verify that a number of odd variables Kasami functions also satisfy the co-prime condition.

## 2 Preliminaries

An $n$-variable Boolean function $f$ can be viewed as a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ and has a unique $n$-variable polynomial representation over $\mathbb{F}_2[x_1, x_2, \cdots, x_n]/(x_1^2 - x_1, x_2^2 - x_2, \cdots, x_n^2 - x_n)$, called the *algebraic normal form* (ANF) of $f$,

$$f(x_1, x_2, \cdots, x_n) = a_0 + \sum_{1 \leqslant i \leqslant n} a_i x_i + \sum_{1 \leqslant i < j \leqslant n} a_{ij} x_i x_j + \cdots + a_{12\cdots n} x_1 x_2 \cdots x_n,$$

where $a_0, a_i, a_{ij}, \ldots, a_{12\cdots n}$ belong to $\mathbb{F}_2$. We denote by $\mathbb{B}_n$ the set of all the $n$-variable Boolean functions.

The algebraic degree of Boolean function $f$, denoted by $\deg(f)$, is the algebraic degree of this polynomial. Boolean functions of degree at most 1 are called *affine functions*.

For $f(x) \in \mathbb{B}_n$, the set of $x = (x_1, x_2, \cdots, x_n) \in \mathbb{F}_2^n$ for which $f(x) = 1$ is called the support of the function, denoted by $\mathrm{supp}(f)$. The Hamming weight of $f$ is the cardinality of $\mathrm{supp}(f)$. Function $f$ is called balanced if its Hamming weight is equal to $2^{n-1}$ exactly.

Let $g \in \mathbb{B}_n$. The Hamming distance of $f$ from $g$ is the Hamming weight of $f + g$. The nonlinearity of $n$-variable function $f$ is its minimum Hamming distance from all the $n$-variable affine functions.

Let $\mathbb{F}_{2^n}$ be the finite field with $2^n$ elements. By identifying the finite field $\mathbb{F}_{2^n}$ with the vector space $\mathbb{F}_2^n$, an $n$-variable Boolean function is a univariate polynomial over $\mathbb{F}_{2^n}$: $f(x) = \sum_{i=0}^{2^n-1} f_i x^i$, where

$f_0$, $f_{2^n-1} \in \mathbb{F}_2$ and $f_{2i} = (f_i)^2 \in \mathbb{F}_{2^n}$, $1 \leqslant i \leqslant 2^n - 2$.

Let $m$ be a divisor of $n$. A trace function $Tr : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^m}$, is given by $Tr_m^n(x) = \sum_{i=0}^{n/m-1} x^{2^{m \cdot i}}$ where $x \in \mathbb{F}_{2^n}$. A cyclotomic coset $C_k$ modulo $2^n - 1$ is defined as $C_k = \{k, k \cdot 2, \cdots, k \cdot 2^{n_k-1}\}$, where $k$ is the coset leader of $C_k$ and $n_k$ is the smallest integer such that $k = k \cdot 2^{n_k} (\mathrm{mod} 2^n - 1)$, i.e., the size of the coset $C_k$. Denote by $\Gamma(n)$ the set of all coset leaders modulo $2^n - 1$.

An $n$-variable Boolean function $f$ using univariate polynomial representation can be further written as a (binary) sum of trace functions:

$$f(x) = \sum_{k \in \Gamma(n)} Tr_1^{n_k}(f_k x^k) + f_{2^n-1} x^{2^n-1}, \quad f_k \in \mathbb{F}_{2^n}, f_{2^n-1} \in \mathbb{F}_2.$$

The algebraic degree of the Boolean function $f$, $\deg(f)$ is given by the largest integer $d = wt_2(k)$ such that $f_k \neq 0$, where $wt_2(k)$ is the number of nonzero coefficients in the binary representation of $k$. In particular, an $n$-variable *Boolean power function* is represented by a monomial or single trace function, i.e.,

$$f(x) = Tr_1^{n_k}(f_k x^k)$$

for some coset leader $k$.

A Boolean function $g \in \mathbb{B}_n$ is called an *annihilator* of $f \in \mathbb{B}_n$ if $fg = 0$. The lowest algebraic degree of all the nonzero annihilators of $f$ and $1 + f$ is called *algebraic immunity* of $f$ or $1 + f$, denoted by $\mathcal{AI}_n(f)$, and it has been proved that $\mathcal{AI}_n(f) \leqslant \lceil \frac{n}{2} \rceil$ for a given $f \in \mathbb{B}_n$ [1, 2, 16]. A Boolean function $f \in \mathbb{B}_n$ has the *maximum algebraic immunity* if $\mathcal{AI}_n(f) = \lceil \frac{n}{2} \rceil$.

Boolean functions with large algebraic immunity can resist (standard) algebraic attacks. but they (even with maximum algebraic immunity) may not resist fast algebraic attacks (FAA's) [3, 4, 5]. For an $n$-variable Boolean function $f$, if there exists a nonzero $n$-variable Boolean function $g$ of low degree such that $fg$ has reasonable algebraic degree (not large with respect to $n$) then a fast algebraic attack is feasible. It was said that $f$ has *optimal resistance against FAA's* if and only if there does not exist a nonzero $n$-variable Boolean function $g$ of degree at most $e$ such that $\deg(g) + \deg(fg) < n$ and $e < \frac{n}{2}$ [7, 18]. Usually, when we consider the resistance of $f$ against FAA's, we need to determine whether

$$\deg(fg) \geqslant n - e$$

holds for any nonzero $n$-variable Boolean function $g$ of degree at most $e$ [17, 18]. Clearly, if it is ture for every positive integer $e$ less than $\frac{n}{2}$ then $f$ has the optimal resistance.

M. Liu et al. further proved that an $n$-variable Boolean function has the optimal resistance against FAA's only if $n = 2^s$ or $n = 2^s + 1$ with positive integer $s$ [8]. For those $n$ and $e$ such that $\deg(fg) \geqslant n - e$ never holds, we can determine whether $\deg(fg) \geqslant n - e - 1$ holds [17, 10]. By convention, $f$ is called a function with *almost optimal resistance* if the inequality holds for every positive integer $e$ less than $\frac{n}{2}$.

**Definition 1.** Let $g$ be a nonzero $n$-variable Boolean function of algebraic degree at most $e$. An $n$-variable Boolean function $f$ has almost optimal resistance against fast algebraic attacks if $\deg(fg) \geqslant n - e - 1$ holds for every positive integer $e$ less than $\frac{n}{2}$, and has the optimal resistance if $\deg(fg) \geqslant n - e$ holds for every positive integer $e$ less than $\frac{n}{2}$.

For simplicity, the algebraic immunity and the resistance against fast algebraic attacks are called the (fast) algebraic immunity of Boolean functions in this paper.

## 3 Determining the (Fast) Algebraic Immunity of Boolean Functions

When deciding the resistance against FAA's, especially for Boolean functions with univariate polynomial representation, the following two sets of integers and a matrix over $\mathbb{F}_{2^n}$ are useful. Denote $\mathcal{W}_e$ by the integer set $\{x \,|\, 0 \leqslant x \leqslant 2^n-1,\, wt_2(x) \leqslant e\}$ and $\overline{\mathcal{W}}_d$ by the integer set $\{x \,|\, 0 \leqslant x \leqslant 2^n-1,\, wt_2(x) \geqslant d+1\}$ where $1 \leqslant e < \lceil \frac{n}{2} \rceil$ and $d < n$. We also need to define the orderings of the integers in $\mathcal{W}_e$ and $\overline{\mathcal{W}}_d$ respectively. Good orderings of these integers may speed up the computation, but do not essentially affect any result on (fast) algebraic immunity.

Let $f, g, h$ be $n$-variable Boolean functions and $g$ be a Boolean function of algebraic degree at most $e$ satisfying that $h = fg$ has algebraic degree at most $d$. Let $f(x) = \sum_{k=0}^{2^n-1} f_k x^k \, (f_k \in \mathbb{F}_{2^n})$ and $h(x) = \sum_{y=0}^{2^n-1} h_y x^y \, (h_y \in \mathbb{F}_{2^n})$ be the univariate polynomial representations of $f$ and $h$ respectively. Function $g$ of degree at most $e$ can be represented as $g(x) = \sum_{z \in \mathcal{W}_e} g_z x^z$, $g_z \in \mathbb{F}_{2^n}$. The algebraic degree of $h = fg$ is at most $d$. For $y \in \overline{\mathcal{W}}_d$ we have $h_y = 0$ and thus

$$0 = h_y = \sum_{\substack{k+z=y \\ z \in \mathcal{W}_e}} f_k g_z = \sum_{z \in \mathcal{W}_e} f_{y-z} g_z,$$

where operation '-' is regarded as the substraction modulo $2^n - 1$. Above equations on $g_z$'s are a homogeneous linear system with $\sum_{i=d+1}^{n} \binom{n}{i}$ equations and $\sum_{i=0}^{e} \binom{n}{i}$ unknowns. Denote by

$$U(f; e, d)$$

the coefficient matrix of these equations about the Boolean funciton $f$, which is a $\sum_{i=d+1}^{n} \times \sum_{i=0}^{e} \binom{n}{i}$ matrix with $ij$-th element equal to

$$u_{yz} = f_{y-z},$$

where $y$ is the $i$-th element in $\overline{\mathcal{W}}_d$ and $z$ is $j$-th element in $\mathcal{W}_e$ .

It is not hard to see and was also shown in [8] that there exists no nonzero function $g$ of degree at most $e$ such that the product $gh$ has degree at most $d$ if and only if matrix $U(f; e, d)$ has full column rank. This means that $\deg(fg) \geqslant d+1$ if matrix $U(f; e, d)$ has full column rank. Therefore, one can determine (almost) optimal resistance by computing the rank of $U(f; e, n-e-1)$ or $U(f; e, n-e-2)$ for all the possible integer $e$.

With above notations, let $f$ be $n$-variable Boolean functions and $g$ be a Boolean function of algebraic degree at most $e$. If $fg = 0$ we have $\sum_{\substack{k+z=y \\ z \in \mathcal{W}_e}} f_k g_z = \sum_{z \in \mathcal{W}_e} f_{y-z} g_z = 0$ for $0 \leqslant y \leqslant 2^n - 1$. This is a homogeneous linear system with $2^n$ equations and $\sum_{i=0}^{e} \binom{n}{i}$ unknowns. Denote by

$$V(f; e)$$

the coefficient matrix, which is a $2^n \times \sum_{i=0}^{e} \binom{n}{i}$ matrix with $ij$-th element equal to $u_{yz} = f_{y-z}$ where $y$ is the $i$-th element in $\{x \,|\, 0 \leqslant x \leqslant 2^n - 1\}$ and $z$ is $j$-th element in $\mathcal{W}_e$. There exists no nonzero function $g$ of degree at most $e$ such that $fg = 0$ if and only if matrix $V(f; e)$ has full column rank. Then one can determine whether $\mathcal{AI}_n(f) > e$ by computing the ranks of $V(f; e)$ and $V(1+f; e)$. In particular, if both $V(f; \lceil \frac{n}{2} \rceil - 1)$ and $V(1+f; \lceil \frac{n}{2} \rceil - 1)$ have full column rank then $f$ must be a function with maximum algebraic immunity.

Matrix $V(f; e)$ and matrix $U(f; e, d)$ have the same structure but different size. Matrix $U(f; e, d)$ are a sub-matrix of $V(f; e)$. The method of determining the algebraic immunity by computing the ranks of $V(f; e)$ and $V(1+f; e)$ is not computationally efficient. But it can help us see some properties of the standard algebraic immunity of Boolean power functions in the next section.

## 4 Determining the (Fast) Algebraic Immunity of Boolean Power Functions

For Boolean power function $f(x) = Tr_1^{n_k}(f_k x^k)$ with $k \in \Gamma(n)$, the entries of matrix $U(f; e, d)$ are in $\mathbb{F}_{2^n}$ and to compute its column rank, $\mathrm{rank}(U(f; e, d))$, maybe not computationally efficient. In this section, if $f(x) = Tr_1^{n_k}(f_k x^k)$ that satisfies specific conditions, we show that one can determine its resistance against FAA's by determining the resistance of its reduced function $r(x) = Tr_1^{n_k}(x^k)$. More precisely, we show that $\mathrm{rank}(U(f; e, d)) = \mathrm{rank}(U(r; e, d))$, i.e., the resistance of $f(x) = Tr_1^{n_k}(f_k x^k)$ is the same as that of $r(x) = Tr_1^{n_k}(x^k)$, if $k$ or $f_k$ satisfies specific conditions. Since $U(r; e, d)$ is a matrix over $\mathbb{F}_2$ its column rank can be determined more efficiently.

Usually we may pay more attention to the ranks of $U(f; e, n-e-1)$ and $U(f; e, n-e-2)$ for positive integer $e$ less than $\frac{n}{2}$. Because it is more interesting for us to determine whether an $n$-variable Boolean function $f$ has optimal or at least almost optimal resistance against FAA's. Recall $1 \leqslant e \leqslant \lceil \frac{n}{2} \rceil - 1$. For $U(f; e, d)$ with $d = n-e-1$ or $d = n-e-2$ we have

$$d + 1 - e \geqslant (n-e-2) + 1 - e = n - 2e - 1 \geqslant n - 2(\lceil \frac{n}{2} \rceil - 1) - 1 \geqslant 0.$$

Therefore, when $d = n-e-1$ or $d = n-e-2$ the weights of the integers in $\overline{\mathcal{W}}_d$ is never less than those of integers in $\mathcal{W}_e$. For $n$-variable Boolean power function $f$ by the following two lemmas we show that $U(f; e, n-e-1)$ or $U(f; e, n-e-2)$ is a zero matrix for some possible $e$ if the algebraic degree of $f$ is not large enough.

**Lemma 1.** If $y \in \overline{\mathcal{W}}_d$ and $z \in \mathcal{W}_e$, then $wt_2(y - z) \geqslant d + 1 - e$, where operation '-' is regarded as the substraction modulo $2^n - 1$.

*Proof.* Let $y = \sum_{i=0}^{n-1} y_i \cdot 2^i$ and $z = \sum_{i=0}^{n-1} z_i \cdot 2^i$, where $y_i, z_i \in \{0, 1\}$ for $0 \leqslant i \leqslant n-1$. Denote by $i_1, i_2, \cdots, i_s$ all the integers in $\{0, 1, 2, \cdots, n-1\}$ such that $i_1 < i_2 < \cdots < i_s$ and $y_{i_1} = z_{i_1} = y_{i_2} = z_{i_2} = \cdots = y_{i_s} = z_{i_s} = 1$, and by $i_{s+1}, i_{s+2}, \cdots, i_n$ the remaining integers in $\{0, 1, 2, \cdots, n-1\}$ such that $i_{s+1} < i_{s+2} < \cdots < i_n$. It is clear $0 \leqslant s \leqslant wt_2(z) \leqslant e$. Then $wt_2(y - \sum_{j=1}^{s} z_{i_j} \cdot 2^{i_j}) \geqslant d + 1 - s$. In particular, if $s = wt_2(z) \leqslant e$ then $wt_2(y - \sum_{j=1}^{s} z_{i_j} \cdot 2^{i_j}) = wt_2(y - z) \geqslant d + 1 - e$ and we are done. Assume that $0 \leqslant s < wt_2(z)$. We define

$$\bar{y} = \sum_{i=0}^{n-1} \bar{y}_i \cdot 2^i = y - \sum_{j=1}^{s} z_{i_j} \cdot 2^{i_j} = \sum_{j=s+1}^{n} y_{i_j} \cdot 2^{i_j} \quad \text{and} \quad \bar{z} = \sum_{i=0}^{n-1} \bar{z}_i \cdot 2^i = \sum_{j=s+1}^{n} z_{i_j} \cdot 2^{i_j}.$$

Since $y - z = \bar{y} - \bar{z}$ and $wt_2(\bar{y}) \geqslant d + 1 - s$ it suffices to show that $wt_2(\bar{y} - \bar{z}) \geqslant wt_2(\bar{y})$.

Denote by $i'_1, i'_2, \cdots i'_t$ all the integers in $\{0, 1, 2, \cdots, n-1\}$ such that $i'_1 < i'_2 < \cdots < i'_t$ and $\bar{y}_{i'_1} = \bar{y}_{i'_2} = \cdots = \bar{y}_{i'_t} = 1$, where $t = wt_2(\bar{y})$. Then $\bar{y}$ can be written as $\bar{y} = \sum_{j=1}^{t} 2^{i'_j}$. Note that $\bar{z}_{i'_1} = \bar{z}_{i'_2} = \cdots = \bar{z}_{i'_t} = 0$. If there does not exist an integer $i'_{t+1} > i'_t$ such that $\bar{z}_{i'_{t+1}} = 1$ and $\bar{y}_{i'_{t+1}} = 0$, then we have $wt_2(\bar{y} - \bar{z})$ is equal to

$$wt_2\left(2^{i'_1} - (\bar{z}_{i'_1 - 1} \cdot 2^{i'_1 - 1} + \cdots + \bar{z}_0)\right) + \sum_{j=2}^{t} wt_2\left(2^{i'_j} - (\bar{z}_{i'_j - 1} \cdot 2^{i'_j - 1} + \cdots + \bar{z}_{i'_{j-1}+1} \cdot 2^{i'_{j-1}+1})\right).$$

We see that $2^{i'_j} - (\bar{z}_{i'_j - 1} \cdot 2^{i'_j - 1} + \cdots + \bar{z}_{i'_{j-1}+1} \cdot 2^{i'_{j-1}+1})$ as well as $2^{i'_1} - (\bar{z}_{i'_1 - 1} \cdot 2^{i'_1 - 1} + \cdots + \bar{z}_0)$ results a positive integer of Hamming weight not less than 1. Thus, $wt_2(\bar{y})$ will not decrease after the subtraction operation. Finally, if there exists an integer $i'_{t+1} > i'_t$ such that $\bar{z}_{i'_{t+1}} = 1$ and $\bar{y}_{i'_{t+1}} = 0$, then $\bar{y} - \bar{z}$ can be implemented by $2^n + \bar{y} - \bar{z} - 1$. It follows that

$$wt_2(\bar{y} - \bar{z}) = wt_2\left(2^n - (\bar{z}_{n-1} \cdot 2^{n-1} + \cdots + \bar{z}_{i'_t + 1} \cdot 2^{i'_t + 1})\right) + wt_2\left(2^{i'_1} - (\bar{z}_{i'_1 - 1} \cdot 2^{i'_1 - 1} + \cdots + \bar{z}_0) - 1\right)$$

$$+\sum_{j=2}^{t} wt_2\left(2^{i'_j}-(\bar{z}_{i'_j-1}\cdot 2^{i'_j-1}+\cdots+\bar{z}_{i'_{j-1}+1}\cdot 2^{i'_{j-1}+1})\right),$$

where

$$wt_2\left(2^n-(\bar{z}_{n-1}\cdot 2^{n-1}+\cdots+\bar{z}_{i'_t+1}\cdot 2^{i'_t+1})\right)\geqslant 1,$$

and

$$wt_2\left(2^{i'_1}-(\bar{z}_{i'_1-1}\cdot 2^{i'_1-1}+\cdots+\bar{z}_0)-1\right)\geqslant 0.$$

This implies that $wt_2(\bar{y})$ will not decrease after the subtraction operation, that is $wt_2(\bar{y}-\bar{z})\geqslant wt_2(\bar{y})$.

By Lemma 1 we see that if $wt_2(k)<d+1-e$ then $f_k$ will not appear as an entry in matrix $U(f;e,d)$. This means that for function $f(x)=Tr_1^{n_k}(f_kx^k)$ and function $r(x)=Tr_1^{n_k}(x^k)$ if $wt_2(k)<d+1-e$ then $U(f;e,d)$ and $U(r;e,d)$ are zero matrices and have trivially the same rank.

Due to this, in fact, it is not necessary for us to discuss the rank of $U(f;e,d)$ with $d=n-e-1$ or $d=n-e-2$ for function $f(x)=Tr_1^{n_k}(f_kx^k)$ if $wt_2(k)<d+1-e$. But for $k\in\Gamma(n)$ such that $wt_2(k)\geqslant d+1-e$ matrix $U(f;e,d)$ always contains $f_k$ as its entries, because we have the following fact.

**Lemma 2.** Let $k\in\Gamma(n)$ such that $wt_2(k)\geqslant d+1-e$. There exist $y\in\overline{\mathcal{W}}_d$ and $z\in\mathcal{W}_e$ such that $y-z=k \bmod (2^n-1)$, that is, matrix $U(f;e,d)$ contains $f_k$ as its entries.

*Proof.* Since $wt_2(k)\geqslant d+1-e$ there exists an integer $i\in(0,2^n-1]$ with $wt_2(i)\leqslant n-(d+1-e)$ such that $(2^n-1)-i=k$. If $wt_2(i)\leqslant e$ then we find a 2-tuple $(y,z)$ with $y=2^n-1\in\overline{\mathcal{W}}_d$ and $z=i\in\mathcal{W}_e$ such that $y-z=k \bmod (2^n-1)$. If $wt_2(i)>e$ then we can find an integer $j\in(0,2^n-1]$ with $wt_2(j)\leqslant n-(d+1-e)-e$ such that $(2^n-1)-j-(i-j)=k$ and $wt_2(i-j)=wt_2(i)-wt_2(j)$. Then we have

$$wt_2(2^n-1-j)\geqslant n-(n-(d+1-e)-e)=d+1,$$

and

$$wt_2(i-j)\leqslant n-(d+1-e)-(n-(d+1-e)-e)=e.$$

Thus, we find a 2-tuple $(y,z)$ with $y=(2^n-1-j)\in\overline{\mathcal{W}}_d$ and $z=(i-j)\in\mathcal{W}_e$ such that $y-z=k \bmod (2^n-1)$. In one word, there always exist $y\in\overline{\mathcal{W}}_d$ and $z\in\mathcal{W}_e$ such that $y-z=k \bmod (2^n-1)$ if $wt_2(k)\geqslant d-e+1$.

Moreover, an interesting fact about the optimal resistance against FAA's, which may be known, can be also explained by Lemma 1.

**Corollary 1.** If $f$ is $n$-variable Boolean function with the optimal resistance against FAA's then $1+f$ is also a function with the optimal resistance.

*Proof.* Except the coefficient of the constant term, all the coefficients of $f$ and $1+f$ are always the same. Note that $d+1-e=(n-e-1)+1-e=n-2e\geqslant n-2\cdot(\lceil\frac{n}{2}\rceil-1)\geqslant 1$ when $d=n-e-1$. By Lemma 1 the coefficients of the constant term of $f$ and $1+f$ will not not appear as entries in $U(f;e,n-e-1)$ and $U(1+f;e,n-e-1)$. Therefore, both $U(f;e,n-e-1)$ and $U(1+f;e,n-e-1)$ have full column rank for every $1\leqslant e\leqslant\lceil\frac{n}{2}\rceil-1$.

Now we consider relation between $U(f;e,d)$ and $U(r;e,d)$ for any possible $e$ and $d$. The idea is based on the following lemma, which may be well-known. Here we give its proof for self-completeness.

**Lemma 3.** For $m\geqslant n$, let $A=(a_{ij})_{m\times n}$ and $B=(b_{ij})_{m\times n}$ be $m\times n$ matrix with $a_{ij}=\beta_i\gamma_jb_{ij}$ and $\beta_i,\gamma_j\neq 0$ for $1\leqslant i\leqslant m, 1\leqslant j\leqslant n$. Then $\mathrm{rank}(A)=n$ if and only if $\mathrm{rank}(B)=n$.

*Proof.* Denote by $\mathrm{diag}(x_1,x_2,\cdots,x_n)$ an $n\times n$ diagonal matrix with diagonal entries $x_1,x_2,\cdots,x_n$. Let $P=\mathrm{diag}(\beta_1,\beta_2,\cdots,\beta_m)$ and $Q=\mathrm{diag}(\gamma_1,\gamma_2,\cdots,\gamma_n)$. Then $\mathrm{rank}(A)=\mathrm{rank}(B)$ follows from $A=PBQ$.

**Theorem 1.** Let $f(x) = Tr_1^{n_k}(f_k x^k)$ be an $n$-variable Boolean power function and $r(x) = Tr_1^{n_k}(x^k)$, where $n_k$ is the size of the cyclotomic coset $C_k$ modulo $2^n - 1$. If $f_k = \alpha^k$ and $\alpha$ is a primitive element of finite field $\mathbb{F}_{2^n}$, then $\text{rank}(U(f; e, d)) = \text{rank}(U(r; e, d))$.

*Proof.* For $1 \leqslant i \leqslant \sum_{i=d+1}^{n} \binom{n}{i}$ and $1 \leqslant j \leqslant \sum_{i=0}^{e} \binom{n}{i}$, we denote by $a_{ij}$ the $ij$-th element of $U(f; e, d)$ and by $b_{ij}$ the $ij$-th element of $U(r; e, d)$. Only $f_k, f_{2k}, \cdots, f_{2^{n_k-1}k}$ are nonzero in the univariate polynomial representation of $f$. According to the definition of matrix $U(f; e, d)$ we have

$$a_{ij} = \begin{cases} f_{2^l k}, \text{ if } (y - z) = 2^l k \bmod (2^n - 1); \\ 0, \quad \text{otherwise.} \end{cases},$$

and

$$b_{ij} = \begin{cases} 1, \text{ if } (y - z) = 2^l k \bmod (2^n - 1); \\ 0, \text{ otherwise.} \end{cases},$$

where $y$ is the $i$-th element in $\overline{\mathcal{W}}_d$, $z$ is $j$-th element in $\mathcal{W}_e$ and $0 \leqslant l \leqslant n_k - 1$. Let $\beta_i = \alpha^y$ and $\gamma_j = \alpha^{-z}$. If $(y - z) = 2^l k \bmod (2^n - 1)$ then

$$a_{ij} = f_{2^l k} = (f_k)^{2^l} = \alpha^{2^l \cdot k} = \alpha^{(y-z)} = \alpha^y \cdot \alpha^{-z} = \beta_i \gamma_j b_{ij},$$

otherwise $a_{ij} = \beta_i \gamma_j b_{ij} = 0$. By Lemma 3 we have $\text{rank}(U(f; e, d)) = \text{rank}(U(r; e, d))$.

Theorem 1 can be directly generalized to a small sub-class of Boolean functions with polynomial trace functions. The result may help us find a few of Boolean functions using the trace representation that have good resistance against FAA's.

**Corollary 2.** Let $\Lambda$ be a subset of $\Gamma(n)$. For $n$-variable Boolean function

$$f(x) = \sum_{k \in \Lambda \subseteq \Gamma(n)} Tr_1^{n_k}(f_k x^k)$$

and its reduced function $r(x) = \sum_{k \in \Lambda \subseteq \Gamma(n)} Tr_1^{n_k}(x^k)$, if $f_k = \alpha^k$ for every $k \in \Lambda$ and $\alpha$ is a primitive element of finite field $\mathbb{F}_{2^n}$, then $\text{rank}(U(f; e, d)) = \text{rank}(U(r; e, d))$.

*Proof.* As the proof of Theorem 1 we let $\beta_i = \alpha^y$ and $\gamma_j = \alpha^{-z}$, where $y$ is the $i$-th element in $\overline{\mathcal{W}}_d$, $z$ is $j$-th element in $\mathcal{W}_e$. If $(y - z) = 2^l k \bmod (2^n - 1)$ for some $k \in \Lambda \subseteq \Gamma(n)$ then $a_{ij} = f_{2^l k} = \alpha^y \cdot \alpha^{-z} = \beta_i \gamma_j b_{ij}$, otherwise $a_{ij} = \beta_i \gamma_j b_{ij} = 0$.

**Theorem 2.** For $n$-variable Boolean power function $f(x) = Tr_1^{n_k}(f_k x^k)$ and $r(x) = Tr_1^{n_k}(x^k)$, if $\gcd(k, 2^n - 1) = 1$ then $\text{rank}(U(f; e, d)) = \text{rank}(U(r; e, d))$.

*Proof.* Suppose that $f_k = \alpha^\lambda$ with $0 \leqslant \lambda \leqslant 2^n - 2$ and $\alpha$ is a primitive element of $\mathbb{F}_{2^n}$. Since $\gcd(k, 2^n - 1) = 1$ we let $l = k^{-1} \cdot \lambda \bmod (2^n - 1)$. Denote by $a_{ij}$ the $ij$-th element of $U(f; e, d)$ and by $b_{ij}$ the $ij$-th element of $U(r; e, d)$. Let $\beta_i = \alpha^{l \cdot y}$ and $\gamma_j = \alpha^{-l \cdot z}$. For $0 \leqslant s \leqslant n_k - 1$ if $(y - z) = 2^s k \bmod (2^n - 1)$ then

$$a_{ij} = f_{2^s k} = (f_k)^{2^s} = \alpha^{\lambda \cdot 2^s} = \alpha^{(k^{-1}\lambda) \cdot 2^s k} = \alpha^{l \cdot (y-z)} = \alpha^{l \cdot y} \cdot \alpha^{-l \cdot z} = \beta_i \gamma_j b_{ij},$$

otherwise $a_{ij} = \beta_i \gamma_j b_{ij} = 0$, where $y$ is the $i$-th element in $\overline{\mathcal{W}}_d$ and $z$ is $j$-th element in $\mathcal{W}_e$. Therefore we have $\text{rank}(U(f; e, d)) = \text{rank}(U(r; e, d))$ by Lemma 3.

Before the end of this section, we consider the standard algebraic immunity of $n$-variable Boolean power function $f(x) = Tr_1^{n_k}(f_k x^k)$ via matrix $V(f; e)$ and matrix $V(1 + f; e)$. We have the following result, which can be seen as a corollary of Theorem 1 and Theorem 2. And the conclusion is that the standard algebraic immunity of $f(x) = Tr_1^{n_k}(f_k x^k)$ is the same as that of function $r(x) = Tr_1^{n_k}(x^k)$ if $f_k = \alpha^k$ and $\alpha$ is a primitive element of finite field $\mathbb{F}_{2^n}$, or if $\gcd(k, 2^n - 1) = 1$.

**Corollary 3.** For $n$-variable Boolean power function $f(x) = Tr_1^{n_k}(f_k x^k)$ and $r(x) = Tr_1^{n_k}(x^k)$, If $f_k = \alpha^k$ and $\alpha$ is a primitive element of finite field $\mathbb{F}_{2^n}$, or if $\gcd(k, 2^n - 1) = 1$, then $\text{rank}(V(f; e)) = \text{rank}(V(r; e))$ and $\text{rank}(V(1 + f; e)) = \text{rank}(V(1 + r; e))$.

The proof procedures of Theorem 1 and Theorem 2 still work for Corollary 3 except the difference that $y$ in the proof is the $i$-th element in $\{x \,|\, 0 \leqslant x \leqslant 2^n - 1\}$ rather than the $i$-th element in $\overline{\mathcal{W}}_d$.

## 5 On Inverse functions, Kasami functions and Niho functions

As the applications of Theorem 2, we consider three classes of Boolean power functions. They are famous inverse functions, Kasami functions and Niho functions. Inverse functions, firstly introduced by K. Nyberg [19], were adopted in many symmetric algorithms, such as block cipher AES [20] and stream cipher SNOW [21]. Kasami functions and Niho functions are classic bent or almost bent functions, that have very large nonlinearity [22, 23, 24].

Let $\lambda \in \mathbb{F}_{2^n}$. An $n$-variable inverse function can be defined as $f(x) = Tr_1^n(\lambda x^{-1})$. An $n$-variable Kasami function can be written as $f(x) = Tr_1^n(\lambda x^{2^{2t}-2^t+1})$ where $1 \leqslant t \leqslant \lfloor n/2 \rfloor$ and $\gcd(t, n) = 1$. For odd integer $n = 2t + 1$, an $n$-variable Niho function can be defined as

$$f(x) = \begin{cases} Tr_1^n(\lambda x^{2^t+2^{\frac{t}{2}}-1}) & t \text{ even} \\ Tr_1^n(\lambda x^{2^t+2^{\frac{3t+1}{2}}-1}) & t \text{ odd} \end{cases}.$$

For inverse functions, since $Tr_1^n(\lambda x^{-1}) = Tr_1^n(\lambda x^{2^n-2})$ and $\gcd(2^n - 2, 2^n - 1) = 1$, applying Theorem 2 (and Corollary 3), one can directly see the fact that the (fast) algebraic immunity of $f(x) = Tr_1^n(\lambda x^{-1})$ is the same as that of $r(x) = Tr_1^n(x^{-1})$. It was also shown in [13] that $Tr_1^n(\lambda x^{-1})$ and $Tr_1^n(x^{-1})$ have the same algebraic immunity. It is a simple special case of the fact we obtain. Furthermore, we also show the following three propositions related to Niho exponent and Kasami exponent.

**Proposition 1.** Let $n = 2t + 1$. If $t$ is even then $\gcd(2^t + 2^{\frac{t}{2}} - 1, 2^n - 1) = 1$.

*Proof.* For $t = 2, 4, 6, 8$ it can be verified directly that $\gcd(2^t + 2^{\frac{t}{2}} - 1, 2^n - 1) = 1$. For even $t > 8$ applying the Euclidean algorithm, we have

$$\begin{aligned} 2^n - 1 &= (2^{t+1} - 2^{\frac{t}{2}+1} + 3) \cdot (2^t + 2^{\frac{t}{2}} - 1) + (2^t - 2^{\frac{t}{2}} + 2) \\ 2^t + 2^{\frac{t}{2}} - 1 &= 1 \cdot (2^t - 2^{\frac{t}{2}} + 2) + (2^{\frac{t}{2}+1} - 3) \\ 2^t - 2^{\frac{t}{2}} + 2 &= 2^{\frac{t}{2}-1} \cdot (2^{\frac{t}{2}+1} - 3) + (2^{\frac{t}{2}-1} + 2) \\ 2^{\frac{t}{2}+1} - 3 &= 3 \cdot (2^{\frac{t}{2}-1} + 2) + (2^{\frac{t}{2}-1} - 9) \\ 2^{\frac{t}{2}-1} + 2 &= 1 \cdot (2^{\frac{t}{2}-1} - 9) + 11, \end{aligned}$$

Above equations mean that

$$\gcd(2^t + 2^{\frac{t}{2}} - 1, 2^n - 1) = \gcd(2^{\frac{t}{2}-1} - 9, 11).$$

We see that $\gcd(2^{\frac{t}{2}-1} - 9, 11) = 1$ if and only if $(2^{\frac{t}{2}-1}) \bmod 11 \neq 9$. But 2 power of any positive integer modulo 11 never results a number with factor 3. Therefore $(2^{\frac{t}{2}-1}) \bmod 11 \neq 9$ and $\gcd(2^t + 2^{\frac{t}{2}} - 1, 2^n - 1) = \gcd(2^{\frac{t}{2}-1} - 9, 11) = 1$ holds for any even $t > 8$.

**Proposition 2.** Let $n = 2t + 1$. If $t$ is odd then $\gcd(2^t + 2^{\frac{3t+1}{2}} - 1, 2^n - 1) = 1$.

*Proof.* For $t = 1$ it can be verified directly that $\gcd(2^t + 2^{\frac{3t+1}{2}} - 1, 2^n - 1) = 1$. For $t \geqslant 3$ applying the Euclidean algorithm, we have

$$\begin{aligned} 2^n - 1 &= (2^{\frac{t+1}{2}} - 1) \cdot (2^t + 2^{\frac{3t+1}{2}} - 1) + (2^t + 2^{\frac{t+1}{2}} - 2) \\ 2^t + 2^{\frac{3t+1}{2}} - 1 &= (2^{\frac{t+1}{2}} - 1) \cdot (2^t + 2^{\frac{t+1}{2}} - 2) + 3 \cdot (2^{\frac{t+1}{2}} - 1) \end{aligned}$$

Above two equations imply that

$$\gcd(2^t + 2^{\frac{3t+1}{2}} - 1, 2^n - 1) = \gcd(2^t + 2^{\frac{t+1}{2}} - 2, 3 \cdot (2^{\frac{t+1}{2}} - 1)).$$

Note that $\gcd(2^t + 2^{\frac{t+1}{2}} - 2, 2^{\frac{t+1}{2}} - 1) = \gcd(2^t - 1, 2^{\frac{t+1}{2}} - 1) = 2^{\gcd(t, \frac{t+1}{2})} - 1 = 1$. Thus

$$\gcd(2^t + 2^{\frac{3t+1}{2}} - 1, 2^n - 1) = \gcd(2^t + 2^{\frac{t+1}{2}} - 2, 3).$$

We can see that $2^t \bmod 3 = 2$ and $2^{\frac{t+1}{2}} \bmod 3 = 1, 2$ for any odd $t$, which mean that $(2^t + 2^{\frac{t+1}{2}} - 2) \bmod 3 \neq 0$ and $\gcd(2^t + 2^{\frac{3t+1}{2}} - 1, 2^n - 1) = \gcd(2^t + 2^{\frac{t+1}{2}} - 2, 3) = 1$.

**Proposition 3.** If $n$ is odd then $\gcd(2^{n-1} - 2^{\frac{n-1}{2}} + 1, 2^n - 1) = 1$.

*Proof.* It can be shown that $\gcd(2^{n-1} - 2^{\frac{n-1}{2}} + 1, 2^n - 1) = \gcd(2^{\frac{n-3}{2}} + 1, 7) = 1$ by the Euclidean algorithm. We need to see that $2^{\frac{n-3}{2}} \neq 6 \bmod 7$, because 2 power of any positive integer modulo 7 never results a number with factor 3.

By Proposition 1 and Proposition 2, we see that an $n$-variable Niho function has the same (fast) algebraic immunity as that of $Tr_1^n(x^{2^t + 2^{\frac{t}{2}} - 1})$ or $Tr_1^n(x^{2^t + 2^{\frac{3t+1}{2}} - 1})$ respectively. By Proposition 3 we see that an odd $n$-variable Kasami function of algebraic degree $\frac{n+1}{2}$ has the same (fast) algebraic immunity as that of $Tr_1^n(x^{2^{n-1} - 2^{\frac{n-1}{2}} + 1})$.

As a matter of fact, one can also quickly check the (non-)coprimality between $2^{2t} - 2^t + 1$ and $2^n - 1$ for odd $n$ and $1 \leqslant t \leqslant \lfloor n/2 \rfloor$. We've verified by a computer that a large number of Kasami functions in odd variables satisfy the co-prime condition of Theorem 2. More precisely, we are not able to find a Kasami function in odd $n$ variables that does not satisfy the co-prime condition up to $n = 9999$.

On the contrary, unfortunately, all the Kasami functions in even variables can not satisfy the co-prime condition. This is because $2^{2t} - 2^t + 1 \equiv 2^n - 1 \equiv 0 \bmod 3$ if $n$ is even and $t$ is odd, i.e., $\gcd(2^{2t} - 2^t + 1, 2^n - 1) = \gcd(2^{2t} - 2^t + 1, 2^{n-3t} + 1) \geqslant 3 \neq 1$.

## 6 Conclusion

In this paper, we discuss the relation between the (fast) algebraic immunity of $f(x) = Tr_1^{n_k}(\lambda x^k)$ and that of its reduced function $r(x) = Tr_1^{n_k}(x^k)$. We provide two sufficient conditions such that the (fast) algebraic immunity of Boolean power function $Tr_1^{n_k}(\lambda x^k)$ is the same as that of $Tr_1^{n_k}(x^k)$. This may help us determine the immunity of some Boolean power functions more efficiently.

## References


[1] Courtois N, Meier W. Algebraic attacks on stream ciphers with linear feedback. In: Advances in Cryptology - EUROCRYPT 2003. Heidelberg: Springer, LNCS, 2003, vol. 2729, 345-359.

[2] Meier W, Pasalic E, Carlet C. Algebraic attacks and decomposition of Boolean functions. In: Advances in Cryptology - EUROCRYPT 2004. Heidelberg: Springer, 2004, LNCS, vol. 3027, 474-491.

[3] Courtois N. Fast algebraic attacks on stream ciphers with linear feedback. In: CRYPTO 2003. Heidelberg: Springer, 2003, LNCS, vol. 2729, 176-194.

[4] Armknecht F. Improving fast algebraic attacks. In: FSE 2004. Heidelberg: Springer, LNCS, vol. 3017, 65-82.

[5] Courtois N. Cryptanalysis of SFINKS. In: ICISC 2005, Heidelberg: Springer, 2006, LNCS, vol. 3935, 261-269.

[6] Liu M, Lin D. Fast Algebraic Attacks and Decomposition of Symmetric Boolean Functions. IEEE Transactions on Information Theory, 2011, 57(7), 4817-4821.

[7] Carlet C, Feng K. An Infinite Class of Balanced Functions with Optimal Algebraic Immunity, Good Immunity to Fast Algebraic Attacks and Good Nonlinearity. In: Advances in Cryptology - ASIACRYPT 2008, Heidelberg: Springer, 2008, LNCS, vol. 5350, 425-440,

[8] Liu M, Zhang Y, Lin D. Perfect Algebraic Immune Functions. In: ASIACRYPT 2012. Heidelberg: Springer, 2012, LNCS, vol. 7658, 172-189.

[9] Tang D, Carlet C, Tang X. Highly Nonlinear Boolean Functions With Optimal Algebraic Immunity and Good Behavior Against Fast Algebraic Attacks. IEEE Transactions on Information Theory, 2013, 59(1): 653-664.

[10] Liu M, Lin D. Almost perfect algebraic immune functions with good nonlinearity. In: International Symposium on Information Theory, ISIT 2014. New York: IEEE, 2014, 1837-1841.

[11] Zhang Y, Liu M, Lin D. On the immunity of rotation symmetric Boolean functions against fast algebraic attacks. Discrete Applied Mathematics, 2014, 162: 17-27.

[12] Nawaz Y, Gong G, Gupta K C. Upper bounds on algebraic immunity of Boolean power functions. In: FSE 2006. Heidelberg: Springer, 2006, LNCS, vol. 4047, 375-389.

[13] Bayev V V. Some lower bounds on the algebraic immunity of functions given by their trace forms. Problems of Information Transmission, 2008, 44(3), 243- 265, 2008.

[14] Dalai D K. Computing the rank of incidence matrix and algebraic immunity of Boolean functions. http://eprint.iacr.org/2013/273.pdf.

[15] Feng X, Gong G. On Algebraic Immunity of Trace Inverse Functions over Finite Fields with Characteristic Two. http://eprint.iacr.org/2013/585.pdf

[16] Carlet C, Dalai D K. Gupta K C, Maitra S. Algebraic Immunity for Cryptographically Significant Boolean Functions: Analysis and Construction. IEEE Transactions on Information Theory, 2006, 52(7), 3105-3121.

[17] Pasalic E. Almost Fully Optimized Infinite Classes of Boolean Functions Resistant to (Fast) Algebraic Cryptanalysis. In: ICISC 2008. Heidelberg: Springer, 2009, LNCS, vol. 5461, 399-414.

[18] Du Y, Zhang F, Liu M. On the Resistance of Boolean Functions against Fast Algebraic Attacks. In: ICISC 2011. Heidelberg: Springer, 2012, LNCS, vol. 7259, 261-274.

[19] Nyberg K. Differentially uniform mappings for cryptography. In: EUROCRYPT'93, Heidelberg: Springer, 1994, LNCS, vol. 765, 55-64.

[20] Daemen J, Rijmen V. The Design of Rijndael, Springer-Verlag, 2002.

[21] Ekdahl P, Johansson T. A new version of the stream cipher SNOW, In: SAC 2002, Heidelberg: Springer, 2003, LNCS, vol. 2595, 47-61.

[22] Kasami T. The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes. Information and Control, 1971, 18(4), 369-394.

[23] Langevina P, Leander G. Monomial bent functions and Stickelberger's theorem. Finite Fields and Their Applications, 2008, 14(3), 727-742.

[24] Hollmann H, Xiang Q. A Proof of the Welch and Niho Conjectures on Cross-Correlations of Binary m-Sequences. Finite Fields and Their Applications 2001, 7(2), 253-286.